快速通道

文档分类
- 红盟公告
- 新手上路 <=
- 漏洞分析
- 工具介绍
- 安全配置
- 编程技术
- 安全技术
- 业界动态

本类热门
- ftp使用经典
- 一个木马的查杀过程
- 基于arp欺骗的网络攻击程序(BtNet.exe)
- 终端服务全攻略
- 握着你的“手”清除DLL后门
- 巧用asp木马和KV2004得到管理员权限

巧用asp木马和KV2004得到管理员权限

提交文章： jimmy415
提交日期： 2004-05-27
文章属性： 原创
文档类别： 新手上路
浏览次数： 今10次/总10109次

重来没写过什么文章，这是第一次，写的不好请大家原谅，高手也不要取笑哦。这里也没什么技术可言，只是我这个菜鸟的一点心得，ok开始。。。
前段时间动网的UPfile.asp漏洞可谓闹的沸沸扬扬，这个漏洞确实很厉害，相信不少新手和我一样种了不少后门在有动网的网站上，但是asp木马的权限确实很底，除了删点文章，删点图片好象没什么用了。不行不得到管理员权限简直就辜负了发现这个漏洞的高手们~v~。好，想办法提升权限，我找啊找！网上提升权限的方法几乎都用过了，都没什么用，补丁打的很全啊！接下来用findpass想解开管理员的密码，又失败，findpass要管理员权限才有用。用pslist看看晕装的是瑞星+天网，网上的大部分工具遇上这个防御组合一般都没用了。种木马？不行一来
权限太底，二来在瑞星杀天网堵的包围下很少能活出来的。做个添加用户权限的bat文件想放到启动组中去，这个方法虽然有点傻但是有一定的可行性，晕又是权限不够加不进去。c盘下的"Program Files" "winnt" "Documents and Settings"三个文件甲都没有写权限，更不要说注册表了。郁闷了，给管理员留了句话，然后匆匆下线。
第2天上来一看，嘿嘿图被改回来了，管理员应该发现了，这次更不容易得手。登上asp木马进去看了一下，昨天传上去的几个exe被删了，还好asp木马活下来了，咦！c盘多了文件甲叫KV2004，原来管理员把瑞星卸了，安了个kv2004，进Program Files看看确实瑞星被卸了。（这里说一下，大部分的杀毒软件默认的安装路径c:\Program Files\,但是kv默认的安装路径是c:\kv2004\）到这里机会就来了我们可以把执行文件捆绑在kv2004上，跟随kv一起启动。因为kv不在"Program Files" "winnt" "Documents and Settings"这三个文件甲中，很大可能我可以修改

或者上传文件。行动！在kv2004下随便找个htm文件删除：(看看有无写删权限）
C:\>del c:\kv2004\GetLicense.htm
拒绝访问

奇怪了，再来看看文件甲属性
C:\>attrib c:\kv2004
S R C:\KV2004

哦是只读。
C:\>attrib -r -s c:\kv2004

ok！在试试
C:\>del c:\kv2004\GetLicense.htm

成功了！好写个起用帐号和提升权限的bat文件，然后把bat文件和kv2004的系统服务文件KVSrvXP.exe捆绑起来，（注意多下种捆绑器，捆绑一

次用kv2004来扫描一次，因为很多捆绑器生成的文件kv会把他作为病毒来处理掉）准备上传了，先删掉原来的KVSrvXP.exe。
C:\>del c:\kv2004\KVSrvXP.exe

拒绝访问

可能是KVSrvXP.exe被windows调用中，删不掉。没办法了吗？不，删不掉我改名
C:\>ren c:\kv2004\KVSrvXP.exe kv.exe

OK!然后用asp木马把修改了的KVSrvXP.exe上传到kv2004中，接下来就去睡觉把。
4个小时后登上来用：
net user 起用的帐户

已经在administrators组中，接下来要关防火墙，关杀毒软件，还是种木马你随便我了，哈哈！
我觉得入侵没什么固定的模式，具体情况具体分析，杀毒软件同样也可以帮我们忙，这里我只提供了一种思路。请大家指教。
-----jimmy415

返回上页

Copyright © 2000-2004 **HUC** All Rights Reserved.
中国红客网络技术联盟 www.cnhonker.com
webmaster@cnhonker.net