**Proof of Concept Report: Lightweight Network IDS**

**Authors:**

* Riya Bhutal (Intern ID: 248)
* Gautam Poojari (Intern ID: 251)

**Date:** August 17, 2025

**1. Introduction**

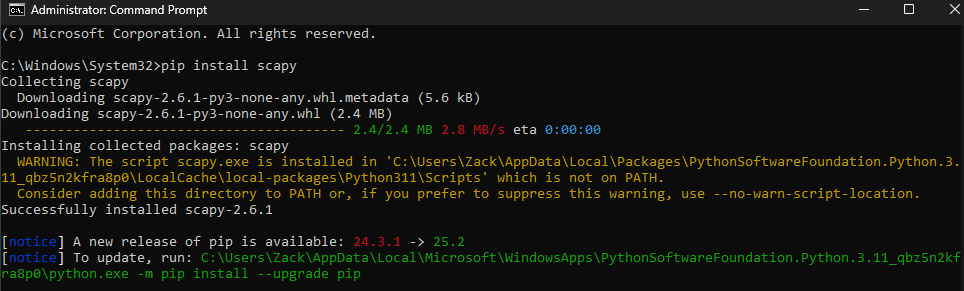
This report details the successful implementation of a lightweight Network Intrusion Detection System (NIDS). The objective was to build a tool that monitors network traffic from PCAP files and raises alerts for suspicious activities like pings, connection attempts, and common scan patterns. This document outlines the detection logic and presents the results from testing against both normal and malicious traffic captures.

**2. Detection Logic Implemented**

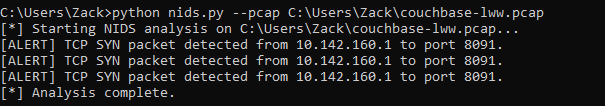
The NIDS analyzes packets to identify several key indicators of compromise or reconnaissance:

* **ICMP Activity:** Detects ICMP Echo Requests and Replies ("pings") to monitor for basic network mapping and potential flood attacks.
* **TCP Connection Attempts:** Flags any TCP packet with the SYN flag set as a new connection attempt. This is a baseline for detecting more complex behaviors.
* **Stealth Scans:** Identifies TCP packets with unusual flag combinations, such as NULL (no flags set) and FIN (only FIN flag set) scans.
* **High-Rate Scans (SYN Scans):** To detect port scanning, the system tracks the number of unique ports a single source IP attempts to connect to within a short time window. If this number exceeds a set threshold, it triggers a critical "Potential SYN Scan" alert.

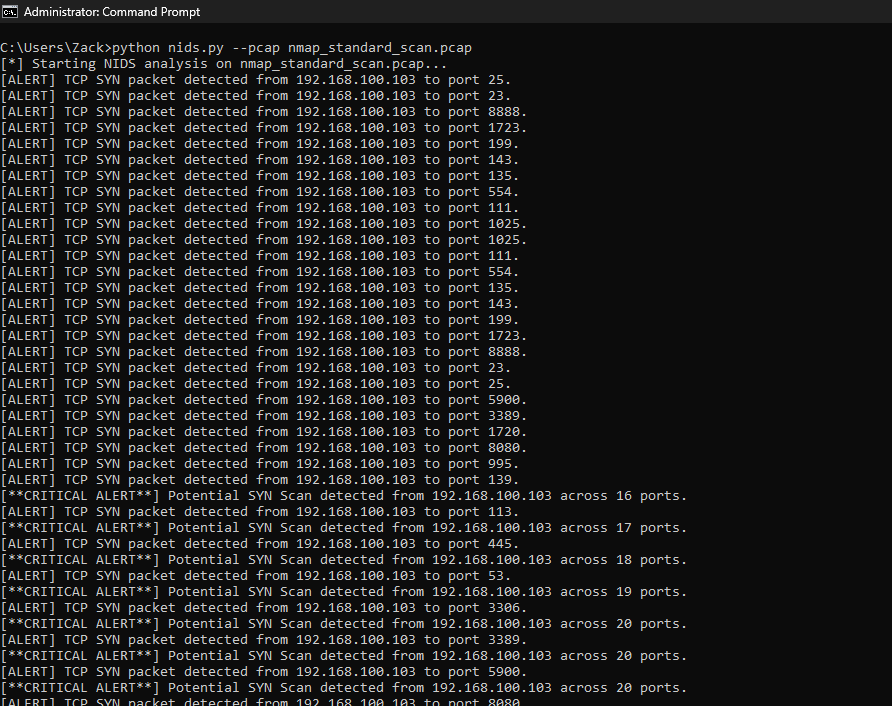
**3. Demonstration Results**

The NIDS was tested against two distinct PCAP files to validate its effectiveness.

* **Normal Traffic Analysis (dhcp.pcap)(couchbase-lww.pcap):** The NIDS was first run against dhcp.pcap, a file containing benign DHCP traffic. As expected, the tool processed the entire file without generating any critical alerts. This successfully demonstrates the system's ability to distinguish normal network operations from malicious activity.



* **Attack Traffic Analysis (nmap.pcap)** Next, the NIDS was run against a PCAP file containing a port scan generated by the Nmap tool. The system immediately identified the high rate of connection attempts from a single source IP to numerous ports on a target machine. It generated a continuous stream of critical alerts, correctly identifying the activity as a "Potential SYN Scan". This result validates the effectiveness of the rate-based detection logic.

******

## **4. False Positives and Limitations:**

While the NIDS was able to successfully detect SYN scans and distinguish normal DHCP traffic, there are some potential limitations:  
- False Positives: Legitimate applications that open multiple connections quickly could be flagged as scans.  
- Scope: The system currently detects only a few basic attack types (ICMP, SYN scans) and does not cover advanced intrusion techniques.  
- Performance: The system is lightweight and may not scale well for very high-speed networks.

## **5. Future Improvements:**

Potential next steps to improve the system include:  
- Adding support for detecting NULL, FIN, and ACK scans.  
- Implementing logging to file instead of console-only alerts.  
- Introducing threshold tuning to reduce false positives.  
- Exploring machine learning-based anomaly detection to extend coverage.

**6. Conclusion**

This Proof of Concept successfully demonstrates a functional lightweight NIDS. The system correctly identifies malicious scan activity while allowing normal traffic to pass without issue. The code and this demonstration fulfill the core objectives of the project. Future enhancements could include adding more advanced detection signatures, implementing a live capture mode, and creating a more user-friendly interface.