

# Assignment - 10

Karthikeyan G  
Roll No: CB.SC.P2CYS24008

March 28, 2025

## 1 Exploring the SEToolkit for Social Engineering Attacks

- Social-Engineering Attack is selected.

The screenshot shows a terminal window titled 'root@kali: /home/karthikeyan'. The window displays the following text:

```
[—] 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!

Unable to check for new version of SET (is your network up?)

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> 0
```

- Website Attack Vectors are chosen.

```
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) Spear-Phishing Attack Vectors
- 2) Website Attack Vectors
- 3) Infectious Media Generator
- 4) Create a Payload and Listener
- 5) Mass Mailer Attack
- 6) Arduino-Based Attack Vector
- 7) Wireless Access Point Attack Vector
- 8) QRCode Generator Attack Vector
- 9) Powershell Attack Vectors
- 10) Third Party Modules
  
- 99) Return back to the main menu.

```
set> 2
```

- Credential Harvester Attack is attempted.

```
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
```

- Site Cloner option is selected.

```
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

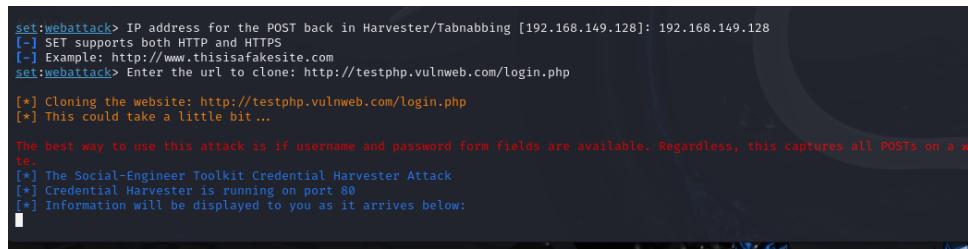
```
set:webattack>2
```

- IP address of the host system (for credential retrieval) is provided.

```
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 \[192.168.149.128\]: 192.168.149.128
```

- Target credential site is specified.



```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.149.128]: 192.168.149.128
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: http://testphp.vulnweb.com/login.php

[*] Cloning the website: http://testphp.vulnweb.com/login.php
[*] 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:
```

- After this step, an attempt was made to clone the website using the SET toolkit's Credential Harvester Attack. The URL was provided correctly, and the cloning process was initiated. However, despite multiple attempts, the cloned website did not function as expected. Various troubleshooting methods were applied, including:
  - Checking for conflicting services such as Apache or NGINX running on port 80 and stopping them using 'sudo systemctl stop apache2' or 'sudo systemctl stop nginx'.
  - Attempting to bind the Credential Harvester to an alternative port, such as 8080, by setting 'set PORT 8080' in SET toolkit.
  - Verifying network connectivity by checking firewall settings and temporarily disabling 'ufw' using 'sudo ufw disable'.
  - Ensuring that the cloned website was accessible by trying to open it from a browser on the attacker's machine as well as a remote victim machine.
  - Reinstalling SET toolkit and its dependencies using 'sudo apt update sudo apt install set' to rule out missing packages or corrupted installations.

Despite these efforts, the website cloning process failed, and the expected phishing page did not load correctly. The issue remains unresolved and may require further debugging or an alternative approach.