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 Blos 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-*

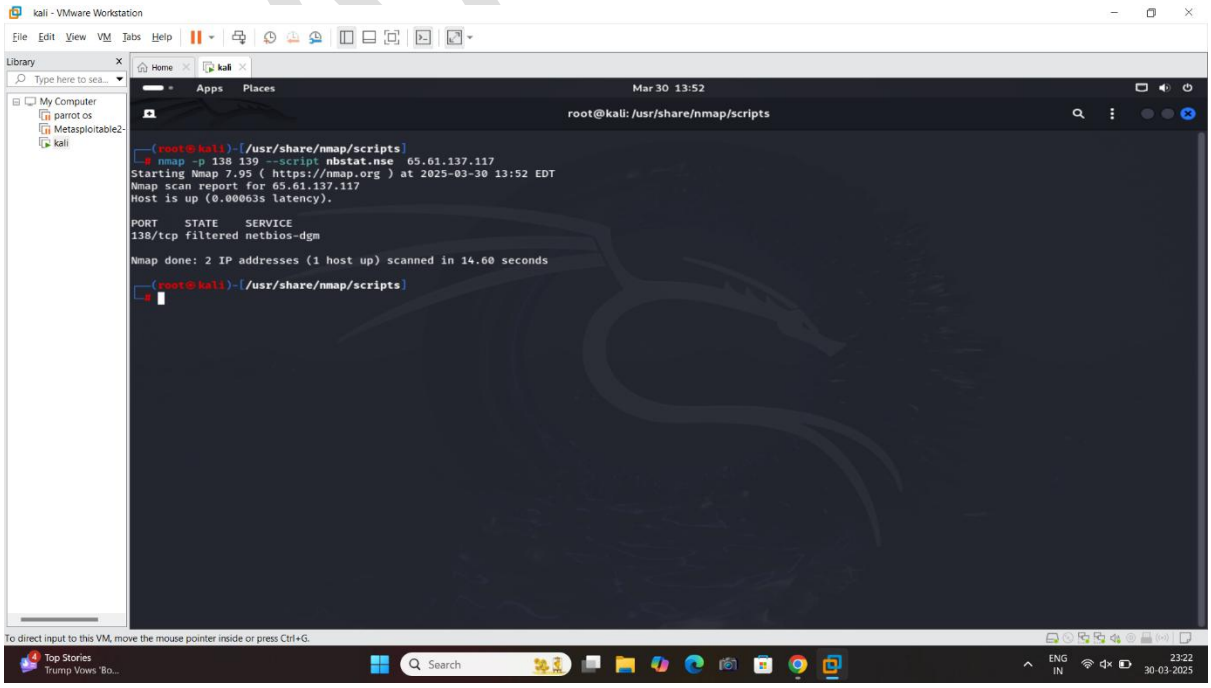
Uses: Identifies Active Hosts & Services – Helps discover computers and services on a network.

 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:



How to Enumeration protocol using window machine using nbstat

Step1: open the window cmd

How to Enumeration Using LDAP Protocol

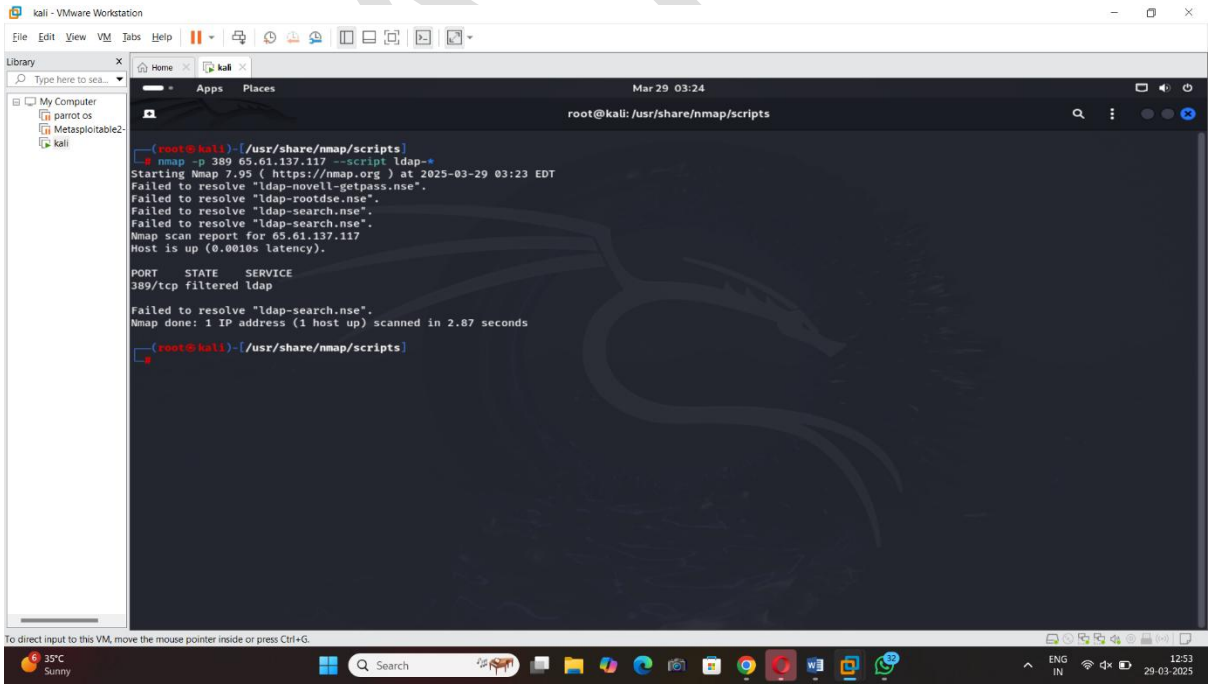
2 **LDAP: (Lightweight Directory Access Protocol**) is an application protocol used for accessing and managing **directory services** over a network. It is widely used for authentication, authorization, and directory lookups in enterprise environments.

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



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**)

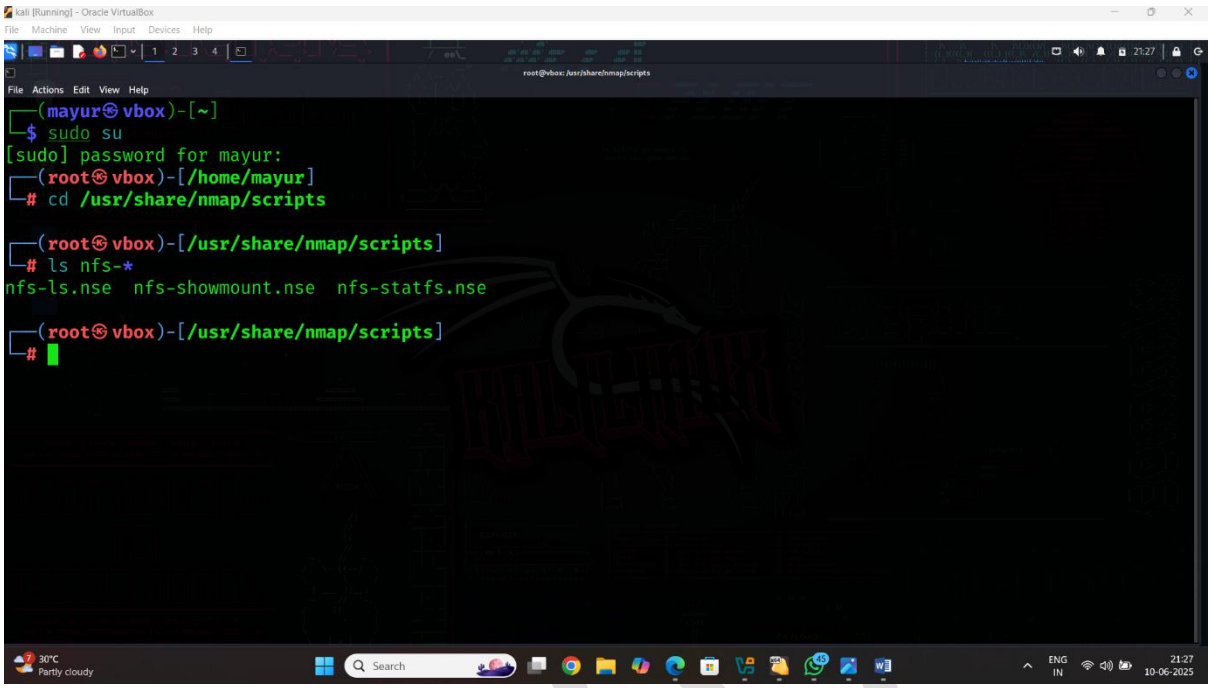
✓ Checking for misconfigured permissions (world-readable/writable)

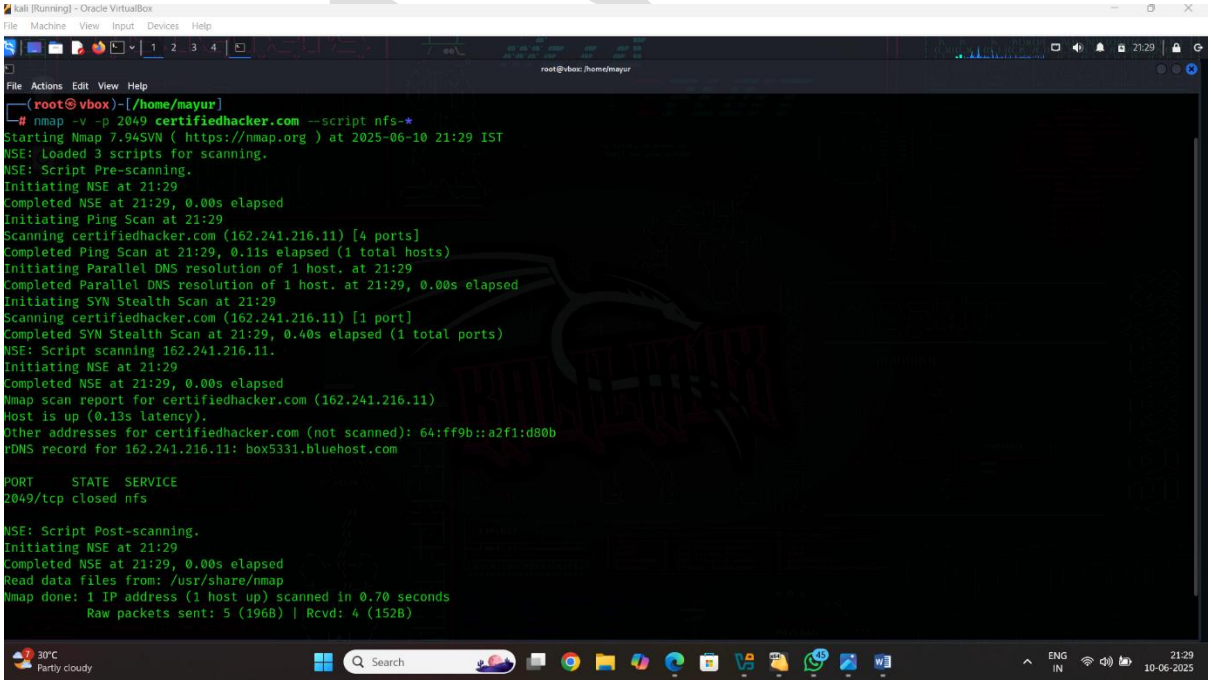
✓ Finding potential data leakage or security vulnerabilities

✓ 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
File Actions Edit View Help
(mayur㉿vbox)-[~]
$ sudo su
[sudo] password for mayur:
(root㉿vbox)-[/home/mayur]
cd /usr/share/nmap/scripts
(root㉿vbox)-[/usr/share/nmap/scripts]
ls nfs-*
nfs-ls.nse nfs-showmount.nse nfs-statfs.nse
(root㉿vbox)-[/usr/share/nmap/scripts]
#
30°C
Partly cloudy
Search
ENG
IN
21:27
10-06-2025


kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@vbox: /home/mayur
File Actions Edit View Help
(root㉿vbox)-[/home/mayur]
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)
30°C
Partly cloudy
Search
ENG
IN
21:29
10-06-2025

How to Enumeration Using DNS Protocol

4 DNS for (Domain Name System)

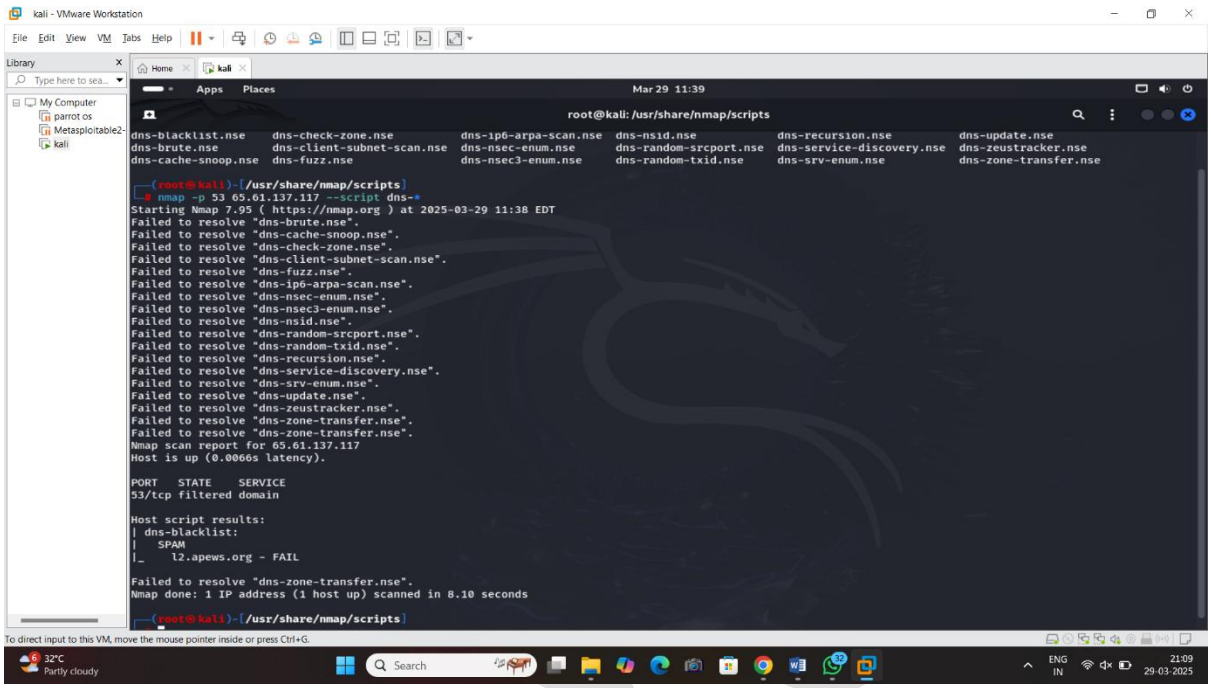
enumeration is the process of gathering information about a domain's DNS records to map out its network infrastructure. It is commonly used by cybersecurity professionals for penetration testing and by attackers for reconnaissance

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-*



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.

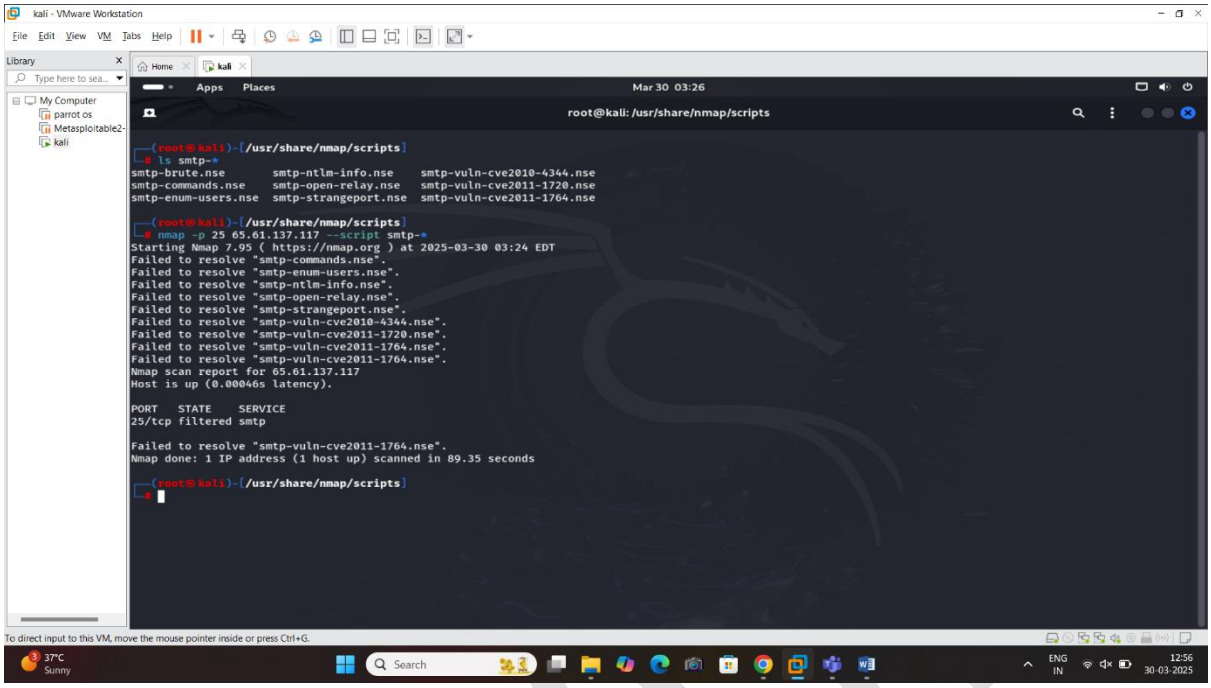
✅ **Check for Misconfigurations** – Identifies open relays and other security weaknesses.

✅ **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:



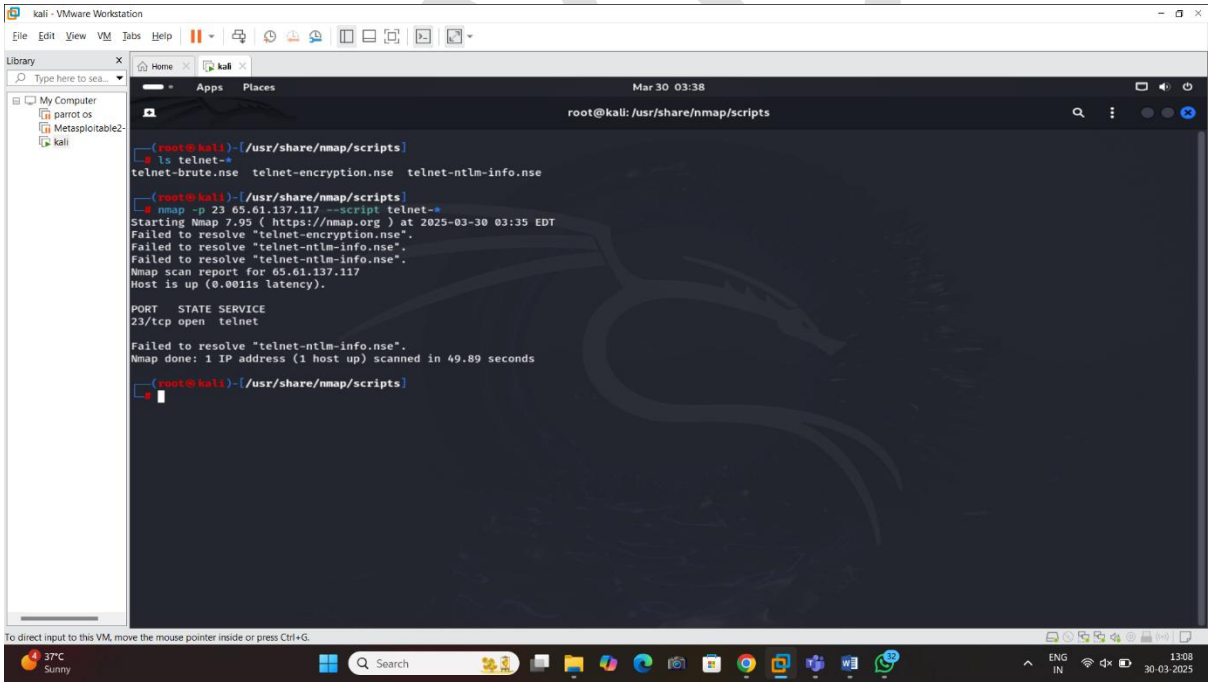
6 Telnet: Telnet (short for **Telecommunication Network**) is a network protocol used to provide a **command-line interface (CLI) for communication with remote devices** over a TCP/IP network. It allows users to log into another computer or network device remotely and execute commands as if they were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

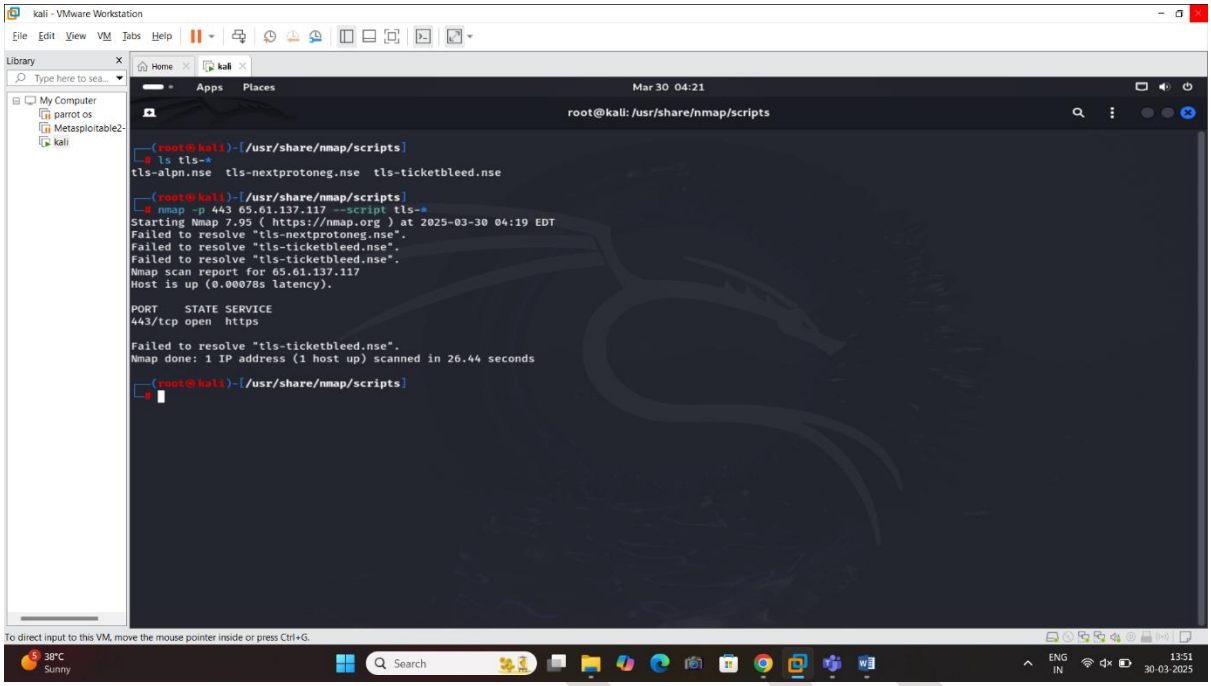


7 **TLC (Transaction Logic and Concurrency**)
Protocol isn't a widely recognized term, but it could refer to different things depending on the context. Can you clarify whether you're asking

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-*



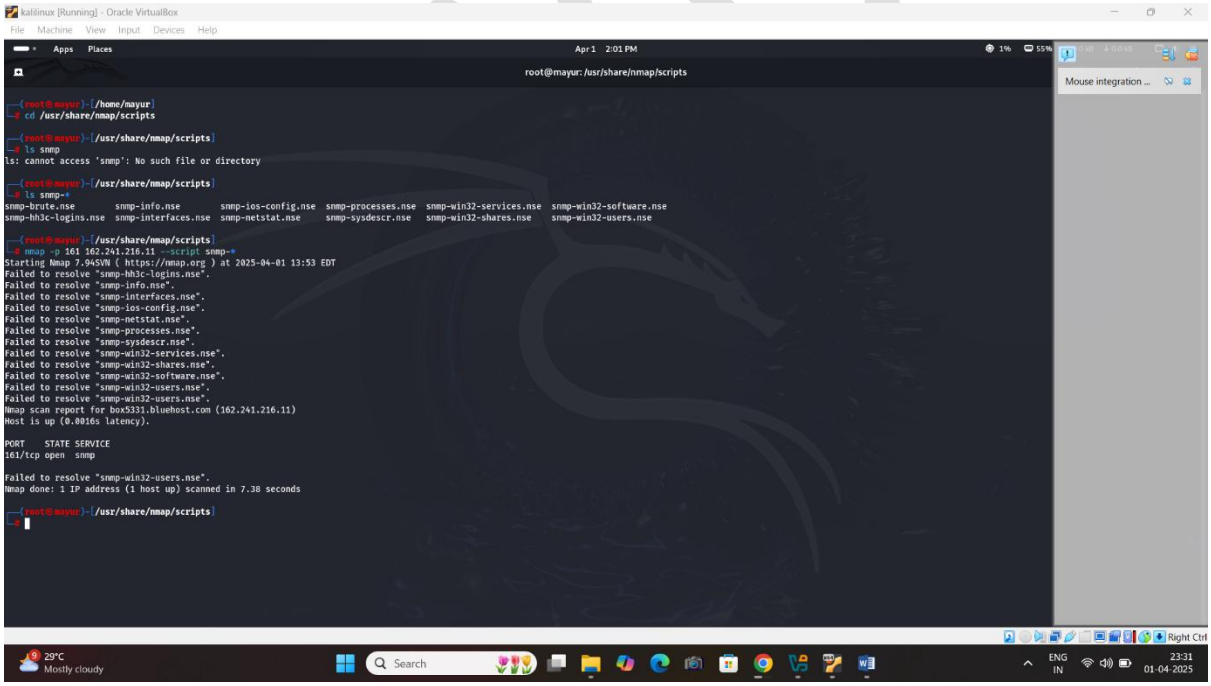
8 **SNMP (Simple Network Management Protocol)** enumeration is the process of gathering information from network devices using SNMP queries. SNMP is used for managing and monitoring network devices such as routers, switches, printers, and servers. It operates over UDP ports **161 (queries) and 162 (traps/alerts).**

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

SNMP. Attackers and penetration testers leverage SNMP enumeration to gather:

- 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

Command:nmap –p 161 65.61.137.117 –script snmp-*



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.

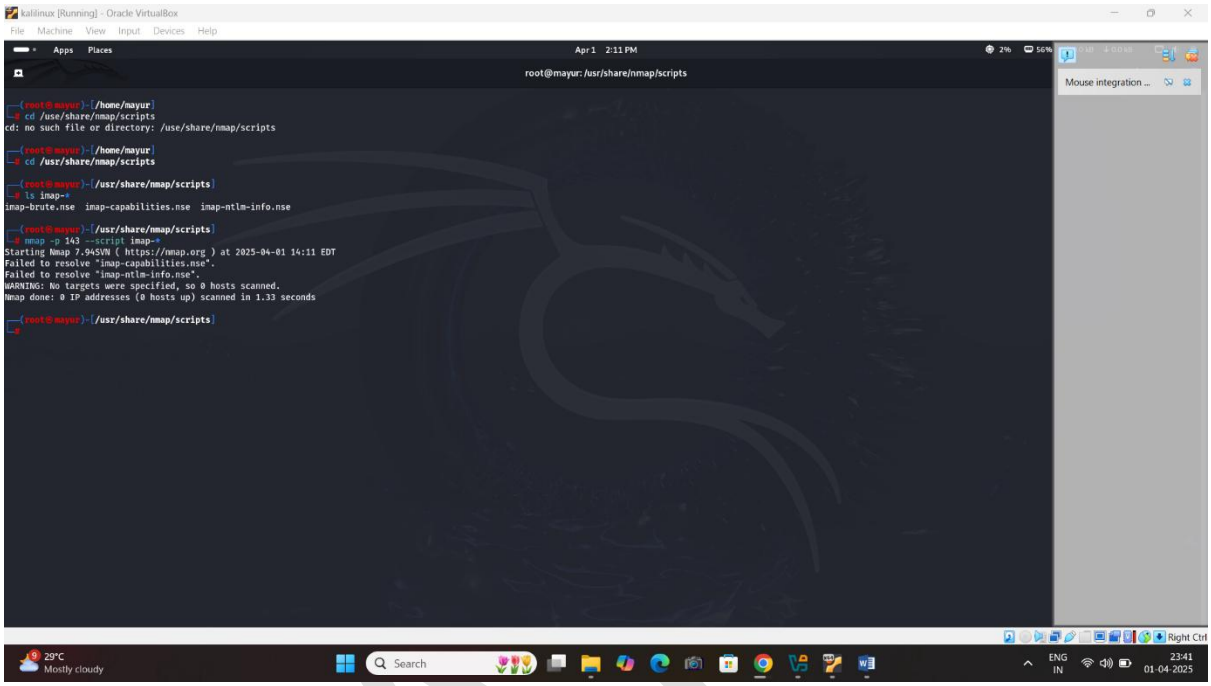
• **Enforce strong authentication** (e.g., IMAP over TLS, multi-factor authentication).

• **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-*



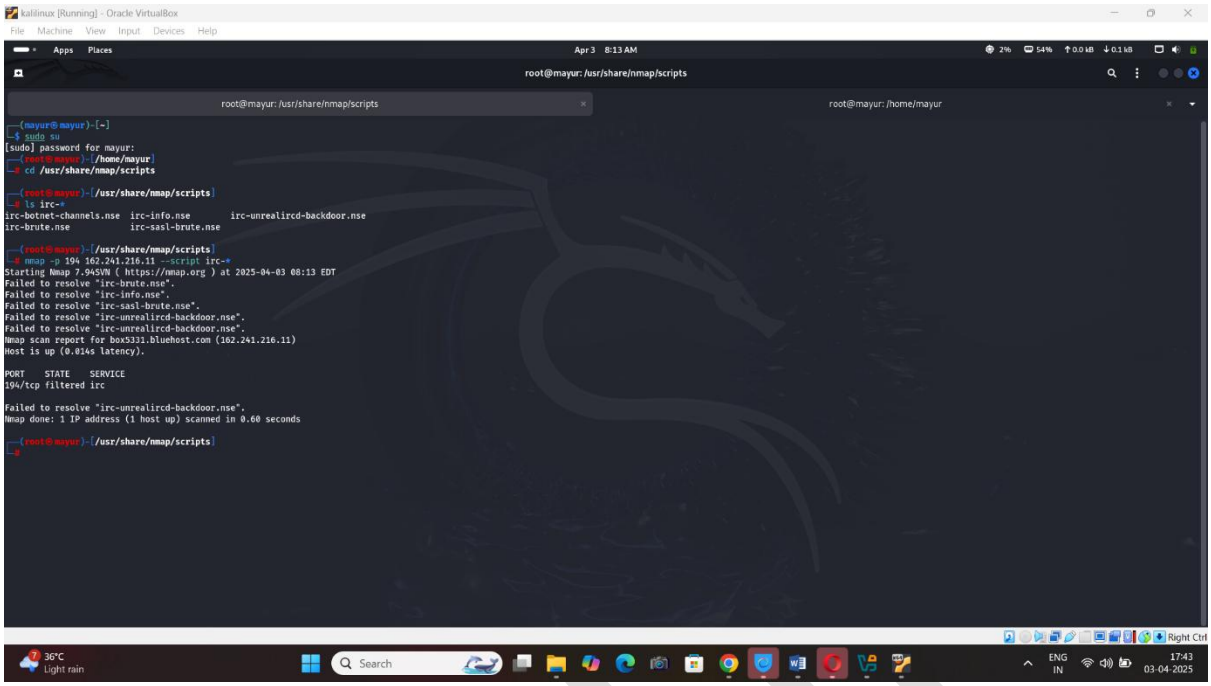
Internet Relay Chat (IRC) is a text-based communication protocol that supports real-time messaging, mainly used for group discussions and private messaging. Enumeration in the context of

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

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

Explination:

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



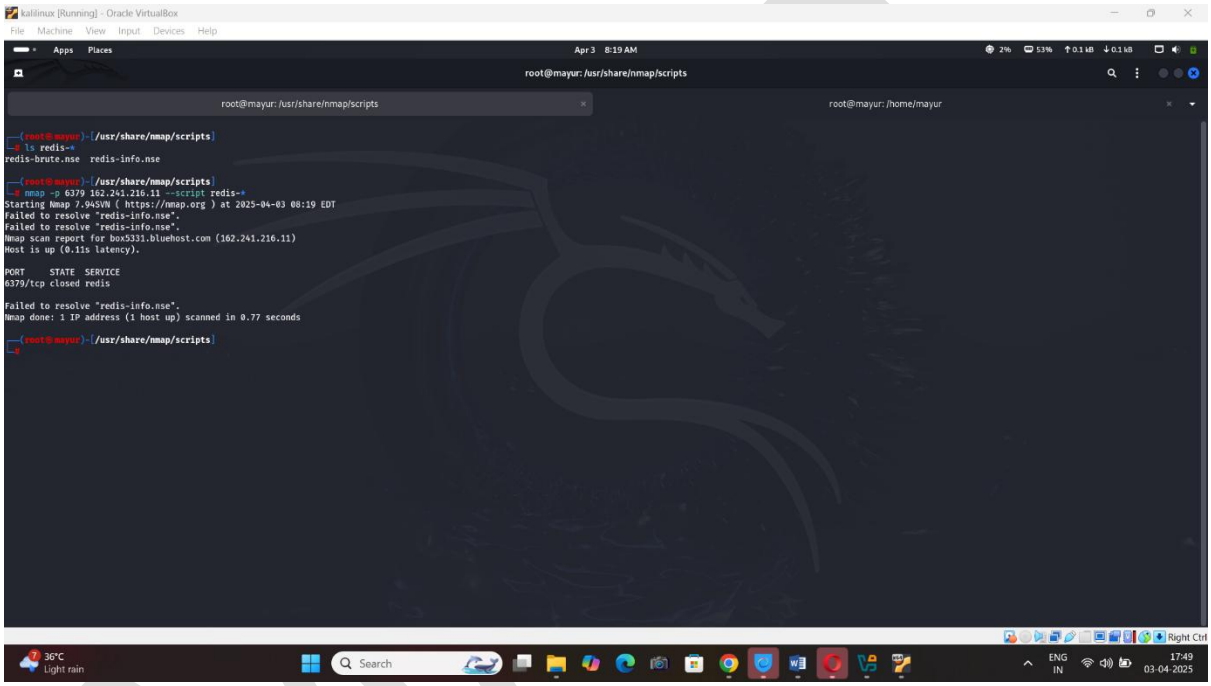
Redis Protocol (RESP - Redis Serialization Protocol)

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-*

Explination:

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.



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-*

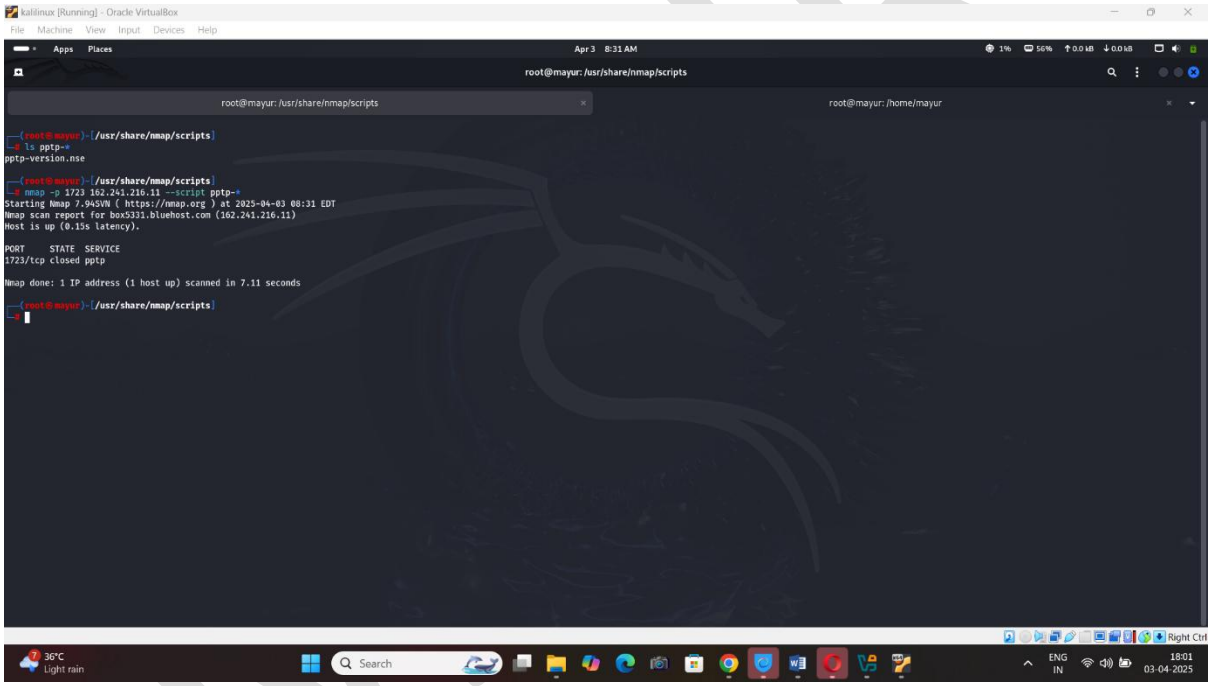
explination

: 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.



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

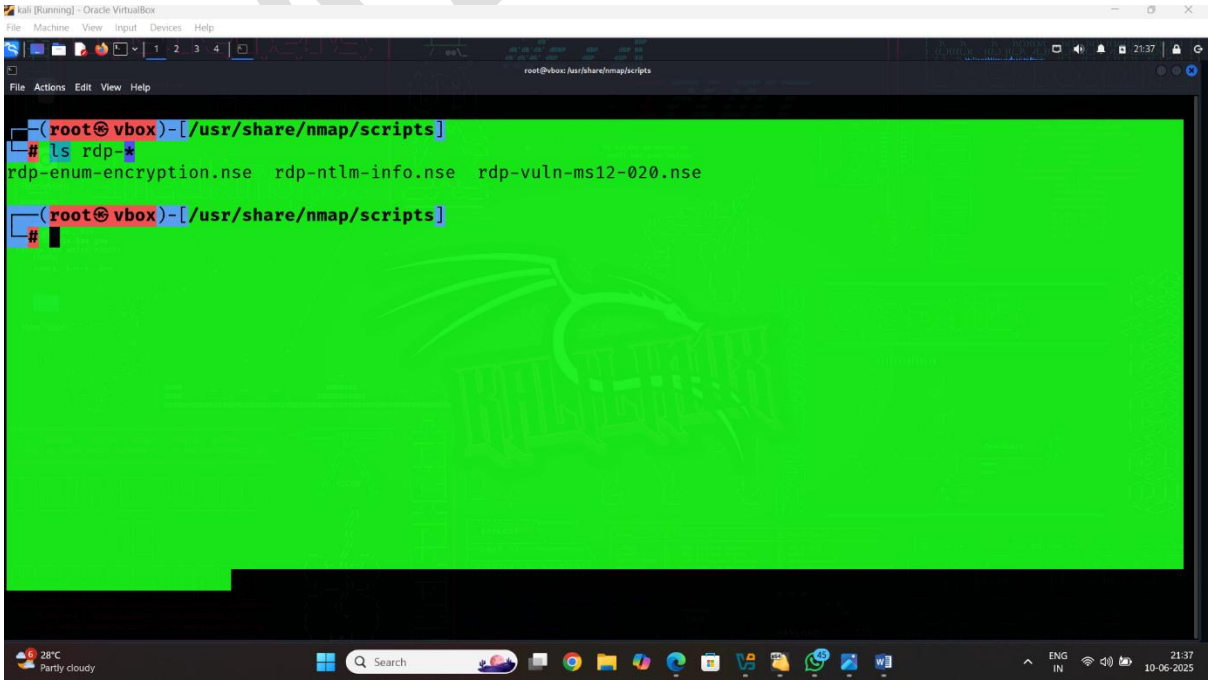
operate a computer that may be in another city or country — as if you were sitting in front of it.

Key Use Cases

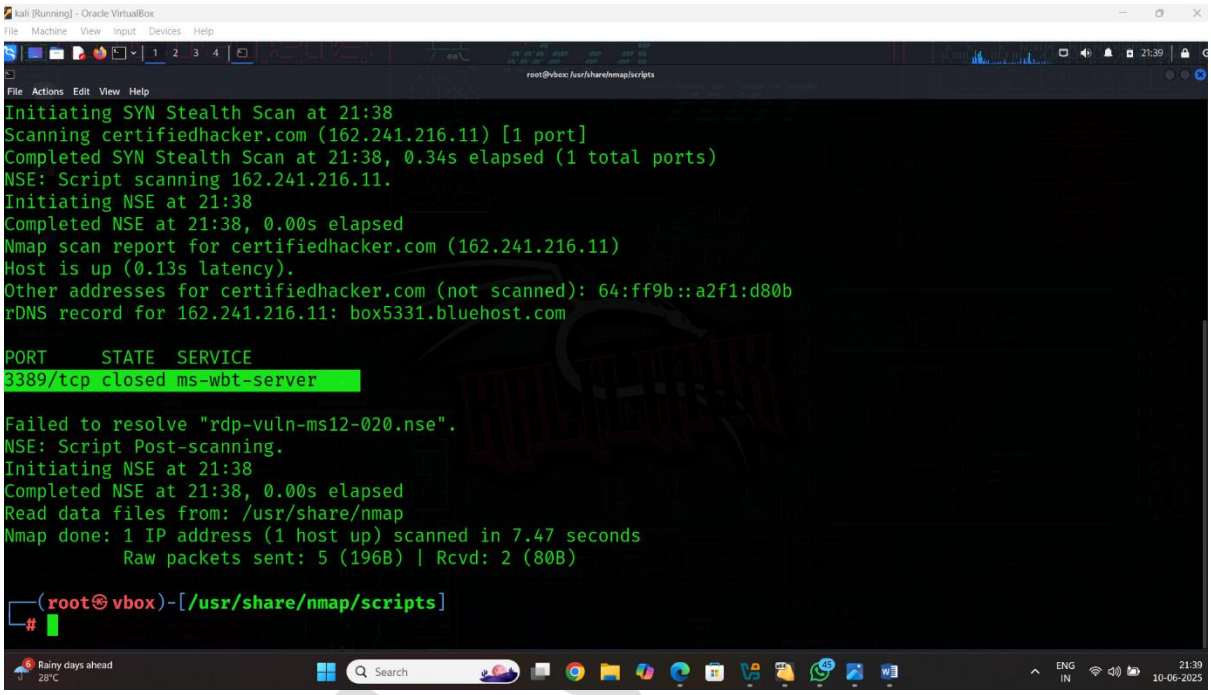
- **Remote administration** of servers and desktops.
- **Remote support** for troubleshooting user issues.
- **Work from home** scenarios.
- **Virtual desktops** in enterprise environments.

Step1 open the kli linux terminal

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



Result:



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).

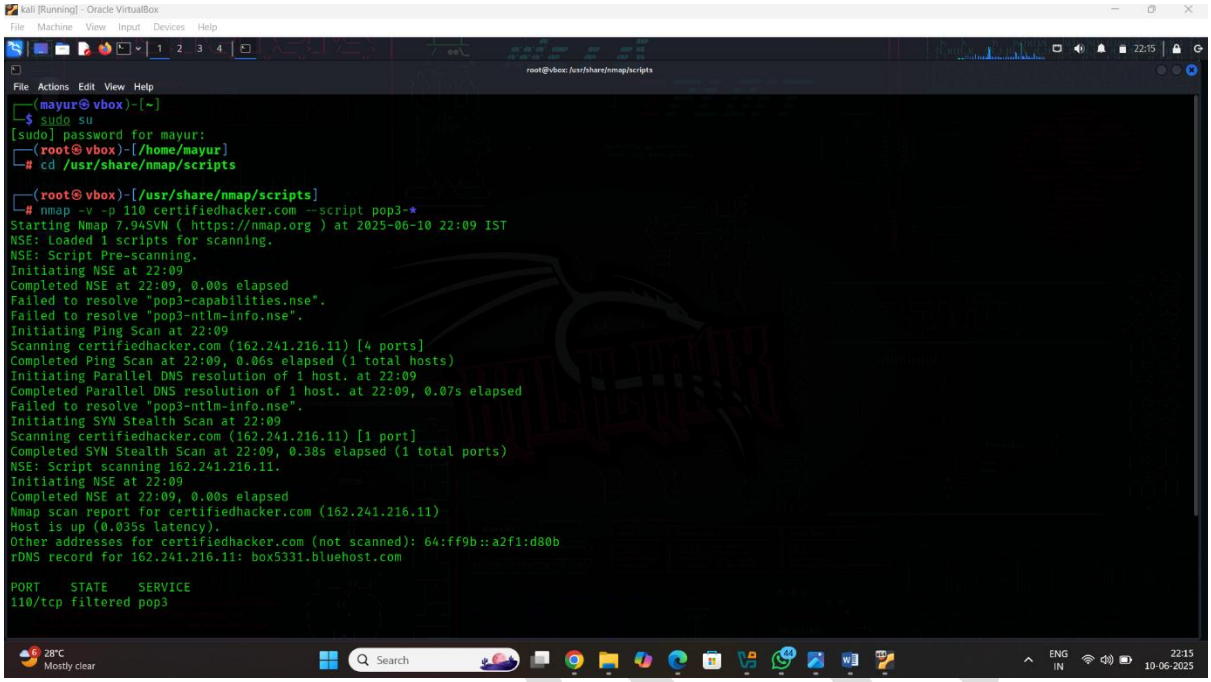
- **Offline Access**:

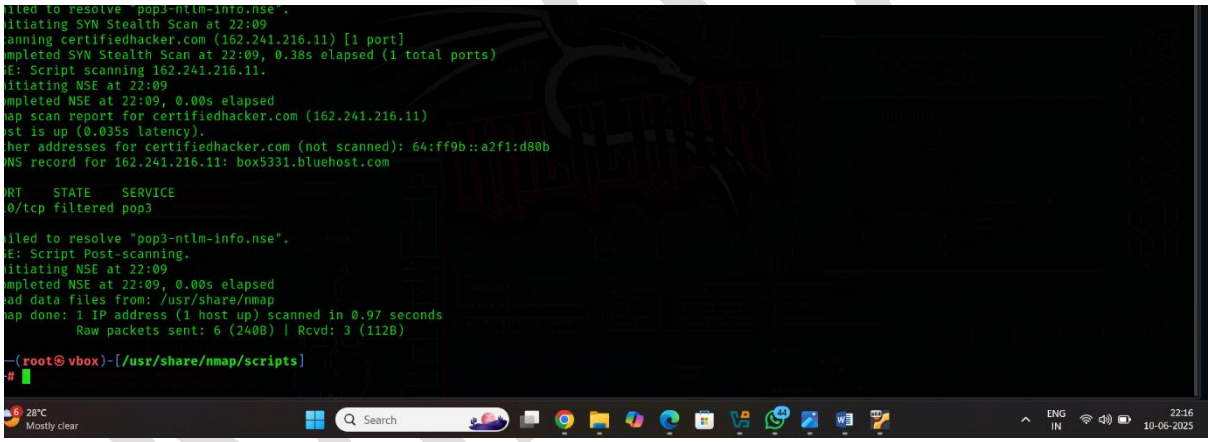
You can now **read emails locally** even without an internet connection.

Step1: open the kali linux terminal

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

Result:


kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(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
28°C Mostly clear
Search
ENG IN
22:15 10-06-2025


iled to resolve "pop3-ntlm-info.nse".
itiating SYN Stealth Scan at 22:09
anning certifiedhacker.com (162.241.216.11) [1 port]
mpleted SYN Stealth Scan at 22:09, 0.38s elapsed (1 total ports)
E: Script scanning 162.241.216.11.
itiating NSE at 22:09
mpleted NSE at 22:09, 0.00s elapsed
ap scan report for certifiedhacker.com (162.241.216.11)
st is up (0.035s latency).
her addresses for certifiedhacker.com (not scanned): 64:ff9b::a2f1:d80b
NS record for 162.241.216.11: box5331.bluehost.com
RT STATE SERVICE
0/tcp filtered pop3
iled to resolve "pop3-ntlm-info.nse".
E: Script Post-scanning.
itiating NSE at 22:09
mpleted NSE at 22:09, 0.00s elapsed
ad data files from: /usr/share/nmap
ap 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]
#
28°C Mostly clear
Search
ENG IN
22:16 10-06-2025