**借用UAC完成的提权思路分享**

<http://static.hx99.net/static/drops/tips-8989.html>

# 提权过程概述

目标程序，查找其动态加载的dll文件然后将其替换掉，插入我们包含shellcode的dll文件，这样用户在安装此文件的时候就会调用我们的dll文件，并执行我们的shellcode代码。

**0x02 实验环境**

*Kali Debian7*

Kali集成Metasploit等漏洞利用工具，方便提取shellcode和反弹TCP连接。最好安装一个Mingw-w64用于编译c代码。

*windows7 x64*

主要的目标测试环境。

*Procmon.exe*

Procmon是微软出的一款强大的Windows监视工具，不但可以监视进程/线程，还可以监控到文件系统，注册表的变化等。

*install\_flashplayer15x32\_mssd\_aaa\_aih*

这里我们以flashplayer安装文件作为目标文件，版本为15x32\_mssd\_aaa\_aih，可自行下载，或者从最后的打包附件中找到。