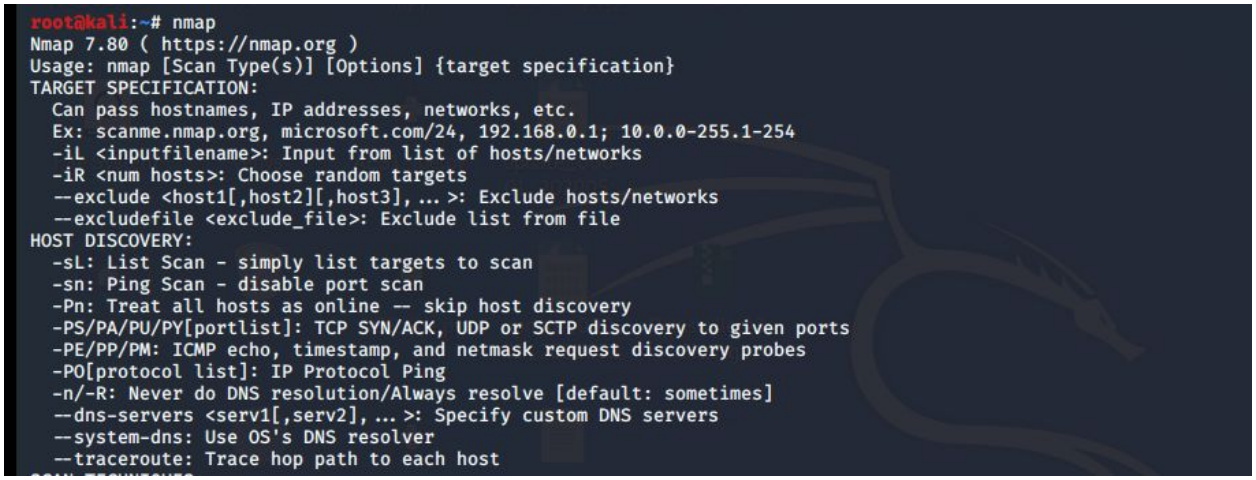
“NMAP”

---S.JOE MATHEW
(192IT159)

Nmap is a network mapper tool which helps us to scan the ip address or host and list various details such as ports,states of the ports etc..

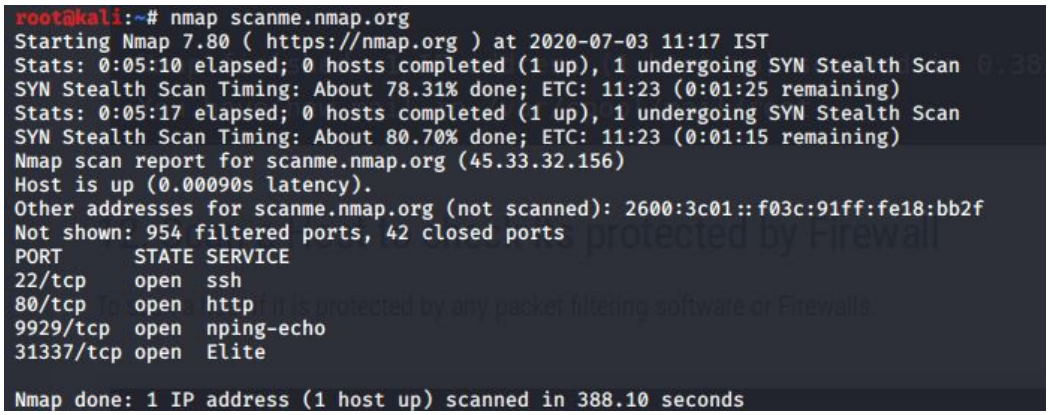


Steps:

Lets see the various commands in nmap

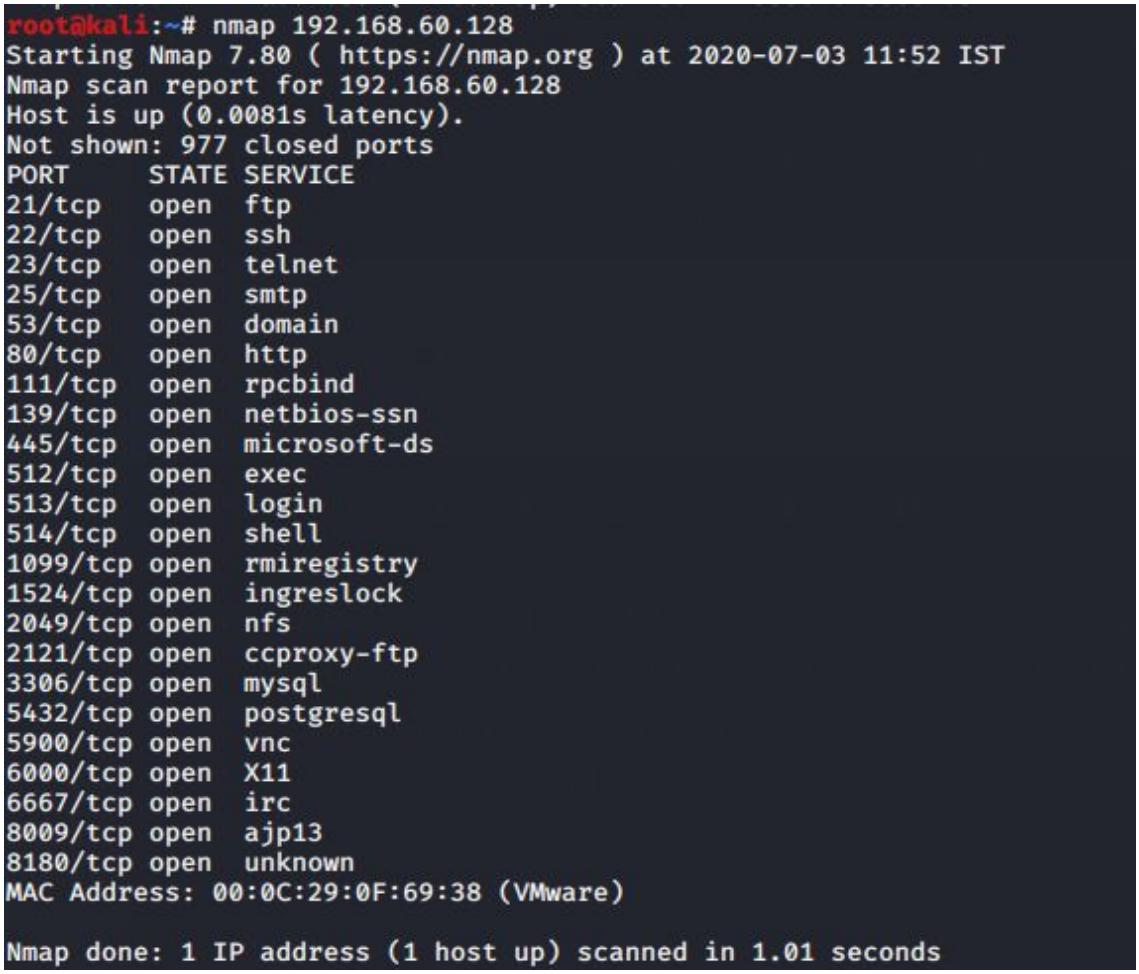
1.Simple host scanning.

Command:**nmap scanme.nmap.org**



2.Scan a particular ip address.

Command : **nmap 192.168.60.128**



3.To get a scan result more powerful than normal we use -v(verbose)

Command: **nmap -v 192.168.60.128**

```
root@kali:~# nmap -v 192.168.60.128
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-03 11:53 IST
Initiating ARP Ping Scan at 11:53
Scanning 192.168.60.128 [1 port]
Completed ARP Ping Scan at 11:53, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:53
Completed Parallel DNS resolution of 1 host. at 11:53, 0.00s elapsed
Initiating SYN Stealth Scan at 11:53
Scanning 192.168.60.128 [1000 ports]
Discovered open port 445/tcp on 192.168.60.128
Discovered open port 23/tcp on 192.168.60.128
Discovered open port 80/tcp on 192.168.60.128
Discovered open port 5900/tcp on 192.168.60.128
Discovered open port 22/tcp on 192.168.60.128
Discovered open port 139/tcp on 192.168.60.128
Discovered open port 53/tcp on 192.168.60.128
Discovered open port 21/tcp on 192.168.60.128
Discovered open port 25/tcp on 192.168.60.128
Discovered open port 3306/tcp on 192.168.60.128
Discovered open port 111/tcp on 192.168.60.128
Discovered open port 2049/tcp on 192.168.60.128
Discovered open port 513/tcp on 192.168.60.128
Discovered open port 6000/tcp on 192.168.60.128
Discovered open port 512/tcp on 192.168.60.128
Discovered open port 514/tcp on 192.168.60.128
Discovered open port 2121/tcp on 192.168.60.128
Discovered open port 5432/tcp on 192.168.60.128
Discovered open port 1099/tcp on 192.168.60.128
Discovered open port 8180/tcp on 192.168.60.128
Discovered open port 8009/tcp on 192.168.60.128
Discovered open port 6667/tcp on 192.168.60.128
Discovered open port 1524/tcp on 192.168.60.128
Completed SYN Stealth Scan at 11:53, 0.29s elapsed (1000 total ports)
Nmap scan report for 192.168.60.128
```

4.To scan the whole subnet .

Command : **nmap 192.168.60.***

```
root@kali:~# nmap  192.168.60.*
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-03 11:55 IST
Nmap scan report for 192.168.60.1
Host is up (0.00067s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
443/tcp  open  https
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
5357/tcp open  wsdapi
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.60.2
Host is up (0.00030s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:FF:97:FA (VMware)

Nmap scan report for 192.168.60.128
Host is up (0.0043s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
```

5.Scan a range of ip addresses .

Command: **nmap 192.168.60.128-132**

```
root@kali:~# nmap  192.168.60.128-132
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-03 11:57 IST
Nmap scan report for 192.168.60.128
Host is up (0.0063s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:0F:69:38 (VMware)

Nmap scan report for 192.168.60.131
Host is up (0.000032s latency).
All 1000 scanned ports on 192.168.60.131 are closed

Nmap done: 5 IP addresses (2 hosts up) scanned in 1.65 seconds
```

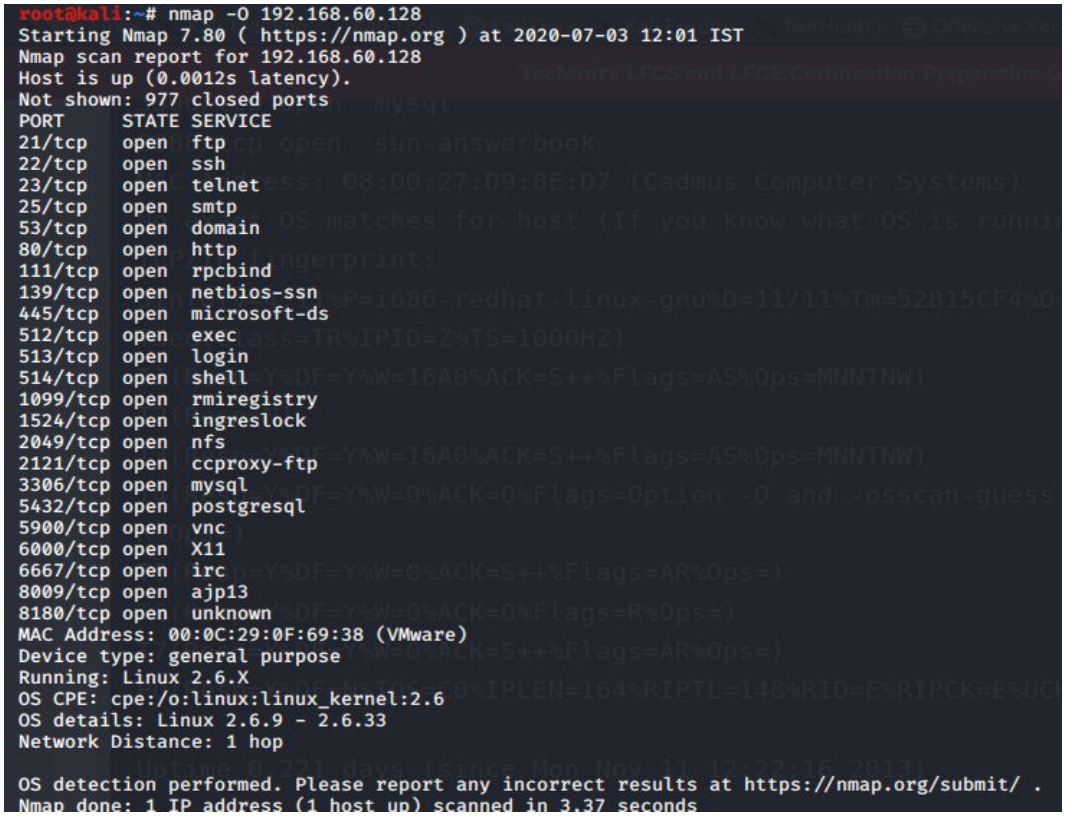
6.To do an aggressive scan which displays all possible information of that ip.

Command: **nmap -A 192.168.60.128**

```
root@kali:~# nmap -A 192.168.60.128
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-03 11:58 IST
Nmap scan report for 192.168.60.128
Host is up (0.0031s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.60.131
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|_ssl-date: 2020-07-03T06:29:31+00:00; +2s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_WITH_MD5
```

7.To Detect the OS Information.

Command: **nmap -O 192.168.60.128**

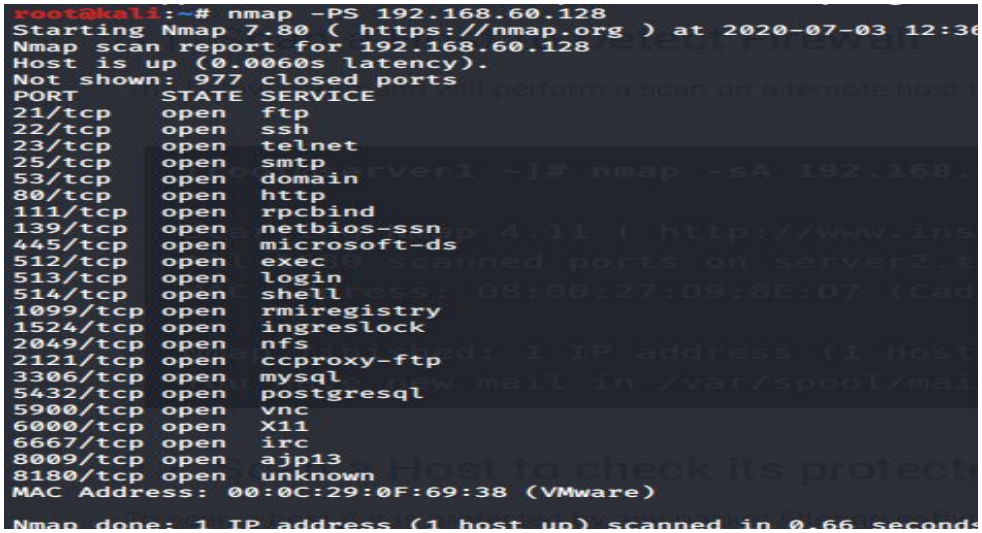


8.To detect there is a firewall

Command : **nmap -sA 192.168.60.128**

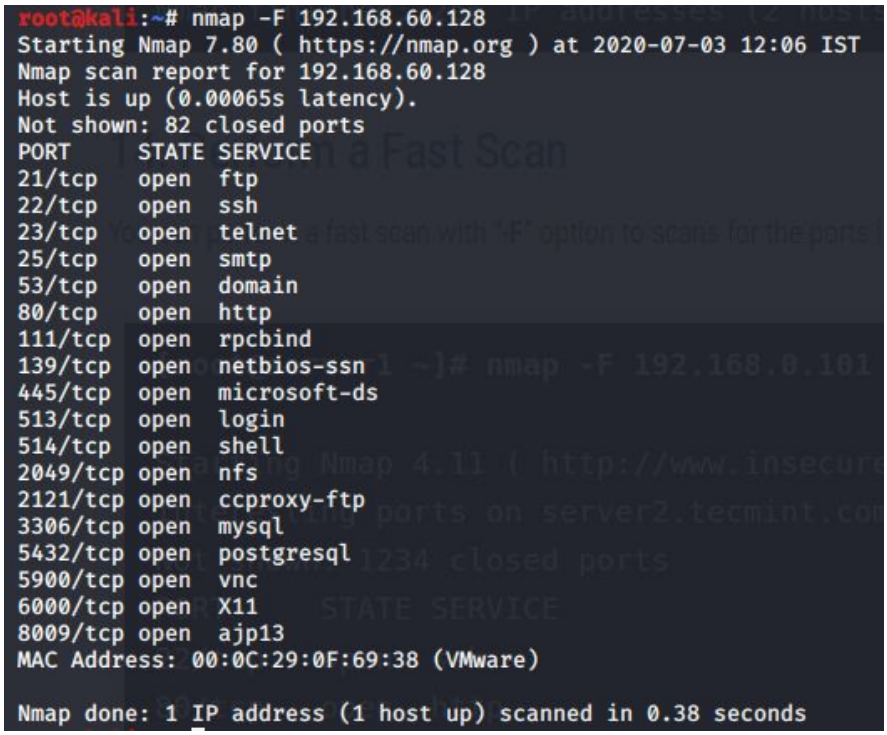
9.If the firewall is blocked i.e there is no ping response we can send TCP acknowledgement packet to get the response.

Command : **nmap -PS 192.168.60.128**



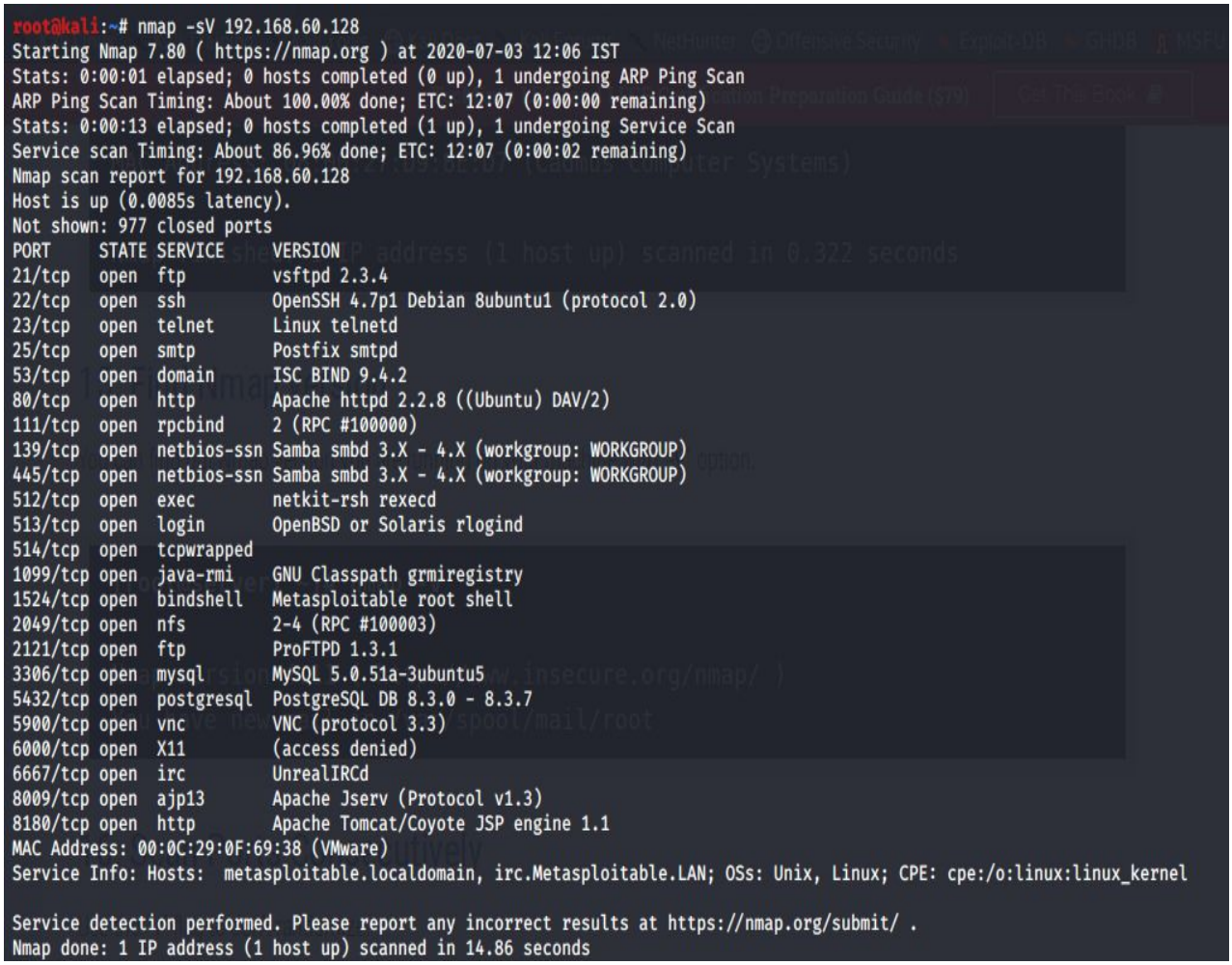
10. If we want to perform a fast scan.

Command: **nmap -F 192.168.60.128**



10. If we want to know the version number .

Command **nmap -sV 192.168.60.128**

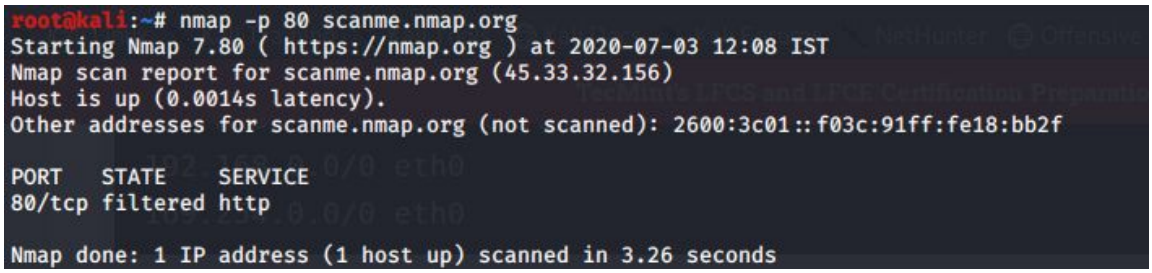


```
root@kali:~# nmap -sV 192.168.60.128
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-03 12:06 IST
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 100.00% done; ETC: 12:07 (0:00:00 remaining)
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 86.96% done; ETC: 12:07 (0:00:02 remaining)
Nmap scan report for 192.168.60.128
Host is up (0.0085s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:0F:69:38 (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, 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 14.86 seconds
```

11. If we want to scan a particular port .

Command :**nmap -p 80 192.168.60.128**



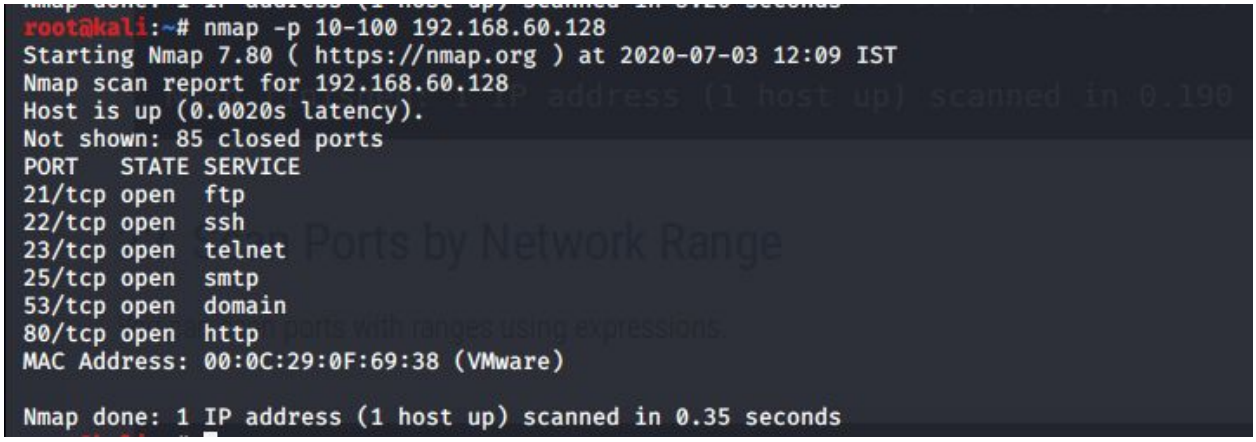
```
root@kali:~# nmap -p 80 scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-03 12:08 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.0014s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f

PORT   STATE    SERVICE
80/tcp filtered http

Nmap done: 1 IP address (1 host up) scanned in 3.26 seconds
```

12. For range of ports.

Command: **nmap -p 10-100 192.168.60.128**



--THANK YOU ...