<<大中型网络入侵要案直击与防御>>

图书基本信息

书名：<<大中型网络入侵要案直击与防御>>

13位ISBN编号：9787121117404

10位ISBN编号：7121117401

出版时间：2010年11月

出版时间：电子工业出版社

作者：肖遥

页数：598

前言

目前互联网应用越来越广泛，黑客与病毒无孔不入，这极大地影响了Internet的可靠性和安全性，保护Internet、加强网络安全建设已经迫在眉睫。
相对于普通个人用户或小型网络来说，各种企业公司的大中型复杂网络的信息安全工作尤其困难。
许多实际经验不足的网络管理员和信息安全工作者，在面对大中型网络安全管理与维护时，常常无从下手，或者步入误区和歧途。
大中型网络安全防御中的误区在各种企业公司的大中型网络中，网络信息安全尤其重要，一旦网络系统安全受到严重威胁，甚至处于瘫痪状态，企业将遭受巨大的经济损失。
然而在众多大中型网络信息安全管理员者和工作者中，却存在着一个很普遍的意识误区。
许多网络信息安全管理员者和工作者，在工作中往往过于依赖硬件防火墙、入侵检测系统等安全设备，对各种安全理论也有比较深的认识，然而却无法应付现实工作中的一些“脚本小子”的攻击行为。
尤其是在各种大中型网络管理中，由于网络结构复杂，安全工作常常无法做到位。
借助于各种硬件安全设备和现成的防御方案，建立起一道看似坚固的安全防线，可是由于对黑客入侵攻击的方法与途径并不是很了解，导致表面坚固的安全防线之下，其实却隐藏着许多遗漏的安全死角。
许多结构复杂的大中型企业、公司、政府、网站等网络中，貌似坚固安全，实际不堪一击，黑客可以轻易入侵攻击整个网络。
在本书开篇中，对国内互联网上的四大门户网站进行了入侵检测。
事实证明即使是如此知名的网络公司，拥有众多的信息安全管理员者和工作者，依然会被黑客轻易地入侵攻击。
这在很大程度上反映了一个很严重的问题，国内大中型网络安全防御面临着极大的危机和威胁，大中型网络安全防御工作中有着许多不足，必须加以实质性地改进。
“双手互搏”，安全之道如何才能更好地完善各种大中型网络安全防御工作呢？
国内一位资深网络安全专家曾说过，从事计算机网络管理与信息安全的人员，应该学会“左手画方，右手画圆”的双手互搏之术，让自己的左脑成为网络安全方面的顶尖高手，让自己的右脑成为顶尖的黑客高手，这样才能真正理解和保障网络信息安全。
一个合格的网络信息安全管理员者，首先应该是一个技术很好的黑客。
作为经过系统的网络信息安全理论学习的管理员或工作者，往往有一种天生的优越感，看不起一些所谓的黑客，视黑客技术为旁门左道。
正是这样的认识，阻碍了许多网络信息安全管理员者和工作者前进的脚步。
正所谓知己知彼，方能百战不殆，学习并且精通黑客技术，才能了解知道黑客从何处入侵进入，利用哪种方法或漏洞进行攻击，从而更有针对性地进行安全防御，提高安全工作的效率。
特别是在各种环境复杂的大中型网络中，如果对黑客入侵攻击的途径与方法不熟悉，安全工作常常挂一漏万，又或者失之毫厘，谬以千里。
网络信息安全管理员者和工作者，是非常有必要了解和学习黑客入侵技术的。
因此，本书对各种常见的大中型网络攻击类型，对黑客入侵攻击大中型网络的途径、方法、利用的工具与防范方法等进行了详细的介绍，以弥补网络信息安全管理员者和工作者经验的不足和技术上的欠缺，以期更好地完善安全防御工作。
关于本书的内容安排本书主要针对大中型网络中最常碰到的木马攻击、网站入侵、内部渗透等进行了介绍，以各种最典型的大中型网络攻击案例解析的形式，来安排讲解各种网络攻击与防护技术。
各篇章的内容按照以下形式进行安排：1．典型攻防案例再现；2．案例的简单分析；3．黑客攻击技术的系统讲解；4．网管安全防护解决方案；5．入侵手法与防护难点深度分析。
其中，第1部分的典型案例再现真实的黑客攻击大中型网络事件，作为整章内容的引子与线索。
在案例介绍中，读者将会看到黑客入侵攻击的真实过程，从中对黑客入侵的目标、途径与方法有一个直观感性的认识。
在第2部分中，简单分析案例中所涉及的攻击技术与安全防护手段，以对整篇内容提纲携领。

第3部分与第4部分是重点内容。
其中第3部分从黑客攻击者的角度，系统详细全面地讲解相应网络环境下的黑客攻击技术，第4部分则从网络信息安全管理员与工作者的角度介绍详细专业的安全防护方案。
第5部分是各种安全攻击技术及相应理论知识的深度分析，从攻击与防守的角度结合，深入分析一些新技术和有价值的技术难点。
此外，除了每一篇中的典型案例，又加入了许多辅助和参考案例，使所介绍的知识与实际结合更为紧密。

内容概要

本书以解析各种网络环境下攻防案例的形式来讲解各种网络攻击与防护技术，从“黑客攻击”与“安全工作者防守”双向角度来进行介绍。
每一章节的内容按照如下脉络展开：典型攻防案例再现→案例的简单分析→黑客攻击技术的系统讲解→网管安全防护解决方案→入侵手法与防护难点深度分析。
全书真实呈现完整的攻击与防护事件，可让读者了解到攻击者如何选择攻击目标，如何制订攻击方案，如何绕过攻击中碰到的问题，网管通常采用哪些防护手法，安全漏洞在何处，网管又如何追踪攻击者，等等，因此对学习者和工作者来说都很有吸引力和参考价值。
本书是网络管理员、信息安全管理员、对网络安全感兴趣的人员必备的参考书，也可供大中院校或培训学校教师和学生阅读和参考。

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安全顾问，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》等国内安全专业媒体上与同行分享最新研究成果。
出版有《网络渗透攻击与安防修炼》、《网站入侵与脚本安全攻防修炼》、《黑客大曝光》、《黑客攻防大揭密》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》一书已输出至中国台湾等地。

<<大中型网络入侵要案直击与防御>>

书籍目录

章节摘录

插图：在上一章的入侵测试过程中，我们可以看到，众多的门户网站表面上看起来固若金汤，但事实上却存在着一些不为安全管理人员所注意的漏洞。
然而正是这看起来“小、旧”的漏洞，成为整个安全防线上的最弱之处，最终可能导致整个网络安全防线全面失守。
这次的入侵测试，事实上也反映了当前国内网络安全行业中最为普遍的一些安全意识误区，许多大型的公司企业及各种行业网络中，都或多或少地存在着下面一些安全误区。
误区1：缺乏网络安全整体意识，过于偏重或忽略了网络安全维护工作中的某一方面。
·误区2：过于侧重网络安全的理论研究，是典型的网络安全学院派，而不屑于各种黑客入侵技术。
·误区3：过于依赖于入侵检测系统、硬件防毒墙、防火墙等网络安全设备，认为安装了这些安全设备就可以高枕无忧了，忽视了在网络安全维护中人为因素也很重要。
误区4：对各种新出现的漏洞很重视，对一些过时的旧漏洞不太关注。
有许多网络安全管理人员定期进行着各种网络安全维护工作，例如随时为服务器打补丁，能够补救安全漏洞：安装防病毒软件和防火墙；为确保服务器安全，频繁更改复杂的口令；定期对数据进行备份；严格控制邮件、网页与移动存储设备病毒传播等。
这些工作都落到了实处，但为什么网络还是遭受黑客入侵攻击呢？
在网络安全业内流传着一句经典的话——“网络安全是一个整体，安全等级取决于最弱处”。
木桶理论同样适用于网络安全行业，对整个网络安全工作意义的评估，不在于安全防护最强处有多么强，而取决于网络安全防护的最弱处。
“一只木桶盛水的多少，并不取决于桶壁上最高的那块木块，而恰恰取决于桶壁上最短的那块。”根据这一核心内容，木桶理论还有两个推论：其一，只有桶壁上的所有木板都足够高，那木桶才能盛满水。
其二，只要这个木桶里有一块不够高度，木桶里的水就不可能是满的。
同样，在网络安全中只有各方面的安全维护工作都做充分，网络才是安全的；只要网络安全维护工作中有任何一处疏忽遗漏，那么即使其他方面安全性再强，整个网络也是不安全的。
在前面的入侵测试中，可以看到虽然新浪青岛分站服务器操作系统及时进行了更新，打上了各种系统软件漏洞补丁，屏蔽了各种危险的端口，但是却忽视了对网站网页程序漏洞的弥补，因此导致分站服务器被入侵控制。
网站程序漏洞，成为新浪青岛分站服务器安全维护中最短的那一块木板。

编辑推荐

《大中型网络入侵要案直击与防御》：从门户网站窥见网络安全洞，网络安全“木桶理论”与“整体观”的实践，现场直击大中型网络安全漏洞，提示大中型网络安全防护缺陷大中型网络攻击重大案件还原，马行天下，特洛伊之计，木马不被查杀的秘密，行为监控，木马与主动防御的较量，大中型网络中阻截木马，嫁祸网站-网页挂马藏危机，网页木马的加密与解密，Serv-U7／8提权新技术，MSSQL/MYSQL/ORACEL注入攻击剖析，各种数据库提权漏洞，内网ARP欺骗与嗅探技术，L-IIUX系统环境下的入侵提权与远程控制，《大中型网络入侵要案直击与防御》的目的绝不是为那些怀有不良动机的人提供支持，也不承担因为技，术被滥用所产生的连带责任：《大中型网络入侵要案直击与防御》的目的在于最大限度地唤起大家的网络安全意识，正视我们的网络世界所面临的一场危机，并采取行动。