第一图书网, tushu007.com

<<黑客攻防实例100%>>

图书基本信息

书名：<<黑客攻防实例100%>>

13位ISBN编号：9787894916426

10位ISBN编号：7894916420

出版时间：2008-7

出版时间：山东电子

作者：电脑报

页数：240

字数：300000

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

内容概要

本书通过对100余个黑客攻击与防范的实战演示进行讲解，详细的剖析了黑客的攻击手段和对应防范方法，让读者能够对黑客技术有系统全面的了解，以便更好地防范黑客，保障系统安全。
　全书共分10章，其中信息的收集和反收集、病毒木马及流氓软件的防范与查杀、识别网络欺骗和突破网络限制的方法等章节是黑客攻防的基础，漏洞攻击与恶意代码的防范、控制与反控制、加密解密、账户与口令密码的攻防是黑客常用的手段和方法；而嗅探与监控，暴力攻击与恶意绑架等黑客攻防的进阶法宝。
全书均以实例形式讲解相关内容，直观、易学、易懂。
　本书内容丰富，讲解详细，内容可以作为初、中级读者的安全类入门读物，同时也可作为广大网络爱好者和初级黑客的案头必备速查手册。

书籍目录

第一章 信息收集与行踪隐藏　案例1　利用安检工具扫描本机漏洞　一、安装微软基准安全分析器　二、单台计算机扫描　三、多台计算机扫描　案例2　利用x-scan扫描本机漏洞　一、查知本机IP地址　二、添加IP地址　三、开始扫描　四、让X-scan充分发挥性能　案例3　追踪好友IP地址　一、网络定位　二、获取好友IP地址　三、追踪更多信息　案例4　批量扫描主机漏洞　一、扫描准备　二、选择扫描引擎　三、FTP漏洞扫描　案例5　扫描局域网内计算机信息　一、添加使用密码　二、设置弹出热键　三、监控浏览过的网站　四、键盘输入内容监控　五、程序执行情况监控　六、即时截图监控　案例6　扫描局域网安全信息　一、选择扫描范围　二、选择计算机　三、安全漏洞扫描　案例7　监控局域网计算机　一、工具介绍　二、搜索计算机　三、搜索共享资源　四、检查端口连接状态　案例8　防范黑客扫描追踪　一、ProtectX功能组件介绍　二、防护扫描器攻击的要点　案例9　用代理改变自己的IP地址　一、安装代理猎手　二、并发连接数目设置　三、验证数据设置　四、IP地址列表的获取　五、搜索代理服务器　六、代理数据的过滤　案例10　自由变换自己的IP地址　一、工具选择　二、操作过程　案例11　让IP地址在255个跳板之间变换　一、了解Sksockserver和Sockscap　二、安装与设置　三、连通性测试第二章 系统帐户与口令密码第三章 识别网络欺骗与突破限制第四章 控制与反控制第五章 漏洞攻击与恶意代码第六章 病毒与木马第七章 流氓软件与间谍程序第八章 数据的加密与解密第九章 网络嗅探与监控第十章 暴力攻击与恶意绑架

章节摘录

第十章 暴力攻击与恶意绑架案例1　网络炸弹“ 网络炸弹 ”称呼的由来是因为黑客在使用一种大量信息瞬间发送式的攻击后，被攻击主机立即会产生网络阻塞、蓝屏、死机等现象，使被攻击主机无法正常被使用，这与战争中的杀伤力较大的武器炸弹有异曲同工之妙，所以大家称这类攻击为网络炸弹。
一、炸弹的分类在网络中，最为常见中的炸弹有：IP炸弹、E—mail炸弹、Java炸弹以及硬盘炸弹等等。
（1）IP炸弹：这类炸弹是利用Windows的系统协议漏洞过行攻击的，黑客们只要查到你的IP地址便可用专用的 ”炸弹 ”进行轰炸，而你中弹后系统就会出现断线，蓝屏，死机或重新启动等。
（2）E-mail炸弹：它是黑客常用的攻击手段，就是以地址不详，容量庞大的邮件反复地发送到被攻击的信箱，造成信箱挤爆，不能收到信件，更严惩的会使邮件服务器瘫痪，不能成常工作。
（3）Java炸弹：在众多的聊天室中有些是可以直接发送HTML语句的，那么功击者就会通过发送一条带有恶意的代码，使具有这方面露洞的Windows用户电脑出现蓝屏、让浏览器打开无数个窗口，或显示巨大的图片。
最终使计算机系统耗尽资源而死机。
（4）硬盘炸弹：逻辑炸弹运行后会造成假0道损坏，造成硬盘不能启动。
是这么多炸弹中危害性最大的一个。
“ 洪水 ”：即信息垃圾炸弹，通过大量的垃圾请求可以导致目标服务器负载超负荷而崩溃，网络上流行的DOS攻击，简单地说也可以将其归入炸弹一类。

编辑推荐

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