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 sucessfully.we can launch the toolkit using the shown below,

```
#setoolkit
```

select the menu;

```
1)Social-Engineering Attacks

2)penetratration 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 Listenner

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

Relevent option is choose:

1)Java Applet Attack Method

2)Metaspoilit Browser Expolit 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[192.168.1.110] :

set:webattack>IPAddress for the page

Website templae from the list below:

1)Java Requiired

2)Google

3)Twitter

set>2

[*]Cloning the Website

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

PARAM:

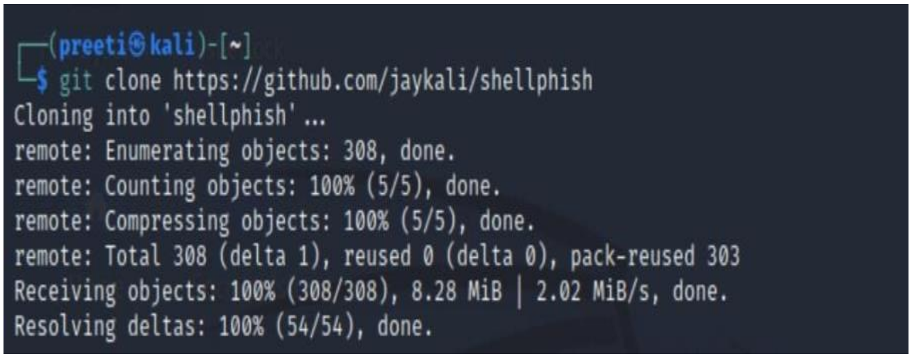
scrible_log=

PARAM:

authnticity_token=db333456734abcdefg23456

when you are Finished

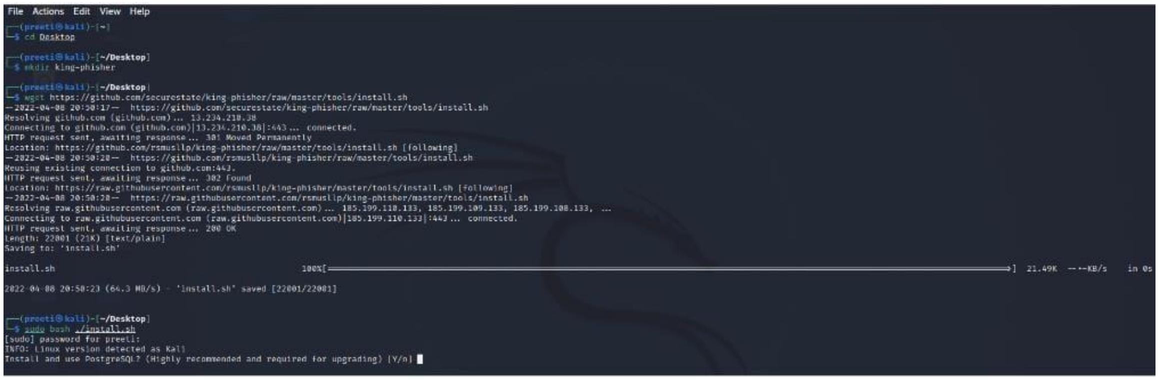
Hit Control C to Generate a Report



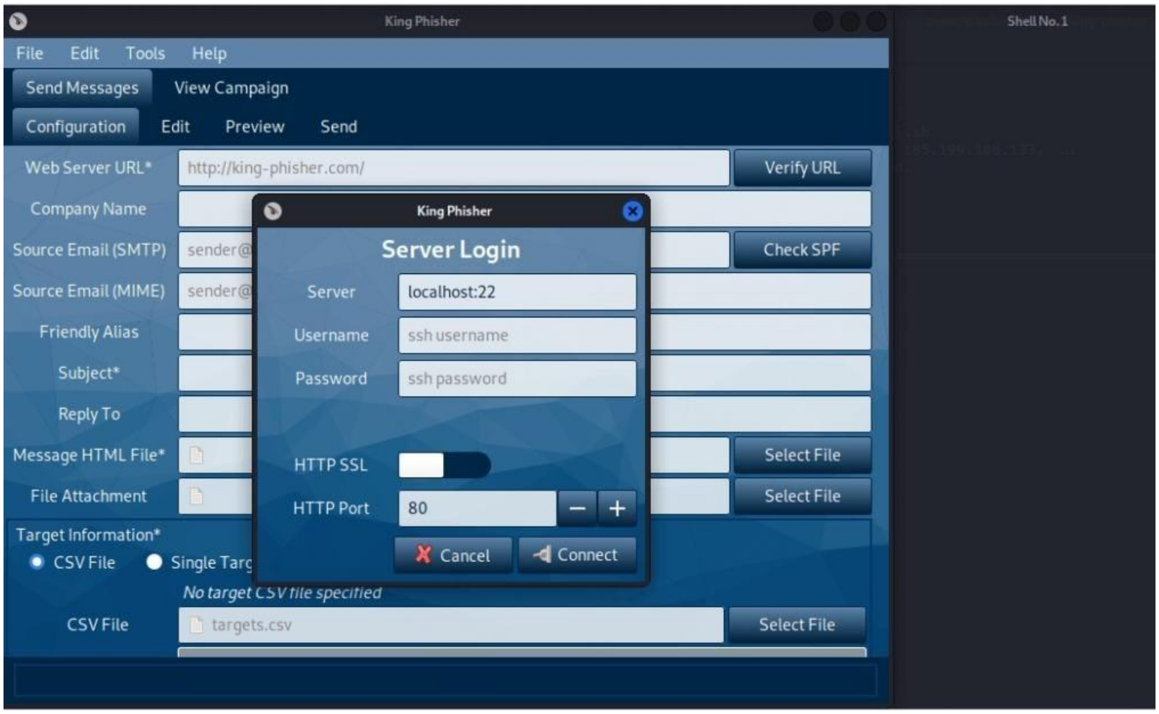
```
┌──(preeti㉿kali)-[~]
└─$ git clone https://github.com/jaykali/shellphish
Cloning into 'shellphish'...
remote: Enumerating objects: 308, done.
remote: Counting objects: 100% (5/5), done.
remote: Compressing objects: 100% (5/5), done.
remote: Total 308 (delta 1), reused 0 (delta 0), pack-reused 303
Receiving objects: 100% (308/308), 8.28 MiB | 2.02 MiB/s, done.
Resolving deltas: 100% (54/54), done.
```

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:



```
┌──(preeti㉿kali)-[~]
└─$ cd Desktop

┌──(preeti㉿kali)-[~/Desktop]
└─$ mkdir king-phisher

┌──(preeti㉿kali)-[~/Desktop]
└─$ wget https://github.com/securestate/king-phisher/raw/master/tools/install.sh
--2022-04-08 20:50:17--  https://github.com/securestate/king-phisher/raw/master/tools/install.sh
Resolving github.com (github.com)... 13.234.210.38
Connecting to github.com (github.com)|13.234.210.38|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://github.com/rsmusllp/king-phisher/raw/master/tools/install.sh [following]
--2022-04-08 20:50:20--  https://github.com/rsmusllp/king-phisher/raw/master/tools/install.sh
Reusing existing connection to github.com:443.
HTTP request sent, awaiting response... 302 Found
Location: https://raw.githubusercontent.com/rsmusllp/king-phisher/master/tools/install.sh [following]
--2022-04-08 20:50:20--  https://raw.githubusercontent.com/rsmusllp/king-phisher/master/tools/install.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.110.133, 185.199.109.133, 185.199.108.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.110.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 22001 (21K) [text/plain]
Saving to: 'install.sh'

install.sh                    100%[=====================================================>]  21.49K  --.-KB/s    in 0s

2022-04-08 20:50:23 (64.3 MB/s) - 'install.sh' saved [22001/22001]


┌──(preeti㉿kali)-[~/Desktop]
└─$ sudo bash ./install.sh
[sudo] password for preeti:
INFO: Linux version detected as Kali
Install and use PostgreSQL? (Highly recommended and required for upgrading) [Y/n] █
```



Web Server URL*: http://king-phisher.com/
Company Name:
Source Email (SMTP): sender@
Source Email (MIME): sender@
Friendly Alias:
Subject*:
Reply To:
Message HTML File*:
File Attachment:
Target Information*: ● CSV File ○ Single Targ
No target CSV file specified
CSV File: targets.csv

King Phisher

Server Login

Server: localhost:22
Username: ssh username
Password: ssh password
HTTP SSL
HTTP Port: 80