

ENUMERATION



REPORT OF ENUMERATION

BY SACHCHITANAND YADAV

Enumeration

MODULE - 4

Learning Objectives -

- Explain Enumeration Concepts
- Demonstrate Different Techniques for NetBIOS Enumeration
- Demonstrate Different Techniques for SNMP Enumeration
- Use Different Techniques for LDAP Enumeration
- Different Techniques for NFS Enumeration
- Perform DNS Enumeration
- Demonstrate Different Techniques for SMTP
- Perform MSRPC Enumeration
- Perform SMB Enumeration
- Perform Enumeration using AI
- Explain Enumeration Countermeasures

Table of Contents

1. Explain Enumeration Concepts

- 1.1 Introduction
- 1.2 Why Enumeration Matters
- 1.3 What Enumeration Reveals
- 1.4 Common Enumeration Techniques
- 1.5 Services and Ports Commonly Enumerated
- 1.6 Practical Notes for Reporting
- 1.7 Defensive Checklist

2. Perform NetBIOS Enumeration

- 2.1 Introduction
- 2.2 Lab Objective
- 2.3 Tools Used (Windows CMD)
- 2.4 Steps to Perform NetBIOS Enumeration
- 2.5 Findings and Usage

3. Perform SNMP Enumeration

- 3.1 Introduction
- 3.2 Lab Scenario
- 3.3 Lab Objective
- 3.4 Performing SNMP Enumeration using Nmap
- 3.5 Interpretation of Results

4. Perform LDAP Enumeration

- 4.1 Overview
- 4.2 Lab Scenario
- 4.3 Lab Objective
- 4.4 Commands Used

MODULE - 4 ENUMERATION

4.5 LDAP Enumeration using Nmap

4.6 Conclusion

5. Perform NFS Enumeration

5.1 Overview

5.2 Lab Scenario

5.3 Lab Objective

5.4 Nmap NFS Scan

5.5 Conclusion

6. Perform DNS Enumeration

6.1 Overview

6.2 Lab Scenario

6.3 Lab Objective

6.4 DNS Enumeration using Nmap

6.5 Conclusion

7. Perform SMTP Enumeration

7.1 Overview

7.2 Lab Scenario

7.3 Lab Objective

7.4 SMTP Enumeration using Nmap

7.5 Conclusion

8. Perform MSRPC Enumeration

8.1 Overview

8.2 Lab Scenario

8.3 Lab Objective

8.4 MSRPC Enumeration using Nmap

8.5 Conclusion

9. Perform SMB Enumeration

- 9.1 Overview
- 9.2 SMB Enumeration using Nmap
- 9.3 Additional Useful Commands
- 9.4 Conclusion

10. Perform Enumeration using AI Tools

- 10.1 Overview
- 10.2 Lab Scenario
- 10.3 Lab Objective
- 10.4 AI Prompts for Enumeration Tasks

11. Enumeration Countermeasures

- 11.1 Disable Unnecessary Services
- 11.2 Enforce Strong Authentication
- 11.3 Restrict and Monitor Network Ports
- 11.4 Apply Account Lockout Policies
- 11.5 Harden DNS and Directory Services
- 11.6 Patch and Update Regularly
- 11.7 Remove Default Accounts and Rename Admins
- 11.8 Use Encryption
- 11.9 Reduce Banner Leakage
- 11.10 Perform Regular Auditing and Pen Testing

Explain Enumeration Concepts

Enumeration.

Introduction

Enumeration is the active, probe-and-listen stage where an attacker moves from passive reconnaissance to direct interaction with a target. Instead of just watching, the attacker opens connections and issues targeted queries to collect actionable details — usernames, shared resources, services, routing data and more — that can be turned into an attack path. In a professional security test, enumeration is run only with explicit authorization.

Why it matters (plain talk)

Think of enumeration like peeking behind doors in a building: every door you identify is a potential entry point. The data you gather tells you where to knock, which locks might be weak, and which doors accidentally open themselves.

What enumeration reveals

Attackers (or a pen tester) commonly extract:

- Hostnames and machine identities
- Network shares and accessible file systems
- Usernames, groups and account metadata
- Running services and service versions (banners)
- Routing and topology details
- SNMP/FQDN and directory service information (e.g., LDAP)
- Audit and service configuration settings

A common escalation vector: discovering an IPC or administrative share (for example, a Windows administrative share) and using that to enumerate filesystem contents or attempt credential attacks.

Common enumeration techniques

1. **Email → username harvesting** — split addresses (user@domain) to build candidate usernames.

2. **Default credentials lookup** — many devices remain with factory accounts that aren't changed. Attackers try well-known defaults.
3. **Active Directory probing / brute force** — AD can leak username validity through differing error messages (e.g., login failures vs. disabled account messages). Extracting valid usernames makes password attacks much easier.
4. **DNS zone transfer** — a misconfigured DNS server may allow a zone transfer, revealing hostnames and IPs for an entire domain. Tools: dig, nslookup.
5. **SNMP queries** — guessing community strings (especially "public" / "private") can disclose device and user info.
6. **OS and protocol banner grabbing** — connecting to services (SSH, SMTP, FTP, HTTP, etc.) to learn software and version details.
7. **Local group enumeration** — with a valid domain account, attackers can query group memberships and permissions.

Services & ports commonly enumerated

(Security teams should audit and monitor these by default.)

- **DNS** — TCP/UDP **53**: zone transfers, name resolution.
- **RPC endpoint mapper** — **TCP 135**: reveals running RPC services.
- **NetBIOS / SMB** — **UDP 137, TCP 139, TCP/UDP 445**: name service, sessions, file/printer sharing and null sessions.
- **SNMP** — **UDP 161 / 162 (traps)**: device management, monitoring data.
- **LDAP / Global Catalog** — **TCP/UDP 389, 3268**: directory queries and object listings.
- **NFS** — **TCP 2049**: remote filesystem mounts and exports.
- **SMTP** — **TCP 25**: mail server commands, VRFY/EXPN may leak addresses.
- **SSH / Telnet** — **TCP 22, 23**: remote admin access; valuable for brute force/banners.
- **FTP / TFTP** — **TCP 20/21, UDP 69**: file transfers and sometimes anonymous access.
- **ISAKMP / IKE** — **UDP 500**: VPN and IPsec negotiation.
- **SIP** — **TCP/UDP 5060, 5061**: VoIP signaling and endpoints.
- **BGP** — **TCP 179**: routing — misconfig can enable serious routing attacks.

(When listing in a report, annotate each port with why it's sensitive for your target environment.)

Practical notes for a report: how to present findings

- Group findings by **service criticality** (high/medium/low) and **exploitability** (easy/moderate/difficult).
- Include **sample commands/output** (sanitized) so readers see the evidence, e.g., `dig AXFR example.com @ns1.example.com` or an `smbclient` enumeration snippet.

- Always state **authorization** and the **time window** used for tests. Enumeration without permission may be illegal.
- Recommend **quick mitigations** beside each finding (e.g., disable zone transfers, restrict SNMP access, firewall SMB ports, enforce strong password policy).

Defensive checklist

- Block or restrict unnecessary ports at the perimeter and internal firewalls.
- Disable or restrict DNS zone transfers.
- Change default credentials and audit devices for factory accounts.
- Use strong SNMP community strings or replace SNMPv2 with authenticated SNMPv3.
- Harden AD: limit detailed error messages, monitor failed enumeration patterns, enable conditional access.
- Disable legacy protocols (Telnet, NetBIOS) where possible.
- Monitor for suspicious banner/banner-change and unusual queries to RPC/LDAP/SNMP.

Perform NetBIOS Enumeration

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) .

NetBIOS enumeration is the process of extracting network details from Windows systems using the NetBIOS API. It helps identify computers in a domain, shared folders, user accounts, and system policies.

Lab Objective

To gather information about Windows hosts by performing NetBIOS enumeration through built-in Windows command-line tools.

Perform NetBIOS Enumeration using Windows CommandLine Utilities

Tools Used (Windows CMD)

- nbtstat
- net view
- net use

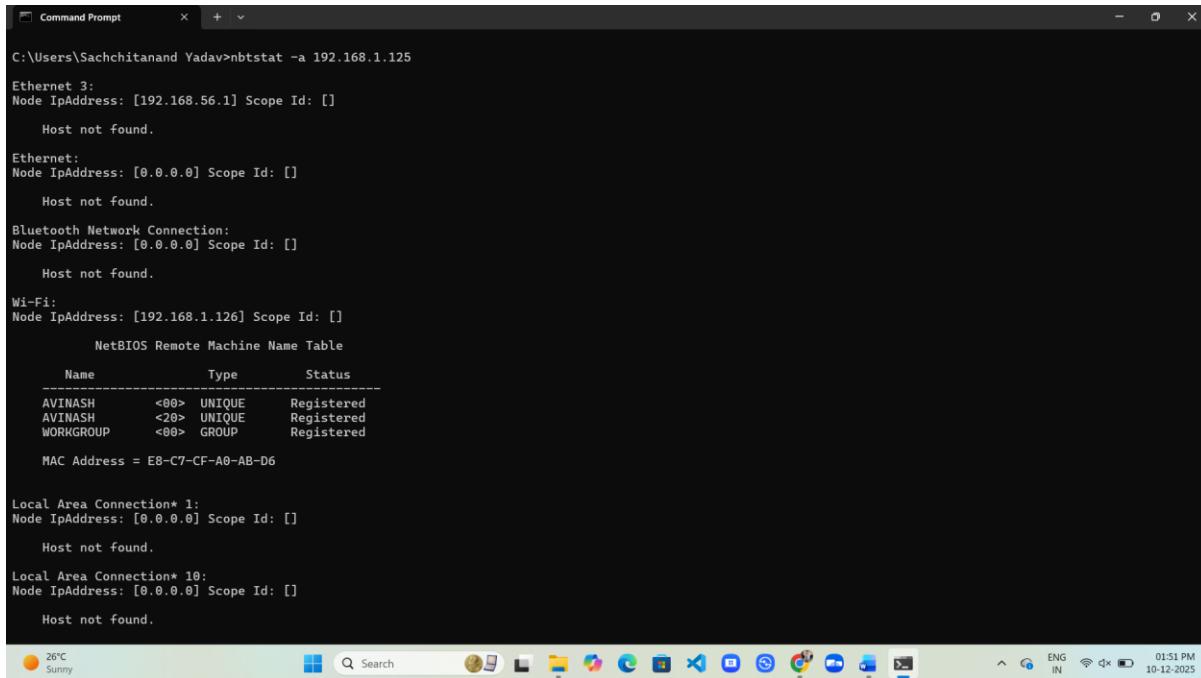
Steps

1. Find NetBIOS name table of a target:

`nbtstat -a <IP>`

→ Shows workstation name, domain, and logged-in users.

MODULE - 4 ENUMERATION



```
C:\Users\Sachchitanand Yadav>nbtstat -a 192.168.1.125

Ethernet 3:
Node IpAddress: [192.168.56.1] Scope Id: []
    Host not found.

Ethernet:
Node IpAddress: [0.0.0.0] Scope Id: []
    Host not found.

Bluetooth Network Connection:
Node IpAddress: [0.0.0.0] Scope Id: []
    Host not found.

Wi-Fi:
Node IpAddress: [192.168.1.126] Scope Id: []

        NetBIOS Remote Machine Name Table

        Name          Type      Status
        AVINASH       <00>    UNIQUE    Registered
        AVINASH       <20>    UNIQUE    Registered
        WORKGROUP     <00>    GROUP     Registered

        MAC Address = E8-C7-CF-A0-AB-D6

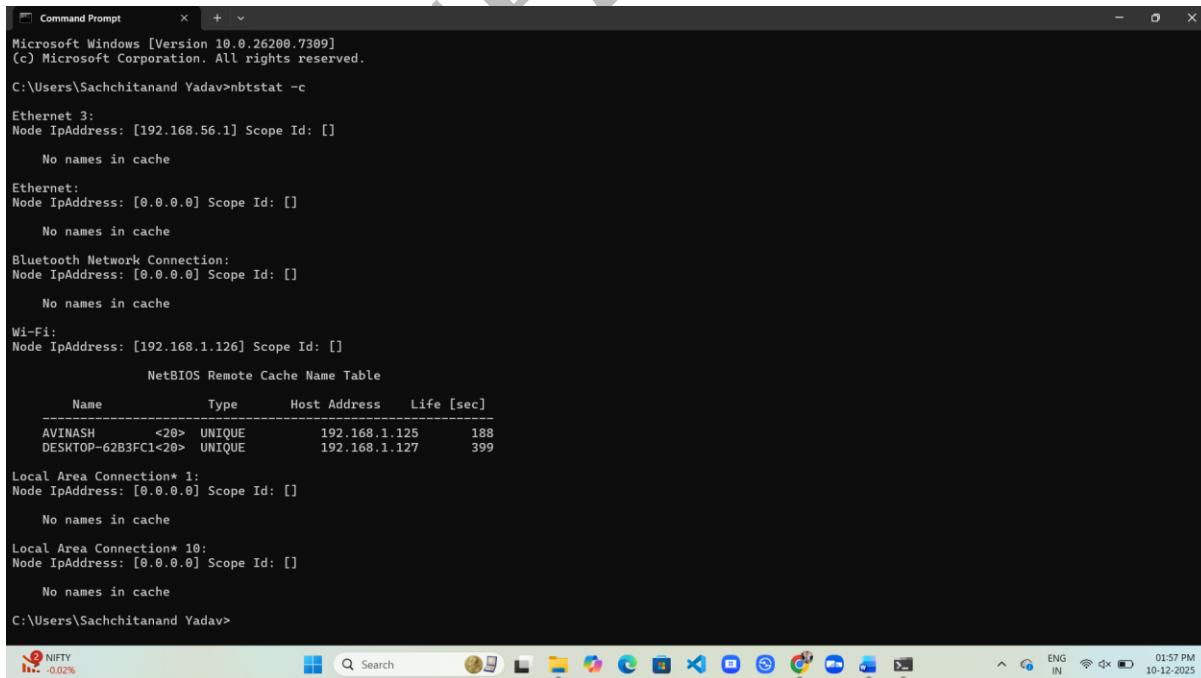
Local Area Connection* 1:
Node IpAddress: [0.0.0.0] Scope Id: []
    Host not found.

Local Area Connection* 10:
Node IpAddress: [0.0.0.0] Scope Id: []
    Host not found.

26°C
Sunny
01:51 PM
10-12-2025
```

2. In the same Command Prompt window, run nbtstat -c command.

Note: In this command, -c lists the contents of the NetBIOS name cache of the remote computer.



```
Microsoft Windows [Version 10.0.26200.7309]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Sachchitanand Yadav>nbtstat -c

Ethernet 3:
Node IpAddress: [192.168.56.1] Scope Id: []
    No names in cache

Ethernet:
Node IpAddress: [0.0.0.0] Scope Id: []
    No names in cache

Bluetooth Network Connection:
Node IpAddress: [0.0.0.0] Scope Id: []
    No names in cache

Wi-Fi:
Node IpAddress: [192.168.1.126] Scope Id: []

        NetBIOS Remote Cache Name Table

        Name          Type      Host Address   Life [sec]
        AVINASH       <20>    UNIQUE        192.168.1.125  188
        DESKTOP-62B3FC1<20> UNIQUE        192.168.1.127  399

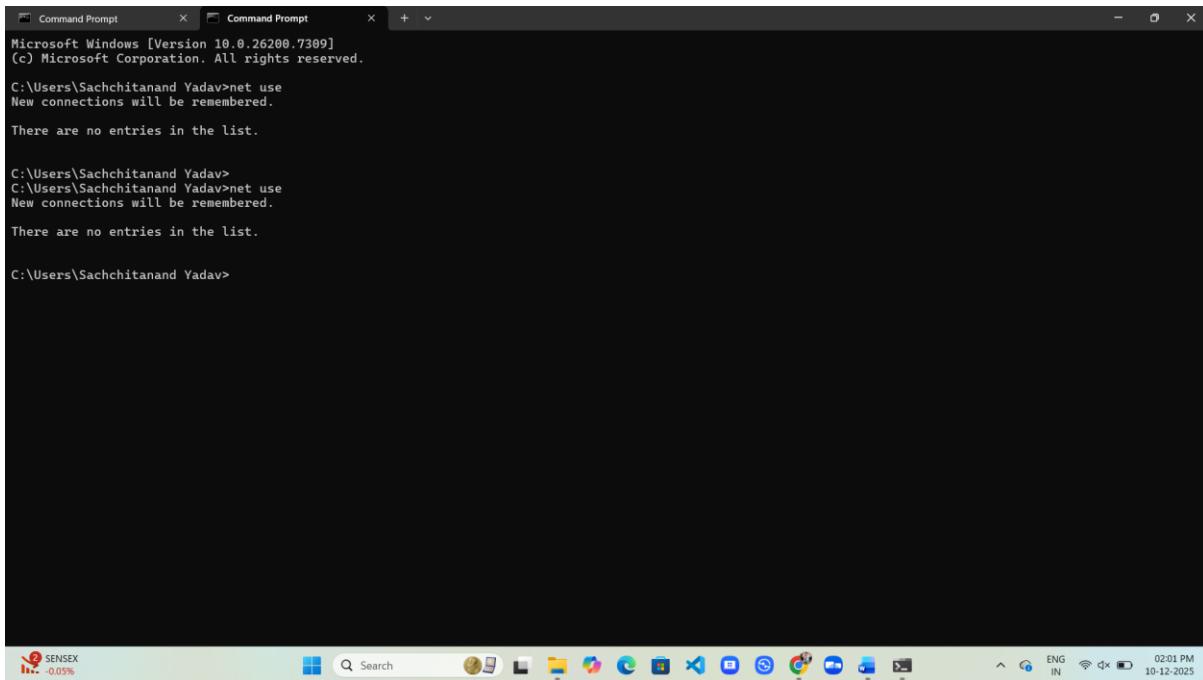
Local Area Connection* 1:
Node IpAddress: [0.0.0.0] Scope Id: []
    No names in cache

Local Area Connection* 10:
Node IpAddress: [0.0.0.0] Scope Id: []
    No names in cache

C:\Users\Sachchitanand Yadav>
```

MODULE - 4 ENUMERATION

3. Now, run net use command. The output displays information about the target such as connection status, shared folder/drive and network information, as shown in the screenshot.



```
Microsoft Windows [Version 10.0.26200.7309]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Sachchitanand Yadav>net use
New connections will be remembered.

There are no entries in the list.

C:\Users\Sachchitanand Yadav>net use
New connections will be remembered.

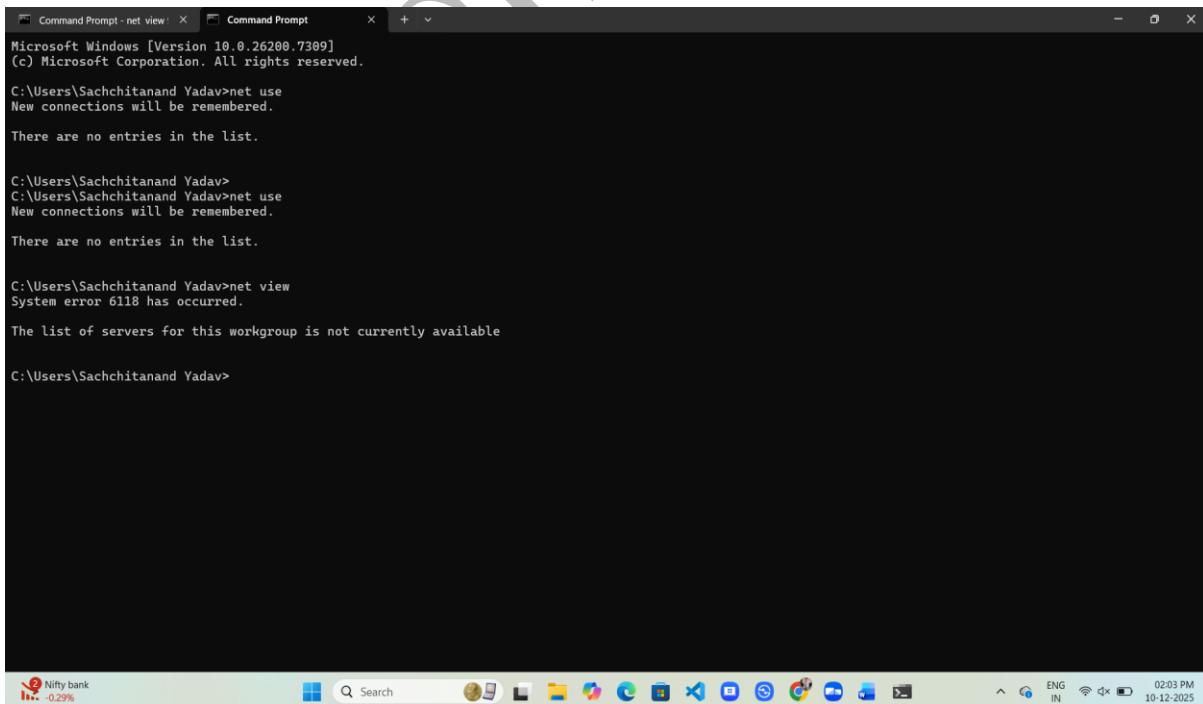
There are no entries in the list.

C:\Users\Sachchitanand Yadav>
```

4. View all computers in the network:

net view

→ Lists available systems in the target domain/workgroup.



```
Microsoft Windows [Version 10.0.26200.7309]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Sachchitanand Yadav>net use
New connections will be remembered.

There are no entries in the list.

C:\Users\Sachchitanand Yadav>net view
System error 6118 has occurred.

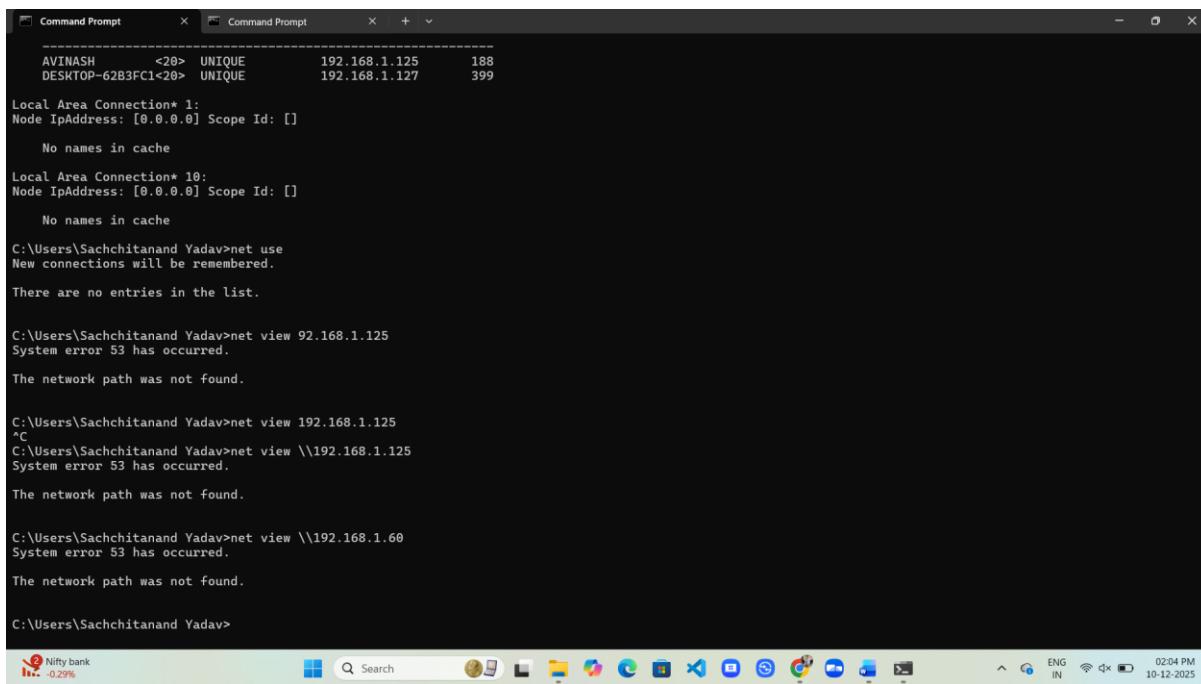
The list of servers for this workgroup is not currently available

C:\Users\Sachchitanand Yadav>
```

5. View shared resources on a target system:

net view \\<target-IP>

→ Displays shared folders and printers.



The screenshot shows a Windows Command Prompt window with two tabs open. The left tab displays network connection information for 'Local Area Connection* 1' and 'Local Area Connection* 10'. The right tab shows the output of the 'net use' command, which lists 'New connections will be remembered.' and 'There are no entries in the list.' When the user runs 'net view 92.168.1.125', it returns 'System error 53 has occurred.' and 'The network path was not found.' Subsequent attempts to view shares on '192.168.1.125' and '192.168.1.60' also result in the same error message. The taskbar at the bottom shows various pinned icons and the date/time as 10-12-2025.

```
AVINASH <20> UNIQUE 192.168.1.125 188  
DESKTOP-62B3FC1<20> UNIQUE 192.168.1.127 399  
  
Local Area Connection* 1:  
Node IpAddress: [0.0.0.0] Scope Id: []  
No names in cache  
  
Local Area Connection* 10:  
Node IpAddress: [0.0.0.0] Scope Id: []  
No names in cache  
  
C:\Users\Sachchitanand Yadav>net use  
New connections will be remembered.  
There are no entries in the list.  
  
C:\Users\Sachchitanand Yadav>net view 92.168.1.125  
System error 53 has occurred.  
The network path was not found.  
  
C:\Users\Sachchitanand Yadav>net view 192.168.1.125  
"C"  
C:\Users\Sachchitanand Yadav>net view \\192.168.1.125  
System error 53 has occurred.  
The network path was not found.  
  
C:\Users\Sachchitanand Yadav>net view \\192.168.1.60  
System error 53 has occurred.  
The network path was not found.  
  
C:\Users\Sachchitanand Yadav>
```

Perform SNMP Enumeration

SNMP Enumeration

SNMP enumeration is the process of gathering detailed information from network devices using the Simple Network Management Protocol. It helps identify users, devices, ARP tables, routing paths, and system-level details that can guide deeper penetration testing.

Lab Scenario (SNMP Enumeration)

As an ethical hacker, you use SNMP to gather details about network devices such as routers, switches, and servers. SNMP enumeration helps you extract system info, users, ARP tables, routing data, and device statistics, which are then used to analyze vulnerabilities and plan further attacks.

Lab Objective

Perform SNMP enumeration using **nmap** to extract device information from the target system.

Perform SNMP Enumeration using nmap

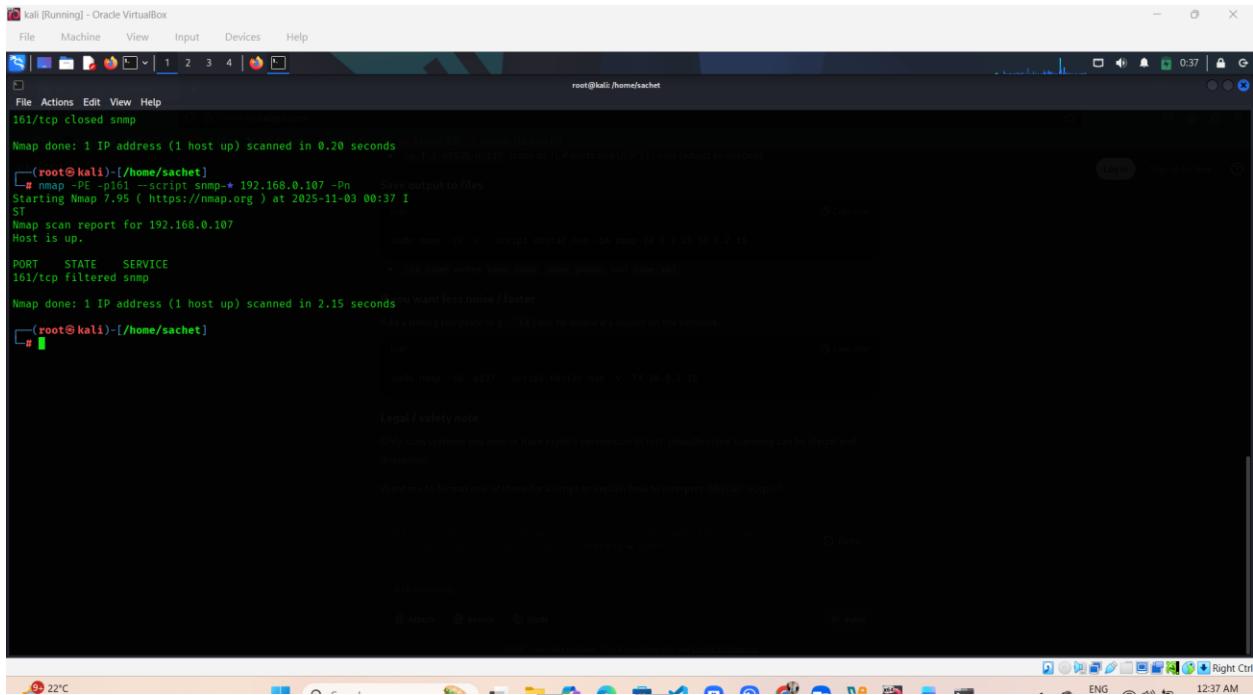
Go to nmap scripts Directory using command

- cd /usr/share/nmap/scripts

MODULE - 4 ENUMERATION

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

Command - Nmap -PE -p161 --script snmp-* 192.168.0.107 -Pn



```
kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali:~/home/sachet
161/tcp closed snmp
Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
# nmap -PE -p161 --script snmp-* 192.168.0.107 -Pn
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-03 00:37 I
Nmap scan report for 192.168.0.107
Host is up.
PORT      STATE      SERVICE
161/tcp    filtered   snmp
Nmap done: 1 IP address (1 host up) scanned in 2.15 seconds
#
```

Perform LDAP Enumeration

Overview

LDAP enumeration is the process of extracting detailed directory information from systems that use the Lightweight Directory Access Protocol. It helps reveal the internal structure of an organization by pulling data from its directory services — the digital version of a company's org chart.

You're basically uncovering how the network is arranged and who's part of it: users, groups, departments, servers, and more.

Lab Scenario

Once SNMP enumeration is completed, the next logical move for an ethical hacker or penetration tester is LDAP enumeration. Most modern enterprises still rely on **Active Directory** or similar directory services to maintain structured information about their network resources.

These directory services store everything neatly — users, computers, printers, groups, email details — in a hierarchical layout. LDAP enumeration taps into this structure to gather:

- Usernames and login information
- Email addresses
- Organizational units (OUs)
- Group memberships
- Departmental information
- Server/domain details

It's like walking through the quiet hallways of a company's internal operations, noticing how everything is arranged without making too much noise.

Lab Objective

Perform LDAP enumeration using Nmap

MODULE - 4 ENUMERATION

namp is a command that lets you visually connect to an LDAP directory and explore its structure.

Showing open ports and services -

This command performs a **fast, detailed TCP connect scan** on the target, showing open ports and services without trying to be stealthy.

Command:

```
nmap -v -sT -T4 192.168.1.33
```

Use / Meaning:

-v → Verbose.

Shows extra details so you're not scanning blind.

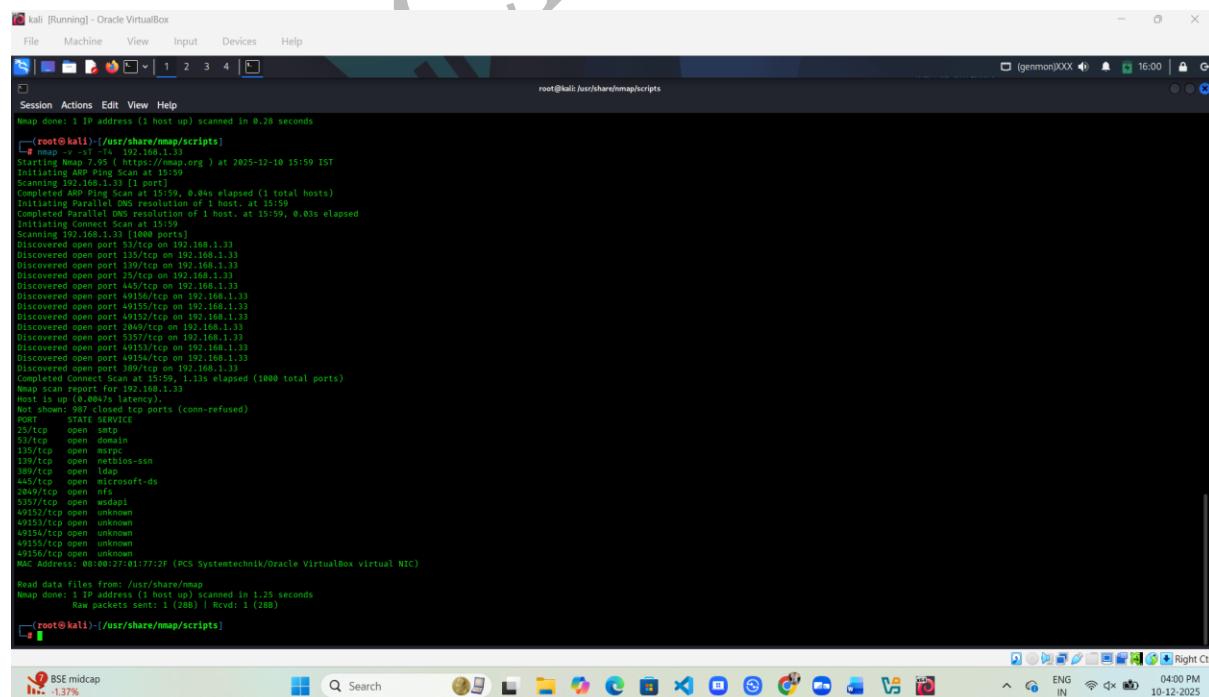
-sT → TCP Connect Scan.

The classic, “by-the-book” full TCP handshake scan. Reliable, but not sneaky.

-T4 → Speed it up.

Aggressive timing — faster scan but makes more noise on the network.

192.168.1.33 → Target IP.



```
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
[...]
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-10 15:59 IST
Initiating ARP Ping Scan at 15:59
Scanning 192.168.1.33 [1 port]
Completed ARP Ping Scan at 15:59 (1 total hosts)
Initiating Parallel DNS resolution of 1 host at 15:59
Completed Parallel DNS resolution of 1 host at 15:59, 0.03s elapsed
Initiating Connect Scan at 15:59
Completed Connect Scan at 15:59 (1000 total ports)
Scanning 192.168.1.33 [1000 ports]
Discovered open port 53/tcp on 192.168.1.33
Discovered open port 135/tcp on 192.168.1.33
Discovered open port 49156/tcp on 192.168.1.33
Discovered open port 49157/tcp on 192.168.1.33
Discovered open port 49158/tcp on 192.168.1.33
Discovered open port 49159/tcp on 192.168.1.33
Discovered open port 49160/tcp on 192.168.1.33
Discovered open port 49161/tcp on 192.168.1.33
Discovered open port 49162/tcp on 192.168.1.33
Discovered open port 49163/tcp on 192.168.1.33
Discovered open port 49164/tcp on 192.168.1.33
Discovered open port 49165/tcp on 192.168.1.33
Discovered open port 49166/tcp on 192.168.1.33
Discovered open port 49167/tcp on 192.168.1.33
Discovered open port 49168/tcp on 192.168.1.33
Discovered open port 49169/tcp on 192.168.1.33
Discovered open port 49170/tcp on 192.168.1.33
Discovered open port 49171/tcp on 192.168.1.33
Discovered open port 49172/tcp on 192.168.1.33
Discovered open port 49173/tcp on 192.168.1.33
Discovered open port 49174/tcp on 192.168.1.33
Discovered open port 49175/tcp on 192.168.1.33
Discovered open port 49176/tcp on 192.168.1.33
Discovered open port 49177/tcp on 192.168.1.33
Discovered open port 49178/tcp on 192.168.1.33
Discovered open port 49179/tcp on 192.168.1.33
Discovered open port 49180/tcp on 192.168.1.33
Discovered open port 49181/tcp on 192.168.1.33
Discovered open port 49182/tcp on 192.168.1.33
Discovered open port 49183/tcp on 192.168.1.33
Discovered open port 49184/tcp on 192.168.1.33
Discovered open port 49185/tcp on 192.168.1.33
Discovered open port 49186/tcp on 192.168.1.33
Discovered open port 49187/tcp on 192.168.1.33
Discovered open port 49188/tcp on 192.168.1.33
Discovered open port 49189/tcp on 192.168.1.33
Discovered open port 49190/tcp on 192.168.1.33
Discovered open port 49191/tcp on 192.168.1.33
Discovered open port 49192/tcp on 192.168.1.33
Discovered open port 49193/tcp on 192.168.1.33
Discovered open port 49194/tcp on 192.168.1.33
Discovered open port 49195/tcp on 192.168.1.33
Discovered open port 49196/tcp on 192.168.1.33
Discovered open port 49197/tcp on 192.168.1.33
Discovered open port 49198/tcp on 192.168.1.33
Discovered open port 49199/tcp on 192.168.1.33
Discovered open port 49200/tcp on 192.168.1.33
Completed Connect Scan at 15:59, 1.13s elapsed (1000 total ports)
Nmap done: 1 IP address (1 host up) scanned in 1.13s
Host is up (0.0007s latency)
Not shown: 987 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
22/tcp    open  ssh
53/tcp    open  domain
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
49156/tcp open  ldap
445/tcp   open  microsoft-ds
2049/tcp  open  nfs
323/tcp   open  smb
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 08:00:27:01:77:2F (PC5 Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.25 seconds
Raw packets sent: 1 (28B) | Rcvd: 1 (28B)
[...]
```

Command :-

```
nmap -v -p 389 --script ldap-* 192.168.1.33
```

```
(root㉿kali:[/usr/share/nmap/scripts])
└─# nmap -v -p 389 --script ldap-* 192.168.1.33
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-10 16:14 IST
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:14
Completed NSE at 16:14, 0.00s elapsed
NSE: Script Post-scanning.
Initiating NSE at 16:14
Completed NSE at 16:14, 0.00s elapsed
Failed to resolve "ldap-novell-getpass.nse".
Failed to resolve "ldap-nisse.nse".
Failed to resolve "ldap-search.nse".
Initiating ARP Ping Scan at 16:14
Scanning 192.168.1.33 [1 port]
Completed ARP Ping Scan at 16:14, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:14
Completed Parallel DNS resolution of 1 host. at 16:14, 0.04s elapsed
Initiating SYN Stealth Scan at 16:14
Scanning 192.168.1.33 [1 port]
Discovered open port 389/tcp on 192.168.1.33
Completed SYN Stealth Scan at 16:14, 0.03s elapsed (1 total ports)
NSE: Script scanning 192.168.1.33.
Initiating NSE at 16:14
Completed NSE at 16:14, 8.01s elapsed
Nmap scan report for 192.168.1.33
Host is up (0.00093s latency).

PORT      STATE SERVICE
389/tcp    open  ldap
MAC Address: 08:00:27:01:77:2F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

NSE: Script Post-scanning.
Initiating NSE at 16:14
Completed NSE at 16:14, 0.00s elapsed
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 8.69 seconds
  Raw packets sent: 2 (72B) | Rcvd: 2 (72B)

(root㉿kali:[/usr/share/nmap/scripts])
└─#
```

Conclusion

LDAP enumeration is a crucial step in understanding how a network organizes its resources. By using Nmap, you can access a structured view of users, groups, and system components. This information lays the groundwork for deeper penetration testing steps and helps identify potential weaknesses in the network's identity and access management setup.

Perform NFS Enumeration

Overview

NFS enumeration is used to identify **exported directories** and **shared data** on a target system. It reveals what folders are shared, who can access them, and how the NFS service is configured.

Lab Scenario

After LDAP enumeration, the next step is checking the NFS service. Many systems use NFS for file sharing, and misconfigurations can expose:

- Exported directories
- Connected clients
- Client IP addresses
- Access permissions

With this information, an attacker could spoof a trusted IP and access shared files.

Lab Objective

Perform NFS enumeration using Nmap to identify exported directories and analyze access permissions on the target server.

Scan for NFS Service (Port 2049)

Command - nmap -v -p 2049 --script nfs-* 192.168.1.33

```

kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
nfs-ls.nse nfs-showmount.nse nfs-statsfs.nse
[root@Kali ~]# [usr/share/nmap/scripts]
# nmap -v -p 2049 --script nfs-* 192.168.1.33
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-10 16:18 IST
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:18
Completed NSE at 16:18, 0.00s elapsed
Failed to resolve "nfs-showmount.nse".
Failed to resolve "nfs-statsfs.nse".
Initiating ARP Ping Scan at 16:18
Scanning 192.168.1.33 [1 port]
Completed ARP Ping Scan at 16:18, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:18
Completed Parallel DNS resolution of 1 host. at 16:18, 0.003s elapsed
Initiating SYN Stealth Scan at 16:18
Scanning 192.168.1.33 [1 port]
Discovered open port 2049/tcp on 192.168.1.33
Completed SYN Stealth Scan at 16:18, 0.003s elapsed (1 total ports)
NSE: Script scanning 192.168.1.33.
Initiating NSE at 16:18
Completed NSE at 16:18, 0.00s elapsed
Nmap scan report for 192.168.1.33
Host is up (0.002s latency).

PORT      STATE SERVICE
2049/tcp  open  nfs
MAC Address: 08:00:27:01:77:2F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

NSE: Script Post-scanning.
Initiating NSE at 16:18
Completed NSE at 16:18, 0.00s elapsed
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
Raw packets sent: 2 (72B) | Rcvd: 2 (72B)

[root@Kali ~]# 

```

Conclusion

NFS enumeration using Nmap helps uncover exported directories and the permissions tied to them. It's one of those timeless techniques — simple, effective, and often overlooked by administrators. The insights gathered can reveal misconfigurations that lead to unauthorized access or data exposure.

Perform DNS Enumeration

Overview

DNS enumeration is the process of discovering **all publicly available DNS records** for a target domain. Think of DNS as the phonebook of the internet — and you’re flipping through every page to see who’s listed, where they live, and what names they go by.

This technique exposes hostnames, IP addresses, subdomains, mail servers, and sometimes even usernames. It’s one of those classic enumeration steps that never goes out of style.

Lab Scenario

After completing NFS enumeration, the next task in a penetration-testing workflow is DNS enumeration. Most organizations rely heavily on DNS to keep their networks functional, and misconfigured DNS servers can unintentionally reveal a treasure chest of information.

During DNS enumeration, you can gather:

- DNS server names
- Hostnames and machine names
- IP addresses associated with hosts
- Usernames embedded in DNS records

If the target’s DNS server is loose with its configurations, it might even allow zone transfers — basically handing you its entire internal map. Not smart, but it happens more than you’d think.

Lab Objective

Perform DNS enumeration using Nmap to extract DNS records and identify valuable information associated with the target domain.

Nmap provides DNS-focused NSE scripts that automate record collection and check for zone transfer weaknesses.

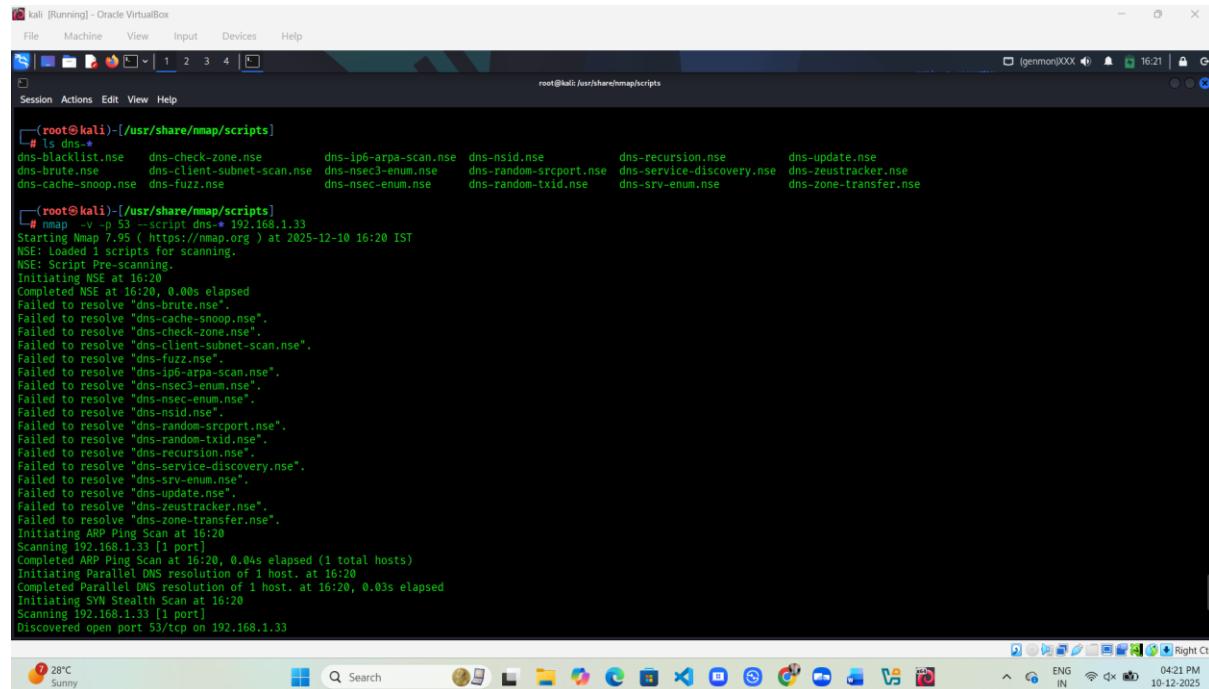
Using Nmap for DNS Enumeration

ls dns-*

Shows all files in the current directory whose names start with dns-.

MODULE - 4 ENUMERATION

Command: - nmap -v -p 53 --script dns-* 192.168.1.33



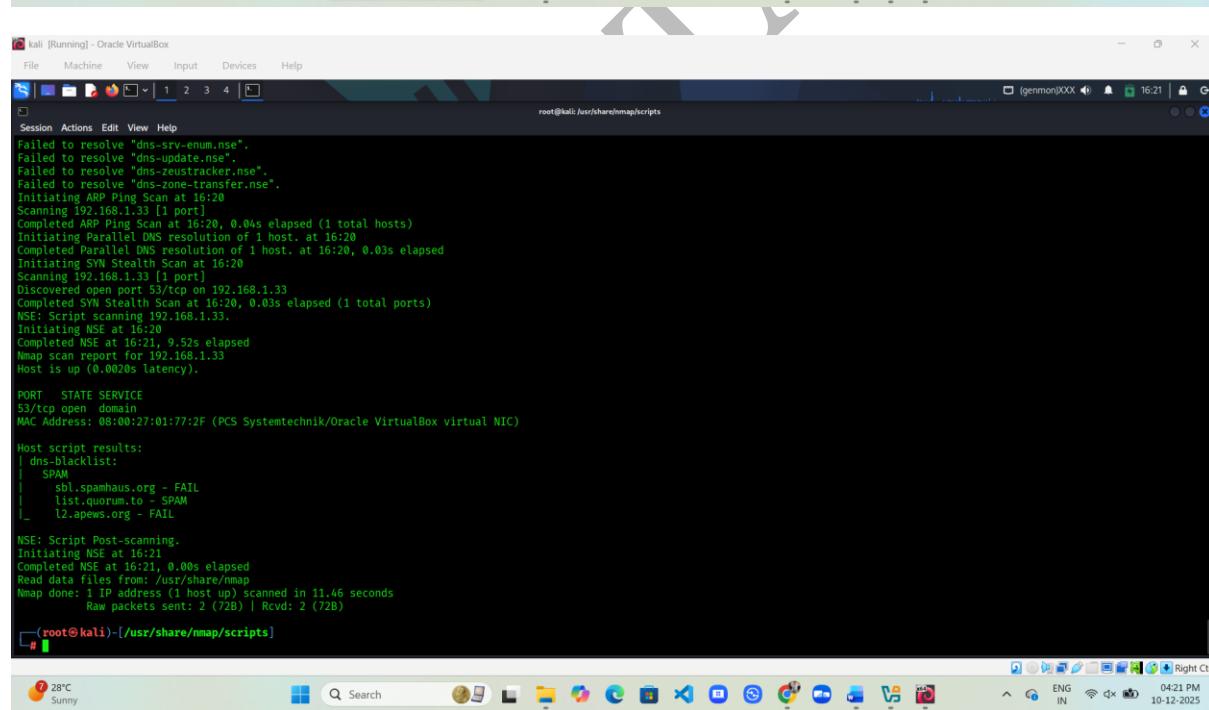
```
# ls dns-*
dns-blacklist.nse  dns-check-zone.nse  dns-ip6-arpascan.nse  dns-nsid.nse  dns-recursion.nse  dns-update.nse
dns-brute.nse       dns-client-subnet-scan.nse  dns-nsec3-enum.nse  dns-random-srcport.nse  dns-service-discovery.nse  dns-zeustracker.nse
dns-cache-snoop.nse  dns-fuzz.nse      dns-nsec3-enum.nse  dns-random-txid.nse  dns-srv-enum.nse  dns-zone-transfer.nse

# nmap -v -p 53 --script dns-* 192.168.1.33
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-10 16:20 IST
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:20
Completed NSE at 16:20, 0.00s elapsed
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-arpascan.nse".
Failed to resolve "dns-nsec3-enum.nse".
Failed to resolve "dns-nsec-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".
Initiating ARP Ping Scan at 16:20
Scanning 192.168.1.33 [1 port]
Completed ARP Ping Scan at 16:20, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:20
Completed Parallel DNS resolution of 1 host. at 16:20, 0.03s elapsed
Initiating SYN Stealth Scan at 16:20
Scanning 192.168.1.33 [1 port]
Discovered open port 53/tcp on 192.168.1.33
Discovering open port 53/tcp on 192.168.1.33
Completed SYN Stealth Scan at 16:20, 0.03s elapsed (1 total ports)
NSE: Script scanning 192.168.1.33.
Initiating NSE at 16:20
Completed NSE at 16:21, 9.52s elapsed
Nmap scan report for 192.168.1.33
Host is up (0.0020s latency).

PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 08:00:27:01:77:2F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Host script results:
| dns-blacklist:
|_  SPAM
|_  SRS.spamhaus.org = FAIL
|_  list.quotum.to = SPAM
|_  I2.apnews.org = FAIL

NSE: Script Post-scanning.
Initiating NSE at 16:21
Completed NSE at 16:21, 0.00s elapsed
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 11.46 seconds
Raw packets sent: 2 (72B) | Rcvd: 2 (72B)
```



```
#
```

Conclusion: -

DNS enumeration with Nmap reveals key DNS records and host details, helping you understand the target's network structure. If DNS is misconfigured, it can leak valuable information that aids further reconnaissance.

Perform SMTP Enumeration

Overview

SMTP enumeration is used to identify **valid user accounts** on a mail server. By interacting with the SMTP service, you can verify which usernames actually exist, spot valid email addresses, and understand how the server handles mail delivery. It's a classic move in the ethical hacking playbook — old technique, still effective, still exposing weak spots.

SMTP servers often respond differently when you test usernames, and those tiny differences are exactly what you harvest.

Lab Scenario

In a penetration testing workflow, once you've explored the basic network footprint, the next logical step is to check the SMTP service for weak spots. Many organizations still rely on traditional mail servers, and these servers can leak user information if not configured properly.

With SMTP enumeration, you can gather:

- Valid usernames
- Delivery addresses
- Email recipients
- How the server responds to various SMTP commands (VRFY, EXPN, RCPT TO)

This intel becomes the foundation for future attacks like password guessing, social engineering prep, or targeted phishing simulations.

Lab Objective

Perform SMTP enumeration using Nmap to identify which users exist on the target SMTP server.

Nmap has a set of NSE (Nmap Scripting Engine) scripts designed exactly for this task. These scripts interact with the mail server and try to validate user accounts using standard SMTP commands.

Using Nmap for SMTP Enumeration

1. Check if SMTP is running.
 2. Use Nmap SMTP enumeration scripts

ls smtp-*

Shows all files in the current directory whose names start with smtp-.

Command - nmap -v -p 25 --script smtp-* 192.168.1.33

```
kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@kali:~# nmap -p 25 --script smtp-* 192.168.1.33
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-10 16:07 IST
NSE: Loaded 1 script for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:07
Completed NSE at 16:07, 0.00s elapsed.
Failed to resolve "smtp-commands.nse".
Failed to resolve "smtp-enum-users.nse".
Failed to resolve "smtp-enum-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-cve2011-1728.nse".
Failed to resolve "smtp-vuln-cve2011-1764.nse".
Initiating ARP Ping Scan at 16:07
Scanning 192.168.1.33 [1 port]
Completed ARP Ping Scan at 16:07, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:07
Completed Parallel DNS resolution of 1 host. at 16:07, 0.04s elapsed
Initiating SYN Stealth Scan at 16:07
Scanning 192.168.1.33 [1 port]
Discovering open port 25/tcp 192.168.1.33
Completed SYN Stealth Scan at 16:07, 0.02s elapsed (1 total ports)
NSE: Script Scanning 192.168.1.33.
Initiating NSE at 16:07
Completed NSE at 16:07, 8.01s elapsed
Nmap scan report for 192.168.1.33
Host is up (0.0016s latency).

PORT      STATE SERVICE
25/tcp    open  smtp
MAC Address: 08:00:27:01:77:2F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

root@kali:~# Watchlist Ideas
File Machine View Input Devices Help
root@kali:~# ENG IN 04:28 10-12-2025
```

MODULE - 4 ENUMERATION

The screenshot shows a terminal window titled "kali [Running] - Oracle VirtualBox" running on a Kali Linux system. The command entered was "nmap -v -p 389 --script ldap-* 192.168.1.33". The output indicates that NSE (Nmap Script Engine) is performing various SMTP-related scans, including "smtp-commands.nse", "smtp-enum-users.nse", and "smtp-vuln-cve2010-4344.nse". It also performs a SYN Stealth Scan and an ARP Ping Scan. The results show an open TCP port 25 at 192.168.1.33, which is identified as the SMTP service. The Nmap scan report concludes that the host is up with 0.0016s latency.

```
NSE: Script Pre-scanning.
Initiating NSE at 16:07
Completed NSE at 16:07, 0.00s elapsed
Failed to resolve "smtp-commands.nse".
Failed to resolve "smtp-enum-users.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".
Initiating ARP Ping Scan at 16:07
Scanning 192.168.1.33 [1 port]
Completed ARP Ping Scan at 16:07, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:07
Completed Parallel DNS resolution of 1 host. at 16:07, 0.04s elapsed
Initiating SYN Stealth Scan at 16:07
Scanning 192.168.1.33 [1 port]
Discovered open port 25/tcp on 192.168.1.33
Completed SYN Stealth Scan at 16:07, 0.02s elapsed (1 total ports)
NSE: Script Post-scanning.
Initiating NSE at 16:07
Completed NSE at 16:07, 0.00s elapsed
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 9.10 seconds
Raw packets sent: 2 (72B) | Rcvd: 2 (72B)

[root@kali] ~[us/share/nmap/scripts]
# nmap -v -p 389 --script ldap-* 192.168.1.33
```

Conclusion

SMTP enumeration using Nmap helps uncover **valid user accounts** on a mail server by testing how it responds to specific SMTP commands. This information can expose weak configurations and guide further security assessments. It's one of those timeless techniques: reliable, straightforward, and essential for understanding a target's email infrastructure.

Perform MSRPC Enumeration

Overview

MSRPC enumeration gathers information from Windows systems through RPC services running on port 135. These services can reveal users, groups, shares, and system details.

Lab Scenario

As the next step after DNS enumeration, MSRPC enumeration helps identify exposed RPC services and system information on Windows targets.

Lab Objective

Perform MSRPC enumeration using Nmap.

Command Used: -

ls msrpc-*

Shows all files in the current directory whose names start with msrpc-*.

Command: -

```
nmap -v -p 135 --script msrpc-* 192.168.1.33
```

Use

This command performs a **verbose scan on port 135** of the target and runs all Nmap scripts starting with **msrpc-** to enumerate **Microsoft RPC services** on the system.

MODULE - 4 ENUMERATION

```
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:39
Completed NSE at 16:39, 0.00s elapsed
Initiating ARP Ping Scan at 16:39
Scanning 192.168.1.33 [1 port]
Completed ARP Ping Scan at 16:39, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:39
Completed Parallel DNS resolution of 1 host. at 16:39, 0.03s elapsed
Initiating SYN Stealth Scan at 16:39
Scanning 192.168.1.33 [1 port]
Discovered open port 135/tcp on 192.168.1.33
Completed SYN Stealth Scan at 16:39, 0.02s elapsed (1 total ports)
NSE: Script scanning 192.168.1.33.
Initiating NSE at 16:39
Completed NSE at 16:39, 0.00s elapsed
Nmap scan report for 192.168.1.33
Host is up (0.0043s latency).

PORT      STATE SERVICE
135/tcp    open  msrpc
MAC Address: 08:00:27:01:77:2F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

NSE: Script Post-scanning.
Initiating NSE at 16:39
Completed NSE at 16:39, 0.00s elapsed
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
Raw packets sent: 2 (72B) | Rcvd: 2 (72B)

[root@kali]:~[~/usr/share/nmap/scripts]
#
[root@kali]:~[~/usr/share/nmap/scripts]
# ls msrpc-
msrpc-enum.nse
[root@kali]:~[~/usr/share/nmap/scripts]
#
[root@kali]:~[~/usr/share/nmap/scripts]
```

```
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.32 seconds
Raw packets sent: 1 (28B) | Rcvd: 1 (28B)

[root@kali]:~[~/usr/share/nmap/scripts]
# nmap -v -p 135 --script msrpc-* 192.168.1.33
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-10 16:39 IST
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:39
Completed NSE at 16:39, 0.00s elapsed
Initiating ARP Ping Scan at 16:39
Scanning 192.168.1.33 [1 port]
Completed ARP Ping Scan at 16:39, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:39
Completed Parallel DNS resolution of 1 host. at 16:39, 0.03s elapsed
Initiating SYN Stealth Scan at 16:39
Scanning 192.168.1.33 [1 port]
Discovered open port 135/tcp on 192.168.1.33
Completed SYN Stealth Scan at 16:39, 0.02s elapsed (1 total ports)
NSE: Script scanning 192.168.1.33.
Initiating NSE at 16:39
Completed NSE at 16:39, 0.00s elapsed
Nmap scan report for 192.168.1.33
Host is up (0.0043s latency).

PORT      STATE SERVICE
135/tcp    open  msrpc
MAC Address: 08:00:27:01:77:2F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

NSE: Script Post-scanning.
Initiating NSE at 16:39
Completed NSE at 16:39, 0.00s elapsed
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
Raw packets sent: 2 (72B) | Rcvd: 2 (72B)

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

Conclusion

MSRPC enumeration with Nmap reveals RPC services and key Windows system information, helping assess security weaknesses.

Perform SMB Enumeration

SMB Enumeration means collecting info from a target's SMB service to find shared folders, users, security settings, and potential entry points.

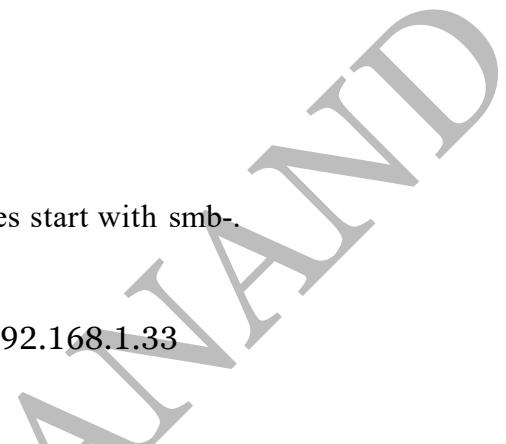
1. Nmap SMB Enumeration

```
nmap -v -p 139,445 --script smb-* <target>
```

ls smb-*

Shows all files in the current directory whose names start with smb-.

Command - nmap -v -p 139 --script smb-* 192.168.1.33



```

kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
Host is up (0.0033s latency).
Not shown: 987 closed tcp ports (conn-refused)
PORT      STATE SERVICE
25/tcp    open  smtp
53/tcp    open  domain
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
2049/tcp  open  nfs
5357/tcp  open  wsddapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 08:00:27:01:77:3F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.37 seconds
  Raw packets sent: 1 (28B) | Rcvd: 1 (28B)

[root@kali]~[~/usr/share/nmap/scripts]
# ls netbios-ssn/*
ls: cannot access 'netbios-ssn-*': No such file or directory
#
[root@kali]~[~/usr/share/nmap/scripts]
# 
[root@kali]~[~/usr/share/nmap/scripts]
# ls smb-*
smb-brute.nse          smb-enum-services.nse    smb-ls.nse           smb-psexec.nse      smb-vuln-cve2009-3103.nse  smb-vuln-ms10-054.nse  smb-webexec-exploit.nse
smb-double-pulsar-backdoor.nse  smb-enum-sessions.nse  smb-mbenum.nse       smb-psexec-mode.nse  smb-vuln-cve-2017-7494.nse  smb-vuln-ms10-061.nse
smb-enum-domains.nse    smb-enum-shares.nse     smb-os-discovery.nse  smb-server-stats.nse  smb-vuln-ms06-025.nse    smb-vuln-ms17-010.nse
smb-enum-groups.nse     smb-enum-users.nse      smb-print-text.nse   smb-system-info.nse   smb-vuln-ms07-029.nse    smb-vuln-regsvc-dos.nse
smb-enum-processes.nse  smb-flood.nse          smb-protocols.nse   smb-vuln-conficker.nse  smb-vuln-ms08-067.nse    smb-vuln-webexec.nse

[root@kali]~[~/usr/share/nmap/scripts]
# 

```

MODULE - 4 ENUMERATION

```
# nmap -v -p 139 --script smb-* 192.168.1.33
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-10 16:44 IST
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:44
Completed NSE at 16:44; 0.00s elapsed
Failed to resolve "smb-double-pulsar-backdoor.nse".
Failed to resolve "smb-enum-domains.nse".
Failed to resolve "smb-enum-groups.nse".
Failed to resolve "smb-enum-processes.nse".
Failed to resolve "smb-enum-services.nse".
Failed to resolve "smb-enum-sessions.nse".
Failed to resolve "smb-enum-shares.nse".
Failed to resolve "smb-enum-users.nse".
Failed to resolve "smb-flood.nse".
Failed to resolve "smb-ls.nse".
Failed to resolve "smb-mbenum.nse".
Failed to resolve "smb-os-discovery.nse".
Failed to resolve "smb-print-text.nse".
Failed to resolve "smb-protocols.nse".
Failed to resolve "smb-psexec.nse".
Failed to resolve "smb-security-code.nse".
Failed to resolve "smb-system-privileges.nse".
Failed to resolve "smb-system-info.nse".
Failed to resolve "smb-vuln-conficker.nse".
Failed to resolve "smb-vuln-cve2009-3103.nse".
Failed to resolve "smb-vuln-cve-2017-7494.nse".
Failed to resolve "smb-vuln-ms06-025.nse".
Failed to resolve "smb-vuln-ms07-029.nse".
Failed to resolve "smb-vuln-ms08-067.nse".
Failed to resolve "smb-vuln-ms10-054.nse".
Failed to resolve "smb-vuln-ms10-061.nse".
Failed to resolve "smb-vuln-ms17-010.nse".
Failed to resolve "smb-vuln-regsvc-dos.nse".
Failed to resolve "smb-vuln-webexec.nse".
Failed to resolve "smb-webexec-exploit.nse".
Initiating ARP Ping Scan at 16:44
Scanning 192.168.1.33 [1 port]
Completed ARP Ping Scan at 16:44, 0.04s elapsed (1 total hosts)
```

```
Failed to resolve "smb-vuln-ms10-054.nse".
Failed to resolve "smb-vuln-ms10-061.nse".
Failed to resolve "smb-vuln-ms17-010.nse".
Failed to resolve "smb-vuln-regsvc-dos.nse".
Failed to resolve "smb-vuln-webexec.nse".
Failed to resolve "smb-webexec-exploit.nse".
Initiating ARP Ping Scan at 16:44
Scanning 192.168.1.33 [1 port]
Completed ARP Ping Scan at 16:44, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:44
Completed Parallel DNS resolution of 1 host. at 16:44, 0.03s elapsed
Initiating SYN Stealth Scan at 16:44
Scanning 192.168.1.33 [1 port]
Discovered open port 139/tcp on 192.168.1.33
Completed SYN Stealth Scan at 16:44, 0.02s elapsed (1 total ports)
NSE: Script scanning 192.168.1.33.
Initiating NSE at 16:47
Completed NSE at 16:47, 44.52s elapsed
Nmap scan report for 192.168.1.33
Host is up (0.0022s latency).

PORT      STATE SERVICE
139/tcp    open  netbios-ssn
MAC Address: 08:00:27:01:77:2F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Host script results:
| smb-brute:
|_ administrator:<blank> => Valid credentials, account disabled
|_ guest:<blank> => Valid credentials, account disabled

NSE: Script Post-scanning.
Initiating NSE at 16:47
Completed NSE at 16:47, 0.00s elapsed
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 145.07 seconds
    Raw packets sent: 2 (72B) | Rcvd: 2 (72B)

[root@kali ~]#
```

MODULE - 4 ENUMERATION

Command - nmap -v -p 445 --script smb-* 192.168.1.33

```
kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
Raw packets sent: 2 (72B) | Rcvd: 2 (72B)
[root@kali]-[/usr/share/nmap/scripts]
# nmap -v -p 445 --script smb-* 192.168.1.33
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-10 16:49 IST
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:49
Completed NSE at 16:49
0.00s elapsed
Failed to resolve "smb-double-pulsar-backdoor.nse".
Failed to resolve "smb-enum-domains.nse".
Failed to resolve "smb-enum-groups.nse".
Failed to resolve "smb-enum-processes.nse".
Failed to resolve "smb-enum-services.nse".
Failed to resolve "smb-enum-sessions.nse".
Failed to resolve "smb-enum-shares.nse".
Failed to resolve "smb-enum-users.nse".
Failed to resolve "smb-flood.nse".
Failed to resolve "smb-ls.nse".
Failed to resolve "smb-mbenum.nse".
Failed to resolve "smb-os-discovery.nse".
Failed to resolve "smb-print-text.nse".
Failed to resolve "smb-protocols.nse".
Failed to resolve "smb-psexec.nse".
Failed to resolve "smb-security-mode.nse".
Failed to resolve "smb-serverinfo.nse".
Failed to resolve "smb-symlink-info.nse".
Failed to resolve "smb-vuln-conficker.nse".
Failed to resolve "smb-vuln-cve2009-3103.nse".
Failed to resolve "smb-vuln-cve-2017-7494.nse".
Failed to resolve "smb-vuln-ms06-025.nse".
Failed to resolve "smb-vuln-ms07-029.nse".
Failed to resolve "smb-vuln-ms08-067.nse".
Failed to resolve "smb-vuln-ms10-054.nse".
Failed to resolve "smb-vuln-ms10-061.nse".
Failed to resolve "smb-vuln-ms17-010.nse".
Failed to resolve "smb-vuln-regsvc-dos.nse".
Failed to resolve "smb-vuln-webexec.nse".
Failed to resolve "smb-webexec-exploit.nse".
[root@kali]-[/usr/share/nmap/scripts]
# 28C
Sunny
Search
ENG IN
04:51 PM
10-12-2025
Right Ctrl
```

```
kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
root@kali:/usr/share/nmap/scripts
root@kali:/usr/share/nmap/scripts
Failed to resolve "smb-vuln-ms10-054.nse".
Failed to resolve "smb-vuln-ms10-061.nse".
Failed to resolve "smb-vuln-ms17-010.nse".
Failed to resolve "smb-vuln-regsvc-dos.nse".
Failed to resolve "smb-vuln-webexec.nse".
Failed to resolve "smb-webexec-exploit.nse".
Initiating ARP Ping Scan at 16:49
Scanning 192.168.1.33 [1 port]
Completed ARP Ping Scan at 16:49, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:49
Completed Parallel DNS resolution of 1 host. at 16:49, 0.02s elapsed
Initiating SYN Stealth Scan at 16:49
Scanning 192.168.1.33 [1 port]
DNS resolution took 0.0005s on 192.168.1.33
Completed SYN Stealth Scan at 16:49, 0.03s elapsed (1 total ports)
NSE: Script scanning 192.168.1.33.
Initiating NSE at 16:49
Completed NSE at 16:52, 133.28s elapsed
Nmap scan report for 192.168.1.33
Host is up (0.00086s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds
MAC Address: 08:00:27:01:77:2F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Host script results:
| smb-brute:
|   administrator:<blank> => Valid credentials, account disabled
|_ guest:<blank> => Valid credentials, account disabled

NSE: Script Post-scanning.
Initiating NSE at 16:52
Completed NSE at 16:52, 0.00s elapsed
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 138.65 seconds
Raw packets sent: 2 (72B) | Rcvd: 2 (72B)

[root@kali]-[/usr/share/nmap/scripts]
# 28C
Sunny
Search
ENG IN
04:52 PM
10-12-2025
Right Ctrl
```

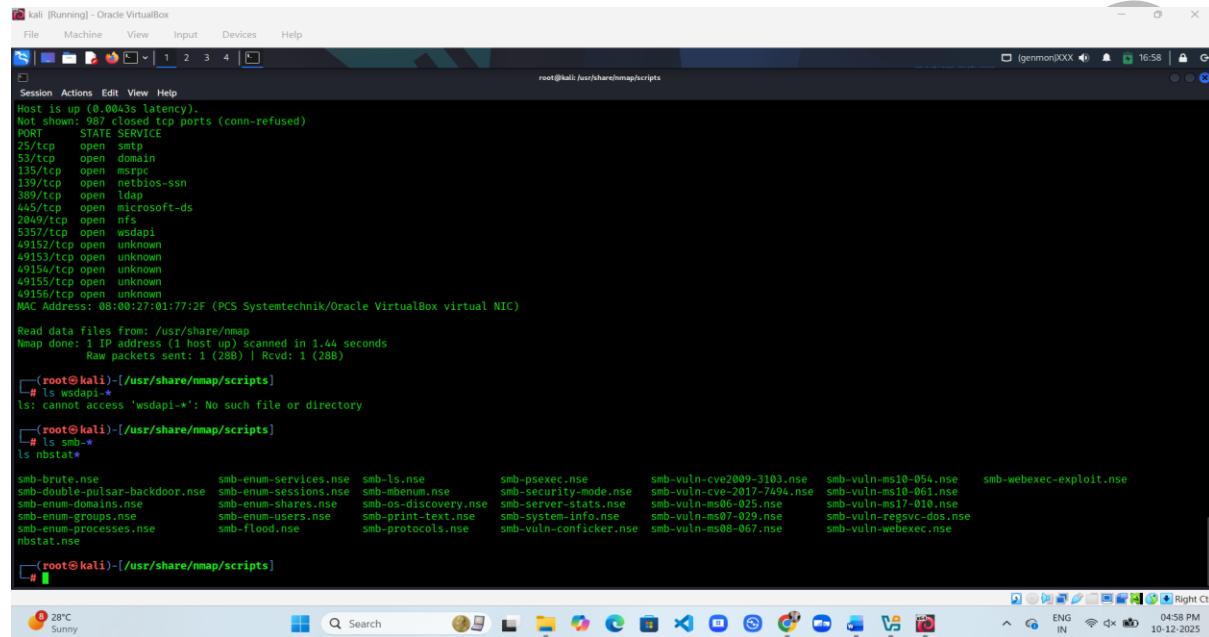
MODULE - 4 ENUMERATION

Use:

This command checks NetBIOS info and lists SMB shared folders on the target system. It helps identify available network shares, host details, and possible access points.

ls smb-* ,ls nbstat-*

Shows all files in the current directory whose names start with smb-, ls nbstat-*.



```
kali [Running] - OracleVirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
Host is up (0.0043s latency).
Not shown: 987 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
2049/tcp  open  nmb
5357/tcp  open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 08:00:27:01:77:2F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.44 seconds
Raw packets sent: 1 (28B) | Rcvd: 1 (28B)

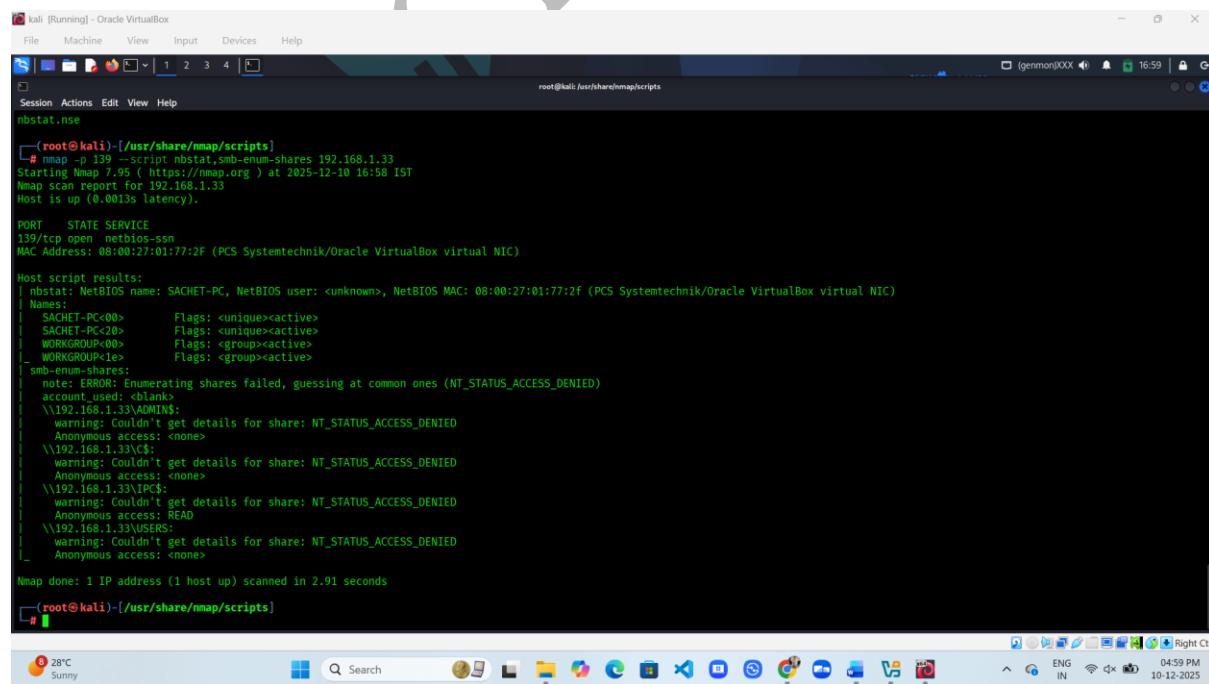
[root@kali]~[~/usr/share/nmap/scripts]
# ls wsdapi/*
ls: cannot access 'wsdapi-*': No such file or directory

[root@kali]~[~/usr/share/nmap/scripts]
# ls smb-*
ls nbstat*

smb-brute.nse          smb-enum-services.nse      smb-ls.nse           smb-psexec.nse      smb-vuln-cve2009-3103.nse  smb-vuln-ms10-054.nse      smb-webexec-exploit.nse
smb-brute-pulsar-backdoor.nse  smb-enum-sessions.nse  smb-mbenum.nse       smb-security-mode.nse  smb-vuln-cve-2017-7494.nse  smb-vuln-ms10-061.nse
smb-enum-domains.nse     smb-enum-shares.nse       smb-os-discovery.nse  smb-server-stats.nse   smb-vuln-ms06-025.nse      smb-vuln-ms17-010.nse
smb-enum-groups.nse      smb-enum-users.nse        smb-print-text.nse   smb-system-info.nse   smb-vuln-ms07-029.nse      smb-vuln-regsvc-dos.nse
smb-enum-processes.nse   smb-flood.nse            smb-protocols.nse   smb-vuln-conficker.nse  smb-vuln-ms08-067.nse      smb-vuln-webexec.nse
hostlist.nse

[root@kali]~[~/usr/share/nmap/scripts]
# 
```

Command - nmap -p 139 --script nbstat,smb-enum-shares <target-IP>



```
kali [Running] - OracleVirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
nbstat.nse

[root@kali]~[~/usr/share/nmap/scripts]
# nmap -p 139 --script nbstat,smb-enum-shares 192.168.1.33
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-10 16:58 IST
Nmap scan report for 192.168.1.33
Host is up (0.0013s latency).

PORT      STATE SERVICE
139/tcp   open  netbios-ssn
MAC Address: 08:00:27:01:77:2F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Host script results:
| nbstat: NetBIOS name: SACHET-PC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:01:77:2F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
|_ Names:
|   | SACHET-PC<0>  Flags: <unique><active>
|   | SACHET-PC<2>  Flags: <unique><active>
|   | WORKGROUP<0>  Flags: <group><active>
|   | WORKGROUP<2>  Flags: <group><active>
|   | Smb-enum-shares:
|   |_ Script ERROR: Enumerating shares failed, guessing at common ones (NT_STATUS_ACCESS_DENIED)
|   account_used: <blank>
|   \\\192.168.1.33\ADMIN$:
|       warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|       Anonymous access: <none>
|   \\\192.168.1.33\$: 
|       warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|       Anonymous access: <none>
|   \\\192.168.1.33\IPC$:
|       warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|       Anonymous access: READ
|   \\\192.168.1.33\USERS:
|       warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|       Anonymous access: <none>

Nmap done: 1 IP address (1 host up) scanned in 2.91 seconds

[root@kali]~[~/usr/share/nmap/scripts]
# 
```

Perform Enumeration using AI

AI-powered tools make the enumeration phase faster and more precise. Instead of manually checking each service, AI helps analyze network data, suggest commands, and highlight weak points.

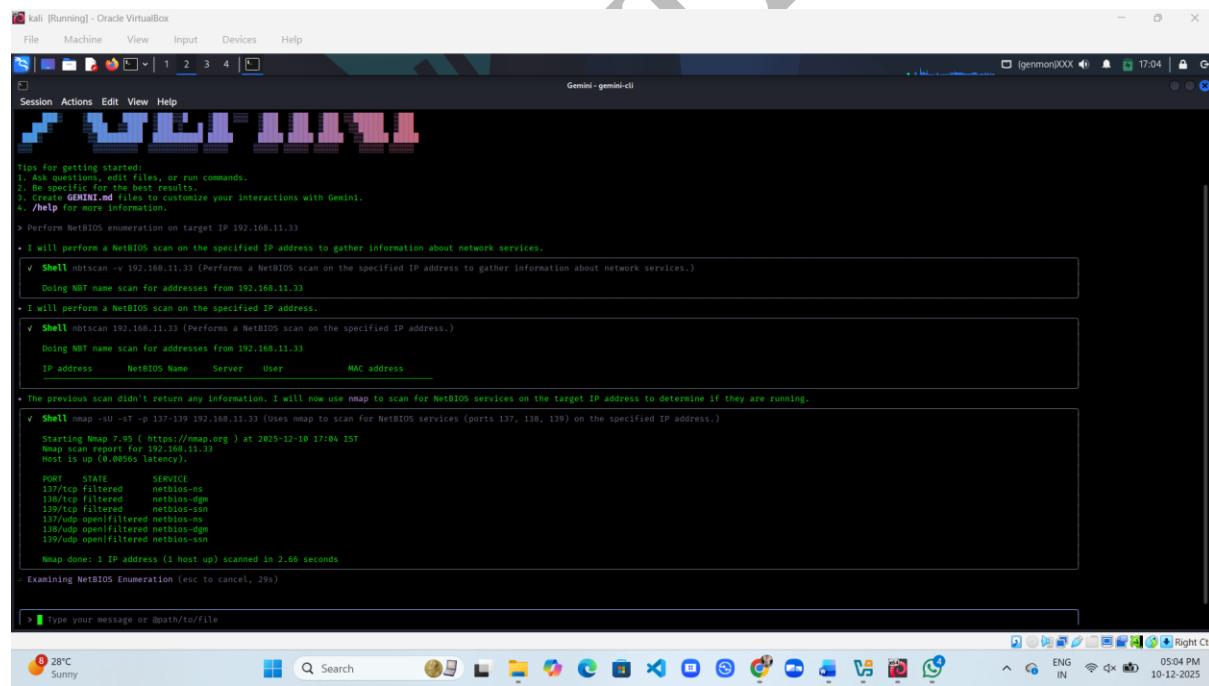
Lab Scenario

In this task, you use AI-assisted tools to gather detailed info about the target network. The aim is to uncover resources, services, and potential vulnerabilities with higher efficiency.

Lab Objective

- Perform enumeration using **Gemini-CLI**.

Prompt - Perform NetBIOS enumeration on target IP <ip>



```

kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
Gemini - gemini-cli
Gemini - gemini-cli
Tips for getting started:
1. Ask questions, edit files, or run commands.
2. Use the arrow keys to scroll.
3. Create GEMINI.md files to customize your interactions with Gemini.
4. /help for more information.

> Perform NetBIOS enumeration on target IP 192.168.11.33
* I will perform a NetBIOS scan on the specified IP address to gather information about network services.
  ✓ Shell nbtscan -v 192.168.11.33 (Performs a NetBIOS scan on the specified IP address to gather information about network services.)
    Doing NBT name scan for addresses from 192.168.11.33
* I will perform a NetBIOS scan on the specified IP address.
  ✓ Shell nbtscan 192.168.11.33 (Performs a NetBIOS scan on the specified IP address.)
    Doing NBT name scan for addresses from 192.168.11.33
    IP address      NetBIOS Name      Server      User      MAC address
    192.168.11.33  KALI-LAB-PC-01  KALI-LAB-PC-01  KALI-LAB-PC-01  08:00:27:00:00:00

* The previous scan didn't return any information. I will now use nmap to scan for NetBIOS services on the target IP address to determine if they are running.
  ✓ Shell nmap -sU -sT -p 137-139 192.168.11.33 (Uses nmap to scan for NetBIOS services (ports 137, 138, 139) on the specified IP address.)
    Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-10 17:04 IST
    Nmap scan report for 192.168.11.33
    Host is up (0.0006s latency).
    PORT      STATE      SERVICE
    137/tcp    filtered  netbios-ns
    138/tcp    filtered  netbios-dgm
    139/tcp    filtered  netbios-ssn
    137/udp   open|filtered netbios-ns
    138/udp   open|filtered netbios-dgm
    139/udp   open|filtered netbios-ssn

    Nmap done: 1 IP address (1 host up) scanned in 2.66 seconds
Examining NetBIOS Enumeration (esc to cancel, 29s)

Type your message or &path/to/file

28°C
Sunny
ENG IN
05:04 PM
10-12-2025
Right Ctrl

```

MODULE - 4 ENUMERATION

Prompt - Get NetBIOS info for IP 192.168.1.33 and display the associated names

```
v kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
Gemini - gemini-cli

v Shell nbiscan 192.168.1.33 (Performs a NetBIOS scan on the specified IP address.)
Doing NBT name scan for addresses from 192.168.1.33
IP address NetBIOS Name Server User MAC address

* The previous scan didn't return any information. I will now use nmap to scan for NetBIOS services on the target IP address to determine if they are running.
v Shell nmap -sU -p 137-139 192.168.1.33 (Uses nmap to scan for NetBIOS services (ports 137, 138, 139) on the specified IP address.)
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-10 17:04 IST
Nmap scan report for 192.168.1.33
Host is up (0.0005s latency).

PORT      STATE      SERVICE
137/tcp    filtered  netbios-ns
138/tcp    filtered  netbios-dgm
139/tcp    filtered  netbios-ssn
137/udp   open|filtered netbios-ns
138/udp   open|filtered netbios-dgm
139/udp   open|filtered netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 2.66 seconds

iRequest cancelled.

> Get NetBIOS info for IP 192.168.1.33 and display the associated names
* I will perform a NetBIOS scan on the specified IP address to gather information about network services and display the associated names.
v Shell nbiscan 192.168.1.33 (Performs a NetBIOS scan on the specified IP address to get the associated names.)
Doing NBT name scan for addresses from 192.168.1.33
IP address NetBIOS Name Server User MAC address

192.168.1.33 SACHET-PC <sachet> <unknown> 00:00:12:71:77:2f

* The NetBIOS name for the IP address 192.168.1.33 is SACHET-PC.

> Type your message or &path/to/file
/usr/lib/gemini-cli                                     no sandbox (see /docs)                                     gemini-2.5-pro (99% context left)
28°C Sunny                                         Search                                          ENG IN 05:07 PM 10-12-2025 Right Ctrl
```

Prompt - Perform SNMP enumeration on target IP 10.10.1.22 using SnmpWalk and display the result here

```
v kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
Gemini - gemini-cli

* The NetBIOS name for the IP address 192.168.1.33 is SACHET-PC.

> Perform SNMP enumeration on target IP 10.10.1.22 using nmap and display the result here
* I will use nmap to perform an SNMP scan on the specified IP address to enumerate SNMP information.
v Shell nmap -sU -p 161 --script=snmp-brute 192.168.1.33 (Performs an SNMP scan using nmap on the specified IP address to enumerate SNMP information.)
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-10 17:09 IST
Nmap scan report for 192.168.1.33
Host is up (0.0007s latency).

PORT      STATE      SERVICE
161/udp  open|filtered  snmp
MAC Address: 00:00:12:71:77:2f (PC Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.76 seconds

* The nmap scan shows that the SNMP port is open, but it did not return detailed information. I will now use snmpwalk, a dedicated SNMP enumeration tool, to get more details.

v Shell snmpwalk -c public -v1 192.168.1.33 (Uses snmpwalk to perform a more detailed SNMP enumeration on the specified IP address.)
Timeout: No Response from 192.168.1.33

* The previous attempts to enumerate SNMP using nmap and snmpwalk with the 'public' community string were unsuccessful. This could be due to an incorrect community string. I will now try to find the correct community string. First, I will try the common community strings 'private' and 'manager' with snmpwalk.

v Shell snmpwalk -c private -v1 192.168.1.33 (Uses snmpwalk with the 'private' community string to enumerate SNMP on the specified IP address.)
Timeout: No Response from 192.168.1.33

* I will now try the 'manager' community string with snmpwalk.

? Shell snmpwalk -c manager -v1 192.168.1.33 (Uses snmpwalk with the 'manager' community string to enumerate SNMP on the specified IP address.) +
snmpwalk -c manager -v1 192.168.1.33
Allow execution of: 'snmpwalk'?

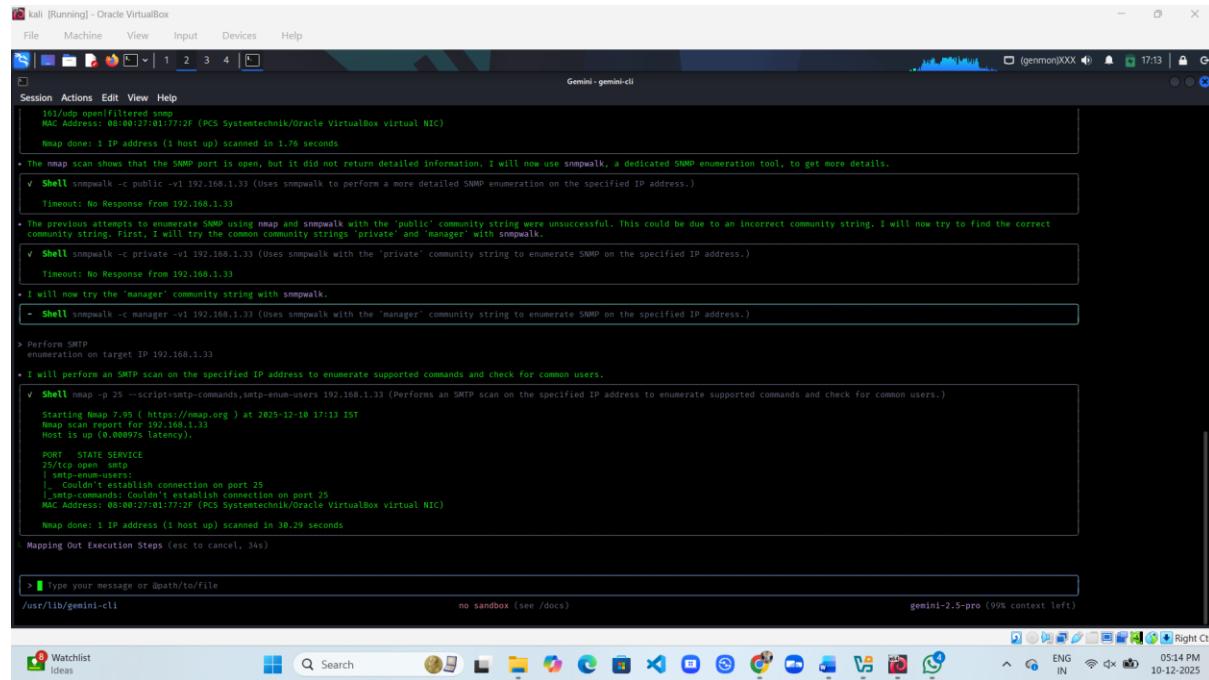
* 1. Yes, allow once
* 2. Yes, allow always?
* 3. No, suggest changes (esc)

Waiting for user confirmation ...

/usr/lib/gemini-cli                                     no sandbox (see /docs)                                     gemini-2.5-pro (99% context left)
Air: Moderate Now                                         Search                                          ENG IN 05:10 PM 10-12-2025 Right Ctrl
```

MODULE - 4 ENUMERATION

Prompt - Perform SMTP enumeration on target IP <ip>



```

kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Gemini - gemini-cli
Session Actions Edit View Help
[!] /usr/bin/nc -l -p 25 -e /bin/sh
MAC Address: 00:0B:27:D1:77:2F (PC Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 1.70 seconds
* The nmap scan shows that the SNMP port is open, but it did not return detailed information. I will now use snmpwalk, a dedicated SNMP enumeration tool, to get more details.
v Shell snmpwalk -c public -v1 192.168.1.33 (Uses snmpwalk to perform a more detailed SNMP enumeration on the specified IP address.)
Timeout: No Response from 192.168.1.33
* The previous attempts to enumerate SNMP using nmap and snmpwalk with the 'public' community string were unsuccessful. This could be due to an incorrect community string. I will now try the common community strings 'private' and 'manager' with snmpwalk.
v Shell snmpwalk -c private -v1 192.168.1.33 (Uses snmpwalk with the 'private' community string to enumerate SNMP on the specified IP address.)
Timeout: No Response from 192.168.1.33
* I will now try the 'manager' community string with snmpwalk.
- Shell snmpwalk -c manager -v1 192.168.1.33 (Uses snmpwalk with the 'manager' community string to enumerate SNMP on the specified IP address.)

> Perform SMTP enumeration on target IP 192.168.1.33
* I will perform an SMTP scan on the specified IP address to enumerate supported commands and check for common users.
v Shell nmap -p 25 --script=smtp-commands,smtp-enum-users 192.168.1.33 (Performs an SMTP scan on the specified IP address to enumerate supported commands and check for common users.)
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-10 17:13 IST
Nmap scan report for 192.168.1.33
Host is up (0.00007s latency).
|_ STATE SERVICE
|_ TCP 25/tcp open
|_ _auto-enum-users:
|   |_ Couldnt establish connection on port 25
|_ _auto-commands: Couldnt establish connection on port 25
MAC Address: 00:0B:27:D1:77:2F (PC Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 30.29 seconds

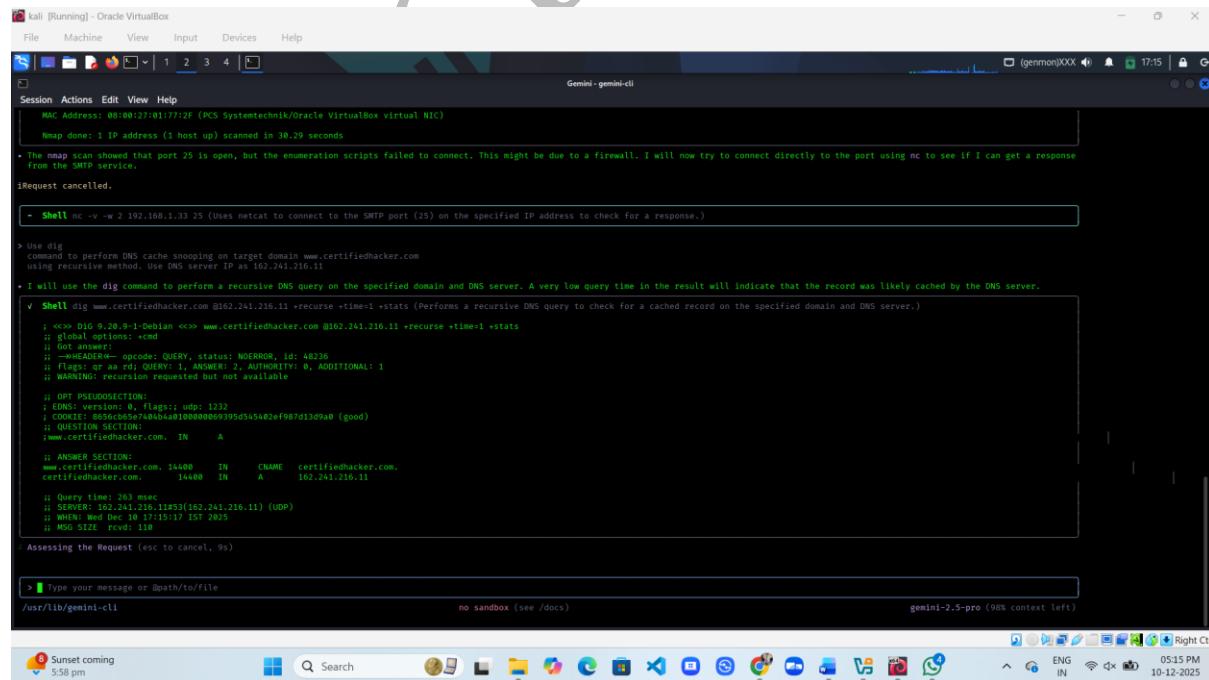
Mapping Out Execution Steps (esc to cancel, 34s)

2 Type your message or @path/to/file
/usr/lib/gemini-cli                                     no sandbox (see /docs)                                     gemini-2.5-pro (99% context left)

```

The screenshot shows a Kali Linux terminal window titled "Gemini - gemini-cli". It displays the results of an nmap scan on port 25, which found the service to be open. The user then runs a script to enumerate supported commands and check for common users. The output shows that the connection to port 25 could not be established, likely due to a firewall. The terminal prompt is at the bottom, ready for the user to type their message or file path.

Prompt - Use dig command to perform DNS cache snooping on target domain www.certifiedhacker.com using recursive method. Use DNS server IP as 162.241.216.11



```

kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Gemini - gemini-cli
Session Actions Edit View Help
[!] /usr/bin/nc -l -p 25 -e /bin/sh
MAC Address: 00:0B:27:D1:77:2F (PC Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 30.29 seconds
* The nmap scan showed that port 25 is open, but the enumeration scripts failed to connect. This might be due to a firewall. I will now try to connect directly to the port using nc to see if I can get a response from the SMTP service.
iRequest cancelled.
- Shell nc -v -w 2 192.168.1.33 25 (Uses netcat to connect to the SMTP port (25) on the specified IP address to check for a response.)

> Use dig command to perform DNS cache snooping on target domain www.certifiedhacker.com using recursive method. Use DNS server IP as 162.241.216.11
* I will use the dig command to perform a recursive DNS query on the specified domain and DNS server. A very low query time in the result will indicate that the record was likely cached by the DNS server.
v Shell dig www.certifiedhacker.com @162.241.216.11 +recurse +time1 +stats (Performs a recursive DNS query to check for a cached record on the specified domain and DNS server.)
; <>> DIG 6 2.20.9-1+Optimal <>> www.certifiedhacker.com @162.241.216.11 +recurse +time1 +stats
;; global options: +cmd
;; Got answer:
;; ANSWER SECTION:
www.certifiedhacker.com. 40800 IN A 162.241.216.11
;; OPT PREFERENCE:
;; EDNS: version 0, Flags: ud 1232
;; COOKIE: 0056cb5e7a0d4a9100000009395d5454b2ef997d13d9a0 (good)
;; QUESTION SECTION:
www.certifiedhacker.com. IN A
;; ANSWER SECTION:
www.certifiedhacker.com. 16400 IN CNAME certifiedhacker.com.
certifiedhacker.com. 16400 IN A 162.241.216.11
;; Query time: 263 msec
;; WHEN: Wed Dec 10 17:15:17 IST 2025
;; MSG SIZE rcvd: 118

Assessing the Request (esc to cancel, 9s)

2 Type your message or @path/to/file
/usr/lib/gemini-cli                                     no sandbox (see /docs)                                     gemini-2.5-pro (98% context left)

```

The screenshot shows a Kali Linux terminal window titled "Gemini - gemini-cli". It displays the results of a dig command to perform DNS cache snooping on the domain www.certifiedhacker.com using a recursive method. The output shows the domain's A record and its CNAME mapping. The terminal prompt is at the bottom, ready for the user to type their message or file path.

Prompt - Use dig command to perform DNS cache snooping on the target domain www.certifiedhacker.com using non-recursive method. Use DNS server IP as 162.241.216.11"

```

kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
Gemini - gemini-cli
[...]
ii SERVER: 162.241.216.11#53(162.241.216.11) (UDP)
ii Query: www.certifiedhacker.com, type: A, class: IN
ii WHEN: Wed Dec 10 17:17:07 IST 2025
ii MSG SIZE rcvd: 110
Based on the output, the DNS cache snooping attempt shows that the record for www.certifiedhacker.com was not cached on the DNS server at 162.241.216.11.
This is indicated by two key points in the result:
1. High Query Time: The query time was 263 msec. A cached record would have resulted in a much lower time (typically under 10ms).
2. Recursion Not Available: The server responded with WARNING: recursion requested but not available, which means it would not perform a recursive lookup for you anyway.

> Use dig command to perform DNS cache snooping on the target domain www.certifiedhacker.com using non-recursive method. Use DNS server IP as 162.241.216.11
I will use the dig command to perform a non-recursive DNS query on the specified domain and DNS server. This will reveal whether the record is cached on that server without asking it to perform a new lookup.

v Shell dig www.certifiedhacker.com @162.241.216.11 +noredirect +stats (Performs a non-recursive DNS query to check for a cached record on the specified domain and DNS server.)
i <>> DIG 9.28.9-1-Optimistic <>> www.certifiedhacker.com @162.241.216.11 +noredirect +stats
ii global options: +read
ii Got answer:
ii =>HEADER=< opcode: QUERY, status: NOERROR, id: 13304
ii Flags: qr aa; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
ii OPT PSEUDOSECTION:
ii ;QUERY SECTION:
i www.certifiedhacker.com. IN A
ii ANSWER SECTION:
www.certifiedhacker.com. 14400 IN CNAME certifiedhacker.com.
certifiedhacker.com. 14400 IN A 162.241.216.11
ii AUTHORITY SECTION:
certifiedhacker.com. 86400 IN NS ns1.bluehost.com.
certifiedhacker.com. 86400 IN NS ns2.bluehost.com.
ii Query time: 267 msec
ii SERVER: 162.241.216.11#53(162.241.216.11) (UDP)
ii WHEN: Wed Dec 10 17:17:07 IST 2025
ii MSG SIZE rcvd: 158
Synthesizing the Solution (esc to cancel, aa)

> Type your message or @path/to/file
/usr/lib/gemini-cli
no sandbox (see /docs)
gemini-2.5-pro (98% context left)
Trending videos The Hunger Ga... Search
ENG IN 05:17 PM 10-12-2025 Right Ctrl

```

Enumeration Countermeasures Explained

1. Disable Unnecessary Services

Every running service is a potential leak. If your system doesn't *need* SNMP, Telnet, or FTP — kill them. Each open service gives away banners, usernames, and version info that make a hacker's day a little too easy.

2. Use Strong Authentication & Access Controls

Don't let anonymous or guest access slide. Disable null sessions and force authentication on SMB, LDAP, SNMP, and RPC. Give users only the privileges they actually need — least privilege isn't just a buzzword, it's survival.

3. Restrict and Monitor Network Ports

Enumeration often relies on open ports like 161 (SNMP), 389 (LDAP), or 445 (SMB). Use firewalls to block or filter these ports, especially from external networks. Monitor logs for unusual requests — those repeated “who's there?” packets aren't friendly pings.

4. Implement Account Lockout Policies

Limit login attempts so attackers can't brute-force their way through username or password guessing. After a few fails, the account should lock temporarily. This frustrates automated tools big time.

5. Harden DNS and Directory Services

Attackers love DNS zone transfers and LDAP dumps. Disable zone transfers to unauthorized hosts and restrict LDAP queries to authenticated users only. A locked-down directory is a quiet directory.

6. Update and Patch Regularly

Old software versions scream “exploit me.” Keep your OS, network devices, and applications updated so enumeration tools can't exploit outdated responses or banners.

7. Disable Default Accounts & Rename Admins

Default usernames like “admin,” “guest,” or “root” are hacker candy.

Rename or disable them, and make sure the real admin accounts are unpredictable.

8. Use Encryption (TLS/SSL)

Encrypt communications for protocols like LDAP (LDAPS), SNMPv3, and HTTPS. That way, even if someone sniffs around, all they’ll see is gibberish.

9. Security Through Obscurity (Smartly Used)

Don’t announce server info in banners or welcome messages. Disable verbose responses that leak OS or software versions. It’s not foolproof, but it removes the low-hanging fruit.

10. Regular Auditing & Pen Testing

Pretend to be your own attacker. Use tools like Nmap, SNMP-check, or ldapsearch internally to see what outsiders could learn — and fix it before they do.

SACHCHITANAND
THANK YOU