Window 服务器安全设置

- ✓ 出处：站长百科
- ✓ 原文地址：http://www.zzbaike.com/wiki/Window_服务器安全设置
- ✓ 本电子书整理自站长百科 Window_服务器安全设置词条，查看内容请访问网站。

目录

✓ *出处：站长百科*
✓ *原文地址：http://www.zzbaike.com/wiki/Window_服务器安全设置*
✓ *本电子书整理自站长百科 Window_服务器安全设置词条，查看内容请访问网站*

第一节 安装补丁

安装好操作系统之后，最好能在托管之前就完成补丁的安装，配置好网络后，如果是2000则确定安装上了SP4，如果是2003，则最好安装上SP1，然后点击开始→Windows Update，安装所有的关键更新。

第二节 安装杀毒软件

虽然杀毒软件有时候不能解决问题，但是杀毒软件避免了很多问题。我一直在用诺顿2004，据说2005可以杀木马，不过我没试过。还有人用瑞星，瑞星是确定可以杀木马的。更多的人说卡巴司机好，不过我没用过。

不要指望杀毒软件杀掉所有的木马，因为ASP木马的特征是可以通过一定手段来避开杀毒软件的查杀。

第三节 设置端口保护和防火墙、删除默认共享

都是服务器防黑的措施，即使你的服务器上没有IIS，这些安全措施都最好做上。这是阿江的盲区，大概知道屏蔽端口用本地安全策略，不过这方面的东西网上攻略很多，大家可以撅出来看看，晚些时候我或者会复制一些到我的网站上。

第四节 权限设置

这是防止 ASP 漏洞攻击的关键所在，优秀的权限设置可以将危害减少在一个 IIS 站点甚至一个虚拟目录里。我这里讲一下原理和设置思路，聪明的朋友应该看完这个就能解决问题了。

权限设置的原理

WINDOWS用户，在WINNT系统中大多数时候把权限按用户（组）来划分。在【开始→程序→管理工具→计算机管理→本地用户和组】管理系统用户和用户组。NTFS权限设置，请记住分区的时候把所有的硬盘都分为NTFS分区，然后我们可以确定每个分区对每个用户开放的权限。【文件（夹）上右键→属性→安全】在这里管理NTFS文件（夹）权限。 IIS匿名用户，每个IIS站点或者虚拟目录，都可以设置一个匿名访问用户（现在暂且把它叫“IIS匿名用户”），当用户访问你的网站的.ASP文件的时候，这个.ASP文件所具有的权限，就是这个“IIS匿名用户”所具有的权限。

第五节 权限设置的思路

要为每个独立的要保护的个体（比如一个网站或者一个虚拟目录）创建一个系统用户，让这个站点在系统中具有惟一的可以设置权限的身份。

在 IIS 的【站点属性或者虚拟目录属性→目录安全性→匿名访问和验证控制→编辑→匿名访问→编辑】填写刚刚创建的那个用户名。

设置所有的分区禁止这个用户访问，而刚才这个站点的主目录对应的那个文件夹设置允许这个用户访问（要去掉继承父权限，并且要加上超管组和 SYSTEM 组）。这样设置了之后，这个站点里的 ASP 程序就只有当前这个文件夹的权限了，从探针上看，所有的硬盘都是红叉叉。

第六节 设置方法

我是先创建一个用户组，以后所有的站点的用户都建在这个組里，然后设置这个组在各个分区没病权限。然后再设置各个IIS用户在各在的文件夹里的权限。

因为比较多，所以我很不想写，其实知道了上面的原理，大多数人都应该懂了，除非不知道怎么添加系统用户和組，不知道怎么设置文件夹权限，不知道IIS站点属性在那里。真的有那样的人，你也不要着急，要沉住气慢慢来，具体的方法其实自己也能摸索出来的，我就是这样。当然，如果我有空，我会写我的具体设置方法，很傲能还会配上图片。

第七节 改名或卸载不安全组件

最危险的组件是 WSH 和 Shell，因为它可以运行你硬盘里的 EXE 等程序，比如它可以运行提升程序来提升 SERV-U 权限甚至用 SERVU 来运行更高权限的系统程序。

第八节 卸载最不安全的组件

最简单的办法是直接卸载后删除相应的程序文件。将下面的代码保存为一个.BAT 文件，复制内容到剪贴板代码:

```
regsvr32/u C:\WINNT\System32\wshom.ocx
del C:\WINNT\System32\wshom.ocx
regsvr32/u C:\WINNT\system32\shell32.dll
del C:\WINNT\system32\shell32.dll
```

然后运行一下，WScript.Shell, Shell.application, WScript.Network 就会被卸载了。可能会提示无法删除文件，不用管它，重启一下服务器，你会发现这三个都提示“×安全”了。

第九节 改名不安全组件

需要注意的是组件的名称和 Clsid 都要改，并且要改彻底了。下面以 Shell.application 为例来介绍方法。

打开注册表编辑器【开始→运行→regedit 回车】，然后【编辑→查找→填写 Shell.application→查找下一个】，用这个方法能找到两个注册表项：

“{13709620-C279-11CE-A49E-444553540000}”和“Shell.application”。为了确保万无一失，把这两个注册表项导出来，保存为 .reg 文件。

比如我们想做这样的更改复制内容到剪贴板代码:

regsvr32/u C:\WINNT\System32\wshom.ocx

del C:\WINNT\System32\wshom.ocx

regsvr32/u C:\WINNT\system32\shell32.dll

del C:\WINNT\system32\shell32.dll 然后运行一下，WScript.Shell, Shell.application, WScript.Network 就会被卸载了。可能会提示无法删除文件，不用管它，重启一下服务器，你会发现这三个都提示“×安全”了。

改名不安全组件

需要注意的是组件的名称和 Clsid 都要改，并且要改彻底了。下面以 Shell.application 为例来介绍方法。

打开注册表编辑器【开始→运行→regedit 回车】，然后【编辑→查找→填写 Shell.application→查找下一个】，用这个方法能找到两个注册表项：“{13709620-C279-11CE-A49E-444553540000}”和“Shell.application”。为了确保万无一失，把这两个注册表项导出来，保存为 .reg 文件。

比如我们想做这样的更改复制内容到剪贴板代码:

13709620-C279-11CE-A49E-444553540000 改名为 13709620-C279-11CE-A49E-444553540001

Shell.application 改名为 Shell.application_ajiang 那么，就把刚才导出的.reg 文件里的内容按上面的对应关系替换掉，然后把修改好的.reg 文件导入到注册表中（双击即可），导入了改名后的注册表项之后，别忘记了删除原有的那两个项目。这里需要注意一点，Clsid 中只能是十个数字和 ABCDEF 六个字母。

下面是我修改后的代码（两个文件我合到一起了）：复制内容到剪贴板代码:

Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\CLSID\{13709620-C279-11CE-A49E-444553540001}]

@="Shell Automation Service"

[HKEY_CLASSES_ROOT\CLSID\{13709620-C279-11CE-A49E-444553540001}\InProcServer32]

@="C:\\WINNT\\system32\\shell32.dll"

"ThreadingModel"="Apartment"

[HKEY_CLASSES_ROOT\CLSID\{13709620-C279-11CE-A49E-444553540001}\ProgID]

@="Shell.Application_ajiang.1"

[HKEY_CLASSES_ROOT\CLSID\{13709620-C279-11CE-A49E-444553540001}\TypeLib]

@="{50a7e9b0-70ef-11d1-b75a-00a0c90564fe}"

[HKEY_CLASSES_ROOT\CLSID\{13709620-C279-11CE-A49E-444553540001}\Version]

@="1.1"

[HKEY_CLASSES_ROOT\CLSID\{13709620-C279-11CE-A49E-444553540001}\VersionIndependentProgID]

@="Shell.Application_ajiang"

[HKEY_CLASSES_ROOT\Shell.Application_ajiang]

@="Shell Automation Service"

[HKEY_CLASSES_ROOT\Shell.Application_ajiang\CLSID]

@="{13709620-C279-11CE-A49E-444553540001}"

[HKEY_CLASSES_ROOT\Shell.Application_ajiang\CurVer]

@="Shell.Application_ajiang.1" 然后运行一下， WScript.Shell, Shell.application, WScript.Network 就会被卸载了。可能会提示无法删除文件，不用管它，重启一下服务器，你会发现这三个都提示“×安全”了。

第十节 改名不安全组件注意

需要注意的是组件的名称和 Clsid 都要改，并且要改彻底了。下面以 Shell.application 为例来介绍方法。

打开注册表编辑器【开始→运行→regedit 回车】，然后【编辑→查找→填写 Shell.application→查找下一个】，用这个方法能找到两个注册表项：

“{13709620-C279-11CE-A49E-444553540000}”和“Shell.application”。为了确保万无一失，把这两个注册表项导出来，保存为 .reg 文件。

比如我们想做这样的更改

你可以把这个保存为一个.reg 文件运行试一下，但是可别就此了事，因为万一黑客也看了我的这篇文章，他会试验我改出来的这个名字的。

防止列出用户组和系统进程

利用 getobject("WINNT")获得了系统用户和系统进程的列表，这个列表可能会被黑客利用，我们应当隐藏起来，方法是：

【开始→程序→管理工具→服务】，找到 Workstation，停止它，禁用它。

第十一节 防止Serv-U权限提升

其实，注销了 Shell 组件之后，侵入者运行提升工具的可能性就很小了，但是 prel 等别的脚本语言也有 shell 能力，为防万一，还是设置一下为好。

用 Ultraedit 打开 ServUDaemon.exe 查找 Ascii：LocalAdministrator，和 #l@$ak#.lk;O@P，修改成等长度的其它字符就可以了，ServUAdmin.exe 也一样处理。

另外注意设置 Serv-U 所在的文件夹的权限，不要让 IIS 匿名用户有读取的权限，否则人家下走你修改过的文件，照样可以分析出你的管理员名和密码。

第十二节 利用ASP漏洞攻击的常见方法及防范

一般情况下，黑客总是瞄准论坛等程序，因为这些程序都有上传功能，他们很容易的就可以上传ASP木马，即使设置了权限，木马也可以控制当前站点的所有文件了。另外，有了木马就然后用木马上传提升工具来获得更高的权限，我们关闭shell组件的目的很大程度上就是为了防止攻击者运行提升工具。

如果论坛管理员关闭了上传功能，则黑客会想办法获得超管密码，比如，如果你用动网论坛并且数据库忘记了改名，人家就可以直接下载你的数据库了，然后距离找到论坛管理员密码就不远了。

作为管理员，我们首先要检查我们的ASP程序，做好必要的设置，防止网站

被黑客进入。另外就是防止攻击者使用一个被黑的网站来控制整个服务器，因为如果你的服务器上还为朋友开了站点，你可能无法确定你的朋友会把他上传的论坛做好安全设置。这就用到了前面所说的那一大堆东西，做了那些权限设置和防提升之后，黑客就算是进入了一个站点，也无法破坏这个网站以外的东西。

更多电子书

站长常用工具：

Alexa查询：http://alexa.zzbaike.com/ Alexa中文专题站 Alexa工具条下载

关键词排名检索工具：http://keywordsrank.zzbaike.com/

在线FTP工具：http://webftp.zzbaike.com/

PR查询工具：http://pr.zzbaike.com/

关键词密度检测工具：http://keywords.zzbaike.com/

收录数量查询：http://indexed.zzbaike.com/

Whois查询：http://whois.zzbaike.com/

反向链接查询：http://linksincount.zzbaike.com/

Gzip查询工具：http://gzip.zzbaike.com

站长百科免费美国空间

freehost4life美国免费空间（http://www.freehost4life.com)， 服务器位于softlayer的达拉斯机房，是中国访问速度最快的美国主机之一。

- ✓ *出处：站长百科*
- ✓ *原文地址：http://www.zzbaike.com/wiki/Window 服务器安全设置*
- ✓ *本电子书整理自站长百科Window 服务器安全设置词条，查看内容请访问网站*

站长百科 1 美元银币竞价活动

每周总共举行 3 次美元竞价：http://bbs.zzbaike.com/forum-45-1.html

SEO 优化教程

SEO 方面的知识有很多，对于新手来说，如果你不知道，不清楚这方面的知识，那么，你可以看看这两部搜索引擎指南：

SEO搜索引擎优化基础教程：http://bbs.zzbaike.com/thread-9952-1-1.html

SEO搜索引擎优化高级教程：http://bbs.zzbaike.com/thread-12692-1-1.html

WordPress 开发文档

wordpress的中文翻译文档http://www.wordpress.la/codex.html，wordpress开发的相关知识都有，对WordPress开发感兴趣的博主会有一定的用处。

WordPress免费主题：http://www.wordpress.la/theme.html

WordPress免费插件：http://www.wordpress.la/plugin.html

WordPress主题制作电子书：http://bbs.zzbaike.com/thread-9954-1-1.html

1. Apache2.2 中文文档电子书（PDF+在线版）http://bbs.zzbaike.com/thread-9955-1-1.html
2. IXWeHosting 控制面板使用手册(在线版+PDF 电子书)
   http://bbs.zzbaike.com/thread-9953-1-1.html

更多电子书下载：http://down.zzbaike.com/ebook/

视频教程：

1. 美国主机 IXWebHosting 使用视频教程（在线观看及下载）
   http://bbs.zzbaike.com/thread-47008-1-1.html
2. Godaddy 主机及域名使用视频教程（在线观看及下载）
   http://bbs.zzbaike.com/thread-50005-1-1.html

如果您有站长类电子书，请到这里与我们分享：
http://bbs.zzbaike.com/forum-69-1.html
发电子书得金币，兑换礼品/主机/域名/文化衫

- ✓ *出处：站长百科*
- ✓ *原文地址：http://www.zzbaike.com/wiki/Window 服务器安全设置*
- ✓ *本电子书整理自站长百科Window 服务器安全设置词条，查看内容请访问网站*

详情见： http://bbs.zzbaike.com/thread-23156-1-1.html

站长百科感谢您下载阅读，多谢支持！