<<企业网络安全维护案例精粹>>

图书基本信息

书名：<<企业网络安全维护案例精粹>>

13位ISBN编号：9787121069642

10位ISBN编号：7121069644

出版时间：2008-7

出版时间：电子工业出版社

作者：曹鹏

页数：338

<<企业网络安全维护案例精粹>>

内容概要

本书来自作者的实际工作经验积累，所有章节都由现场精彩案例积累而成，涉及当前经常困扰企业安全管理员的常见问题。
本书一开始就从真正的黑客攻击讲起，首先带领读者尝试站在一个攻击者的角度看待系统的脆弱性，体会一个攻击者的攻击思路，为全书的安全防护技巧打下基础。
然后从前门攻击、后门攻击、非直接攻击与网络设备的安全隐患全面介绍当前网络攻击者的攻击方式，此外，还介绍了企业环境内安全漏洞的评估方法、入侵与入侵检测系统分析、日志分析、压力测试与性能测试等内容。

<<企业网络安全维护案例精粹>>

书籍目录

章节摘录

第1章　隐蔽的非直接攻击今天的信息安全技术已不再简单地停留在理论探讨的层面，网络中无所不在的攻击者随时可能出现，真正掌握信息安全技术操作非常关键。
本书的重点是介绍一种真正可以操作的日常信息安全管理技术。
信息安全风险包含的范围很大，本书仅仅是探讨由于攻击者出现所带来的实际威胁和服务器的安全弱点，让我们从了解攻击和攻击者开始本书的内容吧。
攻击的分类在不同的安全标准和安全专家的解释中都是不大相同的，对于一些专门研究攻击方法的组织来说可能细化到10多个种类。
本着将复杂的事情尽量简单化的原则，我们将攻击的种类分成了3类：即非直接攻击、前门攻击和后门攻击，这种分类方法简单可行并且容易理解和记忆。
1.1 目标服务信息收集（踩点）很多时候收集被攻击目标的各种信息是攻击者开始一次攻击的第一个步骤，把它放在非直接攻击来讲是因为我们很难分清正常访问和攻击者踩点访问的区别，他们都是通过正常的开放端口进来访问，只不过获取的信息不同而已。
当一个攻击者确定了一个攻击目标主机后第一步做的就是对目标主机进行一次详细的信息收集，扫描工具是必不可少的，但如果仅仅依靠扫描工具的可怜的报告来判断我们的目标存在什么漏洞是非常不可信的。
到目前为止，还没看到哪款软件可以产生完全让人满意和信服的报告结果。
显然，真正的攻击者也早就意识到了这一点，下面介绍手动的信息收集步骤，希望可以对读者有所帮助。
1.1.1　小心域名服务解析你的站点结构通过DNS查询得到目标的网络拓扑基本情况，目前很多主机的DNS服务器配置得并不安全，用1s命令就可以泄露出自己的内部网络结构，得到这些信息可以方便我们摸清对方网络的组成情况。

<<企业网络安全维护案例精粹>>

编辑推荐

《企业网络安全维护案例精粹》适合网络安全技术爱好者、企事业单位的网络管理维护人员阅读，也可作为网络工程师、高等院校相关专业师生的学习参考用书。

<<企业网络安全维护案例精粹>>

版权说明