PoC – Lightweight Network IDS

Objective

Demonstrate a Python-based Network IDS that detects:
1. ICMP pings (echo requests/replies)
2. TCP connection attempts (SYN packets)
3. Port scans (SYN, NULL, FIN scans)
4. Suspicious high-rate activity (floods or repeated scans)

1. Tool Overview

Name: Lightweight Network IDS (Python + Scapy)

Purpose: Monitor network traffic from a PCAP file and raise alerts for suspicious activity.

Input: .pcap file containing captured network traffic.

Output: Alerts printed in IDLE showing source/destination IPs and suspicious behavior.

2. How the Code Works

Step-by-Step

1. Import Scapy to read and analyze packets:
```
from scapy.all import rdpcap, TCP, ICMP
```

2. Read packets from the PCAP file given by the user:
```
pcap_file = input("Enter PCAP file path: ")
packets = rdpcap(pcap_file)
```

3. Check each packet:
   * If ICMP → print ping requests/replies.
   * If TCP SYN → print connection attempts and detect SYN scans.
   * If NULL or FIN → print alerts for unusual TCP flags.

4. Track counts for repeated activity to detect floods or high-rate scans.

5. Print alerts for suspicious activity.

Example Output

```
Enter PCAP file path: nmap_zombie_scan.pcap
[*] Reading packets from nmap_zombie_scan.pcap...
[TCP] SYN attempt from 192.168.100.101 to 192.168.100.102:80
[TCP] SYN attempt from 192.168.100.101 to 192.168.100.102:80
[+] Analysis complete.
```

3. Giving Input

When prompted in IDLE:
Enter PCAP file path:
Type the PCAP file name you want to analyze, for example:
nmap_scan_ping.pcap
nmap_scan_syn.pcap
nmap_zombie_scan.pcap
Press Enter → the IDS reads the file and prints alerts.
Tip: Place the PCAP file in the same folder as your Python script to make input easier.

4. Sample PCAP Files for Demo

PCAP File	What It Shows
nmap_scan_ping.pcap	ICMP pings
nmap_scan_syn.pcap	SYN scan on multiple ports
nmap_scan_null.pcap	NULL scan (no TCP flags)
nmap_scan_fin.pcap	FIN scan (TCP FIN flag)
nmap_zombie_scan.pcap	Advanced stealth scan, repeated SYNs

5. What You Will See

[ICMP] Ping request from ... to ...

[TCP] SYN attempt from ... to ...

[ALERT] Possible SYN/NULL/FIN scan from ...

[ALERT] High-rate SYNs or ICMP from ...

6. How to Run in IDLE

1. Open IDLE → File → Open → network_ids.py
2. Press F5 to run.
3. Enter the PCAP file name when prompted.
4. Watch the alerts in the shell.

Screenshots:

```
PS C:\Users\3520 i5 16GB> pip install scapy
Collecting scapy
  Downloading scapy-2.6.1-py3-none-any.whl.metadata (5.6 kB)
Downloading scapy-2.6.1-py3-none-any.whl (2.4 MB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 2.4/2.4 MB 2.2 MB/s eta 0:00:00
Installing collected packages: scapy
Successfully installed scapy-2.6.1

[notice] A new release of pip is available: 24.0 -> 25.2
[notice] To update, run: python.exe -m pip install --upgrade pip
PS C:\Users\3520 i5 16GB>
```

Network-ids	✓	15-08-2025 07:31 PM	Python Source File	4 KB
nmap_zombie_scan	✓	15-08-2025 07:24 PM	Wireshark capture ...	4 KB

```
Enter PCAP file path: nmap_zombie_scan.pcap
[*] Reading packets from nmap_zombie_scan.pcap...
[TCP] SYN attempt from 192.168.100.101 to 192.168.100.102:80
[TCP] SYN attempt from 192.168.100.101 to 192.168.100.102:80

[+] Analysis complete.
```

Source of the pcap files from Wireshark Nmap-Captures.zip

NMap Captures.zip (libpcap) Some captures of various NMap port scan techniques.

nmap_OS_scan	✓	15-08-2025 07:24 PM	Wireshark capture ...	158 KB

```
[TCP] SYN attempt from 192.168.100.103 to 192.168.100.102:9594
[ALERT] Possible SYN scan from 192.168.100.103
[ALERT] High-rate SYNs from 192.168.100.103
[TCP] SYN attempt from 192.168.100.103 to 192.168.100.102:9207
[ALERT] Possible SYN scan from 192.168.100.103
[ALERT] High-rate SYNs from 192.168.100.103
[TCP] SYN attempt from 192.168.100.103 to 192.168.100.102:10024
[ALERT] Possible SYN scan from 192.168.100.103
[ALERT] High-rate SYNs from 192.168.100.103
[TCP] SYN attempt from 192.168.100.103 to 192.168.100.102:2557
[ALERT] Possible SYN scan from 192.168.100.103
[ALERT] High-rate SYNs from 192.168.100.103
[TCP] SYN attempt from 192.168.100.103 to 192.168.100.102:7200
[ALERT] Possible SYN scan from 192.168.100.103
[ALERT] High-rate SYNs from 192.168.100.103
[TCP] SYN attempt from 192.168.100.103 to 192.168.100.102:2601
[ALERT] Possible SYN scan from 192.168.100.103
[ALERT] High-rate SYNs from 192.168.100.103
[TCP] SYN attempt from 192.168.100.103 to 192.168.100.102:7004
[ALERT] Possible SYN scan from 192.168.100.103
[ALERT] High-rate SYNs from 192.168.100.103
[TCP] SYN attempt from 192.168.100.103 to 192.168.100.102:10002
[ALERT] Possible SYN scan from 192.168.100.103
[ALERT] High-rate SYNs from 192.168.100.103
[TCP] SYN attempt from 192.168.100.103 to 192.168.100.102:787
[ALERT] Possible SYN scan from 192.168.100.103
[ALERT] High-rate SYNs from 192.168.100.103
[TCP] SYN attempt from 192.168.100.103 to 192.168.100.102:1999
[ALERT] Possible SYN scan from 192.168.100.103
[ALERT] High-rate SYNs from 192.168.100.103
[TCP] SYN attempt from 192.168.100.103 to 192.168.100.102:10621
[ALERT] Possible SYN scan from 192.168.100.103
[ALERT] High-rate SYNs from 192.168.100.103
[TCP] SYN attempt from 192.168.100.103 to 192.168.100.102:9071
[ALERT] Possible SYN scan from 192.168.100.103
[ALERT] High-rate SYNs from 192.168.100.103
[TCP] SYN attempt from 192.168.100.103 to 192.168.100.102:9998
[ALERT] Possible SYN scan from 192.168.100.103
[ALERT] High-rate SYNs from 192.168.100.103
[TCP] SYN attempt from 192.168.100.103 to 192.168.100.102:61532
```

Name: Shreya Bishwas Pandey

InternId: 120

What is the objective of this POC:

The objective of this PoC is to demonstrate a simple Python-based Network IDS that analyzes PCAP files to detect ICMP pings, TCP connection attempts, and common port scans. It highlights how suspicious network activity can be identified and alerted in a safe, controlled environment.