Nmap Scanning

_

```
Nmap - - version
(david㉿vbox)-[~]
└─$ nmap -- version
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-15 09:09 CDT
Failed to resolve "version".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.47 seconds
```

Basic Scan:

```
Ls
$ nmap scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-15 09:06 CDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.030s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 filtered tcp ports (no-response)
PORT          STATE SERVICE
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
443/tcp   open  https
5060/tcp  open  sip
8080/tcp  open  http-proxy
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 13.54 seconds
```

992 closed ports. Port 80 open with http services running.

Scan for more open ports searching a range of IP address.

```
map scanme.nmap.org/30
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-15 09:11 CDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.027s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 filtered tcp ports (no-response)
PORT          STATE SERVICE
22/tcp open  ssh
```

```
53/tcp open  domain
80/tcp open  http
443/tcp   open  https
5060/tcp  open  sip
8080/tcp  open  http-proxy
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap scan report for 45-33-32-157.ip.linodeusercontent.com (45.33.32.157)
Host is up (0.012s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT          STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
443/tcp  open  https
5060/tcp open  sip
8080/tcp open  http-proxy

Nmap scan report for 45-33-32-158.ip.linodeusercontent.com (45.33.32.158)
Host is up (0.031s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT          STATE SERVICE
21/tcp   open  ftp
53/tcp   open  domain
80/tcp   open  http - open port to web server
110/tcp  open  pop3
111/tcp  open  rpcbind
143/tcp  open  imap
443/tcp  open  https
465/tcp  open  smtps
993/tcp  open  imaps
995/tcp  open  pop3s
3306/tcp open  mysql - open port to database.
5060/tcp open  sip
8080/tcp open  http-proxy

Nmap scan report for 45-33-32-159.ip.linodeusercontent.com (45.33.32.159)
Host is up (0.013s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT          STATE SERVICE
```

```
53/tcp   open  domain
80/tcp   open  http
443/tcp  open  https
5060/tcp open  sip
8080/tcp open  http-proxy

Nmap done: 4 IP addresses (4 hosts up) scanned in 18.87 seconds
```

Nmap with options

Nmap -A -T4 **scanme.nmap.org**
-A Enable OS detection, version detection, script scanning and traceroute
-T4 Set Timing template (1-5) higher is faster.

```
nmap -A -T4 scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-15 09:57 CDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.010s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 986 filtered tcp ports (no-response)
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)
53/tcp open   domain          ISC BIND
80/tcp open   http               Apache httpd 2.4.7 ((Ubuntu))
|_http-favicon: Nmap Project
|_http-title: Go ahead and ScanMe!
|_http-server-header: Apache/2.4.7 (Ubuntu)
443/tcp   open   tcpwrapped
902/tcp   closed iss-realsecure
2701/tcp  closed sms-rcinfo
5060/tcp  open   tcpwrapped
5269/tcp  closed xmpp-server
5815/tcp  closed unknown
8080/tcp  open   tcpwrapped
```

```
8888/tcp  closed sun-answerbook
9929/tcp  open   nping-echo       Nping echo
31337/tcp open   tcpwrapped
64680/tcp closed unknown
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (93%), Bay Networks
embedded (86%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_450
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway
(93%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.70 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 185.78 seconds
```

Target IP address is running linux on an Oracle Virtualbox.
Open ports that could be vulnerable to attack.
Port 22 SSH
Port 80 http webserver
9929/tcp open   nping-echo   Nping echo

Scan Ports 20 - 80 Aggressively detecting os, scripts, and traceroutes. Save output to file called output.txt

```
 nmap -p22-80 -A -T3 -oN output.txt scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-15 11:26 CDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.010s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 56 filtered tcp ports (no-response)
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)
53/tcp open  domain  ISC BIND
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
|_http-favicon: Nmap Project
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (94%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway
(94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   2.95 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 28.26 seconds
```