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

Which of the following stakeholders would need to be aware of an e-discovery notice received by the security office about an ongoing case within the manufacturing department?

A. Board of trustees

B. Human resources

C. Legal

D. Marketing

Correct Answer: C

QUESTION 2

A computer at a company was used to commit a crime. The system was seized and removed for further analysis. Which of the following is the purpose of labeling cables and connections when seizing the computer system?

A. To capture the system configuration as it was at the time it was removed

B. To maintain the chain of custody

C. To block any communication with the computer system from attack

D. To document the model, manufacturer, and type of cables connected

Correct Answer: A

QUESTION 3

An organization has a practice of running some administrative services on non-standard ports as a way of frustrating any attempts at reconnaissance. The output of the latest scan on host 192.168.1.13 is shown below:

```
Starting Nmap 4.67 (http://nmap.org) at 2011-11-03 18:32 EDT

Nmap scan report for 192.168.1.13

Host is up (0.00066s latency).

Not shown: 990 closed ports
PORT      STATE     SERVICE
23/tcp    open      ssh
111/tcp   open      rpcbind
139/tcp   open      netbios-ssn
1417/tcp  open      OpenSSH
3306/tcp  open      mysql

MAC Address:01:AA:FB:23:21:45

Nmap done: 1 IPaddress (1 host up) scanned in 4.22 seconds
```


Which of the following statements is true?

A. Running SSH on the Telnet port will now be sent across an unencrypted port.

B. Despite the results of the scan, the service running on port 23 is actually Telnet and not SSH, and creates an additional vulnerability

C. Running SSH on port 23 provides little additional security from running it on the standard port.

D. Remote SSH connections will automatically default to the standard SSH port.

E. The use of OpenSSH on its default secure port will supersede any other remote connection attempts.

Correct Answer: C

QUESTION 4

There have been several exploits to critical devices within the network. However, there is currently no process to perform vulnerability analysis.

Which of the following should the security analyst implement during production hours to identify critical threats and vulnerabilities?

A. Asset inventory of all critical devices

B. Vulnerability scanning frequency that does not interrupt workflow

C. Daily automated reports of exploited devices

D. Scanning of all types of data regardless of sensitivity levels

Correct Answer: B

QUESTION 5

A computer has been infected with a virus and is sending out a beacon to command and control server through an unknown service. Which of the following should a security technician implement to drop the traffic going to the command and control server and still be able to identify the infected host through firewall logs?

A. Sinkhole

B. Block ports and services

C. Patches

D. Endpoint security

Correct Answer: A

Reference: https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Configure-DNS-Sinkhole/ta-p/58891