

## nmap Lab

### nmap -v scanme.nmap.org

- This option scans all reserved TCP ports on the machine scanme.nmap.org . The -v option enables verbose mode.

```
(kali㉿kali)-[~]
└─$ nmap -v scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-09 00:10 EDT
Initiating Ping Scan at 00:10
Scanning scanme.nmap.org (45.33.32.156) [2 ports]
Completed Ping Scan at 00:10, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:10
Completed Parallel DNS resolution of 1 host. at 00:10, 6.59s elapsed
Initiating Connect Scan at 00:10
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Completed Connect Scan at 00:10, 1.90s elapsed (1000 total ports)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.065s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE     SERVICE
22/tcp    open      ssh
25/tcp    filtered  smtp
80/tcp    filtered  http
111/tcp   filtered  rpcbind
135/tcp   filtered  msrpc
139/tcp   filtered  netbios-ssn
445/tcp   filtered  microsoft-ds
9929/tcp  open      nping-echo
31337/tcp open      Elite

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 8.70 seconds

(kali㉿kali)-[~]
└─$ █
```

nmap -sS -O scanme.nmap.org/24

- Launches a stealth SYN scan against each machine that is up out of the 256 IPs on the /24 sized network where Scanme resides. It also tries to determine what operating system is running on each host that is up and running. This requires root privileges because of the SYN scan and OS detection.

```
nmap -sS -O scanme.nmap.org/24
You requested a scan type which requires root privileges.
QUITTING!
```

**nmap -sV -p 22,53,110,143,4564 198.116.0-255.1-127**

- Launches host enumeration and a TCP scan at the first half of each of the 255 possible eight-bit subnets in the 198.116.0.0/16 address space. This tests whether the systems run SSH, DNS, POP3, or IMAP on their standard ports, or anything on port 4564. For any of these ports found open, version detection is used to determine what application is running.

```
nmap -sV -p 22,53,110,143,4564,198.116.0-255.1-127
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-09 00:12 EDT
Error #487: Your port specifications are illegal. Example of proper form: "-100,200-1024,T:3000-4000,U:60000-"
QUITTING!
[(kali㉿kali)-[~]]$
```

**nmap -v -iR 100000 -Pn -p 80**

- Asks Nmap to choose 100,000 hosts at random and scan them for web servers (port 80). Host enumeration is disabled with -Pn since first sending a couple probes to determine whether a host is up is wasteful when you are only probing one port on each target host anyway.

```
nmap -v -iR 100000 -Pn -p 80
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-09 00:14 EDT
Initiating Parallel DNS resolution of 4096 hosts. at 00:14
Completed Parallel DNS resolution of 4096 hosts. at 00:18, 209.22s elapsed
Initiating Connect Scan at 00:18
Scanning 1024 hosts [1 port/host]
Discovered open port 80/tcp on 89.161.227.16
Discovered open port 80/tcp on 184.50.187.94
Discovered open port 80/tcp on 18.164.37.152
Discovered open port 80/tcp on 46.57.87.186
Discovered open port 80/tcp on 51.83.253.187
Discovered open port 80/tcp on 18.220.64.237
Discovered open port 80/tcp on 52.9.150.238
Discovered open port 80/tcp on 168.205.218.4
Discovered open port 80/tcp on 123.57.79.211
Discovered open port 80/tcp on 208.109.73.138
Discovered open port 80/tcp on 96.17.83.181
Discovered open port 80/tcp on 49.212.193.234
Discovered open port 80/tcp on 34.160.104.205
Completed Connect Scan at 00:18, 39.92s elapsed (1024 total ports)
Nmap scan report for 8.137.176.147
Host is up.

PORT      STATE      SERVICE
80/tcp     filtered   http

Nmap scan report for 51.212.30.56
Host is up.

PORT      STATE      SERVICE
80/tcp     filtered   http

Nmap scan report for 94-167-167-181.fibertel.com.ar (181.167.167.94)
Host is up.

PORT      STATE      SERVICE
80/tcp     filtered   http

Nmap scan report for 185.112.40.200
Host is up.
```

**nmap -Pn -p80 -oX logs/pb-port80scan.xml -oG logs/pb-port80scan.gnmap  
216.163.128.20/20**

- This scans 4096 IPs for any web servers (without pinging them) and saves the output in grepable and XML formats.

```
[(kali㉿kali)-[~]]$ nmap -Pn -p80 -oX logs/pb-port80scan.xml -oG logs/pb-port80scan.gnmap 216.163.128.20/20
Failed to open machine output file logs/pb-port80scan.gnmap for writing: No such file or directory (2)

[(kali㉿kali)-[~]]$
```