

Task 3: Networking Basics for Cyber Security

Task Execution

1. Learn Basic Networking Concepts

- IP Address: Identifies a device on a network.
- MAC Address: Physical address of a network interface.
- DNS: Resolves domain names into IP addresses.
- TCP: Reliable, connection-oriented protocol.
- UDP: Fast, connectionless protocol.

2. Capture Live Network Traffic

- Install Wireshark.
- Run Wireshark as administrator.
- Select an active network interface (Wi-Fi or Ethernet).
- Start capturing live packets.

The screenshot shows the Wireshark interface with the following details:

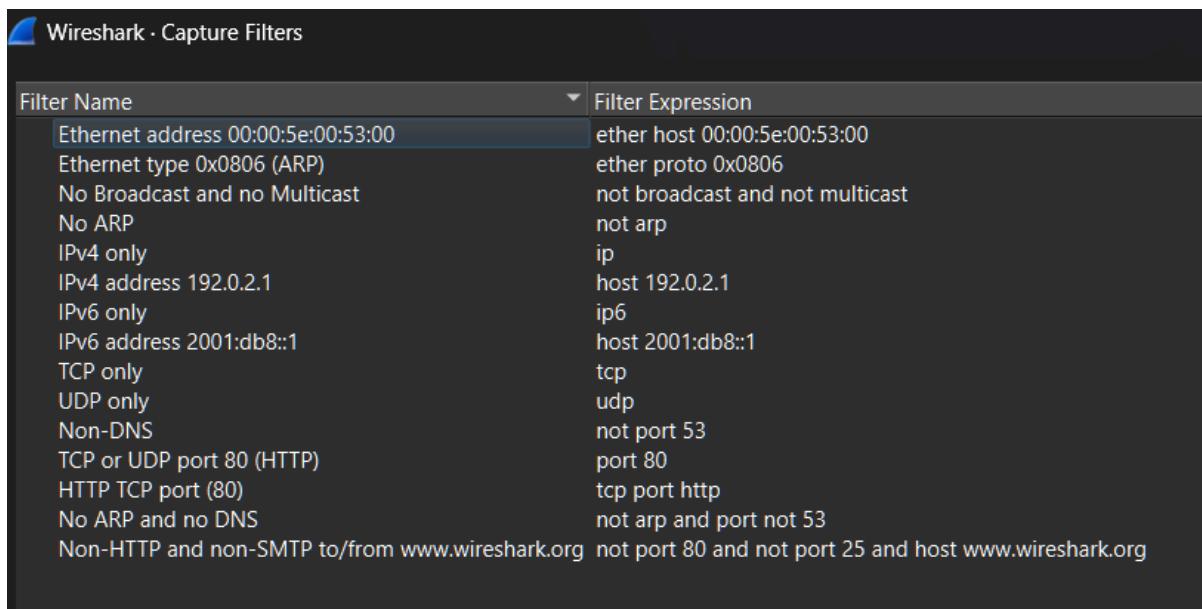
- Capturing from Wi-Fi**: The interface being used for capturing.
- File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help**: The menu bar.
- Apply a display filter ... <Ctrl-/>**: The display filter input field.
- Packet List**: Shows a list of 94 captured frames. Frame 76 is highlighted in red, showing a Client Hello message to port 443. Frame 94 is highlighted in red, showing a RST, ACK message.
- Details**: Shows the detailed structure of the selected frame (Frame 76).
- Bytes**: Shows the raw byte representation of the selected frame.
- Status**: Shows the status bar at the bottom indicating the capture is from the Wi-Fi interface \Device\NPF_{08e...}.

3. Filter Packets by Protocol

Use display filters in Wireshark:

- http
- dns
- tcp

This helps analyze specific types of traffic.



4. Observe TCP Three-Way Handshake

Identify the following TCP flags:

1. SYN
2. SYN-ACK
3. ACK

This handshake establishes a TCP connection between client and server.

TCP packets showing SYN, SYN-ACK, and ACK flags.

5. Identify Plain-Text vs Encrypted Traffic

- HTTP: Data is visible in plain text.
 - HTTPS: Data is encrypted and not readable.
-
- HTTP traffic showing readable data.
 - HTTPS/TLS traffic showing encrypted data.

6. Capture and Analyze DNS Queries

- Apply the dns filter.
- Open a website in a browser.
- Observe DNS queries and responses with IP addresses.

DNS query and response visible in Wireshark.

This file is mandatory for submission.

7. Write Observations in Simple Language

Write short observations based on what you captured.

```
Checksum: 0x262f [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
▼ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▶ TCP Option - No-Operation (NOP)
  ▶ TCP Option - No-Operation (NOP)
  ▶ TCP Option - Timestamps: TStamp 824635422, TSectr 3249934137
▼ [SEQ/ACK analysis]
  [This is an ACK to the segment in frame: 15]
  [The RTT to ACK the segment was: 0.002592000 seconds]
▼ [TCP Analysis Flags]
  ▼ [Expert Info (Warning/Sequence): Previous segment not captured (common at capture start)]
    [Previous segment not captured (common at capture start)]
    [Severity level: Warning]
    [Group: Sequence]
```

Tools Used

- Primary Tool: Wireshark
- Alternative Tools: tcpdump, Microsoft Network Monitor

Task Execution (According to Given Steps)

1. Learn Basic Networking Concepts

- IP Address: Identifies a device on a network.
- MAC Address: Physical address of a network interface.
- DNS: Resolves domain names into IP addresses.
- TCP: Reliable, connection-oriented protocol.
- UDP: Fast, connectionless protocol.

2. Capture Live Network Traffic

- Install Wireshark.
- Run Wireshark as administrator.
- Select an active network interface (Wi-Fi or Ethernet).
- Start capturing live packets.

Live packet capture running in Wireshark.

3. Filter Packets by Protocol

Use display filters in Wireshark:

- http
- dns
- tcp

This helps analyze specific types of traffic.

Protocol filter applied (HTTP, DNS, or TCP).

4. Observe TCP Three-Way Handshake

Identify the following TCP flags:

1. SYN
2. SYN-ACK
3. ACK

This handshake establishes a TCP connection between client and server.

TCP packets showing SYN, SYN-ACK, and ACK flags.

5. Identify Plain-Text vs Encrypted Traffic

- HTTP: Data is visible in plain text.
- HTTPS: Data is encrypted and not readable.
- HTTP traffic showing readable data.
- HTTPS/TLS traffic showing encrypted data.

6. Capture and Analyze DNS Queries

- Apply the dns filter.
- Open a website in a browser.
- Observe DNS queries and responses with IP addresses.
DNS query and response visible in Wireshark.