

Exam : SY0-201

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

Version : DEMO

<http://www.test4actual.com>

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

21. Which of the following system security threats negatively affects confidentiality?

- A. Spam
- B. Adware
- C. Spyware
- D. Worm

Answer: C

22. Which of the following BEST describes how the private key is handled when connecting to a secure web server?

- A. The key is not shared and remains on the server
- B. Anyone who connects receives the key
- C. Only users from configured IP addresses received the key
- D. All authenticated users receive the key

Answer: A

23. Which of the following IPSec modes retains the original IP header for each packet?

- A. Transport
- B. Tunnel
- C. ESP
- D. AH

Answer: A

24. Which of the following uses a three-way-handshake for authentication and is commonly used in PPP connections?

- A. MD5
- B. CHAP
- C. Kerberos
- D. SLIP

Answer: B

25. Which of the following presents the GREATEST security risk to confidentiality of proprietary corporate data when attackers have physical access to the datacenter?

- A. Solid state drives
- B. Cell phone cameras
- C. USB drives
- D. NAS

Answer: C

26. Which of the following describes a false negative when using a scanning tool?

- A. Occurs when a scanning tool reports a vulnerability that does exist
- B. Occurs when a scanning tool reports a vulnerability that does not exist
- C. Occurs when a scanning tool does not report a vulnerability when they do exist
- D. Occurs when a scanning tool does not report a vulnerability when they do not exist

Answer: C

27. A technician sends out a ping request with an invalid MAC address to detect a rogue protocol analyzer on a network. Which of the following responses will the technician receive?

- A. An ICMP source quench (type 4)
- B. An ICMP reply (type 0)
- C. An ICMP redirect (type 5)
- D. An ICMP destination unreachable (type 3)

Answer: B

28. An administrator is explaining the conditions under which penetration testing is preferred over vulnerability testing.

Which of the following statements correctly describes these advantages?

- A. Identifies surface vulnerabilities and can be run on a regular basis
- B. Proves that the system can be compromised
- C. Safe for even inexperienced testers to conduct
- D. Can be fairly fast depending on number of hosts

Answer: B

29. All of the following requires a new baseline after new software is installed EXCEPT:

- A. anomaly-based NIDS.
- B. heuristic-based NIDS.
- C. signature-based NIDS.
- D. behavior-based NIDS.

Answer: C

30. Digital signatures can be created using which of the following functions?

- A. IPSec
- B. AES
- C. MD5
- D. TLS

Answer: C