

Cyber Security Internship – Task 2 Report:

Task Title: Social Engineering & Phishing Simulation

Track Code: FUTURE_CS_02

Intern Name: Shreya V

Date: 15/06/2025

AIM:

- To simulate a phishing attack by cloning a legitimate Google Sign-In page using the Social Engineering Toolkit (SEToolkit) and testing how credential harvesting and redirection techniques work in a controlled lab environment. This helps understand the risks of phishing and the importance of user awareness in cyber defense.
-

TOOLS USED:

- Social Engineering Toolkit (SEToolkit)
 - Kali Linux
 - Apache Server (used internally by SET)
 - Browser (Chrome/Firefox)
 - Ngrok or local IP for testing on other devices
-

METHOD USED:

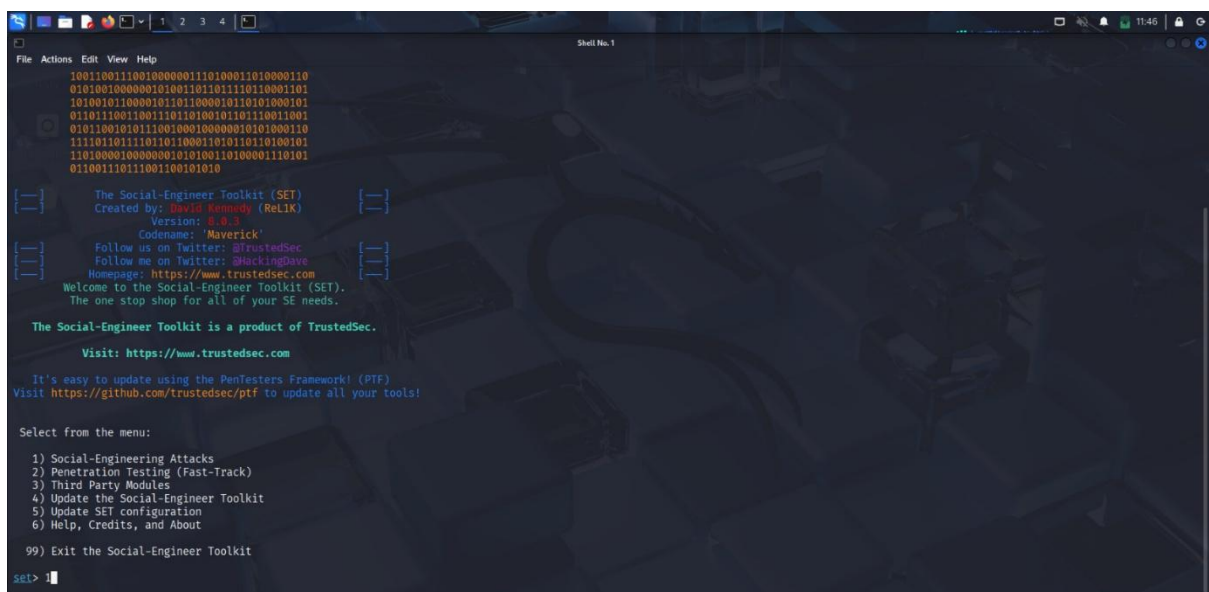
1. Launched the SEToolkit from Kali Linux.
2. Selected the following options:
 - ✓ Social-Engineering Attacks
 - ✓ Website Attack Vectors
 - ✓ Credential Harvester Attack Method
 - ✓ Web template
3. The toolkit cloned the original Google login page and hosted it locally.

4. When the test user entered credentials into the fake page, the information was captured and saved to a local file (harvester.txt).
4. After submission, the fake page redirected the user to the **real** Google login page to avoid raising suspicion.

OBSERVATIONS:

- ❖ The phishing page appeared visually identical to the real Google login screen.
 - ❖ Credentials were harvested and saved in cleartext.
 - ❖ Redirection back to the real site after login made the attack look seamless.
 - ❖ The attack would be convincing for non-technical users without training.
-

SCREENSHOTS TO ATTACH:

A screenshot of a terminal window titled 'Shell No. 1' showing the Social-Engineer Toolkit (SET) interface. The terminal displays a welcome message, version information (3.8.3), and a menu of options. The background of the terminal has a dark, abstract, geometric pattern. The menu options are: 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, and 99) Exit the Social-Engineer Toolkit. The prompt 'SET>' is visible at the bottom left.

```
File Actions Edit View Help
1001100111001000000110100011010000110
010100100000010100110110111010001101
101001011000001011011000010110101000101
011011001100110110100010110110011001
010110010111001000100000010101000110
111101101110110110001101010110100101
11010000100000001010100110100001110101
011001110111001100101010101010101010101

The Social-Engineer Toolkit (SET)
Created by: David Kennedy (Relik)
Version: 3.8.3
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> |
```

- Select the 1. Social-Engineering Attack

```
File Actions Edit View Help

The Social-Engineer Toolkit (SET)
Created by: Travis Heavens (ReL1K)
Version: 5.0.3
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) 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
```

➤ Select the Website Attack Vendors

```
File Actions Edit View Help

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

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a Metasploit-based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.

The Tabnabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements 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 it's 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>
```

➤ Select the Credential Harvester Attack Method

```
File Actions Edit View Help

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements 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 it's 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>
```

➤ Select the Web Templates

```
File Actions Edit View Help
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 "HTML" 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.

setwebattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:

**** Important Information ****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.
You can configure this option under:

/etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

1. Java Required
2. Google
3. Twitter

setwebattack> Select a template: █
```

➤ Select the Google

```
File Actions Edit View Help
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.

setwebattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:

**** Important Information ****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.
You can configure this option under:

/etc/setoolkit/set.config

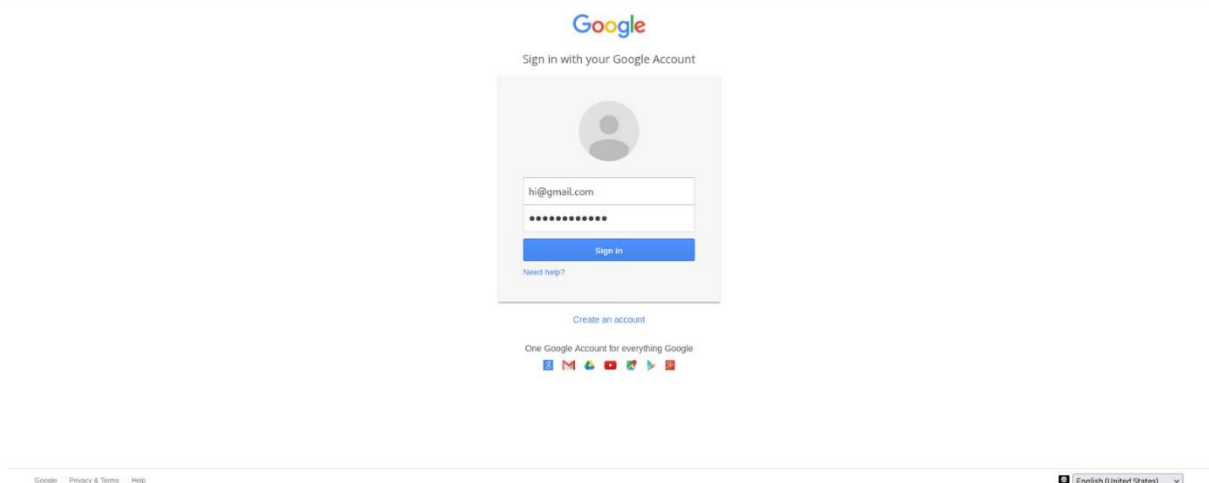
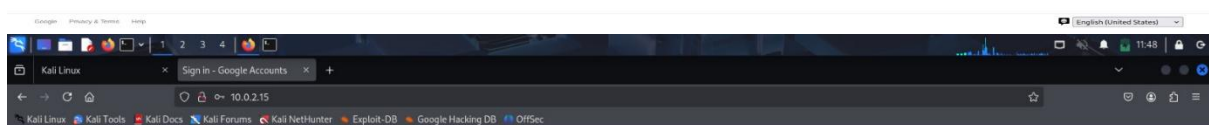
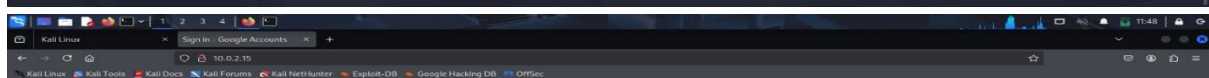
Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

1. Java Required
2. Google
3. Twitter

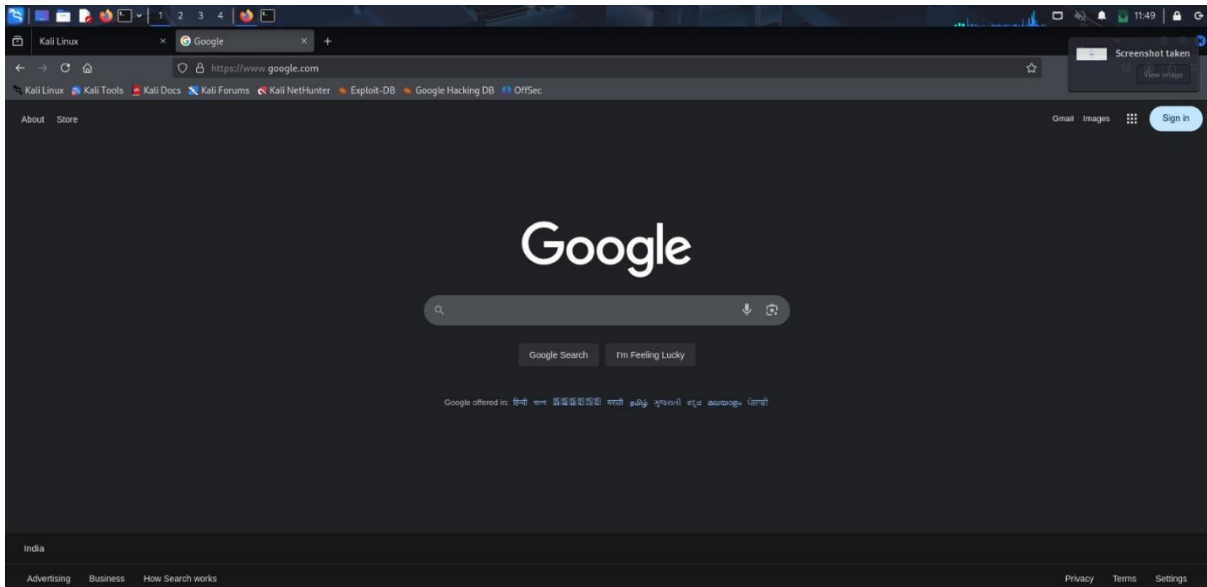
setwebattack> Select a template: 2

[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

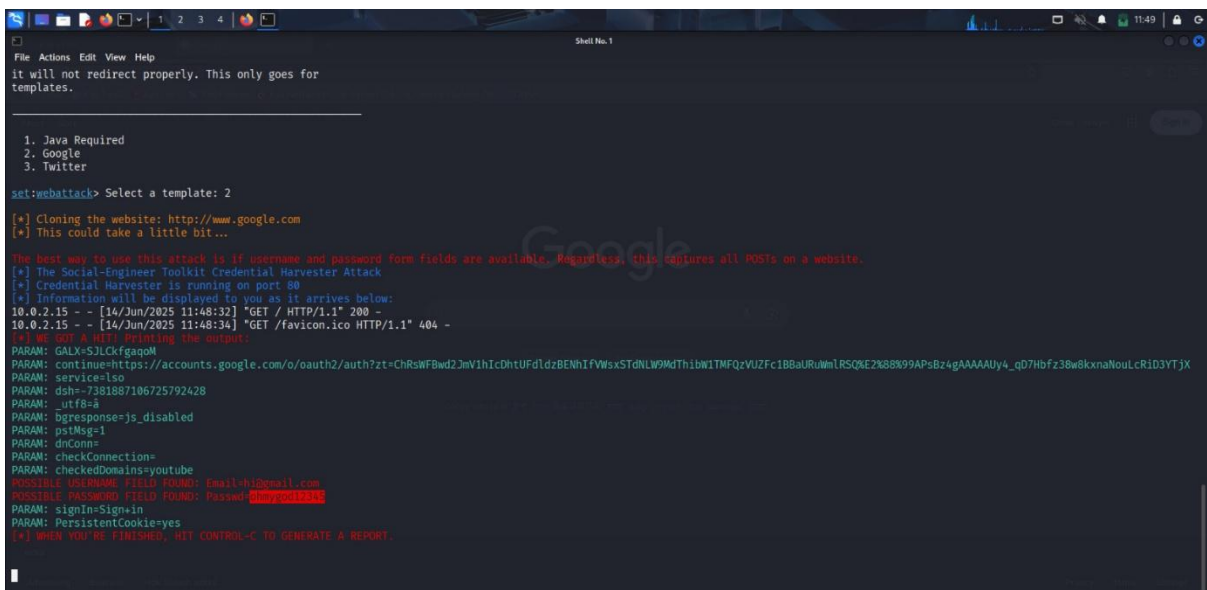
[+] Hosts set. The following is a common set provided from fields are available. Regardless, this captures all hosts on a website.
[+] The Social-Engineer Toolkit Credential Harvester Attack
[+] Credential Harvester is running on port 80
[+] Information will be displayed to you as it arrives below:
```



- After sign in they automatically redirect the normal google page



- In SEToolkit they capture username and password.



FINDINGS SUMMARY:

- ❖ The phishing setup was effective in capturing login credentials without alerting the user.
- ❖ Visual design and redirection increased believability.
- ❖ Credential harvesting was successful through cloned page.

- ❖ This test shows how easy it is to exploit trust in major brands for malicious purposes.
-

RECOMMENDATIONS:

- ❖ Users should always verify the URL before logging in.
 - ❖ Avoid clicking unknown or suspicious links, even if the page looks legitimate.
 - ❖ Enable multi-factor authentication (MFA) to reduce risk of credential misuse.
 - ❖ IT teams should use email and browser filters to detect phishing pages.
 - ❖ Organizations must conduct regular phishing awareness training.
-

LEARNING OUTCOME:

- ❖ This task gave me hands-on experience with phishing simulation using SEToolkit. I learned how phishing pages are created, how credentials are harvested, and how redirection adds to the realism of an attack. This exercise improved my understanding of social engineering tactics and highlighted the need for both technical controls and end-user education in defending against phishing threats.
-