CS0-003 Q&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.geekcert.com/cs0-003.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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

A. Information sharing organization

B. Blogs/forums

C. Cybersecuritv incident response team

D. Deep/dark web

Correct Answer: A

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

QUESTION 2

A security analyst is supporting an embedded software team. Which of the following is the best recommendation to ensure proper error handling at runtime?

A. Perform static code analysis.

B. Require application fuzzing.

C. Enforce input validation.

D. Perform a code review.

Correct Answer: C

QUESTION 3

A security analyst responds to a series of events surrounding sporadic bandwidth consumption from an endpoint device. The security analyst then identifies the following additional details:

Bursts of network utilization occur approximately every seven days. The content being transferred appears to be encrypted or obfuscated. A separate but persistent outbound TCP connection from the host to infrastructure in a third-party

cloud is in place.

The HDD utilization on the device grows by 10GB to 12GB over the course of every seven days.

Single file sizes are 10GB.

Which of the following describes the most likely cause of the issue?

A. Memory consumption

B. Non-standard port usage

C. Data exfiltration

D. System update

E. Botnet participant

Correct Answer: C

data exfiltration is the unauthorized transfer of data from an " destination, usually for malicious purposes such as espionage, sabotage, or theft. The details given in the question suggest that data exfiltration is occurring from an endpoint device. The bursts of network utilization every seven days indicate periodic data transfers. The content being transferred appears to be encrypted or obfuscated to avoid detection or analysis. The persistent outbound TCP connection from the host to infrastructure in a third-party cloud indicates a possible command and control channel for an attacker. The HDD utilization on the device grows by 10GB to 12GB over the course of every seven days, and single file sizes are 10GB, indicating that large amounts of data are being collected and compressed before being exfiltrated.

QUESTION 4

A security analyst is trying to identify possible network addresses from different source networks belonging to the same company and region.

Which of the following shell script functions could help achieve the goal?

A. function x() { b=traceroute -m"" }

B. "u.com TXT +short }

C. function z() { c=$(geoip" }

Correct Answer: B

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

"u.com TXT +short }

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

QUESTION 5

A security analyst is logged on to a jump server to audit the system configuration and status. The organization\\'s policies for access to and configuration of the jump server include the following:

1.

No network access is allowed to the internet.

2.

SSH is only for management of the server.

3.

Users must utilize their own accounts, with no direct login as an administrator.

4.

Unnecessary services must be disabled.

The analyst runs netstar with elevated permissions and receives the following output: Which of the following policies does the server violate?

Active connections

Protocol	Local address	Foreign address	State
TCP	127.0.0.1:5357	VM-Windows-10:49229	TIME_WAIT
TCP	192.168.1.100	192.168.1.43	TIME_WAIT
TCP	192.168.1.100	security-updates.microsoft.com	ESTABLISHED
TCP	192.168.1.100	192.168.1.22	ESTABLISHED

A. Unnecessary services must be disabled.

B. SSH is only for management of the server.

C. No network access is allowed to the internet.

D. Users must utilize their own accounts, with no direct login as an administrator.

Correct Answer: C

The server violates the policy of no network access to the internet because it has an established connection to an external IP address (216.58.194.174) on port 443, which is used for HTTPS traffic. This indicates that the server is communicating with a web server on the internet, which is not allowed by the policy. The other policies are not violated because SSH is only used for management of the server (not for accessing other devices), users are utilizing their own accounts (not logging in as an administrator), and unnecessary services are not enabled (only SSH and HTTPS are running). CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 9; https://en.wikipedia.org/ wiki/Jump_server