

1. Of the following types of security, which would be primarily concerned with someone stealing the server from the premises?

- A.** Physical security
- B.** Operational security
- C.** Management and policy
- D.** Authentication

A. Physical security is primarily concerned with the loss or theft of physical assets. This would include theft, fire, and other acts that physically deny a service or information to the organization.

2. Upper management has suddenly become concerned about security. As the senior network administrator, you are asked to suggest changes that should be implemented. Which of the following access methods should you recommend if the method is to be one that is primarily based on preestablished access and can't be changed by users?

- A.** MAC
- B.** DAC
- C.** RBAC
- D.** Kerberos

A. Mandatory Access Control (MAC) is oriented toward preestablished access. This access is typically established by network administrators and can't be changed by users.

3. Your office administrator is being trained to perform server backups. Which authentication method would be ideal for this situation?

A. MAC

B. DAC

C. RBAC

D. Security tokens

C. Role Based Access Control (RBAC) allows specific people to be assigned to specific roles with specific privileges. A backup operator would need administrative privileges to back up a server. This privilege would be limited to the role and wouldn't be present during the employee's normal job functions.

4. You've been assigned to mentor a junior administrator and bring him up to speed quickly. The topic you're currently explaining is authentication. Which method uses a KDC to accomplish authentication for users, programs, or systems?

- A.** CHAP
- B.** Kerberos
- C.** Biometrics
- D.** Smart cards

B. Kerberos uses a Key Distribution Center to authenticate a principle. The KDC provides a credential that can be used by all Kerberos-enabled servers and applications.

5. Which authentication method sends a challenge to the client that is encrypted and then sent back to the server?

- A.** Kerberos
- B.** PAP
- C.** DAC
- D.** CHAP

D. Challenge Handshake Authentication Protocol (CHAP) sends a challenge to the originating client. This challenge is sent back to the server, and the encryption results are compared. If the challenge is successful, the client is logged on.

6. After a careful risk analysis, the value of your company's data has been increased. Accordingly, you're expected to implement authentication solutions that reflect the increased value of the data. Which of the following authentication methods uses more than one authentication process for a logon?

- A.** Multi-factor
- B.** Biometrics
- C.** Smart card
- D.** Kerberos

A. A multi-factor authentication process uses two or more processes for logon.
A two-factor method might use smart cards and biometrics for logon.

7. Which of the following services or protocols should be avoided in a network if possible in order to increase security?

- A.** E-mail
- B.** Telnet
- C.** WWW
- D.** ICMP

B. Telnet shouldn't be used if possible. Telnet sends user ID and password information to the Telnet server unencrypted. This creates a potential security problem in an Internet environment.

8. After acquiring another company, your organization is in a unique position to create a new— much larger—network from scratch. You want to take advantage of this reorganization to implement the most secure environment that users, and managers, can live with. You've already decided that the only way this will be possible is to implement security zones. Which of the following isn't an example of a type of security zone?

- A.** Internet
- B.** Intranet
- C.** Extranet
- D.** NAT

D. Network Address Translation (NAT) is a method of hiding TCP/IP addresses from other networks. The Internet, intranets, and extranets are the three most common security zones in use.

9. Which of the following protocols allows an organization to present a single TCP/IP address to the Internet while utilizing private IP addressing across the LAN?

- A.** NAT
- B.** VLAN
- C.** DMZ
- D.** Extranet

A. Network Address Translation (NAT) allows an organization to present a single address to the Internet. Typically, the router or NAT server accomplishes this. The router or NAT server maps all inbound and outbound requests and maintains a table for returned messages.

10. You're the administrator for Mercury Technical. Due to several expansions, the network has grown exponentially in size within the past two years. Which of the following is a popular method for breaking a network into smaller private networks that can coexist on the same wiring and yet be unaware of each other?

- A.** VLAN
- B.** NAT
- C.** MAC
- D.** Security zone

A. Virtual local area networks (VLANs) break a large network into smaller networks. These networks can coexist on the same wiring and be unaware of each other. A router or other routing type device would be needed to connect these VLANs together.

11. Of the following services, which one would be most likely to utilize a retinal scan?

- A.** Auditing
- B.** Authentication
- C.** Access control
- D.** Data confidentiality

B. Authentication is a service that requests the principal user to provide proof of their identity. A retinal scan is a very secure form of evidence used in high-security companies and government agencies.

12. One of the vice presidents of the company calls a meeting with information technology after a recent trip to competitors' sites. She reports that many of the companies she visited granted access to their buildings only after fingerprint scans, and she wants similar technology employed at this company. Of the following, which technology relies on a physical attribute of the user for authentication?

- A.** Smart card
- B.** Biometrics
- C.** Mutual authentication
- D.** Tokens

B. Biometric technologies rely on a physical characteristic of the user to verify identity. Biometric devices typically use either a hand pattern or a retinal scan to accomplish this.

13. Which technology allows a connection to be made between two networks using a secure protocol?

- A.** Tunneling
- B.** VLAN
- C.** Internet
- D.** Extranet

A. Tunneling allows a network to make a secure connection to another network through the Internet or other network. Tunnels are usually secure and present themselves as extensions of both networks.

14. A new director of information technology has been hired and you report directly to him. At the first meeting, he assigns you the task of identifying all the company resources that IT is responsible for and assigning a value to each. The process of determining the value of information or equipment in an organization is referred to as which of the following?

- A.** Asset identification
- B.** Risk assessment
- C.** Threat identification
- D.** Vulnerabilities scan

A. Asset identification is the process of identifying the types and values of assets in an organization.

15. You have been asked to address a management meeting and present the types of threats your organization could face from hackers. Which of the following would best categorize this type of information?

- A.** Asset identification
- B.** Risk assessment
- C.** Threat identification
- D.** Vulnerabilities

C. A threat assessment examines the potential for internal and external threats to your systems and information.

16. Over the years, your company has upgraded its operating systems and networks as it has grown. A recent survey shows that numerous databases on the network haven't been accessed in more than a year. Unfortunately, the survey doesn't identify who created or last accessed those databases. What is the process of determining who owns a particular database file called?

- A.** Auditing
- B.** Access control
- C.** Threat analysis
- D.** Accountability

D. Accountability identifies who owns or is responsible for the accuracy of certain information in an organization. The department or individual that is accountable for certain information would also be responsible for verifying accuracy in the event of a data-tampering incident.

17. A user just complained to you that his system has been infected with a new virus. Which of the following would be a first step to take in addressing and correcting this problem?

- A.** Verifying the most current virus definition file is installed
- B.** Reformatting the hard disk
- C.** Reinstalling the operating system
- D.** Disabling the user's e-mail account

A. Your first step would be to verify that the user's antivirus software is the most current version. This includes checking the virus definition files.

18. You're awakened in the middle of the night by a frantic junior administrator. The caller reports that the guest account—which you have forbidden anyone to use—suddenly logged in and out of the network, and the administrator believes an attack occurred. Which of the following would be the most useful in determining what was accessed during an external attack?

- A.** System logs
- B.** Antivirus software
- C.** Kerberos
- D.** Biometrics

A. System logs will frequently tell you what was accessed and in what manner. These logs are usually explicit in describing the events that occurred during a security violation.

19. You want to install a server in the network area that provides web services to Internet clients. You don't want to expose your internal network to additional risks. Which method should you implement to accomplish this?

- A.** Install the server in an intranet.
- B.** Install the server in a DMZ.
- C.** Install the server in a VLAN.
- D.** Install the server in an extranet.

B. A DMZ is an area in a network that allows access to outside users while not exposing your internal users to additional threats.

20. Your company provides medical data to doctors from a worldwide database. Because of the sensitive nature of the data you work with, it's imperative that authentication be established on each session and be valid only for that session. Which of the following authentication methods provides credentials that are valid only during a single session?

- A.** Tokens
- B.** Certificate
- C.** Smart card
- D.** Kerberos

A. Tokens are created when a user or system successfully authenticates. The token is destroyed when the session is over.