文章编号:1005－0523(2003)05－0062－04

基于 IIS 的 Web 网站的安全研究与设计

谢剑猛，许 飞

(华东交通大学 现代教育技术中心,江西 南昌 330013)

摘要:详细分析了 Web 网站的安全隐患,给出了 Web 网站安全设计原则,并结合实践经验,从网络体系、操作系统、Web 服务器、脚本程序、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 网站的安全设计.

关 键 词:Web 网站;安全隐患分析;安全设计;IIS(Internet Information Server);ASP

中图分类号:TH117.1 **文献标识码**:A

1 Web 网站安全隐患分析与安全设计原则

Web 网站是 Internet/Intranet 的主要组成部分,在黑客猖獗、病毒肆意的网络中,如何保障 Web 网站信息的有效性和安全性是 Web 网站建设中的重要课题.众所周知,当前国内很多 Web 网站都存在这样那样的安全隐患,有些甚至是漏洞百出,不堪一击.形成这种状态的原因是多方面的,有产品方面的缺陷,有技术经验的不足,也有安全意识的缺乏和管理制度的不健全.认真分析来自各方面的安全威胁和各个层次存在的安全隐患,明确安全设计的原则是 Web 网站安全设计的第一步.

1.1 Web 网站安全隐患

Web 网站的信息安全目标主要有:保密性安全、完整性安全、可用性安全和认证安全.Web 网站是个复杂的系统,包含了操作系统、Web 服务器、应用程序和数据库等多个层次,安全隐患存在于各个层次中.同时,Web 网站又是置于错综复杂的网络中,对 Web 网站的威胁可能来自网络协议的各个层次.Web 网站信息安全可用一个三维空间图来描述,如图 1 所示.

据此具体分析,Web 网站的安全隐患主要有以下几个方面:

1) 网络体系:来自 Internet 的 DDoS(分布式拒绝服务)攻击是 Web 网站经常遭遇的攻击之一.当然,从现有技术的角度来说,还没有一种有效的方法来对付 DDoS 攻击,但是通过在加强网络体系的安全策略,实时检测网络设备和及时追踪处理 DDos 都是防止 DDoS 的积极手段.

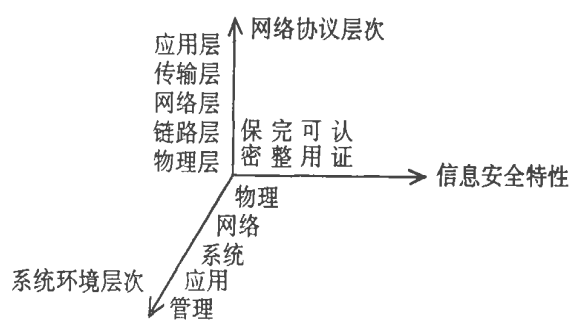

图 1 Web 网站信息安全空间

2) 服务器系统:任何操作系统和 Web 服务器都存在这样那样的漏洞,尤其是系统默认设置存在很多潜在的威胁.一些黑客和病毒木马就是利用了这些漏洞来破坏系统.另外,一个服务器上安装过多服务也会降低系统的安全性.服务器系统的漏洞主要通过打补丁和系统安全配置来解决.

3) 服务器用户:服务器系统上的各种用户是构成服务器安全的一大隐患.比如用户的口令强度过

收稿日期:2003－04－28

作者简介:谢剑猛(1975－),男,江西崇仁人,华东交通大学助教.

弱导致被破解、特殊用户(如 guest)的潜在威胁、用户权限设置不当等.通过分组管理系统用户和审核用户的行为可以有效防止这类威胁.

4) 脚本程序和数据库:Web 网站脚本程序和数据库存在两方面的安全问题,一是解释执行脚本的系统和数据库本身的漏洞,比如 ASP 的源代码泄漏和 SQL 语句的客户资料认证漏洞等,一是程序设计逻辑上存在漏洞,比如身份认证逻辑不严密、重要文件和数据没有加密等.通过为系统打补丁和优化安全认证程序能有效降低这类漏洞的危害.

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 网站安全的重要因素.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.

1.2 Web 网站安全设计原则

1) 网站安全的"木桶原则",木桶原则指出:木桶的最大容积取决于最短的一块木板.如前面所述,对 Web 网站的安全威胁是多方面和多层次的,其安全性同样取决于系统中最薄弱环节的安全性,所以必须对每个环节的安全性都有足够的认识和考虑,清楚意识到 Web 网站的安全不能简单地靠某个环节的安全性的增加而得到提高.

2) 网站安全的整体性原则:依据 PDRR 网络安全模型,网站的安全系统应该包括 4 种机制:防护(Protection)、检测(Detection)、响应(Response)和恢复(Recovery).安全防护机制是根据系统存在的各种安全漏洞和安全威胁采取相应防护措施;安全检测机制是监测系统的运行情况,及时发现和制止对系统的各种攻击;响应和应急恢复机制是在安全防护失效的情况下,进行应急处理,尽量、及时地恢复信息,减少攻击地破坏程度.

3) 网站安全的有效性与实用性原则:信息利用与安全是一对矛盾,越安全就意味着使用越不方便.网站安全应以不能影响系统的正常运行和合法用户的操作活动为前提.因此,要在确保安全性的基础上,把安全处理的运算量减少或分摊,减少用户的记忆和存储工作量.

4) 网站安全的等级原则:根据网站上的目录和信息的保密程度级别不同,可以划分出安全等级,针对不同级别的安全对象,提供全面、可选的安全设计,以满足不同层次的需求.比如对用户分组管理.

5) 网站安全的有价原则:现实中,网站的安全设计是受各种条件限制的,尤其是经费.在有限的代价下寻求一种合适的安全方案是网站安全设计的一个重要原则.

2 网络系统的安全设计

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.

2.1 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.

2.2 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.

2.3 保护相关的 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.

2.4 安装入侵检测和实时监控软件

在网络系统中安装入侵检测和实时监控软件,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 操作系统的安全设计

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.IIS 5.0+Windows 2000 Server 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 Windows 2000 Server 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.

3.1 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) Server Packs 和补丁:安装微软官方公布的最新 Server Packs 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 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(Full Control),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:Windows 2000 Server 的默认安装是不开任何安全审核的! 利用 Windows 2000 Server 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.

3.3 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、更具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.

4 Web 服务器的安全设计

IIS5.0 作为目前流行的 Web 服务器,遭受的攻击也非常多,下面同样从安装、配置和管理三个方面给出 IIS 的安全设计方案.

4.1 安全安装

IIS5.0 可以在安装 Windows2000 Server 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 Com Files、IIS Snap-In、WWW Server、FTP Server 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 Windows 2000 Server 进行管理(尤其是访问权限的控制).

4.2 安全配置

1) IP 限制:如果站点面向的访问者有明确的网络范围,可通过 IIS 的 IP 过滤功能来制定拥有站点访问权的 IP 或 IP 范围.

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.

7) 使用 IIS 锁定工具和 URLScan 来配置 IIS:为了方便 Web 站点管理员安全配置 IIS,微软公司提供了 IIS 锁定工具(IISLockdown),IISLockdown 最新版本集成了 URLScan.IISLockdown 有模板配置和手动配置两种方式,使用起来非常简单.

4.3 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

5 脚本程序和数据库的安全设计

程序本身设计上存在的错误和漏洞是 Web 网站安全的一大隐患,因此在设计 Web 网站应用系统时应特别注意程序代码的自身逻辑上的安全性.当然,一些安全漏洞,除了基本的身份认证和授权控制之外,还要求程序设计时采用一些特别的措施,比如一些恶性代码的得逞就是脚本程序设计上没有进行过滤造成.

对于有特殊安全要求的场合,可选用如下措施:

1) 采用数据加密技术,对敏感数据的传输和存储进行加密,或利用安全套接字协议(SSL)加密方法,通过使用公共密钥和对称性加密提供非公开通信、身份验证和消息集成,以防敏感信息被窃听.

2) 利用 IIS 实现限制 IP 访问,或者取消 IIS 匿名访问,利用操作系统的身份认证机制来保护重要的数据.

3) 利用 ASP 的 Request 对象的 Server Variables 属性来比较用户主机的 IP 的合法性,进一步保障系统安全.

6 完善管理制度、加强安全意识并建立安全事件的应急措施

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;第三电源和物理安全,服务器要配置不间断电源系统,服务器机房要安装防盗和报警系统;第四,要做好重要数据和配置信息的备份和安全事故发生后的应急措施.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.

参考文献:

[1] 杨卫东.网络系统集成与工程设计[M].北京:科学出版社,2002.

[2] 张千里,陈光英.网络安全新技术[M].北京:人民邮电出版社,2003.

[3] 窦丽华,蒋庆华,晨　晖.基于 Web 的信息系统安全研究[J].北京理工大学学报,2002,(6):360～364.

[4] http://www.microsoft.com/china/technet/columns/insider/default.asp

Study and Design of the Website Secutiry Based on IIS

XIE Jian-meng, XU-fei

(Center of Modern Education and Technology, East China Jiaotong Univ., Nanchang 330013, China)

Abstract: This paper gives out the detailed analysis of Website security subsistent and the principle of Website security design. And combined with actual experience, from the respects of network, operate system, Web server, script program, database, management and security consciousness, it studies the Website security design which are based on IIS.

Key words: Website; security subsistent analysis; security design; IIS(Internet Information Server); ASP