

Security + Practice Questions

- 1. From the list below, choose the events or scenarios that pose a security threat.**
 - a. The activities of authorized users performing their daily duties.
 - b. An exposed vulnerability on a system attached to the network.
 - c. An inexperienced attacker running pre-made scripts.
 - d. Authorized application services running on network servers.

- 2. Which of the following statements best describes a Trojan?**
 - a. A Trojan is a program that appears to be benign or a useful administrative utility but compromises a system's integrity.
 - b. A Trojan is a freestanding program that replicates itself to other systems and consumes resources on the system or the network and often causes disruption of services.
 - c. A Trojan is a computer program that requires user intervention and spreads by attaching itself to a document or executable.
 - d. A Trojan is a necessary protection for the system's integrity.

- 3. Equipment has been disappearing from the office. What security measures can be undertaken that would prevent this problem? Choose all that apply.**
 - a. Installation of CCTV systems.
 - b. Automated routine for installing security updates and hotfixes.
 - c. A security policy disallowing office equipment from being removed without authorization.
 - d. A Security policy that specifies all data on the network must be encrypted and stored encrypted, including the backups.

- 4. Which best describes a company's implementation of their trusted computing base?**
 - a. A trusted computing base is all of the security settings for a single computer.
 - b. A trusted computing base is an extension that should not be part of the security policy.
 - c. Threats to the trusted computing base should always be documented.
 - d. A trusted computing base is specified within a security policy and requires specific documentation of services and software on systems used within the network.

5. You wish to implement a security baseline for the systems and servers in the company. Which of the following would allow for the best administrative way to fulfill this requirement?

- a. Create security settings based on the users using the system and save as a security template.
- b. Create separate security settings based on the computers' role in the company and save as a series of templates. Implement the templates using automated tools and scripts.
- c. Create security settings for a single system that is based on the trusted computing base and create a single security template to be used throughout the company.
- d. Create security settings for each type of system and copy these settings to a file. Manually maintain these same settings on each of the designated types of systems.

6. Which of the following vulnerabilities can a security analyzer detect? Choose all that apply.

- a. Incorrect permission assignments on data files.
- b. Blank or weak passwords.
- c. Missing security patches and hotfixes.
- d. Services that are exposed on a system.

7. A company is concerned with physical security of the laptops used within the company. Which of the following procedures should be taken to ensure the security of the information on the laptops?

- a. When a laptop has been designated as unusable for the company, erase all data from the portable computer's hard disk and sell the computer.
- b. Only allow authorized access to all non-confidential data on the portable computer.
- c. Disallow all access to all confidential data on the portable computer.
- d. Create an encryption policy, and implement correct procedures for its use on the laptop.

8. You wish to implement the proper access controls to your company's resources. What would be the best administrative approach to determine the security settings for the resources?

- a. Implement an access control system that mirrors the significance of the resources that you are trying to protect.
- b. Require password access for each resource. The password should have a level of difficulty dependant upon the resources' security importance.
- c. Require a single password for access to all resources. Require the password to adhere to the specifications outlined in the security policy.
- d. Implement an access control system that enables you to specify the permissions and privileges to user accounts that users require to do their jobs as outlined in the security policy.

9. How should administrators logon to perform their daily work and administrative functions?

- a. All administrators should logon as ordinary users to perform their administrative functions.
- b. An administrator should only have one account for all access but always ensure the safety of the consoles she is logged on to by locking the console after each use.
- c. An administrator can always logon as an ordinary user, but run a separate logon within a session to perform administrative duties and close the session upon completion of the task.
- d. Require administrative access for user accounts for their local systems and only administrative access for network functions to specific administrators. This will minimize the necessity of the network administrator's logon to manage users' workstations.

10. What is the relationship between keys and algorithms in cryptography? Choose the correct answer.

- a. A key determines the type of algorithm that is used.
- b. An algorithm and a key must be kept secret to maintain cryptographic strength.
- c. The key is the mathematical formula that is used to encrypt text, and the algorithm is the decrypted text.
- d. The length of the key and the strength of the algorithm determine the strength of the cryptography used.
- e. The algorithm adds the key to plaintext and then encrypts the combination.

11. You must ensure the confidentiality and integrity of e-mail messages that you send over the Internet. Which of the following statements is true?

- a. You can provide only message confidentiality by using a hash function.
- b. You can provide only message integrity by using a hash function.
- c. You can provide both message confidentiality and message integrity by using a hash function.
- d. You can provide neither message confidentiality nor message integrity by using a hash function.

12. Should asymmetric encryption be used to encrypt large amount of data transferred between a client and a server?

- a. Yes, symmetric encryption should only be used in low security areas when necessary.
- b. Yes. Public key encryption is very efficient for large amounts of data.
- c. No. Key distribution is more secure for symmetric encryption than for asymmetric encryption.
- d. No. Public key encryption is very inefficient for large amounts of data.

13. You connect to a website that is using SSL. The web browser informs you that the web site's certificate has some problems. Upon inspection of the certificate, you discover that the certificate was issued to www.trainco.net and the website you are connecting to is https://www.trainco.com. Of the following, which statement can you be ensured if you continue communicating with this website?

- a. Information exchanged with this website will be in the clear.
- b. All information exchanged with this website will be in encrypted.
- c. You can be sure that the website you are connecting to is not trustworthy and has been cracked.
- d. You were originally communicating with www.trainco.com and were redirected to www.trainco.net.

14. What is included in a Certificate Revocation List?

- a. Certificates that have expired.
- b. Certificates that require renewal.
- c. Certificates that have been disabled before expiration.
- d. Certificates that have been disabled after expiration.

15. What are two widely used applications for cryptography.

- a. Accounting and Identification
- b. Accounting and Authorization
- c. Authentication and Encryption
- d. Authorizing and Identification

16. Accountability is the principle of tracing specific actions to _____.

- a. SID
- b. Specific Certificate
- c. Users
- d. Security Descriptors
- e. Groups

17. Which access control method uses data classifications and security labels of the resources to determine permission levels of the users?

- a. Discretionary Access Controls (DAC)
- b. Mandatory Access Controls (MAC)
- c. Role Based Access Controls (RBAC)
- d. List Based Access Controls (LBAC)

18. Three Canons of Information Security

- a. Confidentiality
- b. Integrity
- c. Authorization
- d. Encryption
- e. Availability
- f. Accountability

19. The primary tenets of User access to resources and provide tracking of activities of users:

- a. Privacy
- b. Integrity
- c. Authorization
- d. Authentication
- e. Encryption
- f. Accountability

20. Which type of an attack prevents a resource from being available to its intended and authorized users?

- a. Hijacking
- b. Brute Force
- c. Dictionary Attack
- d. Denial of Service

21. Access Controls that are administered by the data owners are known as

- a. Role Based Access Controls (RBAC)
- b. Mandatory Access Controls (MAC)
- c. Discretionary Access Controls (DAC)
- d. Authorization, Authentication, Accountability (AAA)

22. Choose 3 primary methods of user authentication.

- a. Cryptography
- b. Passwords
- c. Tokens
- d. Scanning
- e. Biometrics
- f. Encryption

23. Identifying suspicious activity and recording the attempts at compromising a system and network is known as _____.

- a. Accounting
- b. Auditing
- c. Intrusion Detection
- d. Authentication
- e. Integrity Checking

24. Which of the following provide single sign-on functionality?

- a. Workgroup Authentication
- b. RSA services
- c. Kerberos
- d. LDAP
- e. X.500

25. When a Biometric authentication system allows access to a resource to an unauthorized user, this is referred to as _____.

- a. False Negative
- b. True Positive
- c. True Negative
- d. False Positive

26. Which type of attack is characterized by traffic being intercepted by an individual and the client appears to be communicating with the server and the server appears to be communicating with the original client?

- a. Hijacking
- b. Denial of Service
- c. Tear Drop attack
- d. Syn Attack
- e. Man in the middle attack

27. Which of the following is a layer 3 VPN?

- a. L2TP
- b. PPTP
- c. IPSEC
- d. SSH
- e. Radius

Answers

1. B and C
2. A
3. A and C
4. D
5. B
6. B, C, and D
7. D
8. D
9. C
10. D
11. B
12. D
13. B
14. C
15. C
16. C
17. B
18. A, B, and E
19. C, D, and F
20. D
21. C
22. B, C, and E
23. C
24. C
25. D
26. E
27. C