Network Traffic Analysis & Threat Detection Report

🗓️ Date: March 30, 2025

🥷 Author: Vanessa

🔷 TryHackMe Room(s) Used: Wireshark 101, Splunk 101, Blue Team Labs

---

1. Introduction

*Objective:**

This report documents network traffic analysis and security log monitoring performed using TryHackMe labs. The goal was to:

- Identify potential security threats in network traffic.

- Use Wireshark and Splunk to analyze logs and detect anomalies.

- Provide recommendations for mitigating identified risks.

Tools Used:

- **Wireshark** (Packet Capture & Analysis)

- **Splunk** (Log Management & Security Information Event Management - SIEM)

- **Linux CLI Commands** (tcpdump, netstat, ping, tracert)

Key Skills Demonstrated:

✅ Network Traffic Monitoring

✅ Incident Detection & Response

✅ Log Analysis with Splunk

✅ Security Threat Investigation

2. Methodology

2.1 TryHackMe Lab Setup

- Connected to TryHackMe virtual environment.

- Captured live network traffic using Wireshark.

- Analyzed Splunk security event logs.

2.2 Data Collection & Analysis

Wireshark Filtering Example:

- Applied filters to detect HTTP traffic:

```bash
http.request.method == "POST"
```

- Checked for failed login attempts:

```bash
tcp contains "login failed"
```

2.3 Key Observations

Timestamp	IP Address	Issue Detected	Severity
10:45am	192.168.1.10	Multiple failed logins	High
11:02am	192.168.1.20	Unusual high traffic	Medium

3. Findings & Analysis

3.1 Network Performance Issues:

- High **latency and packet loss** detected from 192.168.1.20.

- Possible **bandwidth congestion** caused by unauthorized streaming services.

3.2 Security Threats Identified:

- **Brute-force login attempts** detected from external IPs.

- **Port scanning** activity, indicating possible reconnaissance for an attack.

- **Unusual data transfer spikes** from a specific device, indicating potential data exfiltration.

📌 **Splunk Log Example (Failed SSH Logins):**

```bash
host=192.168.1.10 sourcetype=linux_secure | grep "Failed password"
```

🔷 *Result: 50 failed login attempts within 5 minutes from IP 198.51.100.22 (possible brute-force attack).*

---

4. Remediation & Recommendations

Issue	**Solution**
Brute-force login attempts	Implement account lockout policy after 5 failed attempts
High network congestion	Monitor bandwidth usage and restrict non-essential traffic
Unauthorized port scanning	Block suspicious IPs using firewall rules
Data exfiltration risk	Enable **Data Loss Prevention (DLP)** policies and alerts

---

5. Conclusion

This project successfully demonstrated network traffic monitoring and security log analysis using Wireshark and Splunk. By identifying suspicious activities like brute-force attempts and port scanning, I gained hands-on experience with real-world NOC and cybersecurity tasks. These skills are essential for roles in **Network Operations Centers (NOC) and Security Operations Centers (SOC).**