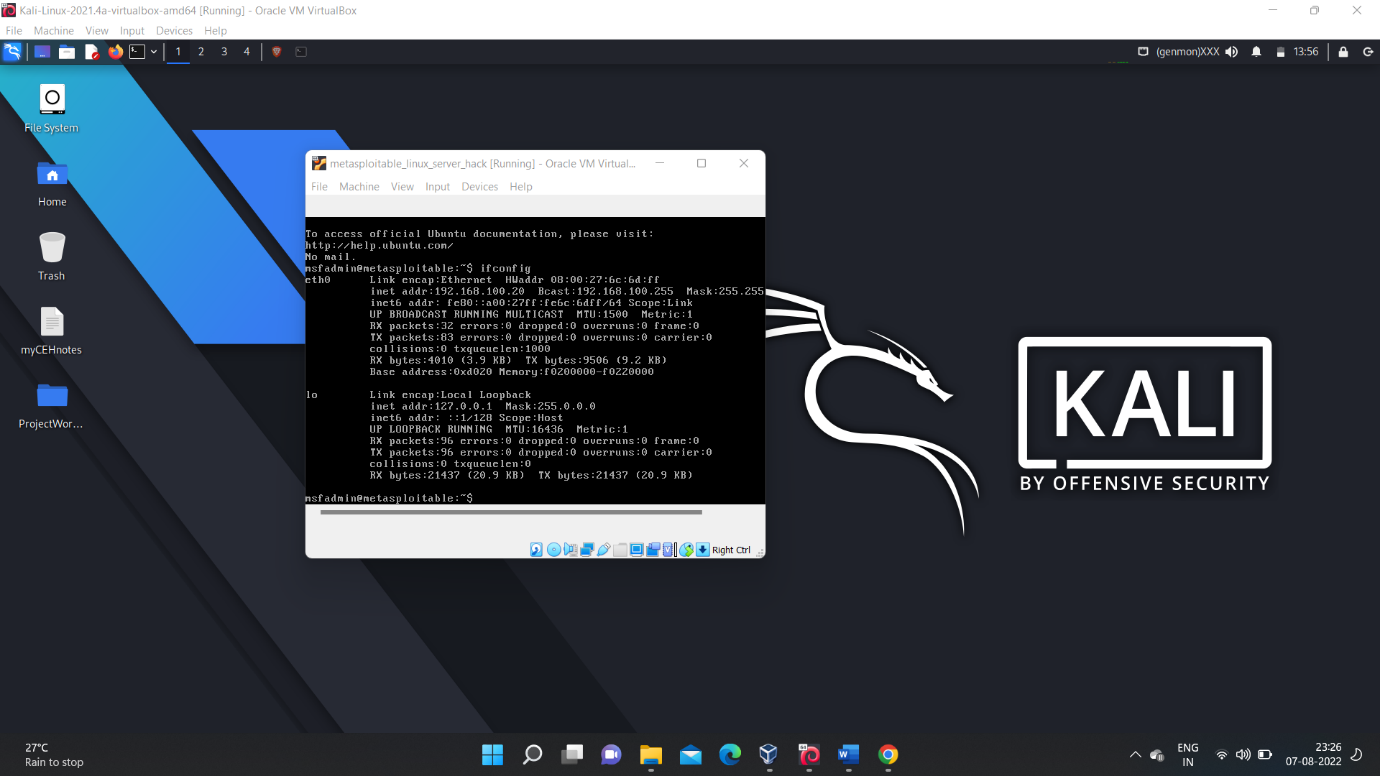
Project\_2

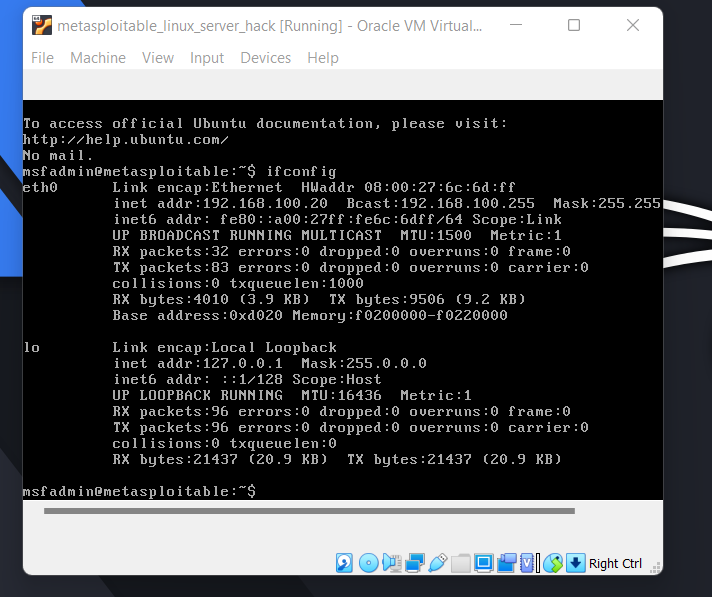
* *Introduction*
* The project is about scanning for the open ports and attacking them .
* *Steps involved*
* Login to Metasploit and extract Ip address.
* Do nmap scanning on the Ip, extract open port and version details.
* Checking the vulnerable version exploitation’s procedure in rapid7 and start exploiting the ports.
* *Exploitation*

1. *Telnet Exploitation*

* Start running kali linux and metasploitable linux
* Find the Ip of metasploitable linux machine using the command

$ ifconfig

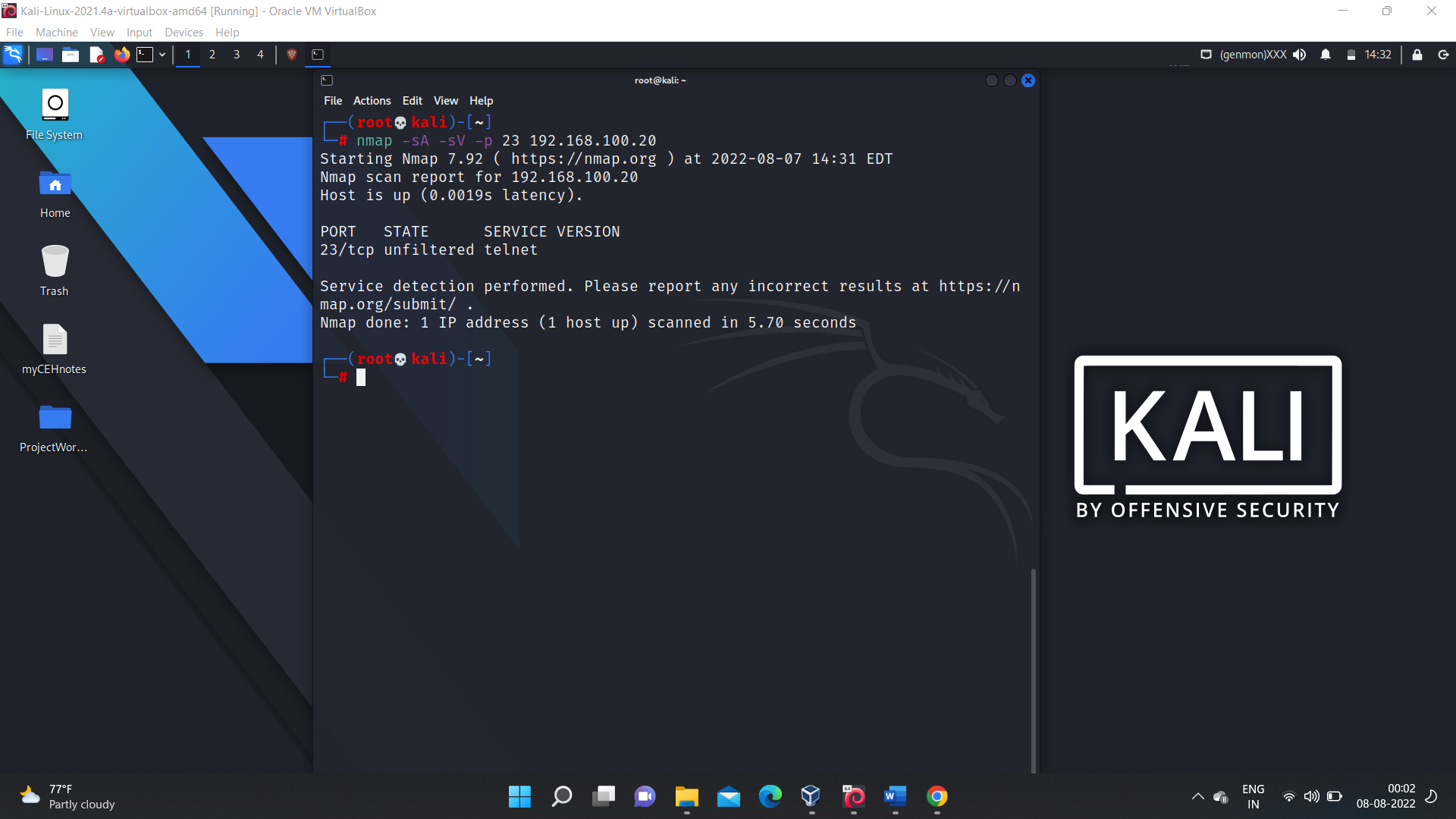




🡪 Then after finding the Ip address ( let say in our case it is 192.168.100.20) then open terminal and then perform nmap scan on the “telnet port” i.e port number 23 to find the version details.

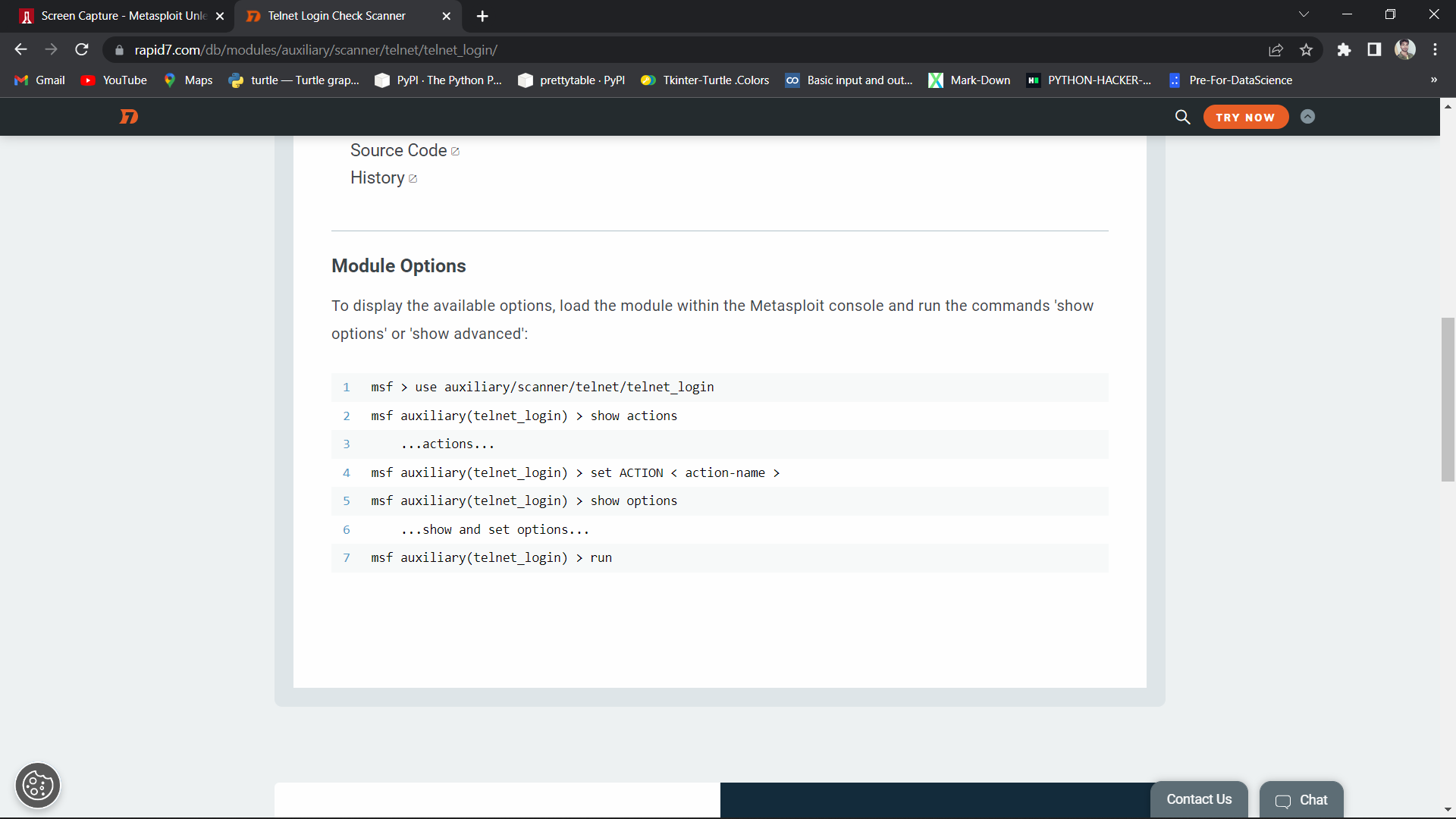
🡪 Nmap command :-

$ nmap -sA -sV -p 23 192.168.100.20

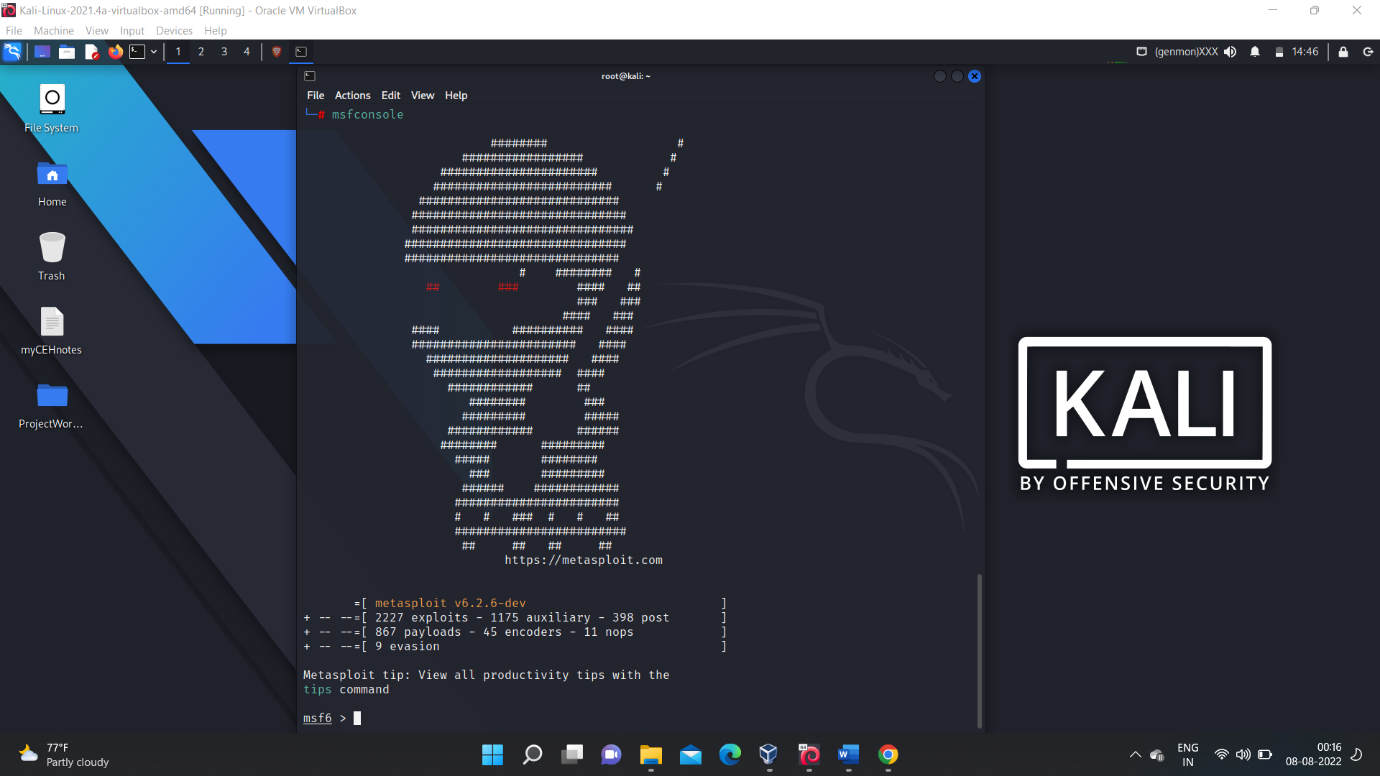


🡪 Then search for the “telnet exploit” along with its version which we found by the nmap scanning.

🡪 From the search results we found “rapid7” website it contains an steps to exploit.



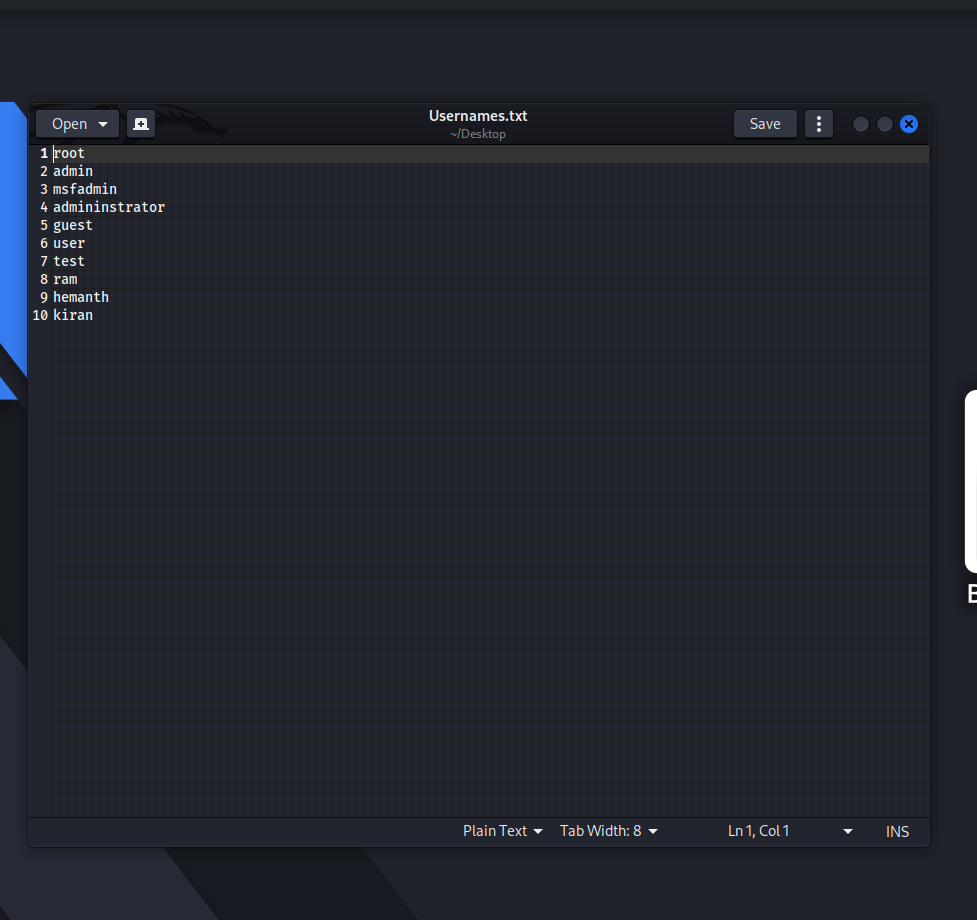
🡪Then using the linux terminal get into the “msfconsole” i.e the metasploitable frame work ,then use the commands given in rapid7 to load the modules in the msfconsole and exploit step by step.



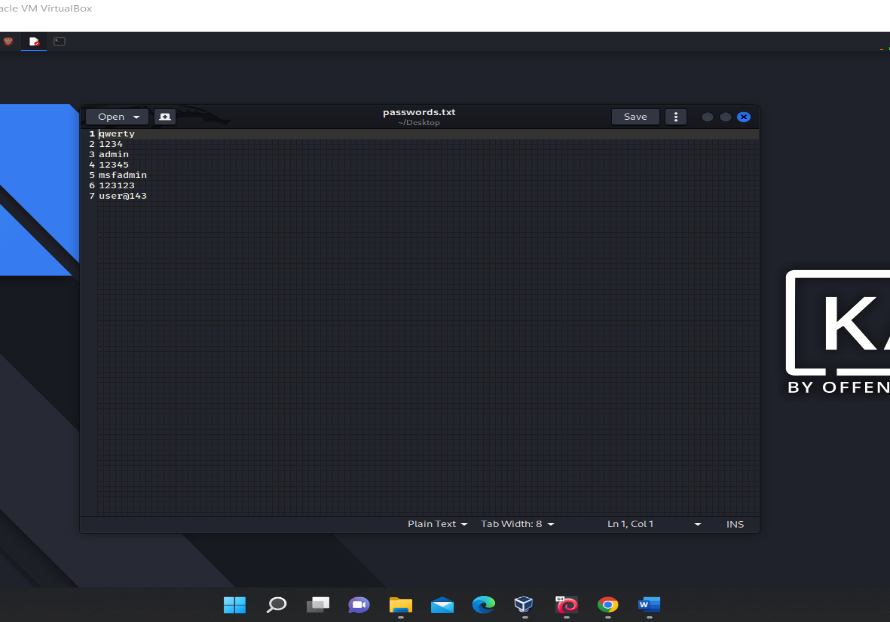
🡪 In this exploitation process we are doing an “brute force” attack and it needs an “username file “ and “password file”.

🡪 In our case we stored some “user names” and “passwords” in text files and we loading it into the msfconsole.

🡪”username” file



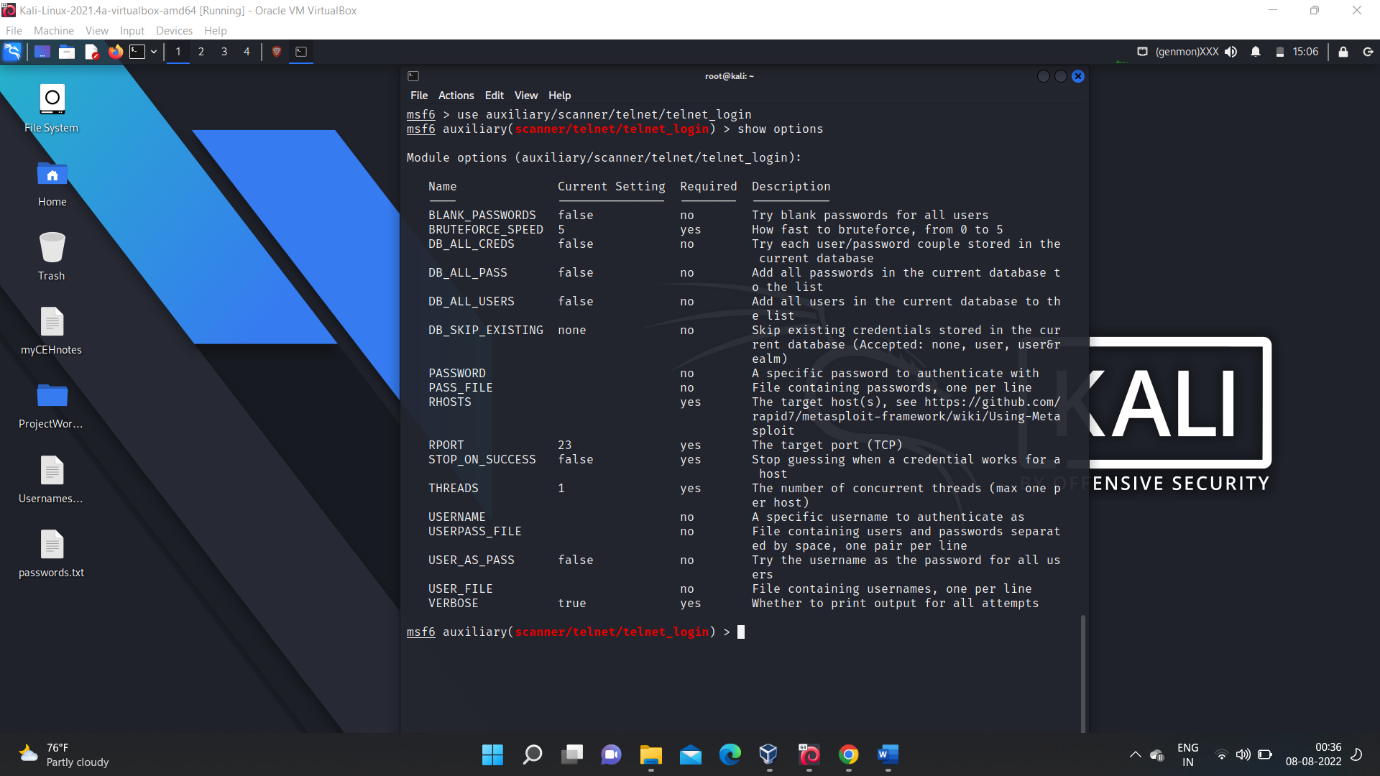
🡪”password” file



🡪Then on getting into the msfconsole and loading the auxiliary module which is given in the steps of the “rapid7.com” website and then using the command

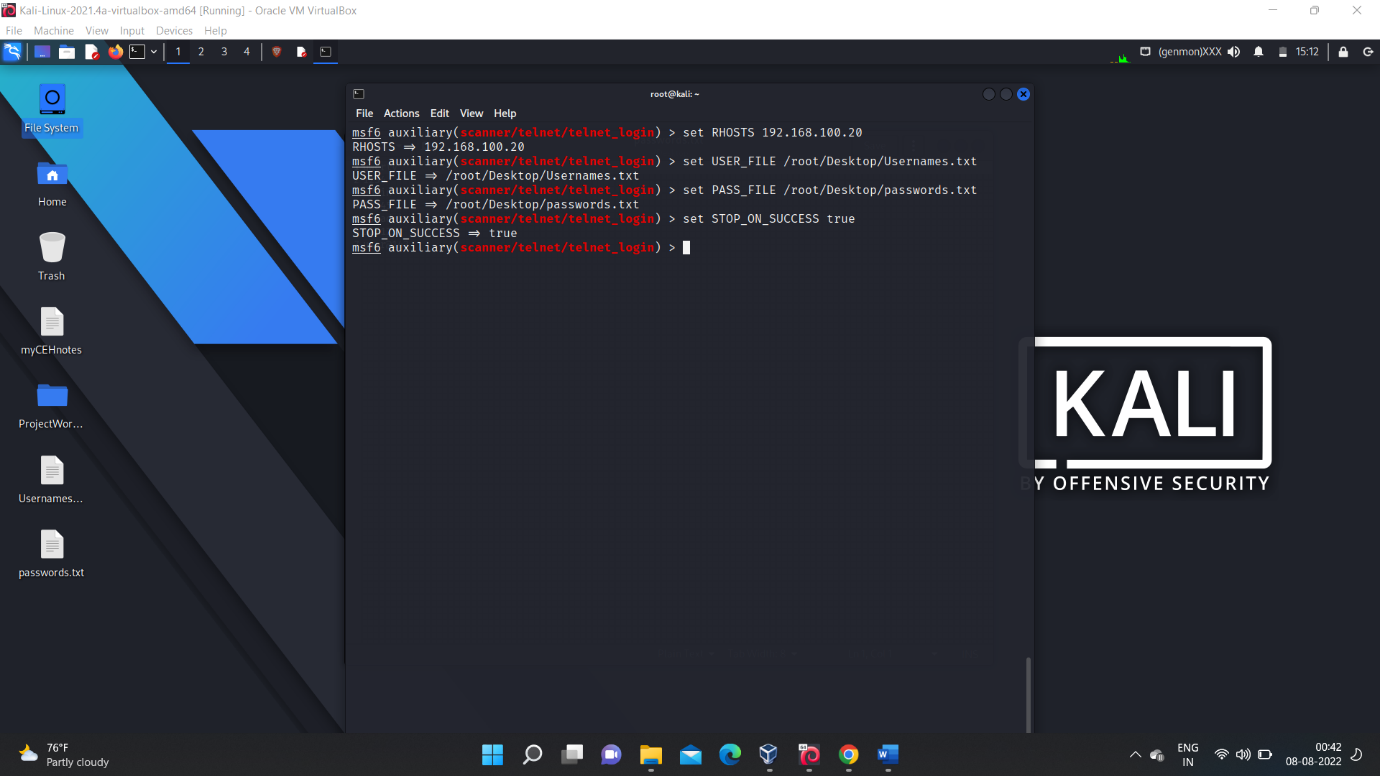
$ show options

* It gives the detailed view of how to use the options in that specific loaded module.

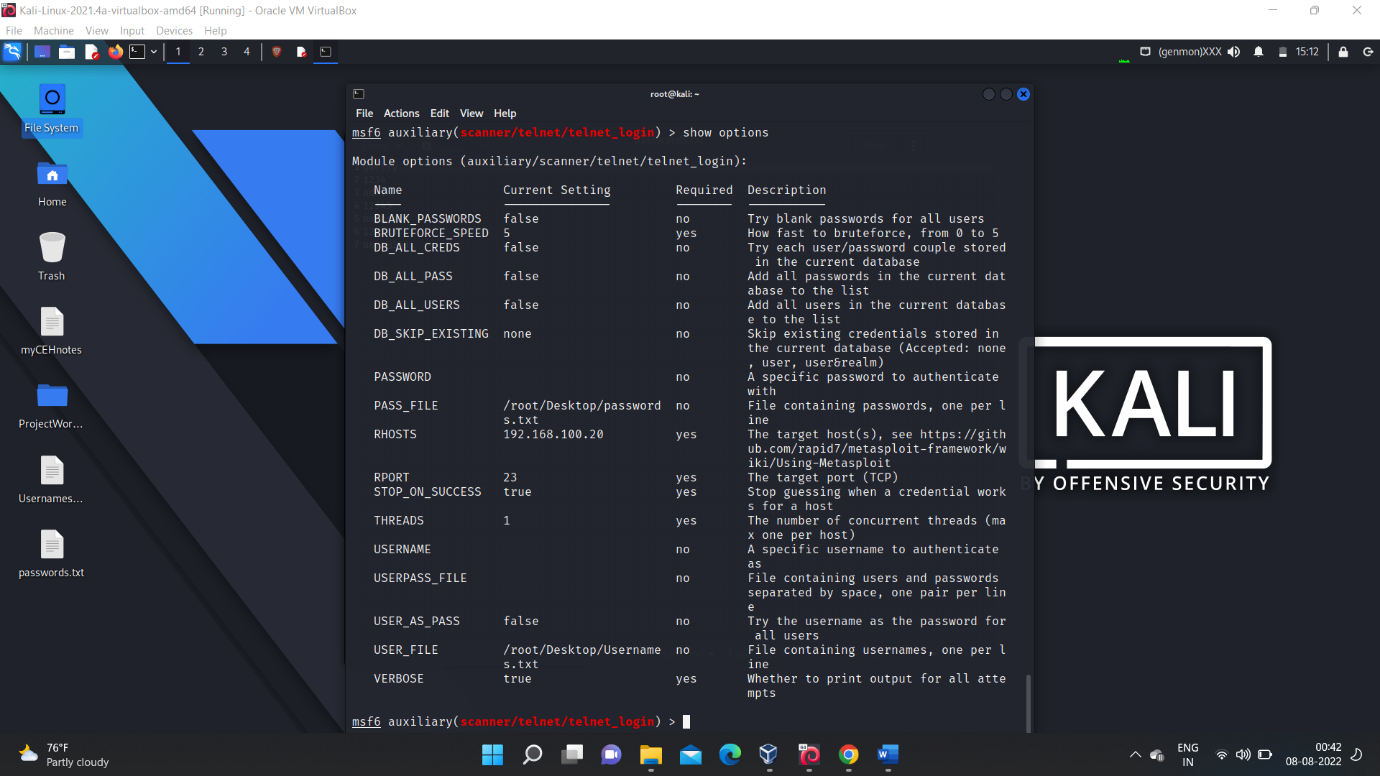


🡪Then set the “rhost” address as the target Ip, In our case it is the Ip of metasploitable linux i.e 192.168.100.20

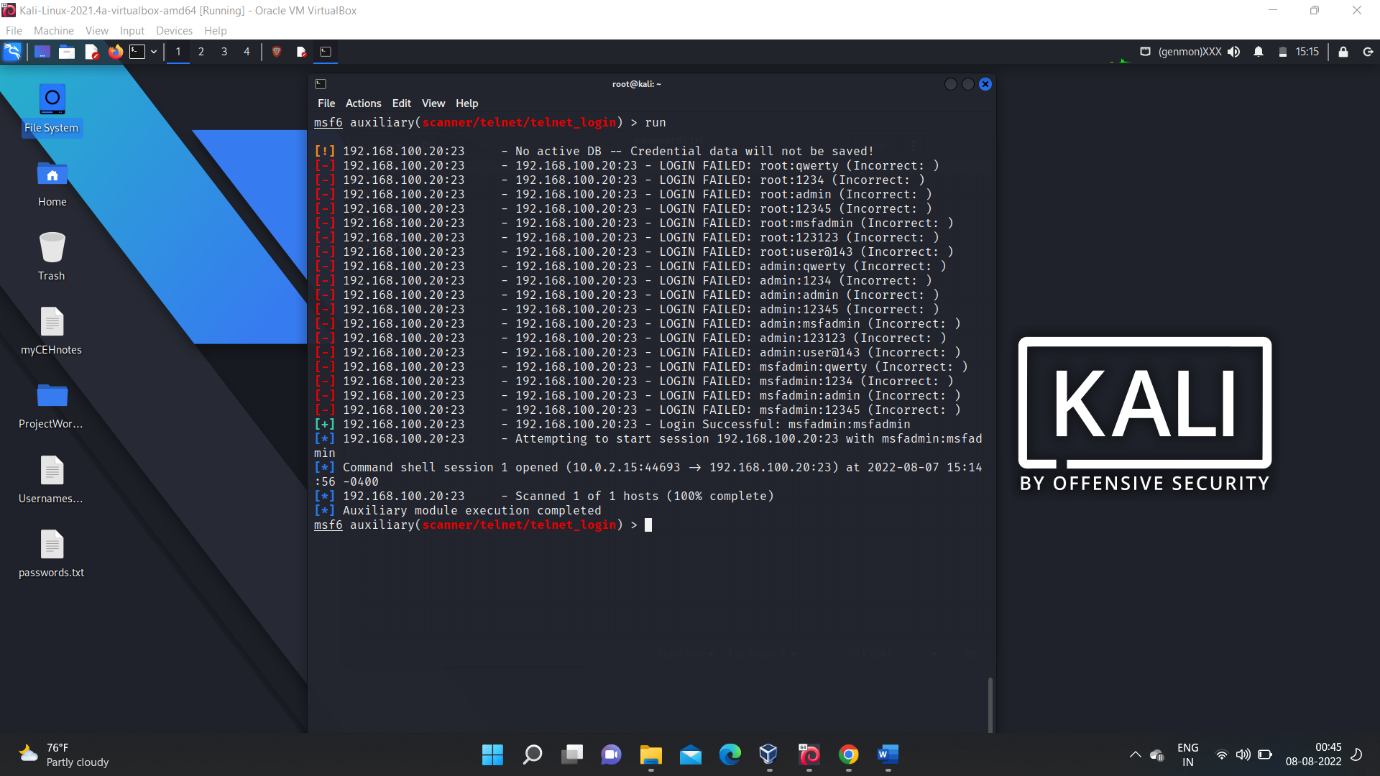
🡪Then load the “username “ and “password” file and set STOP\_ON\_SUCCESS value “true “ , for stopping the exploitation when we found the login.



🡪 after setting the options then it look like this.

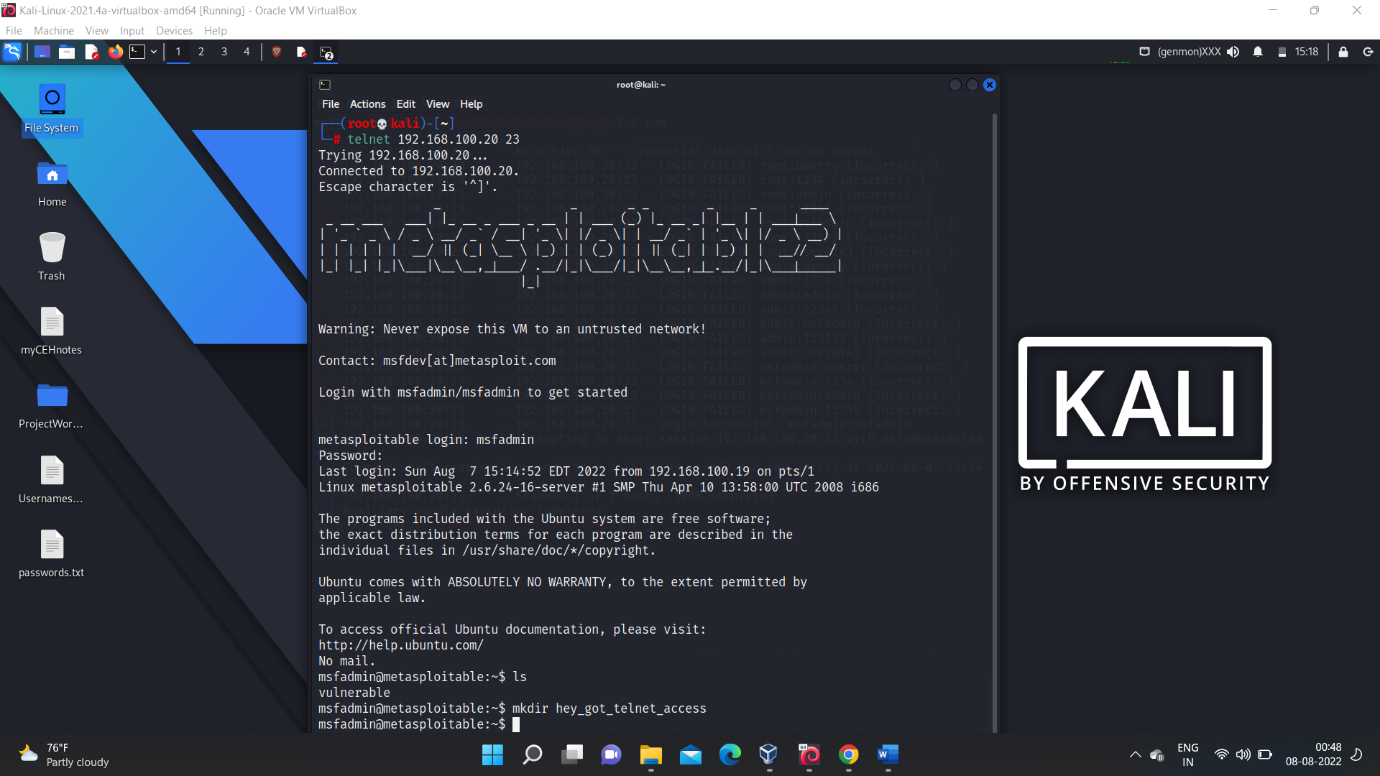


🡪Then on executing the command $ run , the exploitation starts .

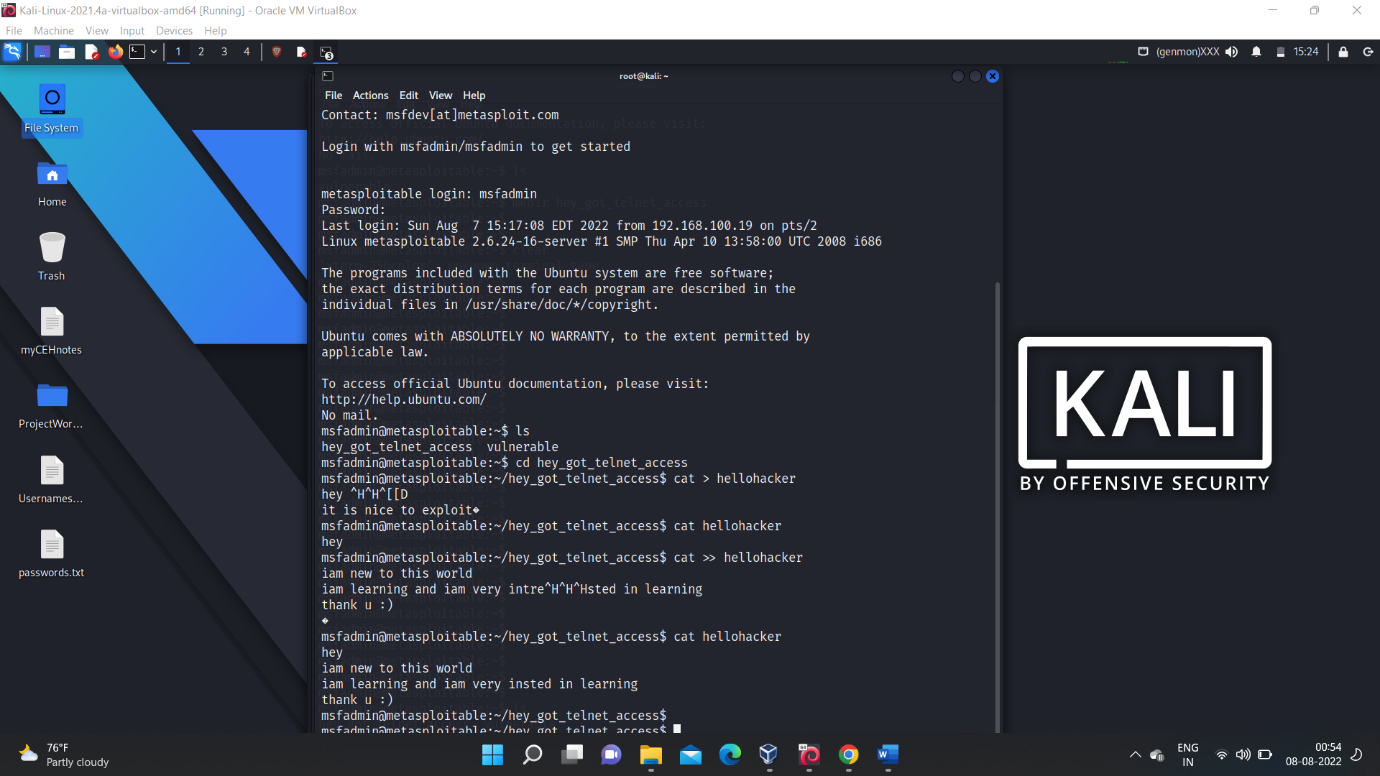


🡪Then after getting the login credentials ,we can login into the metasploitable linux machine using “telnet”

* The command is : $ telnet target\_Ip telnet\_portnumber

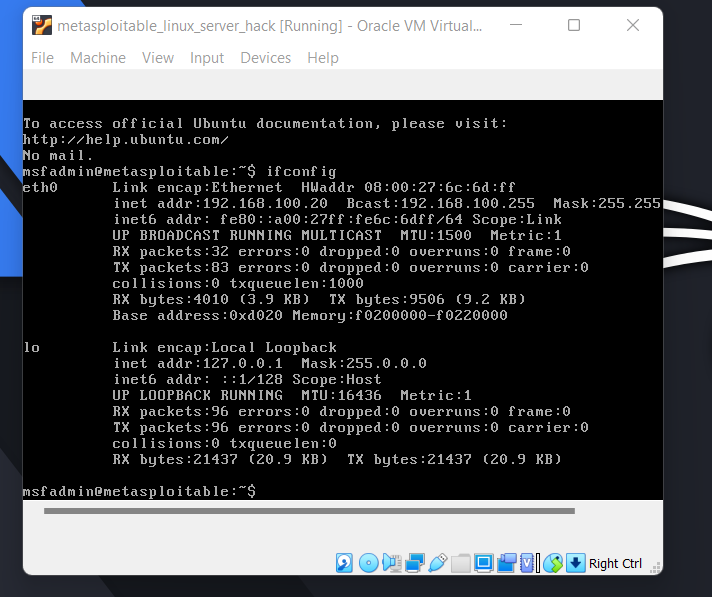


🡪Then we get access then we can do any operations like creating files, deleting files etc.

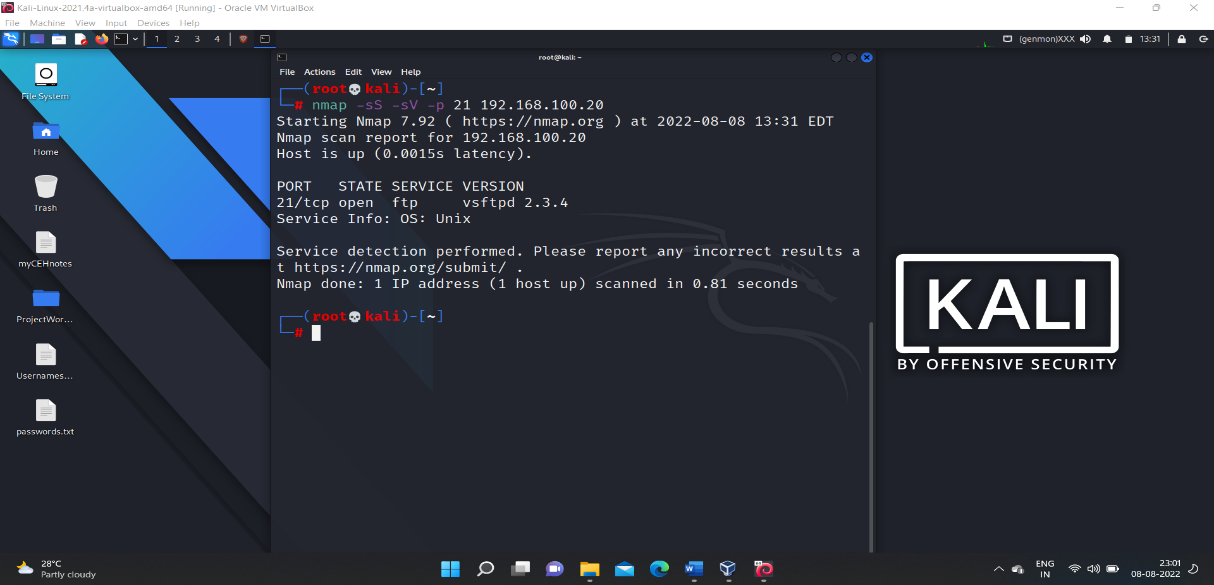


1. **FTP :**

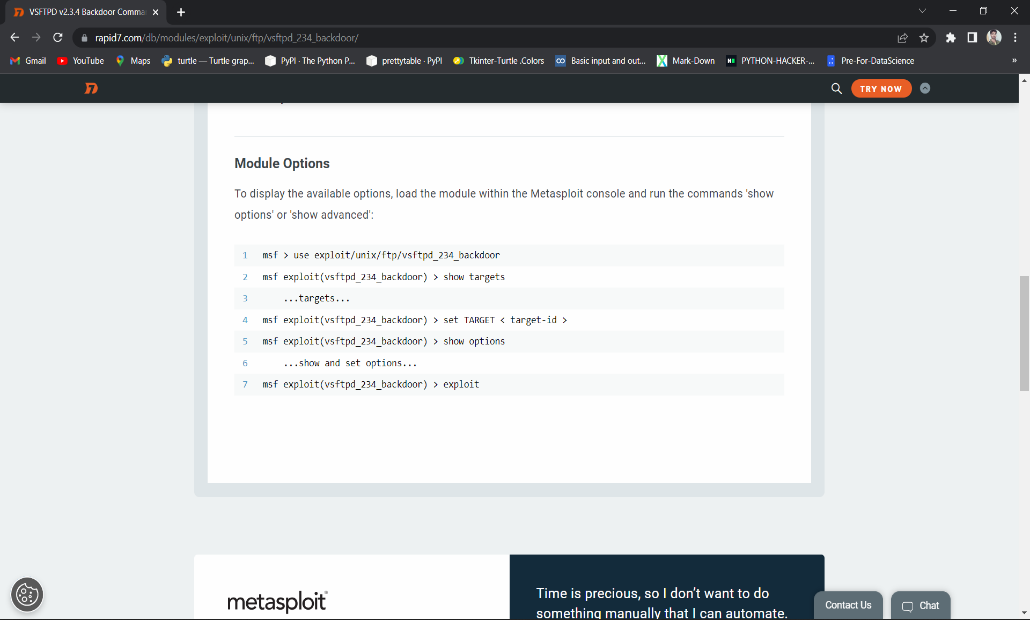
* For ftp exploitation also the steps are almost same
* Finding the target machine Ip and version of the ftp using the Nmap scan.
* In our case the target machine is our metasploitable linux machine.



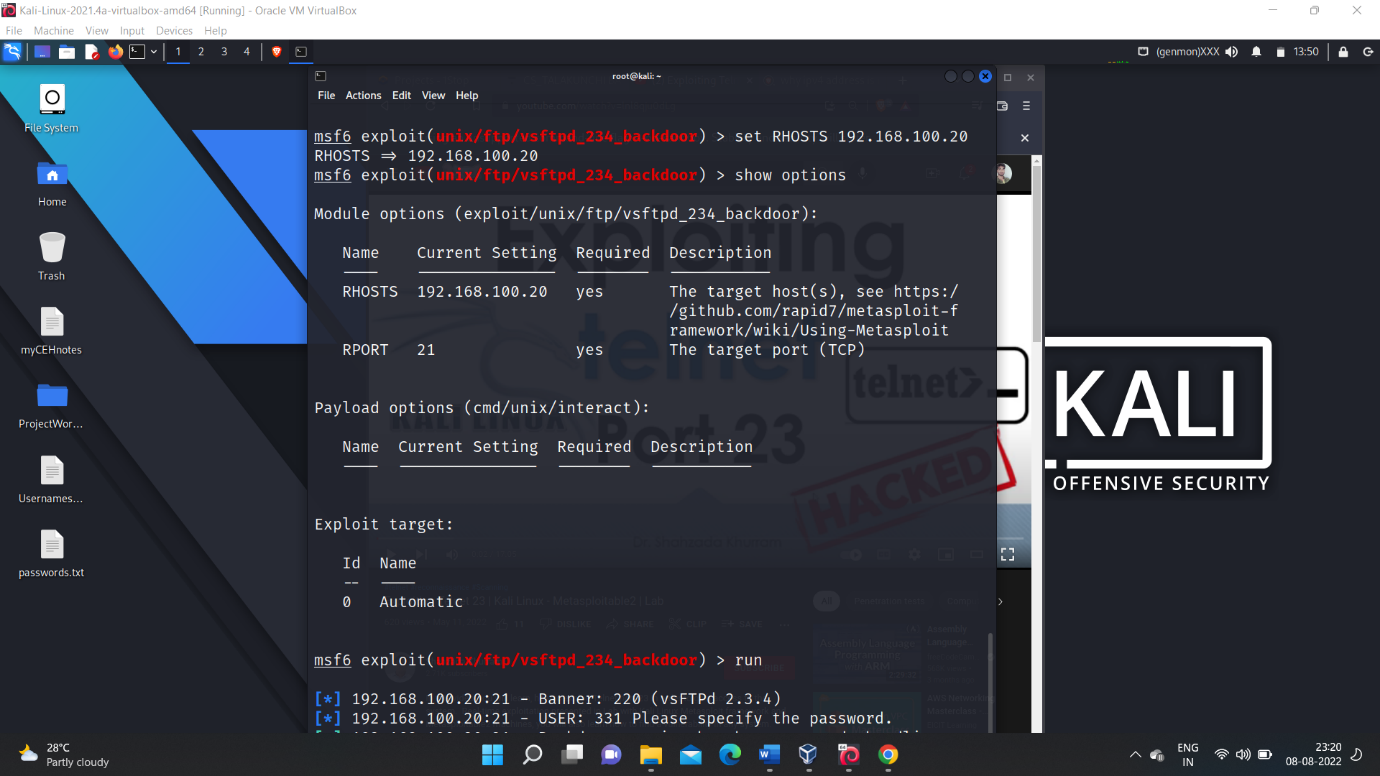
🡪Nmap scanning details of the ftp port .



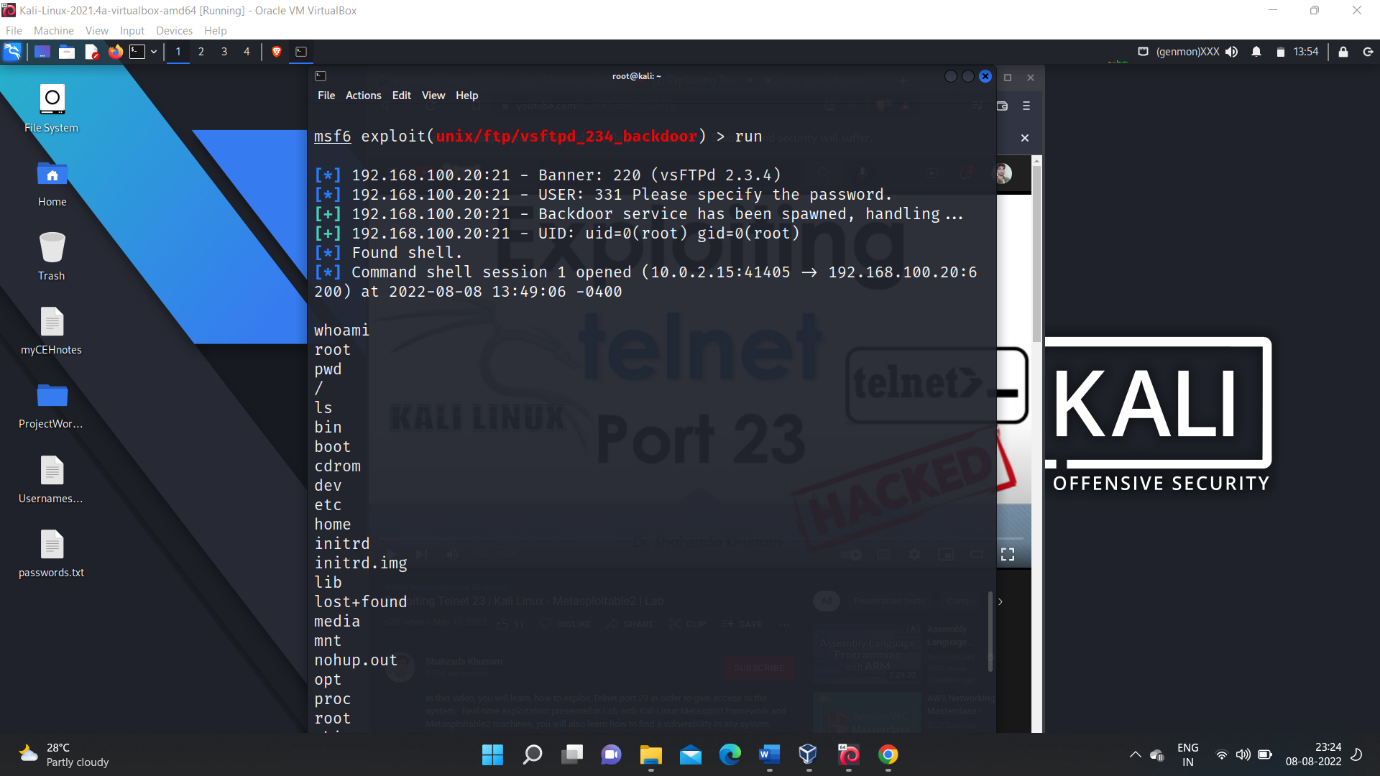
🡪Then exploiting the find out version using the commands found In the rapid7.com.



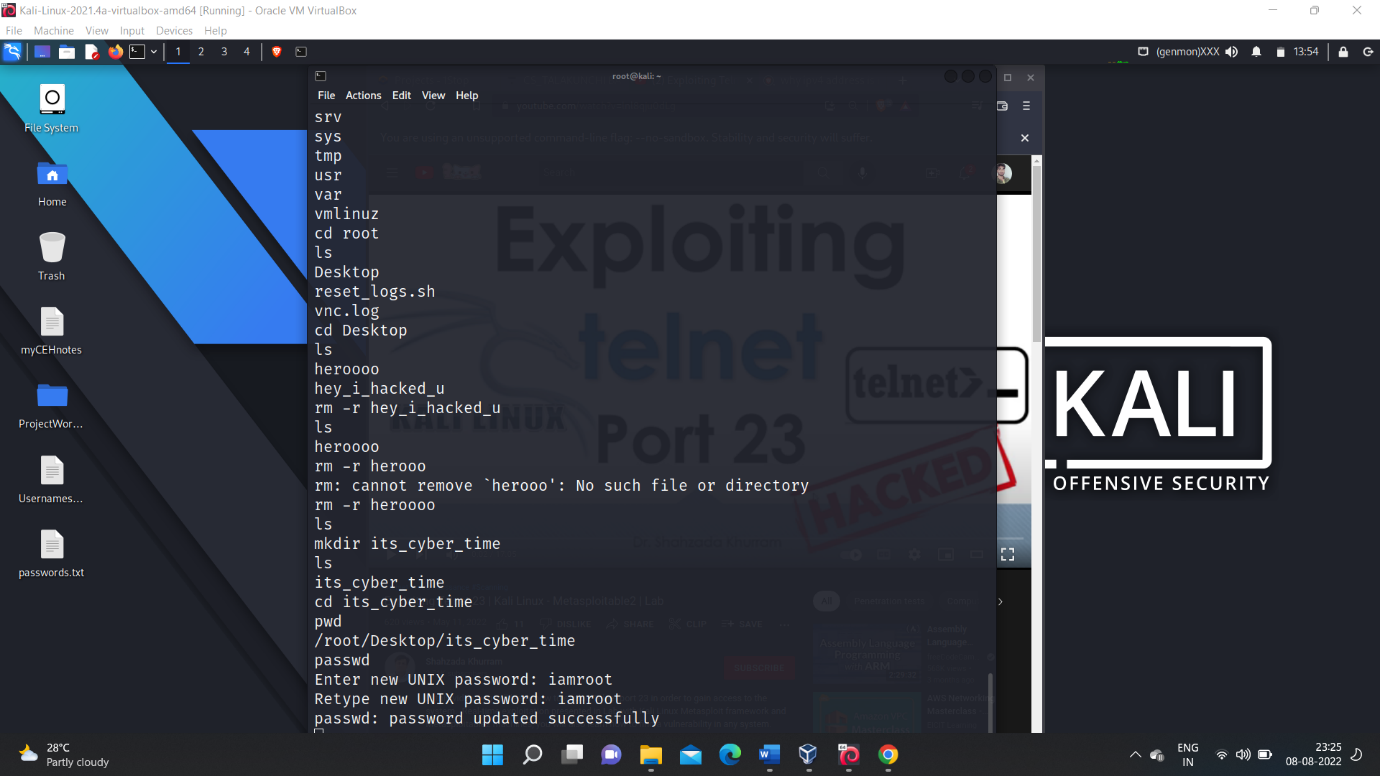
🡪Then getting into the msfconsole and loading the auxiliary modules and setting the target Ip in RHOST given in the exploitation instruction in rapid7.com



🡪After exploitation we get into the session then we can perform any actions we can get full control of the exploited user in our case it is “root”.

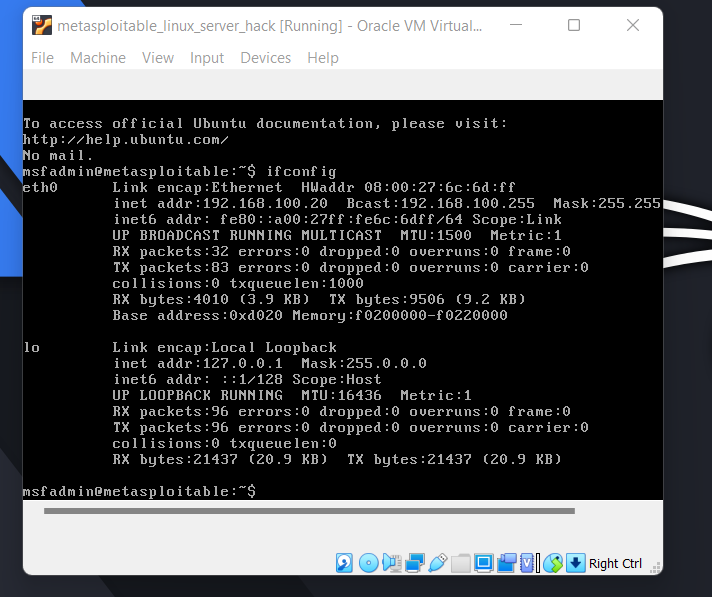


🡪Multiple actions that I performed are shown In below screenshot which include creating and deleting files and folders and even password change for the root account.



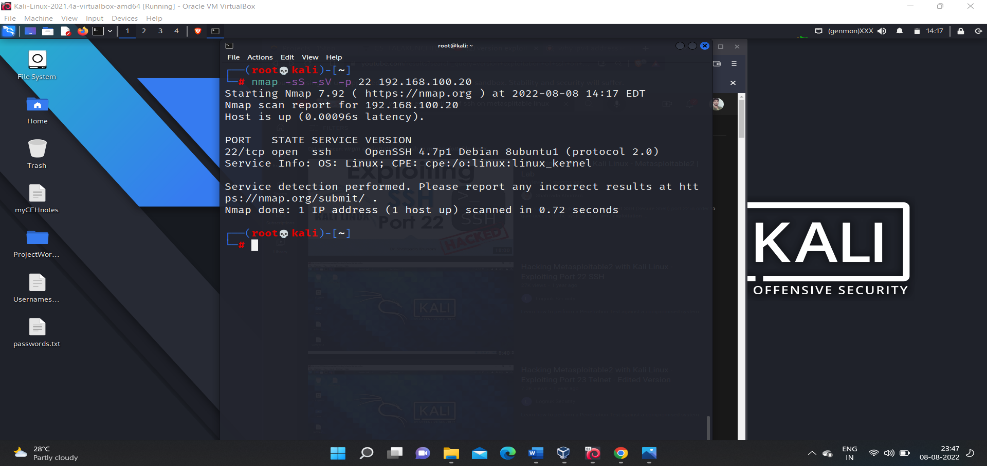
1. **SSH:-**

* The steps to exploit the “ssh” is same that of above.
* Firstly find the target machine Ip ,in our case it is metasploitable linux.

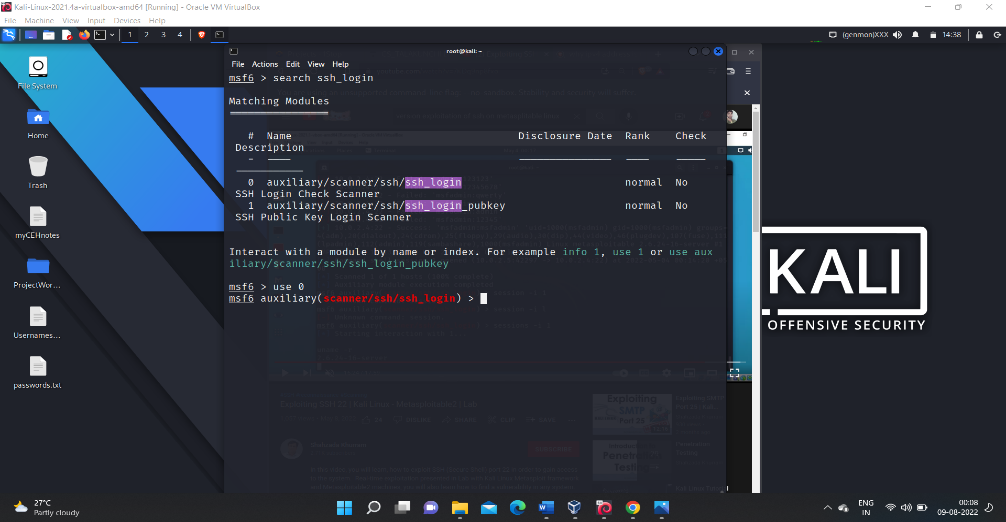
****

* And then find the version of the ssh port i.e port number 22 using Nmap scanning.
* Then find the steps to exploit the port using the version that is found using the Nmap scanning , we ill the steps to exploit in the rapid7.com

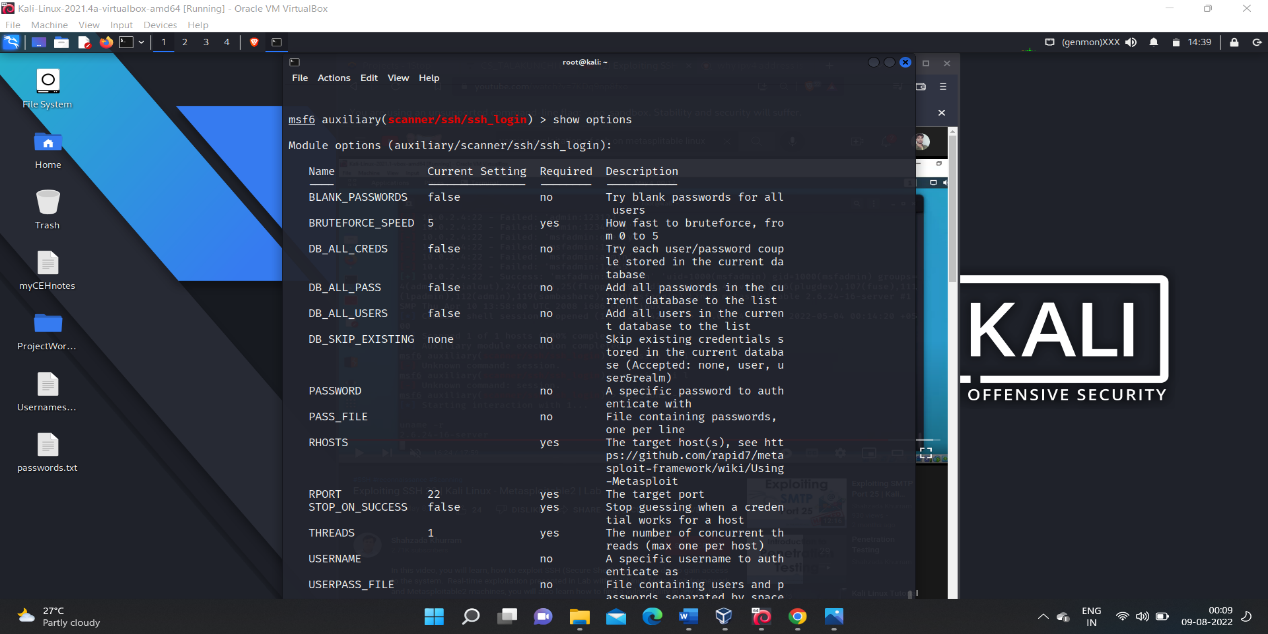
🡪 Nmap scanning result for the ssh port of the metasploitable linux machine.



🡪Then getting into the “msfconsole” and loading the necessary modules for exploiting the ssh port.



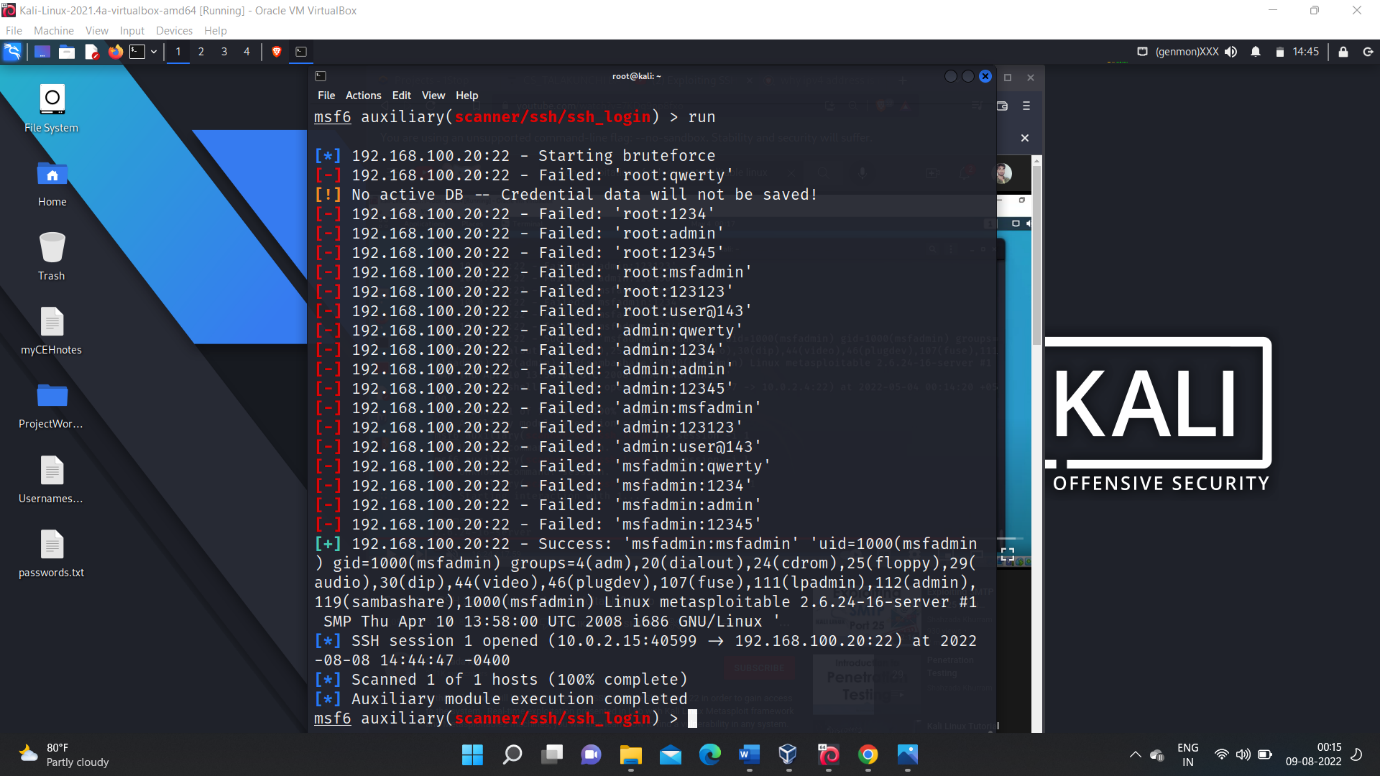
🡪Then using the command $ show options , we can find the list of options and how to use them in detail.



🡪Then after setting the values for the specific options that need to use during the exploitation and we are doing the “brute force “ attack.

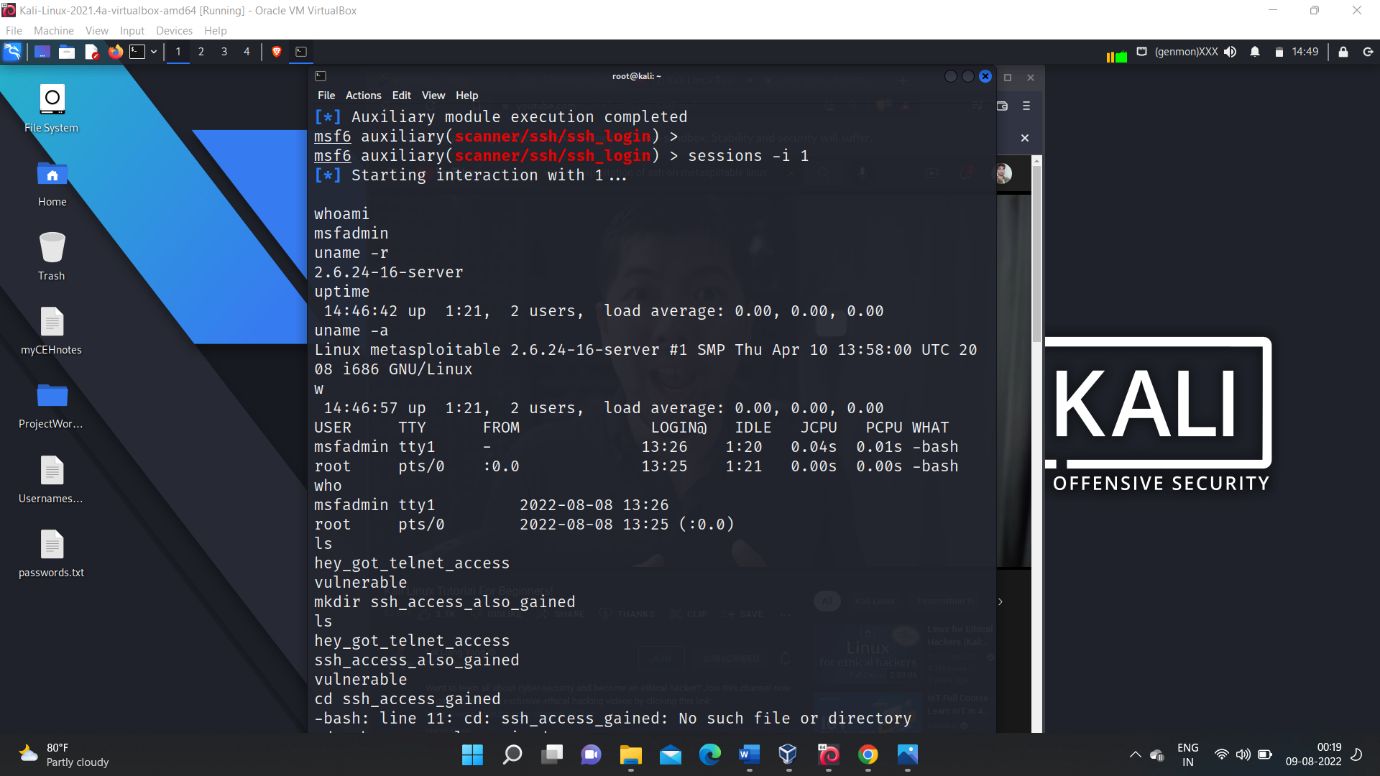


🡪Then after executing the command $ run ,the exploitation starts and as soon as we gain the login access the attack is stopped and it allows us for an interactive session with the target machine.



🡪After gaining an interactive session with the target machine we can perform any sort of operations we will have full control over the target machine.

🡪In our case I performed some file operatons and user related operations and it is shown in the below screen shot.



***Conclusion:-***

*Thus successfully exploited the target machine in our case it is metasploitable linux in the ports like telnet, ftp, and ssh using the concept of version exploitation.*