NMAP is an Open Source Tool

Use for Network Discovery & Security Auditing

Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

Nmap features include:

- **Host discovery –** Identifying hosts on a network. For example, listing the hosts that respond to TCP and/or ICMP requests or have a particular port open.
- **Port scanning –** Enumerating the open ports on target hosts.
- **Version detection –** Interrogating network services on remote devices to determine application name and version number.
- **OS detection –** Determining the operating system and hardware characteristics of network devices.
- Scriptable interaction with the target
- Nmap can provide further information on targets, including reverse DNS names, device types, and MAC addresses

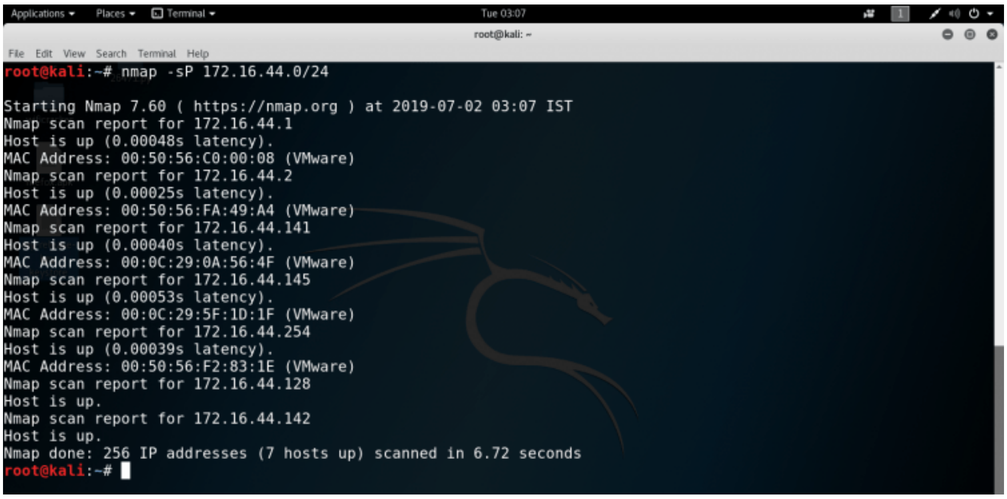
Let's get started with installation and how to use nmap:

Install nmap on your kali machine, type command **-** sudo apt install nmap

In order to run the ifconfig command, we need to have net-tools installed on machine, type command - sudo apt install net-tools

Basic commands,

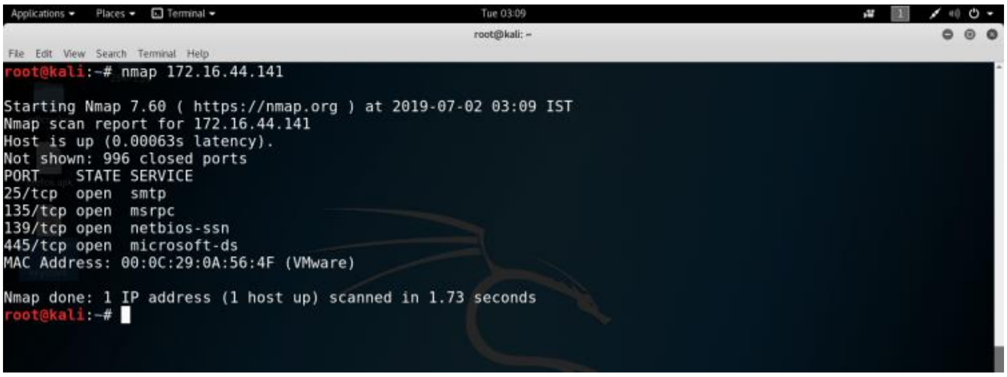
Scan network for connected devices



```
root@kali:~# nmap -sP 172.16.44.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2019-07-02 03:07 IST
Nmap scan report for 172.16.44.1
Host is up (0.00048s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 172.16.44.2
Host is up (0.00025s latency).
MAC Address: 00:50:56:FA:49:A4 (VMware)
Nmap scan report for 172.16.44.141
Host is up (0.00040s latency).
MAC Address: 00:0C:29:0A:56:4F (VMware)
Nmap scan report for 172.16.44.145
Host is up (0.00053s latency).
MAC Address: 00:0C:29:5F:1D:1F (VMware)
Nmap scan report for 172.16.44.254
Host is up (0.00039s latency).
MAC Address: 00:50:56:F2:83:1E (VMware)
Nmap scan report for 172.16.44.128
Host is up.
Nmap scan report for 172.16.44.142
Host is up.
Nmap done: 256 IP addresses (7 hosts up) scanned in 6.72 seconds
root@kali:~#
```

Scan a single IP

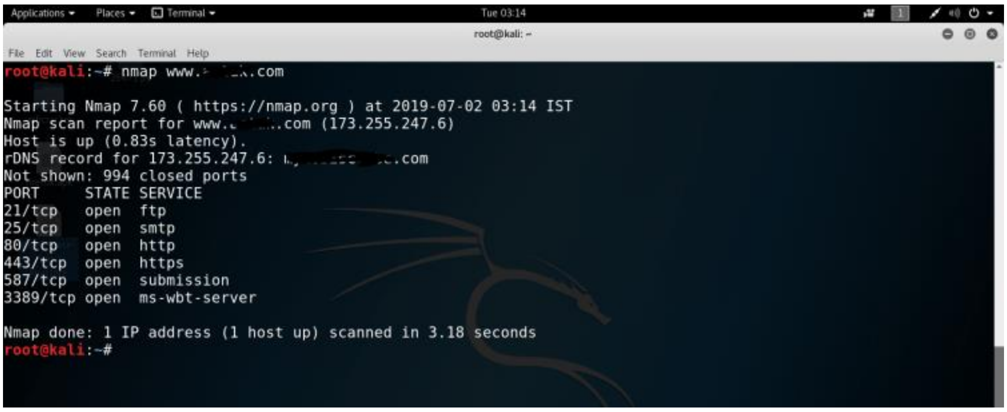


```
root@kali:~# nmap 172.16.44.141

Starting Nmap 7.60 ( https://nmap.org ) at 2019-07-02 03:09 IST
Nmap scan report for 172.16.44.141
Host is up (0.00063s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
25/tcp  open  smtp
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:0A:56:4F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.73 seconds
root@kali:~#
```

Scan a host

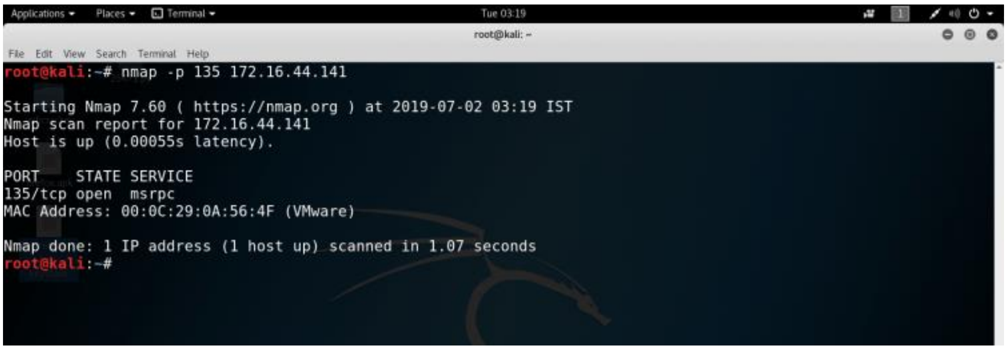


```
root@kali:~# nmap www.[redacted].com

Starting Nmap 7.60 ( https://nmap.org ) at 2019-07-02 03:14 IST
Nmap scan report for www.[redacted].com (173.255.247.6)
Host is up (0.83s latency).
rDNS record for 173.255.247.6: [redacted].com
Not shown: 994 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
80/tcp   open  http
443/tcp  open  https
587/tcp  open  submission
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 3.18 seconds
root@kali:~#
```

Scan a port



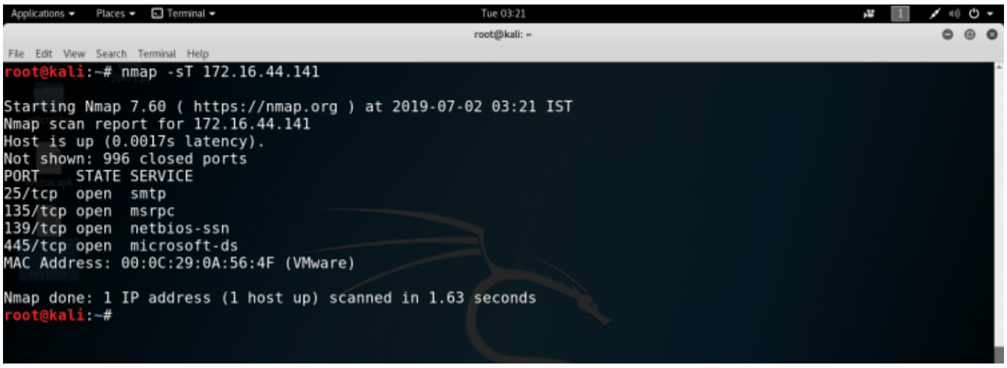
```
root@kali:~# nmap -p 135 172.16.44.141

Starting Nmap 7.60 ( https://nmap.org ) at 2019-07-02 03:19 IST
Nmap scan report for 172.16.44.141
Host is up (0.00055s latency).

PORT    STATE SERVICE
135/tcp open  msrpc
MAC Address: 00:0C:29:0A:56:4F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.07 seconds
root@kali:~#
```

Scan using TCP connect



```
root@kali:~# nmap -sT 172.16.44.141

Starting Nmap 7.60 ( https://nmap.org ) at 2019-07-02 03:21 IST
Nmap scan report for 172.16.44.141
Host is up (0.0017s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
25/tcp  open  smtp
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:0A:56:4F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.63 seconds
root@kali:~#
```

Some more basic commands which we can use are :

Target Selection

- Scan a range of IPs – nmap 172.16.44.10-200
- Scan a subnet – nmap 172.16.44.0/24
- Scan targets from Text file – nmap -iL ips.txt

Port Selection

- Scan a range of ports – nmap -p 1-100 172.16.44.141
- Scan 100 common ports – nmap -F 172.16.44.141
- Scan all ports – nmap -p- 172.16.44.141
- Specify UDP or TCP scan- nmap -p U:137,T:139 172.16.44.141

Scan Types

- Scan using TCP SYN scan – nmap -sS 172.16.44.141
- Scan UDP ports – nmap -sU -p 123,161,162 172.16.44.141
- Scan Selected ports (Ignore Discovery) – nmap -Pn -F 172.16.44.141

Service and OS Detection

- Detect OS and Services – nmap -A 172.16.44.141
- Standard service detection – nmap -sV 172.16.44.141
- Aggressive service detection – nmap -sV –version-intensity 5 172.16.44.141

Output Formats

- Save default output to file – nmap -oN result.txt 172.16.44.141
- Save results as XML – nmap -oX resultxml.xml 172.16.44.141
- Save formatted results (Grep) – nmap -oG formattable.txt 172.16.44.141
- Save in all formats – nmap -oA allformats 172.16.44.141

Scripting Engine

- Scan using default safe scripts – nmap -sV -sC 172.16.44.141
- Get help for a script – nmap –script-help=ssl-heartbleed
- Scan using a specific script – nmap -sV -p 443 -script=ssl-heartbleed 172.16.44.141
- Update script database – nmap –script-updatedb

Some Useful NSE Scripts

- Scan for UDP DDOS reflectors – nmap -sU -A -PN -n -pU:19,53,123,161 -script=ntp-monlist,dns-recursion,snmp-sysdescr 172.16.44.2/24
- Gather page titles from HTTP Servers – nmap –script=http-title 172.16.44.141
- Get HTTP headers of web services – nmap –script=http-headers 172.16.44.141
- Find web apps from known paths – nmap –script=http-enum 172.16.44.141
- Find exposed Netbios servers – nmap -sU –script nbtstat.nse -p 137 172.16.44.141