



# **REPORT OF ENUMERATION**

## **MODULE 4**

**Aniket Sunil Pagare.**

# Enumeration.

**Enumeration** is the process of actively gathering detailed information about a target system, network, or application to identify potential attack vectors.

Objectives -:

- Machine names, their OSes, services, and ports
- Network resources
- Usernames and user groups
- Lists of shares on individual hosts on the network
- Policies and passwords
- Routing tables
- Audit and service settings
- SNMP details

# Netbios Enumeration .

NetBIOS stands for Network Basic Input Output System. Windows uses NetBIOS for file and printer sharing.

NetBIOS used port number 137 (UDP) , 138 (UDP) , 139 (TCP) .

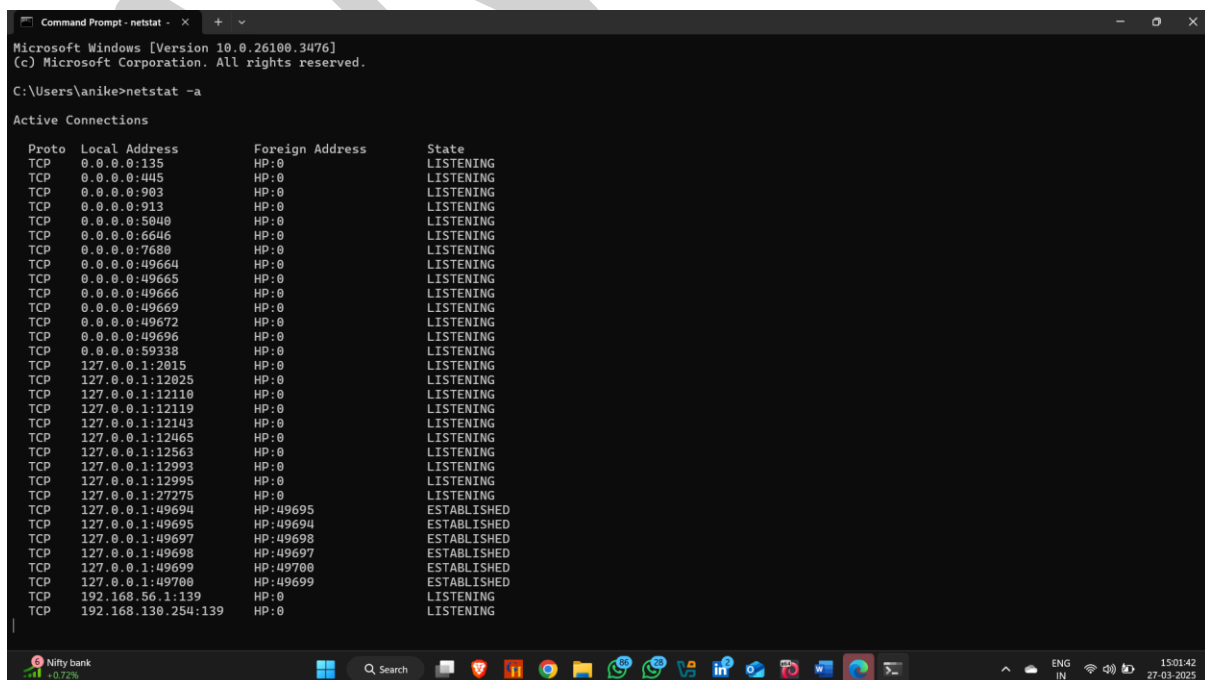
## 1.Netbios Enumeration With Windows

**How to use it –**

Step 1 : open windows command line (CMD).

Step 2 : type netstat -a

- the -a option in the netstat command is used to **display all active connections and listening ports.**



```
Microsoft Windows [Version 10.0.26100.3476]
(c) Microsoft Corporation. All rights reserved.

C:\Users\anike>netstat -a

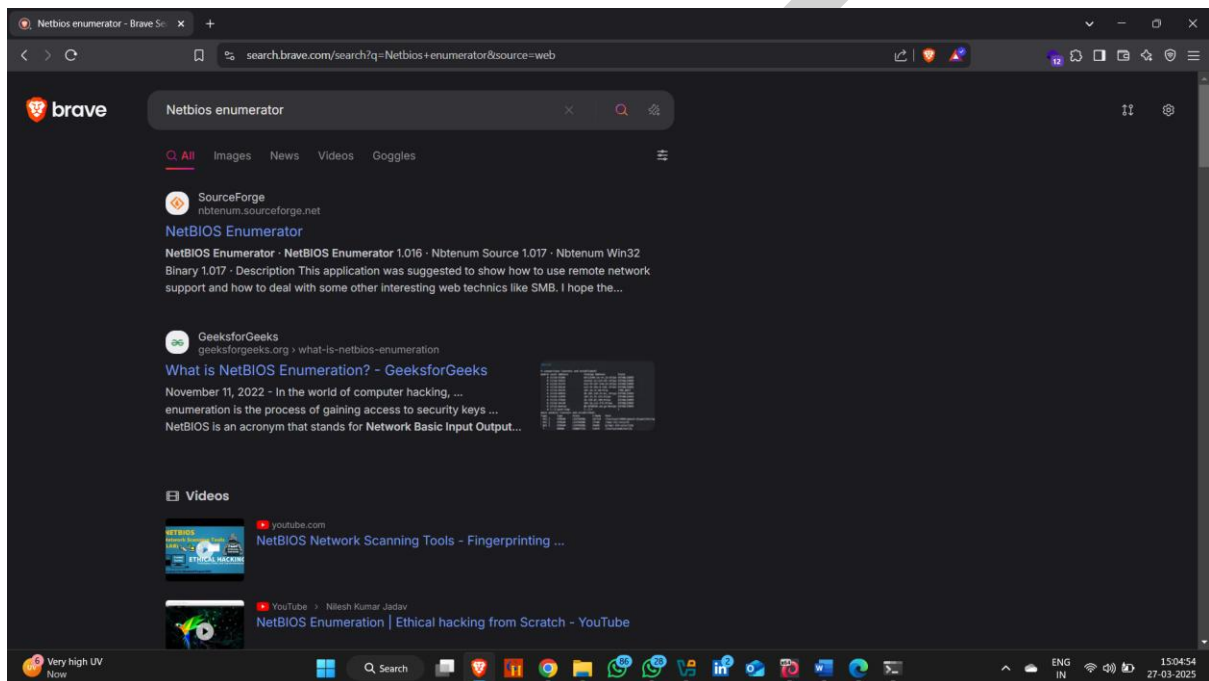
Active Connections
Proto Local Address           Foreign Address         State
TCP    0.0.0.0:135              HP:0                    LISTENING
TCP    0.0.0.0:445              HP:0                    LISTENING
TCP    0.0.0.0:903              HP:0                    LISTENING
TCP    0.0.0.0:913              HP:0                    LISTENING
TCP    0.0.0.0:5040             HP:0                    LISTENING
TCP    0.0.0.0:6646             HP:0                    LISTENING
TCP    0.0.0.0:7680             HP:0                    LISTENING
TCP    0.0.0.0:49664            HP:0                    LISTENING
TCP    0.0.0.0:49665            HP:0                    LISTENING
TCP    0.0.0.0:49666            HP:0                    LISTENING
TCP    0.0.0.0:49669            HP:0                    LISTENING
TCP    0.0.0.0:49672            HP:0                    LISTENING
TCP    0.0.0.0:49696            HP:0                    LISTENING
TCP    0.0.0.0:59338            HP:0                    LISTENING
TCP    127.0.0.1:2015            HP:0                    LISTENING
TCP    127.0.0.1:12025           HP:0                    LISTENING
TCP    127.0.0.1:12110           HP:0                    LISTENING
TCP    127.0.0.1:12119           HP:0                    LISTENING
TCP    127.0.0.1:12143           HP:0                    LISTENING
TCP    127.0.0.1:12465           HP:0                    LISTENING
TCP    127.0.0.1:12563           HP:0                    LISTENING
TCP    127.0.0.1:12993           HP:0                    LISTENING
TCP    127.0.0.1:12995           HP:0                    LISTENING
TCP    127.0.0.1:27275           HP:0                    LISTENING
TCP    127.0.0.1:49694           HP:49695               ESTABLISHED
TCP    127.0.0.1:49695           HP:49694               ESTABLISHED
TCP    127.0.0.1:49696           HP:49698               ESTABLISHED
TCP    127.0.0.1:49697           HP:49697               ESTABLISHED
TCP    127.0.0.1:49699           HP:49700               ESTABLISHED
TCP    127.0.0.1:49700           HP:49699               ESTABLISHED
TCP    192.168.56.1:139          HP:0                    LISTENING
TCP    192.168.130.254:139      HP:0                    LISTENING
```

## 2.NetBIOS Enumeration Using NetBIOS Enumerator

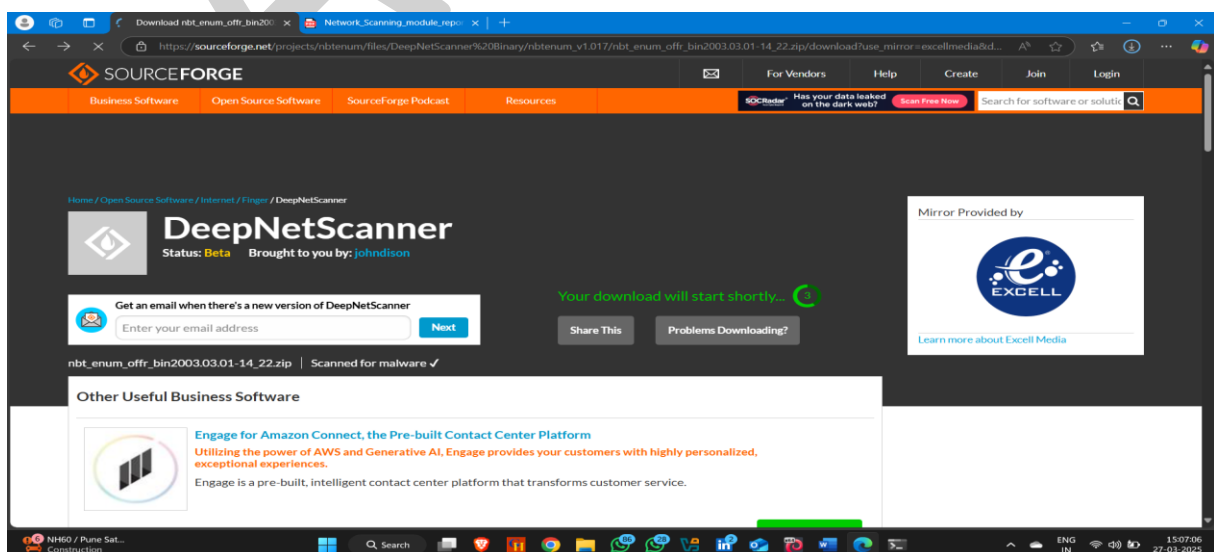
**How to use it -:**

Step 1 : open your browser and search netbios enumerator

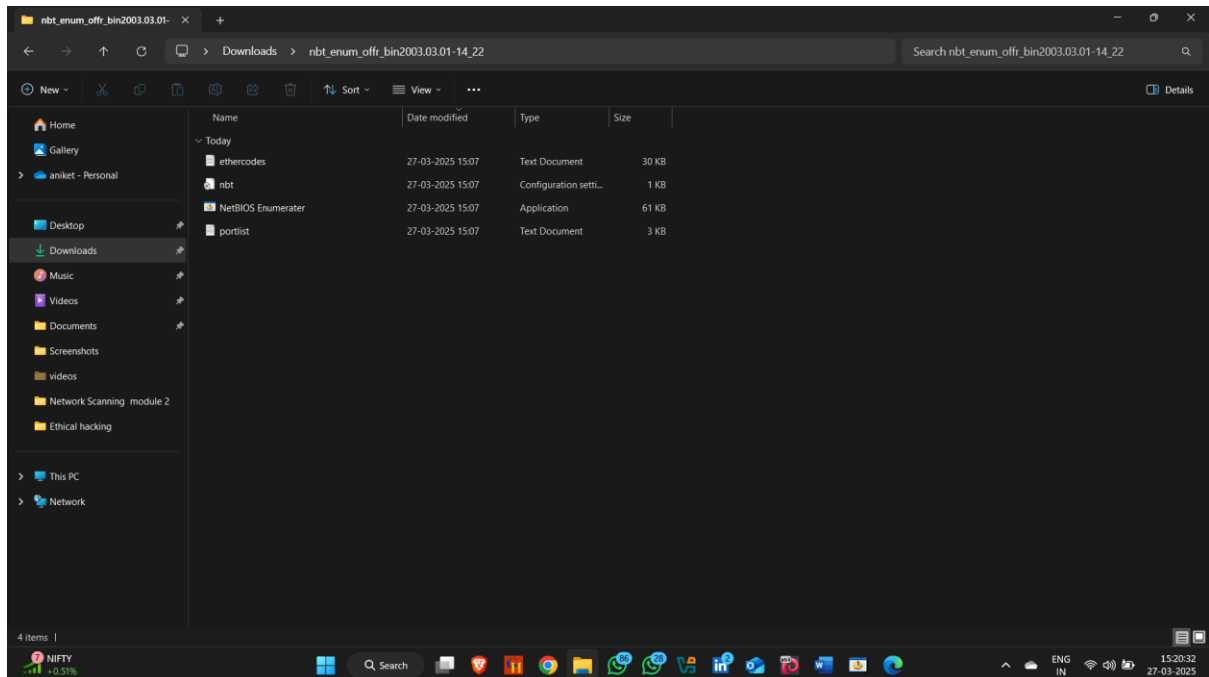
Step 2 : click on **sourceforge** website



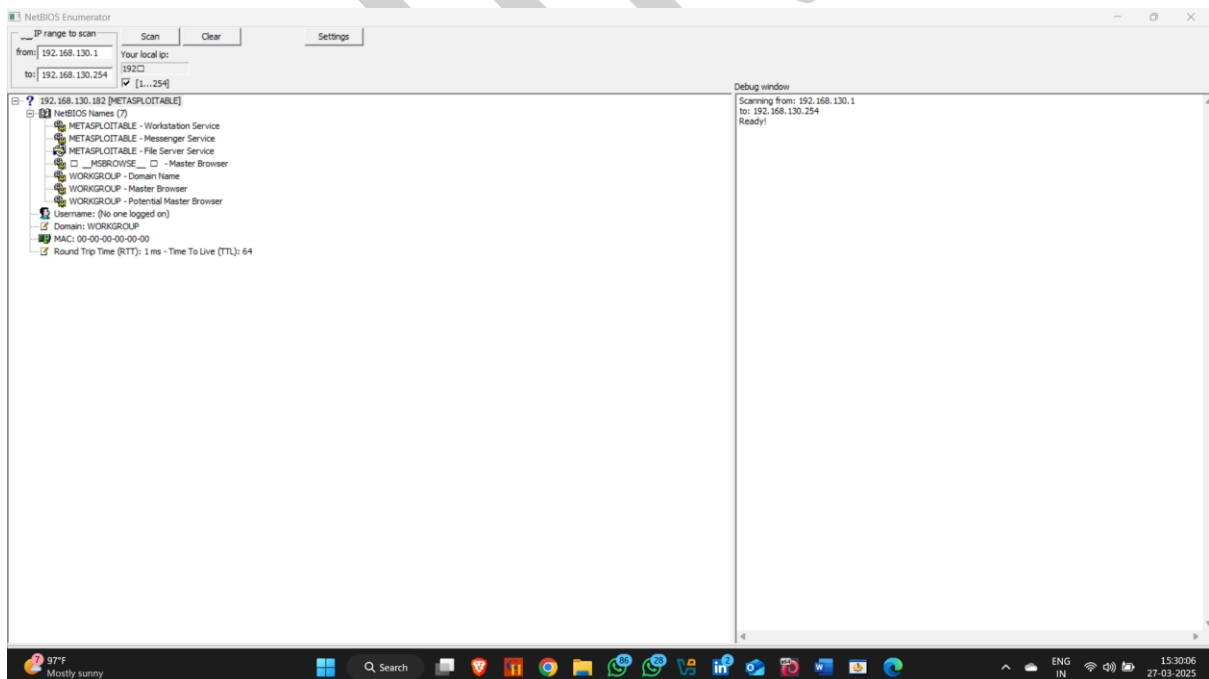
Wait few seconds download will start automatically



### Step 3 : Extract folder and then open it , now double click on **NetBIOS Enumerator**



### Step 4 : Provide IP range and click on scan



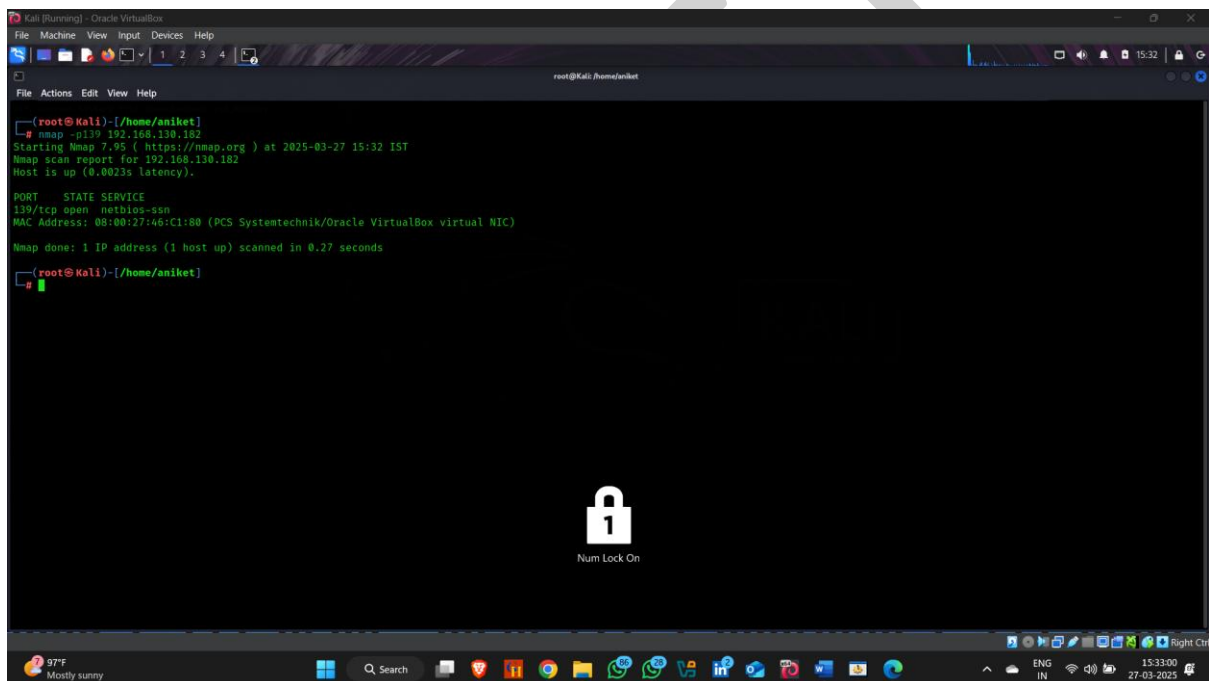
## 3. Netbios Enumeration With NSE Scripts.

How to use it -:

Step 1 : Open kali linux / Parrot Os

Step 2 : To perform NetBIOS using NSE script ,**kindly check the netbios port are open or close on your target**

Step 3 : Check netbios port are open or closed using nmap



```
(root@kali)-[/home/aniket]
# nmap -p139 192.168.130.162
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-27 15:32 IST
Nmap scan report for 192.168.130.162
Host is up (0.0023s latency).

PORT      STATE SERVICE
139/tcp    open  netbios-ssn
MAC Address: 08:00:27:46:C1:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds

(root@kali)-[/home/aniket]
```

Step 4 : Go to nmap scripts Directory using command

- **cd /usr/share/nmap/scripts**

step 5 : type `nmap -p139 --script=nbstat.nse <target ip>`

step 6 : perform a netbios enumeration on port number 139

```
Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@Kali: /home/aniket

ether 08:00:27:28:75:fa txqueuelen 1000 (Ethernet)
RX packets 512 bytes 68260 (66.6 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 422 bytes 41030 (40.0 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 8 bytes 480 (480.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 8 bytes 480 (480.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root@Kali)-[/home/aniket]
# nmap -p139 --script=nbstat.nse 192.168.130.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-27 16:02 IST
Nmap scan report for 192.168.130.102
Host is up (0.0015s latency).

PORT      STATE SERVICE
139/tcp   open  netbios-ssn
MAC Address: 08:00:27:46:C1:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Host script results:
nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
Names:
METASPLOITABLE<00>  Flags: <unique><active>
METASPLOITABLE<03>  Flags: <unique><active>
METASPLOITABLE<20>  Flags: <unique><active>
\*01\*02_MSSROWSE_  \*02\*01  Flags: <group><active>
WORKGROUP<00>      Flags: <group><active>
WORKGROUP<1d>      Flags: <unique><active>
WORKGROUP<1e>      Flags: <group><active>

Nmap done: 1 IP address (1 host up) scanned in 13.41 seconds

(root@Kali)-[/home/aniket]
#
```

# SNMP Enumeration

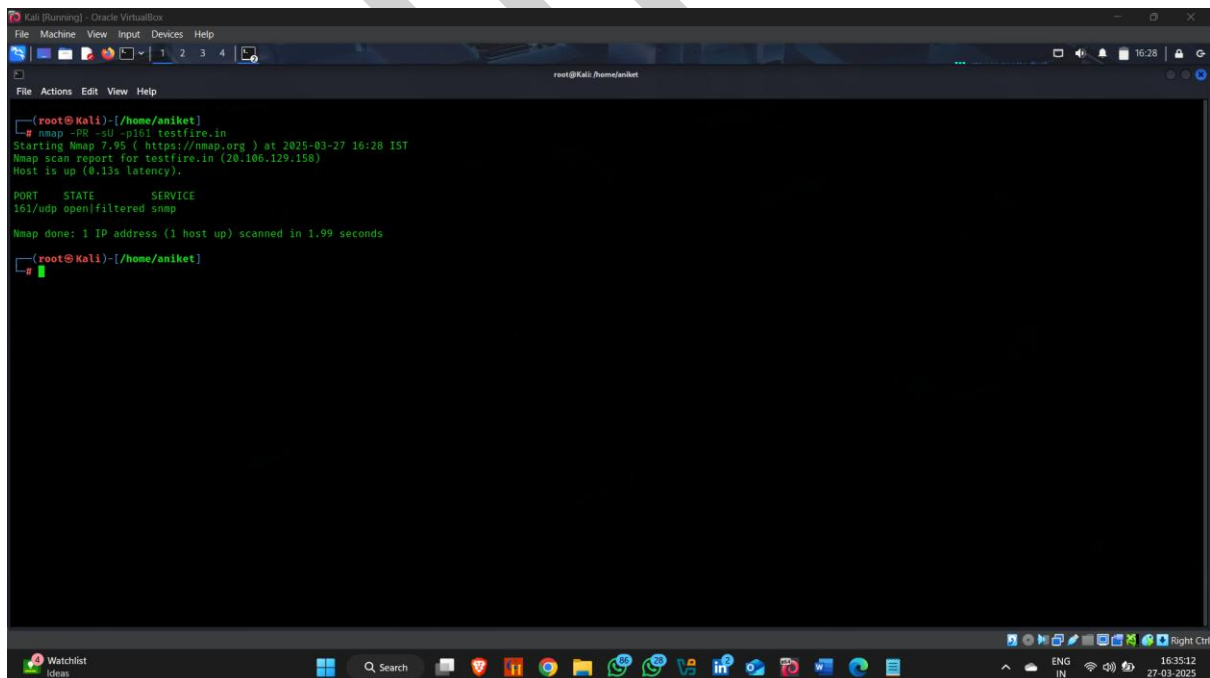
SNMP (application layer protocol) to obtain a list of user accounts and devices on system

SNMP operates on **UDP ports 161 and 162**.

## 1. SNMP Enumeration Using snmp-check

How to use it –

- Step 1 : first scan the target to check open port



```
(root@Kali)-[/home/aniket]
# nmap -PR -sU -p161 testfire.in
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-27 16:28 IST
Nmap scan report for testfire.in (20.106.129.158)
Host is up (0.13s latency).

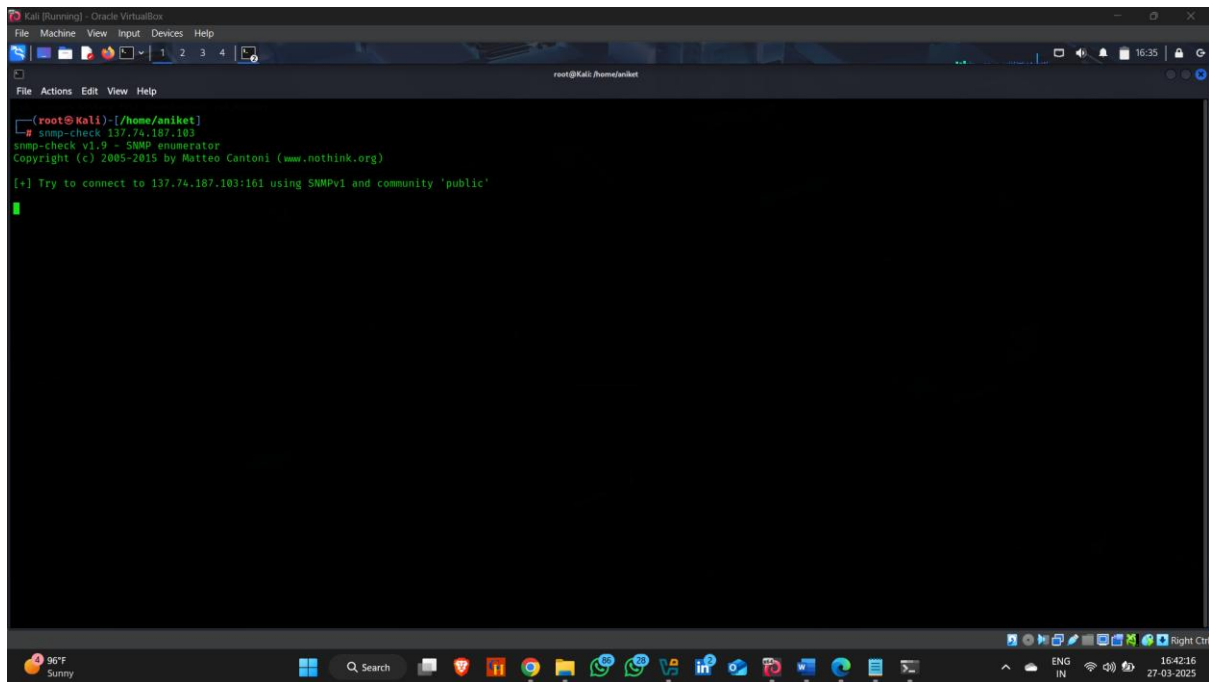
PORT      STATE      SERVICE
161/udp   open|filtered  snmp

Nmap done: 1 IP address (1 host up) scanned in 1.99 seconds

(root@Kali)-[/home/aniket]
```



- Step 2 : type snmp-check <target ip >



The screenshot shows a Kali Linux terminal window with the following text:

```
(root@kali)-[/home/aniket]
# snmp-check 137.74.187.103
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)
[+] Try to connect to 137.74.187.103:161 using SNMPv1 and community 'public'
```

## 2.SNMP Enumeration Using NSE

### How to use it -:

Step 1 : Open kali linux / Parrot Os

Step 2 : To perform SNMP using NSE script ,**kindly check the SNMP port are open or close on your target**

Step 3 : Check SNMP port are open or closed using nmap , **if filtered option display it means that firewall is there.**

```
Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

root@Kali: /usr/share/nmap/scripts

root@kali:~# nmap -iL 192.168.210.87
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-28 16:20 EST
Nmap scan report for 192.168.210.87
Host is up (0.0092s latency).

PORT      STATE SERVICE
201/tcp   filtered nmap
MAC Address: 08:00:27:4A:3F:9F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds

root@kali:~# nmap -iL 192.168.210.87
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-28 16:21 EST
Failed to resolve "nmap-ssh-login.nse".
Failed to resolve "nmap-info.nse".
Failed to resolve "nmap-interfaces.nse".
Failed to resolve "nmap-ssh-config.nse".
Failed to resolve "nmap-outstat.nse".
Failed to resolve "nmap-processexec.nse".
Failed to resolve "nmap-sysdescr.nse".
Failed to resolve "nmap-win32-services.nse".
Failed to resolve "nmap-win32-shares.nse".
Failed to resolve "nmap-win32-software.nse".
Failed to resolve "nmap-win32-users.nse".
Nmap scan report for 192.168.210.87
Host is up (0.058s latency).

PORT      STATE SERVICE
201/tcp   filtered nmap
MAC Address: 08:00:27:4A:3F:9F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 3.19 seconds

root@kali:~#
```

# SMB Enumeration

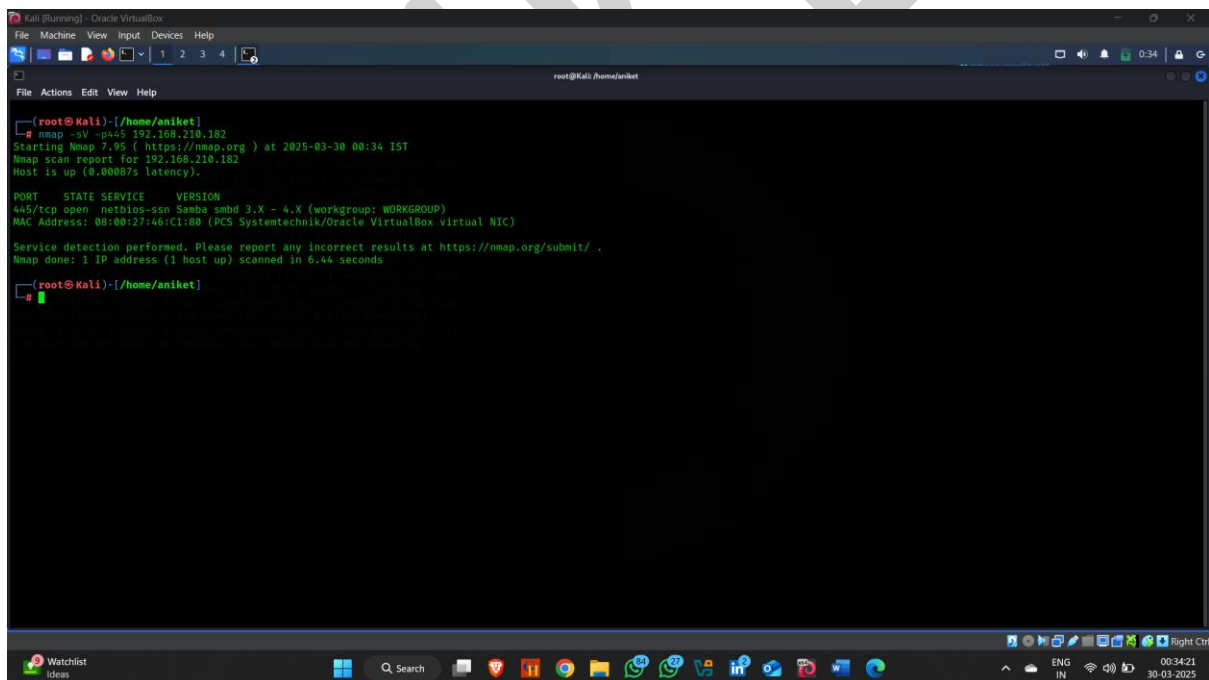
**SMB Enumeration** is the process of gathering information from **Server Message Block (SMB)** services on a network. SMB is a protocol used for file sharing, printer sharing, and communication between devices on a Windows network.

SMB operates on **TCP ports 445**

## SMB Enumeration Using NSE

**How to use it –**

- Step 1 : Open kali linux / Parrot Os
- Step 2 : first scan the target to check open port



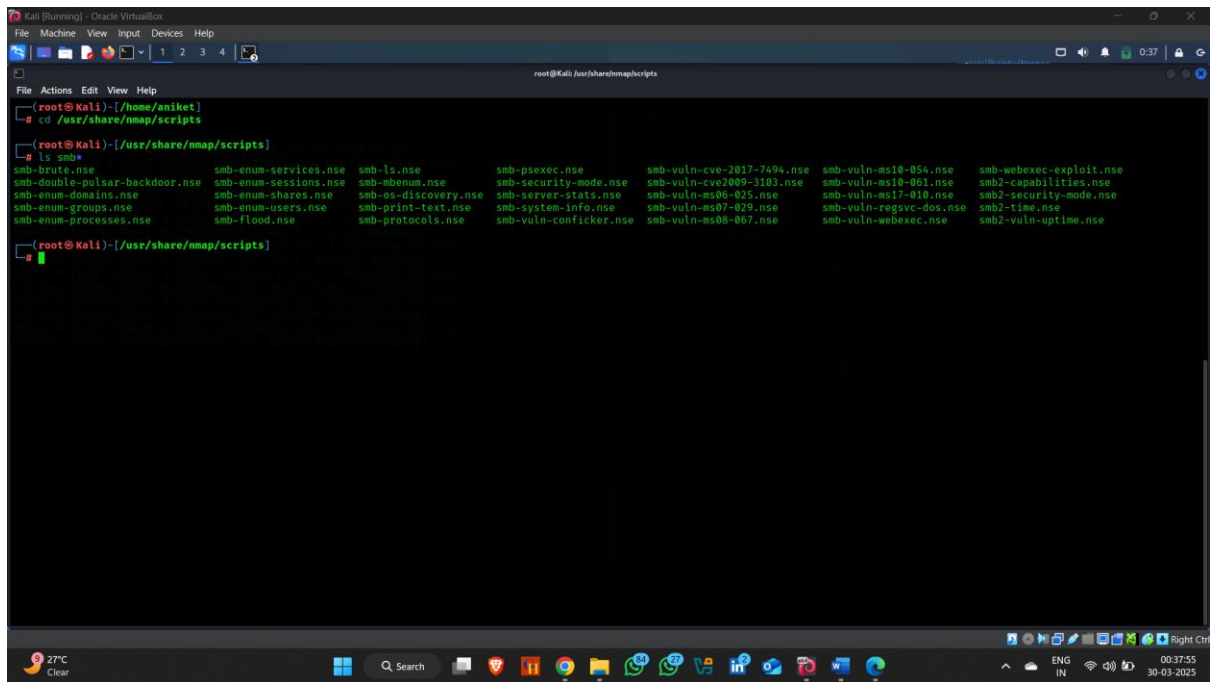
```
(root@kali)-[/home/aniket]
└─$ nmap -sV -p445 192.168.210.182
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-30 00:34 IST
Nmap scan report for 192.168.210.182
Host is up (0.00087s latency).

PORT      STATE SERVICE      VERSION
445/tcp   open  netbios-ssn  Samba smb2 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 08:00:27:46:C1:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

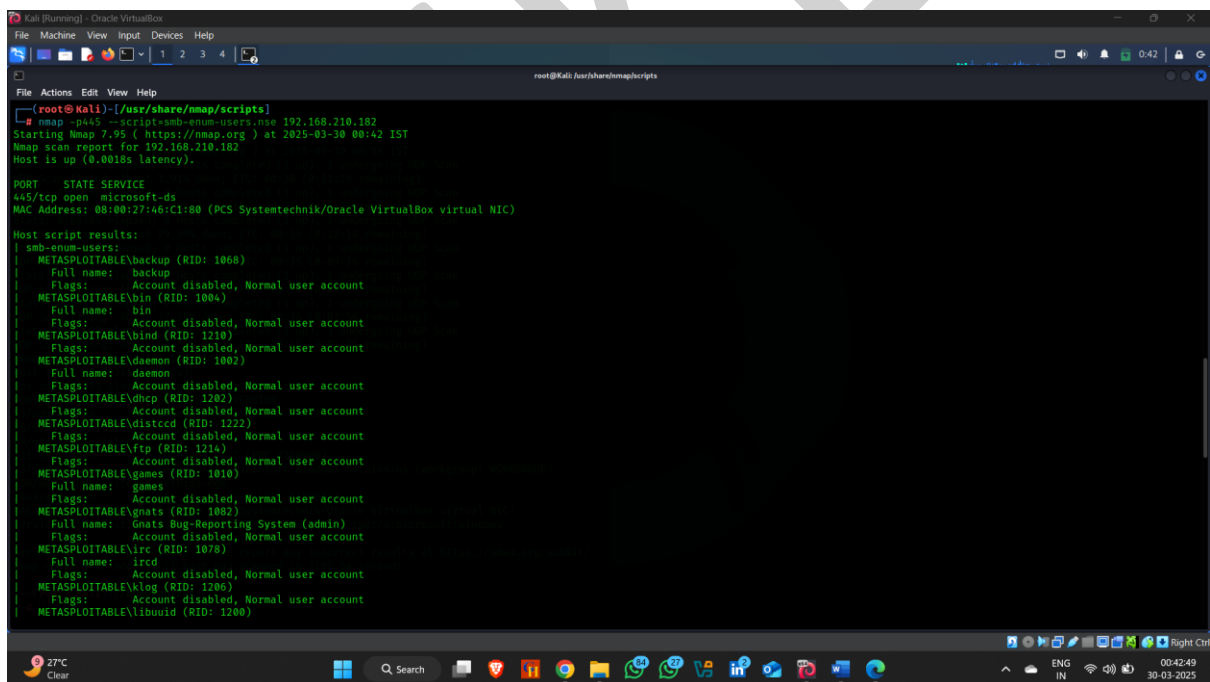
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 6.44 seconds

(root@kali)-[/home/aniket]
```

- Step 3 : Go to nmap scripts Directory using command  
**cd /usr/share/nmap/scripts**
- Step 4 : search how many SMB scripts are available using  
**ls smb\***



- Step 5 : perform nmap script



# NFS Enumeration

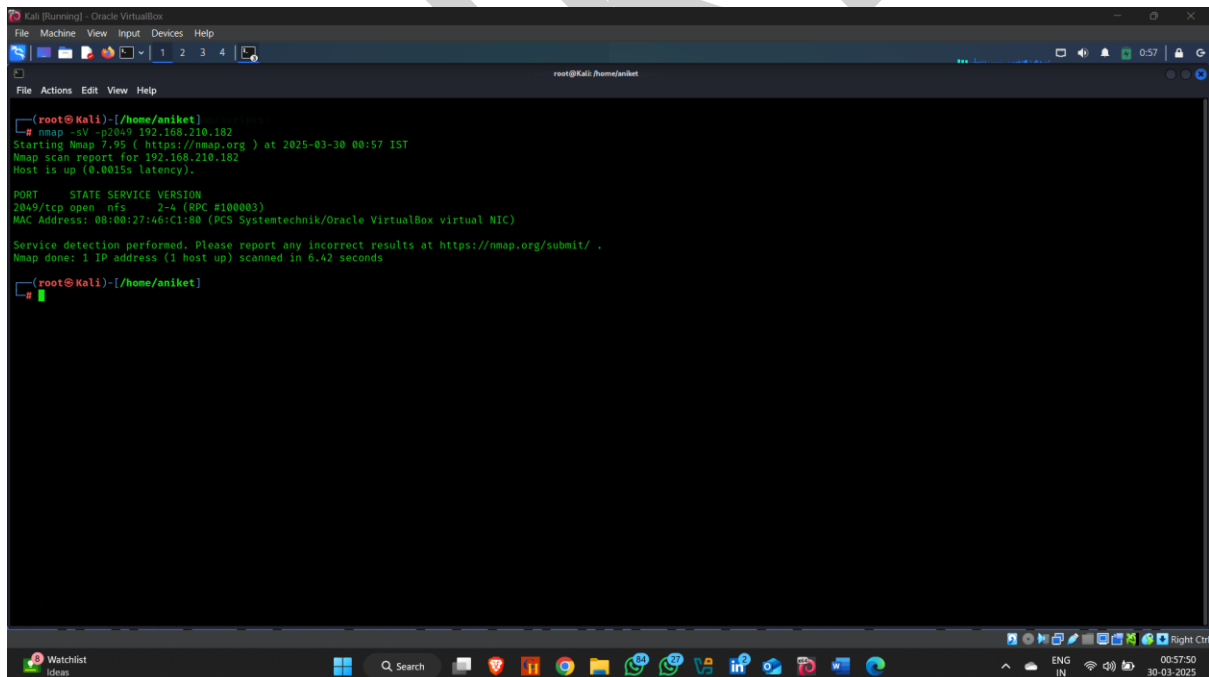
**NFS Enumeration** refers to the process of gathering information about **Network File System (NFS)** services running on a target system. NFS is a protocol that allows remote file sharing across networks, primarily used in Unix and Linux environments.

NFS Operates on **UDP port 2049**

## NFS Enumeration Using NSE

**How to use it –**

- Step 1 : Open kali linux / Parrot Os
- Step 2 : first scan the target to check open port



```
(root@Kali)-[/home/aniket]
# nmap -iP -o2049 192.168.210.182
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-30 00:57 IST
Nmap scan report for 192.168.210.182
Host is up (0.0015s latency).

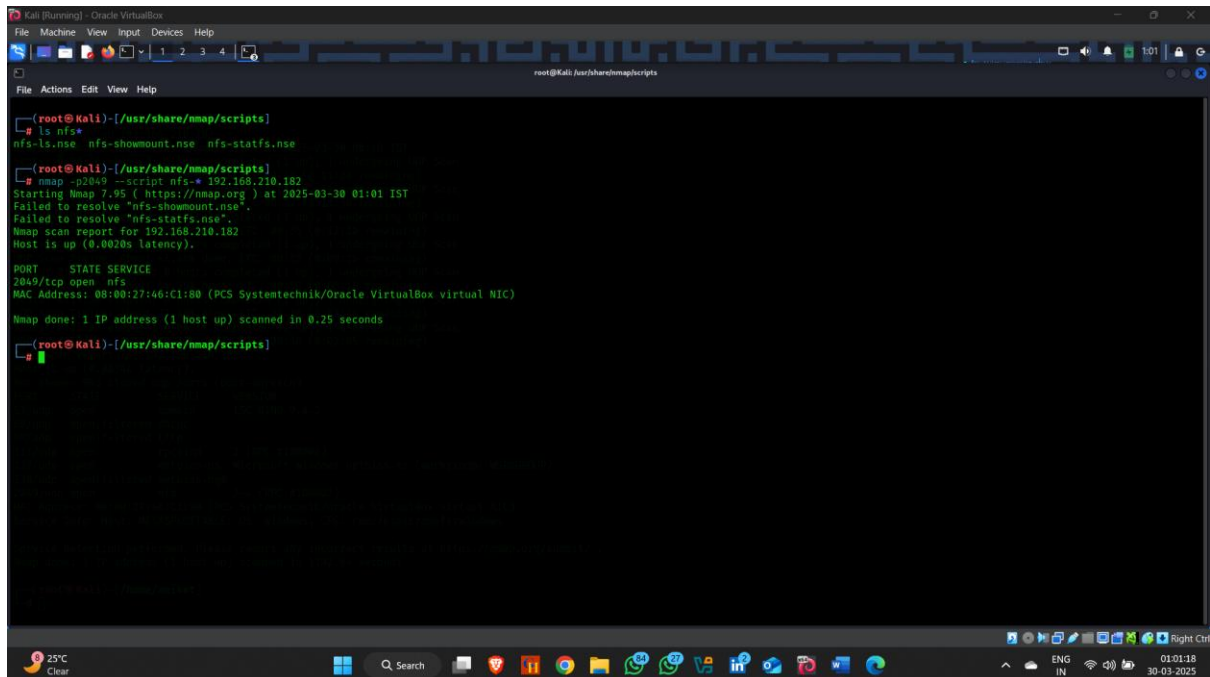
PORT      STATE SERVICE VERSION
2049/tcp  open  nfs      2-4 (RPC #100003)
MAC Address: 08:00:27:46:C1:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.42 seconds

(root@Kali)-[/home/aniket]
```

- Step 3 : Go to nmap scripts Directory using command  
**cd /usr/share/nmap/scripts**

- Step 4 : search how many NFS scripts are available using **ls nfs\***



The screenshot shows a Kali Linux terminal window with the following content:

```
(root@Kali)-[/usr/share/nmap/scripts]
# ls nfs*
nfs-ls.nse  nfs-showmount.nse  nfs-statfs.nse

(root@Kali)-[/usr/share/nmap/scripts]
# nmap -p2049 --script nfs-* 192.168.210.182
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-30 01:01 IST
Failed to resolve "nfs-showmount.nse".
Failed to resolve "nfs-statfs.nse".
Nmap scan report for 192.168.210.182
Host is up (0.0020s latency).

PORT      STATE SERVICE
2049/tcp  open  nfs
MAC Address: 08:00:27:46:C1:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds

(root@Kali)-[/usr/share/nmap/scripts]
```

The terminal window is titled "Kali (Running) - Oracle VM VirtualBox" and shows the standard Kali Linux desktop environment at the bottom with a taskbar and system tray.

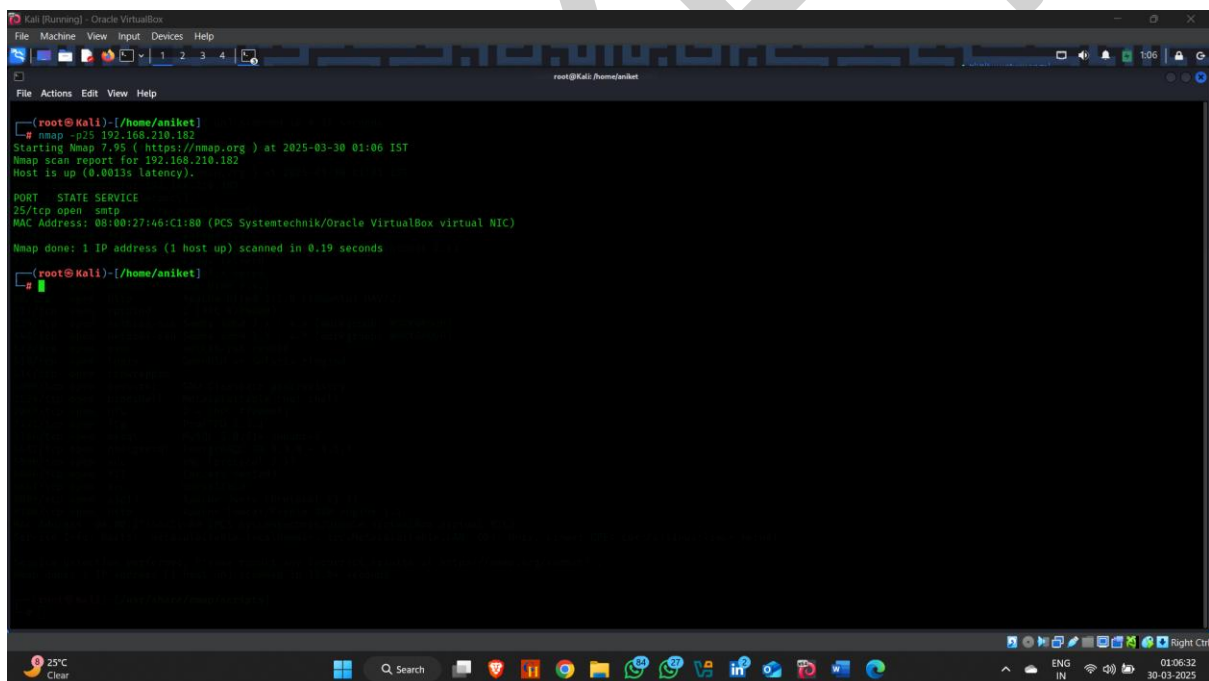
# SMTP Enumeration

**SMTP Enumeration** refers to the process of gathering information from an **SMTP (Simple Mail Transfer Protocol)** server, which is used for sending emails. Enumerating an SMTP server can help identify valid email addresses, user accounts, and server configurations.

SMTP operates on **TCP port 25**

**How to use it –**

- Step 1 : Open kali linux / Parrot Os
- Step 2 : first scan the target to check open port



```
(root@kali)-[/home/aniket]
# nmap -p25 192.168.210.182
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-30 01:06 IST
Nmap scan report for 192.168.210.182
Host is up (0.0013s latency).

PORT      STATE SERVICE
25/tcp    open  smtp
MAC Address: 08:00:27:46:C1:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
(root@kali)-[/home/aniket]
#
```

- Step 3 : Go to nmap scripts Directory using command  
**cd /usr/share/nmap/scripts**
- Step 4 : search how many SMTP scripts are available using  
**ls SMTP\***

```
Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@Kali: /usr/share/nmap/scripts

(root@Kali)-[/usr/share/nmap/scripts]
# ls smtp*
smtp-brute.nse      smtp-enum-users.nse  smtp-open-relay.nse  smtp-vuln-cve2010-4344.nse  smtp-vuln-cve2011-1764.nse
smtp-commands.nse  smtp-ntlm-info.nse  smtp-strangeport.nse  smtp-vuln-cve2011-1720.nse

(root@Kali)-[/usr/share/nmap/scripts]
# nmap -p25 --script=smtp-enum-users.nse 192.168.210.182
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-30 01:09 IST
Nmap scan report for 192.168.210.182
Host is up (0.0018s latency).

PORT      STATE SERVICE
25/tcp    open  smtp
| smtp-enum-users:
|_ Method RCPT returned a unhandled status code.
MAC Address: 08:00:27:46:C1:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds

(root@Kali)-[/usr/share/nmap/scripts]
```

25°C  
Clear



Search



Right Ctrl





# DNS Enumeration

DNS Enumeration is the process of gathering information about a **domain's DNS (Domain Name System) records** to uncover details about the infrastructure, subdomains, mail servers, and other network assets.

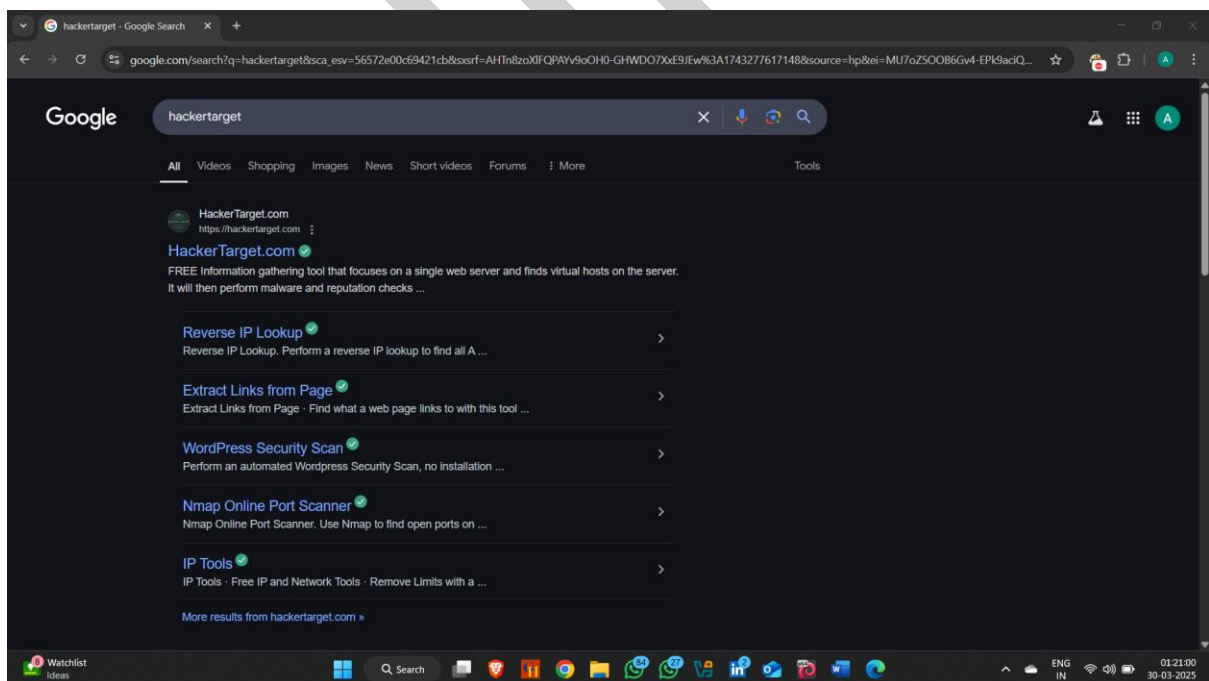
DNS Operates on **UDP Port 53**

## DNS Enumeration Using Hacker Target Website

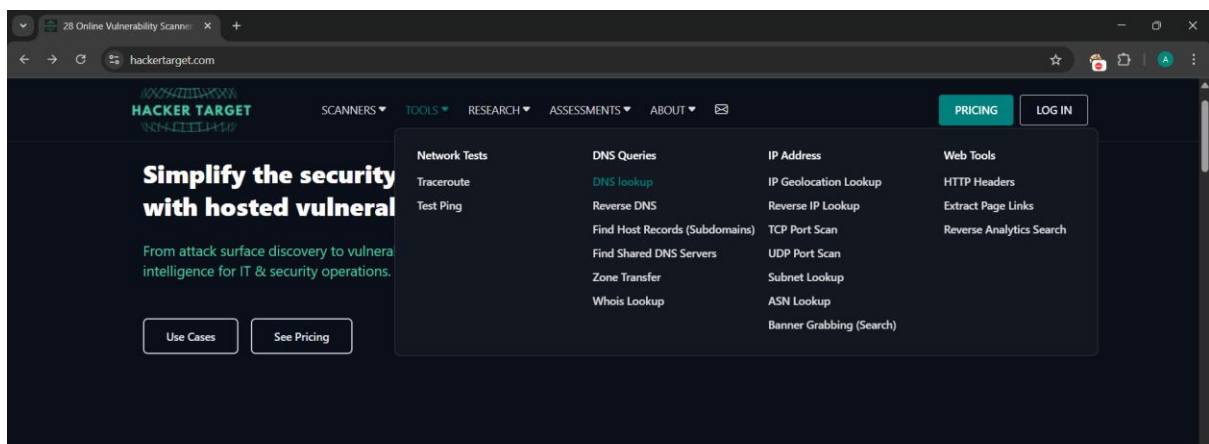
**How to use it –**

**Step 1 : open Browser and search hackertarget**

**Step 2 : click on first website**

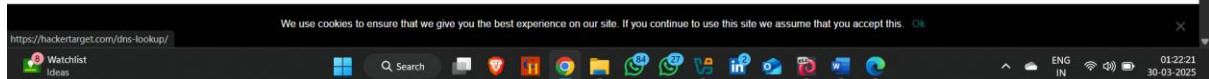


### Step 3 : click on Tools and then click on DNS lookup

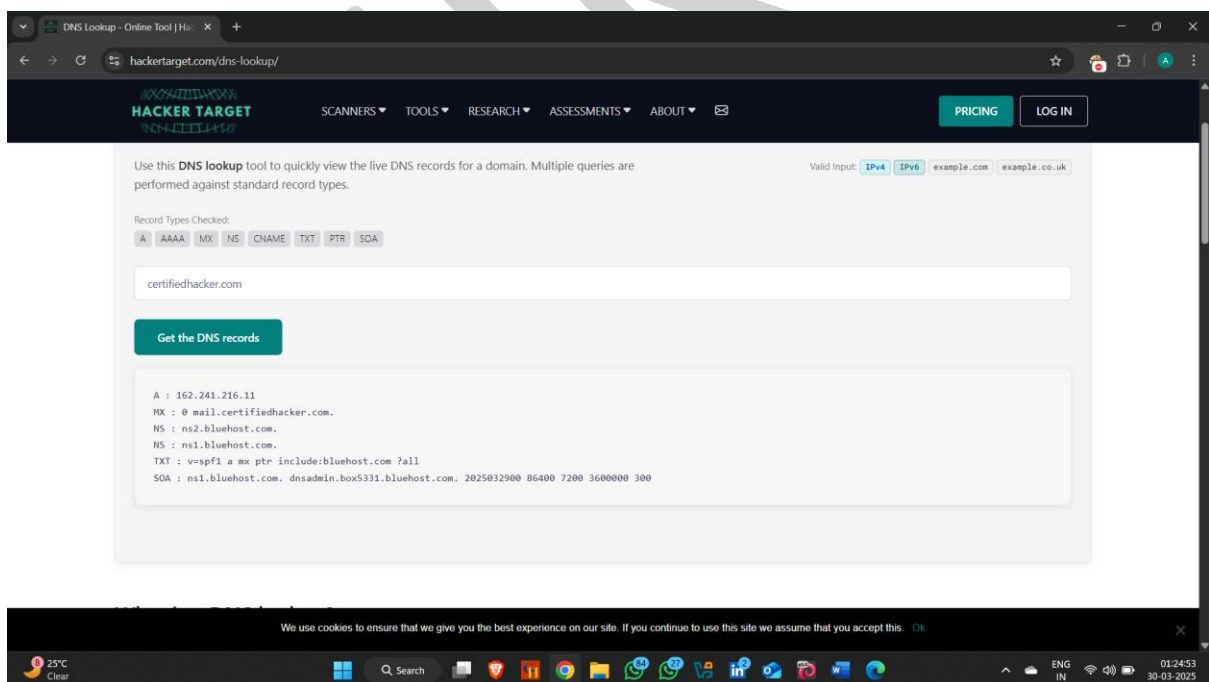


### Online Vulnerability Scanners

Proactively hunt for security weakness. Pivot from attack surface discovery to vulnerability identification.



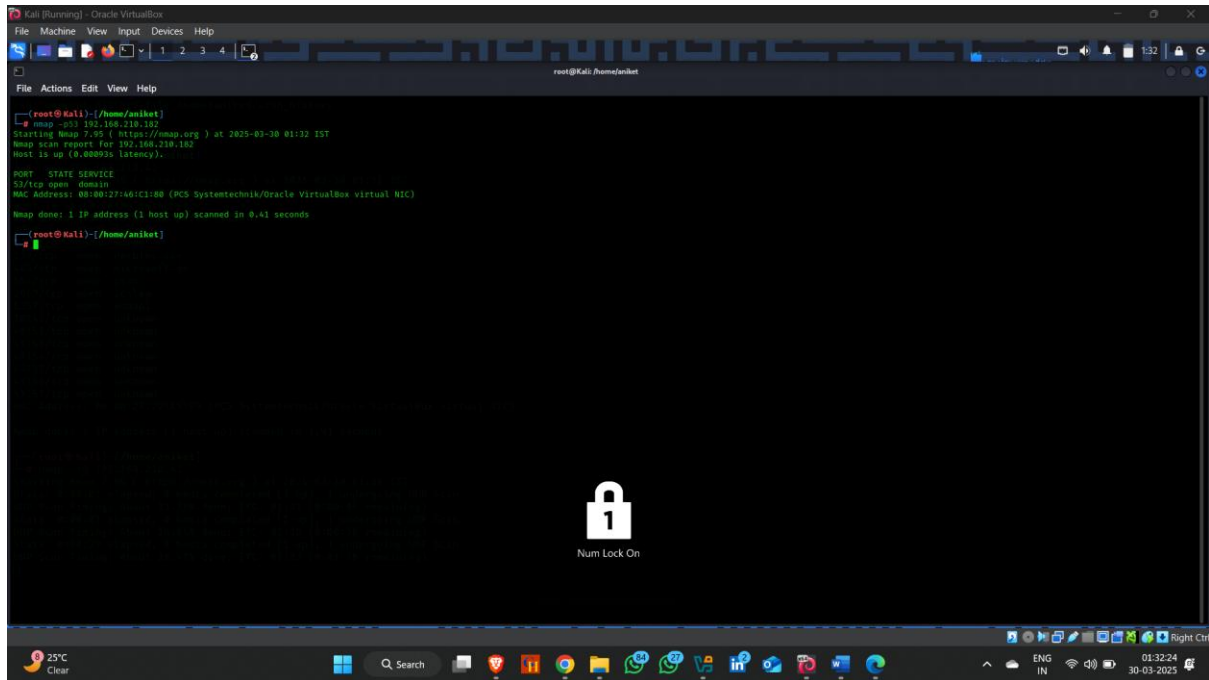
### Step 4 : provide a domain name and click on get the DNS record



# DNS Enumeration Using NSE

## How to use it –

- Step 1 : Open kali linux / Parrot Os
- Step 2 : first scan the target to check open port



```
(root@kali)~[/home/aniket]
# nmap -sS 192.168.218.182
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-30 01:32 IST
Nmap scan report for 192.168.218.182
Host is up (0.00000s latency).

PORT      STATE SERVICE
53/tcp    open  domain
Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
(root@kali)~[/home/aniket]
```

- Step 3 : Go to nmap scripts Directory using command  
**cd /usr/share/nmap/scripts**
- Step 4 : search how many DNS scripts are available using  
**ls DNS\***

```
Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@Kali: /usr/share/nmap/scripts

root@kali:~# ls dns
dns-blacklist.nse  dns-cache-nmap.nse  dns-client-subnet-scan.nse  dns-ip6-args-scan.nse  dns-nsec3-enum.nse  dns-random-srptest.nse  dns-recursion.nse  dns-srv-enum.nse  dns-ssuistracker.nse
dns-brute.nse      dns-check-zone.nse  dns-fuzz2.nse              dns-nsec-enum.nse    dns-ssid.nse       dns-random-txid.nse  dns-service-discovery.nse  dns-update.nse  dns-zone-transfer.nse

root@kali:~# ./usr/share/nmap/scripts
nmap -ps1 -script=dns-nsec3-enum.nse 192.168.210.182
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-30 01:41 IST
Nmap scan report for 192.168.210.182
Host is up (0.0021s latency).

PORT      STATE SERVICE
53/tcp    open  domain
|_ dns-nsec3-enum: Can't determine domain for host 192.168.210.182; use dns-nsec3-enum.domains script arg.
MAC Address: 08:00:27:46:C3:80 (PCS Systemtechnik/Oracle VM VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds

root@kali:~# ./usr/share/nmap/scripts
```