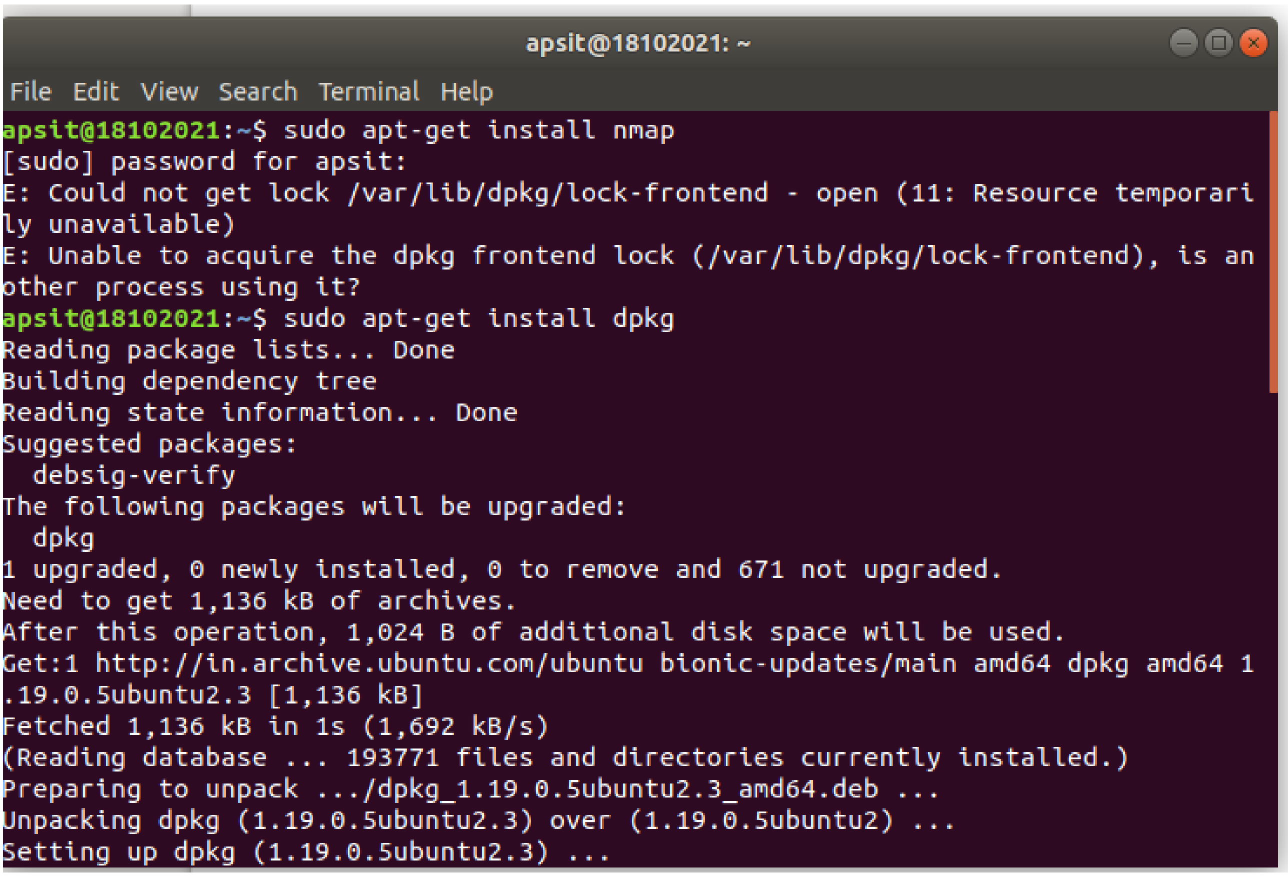
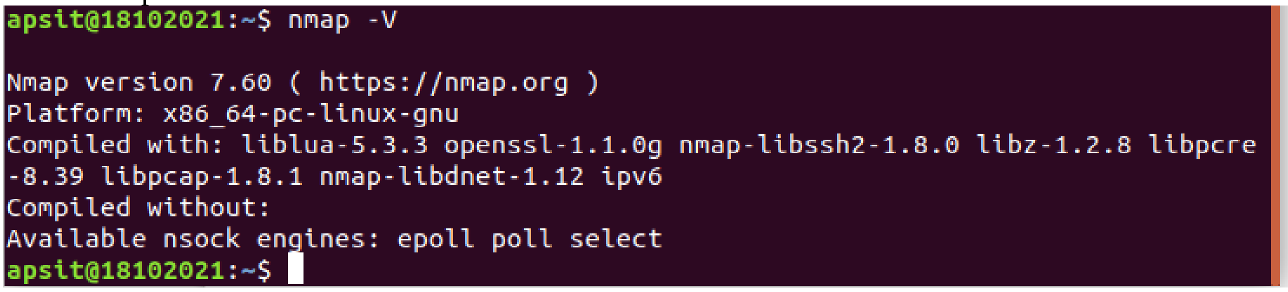
Install nmap



```
apsit@18102021:~$ sudo apt-get install nmap
[sudo] password for apsit:
E: Could not get lock /var/lib/dpkg/lock-frontend - open (11: Resource temporari
ly unavailable)
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontend), is an
other process using it?
apsit@18102021:~$ sudo apt-get install dpkg
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  debsig-verify
The following packages will be upgraded:
  dpkg
1 upgraded, 0 newly installed, 0 to remove and 671 not upgraded.
Need to get 1,136 kB of archives.
After this operation, 1,024 B of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu bionic-updates/main amd64 dpkg amd64 1
.19.0.5ubuntu2.3 [1,136 kB]
Fetched 1,136 kB in 1s (1,692 kB/s)
(Reading database ... 193771 files and directories currently installed.)
Preparing to unpack .../dpkg_1.19.0.5ubuntu2.3_amd64.deb ...
Unpacking dpkg (1.19.0.5ubuntu2.3) over (1.19.0.5ubuntu2) ...
Setting up dpkg (1.19.0.5ubuntu2.3) ...
```

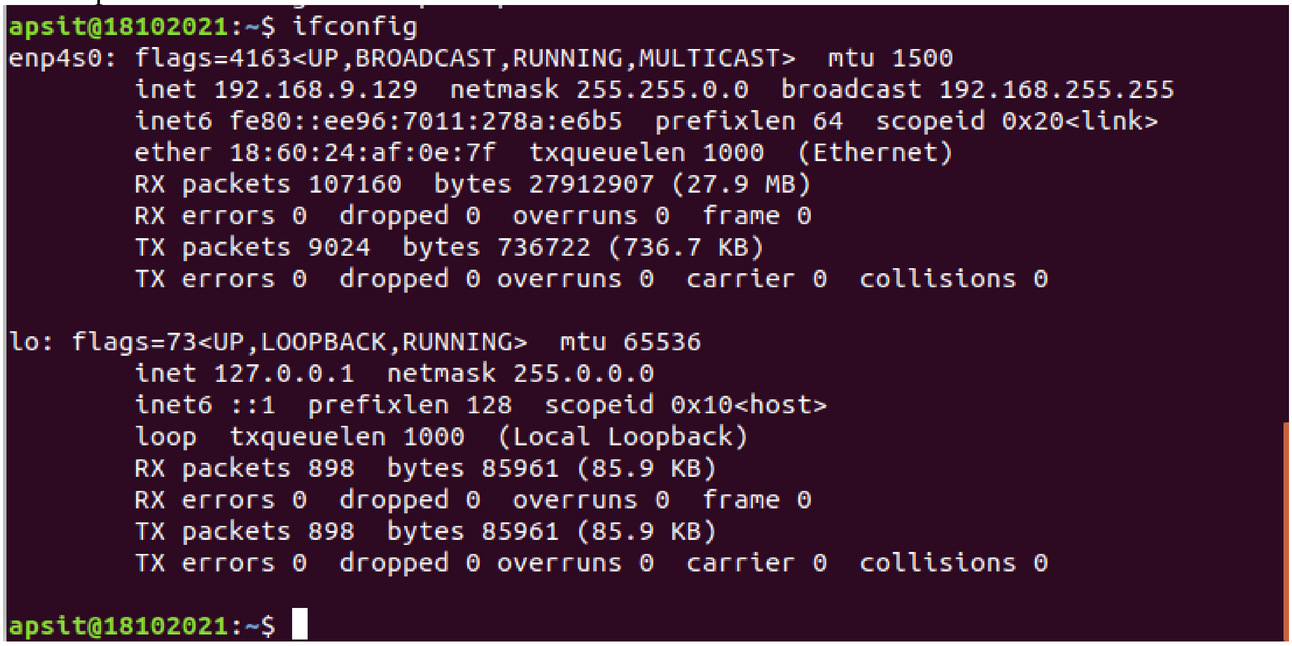
check nmap version



```
apsit@18102021:~$ nmap -V

Nmap version 7.60 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.3.3 openssl-1.1.0g nmap-libssh2-1.8.0 libz-1.2.8 libpcre
-8.39 libpcap-1.8.1 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
apsit@18102021:~$
```

check ip

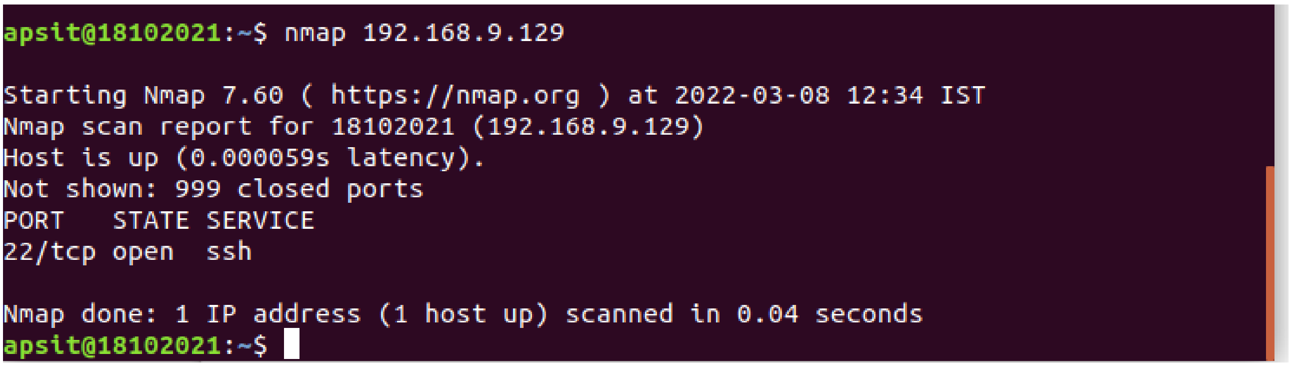


```
apsit@18102021:~$ ifconfig
enp4s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.9.129  netmask 255.255.0.0  broadcast 192.168.255.255
        inet6 fe80::ee96:7011:278a:e6b5  prefixlen 64  scopeid 0x20<link>
        ether 18:60:24:af:0e:7f  txqueuelen 1000  (Ethernet)
        RX packets 107160  bytes 27912907 (27.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 9024  bytes 736722 (736.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 898  bytes 85961 (85.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 898  bytes 85961 (85.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

apsit@18102021:~$
```

details about perticular host

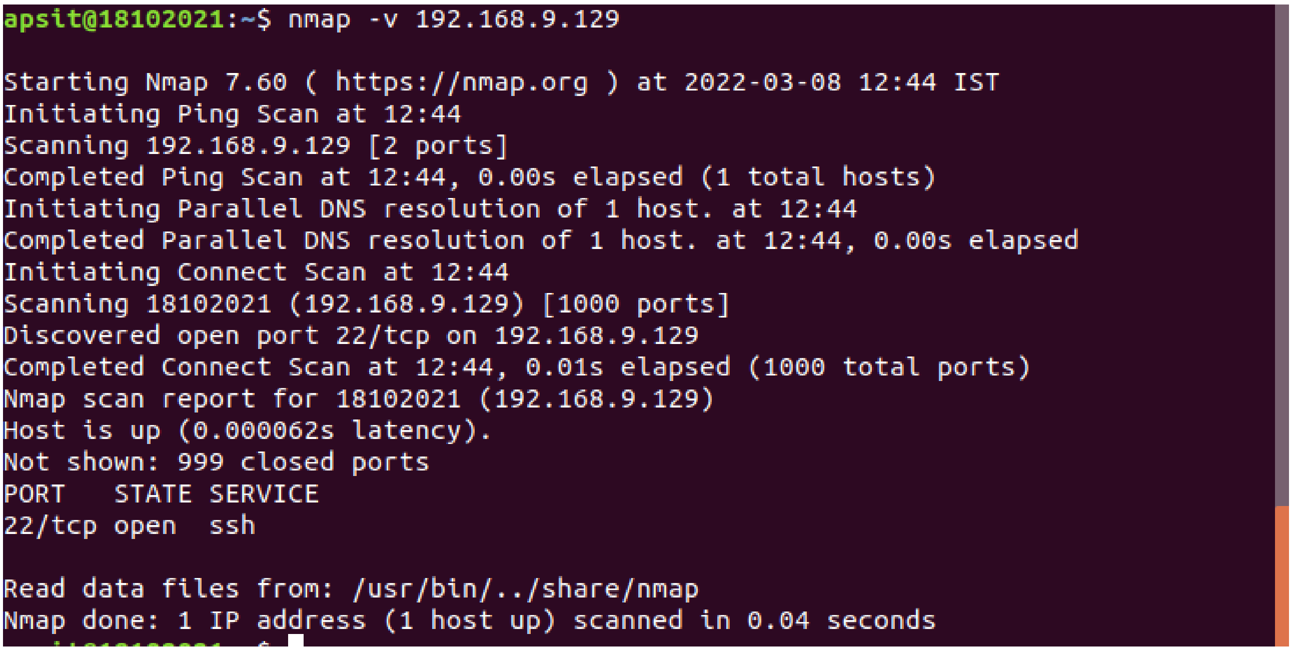


```
apsit@18102021:~$ nmap 192.168.9.129

Starting Nmap 7.60 ( https://nmap.org ) at 2022-03-08 12:34 IST
Nmap scan report for 18102021 (192.168.9.129)
Host is up (0.000059s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
apsit@18102021:~$
```

detail info about host

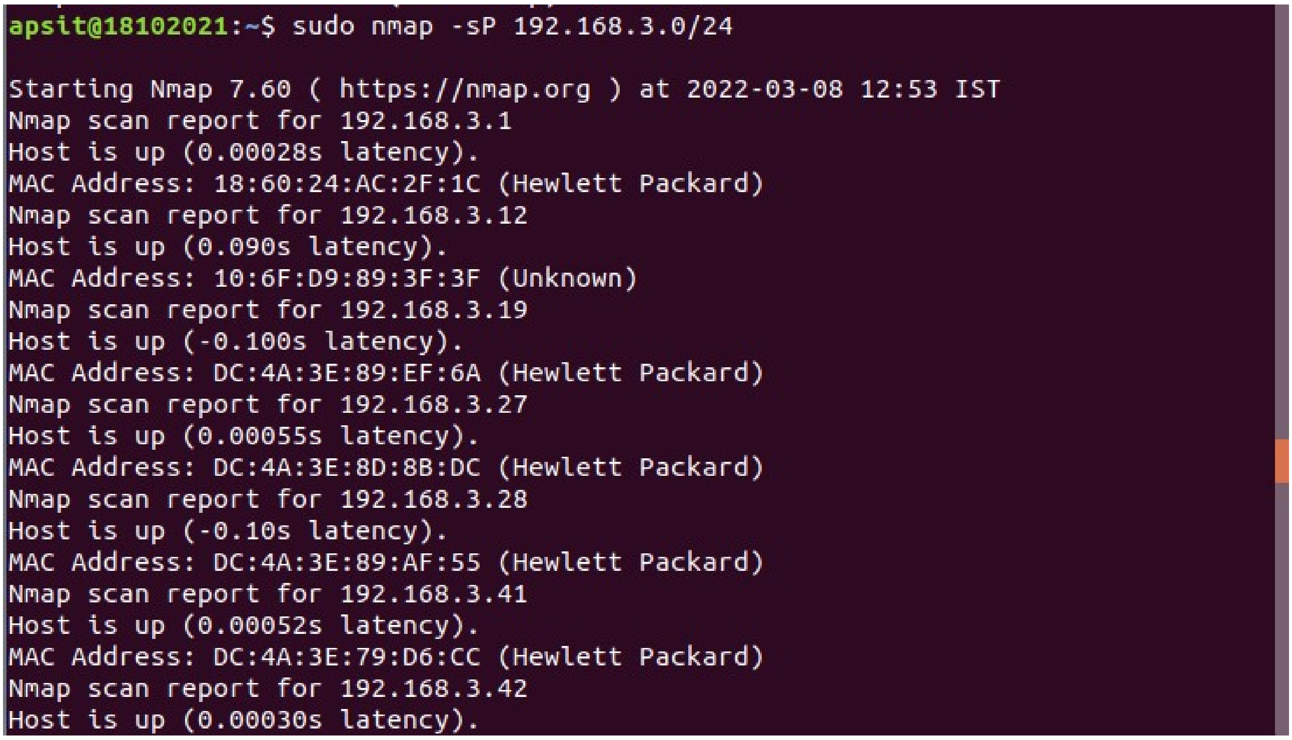


```
apsit@18102021:~$ nmap -v 192.168.9.129

Starting Nmap 7.60 ( https://nmap.org ) at 2022-03-08 12:44 IST
Initiating Ping Scan at 12:44
Scanning 192.168.9.129 [2 ports]
Completed Ping Scan at 12:44, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:44
Completed Parallel DNS resolution of 1 host. at 12:44, 0.00s elapsed
Initiating Connect Scan at 12:44
Scanning 18102021 (192.168.9.129) [1000 ports]
Discovered open port 22/tcp on 192.168.9.129
Completed Connect Scan at 12:44, 0.01s elapsed (1000 total ports)
Nmap scan report for 18102021 (192.168.9.129)
Host is up (0.000062s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
```

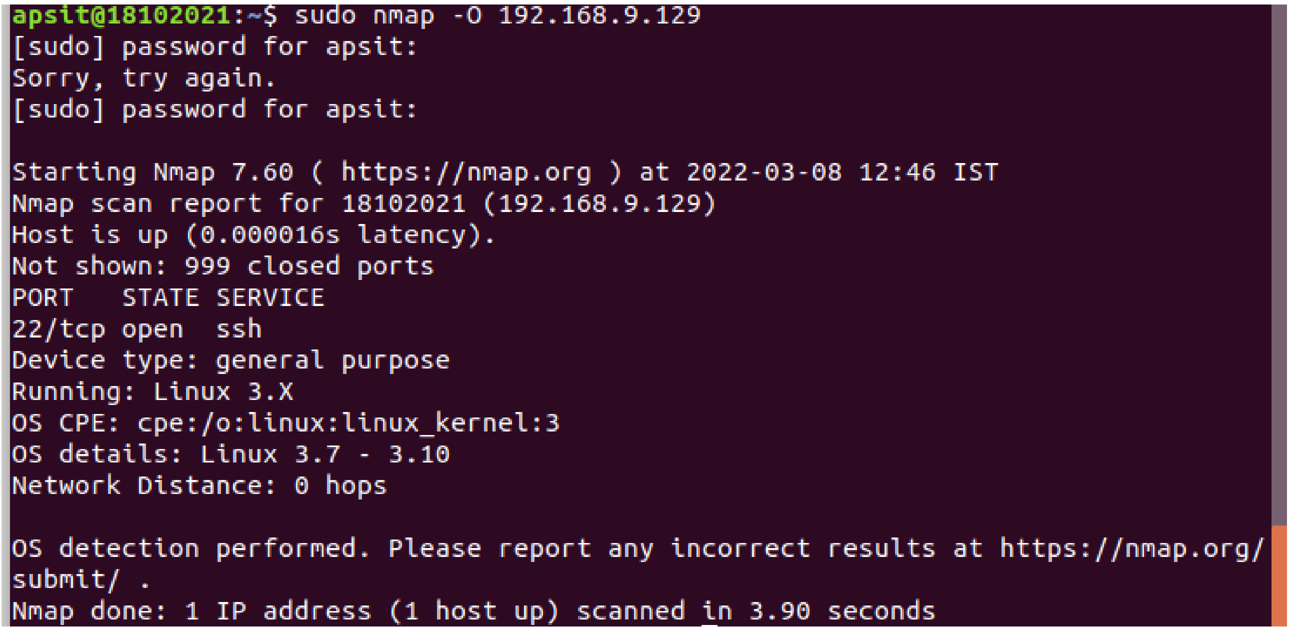
scans network and devices which are up and running



```
apsit@18102021:~$ sudo nmap -sP 192.168.3.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2022-03-08 12:53 IST
Nmap scan report for 192.168.3.1
Host is up (0.00028s latency).
MAC Address: 18:60:24:AC:2F:1C (Hewlett Packard)
Nmap scan report for 192.168.3.12
Host is up (0.090s latency).
MAC Address: 10:6F:D9:89:3F:3F (Unknown)
Nmap scan report for 192.168.3.19
Host is up (-0.100s latency).
MAC Address: DC:4A:3E:89:EF:6A (Hewlett Packard)
Nmap scan report for 192.168.3.27
Host is up (0.00055s latency).
MAC Address: DC:4A:3E:8D:8B:DC (Hewlett Packard)
Nmap scan report for 192.168.3.28
Host is up (-0.10s latency).
MAC Address: DC:4A:3E:89:AF:55 (Hewlett Packard)
Nmap scan report for 192.168.3.41
Host is up (0.00052s latency).
MAC Address: DC:4A:3E:79:D6:CC (Hewlett Packard)
Nmap scan report for 192.168.3.42
Host is up (0.00030s latency).
```

host os details

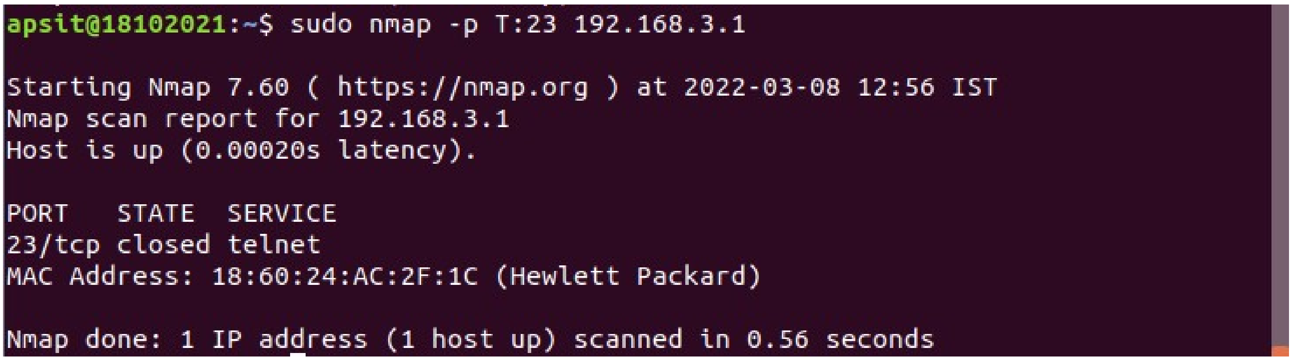


```
apsit@18102021:~$ sudo nmap -O 192.168.9.129
[sudo] password for apsit:
Sorry, try again.
[sudo] password for apsit:

Starting Nmap 7.60 ( https://nmap.org ) at 2022-03-08 12:46 IST
Nmap scan report for 18102021 (192.168.9.129)
Host is up (0.000016s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.7 - 3.10
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.90 seconds
```

scans tcp port 23



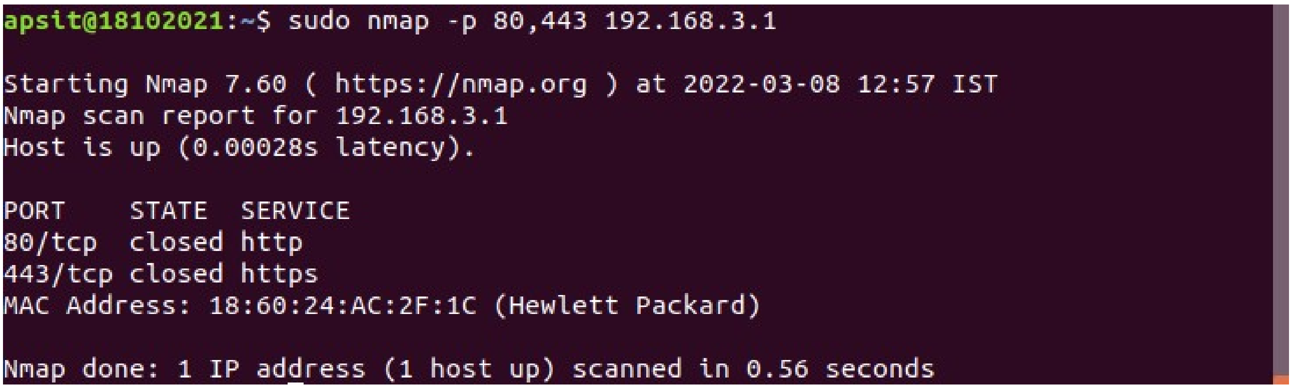
```
apsit@18102021:~$ sudo nmap -p T:23 192.168.3.1

Starting Nmap 7.60 ( https://nmap.org ) at 2022-03-08 12:56 IST
Nmap scan report for 192.168.3.1
Host is up (0.00020s latency).

PORT   STATE  SERVICE
23/tcp closed telnet
MAC Address: 18:60:24:AC:2F:1C (Hewlett Packard)

Nmap done: 1 IP address (1 host up) scanned in 0.56 seconds
```

scans multiple ports



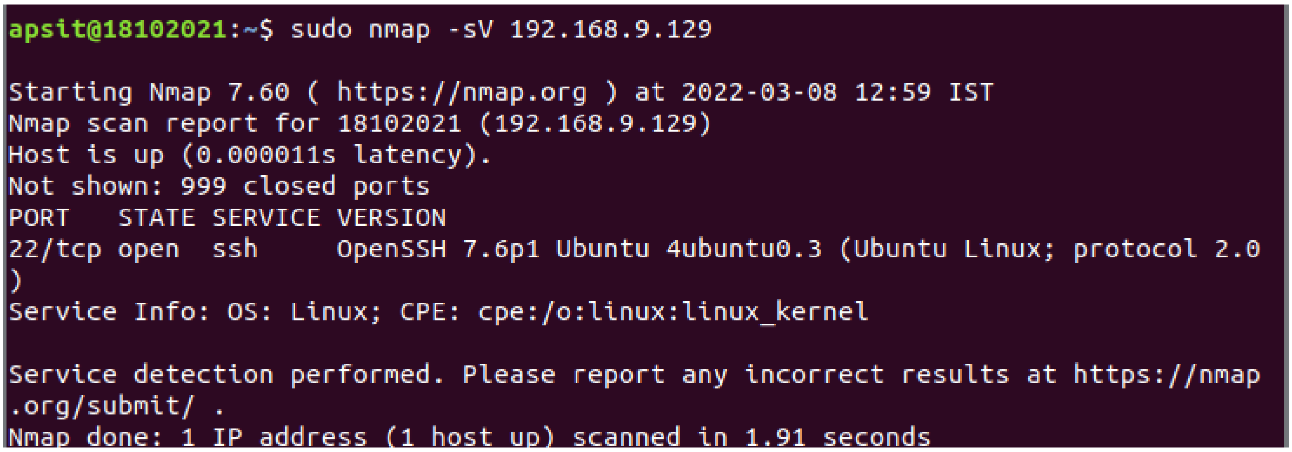
```
apsit@18102021:~$ sudo nmap -p 80,443 192.168.3.1

Starting Nmap 7.60 ( https://nmap.org ) at 2022-03-08 12:57 IST
Nmap scan report for 192.168.3.1
Host is up (0.00028s latency).

PORT    STATE  SERVICE
80/tcp  closed http
443/tcp closed https
MAC Address: 18:60:24:AC:2F:1C (Hewlett Packard)

Nmap done: 1 IP address (1 host up) scanned in 0.56 seconds
```

detect remote service version number

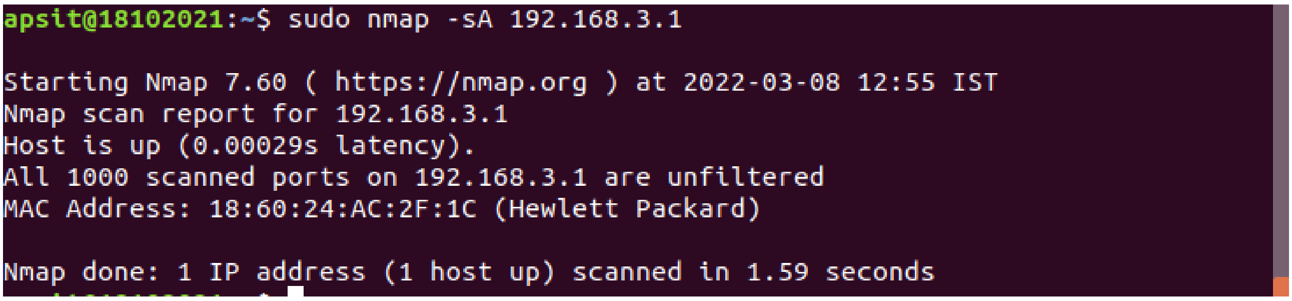


```
apsit@18102021:~$ sudo nmap -sV 192.168.9.129

Starting Nmap 7.60 ( https://nmap.org ) at 2022-03-08 12:59 IST
Nmap scan report for 18102021 (192.168.9.129)
Host is up (0.000011s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0
)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.91 seconds
```

discovers host or network is protected by firewall



```
apsit@18102021:~$ sudo nmap -sA 192.168.3.1

Starting Nmap 7.60 ( https://nmap.org ) at 2022-03-08 12:55 IST
Nmap scan report for 192.168.3.1
Host is up (0.00029s latency).
All 1000 scanned ports on 192.168.3.1 are unfiltered
MAC Address: 18:60:24:AC:2F:1C (Hewlett Packard)

Nmap done: 1 IP address (1 host up) scanned in 1.59 seconds
```