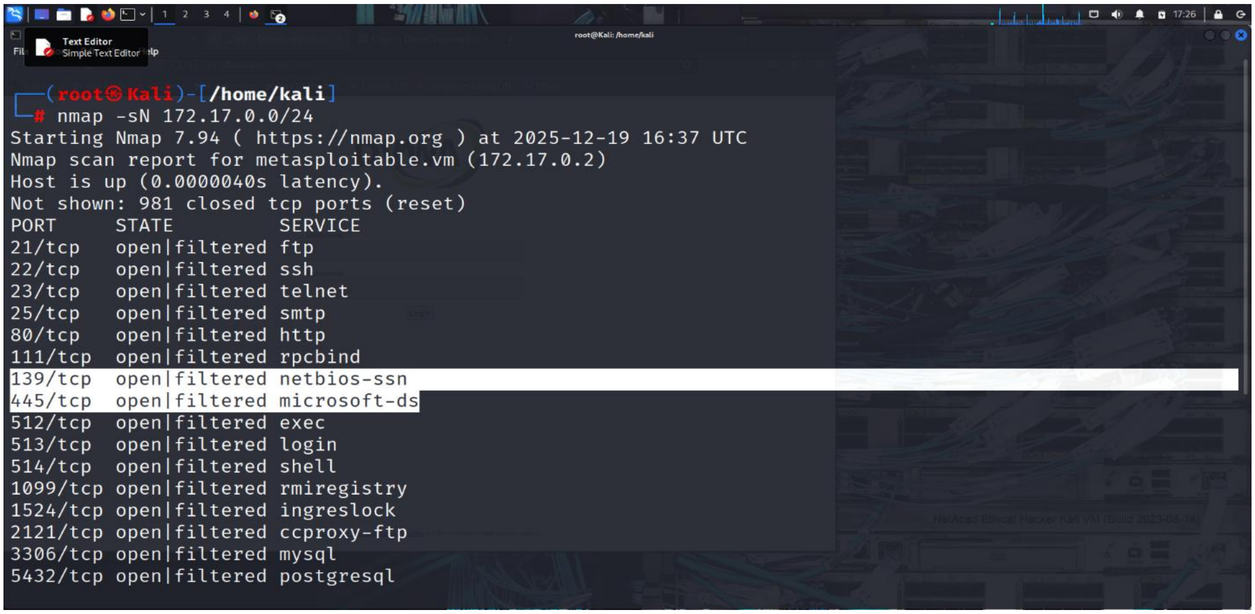
SMB PROJECT

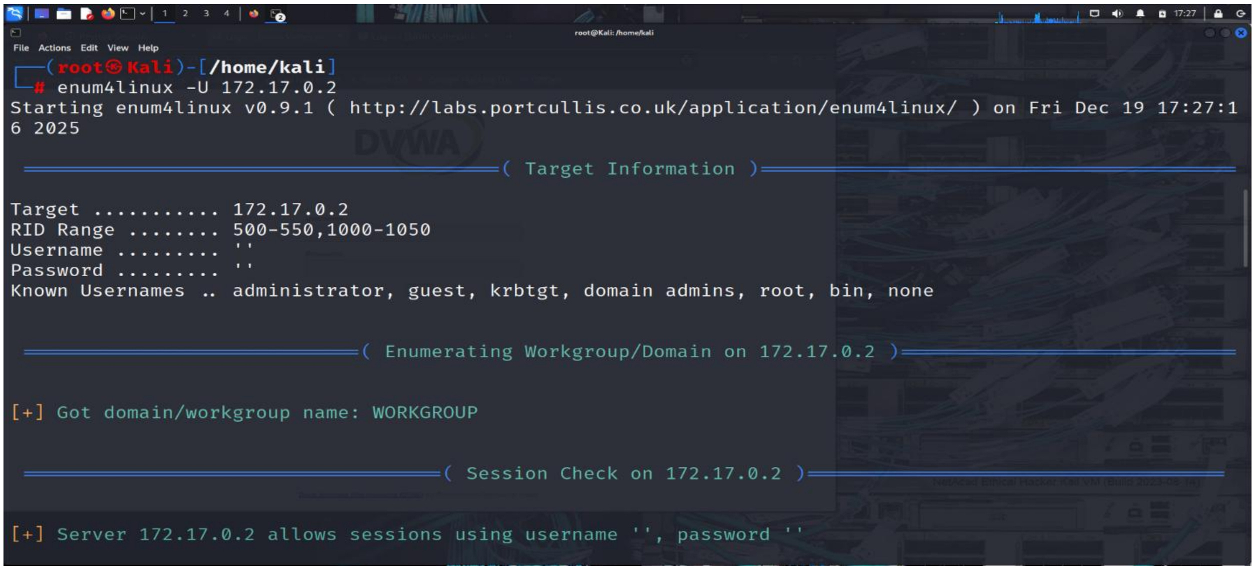
SMB, or Server Message Block, is a core network protocol for sharing files, printers, and serial ports, acting as a way for computers (Windows, macOS, Linux) to talk and access resources over a network, essentially creating a "remote file system" for shared access

1. We run a nmap scan to identify open ports and up hosts where we discovered port 139 and 445 which is our target for this SMB lab.

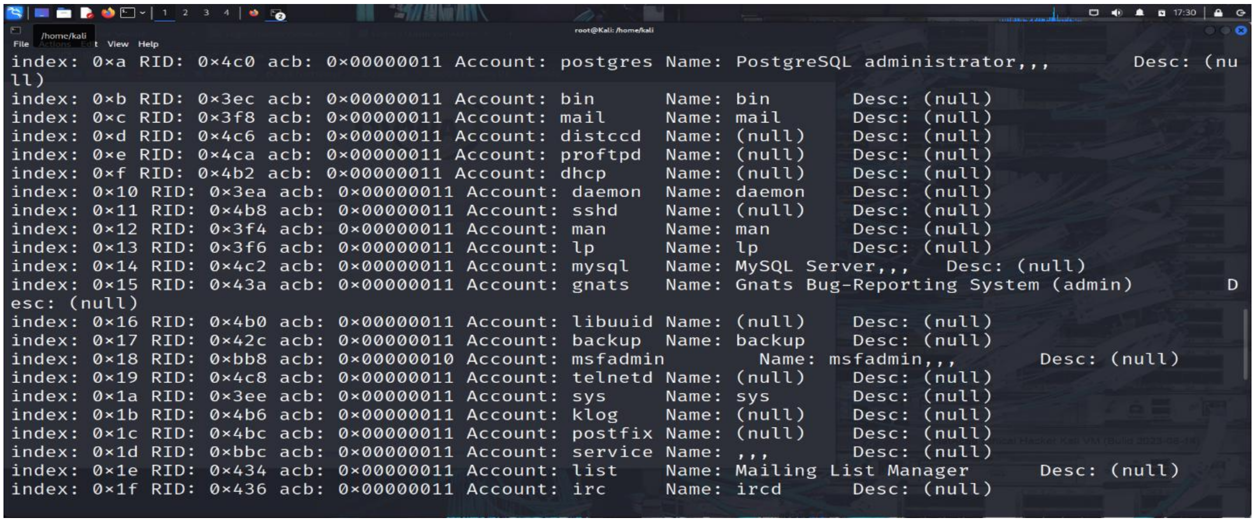


```
┌──(root㉿Kali)-[/home/kali]
└─# nmap -sN 172.17.0.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-19 16:37 UTC
Nmap scan report for metasploitable.vm (172.17.0.2)
Host is up (0.0000040s latency).
Not shown: 981 closed tcp ports (reset)
PORT     STATE         SERVICE
21/tcp   open|filtered 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
```

2. We run **enum4linux -U [ip address]** option to get user list.

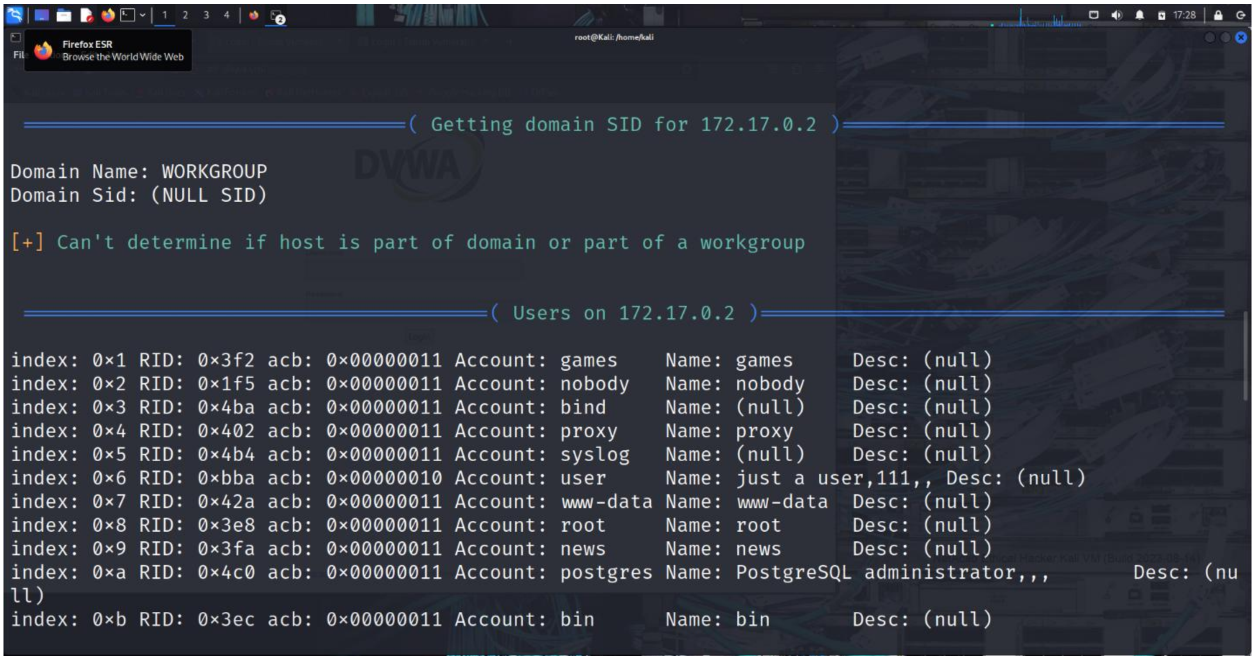


```
┌──(root㉿Kali)-[/home/kali]
└─# enum4linux -U 172.17.0.2
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Dec 19 17:27:1
6 2025

 ========================================( 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 ''
```

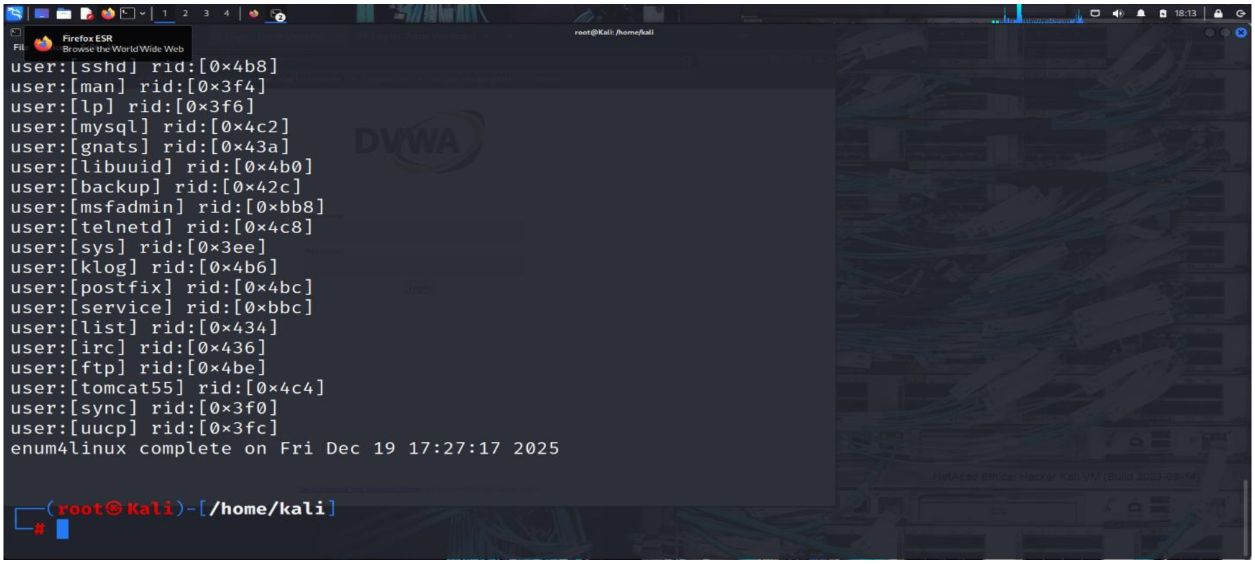


```
index: 0xa RID: 0x4c0 acb: 0x00000011 Account: postgres Name: PostgreSQL administrator,,,       Desc: (nu
ll)
index: 0xb RID: 0x3ec acb: 0x00000011 Account: bin      Name: bin       Desc: (null)
index: 0xc RID: 0x3f8 acb: 0x00000011 Account: mail     Name: mail      Desc: (null)
index: 0xd RID: 0x4c6 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: 0x43a acb: 0x00000011 Account: gnats   Name: Gnats Bug-Reporting System (admin)        D
esc: (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)
```

The screenshot below shows all the users that are in the domain

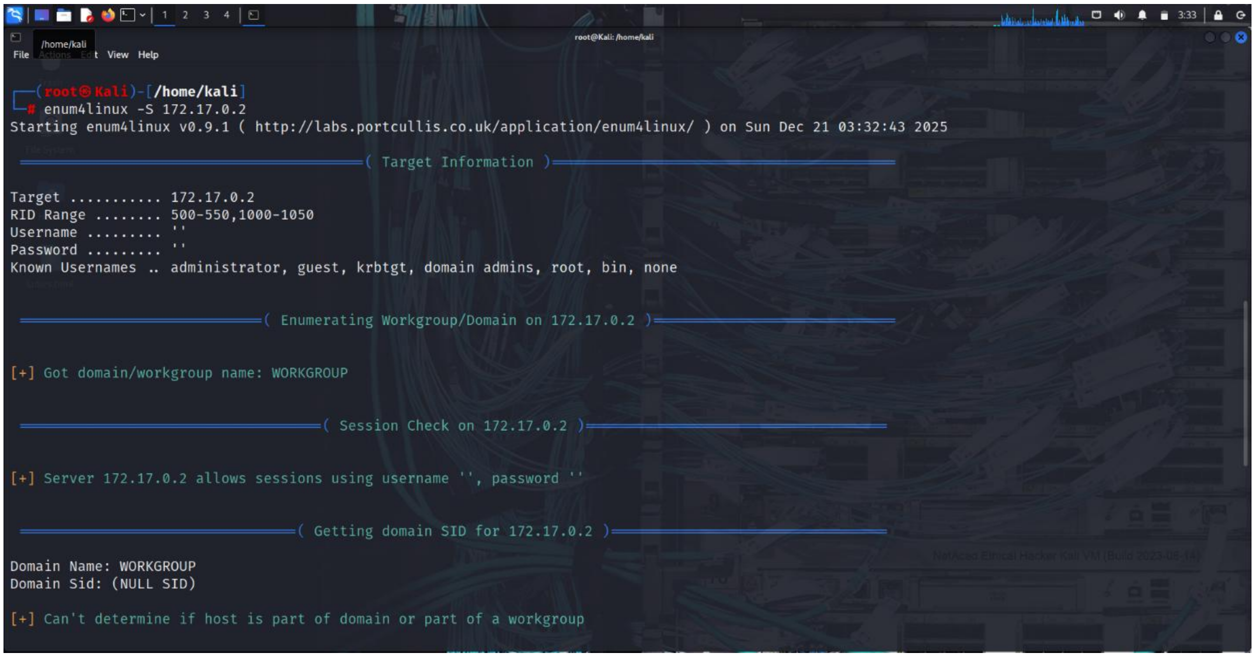


```
 ===============================( Getting domain SID for 172.17.0.2 )===============================

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: (nu
ll)
index: 0xb RID: 0x3ec acb: 0x00000011 Account: bin      Name: bin       Desc: (null)
```

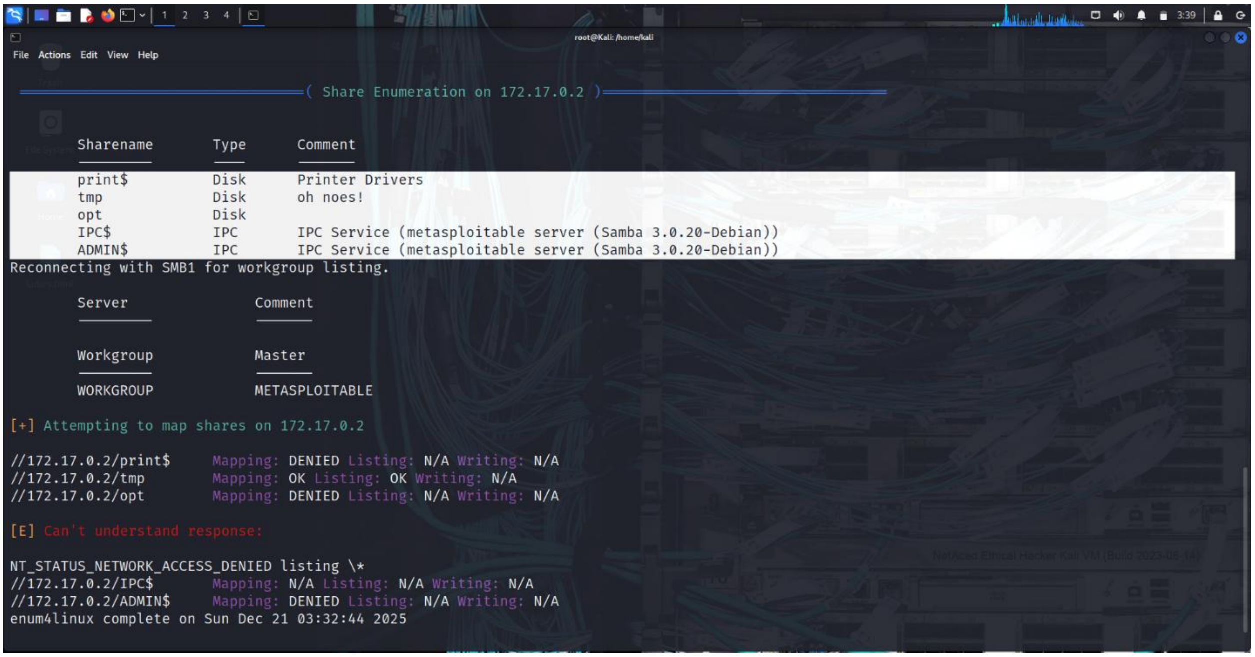


```
user:[sshd] rid:[0×4b8]
user:[man] rid:[0×3f4]
user:[lp] rid:[0×3f6]
user:[mysql] rid:[0×4c2]
user:[gnats] rid:[0×43a]
user:[libuuid] rid:[0×4b0]
user:[backup] rid:[0×42c]
user:[msfadmin] rid:[0×bb8]
user:[telnetd] rid:[0×4c8]
user:[sys] rid:[0×3ee]
user:[klog] rid:[0×4b6]
user:[postfix] rid:[0×4bc]
user:[service] rid:[0×bbc]
user:[list] rid:[0×434]
user:[irc] rid:[0×436]
user:[ftp] rid:[0×4be]
user:[tomcat55] rid:[0×4c4]
user:[sync] rid:[0×3f0]
user:[uucp] rid:[0×3fc]
enum4linux complete on Fri Dec 19 17:27:17 2025

┌──(root㉿Kali)-[/home/kali]
└─#
```

3. We run **enum4linux -S [ip address]** option to get sharelist where we can enumerate what shares are available for us and they are highlighted below.

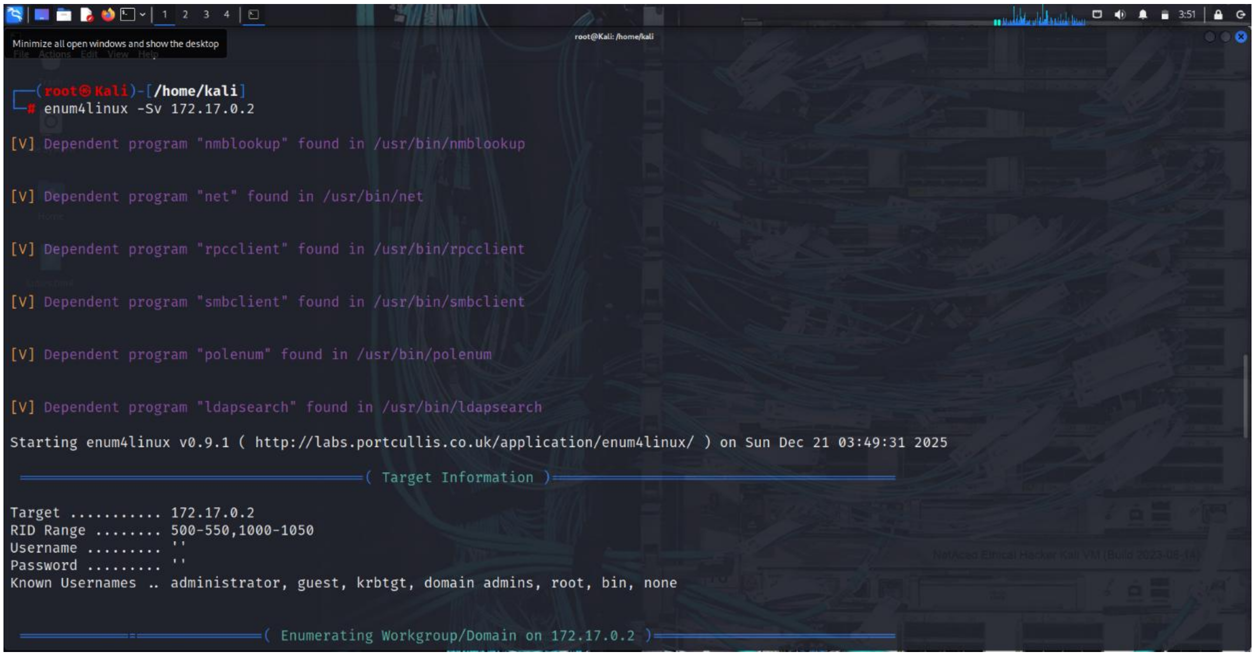


```
┌──(root㉿Kali)-[/home/kali]
└─# enum4linux -S 172.17.0.2
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Dec 21 03:32:43 2025

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



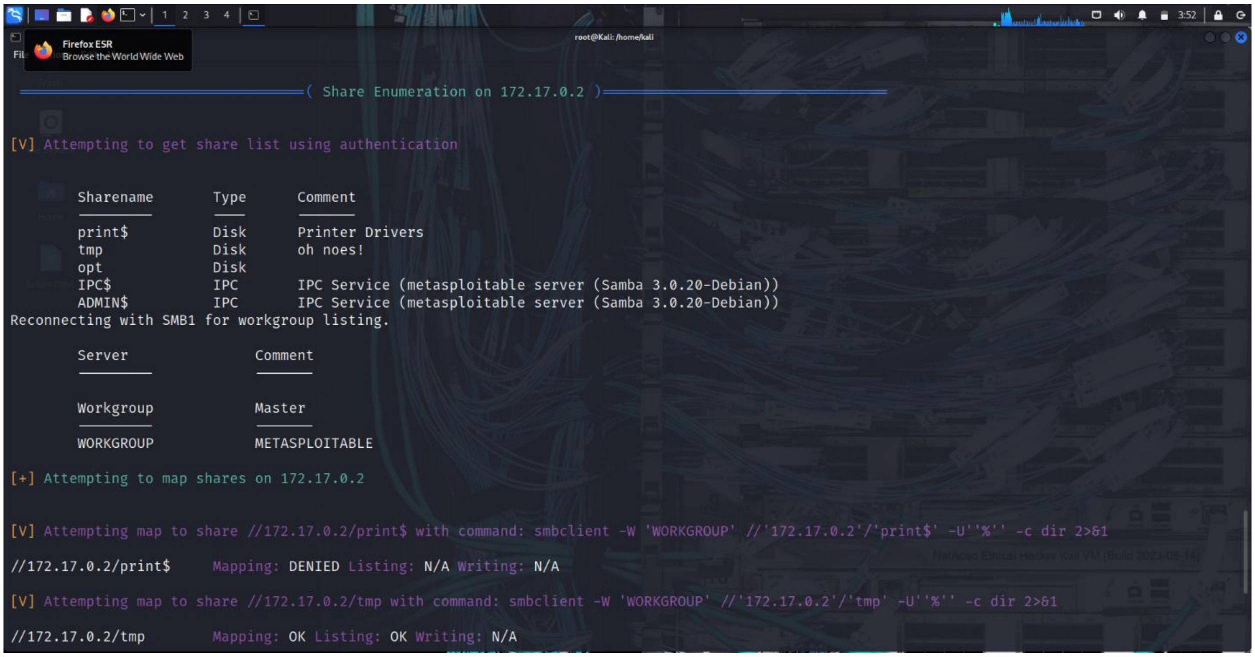
```
 ==================================( Share Enumeration on 172.17.0.2 )==================================

        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.

        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 Sun Dec 21 03:32:44 2025
```

4. We run **enum4linux -Sv [ip address]** option (known as Verbose) to move from the normal sharelist to see what mode are being used within enum4linux.



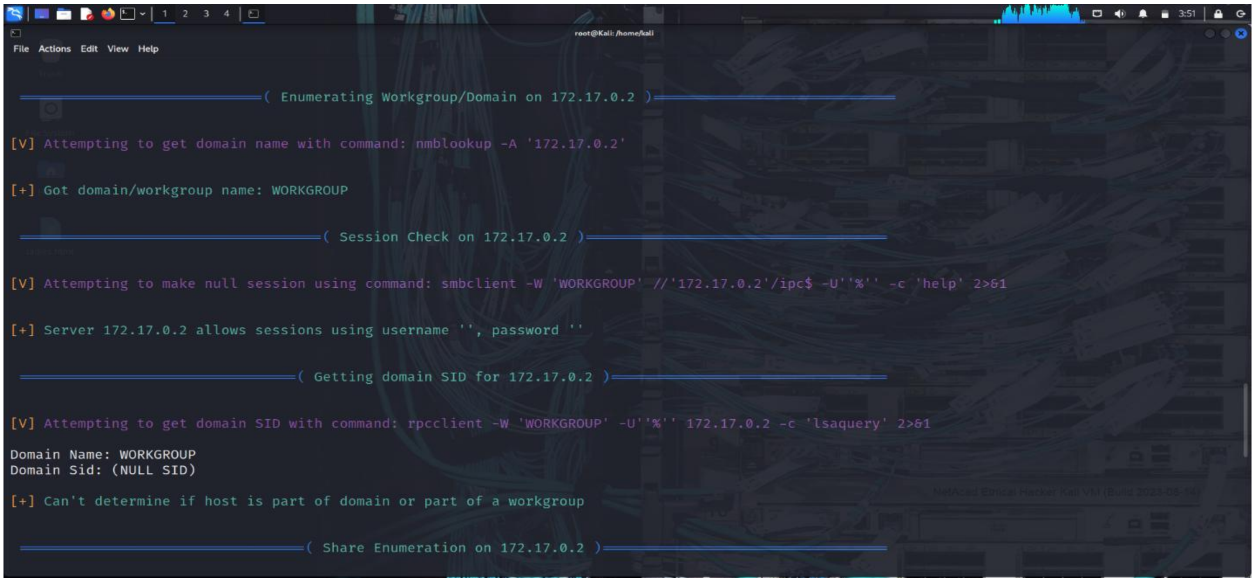
```
┌──(root㉿Kali)-[/home/kali]
└─# enum4linux -Sv 172.17.0.2

[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/ ) on Sun Dec 21 03:49:31 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 )============================
```

From the screenshot below we can get the different share like **print$, tmp**, etc

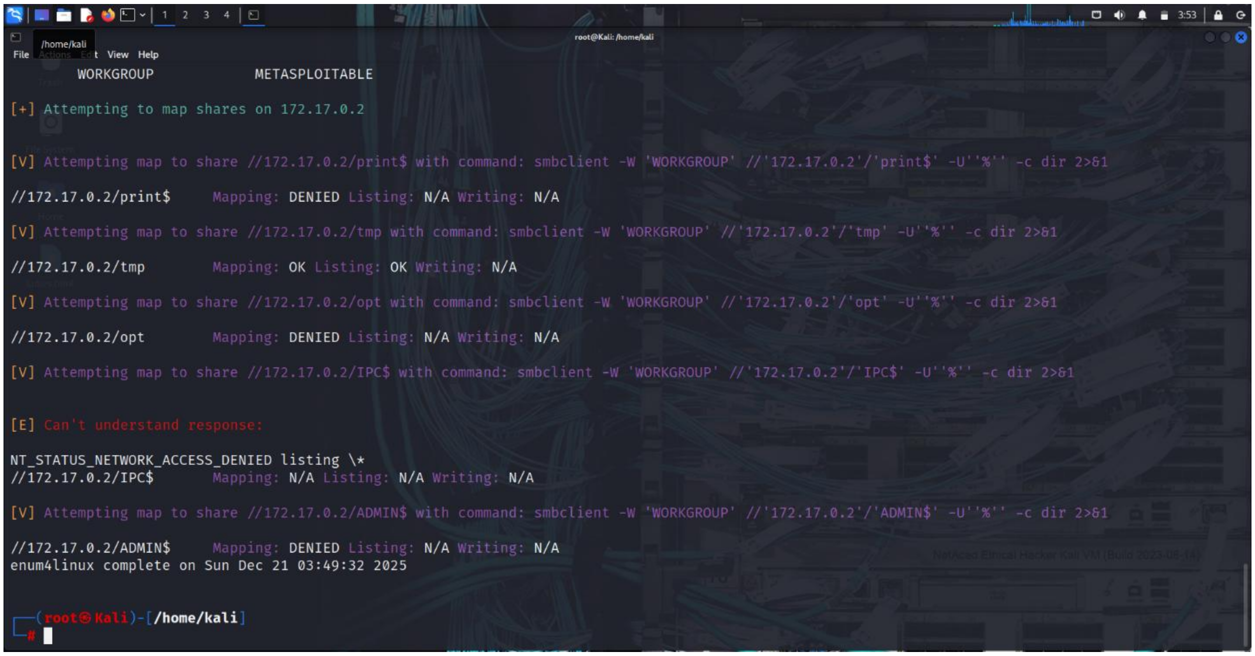


```
 ==================================( Share Enumeration on 172.17.0.2 )==================================

[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
```

From the screenshot below we get the domain group we are attacking

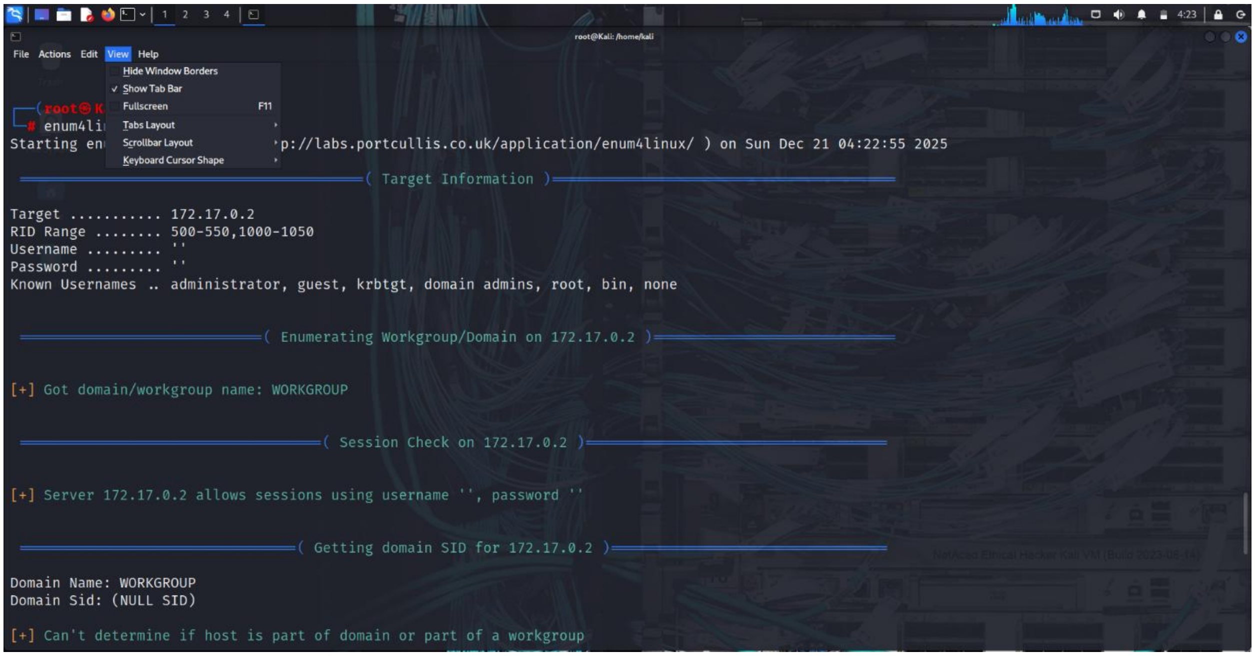


```
 ============================( Enumerating Workgroup/Domain on 172.17.0.2 )============================

[V] Attempting to get domain name with command: nmblookup -A '172.17.0.2'

[+] Got domain/workgroup name: WORKGROUP

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

[V] Attempting to make null session using command: smbclient -W 'WORKGROUP' //'172.17.0.2'/ipc$ -U''%'' -c 'help' 2>&1

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

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

[V] Attempting to get domain SID with command: rpcclient -W 'WORKGROUP' -U''%'' 172.17.0.2 -c 'lsaquery' 2>&1

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 )==================================
```



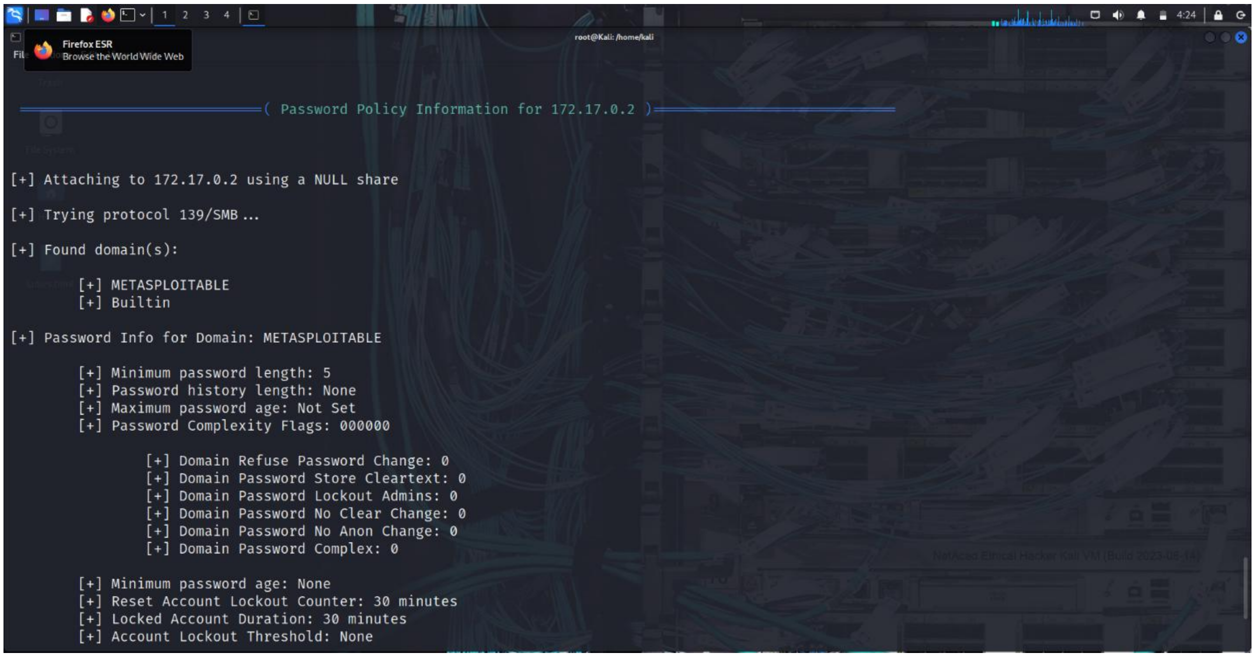
```
      WORKGROUP            METASPLOITABLE

[+] 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


[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

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

//172.17.0.2/ADMIN$     Mapping: DENIED Listing: N/A Writing: N/A
enum4linux complete on Sun Dec 21 03:49:32 2025


┌──(root㉿Kali)-[/home/kali]
└─# 
```

5. We use **enum4linux -P [ip address]** to determine how the security password policy has been set for that domain.

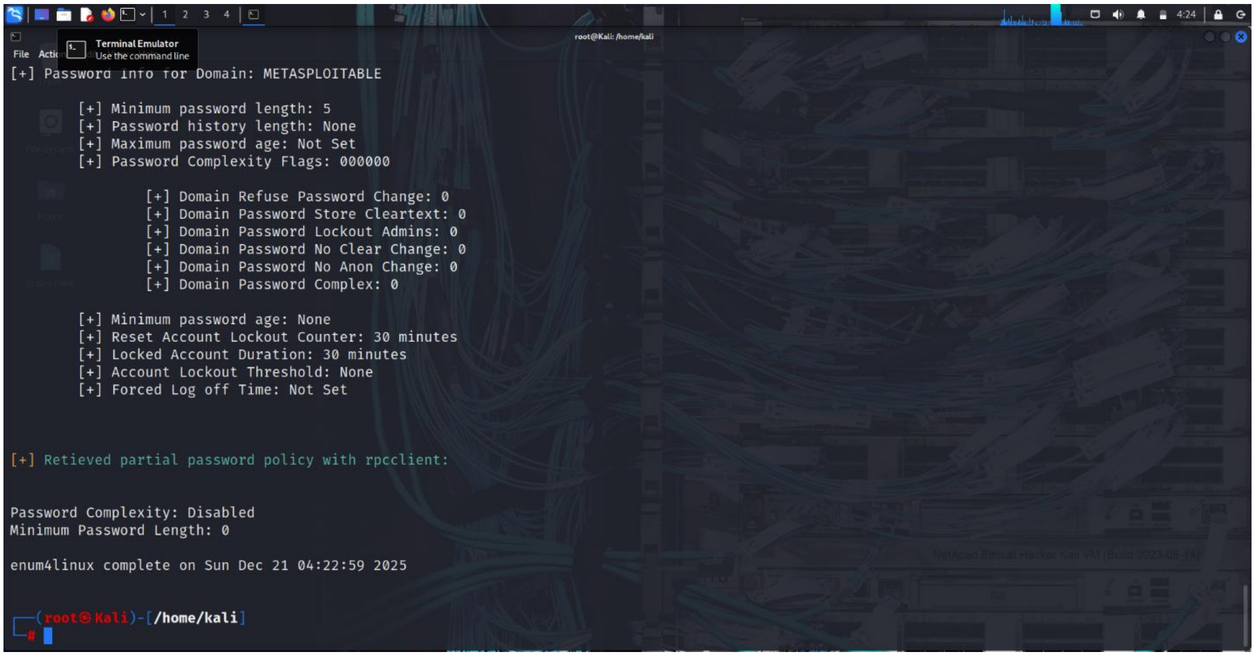


```
┌──(root㉿K
└─# enum4li
Starting en                             p://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Dec 21 04:22:55 2025

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

Below we can see some of the password policies the domain is using which can tell us how vulnerable they are to attacks as they only use 5 as the minimum password length.



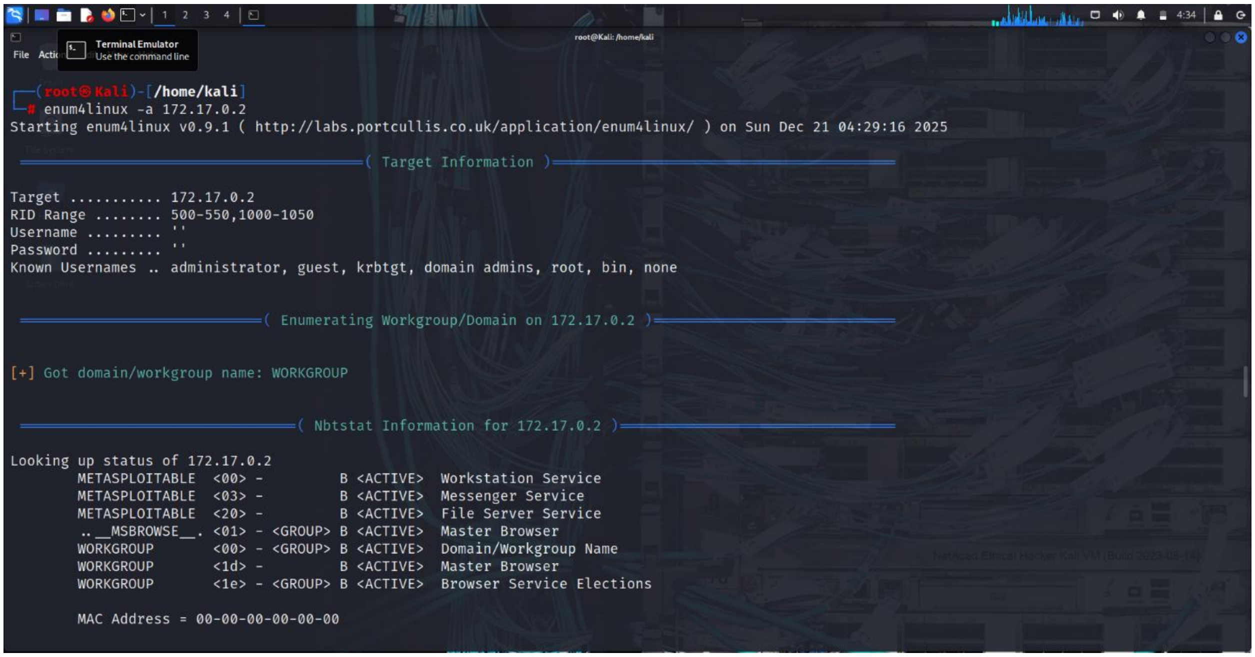
```
=====================( Password Policy Information for 172.17.0.2 )=====================

[+] 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
```



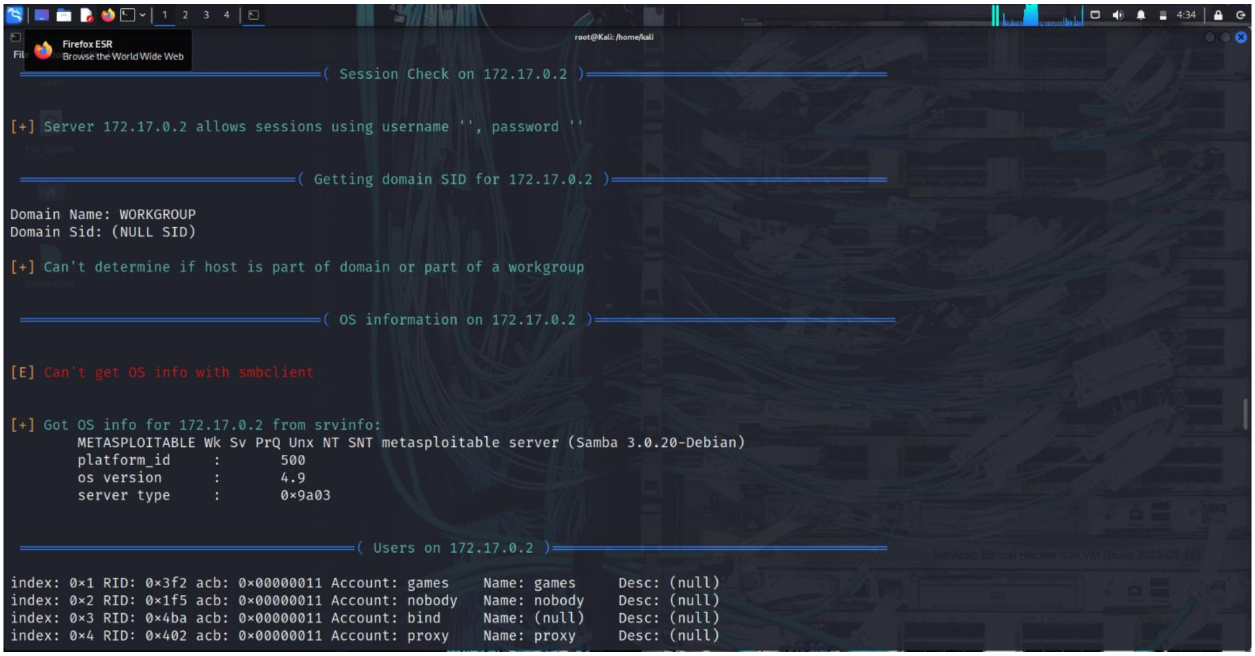
```
[+] Password Info for Domain: METASPLOITABLE

        [+] 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 Sun Dec 21 04:22:59 2025

┌──(root㉿Kali)-[/home/kali]
└─#
```

6. We use **enum4linux -a [ip address]** to perform everything at once. This command is an overall scan which can perform the whole reconnaissance in 1 command. This includes everything we have performed above and much more as it is performing

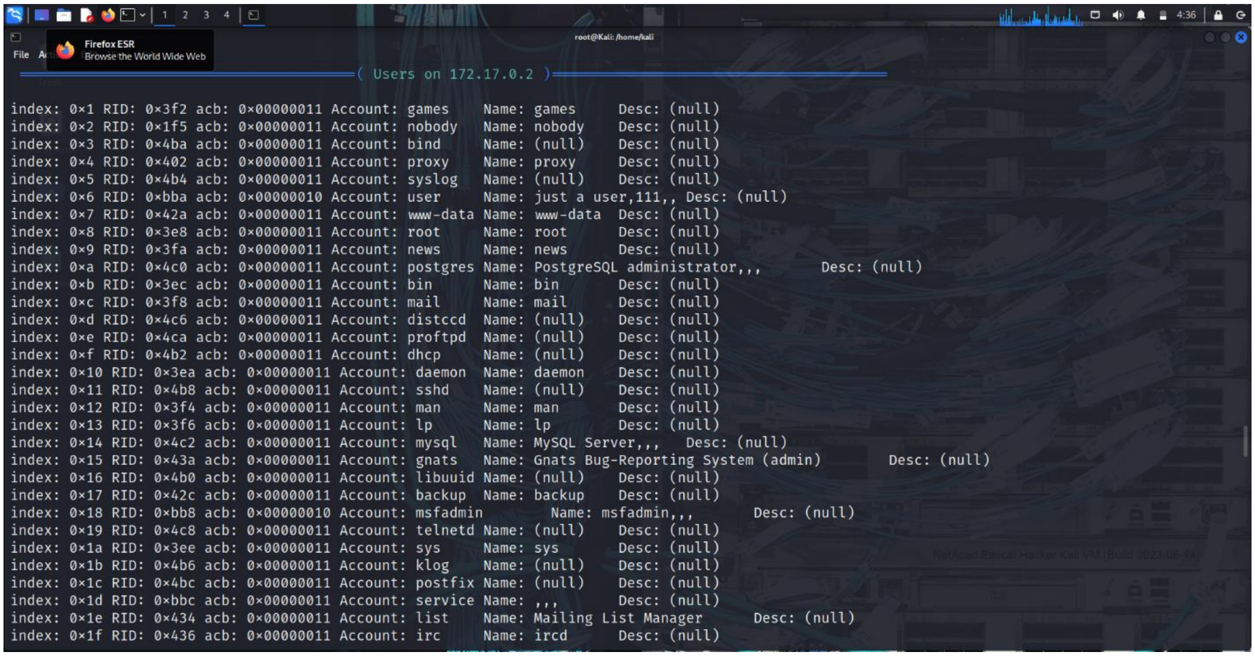
whole recon stage, like users that are on the domain, the OS, and enumerated shares etc



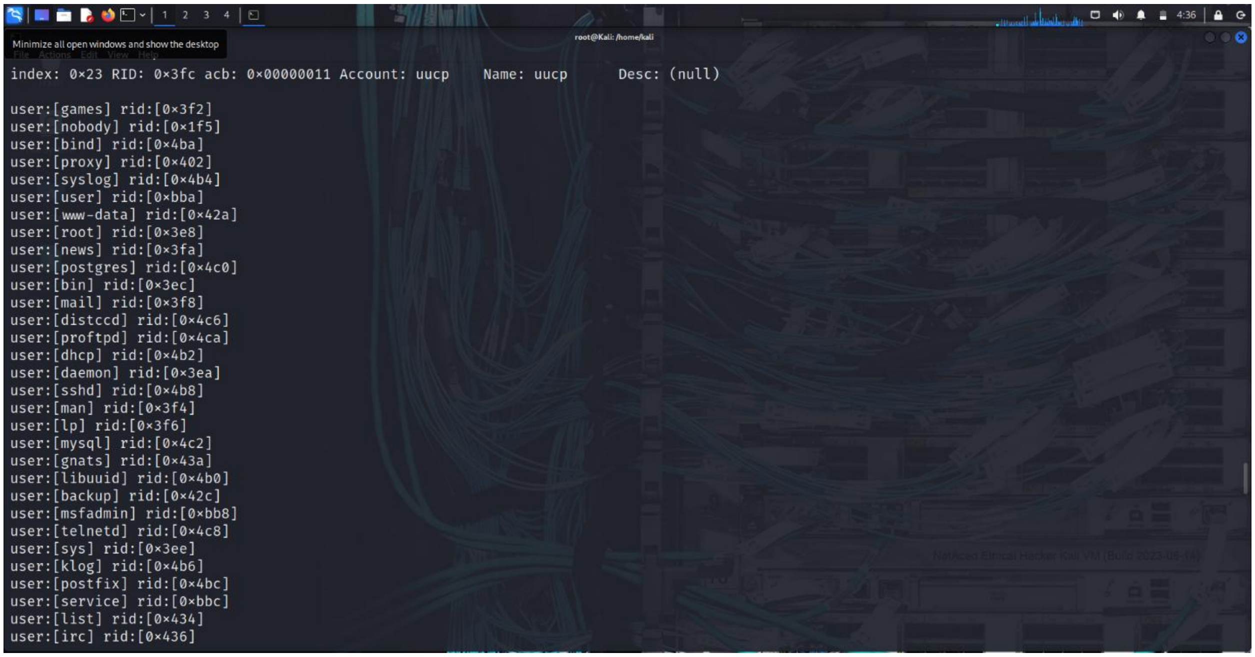
```
┌──(root㉿Kali)-[/home/kali]
└─# enum4linux -a 172.17.0.2
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Dec 21 04:29:16 2025

 =========================================( 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


 =================================( Nbtstat Information for 172.17.0.2 )=================================

Looking up status of 172.17.0.2
        METASPLOITABLE  <00> -         B <ACTIVE>  Workstation Service
        METASPLOITABLE  <03> -         B <ACTIVE>  Messenger Service
        METASPLOITABLE  <20> -         B <ACTIVE>  File Server Service
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser
        WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        WORKGROUP       <1d> -         B <ACTIVE>  Master Browser
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

        MAC Address = 00-00-00-00-00-00
```



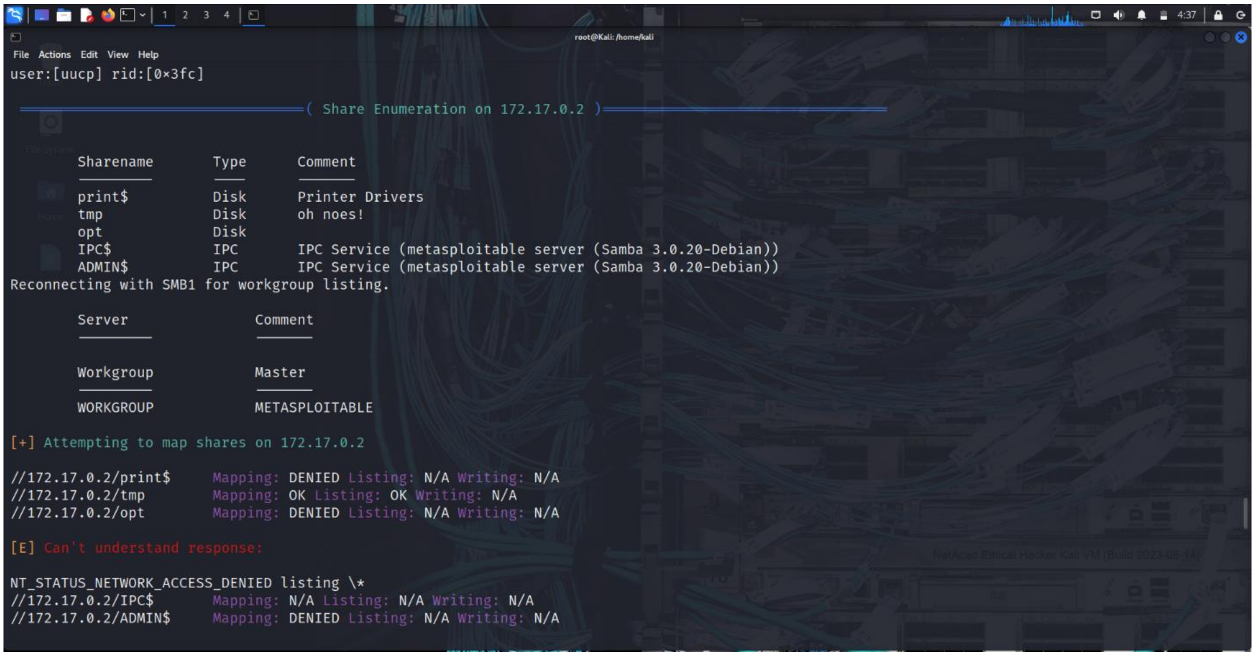
```
 ====================================( Session Check on 172.17.0.2 )====================================


[+] 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


 ====================================( OS information on 172.17.0.2 )====================================


[E] Can't get OS info with smbclient


[+] Got OS info for 172.17.0.2 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 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)
```



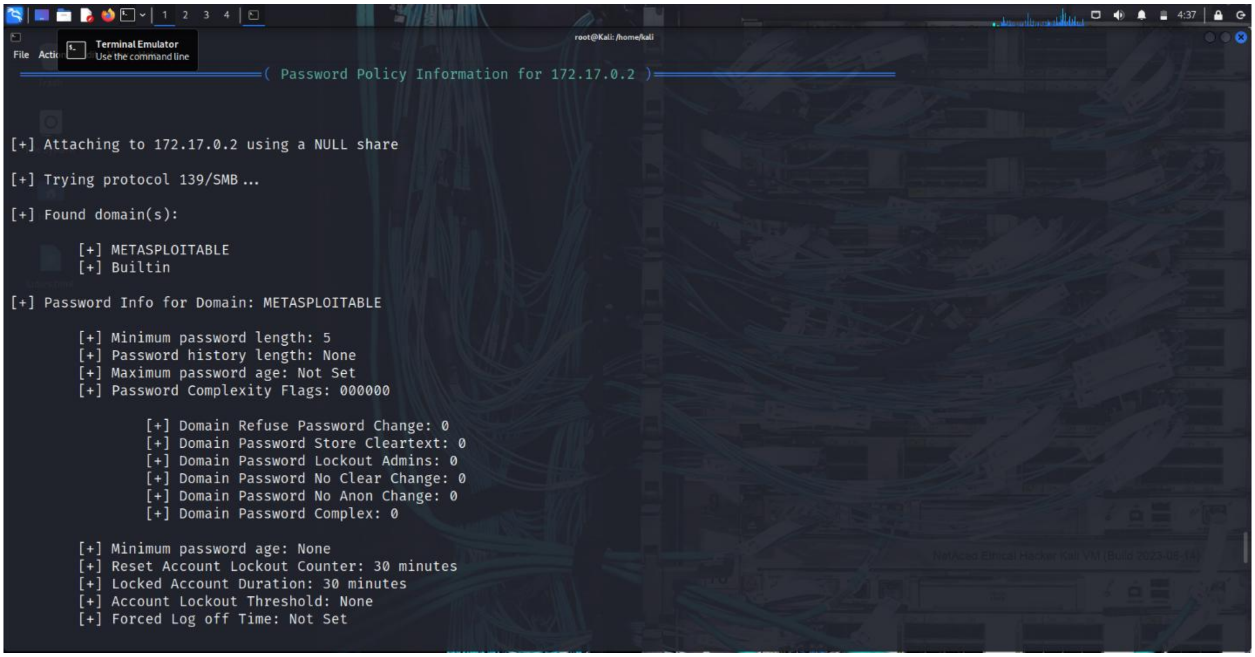
```
( Users on 172.17.0.2 )

index: 0×1 RID: 0×3f2 acb: 0×00000011 Account: games    Name: games     Desc: (null)
index: 0×2 RID: 0×1f5 acb: 0×00000011 Account: nobody   Name: nobody    Desc: (null)
index: 0×3 RID: 0×4ba acb: 0×00000011 Account: bind     Name: (null)    Desc: (null)
index: 0×4 RID: 0×402 acb: 0×00000011 Account: proxy    Name: proxy     Desc: (null)
index: 0×5 RID: 0×4b4 acb: 0×00000011 Account: syslog   Name: (null)    Desc: (null)
index: 0×6 RID: 0×bba acb: 0×00000010 Account: user     Name: just a user,111,, Desc: (null)
index: 0×7 RID: 0×42a acb: 0×00000011 Account: www-data Name: www-data  Desc: (null)
index: 0×8 RID: 0×3e8 acb: 0×00000011 Account: root     Name: root      Desc: (null)
index: 0×9 RID: 0×3fa acb: 0×00000011 Account: news     Name: news      Desc: (null)
index: 0×a RID: 0×4c0 acb: 0×00000011 Account: postgres Name: PostgreSQL administrator,,,       Desc: (null)
index: 0×b RID: 0×3ec acb: 0×00000011 Account: bin      Name: bin       Desc: (null)
index: 0×c RID: 0×3f8 acb: 0×00000011 Account: mail     Name: mail      Desc: (null)
index: 0×d RID: 0×4c6 acb: 0×00000011 Account: distccd  Name: (null)    Desc: (null)
index: 0×e RID: 0×4ca acb: 0×00000011 Account: proftpd  Name: (null)    Desc: (null)
index: 0×f RID: 0×4b2 acb: 0×00000011 Account: dhcp     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: (null)
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)
```



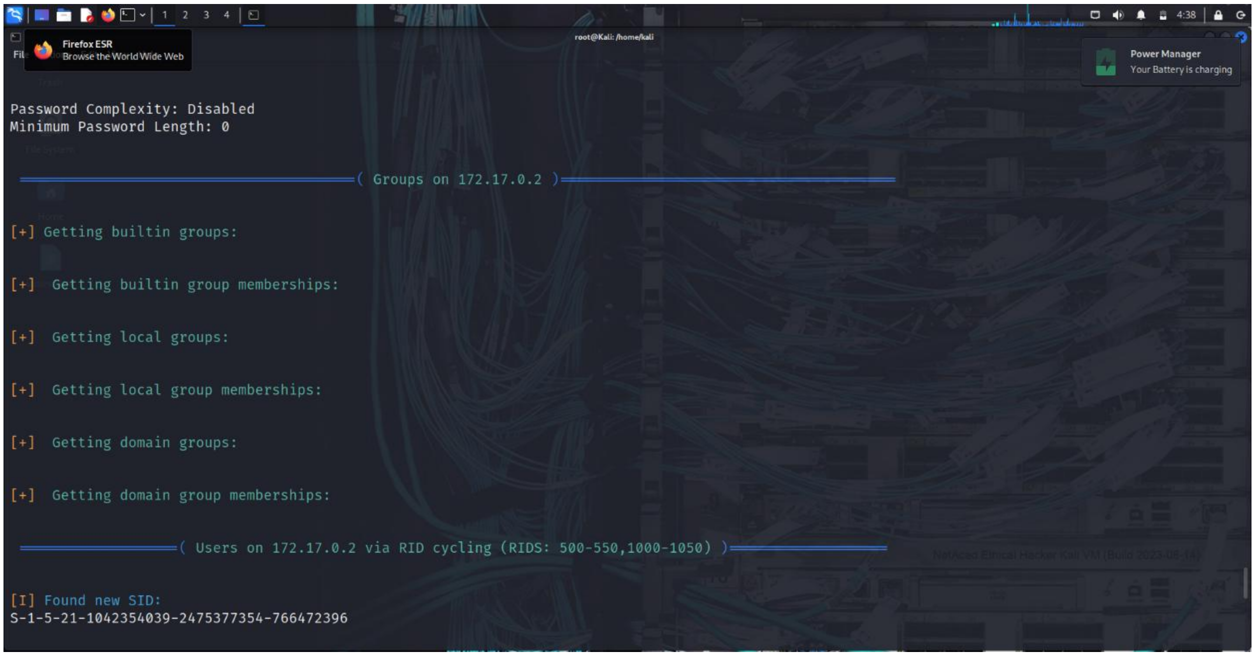
```
index: 0×23 RID: 0×3fc acb: 0×00000011 Account: uucp    Name: uucp      Desc: (null)

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]
```



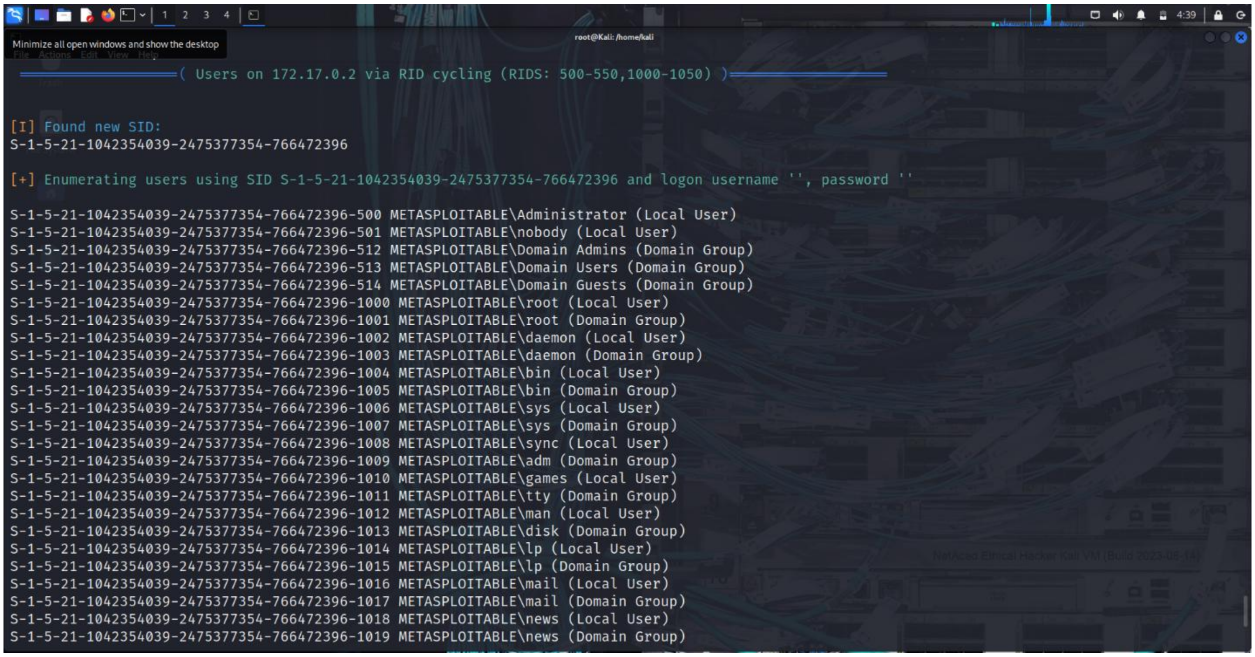
```
user:[uucp] rid:[0×3fc]

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



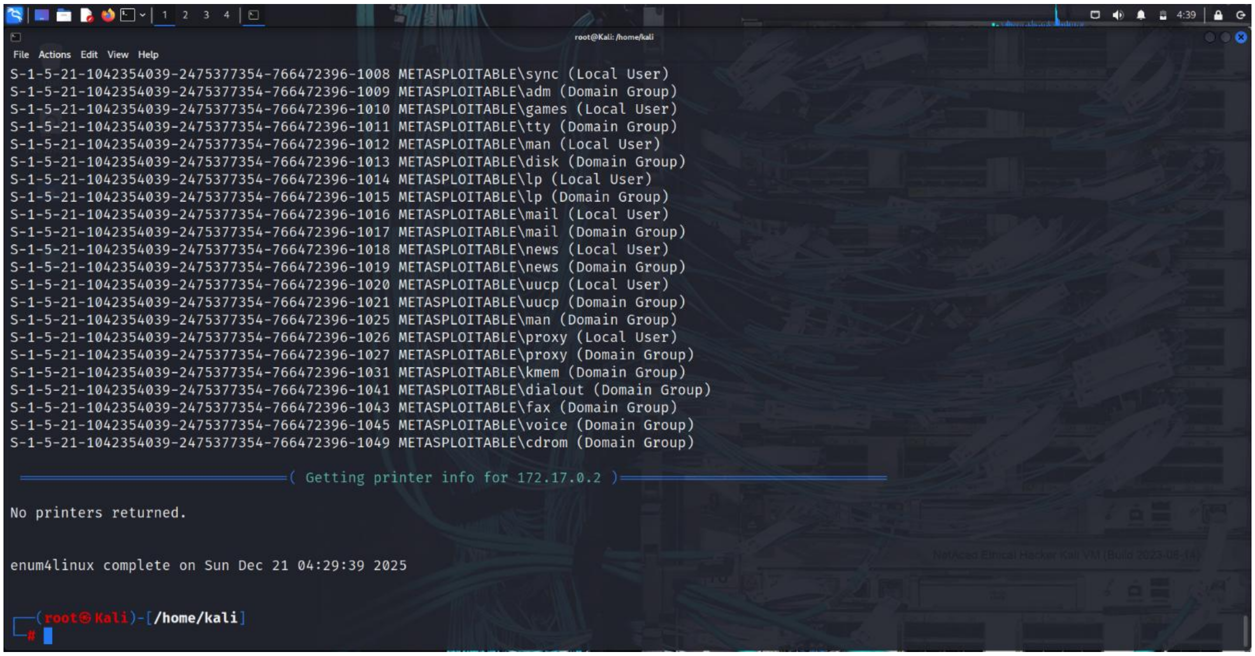
```
 ===========================( Password Policy Information for 172.17.0.2 )===========================


[+] 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
```



```
Password Complexity: Disabled
Minimum Password Length: 0

 ========================================( Groups on 172.17.0.2 )========================================

[+] Getting builtin groups:

[+]  Getting builtin group memberships:

[+]  Getting local groups:

[+]  Getting local group memberships:

[+]  Getting domain groups:

[+]  Getting domain group memberships:

 ===================( Users on 172.17.0.2 via RID cycling (RIDS: 500-550,1000-1050) )===================

[I] Found new SID:
S-1-5-21-1042354039-2475377354-766472396
```

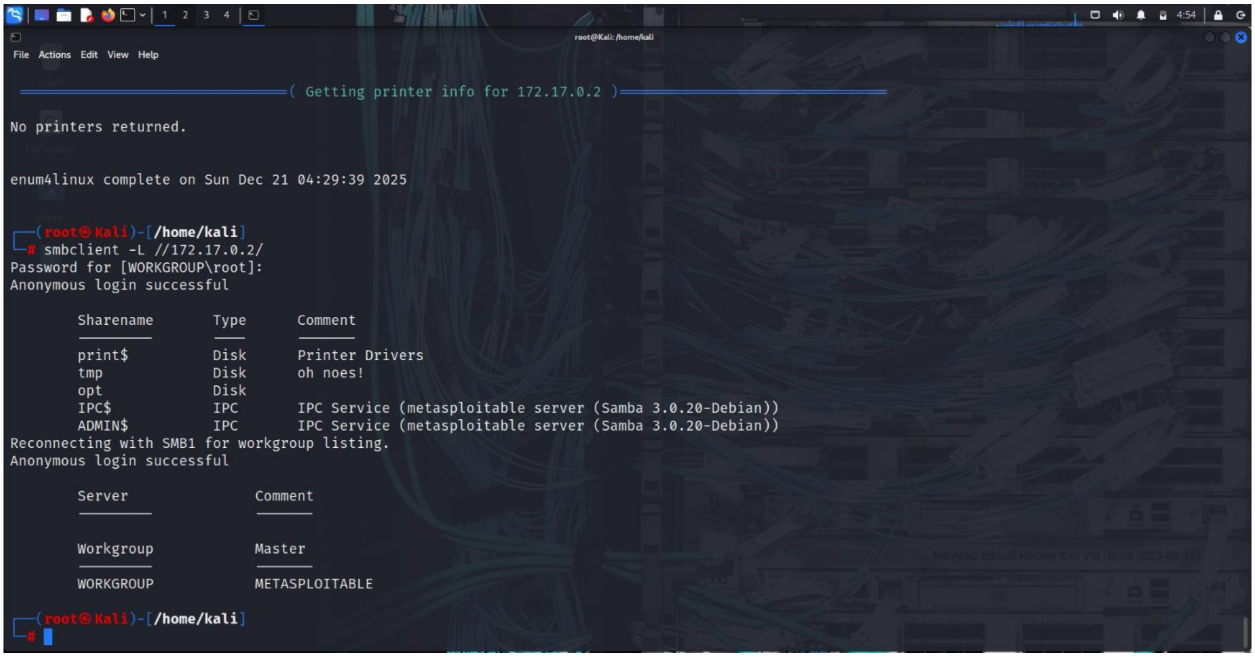


```
 ===================( Users on 172.17.0.2 via RID cycling (RIDS: 500-550,1000-1050) )===================

[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)
S-1-5-21-1042354039-2475377354-766472396-1011 METASPLOITABLE\tty (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1012 METASPLOITABLE\man (Local User)
S-1-5-21-1042354039-2475377354-766472396-1013 METASPLOITABLE\disk (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1014 METASPLOITABLE\lp (Local User)
S-1-5-21-1042354039-2475377354-766472396-1015 METASPLOITABLE\lp (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1016 METASPLOITABLE\mail (Local User)
S-1-5-21-1042354039-2475377354-766472396-1017 METASPLOITABLE\mail (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1018 METASPLOITABLE\news (Local User)
S-1-5-21-1042354039-2475377354-766472396-1019 METASPLOITABLE\news (Domain Group)
```



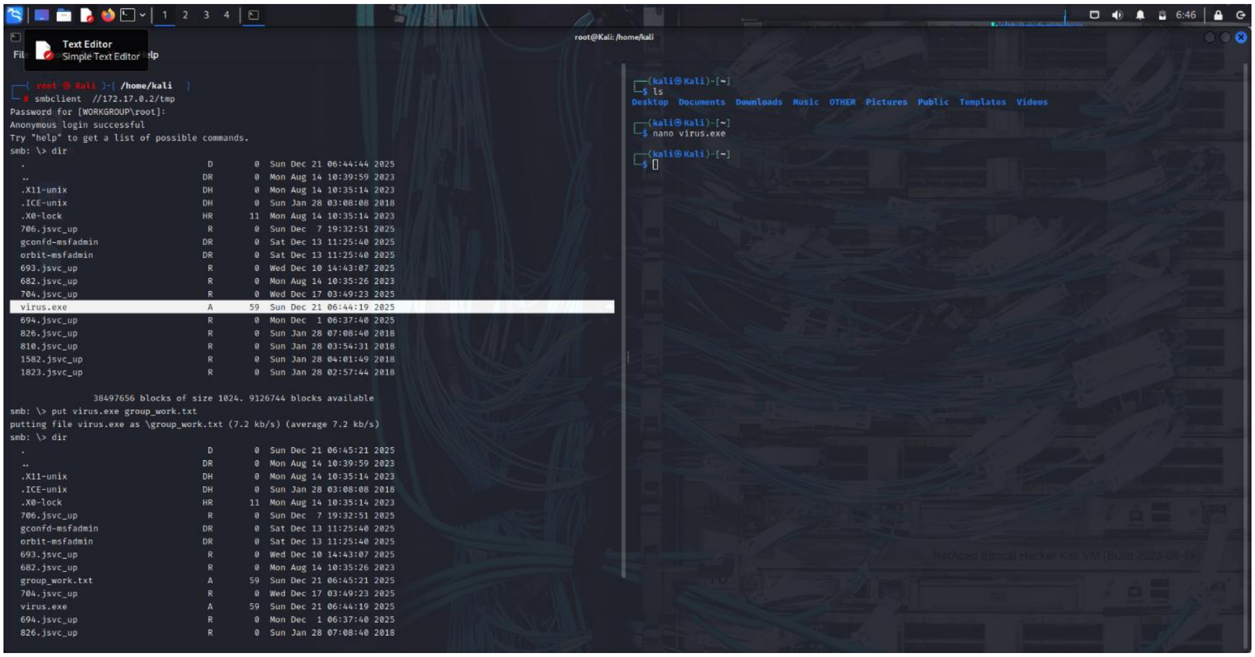
```
S-1-5-21-1042354039-2475377354-766472396-1008 METASPLOITABLE\sync (Local User)
S-1-5-21-1042354039-2475377354-766472396-1009 METASPLOITABLE\adm (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1010 METASPLOITABLE\games (Local User)
S-1-5-21-1042354039-2475377354-766472396-1011 METASPLOITABLE\tty (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1012 METASPLOITABLE\man (Local User)
S-1-5-21-1042354039-2475377354-766472396-1013 METASPLOITABLE\disk (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1014 METASPLOITABLE\lp (Local User)
S-1-5-21-1042354039-2475377354-766472396-1015 METASPLOITABLE\lp (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1016 METASPLOITABLE\mail (Local User)
S-1-5-21-1042354039-2475377354-766472396-1017 METASPLOITABLE\mail (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1018 METASPLOITABLE\news (Local User)
S-1-5-21-1042354039-2475377354-766472396-1019 METASPLOITABLE\news (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1020 METASPLOITABLE\uucp (Local User)
S-1-5-21-1042354039-2475377354-766472396-1021 METASPLOITABLE\uucp (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1025 METASPLOITABLE\man (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1026 METASPLOITABLE\proxy (Local User)
S-1-5-21-1042354039-2475377354-766472396-1027 METASPLOITABLE\proxy (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1031 METASPLOITABLE\kmem (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1041 METASPLOITABLE\dialout (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1043 METASPLOITABLE\fax (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1045 METASPLOITABLE\voice (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1049 METASPLOITABLE\cdrom (Domain Group)

 ================================( Getting printer info for 172.17.0.2 )================================

No printers returned.


enum4linux complete on Sun Dec 21 04:29:39 2025


┌──(root㉿Kali)-[/home/kali]
└─#
```

7. This will help us to list the shares available on the target host



```
 ================================( Getting printer info for 172.17.0.2 )================================

No printers returned.


enum4linux complete on Sun Dec 21 04:29:39 2025


┌──(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]
└─#
```

8. From the screenshot below we create a virus, and we put it into the host machine and masquerade it as **group_work.text**



```
┌──( 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  Sun Dec 21 06:44:44 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
  706.jsvc_up                         R        0  Sun Dec  7 19:32:51 2025
  gconfd-msfadmin                    DR        0  Sat Dec 13 11:25:40 2025
  orbit-msfadmin                     DR        0  Sat Dec 13 11:25:40 2025
  693.jsvc_up                         R        0  Wed Dec 10 14:43:07 2025
  682.jsvc_up                         R        0  Mon Aug 14 10:35:26 2023
  704.jsvc_up                         R        0  Wed Dec 17 03:49:23 2025
  virus.exe                           A       59  Sun Dec 21 06:44:19 2025
  694.jsvc_up                         R        0  Mon Dec  1 06:37:40 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. 9126744 blocks available
smb: \> put virus.exe group_work.txt
putting file virus.exe as \group_work.txt (7.2 kb/s) (average 7.2 kb/s)
smb: \> dir
  .                                   D        0  Sun Dec 21 06:45:21 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
  706.jsvc_up                         R        0  Sun Dec  7 19:32:51 2025
  gconfd-msfadmin                    DR        0  Sat Dec 13 11:25:40 2025
  orbit-msfadmin                     DR        0  Sat Dec 13 11:25:40 2025
  693.jsvc_up                         R        0  Wed Dec 10 14:43:07 2025
  682.jsvc_up                         R        0  Mon Aug 14 10:35:26 2023
  group_work.txt                      A       59  Sun Dec 21 06:45:21 2025
  704.jsvc_up                         R        0  Wed Dec 17 03:49:23 2025
  virus.exe                           A       59  Sun Dec 21 06:44:19 2025
  694.jsvc_up                         R        0  Mon Dec  1 06:37:40 2025
  826.jsvc_up                         R        0  Sun Jan 28 07:08:40 2018
```

```
┌──(kali㉿Kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  OTHER  Pictures  Public  Templates  Videos

┌──(kali㉿Kali)-[~]
└─$ nano virus.exe

┌──(kali㉿Kali)-[~]
└─$ 
```