Group no: - 8

Group Member:- Shrut Shah – 19BCP125

Shubham Kathiriya – 19BCP127

Vedant Patel – 19BCP138

Subject: - Cyber Security Lab

Division:-2

Lab 3:- NMAP

Aim:-

Detailed Study of NMAP(NETWORK MAPPER) Tool.

Introduction:-

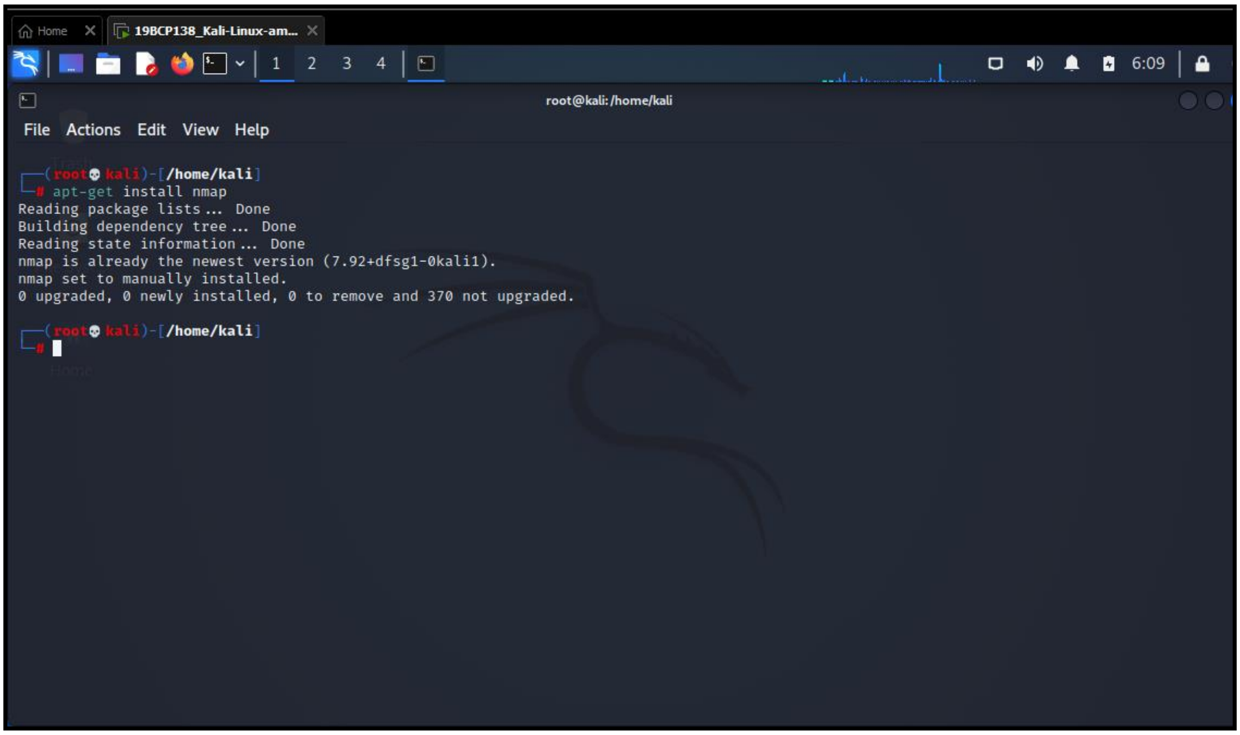
- Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X.

- Nmap, Network Mapper is an industry-standard tool used for scanning the network. As a cybersecurity professional, it's always necessary to understand the target’s network infrastructure to gain a better understanding. It’s a useful tool for those who want to choose Network pentesting as their career path.

Working:-

1. Using Nmap for first time(Download):-

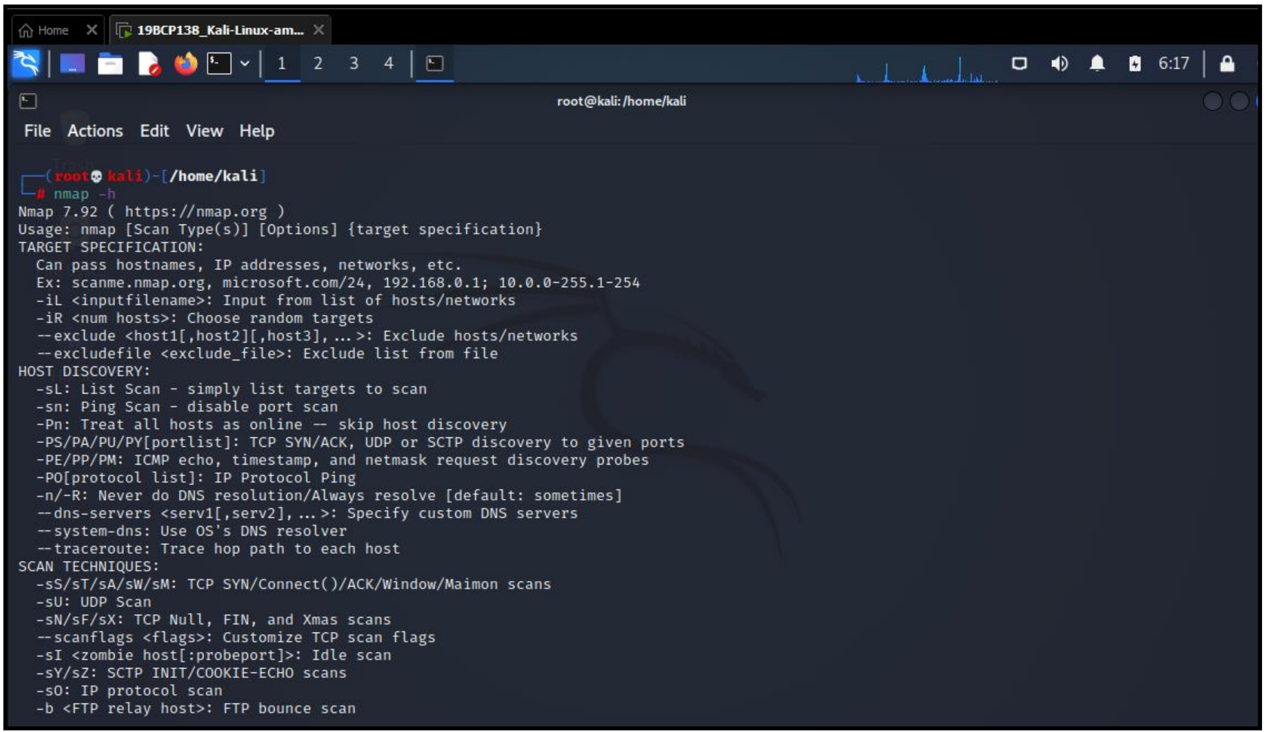
- Nmap comes preinstalled with Kali Linux (and it’s recommended to use Kali Linux), alternatively on other Linux OS using the command ‘**apt-get install nmap**’.



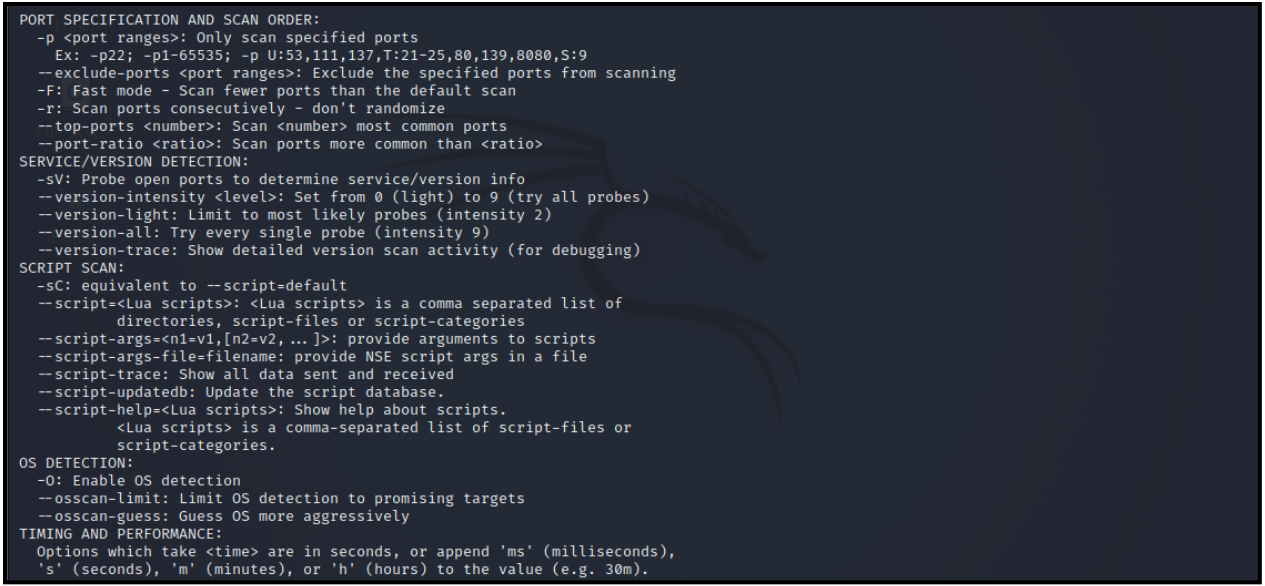
```
┌──(root💀kali)-[/home/kali]
└─# apt-get install nmap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nmap is already the newest version (7.92+dfsg1-0kali1).
nmap set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 370 not upgraded.

┌──(root💀kali)-[/home/kali]
└─# 
```

2. Using Nmap for Switches:-

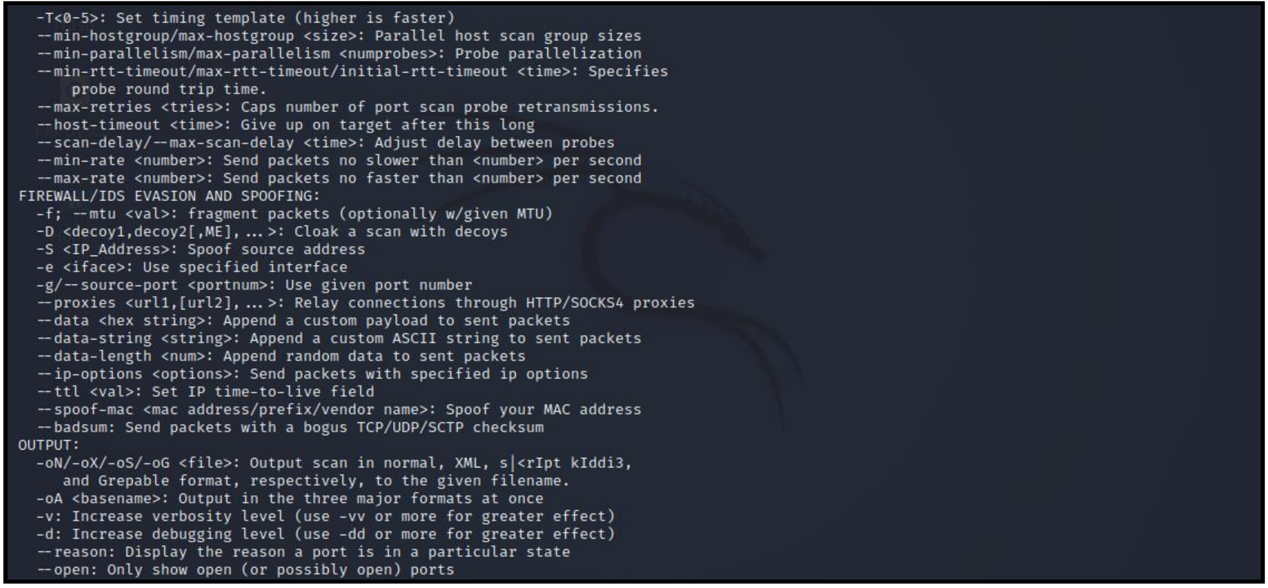
- Switches are divided in various categories like Host Discovery, Scan Techniques, Port Specifications and Scan Order, Service / Version Detection, Script Scan, OS Detection, Timing and Performance, Firewalls / IDSs evasion and spoofing, and few more.



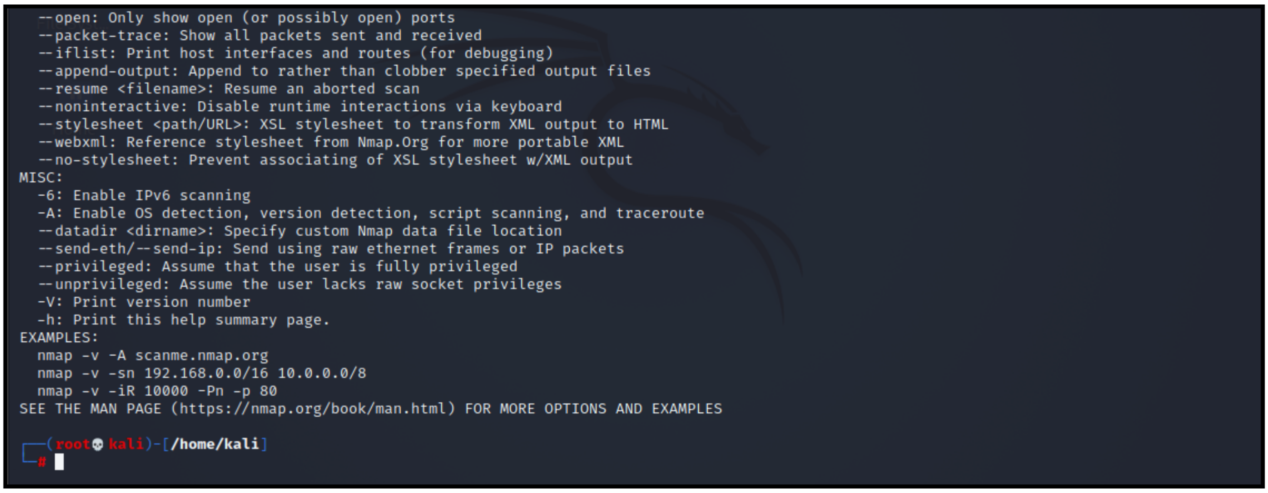
```
┌──(root💀kali)-[/home/kali]
└─# nmap -h
Nmap 7.92 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
```



```
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
           directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
  --script-args-file=filename: provide NSE script args in a file
  --script-trace: Show all data sent and received
  --script-updatedb: Update the script database.
  --script-help=<Lua scripts>: Show help about scripts.
           <Lua scripts> is a comma-separated list of script-files or
           script-categories.
OS DETECTION:
  -O: Enable OS detection
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
  Options which take <time> are in seconds, or append 'ms' (milliseconds),
  's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
```



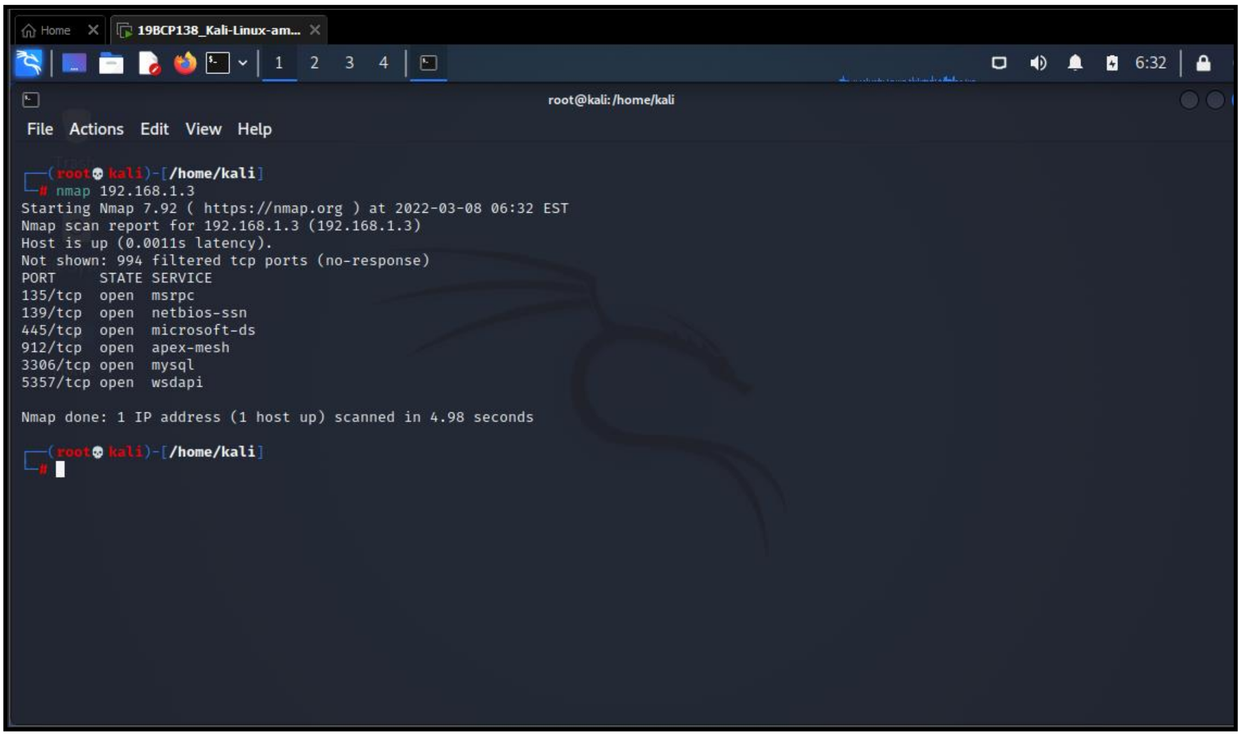
```
  -T<0-5>: Set timing template (higher is faster)
  --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
  --min-parallelism/max-parallelism <numprobes>: Probe parallelization
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
      probe round trip time.
  --max-retries <tries>: Caps number of port scan probe retransmissions.
  --host-timeout <time>: Give up on target after this long
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
  --min-rate <number>: Send packets no slower than <number> per second
  --max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
  -f; --mtu <val>: fragment packets (optionally w/given MTU)
  -D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
  -S <IP_Address>: Spoof source address
  -e <iface>: Use specified interface
  -g/--source-port <portnum>: Use given port number
  --proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
  --data <hex string>: Append a custom payload to sent packets
  --data-string <string>: Append a custom ASCII string to sent packets
  --data-length <num>: Append random data to sent packets
  --ip-options <options>: Send packets with specified ip options
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
  --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  --reason: Display the reason a port is in a particular state
  --open: Only show open (or possibly open) ports
```



```
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --noninteractive: Disable runtime interactions via keyboard
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES

┌──(root💀 kali)-[/home/kali]
└─# 
```

3. Using Nmap for Simple Scan:-

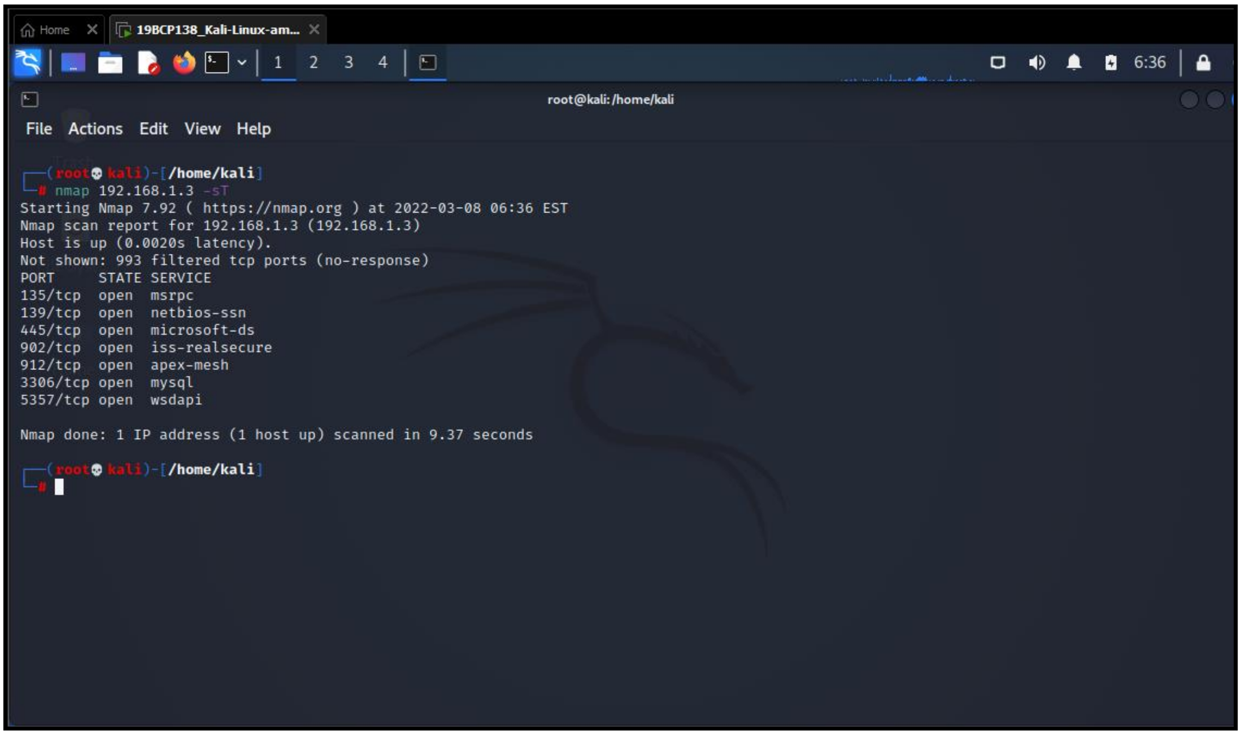
- By providing only the IP address, Nmap will simply try to scan all the possible alive host in the network and will check which ports are open using the default port list. In the above result it can be seen that Nmap has reported total of 4 hosts as alive in thenetwork.



```
┌──(root💀 kali)-[/home/kali]
└─# nmap 192.168.1.3
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-08 06:32 EST
Nmap scan report for 192.168.1.3 (192.168.1.3)
Host is up (0.0011s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
912/tcp  open  apex-mesh
3306/tcp open  mysql
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 4.98 seconds

┌──(root💀 kali)-[/home/kali]
└─# 
```

4. TCP Connect Port Scan:-

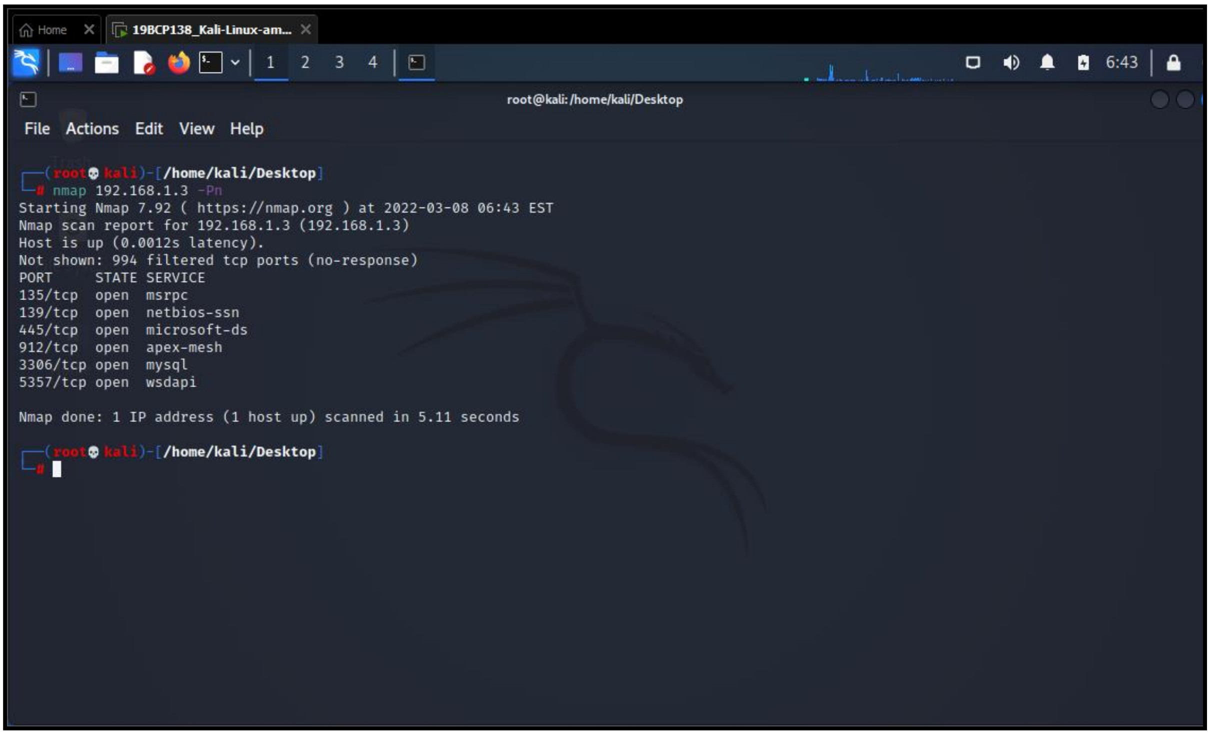
- -sT switch performs full TCP handshake while scanning the target host. This can gets logged into the target host's logs and can be tracked. Here in this scan Nmap will try to establish full connection with the target host by completing full 3-way process.



```
┌──(root💀 kali)-[/home/kali]
└─# nmap 192.168.1.3 -sT
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-08 06:36 EST
Nmap scan report for 192.168.1.3 (192.168.1.3)
Host is up (0.0020s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
3306/tcp open  mysql
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 9.37 seconds

┌──(root💀 kali)-[/home/kali]
└─#
```

5. Skipping Ping while Scan:-

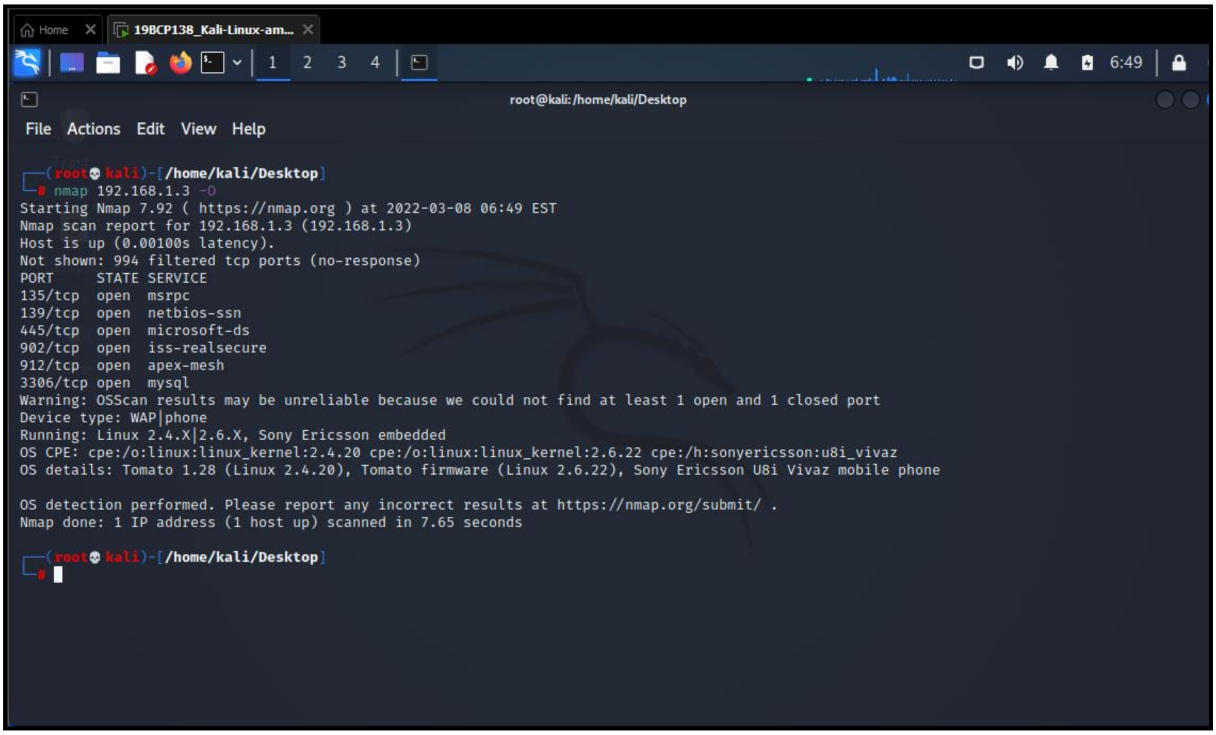
- -Pn switch is used to treat the given targets as alive by default and skip the ping test during the scan. When this switch is not used, Nmap will send ping requests to the mentioned target hosts to check which hosts in the network are alive, but when this switch is used Nmap will consider the mentioned hosts ass alive and perform other scanning like port scanning and service scanning and such stuffs. If we know in advance that the particular host/hosts that we are going to scan are alive in the network than this switch is recommend to be used as this will help reduce the scanning time.


Home
19BCP138_Kali-Linux-am...
1 2 3 4
6:43
root@kali: /home/kali/Desktop
File Actions Edit View Help

```
┌──(root💀kali)-[/home/kali/Desktop]
└─# nmap 192.168.1.3 -Pn
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-08 06:43 EST
Nmap scan report for 192.168.1.3 (192.168.1.3)
Host is up (0.0012s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
912/tcp  open  apex-mesh
3306/tcp open  mysql
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 5.11 seconds

┌──(root💀kali)-[/home/kali/Desktop]
└─#
```

6. Detecting Operating System of the Target:-

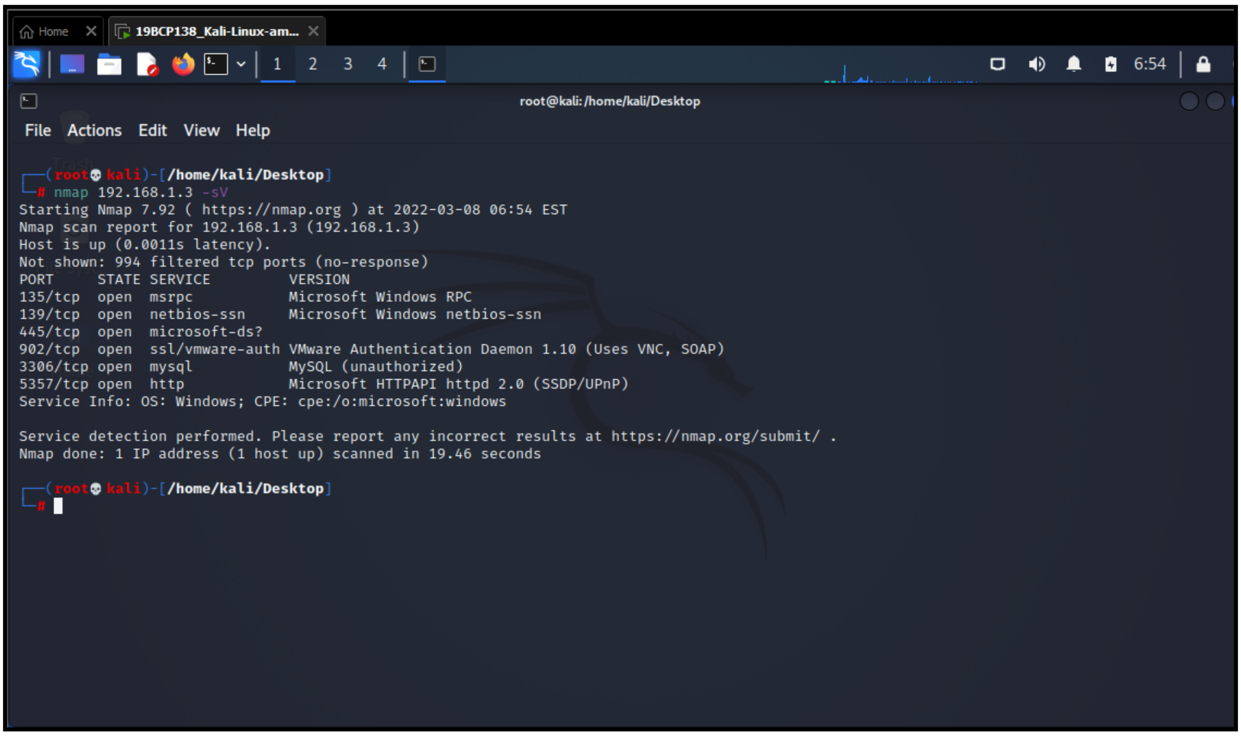
- -O switch is used to detect the operating system of the target. Not every time the results are precise and accurate, in the above snapshot it can be seen that Nmap has guessed various operating systems and also with it shown the confidence percentage.


Home
19BCP138_Kali-Linux-am...
1 2 3 4
6:49
root@kali: /home/kali/Desktop
File Actions Edit View Help

```
┌──(root💀kali)-[/home/kali/Desktop]
└─# nmap 192.168.1.3 -O
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-08 06:49 EST
Nmap scan report for 192.168.1.3 (192.168.1.3)
Host is up (0.00100s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
3306/tcp open  mysql
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|phone
Running: Linux 2.4.X|2.6.X, Sony Ericsson embedded
OS CPE: cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6.22 cpe:/h:sonyericsson:u8i_vivaz
OS details: Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.22), Sony Ericsson U8i Vivaz mobile phone

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.65 seconds

┌──(root💀kali)-[/home/kali/Desktop]
└─#
```

7. Service and its Version Detection:-

- -sV switch is used to detect service and its version that are running on the mentioned target. In the results it can be seen that Nmap has detected services and its version running on different ports. This version details can be used to exploit particular running service on the target and may be further used to gain access to whole systemin the worst case.



```
┌──(root💀 kali)-[/home/kali/Desktop]
└─# nmap 192.168.1.3 -sV
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-08 06:54 EST
Nmap scan report for 192.168.1.3 (192.168.1.3)
Host is up (0.0011s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE         VERSION
135/tcp  open  msrpc           Microsoft Windows RPC
139/tcp  open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
902/tcp  open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
3306/tcp open  mysql           MySQL (unauthorized)
5357/tcp open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.46 seconds

┌──(root💀 kali)-[/home/kali/Desktop]
└─# 
```