Title Network IDS

Name : **Lavanya Chilukamari**

Intern ID : **308**

Objective

Build a lightweight Intrusion Prevention System (IPS) that not only detects but also

blocks malicious traffic in real time.

The IPS should:

- Block ICMP ping floods.
- Drop repeated TCP SYN floods or half-open connections.
- Prevent simple scan patterns (SYN/NULL/FIN/Xmas scans, repeated/multiport attempts).
- Enforce simple rules to block suspicious HTTP payloads (e.g., SQL injection,
- XSS).

Required Modules

- **scapy** → for reading and analyzing packets from PCAP files.
- Install using:
- pip install scapy
- **re** → for regex-based payload inspection.
- **collections** → for tracking connections and port attempts.

Main Parts of the Code

1. Packet Reading

- Uses rdpcap() from Scapy to load packets from .pcap files.

2. ICMP Handling

- Blocks ICMP ping floods.

3. TCP Scan Detection

- Detects and blocks SYN floods, NULL scans, FIN scans, Xmas scans.
- Tracks source IPs scanning multiple ports (multi-port scan detection).

4. Payload Inspection

- Uses regex to identify malicious patterns in HTTP payloads (e.g., SQL injection, XSS).

5. Output

- For every packet, prints whether the action is ALLOW or BLOCK with
- the reason.

How to Run

1. Save the code as network_ips.py.
2. Place PCAP files (e.g., normal.pcap, nmap_zombie_scan.pcap) in the same folder.
3. Run the IPS:

python3 network_ips.py

Deliverables

1. Demo

- Run against at least two PCAPs.
    - Normal traffic → mostly **ALLOW**.
    - Malicious traffic (Nmap scan, ICMP flood) → multiple **BLOCK** messages.

2. Short Report (1–2 pages)

- Describe prevention logic (ICMP block, TCP scan detection, payload
  filtering).
- Mention false-positive handling (e.g., legitimate pings may be blocked,
  payload regex may overmatch).
- Suggest improvements (stateful inspection, ML-based anomaly detection, logging).

3. Unit/Integration Tests

- Write test cases for functions like:
    - ICMP detection.
    - TCP scan detection.
    - Suspicious payload regex detection.