There are several types of firewalls that are commonly used in network security. These include:

a) **Packet-filtering firewalls:** These are the simplest and most basic type of firewall. They work by examining each packet of data that passes through the network and determining whether to allow or block the packet based on a set of predefined rules.

b) **Stateful inspection firewalls:** These firewalls are more advanced than packet-filtering firewalls. They not only examine each packet of data but also keep track of the state of network connections. This allows them to identify and block suspicious traffic that may be part of a larger attack.

c) **Application-level gateways:** These firewalls operate at the application layer of the network and are designed to monitor specific types of traffic, such as email or web traffic. They are often used in conjunction with other types of firewalls to provide additional layers of protection.

d) **Circuit-level gateways:** These firewalls operate at the transport layer of the network and are designed to monitor the flow of traffic between two hosts. They are often used in conjunction with other types of firewalls to provide additional layers of protection.

e) **Next-generation firewalls:** These are advanced firewalls that combine several different types of firewall technologies and security features. They are designed to provide a high level of security and are often used in large enterprise environments.

MULTIPLE CHOICE QUESTIONS

1. **_____ is not true in case of OSI and TCP/IP model.**
   A. The OSI Model is a logical and conceptual model that defines how communication needs to be done
   B. TCP/IP model depends on standard protocols that assigns the network of hosts over the Internet.
   C. Both OSI and TCP/IP models are protocol independent
   D. None of these
2. **A computer has just been installed on the Ethernet LAN but it is not communicating with the network, then what should be done at first?**
   A. Update the NIC driver
   B. Verify the IP address configuration on the workstation
   C. Verify the connectivity on the computer's network card
   D. All of the above
3. **Which of the following commands is not used in the troubleshooting of computer networks?**
   A. Ping B. Tracert
   C. Ipconfig D. Chkdsk
4. **In network troubleshooting, which of the following commands is used?**
   A. Netstat B. Nslookup
   C. Tracert D. All of the above
5. **Which server maintains a directory of domain names and translate them to Internet Protocol (IP) addresses.**
   A. DNS Server
   B. DHCP Server
   C. Web Server
   D. Database Server
6. **Which data link sub-layer carries out data link functions that depend upon the type of medium?**
   A. Logical link control
   B. Media access control
   C. Network interface control
   D. Error Control
7. **When connected to the Internet, the device used to perform modulation and demodulation is called**
   A. Trans receiver B. Modem
   C. Repeater D. All of the above
8. **An web-site is a collection of**
   A. Components of internet
   B. Web-pages
   C. Web links
   D. All of the above
9. **In web applications, _____ is the correct order to form URLs.**
   A. Protocol name, File name, DNS name
   B. DNS name, Protocol name, File name
   C. Protocol name, DNS name, File name
   D. Protocol name, File name, DNS name
10. **In computer networking, MAN lies in between LAN and WAN in terms of**
    A. Area coverage
    B. Data transfer rate
    C. Both of the above
    D. None of these

11. **Which type of network is an Internet?**
A. LAN B. MAN
C. WAN D. All of the above

12. **The most commonly used network media for small local area network is———.**
A. Twisted pair cable
B. Co-axial cable
C. Optical fiber
D. All of the above

13. **In computer networking, a Network Interface Card (NIC) has**
A. MAC address
B. IP address
C. Subnet mask
D. All of the above

14. **Which statement is true in case of IP address?**
A. Every computer connected to the network must have an IP address to communicate
B. Every computer connected to the Internet must have an IP address to communicate
C. Both of the above
D. None of these

15. **Which of the following statement is false in case of IP**
A. IP is an Internet path
B. Every computer must have an IP address
C. IP is a unique address of a computer connected to the network
D. Both A and B

16. **In computer networking, the commonly used topology for LAN is ———————.**
A. Star topology B. Ring topology
C. Bus topology D. Tree topology

17. **In network security, which statement is true in case of IPS?**
A. IPS is a network security technology that examines network traffic flows to detect and prevent vulnerability exploits.
B. If an attack is detected, IPS can stop the malicious traffic before it makes it to rest of the network
C. Both of the above
D. None of these

18. **In network security, which statement is false in case of IPS and IDS?**
A. IDS is a device or software application that monitors a network or systems for malicious activity or policy violations
B. IPS controls access to IT networks in order to protect systems from attack and abuse
C. IDS are designed to identify suspicious attacks and to take the corrective action to block them
D. If an attack is detected, IPS can stop the malicious traffic before it makes it to rest of the network

19. **Which statement is false in case of peer-to-peer network?**
A. In peer-to-peer networks all nodes are act as server as well as client.
B. Peer-to-peer network is easier to setup.
C. Peer-to-peer network is more expensive than client server network.
D. Each workstation on the network shares its files equally with the others.

20. **In computer networking, ——— is the most reliable network topology.**
A. Bus topology
B. Mesh topology
C. Tree topology
D. None of these

21. **Which networking device can perform Network Address Translation (NAT)?**
A. Bridge B. Switch
C. Router D. All of the above

22. **What is Data Encryption Standards (DES) used in network security?**
A. It is symmetric key cryptography
B. It uses only one key for encryption and decryption
C. It is asymmetric key cryptography
D. Both A and B

23. **Which of the following statement is true in case of IP address and MAC address?**
A. Every network device must have IP address and MAC address to communicate.
B. IP address is logical address and MAC address is physical address.
C. IP address can be changed but MAC address can never be changed.
D. All of the above

24. **What type of communication media is used to develop internet backbone for a bigger and wider Information Highway in the country?**
A. Wireless microwave link
B. Co-axial cable
C. Optical fiber
D. All of the above

25. **In OSI reference mode, which layer takes care that the data is sent in such a way that the receiver will understand the data or information and will be able to use the data?**
A. Transport layer
B. Session layer
C. Presentation layer
D. Application layer

26. **Which protocol is preferred for the streaming applications that require constant data flow, bulk data and fastness than reliability?**
A. TCP B. UDP
C. FTP D. ARP

27. **In HTTPS, the communication protocol is encrypted using.....**
A. Application layer security
B. Transport layer security
C. Network layer security
D. None of these

28. **A malware which attempts to obtain sensitive information for malicious reasons, by disguising as a trustworthy entity is called.....**
A. Trojan horse B. Phishing
C. Logic bomb D. All of the above

29. **Which of the following malware do not reproduce or replicate itself but is still destructive?**
A. Virus B. Trojan
C. Worm D. Both B and C

30. **A network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules is called**
A. Router
B. Switch
C. Firewall
D. None of these

31. In computer networks, ———— is categorized in the computer related threats.
A. Phishing B. Spyware
C. Trojan horse D. All of the above

32. A universe of network-accessible information where web resources are identified by URLs and accessible via the Internet is called————.
A. Local Area Network (LAN)
B. Wide Area Network (WAN)
C. World Wide Web (WWW)
D. Storage Area Network (SAN)

33. In computer networking, ————is not any network type.
A. Metropolitan Area Network
B. Public Area Network
C. Wireless Local Area Network
D. Personal Area Network

34. A private enterprise network which is designed to support an organization's employees to communicate, collaborate and perform their roles in a secure manner is called.....
A. Email B. Internet
C. Extranet D. Intranet

35. Which computer related threat attempts to obtain sensitive information by disguising as a trustworthy entity?
A. Virus B. Trojan
C. Worms D. Phishing

36. In network communication, which medium has the highest data transmission speed?
A. Optical Fiber
B. Satellite
C. Coaxial Cable
D. Microwave Link

37. Which statement is false in case of Digital Signature?
A. A digital signature is a mathematical algorithm routinely used to validate the authenticity and integrity of a message, software or digital document.
B. Digital signature provides far more inherent security than handwritten signature.
C. Just like a handwritten signature, a digital signature is unique for every document.
D. None of these

38. In web applications, which security is applied in HTTPS?
A. Application layer security
B. Transport layer security
C. Network layer security
D. None of these

39. In Nepal, the prevailing law which deals with the issues relating to cyber-crime is.....
A. Electronic Transaction Act, 2063
B. Criminal Act, 2074
C. Copyright Act, 2059
D. Right to Information Act, 2064

40. In OSI reference mode, which layer takes care that the data is sent in such a way that the receiver will understand the data or information and will be able to use the data?
A. Transport layer
B. Session layer
C. Presentation layer
D. Application layer

41. An ———— is a network security tool that continuously monitors a network for harmful activity and takes corrective action to block it.
A. Intrusion Detection System (IDS)
B. Intrusion Prevention System (IPS)
C. Both of the above
D. None of these

42. Which of the following statements is false in case of Denial of Services (DoS) and Distributed Denial of Services (DDos) attacks?
A. Both attacks overload a server, rendering a website or resource inaccessible to the intended users.
B. DDoS attack is a DoS attack that floods a targeted resource with several computers or machines.
C. DoS attack is faster as compared to DDoS.
D. None of these

43. Which statement is false in case of Digital Signature?
A. A digital signature is a mathematical algorithm routinely used to validate the authenticity and integrity of a message, software or digital document.
B. Digital signature provides far more inherent security than handwritten signature.
C. Digital signature, like handwritten signature, becomes unique for each document.
D. None of these

44. ———— command can be used to check network connectivity between the host and the server/host when troubleshooting computer networks?
A. IPCONFIG B. PING
C. TRACERT D. Both B and C

45. An ———— is a private network that provides controlled access to authorized customers, vendors, partners, or others outside the company.
A. Internet B. Intranet
C. Extranet D. All of the above

46. A network in which two or more PCs are linked together to share files and get access to common devices like printers, scanners is called
A. Client – Server Network
B. Peer to Peer Network
C. Both of the above
D. None of these

47. Which of the following is not a network device?
A. Hub B. Bridge
C. Router D. Tape Drive

48. A type of malicious code which disguises itself as a desirable code or software but can take control of your computer is
A. Virus
B. Worms
C. Trojan
D. Phishing

49. A piece of code intentionally inserted into a software system that will cause malicious function when specified conditions are met is called
A. Worm
B. Torjan horse
C. Logic bomb
D. None of these

50. ———— is not a valid subnet mask in computer networking.
A. 255.0.255.0
B. 255.255.255.248
C. 255.255.248.0
D. 255.0.0.0

51. Which of the following networking devices is used to connect two different networks?
A. Hub B. Switch
C. Router D. All of the above

52. An ————is a network security tool that monitors network traffic for suspicious activity and issues alerts when such activity is discovered.
A. Intrusion Detection System (IDS)
B. Intrusion Prevention System (IPS)
C. Both of the above
D. None of these

53. In computer networking, which protocol is used to map IP network address to hardware MAC address?
A. SNMP B. ARP
C. TCP/IP D. PPP

54. In OSI reference model, which layer is responsible for error-free, end-to-end (process-to-process) delivery of data from source host to destination host?
A. Network layer
B. Transport layer
C. Presentation layer
D. Application layer

55. The X.25 standard specifies
A. DTE/DCE interface
B. Start – stop data
C. Data bit rate
D. Dial up access

56. Which one of the following network devices uses the higher number of layers in the OSI Model?
A. Switch
B. Router
C. Bridge
D. All use the same number of layers

57. Firewall which is designed to monitor and filter incoming and outgoing network traffic based on an organization's previously established security policies is implemented in
A. Hardware
B. Software
C. Combination of hardware and software
D. All of the above

58. In information security, asymmetric cryptography uses————.
A. Public and private keys for encryption and decryption
B. Same key for both encryption and decryption
C. Both of the above
D. None of these

59. Protocol Data Unit (PDU) of data link layer is known as
A. Frame B. Datagram
C. Message D. Segment

60. Protocol Data Unit (PDU) of transport layer is known as
A. Frame B. Datagram
C. Segment D. Both B and C

61. Protocol Data Unit (PDU) of network layer is known as
A. Frame B. Packet
C. Datagram D. Segment

62. A pseudo private data network that uses public bandwidth in combination with a tunneling protocol and security procedures is called
A. Value Added Network (VAN)
B. Virtual Private Network (VPN)
C. Virtual Local Area Network (VLAN)
D. Intranet

63. In OSI model, --------- layer is responsible for getting packets from source node to the destination node.
A. Transport layer B. Network layer
C. Data link layer D. Physical layer

64. Medium Access Control (MAC) address consists of ----- number of bits.
A. 32 B. 48
C. 64 D. 128

65. FDDI stands for
A. Fiber Detected Data Interface
B. Fiber Detected Data Interchange
C. Fiber Distributed Data Interchange
D. Fiber Distributed Data Interface

66. Firewalls cannot prevent ---------- attack.
A. Denial of Service (DoS)
B. Distributed Denial of Service (DDoS)
C. Both of the above
D. None of these

67. Symmetric cryptography uses
A. Public and private keys for encryption and decryption
B. Same key for both encryption and decryption
C. Both of the above
D. None of these

68. In OSI network architecture, the dialogue control and token management are the responsibilities of
A. Session layer B. Network layer
C. Transport layer D. Data link layer

69. How many OSI layers are covered in the X.25 standard?
A. Two B. Three
C. Four D. Seven

70. Which of the following communication modes support two-way traffic but in only one direction at a time?
A. Simplex
B. Half Duplex
C. Duplex
D. None of these

71. Which one of the following uses the highest number of layers in the OSI model?
A. Bridge B. Switch
C. Router D. Gateway

72. What is the subnet mask of Class C IP address with 4 bits of subnetting?
A. 255.255.240.0
B. 255.255.255.240
C. 255.255.16.0
D. 255.255.255.16

73. In Local Area Network (LAN), ——— protocol maps a dynamic IP address to a permanent physical media access control (MAC) address.
A. Address Resolution protocol
B. Point to Point protocol
C. Network Address Translation protocol
D. None of these

74. While transmitting signal in the data link layer, ————is correct in case of CSMA/CD.
A. CSMA/CD is effective before a collision
B. CSMA/CD is effective after a collision
C. CSMA/CD is effective in both before and after a collision
D. None of these

75. Which statement is not correct in case of VLAN?
A. VLAN is a logical overlay network that groups together a subset of devices that share a physical LAN
B. VLANs can help manage broadcast traffic by forming multiple broadcast domains.
C. VLAN separates an existing physical network into multiple physical networks
D. Implementing VLANs reduces the security risks

76. **While transmitting signal in the data link layer, ---------- method has the highest number of collisions observed.**
A. 1-Persistent CSMA
B. P-Persistent CSMA
C. Non-Persistent CSMA
D. None of these

77. **The subnet mask represented by the CIDR notation 20 (/20) is**
A. 255.255.255.0 B. 255.255.248.0
C. 255.255.240.0 D. 255.255.224.0

78. **------- is the feature of NAT in Internet connectivity.**
A. It connects a large number of hosts to the global Internet using a smaller number of public IP address, thereby conserving IP address space
B. It enhances security for private networks by keeping internal addressing private from the external network
C. Both of the above
D. None of these

79. **A routing protocol that refers to a gateway protocol which enables the Internet to exchange routing information between autonomous systems (AS) is known as**
A. BGP B. OSPF
C. RIP D. Both B and C

80. **Which transport layer protocol doesn't guarantee the delivery of packets?**
A. TCP
B. UDP
C. Both of the above
D. None of these

81. **Which of the following statements is not true in case of circuit switching and packet switching?**
A. Circuit switching is connection oriented but packet switching is connectionless
B. In-Circuit switching, data is processed at the source system only
C. In Packet switching, data is processed at all intermediate nodes including the source system
D. Bandwidth utilization is more in circuit switching than packet switching

82. **--------- is a network server that automatically assigns IP addresses, default gateways and other network parameters to client devices.**
A. DNS B. DHCP
C. Web Server D. Proxy Server

83. **In IT/IS security, which happens first, Authentication or Authorization?**
A. Authentication
B. Authorization
C. Simultaneously
D. Anyone can happen first

84. **A computer related threat which attempts to obtain sensitive information by masquerading as a trustworthy entity is called**
A. E-mail fraud
B. SPAM
C. Phishing
D. None of these

85. **--------- VPN allows users to connect remotely to an entire network and all its applications.**
A. IPSec VPN B. SSL VPN
C. TLS VPN D. All of the above

86. **In IT/IS security, which access control type is the most secure and inflexible?**
A. Discretionary Access Control
B. Mandatory Access Control
C. Role-Based Access Control
D. Rule-Based Access Control

87. **Which of the following statements is not true in case of IP address and MAC address?**
A. Both addresses uniquely identify the device on a network
B. Both IP and MAC are logical addresses
C. Compared to MAC address, IP address operates on a higher layer of the OSI model
D. None of these

88. **In computer networks, ------- refers to a gateway protocol that enables the internet to exchange routing information between autonomous systems (ASs).**
A. Open Shortest Path First
B. Routing Information Protocol
C. Border Gateway Protocol
D. All of the above

89. **In computer networks, -------- is not a remote access protocol.**
A. SSH B. RDP
C. RAS D. SNMP

90. **Which of the following windows commands is used in network troubleshooting?**
A. Ping
B. Tracert
C. Ipconfig
D. All of the above

91. **Which statement is not correct in case of digital and handwritten signatures?**
A. A digital signature is a mathematical algorithm used to validate the authenticity and integrity of an electronic document
B. Digital signature provides far more inherent security than handwritten signature
C. Just like a handwritten signature, a digital signature is unique for every document
D. Digital signature ensures authentication, integrity and non-repudiation of the signed document

92. **Identify the incorrect statement in case of IPS and IDS, in network security.**
A. IDS is a device or software application that monitors a network or systems for malicious activity or policy violations
B. IPS controls access to IT networks in order to protect systems from attack and abuse
C. Both IDS and IPS can block malicious traffic if an attack is identified before it spreads to the rest of the network
D. None of these

93. **Which cryptography needs an encryption key to be shared among users to communicate securely with each other?**
A. Symmetric cryptography
B. Asymmetric cryptography
C. Both of the above
D. None of these

94. While transmitting signal in the data link layer, CSMA/CA is effective ----.
A. Before a collision
B. After a collision
C. Both before and after a collision
D. None of these

95. The subnet mask represented by the CIDR notation 25 (/25) is
A. 255.255.255.0
B. 255.255.255.128
C. 255.255.255.192
D. 255.255.128.0

96. A routing protocol that refers to a gateway protocol which enables the Internet to exchange routing information within an autonomous system (AS) is known as
A. BGP
B. OSPF
C. RIP
D. Both B and C

97. In ————, receiver's data is prevented from being overwhelmed.
A. Flow control
B. Congestion control
C. Both flow and congestion control
D. None of these

98. Which mechanism controls the entry of data packets into the network, enabling a better use of a shared network infrastructure and avoiding congestive collapse?
A. Flow control
B. Congestion control
C. Both flow and congestion control
D. None of these

99. In the cryptography world, RSA algorithm is used for ————.
A. Symmetric cryptography
B. Asymmetric cryptography
C. Both of the above
D. None of these

100. A digital signature is a mathematical technique which validates ———— of the message, software or digital documents.
A. Authenticity
B. Message Integrity
C. Non-repudiation
D. All of the above

101. A process which verifies the identity of a user who wants to access the system is called
A. Authentication
B. Non-repudiation
C. Integrity
D. None of these

102. In information security, ———— ensures that a message has not been tampered with or altered during transmission.
A. Authentication
B. Non-repudiation
C. Integrity
D. None of these

103. Which feature of digital signature ensures that no party can deny the authenticity of their signature on a document?
A. Authentication
B. Non-repudiation
C. Integrity
D. None of these

ANSWER SHEET

1.C	2.B	3.D	4.D	5.A	6.B	7.B	8.B	9.C	10.C
11.C	12.A	13.A	14.C	15.D	16.A	17.C	18.C	19.C	20.B
21.C	22.D	23.D	24.C	25.C	26.B	27.B	28.B	29.B	30.C
31.D	32.C	33.B	34.D	35.D	36.A	37.C	38.B	39.A	40.C
41.B	42.C	43.C	44.D	45.C	46.B	47.D	48.C	49.C	50.A
51.C	52.A	53.B	54.B	55.A	56.B	57.D	58.A	59.A	60.D
61.B	62.B	63.B	64.B	65.D	66.C	67.B	68.A	69.B	70.B
71.D	72.B	73.A	74.B	75.C	76.A	77.C	78.C	79.A	80.B
81.D	72.B	83.A	84.C	85.A	86.B	87.B	88.C	89.D	90.D
91.C	92.C	93.A	94.A	95.B	96.D	97.A	98.B	99.B	100.D
101.A	102.C	103.B							