CompTIA

Exam SY0-401

CompTIA Security+ Certification

Version: Demo

[Total Questions: 10]

Topic break down

Topic	No. of Questions
Topic 1: Network Security	1
Topic 4: Application, Data and Host Security	1
Topic 5: Access Control and Identity Management	2
Topic 6: Cryptography	2
Topic 7: Mixed Questions	4

Topic 1, Network Security

Question No : 1 - (Topic 1)

A technician wants to securely collect network device configurations and statistics through a scheduled and automated process. Which of the following should be implemented if configuration integrity is most important and a credential compromise should not allow interactive logons?

A. SNMPv3
B. TFTP
C. SSH
D. TLS

Answer: A

Explanation:
SNMPv3 provides the following security features:
Message integrity--Ensures that a packet has not been tampered with in transit.
Authentication--Determines that the message is from a valid source.
Encryption--Scrambles the content of a packet to prevent it from being learned by an unauthorized source.

Topic 4, Application, Data and Host Security

Question No : 2 - (Topic 4)

An administrator finds that non-production servers are being frequently compromised, production servers are rebooting at unplanned times and kernel versions are several releases behind the version with all current security fixes.

Which of the following should the administrator implement?

A. Snapshots
B. Sandboxing
C. Patch management
D. Intrusion detection system

Answer: C

Explanation:
Patch management is the process of maintaining the latest source code for applications and operating systems by applying the latest vendor updates. This helps protect a systems from newly discovered attacks and vulnerabilities.

Topic 5, Access Control and Identity Management

Question No : 3 - (Topic 5)

Which of the following is an authentication method that can be secured by using SSL?

A. RADIUS
B. LDAP
C. TACACS+
D. Kerberos

Answer: B
Explanation:
With secure LDAP (LDAPS), all LDAP communications are encrypted with SSL/TLS

Question No : 4 - (Topic 5)

Which of the following security benefits would be gained by disabling a terminated user account rather than deleting it?

A. Retention of user keys
B. Increased logging on access attempts
C. Retention of user directories and files
D. Access to quarantined files

Answer: A
Explanation:
Account Disablement should be implemented when a user will be gone from a company whether they leave temporary or permanently. In the case of permanently leaving the company the account should be disabled. Disablement means that the account will no longer be an active account and that the user keys for that account are retained which

would not be the case if the account was deleted from the system.

Topic 6, Cryptography

Question No : 5 - (Topic 6)

Which of the following is true about the recovery agent?

A. It can decrypt messages of users who lost their private key.
B. It can recover both the private and public key of federated users.
C. It can recover and provide users with their lost or private key.
D. It can recover and provide users with their lost public key.

Answer: A

Explanation:

A key recovery agent is an entity that has the ability to recover a private key, key components, or plaintext messages as needed. Using the recovered key the recovery agent can decrypt encrypted data.

Question No : 6 - (Topic 6)

A company's security administrator wants to manage PKI for internal systems to help reduce costs. Which of the following is the FIRST step the security administrator should take?

A. Install a registration server.
B. Generate shared public and private keys.
C. Install a CA
D. Establish a key escrow policy.

Answer: C

Explanation:

PKI is a two-key, asymmetric system with four main components: certificate authority (CA), registration authority (RA), RSA (the encryption algorithm), and digital certificates. When you implement a PKI you should start by installing a CA.

Topic 7, Mixed Questions

Question No : 7 - (Topic 7)

An administrator wants to provide onboard hardware based cryptographic processing and secure key storage for full-disk encryption. Which of the following should the administrator use to fulfil the requirements?

A. AES
B. TPM
C. FDE
D. PAM

Answer: B

Question No : 8 - (Topic 7)

Which of the following is a proprietary protocol commonly used for router authentication across an enterprise?

A. SAML
B. TACACS
C. LDAP
D. RADIUS

Answer: B

Question No : 9 - (Topic 7)

While responding to an incident on a new Windows server, the administrator needs to disable unused services. Which of the following commands can be used to see processes that are listening on a TCP port?

A. IPCONFIG
B. Netstat

C. PSINFO
D. Net session

Answer: B

Question No : 10 - (Topic 7)

A user, Ann, has been issued a smart card and is having problems opening old encrypted email. Ann published her certificates to the local windows store and to the global address list. Which of the following would still need to be performed?

A. Setup the email security with her new certificates
B. Recover her old private certificate
C. Reinstall her previous public certificate
D. Verify the correct email address is associated with her certificate

Answer: A