



CompTIA

Exam Questions CAS-005

CompTIA SecurityX Exam

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

A company's help desk is experiencing a large number of calls from the finance department slating access issues to www.bank.com. The security operations center reviewed the following security logs:

User	User IP & Subnet	Location	Website	DNS Resolved IP (public)	HTTP Status Code
User12	10.200.2.52/24	Finance	www.bank.com	65.146.76.34	495
User31	10.200.2.213/24	Finance	www.bank.com	65.146.76.34	495
User46	10.200.5.76/24	IT	www.bank.com	98.17.62.78	200
User23	10.200.2.156/24	Finance	www.bank.com	65.146.76.34	495
User51	10.200.4.138/24	Legal	www.bank.com	98.17.62.78	200

Which of the following is most likely the cause of the issue?

- A. Recursive DNS resolution is failing
- B. The DNS record has been poisoned.
- C. DNS traffic is being sinkholed.
- D. The DNS was set up incorrectly.

Answer: C

Explanation:

Sinkholing, or DNS sinkholing, is a method used to redirect malicious traffic to a safe destination. This technique is often employed by security teams to prevent access to malicious domains by substituting a benign destination IP address.

In the given logs, users from the finance department are accessing www.bank.com and receiving HTTP status code 495. This status code is typically indicative of a client certificate error, which can occur if the DNS traffic is being manipulated or redirected incorrectly. The consistency in receiving the same HTTP status code across different users suggests a systematic issue rather than an isolated incident.

? Recursive DNS resolution failure (A) would generally lead to inability to resolve DNS at all, not to a specific HTTP error.

? DNS poisoning (B) could result in users being directed to malicious sites, but again, would likely result in a different set of errors or unusual activity.

? Incorrect DNS setup (D) would likely cause broader resolution issues rather than targeted errors like the one seen here.

By reviewing the provided data, it is evident that the DNS traffic for www.bank.com is being rerouted improperly, resulting in consistent HTTP 495 errors for the finance department users. Hence, the most likely cause is that the DNS traffic is being sinkholed.

References:

? CompTIA SecurityX study materials on DNS security mechanisms.

? Standard HTTP status codes and their implications.

NEW QUESTION 2

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

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

Answer: D

Explanation:

Encrypting patient data at rest is a critical requirement for healthcare providers to ensure compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA). The primary business requirement fulfilled by this practice is the protection of patient privacy while supporting the portability of medical information. By encrypting data at rest, healthcare providers safeguard sensitive patient information from unauthorized access, ensuring that privacy is maintained even if the storage media are compromised. Additionally, encryption supports the portability of patient records, allowing for secure transfer and access across different systems and locations while ensuring that privacy controls are in place.

References:

? CompTIA SecurityX Study Guide: Emphasizes the importance of data encryption for protecting sensitive information and ensuring compliance with regulatory requirements.

? HIPAA Security Rule: Requires healthcare providers to implement safeguards, including encryption, to protect patient data.

? "Health Informatics: Practical Guide for Healthcare and Information Technology Professionals" by Robert E. Hoyt: Discusses encryption as a key measure for protecting patient data privacy and supporting data portability.

NEW QUESTION 3

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

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

Answer: B

Explanation:

A Cloud Access Security Broker (CASB) is a security policy enforcement point placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as cloud-based resources are accessed. Implementing a CASB provides several benefits:

? A. Improve firewall rules to avoid access to those platforms: This can help but is not as effective or comprehensive as a CASB.

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

NEW QUESTION 4

A developer needs to improve the cryptographic strength of a password-storage component in a web application without completely replacing the crypto-module. Which of the following is the most appropriate technique?

- A. Key splitting
- B. Key escrow
- C. Key rotation
- D. Key encryption
- E. Key stretching

Answer: E

Explanation:

The most appropriate technique to improve the cryptographic strength of a password-storage component in a web application without completely replacing the crypto-module is key stretching. Here's why:

- ? Enhanced Security: Key stretching algorithms, such as PBKDF2, bcrypt, and scrypt, increase the computational effort required to derive the encryption key from the password, making brute-force attacks more difficult and time-consuming.
- ? Compatibility: Key stretching can be implemented alongside existing cryptographic modules, enhancing their security without the need for a complete overhaul.
- ? Industry Best Practices: Key stretching is a widely recommended practice for securely storing passwords, as it significantly improves resistance to password-cracking attacks.
- ? References:

NEW QUESTION 5

A news organization wants to implement workflows that allow users to request that untruthful data be retraced and scrubbed from online publications to comply with the right to be forgotten. Which of the following regulations is the organization most likely trying to address?

- A. GDPR
- B. COPPA
- C. CCPA
- D. DORA

Answer: A

Explanation:

The General Data Protection Regulation (GDPR) is the regulation most likely being addressed by the news organization. GDPR includes provisions for the "right to be forgotten," which allows individuals to request the deletion of personal data that is no longer necessary for the purposes for which it was collected. This regulation aims to protect the privacy and personal data of individuals within the European Union.

References:

- ? CompTIA SecurityX Study Guide: Covers GDPR and its requirements, including the right to be forgotten.
- ? GDPR official documentation: Details the rights of individuals, including data erasure and the right to be forgotten.
- ? "GDPR: A Practical Guide to the General Data Protection Regulation" by IT Governance Privacy Team: Provides a comprehensive overview of GDPR compliance, including workflows for data deletion requests.

NEW QUESTION 6

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 7

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/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 (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 8

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 9

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 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

A security engineer performed a code scan that resulted in many false positives. The security engineer must find a solution that improves the quality of scanning results before application deployment. Which of the following is the best solution?

- A. Limiting the tool to a specific coding language and tuning the rule set
- B. Configuring branch protection rules and dependency checks
- C. Using an application vulnerability scanner to identify coding flaws in production
- D. Performing updates on code libraries before code development

Answer: A

Explanation:

To improve the quality of code scanning results and reduce false positives, the best solution is to limit the tool to a specific coding language and fine-tune the rule set. By configuring the code scanning tool to focus on the specific language used in the application, the tool can more accurately identify relevant issues and reduce the number of false positives. Additionally, tuning the rule set ensures that the tool's checks are appropriate for the application's context, further improving the accuracy of the scan results.

References:

? CompTIA SecurityX Study Guide: Discusses best practices for configuring code scanning tools, including language-specific tuning and rule set adjustments.

? "Secure Coding: Principles and Practices" by Mark G. Graff and Kenneth R. van Wyk: Highlights the importance of customizing code analysis tools to reduce false positives.

? OWASP (Open Web Application Security Project): Provides guidelines for configuring and tuning code scanning tools to improve accuracy.

NEW QUESTION 15

An organization that performs real-time financial processing is implementing a new backup solution. Given the following business requirements?

- * The backup solution must reduce the risk for potential backup compromise
- * The backup solution must be resilient to a ransomware attack.
- * The time to restore from backups is less important than the backup data integrity
- * Multiple copies of production data must be maintained

Which of the following backup strategies best meets these requirements?

- A. Creating a secondary, immutable storage array and updating it with live data on a continuous basis
- B. Utilizing two connected storage arrays and ensuring the arrays constantly sync
- C. Enabling remote journaling on the databases to ensure real-time transactions are mirrored
- D. Setting up antitempering on the databases to ensure data cannot be changed unintentionally

Answer: A

Explanation:

? A. Creating a secondary, immutable storage array and updating it with live data on a continuous basis: An immutable storage array ensures that data, once written, cannot be altered or deleted. This greatly reduces the risk of backup compromise

and provides resilience against ransomware attacks, as the ransomware cannot modify or delete the backup data. Maintaining multiple copies of production data with an immutable storage solution ensures data integrity and compliance with the requirement for multiple copies.

Other options:

? B. Utilizing two connected storage arrays and ensuring the arrays constantly sync: While this ensures data redundancy, it does not provide protection against ransomware attacks, as both arrays could be compromised simultaneously.

? C. Enabling remote journaling on the databases: This ensures real-time transaction mirroring but does not address the requirement for reducing the risk of backup compromise or resilience to ransomware.

? D. Setting up anti-tampering on the databases: While this helps ensure data integrity, it does not provide a comprehensive backup solution that meets all the specified requirements.

References:

? CompTIA Security+ Study Guide

? NIST SP 800-209, "Security Guidelines for Storage Infrastructure"

? "Immutable Backup Architecture" by Veeam

NEW QUESTION 20

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

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

Answer: B

Explanation:

A centralized Software Bill of Materials (SBOM) is the best solution for identifying vulnerabilities in container images in a private repository. An SBOM provides a comprehensive inventory of all components, dependencies, and their versions within a container image, facilitating quick evaluation and response to vulnerabilities. Why Centralized SBOM?

? Comprehensive Inventory: An SBOM lists all software components, including their versions and dependencies, allowing for thorough vulnerability assessments.

? Quick Identification: Centralizing SBOM data enables rapid identification of affected containers when a vulnerability is disclosed.

? Automation: SBOMs can be integrated into automated tools for continuous monitoring and alerting of vulnerabilities.

? Regulatory Compliance: Helps in meeting compliance requirements by providing a clear and auditable record of all software components used.

Other options, while useful, do not provide the same level of comprehensive and efficient vulnerability management:

- ? A. SAST scan reports: Focuses on static analysis of code but may not cover all components in container images.
- ? C. CIS benchmark compliance reports: Ensures compliance with security benchmarks but does not provide detailed component inventory.
- ? D. Credentialed vulnerability scan: Useful for in-depth scans but may not be as efficient for quick vulnerability evaluation.

References:

- ? CompTIA SecurityX Study Guide
- ? "Software Bill of Materials (SBOM)," NIST Documentation
- ? "Managing Container Security with SBOM," OWASP

NEW QUESTION 25

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

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

Answer: B

Explanation:

When differentiating between valid and invalid findings from vulnerability scans, the systems administrator should verify that the scanning credentials are properly configured. Valid credentials ensure that the scanner can authenticate and access the systems being evaluated, providing accurate and comprehensive results. Without proper credentials, scans may miss vulnerabilities or generate false positives, making it difficult to prioritize and address the findings effectively.

References:

- ? CompTIA SecurityX Study Guide: Highlights the importance of using valid credentials for accurate vulnerability scanning.
- ? "Vulnerability Management" by Park Foreman: Discusses the role of scanning credentials in obtaining accurate scan results and minimizing false positives.
- ? "The Art of Network Security Monitoring" by Richard Bejtlich: Covers best practices for configuring and using vulnerability scanning tools, including the need for valid credentials.

NEW QUESTION 28

A security analyst Detected unusual network traffic related to program updating processes The analyst collected artifacts from compromised user workstations. The discovered artifacts were binary files with the same name as existing, valid binaries but. with different hashes which of the following solutions would most likely prevent this situation from reoccurring?

- A. Improving patching processes
- B. Implementing digital signature
- C. Performing manual updates via USB ports
- D. Allowing only dies from internal sources

Answer: B

Explanation:

Implementing digital signatures ensures the integrity and authenticity of software binaries. When a binary is digitally signed, any tampering with the file (e.g., replacing it with a malicious version) would invalidate the signature. This allows systems to verify the origin and integrity of binaries before execution, preventing the execution of unauthorized or compromised binaries.

- ? A. Improving patching processes: While important, this does not directly address the issue of verifying the integrity of binaries.
- ? B. Implementing digital signatures: This ensures that only valid, untampered binaries are executed, preventing attackers from substituting legitimate binaries with malicious ones.
- ? C. Performing manual updates via USB ports: This is not practical and does not scale well, especially in large environments.
- ? D. Allowing only files from internal sources: This reduces the risk but does not provide a mechanism to verify the integrity of binaries.

References:

- ? CompTIA Security+ Study Guide
- ? NIST SP 800-57, "Recommendation for Key Management"
- ? OWASP (Open Web Application Security Project) guidelines on code signing

NEW QUESTION 29

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

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

Answer: D

Explanation:

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

Reference: CompTIA SecurityX Study Guide, Chapter on Zero Trust Security, Section on Microsegmentation and Network Segmentation.

NEW QUESTION 34

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

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

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

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

Answer: D

Explanation:

The log-in activity indicates a security threat, particularly involving the ADMIN account with a high-risk failure status. This suggests that the account may be targeted by malicious activities such as credential stuffing or brute force attacks.

? Updating log configuration settings (A) may help in better logging future activities but does not address the immediate threat.

? Changing the admin account password (B) is a good practice but may not fully mitigate the ongoing threat if the account has already been compromised.

? Blocking employees (C) from logging into non-business applications might help in reducing attack surfaces but doesn't directly address the compromised account issue.

Implementing automation to disable accounts associated with high-risk activities ensures an immediate response to the detected threat, preventing further unauthorized access and allowing time for thorough investigation and remediation.

References:

? CompTIA SecurityX guide on incident response and account management.

? Best practices for handling compromised accounts.

? Automation tools and techniques for security operations centers (SOCs).

NEW QUESTION 36

After an incident occurred, a team reported during the lessons-learned review that the team.

* Lost important information for further analysis.

* Did not utilize the chain of communication

* Did not follow the right steps for a proper response

Which of the following solutions is the best way to address these findings?

- A. Requesting budget for better forensic tools to improve technical capabilities for incident response operations
- B. Building playbooks for different scenarios and performing regular table-top exercises
- C. Requiring professional incident response certifications for each new team member
- D. Publishing the incident response policy and enforcing it as part of the security awareness program

Answer: B

Explanation:

Building playbooks for different scenarios and performing regular table-top exercises directly addresses the issues identified in the lessons-learned review. Here's why:

? Lost important information for further analysis: Playbooks outline step-by-step procedures for incident response, ensuring that team members know exactly what to document and how to preserve evidence.

? Did not utilize the chain of communication: Playbooks include communication protocols, specifying who to notify and when. Regular table-top exercises reinforce these communication channels, ensuring they are followed during actual incidents.

? Did not follow the right steps for a proper response: Playbooks provide a clear sequence of actions to be taken during various types of incidents, helping the team to respond in a structured and effective manner. Regular exercises allow the team to practice these steps, identifying and correcting any deviations from the plan.

Investing in better forensic tools (Option A) or requiring certifications (Option C) are also valuable, but they do not directly address the procedural and communication gaps identified. Publishing and enforcing the incident response policy (Option D) is important but not as practical and hands-on as playbooks and exercises in ensuring the team is prepared.

References:

? CompTIA Security+ Study Guide

? NIST SP 800-61 Rev. 2, "Computer Security Incident Handling Guide"

? SANS Institute, "Incident Handler's Handbook"

NEW QUESTION 37

An organization wants to manage specialized endpoints and needs a solution that provides the ability to

* Centrally manage configurations

* Push policies.

• Remotely wipe devices

- Maintain asset inventory

Which of the following should the organization do to best meet these requirements?

- A. Use a configuration management database
- B. Implement a mobile device management solution.
- C. Configure contextual policy management
- D. Deploy a software asset manager

Answer: B

Explanation:

To meet the requirements of centrally managing configurations, pushing policies, remotely wiping devices, and maintaining an asset inventory, the best solution is to implement a Mobile Device Management (MDM) solution.

MDM Capabilities:

- ? Central Management: MDM allows administrators to manage the configurations of all devices from a central console.
- ? Policy Enforcement: MDM solutions enable the push of security policies and updates to ensure compliance across all managed devices.
- ? Remote Wipe: In case a device is lost or stolen, MDM provides the capability to remotely wipe the device to protect sensitive data.
- ? Asset Inventory: MDM maintains an up-to-date inventory of all managed devices, including their configurations and installed applications.

Other options do not provide the same comprehensive capabilities required for managing specialized endpoints.

References:

- ? CompTIA SecurityX Study Guide
- ? NIST Special Publication 800-124 Revision 1, "Guidelines for Managing the Security of Mobile Devices in the Enterprise"
- ? "Mobile Device Management Overview," Gartner Research

NEW QUESTION 41

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:

- Unauthorized reading and modification of data and programs
- Bypassing application security mechanisms
- Privilege escalation
- 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

Answer: A

Explanation:

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:

NEW QUESTION 43

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 48

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 53

A security architect is establishing requirements to design resilience in an enterprise system. The system must be extended to other physical locations. 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 55

.....

Relate Links

100% Pass Your CAS-005 Exam with ExamBible Prep Materials

<https://www.exambible.com/CAS-005-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>