

Exam Questions CAS-005

CompTIA SecurityX Exam

<https://www.2passeasy.com/dumps/CAS-005/>



NEW QUESTION 1

Within a SCADA a business needs access to the historian server in order together metric about the functionality of the environment. Which of the following actions should be taken to address this requirement?

- A. Isolating the historian server for connections only from The SCADA environment
- B. Publishing the C\$ share from SCADA to the enterprise
- C. Deploying a screened subnet between 11 and SCADA
- D. Adding the business workstations to the SCADA domain

Answer: A

Explanation:

The best action to address the requirement of accessing the historian server within a SCADA system is to isolate the historian server for connections only from the SCADA environment. Here??s why:

? Security and Isolation: Isolating the historian server ensures that only authorized devices within the SCADA environment can connect to it. This minimizes the attack surface and protects sensitive data from unauthorized access.

? Access Control: By restricting access to the historian server to only SCADA devices, the organization can better control and monitor interactions, ensuring that only legitimate queries and data retrievals occur.

? Best Practices for Critical Infrastructure: Following the principle of least privilege, isolating critical components like the historian server is a standard practice in securing SCADA systems, reducing the risk of cyberattacks.

? References:

NEW QUESTION 2

A company's SICM Is continuously reporting false positives and false negatives The security operations team has Implemented configuration changes to troubleshoot possible reporting errors Which of the following sources of information best supports the required analysts process? (Select two).

- A. Third-party reports and logs
- B. Trends
- C. Dashboards
- D. Alert failures
- E. Network traffic summaries
- F. Manual review processes

Answer: AB

Explanation:

When dealing with false positives and false negatives reported by a Security Information and Event Management (SIEM) system, the goal is to enhance the accuracy of the alerts and ensure that actual threats are identified correctly. The following sources of information best support the analysis process:

* A. Third-party reports and logs: Utilizing external sources of information such as threat intelligence reports, vendor logs, and other third-party data can provide a broader

perspective on potential threats. These sources often contain valuable insights and context that can help correlate events more accurately, reducing the likelihood of false positives and false negatives.

* B. Trends: Analyzing trends over time can help in understanding patterns and anomalies in the data. By observing trends, the security team can distinguish between normal and abnormal behavior, which aids in fine-tuning the SIEM configurations to better detect true positives and reduce false alerts.

Other options such as dashboards, alert failures, network traffic summaries, and manual review processes are also useful but are more operational rather than foundational for understanding the root causes of reporting errors in SIEM configurations.

References:

? CompTIA SecurityX Study Guide: Emphasizes the importance of leveraging external threat intelligence and historical trends for accurate threat detection.

? NIST Special Publication 800-92, "Guide to Computer Security Log Management": Highlights best practices for log management, including the use of third-party sources and trend analysis to improve incident detection.

? "Security Information and Event Management (SIEM) Implementation" by David Miller: Discusses the use of external intelligence and trends to enhance SIEM accuracy.

NEW QUESTION 3

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 4

Users must accept the terms presented in a captive portal when connecting to a guest network. Recently, users have reported that they are unable to access the Internet after joining the network. A network engineer observes the following:

- Users should be redirected to the captive portal.
- The Motive portal runs TL. S 1 2
- Newer browser versions encounter security errors that cannot be bypassed
- Certain websites cause unexpected re directs

Which of the following now likely explains this behavior?

- A. The TLS ciphers supported by the captive portal are deprecated
- B. Employment of the HSTS setting is proliferating rapidly.
- C. Allowed traffic rules are causing the NIPS to drop legitimate traffic
- D. An attacker is redirecting supplicants to an evil twin WLAN.

Answer: A

Explanation:

The most likely explanation for the issues encountered with the captive portal is that the TLS ciphers supported by the captive portal are deprecated. Here's why:

? TLS Cipher Suites: Modern browsers are continuously updated to support the latest security standards and often drop support for deprecated and insecure cipher suites. If the captive portal uses outdated TLS ciphers, newer browsers may refuse to connect, causing security errors.

? HSTS and Browser Security: Browsers with HTTP Strict Transport Security

(HSTS) enabled will not allow connections to sites with weak security configurations. Deprecated TLS ciphers would cause these browsers to block the connection.

? References:

By updating the TLS ciphers to modern, supported ones, the security engineer can ensure compatibility with newer browser versions and resolve the connectivity issues reported by users.

NEW QUESTION 5

A user submits a help desk ticket stating their account does not authenticate sometimes. An analyst reviews the following logs for the user:

Which of the following best explains the reason the user's access is being denied?

- A. incorrectly typed password
- B. Time-based access restrictions
- C. Account compromise
- D. Invalid user-to-device bindings

Answer: B

Explanation:

The logs reviewed for the user indicate that access is being denied due to time-based access restrictions. These restrictions are commonly implemented to limit access to systems during specific hours to enhance security. If a user attempts to authenticate outside of the allowed time window, access will be denied. This measure helps prevent unauthorized access during non-business hours, reducing the risk of security incidents.

References:

? CompTIA SecurityX Study Guide: Covers various access control methods, including time-based restrictions, as a means of enhancing security.

? NIST Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations": Recommends the use of time-based access restrictions as part of access control policies.

? "Access Control and Identity Management" by Mike Chapple and Aaron French: Discusses the implementation and benefits of time-based access restrictions.

NEW QUESTION 6

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 be 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 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/smtpd smtpd
587/tcp   open  ssl/smtpd 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 (0)

+Add Device For

10.1.45.65
 10.1.45.66
 10.1.45.67
 10.1.45.68

```

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

SFTP Server

Email Server

FTP Server

UTM Appliance

Web Server

Database Server

AD Server

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 7

During a security assessment using an EDR solution, a security engineer generates the following report about the assets in the system:

Device	Type	Status
LN002	Linux SE	Enabled (unmanaged)
OWIN23	Windows 7	Enabled
OWIN29	Windows 10	Enabled (bypass)

After five days, the EDR console reports an infection on the host OWIN23 by a remote access Trojan. Which of the following is the most probable cause of the infection?

- A. OWIN23 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. OWIN29 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 8

Developers have been creating and managing cryptographic material on their personal laptops for 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 to prevent LFI
- 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 9

A security engineer is developing a solution to meet the following requirements?

- All endpoints should be able to establish telemetry with a SIEM.
- All endpoints should be able to be integrated into the XDR platform.
- SOC services should be able to monitor the XDR platform

Which of the following should the security engineer implement to meet the requirements?

- A. CDR and central logging
- B. HIDS and vTPM
- C. WAF and syslog
- D. HIPS and host-based firewall

Answer: D

Explanation:

To meet the requirements of having all endpoints establish telemetry with a SIEM, integrate into an XDR platform, and allow SOC services to monitor the XDR platform, the best approach is to implement Host Intrusion Prevention Systems (HIPS) and a host-based firewall. HIPS can provide detailed telemetry data to the

SIEM and can be integrated into the XDR platform for comprehensive monitoring and response. The host-based firewall ensures that only authorized traffic is allowed, providing an additional layer of security.

References:

? CompTIA SecurityX Study Guide: Describes the roles of HIPS and host-based firewalls in endpoint security and their integration with SIEM and XDR platforms.

? NIST Special Publication 800-94, "Guide to Intrusion Detection and Prevention Systems (IDPS)": Highlights the capabilities of HIPS for security monitoring and incident response.

? "Network Security Monitoring" by Richard Bejtlich: Discusses the integration of various security tools, including HIPS and firewalls, for effective security monitoring.

NEW QUESTION 10

A security engineer is building a solution to disable weak CBC configuration for remote access connections to Linux systems. Which of the following should the security engineer modify?

- A. The /etc/openssl.conf file, updating the virtual site parameter
- B. The /etc/nsswitch.conf file, updating the name server
- C. The /etc/hosts file, updating the IP parameter
- D. The /etc/ssh/sshd_config file, updating the ciphers

Answer: D

Explanation:

The sshd_config file is the main configuration file for the OpenSSH server. To disable weak CBC (Cipher Block Chaining) ciphers for SSH connections, the security engineer should modify the sshd_config file to update the list of allowed ciphers. This file typically contains settings for the SSH daemon, including which encryption algorithms are allowed.

By editing the /etc/ssh/sshd_config file and updating the Ciphers directive, weak ciphers can be removed, and only strong ciphers can be allowed. This change ensures that the

SSH server does not use insecure encryption methods.

References:

? CompTIA Security+ Study Guide

? OpenSSH manual pages (man sshd_config)

? CIS Benchmarks for Linux

NEW QUESTION 10

Recent reports indicate that a software tool is being exploited. Attackers were able to bypass user access controls and load a database. A security analyst needs to find the vulnerability and recommend a mitigation. The analyst generates the following output:

```
C:\>whoami
local-user
C:\>netuser local-user Welcome!
The command completed successfully!
C:\>dbloader.exe local-user Welcome!
Insufficient Permissions. Now Closing...
C:\>strings dbloader.exe
!This program cannot be run in DOS Mode
dB10ad3r!
Load Database jmp
182(*nx
(i3jN*jk
fahn82mk0a
C:\>dbloader.exe admin dB10ad3r!
```

Which of the following would the analyst most likely recommend?

- A. Installing appropriate EDR tools to block pass-the-hash attempts
- B. Adding additional time to software development to perform fuzz testing
- C. Removing hard-coded credentials from the source code
- D. Not allowing users to change their local passwords

Answer: C

Explanation:

The output indicates that the software tool contains hard-coded credentials, which attackers can exploit to bypass user access controls and load the database. The most likely recommendation is to remove hard-coded credentials from the source code. Here's why:

? Security Best Practices: Hard-coded credentials are a significant security risk

because they can be easily discovered through reverse engineering or simple inspection of the code. Removing them reduces the risk of unauthorized access.

? Credential Management: Credentials should be managed securely using

environment variables, secure vaults, or configuration management tools that provide encryption and access controls.

? Mitigation of Exploits: By eliminating hard-coded credentials, the organization can

prevent attackers from easily bypassing authentication mechanisms and gaining

unauthorized access to sensitive systems.

? References:

NEW QUESTION 13

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 16

Company A and Company D are merging. Company A's compliance reports indicate branch protections are not in place. A security analyst needs to ensure that potential threats to the software development life cycle are addressed. Which of the following should the analyst consider when completing this task?

- A. If developers are unable to promote to production
- B. If DAST code is being stored to a single code repository
- C. If DAST scans are routinely scheduled
- D. If role-based training is deployed

Answer: C

Explanation:

Dynamic Application Security Testing (DAST) is crucial for identifying and addressing security vulnerabilities during the software development life cycle (SDLC). Ensuring that DAST scans are routinely scheduled helps in maintaining a secure development process. Why Routine DAST Scans?

? Continuous Security Assessment: Regular DAST scans help in identifying vulnerabilities in real-time, ensuring they are addressed promptly.

? Compliance: Routine scans ensure that the development process complies with security standards and regulations.

? Proactive Threat Mitigation: Regular scans help in early detection and mitigation of potential security threats, reducing the risk of breaches.

? Integration into SDLC: Ensures security is embedded within the development process, promoting a security-first approach.

Other options, while relevant, do not directly address the continuous assessment and proactive identification of threats:

? A. If developers are unable to promote to production: This is more of an operational issue than a security assessment.

? B. If DAST code is being stored to a single code repository: This concerns code management rather than security testing frequency.

? D. If role-based training is deployed: While important, training alone does not ensure continuous security assessment.

References:

? CompTIA Security+ Study Guide

? OWASP Testing Guide

? NIST Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations"

NEW QUESTION 19

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

A company hosts a platform-as-a-service solution with a web-based front end, through which customer interact with data sets. A security administrator needs to deploy controls to prevent application-focused attacks. Which of the following most directly supports the administrator's objective'

- A. improving security dashboard visualization on SIEM
- B. Rotating API access and authorization keys every two months
- C. Implementing application load balancing and cross-region availability
- D. Creating WAF policies for relevant programming languages

Answer: D

Explanation:

The best way to prevent application-focused attacks for a platform-as-a-service solution with a web-based front end is to create Web Application Firewall (WAF) policies for relevant programming languages. Here's why:

? Application-Focused Attack Prevention: WAFs are designed to protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. They help prevent attacks such as SQL injection, cross-site scripting (XSS), and other application-layer attacks.

? Customizable Rules: WAF policies can be tailored to the specific programming languages and frameworks used by the web application, providing targeted protection based on known vulnerabilities and attack patterns.

? Real-Time Protection: WAFs provide real-time protection, blocking malicious requests before they reach the application, thereby enhancing the security posture of the platform.

? References:

NEW QUESTION 28

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 33

SIMULATION

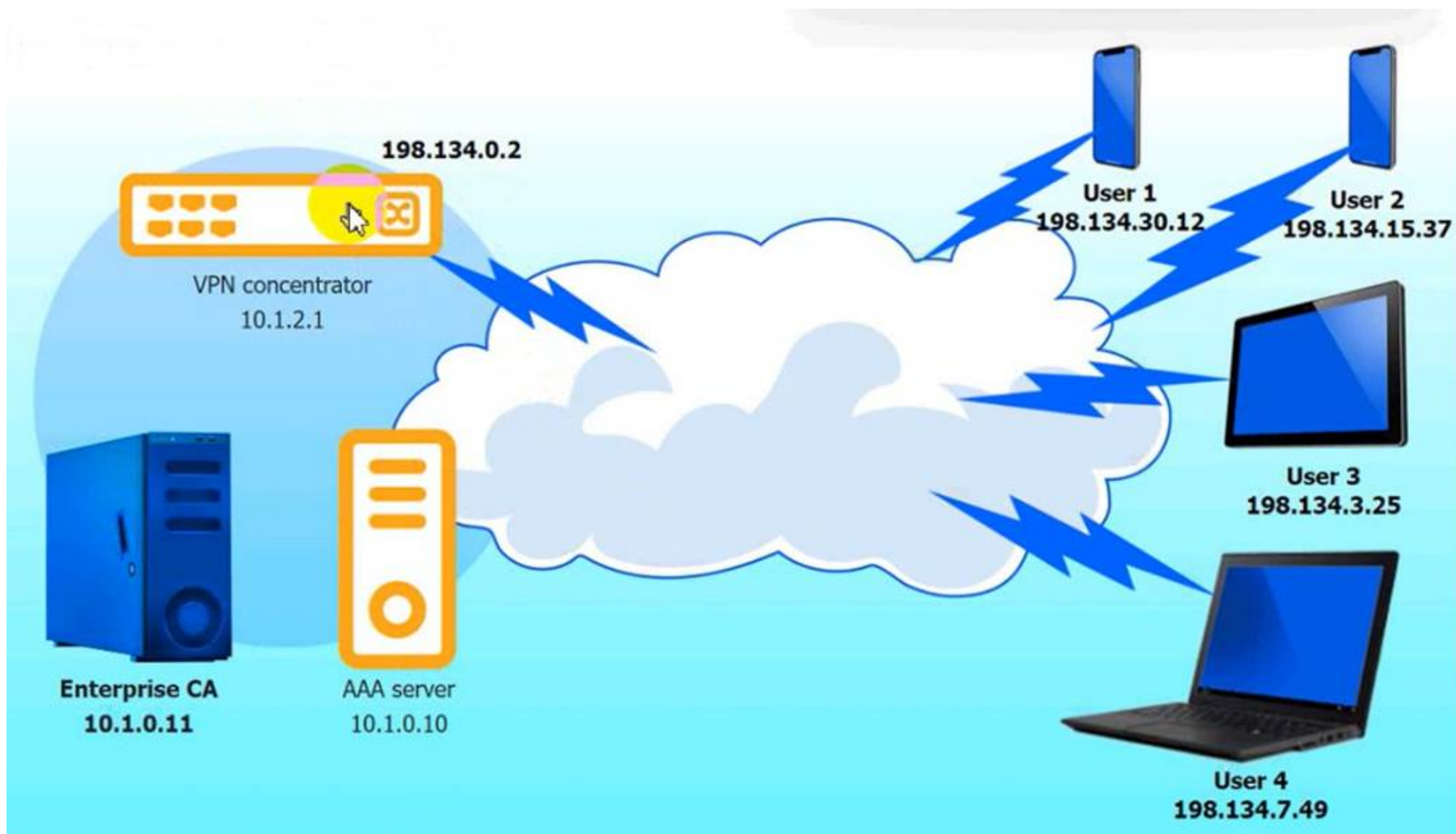
An IPSec solution is being deployed. The configuration files for both the VPN concentrator and the AAA server are shown in the diagram.

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:

VPN concentrator

Select proposal

peap
blowfish256
md5
aes256ccm128
aes128ctr
cast128
camellia256ctr
tls
ttls
psk
aes256gcm128

```

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

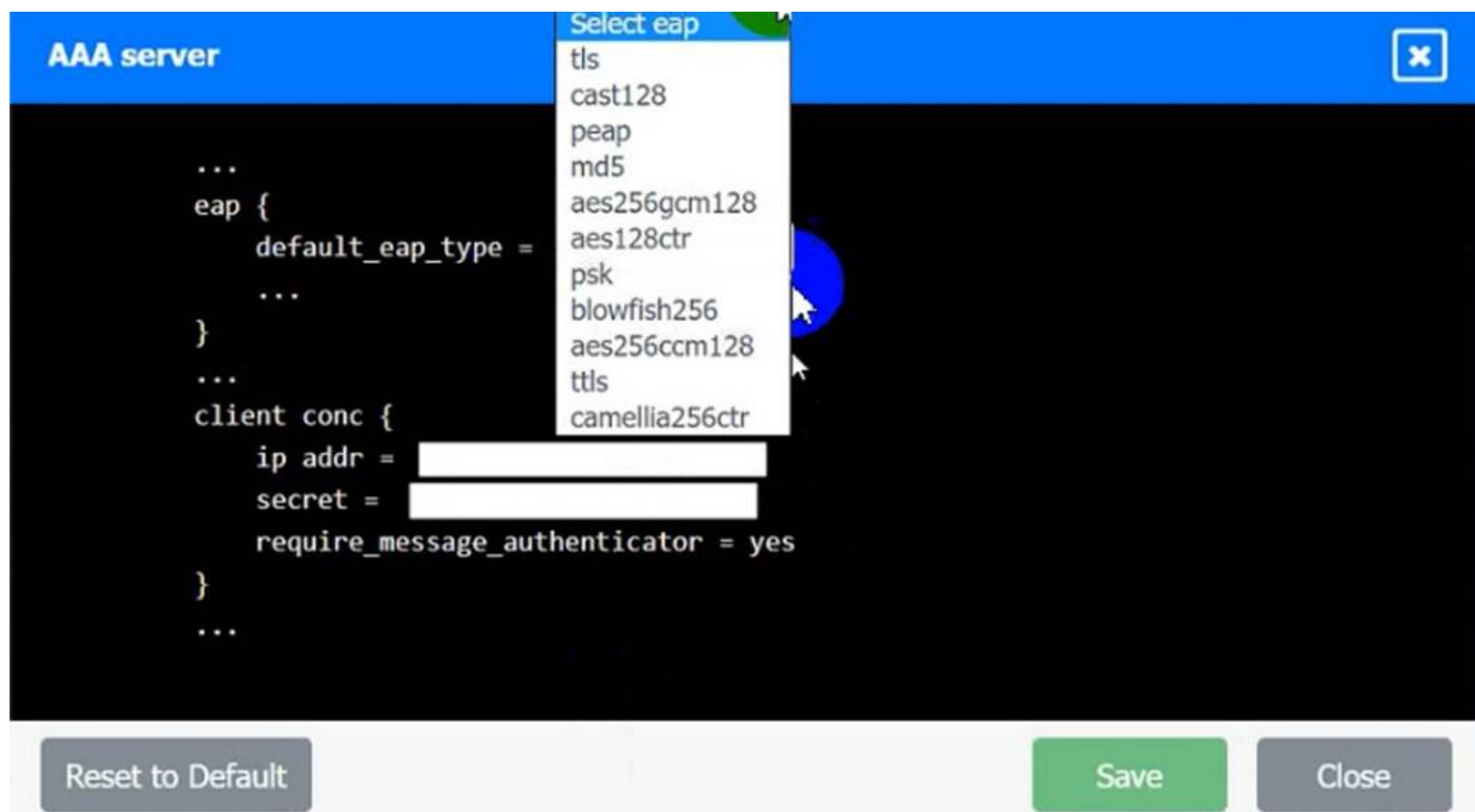
```

Reset to Default

Save

Close

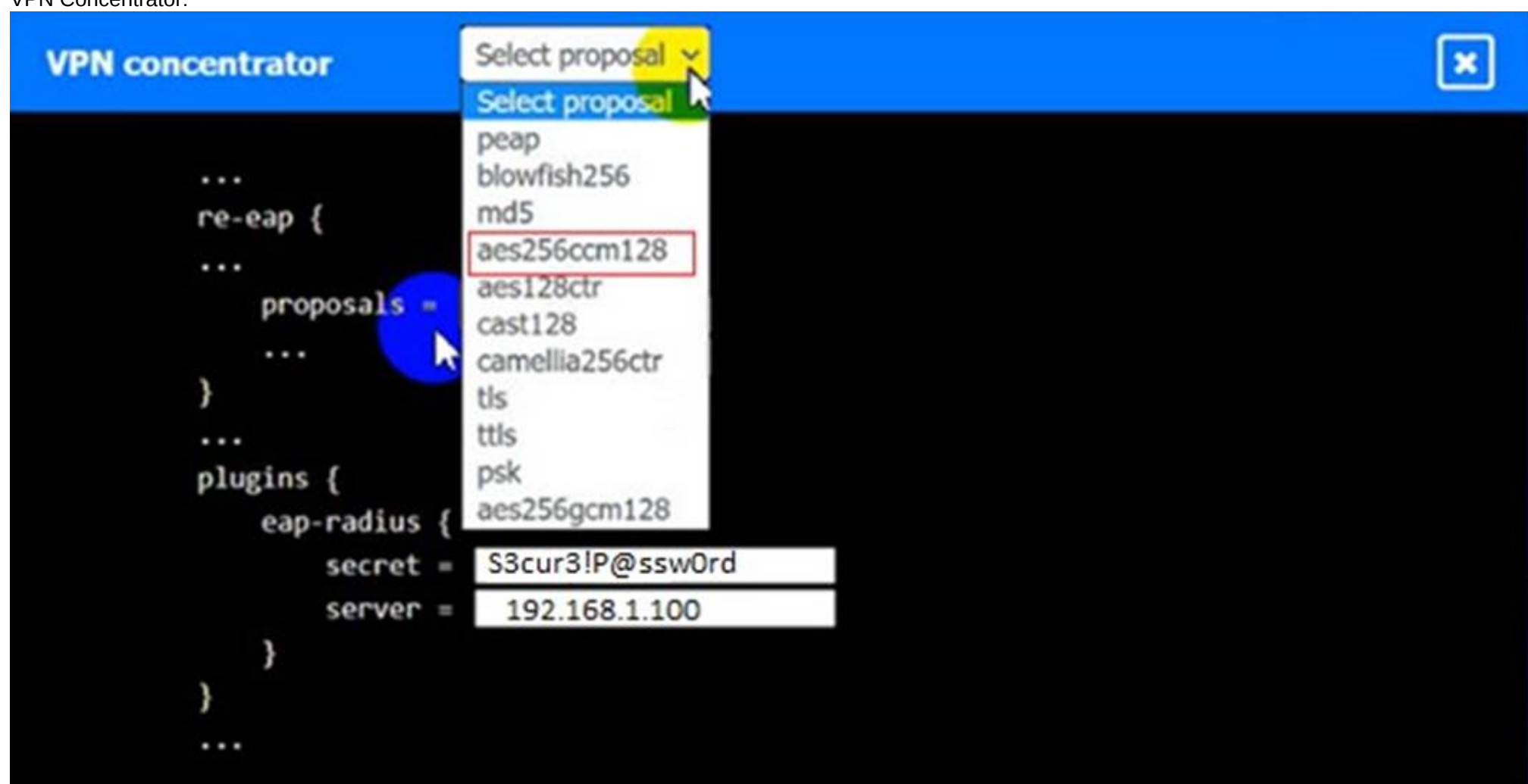
AAA Server:



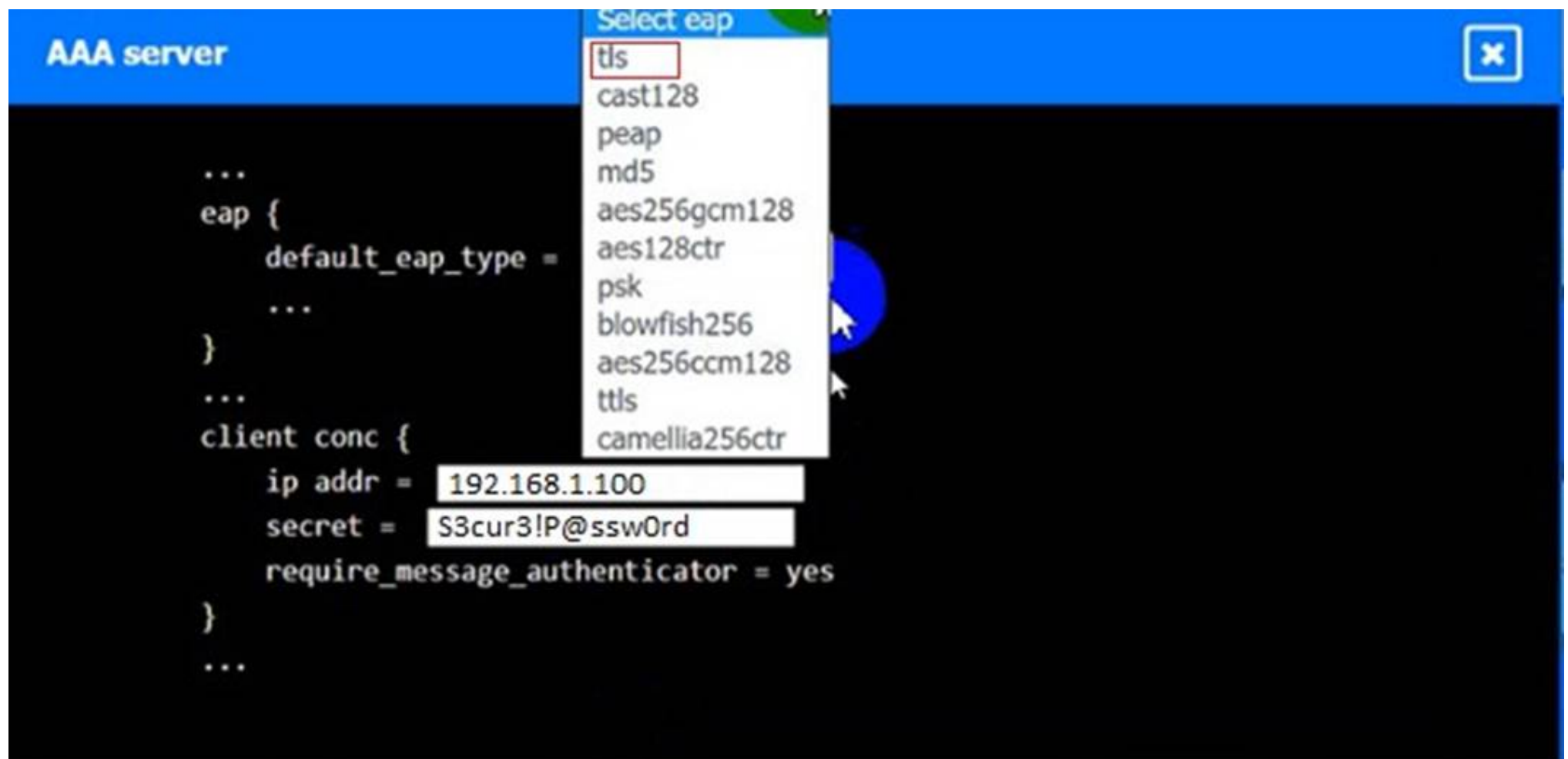
- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
 VPN Concentrator:



AAA Server:



NEW QUESTION 35

A central bank implements strict risk mitigations for the hardware supply chain, including an allow list for specific countries of origin. Which of the following best describes the cyberthreat to the bank?

- A. Ability to obtain components during wartime
- B. Fragility and other availability attacks
- C. Physical Implants and tampering
- D. Non-conformance to accepted manufacturing standards

Answer: C

Explanation:

The best description of the cyber threat to a central bank implementing strict risk mitigations for the hardware supply chain, including an allow list for specific countries of origin, is the risk of physical implants and tampering. Here's why:

? Supply Chain Security: The supply chain is a critical vector for hardware tampering and physical implants, which can compromise the integrity and security of hardware components before they reach the organization.

? Targeted Attacks: Banks and financial institutions are high-value targets, making them susceptible to sophisticated attacks, including those involving physical implants that can be introduced during manufacturing or shipping processes.

? Strict Mitigations: Implementing an allow list for specific countries aims to mitigate the risk of supply chain attacks by limiting the sources of hardware. However, the primary concern remains the introduction of malicious components through tampering.

? References:

NEW QUESTION 39

An organization is required to

- * Respond to internal and external inquiries in a timely manner
- * Provide transparency.
- * Comply with regulatory requirements

The organization has not experienced any reportable breaches but wants to be prepared if a breach occurs in the future. Which of the following is the best way for the organization to prepare?

- A. Outsourcing the handling of necessary regulatory filing to an external consultant
- B. Integrating automated response mechanisms into the data subject access request process
- C. Developing communication templates that have been vetted by internal and external counsel
- D. Conducting lessons-learned activities and integrating observations into the crisis management plan

Answer: C

Explanation:

Preparing communication templates that have been vetted by both internal and external counsel ensures that the organization can respond quickly and effectively to internal and external inquiries, comply with regulatory requirements, and provide transparency in the event of a breach.

Why Communication Templates?

? Timely Response: Pre-prepared templates ensure that responses are ready to be deployed quickly, reducing response time.

? Regulatory Compliance: Templates vetted by counsel ensure that all communications meet legal and regulatory requirements.

? Consistent Messaging: Ensures that all responses are consistent, clear, and accurate, maintaining the organization's credibility.

? Crisis Management: Pre-prepared templates are a critical component of a broader crisis management plan, ensuring that all stakeholders are informed appropriately.

Other options, while useful, do not provide the same level of preparedness and compliance:

? A. Outsourcing to an external consultant: This may delay response times and lose

internal control over the communication.

? B. Integrating automated response mechanisms: Useful for efficiency but not for ensuring compliant and vetted responses.

? D. Conducting lessons-learned activities: Important for improving processes but does not provide immediate preparedness for communication.

References:

? CompTIA SecurityX Study Guide

? NIST Special Publication 800-61 Revision 2, "Computer Security Incident Handling Guide"

? ISO/IEC 27002:2013, "Information technology — Security techniques — Code of practice for information security controls"

NEW QUESTION 42

A vulnerability can on a web server identified the following:

```
* TLS 1.2 Cipher Suites:
The server accepted the following 4 cipher suites:
TLS_RSA_WITH_DES_CBC_SHA          56
TLS_RSA_WITH_AES_128_CBC_SHA       128
TLS_RSA_WITH_3DES_EDE_CBC_SHA      168
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA  168 DH (1024 bits)
```

Which of the following actions would most likely eliminate on path decryption attacks? (Select two).

A. Disallowing cipher suites that use ephemeral modes of operation for key agreement

B. Removing support for CBC-based key exchange and signing algorithms

C. Adding TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA256

D. Implementing HIPS rules to identify and block BEAST attack attempts

E. Restricting cipher suites to only allow TLS_RSA_WITH_AES_128_CBC_SHA

F. Increasing the key length to 256 for TLS_RSA_WITH_AES_128_CBC_SHA

Answer: BC

Explanation:

On-path decryption attacks, such as BEAST (Browser Exploit Against SSL/TLS) and other related vulnerabilities, often exploit weaknesses in the implementation of CBC (Cipher Block Chaining) mode. To mitigate these attacks, the following actions are recommended:

? B. Removing support for CBC-based key exchange and signing algorithms: CBC

mode is vulnerable to certain attacks like BEAST. By removing support for CBC- based ciphers, you can eliminate one of the primary vectors for these attacks.

Instead, use modern cipher modes like GCM (Galois/Counter Mode) which offer better security properties.

? C. Adding TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA256: This cipher

suite uses Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) for key exchange, which provides perfect forward secrecy. It also uses AES in GCM mode, which is not susceptible to the same attacks as CBC. SHA-256 is a strong hash function that ensures data integrity.

References:

? CompTIA Security+ Study Guide

? NIST SP 800-52 Rev. 2, "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations"

? OWASP (Open Web Application Security Project) guidelines on cryptography and secure communication

NEW QUESTION 45

A security analyst needs to ensure email domains that send phishing attempts without previous communications are not delivered to mailboxes The following email headers are being reviewed

Date	Sending domain	Reply-to domain	Subject
April 16	sales.com	sales-mail.com	Updated Security Questions
April 18	vendor.com	vendor.com	New Sales Catalog
April 18	partner.com	partner.com	B2B Sales Increase
April 19	hr-saas.com	hr-saas.com	Employee Payroll Update Request
April 19	vendor.com	vendor.com	Password Requirements Not Met

Which of the following is the best action for the security analyst to take?

A. Block messages from hr-saas.com because it is not a recognized domain.

B. Reroute all messages with unusual security warning notices to the IT administrator

C. Quarantine all messages with sales-mail.com in the email header

D. Block vendor com for repeated attempts to send suspicious messages

Answer: D

Explanation:

In reviewing email headers and determining actions to mitigate phishing attempts, the security analyst should focus on patterns of suspicious behavior and the reputation of the sending domains. Here??s the analysis of the options provided:

* A. Block messages from hr-saas.com because it is not a recognized domain: Blocking a domain solely because it is not recognized can lead to legitimate emails being missed. Recognition alone should not be the criterion for blocking.

* B. Reroute all messages with unusual security warning notices to the IT administrator: While rerouting suspicious messages can be a good practice, it is not specific to the domain sending repeated suspicious messages.

* C. Quarantine all messages with sales-mail.com in the email header: Quarantining messages based on the presence of a specific domain in the email header can be too broad and may capture legitimate emails.

* D. Block vendor com for repeated attempts to send suspicious messages: This option is the most appropriate because it targets a domain that has shown a pattern of sending suspicious messages. Blocking a domain that repeatedly sends phishing attempts without previous communications helps in preventing future attempts from the same source and aligns with the goal of mitigating phishing risks.

References:

? CompTIA SecurityX Study Guide: Details best practices for handling phishing attempts, including blocking domains with repeated suspicious activity.

? NIST Special Publication 800-45 Version 2, "Guidelines on Electronic Mail Security": Provides guidelines on email security, including the management of suspicious email domains.

? "Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft" by Markus Jakobsson and Steven Myers: Discusses effective measures to counter phishing attempts, including blocking persistent offenders.

By blocking the domain that has consistently attempted to send suspicious messages, the security analyst can effectively reduce the risk of phishing attacks.

NEW QUESTION 49

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 54

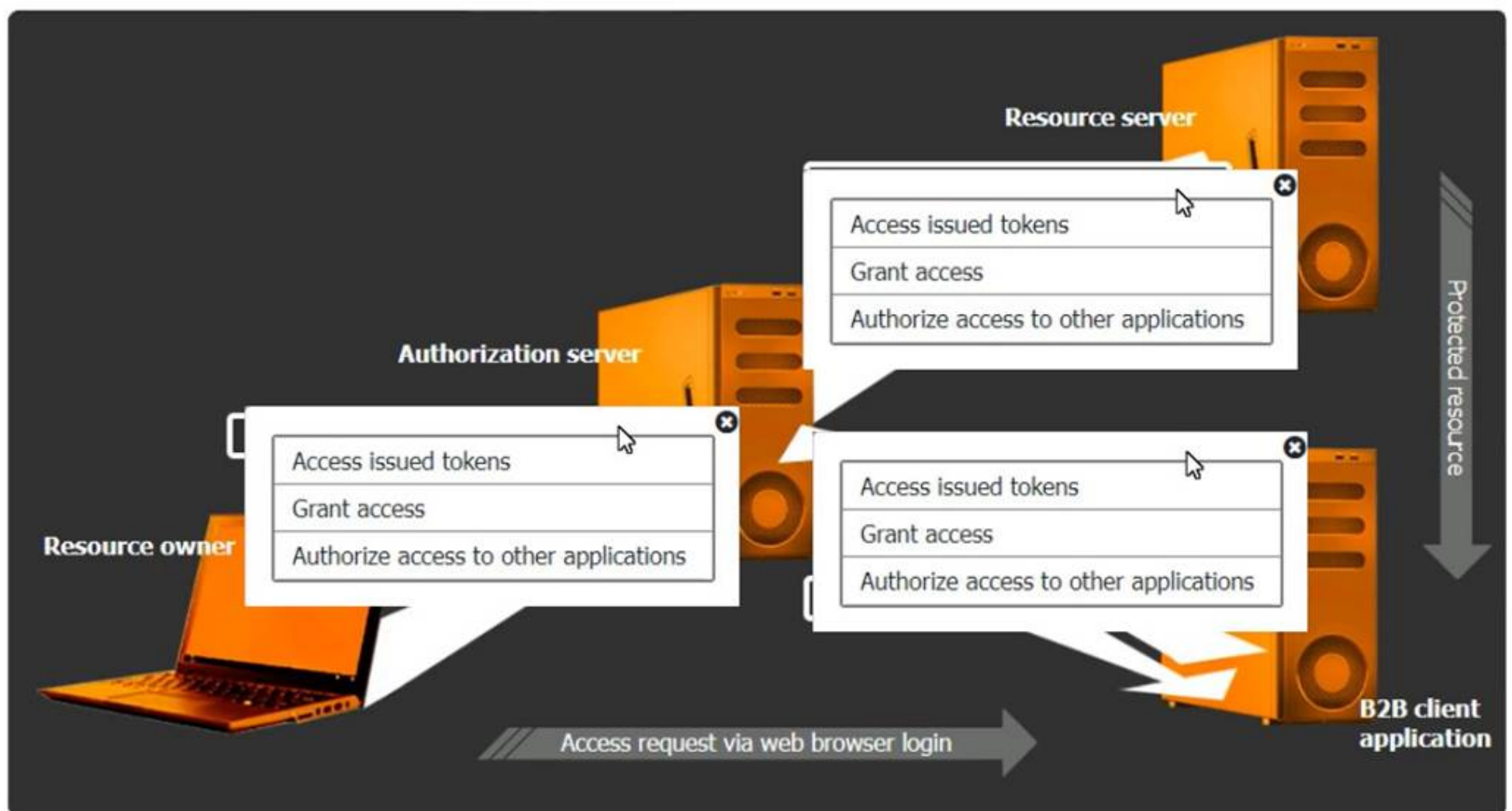
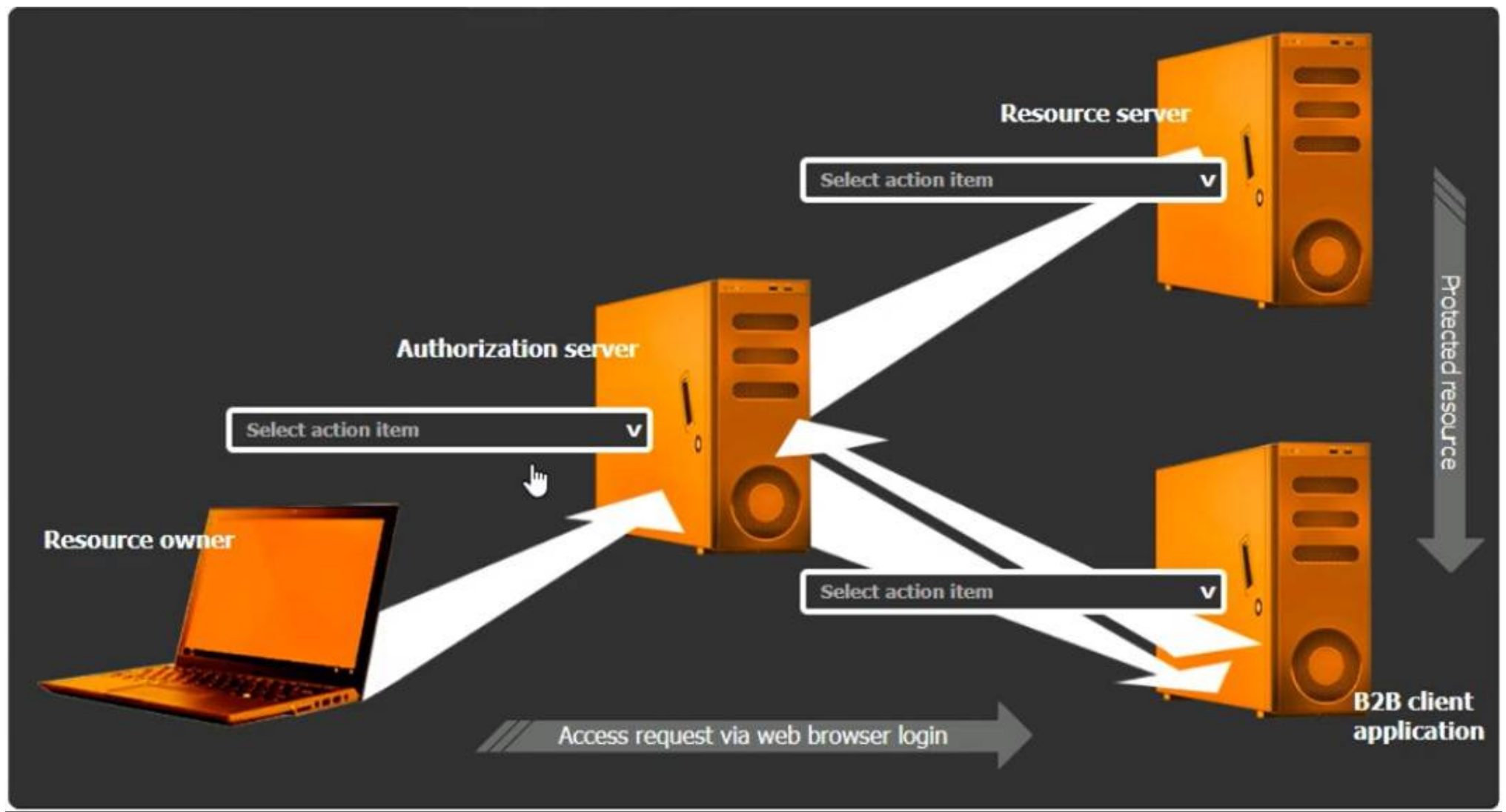
SIMULATION

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 59

Which of the following best describes the challenges associated with widespread adoption of homomorphic encryption techniques?

- A. Incomplete mathematical primitives
- B. No use cases to drive adoption
- C. Quantum computers not yet capable
- D. insufficient coprocessor support

Answer: D

Explanation:

Homomorphic encryption allows computations to be performed on encrypted data without decrypting it, providing strong privacy guarantees. However, the adoption of homomorphic encryption is challenging due to several factors:

? A. Incomplete mathematical primitives: This is not the primary barrier as the theoretical foundations of homomorphic encryption are well-developed.

? B. No use cases to drive adoption: There are several compelling use cases for homomorphic encryption, especially in privacy-sensitive fields like healthcare and finance.

? C. Quantum computers not yet capable: Quantum computing is not directly related to the challenges of adopting homomorphic encryption.

? D. Insufficient coprocessor support: The computational overhead of homomorphic encryption is significant, requiring substantial processing power. Current general-purpose processors are not optimized for the intensive computations required by homomorphic encryption, limiting its practical deployment. Specialized hardware or coprocessors designed to handle these computations more efficiently are not yet widely available.

References:

? CompTIA Security+ Study Guide

? "Homomorphic Encryption: Applications and Challenges" by Rivest et al.

? NIST, "Report on Post-Quantum Cryptography"

NEW QUESTION 61

A security architect for a global organization with a distributed workforce recently received funding to deploy a CASB solution. Which of the following most likely explains the choice to use a proxy-based CASB?

- A. The capability to block unapproved applications and services is possible
- B. Privacy compliance obligations are bypassed when using a user-based deployment.
- C. Protecting and regularly rotating API secret keys requires a significant time commitment
- D. Corporate devices cannot receive certificates when not connected to on-premises devices

Answer: A

Explanation:

A proxy-based Cloud Access Security Broker (CASB) is chosen primarily for its ability to block unapproved applications and services. Here's why:

? Application and Service Control: Proxy-based CASBs can monitor and control the use of applications and services by inspecting traffic as it passes through the proxy. This allows the organization to enforce policies that block unapproved applications and services, ensuring compliance with security policies.

? Visibility and Monitoring: By routing traffic through the proxy, the CASB can provide detailed visibility into user activities and data flows, enabling better monitoring and threat detection.

? Real-Time Protection: Proxy-based CASBs can provide real-time protection against threats by analyzing and controlling traffic before it reaches the end user, thus preventing the use of risky applications and services.

? References:

NEW QUESTION 62

A security administrator is performing a gap assessment against a specific OS benchmark. The benchmark requires the following configurations be applied to endpoints:

- Full disk encryption
- * Host-based firewall
- Time synchronization
- * Password policies
- Application allow listing
- * Zero Trust application access

Which of the following solutions best addresses the requirements? (Select two).

- A. CASB
- B. SBoM
- C. SCAP
- D. SASE
- E. HIDS

Answer: CD

Explanation:

To address the specific OS benchmark configurations, the following solutions are most appropriate:

- * C. SCAP (Security Content Automation Protocol): SCAP helps in automating vulnerability management and policy compliance, including configurations like full disk encryption, host-based firewalls, and password policies.
- * D. SASE (Secure Access Service Edge): SASE provides a framework for Zero Trust network access and application allow listing, ensuring secure and compliant access to applications and data.

These solutions together cover the comprehensive security requirements specified in the OS benchmark, ensuring a robust security posture for endpoints.

References:

? CompTIA SecurityX Study Guide: Discusses SCAP and SASE as part of security configuration management and Zero Trust architectures.

? NIST Special Publication 800-126, "The Technical Specification for the Security Content Automation Protocol (SCAP)": Details SCAP's role in security automation.

? "Zero Trust Networks: Building Secure Systems in Untrusted Networks" by Evan Gilman and Doug Barth: Covers the principles of Zero Trust and how SASE can implement them.

By implementing SCAP and SASE, the organization ensures that all the specified security configurations are applied and maintained effectively.

NEW QUESTION 67

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 71

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 73

A security analyst wants to use lessons learned from a poor incident response to reduce dwell time 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 77

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

Code Snippet 1

Code Snippet 2

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 80

An organization is developing on AI-enabled digital worker to help employees complete common tasks such as template development, editing, research, and scheduling. As part of the AI workload the organization wants to Implement guardrails within the platform. Which of the following should the company do to secure the AI environment?

- A. Limit the platform's abilities to only non-sensitive functions
- B. Enhance the training model's effectiveness.
- C. Grant the system the ability to self-govern
- D. Require end-user acknowledgement of organizational policies.

Answer: A

Explanation:

Limiting the platform's abilities to only non-sensitive functions helps to mitigate risks associated with AI operations. By ensuring that the AI-enabled digital worker is only allowed to perform tasks that do not involve sensitive or critical data, the organization reduces the potential impact of any security breaches or misuse. Enhancing the training model's effectiveness (Option B) is important but does not directly address security guardrails. Granting the system the ability to self-govern (Option C) could increase risk as it may act beyond the organization's control. Requiring end-user acknowledgement of organizational policies (Option D) is a good practice but does not implement technical guardrails to secure the AI environment.

References:

? CompTIA Security+ Study Guide

? NIST SP 800-53 Rev. 5, "Security and Privacy Controls for Information Systems and Organizations"

? ISO/IEC 27001, "Information Security Management"

NEW QUESTION 83

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 of the following best 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 85

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 87

A security architect is establishing requirements to design resilience in an enterprise system. The system must

- Be survivable to one environmental catastrophe
- Be recoverable within 24 hours of critical loss of availability
- Be resilient to active exploitation of one site-to-site VPN solution

- A. Load-balance connection attempts and data ingress at internet gateways

- B. Allocate fully redundant and geographically distributed standby sites.
- C. Employ layering of routers from diverse vendors
- D. Lease space to establish cold sites throughout other countries
- E. Use orchestration to procure, provision, and transfer application workloads to cloud services
- F. Implement full weekly backups to be stored off-site for each of the company's sites

Answer: B

Explanation:

To design resilience in an enterprise system that can survive environmental catastrophes, recover within 24 hours, and be resilient to active exploitation, the best strategy is to allocate fully redundant and geographically distributed standby sites. Here's why:

? Geographical Redundancy: Having geographically distributed standby sites ensures that if one site is affected by an environmental catastrophe, the other sites can take over, providing continuity of operations.

? Full Redundancy: Fully redundant sites mean that all critical systems and data are replicated, enabling quick recovery in the event of a critical loss of availability.

? Resilience to Exploitation: Distributing resources across multiple sites reduces the risk of a single point of failure and increases resilience against targeted attacks.

? References:

NEW QUESTION 92

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 93

SIMULATION

During the course of normal SOC operations, three anomalous events occurred and were flagged as potential IoCs. Evidence for each of these potential IoCs is provided.

INSTRUCTIONS

Review each of the events and select the appropriate analysis and remediation options for each IoC.

IoC 1		IoC 2		IoC 3	
Source	Svc	Type	Dest	Data	
Apache_httpd		DNSQ	@10.1.1.1:53	update.s.domain	
Apache_httpd		DNSQR	@10.1.2.5	CNAME 3a129sk219r0slsmfkzzz000.s.domain	
Apache_httpd		DNSQ	@10.1.1.1:53	3a129sk219r0slsmfkzzz000.s.domain	
Apache_httpd		DNSQR	@10.1.2.5	IN A 108.158.253.253	

Analysis

Select analysis

An employee is attempting to access a blocked website.
Someone is footprinting a network subnet.
A host is participating in an IRC-based botnet.
Service identification and fingerprinting are occurring.
Canonical name records in a public DNS cache are being updated.
An application is performing an automatic update.
An employee is using P2P services to download files.
The service is attempting to resolve a malicious domain.

Select analysis

Remediation

Select remediation

Enforce endpoint controls on third-party software installations.
Investigate for software supply-chain attacks.
Configure the DNS server to perform recursion.
Block ping requests across the WAN interface.
Deploy a network-based DLP solution.
Implement a blocklist for known malicious ports.
No further action is needed.

Select remediation

IoC 1		IoC 2		IoC 3	
Src	Dst	Proto	Data	Action	
10.0.5.5	10.1.2.1	IP_ICMP	ECHO	Drop	
10.0.5.5	10.1.2.2	IP_ICMP	ECHO	Drop	
10.0.5.5	10.1.2.3	IP_ICMP	ECHO	Drop	
10.0.5.5	10.1.2.4	IP_ICMP	ECHO	Drop	
10.0.5.5	10.1.2.5	IP_ICMP	ECHO	Drop	

Analysis

Select analysis

An employee is attempting to access a blocked website.
Someone is footprinting a network subnet.
A host is participating in an IRC-based botnet.
Service identification and fingerprinting are occurring.
Canonical name records in a public DNS cache are being updated.
An application is performing an automatic update.
An employee is using P2P services to download files.
The service is attempting to resolve a malicious domain.

Select analysis

Remediation

Select remediation

Enforce endpoint controls on third-party software installations.
Investigate for software supply-chain attacks.
Configure the DNS server to perform recursion.
Block ping requests across the WAN interface.
Deploy a network-based DLP solution.
Implement a blocklist for known malicious ports.
No further action is needed.

Select remediation

IoC 1

IoC 2

IoC 3

Proxylog>
> GET /announce?info_hash=%01d%FE%7E%F1%10%5CwvAp%ED%F6%03%C49%D6B%14%F1&
> peer_id=%B8js%7F%E8%0C%AFh%02Y%967%24e%27V%EEM%16%5B&port=41730&
> uploaded=0&downloaded=0&left=3767869&compact=1&ip=10.5.1.26&event=started
> HTTP/1.1
> Accept: application/x-bittorrent
> Accept-Encoding: gzip
> User-Agent: RAZA 2.1.0.0
> Host: localhost
> Connection: Keep-Alive
<
< HTTP 200 OK

Select analysis

An employee is attempting to access a blocked website.
Someone is footprinting a network subnet.
A host is participating in an IRC-based botnet.
Service identification and fingerprinting are occurring.
Canonical name records in a public DNS cache are being updated.
An application is performing an automatic update.
An employee is using P2P services to download files.
The service is attempting to resolve a malicious domain.

Select analysis

Select remediation

Enforce endpoint controls on third-party software installations.
Investigate for software supply-chain attacks.
Configure the DNS server to perform recursion.
Block ping requests across the WAN interface.
Deploy a network-based DLP solution.
Implement a blocklist for known malicious ports.
No further action is needed.

Select remediation

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Analysis and Remediation Options for Each IoC: IoC 1:

? Evidence:

? Analysis:

? Remediation:

IoC 2:

? Evidence:

? Analysis:

? Remediation:

IoC 3:

? Evidence:

? Analysis:

? Remediation:

References:

? CompTIA Security+ Study Guide: This guide offers detailed explanations on identifying and mitigating various types of Indicators of Compromise (IoCs) and the corresponding analysis and remediation strategies.

? CompTIA Security+ Exam Objectives: These objectives cover key concepts in network security monitoring and incident response, providing guidelines on how to handle different types of security events.

? Security Operations Center (SOC) Best Practices: This resource outlines effective strategies for analyzing and responding to anomalous events within a SOC, including the use of blocklists, endpoint controls, and network configuration changes.

By accurately analyzing the nature of each IoC and applying the appropriate remediation measures, the organization can effectively mitigate potential security threats and maintain a robust security posture.

NEW QUESTION 97

After an incident response exercise, a security administrator reviews the following table:

Service	Risk rating	Criticality rating	Alert severity
Public website	Medium	Low	Low
Email	High	High	High
Human resources systems	High	Medium	Medium
Phone system	High	Critical	Critical
Intranet	Low	Low	Low

Which of the following should the administrator do to beat support rapid incident response in the future?

- A. Automate alerting to IT support for phone system outages.
- B. Enable dashboards for service status monitoring
- C. Send emails for failed log-In attempts on the public website
- D. Configure automated Isolation of human resources systems

Answer: B

Explanation:

Enabling dashboards for service status monitoring is the best action to support rapid incident response. The table shows various services with different risk, criticality, and alert severity ratings. To ensure timely and effective incident response, real-time visibility into the status of these services is crucial.

Why Dashboards for Service Status Monitoring?

? Real-time Visibility: Dashboards provide an at-a-glance view of the current status of all critical services, enabling rapid detection of issues.

? Centralized Monitoring: A single platform to monitor the status of multiple services helps streamline incident response efforts.

? Proactive Alerting: Dashboards can be configured to show alerts and anomalies immediately, ensuring that incidents are addressed as soon as they arise.

? Improved Decision Making: Real-time data helps incident response teams make informed decisions quickly, reducing downtime and mitigating impact.

Other options, while useful, do not offer the same level of comprehensive, real-time visibility and proactive alerting:

? A. Automate alerting to IT support for phone system outages: This addresses one service but does not provide a holistic view.

? C. Send emails for failed log-in attempts on the public website: This is a specific alert for one type of issue and does not cover all services.

? D. Configure automated isolation of human resources systems: This is a reactive measure for a specific service and does not provide real-time status monitoring.

References:

? CompTIA SecurityX Study Guide

? NIST Special Publication 800-61 Revision 2, "Computer Security Incident Handling Guide"

? "Best Practices for Implementing Dashboards," Gartner Research

NEW QUESTION 100

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CAS-005 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CAS-005 Product From:

<https://www.2passeasy.com/dumps/CAS-005/>

Money Back Guarantee

CAS-005 Practice Exam Features:

- * CAS-005 Questions and Answers Updated Frequently
- * CAS-005 Practice Questions Verified by Expert Senior Certified Staff
- * CAS-005 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * CAS-005 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year