CAS-005$^{Q\&As}$

CompTIA SecurityX Exam

QUESTION 1

After investigating a recent security incident, a SOC analyst is charged with creating a reference guide for the entire team to use. Which of the following should the analyst create to address future incidents?

A. Root cause analysis

B. Communication plan

C. Runbook

D. Lessons learned

Correct Answer: C

QUESTION 2

Users must accept the terms presented in a captive petal 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:

1.

Users should be redirected to the captive portal.

2.

The Motive portal runs Tl. S 1 2

3.

Newer browser versions encounter security errors that cannot be bypassed

4.

Certain websites cause unexpected re directs

Which of the following mow likely explains this behavior?

A. The TLS ciphers supported by the captive portal ate 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.

Correct Answer: A

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.

QUESTION 3

A systems engineer is configuring a system baseline for servers that will provide email services. As part of the architecture design, the engineer needs to improve performance of the systems by using an access vector cache, facilitating mandatory access control and protecting against:

1.

Unauthorized reading and modification of data and programs

2.

Bypassing application security mechanisms

3.

Privilege escalation

4.

interference with other processes

Which of the following is the most appropriate for the engineer to deploy?

A. SELinux

B. Privileged access management

C. Self-encrypting disks

D. NIPS

Correct Answer: A

The most appropriate solution for the systems engineer to deploy is SELinux (Security- Enhanced Linux). Here\\'s why:

Mandatory Access Control (MAC): SELinux enforces MAC policies, ensuring that only authorized users and processes can access specific resources. This helps in preventing unauthorized reading and modification of data and programs.

Access Vector Cache: SELinux utilizes an access vector cache (AVC) to improve performance. The AVC caches access decisions, reducing the need for repetitive policy lookups and thus improving system efficiency. Security

Mechanisms:

SELinux provides a robust framework to enforce security policies and prevent bypassing of application security mechanisms. It controls access based on defined policies, ensuring that security measures are consistently applied. Privilege

Escalation and Process Interference: SELinux limits the ability of processes to escalate privileges and interfere with each other by enforcing strict access controls. This containment helps in isolating processes and minimizing the risk of

privilege escalation attacks.

References:

QUESTION 4

A company recently migrated its critical web application to a cloud provider\\'s environment. As part of the company\\'s risk management program, the company intends to conduct an external penetration test. According to the scope of work and the rules of engagement, the penetration tester will validate the web application\\'s security and check for opportunities to expose sensitive company information in the newly migrated cloud environment. Which of the following should be the first consideration prior to engaging in the test?

A. Prepare a redundant server to ensure the critical web application\\'s availability during the test.

B. Obtain agreement between the company and the cloud provider to conduct penetration testing.

C. Ensure the latest patches and signatures are deployed on the web server.

D. Create an NDA between the external penetration tester and the company.

Correct Answer: B

Obtain agreement between the company and the cloud provider to conduct penetration testing is the most critical first consideration. This ensures that the test is conducted legally and within the cloud provider\\'s policies, preventing any potential violations or disruptions.

QUESTION 5

A security researcher identified the following messages while testing a web application:

/file/admin/myprofile.php ERROR file does not exist.

/file/admin/userinfo.php ERROR file does not exist.

/file/admin/adminprofile.php ERROR file does not exist.

/file/admin/admininfo.php ERROR file does not exist.

/file/admin/universalprofile.php ERROR file does not exist. /file/admin/universalinfo.php ERROR file does not exist.

/file/admin/restrictedprofile.php ACCESS is denied.

/file/admin/restrictedinfo.php ERROR file does not exist.

Which of the following should the researcher recommend to remediate the issue?

A. Software composition analysis

B. Packet inspection

C. Proper error handling

D. Elimination of the use of unsafe functions

Correct Answer: C

The messages provide information about the existence and access permissions of certain files, which can be useful to an attacker. Proper error handling involves:

Ensuring that error messages do not reveal sensitive information about the server or its structure. Customizing error messages to be generic and user-friendly without disclosing specifics about the error (e.g., "An error occurred" instead of "ERROR file does not exist" or "ACCESS is denied"). Logging detailed error information on the server-side for debugging purposes without exposing it to the end user.

QUESTION 6

An organization has deployed a cloud-based application that provides virtual event services globally to clients. During a typical event, thousands of users access various entry pages within a short period of time. The entry pages include sponsor-related content that is relatively static and is pulled from a database. When the first major event occurs, users report poor response time on the entry pages. Which of the following features is the most appropriate for the company to implement?

A. Horizontal scalability

B. Vertical scalability

C. Containerization

D. Static code analysis

E. Caching

Correct Answer: E

Caching is the most appropriate feature for the company to implement in this scenario. Caching involves storing frequently accessed data closer to the user, reducing the need to retrieve data from the original source repeatedly. In the context of the virtual event services application, caching sponsor-related content on the entry pages can significantly improve response times for users. This approach leverages the static nature of the content and reduces the load on the database during peak usage times.

QUESTION 7

A software developer has been tasked with creating a unique threat detection mechanism that is based on machine learning. The information system for which the tool is being developed is on a rapid CI/CD pipeline, and the tool developer is considered a supplier to the process. Which of the following presents the most risk to the development life cycle and to the ability to deliver the security tool on time?

A. Deep learning language barriers

B. Big Data processing required for maturity

C. Secure, multiparty computation requirements

D. Computing capabilities available to the developer

Correct Answer: B

QUESTION 8

A compliance officer is responsible for selecting the right governance framework to protect individuals\\' data. Which of the following is the appropriate framework for the company to consult when collecting international user data for the

purpose of processing credit cards?

A. ISO 27001

B. COPPA

C. NIST 800-53

D. PCI DSS

Correct Answer: D

QUESTION 9

A company has identified a number of vulnerable, end-of-support systems with limited defensive capabilities. Which of the following would be the first step in reducing the attack surface in this environment?

A. Utilizing hardening recommendations

B. Deploying IPS/IDS throughout the environment

C. Installing and updating antivirus

D. Installing all available patches

Correct Answer: A

QUESTION 10

A company uses a CSP to provide a front end for its new payment system offering. The new offering is currently certified as PCI compliant. In order for the integrated solution to be compliant, the customer:

A. must also be PCI compliant, because the risk is transferred to the provider.

B. still needs to perform its own PCI assessment of the provider\\'s managed serverless service.

C. needs to perform a penetration test of the cloud provider\\'s environment.

D. must ensure in-scope systems for the new offering are also PCI compliant.

Correct Answer: D

QUESTION 11

A systems administrator wants to reduce the number of failed patch deployments in an organization. The administrator discovers that system owners modify systems or applications in an ad hoc manner.

Which of the following is the best way to reduce the number of failed patch deployments?

A. Compliance tracking

B. Situational awareness

C. Change management

D. Quality assurance

Correct Answer: C

To reduce the number of failed patch deployments, the systems administrator should implement a robust change management process. Change management ensures that all modifications to systems or applications are planned, tested, and

approved before deployment. This systematic approach reduces the risk of unplanned changes that can cause patch failures and ensures that patches are deployed in a controlled and predictable manner.

References:

CompTIA SecurityX Study Guide: Emphasizes the importance of change management in maintaining system integrity and ensuring successful patch deployments.

ITIL (Information Technology Infrastructure Library) Framework: Provides best practices for change management in IT services.

"The Phoenix Project" by Gene Kim, Kevin Behr, and George Spafford: Discusses the critical role of change management in IT operations and its impact on system stability and reliability.

QUESTION 12

A senior cybersecurity engineer is solving a digital certificate issue in which the CA denied certificate issuance due to failed subject identity validation. At which of the following steps within the PKI enrollment process would the denial have occurred?

A. RA

B. OCSP

C. CA

D. IdP

Correct Answer: C

While the CA is responsible for issuing the certificates, it relies on the RA (if one is used) to perform the identity validation. If the RA performs its duties correctly, any failed identity validation would be handled at the RA level, and the CA would not issue the certificate.

QUESTION 13

A security analyst received a notification from a cloud service provider regarding an attack detected on a web server The cloud service provider shared the following information about the attack:

1.

The attack came from inside the network.

2.

The attacking source IP was from the internal vulnerability scanners.

3.

The scanner is not configured to target the cloud servers.

Which of the following actions should the security analyst take first?

A. Create an allow list for the vulnerability scanner IPs m order to avoid false positives

B. Configure the scan policy to avoid targeting an out-of-scope host

C. Set network behavior analysis rules

D. Quarantine the scanner sensor to perform a forensic analysis

Correct Answer: D

When a security analyst receives a notification about an attack that appears to originate from an internal vulnerability scanner, it suggests that the scanner itself might have been compromised. This situation is critical because a compromised scanner can potentially conduct unauthorized scans, leak sensitive information, or execute malicious actions within the network. The appropriate first action involves containing the threat to prevent further damage and allow for a thorough investigation. Here\\'s why quarantining the scanner sensor is the best immediate action: Containment and Isolation: Quarantining the scanner will immediately prevent it from continuing any malicious activity or scans. This containment is crucial to protect the rest of the network from potential harm. Forensic Analysis: By isolating the scanner, a forensic analysis can be performed to understand how it was compromised, what actions it took, and what data or systems might have been affected. This analysis will provide valuable insights into the nature of the attack and help in taking appropriate remedial actions. Preventing Further Attacks: If the scanner is allowed to continue operating, it might execute more unauthorized actions, leading to greater damage. Quarantine ensures that the threat is neutralized promptly. Root Cause Identification: A forensic analysis can help identify vulnerabilities in the scanner\\'s configuration, software, or underlying system that allowed the compromise. This information is essential for preventing future incidents. Other options, while potentially useful in the long term, are not appropriate as immediate actions in this scenario:

A. Create an allow list for the vulnerability scanner IPs to avoid false positives:

This action addresses false positives but does not mitigate the immediate threat posed by the compromised scanner.

B. Configure the scan policy to avoid targeting an out-of-scope host: This step is preventive for future scans but does not deal with the current incident where the scanner is already compromised. C. Set network behavior analysis rules: While

useful for ongoing monitoring and detection, this does not address the immediate need to stop the compromised scanner\\'s activities. In conclusion, the first and most crucial action is to quarantine the scanner sensor to halt any malicious

activity and perform a forensic analysis to understand the scope and nature of the compromise. This step ensures that the threat is contained and provides a basis for further remediation efforts.

References:

CompTIA SecurityX Study Guide

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

QUESTION 14

DRAG DROP

A vulnerability scan with the latest definitions was performed across Sites A and B.

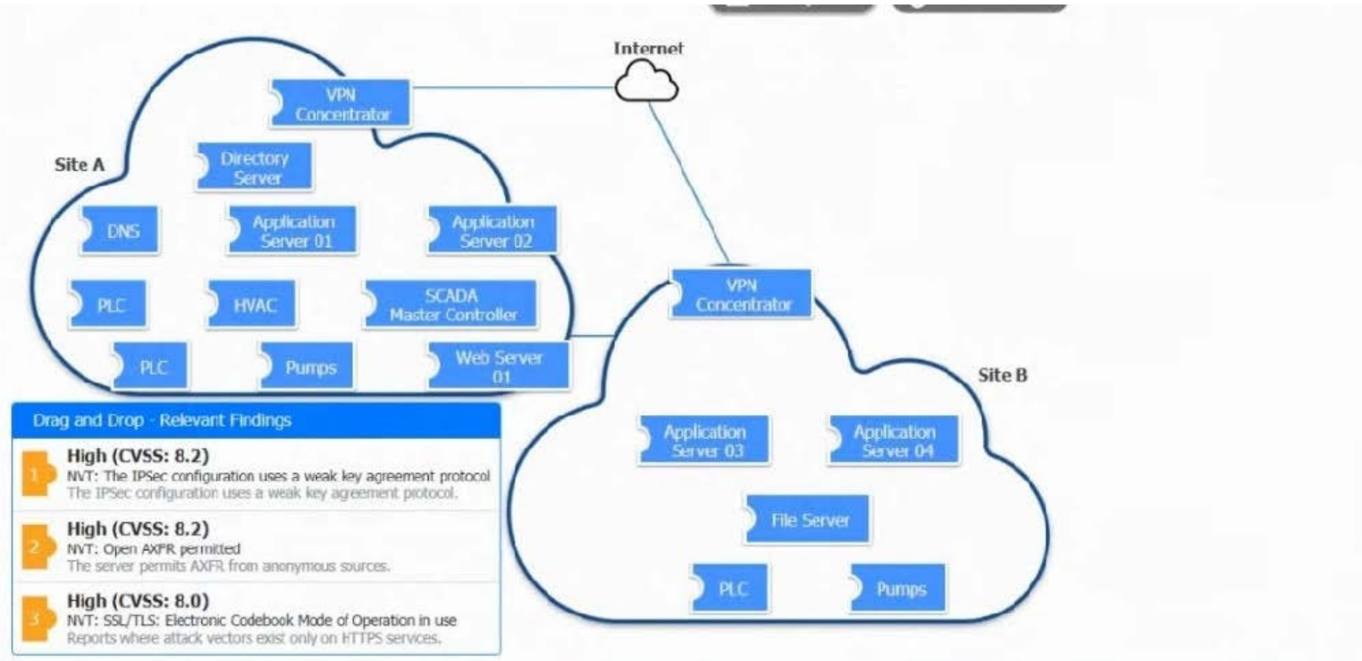
INSTRUCTIONS

Match each relevant finding to the affected host.

After associating the finding with the appropriate host(s), click the host to select the appropriate corrective action for that finding.

Each finding may be used more than once.

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



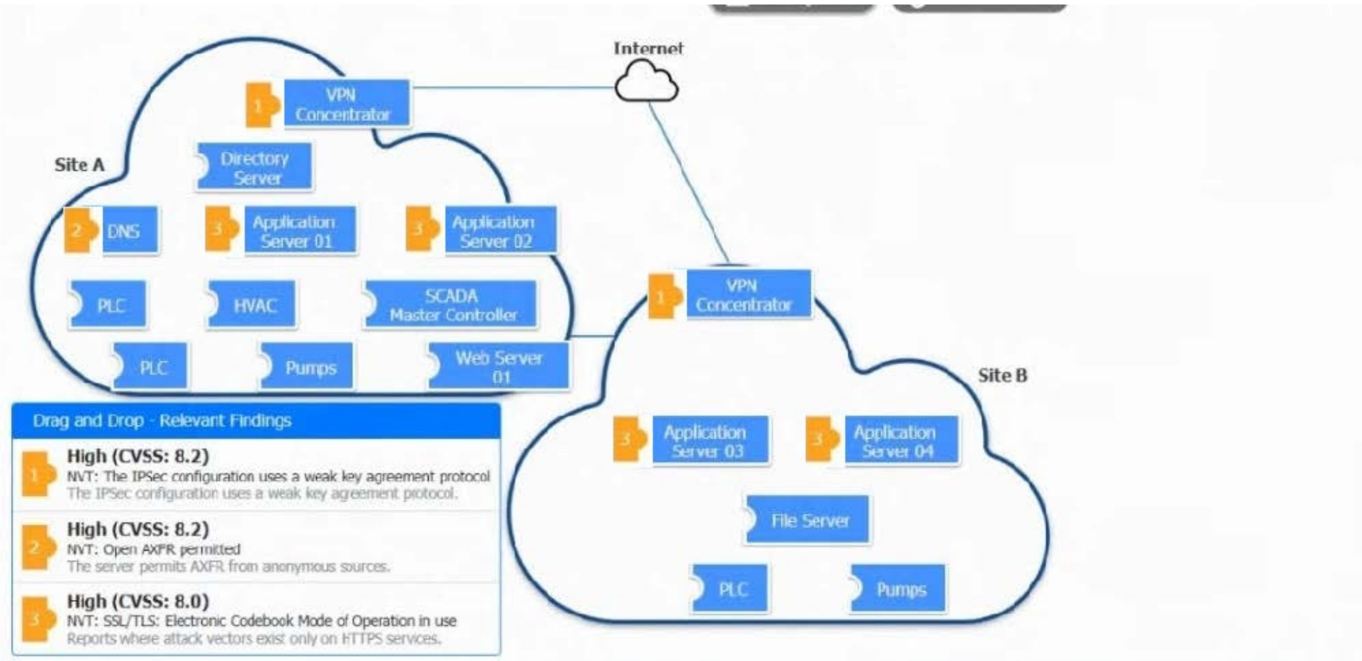
Drag and Drop - Relevant Findings

1 High (CVSS: 8.2)
NVT: The IPSec configuration uses a weak key agreement protocol
The IPSec configuration uses a weak key agreement protocol.

2 High (CVSS: 8.2)
NVT: Open AXFR permitted
The server permits AXFR from anonymous sources.

3 High (CVSS: 8.0)
NVT: SSL/TLS: Electronic Codebook Mode of Operation in use
Reports where attack vectors exist only on HTTPS services.

Correct Answer:



Drag and Drop - Relevant Findings

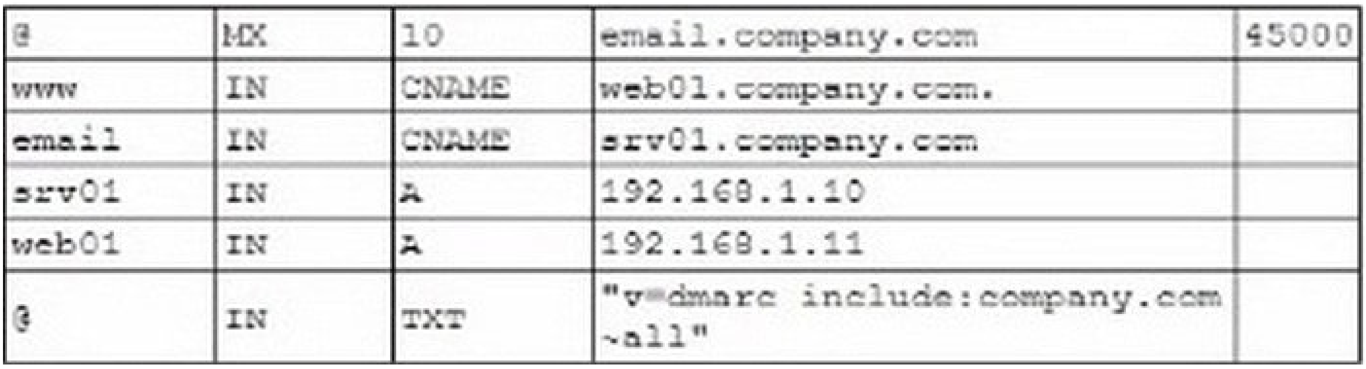
1 High (CVSS: 8.2)
NVT: The IPSec configuration uses a weak key agreement protocol
The IPSec configuration uses a weak key agreement protocol.

2 High (CVSS: 8.2)
NVT: Open AXFR permitted
The server permits AXFR from anonymous sources.

3 High (CVSS: 8.0)
NVT: SSL/TLS: Electronic Codebook Mode of Operation in use
Reports where attack vectors exist only on HTTPS services.

QUESTION 15

A company lined an email service provider called my-email.com to deliver company emails. The company stalled having several issues during the migration. A security engineer is troubleshooting and observes the following configuration snippet:



@	MX	10	email.company.com	45000
www	IN	CNAME	web01.company.com.	
email	IN	CNAME	srv01.company.com	
srv01	IN	A	192.168.1.10	
web01	IN	A	192.168.1.11	
@	IN	TXT	"v=dmarc include:company.com ~all"	

Which of the following should the security engineer modify to fix the issue? (Select two).

A. The email CNAME record must be changed to a type A record pointing to 192.168.111

B. The TXT record must be Changed to "v=dmarc ip4:192.168.1.10 include:my-email.com - all"

C. The srvo1 A record must be changed to a type CNAME record pointing to the email server

D. The email CNAME record must be changed to a type A record pointing to 192.168.1.10

E. The TXT record must be changed to "v=dkim ip4:l92.168.1.11 include my-email.com - ell"

F. The TXT record must be Changed to "v=dkim ip4:192.168.1.10 include:email-all"

G. The srv01 A record must be changed to a type CNAME record pointing to the web01 server

Correct Answer: BD

The security engineer should modify the following to fix the email migration issues:

Email CNAME Record: The email CNAME record must be changed to a type A record pointing to 192.168.1.10. This is because CNAME records should not be used where an IP address (A record) is required. Changing it to an A record

ensures direct pointing to the correct IP.

TXT Record for DMARC: The TXT record must be changed to "v=dmarc ip4:192.168.1.10 include

com -all". This ensures proper configuration of DMARC (Domain-based Message Authentication, Reporting and Conformance) to include the correct IP address and the email service provider domain.

uk.co.certification.simulator.questionpool.PList@492af720 References:

[Latest CAS-005 Dumps](#) [CAS-005 Practice Test](#) [CAS-005 Braindumps](#)