Ex.4 **Port Scan using nmap**

Aim:

To perform port scan using Nmap tool and Kali Linux nmap

Port scanning

Ports are essential for computers to communicate with other computers or for applications to communicate with their corresponding services over the internet. These ports have assigned numbers dedicated to specific services and are used by hackers to try and break into them, using the vulnerabilities of the hardware and software that use these ports.

A port scan is a common technique hackers use to discover open doors or weak points in a network. A port scan attack helps cyber criminals find open ports and figure out whether they are receiving or sending data. It can also reveal whether active security devices like firewalls are being used by an organization. When hackers send a message to a port, the response they receive determines whether the port is being used and if there are any potential weaknesses that could be exploited. They can use tools like IP scanning, network mapper (Nmap), and Netcat to ensure their network and systems are secure.

Port scanning can provide information such as:

1. Services that are running
2. Users who own services
3. Whether anonymous logins are allowed
4. Which network services require authentication

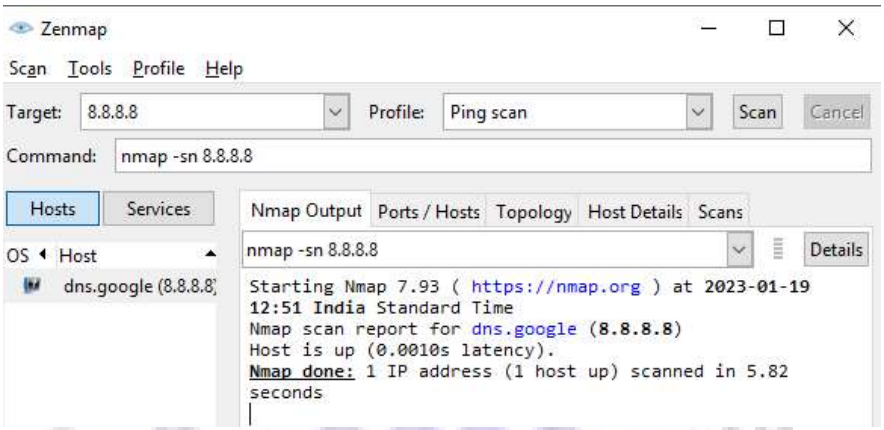
Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services those hosts are offering, what operating systems 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.

Scan types using Nmap

1) Ping scan:

Command: nmap -sn <target>

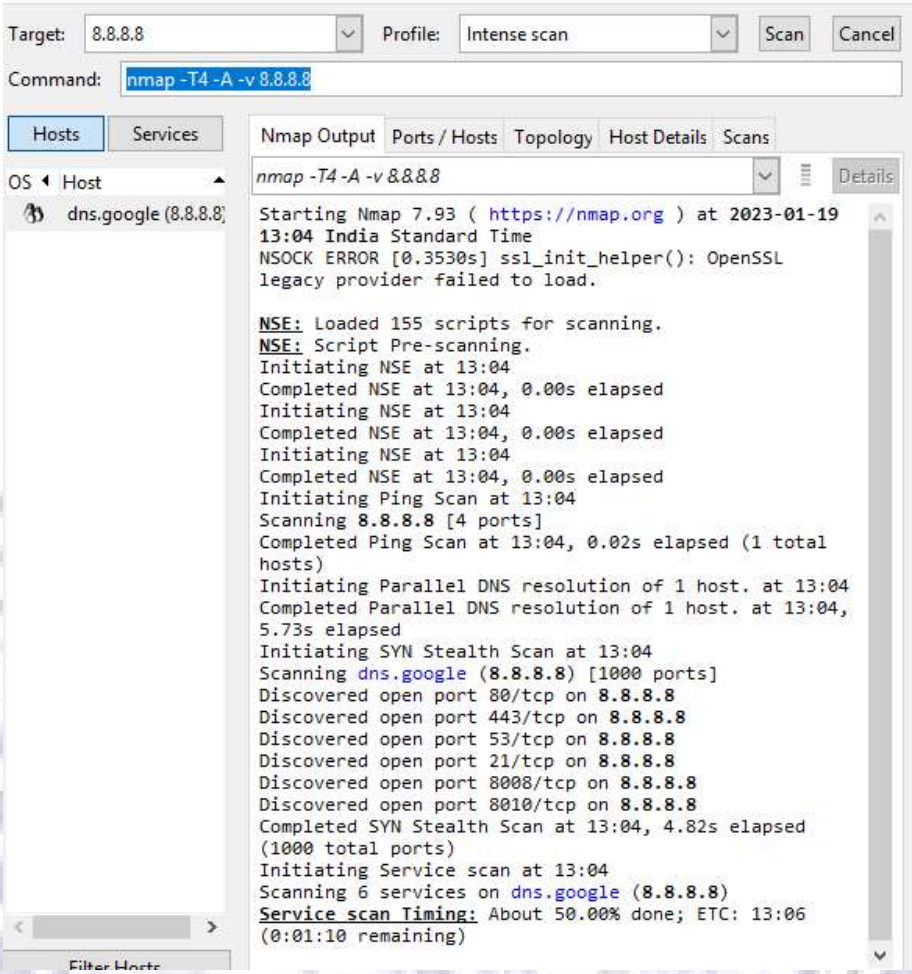
Do a ping on the target, no port scan. Type in target as 8.8.8.8 and Profile as ‘Ping scan’ and click scan button. Automatically the equivalent command will be displayed in the command text box. Example: nmap –sn 8.8.8.8



2) Intense scan:

Command: nmap -T4 -A -v <target>

It is a quick and scan the most common TCP ports. It will make an effort in determining the OS type and what services and their versions are running. The option (-T4) is for fast timing template, -A option which will try determine services, versions and OS. With the verbose output (-v) it will also give us a lot of feedback as Nmap makes progress in the scan. Type in target as 8.8.8.8 and Profile as 'Intense scan' and click scan button. Example: nmap -T4 -A -v 8.8.8.8



3) Intense scan plus UDP:

Command: nmap -sS -sU -T4 -A -v <target>

Same as the regular Intense scan, just that we will also scan UDP ports (-sU). The -sS option is telling Nmap that it should also scan TCP ports using SYN packets. Because this scan includes UDP ports this explicit definition of -sS is necessary. Example: nmap -sS -sU -T4 -A -v 8.8.8.8

Output:

Starting Nmap 7.93 (https://nmap.org) at 2023-01-19 13:07 India Standard Time
NSOCK ERROR [0.3590s] ssl_init_helper(): OpenSSL legacy provider failed to load.
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 13:07
Completed NSE at 13:07, 0.00s elapsed
Initiating NSE at 13:07
Completed NSE at 13:07, 0.00s elapsed
Initiating NSE at 13:07
Completed NSE at 13:07, 0.00s elapsed

Initiating Ping Scan at 13:07
Scanning 8.8.8.8 [4 ports]
Completed Ping Scan at 13:07, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:07
Completed Parallel DNS resolution of 1 host. at 13:07, 5.55s elapsed
Initiating SYN Stealth Scan at 13:07
Scanning dns.google (8.8.8.8) [1000 ports]
Discovered open port 53/tcp on 8.8.8.8
Discovered open port 80/tcp on 8.8.8.8
Discovered open port 21/tcp on 8.8.8.8
Discovered open port 443/tcp on 8.8.8.8
Discovered open port 8010/tcp on 8.8.8.8
Discovered open port 8008/tcp on 8.8.8.8
Completed SYN Stealth Scan at 13:07, 4.73s elapsed (1000 total ports)
Initiating UDP Scan at 13:07
Scanning dns.google (8.8.8.8) [1000 ports]
Increasing send delay for 8.8.8.8 from 0 to 50 due to 11 out of 11 dropped probes since last increase.
Increasing send delay for 8.8.8.8 from 50 to 100 due to 11 out of 11 dropped probes since last increase.
UDP Scan Timing: About 14.80% done; ETC: 13:11 (0:02:58 remaining)
Increasing send delay for 8.8.8.8 from 100 to 200 due to 11 out of 11 dropped probes since last increase.
Increasing send delay for 8.8.8.8 from 200 to 400 due to 11 out of 12 dropped probes since last increase.
UDP Scan Timing: About 26.55% done; ETC: 13:12 (0:03:14 remaining)
UDP Scan Timing: About 30.00% done; ETC: 13:13 (0:03:53 remaining)

4) Intense scan, all TCP ports:

Command: nmap -p 1-65535 -T4 -A -v <target>

Leave no TCP ports unchecked. Normally Nmap scans a list of 1000 most common protocols, but instead we will in this example scan everything from port 1 to 65535 (max). The 1000 most common protocols listing can be found in the file called nmap-services. (NSE – Nmap Scripting Engine)

Example: nmap -p 1-65535 -T4 -A -v 8.8.8.8

Output:

Starting Nmap 7.93 (https://nmap.org) at 2023-01-19 14:57 India Standard Time
NSOCK ERROR [0.3670s] ssl_init_helper(): OpenSSL legacy provider failed to load.
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:57
Completed NSE at 14:57, 0.00s elapsed
Initiating NSE at 14:57
Completed NSE at 14:57, 0.00s elapsed
Initiating NSE at 14:57
Completed NSE at 14:57, 0.00s elapsed
Initiating Ping Scan at 14:57
Scanning 8.8.8.8 [4 ports]

Completed Ping Scan at 14:57, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:57
Completed Parallel DNS resolution of 1 host. at 14:57, 5.73s elapsed
Initiating SYN Stealth Scan at 14:57
Scanning dns.google (8.8.8.8) [65535 ports]
Discovered open port 443/tcp on 8.8.8.8
Discovered open port 21/tcp on 8.8.8.8
Discovered open port 53/tcp on 8.8.8.8
Discovered open port 80/tcp on 8.8.8.8
Discovered open port 8008/tcp on 8.8.8.8
SYN Stealth Scan Timing: About 22.35% done; ETC: 15:00 (0:01:48 remaining)
Discovered open port 8020/tcp on 8.8.8.8
SYN Stealth Scan Timing: About 57.93% done; ETC: 14:59 (0:00:44 remaining)
Discovered open port 8010/tcp on 8.8.8.8
Discovered open port 8015/tcp on 8.8.8.8
Completed SYN Stealth Scan at 14:59, 88.75s elapsed (65535 total ports)
Initiating Service scan at 14:59
Scanning 8 services on dns.google (8.8.8.8)
Service scan Timing: About 50.00% done; ETC: 15:01 (0:01:10 remaining)
Service scan Timing: About 75.00% done; ETC: 15:02 (0:00:52 remaining)
Completed Service scan at 15:01, 156.06s elapsed (8 services on 1 host)
Initiating OS detection (try #1) against dns.google (8.8.8.8)
Retrying OS detection (try #2) against dns.google (8.8.8.8)
Initiating Traceroute at 15:01
Completed Traceroute at 15:01, 0.02s elapsed
Initiating Parallel DNS resolution of 1 host. at 15:01
Completed Parallel DNS resolution of 1 host. at 15:02, 5.55s elapsed
NSE: Script scanning 8.8.8.8.
Initiating NSE at 15:02
Completed NSE at 15:04, 130.47s elapsed
Initiating NSE at 15:04
Completed NSE at 15:04, 44.79s elapsed
Initiating NSE at 15:04
Completed NSE at 15:04, 0.00s elapsed
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.0020s latency).
Not shown: 65526 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
21/tcp open ftp?
53/tcp open tcpwrapped
80/tcp open http?
113/tcp closed ident
443/tcp open ssl/https HTTP server (unknown)
| ssl-cert: Subject: commonName=dns.google
| Subject Alternative Name: DNS:dns.google, DNS:dns.google.com, DNS:*.dns.google.com, DNS:8888.google, DNS:dns64.dns.google, IP Address:8.8.8.8, IP Address:8.8.4.4, IP Address:2001:4860:4860:0:0:0:0:8888, IP Address:2001:4860:4860:0:0:0:0:8844, IP

Address:2001:4860:4860:0:0:0:0:6464, IP Address:2001:4860:4860:0:0:0:0:64
...
8015/tcp open cfg-cloud?
8020/tcp open http-proxy FortiGate Web Filtering Service
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-title: Web Filter Block Override
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8008-TCP:V=7.93%I=7%D=1/19%Time=63C90D73%P=i686-pc-windows-windows%
...
Device type: general purpose
Running (JUST GUESSING): Linux 3.X|2.6.X|4.X (92%), Microsoft Windows Vista (85%)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:4 cpe:/o:microsoft:windows_vista::sp1:home_premium
Aggressive OS guesses: Linux 3.2 - 3.8 (92%), Linux 2.6.32 - 2.6.39 (88%), Linux 2.6.38 (88%), Linux 2.6.32 (87%), Linux 2.6.32 or 3.10 (86%), Linux 3.11 - 4.1 (86%), Microsoft Windows Vista Home Premium SP1 (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 35.989 days (since Wed Dec 14 15:21:06 2022)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incremental
TRACEROUTE (using port 113/tcp)
HOP RTT ADDRESS
1 3.00 ms 10.0.12.1
2 1.00 ms dns.google (8.8.8.8)
NSE: Script Post-scanning.
Initiating NSE at 15:04
Completed NSE at 15:04, 0.00s elapsed
Initiating NSE at 15:04
Completed NSE at 15:04, 0.00s elapsed
Initiating NSE at 15:04
Completed NSE at 15:04, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 437.03 seconds
Raw packets sent: 131217 (5.778MB) | Rcvd: 109 (4.796KB)

5) Intense scan, no ping:

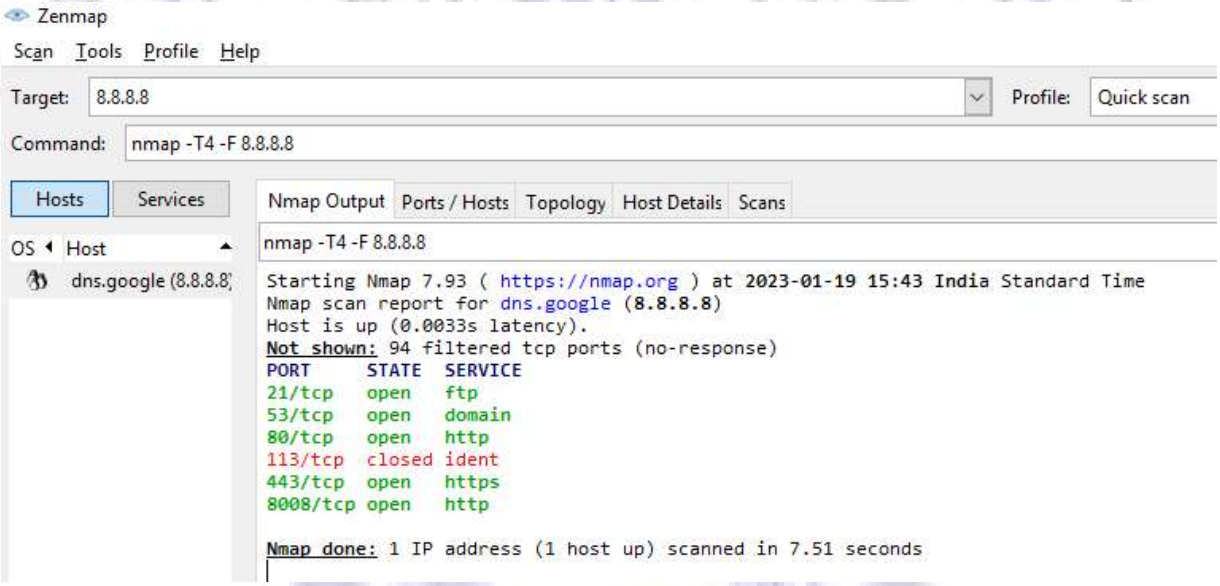
Command: nmap -T4 -A -v -Pn <target>
Just like the other intense scans, however this will assume the host is up. Useful if the target is blocking ping request and you already know the target is up. Example: nmap -T4 -A -v -Pn 8.8.8.8

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-19 14:57 India Standard Time
NSOCK ERROR [0.3670s] ssl_init_helper(): OpenSSL legacy provider failed to load.
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:57
Completed NSE at 14:57, 0.00s elapsed
Initiating Ping Scan at 14:57
Scanning 8.8.8.8 [4 ports]
Completed Ping Scan at 14:57, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:57
Completed Parallel DNS resolution of 1 host. at 14:57, 5.73s elapsed
Initiating SYN Stealth Scan at 14:57
Scanning dns.google (8.8.8.8) [65535 ports]
Discovered open port 443/tcp on 8.8.8.8
Discovered open port 21/tcp on 8.8.8.8
Discovered open port 53/tcp on 8.8.8.8
Discovered open port 80/tcp on 8.8.8.8
Discovered open port 8008/tcp on 8.8.8.8
Scanning 8 services on dns.google (8.8.8.8)
Initiating OS detection (try #1) against dns.google (8.8.8.8)
Retrying OS detection (try #2) against dns.google (8.8.8.8)
Initiating Traceroute at 15:01
Completed Traceroute at 15:01, 0.02s elapsed
Initiating Parallel DNS resolution of 1 host. at 15:01
Completed Parallel DNS resolution of 1 host. at 15:02, 5.55s elapsed
NSE: Script scanning 8.8.8.8.
Initiating NSE at 15:02
Completed NSE at 15:04, 0.00s elapsed
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.0020s latency).
Not shown: 65526 filtered tcp ports (no-response)
PORT     STATE  SERVICE       VERSION
21/tcp   open   ftp?
53/tcp   open   tcpwrapped
80/tcp   open   http?
113/tcp  closed ident
443/tcp  open   ssl/https      HTTP server (unknown)
...
Device type: general purpose
Running (JUST GUESSING): Linux 3.X|2.6.X|4.X (92%), Microsoft Windows Vista (85%)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:4
cpe:/o:microsoft:windows_vista::sp1:home_premium
Aggressive OS guesses: Linux 3.2 - 3.8 (92%), Linux 2.6.32 - 2.6.39 (88%), Linux 2.6.38 (88%),
Linux 2.6.32 (87%), Linux 2.6.32 or 3.10 (86%), Linux 3.11 - 4.1 (86%), Microsoft Windows
Vista Home Premium SP1 (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 35.989 days (since Wed Dec 14 15:21:06 2022)
```

Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incremental
TRACEROUTE (using port 113/tcp)
HOP RTT ADDRESS
1 3.00 ms 10.0.12.1
2 1.00 ms dns.google (8.8.8.8)
NSE: Script Post-scanning.
Initiating NSE at 15:04
Completed NSE at 15:04, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 437.03 seconds
Raw packets sent: 131217 (5.778MB) | Rcvd: 109 (4.796KB)

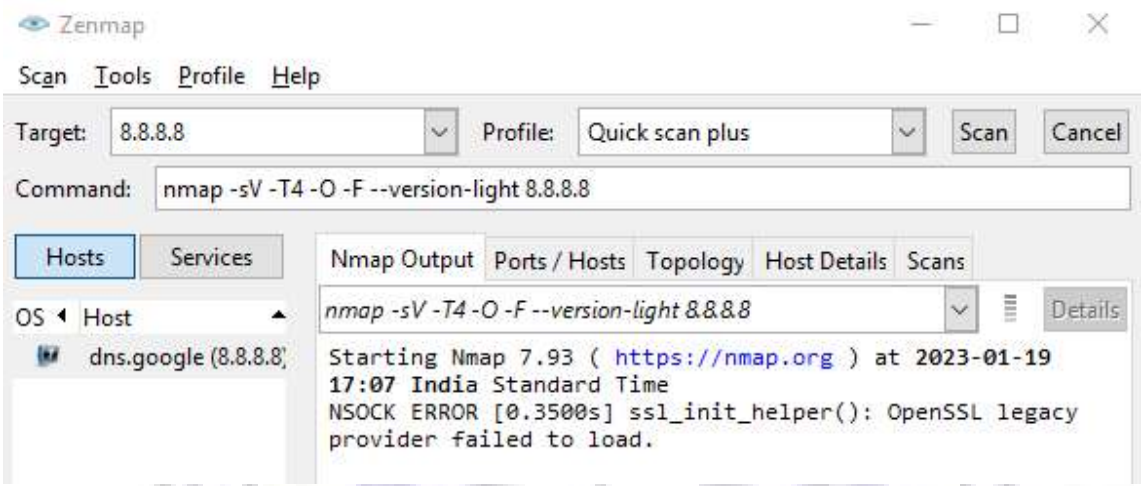
6) Quick scan:

Command: nmap -T4 -F <target>
Scan faster than the intense scan by limiting the number of TCP ports scanned to only the top 100 most common TCP ports. Example: nmap -T4 -F 8.8.8.8



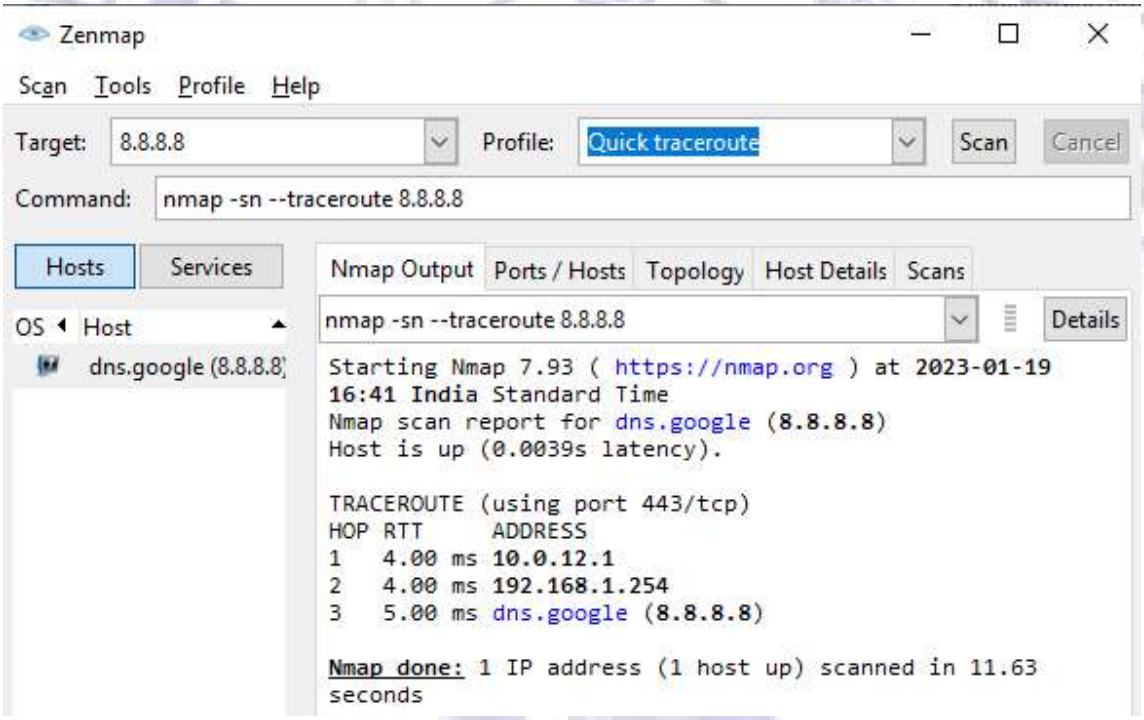
7) Quick scan plus:

Command: nmap -sV -T4 -O -F –version-light <target>
Add a little bit of version and OS detection and you got the Quick scan plus. Example: nmap -sV -T4 -O -F --version-light 8.8.8.8



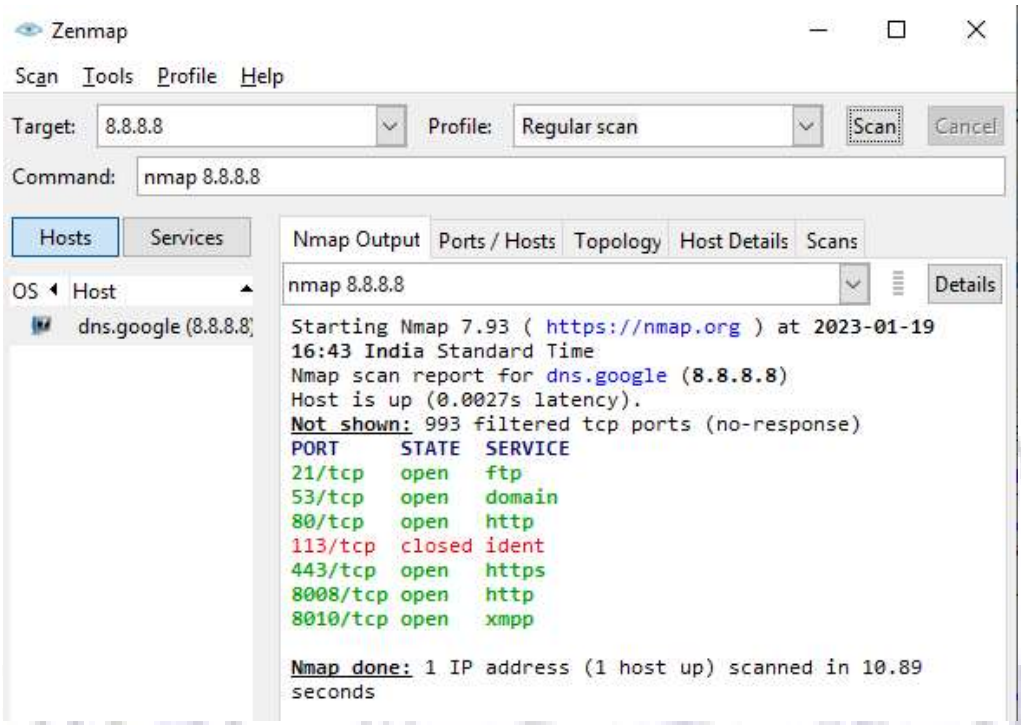
8) Quick traceroute:

Command: nmap -sn –traceroute <target>
We can use this option when we need to determine hosts and routers in a network scan. It will traceroute and ping all hosts defined in the target. Example: nmap -sn --traceroute 8.8.8.8



9) Regular scan:

Command: nmap <target>
Default everything. This means it will issue a TCP SYN scan for the most common 1000 TCP ports, using ICMP Echo request (ping) for host detection. Example: nmap 8.8.8.8



10) Slow comprehensive scan:

Command: nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 –script "default or (discovery and safe)" <target>

This scan has a whole bunch of options in it and it may seem daunting to understand at first. It is however not so complicated once you take a closer look at the options. The scan can be said to be a "Intense scan plus UDP" plus some extras features. It will put a whole lot of effort into host detection, not giving up if the initial ping request fails. It uses three different protocols in order to detect the hosts; TCP, UDP and SCTP. If a host is detected it will do its best in determining what OS, services and versions the host are running based on the most common TCP and UDP services. Also the scan camouflages itself as source port 53 (DNS).
Example: nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" 8.8.8.8

Output:

Starting Nmap 7.93 (https://nmap.org) at 2023-01-19 16:44 India Standard Time
NSOCK ERROR [0.3530s] ssl_init_helper(): OpenSSL legacy provider failed to load.
NSE: Loaded 296 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:44
NSE: [mtrace] A source IP must be provided through fromip argument.
NSE: [shodan-api] Error: Please specify your ShodanAPI key with the shodan-api.apikey argument
Completed NSE at 16:44, 0.00s elapsed
Pre-scan script results:

...
Initiating Ping Scan at 16:44
Scanning 8.8.8.8 [7 ports]
Completed Ping Scan at 16:44, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:44
Completed Parallel DNS resolution of 1 host. at 16:44, 5.74s elapsed
Initiating SYN Stealth Scan at 16:44
Scanning dns.google (8.8.8.8) [1000 ports]
Discovered open port 443/tcp on 8.8.8.8
Discovered open port 80/tcp on 8.8.8.8
Discovered open port 21/tcp on 8.8.8.8
Discovered open port 53/tcp on 8.8.8.8
Discovered open port 8008/tcp on 8.8.8.8
Discovered open port 8010/tcp on 8.8.8.8
Completed SYN Stealth Scan at 16:44, 4.76s elapsed (1000 total ports)
Initiating UDP Scan at 16:44
Scanning dns.google (8.8.8.8) [1000 ports]
Increasing send delay for 8.8.8.8 from 0 to 50 due to 11 out of 11 dropped probes since last increase.
Increasing send delay for 8.8.8.8 from 50 to 100 due to 11 out of 11 dropped probes since last increase.
UDP Scan Timing: About 14.05% done; ETC: 16:48 (0:03:10 remaining)
Increasing send delay for 8.8.8.8 from 100 to 200 due to 11 out of 11 dropped probes since last increase.
Increasing send delay for 8.8.8.8 from 200 to 400 due to 11 out of 11 dropped probes since last increase.
UDP Scan Timing: About 25.20% done; ETC: 16:49 (0:03:28 remaining)
UDP Scan Timing: About 28.55% done; ETC: 16:50 (0:04:10 remaining)
Increasing send delay for 8.8.8.8 from 400 to 800 due to 11 out of 11 dropped probes since last increase.
UDP Scan Timing: About 31.25% done; ETC: 16:51 (0:04:46 remaining)
UDP Scan Timing: About 32.95% done; ETC: 16:53 (0:05:26 remaining)
UDP Scan Timing: About 34.60% done; ETC: 16:54 (0:05:59 remaining)
Increasing send delay for 8.8.8.8 from 800 to 1000 due to 11 out of 11 dropped probes since last increase.
UDP Scan Timing: About 36.25% done; ETC: 16:55 (0:06:27 remaining)
UDP Scan Timing: About 37.90% done; ETC: 16:56 (0:06:59 remaining)
UDP Scan Timing: About 39.90% done; ETC: 16:57 (0:07:33 remaining)
UDP Scan Timing: About 43.05% done; ETC: 16:59 (0:08:11 remaining)

Port Scan using Kali Linux:

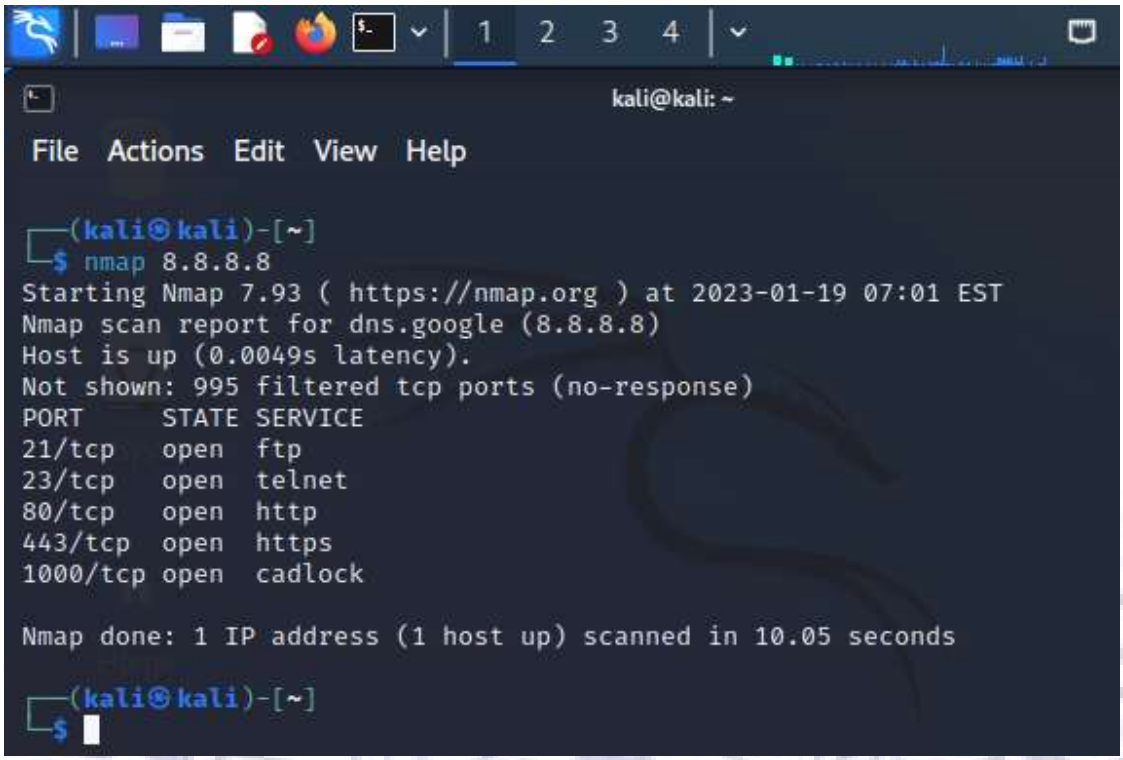
Procedure:

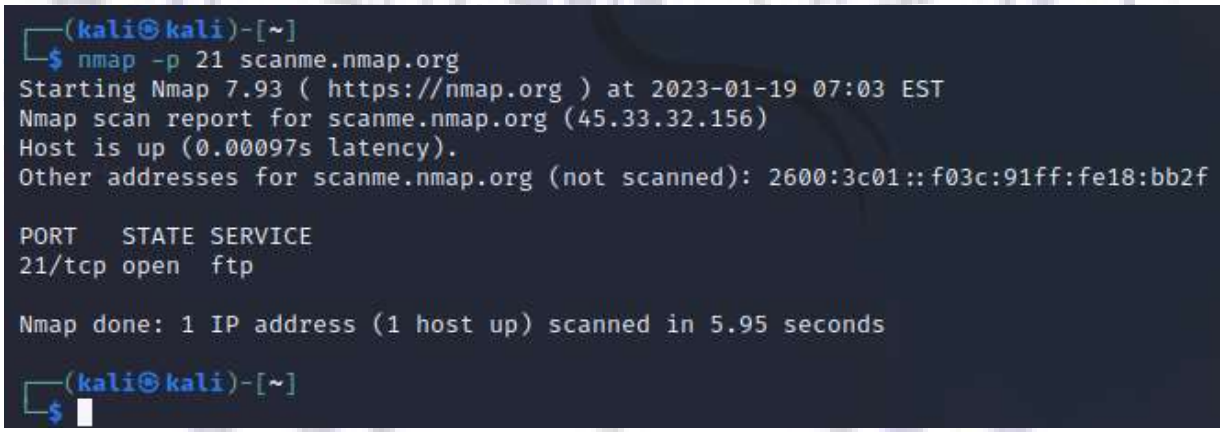
1. Open kali linux
2. Select the option Applications -> Information Gathering -> Nmap
3. Default url we can use for target can be scanme.nmap.org or google.com
4. To scan a host or single target type as nmap scanme.nmap.org

5. To scan a single IP address type as nmap 8.8.8.8
6. To scan a single port type as nmap –p 21 scanme.nmap.org
7. To scan a range of ports type as nmap -p 81-90 scanme.nmap.org
8. To scan the operating system type as sudo nmap –O scanme.nmap.org
9. To detect the service version type as nmap –sV scanme.nmap.org
10. To write the scan results to a file type as nmap –oN scan1.txt scanme.nmap.org

```
┌──(kali㉿kali)-[~]
└─$ nmap scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-19 06:54 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.0042s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
443/tcp  open  https
8008/tcp open  http
8010/tcp open  xmpp

Nmap done: 1 IP address (1 host up) scanned in 10.61 seconds

┌──(kali㉿kali)-[~]
└─$
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -6 scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-19 06:49 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.05 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -Pn scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-19 06:50 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.042s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
113/tcp  closed ident
443/tcp  open   https
8008/tcp open   http
8010/tcp open   xmpp

Nmap done: 1 IP address (1 host up) scanned in 19.97 seconds

┌──(kali㉿kali)-[~]
└─$
```


1 2 3 4
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap 8.8.8.8
Starting Nmap 7.93 (https://nmap.org) at 2023-01-19 07:01 EST
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.0049s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT STATE SERVICE
21/tcp open ftp
23/tcp open telnet
80/tcp open http
443/tcp open https
1000/tcp open cadlock
Nmap done: 1 IP address (1 host up) scanned in 10.05 seconds
(kali㉿kali)-[~]
$


(kali㉿kali)-[~]
$ nmap -p 21 scanme.nmap.org
Starting Nmap 7.93 (https://nmap.org) at 2023-01-19 07:03 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.00097s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
PORT STATE SERVICE
21/tcp open ftp
Nmap done: 1 IP address (1 host up) scanned in 5.95 seconds
(kali㉿kali)-[~]
$

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 81-90 scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-19 07:06 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.00076s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f

PORT   STATE    SERVICE
81/tcp filtered hosts2-ns
82/tcp filtered xfer
83/tcp filtered mit-ml-dev
84/tcp filtered ctf
85/tcp filtered mit-ml-dev
86/tcp filtered mfcobol
87/tcp filtered priv-term-l
88/tcp filtered kerberos-sec
89/tcp filtered su-mit-tg
90/tcp filtered dnsix

Nmap done: 1 IP address (1 host up) scanned in 6.82 seconds

┌──(kali㉿kali)-[~]
└─$
```

```
File  Actions  Edit  View  Help
└─$ sudo nmap -O scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-19 07:12 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.0069s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
23/tcp   open   telnet
80/tcp   open   http
113/tcp  closed ident
443/tcp  open   https
1000/tcp open   cadlock
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (99%), QEMU (99%), Bay Networks embedded (90
%), Linux (89%), Allied Telesyn embedded (89%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_450 cpe:/
o:linux:linux_kernel:2.6.18 cpe:/h:alliedtelesyn:at-9006
Aggressive OS guesses: Oracle Virtualbox (99%), QEMU user mode network gateway (99%), B
ay Networks BayStack 450 switch (software version 3.1.0.22) (90%), Linux 2.6.18 (CentOS
 5, x86_64, SMP) (89%), Allied Telesyn AT-9006SX/SC switch (89%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/
 .
Nmap done: 1 IP address (1 host up) scanned in 35.47 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-19 07:17 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.0045s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp      FortiGate Application filtering
23/tcp   open  telnet   FortiGate Application Filtering
80/tcp   open  http     FortiGate Application filtering (Auth server 192.168.1.254:1000)
443/tcp  open  ssl/http FortiGate Application filtering (Auth server 192.168.1.254:1003)
1000/tcp open  http     FortiGate Application filtering (Auth server 192.168.1.254:1000)

Service detection performed. Please report any incorrect results at https://nmap.org/submi
t/ .
Nmap done: 1 IP address (1 host up) scanned in 23.88 seconds

┌──(kali㉿kali)-[~]
└─$
```

```
File  Actions  Edit  View  Help
└─$ nmap -oN scan1.txt scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-19 07:19 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.0031s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
23/tcp   open  telnet
80/tcp   open  http
443/tcp  open  https
1000/tcp open  cadlock

Nmap done: 1 IP address (1 host up) scanned in 10.58 seconds

┌──(kali㉿kali)-[~]
└─$ cat scan1.txt
# Nmap 7.93 scan initiated Thu Jan 19 07:19:42 2023 as: nmap -oN scan1.txt scanme.nma
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.0031s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
23/tcp   open  telnet
80/tcp   open  http
443/tcp  open  https
1000/tcp open  cadlock
```