# <<黑客攻防实战入门与提高>>

## 图书基本信息

书名：<<黑客攻防实战入门与提高>>

13位ISBN编号：9787030292711

10位ISBN编号：7030292715

出版时间：2011-1

出版时间：科学出版社

作者：叶刚，陈文萍　主编

页数：278

## 前言

近几年来，随着网络应用的飞速发展，各种网络攻击事件层出不穷，对网络管理员和网络安全工作者提出了更高的要求。
本书从实际应用出发，以任务的形式介绍网络中常见的攻击和防御手段，揭露出网络中广泛存在、却总被忽视的安全漏洞，并结合笔者长期积累的安全防护经验，指出相应的防范要点。
编写原则本书符合国家高技能人才培养目标和相关网络专业技术领域的岗位要求，对学生职业能力培养和素质的养成具有重要的支撑与促进作用，在编写过程中遵循以下原则。
（1）理论知识以“够用”为前提，培养创新型的应用人才本书是根据全国高职课程改革的要求而编写的，是信息安全专业课程建设改革的一个全新的思路。
本书以培养应用型人才为目标，确保理论知识够用，加大新知识、新技术的介绍，加强实验、实践力度，以培养创新型的应用人才。
（2）注重现代化教育技术在教学中的应用众多网络专家、教师和职业经理一致认为技术与团队合作精神是新技术人员必备的素质。
本书的编写也正是以此为目标，让学员在模拟环境中反复训练，知识与技能并重，职业素质与职业道德并行。
（3）重视应用能力的培养与训练本书以“任务驱动”的方式来设计实例与实验，使学员在了解理论的基础上，具备相应的操作技能。
我们在写作过程中本着“在娱乐中学习，在团队建设中锻炼”的理念，让学员在不同层次与不同阶段的学习中一步步地适应工作，适应企业的就业环境。
_内容特色·以项目为导向的学习模式：以项目为导向的学习模式避开了大量理论的学习，以实践为主导，非常适合自学和教学使用。
·实例丰富：涵盖扫描、嗅探、服务器入侵、脚本入侵、注入攻击等多种黑客攻防手法，读者可同时获取技术和理论两方面的知识。
·针对性强：围绕黑客攻防最新技术，让读者用最短的时间学到最有用的技术。
由于作者水平有限，书中难免存在不足之处，真诚地希望业界同仁和读者朋友们批评指正。

## 内容概要

本书着眼于网络安全工程师岗位，结合网络安全应用和发展现状，以应用为目标，以网络安全技术为主导，以搭建、配置与维护安全网络为主线，按照信息搜集与嗅探、木马的远程控制、经典脚木入侵、木马免杀技术、网络安全测试与安全故障诊断、常见网络安全设备的配置和管理为流程，循序渐进地讲解相应的网络安全实训任务。
本书的编写以“提高学生应用能力”为宗旨，按照企业对高校学生的实际需求来设计任务与实验，使学生能够在了解相关理论的基础上，具备相应的实际操作技能。
本书适合作为大中专院校、计算机培训班的实训指导教材，也可作为网络安全技术人员、网络安全爱好者的参考书，还可作为网络安全管理人员的参考手册。

## 作者简介

叶刚 软件学院黑客攻防实验室主任
　具有丰富的安全顾问咨询经验；透彻了解网络安全领域中的关键技术，对于黑客的攻击手段与黑客工具有较深入的研究，熟练掌握各主流防火墙、IDS、扫描器等安全产品的原理和应用技术。
擅长网络的攻击和防御，熟练使用黑客攻击的工具，熟悉木马、病毒的危害和防御，透彻掌握路由器的安全配置及网络的安全管理。
讲课生动、幽默、风趣，深得学生的喜爱。

# <<黑客攻防实战入门与提高>>

## 书籍目录

## 章节摘录

插图：（2）捆绑文件这种伪装手段是将木马捆绑到一个安装程序上，当安装程序运行时，木马在用户毫无察觉的情况下，偷偷地入驻系统。
至于被捆绑的文件，一般是可执行文件（即EXE、COM一类的文件）。
（3）出错显示当服务端用户打开木马程序时，为了迷惑用户，木马程序会弹出一个错误提示框。
错误内容大多会定制成诸如“文件已破坏，无法打开！
”之类的信息，如果服务端用户信以为真，木马会悄悄入驻系统。
（4）定制端口很多老式木马的端口都是固定的，这给判断是否感染了木马带来了方便，只要查一下特定的端口就知道感染了什么木马，所以现在很多新式木马都加入了定制端口的功能，控制端用户可以在1024～65535之间任选一个端口作为木马端口（一般不选1024以下的端口），这样就给判断木马的类型带来了麻烦。
（5）自我销毁木马的自我销毁功能是指安装完木马后，原木马文件将自动销毁。
这样服务端用户就很难找到木马的来源，在没有查杀木马工具的帮助下很难删除木马。
（6）木马更名现在有很多木马都允许控制端用户自由定制安装后的木马文件名，这样很难根据文件名来判断所感染的木马类型。

## 编辑推荐

《黑客攻防实战入门与提高》编辑推荐：超值多媒体教学光盘，时长超过300分钟的20个实训任务的多媒体语音教学录像，实验环境的搭建说明和所用的软件工具，实验中入侵与防御思路的参考文档，视频由北大方正软件学院名师亲自录制，讲解生动、细致，任务驱动教学，以项目为导向的学习模式，避开大量理论的学习，以实践为主导，非常适合自学和教学使用，25个攻防实训，涵盖扫描、嗅探、服务器入侵、脚本入侵、注入攻击等多种黑客攻防手法，可同时获取技术和理论两方面的知识，视频与图书互补，采用最为通俗易懂的图文解说.并配有多媒体视频讲解.让读者可以轻松上手。
〈br〉上兴木马入侵，简单文件型DOS病毒制作，基于溢出的入侵，信息收集及嗅探，终极免杀，针对服务器的网络僵尸DDOS攻击，上兴木马手工查杀，缓冲区溢出工具编写，远程登录入侵，用WinRAR打造捆绑利器，木马加壳技术，肉鸡跳板制作，利用Google得到敏感信息，经典脚本入侵，Cookies欺骗，Access+ASP网站入侵（工具篇），Access+ASP网站入侵（手工篇），SQL注射入侵（工具篇），SQL注射入侵（手工篇），基于IIS服务器的入侵，基础网络硬件设备防火墙的安全部署，锐捷交换机的部署，漏洞扫描设备的部署，联想网御SSL-VPN设备的部署。

## 版权说明