Practical - 03

Aim:

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.

Objective:

Objective of this module to learn nmap installation & use this to scan different ports.

Scope:

Used for ip spoofing and port scanning

Technology: Networking

Theory:

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>

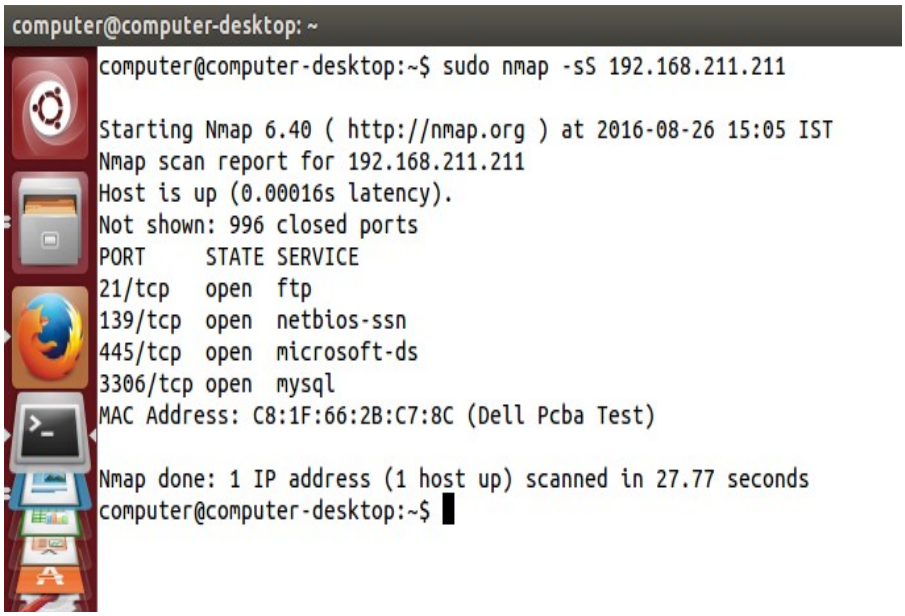
For OS detection: nmap -O <target-host's URL or IP>

For version detection: nmap -sV <target-host's URL or IP>

After the installation of nmap: sudo apt-get install nmap

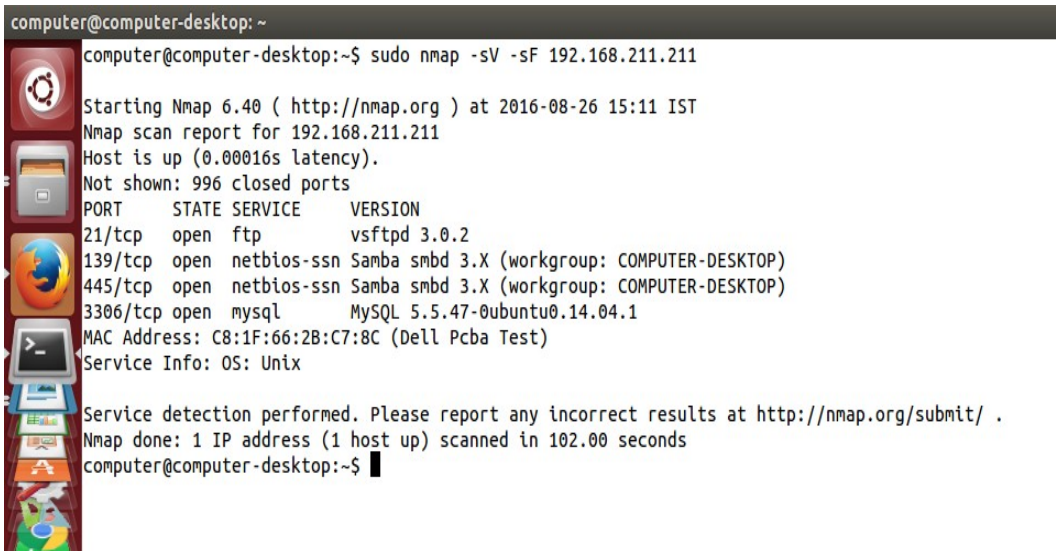
```
computer@computer-desktop: ~
computer@computer-desktop:~$ sudo apt-get install nmap
[sudo] password for computer:
Reading package lists... Done
Building dependency tree
Reading state information... Done
nmap is already the newest version.
The following packages were automatically installed and are no longer required:
  debugedit dh-apparmor diffstat fonts-horai-umefont gnome-exe-thumbnailer
  icoutils intltool-debian libalgorithm-diff-perl libalgorithm-diff-xs-perl
  libalgorithm-merge-perl libapt-pkg-perl libarchive-zip-perl
  libasn1-8-heimdal:i386 libasound2:i386 libasound2-plugins:i386
  libasyncns0:i386 libautodie-perl libcapi20-3 libcapi20-3:i386
  libclass-accessor-perl libdpkg-perl libemail-valid-perl libexif12:i386
  libfile-fcntllock-perl libflac8:i386 libgd3:i386 libgif4:i386
  libglu1-mesa:i386 libgphoto2-6:i386 libgphoto2-port10:i386
  libgssapi3-heimdal:i386 libgstreamer-plugins-base0.10-0:i386
  libgstreamer0.10-0:i386 libhcrypto4-heimdal:i386 libheimbase1-heimdal:i386
  libheimntlm0-heimdal:i386 libhx509-5-heimdal:i386 libieee1284-3:i386
  libio-pty-perl libio-string-perl libipc-run-perl libipc-system-simple-perl
  libjack-jackd2-0:i386 libkrb5-26-heimdal:i386 liblcms2-2:i386
  libldap-2.4-2:i386 liblist-moreutils-perl libltdl-dev libltdl7:i386
  libmail-sendmail-perl libmpg123-0 libmpg123-0:i386 libnet-dns-perl
  libnet-domain-tld-perl libnet-ip-perl libodbc1 libogg0:i386 libopenal-data
  libopenal1 libopenal1:i386 libosmesa6 libosmesa6:i386
  libp11-kit-gnome-keyring:i386 libparse-debianchangelog-perl
  libperlio-gzip-perl libpulse0:i386 libroken18-heimdal:i386 librpmbuild3
  librpmsign1 libsamplerate0:i386 libsane:i386 libsasl2-2:i386
  libsasl2-modules:i386 libsasl2-modules-db:i386 libsndfile1:i386
  libspeexdsp1:i386 libsub-identify-perl libsub-name-perl
  libsys-hostname-long-perl libtext-levenshtein-perl libusb-1.0-0:i386
  libv4l-0:i386 libv4lconvert0:i386 libvorbis0a:i386 libvorbisenc2:i386
  libvpx1:i386 libwind0-heimdal:i386 libwrap0:i386 libxcomposite1:i386
  libxcursor1:i386 libxinerama1:i386 libxpm4:i386 libxrandr2:i386
  ocl-icd-libopencl1:i386 odbcinst odbcinst1debian2 p11-kit-modules:i386 p7zip
  patchutils po-debconf rpm unixodbc wine wine-gecko2.21 wine-gecko2.21:i386
  wine-mono0.0.8 wine1.6 wine1.6-amd64 wine1.6-i386:i386 winetricks
Use 'apt-get autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 518 not upgraded.
computer@computer-desktop:~$
```

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



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.



-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.

```
computer@computer-desktop: ~
computer@computer-desktop:~$ nmap -p 1-1000  192.168.211.211

Starting Nmap 6.40 ( http://nmap.org ) at 2016-08-26 13:39 IST
Nmap scan report for 192.168.211.211
Host is up (0.00046s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
21/tcp  open  ftp
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
computer@computer-desktop:~$
```

-O (Enable OS detection)

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

```
computer@computer-desktop:~$ nmap -A 192.168.211.211

Starting Nmap 6.40 ( http://nmap.org ) at 2016-08-26 13:42 IST
Nmap scan report for 192.168.211.211
Host is up (0.00086s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 3.0.2
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: COMPUTER-DESKTOP)
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: COMPUTER-DESKTOP)
3306/tcp open  mysql       MySQL 5.5.47-0ubuntu0.14.04.1
| mysql-info: Protocol: 10
| Version: 5.5.47-0ubuntu0.14.04.1
| Thread ID: 41
| Some Capabilities: Long Passwords, Connect with DB, Compress, ODBC, Transactio
ns, Secure Connection
| Status: Autocommit
|_Salt: iX]MH_&=
Service Info: OS: Unix

Host script results:
|_nbstat: NetBIOS name: , NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
| smb-os-discovery:
|   OS: Unix (Samba 4.1.6-Ubuntu)
|   Computer name: computer-desktop
|   NetBIOS computer name: COMPUTER-DESKTOP
|   Domain name:
|   FQDN: computer-desktop
|_  System time: 2016-08-26T13:42:47+05:30
| smb-security-mode:
|   Account that was used for smb scripts: guest
|   User-level authentication
|   SMB Security: Challenge/response passwords supported
|_  Message signing disabled (dangerous, but default)
|_smbv2-enabled: Server supports SMBv2 protocol

Service detection performed. Please report any incorrect results at http://nmap.
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.55 seconds
computer@computer-desktop:~$
```

--open (Show only open (or possibly open) ports)

Sometimes you only care about ports you can actually connect to (open ones), and don´t want results cluttered with closed, filtered, and closed|filtered ports.

```
computer@computer-desktop:~$ nmap --open 192.168.211.211

Starting Nmap 6.40 ( http://nmap.org ) at 2016-08-26 15:17 IST
Nmap scan report for 192.168.211.211
Host is up (0.00021s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
computer@computer-desktop:~$
```

-sT (TCP connect scan)

TCP connect scan is the default TCP scan type when SYN scan is not an option. This is the case when a user does not have raw packet privileges or is scanning IPv6 networks. Instead of writing raw packets as most other scan types do, Nmap asks the underlying operating system to establish a connection with the target machine and port by issuing the connect system call along with spoofing.

```
computer@computer-desktop:~$ nmap -sT 192.168.211.211

Starting Nmap 6.40 ( http://nmap.org ) at 2016-08-26 14:16 IST
Nmap scan report for 192.168.211.211
Host is up (0.00085s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
computer@computer-desktop:~$
```

-PS port list (TCP SYN Ping)

This option sends an empty TCP packet with the SYN flag set. The default destination port is 80 (configurable at compile time by changing DEFAULT_TCP_PROBE_PORT_SPEC in nmap.h).
Alternate ports can be specified as a parameter.
The syntax is the same as for the -p except that port type specifiers like T: are not allowed.

```
computer@computer-desktop: ~
computer@computer-desktop:~$ sudo nmap -sT -PS 192.168.211.211

Starting Nmap 6.40 ( http://nmap.org ) at 2016-08-26 15:25 IST
Nmap scan report for 192.168.211.211
Host is up (0.0011s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
MAC Address: C8:1F:66:2B:C7:8C (Dell Pcba Test)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
computer@computer-desktop:~$
```

nmap –iflist

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

```
computer@computer-desktop: ~
computer@computer-desktop:~$ nmap -iflist

Starting Nmap 6.40 ( http://nmap.org ) at 2016-08-26 15:28 IST
************************INTERFACES************************
DEV   (SHORT) IP/MASK                      TYPE     UP   MTU   MAC
eth0  (eth0)  192.168.211.18/24            ethernet up   1500  C8:1F:66:2B:CB:E9
eth0  (eth0)  fe80::ca1f:66ff:fe2b:cbe9/64 ethernet up   1500  C8:1F:66:2B:CB:E9
wlan0 (wlan0) (null)/0                     ethernet down 1500  54:35:30:26:9F:56
lo    (lo)    127.0.0.1/8                  loopback up   65536
lo    (lo)    ::1/128                      loopback up   65536

**************************ROUTES**************************
DST/MASK                      DEV  METRIC GATEWAY
192.168.211.0/24              eth0 1
0.0.0.0/0                     eth0 0      192.168.211.253
::1/128                       lo   0
fe80::ca1f:66ff:fe2b:cbe9/128 lo   0
ff02::fb/128                  eth0 0
fe80::/64                     eth0 256
ff00::/8                      eth0 256

computer@computer-desktop:~$
```

-sU (Scan UDP ports)

This is use to find only UDP ports currently open on target system.

```
computer@computer-desktop:~$ sudo nmap -sU 192.168.211.211

Starting Nmap 6.40 ( http://nmap.org ) at 2016-08-26 14:18 IST



Nmap scan report for 192.168.211.211
Host is up (0.00020s latency).
Not shown: 995 closed ports
PORT     STATE         SERVICE
68/udp   open|filtered dhcpc
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
631/udp  open|filtered ipp
5353/udp open          zeroconf
MAC Address: C8:1F:66:2B:C7:8C (Dell Pcba Test)

Nmap done: 1 IP address (1 host up) scanned in 1095.64 seconds
computer@computer-desktop:~$
computer@computer-desktop:~$
computer@computer-desktop:~$
computer@computer-desktop:~$
```

Conclusion: NMap Port scanner is studied with its various commands.