Proof of Concept — Network IDS

Objective

The purpose of this Proof of Concept is to show that the **Network Intrusion Detection System (IDS)** developed during the internship can successfully detect normal traffic (pings), malicious scans (SYN scans), and simple suspicious payloads.

ICMP Ping Detection

- **Action:** A normal ping command (`ping 8.8.8.8`) was run and recorded in a capture file.
- **Result:** The IDS correctly raised alerts for both **ICMP Echo Request** and **ICMP Echo Reply** packets.
- **Interpretation:** The IDS can identify normal connectivity checks and potential ICMP misuse.

SYN Scan Detection

- **Action:** An Nmap scan was performed on local ports (22, 80, 443).
- **Result:** The IDS generated alerts for multiple **TCP SYN packets**, showing that it recognized repeated connection attempts across different ports.
- **Interpretation:** The IDS can detect basic port scanning activity, which is commonly used by attackers to map available services.

Payload Signature Detection

- **Action:** A packet with the word *"malware"* in its content was sent and captured.
- **Result:** The IDS triggered a **signature match alert**, identifying the suspicious keyword in the payload.
- **Interpretation:** The IDS can apply simple signature rules to highlight potentially malicious data transfers.

Observations

- The IDS consistently raised alerts for expected events.
- Detection worked for both **normal behavior** (pings) and **potential attacks** (port scans, malicious keywords).

- Alerts were printed in structured format, making them easy to review.

Conclusion

This Proof of Concept confirms that the IDS fulfills its goal:

- It can **detect pings**, **connection attempts**, and **basic scanning activity**.
- It can highlight **suspicious payloads** based on simple rules.
- While lightweight, it demonstrates the foundation of a functional IDS.