Wireshark Network Traffic Analysis Report

Analyst: Edmond Degand

Date: February 2025

Target Environment: Simulated Network Lab

1. Executive Summary

This report documents the findings from a network traffic capture and analysis exercise conducted using Wireshark. The goal was to detect potential security threats, unusual network behavior, and indicators of compromise (IoCs) within a simulated environment.

Multiple signs of host reconnaissance, unauthorized access attempts, and poor security configurations were detected during the analysis. Immediate security enhancements are recommended.

2. Scope and Methodology

Scope:
- Monitored internal network traffic on subnet 192.168.1.0/24.
- Captured all traffic on interface eth0 within a controlled lab environment.

Tools Used:
- Wireshark: Packet capture and analysis
- tcpdump: Initial traffic collection
- Kali Linux: Traffic generation (simulated attacks)
- Nmap: External port scanning

3. Analysis Findings

Finding	Description	Severity
Port Scan Detection	Multiple SYN packets observed from a single external IP.	High
Unencrypted HTTP Credentials	Login form transmitted in plaintext.	High
Suspicious DNS Queries	Unusually high DNS queries to untrusted domains.	Medium
ARP Spoofing	Duplicate ARP responses detected.	Medium
Excessive Failed SSH Logins	Multiple failed SSH login attempts detected.	Medium

4. Packet Capture Evidence

Sample Packet - Unencrypted HTTP Login:

```
POST /login HTTP/1.1
Host: 192.168.1.102
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 42
username=admin&password=123456
```

Sample Packet - Port Scan SYN:

```
Frame 15: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: 08:00:27:ab:cd:ef, Dst: 08:00:27:12:34:56
Internet Protocol Version 4, Src: 192.168.1.50, Dst: 192.168.1.105
Transmission Control Protocol, Src Port: 45000, Dst Port: 22, SYN
```

5. Recommendations

- Enable encryption (HTTPS, SSH) for all sensitive traffic.
- Implement network segmentation to isolate critical systems.
- Deploy Intrusion Detection Systems (IDS) to monitor for scanning and attacks.
- Restrict outbound DNS queries to trusted domains.
- Harden authentication mechanisms and limit SSH access to known IPs.
- Conduct regular network audits to identify anomalies and misconfigurations.

6. Conclusion

This analysis revealed multiple critical issues, including cleartext credential transmission, port scans, and anomalous DNS traffic. Implementing the recommended security controls will significantly improve the network's overall security posture.

7. Analyst

Edmond Degand
LinkedIn: https://linkedin.com/in/edmonddegand
Email: edmonddeg@gmail.com