# Website Cloning & Credential Harvesting

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

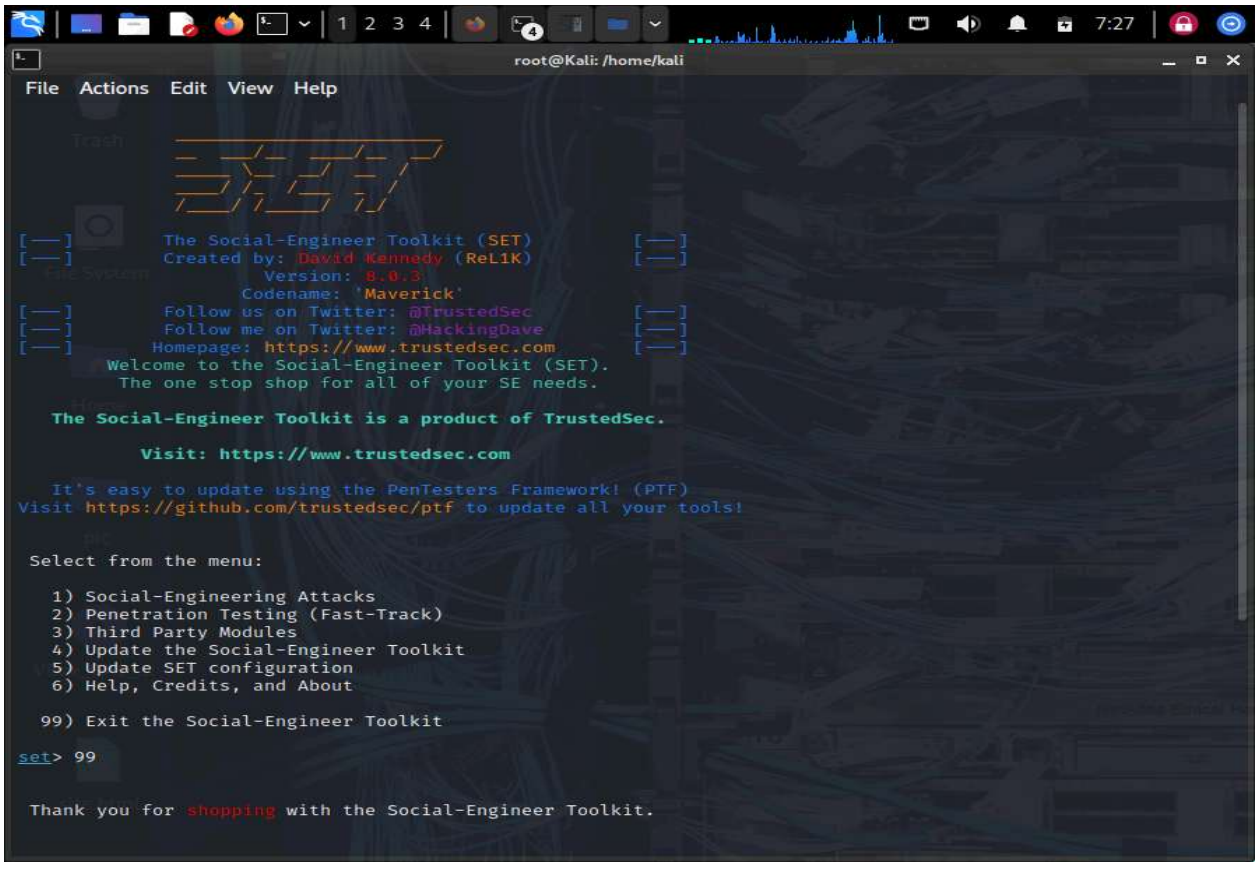
## 1. Prerequisites

- **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.

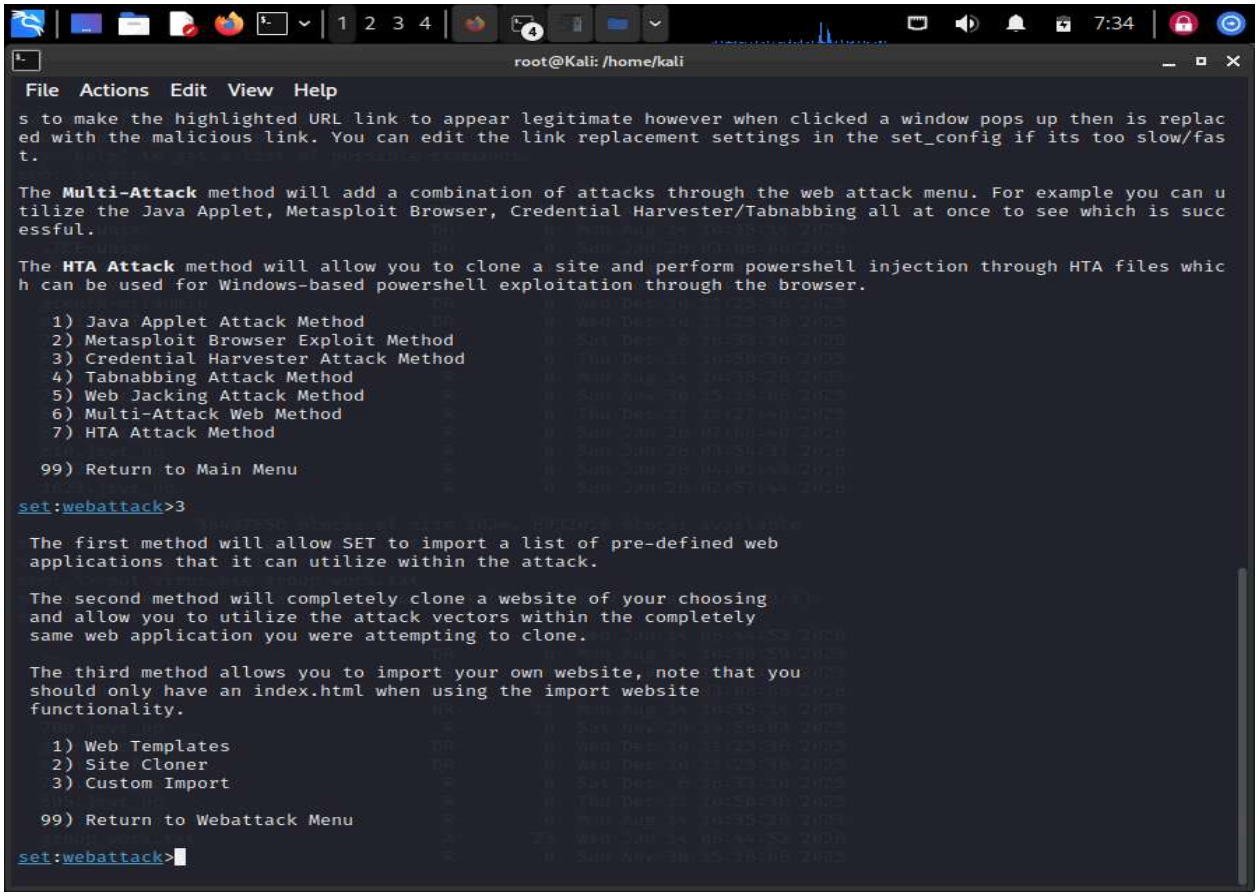
## 2. Launching the Social Engineering Toolkit (SET)

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**.




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

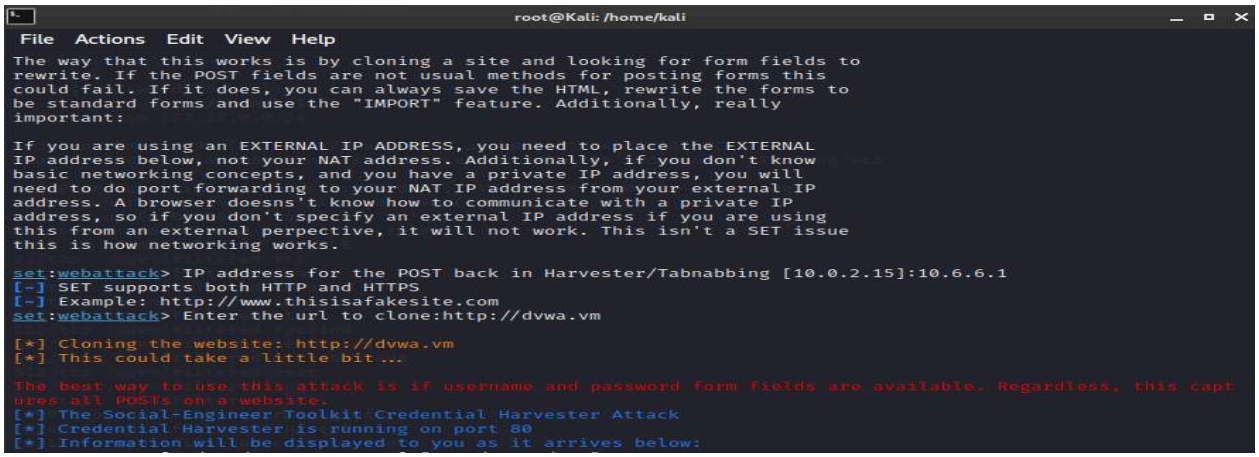



6. Select **2) Site Cloner**.

---

## 3. Configuring the Attack

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



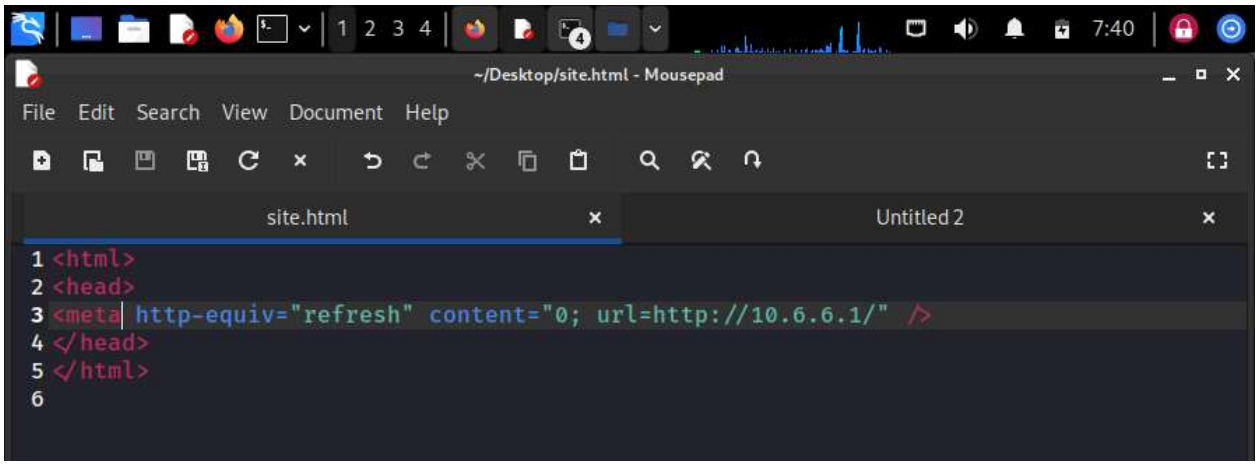
- **IP Address for POST back:** SET will ask where the harvested credentials should be sent. Enter your Attacker IP: `10.6.6.1`.
- **URL to Clone:** Enter the full URL of the target site: `http://dvwa.vm/login.php`.

**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.

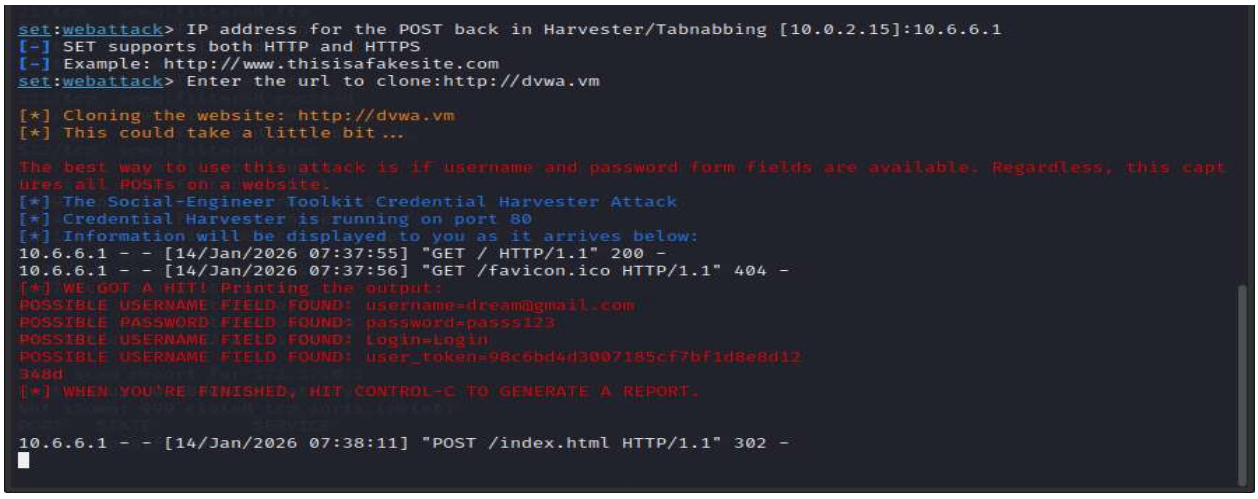
---

## 4. Capturing Credentials

Incorporating the Custom HTML File




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.



---

### 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

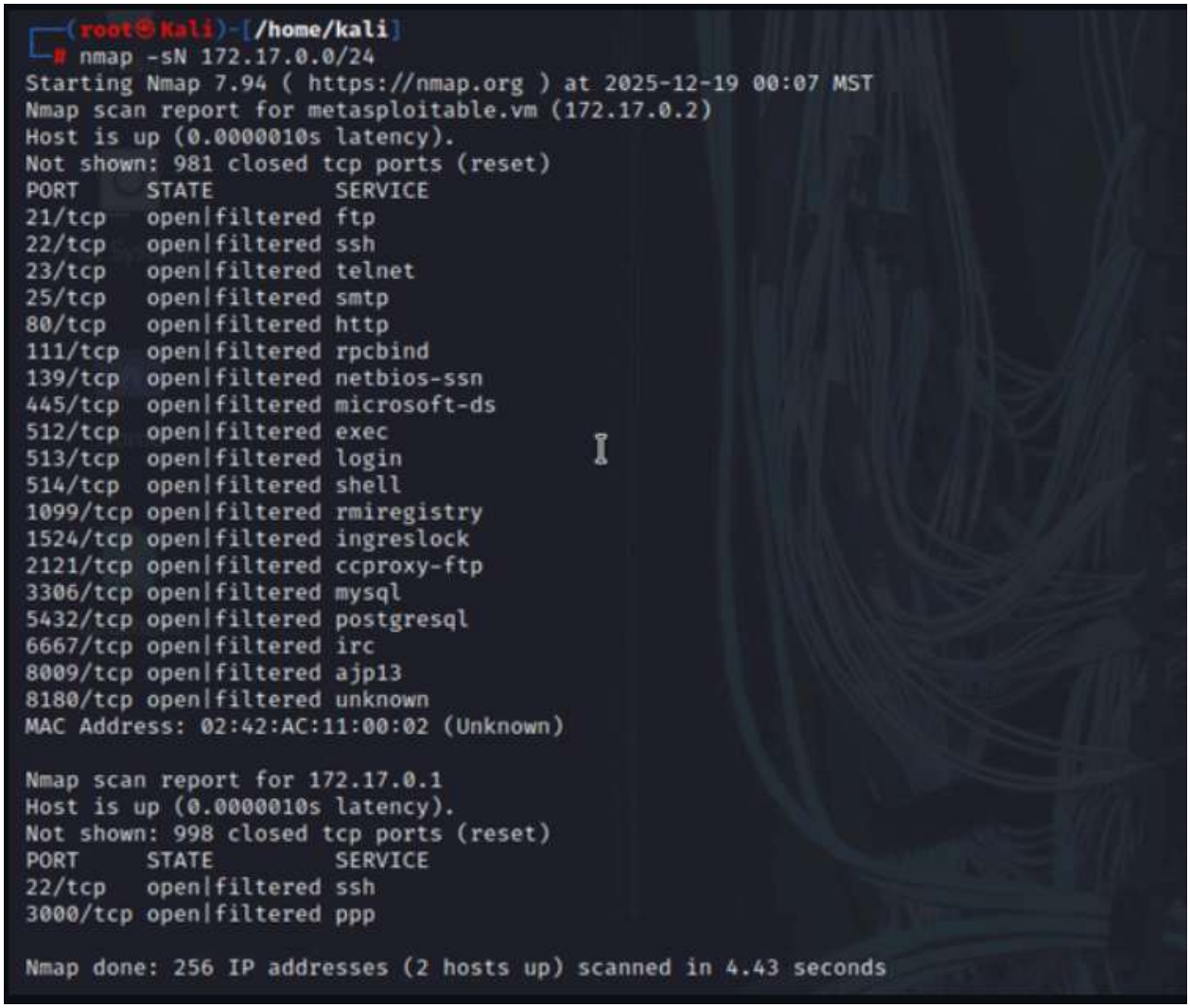
To perform targeted enumeration of SMB services to identify user accounts, machine information, shared folders, and password policies. Additionally, to demonstrate file transfer techniques using unauthorized share access.

### 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.



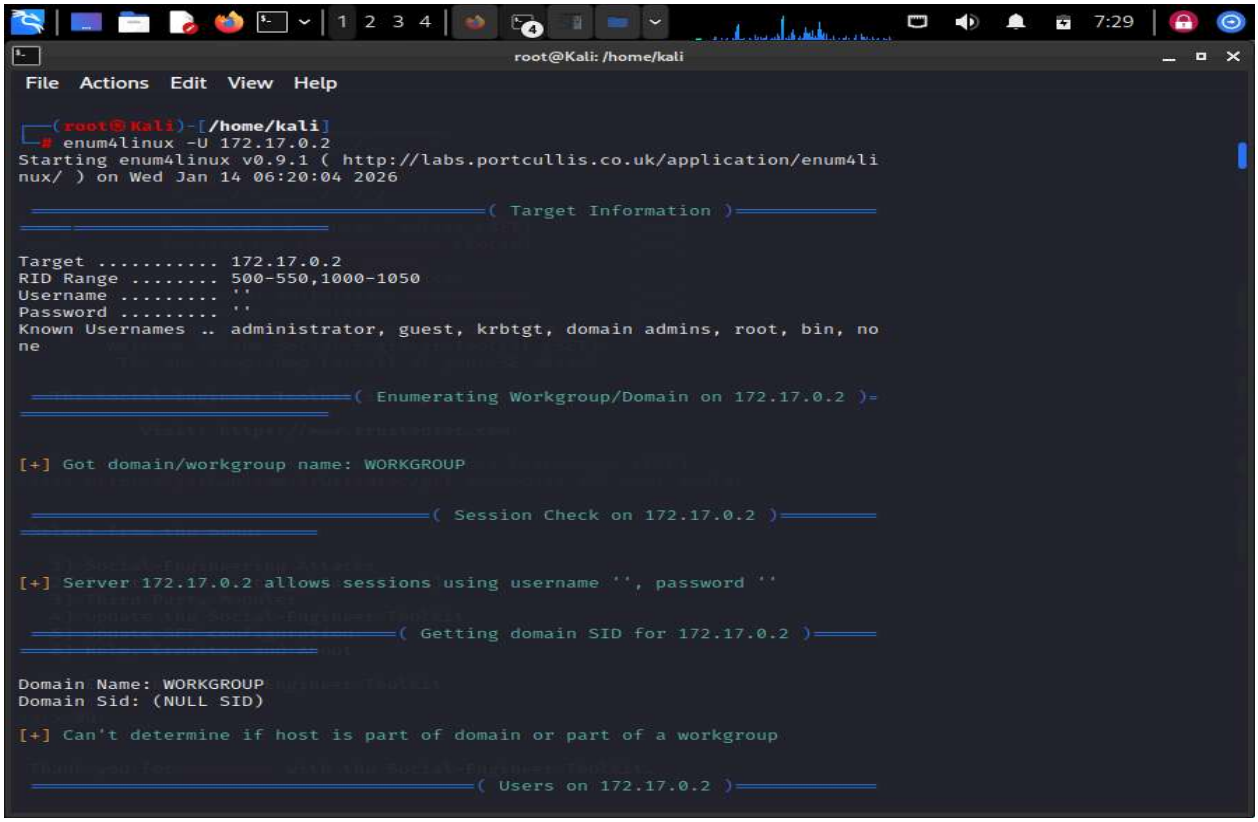

---

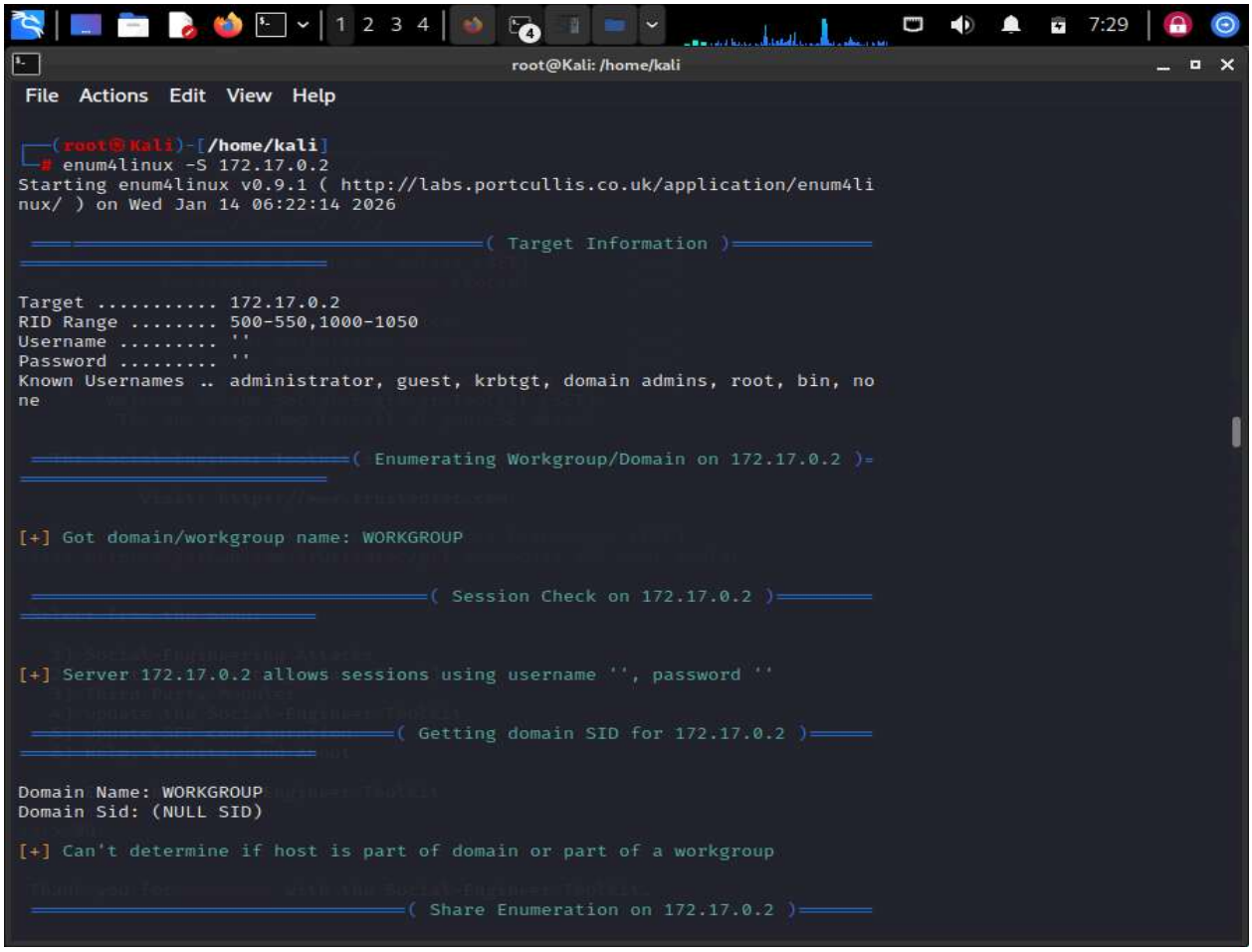
## 3. Phase 2: Targeted Enumeration (Enum4Linux)

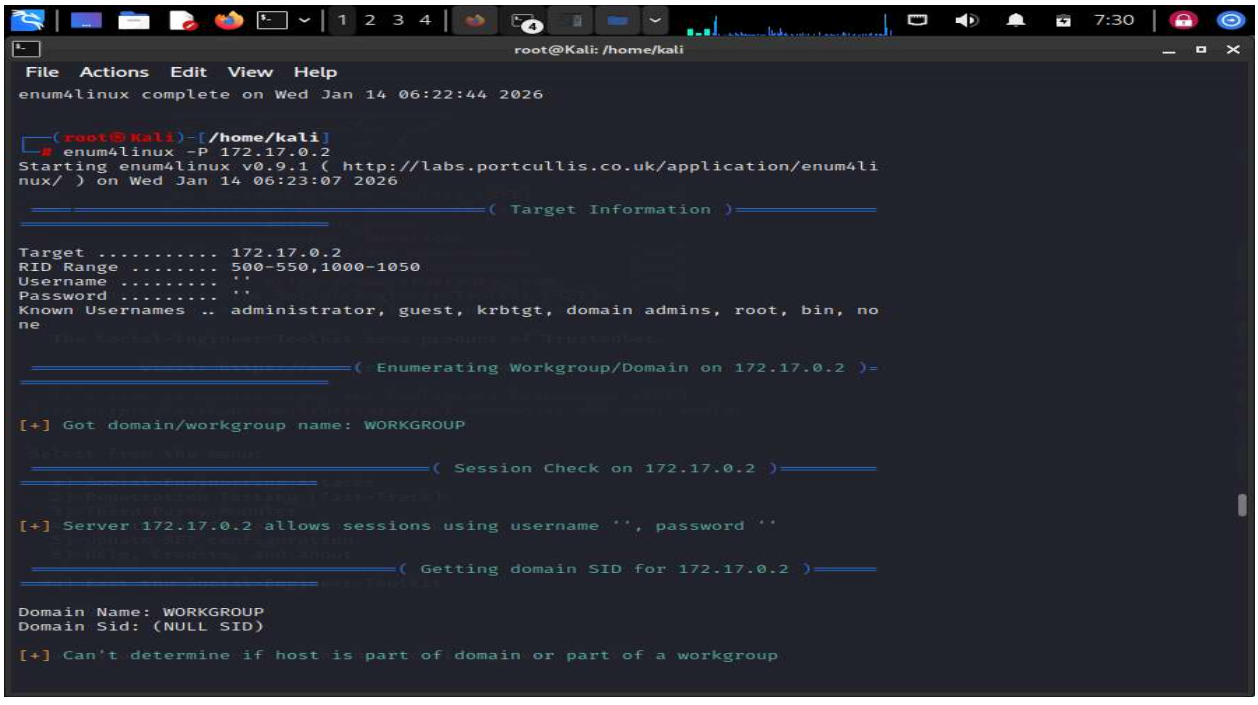
We use enum4linux with specific flags to extract granular data from the target.

| Command | Purpose | Expected Output |
|---|---|---|
| enum4linux -U 172.17.0.2 | **User Enumeration** | Lists local user accounts found via SAMR or local APIs. |

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




1 2 3 4
7:29
root@Kali: /home/kali
File Actions Edit View Help
┌──(root㉿Kali)-[/home/kali]
└─# enum4linux -S 172.17.0.2
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Jan 14 06:22:14 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
( Share Enumeration on 172.17.0.2 )


1 2 3 4
7:30
root@Kali: /home/kali
File Actions Edit View Help
enum4linux complete on Wed Jan 14 06:22:44 2026
┌──(root㉿Kali)-[/home/kali]
└─# enum4linux -P 172.17.0.2
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Jan 14 06:23:07 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

## 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.

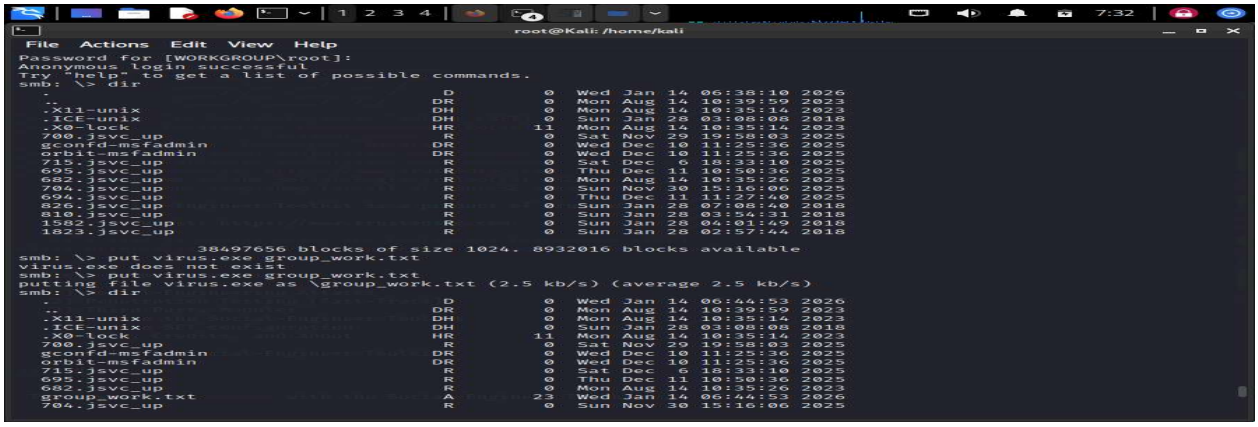
**Command 2:** smbclient //172.17.0.2/tmp

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

### C. File Transfer Techniques

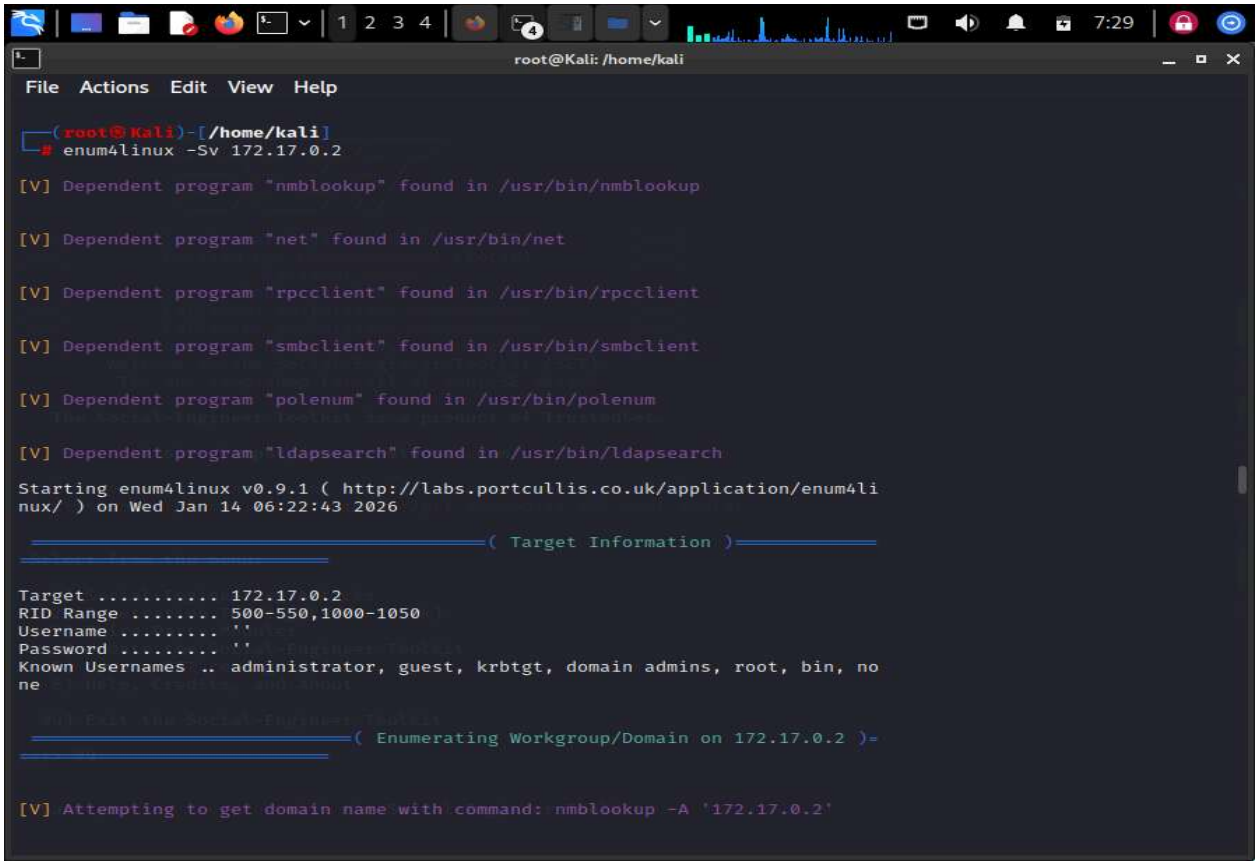
Once inside an SMB prompt (smb: \>), the following commands are used for data exfiltration or delivery:

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



## 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.




## 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.