Practice Set

A. Networking Concepts & Protocols (1–20)

1. **Which OSI layer is responsible for routing packets between networks?**
   A) Data Link
   B) Network
   C) Transport
   D) Session
   Ans: B

2. **TCP is a ______ protocol.**
   A) Connectionless
   B) Connection-oriented
   C) Stateless
   D) Non-reliable
   Ans: B

3. **Which protocol translates domain names to IP addresses?**
   A) DHCP
   B) DNS
   C) FTP
   D) SNMP
   Ans: B

4. **Which layer ensures end-to-end error recovery and flow control?**
   A) Network
   B) Transport
   C) Application
   D) Data Link
   Ans: B

5. **HTTP operates at which layer of the OSI model?**
   A) Network
   B) Transport
   C) Application
   D) Physical
   Ans: C

6. **Which protocol is used for secure communication on the web?**
   A) HTTP
   B) FTP
   C) HTTPS
   D) SMTP
   Ans: C

7. **Which of the following uses port 22?**
   A) FTP
   B) Telnet
   C) SSH

D) SMTP
Ans: C

8. **ARP resolves:**
A) MAC to IP
B) IP to MAC
C) URL to IP
D) IP to URL
Ans: B

9. **Which protocol sends email?**
A) SMTP
B) POP3
C) IMAP
D) SNMP
Ans: A

10. **ICMP is used for:**
A) File transfer
B) Routing
C) Error reporting and diagnostics
D) Encryption
Ans: C

11. **Which protocol provides dynamic IP addressing?**
A) DNS
B) FTP
C) DHCP
D) HTTP
Ans: C

12. **Which layer converts bits to signals?**
A) Data Link
B) Network
C) Physical
D) Transport
Ans: C

13. **Which is NOT a routing protocol?**
A) RIP
B) OSPF
C) BGP
D) DHCP
Ans: D

14. **A switch operates at which OSI layer?**
A) Physical
B) Data Link
C) Transport
D) Application
Ans: B

15. **A router operates at:**

    A) Layer 1

    B) Layer 2

    C) Layer 3

    D) Layer 4

    Ans: C

16. **Port number of DNS is:**

    A) 20

    B) 53

    C) 80

    D) 161

    Ans: B

17. **Port number for HTTPS:**

    A) 443

    B) 21

    C) 25

    D) 69

    Ans: A

18. **Which device broadcasts data to all ports?**

    A) Switch

    B) Router

    C) Hub

    D) Firewall

    Ans: C

19. **UDP is best suited for:**

    A) Email

    B) Video streaming

    C) File transfers

    D) Web browsing

    Ans: B

20. **Which address is unique to a network card?**

    A) IP

    B) MAC

    C) DNS

    D) Port

    Ans: B

B. Introduction to Network Forensics (21–40)

21. **Network forensics deals with:**

    A) Disk analysis

    B) Packet capture & analysis

    C) Password cracking

    D) File recovery

    Ans: B

22. **Primary goal of network forensics:**
    A) Speed
    B) Evidence collection
    C) Bandwidth optimization
    D) Data compression
    Ans: B

23. **Volatile data refers to:**
    A) Hard drive data
    B) Data erased after reboot
    C) Archived logs
    D) Email data
    Ans: B

24. **Network forensics follows the principle of:**
    A) Random collection
    B) Chain of custody
    C) Destroying evidence
    D) Data obfuscation
    Ans: B

25. **Which of the following is volatile evidence?**
    A) RAM
    B) HDD
    C) Backup tapes
    D) APK files
    Ans: A

26. **Which phase includes capturing network traffic?**
    A) Preservation
    B) Collection
    C) Presentation
    D) Reporting
    Ans: B

27. **Real-time traffic capture is called:**
    A) Passive logging
    B) Live forensics
    C) Offline analysis
    D) Background monitoring
    Ans: B

28. **Which technique monitors data without altering it?**
    A) Active sniffing
    B) Passive sniffing
    C) Injection
    D) Spoofing
    Ans: B

29. **Packet sniffing is part of:**
    A) Host forensics
    B) Network forensics
    C) Cloud forensics

D) Email forensics

Ans: B

30. **Evidence collected from network traffic must be:**

    A) Editable

    B) Tamper-proof

    C) Compressed

    D) Randomized

    Ans: B

31. **Network forensics helps detect:**

    A) Hardware failures

    B) Malware communication

    C) Sound waves

    D) Weather patterns

    Ans: B

32. **Full packet capture includes:**

    A) Only headers

    B) Only payload

    C) Headers + payload

    D) No data

    Ans: C

33. **The time synchronization protocol essential for forensic logs:**

    A) NTP

    B) DHCP

    C) FTP

    D) ARP

    Ans: A

34. **Logs are considered:**

    A) Non-digital evidence

    B) Digital evidence

    C) Physical evidence

    D) Secondary evidence

    Ans: B

35. **Which method stores captured traffic?**

    A) PCAP

    B) EXE

    C) TXT

    D) ISO

    Ans: A

36. **Anomaly detection is part of:**

    A) Forensic reporting

    B) Network monitoring

    C) File hashing

    D) Disk imaging

    Ans: B

37. **Hashing ensures:**
    A) Confidentiality
    B) Integrity
    C) Availability
    D) Access control
    Ans: B

38. **Spoofing affects:**
    A) MAC or IP identity
    B) Clock speed
    C) RAM storage
    D) Username
    Ans: A

39. **Network forensics helps reconstruct:**
    A) Deleted photos
    B) Attack sequences
    C) Browser bookmarks
    D) Memory dumps
    Ans: B

40. **Which technique is used for intrusion analysis?**
    A) URL filtering
    B) Packet reassembly
    C) Heat-mapping
    D) Sound analysis
    Ans: B

C. Network Forensic Tools & Techniques (41–80)

41. **Wireshark is used for:**
    A) Malware coding
    B) Data wiping
    C) Packet analysis
    D) File hosting
    Ans: C

42. **Which tool captures network packets in Linux?**
    A) Notepad
    B) TCPDump
    C) Excel
    D) Photoshop
    Ans: B

43. **Syslog records:**
    A) Images
    B) System and network logs
    C) Passwords
    D) Videos
    Ans: B

44. **NMS stands for:**

A) Network Management System

B) Node Messaging Service

C) Network Monitoring Server

D) Net Mail System

Ans: A

45. **Promiscuous mode allows a NIC to:**

A) Only send packets

B) Receive all packets on network

C) Reject broadcast traffic

D) Change MAC addresses

Ans: B

46. **Port mirroring duplicates:**

A) Hard drive

B) RAM

C) Switch port traffic

D) Firewall logs

Ans: C

47. **Which tool analyzes traffic in real-time?**

A) Paint

B) Wireshark

C) VLC

D) Zoom

Ans: B

48. **Nmap is primarily used for:**

A) Video streaming

B) Network scanning

C) Photo editing

D) Email tracking

Ans: B

49. **Which is NOT a packet capture tool?**

A) TCPDump

B) Wireshark

C) Netcat

D) Tshark

Ans: C

50. **A sniffer captures:**

A) Packets

B) Passwords only

C) Hardware logs

D) Graphics

Ans: A

51. **Which device stores MAC address tables?**

A) Router

B) Switch

C) Hub

D) Firewall
Ans: B

52. **ARP table contains mapping of:**
A) DNS to URL
B) IP to MAC
C) MAC to port
D) IP to hostname
Ans: B

53. **NetFlow is a feature of:**
A) Cisco devices
B) Apple devices
C) Android
D) Firewalls only
Ans: A

54. **Syslog uses default port:**
A) 514
B) 80
C) 22
D) 110
Ans: A

55. **Which tool can perform packet injection?**
A) Wireshark
B) Aircrack-ng
C) Notepad
D) Cisco IOS
Ans: B

56. **A mirrored port is also known as:**
A) SPAN port
B) WAN port
C) DMZ port
D) Console port
Ans: A

57. **TCPDump output can be saved in:**
A) .exe
B) .pcap
C) .pdf
D) .zip
Ans: B

58. **Which tool helps detect open ports?**
A) MS Word
B) Nmap
C) Excel
D) VLC
Ans: B

59. **Wireshark filter to capture only HTTP traffic:**

A) tcp.port==80

B) udp.port==80

C) ip.addr==80

D) http-only

Ans: A

60. **Which tool creates network topology diagrams?**

A) Cisco Packet Tracer

B) Wordpad

C) GIMP

D) Blender

Ans: A

61. **SNMP is used for:**

A) File editing

B) Network management

C) Sound processing

D) Password cracking

Ans: B

62. **Tshark is the command-line version of:**

A) Snort

B) Wireshark

C) Nmap

D) Netstat

Ans: B

63. **Snooping refers to:**

A) Passive monitoring of traffic

B) Updating firmware

C) Backup creation

D) Temperature control

Ans: A

64. **Which mode allows wireless packet capturing?**

A) Monitor mode

B) SSH mode

C) Airplane mode

D) Calibration mode

Ans: A

65. **Firewall logs contain details about:**

A) Blocked/allowed traffic

B) CPU temperature

C) RAM usage

D) Printer settings

Ans: A

66. **Which tool is used for network intrusion detection?**

A) Snort

B) VLC

C) MS Paint

D) Chrome

Ans: A

67. **Netcat is used for:**

A) Port scanning and communication

B) Taking screenshots

C) Watching videos

D) Wifi boosting

Ans: A

68. **Bandwidth monitoring is done by:**

A) NMS

B) Photoshop

C) Notepad

D) BIOS

Ans: A

69. **Which system generates alerts for suspicious traffic?**

A) IDS

B) ZIP

C) DOCX

D) VNC

Ans: A

70. **Which is a centralized logging system?**

A) Syslog

B) Excel

C) VLC

D) GIMP

Ans: A

71. **Port scanning can detect:**

A) Email addresses

B) Network services

C) MAC passwords

D) HDD partitions

Ans: B

72. **Which Wireshark view shows application-level information?**

A) Packet Bytes

B) Packet Details

C) Packet List

D) Statistics

Ans: B

73. **Wireshark captures packets at:**

A) Data Link layer

B) Physical layer

C) Session layer

D) Application layer

Ans: A

74. **Filtering traffic reduces:**
A) Storage and noise
B) RAM size
C) CPU frequency
D) Router speed
Ans: A

75. **Which scanning technique sends SYN packets?**
A) TCP SYN scan
B) UDP flood
C) Ping sweep
D) HTTP scan
Ans: A

76. **ARP poisoning is detected through:**
A) ARP table inconsistencies
B) Disk errors
C) Email logs
D) Browser history
Ans: A

77. **Wireshark protocol hierarchy analysis shows:**
A) CPU usage
B) Traffic distribution
C) NIC temperature
D) RAM fragmentation
Ans: B

78. **Packet decapsulation reveals:**
A) Website names
B) Lower-layer headers
C) Hardware failures
D) Power logs
Ans: B

79. **SSL traffic is harder to inspect because it is:**
A) Fast
B) Encrypted
C) Lightweight
D) Static
Ans: B

80. **Log correlation helps in:**
A) Identifying related events
B) Compressing files
C) Updating firmware
D) Changing passwords
Ans: A

D. Data Link & Physical Layer Forensics (81–100)

81. **A MAC table maps:**
    A) IP ↔ port
    B) MAC ↔ port
    C) DNS ↔ IP
    D) URL ↔ MAC
    Ans: B

82. **Physical layer deals with:**
    A) Binary transmission
    B) Routing
    C) Encryption
    D) Application logic
    Ans: A

83. **Ethernet uses which frame type?**
    A) ATM
    B) PPP
    C) 802.3
    D) Token ring
    Ans: C

84. **Collision domain is related to:**
    A) Switch
    B) Hub
    C) Router
    D) Firewall
    Ans: B

85. **Which table stores dynamic MAC entries?**
    A) Routing table
    B) ARP table
    C) CAM table
    D) NAT table
    Ans: C

86. **ARP table poisoning manipulates:**
    A) IP-to-MAC mappings
    B) URLs
    C) Browser history
    D) Email logs
    Ans: A

87. **Which device divides broadcast domains?**
    A) Hub
    B) Switch
    C) Router
    D) Repeater
    Ans: C

88. **Duplex mismatch leads to:**
    A) Packet loss
    B) Firewall failure
    C) DNS poisoning

D) MAC spoofing
Ans: A

89. **Physical evidence includes:**
A) Ethernet cables
B) ARP logs
C) Syslog
D) Wireshark capture
Ans: A

90. **A switch sends unknown unicast traffic to:**
A) All ports
B) Router
C) Firewall
D) Logs only
Ans: A

91. **WiFi logs include:**
A) SSID and MAC addresses
B) Password hashes
C) Email content
D) Browser cookies
Ans: A

92. **Physical layer forensics includes inspection of:**
A) Fiber cuts
B) Firewall logs
C) Email headers
D) Browser cookies
Ans: A

93. **Ethernet switch logs can show:**
A) Port flapping
B) Browser activity
C) Email headers
D) RAM usage
Ans: A

94. **ARP requests are:**
A) Unicast
B) Broadcast
C) Multicast only
D) Encrypted
Ans: B

95. **MAC flooding attacks target:**
A) Switch CAM table
B) Router RIB
C) Firewall rules
D) DNS cache
Ans: A

96. **VLAN hopping exploits:**
A) Misconfigured switches
B) DNS logs
C) Email servers
D) File systems
Ans: A

97. **Signal attenuation occurs in:**
A) Physical layer
B) Network layer
C) Transport layer
D) Presentation layer
Ans: A

98. **Forensic examination of WiFi includes:**
A) Probe requests
B) Printer logs
C) BIOS settings
D) Memory partitions
Ans: A

99. **MAC spoofing changes:**
A) NIC hardware address
B) IP subnet
C) DNS zone
D) Web server port
Ans: A

100. **Network layer logs include:**
A) Router logs
B) File logs
C) Printer logs
D) BIOS logs
Ans: A

E. System, Server, Browser & Application Logs (101–130)

101. **Server logs help identify:**
A) Unauthorized login attempts
B) Screen brightness
C) Mouse clicks
D) USB voltage
Ans: A

102. **Audit logs track:**
A) User actions
B) Cable types
C) Power supply
D) CPU temperature
Ans: A

103. **Windows logs are stored in:**

A) Event Viewer
B) Disk Manager
C) Notepad
D) BIOS
Ans: A

104. **Linux system logs are stored in:**

A) /home
B) /sys
C) /var/log
D) /boot
Ans: C

105. **Browser history records:**

A) Visited URLs
B) WiFi passwords
C) IP routing
D) DHCP logs
Ans: A

106. **Proxy server logs capture:**

A) User web requests
B) Printer status
C) RAM usage
D) Microphone data
Ans: A

107. **Antivirus logs help detect:**

A) Malware activity
B) Audio noise
C) Display issues
D) Heating
Ans: A

108. **Email header analysis reveals:**

A) Sender and IP hops
B) Attachment content
C) Browser bookmarks
D) Keyboard actions
Ans: A

109. **Which log detects brute-force attacks?**

A) Authentication logs
B) DHCP logs
C) DNS logs
D) NTP logs
Ans: A

110. **Proxy log includes:**

A) URL accessed
B) Hard drive failures
C) Temperature

D) RAM usage
Ans: A

111. **Server logs can show:**

A) Service start/stop events
B) Fiber cuts
C) Cable resistance
D) CPU pin count
Ans: A

112. **Browser cache stores:**

A) Web content
B) Email drafts
C) MAC tables
D) SNMP traps
Ans: A

113. **Firewall logs show:**

A) Allowed/blocked traffic
B) Application code
C) Installed drivers
D) Camera access
Ans: A

114. **SIEM aggregates:**

A) Logs from multiple sources
B) Audio signals
C) WiFi radiation
D) Printer settings
Ans: A

115. **DHCP logs record:**

A) IP allocation events
B) Website cookies
C) Browser plugins
D) WiFi password
Ans: A

116. **DNS logs help detect:**

A) Domain queries
B) Hard disk failures
C) BIOS errors
D) USB access
Ans: A

117. **System audit logs track:**

A) User login/logout
B) CPU speed
C) File fragmentation
D) Power supply
Ans: A

118. **Email forensics involves:**

A) Header, body, attachment investigation
B) Video editing
C) Packet routing
D) GPU analysis
Ans: A

119. **Web server log includes:**

A) Access logs
B) Temperature logs
C) BIOS logs
D) Fan logs
Ans: A

120. **VPN logs track:**

A) Connection source IP
B) Wallpaper changes
C) Volume level
D) Keystrokes
Ans: A

121. **Proxy logs help detect:**

A) Web browsing patterns
B) Power surge
C) Router reboot
D) RAM aging
Ans: A

122. **Antivirus quarantine stores:**

A) Suspicious files
B) Video files
C) Logs
D) Music
Ans: A

123. **Which is a host-based log?**

A) Authentication log
B) Firewall log
C) Router log
D) NetFlow log
Ans: A

124. **Web browser cookies contain:**

A) Session identifiers
B) MAC addresses
C) Password hash
D) ARP mappings
Ans: A

125. **System logs indicate:**

A) Application crashes
B) Monitor brightness
C) Cable type

D) IP rating
Ans: A

126. **Email log includes:**
A) Delivery timestamps
B) Sound output
C) GPU info
D) Printer queue
Ans: A

127. **Browser download history reveals:**
A) User file acquisition
B) RAM errors
C) CPU fan data
D) Email contacts
Ans: A

128. **Server access logs identify:**
A) Remote login attempts
B) Screen brightness
C) RAM size
D) Microphone input
Ans: A

129. **Syslog centralization helps in:**
A) Easier investigation
B) Faster downloads
C) Data encryption
D) Software installation
Ans: A

130. **Application logs help detect:**
A) Crashes and errors
B) Monitor refresh rate
C) Mouse acceleration
D) Wire resistance
Ans: A

F. Limitations & Challenges in Network Forensics (131–150)

131. **Encrypted traffic makes analysis:**
A) Easier
B) Harder
C) Unnecessary
D) Automatic
Ans: B

132. **Spoofing hides the:**
A) True identity of sender
B) Browser history
C) Disk contents

D) RAM size
Ans: A

133. **Privacy laws restrict:**
A) Unauthorized monitoring
B) File compression
C) Network speed
D) Programming languages
Ans: A

134. **VPN use makes forensic tracing:**
A) Easier
B) Difficult
C) Faster
D) Unregulated
Ans: B

135. **Mobile devices challenge forensics due to:**
A) Mobility
B) File size
C) Color display
D) Battery life
Ans: A

136. **NAT hides:**
A) Internal IPs
B) MAC addresses
C) Hostnames
D) Browsers
Ans: A

137. **Encrypted HTTPS traffic hides:**
A) Payload
B) IP headers
C) MAC addresses
D) Ports
Ans: A

138. **Storage limitation impacts:**
A) Long-term packet capture
B) DNS queries
C) Email reading
D) Printing
Ans: A

139. **High bandwidth networks produce:**
A) Large data volumes
B) No logs
C) No errors
D) No packets
Ans: A

140. **Jurisdiction issues arise due to:**

A) Multi-country logs
B) Single device
C) RAM usage
D) CPU speed

Ans: A

141. **Incomplete logs cause:**

A) Gaps in investigation
B) Fast processing
C) Higher speed
D) No issues

Ans: A

142. **Time drift between devices affects:**

A) Log correlation
B) Bandwidth
C) RAM
D) CPU

Ans: A

143. **Cloud logging challenges include:**

A) Multi-tenant environments
B) Printer issues
C) Keyboard issues
D) Battery consumption

Ans: A

144. **Over-encryption leads to:**

A) Lack of visibility
B) Faster browsing
C) Less traffic
D) Simple logs

Ans: A

145. **Attackers may delete logs to:**

A) Cover tracks
B) Increase storage
C) Speed up CPU
D) Change DNS

Ans: A

146. **Log tampering affects:**

A) Integrity of evidence
B) Color display
C) RAM usage
D) Internet speed

Ans: A

147. **Packet loss reduces:**

A) Evidence accuracy
B) RAM
C) CPU

D) Noise

Ans: A

148. **Privacy laws require:**

A) User consent

B) Packet fragmentation

C) URL rotation

D) ARP caching

Ans: A

149. **Encrypted DNS (DoH/DoT) hides:**

A) DNS queries

B) IP addresses

C) Ports

D) TTL

Ans: A

150. **Zero-log policies limit:**

A) Forensic investigation

B) Video playback

C) RAM performance

D) Network speed

Ans: A

**50 3-Marks Questions and Answers

1. What is Network Forensics?

Answer:

- A branch of digital forensics focused on monitoring and analyzing network traffic.
- Used to detect intrusions, policy violations, and malicious activities.
- Helps reconstruct events by examining packets, logs, and network artifacts.

---

2. Define a network protocol. Give two examples.

Answer:

- A protocol is a set of communication rules used between devices.
- Ensures structured data exchange.
- Examples: TCP/IP, HTTP.

---

3. What is the role of TCP in communication?

Answer:

- Provides reliable, connection-oriented communication.
- Ensures ordered delivery and error correction.
- Uses acknowledgements and retransmissions.

---

4. What is the OSI model? Name its seven layers.

Answer:

- A conceptual networking framework.
- Layers: Physical, Data Link, Network, Transport, Session, Presentation, Application.

---

5. Why is the Physical Layer important in forensics?

Answer:

- Deals with hardware evidence (cables, NICs, signals).
- Helps detect physical tampering or connectivity issues.
- Essential for verifying link availability.

---

6. What is the Data Link Layer?

Answer:

- Handles MAC addressing and frame delivery within the same network.
- Controls error detection.
- Uses switches and NICs.

---

7. Define MAC address and its forensic importance.

Answer:

- A unique hardware identifier for network interfaces.
- Helps trace devices.
- Useful when IP addresses change dynamically.

---

8. What is an ARP Table?

Answer:

- A mapping of IP addresses to MAC addresses.
- Helps detect ARP spoofing.
- Stored on routers and hosts.

---

9. What is an Ethernet Switch Log?

Answer:

- Record of switch operations like port activity and MAC learning.
- Helps trace traffic paths.
- Useful in incident reconstruction.

---

10. Define Router Logs.

Answer:

- Logs maintained by routers for routing updates, interface status, and security events.
- Help detect unauthorized access.
- Useful for path tracing.

---

11. What are WiFi device logs used for?

Answer:

- Record wireless authentication and association events.
- Help identify connected devices.
- Useful for detecting rogue access points.

---

12. What is Syslog?

Answer:

- A standard for sending system logs to a server.
- Centralizes network device logs.
- Used for monitoring and incident detection.

---

13. What is Network Management System (NMS)?

Answer:

- Software for monitoring, controlling, and analyzing network devices.
- Provides alerts and performance statistics.
- Useful for anomaly detection.

---

14. Explain Promiscuous Mode.

Answer:

- NIC mode where all packets on the network are captured.
- Used in packet sniffing tools like Wireshark.
- Helps observe full traffic for analysis.

---

15. What is Port Mirroring?

Answer:

- Technique where a switch copies traffic from one port to another for monitoring.
- Used for real-time traffic analysis.
- Helps forensic investigators collect evidence.

---

16. What is Wireshark?

Answer:

- A packet capture and protocol analysis tool.
- Displays packets in detail (headers + payload).
- Useful for detecting intrusions and anomalies.

---

17. What is TCPDump?

Answer:

- A command-line packet capture tool.
- Used on Unix/Linux for sniffing live traffic.
- Generates raw packet data for forensic analysis.

---

18. Define Packet Sniffing.

Answer:

- Capturing network packets for analysis.
- Helps detect malicious traffic.
- Uses tools like Wireshark and TCPDump.

---

19. What are Scanning Tools? Give examples.

Answer:

- Tools used to identify open ports, services, and vulnerabilities.
- Examples: Nmap, Nessus.
- Useful in forensic investigations of attacks.

---

20. What is Network Snooping?

Answer:

- Monitoring network traffic without permission.
- Can be legitimate (forensics) or malicious (attacks).
- Detects unauthorized communications.

---

21. What is a Firewall Log?

Answer:

- Record of allowed and blocked traffic.
- Includes source/destination IPs, ports, timestamps.
- Helps detect intrusions and policy violations.

---

22. Define Network Layer in OSI model.

Answer:

- Responsible for logical addressing (IP).
- Handles routing.
- Devices: routers.

---

23. What is IP Spoofing?

Answer:

- Altering IP address to hide identity.
- Used in DoS, session hijacking.
- Makes forensic identification difficult.

---

24. What is Encryption? How does it affect forensics?

Answer:

- Converts plaintext into cipher text.
- Protects confidentiality.
- Forensics faces challenges in inspecting encrypted traffic.

---

25. What is Server Log Analysis?

Answer:

- Examining logs from web, application, or database servers.
- Helps detect unauthorized access.
- Provides timestamps and request details.

---

26. What are User Activity Logs?

Answer:

- Records of user logins, commands, and actions.
- Help trace insider threats.
- Stored by OS or applications.

---

27. Why is Browser History Analysis important?

Answer:

- Reveals visited websites and timestamps.
- Helps identify malicious downloads.
- Provides digital footprints.

---

28. What are Proxy Server Logs?

Answer:

- Logs of web requests made through proxy.
- Contain URLs, IP addresses, and timestamps.
- Useful in tracking user Internet behavior.

---

29. What are Antivirus Logs?

Answer:

- Records malware detections, quarantines, and scans.
- Help identify infection timelines.
- Provide threat signatures and file paths.

---

30. What are Email Logs?

Answer:

- Track email transmission details.
- Include sender, recipient, message ID, and time.
- Help investigate phishing and fraud.

---

31. Explain the role of timestamps in network forensics.

Answer:

- Provide chronological event order.
- Enable correlation across devices.
- Essential for incident reconstruction.

---

32. What is Audit Logging?

Answer:

- Recording system and user activities.
- Helps ensure accountability.
- Supports security and forensic investigations.

---

33. What are the challenges of encrypted traffic in forensics?

Answer:

- Packet payload becomes unreadable.
- Deep packet inspection fails.
- Requires decryption keys or endpoint analysis.

34. What is Log Retention and why is it important?

Answer:

- Storing logs for a fixed time period.
- Helps support legal investigations.
- Ensures availability for analysis.

35. What is Network Forensic Investigation Workflow?

Answer:

- Identification of incident.
- Collection of network artefacts.
- Analysis and reporting.

36. What is Packet Reconstruction?

Answer:

- Reassembling fragmented packets.
- Required for analyzing flows and sessions.
- Helps understand complete communication.

37. Define Session Reconstruction.

Answer:

- Rebuilding full conversations between hosts.
- Useful for analyzing chat, browsing, or file transfers.
- Performed using forensic tools.

38. Explain the concept of network metadata.

Answer:

- Data about data (IP, ports, protocol, length).
- Useful even when payload is encrypted.
- Helps identify communication patterns.

39. What is a Log Correlation?

Answer:

- Combining log data from multiple devices.
- Identifies multi-stage attacks.
- Uses SIEM tools.

40. What is SIEM?

Answer:

- Security Information and Event Management system.
- Aggregates and analyzes logs.
- Provides alerts and dashboards.

41. What is DHCP Log analysis used for?

Answer:

- Identifies device IP assignments.
- Useful when IP addresses are dynamic.
- Helps match MAC to IP.

42. What is DNS Log Analysis?

Answer:

- Examines domain lookups.
- Detects malicious domains (phishing, C2 servers).
- Helps track user browsing behavior.

43. How does spoofing affect network forensics?

Answer:

- Alters identity information (MAC/IP).
- Misleads investigators.
- Requires additional correlation for verification.

44. Explain mobility challenges in forensics.

Answer:

- Devices frequently change networks.
- Dynamic IPs and new access points complicate tracking.
- Logs may be distributed across multiple networks.

45. What is log tampering?

Answer:

- Deliberate modification or deletion of logs.
- Hides attacker activity.
- Requires integrity checks and backups.

46. What is Chain of Custody in network forensics?

Answer:

- Documentation of evidence handling.
- Ensures admissibility in court.
- Records collection, transfer, and storage steps.

47. What is Deep Packet Inspection (DPI)?

Answer:

- Examines packet headers and payload.
- Detects anomalies and policy violations.
- Limited when traffic is encrypted.

48. What are Privacy Laws in network forensics?

Answer:

- Regulations controlling data monitoring & retention.
- Examples: GDPR, IT Act 2000 (India).
- Require consent, minimization, and proper use.

49. What is Log Normalization?

Answer:

- Converting logs to a standard format.
- Makes analysis easier.
- Used by SIEM systems.

50. Why does storage limitation affect network forensics?

Answer:

- High-volume traffic generates huge data.
- Logs may be overwritten quickly.
- Leads to incomplete forensic evidence.

50 5-Marks Questions & Answers (Network Forensics & Networking Concepts)

1. What is Network Forensics? Explain its objectives.

Answer:
Network Forensics involves capturing, recording, and analyzing network events to discover evidence of security breaches or policy violations. Its objectives include:

- Identifying intrusion sources
- Reconstructing attack steps
- Preserving evidence for legal use
- Monitoring abnormal activities
- Detecting policy violations and malware communication

2. Differentiate between Network Forensics and Computer Forensics.

Answer:

- Network forensics deals with **live network data**, while computer forensics focuses on **stored data** on devices.
- Network forensics captures **volatile data** (packets, sessions), whereas computer forensics captures **static data** (files, disks).
- Network forensics requires **continuous monitoring**, while computer forensics is often **post-incident**.
- Tools differ: Wireshark/TCPDump vs. EnCase/FTK.

3. Explain the importance of reviewing networking concepts before studying network forensics.

Answer:
Understanding networking concepts helps analysts interpret packet structures, protocols, OSI architecture, routing behavior, and traffic anomalies. Without this foundation, identifying malicious patterns such as scanning, spoofing, ARP poisoning, or abnormal routing becomes difficult.

4. What is the OSI model? Explain its relevance to network forensics.

Answer:
The OSI model defines 7 layers of communication. In forensics, it helps analysts:

- Identify where attacks occur (e.g., ARP at Layer 2).
- Examine logs layer-wise (router logs = Layer 3).
- Analyze protocols specific to each layer.
- Map packet data to OSI structure during investigation.

5. Explain TCP/IP model layers and their significance in network forensics.

Answer:
TCP/IP has 4 layers (Link, Internet, Transport, Application). Forensics relevance:

- **Link:** MAC addresses, ARP, Ethernet frames
- **Internet:** IP addresses, routing, fragmentation
- **Transport:** TCP/UDP ports, sessions
- **Application:** HTTP, DNS, SMTP logs

6. What is a network protocol? Give examples and forensic relevance.

Answer:
Protocols define communication rules. Examples: HTTP, DNS, TCP, ARP. In forensics, analyzing protocol behavior helps detect anomalies like DNS exfiltration, TCP retransmission attacks, or ARP spoofing.

---

7. Describe the role of Wireshark in network forensics.

Answer:
Wireshark is a packet analyzer used to capture and inspect network packets. It helps identify attack signatures, reconstruct sessions, filter malicious traffic, detect scanning, observe payloads, analyze protocol behavior, and export evidence.

---

8. What is TCPDump? How is it used in investigations?

Answer:
TCPDump is a command-line packet capture tool. It captures raw packets using filters. Investigators use it to monitor suspicious traffic, collect evidence during live attacks, and capture packets for offline analysis.

---

9. Explain Syslog and its significance in network forensics.

Answer:
Syslog is a standard protocol for sending log messages. It centralizes logs from routers, firewalls, switches, and servers. Analysts use Syslog for timeline analysis, detecting suspicious login attempts, configuration changes, or traffic anomalies.

---

10. What is Network Management System (NMS)? Describe its forensic use.

Answer:
NMS manages and monitors network devices. It provides alerts, bandwidth reports, SNMP logs, and topology maps. Forensics uses NMS to track historical device behavior, outages, unauthorized access, or abnormal traffic surges.

---

11. Explain Promiscuous Mode in network monitoring.

Answer:
Promiscuous mode allows NICs to capture all network packets, not just those addressed to them. It is essential for forensics to record complete traffic but can also be exploited by attackers for sniffing.

---

12. What is Port Mirroring? How is it useful in investigations?

Answer:
Port mirroring duplicates traffic from one switch port to another. Investigators attach analyzers to the mirrored port to capture complete traffic without interrupting the network.

---

13. Define network snooping and give tools used.

Answer:
Network snooping means intercepting and inspecting data packets. Tools include Wireshark, Ettercap, and tcpdump. It is used to detect anomalies, perform investigations, and analyze protocol misuse.

---

14. What are scanning tools? Give examples and forensic relevance.

Answer:
Scanning tools identify network ports, services, and vulnerabilities. Examples: Nmap, Nessus. They detect attacker reconnaissance patterns and help validate system exposure.

---

15. What is captured in Data Link Layer forensics?

Answer:
Layer 2 evidence includes:

- MAC addresses
- Ethernet frames
- VLAN tags
- ARP packets
  Useful for detecting MAC spoofing, ARP poisoning, and switch attacks.

---

16. Explain the importance of analyzing Physical Layer in forensics.

Answer:
Physical layer evidence includes cable connections, signal integrity, physical tampering, device theft, and damaged hardware. Forensics ensures availability and integrity of network infrastructure.

---

17. What are Ethernet Switch Logs? What can they reveal?

Answer:
Switch logs record port activity, errors, VLAN changes, MAC learning events, port security violations. They help detect unauthorized device connections or abnormal broadcast storms.

---

18. Describe MAC Table analysis in network forensics.

Answer:
MAC tables map MAC addresses to switch ports. Investigation uses MAC tables to:

- Trace devices
- Detect spoofed addresses
- Identify rogue systems
- Establish communication timelines

---

19. Explain significance of ARP Table in forensics.

Answer:
ARP tables map IP-MAC pairs. Investigators use them to detect ARP spoofing, MITM attacks, rogue gateways, and inconsistencies between real and spoofed devices.

---

20. What is examined in Network Layer forensics?

Answer:
Layer 3 analysis includes:

- IP routing
- Packet headers
- TTL values
- Fragmentation
  Detects spoofing, scanning, route hijacking, DoS attacks.

---

21. Describe Router Logs and their forensic importance.

Answer:
Router logs record routing updates, access control hits, interface status, NAT translations. They help trace attacker movements, identify dropped packets, and reconstruct routing events.

---

22. What are WiFi device logs used for in investigations?

Answer:
They reveal:

- Authentication failures
- Connected devices
- MAC addresses
- Channel interference
  Useful for detecting rogue APs, unauthorized access, and wireless attacks.

---

23. Explain Firewall logs and what evidence they provide.

Answer:
Firewall logs show allowed/blocked traffic, source/destination IPs, ports, and protocols. They help detect scanning, brute force, malware communication, and intrusion attempts.

---

24. Why are OS audit features important in forensics?

Answer:
They record system calls, login attempts, privilege changes, file access events. These logs reconstruct user activities and identify malicious behavior.

---

25. Explain enabling and examining server logs.

Answer:
Servers log authentication, application errors, access logs, and configuration changes. Forensics uses these logs to track intrusions, malware execution, and unauthorized file access.

---

26. What are user activity logs and why are they important?

Answer:
These logs include login times, command history, file access. They help confirm or disprove suspect actions and identify insider threats.

---

27. Explain browser history analysis in network forensics.

Answer:
Browser history reveals visited URLs, cookies, downloads, cached files. Investigators reconstruct user behavior, phishing attempts, or malware downloads.

---

28. Describe proxy server logs in investigations.

Answer:
Proxy logs show HTTP requests, timestamps, destination URLs, and user IDs. They help track browsing behavior, data exfiltration attempts, or policy violations.

---

29. Explain antivirus logs and their forensic value.

Answer:
Antivirus logs capture malware detections, quarantine events, scan reports, and signature updates. Analysts identify infection sources and malware behavior.

---

30. Describe email logs and their relevance to forensic analysis.

Answer:
Email logs record sender/receiver information, IPs, timestamps, and spam filtering results. They help analyze phishing, spoofing, or insider data leak cases.

---

31. What is encryption? How does it challenge network forensics?

Answer:
Encryption secures data by converting it into unreadable form. Challenges:

- Payload cannot be inspected
- SSL/TLS hides malicious commands
- Requires keys for decryption
- Limits DPI and traffic reconstruction

32. Explain spoofing and its impact on network forensics.

Answer:
Spoofing falsifies IP/MAC addresses to hide identity. It makes attribution difficult, complicates packet tracing, and enables MITM attacks.

33. How does network mobility affect forensic investigations?

Answer:
Mobile devices frequently change IPs, locations, and networks. Logs become distributed, tracking becomes difficult, and evidence may be incomplete.

34. Explain storage limitations in network forensics.

Answer:
Network captures generate huge data. Limited storage leads to overwritten logs, incomplete evidence, difficulty in long-term monitoring, and potential legal issues.

35. How do privacy laws affect network forensics?

Answer:
Laws like GDPR restrict capturing personal data, require consent for monitoring, impose retention limits, and restrict cross-border log sharing.

36. What is packet analysis and how is it performed?

Answer:
Packet analysis involves examining headers and payloads using tools like Wireshark. Filters, protocol decoders, and stream reassembly reconstruct communication patterns.

37. What is log correlation? Why is it important?

Answer:
Log correlation merges data from multiple sources (firewall, router, OS logs). It reveals full attack paths, timelines, patterns, and relationships between events.

38. Explain deep packet inspection (DPI).

Answer:
DPI inspects packet payloads to detect anomalies, malware signatures, or policy violations. It is vital for forensics but limited by encryption.

---

39. What is flow analysis (NetFlow)?

Answer:
NetFlow records communication flows (source/destination IPs, ports, bytes transferred). It helps detect scanning, DDoS, exfiltration, and unusual traffic patterns.

---

40. Describe intrusion detection systems (IDS) logs.

Answer:
IDS logs show alerts for signatures, anomalies, rule matches, and suspicious patterns. They are used to detect attacks early and verify intrusion attempts.

---

41. What is chain of custody in network forensics?

Answer:
Chain of custody maintains legal integrity of evidence. It documents collection, handling, timestamps, and access history, ensuring admissibility in court.

---

42. Explain session reconstruction in forensics.

Answer:
Rebuilding communication streams from packet captures reveals user actions, commands, file transfers, and attacker behavior.

---

43. What are time-stamps and why are they critical in forensics?

Answer:
Timestamps allow event sequencing, correlate logs, identify attack windows, and detect tampering or anomalies in activities.

---

44. Explain log retention policy.

Answer:
Defines how long logs are stored. Helps balance storage costs, forensic reliability, and legal compliance.

---

45. What is DoS/DDoS attack analysis in network forensics?

Answer:
Investigators analyze traffic spikes, SYN floods, botnet patterns, and source diversity. Logs help identify attack vectors and mitigation needs.

46. Explain ARP spoofing detection in forensics.

Answer:
Detected through incorrect ARP table entries, duplicate MAC addresses, sudden ARP broadcasts, and mismatch between IP–MAC bindings.

47. What is DNS forensics?

Answer:
DNS logs reveal domain lookups, suspicious queries, fast-flux domains, or malware command & control (C2) activity.

48. Explain tunneling and its forensic challenges.

Answer:
Tunneling hides data inside other protocols (e.g., DNS tunneling). Forensics challenges include encrypted payloads, hidden exfiltration, and hard-to-detect communication.

49. What is anomaly-based analysis?

Answer:
Detects deviations from normal traffic patterns, helping identify zero-day attacks, malware behavior, and insider threats.

50. Explain the end-to-end process of a network forensic investigation.

Answer:
Steps include:

1. Identification
2. Preservation (packet capture, log retention)
3. Collection (tools, mirroring)
4. Analysis (protocols, logs, correlations)
5. Documentation
6. Reporting
   Ensures complete, legal, and accurate findings.