# SY0-501 Q&As

CompTIA Security+ Certification Exam

## Pass CompTIA SY0-501 Exam with 100% Guarantee

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

**https://www.passapply.com/sy0-501.html**

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

**QUESTION 1**

The Chief Information Officer (CIO) has heard concerns from the business and the help desk about frequent user account lockouts Which of the following account management practices should be modified to ease the burden?

A. Password complexity

B. Account disablement

C. False-rejection rate

D. Time-of-day restrictions

Correct Answer: A

**QUESTION 2**

A security program manager wants to actively test the security posture of a system. The system is not yet in production and has no uptime requirement or active user base. Which of the following methods will produce a report which shows vulnerabilities that were actually exploited?

A. Peer review

B. Component testing

C. Penetration testing

D. Vulnerability testing

Correct Answer: C

A penetration test, or pen test, is an attempt to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities.

**QUESTION 3**

An in-house penetration tester has been asked to evade a new DLP system. The tester plans to exfiltrate data through steganography. Discovery of which of the following would help catch the tester in the act?

A. Abnormally high numbers of outgoing instant messages that contain obfuscated text

B. Large-capacity USB drives on the tester\\'s desk with encrypted zip files

C. Outgoing emails containing unusually large image files

D. Unusual SFTP connections to a consumer IP address

Correct Answer: C

**QUESTION 4**

Which of the following is the MOST significant difference between intrusive and non-intrusive vulnerability scanning?

A. One uses credentials, but the other does not

B. One has a higher potential for disrupting system operations.

C. One allows systems to activate firewall countermeasures.

D. One returns service banners, including running versions

Correct Answer: B

**QUESTION 5**

A technician has been asked to document which services are running on each of a collection of 200 servers. Which of the following tools BEST meets this need while minimizing the work required?

A. Nmap

B. Nslookup

C. Netcat

D. Netstat

Correct Answer: A

**QUESTION 6**

A user has attempted to access data at a higher classification level than the user\\'s account is currently authorized to access. Which of the following access control models has been applied to this user\\'s account?

A. MAC

B. DAC

C. RBAC

D. ABAC

Correct Answer: A

**QUESTION 7**

A company wants to configure its wireless network to require username and password authentication. Which of the following should the systems administrator Implement?

A. WPS

B. PEAP

C. TKIP

D. PKI

Correct Answer: A

**QUESTION 8**

Which of the following attacks is used to capture the WPA2 handshake?

A. Replay

B. IV

C. Evil twin

D. Disassociation

Correct Answer: A

**QUESTION 9**

A security administrator is implementing a new WAF solution and has placed some of the web servers behind the WAF, with the WAF set to audit mode. When reviewing the audit logs of external requests and posts to the web servers, the administrator finds the following entry:

```
Context Details for Signature 20000018334
Context: Parameter
Actual Parameter Name: Account_Name
Parameter Value: SELECT * FROM Users WHERE Username='1' OR '1'='1' AND Password='1' OR '1'='1'
```

Based on this data, which of the following actions should the administrator take?

A. Alert the web server administrators to a misconfiguration.

B. Create a blocking policy based on the parameter values.

C. Change the parameter name `Account_Name\\' identified in the log.

D. Create an alert to generate emails for abnormally high activity.

Correct Answer: D

**QUESTION 10**

A network administrator wants to ensure that users do not connect any unauthorized devices to the company network. Each desk needs to connect a VoIP phone and computer. Which of the following is the BEST way to accomplish this?

A. Enforce authentication for network devices

B. Configure the phones on one VLAN, and computers on another

C. Enable and configure port channels

D. Make users sign an Acceptable use Agreement

Correct Answer: A

**QUESTION 11**

An administrator thinks the UNIX systems may be compromised, but a review of system log files provides no useful information. After discussing the situation with the security team, the administrator suspects that the attacker may be altering the log files and removing evidence of intrusion activity. Which of the following actions will help detect attacker attempts to further alter log files?

A. Enable verbose system logging

B. Change the permissions on the user\\'s home directory

C. Implement remote syslog

D. Set the bash_history log file to "read only"

Correct Answer: C

**QUESTION 12**

Which of the following are the MAIN reasons why a systems administrator would install security patches in a staging environment before the patches are applied to the production server? (Select two.)

A. To prevent server availability issues

B. To verify the appropriate patch is being installed

C. To generate a new baseline hash after patching

D. To allow users to test functionality

E. To ensure users are trained on new functionality

Correct Answer: AD