Workshop 12 – NMAP

Description:

The nmap utility is used for port scanning and finding out all the ways a computer communicates with other computers on a network. You can find open ports on a server or computer and find what services are using those ports. It can even determine what operating system is running on the server and much more.

Part 1: Installation:

Step 1: Check the availability of Nmap packages

```
# rpm –q nmap
# rpm –q nmap-frontend    (check for nmap graphical front-end)
```

Step 2: install the packages if not exists.

```
# yum install nmap nmap-frontend
```

Step 3: find out Nmap version

```
# nmap –version
```

Part 2: Scan a single host or an IP address

Step 1: Scan ip address

```
# nmap 127.0.0.1
```

Step 2: Scan a hostname

```
# nmap localhost
```

Step 3: Scan a host name with more info

```
# nmap -v localhost
```

Part 3: Scan multiple IP address or subnet

```
# nmap 192.168.1.1 192.168.1.2 192.168.1.3
# nmap 192.168.1.1,2,3
# nmap 192.168.1.1-3
# nmap 192.168.1.*              (Scan entire subnet)
# nmap 192.168.1.0/24           (Scan entire subnet)
```

Part 4: Read list of hosts/networks from a file

This is useful to scan a large number of hosts/networks.

```
# cat > /var/list
192.168.1.1
192.168.1.2



# nmap –iL /var/list
```

Part 5: excluding hosts/networks

```
# nmap 192.168.1.0/24 --exclude 192.168.1.5
# nmap -iL /var/list --excludefile /var/exclude
```

Part 6: Turn on OS and version detection scanning script

```
# nmap -A 192.168.1.1
# nmap -v -A 192.168.1.1
# nmap -A -iL /var/list
```

Part 7: Find out if a host/network is protected by a firewall

```
# nmap -sA 192.168.1.1
```

Part 8: Scan a host when protected by the firewall

```
# nmap -PN www.lpi.org
```

Part 9: Scan a network and find out which servers and devices are up and running

```
# nmap -sP 192.168.1.0/24
```

Part 10: perform a fast scan

```
# nmap -F 192.168.1.1
```

Part 11: Show host interfaces and routes

```
# nmap –iflist
```

Part 12: scan specific ports

map -p [port] hostName

Step 1: Scan port 80

```
# nmap -p 80 192.168.1.1
```

Step 2: Scan TCP port 80

```
# nmap -p T:80 192.168.1.1
```

Step 3: Scan UDP port 53

```
# nmap -p U:53 192.168.1.1
```

Step 4: Scan two ports

```
# nmap -p 80,443 192.168.1.1
```

Step 5: Scan port ranges

```
# nmap -p 80-200 192.168.1.1
```

Step 6: Combine all options

```
# nmap -p U:53,111,137,T:21-25,80,139,8080 192.168.1.1
```

Part 13: The fastest way to scan all your devices/computers for open ports ever

```
# nmap -T5 192.168.1.0/24
```

Part 14: detect remote services (server / daemon) version numbers

```
# nmap -sV 192.168.1.1
```

Part 15: can a host for UDP services (UDP scan)

```
# nmap -sU 192.168.1.1
```

Part 16: Save the result on the file

```
# nmap –T5 192.168.1.1 –o /var/file
```

Part 17: Save the result on the file with xml format

```
# nmap –T5 192.168.1.1 –ox /var/file
# firefox /var/file
```

Part 18: running nmap-frontend

```
# nmapfe
```