Packet-Level Analysis of Network Reconnaissance Techniques Using Nmap and Wireshark

Author: Frankie Rodriguez Rivera
Advisor: Dr. Jeffrey Duffany
Master in Computer Science
Polytechnic University of Puerto Rico

Abstract

This project examines network reconnaissance methods, packet-level traffic inspection, and authentication security using Nmap and Wireshark. The study investigates how scanning activities manifest in network traffic and how defenders can identify these patterns. Experiments demonstrated that different scan types produce distinct TCP flag signatures. SYN scans generated half-open attempts, while ACK scans revealed firewall filtering. Authentication analysis showed weak credentials can be compromised rapidly. Results support defense-in-depth combining network visibility, packet analysis, and strong authentication.

Introduction

As digital systems become more interconnected, cybersecurity is a central concern. Many cyberattacks begin with reconnaissance, where attackers collect details about possible targets. This project examines how reconnaissance tools generate observable network traffic patterns that defenders can use for early detection. The study combines Nmap scanning with Wireshark packet capture to compare theoretical expectations with real network behavior.

Background

Modern networks are a common starting point for cyberattacks because exposed services and traffic patterns can be observed remotely. Reconnaissance involves checking which hosts are reachable, which ports are open, and what services are exposed. Nmap is widely used for host discovery, port scanning, service enumeration, and OS fingerprinting, supporting several scan types that behave differently at the transport layer. Wireshark enables researchers to capture and analyze packets produced during scans and routine traffic, providing concrete data such as TCP flag patterns and protocol distribution. Together, these tools allow security professionals to study reconnaissance as a protocol exchange rather than simply reviewing scan output summaries.

Problem

Network reconnaissance is often the first step in a cyberattack but is frequently missed by defenders because it does not cause immediate visible disruption. Scanning methods produce different packet-level signatures in TCP control flags and protocol responses. Without packet-level inspection, it is difficult to distinguish host discovery from port scanning, firewall probing, or OS fingerprinting. Additionally, weak authentication controls significantly increased risk after reconnaissance identifies reachable services. This project addresses the gap in packet-level understanding of reconnaissance traffic and its relationship to authentication vulnerabilities.

Methodology

The project followed four phases in a controlled environment:

1. Network Reconnaissance Using Nmap: Host discovery scans identified active devices on subnet 192.168.0.0/24. TCP SYN scanning revealed open ports (HTTP/80, HTTPS/443, UPnP/5000). Multiple scan types were compared: SYN, ACK, fast, and aggressive scans. External validation used scanme.nmap.org.

Figure 1. Network Reconnaissance Using Nmap: Host discovery scans identified active devices on subnet 192.168.0.0/24. TCP SYN scanning revealed open ports (HTTP/80, HTTPS/443, UPnP/5000).

2. Traffic Analysis Using Wireshark: A one-minute controlled capture recorded several thousand packets. Protocol analysis examined TCP, UDP, DNS, ARP, TLS, and QUIC distribution. Display filters isolated reconnaissance traffic from background noise.

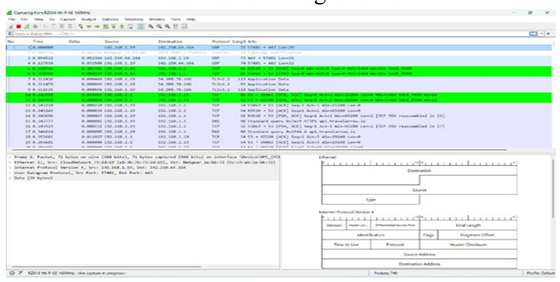

Figure 2. ACK scan packet trace illustrating firewall rule probing behavior.

3. Advanced Packet-Level Correlation: Live traffic was captured during multiple scan executions to correlate scan types with TCP flag behavior. SYN scans showed half-open attempts; ACK scans showed unsolicited probes for firewall testing.

4. Authentication and Cryptographic Analysis: Password security was tested using John the Ripper with dictionary attacks. Cryptographic hash functions were evaluated for the avalanche effect and data integrity verification using MD5, SHA-1, and SHA-256.

Results and Discussion

Network reconnaissance and attack preparation created consistent, observable packet-level patterns across all tests.

Reconnaissance Findings: TCP SYN probes consistently showed half-open attempts where the three-way handshake was never completed, characteristic of stealthy scanning. ACK-based scans returned flag patterns indicating firewall filtering rules rather than service availability. Aggressive and OS fingerprinting scans produced complex multi-protocol traffic using TCP, UDP, and ICMP probes.

Traffic Analysis: Modern networks produced large volumes of traffic in short periods. Encrypted protocols (TLS, QUIC) dominated with no unencrypted HTTP observed. Statistical tools and display filters were essential for separating reconnaissance traffic from background noise.

Authentication Results: Dictionary attacks using John the Ripper recovered weak passwords (e.g., “abc”) in seconds, demonstrating how low-entropy credentials undermine encryption protections. Cryptographic hashing confirmed the avalanche effect, where single-character input changes produced entirely different hash outputs.

Advanced password exercises demonstrated how quickly weak authentication mechanisms can be compromised once reconnaissance identifies accessible services. Dictionary-based attacks using John the Ripper successfully recovered low-entropy passwords within seconds, confirming that password complexity is often the weakest link in otherwise secure systems.

As shown in **Figure 3**, simple passwords such as “abc” provided minimal resistance despite being protected by encryption mechanisms. This illustrates that encryption strength is fundamentally undermined when weak credentials are used.

Additional experiments with cryptographic hash functions highlighted the avalanche effect, where minor input changes produced completely different hash outputs. While hashing ensures data integrity, these results emphasize that strong password policies and modern authentication controls are essential to prevent rapid credential compromise following reconnaissance activity.

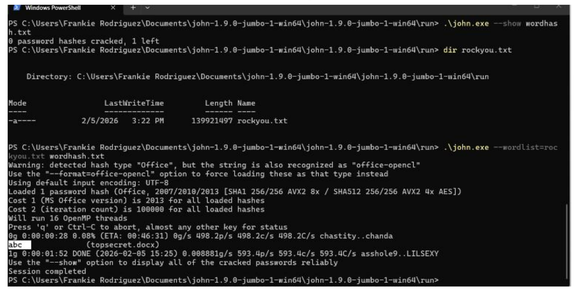

Figure 3. Dictionary-based password crack using John the Ripper.

Conclusion and Future Work

This project demonstrated that packet-level inspection can effectively reveal network reconnaissance activity and authentication weaknesses. Analysis of Nmap scans showed that different reconnaissance techniques generate consistent and identifiable TCP flag patterns, allowing defenders to distinguish between host discovery, port scanning, and firewall probing through packet inspection.

Authentication experiments further showed that once services are identified, weak credentials significantly increase the likelihood of compromise. Dictionary-based password attacks recovered low-entropy passwords in seconds, and cryptographic hashing experiments confirmed the avalanche effect, highlighting the importance of strong password policies alongside encryption mechanisms.

Future work will extend this analysis to enterprise-scale environments using IDS/IPS and advanced firewall deployments. Additional research may integrate automated detection tools such as Suricata or Snort to correlate packet-level observations with alert generation. Authentication analysis can also be expanded to evaluate multi-factor authentication and modern adaptive hashing algorithms such as bcrypt and Argon2.

References

[1] Zscaler Directory Authentication, Google Books, 2026.
[2] TryHackMe, Wireshark: The Basics.
[3] Learn Wireshark, Google Books, 2022.
[4] Brute-force attack, Wikipedia.
[5] Password cracking, Wikipedia.
[6] MD5, Wikipedia.
[7] SHA-1, Wikipedia.

Acknowledgements

The author acknowledges the guidance and support of Dr. Jeffrey Duffany, advisor, and the faculty and staff of the Computer Science Department at Polytechnic University of Puerto Rico. Special thanks to the graduate program for providing the resources and environment necessary to conduct this research.