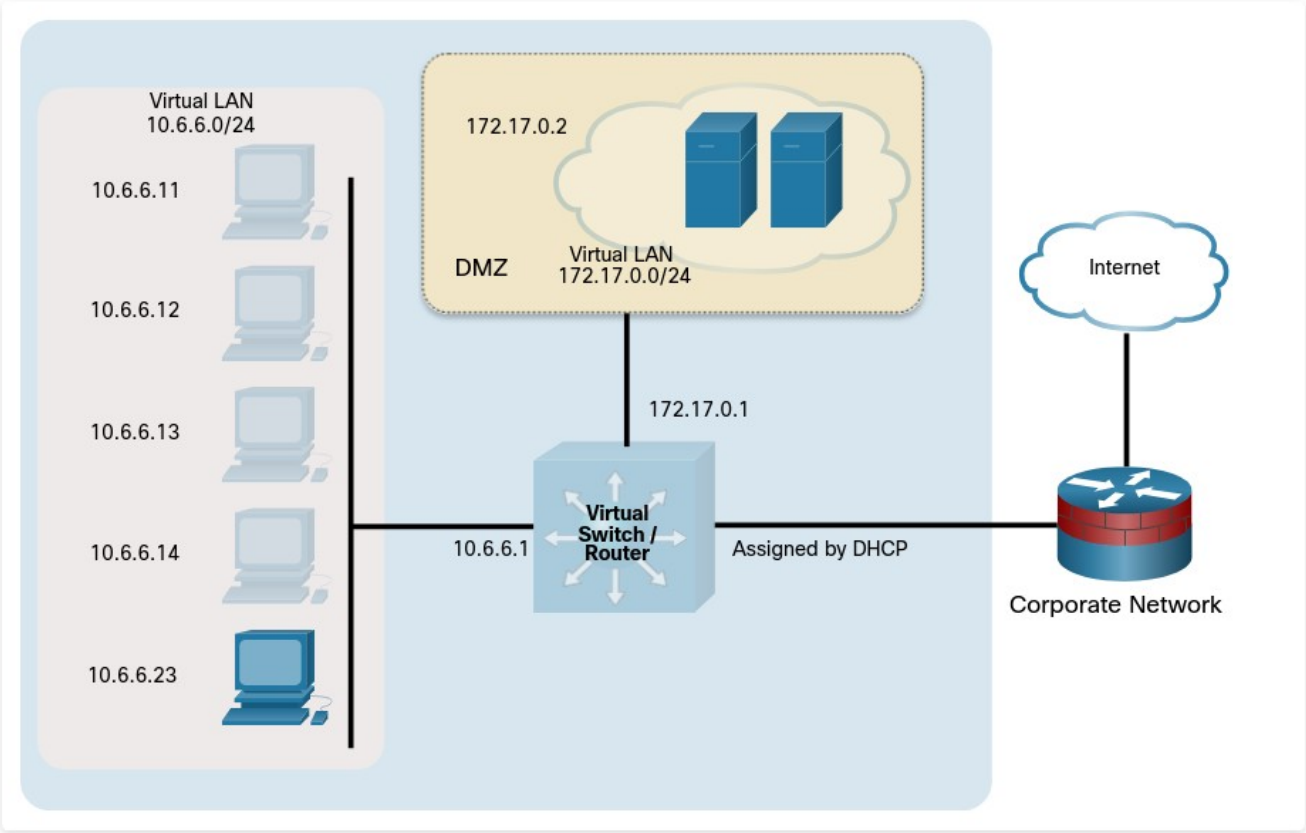

SMB
SMB VULNERABLE

Lab - Scanning for SMB Vulnerabilities with enum4linux
Introduction
Server Message Block (SMB) is a Microsoft protocol that is available on non-Microsoft networks through the open-source Samba service.
SMB makes it easy to set up and access network shares on LANs.
Many vulnerabilities have been found in it, and a number of high-profile exploits of it have appeared, such as WannaCry, Conficker, and EternalBlue.
In this lab you will get familiar with a popular tool that is used to discover network shares and other sensitive information through the exploitation of SMB.
You will also conduct a simulated exploit in which you transfer an unauthorized and potentially malicious file to an unprotected share.

Topology



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.

Required Resources

- Kali VM customized for the Ethical Hacker course

Instructions

Part 1: Launch enum4linux and explore its capabilities.

Step 1: Verify that enum4linux is installed and view the help file.

a. Load Kali Linux using the username **kali** and the password **kali**. Open a terminal session from the menu bar at the top of the screen.
b. Most enum4linux commands must be run as root, so use the **sudo su** command to obtain persistent root access.

At the prompt, enter the command to view the enum4linux help file.

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

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

Usage: ./enum4linux.pl [options] ip

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

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

Additional options:
    -a        Do all simple enumeration (-U -S -G -P -r -o -n -i).
              This option is enabled if you don't provide any other options.
    -h        Display this help message and exit
    -r        enumerate users via RID cycling
    -R range  RID ranges to enumerate (default: 500-550,1000-1050, implies -r)
    -K n      Keep searching RIDs until n consective RIDs don't correspond to
              a username.  Impies RID range ends at 999999. Useful
              against DCs.
    -l        Get some (limited) info via LDAP 389/TCP (for DCs only)
    -s file   brute force guessing for share names
    -k user   User(s) that exists on remote system (default: administrator,guest,krbtgt,domain admins,roo
              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
access: Allow anonymous SID/Name translation" enabled (XP, 2003).

NB: Samba servers often seem to have RIDs in the range 3000-3050.

Dependancy info: You will need to have the samba package installed as this
script is basically just a wrapper around rpcclient, net, nmblookup and
smbclient.  Polenum from http://labs.portcullis.co.uk/application/polenum/
is required to get Password Policy info.


┌──(root㉿Kali)-[/home/kali]
└─#
```

The help file contains the syntax and options available to enumerate host and server information on networks that use SMB. Enum4linux requires that Samba be installed on the host system, in this case the Kali Linux computer, because it is dependent on the built-in Samba utilities.

Which Samba utilities does the help file indicate are used by the enum4linux tool? **rpcclient, net, nmblookup and smbclient.**

Step 2: Research terms associated with SMB functions.

Many terms used in Windows and SMB functions may not be familiar to you, so the output of the enum4linux commands may be difficult to interpret at first. Use an internet search engine to find the definition of the terms listed.

Relative Identifier (RID): The final numeric component of a SID that uniquely identifies a security principal within its domain or local system.
Security Identifier (SID): The unique alphanumeric string that identifies a security principal in Windows environments.
Domain Controller (DC): a server that responds to security authentication requests within a computer network domain.
Lightweight Directory Access Protocol (LDAP): an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.
Workgroup: a peer-to-peer local area network(LAN).

Part 2: Use Nmap to Find SMB Servers.

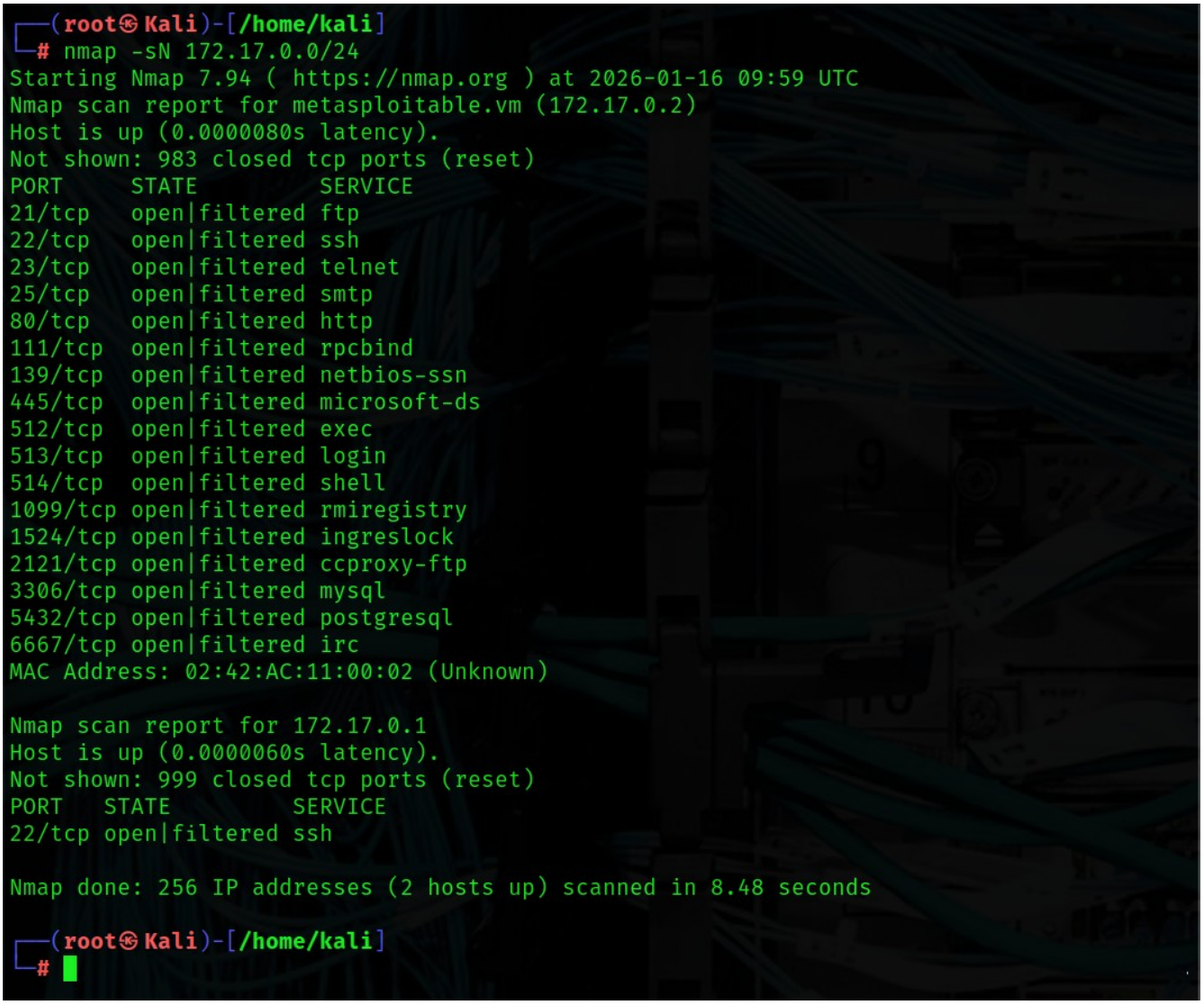
Step 1: Scan the virtual networks to find potential targets.

One way to identify potential targets for SMB enumeration is to examine the open ports. Common open ports on SMB servers are:

TCP 135	RPC
TCP 139	NetBIOS Session
TCP 389	LDAP Server
TCP 445	SMB File Service
TCP 9389	Active Directory Web Services
TCP/UDP 137	NetBIOS Name Service
UDP 138	NetBIOS Datagram

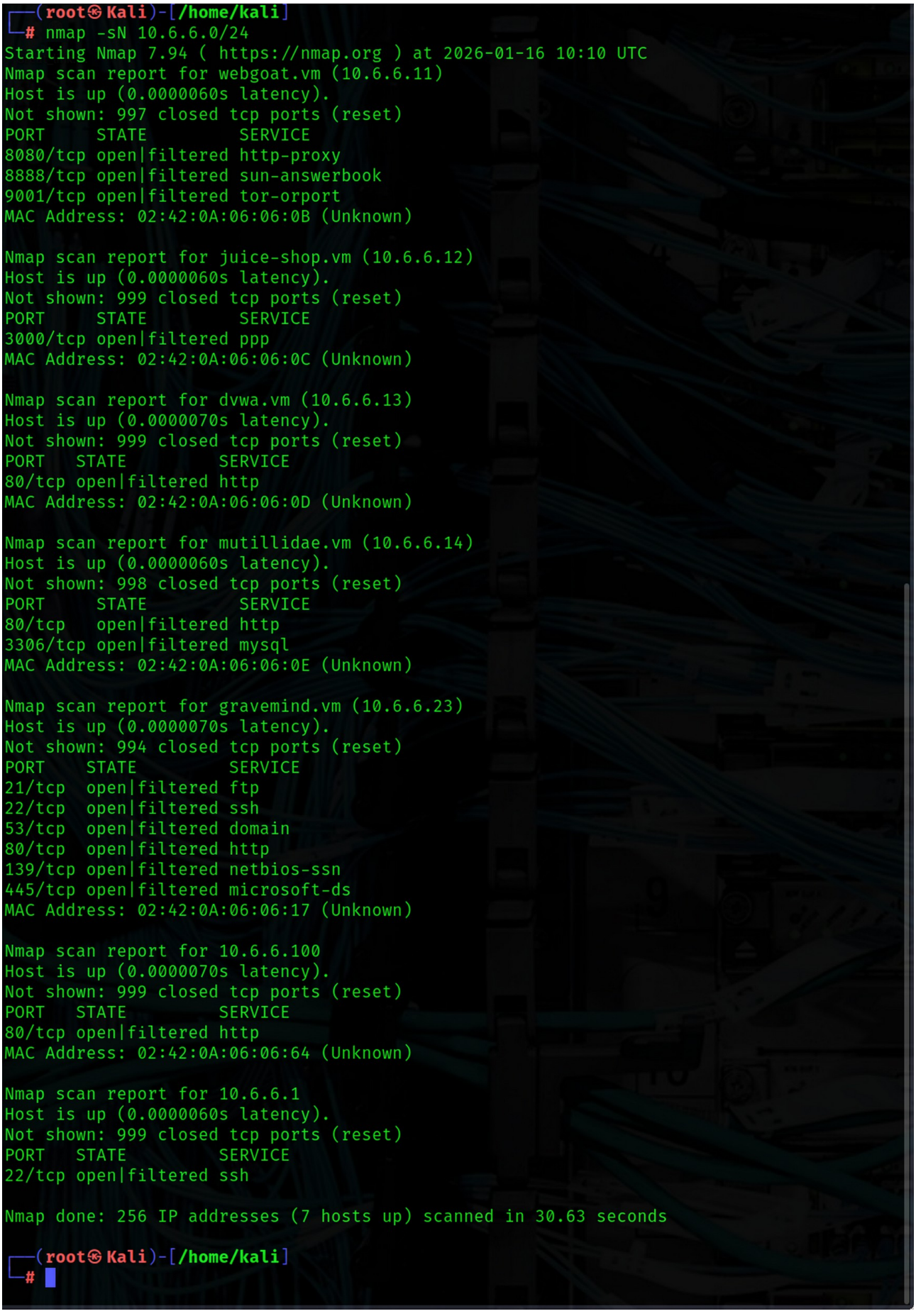
a. Two virtual networks are included in the Kali VM with Docker containers. Use the **nmap -sN** command to find the services available on hosts in the 172.17.0.0 virtual network.

What does Nmap reveal about hosts on the 172.17.0.0/24 network? **Only 2 host are present 172.17.0.1 and 172.17.0.2**



What ports are open on the host that identify running SMB services? What does Nmap call these services? **TCP 139 netbios-ssn and TCP 445 microsoft-ds.**

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



Are there any potential target computers on this subnet running SMB services? Which computer or computers? How do you know?
Yes, 10.6.6.23, it has open port 139, netbios-ssn and 445, microsoft-ds.

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.

Step 1: Perform an enum4linux scan on target 172.17.0.2.

In Part 1, Step 1c, you used the enum4linux help page to learn about the options available to enumerate potential targets. The most common options are:

-U find configured users

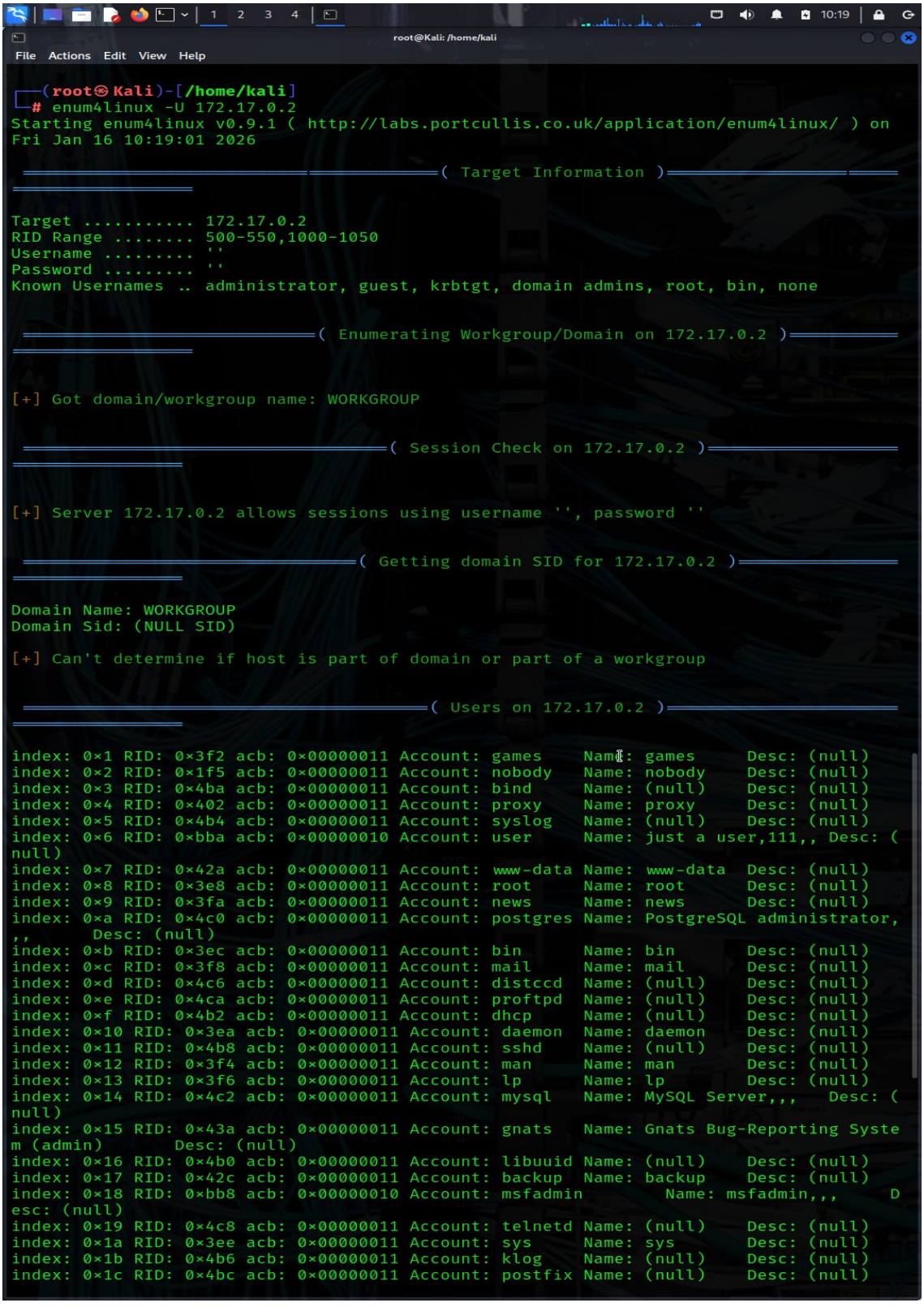
-S get a list of file shares

-G get a list of the groups and their members

-P list the password policies

-i get a list of printers

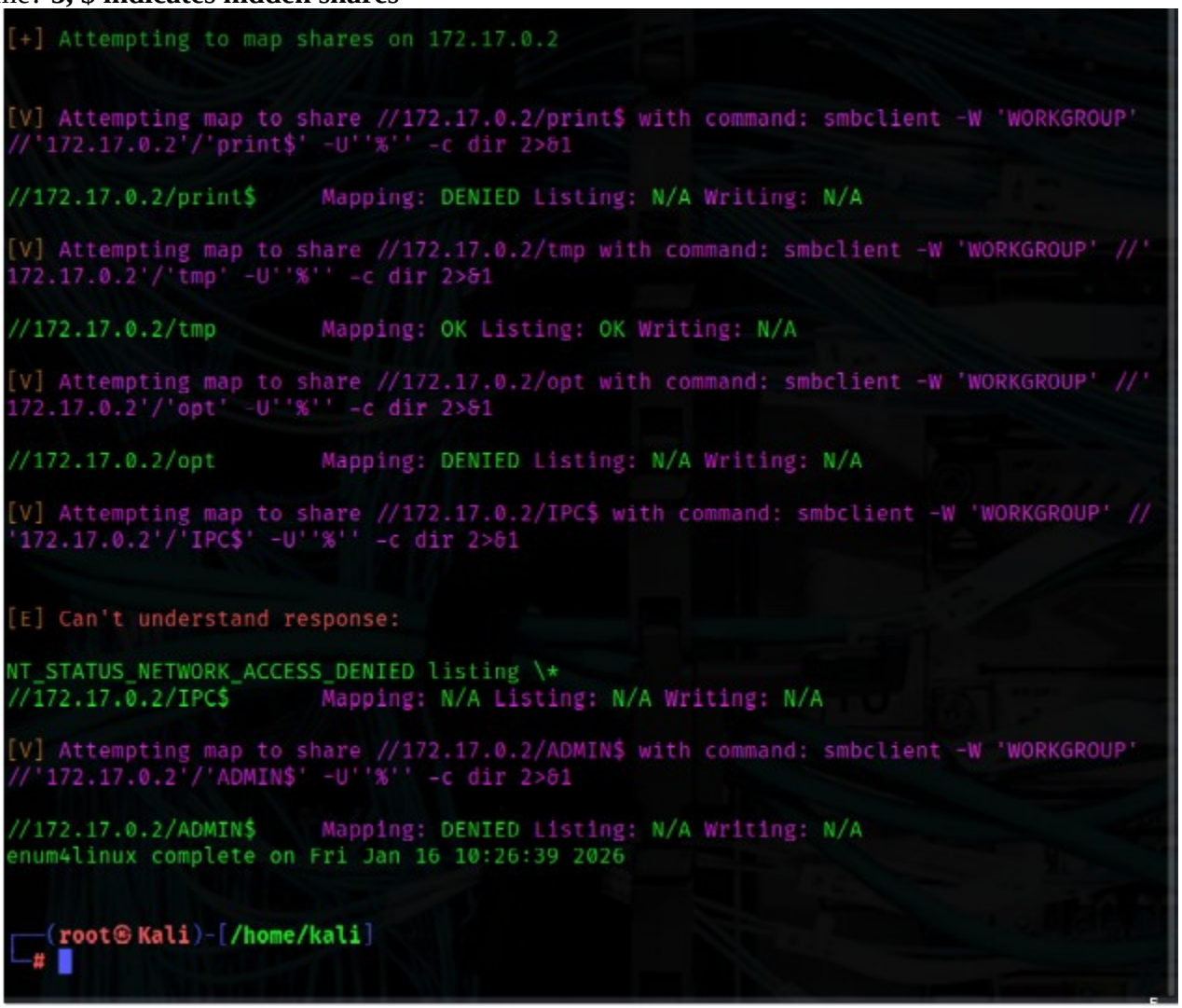
a. Use the **enum4linux -U** option to list the users configured on the target 172.17.0.2. Remember that enum4linux commands require root permissions to execute.


root@Kali: /home/kali
File Actions Edit View Help
┌──(root㉿Kali)-[/home/kali]
└─# enum4linux -U 172.17.0.2
Starting enum4linux v0.9.1 (http://labs.portcullis.co.uk/application/enum4linux/) on Fri Jan 16 10:19:01 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
(Session Check on 172.17.0.2)
[+] Server 172.17.0.2 allows sessions using username '', password ''
(Getting domain SID for 172.17.0.2)
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup
(Users on 172.17.0.2)
index: 0x1 RID: 0x3f2 acb: 0x00000011 Account: games Name: games Desc: (null)
index: 0x2 RID: 0x1f5 acb: 0x00000011 Account: nobody Name: nobody Desc: (null)
index: 0x3 RID: 0x4ba acb: 0x00000011 Account: bind Name: (null) Desc: (null)
index: 0x4 RID: 0x402 acb: 0x00000011 Account: proxy Name: proxy Desc: (null)
index: 0x5 RID: 0x4b4 acb: 0x00000011 Account: syslog Name: (null) Desc: (null)
index: 0x6 RID: 0xbba acb: 0x00000010 Account: user Name: just a user,111,, Desc: (null)
index: 0x7 RID: 0x42a acb: 0x00000011 Account: www-data Name: www-data Desc: (null)
index: 0x8 RID: 0x3e8 acb: 0x00000011 Account: root Name: root Desc: (null)
index: 0x9 RID: 0x3fa acb: 0x00000011 Account: news Name: news Desc: (null)
index: 0xa RID: 0x4c0 acb: 0x00000011 Account: postgres Name: PostgreSQL administrator,,, Desc: (null)
index: 0xb RID: 0x3ec acb: 0x00000011 Account: bin Name: bin Desc: (null)
index: 0xc RID: 0x3f8 acb: 0x00000011 Account: mail Name: mail Desc: (null)
index: 0xd RID: 0x4c6 acb: 0x00000011 Account: distccd Name: (null) Desc: (null)
index: 0xe RID: 0x4ca acb: 0x00000011 Account: proftpd Name: (null) Desc: (null)
index: 0xf RID: 0x4b2 acb: 0x00000011 Account: dhcp Name: (null) Desc: (null)
index: 0x10 RID: 0x3ea acb: 0x00000011 Account: daemon Name: daemon Desc: (null)
index: 0x11 RID: 0x4b8 acb: 0x00000011 Account: sshd Name: (null) Desc: (null)
index: 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) Desc: (null)
index: 0x16 RID: 0x4b0 acb: 0x00000011 Account: libuuid Name: (null) Desc: (null)
index: 0x17 RID: 0x42c acb: 0x00000011 Account: backup Name: backup Desc: (null)
index: 0x18 RID: 0xbb8 acb: 0x00000010 Account: msfadmin Name: msfadmin,,, Desc: (null)
index: 0x19 RID: 0x4c8 acb: 0x00000011 Account: telnetd Name: (null) Desc: (null)
index: 0x1a RID: 0x3ee acb: 0x00000011 Account: sys Name: sys Desc: (null)
index: 0x1b RID: 0x4b6 acb: 0x00000011 Account: klog Name: (null) Desc: (null)
index: 0x1c RID: 0x4bc acb: 0x00000011 Account: postfix Name: (null) Desc: (null)

The output of this command can generate multiple screens of information if many users are discovered. Enum4linux aggregates output from multiple Samba tools to produce a concise result. If you want to see how each feature is used, use the verbose option (**-v**) with the command.

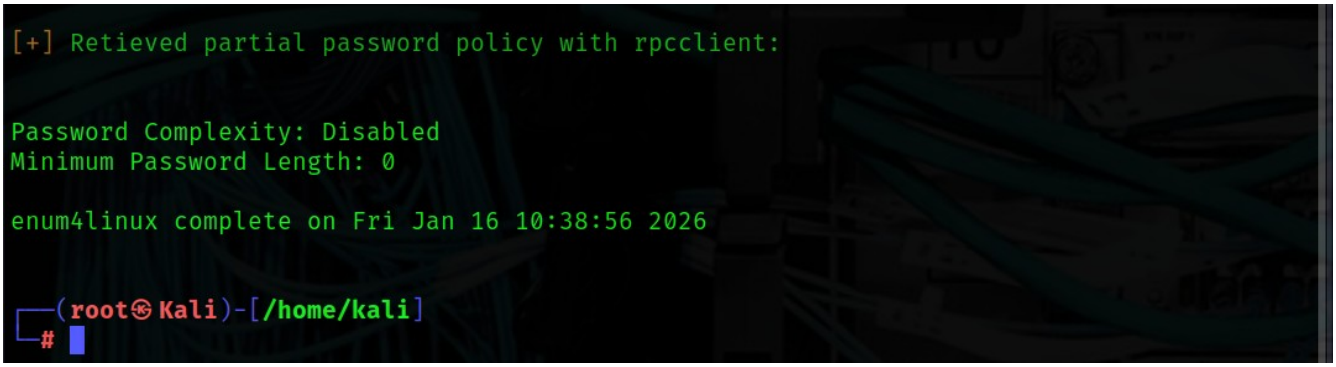
Note the **[V]** at the beginning of some of the lines of output. The verbose mode provides a narrative of how the results were obtained. For example, in the **Enumerating Workgroup/Domain** section of the output, enum4linux attempted to get the domain name using the command: **nmblookup -A '172.17.0.2'**.

Which Samba tool was used to map the file shares? **smbclient**
How many file shares are listed for target 172.17.0.2? What does the $ indicate at the end of the share name? **5, $ indicates hidden shares**



c. 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.


root@Kali: /home/kali
File Actions Edit View Help
└─# enum4linux -P 172.17.0.2
Starting enum4linux v0.9.1 (http://labs.portcullis.co.uk/application/enum4linux/) on Fri Jan 16 10:38:55 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
(Session Check on 172.17.0.2)
[+] Server 172.17.0.2 allows sessions using username '', password ''
(Getting domain SID for 172.17.0.2)
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup
(Password Policy Information for 172.17.0.2)
[+] Attaching to 172.17.0.2 using a NULL share
[+] Trying protocol 139/SMB ...
[+] Found domain(s):
[+] METASPLOITABLE
[+] Builtin
[+] Password Info for Domain: METASPLOITABLE
[+] Minimum password length: 5
[+] Password history length: None
[+] Maximum password age: Not Set
[+] Password Complexity Flags: 000000
[+] Domain Refuse Password Change: 0
[+] Domain Password Store Cleartext: 0
[+] Domain Password Lockout Admins: 0
[+] Domain Password No Clear Change: 0
[+] Domain Password No Anon Change: 0
[+] Domain Password Complex: 0
[+] Minimum password age: None
[+] Reset Account Lockout Counter: 30 minutes
[+] Locked Account Duration: 30 minutes
[+] Account Lockout Threshold: None
[+] Forced Log off Time: Not Set
[+] Retieved partial password policy with rpcclient:



What is the minimum password length set for accounts on this server? What is the account lockout threshold setting? **5, none**

How would rate the security of the password policy set for this domain? Low, medium, or high? Explain.
Low. The minimum password length is too short. The password complexity flag is 000000. Microsoft documents this value as meaning no password complexity policy is set. Also, no minimum password age is configured.

Step 2: 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.

Use the **enum4linux -a** command to perform a scan on the potential Samba server target that you identified in Part 2.

Command: **`enum4linux -a 10.6.6.23`**

```
┌──(root㉿Kali)-[/home/kali]
└─# enum4linux -a 10.6.6.23
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on
Fri Jan 16 10:45:21 2026

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

Target ..... 10.6.6.23
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ==========( Enumerating Workgroup/Domain on 10.6.6.23 )==========


[E] Can't find workgroup/domain


 ==========( Nbtstat Information for 10.6.6.23 )==========

Looking up status of 10.6.6.23
No reply from 10.6.6.23

 ==========( Session Check on 10.6.6.23 )==========


[+] Server 10.6.6.23 allows sessions using username '', password ''


 ==========( Getting domain SID for 10.6.6.23 )==========

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

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


 ==========( OS information on 10.6.6.23 )==========


[E] Can't get OS info with smbclient


[+] Got OS info for 10.6.6.23 from srvinfo:
        GRAVEMIND      Wk Sv PrQ Unx NT SNT Samba 4.9.5-Debian
        platform_id     :       500
        os version      :       6.1
        server type     :       0x809a03


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

```
index: 0x1 RID: 0x3e8 acb: 0x00000015 Account: masterchief      Name:   Desc:
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

 ==========================================( Password Policy Information for 10.6.6.23 )==========================================


[+] Attaching to 10.6.6.23 using a NULL share

[+] Trying protocol 139/SMB ...

[+] Found domain(s):

        [+] GRAVEMIND
        [+] Builtin

[+] Password Info for Domain: GRAVEMIND

        [+] Minimum password length: 5
        [+] Password history length: None
        [+] Maximum password age: 37 days 6 hours 21 minutes
        [+] 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: 37 days 6 hours 21 minutes
```

```
[+] Retieved partial password policy with rpcclient:

Password Complexity: Disabled
Minimum Password Length: 5

 ═══════════════════════════════════════( 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-1-22-1 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)

[+] 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 use
rname '', password ''

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)

 ==========( Getting printer info for 10.6.6.23 )==========
==========

No printers returned.


enum4linux complete on Fri Jan 16 10:46:04 2026


┌──(root㉿Kali)-[/home/kali]
└─#
```

How many local users and groups are there on target 10.6.6.23? **3 local user and 7 local groups**

What are the shares that are located on this target? **homes, workfiles, and print$. The IPC$ share is for the server process itself. It is created by default.**

```
  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)
ecting with SMB1 for workgroup listing
```

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.

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

b. Take a look at the options available with smbclient using the command **smbclient –help** command.

c. Use the **smbclient -L** command to list the shares on the target host. This command produces a similar output to what the enum4linx command did in Part 3. 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.

d. Connect to the **tmp** share using the **smbclient** command by specifying the share name and IP address.

```
┌──(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: \>
```

Note that the prompt changed to the **smb:>** prompt. Type **help** to see what commands are available.

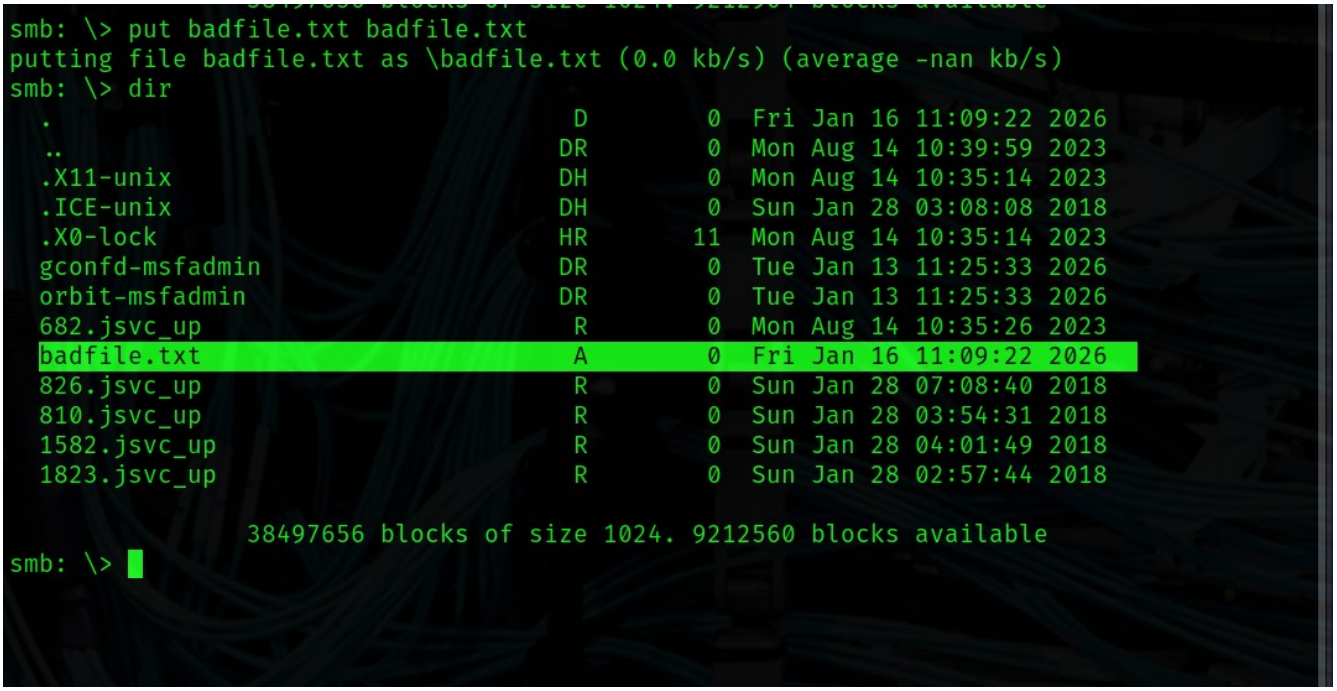
e. Enter **dir** to view the contents of the share.

```
┌──(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  Fri Jan 16 11:07:55 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
  gconfd-msfadmin                    DR        0  Tue Jan 13 11:25:33 2026
  orbit-msfadmin                     DR        0  Tue Jan 13 11:25:33 2026
  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. 9212904 blocks available
smb: \>
```

f. Upload the **badfile.txt** to the target server using the **put** command. The syntax for the command is: **put** ***local-file-name remote-file-name***

g. Verify that the file successfully uploaded using the **dir** command.



h. Type **quit** to exit the **smbclient** and return to the CLI prompt.

Reflect:

You are conducting a penetration test of a client network. You have gained access to an internal network by social engineering the username and password of an ad hoc webserver that is not behind the firewall. You can remotely access the network from a Kali VM configured with the enum4linux tool. What steps would you follow to send a dummy malware file to hosts on the network as part of the penetration test?

- Use a network scanning tool like **`Nmap to i`**dentify hosts on the internal network that have SMB services running.
- Once potential targets with open SMB ports are identified, use the **`enum4linux`** tool to enumerate detailed information, specifically the available network shares.
- Review the **`enum4linux`** output to find shares that allow write access (e.g., shares without a `$` indicating a hidden share, or those explicitly marked as writable). The goal is to find a location where files can be successfully uploaded for testing.
- Create a harmless file (e.g., a simple text file named `testfile.txt`) on your Kali VM that acts as a safe, testable file for confirming file transfer capabilities.
- Use the `smbclient` utility to connect to the identified writable share
- Use the `dir` or `ls` command at the `smb: \>` prompt to confirm that the `testfile.txt` was successfully copied to the target system's share.
- Type `quit` to exit the `smbclient` session.