Table of Contents

Network Traffic Analysis Report

Prepared By: Giovanni Farid Shawki

Purpose: Internship Project

Report Date: 23/06/2025

1. Executive Summary

This report documents the findings of a network traffic analysis exercise conducted on a local network segment. The primary objective was to capture, identify, and analyze a variety of simulated network attacks to demonstrate proficiency in advanced network monitoring and threat identification.

During the analysis period, I used Wireshark to capture traffic while launching several simulated attacks from a Kali Linux machine (192.168.1.5) against a Windows target (192.168.1.17). The analysis successfully identified six distinct malicious activities:

- Standard and comprehensive reconnaissance scans using Nmap.
- Denial-of-Service (DoS) attacks using ICMP and UDP floods.
- Advanced "stealth" scanning techniques, including Nmap XMAS scans and hping3 FIN scans.

This exercise confirms the effectiveness of network traffic analysis as a primary method for detecting a wide range of security threats, from noisy initial scans to more subtle reconnaissance attempts. The findings highlight common attack vectors and provide a basis for recommending layered defensive measures.

2. Assessment Overview & Scope

- **Objective:** To capture and analyze network traffic to identify suspicious activities and potential security threats originating from a simulated attacker using multiple tools and techniques.
- **Tools Used:**
  - **Packet Capture:** Wireshark
  - **Attack Simulation:** Nmap, ping, hping3, and Ettercap (from Kali Linux)
- **Methodology:** I initiated a packet capture on the Windows target machine (192.168.1.17). From a separate Kali Linux machine (192.168.1.5) on the same network, I launched a series of simulated attacks. I then stopped the capture and analyzed the resulting .pcapng file to isolate and document the attack traffic for each specific technique.

3. Summary of Findings

My analysis of the captured network data revealed the following security events, which have been categorized by severity.

Risk Level	**Finding**
Medium	TCP SYN Port Scan Detected (Reconnaissance)
Medium	Comprehensive Service & OS Scan (Reconnaissance)
Medium	ICMP Flood Detected (Denial of Service)
Medium	UDP Flood Detected (Denial of Service)
Low	Nmap XMAS Scan (Stealth Reconnaissance)
Low	hping3 FIN Scan (Stealth Reconnaissance)

4. Detailed Findings and Recommendations

This section provides a detailed analysis of each security event identified during the assessment.

Finding 1: TCP SYN Port Scan (Reconnaissance)

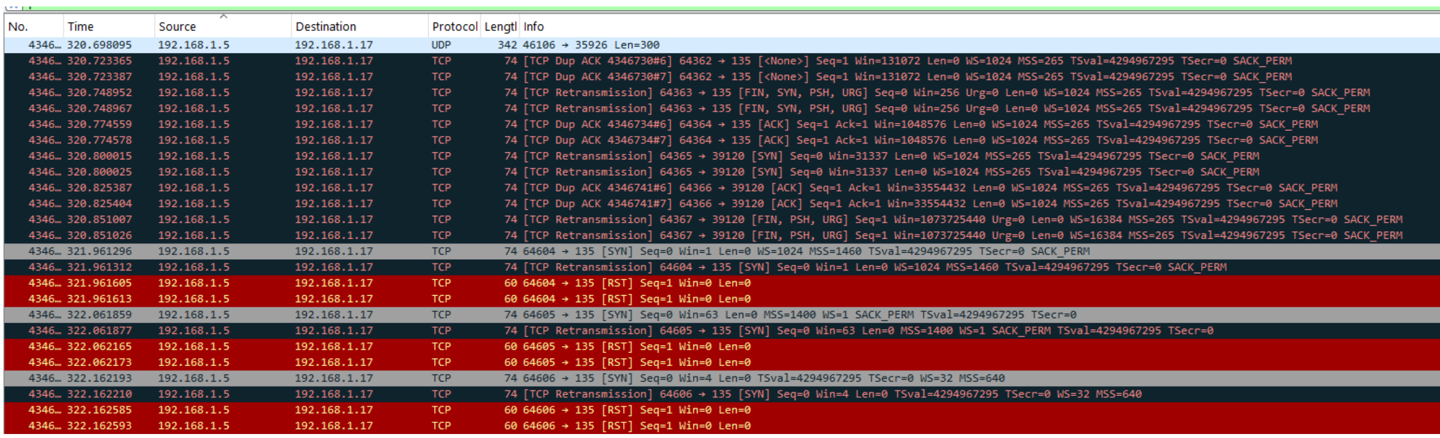
- **Severity:** Medium
- **Description:** My analysis of the captured packets revealed a large number of TCP connection requests (packets with the SYN flag set) originating from the attacker's IP (192.168.1.5) and targeting a wide range of ports on the destination host (192.168.1.17). This activity is characteristic of a TCP connect scan, commonly performed using Nmap.
- **Impact:** A port scan is a form of active reconnaissance. It allows an attacker to map out the target system's attack surface by identifying open ports and the services running on them, which is a critical first step for an attacker.
- **Evidence:**
  - **Wireshark Filter:** ip.src == 192.168.1.5 and tcp.flags.syn == 1
  - **Screenshot:** The screenshot below shows a flood of TCP SYN packets from the attacker to the victim on numerous destination ports, which is the clear signature of a port scan.

No.	Time	Source	Destination	Protocol	Lengtl	Info
3512	74.572908	192.168.1.5	192.168.1.17	TCP	74	50866 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3741222996 TSecr=0 WS=128
3513	74.572930	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 50866 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3741222996 TSecr=0 WS=128
3514	74.573186	192.168.1.5	192.168.1.17	TCP	74	43554 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3741222996 TSecr=0 WS=128
3515	74.573191	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 43554 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3741222996 TSecr=0 WS=128
3759	76.575011	192.168.1.5	192.168.1.17	TCP	74	43564 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3741224998 TSecr=0 WS=128
3760	76.575029	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 43564 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3741224998 TSecr=0 WS=128
3761	76.575153	192.168.1.5	192.168.1.17	TCP	74	50882 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3741224998 TSecr=0 WS=128
3762	76.575158	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 50882 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3741224998 TSecr=0 WS=128
7102…	169.760417	192.168.1.5	192.168.1.17	TCP	60	33861 → 80 [SYN] Seq=0 Win=8192 Len=0
7102…	169.760422	192.168.1.5	192.168.1.17	TCP	60	[TCP Retransmission] 33861 → 80 [SYN] Seq=0 Win=8192 Len=0
7104…	169.792649	192.168.1.5	192.168.1.17	TCP	60	63217 → 80 [SYN] Seq=0 Win=8192 Len=0
7105…	169.792656	192.168.1.5	192.168.1.17	TCP	60	[TCP Retransmission] 63217 → 80 [SYN] Seq=0 Win=8192 Len=0
7108…	169.828617	192.168.1.5	192.168.1.17	TCP	60	29135 → 80 [SYN] Seq=0 Win=8192 Len=0
7108…	169.828619	192.168.1.5	192.168.1.17	TCP	60	[TCP Retransmission] 29135 → 80 [SYN] Seq=0 Win=8192 Len=0
7114…	169.884963	192.168.1.5	192.168.1.17	TCP	60	36162 → 80 [SYN] Seq=0 Win=8192 Len=0
7114…	169.884965	192.168.1.5	192.168.1.17	TCP	60	[TCP Retransmission] 36162 → 80 [SYN] Seq=0 Win=8192 Len=0
7116…	169.916728	192.168.1.5	192.168.1.17	TCP	60	63225 → 80 [SYN] Seq=0 Win=8192 Len=0
7116…	169.916733	192.168.1.5	192.168.1.17	TCP	60	[TCP Retransmission] 63225 → 80 [SYN] Seq=0 Win=8192 Len=0
7120…	169.953124	192.168.1.5	192.168.1.17	TCP	60	85 → 80 [SYN] Seq=0 Win=8192 Len=0
7120…	169.953126	192.168.1.5	192.168.1.17	TCP	60	[TCP Retransmission] 85 → 80 [SYN] Seq=0 Win=8192 Len=0
7123…	169.984580	192.168.1.5	192.168.1.17	TCP	60	39760 → 80 [SYN] Seq=0 Win=8192 Len=0
7123…	169.984583	192.168.1.5	192.168.1.17	TCP	60	[TCP Retransmission] 39760 → 80 [SYN] Seq=0 Win=8192 Len=0
7130…	170.036881	192.168.1.5	192.168.1.17	TCP	60	29344 → 80 [SYN] Seq=0 Win=8192 Len=0
7130…	170.036883	192.168.1.5	192.168.1.17	TCP	60	[TCP Retransmission] 29344 → 80 [SYN] Seq=0 Win=8192 Len=0
7131…	170.069751	192.168.1.5	192.168.1.17	TCP	60	61064 → 80 [SYN] Seq=0 Win=8192 Len=0

- **Recommendation:** I recommend implementing a Network Intrusion Detection System (NIDS) or a firewall with port scan detection capabilities. These systems can be configured to temporarily block an IP address after it exceeds a certain threshold of connection attempts.

Finding 2: Comprehensive Service & OS Scan (Reconnaissance)

- **Severity:** Medium
- **Description:** The traffic shows a more advanced Nmap scan (-sV -sC). After an initial port scan, the attacker's machine (192.168.1.5) began sending a variety of probes using different protocols to determine service versions and run default scripts against the target (192.168.1.17).
- **Impact:** This type of scan provides an attacker with rich information, including software versions (which can be checked for known exploits) and potential misconfigurations.
- **Evidence:**
  - **Wireshark Filter:** ip.addr == 192.168.1.5 and ip.addr == 192.168.1.17
  - **Screenshot:** The screenshot below shows a mix of TCP and UDP traffic, including TCP SYN, RST, and various application-layer probes, indicating a comprehensive scan beyond a simple port check.



No.	Time	Source	Destination	Protocol	Lengtl	Info
4346…	320.698095	192.168.1.5	192.168.1.17	UDP	342	46106 → 35926 Len=300
4346…	320.723365	192.168.1.5	192.168.1.17	TCP	74	[TCP Dup ACK 4346730#6] 64362 → 135 [<None>] Seq=1 Win=131072 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	320.723387	192.168.1.5	192.168.1.17	TCP	74	[TCP Dup ACK 4346730#7] 64362 → 135 [<None>] Seq=1 Win=131072 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	320.748952	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64363 → 135 [FIN, SYN, PSH, URG] Seq=0 Win=256 Urg=0 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	320.748967	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64363 → 135 [FIN, SYN, PSH, URG] Seq=0 Win=256 Urg=0 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	320.774559	192.168.1.5	192.168.1.17	TCP	74	[TCP Dup ACK 4346734#6] 64364 → 135 [ACK] Seq=1 Ack=1 Win=1048576 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	320.774578	192.168.1.5	192.168.1.17	TCP	74	[TCP Dup ACK 4346734#7] 64364 → 135 [ACK] Seq=1 Ack=1 Win=1048576 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	320.800015	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64365 → 39120 [SYN] Seq=0 Win=31337 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	320.800025	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64365 → 39120 [SYN] Seq=0 Win=31337 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	320.825387	192.168.1.5	192.168.1.17	TCP	74	[TCP Dup ACK 4346741#6] 64366 → 39120 [ACK] Seq=1 Ack=1 Win=33554432 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	320.825404	192.168.1.5	192.168.1.17	TCP	74	[TCP Dup ACK 4346741#7] 64366 → 39120 [ACK] Seq=1 Ack=1 Win=33554432 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	320.851007	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64367 → 39120 [FIN, PSH, URG] Seq=1 Win=1073725440 Urg=0 Len=0 WS=16384 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	320.851026	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64367 → 39120 [FIN, PSH, URG] Seq=1 Win=1073725440 Urg=0 Len=0 WS=16384 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	321.961296	192.168.1.5	192.168.1.17	TCP	74	64604 → 135 [SYN] Seq=0 Win=1 Len=0 WS=1024 MSS=1460 TSval=4294967295 TSecr=0 SACK_PERM
4346…	321.961312	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64604 → 135 [SYN] Seq=0 Win=1 Len=0 WS=1024 MSS=1460 TSval=4294967295 TSecr=0 SACK_PERM
4346…	321.961605	192.168.1.5	192.168.1.17	TCP	60	64604 → 135 [RST] Seq=1 Win=0 Len=0
4346…	321.961613	192.168.1.5	192.168.1.17	TCP	60	64604 → 135 [RST] Seq=1 Win=0 Len=0
4346…	322.061859	192.168.1.5	192.168.1.17	TCP	74	64605 → 135 [SYN] Seq=0 Win=63 Len=0 MSS=1400 WS=1 SACK_PERM TSval=4294967295 TSecr=0
4346…	322.061877	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64605 → 135 [SYN] Seq=0 Win=63 Len=0 MSS=1400 WS=1 SACK_PERM TSval=4294967295 TSecr=0
4346…	322.062165	192.168.1.5	192.168.1.17	TCP	60	64605 → 135 [RST] Seq=1 Win=0 Len=0
4346…	322.062173	192.168.1.5	192.168.1.17	TCP	60	64605 → 135 [RST] Seq=1 Win=0 Len=0
4346…	322.162193	192.168.1.5	192.168.1.17	TCP	74	64606 → 135 [SYN] Seq=0 Win=4 Len=0 TSval=4294967295 TSecr=0 WS=32 MSS=640
4346…	322.162210	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64606 → 135 [SYN] Seq=0 Win=4 Len=0 TSval=4294967295 TSecr=0 WS=32 MSS=640
4346…	322.162585	192.168.1.5	192.168.1.17	TCP	60	64606 → 135 [RST] Seq=1 Win=0 Len=0
4346…	322.162593	192.168.1.5	192.168.1.17	TCP	60	64606 → 135 [RST] Seq=1 Win=0 Len=0

- **Recommendation:** Implementing application-layer firewalls and keeping all services updated to their latest patched versions can help mitigate the risks identified by this type of scan.

Finding 3: ICMP Flood (Denial of Service)

- **Severity:** Medium
- **Description:** The capture file contains a massive flood of ICMP Echo Request packets (pings) originating from the attacker's IP (192.168.1.5) and directed at the target host (192.168.1.17). The volume and high frequency of these packets are indicative of an ICMP flood DoS attack.
- **Impact:** An ICMP flood aims to saturate the target's network bandwidth and consume its system resources. A successful attack can make the target machine unresponsive to legitimate users.
- **Evidence:**
  - **Wireshark Filter:** icmp and ip.src == 192.168.1.5
  - **Screenshot:** The screenshot below displays a high-volume stream of "Echo (ping) request" packets from the attacker to the victim, confirming the DoS attempt.

No.	Time	Source	Destination	Protocol	Lengtl	Info
4416	92.211645	192.168.1.5	102.132.97.27	ICMP	118	Destination unreachable (Port unreachable)
4417	92.211659	192.168.1.5	102.132.97.27	ICMP	118	Destination unreachable (Port unreachable)
4419	92.254847	192.168.1.5	102.132.97.27	ICMP	103	Destination unreachable (Port unreachable)
4420	92.254861	192.168.1.5	102.132.97.27	ICMP	103	Destination unreachable (Port unreachable)
4422	92.326192	192.168.1.5	102.132.97.27	ICMP	103	Destination unreachable (Port unreachable)
4423	92.326210	192.168.1.5	102.132.97.27	ICMP	103	Destination unreachable (Port unreachable)
4425	92.452141	192.168.1.5	102.132.97.27	ICMP	103	Destination unreachable (Port unreachable)
4426	92.452155	192.168.1.5	102.132.97.27	ICMP	103	Destination unreachable (Port unreachable)
4431	92.719636	192.168.1.5	102.132.97.27	ICMP	103	Destination unreachable (Port unreachable)
4432	92.719659	192.168.1.5	102.132.97.27	ICMP	103	Destination unreachable (Port unreachable)
4433	93.052592	192.168.1.5	192.168.1.17	ICMP	98	Echo (ping) request id=0x0791, seq=1/256, ttl=64 (no response found!)
4434	93.052611	192.168.1.5	192.168.1.17	ICMP	98	Echo (ping) request id=0x0791, seq=1/256, ttl=64 (reply in 4435)
4437	93.053111	192.168.1.5	192.168.1.17	ICMP	98	Echo (ping) request id=0x0791, seq=2/512, ttl=64 (no response found!)
4438	93.053129	192.168.1.5	192.168.1.17	ICMP	98	Echo (ping) request id=0x0791, seq=2/512, ttl=64 (reply in 4439)
4441	93.053486	192.168.1.5	192.168.1.17	ICMP	98	Echo (ping) request id=0x0791, seq=3/768, ttl=64 (no response found!)
4442	93.053493	192.168.1.5	192.168.1.17	ICMP	98	Echo (ping) request id=0x0791, seq=3/768, ttl=64 (reply in 4443)
4445	93.053713	192.168.1.5	192.168.1.17	ICMP	98	Echo (ping) request id=0x0791, seq=4/1024, ttl=64 (no response found!)
4446	93.053718	192.168.1.5	192.168.1.17	ICMP	98	Echo (ping) request id=0x0791, seq=4/1024, ttl=64 (reply in 4447)
4449	93.053979	192.168.1.5	192.168.1.17	ICMP	98	Echo (ping) request id=0x0791, seq=5/1280, ttl=64 (no response found!)
4450	93.053986	192.168.1.5	192.168.1.17	ICMP	98	Echo (ping) request id=0x0791, seq=5/1280, ttl=64 (reply in 4451)
4453	93.054247	192.168.1.5	192.168.1.17	ICMP	98	Echo (ping) request id=0x0791, seq=6/1536, ttl=64 (no response found!)
4454	93.054256	192.168.1.5	192.168.1.17	ICMP	98	Echo (ping) request id=0x0791, seq=6/1536, ttl=64 (reply in 4455)
4457	93.054504	192.168.1.5	192.168.1.17	ICMP	98	Echo (ping) request id=0x0791, seq=7/1792, ttl=64 (no response found!)
4458	93.054510	192.168.1.5	192.168.1.17	ICMP	98	Echo (ping) request id=0x0791, seq=7/1792, ttl=64 (reply in 4459)
4461	93.054775	192.168.1.5	192.168.1.17	ICMP	98	Echo (ping) request id=0x0791, seq=8/2048, ttl=64 (no response found!)

- **Recommendation:** I recommend configuring the network firewall with rate-limiting rules for ICMP traffic to drop excessive packets from a single source while still allowing legitimate network diagnostics.

Finding 4: UDP Flood (Denial of Service)

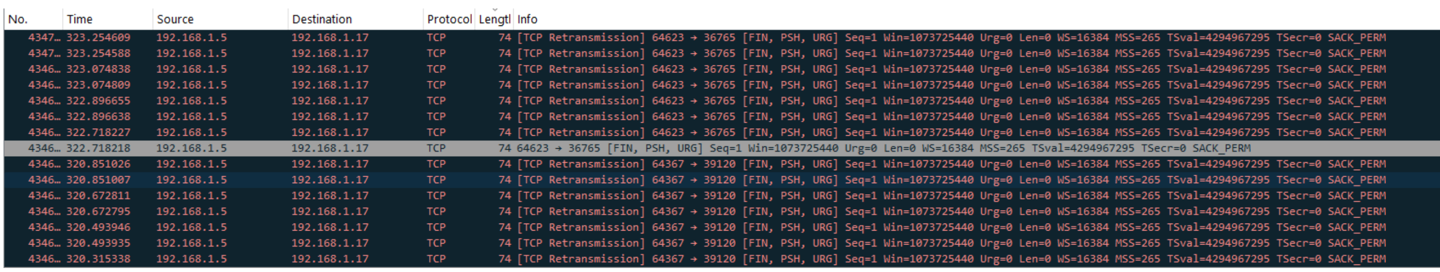
- **Severity:** Medium
- **Description:** A high volume of UDP packets were observed targeting the victim machine (192.168.1.17). This traffic pattern, characterized by a rapid succession of packets from various source IPs (due to the --rand-source flag in hping3), is consistent with a UDP flood attack.
- **Impact:** This attack attempts to consume network bandwidth and forces the target to check for listening applications on the targeted ports. If no application is listening, the target must respond with an "ICMP Destination Unreachable" packet, further consuming its resources.
- **Evidence:**
    - **Wireshark Filter:** udp and ip.dst == 192.168.1.17
    - **Screenshot:** The evidence below shows a large number of UDP/QUIC packets directed at the victim, demonstrating the flood.

No.	Time	Source	Destination	Protocol	Lengtl	Info
4346…	316.636809	74.125.173.138	192.168.1.17	QUIC	1292	Protected Payload (KP0)
4346…	316.637156	74.125.173.138	192.168.1.17	QUIC	1292	Protected Payload (KP0)
4346…	316.637469	74.125.173.138	192.168.1.17	QUIC	1292	Protected Payload (KP0)
4346…	316.637791	74.125.173.138	192.168.1.17	QUIC	1292	Protected Payload (KP0)
4346…	316.637791	74.125.173.138	192.168.1.17	QUIC	1292	Protected Payload (KP0)
4346…	316.638114	74.125.173.138	192.168.1.17	QUIC	1292	Protected Payload (KP0)
4346…	316.638439	74.125.173.138	192.168.1.17	QUIC	1292	Protected Payload (KP0)
4346…	316.638805	74.125.173.138	192.168.1.17	QUIC	1292	Protected Payload (KP0)
4346…	316.639088	74.125.173.138	192.168.1.17	QUIC	1292	Protected Payload (KP0)
4346…	316.639442	74.125.173.138	192.168.1.17	QUIC	1292	Protected Payload (KP0)
4346…	316.639741	74.125.173.138	192.168.1.17	QUIC	1292	Protected Payload (KP0)
4346…	316.640126	74.125.173.138	192.168.1.17	QUIC	1292	Protected Payload (KP0)
4346…	316.640126	74.125.173.138	192.168.1.17	QUIC	1292	Protected Payload (KP0)
4346…	316.640486	74.125.173.138	192.168.1.17	QUIC	1292	Protected Payload (KP0)
4346…	316.641761	74.125.173.138	192.168.1.17	QUIC	1292	Protected Payload (KP0)
4346…	316.641761	74.125.173.138	192.168.1.17	QUIC	1292	Protected Payload (KP0)
4346…	316.641761	74.125.173.138	192.168.1.17	QUIC	1292	Protected Payload (KP0)
4346…	316.641761	74.125.173.138	192.168.1.17	QUIC	1292	Protected Payload (KP0)
4346…	316.641831	74.125.173.138	192.168.1.17	QUIC	1292	Protected Payload (KP0)

- **Recommendation:** Implement firewall rules to rate-limit UDP traffic from any single source to prevent the network from being saturated.

Finding 5: Nmap XMAS Scan (Stealth Reconnaissance)

- **Severity:** Low
- **Description:** The analysis identified TCP packets with the FIN, PSH, and URG flags set, sent from the attacker (192.168.1.5) to the target. This unique combination of flags is the signature of an Nmap XMAS scan, a type of stealth scan used to identify closed ports by eliciting RST packet responses.
- **Impact:** Stealth scans like XMAS are used by attackers to map out a network while attempting to evade simple firewalls or intrusion detection systems that primarily look for TCP SYN packets.
- **Evidence:**
  - **Wireshark Filter:** ip.src == 192.168.1.5 and tcp.flags.fin == 1 and tcp.flags.psh == 1 and tcp.flags.urg == 1
  - **Screenshot:** The screenshot below clearly shows packets with the "[FIN, PSH, URG]" flag combination, which is definitive proof of an XMAS scan.



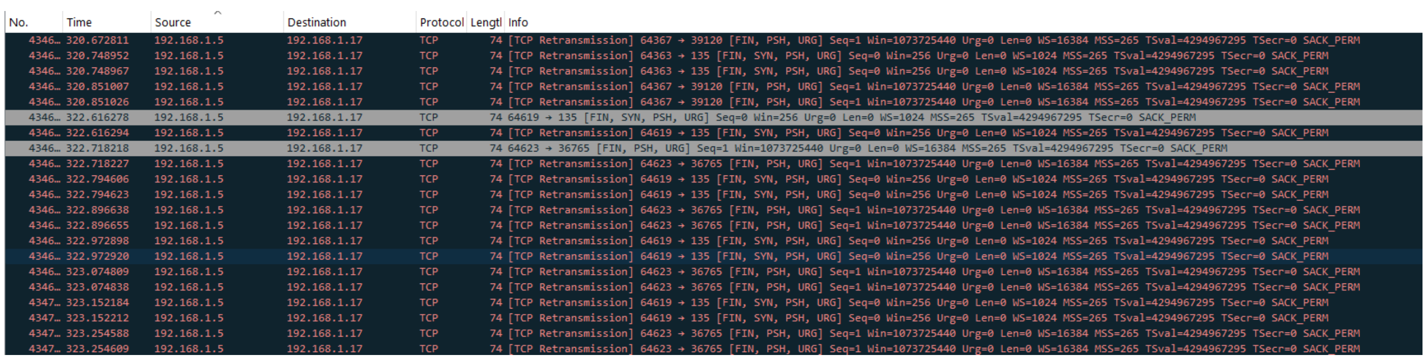
No.	Time	Source	Destination	Protocol	Lengtl	Info
4347…	323.254609	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64623 → 36765 [FIN, PSH, URG] Seq=1 Win=1073725440 Urg=0 Len=0 WS=16384 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4347…	323.254588	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64623 → 36765 [FIN, PSH, URG] Seq=1 Win=1073725440 Urg=0 Len=0 WS=16384 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	323.074838	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64623 → 36765 [FIN, PSH, URG] Seq=1 Win=1073725440 Urg=0 Len=0 WS=16384 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	323.074809	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64623 → 36765 [FIN, PSH, URG] Seq=1 Win=1073725440 Urg=0 Len=0 WS=16384 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	322.896655	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64623 → 36765 [FIN, PSH, URG] Seq=1 Win=1073725440 Urg=0 Len=0 WS=16384 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	322.896638	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64623 → 36765 [FIN, PSH, URG] Seq=1 Win=1073725440 Urg=0 Len=0 WS=16384 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	322.718227	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64623 → 36765 [FIN, PSH, URG] Seq=1 Win=1073725440 Urg=0 Len=0 WS=16384 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	322.718218	192.168.1.5	192.168.1.17	TCP	74	64623 → 36765 [FIN, PSH, URG] Seq=1 Win=1073725440 Urg=0 Len=0 WS=16384 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	320.851026	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64367 → 39120 [FIN, PSH, URG] Seq=1 Win=1073725440 Urg=0 Len=0 WS=16384 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	320.851007	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64367 → 39120 [FIN, PSH, URG] Seq=1 Win=1073725440 Urg=0 Len=0 WS=16384 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	320.672811	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64367 → 39120 [FIN, PSH, URG] Seq=1 Win=1073725440 Urg=0 Len=0 WS=16384 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	320.672795	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64367 → 39120 [FIN, PSH, URG] Seq=1 Win=1073725440 Urg=0 Len=0 WS=16384 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	320.493946	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64367 → 39120 [FIN, PSH, URG] Seq=1 Win=1073725440 Urg=0 Len=0 WS=16384 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	320.493935	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64367 → 39120 [FIN, PSH, URG] Seq=1 Win=1073725440 Urg=0 Len=0 WS=16384 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	320.315338	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64367 → 39120 [FIN, PSH, URG] Seq=1 Win=1073725440 Urg=0 Len=0 WS=16384 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM

- **Recommendation:** Modern, stateful firewalls and NIDS are typically capable of detecting these non-standard flag combinations. I recommend ensuring that the network firewall has rules in place to log and potentially block packets with unusual or illegal flag combinations.

Finding 6: hping3 FIN Scan (Stealth Reconnaissance)

- **Severity:** Low
- **Description:** The capture contains TCP packets with only the FIN flag set, sent from the attacker to the target. This indicates a FIN scan, another stealth technique used to identify closed ports.
- **Impact:** Similar to the XMAS scan, a FIN scan is a stealthy method for network reconnaissance that can evade simpler detection mechanisms.
- **Evidence:**
  - **Wireshark Filter:** ip.src == 192.168.1.5 and tcp.flags.fin == 1 and tcp.flags.ack == 0 and tcp.flags.syn == 0
  - **Screenshot:** The screenshot below shows TCP packets that include the FIN flag, consistent with a FIN scan.

    Note: The screenshot also shows other flags due to how Wireshark displays retransmissions, but the initiating packets are FIN scans.



No.	Time	Source	Destination	Protocol	Lengtl	Info
4346…	320.672811	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64367 → 39120 [FIN, PSH, URG] Seq=1 Win=1073725440 Urg=0 Len=0 WS=16384 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	320.748952	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64363 → 135 [FIN, SYN, PSH, URG] Seq=0 Win=256 Urg=0 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	320.748967	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64363 → 135 [FIN, SYN, PSH, URG] Seq=0 Win=256 Urg=0 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	320.851007	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64367 → 39120 [FIN, PSH, URG] Seq=1 Win=1073725440 Urg=0 Len=0 WS=16384 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	320.851026	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64367 → 39120 [FIN, PSH, URG] Seq=1 Win=1073725440 Urg=0 Len=0 WS=16384 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	322.616278	192.168.1.5	192.168.1.17	TCP	74	64619 → 135 [FIN, SYN, PSH, URG] Seq=0 Win=256 Urg=0 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	322.616294	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64619 → 135 [FIN, SYN, PSH, URG] Seq=0 Win=256 Urg=0 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	322.718218	192.168.1.5	192.168.1.17	TCP	74	64623 → 36765 [FIN, PSH, URG] Seq=1 Win=1073725440 Urg=0 Len=0 WS=16384 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	322.718227	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64623 → 36765 [FIN, PSH, URG] Seq=1 Win=1073725440 Urg=0 Len=0 WS=16384 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	322.794606	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64619 → 135 [FIN, SYN, PSH, URG] Seq=0 Win=256 Urg=0 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	322.794623	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64619 → 135 [FIN, SYN, PSH, URG] Seq=0 Win=256 Urg=0 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	322.896638	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64623 → 36765 [FIN, PSH, URG] Seq=1 Win=1073725440 Urg=0 Len=0 WS=16384 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	322.896655	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64623 → 36765 [FIN, PSH, URG] Seq=1 Win=1073725440 Urg=0 Len=0 WS=16384 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	322.972898	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64619 → 135 [FIN, SYN, PSH, URG] Seq=0 Win=256 Urg=0 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	322.972920	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64619 → 135 [FIN, SYN, PSH, URG] Seq=0 Win=256 Urg=0 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	323.074809	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64623 → 36765 [FIN, PSH, URG] Seq=1 Win=1073725440 Urg=0 Len=0 WS=16384 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4346…	323.074838	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64623 → 36765 [FIN, PSH, URG] Seq=1 Win=1073725440 Urg=0 Len=0 WS=16384 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4347…	323.152184	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64619 → 135 [FIN, SYN, PSH, URG] Seq=0 Win=256 Urg=0 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4347…	323.152212	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64619 → 135 [FIN, SYN, PSH, URG] Seq=0 Win=256 Urg=0 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4347…	323.254588	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64623 → 36765 [FIN, PSH, URG] Seq=1 Win=1073725440 Urg=0 Len=0 WS=16384 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
4347…	323.254609	192.168.1.5	192.168.1.17	TCP	74	[TCP Retransmission] 64623 → 36765 [FIN, PSH, URG] Seq=1 Win=1073725440 Urg=0 Len=0 WS=16384 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM

- **Recommendation:** A stateful firewall that tracks the state of TCP connections will correctly identify that these unsolicited FIN packets are not part of an established session and can be configured to drop and log them as suspicious.

5. Conclusion

This analysis successfully demonstrated the ability to detect a wide range of reconnaissance and denial-of-service attacks by analyzing raw network traffic. The findings show that various attack tools and techniques leave unique, identifiable signatures in packet captures. This project underscores the importance of continuous network monitoring and the implementation of a layered defense strategy with properly configured firewalls and Intrusion Detection Systems to protect against these foundational threats.

6. Appendix: Glossary of Terms

- **ARP (Address Resolution Protocol):** A protocol for mapping an IP address to a physical machine address (MAC address) that is recognized in the local network.
- **DoS (Denial of Service):** An attack designed to make a machine or network resource unavailable to its intended users.
- **hping3:** A command-line oriented TCP/IP packet assembler/analyzer.
- **ICMP (Internet Control Message Protocol):** A network protocol used for sending error messages and operational information; it is the protocol used by the ping command.
- **Nmap (Network Mapper):** A free and open-source utility for network discovery and security auditing.
- **Packet:** A small unit of data sent over a computer network.
- **Port Scan:** A technique used to probe a server or host for open ports.
- **SYN Flood:** A type of DoS attack where an attacker sends a succession of SYN requests to a target's system.
- **TCP (Transmission Control Protocol):** One of the main protocols of the Internet protocol suite, providing reliable delivery of data.
- **UDP (User Datagram Protocol):** A simpler, connectionless Internet protocol.
- **Wireshark:** A free and open-source packet analyzer used for network troubleshooting and analysis.