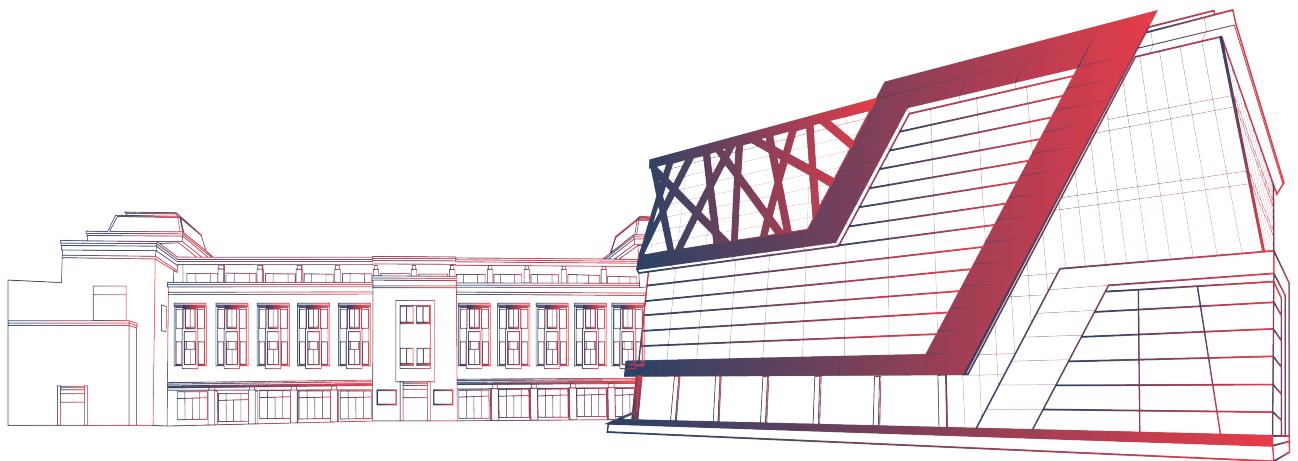


Types of Scan

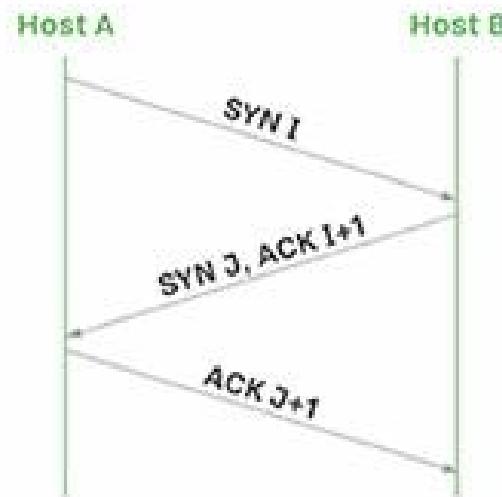
NMAP



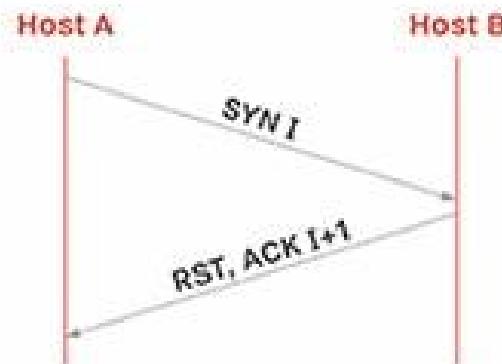
TCP/Connect/Regular Scan (Nmap -sT)

TCP PORT SCANNING TECHNIQUES

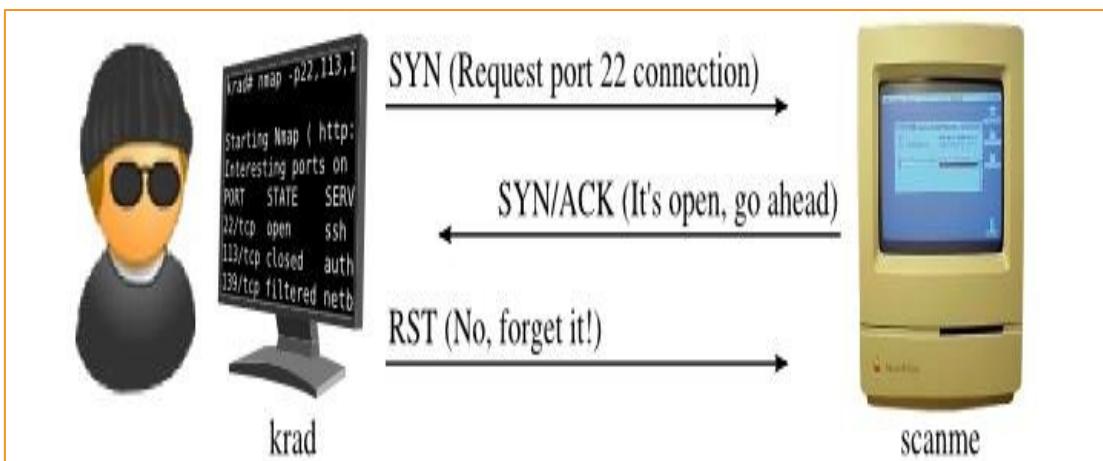
OPEN PORT



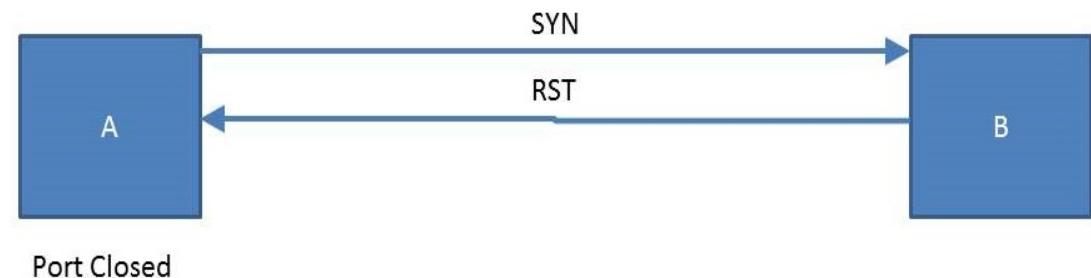
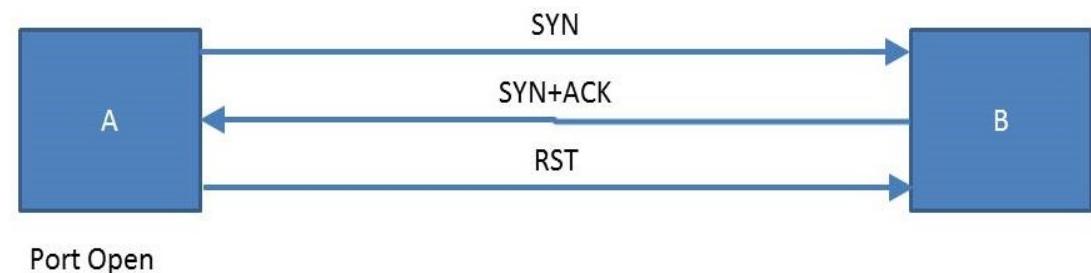
CLOSED PORT



TCP Syn/Stealth scan (Nmap -sS)



Port is open



Nmap features

Regular Scan

Attempt **full connection** with port

Scanned system **knows scan is occurring**

SYN, ACK+SYN, ACK

Can identify scanner

Stealth Scanning

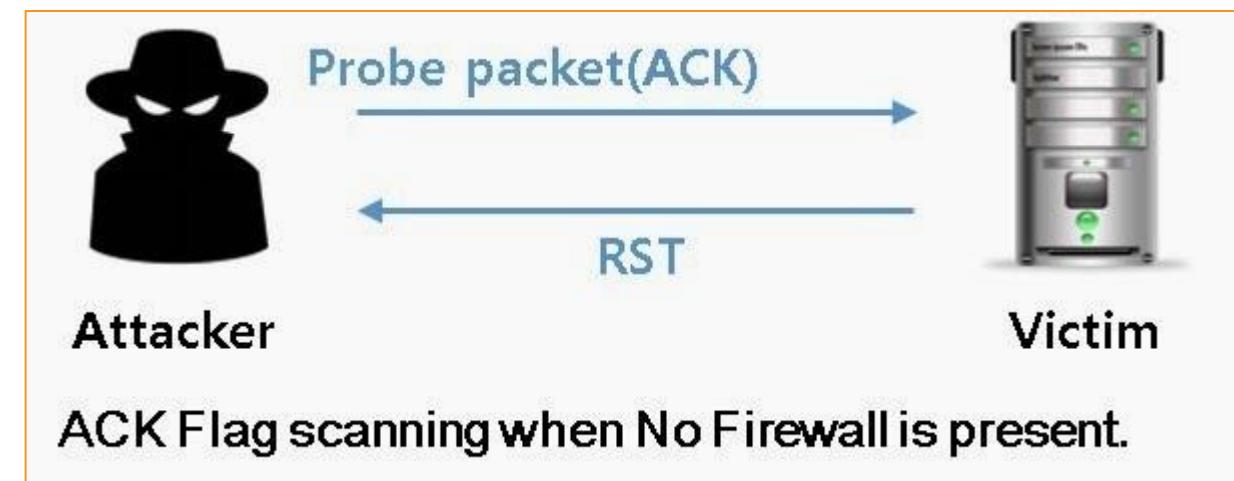
Attempt **partial connection** with port

System **may not know scan is occurring**

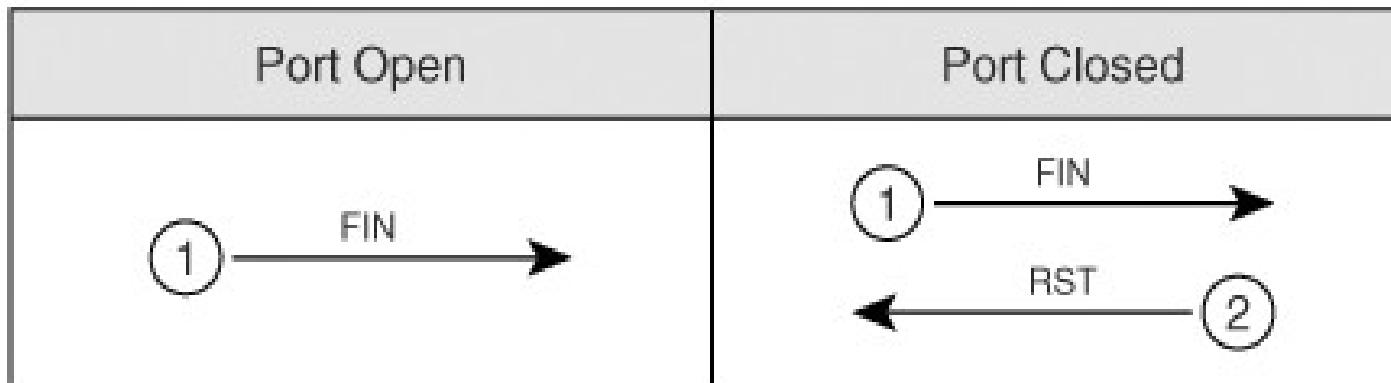
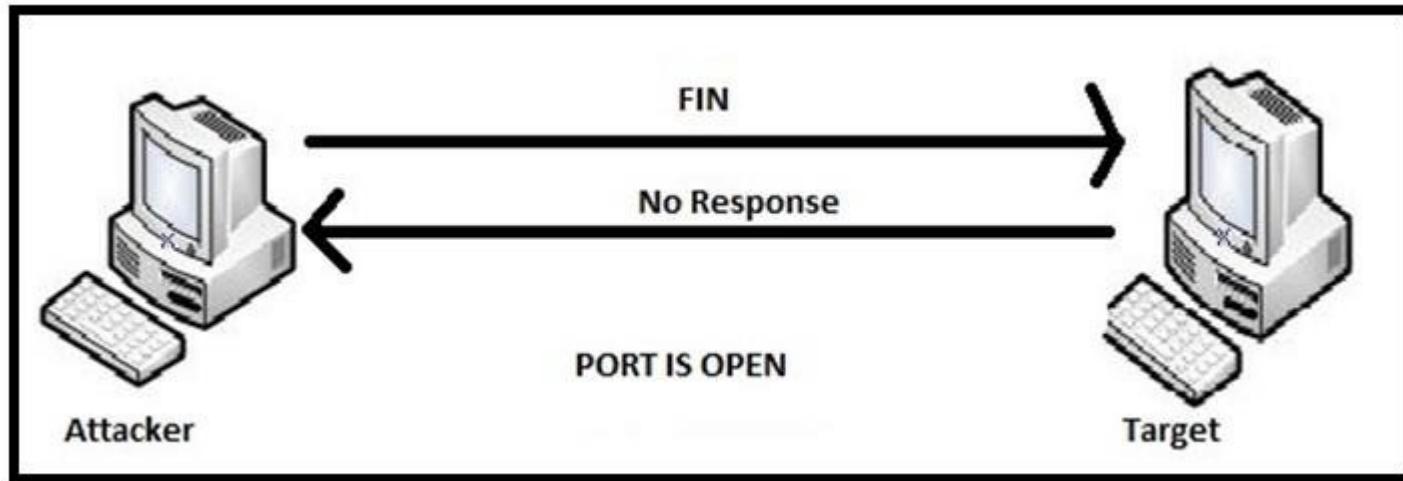
SYN, ACK+SYN

May not be able to identify scanner

ACK Scan (Nmap -sA)



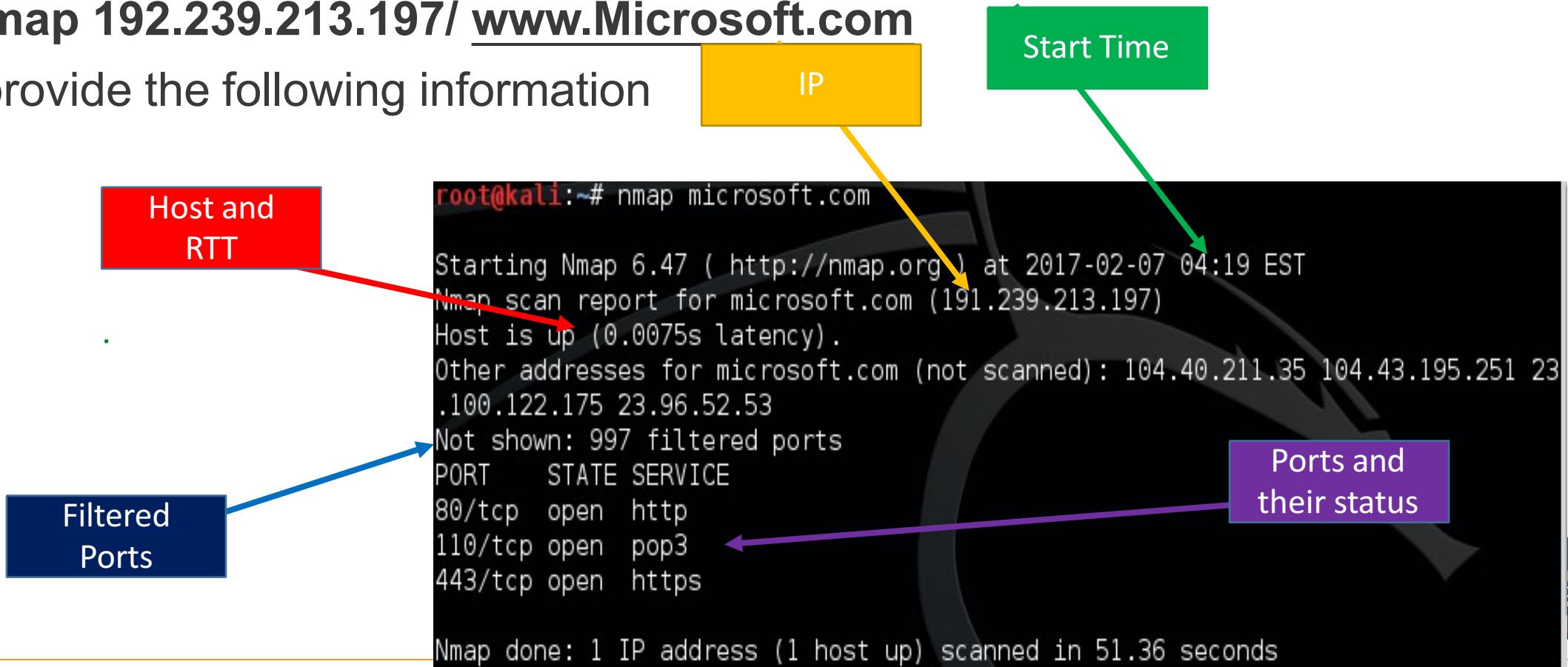
FIN Scan (Nmap -sF)



Basic scanning with Nmap

1. nmap <target> IP or Domain name

- scans 1,000 TCP ports on the host <target>.
- e.g. nmap 192.239.213.197/ www.Microsoft.com
- It will provide the following information



The screenshot shows the terminal output of an Nmap scan for the domain `microsoft.com`. The output includes the start time, host status, filtered ports, and open ports with their services.

```
root@kali:~# nmap microsoft.com
Starting Nmap 6.47 ( http://nmap.org ) at 2017-02-07 04:19 EST
Nmap scan report for microsoft.com (191.239.213.197)
Host is up (0.0075s latency).
Other addresses for microsoft.com (not scanned): 104.40.211.35 104.43.195.251 23
  .100.122.175 23.96.52.53
Not shown: 997 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
110/tcp   open  pop3
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 51.36 seconds
```

Annotations pointing to specific parts of the output:

- Host and RTT**: Points to the line "Host is up (0.0075s latency)".
- IP**: Points to the IP address "191.239.213.197".
- Start Time**: Points to the timestamp "2017-02-07 04:19 EST".
- Filtered Ports**: Points to the line "Not shown: 997 filtered ports".
- Ports and their status**: Points to the table showing open ports and their services.

Nmap commands

- **How will you identify is this machine-linux/windows?**
 - In windows, 3 ports will always be open
 - 135 - msrp
 - 139 - netbios-ssn
 - 445 – Microsoft-ds
- Try on Linux machine- Take IP address of Linux- all these 3 ports are closed
 - Start SMBD service
 - Service smbd start
 - Scan all ports again in Linux
 - Check for all ports
 - It will show 2 ports open

Nmap scan commands



Nmap Examples

2. Scan multiple IP address or subnet (IPv4)

Nmap 192.168.195.1-255 (check for whole range of IP from 1 to 255)

Nmap 192.168.195.1/16

- It will check for 254 hosts (16 network and 16 host) Nmap

192.168.1.*

```
nmap 192.168.1.1 192.168.1.2 192.168.1.3

## works with same subnet i.e. 192.168.1.0/24
nmap 192.168.1.1,2,3

## You can scan a range of IP address too:
nmap 192.168.1.1-20

## You can scan a range of IP address using a wildcard:
nmap 192.168.1.1-20

## Finally, you scan an entire subnet:
nmap 192.168.1.0/24
```

Nmap commands

3. Nmap -p 25 192.168.195.249

- Port is closed

Check specific range

3a. Nmap -p 1000-1200 192.168.195.249

- Scans from 1000-1200
- Fast because less scan

Nmap -p 80,443 192.168.1.1

Nmap --top-ports 5 192.168.1.1

Scan top ports i.e. scan \$number most common ports

Nmap --top-ports 10 192.168.1.1



Scan on Specific port

```
root@kali:~# nmap -p 20-25,80,443 microsoft.com

Starting Nmap 6.47 ( http://nmap.org ) at 2017-02-07 05:06 EST
Nmap scan report for microsoft.com (104.40.211.35)
Host is up (0.0032s latency).
Other addresses for microsoft.com (not scanned): 104.43.195.251 23.100.122.175 2
3.96.52.53 191.239.213.197
PORT      STATE     SERVICE
20/tcp    filtered  ftp-data
21/tcp    filtered  ftp
22/tcp    filtered  ssh
23/tcp    filtered  telnet
24/tcp    filtered  priv-mail
25/tcp    filtered  smtp
80/tcp    open       http
443/tcp   open       https
```

```
root@kali:~# nmap -p http,mysql microsoft.com

Starting Nmap 6.47 ( http://nmap.org ) at 2017-02-07 05:08 EST
Nmap scan report for microsoft.com (104.43.195.251)
Host is up (0.00080s latency).
Other addresses for microsoft.com (not scanned): 23.100.122.175 23.96.52.53 191.
239.213.197 104.40.211.35
PORT      STATE     SERVICE
80/tcp    open       http
3306/tcp  filtered mysql
8008/tcp  filtered http
```



Nmap Examples

Check all port range open/closed

Nmap -p 0-65535 192.168.195.249

Nmap -p- 192.168.195.249

Nmap -p "*" 192.168.195.249

Scan on all port

```
root@kali:~# nmap -p "*" 191.239.213.197
```

```
Starting Nmap 6.47 ( http://nmap.org ) at 2017-02-08 04:58 EST
```

```
Nmap scan report for 191.239.213.197
```

```
Host is up (0.00054s latency).
```

```
Not shown: 4239 filtered ports
```

PORT	STATE	SERVICE
------	-------	---------

80/tcp	open	http
--------	------	------

110/tcp	open	pop3
---------	------	------

443/tcp	open	https
---------	------	-------

5222/tcp	open	xmpp-client
----------	------	-------------

```
Nmap done: 1 IP address (1 host up) scanned in 88.00 seconds
```

Nmap commands

Find OS

4. Nmap -O 192.168.195.249

- It requires root privilege, enter command sudo su
- Device type: general purpose
 - If android- smartphone
 - If IOS- Iphone
- OS details: it tells on the basis of services

Remote Host OS Detection

```
root@kali:~# nmap -O microsoft.com

Starting Nmap 6.47 ( http://nmap.org ) at 2017-02-07 04:46 EST
Nmap scan report for microsoft.com (104.43.195.251)
Host is up (0.0059s latency).
Other addresses for microsoft.com (not scanned): 23.100.122.175 23.96.52.53 191.
239.213.197 104.40.211.35
Not shown: 996 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
110/tcp   open  pop3
443/tcp   open  https
5222/tcp  open  xmpp-client
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: general purpose
Running: Linux 2.4.X, Microsoft Windows 7
OS CPE: cpe:/o:linux:linux_kernel:2.4 cpe:/o:microsoft:windows_7:::enterprise
OS details: DD-WRT v24-sp2 (Linux 2.4.37), Microsoft Windows 7 Enterprise

OS detection performed. Please report any incorrect results at http://nmap.org/s
ubmit/
Nmap done: 1 IP address (1 host up) scanned in 53.87 seconds
```

Nmap commands

For Fast scan

5a. Nmap -F 192.168.195.249

- F means that we going to scan 100 most popular ports (this option also required for quick scans)

5b. Nmap –T4 192.168.195.249

- T1- 1 packet in 1 sec
- T4- 4 packets in 1 sec - more power scan/fast
- T5 is the maximum, most aggressive scan)

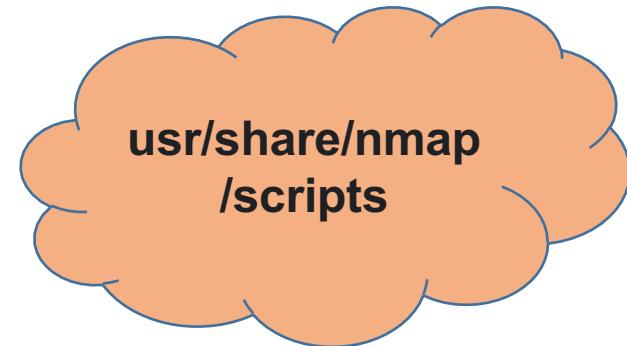
```
root@kali:~# nmap -F 23.96.52.53
Starting Nmap 6.47 ( http://nmap.org ) at 2017-02-07 05:04 EST
Nmap scan report for 23.96.52.53
Host is up (0.0056s latency).
Not shown: 98 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
110/tcp   open  pop3
Nmap done: 1 IP address (1 host up) scanned in 1.76 seconds
```



Nmap commands/Scripts

6. Stealthy scan

nmap -sS 192.168.1.1



usr/share/nmap
/scripts

TCP ports using **TCP connect scan** (warning: no stealth scan)- **OS Fingerprinting**
nmap -sT 192.168.1.1

Find out the most commonly used TCP ports using **TCP ACK scan**
nmap -sA 192.168.1.1

Find out the most commonly used TCP ports using **TCP Window scan**
nmap -sW 192.168.1.1



Nmap Examples

Find out the most commonly used TCP ports using TCP SYN Scan

```
### Stealthy scan ###
nmap -sS 192.168.1.1
```

```
### Find out the most commonly used TCP ports using TCP connect scan (warning: no stealth scan)
```

```
### OS Fingerprinting ###
nmap -sT 192.168.1.1
```

```
### Find out the most commonly used TCP ports using TCP ACK scan
```

```
nmap -sA 192.168.1.1
```

```
### Find out the most commonly used TCP ports using TCP Window scan
```

```
nmap -sW 192.168.1.1
```

Nmap Examples

6. Detect remote services (server / daemon) version numbers:

- Nmap -sV 192.168.195.249
 - -s script /--script
 - V Verbose

7. Nmap -sS -sV 192.168.195.249

- -s script /--script
- S sync
- V Verbose-> bring data from/of header

Nmap commands

There are total 602 NSE scripts

- Cd path usr/share/nmap/scripts
- Now run the next command (9, 10)
- You can also explicitly use a script

8. Nmap --script=dhcp-discover google.com

Aggressive Scan/ Intense Scan

9. Nmap -A -T4 192.168.195.249

- A-Aggressive
- T4 increase power of nmap
- Gives service
- OS



Aggressive Scan-OS & Service Detection

```
root@kali:~# nmap -A microsoft.com
```

```
Starting Nmap 6.47 ( http://nmap.org ) at 2017-02-07 04:21 EST
Nmap scan report for microsoft.com (104.40.211.35)
Host is up (0.0026s latency).
Other addresses for microsoft.com (not scanned): 104.43.195.251 23.100.122.175 2
3.96.52.53 191.239.213.197
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http?
110/tcp   open  pop3?
443/tcp   open  https?
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: general purpose
Running: Linux 2.4.X, Microsoft Windows 7|XP
OS CPE: cpe:/o:linux:linux_kernel:2.4 cpe:/o:microsoft:windows_7:::enterprise cp
e:/o:microsoft:windows_xp::sp3
OS details: DD-WRT v24-sp2 (Linux 2.4.37), Microsoft Windows 7 Enterprise, Micro
soft Windows XP SP3
Network Distance: 2 hops
```

```
TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1  0.09 ms  192.168.134.2
2  0.12 ms  104.40.211.35
```

```
OS and Service detection performed. Please report any incorrect results at http:
//nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 145.49 seconds
```

Nmap Examples

10. Only show open (or possibly open) ports

```
nmap --open 192.168.1.1
nmap --open example.com
```

```
root@kali:~# nmap --iflist
Starting Nmap 6.47 ( http://nmap.org ) at 2017-02-07 08:21 EST
*****INTERFACES*****
DEV (SHORT) IP/MASK          TYPE   UP MTU  MAC
lo (lo)   127.0.0.1/8        loopback up 65536
lo (lo)   ::1/128           loopback up 65536
eth0 (eth0) 192.168.134.151/24  ethernet up 1500  00:0C:29:F6:C8:43
eth0 (eth0) fe80::20c:29ff:fef6:c843/64  ethernet up 1500  00:0C:29:F6:C8:43
*****ROUTES*****
DST/MASK          DEV METRIC GATEWAY
192.168.134.0/24 eth0 0
0.0.0.0/0         eth0 0      192.168.134.2
::1/128           lo 0
fe80::/64          eth0 256
ff00::/8           eth0 256
```

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.51 seconds

11. Show host interfaces and routes

This is useful for debugging

Nmap --iflist