

浅谈 PSEXEC 做的那些事 - SecPulse.COM | 安全脉搏

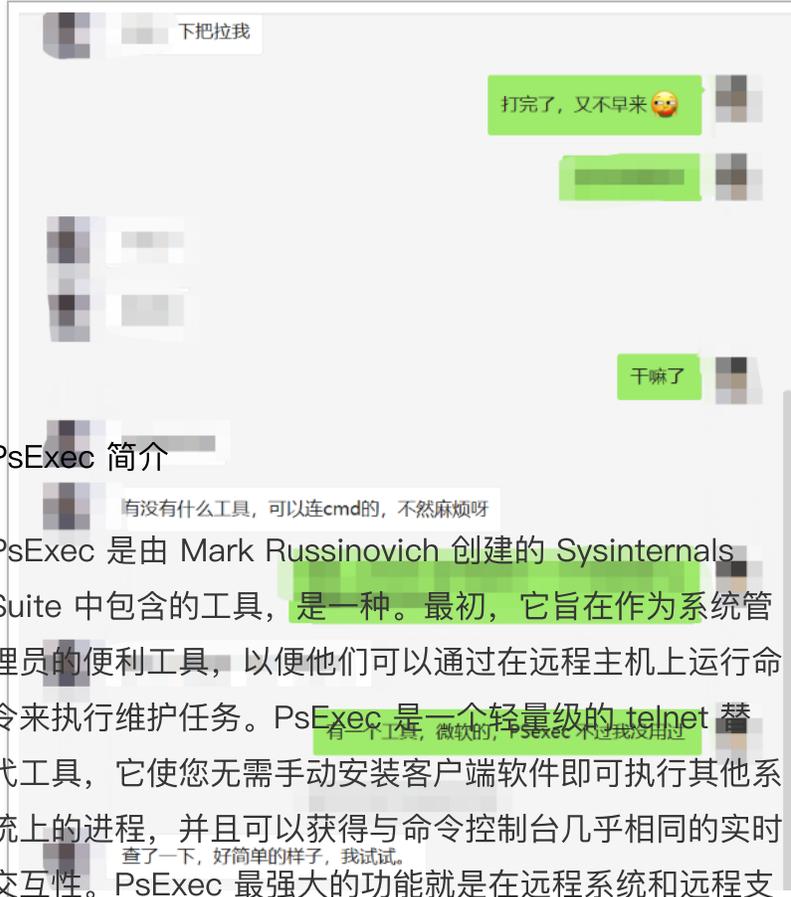
“ 这是 酒仙桥六号部队 的第 108 篇文章。
章。

这是 酒仙桥六号部队 的第 108 篇文章。

全文共计 3058 个字，预计阅读时长 9 分钟。

前言

在某个游戏的夜晚，兄弟找我问个工具，顺手聊到 PsExec 的工具，之前没用过，看到兄弟用的时候出现了点问题，那就试用用，顺便分析一下它做了什么。



PsExec 简介

PsExec 是由 Mark Russinovich 创建的 Sysinternals Suite 中包含的工具, 是一种。最初, 它旨在作为系统管理员的便利工具, 以便他们可以通过在远程主机上运行命令来执行维护任务。PsExec 是一个轻量级的 telnet 替代工具, 它使您无需手动安装客户端软件即可执行其他系统上的进程, 并且可以获得与命令控制台几乎相同的实时交互性。PsExec 最强大的功能就是在远程系统和远程支持工具 (如 ipconfig、whoami) 中启动交互式命令提示窗口, 以便显示无法通过其他方式显示的有关远程系统的信息。

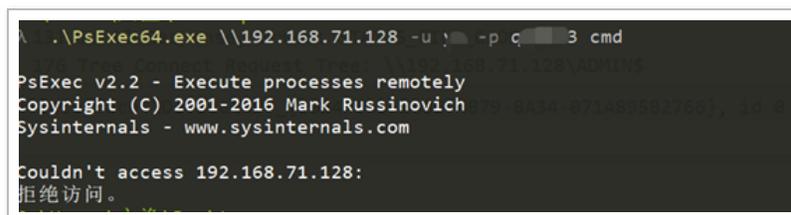
- PsExec 特点

1. psexec 远程运行需要远程计算机启用文件和打印共享且默认的 Admin\$ 共享映射到 C:windows 目录。
2. psexec 建立连接之后目标机器上会被安装一个“PSEXESVC”服务。但是 psexec 安全退出之后这个服务会自动删除 (在命令行下使用 exit 命令退出)。

工作原理

- PsExec 详细运行过程简介
正式开展测试，启用 net sharAdmin \$ 共享。拒绝访问？这是要出师未捷身先死？
 1. TCP 三次握手，通过 SMB 会话进行身份验证。
 2. 连接 admin\$ 共享，通过 SMB 访问默认共享文件夹 ADMIN\$，写入 PSEXESVC.exe 文件；
 3. 利用 ipc 命名管道调用 svcctl 服务
 4. 利用 svcctl 服务开启 psexesvc 服务
 5. 生成 4 个命名管道以供使用。一个 psexesvc 管道用于服务本身，另外的管道 stdin（输入）、stdout（输出）、stderr（输出）用于重定向进程。

正式开展测试，启用 net sharAdmin \$ 共享。拒绝访问？这是要出师未捷身先死？



```
.\PsExec64.exe \\192.168.71.128 -u y... -p c... 3 cmd
PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Couldn't access 192.168.71.128:
拒绝访问。
```

稳住，先别慌，抓包看看，目测是 admin\$ 无法访问导致的。

192.168.71.1	192.168.71.128	SMB2	172 Tree Connect Request Tree: \\192.168.71.128\IPC\$
192.168.71.128	192.168.71.1	SMB2	138 Tree Connect Response
192.168.71.1	192.168.71.128	SMB2	212 Ioctl Request FSCTL_VALIDATE_NEGOTIATE_INFO
192.168.71.128	192.168.71.1	SMB2	131 Ioctl Response, Error: STATUS_FILE_CLOSED
192.168.71.1	192.168.71.128	SMB2	176 Tree Connect Request Tree: \\192.168.71.128\ADMIN\$
192.168.71.128	192.168.71.1	SMB2	131 Tree Connect Response, Error: STATUS_ACCESS_DENIED
192.168.71.1	192.168.71.128	SMB2	176 Tree Connect Request Tree: \\192.168.71.128\ADMIN\$
192.168.71.128	192.168.71.1	SMB2	131 Tree Connect Response, Error: STATUS_ACCESS_DENIED
192.168.71.1	192.168.71.128	SMB2	176 Tree Connect Request Tree: \\192.168.71.128\ADMIN\$
192.168.71.128	192.168.71.1	SMB2	131 Tree Connect Response, Error: STATUS_ACCESS_DENIED
192.168.71.1	192.168.71.128	SMB2	176 Tree Connect Request Tree: \\192.168.71.128\ADMIN\$
192.168.71.128	192.168.71.1	SMB2	131 Tree Connect Response, Error: STATUS_ACCESS_DENIED
192.168.71.1	192.168.71.128	SMB2	176 Tree Connect Request Tree: \\192.168.71.128\ADMIN\$
192.168.71.128	192.168.71.1	SMB2	131 Tree Connect Response, Error: STATUS_ACCESS_DENIED
192.168.71.1	192.168.71.128	SMB2	176 Tree Connect Request Tree: \\192.168.71.128\ADMIN\$

检查 admin \$、IPC\$，已经开启共享。

```
C:\Windows\system32>net share
```

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

命令成功完成。

尝试访问一下，果然是 admin\$ 访问不了，咋办呢（陷入沉思~~）

```
λ net use \\192.168.71.128\ipc$
密码或用户名在 \\192.168.71.128\ipc$ 无效。

为“192.168.71.128”输入用户名:
输入 192.168.71.128 的密码:
命令成功完成。

C:\User\...\Desktop
λ net use \\192.168.71.128\admin$
密码在 \\192.168.71.128\admin$ 无效。

为“192.168.71.128”输入用户名:
输入 192.168.71.128 的密码:
发生系统错误 5。

拒绝访问。
```

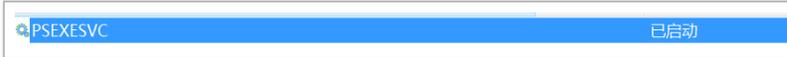
本地策略原因限制了访问？打来看看“网络访问、拒绝本地登陆、拒绝从网络远程访问这台计算机”的策略，没异常啊。不是策略，机制么？remote UAC？很大可能呀，不管，关了！



再运行 psexec:

```
λ .\PsExec64.exe \\192.168.71.128 -u : -p q 3 cmd  
PsExec v2.2 - Execute processes remotely  
Copyright (C) 2001-2016 Mark Russinovich  
Sysinternals - www.sysinternals.com  
Starting PSEXESVC service on 192.168.71.128...
```

哦豁，可以了，目标服务器被添加“PSEXESVC”服务。为什么关了 remote UAC 就可以了？（陷入了反思~）



UAC 是什么？UAC 是微软在 Windows Vista 以后版本引入的一种安全机制，可以阻止未经授权的应用程序自动进行安装，并防止无意中更改系统设置。那么对于防御是不是不改 UAC，保持默认或更高就可以了？并不是，可以改注册表的嘛。

方法二：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System 添加新 DWORD 值，键值：LocalAccountTokenFilterPolicy 为 1。

进一步分析

条件具备，软件正常，开始抓包分析。psexec 刚开始运行就做了三件事，第一：通过 TCP3 次握手连接目标 445 端口；第二：SMB 协商使用 SMBv2 协议通信；第三：进行 NTLM 认证。

Time	Source IP	Destination IP	Protocol	Details
208 9.948769	192.168.71.1	192.168.71.128	TCP	66 36831 -> 445 [SYN] Seq=0 Win=64288 Len=0 MSS=1460 WS=256 SACK_PERM=1
211 9.949288	192.168.71.128	192.168.71.1	TCP	66 445 -> 36831 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
212 9.949696	192.168.71.1	192.168.71.128	TCP	68 36831 -> 445 [ACK] Seq=1 Ack=1 Win=1051136 Len=0 TCP三次握手
213 9.949886	192.168.71.1	192.168.71.128	SMB2	210 NEGOTIATE_PROTOCOL_REQUEST 协商使用SMBV2协议
214 9.968596	192.168.71.128	192.168.71.1	SMB2	218 Negotiate Protocol Response
215 9.969684	192.168.71.1	192.168.71.128	SMB2	220 Session Setup Request, NTLMSSP_NEGOTIATE
216 9.978154	192.168.71.128	192.168.71.1	SMB2	481 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
217 9.972638	192.168.71.1	192.168.71.128	SMB2	671 Session Setup Request, NTLMSSP_AUTH, User: \yu NTLM认证
218 9.973966	192.168.71.128	192.168.71.1	SMB2	159 Session Setup Response

三次握手略过，直接分析 SMB 协议。SMB(全称是 Server MessageBlock) 是一个协议名，可用于在计算机间共享文件、打印机、串口等，电脑上的网上邻居就是靠它实现的，SMB 工作原理如下：攻击机向目标机器发送一个 SMB negotiate protocol request 请求数据包，并列出来它所支持的所有 SMB 协议版本（其中 Dialect 带有一串 16 进制的 code 对应着 SMB 的不同版本以此分辨

务, 并开始创建且运行了该服务程序。

```
v130 = 0;
SetConsoleCtrlHandler(HandlerRoutine, 1);
nSize = 260;
GetComputerNameW(&Buffer, &nSize);
v4 = wcsicmp(&Buffer, &::Buffer);
v5 = v133;
if ( !v4 )
    v5 = 1;
v133 = v5;
swprintf(&Dest, L"%s.exe", aPsexesvc);
v6 = L"PSEXESVC_ARM";
if ( byte_140030B6B != 1 )
    v6 = L"PSEXESVC";
if ( !sub_1400032E0(
    0,
    v1,
    aPsexesvc,
    (__int64)aPsexesvc,
    (__int64)&Dest,
    (__int64)v6,
    (__int64)&Str,
    (__int64)word_140056360,
    0,
    dword_14002E1EC,
    1)
    && (GetLastError() == 1460
    || !sub_1400032E0(
        0,
        v1,
        aPsexesvc,
        (__int64)aPsexesvc,
        (__int64)&Dest,
        (__int64)v6,
        (__int64)&v118,
        (__int64)&v117,
        0,
```

接着查看 openservicew request 的数据包，发现攻击机开始远程调用 svcctl 协议并打开 psexesvc 服务 (psexec 必须调用 svcctl 协议，否则 psexesvc 服务无法启动)

```
206 22.171570 192.168.71.128 192.168.71.1 SVCCTL 218 CloseServiceHandle response
207 22.172585 192.168.71.1 192.168.71.128 SVCCTL 258 OpenService request
208 22.175810 192.168.71.128 192.168.71.1 SVCCTL 218 OpenService response
209 22.176875 192.168.71.1 192.168.71.128 SVCCTL 230 StartService request
210 22.186758 192.168.71.128 192.168.71.1 SMB2 131 Ioctl Response, Error: STATUS_PENDING
211 22.215391 192.168.71.128 192.168.71.1 SVCCTL 198 StartService response
212 22.216363 192.168.71.1 192.168.71.128 TCP 60 25393 -> 445 [ACK] Seq=167731 Ack=3907 Win=1050368 Len=

Reserved: 0000
  Function: FSCTL_PIPE_TRANSCEIVE (0x0011c017)
  GUID handle file: svcctl
  Max Ioctl In Size: 0
  Max Ioctl Out Size: 1024
  Flags: 0x00000001
  .... 1 = Is FSCTL: True
Reserved: 00000000
1050 00 00 19 00 00 00 00 00 00 ff fe 00 00 31 00 .....
1060 00 00 15 00 00 00 04 00 00 00 00 00 00 00 .....
1070 00 00 00 00 00 00 00 00 00 39 00 00 00 17 c0 .....
1080 11 00 51 00 00 00 00 00 00 05 00 00 ff ff .....
1090 ff ff 78 00 00 00 50 00 00 00 00 00 00 78 00 .....
10a0 00 00 00 00 00 00 04 00 00 01 00 00 00 00 .....
10b0 00 00 05 00 00 03 10 00 00 50 00 00 00 06 00 .....
10c0 00 00 38 00 00 00 00 10 00 00 00 00 00 05 b1 .....
10d0 61 17 f3 1f d2 42 a5 25 26 Be e1 60 60 35 00 00 .....
10e0 00 00 00 00 00 00 09 00 00 50 00 53 00 45 00 .....
10f0 58 00 45 00 53 00 56 00 43 00 00 00 00 ff 01 .....
1100 0f 00 X E S V C .....
```

从代码层面看到，还需要创建与服务端通信的管道名。PsExec 使用命名管道可在同一台计算机的不同进程之间或在跨越一个网络的不同计算机的不同进程之间，支持可靠的、单向或双向的数据通信。

```

fwprintf(v12 + 2, L"\rConnecting with PsExec service on %s...", v1);
swprintf(&FileName, L"\\\\%s\\pipe\\%s", v1, apsexesvc);
do
{
    swprintf(&FileName, L"\\\\%s\\pipe\\%s-%d-stdin", v42, apsexesvc, &word_14005A580, dwFlagsAndAttributes);
    qword_14002E1F0 = (__int64)sub_1400047B0(&FileName, 0x40000000);
    if ( qword_14002E1F0 == -1 )
        v43 = GetLastError();
    LOWORD(dwFlagsAndAttributes) = GetCurrentProcessId();
    swprintf(&FileName, L"\\\\%s\\pipe\\%s-%d-stdout", v42, apsexesvc, &word_14005A580, dwFlagsAndAttributes);
    qword_14002E1F8 = (__int64)sub_1400047B0(&FileName, 0x80000000);
    if ( qword_14002E1F8 == -1 )
        v43 = GetLastError();
    LOWORD(dwFlagsAndAttributesb) = GetCurrentProcessId();
    swprintf(&FileName, L"\\\\%s\\pipe\\%s-%d-stderr", v42, apsexesvc, &word_14005A580, dwFlagsAndAttributesb);
    qword_14002E200 = (__int64)sub_1400047B0(&FileName, 0x80000000);
    if ( qword_14002E200 == -1 && !v43 )
        v43 = GetLastError();
}
while ( hFile == (HANDLE)-1i64 );
Mode = 2;
SetNamedPipeHandleState(v13, &Mode, 0i64, 0i64);

```

从数据包层发现开始创建 psexesvc、stdin、stdout、stderr 4 个命名管道。

192.168.71.1	192.168.71.128	SMB2	194	Ioctl Request FSCTL_PIPE_TRANSCEIVE File: PSEXESVC
192.168.71.128	192.168.71.1	SMB2	186	Ioctl Response FSCTL_PIPE_TRANSCEIVE File: PSEXESVC
192.168.71.1	192.168.71.128	SMB2	174	Write Request Len:4 Off:0 File: PSEXESVC

192.168.71.128	192.168.71.1	SMB2	154	Read Response
192.168.71.1	192.168.71.128	SMB2	264	Ioctl Request FSCTL_PIPE_WAIT Pipe: PSEXESVC-LAPTOP-NABCAK88-16756-stdin
192.168.71.128	192.168.71.1	SMB2	170	Ioctl Response FSCTL_PIPE_WAIT
192.168.71.1	192.168.71.128	SMB2	250	Create Request File: PSEXESVC-LAPTOP-NABCAK88-16756-stdin
192.168.71.128	192.168.71.1	SMB2	210	Create Response File: PSEXESVC-LAPTOP-NABCAK88-16756-stdin
192.168.71.1	192.168.71.128	SMB2	162	GetInfo Request FILE_INFO/SMB2_FILE_STANDARD_INFO File: PSEXESVC-LAPTOP-NABCAK88-16756-stdin
192.168.71.128	192.168.71.1	SMB2	154	GetInfo Response
192.168.71.1	192.168.71.128	SMB2	266	Ioctl Request FSCTL_PIPE_WAIT Pipe: PSEXESVC-LAPTOP-NABCAK88-16756-stdout
192.168.71.128	192.168.71.1	SMB2	170	Ioctl Response FSCTL_PIPE_WAIT
192.168.71.1	192.168.71.128	SMB2	252	Create Request File: PSEXESVC-LAPTOP-NABCAK88-16756-stdout
192.168.71.128	192.168.71.1	SMB2	210	Create Response File: PSEXESVC-LAPTOP-NABCAK88-16756-stdout
192.168.71.1	192.168.71.128	SMB2	162	GetInfo Request FILE_INFO/SMB2_FILE_STANDARD_INFO File: PSEXESVC-LAPTOP-NABCAK88-16756-stdout
192.168.71.128	192.168.71.1	SMB2	154	GetInfo Response
192.168.71.1	192.168.71.128	SMB2	266	Ioctl Request FSCTL_PIPE_WAIT Pipe: PSEXESVC-LAPTOP-NABCAK88-16756-stderr
192.168.71.128	192.168.71.1	SMB2	170	Ioctl Response FSCTL_PIPE_WAIT
192.168.71.1	192.168.71.128	SMB2	252	Create Request File: PSEXESVC-LAPTOP-NABCAK88-16756-stderr

管道创建成功，psexec 可以正常使用，已成功连上目标机器 cmd。

```

.\PsExec64.exe \\192.168.71.128 -u qv -p qw 3 cmd

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Windows\system32>

```

在连接过程中，攻击机会每隔 30s 向目标机器发送一次

TCP-keep-alive 数据包，保持 TCP 心跳连接。

17956	697407	192.168.71.1	192.168.71.128	TCP	60	[TCP Keep-Alive]	4818 → 445 [ACK] Seq=27138 Ack=6418 Win=10506
17956	697436	192.168.71.128	192.168.71.1	TCP	66	[TCP Keep-Alive ACK]	445 → 4818 [ACK] Seq=6418 Ack=27139 Win=6
17986	712851	192.168.71.1	192.168.71.128	TCP	60	[TCP Keep-Alive]	4818 → 445 [ACK] Seq=27138 Ack=6418 Win=10506
17986	712878	192.168.71.128	192.168.71.1	TCP	66	[TCP Keep-Alive ACK]	445 → 4818 [ACK] Seq=6418 Ack=27139 Win=6
18016	712733	192.168.71.1	192.168.71.128	TCP	60	[TCP Keep-Alive]	4818 → 445 [ACK] Seq=27138 Ack=6418 Win=10506
18016	712754	192.168.71.128	192.168.71.1	TCP	66	[TCP Keep-Alive ACK]	445 → 4818 [ACK] Seq=6418 Ack=27139 Win=6

攻击机退出远程连接时，tcp 四次挥手关闭连接，psexesvc、stdin、stdout、stderr4 个管道也会关闭，会话结束。

192.168.71.128	192.168.71.1	TCP	54	445 → 4818 [ACK] Seq=7594 Ack=28835 Win=65280 Len=0
192.168.71.128	192.168.71.1	SMB2	182	Close Response
192.168.71.128	192.168.71.1	SMB2	182	Close Response
192.168.71.1	192.168.71.128	TCP	60	4818 → 445 [ACK] Seq=28835 Ack=7850 Win=1050880 Len=0
192.168.71.1	192.168.71.128	SMB2	171	Read Request Len:4 Off:0 File: PSEXESVC
192.168.71.128	192.168.71.1	SMB2	142	Read Response
192.168.71.1	192.168.71.128	SMB2	171	Read Request Len:19040 Off:0 File: PSEXESVC
192.168.71.128	192.168.71.1	TCP	102.	445 → 4818 [ACK] Seq=7938 Ack=29069 Win=65280 Len=10220 [TCP
192.168.71.1	192.168.71.128	TCP	60	4818 → 445 [ACK] Seq=29069 Ack=18158 Win=1051136 Len=0
192.168.71.128	192.168.71.1	SMB2	8958	Read Response
192.168.71.1	192.168.71.128	TCP	60	4818 → 445 [ACK] Seq=29069 Ack=27062 Win=1051136 Len=0
192.168.71.1	192.168.71.128	SMB2	146	Close Request File: PSEXESVC
192.168.71.128	192.168.71.1	SMB2	182	Close Response
192.168.71.1	192.168.71.128	SMB2	146	Close Request File: PSEXESVC-LAPTOP-NABCAK88-18744-stdin
192.168.71.128	192.168.71.1	SMB2	182	Close Response
192.168.71.1	192.168.71.128	TCP	60	4818 → 445 [ACK] Seq=29253 Ack=27318 Win=1050880 Len=0
192.168.71.1	192.168.71.128	SMB2	126	Tree Disconnect Request
192.168.71.128	192.168.71.1	SMB2	126	Tree Disconnect Response
192.168.71.1	192.168.71.128	SMB2	126	Session Logoff Request
192.168.71.128	192.168.71.1	SMB2	126	Session Logoff Response

psexec 成功登录退出后，会在目标机器的安全日志中产生 Event 4624、4628、4634，在系统日志中产生 Event 7045（记录 PSEXESVC 安装）、Event 7036（记录 PSEXESVC 服务状态）。



另外，当 psexec 远控目标机器时，可执行程序 PSEXESVC.EXE 被提取至目标机器的 C:Windows 目录下，然后再执行远程操作命令，psexec 断开后，目标机器 C:Windows 目录下的 PSEXESVC.EXE 被删除。

pexec 连接成功，打开目标机器 cmd，可执行 cmd 相关命令，还有其它相关命令：

```
psexec \\ip -u administrator -p 123456 -d -s calc
```

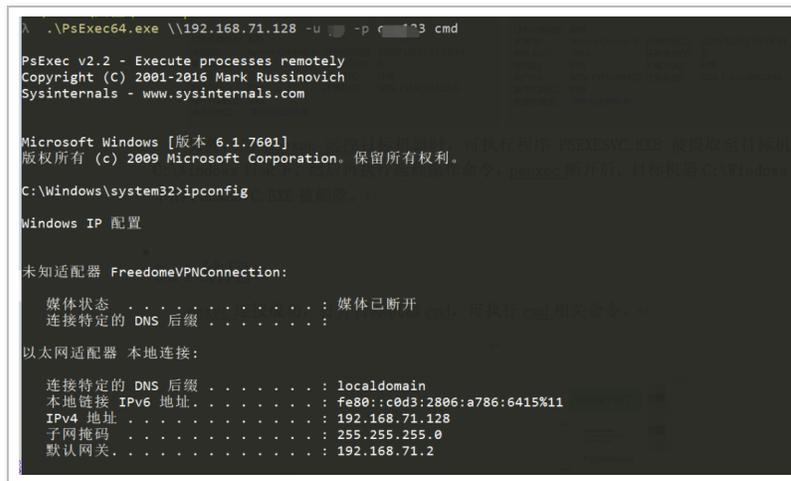
运行 calc 后返回，目标机器上会有一个 calc 进程，-s 意思是以系统身份运行。窗口是看不到的，如果需要目标机器看到这个窗口，需要加参数 -i。

```
psexec \\ip -u administrator -p 123456 -d calc
```

以当前身份运行 calc，然后返回。

```
psexec \\ip -u administrator -p 123456 -i -d cmd /c st
```

以目标机器当前用户身份打开百度网页，并让他看到这个网页。



```
λ .\PsExec64.exe \\192.168.71.128 -u [redacted] -p [redacted] 123 cmd
PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Windows\system32>ipconfig

Windows IP 配置

未知适配器 FreedomVPNConnection:

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

以太网适配器 本地连接:

    连接特定的 DNS 后缀 . . . . . : localdomain
    本地链接 IPv6 地址 . . . . . : fe80::c0d3:2806:a786:6415%11
    IPv4 地址 . . . . . : 192.168.71.128
    子网掩码 . . . . . : 255.255.255.0
    默认网关 . . . . . : 192.168.71.2
```

结尾



如果运营过程发现安全设备有 psexec 相关告警，检查的时候围绕着 psexec 的特性针对性地对数据包进行检查，发现误报及时添加相关白名单过滤持续性的安全运营，能显著地提高安全运营能力。

本文作者： 酒仙桥六号部队

本文为安全脉搏专栏作者发布，转载请注明：

<https://www.secpulse.com/archives/146441.html>

全文完

本文由 简悦 SimpRead 优化，用以提升阅读体验

使用了 全新的简悦词法分析引擎 beta，点击查看详细说明

