TCPDump Incident Report

Author: Tiago Sants

Date: July 03, 2025

This project focuses on identifying a brute-force attack captured using tcpdump. Network traffic was analyzed to determine the protocol in use (TCP), source of attack, and affected services. The report includes evidence from packet capture logs, explanation of the methodology, and proposed mitigation strategies.

Incident Summary:

A brute-force attack was detected targeting port 22 (SSH) from a single IP address.

Packet captures revealed multiple login attempts using different credentials.

Network Protocol Involved:

TCP protocol over IPv4 was identified in the capture logs.

Evidence:

The tcpdump file showed multiple SYN packets followed by RST, indicating failed connections.

The source IP address attempted connections in rapid succession without success.

Tools Used:

- tcpdump
- Wireshark (for visualization)
- Linux CLI for inspection

Mitigation Steps:

- Block the IP address using firewall rules (iptables or ufw).
- Configure fail2ban to detect and prevent brute-force attempts.
- Enforce public key authentication for SSH access.

Outcome:

The incident was contained and documented. Future access will rely on enhanced logging and real-time alerts.