

# Investigation into Network Traffic Scanners

## Intro:

*The project delves into how beneficial security software can be for a network. New threats are always emerging, so new security software is always needed.*

## AIM:

Create a network scanner that notifies the user for potential attacks or malicious activity.

Research Gaps: These being third party suppliers, poor security measures still put in place and unsafe public Wi-Fi. Third party suppliers have been targeted multiple times in 2025 and will continue to be targeted [1],[2]. Small networks have poor security measures put in place and sometimes none.

## Design and Development:

Prototype developed with python. Python contains network-based libraries to capture and manipulate traffic.

The software will use multiple metrics to determine if network traffic is malicious or not. Such as traffic volume, IP address, packet loss, packet types and more.

The main python library used was 'scapy'. This allowed traffic to be monitored and manipulated. Aspects of random forest tree machine learning model has been implemented.

## The software monitoring a small network

```
What is your devices IP address: 192.168.0.175
Captured 7 packets in 5 seconds.
7
The average amount of packets every 5 seconds is: 7.0
Captured 12 packets in 5 seconds.
12
The average amount of packets every 5 seconds is: 9.5
GAP DETECTED: Expected 1193919994, got 1193919995 (Loss: 1 bytes)
GAP DETECTED: Expected 1335249782, got 1335249783 (Loss: 1 bytes)
```

## Results:

The software accurately detected a denial-of-service attack and a man in the middle attack. Using multiple network metrics malicious activity can be detected by this python software. When multiple indicators are triggered, a critical warning is given.

```
Slight increase in traffic
NOW LARGE INCREASE IN TRAFFIC

IP irregular
There has been a large number of packets sent by the same IP address

Medium level of malicious activity
High level of malicious activity
Critical levels of malicious activity!
```

## References:

- [1] Christine Horton, Third-Party Threats: The Supply Chain Risk You Can't Afford to Ignore, 22 October 2025
- [2] Jed Nykolle Harme, Supply chain risks overwhelm cybersecurity leaders, report finds, 2025.