Report On Enumeration

-Tanmay Khedekar

Table of Content-

Introduction

Enumeration is the process of actively gathering detailed information from a target system or network to understand how it is structured and where potential weaknesses may exist. In this phase, the tester interacts directly with services to collect useful data such as usernames, device names, shared folders, running services, open ports, and system configuration details.

This information helps identify misconfigurations, weak authentication settings, exposed resources, and other security gaps that attackers may exploit. Enumeration plays an important role in building a clear picture of the internal environment, allowing better planning for further testing and helping organizations strengthen their overall security posture.

Overall, enumeration acts as a bridge between scanning and exploitation. By revealing how systems communicate, what services are available, and what resources are accessible, it provides the foundation needed to determine the most effective approach for identifying and addressing security issues.

Additionally, enumeration helps validate the accuracy of earlier reconnaissance results and ensures that the assessment is based on reliable, real-time information. The data collected in this phase supports deeper analysis, guiding testers toward areas that require further investigation and helping organizations improve the overall security of their network infrastructure.

Objective of Enumeration

The primary objective of enumeration is to actively gather in-depth and structured information about the target system, network, or environment to identify potential weaknesses that may lead to security compromise. Unlike passive reconnaissance, which focuses on observing information without directly interacting with the target, enumeration involves deliberate communication with network services, protocols, and systems to extract meaningful and actionable data. This step aims to uncover critical details such as usernames, machine names, network shares, open ports, running services, software versions, domain information, and configuration settings that may expose security gaps.

Another major purpose of enumeration is to validate earlier reconnaissance results and build a more accurate understanding of the internal architecture. By collecting this information, testers can map how systems interact, identify trust relationships, and detect inconsistencies or misconfigurations that could be exploited. Enumeration also plays an essential role in identifying weak authentication mechanisms, publicly accessible services, unnecessary user privileges, and misconfigured network shares, all of which increase the risk of unauthorized access.

Additionally, the objective extends to supporting further phases of the security assessment, such as vulnerability analysis and exploitation. The information gathered helps in determining attack paths, prioritizing risks, and recognizing areas that require immediate attention. Through effective enumeration, organizations gain insight into their exposure level and can take informed steps to enhance their security posture.

Overall, enumeration aims to provide a clear and detailed picture of the target environment, enabling better decision-making, improved defences, and stronger protection against potential cyberattacks.

1.Performing NetBIOS Enumeration:

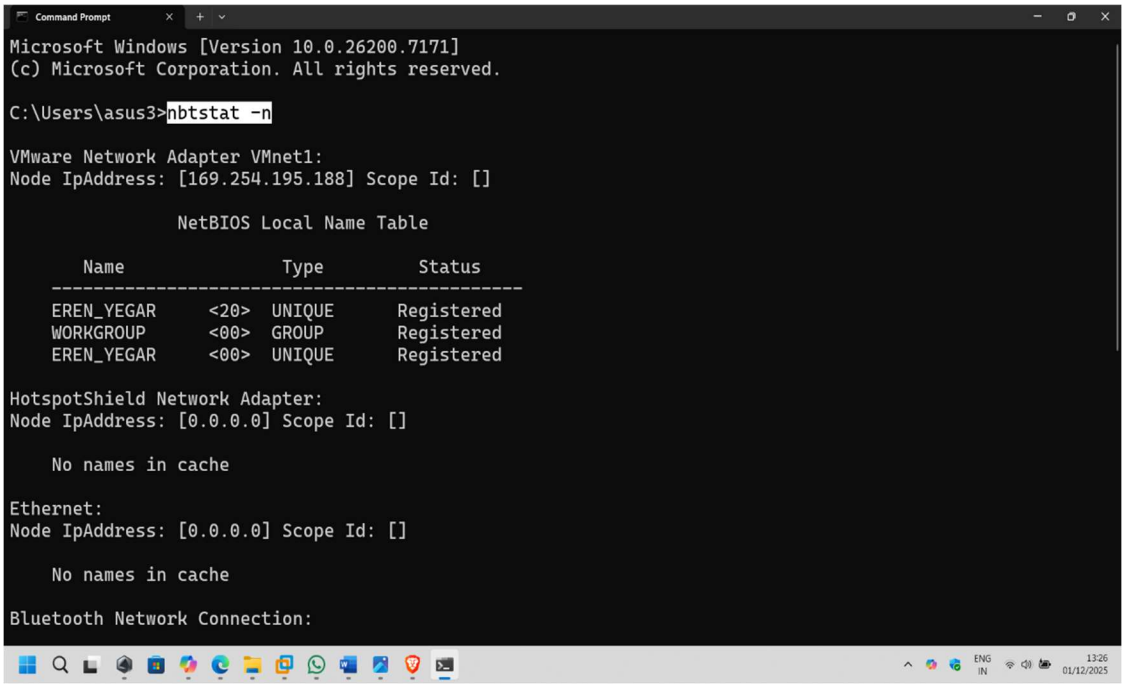

Figure 1Running nbtstat and showing local names

Command- nbtstat -n:

The nbtstat -n command is used to display the local NetBIOS names that are registered on the system. It shows information such as the computer name, user name, workgroup, and other NetBIOS services that the machine has registered. This helps in identifying how the system is recognized on the network and what NetBIOS roles or services it is currently running.

How To Run- On Windows:

1. Open Command Prompt
   - Press Windows + R
   - Type cmd
   - Press Enter
2. Run the Command
   - Type the following command:
   - nbtstat -n
   - Press Enter
3. View the Output
   - The system will display all local NetBIOS names registered on the device, such as:

- Computer name
- Workgroup/domain name
- Logged-in user
- NetBIOS services

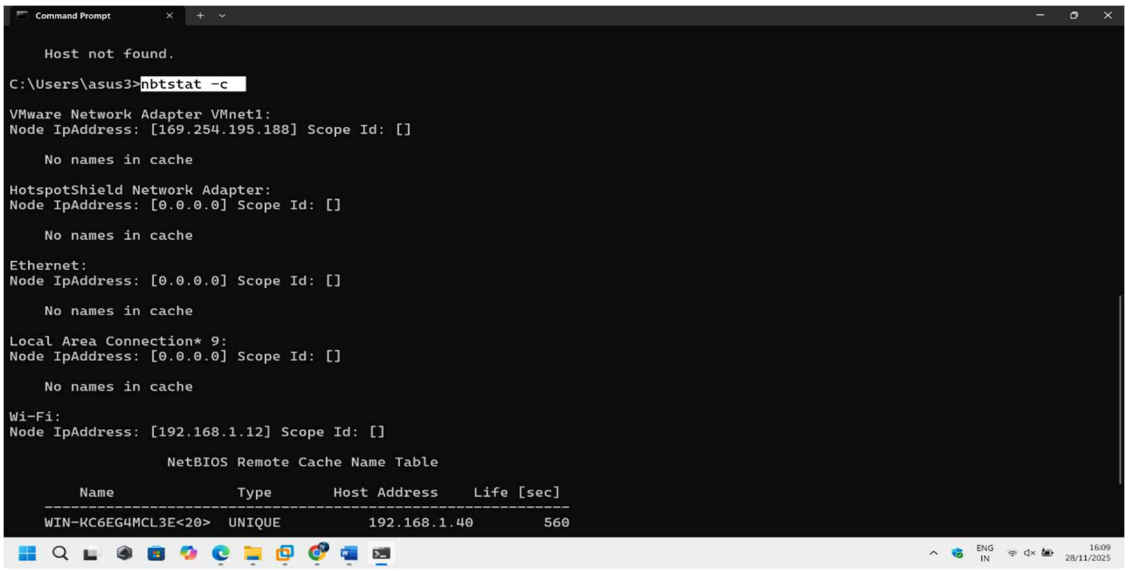

Figure 2Showing cache files

Command: nbtstat -c:

The nbtstat -c command displays the **NetBIOS name cache** on your system. This cache stores recently resolved NetBIOS names and their corresponding IP addresses.

How to Run nbtstat -c

Steps (Windows Only):

1. Open Command Prompt
    - Press Windows + R
    - Type cmd
    - Hit Enter
2. Run the command:
3. nbtstat -c
4. Press Enter and you will see a table showing:
    - NetBIOS Name
    - Type (Unique/Group)

- IP Address
- Status (Resolved or Not)

Result:

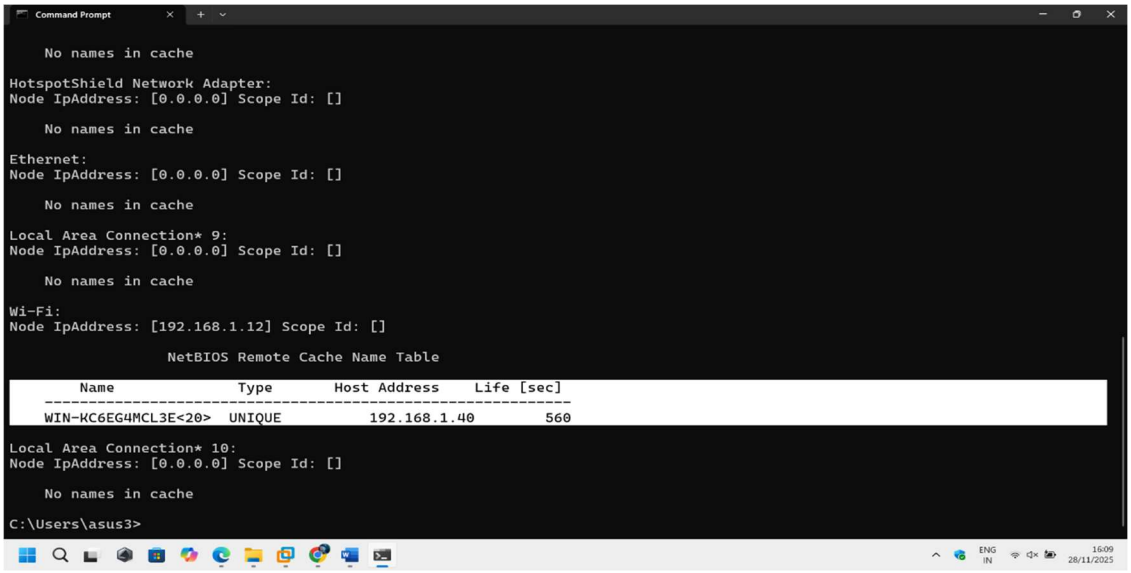

Figure 4 Showing Result

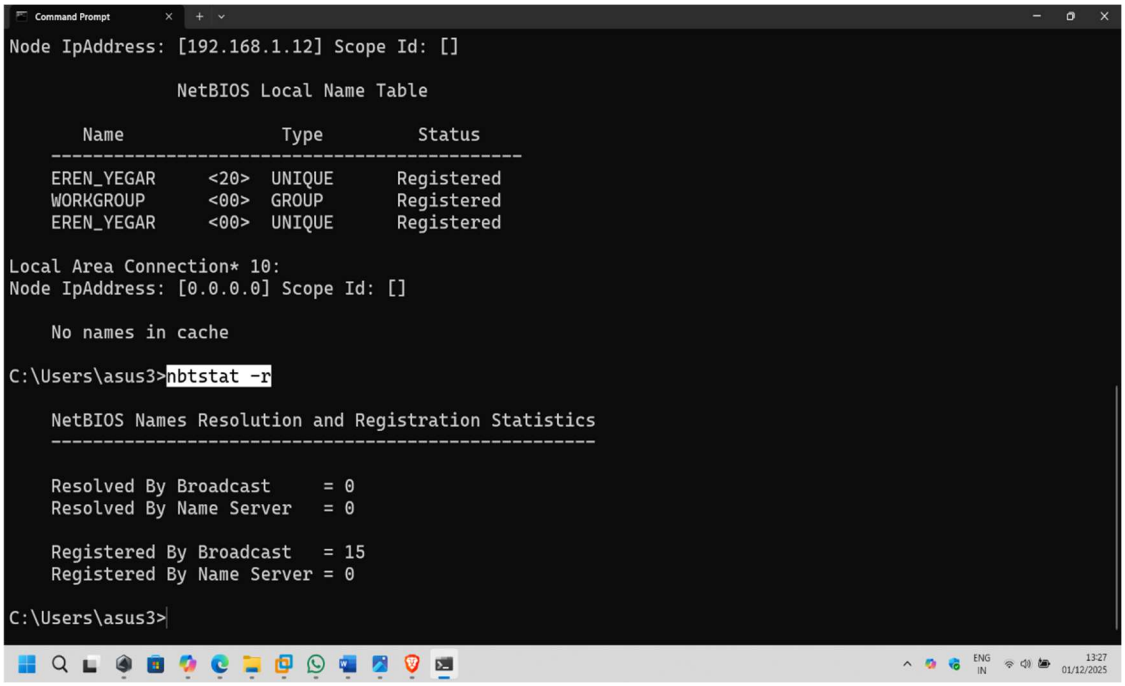

Figure 3 Running nbtstat -r for brodcast

Command: nbtstat -r:

The nbtstat -r command displays **NetBIOS name resolution statistics** on your system.
It shows how many NetBIOS names were resolved using:

- **Broadcast**
- **WINS (Windows Internet Name Service)**

This helps you understand how your computer is resolving NetBIOS names on the network and whether the system is relying more on broadcast or on a WIN'S server.

How to Run nbtstat -r

Steps (Windows Only):

1. **Open Command Prompt**
   - Press **Windows + R**
   - Type **cmd**
   - Press **Enter**
2. **Run the Command**
3. nbtstat -r
4. **Press Enter**
   You will see statistics such as:
   - Number of names resolved by broadcast
   - Number of names resolved by WINS
   - Number of failed resolutions

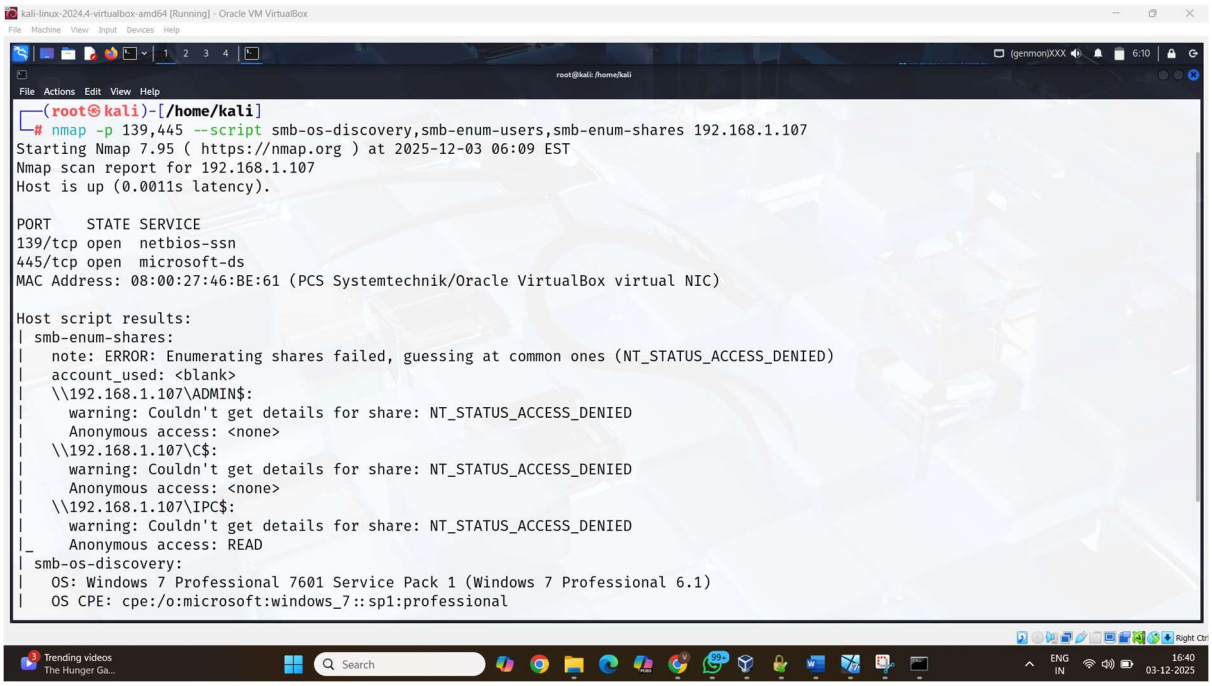

Figure 5 Shows script result

Command: nmap -p 139,445 --script smb-os-discovery, smb-enum-users, smb-enum-shares <target IP>

This command is used to gather important SMB information from a target system by scanning ports 139 and 445 and running SMB enumeration scripts.

Results:

• Operating System Info (smb-os-discovery)

Shows basic details about the target's OS, such as:

- Windows version
- Computer/host name
- Workgroup or domain

• User Enumeration (smb-enum-users)

Lists the user accounts found on the target, such as:

- Administrator
- Guest
- Local users

• Share Enumeration (smb-enum-shares)

Displays shared folders available on the system, including:

- Public shares
- Hidden administrative shares (like C$, ADMIN$)
- Access permissions

Overall Use: This command helps identify OS details, users, shared folders, and possible weaknesses in SMB configuration that can be used for further testing.

How to Run This Command

1. **Open your terminal (Linux or Kali)**
2. **Run the command** Example:
3. nmap -p 139,445 --script smb-os-discovery,smb-enum-users,smb-enum-shares 192.168.1.107
4. **Press Enter.**
   Nmap will begin scanning the target's SMB services and return the results.

Result:

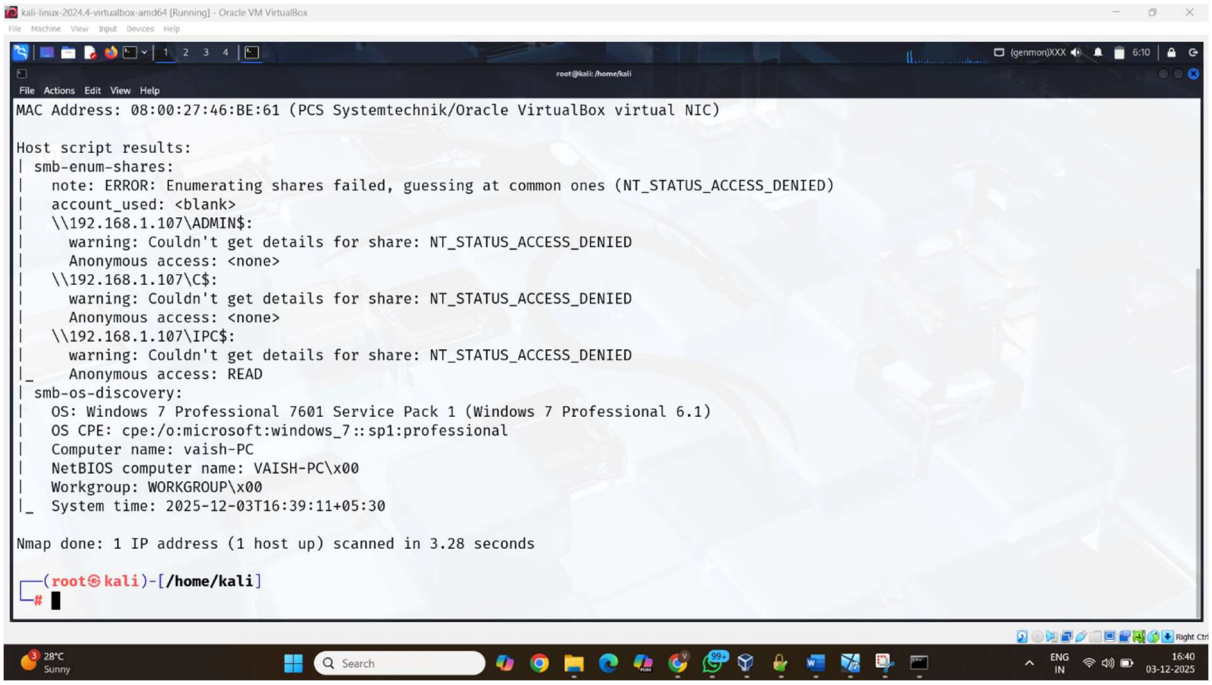

Figure 6 Showing result

2.Perform SNMP Enumeration:

SNMP stands for Simple Network Management Protocol. It is an application-layer protocol used to manage and monitor network devices and their functions.

What is SNMP?

- **Function:** SNMP allows a **manager** (monitoring station) to query an **Agent** (software running on a device) to retrieve or modify configuration and status data.
- **Ports:** SNMP uses **UDP port 161** for agent queries and **UDP port 162** for receiving unsolicited alerts (traps).
- **Core Database (MIB):** The information on the managed device is organized in a structured, hierarchical database called the **Management Information Base (MIB)**. Each data point is uniquely identified by an **Object Identifier (OID)**.

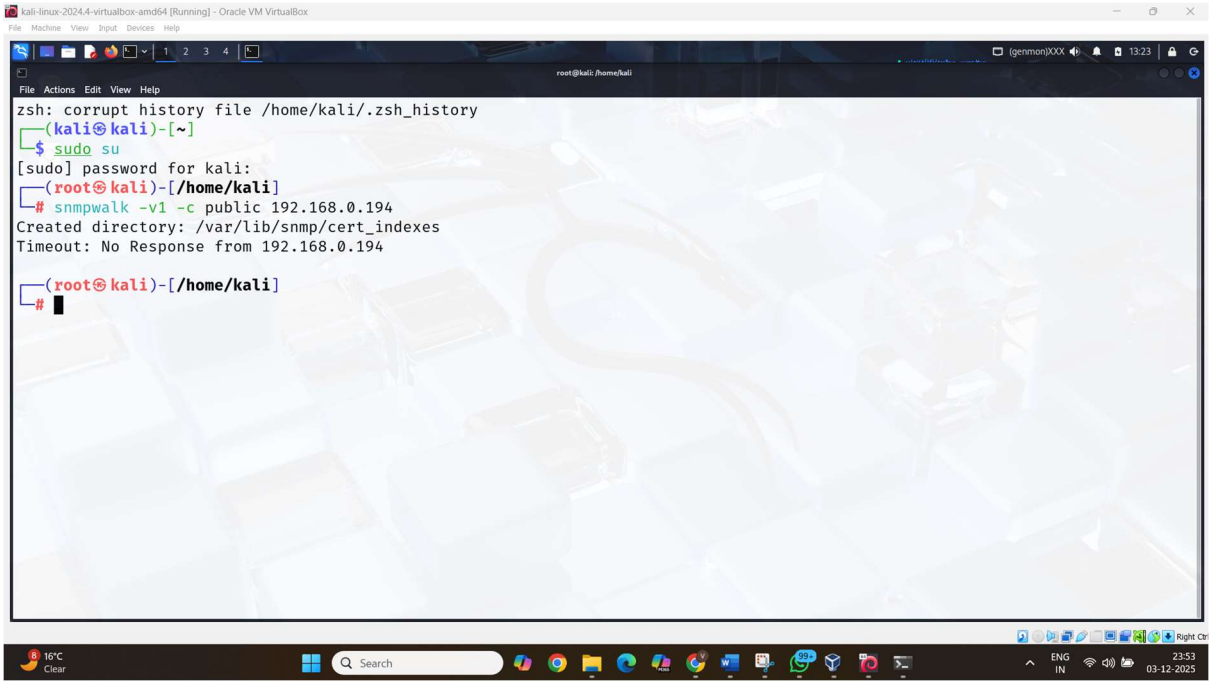

Figure 7 Showing result of snmpwalk

Command: snmpwalk -v1 -c public [target IP]

The snmpwalk command is used to collect information from a device using the **SNMP (Simple Network Management Protocol)**. It queries the target device and retrieves a list of SNMP data, such as system details, network information, running services, and hardware statistics.

This command uses:

- **-v1** → Specifies SNMP version 1
- **-c public** → Uses "public" as the SNMP community string (like a password for read-only access)
- **[target IP]** → The device you want to query

How to Run:

Step 1: Open Terminal

On Linux/Kali

Step 2: Check if SNMP tools are installed

Run:

snmpwalk --version

If not installed, install with:

sudo apt install snmp

Step 3: Run the Command

Example:

snmpwalk -v1 -c public 192.168.1.194

3.Perform LDAP Enumeration:

LDAP stands for Lightweight Directory Access Protocol. It is an application protocol used over an IP network to manage and access distributed directory information services.

LDAP is essentially a standardized way of **organizing and querying centralized directory data**—like usernames, passwords, email addresses, and server locations—stored in a server known as a **Directory Server** (or Directory Information Tree).

- **Protocol:** LDAP defines the **language** used to communicate with the directory server.
- **Purpose:** It's primarily used for **centralized authentication** and **authorization**. Instead of every application managing its own list of users, applications can query a single LDAP server to verify a user's credentials and retrieve their access rights.
- **Ports:** LDAP typically uses **TCP port 389**. The secure version, **LDAPS** (LDAP over SSL/TLS), uses **TCP port 636**.

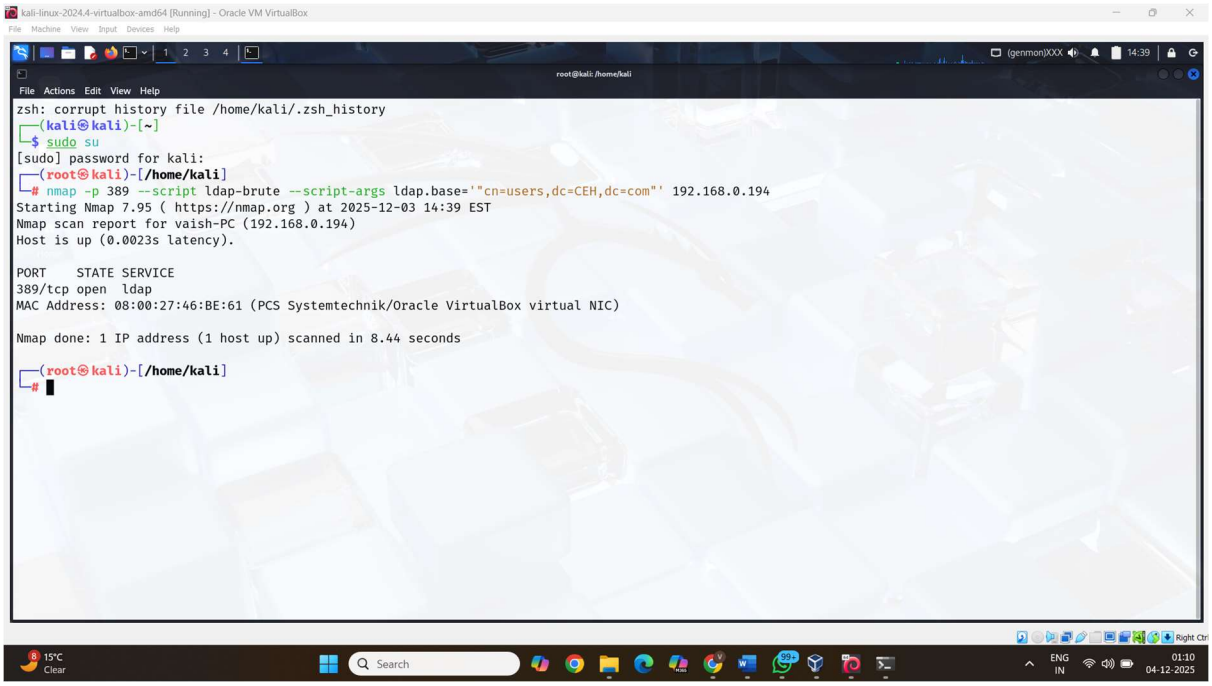

Figure 8 Using Scripting LDPA

Command-nmap -p 389 –script ldap-brute –script-args ldap.base="'cn=users,dc=CEH,dc=com"' 192.168.0.194

This Nmap command is used to perform **LDAP brute-force enumeration** on a target system that is running an LDAP service on port **389**.
It attempts to find valid usernames and passwords in an LDAP directory by trying multiple login combinations.

Breakdown of the Command

- **-p 389**

Specifies scanning **port 389**, which is the default port for **LDAP** (Lightweight Directory Access Protocol).

- **--script ldap-brute**

Runs the **ldap-brute** script to perform brute-force attempts against the LDAP server.
It tries various username/password combinations to check if any credentials are valid.

- **--script-args ldap.base="cn=users,dc=CEH,dc=com"**

This tells Nmap the **LDAP base DN** (directory path) where it should search for users.
Example meaning:

- cn=users → Container where user accounts are stored

- dc=CEH,dc=com → Domain components of the LDAP directory

• **192.168.0.194**

Target IP address.

How to Run:

Step 1: Open Terminal

On Kali/Linux

Step 2: Run the Command

Type the command into your terminal, replacing the IP address with your target's IP:

nmap -p 389 --script ldap-brute --script-args ldap.base="cn=users,dc=CEH,dc=com" 192.168.0.194

Press **Enter**.

4.Perform NFS Enumeration:

NFS stands for **Network File System**. It is a distributed file system protocol that allows a user on a client computer to **access files over a computer network** as if the files were stored locally.

NFS was originally developed by Sun Microsystems in the 1980s and is primarily used with Unix and Linux systems, though implementations are available for nearly every operating system.

- Client-Server Model: NFS operates using the client-server model.
  - The NFS Server is the machine that stores the files and directories and makes them available (or "exports" them) to the network.
  - The NFS Client is the machine that mounts the remote file system and accesses the files as if they were local.
- Transparency: The goal of NFS is file access transparency. Users and applications on the client machine should not need to know that the files they are reading or writing are physically located on another machine.
- Protocol: NFS uses Remote Procedure Calls (RPC) to communicate between the client and server.

NFS relies on several ports to function:

- Port 2049/TCP & UDP: The standard port for the NFS Daemon itself.

- Port 111/TCP & UDP: Used by the Portmapper (or rpcbind), which is the service clients first contact to discover which dynamic ports the NFS-related services are currently using**.**

NFS Enumeration is the process of identifying and gathering information about exported directories (shares) on a remote NFS server, and then attempting to access those shares to list their contents.

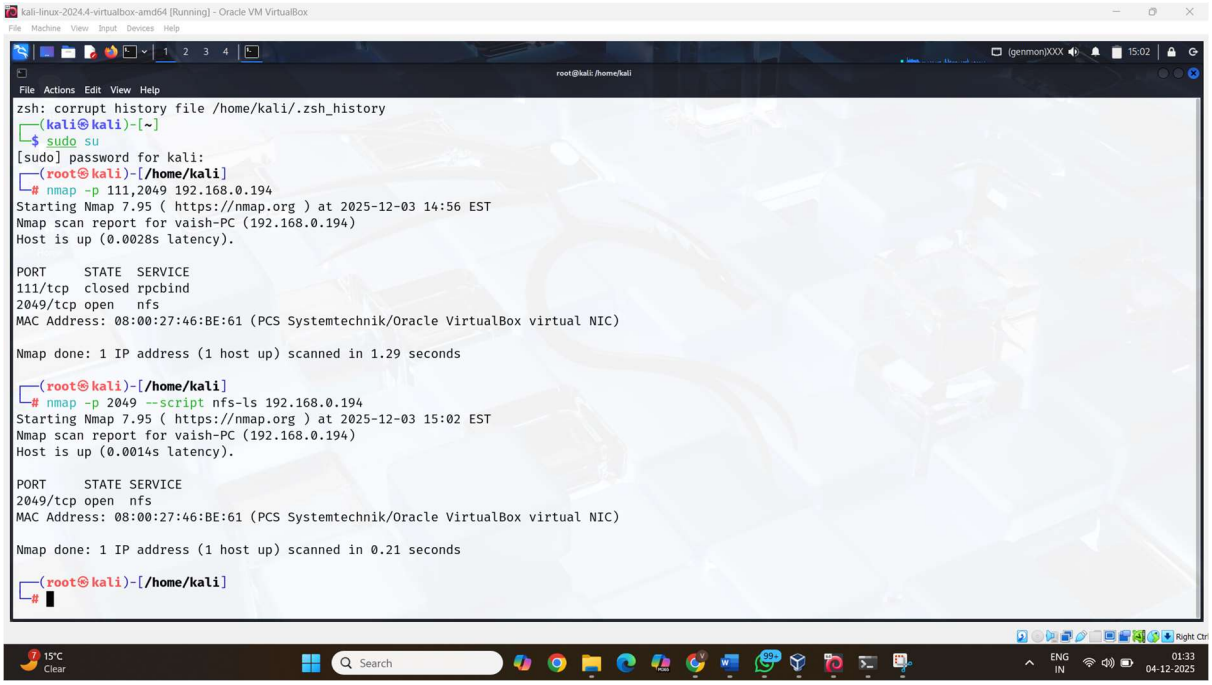

Figure 9Using Scripting NFS enumeration

Command: nmap -p 2049 --script nfs-ls <Target_IP_Address>

This Nmap command is used to enumerate NFS (Network File System) shares on a target machine.

Port 2049 is the default port for NFS services. The script nfs-ls lists the files and directories available on the NFS server, similar to how you browse a shared folder.

How to Run

Step 1: Open Terminal

On Kali/Linux

Step 2: Run the Command

Example:

nmap -p 2049 --script nfs-ls 192.168.1.194

Press **Enter.**

5.Perform DNS Enumeration

DNS enumeration is the process of locating all the DNS records and subdomains for a given domain name to create a map of the network's structure. It's a crucial reconnaissance step that reveals IP addresses, hostnames, mail servers, and potentially internal server names.

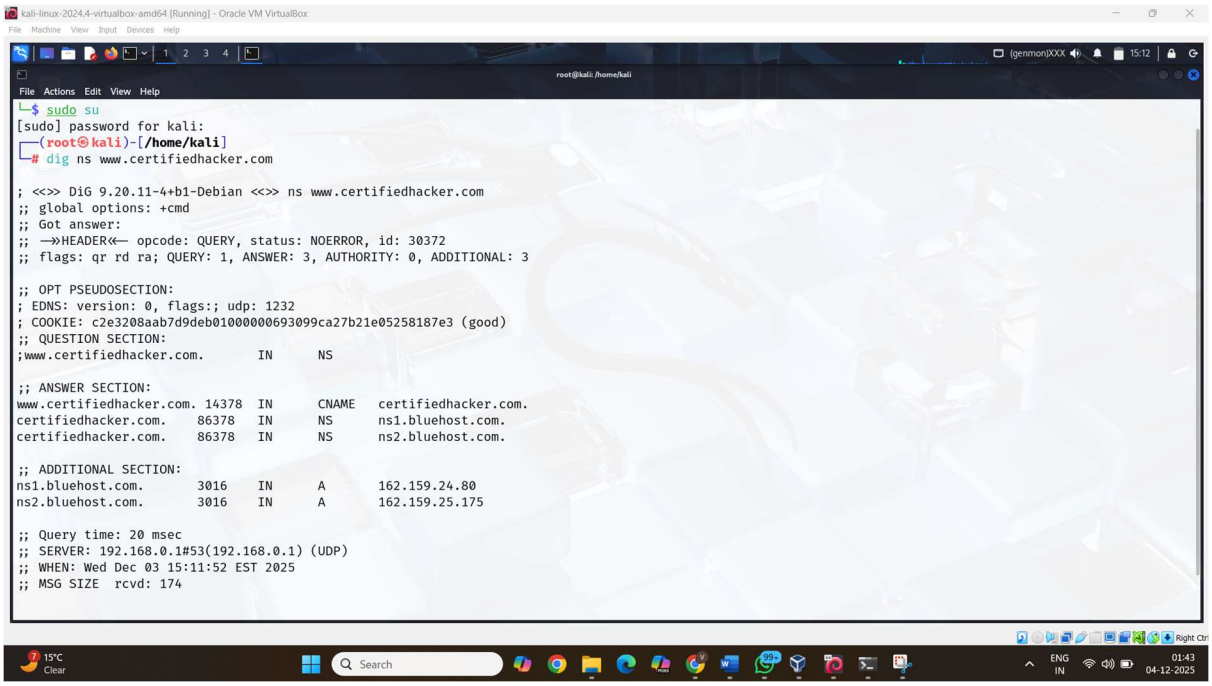

Figure 10Pefroming enumeration using dig

Command- dig ns certifiedhacker.com

This command uses **DIG (Domain Information Groper)** to query the DNS system and retrieve the **Name Servers (NS records)** for the domain *certifiedhacker.com*.

NS records show which servers are responsible for managing and responding to DNS queries for that domain.

How to Run

Step 1: Open Terminal

On Linux/Kali.

Step 2: Run the DIG Command

Simply type:

dig ns certifiedhacker.com

Then press **Enter**.

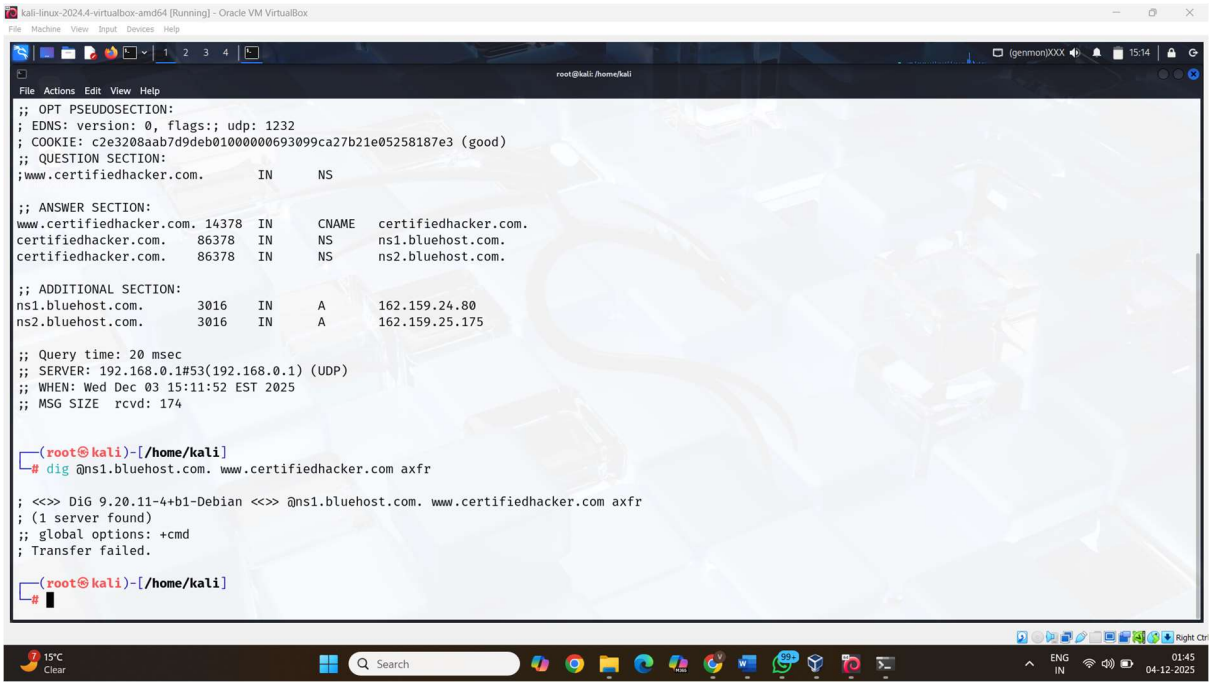

Figure 11Zone Transfer Result

Command-dig @ns1.bluehost.com certifiedhacker.com

This DIG command queries a **specific DNS server**, in this case:
ns1.bluehost.com → A name server belonging to Bluehost.
Instead of asking your default DNS server, DIG directly asks **Bluehost's DNS server** for information about the domain **certifiedhacker.com**.

How to Run

Step 1: Open Terminal

Linux/Kali.

Step 2: Run the DIG Query

Type the command:

dig @ns1.bluehost.com certifiedhacker.com

Press **Enter**.

6.Perform SMTP Enumeration

SMTP stands for **Simple Mail Transfer Protocol**. It is an application-layer protocol used to **send and receive email** across the internet.

SMTP's primary role is to handle the transfer of email messages from one mail server to another, or from a local email client (like Outlook or Thunderbird) to a mail server.

- Sending Mail: When you hit "Send," your email client communicates with the Outgoing Mail Server (SMTP Server) to deliver the message.
- Server-to-Server Transfer: The sending SMTP server then communicates with the receiving SMTP server to relay the message to the recipient's mailbox.

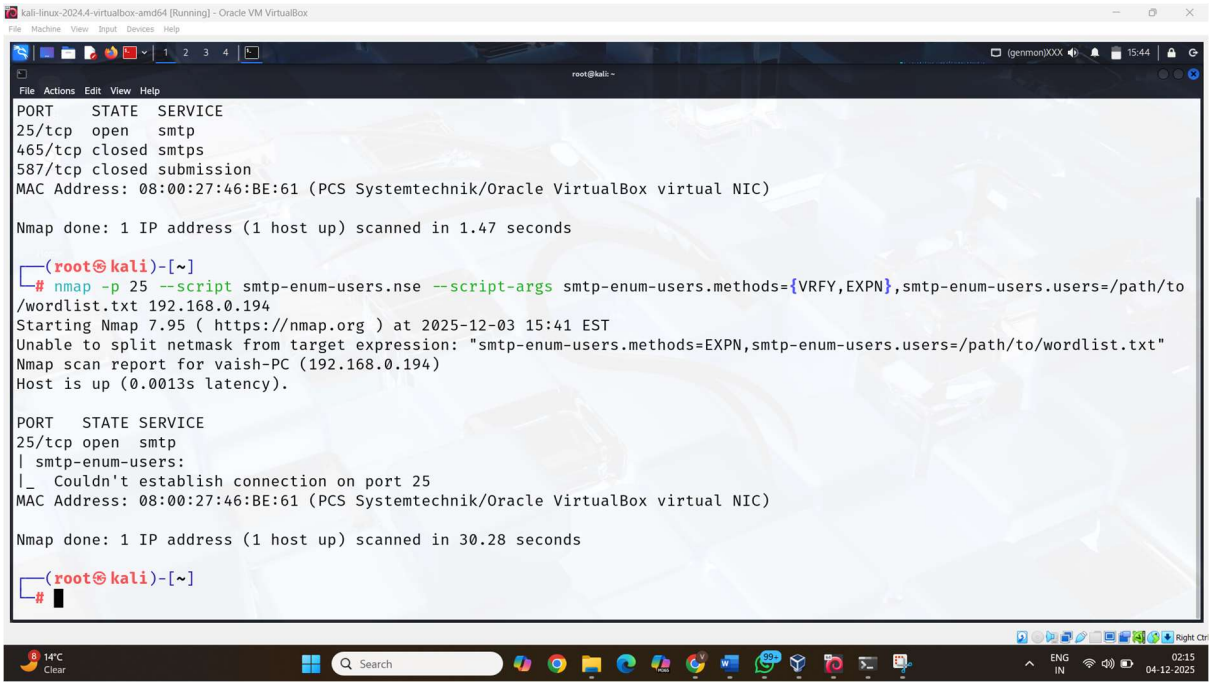

Figure 12Enumeration of SNMP

Command-nmap -p 25 --script smtp-enum-users.nse --script-args smtp-enum-users.methods={VRFY,EXPN},smtp-enum-users.users=/path/to/wordlist.txt <Target_IP_Address>

This Nmap command is used to **enumerate SMTP users** on a mail server running on port **25**.
It attempts to discover valid email usernames by sending SMTP commands to the target server.

What Each Part Does:

• -p 25

Scans **port 25**, which is the default port for the **SMTP service**.

• --script smtp-enum-users.nse

Runs Nmap's **SMTP user enumeration script** that attempts to identify valid users on the server.

• smtp-enum-users.methods={VRFY,EXPN}

Specifies which SMTP methods to use:

- **VRFY** – Checks if a user exists
- **EXPN** – Expands mailing lists or reveals actual user addresses

• smtp-enum-users.users=/path/to/wordlist.txt

Provides a **wordlist** containing possible usernames to test.

How to Run

Step 1: Open Terminal

In Linux/Kali.

Step 2: Prepare Your Wordlist

Use any username list, for example:
/usr/share/wordlists/metasploit/unix_users.txt

Step 3: Run the Command

Replace the path and target IP, example:

```
nmap -p 25 --script smtp-enum-users.nse --script-args smtp-enum-users.methods={VRFY,EXPN},smtp-enum-users.users=/usr/share/wordlists/metasploit/unix_users.txt 192.168.0.194
```

press **ENTER**