NMAP PORT SCANNING TECHNIQUES

This report provides a breakdown of multiple Nmap port scanning techniques performed in a controlled home lab environment. The objective is to understand how each scan works, interpret responses, and analyze packet level behavior using Wireshark.

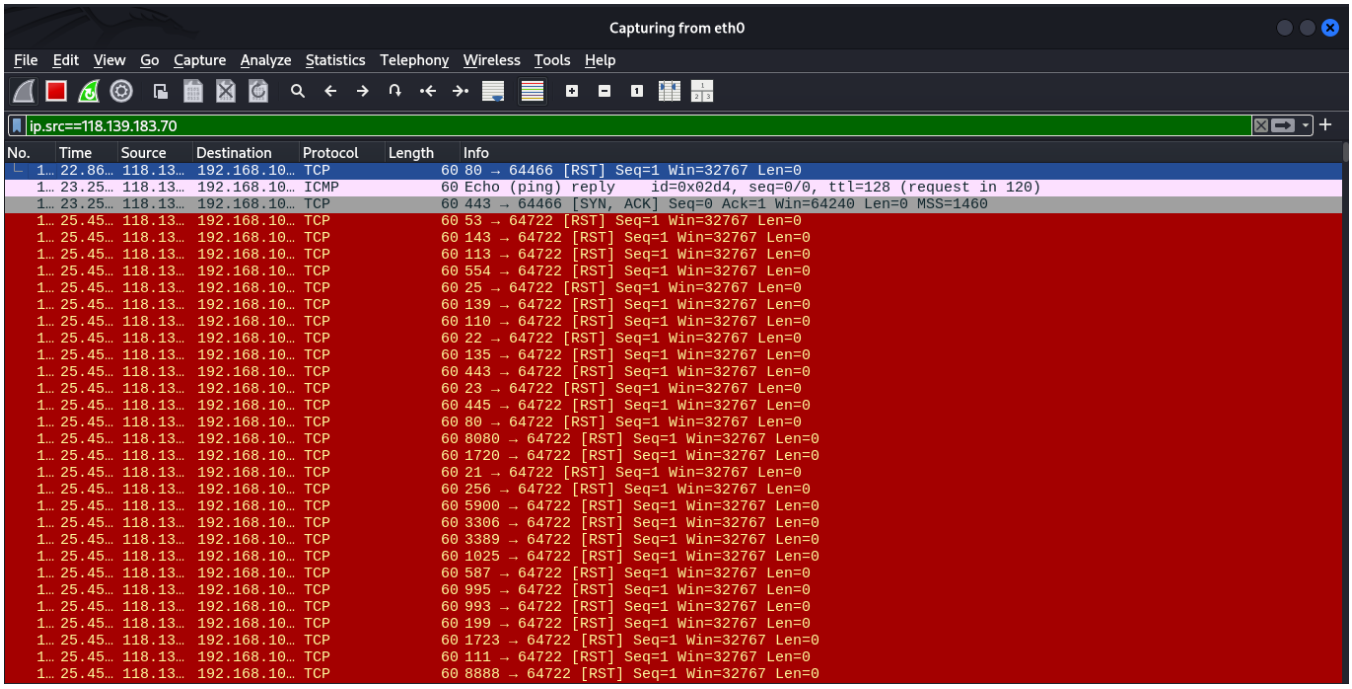
Introduction :

In this project, I performed multiple Nmap port scanning techniques in my home lab environment to understand how each scan works, how hosts respond, and how traffic appears in Wireshark.

1) ACK Scan (-sA) :

ACK scan is used to identify firewall filtering rules. It helps determine whether ports are filtered or unfiltered.

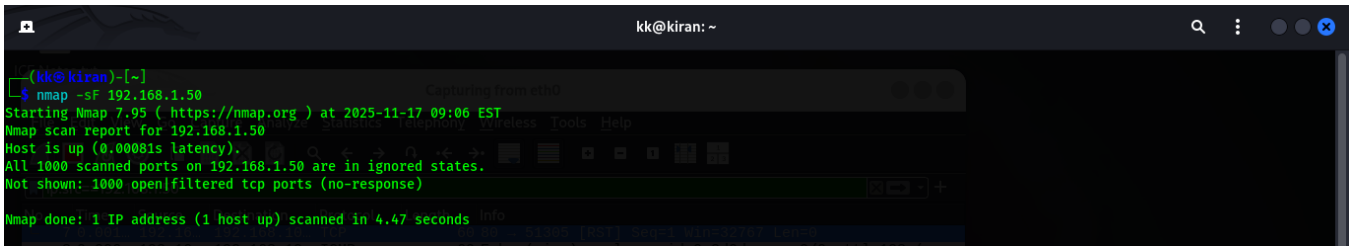
nmap –sA <Target ipaddress>

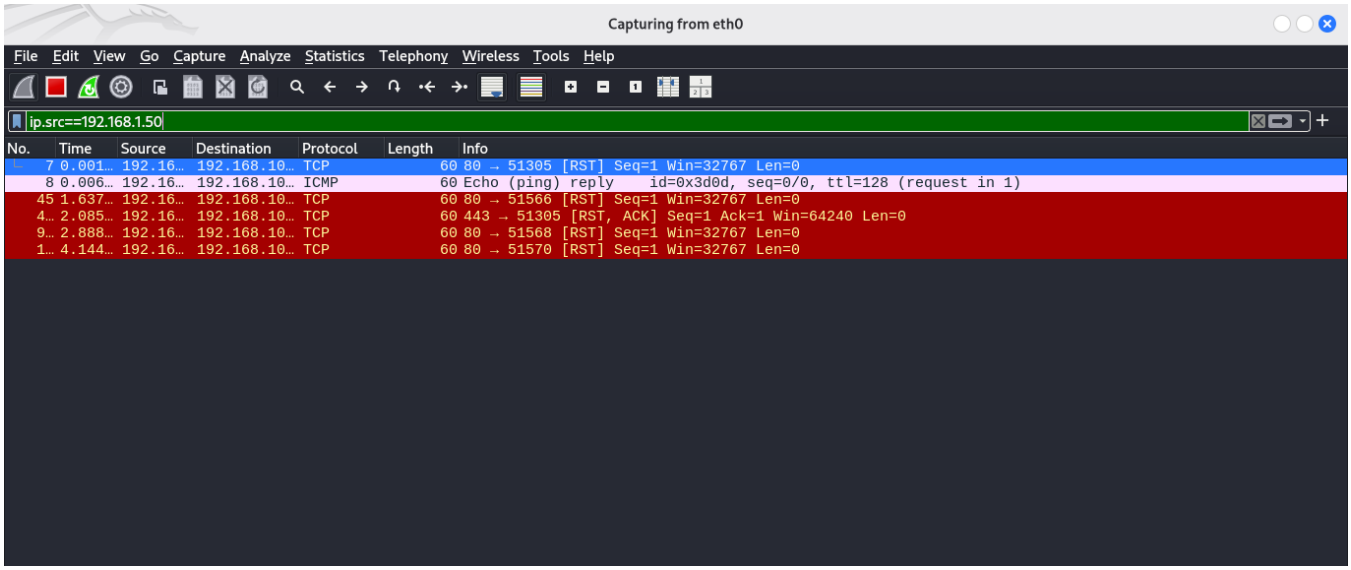


2) **FIN Scan :**

- Stealth scanning (avoids detection on some systems)
- Discovering **open vs closed ports** based on response behavior
- Testing systems that follow RFC 793 behavior

Command - nmap –sF <Target ipaddress>

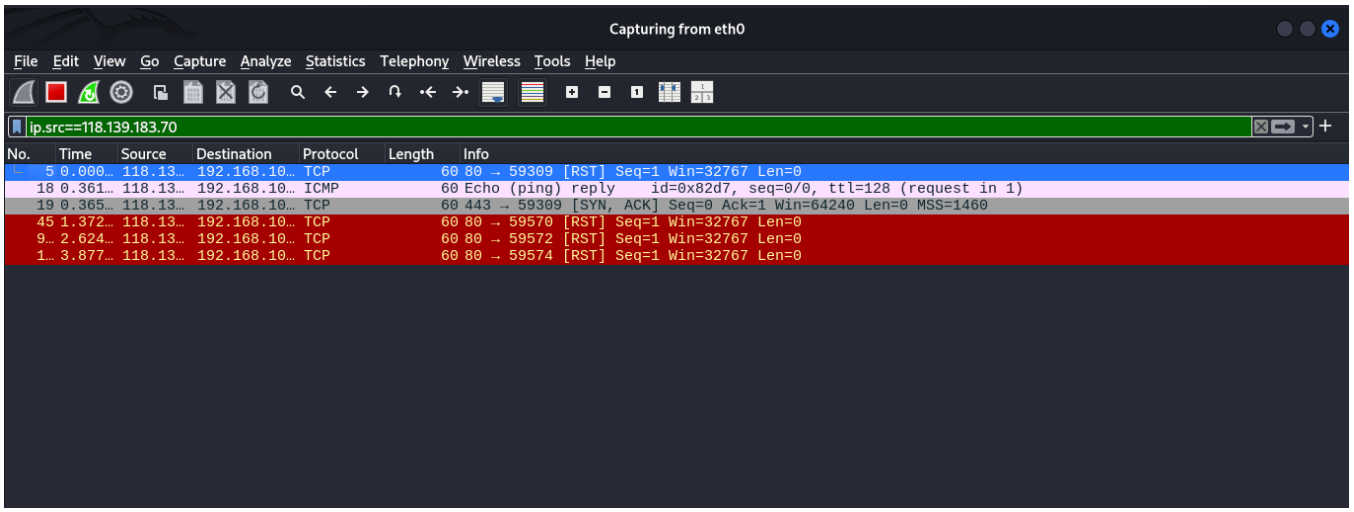




3) NULL Scan :

- Stealth scanning
- Identifying how targets respond to packets with **no flags**
- Detecting open ports on systems that ignore malformed packets

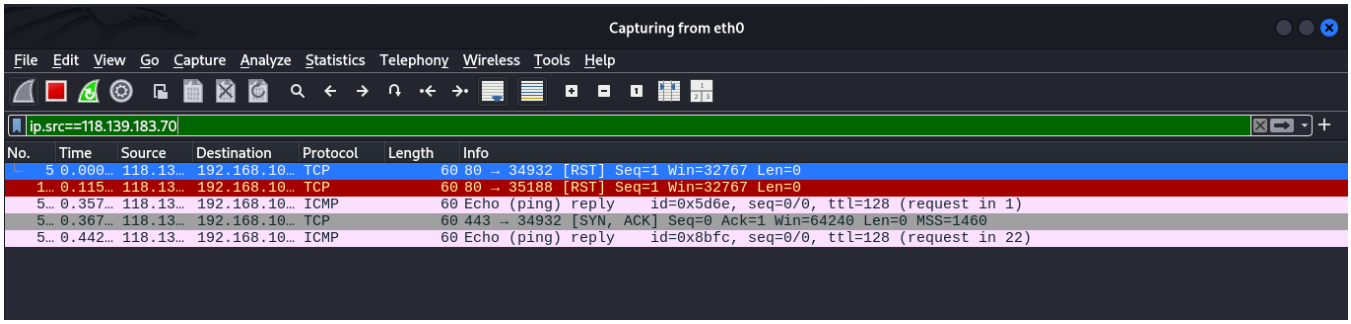
Command - nmap –sN <Target ipaddress>



3) Protocol Scan :

- Host discovery (checking if a machine is up)
- Network mapping and live host scanning

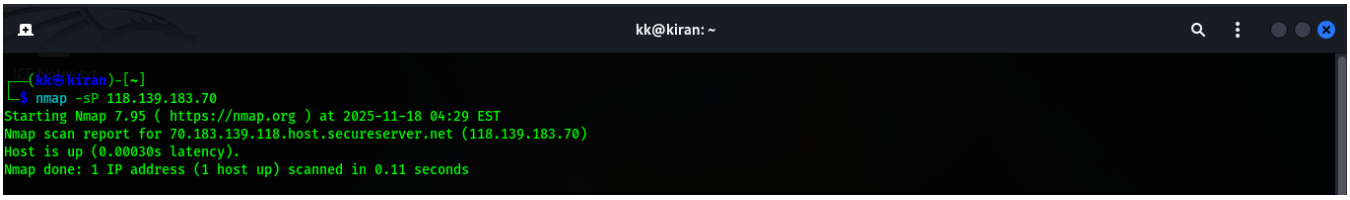
nmap –sO <Target ipaddress>

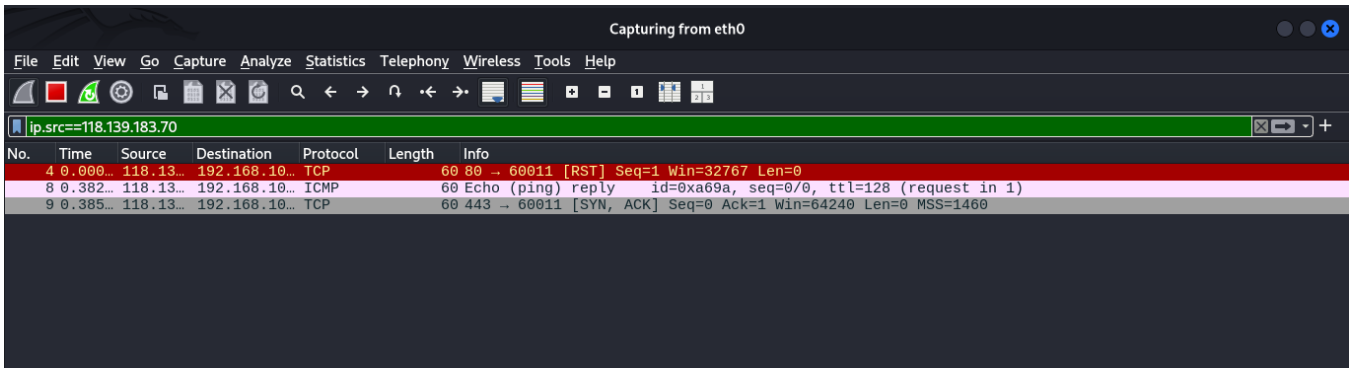


4) Ping Scan :

- Host discovery (checking if a machine is up)
- Network mapping and live host scanning

Command - nmap –sP <Target ipaddress>

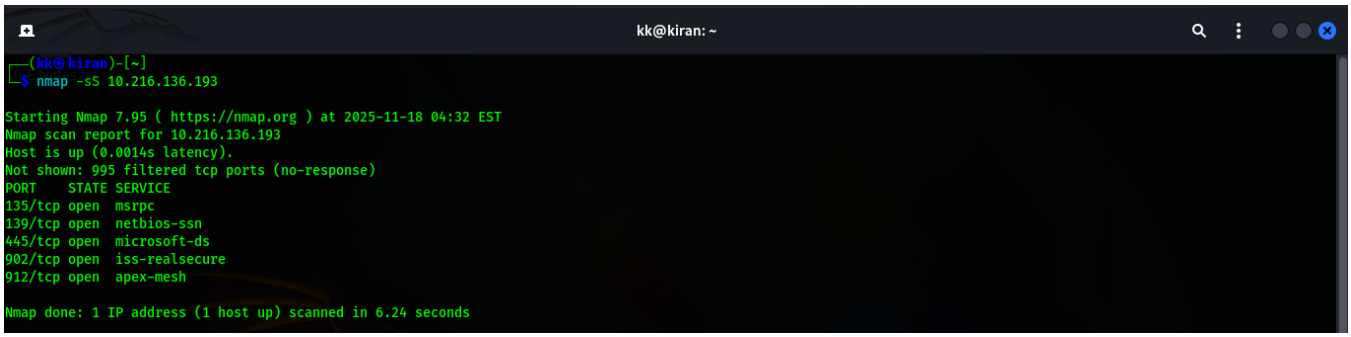


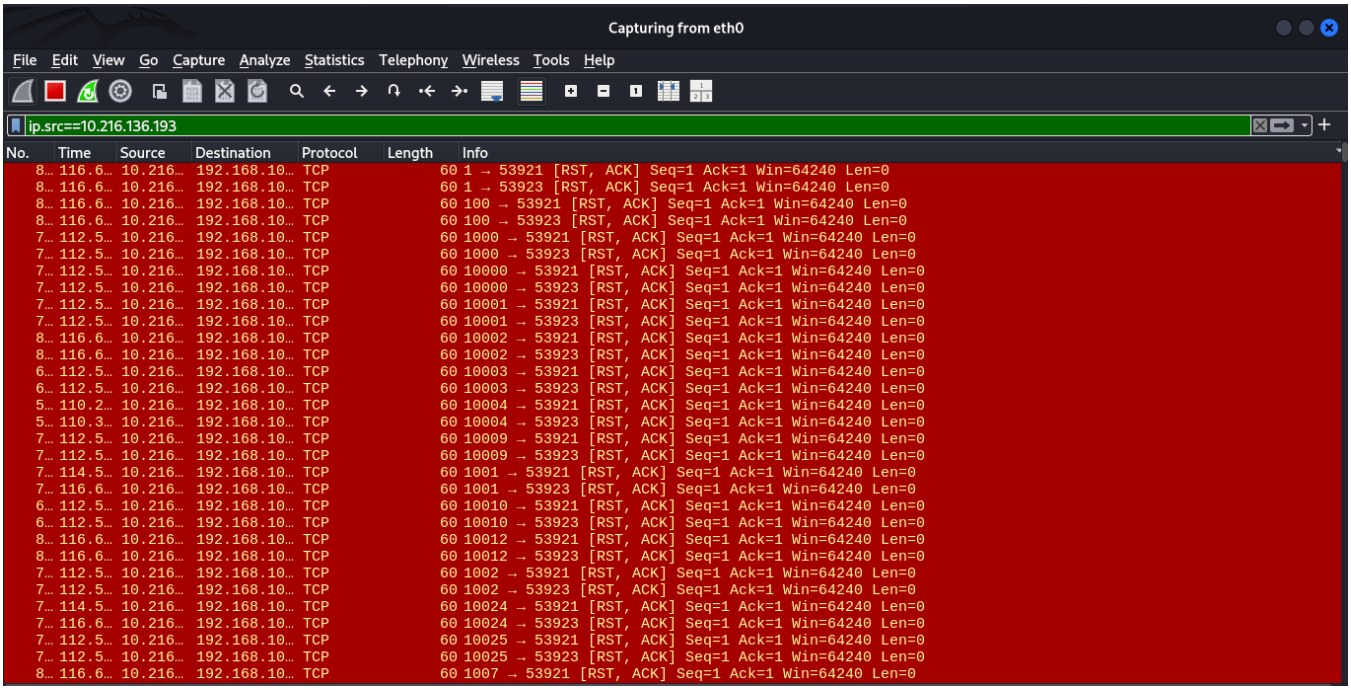


6) SYN Scan :

- Fast, stealthy port scanning
- Half-open scan avoids completing TCP handshake
- Identifying **open/closed/filtered** ports accurately

Command - Nmap –sS <Target ipaddress>

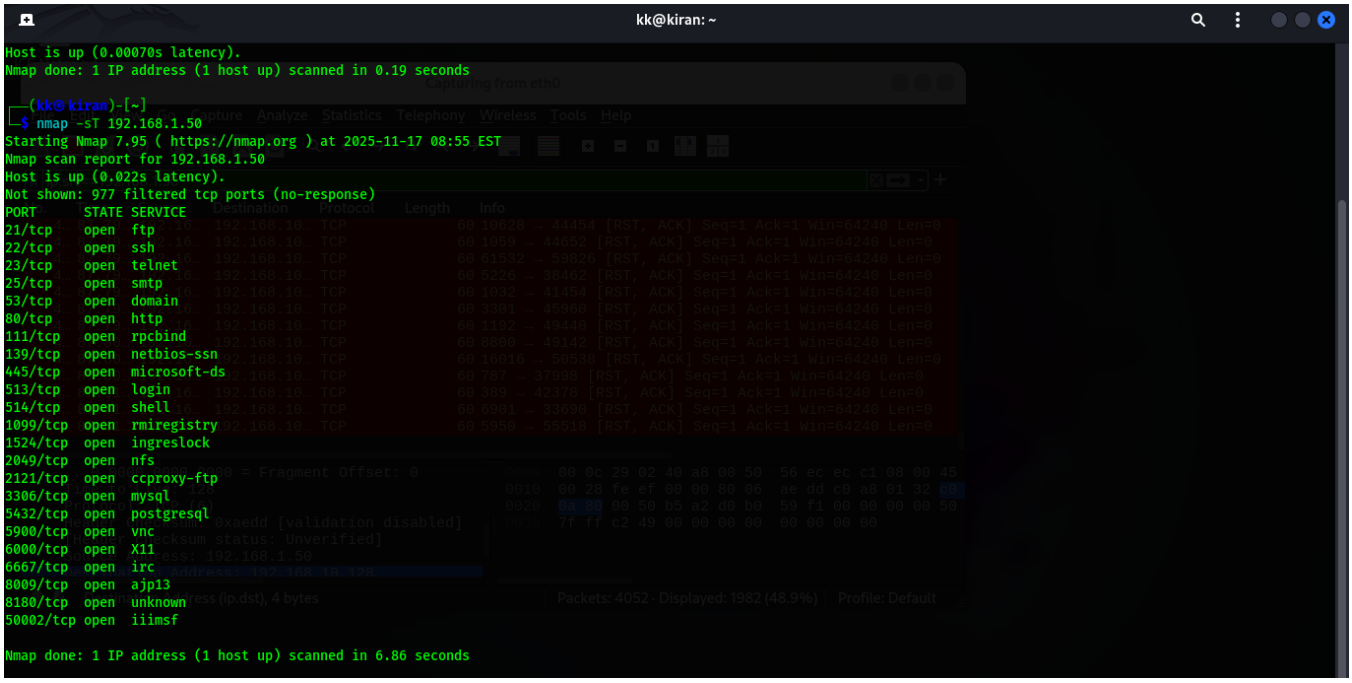


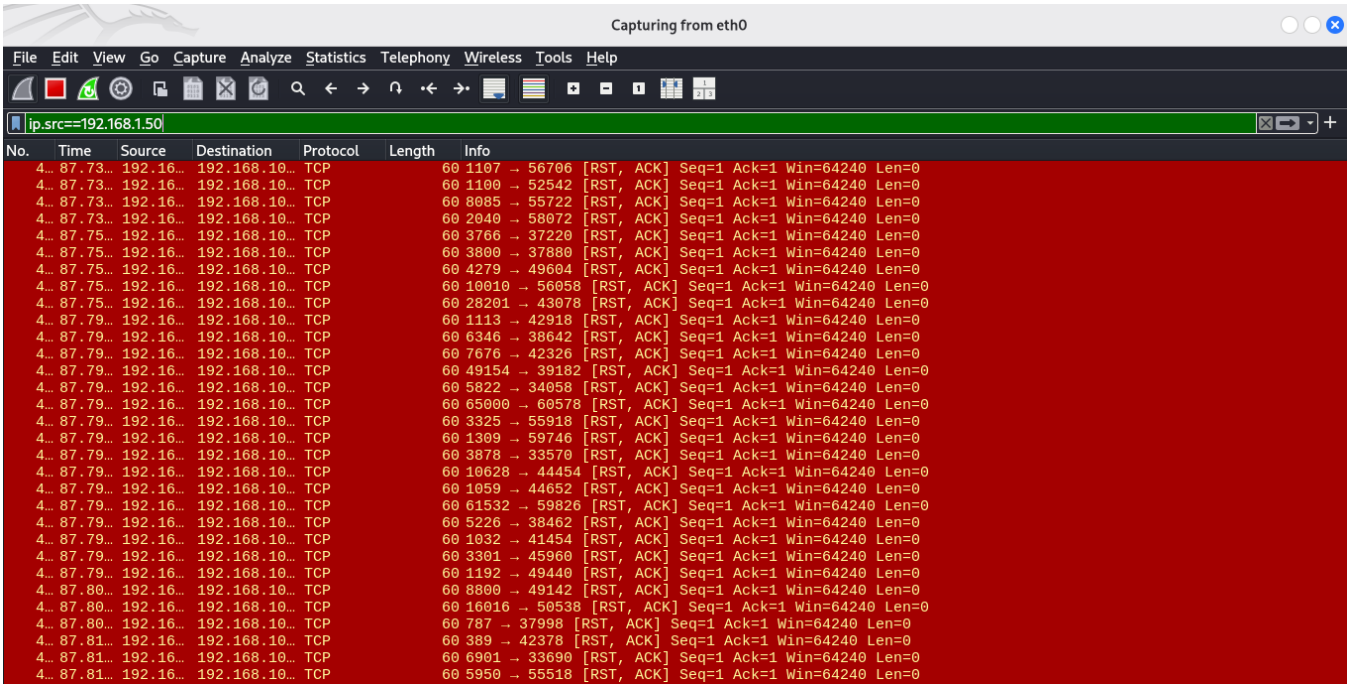


7) TCP Scan :

- Scanning when SYN scan is **not allowed** or requires privileges
- Fully completes TCP handshake to identify open ports
- Reliable but less stealthy

Command - nmap –sT <Target ipaddress>

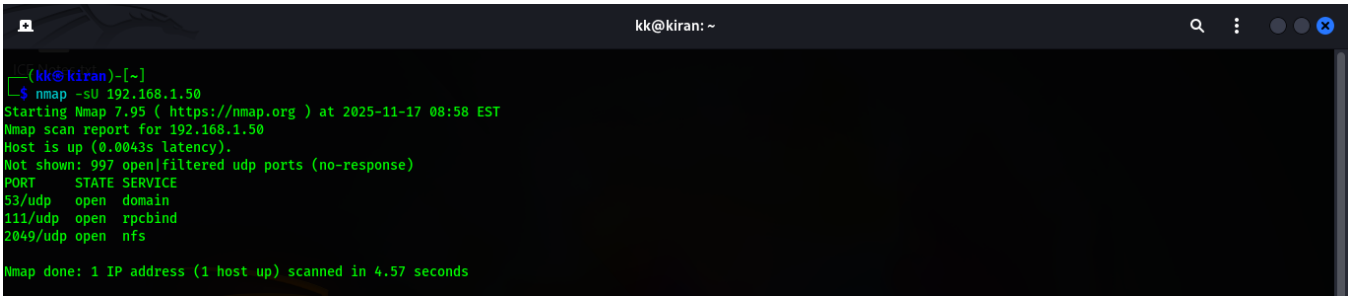


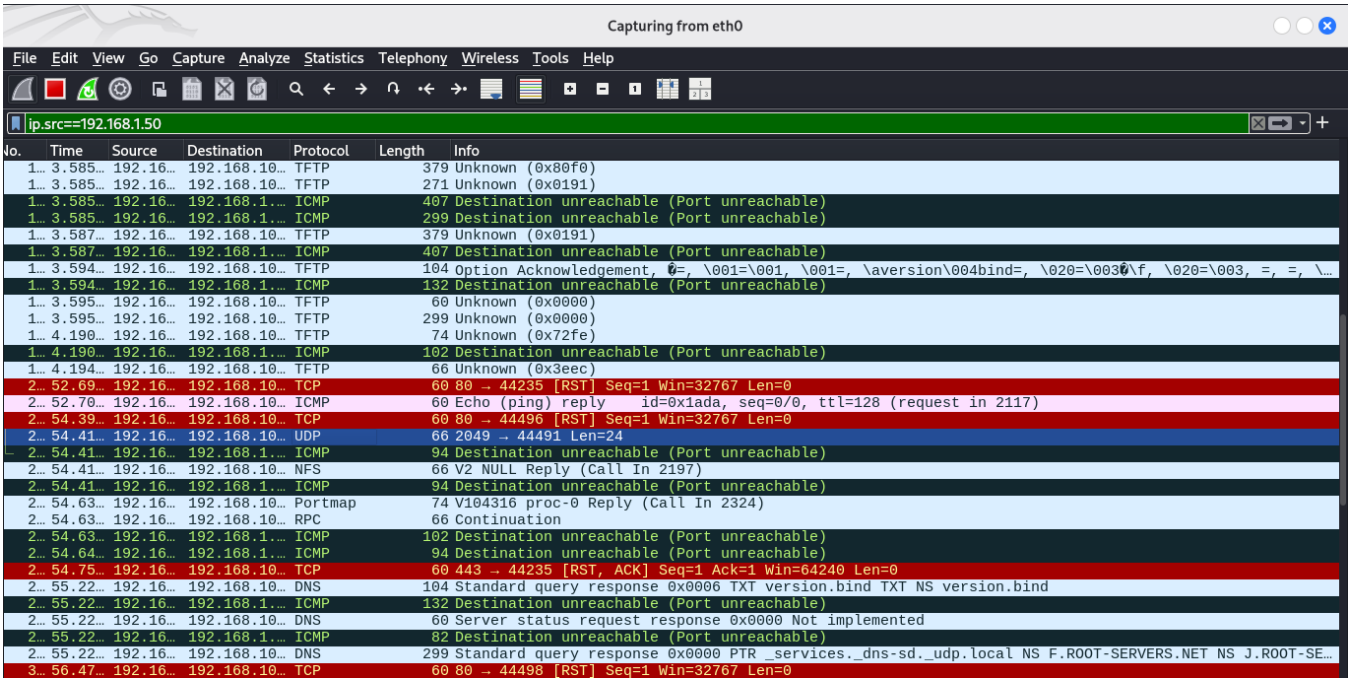


8) UDP Scan :

- Discovering opened **UDP-based services** (DNS, DHCP, SNMP)
- Finding services not detected by TCP scans
- Network enumeration

Command - nmap –sU <Target ipaddress>

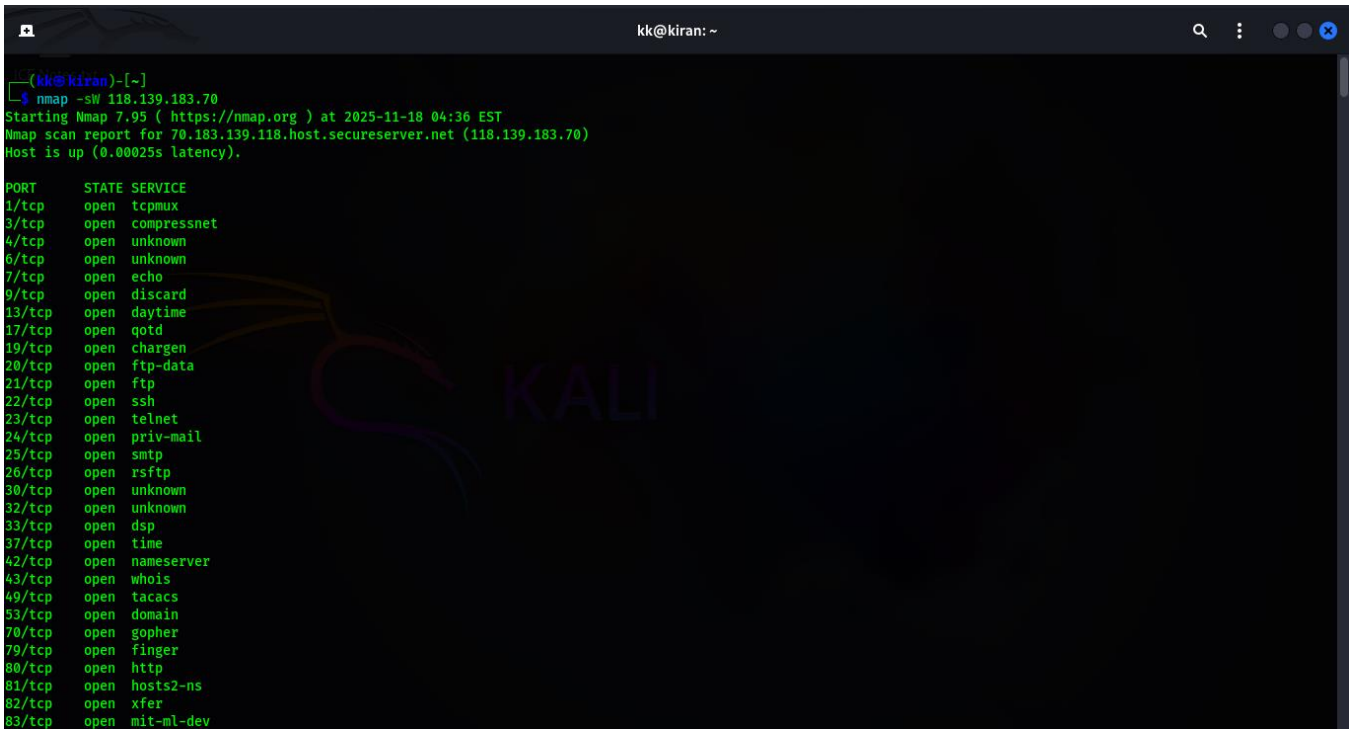


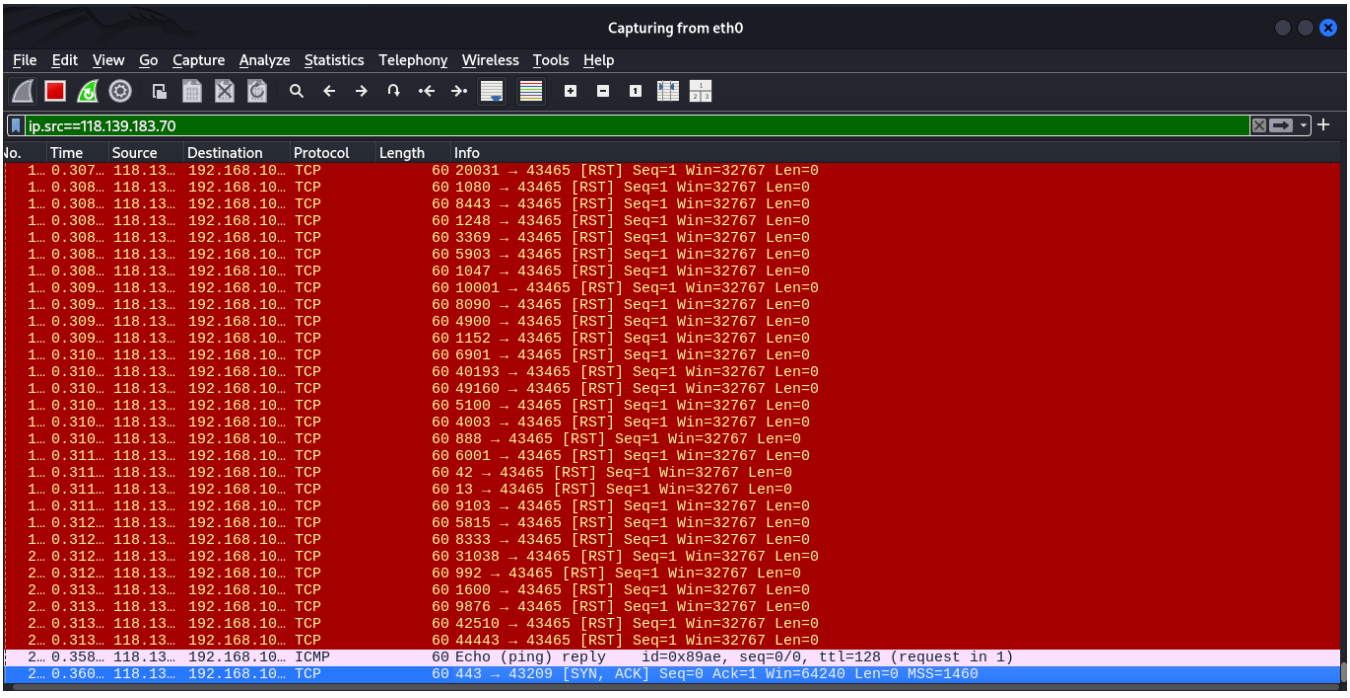


9) Windows Scan :

- Detecting open ports using TCP window size differences
- Works well on **Windows-based systems**
- Alternative to SYN/FIN/NULL scans

Command - nmap –sW <Target ipaddress>

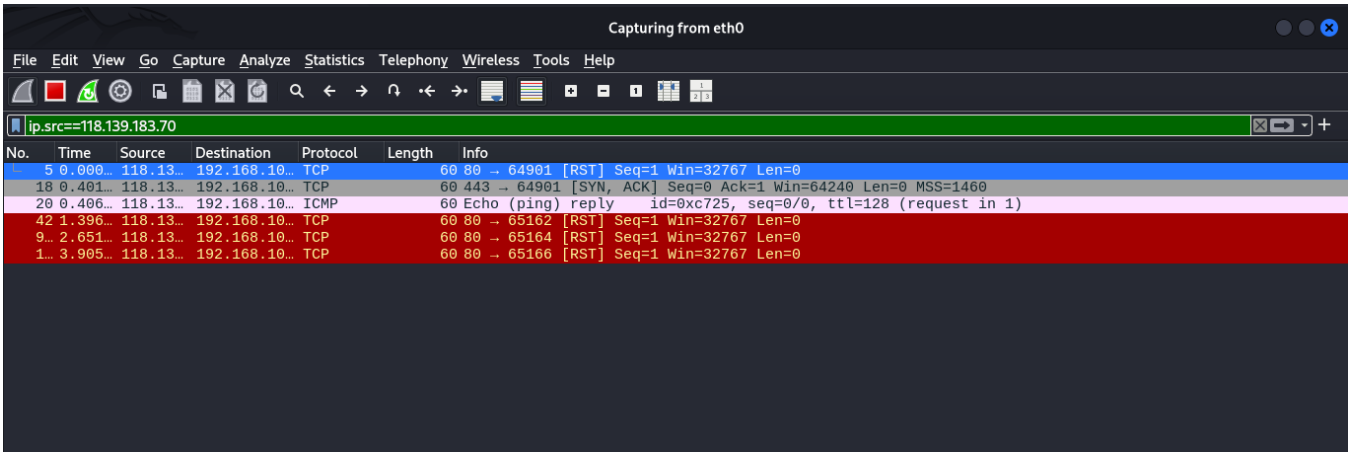




10) XMAS Scan :

- Stealth scanning with FIN + PSH + URG flags
- Detecting open/closed ports on RFC-compliant systems
- Avoiding some IDS/IPS detection methods

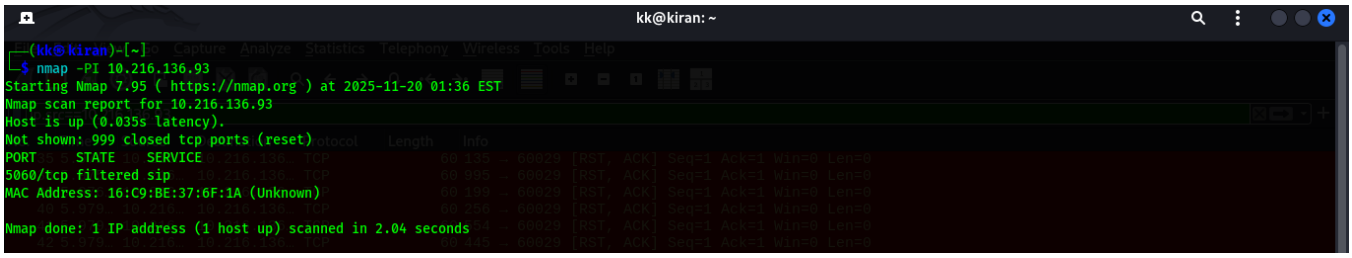
Command - nmap –sX <Target ipaddress>

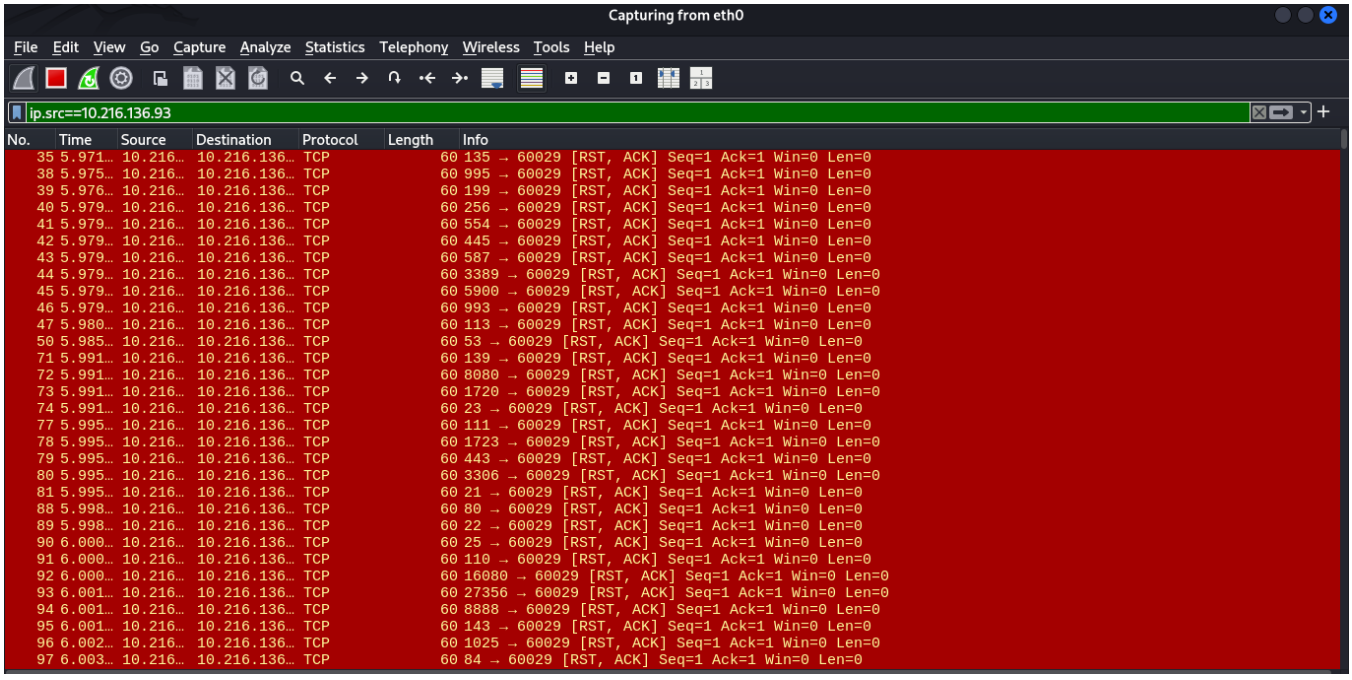


11) ICMP Ping :

- Host discovery using **ICMP Echo Request**
- Detecting reachable hosts in a network
- Network reconnaissance

Command - nmap -PI <Target ip address

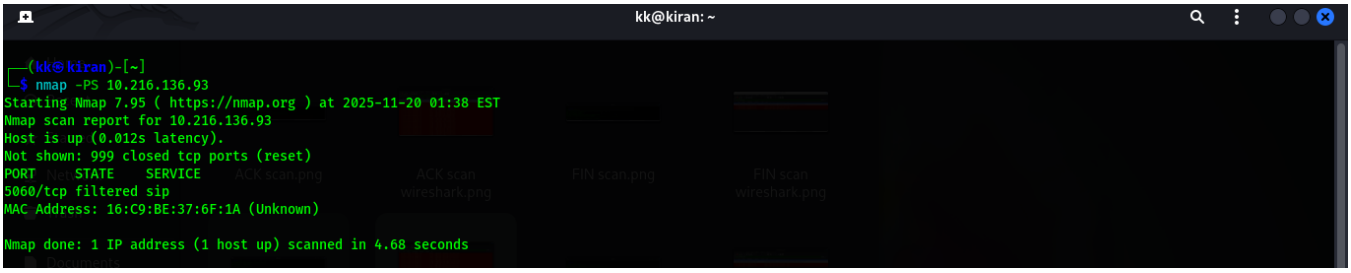


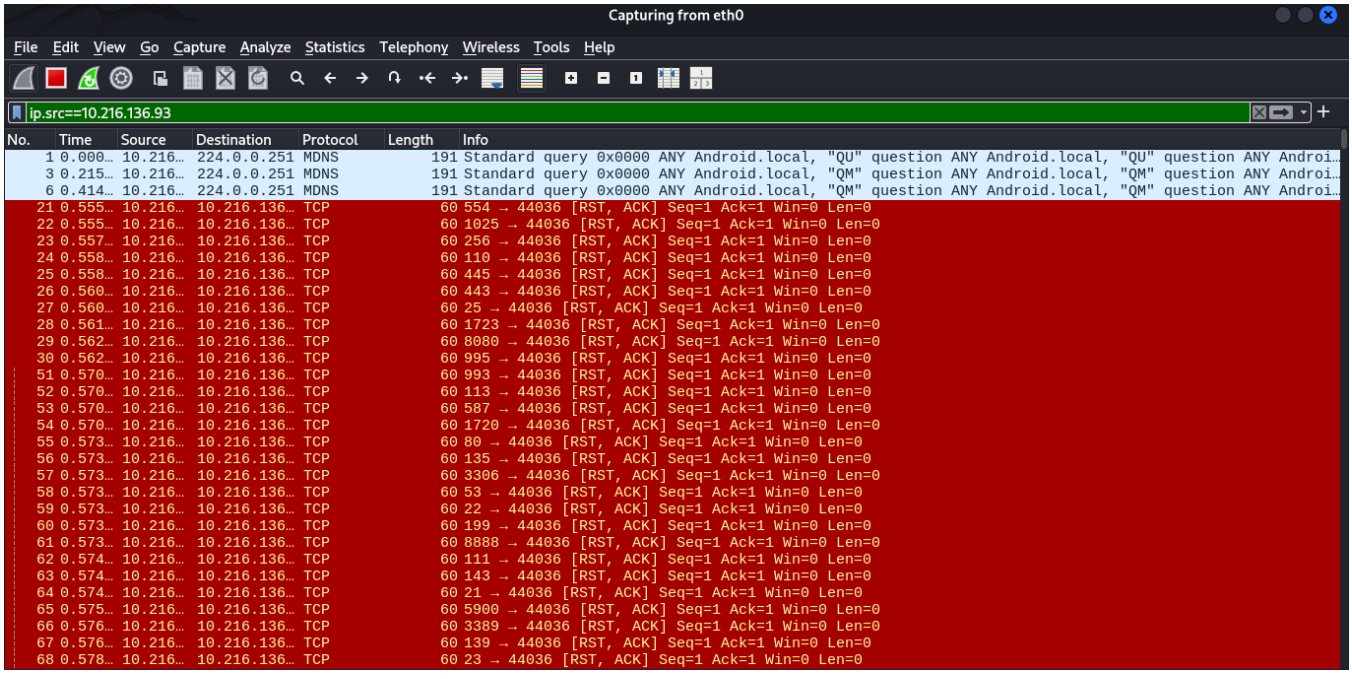


12) SYN Ping :

- Host discovery using SYN packets
- Useful when ICMP is blocked
- Detecting active hosts behind firewalls

Command - nmap -PS <Target ip address>

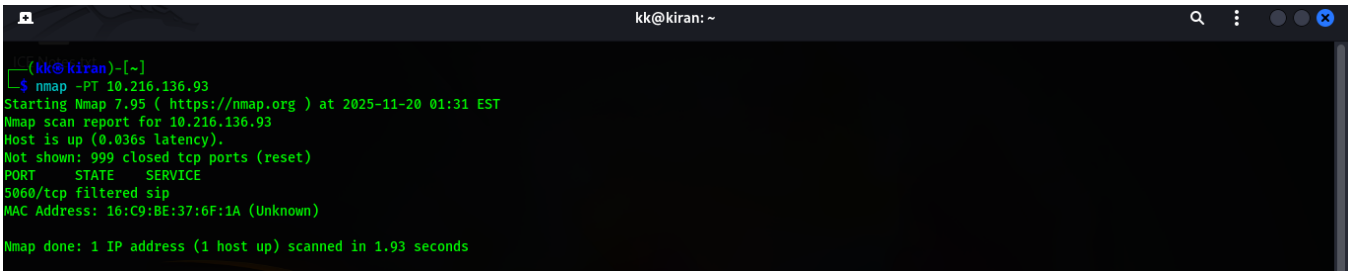


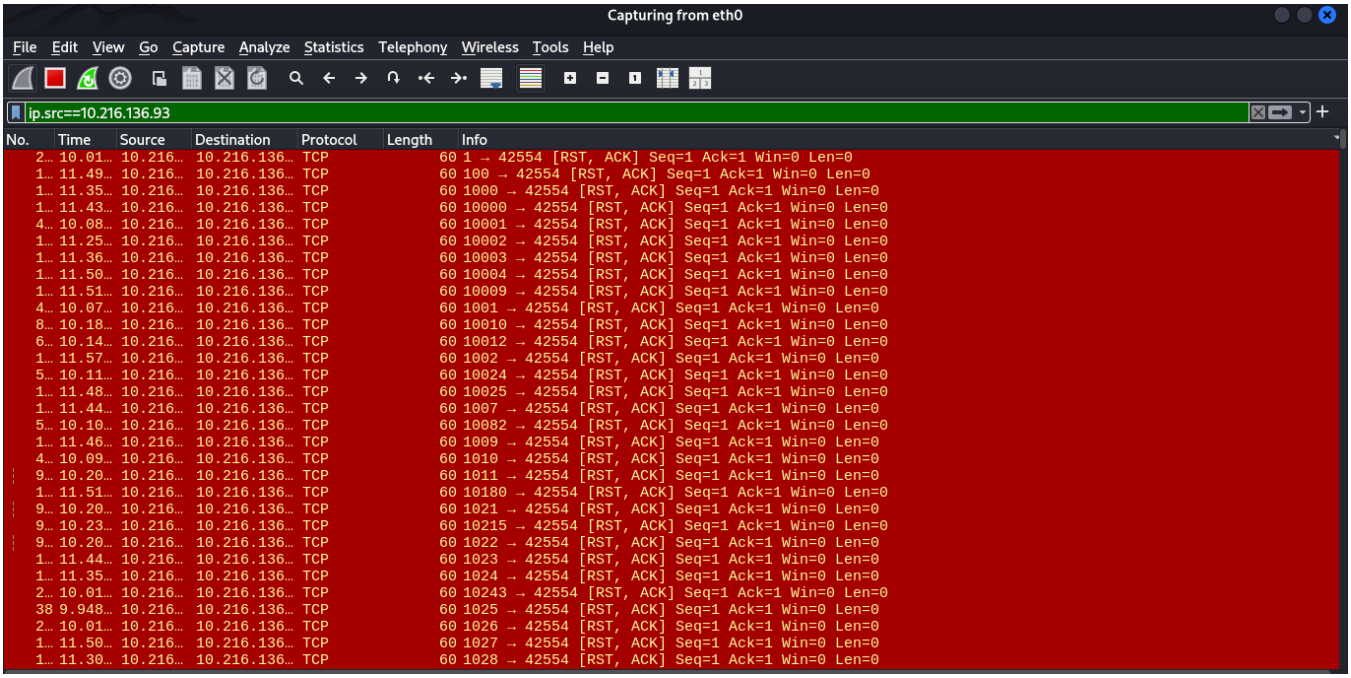


13) TCP Ping :

- Host discovery using TCP ACK packets
- Works even when ICMP is filtered
- Identifying ALIVE hosts without scanning ports

Command - nmap -PT <Target ip address>

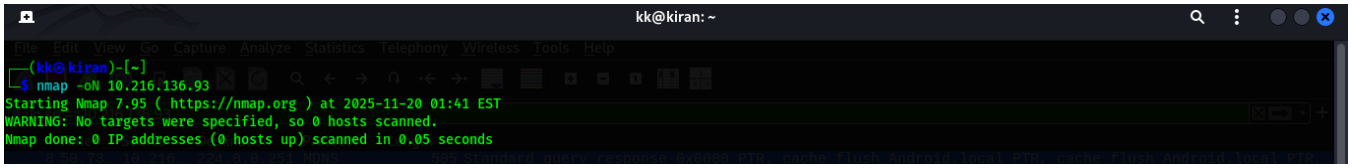


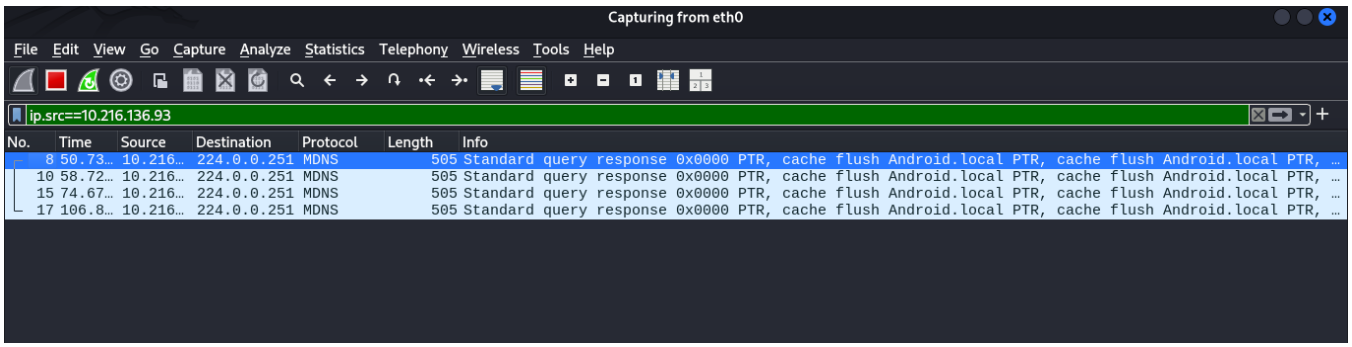


14) Normal Output :

- Saving scan results in **human-readable format**
- Good for reports and documentation
- Easily readable in text editors

Command - nmap -oN <Target ip address>

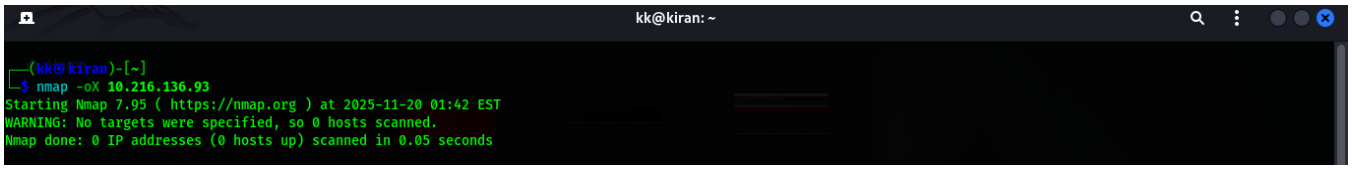


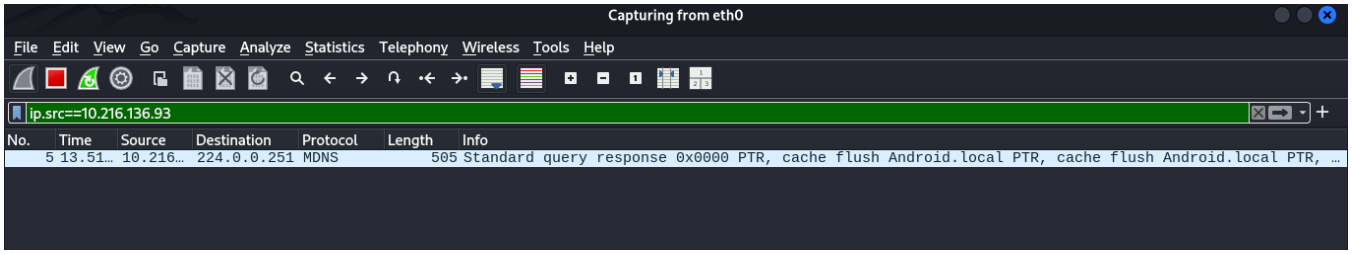


15) XML Output :

- Saving scan results in XML format
- Automation, scripting, and log parsing
- Importing results into security tools (e.g., Nessus, OpenVAS dashboards)

Command - nmap -oX <Target ip address>





Summary Table :

Scan Type	Purpose	Typical Response / Behavior
ACK Scan (-sA)	Detect firewall filtering rules	RST = unfiltered, No response = filtered
FIN Scan (-sF)	Stealth scan; identify open/closed ports	No response = open/filtered, RST = closed
NULL Scan (-sN)	Stealth scan with no flags	No response = open/filtered, RST = closed
Protocol Scan (-sO)	Discover supported IP protocols	ICMP unreachable or protocol responses
Ping Scan (-sP)	Check if host is up	ICMP echo reply = host alive
SYN Scan (-sS)	Fast, stealthy half-open scan	SYN/ACK = open, RST = closed
TCP Connect Scan (-sT)	Full connection scan (3-way handshake)	Full connect = open, RST = closed
UDP Scan (-sU)	Identify UDP services	No response = open/filtered, ICMP unreachable = closed
Windows Scan (-sW)	Detect open/closed ports using Windows TCP	Closed ports send RST with specific window size
XMAS Scan (-sX)	FIN+PSH+URG stealth scan	No response = open/filtered, RST = closed
ICMP Ping (-PI)	Host discovery using ICMP	ICMP echo reply = host reachable
SYN Ping (-PS)	Host discovery with SYN packets	SYN/ACK or RST = host alive
TCP Ping (-PT)	Host discovery with TCP ACK packets	RST = host alive
Normal Output (-oN)	Save human-readable scan output	Stores readable results in .txt file
XML Output (-oX)	Save output in XML format	Used for automation, scripts, parsing tools

Conclusion : This project helped me understand how different port scanning techniques work, how firewalls respond, and how traffic appears inside Wireshark. This knowledge is essential for both offensive and defensive cybersecurity roles.