Network Intrusion Detection Report

Project Title: Network Intrusion Detection using Zeek and Wireshark

Analyst: Brett Banks

Environment: Kali Linux (Attacker) + Windows 10 (Target) | Host-Only VirtualBox Network

Tools: Zeek, Wireshark, tcpdump, FTP, nslookup, nmap

Date: June 01, 2025

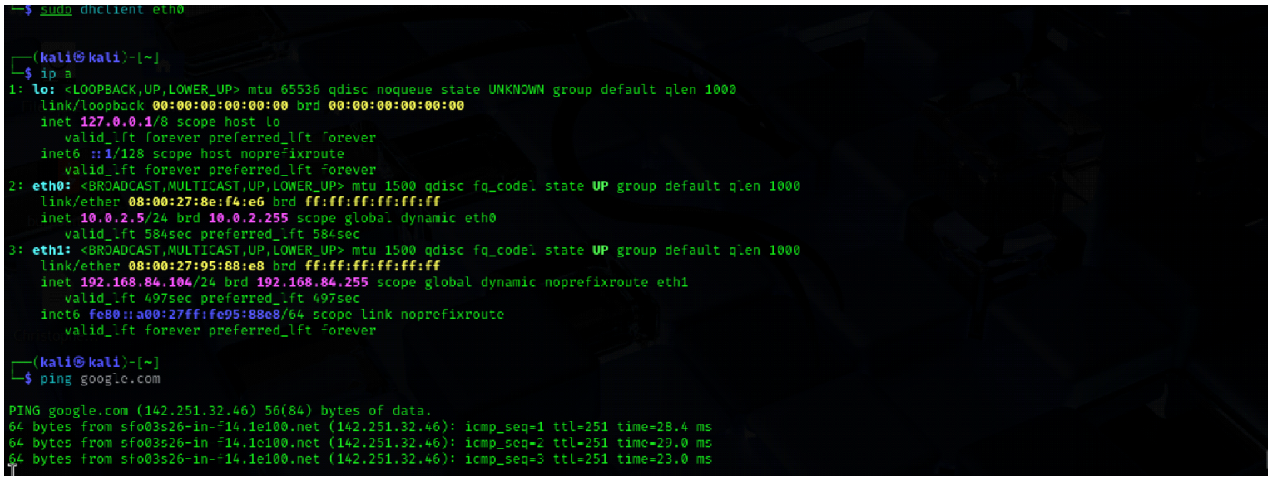
🌟 Objective

To simulate and detect malicious network behaviors including insecure credential transmission, DNS tunneling, and port scanning. Analyze traffic using Zeek to extract indicators, evaluate the threat, and summarize actionable findings as would be done in a SOC environment.

🧪 Lab Setup

Component	Configuration
Kali Linux	Attacker / Monitor (Wireshark + Zeek)
Windows 10	Victim with FTP service enabled
Network Type	Host-Only Adapter (192.168.84.0/24)
Capture Tool	tcpdump -i eth1 -w ftp_test.pcap

📌 Screenshot – Interface Configuration and NAT:



📌 Screenshot – tcpdump capturing FTP traffic:

📡 Attack Simulation Actions

FTP Login with Cleartext Credentials

Command: ftp 192.168.84.102
Used fake creds: testuser / weakpass

📂 Zeek Output Analysis

Connection Log (conn.log)

⚠️ Findings Summary

1. FTP Credential Exposure

Protocol: FTP (port 21)
Credential: USER testuser, PASS weakpass
Risk: Exposed credentials could be intercepted on flat networks
Mitre Mapping: T1078 – Valid Accounts

🧐 Conclusion

This lab demonstrated how basic attacker techniques can be detected with Zeek when cleartext protocols like FTP are used. Zeek successfully logged the session metadata through conn.log. With additional analyzers or forced module loading, full FTP logging could also be observed.