**GATHERING LOGIN INFORMATION USING CREDENTIAL HARVESTER**

**Introduction**

Credential harvester is a tool in Social Engineering Toolkit (SET) that is used to acquire credentials of victims by cloning social sites to lure them into entering their login credentials and give access to their accounts.

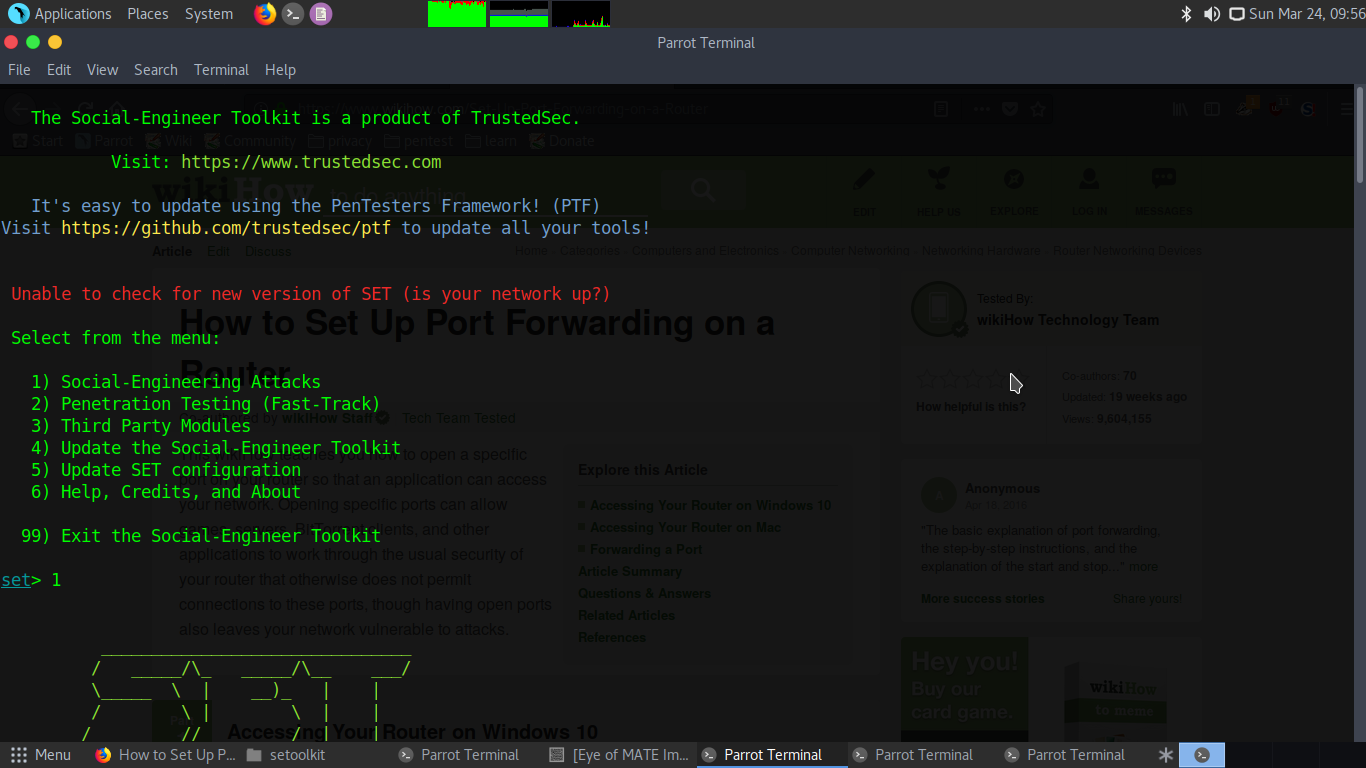
After a successful process (When user logins in and credentials saved), credential harvester gives back the session token that can be used to get access to users account without the attacker login in.

**How It Works**

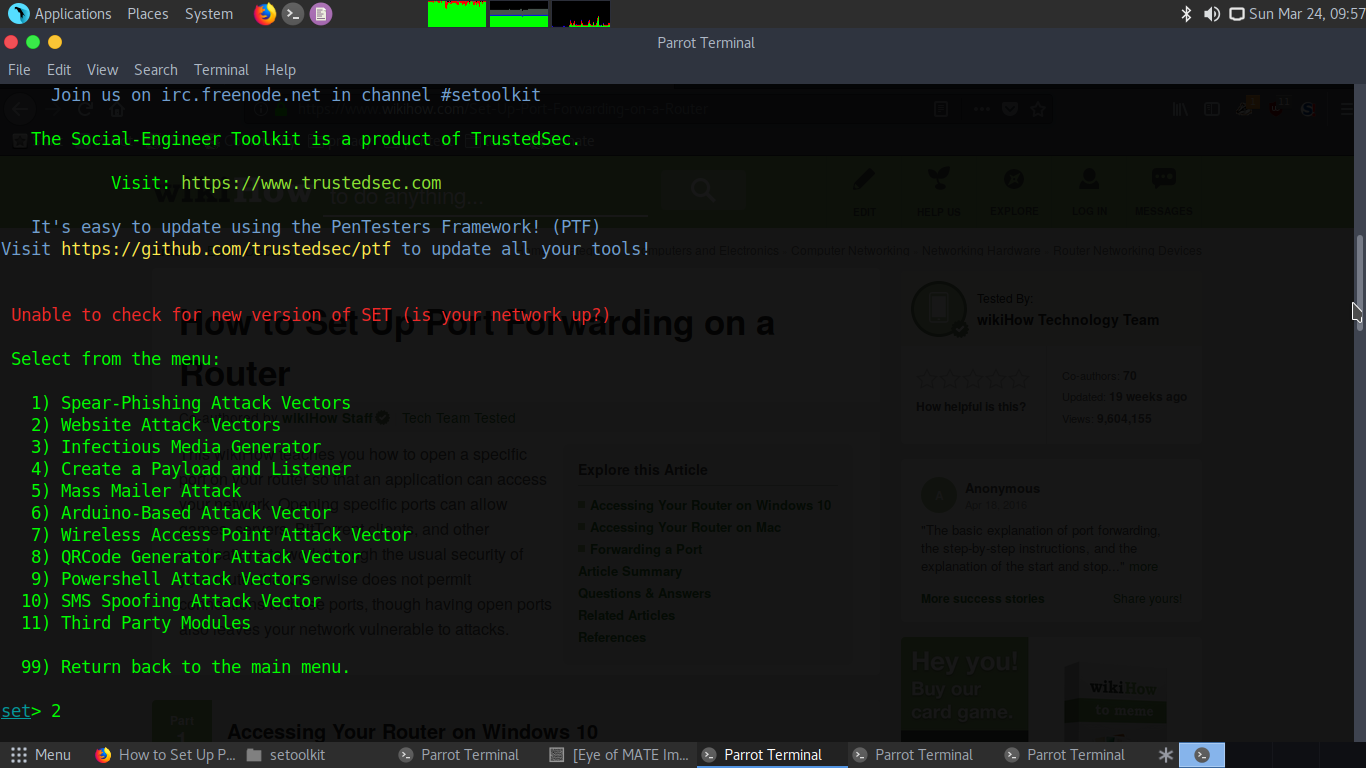
1. Fire up Kali Linux or Parrot and navigate to **Applications.** From there select **Kali Linux** and select **Social Engineering Toolkit**.

If you are running Parrot navigate to **Menu** on the bottom left of the screen, type and select **Social Engineering Toolkit.**

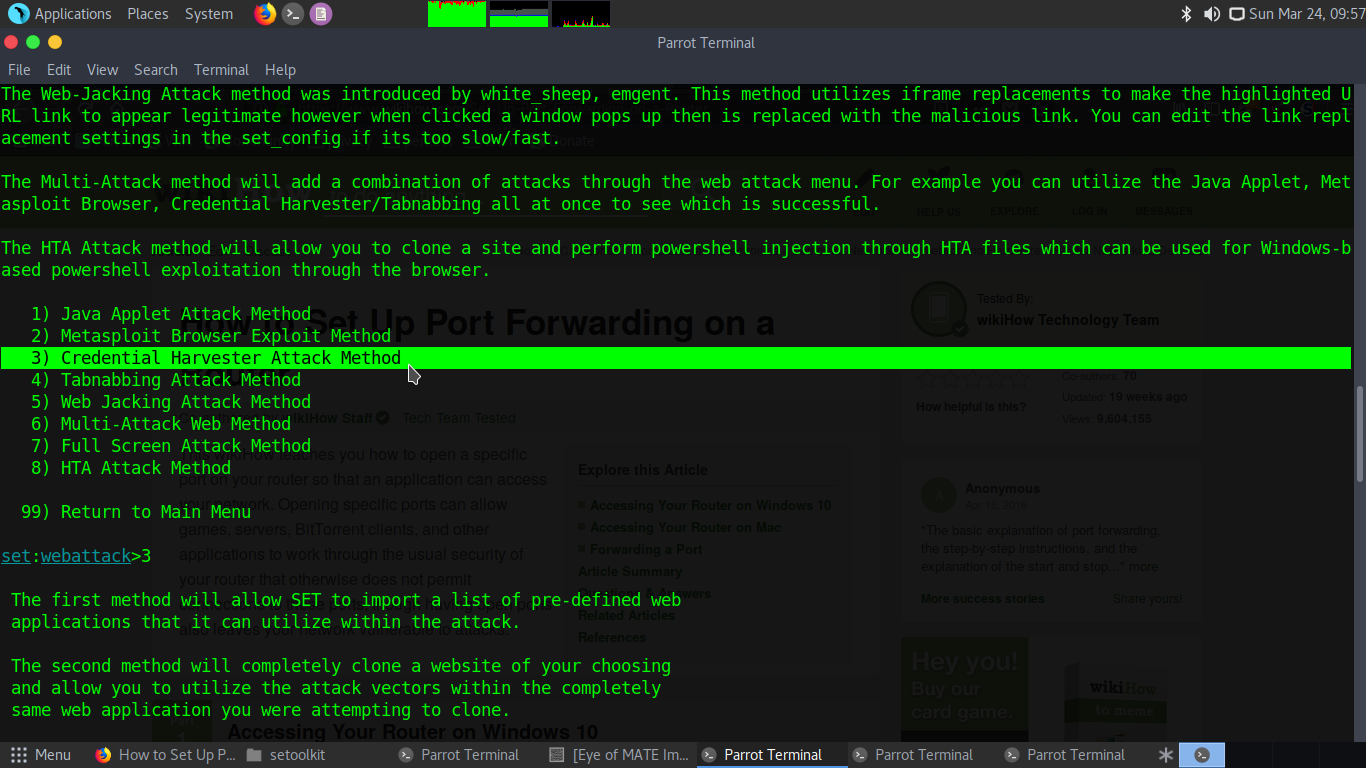
1. After launching Social Engineering Toolkit it will display a menu as shown in the diagram below.



1. Below the menu the console input will change to **set.** Type in 1 to select **Social Engineering Attacks.** We select social engnnering attacks to get the credentials on social sites.
2. After selecting the first option, we get another menu displaying the different attacks that we can use. For our case, we are only interested in **Websites Attack Vectors** since we are cloning a social site. So select 2.

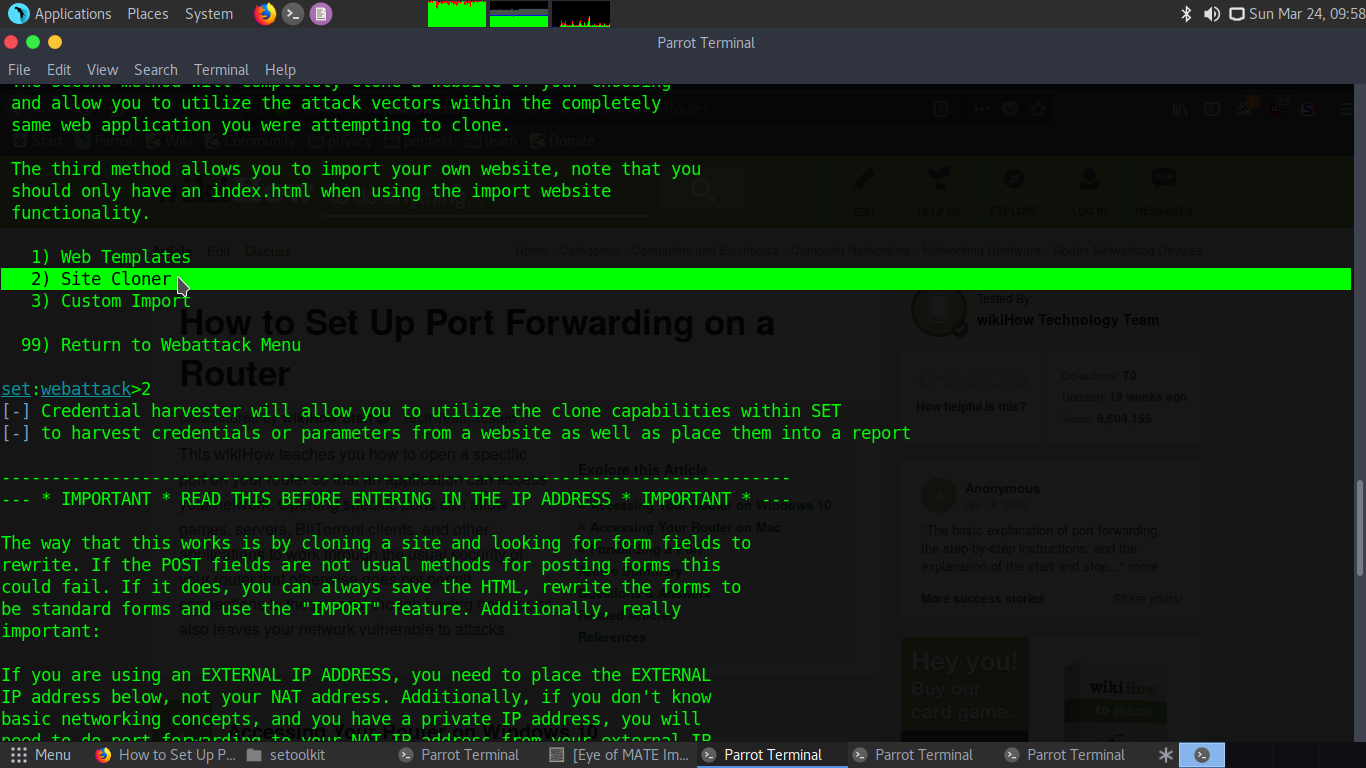


1. After we are fed with a menu containing methods that we will use to run. We select **Credential Harvester** since our tutorial focuses on using cloned sites to acquire credentials. Select 3



1. Now we have to choose between the three options provided for sites. **Site Cloner** is our best choice for reason of luring the client to believe that he/she is running on the original site.

Select 2.



1. Lets now set our IP Address that we are to use. Here we have two options, either set it as default (that’s our Local IP or system’s IP) or we can decide to use it over WAN where we will need to do port forwarding to get our Public IP. But we will first concentrate on using it locally then we do over wan on our next tutorial. **Enter your IP if its not displayed and press ENTER**.
2. We are almost set, (Read through the info messages displayed also). Lastly we will enter the site we want to clone. In our Example we take [**www.github.com**](http://www.github.com)
3. Now Credential harvester will start cloning the site. It may take a while depending on your internet connectivity. After its done, fire up your browser and type **localhost.** It will load the site you cloned and you can now enter the credentials.
4. Press Login (May differ with different sites). Go back to your terminal and VOILA! The credentials you entered appear.

