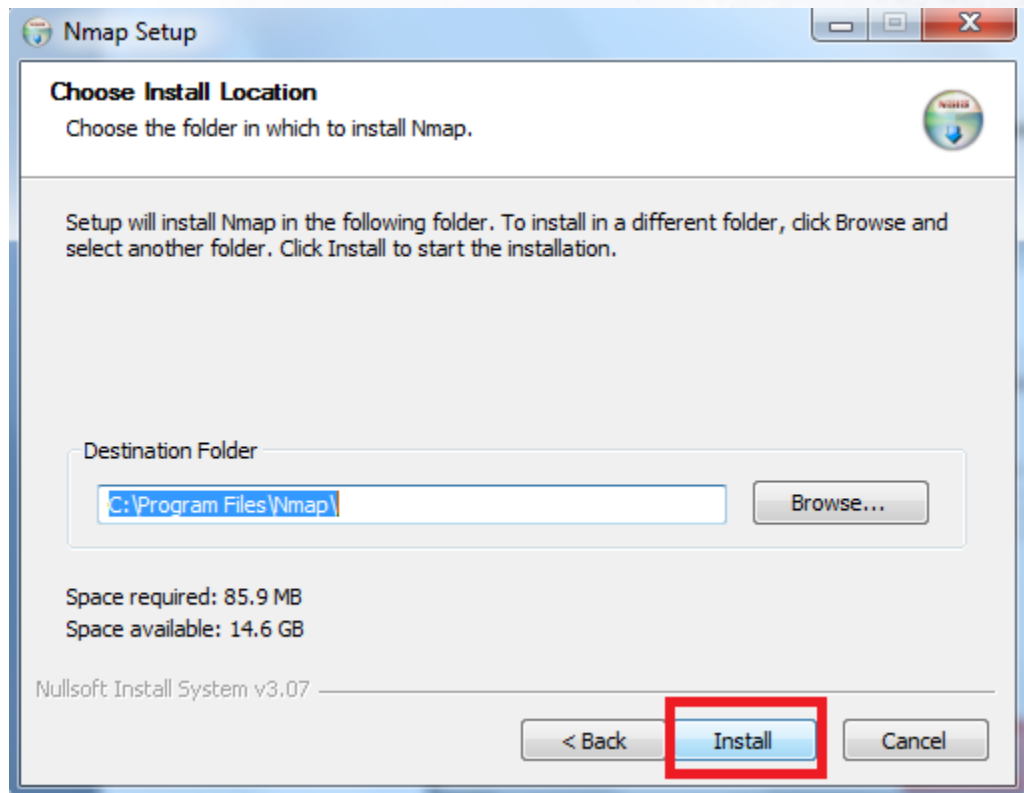


- **Nmap core files includes the Nmap scanning engine**
- **Register Nmap path allows you to execute Nmap from the command line in any directory**
- **Network performance improvements optimization your system for running scans.**
- **Zenmap is a graphical front end for Nmap**
- **Ndiff allows you to compare the results of two Nmap scans.**
- **Ncat allows you to read and write data to network connections from the command line**
- **Nping is a packet generation utility that provides enhancements over the basic ping command.**





```

D:\>nmap [REDACTED]
Nmap 7.93 ( 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 sequentially - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sU: 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)

```

Nmap syntax is the same regardless of the operating system.

```
D:\>nmap -v [REDACTED]  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-31 22:44 Pakistan Standard Time  
Read data files from: C:\Program Files\Nmap  
WARNING: No targets were specified, so 0 hosts scanned.  
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.08 seconds  
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)  
D:\>_
```

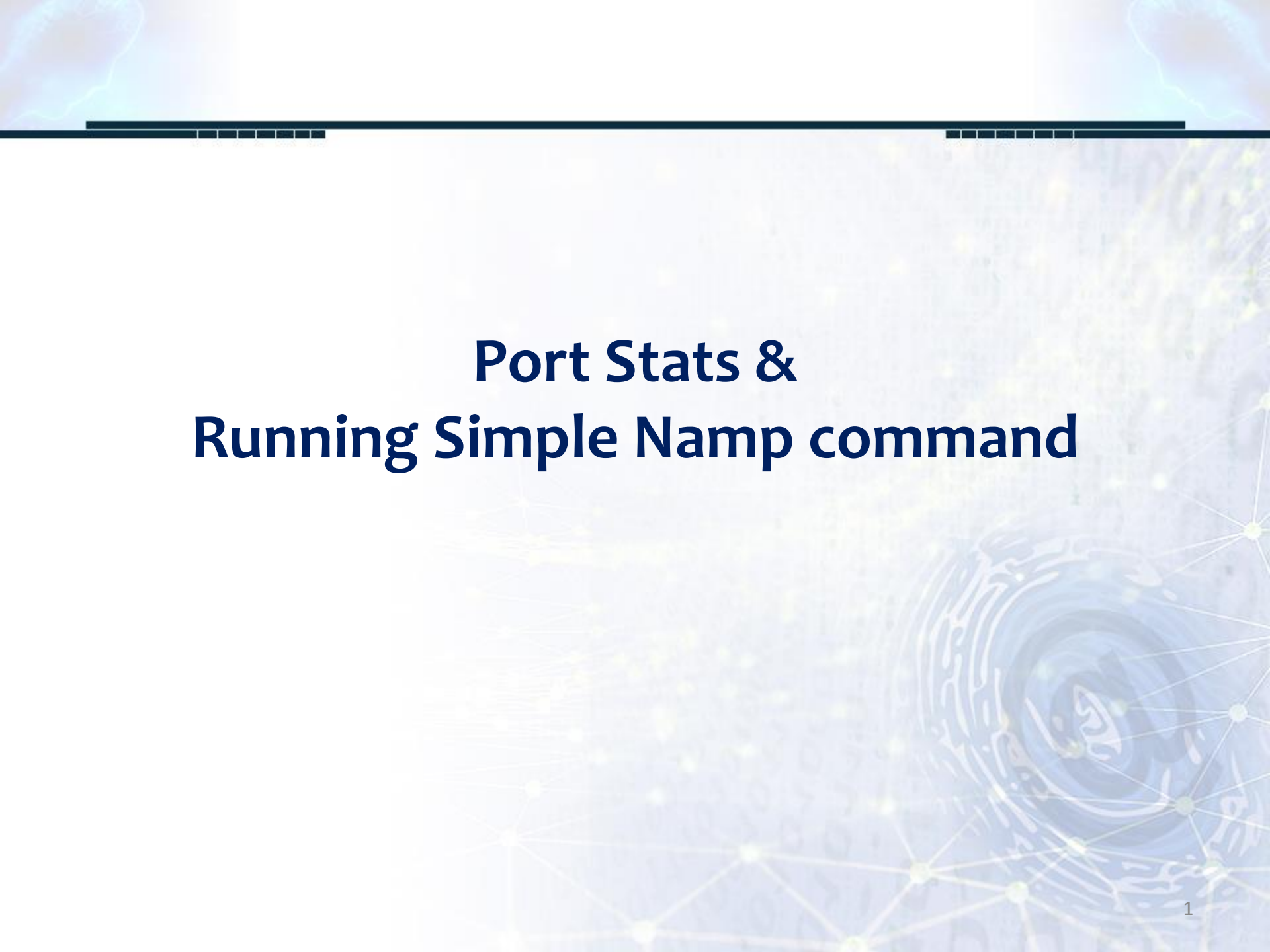
```
D:\>nmap scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-31 22:49 Pakistan Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.34s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 33.13 seconds
D:\>_
```

Use the Snap container manager to install Nmap on Ubuntu and Debian systems.

```
ubuntu@ip-172-31-93-59:~$ sudo snap install nmap
nmap 7.91 from Maximiliano Bertacchini (maxiberta) installed
ubuntu@ip-172-31-93-59:~$ █
```

```
ubuntu@ip-172-31-93-59:~$ sudo snap install nmap
nmap 7.91 from Maximiliano Bertacchini (maxiberta) installed
ubuntu@ip-172-31-93-59:~$ nmap -V
Nmap version 7.91 ( https://nmap.org )
Platform: x86_64-unknown-linux-gnu
Compiled with: liblua-5.3.3 openssl-1.1.1 libssh2-1.8.0 libz-1.2.11 libpcre-8.39 libpcap-1.8.1 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
ubuntu@ip-172-31-93-59:~$
```



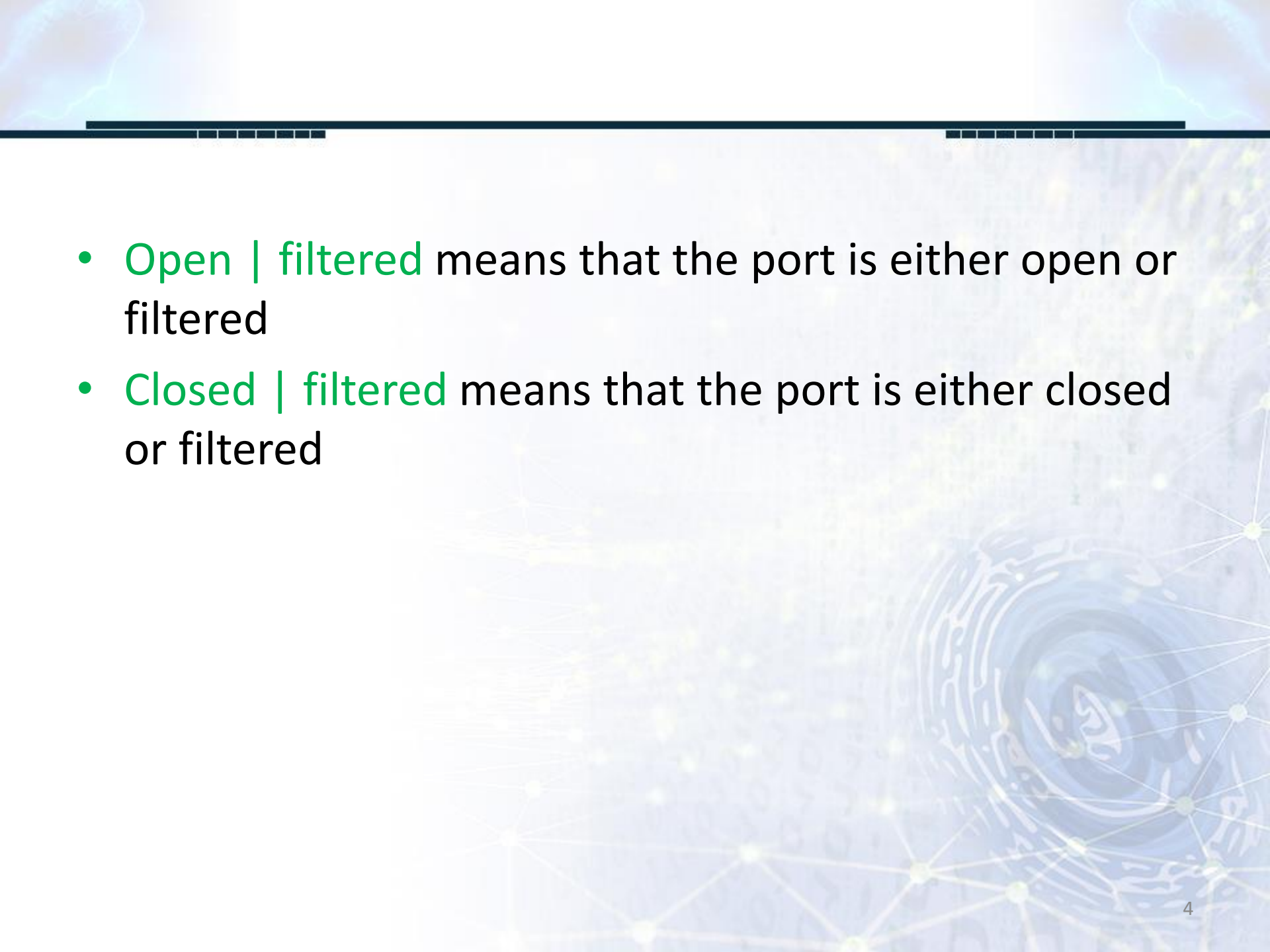
Port Stats & Running Simple Namp command

Port Stats in Nmap

State	Description
open	Accepting connection requests
closed	No service responding to requests
filtered	Blocked by a firewall
unfiltered	Accessible, but scanner was unable to determine whether open or closed

Special cases of port states

- Nmap might be unable to make a definitive statement about the state of the port
- If the Nmap is unsure of the state, it may reports two options.

- 
- **Open | filtered** means that the port is either open or filtered
 - **Closed | filtered** means that the port is either closed or filtered

Scan with DNS

```
[ec2-user@ip-172-31-83-84 ~]$ nmap scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-14 20:30 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.072s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp   open  nping-echo
31337/tcp  open  Elite

Nmap done: 1 IP address (1 host up) scanned in 1.18 seconds
[ec2-user@ip-172-31-83-84 ~]$
```

```
[ec2-user@ip-172-31-83-84 ~]$ nmap scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-14 20:30 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.072s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp   open  nping-echo
31337/tcp  open  Elite

Nmap done: 1 IP address (1 host up) scanned in 1.18 seconds
```

- (Microsoft Windows uses **nslookup**, while Mac OS X and Linux use **dig**.)
- Both perform **DNS queries**, and to test out your DNS configuration.
- determine the **IP address** associated with a **domain name**

```
D:\>nslookup scanme.nmap.org
Server: 192.168.1.1
Address: 192.168.1.11

Non-authoritative answer:
Name: scanme.nmap.org
Addresses: 2600:3c01::f03c:91ff:fe18:bb2f
          45.33.32.156

D:\>nslookup 45.33.32.156
Server: 192.168.1.1
Address: 192.168.1.11

Name: scanme.nmap.org
Address: 45.33.32.156
```

```
[ec2-user@ip-172-31-83-84 ~]$ dig scanme.nmap.org

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.amzn2.5 <<>> scanme.nmap.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15745
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;scanme.nmap.org.                IN      A

;; ANSWER SECTION:
scanme.nmap.org.                103     IN      A      45.33.32.156

;; Query time: 0 msec
;; SERVER: 172.31.0.2#53(172.31.0.2)
;; WHEN: Mon Jun 14 20:30:33 UTC 2021
;; MSG SIZE rcvd: 60
```

Scan with server IP

```
[ec2-user@ip-172-31-83-84 ~]$ nmap 45.33.32.156
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-14 20:31 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.071s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp   open  nping-echo
31337/tcp  open  Elite

Nmap done: 1 IP address (1 host up) scanned in 1.19 seconds
[ec2-user@ip-172-31-83-84 ~]$
```

```
D:\>nmap scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-01 14:53 Pakistan Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.32s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

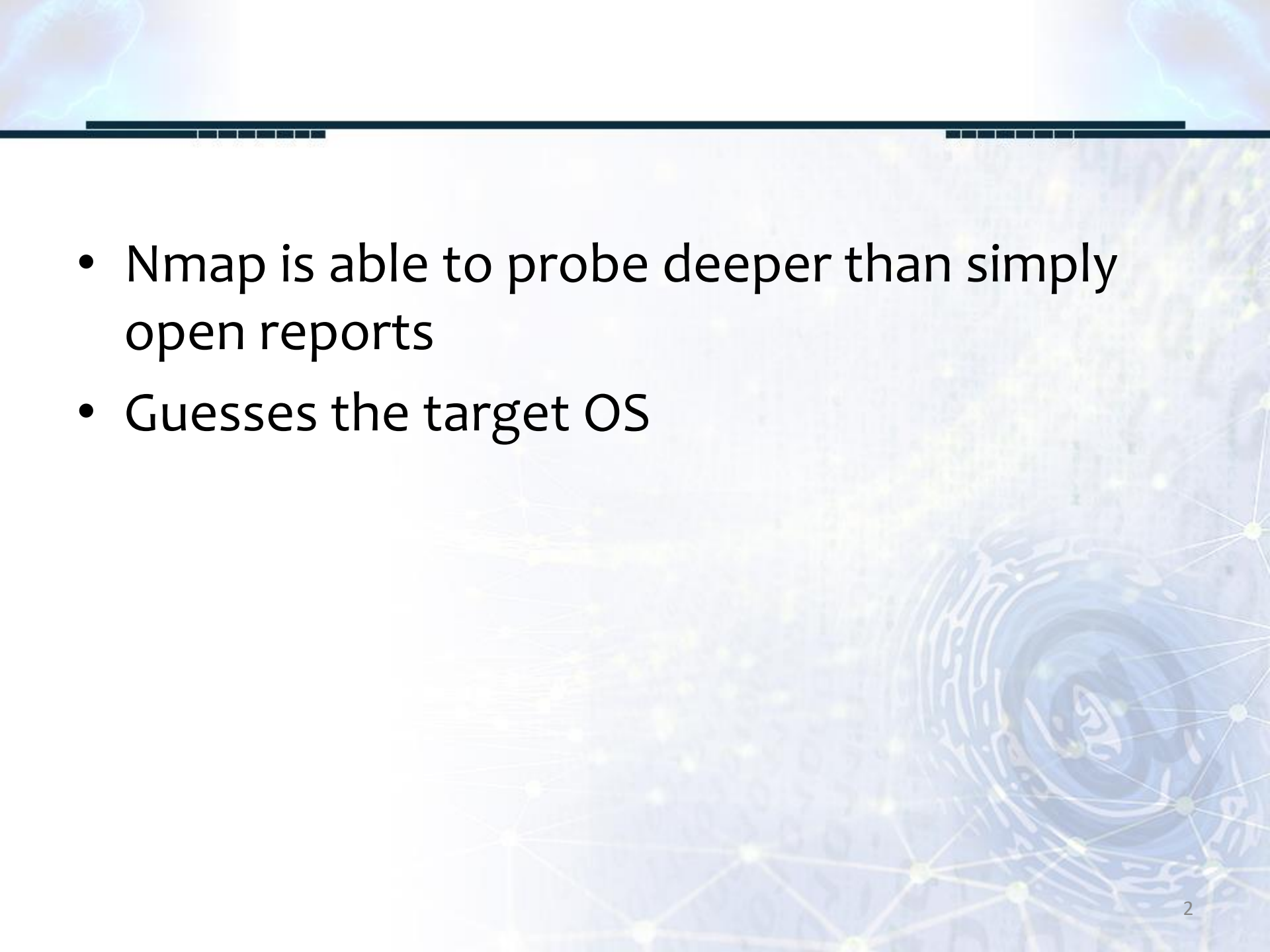
Nmap done: 1 IP address (1 host up) scanned in 34.77 seconds

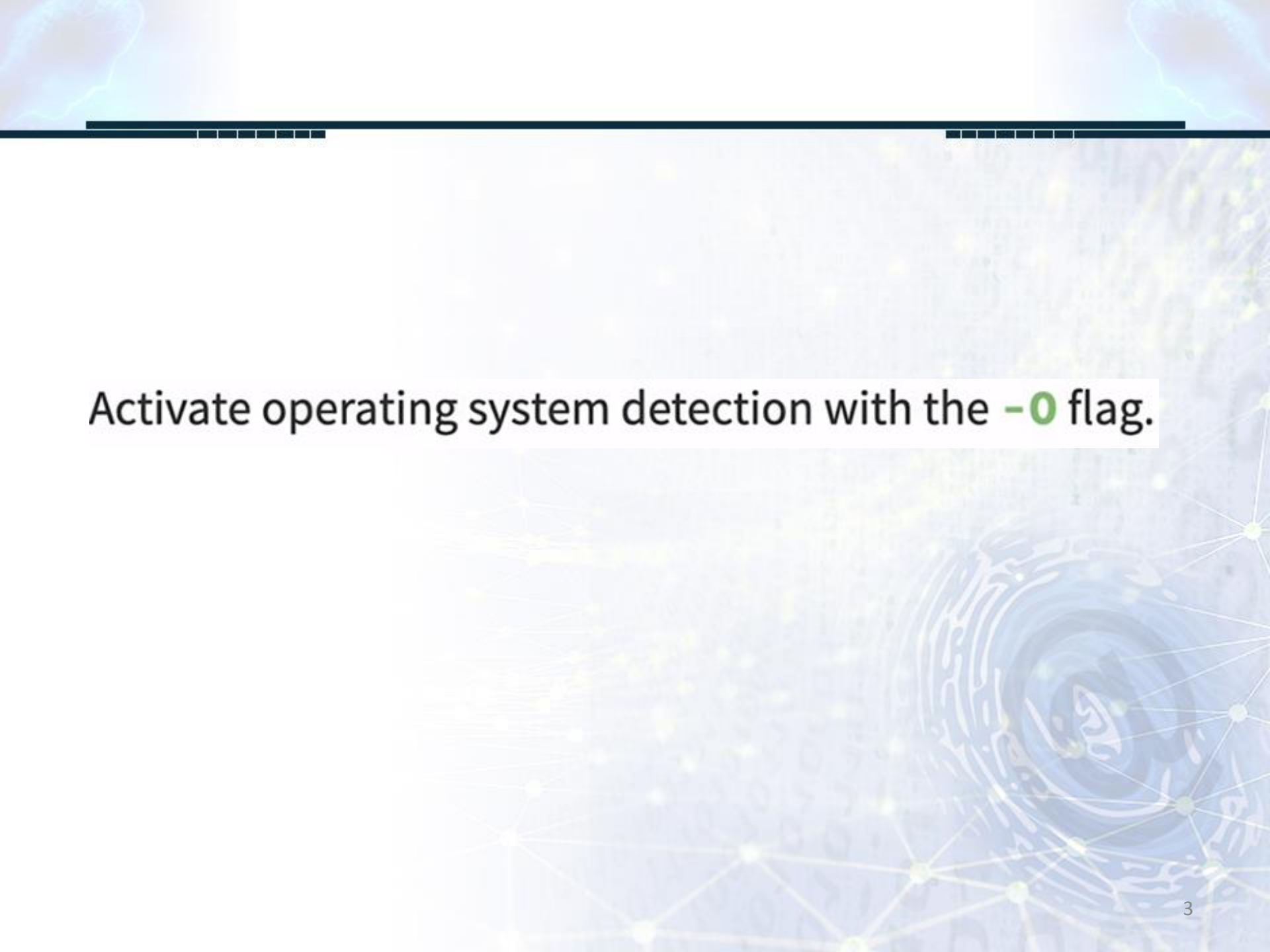
D:\>nmap 45.33.32.156
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-01 15:05 Pakistan Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.34s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 55.42 seconds
```



OS and service Version Detection

- 
- Nmap is able to probe deeper than simply open reports
 - Guesses the target OS



Activate operating system detection with the **-O** flag.

```
Mikes-Mac-mini:~ root# nmap -O scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 15:23 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.080s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    filtered smtp
80/tcp    open  http
135/tcp    filtered msrpc
139/tcp    filtered netbios-ssn
445/tcp    filtered microsoft-ds
9929/tcp   open  nping-echo
31337/tcp  open  Elite
Aggressive OS guesses: Linux 2.6.32 (93%), Linux 2.6.32 or 3.10 (93%), Linux 4.4 (92%), Linux 2.6.32 - 2.6.35 (91%), Linux 2.6.32 - 2.6.39 (91%), Linux 4.0 (90%), Linux 5.4 (90%), Linux 3.11 - 4.1 (89%), Linux 3.2 - 3.8 (89%), Linux 2.6.18 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 16 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.54 seconds
```

```
Mikes-Mac-mini:~ root# nmap -O 192.168.1.54 [REDACTED]
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 15:27 EDT
Nmap scan report for 192.168.1.54
Host is up (0.012s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
28201/tcp open  unknown
MAC Address: F0:18:98:5A:B1:A0 (Apple)
Device type: general purpose|media device
Running: Apple OS X 10.11.X, Apple iOS 12.X
OS CPE: cpe:/o:apple:mac_os_x:10.11 cpe:/o:apple:iphone_os:12
OS details: Apple Mac OS X 10.11 (El Capitan) or iOS 12.4 - 13.0 (Darwin 15.6.0 - 19.0.0)
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address_ (1 host up) scanned in 11.98 seconds
```

- **Service version detection**

- Guesses the service versions running on an open port of target system

Activate service version detection with the **-sV** flag.

```
Mikes-Mac-mini:~ root# nmap -sV scanme.nmap.org [REDACTED]
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 15:30 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.089s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered smtp
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
135/tcp    filtered msrpc
139/tcp    filtered netbios-ssn
445/tcp    filtered microsoft-ds
9929/tcp   open  nping-echo    Nping echo
31337/tcp  open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

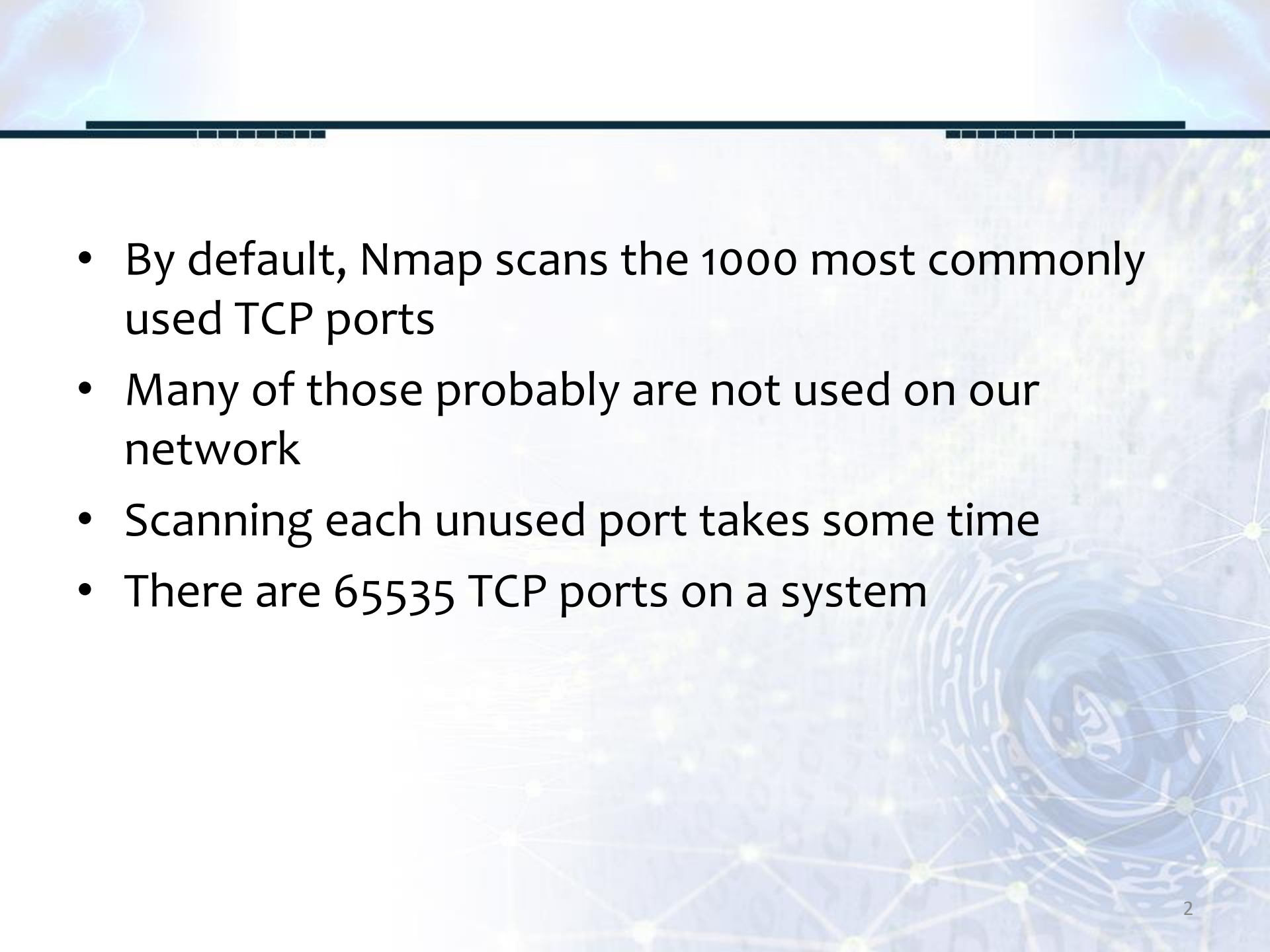
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.80 seconds
```

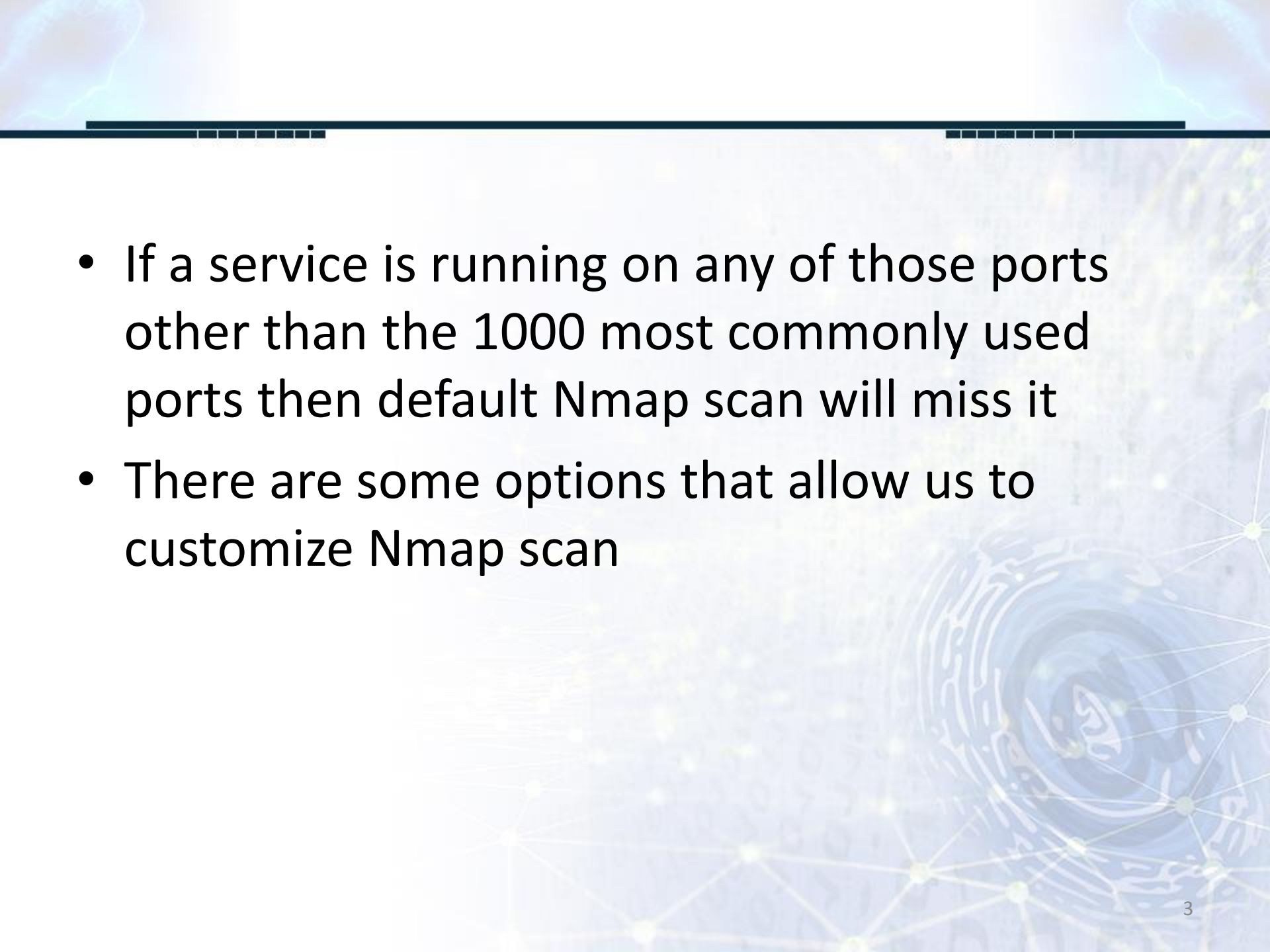
```
Mikes-Mac-mini:~ root# nmap -sV scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 15:30 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.089s latency).
Not shown: 992 closed ports
PORT      STATE      SERVICE      VERSION
22/tcp    open      ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered  smtp
80/tcp    open      http         Apache httpd 2.4.7 ((Ubuntu))
135/tcp    filtered  msrpc
139/tcp    filtered  netbios-ssn
445/tcp    filtered  microsoft-ds
9929/tcp   open      nping-echo   Nping echo
31337/tcp  open      tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.80 seconds
```



Port selection Controls scan behavior

- 
- By default, Nmap scans the 1000 most commonly used TCP ports
 - Many of those probably are not used on our network
 - Scanning each unused port takes some time
 - There are 65535 TCP ports on a system

- 
- If a service is running on any of those ports other than the 1000 most commonly used ports then default Nmap scan will miss it
 - There are some options that allow us to customize Nmap scan

The **-F** flag requests a fast scan of the top 100 TCP ports.

```
recording@Mikes-Mac-mini ~ % nmap 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 14:11 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0074s latency).
Not shown: 994 closed ports
PORT      STATE      SERVICE
21/tcp    filtered  ftp
53/tcp    open       domain
80/tcp    open       http
443/tcp   open       https
3333/tcp  open       dec-notes
5555/tcp  open       freeciv

Nmap done: 1 IP address (1 host up) scanned in 2.98 seconds
```

```
recording@Mikes-Mac-mini ~ % nmap 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 14:11 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0074s latency).
Not shown: 994 closed ports
PORT      STATE      SERVICE
21/tcp    filtered  ftp
53/tcp    open       domain
80/tcp    open       http
443/tcp   open       https
3333/tcp  open       dec-notes
5555/tcp  open       freeciv
```

```
Nmap done: 1 IP address (1 host up) scanned in 2.98 seconds
recording@Mikes-Mac-mini ~ % nmap -F 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 14:11 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0090s latency).
Not shown: 96 closed ports
PORT      STATE      SERVICE
21/tcp    filtered  ftp
53/tcp    open       domain
80/tcp    open       http
443/tcp   open       https
```

```
Nmap done: 1 IP address (1 host up) scanned in 1.44 seconds
```

```
recording@Mikes-Mac-mini ~ % nmap 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 14:11 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0074s latency).
```

```
Not shown: 994 closed ports
```

PORT	STATE	SERVICE
21/tcp	filtered	ftp
53/tcp	open	domain
80/tcp	open	http
443/tcp	open	https
3333/tcp	open	dec-notes
5555/tcp	open	freeciv

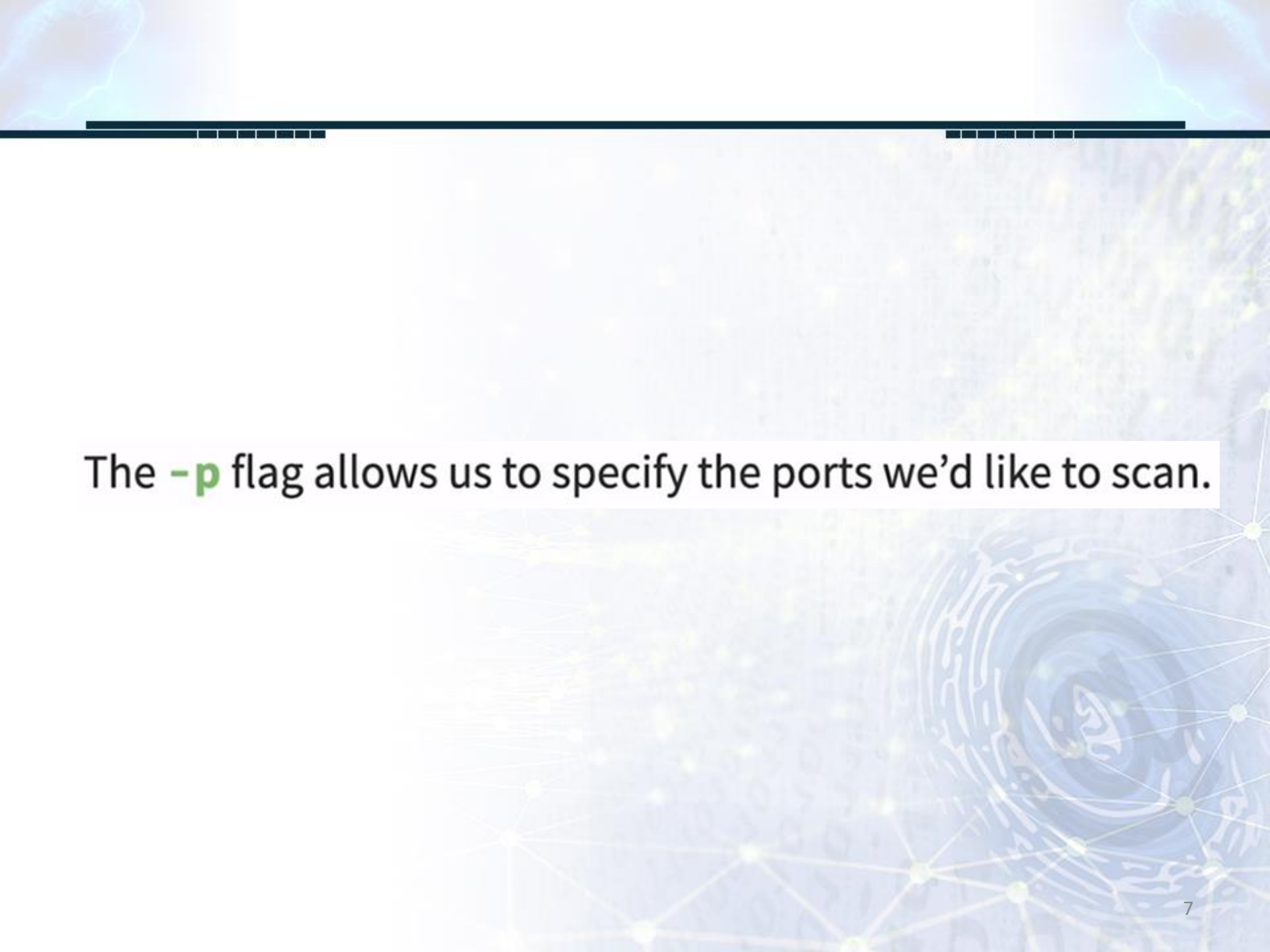
```
Nmap done: 1 IP address (1 host up) scanned in 2.98 seconds
```

```
recording@Mikes-Mac-mini ~ % nmap -F 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 14:11 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0090s latency).
```

```
Not shown: 96 closed ports
```

PORT	STATE	SERVICE
21/tcp	filtered	ftp
53/tcp	open	domain
80/tcp	open	http
443/tcp	open	https

```
Nmap done: 1 IP address (1 host up) scanned in 1.44 seconds
```



The **-p** flag allows us to specify the ports we'd like to scan.

```
recording@Mikes-Mac-mini ~ % nmap -p 80 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 14:12 EDT
Nmap scan report for 192.168.1.1
Host is up (0.015s latency).
```

```
PORT      STATE SERVICE
80/tcp    open  http
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

```
recording@Mikes-Mac-mini ~ % nmap -p 80,443 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 14:13 EDT
Nmap scan report for 192.168.1.1
Host is up (0.012s latency).
```

PORT	STATE	SERVICE
80/tcp	open	http
443/tcp	open	https

```
Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

Scan Service

```
recording@Mikes-Mac-mini ~ % nmap -p http,https 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 14:14 EDT
Nmap scan report for 192.168.1.1
Host is up (0.013s latency).
```

PORT	STATE	SERVICE
80/tcp	open	http
443/tcp	open	https
8008/tcp	closed	http

```
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

```
recording@Mikes-Mac-mini ~ % nmap -p 80 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 14:12 EDT
Nmap scan report for 192.168.1.1
Host is up (0.015s latency).
```

PORT	STATE	SERVICE
80/tcp	open	http

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds

```
recording@Mikes-Mac-mini ~ % nmap -p 80,443 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 14:13 EDT
Nmap scan report for 192.168.1.1
Host is up (0.012s latency).
```

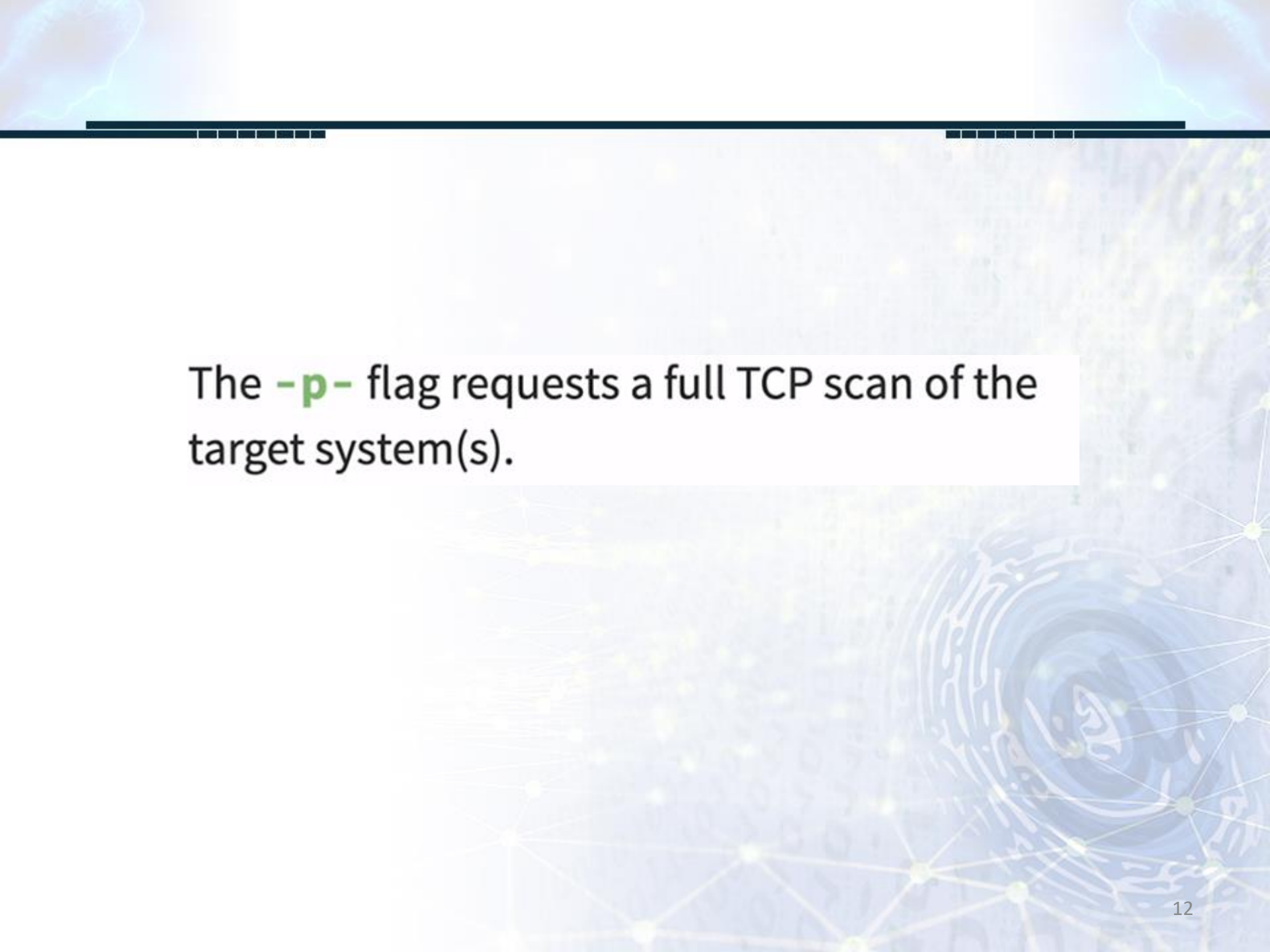
PORT	STATE	SERVICE
80/tcp	open	http
443/tcp	open	https

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds

```
recording@Mikes-Mac-mini ~ % nmap -p http,https 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 14:14 EDT
Nmap scan report for 192.168.1.1
Host is up (0.013s latency).
```

PORT	STATE	SERVICE
80/tcp	open	http
443/tcp	open	https
8008/tcp	closed	http

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds



The **-p-** flag requests a full TCP scan of the target system(s).

```
recording@Mikes-Mac-mini ~ % nmap -p- 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 14:15 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0078s latency).
Not shown: 65528 closed ports
PORT      STATE      SERVICE
21/tcp    filtered  ftp
53/tcp    open       domain
80/tcp    open       http
443/tcp   open       https
3333/tcp  open       dec-notes
5555/tcp  open       freeciv
7272/tcp  open       watchme-7272

Nmap done: 1 IP address (1 host up) scanned in 121.38 seconds
```

Specifying Scan Targets

- Single IP address or DNS name
- List of addresses and names, separated by spaces
- Range of IP addresses
- Subnet mask
- File containing addresses and names
- Scan IPv6

```
recording@Mikes-Mac-mini ~ % nmap 192.168.1.1 192.168.1.3 192.168.1.6 [REDACTED]
```

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 13:38 EDT
```

```
Nmap scan report for 192.168.1.1
```

```
Host is up (0.0081s latency).
```

```
Not shown: 994 closed ports
```

PORT	STATE	SERVICE
21/tcp	filtered	ftp
53/tcp	open	domain
80/tcp	open	http
443/tcp	open	https
3333/tcp	open	dec-notes
5555/tcp	open	freeciv

```
Nmap scan report for 192.168.1.3
```

```
Host is up (0.012s latency).
```

```
Not shown: 996 closed ports
```

PORT	STATE	SERVICE
23/tcp	open	telnet
80/tcp	open	http
111/tcp	open	rpcbind
8080/tcp	open	http-proxy

```
Nmap scan report for 192.168.1.6
```

```
Host is up (0.0090s latency).
```

```
Not shown: 998 closed ports
```

PORT	STATE	SERVICE
80/tcp	open	http
443/tcp	open	https

```
Nmap done: 3 IP addresses (3 hosts up) scanned in 7.16 seconds
```

```
recording@Mikes-Mac-mini ~ % █
```

```
recording@Mikes-Mac-mini ~ % nmap 192.168.1.1,3,6 [REDACTED]
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 13:39 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0087s latency).
Not shown: 994 closed ports
PORT      STATE      SERVICE
21/tcp    filtered  ftp
53/tcp    open       domain
80/tcp    open       http
443/tcp   open       https
3333/tcp  open       dec-notes
5555/tcp  open       freeciv

Nmap scan report for 192.168.1.3
Host is up (0.0087s latency).
Not shown: 996 closed ports
PORT      STATE      SERVICE
23/tcp    open       telnet
80/tcp    open       http
111/tcp   open       rpcbind
8080/tcp  open       http-proxy

Nmap scan report for 192.168.1.6
Host is up (0.014s latency).
Not shown: 998 closed ports
PORT      STATE      SERVICE
80/tcp    open       http
443/tcp   open       https

Nmap done: 3 IP addresses (3 hosts up) scanned in 7.75 seconds
```

```
recording@Mikes-Mac-mini ~ % nmap 192.168.1.1-6
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 13:40 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0083s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
21/tcp    filtered ftp
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
3333/tcp  open  dec-notes
5555/tcp  open  freeciv

Nmap scan report for 192.168.1.3
Host is up (0.011s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
80/tcp    open  http
111/tcp   open  rpcbind
8080/tcp  open  http-proxy

Nmap scan report for 192.168.1.4
Host is up (0.011s latency).
All 1000 scanned ports on 192.168.1.4 are closed

Nmap scan report for 192.168.1.5
Host is up (0.013s latency).
All 1000 scanned ports on 192.168.1.5 are closed

Nmap scan report for 192.168.1.6
Host is up (0.019s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 6 IP addresses (5 hosts up) scanned in 16.02 seconds
```

Scan subnet

```
recording@Mikes-Mac-mini ~ % nmap 192.168.1.0/29
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 13:41 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0080s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
21/tcp    filtered ftp
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
3333/tcp  open  dec-notes
5555/tcp  open  freeciv

Nmap scan report for 192.168.1.3
Host is up (0.010s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
80/tcp    open  http
111/tcp   open  rpcbind
8080/tcp  open  http-proxy

Nmap scan report for 192.168.1.4
Host is up (0.014s latency).
All 1000 scanned ports on 192.168.1.4 are closed

Nmap scan report for 192.168.1.5
Host is up (0.014s latency).
All 1000 scanned ports on 192.168.1.5 are closed

Nmap scan report for 192.168.1.6
Host is up (0.015s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap scan report for 192.168.1.7
Host is up (0.014s latency).
All 1000 scanned ports on 192.168.1.7 are closed

Nmap done: 8 IP addresses (6 hosts up) scanned in 14.75 seconds
```

Scan from file

```
recording@Mikes-Mac-mini ~ % cat scan_targets.txt
```

```
192.168.1.1
```

```
192.168.1.3
```

```
192.168.1.6
```

```
192.168.1.8
```

```
192.168.1.38
```

```
192.168.1.40
```

```
192.168.1.42
```

```
recording@Mikes-Mac-mini ~ % nmap -iL scan_targets.txt
```

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 13:42 EDT
```

```
Host is up (0.012s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
```

```
Nmap scan report for 192.168.1.8
Host is up (0.0098s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
5555/tcp   open  freeciv
8009/tcp   open  ajp13
```

```
Nmap scan report for 192.168.1.38
Host is up (0.011s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
80/tcp    open  http
443/tcp   open  https
515/tcp   open  printer
631/tcp   open  ipp
9100/tcp  open  jetdirect
```

```
Nmap scan report for 192.168.1.40
Host is up (0.013s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
62078/tcp  open  iphone-sync
```

```
Nmap scan report for 192.168.1.42
Host is up (0.010s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
5000/tcp   open  upnp
7000/tcp   open  afs3-fileserver
7100/tcp   open  font-service
49152/tcp  open  unknown
49153/tcp  open  unknown
62078/tcp  open  iphone-sync
```

```
Nmap done: 7 IP addresses (7 hosts up) scanned in 27.92 seconds
```

Scan from file on windows

```
D:\>type scanme.txt
```

```
45.33.32.156
```

```
18.213.119.84
```

```
D:\>more scanme.txt
```

```
45.33.32.156
```

```
18.213.119.84
```

Nslookup

```
D:\>nslookup scanme.nmap.org
Server:    Unknown
Address:   192.168.242.235

Non-authoritative answer:
Name:      scanme.nmap.org
Addresses: 2600:3c01::f03c:91ff:fe18:bb2f
           45.33.32.156
```

```
D:\>nslookup scan1.certmike.com
Server:    Unknown
Address:   192.168.242.235

Non-authoritative answer:
Name:      scan1.certmike.com
Address:   18.213.119.84
```

```
D:\>nmap -iL scanme.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-02 10:19 Pakistan Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.39s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
9929/tcp  open  nping-echo

Nmap scan report for ec2-18-213-119-84.compute-1.amazonaws.com (18.213.119.84)
Host is up (0.23s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 2 IP addresses (2 hosts up) scanned in 102.17 seconds
D:\>_
```

Scanning IPv6

Nmap is able to scan IPv6 addresses with the **-6** flag.

```
recording@Mikes-Mac-mini ~ % nmap 2600:1f18:2763:3000:6b7a:868d:b048:78af
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 13:44 EDT
2600:1f18:2763:3000:6b7a:868d:b048:78af looks like an IPv6 target specification -- you have to use the -6 option.
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.08 seconds
recording@Mikes-Mac-mini ~ %
```

```
recording@Mikes-Mac-mini ~ % nmap 2600:1f18:2763:3000:6b7a:868d:b048:78af
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 13:44 EDT
2600:1f18:2763:3000:6b7a:868d:b048:78af looks like an IPv6 target specification -- you have to use the -6 option.
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.08 seconds
recording@Mikes-Mac-mini ~ % nmap -6 2600:1f18:2763:3000:6b7a:868d:b048:78af
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 13:45 EDT
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 0.16 seconds
recording@Mikes-Mac-mini ~ %
```

Scan Shortcut and Disable DNS option

scanning shortcut

- The **-A** flag offers a scanning shortcut that activate several popular options

-A Options

- Remote operating system detection
- Service and version detection
- Traceroute
- Nmap Scripting engine (NSE)

```

Mikes-Mac-mini:~ root# nmap -A -T4 scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 15:33 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.079s latency).
Not shown: 992 closed ports
PORT      STATE      SERVICE      VERSION
22/tcp    open      ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
25/tcp    filtered  smtp
80/tcp    open      http         Apache httpd 2.4.7 ((Ubuntu))
|_ http-favicon: Nmap Project
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Go ahead and ScanMe!
135/tcp   filtered  msrpc
139/tcp   filtered  netbios-ssn
445/tcp   filtered  microsoft-ds
9929/tcp  open      nping-echo   Nping echo
31337/tcp open      tcpwrapped
Aggressive OS guesses: Linux 2.6.32 (93%), Linux 2.6.32 or 3.10 (93%), Linux 4.4 (93%), Linux 2.6.32 - 2.6.35 (91%), Linux 2.6.32 - 3.0 (90%), Linux 3.11 - 4.1 (89%), Linux 3.2 - 3.8 (89%), Linux 5.0 - 5.4 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 16 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 5900/tcp)
HOP RTT      ADDRESS
1   8.82 ms   192.168.1.1
2   12.34 ms  10.0.0.1
3   30.27 ms  96.120.26.197
4   30.27 ms  96.110.154.133
5   21.36 ms  68.87.231.137
6   30.29 ms  be-167-ar01.area4.il.chicagoc.comcast.net (162.151.144.101)
7   31.34 ms  24.153.89.45
8   31.33 ms  be-32241-cs04.350ecermak.il.ibone.comcast.net (96.110.40.61)

```

```

Mikes-Mac-mini:~ root# nmap -A -T4 scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 15:33 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.079s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE          VERSION
22/tcp    open  ssh              OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
25/tcp    filtered smtp
80/tcp    open  http             Apache httpd 2.4.7 ((Ubuntu))
|_ http-favicon: Nmap Project
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Go ahead and ScanMe!
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open  nping-echo       Nping echo
31337/tcp open  tcpwrapped
Aggressive OS guesses: Linux 2.6.32 (93%), Linux 2.6.32 or 3.10 (93%), Linux 4.4 (93%), Linux 2.6.32 - 2.6.35 (91%), Linux 4.0
%), Linux 2.6.32 - 3.0 (90%), Linux 3.11 - 4.1 (89%), Linux 3.2 - 3.8 (89%), Linux 5.0 - 5.4 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 16 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 5900/tcp)
HOP RTT      ADDRESS
1   8.82 ms  192.168.1.1
2   12.34 ms 10.0.0.1
3   30.27 ms 96.120.26.197

```

```
Mikes-Mac-mini:~ root# nmap -A -T4 scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 15:33 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
```

Host is up (0.079s latency).

Not shown: 992 closed ports

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)

```
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
```

Namp Scrpiting engine that retrieves the SSH key as presented by the host

```
25/tcp    filtered smtp
80/tcp    open      http        Apache httpd 2.4.7 ((Ubuntu))
```

|_http-favicon: Nmap Project

|_http-server-header: Apache/2.4.7 (Ubuntu)

|_http-title: Go ahead and ScanMe!

135/tcp filtered msrpc

139/tcp filtered netbios-ssn

445/tcp filtered microsoft-ds

9929/tcp open nping-echo Nping echo

31337/tcp open tcpwrapped

Aggressive OS guesses: Linux 2.6.32 (93%), Linux 2.6.32 or 3.10 (93%), Linux 4.4 (93%), Linux 2.6.32 - 2.6.35 (91%), Linux 3.0 (90%), Linux 2.6.32 - 3.0 (90%), Linux 3.11 - 4.1 (89%), Linux 3.2 - 3.8 (89%), Linux 5.0 - 5.4 (89%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 16 hops

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 5900/tcp)

HOP	RTT	ADDRESS
1	8.82 ms	192.168.1.1
2	12.34 ms	10.0.0.1
3	20.27 ms	10.128.0.1

1 8.82 ms 192.168.1.1

2 12.34 ms 10.0.0.1

3 20.27 ms 10.128.0.1

```

Mikes-Mac-mini:~ root# nmap -A -T4 scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 15:33 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.079s latency).
Not shown: 992 closed ports
PORT      STATE      SERVICE      VERSION
22/tcp    open      ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256  96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256  33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
25/tcp    filtered  smtp
80/tcp    open      http         Apache httpd 2.4.7 ((Ubuntu))
|_ http-favicon: Nmap Project
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Go ahead and ScanMe!
135/tcp   filtered  msrpc
139/tcp   filtered  netbios-ssn
445/tcp   filtered  microsoft-ds
9929/tcp  open      nping-echo   Nping echo
31337/tcp open      tcpwrapped
Aggressive OS guesses: Linux 2.6.32 (93%), Linux 2.6.32 or 3.10 (93%), Linux 4.4 (93%), Linux 2.6.32 (93%), Linux 2.6.32 - 3.0 (90%), Linux 3.11 - 4.1 (89%), Linux 3.2 - 3.8 (89%), Linux 5.0 - 5.4 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 16 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 5900/tcp)
HOP RTT      ADDRESS
1   8.82 ms  192.168.1.1
2   12.34 ms 10.0.0.1
3   30.27 ms 96.120.26.197

```

```

25/tcp    filtered smtp
80/tcp    open      http          Apache httpd 2.4.7 ((Ubuntu))
|_http-favicon: Nmap Project
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
135/tcp    filtered msrpc
139/tcp    filtered netbios-ssn
445/tcp    filtered microsoft-ds
9929/tcp   open      nping-echo    Nping echo
31337/tcp  open      tcpwrapped
Aggressive OS guesses: Linux 2.6.32 (93%), Linux 2.6.32 or 3.10 (93%), Linux 4.4 (93%), Linux 2.6.32 - :
%), Linux 2.6.32 - 3.0 (90%), Linux 3.11 - 4.1 (89%), Linux 3.2 - 3.8 (89%), Linux 5.0 - 5.4 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 16 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

TRACEROUTE (using port 5900/tcp)

HOP	RTT	ADDRESS
1	8.82 ms	192.168.1.1
2	12.34 ms	10.0.0.1
3	30.27 ms	96.120.26.197
4	30.27 ms	96.110.154.133
5	21.36 ms	68.87.231.137
6	30.29 ms	be-167-ar01.area4.il.chicago.comcast.net (162.151.144.101)
7	31.34 ms	24.153.89.45
8	31.33 ms	be-32241-cs04.350ecermak.il.ibone.comcast.net (96.110.40.61)
9	33.63 ms	be-2211-pe11.350ecermak.il.ibone.comcast.net (96.110.33.198)
10	27.18 ms	ae-3.r08.chcgil09.us.bb.gin.ntt.net (129.250.8.65)
11	31.36 ms	ae-4.r23.chcgil09.us.bb.gin.ntt.net (129.250.2.205)
12	96.78 ms	ae-1.r24.snjsca04.us.bb.gin.ntt.net (129.250.5.17)
13	96.79 ms	ae-40.r02.snjsca04.us.bb.gin.ntt.net (129.250.3.121)
14	96.79 ms	ce-0-18-0-1.r02.snjsca04.us.ce.gin.ntt.net (192.80.17.170)
15	96.79 ms	if-1-4.csw6-fnc1.linode.com (173.230.159.83)
16	96.81 ms	scanme.nmap.org (45.33.32.156)

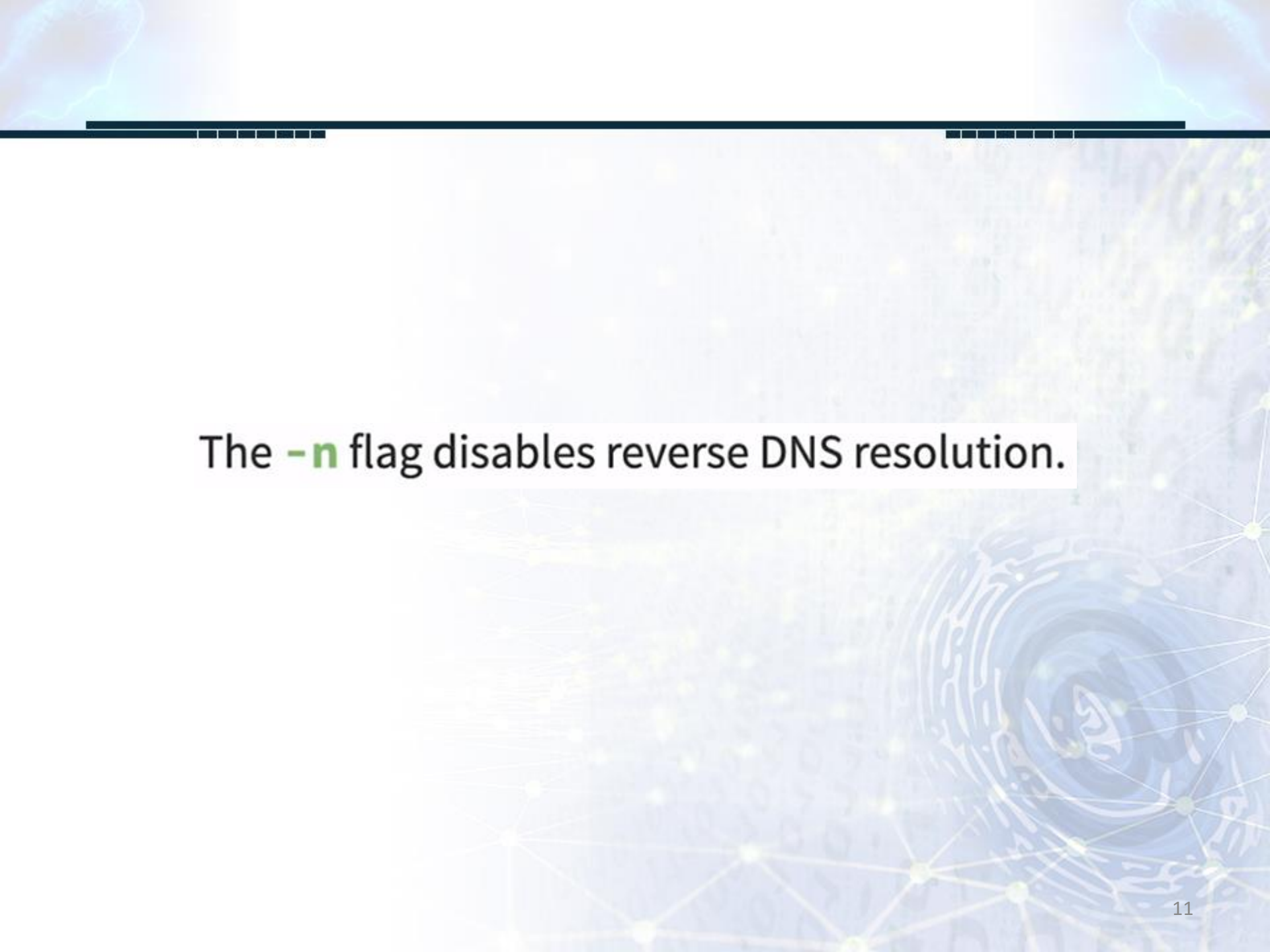
OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 20.98 seconds

nikto -h 192.168.1.1 -u root# ■

- **DNS Resolution**

DNS resolution

- Adds information, but consumes time
- By default, Nmap perform DNS resolution to identify the names of any systems that are scanned by the IP addresses



The **-n** flag disables reverse DNS resolution.

```
recording@Mikes-Mac-mini ~ % nmap 45.33.32.156 [REDACTED]
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 13:56 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.077s latency).
Not shown: 992 closed ports
PORT      STATE      SERVICE
22/tcp    open       ssh
25/tcp    filtered   smtp
80/tcp    open       http
135/tcp    filtered   msrpc
139/tcp    filtered   netbios-ssn
445/tcp    filtered   microsoft-ds
9929/tcp   open       nping-echo
31337/tcp  open       Elite

Nmap done: 1 IP address (1 host up) scanned in 17.09 seconds
```

```
recording@Mikes-Mac-mini ~ % nmap 45.33.32.156
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 13:56 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.077s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    filtered smtp
80/tcp    open  http
135/tcp    filtered msrpc
139/tcp    filtered netbios-ssn
445/tcp    filtered microsoft-ds
9929/tcp   open  nping-echo
31337/tcp  open  Elite
```

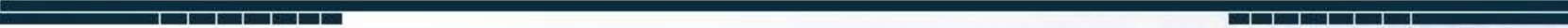
```
Nmap done: 1 IP address (1 host up) scanned in 17.09 seconds
```

```
recording@Mikes-Mac-mini ~ % nmap -n 45.33.32.156
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 13:57 EDT
Nmap scan report for 45.33.32.156
Host is up (0.079s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    filtered smtp
80/tcp    open  http
135/tcp    filtered msrpc
139/tcp    filtered netbios-ssn
445/tcp    filtered microsoft-ds
9929/tcp   open  nping-echo
31337/tcp  open  Elite
```

```
Nmap done: 1 IP address (1 host up) scanned in 16.89 seconds
```

Zenmap

<https://nmap.org/book/zenmap-results.html>

- 
- Zenmap is the official graphical user interface (GUI) for the Nmap Security Scanner.
 - Easy for beginners to use while providing advanced features for experienced Nmap users.

Zenmap

Scan Tools Profile Help

Target: scanme.nmap.org Profile: Quick traceroute

Command: nmap -sn --traceroute scanme.nmap.org

Hosts Services

OS Host

scanme.nmap.org

www.vu.edu.pk (11)

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sn --traceroute scanme.nmap.org

Starting Nmap 7.93 (<https://nmap.org>) at 2023-04-08 09:50 Pakistan
 Nmap scan report for scanme.nmap.org (45.33.32.156)
 Host is up (0.29s latency).

TRACEROUTE (using proto 1/icmp)

HOP	RTT	ADDRESS
1	2.00 ms	192.168.167.96
2	8.00 ms	XiaoQiang (192.168.31.1)
3	12.00 ms	192.168.100.1
4	16.00 ms	123.108.92.20
5	19.00 ms	119.63.130.252
6	22.00 ms	110.93.252.48
7	25.00 ms	110.93.255.168
8	28.00 ms	110.93.255.230
9	141.00 ms	be5685.ccr22.fra06.atlas.cogentco.com (149.14.211.241)
10	144.00 ms	be2845.ccr41.fra03.atlas.cogentco.com (154.54.56.189)
11	150.00 ms	be2813.ccr41.ams03.atlas.cogentco.com (130.117.0.121)
12	245.00 ms	be12194.ccr41.lon13.atlas.cogentco.com (154.54.56.93)
13	244.00 ms	be2317.ccr41.jfk02.atlas.cogentco.com (154.54.30.185)
14	243.00 ms	be2889.ccr21.cle04.atlas.cogentco.com (154.54.47.49)
15	253.00 ms	be2717.ccr41.ord01.atlas.cogentco.com (154.54.6.221)
16	257.00 ms	be2831.ccr21.mci01.atlas.cogentco.com (154.54.42.165)
17	266.00 ms	be3035.ccr21.den01.atlas.cogentco.com (154.54.5.89)

Intense scan

Intense scan plus UDP

Intense scan, all TCP ports

Intense scan, no ping

Ping scan

Quick scan

Quick scan plus

Quick traceroute

Regular scan

Slow comprehensive scan

Zenmap

Scan Tools Profile Help

Target: scanme.nmap.org Profile: Regular scan Scan Cancel

Command: nmap scanme.nmap.org

Hosts Services

Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

- scanme.nmap.org
- www.vu.edu.pk (11)

nmap scanme.nmap.org

Starting Nmap 7.93 (<https://nmap.org>) at 2023-04-08 09:54 Pakistan Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.30s latency).
Not shown: 997 filtered tcp ports (no-response)

PORT	STATE	SERVICE
80/tcp	open	http
9929/tcp	open	nping-echo
31337/tcp	open	Elite

Nmap done: 1 IP address (1 host up) scanned in 20.49 seconds

Zenmap

Scan Tools Profile Help

Target: Profile:

Command:

Hosts Services

OS Host

scanme.nmap.org | www.vu.edu.pk (11)

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sn --traceroute scanme.nmap.org

Starting Nmap 7.93 (<https://nmap.org>) at 2023-04-08 09:50 Pakistan Standard Time
 Nmap scan report for scanme.nmap.org (45.33.32.156)
 Host is up (0.29s latency).

TRACEROUTE (using proto 1/icmp)

HOP	RTT	ADDRESS
1	2.00 ms	192.168.167.96
2	8.00 ms	XiaoQiang (192.168.31.1)
3	12.00 ms	192.168.100.1
4	16.00 ms	123.108.92.20
5	19.00 ms	119.63.130.252
6	22.00 ms	110.93.252.48
7	25.00 ms	110.93.255.168
8	28.00 ms	110.93.255.230
9	141.00 ms	be5685.rcr22.fra06.atlas.cogentco.com (149.14.211.241)
10	144.00 ms	be2845.ccr41.fra03.atlas.cogentco.com (154.54.56.189)
11	150.00 ms	be2813.ccr41.ams03.atlas.cogentco.com (130.117.0.121)
12	245.00 ms	be12194.ccr41.lon13.atlas.cogentco.com (154.54.56.93)
13	244.00 ms	be2317.ccr41.jfk02.atlas.cogentco.com (154.54.30.185)
14	243.00 ms	be2889.ccr21.cle04.atlas.cogentco.com (154.54.47.49)
15	253.00 ms	be2717.ccr41.ord01.atlas.cogentco.com (154.54.6.221)
16	257.00 ms	be2831.ccr21.mci01.atlas.cogentco.com (154.54.42.165)
17	266.00 ms	be3035.ccr21.den01.atlas.cogentco.com (154.54.5.89)
18	277.00 ms	be3037.ccr21.slc01.atlas.cogentco.com (154.54.41.145)
19	294.00 ms	be3109.ccr21.sfo01.atlas.cogentco.com (154.54.44.137)
20	293.00 ms	be3178.ccr21.sjc01.atlas.cogentco.com (154.54.43.70)
21	295.00 ms	be2063.rcr21.b001848-1.sjc01.atlas.cogentco.com (154.54.1.162)
22	291.00 ms	38.142.11.154
23	307.00 ms	if-1-4.csw5-fnc1.linode.com (173.230.159.81)
24	287.00 ms	scanme.nmap.org (45.33.32.156)

Nmap done: 1 IP address (1 host up) scanned in 15.82 seconds

Zenmap

Scan Tools Profile Help

Target: scanme.nmap.org Profile: Quick scan Scan Cancel

Command: nmap -T4 -F scanme.nmap.org

Hosts Services

OS Host

scanme.nmap.org |

www.vu.edu.pk (11

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -T4 -F scanme.nmap.org

Starting Nmap 7.93 (<https://nmap.org>) at 2023-04-08 10:08 Pakistan Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.29s latency).
Not shown: 99 filtered tcp ports (no-response)
PORT STATE SERVICE
80/tcp open http

Nmap done: 1 IP address (1 host up) scanned in 8.17 seconds

Zenmap

Scan Tools Profile Help

Target: scanme.nmap.org Profile: Intense scan, no ping

Command: nmap -T4 -A -v -Pn scanme.nmap.org

Hosts Services

OS Host

scanme.nmap.org

www.vu.edu.pk (11)

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -T4 -A -v -Pn scanme.nmap.org

Completed Parallel DNS Resolution of 22 hosts: at 10:10, 15.00s elapsed

NSE: Script scanning 45.33.32.156.

Initiating NSE at 10:10

Completed NSE at 10:10, 6.04s elapsed

Initiating NSE at 10:10

Completed NSE at 10:10, 1.31s elapsed

Initiating NSE at 10:10

Completed NSE at 10:10, 0.00s elapsed

Nmap scan report for scanme.nmap.org (45.33.32.156)

Host is up (0.23s latency).

Not shown: 997 filtered tcp ports (no-response)

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	Apache httpd 2.4.7 ((Ubuntu))

|_ http-methods:

|_ Supported Methods: GET HEAD POST OPTIONS

|_ http-title: Go ahead and ScanMe!

|_ http-favicon: Nmap Project

|_ http-server-header: Apache/2.4.7 (Ubuntu)

9929/tcp open nping-echo Nping echo

31337/tcp open tcpwrapped

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Aggressive OS guesses: Linux 2.6.32 (88%), Linux 3.10 (88%), Linux 2.6.18 (88%), Linux 4.15 - 5.6 (87%), Linux 2.6.32 or 3.10 (87%), Linux 2.6.35 (87%), Linux 2.6.39 (87%), Linux 3.10 - 3.12 (87%), Linux 3.4 (87%), Linux 3.5 (87%)

No exact OS matches for host (test conditions non-ideal).

Uptime guess: 40.238 days (since Mon Feb 27 04:27:33 2023)

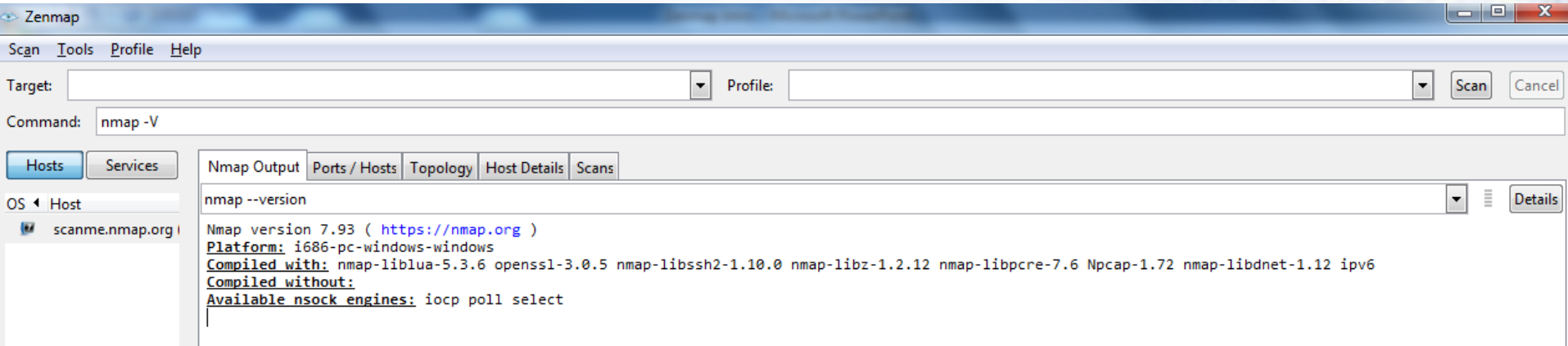
Network Distance: 24 hops

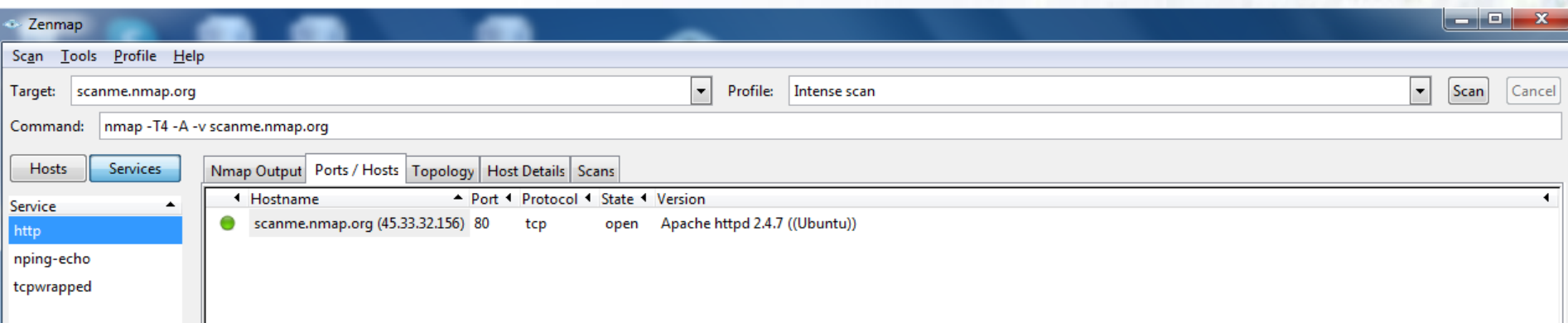
TCP Sequence Prediction: Difficulty=258 (Good luck!)

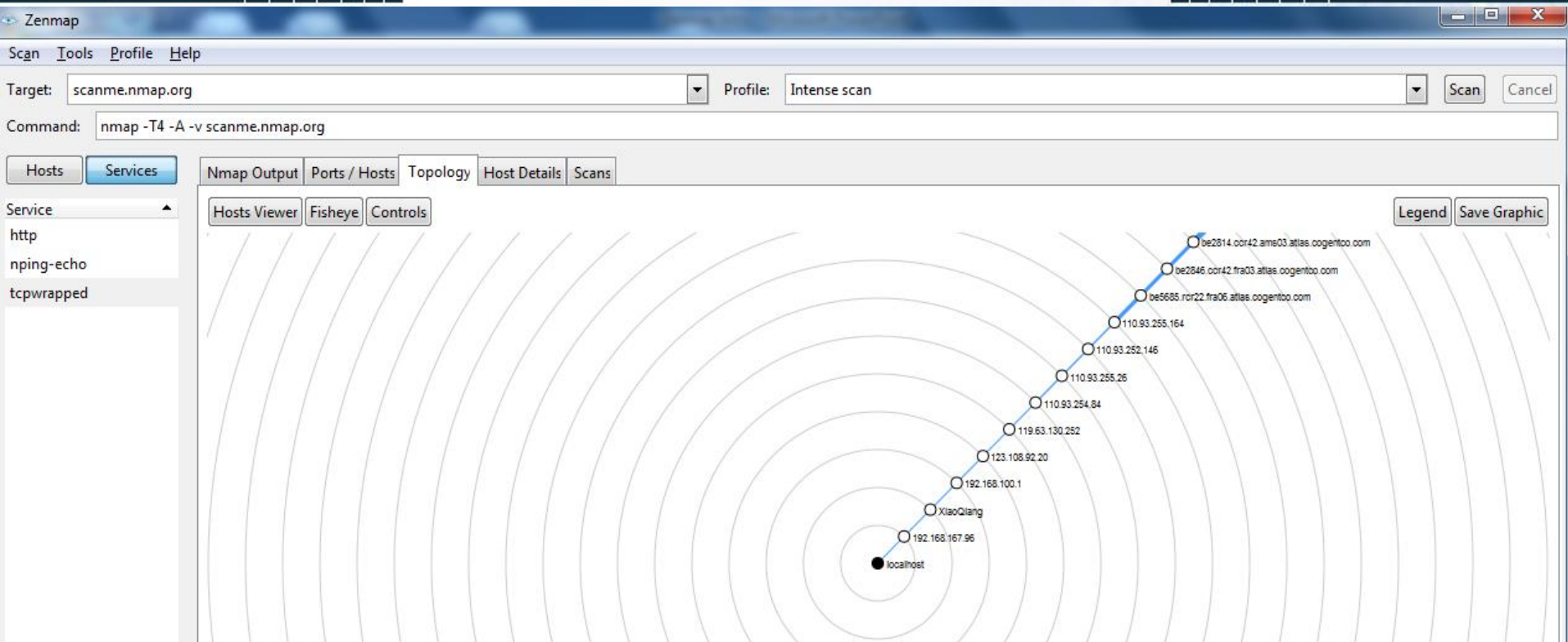
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 80/tcp)

HOP	RTT	ADDRESS
1	3.00 ms	192.168.167.96
2	11.00 ms	XiaoQiang (192.168.31.1)
3	12.00 ms	192.168.100.1
4	12.00 ms	123.108.92.20
5	15.00 ms	119.63.130.252
6	23.00 ms	110.93.252.48







Zenmap

Scan Tools Profile Help

Target: scanme.nmap.org Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v scanme.nmap.org

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

scanme.nmap.org

scanme.nmap.org (45.33.32.156)

- Host Status**
 - State: up
 - Open ports: 3
 - Filtered ports: 997
 - Closed ports: 0
 - Scanned ports: 1000
 - Up time: 3476823
 - Last boot: Mon Feb 27 04:27:33 2023
- Addresses**
 - IPv4: 45.33.32.156
 - IPv6: Not available
 - MAC: Not available
- Hostnames**
 - Name - Type: scanme.nmap.org - user
 - Name - Type: scanme.nmap.org - PTR
- Operating System**
 - Name: Linux 2.6.18
 - Accuracy: 88%
 - Ports used**
 - Port-Protocol-State: 80 - tcp - open
 - Port-Protocol-State: 30700 - udp - closed
 - OS Classes**
- TCP Sequence**

Zenmap

Scan Tools Profile Help

Target: scanme.nmap.org Profile: Intense scan, all TCP ports Scan

Command: nmap -p 1-65535 -T4 -A -v scanme.nmap.org

Hosts Services

OS Host

scanme.nmap.org

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -p 1-65535 -T4 -A -v scanme.nmap.org

Not shown: 65532 filtered tcp ports (no-response)

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	Apache httpd 2.4.7 ((Ubuntu))

|_http-title: Go ahead and ScanMe!
|_http-methods:
|_Supported Methods: GET HEAD POST OPTIONS
|_http-favicon: Nmap Project
|_http-server-header: Apache/2.4.7 (Ubuntu)

9929/tcp open nping-echo Nping echo
31337/tcp open tcpwrapped

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Aggressive OS guesses: Linux 2.6.18 (89%), Linux 2.6.32 (88%), Linux 3.10 (88%), Linux 4.15 - 5.6 (88%), Linux 2.6.32 or 3.10 (88%), Linux 2.6.35 (88%), Linux 3.5 (88%), Linux 4.4 (88%), Linux 4.9 (88%), Synology DiskStation Manager 5.1 (88%)

No exact OS matches for host (test conditions non-ideal).

Uptime guess: 40.252 days (since Mon Feb 27 04:27:34 2023)

Network Distance: 24 hops

TCP Sequence Prediction: Difficulty=256 (Good luck!)

IP ID Sequence Generation: All zeros

TRACEROUTE (using port 80/tcp)

HOP	RTT	ADDRESS
1	12.00 ms	192.168.167.96
2	21.00 ms	XiaoQiang (192.168.31.1)
3	11.00 ms	192.168.100.1
4	12.00 ms	123.108.92.20
5	22.00 ms	119.63.130.252
6	38.00 ms	110.93.252.48
7	32.00 ms	110.93.252.172
8	32.00 ms	110.93.255.164
9	152.00 ms	be5685.rcr22.fra06.atlas.cogentco.com (149.14.211.241)
10	155.00 ms	be2846.ccr42.fra03.atlas.cogentco.com (154.54.37.29)
11	160.00 ms	be2813.ccr41.ams03.atlas.cogentco.com (130.117.0.121)
12	251.00 ms	be12488.ccr42.lon13.atlas.cogentco.com (130.117.51.41)
13	243.00 ms	be2317.ccr41.jfk02.atlas.cogentco.com (154.54.30.185)
14	249.00 ms	be2890.ccr22.cle04.atlas.cogentco.com (154.54.82.245)
15	250.00 ms	be2717.ccr41.ord01.atlas.cogentco.com (154.54.6.221)
16	254.00 ms	be2832.ccr22.mci01.atlas.cogentco.com (154.54.44.169)

Zenmap

Scan Tools Profile Help

Target: scanme.nmap.org Profile: Scan Cancel

Command: nmap -p 80 scanme.nmap.org

Hosts Services

OS Host

scanme.nmap.org

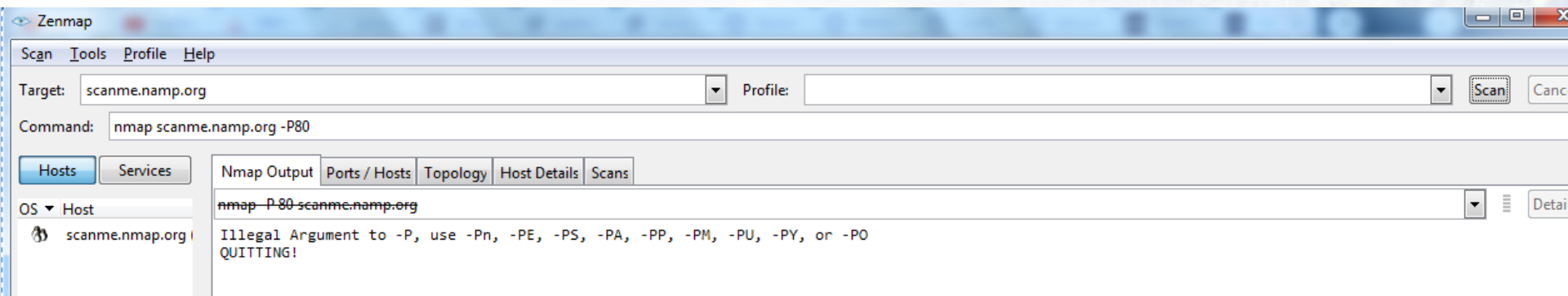
Nmap Output Ports / Hosts Topology Host Details Scans

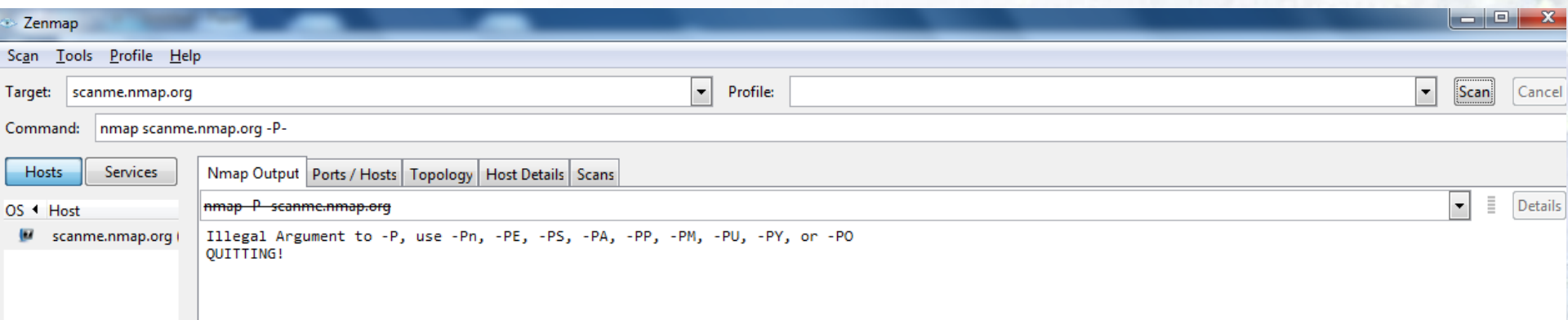
nmap -p 80 scanme.nmap.org

Starting Nmap 7.93 (<https://nmap.org>) at 2023-04-08 10:38 Pakistan Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.41s latency).

PORT	STATE	SERVICE
80/tcp	open	http

Nmap done: 1 IP address (1 host up) scanned in 2.00 seconds





Zenmap

Scan Tools Profile Help

Target: 127.0.0.1 Profile:

Command: nmap -p - 127.0.0.1

Hosts Services

Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

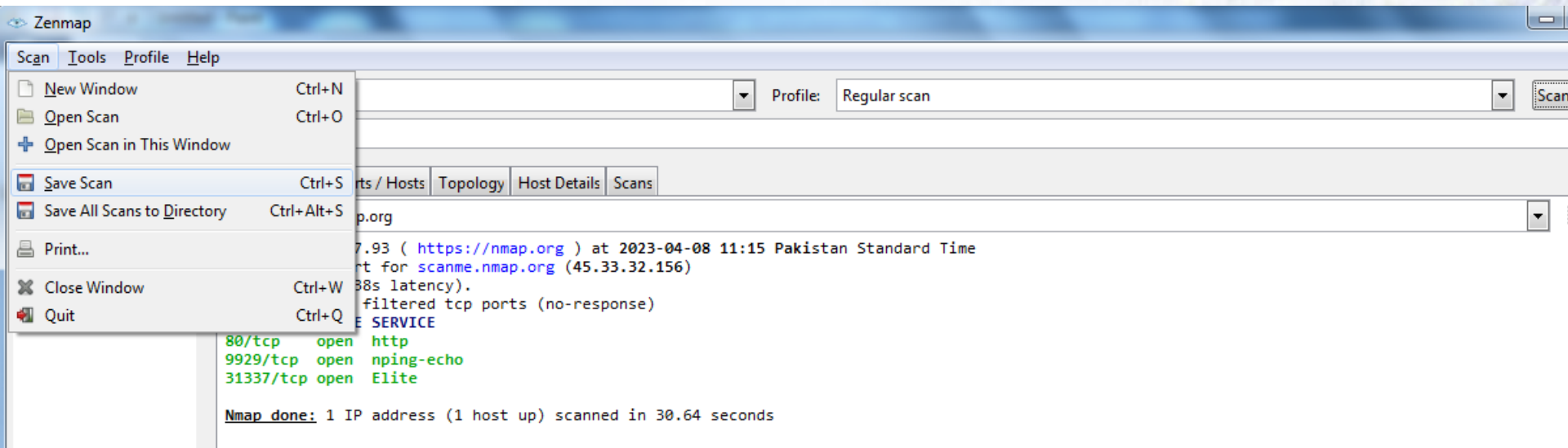
localhost (127.0.0.1)

nmap -p - 127.0.0.1

Starting Nmap 7.93 (<https://nmap.org>) at 2023-04-08 11:10 Pakistan Standard Time
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0021s latency).
Not shown: 65518 closed tcp ports (reset)

PORT	STATE	SERVICE
135/tcp	open	msrpc
445/tcp	open	microsoft-ds
554/tcp	open	rtsp
895/tcp	open	unknown
1025/tcp	open	NFS-or-IIS
1026/tcp	open	LSA-or-nterm
1027/tcp	open	IIS
1028/tcp	open	unknown
1029/tcp	open	ms-lsa
1030/tcp	open	iad1
1031/tcp	open	iad2
1035/tcp	open	multidrop
1783/tcp	open	unknown
2869/tcp	open	icslap
5939/tcp	open	unknown
10243/tcp	open	unknown
50911/tcp	open	unknown

Nmap done: 1 IP address (1 host up) scanned in 22.52 seconds



nmap scanme.nmap.org

Starting Nmap 7.93 (<https://nmap.org>) at 2023-04-08 11:15 Pakistan Standard Time

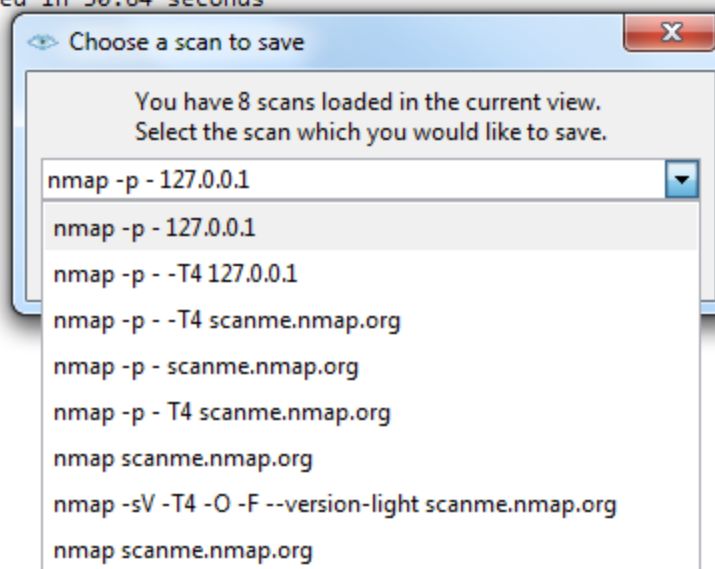
Nmap scan report for scanme.nmap.org (45.33.32.156)

Host is up (0.38s latency).

Not shown: 997 filtered tcp ports (no-response)

PORT	STATE	SERVICE
80/tcp	open	http
9929/tcp	open	nping-echo
31337/tcp	open	Elite

Nmap done: 1 IP address (1 host up) scanned in 30.64 seconds



nmap scanme.nmap.org

Starting Nmap 7.93 (<https://nmap.org>) at 2023-04-08 11:45: Pakistan Standard Time

Nmap scan report for scanme.nmap.org

Host is up (0.38s latency)

Not shown: 997 filtered

PORT STATE SERVICE

80/tcp open http

9929/tcp open nping-echo

31337/tcp open Elite

Nmap done: 1 IP address

Search Scans

Search:

Expressions

Scan	Date
Quick scan on 192.168.15.62	2023-03-07 15:40
Quick scan on 192.168.15.62	2023-03-07 15:40
Quick scan on www.vu.edu.pk	2023-03-07 16:46
Quick scan on nmap 127.0.0.1	2023-03-08 16:58
Intense scan on nmap 127.0.0.1	2023-03-08 16:57
Regular scan on nmap 127.0.0.1	2023-03-08 16:59
nmap scanme.namp.org	2023-04-08 09:38
Regular scan on scanme.namp.org	2023-04-08 09:39
nmap -T5 www.vu.edu.pk	2023-04-08 09:42
Regular scan on www.vu.edu.pk	2023-04-08 09:49
Ping scan on www.vu.edu.pk	2023-04-08 09:49
nmap -T5 -Pn www.vu.edu.pk	2023-04-08 09:48
Quick traceroute on scanme.nmap.org	2023-04-08 09:50

Matched 30 out of 30 scans.

Close

+ Append

Open