POC: Network IDS – Weekly Task

Name: Purva Ramchandra Pawaskar
Intern Id: 259

Objective

The purpose of this task is to build a **lightweight Network Intrusion Detection System (NIDS)** that can monitor live network traffic or analyze packet captures (PCAP files). The system detects common suspicious activities, such as:

- **ICMP traffic** (ping echo requests/replies)
- **TCP connection attempts** (SYN packets and half-open connections)
- **Common scan patterns** (SYN, NULL, FIN scans, repeated port attempts)
- **Suspicious behaviors** (ICMP floods, SYN floods)

Detection Logic

The NIDS was implemented in Python using the **Scapy** library. Detection logic includes:

1. **ICMP Detection**
    - Normal echo requests and replies are logged.
    - If more than **5 ICMP packets within 5 seconds** from one host → flagged as **ICMP flood**.
2. **TCP Connection Attempts**
    - SYN packets (flags & 0x02) are logged as connection attempts.
    - If more than **10 SYNs within 5 seconds** from one host → flagged as **SYN scan**.
3. **Scan Pattern Detection**
    - **NULL scan**: TCP packet with no flags.
    - **FIN scan**: TCP packet with FIN flag set.

Implementation

- Code: nids_poc.py (Python 3 + Scapy).
- Modes of operation:

- **Live sniffing** (using sniff())
- **Offline PCAP analysis** (using rdpcap())
- **CMD Test** (ping 127.0.0.1)

Demo

1. **Normal Traffic PCAP (icmp.pcap)**
   - Shows simple ICMP requests/replies without alerts.
2. **Attack Traffic PCAP (nmap_scan.pcap)**
   - SYN scans trigger [ALERT] SYN scan detected.
   - NULL and FIN scans generate corresponding alerts.
   - ICMP flood detection triggers if packet volume exceeds threshold.

Example Output:

[ICMP] Ping 192.168.1.20 -> 8.8.8.8

[ALERT] ICMP flood from 192.168.1.20

[TCP] SYN 192.168.1.30 -> 192.168.1.10:22

[ALERT] SYN scan detected from 192.168.1.30

[ALERT] NULL scan 192.168.1.40 -> 192.168.1.10:443

False Positives Considerations

- **High-volume legitimate traffic** (e.g., many HTTP connections) may appear similar to SYN scans.
- **Bulk ICMP monitoring tools** could trigger ICMP flood alerts.
- Thresholds (ICMP_THRESHOLD, SYN_THRESHOLD) should be tuned to reduce noise.