**Module 9**

**Social engineering**

We will start our module by asking question about module , lets start.

**What is social engineering ?**

Social engineering is a art of convincing the victim to give confidential information .

But before doing social engineering we need to collect tough information of victim ,so we will gain trust of victim .

Many types of information gathering is already shown in 2nd module of CEH

**Why social engineer take place?**

**Employee has:**

Lack of security knowledge.

Lack of security policy.

Don’t get training about awareness of malicious mail and link.

**Attacker attack the person !**

*Common person who always face social engineer attack*

* Receptionist and help desk personnel
* System administrator
* Technical support executive
* Senior executive.

**Types of social engineering:-**

**Human-based social engineering:**

* Shoulder Surfing
* Eavesdropping
* Dumpster Diving

**Computer-based social engineering:**

* Phising
* Spam mail
* Instant Chat Messenger

**Mobile-based social engineering:**

* Publishing Malicious apps
* Repackaging legitimate app

Some real factor which among this days is famous.

**Vishing:-** In this attack, a person receivese the call that he won the lottery, lucky prizes etc , which is totally fraud. In simple word Fraud call with intension to loot the victim is a Vishing.

**Call spoofing:-** In this attack, caller changes their no, means each time he will call you with different number.

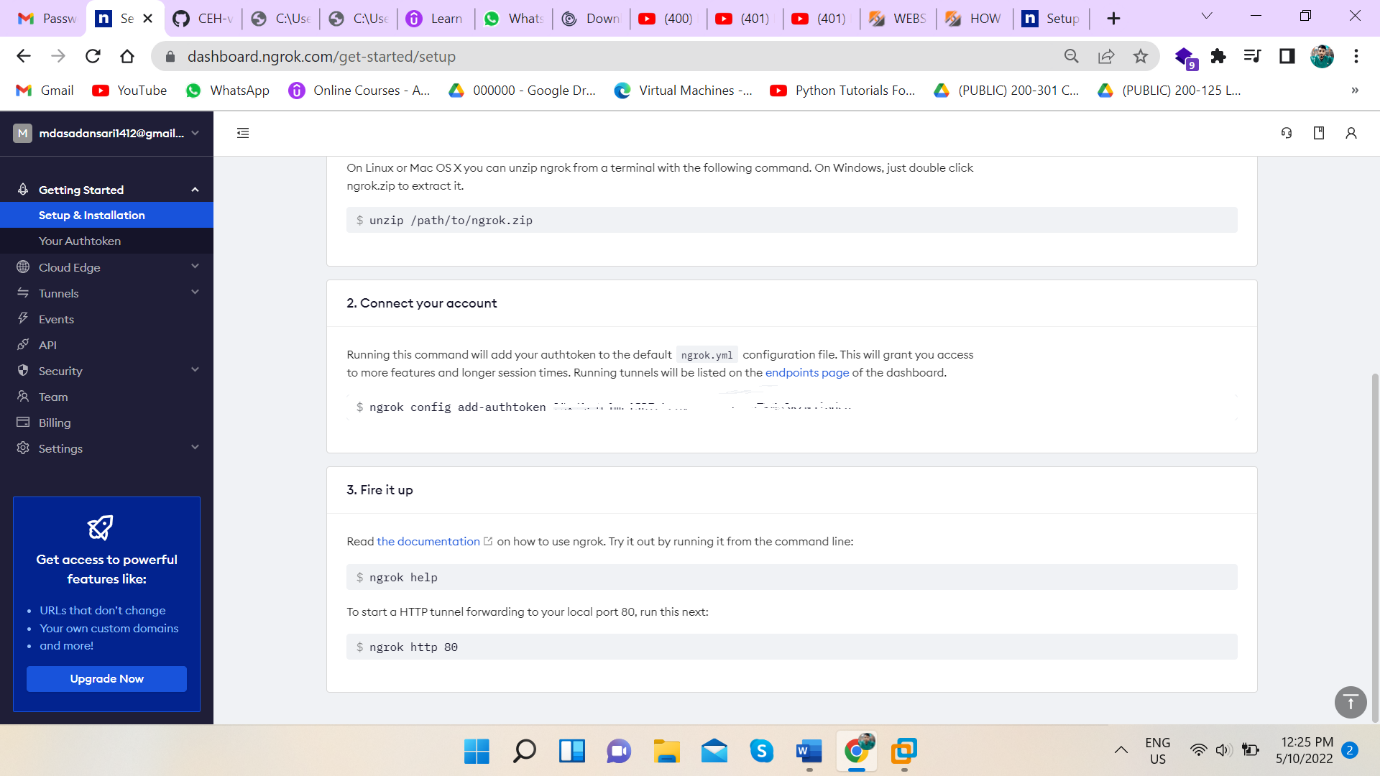
**Set up :**

**Lets set up the ngrok**

This is server which is mostly used in phising

Go to the :- ngrok.com

Signup with your valid gmail.



After sign up just follow the website step , we will get the local host link .

Know launch the phising tool

Tool name is **zphisher**

**Zphisher** :- <https://github.com/htr-tech/zphisher>

Download it with command :- git clone <https://github.com/htr-tech/zphisher>

Launch the ngrok in other tab

So many template is there



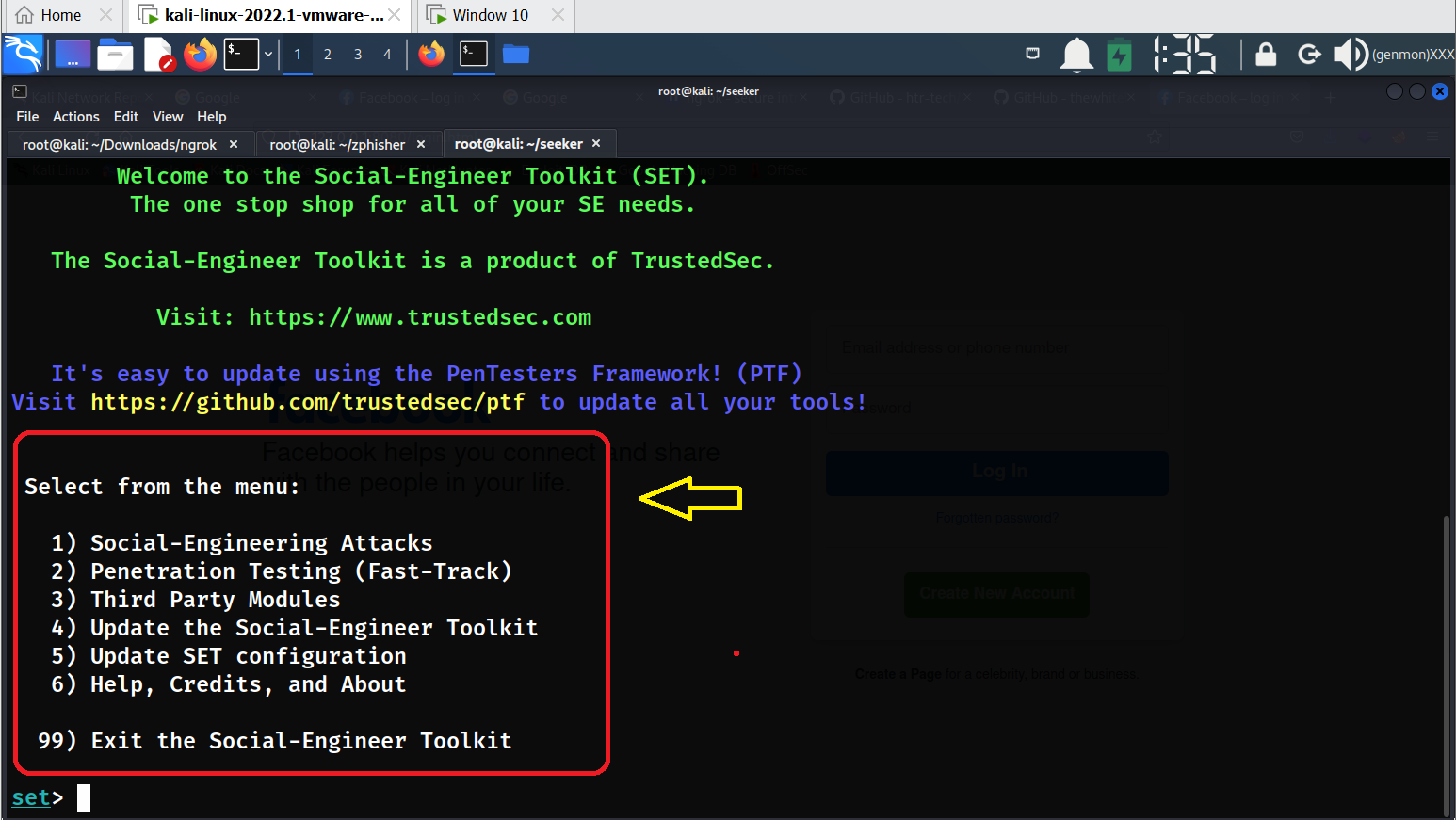
As we are seeing in above pic all template are there

Use any one and chose server for local host.

Another tool is most usefull and power full tool is

Social engineer toolkit

Command :- setoolkit



It will pop option select social eng.

Select website attack

Select credential harvester

Select site cloner

Here we can use the ngrok forwarding link or we can use our local ip for cloning website .

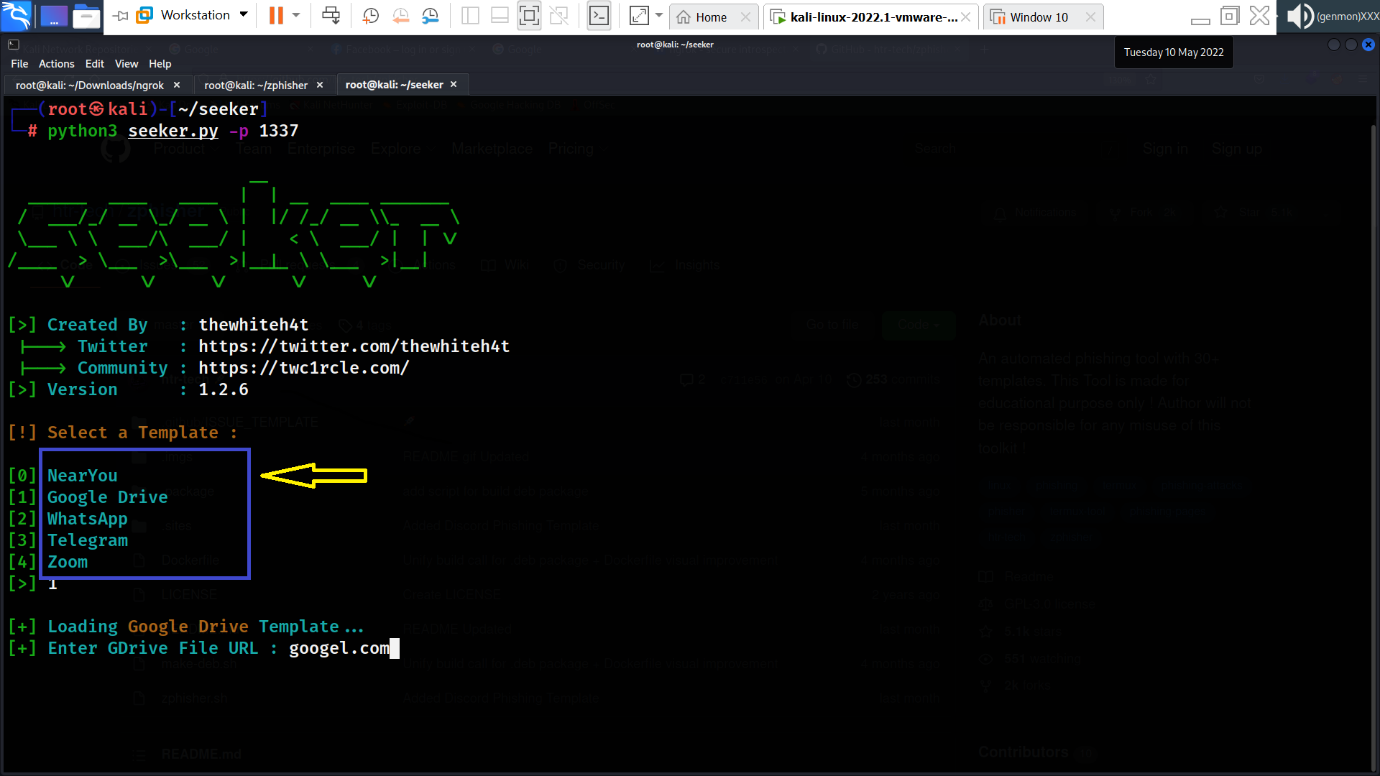
Know give cloning website domain whom we want to clone.

Boom we got link, know we can send this link to victim.

This link is universally connected .

Lets see another powerfull tool

Seekers:- <https://github.com/thewhiteh4t/seeker>



After install it , run bash file of seekers, name is install.sh

After that here is the man thing we need to do

Open one new tab go to the ngrok tab

And run the ngrok

Command :- ./ngrok http 2222

And in previous tab run seekers

Command :- python3 seekers -p 2222

[*one thing is here which can be notice and take care of it ports of ngrok and seekers must have same*]

**Step** - Than select google drive options

**Step** – Than give google domain : google.com

**Step** – Than go to the ngrok tab and copy the link and send to the victim , as he open the link he will be ask for the permission for location by google . After giving permission that page will redirect him to the google page.

Another tool is cam phis

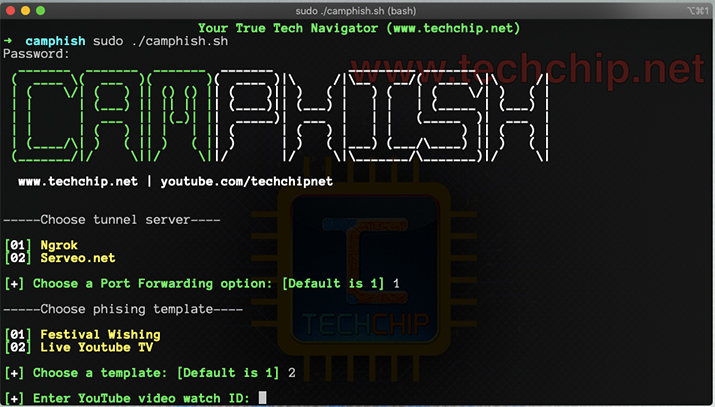
Source :- <https://github.com/techchipnet/CamPhish>

Just install it and launch it bash file

Go with ngrok and it will token of ngrok

Provide it .

We will get link , it will be universally accessible .



**Malicious link or mail delivery method**

First sign up in send in blue website – SMTP server provider

**Source :-** <https://www.sendinblue.com/?utm_source=adwords_brand&utm_medium=lastclick&utm_content=SendinBlue&utm_extension&utm_term=sendinblue&utm_matchtype=e&utm_campaign=14918501916&utm_network=g&km_adid=552063131976&km_adposition&km_device=c&utm_adgroupid=127978740373&gclid=Cj0KCQjwmuiTBhDoARIsAPiv6L-xvdO9qU6tF4o-6QKFkuyjXePS5wCfthnZDHIAw3jiMsYKm-bu2XIaAnfqEALw_wcB>

All important tab are there in Transactional section

We will take help of send in Blue which is SMTP server provider

Command :-

Sendemail -xu [server\_mail] -xp [server\_password] -s [server\_name:(along\_with\_port)] -f [sender\_mail] -t [reciver\_mail] -u [subject\_of\_mail] -m [message\_Body] -o message-header=”From: [name of sender] <sender\_mail\_again>

Above command is used for to deliver the malicious mail with legitimate way.