

Network scanning using Nmap

Name-> Vijay Bhushan Singh

E-mail-> vijay8303blw@gmail.com

College-> Indian Institute of Information Technology, Manipur

Phone_no-> 8303420912

1) Basic Nmap Scan against IP or host.

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



```
172.31.111.44 - Remote Desktop Connection
Applications Places Terminal Jun 8 14:32
cdac@kali: ~
(cdac@kali)-[~]
$ nmap 172.31.109.108
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-08 14:29 PDT
Nmap scan report for 172.31.109.108
Host is up (0.00027s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server
5157/tcp   open  wsdaapi

Nmap done: 1 IP address (1 host up) scanned in 3.55 seconds

(cdac@kali)-[~]
$ nmap -p 1-65535 172.31.109.108
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-08 14:29 PDT
Stats: 0:01:32 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 85.18% done; ETC: 14:31 (0:00:16 remaining)
Nmap scan report for 172.31.109.108
Host is up (0.00030s latency).
Not shown: 65522 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1536/tcp   open  wopr-inter
1537/tcp   open  sdsc-lm
1538/tcp   open  3ds-lm
1540/tcp   open  rds
1541/tcp   open  rds2
1552/tcp   open  pciarray
1589/tcp   open  vqp
3389/tcp   open  ms-wbt-server
5157/tcp   open  wsdaapi
8834/tcp   open  nessus-xmllrpc

Nmap done: 1 IP address (1 host up) scanned in 114.36 seconds

(cdac@kali)-[~]
$
```

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

4) Scan multiple IP addresses.

```
172.31.111.44 - Remote Desktop Connection
Applications Places Terminal Jun 8 14:34
cdac@kali: -
(cdac@kali)-[~]
└─$ nmap -p 69,720 172.31.109.108
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-08 14:33 PDT
Nmap scan report for 172.31.109.108
Host is up (0.00076s latency).

PORT      STATE SERVICE
69/tcp    closed tftp
720/tcp   closed unknown

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds

(cdac@kali)-[~]
└─$ nmap 172.31.109.108,169
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-08 14:34 PDT
Nmap scan report for 172.31.109.108
Host is up (0.00013s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsddapi

Nmap scan report for 172.31.109.169
Host is up (0.00015s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server

Nmap done: 2 IP addresses (2 hosts up) scanned in 2.98 seconds

(cdac@kali)-[~]
└─$
```

5) Scan IP ranges.

```
172.31.111.44 - Remote Desktop Connection
Applications Places Terminal Jan 8 14:18
cnc@kali:~$ nmap 172.31.109.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-08 14:18 PST
Nmap scan report for 172.31.109.39
Host is up (0.0001s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
3337/tcp  open  wsdapi

Nmap scan report for 172.31.109.37
Host is up (0.0001s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
3337/tcp  open  wsdapi

Nmap scan report for 172.31.109.36
Host is up (0.0001s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
3337/tcp  open  wsdapi

Nmap scan report for 172.31.109.71
Host is up (0.0002s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
3337/tcp  open  wsdapi

Nmap scan report for 172.31.109.83
Host is up (0.0002s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
3337/tcp  open  wsdapi

Nmap scan report for 172.31.109.106
Host is up (0.0002s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
3337/tcp  open  wsdapi
```

```
172.31.111.44 - Remote Desktop Connection
3389/tcp open  ms-wbt-server

Nmap scan report for 172.31.109.109
Host is up (0.0001s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
3337/tcp  open  wsdapi

Nmap scan report for 172.31.109.170
Host is up (0.0002s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
3337/tcp  open  wsdapi

Nmap scan report for 172.31.109.185
Host is up (0.0004s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
3337/tcp  open  wsdapi

Nmap scan report for 172.31.109.190
Host is up (0.0002s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
3337/tcp  open  wsdapi

Nmap scan report for 172.31.109.242
Host is up (0.0002s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
3337/tcp  open  wsdapi

Nmap scan report for 172.31.109.246
Host is up (0.0001s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
3337/tcp  open  wsdapi

Nmap done: 256 IP addresses (16 hosts up) scanned in 7.11 seconds
```

Scanning the class range using (*)

```
172.31.111.44 - Remote Desktop Connection
Applications Places Terminal Jun 8 14:40
cdac@kali: ~
Nmap done: 256 IP addresses (16 hosts up) scanned in 7.11 seconds
--[cdac@kali]--[
_ _ _ _ _
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-08 14:38 PDT
Nmap scan report for 172.31.109.18
Host is up (0.00092s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi

Nmap scan report for 172.31.109.17
Host is up (0.00075s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1556/tcp  open  veritas_pbx
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi

Nmap scan report for 172.31.109.58
Host is up (0.0011s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server

Nmap scan report for 172.31.109.71
Host is up (0.0011s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server

Nmap scan report for 172.31.109.85
Host is up (0.0011s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server

Nmap scan report for 172.31.109.186
Host is up (0.0011s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
```

```
172.31.111.44 - Remote Desktop Connection
Applications Places Terminal Jun 8 14:40
cdac@kali: ~
Nmap scan report for 172.31.109.169
Host is up (0.00068s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server

Nmap scan report for 172.31.109.170
Host is up (0.0012s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server

Nmap scan report for 172.31.109.185
Host is up (0.0014s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server

Nmap scan report for 172.31.109.190
Host is up (0.00088s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server

Nmap scan report for 172.31.109.242
Host is up (0.00061s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server

Nmap scan report for 172.31.109.246
Host is up (0.00055s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi

Nmap done: 256 IP addresses (16 hosts up) scanned in 6.31 seconds
```

When scanning entire range we may need to exclude some IP address

```
172.31.111.44 - Remote Desktop Connection

[~](cdac@kali)-[~]
└─$ nmap 172.31.109.* --exclude 172.31.109.108 235
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-06 14:37 PDT
Nmap scan report for 172.31.109.38
Host is up (0.00063s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi

Nmap scan report for 172.31.109.37
Host is up (0.00037s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1356/tcp  open  veritas_pbx
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi

Nmap scan report for 172.31.109.38
Host is up (0.00031s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server

Nmap scan report for 172.31.109.71
Host is up (0.00037s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server

Nmap scan report for 172.31.109.05
Host is up (0.00035s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server

Nmap scan report for 172.31.109.137
Host is up (0.00048s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
```

```
172.31.111.44 - Remote Desktop Connection

nmap scan report for 172.31.109.109
Host is up (0.00029s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server

Nmap scan report for 172.31.109.170
Host is up (0.00037s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server

Nmap scan report for 172.31.109.185
Host is up (0.00055s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server

Nmap scan report for 172.31.109.198
Host is up (0.00045s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server

Nmap scan report for 172.31.109.242
Host is up (0.00046s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server

Nmap scan report for 172.31.109.246
Host is up (0.00033s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi

Nmap done: 255 IP addresses (15 hosts up) scanned in 5.49 seconds
[~](cdac@kali)-[~]
```

6) Scan the most popular ports.

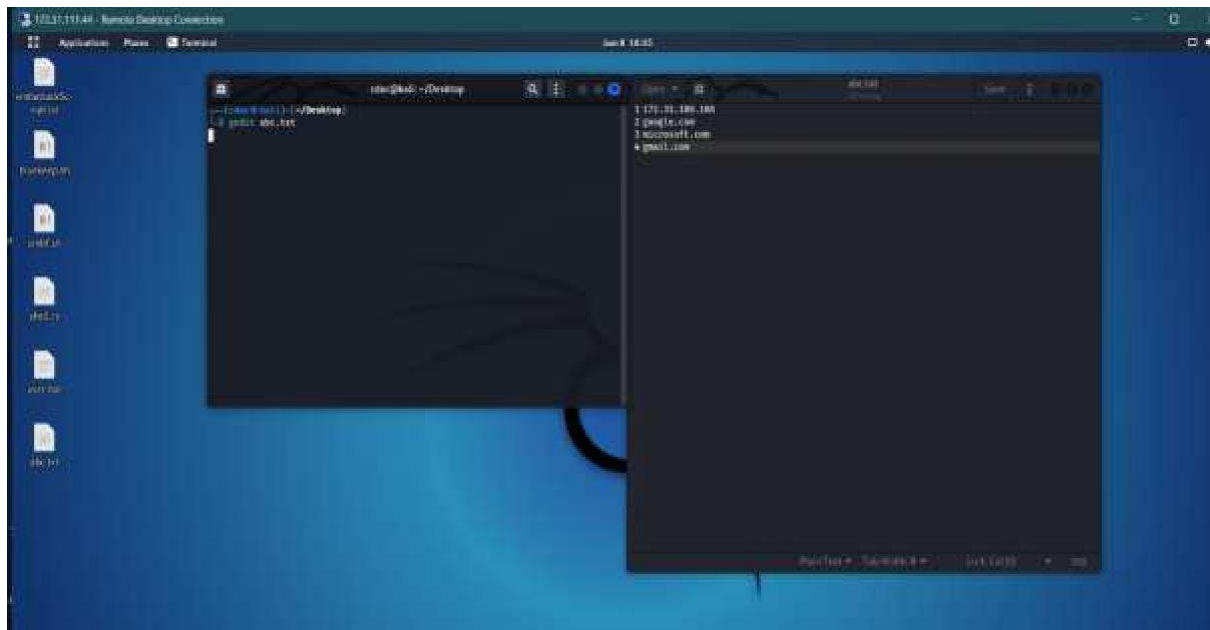
```
172.31.111.44 - Remote Desktop Connection
Applications Places Terminal Jun 8 14:47
cdac@kali: ~
—(cdac@kali)~—
$ nmap --top-ports 20 172.31.109.108
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-08 14:46 PDT
Nmap scan report for 172.31.109.108
Host is up (0.00045s latency).

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   open  msrpc
139/tcp   open  netbios-ssn
143/tcp   closed imap
443/tcp   closed https
445/tcp   open  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

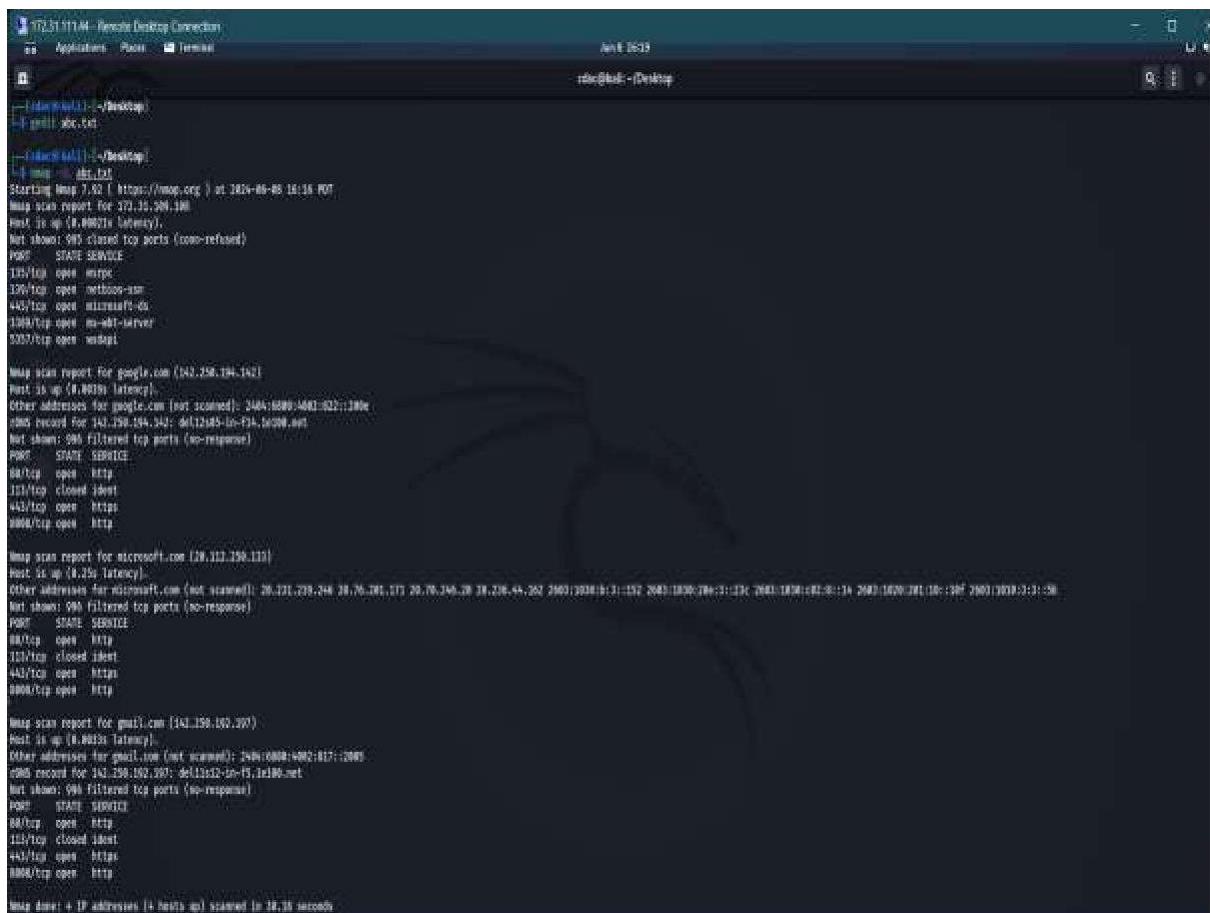
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
—(cdac@kali)~—
```


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

TEXT FILE NAME- abc.txt



Scanning all the hosts listed.



8) Save your Nmap scan results to a file.

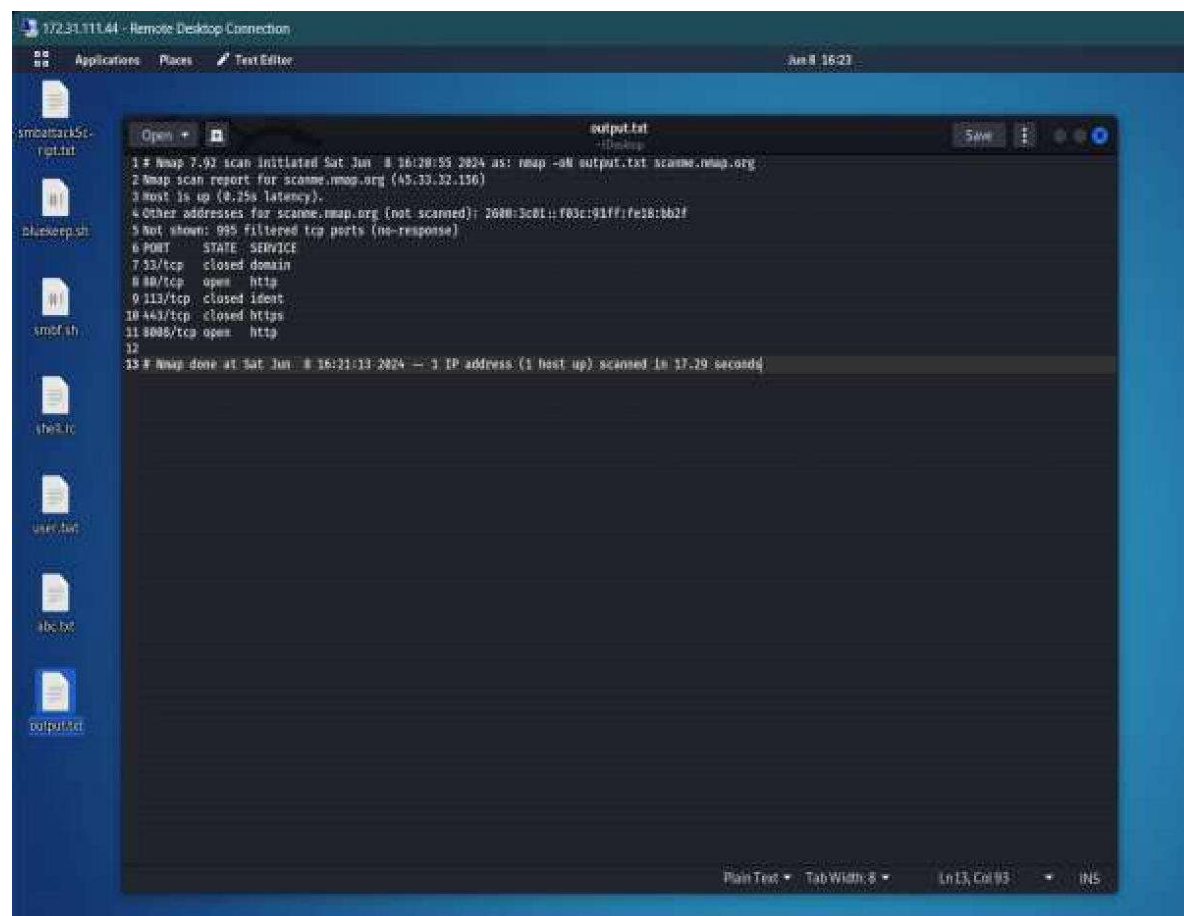
```
Nmap done: 4 IP addresses (4 hosts up) scanned in 30.18 seconds

(cdar@kali)-[~/Desktop]
$ nmap -oN output.txt scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-08 16:20 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
53/tcp    closed domain
80/tcp    open  http
113/tcp   closed ident
443/tcp   closed https
8080/tcp  open  http

Nmap done: 1 IP address (1 host up) scanned in 17.29 seconds

(cdar@kali)-[~/Desktop]
$
```

OUTPUT FILE- output.txt



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

```
172.31.111.44 - Remote Desktop Connection
Applications Places Terminal Jun 8 16:50
cdac@kali: ~
[cdac@kali]~$ nmap -A -T5 scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-08 16:27 PDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.32 seconds

[cdac@kali]~$ nmap -A -T5 scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-08 16:28 PDT
Stats: 0:01:22 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 30.00% done; ETC: 10:30 (0:01:04 remaining)
Stats: 0:03:39 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.64% done; ETC: 16:32 (0:00:00 remaining)
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))
111/tcp   closed ident
443/tcp   closed https
8080/tcp  open  http?

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 239.33 seconds

[cdac@kali]~$ nmap -A -T6 172.31.109.108
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-08 16:33 PDT
Nmap scan report for 172.31.109.108
Host is up (0.00022s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
135/tcp   open  wsrpc   Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 10 Pro 10240 microsoft-ds (workgroup: WORKGROUP)
3389/tcp  open  ssl/ms-wbt-server?
ssl-cert: Subject: commonName=DESKTOP-K0E0N56
Not valid before: 2024-05-19T19:05:16
Not valid after: 2024-11-18T19:05:16
ssl-date: 2024-06-09T06:34:15+00:00; +7h00m00s from scanner time.
rdp-ntlm-info:
Target_Name: DESKTOP-K0E0N56
NetBIOS_Domain_Name: DESKTOP-K0E0N56
NetBIOS_Computer_Name: DESKTOP-K0E0N56
DNS_Domain_Name: DESKTOP-K0E0N56
DNS_Computer_Name: DESKTOP-K0E0N56
Product_Version: 10.0.10240
System_Time: 2024-06-09T06:34:09+00:00
5357/tcp  open  http    Microsoft HTTPAPI httpd 2.0 (SSOP/UPnP)
_http-server-header: Microsoft-HTTPAPI/2.0
_http-title: Service Unavailable
Service Info: Host: DESKTOP-K0E0N56; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
_smb2-security-mode:
3.1.1:
- Message signing enabled but not required
_clock-skew: mean: 8h23m59s, deviation: 3h07m49s, median: 6h59m59s
_nbstat: NetBIOS name: nil, NetBIOS user: <unknown>, NetBIOS MAC: 50:6b:8d:aa:46:73 (Nutanix)
_smb-security-mode:
account_used: guest
authentication_level: user
challenge_response: supported
message_signing: disabled (dangerous, but default)
_smb2-time:
date: 2024-06-09T06:34:09
start_date: 2024-06-09T03:56:26
_smb-os-discovery:
OS: Windows 10 Pro 10240 (Windows 10 Pro 6.3)
OS CPE: cpe:/o:microsoft:windows_10::-
Computer name: DESKTOP-K0E0N56
NetBIOS computer name: DESKTOP-K0E0N56\x00
Workgroup: WORKGROUP\x00
System time: 2024-06-08T23:34:09-07:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 75.49 seconds

[cdac@kali]~$
```

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

10) Detect service/daemon versions.

```
172.31.111.44 - Remote Desktop Connection
Applications Places Terminal Jun 8 17:01
cdac@kali: ~
(cdac@kali)-[~]
$ nmap -sV localhost
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-08 16:52 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000081s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 998 closed tcp ports (conn-refused)
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 11.99 seconds

(cdac@kali)-[~]
$ nmap -sV 172.31.109.108
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-08 16:59 PDT
Nmap scan report for 172.31.109.108
Host is up (0.00029s latency).
Not shown: 995 closed tcp ports (conn-refused)
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 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3389/tcp  open  ssl/ms-wbt-server?
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: Host: DESKTOP-K0E0N56; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 68.79 seconds

(cdac@kali)-[~]
$
```

11) Scan using TCP or UDP protocols.

TCP protocol:

```
172.31.111.44 - Remote Desktop Connection
Applications Places Terminal Jun 8 17:03
cdac@kali: ~
(cdac@kali)-[~]
$ nmap -sT 172.31.109.108
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-08 17:02 PDT
Nmap scan report for 172.31.109.108
Host is up (0.00044s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server
5357/tcp   open  wsdapi
Nmap done: 1 IP address (1 host up) scanned in 10.13 seconds

(cdac@kali)-[~]
$ nmap -sT localhost
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-08 17:02 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000055s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
3001/tcp   open  nessus
3389/tcp   open  ms-wbt-server
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

UDP Protocol:

```
172.31.111.44 - Remote Desktop Connection
Applications Places Terminal Jun 8 17:08
cdac@kali: ~
(cdac@kali)-[~]
$ sudo nmap -sU 172.31.109.108
[sudo] password for cdac:
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-08 17:05 PDT
Nmap scan report for 172.31.109.108
Host is up (0.00041s latency).
Not shown: 743 closed udp ports (port-unreach), 256 open/filtered udp ports (no-response)
PORT      STATE SERVICE
137/udp    open  netbios-ns
MAC Address: 50:6B:BD:AA:46:73 (Nutanix)
Nmap done: 1 IP address (1 host up) scanned in 63.27 seconds

(cdac@kali)-[~]
$ sudo nmap -sU localhost
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-08 17:08 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000050s latency).
Other addresses for localhost (not scanned): ::1
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed udp ports (port-unreach)
Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds

(cdac@kali)-[~]
$
```

12) Finding multiple live hosts in the network.

```
172.31.111.44 - Remote Desktop Connection
Applications Places Terminal Jun 8 17:11
cdac@kali: ~
(cdac@kali)-[~]
$ nmap -sP 172.31.109.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-08 17:11 PDT
Nmap scan report for 172.31.109.30
Host is up (0.0032s latency).
Nmap scan report for 172.31.109.37
Host is up (0.0020s latency).
Nmap scan report for 172.31.109.50
Host is up (0.0057s latency).
Nmap scan report for 172.31.109.71
Host is up (0.0016s latency).
Nmap scan report for 172.31.109.85
Host is up (0.0032s latency).
Nmap scan report for 172.31.109.98
Host is up (0.010s latency).
Nmap scan report for 172.31.109.108
Host is up (0.0030s latency).
Nmap scan report for 172.31.109.137
Host is up (0.0015s latency).
Nmap scan report for 172.31.109.139
Host is up (0.0043s latency).
Nmap scan report for 172.31.109.160
Host is up (0.0016s latency).
Nmap scan report for 172.31.109.162
Host is up (0.0057s latency).
Nmap scan report for 172.31.109.169
Host is up (0.0041s latency).
Nmap scan report for 172.31.109.170
Host is up (0.0061s latency).
Nmap scan report for 172.31.109.185
Host is up (0.0029s latency).
Nmap scan report for 172.31.109.190
Host is up (0.0034s latency).
Nmap scan report for 172.31.109.242
Host is up (0.0035s latency).
Nmap scan report for 172.31.109.246
Host is up (0.0019s latency).
Nmap done: 256 IP addresses (17 hosts up) scanned in 4.99 seconds
(cdac@kali)-[~]
$
```

14) Finding the system with incremental ip-id.

```
172.31.111.44 - Remote Desktop Connection
Applications Places Terminal Jun 8 17:20
cdac@kali: ~
[cdac@kali]~$ nmap -p 80 --rate ipidseq -iL 1000
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-08 17:17 PDT
NSE: [ipidseq] not running for lack of privileges.
Nmap scan report for ec2-34-198-177-3.compute-1.amazonaws.com (34.198.177.3)
Host is up (0.26s latency).

PORT      STATE SERVICE
80/tcp    filtered http

Nmap scan report for 43.250.82.161
Host is up (0.056s latency).

PORT      STATE SERVICE
80/tcp    closed http

Nmap scan report for 191.62.100.100
Host is up (0.38s latency).

PORT      STATE SERVICE
80/tcp    closed http

Nmap scan report for 183.171.51.48
Host is up (0.839s latency).

PORT      STATE SERVICE
80/tcp    closed http

Nmap scan report for broadband-178-148-65-162.ip.moscow.rt.ru (178.148.65.162)
Host is up (0.25s latency).

PORT      STATE SERVICE
80/tcp    closed http

Nmap scan report for softbank126221160240.bbtec.net (126.221.160.240)
Host is up (0.18s latency).

PORT      STATE SERVICE
80/tcp    filtered http

Nmap scan report for sp-fo-97.spectar.tv (23.109.150.201)
Host is up (0.16s latency).

PORT      STATE SERVICE
80/tcp    open  http

Nmap scan report for 49.166.75.1
Host is up (0.16s latency).
```

```
172.31.111.44 - Remote Desktop Connection
Nmap scan report for 14.50.94.144
Host is up (0.16s latency).

PORT      STATE SERVICE
80/tcp    filtered http

Nmap scan report for 211.194.201.143
Host is up (0.17s latency).

PORT      STATE SERVICE
80/tcp    filtered http

Nmap scan report for host-79-26-115-61.retail.telecomitalia.it (79.26.115.61)
Host is up (0.21s latency).

PORT      STATE SERVICE
80/tcp    closed http

Nmap scan report for 61.174.90.112
Host is up (0.26s latency).

PORT      STATE SERVICE
80/tcp    filtered http

Nmap scan report for 4.241.24.86
Host is up (0.14s latency).

PORT      STATE SERVICE
80/tcp    open  http

Nmap scan report for host-79-10-34-20.business.telecomitalia.it (79.10.34.20)
Host is up (0.18s latency).

PORT      STATE SERVICE
80/tcp    closed http

Nmap scan report for 40.44.140.31
Host is up (0.0060s latency).

PORT      STATE SERVICE
80/tcp    open  http

Nmap scan report for 154.212.8.238
Host is up (0.30s latency).

PORT      STATE SERVICE
80/tcp    closed http

Nmap done: 1000 IP addresses (51 hosts up) scanned in 37.33 seconds
[cdac@kali]~$
```


15) Performing idle scanning using nmap(zombie scanning).

```
(cdac@kali)-[~]
└─$ nmap --script ipidseq 172.31.109.108
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-08 17:44 PDT
NSE: [ipidseq] not running for lack of privileges.
Nmap scan report for 172.31.109.108
Host is up (0.00013s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server
5357/tcp   open  wsddapi

Nmap done: 1 IP address (1 host up) scanned in 3.66 seconds

(cdac@kali)-[~]
```

16) Bypassing firewall using fragmentation.

```
172.31.111.44 - Remote Desktop Connection
Applications Places Terminal Jun 8 17:52
cdac@kali: ~

(cdac@kali)-[~]
└─$ nmap -mtu 16 scanme.org
Sorry, but fragscan requires root privileges.
QUITTING!

(cdac@kali)-[~]
└─$ sudo nmap -mtu 16 scanme.org
[sudo] password for cdac:
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-08 17:51 PDT
Nmap scan report for scanme.org (45.33.32.156)
Host is up (0.22s latency).
Other addresses for scanme.org (not scanned): 2600:3c01::f03c:91ff:fe18:b02f
vDNS record for 45.33.32.156: scanme.nmap.org
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    closed domain
80/tcp    open  http
113/tcp   closed ident
443/tcp   closed https
8080/tcp   open  http

Nmap done: 1 IP address (1 host up) scanned in 19.17 seconds

(cdac@kali)-[~]
└─$ sudo nmap -mtu 16 172.31.109.108
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-08 17:52 PDT
Nmap scan report for 172.31.109.108
Host is up (0.00029s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server
5357/tcp   open  wsddapi
MAC Address: 58:6B:BD:AA:46:73 (Nutanix)

Nmap done: 1 IP address (1 host up) scanned in 10.27 seconds

(cdac@kali)-[~]
└─$
```


17) Stealthy scan to avoid firewall detection.

```
172.31.111.44 - Remote Desktop Connection
Applications Places Terminal Jun 8 17:58
cdac@kali: ~
(cdac@kali)-[~]
$ sudo nmap -ss 172.31.109.108
[sudo] password for cdac:
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-08 17:56 PDT
Nmap scan report for 172.31.109.108
Host is up (0.00045s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  nsrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server
5357/tcp   open  wsdapi
MAC Address: 50:6B:8D:AA:46:73 (Nutanix)

Nmap done: 1 IP address (1 host up) scanned in 10.21 seconds

(cdac@kali)-[~]
$ sudo nmap -ss scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-08 17:56 PDT
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 tcp ports (no-response)
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 17.72 seconds

(cdac@kali)-[~]
$
```

18) Using Nmap Script engine.

USING:



```
172.31.111.44 - Remote Desktop Connection
Applications Places Terminal Jun 8 18:13
cdac@kali: -
(cdac@kali)-[~]
$ nmap --script vuln 172.31.109.108
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-08 18:12 PDT
Nmap scan report for 172.31.109.108
Host is up (0.00012s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server
5357/tcp   open  wsddapi

Host script results:
_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
_smb-vuln-ms17-010:
  VULNERABLE:
  Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
  State: VULNERABLE
  IDs: CVE:CVE-2017-0143
  Risk factor: HIGH
  A critical remote code execution vulnerability exists in Microsoft SMBv1
  servers (ms17-010).

  Disclosure date: 2017-03-14
  References:
    https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
    https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
    https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 42.74 seconds

(cdac@kali)-[~]
$
```

19) DNS Enumeration.

```
172.31.111.44 - Remote Desktop Connection
Applications Places Terminal Jun 8 18:06
cdac@kali: -
(cdac@kali)-[~]
$ nmap --script=broadcast-dns-service-discovery scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-08 18:05 PDT
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 tcp ports (no-response)
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 28.06 seconds
(cdac@kali)-[~]
$
```

Trying to enumerate DNS hostnames by brute force guessing of common subdomains.

```
172.31.111.44 - Remote Desktop Connection
Applications Places Terminal Jun 8 18:08
cdac@kali: -
(cdac@kali)-[~]
$ nmap -T4 -p 53 --script=dns-brute scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-08 18:07 PDT
Stats: 0:00:00 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done
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

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 24.51 seconds
(cdac@kali)-[~]
$ nmap -T4 -p 53 --script=dns-brute 172.31.109.108
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-08 18:08 PDT
Nmap scan report for 172.31.109.108
Host is up (0.00092s latency).

PORT      STATE SERVICE
53/tcp    closed domain

Host script results:
|_ dns-brute: Can't guess domain of "172.31.109.108"; use dns-brute.domain script argument.

Nmap done: 1 IP address (1 host up) scanned in 0.51 seconds
(cdac@kali)-[~]
$
```