# Module 4

# Enumeration

**28.11.25**

**Name : Mugdha Makarand Govilkar**

**Instructor : Satish Singh**

# INDEX

# Concept :

## Enumeration

1. **Enumeration :**
2. **Enumeration is the process of gathering detailed information about a target system.**
3. **It comes after scanning and is the first active phase of ethical hacking.**
4. **The goal is to extract specific, valuable data about the target.**
5. **Attackers connect directly to the target to gather information.**
6. **It helps to identify:**
   - **Users**
   - **Network shares**
   - **Services**
   - **Ports**
   - **Operating systems**
   - **Applications**
7. **Enumeration reveals information that scanning cannot show.**
8. **It often uses protocols like:**
   - **SNMP**
   - **LDAP**
   - **SMB**
   - **DNS**
   - **SMTP**
   - **FTP**
9. **The information collected helps in finding vulnerabilities.It is an important step in penetration testing and red teaming.**

# 1.NetBIOS :

**1 . NetBIOS stands for Network Basic Input Output System.**

**2 . As a ethical hacker our first step in the enumeration of a windows system is to exploit the NetBIOS API.**

**3 . NetBIOS enumeration allows you to collect information about the target such as a list of computers that belong to a target domain,shares on individual hosts in the target network,policies,passwords,etc**

**4 . Windows uses NetBIOS for file and printer sharing.**

**5 . A NetBIOS name is a unique computer name assigned to windows system.**

**6 . NetBIOS enumeration is a process of obtaining sensitive information about the target such as a list of computers belonging to a target domain,network shares,politics,etc.**

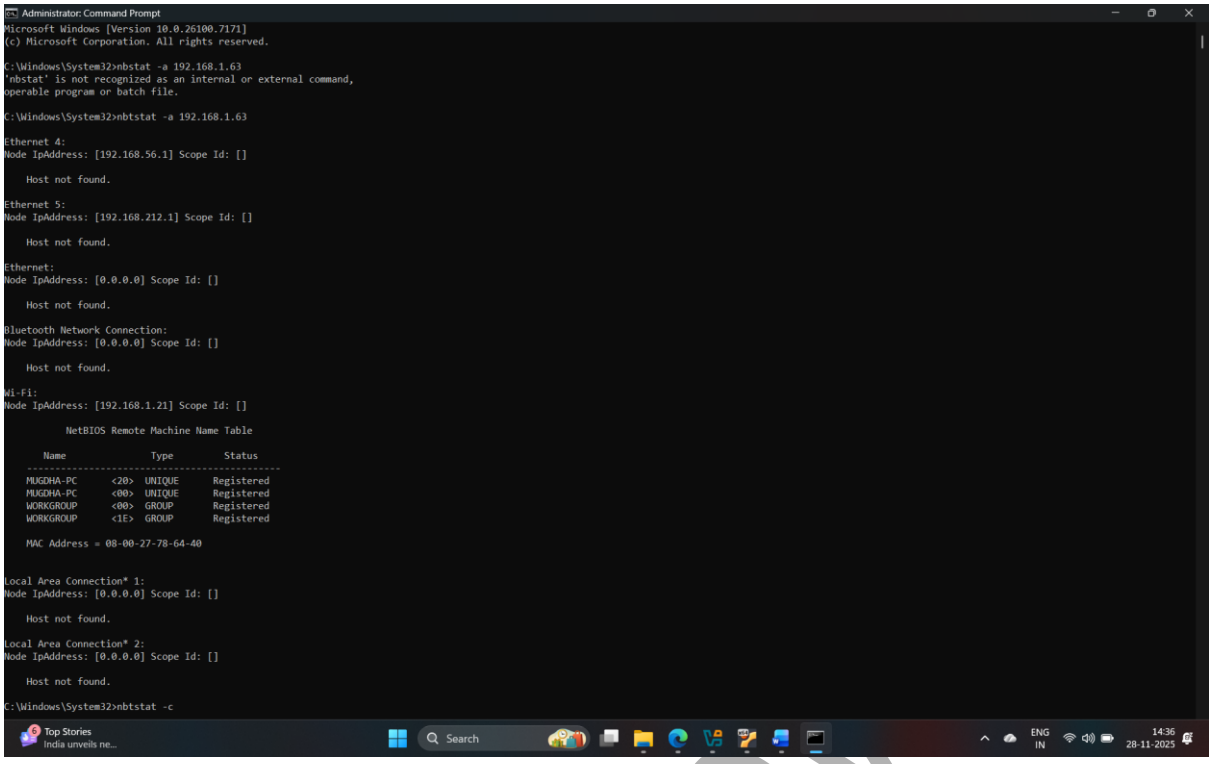
**7 . Steps :**

**1 . nbtstat is a Windows command-line tool used to troubleshoot and gather information about NetBIOS over TCP/IP (NetBT).It displays the information about Computer name,Workgroup/domain name,Logged-in user name,Services running under NetBIOS.**

**2 . here we use nbtstat -a 192.168.1.63 , -a displays the NetBIOS name table of remote computer.**

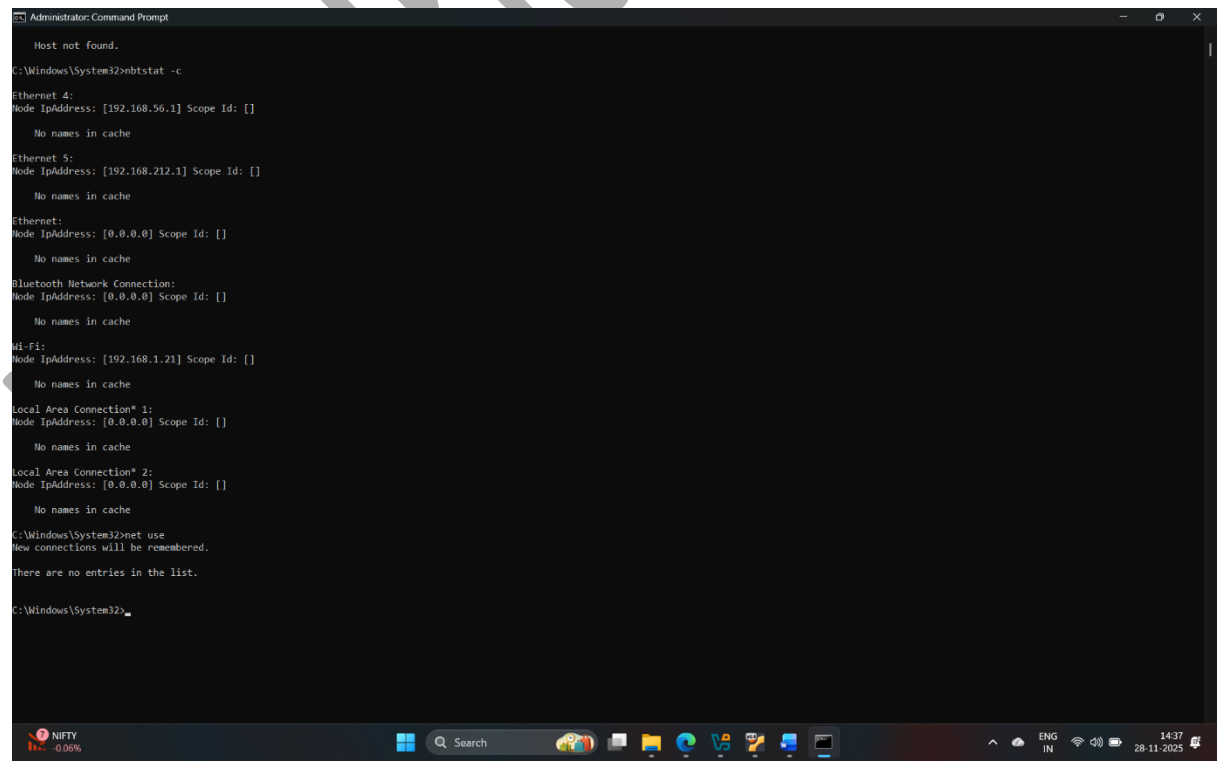
**3 . The result displays the NetBIOS name table of remote computer.**

**4 . In the same command promt run nbtstat -c here, -c lists the content of the NetBIOS name cache of the remote computer.**




**1.1**

**5 . then run net use in the same command promt it displays the information about the target such as connection status,shared folder/drive,and network information.**




**1.2**

# 2 .SNMP :

**1 . SNMP stands for simple network management protocol.**

**2 . As a ethical hacket our next step is to carry out snmp enumeration to extract information about network resources such as host,router,devices and shares and network information such as ARP tables,routing table devices specific information and traffic statistics.**

**3 .Steps :**

**1 . Used snmpwalk but the result is Timeout: No Response from 192.168.1.63 this means SNMP is not enabled or blocked on the target machine.**

**2 . Navigated to Nmap scripts directory cd /usr/share/nmap/scripts To check SNMP-related Nmap NSE scripts.**

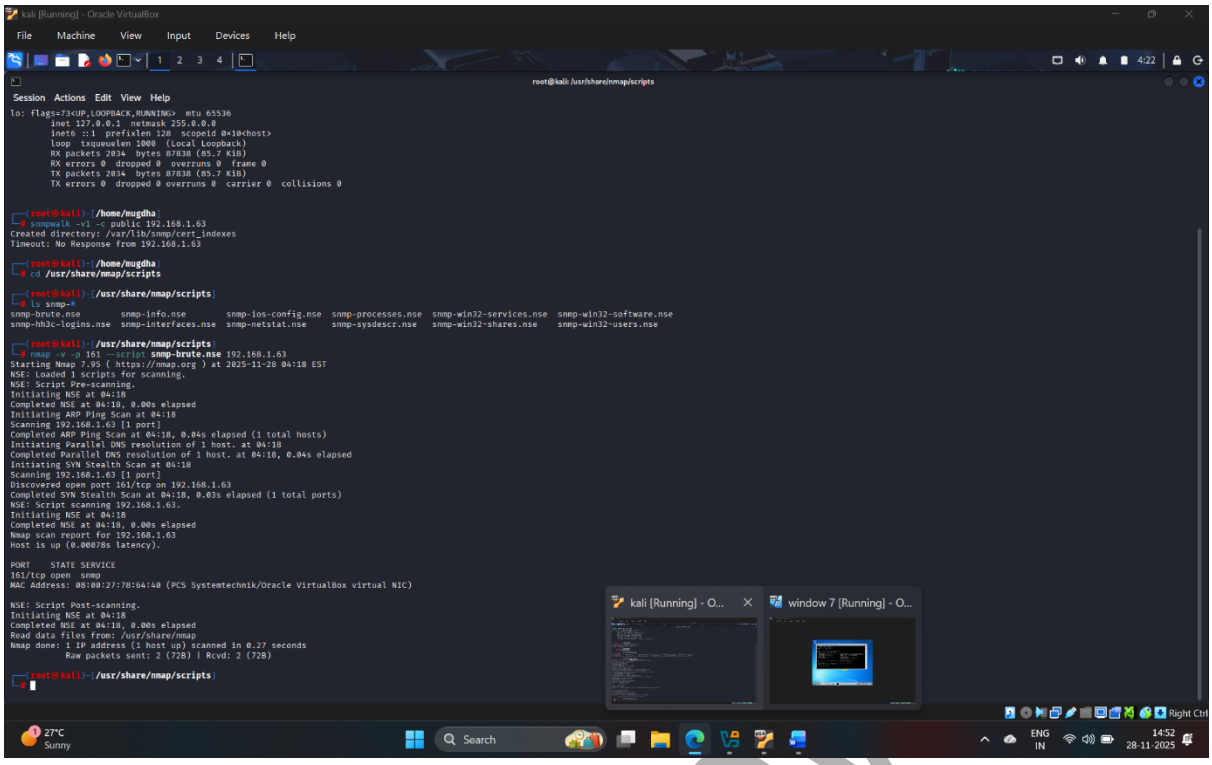
**3 . Listed SNMP scripts: ls snmp* Nmap provides multiple SNMP scripts like:**

- **1 . snmp-brute.nse**
- **2 . snmp-info.nse**
- **3 . snmp-interfaces.nse**
- **4 . snmp-processes.nse**

**4 . Run Nmap SNMP brute-force script nmap -sU -p 161 --script snmp-brute 192.168.1.63**

- **1 . -sU → UDP scan**
- **2 . -p 161 → SNMP port**
- **3 . --script snmp-brute → brute-forces SNMP community strings**
- **4 . 192.168.1.63 → target IP**

**5 . The result is port 161 is unreachable.**


kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@kali: /usr/share/nmap/scripts
Session Actions Edit View Help
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 2034 bytes 87838 (85.7 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 2034 bytes 87838 (85.7 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
┌──(root㉿kali)-[/home/mugdha]
└─# snmpwalk -v1 -c public 192.168.1.63
Created directory: /var/lib/snmp/cert_indexes
Timeout: No Response from 192.168.1.63
┌──(root㉿kali)-[/home/mugdha]
└─# cd /usr/share/nmap/scripts
┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─# ls snmp-*
snmp-brute.nse snmp-info.nse snmp-ios-config.nse snmp-processes.nse snmp-win32-services.nse snmp-win32-software.nse
snmp-hh3c-logins.nse snmp-interfaces.nse snmp-netstat.nse snmp-sysdescr.nse snmp-win32-shares.nse snmp-win32-users.nse
┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─# nmap -v -p 161 --script snmp-brute.nse 192.168.1.63
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-28 04:18 EST
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:18
Completed NSE at 04:18, 0.00s elapsed
Initiating ARP Ping Scan at 04:18
Scanning 192.168.1.63 [1 port]
Completed ARP Ping Scan at 04:18, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:18
Completed Parallel DNS resolution of 1 host. at 04:18, 0.04s elapsed
Initiating SYN Stealth Scan at 04:18
Scanning 192.168.1.63 [1 port]
Discovered open port 161/tcp on 192.168.1.63
Completed SYN Stealth Scan at 04:18, 0.03s elapsed (1 total ports)
NSE: Script scanning 192.168.1.63.
Initiating NSE at 04:18
Completed NSE at 04:18, 0.00s elapsed
Nmap scan report for 192.168.1.63
Host is up (0.00078s latency).
PORT STATE SERVICE
161/tcp open snmp
MAC Address: 08:00:27:78:64:40 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
NSE: Script Post-scanning.
Initiating NSE at 04:18
Completed NSE at 04:18, 0.00s elapsed
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
Raw packets sent: 2 (72B) | Rcvd: 2 (72B)
┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─#
kali [Running] - O...
window 7 [Running] - O...
Right Ctrl
27°C Sunny
Search
ENG IN
14:52 28-11-2025

# 3 .LDAP :

**1 . LDAP stands for Lightweight Directory Access Protocol.**

**2 . LDAP is a protocol used to access and manage directory services.**

**3 . It stores and retrieves information about:Users,Groups,Computers,Printers,Applications.**

**4 . Steps :**

**1 . cd /usr/share/nmap/scripts To access all Nmap NSE scripts related to LDAP for enumeration.**

**2 . ls ldap* This showed NSE scripts such as ldap-rootdse.nse,ldap-search.nse,ldap-num.nse,ldap-brute.nse,ldap-novell-getpass.nse these scripts are used to enumerate LDAP servers.**

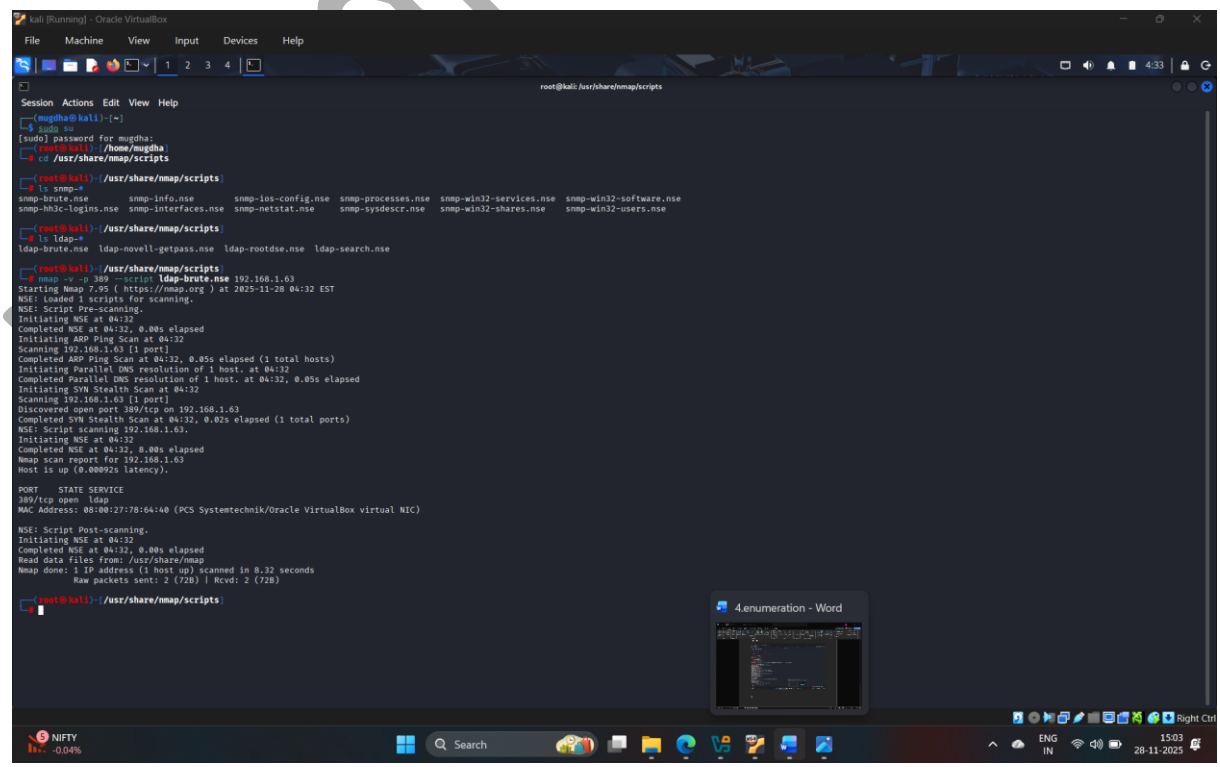
**1 . nmap -p 389 --script ldap-brute 192.168.1.63**

**2 . -p 389 → LDAP default port**

**3 . --script ldap-brute → Tries to brute-force LDAP username/password**

**4 . 192.168.1.63 → Target machine**

**3 . 389/tcp open ldap SCRIPT RESULT: no login credentials found LDAP port is open,Brute-force could not find valid username/password,Target is running LDAP but does not allow anonymous access.**



# 4 .NFS :

**1 . NFS stands for Network File System.**

**2 . It is a protocol used to share files and folders over a network.**

**3 . Developed by Sun Microsystems for Unix/Linux systems.**

**4. It allows a client computer to access files on a remote server as if they were local files.**

**5 . Steps :**

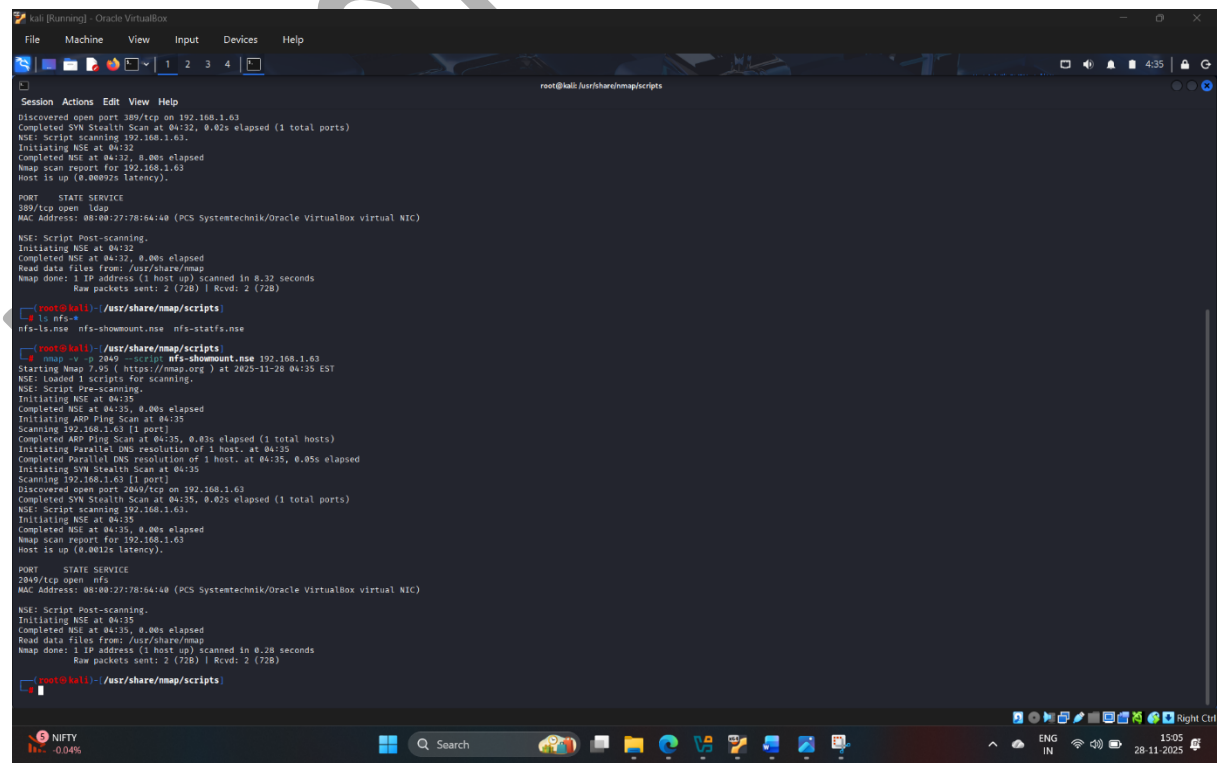
**1 . ls nfs* found scripts such as nfs-ls.nse,nfs-showmount.nse,nfs-statfs.nse.These scripts help enumerate NFS shares on a target.**

**2 . nmap -p 2049 --script=nfs-ls 192.168.1.63**

- **1 . -p 2049 → NFS default port**
- **2 . --script=nfs-ls → Lists files on NFS shares (if share is open)**

**3 . 2049/tcp open nfs but the script output shows no file listing, meaning:**

- **1 . The NFS share is empty**
- **2 . The NFS share is not accessible**
- **3 . Exported directory has no read permission**



# 5 .DNS :

**1 . DNS enumeration is a process that locates and lists all possible DNS records for a target domain,including usernames**
**2 . as a hacker the next step after NFS enumeration is to prform DNS enumeration.this process yields information such as DNS server names,hostnames,machine names,usernames,ip addresses**
**3 . DNS enumeration techniques are used to obtain information about the DNS servers and network infrastructure of the target organization.**

**4 . Steps :**

**1 . /usr/share/nmap/scripts  This folder contains all Nmap NSE scripts.**

**These scripts extend Nmap's functionality (DNS enumeration, brute force, vuln scan, etc.)**

**2 . ls dns-*.nse This displays all scripts starting with dns-.**

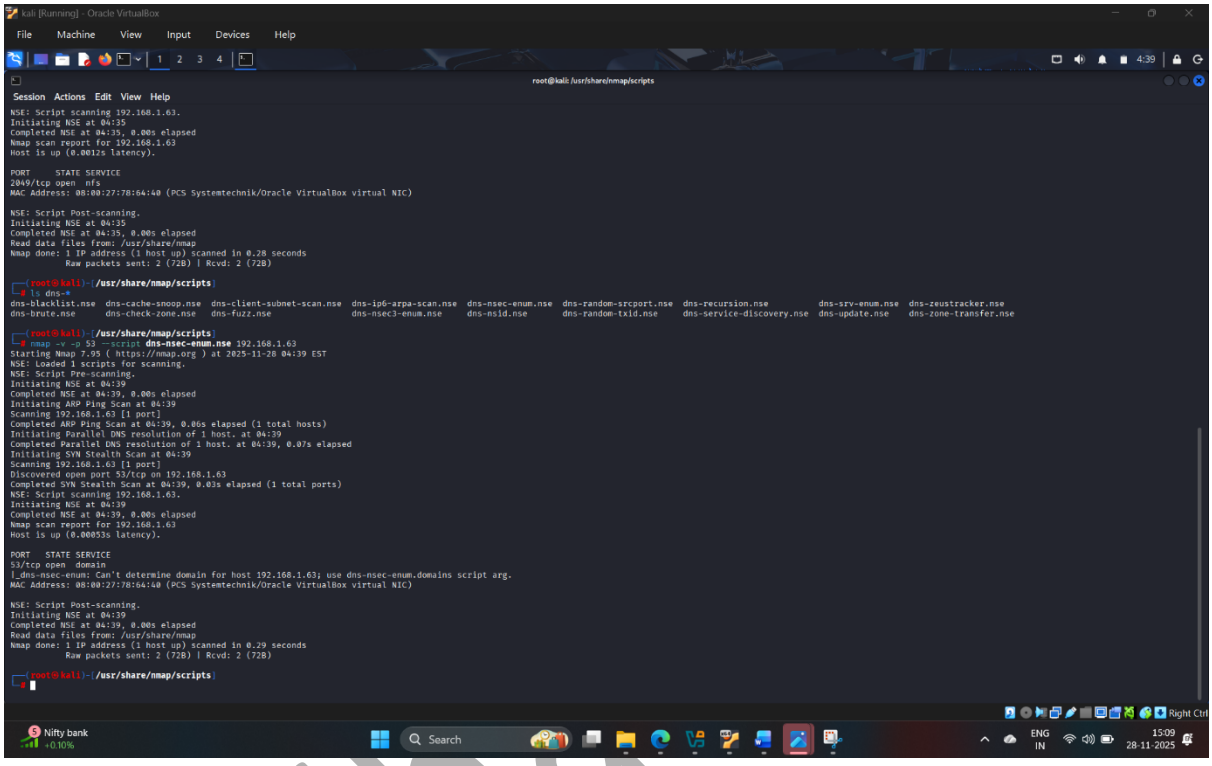
- **1 . dns-brute.nse → brute-force DNS subdomains**
- **2 . dns-check-zone.nse → validates DNS zone**
- **3 . dns-zone-transfer.nse → attempts zone transfer**
- **4 . dns-recursion.nse → checks if recursion is allowed**
- **5 . dns-service-discovery.nse → finds DNS services**
- **6 . dns-nsec-enum.nse → enumerates DNSSEC**
- **7. dns-srv-enum.nse → enumerates SRV records**

**3 . run nmap --script=dns-nsec-enum.nse 192.168.1.63 Nmap tried to do DNSSEC NSEC enumeration.**

**4 . the result is**

- **1 . Scanned in 0.29s**
- **2 . NSE: Script Post-scanning**
- **3 . NSE: dns-nsec-enum.nse did not find any results Target does not support DNSSEC**

**OR NSEC records not configured so no data was returned (normal for most networks)**


kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@kali: /usr/share/nmap/scripts
Session Actions Edit View Help
NSE: Script scanning 192.168.1.63.
Initiating NSE at 04:35
Completed NSE at 04:35, 0.00s elapsed
Nmap scan report for 192.168.1.63
Host is up (0.0012s latency).
PORT STATE SERVICE
2049/tcp open nfs
MAC Address: 08:00:27:78:64:40 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
NSE: Script Post-scanning.
Initiating NSE at 04:35
Completed NSE at 04:35, 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]
# ls dns-*
dns-blacklist.nse dns-cache-snoop.nse dns-client-subnet-scan.nse dns-ip6-arpa-scan.nse dns-nsec-enum.nse dns-random-srcport.nse dns-recursion.nse dns-srv-enum.nse dns-zeustracker.nse
dns-brute.nse dns-check-zone.nse dns-fuzz.nse dns-nsec3-enum.nse dns-nsid.nse dns-random-txid.nse dns-service-discovery.nse dns-update.nse dns-zone-transfer.nse
(root@kali)-[/usr/share/nmap/scripts]
# nmap -v -p 53 --script dns-nsec-enum.nse 192.168.1.63
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-28 04:39 EST
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:39
Completed NSE at 04:39, 0.00s elapsed
Initiating ARP Ping Scan at 04:39
Scanning 192.168.1.63 [1 port]
Completed ARP Ping Scan at 04:39, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:39
Completed Parallel DNS resolution of 1 host. at 04:39, 0.07s elapsed
Initiating SYN Stealth Scan at 04:39
Scanning 192.168.1.63 [1 port]
Discovered open port 53/tcp on 192.168.1.63
Completed SYN Stealth Scan at 04:39, 0.03s elapsed (1 total ports)
NSE: Script scanning 192.168.1.63.
Initiating NSE at 04:39
Completed NSE at 04:39, 0.00s elapsed
Nmap scan report for 192.168.1.63
Host is up (0.00053s latency).
PORT STATE SERVICE
53/tcp open domain
| dns-nsec-enum: Can't determine domain for host 192.168.1.63; use dns-nsec-enum.domains script arg.
MAC Address: 08:00:27:78:64:40 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
NSE: Script Post-scanning.
Initiating NSE at 04:39
Completed NSE at 04:39, 0.00s elapsed
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
Raw packets sent: 2 (72B) | Rcvd: 2 (72B)
(root@kali)-[/usr/share/nmap/scripts]
#
Nifty bank +0.10%
Search
ENG IN
15:09 28-11-2025
Right Ctrl

# 6 .SMTP :

**1 . SMTP stands for Simple Mail Transfer Protocol.**

**2 . It is used for sending emails from one server to another.**

**3 . Works at Application Layer of the OSI model.**

**4 . SMTP uses port numbers**

**1 .2Port 25 → Default port (non-encrypted, often blocked by ISPs)**

**2 . Port 465 → Secure SMTP (SMTPS, with SSL)**

**3 . Port 587 → Secure mail submission(TLS)**

**5 . as a hacker the next step is to perform SMTP enumeration.SMTP enumeration is performed to obtain a list of valid users,delivery addresses,message recepients on an SMTP server.**

**6 . Steps :**

1 **. cd /usr/share/nmap/scripts This folder contains all Nmap NSE scripts.You are specifically looking at SMTP-related scripts.**

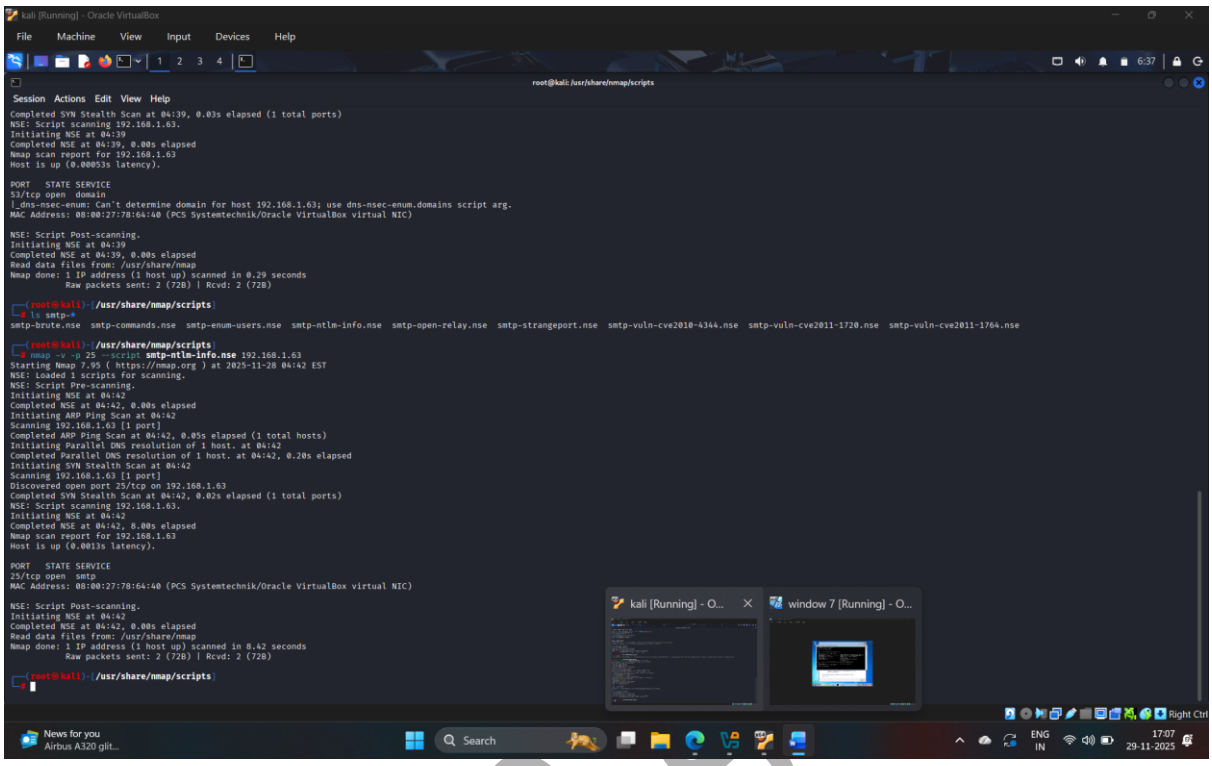
2 **. ls smtp* This command shows all scripts whose names start with smtp.These scripts are used for SMTP enumeration, testing, and vulnerability scanning.**

**scripts like:**

1. **smtp-commands.nse**
2. **smtp-enum-users.nse**
3. **smtp-open-relay.nse**
4. **smtp-strangeport.nse**
5. **smtp-vuln-cve2010-4344.nse**
6. **smtp-vuln-cve2011-1720.nse**
7. **smtp-vuln-cve2011-1764.nse**

**3 . This script tries to detect:**

1. **SMTP NTLM authentication**
2. **Domain name**
3. **Server OS information**


kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
root@kali: /usr/share/nmap/scripts
Completed SYN Stealth Scan at 04:39, 0.03s elapsed (1 total ports)
NSE: Script scanning 192.168.1.63.
Initiating NSE at 04:39
Completed NSE at 04:39, 0.00s elapsed
Nmap scan report for 192.168.1.63
Host is up (0.00053s latency).
PORT STATE SERVICE
53/tcp open domain
|_dns-nsec-enum: Can't determine domain for host 192.168.1.63; use dns-nsec-enum.domains script arg.
MAC Address: 08:00:27:78:64:40 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
NSE: Script Post-scanning.
Initiating NSE at 04:39
Completed NSE at 04:39, 0.00s elapsed
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
Raw packets sent: 2 (72B) | Rcvd: 2 (72B)
(root@kali)-[/usr/share/nmap/scripts]
# ls smtp-*
smtp-brute.nse smtp-commands.nse smtp-enum-users.nse smtp-ntlm-info.nse smtp-open-relay.nse smtp-strangeport.nse smtp-vuln-cve2010-4344.nse smtp-vuln-cve2011-1720.nse smtp-vuln-cve2011-1764.nse
(root@kali)-[/usr/share/nmap/scripts]
# nmap -v -p 25 --script smtp-ntlm-info.nse 192.168.1.63
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-28 04:42 EST
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:42
Completed NSE at 04:42, 0.00s elapsed
Initiating ARP Ping Scan at 04:42
Scanning 192.168.1.63 [1 port]
Completed ARP Ping Scan at 04:42, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:42
Completed Parallel DNS resolution of 1 host. at 04:42, 0.20s elapsed
Initiating SYN Stealth Scan at 04:42
Scanning 192.168.1.63 [1 port]
Discovered open port 25/tcp on 192.168.1.63
Completed SYN Stealth Scan at 04:42, 0.02s elapsed (1 total ports)
NSE: Script scanning 192.168.1.63.
Initiating NSE at 04:42
Completed NSE at 04:42, 0.00s elapsed
Nmap scan report for 192.168.1.63
Host is up (0.0013s latency).
PORT STATE SERVICE
25/tcp open smtp
MAC Address: 08:00:27:78:64:40 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
NSE: Script Post-scanning.
Initiating NSE at 04:42
Completed NSE at 04:42, 0.00s elapsed
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
Raw packets sent: 2 (72B) | Rcvd: 2 (72B)
(root@kali)-[/usr/share/nmap/scripts]
kali [Running] - O...
window 7 [Running] - O...
Right Ctrl
News for you
Airbus A320 glit...
Search
ENG
IN
17:07
29-11-2025