

<<网络安全与黑客攻防宝典>>

图书基本信息

书名：<<网络安全与黑客攻防宝典>>

13位ISBN编号：9787121100819

10位ISBN编号：7121100819

出版时间：2010-3

出版时间：电子工业

作者：李俊民//郭丽艳

页数：782

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>

## <<网络安全与黑客攻防宝典>>

### 前言

在当今的网络时代，黑客、病毒让人们谈虎色变，那么到底什么是黑客，他们如何工作，病毒到底是什么，病毒的出现又会对人们的生活造成什么样的影响？

本书将给出这些问题的答案。

计算机网络安全是现今网络的主旋律，关于网络安全的话题在媒体上随处可见。

随着黑客工具的日益“傻瓜”化，黑客已经被剥离了神秘的外衣。

但是计算机安全、网络安全知识的普及仍然是一个严峻的问题，为了解决这个问题，本书以普及安全知识为己任，帮助用户深入了解网络安全的方方面面，如深入分析黑客入侵计算机的全部过程，模仿黑客入侵计算机并提升远程计算机的权限进而达到控制的目的，剖析病毒和木马的来龙去脉，预测入侵检测的技术发展及趋势，此外，神秘的计算机取证技术和热点的无线网络安全问题都将在本书中呈现。

本书依照读者的学习规律，首先从了解网络安全的基础知识讲起，介绍基本概念和基本观点，在读者掌握了这些基本知识的基础上，再介绍历史上著名的黑客人物及历史事件，以立体的角度、有趣的故事情节为依托，严格遵循由浅入深、循序渐进的原则。

本书以计算机网络安全知识的层次结构为主线将各种工具、命令和理论知识交织编排在一起，使读者可以深入学习任何一章的内容。

本书在内容编排和目录组织上都十分讲究，章节之间既可相互呼应也可各自成章。

比如在第1章熟悉了网络的基础知识以后，立刻引入一些著名的黑客人物的经历，以一个实例告诉读者这些知识的重要性，让读者在茶余饭后的闲谈中即可快速入门。

同时，每章之间又相互独立，如果读者希望直接了解病毒的相关知识，可快速查阅第9章和第10章。

第9章对木马进行了深入的分析，第10章按照病毒的机制对病毒进行了深入的剖析。

## <<网络安全与黑客攻防宝典>>

### 内容概要

本书由浅入深、循序渐进地介绍了计算机网络安全知识体系。全书共分21章，内容涵盖了网络基础知识、黑客初步、操作系统漏洞与应用软件漏洞的攻防、BBS与Blog的漏洞分析、信息收集、扫描目标、渗透测试、网络设备的攻击与防范、木马分析、病毒分析、网络脚本攻防、SQL注入攻防、防火墙技术、入侵检测技术、计算机取证、无线网络安全等内容。本书最大的特色在于知识全面、实例丰富，每一节的例子都是经过精挑细选，具有很强的针对性，读者可以通过亲手实践而掌握安全防护的基本要领和技巧。

本书适合初、中级用户学习网络安全知识时使用，同时也可作为高级安全工程师的参考资料。

# <<网络安全与黑客攻防宝典>>

## 书籍目录

第1部分 黑客基础篇 第1章 网络基础知识 第2章 黑客基础第2部分 漏洞、木马与病毒篇 第3章 漏洞基础知识 第4章 BBS与Blog的入侵实例 第5章 信息收集 第6章 扫描目标 第7章 渗透测试 第8章 网络设备的攻击 第9章 木马分析 第10章 病毒分析第3部分 网络攻防篇 第11章 网络安全防范 第12章 网站脚本的攻防 第13章 防火墙技术 第14章 入侵检测技术第4部分 常见攻防技术篇 第15章 网络封锁与代理突破 第16章 操作系统与文件加密技术 第17章 SQL注入攻防技术 第18章 欺骗攻击技术与安全防范 第19章 后门技术与痕迹清理 第20章 计算机取证 第21章 无线网络安全附录A Windows的“运行”命令附录B 常见程序进程详解附录C 网络管理命令大全附录D 病毒特征码和木马进程附录E 术语表

章节摘录

插图：当用户主机与远程主机开始一个FTP会话前，FTP的客户端首先在21号端口上发起一个用于控制的与服务器的TCP连接。

FTP客户端通过该控制连接发送用户标识和口令，也通过其发送改变远程目录的命令。

当FTP的服务器端从该连接上收到一个文件传输命令后，就建立一个到客户端的数据连接。

FTP在该数据连接上准确地传送一个文件并完成后关闭该连接。

如果在同一个会话期间，用户还需要传输另一个文件，FTP则打开另一个数据连接。

因而对FTP传输而言，控制连接贯穿了整个用户会话期间，但是针对会话中的每一次文件传输都需要建立一个新的数据连接。

FTP传输的是需要保留用户的状态信息。

特别是服务器必须把指定的用户账户和控制连接联系起来，必须跟踪用户在远程目录上的当前位置。

可以对每个活动着的用户会话状态进行跟踪，还可以对FTP会话总数进行限制。

网络分析王具是学习和诊断TCP / IP的有力助手。

现行的网络工具多种多样，但是万变不离其宗，读者只需要掌握其中的三种即可。

这些王具是：令协议分析仪Ettlereal入侵检测工具Snort Windows自带的工具Netstat如果设备出现了故障，需要判断问题到底是设备本身引起的还是由于网络原因时，协议分析仪就是网络工程师的好帮手。

虽然协议分析仪不够直观，不能用图表来显示出网络的运行状况，而且如果对协议一无所知，协议分析仪便是一块无用的“废铁”，但是协议分析仪仍然是避免)中突、解决疑难杂症的重要工具，也是分析网络攻击的重要王具。

Ethereal是免费的开源软件，该软件现在最新的版本是0.10，如图1.13所示。

## <<网络安全与黑客攻防宝典>>

### 编辑推荐

《网络安全与黑客攻防宝典(第2版)》包括根据实战经验精心改编的实例。

充分考虑读者的理解水平,使其能够根据自身的知识水平有针对性地学习,思路变得更加开拓。

《网络安全与黑客攻防宝典(第2版)》知识面开阔,有基础性知识,也有深入的理论探讨,满足不同程度读者的阅读需求。

《网络安全与黑客攻防宝典(第2版)》使用大量的新知识,如Metasploit、Nessus,UTM、EnCase、网络钓鱼,流氓软件和NetStumbler等,使《网络安全与黑客攻防宝典(第2版)》与同类书中陈旧的技术内容形成鲜明的对比,阅读价值得到极大提升。

《网络安全与黑客攻防宝典(第2版)》依照读者的学习规律,首先从网络安全的基础知识讲起,介绍其基本概念和基本观点,然后在读者掌握了这些基本知识的基础上,进一步介绍历史上著名的黑客人物及历史事件,并以计算机网络安全知识的层次结构为主线将各种工具、命令和理论知识交织编排在一起,使读者可以轻松进行深入的学习。

<<网络安全与黑客攻防宝典>>

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>