

## Module-4

### Enumeration

What is enumeration

Enumeration is the process of systematically probing a target for information, and it remains an essential tool in the hacker's arsenal

### Task1 How to Enumeration protocols

#### 1 Net Bios Enumeration:

NetBIOS enumeration is a technique used to gather information about networked systems using the NetBIOS protocol. It is commonly used by both system administrators for network auditing and attackers for reconnaissance.

NetBIOS (Network Basic Input/Output System) allows computers to communicate over a local network and provides services such as name resolution and resource sharing.

**Command:** Nmap -p 138,139 65.61.137.117 --script nbstat-\*

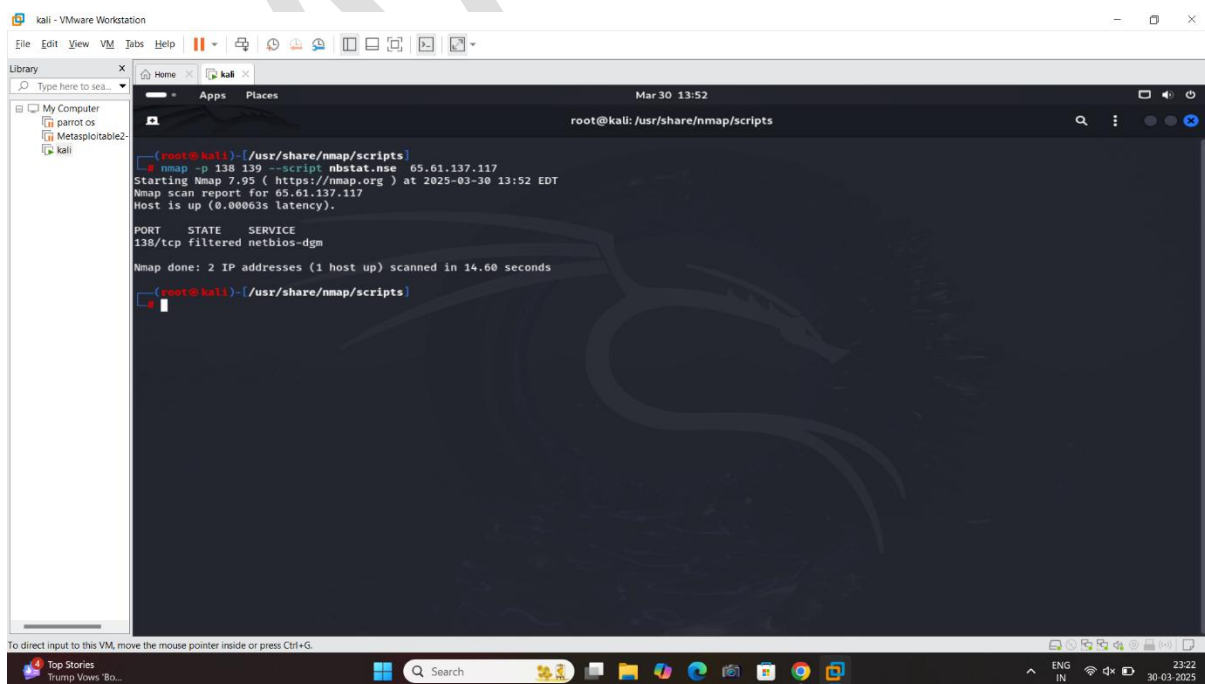
**Uses:** ☐ Identifies Active Hosts & Services – Helps discover computers and services on a network.

☐ **Extracts** NetBIOS Name Table – Reveals machine names, domain names, and workgroups.

☐ **Gathers Logged-in Users & Sessions** – Shows active connections between networked devices.

☐ **Detects Possible Security Risks** – Identifies misconfigured shares and open NetBIOS services.

**Result:**



```
(root@kali)-[/usr/share/nmap/scripts]
└─$ nmap -p 138 139 --script nbstat.nse 65.61.137.117
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-30 13:52 EDT
Nmap scan report for 65.61.137.117
Host is up (0.00063s latency).

PORT      STATE SERVICE
138/tcp    filtered netbios-dgm

Nmap done: 2 IP addresses (1 host up) scanned in 14.60 seconds
(root@kali)-[/usr/share/nmap/scripts]
```

## How to Enumeration protocol using window machine using nbstat

**Step1:** open the window cmd

## How to Enumeration Using LDAP Protocol

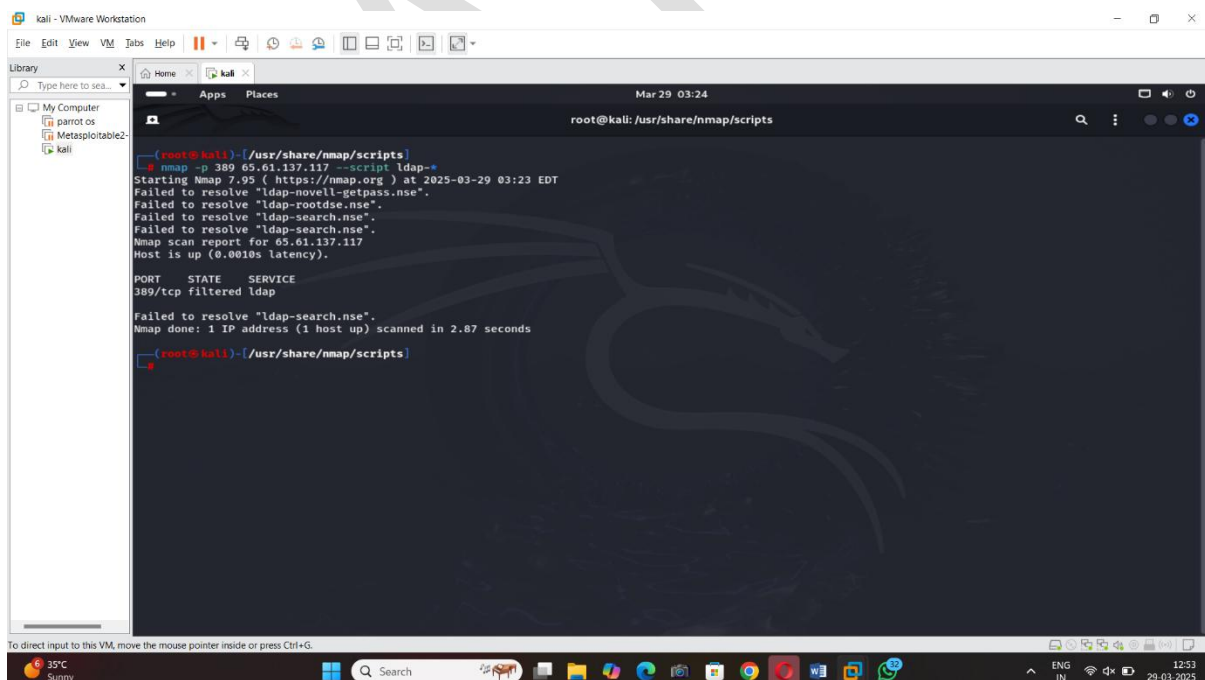
**2 LDAP: (Lightweight Directory Access Protocol)** is an application protocol used for accessing and managing **directory services** over a network. It is widely used for authentication, authorization, and directory lookups in enterprise environments.

**Uses:** • LDAP is commonly used in enterprise environments for **centralized authentication**.

❓ When a user logs into a system (e.g., corporate computer, VPN, web application), their username and password are validated against the LDAP directory.

**Command:** Nmap -p 389 65.61.137.117 --script ldap-\*

## Result



```
(root@kali) [/usr/share/nmap/scripts]
# nmap -p 389 65.61.137.117 --script ldap-*
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-29 03:23 EDT
Failed to resolve "ldap-novell-getpass.nse".
Failed to resolve "ldap-rootdse.nse".
Failed to resolve "ldap-search.nse".
Failed to resolve "ldap-search.nse".
Nmap scan report for 65.61.137.117
Host is up (0.0010s latency).

PORT      STATE SERVICE
389/tcp    filtered ldap
Failed to resolve "ldap-search.nse".
Nmap done: 1 IP address (1 host up) scanned in 2.87 seconds
(root@kali) [/usr/share/nmap/scripts]
```

## How to Enumeration Using NFS Protocol

3 NFS : (**Network File System**) is a protocol that allows a client to access shared directories and files over a network as if they were local. It is commonly used in Unix/Linux environments for sharing files across systems. However, if misconfigured, NFS can expose sensitive files and directories to unauthorized users

**Uses:** NFS enumeration helps in: ✓ Identifying shared directories (**exports**)

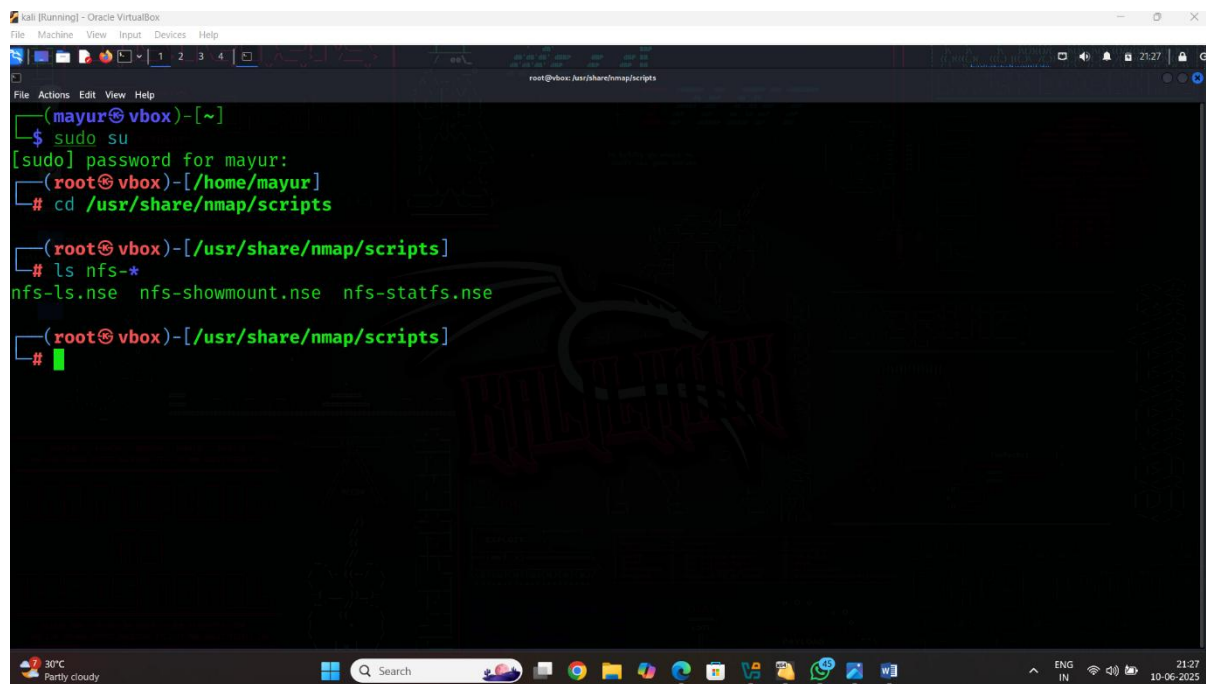
✓ Checking for misconfigured permissions (world-readable/writable)

✓ Finding potential data leakage or security vulnerabilities

✓ Assessing access controls and security settings

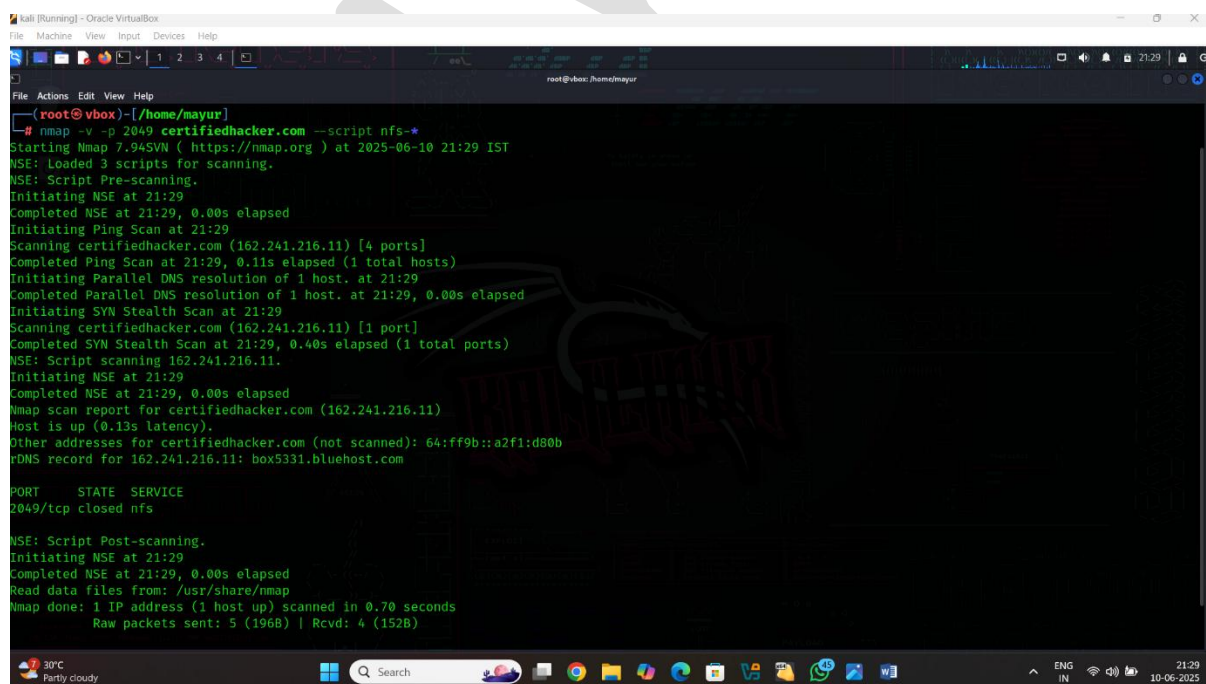
**Command:** Nmap -p 2049 65.61.137.117 --script nfs-\*

# Result:



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

(mayur@vbox)~$ sudo su
[sudo] password for mayur:
(root@vbox)~$ cd /usr/share/nmap/scripts
(root@vbox)~$ ls nfs-*
nfs-ls.nse  nfs-showmount.nse  nfs-statfs.nse
(root@vbox)~$
```



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

(root@vbox)~$ nmap -v -p 2049 certifiedhacker.com --script nfs-*
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-10 21:29 IST
NSE: Loaded 3 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 21:29
Completed NSE at 21:29, 0.00s elapsed
Initiating Ping Scan at 21:29
Scanning certifiedhacker.com (162.241.216.11) [4 ports]
Completed Ping Scan at 21:29, 0.11s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:29
Completed Parallel DNS resolution of 1 host. at 21:29, 0.00s elapsed
Initiating SYN Stealth Scan at 21:29
Scanning certifiedhacker.com (162.241.216.11) [1 port]
Completed SYN Stealth Scan at 21:29, 0.40s elapsed (1 total ports)
NSE: Script scanning 162.241.216.11.
Initiating NSE at 21:29
Completed NSE at 21:29, 0.00s elapsed
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.13s latency).
Other addresses for certifiedhacker.com (not scanned): 64:ff9b::a2f1:d80b
rDNS record for 162.241.216.11: box5331.bluehost.com

PORT      STATE SERVICE
2049/tcp  closed nfs

NSE: Script Post-scanning.
Initiating NSE at 21:29
Completed NSE at 21:29, 0.00s elapsed
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.70 seconds
Raw packets sent: 5 (196B) | Rcvd: 4 (152B)
```

# How to Enumeration Using DNS Protocol

## 4 DNS for (Domain Name System)

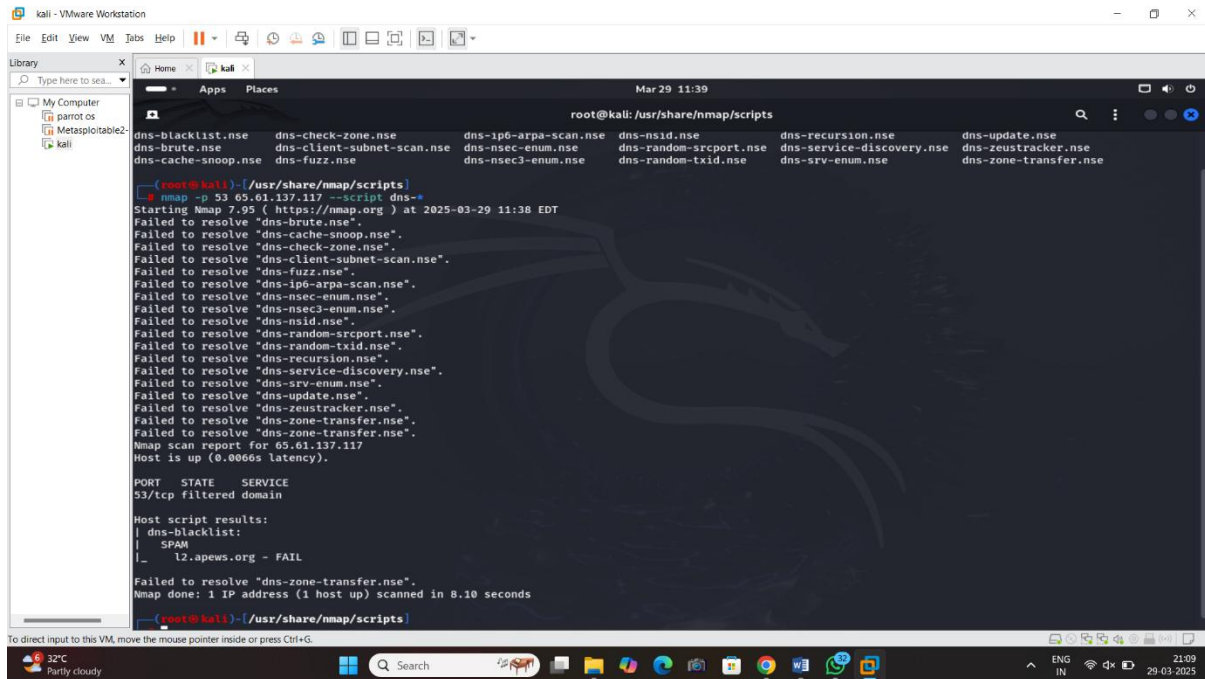
enumeration is the process of gathering information about a domain's DNS records to map out its network infrastructure. It is commonly used by cybersecurity professionals for penetration testing and by attackers for reconnaissance

Uses: • **Reconnaissance for Ethical Hacking:**

Security professionals use DNS enumeration to gather information about a target before performing penetration tests.

- **Identifying Attack Vectors:** Helps in detecting vulnerable subdomains, outdated services, and potential entry points.
- **Detecting Misconfigurations:** Finds improperly configured DNS records, such as open zone transfers, that could expose critical network details.

**Commands:** Nmap -p 53 65.61.137.117 -  
Script dns-\*



```
root@kali: /usr/share/nmap/scripts
dns-blacklist.nse dns-check-zone.nse dns-ip6-arpa-scan.nse dns-nsid.nse dns-recursion.nse dns-update.nse
dns-brute.nse dns-client-subnet-scan.nse dns-ip6-arpa-scan.nse dns-random-srcport.nse dns-service-discovery.nse dns-zeustracker.nse
dns-cache-snoop.nse dns-fuzz.nse dns-nsec3-enum.nse dns-random-txid.nse dns-srv-enum.nse dns-zone-transfer.nse

root@kali: /usr/share/nmap/scripts
nmap -p 53 65.61.137.117 --script dns-*
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-29 11:38 EDT
Failed to resolve "dns-brute.nse".
Failed to resolve "dns-cache-snoop.nse".
Failed to resolve "dns-check-zone.nse".
Failed to resolve "dns-client-subnet-scan.nse".
Failed to resolve "dns-fuzz.nse".
Failed to resolve "dns-ip6-arpa-scan.nse".
Failed to resolve "dns-nsec3-enum.nse".
Failed to resolve "dns-nsec3-enum.nse".
Failed to resolve "dns-nsid.nse".
Failed to resolve "dns-random-srcport.nse".
Failed to resolve "dns-random-txid.nse".
Failed to resolve "dns-recursion.nse".
Failed to resolve "dns-service-discovery.nse".
Failed to resolve "dns-srv-enum.nse".
Failed to resolve "dns-update.nse".
Failed to resolve "dns-zeustracker.nse".
Failed to resolve "dns-zone-transfer.nse".
Failed to resolve "dns-zone-transfer.nse".
Nmap scan report for 65.61.137.117
Host is up (0.0066s latency).

PORT      STATE SERVICE
53/tcp    filtered domain

Host script results:
| dns-blacklist:
|   SPAM
|_  l2.apews.org - FAIL

Failed to resolve "dns-zone-transfer.nse".
Nmap done: 1 IP address (1 host up) scanned in 8.10 seconds

root@kali: /usr/share/nmap/scripts
```

## How to Enumeration Using SMTP Protocol

**5 SMTP (Simple Mail Transfer Protocol)**  
enumeration is the process of gathering information about an SMTP server to identify valid email addresses, supported authentication mechanisms, and potential vulnerabilities. It is commonly used by penetration testers, ethical hackers, and sometimes attackers to map out email services.



Uses: ✓ **Identify Valid Email Addresses** – Helps in finding valid users for social engineering or brute-force attacks.

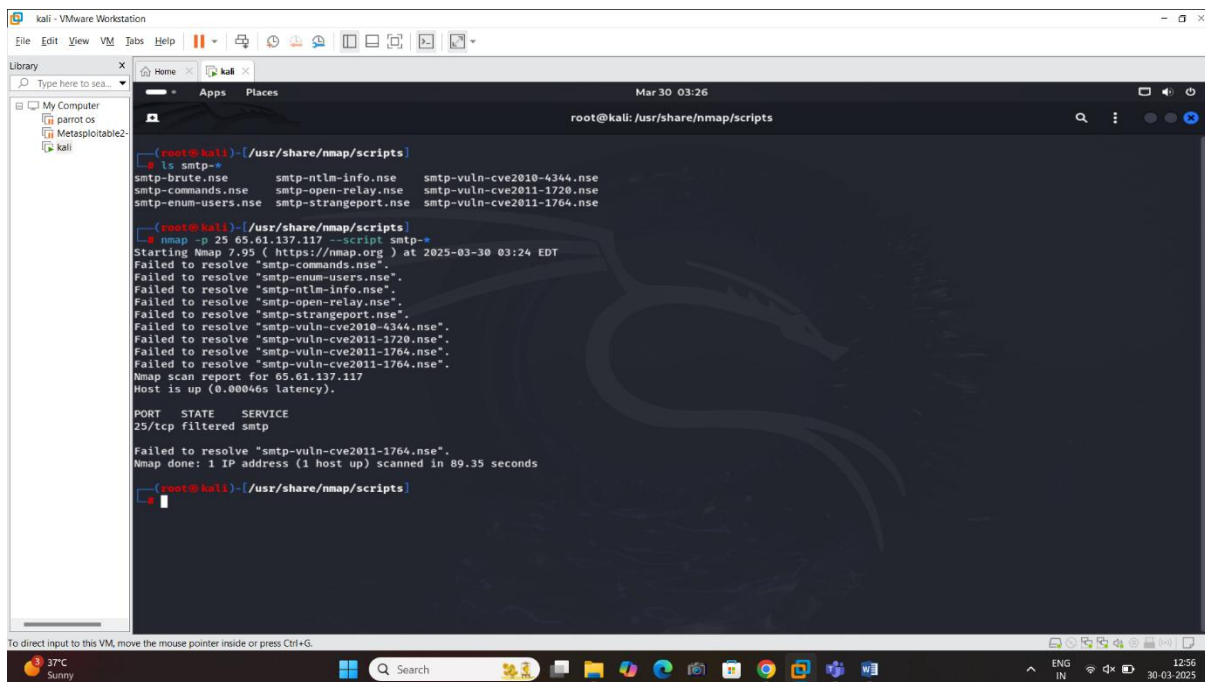
✓ **Check for Misconfigurations** – Identifies open relays and other security weaknesses.

✓ **Determine Supported Authentication Methods** – Helps in discovering authentication weaknesses.

✓ **Detect Email Spoofing Vulnerabilities** – Helps check whether the server allows email spoofing.

**Command:** `Nmap -p 25 65.61.137.117 -script smtp-*`

## Result:



```
(root@kali)~# ls smtp-  
smtp-brute.nse      smtp-ntlm-info.nse  smtp-vuln-cve2010-4344.nse  
smtp-commands.nse  smtp-open-relay.nse smtp-vuln-cve2011-1720.nse  
smtp-enum-users.nse smtp-strangeport.nse smtp-vuln-cve2011-1764.nse  
  
(root@kali)~# nmap -p 25 65.61.137.117 --script smtp-  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-30 03:24 EDT  
Failed to resolve "smtp-commands.nse".  
Failed to resolve "smtp-enum-users.nse".  
Failed to resolve "smtp-ntlm-info.nse".  
Failed to resolve "smtp-open-relay.nse".  
Failed to resolve "smtp-strangeport.nse".  
Failed to resolve "smtp-vuln-cve2010-4344.nse".  
Failed to resolve "smtp-vuln-cve2011-1720.nse".  
Failed to resolve "smtp-vuln-cve2011-1764.nse".  
Failed to resolve "smtp-vuln-cve2011-1764.nse".  
Nmap scan report for 65.61.137.117  
Host is up (0.00046s latency).  
  
PORT      STATE SERVICE  
25/tcp    filtered smtp  
  
Failed to resolve "smtp-vuln-cve2011-1764.nse".  
Nmap done: 1 IP address (1 host up) scanned in 89.35 seconds  
  
(root@kali)~#
```

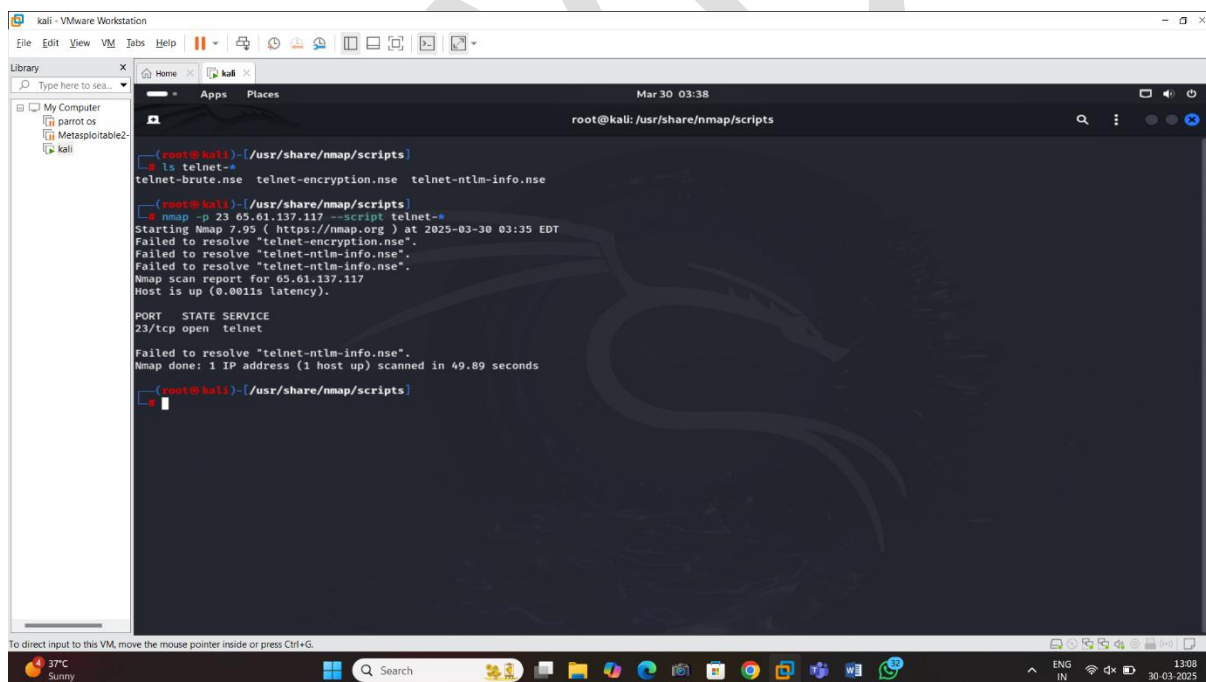
6 Telnet: Telnet (short for **Telecommunication Network**) is a network protocol used to provide a **command-line interface (CLI) for communication with remote devices** over a TCP/IP network. It allows users to log into another computer or network device remotely and execute commands as if they were physically present at the machine.

Uses:

- **Remote administration** of servers and networking devices.

- **Testing network services** like web servers, mail servers, and other TCP/IP services.
- **Debugging and troubleshooting** network issues.
- **Accessing legacy systems** that do not support modern secure protocols.

Command: `Nmap -p 23 65.61.137.117 --script telnet-*`



```
(root@kali)-[/usr/share/nmap/scripts]
└─$ ls telnet-*
telnet-brute.nse  telnet-encryption.nse  telnet-ntlm-info.nse

(root@kali)-[/usr/share/nmap/scripts]
└─$ nmap -p 23 65.61.137.117 --script telnet-*
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-30 03:35 EDT
Failed to resolve "telnet-encryption.nse".
Failed to resolve "telnet-ntlm-info.nse".
Failed to resolve "telnet-ntlm-info.nse".
Nmap scan report for 65.61.137.117
Host is up (0.0011s latency).

PORT      STATE SERVICE
23/tcp    open  telnet

Failed to resolve "telnet-ntlm-info.nse".
Nmap done: 1 IP address (1 host up) scanned in 49.89 seconds

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

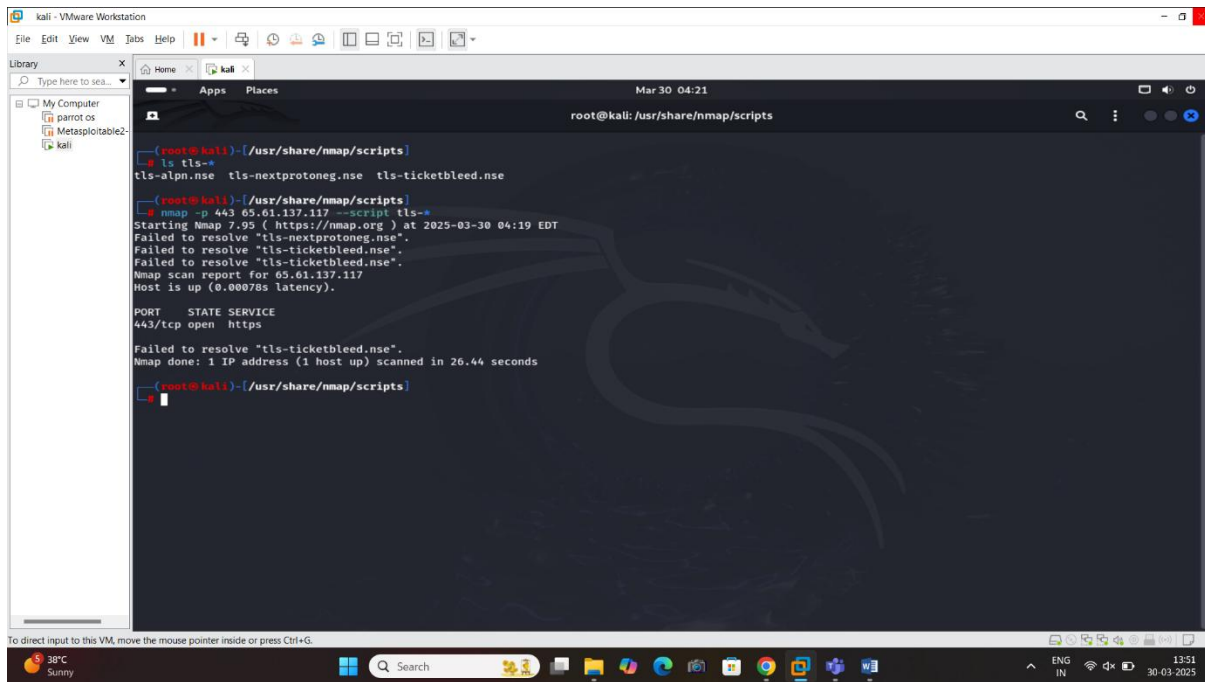
## 7 TLC (Transaction Logic and Concurrency)

Protocol isn't a widely recognized term, but it could refer to different things depending on the context. Can you clarify whether you're asking

Uses:

- **TLC Protocol in Networking** – Possibly referring to a transport layer protocol or a custom protocol for ensuring reliable communication.
- **TLC in Blockchain/Cryptography** – A protocol related to transactions in distributed ledger systems.
- **TLC in Automation/Testing** – A protocol used for model checking or software verification (like Temporal Logic of Computations).

**Command:** Nmap -p 443 65.61.137.117 tls-\*



## 8 SNMP (Simple Network Management Protocol)

enumeration is the process of gathering information from network devices using SNMP queries. SNMP is used for managing and monitoring network devices such as routers, switches, printers, and servers. It operates over UDP ports **161 (queries)** and **162 (traps/alerts)**.

**Uses:** SNMP enumeration involves extracting valuable data from a networked device using

- System details (OS, hostname, uptime)
- Network interfaces and IP addresses
- Running services and open ports
- User accounts and credentials
- Routing tables
- Installed software and processes

```
KaliLinux (Running) - Oracle VM VirtualBox
File Machine View Input Devices Help

Apps Places

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

root@mayur:~# cd /usr/share/nmap/scripts
root@mayur:~/usr/share/nmap/scripts# ls
ls: cannot access 'snmp': No such file or directory

root@mayur:~/usr/share/nmap/scripts# ls
snmp-brute.nse      snmp-info.nse      snmp-ios-config.nse  snmp-processes.nse  snmp-win32-services.nse  snmp-win32-software.nse
snmp-hh3c-logins.nse  snmp-interfaces.nse  snmp-netstat.nse     snmp-sysdescr.nse   snmp-win32-shares.nse    snmp-win32-users.nse

root@mayur:~/usr/share/nmap/scripts# ./snmp -i 162.241.216.11 --script snmp-brute
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-01 13:53 EDT
Failed to resolve "snmp-hh3c-logins.nse".
Failed to resolve "snmp-info.nse".
Failed to resolve "snmp-interfaces.nse".
Failed to resolve "snmp-ios-config.nse".
Failed to resolve "snmp-netstat.nse".
Failed to resolve "snmp-processes.nse".
Failed to resolve "snmp-sysdescr.nse".
Failed to resolve "snmp-win32-services.nse".
Failed to resolve "snmp-win32-shares.nse".
Failed to resolve "snmp-win32-software.nse".
Failed to resolve "snmp-win32-users.nse".
Failed to resolve "snmp-win32-users.nse".
Nmap scan report for box5331.bluehost.com (162.241.216.11)
Host is up (0.0016s latency).

PORT      STATE SERVICE
161/tcp   open  snmp

Failed to resolve "snmp-win32-users.nse".
Nmap done: 1 IP address (1 host up) scanned in 7.38 seconds

root@mayur:~/usr/share/nmap/scripts#
```

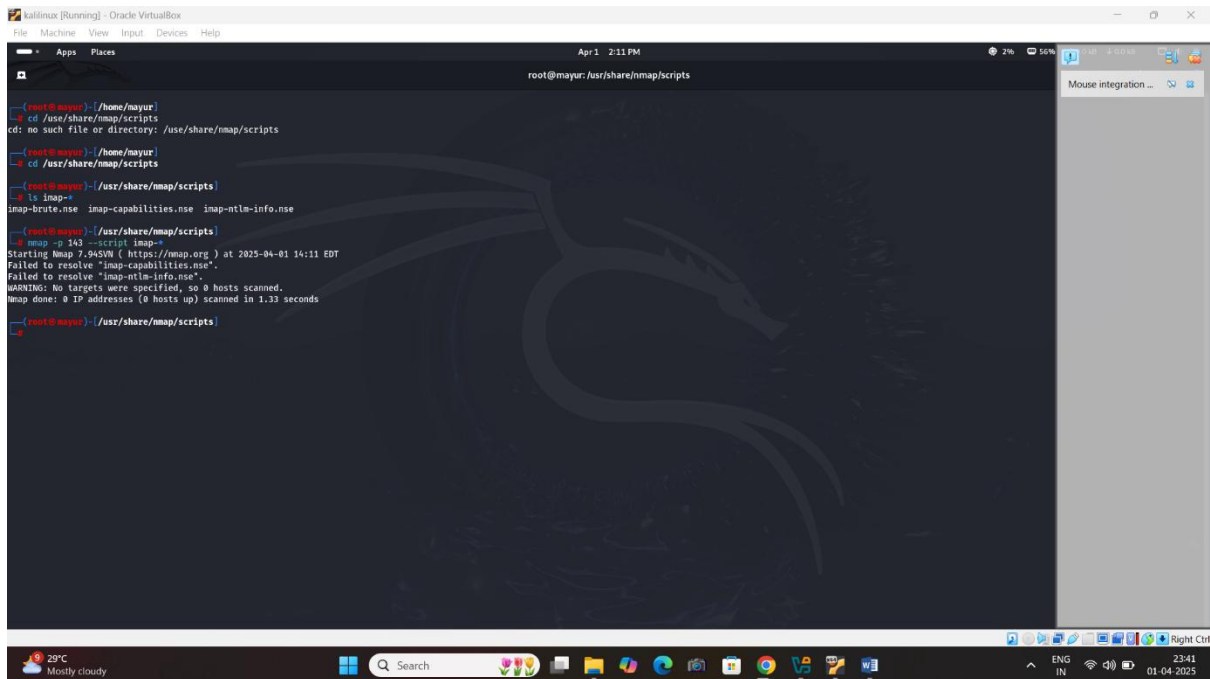
## **IMAP (internet Message Access protocol)**

enumeration involves gathering user credentials, mailbox information, and capabilities of the email server. Attackers and penetration testers use enumeration techniques to identify valid users, exploit weak authentication mechanisms, and potentially gain unauthorized access.

Uses: • **Disable verbose authentication error messages** to prevent user enumeration.

- **Enforce strong authentication** (e.g., IMAP over TLS, multi-factor authentication).
- **Limit login attempts** to prevent brute force attacks.
- **Use secure authentication mechanisms** (avoid AUTH=PLAIN, prefer OAuth or strong password policies).
- **Monitor and log IMAP access** to detect unusual login attempts

Command: Nmap -p 143 161 65.61.137.117 --script imap-\*

A screenshot of a Kali Linux terminal window running inside an Oracle VM VirtualBox. The terminal shows a user navigating to the directory /usr/share/nmap/scripts and running the command nmap -p 143 --script imap-\*. The output indicates that Nmap 7.94SNV is starting at 2025-04-01 14:11 EDT, but it fails to resolve the script names and reports that no targets were specified, scanning 0 hosts in 1.33 seconds. The terminal window has a dark background with a dragon logo. The host's taskbar at the bottom shows the date as 01-04-2025 and time as 23:41.

```
kali:linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Apr 1 2:11 PM
root@mayur: /usr/share/nmap/scripts

root@mayur: /home/mayur
- cd /usr/share/nmap/scripts
cd: no such file or directory: /usr/share/nmap/scripts

root@mayur: /home/mayur
- cd /usr/share/nmap/scripts

root@mayur: /usr/share/nmap/scripts
- ls imap-*
imap-brute.nse  imap-capabilities.nse  imap-ntlm-info.nse

root@mayur: /usr/share/nmap/scripts
- nmap -p 143 --script imap-*
Starting Nmap 7.94SNV ( https://nmap.org ) at 2025-04-01 14:11 EDT
Failed to resolve "imap-capabilities.nse".
Failed to resolve "imap-ntlm-info.nse".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 1.33 seconds

root@mayur: /usr/share/nmap/scripts
```

**Internet Relay Chat (IRC)** is a text-based communication protocol that supports real-time messaging, mainly used for group discussions and private messaging. Enumeration in the context of

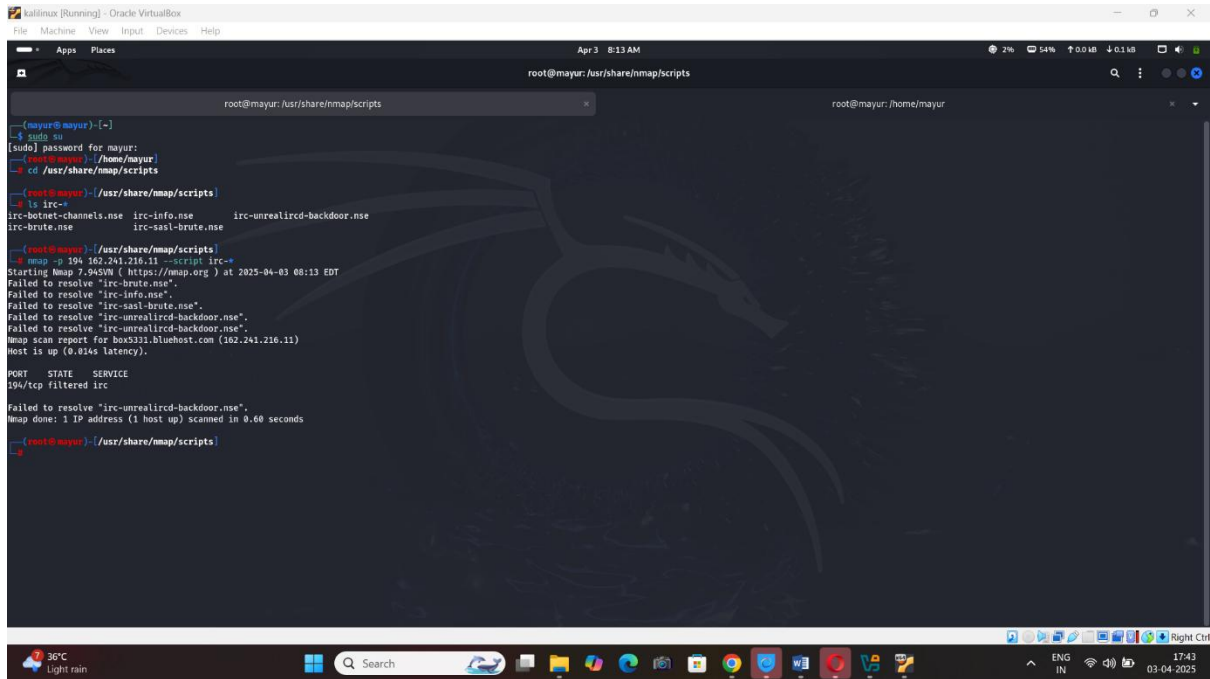


IRC typically involves identifying available servers, channels, users, and service

**Command:** Nmap -p 194 65.61.137.117 -script itc-\*

**Explanation:**

- Many IRC servers use **Cloaking** to hide user IPs.
- Some servers require authentication via **NickServ**.
- Some servers enforce **anti-enumeration measures** to prevent abuse.



```
root@mayur:/usr/share/nmap/scripts
[mayur@mayur]~$ sudo su
[sudo] password for mayur:
root@mayur:~# cd /usr/share/nmap/scripts
root@mayur:~/usr/share/nmap/scripts# ls irc-
irc-botnet-channels.nse  irc-info.nse  irc-unrealircd-backdoor.nse
irc-brute.nse           irc-sasl-brute.nse
root@mayur:~/usr/share/nmap/scripts# nmap -p 194.102.241.216 -sC --script irc-
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-03 08:13 EDT
Failed to resolve "irc-brute.nse".
Failed to resolve "irc-info.nse".
Failed to resolve "irc-sasl-brute.nse".
Failed to resolve "irc-unrealircd-backdoor.nse".
Failed to resolve "irc-unrealircd-backdoor.nse".
Nmap scan report for box3331.bluehost.com (192.241.216.11)
Host is up (0.014s latency).
PORT      STATE SERVICE
194/tcp    filtered irc
Failed to resolve "irc-unrealircd-backdoor.nse".
Nmap done: 1 IP address (1 host up) scanned in 0.60 seconds
root@mayur:~/usr/share/nmap/scripts#
```

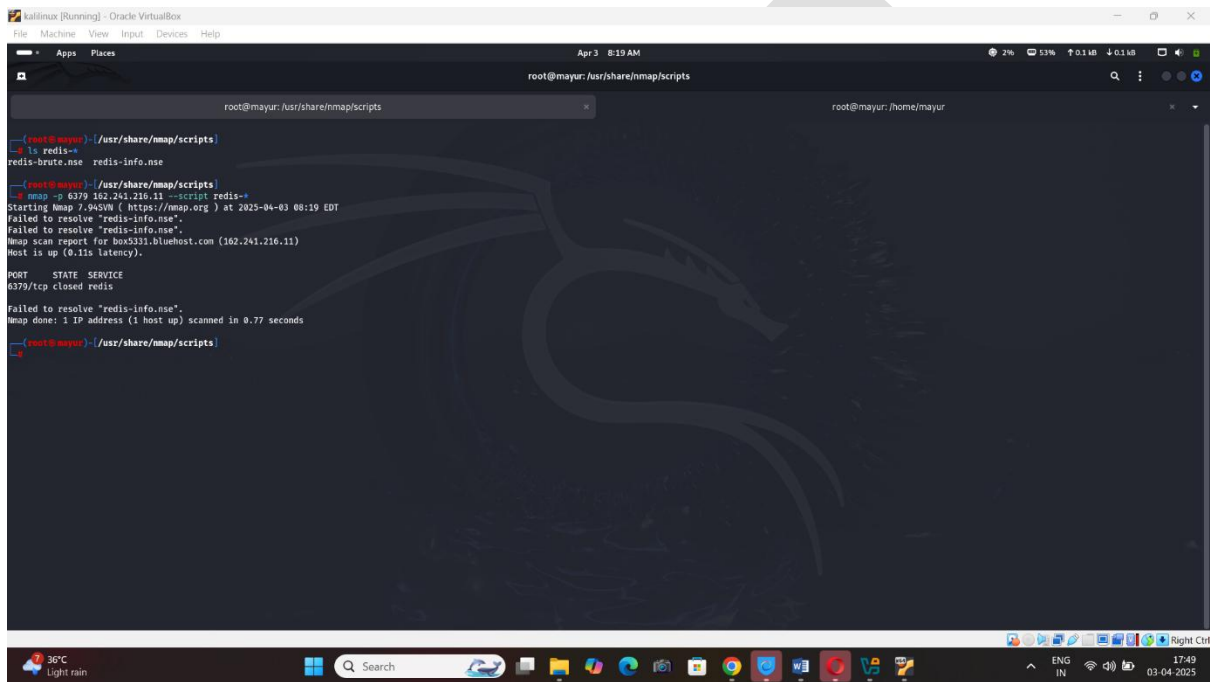
## Redis Protocol (RESP - Redis Serialization Protocol)

Redis uses the **Redis Serialization Protocol (RESP)** for communication between clients and the Redis server. RESP is a simple, efficient, and human-readable protocol that supports multiple data types like strings, lists, hashes, sets, and more.

**Command :** Nmap -p 6379 65.61.137.117 --script redis-\*

**Explanation:**

Redis enumeration involves discovering Redis instances, identifying misconfigurations, and extracting useful information like keys, users, and configurations. Attackers use enumeration to gain access, but it's also a crucial step in security audits.



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

Apr 3 8:19 AM
root@mayur: /usr/share/nmap/scripts

root@mayur: /usr/share/nmap/scripts
root@mayur: /home/mayur

root@mayur: /usr/share/nmap/scripts
ls redis-
redis-brute.nse redis-info.nse

root@mayur: /usr/share/nmap/scripts
nmap -p 6379 162.241.216.11 --script redis-
Starting Nmap 7.94.0 ( https://nmap.org ) at 2023-04-03 08:19 EDT
Failed to resolve "redis-info.nse".
Failed to resolve "redis-info.nse".
Nmap scan report for box5331.bluehost.com (162.241.216.11)
Host is up (0.11s latency).

PORT      STATE SERVICE
6379/tcp  closed redis

Failed to resolve "redis-info.nse".
Nmap done: 1 IP address (1 host up) scanned in 0.77 seconds

root@mayur: /usr/share/nmap/scripts
```

## PPTP Protocol

Point-to-Point Tunneling Protocol (PPTP) is an older VPN protocol used for secure communication. PPTP enumeration involves identifying vulnerable PPTP services, extracting authentication mechanisms, and testing for weak credentials.

Command: `Nmap -p 1723 65.61.137.117 --script pptp-*`

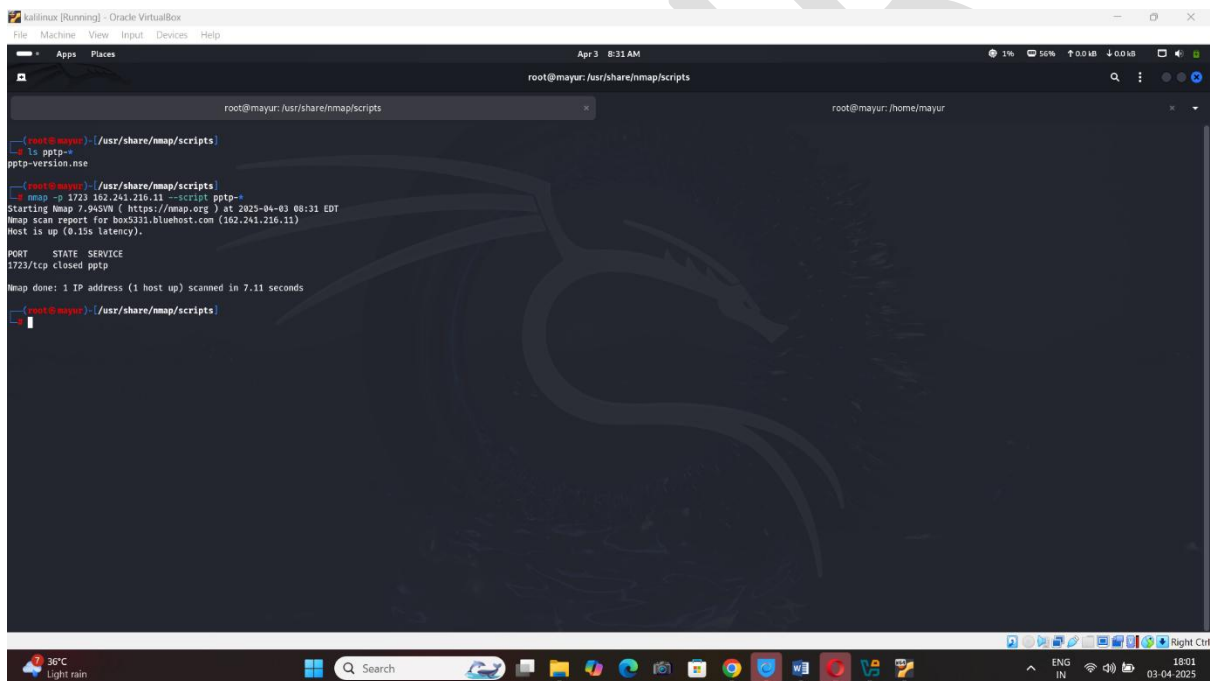
explanation

: PPTP creates a **tunnel** between a client and a VPN server, allowing the client to securely access a private network over the internet.

## Key Components of PPTP

- **Control Channel:** Uses **TCP port 1723** to establish and maintain the connection.

- **Data Transmission:** Uses **GRE (Generic Routing Encapsulation, Protocol 47)** to encapsulate packets.
- **Encryption:** Uses **MPPE (Microsoft Point-to-Point Encryption)**, which is vulnerable to attacks.

A screenshot of a Kali Linux terminal window. The terminal shows a netmap scan being performed on the IP address 162.241.216.11. The output indicates that the host is up and that port 1723/tcp is closed. The terminal window is titled 'root@mayur: /usr/share/netmap/scripts' and shows the command 'netmap -p 1723 162.241.216.11 -script netmap-nse' being executed. The terminal output includes the following text: 'Starting Netmap 7.9450N ( https://netmap.org ) at 2025-04-03 08:31 EDT', 'Netmap scan report for box5331.bluehost.com (162.241.216.11)', 'Host is up (0.13s latency).', and a table showing the scan results for port 1723/tcp. The table has columns for PORT, STATE, and SERVICE, and shows that port 1723/tcp is closed and the service is netmap. The terminal also shows the command 'netmap done: 1 IP address (1 host up) scanned in 7.11 seconds'.

## How to Enumeration Using RDP Protocol

**RDP (Remote Desktop Protocol)** is a **proprietary protocol developed by Microsoft** that allows a user to remotely connect and control another computer over a network.

Think of it like a virtual keyboard, mouse, and screen being sent over the internet, so you can

operate a computer that may be in another city or country — as if you were sitting in front of it.

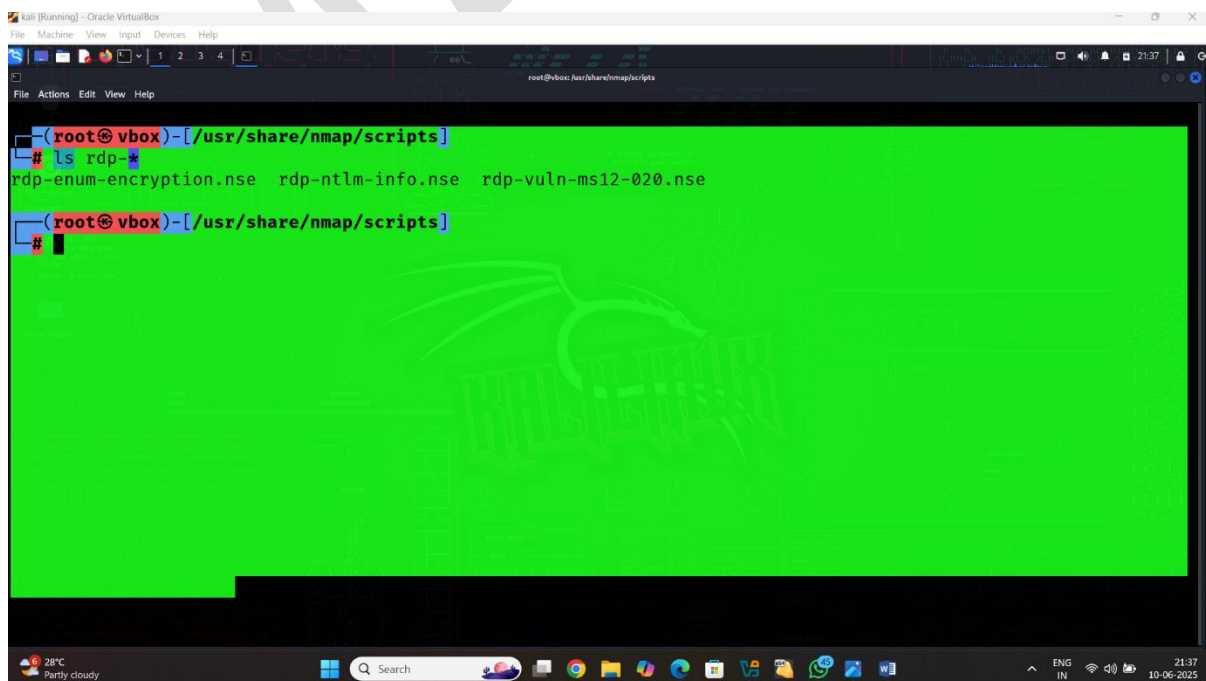
---

## ◆ Key Use Cases

- **Remote administration** of servers and desktops.
- **Remote support** for troubleshooting user issues.
- **Work from home** scenarios.
- **Virtual desktops** in enterprise environments.

Step1 open the kali linux terminal

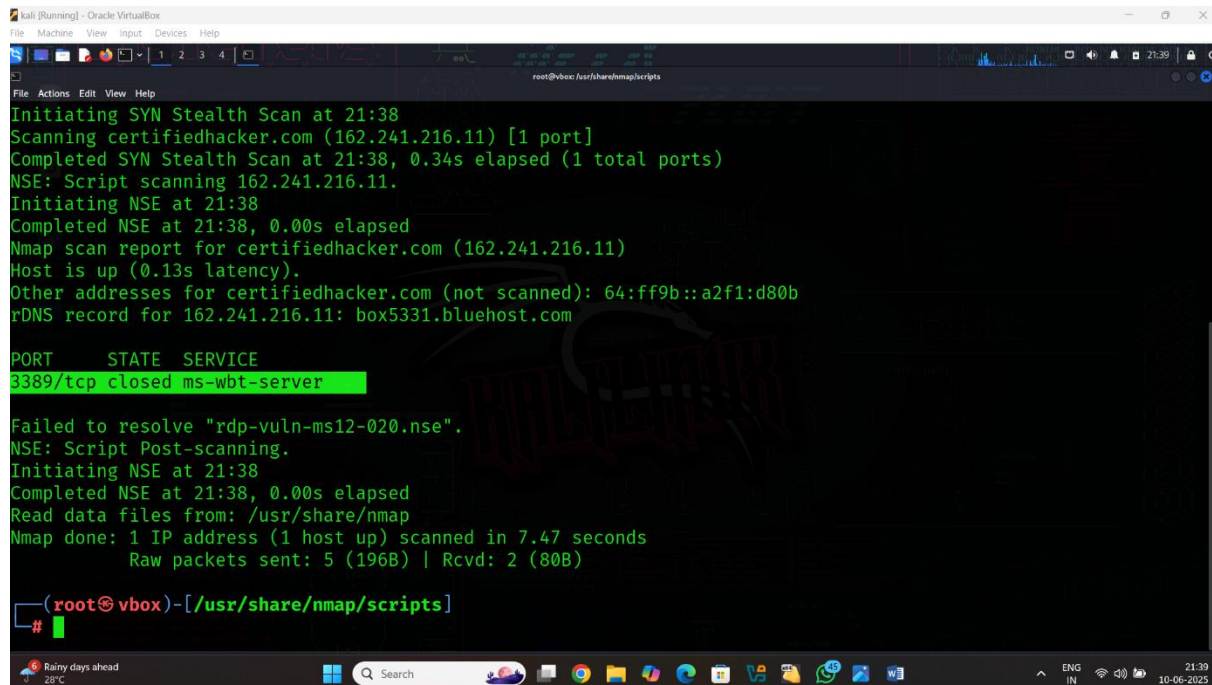
Command: `nmap -v -p 3389 --script certifiedhacker.com rdp-*`



The screenshot shows a Kali Linux terminal window with a green background. The prompt is `(root@vbox)-[/usr/share/nmap/scripts]`. The user has entered the command `ls rdp-*`, and the output lists several Nmap scripts: `rdp-enum-encryption.nse`, `rdp-ntlm-info.nse`, and `rdp-vuln-ms12-020.nse`. The terminal window is titled "kali [Running] - Oracle VM VirtualBox" and has a menu bar with "File", "Machine", "View", "Input", "Devices", and "Help". The bottom of the window shows a Windows taskbar with a search bar, task icons, and system tray information including "28°C Partly cloudy", "ENG IN", and "21:37 10-06-2025".

```
(root@vbox)-[/usr/share/nmap/scripts]
# ls rdp-*
rdp-enum-encryption.nse  rdp-ntlm-info.nse  rdp-vuln-ms12-020.nse
(root@vbox)-[/usr/share/nmap/scripts]
#
```

## Result:



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

Initiating SYN Stealth Scan at 21:38
Scanning certifiedhacker.com (162.241.216.11) [1 port]
Completed SYN Stealth Scan at 21:38, 0.34s elapsed (1 total ports)
NSE: Script scanning 162.241.216.11.
Initiating NSE at 21:38
Completed NSE at 21:38, 0.00s elapsed
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.13s latency).
Other addresses for certifiedhacker.com (not scanned): 64:ff9b::a2f1:d80b
rDNS record for 162.241.216.11: box5331.bluehost.com

PORT      STATE SERVICE
3389/tcp  closed ms-wbt-server

Failed to resolve "rdp-vuln-ms12-020.nse".
NSE: Script Post-scanning.
Initiating NSE at 21:38
Completed NSE at 21:38, 0.00s elapsed
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 7.47 seconds
Raw packets sent: 5 (196B) | Rcvd: 2 (80B)

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

## How to Enumeration Using POP3 Protocol

**POP3 (Post Office Protocol version 3)** is a standard internet protocol used by email clients to retrieve emails from a mail server.

It allows you to **download emails** from a server to your local device and read them **offline**.

---

## ◆ How It Works – Step-by-Step

### 1. **Email Client Connects:**

Your email app (like Outlook, Thunderbird, or Apple Mail) connects to your mail server using POP3.

### 2. **Authentication:**

You log in with your **email address and password**.

### 3. **Email Download:**

- The server sends the **emails** to your client.

**Emails are usually deleted from the server** after download (unless configured otherwise).

### ● **Offline Access:**

You can now **read emails locally** even without an internet connection.

Step1: open the kali linux terminal

Command: `nmap -v -p 110 certifiedhacker.com --script pop3-*`



# Result:

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

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

(mayur@vbox)-[~]
$ sudo su
[sudo] password for mayur:
(root@vbox)-[/home/mayur]
# cd /usr/share/nmap/scripts

(root@vbox)-[/usr/share/nmap/scripts]
# nmap -v -p 110 certifiedhacker.com --script pop3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-10 22:09 IST
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:09
Completed NSE at 22:09, 0.00s elapsed
Failed to resolve "pop3-capabilities.nse".
Failed to resolve "pop3-ntlm-info.nse".
Initiating Ping Scan at 22:09
Scanning certifiedhacker.com (162.241.216.11) [4 ports]
Completed Ping Scan at 22:09, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:09
Completed Parallel DNS resolution of 1 host. at 22:09, 0.07s elapsed
Failed to resolve "pop3-ntlm-info.nse".
Initiating SYN Stealth Scan at 22:09
Scanning certifiedhacker.com (162.241.216.11) [1 port]
Completed SYN Stealth Scan at 22:09, 0.38s elapsed (1 total ports)
NSE: Script scanning 162.241.216.11.
Initiating NSE at 22:09
Completed NSE at 22:09, 0.00s elapsed
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.035s latency).
Other addresses for certifiedhacker.com (not scanned): 64:ff9b::a2f1:d80b
rDNS record for 162.241.216.11: box5331.bluehost.com

PORT      STATE SERVICE
110/tcp    filtered pop3
```

```
Failed to resolve "pop3-ntlm-info.nse".
Initiating SYN Stealth Scan at 22:09
Scanning certifiedhacker.com (162.241.216.11) [1 port]
Completed SYN Stealth Scan at 22:09, 0.38s elapsed (1 total ports)
NSE: Script scanning 162.241.216.11.
Initiating NSE at 22:09
Completed NSE at 22:09, 0.00s elapsed
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.035s latency).
Other addresses for certifiedhacker.com (not scanned): 64:ff9b::a2f1:d80b
rDNS record for 162.241.216.11: box5331.bluehost.com

PORT      STATE SERVICE
110/tcp    filtered pop3

Failed to resolve "pop3-ntlm-info.nse".
NSE: Script Post-scanning.
Initiating NSE at 22:09
Completed NSE at 22:09, 0.00s elapsed
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.97 seconds
Raw packets sent: 6 (240B) | Rcvd: 3 (112B)

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