Ethical Hacking and Penetration Testing

Assignment 6

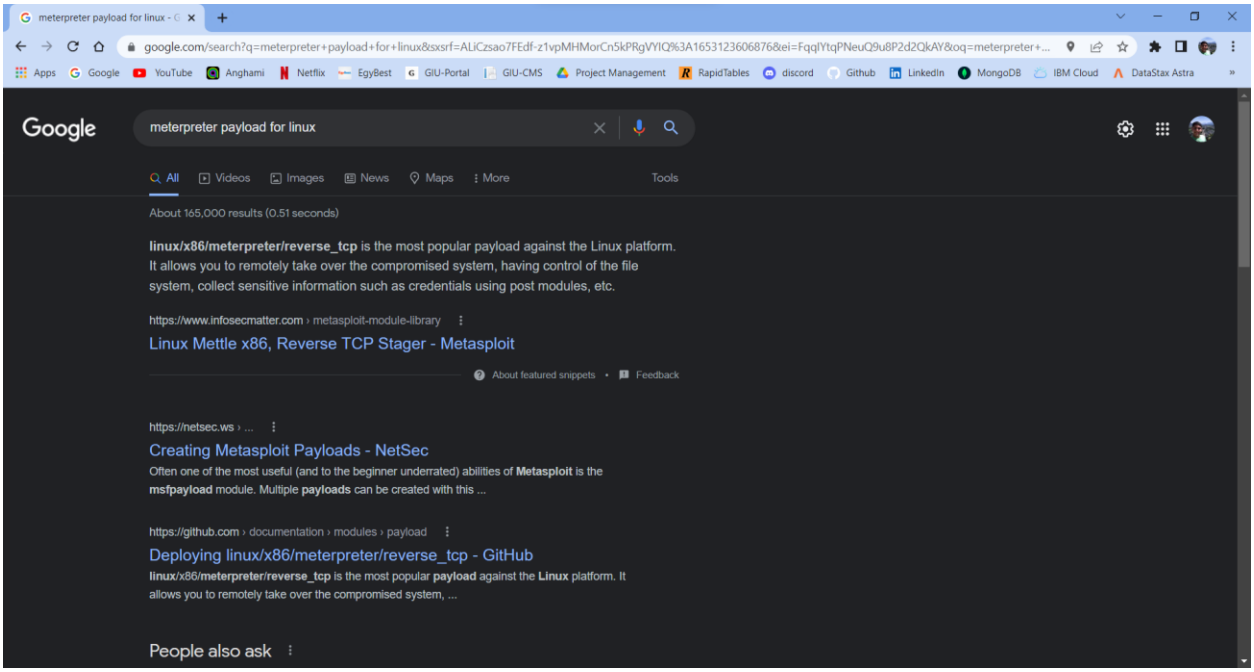
Maintaining Access
(Metasploitable machine)

Name: John Ehab

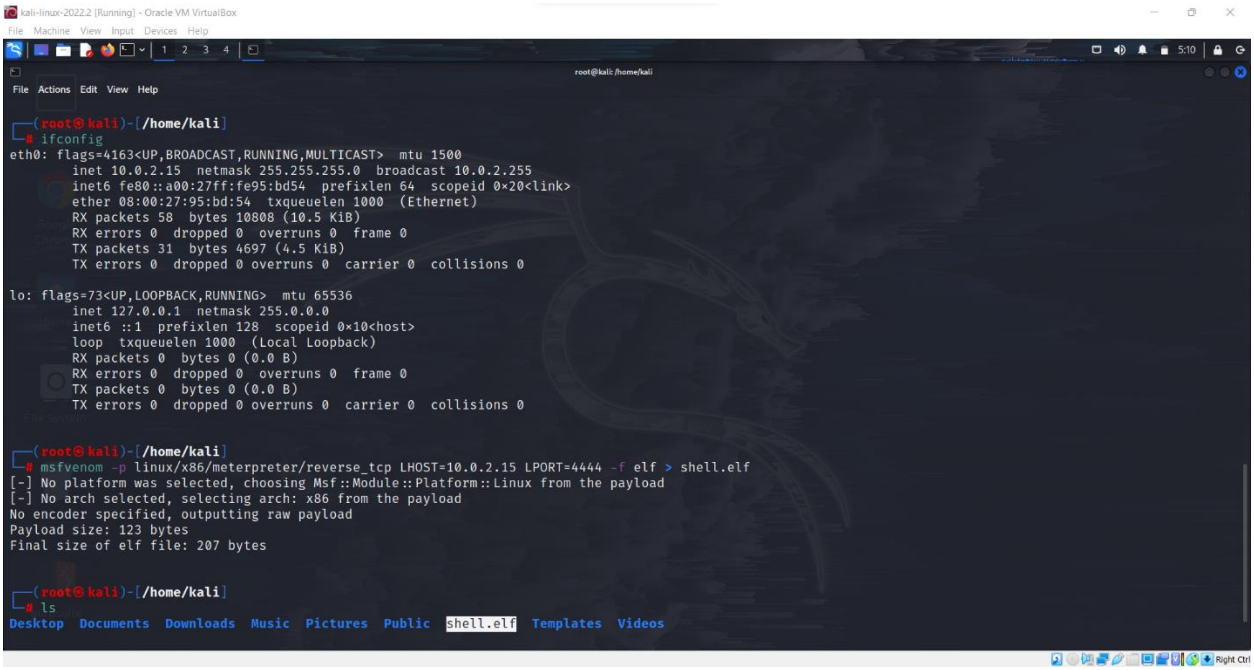
ID: 100-2096

1- Persistence backdoor

1- First open both kali machine and metasploitable machine, username and password of the metasploitable machine is msfadmin, then open google to search for the path of the payload that u want.

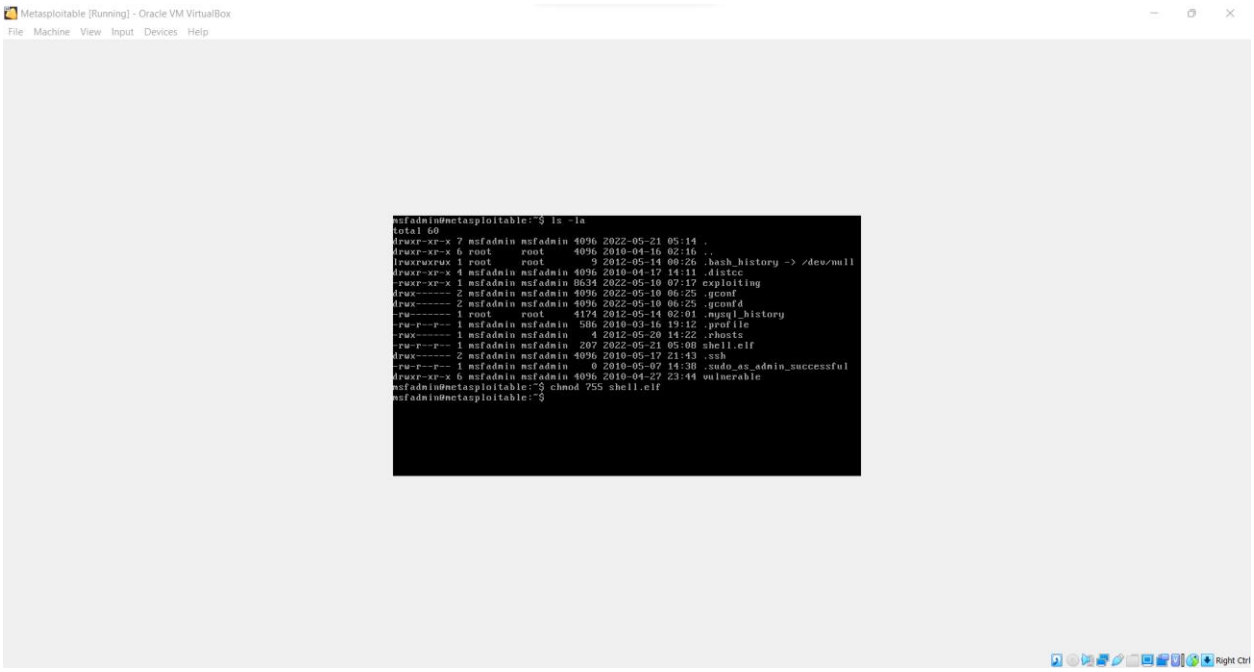


2- Then open kali terminal and download this payload and save it to a file named shell.elf, write the IP of kali gotten from ifconfig and port 4444.

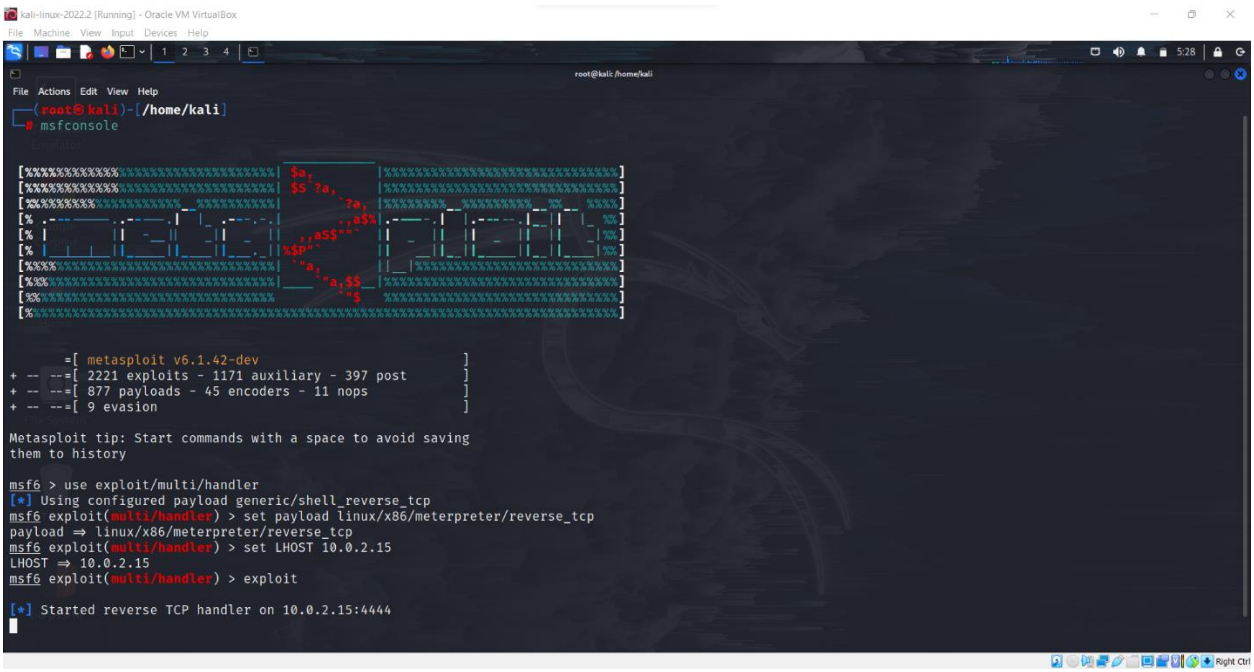


3- Then send the file from kali to metasploitable using python http server and wget cmd.

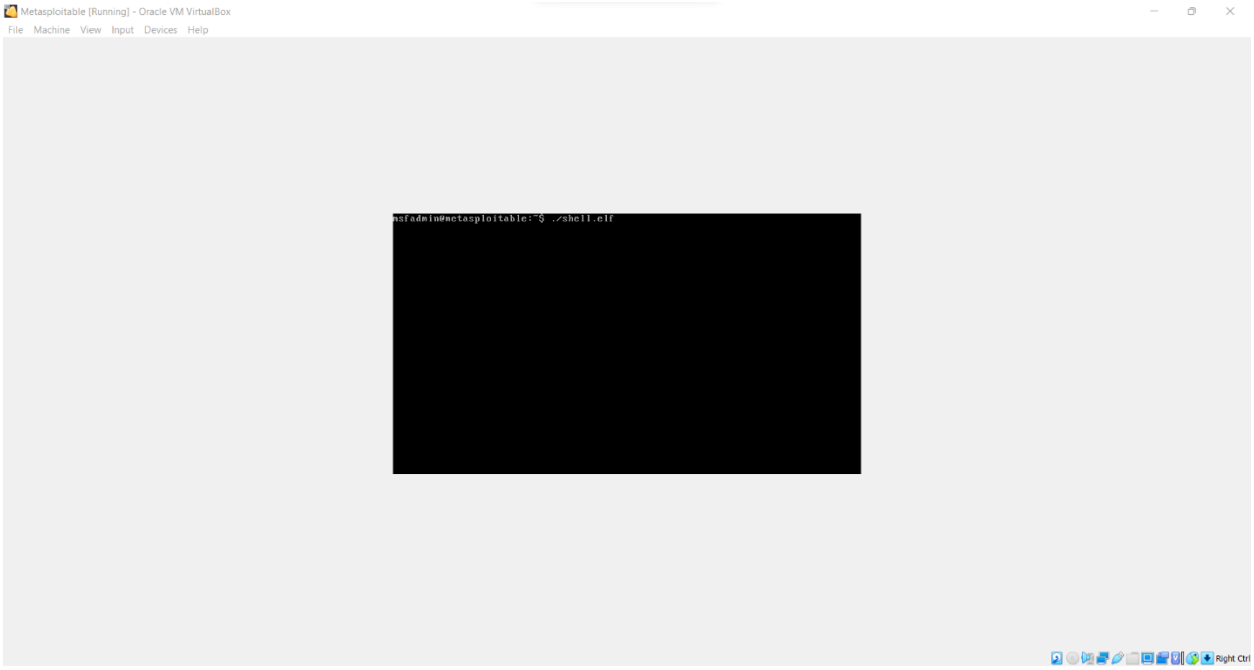
4- Then I'll change the permission of this file on metasploitable to make it executable, cmd chmod 755 shell.elf.

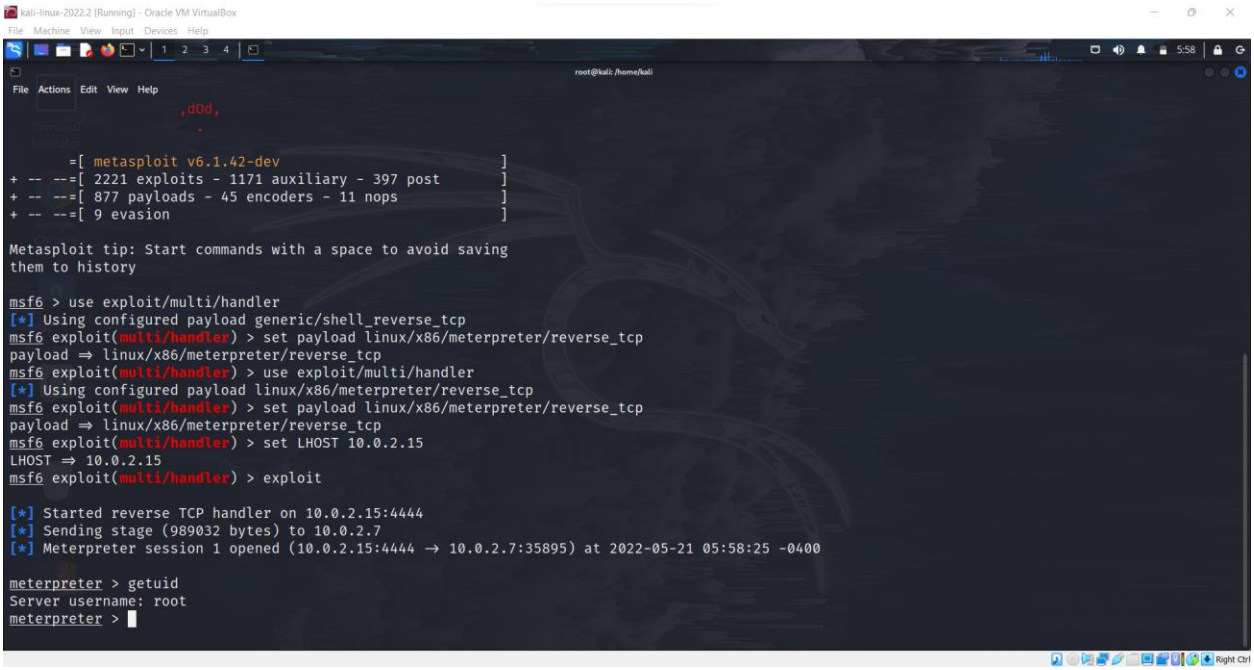


5- Then re-open kali to connect it to the victim's payload. Open Metasploit, then use the multi handler module, then set the payload to adjust it to be the same as we sent to the victim machine and the lhost to be the IP of kali, then start listening using the cmd exploit.

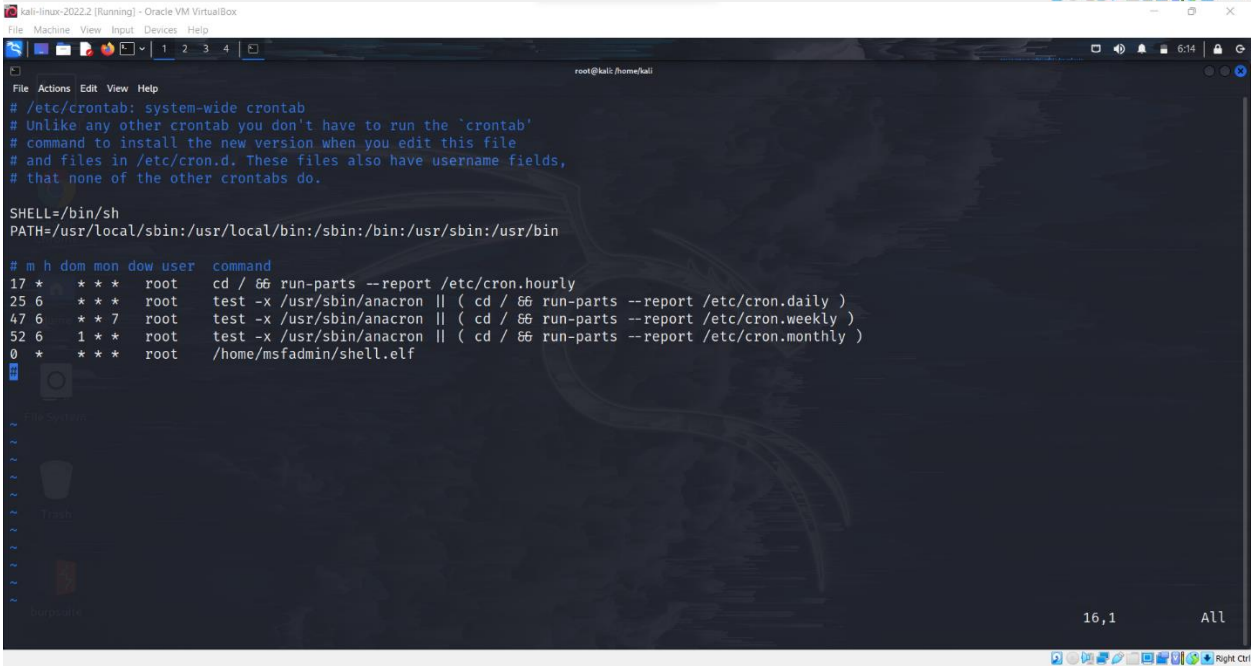


6- Then open metasploitable machine and run the file, and re-open kali to test that it's connected successfully when it shows root when u type the getuid cmd.





7- Lastly to maintain my access we'll need this file to re-run every now and then to connect to my machine (kali), so I'll open the crontab file from meterpreter, and edit it to make it run periodically every 1 hour "0 * * * *".



2- Metsvc backdoor

- Metsvc is a powerfull meterpreter service payload, it offers the ability to place a backdoor on the victim machine to maintain access after the exploitation is done, just like the persistent backdoor but designed especially for victim machines that work on windows.

- The steps of using it is just like what is shown above, but we will use the payload “windows/metsvc_bind_tcp” instead of “linux/x86/meterpreter/reverse_tcp”. And we’ll target a victim machine that works with windows OS instead of metasploitable that works with linux.

- First we’ll download the payload and save it to a file, then send this payload file from kali to the windows victim machine, then open metasploit from kali and use the multi handler module and set the payload and the LHOST and start exploiting, and go to the victim machine to run the file and go back to kali to test using sysinfo cmd for example, then finally change the crontab to make this payload file re-run periodically on the victim machine.