Phishing Attack Simulation using Social Engineering Toolkit

Introduction

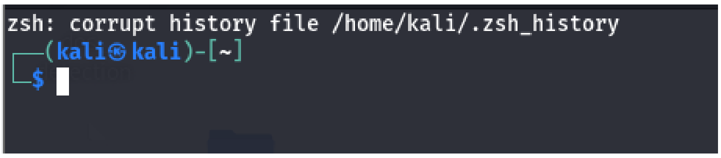
Social Engineering is a cyber attack technique that exploits human psychology rather than technical vulnerabilities. Attackers trick users into revealing sensitive information such as login credentials, banking details, or personal data. Phishing is one of the most common forms of social engineering. The Social Engineering Toolkit (SET) is an open-source framework used to simulate such attacks for educational and awareness purposes.

Theory

Phishing attacks are carried out by sending fake emails or messages that appear to be from trusted sources. These emails may contain malicious links or attachments. When a user interacts with them, sensitive information may be compromised. SET allows security students to understand how attackers design phishing campaigns and how users can identify them.

Procedure

1. Open the terminal in Kali Linux.

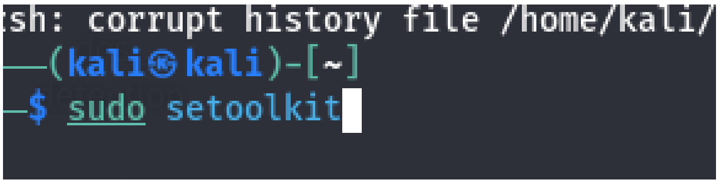


```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ 
```

Figure 1: Opening Terminal in Kali Linux

2. Start the Social Engineering Toolkit using the following command:

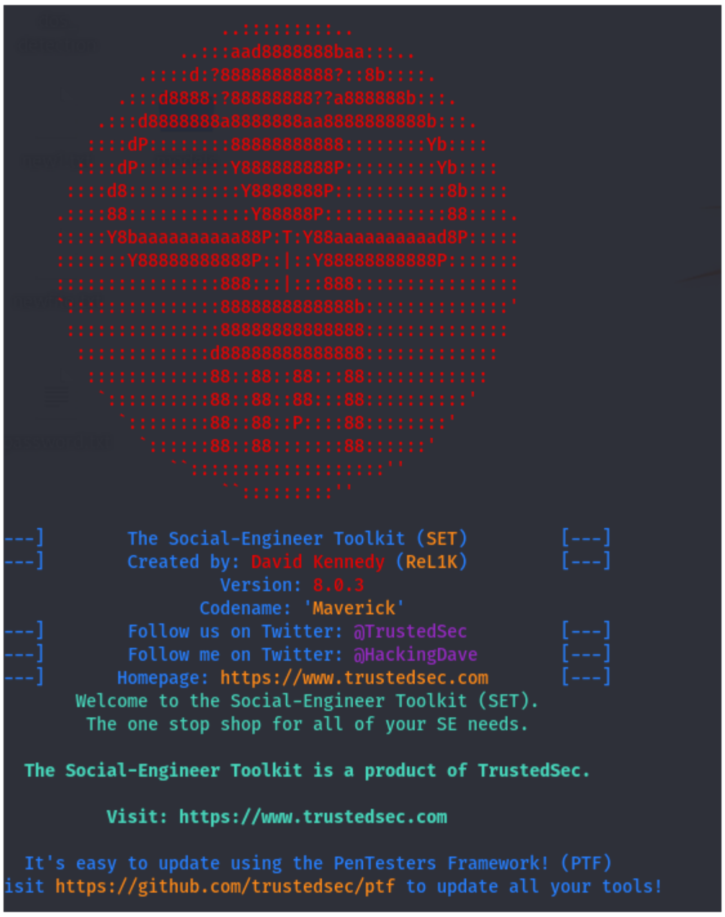
```
sudo setoolkit
```



```
sh: corrupt history file /home/kali/
──(kali㉿kali)-[~]
─$ sudo setoolkit
```

Figure 2: Starting SET Toolkit

3. Accept the SET disclaimer by typing `y` and pressing Enter.

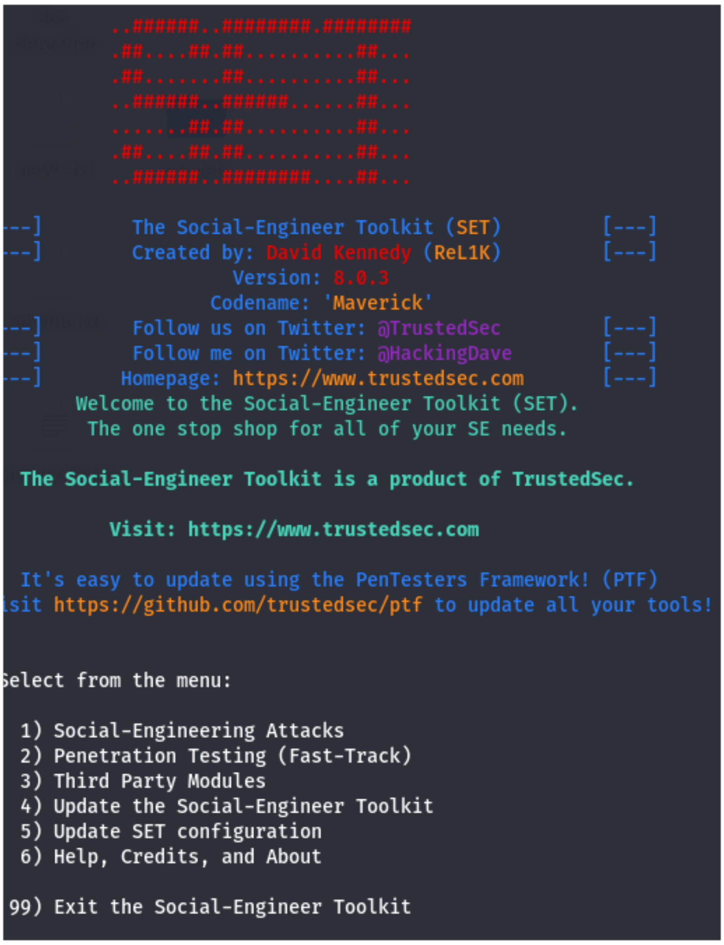


```
                 ..:::::::::..
              ..:::aad8888888baa:::..
           .::::d:?88888888888?::8b::::.
         .:::d8888:?88888888??a888888b:::.
       .:::d8888888a8888888aa8888888888b:::.
      ::::dP::::::::88888888888::::::::Yb::::
     ::::dP:::::::::Y888888888P:::::::::Yb::::
    ::::d8:::::::::::Y8888888P:::::::::::8b::::
   .::::88::::::::::::Y88888P::::::::::::88::::.
   :::::Y8baaaaaaaaaa88P:T:Y88aaaaaaaaaad8P:::::
   :::::::Y88888888888P::|::Y88888888888P:::::::
   ::::::::::::::::888:::|:::888::::::::::::::::
   `:::::::::::::::8888888888888b::::::::::::::'
    :::::::::::::::88888888888888::::::::::::::
     :::::::::::::d88888888888888:::::::::::::
      ::::::::::::88::88::88:::88::::::::::::
       `::::::::::88::88::88:::88::::::::::'
         `::::::::88::88::P::::88::::::::'
           `::::::88::88:::::::88::::::'
              ``:::::::::::::::::::''
                   ``:::::::::''

---]       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)
isit https://github.com/trustedsec/ptf to update all your tools!
```

Figure 3: SET Disclaimer Acceptance

4. From the main menu, select:

```
1) Social-Engineering Attacks
```

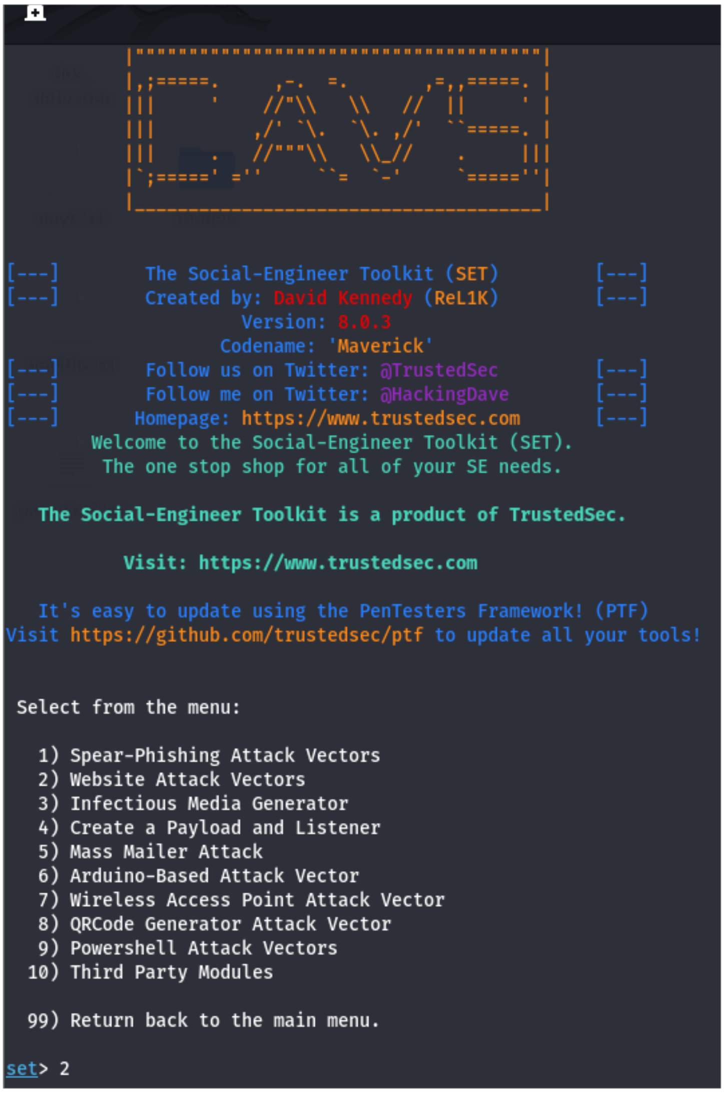


```
          ..######..########.########
          .##....##.##..........##...
          .##.......##..........##...
          ..######..######......##...
          .......##.##..........##...
          .##....##.##..........##...
          ..######..########....##...

---]        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)
isit https://github.com/trustedsec/ptf to update all your tools!


elect 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
```

Figure 4: SET Main Menu Selection

5. Select the phishing attack vector:

```
1) Spear-Phishing Attack Vectors
```

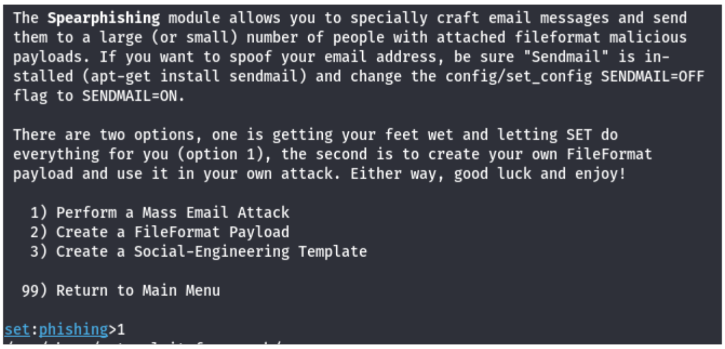


```
          |""""""""""""""""""""""""""""""""""""""""|
          |,;=====.     ,-.  =.           ,=,,=====.|
          |||      '   //"\\   \\       //  ||      '|
          |||        ,/'  `\.  `\.   ,/'   ``=====.|
          |||      .  //"""\\   \\_//       .     |||
          |`;====='  =''     ``=  `-'       `=====''|
          |________________________________________|


[---]        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
```

Figure 5: Selecting Spear Phishing Attack Vector

6. Choose the email-based phishing option:

```
1) Perform a Mass Email Attack
```



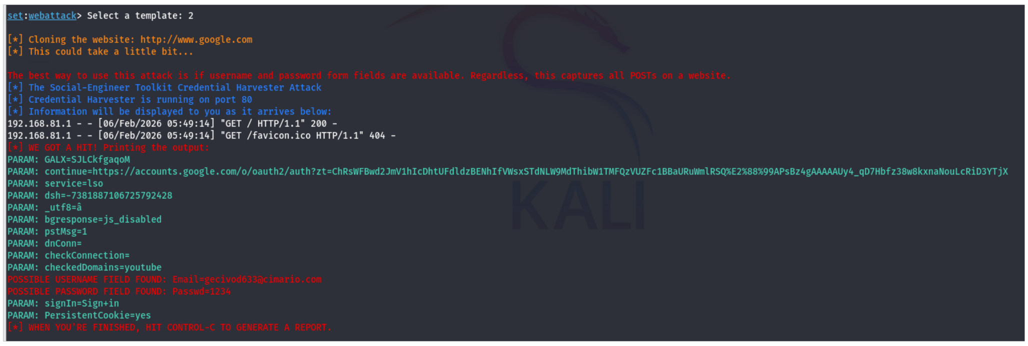
```
The Spearphishing module allows you to specially craft email messages and send
them to a large (or small) number of people with attached fileformat malicious
payloads. If you want to spoof your email address, be sure "Sendmail" is in-
stalled (apt-get install sendmail) and change the config/set_config SENDMAIL=OFF
flag to SENDMAIL=ON.

There are two options, one is getting your feet wet and letting SET do
everything for you (option 1), the second is to create your own FileFormat
payload and use it in your own attack. Either way, good luck and enjoy!

   1) Perform a Mass Email Attack
   2) Create a FileFormat Payload
   3) Create a Social-Engineering Template

  99) Return to Main Menu

set:phishing>1
```

Figure 6: Mass Email Attack Option

7. SET displays FileFormat or payload-based options which represent attachment-

based phishing methods.

8. Select a social engineering based payload option to continue the simulation.
9. Enter the required email details such as sender email address, target test email address, subject, and message content.
10. SET sends the phishing email to the specified test email address.
11. Monitor the terminal for responses or interactions.



```
set:webattack> 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
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.81.1 - - [06/Feb/2026 05:49:14] "GET / HTTP/1.1" 200 -
192.168.81.1 - - [06/Feb/2026 05:49:14] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=gecivod633@cimario.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=1234
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Figure 7: Monitoring Phishing Responses

Result

The phishing attack simulation using Social Engineering Toolkit was successfully performed in a controlled lab environment.

Detection of Phishing Attacks

- Suspicious sender email addresses
- Urgent or threatening language
- Unexpected attachments or links
- Mismatched or shortened URLs
- Spelling and grammatical errors

Prevention Techniques

- User security awareness training
- Avoid clicking unknown links or attachments
- Verify website URLs before entering credentials
- Use Multi-Factor Authentication (MFA)
- Report phishing emails to administrators

Conclusion

Social Engineering attacks are highly effective because they target human behavior. The SET Toolkit helps learners understand phishing attack techniques and emphasizes the importance of user awareness and preventive security measures.

Ethical Considerations

This experiment was conducted strictly for educational purposes in a controlled environment. Phishing attacks without proper authorization are illegal and unethical.