IIS Web服务器安全加固步骤:

<table>
<tr><th></th><th>步骤</th><th>注意:</th></tr>
<tr><td>❑</td><td>安装和配置 Windows Server 2003。</td><td>
1. 将<systemroot>\System32\cmd.exe转移到其他目录或更名;
2. 系统帐号尽量少,更改默认帐户名(如Administrator)和描述,密码尽量复杂;
3. 拒绝通过网络访问该计算机(匿名登录;内置管理员帐户;Support_388945a0;Guest;所有非操作系统服务帐户)
4. 建议对一般用户只给予读取权限,而只给管理员和System以完全控制权限,但这样做有可能使某些正常的脚本程序不能执行,或者某些需要写的操作不能完成,这时需要对这些文件所在的文件夹权限进行更改,建议在做更改前先在测试机器上作测试,然后慎重更改。
5. NTFS文件权限设定(注意文件的权限优先级别比文件夹的权限高):
<table>
<tr><th>文件类型</th><th>建议的 NTFS 权限</th></tr>
<tr><td>CGI 文件(.exe、.dll、.cmd、.pl)
脚本文件 (.asp)
包含文件(.inc、.shtm、.shtml)
静态内容(.txt、.gif、.jpg、.htm、.html)</td><td>Everyone(执行)
Administrators(完全控制)
System(完全控制)</td></tr>
</table>
6. 禁止C$、D$一类的缺省共享
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters
AutoShareServer、REG_DWORD、0x0
7. 禁止ADMIN$缺省共享
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters
AutoShareWks、REG_DWORD、0x0
8. 限制IPC$缺省共享
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
restrictanonymous REG_DWORD 0x0 缺省
</td></tr>
</table>

		0x1 匿名用户无法列举本机用户列表 0x2 匿名用户无法连接本机IPC$共享 说明:不建议使用2,否则可能会造成你的一些服务无法启动,如SQL Server 9. 仅给用户真正需要的权限,权限的最小化原则是安全的重要保障 10. 在本地安全策略->审核策略中打开相应的审核,推荐的审核是: 账户管理 成功 失败 登录事件 成功 失败 对象访问 失败 策略更改 成功 失败 特权使用 失败 系统事件 成功 失败 目录服务访问 失败 账户登录事件 成功 失败 审核项目少的缺点是万一你想看发现没有记录那就一点都没辙;审核项目太多不仅会占用系统资源而且会导致你根本没空去看,这样就失去了审核的意义。与之相关的是: 在账户策略->密码策略中设定: 密码复杂性要求 启用 密码长度最小值 6位 强制密码历史 5次 最长存留期 30天 在账户策略->账户锁定策略中设定: 账户锁定 3次错误登录 锁定时间 20分钟 复位锁定计数 20分钟

		11. 在Terminal Service Configration(远程服务配置)-权限-高级中配置安全审核，一般来说只要记录登录、注销事件就可以了。 12. 解除NetBios与TCP/IP协议的绑定 控制面版——网络——绑定——NetBios接口——禁用 2000:控制面版——网络和拨号连接——本地网络——属性——TCP/IP——属性——高级——WINS——禁用TCP/IP上的NETBIOS 13. 在网络连接的协议里启用TCP/IP筛选，仅开放必要的端口(如80) 14. 通过更改注册表Local_Machine\System\CurrentControlSet\Control\LSA-RestrictAnonymous = 1来禁止139空连接 15. 修改数据包的生存时间(TTL)值 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters DefaultTTL REG_DWORD 0-0xff(0-255 十进制,默认值128) 16. 防止SYN洪水攻击 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters SynAttackProtect REG_DWORD 0x2(默认值为0x0) 17. 禁止响应ICMP路由通告报文 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\interface PerformRouterDiscovery REG_DWORD 0x0(默认值为0x2) 18. 防止ICMP重定向报文的攻击 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters EnableICMPRedirects REG_DWORD 0x0(默认值为0x1) 19. 不支持IGMP协议 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters IGMPLevel REG_DWORD 0x0(默认值为0x2) 20. 设置arp缓存老化时间设置 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services:\Tcpip\Parameters ArpCacheLife REG_DWORD 0-0xFFFFFFFF(秒数,默认值为120秒)

ArpCacheMinReferencedLife REG_DWORD 0-0xFFFFFFFF(秒数,默认值为600)

21. 禁止死网关监测技术

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services:\Tcpip\Parameters
EnableDeadGWDetect REG_DWORD 0x0(默认值为ox1)

22. 不支持路由功能

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services:\Tcpip\Parameters
IPEnableRouter REG_DWORD 0x0(默认值为0x0)

❑ **安装和配置 IIS 服务:**

1. 仅安装必要的 IIS 组件。(禁用不需要的如FTP 和 SMTP 服务)
2. 仅启用必要的服务和 Web Service 扩展, 推荐配置:

UI 中的组件名称	设置	设置逻辑
后台智能传输服务 (BITS) 服务器扩展	启用	BITS 是 Windows Updates 和"自动更新"所使用的后台文件传输机制。如果使用 Windows Updates 或"自动更新"在 IIS 服务器中自动应用 Service Pack 和热修补程序, 则必须有该组件。
公用文件	启用	IIS 需要这些文件, 一定要在 IIS 服务器中启用它们。
文件传输协议 (FTP) 服务	禁用	允许 IIS 服务器提供 FTP 服务。专用 IIS 服务器不需要该服务。
FrontPage 2002 Server Extensions	禁用	为管理和发布 Web 站点提供 FrontPage 支持。如果没有使用 FrontPage 扩展的 Web 站点, 请在专用 IIS 服务器中禁用该组件。
Internet 信息服务管理器	启用	IIS 的管理界面。
Internet 打印	禁用	提供基于 Web 的打印机管理, 允许通过 HTTP 共享打印机。专用 IIS 服务器不需要该组件。
NNTP 服务	禁用	在 Internet 中分发、查询、检索和投递 Usenet 新闻文章。专用 IIS 服务器不需要该组件。
SMTP 服务	禁用	支持传输电子邮件。专用 IIS 服务器不需要该组件。

万维网服务	启用	为客户端提供 Web 服务、静态和动态内容。专用 IIS 服务器需要该组件。

万维网服务子组件

UI 中的组件名称	安装选项	设置逻辑
Active Server Page	启用	提供 ASP 支持。如果 IIS 服务器中的 Web 站点和应用程序都不使用 ASP，请禁用该组件；或使用 Web 服务扩展禁用它。
Internet 数据连接器	禁用	通过扩展名为 .idc 的文件提供动态内容支持。如果 IIS 服务器中的 Web 站点和应用程序都不包括 .idc 扩展文件，请禁用该组件；或使用 Web 服务扩展禁用它。
远程管理 (HTML)	禁用	提供管理 IIS 的 HTML 界面。改用 IIS 管理器可使管理更容易，并减少了 IIS 服务器的攻击面。专用 IIS 服务器不需要该功能。
远程桌面 Web 连接	禁用	包括了管理终端服务客户端连接的 Microsoft ActiveX® 控件和范例页面。改用 IIS 管理器可使管理更容易，并减少了 IIS 服务器的攻击面。专用 IIS 服务器不需要该组件。
服务器端包括	禁用	提供 .shtm、.shtml 和 .stm 文件的支持。如果在 IIS 服务器中运行的 Web 站点和应用程序都不使用上述扩展的包括文件，请禁用该组件。
WebDAV	禁用	WebDAV 扩展了 HTTP/1.1 协议，允许客户端发布、锁定和管理 Web 中的资源。专用 IIS 服务器禁用该组件；或使用 Web 服务扩展禁用该组件。
万维网服务	启用	为客户端提供 Web 服务、静态和动态内容。专用 IIS 服务器需要该组件

3. 将IIS目录&数据与系统磁盘分开，保存在专用磁盘空间内。
4. 在IIS管理器中删除必须之外的任何没有用到的映射(保留asp等必要映射即可)
5. 在IIS中将HTTP404 Object Not Found出错页面通过URL重定向到一个定制HTM文件
6. Web站点权限设定(建议)

Web 站点权限：	授予的权限：
读	允许

<table>
<tr><td></td><td></td><td>
<table>
<tr><td>写</td><td>不允许</td></tr>
<tr><td>脚本源访问</td><td>不允许</td></tr>
<tr><td>目录浏览</td><td>建议关闭</td></tr>
<tr><td>日志访问</td><td>建议关闭</td></tr>
<tr><td>索引资源</td><td>建议关闭</td></tr>
<tr><td>执行</td><td>推荐选择“仅限于脚本”</td></tr>
</table>
7. 建议使用W3C扩充日志文件格式，每天记录客户IP地址，用户名，服务器端口，方法，URI字根，HTTP状态，用户代理，而且每天均要审查日志。(最好不要使用缺省的目录，建议更换一个记日志的路径，同时设置日志的访问权限，只允许管理员和system为Full Control)。
8. 程序安全：
1) 涉及用户名与口令的程序最好封装在服务器端，尽量少的在ASP文件里出现，涉及到与数据库连接地用户名与口令应给予最小的权限；
2) 需要经过验证的ASP页面，可跟踪上一个页面的文件名，只有从上一页面转进来的会话才能读取这个页面。
3) 防止ASP主页.inc文件泄露问题；
4) 防止UE等编辑器生成some.asp.bak文件泄露问题。</td></tr>
<tr><td>❑</td><td>安全更新。</td><td>应用所需的所有 Service Pack 和 定期手动更新补丁。</td></tr>
<tr><td>❑</td><td>安装和配置防病毒保护。</td><td>推荐NAV 8.1以上版本病毒防火墙(配置为至少每周自动升级一次)。</td></tr>
<tr><td>❑</td><td>安装和配置防火墙保护。</td><td>推荐最新版BlackICE Server Protection防火墙(配置简单，比较实用)</td></tr>
<tr><td>❑</td><td>监视解决方案。</td><td>根据要求安装和配置 MOM代理或类似的监视解决方案。</td></tr>
<tr><td>❑</td><td>加强数据备份。</td><td>Web数据定时做备份，保证在出现问题后可以恢复到最近的状态。</td></tr>
<tr><td>❑</td><td>考虑实施 IPSec 筛选器。</td><td>用 IPSec 过滤器阻断端口
Internet 协议安全性 (IPSec)
过滤器可为增强服务器所需要的安全级别提供有效的方法。本指南推荐在指南中定义的高安全性环境中使用该选项，以便进一步减少服务器的受攻击面。
有关使用 IPSec 过滤器的详细信息，请参阅模块其他成员服务器强化过程。</td></tr>
</table>

下表列出在本指南定义的高级安全性环境下可在 IIS 服务器上创建的所有 IPSec 过滤器。

服务	协议	源端口	目标端口	源地址	目标地址	操作	镜像
Terminal Services	TCP	所有	3389	所有	ME	允许	是
HTTP Server	TCP	所有	80	所有	ME	允许	是
HTTPS Server	TCP	所有	443	所有	ME	允许	是

在实施上表所列举的规则时，应当对它们都进行镜像处理。这样可以确保任何进入服务器的网络通信也可以返回到源服务器。

SQL服务器安全加固

步骤	说明
MDAC 升级	安装最新的MDAC(http://www.microsoft.com/data/download.htm)
密码策略	由于SQL Server不能更改sa用户名称，也不能删除这个超级用户，所以，我们必须对这个帐号进行最强的保护，当然，包括使用一个非常强壮的密码，最好不要在数据库应用中使用sa帐号。新建立一个拥有与sa一样权限的超级用户来管理数据库。同时养成定期修改密码的好习惯。数据库管理员应该定期查看是否有不符合密码要求的帐号。比如使用下面的SQL语句： Use master Select name,Password from syslogins where password is null
数据库日志的记录	核数据库登录事件的“失败和成功”，在实例属性中选择“安全性”，将其中的审核级别选定为全部，这样在数据库系统和操作系统日志里面，就详细记录了所有帐号的登录事件。
管理扩展存储过程	xp_cmdshell是进入操作系统的最佳捷径，是数据库留给操作系统的一个大后门。请把它去掉。使用这个SQL语句： use master sp_dropextendedproc 'xp_cmdshell'

	如果你需要这个存储过程，请用这个语句也可以恢复过来。 sp_addextendedproc 'xp_cmdshell', 'xpsql70.dll' OLE自动存储过程(会造成管理器中的某些特征不能使用)，这些过程包括如下(不需要可以全部去掉： Sp_OACreate Sp_OADestroy Sp_OAGetErrorInfo Sp_OAGetProperty Sp_OAMethod Sp_OASetProperty Sp_OAStop 去掉不需要的注册表访问的存储过程，注册表存储过程甚至能够读出操作系统管理员的密码来，如下： Xp_regaddmultistring Xp_regdeletekey Xp_regdeletevalue Xp_regenumvalues Xp_regread Xp_regremovemultistring Xp_regwrite
防TCP/IP端口探测	在实例属性中选择TCP/IP协议的属性。选择隐藏 SQL Server 实例。 请在上一步配置的基础上，更改原默认的1433端口。 在IPSec过滤拒绝掉1434端口的UDP通讯，可以尽可能地隐藏你的SQL Server。
对网络连接进行IP限制	使用操作系统自己的IPSec可以实现IP数据包的安全性。请对IP连接进行限制，保证只有自己的IP能够访问，拒绝其他IP进行的端口连接。

附：Win2003系统建议禁用服务列表

名 称	服务名	建议设置

自动更新	wuauserv	禁用
Background Intelligent Transfer Service	BITS	禁用
Computer Browser	Browser	禁用
DHCP Client	Dhcp	禁用
NTLM Security Support Provider	NtLmSsp	禁用
Network Location Awareness	NLA	禁用
Performance Logs and Alerts	SysmonLog	禁用
Remote Administration Service	SrvcSurg	禁用
Remote Registry Service	RemoteRegistry	禁用
Server	lanmanserver	禁用
TCP/IP NetBIOS Helper Service	LmHosts	禁用
DHCP Client	Dhcp	禁用
NTLM Security Support Provider	NtLmSsp	禁用
Terminal Services	TermService	禁用
Windows Installer	MSIServer	禁用
Windows Management Instrumentation Driver Extensions	Wmi	禁用
WMI Performance Adapter	WMIApSrv	禁用
Error Reporting	ErrRep	禁用