

<<铜墙铁壁>>

图书基本信息

书名：<<铜墙铁壁>>

13位ISBN编号：9787111266563

10位ISBN编号：7111266560

出版时间：2009-6

出版时间：机械工业出版社

作者：武新华 等编著

页数：378

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## &lt;&lt;铜墙铁壁&gt;&gt;

## 前言

随着社会各行各业对网络技术依赖性的不断增强，人们在体验网络所带来的极大便利的同时，黑客入侵和网络安全问题也同样在困扰着网络的发展，如僵尸网络（Botnet）、网络钓鱼（Phishing）、木马及间谍软件、零时间威胁、熊猫烧香、网站挂马事件、木马产业链的曝光等，更使得网络安全问题成为大家关注的焦点。

由于互联网本身的设计缺陷及其复杂性、开放性等特点，网络的安全性已成为阻碍信息化进程的重要因素，其影响已从互联网领域逐步扩大到政府、通信、金融、电力、交通等应用和建设领域。

网络安全问题已引起了全世界的密切关注，黑客的恶意行为已成为全球新的公害。

或许大家都曾碰到过这样的情况，正当自己为精彩的网页着迷时，突然硬盘狂响不止，最后发现所有的程序都不能运行了；正在给网友写E-mail时，突然弹出一个对话框，上面写着“我是幽灵，我要毁了你的电脑！”

正在聊天室里与网友聊天时，突然弹出一堆对话框，无论怎么关都关不掉，最后只能无奈地重启计算机；在登录QQ时却突然提示密码错误，试遍所有可能的密码却依然不能通过，这时才发现自己的QQ密码被盗了。

因此，大家必须采取有力措施加强网络的自身安全防护性能，以有效抵抗入侵和攻击破坏。

但随着攻击手段的日趋复杂，有组织、有预谋、有目的、有针对性、多样化攻击和破坏活动的频繁发生，攻击点也越来越趋于集中和精确，攻击破坏的影响面不断扩大并产生连环效应，这就势必需要构筑一种主动的安全防御，才有可能最大限度地有效应对攻击方式的变化。

写作本书的目的主要是通过介绍黑客的攻击手段和提供相应的主动防御保护措施，使读者能够循序渐进地了解黑客入侵防御的关键技术与方法，提高安全防护意识，在实际遇到黑客攻击时能够做到“胸有成竹”。

希望读者能够运用本书介绍的知识去了解黑客，进而防范黑客的攻击，使自己的网络更加安全。

本书特别注重实例的讲解，针对每一种攻防手段，都结合实例来进行介绍，并紧紧围绕黑客的“攻与防”这一主线，告诉读者如何建立个人电脑的安全防护措施，使自己远离黑客攻击的困扰，确保自己电脑数据的安全。

本书通俗易懂、图文并茂，即使是电脑新手也能无障碍阅读；任务驱动式的黑客软件讲解，揭秘每一种黑客攻击的手法；最新的黑客技术盘点，让用户“先下手为强”；攻防互参的防御方法，全面确保用户的网络安全。

本书具有如下特色：讲解从零起步，由浅入深，步步深入，通俗易懂，使初学者和具有一定基础的用户都能逐步提高，快速掌握黑客防范技巧与工具的使用方法。

理论和实例相结合，实用性强，并配以大量插图和配套光盘视频讲解，力图使读者能够融会贯通。

介绍大量的小技巧和小窍门，可使读者节省大量宝贵的摸索时间。

重点突出，内容丰富，操作步骤详细，并附有大量的操作实例，读者可以一边学习，一边在电脑上操作，做到即学即用、即用即得，快速学会操作方法。

本书在编写的过程中，得到了许多热心网友的支持，部分参考了来自网络的资料，并对这些资料进行了再加工和深化处理，在此对这些资料的原作者表示衷心的感谢。

参与本书编写的人员有武新华、刘岩、段玲华、杨平、李防、李秋菊、陈艳艳、李伟、冯世雄、孙世宁、张晓新等。

我们虽满腔热情，但限于自己的水平，书中的疏漏之处在所难免，欢迎广大读者批评指正。

最后，须要提醒大家的是：根据国家有关法律规定，任何利用黑客技术攻击他人的行为都属于违法行为，希望读者在阅读本书后不要使用本书中所介绍的黑客技术对别人进行攻击，否则后果自负。

## <<铜墙铁壁>>

### 内容概要

本书紧紧围绕黑客防范技巧与工具展开，在剖析用户进行黑客防御中迫切需要用到或想要用到的技术时，力求对其进行“傻瓜式”的讲解，使读者对网络防御技术形成系统了解，能够更好地防范黑客的攻击。

全书共分为11章，主要内容包括：Windows系统漏洞防范，木马和间谍软件的伪装与查杀，Web攻防实战演练，QQ与MSN的攻击与防御技术，电子邮件攻防实战，后门与自身防护技术，网络代理与恶意进程清除，全面提升自己的网络功能，数据备份与恢复，打好网络安全防御战等。

本书内容丰富、图文并茂、深入浅出，不仅适用于广大网络爱好者，而且适用于网络安全从业人员及网络管理员。

## 书籍目录

前言第1章 Windows系统中的漏洞 1.1 Windows系统的安全隐患 1.2 Windows操作系统中的漏洞 1.3 黑客常用的入侵方式 1.4 系统安全防护对策 1.5 可能出现的问题与解决 1.6 总结与经验积累 第2章 Windows系统漏洞防范 2.1 设置组策略提高系统性能 2.2 注册表编辑器实用防范 2.3 Windows系统的密码保护 2.4 Windows系统的安全设置 2.5 可能出现的问题与解决 2.6 总结与经验积累 第3章 木马和间谍软件的伪装与查杀 3.1 火眼金睛识别木马 3.2 使用木马清除软件清除木马 3.3 自动安装“后门程序”的间谍软件 3.4 来自微软的反间谍专家 3.5 可能出现的问题与解决 3.6 总结与经验积累 第4章 Web攻防实战演练 4.1 恶意代码简介 4.2 修改注册表防范恶意代码 4.3 Web攻击与防范技术 4.4 可能出现的问题与解决 4.5 总结与经验积累 第5章 QQ与MSN的攻击与防御技术 5.1 常见的QQ攻击技术曝光 5.2 QQ信息炸弹与病毒攻击曝光 5.3 保护自己的QQ 5.4 MSN的攻击和防御 5.5 可能出现的问题与解决 5.6 总结与经验积累 第6章 电子邮件攻防实战 6.1 WebMail邮件攻防实战 6.2 揭秘POP3邮箱密码探测 6.3 常见E-mail攻击手段与防范 6.4 全面防范邮件病毒 6.5 邮件收发软件的漏洞攻防 6.6 可能出现的问题与解决 6.7 总结与经验积累 第7章 后门与自身防护技术 7.1 后门技术的实际应用 7.2 清除登录服务器的日志信息 7.3 清除日志工具elsave和CleanIISLog 7.4 网络防火墙技术 7.5 可能出现的问题与解决 7.6 总结与经验积累 第8章 网络代理与恶意进程清除 8.1 跳板与代理服务器 8.2 代理工具的使用 8.3 恶意进程的追踪与清除 8.4 可能出现的问题与解决 8.5 总结与经验积累 第9章 全面提升自己的网络功能 第10章 数据备份与恢复 第11章 打好网络安全防御战

## &lt;&lt;铜墙铁壁&gt;&gt;

## 章节摘录

插图：4.4可能出现的问题与解决（1）不必要代码和恶作剧程序能否被看作是恶意代码？

解答：不必要代码（Unwanted Code）是指没有作用却会带来危险的代码。

它比恶意代码具有更宽泛的含义，包括所有可能与某个组织安全策略相冲突的软件。

一个更为安全的理解就是把所有不必要的代码都看作是恶意的。

相比恶意代码的特征来讲，虽然一些恶作剧程序或游戏本身也是程序，且通过执行来发生作用，但因其没有恶意的目的，故不能看作是恶意代码。

（2）XSS漏洞能否在服务器上执行？

通过网站加密能否防止XSS攻击？

解答：XSS漏洞会导致Javascript恶意脚本的插入，但其执行也会受到很多限制。

因此，如果攻击者利用浏览器的漏洞，就有可能在用户的计算机上执行命令，若其执行命令只能在客户机上，而不能在服务器上执行。

简单地说，通过XSS漏洞可以触发客户端的其他漏洞。

对网站加密（如使用SST加密）之后，Web程序仍然是以同样的方式在工作，而攻击也可能会通过加密的连接实现，故而即使对网站加密也不能防止利用XSS漏洞的攻击。

要防范XSS攻击最好还是过滤所有特殊字符、对数据的写入和读出均进行特殊编码。

而对于用户来讲，就是不要随便点击陌生的链接等。

## <<铜墙铁壁>>

### 编辑推荐

《铜墙铁壁:黑客防范技巧与工具》特别注重实例的讲解，针对每一种攻防手段，都结合实例来进行介绍，并紧紧围绕黑客的“攻与防”这一主线，告诉读者如何建立个人电脑的安全防护措施，使自己远离黑客攻击的困扰，确保自己电脑数据的安全。

<<铜墙铁壁>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>