**System Hacking**

***Internship Project From Talakunchi Networks***

1. **Using Hydra Tool:-**

🡪Hydra is an built in tool in kali-linux os,

It is used to crack the password and get into the system.

🡪The syntax for the usage of the command :-

**$ hydra -L [user\_name\_file\_path] -P [passwords\_file\_path] open\_port // target\_ip**

🡪And to get the open port of the target use ‘namp scanning’.

🡪In our case the target ip is my metasploitable machine.

* Target ip:-

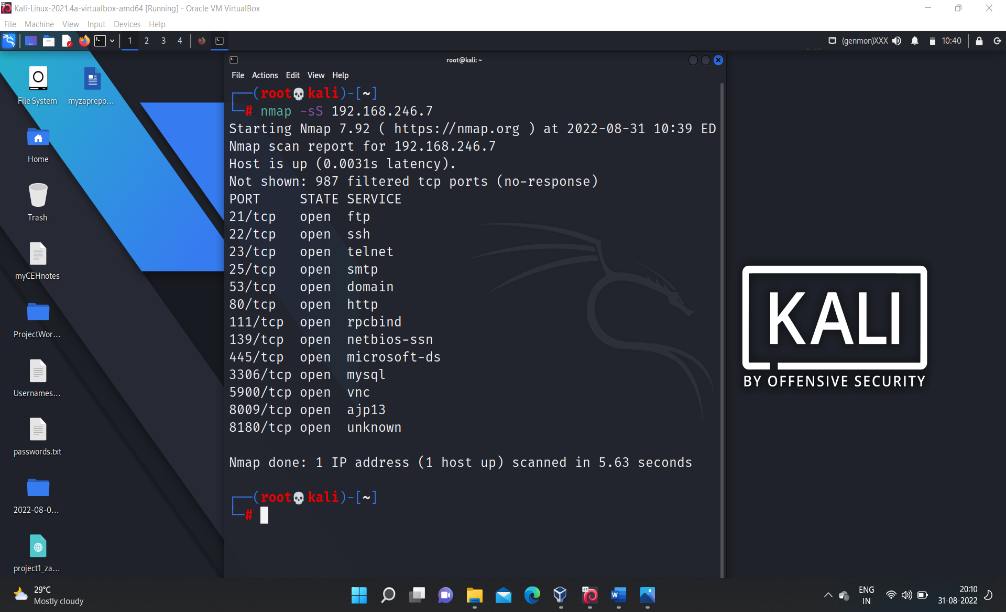


🡪the target ip is :-192.168.246.7

* Performing N-map scanning to get the open port information:-

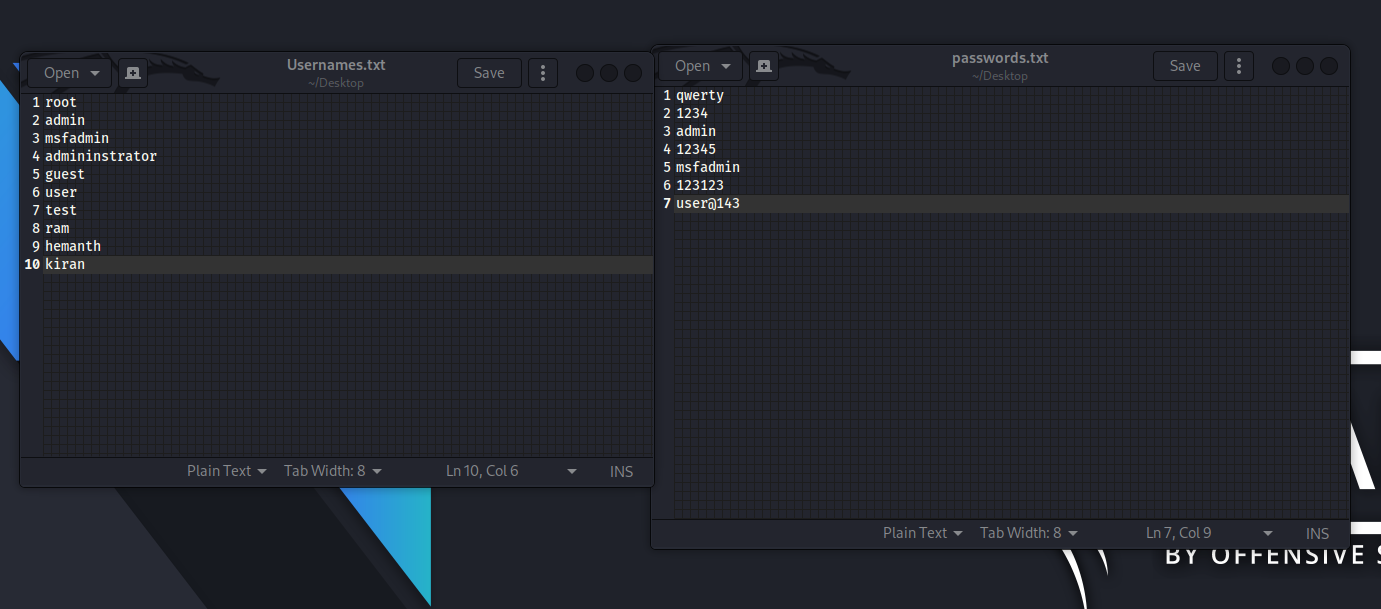
🡪$ nmap -sS 192.168.246.7

🡪The following are the open port’s in our target machine.

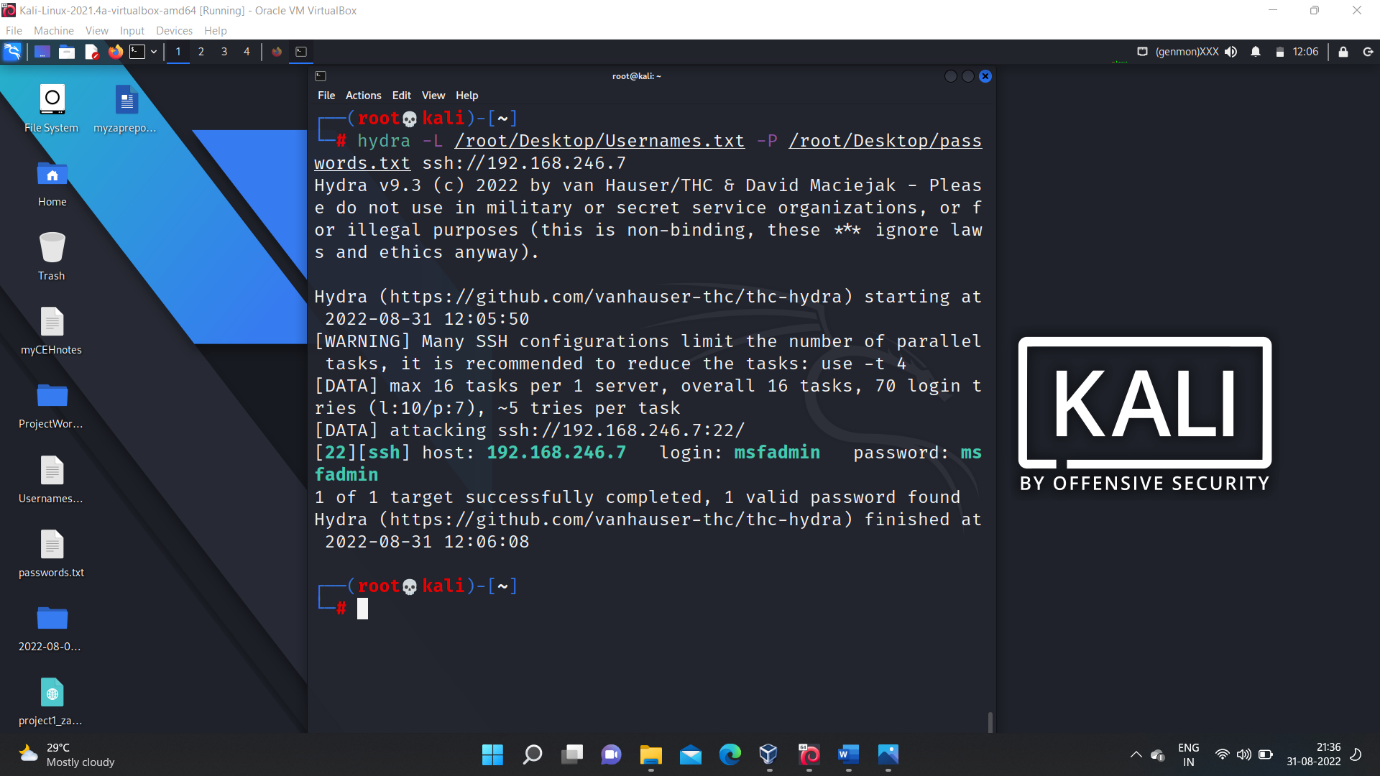


🡪Then now using the ‘hydra’ exploiting the open port to get into the target machine.

🡪**consider username file and password file.**

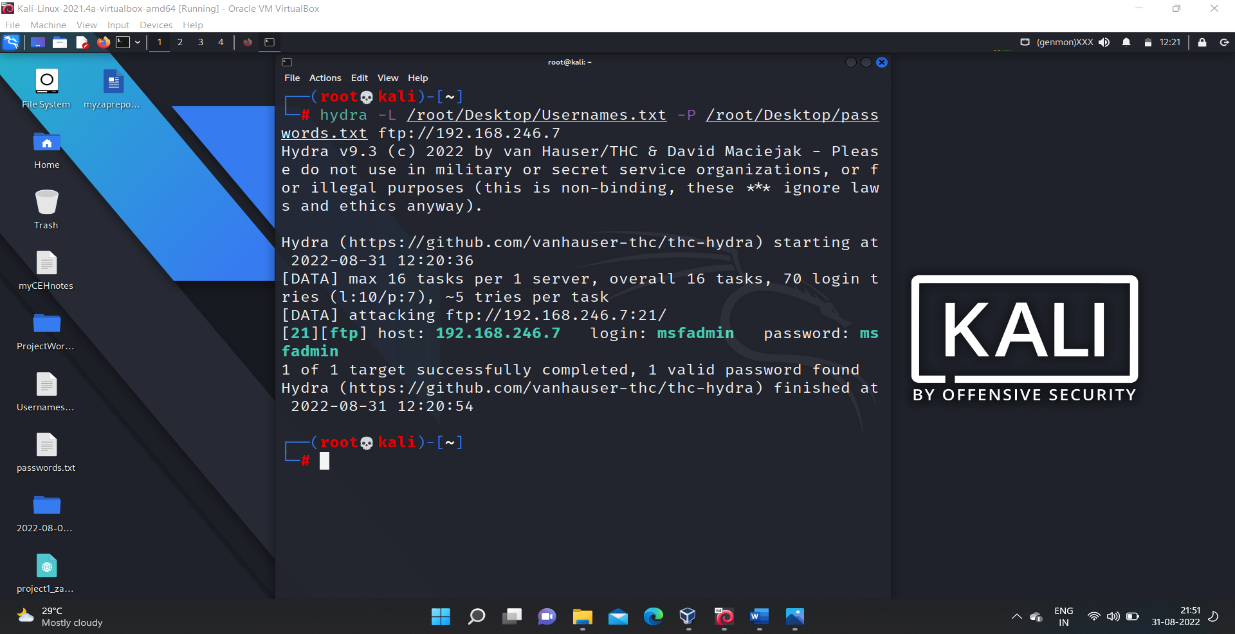


🡪Now let us perform the exploitation on one of the open port shown in the above screenshot (say ‘ssh’)



🡪After exploiting we get the login credentials which is shown in above screenshot.

🡪we can perform it on any open port of the target machine let us consider another port (say ‘ftp’)



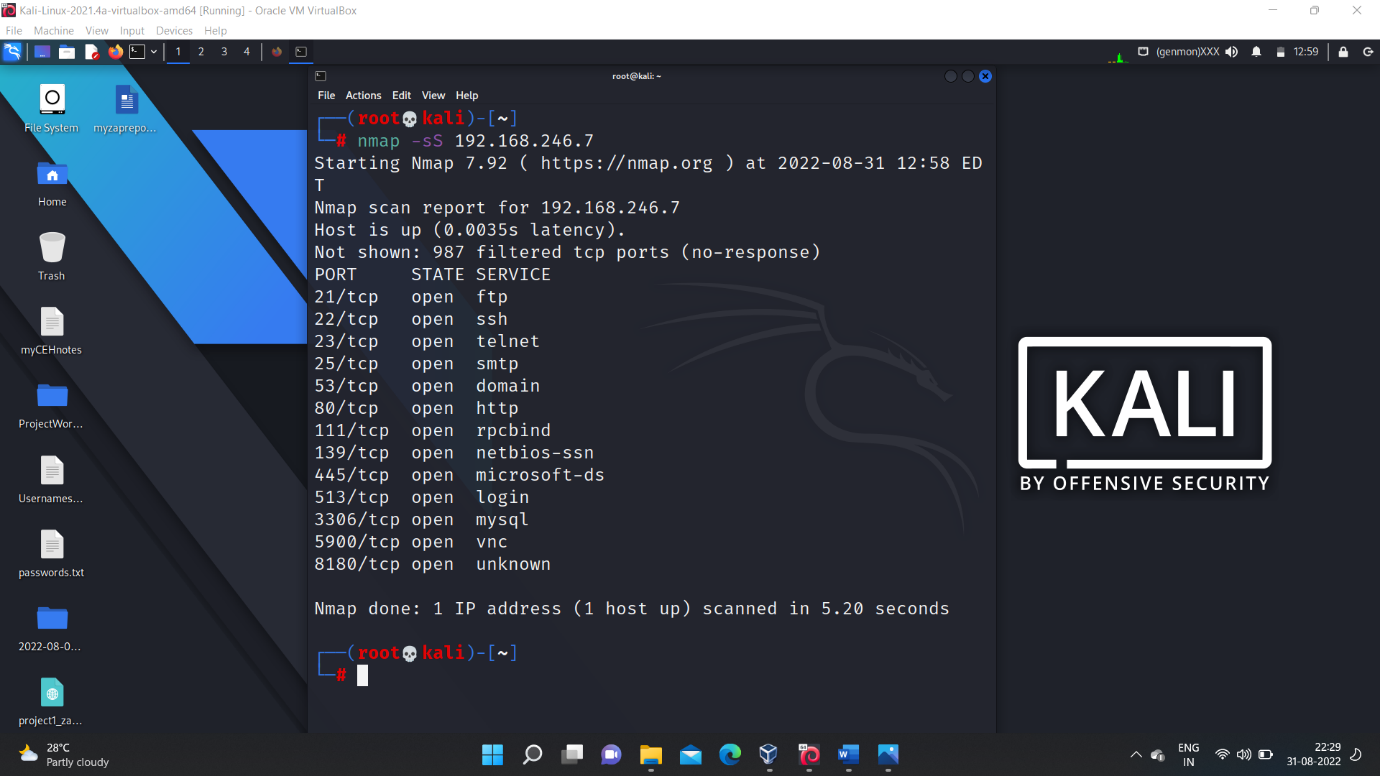
🡪This is all about system hacking using ‘hydra’ tool.

1. **Using Auxiliary :-**

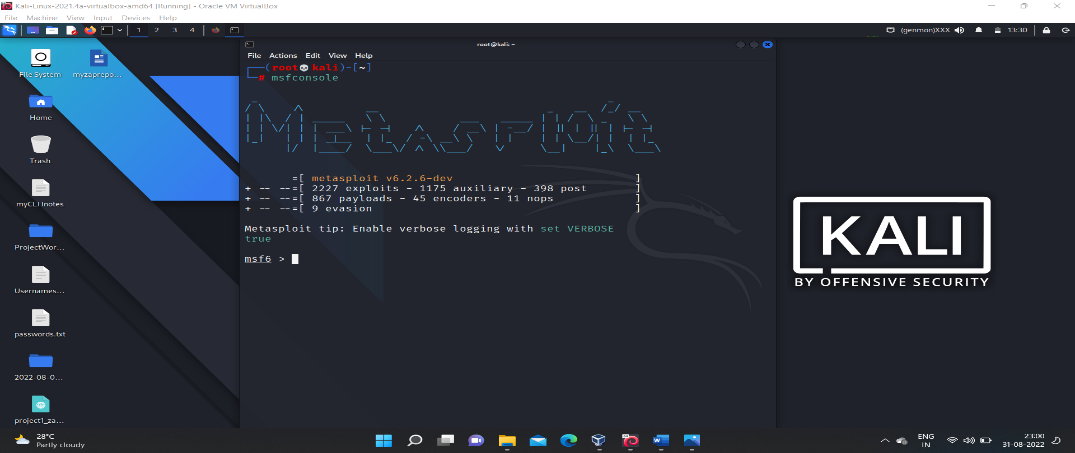
-->auxiliary modules are under the metasploit frame work which is an built-in tool available in the kali-linux os.

-->first find the open port details of the target machine in our case it is metasploitable machine

--> Target ip :- 192.168.246.7 -->open ports are:-



🡪Then get into the metasploitable frame work using the command **$ msfconsole**

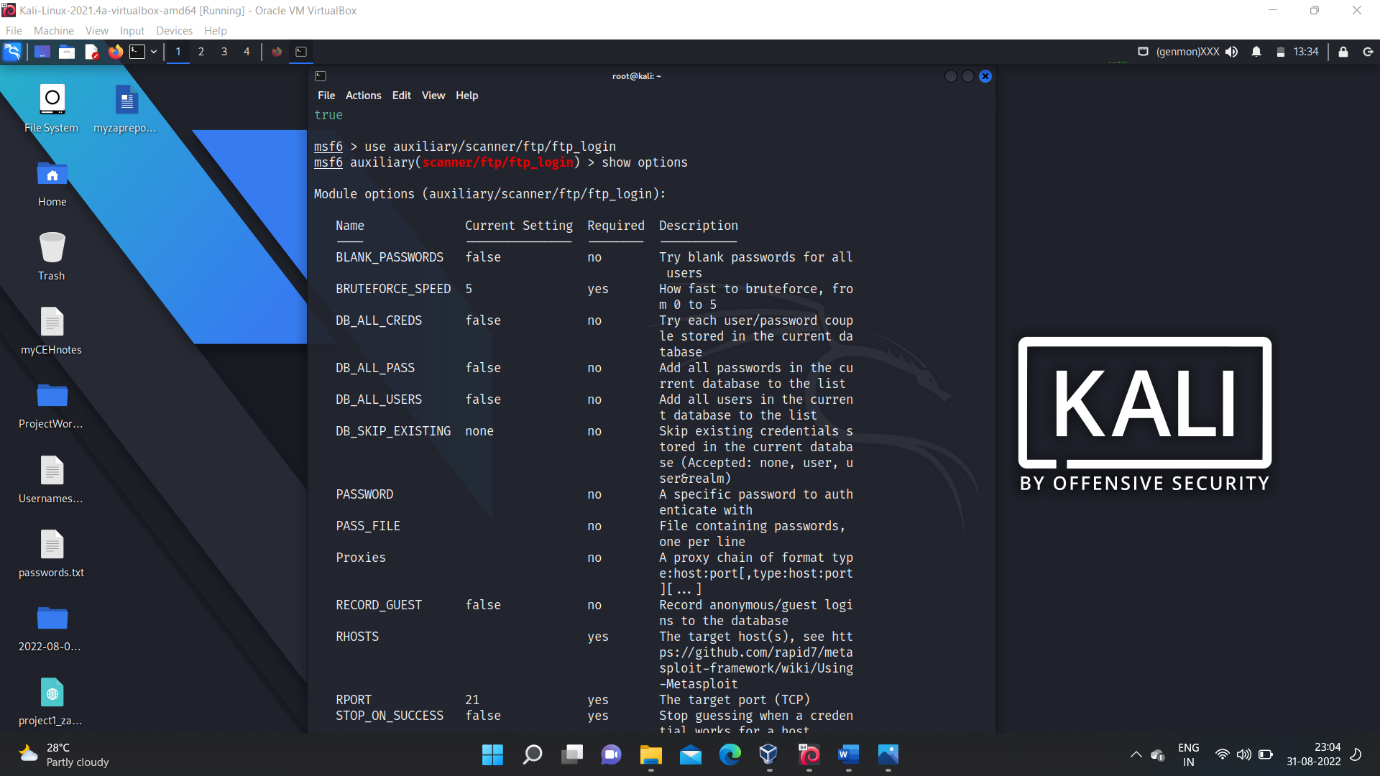
****

🡪then based on which open port you want to exploit the target machine choose the corresponding ‘auxiliary module’

🡪for example if you want to exploit based on the ‘ftp port’ then select corresponding ‘auxiliary module’

**$ use auxiliary scanner/ftp/ftp\_login**

**🡪**then on using the command $ show options.

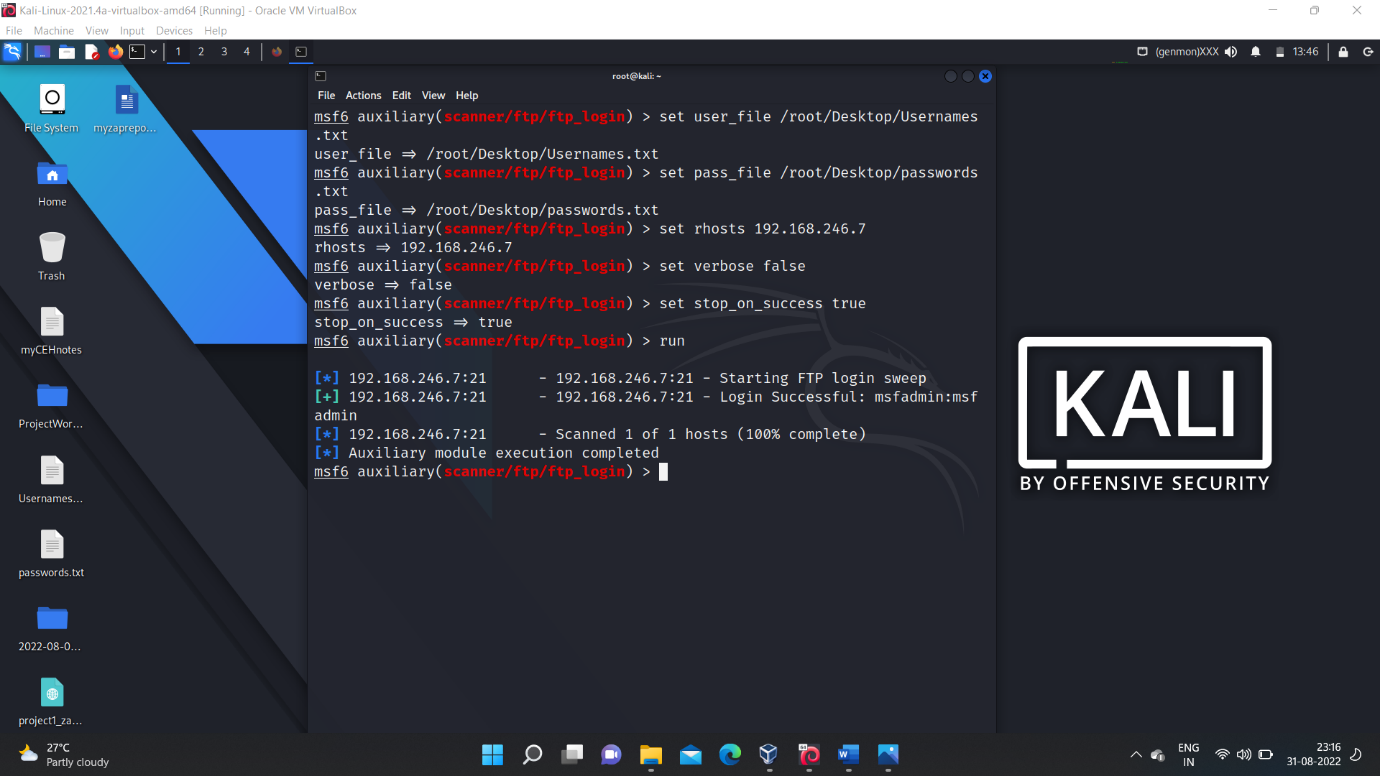


🡪then set the required fields with the values like

for (user\_file and pass\_file setting their respective file paths )and setting (rhosts = target\_ip),(setting verbose = false ,will help to prevent showing the task involved in exploitation) and setting (stop\_on\_success = true)

🡪then after setting all those values then use the command **$ run** to start exploitation.

🡪after the exploitation completion we get the login credentials.



🡪similarly we can do with any another open port also (say ‘ssh’)

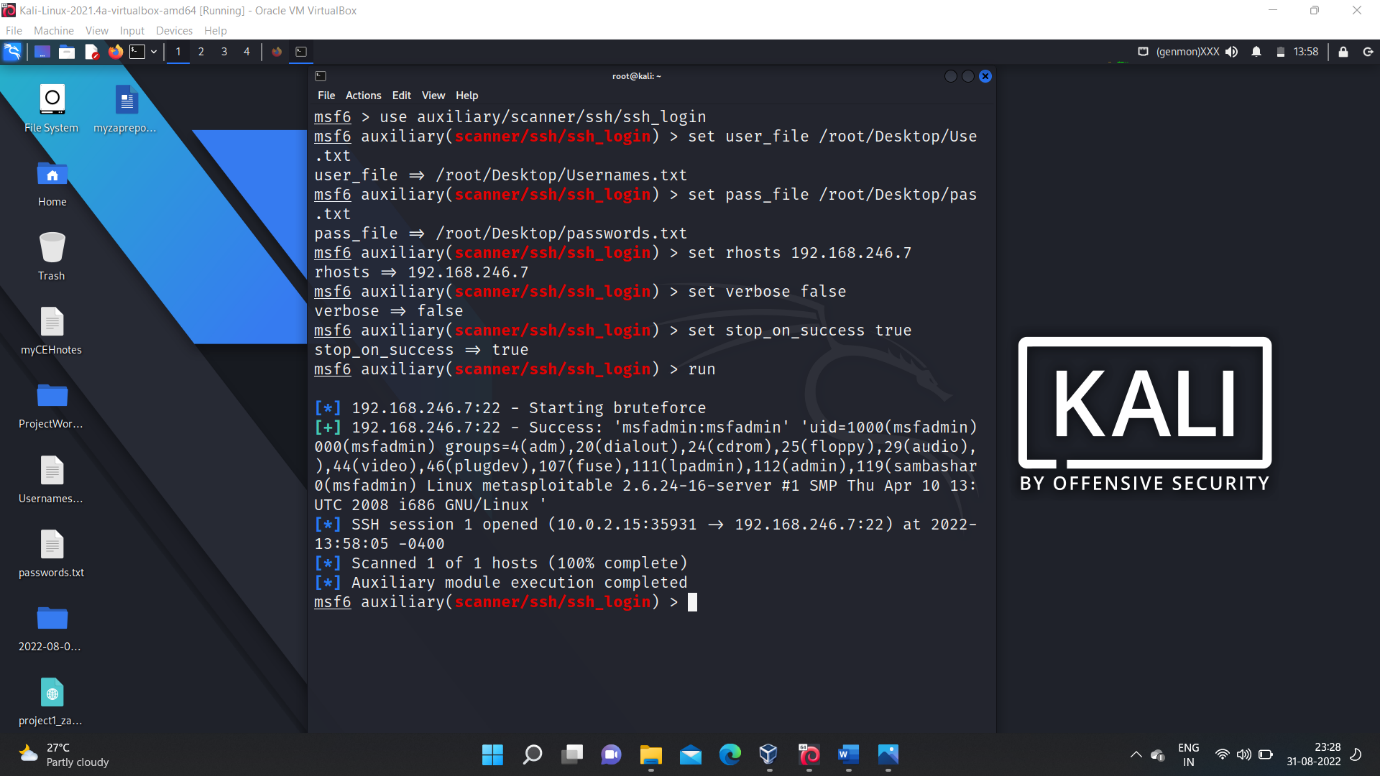
🡪it involves:-

**$ use auxiliary scanner/ssh/ssh\_login**

🡪setting the required values as show for the ‘ftp’ above.

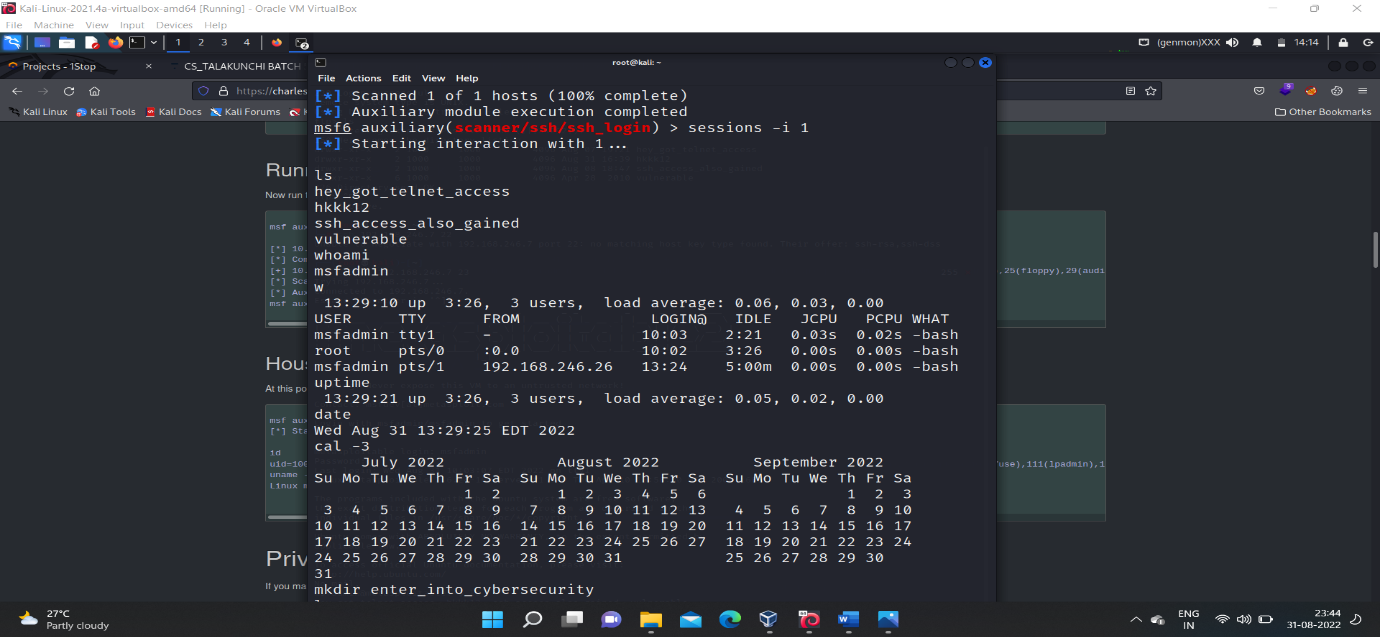
🡪then **$ run** to start exploitation.

🡪then we get the login credentials.



🡪After getting the login credentials we can login into the target system through the gained acess through the session.

🡪**$ session -i 1**  to get an interactive session with the target system and we can perform any action.



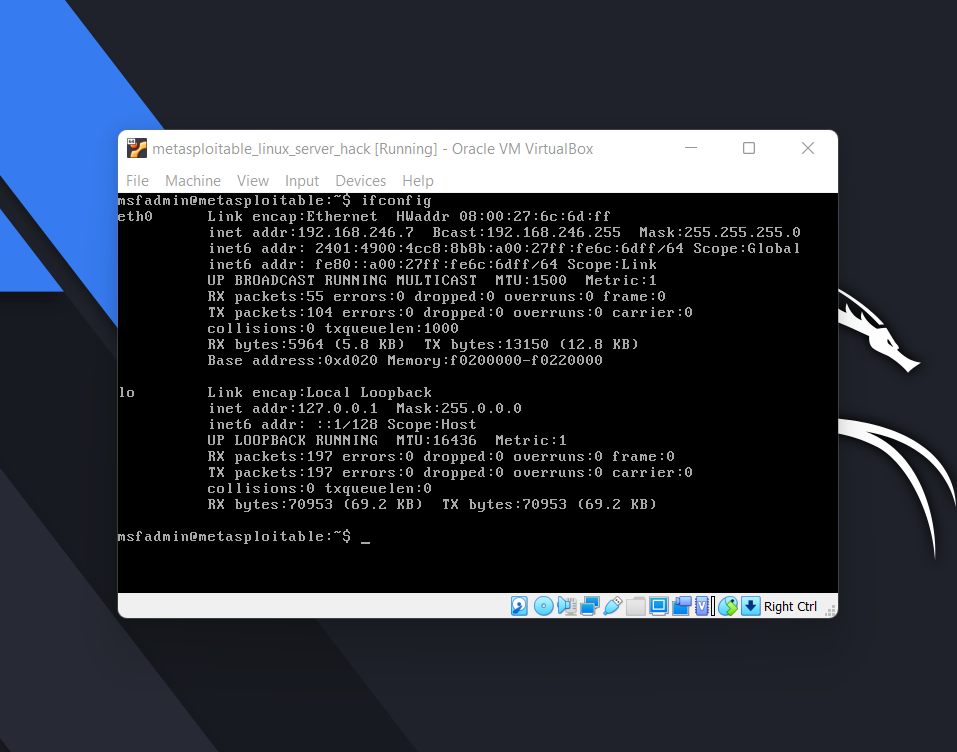
🡪This is all about system hacking using auxilixary modules.

1. **Using NSE – Scripts :-**

🡪The ‘NSE-scripts’ are also known as ‘automated scripts’ or ‘nmap scripts’ these are the built in scripts in the ‘kali-linux’ os and it doesn’t require any file as input like ‘user\_name or password\_file’ .

🡪The scripts itself contains all the required thing to perform an bruteforce activity on the open port of the target machine.

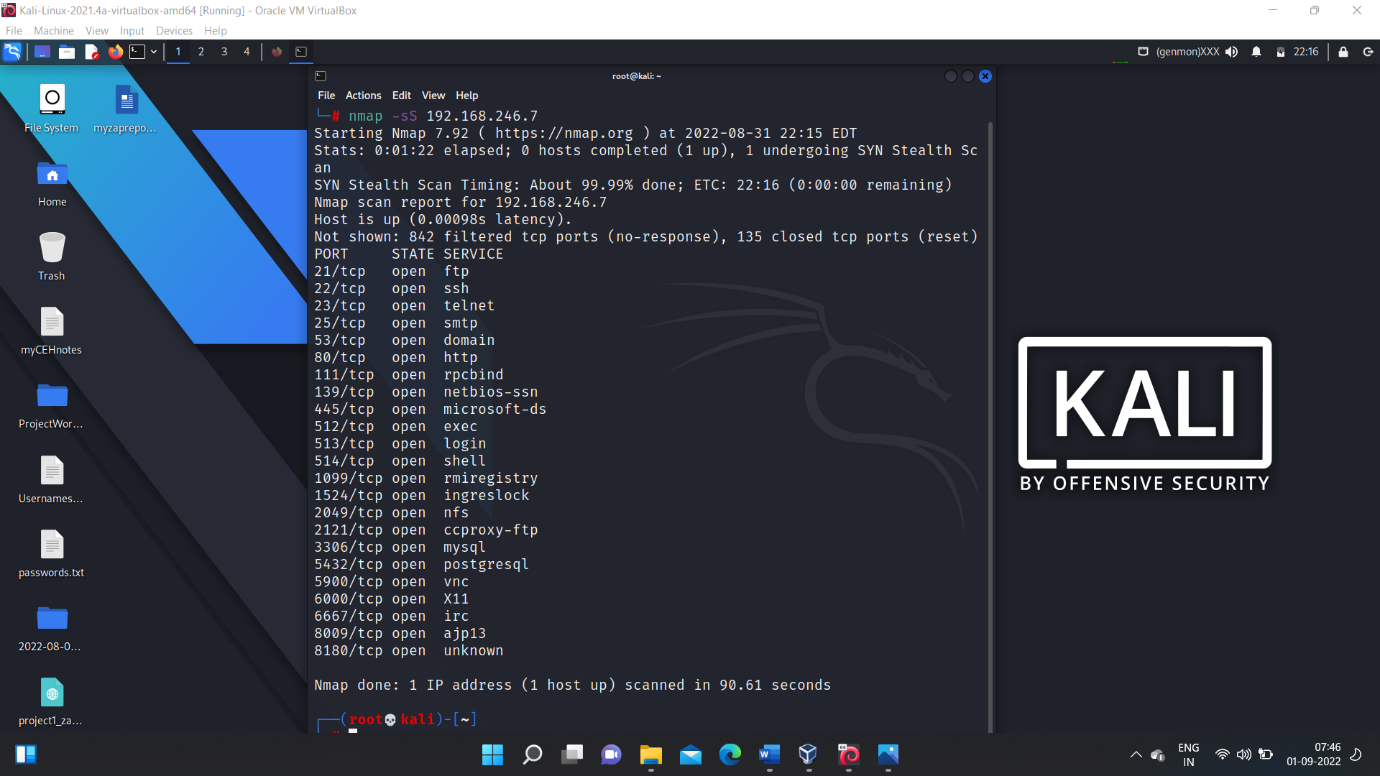
🡪target\_ip : - in our case it is ‘metasploitable machine’. --> 192.168.246.7



🡪Then find the open ports on the target machine using the command.

$ nmap -sS 192.168.246.7

* It gives the information of the list of open ports on the target machine.



* Select one of the open port and load the corresponding ‘-brute.nse’ script and the start exploiting.
* Steps involved in exploiting using ‘nse-scripts’:-
* (1) navigate to the location where the ‘nse-scripts’ are located.

$ cd /usr/share/nmap/scripts

* Then when we give ‘ls’ we will find so many scripts in that location.
* Then choose the script that is corresponding to the open port(let say ‘ssh’) on which you want to exploit target machine.

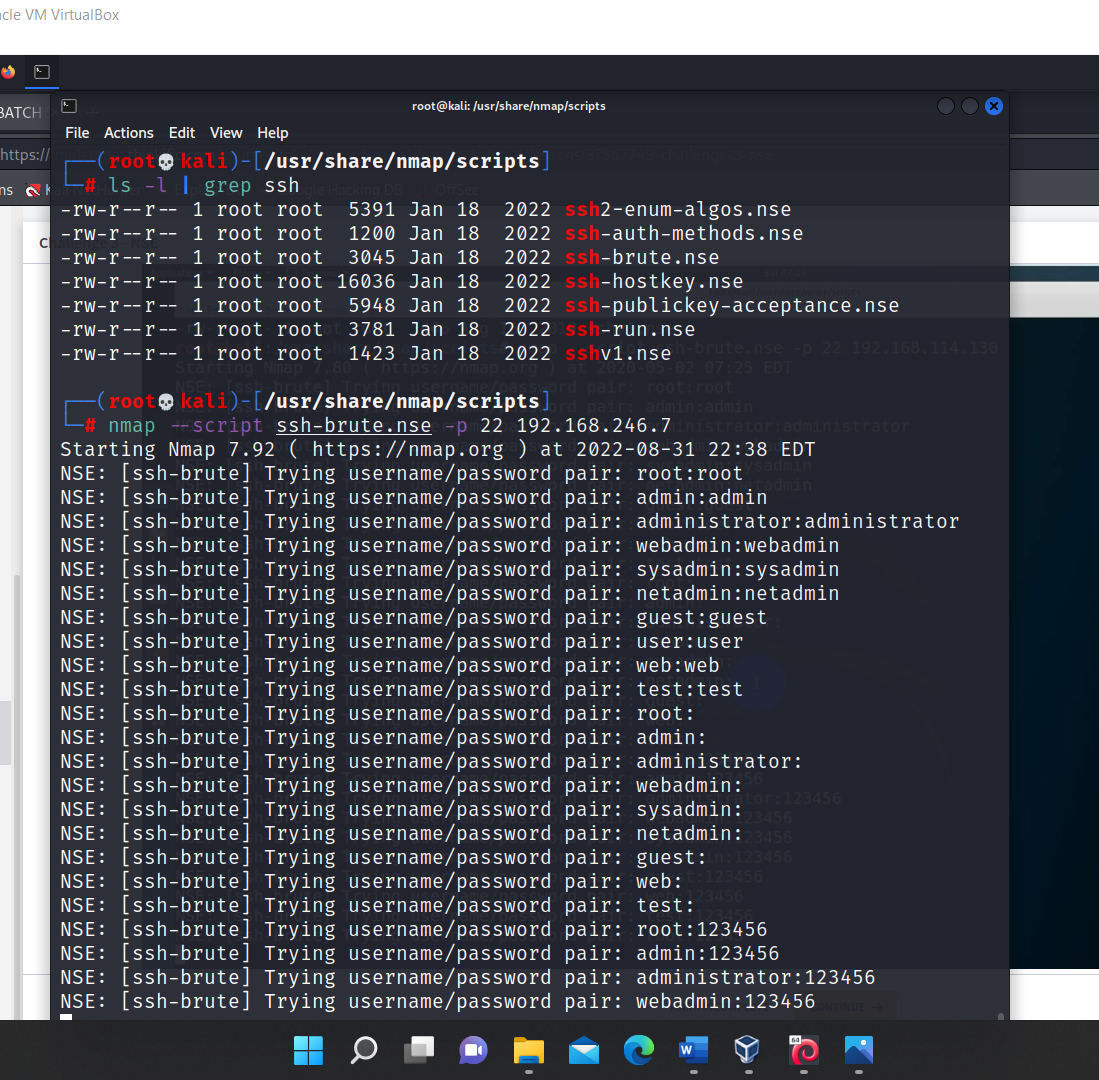
**$ ls -l | grep ssh**

* Then you can find the corresponding ‘ssh’ nse scripts, from that choose the ‘ssh-brute.nse’ to exploit the target machine.



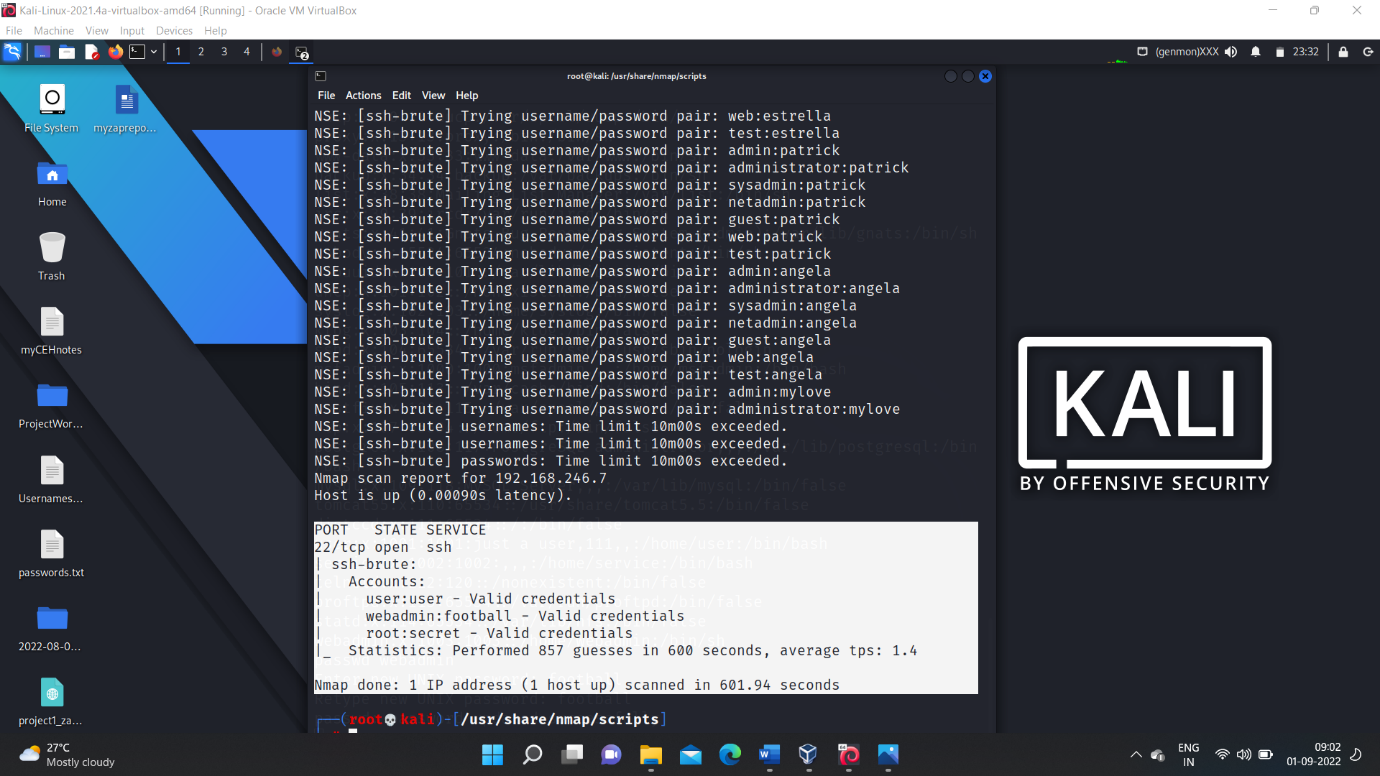
* Command to load the selected script .

**$ nmap --script ssh-brute.nse -p 22 target\_ip**



>Then the script performs exploitation on the target-

machine with the ‘username’ and ‘password’ pairs it contains and it takes few minutes of time to perform the exploitation with all those pairs and it gives the credentials after finding the correct ‘user\_name and password ‘pair



>from above exploitation we get 3 valid user credentials they are:-

**> user : user**

**> webadmin : football**

**> root : secret**

>Then we can able to login into the target machine and we can perform any actions.

>This is all about the system hacking using ‘nse-scripts’.