# Internship Program - Cyber Security

**Group1:**

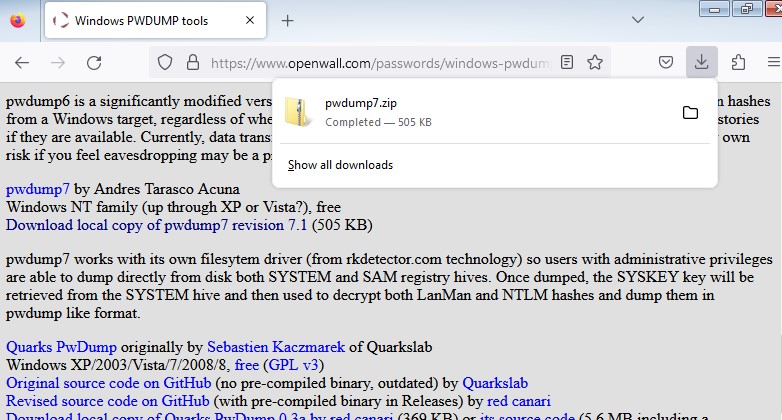
1. Install the below software:
   1. Virtual box
   2. Kali Linux
   3. Metasploit machine
   4. Windows 7 machine
2. Perform password cracking
   1. Perform password cracking of windows 7 machine

Steps:

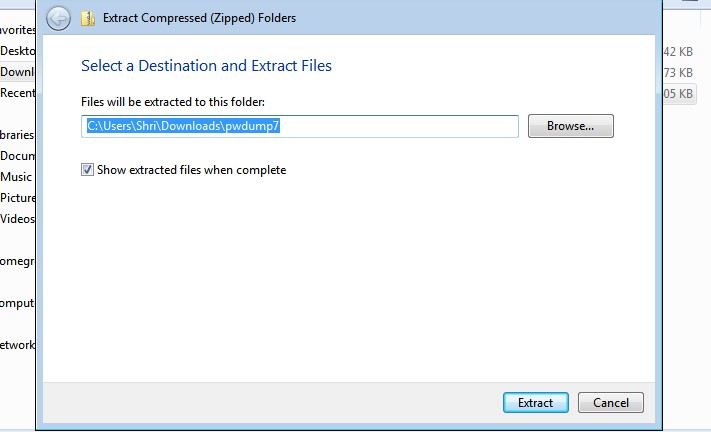
1. Simultaneously open your kali linux and your windows7 on your virtual machine. Then Download the *pwdump* tool in windows 7 machine.



1. The tool is downloaded from [**https://www.openwall.com**](https://www.openwall.com/)**.** Using the version 7.1(505 kB).

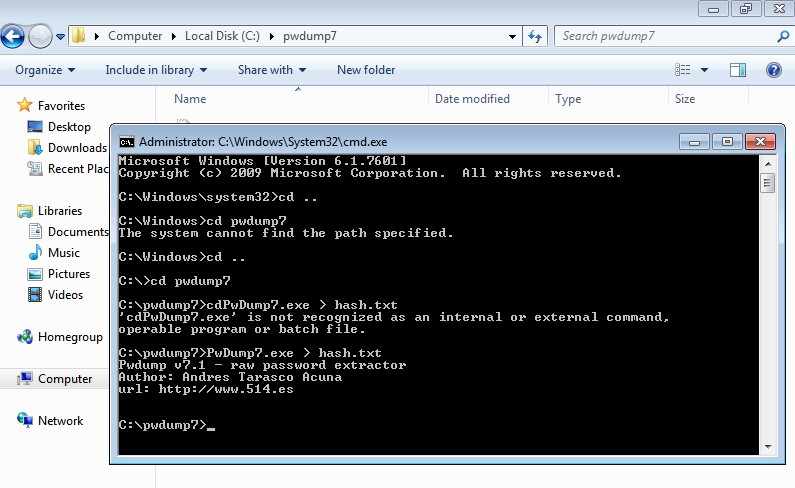


1. Extract downloaded zip file and paste the file in the path c:/windows.

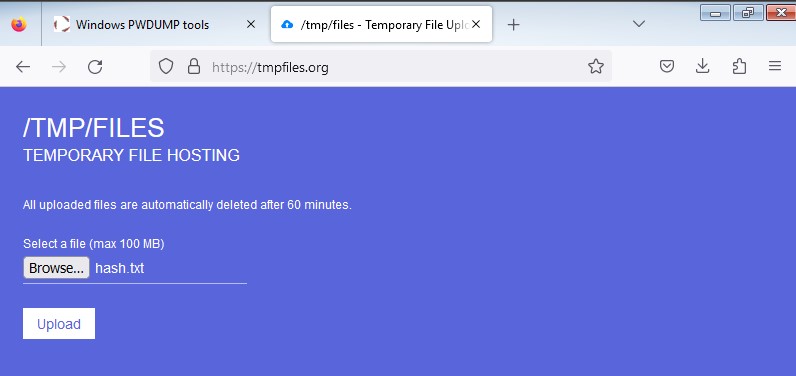


1. Open command prompt as administrator and run below command:

C:\ pwdump7 > PuDump7.exe > hash.txt

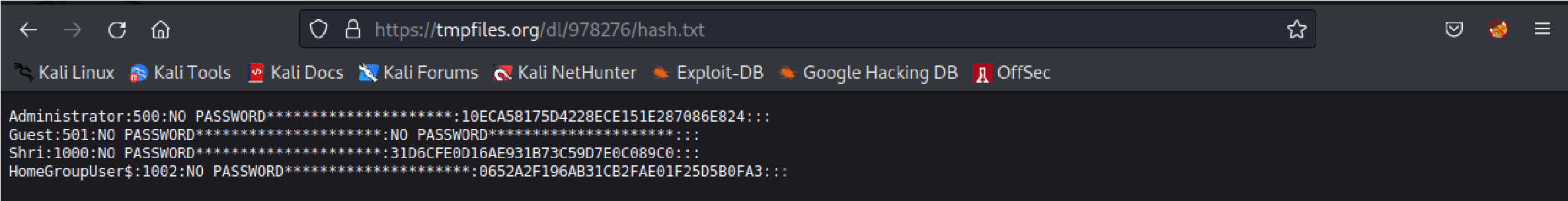


1. By using [**https://tmpfiles.org**](https://tmpfiles.org/)upload file to get downloaded in kali machine.





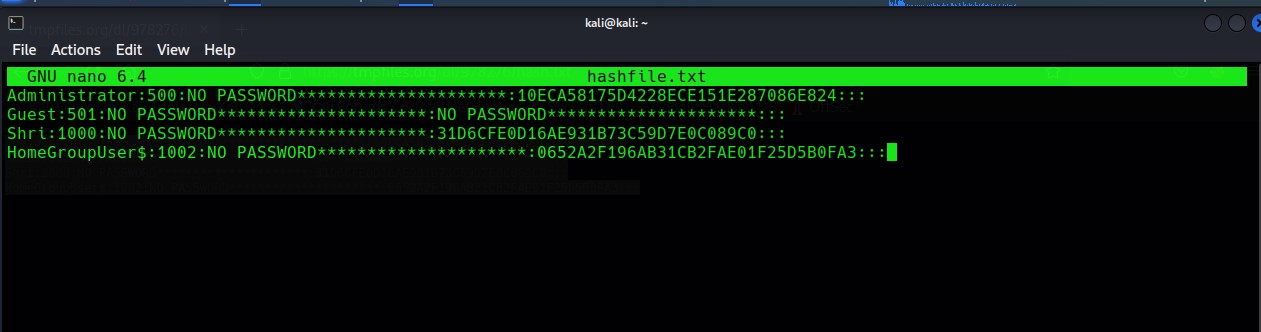
1. The file content is viewed from kali.



1. Now, create a file and copy the content into it. Using below command:

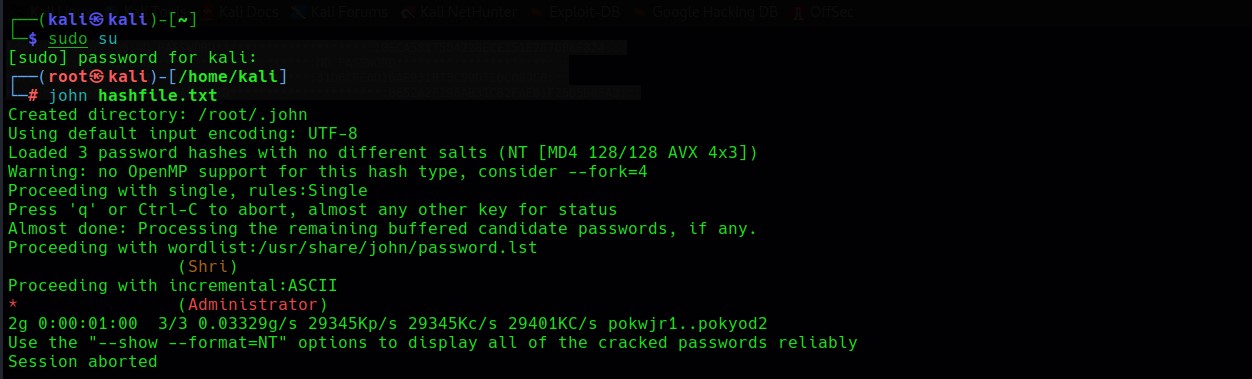
**$ nano hashfile.txt**

Now, paste content save and exit from the window.



1. To Get password of windows7 machine by below command:

**john hashfile.txt**



* 1. Password cracking of metasploit machine using Hydra

**Steps:**

1)Run the metasploitable and kali parallely.

2)create a file using nano filename command

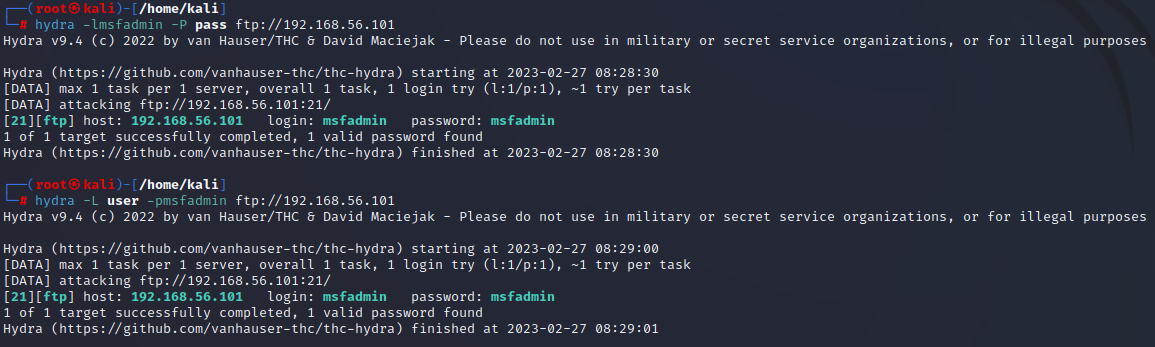
3)Use the tool hydra to know the user password and username.

Note:If we are unaware about username or password then use capital L(username) and P(password).

If we know username and unaware of the password then write the command as :hydra -lmsfadmin -P pass

If we know password and unaware of the username then write the command as :hydra -pmsfadmin -L pass

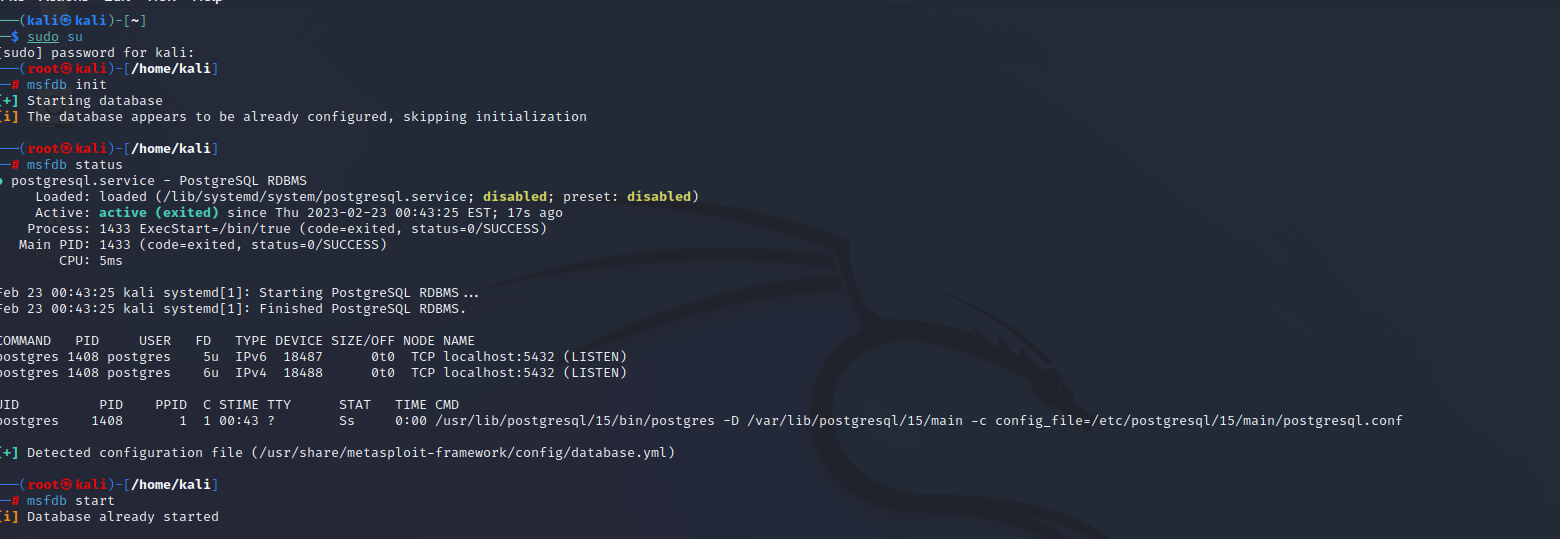




1. Perform password cracking of online vulnerable website(testfire.net) using Burpsuite
2. Perform Exploiting Metasploit
   1. Exploiting Metasploit using FTP

Steps:

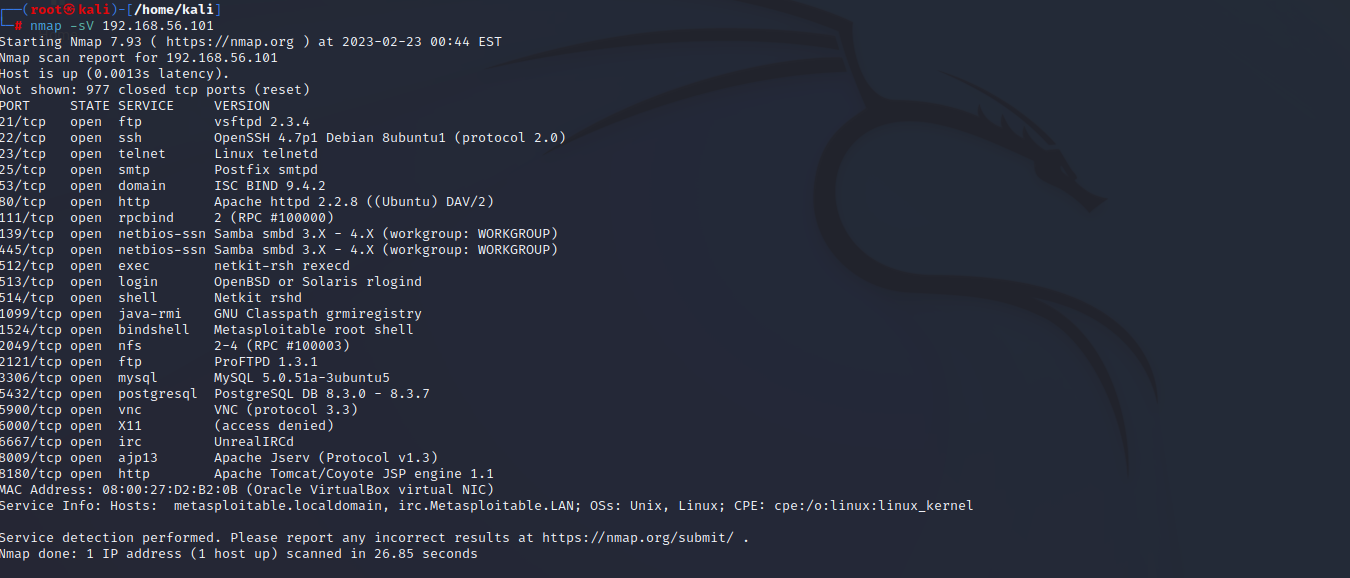
1)Login as superuser using *sudo su* command. To start the database type the command as msfdb init .To check the status type the command as msfdb status, this will say us is it active or unactive.To check database write as msfdb start.



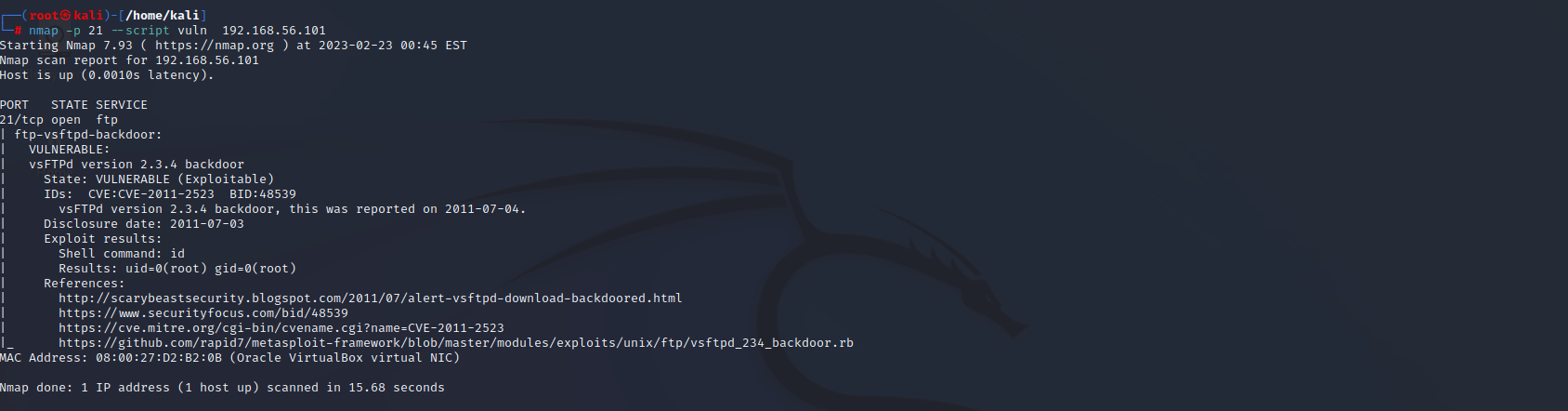
2)To scan IP address use as nbtscan 192.168.56.102/24



3)To find the version nmap -sV 192.168.56.101



4)To find the vulnerability in port 21(ftp) nmap -p 21 --script vuln 192.168.56.101



5) To enter metasploitable use the command msfconsole



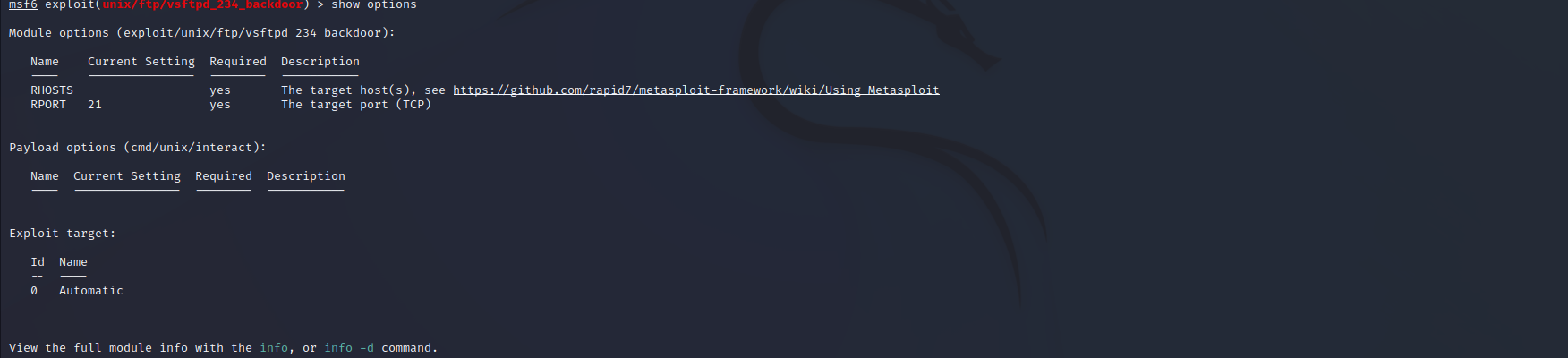
6)search vsftpd to get the matching module of vsftpd.



7)Then select the matching module and use it as use 0

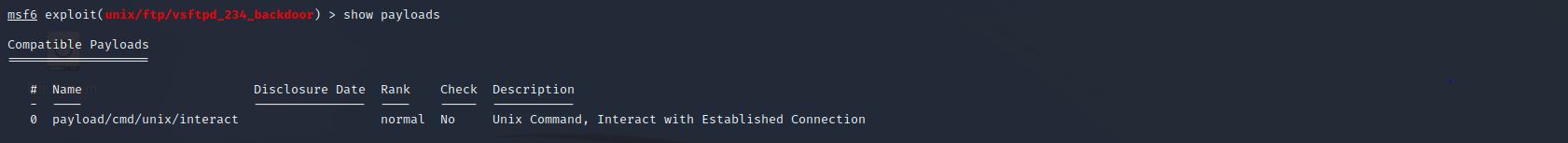


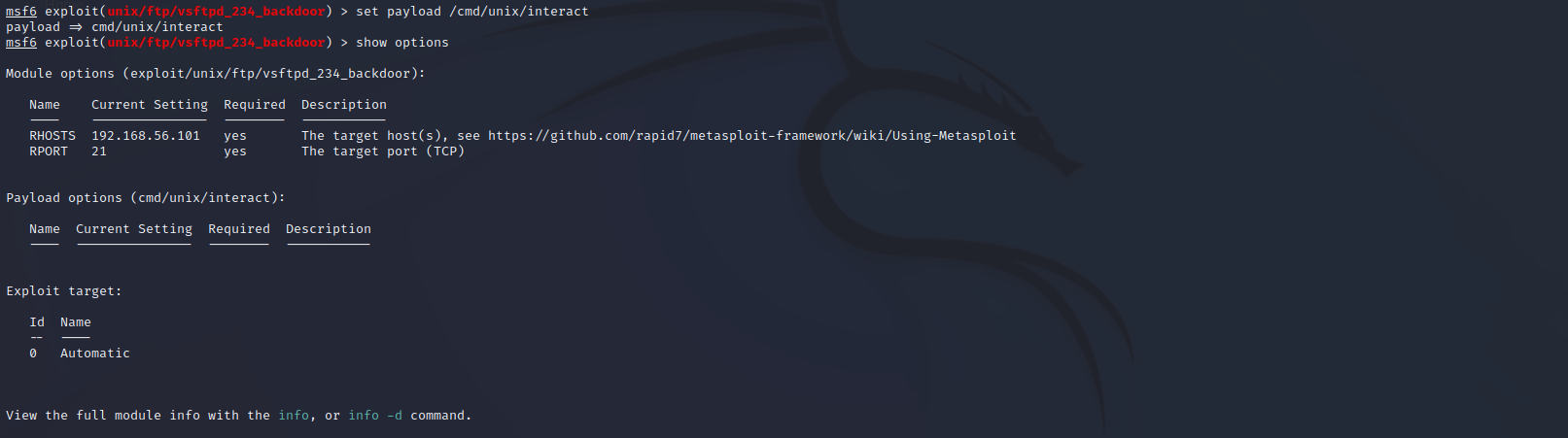
8)show options it shows all the information that is associated with matching modules.



9)Now we have to set the rhost and the payload for the exploitation as shown in the below figure. show payloads shows all the compatible module/matching module.Payload is called the heart of the metasploitable.

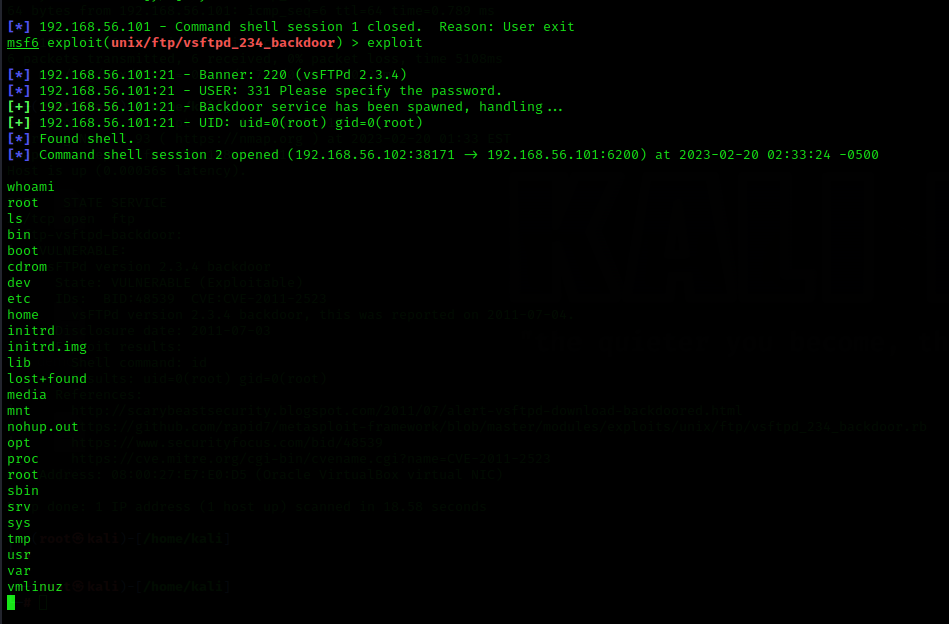






10)After that enter the command exploit. Then you will be logged to the target machines kernel.

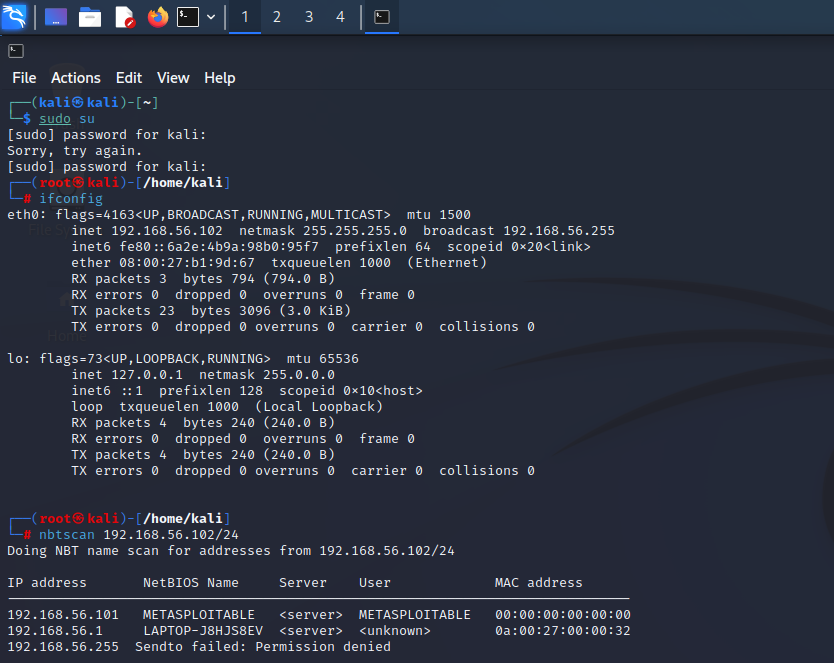
enter the command whoami to know which directory you are currently in.

****

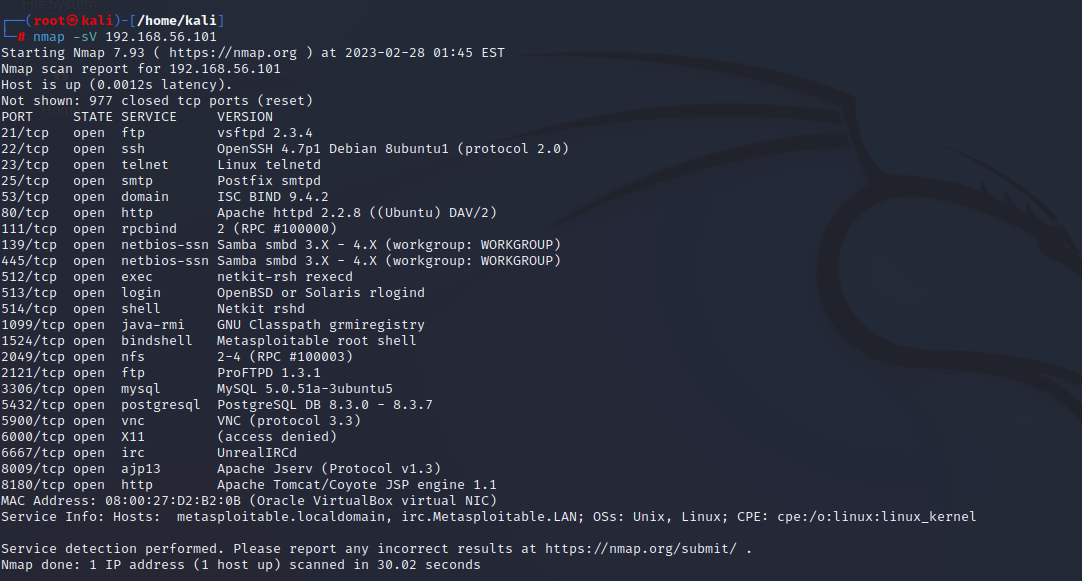
* 1. Exploiting Metasploit using SMTP

Steps:

1) Open both kali linux and the metasploitable then find the ip address of both kali linux and metasploitable machine by using the command ifconfig and using nmap tool.



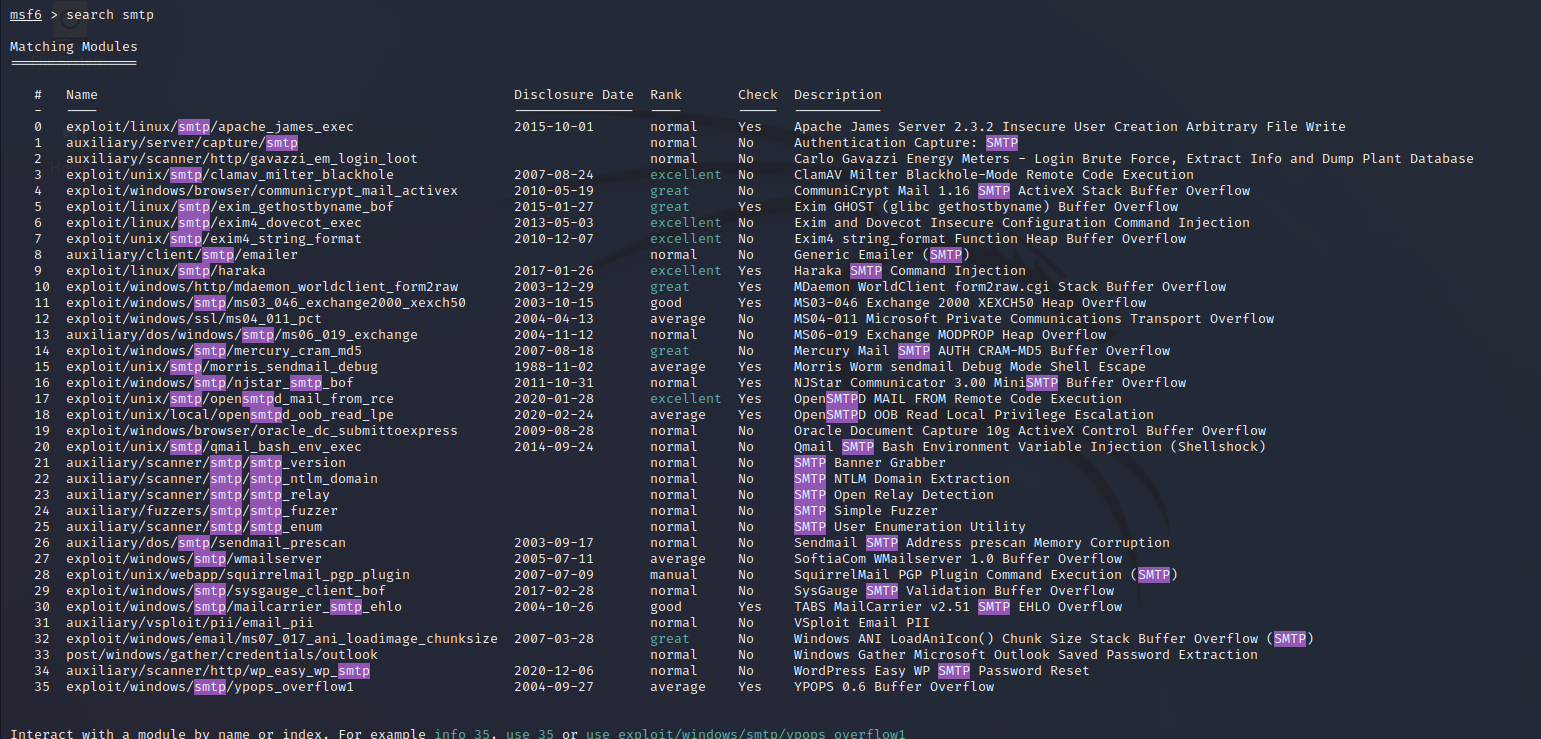
2)Then scan the port smtp for all the information by giving the command nmap – sV 192.168.56.101.



3)To enter metasploitable use the command msfconsole.



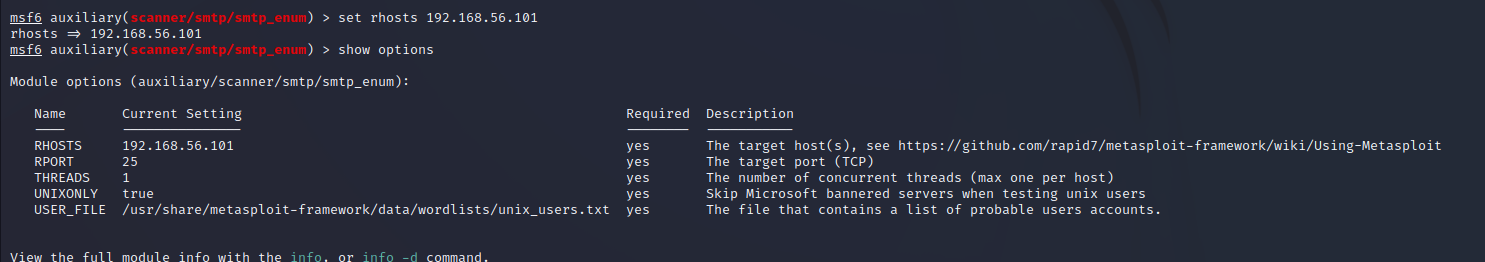
4)enter the command search smtp.



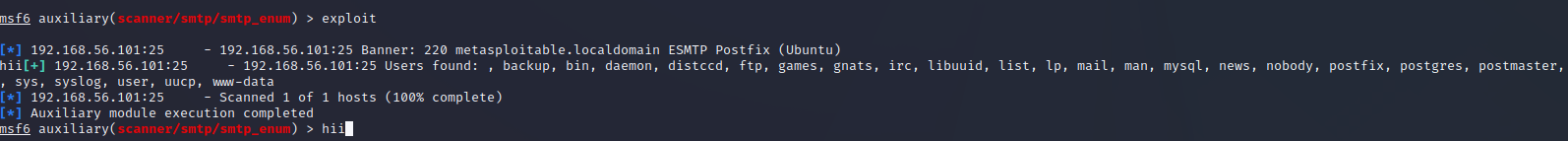
5)use the path 25 to use it use the command use 25. Which will have the path ending with smtp\_enum.



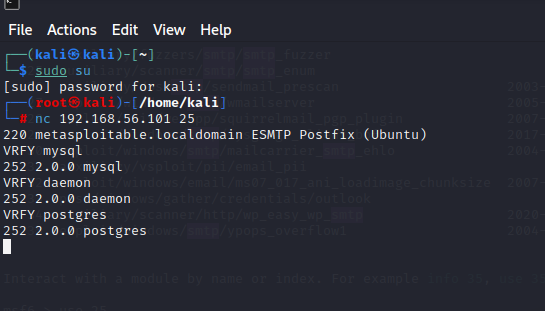
6)Now set the RHOSTS to the metasploitable ip address



7)After enter the command exploit and enter the shell.



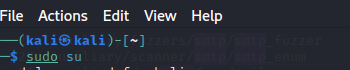
8)Open another terminal and enter the root and scan the port using the command nc 192.168.56.101 25.where nc (netcat) is used to listening &scanning the port. enter the command to verify the database using the commands VRFY mysql , VRFY daemon &VRFY postgres.

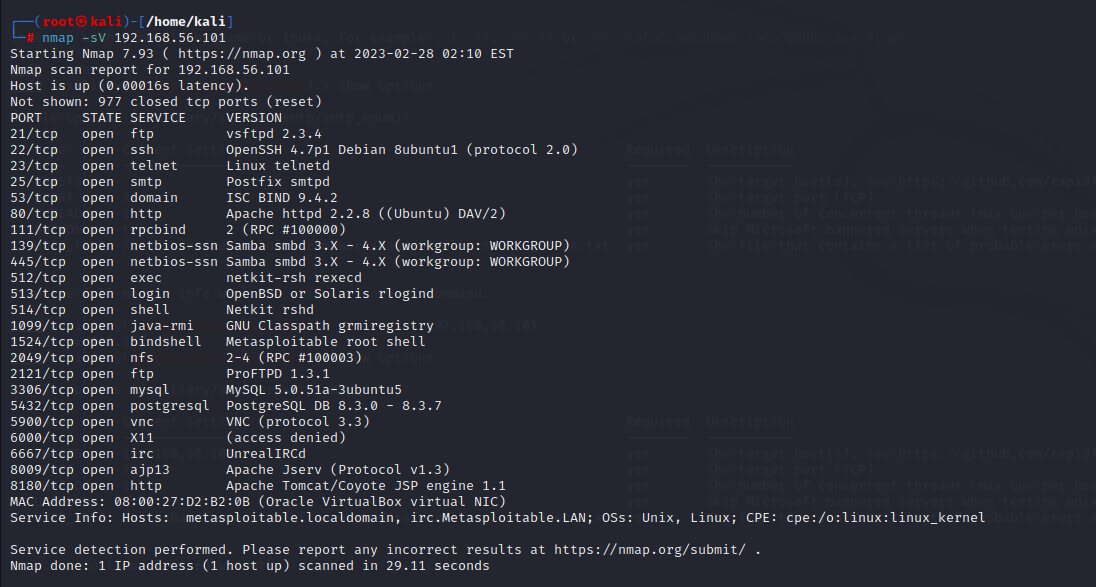


* 1. Exploiting Metasploit using Blind shell

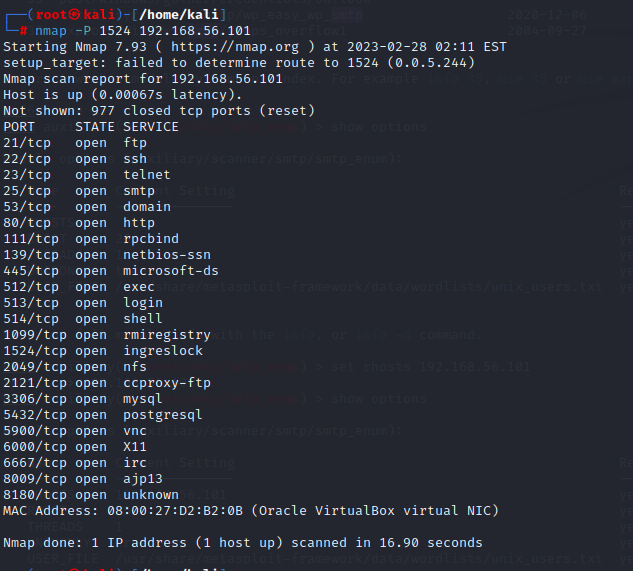
Steps:

1)Turn on the kali linux and the metasploitable simultaneously.find the metaspoitable machine IP address. Enter the command nmap -sV 192.168.56.101 to find the port number and the version of bind shell some of the cases it may be as ingreslock.

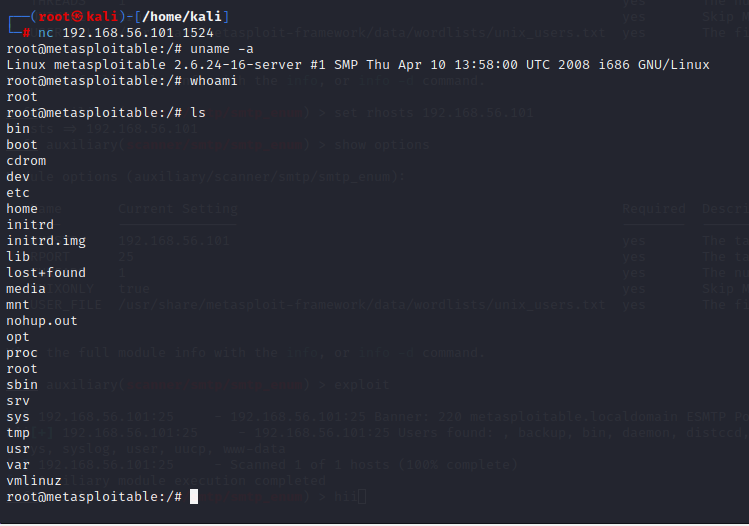




2)Enter the command nmap -p 1524 192.168.56.101 to know more vulnerabilities of the port.



3)Enter the command nc 192.168.56.101 1524 you will be inside the bindshell to know about the username use the command *uname -a* and then type *whoami* command to know the present working directory and *ls* to know the list of directories or files.



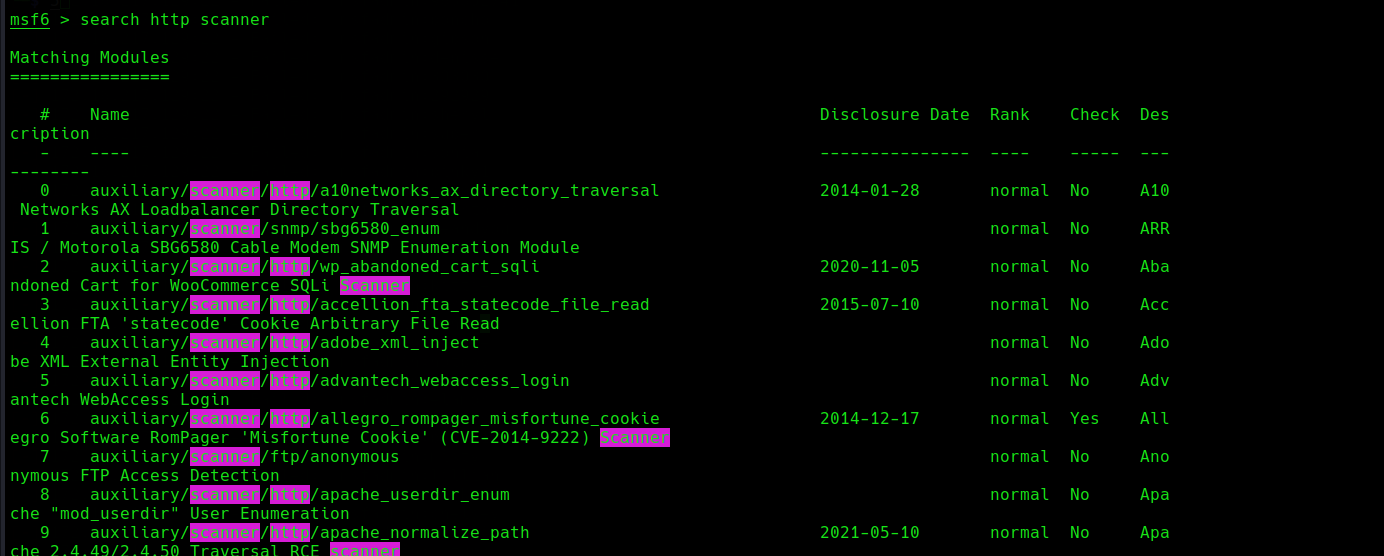
* 1. Exploiting Metasploit using HTTP

Steps:

1) Turn on the kali linux and the metasploitable simultaneously.find the metaspoitable machine IP address.Now use the Metasploitable tool and enter the msfconsole.

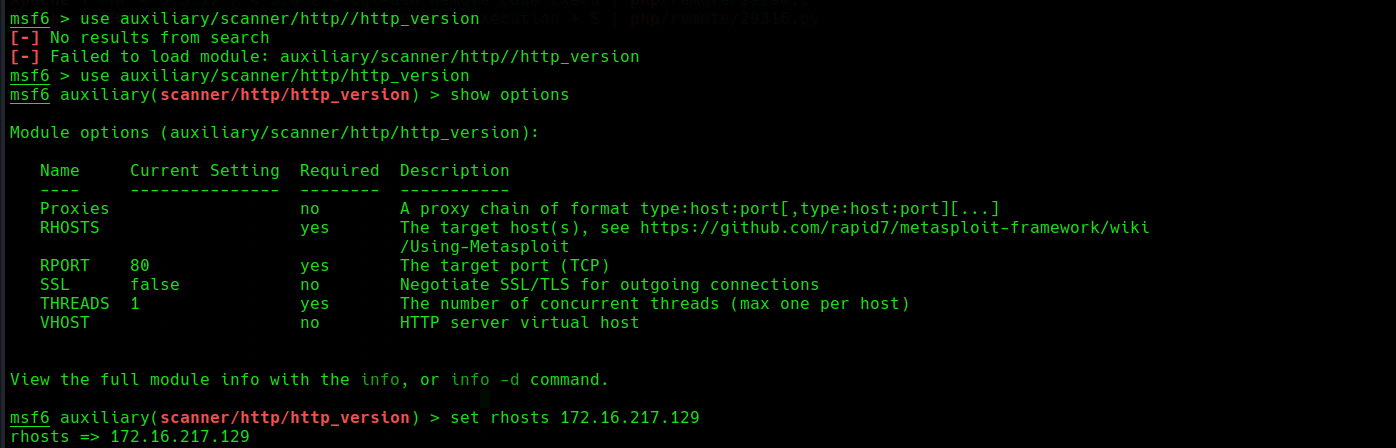


2)Enter the command as search http scanner.

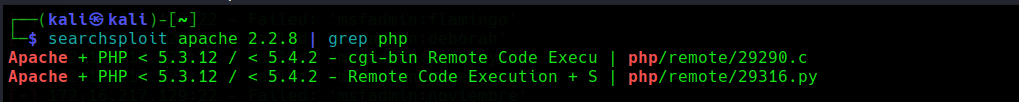


3)Now use the path as auxiliary/scanner/http/http\_version.

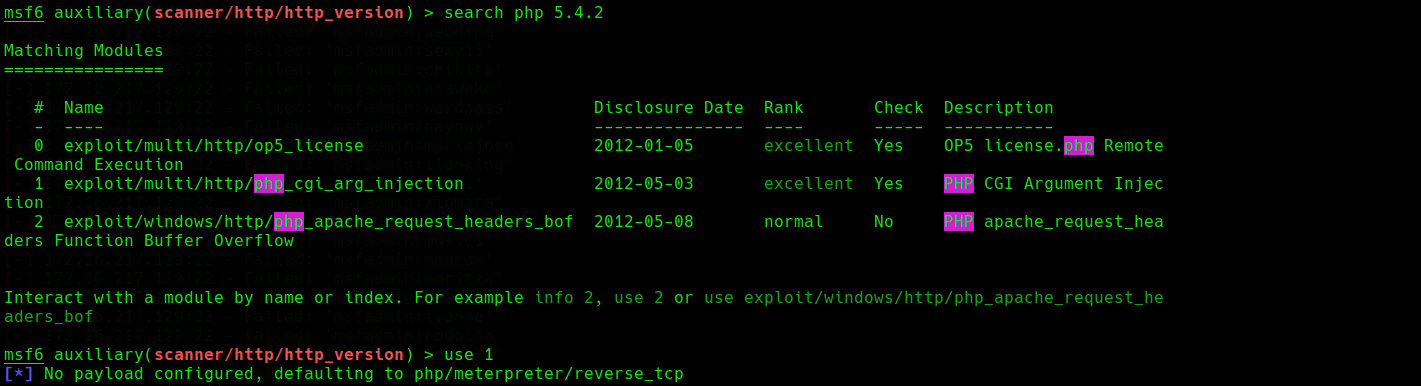
Now set the Rhosts to metasploitable IP address.



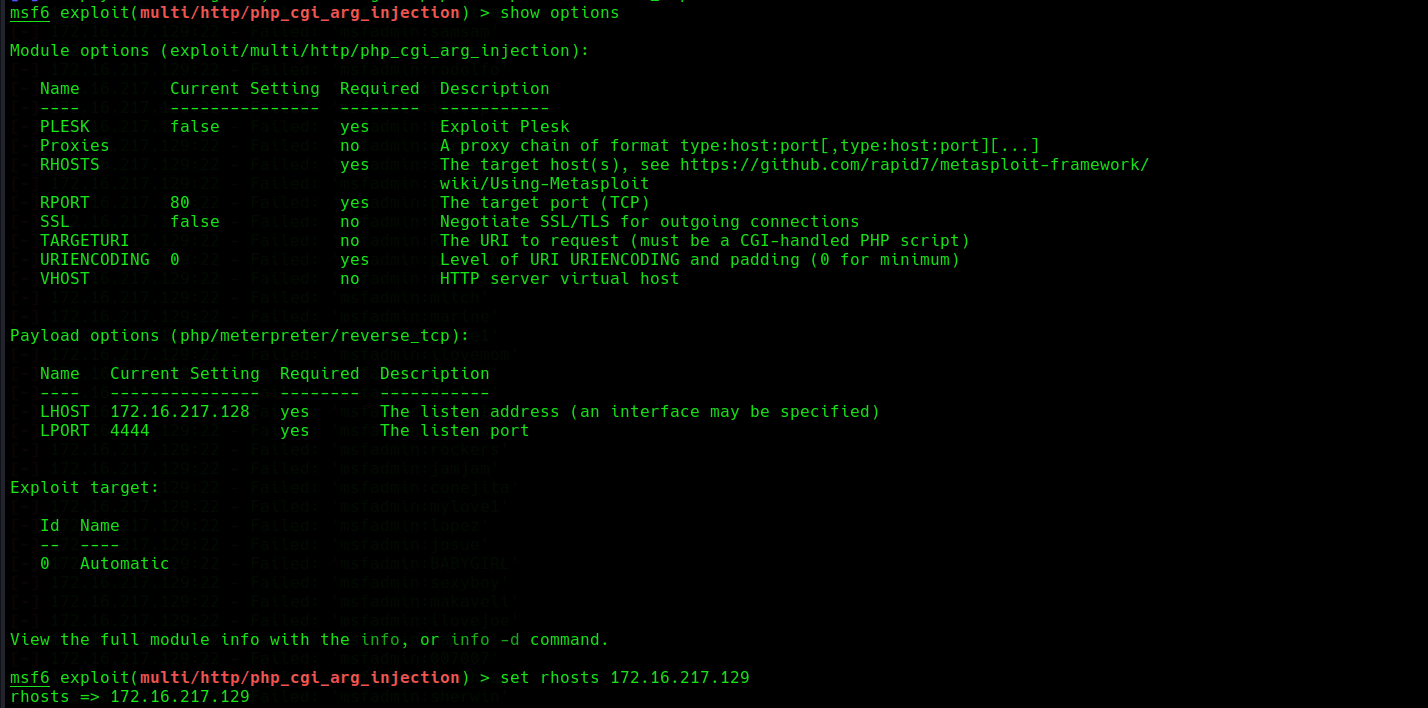
4)To find the php version we use the above command.

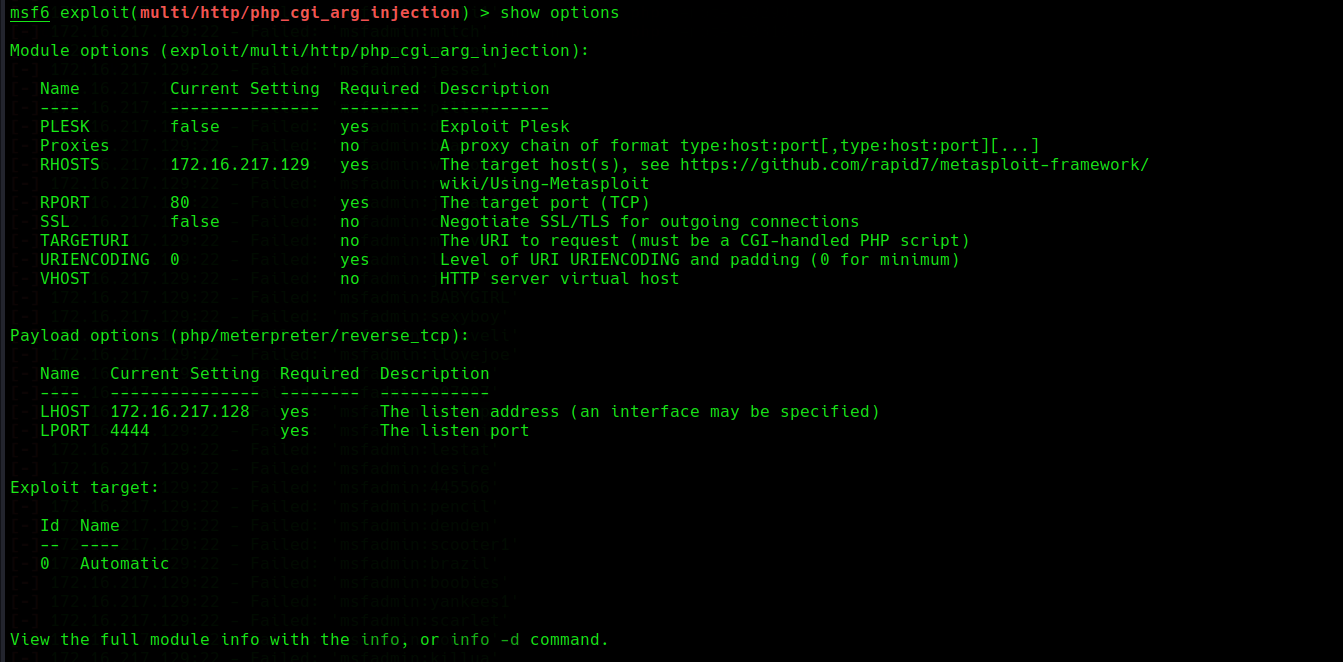


5)search php 5.4.3 will show the rank and their description of the matching module.now use 1.

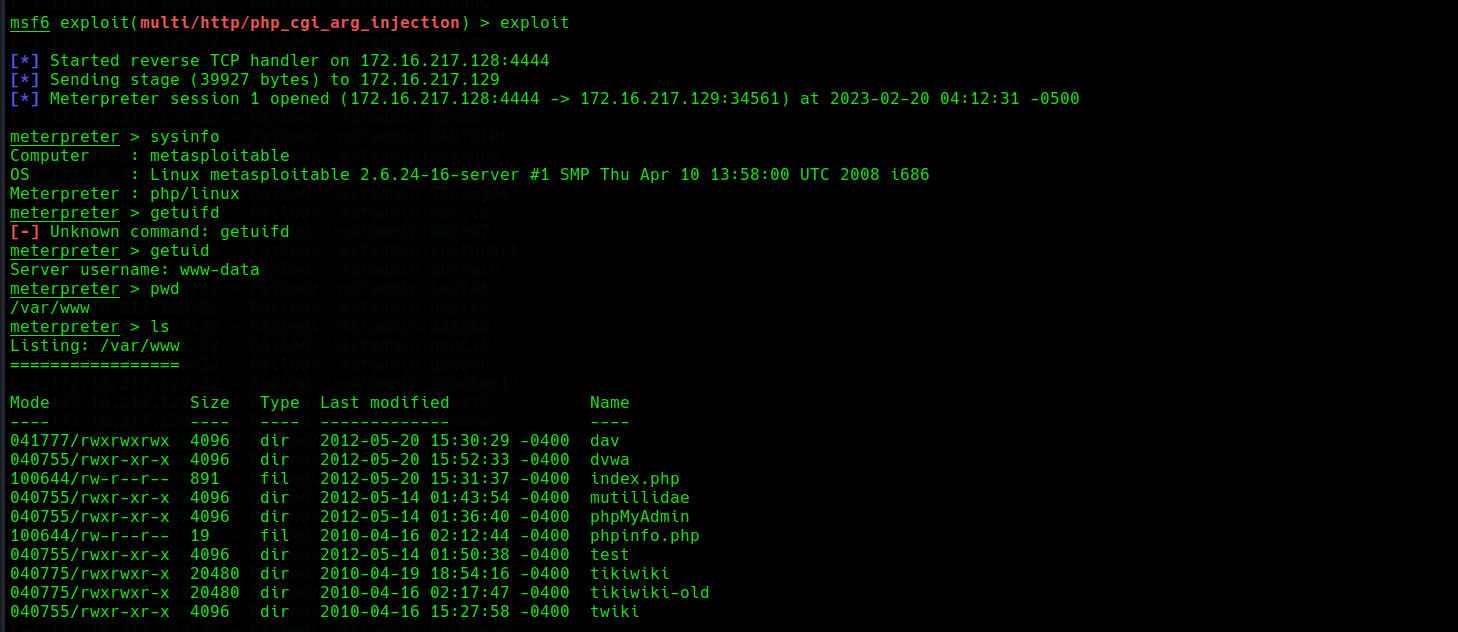


6)show options will show the module options that was present in the use 1. Now set the Rhosts to metasploitable IP address.





7) After that enter the command exploit.



1. Perform Network scanning using following nmap commands:
   1. nmap -p
   2. nmap -sV
   3. nmap -sT
   4. nmap -O
   5. nmap -A
   6. nmap –Pt
2. Networking project on Fire extinguisher using cisco packet tracer.

**Group2:**

1. Perform exploiting DVWA
2. Perform SQL injection on DVWA
3. Perform Cross-site scripting on DVWA
4. Perform File upload DVWA

2. Perform Sniffing

1. Perform Sniffing using Wireshark in kali linux
2. Perform Sniffing using Ettercap in kali linux

**Group3:**

1. Perform malware attack using msfvenom

2. Perform footprinting and reconnaissance using following websites.

1. Netkraft
2. Google dorking
3. Whois
4. Builtwith

**Other instructions:**

* Offline Report Start date: 2nd March 2023, End date: 15th March 2023, Final report should be submitted by March 15th 2023.
* Along with Internship Report, students need to complete technical blog and also share Github repository link.
* Keep the documents in your respective google drive and send the drive link to [arun\_vr@dlithe.com](mailto:Arun_vr@dlithe.com), [chaitra.b@dlithe.com](mailto:chaitra.b@dlithe.com) [,vijay.gh@dlithe.com](mailto:,vijay.gh@dlithe.com)
* Mention email subject line as: DLithe Cyber Security Internship Report - Full Name - USN - Feb 2023.
* In case of any technical queries, please be free to chat in the WhatsApp group / google classroom.