Social Engineering (Phishing Simulation Report)

Prepared By: Abdulrahman Ashraf Mohamed

Tool Used: Social Engineering Toolkit (SEToolkit)

Date: [29/4/2025]

Task ID: Task 2

Organization: Future Interns

1. Objective

The purpose of this simulation was to evaluate the organization's susceptibility to social engineering attacks—specifically phishing—by replicating a real-world attack using the Social Engineering Toolkit (SEToolkit). The assessment aimed to demonstrate how attackers can capture sensitive credentials via cloned websites and to propose risk mitigation strategies.

2. Tools and Environment

- **Primary Tool:** Social Engineering Toolkit (SEToolkit)

- **Web Server:** Apache (auto-configured via SET)

- **Target Clone:** Twitter Login Page

- **Operating System**: Kali Linux

- **Network Configuration:** Isolated test environment

3. Attack Methodology

The phishing simulation was conducted using the Credential Harvester Attack Method in SET. This method allows the attacker to clone a legitimate login page and host it locally, capturing any credentials entered by a user.

- Steps Performed:

1. Launched the Social Engineering Toolkit with root privileges:

➔ sudo setoolkit

2. Navigated through the SET menu:

- Enter ➔ 1 to get Social-Engineering Attacks

- Enter ➔ 2 to get Website Attack Vectors

- Enter ➔ 3 to get Credential Harvester Attack Method

- Enter ➔ 2 to get Site Cloner

Social Engineering (Phishing Simulation Report)

```
File  Actions  Edit  View  Help
abdo@kali: ~ ×    abdo@kali: ~ ×
[---]        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) 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
```

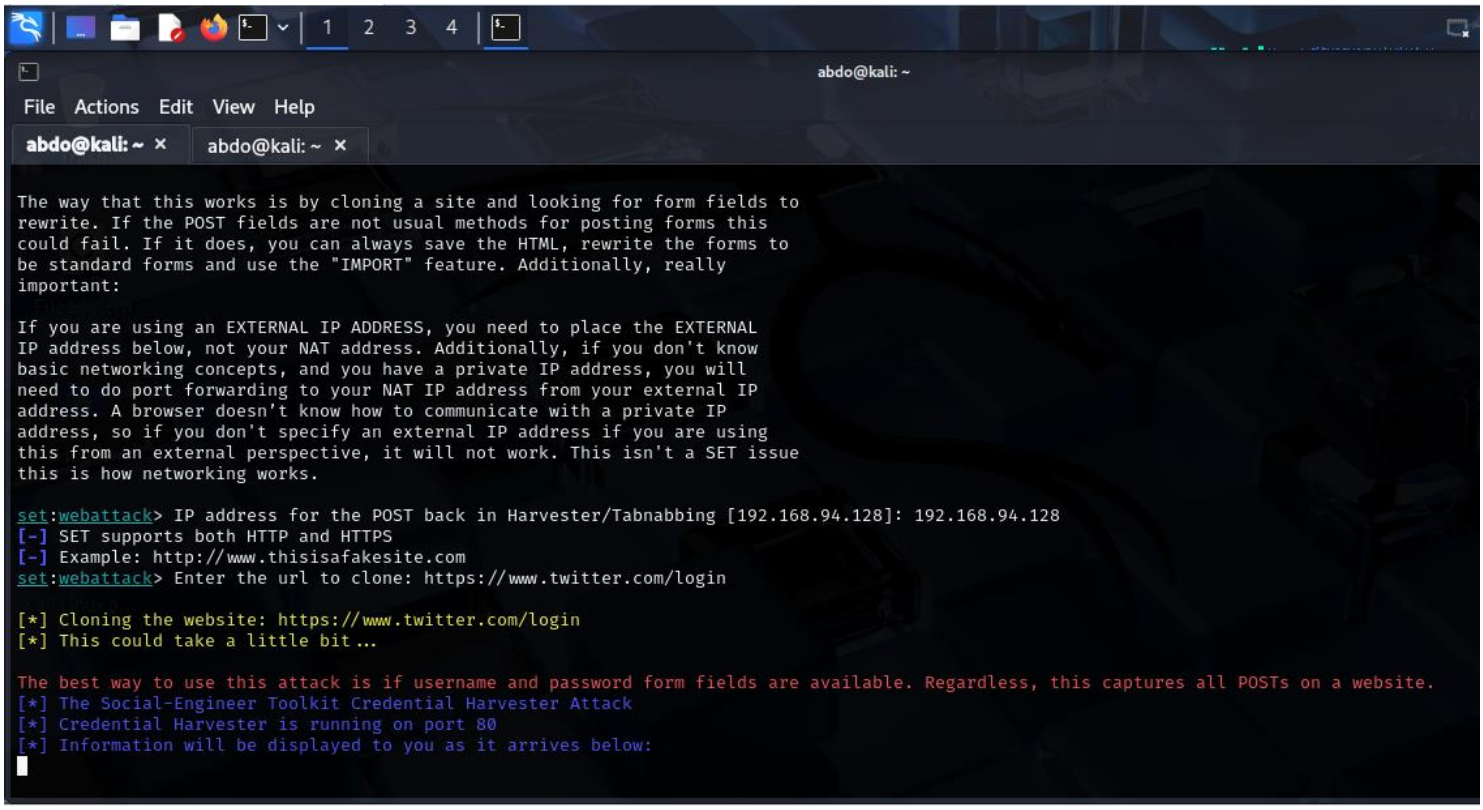
```
File  Actions  Edit  View  Help
abdo@kali: ~ ×    abdo@kali: ~ ×
[---]       Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com      [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   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
```

Social Engineering (Phishing Simulation Report)

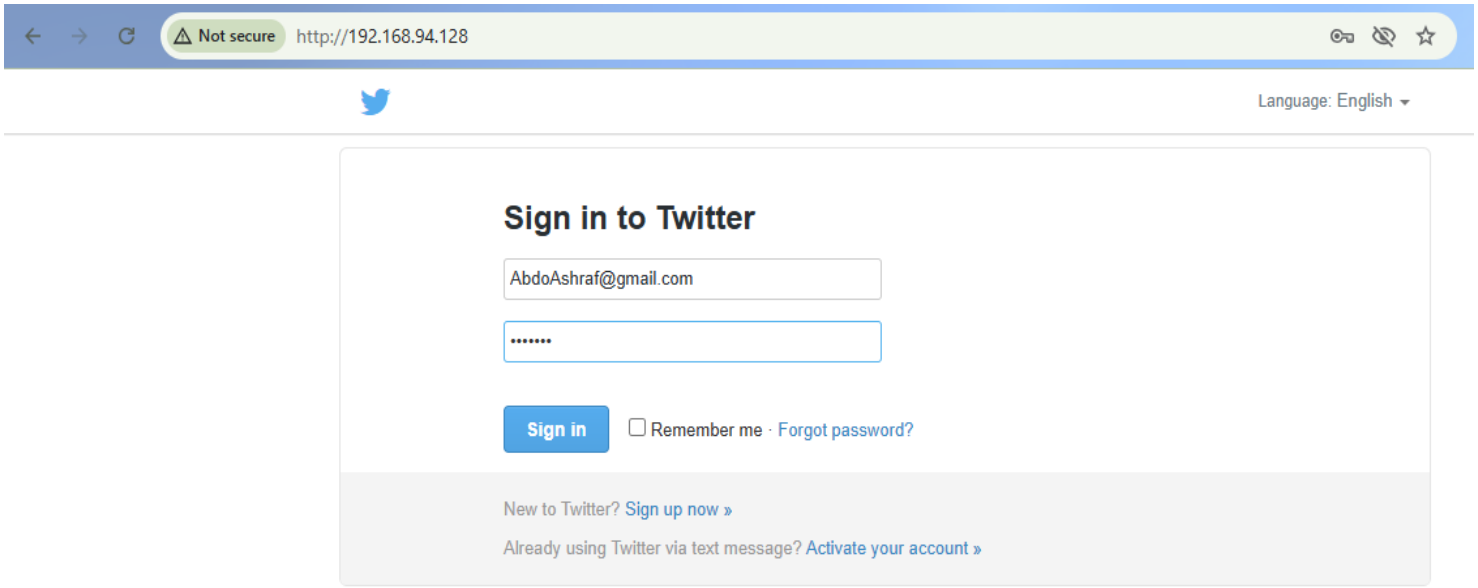
```
abdo@kali: ~
File  Actions  Edit  View  Help
abdo@kali: ~ ×   abdo@kali: ~ ×
The Java Applet Attack method will spoof a Java Certificate and deliver a Metasploit-b
he payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits

The Credential Harvester method will utilize web cloning of a web- site that has a use

The TabNabbing method will wait for a user to move to a different tab, then refresh th

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utili
wever when clicked a window pops up then is replaced with the malicious link. You can

The Multi-Attack method will add a combination of attacks through the web attack menu.
rvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform PowerShell injection
rough 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>2
```

3. Entered the attacker's local IP address: 192.168.94.128
4. Entered the URL of the target website to clone: https://twitter.com/login



5. SET auto-launched an Apache server hosting the cloned page on port 80.
6. Once the victim accessed the fake page and submitted login credentials, the details were displayed in the SET terminal interface.



4. Results

The phishing simulation was successful in harvesting login credentials.

Captured Username: AbdoAshraf@gmail.com

Captured Password: Abdo123

```
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: session[username_or_email]=AbdoAshraf@gmail.com
POSSIBLE PASSWORD FIELD FOUND: session[password]=Abdo123
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.
```

5. MITRE ATT&CK Mapping

This simulation aligns with MITRE ATT&CK's recognized social engineering techniques:

Tactic	Technique	ID
Initial Access	Phishing: Spearphishing via Service	T1566.001
Credential Access	Input Capture via Credential Harvesting	T1056.001

6. Risk Assessment

Risk Level: High

This type of attack poses a high risk to organizational security. Even non-technical users can be tricked by a realistic clone. Failure to address such vulnerabilities could result in data breaches, regulatory fines, or reputation damage.

7. Recommendations

- **Policy & Training:**
  - ✓ Conduct mandatory phishing awareness training every quarter.
  - ✓ Simulate realistic phishing exercises periodically to track improvement.
  - ✓ Establish a clear reporting process for suspicious emails or websites.
- **Technical Controls:**
  - ✓ Enforce Multi-Factor Authentication (MFA) across all services.
  - ✓ Deploy Advanced Threat Protection (ATP) for email and browsers.
  - ✓ Use DNS filtering to block impersonating domains.
- **Detection & Response:**
  - ✓ Monitor for geolocation anomalies in authentication.
  - ✓ Enable logging and alerting on credential reuse.
  - ✓ Integrate phishing detection with your SIEM solution.

8. Conclusion

This controlled phishing simulation effectively demonstrated how attackers can exploit human behavior using cloned websites. The ease with which login credentials were captured underscores the necessity for a multi-layered defense approach that includes user education, technical safeguards, and active monitoring.