

Exam : [CompTIA SY0-201](#)

Title : **CompTIA Security+(2008
Edition) Exam**

Version : **Demo**

1. Which of the following devices would be used to gain access to a secure network without affecting network connectivity?

- A. Router
- B. Vampire tap
- C. Firewall
- D. Fiber-optic splicer

Answer: B

2. A technician needs to ensure that all major software revisions have been installed on a critical network machine. Which of the following must they install to complete this task?

- A. HIDS
- B. Hotfixes
- C. Patches
- D. Service packs

Answer: D

3. Which of the following can increase risk? (Select TWO).

- A. Vulnerability
- B. Mantrap
- C. Configuration baselines
- D. Threat source
- E. Mandatory vacations

Answer: AD

4. Which of the following is the MOST secure way to encrypt traffic and authenticate users on a wireless network?

- A. WPA2 encryption using a RADIUS server
- B. WEP encryption using a pre-shared key (PSK)
- C. WEP encryption using a RADIUS server
- D. WPA2 encryption using a pre-shared key (PSK)

Answer: A

5. Which of the following is the MOST appropriate way to set permissions on the server log that records logins and logouts?

- A. Developers group full control
- B. Users group full control
- C. Power users group full control
- D. Security group full control

Answer: D

6. Which of the following is MOST likely to be an issue when turning on all auditing functions within a system?

- A. Flooding the network with all of the log information
- B. Lack of support for standardized log review tools
- C. Too much information to review
- D. Too many available log aggregation tools

Answer: C

7. Which of the following practices improves forensic analysis of logs?

- A. Ensuring encryption is deployed to critical systems.
- B. Ensuring SNMP is enabled on all systems.
- C. Ensuring switches have a strong management password.
- D. Ensuring the proper time is set on all systems.

Answer: D

8. A user reports that they cannot download an application from a website on the Internet. Which of the following logs is MOST likely to contain the cause of this problem?

- A. Application logs
- B. Antivirus logs
- C. Firewall logs

D. System logs

Answer: C

9. Which of the following methods assists in determining if user permissions are following the principle of least privilege?

A. Penetration test

B. User rights audit

C. Physical security assessment

D. Vulnerability assessment

Answer: B

10. Which of the following combinations of items would constitute a valid three factor authentication system?

A. Password, retina scan, and a one-time token

B. PIN, password, and a thumbprint

C. PKI smartcard, password and a one-time token

D. Fingerprint, retina scan, and a hardware PKI token

Answer: A

11. A user reports that after searching the Internet for office supplies and visiting one of the search engine results websites, they began receiving unsolicited pop-ups on subsequent website visits. Which of the following is the MOST likely cause of the unsolicited pop-ups?

A. Virus

B. Trojan

C. Adware

D. Spam

Answer: C

12. In a standard PKI implementation, which of the following keys is used to sign outgoing messages?

A. Senders private key

- B. Recipients public key
- C. Senders public key
- D. Recipients private key

Answer: A

13. AES and DES use which of the following encryption key types?

- A. Symmetric
- B. PGP
- C. Public key
- D. Asymmetric

Answer: A

14. A companys primary server is plugged into a power source that is not served by a UPS or backup generator. This is an example of a:

- A. disaster recovery exercise.
- B. redundant connections.
- C. single point of failure.
- D. cold site.

Answer: C

15. Which of the following should a technician deploy to detect malicious changes to the system and configuration?

- A. Pop-up blocker
- B. File integrity checker
- C. Anti-spyware
- D. Firewall

Answer: B

16. Which of the following logical access control methods would a security administrator need to modify in order to control network traffic passing through a router to a different network?

- A. Configuring VLAN 1
- B. ACL
- C. Logical tokens
- D. Role-based access control changes

Answer: B

17. Which of the following asymmetric algorithms was designed to provide both encryption and digital signatures?

- A. Diffie-Hellman
- B. DSA
- C. SHA
- D. RSA

Answer: D

18. Which of the following would be used to look for suspicious processes?

- A. System monitor
- B. Network mapper
- C. TACACS
- D. Protocol analyzer

Answer: A

19. Which of the following protocols is considered more secure than SSL?

- A. TLS
- B. WEP
- C. HTTP
- D. Telnet

Answer: A

20. Which of the following controls would require account passwords to be changed on a regular basis?

- A. Password complexity requirements

- B. Logical tokens
- C. Domain group policy
- D. Account expiration

Answer: C