Session 4 Task

1. What is Scanning?

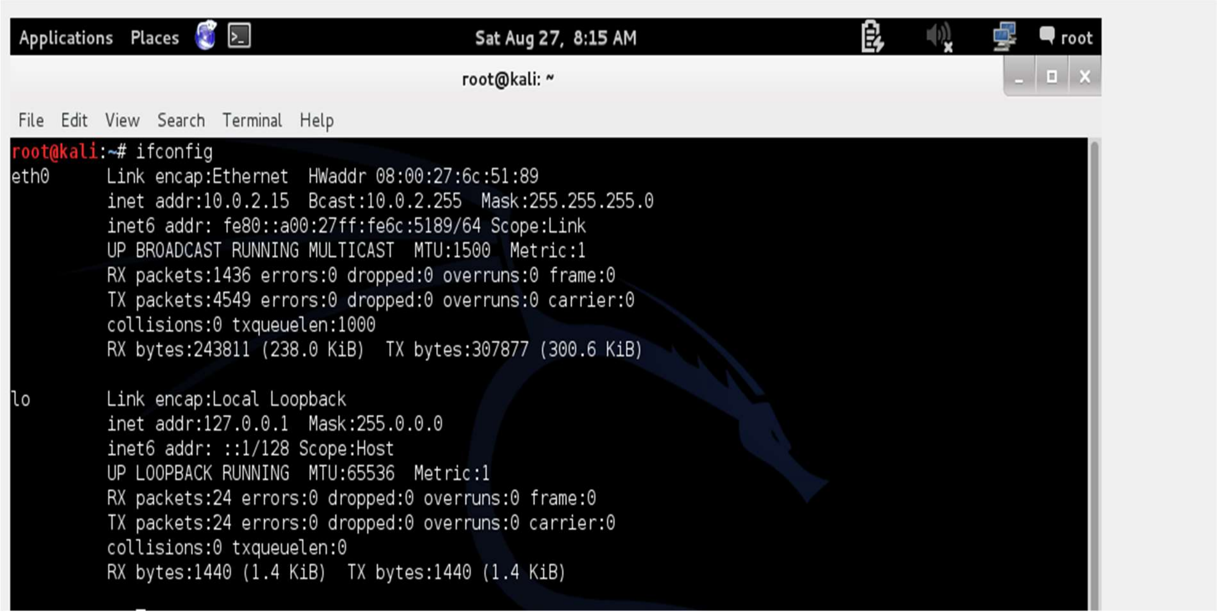
Scanning can be considered a logical extension (and overlap) of active reconnaissance that helps attackers identify specific vulnerabilities, an attacker follows a particular sequence of steps in order to scan a network. The scanning methods may differ based on the attack objectives, which are set up before the attackers actually begin this process.

2. What is Subnet?

An IP address is divided into two fields Network ID and a Host ID. What separates the Network Prefix and the Host ID depends on whether the address is a Class A, B or C address, every IP address has two parts. the length of the "first part" changes depending on the network's class.

3. IfConfig Command:

In "inet" section containing your IP address.



```
root@kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:6c:51:89
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe6c:5189/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1436 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4549 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:243811 (238.0 KiB)  TX bytes:307877 (300.6 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:24 errors:0 dropped:0 overruns:0 frame:0
          TX packets:24 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1440 (1.4 KiB)  TX bytes:1440 (1.4 KiB)
```

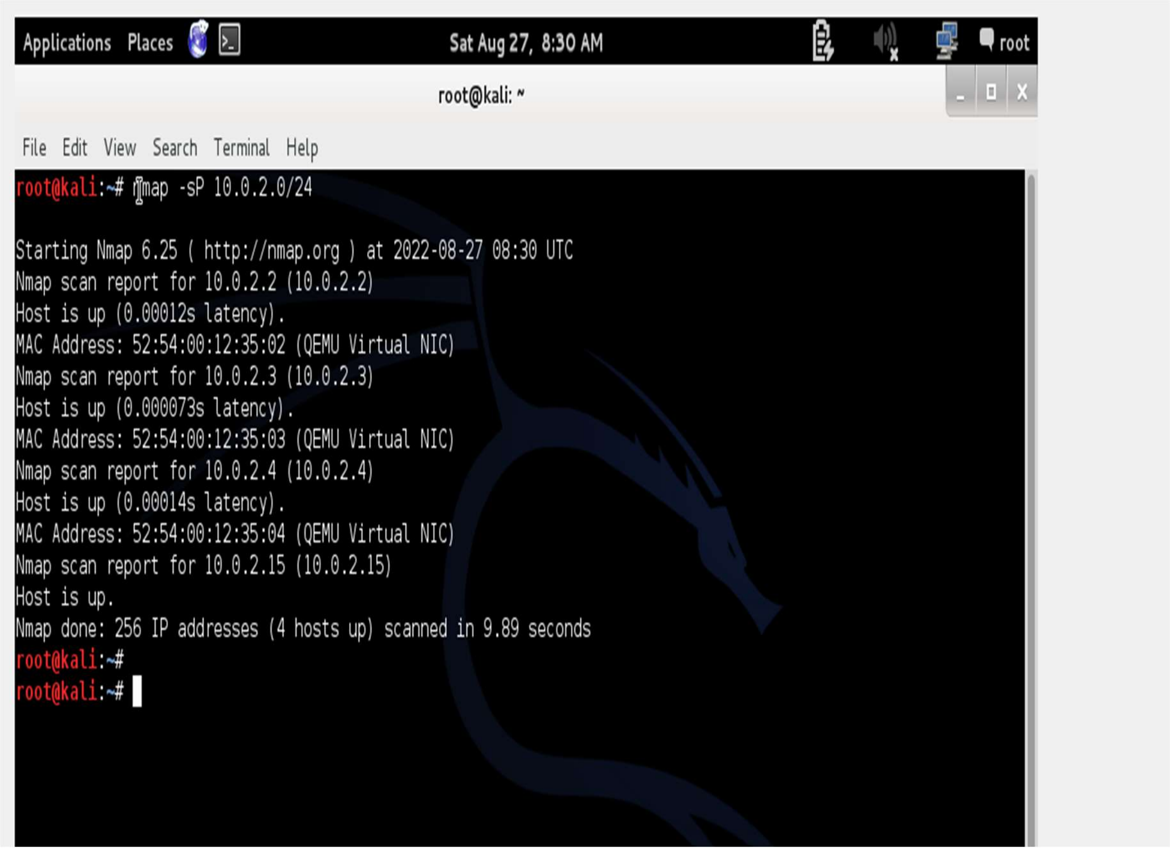
4. nmap (*nmap<scan type><option><target>*)

is short for Network Mapper. It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications, map allows to find which devices are running on their network, discover open ports and services.

- **Ping scan**

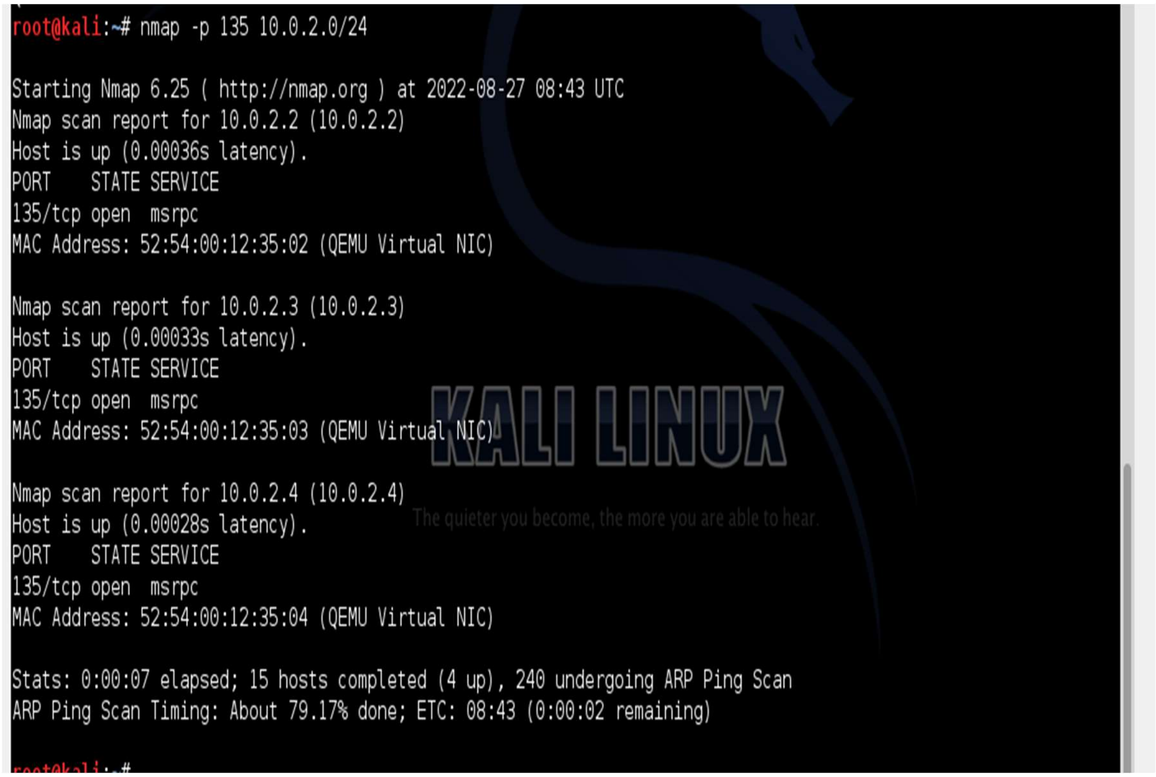
  nmap -sP 10.0.2.0/24→ possible hosts 256 host

  This command then returns a list of hosts on your network and the total number of assigned IP addresses.



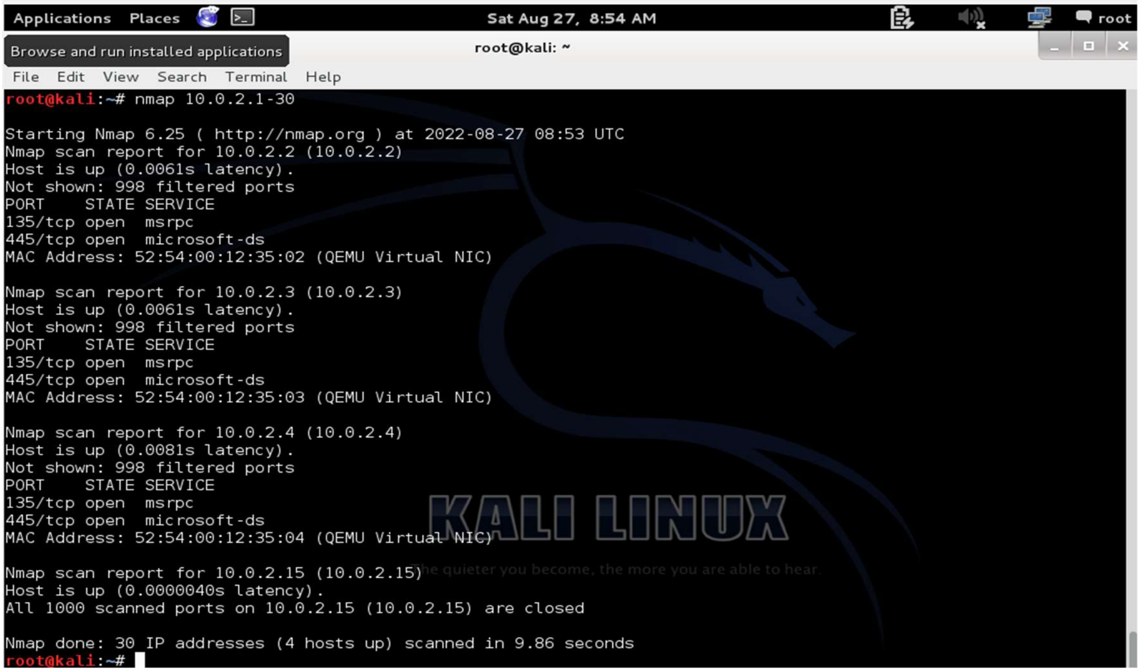
```
root@kali:~# nmap -sP 10.0.2.0/24

Starting Nmap 6.25 ( http://nmap.org ) at 2022-08-27 08:30 UTC
Nmap scan report for 10.0.2.2 (10.0.2.2)
Host is up (0.00012s latency).
MAC Address: 52:54:00:12:35:02 (QEMU Virtual NIC)
Nmap scan report for 10.0.2.3 (10.0.2.3)
Host is up (0.000073s latency).
MAC Address: 52:54:00:12:35:03 (QEMU Virtual NIC)
Nmap scan report for 10.0.2.4 (10.0.2.4)
Host is up (0.00014s latency).
MAC Address: 52:54:00:12:35:04 (QEMU Virtual NIC)
Nmap scan report for 10.0.2.15 (10.0.2.15)
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 9.89 seconds
root@kali:~#
root@kali:~#
```

- **Scan Port/s Is Up or not in Specific Subnet:**



```
root@kali:~# nmap -p 135 10.0.2.0/24

Starting Nmap 6.25 ( http://nmap.org ) at 2022-08-27 08:43 UTC
Nmap scan report for 10.0.2.2 (10.0.2.2)
Host is up (0.00036s latency).
PORT    STATE SERVICE
135/tcp open  msrpc
MAC Address: 52:54:00:12:35:02 (QEMU Virtual NIC)

Nmap scan report for 10.0.2.3 (10.0.2.3)
Host is up (0.00033s latency).
PORT    STATE SERVICE
135/tcp open  msrpc
MAC Address: 52:54:00:12:35:03 (QEMU Virtual NIC)

Nmap scan report for 10.0.2.4 (10.0.2.4)
Host is up (0.00028s latency).
PORT    STATE SERVICE
135/tcp open  msrpc
MAC Address: 52:54:00:12:35:04 (QEMU Virtual NIC)

Stats: 0:00:07 elapsed; 15 hosts completed (4 up), 240 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 79.17% done; ETC: 08:43 (0:00:02 remaining)

root@kali:~#
```

- **Scan a Range with Ip Address:**
  Command: nmap <IP range>Example: nmap 10.0.2.1-30
  (here IP range is separated by a dash)



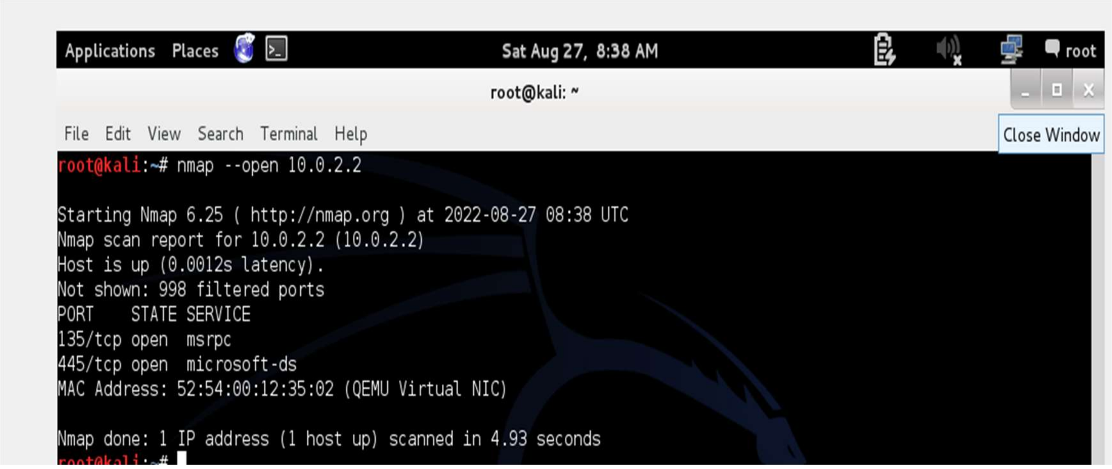
```
root@kali:~# nmap 10.0.2.1-30

Starting Nmap 6.25 ( http://nmap.org ) at 2022-08-27 08:53 UTC
Nmap scan report for 10.0.2.2 (10.0.2.2)
Host is up (0.0061s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
135/tcp open  msrpc
445/tcp open  microsoft-ds
MAC Address: 52:54:00:12:35:02 (QEMU Virtual NIC)

Nmap scan report for 10.0.2.3 (10.0.2.3)
Host is up (0.0061s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
135/tcp open  msrpc
445/tcp open  microsoft-ds
MAC Address: 52:54:00:12:35:03 (QEMU Virtual NIC)

Nmap scan report for 10.0.2.4 (10.0.2.4)
Host is up (0.0081s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
135/tcp open  msrpc
445/tcp open  microsoft-ds
MAC Address: 52:54:00:12:35:04 (QEMU Virtual NIC)

Nmap scan report for 10.0.2.15 (10.0.2.15)
Host is up (0.0000040s latency).
All 1000 scanned ports on 10.0.2.15 (10.0.2.15) are closed

Nmap done: 30 IP addresses (4 hosts up) scanned in 9.86 seconds
root@kali:~#
```

- **Display Open Ports:**

  Command: nmap — open <IP address/domain name>

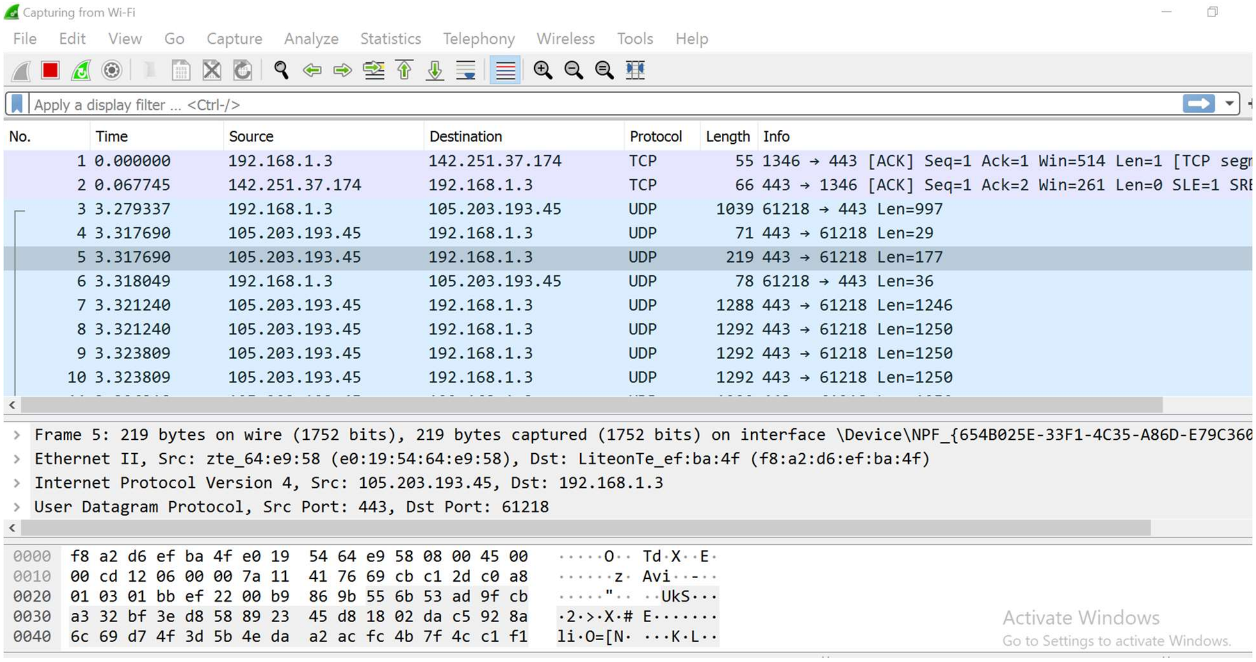
  Example: nmap — open 10.0.2.2

  In the above example, we are using "–open" parameter with IP address 10.0.2.2 so that the Nmap command only shows us the ports with the open state.



```
root@kali:~# nmap --open 10.0.2.2

Starting Nmap 6.25 ( http://nmap.org ) at 2022-08-27 08:38 UTC
Nmap scan report for 10.0.2.2 (10.0.2.2)
Host is up (0.0012s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
135/tcp open  msrpc
445/tcp open  microsoft-ds
MAC Address: 52:54:00:12:35:02 (QEMU Virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 4.93 seconds
root@kali:~#
```

- **Wireshark:**



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.3	142.251.37.174	TCP	55	1346 → 443 [ACK] Seq=1 Ack=1 Win=514 Len=1 [TCP segr
2	0.067745	142.251.37.174	192.168.1.3	TCP	66	443 → 1346 [ACK] Seq=1 Ack=2 Win=261 Len=0 SLE=1 SRE
3	3.279337	192.168.1.3	105.203.193.45	UDP	1039	61218 → 443 Len=997
4	3.317690	105.203.193.45	192.168.1.3	UDP	71	443 → 61218 Len=29
5	3.317690	105.203.193.45	192.168.1.3	UDP	219	443 → 61218 Len=177
6	3.318049	192.168.1.3	105.203.193.45	UDP	78	61218 → 443 Len=36
7	3.321240	105.203.193.45	192.168.1.3	UDP	1288	443 → 61218 Len=1246
8	3.321240	105.203.193.45	192.168.1.3	UDP	1292	443 → 61218 Len=1250
9	3.323809	105.203.193.45	192.168.1.3	UDP	1292	443 → 61218 Len=1250
10	3.323809	105.203.193.45	192.168.1.3	UDP	1292	443 → 61218 Len=1250

```
> Frame 5: 219 bytes on wire (1752 bits), 219 bytes captured (1752 bits) on interface \Device\NPF_{654B025E-33F1-4C35-A86D-E79C360
> Ethernet II, Src: zte_64:e9:58 (e0:19:54:64:e9:58), Dst: LiteonTe_ef:ba:4f (f8:a2:d6:ef:ba:4f)
> Internet Protocol Version 4, Src: 105.203.193.45, Dst: 192.168.1.3
> User Datagram Protocol, Src Port: 443, Dst Port: 61218
```

```
0000  f8 a2 d6 ef ba 4f e0 19  54 64 e9 58 08 00 45 00   ·····O·· Td·X··E·
0010  00 cd 12 06 00 00 7a 11  41 76 69 cb c1 2d c0 a8   ······z· Avi··-··
0020  01 03 01 bb ef 22 00 b9  86 9b 55 6b 53 ad 9f cb   ·····"·· ··UkS···
0030  a3 32 bf 3e d8 58 89 23  45 d8 18 02 da c5 92 8a   ·2·>·X·# E·······
0040  6c 69 d7 4f 3d 5b 4e da  a2 ac fc 4b 7f 4c c1 f1   li·O=[N· ···K·L··
```