OSI Layer Packet Simulation using Wireshark

Mini-Project: Cybersecurity Lab

Made by: Raghunandan Sharma
Roll number: 2023A7R020
Branch: CSE-Cybersecurity

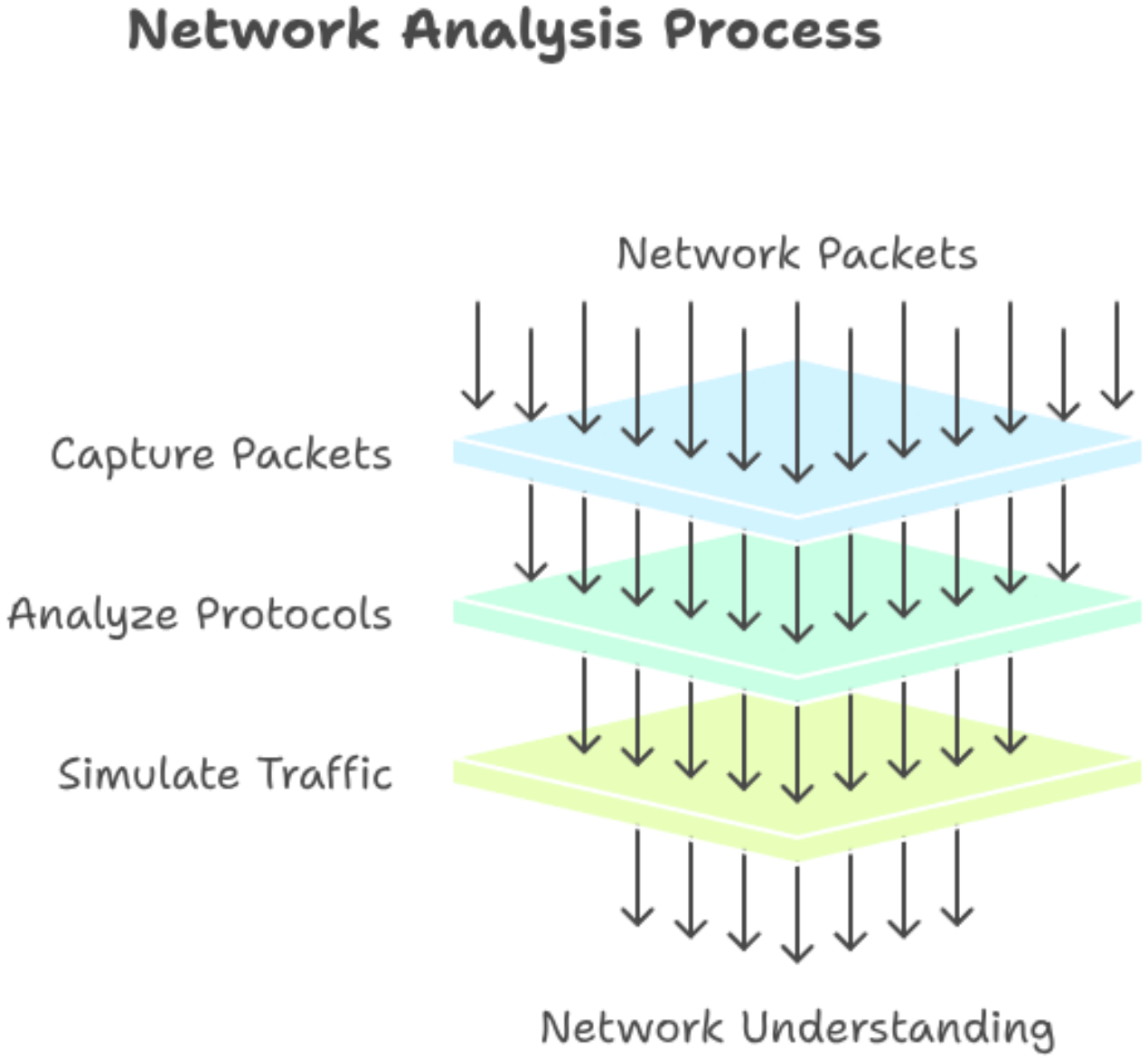
Objectives and Tools Used

Objective:

- Capture and analyze packets at different OSI layers.
- Identify protocols and simulate basic traffic

Tools Used:

- Wireshark
- Netcat
- Curl
- Ping
- Telnet



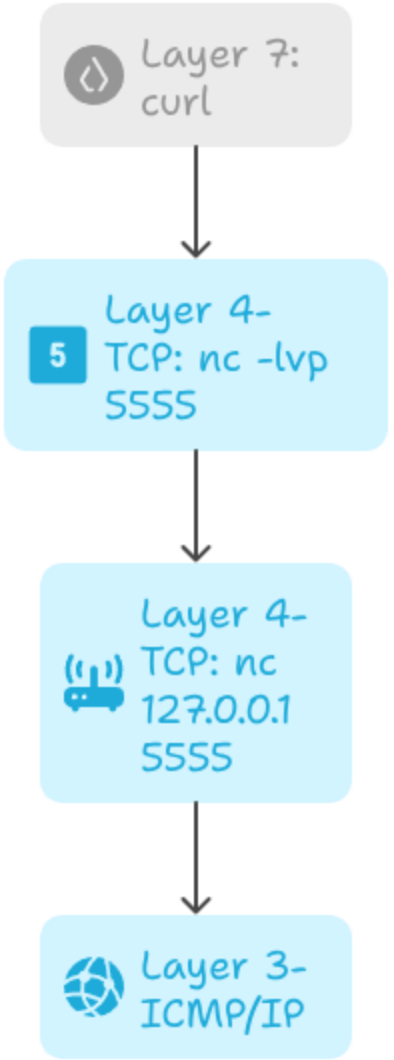
OSI Layers and Protocols Mapped

OSI Layer	Protocol Used	Tool/Command	Wireshark Filter
Layer 7	HTTP, Telnet	curl, telnet	http, telnet
Layer 4	TCP	nc	tcp.port == 5555
Layer 3	ICMP/IP	ping	icmp, ip
Layer 2	Ethernet	auto	eth.addr == ...

Commands Used for Simulation

- Layer 7: curl http://example.com
- Layer 4-TCP: nc -lvp 5555 # Terminal 1

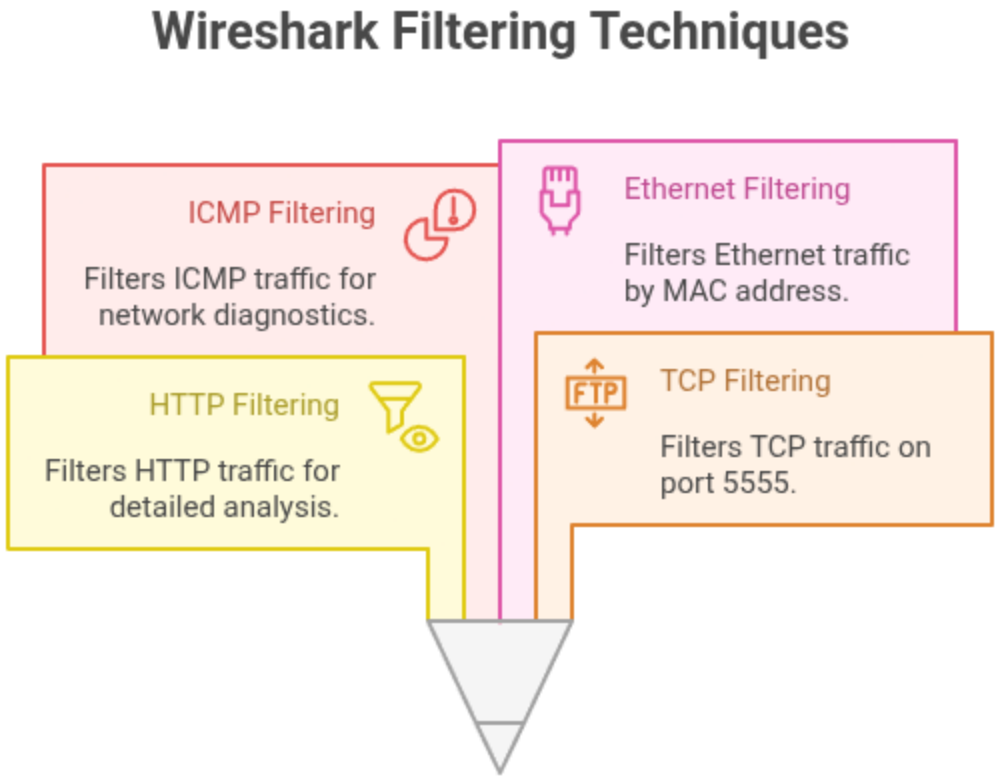
  nc 127.0.0.1 5555 # Terminal 2
- Layer 3-ICMP/IP:



Packet Captures & Filters

Wireshark Filters and Captures:

- HTTP → Filter: `http`
- TCP (Netcat) → Filter: `tcp.port == 5555`
- ICMP (Ping) → Filter: `icmp`
- Ethernet → Filter: `eth.addr == xx:xx:xx:xx`



Observations & Analysis

Observations and Analysis:

- HTTP shows GET/Response packets clearly
- TCP shows 3-way handshake and data transmission
- Ping generates ICMP Echo and Reply
- Ethernet frames show source/destination MACs
- Protocols can be linked to specific OSI layers using filters

Conclusion & Submission Links

- Learned real-time protocol behavior per OSI layer
- Understood how to use Wireshark for practical packet analysis
- Tools like Netcat, Ping, Curl proved useful
- ***Deliverables:***
  - `.pcap` file
  - Screenshot PDF of captures
  - Protocol mapping report (tabular)
  - Link for the output link:

https://drive.google.com/file/d/1lB99aVpQqFNY6C-_WhqEiRMvnpVCgZ6o/view?usp=sharing