This repository documents a hands-on ethical hacking lab focused on enumerating Server Message Block (SMB) services using Enum4linux.

Enum4linux is a tool for enumerating information from Windows and Samba. Samba is an application that enables Linux and Apple clients to participate in Windows networks. It enables non-Windows clients to utilize the Server Message Block (SMB) protocol to access file and print services. Samba servers can participate in a Windows domain, both as a client and a server The goal is to:

- Launch enum4linux and explore its capabilities.
- Identify computers with SMB services running.
- Use enum4linux to enumerate users and network file shares.
- Use smbclient to transfer files between systems.

This lab is performed in a fully controlled virtual lab environment using intentionally vulnerable machines (e.g., Metasploitable 2).

Poorly secured and managed Windows server networks are a huge security risk. Penetration testers must uncover any vulnerabilities in file and print sharing functions that can leave an organization vulnerable to attack. In this activity, you will explore the capabilities of the enum4linux tool to enumerate user and file sharing information from Samba servers. Finally, you will use the smbclient utility to transfer files between systems.

Lab Enviroment

attacker: Kali Linux (Provided by CISCO NetAcad)

Tools: Enum4linux, Nmap (for initial discovery)

Step 1: Verify Installation and Review Help Options

Objective:

Confirm that Enum4linux is installed on the Kali Linux system and examine its available options to understand the tool's full capabilities.

Boot into Kali Linux and log in with the default credentials:

Username: kali

Password: kali

Open a terminal:

Elevate privileges to root (recommended for most Enum4linux operations):

In the terminal, run: sudo su

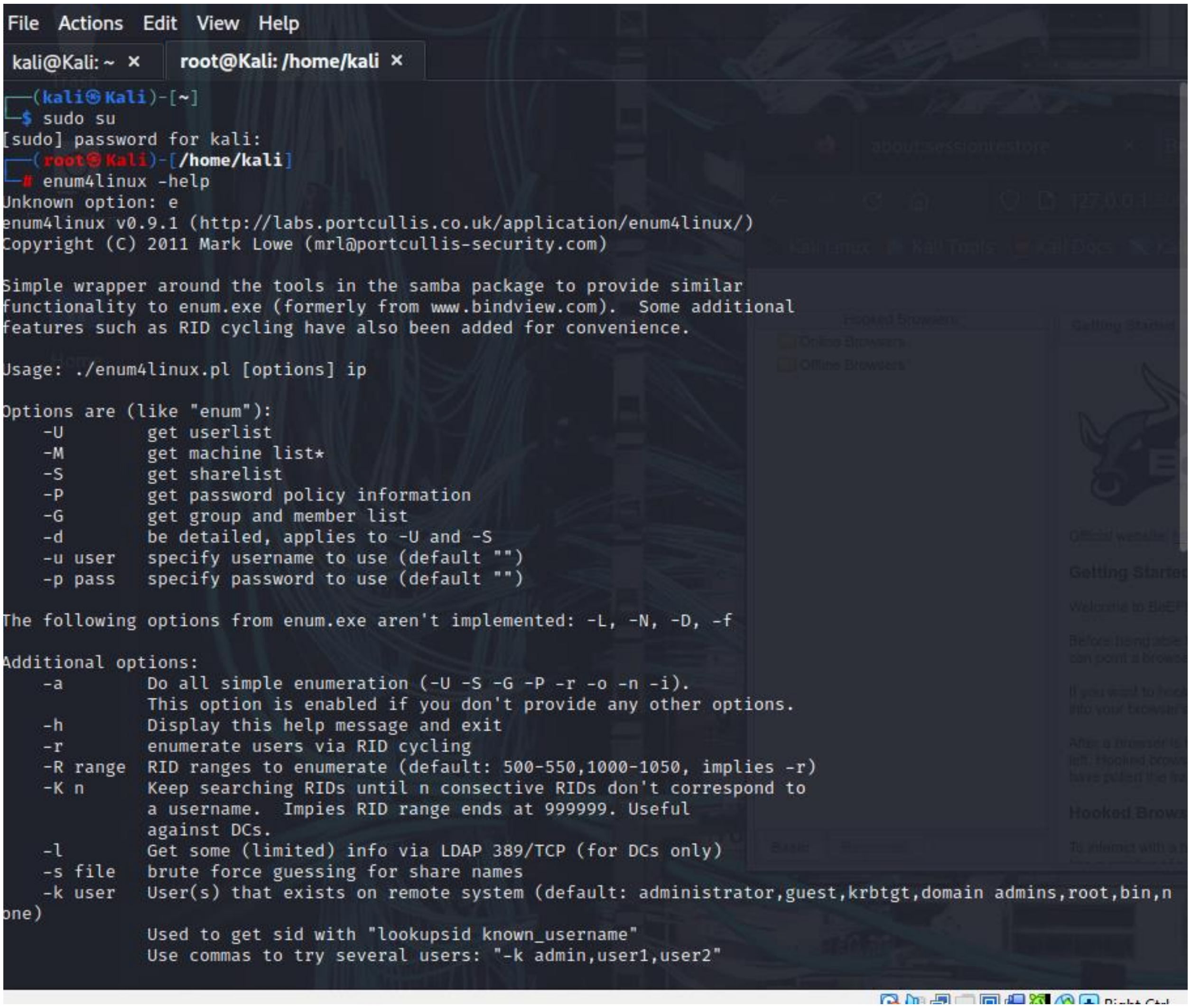
Enter the password kali when prompted.

The prompt will change to indicate root access.

Enum4linux supports targeted enumeration (e.g., -u for users, -S for shares, -G for groups).

The -a flag performs all basic enumeration tasks in one pass (commonly used).

Options like -r (enumerate users via RID cycling) and -P (password policy) are useful for deeper assessment.



```
┌──(kali㉿Kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿Kali)-[/home/kali]
└─# enum4linux -help
Unknown option: e
enum4linux v0.9.1 (http://labs.portcullis.co.uk/application/enum4linux/)
Copyright (C) 2011 Mark Lowe (mrl@portcullis-security.com)

Simple wrapper around the tools in the samba package to provide similar
functionality to enum.exe (formerly from www.bindview.com).  Some additional
features such as RID cycling have also been added for convenience.

Usage: ./enum4linux.pl [options] ip

Options are (like "enum"):
    -U        get userlist
    -M        get machine list*
    -S        get sharelist
    -P        get password policy information
    -G        get group and member list
    -d        be detailed, applies to -U and -S
    -u user   specify username to use (default "")
    -p pass   specify password to use (default "")

The following options from enum.exe aren't implemented: -L, -N, -D, -f

Additional options:
    -a        Do all simple enumeration (-U -S -G -P -r -o -n -i).
              This option is enabled if you don't provide any other options.
    -h        Display this help message and exit
    -r        enumerate users via RID cycling
    -R range  RID ranges to enumerate (default: 500-550,1000-1050, implies -r)
    -K n      Keep searching RIDs until n consective RIDs don't correspond to
              a username.  Impies RID range ends at 999999. Useful
              against DCs.
    -l        Get some (limited) info via LDAP 389/TCP (for DCs only)
    -s file   brute force guessing for share names
    -k user   User(s) that exists on remote system (default: administrator,guest,krbtgt,domain admins,root,bin,n
one)
              Used to get sid with "lookupsid known_username"
              Use commas to try several users: "-k admin,user1,user2"
```

This step ensures that the tool is ready and gives a clear overview of its functionality before proceeding to active scanning.

Ethical Reminder: Always perform enumeration only on systems you own or have explicit written permission to test.

Part 2: Discovering SMB Servers with Nmap

Step 1: Scanning the Network for Potential SMB Targets

Objective:

Identify hosts on the lab network that expose SMB-related services by scanning common SMB ports. This helps locate potential targets for further enumeration with Enum4linux.

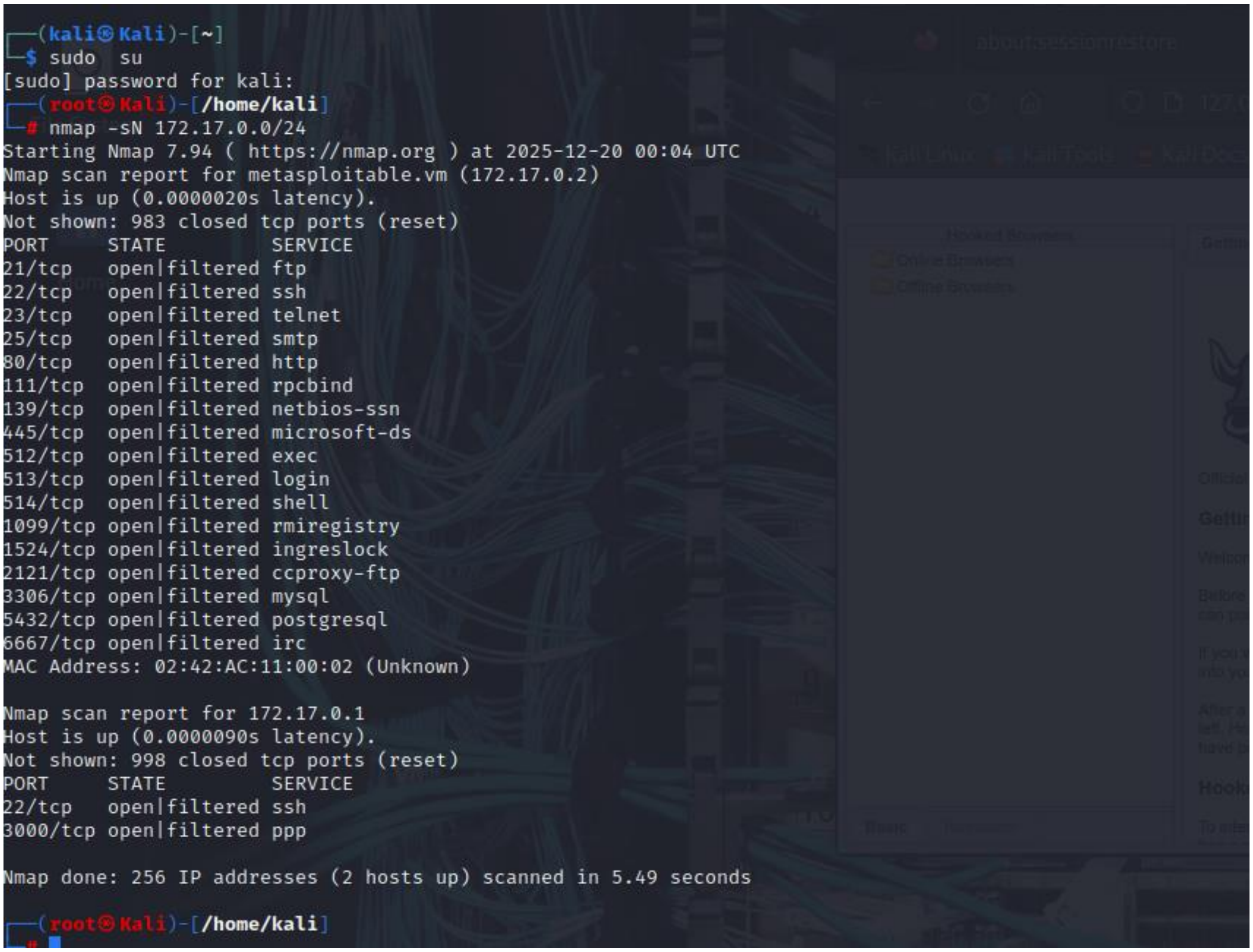
Common SMB-Related Ports:

The following ports are typically associated with SMB and supporting services

Port	Prptocol	Service Description
TCP 135	TCP	RPC (Remote Procedure Call)
TCP 139	TCP	NetBIOS Session Service
TCP 389	TCP	LDAP Server
TCP 445	TCP	SMB File Service (Direct hosting)
TCP 9389	TCP	Active Directory Web Server
TCP/UDP 137	UDP	NetBios Name Service
UDP 138	UDP	NetBIOS Datagram Service

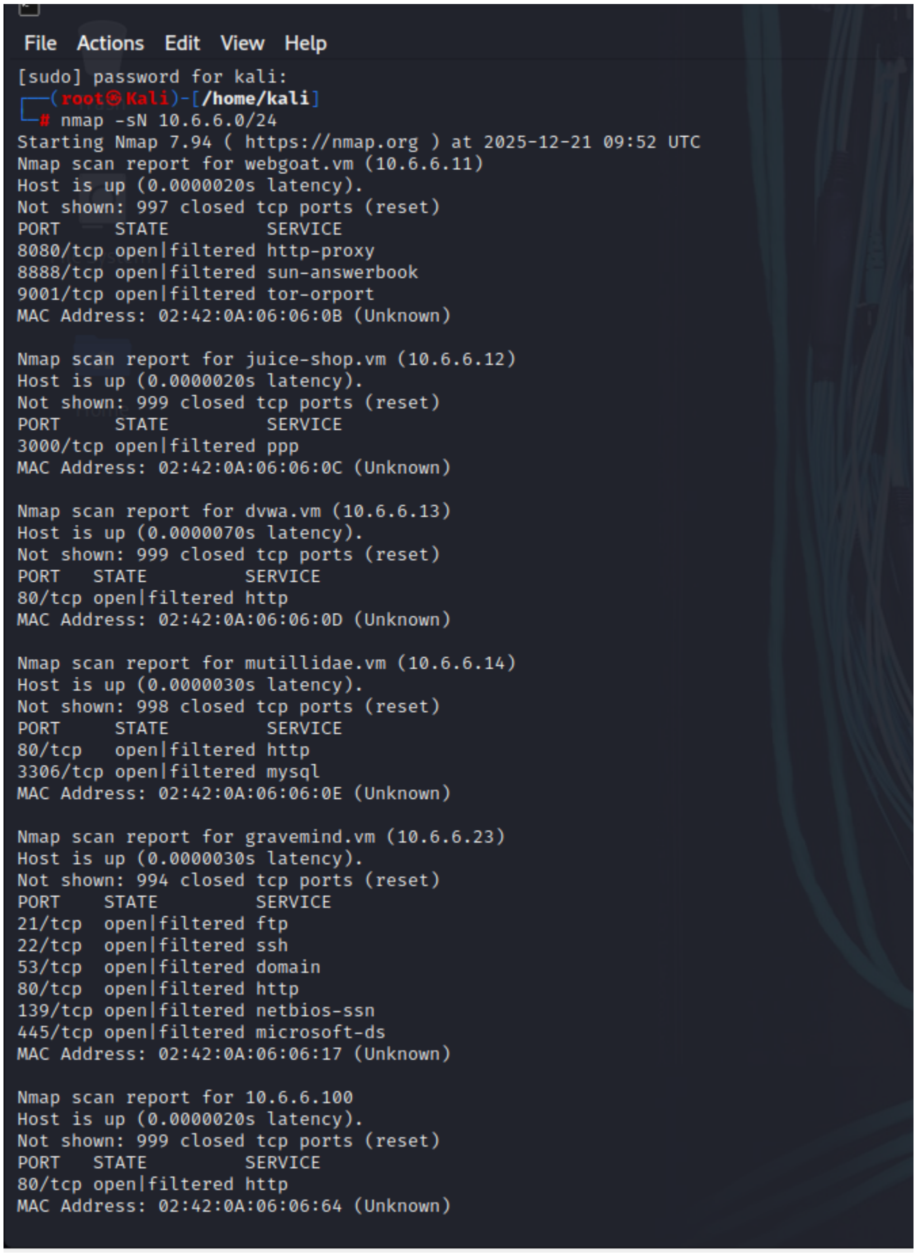
Two virtual networks are included in the Kali VM with Docker containers. Use the nmap -sN command to find the services available on hosts in the 172.17.0.0 virtual network. Note: sudo is not required if you executed the sudo su command above.

```
┌──(root㉿kali)-[/home/kali] └─# nmap -sN 172.17.0.0/24
```



```
┌──(kali㉿Kali)-[~]
└─$ sudo  su
[sudo] password for kali:
┌──(root㉿Kali)-[/home/kali]
└─# nmap -sN 172.17.0.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-20 00:04 UTC
Nmap scan report for metasploitable.vm (172.17.0.2)
Host is up (0.0000020s latency).
Not shown: 983 closed tcp ports (reset)
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
80/tcp   open|filtered http
111/tcp  open|filtered rpcbind
139/tcp  open|filtered netbios-ssn
445/tcp  open|filtered microsoft-ds
512/tcp  open|filtered exec
513/tcp  open|filtered login
514/tcp  open|filtered shell
1099/tcp open|filtered rmiregistry
1524/tcp open|filtered ingreslock
2121/tcp open|filtered ccproxy-ftp
3306/tcp open|filtered mysql
5432/tcp open|filtered postgresql
6667/tcp open|filtered irc
MAC Address: 02:42:AC:11:00:02 (Unknown)

Nmap scan report for 172.17.0.1
Host is up (0.0000090s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE         SERVICE
22/tcp   open|filtered ssh
3000/tcp open|filtered ppp

Nmap done: 256 IP addresses (2 hosts up) scanned in 5.49 seconds

┌──(root㉿Kali)-[/home/kali]
└─#
```

Conduct a nmap -sN scan on the 10.6.6.0/24 subnet. ┌──(root㉿kali)-[/home/kali] └─# nmap -sN 10.6.6.0/24



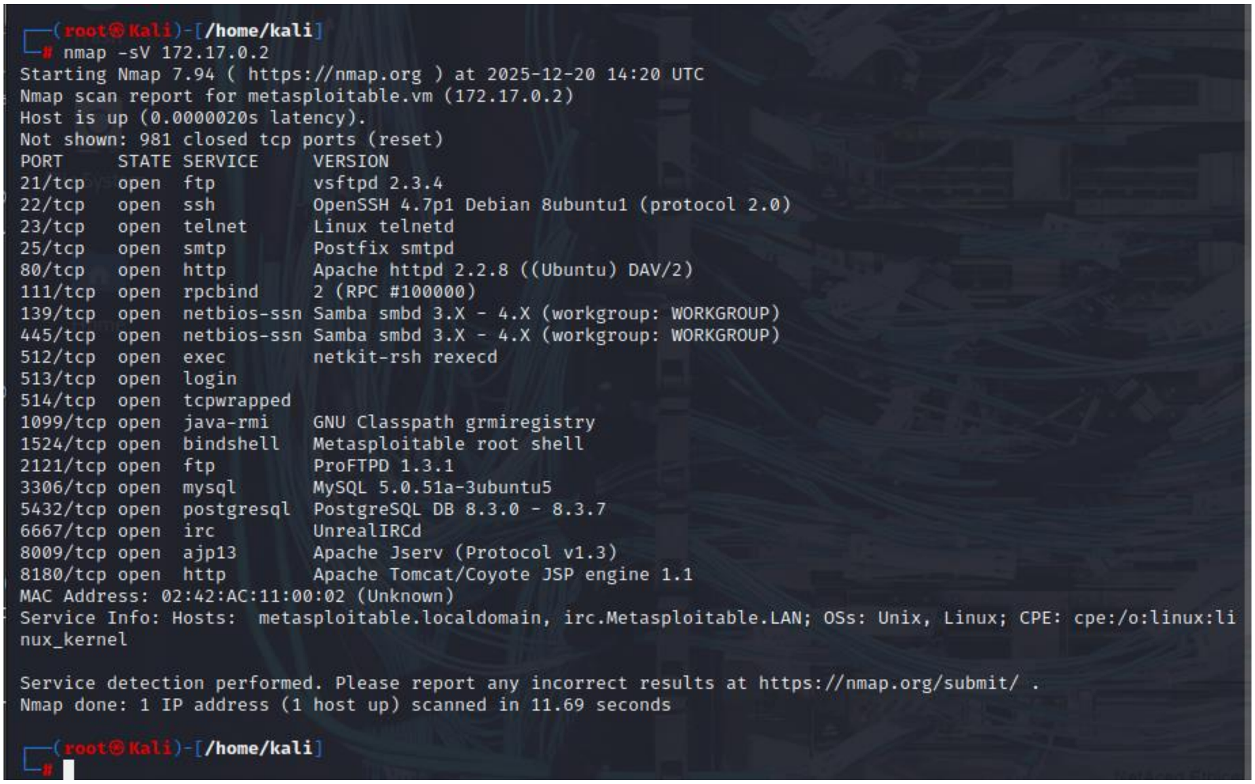
```
[sudo] password for kali:
┌──(root㉿Kali)-[/home/kali]
└─# nmap -sN 10.6.6.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-21 09:52 UTC
Nmap scan report for webgoat.vm (10.6.6.11)
Host is up (0.0000020s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE         SERVICE
8080/tcp open|filtered http-proxy
8888/tcp open|filtered sun-answerbook
9001/tcp open|filtered tor-orport
MAC Address: 02:42:0A:06:06:0B (Unknown)

Nmap scan report for juice-shop.vm (10.6.6.12)
Host is up (0.0000020s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE         SERVICE
3000/tcp open|filtered ppp
MAC Address: 02:42:0A:06:06:0C (Unknown)

Nmap scan report for dvwa.vm (10.6.6.13)
Host is up (0.0000070s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE         SERVICE
80/tcp open|filtered http
MAC Address: 02:42:0A:06:06:0D (Unknown)

Nmap scan report for mutillidae.vm (10.6.6.14)
Host is up (0.0000030s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE         SERVICE
80/tcp   open|filtered http
3306/tcp open|filtered mysql
MAC Address: 02:42:0A:06:06:0E (Unknown)

Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.0000030s latency).
Not shown: 994 closed tcp ports (reset)
PORT    STATE         SERVICE
21/tcp  open|filtered ftp
22/tcp  open|filtered ssh
53/tcp  open|filtered domain
80/tcp  open|filtered http
139/tcp open|filtered netbios-ssn
445/tcp open|filtered microsoft-ds
MAC Address: 02:42:0A:06:06:17 (Unknown)

Nmap scan report for 10.6.6.100
Host is up (0.0000020s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE         SERVICE
80/tcp open|filtered http
MAC Address: 02:42:0A:06:06:64 (Unknown)
```

Are there any potential target computers on this subnet running SMB services? Which computer or computers? How do you know? Yes, 10.6.6.23. It has ports 139 and 445 open

----

I did further enum on Ports 139 and 445 using nmap –sV 172.17.0.2

The respective ports with the versions are shown Samba smbd 3.x -4.x



```
┌──(root㉿Kali)-[/home/kali]
└─# nmap -sV 172.17.0.2
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-20 14:20 UTC
Nmap scan report for metasploitable.vm (172.17.0.2)
Host is up (0.0000020s latency).
Not shown: 981 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:li
nux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.69 seconds

┌──(root㉿Kali)-[/home/kali]
└─#
```

Use enum4linux to enumerate users and network file shares.

Step 1: Perform an enum4linux scan on target 172.17.0.2.

In Part 1, Step 1c, you used the enum4linux help page to learn about the options available to enumerate potential targets. The most common options are: -U find configured users -S get a list of file shares -G get a list of the groups and their members -P list the password policies -i get a list of printers

Use the enum4linux -U option to list the users configured on the target 172.17.0.2. Remember that enum4linux commands require root permissions to execute.

```
┌──(root㉿kali)-[/home/kali] └─# enum4linux -U 172.17.0.2
```

The output of this command can generate multiple screens of information if many users are discovered. Enum4linux aggregates output from multiple Samba tools to produce a concise result.

```
enum4linux -U 172.17.0.2
```

Breakdown

enum4linux → SMB enumeration tool

-U → Enumerate user accounts

172.17.0.2 → Target IP address

What information it tries to retrieve:

If SMB allows it, this will attempt to list:

-Local Windows/Samba usernames

- Domain users (if the host is domain-joined)

-Users accessible via anonymous (null session) or guest access

Possible outcomes & what they mean

Users are listed

This usually means:

SMB allows anonymous enumeration

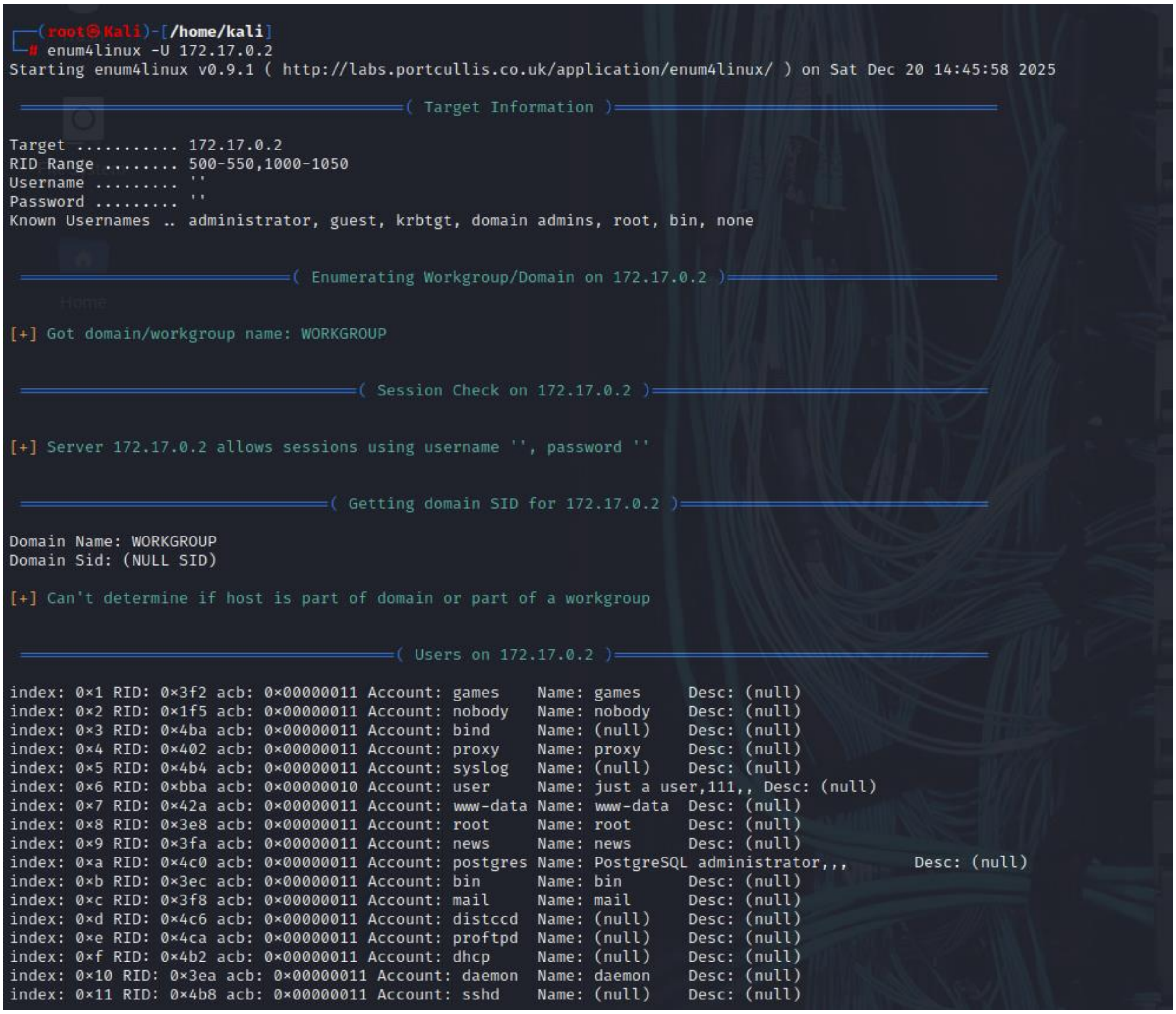
Weak or legacy SMB configuration

This is valuable for:

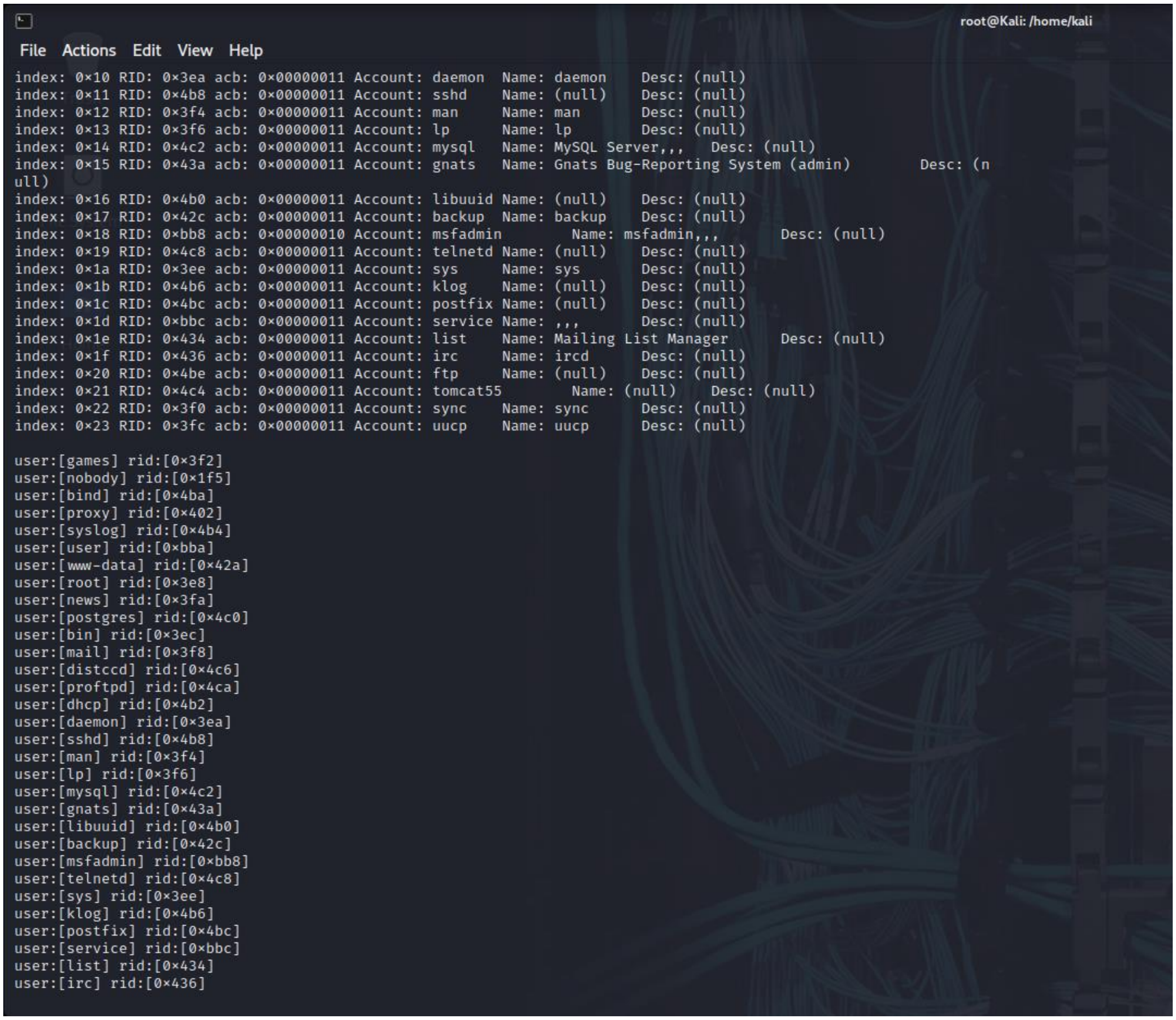
Password spraying

Brute-force attacks

Further privilege escalation



```
┌──(root㉿Kali)-[/home/kali]
└─# enum4linux -U 172.17.0.2
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Dec 20 14:45:58 2025

 ========================================( Target Information )========================================

Target ........... 172.17.0.2
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on 172.17.0.2 )============================


[+] Got domain/workgroup name: WORKGROUP


 ====================================( Session Check on 172.17.0.2 )====================================


[+] Server 172.17.0.2 allows sessions using username '', password ''


 =================================( Getting domain SID for 172.17.0.2 )=================================

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup


 ========================================( Users on 172.17.0.2 )========================================

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: 0x402 acb: 0x00000011 Account: proxy    Name: proxy     Desc: (null)
index: 0x5 RID: 0x4b4 acb: 0x00000011 Account: syslog   Name: (null)    Desc: (null)
index: 0x6 RID: 0xbba 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: 0×10 RID: 0×3ea acb: 0×00000011 Account: daemon  Name: daemon    Desc: (null)
index: 0×11 RID: 0×4b8 acb: 0×00000011 Account: sshd    Name: (null)    Desc: (null)
index: 0×12 RID: 0×3f4 acb: 0×00000011 Account: man     Name: man       Desc: (null)
index: 0×13 RID: 0×3f6 acb: 0×00000011 Account: lp      Name: lp        Desc: (null)
index: 0×14 RID: 0×4c2 acb: 0×00000011 Account: mysql   Name: MySQL Server,,,   Desc: (null)
index: 0×15 RID: 0×43a acb: 0×00000011 Account: gnats   Name: Gnats Bug-Reporting System (admin)        Desc: (n
ull)
index: 0×16 RID: 0×4b0 acb: 0×00000011 Account: libuuid Name: (null)    Desc: (null)
index: 0×17 RID: 0×42c acb: 0×00000011 Account: backup  Name: backup    Desc: (null)
index: 0×18 RID: 0×bb8 acb: 0×00000010 Account: msfadmin        Name: msfadmin,,,       Desc: (null)
index: 0×19 RID: 0×4c8 acb: 0×00000011 Account: telnetd Name: (null)    Desc: (null)
index: 0×1a RID: 0×3ee acb: 0×00000011 Account: sys     Name: sys       Desc: (null)
index: 0×1b RID: 0×4b6 acb: 0×00000011 Account: klog    Name: (null)    Desc: (null)
index: 0×1c RID: 0×4bc acb: 0×00000011 Account: postfix Name: (null)    Desc: (null)
index: 0×1d RID: 0×bbc acb: 0×00000011 Account: service Name: ,,,       Desc: (null)
index: 0×1e RID: 0×434 acb: 0×00000011 Account: list    Name: Mailing List Manager      Desc: (null)
index: 0×1f RID: 0×436 acb: 0×00000011 Account: irc     Name: ircd      Desc: (null)
index: 0×20 RID: 0×4be acb: 0×00000011 Account: ftp     Name: (null)    Desc: (null)
index: 0×21 RID: 0×4c4 acb: 0×00000011 Account: tomcat55        Name: (null)    Desc: (null)
index: 0×22 RID: 0×3f0 acb: 0×00000011 Account: sync    Name: sync      Desc: (null)
index: 0×23 RID: 0×3fc acb: 0×00000011 Account: uucp    Name: uucp      Desc: (null)

user:[games] rid:[0×3f2]
user:[nobody] rid:[0×1f5]
user:[bind] rid:[0×4ba]
user:[proxy] rid:[0×402]
user:[syslog] rid:[0×4b4]
user:[user] rid:[0×bba]
user:[www-data] rid:[0×42a]
user:[root] rid:[0×3e8]
user:[news] rid:[0×3fa]
user:[postgres] rid:[0×4c0]
user:[bin] rid:[0×3ec]
user:[mail] rid:[0×3f8]
user:[distccd] rid:[0×4c6]
user:[proftpd] rid:[0×4ca]
user:[dhcp] rid:[0×4b2]
user:[daemon] rid:[0×3ea]
user:[sshd] rid:[0×4b8]
user:[man] rid:[0×3f4]
user:[lp] rid:[0×3f6]
user:[mysql] rid:[0×4c2]
user:[gnats] rid:[0×43a]
user:[libuuid] rid:[0×4b0]
user:[backup] rid:[0×42c]
user:[msfadmin] rid:[0×bb8]
user:[telnetd] rid:[0×4c8]
user:[sys] rid:[0×3ee]
user:[klog] rid:[0×4b6]
user:[postfix] rid:[0×4bc]
user:[service] rid:[0×bbc]
user:[list] rid:[0×434]
user:[irc] rid:[0×436]
```

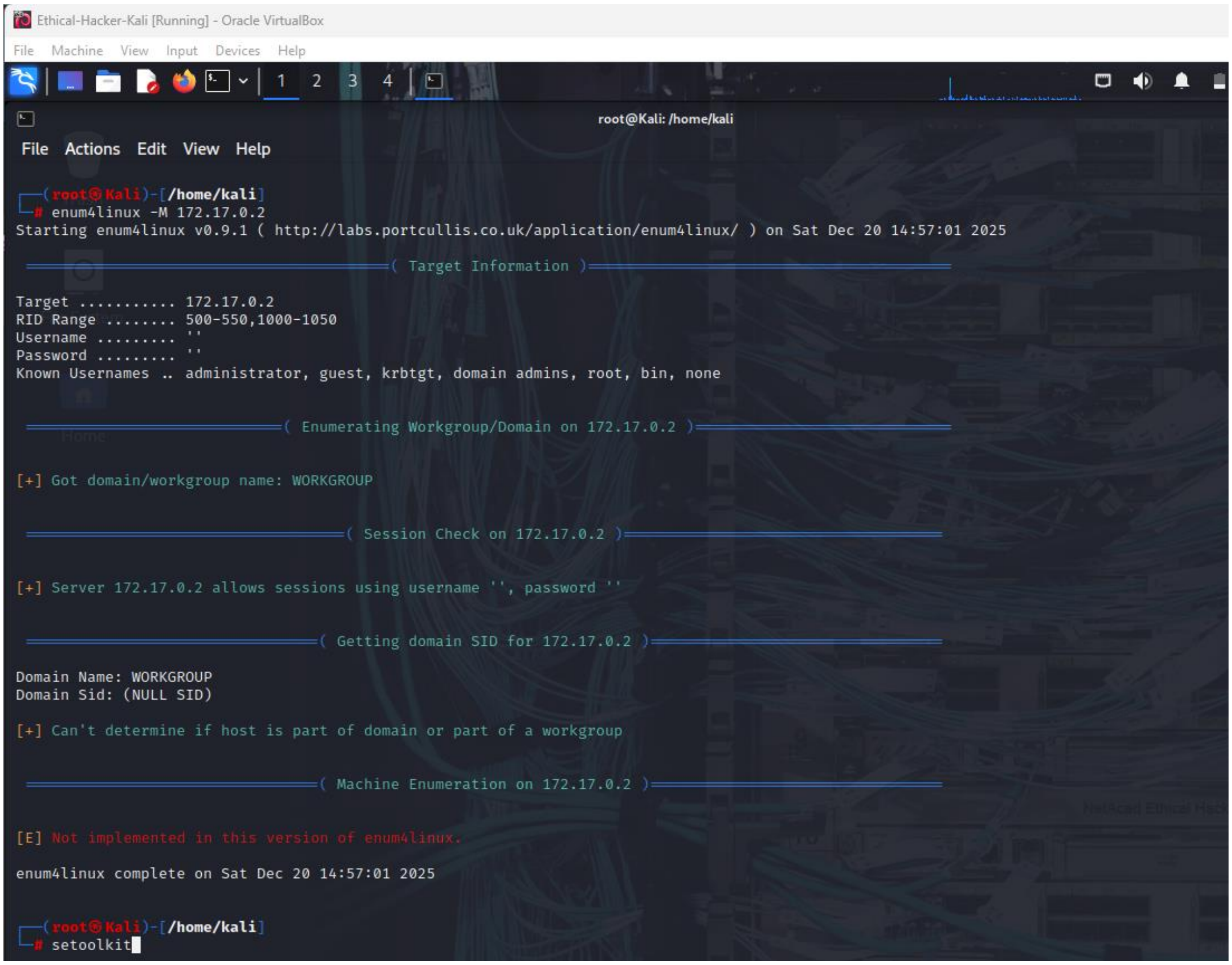
----

enum4linux -M 172.17.0.2

What -M tries to enumerate

The `-M` option attempts to gather **machine-level information**, such as:

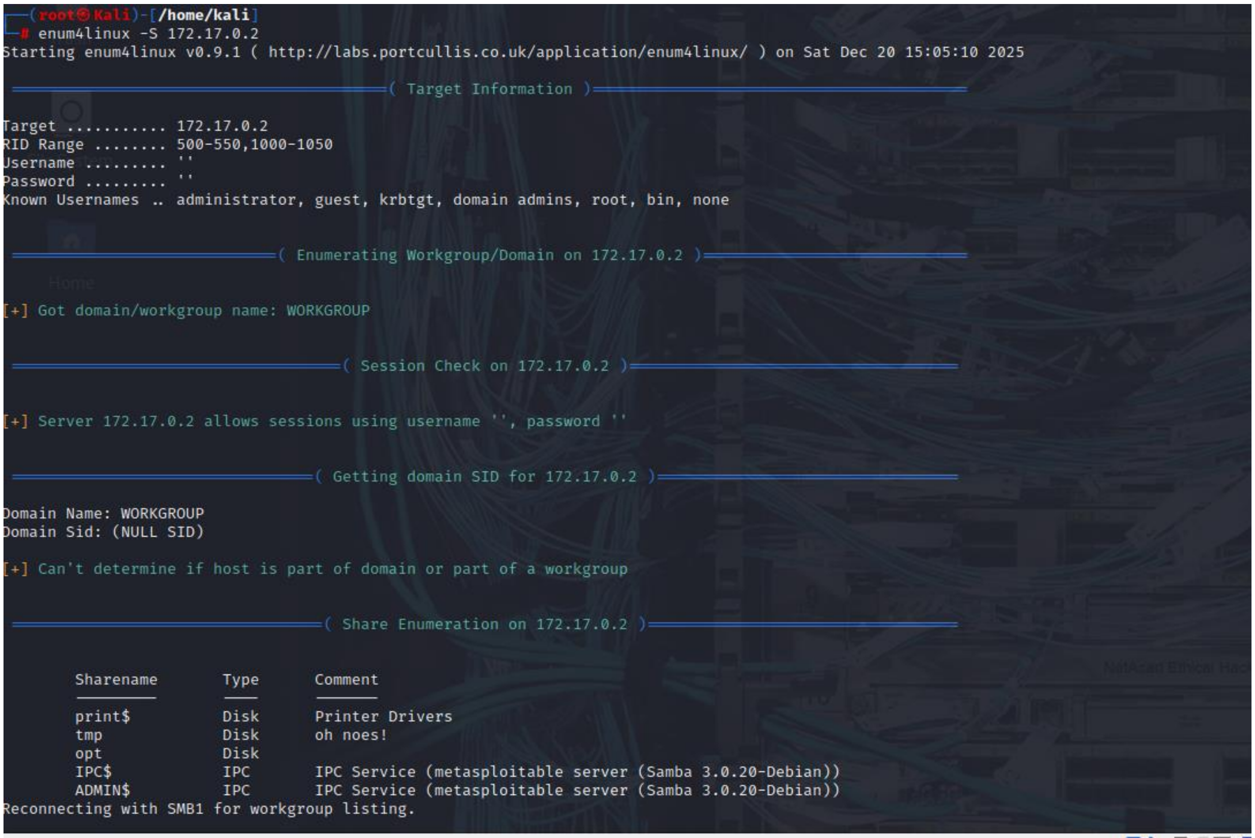
- Computer / machine name
- Domain or workgroup membership
- Machine account details
- Trust relationships (if any)
- □ Domain SID (Security Identifie


Ethical-Hacker-Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
root@Kali: /home/kali
File Actions Edit View Help

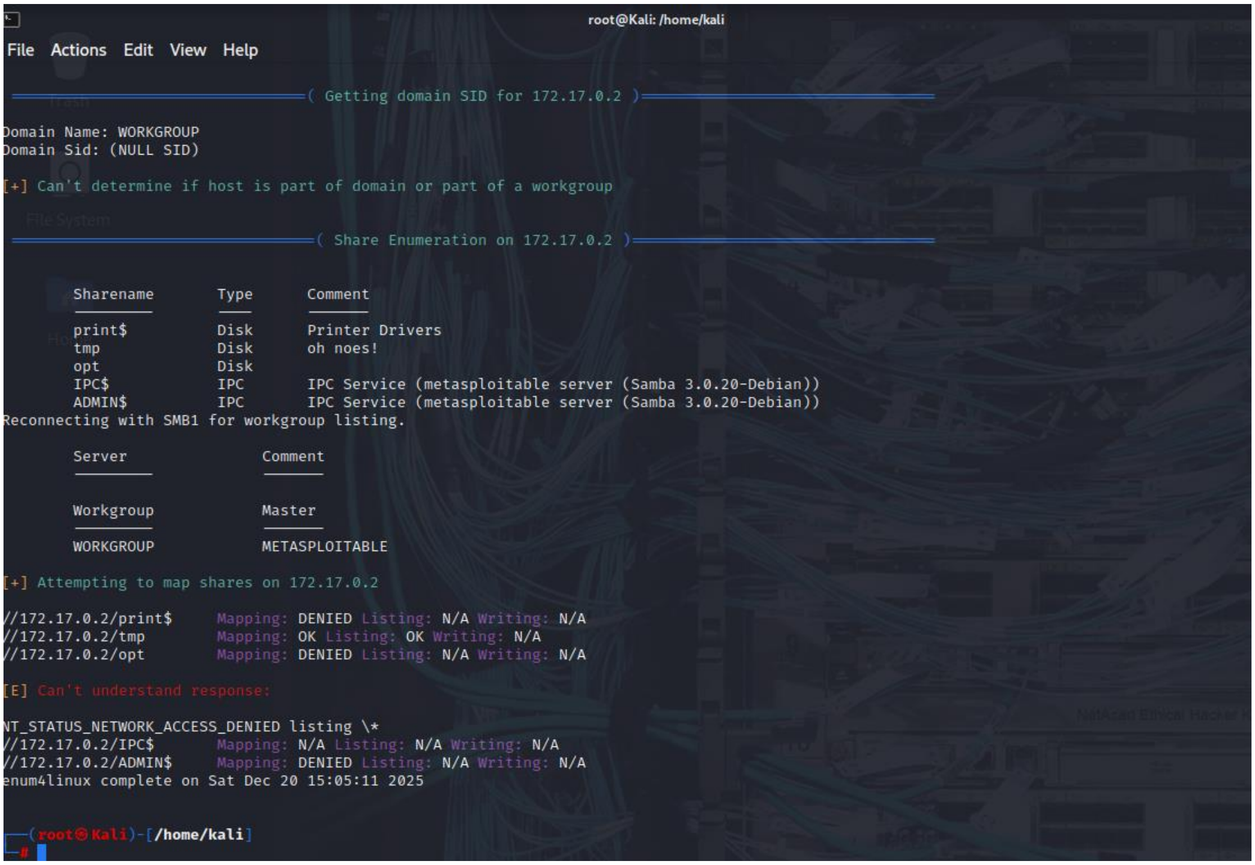
```
┌──(root㉿Kali)-[/home/kali]
└─# enum4linux -M 172.17.0.2
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Dec 20 14:57:01 2025

 ==========================( Target Information )==========================

Target ........... 172.17.0.2
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

 ===================( Enumerating Workgroup/Domain on 172.17.0.2 )===================

[+] Got domain/workgroup name: WORKGROUP

 ======================( Session Check on 172.17.0.2 )======================

[+] Server 172.17.0.2 allows sessions using username '', password ''

 ====================( Getting domain SID for 172.17.0.2 )====================

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup

 ====================( Machine Enumeration on 172.17.0.2 )====================

[E] Not implemented in this version of enum4linux.

enum4linux complete on Sat Dec 20 14:57:01 2025

┌──(root㉿Kali)-[/home/kali]
└─# setoolkit
```

Enumerate SMB shares - This check **what folders/services are exposed over SMB**, and whether they are accessible anonymous.

enum4linux - S 172.17.0.2



```
┌──(root㉿Kali)-[/home/kali]
└─# enum4linux -S 172.17.0.2
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Dec 20 15:05:10 2025

 ==========================================( Target Information )==========================================

Target ........... 172.17.0.2
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ==============================( Enumerating Workgroup/Domain on 172.17.0.2 )==============================


[+] Got domain/workgroup name: WORKGROUP


 ==================================( Session Check on 172.17.0.2 )==================================


[+] Server 172.17.0.2 allows sessions using username '', password ''


 ===============================( Getting domain SID for 172.17.0.2 )===============================

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup


 ================================( Share Enumeration on 172.17.0.2 )================================


        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.
```



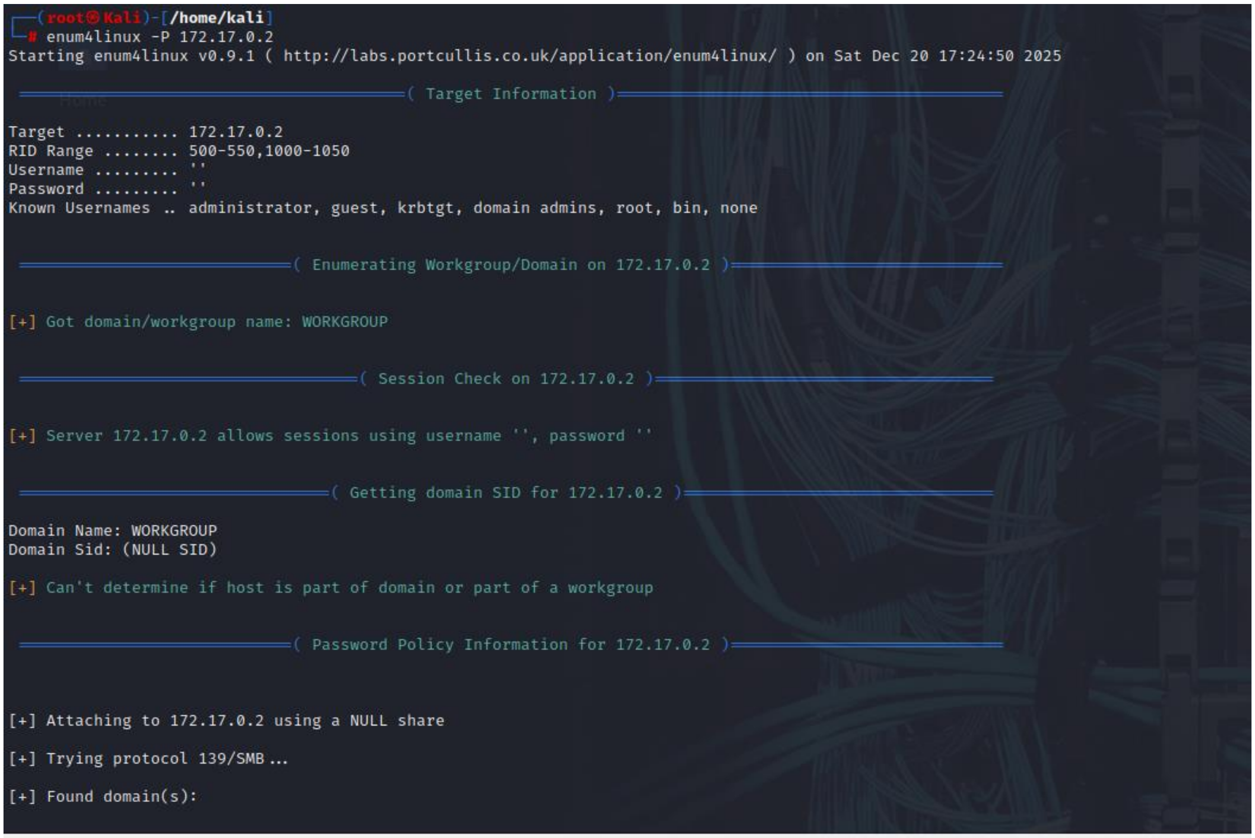
```
 ===============================( Getting domain SID for 172.17.0.2 )===============================

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup


 ================================( Share Enumeration on 172.17.0.2 )================================


        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 172.17.0.2

//172.17.0.2/print$     Mapping: DENIED Listing: N/A Writing: N/A
//172.17.0.2/tmp        Mapping: OK Listing: OK Writing: N/A
//172.17.0.2/opt        Mapping: DENIED Listing: N/A Writing: N/A

[E] Can't understand response:

NT_STATUS_NETWORK_ACCESS_DENIED listing \*
//172.17.0.2/IPC$       Mapping: N/A Listing: N/A Writing: N/A
//172.17.0.2/ADMIN$     Mapping: DENIED Listing: N/A Writing: N/A
enum4linux complete on Sat Dec 20 15:05:11 2025


┌──(root㉿Kali)-[/home/kali]
└─#
```

The **-P flag enumerates the SMB password policy** of the target system.

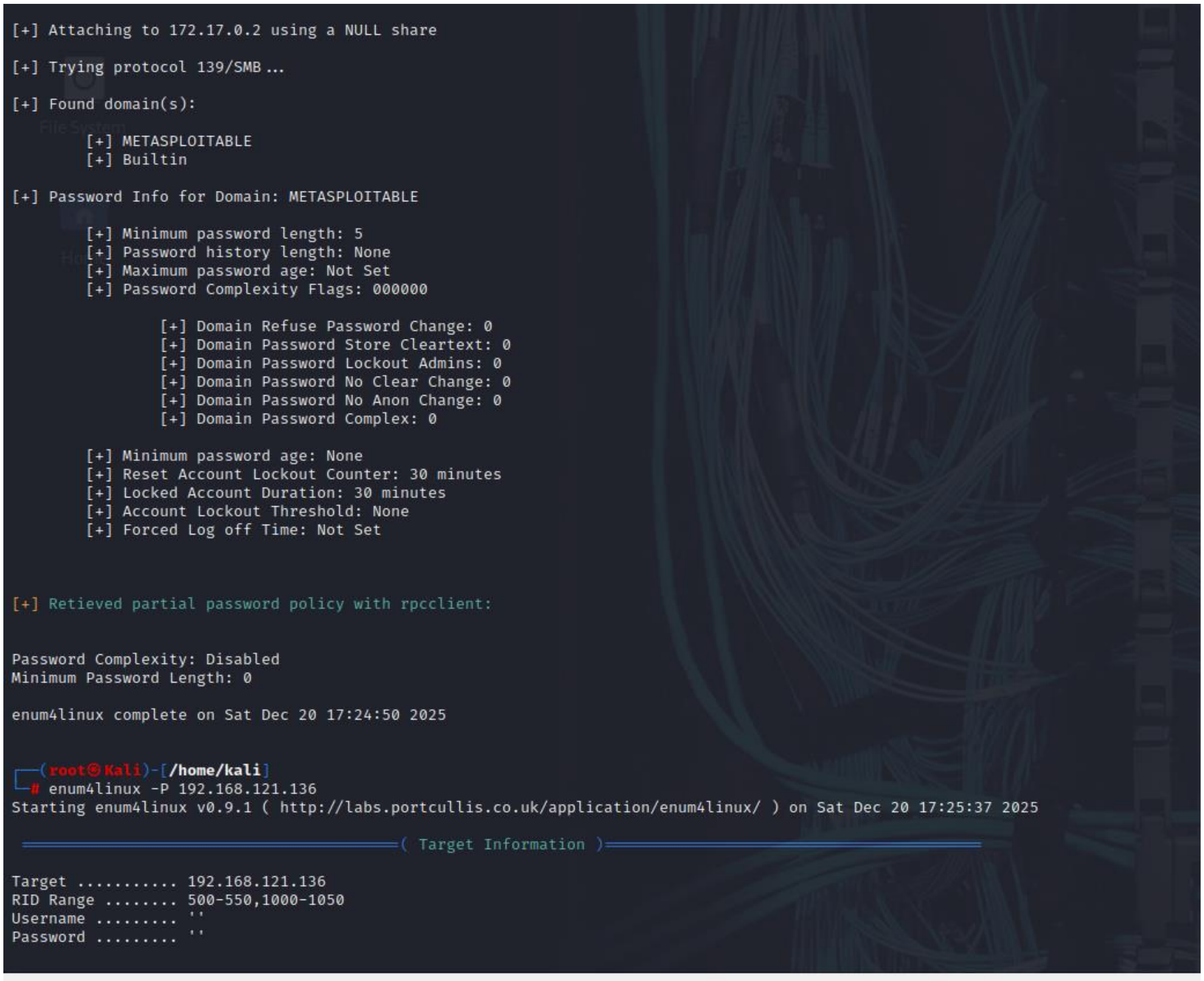
enum4linux - P 172.17.0.2

If allowed, it will show things like:

- **Minimum password length**
- **Maximum password age**
- **Password history length**
- **Account lockout threshold**
- **Lockout duration**
- **Whether complexity is enforced**



```
┌──(root㉿Kali)-[/home/kali]
└─# enum4linux -P 172.17.0.2
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Dec 20 17:24:50 2025

 ========================================( Target Information )========================================

Target ........... 172.17.0.2
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on 172.17.0.2 )============================


[+] Got domain/workgroup name: WORKGROUP


 ===================================( Session Check on 172.17.0.2 )===================================


[+] Server 172.17.0.2 allows sessions using username '', password ''


 ================================( Getting domain SID for 172.17.0.2 )================================

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup


 ============================( Password Policy Information for 172.17.0.2 )============================



[+] Attaching to 172.17.0.2 using a NULL share

[+] Trying protocol 139/SMB ...

[+] Found domain(s):
```

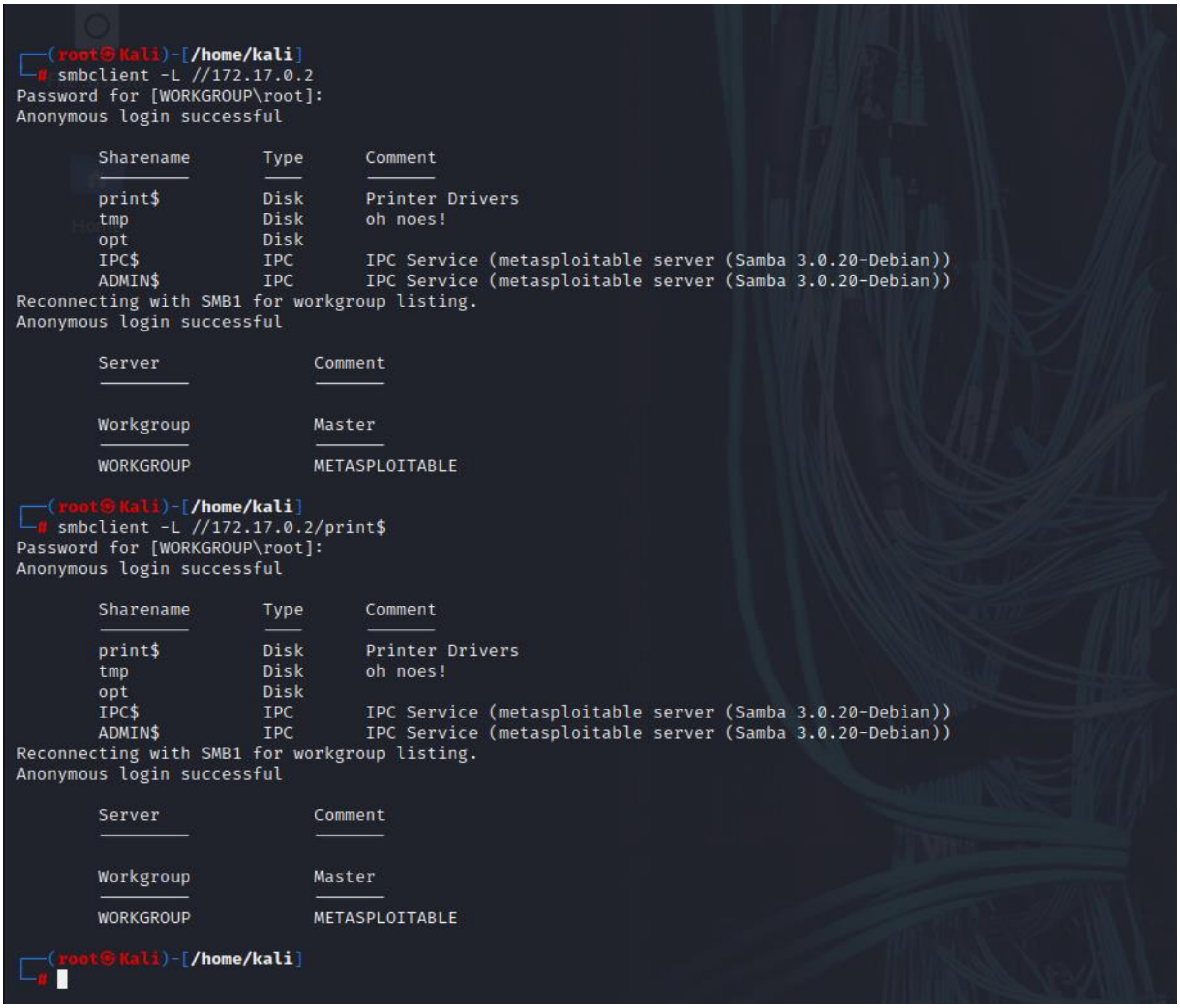


```
[+] Attaching to 172.17.0.2 using a NULL share

[+] Trying protocol 139/SMB ...

[+] Found domain(s):

        [+] METASPLOITABLE
        [+] Builtin

[+] Password Info for Domain: METASPLOITABLE

        [+] Minimum password length: 5
        [+] Password history length: None
        [+] Maximum password age: Not Set
        [+] Password Complexity Flags: 000000

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 0

        [+] Minimum password age: None
        [+] Reset Account Lockout Counter: 30 minutes
        [+] Locked Account Duration: 30 minutes
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: Not Set



[+] Retieved partial password policy with rpcclient:


Password Complexity: Disabled
Minimum Password Length: 0

enum4linux complete on Sat Dec 20 17:24:50 2025


┌──(root㉿Kali)-[/home/kali]
└─# enum4linux -P 192.168.121.136
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Dec 20 17:25:37 2025

 ========================================( Target Information )========================================

Target ........... 192.168.121.136
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
```

Access SMB Shares with SMBClient

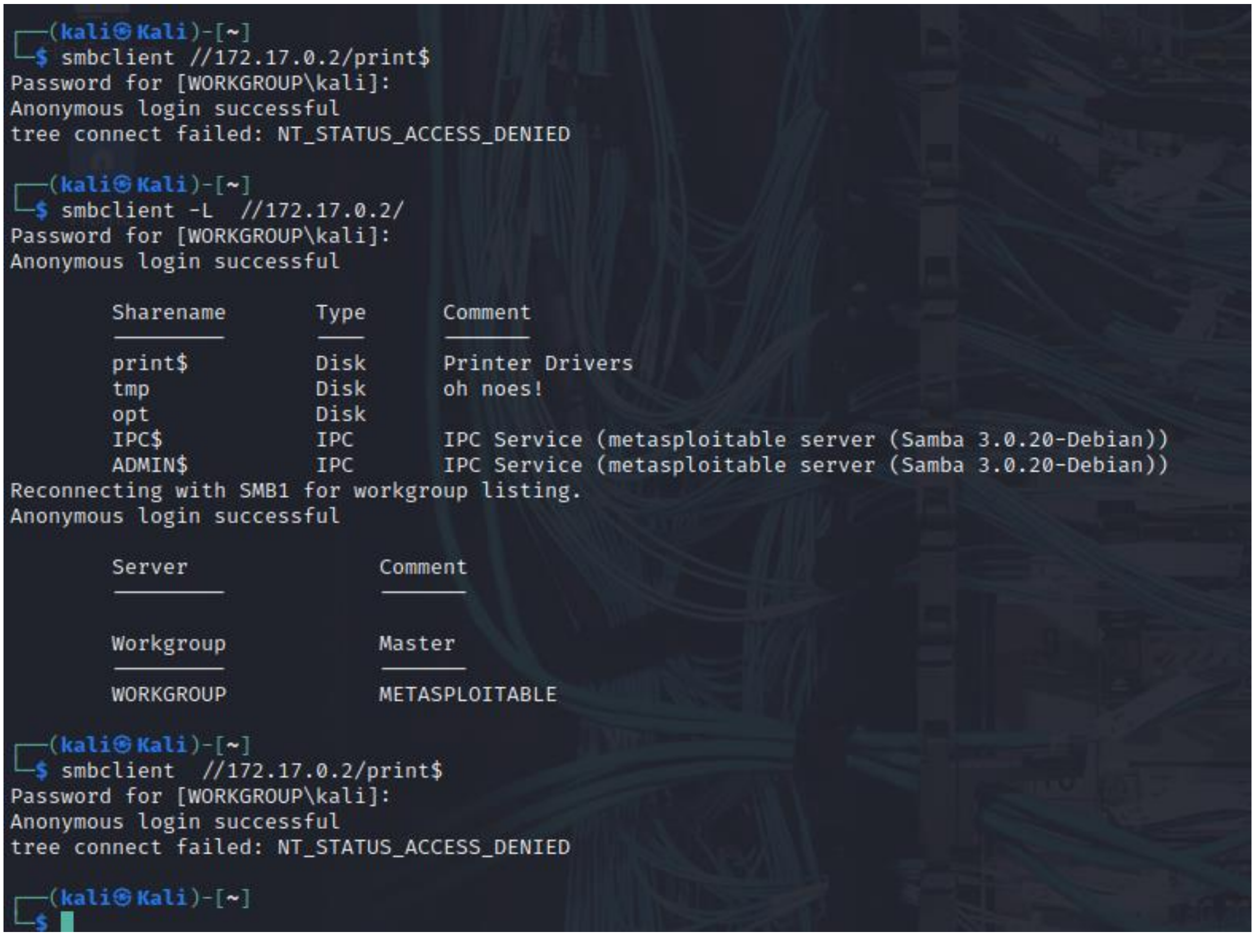
`smbclient` is a command-line tool (like FTP for SMB) that lets you **list, connect to, and browse SMB share**

Using –L - list all available shares on the remote server



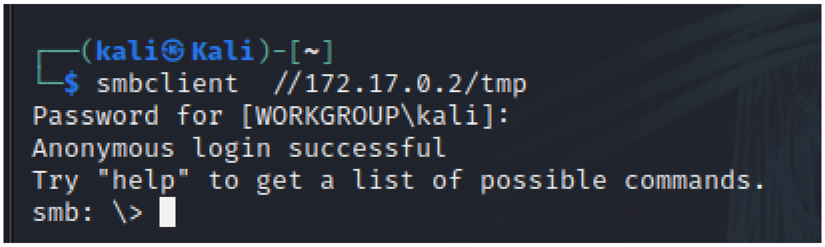
```
┌──(root㉿Kali)-[/home/kali]
└─# smbclient -L //172.17.0.2
Password for [WORKGROUP\root]:
Anonymous login successful

        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.
Anonymous login successful

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            METASPLOITABLE

┌──(root㉿Kali)-[/home/kali]
└─# smbclient -L //172.17.0.2/print$
Password for [WORKGROUP\root]:
Anonymous login successful

        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.
Anonymous login successful

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            METASPLOITABLE

┌──(root㉿Kali)-[/home/kali]
└─# 
```

Accessing the print$ server – access was denied



```
┌──(kali㉿Kali)-[~]
└─$ smbclient //172.17.0.2/print$
Password for [WORKGROUP\kali]:
Anonymous login successful
tree connect failed: NT_STATUS_ACCESS_DENIED

┌──(kali㉿Kali)-[~]
└─$ smbclient -L  //172.17.0.2/
Password for [WORKGROUP\kali]:
Anonymous login successful

        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.
Anonymous login successful

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            METASPLOITABLE

┌──(kali㉿Kali)-[~]
└─$ smbclient  //172.17.0.2/print$
Password for [WORKGROUP\kali]:
Anonymous login successful
tree connect failed: NT_STATUS_ACCESS_DENIED

┌──(kali㉿Kali)-[~]
└─$ 
```

Then I tried accessing tmp server – accessing was granted and got connected to smb



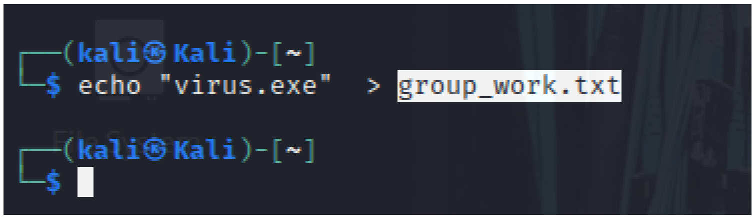
```
┌──(kali㉿Kali)-[~]
└─$ smbclient  //172.17.0.2/tmp
Password for [WORKGROUP\kali]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> 
```

Open a new terminal and enter echo “virus.exe” > group_work.txt

This command does the following:

- `echo "virus.exe"`: prints the string `virus.exe` to the terminal.
- `>`: redirects that output into a file.
- `group_work.txt`: is the file being created or overwritten.

So the result is a new file named `group_work.txt` containing just the text:



```
┌──(kali㉿Kali)-[~]
└─$ echo "virus.exe"  > group_work.txt

┌──(kali㉿Kali)-[~]
└─$ 
```

Then connect to smbclient - smbclient //172.17.0.2/tmp -N

Enter login details

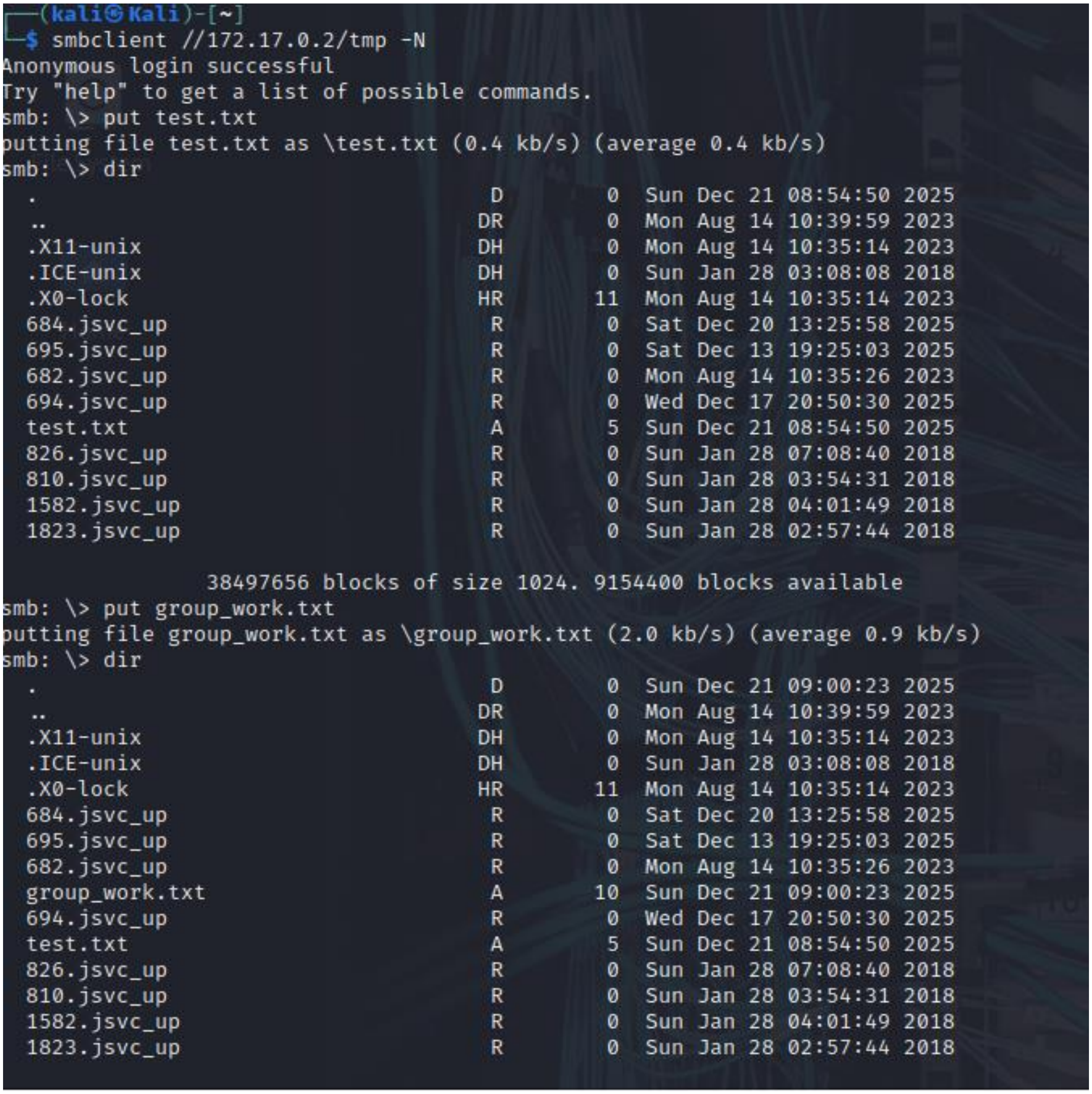
In prompt smb> enter put group_work.txt

This command is executed **inside an active** `smbclient` **session**

- SMB client **upload** the file `group_work.txt` from **local Kali machine** to the **remote SMB share** (in this case, `//172.17.0.2/tmp`).
- If successful, the file will appear in the shared folder on the remote server.

Enter dir to see the file uploaded.

This confirms that the share allows **anonymous write operations,** a major misconfiguration in real-world environments and a key finding in penetration testing lab



```
┌──(kali㉿Kali)-[~]
└─$ smbclient //172.17.0.2/tmp -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> put test.txt
putting file test.txt as \test.txt (0.4 kb/s) (average 0.4 kb/s)
smb: \> dir
  .                                   D        0  Sun Dec 21 08:54:50 2025
  ..                                 DR        0  Mon Aug 14 10:39:59 2023
  .X11-unix                          DH        0  Mon Aug 14 10:35:14 2023
  .ICE-unix                          DH        0  Sun Jan 28 03:08:08 2018
  .X0-lock                           HR       11  Mon Aug 14 10:35:14 2023
  684.jsvc_up                         R        0  Sat Dec 20 13:25:58 2025
  695.jsvc_up                         R        0  Sat Dec 13 19:25:03 2025
  682.jsvc_up                         R        0  Mon Aug 14 10:35:26 2023
  694.jsvc_up                         R        0  Wed Dec 17 20:50:30 2025
  test.txt                            A        5  Sun Dec 21 08:54:50 2025
  826.jsvc_up                         R        0  Sun Jan 28 07:08:40 2018
  810.jsvc_up                         R        0  Sun Jan 28 03:54:31 2018
  1582.jsvc_up                        R        0  Sun Jan 28 04:01:49 2018
  1823.jsvc_up                        R        0  Sun Jan 28 02:57:44 2018

                38497656 blocks of size 1024. 9154400 blocks available
smb: \> put group_work.txt
putting file group_work.txt as \group_work.txt (2.0 kb/s) (average 0.9 kb/s)
smb: \> dir
  .                                   D        0  Sun Dec 21 09:00:23 2025
  ..                                 DR        0  Mon Aug 14 10:39:59 2023
  .X11-unix                          DH        0  Mon Aug 14 10:35:14 2023
  .ICE-unix                          DH        0  Sun Jan 28 03:08:08 2018
  .X0-lock                           HR       11  Mon Aug 14 10:35:14 2023
  684.jsvc_up                         R        0  Sat Dec 20 13:25:58 2025
  695.jsvc_up                         R        0  Sat Dec 13 19:25:03 2025
  682.jsvc_up                         R        0  Mon Aug 14 10:35:26 2023
  group_work.txt                      A       10  Sun Dec 21 09:00:23 2025
  694.jsvc_up                         R        0  Wed Dec 17 20:50:30 2025
  test.txt                            A        5  Sun Dec 21 08:54:50 2025
  826.jsvc_up                         R        0  Sun Jan 28 07:08:40 2018
  810.jsvc_up                         R        0  Sun Jan 28 03:54:31 2018
  1582.jsvc_up                        R        0  Sun Jan 28 04:01:49 2018
  1823.jsvc_up                        R        0  Sun Jan 28 02:57:44 2018
```