基于 IIS 的 Web 信息系统安全策略研究

Studies of Web information system security strategy based on the IIS

庞 芳　沈晓军　杨 帆　王丽玫　(广西壮族自治区气象台 南宁 530022)

摘要:本文从网络体系、操作系统、Web 服务器、应用程序、数据库和管理制度安全意识等几个方面探讨了基于 IIS 的 Web 信息系统的安全问题,并结合目前的技术手段,阐述了构建 Web 信息系统应该采取的一些安全策略,实践证明,这些策略是行之有效。

关键词:信息系统 浏览器 Web 服务器 网络安全 IIS;ASP

1　基于 Web 的信息系统的体系结构

基于 Web 的信息系统一般由浏览器、Web 服务器、数据库服务器组成,结构如图 1 所示。

由图 1 可见,基于 Web 信息系统的安全将涉及服务器所采用的操作系统、数据库管理系统、Web 服务器、应用程序等领域。

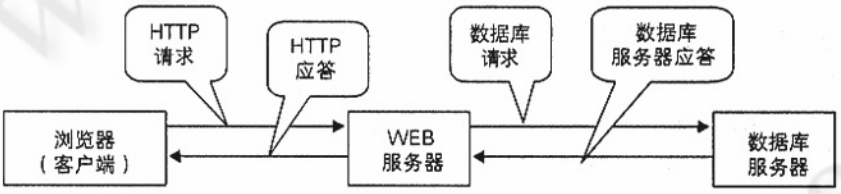

图 1　基于 WEB 的信息系统结构

2　web 信息系统的安全性分析

信息系统的安全性包含两部分内容,一是保证系统正常运行,避免各种非故意的错误与损坏;二是防止系统及数据被非法利用或破坏。在开放的网络环境下,系统安全的保障则更加困难。基于 web 的信息系统安全性体系大致分为网络系统、操作系统、web 服务器及应用程序和数据库等多个层次,如图 2 所示。

由图 2 分析,web 信息安全隐患主要有以下 5 个方面:

(1) 网络系统安全隐患。来自网络系统的安全威胁主要有 DDoS(分布式拒绝服务)攻击、非授权的远程侵入、非法的扫描和探测及网络病毒对网络设备资源的消耗。对付 DDoS 攻击还没有行之有效的办法,只能靠加强网络的安全策略,实时对网络设备检测来防止。对于远程侵入和扫描则可以通过防火墙配合 IPS(入侵检测防御系统)来保障。

(2) 操作系统安全隐患。任何操作系统都存在不同程度的漏洞,特别是默认安装和设置的系统,安全威胁更大。此外,在一台服务器上安装多种服务系统时安全性也会降低。操作系统的安全性要靠我们正确的口令策略和设置、卸载不必要的服务和软件、及时升级不安全的软件版本来保障。

(3) web 服务器安全隐患。web 服务器通常会有以下两个方面的安全要求:

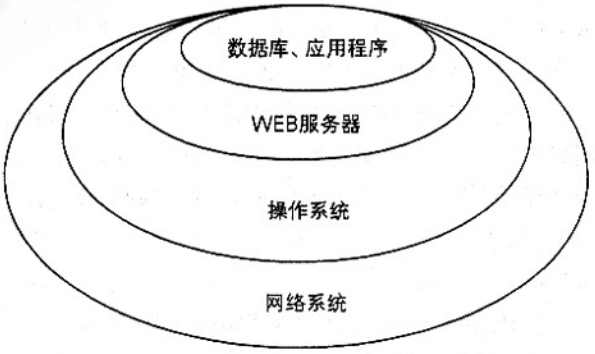

图 2　web 系统的安全体系示意图

① 维持 web 内容的完整性;

② 防止该主机成为入侵你的网络或其它网络的跳板。大多数 web 服务器安全事件的发生是由于没有及时升级不安全的版本和软件配置不当造成的，配置不当的软件可能包括 web 服务器本身或者是 web 服务器运行的应用程序（如 CGI、SSI 和服务器 API 等）。

（4）数据库及应用程序安全隐患。web 站点的数据库和应用程序存在两个方面的安全问题，首先是数据库系统本身的漏洞，包括使用有漏洞的数据库版本或是没有对数据库进行安全配置；其次是应用程序的解释脚本漏洞，比如程序脚本源程序的泄漏，用户认证口令的明码传输，用户使用习惯的考虑不周等。

（5）安全意识和管理制度。许多网站安全事故表明，安全意识的缺乏、管理制度和法规的不健全往往是威胁 Web 信息系统安全的重要因素。比如服务器供电没有 UPS 保护、机房无防盗措施、空闲机器的安全隐患、工作垃圾中安全信息的泄漏、合法用户的误操作、没有做数据备份和系统恢复措施等。

3 基于 IIS 的 web 信息系统安全策略

3.1 网络系统的安全策略

一般 Web 网站都要对 Internet 开放，网站所在的网络系统的安全性能对 Web 网站影响很大。网络系统的安全设计要在网络整体规划中就应该明确，所涉及的内容很多，这里针对保护 Web 网站提出几点措施。

3.1.1 设置防火墙

在内网和外网之间设置防火墙，以隔离和过滤不安全的访问，是防止来自 Internet 的各种攻击的有效手段。防火墙技术主要有基于路由技术的包过滤和基于应用层的代理技术。目前各种防火墙产品非常多，硬件形式的性能通常比较好，但价格贵，基于网络操作系统的软件防火墙则便宜些，但需要丰富的配置经验。通过防火墙，DoS、DDoS 攻击和 ICMP、IGMP 攻击能得到一定的阻止。

3.1.2 划分 VLAN

合理划分 VLAN，减少"冲突域"的范围，减少网络监听的可能性，提高网络的安全性，为网站安全提供基础。当然这要求网络设备支持 VLAN 功能。

3.1.3 Internet 服务

有时造成用户无法访问 Web 网站的原因并不是网站本身出了问题，而是相关的 Internet 服务故障引起，比如 DNS 不能正常解析网站名。因此，Web 网站的安全性还与网络系统中其它相关服务的安全性息息相关。

3.1.4 安装入侵检测防御和实时监控软件

在网络系统中安装入侵检测防御和实时监控软件，及时发现网络系统中的安全漏洞，及时监视系统的安全攻击行为的发生并及时报告，为管理员采取进一步的措施提供依据。这类软件一般有基于网络和基于服务器两类。

3.2 操作系统的安全策略

操作系统的安全是 Web 网站最基本的也是最重要的安全保证。IIS5.0 + Windows2000Server 是目前 Web 网站比较流行的平台，下面主要从安装、配置和管理三个方面探讨 Windows2000Server 的安全设计，其中的大部分原则和措施同样适合微软的其它操作系统平台。

3.2.1 安全安装

操作系统的安全安装要注意以下几点：

（1）选择操作系统的语言版本。在语言不成障碍的条件下，建议选择英文版，因为英文版的 Bug 相对较少，而且英文版的补丁公布较快。

（2）服务器硬盘的分区。至少建立两个以上分区，采用 NTFS 文件分区格式。

（3）系统的安装。根据最小安装原则，安装系统时选择定制安装，根据实际需要选择服务。作为 Web 服务器，建议选择独立域安装。

（4）ServerPacks 和补丁。安装微软官方公布的最新 ServerPacks 和补丁，建议补丁的安装应该在所有的应用程序安装完后。

3.2.2 安全配置

尽管安装时做了很多工作，但系统还是存在非常多安全隐患。根据"最少的服务 + 最小的权限 = 最大的安全"的原则，我们需要进一步对系统进行安全配置：

（1）NTFS 权限设置。NTFS 的目录和文件的访问权限分为：读取、写入、读取及执行、修改、列目录、完全控制。在默认情况下，大多数文件夹对 Everyone 组（也就是所有用户）是完全控制的（FullControl），我们要根据应用的需要和最小权限原则进行重新设置。

(2) 关闭不必要的服务。除非必要,建议禁用不用的服务。

(3) 关闭不必要的端口。在系统 System32\drivers\etc\services 文件中有知名端口和服务的对照表可供参考。通过 TCP/IP 筛选只打开必要的端口。

(4) 账号的管理。更改系统内建的超级用户 Administrator 的名称,给 Guest 用户一个复杂的密码并禁用该账号。通过修改注册表,禁止匿名用户存取 SAM 账号信息和共享信息空连接。5) 配置安全审核策略:Windows2000Server 的默认安装是不开任何安全审核的! 利用 Windows2000Server 的安全配置工具来配置策略,微软提供了一套基于 MMC(管理控制台)的安全配置和分析工具,利用他们你可以很方便的配置服务器的安全策略和账户策略。

3.2.3 安全管理

操作系统的安全管理包括很多方面的工作,主要有:记录服务器安装配置情况和更改日志、留意 Microsoft 最新安全公告、及时打补丁、根据情况的变化增加安全设置、经常查看安全审核日志、备份系统配置信息和其它重要数据等。建议给服务器安装防病毒软件和防火墙系统。

3.3 WEB 服务器的安全策略

IIS 是当前使用最广泛的因特网服务器软件之一,IIS 的安全性是建立在操作系统安全机制之上的,因此,配置 IIS 构建的 Web 站点的安全性除充分利用操作系统的安全性外,还应使用 IIS 本身提供的安全机制。下面从安装、配置和管理三个方面阐述了 IIS 服务器的安全设计策略。

3.3.1 安全安装

IIS5.0 可以在安装 Windows2000Server 时安装,也可以在安装完操作系统后通过添加 Windows 组件来安装。安装 IIS 主要要注意以下几个问题:

(1) 定制组件。IIS 中的组件很多,建议只安装 ComFiles、IISSnap – In、WWWServer、FTPServer 组件。

(2) Inetpub 目录安装位置的选择。IIS 的 Inetpub 目录不要安装在系统分区上。安装完后建议把默认生成的 Inetpub 目录及其下的文件删除,重新建立一个存放 Web 文件的目录。

(3) 规划 Web 文件夹。对网站文件进行分类,比如 .asp、.htm、.inc 等分别放置在不同文件夹下,方便用 IIS 和 Windows2000Server 进行管理(尤其是访问权限的控制)。

3.3.2 安全配置

(1) IP 地址及域名限制。IIS 可以设置允许或拒绝从特定 IP/域名发来的服务请求,有选择地允许特定节点的用户访问服务,可以通过设置来阻止除指定 IP 地址外的整个网络用户来访问你的 Web 服务器。

(2) 安全身份验证。IIS 提供的三种身份验证方式,包括"匿名访问"、"基本验证"、"集成 Windows 验证",另外,IIS 还提供安全通信服务证书验证方式。对于有站点的安全要求等级不同,可分别采用不同的登录身份认证方式。

(3) Web 目录和文件的访问权限的设置。IIS 对用户访问 Web 目录和文件也有不同权限的划分,设置时应该与操作系统的 NTFS 权限设置配合起来用。对于静态页面目录,建议只给读的权限,动态脚本目录,只给脚本资源访问权限,数据库文件给读写的权限。

(4) 带宽限制和 CPU 限制。建议 CPU 使用率最大值设置为 70%,且为强制性限制。

(5) 配置合适的脚本映射。IIS 的很多漏洞都来自脚本映射,删除不必要的脚本映射。

(6) 启用日志记录。日志能为分析网站的安全性能提供依据。

3.3.3 安全管理

IIS 的安全管理工作主要包括:关注微软的安全公告,及时打补丁;根据情况的变化,调整站点的安全配置策略;分析审核日志文件,及时发现存在的安全隐患;备份配置信息;备份数据和文件等。

3.4 数据库及应用程序的安全策略

数据库安全的主要任务是防止非法用户访问或合法用户越权访问数据库中的数据。在网络中用户访问 Web 数据库是通过浏览器和 Web 服务器采用 HTTP 协议,用户执行基于 Web 的数据库应用程序,在浏览器端发出对某一数据库文件的请求,Web 服务器接收到请求后,利用组件(如 ActiveXDateObject)访问后台数据库。因此,根据 Web 数据库的特点,可以采用用户身份认证、授权控制、数据加密、使用日志监视数据库、数据存储安全、审计和备份与数据恢复等安全管理技术。

3.4.1 户身份认证技术

身份识别是用来确定用户是否合法。在 Web 应

用程序级,可利用身份认证机制判断试图访问被限制内容的用户是否拥有有效的 WindowsNT 帐号的用户名和密码。在后台数据库中,用身份验证机制进一步确认用户的合法性。可建立 User 用户表,其信息包括:登录名、口令、用户名及访问权限代码。用户在经过 IP 地址过滤后,在 WebBrowser 端呈现用户登录界面。用户在系统提示下输入登录名、口令,并提交输入结果由系统验证其合法性。由于基于 Web 的数据库应用程序运行在 Internet 的环境中,为避免用户通过一些简单操作绕过登录页面,躲避用户名和口令的验证,可利用 HTTPheaders 信息(ASP 中可利用 Session 对象等)。

3.4.2 授权控制

授权控制经身份认证的合法用户根据自己的权限来访问系统,在该安全体系中,可利用 WindowsNT 的 NTFS 和 DBMS 的用户角色在不同层次分别对用户权限进行限制。

3.4.3 数据加密技术

所谓加密技术是指将一个信息经过加密算法转换,附加密码、加密模块等方法变成无意义的密文,而接受方则将此密文通过解密算法等还原成原文。

3.4.4 数据库安全访问代理服务技术

代理服务是一种网关功能,使用一客户程序,与特定的中间结点链接,然后中间结点与数据库服务器链接,提供用户身份认证和数据库的访问的转发,这样即使防火墙倒塌,数据库也可避免受到攻击。

3.4.5 监视跟踪

许多应用程序的日志记录只用于事后监督,其实对日志的分析还可用于预防入侵,提高网络安全。在数据库应用系统中,日志将记录自用户登录开始起,直到退出系统为止,在这段时间中所执行的所有操作,包括登录失败操作、对数据库的操作及系统功能的使用等。因此,必须建立完善的日志记录功能。另外,还可利用现有的网络监视软件进行日志记录和信息跟踪。

3.4.6 存储过程

在基于 Web 的数据库应用系统中,可建立存储过程,在使用时通过内嵌的 SQL 命令来执行。在存储过程中,采用将用户和数据分开的方法。这种不允许任何对表的完全访问和更新,只是提供实现与表交互的存储过程。这对于数据存储和检索来说,是一个带有更多的面向对象风格的方法,它有助于保证数据的正确与安全。

3.4.7 审计

审计主要是确保可查性。审计作为一项安全技术,对信息系统的安全有着很重要的作用。通过设置完善的审计机制,能及时提供与系统运行过程中的各种可疑现象有关的信息,供有关人员分析、判断用户的身份和使用服务的一些情况,以便工作人员能及时发现隐患。

3.4.8 备份与数据恢复

网络数据库中最宝贵的是数据信息,如果出现故障,系统将无法正常运行,通常在硬件一级可采用磁盘镜像、磁盘陈列、双机容错等备份方案;在软件一级可采用热修复、数据拷贝等措施。

3.5 管理制度与安全意识

安全不仅仅是个技术问题,更多的时候是意识和制度的问题。首先是要重视网络和网站安全的设计,建立机房制度和重要设备的操作规章;其次要制定用户操作守则,对用户进行安全知识培训和操作方法培训;对于安全性要求较高的网站,建议采用国际化标准(ISO)的安全管理模式,即 PDCA 模式来进行网站的安全管理。

4 结语

信息系统的安全性在系统的建设中具有非常重要的作用,WEB 信息系统的安全是一个系统性、综合性的问题,其涉及的范围很广,要求系统管理员在做安全规划和实施时,遵从"木桶理论"原则,从网络系统、操作系统、web 服务器及应用程序和数据库等方面系统考虑,结合实际层层设防,才能保证系统安全运行。

参考文献

1 李书症,网络环境下的信息安全措施[J],计算机系统应用,2003,1。
2 卿斯汉,操作系统安全简论——Windows NT 操作系统安全,计算机系统应用,2002。
3 郑志蓉、沈昌祥,操作系统安全——应用层安全的基础,计算机应用与软件,2002。
4 张陇瑛,IIS 安全设置与性能调整[J],河南气象,2004,2。