The Social Engineering Toolkit (SET)

**Table of Contents**

1. [What is the SET?](#_qnk8g5bk97tj)
2. Setting Up the Environment
   1. Changing the network configurations
   2. Updating the SET version
   3. Enabling the Apache Server

### **What is SET?**

* The Social-Engineer Toolkit is designed to perform attacks against the human element. “The attacks built into the toolkit are designed to be targeted and focused against a person or organization during a penetration test.”

### **Setting up the Environment**

#### Changing the Network Configurations

* Open **Virtual Box.** Right-click on the **Kali Linux Virtual Machine**, then go to **Settings**
* In the Network tab, select “**NAT”,** and enter “**OK”.**

#### Updating the SET version

* Once you have your network setup, you can update the pre-installed SET to the newest version.
* Start your **Kali Linux VM**, and open **Terminal**
* Type the following, one by one, to terminal:

|  |
| --- |
| root@kali:~# git clone https://github.com/trustedsec/social-engineer-toolkit/ set/  root@kali:~# cd set  root@kali:~# python setup.py install |

* Once you have finished updating SET, close your terminal and re-open a new window.

#### Enabling the Apache Server

* We will now enable the Apache server, on which our fake website will be hosted. To do so, in **Terminal**, type:

|  |
| --- |
| root@kali:~# gedit /etc/setoolkit/set.config |

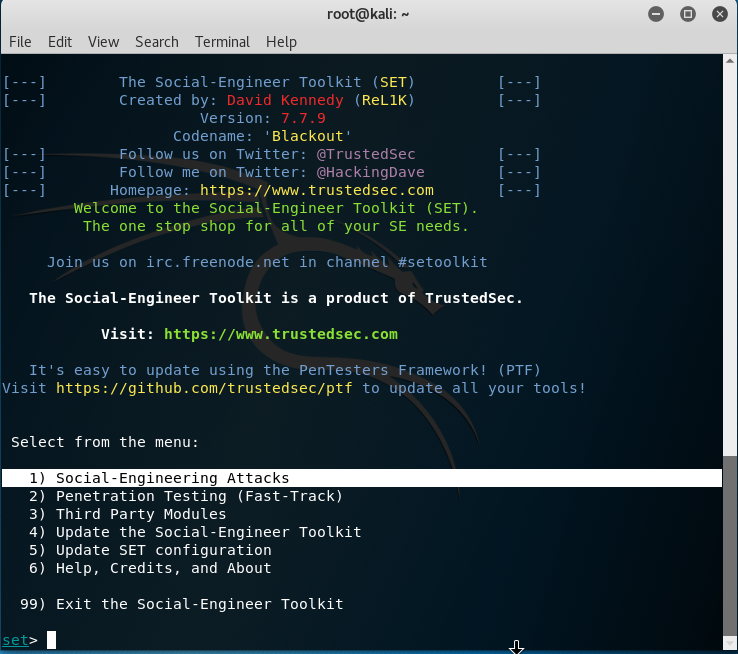
* What this will do is open the configuration file in a text editor. Scroll down until you see “APACHE\_SERVER = OFF”, and change it to -> “APACHE\_SERVER = ON”
* Save the file, and close it.

Great, your environment is ready to go! We will now proceed to the first part of the lab.

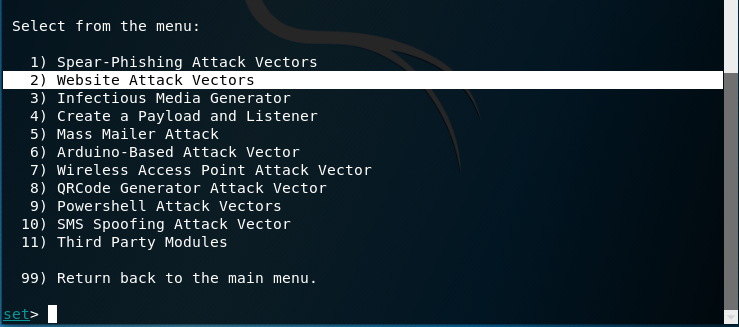
### **Hack Gmail & Facebook of Remote PC using DNS Spoofing and SET**

In this section of the lab, we will be using SET to clone a login page of a website, then monitor when a person accesses it to collect the username and password.

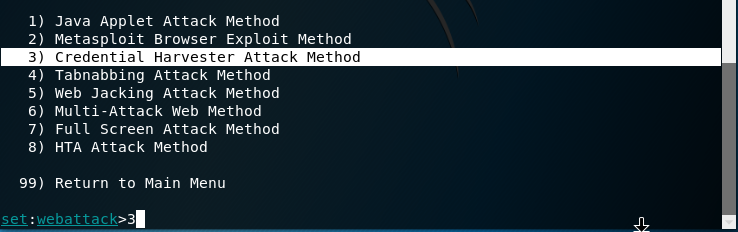
1. In **Terminal,** type: **setoolkit,** which will output this:



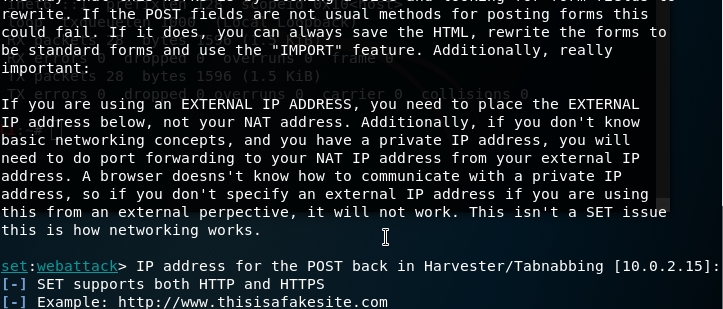
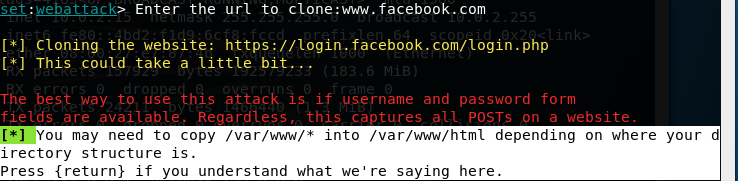
1. Enter **1** for “**Social-Engineering Attacks**”, then 2 for “**Website Attack Vectors**”. This is because we will attack victims via the browser.

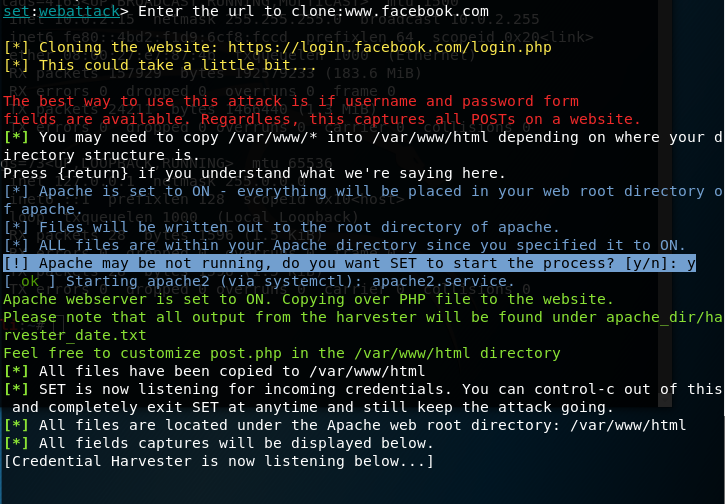


1. Select **3**, for “**Credential Harvester Attack Method**”. This will utilize web-cloning, then harvest all the information posted to that website. Finally, enter **2,** for “**Site Cloner**”.

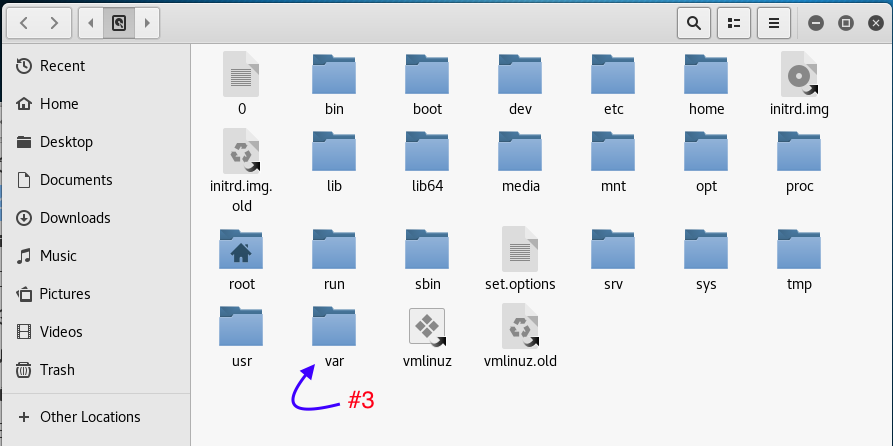
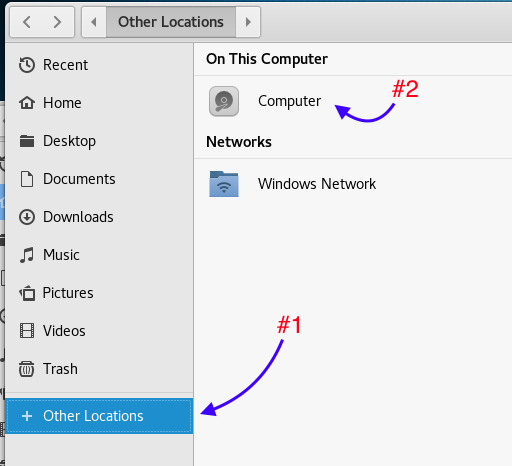


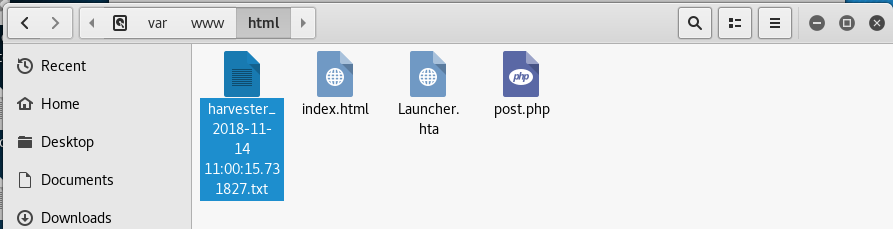


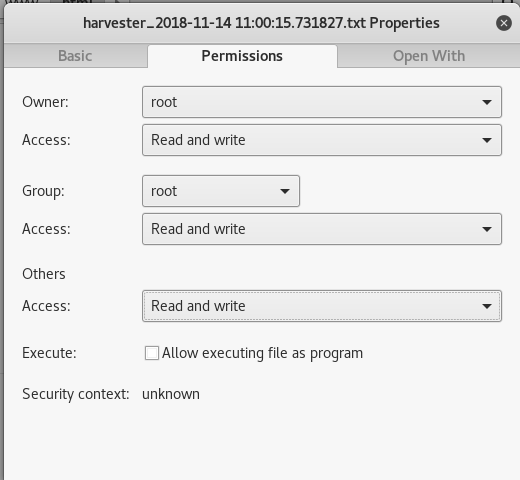
1. You will now be asked for an IP address. This IP address will be used to harvest the usernames & passwords from the fake website.
   1. You may notice that setoolkit has provided an IP address in brackets, which is the IP address of your network.
2. Simply **press enter** to use the IP address provided.
3. When asked which URL to clone, **type:** “[www.facebook.com](http://www.facebook.com)”.
4. If you are given this prompt, press **enter:**
5. “Apache may not be running, do you want SET to start the process? [y/n]”
   1. Type **y** and press enter

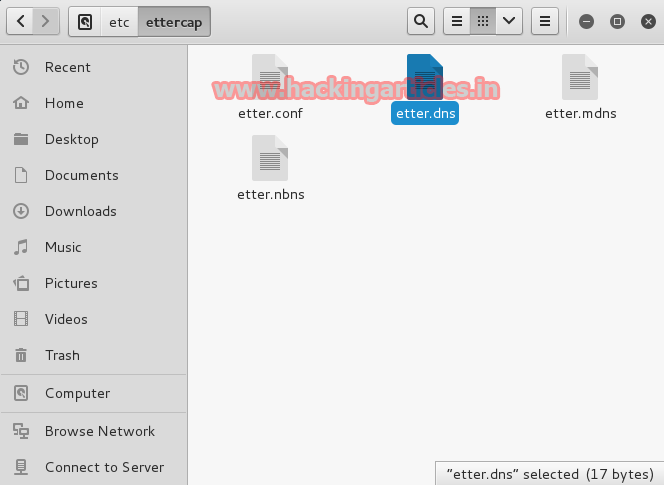


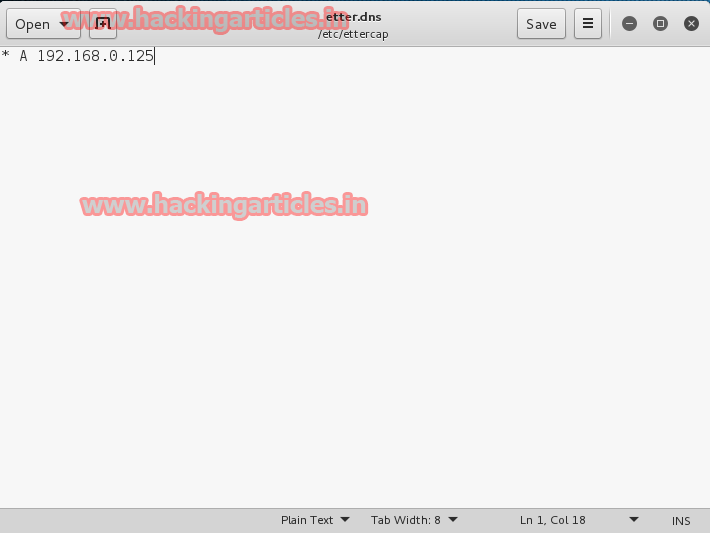
1. Once the website has been harvested, you can find the files located in **/var/www/html**



1. Double-click on “**index.html**” to preview it. That is the cloned website that we will be using!
2. Right-click on the “harvester..” text file and enable “read and write”, and change the directory to “root”.



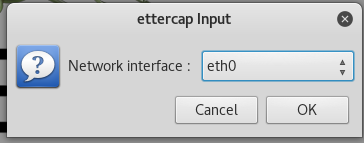
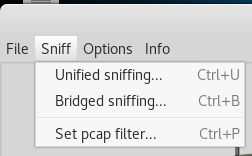
1. Now open **etter.dns** file which is in **/etc/ettercap** folder.
2. Modify the contents of the **etter.dns** and add your own pc **IP** address as **A** record.

**Ettercap **

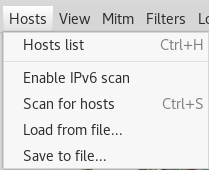
1. Open **Ettercap-Graphical**

****

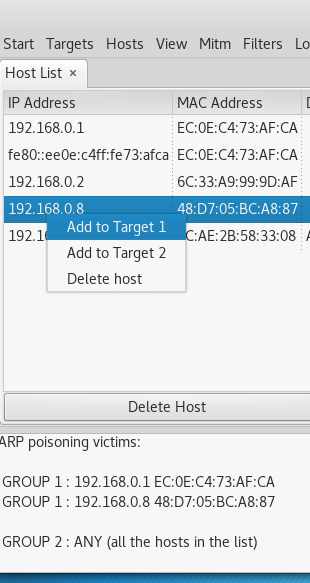
1. Click to **Sniff-> Unified Sniffing**

****

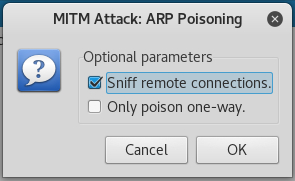
1. On the menu bar, select **Hosts -> Scan for Hosts**



1. Once the scan is complete, click on **Hosts -> Host List**
2. Right click on your IP address (if you’re not sure what your IP address is, go to **Terminal** and type “ifconfig”. Then, in the row labelled “**eth0**”, search for **“inet**”) and click “**Add to Target1**”



1. Click on **MITM -> ARP Poisoning -> Sniff Remote Connections**

****

1. Go to plugins and enable DNS Spoofing.

Now, if you go type in your IP address on the browser, you will see the website that you cloned. If you enter (demo) log-in credentials, then they will show up in the “harvester…” text file.

