

Download and install nmap. Use it with different options to scan open ports, perform OS fingerprinting, do a ping scan, tcp port scan, udp port scan, etc.

Nmap (Network Mapper) is a security scanner originally written by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich) used to discover hosts and services on a computer network, thus creating a "map" of the network. To accomplish its goal, Nmap sends specially crafted packets to the target host and then analyzes the responses. Unlike many simple port scanners that just send packets at some predefined constant rate, Nmap accounts for the network conditions (latency fluctuations, network congestion, the target interference with the scan) during the run. Also, owing to the large and active user community providing feedback and contributing to its features, Nmap has been able to extend its discovery capabilities beyond simply figuring out whether a host is up or down and which ports are open and closed; it can determine the operating system of the target, names and versions of the listening services, estimated uptime, type of device, and presence of a firewall.

Nmap features include:

- Host Discovery – Identifying hosts on a network. For example, listing the hosts which respond to pings or have a particular port open.
- Port Scanning – Enumerating the open ports on one or more target hosts.
- Version Detection – Interrogating listening network services listening on remote devices to determine the application name and version number.
- OS Detection – Remotely determining the operating system and some hardware characteristics of network devices.

Basic commands working in Nmap:

- For target specifications: `nmap <target's URL or IP with spaces between them>`
- For OS detection: `nmap -O <target-host's URL or IP>`
- For version detection: `nmap -sV <target-host's URL or IP>`

SYN scan is the default and most popular scan option for good reasons. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by restrictive firewalls. It is also relatively unobtrusive and stealthy since it never completes TCP connections

Algorithm\Implementation Steps\Installation Steps:

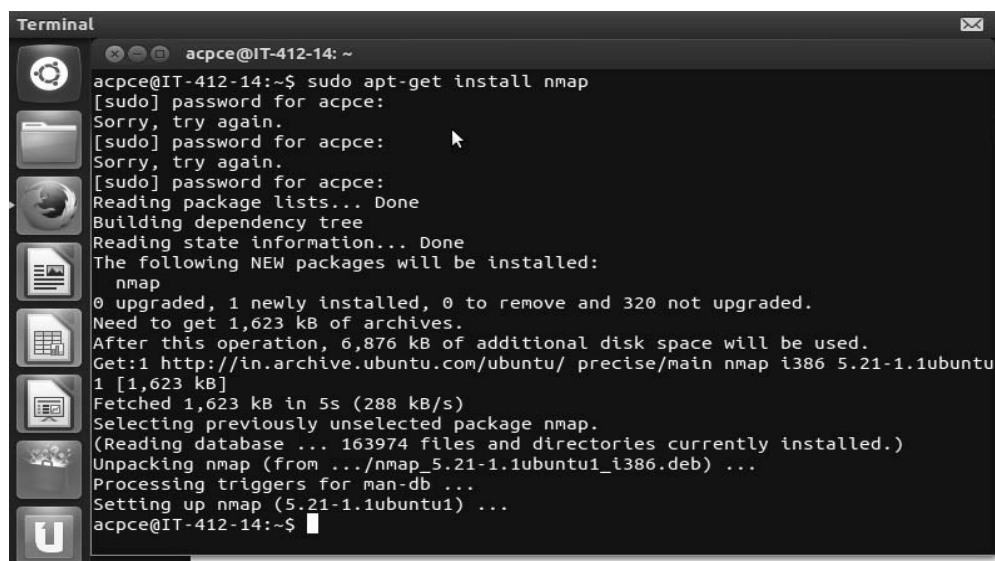
- Installing Nmap from the link.
`sudo apt-get install nmap`
- Obtaining Your IP addresses.

Use the ifconfig command in Linux.

- Performing a Scan of the Local Network.
 1. For the following steps, please use the nmap command line tool installed on Ubuntu
 2. Scan your subnet to determine how many hosts can be found. For example, if you are on the 192.168.1.0 subnet, you would enter the following command: `nmap -sP 192.168.1.*`
 - i. What is your subnet? _____
 - ii. How many hosts were found? _____
 3. Next perform a stealth scan (Please use the IP for your subnet): `nmap -sS -P0 -p 192.169.1.*`
 4. Now, you'll perform an OS identification. Use the Linux O/S to scan your Windows machine:
 - i. `nmap -O Windows_IP_ADDRESS`
 - ii. OS Type 1: _____
 - iii. Now we want to use the Windows machine to scan the Linux O/S. Go to a Windows DOS prompt and enter the following command:
 - iv. `nmap -O Linux_IP_ADDRESS`
 - v. Now we will perform a service selection scan. Let's scan for all computers with FTP running. We would do that as follows:
`nmap -p21 192.168.1.*`
 5. List the IP addresses with that has the FTP open: _____

Input and Output:

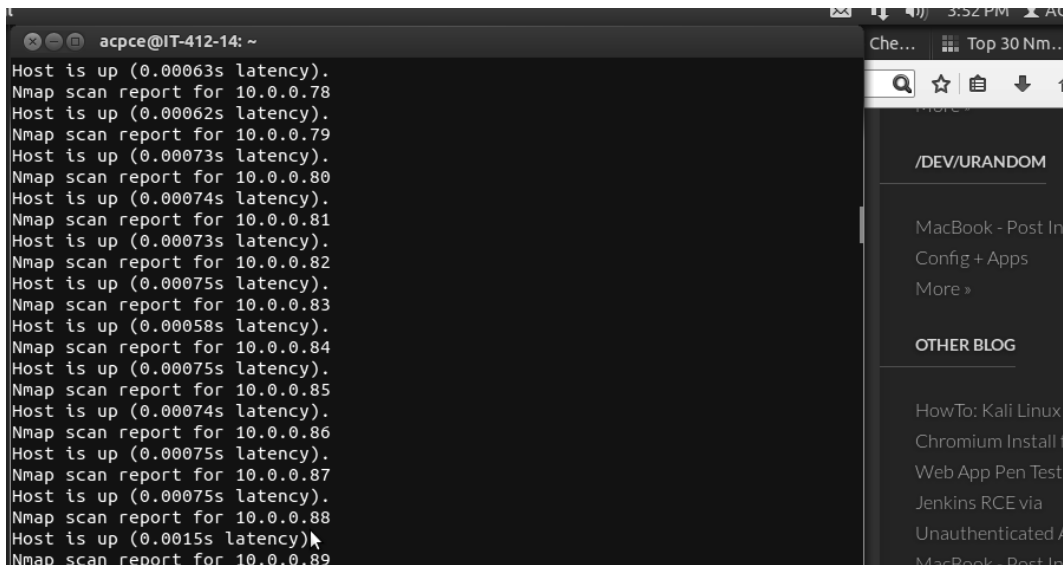
- Installation of nmap:
> `sudo apt-get install nmap`



```
Terminal
acpce@IT-412-14: ~
acpce@IT-412-14:~$ sudo apt-get install nmap
[sudo] password for acpce:
Sorry, try again.
[sudo] password for acpce:
Sorry, try again.
[sudo] password for acpce:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  nmap
0 upgraded, 1 newly installed, 0 to remove and 320 not upgraded.
Need to get 1,623 kB of archives.
After this operation, 6,876 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu/ precise/main nmap i386 5.21-1.1ubuntu
1 [1,623 kB]
Fetched 1,623 kB in 5s (288 kB/s)
Selecting previously unselected package nmap.
(Reading database ... 163974 files and directories currently installed.)
Unpacking nmap (from .../nmap_5.21-1.1ubuntu1_i386.deb) ...
Processing triggers for man-db ...
Setting up nmap (5.21-1.1ubuntu1) ...
acpce@IT-412-14:~$
```

- `nmap -sP 10.0.0.0/24`

Ping scans the network, listing machines that respond to ping.



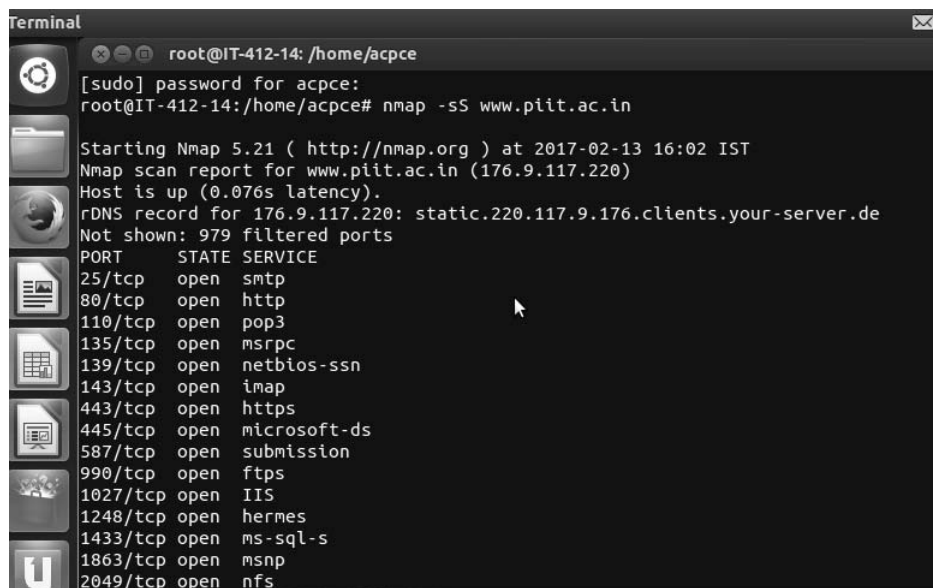
```

acpce@IT-412-14: ~
Host is up (0.00063s latency).
Nmap scan report for 10.0.0.78
Host is up (0.00062s latency).
Nmap scan report for 10.0.0.79
Host is up (0.00073s latency).
Nmap scan report for 10.0.0.80
Host is up (0.00074s latency).
Nmap scan report for 10.0.0.81
Host is up (0.00073s latency).
Nmap scan report for 10.0.0.82
Host is up (0.00075s latency).
Nmap scan report for 10.0.0.83
Host is up (0.00058s latency).
Nmap scan report for 10.0.0.84
Host is up (0.00075s latency).
Nmap scan report for 10.0.0.85
Host is up (0.00074s latency).
Nmap scan report for 10.0.0.86
Host is up (0.00075s latency).
Nmap scan report for 10.0.0.87
Host is up (0.00075s latency).
Nmap scan report for 10.0.0.88
Host is up (0.0015s latency)
Nmap scan report for 10.0.0.89

```

- `FIN scan (-sF)`

Sets just the TCP FIN bit.



```

Terminal
root@IT-412-14: /home/acpce
[sudo] password for acpce:
root@IT-412-14: /home/acpce# nmap -sS www.piit.ac.in
Starting Nmap 5.21 ( http://nmap.org ) at 2017-02-13 16:02 IST
Nmap scan report for www.piit.ac.in (176.9.117.220)
Host is up (0.076s latency).
rDNS record for 176.9.117.220: static.220.117.9.176.clients.your-server.de
Not shown: 979 filtered ports
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
143/tcp   open  imap
443/tcp   open  https
445/tcp   open  microsoft-ds
587/tcp   open  submission
990/tcp   open  ftps
1027/tcp  open  IIS
1248/tcp  open  hermes
1433/tcp  open  ms-sql-s
1863/tcp  open  msnpp
2049/tcp  open  nfs

```

- `-sV (Version detection)` .

Enables version detection, as discussed above. Alternatively, can use `-A`, which enables

version detection among other things.

```
445/tcp open  microsoft-ds
587/tcp open  submission
990/tcp open  ftps
1027/tcp open  IIS
1248/tcp open  hermes
1433/tcp open  ms-sql-s
1863/tcp open  msnp
2049/tcp open  nfs
3306/tcp open  mysql
3389/tcp open  ms-term-serv
5050/tcp open  mmcc
5432/tcp open  postgresql
5666/tcp open  ncp
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 12.99 seconds
root@IT-412-14:/home/acpce# sudo nmap -A -sV www.acpce.ac.in

Starting Nmap 5.21 ( http://nmap.org ) at 2017-02-13 16:07 IST
Failed to resolve given hostname/IP: www.acpce.ac.in. Note that you can't use '
/mask' AND '1-4,7,100-' style IP ranges
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.36 seconds
root@IT-412-14:/home/acpce#
```

- -sO (IP protocol scan) .

IP protocol scan allows you to determine which IP protocols (TCP, ICMP, IGMP, etc.) are supported by target machines. This isn't technically a port scan, since it cycles through IP protocol numbers rather than TCP or UDP port numbers.

```
root@IT-412-14:/home/acpce# sudo nmap -sO 192.168.4.144

Starting Nmap 5.21 ( http://nmap.org ) at 2017-02-13 16:17 IST
Nmap scan report for 192.168.4.144
Host is up (0.14s latency).
Not shown: 249 closed protocols
PROTOCOL STATE SERVICE
1 open icmp
2 open igmp
6 open tcp
17 open udp
103 open|filtered pim
136 open|filtered udplite
255 open|filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 2.52 seconds
root@IT-412-14:/home/acpce#
```

- -O (Enable OS detection) .

Enables OS detection, as discussed above. Alternatively, you can use -A to enable OS detection along with other things.

```
minal
root@IT-412-14: /home/acpce

Starting Nmap 5.21 ( http://nmap.org ) at 2017-02-13 16:20 IST
Nmap scan report for 192.168.4.144
Host is up (0.000016s latency).
All 1000 scanned ports on 192.168.4.144 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at http://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.17 seconds
root@IT-412-14:/home/acpce# sudo nmap -A 192.168.4.144

Starting Nmap 5.21 ( http://nmap.org ) at 2017-02-13 16:20 IST
Nmap scan report for 192.168.4.144
Host is up (0.000017s latency).
All 1000 scanned ports on 192.168.4.144 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at http:
//nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.18 seconds
root@IT-412-14:/home/acpce#
```

- -p port ranges (Only scan specified ports) .

This option specifies which ports you want to scan and overrides the default. Individual port numbers are OK, as are ranges separated by a hyphen (e.g. 1-1023). The beginning and/or end values of a range may be omitted, causing Nmap to use 1 and 65535, respectively.

```
minal
root@IT-412-14: /home/acpce

Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at http:
//nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.18 seconds
root@IT-412-14:/home/acpce# sudo nmap -open 192.168.4.144

Starting Nmap 5.21 ( http://nmap.org ) at 2017-02-13 16:21 IST
Nmap scan report for 192.168.4.144
Host is up (0.0000060s latency).
All 1000 scanned ports on 192.168.4.144 are closed

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
root@IT-412-14:/home/acpce# sudo nmap -p 413 192.168.4.144

Starting Nmap 5.21 ( http://nmap.org ) at 2017-02-13 16:22 IST
Nmap scan report for 192.168.4.144
Host is up (0.000045s latency).
PORT      STATE SERVICE
413/tcp   closed  http

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
root@IT-412-14:/home/acpce#
```

- --top-ports <integer of 1 or greater>

Scans the N highest-ratio ports found in nmap-services file.

```
minal
root@IT-412-14: /home/acpce
Host is up (0.000045s latency).
PORT      STATE SERVICE
413/tcp    closed smsp

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
root@IT-412-14:/home/acpce# nmap --top-ports 10 192.168.4.144

Starting Nmap 5.21 ( http://nmap.org ) at 2017-02-13 16:24 IST
Nmap scan report for 192.168.4.144
Host is up (0.000016s latency).
PORT      STATE SERVICE
21/tcp    closed ftp
22/tcp    closed ssh
23/tcp    closed telnet
25/tcp    closed smtp
80/tcp    closed http
110/tcp   closed pop3
139/tcp   closed netbios-ssn
443/tcp   closed https
445/tcp   closed microsoft-ds
3389/tcp  closed ms-term-serv

Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
root@IT-412-14:/home/acpce#
```

- nmap -iflist
host interface and route information with nmap by using --iflist option.

```
minal
root@IT-412-14: /home/acpce
Failed to resolve given hostname/IP: www.acpce.ac.in. Note that you can't use '
/mask' AND '1-4,7,100-' style IP ranges
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.04 seconds
root@IT-412-14:/home/acpce# sudo nmap -sO 192.168.1.1

Starting Nmap 5.21 ( http://nmap.org ) at 2017-02-13 16:13 IST
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 0.42 seconds
root@IT-412-14:/home/acpce# nmap --iflist

Starting Nmap 5.21 ( http://nmap.org ) at 2017-02-13 16:14 IST
*****INTERFACES*****
DEV (SHORT) IP/MASK      TYPE UP MAC
lo (lo)      127.0.0.1/8      loopback up
eth0 (eth0)   192.168.4.144/16 ethernet up 00:25:64:94:BF:CD

*****ROUTES*****
DST/MASK      DEV GATEWAY
169.254.0.0/0 eth0
192.168.0.0/0 eth0
0.0.0.0/0     eth0 192.168.0.1

root@IT-412-14:/home/acpce#
```