

计算机网络安全系列丛书

构建安全的 Web 站点

启明星辰公司

高鹏 严望佳 编著

清华大学出版社

(京)新登字 158 号

内 容 简 介

本书是阐述 Web 安全的指导性手册。首先介绍 Web 方面的基本概念和原理；然后逐步深入地讲解了配置安全的 Web 服务器的方法。本书中讲述的 Web 服务器包括 UNIX 平台和 Windows NT 平台，基本包括了所有的 Web 服务器。

本书最大的特点是针对性强，且内容全面，无论是刚接触 Web 的初级用户，还是已有数年管理经验的 Web 站点管理员，都会从本书中获得很大的帮助。

版权所有，翻印必究。

本书封面贴有清华大学出版社激光防伪标签，无标签者不得销售。

图书在版编目 (CIP) 数据

构建安全的 Web 站点/高鹏, 严望佳编著. —北京: 清华大学出版社, 1999

(计算机网络安全系列丛书)

ISBN 7-302-03344-7

I. 构… II. ①高… ②严… III. 万维网-安全技术 IV. TP393.4

中国版本图书馆 CIP 数据核字(1999)第 03714 号

出版者: 清华大学出版社 (北京清华大学校内, 邮编: 100084)

<http://www.tup.tsinghua.edu.cn>

印刷者: 北京市清华园胶印厂

发行者: 新华书店总店北京发行所

开 本: 787×1092 1/16 印张: 13 字数: 230 千字

版 次: 1999 年 3 月第 1 版 1999 年 3 月第 1 次印刷

书 号: ISBN 7-302-03344-7 /TP·1804

印 数: 0001~5000

定 价: 25.00 元

谨以此书献给我们的老师

严望佳

丛书序

全球信息高速公路的建设, Internet/Intranet 的发展, 将对整个社会的科学与技术、经济与文化带来巨大的推动与冲击, 同时也给我们带来了许多的挑战。Internet/Intranet 信息安全是一个综合的系统工程, 需要我们在网络安全技术的研究和应用领域做长期的攻关和规划。

在 Internet/Intranet 的大量应用中, Internet/Intranet 安全面临着重大挑战。事实上, 资源共享和信息安全历来是一对矛盾。近年来随着 Internet 的飞速发展, 计算机网络的资源共享进一步加强, 随之而来的信息安全问题日益突出。据美国 FBI 统计, 美国每年因网络安全问题所造成的经济损失高达 75 亿美元。而全球平均每 20 秒钟就发生一起 Internet 计算机侵入事件。

一般认为, 计算机网络系统的安全威胁主要来自黑客攻击、计算机病毒和拒绝服务攻击 3 个方面。目前, 人们也开始重视来自网络内部的安全威胁。

黑客攻击早在主机终端时代就已经出现, 随着 Internet 的发展, 现代黑客则从以系统为主的攻击转变到以网络为主的攻击。新的手法包括: 通过网络监听获取网上用户的帐号和密码; 监听密钥分配过程, 攻击密钥管理服务器, 得到密钥或认证码, 从而取得合法资格; 利用 UNIX 操作系统提供的守护进程的缺省帐户进行攻击, 如 Telnet Daemon、FTP Daemon 和 RPC Daemon 等; 利用 Finger 等命令收集信息, 提高自己的攻击能力; 利用 SendMail, 采用 debug、wizard 和 pipe 等进行攻击; 利用 FTP, 采用匿名用户访问进行攻击; 利用 NFS 进行攻击; 通过隐蔽通道进行非法活动; 突破防火墙等等。目前, 已知的黑客攻击手段多达 500 余种。

计算机病毒与“蠕虫”程序有所不同, 它们主要的区别是, “蠕虫”寄生于操作系统之上, 而计算机病毒寄生于一般的可执行程序上。计算机病毒种类繁多, 极易传播, 影响范围广。它动辄删除、修改文件, 导致程序运行错误, 甚至死机, 已构成对 Internet/Intranet 的严重威胁。

拒绝服务攻击是一种破坏性攻击, 最早的拒绝服务攻击是“电子邮件炸弹”。它的表现形式是用户在很短的时间内收到大量无用的电子邮件, 从而影响正常业务的运行。严重时会使系统关机、网络瘫痪。

总而言之，对 Internet/Intranet 安全构成的威胁可以分为以下若干类型：黑客入侵、来自内部的攻击、计算机病毒的侵入、秘密信息的泄漏和修改网络的关键数据等，这些都可以造成 Internet 瘫痪或引起 Internet 商业的经济损失等等。人们面临的计算机网络系统的安全威胁日益严重。

黑客攻击等威胁行为为什么能够经常得逞呢？主要原因在于 Internet/Intranet 系统内在安全的脆弱性；其次是人们思想麻痹，没有正视黑客入侵所造成的严重后果，因而舍不得投入必要的人力、财力和物力来加强 Internet/Intranet 的安全性，没有采取有效的安全策略和安全机制。另外，缺乏先进的网络安全技术、工具、手段和产品等原因，也导致网络的安全防范能力差。

由于我国网络研究起步晚，网络安全技术还有待整体的提高和发展。我很高兴看到这套丛书的诞生，该丛书系统地介绍了计算机网络安全各方面的问题，并且从一些新的角度进行探讨，例如，如何针对 Internet/Intranet 系统的安全威胁建立正确的安全策略；如何提出 Internet/Intranet 系统安全的整体解决方案；如何严格规范建立 Internet/Intranet 系统的安全机制等。这对提高我国网络安全防范能力将有重要的参考作用。

这套由国家信息中心、国际计算机安全协会 (ICSA) 以及启明星辰信息技术有限公司 (Vtech) 策划的网络安全系列丛书具有起点高、技术覆盖面广等特点。包括了对业界最新的网络安全技术、操作系统漏洞和防范方法、网络安全工具以及黑客攻击手段等的详细分析和介绍。读者可以带着各种问题、从不同的角度来了解这些技术，一定会有所收获。

中国工程院院士 沈昌祥

前言

Internet 的出现，可以说是继个人电脑之后，信息产业最重要的发明，它为人类社会的信息交流方式带来了革命性的变化。对于那些渴望得到迅速而廉价的市场渠道的企业而言，Internet 则象征着一个潜力无穷的市场，如何利用 Internet 将产品及服务销出去，将是这些企业在面对下一世纪的竞争时最大的课题。

然而，在这一片 Internet 网络的热潮中，仍然有许多人存有疑虑，主要集中在安全问题上。而对 Internet 这个开放的环境，不论是最终用户还是提供服务的系统管理人员均深感担忧，面对一次又一次网络安全遭遇挑战的新闻，要如何阻挡黑客无所不用破坏手段？就用户而言，他必须确认在网络上输入的机密性资料(例如，密码及帐户号码等)不会被盗用，此外，输入的交易资料不会被篡改，同时须正确迅速地传送到接收端系统；对提供 Internet 服务的行业人员来说，也需要确定自己的系统不会受到黑客侵入，以致造成业务损失及服务停顿。

传统的安全工作主要是利用防火墙来管理，然而在很多场合下，防火墙仍有其不足之处。防火墙是属于网络安全的产品，它主要是以监管网络协定(例如 TCP/IP、HTTP 和 IPX 等)、通讯包、网络服务及网址等方式来确保网络的安全，即是扮演守门人的角色，以阻挡不当的信息及不合法的使用者侵入。但 Internet 网络基本上属于一个开放的环境，任何一个申请开放的环境，任何一个申请网络帐户的客户均可合法进入。此外，防火墙亦无法阻挡内部的破坏者，根据 Computer Security Institute 在 1995 年就 428 件案例所做的研究，46.8% 的侵入者来自企业内部。此外，黑客经常针对电脑操作系统、Web Server 及网络应用程序中可能包含未被清除的漏洞(Bugs)进行攻击，由于防火墙属于应用环境的范畴，因此它无法提供足够的保护。

本书就是针对 Internet 上的安全问题而编写的。Internet 上的服务包括多种，如 telnet、ftp、mail 和 web 等等。本书将把重点放在 web 上，对于其他的 service，将在本系列丛书的其他书目中讲解。

本书从内容上分为四部分。

第一部分 Internet 安全基础

这部分对 Internet 做了基本介绍，包括 Internet 的结构、Internet 提供的各种服务、Web 服务器软件、Web 客户端软件以及 Internet 上可能出现的安全问题。

第二部分 Web 服务器安全

这部分讲解了 Web 服务器安全配置的方法，包括加密方法、通过 IP 地址进行客户端认证、通过用户名/口令方法进行客户端认证，从而限制客户端对保密数据的访问，如 SSL、SET 和 S-HTTP 等安全协议。并在此基础上分别具体地讲述了 UNIX 平台上的最常见的 Web 服务器 Apache 的安全配置方法和 Windows NT 平台上最常见的 Web 服务器 IIS 的安全配置方法。

第三部分 Web 客户端安全

这部分讲述了 Web 服务经常忽略的安全问题——客户端的安全。由于 Web 服务是客户/服务器的结构，因此除了服务器上有安全问题之外，同样，客户端也存在着安全问题。例如，用户在不经意的情况下泄漏了自己的用户名和口令、泄漏了自己的电子邮件地址和用户本地数据被修改等等。

这部分讲述了用户可能存在的安全问题，并介绍了用户可能会担心的 cookies 问题、Java 小程序的执行和 ActiveX 的执行等问题。

第四部分 已知的 Web 安全漏洞

虽然用户可以通过配置使 Web 服务器更加安全，但不可能保证服务器是绝对安全的。到目前为止，还没有一种方法使 Web 提供的服务是绝对安全的，因为 Web 服务器是用编程语言编写的程序，在该程序中可能会出现各种漏洞；另外，Web 的客户端软件，即浏览器，也是一种程序，也可能存在着各种漏洞。

这部分介绍了目前所知道的各种 Web 软件安全漏洞，它也分为服务器端和客户端两个部分。

在任何时候，安全都是相对的，而不安全是绝对的。因此，读者在阅读本书之后，可以提高系统配置和使用的安全意识和方法，但不能保证系统是绝对安全的。要使系统更加安全，读者还要经常阅读有关的信息，例如，参与一些服务器安全的电子邮件列表、经常访问一些安全站点。下面是一些著名的安全站点：

- ✱ <http://www.cert.org/>
- ✱ <http://www.10pht.com/>
- ✱ <http://www.root.org/warez.html>
- ✱ <http://www/2600.com>

- * <http://www.microagwny.com/home/claw/hackers.html>
- * <http://www.halcyon.com/yakboy/42ff.html>
- * <http://www.netwalk.com/silicon/void-f.html>

这套丛书的策划和出版得到以下朋友的热情支持和帮助，谨在这里表示我们诚挚的谢意：中国信息安全专业委员会李正男主任、刘世键主任、吴亚飞秘书长，中国信息大学执行董事刘建国先生，国家信息大学信息安全处叶红、董小玲、张翔、孙卫红，美国格莱瑞技术公司严立。

目 录

第一章 Internet 简介	1
1.1 Internet 的简史	2
1.2 Internet 功能概要	4
1.3 Web 结构	5
1.3.1 Web 服务器	5
1.3.2 Web 浏览器	6
1.4 通用网关接口(CGI)介绍	7
第二章 Web 的安全问题	9
2.1 Web 安全框架	11
2.1.1 定义资源	11
2.1.2 定义风险	12
2.1.3 建立安全策略	12
2.1.4 定义安全机制	13
2.1.5 Web 服务存在风险的原因	13
2.2 Web 服务器的风险和安全提升机制	14
2.2.1 Internet 主机的风险	14
2.2.2 Internet 主机的安全机制	16
2.2.3 Web 服务器软件易受攻击性	18
2.2.4 Web 服务器安全配置原则	20
2.2.5 认证和访问控制机制	21
2.3 Web 客户端的风险和安全提升机制	25
2.3.1 信息泄漏	26
2.3.2 内容协商与查看器	27
2.4 防火墙的角色	28
2.4.1 防火墙的功能	29
2.4.2 防火墙的使用	29

2.4.3	代理服务器.....	30
2.4.4	Internet 与防火墙的关系.....	31
第三章	Web 服务器的安全.....	33
3.1	安全隐患.....	34
3.2	Internet 各层的安全模型.....	34
3.2.1	传输层的安全.....	38
3.2.2	应用层的安全.....	39
3.3	服务器和文档根目录的权限设置.....	41
3.4	Web 服务器一些功能的安全.....	43
3.4.1	自动目录列表功能.....	43
3.4.2	符号连接.....	44
3.4.3	Server Side Includes.....	44
3.4.4	用户维护的目录.....	44
3.5	以 root 身份运行的 Web 服务器.....	45
3.6	Web 服务器和 FTP 服务器共用文档树的情况.....	46
3.7	在 chroot 环境下运行 Web 服务器.....	46
3.8	检查站点是否被攻破.....	47
第四章	Web 站点上数据的安全.....	49
4.1	访问限制类型.....	50
4.1.1	通过 IP 地址、子网或域名来控制.....	50
4.1.2	通过用户名/口令限制.....	50
4.1.3	用公用密钥加密方法.....	50
4.2	通过 IP 地址或域名限制实例.....	50
4.3	通过用户名/口令限制实例.....	52
4.3.1	用户名/口令的安全性.....	52
4.3.2	授权新的用户.....	53
4.4	用户认证.....	56
4.5	允许用户在线地修改口令的 CGI 程序.....	56
4.6	access.conf 文件与每个目录的访问控制文件的比较.....	57
4.7	加密的工作原理.....	57
4.8	SSL、SHTTP 和 Shen.....	58
4.8.1	SSL.....	58
4.8.2	SHTTP.....	58

4.8.3 Shen	59
4.9 免费的 SSL 软件模块	59
4.10 用个人证书来控制服务器访问	62
4.11 在 Web 上如何接受信用卡订单	62
4.12 First Virtual 帐号、DigiCash、CyberCash 和 SET	63
4.12.1 First Virtual 帐号	63
4.12.2 DigiCash	64
4.12.3 CyberCash	64
4.12.4 SET	65
4.12.5 Open Market Web 商业系统	66
第五章 CGI 脚本的安全性	67
5.1 安全隐患	69
5.2 CGI 脚本带来的安全问题	69
5.2.1 脚本和其他程序的比较	70
5.2.2 表单中数据的真实性	70
5.3 cgi-bin 目录与.cgi 文件	70
5.4 编译型语言与解释型语言的比较	71
5.5 确认 CGI 脚本的安全性	72
5.6 Internet 上含有漏洞的 CGI 程序	73
5.6.1 TextCounter	73
5.6.2 各种 guestbook 脚本	73
5.6.3 Excite Web 搜索引擎 (EWS)	74
5.6.4 info2www	74
5.6.5 count.cgi	74
5.6.6 Web dist.cgi	75
5.6.7 php.cgi	75
5.6.8 files.pl	75
5.6.9 Microsoft FrontPage 扩展	76
5.6.10 nph-test-cgi	76
5.6.11 nph-publish	76
5.6.12 AnyForm	76
5.6.13 FormMail	77
5.7 编写 CGI 脚本时要考虑的问题	77

5.8	CGI 与数据库/搜索引擎连接	79
5.9	PATH 环境变量	80
5.10	CGIWRAP	81
5.11	Sbox	82
5.12	cgi 程序的运行与用户接口	82
5.13	表单中的 hidden 变量	82
5.14	POST 与 PUT 方法	83
5.15	安全的 Perl 脚本程序	83
5.15.1	调用 exec() 和 system() 的问题	83
5.15.2	Perl 的 taint 检查	85
5.15.3	打开 taint 检查后的问题	85
5.15.4	取消某个变量的 taint	86
5.15.5	\$foo=~{/Suser_variable/ 模式匹配的安全性	86
5.15.6	suid	87
第六章	Cookies 及其安全	89
6.1	cookies 介绍	90
6.2	工作方式	90
6.3	cookies 中保存的内容	90
6.4	存放位置	91
6.5	生命周期	92
6.6	cookies 安全须知	92
6.6.1	cookies 不能从用户的硬盘上读取数据	92
6.6.2	cookies 不能被用于收集敏感信息	92
6.6.3	不同站点的 cookies	92
6.7	用户的浏览器泄漏的信息	93
6.8	服务器保存客户端状态信息的方法	93
6.9	用户泄露信息的原因	93
6.10	如何去掉 cookies 的方法	94
第七章	Java 的安全性	97
7.1	Java 的安全模型	98
7.1.1	类装载器	98
7.1.2	字节码验证器	99
7.1.3	安全管理器	100

7.1.4	Java 语言提供的安全特性.....	101
7.2	JavaSecurity API.....	101
7.2.1	数字签名和 JAR 文件.....	102
7.2.2	密钥管理、消息文摘和访问列表.....	103
7.3	Java 应用安全.....	103
7.3.1	Java Applet 安全.....	103
7.3.2	浏览器上 Applet 的安全.....	104
7.4	Applet 不能做什么.....	104
7.5	如何使 Applet 读取文件的方法.....	105
7.6	使 Applet 向文件中写数据的方法.....	106
7.7	Applet 能够获取的系统信息.....	106
7.8	Applet 连接其他主机的方法.....	107
7.9	Applet 维持连续状态的方法.....	108
7.10	Applet 不能在客户端启动其他的程序.....	108
第八章	提高 IIS 的安全性.....	109
8.1	Windows NT 的安全与 IIS 的安全概述.....	111
8.2	Internet Information Server 的安全机制.....	116
8.3	控制对 Web 节点的匿名访问.....	117
8.3.1	配置匿名用户帐号.....	118
8.3.2	允许匿名访问.....	119
8.3.3	更改匿名访问的帐号或密码.....	120
8.3.4	使用域控制器上的匿名帐号.....	120
8.4	帐号的安全.....	122
8.5	身份认证.....	123
8.5.1	WWW 服务的身份认证.....	124
8.5.2	FTP 服务的身份认证.....	124
8.5.3	匿名登录与客户身份认证的交互.....	126
8.6	通过文件夹和文件的权限控制访问.....	127
8.7	设置 WWW 目录访问权.....	132
8.7.1	读取权限.....	132
8.7.2	执行权限.....	133
8.8	通过 IP 地址控制访问权.....	134
8.8.1	拒绝访问特定计算机或计算机组.....	135

8.8.2 允许访问特定计算机或计算机组	135
8.9 运行其他网络服务	136
8.9.1 只运行所需要的服务	136
8.9.2 检查网络共享权限	137
8.9.3 禁止目录浏览	137
8.10 通过 SSL 保护数据传送	138
第九章 Apache 服务器的安全性	141
9.1 Apache 服务器介绍	142
9.2 控制 CGI 脚本的执行	142
9.3 如何使用 SSI	143
9.4 /etc/passwd 与 Web 页面认证	143
9.5 Apache 在每次响应中都加入 cookie	144
9.6 Apache 没有加入 SSL 的原因	144
9.7 Apache 的 suEXEC	145
9.7.1 suEXEC 介绍	145
9.7.2 suEXEC 安全模型	145
9.7.3 配置和安装 suEXEC	147
9.7.4 打开和关闭 suEXEC	150
9.8 DBM 用户认证	151
9.8.1 DBM 介绍	151
9.8.2 准备 Apache 的 DBM 文件	152
9.8.3 创建 DBM 用户文件	152
9.8.4 限制目录访问	153
9.8.5 用户组	154
9.8.6 定制 DBM 文件的管理	154
9.9 Apache 配置技巧	155
9.9.1 ServerRoot 目录权限的设置	155
9.9.2 Server Side Includes 的配置	155
9.9.3 阻止用户修改系统配置	156
9.9.4 缺省地保护服务器文件	156
第十章 客户端的安全性	159
10.1 客户端可能泄漏的信息	160
10.2 配置/bin/csh 作为查看器	160

10.3	SSL 使用的加密方法的安全性	161
10.4	Java 和 JavaScript 的区别	162
10.5	JavaScript 的安全性	163
10.5.1	截取用户的电子邮件地址和其他信息	163
10.5.2	截取用户本地机器上的文件	164
10.5.3	监视用户的会话过程	164
10.5.4	Frame 造成的信息泄漏	165
10.5.5	文件上传漏洞	166
10.6	ActiveX 的安全性	166
10.7	浏览器暴露用户的局域网登录的用户名/口令	168
10.8	UNIX 下的 Lynx 的安全性	168
10.9	Microsoft Internet Explorer 的安全漏洞	169
10.9.1	缓冲区溢出漏洞	169
10.9.2	递归 Frames 漏洞	170
10.9.3	“快捷方式漏洞”	171
10.10	Netscape 的安全漏洞	172
10.10.1	缓冲区溢出漏洞	172
10.10.2	个人喜好漏洞	172
10.10.3	类装载器 Java 漏洞	173
10.10.4	长文件名电子邮件漏洞	173
10.10.5	Singapore 隐私漏洞	173
第十一章	已知的 Web 服务器漏洞	175
11.1	Windows NT 上的 Web 服务器	176
11.1.1	Netscape Communications Server for NT 的安全漏洞	176
11.1.2	O'Reilly WebSite Server for Windows NT 的安全漏洞	178
11.1.3	Purveyor Server for Windows NT 的安全漏洞	178
11.1.4	Microsoft IIS Web 服务器的安全漏洞	179
11.1.5	Sun 的 JavaWebServer for Windows NT 安全漏洞	180
11.1.6	MetaInfo MetaWeb 服务器的安全漏洞	181
11.2	UNIX 系统上的 Web 服务器	181
11.2.1	NCSA httpd 的安全漏洞	181
11.2.2	Apache httpd 的安全漏洞	182
11.2.3	Netscape Servers 的安全漏洞	185

11.2.4 Lotus Domino Go Server 的安全漏洞.....	185
11.3 Macintosh 系统上的 Web 服务器.....	185
11.3.1 WebStar 的安全漏洞.....	185
11.3.2 Quid Pro Quo 的安全漏洞.....	186
11.4 Novell WebServer 的安全漏洞.....	186

第一章

Internet 简介

