



**BestScoreSheet CompTIA Series Demo**

**CompTIA Security+ SY0-101**

Real exam questions & answers from testing centers

1. Pretty Good Privacy (PGP) uses a PKI Trust Model where no certificate authority (CA) is subordinate to another. The model with no single trusted root is known as:

- A. peer-to-peer.
- B. downlevel.
- C. hierarchical.
- D. hybrid.

Answer: A

2. Which of the following is a major reason that social engineering attacks succeed?

- A. Strong passwords are not required
- B. Lack of security awareness
- C. Multiple logins are allowed
- D. Audit logs are not monitored frequently

Answer: B

3. When setting password rules, which of the following would lower the level of security of a network?

- A. Passwords must be greater than six characters and contain at least one non-alpha.
- B. All passwords are set to expire at regular intervals and users are required to choose new passwords that have not been used before.
- C. Complex passwords that users can not remotely change are randomly generated by the administrator and given to users.
- D. After a set number of failed attempts the server will lock out any user account forcing the user to call the administrator to re-enable the account.

Answer: C

4. Which of the following protocols works with 802.1X to authenticate a client to a network?

- A. LDAP
- B. SPAP
- C. EAP
- D. CHAP

Answer: C

5. A person pretends to be a telecommunications repair technician, enters a building stating that there is a networking trouble work order and requests that a security guard unlock the wiring closet. The person connects a packet sniffer to the network switch in the wiring closet and hides the sniffer behind the switch against a wall.

This is an example of:

- A. a vulnerability scan.
- B. social engineering.
- C. a man in the middle attack.
- D. a penetration test.

Answer: B

6. Audit logs must contain which of the following characteristics?

- A. Authorization
- B. Confidentiality
- C. Non-repudiation
- D. Accessibility

Answer: C

7. A company's security specialist is securing a web server that is reachable from the Internet. The web server is located in the core internal corporate network. The network cannot be redesigned and the server cannot be moved. Which of the following should the security specialist implement to secure the web server? (Select TWO).

- A. Router with an IDS module
- B. Network-based IDS
- C. Router with firewall rule set
- D. Host-based IDS
- E. Network-based firewall
- F. Host-based firewall

Answer: DF

8. A company wants to connect the network to a manufacturer's network to be able to order parts. Which of the following types of networks should the company implement to provide the connection while limiting the services

allowed over the connection?

- A. Scatternet
- B. Extranet
- C. VPN
- D. Intranet

Answer: B

9. When building a forensics toolkit using freeware, which of the following tools would be used to make an image of a hard disk?

- A. bit torrent
- B. dd
- C. ntbackup
- D. tcpdump

Answer: B

10. Which of the following is important to ensure a high degree of trust that a transaction is not corrupted?

- A. Authorization
- B. Availability
- C. Confidentiality
- D. Integrity

Answer: D

11. Which of the following connectivity is required for a web server that is hosting an SSL based web site?

- A. Port 443 inbound
- B. Port 443 outbound
- C. Port 80 inbound
- D. Port 80 outbound

Answer: A

12. A URL for an Internet site begins with 'https:' rather than 'http:' which is an indication that this web site uses:

- A. Kerberos.

B. PGP.

C. PKI.

D. SSL.

Answer: D

13. The security of an encryption scheme depends on the secrecy of the:

A. algorithm.

B. software.

C. cipher text.

D. key.

Answer: D

14. A company conducts sensitive research and development and wants a strict environment for enforcing the principles of need to know, separation of duties, and least privilege. Which of the following should the company implement?

A. Single factor authentication

B. Mandatory Access Control (MAC)

C. Single sign on

D. Discretionary Access Control (DAC)

Answer: B

15. Which of the following would be an easy way to determine whether a secure web page has a valid certificate?

A. Right click on the lock at the bottom of the browser and check the certificate information.

B. Contact Thawte or Verisign and ask about the web page.

C. Contact the web page's web master.

D. Ensure that the web URL starts with 'https:\\' .

Answer: A

16. Which of the following describes an attacker encouraging a person to perform an action in order to be successful?

A. Man-in-the-middle

- B. Social engineering
- C. Back door
- D. Password guessing

Answer: B

17. Which of the following would be the BEST step to take to stop unauthorized users from targeting a wireless network with a site survey? (Select TWO).

- A. Physically locking the WAP.
- B. Disabling SSID broadcasting.
- C. Using a switch rather than a hub.
- D. Broadcasting a false domain name.
- E. Changing the default SSID.

Answer: BE

18. Which of the following would be the MOST important step to take to recognize suspicious activity within audit logs?

- A. Determine the usual activity.
- B. Synchronize server time with a time source.
- C. Eliminate unneeded event entries.
- D. Set event log overwrite and retention properties.

Answer: A

19. Which of the following types of encryption would be BEST to use for a large amount of data?

- A. Asymmetric
- B. Symmetric
- C. ROT13
- D. Hash

Answer: B

20. A workstation is being used as a zombie set to attack a web server on a certain date. The infected workstation is MOST likely part of a:

- A. DDoS attack.
- B. TCP/IP hijacking.
- C. spoofing attack.
- D. man-in-the-middle attack.

Answer: A