**Creating a phishing page using Social Engineering Toolkit**

**(SET) -WAN Attack**

In this tutorial we are going to learn how to create a phishing page using social engineering toolkit(SET) over WAN.

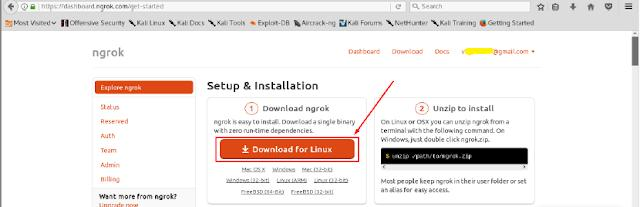
So sit back and set your kali linux ready because you are going to do some real things that may amaze you.

In Kali Linux terminal, execute the below command to remove existing files from web root location.

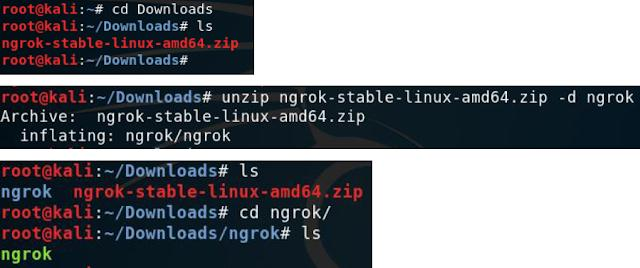


**Ngrok Installation and configuration:**

Ngrok is a tool that opens access to the local ports on the internet and creates a secure tunnel. Visit [https://ngrok.coma](https://ngrok.com/)nd register to download a free version of the software.

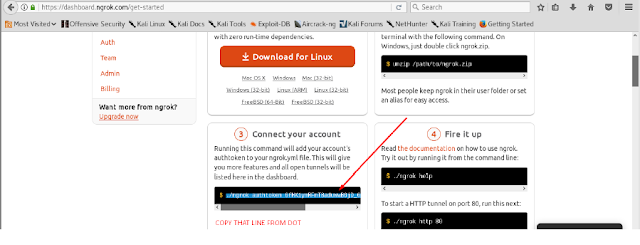


To install ngrok application follow the process shown in below images (We can also get detailed installation steps from the ngrok website).



To run ngrok on our computer (attacker’s kali linux machine), from ngrok directory execute

the command given on the ngrok website.

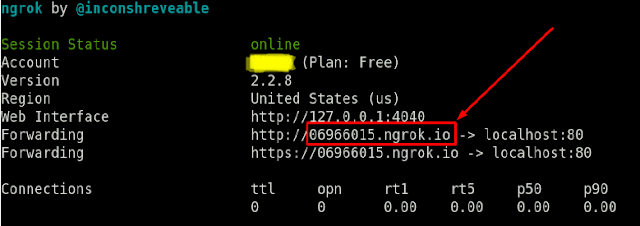




Execute below command that starts ngrok.



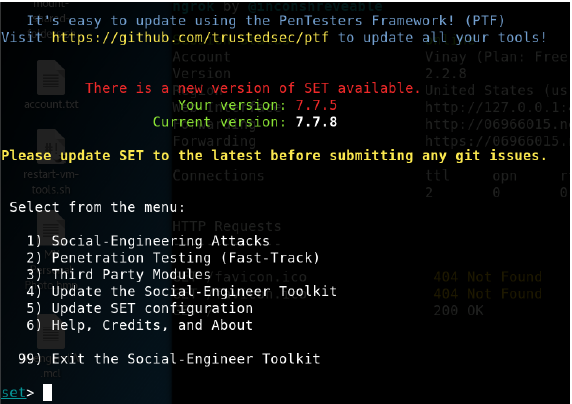
After executing the above command, ngrok opens a new terminal with links to forwarded ports.



**Creating the phishing page:**

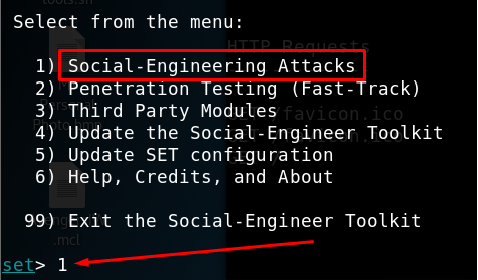
launch Social Engineering Toolkit by executing below command



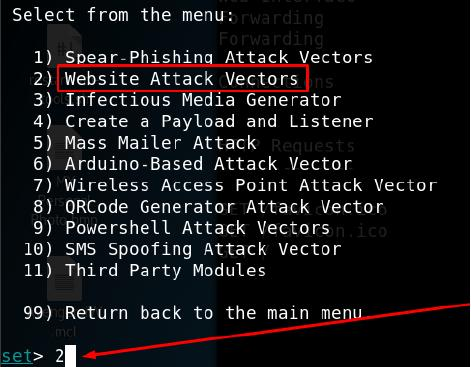


In this practical, we intend to create a phishing a page that looks similar to the Facebook login page which should be available for anyone on the internet.

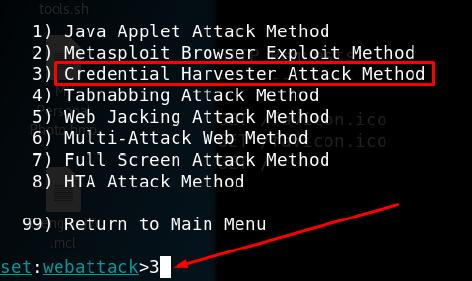
Select option 1 Social-Engineering Attacks



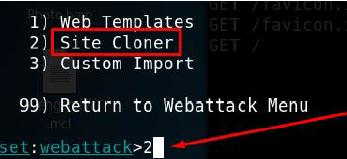
Select option 2 Website Attack Vectors

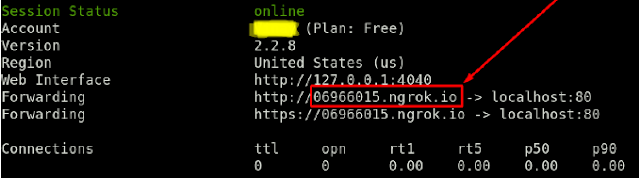


Select option 3 Credential Harvester Attack Method to harvest login credentials with the help of phishing page.



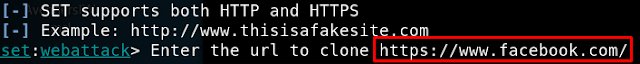
Choose 2 Site Cloner to clone a live website.



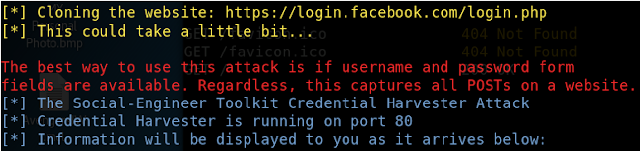




To perform WAN level phishing attack, provide domain generated by ngrok for the postback

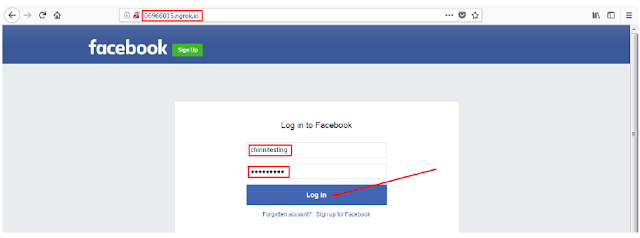


Provide the address of website to be cloned (https:/[/www.facebook.com/)](http://www.facebook.com/) press enter and wait until Credential Harvester is running on port 80 message.

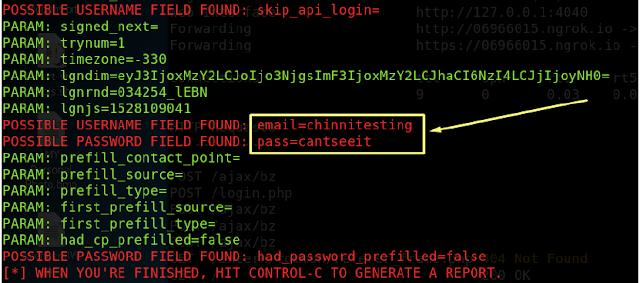


Trick victim to visit [https://06966015.ngrok.io .](http://www.peoplezmind.com/) If the victim submits login credentials on phishing page, then the attacker will be able to view those credentials.

**On the victim’s computer:**



**On the attacker’s computer:**



So by following the above steps you can create a phishing page using SET over WAN level.