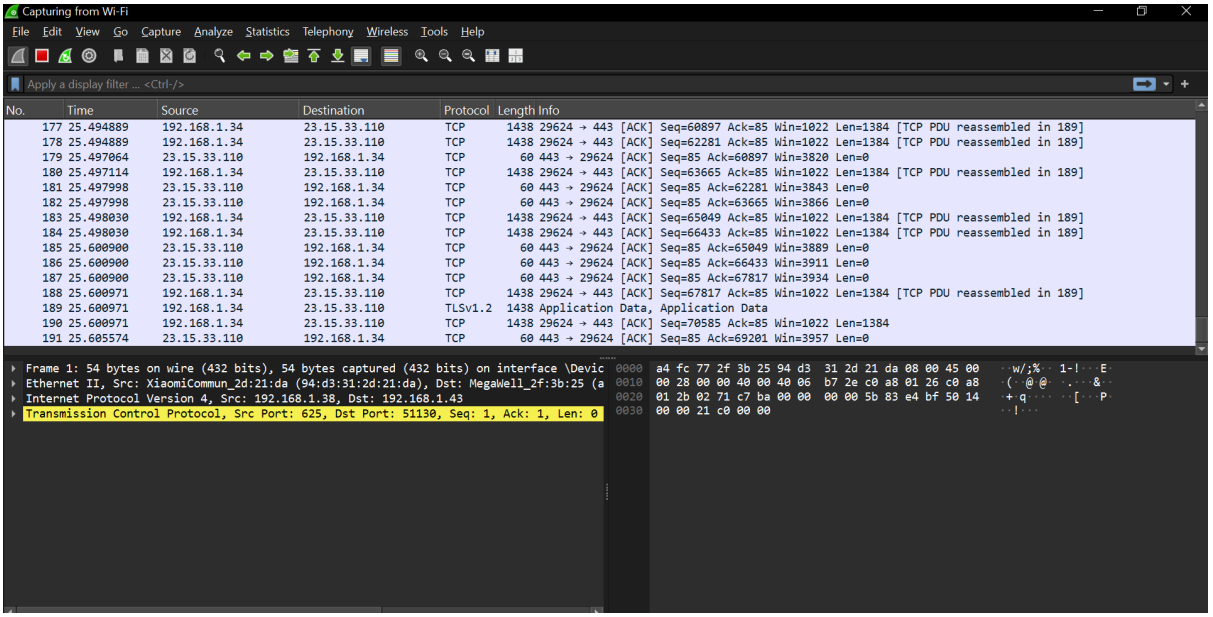
TASK-1


File Actions Edit View Help
(kali㉿kali)-[~/Desktop]
$ nmap -sS 192.168.1.1/24
Starting Nmap 7.95 (https://nmap.org) at 2025-05-26 09:11 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0039s latency).
Not shown: 993 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
23/tcp filtered telnet
53/tcp open domain
80/tcp open http
139/tcp filtered netbios-ssn
443/tcp open https
445/tcp filtered microsoft-ds
MAC Address: 54:47:E8:82:AC:7E (Syrotech Networks.)
Nmap scan report for 192.168.1.34
Host is up (0.0014s latency).
All 1000 scanned ports on 192.168.1.34 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: A4:FC:77:2F:3B:25 (Mega Well Limited)
Nmap scan report for 192.168.1.37
Host is up (0.013s latency).
All 1000 scanned ports on 192.168.1.37 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 7C:46:85:C0:22:47 (Motorola (Wuhan) Mobility Technologies Communication)
Nmap scan report for 192.168.1.38
Host is up (0.33s latency).
All 1000 scanned ports on 192.168.1.38 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 94:D3:31:2D:21:DA (Xiaomi Communications)
Nmap scan report for 192.168.1.49
Host is up (0.0075s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT STATE SERVICE
135/tcp open msrpc
2179/tcp open vmrdp
MAC Address: 90:2E:16:C8:B7:45 (LCFC(HeFei) Electronics Technology)
Nmap scan report for 192.168.1.43
Host is up (0.0000050s latency).
All 1000 scanned ports on 192.168.1.43 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Nmap done: 256 IP addresses (6 hosts up) scanned in 153.33 seconds
(kali㉿kali)-[~/Desktop]
$



1. IP Addresses and Open Ports Found

192.168.1.1:
- Open Ports: 21 (FTP), 53 (DNS), 80 (HTTP), 443 (HTTPS)
- MAC Address: 54:47:E8:82:AC:7E (Syrotech Networks)

192.168.1.34:
- No open ports (all filtered)
- MAC Address: 44:FC:77:2F:3B:25 (Mega Well Limited)

192.168.1.37:
- No open ports (all closed)
- MAC Address: 7C:46:85:C0:22:47 (Motorola, Wuhan Mobility Technologies Communication)

192.168.1.38:
- No open ports (all closed)
- MAC Address: 44:D3:31:2D:1A:03 (Xiaomi Communications)

192.168.1.49:
- Open Ports: 135 (MSRPC), 2179 (VMRDP)
- MAC Address: 90:2E:16:C8:B7:45 (LCFC (HeFei) Electronics Technology)

192.168.1.43:
- No open ports (all closed)
- MAC Address: Not shown

2. Common Services on Open Ports

- Port 21 (FTP): File Transfer Protocol; often insecure if using plaintext authentication.
- Port 53 (DNS): Domain Name System for resolving hostnames.
- Port 80 (HTTP): Unencrypted web traffic.

- Port 443 (HTTPS): Encrypted web traffic using TLS/SSL.
- Port 135 (MSRPC): Microsoft RPC service, used in Windows for remote procedure calls.
- Port 2179 (VMRDP): Virtual Machine Remote Desktop Protocol, typically used by Hyper-V.

3. Potential Security Risks

- FTP (21): Transmits credentials in plaintext. Susceptible to sniffing and brute-force attacks.
- DNS (53): Misconfigured servers may allow DNS amplification or information leaks.
- HTTP (80): No encryption; sensitive data can be intercepted.
- HTTPS (443): Secure, but may be weakened by outdated protocols or weak cipher suites.
- MSRPC (135): Common target for exploits like EternalBlue. Should be restricted or disabled externally.
- VMRDP (2179): If exposed, can allow remote access to virtual machines. Should be secured or disabled.

4. Save Scan Results

Use the following commands to save Nmap scan results:

- Save as text:
  nmap -sS 192.168.1.1/24 -oN scan_results.txt

- Save as HTML:
  nmap -sS 192.168.1.1/24 -oX scan_results.xml
  xsltproc scan_results.xml -o scan_results.html