SOCIAL ENGINEERING AND PHISHING SIMULATION REPORT

Objective: To simulate a phishing attack by creating a fake Google login page for educational purposes.

Tools Used

- **Operating System**: Kali Linux
- **Primary Tool**: SEToolkit (Social-Engineer Toolkit)
- **Text Editor**: Notepad or any basic HTML editor

Step-by-Step Procedure

1. Installing SEToolkit on Kali Linux

First, ensure SEToolkit is installed on Kali Linux:

sudo apt update && sudo apt install setoolkit -y

2. Launching SEToolkit

Run the toolkit with root privileges:

sudo setoolkit

3. Selecting Social Engineering Attacks

Inside SEToolkit:

- **Press** 2 → *Website Attack Vectors*

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ [redacted]
        /oooo  oooo  oooo  oooo /!
       /ooooooooooooooooooooooo/ /
      /ooooooooooooooooooooooo/ /
     /C=_____________________/_/

[──]        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) 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
```

- **Press** 3 → *Credential Harvester Attack Method*

```
kali@kali: ~
File  Actions  Edit  View  Help
set> 2

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

The Java Applet Attack method will spoof a Java Certificate and deliver a Metasploit-based payload. Uses a c
ustomized 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 fie
ld 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 di
fferent.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacement
s to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replac
ed with the malicious link. You can edit the link replacement settings in the set_config if it's too slow/fa
st.

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 suc
cessful.

The HTA Attack method will allow you to clone a site and perform PowerShell injection through HTA files whic
h 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
```

4. Using a Custom Web Template

- Select 1 → *Web Templates*
- Choose a template (e.g., Google Login if available) or use a custom HTML file.

```
kali@kali: ~
File  Actions  Edit  View  Help
ed with the malicious link. You can edit the link replacement settings in the set_config if it's too slow/fa
st.

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 suc
cessful.

The HTA Attack method will allow you to clone a site and perform PowerShell injection through HTA files whic
h 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>1
```

5. Entering Local IP for Phishing Server

- The tool asks: "Enter the IP address for the POST back in Harvester/Tabnabbing"
- Enter your Kali Linux local IP (Find it using ifconfig or ip a).

```
kali@kali: ~
File  Actions  Edit  View  Help

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>1
[-] 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 [[redacted]]: [redacted]
```

6. Selecting the Google Login Template

- Press 2 → *Google* (pre-built phishing template)
- SEToolkit will now host a fake Google login page on your local IP.

```
kali@kali: ~
File  Actions  Edit  View  Help
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 [[redacted]]: [redacted]

 ********************************************************

             **** 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

set:webattack> Select a template: 2
```

7. Creating a Custom Template (Optional)

If using a custom HTML page instead of cloning:

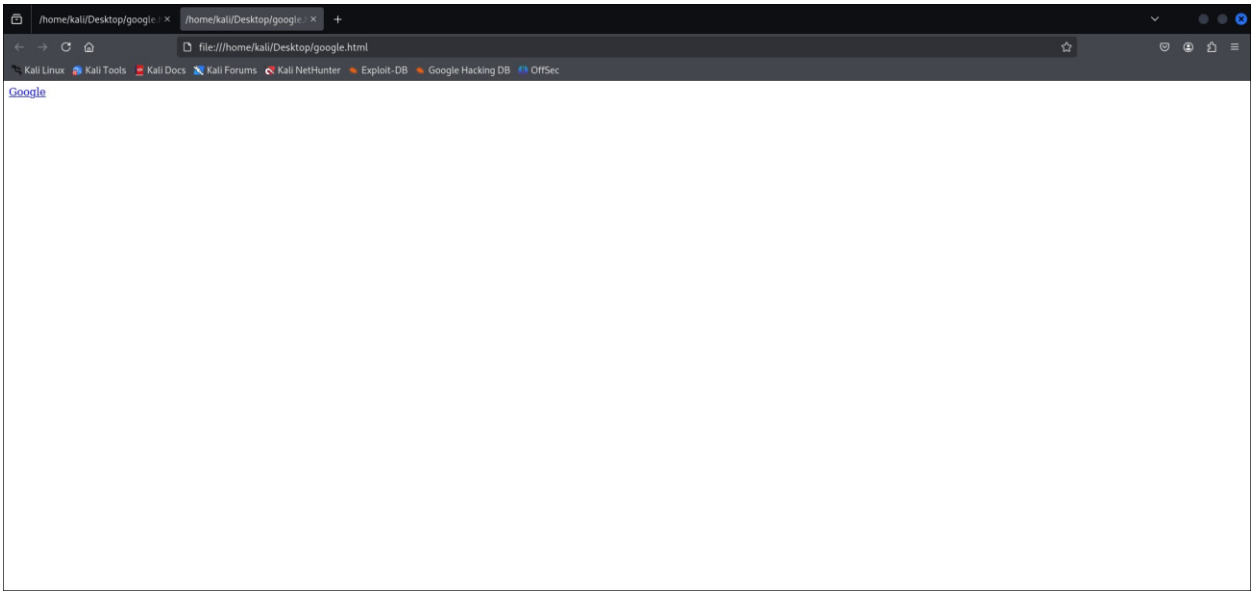
- Save the following code as index.html:

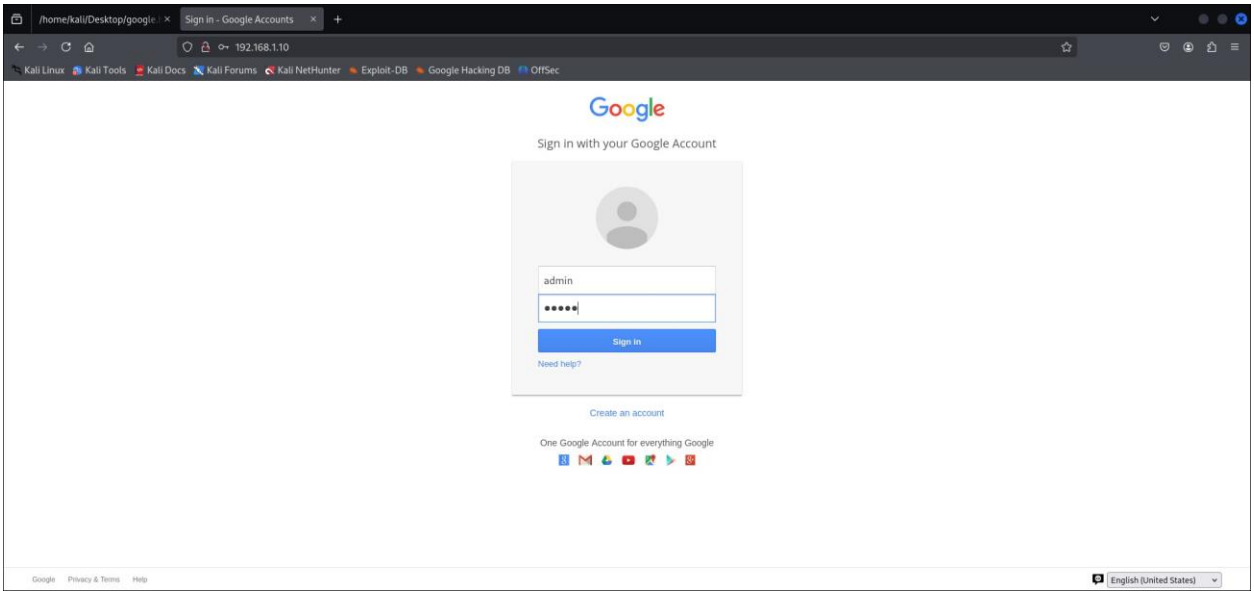
```
<html>
<body>
<a href="http://<ATTACKER_IP>">Click here to login to Google</a>
</body>
</html>
```

- Host this file on a web server (e.g., Apache).

8. Deploying the Phishing Page

- The cloned Google login page will be hosted on the attacker’s machine.
- The victim accesses the page via http://<ATTACKER_IP>.

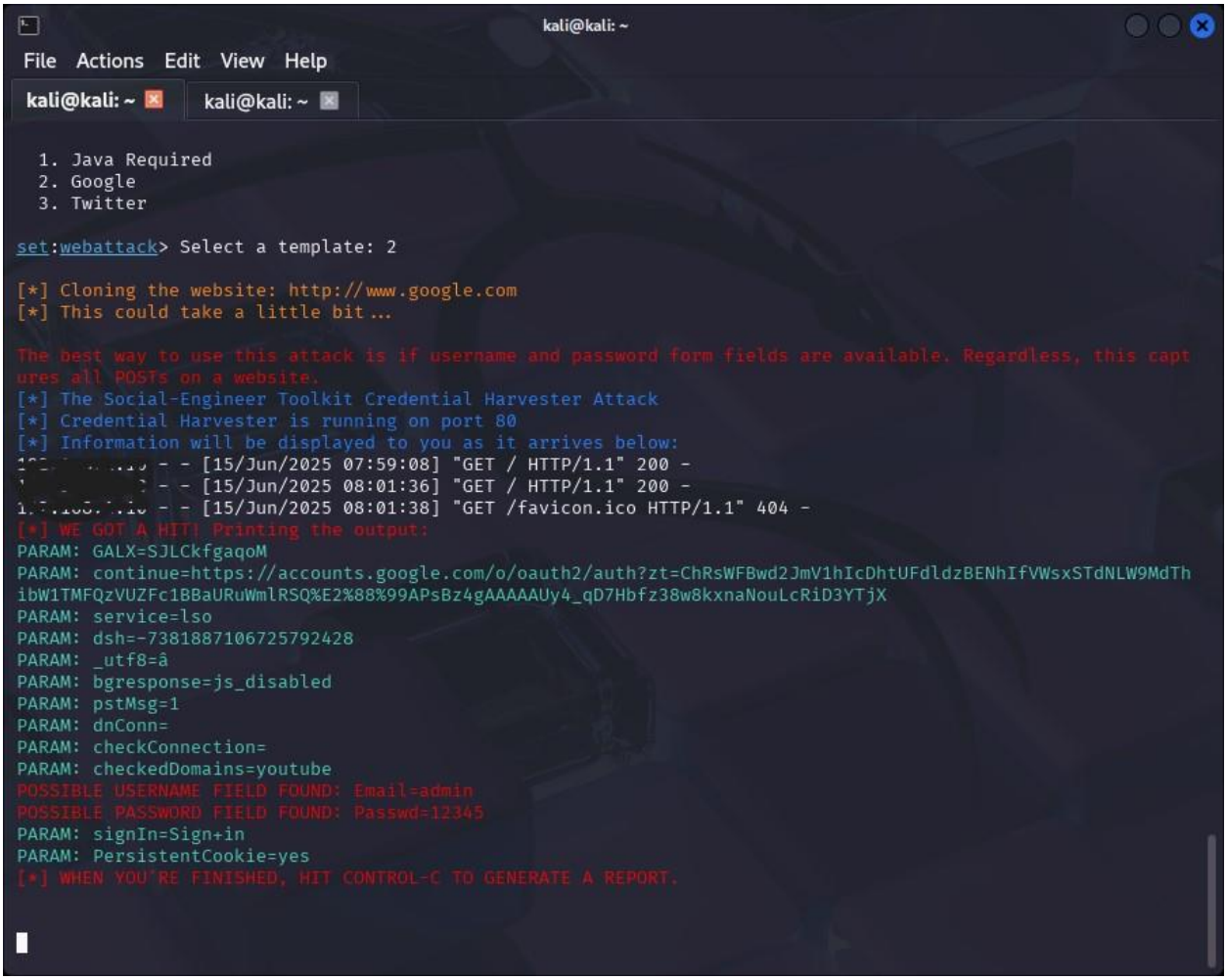




9. Capturing Credentials

- When the victim enters their credentials, SEToolkit logs them in real-time.

- Check SEToolkit's console to see harvested usernames and passwords.



Observations & Results

- Successfully cloned the Google login page.
- Credentials entered by the victim were captured in SEToolkit.
- Demonstrated how easily phishing can trick users into submitting sensitive data.

Ethical Considerations & Legal Disclaimer

- This simulation was conducted strictly for educational purposes.
- Phishing attacks without explicit permission are illegal and punishable by law.
- Always obtain proper authorization before performing security testing.

Mitigation & Prevention

- To protect against phishing: **Verify URLs** before entering credentials.
- **Enable Multi-Factor Authentication (MFA)** on accounts.
- **Educate users** on identifying phishing attempts.
- **Use email filters** to block suspicious links.

Conclusion

This exercise demonstrated how attackers exploit human trust through phishing. Awareness and proper security measures are crucial in preventing such attacks.