CS0-001 Q&As

CompTIA Cybersecurity Analyst

Pass CompTIA CS0-001 Exam with 100% Guarantee

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

https://www.pass4itsure.com/cs0-001.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A threat intelligence feed has posted an alert stating there is a critical vulnerability in the kernel. Unfortunately, the company\\'s asset inventory is not current. Which of the following techniques would a cybersecurity analyst perform to find all affected servers within an organization?

A. A manual log review from data sent to syslog

B. An OS fingerprinting scan across all hosts

C. A packet capture of data traversing the server network

D. A service discovery scan on the network

Correct Answer: B

QUESTION 2

A cybersecurity analyst is reviewing Apache logs on a web server and finds that some logs are missing. The analyst has identified that the systems administrator accidentally deleted some log files. Which of the following actions or rules should be implemented to prevent this incident from reoccurring?

A. Personnel training

B. Separation of duties

C. Mandatory vacation

D. Backup server

Correct Answer: D

QUESTION 3

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

QUESTION 4

An analyst is detecting Linux machines on a Windows network. Which of the following tools should be used to detect a computer operating system?

A. whois

B. netstat

C. nmap

D. nslookup

Correct Answer: C

QUESTION 5

In comparison to non-industrial IT vendors, ICS equipment vendors generally:

A. rely less on proprietary code in their hardware products.

B. have more mature software development models.

C. release software updates less frequently.

D. provide more expensive vulnerability reporting.

Correct Answer: A

QUESTION 6

A security analyst is performing ongoing scanning and continuous monitoring of the corporate datacenter. Over time, these scans are repeatedly showing susceptibility to the same vulnerabilities and an increase in new vulnerabilities on a specific group of servers that are clustered to run the same application. Which of the following vulnerability management processes should be implemented?

A. Frequent server scanning

B. Automated report generation

C. Group policy modification

D. Regular patch application

Correct Answer: D

QUESTION 7

A cybersecurity analyst is reviewing the current BYOD security posture. The users must be able to synchronize their calendars, email, and contacts to a smartphone or other personal device. The recommendation must provide the most flexibility to users. Which of the following recommendations would meet both the mobile data protection efforts and the business requirements described in this scenario?

A. Develop a minimum security baseline while restricting the type of data that can be accessed.

B. Implement a single computer configured with USB access and monitored by sensors.

C. Deploy a kiosk for synchronizing while using an access list of approved users.

D. Implement a wireless network configured for mobile device access and monitored by sensors.

Correct Answer: D

QUESTION 8

An analyst finds that unpatched servers have undetected vulnerabilities because the vulnerability scanner does not have the latest set of signatures. Management directed the security team to have personnel update the scanners with the latest signatures at least 24 hours before conducting any scans, but the outcome is unchanged. Which of the following is the BEST logical control to address the failure?

A. Configure a script to automatically update the scanning tool.

B. Manually validate that the existing update is being performed.

C. Test vulnerability remediation in a sandbox before deploying.

D. Configure vulnerability scans to run in credentialed mode.

Correct Answer: A

QUESTION 9

Nmap scan results on a set of IP addresses returned one or more lines beginning with "cpe:/o:" followed by a company name, product name, and version. Which of the following would this string help an administrator to identify?

A. Operating system

B. Running services

C. Installed software

D. Installed hardware

Correct Answer: A

QUESTION 10

When reviewing network traffic, a security analyst detects suspicious activity:

```
110 172.150.200.129 TCP    1140 > 443 [SYN] Seq=0 Win=15901 Len=0 MSS=1460 SACK_PERM=1
111 172.150.200.129 TCP    1140 > 443 [ACK] Seq=1 ACK=1 Win=15091 Len=0
112 172.150.200.129 SSLv2  Client Hello
113 172.150.200.129 TCP    [TCP Dup ACK 112#1] 1140 > 443 [ACK] Seq=81 ACK=1 Win=15091
114 172.150.200.129 SSLv2  [TCP Retransmission] Client Hello
115 172.150.200.129 TCP    [TCP Dup ACK 114#1] 1140 > 443 [ACK] Seq=81 ACK=1 Win=15091
120 172.150.200.129 TCP    [TCP Dup ACK 114#2] 1140 > 443 [ACK] Seq=81 ACK=1 Win=15091
122 172.150.200.129 SSLv2  [TCP Retransmission] Client Hello
```

Based on the log above, which of the following vulnerability attacks is occurring?

A. ShellShock

B. DROWN

C. Zeus

D. Heartbleed

E. POODLE

Correct Answer: E

QUESTION 11

During a routine review of firewall logs, an analyst identified that an IP address from the organization\\'s server subnet had been connecting during nighttime hours to a foreign IP address, and had been sending between 150 and 500 megabytes of data each time. This had been going on for approximately one week, and the affected server was taken offline for forensic review. Which of the following is MOST likely to drive up the incident\\'s impact assessment?

A. PII of company employees and customers was exfiltrated.

B. Raw financial information about the company was accessed.

C. Forensic review of the server required fall-back on a less efficient service.

D. IP addresses and other network-related configurations were exfiltrated.

E. The local root password for the affected server was compromised.

Correct Answer: A

QUESTION 12

A security analyst is creating baseline system images to remediate vulnerabilities found in different operating systems. Each image needs to be scanned before it is deployed. The security analyst must ensure the configurations match industry standard benchmarks and the process can be repeated frequently. Which of the following vulnerability options would BEST create the process requirements?

A. Utilizing an operating system SCAP plugin

B. Utilizing an authorized credential scan

C. Utilizing a non-credential scan

D. Utilizing a known malware plugin

Correct Answer: A

QUESTION 13

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 14

A company has a popular shopping cart website hosted geographically diverse locations. The company has started hosting static content on a content delivery network (CDN) to improve performance. The CDN provider has reported the company is occasionally sending attack traffic to other CDN-hosted targets.

Which of the following has MOST likely occurred?

A. The CDN provider has mistakenly performed a GeoIP mapping to the company.

B. The CDN provider has misclassified the network traffic as hostile.

C. A vulnerability scan has tuned to exclude web assets hosted by the CDN.

D. The company has been breached, and customer PII is being exfiltrated to the CDN.

Correct Answer: D

QUESTION 15

The security operations team is conducting a mock forensics investigation. Which of the following should be the FIRST action taken after seizing a compromised workstation?

A. Activate the escalation checklist

B. Implement the incident response plan

C. Analyze the forensic image

D. Perform evidence acquisition

Correct Answer: D

Reference: https://staff.washington.edu/dittrich/misc/forensics/