## 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.

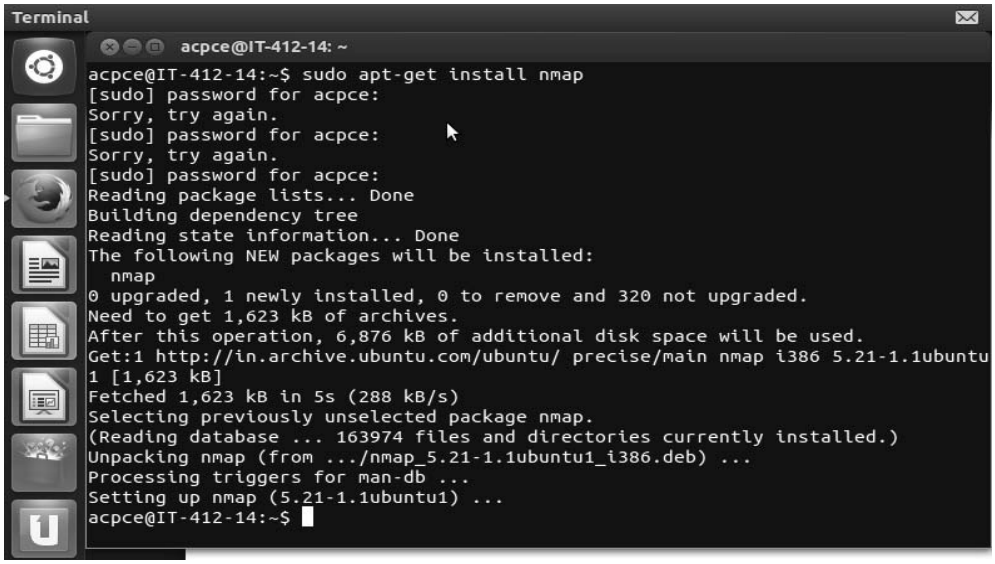
- Performing a Scan of the Local Network.

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:**

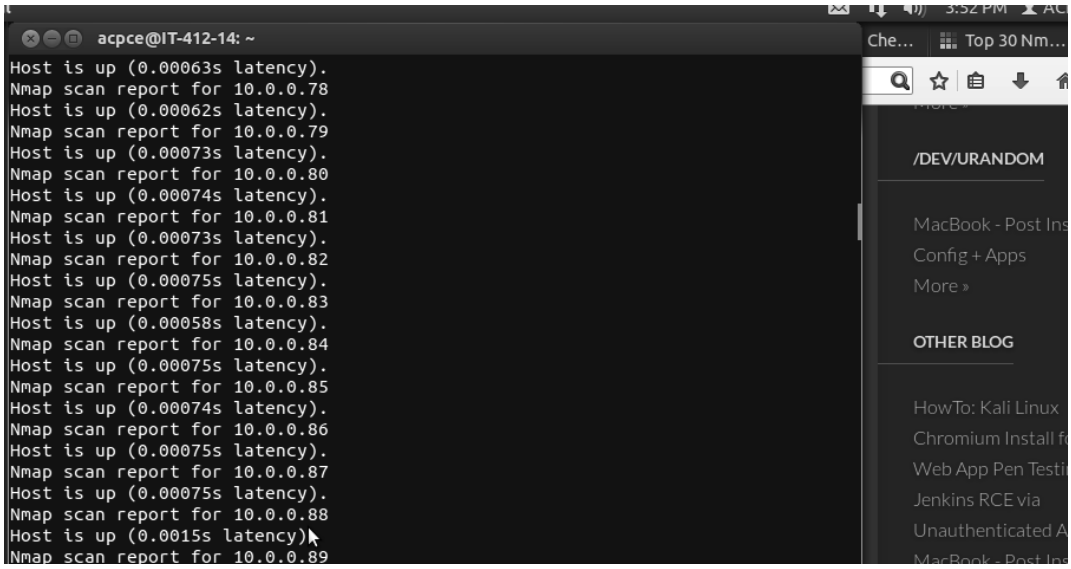
- Installation of nmap:

  > sudo apt-get install nmap



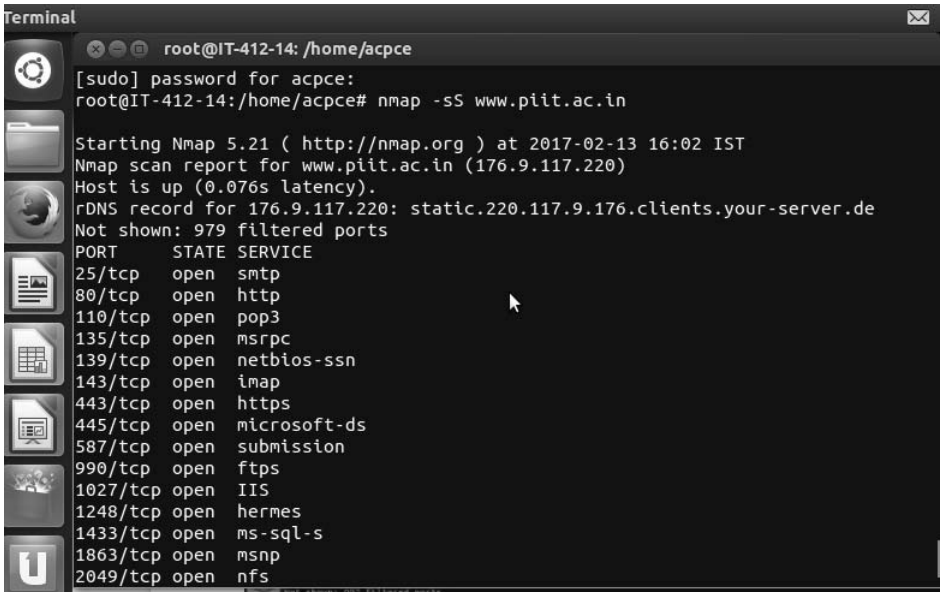
- nmap -sP  10.0.0.0/24

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




- FIN scan (-sF)

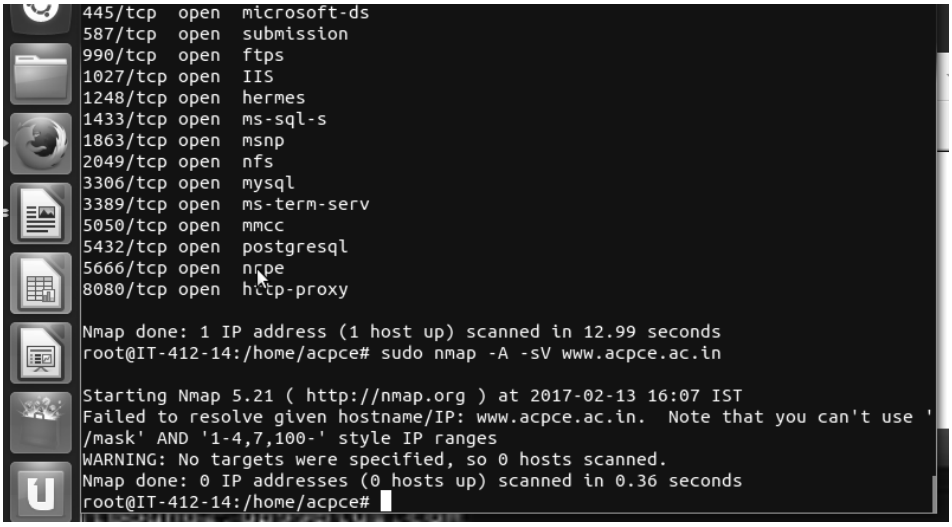
  Sets just the TCP FIN bit.




- -sV (Version detection) .

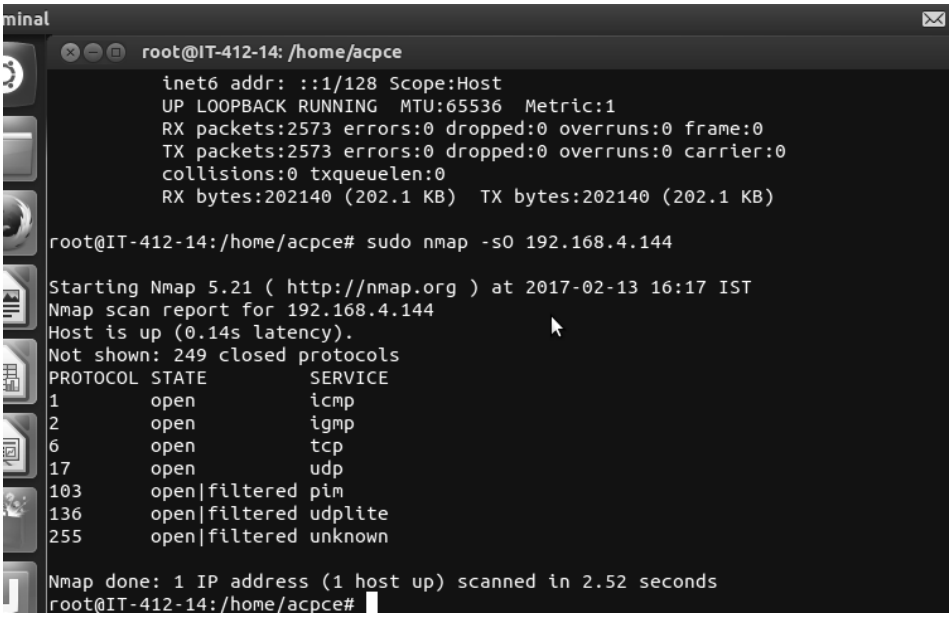
  Enables version detection, as discussed above. Alternatively, can use -A, which enables

version detection among other things.



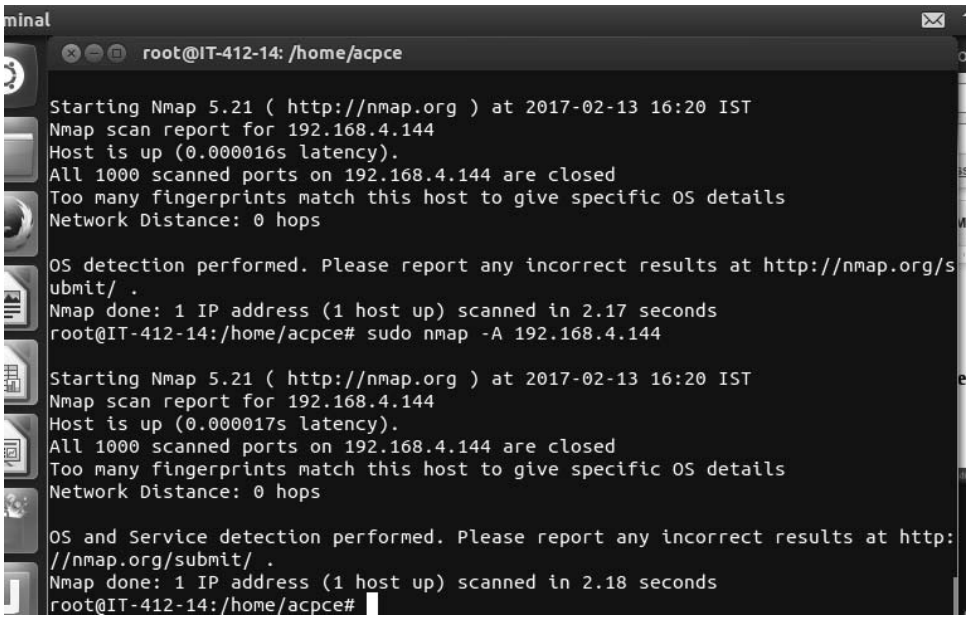

- -sO (IP protocol scan) .

  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.




- -O (Enable OS detection) .

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




- -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.


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

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

```
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.

```
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#
```