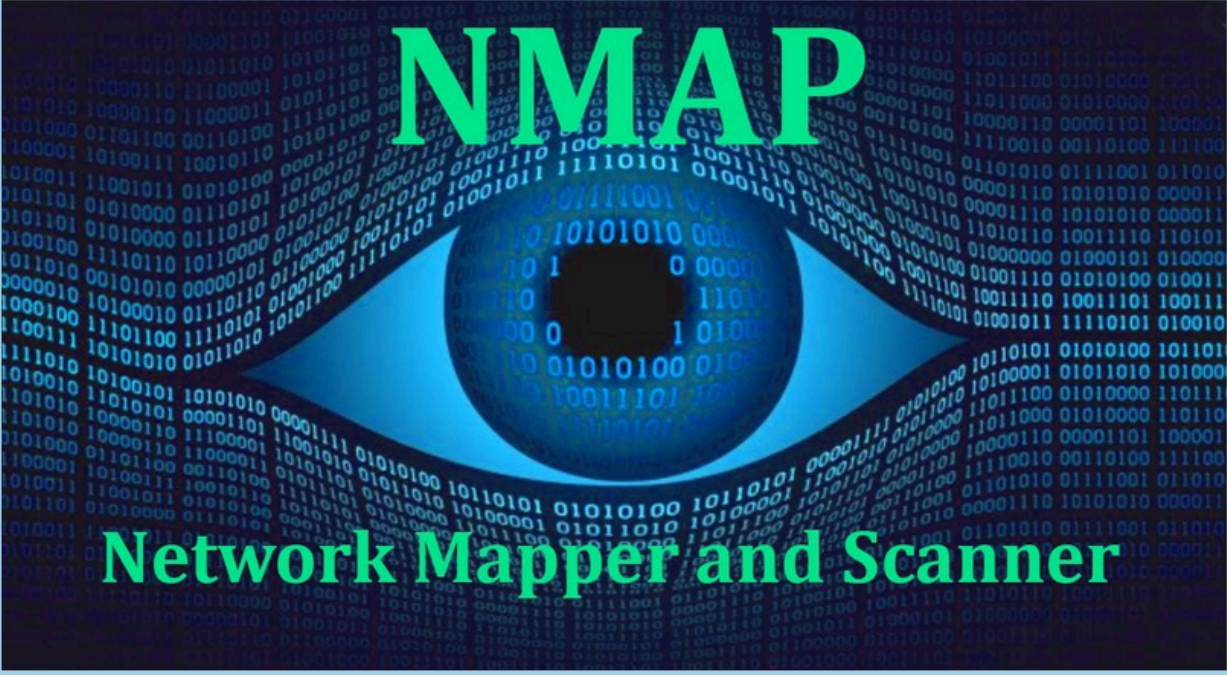




NMAP

Network Mapper and Scanner

Nmap Cheat Sheet for Beginners
Cybersecurity Learning Journey

Target Specification

```
(root@kali)-[/home/kali]
# nmap -sn 192.168.40.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2026-03-02 03:34 EST
Nmap scan report for 192.168.40.1
Host is up (0.0011s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.40.2
Host is up (0.00051s latency).
MAC Address: 00:50:56:F0:A0:EC (VMware)
Nmap scan report for 192.168.40.129
Host is up (0.0015s latency).
MAC Address: 00:0C:29:E7:D4:F9 (VMware)
Nmap scan report for 192.168.40.254
Host is up (0.00050s latency).
MAC Address: 00:50:56:E4:E6:9D (VMware)
Nmap scan report for 192.168.40.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.05 seconds

(root@kali)-[/home/kali]
```

- Performs a ping scan to discover which hosts are alive in the /24 network (no port scan).

```
(root@kali)-[/home/kali]
# nmap 192.168.40.129
Starting Nmap 7.95 ( https://nmap.org ) at 2026-03-02 03:16 EST
Nmap scan report for 192.168.40.129
Host is up (0.0050s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:E7:D4:F9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.40 seconds
```

- Scans a single target IP to find open ports and running services.

```
(root@kali)-[/home/kali]
# nmap 192.168.40.129 192.168.40.254
Starting Nmap 7.95 ( https://nmap.org ) at 2026-03-02 03:17 EST
Nmap scan report for 192.168.40.129
Host is up (0.0028s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:E7:D4:F9 (VMware)

Nmap scan report for 192.168.40.254
Host is up (0.00039s latency).
All 1000 scanned ports on 192.168.40.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:E4:E6:9D (VMware)

Nmap done: 2 IP addresses (2 hosts up) scanned in 10.05 seconds
```

- Scans multiple specific IP addresses in one command

```
(root@kali)-[/home/kali]
# nmap 192.168.40.1-254
Starting Nmap 7.95 ( https://nmap.org ) at 2026-03-02 03:19 EST
Nmap scan report for 192.168.40.1
Host is up (0.0011s latency).
All 1000 scanned ports on 192.168.40.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.40.2
Host is up (0.00014s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 00:50:56:F0:A0:EC (VMware)

Nmap scan report for 192.168.40.129
Host is up (0.0027s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:E7:D4:F9 (VMware)

Nmap scan report for 192.168.40.254
```

- Scans a range of IP addresses (e.g., 192.168.40.1-254) to check active hosts and open ports.

```

8009/tcp open  ajp13
8180/tcp open  unknown
(root@kali)-[/home/kali] ~ (VMware)
# nmap 192.168.40.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2026-03-02 03:25 EST
Nmap scan report for 192.168.40.1
Host is up (0.0011s latency). 168.40.254 are in ignored states.
All 1000 scanned ports on 192.168.40.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.40.128
Nmap scan report for 192.168.40.2
Host is up (0.00027s latency). 168.40.128 are in ignored states.
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
Addresses (4 hosts up) scanned in 18.79 seconds
MAC Address: 00:50:56:F0:A0:EC (VMware)
/home/kali
Nmap scan report for 192.168.40.129
Host is up (0.0023s latency). nmap.org ) at 2026-03-02 03:34 EST
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:E7:D4:F9 (VMware)
Nmap scan report for 192.168.40.254

```

- Scans the entire /24 subnet and performs port scanning on all discovered hosts.

Session Actions Edit View Help

```
(root@kali)-[/home/kali]
# nmap 192.168.40.0/24 -o nmap.targets
Starting Nmap 7.95 ( https://nmap.org ) at 2026-03-02 03:26 EST
Nmap scan report for 192.168.40.1
Host is up (0.00055s latency).
All 1000 scanned ports on 192.168.40.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.40.129
Host is up (0.0020s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain/kali
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:E7:D4:F9 (VMware)

Nmap scan report for 192.168.40.254
Host is up (0.00045s latency).
All 1000 scanned ports on 192.168.40.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:E4:E6:9D (VMware)

Nmap scan report for 192.168.40.128
Host is up (0.0000020s latency).
All 1000 scanned ports on 192.168.40.128 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
```

- Scans the subnet and saves the output results into a file named nmap.targets

Session Actions Edit View Help

(root@kali)-[/home/kali]

cat nmap.targets

Nmap 7.95 scan initiated Mon Mar 22 03:26:08 2026 as: /usr/lib/nmap/nmap -o nmap.targets 192.168.40.0/24

Nmap scan report for 192.168.40.1

Host is up (0.00055s latency).

All 1000 scanned ports on 192.168.40.1 are in ignored states.

Not shown: 1000 filtered tcp ports (no-response)

MAC Address: 00:50:56:C0:00:08 (VMware)

MAC Address: 00:50:56:E4:E6:9D (VMware)

Nmap scan report for 192.168.40.129

Host is up (0.0020s latency).

Not shown: 977 closed tcp ports (reset)

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

23/tcp open telnet

25/tcp open smtp

53/tcp open domain

80/tcp open http

111/tcp open rpcbind

139/tcp open netbios-ssn

445/tcp open microsoft-ds

512/tcp open exec

513/tcp open login

514/tcp open shell

1099/tcp open rmiregistry

1524/tcp open ingreslock

2049/tcp open nfs

2121/tcp open ccproxy-ftp

3306/tcp open mysql

5432/tcp open postgresql

5900/tcp open vnc

6000/tcp open X11

6667/tcp open irc

8009/tcp open ajp13

8180/tcp open unknown

MAC Address: 00:0C:29:E7:D4:F9 (VMware)

Nmap scan report for 192.168.40.254

Host is up (0.00045s latency).

All 1000 scanned ports on 192.168.40.254 are in ignored states.

Not shown: 1000 filtered tcp ports (no-response)

MAC Address: 00:50:56:E4:E6:9D (VMware)

Nmap scan report for 192.168.40.128

Host is up (0.000020s latency).

All 1000 scanned ports on 192.168.40.128 are in ignored states.

Not shown: 1000 closed tcp ports (reset)

- Displays the saved scan results from the file in the terminal.

```
(root@kali)-[/home/kali]
# nmap 192.168.40.1-254 -exclude 192.168.40.2
Starting Nmap 7.95 ( https://nmap.org ) at 2026-03-02 03:30 EST
Nmap scan report for 192.168.40.1
Host is up (0.00055s latency).
All 1000 scanned ports on 192.168.40.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:00:08 (VMware)
```

```
Nmap scan report for 192.168.40.129
Host is up (0.0020s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:E7:D4:F9 (VMware)
```

```
Nmap scan report for 192.168.40.254
Host is up (0.00049s latency).
All 1000 scanned ports on 192.168.40.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:E4:E6:9D (VMware)
```

- Scans an IP range but excludes a specific IP address from being scanned

```
(root@kali)-[/home/kali]
# nmap google.com
Starting Nmap 7.95 ( https://nmap.org ) at 2026-03-02 03:25 EST
Nmap scan report for google.com (142.250.192.206)
Host is up (0.075s latency).
Other addresses for google.com (not scanned): 2404:6800:4002:802::200e
rDNS record for 142.250.192.206: del11s12-in-f14.1e100.net
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 66.66 seconds
```

- Scans the domain by resolving it to its IP address and checking open ports on the server.