Network Traffic Investigation Report

Project: Wireshark SOC Simulation
Analyst: Aryan
Date:

1. Investigation Overview

This investigation was conducted within a controlled lab environment to analyze network traffic using Wireshark. The objective was to observe and understand how DNS resolution, TCP session establishment, and HTTPS communication occur at the packet level.

The capture was performed inside a Kali Linux virtual machine using a NAT-based network configuration.

2. Environment Details

- Host System: VirtualBox
- Virtual Machine: Kali Linux
- Network Type: NAT
- Local IP Address: 10.0.2.15
- DNS Resolver: 10.0.2.3

Traffic was intentionally generated by performing ping tests and browsing websites.

3. Evidence Collected

3.1 DNS Resolution

A DNS query was observed from 10.0.2.15 to the DNS resolver 10.0.2.3 requesting resolution for google.com.

The server responded successfully with an IPv4 address (142.250.x.x). The DNS response contained:

- Standard query response
- No error flags
- One answer record
- Valid IP address returned

This confirms proper DNS resolution behavior.

3.2 TCP Three-Way Handshake

A complete TCP three-way handshake was observed between the client (10.0.2.15) and a remote HTTPS server on port 443.

The handshake sequence included:

1. SYN packet initiated by client
2. SYN-ACK response from server
3. ACK packet from client

This confirmed successful TCP session establishment.

3.3 TLS Handshake (HTTPS Communication)

Immediately following the TCP handshake, a TLS 1.2 negotiation was observed, including:

- Client Hello
- Server Hello
- Server Certificate

This indicates that encrypted HTTPS communication was successfully established between the client and the remote server.

4. Analysis & Findings

The captured traffic reflects normal browsing behavior within a secure environment.

Key observations:

- DNS queries are transmitted in plaintext
- TCP sessions are established using a standard three-way handshake
- HTTPS traffic is encrypted after TLS negotiation
- No suspicious outbound connections or abnormal traffic patterns were observed

The activity during the capture window appears legitimate and consistent with normal web browsing.

5. Risk Assessment

Risk Level: **Low**

The captured traffic did not contain indicators of malicious behavior. However, the visibility of DNS traffic in plaintext highlights the importance of DNS monitoring in enterprise environments.

6. Recommendations

Although no malicious behavior was detected, the following best practices are recommended:

- Enforce HTTPS-only communication policies
- Monitor outbound DNS queries for anomalies
- Implement IDS/IPS for real-time traffic monitoring
- Conduct periodic traffic analysis reviews

7. Conclusion

This investigation provided practical insight into packet-level network communication and demonstrated how a SOC analyst can interpret DNS activity, TCP handshakes, and encrypted HTTPS sessions using Wireshark.

The exercise strengthened understanding of network protocols and reinforced foundational cybersecurity investigation techniques.