Practical No. 2

Aim: Practical on enumerating host, port, and service scanning.

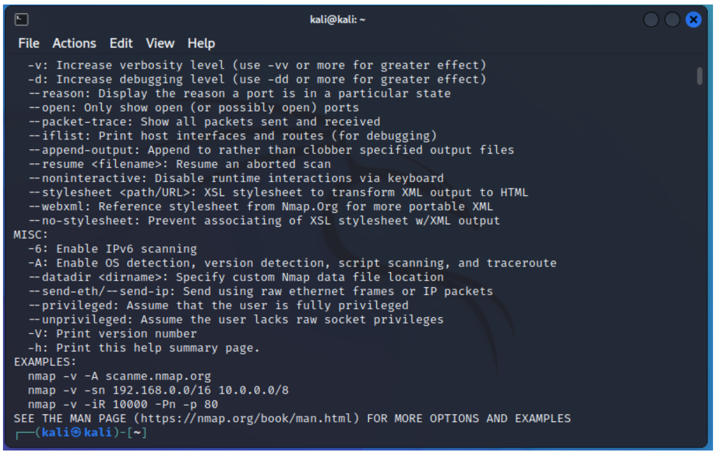
Implementations:

To enumerate services on target machine, perform the following steps:

1. Launch Kali Linux

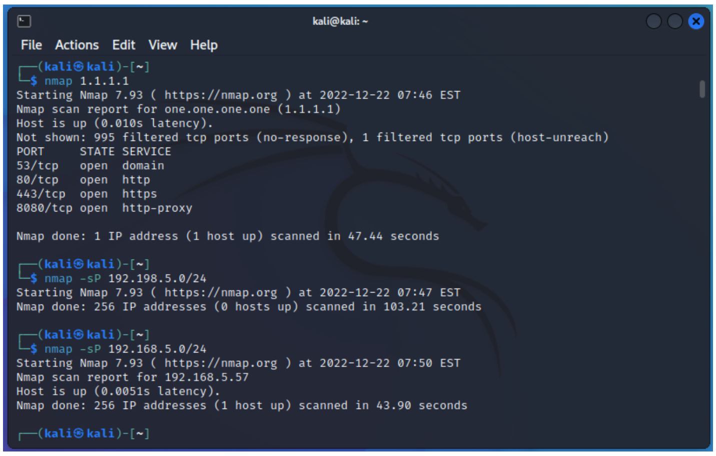
2. Select Application > Information Gathering > Nmap, as shown in the figure.

Then the following screen will appear, as shown in figure.



```
  -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
  --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
┌──(kali㉿kali)-[~]
```

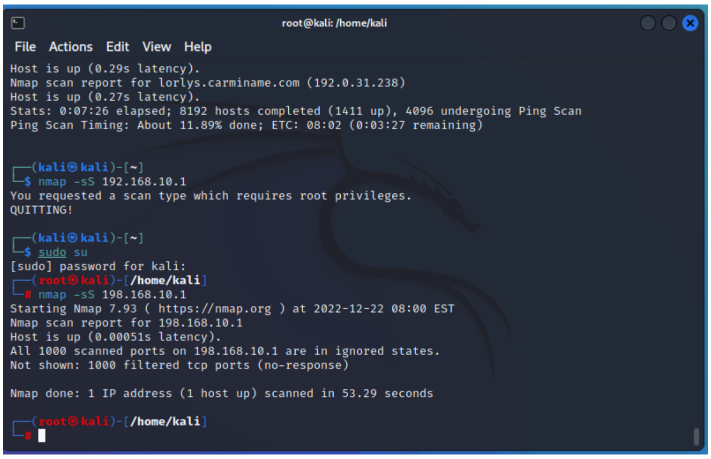
3. Type "nmap -sP 192.xx.xx.xx/2", and press Enter, as shown in figure



```
┌──(kali㉿kali)-[~]
└─$ nmap 1.1.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-22 07:46 EST
Nmap scan report for one.one.one.one (1.1.1.1)
Host is up (0.010s latency).
Not shown: 995 filtered tcp ports (no-response), 1 filtered tcp ports (host-unreach)
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 47.44 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sP 192.198.5.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-22 07:47 EST
Nmap done: 256 IP addresses (0 hosts up) scanned in 103.21 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sP 192.168.5.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-22 07:50 EST
Nmap scan report for 192.168.5.57
Host is up (0.0051s latency).
Nmap done: 256 IP addresses (1 host up) scanned in 43.90 seconds

┌──(kali㉿kali)-[~]
```

Then 'Nmap' will scan all the nodes on the given network range and display all the hosts that are running, as shown in figure.

4. Type "nmap-sS <IP address of the target machine>", and press Enter, as shown in figure (here we used 192.xx.xx.xx as the IP address)



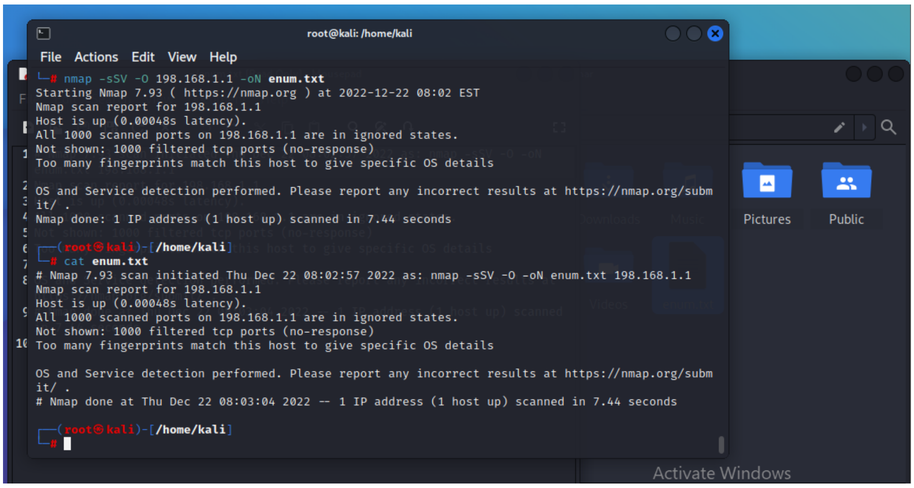
```
Host is up (0.29s latency).
Nmap scan report for lorlys.carminame.com (192.0.31.238)
Host is up (0.27s latency).
Stats: 0:07:26 elapsed; 8192 hosts completed (1411 up), 4096 undergoing Ping Scan
Ping Scan Timing: About 11.89% done; ETC: 08:02 (0:03:27 remaining)


┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.10.1
You requested a scan type which requires root privileges.
QUITTING!

┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 198.168.10.1
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-22 08:00 EST
Nmap scan report for 198.168.10.1
Host is up (0.00051s latency).
All 1000 scanned ports on 198.168.10.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 53.29 seconds

┌──(root㉿kali)-[/home/kali]
└─# 
```

Then a Stealthy syn scan will be initiated, and all the open ports that are running on the machine will be displayed, as shown in figure.

Now we can see all the open ports along with the services.

We will find version of each of these services running on the open port by performing a syn with version detection switch.

5. Type "nmap -sSV -O <IP address of the target machine>", and press Enter, as shown in figure.



```
└─# nmap -sSV -O 198.168.1.1 -oN enum.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-22 08:02 EST
Nmap scan report for 198.168.1.1
Host is up (0.00048s latency).
All 1000 scanned ports on 198.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details

OS and Service detection performed. Please report any incorrect results at https://nmap.org/subm
it/ .
Nmap done: 1 IP address (1 host up) scanned in 7.44 seconds

┌──(root㉿kali)-[/home/kali]
└─# cat enum.txt
# Nmap 7.93 scan initiated Thu Dec 22 08:02:57 2022 as: nmap -sSV -O -oN enum.txt 198.168.1.1
Nmap scan report for 198.168.1.1
Host is up (0.00048s latency).
All 1000 scanned ports on 198.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details

OS and Service detection performed. Please report any incorrect results at https://nmap.org/subm
it/ .
# Nmap done at Thu Dec 22 08:03:04 2022 -- 1 IP address (1 host up) scanned in 7.44 seconds

┌──(root㉿kali)-[/home/kali]
└─# 
```

Now, the Nmap performs the scan and displays the versions of the services, as shown on figure.

We have found the enumerated result. We will now save the scan result.

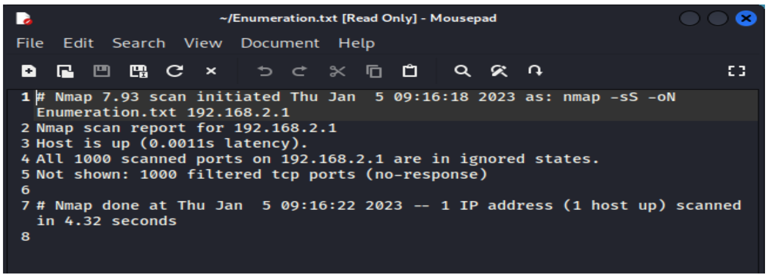
6. Type "nmap sSV -O <IP address of the target machine> oN Enumeration.txt", and press Enter, as shown in figure.

Then following screen will appear, as shown in figure.

Nmap will now perform Stealthy Scan with version and OS detection, and save the result in a text file (Enumeration.txt) , which will be located on home (root) directory.

7. Click on Places > Home Folder

8. Double click on the file Enumeration.txt, as shown in figure.



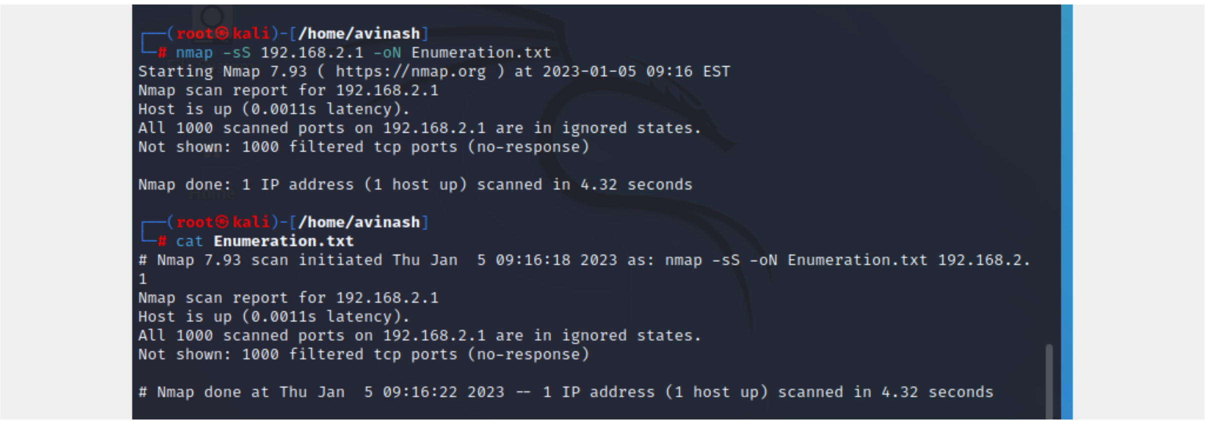
~/Enumeration.txt [Read Only] - Mousepad
File Edit Search View Document Help

```
# Nmap 7.93 scan initiated Thu Jan  5 09:16:18 2023 as: nmap -sS -oN Enumeration.txt 192.168.2.1
Nmap scan report for 192.168.2.1
Host is up (0.0011s latency).
All 1000 scanned ports on 192.168.2.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

# Nmap done at Thu Jan  5 09:16:22 2023 -- 1 IP address (1 host up) scanned in 4.32 seconds
```

Then the following window will appear, as shown in figure.

You can also check the scanning result in the command line terminal.

Type "cat Enumeration.txt", and press Enter, as shown in figure.



```
┌──(root㉿kali)-[/home/avinash]
└─# nmap -sS 192.168.2.1 -oN Enumeration.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-05 09:16 EST
Nmap scan report for 192.168.2.1
Host is up (0.0011s latency).
All 1000 scanned ports on 192.168.2.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 4.32 seconds

┌──(root㉿kali)-[/home/avinash]
└─# cat Enumeration.txt
# Nmap 7.93 scan initiated Thu Jan  5 09:16:18 2023 as: nmap -sS -oN Enumeration.txt 192.168.2.
1
Nmap scan report for 192.168.2.1
Host is up (0.0011s latency).
All 1000 scanned ports on 192.168.2.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

# Nmap done at Thu Jan  5 09:16:22 2023 -- 1 IP address (1 host up) scanned in 4.32 seconds
```

Then the output of the scanning process will be shown in the command line terminal, as shown in figure.