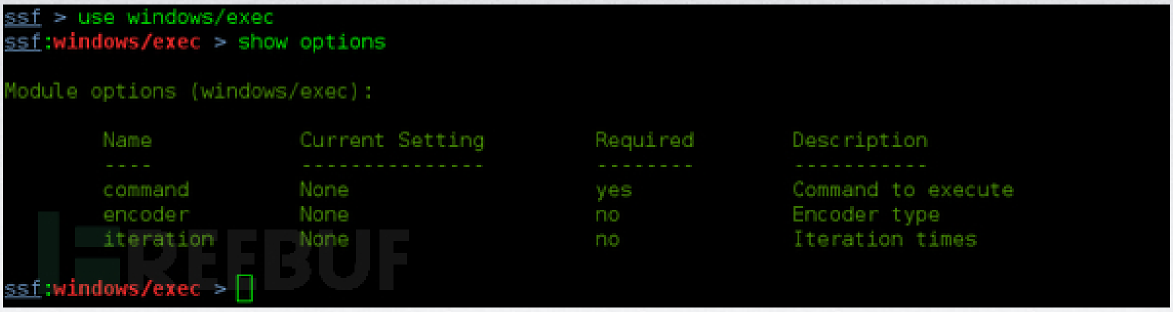
0×00 简介

Shellsploit让你生成定制shellcodes、后门、各种操作系统的攻击代码。同时可以使用它来进行代码混淆工作。

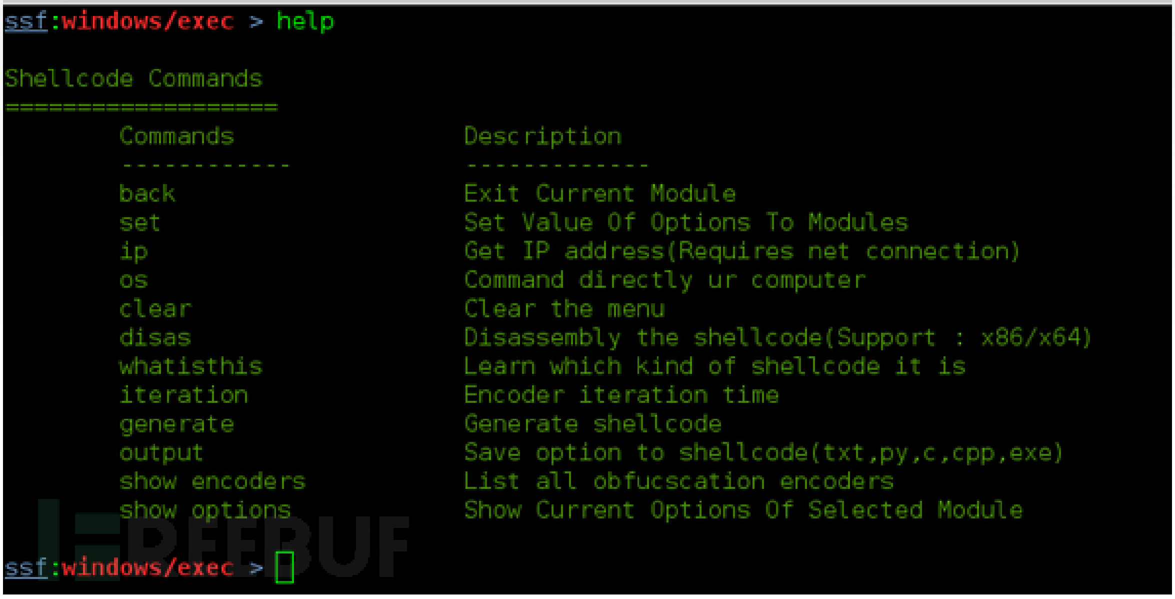


```
ssf > use windows/exec
ssf:windows/exec > show options

Module options (windows/exec):

        Name            Current Setting         Required        Description
        ----            ---------------         --------        -----------
        command         None                    yes             Command to execute
        encoder         None                    no              Encoder type
        iteration       None                    no              Iteration times

ssf:windows/exec > 
```



```
ssf:windows/exec > help

Shellcode Commands
===================
        Commands                Description
        ------------            -------------
        back                    Exit Current Module
        set                     Set Value Of Options To Modules
        ip                      Get IP address(Requires net connection)
        os                      Command directly ur computer
        clear                   Clear the menu
        disas                   Disassembly the shellcode(Support : x86/x64)
        whatisthis              Learn which kind of shellcode it is
        iteration               Encoder iteration time
        generate                Generate shellcode
        output                  Save option to shellcode(txt,py,c,cpp,exe)
        show encoders           List all obfucscation encoders
        show options            Show Current Options Of Selected Module

ssf:windows/exec > 
```

0×01 安装或卸载

如果你想使用Shellsploit，你首先得先安装Capstone

Capstone’s安装如下：

```
sudo pip install capstone
```

同样得安装readline

```
root$ sudo pip install readline
```

安装好以上程序后，你就可以开始安装shellsploit了

```
root$ python setup.py -s/--setup install
root$ chmod +x shellsploit (if you are using windows just pass this step)
root$ ./shellsploit
```

如果哪一天你觉得 shellsploit不好了，你可以进行卸载

```
root$ python setup.py -s/--setup uninstall
```

0×02 参数说明

```
usage: shellsploit  [-l] [-p] [-o] [-n]
                        [--host] [--port]



optional arguments:
       -l, --list            Show  list of backdoors,shellcodes,injectors
       -p, --payload         Set payload for usage
       -n, -nc               Declare netcat for usage
       --host                The connect/listen address
       --port                The connect/listen port

Inline arguments:

    Main Menu:
        help                 Help menu
        os                   Command directly ur computer
        use                  Select Module For Use
        clear                Clear the menu
        show modules         Show Modules of Current Database
        show backdoors       Show Backdoors of Current Database
        show injectors       Show Injectors(Shellcode,dll,so etc..)

    Shellcode Menu:
        back                 Exit Current Module
        set                  Set Value Of Options To Modules
        ip                   Get IP address(Requires net connection)
        os                   Command directly ur computer
        clear                Clear the menu
        disas                Disassembly the shellcode(Support : x86/x64)
        whatisthis           Learn which kind of shellcode it is
        iteration            Encoder iteration time
        generate             Generate shellcode
        output               Save option to shellcode(txt,py,c,cpp,exe)
        show encoders        List all obfucscation encoders

        show options         Show Current Options Of Selected Module

    Injector Menu:
        set                  Set Value Of Options To Modules
        set                 Set value of options to modules
        help                Help menu
        back                Exit Current Module
        os                  Command directly ur computer
        pids                Get PID list of computer
        getpid              Get specific PID on list(Ex. getpid Python)
```

Shellsploit-framework项目地址：https://github.com/b3mb4m/shellsploit-framework

***投稿作者：我是酱油男，转载请注明来自FreeBuf黑客与极客（FreeBuf.COM）**