<<网络渗透攻击与安防修炼>>

图书基本信息

书名：<<网络渗透攻击与安防修炼>>

13位ISBN编号：9787121083198

10位ISBN编号：7121083191

出版时间：2009-4

出版时间：电子工业出版社

作者：肖遥

页数：648

前言

应广大读者朋友的要求，《网络渗透攻击与安防修炼》终于和广大读者见面了。
这部网络安全专著分9章，随书附带教学视频。
本书兼顾学习与参考两个目的，以广大网络管理员、安全工作者和高级网络用户为服务对象，也可供普通电脑用户了解和学习网络安全技术之用。

笔者不避寒暑，历时一载有余，三易其稿，反复修改、增删，其所追求的目标，可以概括为6个字：专业、深入、权威。

挑战与危机　　近几年来，随着网络应用的飞速发展，各种网络攻击事件也层出不穷，对网络管理员和网络安全工作者提出了更高的要求。
以“国家计算机网络应急技术处理协调中心（CNCERT）”于2008年底发布的网站攻击统计表为例，在2008年1月至12月，中国大陆地区.gov.cn网站被篡改数量各月累计达3595次，其中不重复的即有2891个。

针对网站的攻击是明显的、易于统计的，但是针对网络进行的综合渗透攻击事件相对则要隐蔽得多，统计也不容易，因此也未能像其他网络攻击事件一样引起广泛重视。
事实上，渗透攻击的发生率和危害性远远大于普通的网络攻击事件。
许多网络被渗透入侵长期控制，造成大量机密信息泄露和巨额经济损失。

网络渗透攻击事件的发生极为普遍，众多的网络管理员和网络安全工作者却对网络安全环境所面临的严峻考验缺乏足够的认识，因而也未曾采取全面的防范补救措施应对各种攻击行为。

入侵腾讯事件，暴露“学”与“术”的误区　　目前，市面上关于网络入侵与安全防护的书籍已经非常多了，其中不乏许多资深安全专家的精品之作。
同时，有越来越多从事网络安全的管理人员和工作者，开始认识到所面临的网络安全危机，积极参加各种安全培训与认证考试。
然而，许多安全书籍和各种认证培训，往往都走入了一个不易察觉的误区。

<<网络渗透攻击与安防修炼>>

内容概要

这是一本关于网络渗透攻击与防范的书籍。
全书共分为9章，主要内容包括：网络渗透攻击行为及分析、攻击者如何打开渗透突破口、渗透中的入侵与提权、远程控制入侵、大型网络环境的深入探测、渗透入侵中的社会工程学等。

本书与其他书籍不同的特色之处在于，本书特别有针对性地以曾经热炒一时的“入侵腾讯事件”为例，以再现“入侵腾讯事件”为流程，对渗透入侵过程进行了深入的分析揭秘。
书中全面系统地讲解了攻击者在渗透中可能采取的各种入侵手法，并给出了高效的防范方案，有助于网络安全维护人员掌握黑客的攻击行为，更好地维护网络安全。

本书可作为专业的网络安全管理人员、网络安全技术研究者阅读，在实际工作中具有极高的参考价值；也可作为相关专业学生的学习资料和参考资料。
光盘中提供攻防实战演练与视频讲解，以及书中涉及的实例源代码。

作者简介

肖遥，网名“ 冰河洗剑 ”，国内著名网络安全技术独立研究人士。

曾从事国防军工设计，参与过J10A、J11B等战斗机配套武器研制，独立开发出HF25火箭发射器，参与DF8GA及导弹发射架等武器设计。

潜心钻研网络安全技术10余年，长期担任国内多家著名网站的发全顾问，专业从事网络渗透测试与网络风险评估。

长年在《黑客X档案》、《黑客防线》等杂志撰写安全类稿件，也是国内知名电脑杂志《电脑迷》、《大众软件》、《网友世界》、《电脑报》特约作者。
撰稿6年，累计发表报刊作品达五百余万字，出版《黑客大曝光》、《黑客成长日记》、《无毒一身轻》等多部安全类畅销技术专著。
其中，《网站入侵与脚本安全攻防修炼》一书已被中国台湾等地引进版权，以繁体版本中当地发行。

<<网络渗透攻击与安防修炼>>

书籍目录

章节摘录

第1章　分析入侵腾讯事件，初识网络渗透　　1.1　网络渗透概述　　1.1.1　以“蚁穴”引发“堤崩”——渗透的特质　　1. 什么是网络渗透攻击　　网络渗透是攻击者常用的一种攻击手段，也是一种综合的高级攻击技术，同时网络渗透也是安全工作者所研究的一个课题，在他们口中通常被称为“渗透测试(PenetrationTest)”。

无论是网络渗透(Network Penetration)还是渗透测试(Penetration Test)，其实际上所指的都是同一内容，也就是研究如何一步步攻击入侵某个大型网络主机服务器群组。

只不过从实施的角度上看，前者是攻击者的恶意行为，而后者则是安全工作者模拟入侵攻击测试，进而寻找最佳安全防护方案的正当手段。

随着网络技术的发展，在政府、电力、金融、教育、能源、通信、制造等行业的企业网络应用日趋普遍，规模也日渐扩大。

在各个公司企业网络中，网络结构越来越复杂，各种网络维护工作也极为重要，一旦网络出现问题，将会影响公司或企业的正常运作，并给公司或企业带来极大的损失。

在各种网络维护工作中，网络安全维护更是重中之重。

各种网络安全事件频频发生，不时见诸于报纸头条和网络新闻，大型企业公司的网络也逃不过被攻击的命运。

网络安全工作保障着网络的正常运行，避免因攻击者入侵带来的可怕损失。

为了保障网络的安全，网络管理员往往严格地规划网络的结构，区分内部与外部网络进行网络隔离，设置网络防火墙，安装杀毒软件，并做好各种安全保护措施。

然而绝对的安全是不存在的，潜在的危险和漏洞总是相对存在的。

面对越来越多的网络攻击事件，网络管理员们采取了积极主动的应对措施，大大提高了网络的安全性。

恶意的入侵者想要直接攻击一个安全防御到位的网络，看起来似乎是很困难的事情。

于是，网络渗透攻击出现了。

对于大型的网络主机服务器群组，攻击者往往不会采取直接的攻击手段，而是采用一些迂回渐进式的攻击方法，长期而有计划地逐步渗透攻击进入网络，并完全控制整个网络，这就是“网络渗透攻击”。

攻击者要直接通过设置森严的网络关卡进入网络是不可能的，然而无论怎么样设置网络，总会有一些或大或小的安全缺陷或漏洞。

而攻击者所做的，就是在一个看似安全的网络上，找到一个小缺口，然后一步一步地将这些缺口扩大，扩大，再扩大，最终导致整个网络安全防线的失守，掌控整个网络的权限。

对网络管理员来说，网络上的某个小小的安全缺陷，就好似一个微不足道的“蚁穴”，然而忽略了对它的重视，最终的结果将十分可怕，它将会引发整个网络安全防御堤坝的全面崩塌。

因此，作为网络管理员，完全有必要了解甚至掌握网络渗透入侵的技术，这样才能有针对性地进行防御，真正保障网络的安全。

<<网络渗透攻击与安防修炼>>

编辑推荐

探讨所有安全工作者无可回避的话题，揭秘网络服务器群组如何被渗透入侵，基于原理与实例的全面渗透防御方案，视频CD全程再现数十种黑客攻击战法。

一本内行人写给行内人的网络安全著作。

一个跨越新闻、娱乐、游戏、聊天和网购等众多网络平台与业务的大型网络公司，众多网络巡全专家构建的重重安全防线，为何在16岁的少年“ 黑客 ”面前被轻易击破？

权威人士揭秘网络中轰动一时的“ 入侵腾讯事件 ”，还原黑客入侵攻击腾讯事件的真相，分析黑客渗透入侵攻击中的种种手法，指出网络安全的软件与漏洞，加固你的网络安全防线。

<<网络渗透攻击与安防修炼>>

版权说明