# Incident Report – Network Traffic Analysis

## 1. Overview

This incident report documents the analysis of captured network traffic from a simulated Security Operations Center (SOC) environment. The investigation focused on identifying key communication patterns, recognizing potential reconnaissance activity, and evaluating unencrypted traffic vulnerabilities using Wireshark and Nmap.

## 2. Objective

To demonstrate the ability to isolate, analyze, and interpret different types of network traffic including normal operations (DNS and HTTP) and malicious activity (SYN scan) for effective incident detection and reporting.

## 3. Tools Used

* Wireshark – Network protocol analysis
* Nmap – Network scanning tool for reconnaissance simulation
* Web Browser – For generating HTTP and DNS traffic
* Windows 10 PC – Platform for capturing and analyzing network packets

## 4. Evidence Overview

Three significant network and security events were identified during the capture:

1. Unencrypted Web Traffic (HTTP): Detection of clear-text transmission between client and server.
2. Network Reconnaissance (SYN Stealth Scan): Nmap scanning detected through SYN packet patterns.
3. DNS Resolution Activity: Observation of standard DNS query and response behavior.

## 5. Traffic Summary

Total Packets Captured: 1470

Most Common Protocols: TCP, DNS, HTTP, Ethernet

Key IP Addresses:

* Local Host: 10.106.220.142
* External HTTP Server: 188.184.67.127

## 6. Findings

• HTTP Traffic: Visible GET requests and response headers confirmed unencrypted communication. Sensitive data was exposed in plain text, posing a potential security risk.

• DNS Queries: Multiple DNS lookups (A, AAAA, and PTR) were observed. All DNS traffic was unencrypted, creating possible data exposure.

• SYN Scan Detection: Wireshark filter 'tcp.flags.syn==1 && tcp.flags.ack==0' revealed multiple SYN packets from source 10.106.220.142, confirming Nmap port scan activity. This pattern indicates reconnaissance attempts.

## 7. Indicators of Compromise (IOCs)

Although this was a controlled exercise, the following Indicators of Attack (IOAs) were recorded:

* Type: Reconnaissance
* Packet Pattern: High frequency of TCP SYN packets without matching SYN-ACK or RST responses (stealth scan signature).

## 8. Conclusion

The investigation successfully demonstrated traffic inspection skills using Wireshark. It differentiated between normal traffic (DNS, HTTP) and malicious reconnaissance (SYN scanning). The findings underscore the importance of encryption and network defense mechanisms to protect against real-world threats.

## 9. Recommendations

* Implement HTTPS (TLS) for all web communications to prevent clear-text data exposure.
* Deploy Intrusion Detection/Prevention Systems (IDS/IPS) to detect and limit port scanning attempts.
* Harden external services by restricting open ports and filtering unused protocols.
* Regularly monitor network traffic for abnormal SYN flood or connection attempt patterns.

## 10. Learning Outcomes

* Improved understanding of network traffic layers using Wireshark.
* Ability to apply display filters to isolate specific traffic patterns.
* Recognizing reconnaissance techniques like SYN stealth scans.

## 11. Evidence Screenshots (Placeholders)

* [Insert Screenshot\_Main\_Capture.png here]
* [Insert Screenshot\_Finding\_1\_Unencrypted\_HTTP.png here]
* [Insert Screenshot\_Finding\_2\_Nmap\_SYN\_Scan.png here]
* [Insert Screenshot\_Finding\_3\_DNS\_Queries.png here]

© 2025 Mohamed Asmy — Cybersecurity Portfolio Project (CCP2)