Name : Patel Dhruv Nirmalkumar
Email : dhruvpatel.00700@gmail.com
Phone : 9426176903
Task : 3

Tool Used: Wireshark
PCAP File: dos1.pcap

Basic Networking Concepts (Observed from PCAP)

IP Address

- IP addresses identify devices on the network.
- In dos1.pcap, one destination IP receives a very large number of packets.
- This indicates a single target system.

MAC Address

- MAC addresses appear in Ethernet frames.
- Source MAC addresses may repeat or appear spoofed in attack traffic.

TCP

- TCP packets are visible with flags like SYN.
- Many TCP connections are initiated but not completed.

UDP

- Some DoS attacks use UDP because it is faster and connectionless.
- If present, UDP packets appear without handshakes.

DNS

- DNS packets, if present, show domain name lookups in plain text.

Capturing Live Network Traffic

Since a PCAP file is already provided:

- Live capture is not performed.
- The PCAP represents traffic that was already captured during a network event.
- This approach is commonly used in forensic analysis.

Observation:
The PCAP contains abnormal traffic, not normal user browsing.

Filtering Packets by Protocol

TCP Filter

tcp

Observation:

- Large number of TCP packets
- Many SYN packets
- Few completed connections

DNS Filter

dns

Observation:

- If DNS traffic exists, domain names are visible in plain text
- Repeated queries may indicate automated behavior

HTTP Filter

http

Observation:

- Little or no normal HTTP browsing traffic
- Confirms traffic is attack-focused, not user-focused

Three-Way TCP Handshake

Normal TCP Handshake

1. SYN
2. SYN-ACK
3. ACK

Observation in dos1.pcap

- Many SYN packets
- Very few SYN-ACK packets
- Almost no ACK packets

Conclusion:
The handshake is intentionally left incomplete, which is a common DoS technique.

Plain-text vs Encrypted Traffic

Plain-text Traffic

- DNS queries (domain names readable)
- Some TCP headers fully visible

Encrypted Traffic

- No meaningful HTTPS payloads observed
- Payload data is either empty or irrelevant

Key Insight:
DoS attacks focus on volume, not data content.

DNS Queries and Analysis

Observations

- DNS packets may show repeated domain lookups
- Queries are visible in readable text
- UDP is commonly used for DNS

Security Meaning

- Repeated DNS queries can indicate DNS flooding or amplification attempts.

Saving Packet Captures

- The traffic is saved as dos1.pcap
- PCAP files preserve packet structure and timestamps
- Used for:
    - Attack investigation
    - Evidence collection
    - Training and analysis

Final Observations

- The network traffic is abnormal.
- One system is targeted with excessive packets.
- TCP connections are not completed.
- Traffic pattern is automated, not human.
- This behavior matches a Denial of Service attack.