CS0-002 Q&As

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-002 Exam with 100% Guarantee

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

https://www.pass4itsure.com/cs0-002.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

During a recent breach, an attacker was able to use tcpdump on a compromised Linux server to capture the password of a network administrator that logged into a switch using telnet.

Which of the following compensating controls could be implemented to address this going forward?

A. Whitelist tcpdump of Linux servers.

B. Change the network administrator password to a more complex one.

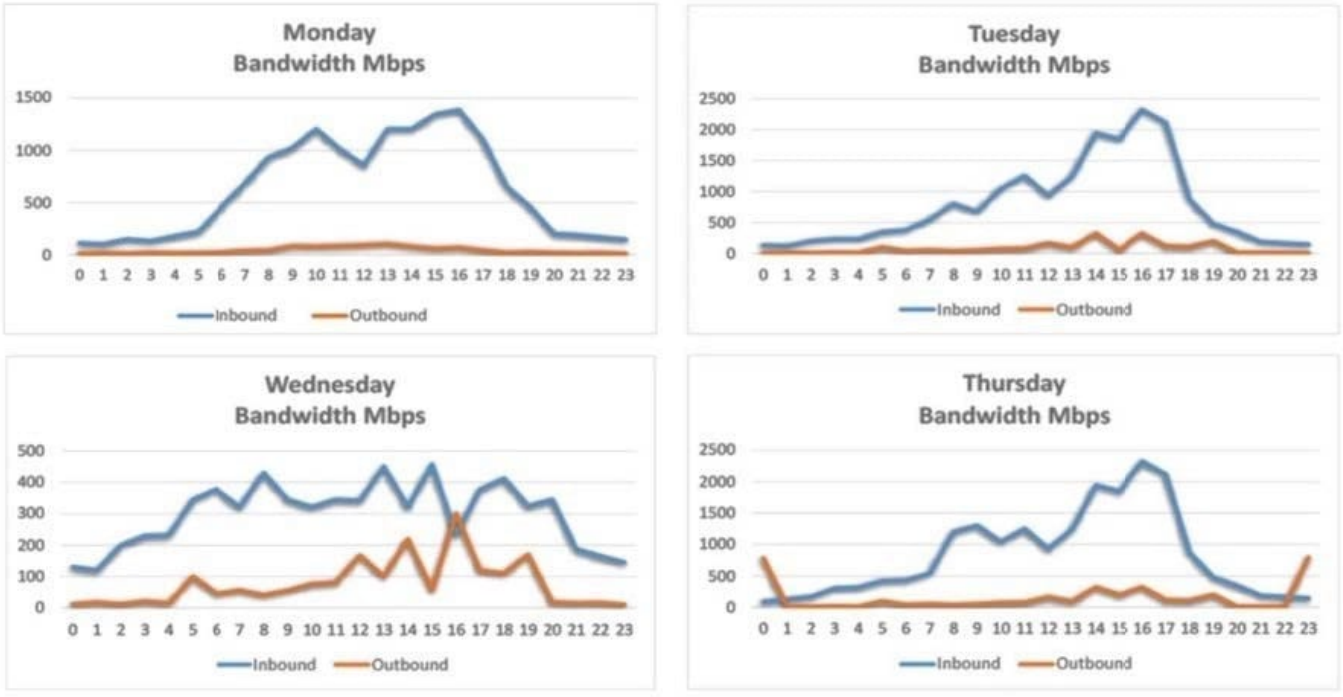
C. Implement separation of duties.

D. Require SSH on network devices.

Correct Answer: D

QUESTION 2

A security analyst is conducting a post-incident log analysis to determine which indicators can be used to detect further occurrences of a data exfiltration incident. The analyst determines backups were not performed during this time and reviews the following:



Which of the following should the analyst review to find out how the data was exfilltrated?

A. Monday\\'s logs

B. Tuesday\\'s logs

C. Wednesday\\'s logs

D. Thursday\\'s logs

Correct Answer: D

QUESTION 3

A forensics investigator is analyzing a compromised workstation. The investigator has cloned the hard drive and needs to verify that a bit-level image copy of a hard drive is an exact clone of the original hard drive that was collected as evidence. Which of the following should the investigator do?

A. Insert the hard drive on a test computer and boot the computer.

B. Record the serial numbers of both hard drives.

C. Compare the file-directory "sting of both hard drives.

D. Run a hash against the source and the destination.

Correct Answer: D

QUESTION 4

An incident responder successfully acquired application binaries off a mobile device for later forensic analysis. Which of the following should the analyst do NEXT?

A. Decompile each binary to derive the source code.

B. Perform a factory reset on the affected mobile device.

C. Compute SHA-256 hashes for each binary.

D. Encrypt the binaries using an authenticated AES-256 mode of operation.

E. Inspect the permissions manifests within each application.

Correct Answer: C

QUESTION 5

The Chief Executive Officer (CEO) instructed the new Chief Information Security Officer (CISO) to provide a list of enhancement to the company\\'s cybersecurity operation. As a result, the CISO has identified the need to align security operations with industry best practices. Which of the following industry references is appropriate to accomplish this?

A. OSSIM

B. NIST

C. PCI

D. OWASP

Correct Answer: B

Reference: https://www.nist.gov/sites/default/files/documents/itl/Cybersecurity_Green-Paper_FinalVersion.pdf

QUESTION 6

A security engineer must deploy X 509 certificates to two web servers behind a load balancer. Each web server is configured identically. Which of the following should be done to ensure certificate name mismatch errors do not occur?

A. Create two certificates, each with the same fully qualified domain name, and associate each with the web servers' real IP addresses on the load balancer.

B. Create one certificate on the load balancer and associate the site with the web servers' real IP addresses.

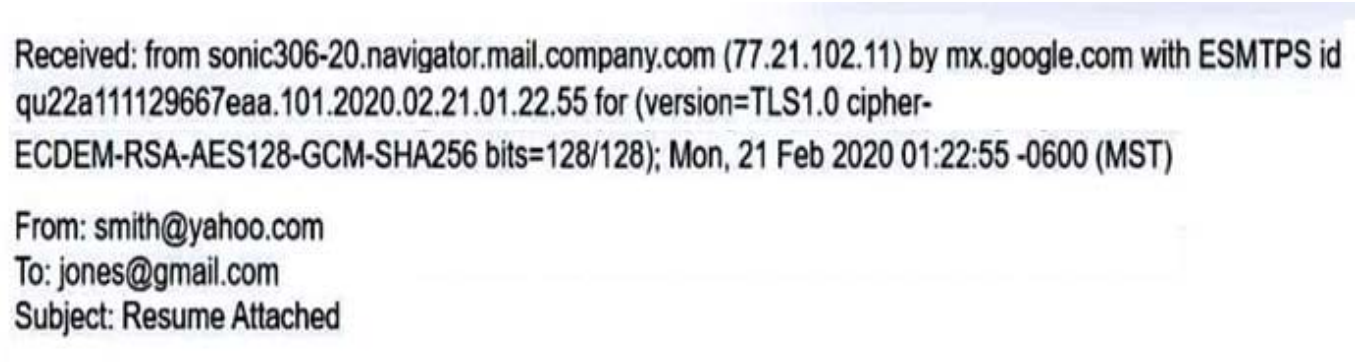
C. Create two certificates, each with the same fully qualified domain name, and associate each with a corresponding web server behind the load balancer.

D. Create one certificate and export it to each web server behind the load balancer.

Correct Answer: C

QUESTION 7

A security analyst inspects the header of an email that is presumed to be malicious and sees the following:



Which of the following is inconsistent with the rest of the header and should be treated as suspicious?

A. The subject line

B. The sender\\'s email address

C. The destination email server

D. The use of a TLS cipher

Correct Answer: B

QUESTION 8

An ATM in a building lobby has been compromised. A security technician has been advised that the ATM must be forensically analyzed by multiple technicians. Which of the following items in a forensic tool kit would likely be used FIRST? (Select TWO).

A. Drive adapters

B. Chain of custody form

C. Write blockers

D. Crime tape

E. Hashing utilities

F. Drive imager

Correct Answer: BC

QUESTION 9

A cybersecurity analyst is reading a daily intelligence digest of new vulnerabilities The type of vulnerability that should be disseminated FIRST is one that:

A. enables remote code execution that is being exploited in the wild.

B. enables data leakage but is not known to be m the environment

C. enables lateral movement and was reported as a proof of concept

D. affected the organization in the past but was probably contained and eradicated

Correct Answer: A

QUESTION 10

Which of the following commands would a security analyst use to make a copy of an image for forensics use?

A. dd

B. wget

C. touch

D. rm

Correct Answer: A

QUESTION 11

Which of the following BEST describes the primary role of a risk assessment as it relates to compliance with risk-based frameworks?

A. It demonstrated the organization\\'s mitigation of risks associated with internal threats.

B. It serves as the basis for control selection.

C. It prescribes technical control requirements.

D. It is an input to the business impact assessment.

Correct Answer: A

QUESTION 12

A business-critical application is unable to support the requirements in the current password policy because it does not allow the use of special characters. Management does not want to accept the risk of a possible security incident due to weak password standards. Which of the following is an appropriate means to limit the risks related to the application?

A. A compensating control

B. Altering the password policy

C. Creating new account management procedures

D. Encrypting authentication traffic

Correct Answer: D

QUESTION 13

A security analyst with an international response team is working to isolate a worldwide distribution of ransomware. The analyst is working with international governing bodies to distribute advanced intrusion detection routines for this variant of ransomware. Which of the following is the MOST important step with which the security analyst should comply?

A. Security operations privacy law

B. Export restrictions

C. Non-disclosure agreements

D. Incident response forms

Correct Answer: D

QUESTION 14

Which of the following attacks can be prevented by using output encoding?

A. Server-side request forgery

B. Cross-site scripting

C. SQL injection

D. Command injection

E. Cross-site request forgery

F. Directory traversal

Correct Answer: B

QUESTION 15

A security analyst is reviewing WAF logs and notes requests against the corporate website are increasing and starting to impact the performance of the web server. The security analyst queries the logs for requests that triggered an alert on the WAF but were not blocked.

Which of the following possible TTP combinations might warrant further investigation? (Select TWO).

A. Requests identified by a threat intelligence service with a bad reputation

B. Requests sent from the same IP address using different user agents

C. Requests blocked by the web server per the input sanitization

D. Failed log-in attempts against the web application

E. Requests sent by NICs with outdated firmware

F. Existence of HTTP/501 status codes generated to the same IP address

Correct Answer: BF