**Intern ID: 298**

Network Intrusion Detection System (IDS) (POC):

1. Objective

The goal of this POC is to design and implement lightweight Network Intrusion Detection System (IDS) capable of monitoring network traffic in real time or from pre-recorded PCAP files.

The IDS should detect and raise alerts for the following:

ICMP Pings (Echo Request/Reply)

TCP Connection Attempts (SYN packets, half-open connections)

Common Port Scan Patterns (SYN, NULL, FIN scans; repeated attempts to multiple ports)

Suspicious Behaviours (ICMP floods, high-rate SYNs to multiple ports)

The system should have modular detection capabilities and produce clear reports for each incident.

2. Architecture & Design

Core Components

1. Packet Capture Module – Uses tools like Scapy, PyShark, or libpcap to capture live network traffic or load PCAPs.

2. Protocol Analysis Module – Classifies packets and extracts metadata such as source/destination IP, ports, protocol type, and flags.

3. Detection Engine – Implements signature-based rules for known attacks and threshold-based alerts for anomalies.

4. Alerting System – Outputs alerts to console, logs, or dashboard.

5. Reporting & Visualization – Summarizes findings, includes statistics and trends.

3. Detection Logic

ICMP Ping Detection – Detects Echo Request/Reply packets and flags if frequency exceeds a set threshold.

TCP SYN Flood Detection – Identifies excessive SYN packets without corresponding ACKs.

Port Scan Detection – Flags repeated attempts to multiple ports within a short time window.

ICMP Flood Detection – Alerts on unusually high ICMP traffic from a single source.

4. False Positive Considerations

• Whitelist trusted internal IPs.

• Adjust detection thresholds according to normal traffic volume.

• Apply rate limiting to avoid false positives from traffic bursts.

• Implement context-aware detection (time of day, expected behaviour).

5. Testing & Validation

Test Scenarios:

Normal Traffic PCAP – Ensure no over-triggering on regular operations.

Attack Simulation PCAP – Includes port scans, floods, and ping sweeps.

Validation Metrics:

True Positives (TP) – Correctly identified malicious activity.

False Positives (FP) – Legitimate traffic incorrectly flagged.

Detection Latency– Time between packet arrival and alert.

6. Next Steps & Enhancements

• Integrate anomaly-based detection using ML models.

• Build a live alert dashboard.

• Implement automated response actions (e.g., IP blocking).

• Expand protocol support (UDP, application-layer protocols).

