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。

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，该丛书系统全面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的破坏手段？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，对于其他的服务，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，也可能会存在各种漏洞。

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