Proof of Concept (PoC) – Network IPS

This document explains how to run a simple Proof of Concept (PoC) Intrusion Prevention System (IPS). The IPS inspects packets from a PCAP file (e.g., nmap_zombie_scan.pcap) and blocks malicious traffic patterns.

Required Modules

1. scapy → for reading and analyzing packets from PCAP files.

Install using:

pip install scapy

Main Parts of the PoC Code

1. Import and Read Packets: Uses rdpcap() from scapy to load all packets.

2. Track Connections: Maintains a dictionary to record which IPs are scanning which ports.

3. Detection Logic: If one source IP scans too many ports, the action is marked as BLOCK.

4. Output: Prints whether a packet is ALLOW or BLOCK.

How to Run in IDLE

1. Save the Python script as ips_poc.py.

2. Place the PCAP file (e.g., nmap_zombie_scan.pcap) in the same folder.

3. Open the script in IDLE.

4. Run using F5 or Run → Run Module.

5. The output will display whether traffic is ALLOW or BLOCK.

Example Output

[32] 192.168.100.101 -> 192.168.100.1 : BLOCK: multi-port scan

```
[*] Reading packets from nmap_zombie_scan.pcap ...
[*] Total packets: 42

[0] Non-IP packet : ALLOW
[1] Non-IP packet : ALLOW
[2] Non-IP packet : ALLOW
[3] Non-IP packet : ALLOW
[4] 192.168.100.103 -> 192.168.100.101 : ALLOW
[5] 192.168.100.101 -> 192.168.100.103 : ALLOW
[6] 192.168.100.103 -> 192.168.100.101 : ALLOW
[7] 192.168.100.101 -> 192.168.100.103 : ALLOW
[8] 192.168.100.103 -> 192.168.100.101 : ALLOW
[9] 192.168.100.101 -> 192.168.100.103 : ALLOW
[10] 192.168.100.103 -> 192.168.100.101 : ALLOW
[11] 192.168.100.101 -> 192.168.100.103 : ALLOW
[12] 192.168.100.103 -> 192.168.100.101 : ALLOW
[13] 192.168.100.101 -> 192.168.100.103 : ALLOW
[14] 192.168.100.103 -> 192.168.100.101 : ALLOW
[15] 192.168.100.101 -> 192.168.100.103 : ALLOW
[16] 192.168.100.102 -> 192.168.100.101 : ALLOW
[17] 192.168.100.101 -> 192.168.100.102 : ALLOW
[18] 192.168.100.102 -> 192.168.100.101 : ALLOW
[19] 192.168.100.101 -> 192.168.100.102 : ALLOW
[20] 192.168.100.102 -> 192.168.100.101 : ALLOW
[21] 192.168.100.101 -> 192.168.100.102 : ALLOW
[22] 192.168.100.102 -> 192.168.100.101 : ALLOW
[23] 192.168.100.101 -> 192.168.100.102 : ALLOW
[24] 192.168.100.103 -> 192.168.100.101 : ALLOW
[25] 192.168.100.101 -> 192.168.100.103 : ALLOW
[26] Non-IP packet : ALLOW
[27] Non-IP packet : ALLOW
[28] 192.168.100.101 -> 192.168.100.102 : ALLOW
[29] 192.168.100.103 -> 192.168.100.101 : ALLOW
[30] 192.168.100.101 -> 192.168.100.103 : ALLOW
[31] 192.168.100.103 -> 192.168.100.101 : ALLOW
[32] 192.168.100.101 -> 192.168.100.103 : BLOCK: multi-port scan
[33] 192.168.100.103 -> 192.168.100.101 : ALLOW
[34] 192.168.100.101 -> 192.168.100.103 : BLOCK: multi-port scan
[35] 192.168.100.101 -> 192.168.100.102 : BLOCK: multi-port scan
[36] 192.168.100.103 -> 192.168.100.101 : ALLOW
[37] 192.168.100.101 -> 192.168.100.103 : BLOCK: multi-port scan
[38] 192.168.100.103 -> 192.168.100.101 : ALLOW
[39] 192.168.100.101 -> 192.168.100.103 : BLOCK: multi-port scan
[40] 192.168.100.103 -> 192.168.100.101 : ALLOW
[41] 192.168.100.101 -> 192.168.100.103 : BLOCK: multi-port scan
```

Name: Shreya Bishwas Pandey

Intern ID:120