<<防御！　网络攻击内幕剖析>

图书基本信息

书名：<<防御！
网络攻击内幕剖析>>

13位ISBN编号：9787115215437

10位ISBN编号：711521543X

出版时间：2010-1

出版时间：人民邮电出版社

作者：穆勇，李培信　编著

页数：388

前言

在全球信息化高速发展的今天，随着互联网普及和企业信息化的快速建设，电子商务、电子政务、网上银行、网络游戏已成为当前IT技术的应用热点，企业服务必须与网络结合才能准确把握未来新技术的趋势。
随着各方面对网络信息技术依赖性的不断加强，网络信息安全的重要性日益突出。
近年来，我国互联网用户保持快速增长，根据2009年中国互联网络信息中心（CNNIC）最新报告，截至2008年底，中国网民规模达到2.98亿人，互联网普及率达到22.6%，略高于全球平均水平（21.9%）。
中国互联网高速发展的同时也出现了很多网络安全事件，尤其近年来，其中的突出问题就是网络伪造、木马及间谍软件、软件破解、黑客网络争斗（例如因黑客利益争斗而导致的区域DNS服务器瘫痪事件）等。
网络安全成为公众和企业关注的焦点。
所以说，网络的安全性已经成为阻碍信息化进程的重要因素之一，而我国网络安全工作起步较晚，许多技术还有待提高，我国网民虽然数量庞大，但整体安全意识不高，再加上网络安全是一门涵盖较多领域的学科，包括加密解密、计算机应用技术、网络接入技术、网络攻防技术等，使得我国网络安全工作更难以展开。
网络安全知识的普及刻不容缓。
净化网络环境，提高网络安全是网络安全工作者必须肩负的使命。
作者曾在信息安全机构针对网络攻防进行了一年的研究。
如今，企业通过广泛部署通信安全协议以及进行各种安全设置，可以解决部分安全问题。
但是，一般性的代码漏洞、操作系统漏洞、木马和病毒等依然严重威胁着网络的安全。
作者在规划本书结构时，曾想把重点放在计算机及网络安全的理论知识，但通过深思熟虑，决定将重点放在技术剖析，因为这样，才能解决技术人员及读者朋友面对的实际问题。
本书以网络安全的攻击演示与防御手段演示为主线，以案例演示的形式对常见的网络安全攻防手段作了介绍，使读者能够更准确地把握这类的攻击手法与防范技巧。
对于重要的操作步骤，本书通过图文结合的形式展现给读者，相信读者能够快速地理解并掌握。
由于作者水平有限，书中的缺点和错误在所难免，欢迎读者批评指正。

<<防御！　网络攻击内幕剖析>

内容概要

网络安全是目前非常热门的领域，无论是个人还是企业都越来越关注网络安全。
本书从网络安全的基础讲起，从“攻”和“防”两个不同的角度，通过多个网络安全案例为读者剖析了常见的入侵和反入侵的手法。
本书从初学者的角度对多种网络威胁的原理和防御方法进行了详细的介绍与演示，能使读者对网络安全领域常见的攻防技术有较为深入的认识。

本书包含的大量攻防演示均有很强的实际指导意义，而且每个演示都给出了详细的操作步骤及图文解说，方便读者更快地掌握网络攻防的原理和技术。

本书适合对网络安全和黑客攻防感兴趣的读者，以及从事网络相关工作，想对网络安全有进一步了解的读者，也可作为高校计算机专业信息安全课程的实践参考资料。

<<防御！　网络攻击内幕剖析>

书籍目录

章节摘录

插图：1.网络物理安全网络的物理安全是整个网络系统安全的前提，由于网络系统属于弱电工程，耐压值很低，因此，在网络工程的设计和施工中，必须优先考虑保护网络设备不受电、火灾和雷电的侵害；考虑布线系统与照明电线、动力电线、通信线路、暖气管道及冷热空气管道之间的距离；考虑布线系统和绝缘线、裸体线以及接地与焊接的安全；必须建设防雷系统，防雷系统不仅考虑建筑物防雷，还必须考虑计算机及其他弱电耐压设备的防雷。
2.网络结构安全网络拓扑结构设计也直接影响到网络系统的安全性。
例如，在外部网络和内部网络进行通信时，内部网络的计算机安全就会受到威胁，同时也影响在同一网络上的许多其他系统，通过网络传播，还会影响连接到互联网／Intranet的其他网络。
因此，我们在设计时有必要将公开服务器（Web、DNS、E-mail等）和外网及内部其他业务网络进行必要的隔离，避免网络结构信息外泄；同时还要对外网的服务请求加以过滤，只允许正常通信的数据包到达相应主机，其他的请求服务在到达主机之前就应该遭到拒绝。
3.系统安全目前恐怕没有绝对安全的操作系统可以选择，无论是微软公司的WindowsServer2003或者其他任何商用UNIX类操作系统，其开发厂商必然有其Back-.Door。
因此，我们可以得出如下结论：没有完全安全的操作系统。
不同的用户应从不同的方面对其网络作详尽的分析，选择安全性尽可能高的操作系统，并对操作系统进行安全配置。
而且，必须加强登录过程的认证（特别是在到达服务器主机之前的认证），确保用户的合法性；其次应该严格限制登录者的操作权限，将其完成的操作限制在最小的范围内。
4.应用系统安全应用系统的安全跟具体的应用有关，它涉及面非常广。
应用系统的安全是动态的、不断变化的，在应用系统的安全性上，主要考虑尽可能建立安全的系统平台，而且通过专业的安全工具不断发现漏洞，修补漏洞，提高系统的安全性。
应用的安全性涉及信息、数据的安全性，例如，在某些网络系统中，涉及很多机密信息，如果一些重要信息遭到窃取或破坏，它的经济影响、社会影响和政治影响将是很严重的。
5.管理的安全风险管理是网络安全中最重要的部分之一。
责权不明，安全管理制度不健全及缺乏可操作性等都可能引起管理安全的风险。
当网络中出现攻击行为或网络受到其他一些安全威胁时（如内部人员的违规操作等），网络管理人员无法进行实时的检测、监控、报告与预警。
同时，当事故发生后，也无法提供入侵行为的追踪线索及破案依据，即缺乏对网络的可控性与可审查性。
这就要求我们必须对站点的访问活动进行多层次的记录，及时发现非法入侵行为。

编辑推荐

《防御！
网络攻击内幕剖析》：网络安全人才网李伟(CEO)推荐网络技术的爱好者和企业的网络安全人员无疑又多了一位良师益友。
《防御!网络攻击内幕剖析》不仅讲述了网络攻击的各种表现形式，更深层次分析了网络攻击的内幕，相信多数的读者在读了此书后，会有更多与时俱进的心得体会，也能够获得在网络安全领域更高的造诣。
精彩范例，原创展现!端口扫描、系统漏洞SQL注入、漏洞提权、跨站脚本后门与口令渗透、脚本、局域网、ARP嗅探、监控、溢出攻击手段、攻击原理多方位技术服务每章节的软件下载、PPT演示、视频指导免费赠送戴威尔网络安全培训中的黑客攻防课程黑客安全技术交流社区安全专家内幕答疑，参透黑客入侵暗器详细的攻防演示操作步骤及图文解说线上赠送海量软件下载，PPT演示，视频指导