CS0-002$^{Q\&As}$

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-002 Exam with 100% Guarantee

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

QUESTION 1

An organization developed a comprehensive incident response policy. Executive management approved the policy and its associated procedures. Which of the following activities would be MOST beneficial to evaluate personnel\\'s familiarity with incident response procedures?

A. A simulated breach scenario involving the incident response team

B. Completion of annual information security awareness training by all employees

C. Tabletop activities involving business continuity team members

D. Completion of lessons-learned documentation by the computer security incident response team

E. External and internal penetration testing by a third party

Correct Answer: A

QUESTION 2

A company\\'s Chief Information Security Officer (CISO) is concerned about the integrity of some highly confidential files. Any changes to these files must be tied back to a specific authorized user\\'s activity session. Which of the following is the BEST technique to address the CISO\\'s concerns?

A. Configure DLP to reject all changes to the files without pre-authorization. Monitor the files for unauthorized changes.

B. Regularly use SHA-256 to hash the directory containing the sensitive information. Monitor the files for unauthorized changes.

C. Place a legal hold on the files. Require authorized users to abide by a strict time context access policy.Monitor the files for unauthorized changes.

D. Use Wireshark to scan all traffic to and from the directory. Monitor the files for unauthorized changes.

Correct Answer: A

QUESTION 3

A security analyst is building a malware analysis lab. The analyst wants to ensure malicious applications are not capable of escaping the virtual machines and pivoting to other networks. To BEST mitigate this risk, the analyst should use __________.

A. an 802.11ac wireless bridge to create an air gap.

B. a managed switch to segment the lab into a separate VLAN.

C. a firewall to isolate the lab network from all other networks.

D. an unmanaged switch to segment the environments from one another.

Correct Answer: C

QUESTION 4

A small organization has proprietary software that is used internally. The system has not been well maintained and cannot be updated with the rest of the environment Which of the following is the BEST solution?

A. Virtualize the system and decommission the physical machine.

B. Remove it from the network and require air gapping.

C. Only allow access to the system via a jumpbox

D. Implement MFA on the specific system.

Correct Answer: A

QUESTION 5

The inability to do remote updates of certificates. keys software and firmware is a security issue commonly associated with:

A. web servers on private networks.

B. HVAC control systems

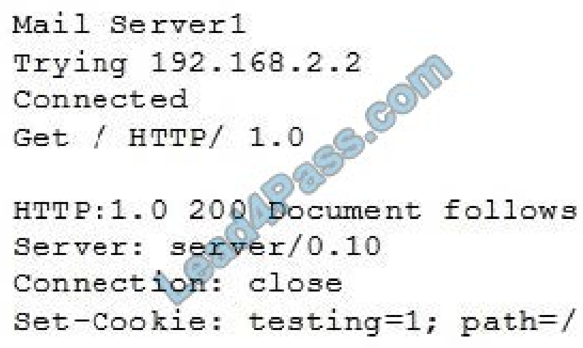
C. smartphones

D. firewalls and UTM devices

Correct Answer: B

QUESTION 6

A cybersecurity analyst is currently checking a newly deployed server that has an access control list applied. When conducting the scan, the analyst received the following code snippet of results:



```
Mail Server1
Trying 192.168.2.2
Connected
Get / HTTP/ 1.0

HTTP:1.0 200 Document follows
Server: server/0.10
Connection: close
Set-Cookie: testing=1; path=/
```

Which of the following describes the output of this scan?

A. The analyst has discovered a False Positive, and the status code is incorrect providing an OK message.

B. The analyst has discovered a True Positive, and the status code is correct providing a file not found error message.

C. The analyst has discovered a True Positive, and the status code is incorrect providing a forbidden message.

D. The analyst has discovered a False Positive, and the status code is incorrect providing a server error message.

Correct Answer: B

QUESTION 7

A company\\'s modem response team is handling a threat that was identified on the network Security analysts have as at remote sites. Which of the following is the MOST appropriate next step in the incident response plan?

A. Quarantine the web server

B. Deploy virtual firewalls

C. Capture a forensic image of the memory and disk

D. Enable web server containerization

Correct Answer: B

QUESTION 8

Which of the following software assessment methods would be BEST for gathering data related to an application\\'s availability during peak times?

A. Security regression testing

B. Stress testing

C. Static analysis testing

D. Dynamic analysis testing

E. User acceptance testing

Correct Answer: B

QUESTION 9

A malicious hacker wants to gather guest credentials on a hotel 802.11 network. Which of the following tools is the malicious hacker going to use to gain access to information found on the hotel network?

A. Nikto

B. Aircrak-ng

C. Nessus

D. tcpdump

Correct Answer: A

QUESTION 10

A security analyst is reviewing the following web server log:

GET %2f..%2f..%2f.. %2f.. %2f.. %2f.. %2f../etc/passwd

Which of the following BEST describes the issue?

A. Directory traversal exploit

B. Cross-site scripting

C. SQL injection

D. Cross-site request forgery

Correct Answer: A

QUESTION 11

A company\\'s senior human resources administrator left for another position, and the assistant administrator was promoted into the senior position. On the official start day, the new senior administrator planned to ask for extended access permissions but noticed the permissions were automatically granted on that day. Which of the following describes the access management policy in place at the company?

A. Mandatory-based

B. Host-based

C. Federated access

D. Role-based

Correct Answer: D

QUESTION 12

Which of the following should a database administrator implement to BEST protect data from an untrusted server administrator?

A. Data deidentification

B. Data encryption

C. Data masking

D. Data minimization

Correct Answer: B

QUESTION 13

Employees of a large financial company are continuously being Infected by strands of malware that are not detected by EDR tools. When of the following Is the BEST security control to implement to reduce corporate risk while allowing employees to exchange files at client sites?

A. MFA on the workstations

B. Additional host firewall rules

C. VDI environment

D. Hard drive encryption

E. Network access control

F. Network segmentation

Correct Answer: B

QUESTION 14

A security analyst is reviewing vulnerability scan results and notices new workstations are being flagged as having outdated antivirus signatures. The analyst observes the following plugin output:

Antivirus is installed on the remote host:

Installation path: C:\Program Files\AVProduct\Win32\

Product Engine: 14.12.101

Engine Version: 3.5.71

Scanner does not currently have information about AVProduct version 3.5.71. It may no longer be supported.

The engine version is out of date. The oldest supported version from the vendor is 4.2.11. The analyst uses the vendor\\'s website to confirm the oldest supported version is correct.

Which of the following BEST describes the situation?

A. This is a false positive, and the scanning plugin needs to be updated by the vendor.

B. This is a true negative, and the new computers have the correct version of the software.

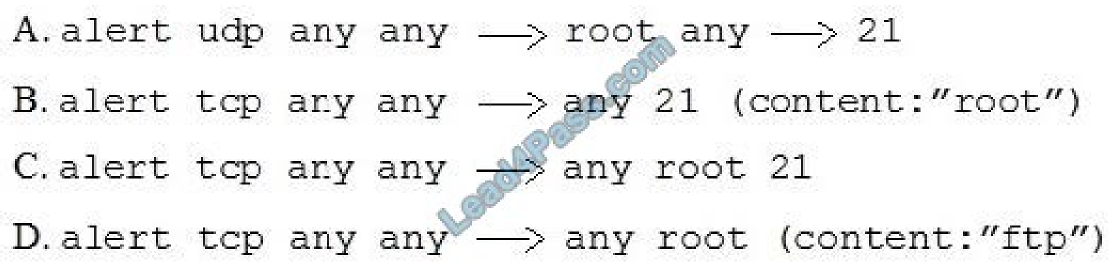
C. This is a true positive, and the new computers were imaged with an old version of the software.

D. This is a false negative, and the new computers need to be updated by the desktop team.

Correct Answer: C

QUESTION 15

A security administrator needs to create an IDS rule to alert on FTP login attempts by root. Which of the following rules is the BEST solution?



```
A.alert udp any any —> root any —> 21
B.alert tcp any any —> any 21 (content:"root")
C.alert tcp any any —> any root 21
D.alert tcp any any —> any root (content:"ftp")
```

A. Option A

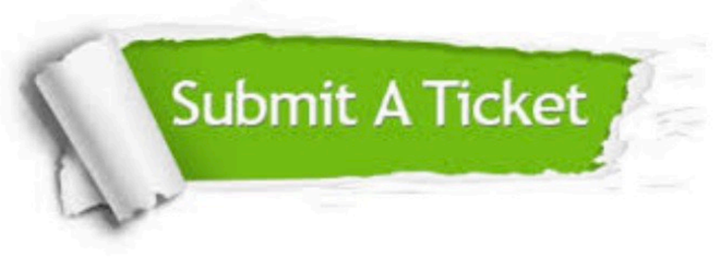
B. Option B

C. Option C

D. Option D

Correct Answer: B

CS0-002 PDF Dumps CS0-002 Exam Questions CS0-002 Braindumps


Submit A Ticket

100%