# MCQ on Network Security

## Basics of Networking

**1. What does PoP stand for?**

A. Pre Office Protocol
B. Post Office Protocol
C. Protocol of Post
D. None

**Answer -** B) PoP stands for Post Office Protocol

**2. What is the port number of PoP?**

A. 35
B. 43
C. 110
D. 25

**Answer -** C) The ports number of PoP is 110

**3. What is the number of layers in the OSI model?**

A. 2 layers
B. 4 layers
C. 7 layers
D. 9 layers

**Answer -** C) OSI model consists of 7 layers.

**4. The full form of OSI is?**

A. Operating System interface
B. Optical System interconnection
C. Operating System Internet
D. Open system interconnection

**Answer -** D) OSI stands for Open system interconnection.

**5. Identify the layer which provides service to the user.**

A. Session layer
B. Application layer
C. Presentation error

D. Physical layer

**Answer -** B) Application layer provides service to the user.

**6. What is a HUB?**

A. Software
B. Computing device
C. Network device
D. Calculating device

**Answer -** C) A HUB is a network device

**7. What does a set of rules define?**

A. SMTP
B. FTP
C. IMAP
D. Protocol

**Answer -** Protocol defines a set of rules.

**8. Identify among the following which is mainly used to host web site.**

A. Mail server
B. Webserver
C. Database server
D. None

**Answer -** B) Web server is mainly used to host web site.

**9. Identify the full form of HTTP?**

A. HyperText Transfer Protocol
B. HyperText Transfer Package
C. Hyper Transfer Text Package
D. Hyper Transfer Text Practice

**Answer -** A) HTTPS stands for HyperText Transfer Protocol

**10. Identify the protocol primarily used for browsing data.**

A. FTP
B. TCP
C. TFTP

D. HTTP

**Answer -** D) HTTP is used for browsing data.

**11. Identify the total versions of IP.**

A. 1
B. 2
C. 3
D. 4

**Answer -** B) IP has 2 versions, IPV4 and IPV6.

**12. Identify the first network which was based on TCP/IP protocol.**

A. ARPANET
B. HUB
C. Ethernet Card
D. Router

**Answer -** A) ARPANET was the first network that was based on TCP/IP protocol.

**13. Choose among the following, which is the most common internet protocol.**

A. PPP
B. FTP
C. TCP/IP
D. SMTP

**Answer -** D) SMTP is the most commonly used internet protocol.

**14. What does TCP/IP stand for?**

A. Telephone control protocol / Internet Protocol
B. Transmission control protocol/Internet protocol
C. Transmission control protocol/International protocol
D. None

**Answer -** B) TCP/IP stands for Transmission control protocol/Internet protocol.

**15. Which of the following layer isn't present in the TCP/IP model but is included in the OSI model?**

A. Network layer
B. Session layer

C. Application layer
D. Transport layer

**Answer -** B) The TCP/IP model does not contain a session layer.

**16. What is the collection of the hyperlinked document on the internet known as?**

HTML
Email
WWW
Internet

**Answer -** The collection of the hyperlinked document on the internet known as WWW.

**17. What is the location of a resource on the internet given by?**

A. Email
B. IP
C. Protocol
D. URL

**Answer -** D) The location of a resource on the internet is given by URL

**18. Identify the incorrect network topology,**

A. Bus
B. Star
C. P2P
D. Ring

**Answer -** C) P2P is not network topology.

**19. Choose the port number of FTP.**

A. 23
B. 21
C. 110
D. 143

**Answer -** B) The port number of FTP is 21.

**20. What is the length of the IPv4 address?**

A. 8 bits
B. 16 bits

C. 32 bits
D. 128 bits

**Answer -** C) The length of the IPv4 address is 32 bits.

**21. What is the length of the IPv6 address?**

A. 8 bits
B. 16 bits
C. 32 bits
D. 128 bits

**Answer -** D) The length of the IPv6 address is 128 bits.

**22. What is the term used when the main server sends mail to another mail server?**

A. FTP
B. SMTP
C. TCP/IP
D. MIME

**Answer -** B) SMTP is the term used when the main server sends mail to another mail server.

**23. What is the port number of SMTP?**

A. 110
B. 143
C. 25
D. 99

**Answer -** C) The port number of SMTP is 25.

**24. What does MIME stand for?**

A. Multipurpose Internet Mail Extra
B. Multi Internet Mail End
C. Multipurpose Internet Mail Email
D. Multipurpose Internet Mail Extension

**Answer -** D) MIME stands for Multipurpose Internet Mail Extension.

**25. What does port number 143 refer to?**

A. SMTP
B. FTP
C. IMAP

D. POP

**Answer -** C) Port number 143 refers to IMAP.

**26. Identify among the following the network device used to connect two dis-similar types of networks.**

A. Switch
B. Hub
C. Bridge
D. Gateway

**Answer -** D) Gateway is used to connect two dis-similar types of networks.

**27. Identify the device used to boost up a weak signal.**

A. Modem
B. Repeater
C. Switch
D. Router

**Answer -** B) Repeater is used to boost up a weak signal.

**28. What does MAC stand for?**

A. Media Access Control
B. Mass Access Control
C. Media Access Carriage
D. None

**Answer -** A) MAC stands for Media Access Control.

**29. What is the length of the MAC address?**

A. 8 bits
B. 16 bits
C. 32 bits
D. 48 bits

**Answer -** D) Length of MAC address is 48 bits.

**30. Which of the following is used to allocate and manage resources for a network?**

A. Bluetooth
B. Server
C. Node
D. None of the above

**Answer -** B) Server is used to allocate and manage resources for a network.

**31. The arrangement where all data pass through a central computer is known as**

A. Ring topology
B. Mesh topology
C. Star topology
D. Bus topology

**Answer -** C) The arrangement where all data pass through a central computer is known as Star topology.

**32. What of the following device is used in the network layer?**

A. Application gateway
B. Switch
C. Router
D. Repeaters

**Answer -** C) Router is used in the network layer.

**33. Identify if the following statement is True or False: Network Interface Card(NIC) is an I/O device.**

A. True
B. False
C. Depends on usage
D. None

**Answer -** A) NIC is an I/O device.

**34. What is required to use a Simple Network Management System?**

A. Servers
B. Protocols
C. Rules
D. IP

**Answer -** C) Rules are required to use a Simple Network Management System.

**35. Identify the major difference between SNMPv3 and SNMPv2.**

A. Classification
B. Integration
C. Management

D. Enhanced security

**Answer -** D) The major difference between SNMPv3 and SNMPv2 is Enhanced security.

**36. Identify the network which extends a private network across a public network.**

A. Storage Area network
B. Virtual private network
C. Enterprise Private network
D. Local area network

**Answer -** B) VPN extends a private network across a public network.

**37. Identify the layer which is responsible for data translating.**

A. Network
B. Datalink
C. Presentation
D. Application

**Answer -** C) Presentation layer is used for data translating.

**38. Identify the layer which determines the interface of the system with the user.**

A. Network
B. Datalink
C. Presentation
D. Application

**Answer -** D) Application layer is used to determine the interface of the system with the user.

**39. Which of the following topology arrangements is a point-to-point line configuration?**

A. RIng
B. Mesh
C. Star
D. All of the above

**Answer -** D) All of the above consists of a point-to-point line configuration.

**40. Identify the device which links two homogeneous packed broadcast local networks.**

A. Hub
B. Router
C. Bridge
D. Gateway

**Answer -** C) Bridge is used to link two homogeneous packed broadcast local networks.

**41. Why are parity bits used?**

A. To encrypt data
B. To detect error
C. To identify user
D. None

**Answer -** B) Parity bits are used to detect the error.

**42. Identify among the following which belongs to class A.**

A. 121.12.12.248
B. 128.12.12.248
C. 129.12.12.248
D. 130.12.12.248

**Answer -** A)121.12.12.248 belongs to class A as the first octet value in the address lies between [0, 127].

**43. What does LAN stand for?**

A. Local Array Network
B. Local Area Network
C. Local Area Net
D. None

**Answer -** B) LAN stands for Local Area Network.

**44. Who keeps the private key in asymmetric key cryptography?**

A. Sender
B. Receiver
C. Both Sender and Receiver
D. None

**Answer -** B) Receiver keeps the private key in asymmetric key cryptography.

**45. Calculate the maximum efficiency of pure ALOHA at G = 0.5?**

A. 16%
B. 1.89%
C. 18.4%
D. 18.999%

**Answer -** D) The maximum efficiency of pure ALOHA is given by G * e^(-2G)
Here G = 0.5
So, 0.5 * e^(-2 * 0.5) = 0.5 * e = 18.4%

**46. Identify the switching method in which the message is divided into small packets.**

A. Virtual switching
B. Packet switching
C. Message switching
D. None

**Answer -** B) In packet switching message is divided into small packets.

**47. What is a proxy server also known as?**

A. Application-level gateway
B. Proxy tools
C. Application proxy
D. None

**Answer -** A) Proxy server is also known as Application-level gateway.

**48. Identify among the following servers which allow LAN users to share data.**

A. Communication server
B. Point server
C. Data server
D. File server

**Answer -** D) File server allows LAN users to share data.

**49. Choose the correct formula for the total vulnerable time value of pure ALOHA.**

A. ½ Tfr
B. Tfr
C. 2*Tfr
D. 4*Tfr

**Answer -** C) The total vulnerable time value of pure ALOHA is 2*Tfr.

**50. Choose among the following which is a bit-oriented protocol.**

A. SSL
B. HDLC
C. HTTP

D. All of the above

**Answer -** B) HDLC or High-level link control is a bit-oriented protocol that is used to transmit info from one network to another.

## Network Security

1: Which of the following is correct in connection with the password policy?

A. Usually, password length must be more than 8 characters
B. Password must contain upper case, lower case, numbers, and special characters
C. There should be different passwords for different login accounts.
D. All of the above

**ANSWER: D**

2: DDoS stands for _____.

A. Distributed Denial of Service
B. Distributed Disc operating Service
C. Dynamic Denial of Service
D. None of the above

**ANSWER: A**

3: Which of the following options doesn't belong to the category of the hacker?

A. White Hat Hackers
B. Grey Hat Hackers
C. Red Hat Hackers
D. Black hat Hackers

**ANSWER: C**

4: Which of the following does not help to protect your computer from external threats?

A. System Restore
B. Internet Security
C. Firewall
D. Antivirus software

**ANSWER: A**

5: _____ type of cyber attack is performed by hackers without the use of any computer software program.

A. Cross-Site Scripting
B. ARP Poisoning
C. SQL Injection

D. Social Engineering

**ANSWER: D**

6: This is a type of cyber attack that has a program running on your server to bypass the authorization.

A. DoS
B. Phishing
C. Backdoor
D. Sniffing

**ANSWER: C**

7: ECB in the context of digital cryptography stands for

A. Electrical Circuit Board
B. Electronic Code Book
C. Electrical Code Book
D. Electronic Circuit Book

**ANSWER: B**

8: Which of the following statements describe a type of Phishing attack?

A. Sending someone an email that contains a malicious link by disguising to appear like an email from someone the person knows.
B. Creating a fake website that appears to be identical to the real website and trick users to enter their login information
C. Sending someone a text message that contains a malicious link that is disguised to look like a notification that the person has won a contest.
D. All of the above

**ANSWER: D**

9: Which of the following statement is true?

A. All the website on the Internet is trustworthy
B. If your email attachments look suspicious, do not open it
C. Keep all the passwords the same for your different login accounts.
D. Using a pirated software doesn't compromise your system security

**ANSWER: B**

10: Which of the following is the oldest hacking techniques used by hackers to make free calls?

A. Phishing
B. Hashing
C. Phreaking
D. Cracking

**ANSWER: C**

11: The term “Cyberspace” was coined by _____.

A. William Gibson
B. Andrew Tannenbaum
C. Richard Stallman
D. Scott Fahlman

**ANSWER: A**

12: Which one of the following techniques used by hackers to trick the users in order to disclose their username and passwords through fake websites?

A. Social Engineering
B. Cookie stealing
C. Phishing
D. Cyberstalking

**ANSWER: C**

13: _____ is the first person who was responsible for distributing computer worms through the Internet.

A. Richard Stallman
B. Vladimir Levin
C. Bill Landreth
D. Robert T. Morris

**ANSWER: D**

14: _____ server is used to create a secure tunnel connection.

A. Radius
B. VPN
C. Proxy
D. DNS

**ANSWER: B**

15: When you access your net-banking account, you are also able to access your credit card details, check-ordering services, and a mortgage site without entering your credentials again. Which of the following services does this describe?

A. SAML
B. SSO
C. Kerberos
D. Multiple authentications

**ANSWER: B**

16: The encryption technique that uses one message to hide another message is called _____ .

A. MDA
B. Hashing
C. Steganography
D. None of the above

**ANSWER: C**

17: Which of the following is the process of investigating a computer system for any evidence about the event?

A. Virus Scanning
B. Security policy
C. Evidence gathering
D. Computer forensics

**ANSWER: D**

18: _____ is the term used in computer security to protect your data from getting disclosed.

A. Integrity
B. Authentication
C. Confidentiality
D. Availability

**ANSWER: C**

19: _____ is the term used in computer security to protect the data from being modified by the unauthorized user.

A. Integrity
B. Authentication
C. Confidentiality
D. Availability

**ANSWER: A**

20: _____ is the term used in computer security that only the authorized users are allowed to access the information.

A. Integrity
B. Authentication
C. Confidentiality
D. Availability

**ANSWER: D**

# Encryption Standards and Algorithms

**1. Which of the following is not a type of encryption?**

A) Symmetric encryption

B) Asymmetric encryption

C) Hashing

D) Compression

**Answer: D)** Compression

**Explanation:** Compression is not a type of encryption, it is a technique used to reduce the size of data.

**2. Which encryption algorithm is used in SSL/TLS?**

A) DES

B) RSA

C) Blowfish

D) Triple-DES

**Answer: B)** RSA

**Explanation:** RSA (Rivest-Shamir-Adleman) is a widely used asymmetric encryption algorithm, and it is used for key exchange in SSL/TLS.

**3. Which type of encryption uses the same key for both encryption and decryption?**

A) Symmetric encryption

B) Asymmetric encryption

C) Hashing

D) None of the above

**Answer: A)** Symmetric encryption

**Explanation:** Symmetric encryption uses the same key for both encryption and decryption.

**4. Which of the following is an example of a hash function?**

A) SHA-1

B) RSA

C) AES

D) Diffie-Hellman

**Answer: A)** SHA-1

**Explanation:** SHA-1 (Secure Hash Algorithm 1) is an example of a hash function, it is used to produce a fixed-size output from a variable-size input.

**5. Which encryption algorithm is considered to be the strongest?**

A) DES

B) RSA

C) Blowfish

D) AES

**Answer: D)** AES

**Explanation:** AES (Advanced Encryption Standard) is considered to be the strongest encryption algorithm.

**6. Which of the following is not a characteristic of a good encryption algorithm?**

A) Confidentiality

B) Integrity

C) Availability

D) Authentication

**Answer: C)** Availability

**Explanation:** Availability is not a characteristic of a good encryption algorithm, it is a characteristic of a good system.

**7. Which of the following is a symmetric encryption algorithm?**

A) RSA

B) AES

C) Diffie-Hellman

D) ECC

**Answer: B)** AES

**Explanation:** AES (Advanced Encryption Standard) is a symmetric encryption algorithm.

**8. Which encryption algorithm is commonly used in PGP (Pretty Good Privacy)?**

A) RSA

B) AES

C) Blowfish

D) Triple-DES

**Answer: A)** RSA

**Explanation:** RSA (Rivest-Shamir-Adleman) is commonly used in PGP (Pretty Good Privacy).

**9. Which of the following is not a type of attack on encryption?**

A) Brute force attack

B) Dictionary attack

C) Collision attack

D) Compression attack

**Answer: D)** Compression attack

**Explanation:** Compression attack is not a type of attack on encryption.

**10. Which of the following is not a key length for AES?**

A) 128-bit

B) 256-bit

C) 512-bit

D) 192-bit

**Answer: C)** 512-bit

**Explanation:** The key length for AES can be 128-bit, 192-bit, or 256-bit.

**11. Which encryption algorithm is used in PGP (Pretty Good Privacy) for symmetric encryption?**

A) DES

B) RSA

C) Blowfish

D) IDEA

**Answer: D)** IDEA

**Explanation:** IDEA (International Data Encryption Algorithm) is used in PGP (Pretty Good Privacy) for symmetric encryption.

**12. Which of the following is a type of attack on encryption that tries every possible key combination?**

A) Brute force attack

B) Dictionary attack

C) Collision attack

D) Rainbow table attack

**Answer: A)** Brute force attack

**Explanation:** A brute force attack tries every possible key combination.

**13. Which encryption algorithm is used in SSH (Secure Shell)?**

A) DES

B) RSA

C) Blowfish

D) AES

**Answer: D)** AES

**Explanation:** AES (Advanced Encryption Standard) is used in SSH (Secure Shell).

**14. Which of the following is a type of asymmetric encryption algorithm?**

A) DES

B) RSA

C) Blowfish

D) AES

**Answer: B)** RSA

**Explanation:** RSA (Rivest-Shamir-Adleman) is a type of asymmetric encryption algorithm.

**15. Which encryption algorithm is used in WPA2 (Wi-Fi Protected Access 2)?**

A) DES

B) RSA

C) Blowfish

D) AES

**Answer: D)** AES

**Explanation:** AES (Advanced Encryption Standard) is used in WPA2 (Wi-Fi Protected Access 2).

**16. Which of the following is not a type of cipher?**

A) Substitution cipher

B) Transposition cipher

C) Vigenere cipher

D) RSA cipher

**Answer: D)** RSA cipher

**Explanation:** RSA is an encryption algorithm, not a type of cipher.

**17. Which encryption algorithm is used in IPsec (Internet Protocol Security)?**

A) DES

B) RSA

C) Blowfish

D) AES

**Answer: D)** AES

**Explanation:** AES (Advanced Encryption Standard) is used in IPsec (Internet Protocol Security).

**18. Which of the following is not a characteristic of a good key?**

A) Length

B) Complexity

C) Reusability

D) Randomness

**Answer: C)** Reusability

**Explanation:** Reusability is not a characteristic of a good key.

**19. Which encryption algorithm is used in SSL 3.0?**

A) DES

B) RSA

C) Blowfish

D) RC4

**Answer: D)** RC4

**Explanation:** RC4 (Rivest Cipher 4) is used in SSL 3.0.

**20. Which of the following is not a type of hash function attack?**

A) Preimage attack

B) Birthday attack

C) Collision attack

D) Rainbow table attack

**Answer: D)** Rainbow table attack

**Explanation:** Rainbow table attack is not a type of hash function attack.

**21. Which encryption algorithm is used in OpenVPN?**

A) DES

B) RSA

C) Blowfish

D) AES

**Answer: D)** AES

**Explanation:** AES (Advanced Encryption Standard) is used in OpenVPN.

**22. Which of the following is a type of transposition cipher?**

A) Caesar cipher

B) Playfair cipher

C) Rail fence cipher

D) Vigenere cipher

**Answer: C)** Rail fence cipher

**Explanation:** Rail fence cipher is a type of transposition cipher.

**23. Which encryption algorithm is used in Kerberos?**

A) DES

B) RSA

C) Blowfish

D) AES

**Answer: A)** DES

**Explanation:** DES (Data Encryption Standard) is used in Kerberos.

**24. Which of the following is not a characteristic of a good hash function?**

A) Collision resistance

B) One-wayness

C) Reversibility

D) Determinism

**Answer: C)** Reversibility

**Explanation:** Hash functions are one-way functions, they cannot be reversed.

**25. Which encryption algorithm is used in TLS 1.2?**

A) DES

B) RSA

C) Blowfish

D) AES

**Answer: D)** AES

**Explanation:** AES (Advanced Encryption Standard) is used in TLS 1.2.

**26. Which of the following is a type of substitution cipher?**

A) Caesar cipher

B) Playfair cipher

C) Rail fence cipher

D) Vigenere cipher

**Answer : A)** Caesar cipher

**Explanation:** Caesar cipher is a type of substitution cipher.

**27. Which encryption algorithm is used in PGP (Pretty Good Privacy)?**

A) DES

B) RSA

C) Blowfish

D) AES

**Answer: B)** RSA

**Explanation:** RSA (Rivest-Shamir-Adleman) is used in PGP (Pretty Good Privacy).

**28. Which of the following is not a type of symmetric encryption algorithm?**

A) DES

B) RSA

C) Blowfish

D) AES

**Answer: B)** RSA

**Explanation:** RSA is a type of asymmetric encryption algorithm.

**29. Which encryption algorithm is used in S/MIME (Secure/Multipurpose Internet Mail Extensions)?**

A) DES

B) RSA

C) Blowfish

D) AES

**Answer: B)** RSA

**Explanation:** RSA (Rivest-Shamir-Adleman) is used in S/MIME (Secure/Multipurpose Internet Mail Extensions).

**30. Which of the following is a type of stream cipher?**

A) Playfair cipher

B) Vernam cipher

C) Rail fence cipher

D) Vigenere cipher

**Answer: B)** Vernam cipher

**Explanation:** Vernam cipher is a type of stream cipher.

**31. Which encryption algorithm is used in GPG (GNU Privacy Guard)?**

A) DES

B) RSA

C) Blowfish

D) AES

**Answer: D)** AES

**Explanation:** AES (Advanced Encryption Standard) is used in GPG (GNU Privacy Guard).

**32. Which of the following is a type of block cipher?**

A) Playfair cipher

B) Vernam cipher

C) Rail fence cipher

D) AES

**Answer: D)** AES

**Explanation:** AES (Advanced Encryption Standard) is a type of block cipher.

**33. Which encryption algorithm is used in HTTPS (Hypertext Transfer Protocol Secure)?**

A) DES

B) RSA

C) Blowfish

D) AES

**Answer: D)** AES

**Explanation:** AES (Advanced Encryption Standard) is used in HTTPS (Hypertext Transfer Protocol Secure).

**34. Which of the following is a type of hash function?**

A) Caesar hash

B) MD5 hash

C) Rail fence hash

D) Vernam hash

**Answer: B)** MD5 hash

**Explanation:** MD5 (Message Digest 5) is a type of hash function.

**35. Which encryption algorithm is used in SSL 2.0?**

A) DES

B) RSA

C) Blowfish

D) RC4

**Answer: D)** RC4

**Explanation:** RC4 (Rivest Cipher 4) is used in SSL 2.0.

**36. Which of the following is not a type of encryption attack?**

A) Brute force attack

B) Dictionary attack

C) Social engineering attack

D) Rainbow table attack

**Answer: C)** Social engineering attack

**Explanation:** Social engineering attack is not a type of encryption attack.

**37. Which encryption algorithm is used in Disk Encryption?**

A) DES

B) RSA

C) Blowfish

D) AES

**Answer: D)** AES

**Explanation:** AES (Advanced Encryption Standard) is used in Disk Encryption.

**38. Which of the following is not a type of digital signature algorithm?**

A) RSA

B) DSA

C) ECDSA

D) Blowfish

**Answer: D)** Blowfish

**Explanation:** Blowfish is an encryption algorithm, not a digital signature algorithm.

**39. Which encryption algorithm is used in SSH File Transfer Protocol (SFTP)?**

A) DES

B) RSA

C) Blowfish

D) AES

**Answer: D)** AES

**Explanation:** AES (Advanced Encryption Standard) is used in SSH File Transfer Protocol (SFTP).

**40. Which of the following is not a type of key exchange algorithm?**

A) RSA

B) Diffie-Hellman

C) Elliptic Curve Diffie-Hellman (ECDH)

D) Blowfish

**Answer: D)** Blowfish

**Explanation:** Blowfish is an encryption algorithm, not a key exchange algorithm.

**41. Which of the following is not a type of encryption mode?**

A) ECB

B) CBC

C) OFB

D) RSA

**Answer: D)** RSA

**Explanation:** RSA is an encryption algorithm, not an encryption mode.

**42. Which of the following is a type of message authentication code?**

A) DES

B) HMAC

C) Blowfish

D) RSA

**Answer: B)** HMAC

**Explanation:** HMAC (Hash-based Message Authentication Code) is a type of message authentication code.

**43. Which of the following is not a type of digital certificate?**

A) SSL certificate

B) Code signing certificate

C) Personal certificate

D) Rail fence certificate

**Answer: D)** Rail fence certificate

**Explanation:** Rail fence is not a type of digital certificate.

**44. Which encryption algorithm is used in 3DES (Triple Data Encryption Standard)?**

A) DES

B) RSA

C) Blowfish

D) AES

**Answer: A)** DES

**Explanation:** DES (Data Encryption Standard) is used in 3DES (Triple Data Encryption Standard).

**45. Which of the following is not a type of public key infrastructure (PKI) component?**

A) Certificate authority (CA)

B) Registration authority (RA)

C) Certificate revocation list (CRL)

D) Brute force attack tool

**Answer: D)** Brute force attack tool

**Explanation:** Brute force attack tool is not a PKI component.

**46. Which of the following is a type of key agreement protocol?**

A) RSA

B) Diffie-Hellman

C) ECDSA

D) Blowfish

**Answer: B)** Diffie-Hellman

**Explanation:** Diffie-Hellman is a type of key agreement protocol.

**47. Which of the following is not a type of attack on cryptography?**

A) Brute force attack

B) Side-channel attack

C) Man-in-the-middle attack

D) Protocol attack

**Answer: D)** Protocol attack

**Explanation:** Protocol attack is not a type of attack on cryptography.

**48. Which encryption algorithm is used in OpenPGP?**

A) DES

B) RSA

C) Blowfish

D) AES

**Answer: D)** AES

**Explanation:** AES (Advanced Encryption Standard) is used in OpenPGP.

**49. Which of the following is a type of digital signature algorithm?**

A) DSA

B) RSA

C) ECDSA

D) All of the above

**Answer: D)** All of the above

**Explanation:** DSA (Digital Signature Algorithm), RSA (Rivest-Shamir-Adleman), and ECDSA (Elliptic Curve Digital Signature Algorithm) are all types of digital signature algorithm.

**50. Which of the following is not a type of digital signature?**

A) Message authentication code (MAC)

B) Public key digital signature

C) Hash-based digital signature

D) Elliptic Curve digital signature

**Answer: A)** Message authentication code (MAC)

**Explanation:** MAC (Message authentication code) is not a type of digital signature.

**51. Which of the following is not a type of cryptographic hash function?**

A) SHA-1

B) SHA-2

C) MD5

D) RSA

**Answer: D)** RSA

**Explanation:** RSA is not a type of cryptographic hash function.

**52. Which of the following is not a type of public key infrastructure (PKI) service?**

A) Certificate authority (CA)

B) Registration authority (RA)

C) Certificate revocation list (CRL)

D) Diffie-Hellman service

**Answer: D)** Diffie-Hellman service

**Explanation:** Diffie-Hellman is a key agreement protocol, not a PKI service.

**53. Which encryption algorithm is used in the WPA2 wireless security protocol?**

A) DES

B) RSA

C) Blowfish

D) AES

**Answer: D)** AES

**Explanation:** AES (Advanced Encryption Standard) is used in the WPA2 wireless security protocol.

**54. Which of the following is a symmetric key algorithm?**

A) RSA

B) Diffie-Hellman

C) AES

D) Elliptic Curve Cryptography (ECC)

**Answer: C)** AES

**Explanation:** AES (Advanced Encryption Standard) is a symmetric key algorithm.

**55. Which encryption algorithm is used in the IPsec protocol?**

A) DES

B) RSA

C) Blowfish

D) AES

**Answer: D)** AES

**Explanation:** AES (Advanced Encryption Standard) is used in the IPsec protocol.

**56. Which of the following is a type of attack on public key infrastructure (PKI)?**

A) Birthday attack

B) Replay attack

C) Padding oracle attack

D) All of the above

**Answer: D)** All of the above

**Explanation:** Birthday attack, replay attack, and padding oracle attack are all types of attacks on PKI.

**57. Which encryption algorithm is used in the PPTP protocol?**

A) DES

B) RSA

C) Blowfish

D) RC4

**Answer: A)** DES

**Explanation:** DES (Data Encryption Standard) is used in the PPTP protocol.

**58. Which of the following is not a type of key agreement protocol?**

A) Diffie-Hellman

B) ECDH

C) RSA

D) MQV

**Answer: C)** RSA

**Explanation:** RSA is not a key agreement protocol.

**59. Which encryption algorithm is used in the S/MIME secure email standard?**

A) DES

B) RSA

C) Blowfish

D) AES

**Answer: D)** AES

**Explanation:** AES (Advanced Encryption Standard) is used in the S/MIME secure email standard.

**60. Which encryption algorithm is used in the TLS 1.2 protocol?**

A) DES

B) RSA

C) Blowfish

D) AES

**Answer: D)** AES

**Explanation:** AES (Advanced Encryption Standard) is used in the TLS 1.2 protocol.

## Network Security Devices

1. A firewall is a network security device

A. it accepts, rejects, or drops that specific traffic.
B. which monitors all incoming and outgoing traffic
C. establishes a barrier between secured internal networks and outside the untrusted networks
D. All of the above

**Answer D.** All of the above

2. Which of the following is not a type of firewall?

A. Host-based Firewalls
B. Network-based Firewalls
C. Packet Filtering Firewall
D. Dual Host Firewall

**Answer D.** Dual Host Firewall

3. Network layer firewall has two sub-categories as _____

A. Network & session layer firewall
B. State full firewall and stateless firewall
C. Bit & byte-oriented firewall
D. Frame firewall and packet firewall

**Answer B.** State full firewall and stateless firewall

4. Firewalls can be of _____ kinds.

A. hardware firewalls
B. software firewalls
C. combination of both hardware and software
D. hardware firewalls, software firewalls, and a combination of both hardware and software.

**Answer D.** hardware firewalls, software firewalls, and a combination of both hardware and software.

5. _____ is connected between the device and the network connecting to internet.

A. Hardware Firewall
B. Software Firewall

C. Stateful Inspection Firewall

D. Microsoft Firewall

**Answer A.** Hardware Firewall

6. _____ they come by-default with operating systems.

A. Hardware Firewall

B. Software Firewall

C. Stateful Inspection Firewall

D. Microsoft Firewall

**Answer B.** Software Firewall

7. Which of the following is a hardware firewall?

A. Windows Firewall

B. Outpost Firewall Pro

C. Endian Firewall

D. Linksys Firewall

**Answer D.** Linksys Firewall

8. How many types of firewalls.

A. 5

B. 4

C. 3

D. 2

**Answer B.** 4

9. Network administrators can create their own ACL rules based on _____ _____ and _____

A. Address, Protocols, and security policies

B. IP Address, policies, and Packet attributes

C. Address, Protocols, and Packet attributes

D. Network topology, Protocols, and data packets

**Answer C.** Address, Protocols, and Packet attributes

10. Gateway  serves as the connection point between

A. Network and Cloud
B. Network and Controller
C. Controller and device
D. cloud and controller, sensors, and intelligent devices.

**Answer D.** cloud and controller, sensors, and intelligent devices.

11. Which of the following is not types of network security devices

A. active devices & passive devices
B. preventative devices
C. Unified Threat Management (UTM) devices
D. /Network interface card

**Answer D.** Network interface card

12. firewalls, antivirus scanning devices, content filtering devices are examples of …….Network Security Devices

A. active devices
B. preventative devices
C. Unified Threat Management (UTM) devices
D. passive devices

**Answer A.** active devices

13. Active devices…

A. Which block the surplus traffic
B. which identify and report on unwanted traffic
C. which scan the networks and identify potential security problems;
D. which serve as all-in-one security devices.

**Answer A.** Which block the surplus traffic

14. Passive devices

A. Which block the surplus traffic
B. which identify and report on unwanted traffic
C. which scan the networks and identify potential security problems;
D. which serve as all-in-one security devices.

**Answer B.** which identify and report on unwanted traffic

15. preventative devices…..

A. Which block the surplus traffic;
B. which identify and report on unwanted traffic
C. which scan the networks and identify potential security problems
D. which serve as all-in-one security devices.

**Answer C.** which scan the networks and identify potential security problems

16. Unified Threat Management (UTM)

A. Which block the surplus traffic
B. which identify and report on unwanted traffic
C. which scan the networks and identify potential security problems;
D. which serve as all-in-one security devices.

**Answer D.** which serves as all-in-one security devices.

## Attack Types

1. The full form of Malware is _____

a) Malfunctioned Software

b) Multipurpose Software

c) Malicious Software

d) Malfunctioning of Security

**Answer: c**

**Explanation:** Different types of harmful software and programs that can pose threats to a

system, network or anything related to cyberspace are termed as Malware. Examples of some common malware are Virus, Trojans, Ransomware, spyware, worms, rootkits etc.

2. Who deploy Malwares to a system or network?

a) Criminal organizations, Black hat hackers, malware developers, cyber-terrorists

b) Criminal organizations, White hat hackers, malware developers, cyber-terrorists

c) Criminal organizations, Black hat hackers, software developers, cyber-terrorists

d) Criminal organizations, gray hat hackers, Malware developers, Penetration testers

**Answer: a**

**Explanation:** Criminal-minded organizations, groups and individuals cyber-terrorist groups, Black hat hackers, malware developers etc are those who can deploy malwares to any target system or network in order to deface that system.

3. _____ is a code injecting method used for attacking the database of a system / website.

a) HTML injection

b) SQL Injection

c) Malicious code injection

d) XML Injection

**Answer: b**

**Explanation:** SQLi (Structured Query Language Injection) is a popular attack where SQL code is targeted or injected; for breaking the web application having SQL vulnerabilities. This allows the attacker to run malicious code and take access to the database of that server.

4. XSS is abbreviated as _____

a) Extreme Secure Scripting

b) Cross Site Security

c) X Site Scripting

d) Cross Site Scripting

**Answer: d**

**Explanation:** Cross Site Scripting is another popular web application attack type that can hamper the reputation of any site.

5. This attack can be deployed by infusing a malicious code in a website's comment section. What is "this" attack referred to here?

a) SQL injection

b) HTML Injection

c) Cross Site Scripting (XSS)

d) Cross Site Request Forgery (XSRF)

**Answer: c**

**Explanation:** XSS attack can be infused by putting the malicious code (which gets automatically run) in any comment section or feedback section of any webpage (usually a blogging page). This can hamper the reputation of a site and the attacker may place any private data or personal credentials.

6. When there is an excessive amount of data flow, which the system cannot handle, _____ attack takes place.

a) Database crash attack

b) DoS (Denial of Service) attack

c) Data overflow Attack

d) Buffer Overflow attack

**Answer: d**

**Explanation:** The Buffer overflow attack takes place when an excessive amount of data occurs in the buffer, which it cannot handle and lead to data being over-flow into its adjoined storage. This attack can cause a system or application crash and can lead to malicious entry-point.

7. Compromising a user's session for exploiting the user's data and do malicious activities or misuse user's credentials is called _____

a) Session Hijacking

b) Session Fixation

c) Cookie stuffing

d) Session Spying

**Answer: a**

**Explanation:** Using session hijacking, which is popularly known as cookie hijacking is an exploitation method for compromising the user's session for gaining unauthorized access to user's information.

8. Which of this is an example of physical hacking?

a) Remote Unauthorised access

b) Inserting malware loaded USB to a system

c) SQL Injection on SQL vulnerable site

d) DDoS (Distributed Denial of Service) attack

**Answer: b**

**Explanation:** If a suspicious gain access to server room or into any confidential area with a malicious pen-drive loaded with malware which will get triggered automatically once inserted to USB port of any employee's PC; such attacks come under physical hacking, because that person in gaining unauthorized physical access to any room or organization first, then managed to get an employee's PC also, all done physically – hence breaching physical security.

9. Which of them is not a wireless attack?

a) Eavesdropping

b) MAC Spoofing

c) Wireless Hijacking

d) Phishing

**Answer: d**

**Explanation:** Wireless attacks are malicious attacks done in wireless systems, networks or devices. Attacks on Wi-Fi network is one common example that general people know. Other such sub-types of wireless attacks are wireless authentication attack, Encryption cracking etc.

10. An attempt to harm, damage or cause threat to a system or network is broadly termed as _____

a) Cyber-crime

b) Cyber Attack

c) System hijacking

d) Digital crime

**Answer: b**

**Explanation:** Cyber attack is an umbrella term used to classify different computer & network attacks or activities such as extortion, identity theft, email hacking, digital spying, stealing hardware, mobile hacking and physical security breaching.

11. Which method of hacking will record all your keystrokes?

a) Keyhijacking

b) Keyjacking

c) Keylogging

d) Keyboard monitoring

**Answer: c**

**Explanation:** Keylogging is the method or procedure of recording all the key strokes/keyboard button pressed by the user of that system.

12. _____ are the special type of programs used for recording and tracking user's keystroke.

a) Keylogger

b) Trojans

c) Virus

d) Worms

**Answer: a**

**Explanation:** Keyloggers are surveillance programs developed for both security purpose as well as done for hacking passwords and other personal credentials and information. This type of programs actually saves the keystrokes done using a keyboard and then sends the recorded keystroke file to the creator of such programs.

13. These are a collective term for malicious spying programs used for secretly monitoring someone's activity and actions over a digital medium.

a) Malware

b) Remote Access Trojans

c) Keyloggers

d) Spyware

**Answer: d**

**Explanation:** Spyware is professional malicious spying software that is hard to detect by anti-malware or anti-virus programs because they are programmed in such a skillful way. These types of software keep on collecting personal information, surfing habits, surfing history as well as credit card details.

14. Stuxnet is a _____

a) Worm

b) Virus

c) Trojan

d) Antivirus

**Answer: a**

**Explanation:** Stuxnet is a popular and powerful worm that came into existence in mid 2010, which was very powerful as it was accountable for the cause of huge damage to Iran's Nuclear program. It mainly targets the PLCs (Programmable Logic Controllers) in a system.

15. _____ is a violent act done using the Internet, which either threatens any technology user or leads to loss of life or otherwise harms anyone in order to accomplish political gain.

a) Cyber-warfare

b) Cyber campaign

c) Cyber-terrorism

d) Cyber attack

**Answer: c**

**Explanation:** Cyber- terrorism is the term used to describe internet terrorism, where individuals and groups are anonymously misusing ethnicities, religions as well as threaten any technology user, which may lead to even loss of life.

## Firewall

1. Network layer firewall works as a _____

a) Frame filter

b) Packet filter

c) Content filter

d) Virus filter

**Answer: b**

**Explanation:** As you know, firewalls are available as hardware appliances, as software-only, or a combination of the two. In every case, the purpose of a firewall is to isolate your trusted internal network (or your personal PC) from the dangers of unknown resources on the Internet and other network connections that may be harmful. The firewall prevents unauthorized access to your internal, trusted network from outside threats.

2. Network layer firewall has two sub-categories as _____

a) State full firewall and stateless firewall

b) Bit oriented firewall and byte oriented firewall

c) Frame firewall and packet firewall

d) Network layer firewall and session layer firewall

**Answer: a**

**Explanation:** Most network layer firewalls can operate as stateful or stateless firewalls, creating two subcategories of the standard network layer firewall. Stateful firewalls have the advantage of being able to track packets over a period of time for greater analysis and accuracy — but they require more memory and operate more slowly. Stateless firewalls do not analyze past traffic and can be useful for systems where speed is more important than security, or for systems that have very specific and limited needs. For example, a computer that only needs to connect to a particular backup server does not need the extra security of a stateful firewall.

3. A firewall is installed at the point where the secure internal network and untrusted external network meet which is also known as _____

a) Chock point

b) Meeting point

c) Firewall point

d) Secure point

**Answer: a**

**Explanation:** A firewall can be a PC, a router, a midrange, a mainframe, a UNIX workstation, or a combination of these that determines which information or services can be accessed from the outside and who is permitted to use the information and services from outside. Generally, a firewall is installed at the point where the secure internal network and untrusted external network meet, which is also known as a chokepoint.

4. Which of the following is / are the types of firewall?

a) Packet Filtering Firewall

b) Dual Homed Gateway Firewall

c) Screen Host Firewall

d) Dual Host Firewall

**Answer: a**

**Explanation:** A firewall can be a PC, a midrange, a mainframe, a UNIX workstation, a router, or combination of these. Depending on the requirements, a firewall can consist of one or more of the following functional components: Packet-filtering router

5. A proxy firewall filters at _____

a) Physical layer

b) Data link layer

c) Network layer

d) Application layer

**Answer: d**

**Explanation:** The application firewall is typically built to control all network traffic on any layer up to the application layer. It is able to control applications or services specifically, unlike a stateful network firewall, which is – without additional software – unable to control network traffic regarding a specific application. There are two primary categories of application firewalls, network-based application firewalls and host-based application firewalls.

6. A packet filter firewall filters at _____

a) Physical layer

b) Data link layer

c) Network layer or Transport layer

d) Application layer

**Answer: c**

**Explanation:** In computing, a firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.[1] A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed not to be secure or trusted.[2] Firewalls are often categorized as either network firewalls or host-based firewalls.

7. What is one advantage of setting up a DMZ with two firewalls?

a) You can control where traffic goes in three networks

b) You can do stateful packet filtering

c) You can do load balancing

d) Improved network performance

**Answer: c**

**Explanation:** DMZ stands for De-Militarized Zone. In a topology with a single firewall serving both internal and external users (LAN and WAN), it acts as a shared resource for these two zones. So load balancing can be done by adding another firewall.

8. What tells a firewall how to reassemble a data stream that has been divided into packets?

a) The source routing feature

b) The number in the header's identification field

c) The destination IP address

d) The header checksum field in the packet header

**Answer: a**

**Explanation:** The source routing feature provides a path address for the packet to help the firewall to reassemble the data stream that was divided into packets. After reassembling, the firewall can then filter the stream.

9. A stateful firewall maintains a _____ which is a list of active connections.

a) Routing table

b) Bridging table

c) State table

d) Connection table

**Answer: a**

**Explanation:** The routing table basically gives the state of each connection i.e. whether the connection is active or not. A routing table ensures the best performance for the stateful firewall.

10. A firewall needs to be _____ so that it can grow proportionally with the network that it protects.

a) Robust

b) Expansive

c) Fast

d) Scalable

**Answer: b**

**Explanation:** The firewall has to be expansive because a network is expected to grow with time and if the firewall is unable to grow with it, the firewall won't be able to handle the growing network traffic flow and will hence fail.