CompTIA

Exam Questions CAS-005

CompTIA SecurityX Exam

NEW QUESTION 1
Which of the following best explains the business requirement a healthcare provider fulfills by encrypting patient data at rest?

A. Securing data transfer between hospitals
B. Providing for non-repudiation data
C. Reducing liability from identity theft
D. Protecting privacy while supporting portability.

Answer: D

Explanation:
Encrypting patient data at rest is a critical requirement for healthcare providers to ensure compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA). The primary business requirement fulfilled by this practice is the protection of patient privacy while supporting the portability of medical information. By encrypting data at rest, healthcare providers safeguard sensitive patient information from unauthorized access, ensuring that privacy is maintained even if the storage media are compromised. Additionally, encryption supports the portability of patient records, allowing for secure transfer and access across different systems and locations while ensuring that privacy controls are in place.
References:
? CompTIA SecurityX Study Guide: Emphasizes the importance of data encryption for protecting sensitive information and ensuring compliance with regulatory requirements.
? HIPAA Security Rule: Requires healthcare providers to implement safeguards, including encryption, to protect patient data.
? "Health Informatics: Practical Guide for Healthcare and Information Technology Professionals" by Robert E. Hoyt: Discusses encryption as a key measure for protecting patient data privacy and supporting data portability.

NEW QUESTION 2
An organization wants to implement a platform to better identify which specific assets are affected by a given vulnerability. Which of the following components provides the best foundation to achieve this goal?

A. SASE
B. CMDB
C. SBoM
D. SLM

Answer: B

Explanation:
A Configuration Management Database (CMDB) provides the best foundation for identifying which specific assets are affected by a given vulnerability. A CMDB maintains detailed information about the IT environment, including hardware, software, configurations, and relationships between assets. This comprehensive view allows organizations to quickly identify and address vulnerabilities affecting specific assets. References:
? CompTIA SecurityX Study Guide: Discusses the role of CMDBs in asset management and vulnerability identification.
? ITIL (Information Technology Infrastructure Library) Framework: Recommends the
use of CMDBs for effective configuration and asset management.
? "Configuration Management Best Practices" by Bob Aiello and Leslie Sachs: Covers the importance of CMDBs in managing IT assets and addressing vulnerabilities.

NEW QUESTION 3
A company is having issues with its vulnerability management program New devices/IPs are added and dropped regularly, making the vulnerability report inconsistent Which of the following actions should the company lake to most likely improve the vulnerability management process'

A. Request a weekly report with all new assets deployed and decommissioned
B. Extend the DHCP lease lime to allow the devices to remain with the same address for a longer period.
C. Implement a shadow IT detection process to avoid rogue devices on the network
D. Perform regular discovery scanning throughout the 11 landscape using the vulnerability management tool

Answer: D

Explanation:
To improve the vulnerability management process in an environment where new devices/IPs are added and dropped regularly, the company should perform regular discovery scanning throughout the IT landscape using the vulnerability management tool. Here??s why:
? Accurate Asset Inventory: Regular discovery scans help maintain an up-to-date
inventory of all assets, ensuring that the vulnerability management process includes all relevant devices and IPs.
? Consistency in Reporting: By continuously discovering and scanning new and
existing assets, the company can generate consistent and comprehensive vulnerability reports that reflect the current state of the network.
? Proactive Management: Regular scans enable the organization to proactively identify and address vulnerabilities on new and existing assets, reducing the window of exposure to potential threats.
? References:

NEW QUESTION 4
The identity and access management team is sending logs to the SIEM for continuous monitoring. The deployed log collector is forwarding logs to the SIEM. However, only false positive alerts are being generated. Which of the following is the most likely reason for the inaccurate alerts?

A. The compute resources are insufficient to support the SIEM
B. The SIEM indexes are 100 large
C. The data is not being properly parsed
D. The retention policy is not property configured

Answer: C

Explanation:

Proper parsing of data is crucial for the SIEM to accurately interpret and analyze the logs being forwarded by the log collector. If the data is not parsed correctly, the SIEM may misinterpret the logs, leading to false positives and inaccurate alerts. Ensuring that the log data is correctly parsed allows the SIEM to correlate and analyze the logs effectively, which is essential for accurate alerting and monitoring.

NEW QUESTION 5
After some employees were caught uploading data to online personal storage accounts, a company becomes concerned about data leaks related to sensitive, internal documentation. Which of the following would the company most likely do to decrease this type of risk?

A. Improve firewall rules to avoid access to those platforms.
B. Implement a cloud-access security broker
C. Create SIEM rules to raise alerts for access to those platforms
D. Deploy an internet proxy that filters certain domains

Answer: B

Explanation:
A Cloud Access Security Broker (CASB) is a security policy enforcement point placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as cloud-based resources are accessed. Implementing a CASB provides several benefits:
? A. Improve firewall rules to avoid access to those platforms: This can help but is not as effective or comprehensive as a CASB.
? B. Implement a cloud-access security broker: A CASB can provide visibility into cloud application usage, enforce data security policies, and protect against data leaks by monitoring and controlling access to cloud services. It also provides advanced features like data encryption, data loss prevention (DLP), and compliance monitoring.
? C. Create SIEM rules to raise alerts for access to those platforms: This helps in
monitoring but does not prevent data leaks.
? D. Deploy an internet proxy that filters certain domains: This can block access to specific sites but lacks the granular control and visibility provided by a CASB.
Implementing a CASB is the most comprehensive solution to decrease the risk of data leaks by providing visibility, control, and enforcement of security policies for cloud services. References:
? CompTIA Security+ Study Guide
? Gartner, "Magic Quadrant for Cloud Access Security Brokers"
? NIST SP 800-144, "Guidelines on Security and Privacy in Public Cloud Computing"

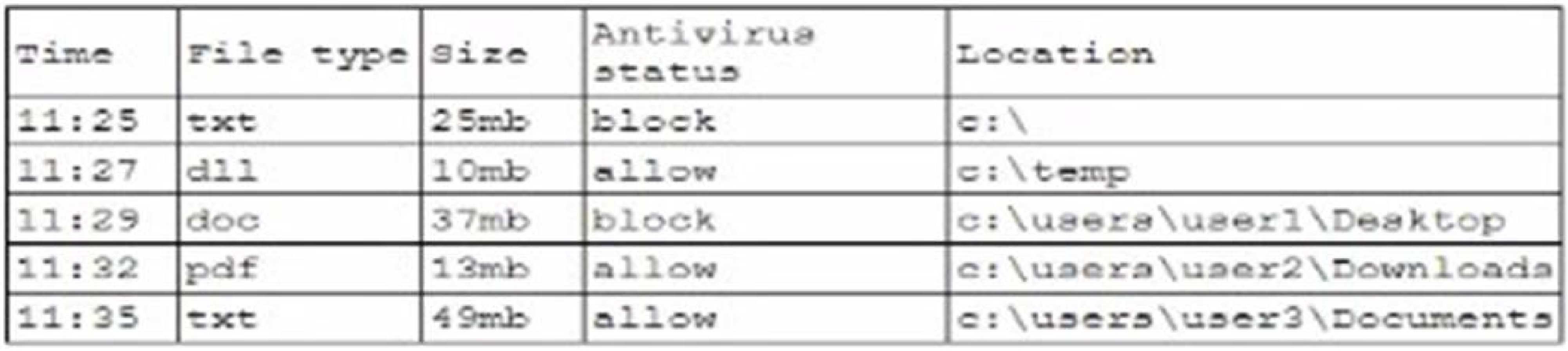
NEW QUESTION 6
A security analyst discovered requests associated with IP addresses known for born legitimate 3nd bot-related traffic. Which of the following should the analyst use to determine whether the requests are malicious?

A. User-agent string
B. Byte length of the request
C. Web application headers
D. HTML encoding field

Answer: A

Explanation:
The user-agent string can provide valuable information to distinguish between legitimate and bot-related traffic. It contains details about the browser, device, and sometimes the operating system of the client making the request.
Why Use User-Agent String?
? Identify Patterns: User-agent strings can help identify patterns that are typical of bots or legitimate users.
? Block Malicious Bots: Many bots use known user-agent strings, and identifying these can help block malicious requests.
? Anomalies Detection: Anomalous user-agent strings can indicate spoofing attempts or malicious activity.
Other options provide useful information but may not be as effective for initial determination of the nature of the request:
? B. Byte length of the request: This can indicate anomalies but does not provide
detailed information about the client.
? C. Web application headers: While useful, they may not provide enough distinction between legitimate and bot traffic.
? D. HTML encoding field: This is not typically used for identifying the nature of the request.
References:
? CompTIA SecurityX Study Guide
? "User-Agent Analysis for Security," OWASP
? NIST Special Publication 800-94, "Guide to Intrusion Detection and Prevention Systems (IDPS)"

NEW QUESTION 7
A security analyst is reviewing the following log:



Time	File type	Size	Antivirus status	Location
11:25	txt	25mb	block	c:\
11:27	dll	10mb	allow	c:\temp
11:29	doc	37mb	block	c:\users\user1\Desktop
11:32	pdf	13mb	allow	c:\users\user2\Downloads
11:35	txt	49mb	allow	c:\users\user3\Documents

Which of the following possible events should the security analyst investigate further?

A. A macro that was prevented from running
B. A text file containing passwords that were leaked
C. A malicious file that was run in this environment

D. A PDF that exposed sensitive information improperly

Answer: B

Explanation:
Based on the log provided, the most concerning event that should be investigated further is
the presence of a text file containing passwords that were leaked. Here's why:
? Sensitive Information Exposure: A text file containing passwords represents a significant security risk, as it indicates that sensitive credentials have been exposed in plain text, potentially leading to unauthorized access.
? Immediate Threat: Password leaks can lead to immediate exploitation by attackers, compromising user accounts and sensitive data. This requires urgent investi

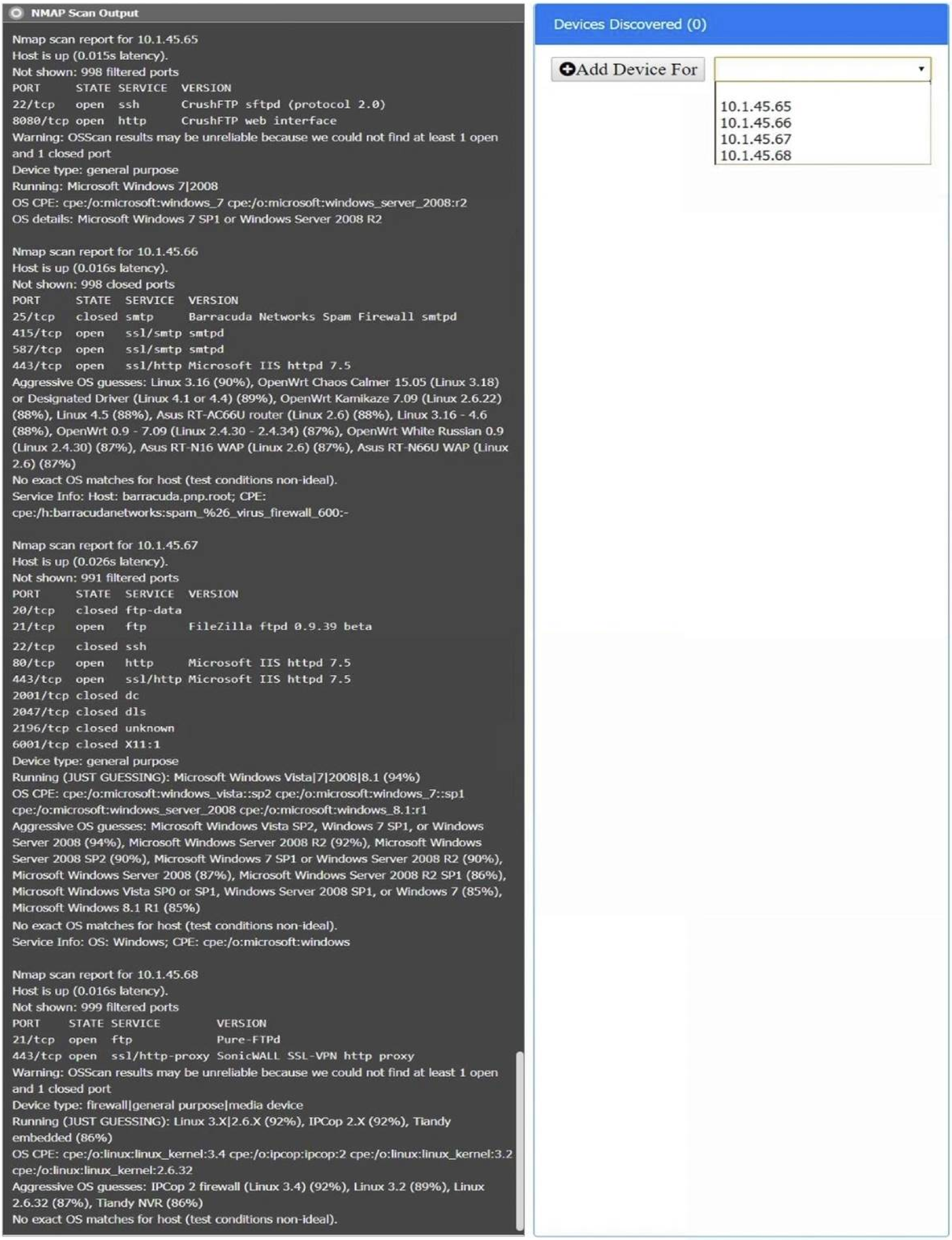
NEW QUESTION 8
A company wants to use loT devices to manage and monitor thermostats at all facilities The thermostats must receive vendor security updates and limit access to other devices within the organization Which of the following best addresses the company's requirements"

A. Only allowing Internet access to a set of specific domains
B. Operating lot devices on a separate network with no access to other devices internally
C. Only allowing operation for loT devices during a specified time window
D. Configuring IoT devices to always allow automatic updates

Answer: B

Explanation:
The best approach for managing and monitoring IoT devices, such as thermostats, is to operate them on a separate network with no access to other internal devices. This segmentation ensures that the IoT devices are isolated from the main network, reducing the risk of potential security breaches affecting other critical systems. Additionally, this setup allows for secure vendor updates without exposing the broader network to potential vulnerabilities inherent in IoT devices.
References:
? CompTIA SecurityX Study Guide: Recommends network segmentation for IoT devices to minimize security risks.
? NIST Special Publication 800-183, "Network of Things": Advises on the isolation of IoT devices to enhance security.
? "Practical IoT Security" by Brian Russell and Drew Van Duren: Discusses best practices for securing IoT devices, including network segmentation.

NEW QUESTION 9
SIMULATION
You are a security analyst tasked with interpreting an Nmap scan output from company??s privileged network.
The company??s hardening guidelines indicate the following: There should be one primary server or service per device. Only default ports should be used. Non-secure protocols should be disabled.
INSTRUCTIONS
Using the Nmap output, identify the devices on the network and their roles, and any open ports that should be closed.
For each device found by Nmap, add a device entry to the Devices Discovered list, with the following information:
The IP address of the device
The primary server or service of the device (Note that each IP should by associated with one service/port only)
The protocol(s) that should be disabled based on the hardening guidelines (Note that multiple ports may need to be closed to comply with the hardening guidelines)
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

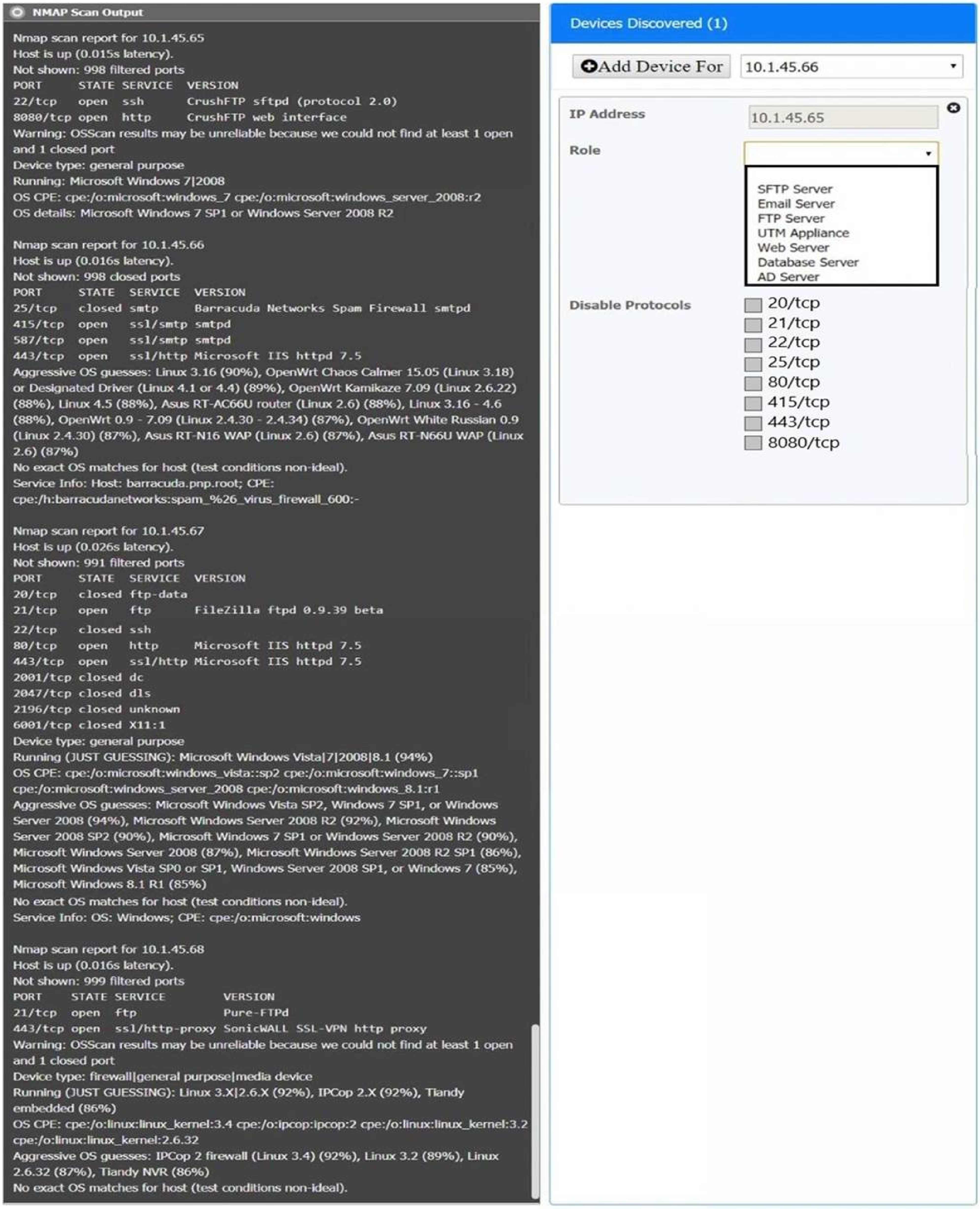


```
Nmap scan report for 10.1.45.65
Host is up (0.015s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      CrushFTP sftpd (protocol 2.0)
8080/tcp open  http     CrushFTP web interface
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008:r2
OS details: Microsoft Windows 7 SP1 or Windows Server 2008 R2

Nmap scan report for 10.1.45.66
Host is up (0.016s latency).
Not shown: 998 closed ports
PORT     STATE  SERVICE  VERSION
25/tcp   closed smtp     Barracuda Networks Spam Firewall smtpd
415/tcp  open   ssl/smtp smtpd
587/tcp  open   ssl/smtp smtpd
443/tcp  open   ssl/http Microsoft IIS httpd 7.5
Aggressive OS guesses: Linux 3.16 (90%), OpenWrt Chaos Calmer 15.05 (Linux 3.18)
or Designated Driver (Linux 4.1 or 4.4) (89%), OpenWrt Kamikaze 7.09 (Linux 2.6.22)
(88%), Linux 4.5 (88%), Asus RT-AC66U router (Linux 2.6) (88%), Linux 3.16 - 4.6
(88%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (87%), OpenWrt White Russian 0.9
(Linux 2.4.30) (87%), Asus RT-N16 WAP (Linux 2.6) (87%), Asus RT-N66U WAP (Linux
2.6) (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: barracuda.pnp.root; CPE:
cpe:/h:barracudanetworks:spam_%26_virus_firewall_600:-

Nmap scan report for 10.1.45.67
Host is up (0.026s latency).
Not shown: 991 filtered ports
PORT      STATE  SERVICE  VERSION
20/tcp    closed ftp-data
21/tcp    open   ftp      FileZilla ftpd 0.9.39 beta
22/tcp    closed ssh
80/tcp    open   http     Microsoft IIS httpd 7.5
443/tcp   open   ssl/http Microsoft IIS httpd 7.5
2001/tcp closed dc
2047/tcp closed dls
2196/tcp closed unknown
6001/tcp closed X11:1
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008|8.1 (94%)
OS CPE: cpe:/o:microsoft:windows_vista::sp2 cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008 cpe:/o:microsoft:windows_8.1:r1
Aggressive OS guesses: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows
Server 2008 (94%), Microsoft Windows Server 2008 R2 (92%), Microsoft Windows
Server 2008 SP2 (90%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (90%),
Microsoft Windows Server 2008 (87%), Microsoft Windows Server 2008 R2 SP1 (86%),
Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (85%),
Microsoft Windows 8.1 R1 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.1.45.68
Host is up (0.016s latency).
Not shown: 999 filtered ports
PORT    STATE SERVICE         VERSION
21/tcp  open  ftp             Pure-FTPd
443/tcp open  ssl/http-proxy SonicWALL SSL-VPN http proxy
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: firewall|general purpose|media device
Running (JUST GUESSING): Linux 3.X|2.6.X (92%), IPCop 2.X (92%), Tiandy
embedded (86%)
OS CPE: cpe:/o:linux:linux_kernel:3.4 cpe:/o:ipcop:ipcop:2 cpe:/o:linux:linux_kernel:3.2
cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: IPCop 2 firewall (Linux 3.4) (92%), Linux 3.2 (89%), Linux
2.6.32 (87%), Tiandy NVR (86%)
No exact OS matches for host (test conditions non-ideal).
```



NMAP Scan Output

```
Nmap scan report for 10.1.45.65
Host is up (0.015s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      CrushFTP sftpd (protocol 2.0)
8080/tcp open  http     CrushFTP web interface
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008::r2
OS details: Microsoft Windows 7 SP1 or Windows Server 2008 R2

Nmap scan report for 10.1.45.66
Host is up (0.016s latency).
Not shown: 998 closed ports
PORT     STATE  SERVICE  VERSION
25/tcp   closed smtp     Barracuda Networks Spam Firewall smtpd
415/tcp  open   ssl/smtp smtpd
587/tcp  open   ssl/smtp smtpd
443/tcp  open   ssl/http Microsoft IIS httpd 7.5
Aggressive OS guesses: Linux 3.16 (90%), OpenWrt Chaos Calmer 15.05 (Linux 3.18)
or Designated Driver (Linux 4.1 or 4.4) (89%), OpenWrt Kamikaze 7.09 (Linux 2.6.22)
(88%), Linux 4.5 (88%), Asus RT-AC66U router (Linux 2.6) (88%), Linux 3.16 - 4.6
(88%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (87%), OpenWrt White Russian 0.9
(Linux 2.4.30) (87%), Asus RT-N16 WAP (Linux 2.6) (87%), Asus RT-N66U WAP (Linux
2.6) (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: barracuda.pnp.root; CPE:
cpe:/h:barracudanetworks:spam_%26_virus_firewall_600:-

Nmap scan report for 10.1.45.67
Host is up (0.026s latency).
Not shown: 991 filtered ports
PORT     STATE  SERVICE  VERSION
20/tcp   closed ftp-data
21/tcp   open   ftp      FileZilla ftpd 0.9.39 beta
22/tcp   closed ssh
80/tcp   open   http     Microsoft IIS httpd 7.5
443/tcp  open   ssl/http Microsoft IIS httpd 7.5
2001/tcp closed dc
2047/tcp closed dls
2196/tcp closed unknown
6001/tcp closed X11:1
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008|8.1 (94%)
OS CPE: cpe:/o:microsoft:windows_vista::sp2 cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008 cpe:/o:microsoft:windows_8.1:r1
Aggressive OS guesses: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows
Server 2008 (94%), Microsoft Windows Server 2008 R2 (92%), Microsoft Windows
Server 2008 SP2 (90%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (90%),
Microsoft Windows Server 2008 (87%), Microsoft Windows Server 2008 R2 SP1 (86%),
Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (85%),
Microsoft Windows 8.1 R1 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.1.45.68
Host is up (0.016s latency).
Not shown: 999 filtered ports
PORT    STATE SERVICE        VERSION
21/tcp  open  ftp            Pure-FTPd
443/tcp open  ssl/http-proxy SonicWALL SSL-VPN http proxy
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: firewall|general purpose|media device
Running (JUST GUESSING): Linux 3.X|2.6.X (92%), IPCop 2.X (92%), Tiandy
embedded (86%)
OS CPE: cpe:/o:linux:linux_kernel:3.4 cpe:/o:ipcop:ipcop:2 cpe:/o:linux:linux_kernel:3.2
cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: IPCop 2 firewall (Linux 3.4) (92%), Linux 3.2 (89%), Linux
2.6.32 (87%), Tiandy NVR (86%)
No exact OS matches for host (test conditions non-ideal).
```

Devices Discovered (1)

Add Device For: 10.1.45.66

IP Address: 10.1.45.65

Role:

Disable Protocols

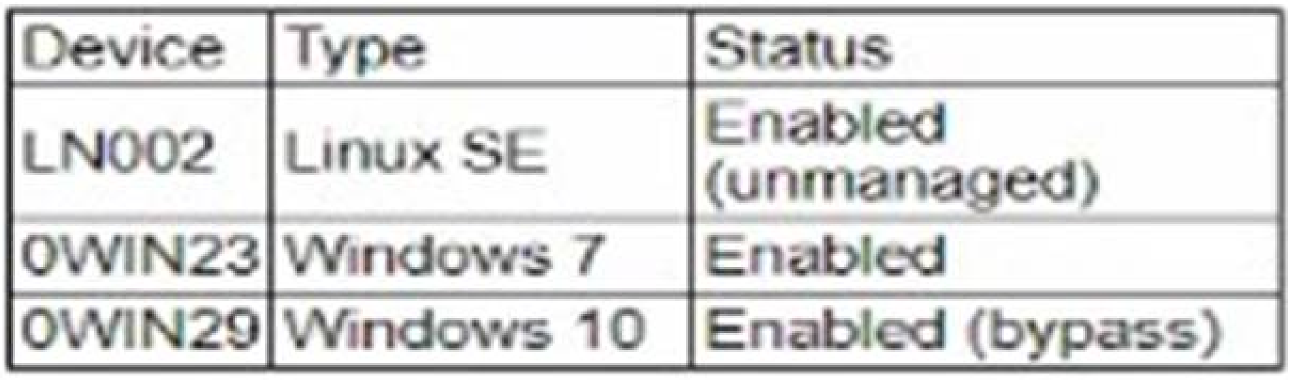
□ 20/tcp
□ 21/tcp
□ 22/tcp
□ 25/tcp
□ 80/tcp
□ 415/tcp
□ 443/tcp
□ 8080/tcp

A. Mastered
B. Not Mastered

Answer: A

Explanation:
* 10.1.45.65 SFTP Server Disable 8080
* 10.1.45.66 Email Server Disable 415 and 443
* 10.1.45.67 Web Server Disable 21, 80
* 10.1.45.68 UTM Appliance Disable 21

NEW QUESTION 10
During a security assessment using an CDR solution, a security engineer generates the following report about the assets in me system:



Device	Type	Status
LN002	Linux SE	Enabled (unmanaged)
0WIN23	Windows 7	Enabled
0WIN29	Windows 10	Enabled (bypass)

After five days, the EDR console reports an infection on the host 0WIN23 by a remote access Trojan Which of the following is the most probable cause of the infection?

A. OW1N23 uses a legacy version of Windows that is not supported by the EDR
B. LN002 was not supported by the EDR solution and propagates the RAT
C. The EDR has an unknown vulnerability that was exploited by the attacker.
D. 0W1N29 spreads the malware through other hosts in the network

Answer: A

Explanation:
OWIN23 is running Windows 7, which is a legacy operating system. Many EDR solutions no longer provide full support for outdated operating systems like Windows 7, which has reached its end of life and is no longer receiving security updates from Microsoft. This makes such systems more vulnerable to infections and attacks, including remote access Trojans (RATs).
? A. OWIN23 uses a legacy version of Windows that is not supported by the EDR:
This is the most probable cause because the lack of support means that the EDR solution may not fully protect or monitor this system, making it an easy target for infections.
? B. LN002 was not supported by the EDR solution and propagates the RAT: While LN002 is unmanaged, it is less likely to propagate the RAT to OWIN23 directly without an established vector.
? C. The EDR has an unknown vulnerability that was exploited by the attacker: This is possible but less likely than the lack of support for an outdated OS.
? D. OWIN29 spreads the malware through other hosts in the network: While this could happen, the status indicates OWIN29 is in a bypass mode, which might limit its interactions but does not directly explain the infection on OWIN23.
References:
? CompTIA Security+ Study Guide
? NIST SP 800-53, "Security and Privacy Controls for Information Systems and Organizations"
? Microsoft's Windows 7 End of Support documentation

NEW QUESTION 10
Which of the following is the main reason quantum computing advancements are leading companies and countries to deploy new encryption algorithms?

A. Encryption systems based on large prime numbers will be vulnerable to exploitation
B. Zero Trust security architectures will require homomorphic encryption.
C. Perfect forward secrecy will prevent deployment of advanced firewall monitoring techniques
D. Quantum computers will enable malicious actors to capture IP traffic in real time

Answer: A

Explanation:
Advancements in quantum computing pose a significant threat to current encryption systems, especially those based on the difficulty of factoring large prime numbers, such as RSA. Quantum computers have the potential to solve these problems exponentially faster than classical computers, making current cryptographic systems vulnerable.
Why Large Prime Numbers are Vulnerable:
? Shor's Algorithm: Quantum computers can use Shor's algorithm to factorize large integers efficiently, which undermines the security of RSA encryption.
? Cryptographic Breakthrough: The ability to quickly factor large prime numbers means that encrypted data, which relies on the hardness of this mathematical problem, can be decrypted.
Other options, while relevant, do not capture the primary reason for the shift towards new encryption algorithms:
? B. Zero Trust security architectures: While important, the shift to homomorphic encryption is not the main driver for new encryption algorithms.
? C. Perfect forward secrecy: It enhances security but is not the main reason for new encryption algorithms.
? D. Real-time IP traffic capture: Quantum computers pose a more significant threat to the underlying cryptographic algorithms than to the real-time capture of traffic.
References:
? CompTIA SecurityX Study Guide
? NIST Special Publication 800-208, "Recommendation for Stateful Hash-Based Signature Schemes"
? "Quantum Computing and Cryptography," MIT Technology Review

NEW QUESTION 14
A security officer received several complaints from users about excessive MPA push notifications at night The security team investigates and suspects malicious activities regarding user account authentication Which of the following is the best way for the security officer to restrict MI~A notifications"

A. Provisioning FID02 devices
B. Deploying a text message based on MFA
C. Enabling OTP via email
D. Configuring prompt-driven MFA

Answer: D

Explanation:
Excessive MFA push notifications can be a sign of an attempted push notification attack, where attackers repeatedly send MFA prompts hoping the user will eventually approve one by mistake. To mitigate this:
? A. Provisioning FIDO2 devices: While FIDO2 devices offer strong authentication,
they may not be practical for all users and do not directly address the issue of excessive push notifications.
? B. Deploying a text message-based MFA: SMS-based MFA can still be vulnerable
to similar spamming attacks and phishing.
? C. Enabling OTP via email: Email-based OTPs add another layer of security but do not directly solve the issue of excessive notifications.
? D. Configuring prompt-driven MFA: This option allows users to respond to prompts in a secure manner, often including features like time-limited approval windows, additional verification steps, or requiring specific actions to approve. This can help prevent users from accidentally approving malicious attempts.
Configuring prompt-driven MFA is the best solution to restrict unnecessary MFA notifications and improve security.
References:
? CompTIA Security+ Study Guide
? NIST SP 800-63B, "Digital Identity Guidelines"
? "Multi-Factor Authentication: Best Practices" by Microsoft

NEW QUESTION 16
Developers have been creating and managing cryptographic material on their personal laptops fix use in production environment. A security engineer needs to initiate a more secure process. Which of the following is the best strategy for the engineer to use?

A. Disabling the BIOS and moving to UEFI
B. Managing secrets on the vTPM hardware
C. Employing shielding lo prevent LMI
D. Managing key material on a HSM

Answer: D

Explanation:
The best strategy for securely managing cryptographic material is to use a Hardware Security Module (HSM). Here??s why:
? Security and Integrity: HSMs are specialized hardware devices designed to protect and manage digital keys. They provide high levels of physical and logical security, ensuring that cryptographic material is well protected against tampering and unauthorized access.
? Centralized Key Management: Using HSMs allows for centralized management of cryptographic keys, reducing the risks associated with decentralized and potentially insecure key storage practices, such as on personal laptops.
? Compliance and Best Practices: HSMs comply with various industry standards and regulations (such as FIPS 140-2) for secure key management. This ensures that the organization adheres to best practices and meets compliance requirements.
? References:

NEW QUESTION 18
Which of the following AI concerns is most adequately addressed by input sanitation?

A. Model inversion
B. Prompt Injection
C. Data poisoning
D. Non-explainable model

Answer: B

Explanation:
Input sanitation is a critical process in cybersecurity that involves validating and cleaning data provided by users to prevent malicious inputs from causing harm. In the context of AI concerns:
? A. Model inversion involves an attacker inferring sensitive data from model
outputs, typically requiring sophisticated methods beyond just manipulating input data.
? B. Prompt Injection is a form of attack where an adversary provides malicious input
to manipulate the behavior of AI models, particularly those dealing with natural language processing (NLP). Input sanitation directly addresses this by ensuring that inputs are cleaned and validated to remove potentially harmful commands or instructions that could alter the AI's behavior.
? C. Data poisoning involves injecting malicious data into the training set to
compromise the model. While input sanitation can help by filtering out bad data, data poisoning is typically addressed through robust data validation and monitoring during the model training phase, rather than real-time input sanitation.
? D. Non-explainable model refers to the lack of transparency in how AI models
make decisions. This concern is not addressed by input sanitation, as it relates more to model design and interpretability techniques.
Input sanitation is most relevant and effective for preventing Prompt Injection attacks, where the integrity of user inputs directly impacts the performance and security of AI models.
References:
? CompTIA Security+ Study Guide
? "Security of Machine Learning" by Battista Biggio, Blaine Nelson, and Pavel Laskov
? OWASP (Open Web Application Security Project) guidelines on input validation and injection attacks
Top of Form Bottom of Form

NEW QUESTION 21
A compliance officer is reviewing the data sovereignty laws in several countries where the organization has no presence Which of the following is the most likely reason for reviewing these laws?

A. The organization is performing due diligence of potential tax issues.
B. The organization has been subject to legal proceedings in countries where it has a presence.
C. The organization is concerned with new regulatory enforcement in other countries
D. The organization has suffered brand reputation damage from incorrect media coverage

Answer: C

Explanation:
Reviewing data sovereignty laws in countries where the organization has no presence is likely due to concerns about regulatory enforcement. Data sovereignty laws dictate how data can be stored, processed, and transferred across borders. Understanding these laws is crucial for compliance, especially if the organization handles data that may be subject to foreign regulations.
? A. The organization is performing due diligence of potential tax issues: This is less
likely as tax issues are generally not directly related to data sovereignty laws.
? B. The organization has been subject to legal proceedings in countries where it has a presence: While possible, this does not explain the focus on countries where the organization has no presence.
? C. The organization is concerned with new regulatory enforcement in other countries: This is the most likely reason. New regulations could impact the organization??s operations, especially if they involve data transfers or processing data from these countries.
? D. The organization has suffered brand reputation damage from incorrect media
coverage: This is less relevant to the need for reviewing data sovereignty laws.
References:
? CompTIA Security+ Study Guide
? GDPR and other global data protection regulations
? "Data Sovereignty: The Future of Data Protection?" by Mark Burdon

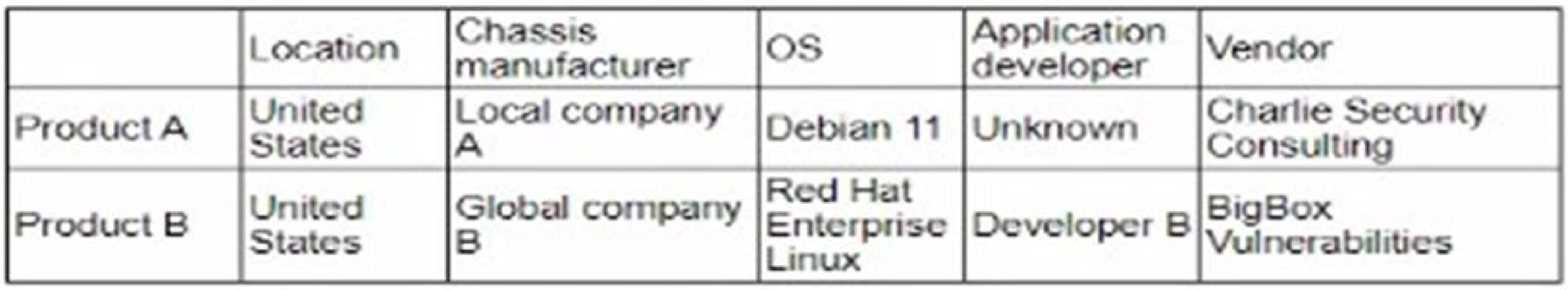
NEW QUESTION 24
Which of the following best explains the importance of determining organization risk appetite when operating with a constrained budget?

A. Risk appetite directly impacts acceptance of high-impact low-likelihood events.
B. Organizational risk appetite varies from organization to organization
C. Budgetary pressure drives risk mitigation planning in all companies
D. Risk appetite directly influences which breaches are disclosed publicly

Answer: A

Explanation:
Risk appetite is the amount of risk an organization is willing to accept to achieve its objectives. When operating with a constrained budget, understanding the organization's risk appetite is crucial because:
? It helps prioritize security investments based on the level of risk the organization is
willing to tolerate.
? High-impact, low-likelihood events may be deemed acceptable if they fall within the organization's risk appetite, allowing for budget allocation to other critical areas.
? Properly understanding and defining risk appetite ensures that limited resources are used effectively to manage risks that align with the organization's strategic goals.
References:
? CompTIA Security+ Study Guide
? NIST Risk Management Framework (RMF) guidelines
? ISO 31000, "Risk Management – Guidelines"

NEW QUESTION 26
A security analyst reviews the following report:



	Location	Chassis manufacturer	OS	Application developer	Vendor
Product A	United States	Local company A	Debian 11	Unknown	Charlie Security Consulting
Product B	United States	Global company B	Red Hat Enterprise Linux	Developer B	BigBox Vulnerabilities

Which of the following assessments is the analyst performing?

A. System
B. Supply chain
C. Quantitative
D. Organizational

Answer: B

Explanation:
The table shows detailed information about products, including location, chassis manufacturer, OS, application developer, and vendor. This type of information is typically assessed in a supply chain assessment to evaluate the security and reliability of components and services from different suppliers.
Why Supply Chain Assessment?
? Component Evaluation: Assessing the origin and security of each component used in the products, including hardware, software, and third-party services.
? Vendor Reliability: Evaluating the security practices and reliability of vendors involved in providing components or services.
? Risk Management: Identifying potential risks associated with the supply chain, such as vulnerabilities in third-party components or insecure development practices.
Other types of assessments do not align with the detailed supplier and component information provided:
? A. System: Focuses on individual system security, not the broader supply chain.
? C. Quantitative: Focuses on numerical risk assessments, not supplier information.
? D. Organizational: Focuses on internal organizational practices, not external
suppliers.
References:
? CompTIA SecurityX Study Guide
? NIST Special Publication 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations"
? "Supply Chain Security Best Practices," Gartner Research

NEW QUESTION 31
A systems administrator wants to introduce a newly released feature for an internal application. The administrate docs not want to test the feature in the production environment. Which of the following locations is the best place to test the new feature?

A. Staging environment
B. Testing environment
C. CI/CO pipeline
D. Development environment

Answer: A

Explanation:
The best location to test a newly released feature for an internal application, without affecting the production environment, is the staging environment. Here??s a detailed Explanation
? Staging Environment: This environment closely mirrors the production environment
in terms of hardware, software, configurations, and settings. It serves as a final testing ground before deploying changes to production. Testing in the staging environment ensures that the new feature will behave as expected in the actual production setup.
? Isolation from Production: The staging environment is isolated from production,
which means any issues arising from the new feature will not impact the live users or the integrity of the production data. This aligns with best practices in change management and risk mitigation.
? Realistic Testing: Since the staging environment replicates the production
environment, it provides realistic testing conditions. This helps in identifying potential issues that might not be apparent in a development or testing environment, which often have different configurations and workloads.
? References:

NEW QUESTION 36
A company that uses containers to run its applications is required to identify vulnerabilities on every container image in a private repository The security team needs to be able to quickly evaluate whether to respond to a given vulnerability Which of the following, will allow the security team to achieve the objective with the last effort?

A. SAST scan reports
B. Centralized SBoM
C. CIS benchmark compliance reports
D. Credentialed vulnerability scan

Answer: B

Explanation:
A centralized Software Bill of Materials (SBoM) is the best solution for identifying vulnerabilities in container images in a private repository. An SBoM provides a comprehensive inventory of all components, dependencies, and their versions within a container image, facilitating quick evaluation and response to vulnerabilities.
Why Centralized SBoM?
? Comprehensive Inventory: An SBoM lists all software components, including their versions and dependencies, allowing for thorough vulnerability assessments.
? Quick Identification: Centralizing SBoM data enables rapid identification of affected containers when a vulnerability is disclosed.
? Automation: SBoMs can be integrated into automated tools for continuous monitoring and alerting of vulnerabilities.
? Regulatory Compliance: Helps in meeting compliance requirements by providing a clear and auditable record of all software components used.
Other options, while useful, do not provide the same level of comprehensive and efficient vulnerability management:
? A. SAST scan reports: Focuses on static analysis of code but may not cover all components in container images.
? C. CIS benchmark compliance reports: Ensures compliance with security benchmarks but does not provide detailed component inventory.
? D. Credentialed vulnerability scan: Useful for in-depth scans but may not be as efficient for quick vulnerability evaluation.
References:
? CompTIA SecurityX Study Guide
? "Software Bill of Materials (SBoM)," NIST Documentation
? "Managing Container Security with SBoM," OWASP

NEW QUESTION 38
Audit findings indicate several user endpoints are not utilizing full disk encryption During me remediation process, a compliance analyst reviews the testing details for the endpoints and notes the endpoint device configuration does not support full disk encryption Which of the following is the most likely reason me device must be replaced'

A. The HSM is outdated and no longer supported by the manufacturer
B. The vTPM was not properly initialized and is corrupt.
C. The HSM is vulnerable to common exploits and a firmware upgrade is needed
D. The motherboard was not configured with a TPM from the OEM supplier.
E. The HSM does not support sealing storage

Answer: D

Explanation:
The most likely reason the device must be replaced is that the motherboard was not configured with a TPM (Trusted Platform Module) from the OEM (Original Equipment Manufacturer) supplier.
Why TPM is Necessary for Full Disk Encryption:
? Hardware-Based Security: TPM provides a hardware-based mechanism to store encryption keys securely, which is essential for full disk encryption.
? Compatibility: Full disk encryption solutions, such as BitLocker, require TPM to ensure that the encryption keys are securely stored and managed.
? Integrity Checks: TPM enables system integrity checks during boot, ensuring that the device has not been tampered with.
Other options do not directly address the requirement for TPM in supporting full disk encryption:
? A. The HSM is outdated: While HSM (Hardware Security Module) is important for
security, it is not typically used for full disk encryption.
? B. The vTPM was not properly initialized: vTPM (virtual TPM) is less common and not typically a reason for requiring hardware replacement.
? C. The HSM is vulnerable to common exploits: This would require a firmware upgrade, not replacement of the device.
? E. The HSM does not support sealing storage: Sealing storage is relevant but not the primary reason for requiring TPM for full disk encryption.

References:
? CompTIA SecurityX Study Guide
? "Trusted Platform Module (TPM) Overview," Microsoft Documentation
? "BitLocker Deployment Guide," Microsoft Documentation

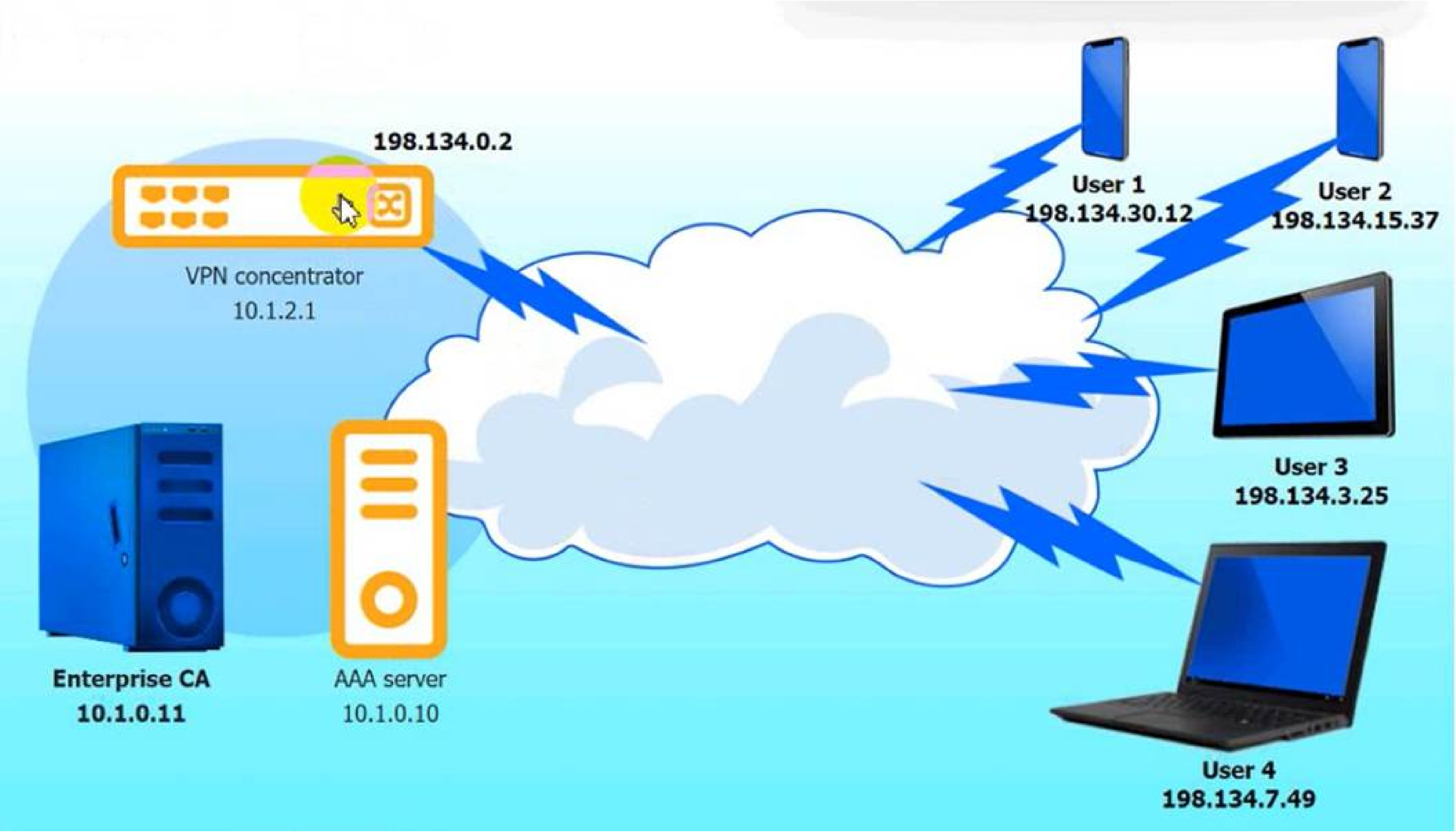
NEW QUESTION 41
A company wants to install a three-tier approach to separate the web. database, and application servers A security administrator must harden the environment which of the following is the best solution?

A. Deploying a VPN to prevent remote locations from accessing server VLANs
B. Configuring a SASb solution to restrict users to server communication
C. Implementing microsegmentation on the server VLANs
D. installing a firewall and making it the network core

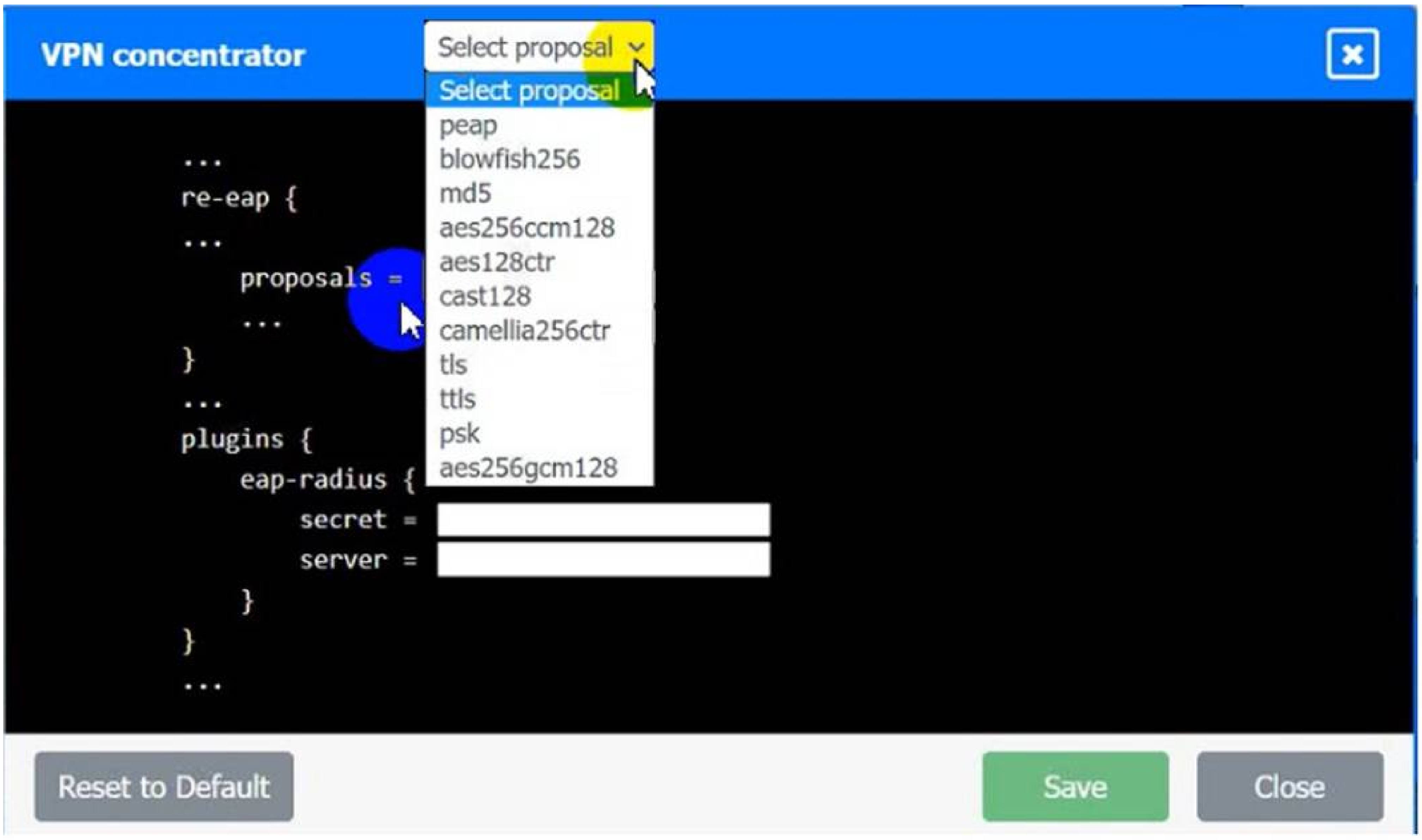
Answer: C

Explanation:
The best solution to harden a three-tier environment (web, database, and application servers) is to implement microsegmentation on the server VLANs. Here??s why:
? Enhanced Security: Microsegmentation creates granular security zones within the data center, allowing for more precise control over east-west traffic between servers. This helps prevent lateral movement by attackers who may gain access to one part of the network.
? Isolation of Tiers: By segmenting the web, database, and application servers, the organization can apply specific security policies and controls to each segment, reducing the risk of cross-tier attacks.
? Compliance and Best Practices: Microsegmentation aligns with best practices for network security and helps meet compliance requirements by ensuring that sensitive data and systems are properly isolated and protected.
? References:

NEW QUESTION 43
SIMULATION
An IPSec solution is being deployed. The configuration files for both the VPN concentrator and the AAA server are shown in the diagram.
Complete the configuration files to meet the following requirements:
• The EAP method must use mutual certificate-based authentication (With issued client certificates).
• The IKEv2 Cipher suite must be configured to the MOST secure authenticated mode of operation,
• The secret must contain at least one uppercase character, one lowercase character, one numeric character, and one special character, and it must meet a minimum length requirement of eight characters,
INSTRUCTIONS
Click on the AAA server and VPN concentrator to complete the configuration. Fill in the appropriate fields and make selections from the drop-down menus.

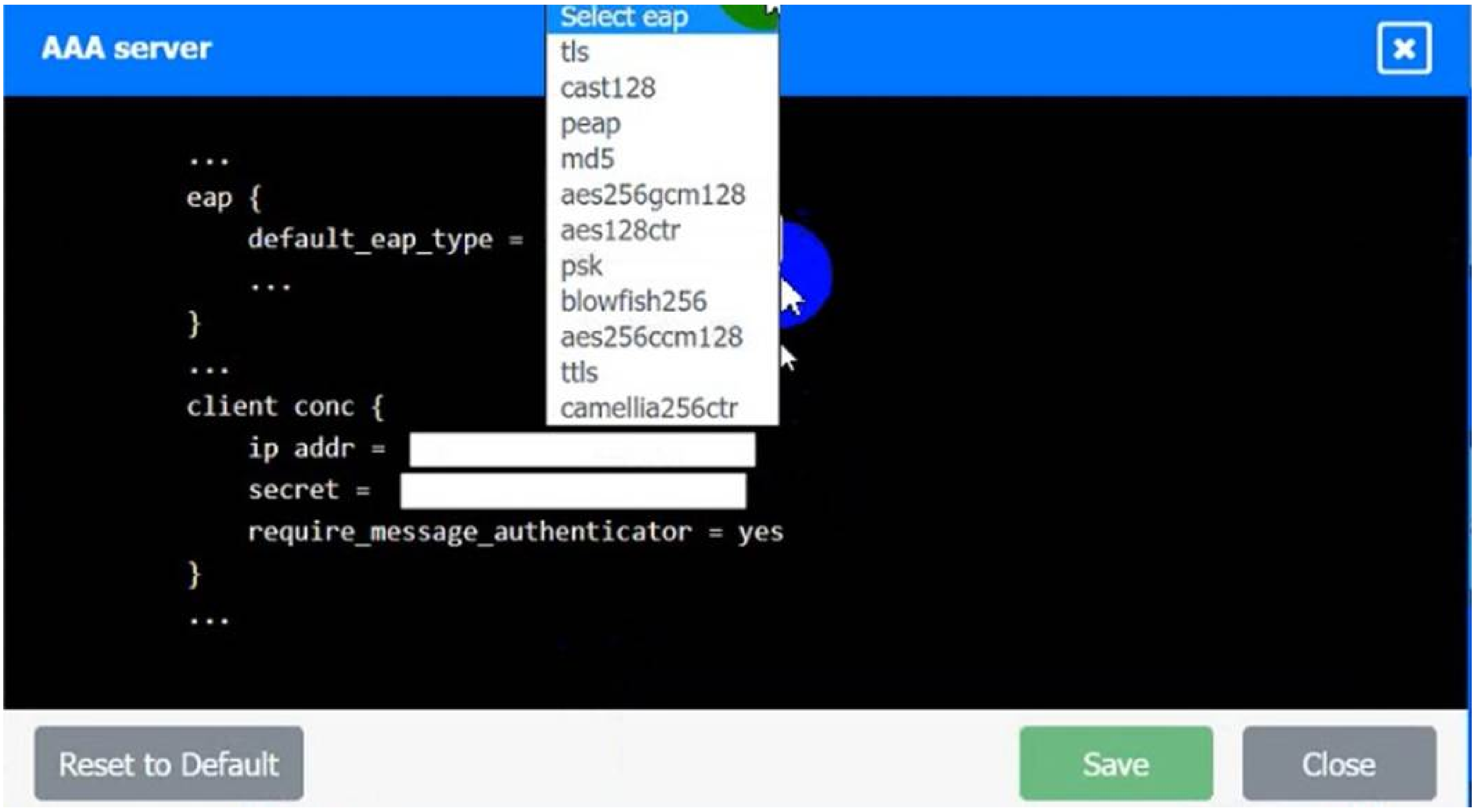


VPN Concentrator:



```
...
re-eap {
...
    proposals =
    ...
}
...
plugins {
    eap-radius {
        secret =
        server =
    }
}
...
```

AAA Server:

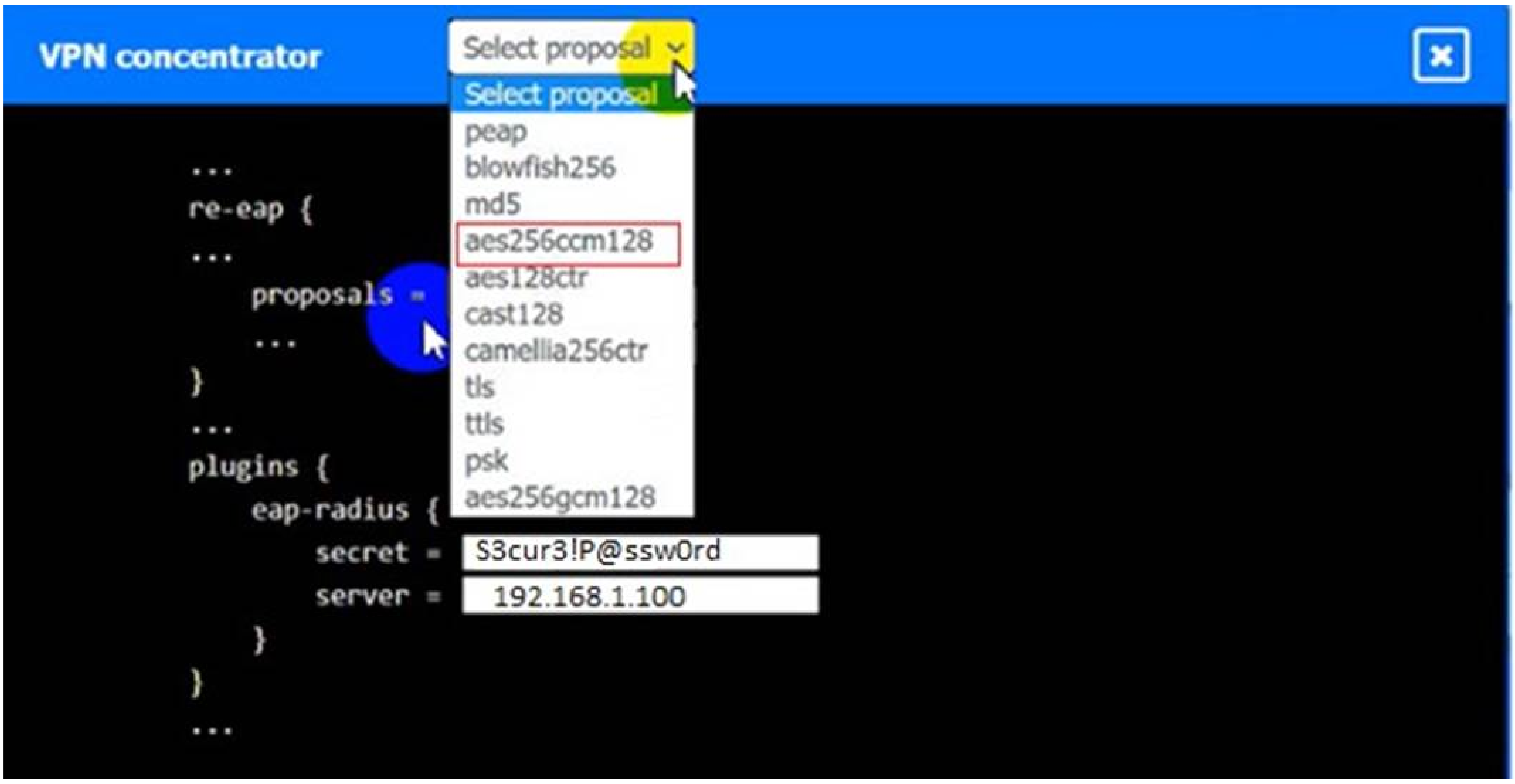


```
...
eap {
    default_eap_type =
    ...
}
...
client conc {
    ip addr =
    secret =
    require_message_authenticator = yes
}
...
```

A. Mastered
B. Not Mastered

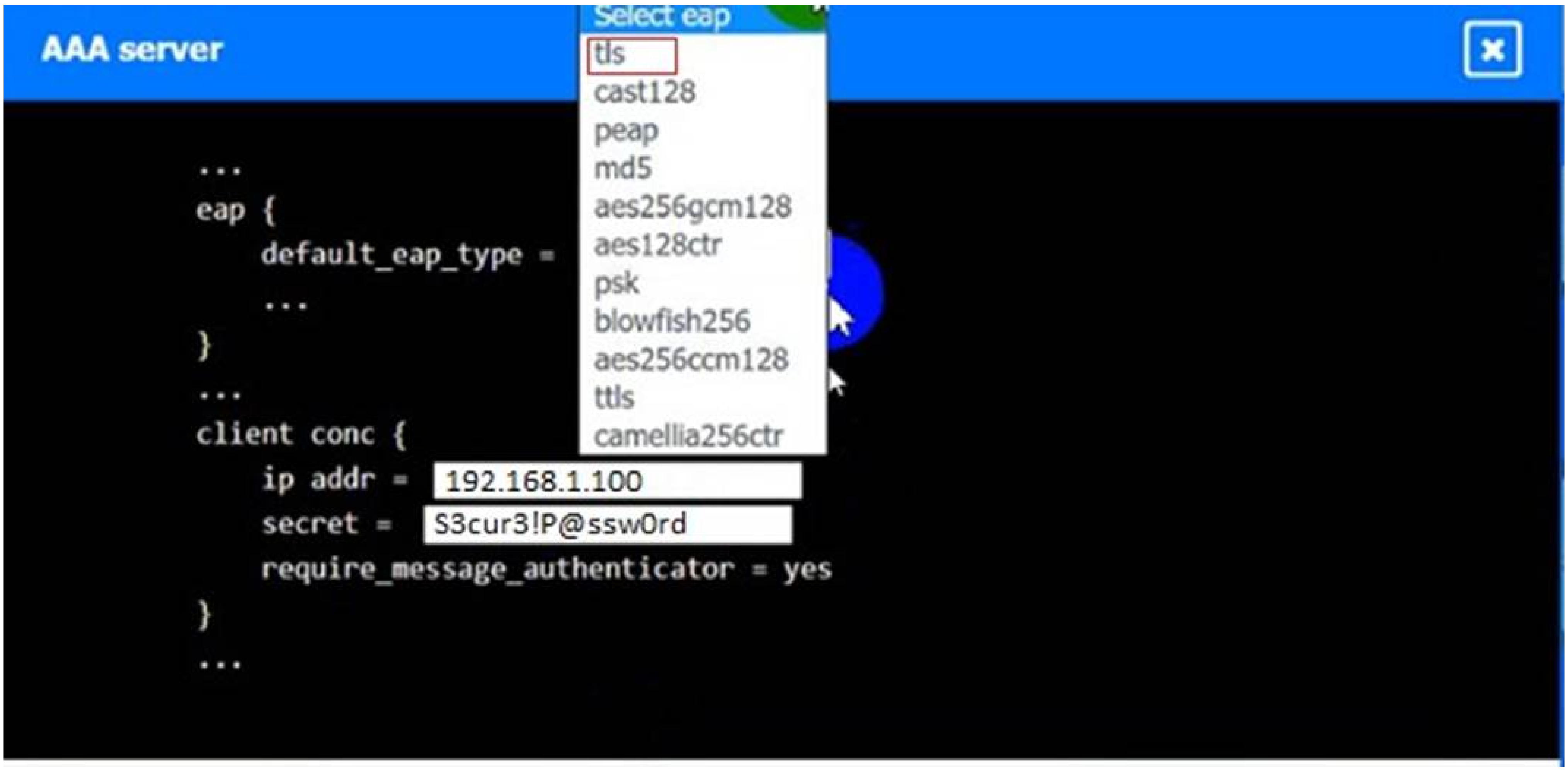
Answer: A

Explanation:
VPN Concentrator:



```
...
re-eap {
...
    proposals =
    ...
}
...
plugins {
    eap-radius {
        secret = S3cur3!P@ssw0rd
        server = 192.168.1.100
    }
}
...
```

AAA Server:



```
...
eap {
    default_eap_type =
    ...
}
...
client conc {
    ip addr = 192.168.1.100
    secret = S3cur3!P@ssw0rd
    require_message_authenticator = yes
}
...
```

NEW QUESTION 46

Third parties notified a company's security team about vulnerabilities in the company's application. The security team determined these vulnerabilities were previously disclosed in third-party libraries. Which of the following solutions best addresses the reported vulnerabilities?

A. Using laC to include the newest dependencies
B. Creating a bug bounty program
C. Implementing a continuous security assessment program
D. Integrating a SASI tool as part of the pipeline

Answer: D

Explanation:

The best solution to address reported vulnerabilities in third-party libraries is integrating a Static Application Security Testing (SAST) tool as part of the development pipeline. Here??s why:

? Early Detection: SAST tools analyze source code for vulnerabilities before the
code is compiled. This allows developers to identify and fix security issues early in the development process.

? Continuous Security: By integrating SAST tools into the CI/CD pipeline, the organization ensures continuous security assessment of the codebase, including third-party libraries, with each code commit and build.

? Comprehensive Analysis: SAST tools provide a detailed analysis of the code, identifying potential vulnerabilities in both proprietary code and third-party dependencies, ensuring that known issues in libraries are addressed promptly.

? References:

NEW QUESTION 51

Company A acquired Company B and needs to determine how the acquisition will impact the attack surface of the organization as a whole. Which of the following is the best way to achieve this goal? (Select two).
Implementing DLP controls preventing sensitive data from leaving Company B's network

A. Documenting third-party connections used by Company B
B. Reviewing the privacy policies currently adopted by Company B
C. Requiring data sensitivity labeling tor all files shared with Company B
D. Forcing a password reset requiring more stringent passwords for users on Company B's network
E. Performing an architectural review of Company B's network

Answer: AB

Explanation:

To determine how the acquisition of Company B will impact the attack surface, the following steps are crucial:
* A. Documenting third-party connections used by Company B: Understanding all external connections is essential for assessing potential entry points for attackers and ensuring that these connections are secure.
* E. Performing an architectural review of Company B's network: This review will identify
vulnerabilities and assess the security posture of the acquired company's network, providing a comprehensive understanding of the new attack surface.
These actions will provide a clear picture of the security implications of the acquisition and help in developing a plan to mitigate any identified risks.
References:
? CompTIA SecurityX Study Guide: Emphasizes the importance of understanding third-party connections and conducting architectural reviews during acquisitions.
? NIST Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems": Recommends comprehensive reviews and documentation of third-party connections.
? "Mergers, Acquisitions, and Other Restructuring Activities" by Donald DePamphilis: Discusses the importance of security assessments during acquisitions.

NEW QUESTION 56

A systems administrator works with engineers to process and address vulnerabilities as a result of continuous scanning activities. The primary challenge faced by the administrator is differentiating between valid and invalid findings. Which of the following would the systems administrator most likely verify is properly configured?

A. Report retention time
B. Scanning credentials
C. Exploit definitions
D. Testing cadence

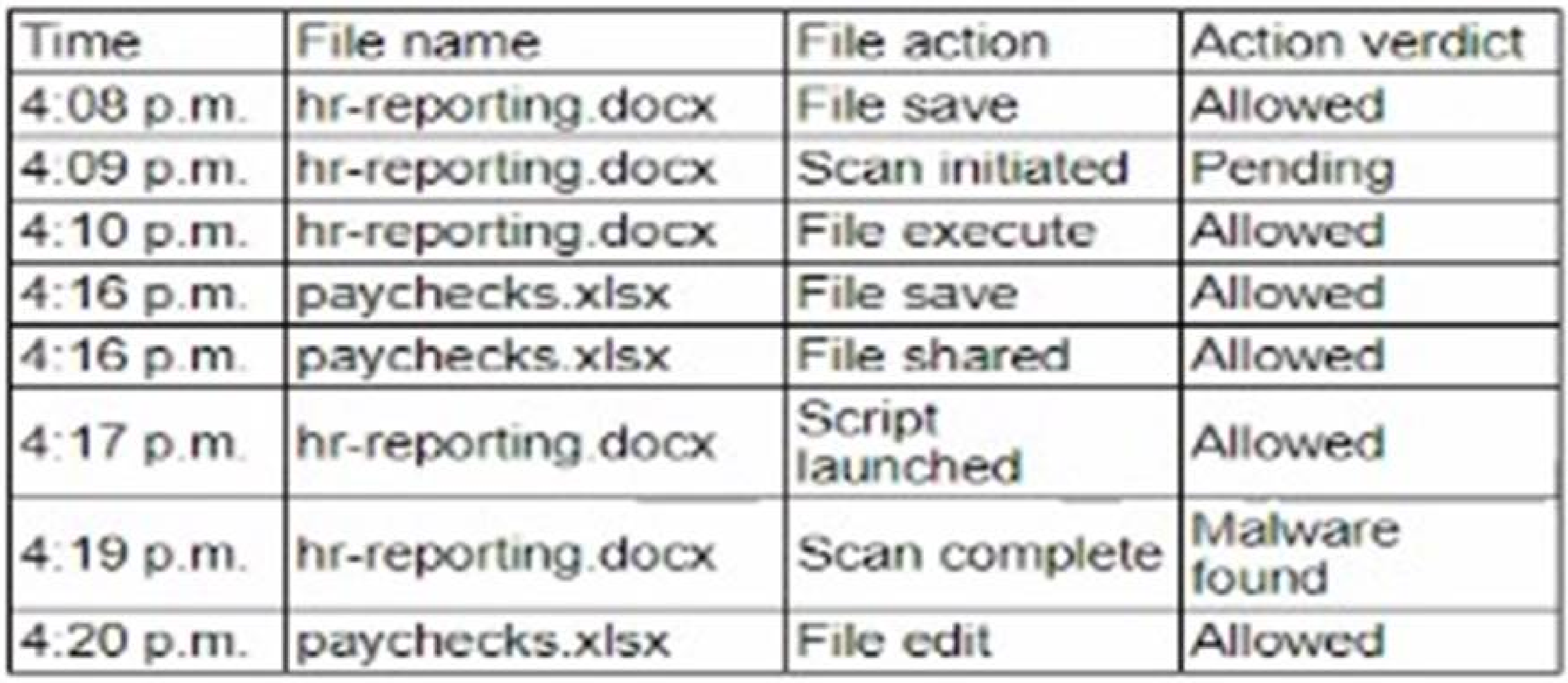
Answer: B

Explanation:

When differentiating between valid and invalid findings from vulnerability scans, the systems administrator should verify that the scanning credentials are properly configured. Valid credentials ensure that the scanner can authenticate and access the systems being evaluated, providing accurate and comprehensive results. Without proper credentials, scans may miss vulnerabilities or generate false positives, making it difficult to prioritize and address the findings effectively.
References:
? CompTIA SecurityX Study Guide: Highlights the importance of using valid credentials for accurate vulnerability scanning.
? "Vulnerability Management" by Park Foreman: Discusses the role of scanning credentials in obtaining accurate scan results and minimizing false positives.
? "The Art of Network Security Monitoring" by Richard Bejtlich: Covers best practices for configuring and using vulnerability scanning tools, including the need for valid credentials.

NEW QUESTION 60

A security analyst is reviewing the following event timeline from an COR solution:



Time	File name	File action	Action verdict
4:08 p.m.	hr-reporting.docx	File save	Allowed
4:09 p.m.	hr-reporting.docx	Scan initiated	Pending
4:10 p.m.	hr-reporting.docx	File execute	Allowed
4:16 p.m.	paychecks.xlsx	File save	Allowed
4:16 p.m.	paychecks.xlsx	File shared	Allowed
4:17 p.m.	hr-reporting.docx	Script launched	Allowed
4:19 p.m.	hr-reporting.docx	Scan complete	Malware found
4:20 p.m.	paychecks.xlsx	File edit	Allowed

Which of the following most likely has occurred and needs to be fixed?

A. The Dl P has failed to block malicious exfiltration and data tagging is not being utilized property
B. An EDR bypass was utilized by a threat actor and updates must be installed by the administrator.

C. A logic law has introduced a TOCTOU vulnerability and must be addressed by the COR vendor
D. A potential insider threat is being investigated and will be addressed by the senior management team.

Answer: C

Explanation:
The event timeline indicates a sequence where a file (hr-reporting.docx) was saved, scanned, executed, and eventually found to contain malware. The critical issue here is that the malware scan completed after the file was already executed. This suggests a Time-Of- Check to Time-Of-Use (TOCTOU) vulnerability, where the state of the file changed between the time it was checked and the time it was used.
References:
? CompTIA SecurityX Study Guide: Discusses TOCTOU vulnerabilities as a timing attack where the state of a resource changes after it has been validated.
? NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations": Recommends addressing TOCTOU vulnerabilities to ensure the integrity of security operations.
? "The Art of Software Security Assessment" by Mark Dowd, John McDonald, and Justin Schuh: Covers logic flaws and timing vulnerabilities, including TOCTOU issues.

NEW QUESTION 62
An organization is implementing Zero Trust architecture A systems administrator must increase the effectiveness of the organization's context-aware access system. Which of the following is the best way to improve the effectiveness of the system?

A. Secure zone architecture
B. Always-on VPN
C. Accurate asset inventory
D. Microsegmentation

Answer: D

Explanation:
Microsegmentation is a critical strategy within Zero Trust architecture that enhances context-aware access systems by dividing the network into smaller, isolated segments. This reduces the attack surface and limits lateral movement of attackers within the network. It ensures that even if one segment is compromised, the attacker cannot easily access other segments. This granular approach to network security is essential for enforcing strict access controls and monitoring within Zero Trust environments.
Reference: CompTIA SecurityX Study Guide, Chapter on Zero Trust Security, Section on
Microsegmentation and Network Segmentation.

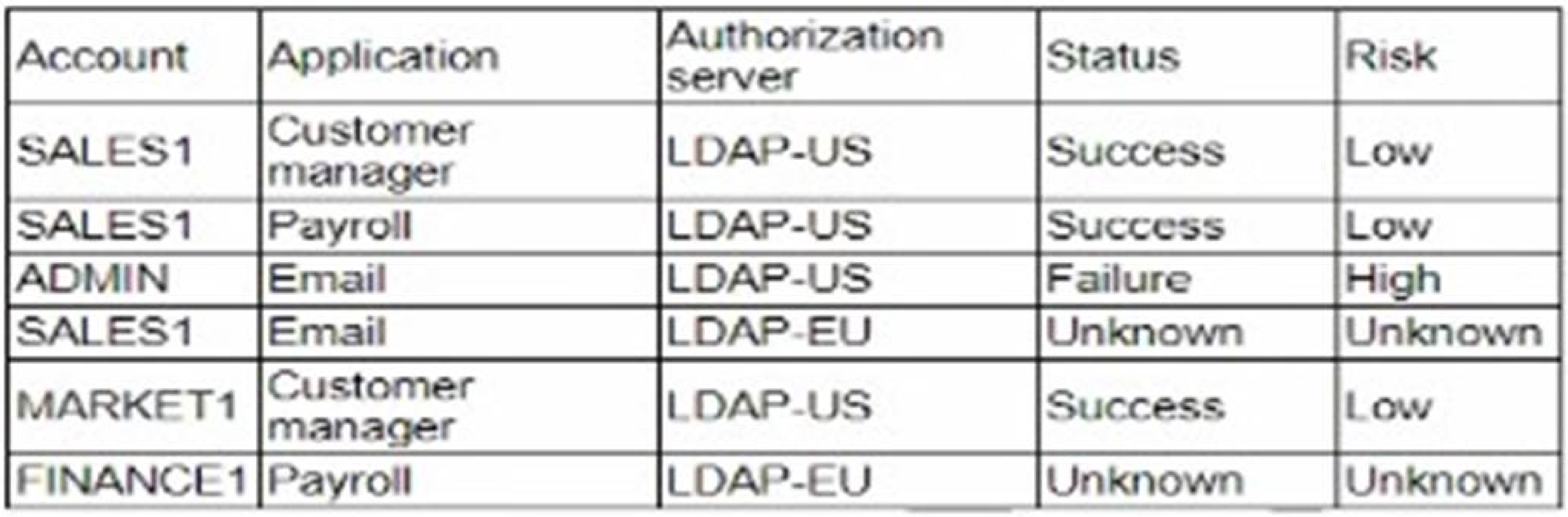
NEW QUESTION 63
An incident response team is analyzing malware and observes the following:
• Does not execute in a sandbox
• No network loCs
• No publicly known hash match
• No process injection method detected
Which of the following should the team do next to proceed with further analysis?

A. Use an online vims analysis tool to analyze the sample
B. Check for an anti-virtualization code in the sample
C. Utilize a new deployed machine to run the sample.
D. Search oilier internal sources for a new sample.

Answer: B

Explanation:
Malware that does not execute in a sandbox environment often contains anti-analysis
techniques, such as anti-virtualization code. This code detects when the malware is running in a virtualized environment and alters its behavior to avoid detection. Checking for anti-virtualization code is a logical next step because:
? It helps determine if the malware is designed to evade analysis tools.
? Identifying such code can provide insights into the malware's behavior and intent.
? This step can also inform further analysis methods, such as running the malware on physical hardware.
References:
? CompTIA Security+ Study Guide
? SANS Institute, "Malware Analysis Techniques"
? "Practical Malware Analysis" by Michael Sikorski and Andrew Honig

NEW QUESTION 65
A security analyst is reviewing suspicious log-in activity and sees the following data in the SICM:



Account	Application	Authorization server	Status	Risk
SALES1	Customer manager	LDAP-US	Success	Low
SALES1	Payroll	LDAP-US	Success	Low
ADMIN	Email	LDAP-US	Failure	High
SALES1	Email	LDAP-EU	Unknown	Unknown
MARKET1	Customer manager	LDAP-US	Success	Low
FINANCE1	Payroll	LDAP-EU	Unknown	Unknown

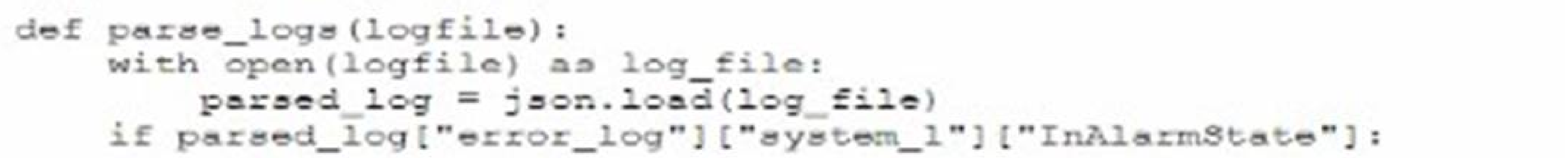
Which of the following is the most appropriate action for the analyst to take?

A. Update the log configuration settings on the directory server that Is not being captured properly.
B. Have the admin account owner change their password to avoid credential stuffing.
C. Block employees from logging in to applications that are not part of their business area.
D. implement automation to disable accounts that nave been associated with high-risk activity.

Answer: D

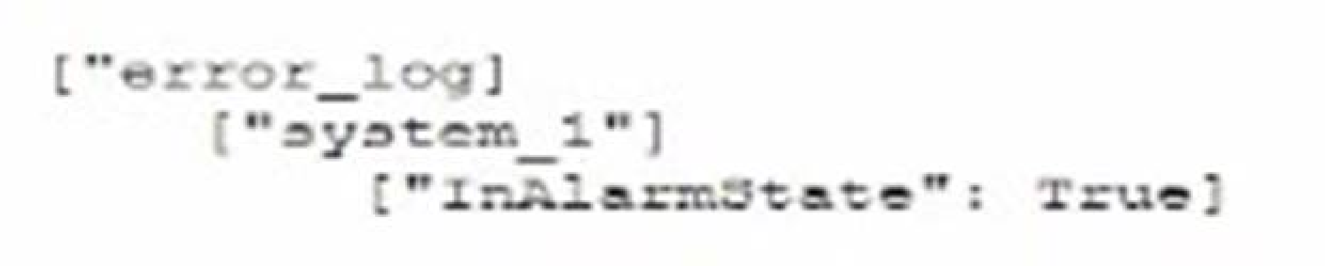
Explanation:
The log-in activity indicates a security threat, particularly involving the ADMIN account with a high-risk failure status. This suggests that the account may be targeted by malicious activities such as credential stuffing or brute force attacks.
? Updating log configuration settings (A) may help in better logging future activities
but does not address the immediate threat.
? Changing the admin account password (B) is a good practice but may not fully mitigate the ongoing threat if the account has already been compromised.
? Blocking employees (C) from logging into non-business applications might help in
reducing attack surfaces but doesn't directly address the compromised account issue.
Implementing automation to disable accounts associated with high-risk activities ensures an immediate response to the detected threat, preventing further unauthorized access and allowing time for thorough investigation and remediation.
References:
? CompTIA SecurityX guide on incident response and account management.
? Best practices for handling compromised accounts.
? Automation tools and techniques for security operations centers (SOCs).

NEW QUESTION 70
A security administrator needs to automate alerting. The server generates structured log files that need to be parsed to determine whether an alarm has been triggered Given the following code function:



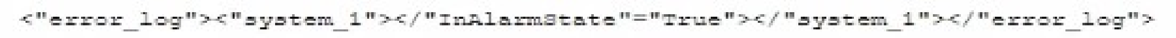
```
def parse_logs(logfile):
    with open(logfile) as log_file:
        parsed_log = json.load(log_file)
    if parsed_log["error_log"]["system_1"]["InAlarmState"]:
```

Which of the following is most likely the log input that the code will parse?
A)



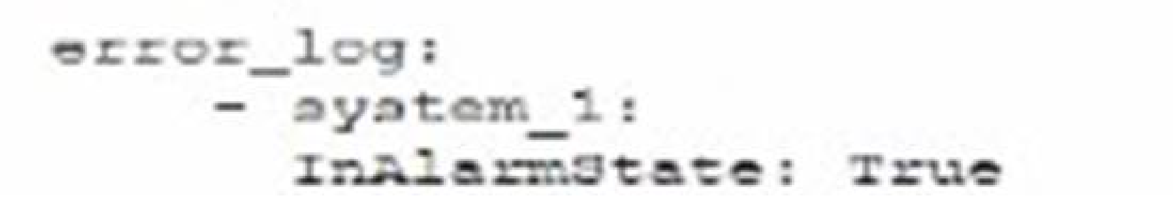
```
["error_log]
    ["system_1"]
        ["InAlarmState": True]
```

B)



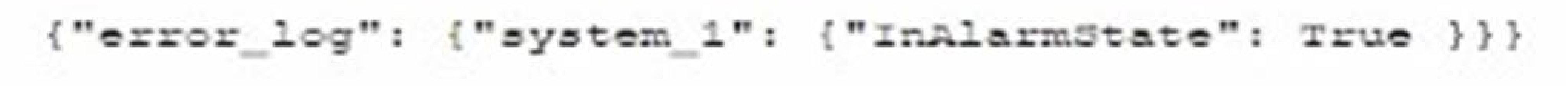
```
<"error_log"><"system_1"></"InAlarmState"="True"></"system_1"></"error_log">
```

C)



```
error_log:
    - system_1:
      InAlarmState: True
```

D)



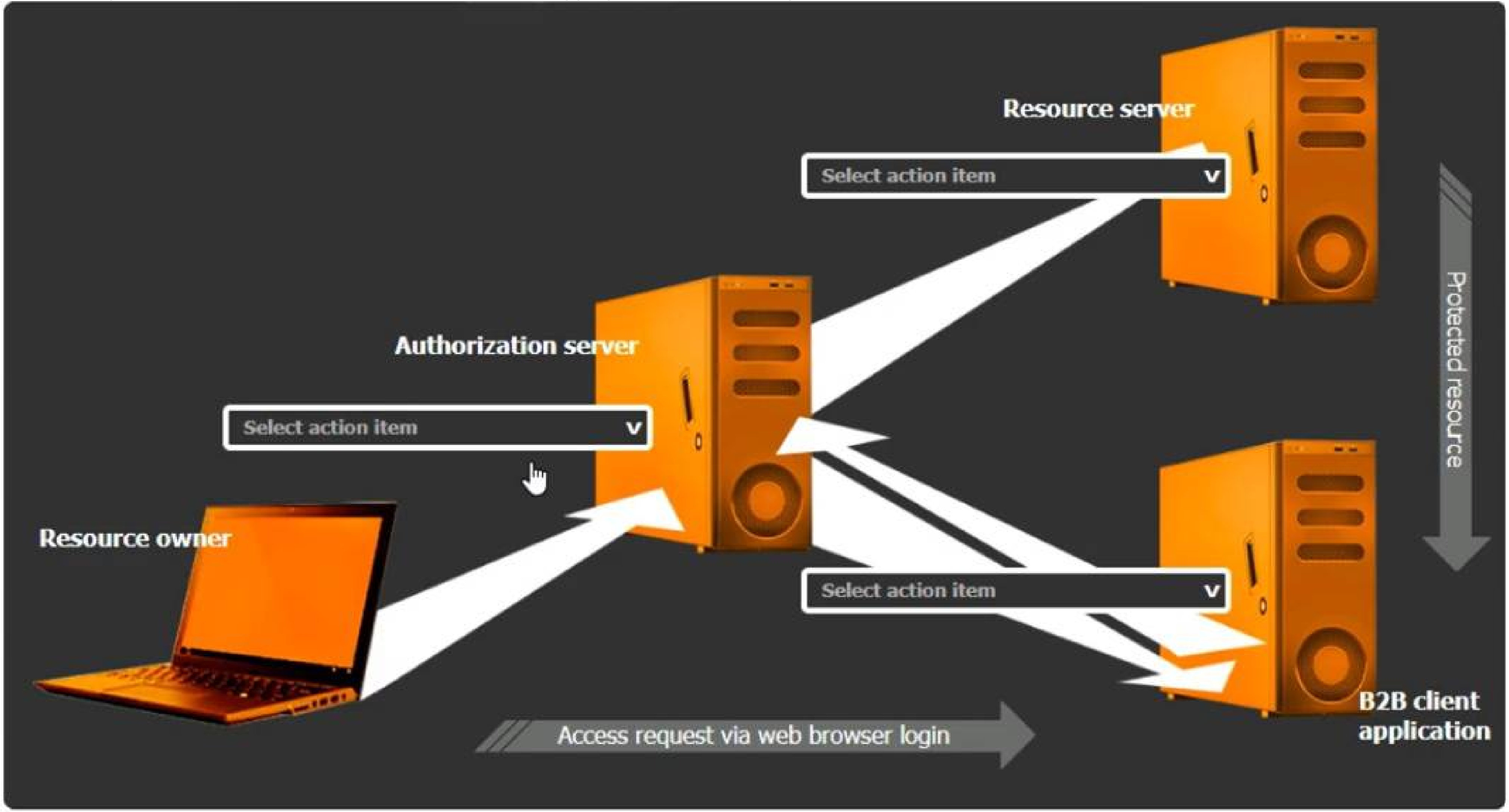
```
{"error_log": {"system_1": {"InAlarmState": True }}}
```

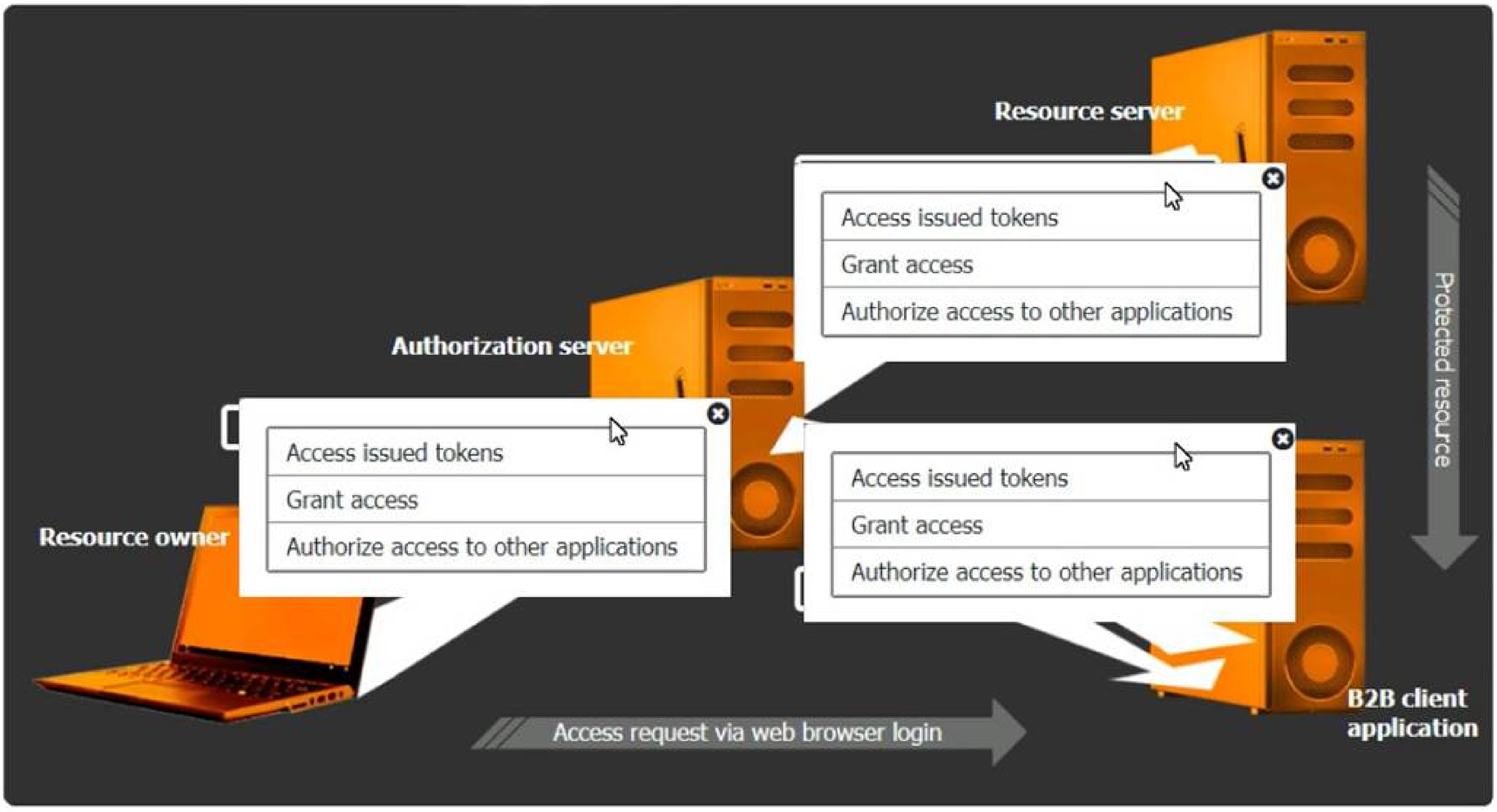
A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

Explanation:
The code function provided in the question seems to be designed to parse JSON formatted logs to check for an alarm state. Option A is a JSON format that matches the structure likely expected by the code. The presence of the "error_log" and "InAlarmState" keys suggests that this is the correct input format.
Reference: CompTIA SecurityX Study Guide, Chapter on Log Management and Automation, Section on Parsing Structured Logs.

NEW QUESTION 73
SIMULATION
You are tasked with integrating a new B2B client application with an existing OAuth workflow that must meet the following requirements:
. The application does not need to know the users' credentials.
. An approval interaction between the users and the HTTP service must be orchestrated.
. The application must have limited access to users' data. INSTRUCTIONS
Use the drop-down menus to select the action items for the appropriate locations. All placeholders must be filled.





A. Mastered
B. Not Mastered

Answer: A

Explanation:
Select the Action Items for the Appropriate Locations:
? Authorization Server:
? Resource Server:
? B2B Client Application:
Detailed Explanation
OAuth 2.0 is designed to provide specific authorization flows for web applications, desktop applications, mobile phones, and living room devices. The integration involves multiple steps and components, including:
? Resource Owner (User):
? Client Application (B2B Client Application):
? Authorization Server:
? Resource Server:
OAuth Workflow:
? The resource owner accesses the client application.
? The client application redirects the resource owner to the authorization server for authentication.
? The authorization server authenticates the resource owner and asks for consent to grant access to the client application.
? Upon consent, the authorization server issues an authorization code or token to the client application.
? The client application uses the authorization code or token to request access to the resources from the resource server.
? The resource server verifies the token with the authorization server and, if valid, grants access to the requested resources.
References:
? CompTIA Security+ Study Guide: Provides comprehensive information on various authentication and authorization protocols, including OAuth.
? OAuth 2.0 Authorization Framework (RFC 6749): The official documentation detailing the OAuth 2.0 framework, its flows, and components.
? OAuth 2.0 Simplified: A book by Aaron Parecki that provides a detailed yet easy- to-understand explanation of the OAuth 2.0 protocol.
By ensuring that each component in the OAuth workflow performs its designated role, the B2B client application can securely access the necessary resources without compromising user credentials, adhering to the principle of least privilege.

NEW QUESTION 78
A cloud engineer needs to identify appropriate solutions to:
• Provide secure access to internal and external cloud resources.
• Eliminate split-tunnel traffic flows.
• Enable identity and access management capabilities.
Which of the following solutions arc the most appropriate? (Select two).

A. Federation
B. Microsegmentation
C. CASB
D. PAM
E. SD-WAN
F. SASE

Answer: CF

Explanation:
To provide secure access to internal and external cloud resources, eliminate split-tunnel traffic flows, and enable identity and access management capabilities, the most appropriate solutions are CASB (Cloud Access Security Broker) and SASE (Secure Access Service Edge).
Why CASB and SASE?
? CASB (Cloud Access Security Broker):
? SASE (Secure Access Service Edge):
Other options, while useful, do not comprehensively address all the requirements:
? A. Federation: Useful for identity management but does not eliminate split-tunnel traffic or provide comprehensive security.
? B. Microsegmentation: Enhances security within the network but does not directly address secure access to cloud resources or split-tunnel traffic.
? D. PAM (Privileged Access Management): Focuses on managing privileged accounts and does not provide comprehensive access control for internal and external resources.
? E. SD-WAN: Enhances WAN performance but does not inherently provide the identity and access management capabilities or eliminate split-tunnel traffic.
References:
? CompTIA SecurityX Study Guide
? "CASB: Cloud Access Security Broker," Gartner Research

NEW QUESTION 82
After remote desktop capabilities were deployed in the environment, various vulnerabilities were noticed.
• Exfiltration of intellectual property
• Unencrypted files
• Weak user passwords
Which of the following is the best way to mitigate these vulnerabilities? (Select two).

A. Implementing data loss prevention
B. Deploying file integrity monitoring
C. Restricting access to critical file services only
D. Deploying directory-based group policies
E. Enabling modem authentication that supports MFA
F. Implementing a version control system
G. Implementing a CMDB platform

Answer: AE

Explanation:
To mitigate the identified vulnerabilities, the following solutions are most appropriate:
? A. Implementing data loss prevention (DLP): DLP solutions help prevent the
unauthorized transfer of data outside the organization. This directly addresses the exfiltration of intellectual property by monitoring, detecting, and blocking sensitive data transfers.
? E. Enabling modern authentication that supports Multi-Factor Authentication
(MFA): This significantly enhances security by requiring additional verification methods beyond just passwords. It addresses the issue of weak user passwords by making it much harder for unauthorized users to gain access, even if they obtain the password.
Other options, while useful in specific contexts, do not address all the vulnerabilities mentioned:
? B. Deploying file integrity monitoring helps detect changes to files but does not
prevent data exfiltration or address weak passwords.
? C. Restricting access to critical file services improves security but is not comprehensive enough to mitigate all identified vulnerabilities.
? D. Deploying directory-based group policies can enforce security policies but might not directly prevent data exfiltration or ensure strong authentication.
? F. Implementing a version control system helps manage changes to files but is not a security measure for preventing the identified vulnerabilities.
? G. Implementing a CMDB platform (Configuration Management Database) helps manage IT assets but does not address the specific security issues mentioned.
References:
? CompTIA Security+ Study Guide
? NIST SP 800-53 Rev. 5, "Security and Privacy Controls for Information Systems and Organizations"
? CIS Controls, "Control 13: Data Protection" and "Control 16: Account Monitoring and Control"

NEW QUESTION 86
A software development team requires valid data for internal tests. Company regulations, however do not allow the use of this data in cleartext. Which of the following solutions best meet these requirements?

A. Configuring data hashing
B. Deploying tokenization
C. Replacing data with null record
D. Implementing data obfuscation

Answer: B

Explanation:
Tokenization replaces sensitive data elements with non-sensitive equivalents, called tokens, that can be used within the internal tests. The original data is stored securely and can be retrieved if necessary. This approach allows the software development team to work with data that appears realistic and valid without exposing the actual sensitive information.
Configuring data hashing (Option A) is not suitable for test data as it transforms the data into a fixed-length value that is not usable in the same way as the original data. Replacing
data with null records (Option C) is not useful as it does not provide valid data for testing. Data obfuscation (Option D) could be an alternative but might not meet the regulatory requirements as effectively as tokenization.
References:
? CompTIA Security+ Study Guide
? NIST SP 800-57 Part 1 Rev. 5, "Recommendation for Key Management"
? PCI DSS Tokenization Guidelines

NEW QUESTION 90
A cybersecurity architect is reviewing the detection and monitoring capabilities for a global company that recently made multiple acquisitions. The architect discovers that the acquired companies use different vendors for detection and monitoring The architect's goal is to:

- Create a collection of use cases to help detect known threats
- Include those use cases in a centralized library for use across all of the companies Which of the following is the best way to achieve this goal?

A. Sigma rules
B. Ariel Query Language
C. UBA rules and use cases
D. TAXII/STIX library

Answer: A

Explanation:
To create a collection of use cases for detecting known threats and include them in a centralized library for use across multiple companies with different vendors, Sigma rules are the best option. Here??s why:
? Vendor-Agnostic Format: Sigma rules are a generic and open standard for writing
SIEM (Security Information and Event Management) rules. They can be translated to specific query languages of different SIEM systems, making them highly versatile and applicable across various platforms.
? Centralized Rule Management: By using Sigma rules, the cybersecurity architect
can create a centralized library of detection rules that can be easily shared and implemented across different detection and monitoring systems used by the acquired companies. This ensures consistency in threat detection capabilities.
? Ease of Use and Flexibility: Sigma provides a structured and straightforward
format for defining detection logic. It allows for the easy creation, modification, and sharing of rules, facilitating collaboration and standardization across the organization.

NEW QUESTION 91
The material finding from a recent compliance audit indicate a company has an issue with excessive permissions. The findings show that employees changing roles or departments results in privilege creep. Which of the following solutions are the best ways to mitigate this issue? (Select two).
Setting different access controls defined by business area

A. Implementing a role-based access policy
B. Designing a least-needed privilege policy
C. Establishing a mandatory vacation policy
D. Performing periodic access reviews
E. Requiring periodic job rotation

Answer: AD

Explanation:
To mitigate the issue of excessive permissions and privilege creep, the best solutions are:
? Implementing a Role-Based Access Policy:
? Performing Periodic Access Reviews:

NEW QUESTION 93
Emails that the marketing department is sending to customers are pomp to the customers' spam folders. The security team is investigating the issue and discovers that the certificates used by the email server were reissued, but DNS records had not been updated. Which of the following should the security team update in order to fix this issue? (Select three.)

A. DMARC
B. SPF
C. DKIM
D. DNSSEC
E. SASC
F. SAN
G. SOA
H. MX

Answer: ABC

Explanation:
To prevent emails from being marked as spam, several DNS records related to email authentication need to be properly configured and updated when there are changes to the email server's certificates:
? A. DMARC (Domain-based Message Authentication, Reporting & Conformance):
DMARC records help email servers determine how to handle messages that fail SPF or DKIM checks, improving email deliverability and reducing the likelihood of emails being marked as spam.
? B. SPF (Sender Policy Framework): SPF records specify which mail servers are authorized to send email on behalf of your domain. Updating the SPF record ensures that the new email server is recognized as an authorized sender.
? C. DKIM (DomainKeys Identified Mail): DKIM adds a digital signature to email
headers, allowing the receiving server to verify that the email has not been tampered with and is from an authorized sender. Updating DKIM records ensures that emails are properly signed and authenticated.
? D. DNSSEC (Domain Name System Security Extensions): DNSSEC adds security
to DNS by enabling DNS responses to be verified. While important for DNS security, it does not directly address the issue of emails being marked as spam.
? E. SASC: This is not a relevant standard for this scenario.
? F. SAN (Subject Alternative Name): SAN is used in SSL/TLS certificates for securing multiple domain names, not for email delivery issues.
? G. SOA (Start of Authority): SOA records are used for DNS zone administration and do not directly impact email deliverability.
? H. MX (Mail Exchange): MX records specify the mail servers responsible for receiving email on behalf of a domain. While important, the primary issue here is the authentication of outgoing emails, which is handled by SPF, DKIM, and DMARC.
References:
? CompTIA Security+ Study Guide
? RFC 7208 (SPF), RFC 6376 (DKIM), and RFC 7489 (DMARC)
? NIST SP 800-45, "Guidelines on Electronic Mail Security"

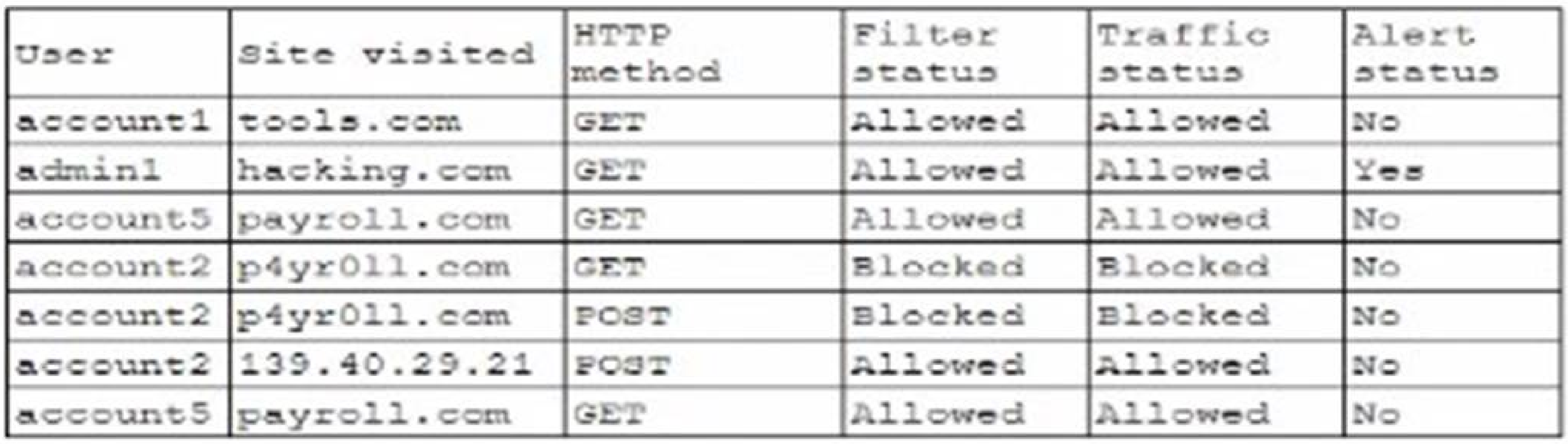
NEW QUESTION 94
All organization is concerned about insider threats from employees who have individual access to encrypted material. Which of the following techniques best addresses this issue?

A. SSO with MFA
B. Sating and hashing
C. Account federation with hardware tokens
D. SAE
E. Key splitting

Answer: E

Explanation:
The technique that best addresses the issue of insider threats from employees who have individual access to encrypted material is key splitting. Here??s why:
? Key Splitting: Key splitting involves dividing a cryptographic key into multiple parts and distributing these parts among different individuals or systems. This ensures that no single individual has complete access to the key, thereby mitigating the risk of insider threats.
? Increased Security: By requiring multiple parties to combine their key parts to access encrypted material, key splitting provides an additional layer of security. This approach is particularly useful in environments where sensitive data needs to be protected from unauthorized access by insiders.
? Compliance and Best Practices: Key splitting aligns with best practices and regulatory requirements for handling sensitive information, ensuring that access is tightly controlled and monitored.
? References:
By employing key splitting, organizations can effectively reduce the risk of insider threats and enhance the overall security of encrypted material.

NEW QUESTION 97
A security analyst wants to use lessons learned from a poor incident response to reduce dwell lime in the future The analyst is using the following data points



User	Site visited	HTTP method	Filter status	Traffic status	Alert status
account1	tools.com	GET	Allowed	Allowed	No
admin1	hacking.com	GET	Allowed	Allowed	Yes
account5	payroll.com	GET	Allowed	Allowed	No
account2	p4yr011.com	GET	Blocked	Blocked	No
account2	p4yr011.com	POST	Blocked	Blocked	No
account2	139.40.29.21	POST	Allowed	Allowed	No
account5	payroll.com	GET	Allowed	Allowed	No

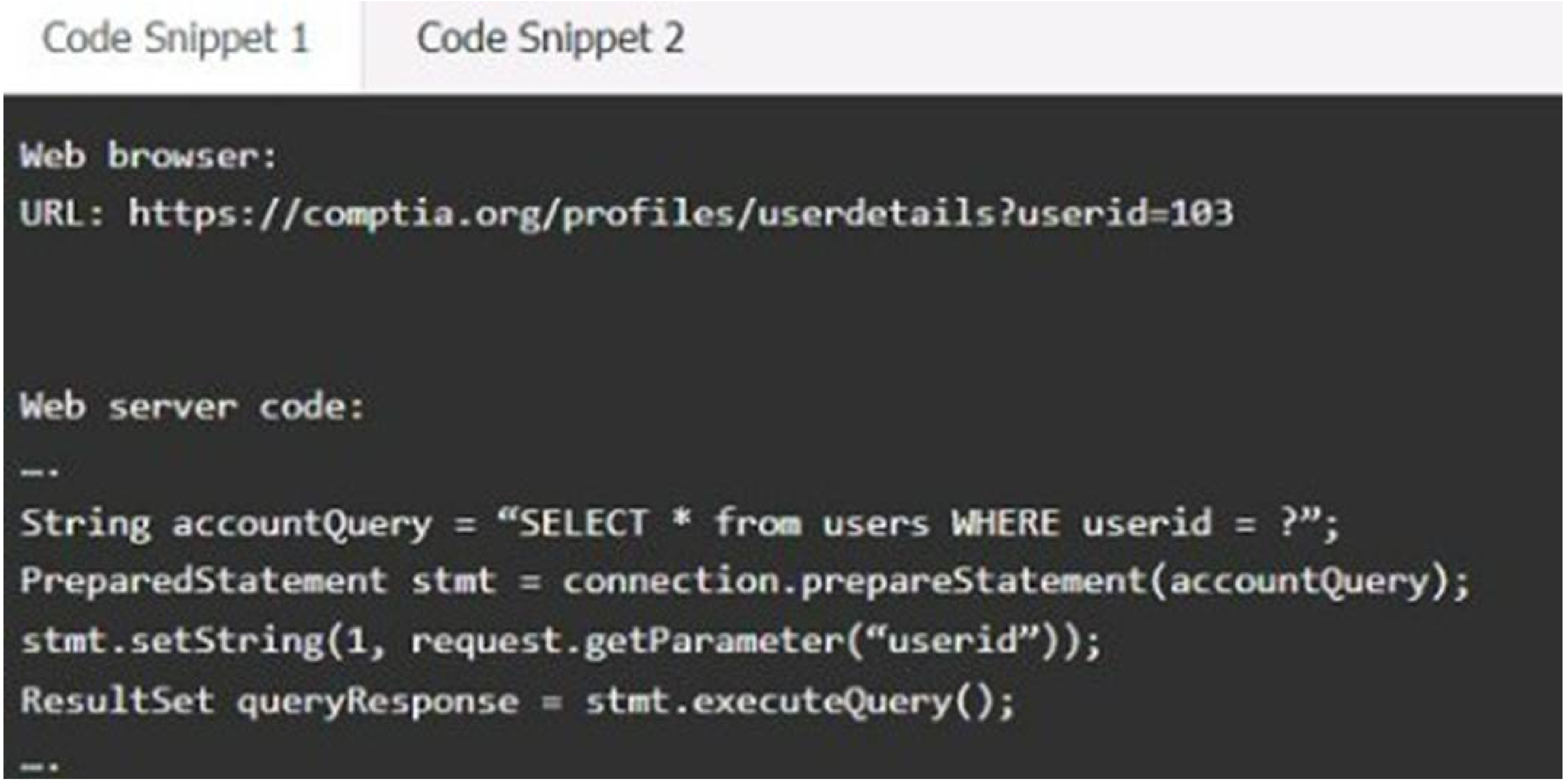
Which of the following would the analyst most likely recommend?

A. Adjusting the SIEM to alert on attempts to visit phishing sites
B. Allowing TRACE method traffic to enable better log correlation
C. Enabling alerting on all suspicious administrator behavior
D. utilizing allow lists on the WAF for all users using GFT methods

Answer: C

Explanation:
In the context of improving incident response and reducing dwell time, the security analyst needs to focus on proactive measures that can quickly detect and alert on potential security breaches. Here??s a detailed analysis of the options provided:
* A. Adjusting the SIEM to alert on attempts to visit phishing sites: While this is a useful measure to prevent phishing attacks, it primarily addresses external threats and doesn??t directly impact dwell time reduction, which focuses on the time a threat remains undetected within a network.
* B. Allowing TRACE method traffic to enable better log correlation: The TRACE method in HTTP is used for debugging purposes, but enabling it can introduce security vulnerabilities. It??s not typically recommended for enhancing security monitoring or incident response.
* C. Enabling alerting on all suspicious administrator behavior: This option directly targets the potential misuse of administrator accounts, which are often high-value targets for attackers. By monitoring and alerting on suspicious activities from admin accounts, the organization can quickly identify and respond to potential breaches, thereby reducing dwell
time significantly. Suspicious behavior could include unusual login times, access to sensitive data not usually accessed by the admin, or any deviation from normal behavior patterns. This proactive monitoring is crucial for quick detection and response, aligning well with best practices in incident response.
* D. Utilizing allow lists on the WAF for all users using GET methods: This measure is aimed at restricting access based on allowed lists, which can be effective in preventing unauthorized access but doesn??t specifically address the need for quick detection and response to internal threats.
References:
? CompTIA SecurityX Study Guide: Emphasizes the importance of monitoring and alerting on admin activities as part of a robust incident response plan.
? NIST Special Publication 800-61 Revision 2, "Computer Security Incident Handling Guide": Highlights best practices for incident response, including the importance of detecting and responding to suspicious activities quickly.
? "Incident Response & Computer Forensics" by Jason T. Luttgens, Matthew Pepe, and Kevin Mandia: Discusses techniques for reducing dwell time through effective monitoring and alerting mechanisms, particularly focusing on privileged account activities.
By focusing on enabling alerting for suspicious administrator behavior, the security analyst addresses a critical area that can help reduce the time a threat goes undetected, thereby improving the overall security posture of the organization.
Top of Form Bottom of Form

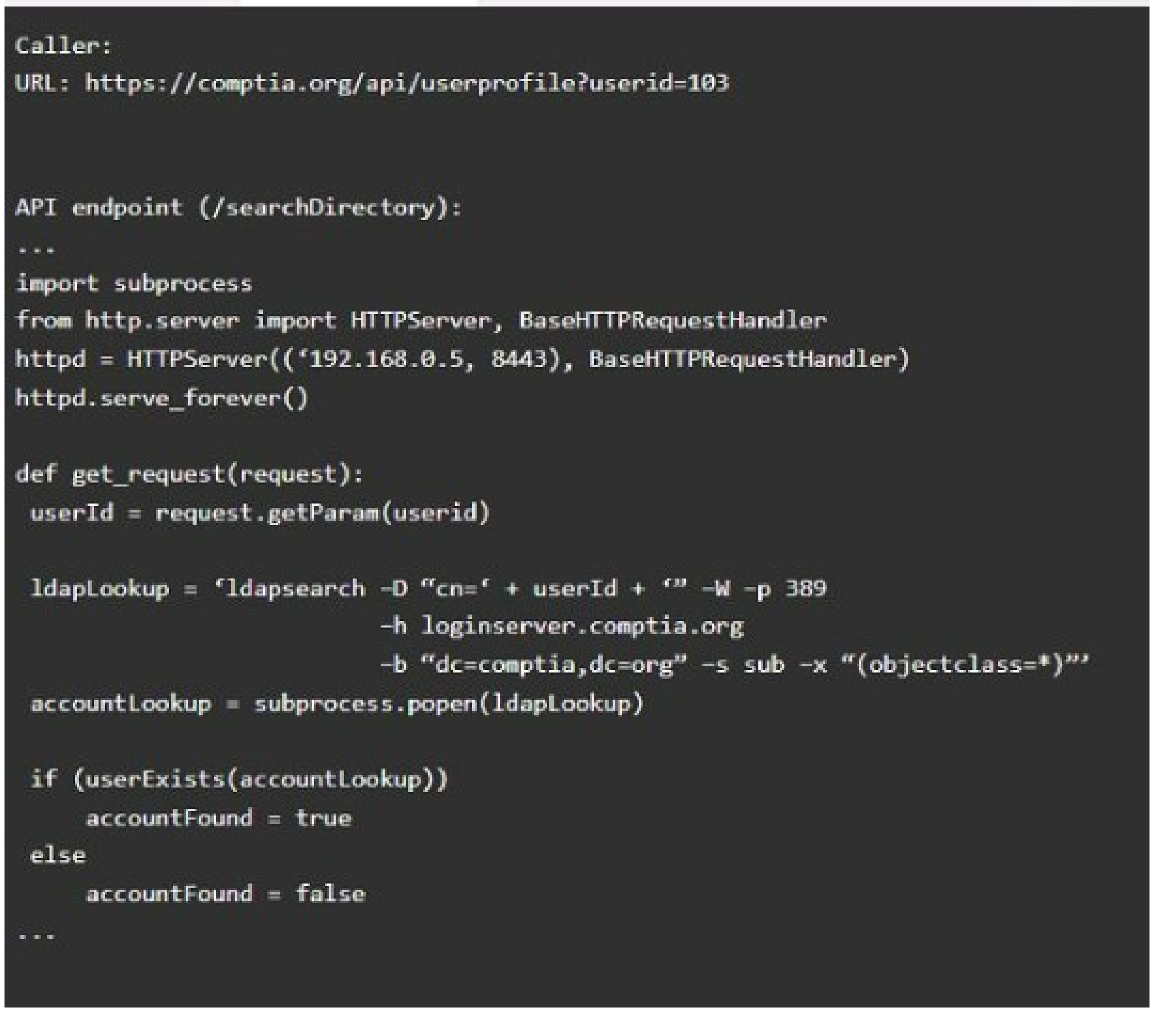
NEW QUESTION 102
SIMULATION
A product development team has submitted code snippets for review prior to release. INSTRUCTIONS
Analyze the code snippets, and then select one vulnerability, and one fix for each code snippet.
Code Snippet 1



```
Web browser:
URL: https://comptia.org/profiles/userdetails?userid=103


Web server code:
...
String accountQuery = "SELECT * from users WHERE userid = ?";
PreparedStatement stmt = connection.prepareStatement(accountQuery);
stmt.setString(1, request.getParameter("userid"));
ResultSet queryResponse = stmt.executeQuery();
...
```

Code Snippet 2



```
Caller:
URL: https://comptia.org/api/userprofile?userid=103


API endpoint (/searchDirectory):
...
import subprocess
from http.server import HTTPServer, BaseHTTPRequestHandler
httpd = HTTPServer(('192.168.0.5, 8443), BaseHTTPRequestHandler)
httpd.serve_forever()

def get_request(request):
 userId = request.getParam(userid)

 ldapLookup = 'ldapsearch -D "cn=' + userId + '" -W -p 389
                           -h loginserver.comptia.org
                           -b "dc=comptia,dc=org" -s sub -x "(objectclass=*)"'
 accountLookup = subprocess.popen(ldapLookup)

 if (userExists(accountLookup))
     accountFound = true
 else
     accountFound = false
...
```

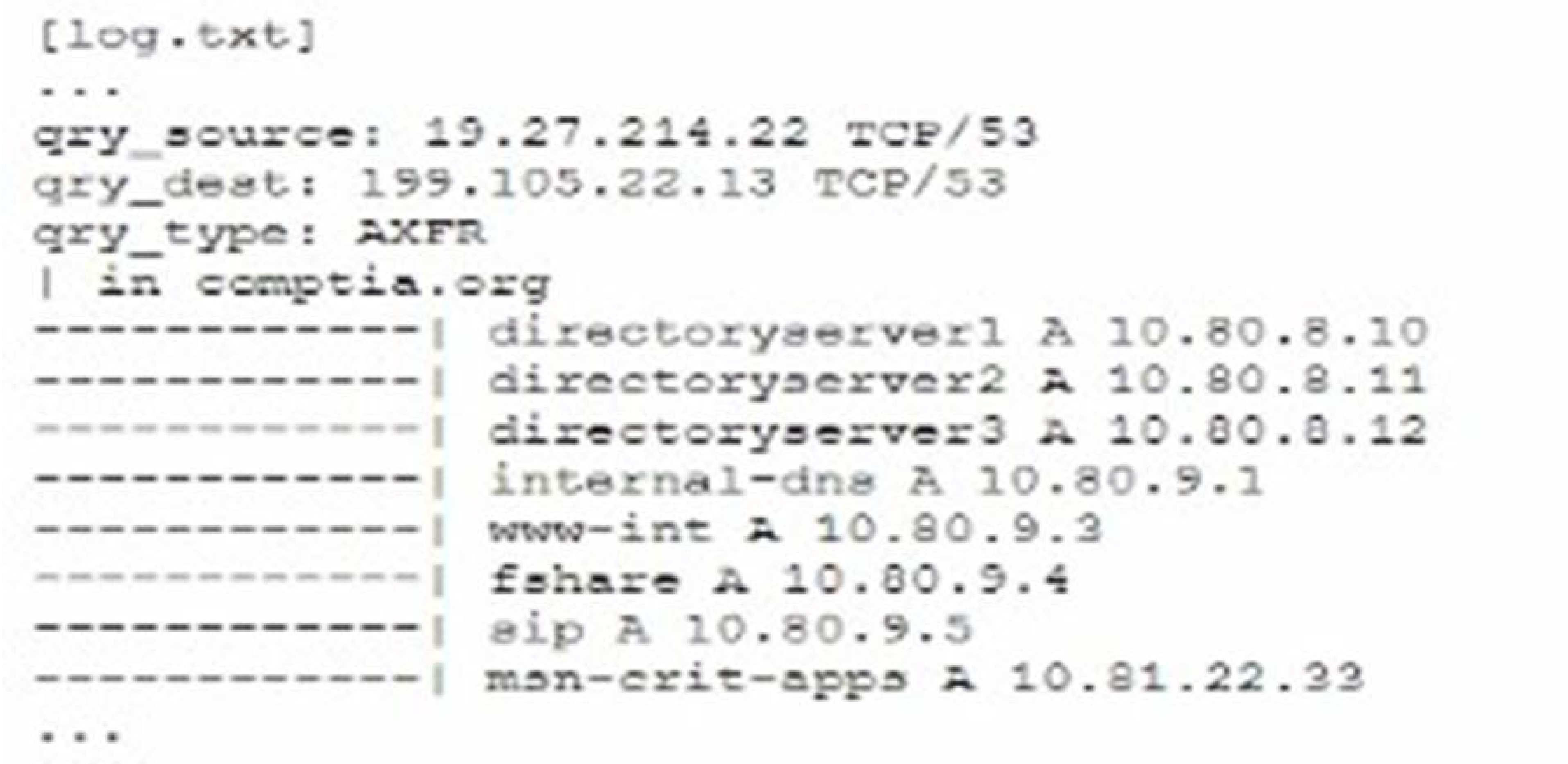
Vulnerability 1:
? SQL injection
? Cross-site request forgery
? Server-side request forgery
? Indirect object reference
? Cross-site scripting
Fix 1:
? Perform input sanitization of the userid field.
? Perform output encoding of queryResponse,
? Ensure usex:ia belongs to logged-in user.
? Inspect URLS and disallow arbitrary requests.
? Implement anti-forgery tokens.
Vulnerability 2
1) Denial of service
2) Command injection
3) SQL injection
4) Authorization bypass
5) Credentials passed via GET
Fix 2
A) Implement prepared statements and bind variables.
B) Remove the serve_forever instruction.
C) Prevent the "authenticated" value from being overridden by a GET parameter.
D) HTTP POST should be used for sensitive parameters.
E) Perform input sanitization of the userid field.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Code Snippet 1
Vulnerability 1: SQL injection
SQL injection is a type of attack that exploits a vulnerability in the code that interacts with a database. An attacker can inject malicious SQL commands into the input fields, such as username or password, and execute them on the database server. This can result in data theft, data corruption, or unauthorized access.
Fix 1: Perform input sanitization of the userid field.
Input sanitization is a technique that prevents SQL injection by validating and filtering the user input values before passing them to the database. The input sanitization should remove any special characters, such as quotes, semicolons, or dashes, that can alter the intended SQL query. Alternatively, the input sanitization can use a whitelist of allowed values and reject any other values.
Code Snippet 2
Vulnerability 2: Cross-site request forgery
Cross-site request forgery (CSRF) is a type of attack that exploits a vulnerability in the code that handles web requests. An attacker can trick a user into sending a malicious web request to a server that performs an action on behalf of the user, such as changing their password, transferring funds, or deleting data. This can result in unauthorized actions, data loss, or account compromise.
Fix 2: Implement anti-forgery tokens.
Anti-forgery tokens are techniques that prevent CSRF by adding a unique and secret value to each web request that is generated by the server and verified by the server before performing the action. The anti-forgery token should be different for each user and each session, and should not be predictable or reusable by an attacker. This way, only legitimate web requests from the user??s browser can be accepted by the server.

NEW QUESTION 105
A senior security engineer flags me following log file snippet as hawing likely facilitated an attacker's lateral movement in a recent breach:



```
[log.txt]
...
qry_source: 19.27.214.22 TCP/53
qry_dest: 199.105.22.13 TCP/53
qry_type: AXFR
| in comptia.org
------------| directoryserver1 A 10.80.8.10
------------| directoryserver2 A 10.80.8.11
------------| directoryserver3 A 10.80.8.12
------------| internal-dns A 10.80.9.1
------------| www-int A 10.80.9.3
------------| fshare A 10.80.9.4
------------| sip A 10.80.9.5
------------| msn-crit-apps A 10.81.22.33
...
```

Which of the following solutions, if implemented, would mitigate the nsk of this issue reoccurnnp?

A. Disabling DNS zone transfers
B. Restricting DNS traffic to UDP'W
C. Implementing DNS masking on internal servers
D. Permitting only clients from internal networks to query DNS

Answer: A

Explanation:
The log snippet indicates a DNS AXFR (zone transfer) request, which can be exploited by attackers to gather detailed information about an internal network's infrastructure. Disabling DNS zone transfers is the best solution to mitigate this risk. Zone transfers should generally be restricted to authorized secondary DNS servers and not be publicly accessible, as they can reveal sensitive network information that facilitates lateral movement during an attack.
References:
? CompTIA SecurityX Study Guide: Discusses the importance of securing DNS configurations, including restricting zone transfers.
? NIST Special Publication 800-81, "Secure Domain Name System (DNS) Deployment Guide": Recommends restricting or disabling DNS zone transfers to prevent information leakage.

NEW QUESTION 108
A network engineer must ensure that always-on VPN access is enabled Curt restricted to company assets Which of the following best describes what the engineer needs to do"

A. Generate device certificates using the specific template settings needed
B. Modify signing certificates in order to support IKE version 2
C. Create a wildcard certificate for connections from public networks
D. Add the VPN hostname as a SAN entry on the root certificate

Answer: A

Explanation:
To ensure always-on VPN access is enabled and restricted to company assets, the network engineer needs to generate device certificates using the specific template settings required for the company's VPN solution. These certificates ensure that only authorized devices can establish a VPN connection.
Why Device Certificates are Necessary:
? Authentication: Device certificates authenticate company assets, ensuring that only authorized devices can access the VPN.
? Security: Certificates provide a higher level of security compared to username and password combinations, reducing the risk of unauthorized access.
? Compliance: Certificates help in meeting security policies and compliance requirements by ensuring that only managed devices can connect to the corporate network.
Other options do not provide the same level of control and security for always-on VPN access:
? B. Modify signing certificates for IKE version 2: While important for VPN protocols,
it does not address device-specific authentication.
? C. Create a wildcard certificate: This is not suitable for device-specific authentication and could introduce security risks.
? D. Add the VPN hostname as a SAN entry: This is more related to certificate management and does not ensure device-specific authentication.
References:
? CompTIA SecurityX Study Guide
? "Device Certificates for VPN Access," Cisco Documentation
? NIST Special Publication 800-77, "Guide to IPsec VPNs"

NEW QUESTION 113
A security engineer needs 10 secure the OT environment based on me following requirements
• Isolate the OT network segment
• Restrict Internet access.
• Apply security updates two workstations
• Provide remote access to third-party vendors
Which of the following design strategies should the engineer implement to best meet these requirements?

A. Deploy a jump box on the third party network to access the OT environment and provide updates using a physical delivery method on the workstations
B. Implement a bastion host in the OT network with security tools in place to monitor access and use a dedicated update server for the workstations.
C. Enable outbound internet access on the OT firewall to any destination IP address and use the centralized update server for the workstations
D. Create a staging environment on the OT network for the third-party vendor to access and enable automatic updates on the workstations.

Answer: B

Explanation:
To secure the Operational Technology (OT) environment based on the given requirements, the best approach is to implement a bastion host in the OT network. The bastion host serves as a secure entry point for remote access, allowing third-party vendors to connect
while being monitored by security tools. Using a dedicated update server for workstations ensures that security updates are applied in a controlled manner without direct internet access.
References:
? CompTIA SecurityX Study Guide: Recommends the use of bastion hosts and dedicated update servers for securing OT environments.
? NIST Special Publication 800-82, "Guide to Industrial Control Systems (ICS) Security": Advises on isolating OT networks and using secure remote access methods.
? "Industrial Network Security" by Eric D. Knapp and Joel Thomas Langill: Discusses strategies for securing OT networks, including the use of bastion hosts and update servers.

NEW QUESTION 115
A software engineer is creating a CI/CD pipeline to support the development of a web application The DevSecOps team is required to identify syntax errors Which of the following is the most relevant to the DevSecOps team's task'

A. Static application security testing
B. Software composition analysis
C. Runtime application self-protection
D. Web application vulnerability scanning

Answer: A

Explanation:
Static Application Security Testing (SAST) involves analyzing source code or compiled code for security vulnerabilities without executing the program. This method is well-suited for identifying syntax errors, coding standards violations, and potential security issues early in the development lifecycle.
? A. Static application security testing (SAST): SAST tools analyze the source code
to detect syntax errors, vulnerabilities, and other issues before the code is run. This is the most relevant task for the DevSecOps team to identify syntax errors and improve code quality.
? B. Software composition analysis: This focuses on identifying vulnerabilities in
open-source components and libraries used in the application but does not address syntax errors directly.
? C. Runtime application self-protection (RASP): RASP involves monitoring and
protecting applications during runtime, which does not help in identifying syntax errors during the development phase.
? D. Web application vulnerability scanning: This involves scanning the running
application for vulnerabilities but does not address syntax errors in the code.
References:
? CompTIA Security+ Study Guide
? OWASP (Open Web Application Security Project) guidelines on SAST
? NIST SP 800-95, "Guide to Secure Web Services" Top of Form
Bottom of Form

NEW QUESTION 118
A company isolated its OT systems from other areas of the corporate network These systems are required to report usage information over the internet to the vendor Which oi the following b*st reduces the risk of compromise or sabotage' (Select two).

A. Implementing allow lists
B. Monitoring network behavior
C. Encrypting data at rest
D. Performing boot Integrity checks
E. Executing daily health checks
F. Implementing a site-to-site IPSec VPN

Answer: AF

Explanation:
? A. Implementing allow lists: Allow lists (whitelisting) restrict network communication to only authorized devices and applications, significantly reducing the attack surface by ensuring that only pre-approved traffic is permitted.
? F. Implementing a site-to-site IPSec VPN: A site-to-site VPN provides a secure, encrypted tunnel for data transmission between the OT systems and the vendor, protecting the data from interception and tampering during transit.
Other options:
? B. Monitoring network behavior: While useful for detecting anomalies, it does not proactively reduce the risk of compromise or sabotage.
? C. Encrypting data at rest: Important for protecting data stored on devices, but does not address network communication risks.
? D. Performing boot integrity checks: Ensures the integrity of the system at startup but does not protect ongoing network communications.
? E. Executing daily health checks: Useful for maintaining system health but does not directly reduce the risk of network-based compromise or sabotage.
References:
? CompTIA Security+ Study Guide
? NIST SP 800-82, "Guide to Industrial Control Systems (ICS) Security"
? "Industrial Network Security" by Eric D. Knapp and Joel Thomas Langill

NEW QUESTION 120
A software company deployed a new application based on its internal code repository Several customers are reporting anti-malware alerts on workstations used to test the application Which of the following is the most likely cause of the alerts?

A. Misconfigured code commit
B. Unsecure bundled libraries
C. Invalid code signing certificate
D. Data leakage

Answer: B

Explanation:
The most likely cause of the anti-malware alerts on customer workstations is unsecure bundled libraries. When developing and deploying new applications, it is common for developers to use third-party libraries. If these libraries are not properly vetted for security, they can introduce vulnerabilities or malicious code.
Why Unsecure Bundled Libraries?
? Third-Party Risks: Using libraries that are not secure can lead to malware infections if the libraries contain malicious code or vulnerabilities.
? Code Dependencies: Libraries may have dependencies that are not secure, leading to potential security risks.
? Common Issue: This is a frequent issue in software development where libraries are used for convenience but not properly vetted for security.
Other options, while relevant, are less likely to cause widespread anti-malware alerts:
? A. Misconfigured code commit: Could lead to issues but less likely to trigger anti- malware alerts.
? C. Invalid code signing certificate: Would lead to trust issues but not typically anti- malware alerts.
? D. Data leakage: Relevant for privacy concerns but not directly related to anti- malware alerts.
References:
? CompTIA SecurityX Study Guide
? "Securing Open Source Libraries," OWASP
? "Managing Third-Party Software Security Risks," Gartner Research

NEW QUESTION 124
During a gap assessment, an organization notes that OYOD usage is a significant risk. The organization implemented administrative policies prohibiting BYOD usage However, the organization has not implemented technical controls to prevent the unauthorized use of BYOD assets when accessing the organization's resources. Which of the following
solutions should the organization implement to b»« reduce the risk of OYOD devices? (Select two).

A. Cloud 1AM to enforce the use of token based MFA
B. Conditional access, to enforce user-to-device binding
C. NAC, to enforce device configuration requirements
D. PA
E. to enforce local password policies
F. SD-WA
G. to enforce web content filtering through external proxies
H. DLP, to enforce data protection capabilities

Answer: BC

Explanation:
To reduce the risk of unauthorized BYOD (Bring Your Own Device) usage, the organization should implement Conditional Access and Network Access Control (NAC). Why Conditional Access and NAC?
? Conditional Access:
? Network Access Control (NAC):
Other options, while useful, do not address the specific need to control and secure BYOD devices effectively:
? A. Cloud IAM to enforce token-based MFA: Enhances authentication security but
does not control device compliance.
? D. PAM to enforce local password policies: Focuses on privileged account management, not BYOD control.
? E. SD-WAN to enforce web content filtering: Enhances network performance and security but does not enforce BYOD device compliance.
? F. DLP to enforce data protection capabilities: Protects data but does not control BYOD device access and compliance.
References:
? CompTIA SecurityX Study Guide

? "Conditional Access Policies," Microsoft Documentation
? "Network Access Control (NAC)," Cisco Documentation

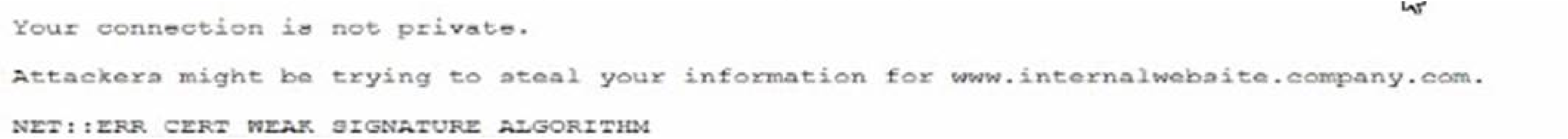
NEW QUESTION 128
A security operations engineer needs to prevent inadvertent data disclosure when encrypted SSDs are reused within an enterprise. Which of the following is the most secure way to achieve this goal?

A. Executing a script that deletes and overwrites all data on the SSD three times
B. Wiping the SSD through degaussing
C. Securely deleting the encryption keys used by the SSD
D. Writing non-zero, random data to all cells of the SSD

Answer: C

Explanation:
The most secure way to prevent inadvertent data disclosure when encrypted SSDs are reused is to securely delete the encryption keys used by the SSD. Without the encryption keys, the data on the SSD remains encrypted and is effectively unreadable, rendering any residual data useless. This method is more reliable and efficient than overwriting data multiple times or using other physical destruction methods.
References:
? CompTIA SecurityX Study Guide: Highlights the importance of managing encryption keys and securely deleting them to protect data.
? NIST Special Publication 800-88, "Guidelines for Media Sanitization": Recommends cryptographic erasure as a secure method for sanitizing encrypted storage devices.

NEW QUESTION 131
A security analyst received a report that an internal web page is down after a company- wide update to the web browser Given the following error message:



```
Your connection is not private.

Attackers might be trying to steal your information for www.internalwebsite.company.com.

NET::ERR CERT WEAK SIGNATURE ALGORITHM
```

Which of the following is the b«« way to fix this issue?

A. Rewriting any legacy web functions
B. Disabling all deprecated ciphers
C. Blocking all non-essential pons
D. Discontinuing the use of self-signed certificates

Answer: D

Explanation:
The error message "NET::ERR_CERT_WEAK_SIGNATURE_ALGORITHM" indicates that the web browser is rejecting the certificate because it uses a weak signature algorithm. This commonly happens with self-signed certificates, which often use outdated or insecure algorithms.
Why Discontinue Self-Signed Certificates?
? Security Compliance: Modern browsers enforce strict security standards and may reject certificates that do not comply with these standards.
? Trusted Certificates: Using certificates from a trusted Certificate Authority (CA) ensures compliance with security standards and is less likely to be flagged as insecure.
? Weak Signature Algorithm: Self-signed certificates might use weak algorithms like MD5 or SHA-1, which are considered insecure.
Other options do not address the specific cause of the certificate error:
? A. Rewriting legacy web functions: Does not address the certificate issue.
? B. Disabling deprecated ciphers: Useful for improving security but not related to the certificate error.
? C. Blocking non-essential ports: This is unrelated to the issue of certificate validation.
References:
? CompTIA SecurityX Study Guide
? "Managing SSL/TLS Certificates," OWASP
? "Best Practices for Certificate Management," NIST Special Publication 800-57

NEW QUESTION 132
......