# Enumeration

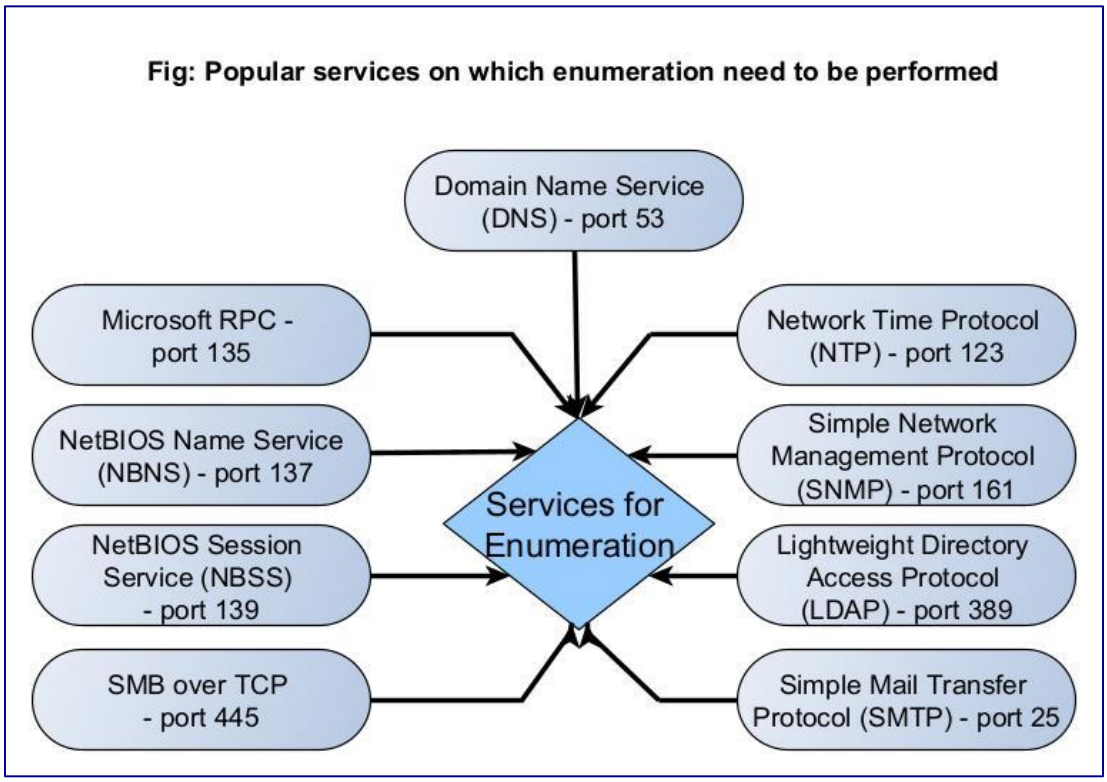
### What is Enumeration?

In Enumeration, an attacker or a Pen Tester performs calculated queries to gather more detailed information about the target. Usually, enumeration is performed on the services running on the target (open ports) with the purpose of gaining access to the target system.

### What information does enumeration reveal?

Enumeration can reveal valuable information like Network shares, usernames and passwords, version of the application running, users and groups, machine names, service settings and other network resources.

### Which services can be enumerated?



Although all services running on the target system can be enumerated upon, there are some specific services which are regularly enumerated to retrieve useful information. They are,

1. DNS (Port 53)
2. Microsoft RPC (Port 153)
3. NetBIOS Name Service (NBNS) (Port 137)
4. NetBIOS Session Service (SMB over NetBIOS)
5. SMB Over TCP (Port 445)
6. Network Time Protocol (NTP) (Port 123)
7. Simple Network Management Protocol (SNMP) (Port 161)
8. Lightweight Directory Access Protocol (LDAP) (Port 389)
9. Simple Mail Transfer Protocol (SMTP) (Port 25)

Let's learn about each of these services in detail.

1. SMTP

Simple Mail Transfer Protocol (SMTP) is a TCP/IP protocol that is used to send email. It is mostly used by email clients but most of the organizations have their own Email Servers to send mail. Enumerating SMTP Service can reveal the list of valid users on the SMTP Servers. Learn how to perform SMTP enumeration.

2. DNS

The function of Domain Name Service (DNS) is explained in our article DNS Footprinting. Enumerating DNS servers can reveal network information like host names, other DNS server names, machine names, IP addresses, potential targets and in some cases usernames too. Learn how to perform DNS enumeration.

3. NetBIOS

NetBIOS service allows programs and computers on a local area network to communicate with each other. These include services like files, printers and device shares. Enumerating NetBIOS can reveal information like list of computers in a specific domain, lists of shares, policies and Passwords etc. Learn how to perform NetBIOS enumeration.

4. SMB

Just like NetBIOS, Server Message Block (SMB) is a protocol that allows applications and computers in a local network talk to each other. The only difference between them is that NetBIOS is an API whereas SMB is a protocol. Starting from Windows 2000, SMB which earlier ran on top of NetBIOS was made to operate on top of TCP and it got a dedicated port 445.

It also enables network services like file, printer and device sharing. Enumerating SMB service can reveal information like host names, lists shares, checking for null session, users, operating system details, password policies, info groups and printers connected etc. Learn how to perform SMB enumeration.

5. NTP

Network Time Protocol (NTP) is a protocol designed to synchronize clocks of all computers on the same network. Enumerating NTP can reveal information about hosts connected to the NTP server and IP addresses of the machines in the network etc. Learn how to perform NTP enumeration.

6. SNMP

Simple Network Management Protocol (SNMP) is a protocol that is used to monitor and manage computer systems in the same network. Enumerating SNMP can reveal information about network resources like hosts, routes, shares, ARP tables, routing tables, etc. Learn how to perform SNMP enumeration.

7. LDAP

Lightweight Directory Access Protocol (LDAP) is an internet protocol that is used to access information from directories like Active Directory. Enumerating LDAP can reveal information such as valid usernames, addresses and other details. Learn how to perform LDAP enumeration.

**Objective of Enumeration**:

- Discover **usernames**, **group names**
- Find **network shares**
- Detect **services and protocols**
- Uncover **DNS details**, **SNMP data**
- Identify **system banners**
- Locate **vulnerable services**

**Types of Enumeration / Tools we use for enumeration**:

1) **dnsenum**

dnsenum is a command-line tool used in ethical hacking and penetration testing to gather information about DNS (Domain Name System) records of a domain. It helps in DNS enumeration, which is a part of the enumeration phase of hacking methodology.

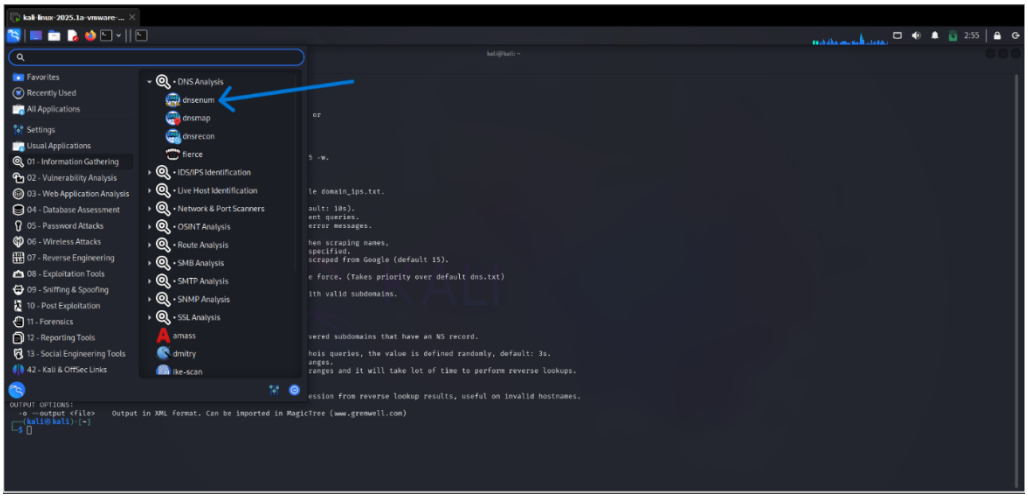
**Purpose of dnsenum:**

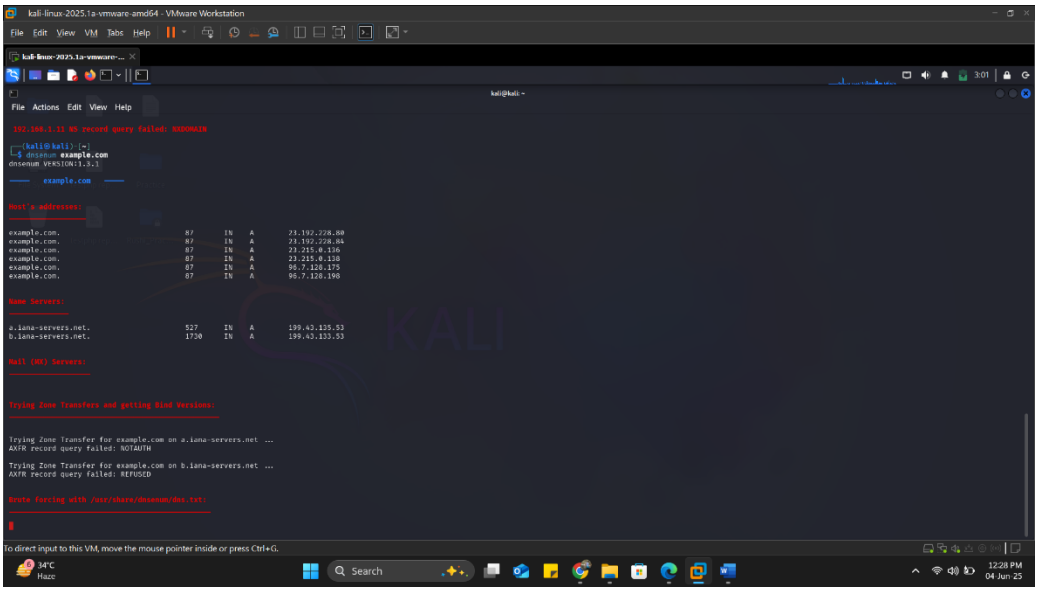
To discover all the DNS-related information of a target domain, such as:

- Subdomains
- IP addresses
- Nameservers (NS)
- Mail servers (MX)
- Zone transfer (AXFR)
- WHOIS info
- Brute-force subdomains using a wordlist

**Example:**

In DNS Enumeration we use kali's inbuild tool called dnsenum and try to enumerate example.com



## 2) Enum4linux

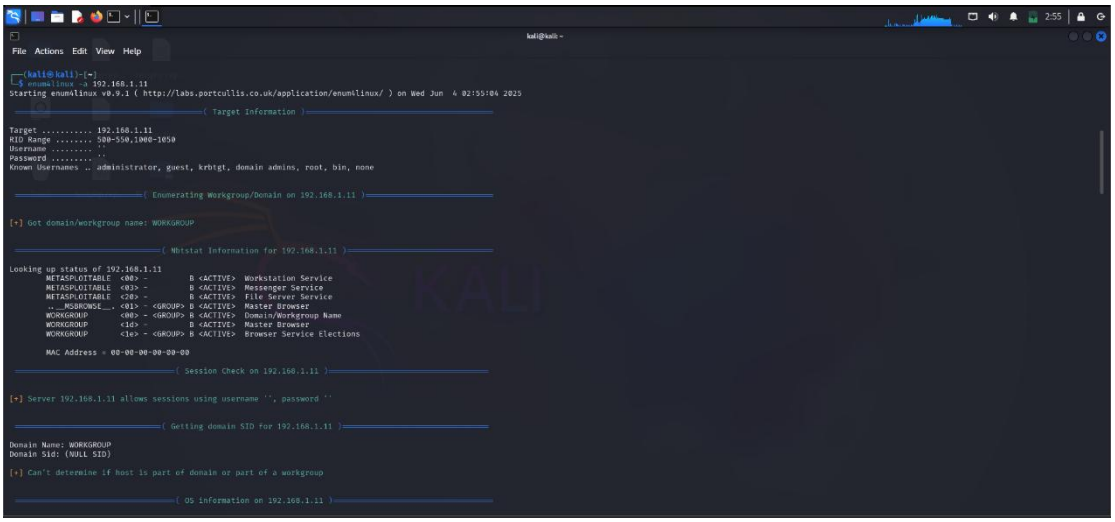
enum4linux is a Linux-based information-gathering tool used for enumerating information from Windows and Samba systems. It helps ethical hackers and penetration testers during the enumeration phase of hacking.

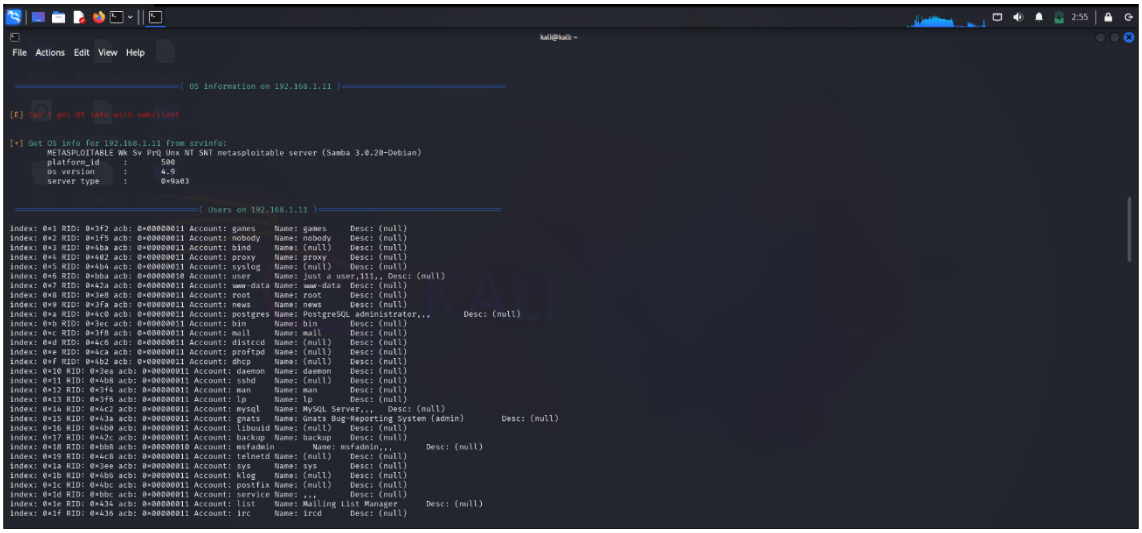
### Purpose of enum4linux:

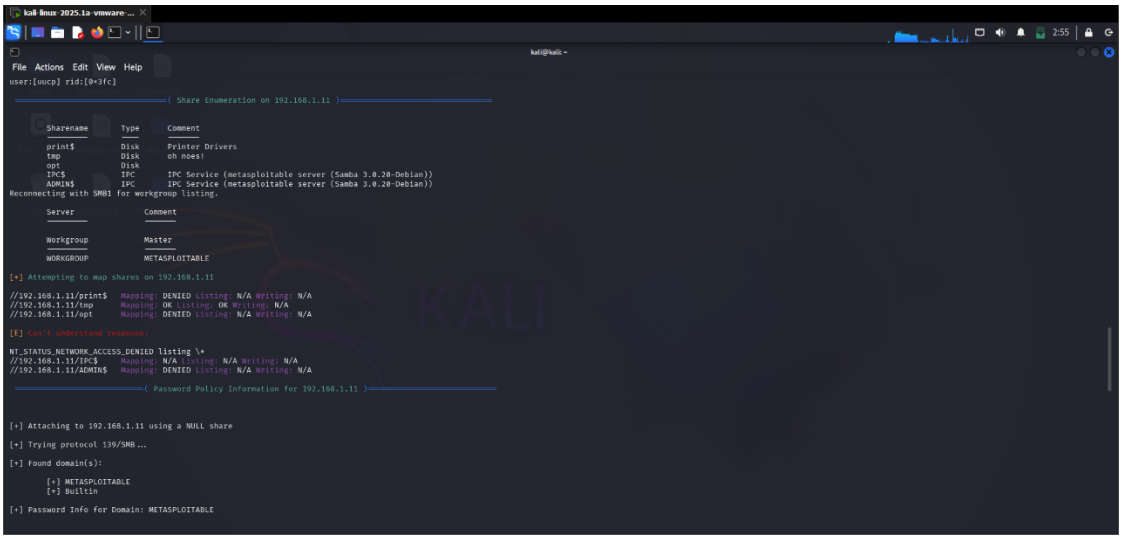
enum4linux extracts useful details from Windows machines using the SMB (Server Message Block) protocol.

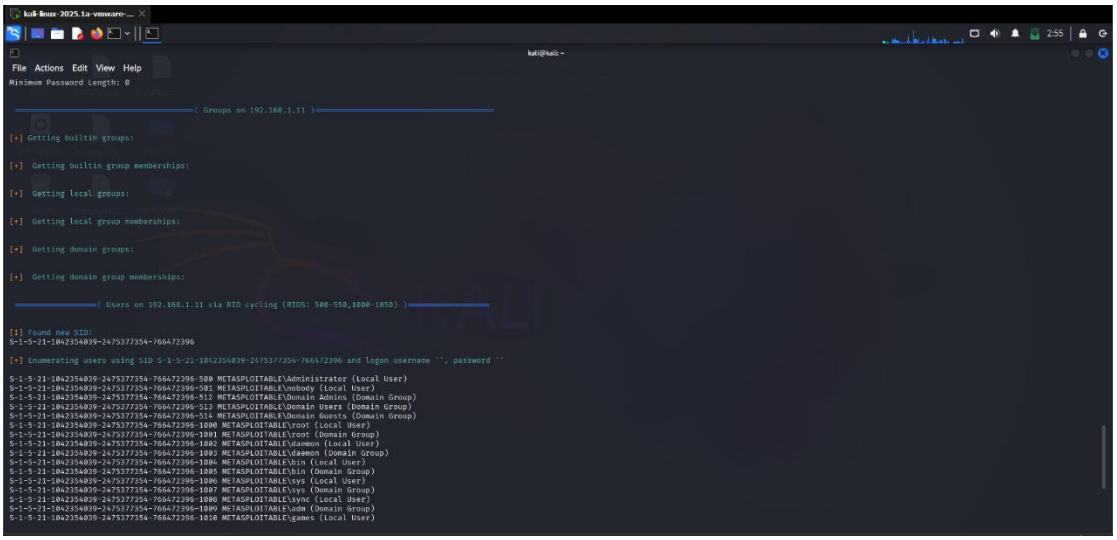
### Example:

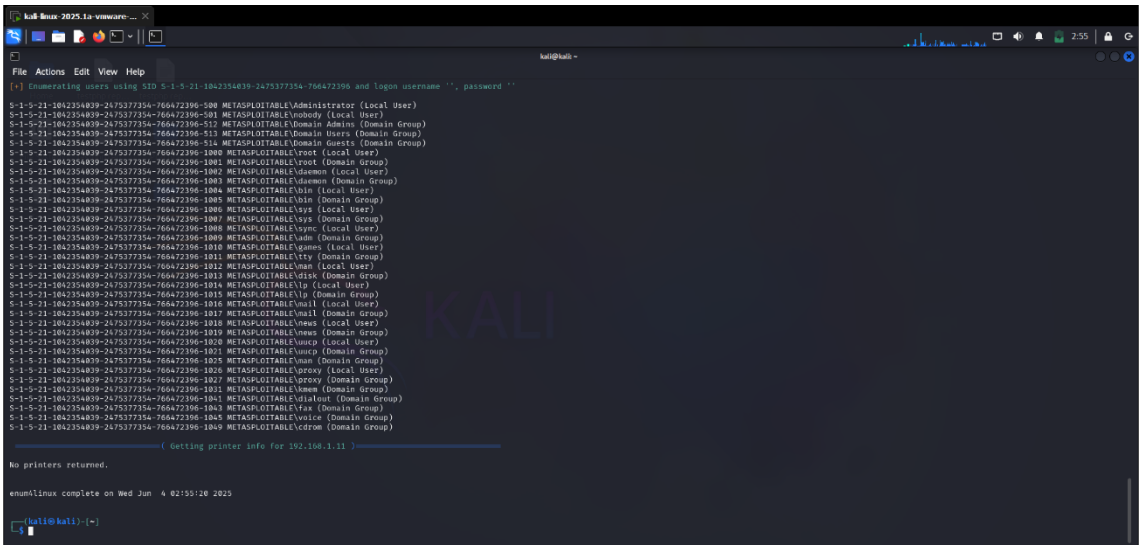
This is also inbuild in kali linux machine some practicle images as follows :


kali@kali: ~
File Actions Edit View Help
( OS information on 192.168.1.11 )
[E] Can't get OS info with smbclient
[+] Got OS info for 192.168.1.11 from srvinfo:
METASPLOITABLE Wk Sv PrQ Unx NT SNT metasploitable server (Samba 3.0.20-Debian)
platform_id : 500
os version : 4.9
server type : 0x9a03
( Users on 192.168.1.11 )
index: 0x1 RID: 0x3f2 acb: 0x00000011 Account: games Name: games Desc: (null)
index: 0x2 RID: 0x1f5 acb: 0x00000011 Account: nobody Name: nobody Desc: (null)
index: 0x3 RID: 0x4ba acb: 0x00000011 Account: bind Name: (null) Desc: (null)
index: 0x4 RID: 0x4b2 acb: 0x00000011 Account: proxy Name: proxy Desc: (null)
index: 0x5 RID: 0x4b4 acb: 0x00000011 Account: syslog Name: (null) Desc: (null)
index: 0x6 RID: 0x0ba acb: 0x00000010 Account: user Name: just a user,111,, Desc: (null)
index: 0x7 RID: 0x42a acb: 0x00000011 Account: www-data Name: www-data Desc: (null)
index: 0x8 RID: 0x3e8 acb: 0x00000011 Account: root Name: root Desc: (null)
index: 0x9 RID: 0x3fa acb: 0x00000011 Account: news Name: news Desc: (null)
index: 0xa RID: 0x4c0 acb: 0x00000011 Account: postgres Name: PostgreSQL administrator,,, Desc: (null)
index: 0xb RID: 0x3ec acb: 0x00000011 Account: bin Name: bin Desc: (null)
index: 0xc RID: 0x3f8 acb: 0x00000011 Account: mail Name: mail Desc: (null)
index: 0xd RID: 0x4c6 acb: 0x00000011 Account: distccd Name: (null) Desc: (null)
index: 0xe RID: 0x4ca acb: 0x00000011 Account: proftpd Name: (null) Desc: (null)
index: 0xf RID: 0x4b2 acb: 0x00000011 Account: dhcp Name: (null) Desc: (null)
index: 0x10 RID: 0x3ea acb: 0x00000011 Account: daemon Name: daemon Desc: (null)
index: 0x11 RID: 0x4b8 acb: 0x00000011 Account: sshd Name: (null) Desc: (null)
index: 0x12 RID: 0x3f4 acb: 0x00000011 Account: man Name: man Desc: (null)
index: 0x13 RID: 0x3f6 acb: 0x00000011 Account: lp Name: lp Desc: (null)
index: 0x14 RID: 0x4c2 acb: 0x00000011 Account: mysql Name: MySQL Server,,, Desc: (null)
index: 0x15 RID: 0x4ja acb: 0x00000011 Account: gnats Name: Gnats Bug-Reporting System (admin) Desc: (null)
index: 0x16 RID: 0x4b0 acb: 0x00000011 Account: libuuid Name: (null) Desc: (null)
index: 0x17 RID: 0x42c acb: 0x00000011 Account: backup Name: backup Desc: (null)
index: 0x18 RID: 0xbb8 acb: 0x00000010 Account: msfadmin Name: msfadmin,,, Desc: (null)
index: 0x19 RID: 0x4c8 acb: 0x00000011 Account: telnetd Name: (null) Desc: (null)
index: 0x1a RID: 0x3ee acb: 0x00000011 Account: sys Name: sys Desc: (null)
index: 0x1b RID: 0x4b6 acb: 0x00000011 Account: klog Name: (null) Desc: (null)
index: 0x1c RID: 0x4bc acb: 0x00000011 Account: postfix Name: (null) Desc: (null)
index: 0x1d RID: 0xbbc acb: 0x00000011 Account: service Name: ,,, Desc: (null)
index: 0x1e RID: 0x434 acb: 0x00000011 Account: list Name: Mailing List Manager Desc: (null)
index: 0x1f RID: 0x436 acb: 0x00000011 Account: irc Name: ircd Desc: (null)


kali-linux-2025.1a-vmware-...
kali@kali: ~
File Actions Edit View Help
user:[uucp] rid:[0x3fc]
( Share Enumeration on 192.168.1.11 )
Sharename Type Comment
print$ Disk Printer Drivers
tmp Disk oh noes!
opt Disk
IPC$ IPC IPC Service (metasploitable server (Samba 3.0.20-Debian))
ADMIN$ IPC IPC Service (metasploitable server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.
Server Comment
Workgroup Master
WORKGROUP METASPLOITABLE
[+] Attempting to map shares on 192.168.1.11
//192.168.1.11/print$ Mapping: DENIED Listing: N/A Writing: N/A
//192.168.1.11/tmp Mapping: OK Listing: OK Writing: N/A
//192.168.1.11/opt Mapping: DENIED Listing: N/A Writing: N/A
[E] Can't understand response:
NT_STATUS_NETWORK_ACCESS_DENIED listing *
//192.168.1.11/IPC$ Mapping: N/A Listing: N/A Writing: N/A
//192.168.1.11/ADMIN$ Mapping: DENIED Listing: N/A Writing: N/A
( Password Policy Information for 192.168.1.11 )
[+] Attaching to 192.168.1.11 using a NULL share
[+] Trying protocol 139/SMB ...
[+] Found domain(s):
[+] METASPLOITABLE
[+] Builtin
[+] Password Info for Domain: METASPLOITABLE


kali-linux-2025.1a-vmware-...
kali@kali: ~
File Actions Edit View Help
Minimum Password Length: 0
( Groups on 192.168.1.11 )
[+] Getting builtin groups:
[+] Getting builtin group memberships:
[+] Getting local groups:
[+] Getting local group memberships:
[+] Getting domain groups:
[+] Getting domain group memberships:
( Users on 192.168.1.11 via RID cycling (RIDS: 500-550,1000-1050) )
[I] Found new SID:
S-1-5-21-1042354039-2475377354-766472396
[+] Enumerating users using SID S-1-5-21-1042354039-2475377354-766472396 and logon username '', password ''
S-1-5-21-1042354039-2475377354-766472396-500 METASPLOITABLE\Administrator (Local User)
S-1-5-21-1042354039-2475377354-766472396-501 METASPLOITABLE\nobody (Local User)
S-1-5-21-1042354039-2475377354-766472396-512 METASPLOITABLE\Domain Admins (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-513 METASPLOITABLE\Domain Users (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-514 METASPLOITABLE\Domain Guests (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1000 METASPLOITABLE\root (Local User)
S-1-5-21-1042354039-2475377354-766472396-1001 METASPLOITABLE\root (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1002 METASPLOITABLE\daemon (Local User)
S-1-5-21-1042354039-2475377354-766472396-1003 METASPLOITABLE\daemon (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1004 METASPLOITABLE\bin (Local User)
S-1-5-21-1042354039-2475377354-766472396-1005 METASPLOITABLE\bin (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1006 METASPLOITABLE\sys (Local User)
S-1-5-21-1042354039-2475377354-766472396-1007 METASPLOITABLE\sys (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1008 METASPLOITABLE\sync (Local User)
S-1-5-21-1042354039-2475377354-766472396-1009 METASPLOITABLE\adm (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1010 METASPLOITABLE\games (Local User)




### 3) Nbt scan

nbtscan is a network scanning tool used to discover NetBIOS names and information of computers on a local network. It is commonly used in ethical hacking to enumerate Windows systems.

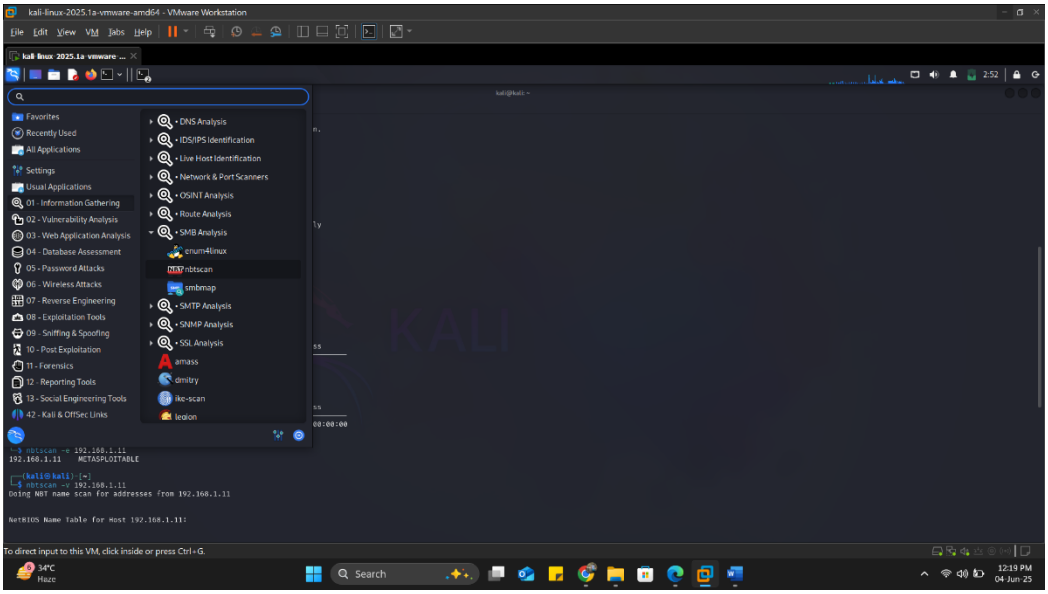
**Purpose of nbt Scan:**

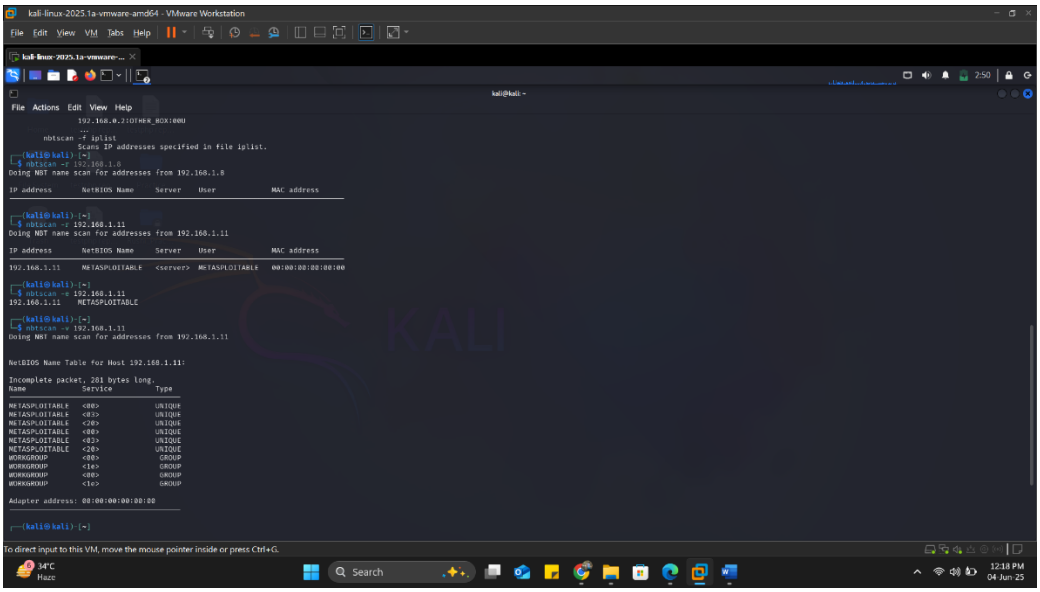
To scan IP ranges and retrieve NetBIOS (Network Basic Input/Output System) details like:

- Computer names
- Usernames
- MAC addresses
- Workgroups or domains

It uses **NetBIOS Name Service (NBNS)** on **UDP port 137.**

## Example:


kali-linux-2025.1a-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali linux 2025.1a vmware ...
Favorites
Recently Used
All Applications
Settings
Usual Applications
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
42 - Kali & OffSec Links
• DNS Analysis
• IDS/IPS Identification
• Live Host Identification
• Network & Port Scanners
• OSINT Analysis
• Route Analysis
• SMB Analysis
enum4linux
nbtscan
smbmap
• SMTP Analysis
• SNMP Analysis
• SSL Analysis
amass
dmitry
ike-scan
legion
┌──(kali㉿kali)-[~]
└─$ nbtscan -e 192.168.1.11
192.168.1.11 METASPLOITABLE
┌──(kali㉿kali)-[~]
└─$ nbtscan -v 192.168.1.11
Doing NBT name scan for addresses from 192.168.1.11
NetBIOS Name Table for Host 192.168.1.11:
To direct input to this VM, click inside or press Ctrl+G.
34°C
Haze
Search
12:19 PM
04-Jun-25


kali-linux-2025.1a-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali@kali: ~
File Actions Edit View Help
nbtscan -f iplist
Scans IP addresses specified in file iplist.
┌──(kali㉿kali)-[~]
└─$ nbtscan -r 192.168.1.0
Doing NBT name scan for addresses from 192.168.1.8
IP address NetBIOS Name Server User MAC address
┌──(kali㉿kali)-[~]
└─$ nbtscan -r 192.168.1.11
Doing NBT name scan for addresses from 192.168.1.11
IP address NetBIOS Name Server User MAC address
192.168.1.11 METASPLOITABLE <server> METASPLOITABLE 00:00:00:00:00:00
┌──(kali㉿kali)-[~]
└─$ nbtscan -e 192.168.1.11
192.168.1.11 METASPLOITABLE
┌──(kali㉿kali)-[~]
└─$ nbtscan -v 192.168.1.11
Doing NBT name scan for addresses from 192.168.1.11
NetBIOS Name Table for Host 192.168.1.11:
Incomplete packet, 281 bytes long.
Name Service Type
METASPLOITABLE <00> UNIQUE
METASPLOITABLE <03> UNIQUE
METASPLOITABLE <20> UNIQUE
METASPLOITABLE <00> UNIQUE
METASPLOITABLE <03> UNIQUE
METASPLOITABLE <20> UNIQUE
WORKGROUP <00> GROUP
WORKGROUP <1e> GROUP
WORKGROUP <00> GROUP
WORKGROUP <1e> GROUP
Adapter address: 00:00:00:00:00:00
┌──(kali㉿kali)-[~]
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
34°C
Haze
Search
12:18 PM
04-Jun-25

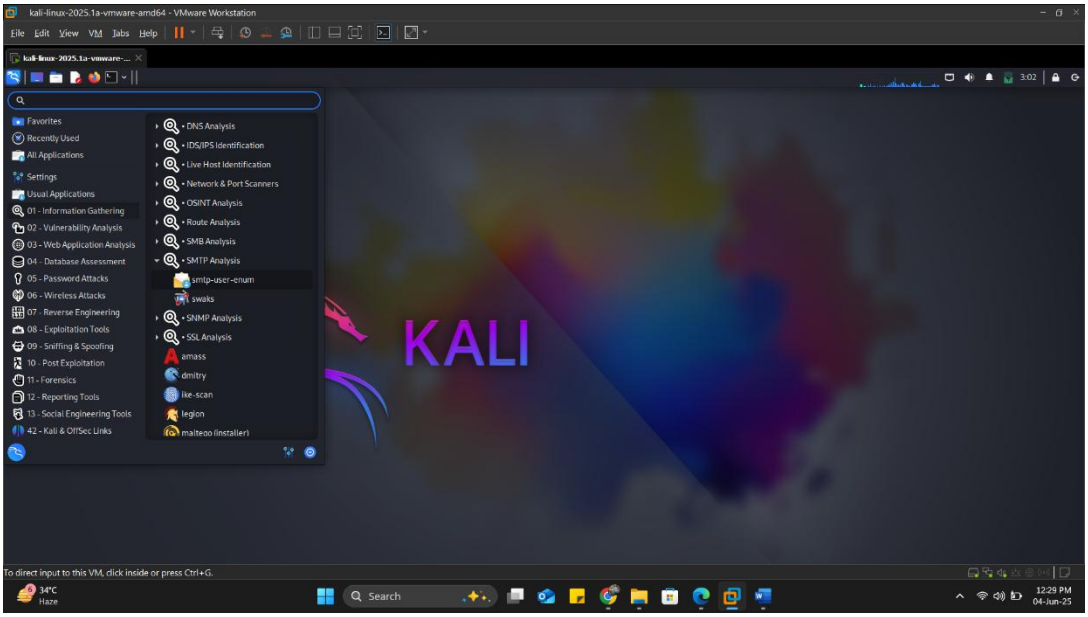
### 4) Smtp user-enum

smtp-user-enum is a command-line tool used to enumerate valid usernames on a mail server using the SMTP (Simple Mail Transfer Protocol) service. It's commonly used by ethical hackers during the enumeration phase to discover existing user accounts on the target system.

**Purpose of smtp user-enum:**

To check if specific usernames exist on an **SMTP** server by sending **SMTP** commands like VRFY, EXPN, or RCPT TO.

**Example:**




```
┌──(kali㉿kali)-[~]
└─$ smtp-user-enum -M EXPN -u admin1 -t 10.0.0.1

Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Mode ..................... EXPN
Worker Processes ......... 5
Target count ............. 1
Username count ........... 1
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............

######## Scan started at Wed Jun  4 03:28:47 2025 #########
######## Scan completed at Wed Jun  4 03:28:52 2025 #########
0 results.

1 queries in 5 seconds (0.2 queries / sec)

┌──(kali㉿kali)-[~]
└─$
```

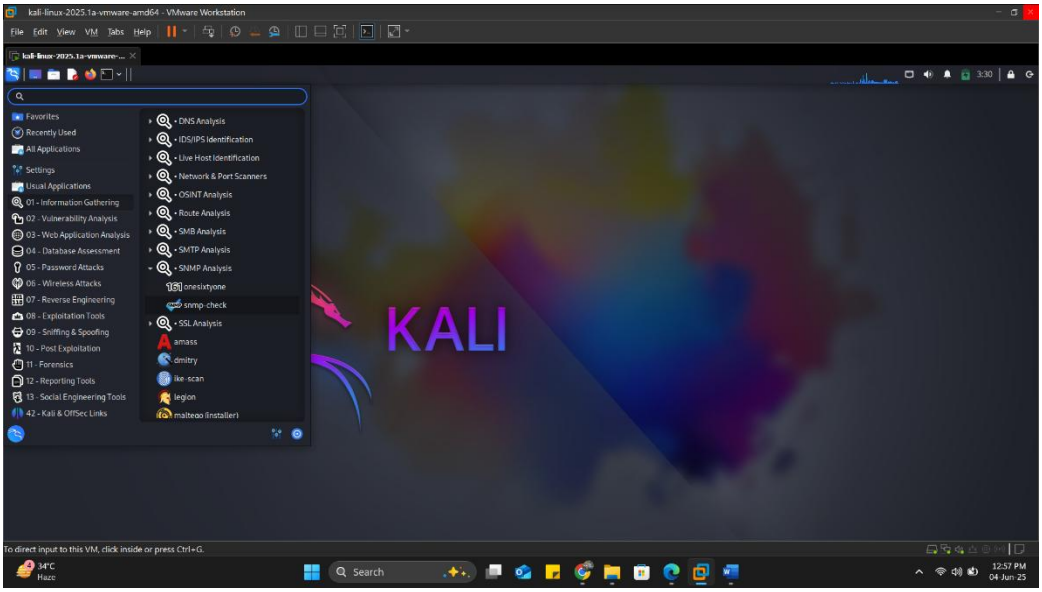
### 5) Snmp-check

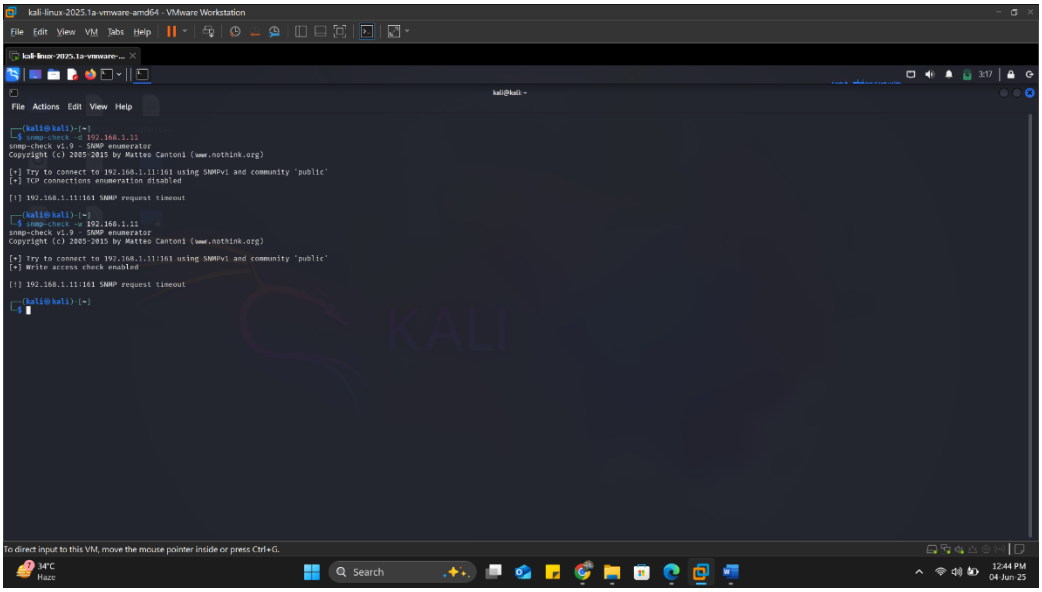
snmp-check is a command-line tool used to enumerate information from systems running SNMP (Simple Network Management Protocol). It is commonly used by ethical hackers to gather detailed system data during the enumeration phase.

**Purpose of snmp-check:**

To query a device using SNMP v1 and retrieve valuable system information using a read-only community string (usually "public" by default).

**Example:**



**Some important point of footprinting**

normal information gathering (footprinting)
spider foot
spiderfoot -1 127.0.0.1:9090