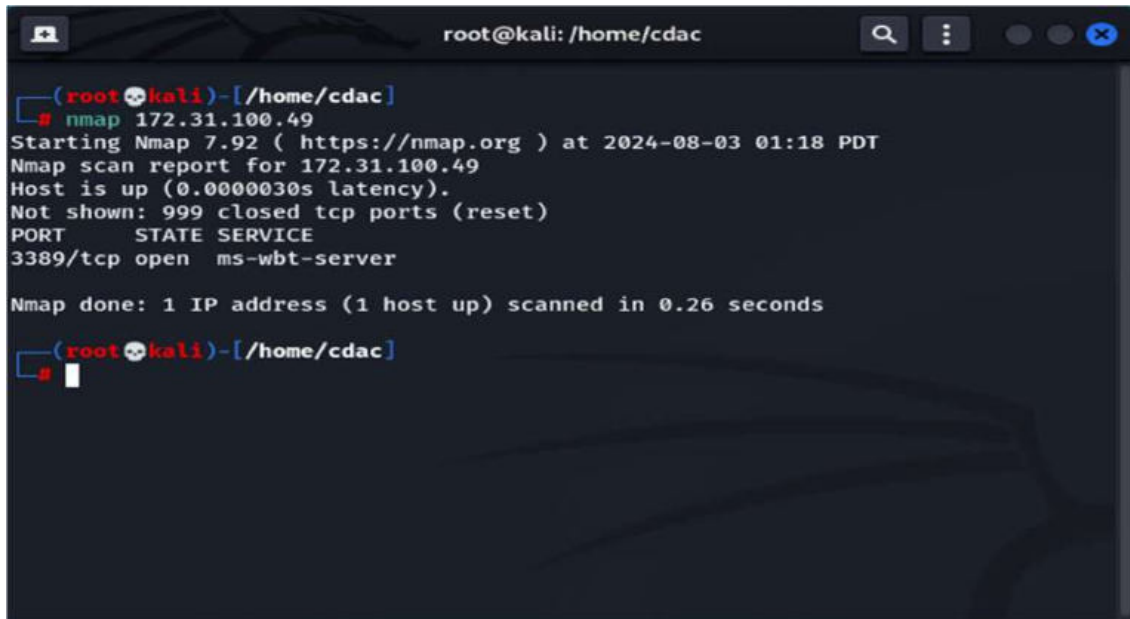


Lab1: Network Scanning using Nmap

1. Basic Nmap Scan Against IP or host

nmap 172.31.100.49

A terminal window titled 'root@kali: /home/cdac' showing the execution of 'nmap 172.31.100.49'. The output indicates the host is up and port 3389/tcp is open, running the ms-wbt-server service. The scan took 0.26 seconds.

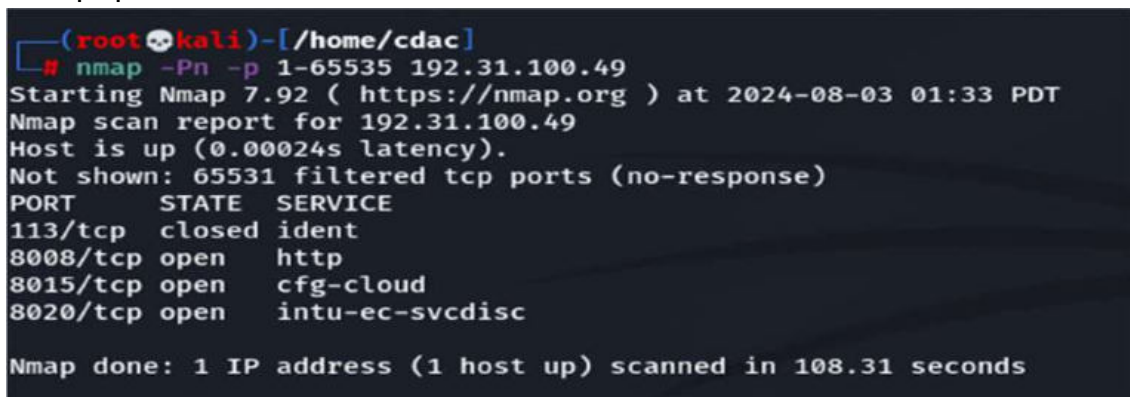
```
(root@kali)-[/home/cdac]
# nmap 172.31.100.49
Starting Nmap 7.92 ( https://nmap.org ) at 2024-08-03 01:18 PDT
Nmap scan report for 172.31.100.49
Host is up (0.0000030s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds

(root@kali)-[/home/cdac]
#
```

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

nmap -p 1-65535 172.31.100.49

A terminal window showing the execution of 'nmap -p 1-65535 172.31.100.49'. The output shows several open ports: 8008/tcp (http), 8015/tcp (cfg-cloud), and 8020/tcp (intu-ec-svcdisc). The scan took 108.31 seconds.

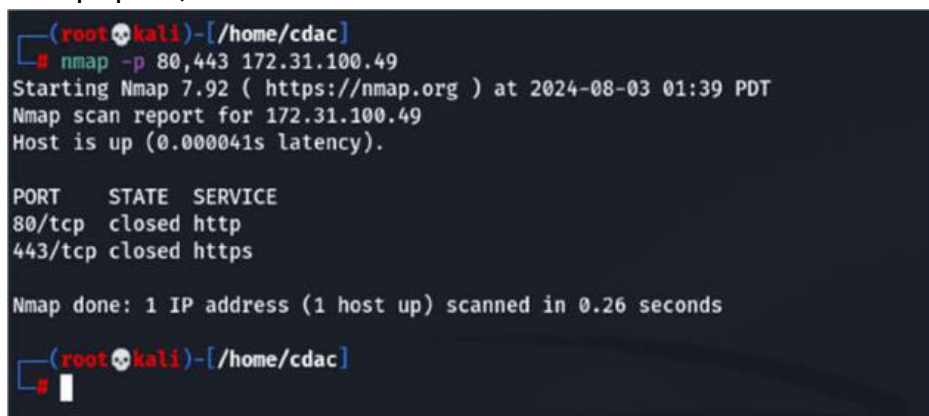
```
(root@kali)-[/home/cdac]
# nmap -Pn -p 1-65535 172.31.100.49
Starting Nmap 7.92 ( https://nmap.org ) at 2024-08-03 01:33 PDT
Nmap scan report for 172.31.100.49
Host is up (0.00024s latency).
Not shown: 65531 filtered tcp ports (no-response)
PORT      STATE SERVICE
113/tcp   closed ident
8008/tcp  open  http
8015/tcp  open  cfg-cloud
8020/tcp  open  intu-ec-svcdisc

Nmap done: 1 IP address (1 host up) scanned in 108.31 seconds

(root@kali)-[/home/cdac]
#
```

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

nmap -p 80,443 172.31.100.49

A terminal window showing the execution of 'nmap -p 80,443 172.31.100.49'. The output shows that port 80/tcp is closed (http) and port 443/tcp is closed (https). The scan took 0.26 seconds.

```
(root@kali)-[/home/cdac]
# nmap -p 80,443 172.31.100.49
Starting Nmap 7.92 ( https://nmap.org ) at 2024-08-03 01:39 PDT
Nmap scan report for 172.31.100.49
Host is up (0.000041s latency).

PORT      STATE SERVICE
80/tcp    closed http
443/tcp   closed https

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds

(root@kali)-[/home/cdac]
#
```

4. Scan multiple IP addresses

nmap 172.31.100.49,50

```
(root@kali)-[/home/cdac]
# nmap 172.31.100.49,50
Starting Nmap 7.92 ( https://nmap.org ) at 2024-08-03 01:50 PDT
Nmap scan report for 172.31.100.49
Host is up (0.0000040s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server

Nmap scan report for 172.31.100.50
Host is up (0.0011s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server
MAC Address: 50:6B:8D:B3:65:85 (Nutanix)

Nmap done: 2 IP addresses (2 hosts up) scanned in 0.50 seconds
```

5. Scan IP ranges

nmap 172.31.100.0/24

```
(root@kali)-[/home/cdac]
# nmap 172.31.100.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-08-03 01:53 PDT
Nmap scan report for 172.31.100.1
Host is up (0.0013s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
113/tcp   closed ident
MAC Address: 84:39:8F:8E:3E:82 (Unknown)

Nmap scan report for 172.31.100.2
Host is up (0.00055s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
3389/tcp  open  ms-wbt-server
MAC Address: 00:24:E8:7C:B4:5B (Dell)

Nmap scan report for 172.31.100.9
Host is up (0.00058s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server
```

Use wildcards to scan the entire C class IP range:

nmap 172.31.100.*

```

(root@kali)-[/home/cdac]
# nmap 172.31.100.*
Starting Nmap 7.92 ( https://nmap.org ) at 2024-08-03 01:57 PDT
Nmap scan report for 172.31.100.1
Host is up (0.0013s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
113/tcp    closed ident
MAC Address: 84:39:8F:8E:3E:82 (Unknown)

Nmap scan report for 172.31.100.2
Host is up (0.00080s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
3389/tcp   open  ms-wbt-server
MAC Address: 00:24:E8:7C:B4:5B (Dell)

Nmap scan report for 172.31.100.9
Host is up (0.00076s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
3389/tcp   open  ms-wbt-server
MAC Address: 50:6B:8D:DC:AF:4C (Nutanix)

```

nmap 172.31.100.* --exclude 172.31.100.49

```

(root@kali)-[/home/cdac]
# nmap 172.31.100.* --exclude 172.31.100.49
Starting Nmap 7.92 ( https://nmap.org ) at 2024-08-03 02:00 PDT
Nmap scan report for 172.31.100.1
Host is up (0.0013s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
113/tcp    closed ident
MAC Address: 84:39:8F:8E:3E:82 (Unknown)

Nmap scan report for 172.31.100.2
Host is up (0.00072s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
3389/tcp   open  ms-wbt-server
MAC Address: 00:24:E8:7C:B4:5B (Dell)

Nmap scan report for 172.31.100.9
Host is up (0.00090s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
3389/tcp   open  ms-wbt-server
MAC Address: 50:6B:8D:DC:AF:4C (Nutanix)

```

6. Scan the most popular ports

`nmap --top-ports 20 172.31.100.49`

```
(root@kali)~[/home/cdac]
# nmap --top-ports 20 172.31.100.49
Starting Nmap 7.92 ( https://nmap.org ) at 2024-08-03 02:04 PDT
Nmap scan report for 172.31.100.49
Host is up (0.0000070s latency).

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   closed 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  open   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
```

`nmap --top-ports 20 localhost`

```
(root@kali)~[/home/cdac]
# nmap --top-ports 20 localhost
Starting Nmap 7.92 ( https://nmap.org ) at 2024-08-03 02:07 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000090s 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   closed 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  open   ms-wbt-server
5900/tcp  closed vnc
8080/tcp  closed http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```


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

```
(root@kali)~[/home/cdac]
# cat >> site.txt
172.31.100.49
cloudflare.com
microsoft.com
securitytrails.com
```

nmap -iL site.txt

```
(root@kali)~[/home/cdac]
# nmap -iL site.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2024-08-03 02:14 PDT
Nmap scan report for 172.31.100.49
Host is up (0.0000060s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server

Nmap scan report for cloudflare.com (172.67.211.231)
Host is up (0.014s latency).
Other addresses for cloudflare.com (not scanned): 104.21.77.216 2606:4700:3034::a
c43:d3e7 2606:4700:3031::6815:4dd8
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
113/tcp   closed ident
443/tcp   open  https
8008/tcp  open  http

Nmap scan report for microsoft.com (20.236.44.162)
Host is up (0.036s latency).
Other addresses for microsoft.com (not scanned): 20.70.246.20 20.231.239.246 20.
112.250.133 20.76.201.171 2603:1010:3:3::5b 2603:1030:20e:3::23c 2603:1020:201:1
0::10f 2603:1030:c02:8::14 2603:1030:b:3::152
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
113/tcp   closed ident
443/tcp   open  https
8008/tcp  open  http

Nmap done: 3 IP addresses (3 hosts up) scanned in 22.71 seconds
```

8. Save your Nmap scan results to a file

nmap -oN output.txt google.com

```
(root@kali)~[/home/cdac]
# nmap -oN output.txt google.com
Starting Nmap 7.92 ( https://nmap.org ) at 2024-08-03 05:23 PDT
Nmap scan report for google.com (142.250.194.110)
Host is up (0.031s latency).
Other addresses for google.com (not scanned): 2404:6800:4002:821::200e
rDNS record for 142.250.194.110: del12s04-in-f14.1e100.net
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
113/tcp   closed ident
443/tcp   open  https
8008/tcp  open  http

Nmap done: 1 IP address (1 host up) scanned in 6.69 seconds
```

```

GNU nano 5.9                                output.txt
# Nmap 7.92 scan initiated Sat Aug 3 05:23:22 2024 as: nmap -oN output.txt google.com
Nmap scan report for google.com (142.250.194.110)
Host is up (0.031s latency).
Other addresses for google.com (not scanned): 2404:6800:4002:821::200e
rDNS record for 142.250.194.110: del12s04-in-f14.1e100.net
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
113/tcp   closed ident
443/tcp   open  https
8008/tcp  open  http

```

9. Scan + OS and service detection with fast execution

`nmap -A -T4 scanme.nmap.org`

```

(root@kali)-[/home/cdac]
# nmap -A -T4 scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2024-08-03 05:52 PDT
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 tcp ports (no-response)
PORT      STATE SERVICE VERSION
53/tcp    closed domain
80/tcp    open  http      Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
113/tcp   closed ident
443/tcp   closed https
8008/tcp  open  http?
Aggressive OS guesses: Linux 2.6.32 (94%), Linux 2.6.32 or 3.10 (94%), Linux 4.4 (94%), Linux 2.6.32 - 2.6.35 (92%), Linux 2.6.32 - 2.6.39 (92%), Linux 2.6.32 - 3.0 (90%), Linux 4.0 (90%), Linux 3.11 - 4.1 (89%), Linux 3.2 - 3.8 (89%), Linux 2.6.18 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 13 hops

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1   0.51 ms   172.31.100.1
2   0.57 ms   220.156.184.2
3   15.66 ms  ns-g-corporate-41.65.186.122.airtel.in (122.186.65.41)
4   78.06 ms  116.119.57.142
5   72.06 ms  unknown.telstraglobal.net (202.127.73.101)
6   80.90 ms  i-91.sgc-core01.telstraglobal.net (202.84.224.198)
7   249.07 ms i-91.sgc-core01.telstraglobal.net (202.84.224.198)
8   250.25 ms unknown.telstraglobal.net (202.84.143.122)
9   257.88 ms eqix-sv1.linode.com (206.223.116.196)
10  248.88 ms eqix-sv1.linode.com (206.223.116.196)
11  ... 12
13  250.64 ms scanme.nmap.org (45.33.32.156)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

```

10. Detect service/daemon versions

`nmap -sV localhost`

```
(root@kali)~[/home/cdac]
# nmap -sV localhost
Starting Nmap 7.92 ( https://nmap.org ) at 2024-08-03 06:02 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000060s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
3001/tcp   open  http         Thin httpd
3389/tcp   open  ms-wbt-server xrdp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.25 seconds
```

11. Scan using TCP or UDP protocols

`nmap -sT 172.31.100.49`

TCP scanning

```
(root@kali)~[/home/cdac]
# nmap -sT 172.31.100.49
Starting Nmap 7.92 ( https://nmap.org ) at 2024-08-03 06:04 PDT
Nmap scan report for 172.31.100.49
Host is up (0.000099s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
3389/tcp   open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

UDP scanning

```
(root@kali)~[/home/cdac]
# nmap -sU 172.31.100.49
Starting Nmap 7.92 ( https://nmap.org ) at 2024-08-03 06:05 PDT
Nmap scan report for 172.31.100.49
Host is up (0.0000040s latency).
All 1000 scanned ports on 172.31.100.49 are in ignored states.
Not shown: 1000 closed udp ports (port-unreach)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
```


12. Finding multiple live hosts in the network

```
(root@kali)~[/home/cdac]
# nmap -sP 172.31.100.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-08-03 06:08 PDT
Nmap scan report for 172.31.100.1
Host is up (0.0072s latency).
MAC Address: 84:39:8F:8E:3E:82 (Unknown)
Nmap scan report for 172.31.100.2
Host is up (0.0072s latency).
MAC Address: 00:24:E8:7C:B4:5B (Dell)
Nmap scan report for 172.31.100.9
Host is up (0.0092s latency).
MAC Address: 50:6B:8D:DC:AF:4C (Nutanix)
Nmap scan report for 172.31.100.10
Host is up (0.0097s latency).
MAC Address: 50:6B:8D:D8:11:E8 (Nutanix)
Nmap scan report for 172.31.100.11
Host is up (0.0050s latency).
MAC Address: 50:6B:8D:AD:3D:77 (Nutanix)
Nmap scan report for 172.31.100.13
Host is up (0.0038s latency).
MAC Address: 50:6B:8D:B4:5E:78 (Nutanix)
Nmap scan report for 172.31.100.14
Host is up (0.0041s latency).
MAC Address: 50:6B:8D:80:9B:88 (Nutanix)
Nmap scan report for 172.31.100.15
Host is up (0.0041s latency).
MAC Address: 50:6B:8D:B8:B8:DD (Nutanix)
Nmap scan report for 172.31.100.18
Host is up (0.0055s latency).
MAC Address: 50:6B:8D:B6:20:13 (Nutanix)
Nmap scan report for 172.31.100.30
```

13. Performing idle scanning using nmap(zombie scanning)

14. Finding the system with incremental ip-id

15. Performing idle scanning using nmap(zombie scanning)

nmap -Pn -p- -sl 172.31.102.82 172.31.96.127

```
(root@kali)~[/home/cdac]
# nmap -Pn -p- -sl 172.31.102.82 172.31.96.127
Starting Nmap 7.92 ( https://nmap.org ) at 2024-08-05 09:16 PDT
Skipping Idle Scan against 172.31.96.127 -- you can't idle scan your own machine
(localhost).
Nmap scan report for 172.31.96.127
Host is up.

PORT      STATE SERVICE
1/tcp    unknown tcpmux
2/tcp    unknown compressnet
3/tcp    unknown compressnet
4/tcp    unknown unknown
5/tcp    unknown rje
6/tcp    unknown unknown
7/tcp    unknown echo
8/tcp    unknown unknown
9/tcp    unknown discard
10/tcp   unknown unknown
11/tcp   unknown sysstat
```

16. Bypassing firewall using fragmentation

nmap -mtu 8 scanme.nmap.org


```

(root@kali)-[/home/cdac]
# nmap -mtu 8 scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2024-08-05 09:21 PDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 265.29 seconds

```

17. Stealthy scan to avoid firewall detection

`nmap -sS scanme.nmap.org`

```

(root@kali)-[/home/kali]
# nmap -sS scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-09 00:57 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.049s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 56.05 seconds

```

18. Using Nmap Script engine

`nmap --script vuln 10.0.2.15`

```

# nmap --script vuln 192.168.1.110
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-09 03:04 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.1.110
Host is up (0.00083s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
2869/tcp  open  icslap
5357/tcp  open  wsdapi
MAC Address: 08:00:27:FB:2C:BD (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 43.50 seconds

```

19. DNS Enumeration

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

```

(root@kali)-[/home/kali]
# nmap --script=broadcast-dns-service-discovery scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-09 03:07 EDT
Pre-scan script results:
| broadcast-dns-service-discovery:
|   224.0.0.251
|   47989/tcp nvstream_dbd
|_   Address=192.168.1.111 fe80::e259:7ab:95f3:9603
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: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 9.85 seconds

```

nmap -T4 -p 53 --script dns-brute scanme.nmap.org

```

(root@kali)-[/home/kali]
# nmap -T4 -p 53 --script dns-brute scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-09 03:09 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.20s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f

PORT      STATE SERVICE
53/tcp    closed domain

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
|   *A: 50.116.1.184
|_  *AAAA: 2600:3c01:e000:3e6::6d4e:7061

Nmap done: 1 IP address (1 host up) scanned in 31.09 seconds

```