GIAC

Exam GISP

GIAC Information Security Professional

Version: 6.0

[Total Questions: 659]

Topic break down

Topic	No. of Questions
Topic 1: Volume A	149
Topic 2: Volume B	144
Topic 3: Volume C	149
Topic 4: Volume D	98
Topic 5: Volume E	119

Topic 1, Volume A

Question No : 1 - (Topic 1)

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 No : 2 - (Topic 1)

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 No : 3 - (Topic 1)

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 No : 4 - (Topic 1)

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 No : 5 - (Topic 1)

Which of the following languages enable programmers to store *cookies* on client computers?

Each correct answer represents a complete solution. Choose two.

A. Perl
B. DHTML
C. JavaScript
D. HTML

Answer: A,C

Question No : 6 - (Topic 1)

Which of the following type of errors occurs when a legitimate user incorrectly denied access to resources by the Biometrics authentication systems?

A. Type II
B. Type I
C. Type III
D. Type IV

Answer: B

Question No : 7 - (Topic 1)

Which of the following statements about *extranet* are true?

Each correct answer represents a complete solution. Choose two.

A. It is an area of a company's Web site, which is only available to selected customers, suppliers, an business partners.
B. It is an area of a company's Web site, which is available to Internet users.
C. It is an arrangement commonly used for business-to-business relationships.
D. It is an arrangement commonly used for a company's employees.

Answer: A,C

Question No : 8 - (Topic 1)

Which of the following statement about *eavesdropping* is true?

A. It is a type of password guessing attack.
B. It is a way of preventing electronic emissions that are generated from a computer or network.
C. It is known as network saturation attack or bandwidth consumption attack.
D. It is the process of hearing or listening in private conversations.

Answer: D

Question No : 9 - (Topic 1)

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

Question No : 10 - (Topic 1)

Which of the following layers of the OSI model provides end-to-end service?

A. The physical layer
B. The application layer
C. The session layer
D. The transport layer

Answer: D

Question No : 11 - (Topic 1)

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 No : 12 - (Topic 1)

Which of the following protocols is built in the Web server and browser to encrypt data traveling over the Internet?

A. UDP
B. HTTP
C. SSL
D. IPSec

Answer: C

Question No : 13 - (Topic 1)

You work as a Network Administrator for NetTech Inc. The company's network has a Windows 2000 domain-based network. You want to prevent malicious e-mails from entering the network from the non-existing domains. What will you do to accomplish this?

A. Disable DNS recursive queries on the DNS server.
B. Enable DNS recursive queries on the DNS server.
C. Enable DNS reverse lookup on the e-mail server.
D. Disable DNS reverse lookup on the e-mail server.

Answer: C

Question No : 14 - (Topic 1)

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 No : 15 - (Topic 1)

Which of the following entities is used by Routers and firewalls to determine which packets should be forwarded or dropped?

A. Rainbow table
B. Rootkit
C. Access control list
D. Backdoor

Answer: C

Question No : 16 - (Topic 1)

You work as a Network Administrator of a TCP/IP network. You are having *DNS* resolution problem. Which of the following utilities will you use to diagnose the problem?

A. NSLOOKUP
B. IPCONFIG
C. PING
D. TRACERT

Answer: A

Question No : 17 - (Topic 1)

Which of the following are used to suppress gasoline and oil fires?

Each correct answer represents a complete solution. Choose three.

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

Answer: B,C,D

Question No : 18 - (Topic 1)

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 No : 19 - (Topic 1)

Which of the following is used to implement a procedure to control inbound and outbound traffic on a network?

A. Sam Spade
B. NIDS
C. ACL
D. Cookies

Answer: C

Question No : 20 - (Topic 1)

Which of the following types of attacks is only intended to make a computer resource unavailable to its users?

A. Teardrop attack
B. Denial of Service attack
C. Land attack
D. Replay attack

Answer: B

Question No : 21 - (Topic 1)

Which of the following statements about *Diffie-Hellman encryption* are true?

Each correct answer represents a complete solution. Choose two.

A. It uses only a private key.
B. It uses both a public key and a private key.
C. It does not authenticate the parties involved.
D. It was developed in 1976.

Answer: B,D

Question No : 22 - (Topic 1)

Which of the following can be prevented by an organization using job rotation and separation of duties policies?

A. Collusion
B. Eavesdropping
C. Buffer overflow
D. Phishing

Answer: A

Question No : 23 - (Topic 1)

Which of the following terms is used for securing an operating system from an attack?

A. System hacking
B. System hardening
C. System mirroring
D. System indexing

Answer: B

Question No : 24 - (Topic 1)

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 No : 25 - (Topic 1)

Which of the following processes is known as *sanitization*?

A. Physically destroying the media and the information stored on it.
B. Assessing the risk involved in discarding particular information.
C. Verifying the identity of a person, network host, or system process.
D. Removing the content from the media so that it is difficult to restore.

Answer: D

Question No : 26 - (Topic 1)

Mark works as a Network Administrator for NetTech Inc. The company has a Windows 2003 domainbased network. The company has two offices in different cities. The offices are connected through the Internet. Both offices have a Windows 2003 server named SERV1 and SERV2 respectively. Mark is required to create a secure connection between both offices. He configures a VPN connection between the offices using the two servers. He uses L2TP for VPN and also configures an IPSec tunnel. Which of the following will he achieve with this configuration?

Each correct answer represents a part of the solution. Choose two.

A. Highest possible encryption for traffic between the offices
B. Encryption for the local files stored on the two servers
C. Extra bandwidth on the Internet connection
D. Mutual authentication between the two servers

Answer: A,D

Question No : 27 - (Topic 1)

Which of the following refers to a condition in which a hacker sends a bunch of packets that leave *TCP ports* half open?

A. Spoofing
B. PING attack
C. SYN attack
D. Hacking

Answer: C

Question No : 28 - (Topic 1)

Which of the following statements about *Discretionary Access Control List (DACL)* is true?

A. It is a rule list containing access control entries.
B. It specifies whether an audit activity should be performed when an object attempts to access a resource.
C. It is a list containing user accounts, groups, and computers that are allowed (or denied) access to the object.
D. It is a unique number that identifies a user, group, and computer account.

Answer: C

Question No : 29 - (Topic 1)

Mark works as a Network Administrator for NetTech Inc. The company has a Windows 2000 domain-based network. Users report that they are unable to log on to the network. Mark finds that accounts are locked out due to multiple incorrect log on attempts. What is the most likely cause of the account lockouts?

A. SYN attack
B. Spoofing
C. PING attack
D. Brute force attack

Answer: D

Question No : 30 - (Topic 1)

Which of the following statements about a *host-based intrusion prevention system (HIPS)* are true?

Each correct answer represents a complete solution. Choose two.

A. It can detect events scattered over the network.
B. It is a technique that allows multiple computers to share one or more IP addresses.
C. It cannot detect events scattered over the network.
D. It can handle encrypted and unencrypted traffic equally.

Answer: C,D

Question No : 31 - (Topic 1)

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 No : 32 - (Topic 1)

Which of the following statements about *DMZ* is true?

A. DMZ is a corporate network used as the Internet.
B. DMZ is a firewall that lies in between two corporate networks.
C. DMZ is a network that is not connected to the Internet.
D. DMZ is a network that lies in between a corporate network and the Internet.

Answer: D

Question No : 33 - (Topic 1)

Mark the list that mentions the correct levels of classification of the *military data-classification system*.

A.
-4

Answer: A

Question No : 34 - (Topic 1)

Which of the following are the examples of administrative controls?

Each correct answer represents a complete solution. Choose all that apply.

A. Data Backup
B. Auditing
C. Security policy
D. Security awareness training

Answer: C,D

Question No : 35 - (Topic 1)

Against which of the following does *SSH* provide protection?

Each correct answer represents a complete solution. Choose two.

A. DoS attack
B. Password sniffing
C. Broadcast storm
D. IP spoofing

Answer: B,D

Question No : 36 - (Topic 1)

Which of the following standards is used in wireless local area networks (WLANs)?

A. IEEE 802.4
B. IEEE 802.11b
C. IEEE 802.5
D. IEEE 802.3

Answer: B

Question No : 37 - (Topic 1)

At which of the following layers Structured Query Language (SQL) works?

A. Physical
B. Network
C. Transport
D. Session

Answer: D

Question No : 38 - (Topic 1)

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 No : 39 - (Topic 1)

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 No : 40 - (Topic 1)