1. 系统的安全加固：我们通过配置目录权限，系统安全策略，协议栈加强，系统服务和访问控制加固您的系统，整体提高服务器的安全性。

2. IIS 手工加固：手工加固 iis 可以有效的提高 iweb 站点的安全性，合理分配用户权限，配置相应的安全策略，有效的防止 iis 用户溢出提权。

3. 系统应用程序加固，提供应用程序的安全性，例如 sql 的安全配置以及服务器应用软件的安全加固。

三. 系统的安全加固：

1. 目录权限的配置：

1.1 除系统所在分区之外的所有分区都赋予 Administrators 和 SYSTEM 有完全控制权，之后再对其下的子目录作单独的目录权限，如果 WEB 站点目录，你要为其目录权限分配一个与之对应的匿名访问帐号并赋予它有修改权限，如果想使网站更加坚固，可以分配只读权限并对特殊的目录作可写权限。

1.2 系统所在分区下的根目录都要设置为不继承父权限，之后为该分区只赋予 Administrators 和 SYSTEM 有完全控制权。

1.3 因为服务器只有管理员有本地登录权限，所在要配置 Documents and Settings 这个目录权限只保留 Administrators 和 SYSTEM 有完全控制权，其下的子目录同样。另外还有一个隐藏目录也需要同样操作。因为如果你安装有 PCAnyWhere 那么他的的配置信息都保存在其下，使用 webshell 或 FSO 可以轻松的调取这个配置文件。

1.4 配置 Program files 目录，为 Common Files 目录之外的所有目录赋予 Administrators 和 SYSTEM 有完全控制权。

1.5 配置 Windows 目录，其实这一块主要是根据自身的情况如果使用默认的安全设置也是可行的，不过还是应该进入 SYSTEM32 目录下，将 cmd.exe、ftp.exe、net.exe、scrrun.dll、shell.dll 这些杀手锏程序赋予匿名帐号拒绝访问。

1．6 审核 MetBase.bin，C:\WINNT\system32\inetsrv 目录只有 administrator 只允许 Administrator 用户读写。

2. 组策略配置：

在用户权利指派下，从通过网络访问此计算机中删除 Power Users 和 Backup Operators；

启用不允许匿名访问 SAM 帐号和共享；

启用不允许为网络验证存储凭据或 Passport；

从文件共享中删除允许匿名登录的 DFS$和 COMCFG；

启用交互登录：不显示上次的用户名；

启用在下一次密码变更时不存储 LANMAN 哈希值；

禁止 IIS 匿名用户在本地登录；

3.本地安全策略设置：

开始菜单—>管理工具—>本地安全策略

A、本地策略——>审核策略

审核策略更改　成功　失败

审核登录事件　成功　失败

审核对象访问失败

审核过程跟踪　无审核

审核目录服务访问失败

审核特权使用失败

审核系统事件　成功　失败

审核账户登录事件　成功　失败

审核账户管理　成功　失败

注：在设置审核登陆事件时选择记失败，这样在事件查看器里的安全日志就会记录登陆失败的信息。

B、本地策略——>用户权限分配

关闭系统：只有 Administrators 组、其它全部删除。

通过终端服务拒绝登陆：加入 Guests、User 组

通过终端服务允许登陆：只加入 Administrators 组，其他全部删除

C、本地策略——>安全选项

交互式登陆：不显示上次的用户名　启用

网络访问：不允许 SAM 帐户和共享的匿名枚举启用

网络访问：不允许为网络身份验证储存凭证　启用

网络访问：可匿名访问的共享　全部删除

网络访问：可匿名访问的命全部删除

网络访问：可远程访问的注册表路径全部删除

网络访问：可远程访问的注册表路径和子路径全部删除

帐户：重命名来宾帐户重命名一个帐户

帐户：重命名系统管理员帐户　重命名一个帐户

4．本地账户策略：

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

5. 修改注册表配置：

5.1 通过更改注册表

local_machine\system\currentcontrolset\control\lsa-restrictanonymous = 1 来禁止 139 空连接

5.2 修改数据包的生存时间**(ttl)**值

hkey_local_machine\system\currentcontrolset\services\tcpip\parameters

defaultttlreg_dword 0-0xff(0-255 十进制,默认值 128)

5.3 防止 **syn** 洪水攻击

hkey_local_machine\system\currentcontrolset\services\tcpip\parameters

synattackprotectreg_dword 0x2(默认值为 0x0)

5.4 禁止响应 **icmp** 路由通告报文

hkey_local_machine\system\currentcontrolset

\services\tcpip\parameters\interfaces\interface

performrouterdiscoveryreg_dword 0x0(默认值为 0x2)

5.5 防止 **icmp** 重定向报文的攻击

hkey_local_machine\system\currentcontrolset\services\tcpip\parameters

enableicmpredirectsreg_dword 0x0(默认值为 0x1)

5.6 不支持 **igmp** 协议

hkey_local_machine\system\currentcontrolset\services\tcpip\parameters

5.7 修改 **3389** 默认端口：

运行 Regedt32 并转到此项：

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control

\Terminal Server\WinStations\RDP-Tcp，找到“PortNumber”子项，您会看到值 00000D3D，它是 3389 的十六进制表示形式。使用十六进制数值修改此端口号，并保存新值。

禁用不必要的服务不但可以降低服务器的资源占用减轻负担，而且可以增强安全性。下面列出了

igmplevelreg_dword 0x0(默认值为 0x2)

5.8 设置 **arp** 缓存老化时间设置

hkey_local_machine\system\currentcontrolset\services:\tcpip\parameters

arpcachelifereg_dword 0-0xffffffff(秒数,默认值为 120 秒)

arpcacheminreferencedlifereg_dword 0-0xffffffff(秒数,默认值为 600)

5.9 禁止死网关监测技术

hkey_local_machine\system\currentcontrolset\services:\tcpip\parameters

enabledeadgwdetectreg_dword 0x0(默认值为 ox1)

5.10 不支持路由功能

hkey_local_machine\system\currentcontrolset\services:\tcpip\parameters

ipenablerouterreg_dword 0x0(默认值为 0x0)

6. 禁用服务：

- Application Experience Lookup Service
- Automatic Updates
- BITS
- Computer Browser
- DHCP Client
- Error Reporting Service
- Help and Support
- Network Location Awareness
- Print Spooler
- Remote Registry
- Secondary Logon
- Server

• Smartcard

• TCP/IP NetBIOS Helper

• Workstation

• Windows Audio

• Windows Time

• Wireless Configuration

7．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

8. 使用 **tcp/ip** 筛选

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）

9．禁止 **WebDAV**

在注册表：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters

加以下注册表值：

数值名称：DisableWebDAV

数据类型：DWORD

数值数据：1

四． iis 加固方案：

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 microsoftactivex? 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

写不允许

脚本源访问不允许

目录浏览建议关闭

日志访问建议关闭

索引资源建议关闭

执行推荐选择 "仅限于脚本"

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。

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。

安全更新

应用所需的所有 service pack 和定期手动更新补丁。

安装和配置防病毒保护

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）。

安装和配置防火墙保护

推荐最新版 blackice server protection 防火墙（配置简单，比较实用）

监视解决方案

根据要求安装和配置 mom 代理或类似的监视解决方案。

加强数据备份

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。

9. 删除不必要的应用程序映射

ISS 中默认存在很多种应用程序映射，除了 ASP 的这个程序映射，其他的文件在网站上都很少用到。

在“Internet 服务管理器”中，右击网站目录，选择“属性”，在网站目录属性对话框的“主目

录”页面中，点击[配置]按钮，弹出“应用程序配置”对话框，在“应用程序映射”页面，删除无用的程序映射。如果需要这一类文件时，必须安装最新的系统修补补丁，并且选中相应的程序映射，再点击[编辑]按钮，在“添加/编辑应用程序扩展名映射”对话框中勾选“检查文件是否存在”选项。这样当客户请求这类文件时，IIS 会先检查文件是否存在，文件存在后才会去调用程序映射中定义的动态链接库来解析。

保护日志安全

日志是系统安全策略的一个重要环节，确保日志的安全能有效提高系统整体安全性。

修改 **IIS** 日志的存放路径

默认情况下，IIS 的日志存放在%WinDir%/System32/LogFiles，黑客当然非常清楚，所以最好修改一下其存放路径。在“Internet 服务管理器”中，右击网站目录，选择“属性”，在网站目录属性对话框的“Web 站点”页面中，在选中“启用日志记录”的情况下，点击旁边的[属性]按钮，在“常规属性”页面，点击[浏览]按钮或者直接在输入框中输入日志存放路径即可。

五。 sql 服务器安全加固

安装最新的 mdac（http://www.microsoft.com/data/download.htm）

5.1 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
```

5.2 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。

5.3 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’
```

注：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_oacreatesp_oadestroysp_oageterrorinfosp_oagetproperty

sp_oamethodsp_oasetpropertysp_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_regaddmultistringxp_regdeletekeyxp_regdeletevaluexp_regenumvalues

xp_regreadxp_regremovemultistringxp_regwrite

5.4 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。

通过以上的配置，禁止了服务器开放不必要的端口，防止服务被植入后门程序，通过配置目录权限可以防止入侵者拿到 welshell 后提权，加强了服务器的安全性，避免了对服务器的攻击和加强了 TCP 协议栈。通过 iis 的配置提高了 iis 的安全性和稳定性。修改了 sql server 的默认端口，可以防止恶意用户对服务器进行扫描尝试暴力破解 sa 账户提供数据库的安全性。对服务器实现了整体的安全加固。