GIAC

GISP Exam

GIAC Information Security Professional

[Questions & Answers Demo]

Version: 5.0

Question: 1

Which of the following is a technique used to attack an Ethernet wired or wireless network?

A. DNS poisoning
B. Keystroke logging
C. Mail bombing
D. ARP poisoning

Answer: D

Question: 2

Which of the following refers to encrypted text?

A. Plaintext
B. Cookies
C. Hypertext
D. Ciphertext

Answer: D

Question: 3

Which of the following are the benefits of information classification for an organization?

A. It helps identify which information is the most sensitive or vital to an organization.
B. It ensures that modifications are not made to data by unauthorized personnel or processes.
C. It helps identify which protections apply to which information.
D. It helps reduce the Total Cost of Ownership (TCO).

Answer: A,C

Question: 4

Mark works as a Network Administrator for NetTech Inc. He wants users to access only those resources that are required for them. Which of the following access control models will he use?

A. Role-Based Access Control
B. Discretionary Access Control

C. Mandatory Access Control
D. Policy Access Control

Answer: A

Question: 5

Which of the following are methods used for authentication?
Each correct answer represents a complete solution. Choose all that apply.

A. Smart card
B. Biometrics
C. Username and password
D. Magnetic stripe card

Answer: A,B,C,D

Question: 6

Which of the following protocols is used to verify the status of a certificate?

A. CEP
B. HTTP
C. OSPF
D. OCSP

Answer: D

Question: 7

Fill in the blank with the appropriate value.
Service Set Identifiers (SSIDs) are case sensitive text strings that have a maximum length of_____ characters.

A. 32

Answer: A

Question: 8

You work as a Network Administrator for NetTech Inc. The company has a network that consists of 200 client computers and ten database servers. One morning, you find that a hacker is accessing unauthorized data on a database server on the network. Which of the following actions will you take to preserve the evidences?
Each correct answer represents a complete solution. Choose three.

A. Prevent a forensics experts team from entering the server room.
B. Preserve the log files for a forensics expert.
C. Prevent the company employees from entering the server room.
D. Detach the network cable from the database server.

Answer: B,C,D

Question: 9

Which of the following heights of fence deters only casual trespassers?

A. 3 to 4 feet
B. 2 to 2.5 feet
C. 8 feet
D. 6 to 7 feet

Answer: A

Question: 10

Which of the following statements about role-based access control (RBAC) model is true?

A. In this model, a user can access resources according to his role in the organization.
B. In this model, the permissions are uniquely assigned to each user account.
C. In this model, the same permission is assigned to each user account.
D. In this model, the users can access resources according to their seniority.

Answer: A

Question: 11

Which of the following statements about a fiber-optic cable are true?
Each correct answer represents a complete solution. Choose three.

A. It is immune to electromagnetic interference (EMI).
B. It can transmit undistorted signals over great distances.
C. It has eight wires twisted into four pairs.
D. It uses light pulses for signal transmission.

Answer: A,B,D

Question: 12

Which of the following statements about the bridge are true?
Each correct answer represents a complete solution. Choose two.

A. It filters traffic based on IP addresses.
B. It forwards broadcast packets.
C. It assigns a different network address per port.
D. It filters traffic based on MAC addresses.

Answer: B,D

Question: 13

Sam works as a Web Developer for McRobert Inc. He wants to control the way in which a Web browser receives information and downloads content from Web sites. Which of the following browser settings will Sam use to accomplish this?

A. Proxy server
B. Security
C. Cookies
D. Certificate

Answer: B

Question: 14

Which of the following are used to suppress paper or wood fires?
Each correct answer represents a complete solution. Choose two.

A. Water
B. Kerosene
C. CO2
D. Soda acid

Answer: A,D

Question: 15

Which of the following steps can be taken to protect laptops and data they hold?
Each correct answer represents a complete solution. Choose all that apply.

A. Use slot locks with cable to connect the laptop to a stationary object.

B. Keep inventory of all laptops including serial numbers.
C. Harden the operating system.
D. Encrypt all sensitive data.

Answer: A,B,C,D

Question: 16

Which of the following attacks involves multiple compromised systems to attack a single target?

A. Brute force attack
B. DDoS attack
C. Dictionary attack
D. Replay attack

Answer: B

Question: 17

Which of the following statements about DMZ are true?
Each correct answer represents a complete solution. Choose two.

A. It is an anti-virus software that scans the incoming traffic on an internal network.
B. It is the boundary between the Internet and a private network.
C. It contains company resources that are available on the Internet, such as Web servers and FTP servers.
D. It contains an access control list (ACL).

Answer: B,C

Question: 18

Which of the following protocols is used to establish a secure TELNET session over TCP/IP?

A. SSL
B. PGP
C. IPSEC
D. SSH

Answer: D

Question: 19

Which methods help you to recover your data in the event of a system or hard disk failure?
Each correct answer represents a complete solution. Choose two.

A. Install a RAID system
B. Use data encryption
C. Install and use a tape backup unit
D. Install UPS systems on all important devices

Answer: A,C

Question: 20

When no anomaly is present in an Intrusion Detection, but an alarm is generated, the response is known as _____.

A. False positive
B. False negative
C. True negative
D. True positive

Answer: A

Question: 21

Which of the following statements about smurf is true?

A. It is an ICMP attack that involves spoofing and flooding.
B. It is a UDP attack that involves spoofing and flooding.
C. It is a denial of service (DoS) attack that leaves TCP ports open.
D. It is an attack with IP fragments that cannot be reassembled.

Answer: A

Question: 22

Which of the following policies is set by a network administrator to allow users to keep their emails and documents for a fixed period of time?

A. Retention policy
B. Password policy
C. Audit policy
D. Backup policy

Answer: A

Question: 23

Which of the following statements about Switched Multimegabit Data Service (SMDS) are true? Each correct answer represents a complete solution. Choose two.

A. It is a logical connection between two devices.
B. It uses fixed-length (53-byte) packets to transmit information.
C. It supports speeds of 1.544 Mbps over Digital Signal level 1 (DS-1) transmission facilities.
D. It is a high-speed WAN networking technology used for communication over public data networks

Answer: C,D

Question: 24

Which of the following terms refers to the protection of data against unauthorized access?

A. Auditing
B. Recovery
C. Confidentiality
D. Integrity

Answer: C

Question: 25

Which of the following is a remote access protocol that supports encryption?

A. PPP
B. SNMP
C. UDP
D. SLIP

Answer: A

Question: 26

Which of the following is the best way of protecting important data against virus attack?

A. Updating the anti-virus software regularly.
B. Taking daily backup of data.
C. Using strong passwords to log on to the network.
D. Implementing a firewall.

Answer: A

Question: 27

Which of the following functions are performed by a firewall?
Each correct answer represents a complete solution. Choose all that apply.

A. It hides vulnerable computers that are exposed to the Internet.
B. It logs traffic to and from the private network.
C. It enhances security through various methods, including packet filtering, circuit-level filtering, and application filtering.
D. It blocks unwanted traffic.

Answer: A,B,C,D

Question: 28

Which of the following statements about Digest authentication are true?
Each correct answer represents a complete solution. Choose two.

A. In Digest authentication, passwords are sent across a network as clear text, rather than as a has value.
B. Digest authentication is used by wireless LANs, which follow the IEEE 802.11 standard.
C. In Digest authentication, passwords are sent across a network as a hash value, rather than as clear text.
D. Digest authentication is a more secure authentication method as compared to Basic authentication.

Answer: C,D

Question: 29

Which of the following types of attacks slows down or stops a server by overloading it with requests?

A. Vulnerability attack
B. Impersonation attack
C. Network attack
D. DoS attack

Answer: D

Question: 30

Which of the following is the most secure authentication method?

A. Certificate-based authentication
B. Basic authentication
C. Digest authentication
D. Integrated Windows authentication

Answer: A

Question: 31

Which of the following practices come in the category of denial of service attack?
Each correct answer represents a complete solution. Choose three.

A. Sending lots of ICMP packets to an IP address
B. Disrupting services to a specific computer
C. Performing Back door attack on a system
D. Sending thousands of malformed packets to a network for bandwidth consumption

Answer: A,B,D

Question: 32

What does the Internet encryption and authentication system named RSA stand for?

A. Rivest-Shamir-Adleman
B. Read System Authority
C. Rivest-System-Adleman
D. Remote System Authority

Answer: A

Question: 33

Which of the following authentication methods support mutual authentication?
Each correct answer represents a complete solution. Choose two.

A. MS-CHAP v2
B. EAP-TLS
C. EAP-MD5
D. NTLM

Answer: A,B

Question: 34

Fill in the blank with the appropriate layer name.
The Network layer of the OSI model corresponds to the _____ layer of the TCP/IP model.

A. Internet

Answer: A

Question: 35

Which of the following are the application layer protocols for security?
Each correct answer represents a complete solution. Choose three.

A. Secure Hypertext Transfer Protocol (S-HTTP)
B. Secure Sockets Layer (SSL)
C. Secure Electronic Transaction (SET)
D. Secure Shell (SSH)

Answer: A,C,D