ELEVATE LABS CYBER SECURITY INTERNSHIP

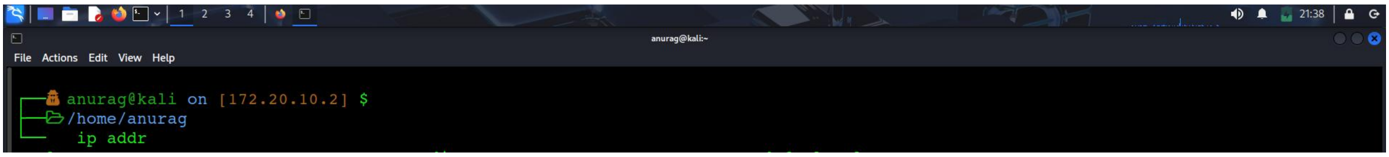
Mothe Anurag Reddy

Task-1:

1) 1.Install Nmap from official website.

Used the linux command sudo apt install nmap in my kali linux and downloaded the nmap.

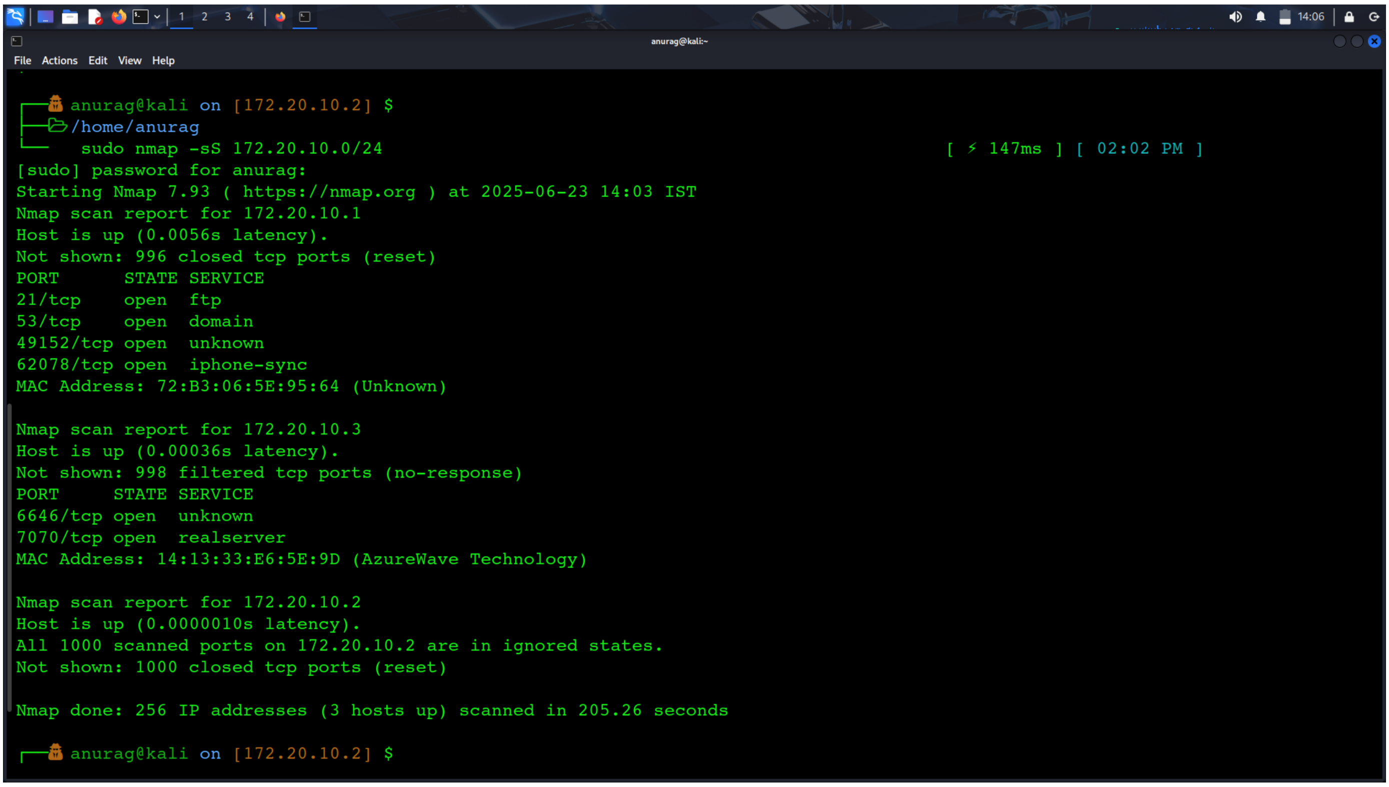
2.Find your local IP range



```
┌──anurag@kali on [172.20.10.2] $
├──/home/anurag
└──  ip addr
```

Here I can find my ip address as 172.20.10.0 with the subnet /24. Now I am scanning this in the nmap using the command sudo nmap -sn 172.20.10.0 /24 to perform ping scan without a port scan

3.Run: nmap -sS 172.20.10.0 /24 to perform TCP SYN scan.



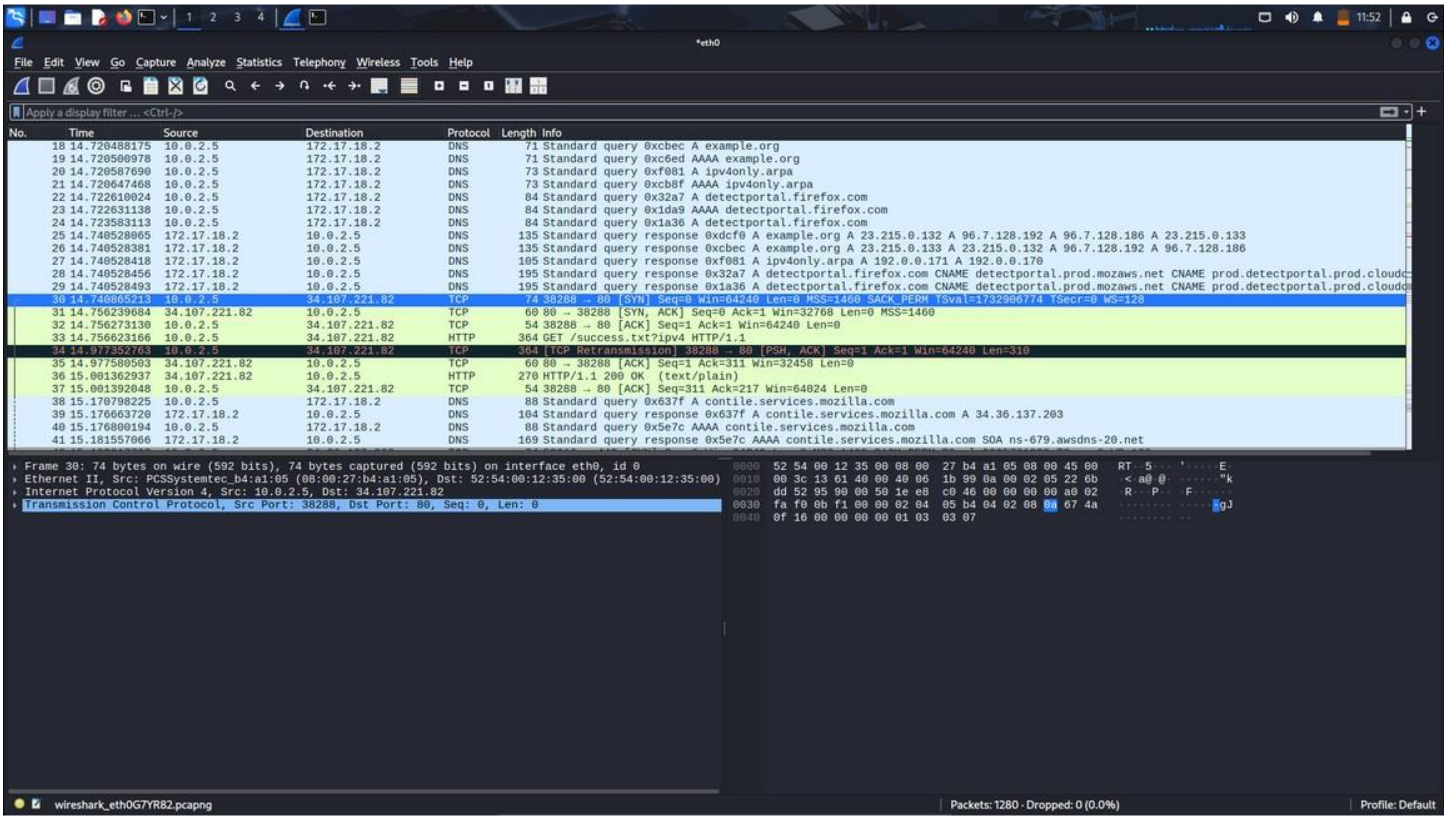
```
┌──anurag@kali on [172.20.10.2] $
├──/home/anurag
└──  sudo nmap -sS 172.20.10.0/24                                    [ ⚡ 147ms ] [ 02:02 PM ]
[sudo] password for anurag:
Starting Nmap 7.93 ( https://nmap.org ) at 2025-06-23 14:03 IST
Nmap scan report for 172.20.10.1
Host is up (0.0056s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
53/tcp    open  domain
49152/tcp open  unknown
62078/tcp open  iphone-sync
MAC Address: 72:B3:06:5E:95:64 (Unknown)

Nmap scan report for 172.20.10.3
Host is up (0.00036s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE
6646/tcp open  unknown
7070/tcp open  realserver
MAC Address: 14:13:33:E6:5E:9D (AzureWave Technology)

Nmap scan report for 172.20.10.2
Host is up (0.0000010s latency).
All 1000 scanned ports on 172.20.10.2 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (3 hosts up) scanned in 205.26 seconds

┌──anurag@kali on [172.20.10.2] $
```

4.Note down IP addresses and open ports found.

The IP addresses of the open ports found are (1 open port) and (3 open ports)

5.Optionally analyze packet capture with Wireshark.

Captured the live traffic through wireshark


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
11:52

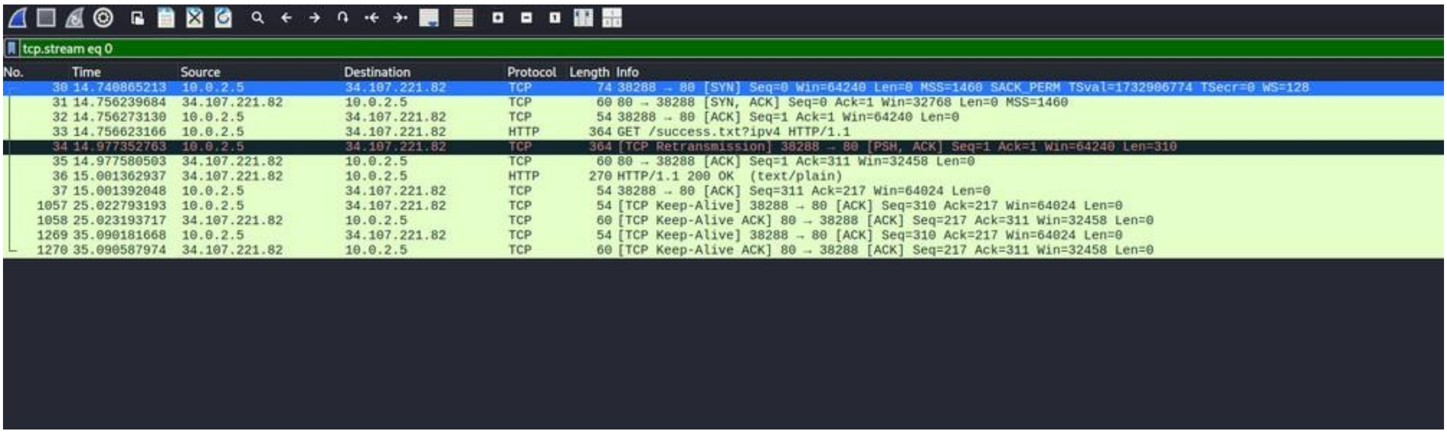
```
No.   Time          Source          Destination     Protocol Length Info
   18 14.720488175  10.0.2.5        172.17.18.2     DNS        71 Standard query 0xcbec A example.org
   19 14.720500978  10.0.2.5        172.17.18.2     DNS        71 Standard query 0xc6ed AAAA example.org
   20 14.720587690  10.0.2.5        172.17.18.2     DNS        73 Standard query 0xf081 A ipv4only.arpa
   21 14.720647468  10.0.2.5        172.17.18.2     DNS        73 Standard query 0xcb8f AAAA ipv4only.arpa
   22 14.722610024  10.0.2.5        172.17.18.2     DNS        84 Standard query 0x32a7 A detectportal.firefox.com
   23 14.722631138  10.0.2.5        172.17.18.2     DNS        84 Standard query 0x1da9 AAAA detectportal.firefox.com
   24 14.723583113  10.0.2.5        172.17.18.2     DNS        84 Standard query 0x1a36 A detectportal.firefox.com
   25 14.740528065  172.17.18.2     10.0.2.5        DNS       135 Standard query response 0xdcf0 A example.org A 23.215.0.132 A 96.7.128.192 A 96.7.128.186 A 23.215.0.133
   26 14.740528381  172.17.18.2     10.0.2.5        DNS       135 Standard query response 0xcbec A example.org A 23.215.0.133 A 23.215.0.132 A 96.7.128.192 A 96.7.128.186
   27 14.740528418  172.17.18.2     10.0.2.5        DNS       105 Standard query response 0xf081 A ipv4only.arpa A 192.0.0.171 A 192.0.0.170
   28 14.740528456  172.17.18.2     10.0.2.5        DNS       195 Standard query response 0x32a7 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME prod.detectportal.prod.cloudo
   29 14.740528493  172.17.18.2     10.0.2.5        DNS       195 Standard query response 0x1a36 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME prod.detectportal.prod.cloudo
   30 14.740865213  10.0.2.5        34.107.221.82   TCP        74 38288 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1732906774 TSecr=0 WS=128
   31 14.756239684  34.107.221.82   10.0.2.5        TCP        60 80 → 38288 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
   32 14.756273130  10.0.2.5        34.107.221.82   TCP        54 38288 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   33 14.756623166  10.0.2.5        34.107.221.82   HTTP      364 GET /success.txt?ipv4 HTTP/1.1
   34 14.977352763  10.0.2.5        34.107.221.82   TCP       364 [TCP Retransmission] 38288 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=310
   35 14.977580503  34.107.221.82   10.0.2.5        TCP        60 80 → 38288 [ACK] Seq=1 Ack=311 Win=32458 Len=0
   36 15.001362937  34.107.221.82   10.0.2.5        HTTP      270 HTTP/1.1 200 OK  (text/plain)
   37 15.001392048  10.0.2.5        34.107.221.82   TCP        54 38288 → 80 [ACK] Seq=311 Ack=217 Win=64024 Len=0
   38 15.170798225  10.0.2.5        172.17.18.2     DNS        88 Standard query 0x637f A contile.services.mozilla.com
   39 15.176663720  172.17.18.2     10.0.2.5        DNS       104 Standard query response 0x637f A contile.services.mozilla.com A 34.36.137.203
   40 15.176800194  10.0.2.5        172.17.18.2     DNS        88 Standard query 0x5e7c AAAA contile.services.mozilla.com
   41 15.181557066  172.17.18.2     10.0.2.5        DNS       169 Standard query response 0x5e7c AAAA contile.services.mozilla.com SOA ns-679.awsdns-20.net
```

```
› Frame 30: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
› Ethernet II, Src: PCSSystemtec_b4:a1:05 (08:00:27:b4:a1:05), Dst: 52:54:00:12:35:00 (52:54:00:12:35:00)
› Internet Protocol Version 4, Src: 10.0.2.5, Dst: 34.107.221.82
› Transmission Control Protocol, Src Port: 38288, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  52 54 00 12 35 00 08 00  27 b4 a1 05 08 00 45 00   RT··5···'·····E·
0010  00 3c 13 61 40 00 40 06  1b 99 0a 00 02 05 22 6b   ·<·a@·@·······"k
0020  dd 52 95 90 00 50 1e e8  c0 46 00 00 00 00 a0 02   ·R···P···F······
0030  fa f0 0b f1 00 00 02 04  05 b4 04 02 08 0a 67 4a   ··············gJ
0040  0f 16 00 00 00 00 01 03  03 07                     ··········
```

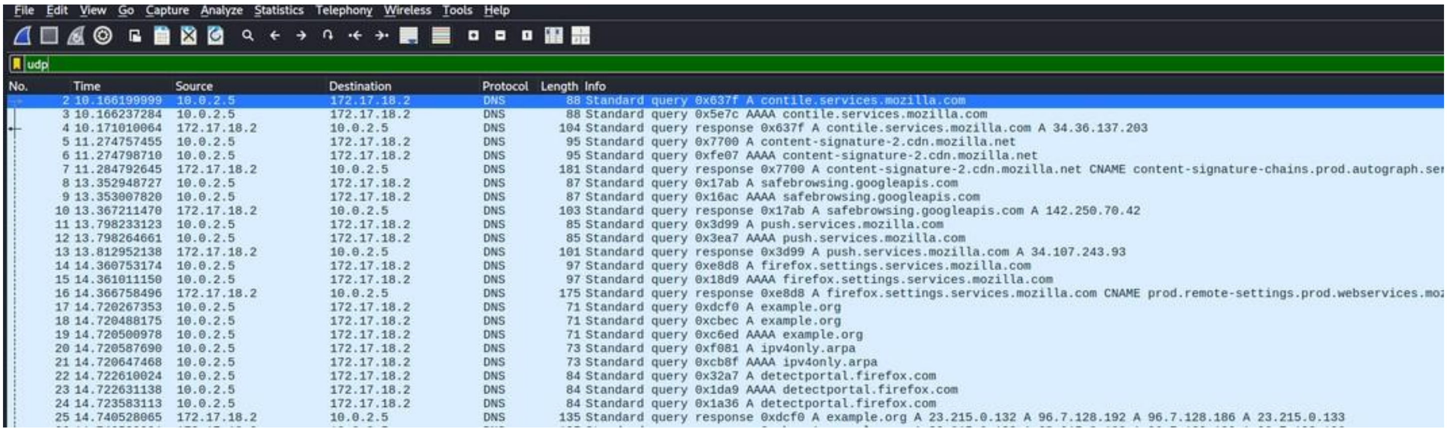
wireshark_eth0G7YR82.pcapng   Packets: 1280 · Dropped: 0 (0.0%)   Profile: Default

Analysing the tarffic using some of the available filters.



tcp.stream eq 0

```
No.   Time          Source          Destination     Protocol Length Info
   30 14.740865213  10.0.2.5        34.107.221.82   TCP        74 38288 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1732906774 TSecr=0 WS=128
   31 14.756239684  34.107.221.82   10.0.2.5        TCP        60 80 → 38288 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
   32 14.756273130  10.0.2.5        34.107.221.82   TCP        54 38288 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   33 14.756623166  10.0.2.5        34.107.221.82   HTTP      364 GET /success.txt?ipv4 HTTP/1.1
   34 14.977352763  10.0.2.5        34.107.221.82   TCP       364 [TCP Retransmission] 38288 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=310
   35 14.977580503  34.107.221.82   10.0.2.5        TCP        60 80 → 38288 [ACK] Seq=1 Ack=311 Win=32458 Len=0
   36 15.001362937  34.107.221.82   10.0.2.5        HTTP      270 HTTP/1.1 200 OK  (text/plain)
   37 15.001392048  10.0.2.5        34.107.221.82   TCP        54 38288 → 80 [ACK] Seq=311 Ack=217 Win=64024 Len=0
 1057 25.022793193  10.0.2.5        34.107.221.82   TCP        54 [TCP Keep-Alive] 38288 → 80 [ACK] Seq=310 Ack=217 Win=64024 Len=0
 1058 25.023193717  34.107.221.82   10.0.2.5        TCP        60 [TCP Keep-Alive ACK] 80 → 38288 [ACK] Seq=217 Ack=311 Win=32458 Len=0
 1269 35.090181668  10.0.2.5        34.107.221.82   TCP        54 [TCP Keep-Alive] 38288 → 80 [ACK] Seq=310 Ack=217 Win=64024 Len=0
 1270 35.090587974  34.107.221.82   10.0.2.5        TCP        60 [TCP Keep-Alive ACK] 80 → 38288 [ACK] Seq=217 Ack=311 Win=32458 Len=0
```


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp

```
No.   Time          Source          Destination     Protocol Length Info
    2 10.166199999  10.0.2.5        172.17.18.2     DNS        88 Standard query 0x637f A contile.services.mozilla.com
    3 10.166237284  10.0.2.5        172.17.18.2     DNS        88 Standard query 0x5e7c AAAA contile.services.mozilla.com
    4 10.171010064  172.17.18.2     10.0.2.5        DNS       104 Standard query response 0x637f A contile.services.mozilla.com A 34.36.137.203
    5 11.274757455  10.0.2.5        172.17.18.2     DNS        95 Standard query 0x7700 A content-signature-2.cdn.mozilla.net
    6 11.274798710  10.0.2.5        172.17.18.2     DNS        95 Standard query 0xfe07 AAAA content-signature-2.cdn.mozilla.net
    7 11.284792645  172.17.18.2     10.0.2.5        DNS       181 Standard query response 0x7700 A content-signature-2.cdn.mozilla.net CNAME content-signature-chains.prod.autograph.ser
    8 13.352948727  10.0.2.5        172.17.18.2     DNS        87 Standard query 0x17ab A safebrowsing.googleapis.com
    9 13.353007820  10.0.2.5        172.17.18.2     DNS        87 Standard query 0x16ac AAAA safebrowsing.googleapis.com
   10 13.367211470  172.17.18.2     10.0.2.5        DNS       103 Standard query response 0x17ab A safebrowsing.googleapis.com A 142.250.70.42
   11 13.798233123  10.0.2.5        172.17.18.2     DNS        85 Standard query 0x3d99 A push.services.mozilla.com
   12 13.798264661  10.0.2.5        172.17.18.2     DNS        85 Standard query 0x3ea7 AAAA push.services.mozilla.com
   13 13.812952138  172.17.18.2     10.0.2.5        DNS       101 Standard query response 0x3d99 A push.services.mozilla.com A 34.107.243.93
   14 14.360753174  10.0.2.5        172.17.18.2     DNS        97 Standard query 0xe8d8 A firefox.settings.services.mozilla.com
   15 14.361011150  10.0.2.5        172.17.18.2     DNS        97 Standard query 0x18d9 AAAA firefox.settings.services.mozilla.com
   16 14.366758496  172.17.18.2     10.0.2.5        DNS       175 Standard query response 0xe8d8 A firefox.settings.services.mozilla.com CNAME prod.remote-settings.prod.webservices.moz
   17 14.720267353  10.0.2.5        172.17.18.2     DNS        71 Standard query 0xdcf0 A example.org
   18 14.720488175  10.0.2.5        172.17.18.2     DNS        71 Standard query 0xcbec A example.org
   19 14.720500978  10.0.2.5        172.17.18.2     DNS        71 Standard query 0xc6ed AAAA example.org
   20 14.720587690  10.0.2.5        172.17.18.2     DNS        73 Standard query 0xf081 A ipv4only.arpa
   21 14.720647468  10.0.2.5        172.17.18.2     DNS        73 Standard query 0xcb8f AAAA ipv4only.arpa
   22 14.722610024  10.0.2.5        172.17.18.2     DNS        84 Standard query 0x32a7 A detectportal.firefox.com
   23 14.722631138  10.0.2.5        172.17.18.2     DNS        84 Standard query 0x1da9 AAAA detectportal.firefox.com
   24 14.723583113  10.0.2.5        172.17.18.2     DNS        84 Standard query 0x1a36 A detectportal.firefox.com
   25 14.740528065  172.17.18.2     10.0.2.5        DNS       135 Standard query response 0xdcf0 A example.org A 23.215.0.132 A 96.7.128.192 A 96.7.128.186 A 23.215.0.133
```

6.Research common services running on those ports.

Port	Service
[redacted]	MSRPC
445/tcp	[redacted]

3306/tcp	MySQL
53/tcp	DNS (TCP)

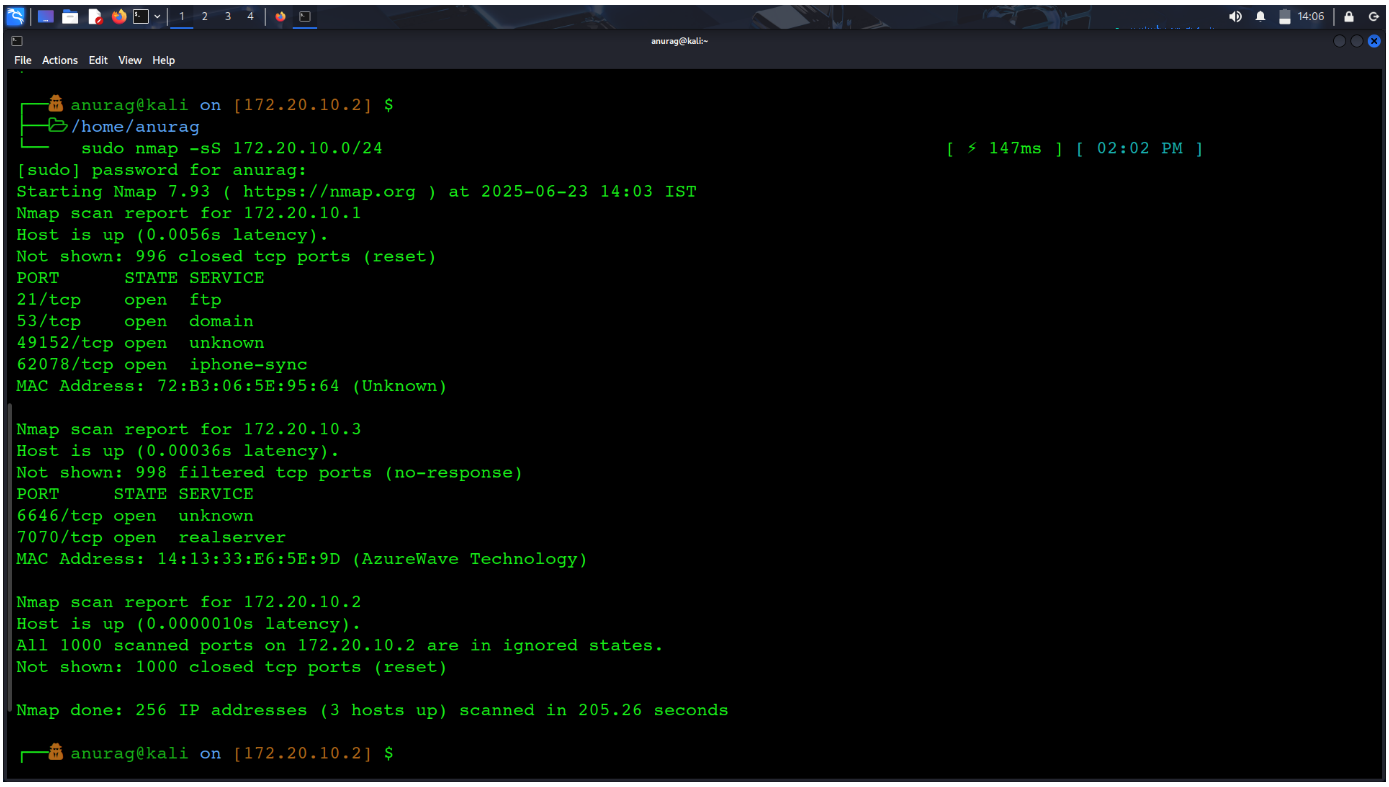
7.Identify potential security risks from open ports.

Port	Service
	MSRPC

445/tcp	[redacted] S (SMB)
3306/tcp	MySQL

53/tcp	DNS (TCP)

8.Save scan results as a text or HTML file.



```
┌──(anurag@kali on [172.20.10.2] $
├──/home/anurag
└──    sudo nmap -sS 172.20.10.0/24                                               [ ⚡ 147ms ] [ 02:02 PM ]
[sudo] password for anurag:
Starting Nmap 7.93 ( https://nmap.org ) at 2025-06-23 14:03 IST
Nmap scan report for 172.20.10.1
Host is up (0.0056s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
53/tcp    open  domain
49152/tcp open  unknown
62078/tcp open  iphone-sync
MAC Address: 72:B3:06:5E:95:64 (Unknown)

Nmap scan report for 172.20.10.3
Host is up (0.00036s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE
6646/tcp open  unknown
7070/tcp open  realserver
MAC Address: 14:13:33:E6:5E:9D (AzureWave Technology)

Nmap scan report for 172.20.10.2
Host is up (0.0000010s latency).
All 1000 scanned ports on 172.20.10.2 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (3 hosts up) scanned in 205.26 seconds

┌──(anurag@kali on [172.20.10.2] $
```