Scanning for SMB Vulnerabilities with enum4linux

Objectives

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.

In this lab, you will complete the following objectives:

- 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.

Background / Scenario

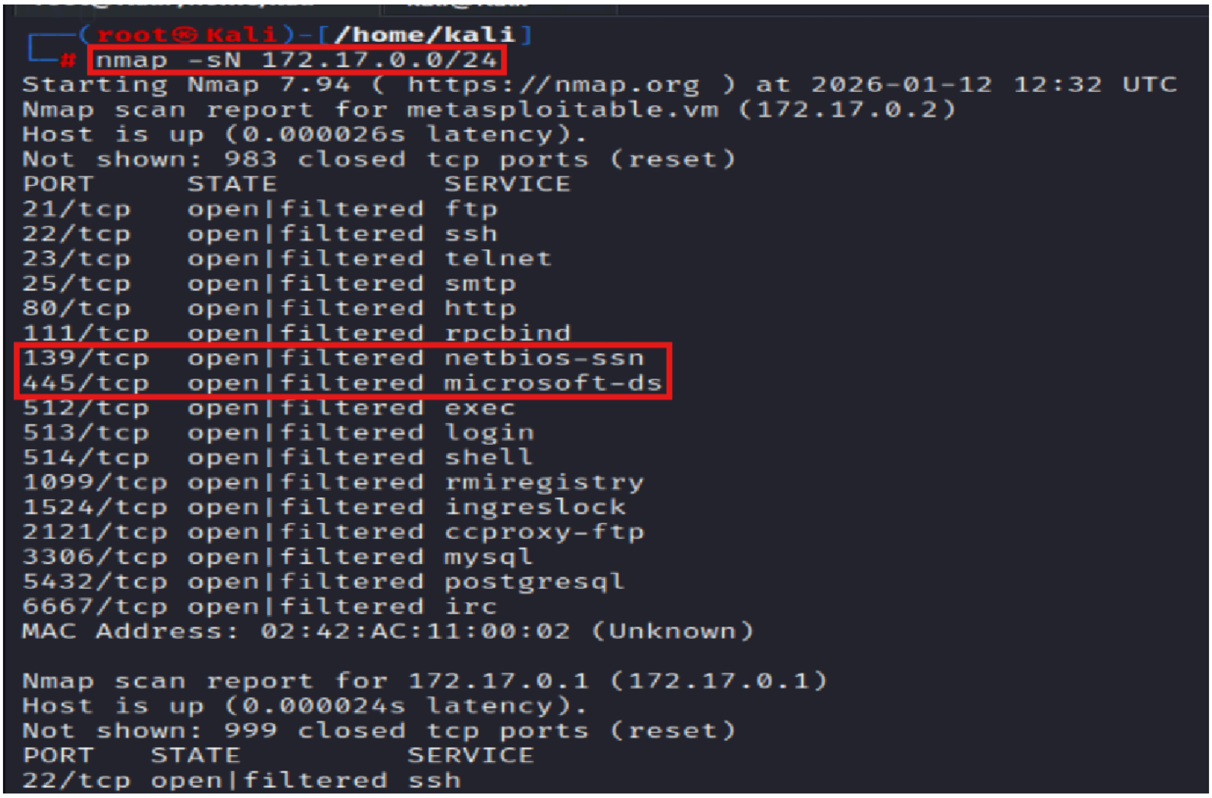
Poorly secured and managed Windows server networks are a huge security risk. Penetration testers must uncover any vulnerabilities in file and print sharing functions that can leave an organization vulnerable to attack. In this activity, you will explore the capabilities of the enum4linux tool to enumerate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

Part 1: Launch enum4linux and explore its capabilities.

Most enum4linux commands must be run as root, so use the **sudo su** command to obtain persistent root access.

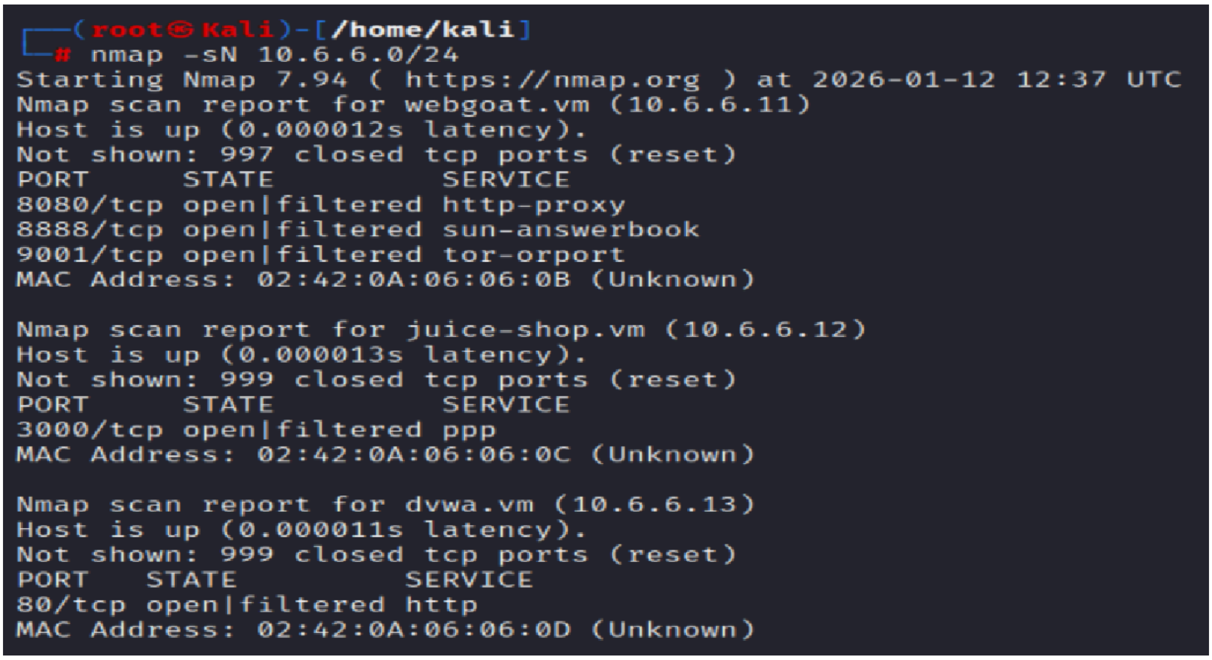
Part 2: Use Nmap to Find SMB Servers.

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.

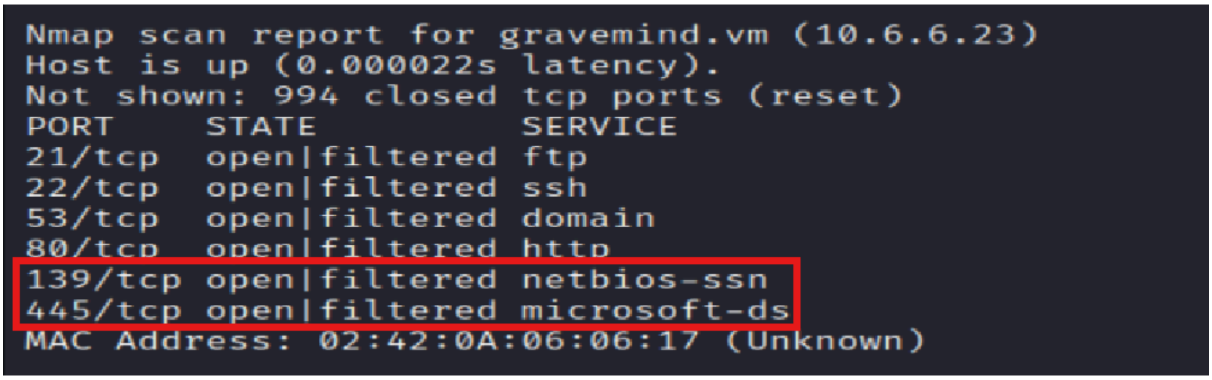


```
┌──(root㉿Kali)-[/home/kali]
└─# nmap -sN 172.17.0.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2026-01-12 12:32 UTC
Nmap scan report for metasploitable.vm (172.17.0.2)
Host is up (0.000026s latency).
Not shown: 983 closed tcp ports (reset)
PORT     STATE         SERVICE
21/tcp   open|filtered 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 (172.17.0.1)
Host is up (0.000024s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE         SERVICE
22/tcp open|filtered ssh
```

- Conduct a **nmap -sN** scan on the **10.6.6.0/24** subnet.



```
┌──(root㉿Kali)-[/home/kali]
└─# nmap -sN 10.6.6.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2026-01-12 12:37 UTC
Nmap scan report for webgoat.vm (10.6.6.11)
Host is up (0.000012s 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 (0.000013s 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 (0.000011s 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)
```



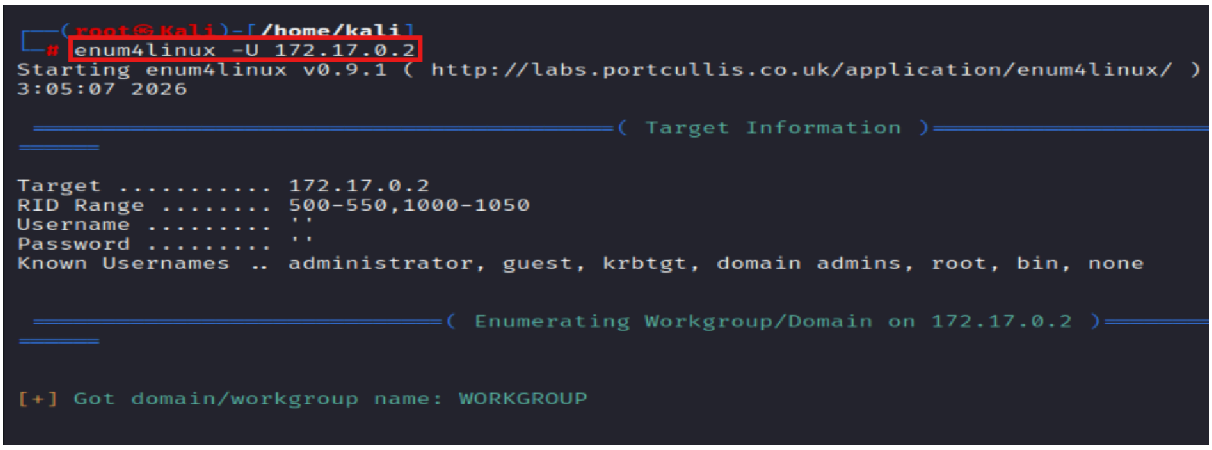
```
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.000022s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
53/tcp   open|filtered domain
80/tcp   open|filtered http
139/tcp  open|filtered netbios-ssn
445/tcp  open|filtered microsoft-ds
MAC Address: 02:42:0A:06:06:17 (Unknown)
```

Part 3: Use enum4linux to enumerate users and network file shares.

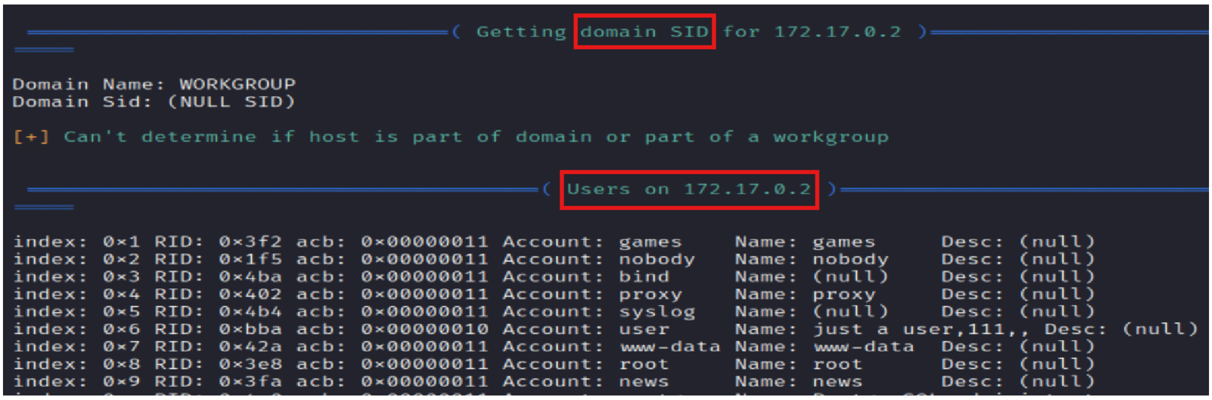
In this part, you will use enum4linux to discover more information about the two potential targets.

Perform an enum4linux scan on target 172.17.0.2.

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.

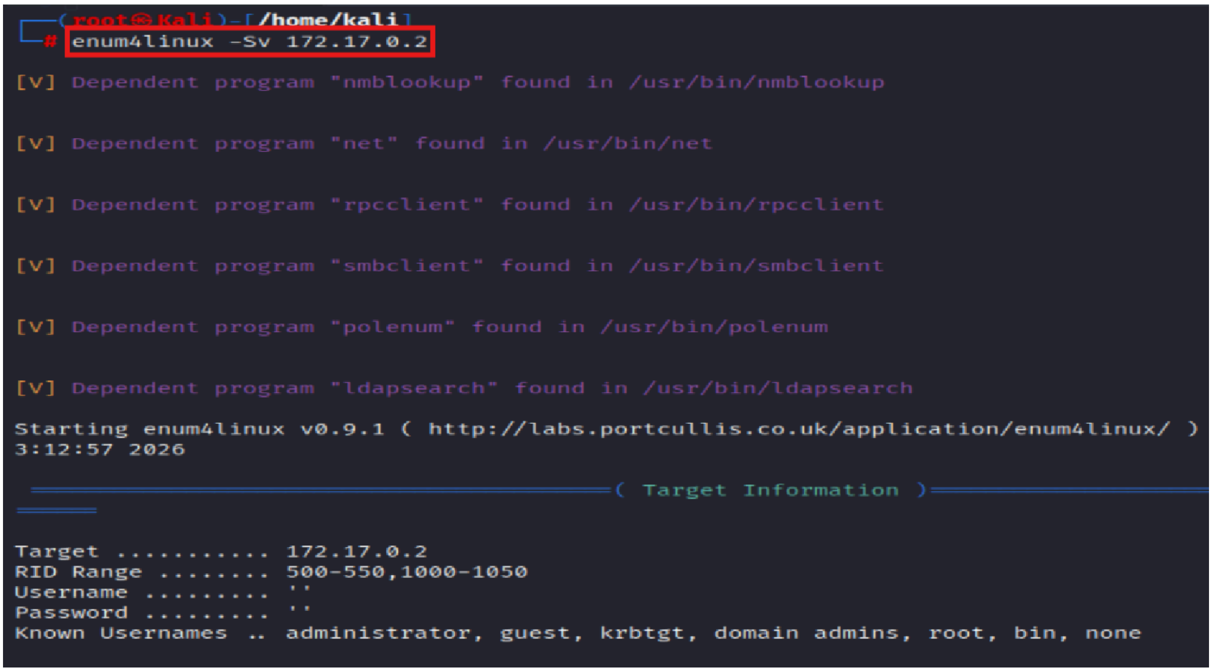


```
┌──(root㉿Kali)-[/home/kali]
└─# enum4linux -U 172.17.0.2
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ )
3:05:07 2026

 =========================================( 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
```

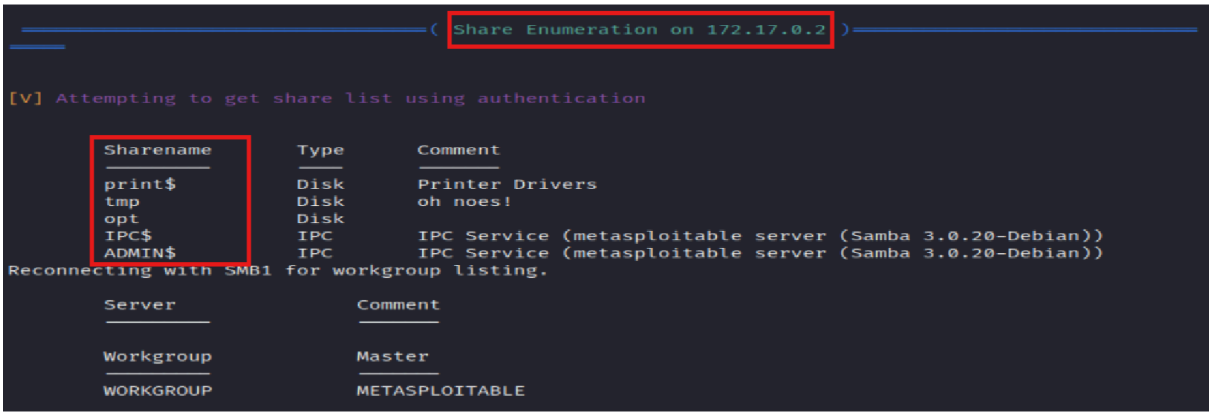


```
 ==============================( Getting domain SID for 172.17.0.2 )==============================

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)
```

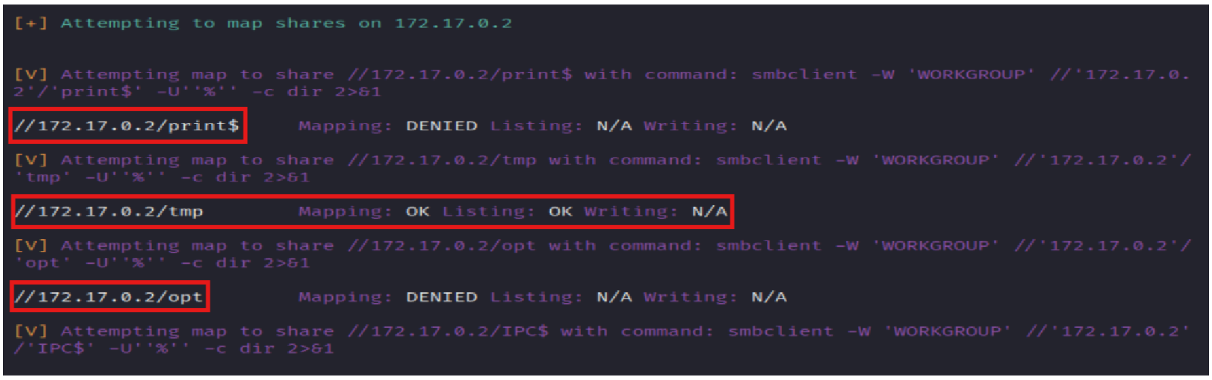
- List the file shares available on 172.17.0.2 using the **enum4linux -S** command. Use the verbose option to see the Samba tools that are used to obtain the information.



```
┌──(root㉿Kali)-[/home/kali]
└─# enum4linux -Sv 172.17.0.2
[V] Dependent program "nmblookup" found in /usr/bin/nmblookup

[V] Dependent program "net" found in /usr/bin/net

[V] Dependent program "rpcclient" found in /usr/bin/rpcclient

[V] Dependent program "smbclient" found in /usr/bin/smbclient

[V] Dependent program "polenum" found in /usr/bin/polenum

[V] Dependent program "ldapsearch" found in /usr/bin/ldapsearch

Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ )
3:12:57 2026

 ==========================================( 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
```

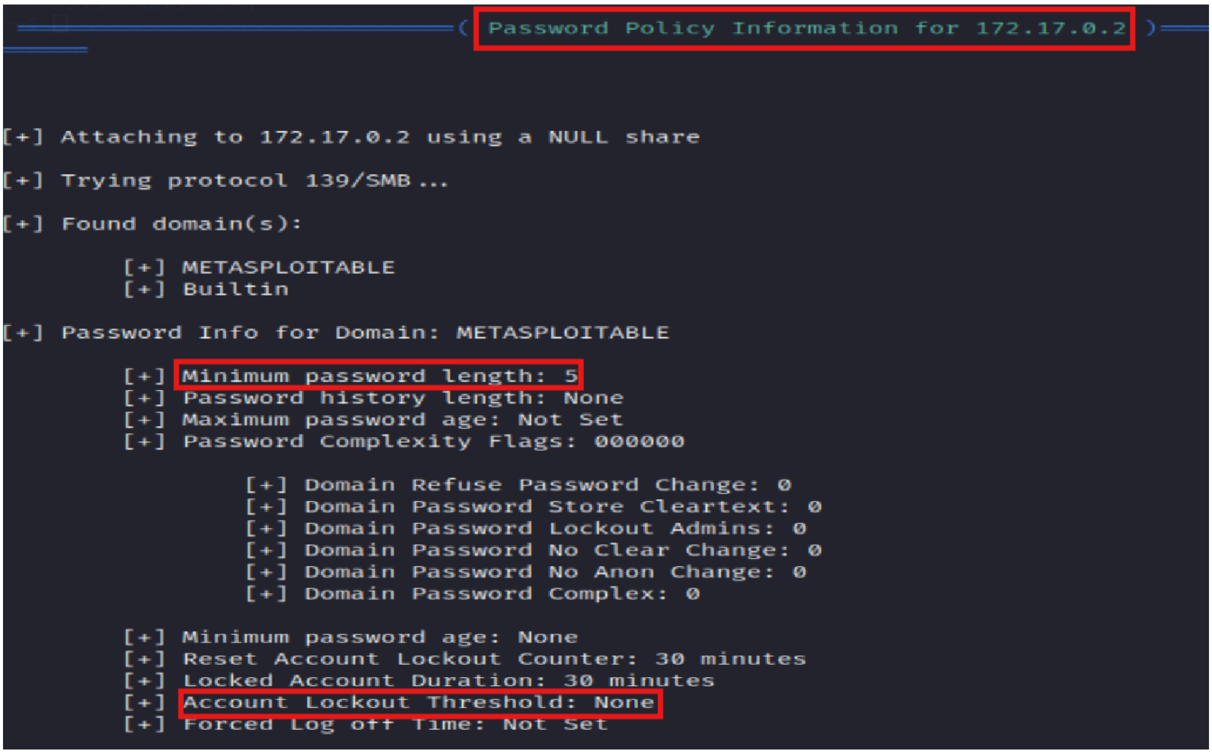


```
 ==========================================( Share Enumeration on 172.17.0.2 )==========
=====

[V] Attempting to get share list using authentication

        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

[V] Attempting map to share //172.17.0.2/print$ with command: smbclient -W 'WORKGROUP' //'172.17.0.
2'/'print$' -U''%'' -c dir 2>&1

//172.17.0.2/print$     Mapping: DENIED Listing: N/A Writing: N/A

[V] Attempting map to share //172.17.0.2/tmp with command: smbclient -W 'WORKGROUP' //'172.17.0.2'/
'tmp' -U''%'' -c dir 2>&1

//172.17.0.2/tmp        Mapping: OK Listing: OK Writing: N/A

[V] Attempting map to share //172.17.0.2/opt with command: smbclient -W 'WORKGROUP' //'172.17.0.2'/
'opt' -U''%'' -c dir 2>&1

//172.17.0.2/opt        Mapping: DENIED Listing: N/A Writing: N/A

[V] Attempting map to share //172.17.0.2/IPC$ with command: smbclient -W 'WORKGROUP' //'172.17.0.2'
/'IPC$' -U''%'' -c dir 2>&1
```

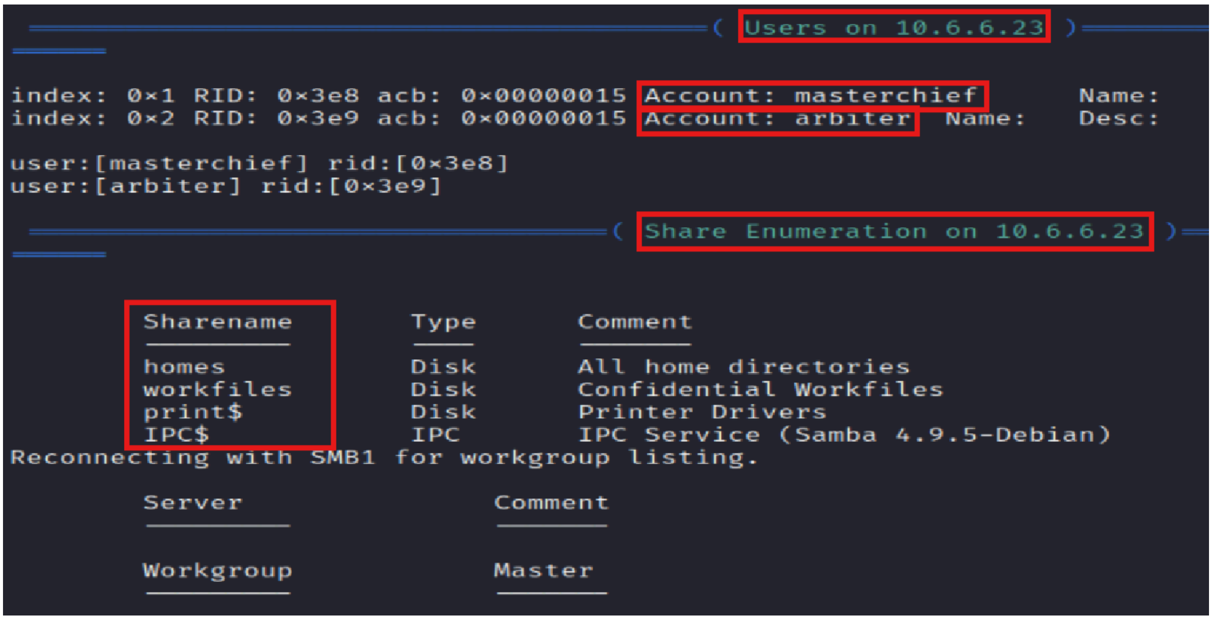
Penetration testers may not have uncovered a known username/password combination to further their exploit. In this case, they need to do a brute-force password attack to obtain the necessary credentials. It is a benefit to know the password policies in place on the target system to structure the brute-force effort. Use the **enum4linux -P** command to list the password policies.



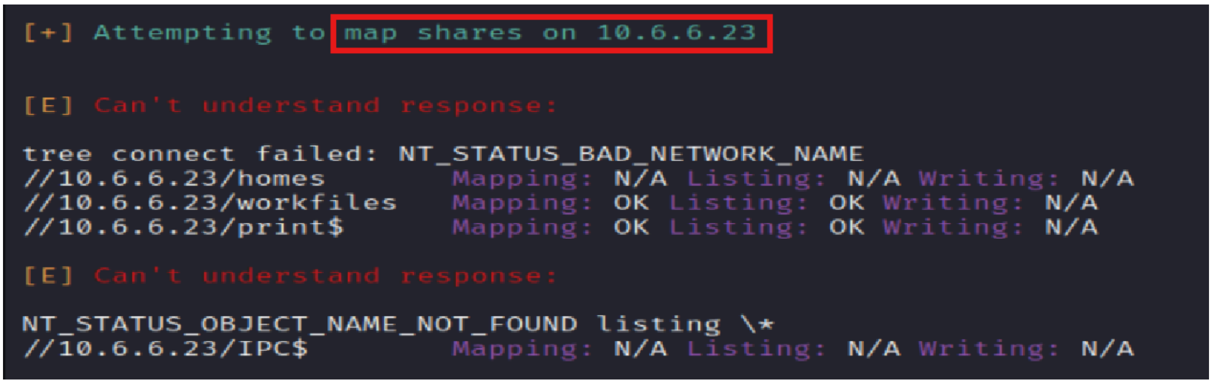
```
==========================( Password Policy Information for 172.17.0.2 )==========
=====


[+] Attaching to 172.17.0.2 using a NULL share

[+] Trying protocol 139/SMB ...

[+] Found domain(s):

        [+] 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
```

Perform a simple enumeration scan on target 10.6.6.23.

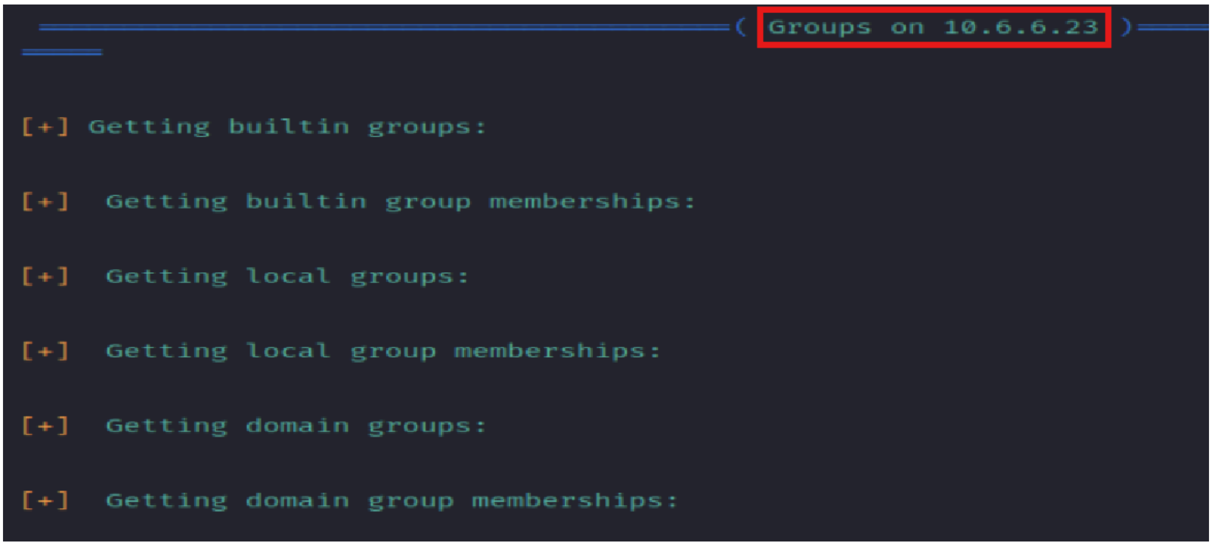
Enum4linux has an option that combines the -U, -S, -G, -P, -r, -o, -n, -i options into one command. This requires using the **-a** argument. This option quickly performs multiple SMB enumeration operations in one scan.



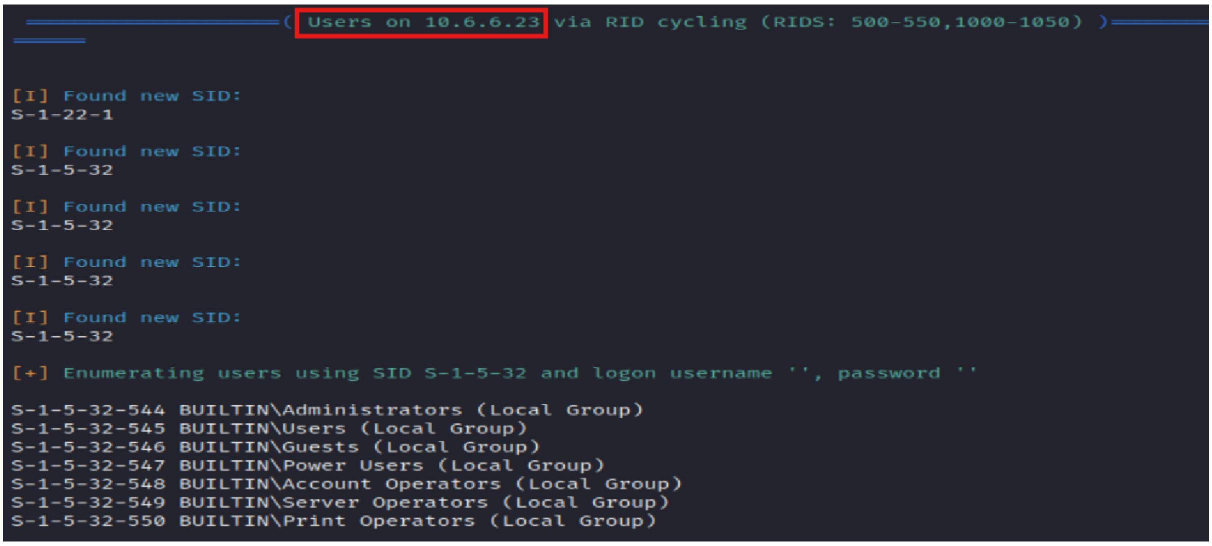
```
 ==================================( Users on 10.6.6.23 )==================================

index: 0x1 RID: 0x3e8 acb: 0x00000015 Account: masterchief     Name:
index: 0x2 RID: 0x3e9 acb: 0x00000015 Account: arbiter   Name:    Desc:

user:[masterchief] rid:[0x3e8]
user:[arbiter] rid:[0x3e9]

 ==================================( Share Enumeration on 10.6.6.23 )==================================


        Sharename       Type      Comment
        ---------       ----      -------
        homes           Disk      All home directories
        workfiles       Disk      Confidential Workfiles
        print$          Disk      Printer Drivers
        IPC$            IPC       IPC Service (Samba 4.9.5-Debian)
Reconnecting with SMB1 for workgroup listing.

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

        Workgroup            Master
        ---------            -------
```



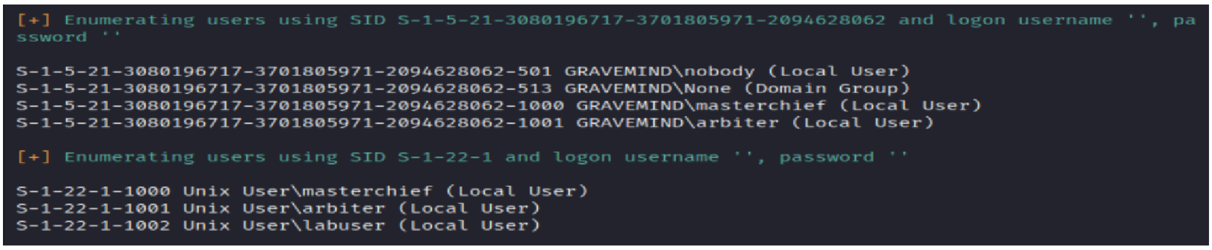
```
[+] Attempting to map shares on 10.6.6.23

[E] Can't understand response:

tree connect failed: NT_STATUS_BAD_NETWORK_NAME
//10.6.6.23/homes          Mapping: N/A Listing: N/A Writing: N/A
//10.6.6.23/workfiles      Mapping: OK Listing: OK Writing: N/A
//10.6.6.23/print$         Mapping: OK Listing: OK Writing: N/A

[E] Can't understand response:

NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
//10.6.6.23/IPC$           Mapping: N/A Listing: N/A Writing: N/A
```



```
 ==================================( Groups on 10.6.6.23 )==================================


[+] Getting builtin groups:


[+]  Getting builtin group memberships:


[+]  Getting local groups:


[+]  Getting local group memberships:


[+]  Getting domain groups:


[+]  Getting domain group memberships:
```



```
==========================( Users on 10.6.6.23 via RID cycling (RIDS: 500-550,1000-1050) )==========
=====

[I] Found new SID:
S-1-22-1

[I] Found new SID:
S-1-5-32

[I] Found new SID:
S-1-5-32

[I] Found new SID:
S-1-5-32

[I] Found new SID:
S-1-5-32

[+] Enumerating users using SID S-1-5-32 and logon username '', password ''

S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)
```

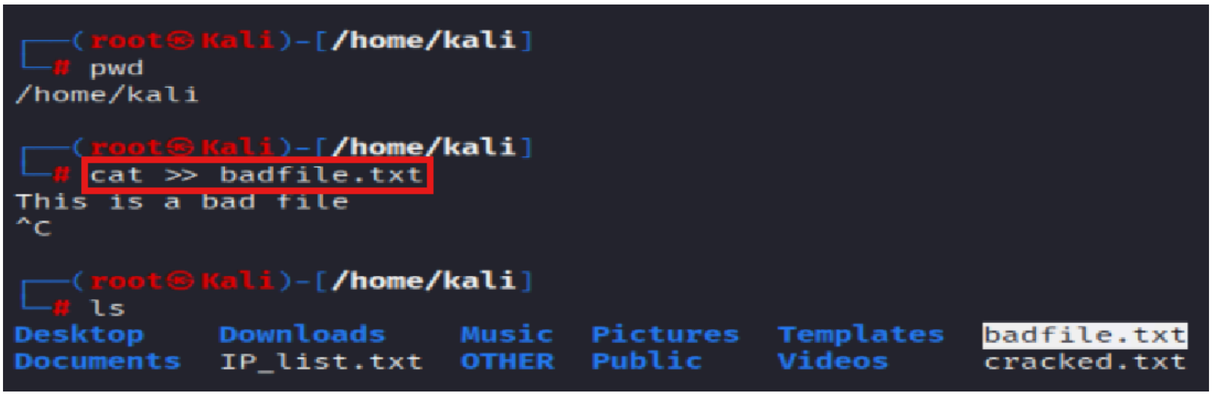


```
[+] Enumerating users using SID S-1-5-21-3080196717-3701805971-2094628062 and logon username '', pa
ssword ''

S-1-5-21-3080196717-3701805971-2094628062-501 GRAVEMIND\nobody (Local User)
S-1-5-21-3080196717-3701805971-2094628062-513 GRAVEMIND\None (Domain Group)
S-1-5-21-3080196717-3701805971-2094628062-1000 GRAVEMIND\masterchief (Local User)
S-1-5-21-3080196717-3701805971-2094628062-1001 GRAVEMIND\arbiter (Local User)

[+] Enumerating users using SID S-1-22-1 and logon username '', password ''

S-1-22-1-1000 Unix User\masterchief (Local User)
S-1-22-1-1001 Unix User\arbiter (Local User)
S-1-22-1-1002 Unix User\labuser (Local User)
```

Part 4: Use smbclient to transfer files between systems.

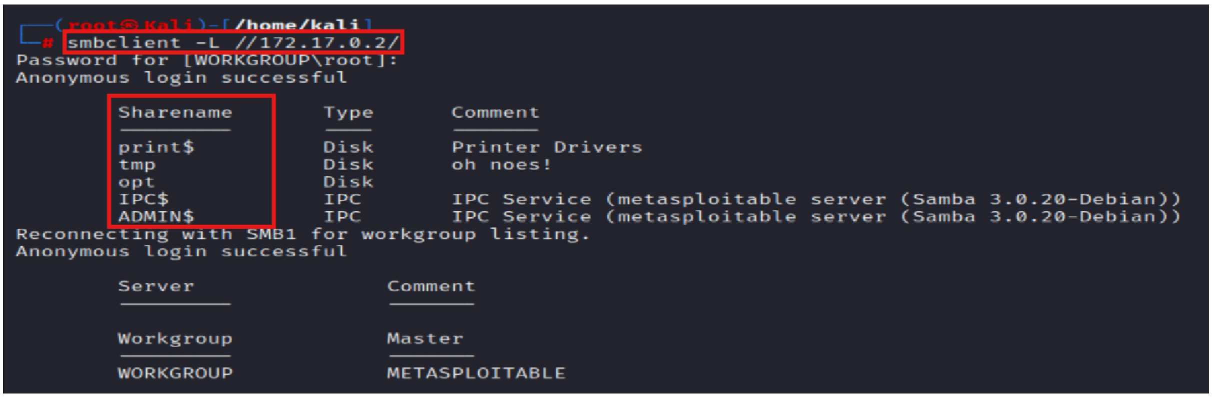
Smbclient is a component of Samba that can store and retrieve files, similar to an FTP client. You will use smbclient to transfer a file to the target system at 172.17.0.2. This simulates exploiting a network host with malware through an SMB vulnerability.

- Create a text file using the **cat** command. Name the file **badfile.txt**. Enter the desired text. In this example, **This is a bad file.** was used. Be sure that you know the path to the file. Press **CTRL-C** to when finished.



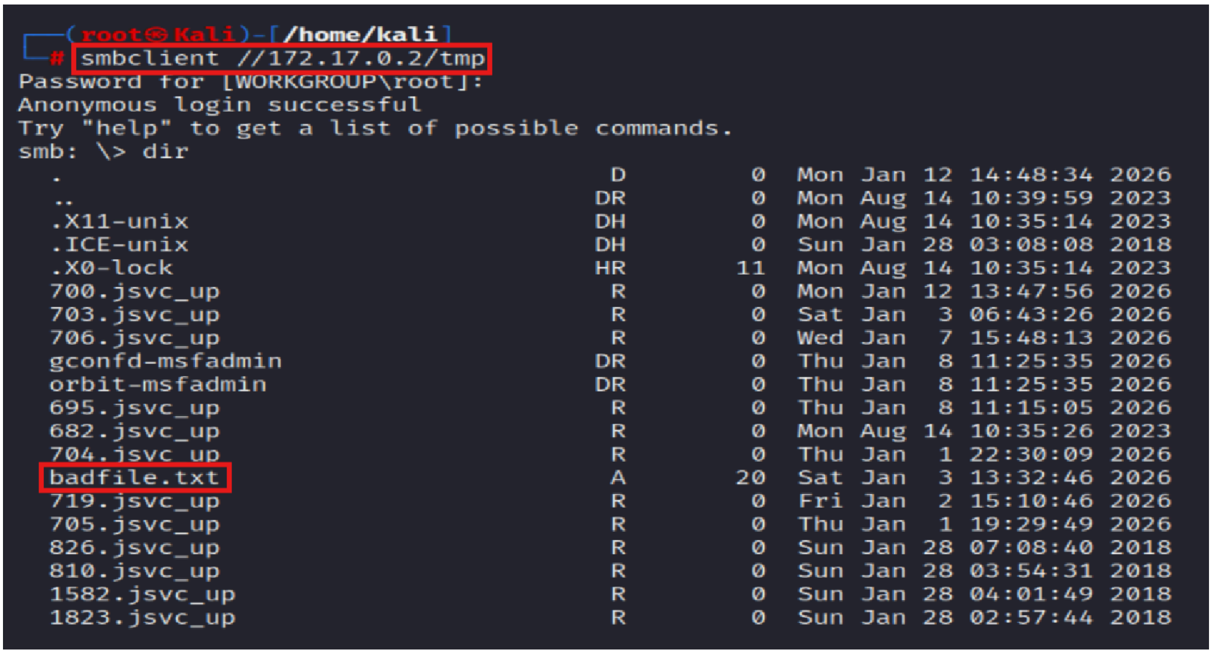
```
┌──(root㉿Kali)-[/home/kali]
└─# pwd
/home/kali

┌──(root㉿Kali)-[/home/kali]
└─# cat >> badfile.txt
This is a bad file
^C

┌──(root㉿Kali)-[/home/kali]
└─# ls
Desktop     Downloads    Music  Pictures  Templates  badfile.txt
Documents   IP_list.txt  OTHER  Public    Videos     cracked.txt
```

- Use the **smbclient -L** command to list the shares on the target host. When asked for a password, press enter. The double / character before the IP address and the / following it are necessary if the target is a Windows computer.

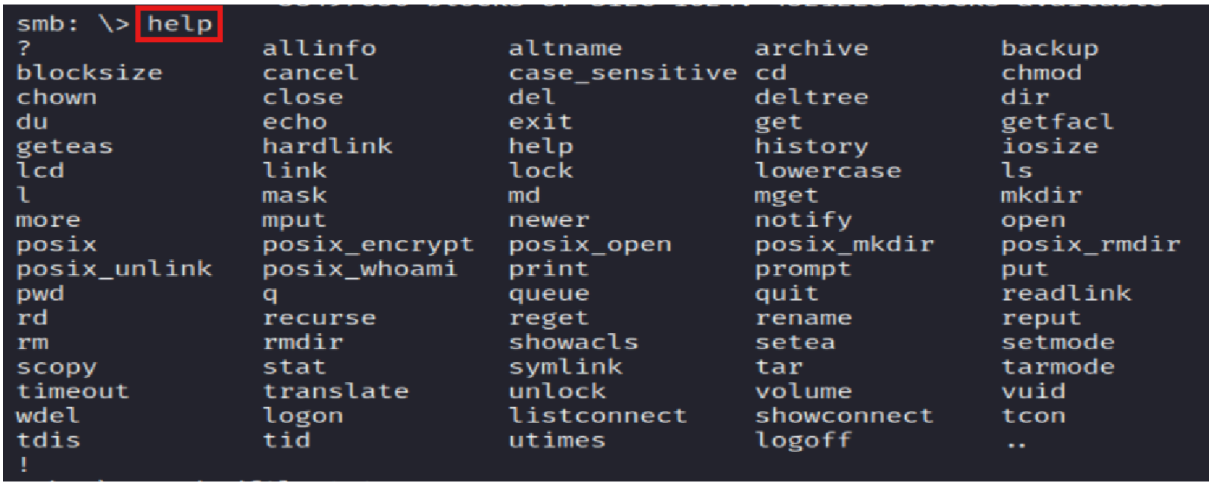


```
┌──(root㉿Kali)-[/home/kali]
└─# smbclient -L //172.17.0.2/
Password for [WORKGROUP\root]:
Anonymous login successful

        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
```

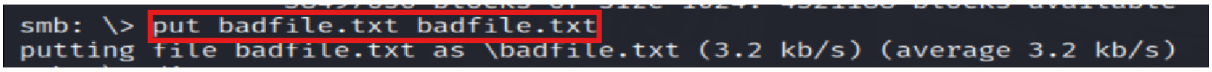
- Connect to the **tmp** share using the **smbclient** command by specifying the share name and IP address.
- Upload the **badfile.txt** to the target server using the **put** command.
- Verify that the file successfully uploaded using the **dir** command.
- Type **quit** to exit the **smbclient** and return to the CLI prompt.



```
┌──(root㉿Kali)-[/home/kali]
└─# smbclient //172.17.0.2/tmp
Password for [WORKGROUP\root]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Mon Jan 12 14:48:34 2026
  ..                                 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
  700.jsvc_up                         R        0  Mon Jan 12 13:47:56 2026
  703.jsvc_up                         R        0  Sat Jan  3 06:43:26 2026
  706.jsvc_up                         R        0  Wed Jan  7 15:48:13 2026
  gconfd-msfadmin                    DR        0  Thu Jan  8 11:25:35 2026
  orbit-msfadmin                     DR        0  Thu Jan  8 11:25:35 2026
  695.jsvc_up                         R        0  Thu Jan  8 11:15:05 2026
  682.jsvc_up                         R        0  Mon Aug 14 10:35:26 2023
  704.jsvc_up                         R        0  Thu Jan  1 22:30:09 2026
  badfile.txt                         A       20  Sat Jan  3 13:32:46 2026
  719.jsvc_up                         R        0  Fri Jan  2 15:10:46 2026
  705.jsvc_up                         R        0  Thu Jan  1 19:29:49 2026
  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
```



```
smb: \> help
?              allinfo        altname        archive        backup
blocksize      cancel         case_sensitive cd             chmod
chown          close          del            deltree        dir
du             echo           exit           get            getfacl
geteas         hardlink       help           history        iosize
lcd            link           lock           lowercase      ls
l              mask           md             mget           mkdir
more           mput           newer          notify         open
posix          posix_encrypt  posix_open     posix_mkdir    posix_rmdir
posix_unlink   posix_whoami   print          prompt         put
pwd            q              queue          quit           readlink
rd             recurse        reget          rename         reput
rm             rmdir          showacls       setea          setmode
scopy          stat           symlink        tar            tarmode
timeout        translate      unlock         volume         vuid
wdel           logon          listconnect    showconnect    tcon
tdis           tid            utimes         logoff         ..
!
```



```
smb: \> put badfile.txt badfile.txt
putting file badfile.txt as \badfile.txt (3.2 kb/s) (average 3.2 kb/s)
```