

<<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

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>

<<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。

书籍目录

第1章 隐蔽的非直接攻击 1.1 目标服务信息收集(踩点) 1.1.1 小心域名服务解析你的站点结构
1.1.2 无声息的路由追踪 1.1.3 SNMP服务可以透露多少小秘密 1.1.4 WHOIS查询与旁注攻击
1.1.5 实地勘察让你大吃一惊 1.2 防不胜防的社交工程学 1.3 网络钓鱼的技术分析 1.4 拒绝服务
攻击 1.4.1 SYN FLOOD和LAND攻击 1.4.2 有趣的QQ消息拒绝服务攻击实例 1.5 搜索引擎隐藏
的秘密 1.6 自己搜索更疯狂 1.7 面对目标扩大攻击范围 1.8 垃圾邮件的深层技术分析第2章 前门攻
击与后门渗透的破坏力 2.1 前门攻击用最快的速度找到你的口令 2.2 本地办公文档文件密码破解
2.2.1 可以直接获取明文密码的Access文件 2.2.2 Office文档RC4加密算法的40位隐藏陷阱 2.3 从网
络中直接嗅探收集密码 2.4 无需口令也可以进入服务器的破解方法 2.5 ADSL拨号设备默认配置不
安全性研究 2.6 挂马式的入侵攻击方式 2.7 利用脚本程序的判断错误无需真正口令进入管理界面
2.8 HP服务器与打印机的两个常见“后门” 2.9 物理上的后门漏洞也不可疏忽 2.10 后门攻击
2.10.1 改变站点动态脚本程序的执行方向ASP注射攻击 2.10.2 ARP欺骗的“中间人攻击” 2.10.3 内
部办公室大面积的ARP欺骗的实施 2.10.4 MS05039的缓冲区溢出攻击第3章 网络设备的安全隐患不
容忽视 3.1 网络设备并非安全固体 3.1.1 采用默认口令的安全问题 3.1.2 SNMP的默认配置问题
3.1.3 HTTP管理接口的越权通道 3.2 设置交换机的侦听口以监视网络会话 3.2.1 交换机侦听口是把
双刃剑 3.2.2 常见交换机端口监听的配置第4章 风险评估之最佳扫描工具 4.1 网络安全评估系统的
使用介绍 4.1.1 排名第一的安全工具NESSUS 4.1.2 Shadow Security Scanner 4.1.3 国产软件天镜漏
洞扫描器 4.1.4 手持性掌上漏洞扫描——漏洞可以随处发现 4.1.5 从FoundStone看未来安全弱点发
现产品的发展方向 4.1.6 漏洞扫描软件的几个使用技巧 4.2 数据库扫描器评估数据安全 4.2.1 一
次SQL Server的渗透攻击测试 4.2.2 数据库服务器的默认用户名与登录口令 4.2.3 针对数据库的漏
洞扫描系统 4.4 利用ARP技术寻找网络隐藏的嗅探攻击 4.5 脆弱性口令的评估方法第5章 手工评
估思路与工作方法 5.1 利用漏洞资料库完成评估工作 5.2 利用SNMP服务的评估方法 5.3 自主开发
业务系统安全性风险分析 5.3.1 C/S结构平台的问题 5.3.2 Web脚本程序的安全分析方法 5.3.3
平台的设置不当与功能局限 5.3.4 底层网络通信的问题 5.3.5 开发过程中的版本控制 5.3.6 测试
应用程序通信接口的抗攻击能力 5.4 Microsoft: Baseline Security Analyzer本地化分析 5.5 安全管理策
略的自动化评估系统 5.5.1 利用“眼镜蛇”来实现标准的问卷调查 5.5.2 微软安全风险自我评测工
具(MSAT) 5.5.3 利用问卷调查分析当前安全管理体系中的问题 5.5.4 常见安全管理体系中出
现的问题举例第6章 入侵者与入侵检测第7章 小投入大产出的日志分析第8章 巧妙的压力测试与性
能测试第9章 为信息传递把锁第10章 兵临城下的加密破坏者第11章 面对攻击的必备工具箱第12章
应对锦囊与精彩案例分析

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

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>