



CompTIA CS0-003 Mock Exam

Shared by Emerson on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page



Question 1

Question Type: MultipleChoice

A security audit for unsecured network services was conducted, and the following output was generated:

```
#nmap --top-ports 7 192.29.0.5
```

PORT	STATE	SERVICE
21	closed	ftp
22	open	ssh
23	filtered	telnet
636	open	ldaps
1723	open	pptp
443	closed	https
3389	closed	ms-term-server

Which of the following services should the security team investigate further? (Select two).

Options:

- A- 21
- B- 22
- C- 23
- D- 636
- E- 1723
- F- 3389

Answer:

C, D

Explanation:

The output shows the results of a port scan, which is a technique used to identify open ports and services running on a network host. Port scanning can be used by attackers to discover potential vulnerabilities and exploit them, or by defenders to assess the security posture and configuration of their network devices.

The output lists six ports that are open on the target host, along with the service name and version associated with each port. The service name indicates the type of application or protocol that is using the port, while the version indicates the specific release or update of the service. The service name and version can provide useful information for both attackers and defenders, as they can reveal the capabilities, features, and weaknesses of the service.

Among the six ports listed, two are particularly risky and should be investigated further by the security team: port 23 and port 636.

Port 23 is used by Telnet, which is an old and insecure protocol for remote login and command execution. Telnet does not encrypt any data transmitted over the network, including usernames and passwords, which makes it vulnerable to eavesdropping, interception, and modification by attackers. Telnet also has many known vulnerabilities that can allow attackers to gain unauthorized access, execute arbitrary commands, or cause denial-of-service attacks on the target host.

Port 636 is used by LDAP over SSL/TLS (LDAPS), which is a protocol for accessing and modifying directory services over a secure connection. LDAPS encrypts the data exchanged between the client and the server using SSL/TLS certificates, which provide authentication, confidentiality, and integrity. However, LDAPS can also be vulnerable to attacks if the certificates are not properly configured, verified, or updated. For example, attackers can use self-signed or expired certificates to perform man-in-the-middle attacks, spoofing attacks, or certificate revocation attacks on LDAPS connections.

Therefore, the security team should investigate further why port 23 and port 636 are open on the target host, and what services are running on them. The security team should also consider disabling or replacing these services with more secure alternatives, such as SSH for port 23 and StartTLS for port 636.

Question 2

Question Type: MultipleChoice

A company's security team is updating a section of the reporting policy that pertains to inappropriate use of resources (e.g., an employee who installs cryptominers on workstations in the office). Besides the security team, which

of the following groups should the issue be escalated to first in order to comply with industry best practices?

Options:

A- Help desk

- B- Law enforcement
- C- Legal department
- D- Board member

Answer:

C

Explanation:

The correct answer is C. Legal department.

According to the CompTIA Cybersecurity Analyst (CySA+) certification exam objectives, one of the tasks for a security analyst is to "report and escalate security incidents to appropriate stakeholders and authorities" 1. This includes reporting any inappropriate use of resources, such as installing cryptominers on workstations, which may violate the company's policies and cause financial and reputational damage. The legal department is the most appropriate group to escalate this issue to first, as they can advise on the legal implications and actions that can be taken against the employee. The legal department can also coordinate with other groups, such as law enforcement, help desk, or board members, as needed. The other options are not the best choices to escalate the issue to first, as they may not have the authority or expertise to handle the situation properly.

Question 3

Question Type: MultipleChoice

A company is launching a new application in its internal network, where internal customers can communicate with the service desk. The security team needs to ensure the application will be able to handle unexpected strings with anomalous formats without crashing. Which of the following processes is the most applicable for testing the application to find how it would behave in such a situation?

Options:

- A- Fuzzing
- B- Coding review
- C- Debugging
- D- Static analysis

Answer:

A

Explanation:

Fuzzing is a process used to test applications by inputting unexpected or random data to see how the application behaves. This method is particularly effective in identifying vulnerabilities such as buffer overflows, input validation errors, and other anomalies that could cause the application to crash or behave unexpectedly. By using fuzzing, the security team can ensure the new application is robust and capable of handling unexpected strings with anomalous formats without crashing.



To Get Premium Files for CS0-003 Visit

<https://www.p2pexams.com/products/cs0-003>

For More Free Questions Visit

<https://www.p2pexams.com/comptia/pdf/cs0-003>

20%
DISCOUNT

P2P
exams