

<<黑客大曝光>>

图书基本信息

书名：<<黑客大曝光>>

13位ISBN编号：9787302122593

10位ISBN编号：7302122598

出版时间：2006-4

出版时间：清华大学出版社

作者：(美) 麦克卢尔

页数：672

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>

## <<黑客大曝光>>

### 前言

回顾《黑客大曝光》第一版面世时的1999年，每个人都在“.com”世界里寻找着自己的立足之地并梦想着自己有朝一日能够成为一家举世瞩目的IPO。

那是一段美好的时光，各种各样的新技术如雨后春笋般地涌现出来。

但我们也都知道，那段先建立一家“.com”公司、然后在12个月内把它变成一家股票公开上市公司的好时光已经一去不复返了。

这不仅是因为资本市场本身发生了戏剧性的变化，信息安全方面的因素也在其中扮演了一个重要的角色。

如果你到现在还不明白信息安全不是一种奢侈而是一种必要的话，我敢说你在过去的5年里不是穴居在某个岩洞的深处、就是你到现在还沉浸在你的“.com”股票还值点儿钱的旧日美好时光..

## <<黑客大曝光>>

### 内容概要

《黑客大曝光》一书享誉全美，被信息安全界奉为圣经，号称信息安全第一书。作者独创“黑客大曝光方法学”，从攻防两方面系统阐述了最常见的黑客入侵手段及对应的防御策略。

作者秉承前4版的一贯写作风格，开篇即以“踩点”、“扫描”、“查点”三部曲，拉开黑客入侵的序幕。

之后，作者拨冗去繁，从系统、网络、软件三个方面对黑客攻击惯用手段进行剖析：“系统攻击”篇针对Windows、UNIX系统攻击给出精辟分析，并覆盖最新热门主题远程连接和VoIP攻击；“网络攻击”篇全面展示无线攻击技术和手段、防火墙攻击和拒绝服务攻击；“软件攻击”篇则引入全新概念——应用程序代码攻击，详细解释源代码泄露、Web应用程序攻击等最新黑客技术手段。

全书结合多个生动案例，环环相扣，引人入胜，读者如临其境。

本书面向各行各业、政府机关、大专院校关注信息安全的从业人员，是信息系统安防人士的宝典，也可作为信息安全相关专业的教材教辅用书。

## &lt;&lt;黑客大曝光&gt;&gt;

## 书籍目录

- 第1部分 收集情报第1章 踩点1.1 什么是踩点1.2 因特网踩点1.2.1 步骤1：确定踩点活动的范围1.2.2 步骤2：获得必要的授权1.2.3 步骤3：可以从公开渠道获得的信息1.2.4 步骤4：WHOIS和DNS查点1.2.5 步骤5：DNS查询1.2.6 步骤6：网络侦察1.3 小结第2章 扫描2.1 确定目标系统是否真实存在2.2 确定目标系统上都哪些服务正在运行或监听2.2.1 扫描类型2.2.2 确定运行的TCP和UDP服务2.2.3 基于Windows的端口扫描工具2.2.4 端口扫描工具汇总表2.3 探查操作系统2.3.1 主动式协议栈指纹分析技术2.3.2 被动式协议栈指纹分析技术2.4 小结第3章 查点3.1 旗标抓取基础3.2 对常用网络服务进行查点3.3 小结第2部分 系统攻击第4章4.1 概述4.2 取得合法身份前的攻击手段4.2.1 针对Windows独有的组网协议和服务的攻击手段4.2.2 Windows因特网服务实现4.3 取得合法身份后的攻击手段4.3.1 权限提升4.3.2 盗取信息4.3.3 远程控制和后门4.3.4 端口重定向4.3.5 通用防御措施：攻击者已经可以“合法地”登录到你的系统时该怎么办4.3.6 掩盖入侵痕迹4.4 Windows平台的安防功能4.4.1 及时打好补丁4.4.2 组策略4.4.3 IPsec4.4.4 tunas命令4.4.5 .NET Framework4.4.6 Windows Firewall4.4.7 Encrypting File System(EFS, 加密文件系统)4.4.8 Windows XP Service Pack 24.4.9 反思：Windows的安全负担4.5 小结第5章 攻击UNIX操作系统5.1 获取root权限5.1.1 简短回顾5.1.2 弱点映射5.2 远程访问与本地访问5.3 远程访问5.3.1 数据驱动攻击5.3.2 我想有个shell5.3.3 常见的远程攻击5.4 本地访问5.5 获取root特权之后5.6 小结第6章 远程连接和VOIP攻击6.1 准备拨号攻击6.2 轰炸拨打6.2.1 硬件6.2.2 法律问题6.2.3 外围成本6.2.4 软件6.3 蛮力脚本——更具针对性的攻击手段6.4 PBX攻击6.5 Voicemail攻击6.6 VPN攻击6.7 VoIP(Voice over IP)攻击6.8 小结第3部分 网络攻击第7章网络设备7.1 寻找潜在的攻击目标7.2 自治系统查询(AS查询)7.2.1 普通的traceroute命令输出7.2.2 带ASN信息的traceroute命令输出7.2.3 show ip bgp命令7.3 公共新闻组7.4 对网络服务进行探测7.5 网络的安防漏洞7.5.1 OSI模型的第I层7.5.2 OSI模型的第2层7.5.3 对基于开关阵列的网络进行嗅探7.5.4 OSI模型的第3层7.5.5 配置失误7.5.6 针对各种路由分配协议的攻击手段7.5.7 利用网络管理协议发动的攻击7.6 小结第8章 无线攻击8.1 无线踩点8.2 无线扫描和查点8.2.1 无线嗅探器8.2.2 无线监控工具8.3 查明目标无线网络已采取的防御措施8.3.1 SSID8.3.2 基于MAC地址的访问控制机制8.4 获得访问权限(攻击802.11协议)8.4.1 改变无线网卡的MAC地址8.4.2 WEP算法的安全弱点8.4.3 让WEP更安全8.5 以WEP为目标的黑客工具8.6 LEAP攻击8.7 拒绝服务攻击8.8 802.1X简介8.9 其他资源8.10 小结第9章 防火墙9.1 防火墙概述9.2 防火墙的识别9.3 穿透防火墙扫描9.4 数据包过滤9.5 应用代理的弱点9.6 小结第10章 拒绝服务攻击10.1 常见的DoS攻击技术10.1.1 早期的DoS攻击技术：安防漏洞10.1.2 现代DoS：能力消耗10.2 针对DoS攻击的防范措施10.2.1 要有切实可行的工作目标10.2.2 防御DoS攻击10.2.3 监测DoS攻击10.2.4 化解DoS攻击10.3 小结第4部分 软件攻击第11章 攻击应用代码11.1 常见的安防漏洞利用技术11.1.1 缓冲区溢出和产品设计缺陷11.1.2 输入检查攻击11.2 通用性防范措施11.2.1 人：改变企业文化11.2.2 流程：产品开发过程中的安全问题11.2.3 技术11.2.4 推荐阅读材料11.3 小结第12章 Web攻击12.1 攻击Web服务器12.1.1 样板文件12.1.2 源代码泄露12.1.3 资源解析攻击12.1.4 服务器功能扩展模块12.1.5 缓冲区溢出12.1.6 Web服务器漏洞扫描器12.1.7 Whisker 2.012.2 针对Web应用程序的攻击12.2.1 利用Google搜索引擎去查找有漏洞的Web应用程序12.2.2 网络爬虫：全站点下载12.2.3 对Web应用程序进行评估12.2.4 Web应用程序的常见安防漏洞12.3 小结第13章 攻击因特网用户13.1 因特网客户软件的常见安防漏洞13.1.1 因特网客户端软件攻击技术简史13.1.2 JavaScript和Active Scripting13.1.3 不能不防的cookie13.1.4 跨站点脚本(XSS)13.1.5 跨窗格/域漏洞13.1.6 SSL攻击13.1.7 定时炸弹：让恶意代码自动执行13.1.8 电子邮件攻击技术13.1.9 即时消息(IM)13.1.10 微软客户端软件的安防漏洞和相关防范措施13.1.11 微软客户端软件的通用安防措施13.1.12 为什么不使用非微软客户端软件13.1.13 非微软因特网客户端软件13.1.14 在线服务13

## <<黑客大曝光>>

. 2 社交工程攻击：网上欺诈和身份盗用13 . 3 烦人和害人的灰色软件： 间谍软件、广告软件与垃圾邮件13 . 3 . 1 灰色软件的常用种植技术13 . 3 . 2 灰色软件的拦截、监测和清除13 . 4 黑色软件13 . 4 . 1 黑色软件的种类和常用技术13 . 4 . 2 查杀黑色软件13 . 5 最终用户应该注意的物理安防问题13 . 6 小结第5部分附录附录A端口附录B最有威胁的14个安全漏洞

## <<黑客大曝光>>

### 编辑推荐

《黑客大曝光》(第5版)从系统、网络、软件三个方面对黑客攻击惯用手段进行剖析：“系统攻击”篇针对Windows、UNIX系统攻击给出精辟分析，并覆盖最新热门主题远程连接和VoIP攻击；“网络攻击”篇全面展示无线攻击技术和手段、防火墙攻击和拒绝服务攻击；“软件攻击”篇则引入全新概念——应用程序代码攻击，详细解释源代码泄露、Web应用程序攻击等最新黑客技术手段。

《黑客大曝光》(第5版)面向各行各业、政府机关、大专院校关注信息安全的从业人员，是信息系统安防人士的宝典，也可作为信息安全相关专业的教材教辅用书。

<<黑客大曝光>>

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>