

NAME :- Atul SHARMA
UID :- 2021700060
Batch : D4

What is Nmap?

Nmap is an open-source utility for network discovery. Network Mapper is a security auditing and network scanning independent tool developed by **Gordon Lyon**. It is used by network administrators to detect the devices currently running on the system and the port number by which the devices are connected.

Many systems and network administrators are used for managing **network inventory, service upgrade schedules, monitoring hosts** and **service uptime**.

Nmap Definition

At the top-level, Nmap is defined as a tool that can detect or diagnose services that are running on an **Internet-connected system** by a network administrator in their networked system used to identify potential security flaws. It is used to automate redundant tasks, such as monitoring the service.

Working of Nmap

Nmap is convenient during penetration testing of networked systems. Nmap provides the network details, and also helps to determine the security flaws present in the system. Nmap is **platform-independent** and runs on popular **operating systems** such as **Linux, Windows** and **Mac**.

Advantages of Nmap

Nmap has a lot of advantages that make it different from other network scanning tools. Nmap is open-source and **free** to use.

Some other advantages are listed below.

- It is used for auditing network systems as it can detect new servers.
- It will search for **subdomain** and Domain Name System
- With the help of Nmap Scripting Engine (**NSE**), interaction can be made with the target host.

- It determines the nature of the service in the host and performs whether the host is a mail service or a web server.

How to install Nmap Command

Before exploring with Nmap commands, the Nmap scanner tool must have installed on your system. So, if it is not downloaded yet, get it by opening up the terminal and executing the following command:

sudo apt install nmap

```
cnlab404@cnlab404-Veriton-M200-H110: ~$ sudo apt install nmap
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libblas3 liblinear4 lua-lpeg nmap-common
Suggested packages:
  liblinear-tools liblinear-dev ncat ndiff zenmap
The following NEW packages will be installed:
  libblas3 liblinear4 lua-lpeg nmap nmap-common
0 upgraded, 5 newly installed, 0 to remove and 14 not upgraded.
Need to get 5,553 kB of archives.
After this operation, 26.3 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu focal/main amd64 libblas3 amd64 3.9.0-1build1 [142 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 liblinear4 amd64 2.3.0+dfsg-3build1 [41.7 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 lua-lpeg amd64 1.0.2-1 [31.4 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 nmap-common all 7.80+dfsg1-2build1 [3,676 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 nmap amd64 7.80+dfsg1-2build1 [1,662 kB]
Fetched 5,553 kB in 3s (1,869 kB/s)
Selecting previously unselected package libblas3:amd64.
(Reading database ... 194593 files and directories currently installed.)
Preparing to unpack .../libblas3_3.9.0-1build1_amd64.deb ...
Unpacking libblas3:amd64 (3.9.0-1build1) ...
Selecting previously unselected package liblinear4:amd64.
Preparing to unpack .../liblinear4_2.3.0+dfsg-3build1_amd64.deb ...
Unpacking liblinear4:amd64 (2.3.0+dfsg-3build1) ...
Selecting previously unselected package lua-lpeg:amd64.
Preparing to unpack .../lua-lpeg_1.0.2-1_amd64.deb ...
Unpacking lua-lpeg:amd64 (1.0.2-1) ...
Selecting previously unselected package nmap-common.
Preparing to unpack .../nmap-common_7.80+dfsg1-2build1_all.deb ...
Unpacking nmap-common (7.80+dfsg1-2build1) ...
Selecting previously unselected package nmap.
Preparing to unpack .../nmap_7.80+dfsg1-2build1_amd64.deb ...
Unpacking nmap (7.80+dfsg1-2build1) ...
Setting up lua-lpeg:amd64 (1.0.2-1) ...
Setting up libblas3:amd64 (3.9.0-1build1) ...
```

sudo

How to scan hostname using Nmap command

To perform a scan using hostname and IP address is the best way to run Nmap commands. For example, I set the hostname as “linuxhint.com

nmap linuxhint.com

```
cnlab404@cnlab404-Veriton-M200-H110:~$ nmap linuxhint.com
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-10 09:41 IST
Nmap scan report for linuxhint.com (104.18.7.55)
Host is up (0.0038s latency).
Other addresses for linuxhint.com (not scanned): 104.18.6.55 2606:4700::6812:637 2606:4700::6812:737
Not shown: 996 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8080/tcp  open  http-proxy
8443/tcp  open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 4.97 seconds
```

```
cnlab404@cnlab404-Veriton-M200-H110:~$ sudo nmap 10.0.2.15
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-10 09:43 IST
Nmap scan report for 10.0.2.15
Host is up (0.00018s latency).
All 1000 scanned ports on 10.0.2.15 are filtered

Nmap done: 1 IP address (1 host up) scanned in 4.23 seconds
```

```
cnlab404@cnlab404-Veriton-M200-H110:~$ nmap -v linuxhint.com
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-10 09:44 IST
Initiating Ping Scan at 09:44
Scanning linuxhint.com (104.18.6.55) [2 ports]
Completed Ping Scan at 09:44, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:44
Completed Parallel DNS resolution of 1 host. at 09:44, 0.00s elapsed
Initiating Connect Scan at 09:44
Scanning linuxhint.com (104.18.6.55) [1000 ports]
Discovered open port 80/tcp on 104.18.6.55
Discovered open port 8080/tcp on 104.18.6.55
Discovered open port 443/tcp on 104.18.6.55
Discovered open port 8443/tcp on 104.18.6.55
Completed Connect Scan at 09:44, 4.71s elapsed (1000 total ports)
Nmap scan report for linuxhint.com (104.18.6.55)
Host is up (0.0043s latency).
Other addresses for linuxhint.com (not scanned): 104.18.7.55 2606:4700::6812:737 2606:4700::6812:637
Not shown: 996 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8080/tcp  open  http-proxy
8443/tcp  open  https-alt

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.80 seconds
```

```
cnlab404@cnlab404-Veriton-M200-H110:~$ nmap 10.0.2.15
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-10 09:45 IST
Note: Host seems down. If it is really up, but blocking our ping probe
s, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.05 seconds
```

```
cnlab404@cnlab404-Veriton-M200-H110:~$ sudo nmap -O linuxhint.com
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-10 09:51 IST
Nmap scan report for linuxhint.com (104.18.7.55)
Host is up (0.0019s latency).
Other addresses for linuxhint.com (not scanned): 104.18.6.55 2606:4700
::6812:737 2606:4700::6812:637
All 1000 scanned ports on linuxhint.com (104.18.7.55) are filtered
Too many fingerprints match this host to give specific OS details

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.64 seconds
```

```
cnlab404@cnlab404-Veriton-M200-H110:~$ sudo nmap -sA 10.0.2.15
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-10 09:53 IST
Nmap scan report for 10.0.2.15
Host is up (0.0021s latency).
Not shown: 999 unfiltered ports
PORT      STATE      SERVICE
5862/tcp  filtered  unknown
Nmap done: 1 IP address (1 host up) scanned in 1.43 seconds
```



```
cnlab404@cnlab404-Veriton-M200-H110:~$ sudo nmap -sP 10.0.2.*
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-10 09:55 IST
Nmap scan report for 10.0.2.0
Host is up (0.00012s latency).
Nmap scan report for 10.0.2.1
Host is up (0.00036s latency).
Nmap scan report for 10.0.2.2
Host is up (0.00025s latency).
Nmap scan report for 10.0.2.3
Host is up (0.00012s latency).
Nmap scan report for 10.0.2.4
Host is up (0.00016s latency).
Nmap scan report for 10.0.2.5
Host is up (0.00019s latency).
Nmap scan report for 10.0.2.6
Host is up (0.00013s latency).
Nmap scan report for 10.0.2.7
Host is up (0.00017s latency).
Nmap scan report for 10.0.2.8
Host is up (0.00017s latency).
Nmap scan report for 10.0.2.9
Host is up (0.00016s latency).
Nmap scan report for 10.0.2.10
Host is up (0.00015s latency).
Nmap scan report for 10.0.2.11
Host is up (0.00014s latency).
Nmap scan report for 10.0.2.12
Host is up (0.00015s latency).
Nmap scan report for 10.0.2.13
Host is up (0.00014s latency).
Nmap scan report for 10.0.2.14
Host is up (0.00014s latency).
Nmap scan report for 10.0.2.15
Host is up (0.00013s latency).
Nmap scan report for 10.0.2.16
Host is up (0.00015s latency).
Nmap scan report for 10.0.2.17
```

```
cnlab404@cnlab404-Veriton-M200-H110:~$ sudo nmap -V
Nmap version 7.80 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.3.3 openssl-1.1.1d nmap-libssh2-1.8.2 libz-1.2
.11 libpcre-8.39 libpcap-1.9.1 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

```

cnlab404@cnlab404-Veriton-M200-H110:~$ sudo nmap --iflist
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-10 10:04 IST
*****INTERFACES*****
DEV      (SHORT)  IP/MASK          TYPE      UP MTU   MAC
lo       (lo)     127.0.0.1/8      loopback  up 65536
enp1s0   (enp1s0)  172.16.41.40/24   ethernet  up 1500   F4:4D:3
0:4E:D5:82
enp1s0   (enp1s0)  fe80::b728:152d:4e2c:88ac/64 ethernet  up 1500   F4:4D:3
0:4E:D5:82

*****ROUTES*****
DST/MASK          DEV      METRIC GATEWAY
172.16.41.0/24    enp1s0   100
169.254.0.0/16    enp1s0   1000
0.0.0.0/0         enp1s0   100     172.16.41.1
fe80::b728:152d:4e2c:88ac/128 enp1s0   0
fe80::/64         enp1s0   100
ff00::/8          enp1s0   256

```

```

cnlab404@cnlab404-Veriton-M200-H110:~$ sudo nmap -p 80 linuxhint.com
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-10 10:05 IST
Nmap scan report for linuxhint.com (104.18.7.55)
Host is up (0.00063s latency).
Other addresses for linuxhint.com (not scanned): 104.18.6.55 2606:4700
::6812:637 2606:4700::6812:737

PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds

```

```

cnlab404@cnlab404-Veriton-M200-H110:~$ sudo nmap 8.8.8.8
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-10 10:05 IST
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.00059s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 4.72 seconds
cnlab404@cnlab404-Veriton-M200-H110:~$ sudo nmap -sU 8.8.8.8
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-10 10:06 IST
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.00060s latency).
Not shown: 999 open|filtered ports
PORT      STATE SERVICE
53/udp    open  domain

Nmap done: 1 IP address (1 host up) scanned in 4.20 seconds

```

```

cnlab404@cnlab404-Veriton-M200-H110:~$ sudo nmap -sT 10.0.2.15
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-10 10:07 IST
Nmap scan report for 10.0.2.15
Host is up (0.00016s latency).
All 1000 scanned ports on 10.0.2.15 are filtered

Nmap done: 1 IP address (1 host up) scanned in 21.18 seconds
cnlab404@cnlab404-Veriton-M200-H110:~$ █

```

Conclusion: -

Successfully understood the use of the network monitoring utility nmap. Also, learned about various commands that can help in diagnosing security issues and also finding hosts and free ports.