

# T estpassport 考題



質 量 更 高 服 務 更 好

一年免費升級服務

[Http://www.testpassport.net](http://www.testpassport.net)

**Exam** : **SY0-201**

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

**Version** : **Demo**

1. Which of the following type of attacks requires an attacker to sniff the network?

- A. Man-in-the-Middle
- B. DDoS attack
- C. MAC flooding
- D. DNS poisoning

**Answer:** A

2. Which of the following should a technician recommend to prevent physical access to individual office areas? (Select TWO).

- A. Video surveillance
- B. Blockade
- C. Key card readers
- D. Mantrap
- E. Perimeter fence

**Answer:** CD

3. An administrator in a small office environment has implemented an IDS on the network perimeter to detect malicious traffic patterns. The administrator still has a concern about traffic inside the network originating between client workstations. Which of the following could be implemented?

- A. HIDS
- B. A VLAN
- C. A network router
- D. An access list

**Answer:** A

4. Which of the following algorithms have the smallest key space?

- A. IDEA
- B. SHA-1
- C. AES
- D. DES

**Answer: D**

5. A CEO is concerned about staff browsing inappropriate material on the Internet via HTTPS. It has been suggested that the company purchase a product which could decrypt the SSL session, scan the content and then repackage the SSL session without staff knowing. Which of the following type of attacks is similar to this product?

- A. Replay
- B. Spoofing
- C. TCP/IP hijacking
- D. Man-in-the-middle

**Answer: D**

6. Which of the following could BEST assist in the recovery of a crashed hard drive?

- A. Forensics software
- B. Drive optimization
- C. Drive sanitization
- D. Damage and loss control

**Answer: A**

7. A CRL contains a list of which of the following type of keys?

- A. Both public and private keys
- B. Steganographic keys
- C. Private keys
- D. Public keys

**Answer: A**

8. Which of the following BEST describes the form used while transferring evidence?

- A. Booking slip
- B. Affidavit
- C. Chain of custody

D. Evidence log

**Answer: C**

9. Which of the following type of attacks is TCP/IP hijacking?

A. Birthday

B. ARP poisoning

C. MAC flooding

D. Man-in-the-middle

**Answer: D**

10. The marketing department wants to distribute pens with embedded USB drives to clients. In the past this client has been victimized by social engineering attacks which led to a loss of sensitive data. The security administrator advises the marketing department not to distribute the USB pens due to which of the following?

A. The risks associated with the large capacity of USB drives and their concealable nature

B. The security costs associated with securing the USB drives over time

C. The cost associated with distributing a large volume of the USB pens

D. The security risks associated with combining USB drives and cell phones on a network

**Answer: A**

11. Which of the following are the functions of asymmetric keys?

A. Decrypt, decipher, encode and encrypt

B. Sign, validate, encrypt and verify

C. Decrypt, validate, encode and verify

D. Encrypt, sign, decrypt and verify

**Answer: D**

12. When deploying 50 new workstations on the network, which of following should be completed FIRST?

A. Install a word processor.

B. Run the latest spyware.

C. Apply the baseline configuration.

D. Run OS updates.

**Answer: C**

13. A corporation has a contractual obligation to provide a certain amount of system uptime to a client.

Which of the following is this contract an example of?

A. PII

B. SLA

C. Due diligence

D. Redundancy

**Answer: B**

14. Snort, TCPDump and Wireshark are commonly used for which of the following?

A. Port scanning

B. Host monitoring

C. DDoS attacks

D. Network sniffing

**Answer: D**

15. Which of the following BEST describes using a third party to store the public and private keys?

A. Public key infrastructure

B. Recovery agent

C. Key escrow

D. Registration authority

**Answer: C**

16. All of the following can be found in the document retention policy EXCEPT:

A. type of storage media.

B. password complexity rules.

C. physical access controls.

D. retention periods.

**Answer: B**

17. An instance where a biometric system identifies users that are authorized and allows them access is called which of the following?

A. False negative

B. True negative

C. False positive

D. True positive

**Answer: D**

18. Which of the following can be used to encrypt FTP or telnet credentials over the wire?

A. SSH

B. HTTPS

C. SHTTP

D. S/MIME

**Answer: A**

19. Classification of information is critical to information security because it:

A. defines what information should have the highest protection.

B. demonstrates that the company is using discretionary access control (DAC).

C. allows a company to share top secret information.

D. is a requirement for service level agreements (SLA).

**Answer: A**

20. A company takes orders exclusively over the Internet. Customers submit orders via a web-based application running on the external web server which is located on Network A. Warehouse employees use an internal application, on its own server, to pick and ship orders, located on Network B. Any changes made after the order is placed are handled by a customer service representative using the same internal application. All information is stored in a database, which is also located on Network B.

The company uses these four sets of user rights:

- NONE
- ADD (read existing data, write new data)
- CHANGE (read, write and change existing data)
- READ (read existing data)

The company has 2 different network zones:

- Network A, the DMZ, a public accessible network
- Network B, the internal LAN, accessible from company systems only

The company wants to restrict warehouse employee access. Which of the following permissions is the MOST appropriate for the warehouse employees?

- A. READ on Network B, NONE on Network A
- B. ADD on Network A, NONE on Network B
- C. CHANGE on Network A, ADD on Network B
- D. READ on Network A and B

**Answer: A**

21. Which of the following is the difference between identification and authentication of a user?

- A. Identification tells who the user is and authentication tells whether the user is allowed to logon to a system.
- B. Identification tells who the user is and authentication proves it.
- C. Identification proves who the user is and authentication is used to keep the users data secure.
- D. Identification proves who the user is and authentication tells the user what they are allowed to do.

**Answer: B**

22. An administrator wishes to deploy an IPSec VPN connection between two routers across a WAN. The administrator wants to ensure that the VPN is encrypted in the most secure fashion possible. Which of the following BEST identifies the correct IPSec mode and the proper configuration?

- A. IPSec in tunnel mode, using both the ESP and AH protocols
- B. IPSec in tunnel mode, using the ESP protocol
- C. IPSec in transport mode, using the AH protocol

D. IPSec in transport mode, using both ESP and AH protocols

**Answer: A**

23. Performance baselines are used to:

A. record which users type their passwords incorrectly.

B. demonstrate a man-in-the-middle attack.

C. indicate anomaly-based network attacks.

D. indicate the current presence of malicious code.

**Answer: D**

24. Which of the following is a reason that NAT would be implemented?

A. Subnetting

B. Address hiding

C. VLAN management

D. Network access control

**Answer: B**

25. While reviewing the firewall logs an administrator notices a number of unauthorized attempted connections from 10.x.x.x on an unused port. Which of the following is the correct procedure to follow when mitigating this risk?

A. Block the domain range \*.cn

B. Block the IP range 10.x.x.x/32

C. Block all traffic on that specific port

D. Block IP 10.x.x.x

**Answer: C**

26. Which of the following demonstrates the process of ensuring that both ends of the connection are in fact who they say they are?

A. Integrity

B. Identification

- C. Authentication
- D. Non-repudiation

**Answer: D**

27. Which of the following is commonly used in a distributed denial of service (DDoS) attack?

- A. Phishing
- B. Adware
- C. Botnet
- D. Trojan

**Answer: C**

28. Which of the following is a best practice for coding applications in a secure manner?

- A. Input validation
- B. Object oriented coding
- C. Rapid Application Development (RAD)
- D. Cross-site scripting

**Answer: A**

29. Which of the following logical access controls would be MOST appropriate to use when creating an account for a temporary worker?

- A. ACL
- B. Account expiration
- C. Time of day restrictions
- D. Logical tokens

**Answer: B**

30. Which of the following may be an indication of a possible system compromise?

- A. A port monitor utility shows that there are many connections to port 80 on the Internet facing web server.
- B. A performance monitor indicates a recent and ongoing drop in speed, disk space or memory utilization

from the baseline.

C. A protocol analyzer records a high number of UDP packets to a streaming media server on the Internet.

D. The certificate for one of the web servers has expired and transactions on that server begins to drop rapidly.

**Answer: B**