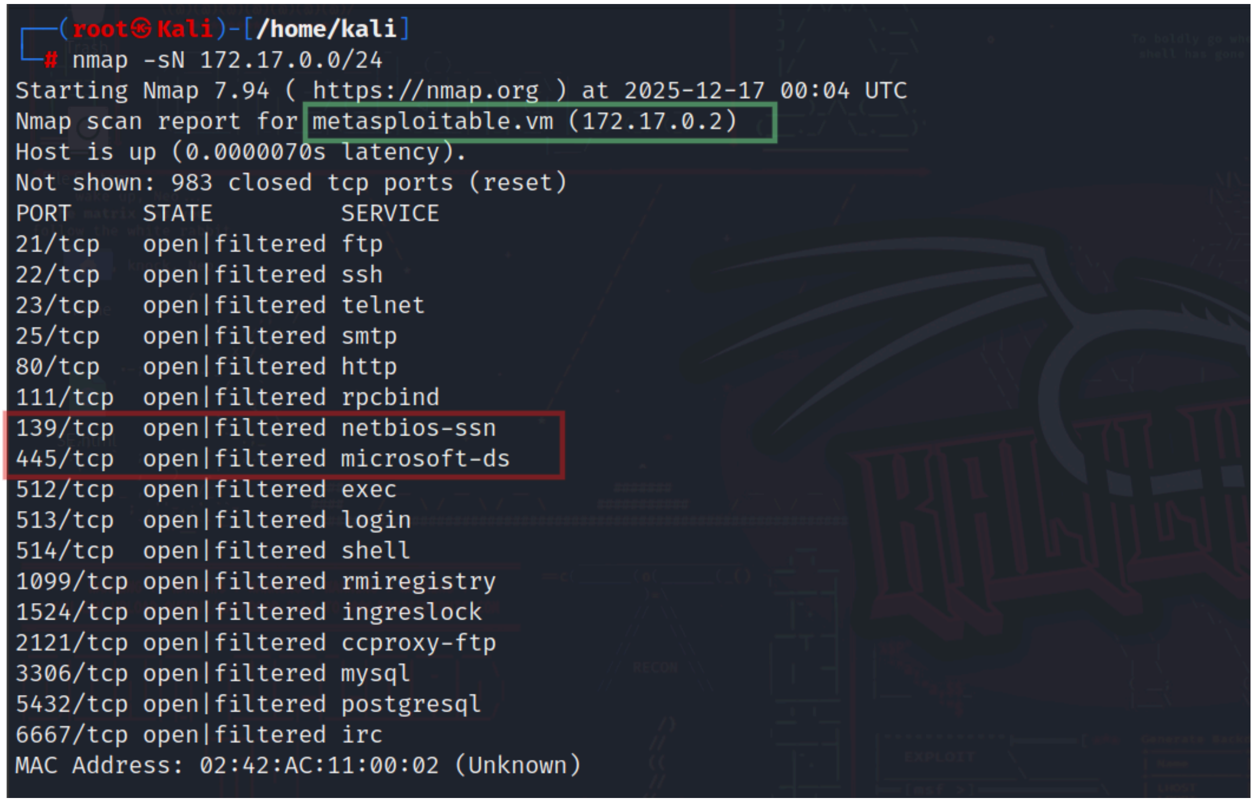
SMB Enumeration

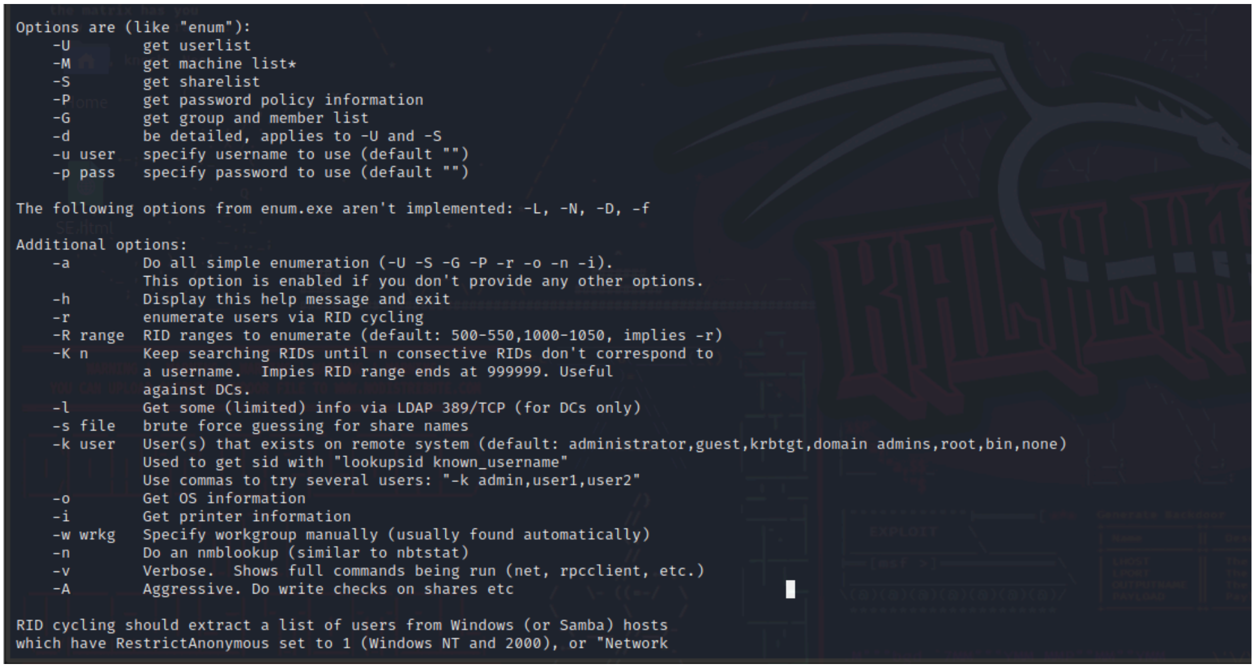
Name : Odebode Sunday Seun

Scan the network to see if smb port are open. Note from the screenshot Metasploit.vm (172.17.0.2) has it port 139 and 445 open which , make use of SMB.



```
┌──(root㉿Kali)-[/home/kali]
└─# nmap -sN 172.17.0.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-17 00:04 UTC
Nmap scan report for metasploitable.vm (172.17.0.2)
Host is up (0.0000070s 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)
```

A comprehensive cheat sheet of options for enumerating Windows/Samba hosts, from basic user/share lookups to advanced RID cycling and verbose checks — essential toolkit for SMB reconnaissance in pentesting labs

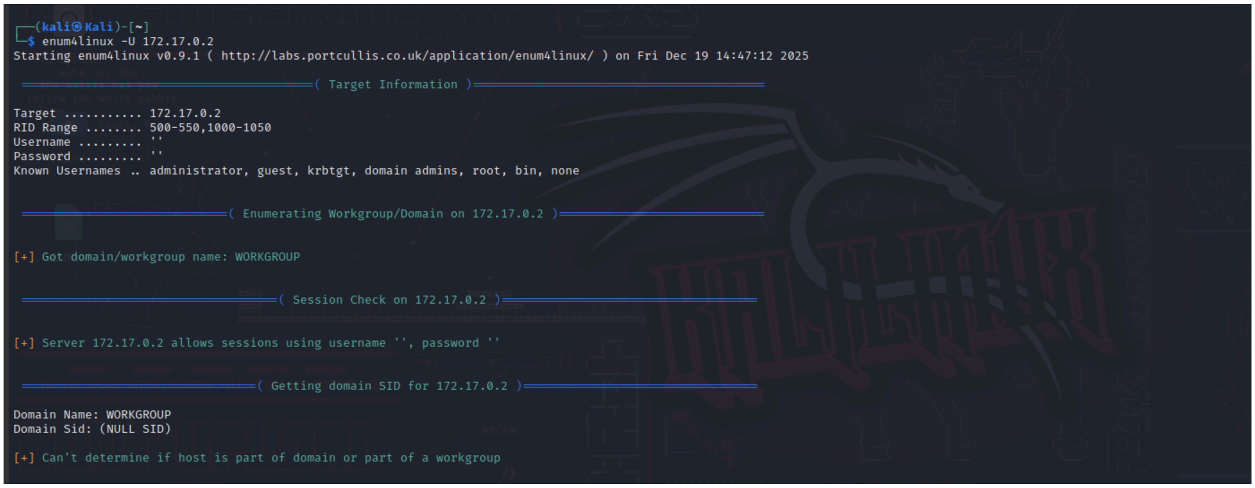


```
Options are (like "enum"):
    -U        get userlist
    -M        get machine list*
    -S        get sharelist
    -P        get password policy information
    -G        get group and member list
    -d        be detailed, applies to -U and -S
    -u user   specify username to use (default "")
    -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,none)
              Used to get sid with "lookupsid known_username"
              Use commas to try several users: "-k admin,user1,user2"
    -o        Get OS information
    -i        Get printer information
    -w wrkg   Specify workgroup manually (usually found automatically)
    -n        Do an nmblookup (similar to nbtstat)
    -v        Verbose.  Shows full commands being run (net, rpcclient, etc.)
    -A        Aggressive. Do write checks on shares etc

RID cycling should extract a list of users from Windows (or Samba) hosts
which have RestrictAnonymous set to 1 (Windows NT and 2000), or "Network
```

Get a list of user accounts on the target.

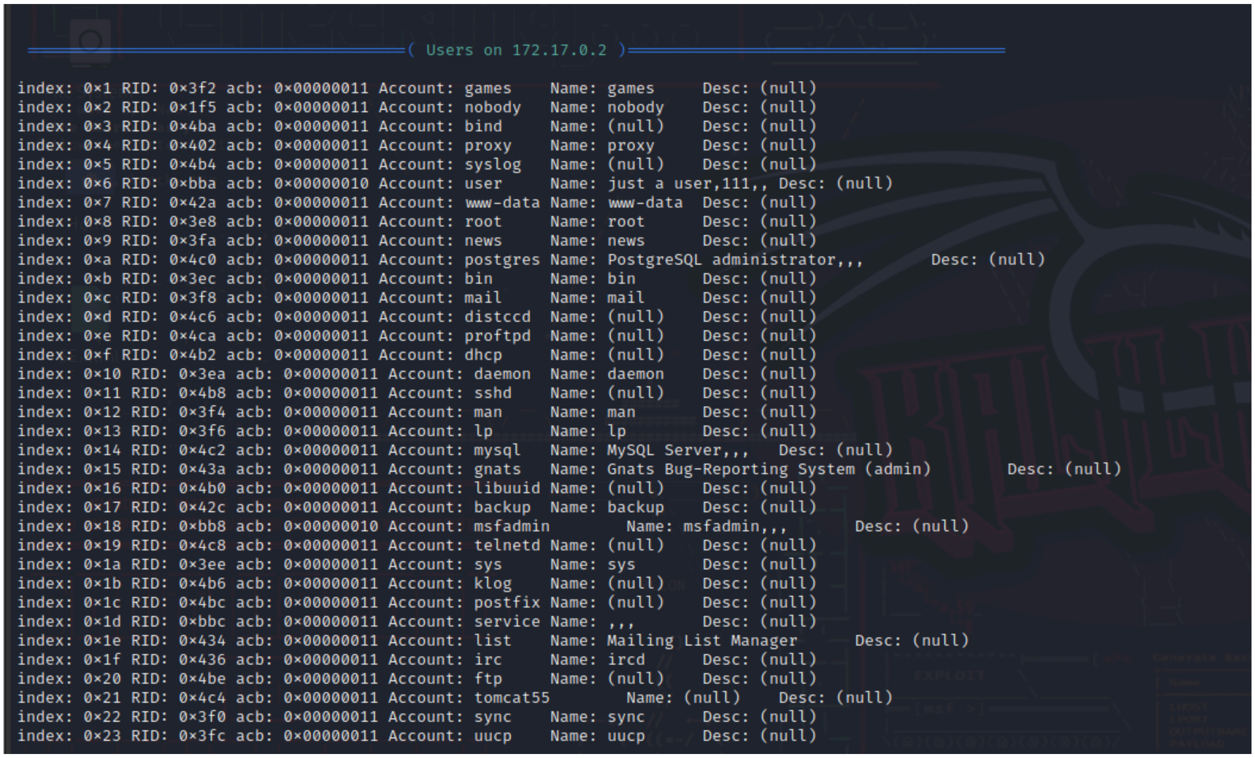
```
enum4linux -U 172.17.0.2
```

- **enum4linux**: A Perl tool (wrapper around Samba utilities like rpcclient, smbclient, net, nmblookup) that extracts information from Windows or Samba hosts, similar to the old Windows tool enum.exe.
- **U**: The option to specifically enumerate the **userlist** (get a list of user accounts on the target).
- **172.17.0.2**: The target IP address (in your previous screenshots, this is a vulnerable Metasploitable 2 machine)



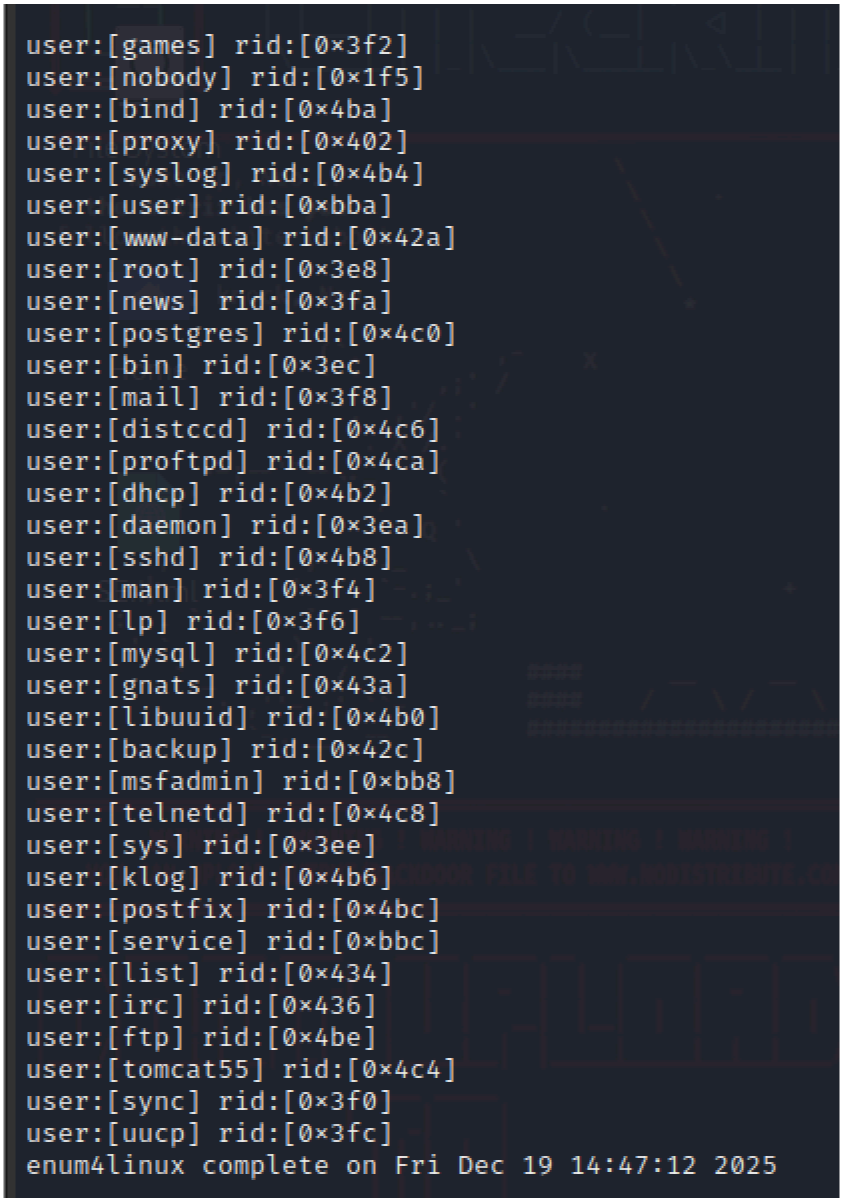
```
┌──(kali㉿Kali)-[~]
└─$ enum4linux -U 172.17.0.2
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Dec 19 14:47:12 2025

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

It shows a detailed list of enumerated user accounts on a Samba server at IP 172.17.0.2 (likely Metasploitable 2), including RIDs, account names (e.g., root, www-data, mysql, postgres, msfadmin), full names, and descriptions (mostly 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: 0×20 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)
```

lists of discovered user accounts with their Relative Identifiers (RIDs) in the format user:[username] rid:[hex_value], including common system accounts like root (0x3e8), www-data, mysql, postfix, sshd, and others.

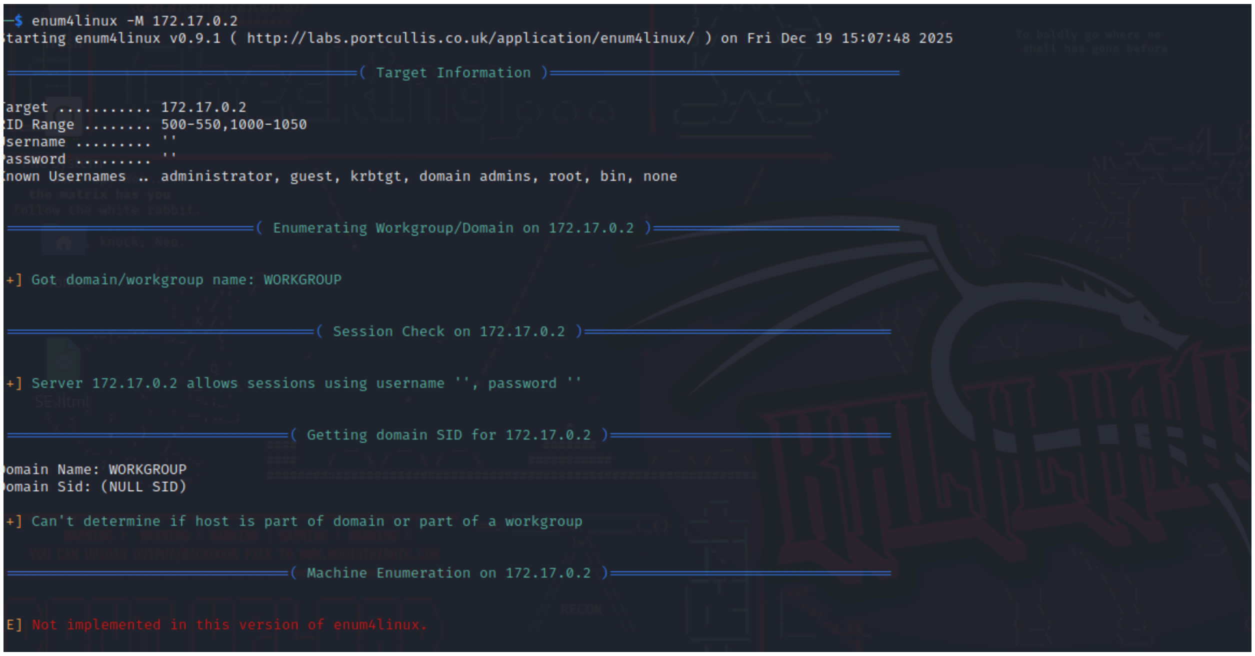


```
user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4]
user:[user] rid:[0xbba]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[postgres] rid:[0x4c0]
user:[bin] rid:[0x3ec]
user:[mail] rid:[0x3f8]
user:[distccd] rid:[0x4c6]
user:[proftpd] rid:[0x4ca]
user:[dhcp] rid:[0x4b2]
user:[daemon] rid:[0x3ea]
user:[sshd] rid:[0x4b8]
user:[man] rid:[0x3f4]
user:[lp] rid:[0x3f6]
user:[mysql] rid:[0x4c2]
user:[gnats] rid:[0x43a]
user:[libuuid] rid:[0x4b0]
user:[backup] rid:[0x42c]
user:[msfadmin] rid:[0xbb8]
user:[telnetd] rid:[0x4c8]
user:[sys] rid:[0x3ee]
user:[klog] rid:[0x4b6]
user:[postfix] rid:[0x4bc]
user:[service] rid:[0xbbc]
user:[list] rid:[0x434]
user:[irc] rid:[0x436]
user:[ftp] rid:[0x4be]
user:[tomcat55] rid:[0x4c4]
user:[sync] rid:[0x3f0]
user:[uucp] rid:[0x3fc]
enum4linux complete on Fri Dec 19 14:47:12 2025
```

Get the machine list

```
enum4linux -M 172.17.0.2
```

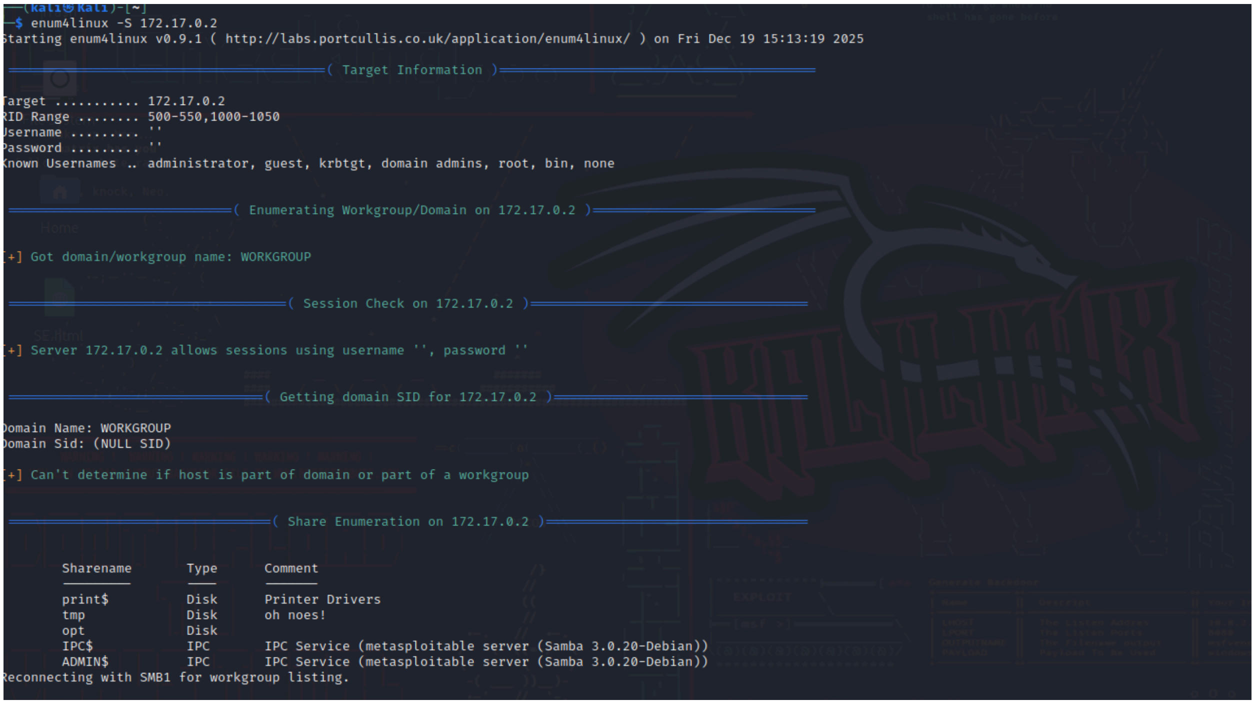
- **enum4linux**: A Perl-based tool that wraps Samba utilities (like rpcclient, net, nmblookup) to extract data from Windows or Samba systems, similar to the old Windows tool enum.exe.
- **M**: The option to specifically **get the machine list** — it attempts to enumerate computer/machine accounts on the target (e.g., domain-joined workstations or servers) via techniques like RID cycling or querying domain/machine SIDs.
- **172.17.0.2**: The target IP (in your context, likely the vulnerable Metasploitable 2 machine).



```
─$ enum4linux -M 172.17.0.2
tarting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Dec 19 15:07:48 2025

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

arget ........... 172.17.0.2
ID Range ........ 500-550,1000-1050
sername ......... ''
assword ......... ''
nown 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 )================================

omain Name: WORKGROUP
omain 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.
```

Get sharelist

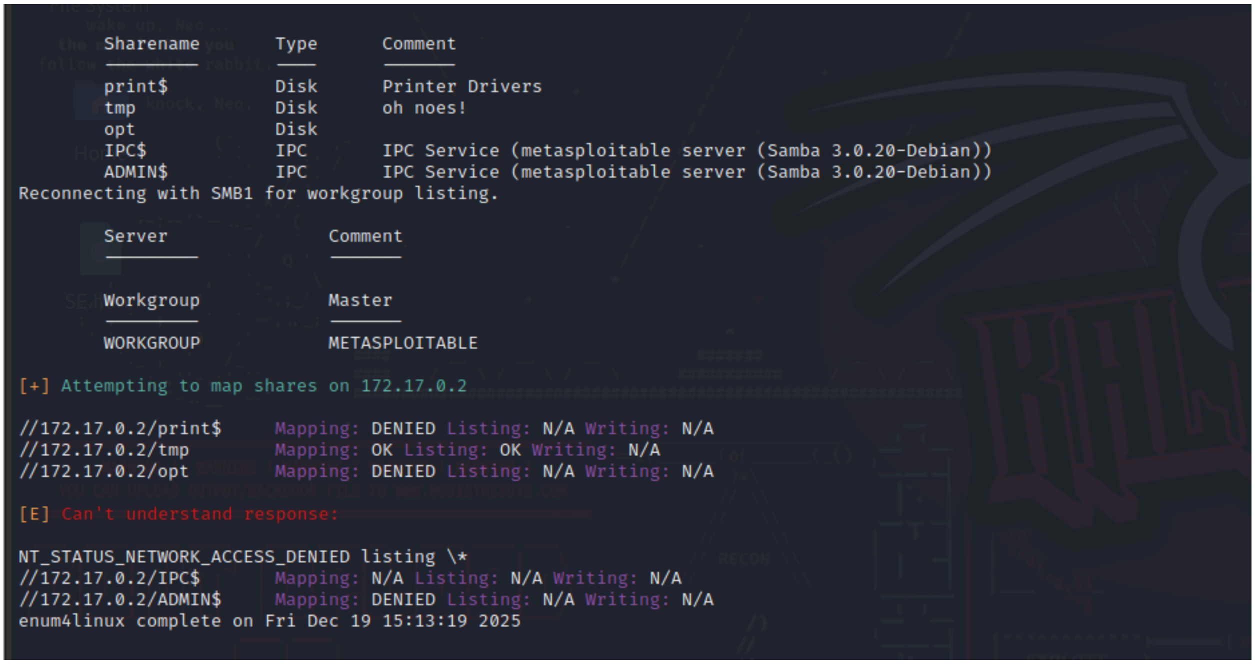
```
enum4linux -S 172.17.0.2
```



```
──(kali㉿kali)-[~]
─$ enum4linux -S 172.17.0.2
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Dec 19 15:13:19 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.
```

The Samba service here has known vulnerabilities, including:

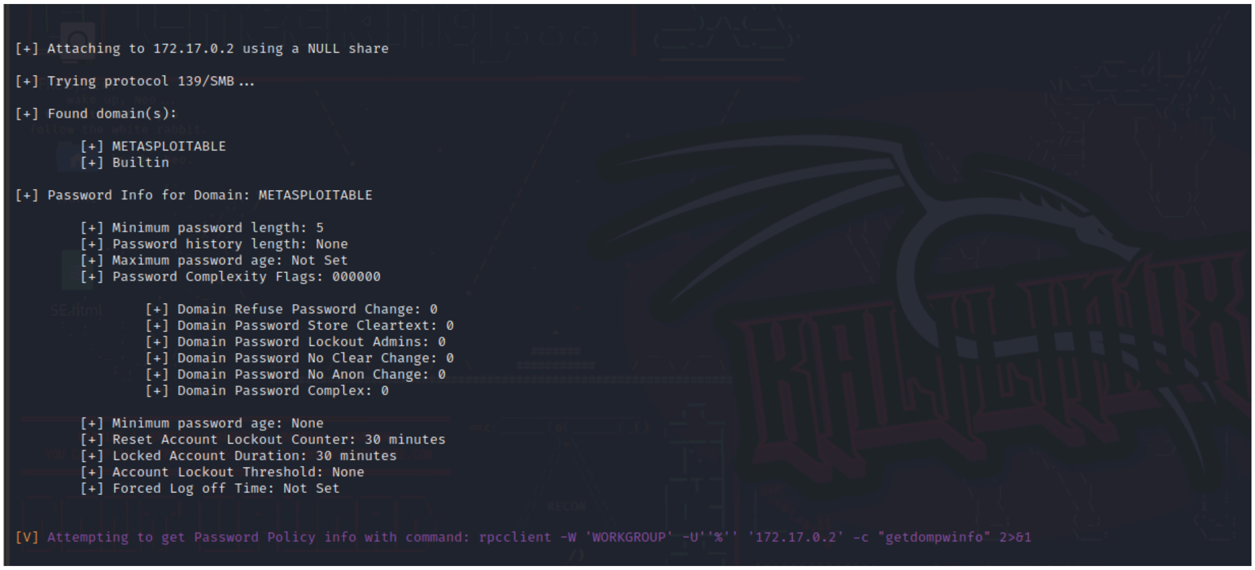
- Anonymous access to certain shares (like tmp).
- Potential for exploits like symlink traversal to gain root filesystem access.
- The famous "username map script" command execution vulnerability (CVE-2007-2447) in Samba 3.0.20–3.0.25.



```
        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 Fri Dec 19 15:13:19 2025
```

Get password policy information

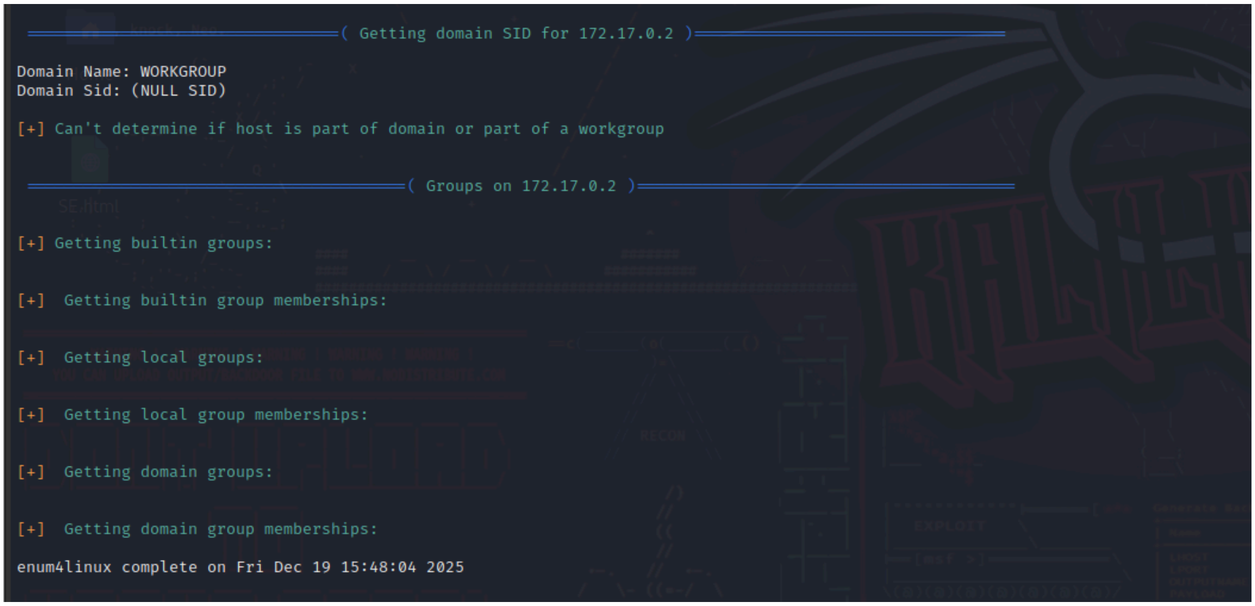
```
enum4linux -P 172.17.0.2
```



```
[+] 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


[V] Attempting to get Password Policy info with command: rpcclient -W 'WORKGROUP' -U''%'' '172.17.0.2' -c "getdompwinfo" 2>&1
```

Get the group and member list

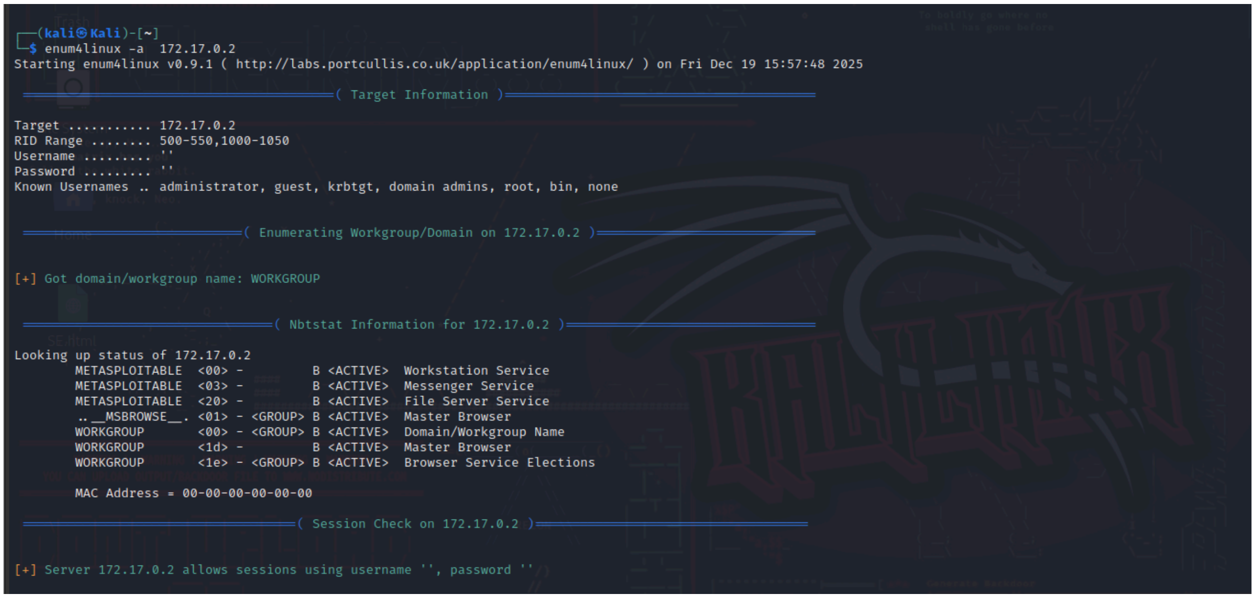
```
enum4linux -G 172.17.0.2
```



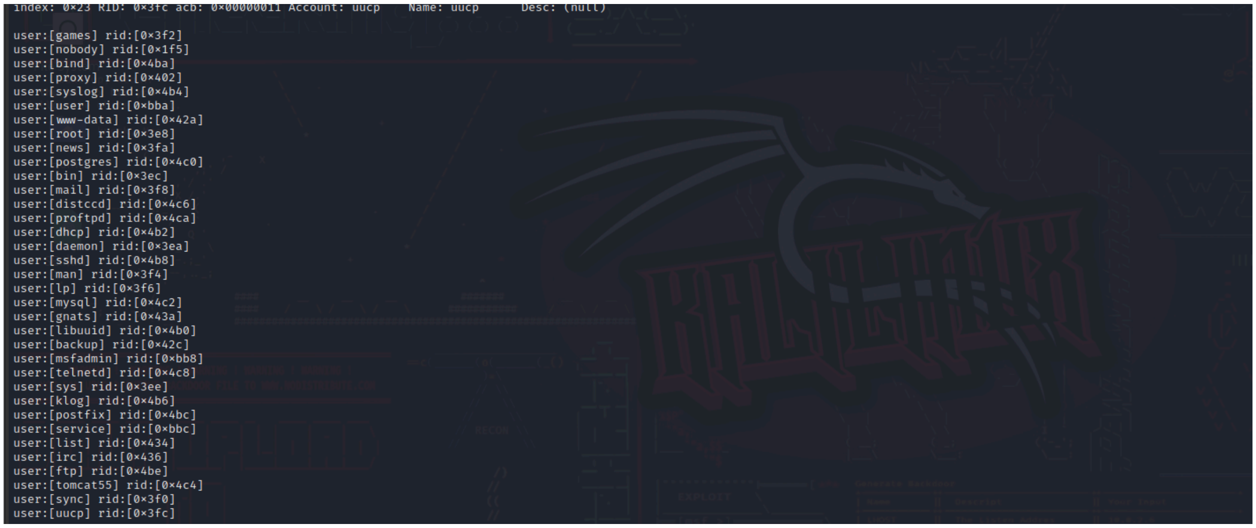
```
 ===========================( Getting domain SID for 172.17.0.2 )===========================

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

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

 ===================================( 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:

enum4linux complete on Fri Dec 19 15:48:04 2025
```

Do all simple enumeration (-U -S -G -P -r -o -n -i) i.e Arggressive enmuration

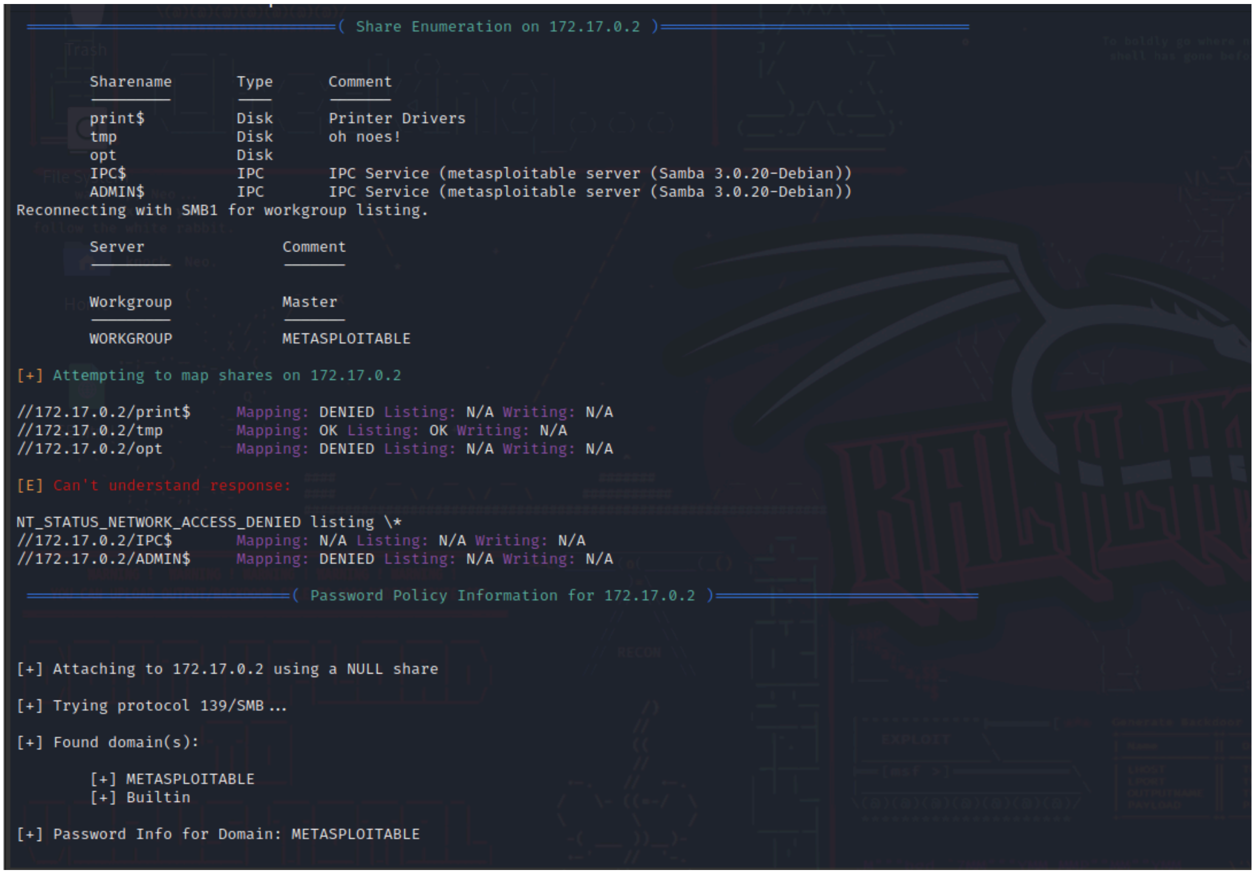
```
enum4linux -A  172.17.0.2
```



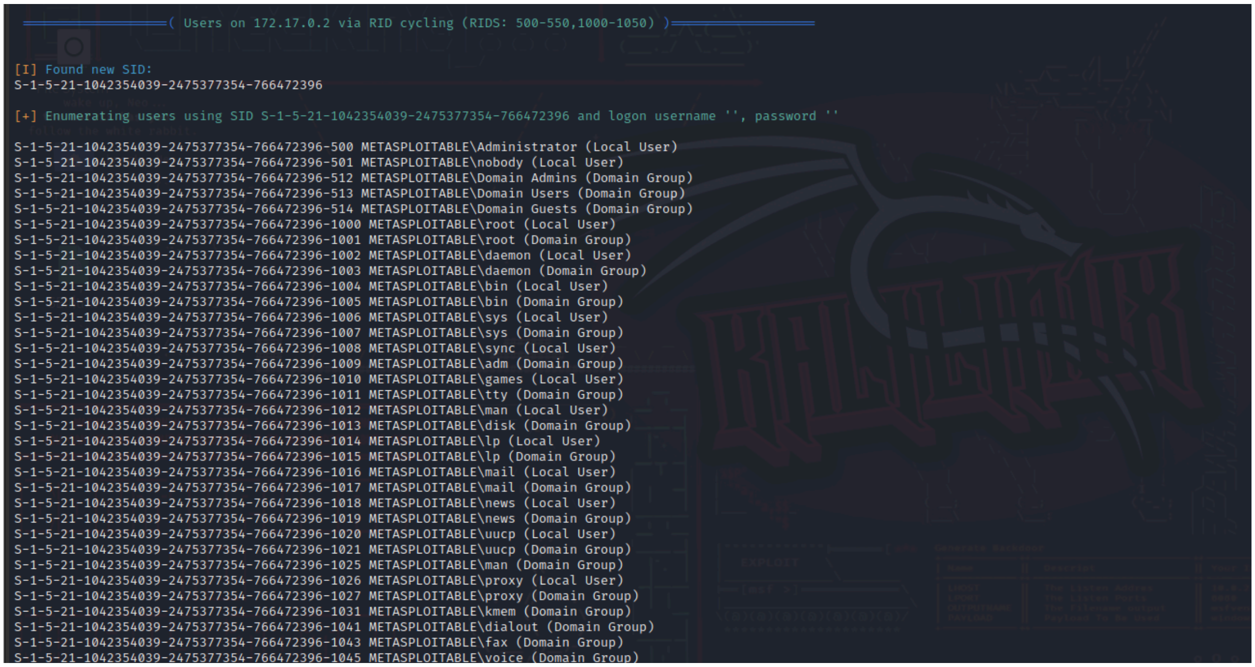
```
┌──(kali㉿Kali)-[~]
└─$ enum4linux -a  172.17.0.2
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Dec 19 15:57:48 2025

 ══════════════════════════════════════( 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 ''
```



```
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:[ftp] rid:[0×4be]
user:[tomcat55] rid:[0×4c4]
user:[sync] rid:[0×3f0]
user:[uucp] rid:[0×3fc]
```



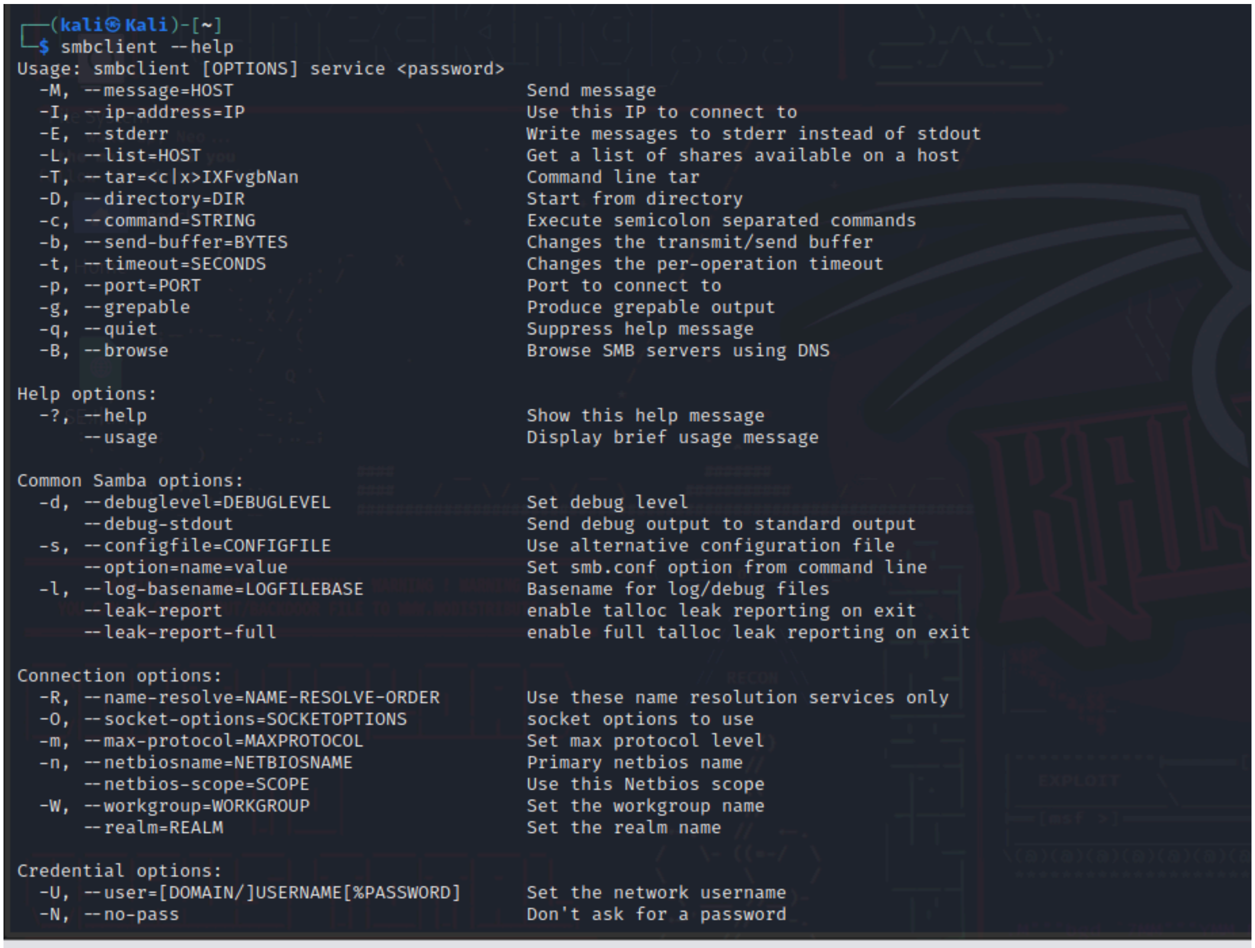
```
 ==========================( Share Enumeration on 172.17.0.2 )==========================

        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
```



```
 ===================( 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-1-5-21-1042354039-2475377354-766472396-1020 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)
```

SMBCIINET

This is like a big instruction book for a magic door tool called "smbclient". It tells you all the secret codes you can type to open doors to shared folders on another computer.

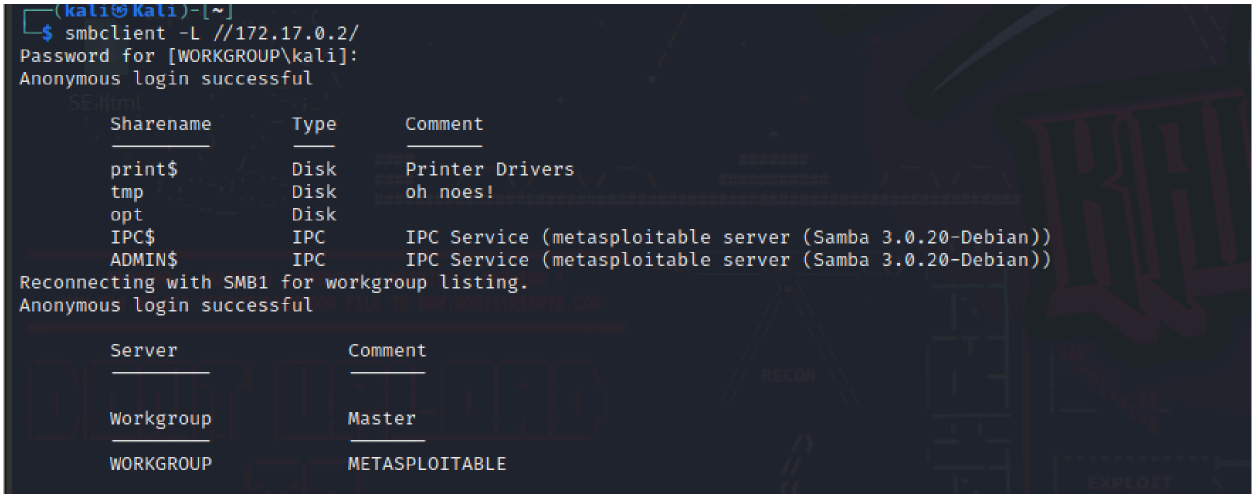


```
┌──(kali㉿Kali)-[~]
└─$ smbclient --help
Usage: smbclient [OPTIONS] service <password>
  -M, --message=HOST                          Send message
  -I, --ip-address=IP                         Use this IP to connect to
  -E, --stderr                                Write messages to stderr instead of stdout
  -L, --list=HOST                             Get a list of shares available on a host
  -T, --tar=<c|x>IXFvgbNan                    Command line tar
  -D, --directory=DIR                         Start from directory
  -c, --command=STRING                        Execute semicolon separated commands
  -b, --send-buffer=BYTES                     Changes the transmit/send buffer
  -t, --timeout=SECONDS                       Changes the per-operation timeout
  -p, --port=PORT                             Port to connect to
  -g, --grepable                              Produce grepable output
  -q, --quiet                                 Suppress help message
  -B, --browse                                Browse SMB servers using DNS

Help options:
  -?, --help                                  Show this help message
      --usage                                 Display brief usage message

Common Samba options:
  -d, --debuglevel=DEBUGLEVEL                 Set debug level
      --debug-stdout                          Send debug output to standard output
  -s, --configfile=CONFIGFILE                 Use alternative configuration file
      --option=name=value                     Set smb.conf option from command line
  -l, --log-basename=LOGFILEBASE              Basename for log/debug files
      --leak-report                           enable talloc leak reporting on exit
      --leak-report-full                      enable full talloc leak reporting on exit

Connection options:
  -R, --name-resolve=NAME-RESOLVE-ORDER       Use these name resolution services only
  -O, --socket-options=SOCKETOPTIONS          socket options to use
  -m, --max-protocol=MAXPROTOCOL              Set max protocol level
  -n, --netbiosname=NETBIOSNAME               Primary netbios name
      --netbios-scope=SCOPE                   Use this Netbios scope
  -W, --workgroup=WORKGROUP                   Set the workgroup name
      --realm=REALM                           Set the realm name

Credential options:
  -U, --user=[DOMAIN/]USERNAME[%PASSWORD]     Set the network username
  -N, --no-pass                               Don't ask for a password
```

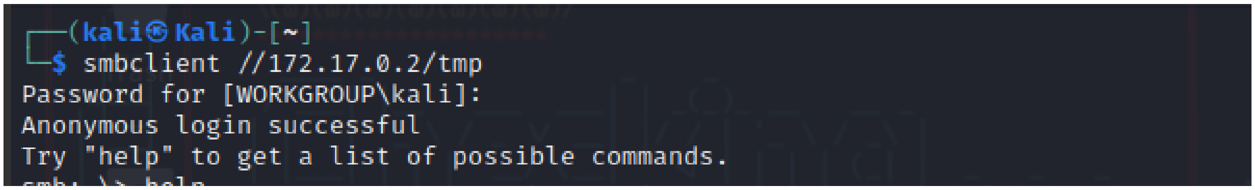
Listing all shares

```
smbclient -L //172.17.0.2/
```

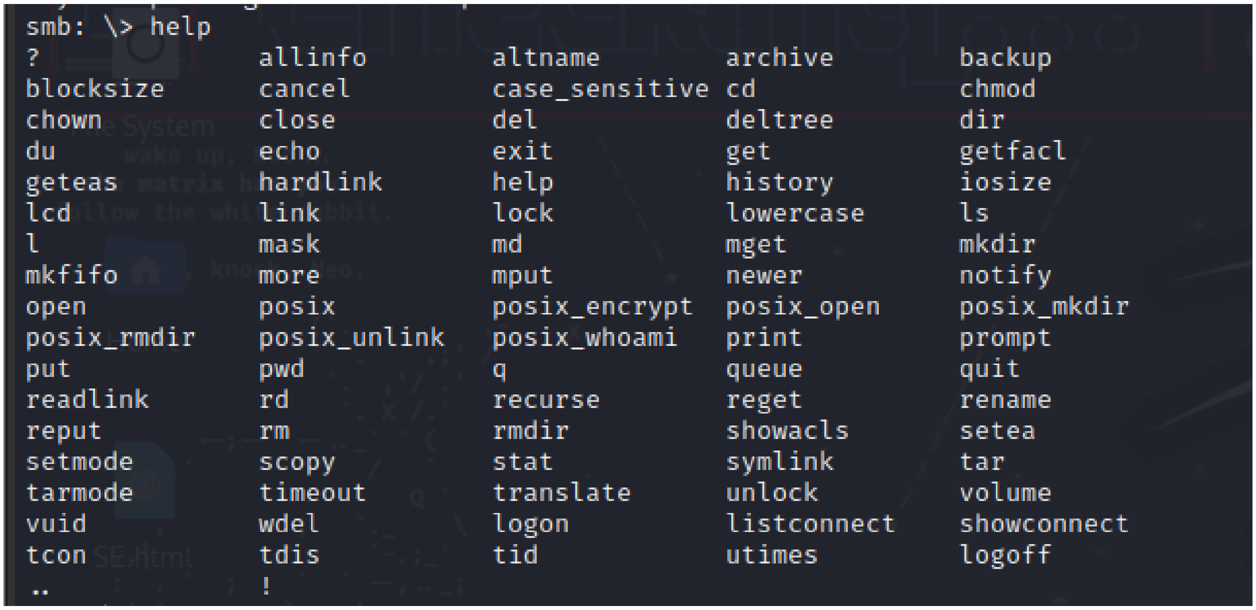
You knocked on the computer’s door and asked, “What folders are you sharing?” The computer answered and showed a list: print$, tmp, opt, IPC$, and ADMIN$. It even said its name is “METASPLOITABLE” and it’s part of a group called “WORKGROUP”.



```
┌──(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
```

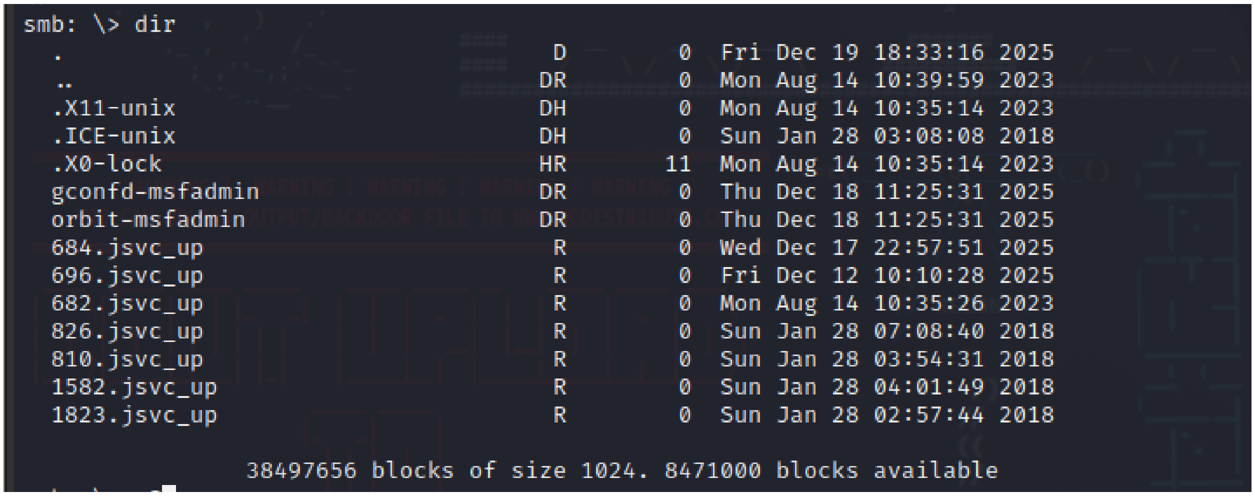


```
┌──(kali㉿Kali)-[~]
└─$ smbclient //172.17.0.2/tmp
Password for [WORKGROUP\kali]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> help
```



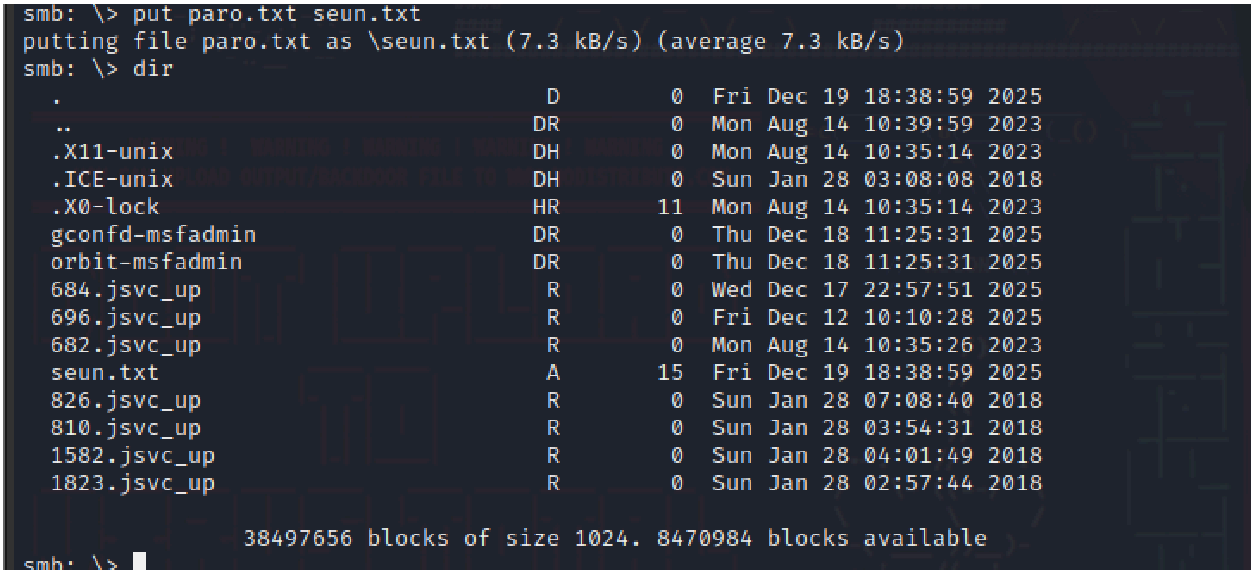
```
smb: \> help
?              allinfo        altname        archive        backup
blocksize      cancel         case_sensitive cd             chmod
chown          close          del            deltree        dir
du             echo           exit           get            getfacl
geteas         hardlink       help           history        iosize
lcd            link           lock           lowercase      ls
l              mask           md             mget           mkdir
mkfifo         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
..             !
```

“dir” which means “show me everything here”. The computer showed a bunch of files and folders with funny names like .X11-unix, .ICE-unix, and some files called jsVC_up.



```
smb: \> dir
  .                                   D        0  Fri Dec 19 18:33:16 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
  gconfd-msfadmin                    DR        0  Thu Dec 18 11:25:31 2025
  orbit-msfadmin                     DR        0  Thu Dec 18 11:25:31 2025
  684.jsvc_up                         R        0  Wed Dec 17 22:57:51 2025
  696.jsvc_up                         R        0  Fri Dec 12 10:10:28 2025
  682.jsvc_up                         R        0  Mon Aug 14 10:35:26 2023
  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. 8471000 blocks available
```

Puting file called “paro.txt” into the folder, and you renamed it “seun.txt” while putting it in. The computer said “Done!” and now your file is sitting there with all the other files.



```
smb: \> put paro.txt seun.txt
putting file paro.txt as \seun.txt (7.3 kB/s) (average 7.3 kB/s)
smb: \> dir
  .                                   D        0  Fri Dec 19 18:38:59 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
  gconfd-msfadmin                    DR        0  Thu Dec 18 11:25:31 2025
  orbit-msfadmin                     DR        0  Thu Dec 18 11:25:31 2025
  684.jsvc_up                         R        0  Wed Dec 17 22:57:51 2025
  696.jsvc_up                         R        0  Fri Dec 12 10:10:28 2025
  682.jsvc_up                         R        0  Mon Aug 14 10:35:26 2023
  seun.txt                            A       15  Fri Dec 19 18:38:59 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. 8470984 blocks available
smb: \>
```