Website Cloning and SMB Vulnerability Scanning

1. Website Cloning Lab

1.1 Objective

The objective of this lab was to reproduce the Website Cloning. The lab aimed to help learners understand how website cloning tools work, how attackers may replicate legitimate websites, and the importance of ethical considerations when performing such activities.

1.2 Tools Used

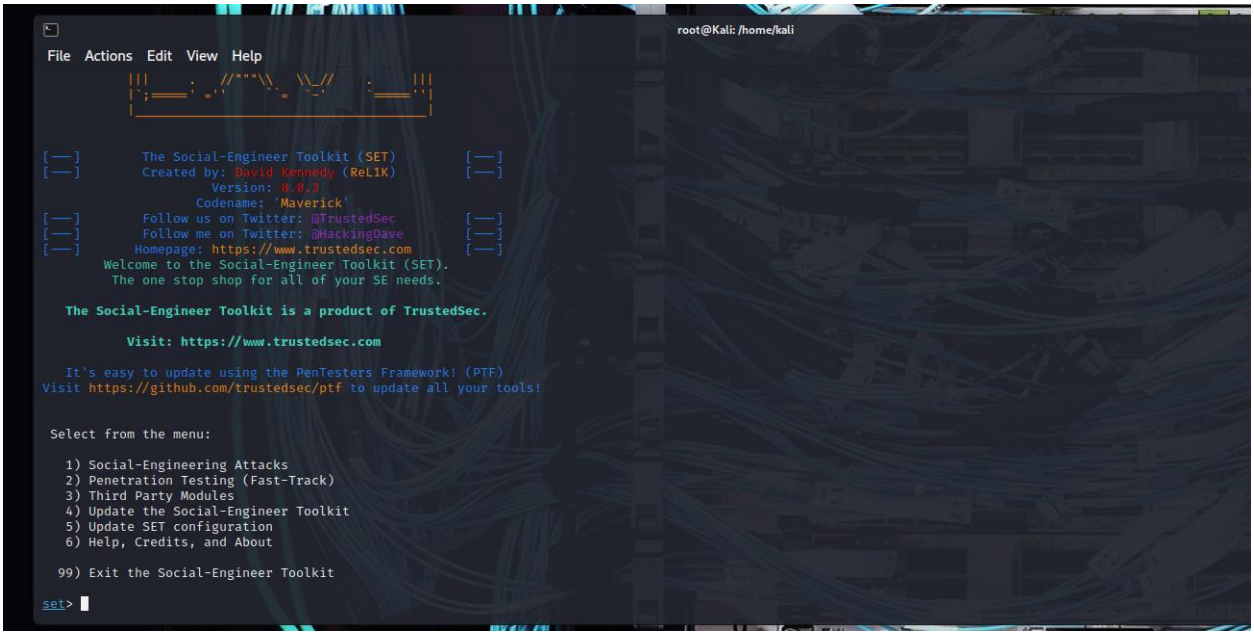
- Website cloning tool demonstrated during the session (SET)
- Web browser (for verification and testing)
- Kali Linux / Lab environment

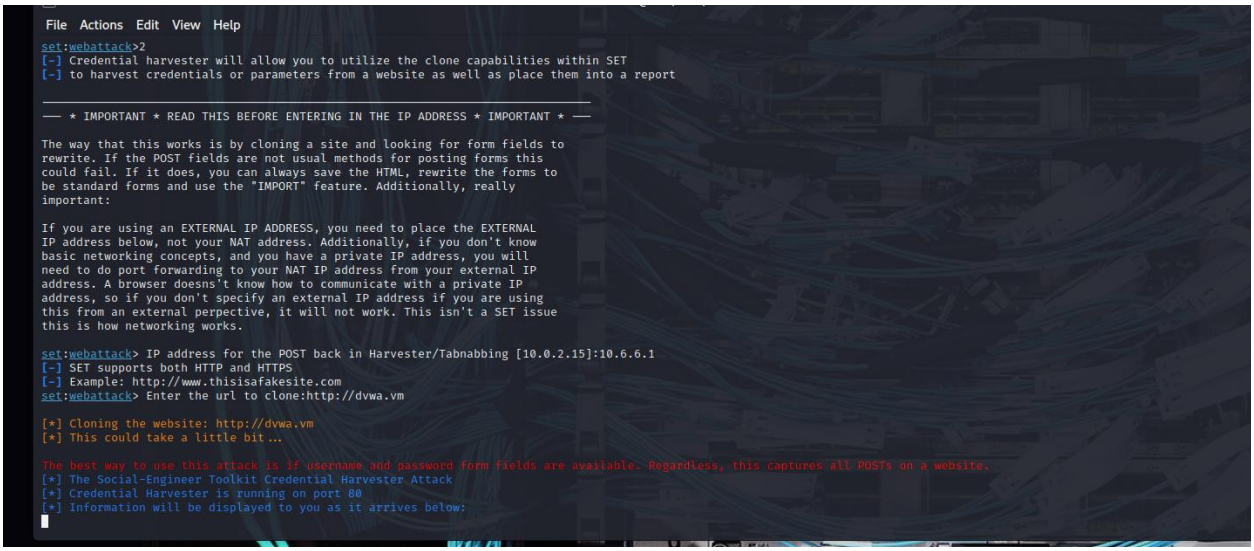
1.3 Target Description

The target website used in this lab was a publicly accessible website selected strictly for educational and testing purposes. No authentication-protected or sensitive systems were targeted.

1.4 Methodology / Steps Performed

1. Logged in as root user using the command sudo su.
2. Launched the Social-Engineer Toolkit by typing setoolkit.
3. Selected **Option 1** (Social-Engineering Attacks).
4. Selected **Option 2** (Website Attack Vectors).
5. Selected **Option 3** (Credential Harvester Attack Method).
6. Selected **Option 2** (Site Cloner).
7. Entered the attacker machine IP address: 10.6.6.1
8. Entered the target website URL: http://dvwa.vm.
9. The website was successfully cloned and hosted locally by SEToolkit.
10. Created a redirection HTML file to forward users to the cloned site.





1.5 Commands Used

sudo su

setoolkit

1.6 Redirection HTML File

A simple HTML file was created to redirect users automatically to the cloned website hosted by SEToolkit.

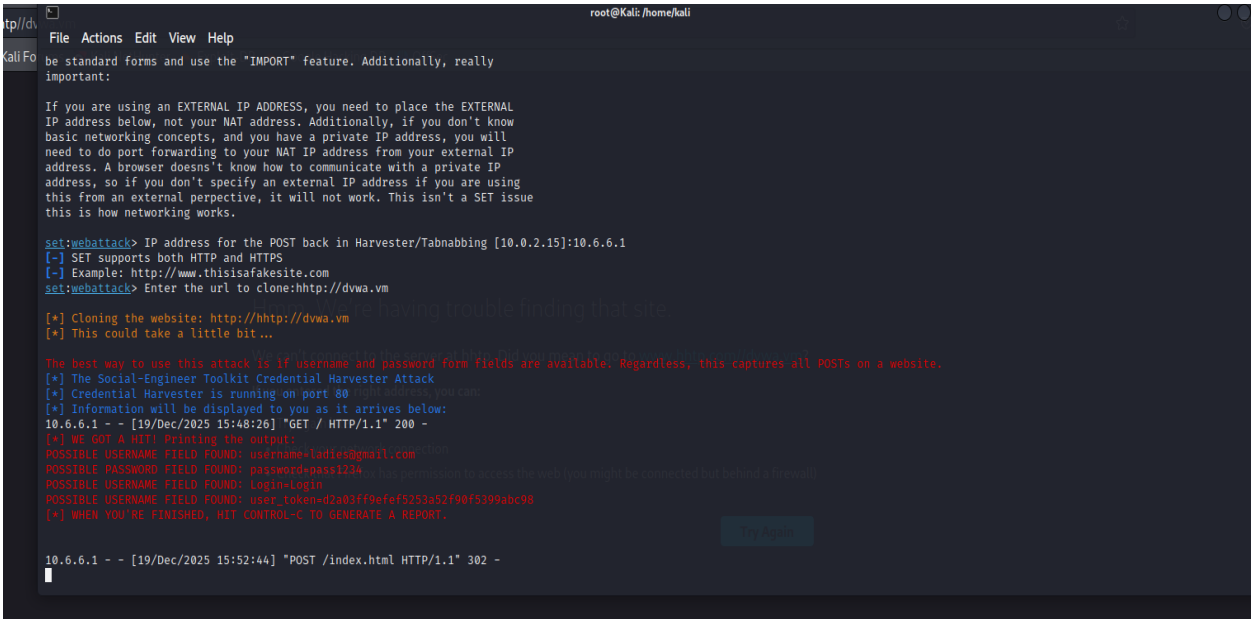
```
<html>
<head>
<meta http-equiv="refresh" content="0; url=http://10.6.6.1/" />
</head>
</html>
```

The file was saved as **ladies.html** on the Desktop. When the file was opened, it redirected the browser to the cloned DVWA login page.

Test credentials used:

- Email: ladies@gmail.com
- Password: 1234

1.7 Results and Observations



- The DVWA website was successfully cloned using SEToolkit.

- The redirection file worked as expected, forwarding users to the cloned site.
- Login credentials entered on the cloned page were captured by SEToolkit.

1.8 Ethical Considerations

This lab was conducted strictly for educational purposes within a controlled environment. Website cloning techniques should only be used for:

- Security awareness
- Penetration testing with proper authorization
- Learning how phishing and spoofing attacks operate

1.8 Conclusion

The lab provided practical insight into how website cloning tools operate and highlighted the importance of ethical usage. Understanding these techniques helps security professionals identify and mitigate phishing and spoofing attacks.

2. SMB Vulnerability Scanning Using Enum4Linux

2.1 Objective

The objective of this lab was to reproduce an SMB vulnerability scanning exercise using **Enum4Linux**. The goal was to identify exposed SMB information, misconfigurations, and insecure access controls on a target system by enumerating users, shares, groups, and SMB configuration details.

2.2 Tools Used

- **Enum4Linux**
- **Kali Linux**
- **smbclient**
- **Target machine with SMB service enabled** (Windows or Samba server)

2.3 Target Setup

- **Target IP Address:** 172.17.0.2
- **Operating System:** Linux (Samba Server)
- **SMB Service Status:** Enabled

2.4 Methodology / Steps Performed

1. **Network Connectivity Verification**
   Connectivity between the attacker (Kali Linux) and the target machine was confirmed using basic network checks.
2. **SMB Port Verification**
   SMB ports **139** and **445** were verified to be open, confirming that the SMB service was accessible.
3. **SMB Enumeration Using Enum4Linux**
   The following Enum4Linux commands were executed:
   - Enumerate SMB users:

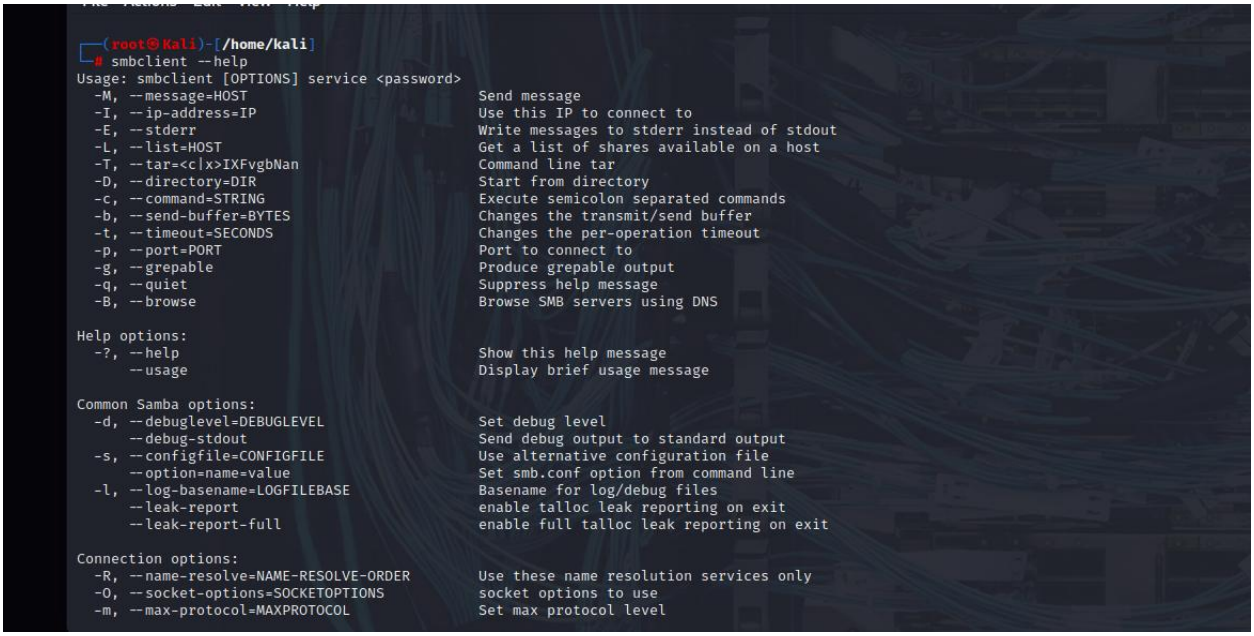
- enum4linux -U 172.17.0.2
- Enumerate OS and service version information:
- enum4linux -SV 172.17.0.2
- Enumerate password policy information:
- enum4linux -P 172.17.0.2
- Perform full SMB enumeration:
- enum4linux -a 172.17.0.2

4. **SMB Share Interaction Using smbclient**

   SMB client functionality was explored using the following commands:

   - Display smbclient help options:
   - smbclient --help
   - List available SMB shares:
   - smbclient -L 172.17.0.2
   - List SMB shares on the target using UNC path:
   - smbclient -L //172.17.0.2/
   - Connect to a specific SMB share and interact with it:
   - smbclient //172.17.0.2/share_name
   - Inside the SMB shell, the following commands were executed:
   - smb:> help

- smb:> dir
- smb:> put virus.exe
- smb:> put group-work.txt



2.6 Findings

The SMB enumeration revealed the following information:

- Available SMB shares on the target system
- Enumerated users and groups
- Operating system and workgroup information
- SMB password policy and configuration details

2.7 Security Implications

Improperly configured SMB services can lead to serious security risks, including:

- Information disclosure of users, groups, and system details
- Unauthorized access to shared resources
- Uploading malicious files to shared directories
- Lateral movement within the internal network

2.8 Conclusion

This lab demonstrated how **Enum4Linux** and **smbclient** can be used to gather sensitive information from SMB services. The results highlight the importance of properly securing SMB configurations by enforcing authentication, limiting anonymous access, and regularly monitoring SMB activity. Proper hardening and access control are critical to preventing SMB-based attacks.