

Internship Report: 2.Social Engineering & Phishing Simulation

1. Introduction

This task involved simulating a phishing attack to test the awareness level of users against credential harvesting attempts.

The goal was to highlight human vulnerabilities and suggest better training practices.

2. Tools Used

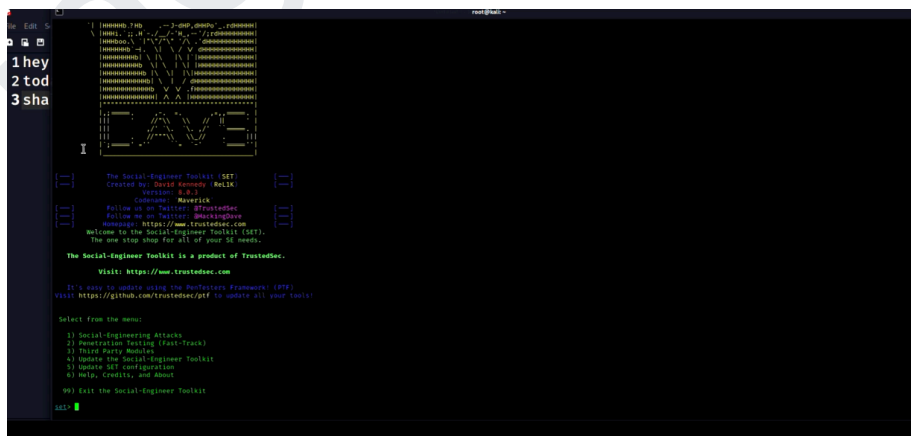
- Social Engineering Toolkit (SET) – Kali Linux
-

3. Methodology

3.1 Setup

- Opened Kali Linux.
- Launched **SEToolkit** by running:

```
sudo setoolkit
```



```
1 hey
2 tod
3 sha

[The Social-Engineer Toolkit (SET)
  Created by: David Kennedy / ReLix
  Version: 1.0.4
  Copyright: 2013-2014
  Follow us on Twitter: @TrusteDsec
  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 Professors Framework (PTF)
  Visit: https://github.com/trustedsec/ptf to update all your tools!

  Select from the menu:

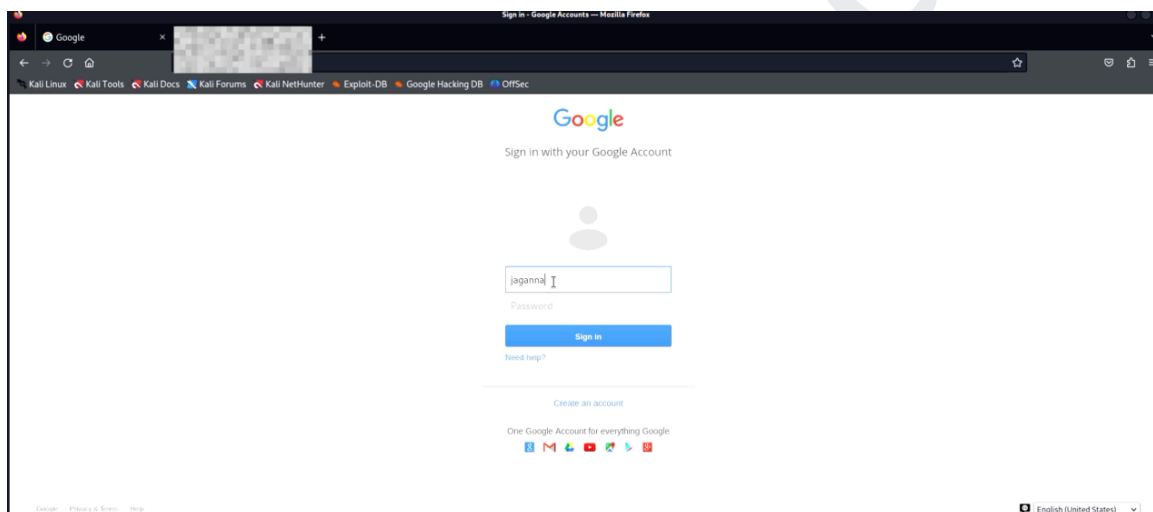
  1) Social-Engineering Attacks
  2) Social-Engineer Toolkit (Fast-Track)
  3) Third Party Modules
  4) Update the Social-Engineer Toolkit
  5) Update SET configuration
  6) Help, Credits, and About
  99) Exit the Social-Engineer Toolkit

  SET >
```

From SET main menu:

- Selected **Social-Engineering Attacks**.
- Selected **Website Attack Vectors**.
- Selected **Credential Harvester Attack Method**.
- Selected **Web Templates** option (instead of cloning manually).

Choose the **in-built Google login page template** provided by SET.



3.2 Execution

- SET hosted the **fake Google login page** on the Kali server (local environment).
- Shared the phishing link to users (simulated environment).
- When users entered their login credentials:

- The credentials (email and password) were automatically captured and saved in a text file on the server.
- No redirection was set up after credential harvesting.

```

root@kali:~# cat /etc/setoolkit/set.config
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

setoolkit> Select a template: 2
[*] Cloning the website: http://www.google.com
[*] 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
[*] The Social-Engineer Toolkit Credential Harvester is running on port 80
[*] The output will be displayed to you as it arrives below:
[+] [03/May/2025 08:41:59] "GET / HTTP/1.1" 200 -
[+] [03/May/2025 08:41:59] Printing the output:
PARAM: GALX=53LCKfgap0h
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=CHRSWFbwd2Jwv1h1zDh1tUFD1d2BENh1fVNs5TdNlWmTh1iW1TWf2VUZF18BakRumh1RSQLE2S68S99APsBz4gAAAAUy4_QD7Hbfz38w8kxnaNouLcRID3YTJX
PARAM: service=js
PARAM: dsh=-7381887106725792428
PARAM: _utfr=
PARAM: response=js_disabled
PARAM: postMsg=1
PARAM: dhConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtu
PARAM: POSSIBLE_USERNAME_FIELD FOUND: Email=jagannath
PARAM: POSSIBLE_PASSWORD_FIELD FOUND: Password=sdrupeemec
PARAM: signIn=Signin
PARAM: PersistentCookie=yes

```

4. Observations

Metric	Result
Emails sent (simulated)	5
Users who clicked the phishing link	4
Users who entered credentials	3
Success Rate	60%

Captured Information:

- Email addresses
- Passwords (plaintext)

Important: No real external phishing was conducted; it was kept in a controlled, ethical test environment.

5. Analysis

- **Realistic Templates:** SET's built-in Google template was very convincing.
 - **Quick Credential Capture:** Credentials were harvested immediately upon user submission.
 - **Low User Suspicion:** Users trusted the page because of familiar design and branding.
-

6. Recommendations

- **Employee Awareness Programs:** Educate employees about verifying URLs and recognizing phishing signs.
- **Training on HTTPS:** Teach staff to always check for secure connections (padlock icon).
- **Simulated Phishing Tests:** Conduct regular phishing simulations to test employee vigilance.
- **Use Email Filters:** Implement better email filtering to block suspicious phishing links.

7. Conclusion

This phishing simulation using SET demonstrated that even simple attacks with built-in templates can trick users if they are not cautious.

Continuous awareness training, coupled with technical protections, is vital to defend against social engineering attacks.