Proof of Concept – Network Intrusion Prevention System (IPS)

Name: Chanchal Teli

Intern ID: 125

1. Objective

The objective of this PoC is to design and implement a simple Intrusion Prevention System (IPS) that can detect and block basic malicious network activities.

The IPS is expected to:

- Block ICMP ping floods (common DoS technique).
- Block TCP SYN floods (half-open connection attacks).
- Detect and block port scanning attempts.
- Identify and block suspicious HTTP payloads such as SQL injection patterns.

This project is aimed at demonstrating the core concepts of an IPS in an understandable way, suitable for learning and small-scale testing.

2. Tools Used

- Programming Language: Python 3
- Library: Scapy (for packet capturing and analysis)
- Traffic Data: PCAP files (benign and malicious samples)
- Simulation Tools for Attacks:
  - ping (for ICMP flood)
  - hping3 (for SYN flood)
  - nmap (for port scanning)
  - curl or browser with crafted query (for SQL injection attempt)
- Platform: Linux/Windows/Mac with Python environment

3. Working of the IPS

The IPS works by analyzing packets from PCAP files (or live traffic) and applying rule-based detection. The process is as follows:

3.1 Packet Analysis

- Packets are read one by one.
- The system checks whether the packet is ICMP, TCP, or HTTP.

3.2 Detection Logic

1. ICMP Flood Detection
    - Count the number of ICMP Echo Requests per source IP.
    - If more than 20 pings are observed, mark it as a flood → block the source.
2. SYN Flood Detection
    - Count TCP SYN packets per source IP.
    - If more than 50 SYN packets are detected, consider it a SYN flood → block the source.
3. Port Scan Detection
    - Track the number of unique destination ports accessed by each IP.
    - If more than 15 unique ports are contacted, consider it a scan → block the source.
4. Suspicious HTTP Payload Detection
    - Monitor HTTP traffic (port 80).
    - If the payload contains suspicious SQL injection patterns such as UNION, SELECT, OR 1=1, DROP TABLE, block the source IP.

3.3 Blocking Action

- When any rule is triggered, the source IP is added to a blocklist.
- Any future traffic from this IP is ignored/dropped.
- A summary of blocked IPs is generated at the end.

4. Testing and Validation

4.1 Test Setup

- Benign Traffic PCAP: Contains only normal browsing and DNS queries.
- Malicious Traffic PCAP: Contains simulated attacks (ICMP flood, SYN flood, port scan, SQL injection attempt).

4.2 Expected Results

- Benign PCAP: No IPs blocked.
- Malicious PCAP: Each type of malicious activity is detected and blocked.

4.3 Results Obtained

- Benign Traffic:
    - System did not block any IPs.
    - ✅ Correct behavior, no false positives.
- Malicious Traffic:
    - Detected ICMP flood and blocked the attacker’s IP.
    - Detected SYN flood and blocked the attacker’s IP.
    - Detected port scan and blocked the attacker’s IP.
    - Detected suspicious SQL injection payload and blocked the attacker’s IP.
    - ✅ Correctly identified and blocked all malicious traffic.

5. False Positives and Limitations

False Positives

- ICMP-based monitoring tools may trigger false detection.
- High-volume legitimate web traffic may resemble SYN floods.
- Authorized security scans may appear as port scans.
- Queries containing SQL keywords in normal traffic may be falsely flagged.

Limitations

- Thresholds are static and not adaptive to normal network usage.
- Cannot inspect encrypted HTTP traffic (HTTPS).
- Blocking is simulated with a blocklist (no direct firewall integration in this PoC).
- Advanced evasion techniques by attackers are not covered.

6. Future Improvements

- Adaptive thresholds to reduce false positives.
- Whitelist mechanism for trusted IPs.
- Integration with firewall rules (e.g., iptables for Linux).
- Extended payload inspection for detecting XSS, command injection, etc.
- Logging & Reporting: Export results to CSV/JSON for auditing.
- Visualization Dashboard for better monitoring.

7. Conclusion

This PoC successfully demonstrates a basic Intrusion Prevention System that:

- Detects and blocks ICMP floods, SYN floods, port scans, and simple SQL injection attempts.
- Works on both benign and malicious PCAP files.
- Provides a foundation for understanding IPS concepts.