https://www.leads4pass.com/sy0-701.html

Vendor: CompTIA
Exam Code: SY0-701
Exam Name: CompTIA Security+
Certification: CompTIA Certifications
Total Questions: 867 Q&A (View Details)
Updated on: Feb 22, 2026

Question 1:

A company is currently utilizing usernames and passwords, and it wants to integrate an MFA method that is seamless, can integrate easily into a user\'s workflow, and can utilize employee-owned devices. Which of the following will meet these requirements?

A. Push notifications

B. Phone call

C. Smart card

D. Offline backup codes

Correct Answer: A

Push notifications offer a seamless and user-friendly method of multi-factor authentication (MFA) that can easily integrate into a user\'s workflow. This method leverages employee-owned devices, like smartphones, to approve authentication

requests through a push notification. It\'s convenient, quick, and doesn\'t require the user to input additional codes, making it a preferred choice for seamless integration with existing workflows.

References:

CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations. CompTIA Security+ SY0-601 Study Guide: Chapter on Identity and Access Management.

Question 2:

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

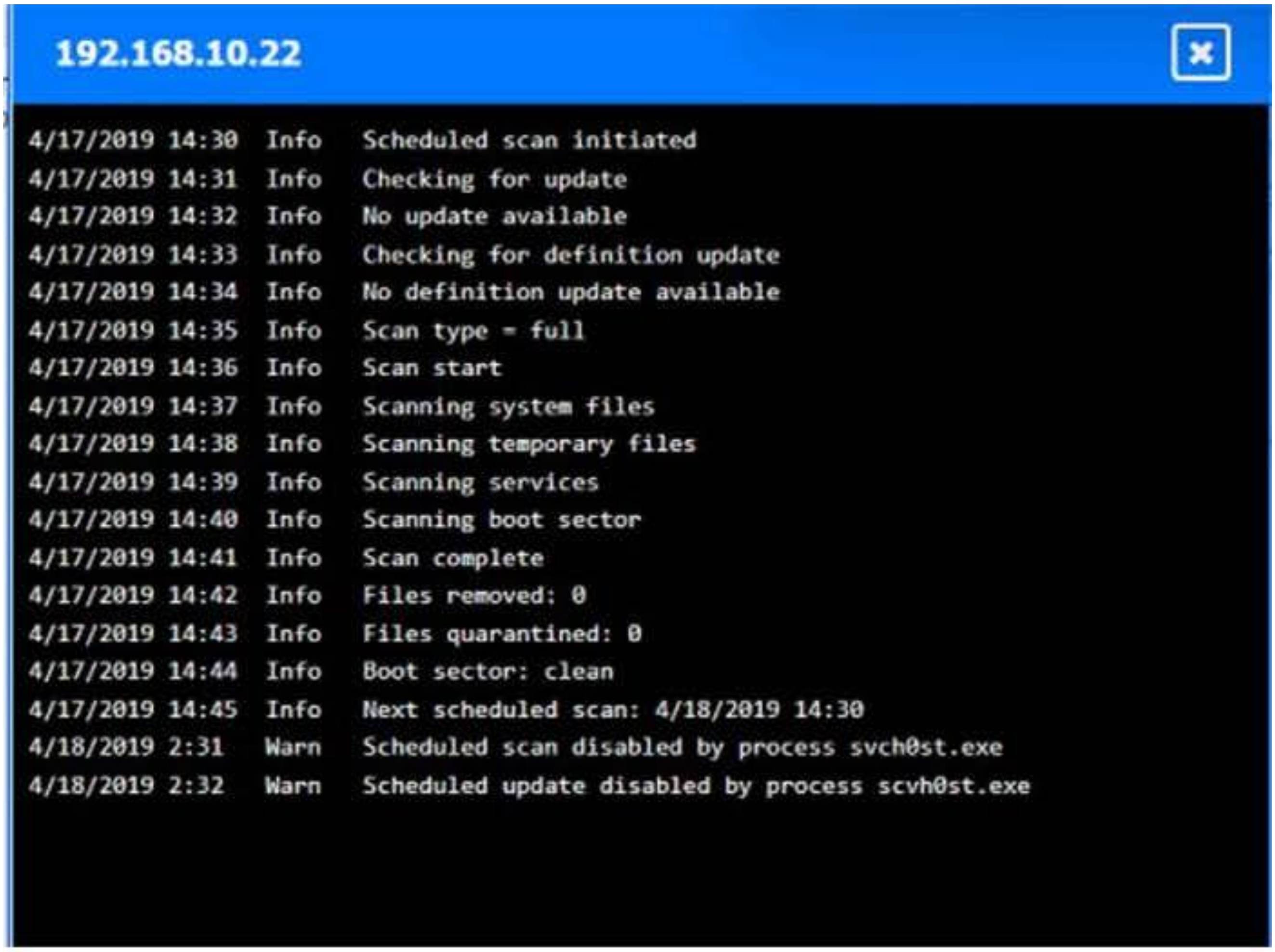
SIEM stands for Security Information and Event Management. It is a security alerting and monitoring tool that collects system, application, and network logs from multiple sources in a centralized system. SIEM can analyze the collected data, correlate events, generate alerts, and provide reports and dashboards. SIEM can also integrate with other security tools and support compliance requirements. SIEM helps organizations to detect and respond to cyber threats, improve security posture, and reduce operational costs.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 10: Monitoring and Auditing, page 393. CompTIA Security+ Practice Tests: Exam SY0-701, 3rd Edition, Chapter 10: Monitoring and Auditing, page 397.

Question 3:

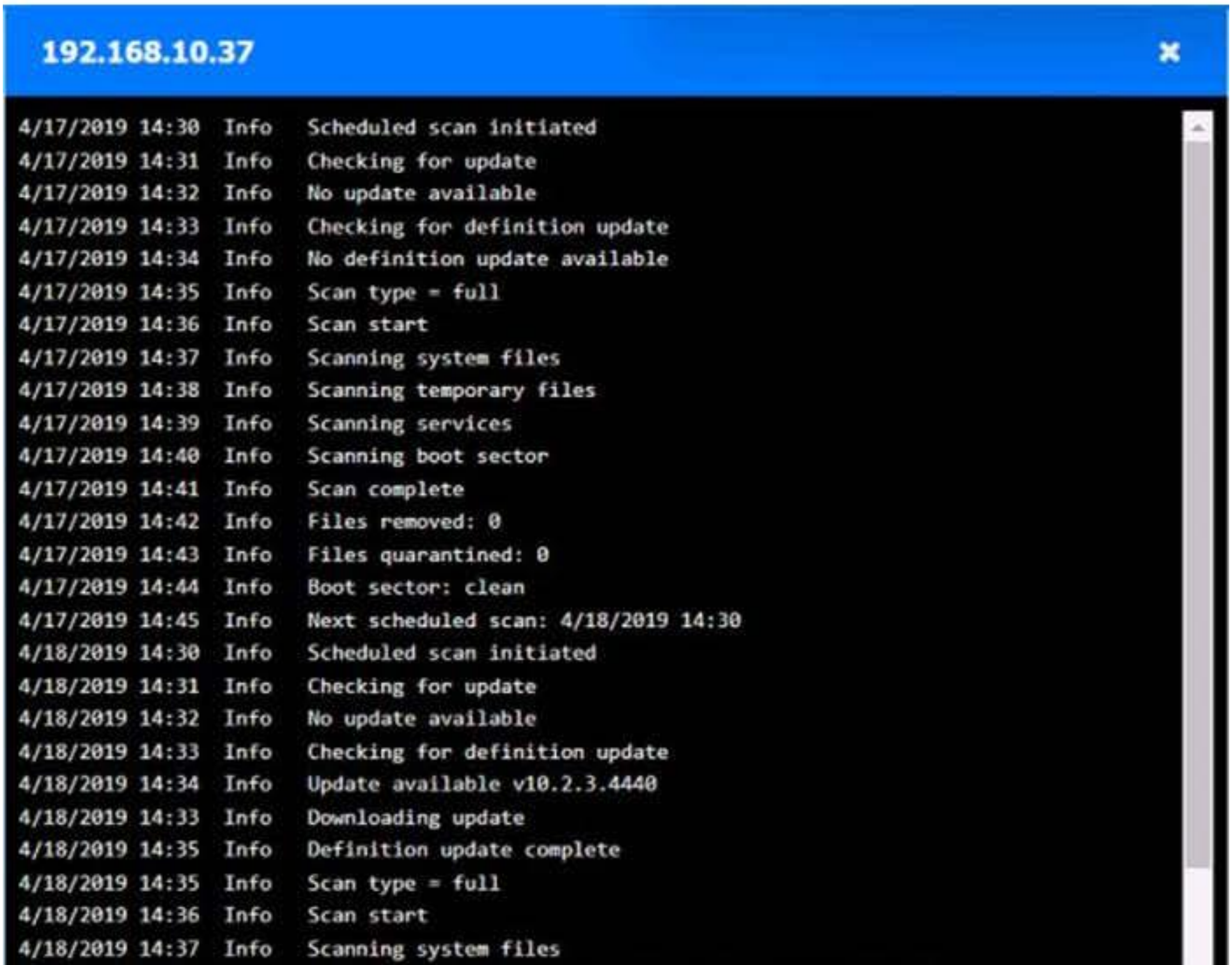
You are security administrator investigating a potential infection on a network.

Click on each host and firewall. Review all logs to determine which host originated the Infecton and then deny each remaining hosts clean or infected.



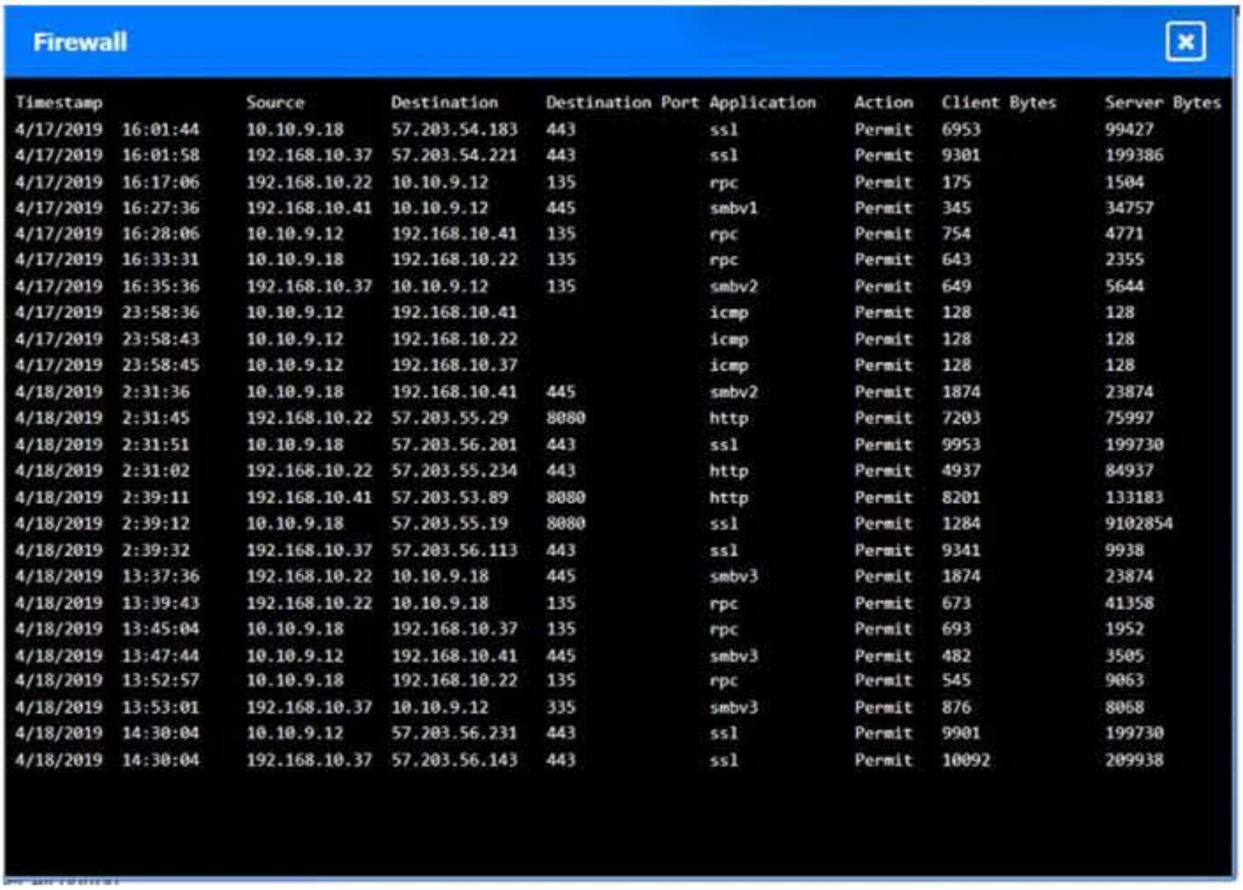
192.168.10.22

```
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
```

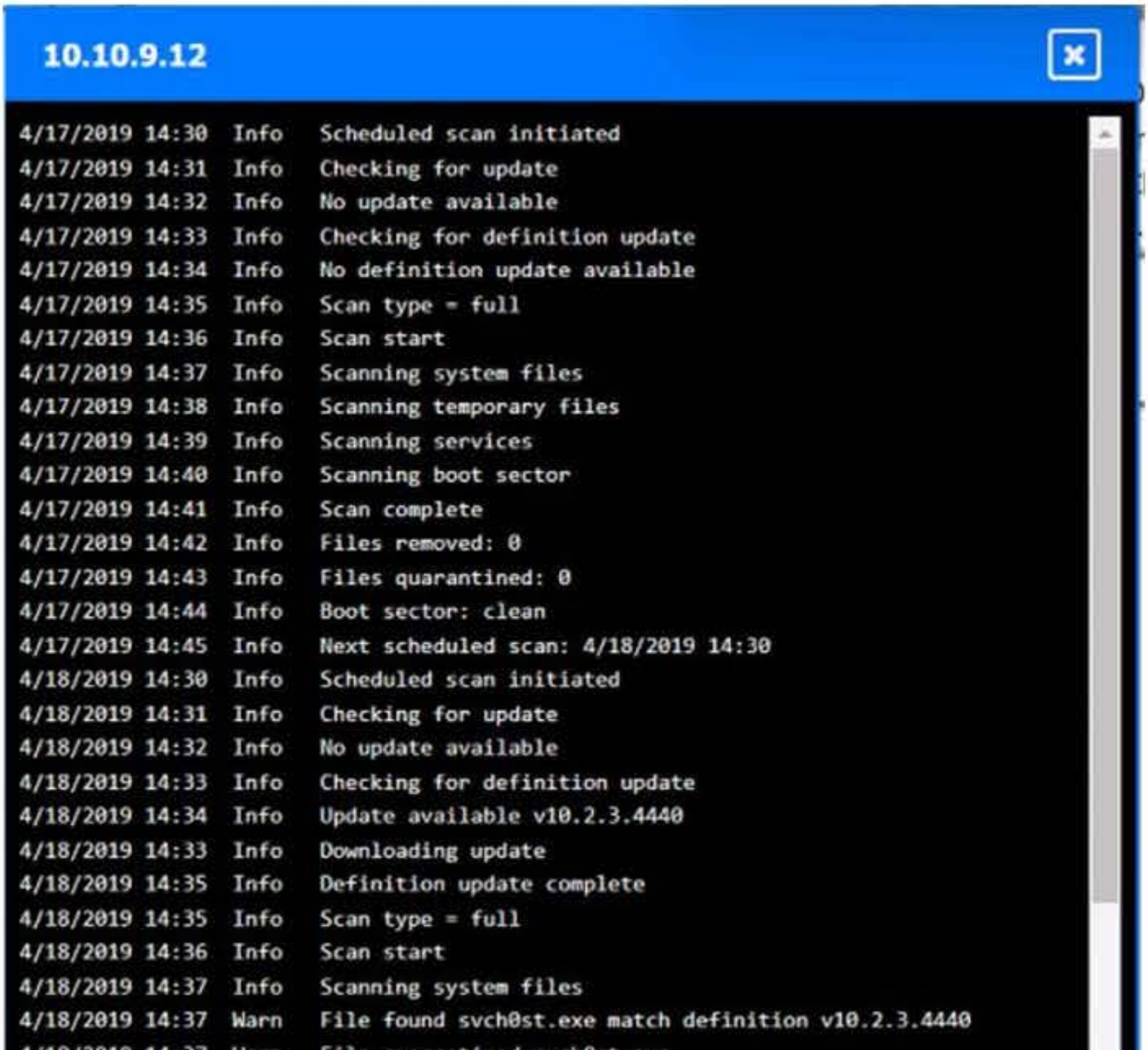


192.168.10.37

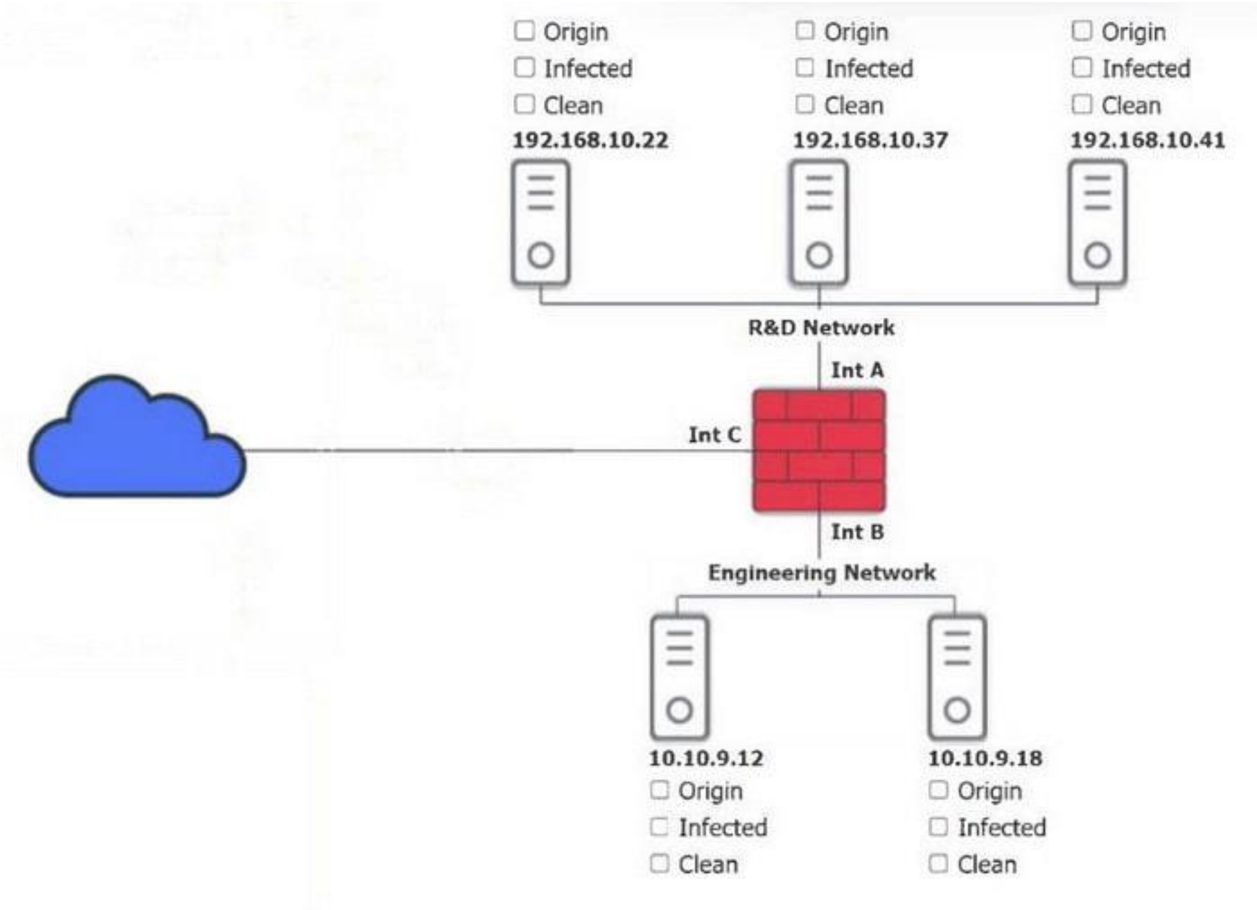
```
4/17/2019 14:30  Info   Scheduled scan initiated
4/17/2019 14:31  Info   Checking for update
4/17/2019 14:32  Info   No update available
4/17/2019 14:33  Info   Checking for definition update
4/17/2019 14:34  Info   No definition update available
4/17/2019 14:35  Info   Scan type = full
4/17/2019 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
```



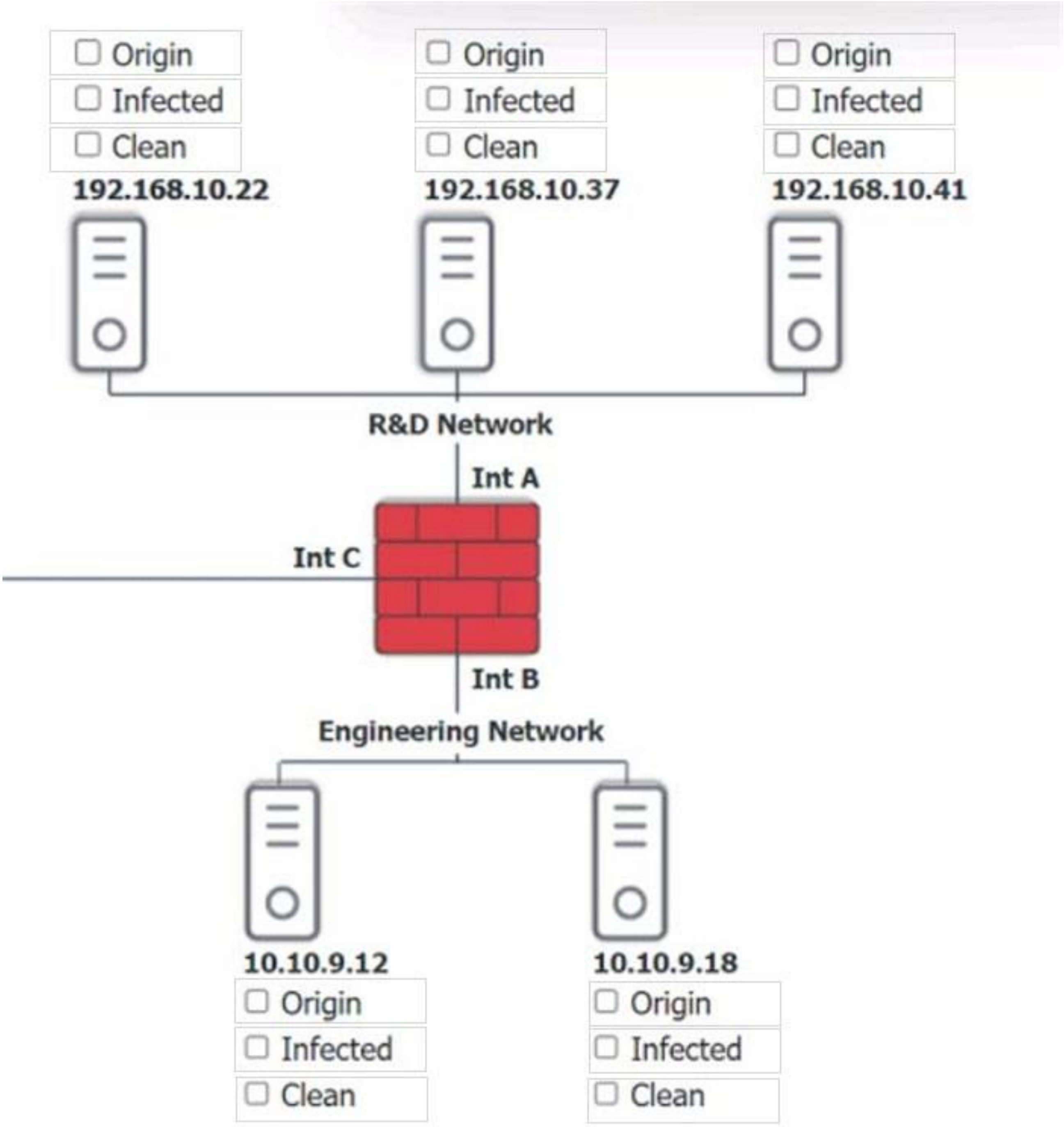
```
Timestamp            Source          Destination     Destination Port Application  Action  Client Bytes  Server Bytes
4/17/2019  16:01:44  10.10.9.18      57.203.54.183   443              ssl          Permit  6953          99427
4/17/2019  16:01:58  192.168.10.37   57.203.54.221   443              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
```



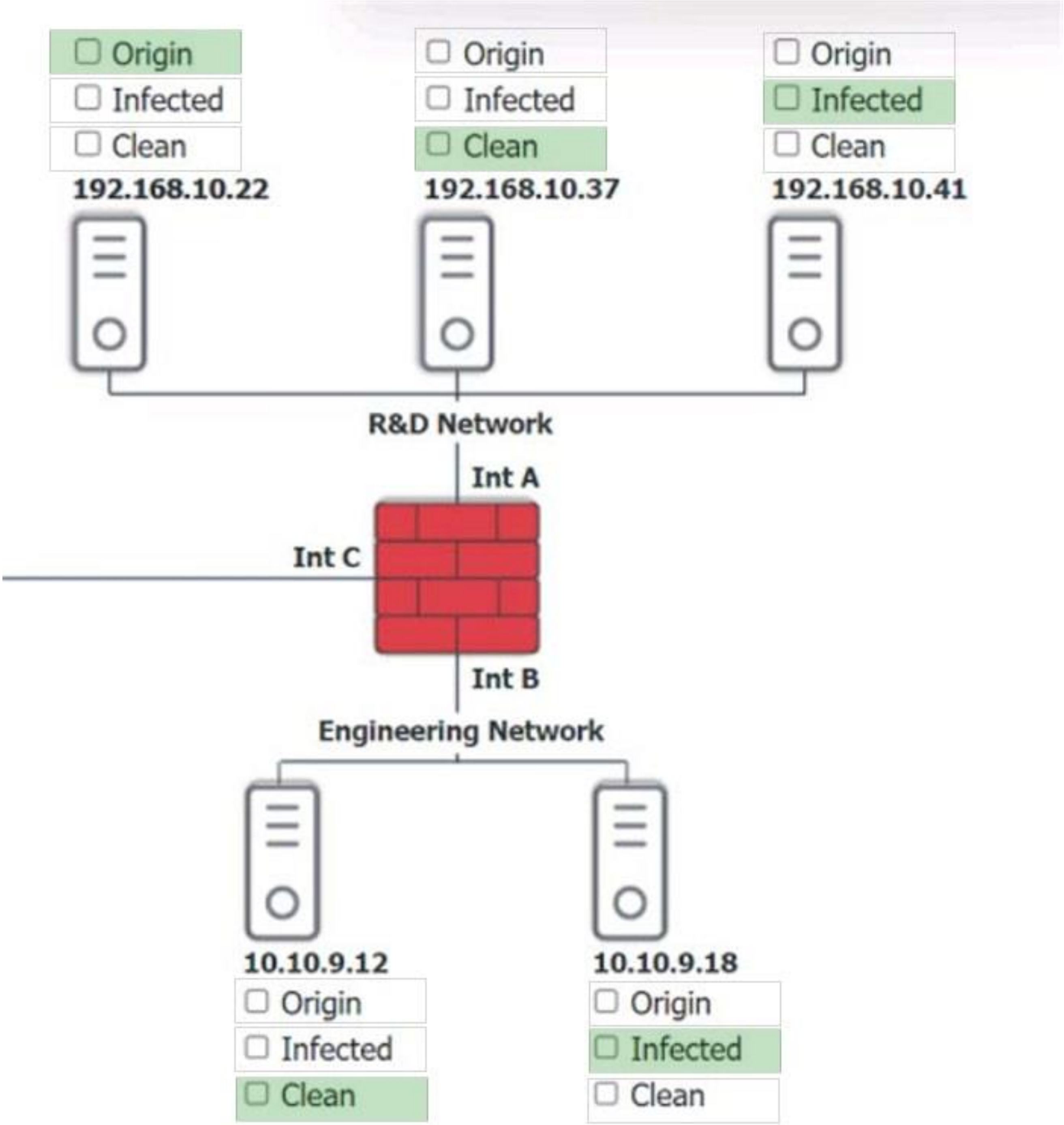
```
4/17/2019 14:30  Info   Scheduled scan initiated
4/17/2019 14:31  Info   Checking for update
4/17/2019 14:32  Info   No update available
4/17/2019 14:33  Info   Checking for definition update
4/17/2019 14:34  Info   No definition update available
4/17/2019 14:35  Info   Scan type = full
4/17/2019 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
```


□ Origin
□ Infected
□ Clean
192.168.10.22
□ Origin
□ Infected
□ Clean
192.168.10.37
□ Origin
□ Infected
□ Clean
192.168.10.41
R&D Network
Int A
Int C
Int B
Engineering Network
10.10.9.12
□ Origin
□ Infected
□ Clean
10.10.9.18
□ Origin
□ Infected
□ Clean

Hot Area:



Correct Answer:



Question 4:

A bank set up a new server that contains customers\' PII. Which of the following should the bank use to make sure the sensitive data is not modified?

A. Full disk encryption

B. Network access control

C. File integrity monitoring

D. User behavior analytics

Correct Answer: C

Question 5:
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

Scheduled downtime is a planned period of time when a system or service is unavailable for maintenance, updates, upgrades, or other changes. Scheduled downtime gives administrators a set period to perform changes to an operational

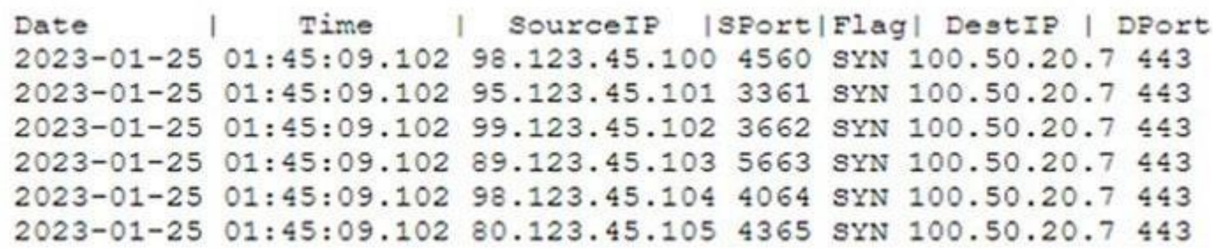
system without disrupting the normal business operations or affecting the availability of the system or service. Scheduled downtime also allows administrators to inform the users and stakeholders about the expected duration and impact of the

changes.

References:

CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 12: Security Operations and Administration, page 579 1

Question 6:
A systems administrator is advised that an external web server is not functioning property. The administrator reviews the following firewall logs containing traffic going to the web server:



```
Date       |     Time     |  SourceIP   |SPort|Flag| DestIP  | DPort
2023-01-25 01:45:09.102 98.123.45.100 4560 SYN 100.50.20.7 443
2023-01-25 01:45:09.102 95.123.45.101 3361 SYN 100.50.20.7 443
2023-01-25 01:45:09.102 99.123.45.102 3662 SYN 100.50.20.7 443
2023-01-25 01:45:09.102 89.123.45.103 5663 SYN 100.50.20.7 443
2023-01-25 01:45:09.102 98.123.45.104 4064 SYN 100.50.20.7 443
2023-01-25 01:45:09.102 80.123.45.105 4365 SYN 100.50.20.7 443
```

Which of the following attacks is likely occurring?

A. DDoS

B. Directory traversal

C. Brute-force

D. HTTPS downgrade

Correct Answer: A

Question 7:

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: D

Question 8:

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 ig source 0.0.0.0/0 destination 10.1.4.9/32

B. access-list inbound deny ig source 10.1.4.9/32 destination 0.0.0.0/0

C. access-list inbound permit ig source 10.1.4.9/32 destination 0.0.0.0/0

D. access-list inbound permit ig source 0.0.0.0/0 destination 10.1.4.9/32

Correct Answer: B

A firewall rule is a set of criteria that determines whether to allow or deny a packet to pass through the firewall. A firewall rule consists of several elements, such as the action, the protocol, the source address, the destination address, and the port number. The syntax of a firewall rule may vary depending on the type and vendor of the firewall, but the basic logic is the same. In this question, the security analyst is creating an inbound firewall rule to block the IP address 10.1.4.9 from accessing the organization\'s network. This means that the action should be deny, the protocol should be any (or ig for IP), the source address should be 10.1.4.9/32 (which means a single IP address), the destination address should be 0.0.0.0/0 (which means any IP address), and the port number should be any. Therefore, the correct firewall rule is: access-list inbound deny ig source 10.1.4.9/32 destination 0.0.0.0/0 This rule will match any packet that has the source IP address of 10.1.4.9 and drop it. The other options are incorrect because they either have the wrong action, the wrong source address, or the wrong destination address. For example, option A has the source and destination addresses reversed, which means that it will block any packet that has the destination IP address of 10.1.4.9, which is not the intended goal. Option C has the wrong action, which is permit, which means that it will allow the packet to pass through the firewall, which is also not the intended goal. Option D has the same problem as option A, with the source and destination addresses reversed.

References: Firewall Rules -CompTIA Security+ SY0-401: 1.2, Firewalls -SY0-601 CompTIA Security+ : 3.3, Firewalls -CompTIA Security+ SY0-501, Understanding Firewall Rules -CompTIA Network+ N10-005: 5.5, Configuring Windows Firewall -CompTIA A+ 220-1102 -1.6.

Question 9:
Which of the following data roles is responsible for identifying risks and appropriate access to data?

A. Owner

B. Custodian

C. Steward D. Controller

Correct Answer: A

The data owner is the role responsible for identifying risks to data and determining who should have access to that data. The owner has the authority to make decisions about the protection and usage of the data, including setting access

controls and ensuring that appropriate security measures are in place.

References: CompTIA Security+ SY0-701 study materials, particularly in the domain of data governance and the roles and responsibilities associated with data management.

Question 10:
A company hired a security manager from outside the organization to lead security operations. Which of the following actions should the security manager perform first in this new role?

A. Establish a security baseline.

B. Review security policies.

C. Adopt security benchmarks.

D. Perform a user ID revalidation.

Correct Answer: B

When a security manager is hired from outside the organization to lead security operations, the first action should be to review the existing security policies. Understanding the current security policies provides a foundation for identifying

strengths, weaknesses, and areas that require improvement, ensuring that the security program aligns with the organization\'s goals and regulatory requirements. Review security policies: Provides a comprehensive understanding of the

existing security framework, helping the new manager to identify gaps and areas for enhancement.

Establish a security baseline: Important but should be based on a thorough understanding of existing policies and practices.

Adopt security benchmarks: Useful for setting standards, but reviewing current policies is a necessary precursor.

Perform a user ID revalidation: Important for ensuring user access is appropriate but not the first step in understanding overall security operations. Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 5.1 - Summarize elements

of effective security governance (Reviewing security policies).

Question 11:
Various stakeholders are meeting to discuss their hypothetical roles and responsibilities in a specific situation, such as a security incident or major disaster. Which of the following best describes this meeting?

A. Penetration test

B. Continuity of operations planning

C. Tabletop exercise

D. Simulation

Correct Answer: C

A tabletop exercise is a discussion-based exercise where stakeholders gather to walk through the roles and responsibilities they would have during a specific situation, such as a security incident or disaster. This type of exercise is designed

to identify gaps in planning and improve coordination among team members without the need for physical execution.

References: CompTIA Security+ SY0-701 study materials, particularly in the domain of security operations and disaster recovery planning.

Question 12:
Which of the following is most likely to be deployed to obtain and analyze attacker activity and techniques?

A. Firewall

B. IDS

C. Honeypot

D. Layer 3 switch

Correct Answer: C

A honeypot is most likely to be deployed to obtain and analyze attacker activity and techniques. A honeypot is a decoy system set up to attract attackers, providing an opportunity to study their methods and behaviors in a controlled

environment without risking actual systems.

Honeypot: A decoy system designed to lure attackers, allowing administrators to observe and analyze attack patterns and techniques. Firewall: Primarily used to block unauthorized access to networks, not for observing attacker behavior. IDS

(Intrusion Detection System): Detects and alerts on malicious activity but does not specifically engage attackers to observe their behavior. Layer 3 switch: Used for routing traffic within networks, not for analyzing attacker techniques.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 2.4 - Indicators of malicious activity (Honeypots).

Question 13:
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

A full inventory of all hardware and software is essential for measuring the overall risk to an organization when a new vulnerability is disclosed, because it allows the security analyst to identify which systems are affected by the vulnerability and prioritize the remediation efforts. Without a full inventory, the security analyst may miss some vulnerable systems or waste time and resources on irrelevant ones. Documentation of system classifications, a list of system owners and their departments, and third-party risk assessment documentation are all useful for risk management, but they are not sufficient to measure the impact of a new vulnerability. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 1221; Risk Assessment and Analysis Methods: Qualitative and Quantitative3

Question 14:
Which of the following automation use cases would best enhance the security posture of an organization by rapidly updating permissions when employees leave a company?

A. Provisioning resources

B. Disabling access

C. Reviewing change approvals

D. Escalating permission requests

Correct Answer: B

Disabling access is an automation use case that would best enhance the security posture of an organization by rapidly updating permissions when employees leave a company. Disabling access is the process of revoking or suspending the access rights of a user account, such as login credentials, email, VPN, cloud services, etc. Disabling access can prevent unauthorized or malicious use of the account by former employees or attackers who may have compromised the account. Disabling access can also reduce the attack surface and the risk of data breaches or leaks. Disabling access can be automated by using scripts, tools, or workflows that can trigger the action based on predefined events, such as employee termination, resignation, or transfer. Automation can ensure that the access is disabled in a timely, consistent, and efficient manner, without relying on manual intervention or human error.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 5: Identity and Access Management, page 2131. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 5: Identity and Access Management, page 2132.

Question 15:
Which of the following is best used to detect fraud by assigning employees to different roles?

A. Least privilege

B. Mandatory vacation

C. Separation of duties

D. Job rotation

Correct Answer: D

Job rotation is a strategy used in organizations to detect and prevent fraud by periodically assigning employees to different roles within the organization. This approach helps ensure that no single employee has exclusive control over a

specific process or set of tasks for an extended period, thereby reducing the opportunity for fraudulent activities to go unnoticed. By rotating roles, organizations can uncover irregularities and discrepancies that might have been concealed by

an employee who had prolonged access to sensitive functions. Job rotation also promotes cross-training, which can enhance the organization\'s overall resilience and flexibility.

References:

CompTIA Security+ SY0-701 Course Content: Domain 05 Security Program Management and Oversight.

CompTIA Security+ SY0-601 Study Guide: Chapter on Risk Management and Compliance.