Exercise Lab Manual: Network scanning using Nmap

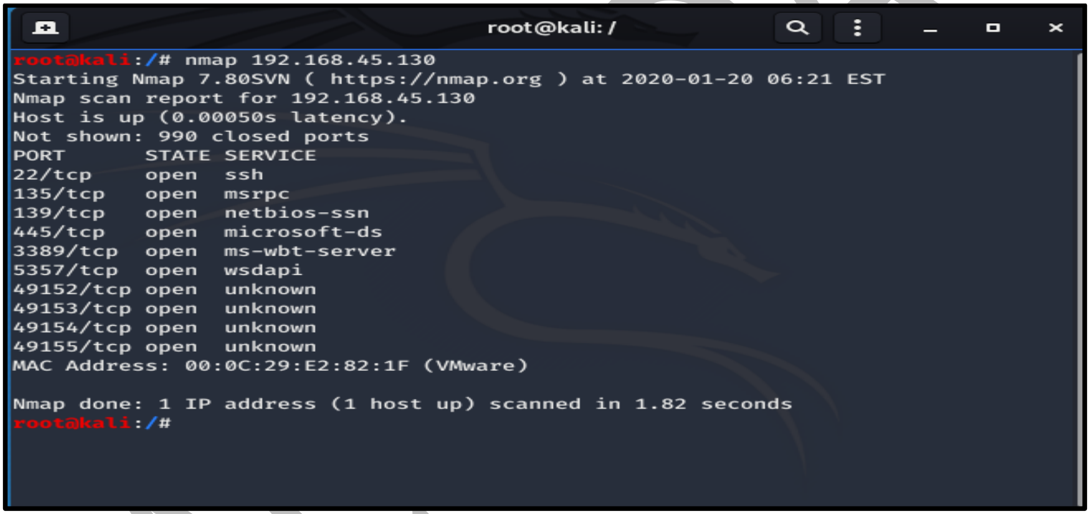
Nmap (Network Mapper) is a free and open-source network scanner. It is used to discover hosts and services running on them in a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection, etc. These features are extensible using scripts that provide more advanced service detection. In this exercise, you will learn, how to use Nmap for various scanning activities and use Nmap scripts for important activities.

1. **Basic Nmap Scan against IP or host**

nmap 192.168.45.130

Now, if you want to scan a hostname, simply replace the IP for the host

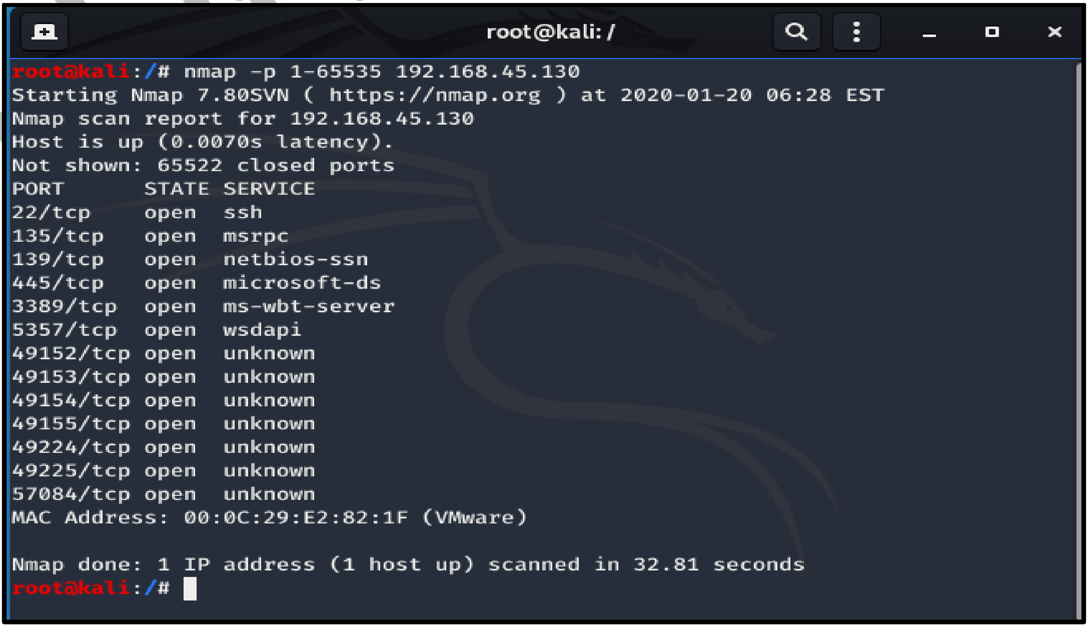
For example, nmap cdac.in



```
root@kali:/# nmap 192.168.45.130
Starting Nmap 7.80SVN ( https://nmap.org ) at 2020-01-20 06:21 EST
Nmap scan report for 192.168.45.130
Host is up (0.00050s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
MAC Address: 00:0C:29:E2:82:1F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.82 seconds
root@kali:/#
```

2. **Scan specific ports or scan entire port ranges on a local or remote server.**

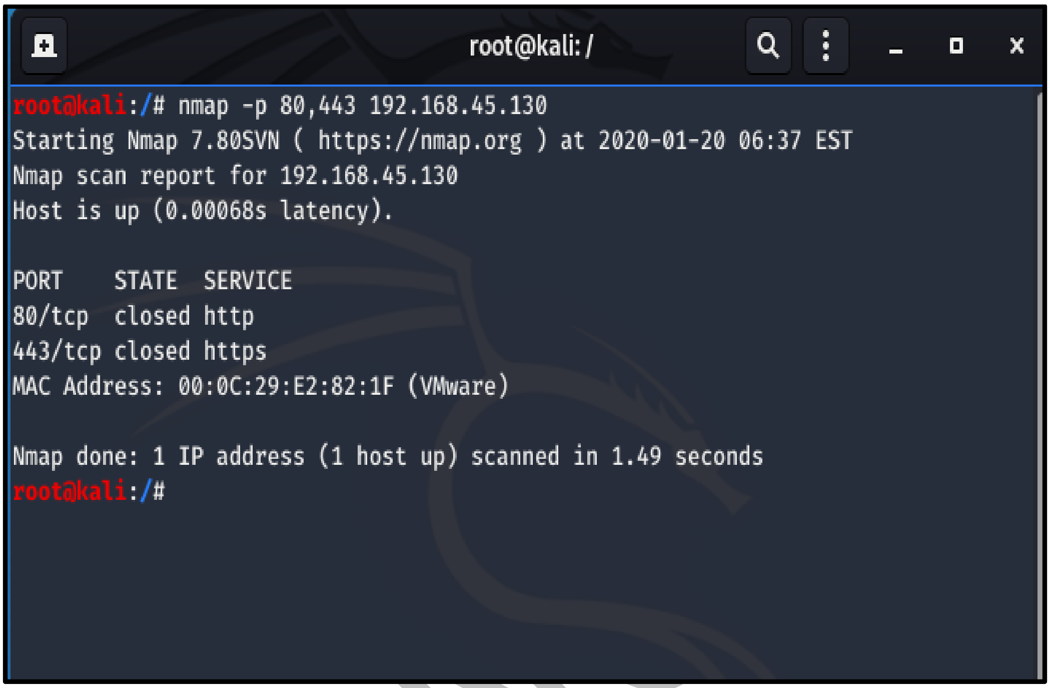
nmap -p 1-65535 localhost
In this example, we scanned all 65535 ports for our local host computer.
Nmap is able to scan all possible ports.



```
root@kali:/# nmap -p 1-65535 192.168.45.130
Starting Nmap 7.80SVN ( https://nmap.org ) at 2020-01-20 06:28 EST
Nmap scan report for 192.168.45.130
Host is up (0.0070s latency).
Not shown: 65522 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49224/tcp open  unknown
49225/tcp open  unknown
57084/tcp open  unknown
MAC Address: 00:0C:29:E2:82:1F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 32.81 seconds
root@kali:/#
```

3. **Nmap is able to scan all possible ports, but it can also scan specific ports**

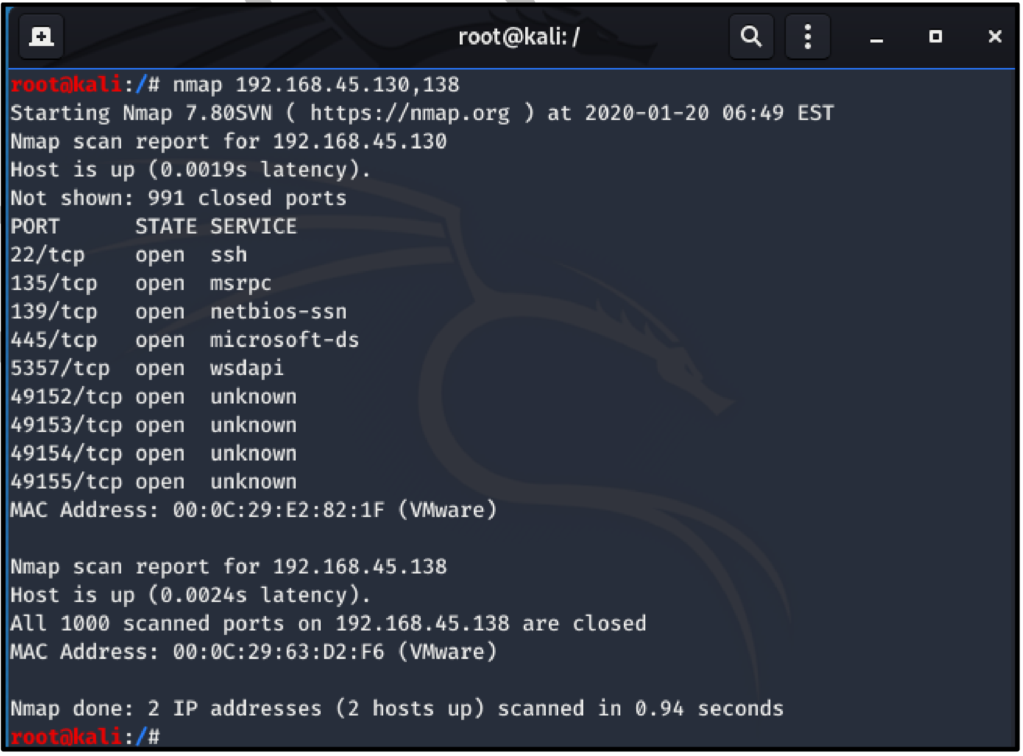
nmap -p 80,443 192.168.45.130
You can also scan specific ports, which will report faster results.



```
root@kali:/# nmap -p 80,443 192.168.45.130
Starting Nmap 7.80SVN ( https://nmap.org ) at 2020-01-20 06:37 EST
Nmap scan report for 192.168.45.130
Host is up (0.00068s latency).

PORT    STATE  SERVICE
80/tcp  closed http
443/tcp closed https
MAC Address: 00:0C:29:E2:82:1F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.49 seconds
root@kali:/#
```

4. **Scan multiple IP addresses**

Nmap -p 192.168.45.130,138
You can also scan consecutive IP addresses.



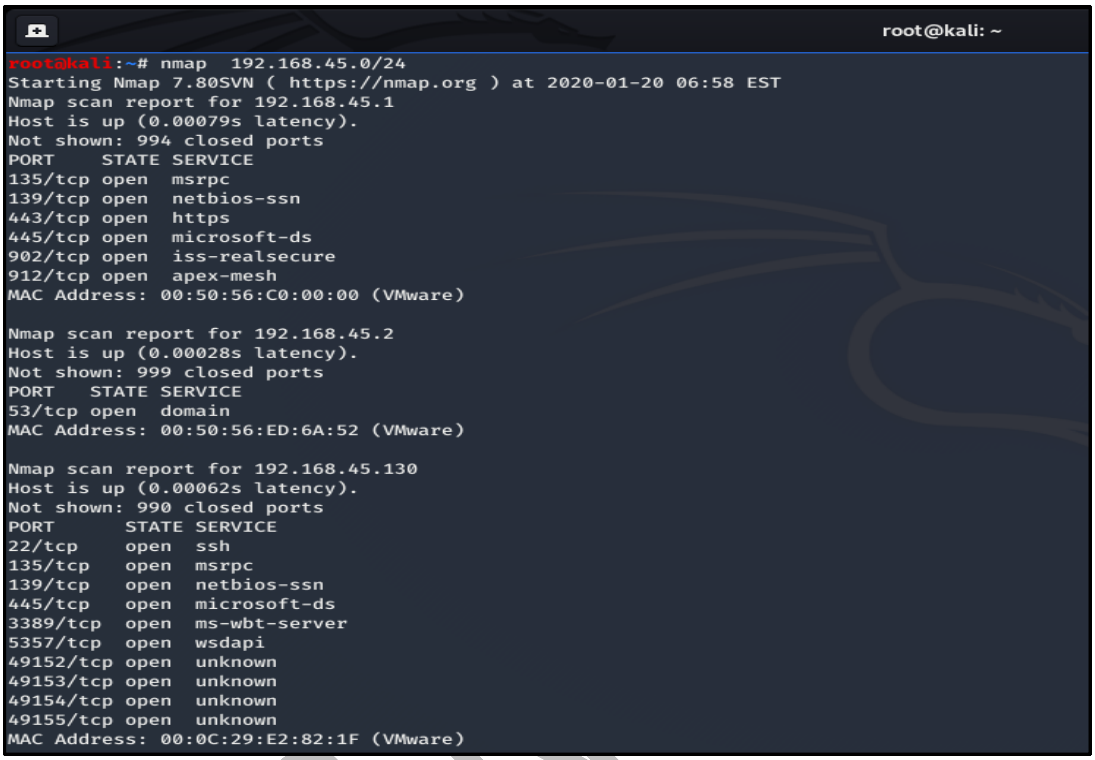
```
root@kali:/# nmap 192.168.45.130,138
Starting Nmap 7.80SVN ( https://nmap.org ) at 2020-01-20 06:49 EST
Nmap scan report for 192.168.45.130
Host is up (0.0019s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
MAC Address: 00:0C:29:E2:82:1F (VMware)

Nmap scan report for 192.168.45.138
Host is up (0.0024s latency).
All 1000 scanned ports on 192.168.45.138 are closed
MAC Address: 00:0C:29:63:D2:F6 (VMware)

Nmap done: 2 IP addresses (2 hosts up) scanned in 0.94 seconds
root@kali:/#
```

5. **Scan IP ranges**

Use Nmap to scan entire CIDR IP ranges, for example:

nmap 192.168.45.0/24

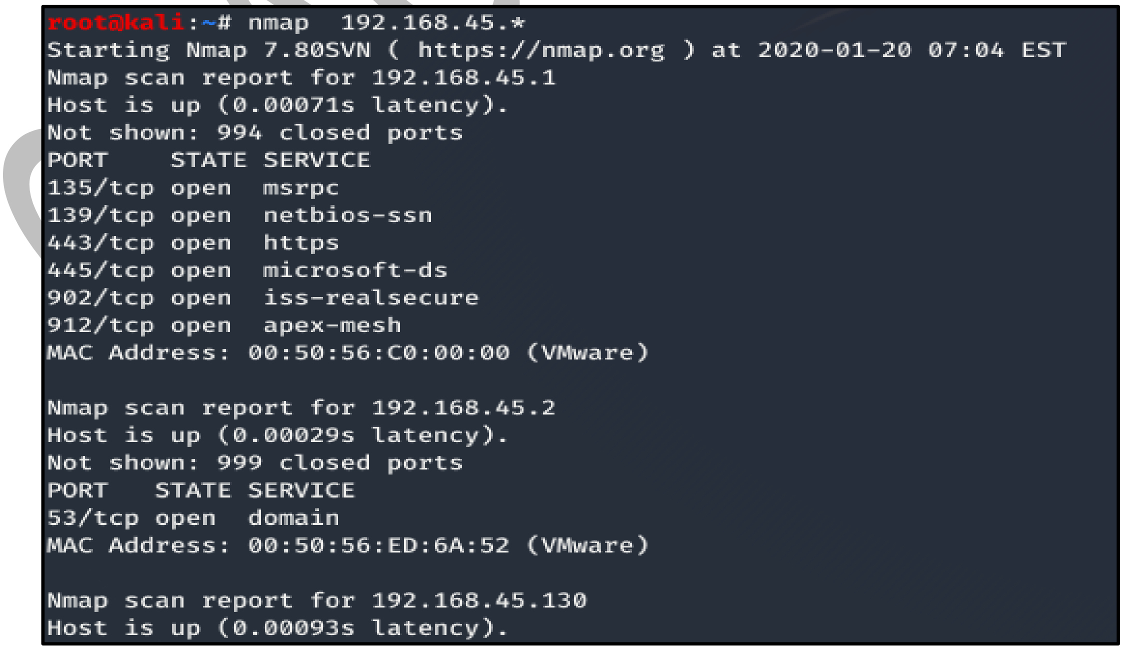
You can also use Nmap to scan entire CIDR IP ranges.



```
root@kali:~# nmap  192.168.45.0/24
Starting Nmap 7.80SVN ( https://nmap.org ) at 2020-01-20 06:58 EST
Nmap scan report for 192.168.45.1
Host is up (0.00079s latency).
Not shown: 994 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
443/tcp open  https
445/tcp open  microsoft-ds
902/tcp open  iss-realsecure
912/tcp open  apex-mesh
MAC Address: 00:50:56:C0:00:00 (VMware)

Nmap scan report for 192.168.45.2
Host is up (0.00028s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:ED:6A:52 (VMware)

Nmap scan report for 192.168.45.130
Host is up (0.00062s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
MAC Address: 00:0C:29:E2:82:1F (VMware)
```

Use wildcards to scan the entire C class IP range, for example:

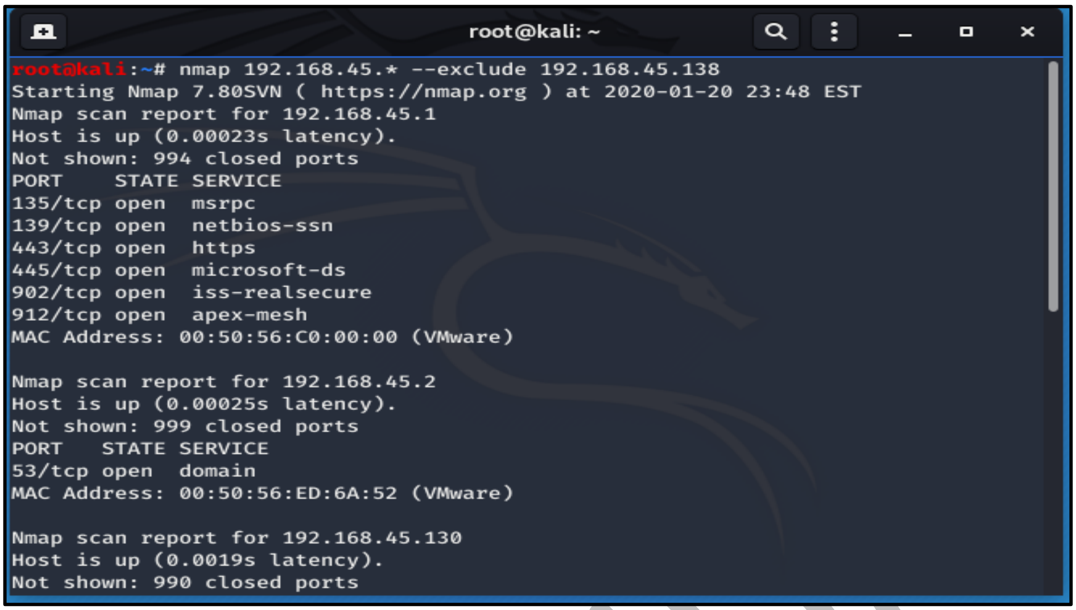
nmap 192.168.45.*



```
root@kali:~# nmap  192.168.45.*
Starting Nmap 7.80SVN ( https://nmap.org ) at 2020-01-20 07:04 EST
Nmap scan report for 192.168.45.1
Host is up (0.00071s latency).
Not shown: 994 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
443/tcp open  https
445/tcp open  microsoft-ds
902/tcp open  iss-realsecure
912/tcp open  apex-mesh
MAC Address: 00:50:56:C0:00:00 (VMware)

Nmap scan report for 192.168.45.2
Host is up (0.00029s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:ED:6A:52 (VMware)

Nmap scan report for 192.168.45.130
Host is up (0.00093s latency).
```

If you ever need to exclude certain IPs from the IP range scan, you can use the "–exclude" option.

nmap 192.168.45.* --exclude 192.168.45.138

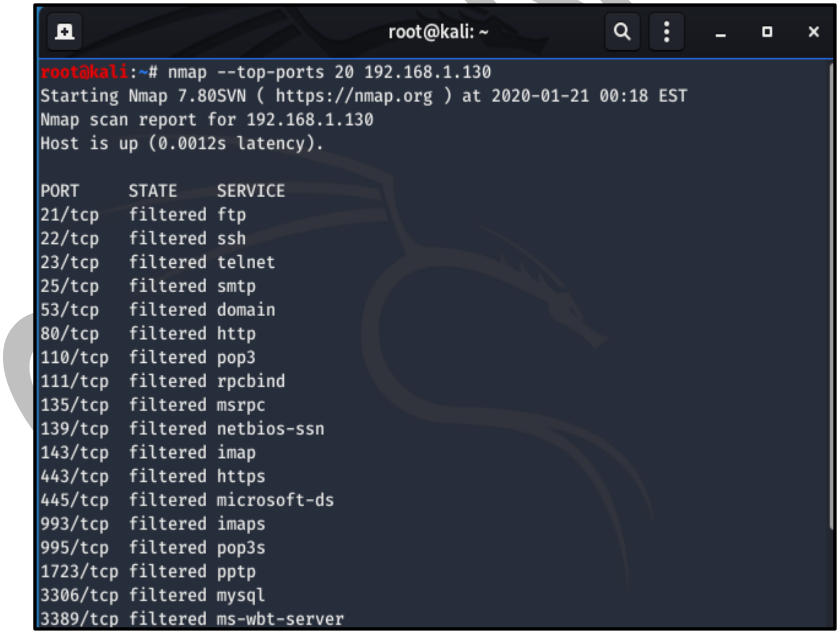


```
root@kali:~# nmap 192.168.45.* --exclude 192.168.45.138
Starting Nmap 7.80SVN ( https://nmap.org ) at 2020-01-20 23:48 EST
Nmap scan report for 192.168.45.1
Host is up (0.00023s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
443/tcp open  https
445/tcp open  microsoft-ds
902/tcp open  iss-realsecure
912/tcp open  apex-mesh
MAC Address: 00:50:56:C0:00:00 (VMware)

Nmap scan report for 192.168.45.2
Host is up (0.00025s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:ED:6A:52 (VMware)

Nmap scan report for 192.168.45.130
Host is up (0.0019s latency).
Not shown: 990 closed ports
```

6. **Scan the most popular ports**

nmap --top-ports 20 192.168.45.1.130

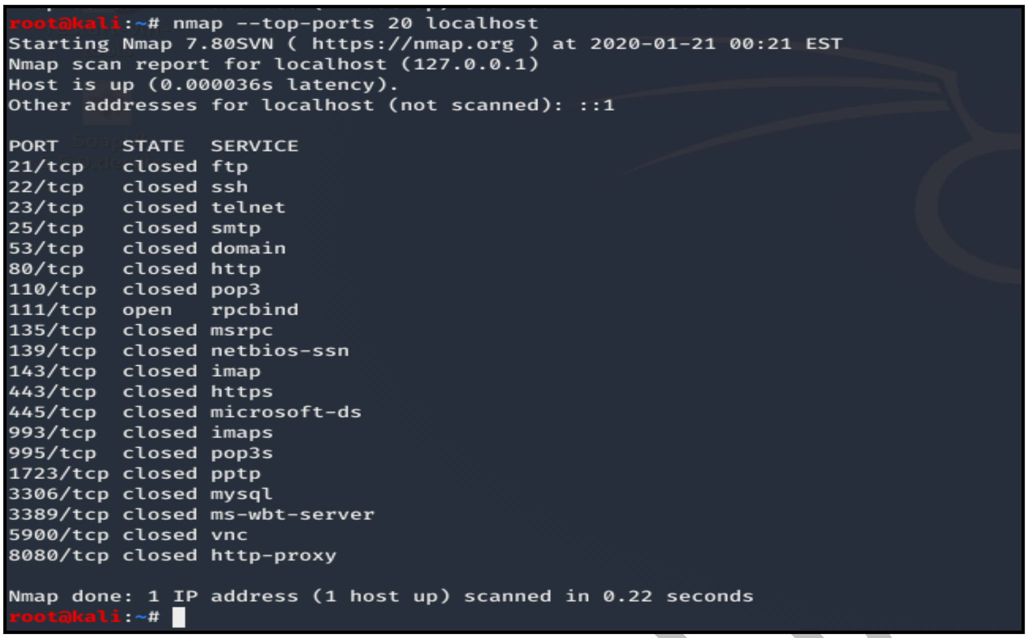
Using "–top-ports" parameter along with a specific number lets you scan the top X most common ports for that host.



```
root@kali:~# nmap --top-ports 20 192.168.1.130
Starting Nmap 7.80SVN ( https://nmap.org ) at 2020-01-21 00:18 EST
Nmap scan report for 192.168.1.130
Host is up (0.0012s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
53/tcp   filtered domain
80/tcp   filtered http
110/tcp  filtered pop3
111/tcp  filtered rpcbind
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  filtered imap
443/tcp  filtered https
445/tcp  filtered microsoft-ds
993/tcp  filtered imaps
995/tcp  filtered pop3s
1723/tcp filtered pptp
3306/tcp filtered mysql
3389/tcp filtered ms-wbt-server
```

Nmap maintains a database of the ports which are *usually* open on Internet machines, known as top ports.

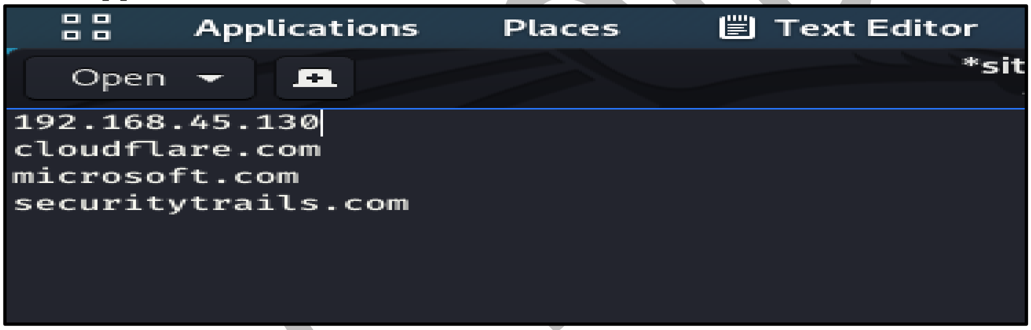
nmap --top-ports 20 localhost



```
root@kali:~# nmap --top-ports 20 localhost
Starting Nmap 7.80SVN ( https://nmap.org ) at 2020-01-21 00:21 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000036s latency).
Other addresses for localhost (not scanned): ::1

PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   closed ssh
23/tcp   closed telnet
25/tcp   closed smtp
53/tcp   closed domain
80/tcp   closed http
110/tcp  closed pop3
111/tcp  open   rpcbind
135/tcp  closed msrpc
139/tcp  closed netbios-ssn
143/tcp  closed imap
443/tcp  closed https
445/tcp  closed microsoft-ds
993/tcp  closed imaps
995/tcp  closed pop3s
1723/tcp closed pptp
3306/tcp closed mysql
3389/tcp closed ms-wbt-server
5900/tcp closed vnc
8080/tcp closed http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
root@kali:~#
```

7. **Scan hosts and IP addresses reading from a text file**

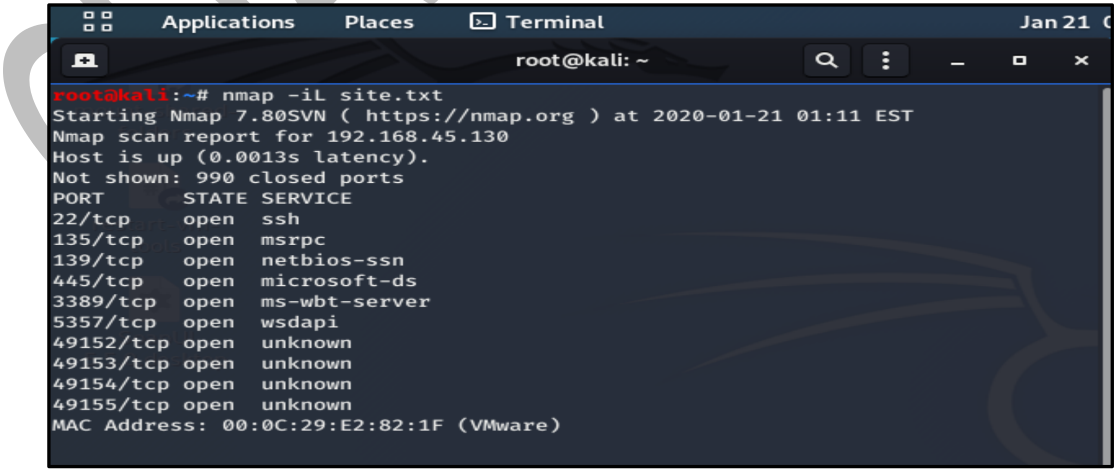
Let’s suppose user creates a list.txt file that contains these lines inside:



```
192.168.45.130
cloudflare.com
microsoft.com
securitytrails.com
```

nmap -iL site.txt

The “-iL” parameter lets user read from that file, and scan all those hosts listed in it.

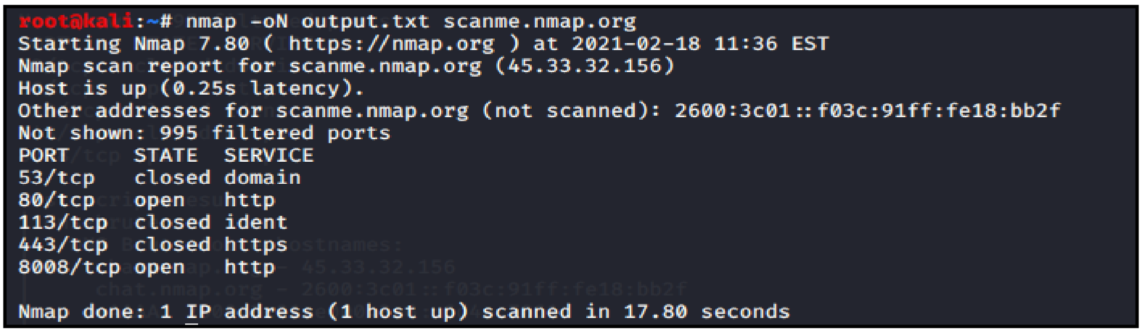


```
root@kali:~# nmap -iL site.txt
Starting Nmap 7.80SVN ( https://nmap.org ) at 2020-01-21 01:11 EST
Nmap scan report for 192.168.45.130
Host is up (0.0013s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
MAC Address: 00:0C:29:E2:82:1F (VMware)
```

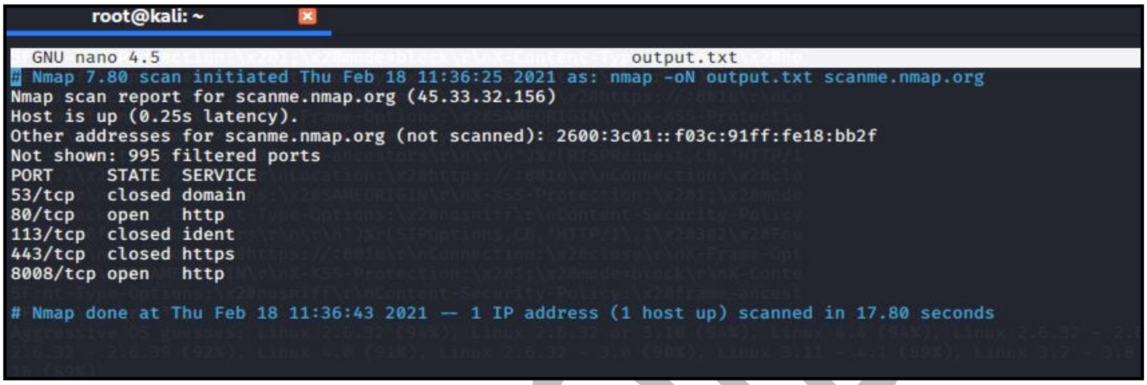
8. **Save your Nmap scan results to a file**

exporting/saving user results into a text file:

nmap -oN output.txt google.com



```
root@kali:~# nmap -oN output.txt scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-18 11:36 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 filtered ports
PORT     STATE  SERVICE
53/tcp   closed domain
80/tcp   open   http
113/tcp  closed ident
443/tcp  closed https
8008/tcp open   http

Nmap done: 1 IP address (1 host up) scanned in 17.80 seconds
```

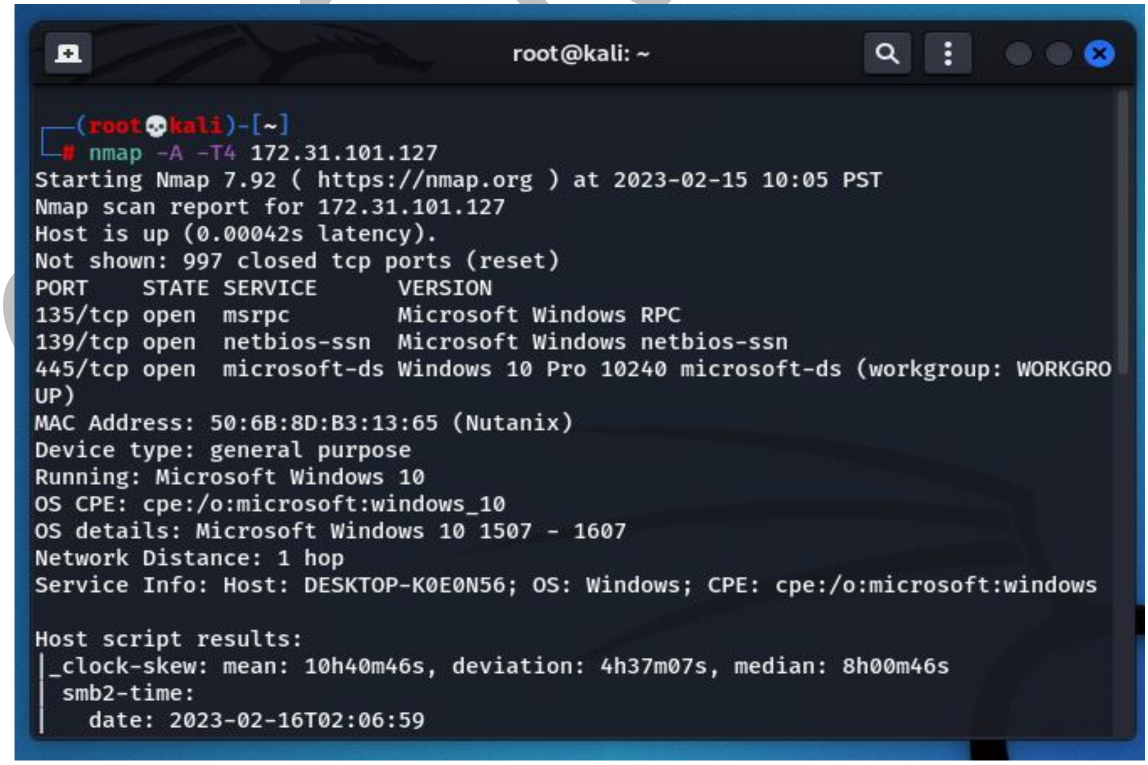


```
GNU nano 4.5                                              output.txt
# Nmap 7.80 scan initiated Thu Feb 18 11:36:25 2021 as: nmap -oN output.txt scanme.nmap.org
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 filtered ports
PORT     STATE  SERVICE
53/tcp   closed domain
80/tcp   open   http
113/tcp  closed ident
443/tcp  closed https
8008/tcp open   http

# Nmap done at Thu Feb 18 11:36:43 2021 -- 1 IP address (1 host up) scanned in 17.80 seconds
```

9. **Scan + OS and service detection with fast execution**

Using the "-A" parameter enables you to perform OS and service detection, and at the same time combining this with "-T4" for faster execution. See the example below:

nmap -A -T4 scanme.nmap.org

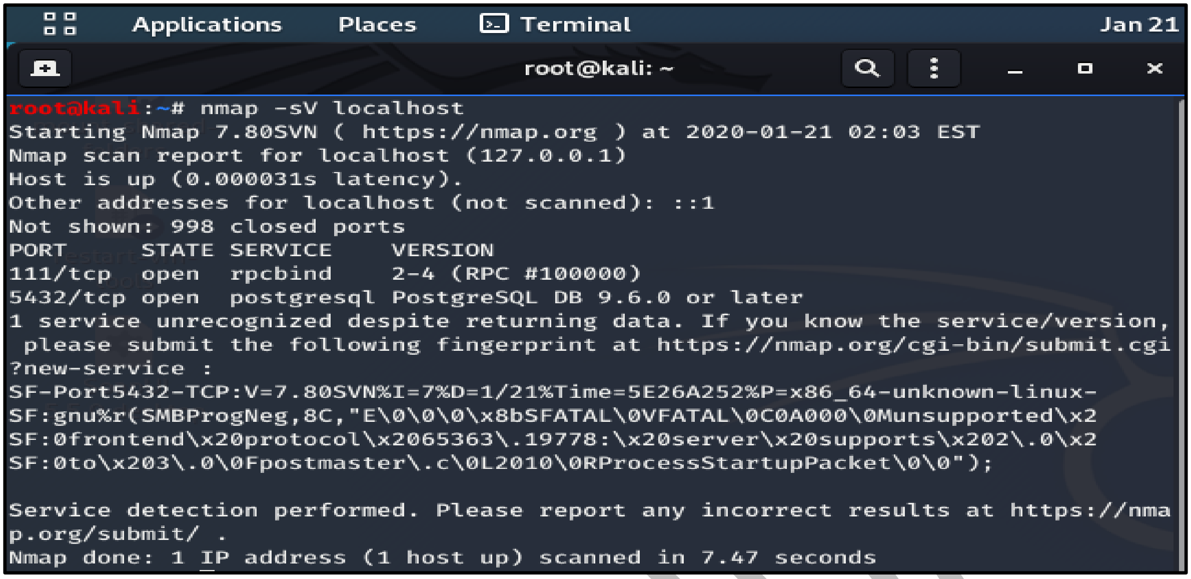


```
┌──(root💀kali)-[~]
└─# nmap -A -T4 172.31.101.127
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-15 10:05 PST
Nmap scan report for 172.31.101.127
Host is up (0.00042s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Windows 10 Pro 10240 microsoft-ds (workgroup: WORKGRO
UP)
MAC Address: 50:6B:8D:B3:13:65 (Nutanix)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1507 - 1607
Network Distance: 1 hop
Service Info: Host: DESKTOP-K0E0N56; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 10h40m46s, deviation: 4h37m07s, median: 8h00m46s
| smb2-time:
|   date: 2023-02-16T02:06:59
```

nmap may control the speed of scanning also (very slow (-T0) to extremely aggressive (-T5))

10. **Detect service/daemon versions**

This can be done by using -sV parameters

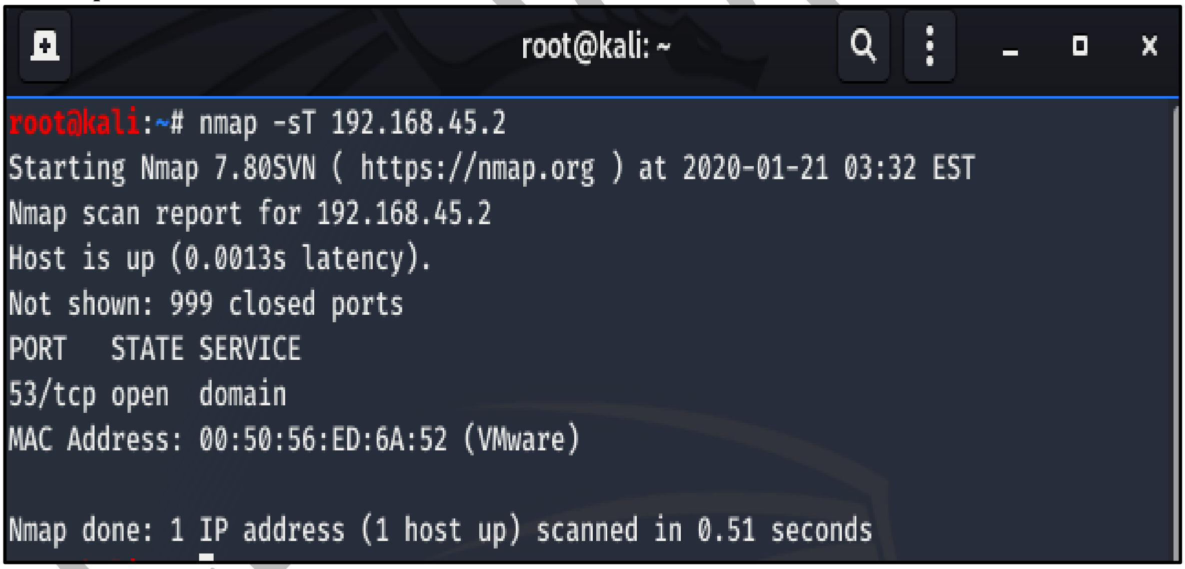


```
root@kali:~# nmap -sV localhost
Starting Nmap 7.80SVN ( https://nmap.org ) at 2020-01-21 02:03 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000031s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 998 closed ports
PORT     STATE SERVICE    VERSION
111/tcp  open  rpcbind    2-4 (RPC #100000)
5432/tcp open  postgresql PostgreSQL DB 9.6.0 or later
1 service unrecognized despite returning data. If you know the service/version,
 please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi
?new-service :
SF-Port5432-TCP:V=7.80SVN%I=7%D=1/21%Time=5E26A252%P=x86_64-unknown-linux-
SF:gnu%r(SMBProgNeg,8C,"E\0\0\0\x8bSFATAL\0VFATAL\0C0A000\0Munsupported\x2
SF:0frontend\x20protocol\x2065363\.19778:\x20server\x20supports\x202\.0\x2
SF:0to\x203\.0\0Fpostmaster\.c\0L2010\0RProcessStartupPacket\0\0");

Service detection performed. Please report any incorrect results at https://nma
p.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.47 seconds
```

11. **Scan using TCP or UDP protocols**

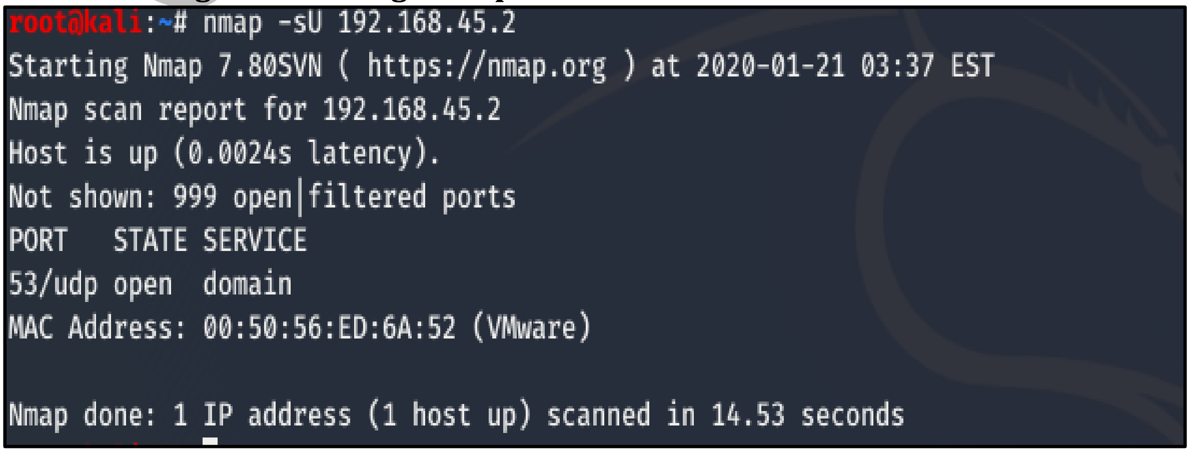
Standard TCP scanning output:

nmap –sT 192.168.45.2



```
root@kali:~# nmap -sT 192.168.45.2
Starting Nmap 7.80SVN ( https://nmap.org ) at 2020-01-21 03:32 EST
Nmap scan report for 192.168.45.2
Host is up (0.0013s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:ED:6A:52 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.51 seconds
```

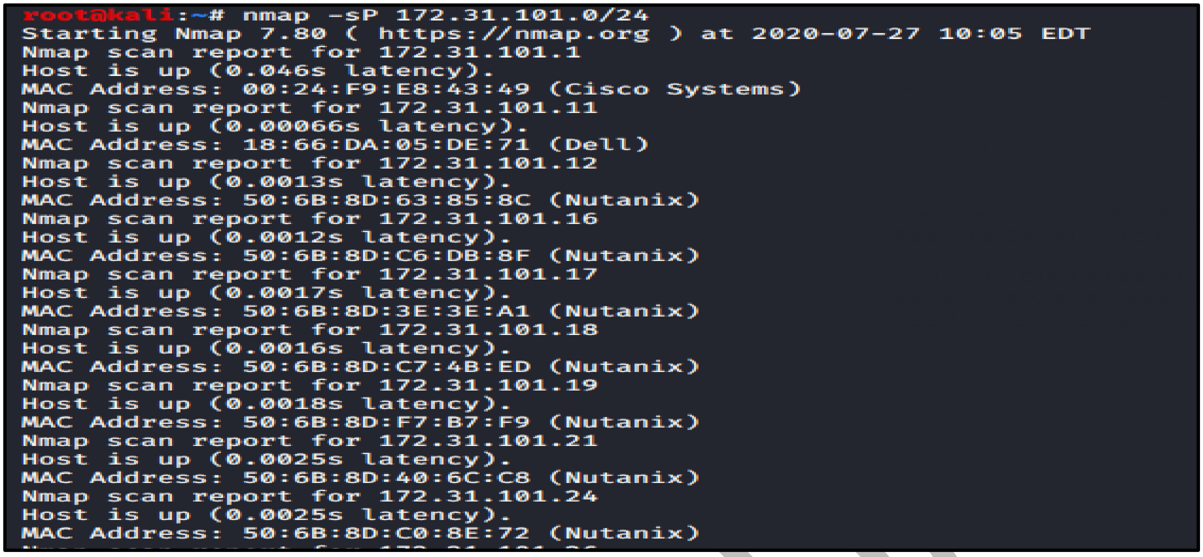
UDP scanning results using "-sU" parameter:



```
root@kali:~# nmap -sU 192.168.45.2
Starting Nmap 7.80SVN ( https://nmap.org ) at 2020-01-21 03:37 EST
Nmap scan report for 192.168.45.2
Host is up (0.0024s latency).
Not shown: 999 open|filtered ports
PORT   STATE SERVICE
53/udp open  domain
MAC Address: 00:50:56:ED:6A:52 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 14.53 seconds
```

12. **Finding multiple live hosts in the network**

Start a ping scan for live hosts using the following command.

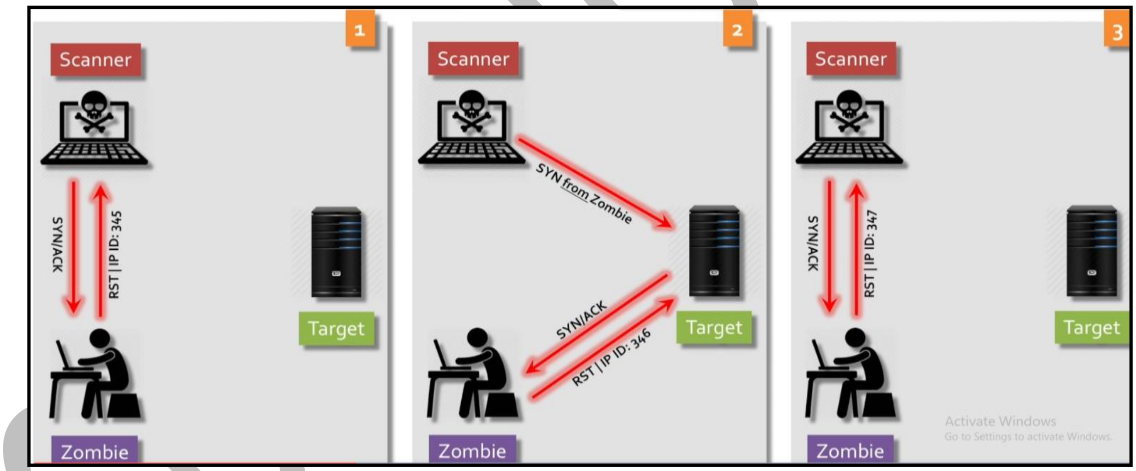


```
root@kali:~# nmap -sP 172.31.101.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-27 10:05 EDT
Nmap scan report for 172.31.101.1
Host is up (0.046s latency).
MAC Address: 00:24:F9:E8:43:49 (Cisco Systems)
Nmap scan report for 172.31.101.11
Host is up (0.00066s latency).
MAC Address: 18:66:DA:05:DE:71 (Dell)
Nmap scan report for 172.31.101.12
Host is up (0.0013s latency).
MAC Address: 50:6B:8D:63:85:8C (Nutanix)
Nmap scan report for 172.31.101.16
Host is up (0.0012s latency).
MAC Address: 50:6B:8D:C6:DB:8F (Nutanix)
Nmap scan report for 172.31.101.17
Host is up (0.0017s latency).
MAC Address: 50:6B:8D:3E:3E:A1 (Nutanix)
Nmap scan report for 172.31.101.18
Host is up (0.0016s latency).
MAC Address: 50:6B:8D:C7:4B:ED (Nutanix)
Nmap scan report for 172.31.101.19
Host is up (0.0018s latency).
MAC Address: 50:6B:8D:F7:B7:F9 (Nutanix)
Nmap scan report for 172.31.101.21
Host is up (0.0025s latency).
MAC Address: 50:6B:8D:40:6C:C8 (Nutanix)
Nmap scan report for 172.31.101.24
Host is up (0.0025s latency).
MAC Address: 50:6B:8D:C0:8E:72 (Nutanix)
```

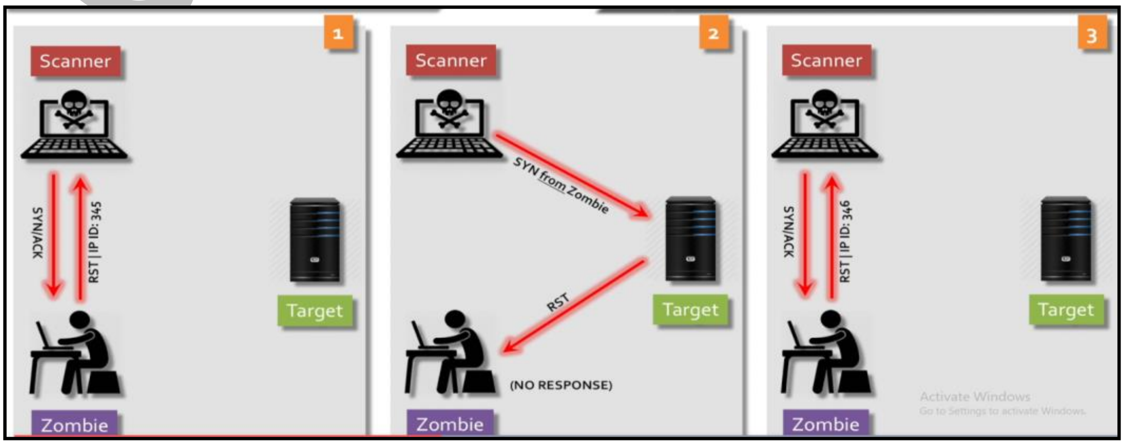
Nmap will return a list of all detected hosts.

13. Performing idle scanning using nmap(zombie scanning)

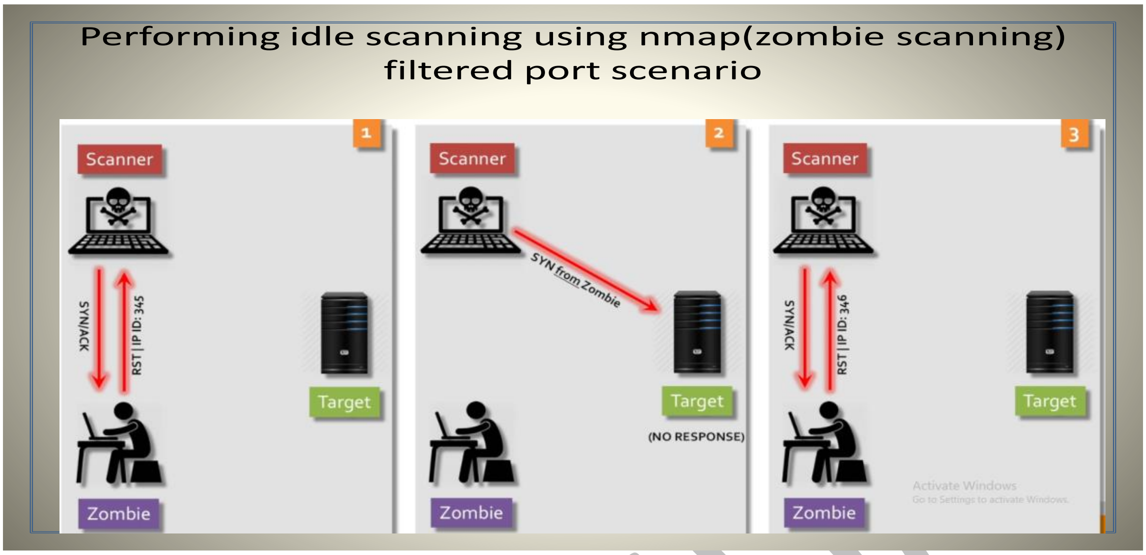
Open port scenario



Closed port scenario

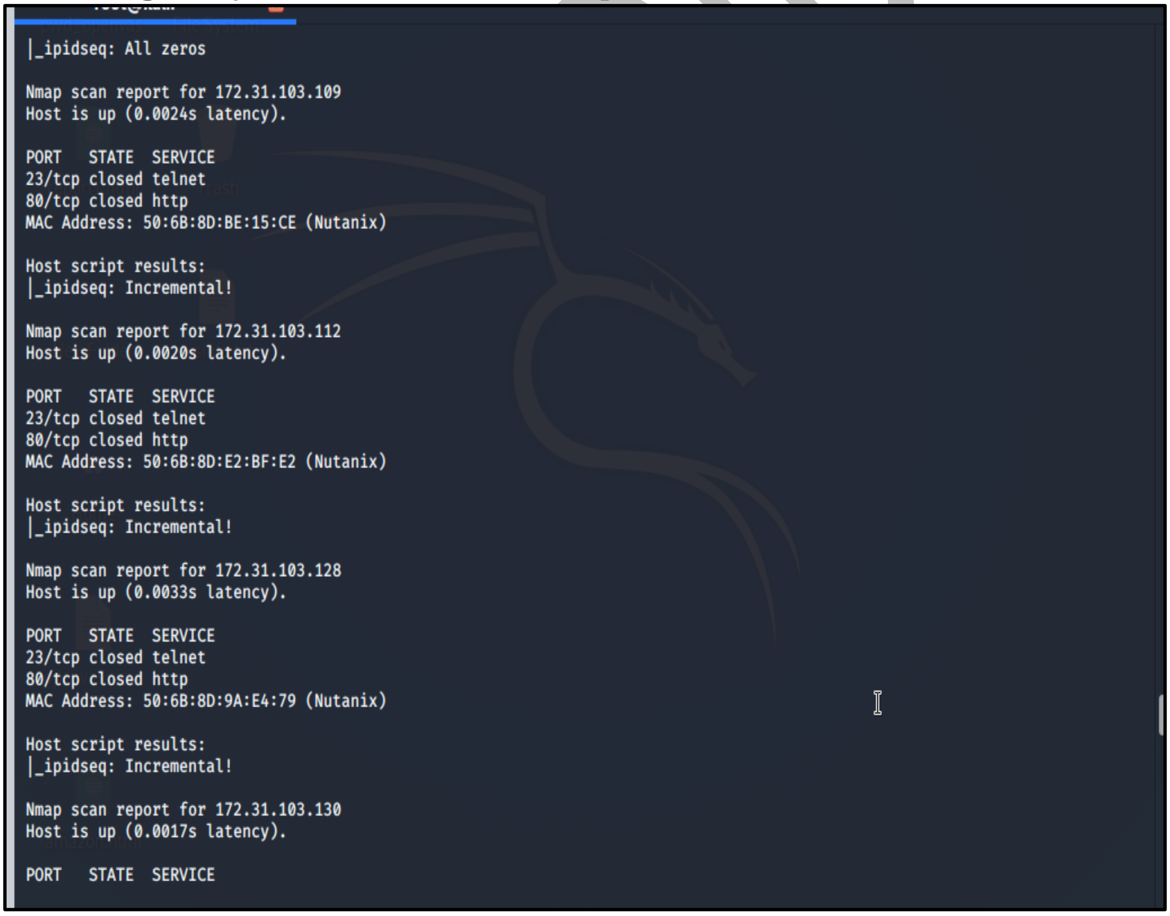


filtered port scenario



Performing idle scanning using nmap(zombie scanning)
filtered port scenario

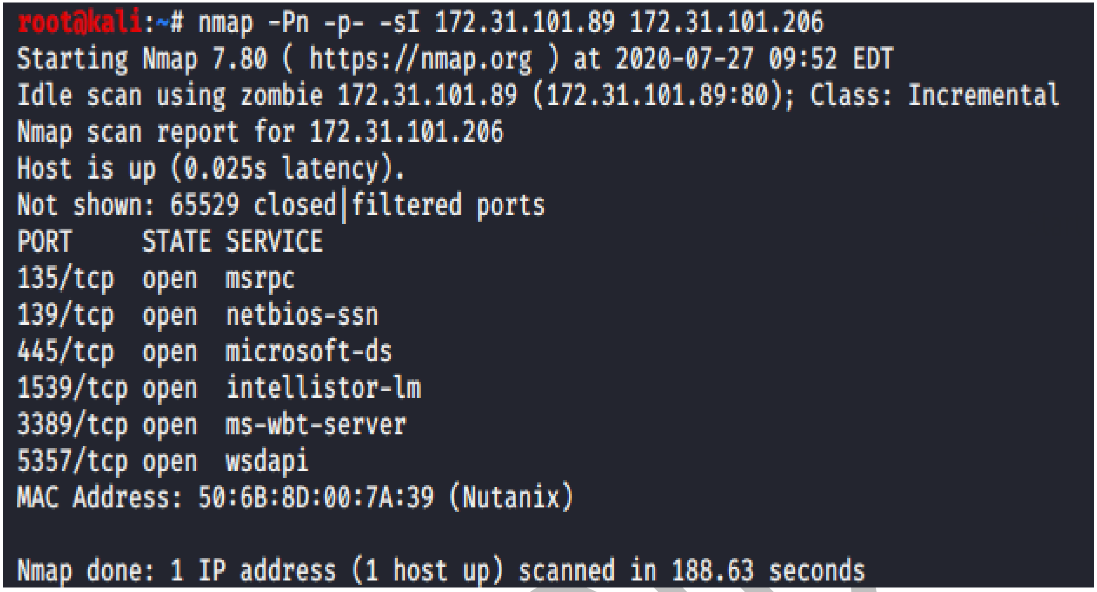
14. Finding the system with incremental ip-id



```
|_ipidseq: All zeros

Nmap scan report for 172.31.103.109
Host is up (0.0024s latency).

PORT   STATE  SERVICE
23/tcp closed telnet
80/tcp closed http
MAC Address: 50:6B:8D:BE:15:CE (Nutanix)

Host script results:
|_ipidseq: Incremental!

Nmap scan report for 172.31.103.112
Host is up (0.0020s latency).

PORT   STATE  SERVICE
23/tcp closed telnet
80/tcp closed http
MAC Address: 50:6B:8D:E2:BF:E2 (Nutanix)

Host script results:
|_ipidseq: Incremental!

Nmap scan report for 172.31.103.128
Host is up (0.0033s latency).

PORT   STATE  SERVICE
23/tcp closed telnet
80/tcp closed http
MAC Address: 50:6B:8D:9A:E4:79 (Nutanix)

Host script results:
|_ipidseq: Incremental!

Nmap scan report for 172.31.103.130
Host is up (0.0017s latency).

PORT   STATE  SERVICE
```

15. Performing idle scanning using nmap(zombie scanning)

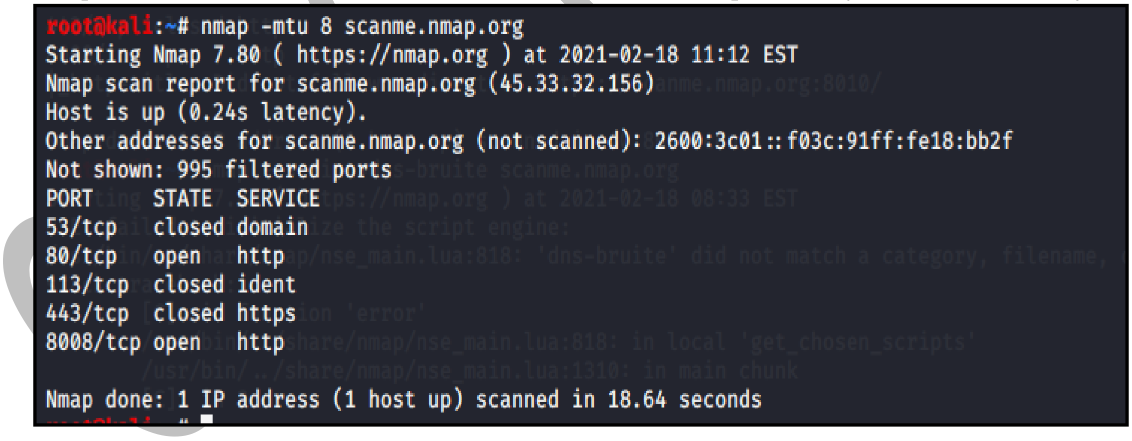
Idle scan is the ultimate stealth scan. An attacker to send some packets to the target from his real IP address in order to get scan results back. One upshot of idle scan is that intrusion detection systems will generally send alerts claiming that the zombie machine has launched a scan against them. So it can be used to frame some other party for a scan. A unique advantage of idle scan is that it can be used to defeat certain packet filtering firewalls and routers. IP source address filtering is a common (though weak) security mechanism for limiting machines that may connect to a sensitive host or network. Simply specify the zombie hostname to the -sI option and Nmap does the rest.



```
root@kali:~# nmap -Pn -p- -sI 172.31.101.89 172.31.101.206
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-27 09:52 EDT
Idle scan using zombie 172.31.101.89 (172.31.101.89:80); Class: Incremental
Nmap scan report for 172.31.101.206
Host is up (0.025s latency).
Not shown: 65529 closed|filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1539/tcp open  intellistor-lm
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
MAC Address: 50:6B:8D:00:7A:39 (Nutanix)

Nmap done: 1 IP address (1 host up) scanned in 188.63 seconds
```

16. **Bypassing firewall using fragmentation**

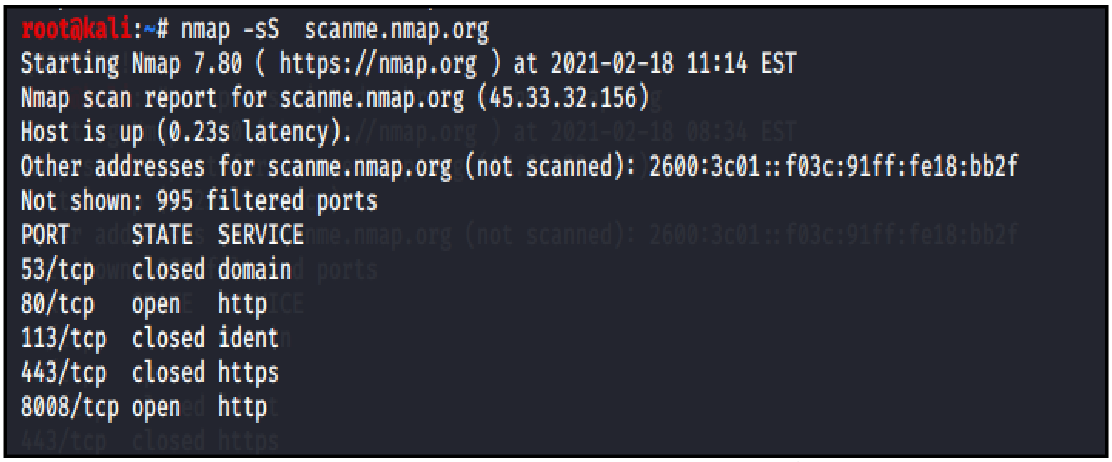
    Nmap gives the option to the user to set a specific MTU (Maximum Transmission Unit) to the packet. This is similar to the packet fragmentation technique.
    During the scan, Nmap will create packets with a size based on the number that we will give. In this example, we gave the number 24, so the Nmap will create 24-byte packets, causing confusion to the firewall.
    Keep in mind that the MTU number must be a multiple of 8 (8, 16, 24, 32, etc.).



```
root@kali:~# nmap -mtu 8 scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-18 11:12 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.24s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 filtered ports
PORT     STATE  SERVICE
53/tcp   closed domain
80/tcp   open   http
113/tcp  closed ident
443/tcp  closed https
8008/tcp open   http

Nmap done: 1 IP address (1 host up) scanned in 18.64 seconds
```

17. **Stealthy scan to avoid firewall detection**

    Nmap has an option that simplifies and streamlines the process of performing TCP stealth scans. You can easily use the -sS command to perform TCP stealth scans with Nmap



```
root@kali:~# nmap -sS  scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-18 11:14 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.23s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 filtered ports
PORT     STATE  SERVICE
53/tcp   closed domain
80/tcp   open   http
113/tcp  closed ident
443/tcp  closed https
8008/tcp open   http
```

18. **Using Nmap Script engine**

One of Nmap's greatest features is "Nmap Scripting Engine" (known as NSE). Using NSE we can do sophisticated version detection, vulnerability detection, backdoor detection etc.

CVE detection using Nmap

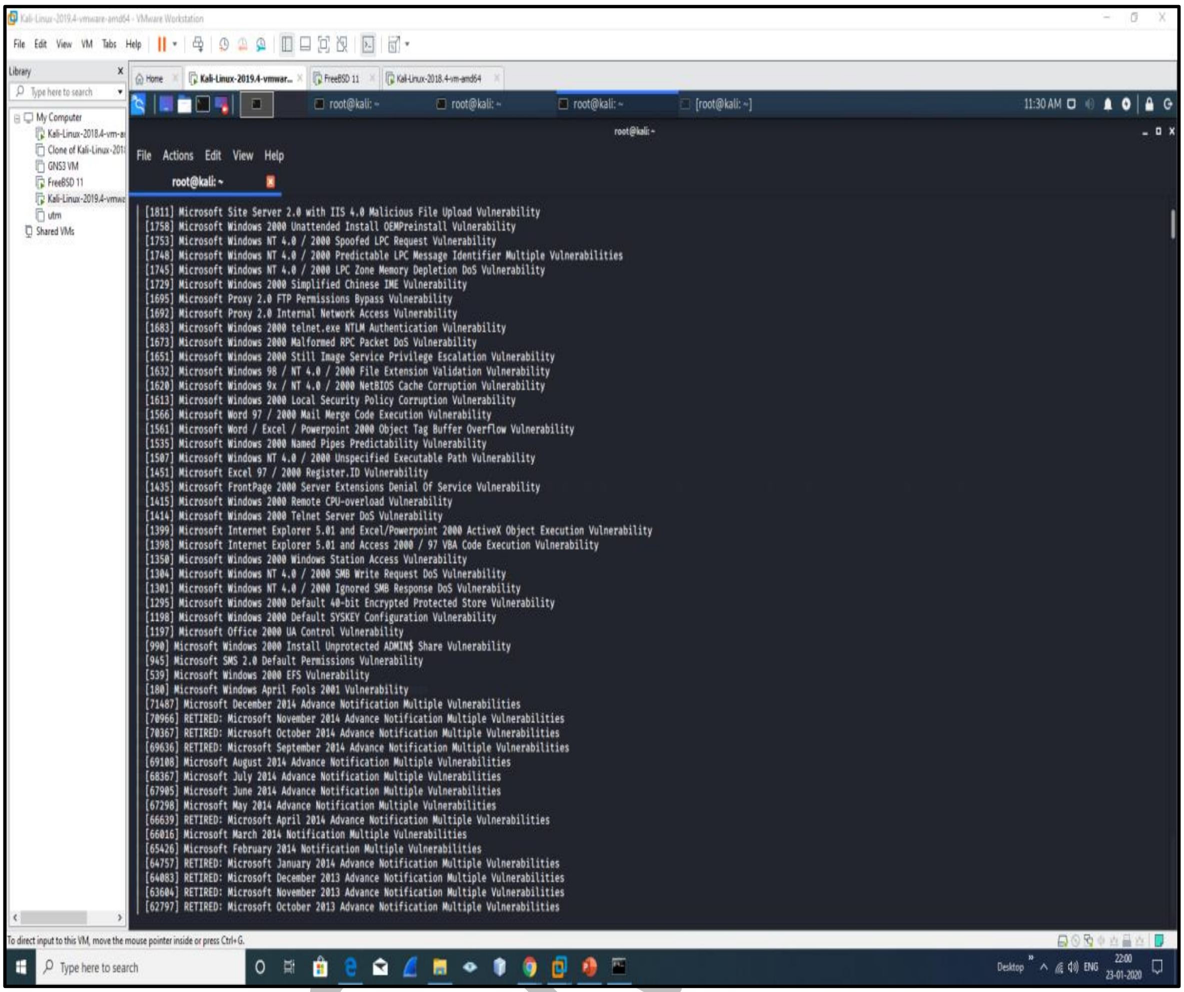
- One of Nmap's greatest features "Nmap Scripting Engine" (known as NSE). Using NSE is crucial in order to automate system and vulnerability scans. For example, if user want to run a full vulnerability test against his target, user can use these parameters:
- Where vuln is a script with known vulnerability databases included.
  Nmap --script vuln 192.168.45.130

Downloading vulnerability script

The following commands will install the vulscan script along with all the databases mentioned:

- git clone https://github.com/scipag/vulscan scipag_vulscan
- ln -s `pwd`/scipag_vulscan /usr/share/nmap/scripts/vulscan
- Run
- Nmap –sV –Pn –T5 –script vulscan<target ip>

CDAC NOIDA



```
[1811] Microsoft Site Server 2.0 with IIS 4.0 Malicious File Upload Vulnerability
[1758] Microsoft Windows 2000 Unattended Install OEMPreinstall Vulnerability
[1753] Microsoft Windows NT 4.0 / 2000 Spoofed LPC Request Vulnerability
[1748] Microsoft Windows NT 4.0 / 2000 Predictable LPC Message Identifier Multiple Vulnerabilities
[1745] Microsoft Windows NT 4.0 / 2000 LPC Zone Memory Depletion DoS Vulnerability
[1729] Microsoft Windows 2000 Simplified Chinese IME Vulnerability
[1695] Microsoft Proxy 2.0 FTP Permissions Bypass Vulnerability
[1692] Microsoft Proxy 2.0 Internal Network Access Vulnerability
[1683] Microsoft Windows 2000 telnet.exe NTLM Authentication Vulnerability
[1673] Microsoft Windows 2000 Malformed RPC Packet DoS Vulnerability
[1651] Microsoft Windows 2000 Still Image Service Privilege Escalation Vulnerability
[1632] Microsoft Windows 98 / NT 4.0 / 2000 File Extension Validation Vulnerability
[1620] Microsoft Windows 9x / NT 4.0 / 2000 NetBIOS Cache Corruption Vulnerability
[1613] Microsoft Windows 2000 Local Security Policy Corruption Vulnerability
[1566] Microsoft Word 97 / 2000 Mail Merge Code Execution Vulnerability
[1561] Microsoft Word / Excel / Powerpoint 2000 Object Tag Buffer Overflow Vulnerability
[1535] Microsoft Windows 2000 Named Pipes Predictability Vulnerability
[1507] Microsoft Windows NT 4.0 / 2000 Unspecified Executable Path Vulnerability
[1451] Microsoft Excel 97 / 2000 Register.ID Vulnerability
[1435] Microsoft FrontPage 2000 Server Extensions Denial Of Service Vulnerability
[1415] Microsoft Windows 2000 Remote CPU-overload Vulnerability
[1414] Microsoft Windows 2000 Telnet Server DoS Vulnerability
[1399] Microsoft Internet Explorer 5.01 and Excel/Powerpoint 2000 ActiveX Object Execution Vulnerability
[1398] Microsoft Internet Explorer 5.01 and Access 2000 / 97 VBA Code Execution Vulnerability
[1350] Microsoft Windows 2000 Windows Station Access Vulnerability
[1304] Microsoft Windows NT 4.0 / 2000 SMB Write Request DoS Vulnerability
[1301] Microsoft Windows NT 4.0 / 2000 Ignored SMB Response DoS Vulnerability
[1295] Microsoft Windows 2000 Default 40-bit Encrypted Protected Store Vulnerability
[1198] Microsoft Windows 2000 Default SYSKEY Configuration Vulnerability
[1197] Microsoft Office 2000 UA Control Vulnerability
[990] Microsoft Windows 2000 Install Unprotected ADMIN$ Share Vulnerability
[945] Microsoft SMS 2.0 Default Permissions Vulnerability
[539] Microsoft Windows 2000 EFS Vulnerability
[180] Microsoft Windows April Fools 2001 Vulnerability
[71487] Microsoft December 2014 Advance Notification Multiple Vulnerabilities
[70966] RETIRED: Microsoft November 2014 Advance Notification Multiple Vulnerabilities
[70367] RETIRED: Microsoft October 2014 Advance Notification Multiple Vulnerabilities
[69636] RETIRED: Microsoft September 2014 Advance Notification Multiple Vulnerabilities
[69108] Microsoft August 2014 Advance Notification Multiple Vulnerabilities
[68367] Microsoft July 2014 Advance Notification Multiple Vulnerabilities
[67905] Microsoft June 2014 Advance Notification Multiple Vulnerabilities
[67298] Microsoft May 2014 Advance Notification Multiple Vulnerabilities
[66639] RETIRED: Microsoft April 2014 Advance Notification Multiple Vulnerabilities
[66016] Microsoft March 2014 Notification Multiple Vulnerabilities
[65426] Microsoft February 2014 Notification Multiple Vulnerabilities
[64757] RETIRED: Microsoft January 2014 Advance Notification Multiple Vulnerabilities
[64083] RETIRED: Microsoft December 2013 Advance Notification Multiple Vulnerabilities
[63604] RETIRED: Microsoft November 2013 Advance Notification Multiple Vulnerabilities
[62797] RETIRED: Microsoft October 2013 Advance Notification Multiple Vulnerabilities
```

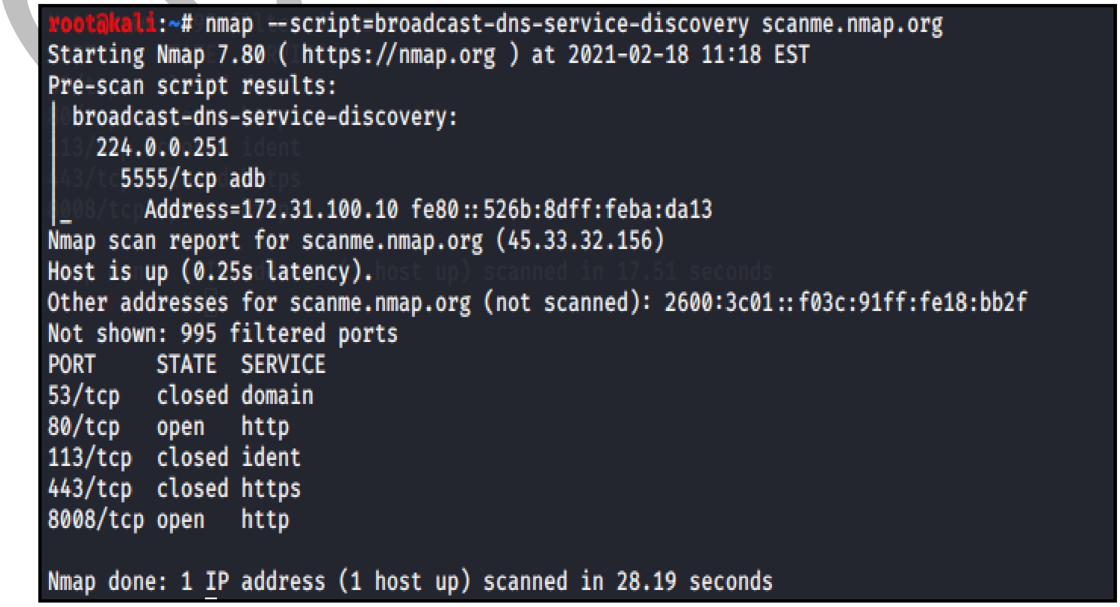
File Actions Edit View Help
root@kali: ~
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search

19. **DNS Enumeration**

The following command will try to discover hosts' services using the DNS Service Discovery protocol. It sends a multicast DNS-SD query and collects all the responses.

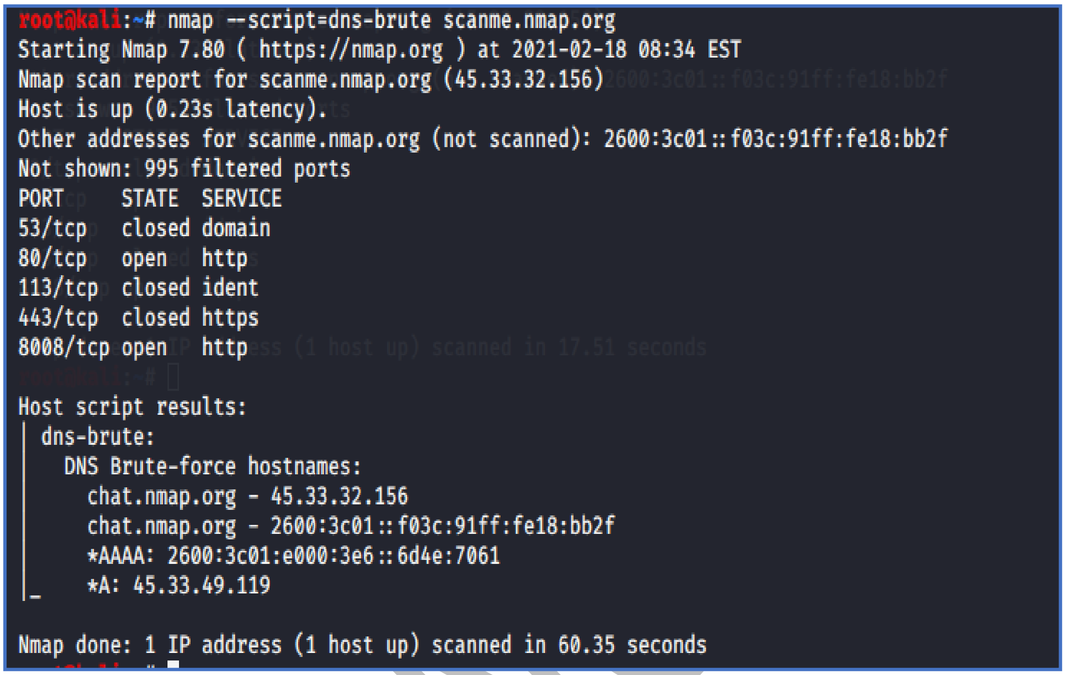
nmap --script=broadcast-dns-service-discovery scanme.nmap.org

CDAC



```
root@kali:~# nmap --script=broadcast-dns-service-discovery scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-18 11:18 EST
Pre-scan script results:
| broadcast-dns-service-discovery:
|   224.0.0.251
|     5555/tcp adb
|_      Address=172.31.100.10 fe80::526b:8dff:feba:da13
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 filtered ports
PORT     STATE  SERVICE
53/tcp   closed domain
80/tcp   open   http
113/tcp  closed ident
443/tcp  closed https
8008/tcp open   http

Nmap done: 1 IP address (1 host up) scanned in 28.19 seconds
```

- Following command will try to enumerate DNS hostnames by brute force guessing of common subdomains. With the dns-brute.srv argument, dns-brute will also try to enumerate common DNS SRV records
  nmap -T4 -p 53 --script dns-brute scanme.nmap.org



```
root@kali:~# nmap --script=dns-brute scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-18 08:34 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.23s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 filtered ports
PORT     STATE  SERVICE
53/tcp   closed domain
80/tcp   open   http
113/tcp  closed ident
443/tcp  closed https
8008/tcp open   http

Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|     chat.nmap.org - 45.33.32.156
|     chat.nmap.org - 2600:3c01::f03c:91ff:fe18:bb2f
|     *AAAA: 2600:3c01:e000:3e6::6d4e:7061
|_    *A: 45.33.49.119

Nmap done: 1 IP address (1 host up) scanned in 60.35 seconds
```

CDAC N

CDAC NOIDA