Network IDS - Weekly Task Report

Objective

The objective of this weekly task was to build a lightweight Network Intrusion Detection System (NIDS) that can analyze PCAP files or live network traffic to detect ICMP pings, TCP SYN attempts, port scans and basic suspicious behaviors such as ICMP floods and high-rate SYNs.

Implementation

The IDS was implemented in Python using Scapy for packet analysis. It raises alerts for:

- ICMP echo requests/replies and potential ICMP floods.
- TCP SYN packets and half-open connections.
- Port scans based on SYNs to many different ports.
- Suspicious TCP packets such as NULL or FIN scans.

Two PCAPs were used for demonstration:

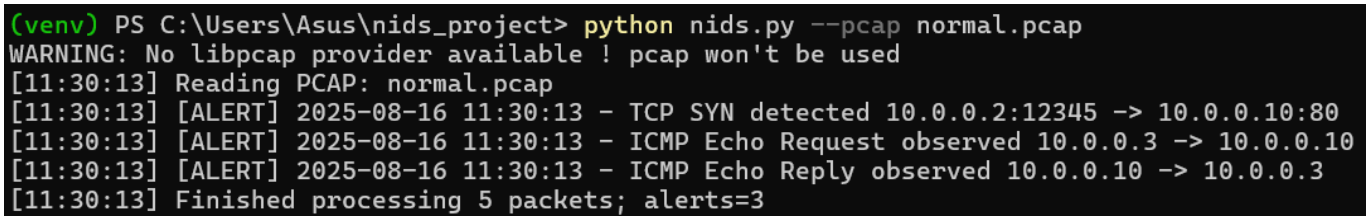
1. normal.pcap - contains benign traffic (TCP handshake and ICMP ping).
2. malicious.pcap - contains simulated attacks including ICMP flood, SYN scan, NULL and FIN scans.

Results

Screenshots below demonstrate the IDS functionality:

- On normal.pcap: minimal alerts (TCP SYN, ICMP Echo Request/Reply).
- On malicious.pcap: multiple alerts including ICMP floods, SYN scans, NULL and FIN scan detections.
- Unit tests (pytest) passed successfully, validating core detection logic.

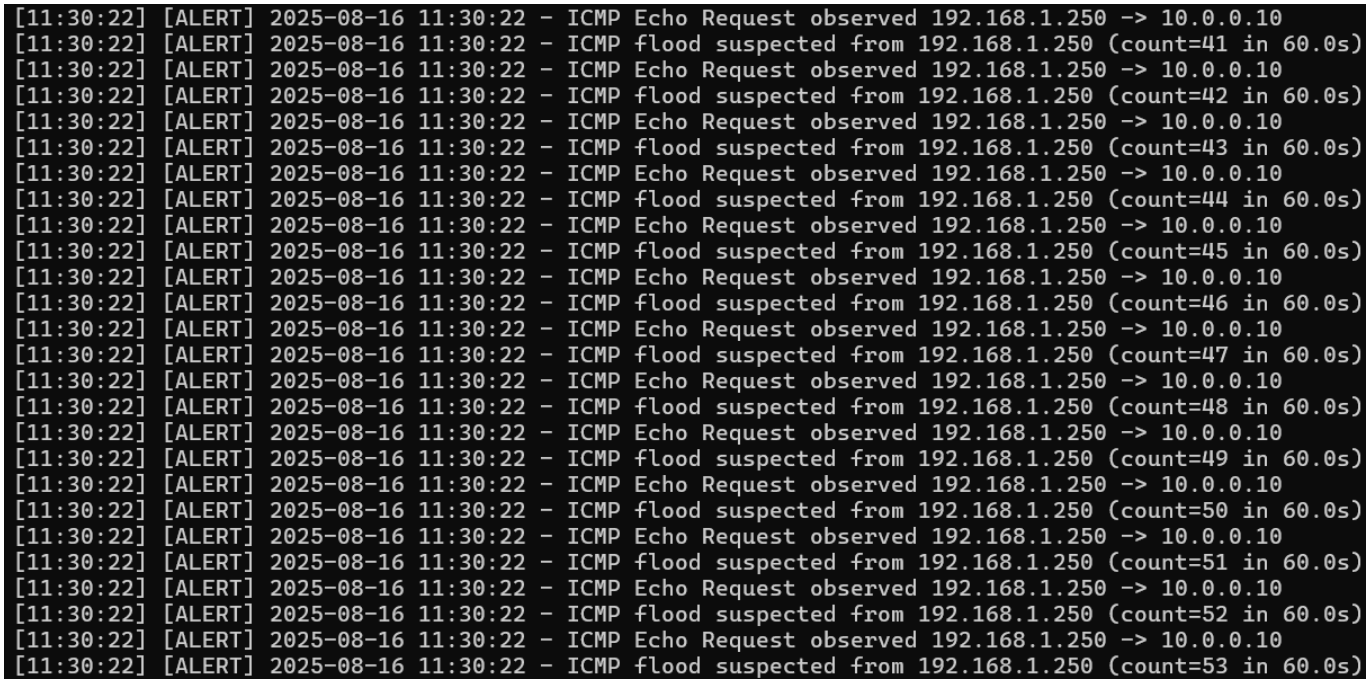
Screenshot: Screenshot 2025-08-16 113210.png



Screenshot: Screenshot 2025-08-16 113240.png

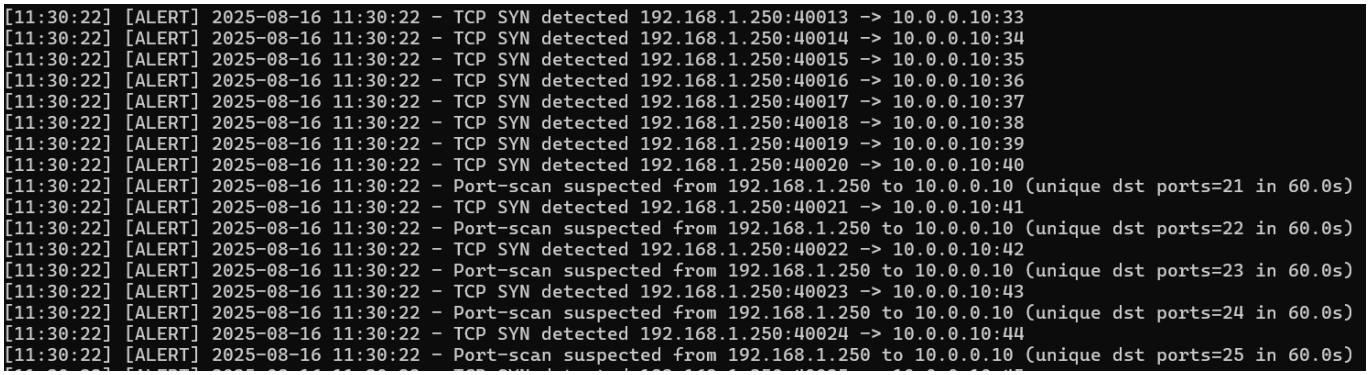
```
(venv) PS C:\Users\Asus\nids_project> python nids.py --pcap malicious.pcap
WARNING: No libpcap provider available ! pcap won't be used
[11:30:22] Reading PCAP: malicious.pcap
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP Echo Request observed 192.168.1.250 -> 10.0.0.10
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP Echo Request observed 192.168.1.250 -> 10.0.0.10
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP Echo Request observed 192.168.1.250 -> 10.0.0.10
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP Echo Request observed 192.168.1.250 -> 10.0.0.10
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP Echo Request observed 192.168.1.250 -> 10.0.0.10
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP Echo Request observed 192.168.1.250 -> 10.0.0.10
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP Echo Request observed 192.168.1.250 -> 10.0.0.10
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP Echo Request observed 192.168.1.250 -> 10.0.0.10
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP Echo Request observed 192.168.1.250 -> 10.0.0.10
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP Echo Request observed 192.168.1.250 -> 10.0.0.10
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP Echo Request observed 192.168.1.250 -> 10.0.0.10
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP Echo Request observed 192.168.1.250 -> 10.0.0.10
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP Echo Request observed 192.168.1.250 -> 10.0.0.10
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP Echo Request observed 192.168.1.250 -> 10.0.0.10
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP Echo Request observed 192.168.1.250 -> 10.0.0.10
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP Echo Request observed 192.168.1.250 -> 10.0.0.10
```

Screenshot: Screenshot 2025-08-16 113254.png

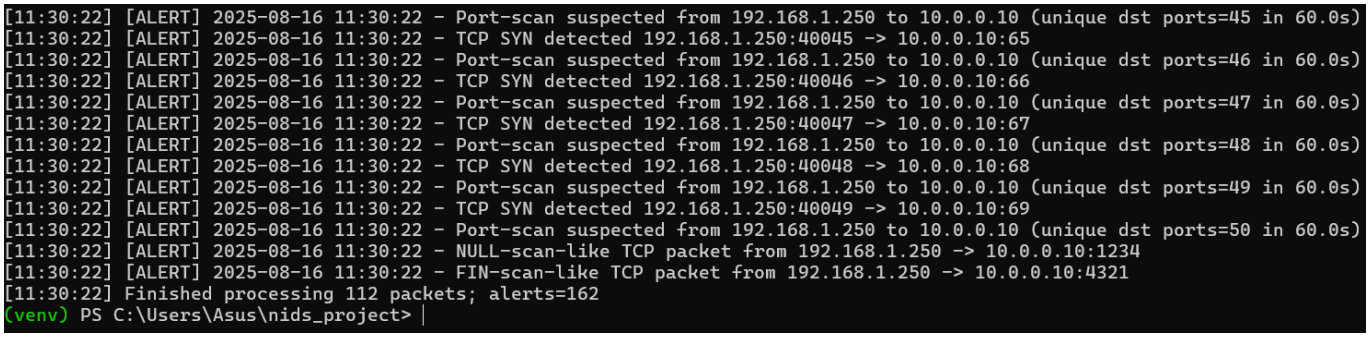


```
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP Echo Request observed 192.168.1.250 -> 10.0.0.10
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP flood suspected from 192.168.1.250 (count=41 in 60.0s)
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP Echo Request observed 192.168.1.250 -> 10.0.0.10
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP flood suspected from 192.168.1.250 (count=42 in 60.0s)
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP Echo Request observed 192.168.1.250 -> 10.0.0.10
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP flood suspected from 192.168.1.250 (count=43 in 60.0s)
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP Echo Request observed 192.168.1.250 -> 10.0.0.10
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP flood suspected from 192.168.1.250 (count=44 in 60.0s)
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP Echo Request observed 192.168.1.250 -> 10.0.0.10
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP flood suspected from 192.168.1.250 (count=45 in 60.0s)
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP Echo Request observed 192.168.1.250 -> 10.0.0.10
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP flood suspected from 192.168.1.250 (count=46 in 60.0s)
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP Echo Request observed 192.168.1.250 -> 10.0.0.10
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP flood suspected from 192.168.1.250 (count=47 in 60.0s)
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP Echo Request observed 192.168.1.250 -> 10.0.0.10
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP flood suspected from 192.168.1.250 (count=48 in 60.0s)
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP Echo Request observed 192.168.1.250 -> 10.0.0.10
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP flood suspected from 192.168.1.250 (count=49 in 60.0s)
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP Echo Request observed 192.168.1.250 -> 10.0.0.10
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP flood suspected from 192.168.1.250 (count=50 in 60.0s)
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP Echo Request observed 192.168.1.250 -> 10.0.0.10
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP flood suspected from 192.168.1.250 (count=51 in 60.0s)
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP Echo Request observed 192.168.1.250 -> 10.0.0.10
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP flood suspected from 192.168.1.250 (count=52 in 60.0s)
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP Echo Request observed 192.168.1.250 -> 10.0.0.10
[11:30:22] [ALERT] 2025-08-16 11:30:22 - ICMP flood suspected from 192.168.1.250 (count=53 in 60.0s)
```

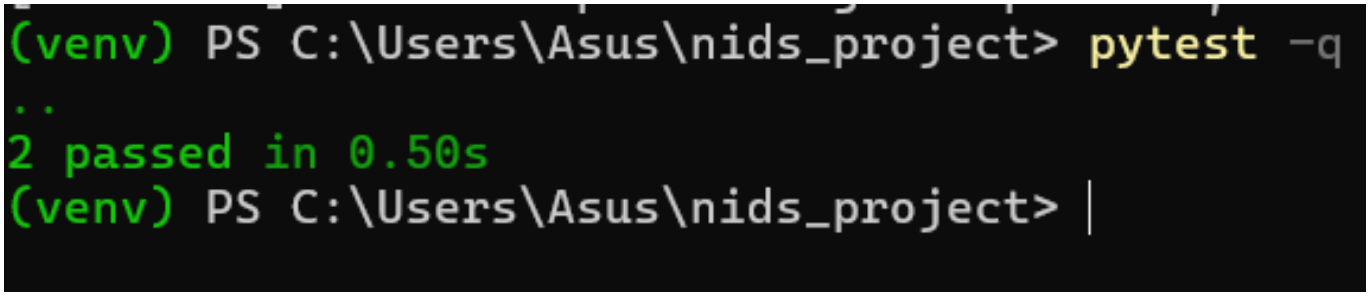
Screenshot: Screenshot 2025-08-16 113313.png



Screenshot: Screenshot 2025-08-16 113331.png



Screenshot: Screenshot 2025-08-16 113359.png



False Positive Considerations

- Monitoring systems may trigger ICMP flood alerts.
- Load balancers or NAT devices may appear as port scanners.
- High connection rates from legitimate clients could raise SYN flood alerts.
- Some uncommon protocols may resemble NULL/FIN scans.

Next Steps / Improvements

- Store alerts in structured logs (CSV/JSON) for SIEM integration.
- Configurable thresholds and whitelists for trusted hosts.
- Visualization dashboard for alerts.
- Deeper packet inspection (DNS, HTTP) for richer context.
- Performance improvements for high-traffic environments.