SY0-701.prepaway.premium.exam.156q

Number: SY0-701
Passing Score: 800
Time Limit: 120 min
File Version: 3.0

SY0-701

Security+ (Plus) Certification

Version 3.0

Exam A

QUESTION 1
Which of the following threat actors is the most likely to be hired by a foreign government to attack critical systems located in other countries?

A. Hacktivist
B. Whistleblower
C. Organized crime
D. Unskilled attacker

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which of the following is used to add extra complexity before using a one-way data transformation algorithm?

A. Key stretching
B. Data masking
C. Steganography
D. Salting

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
An employee clicked a link in an email from a payment website that asked the employee to update contact information. The employee entered the log-in information but received a “page not found” error message. Which of the following types of social engineering attacks occurred?

A. Brand impersonation
B. Pretexting
C. Typosquatting
D. Phishing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
An enterprise is trying to limit outbound DNS traffic originating from its internal network. Outbound DNS requests will only be allowed from one device with the IP address 10.50.10.25. Which of the following firewall ACLs will accomplish this goal?

A. Access list outbound permit 0.0.0.0/0 0.0.0.0/0 port 53
Access list outbound deny 10.50.10.25/32 0.0.0.0/0 port 53

B. Access list outbound permit 0.0.0.0/0 10.50.10.25/32 port 53
Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53

C. Access list outbound permit 0.0.0.0/0 0.0.0.0/0 port 53
Access list outbound deny 0.0.0.0/0 10.50.10.25/32 port 53

D. Access list outbound permit 10.50.10.25/32 0.0.0.0/0 port 53
Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
A data administrator is configuring authentication for a SaaS application and would like to reduce the number of credentials employees need to maintain. The company prefers to use domain credentials to access new SaaS applications. Which of the following methods would allow this functionality?

A. SSO
B. LEAP
C. MFA
D. PEAP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Which of the following scenarios describes a possible business email compromise attack?

A. An employee receives a gift card request in an email that has an executive's name in the display field of the email.
B. Employees who open an email attachment receive messages demanding payment in order to access files.
C. A service desk employee receives an email from the HR director asking for log-in credentials to a cloud administrator account.
D. An employee receives an email with a link to a phishing site that is designed to look like the company's email portal.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
A company prevented direct access from the database administrators' workstations to the network segment that contains database servers. Which of the following should a database administrator use to access the

database servers?

A. Jump server
B. RADIUS
C. HSM
D. Load balancer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
An organization's internet-facing website was compromised when an attacker exploited a buffer overflow. Which of the following should the organization deploy to **best** protect against similar attacks in the future?

A. NGFW
B. WAF
C. TLS
D. SD-WAN

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
An administrator notices that several users are logging in from suspicious IP addresses. After speaking with the users, the administrator determines that the employees were not logging in from those IP addresses and resets the affected users' passwords. Which of the following should the administrator implement to prevent this type of attack from succeeding in the future?

A. Multifactor authentication
B. Permissions assignment
C. Access management
D. Password complexity

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
An employee receives a text message that appears to have been sent by the payroll department and is asking for credential verification. Which of the following social engineering techniques are being attempted? (Choose two.)

A. Typosquatting
B. Phishing

C. Impersonation
D. Vishing
E. Smishing
F. Misinformation

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Several employees received a fraudulent text message from someone claiming to be the Chief Executive Officer (CEO). The message stated:

"I'm in an airport right now with no access to email. I need you to buy gift cards for employee recognition awards. Please send the gift cards to following email address."

Which of the following are the **best** responses to this situation? (Choose two).

A. Cancel current employee recognition gift cards.
B. Add a smishing exercise to the annual company training.
C. Issue a general email warning to the company.
D. Have the CEO change phone numbers.
E. Conduct a forensic investigation on the CEO's phone.
F. Implement mobile device management.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
A company is required to use certified hardware when building networks. Which of the following best addresses the risks associated with procuring counterfeit hardware?

A. A thorough analysis of the supply chain
B. A legally enforceable corporate acquisition policy
C. A right to audit clause in vendor contracts and SOWs
D. An in-depth penetration test of all suppliers and vendors

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Which of the following provides the details about the terms of a test with a third-party penetration tester?

A. Rules of engagement

B. Supply chain analysis
C. Right to audit clause
D. Due diligence

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
A penetration tester begins an engagement by performing port and service scans against the client environment according to the rules of engagement. Which of the following reconnaissance types is the tester performing?

A. Active
B. Passive
C. Defensive
D. Offensive

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Which of the following is required for an organization to properly manage its restore process in the event of system failure?

A. IRP
B. DRP
C. RPO
D. SDLC

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Which of the following vulnerabilities is associated with installing software outside of a manufacturer's approved software repository?

A. Jailbreaking
B. Memory injection
C. Resource reuse
D. Side loading

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 17
A security analyst is reviewing the following logs:

```
[10:00:00 AM] Login rejected - username administrator - password Spring2023
[10:00:01 AM] Login rejected - username jsmith - password Spring2023
[10:00:01 AM] Login rejected - username guest - password Spring2023
[10:00:02 AM] Login rejected - username cpolk - password Spring2023
[10:00:03 AM] Login rejected - username fmartin - password Spring2023
```

Which of the following attacks is **most** likely occurring?

A. Password spraying
B. Account forgery
C. Pass-the-hash
D. Brute-force

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
An analyst is evaluating the implementation of Zero Trust principles within the data plane. Which of the following would be **most** relevant for the analyst to evaluate?

A. Secured zones
B. Subject role
C. Adaptive identity
D. Threat scope reduction

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
An engineer needs to find a solution that creates an added layer of security by preventing unauthorized access to internal company resources. Which of the following would be the **best** solution?

A. RDP server
B. Jump server
C. Proxy server
D. Hypervisor

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
A company's web filter is configured to scan the URL for strings and deny access when matches are found. Which of the following search strings should an analyst employ to prohibit access to non-encrypted websites?

A. encryption=off
B. http://
C. www.*.com
D. :443

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
During a security incident, the security operations team identified sustained network traffic from a malicious IP address: 10.1.4.9. A security analyst is creating an inbound firewall rule to block the IP address from accessing the organization's network. Which of the following fulfills this request?

A. access-list inbound deny ip source 0.0.0.0/0 destination 10.1.4.9/32
B. access-list inbound deny ip source 10.1.4.9/32 destination 0.0.0.0/0
C. access-list inbound permit ip source 10.1.4.9/32 destination 0.0.0.0/0
D. access-list inbound permit ip source 0.0.0.0/0 destination 10.1.4.9/32

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
A company needs to provide administrative access to internal resources while minimizing the traffic allowed through the security boundary. Which of the following methods is **most** secure?

A. Implementing a bastion host
B. Deploying a perimeter network
C. Installing a WAF
D. Utilizing single sign-on

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23

A security analyst is reviewing alerts in the SIEM related to potential malicious network traffic coming from an employee's corporate laptop. The security analyst has determined that additional data about the executable running on the machine is necessary to continue the investigation. Which of the following logs should the analyst use as a data source?

A. Application
B. IPS/IDS
C. Network
D. Endpoint

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
A cyber operations team informs a security analyst about a new tactic malicious actors are using to compromise networks.

SIEM alerts have not yet been configured. Which of the following **best** describes what the security analyst should do to identify this behavior?

A. Digital forensics
B. E-discovery
C. Incident response
D. Threat hunting

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
A company purchased cyber insurance to address items listed on the risk register. Which of the following strategies does this represent?

A. Accept
B. Transfer
C. Mitigate
D. Avoid

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
A security administrator would like to protect data on employees' laptops. Which of the following encryption techniques should the security administrator use?

A. Partition
B. Asymmetric
C. Full disk
D. Database

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Which of the following security control types does an acceptable use policy **best** represent?

A. Detective
B. Compensating
C. Corrective
D. Preventive

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
An IT manager informs the entire help desk staff that only the IT manager and the help desk lead will have access to the administrator console of the help desk software. Which of the following security techniques is the IT manager setting up?

A. Hardening
B. Employee monitoring
C. Configuration enforcement
D. Least privilege

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Which of the following is the most likely to be used to document risks, responsible parties, and thresholds?

A. Risk tolerance
B. Risk transfer
C. Risk register
D. Risk analysis

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Which of the following should a security administrator adhere to when setting up a new set of firewall rules?

A. Disaster recovery plan
B. Incident response procedure
C. Business continuity plan
D. Change management procedure

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
A company is expanding its threat surface program and allowing individuals to security test the company's internet-facing application. The company will compensate researchers based on the vulnerabilities discovered. Which of the following **best** describes the program the company is setting up?

A. Open-source intelligence
B. Bug bounty
C. Red team
D. Penetration testing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Which of the following threat actors is the **most** likely to use large financial resources to attack critical systems located in other countries?

A. Insider
B. Unskilled attacker
C. Nation-state
D. Hacktivist

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Which of the following enables the use of an input field to run commands that can view or manipulate data?

A. Cross-site scripting

B. Side loading
C. Buffer overflow
D. SQL injection

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Employees in the research and development business unit receive extensive training to ensure they understand how to best protect company data. Which of the following is the type of data these employees are **most** likely to use in day-to-day work activities?

A. Encrypted
B. Intellectual property
C. Critical
D. Data in transit

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
A company has begun labeling all laptops with asset inventory stickers and associating them with employee IDs. Which of the following security benefits do these actions provide? (Choose two.)

A. If a security incident occurs on the device, the correct employee can be notified.
B. The security team will be able to send user awareness training to the appropriate device.
C. Users can be mapped to their devices when configuring software MFA tokens.
D. User-based firewall policies can be correctly targeted to the appropriate laptops.
E. When conducting penetration testing, the security team will be able to target the desired laptops.
F. Company data can be accounted for when the employee leaves the organization.

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
A technician wants to improve the situational and environmental awareness of existing users as they transition from remote to in-office work. Which of the following is the **best** option?

A. Send out periodic security reminders.
B. Update the content of new hire documentation.
C. Modify the content of recurring training.
D. Implement a phishing campaign.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
A newly appointed board member with cybersecurity knowledge wants the board of directors to receive a quarterly report detailing the number of incidents that impacted the organization. The systems administrator is creating a way to present the data to the board of directors. Which of the following should the systems administrator use?

A. Packet captures
B. Vulnerability scans
C. Metadata
D. Dashboard

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
A systems administrator receives the following alert from a file integrity monitoring tool:

The hash of the cmd.exe file has changed.

The systems administrator checks the OS logs and notices that no patches were applied in the last two months. Which of the following **most** likely occurred?

A. The end user changed the file permissions.
B. A cryptographic collision was detected.
C. A snapshot of the file system was taken.
D. A rootkit was deployed.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
Which of the following roles, according to the shared responsibility model, is responsible for securing the company's database in an IaaS model for a cloud environment?

A. Client
B. Third-party vendor
C. Cloud provider
D. DBA

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 40
A client asked a security company to provide a document outlining the project, the cost, and the completion time frame. Which of the following documents should the company provide to the client?

A. MSA
B. SLA
C. BPA
D. SOW

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
A security team is reviewing the findings in a report that was delivered after a third party performed a penetration test. One of the findings indicated that a web application form field is vulnerable to cross-site scripting. Which of the following application security techniques should the security analyst recommend the developer implement to prevent this vulnerability?

A. Secure cookies
B. Version control
C. Input validation
D. Code signing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Which of the following must be considered when designing a high-availability network? (Choose two).

A. Ease of recovery
B. Ability to patch
C. Physical isolation
D. Responsiveness
E. Attack surface
F. Extensible authentication

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
A technician needs to apply a high-priority patch to a production system. Which of the following steps should be taken **first**?

A. Air gap the system.
B. Move the system to a different network segment.
C. Create a change control request.
D. Apply the patch to the system.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
Which of the following describes the reason root cause analysis should be conducted as part of incident response?

A. To gather IoCs for the investigation
B. To discover which systems have been affected
C. To eradicate any trace of malware on the network
D. To prevent future incidents of the same nature

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Which of the following is the **most** likely outcome if a large bank fails an internal PCI DSS compliance assessment?

A. Fines
B. Audit findings
C. Sanctions
D. Reputation damage

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
A company is developing a business continuity strategy and needs to determine how many staff members would be required to sustain the business in the case of a disruption. Which of the following **best** describes this step?

A. Capacity planning

B. Redundancy
C. Geographic dispersion
D. Tabletop exercise

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
A company's legal department drafted sensitive documents in a SaaS application and wants to ensure the documents cannot be accessed by individuals in high-risk countries. Which of the following is the **most** effective way to limit this access?

A. Data masking
B. Encryption
C. Geolocation policy
D. Data sovereignty regulation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
Which of the following is a hardware-specific vulnerability?

A. Firmware version
B. Buffer overflow
C. SQL injection
D. Cross-site scripting

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
While troubleshooting a firewall configuration, a technician determines that a "deny any" policy should be added to the bottom of the ACL. The technician updates the policy, but the new policy causes several company servers to become unreachable.

Which of the following actions would prevent this issue?

A. Documenting the new policy in a change request and submitting the request to change management
B. Testing the policy in a non-production environment before enabling the policy in the production network
C. Disabling any intrusion prevention signatures on the "deny any" policy prior to enabling the new policy
D. Including an "allow any" policy above the "deny any" policy

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
An organization is building a new backup data center with cost-benefit as the primary requirement and RTO and RPO values around two days. Which of the following types of sites is the **best** for this scenario?

A. Real-time recovery
B. Hot
C. Cold
D. Warm

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
A company requires hard drives to be securely wiped before sending decommissioned systems to recycling. Which of the following **best** describes this policy?

A. Enumeration
B. Sanitization
C. Destruction
D. Inventory

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
A systems administrator works for a local hospital and needs to ensure patient data is protected and secure. Which of the following data classifications should be used to secure patient data?

A. Private
B. Critical
C. Sensitive
D. Public

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53

A U.S.-based cloud-hosting provider wants to expand its data centers to new international locations. Which of the following should the hosting provider consider **first**?

A. Local data protection regulations
B. Risks from hackers residing in other countries
C. Impacts to existing contractual obligations
D. Time zone differences in log correlation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
Which of the following would be the **best** way to block unknown programs from executing?

A. Access control list
B. Application allow list
C. Host-based firewall
D. DLP solution

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
A company hired a consultant to perform an offensive security assessment covering penetration testing and social engineering.

Which of the following teams will conduct this assessment activity?

A. White
B. Purple
C. Blue
D. Red

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
A software development manager wants to ensure the authenticity of the code created by the company. Which of the following options is the **most** appropriate?

A. Testing input validation on the user input fields
B. Performing code signing on company-developed software
C. Performing static code analysis on the software

D. Ensuring secure cookies are use

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Which of the following can be used to identify potential attacker activities without affecting production servers?

A. Honeypot
B. Video surveillance
C. Zero Trust
D. Geofencing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
During an investigation, an incident response team attempts to understand the source of an incident. Which of the following incident response activities describes this process?

A. Analysis
B. Lessons learned
C. Detection
D. Containment

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
A security practitioner completes a vulnerability assessment on a company's network and finds several vulnerabilities, which the operations team remediates. Which of the following should be done **next**?

A. Conduct an audit.
B. Initiate a penetration test.
C. Rescan the network.
D. Submit a report.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
An administrator was notified that a user logged in remotely after hours and copied large amounts of data to a personal device.

Which of the following **best** describes the user's activity?

A. Penetration testing
B. Phishing campaign
C. External audit
D. Insider threat

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
Which of the following allows for the attribution of messages to individuals?

A. Adaptive identity
B. Non-repudiation
C. Authentication
D. Access logs

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Which of the following is the **best** way to consistently determine on a daily basis whether security settings on servers have been modified?

A. Automation
B. Compliance checklist
C. Attestation
D. Manual audit

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Which of the following tools can assist with detecting an employee who has accidentally emailed a file containing a customer's PII?

A. SCAP
B. NetFlow

C. Antivirus
D. DLP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
An organization recently updated its security policy to include the following statement:

Regular expressions are included in source code to remove special characters such as $, |, ;. &, `, and ? from variables set by forms in a web application.

Which of the following **best** explains the security technique the organization adopted by making this addition to the policy?

A. Identify embedded keys
B. Code debugging
C. Input validation
D. Static code analysis

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
A security analyst and the management team are reviewing the organizational performance of a recent phishing campaign. The user click-through rate exceeded the acceptable risk threshold, and the management team wants to reduce the impact when a user clicks on a link in a phishing message. Which of the following should the analyst do?

A. Place posters around the office to raise awareness of common phishing activities.
B. Implement email security filters to prevent phishing emails from being delivered.
C. Update the EDR policies to block automatic execution of downloaded programs.
D. Create additional training for users to recognize the signs of phishing attempts.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
Which of the following has been implemented when a host-based firewall on a legacy Linux system allows connections from only specific internal IP addresses?

A. Compensating control
B. Network segmentation
C. Transfer of risk

D. SNMP traps

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
The management team notices that new accounts that are set up manually do not always have correct access or permissions.

Which of the following automation techniques should a systems administrator use to streamline account creation?

A. Guard rail script
B. Ticketing workflow
C. Escalation script
D. User provisioning script

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
A company is planning to set up a SIEM system and assign an analyst to review the logs on a weekly basis. Which of the following types of controls is the company setting up?

A. Corrective
B. Preventive
C. Detective
D. Deterrent

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
A systems administrator is looking for a low-cost application-hosting solution that is cloud-based. Which of the following meets these requirements?

A. Serverless framework
B. Type 1 hypervisor
C. SD-WAN
D. SDN

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
A security operations center determines that the malicious activity detected on a server is normal. Which of the following activities describes the act of ignoring detected activity in the future?

A. Tuning
B. Aggregating
C. Quarantining
D. Archiving

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
A security analyst reviews domain activity logs and notices the following:

```
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
```


Which of the following is the **best** explanation for what the security analyst has discovered?

A. The user jsmith's account has been locked out.
B. A keylogger is installed on jsmith's workstation.
C. An attacker is attempting to brute force jsmith's account.
D. Ransomware has been deployed in the domain.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
A company is concerned about weather events causing damage to the server room and downtime. Which of the following should the company consider?

A. Clustering servers
B. Geographic dispersion
C. Load balancers
D. Off-site backups

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
Which of the following is a **primary** security concern for a company setting up a BYOD program?

A. End of life
B. Buffer overflow
C. VM escape
D. Jailbreaking

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
A company decided to reduce the cost of its annual cyber insurance policy by removing the coverage for ransomware attacks.

Which of the following analysis elements did the company **most** likely use in making this decision?

A. MTTR
B. RTO
C. ARO
D. MTBF

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
Which of the following is the **most** likely to be included as an element of communication in a security awareness program?

A. Reporting phishing attempts or other suspicious activities
B. Detecting insider threats using anomalous behavior recognition
C. Verifying information when modifying wire transfer data
D. Performing social engineering as part of third-party penetration testing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
HOTSPOT

Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with

its remediation.

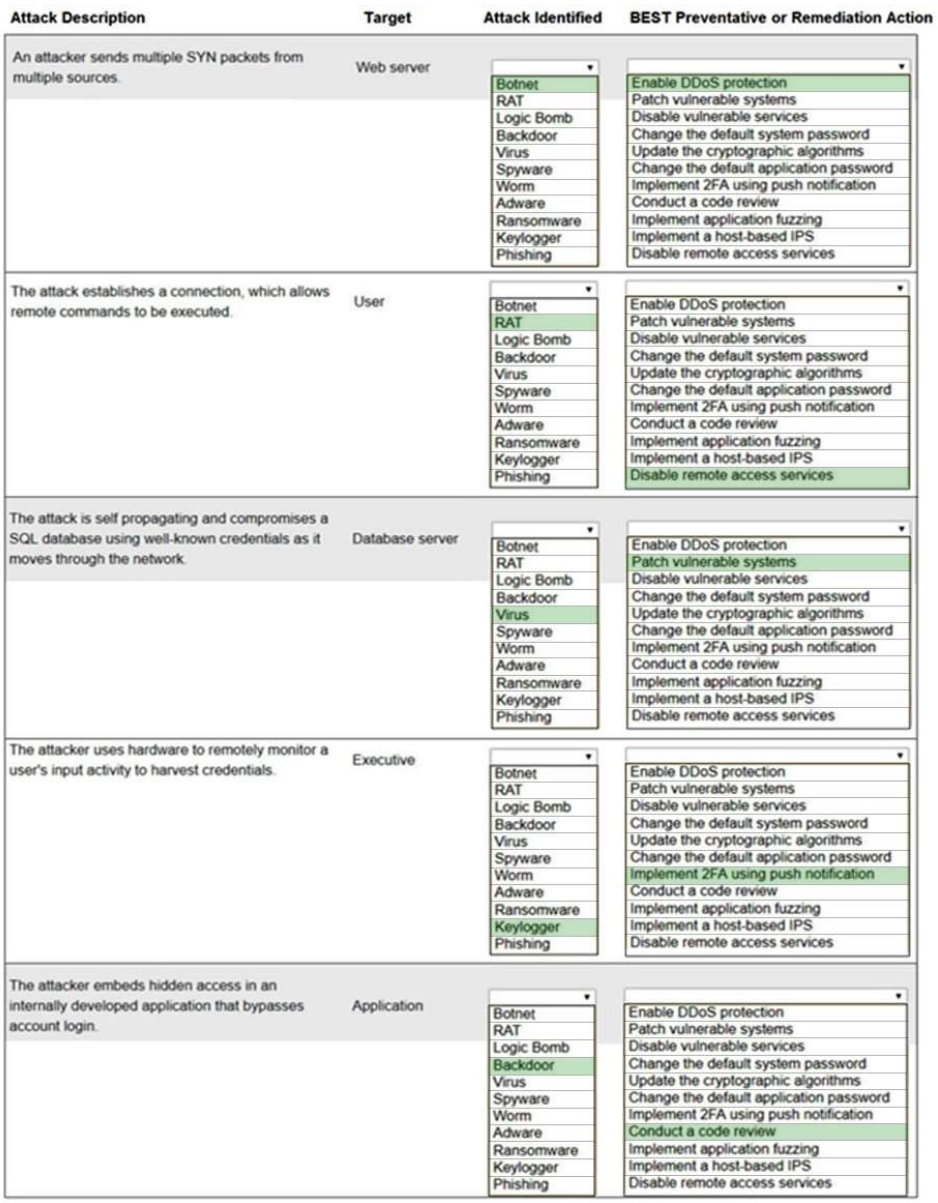
INSTRUCTIONS
Not all attacks and remediation actions will be used.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Hot Area:

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack establishes a connection, which allows remote commands to be executed.	User	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services

Correct Answer:



Section: (none)
Explanation

Explanation/Reference:

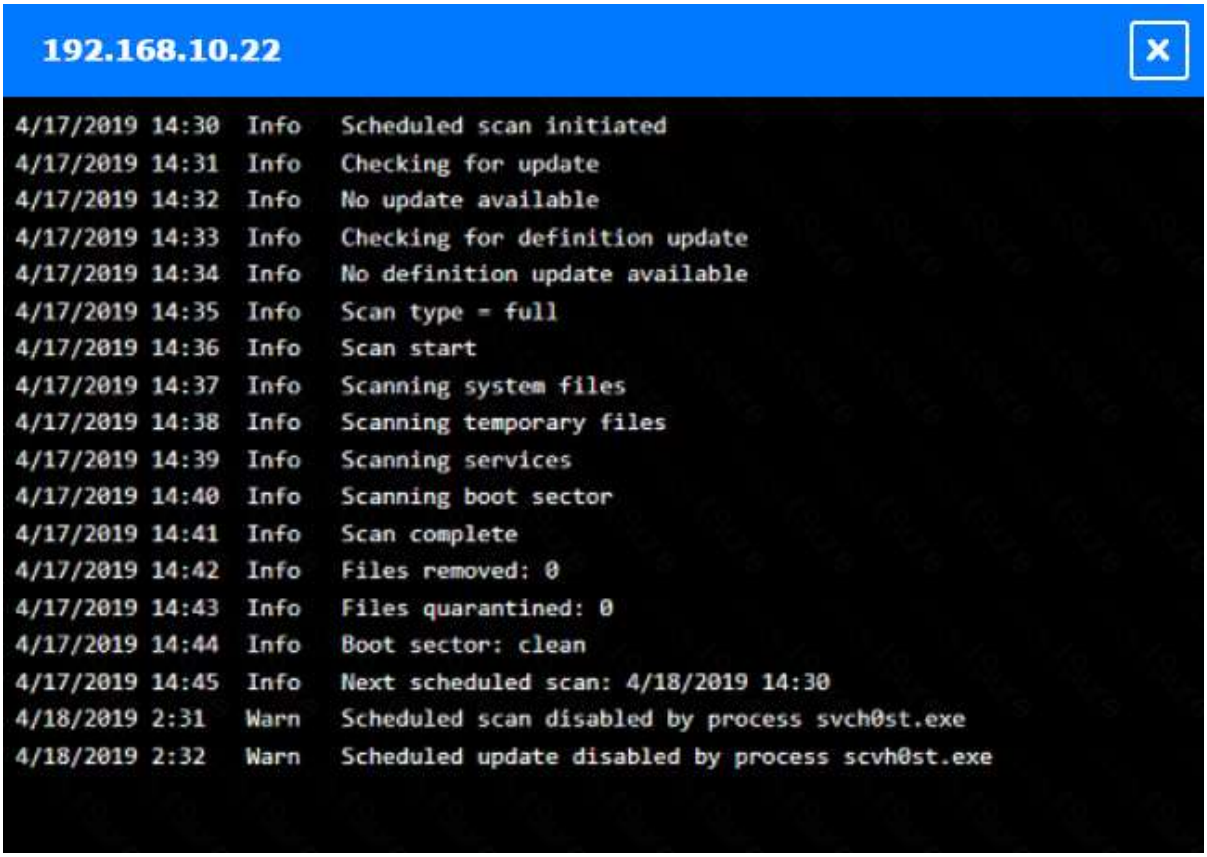
QUESTION 77
HOTSPOT

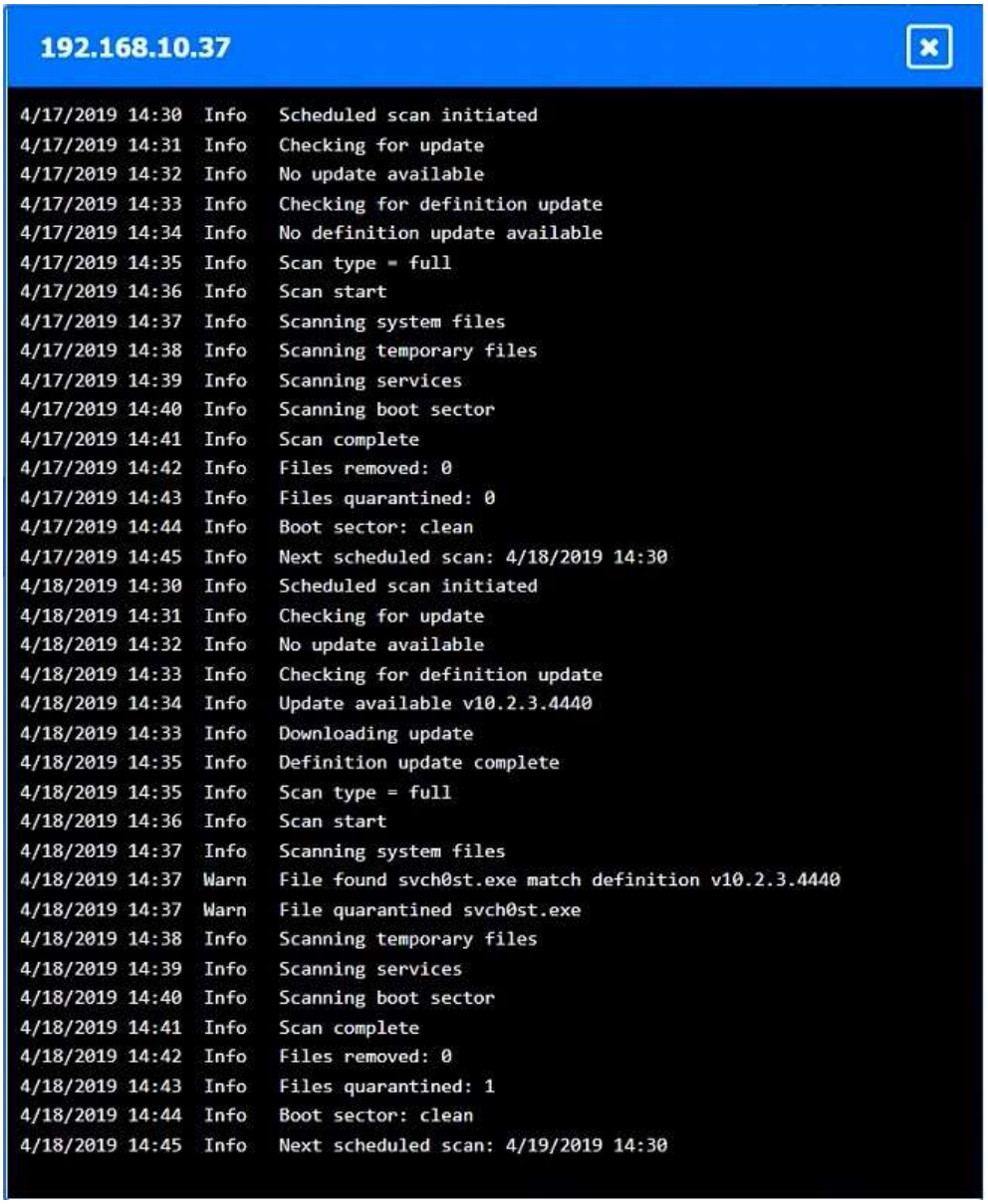
You are a security administrator investigating a potential infection on a network.

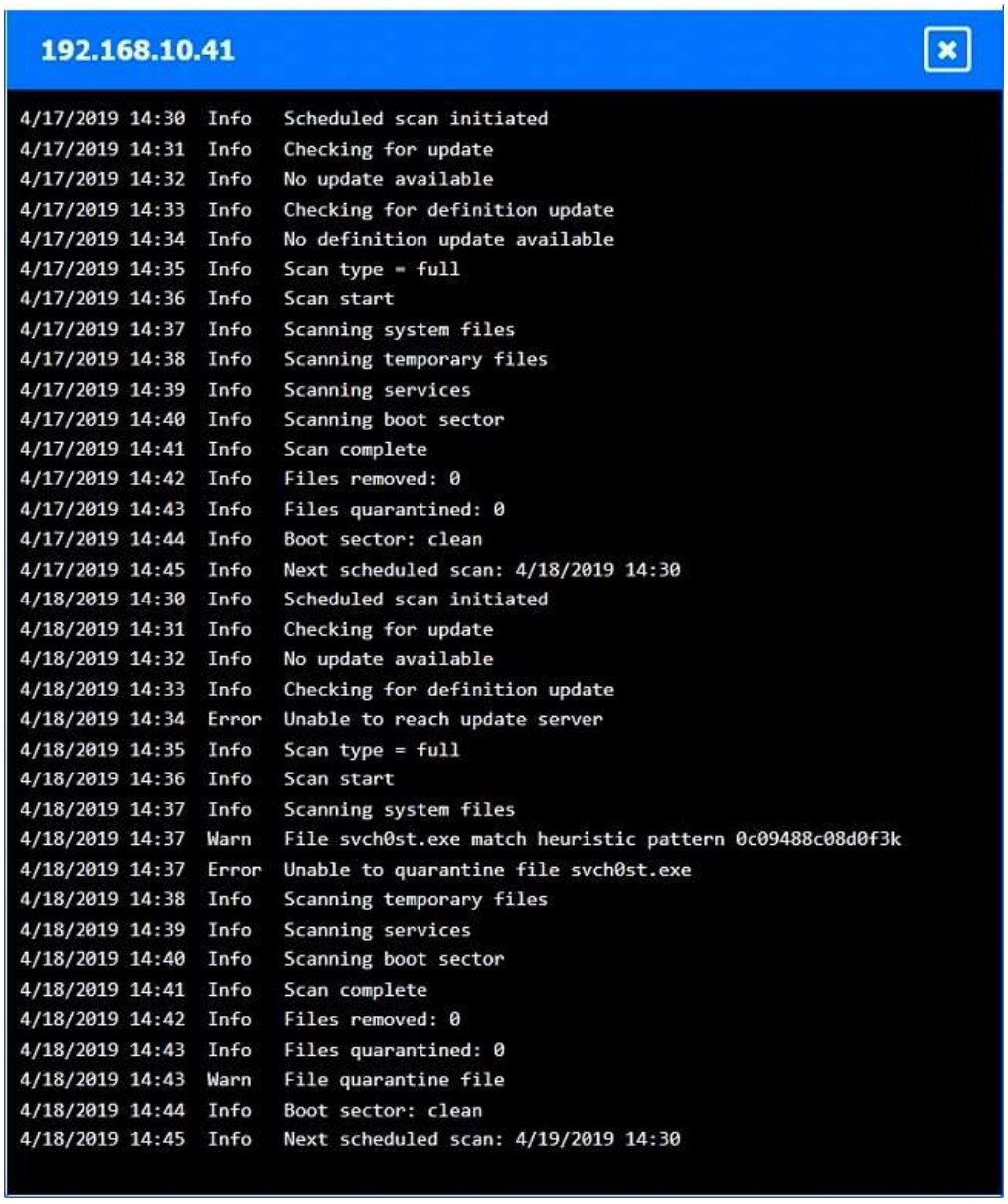
INSTRUCTIONS

Click on each host and firewall. Review all logs to determine which host originated the infection and then identify if each remaining host is clean or infected.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

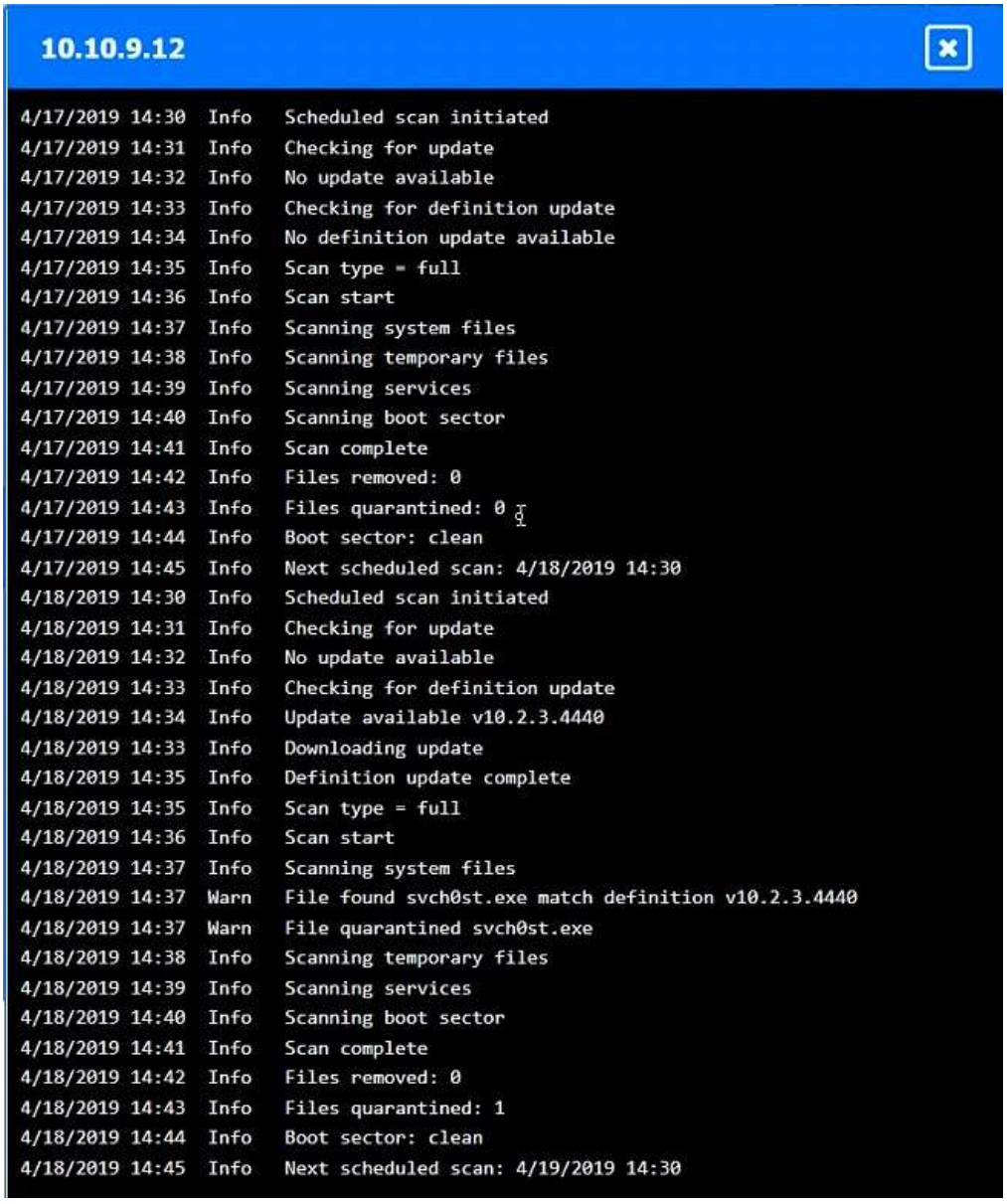

192.168.10.22
4/17/2019 14:30 Info Scheduled scan initiated
4/17/2019 14:31 Info Checking for update
4/17/2019 14:32 Info No update available
4/17/2019 14:33 Info Checking for definition update
4/17/2019 14:34 Info No definition update available
4/17/2019 14:35 Info Scan type = full
4/17/2019 14:36 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 2:31 Warn Scheduled scan disabled by process svch0st.exe
4/18/2019 2:32 Warn Scheduled update disabled by process scvh0st.exe


192.168.10.37
4/17/2019 14:30 Info Scheduled scan initiated
4/17/2019 14:31 Info Checking for update
4/17/2019 14:32 Info No update available
4/17/2019 14:33 Info Checking for definition update
4/17/2019 14:34 Info No definition update available
4/17/2019 14:35 Info Scan type = full
4/17/2019 14:36 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30 Info Scheduled scan initiated
4/18/2019 14:31 Info Checking for update
4/18/2019 14:32 Info No update available
4/18/2019 14:33 Info Checking for definition update
4/18/2019 14:34 Info Update available v10.2.3.4440
4/18/2019 14:33 Info Downloading update
4/18/2019 14:35 Info Definition update complete
4/18/2019 14:35 Info Scan type = full
4/18/2019 14:36 Info Scan start
4/18/2019 14:37 Info Scanning system files
4/18/2019 14:37 Warn File found svch0st.exe match definition v10.2.3.4440
4/18/2019 14:37 Warn File quarantined svch0st.exe
4/18/2019 14:38 Info Scanning temporary files
4/18/2019 14:39 Info Scanning services
4/18/2019 14:40 Info Scanning boot sector
4/18/2019 14:41 Info Scan complete
4/18/2019 14:42 Info Files removed: 0
4/18/2019 14:43 Info Files quarantined: 1
4/18/2019 14:44 Info Boot sector: clean
4/18/2019 14:45 Info Next scheduled scan: 4/19/2019 14:30


192.168.10.41
4/17/2019 14:30 Info Scheduled scan initiated
4/17/2019 14:31 Info Checking for update
4/17/2019 14:32 Info No update available
4/17/2019 14:33 Info Checking for definition update
4/17/2019 14:34 Info No definition update available
4/17/2019 14:35 Info Scan type = full
4/17/2019 14:36 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30 Info Scheduled scan initiated
4/18/2019 14:31 Info Checking for update
4/18/2019 14:32 Info No update available
4/18/2019 14:33 Info Checking for definition update
4/18/2019 14:34 Error Unable to reach update server
4/18/2019 14:35 Info Scan type = full
4/18/2019 14:36 Info Scan start
4/18/2019 14:37 Info Scanning system files
4/18/2019 14:37 Warn File svch0st.exe match heuristic pattern 0c09488c08d0f3k
4/18/2019 14:37 Error Unable to quarantine file svch0st.exe
4/18/2019 14:38 Info Scanning temporary files
4/18/2019 14:39 Info Scanning services
4/18/2019 14:40 Info Scanning boot sector
4/18/2019 14:41 Info Scan complete
4/18/2019 14:42 Info Files removed: 0
4/18/2019 14:43 Info Files quarantined: 0
4/18/2019 14:43 Warn File quarantine file
4/18/2019 14:44 Info Boot sector: clean
4/18/2019 14:45 Info Next scheduled scan: 4/19/2019 14:30

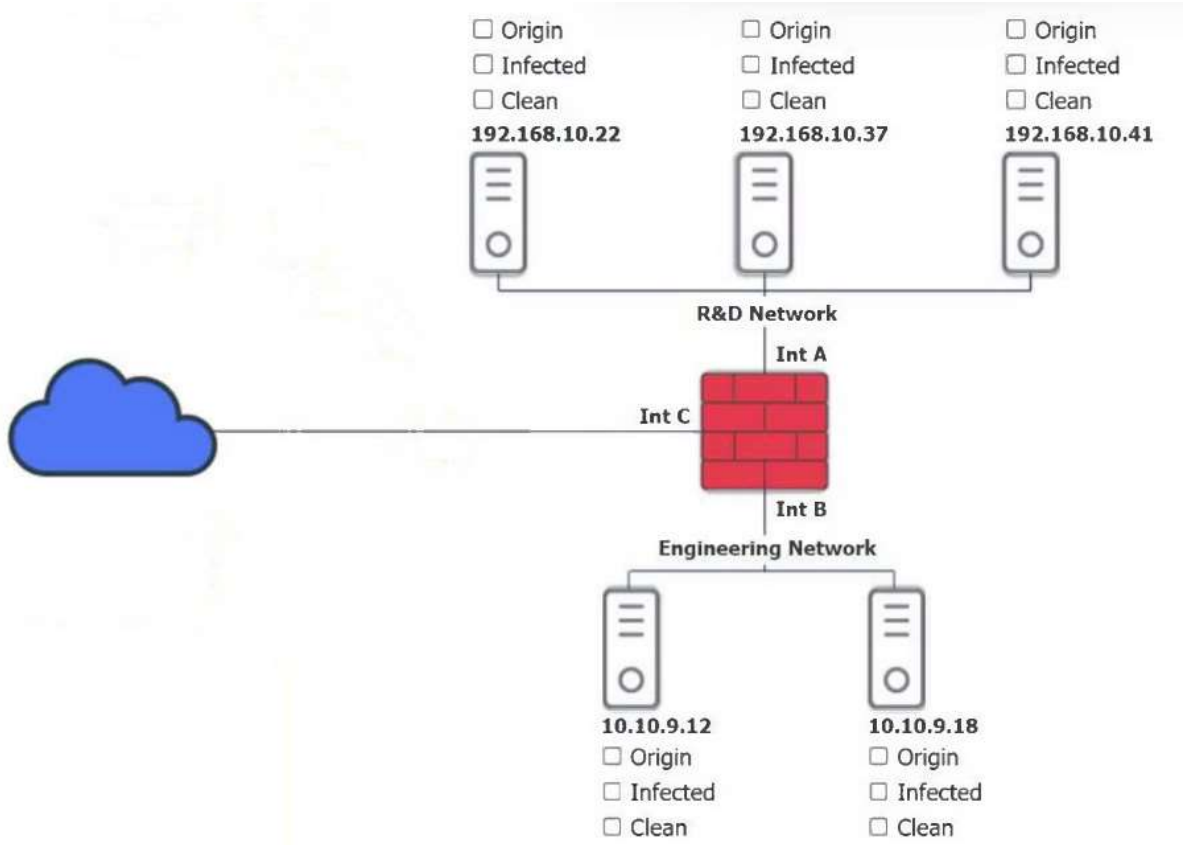
Firewall

Timestamp		Source	Destination	Destination Port	Application	Action	Client Bytes	Server Bytes
4/17/2019	16:01:44	10.10.9.18	57.203.54.183	443	ssl	Permit	6953	99427
4/17/2019	16:01:58	192.168.10.37	57.203.54.221	443	ssl	Permit	9301	199386
4/17/2019	16:17:06	192.168.10.22	10.10.9.12	135	rpc	Permit	175	1504
4/17/2019	16:27:36	192.168.10.41	10.10.9.12	445	smbv1	Permit	345	34757
4/17/2019	16:28:06	10.10.9.12	192.168.10.41	135	rpc	Permit	754	4771
4/17/2019	16:33:31	10.10.9.18	192.168.10.22	135	rpc	Permit	643	2355
4/17/2019	16:35:36	192.168.10.37	10.10.9.12	135	smbv2	Permit	649	5644
4/17/2019	23:58:36	10.10.9.12	192.168.10.41		icmp	Permit	128	128
4/17/2019	23:58:43	10.10.9.12	192.168.10.22		icmp	Permit	128	128
4/17/2019	23:58:45	10.10.9.12	192.168.10.37		icmp	Permit	128	128
4/18/2019	2:31:36	10.10.9.18	192.168.10.41	445	smbv2	Permit	1874	23874
4/18/2019	2:31:45	192.168.10.22	57.203.55.29	8080	http	Permit	7203	75997
4/18/2019	2:31:51	10.10.9.18	57.203.56.201	443	ssl	Permit	9953	199730
4/18/2019	2:31:02	192.168.10.22	57.203.55.234	443	http	Permit	4937	84937
4/18/2019	2:39:11	192.168.10.41	57.203.53.89	8080	http	Permit	8201	133183
4/18/2019	2:39:12	10.10.9.18	57.203.55.19	8080	ssl	Permit	1284	9102854
4/18/2019	2:39:32	192.168.10.37	57.203.56.113	443	ssl	Permit	9341	9938
4/18/2019	13:37:36	192.168.10.22	10.10.9.18	445	smbv3	Permit	1874	23874
4/18/2019	13:39:43	192.168.10.22	10.10.9.18	135	rpc	Permit	673	41358
4/18/2019	13:45:04	10.10.9.18	192.168.10.37	135	rpc	Permit	693	1952
4/18/2019	13:47:44	10.10.9.12	192.168.10.41	445	smbv3	Permit	482	3505
4/18/2019	13:52:57	10.10.9.18	192.168.10.22	135	rpc	Permit	545	9063
4/18/2019	13:53:01	192.168.10.37	10.10.9.12	335	smbv3	Permit	876	8068
4/18/2019	14:30:04	10.10.9.12	57.203.56.231	443	ssl	Permit	9901	199730
4/18/2019	14:30:04	192.168.10.37	57.203.56.143	443	ssl	Permit	10092	209938

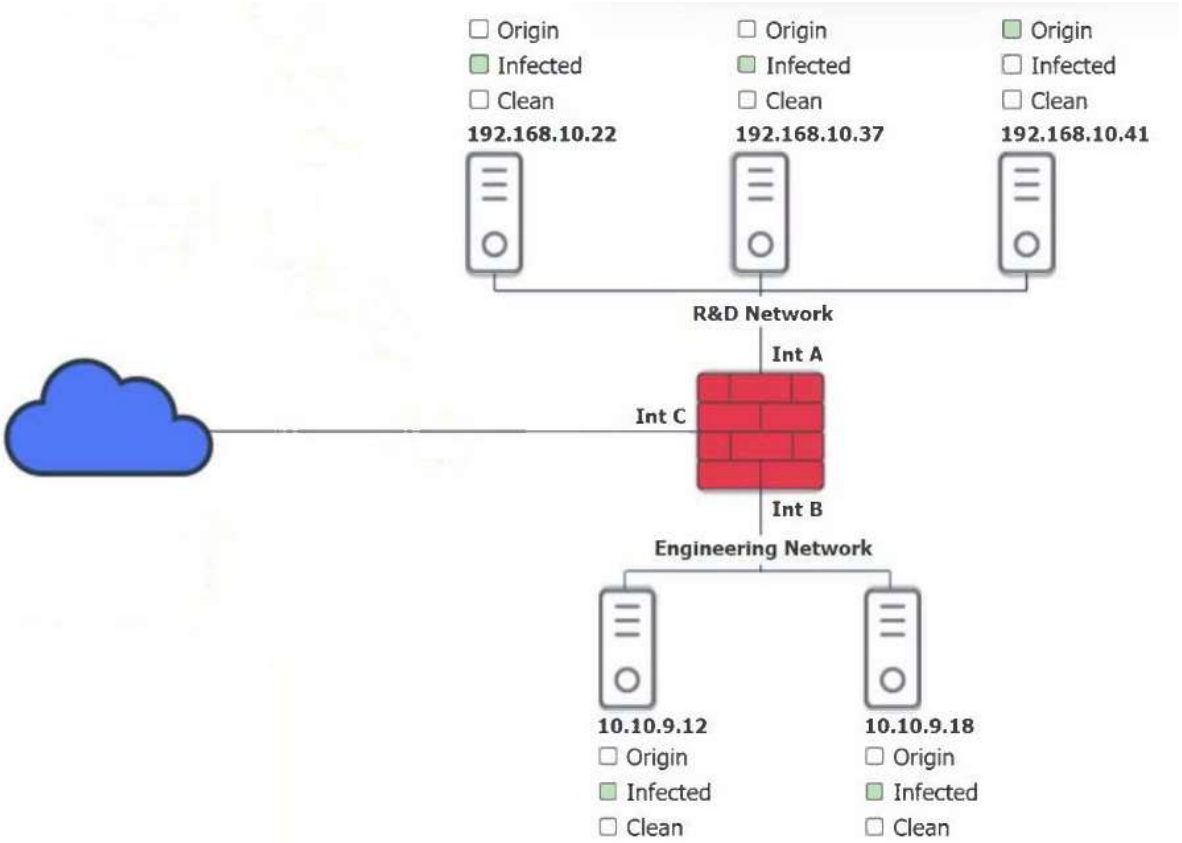

10.10.9.12
4/17/2019 14:30 Info Scheduled scan initiated
4/17/2019 14:31 Info Checking for update
4/17/2019 14:32 Info No update available
4/17/2019 14:33 Info Checking for definition update
4/17/2019 14:34 Info No definition update available
4/17/2019 14:35 Info Scan type = full
4/17/2019 14:36 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30 Info Scheduled scan initiated
4/18/2019 14:31 Info Checking for update
4/18/2019 14:32 Info No update available
4/18/2019 14:33 Info Checking for definition update
4/18/2019 14:34 Info Update available v10.2.3.4440
4/18/2019 14:33 Info Downloading update
4/18/2019 14:35 Info Definition update complete
4/18/2019 14:35 Info Scan type = full
4/18/2019 14:36 Info Scan start
4/18/2019 14:37 Info Scanning system files
4/18/2019 14:37 Warn File found svch0st.exe match definition v10.2.3.4440
4/18/2019 14:37 Warn File quarantined svch0st.exe
4/18/2019 14:38 Info Scanning temporary files
4/18/2019 14:39 Info Scanning services
4/18/2019 14:40 Info Scanning boot sector
4/18/2019 14:41 Info Scan complete
4/18/2019 14:42 Info Files removed: 0
4/18/2019 14:43 Info Files quarantined: 1
4/18/2019 14:44 Info Boot sector: clean
4/18/2019 14:45 Info Next scheduled scan: 4/19/2019 14:30


10.10.9.18
4/17/2019 14:30 Info Scheduled scan initiated
4/17/2019 14:31 Info Checking for update
4/17/2019 14:32 Info No update available
4/17/2019 14:33 Info Checking for definition update
4/17/2019 14:34 Info No definition update available
4/17/2019 14:35 Info Scan type = full
4/17/2019 14:36 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30 Info Scheduled scan initiated
4/18/2019 14:31 Info Checking for update
4/18/2019 14:32 Info No update available
4/18/2019 14:33 Info Checking for definition update
4/18/2019 14:34 Error Unable to reach update server
4/18/2019 14:35 Info Scan type = full
4/18/2019 14:36 Info Scan start
4/18/2019 14:37 Info Scanning system files
4/18/2019 14:37 Warn File svch0st.exe match heuristic pattern 0c09488c08d0f3k
4/18/2019 14:37 Error Unable to quarantine file svch0st.exe
4/18/2019 14:38 Info Scanning temporary files
4/18/2019 14:39 Info Scanning services
4/18/2019 14:40 Info Scanning boot sector
4/18/2019 14:41 Info Scan complete
4/18/2019 14:42 Info Files removed: 0
4/18/2019 14:43 Info Files quarantined: 0
4/18/2019 14:43 Warn File quarantine file
4/18/2019 14:44 Info Boot sector: clean
4/18/2019 14:45 Info Next scheduled scan: 4/19/2019 14:30

Hot Area:



Correct Answer:



Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
Which of the following is the phase in the incident response process when a security analyst reviews roles and responsibilities?

A. Preparation
B. Recovery
C. Lessons learned
D. Analysis

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
After a recent vulnerability scan, a security engineer needs to harden the routers within the corporate network. Which of the following is the most appropriate to disable?

A. Console access
B. Routing protocols

C. VLANs
D. Web-based administration

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
A security administrator needs a method to secure data in an environment that includes some form of checks so track any changes. Which of the following should the administrator set up to achieve this goal?

A. SPF
B. GPO
C. NAC
D. FIM

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
An administrator is reviewing a single server's security logs and discovers the following:

Keywords	Date and Time	Source	Event ID	Task Category
Audit Failure	11:13:05 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:07 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:09 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:11 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:13 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:15 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:17 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:19 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:21 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:23 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:25 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:27 AM	Microsoft Windows security	4625	Logon

Which of the following best describes the action captured in this log file?

A. Brute-force attack
B. Privilege escalation
C. Failed password audit
D. Forgotten password by the user

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
A security engineer is implementing FDE for all laptops in an organization. Which of the following are the most important for the engineer to consider as part of the planning process? (Choose two.)

A. Key escrow
B. TPM presence
C. Digital signatures
D. Data tokenization
E. Public key management
F. Certificate authority linking

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
A security analyst scans a company's public network and discovers a host is running a remote desktop that can be used to access the production network. Which of the following changes should the security analyst recommend?

A. Changing the remote desktop port to a non-standard number
B. Setting up a VPN and placing the jump server inside the firewall
C. Using a proxy for web connections from the remote desktop server
D. Connecting the remote server to the domain and increasing the password length

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
An enterprise has been experiencing attacks focused on exploiting vulnerabilities in older browser versions with well-known exploits. Which of the following security solutions should be configured to best provide the ability to monitor and block these known signature-based attacks?

A. ACL
B. DLP
C. IDS
D. IPS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
Security controls in a data center are being reviewed to ensure data is properly protected and that human life considerations are included. Which of the following best describes how the controls should be set up?

A. Remote access points should fail closed.
B. Logging controls should fail open.

C. Safety controls should fail open.
D. Logical security controls should fail closed.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
Which of the following would be best suited for constantly changing environments?

A. RTOS
B. Containers
C. Embedded systems
D. SCADA

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
Which of the following incident response activities ensures evidence is properly handled?

A. E-discovery
B. Chain of custody
C. Legal hold
D. Preservation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
An accounting clerk sent money to an attacker's bank account after receiving fraudulent instructions to use a new account. Which of the following would most likely prevent this activity in the future?

A. Standardizing security incident reporting
B. Executing regular phishing campaigns
C. Implementing insider threat detection measures
D. Updating processes for sending wire transfers

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
A systems administrator is creating a script that would save time and prevent human error when performing account creation for a large number of end users. Which of the following would be a good use case for this task?

A. Off-the-shelf software
B. Orchestration
C. Baseline
D. Policy enforcement

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
A company's marketing department collects, modifies, and stores sensitive customer data. The infrastructure team is responsible for securing the data while in transit and at rest. Which of the following data roles describes the customer?

A. Processor
B. Custodian
C. Subject
D. Owner

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
Which of the following describes the maximum allowance of accepted risk?

A. Risk indicator
B. Risk level
C. Risk score
D. Risk threshold

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
A security analyst receives alerts about an internal system sending a large amount of unusual DNS queries to systems on the internet over short periods of time during non-business hours. Which of the following is most likely occurring?

A. A worm is propagating across the network.

B. Data is being exfiltrated.
C. A logic bomb is deleting data.
D. Ransomware is encrypting files.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
A technician is opening ports on a firewall for a new system being deployed and supported by a SaaS provider. Which of the following is a risk in the new system?

A. Default credentials
B. Non-segmented network
C. Supply chain vendor
D. Vulnerable software

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
A systems administrator is working on a solution with the following requirements:

• Provide a secure zone.
• Enforce a company-wide access control policy.
• Reduce the scope of threats.

Which of the following is the systems administrator setting up?

A. Zero Trust
B. AAA
C. Non-repudiation
D. CIA

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
Which of the following involves an attempt to take advantage of database misconfigurations?

A. Buffer overflow
B. SQL injection
C. VM escape
D. Memory injection

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
Which of the following is used to validate a certificate when it is presented to a user?

A. OCSP
B. CSR
C. CA
D. CRC

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
One of a company's vendors sent an analyst a security bulletin that recommends a BIOS update. Which of the following vulnerability types is being addressed by the patch?

A. Virtualization
B. Firmware
C. Application
D. Operating system

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
Which of the following is used to quantitatively measure the criticality of a vulnerability?

A. CVE
B. CVSS
C. CIA
D. CERT

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
Which of the following actions could a security engineer take to ensure workstations and servers are properly

monitored for unauthorized changes and software?

A. Configure all systems to log scheduled tasks.
B. Collect and monitor all traffic exiting the network.
C. Block traffic based on known malicious signatures.
D. Install endpoint management software on all systems

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
An organization is leveraging a VPN between its headquarters and a branch location. Which of the following is the VPN protecting?

A. Data in use
B. Data in transit
C. Geographic restrictions
D. Data sovereignty

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
After reviewing the following vulnerability scanning report:

```
Server:192.168.14.6
Service: Telnet
Port: 23 Protocol: TCP
Status: Open Severity: High
Vulnerability: Use of an insecure network protocol
```

A security analyst performs the following test:

```
nmap -p 23 192.168.14.6 --script telnet-encryption

PORT     STATE SERVICE REASON
23/tcp   open  telnet  syn-ack
|  telnet encryption:
|_ Telnet server supports encryption
```

Which of the following would the security analyst conclude for this reported vulnerability?

A. It is a false positive.
B. A rescan is required.
C. It is considered noise.
D. Compensating controls exist.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
An organization disabled unneeded services and placed a firewall in front of a business-critical legacy system. Which of the following best describes the actions taken by the organization?

A. Exception
B. Segmentation
C. Risk transfer
D. Compensating controls

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
A security consultant needs secure, remote access to a client environment. Which of the following should the security consultant most likely use to gain access?

A. EAP
B. DHCP
C. IPSec
D. NAT

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
Which of the following should a systems administrator use to ensure an easy deployment of resources within the cloud provider?

A. Software as a service
B. Infrastructure as code
C. Internet of Things
D. Software-defined networking

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 105
After a security awareness training session, a user called the IT help desk and reported a suspicious call. The suspicious caller stated that the Chief Financial Officer wanted credit card information in order to close an invoice. Which of the following topics did the user recognize from the training?

A. Insider threat
B. Email phishing
C. Social engineering
D. Executive whaling

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
A security administrator is deploying a DLP solution to prevent the exfiltration of sensitive customer data. Which of the following should the administrator do first?

A. Block access to cloud storage websites.
B. Create a rule to block outgoing email attachments.
C. Apply classifications to the data.
D. Remove all user permissions from shares on the file server.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
An administrator assists the legal and compliance team with ensuring information about customer transactions is archived for the proper time period. Which of the following data policies is the administrator carrying out?

A. Compromise
B. Retention
C. Analysis
D. Transfer
E. Inventory

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108

A company is working with a vendor to perform a penetration test. Which of the following includes an estimate about the number of hours required to complete the engagement?

A. SOW
B. BPA
C. SLA
D. NDA

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
A Chief Information Security Officer (CISO) wants to explicitly raise awareness about the increase of ransomware-as-a-service in a report to the management team. Which of the following **best** describes the threat actor in the CISO's report?

A. Insider threat
B. Hacktivist
C. Nation-state
D. Organized crime

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
Which of the following practices would be best to prevent an insider from introducing malicious code into a company's development process?

A. Code scanning for vulnerabilities
B. Open-source component usage
C. Quality assurance testing
D. Peer review and approval

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
Which of the following can best protect against an employee inadvertently installing malware on a company system?

A. Host-based firewall
B. System isolation
C. Least privilege

D. Application allow list

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
A company is adding a clause to its AUP that states employees are not allowed to modify the operating system on mobile devices. Which of the following vulnerabilities is the organization addressing?

A. Cross-site scripting
B. Buffer overflow
C. Jailbreaking
D. Side loading

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
Which of the following would be the **best** ways to ensure only authorized personnel can access a secure facility? (Choose two.)

A. Fencing
B. Video surveillance
C. Badge access
D. Access control vestibule
E. Sign-in sheet
F. Sensor

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
An organization would like to store customer data on a separate part of the network that is not accessible to users on the main corporate network. Which of the following should the administrator use to accomplish this goal?

A. Segmentation
B. Isolation
C. Patching
D. Encryption

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 115
Which of the following is the most common data loss path for an air-gapped network?

A. Bastion host
B. Unsecured Bluetooth
C. Unpatched OS
D. Removable devices

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
Malware spread across a company's network after an employee visited a compromised industry blog. Which of the following best describes this type of attack?

A. Impersonation
B. Disinformation
C. Watering-hole
D. Smishing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
An organization is struggling with scaling issues on its VPN concentrator and internet circuit due to remote work. The organization is looking for a software solution that will allow it to reduce traffic on the VPN and internet circuit, while still providing encrypted tunnel access to the data center and monitoring of remote employee internet traffic. Which of the following will help achieve these objectives?

A. Deploying a SASE solution to remote employees
B. Building a load-balanced VPN solution with redundant internet
C. Purchasing a low-cost SD-WAN solution for VPN traffic
D. Using a cloud provider to create additional VPN concentrators

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
Which of the following is the **best** reason to complete an audit in a banking environment?

A. Regulatory requirement
B. Organizational change
C. Self-assessment requirement
D. Service-level requirement

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
Which of the following security concepts is the best reason for permissions on a human resources fileshare to follow the principle of least privilege?

A. Integrity
B. Availability
C. Confidentiality
D. Non-repudiation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 120
Which of the following are cases in which an engineer should recommend the decommissioning of a network device? (Choose two.)

A. The device has been moved from a production environment to a test environment.
B. The device is configured to use cleartext passwords.
C. The device is moved to an isolated segment on the enterprise network.
D. The device is moved to a different location in the enterprise.
E. The device's encryption level cannot meet organizational standards.
F. The device is unable to receive authorized updates.

Correct Answer: EF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 121
A company is required to perform a risk assessment on an annual basis. Which of the following types of risk assessments does this requirement describe?

A. Continuous
B. Ad hoc
C. Recurring
D. One time

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122
After a recent ransomware attack on a company's system, an administrator reviewed the log files. Which of the following control types did the administrator use?

A. Compensating
B. Detective
C. Preventive
D. Corrective

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 123
Which of the following exercises should an organization use to improve its incident response process?

A. Tabletop
B. Replication
C. Failover
D. Recovery

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
Which of the following best ensures minimal downtime and data loss for organizations with critical computing equipment located in earthquake-prone areas?

A. Generators and UPS
B. Off-site replication
C. Redundant cold sites
D. High availability networking

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125

A newly identified network access vulnerability has been found in the OS of legacy IoT devices. Which of the following would best mitigate this vulnerability quickly?

A. Insurance
B. Patching
C. Segmentation
D. Replacement

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126
After an audit, an administrator discovers all users have access to confidential data on a file server. Which of the following should the administrator use to restrict access to the data quickly?

A. Group Policy
B. Content filtering
C. Data loss prevention
D. Access control lists

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
A client demands at least 99.99% uptime from a service provider's hosted security services. Which of the following documents includes the information the service provider should return to the client?

A. MOA
B. SOW
C. MOU
D. SLA

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128
A company is discarding a classified storage array and hires an outside vendor to complete the disposal. Which of the following should the company request from the vendor?

A. Certification
B. Inventory list
C. Classification
D. Proof of ownership

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 129
A company is planning a disaster recovery site and needs to ensure that a single natural disaster would not result in the complete loss of regulated backup data. Which of the following should the company consider?

A. Geographic dispersion
B. Platform diversity
C. Hot site
D. Load balancing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
A security analyst locates a potentially malicious video file on a server and needs to identify both the creation date and the file's creator. Which of the following actions would most likely give the security analyst the information required?

A. Obtain the file's SHA-256 hash.
B. Use hexdump on the file's contents.
C. Check endpoint logs.
D. Query the file's metadata.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 131
Which of the following teams combines both offensive and defensive testing techniques to protect an organization's critical systems?

A. Red
B. Blue
C. Purple
D. Yellow

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 132
A small business uses kiosks on the sales floor to display product information for customers. A security team discovers the kiosks use end-of-life operating systems. Which of the following is the security team most likely to document as a security implication of the current architecture?

A. Patch availability
B. Product software compatibility
C. Ease of recovery
D. Cost of replacement

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 133
Which of the following would help ensure a security analyst is able to accurately measure the overall risk to an organization when a new vulnerability is disclosed?

A. A full inventory of all hardware and software
B. Documentation of system classifications
C. A list of system owners and their departments
D. Third-party risk assessment documentation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134
Which of the following best practices gives administrators a set period to perform changes to an operational system to ensure availability and minimize business impacts?

A. Impact analysis
B. Scheduled downtime
C. Backout plan
D. Change management boards

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 135
A company must ensure sensitive data at rest is rendered unreadable. Which of the following will the company most likely use?

A. Hashing
B. Tokenization

C. Encryption
D. Segmentation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 136
A legacy device is being decommissioned and is no longer receiving updates or patches. Which of the following describes this scenario?

A. End of business
B. End of testing
C. End of support
D. End of life

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 137
A bank insists all of its vendors must prevent data loss on stolen laptops. Which of the following strategies is the bank requiring?

A. Encryption at rest
B. Masking
C. Data classification
D. Permission restrictions

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 138
A company's end users are reporting that they are unable to reach external websites. After reviewing the performance data for the DNS severs, the analyst discovers that the CPU, disk, and memory usage are minimal, but the network interface is flooded with inbound traffic. Network logs show only a small number of DNS queries sent to this server. Which of the following best describes what the security analyst is seeing?

A. Concurrent session usage
B. Secure DNS cryptographic downgrade
C. On-path resource consumption
D. Reflected denial of service

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 139
A systems administrator wants to prevent users from being able to access data based on their responsibilities. The administrator also wants to apply the required access structure via a simplified format. Which of the following should the administrator apply to the site recovery resource group?

A. RBAC
B. ACL
C. SAML
D. GPO

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 140
During the onboarding process, an employee needs to create a password for an intranet account. The password must include ten characters, numbers, and letters, and two special characters. Once the password is created, the company will grant the employee access to other company-owned websites based on the intranet profile. Which of the following access management concepts is the company most likely using to safeguard intranet accounts and grant access to multiple sites based on a user's intranet account? (Choose two.)

A. Federation
B. Identity proofing
C. Password complexity
D. Default password changes
E. Password manager
F. Open authentication

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 141
Which of the following describes a security alerting and monitoring tool that collects system, application, and network logs from multiple sources in a centralized system?

A. SIEM
B. DLP
C. IDS
D. SNMP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 142
A network manager wants to protect the company's VPN by implementing multifactor authentication that uses:

- Something you know
- Something you have
- Something you are

Which of the following would accomplish the manager's goal?

A. Domain name, PKI, GeoIP lookup
B. VPN IP address, company ID, facial structure
C. Password, authentication token, thumbprint
D. Company URL, TLS certificate, home address

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 143
Which of the following would be the best way to handle a critical business application that is running on a legacy server?

A. Segmentation
B. Isolation
C. Hardening
D. Decommissioning

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 144
Which of the following vulnerabilities is exploited when an attacker overwrites a register with a malicious address?

A. VM escape
B. SQL injection
C. Buffer overflow
D. Race condition

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 145
After a company was compromised, customers initiated a lawsuit. The company's attorneys have requested that the security team initiate a legal hold in response to the lawsuit. Which of the following describes the action the security team will most likely be required to take?

A. Retain the emails between the security team and affected customers for 30 days.
B. Retain any communications related to the security breach until further notice.
C. Retain any communications between security members during the breach response.
D. Retain all emails from the company to affected customers for an indefinite period of time.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 146
Which of the following describes the process of concealing code or text inside a graphical image?

A. Symmetric encryption
B. Hashing
C. Data masking
D. Steganography

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 147
An employee receives a text message from an unknown number claiming to be the company's Chief Executive Officer and asking the employee to purchase several gift cards. Which of the following types of attacks does this describe?

A. Vishing
B. Smishing
C. Pretexting
D. Phishing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 148
Which of the following risk management strategies should an enterprise adopt first if a legacy application is critical to business operations and there are preventative controls that are not yet implemented?

A. Mitigate
B. Accept

C. Transfer
D. Avoid

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 149
Visitors to a secured facility are required to check in with a photo ID and enter the facility through an access control vestibule. Which of the following best describes this form of security control?

A. Physical
B. Managerial
C. Technical
D. Operational

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 150
The local administrator account for a company's VPN appliance was unexpectedly used to log in to the remote management interface. Which of the following would have most likely prevented this from happening?

A. Using least privilege
B. Changing the default password
C. Assigning individual user IDs
D. Reviewing logs more frequently

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 151
Which of the following is the best way to secure an on-site data center against intrusion from an insider?

A. Bollards
B. Access badge
C. Motion sensor
D. Video surveillance

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 152
An engineer moved to another team and is unable to access the new team's shared folders while still being able to access the shared folders from the former team. After opening a ticket, the engineer discovers that the account was never moved to the new group. Which of the following access controls is most likely causing the lack of access?

A. Role-based
B. Discretionary
C. Time of day
D. Least privilege

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 153
Which of the following factors are the most important to address when formulating a training curriculum plan for a security awareness program? (Choose two.)

A. Channels by which the organization communicates with customers
B. The reporting mechanisms for ethics violations
C. Threat vectors based on the industry in which the organization operates
D. Secure software development training for all personnel
E. Cadence and duration of training events
F. Retraining requirements for individuals who fail phishing simulations

Correct Answer: BF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 154
A network administrator is working on a project to deploy a load balancer in the company's cloud environment. Which of the following fundamental security requirements does this project fulfil?

A. Privacy
B. Integrity
C. Confidentiality
D. Availability

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 155
A systems administrator is changing the password policy within an enterprise environment and wants this

update implemented on all systems as quickly as possible. Which of the following operating system security measures will the administrator most likely use?

A. Deploying PowerShell scripts
B. Pushing GPO update
C. Enabling PAP
D. Updating EDR profiles

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 156
Which of the following would be most useful in determining whether the long-term cost to transfer a risk is less than the impact of the risk?

A. ARO
B. RTO
C. RPO
D. ALE
E. SLE

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference: