

《暗战亮剑》

图书基本信息

书名：《暗战亮剑》

13位ISBN编号：9787115230461

10位ISBN编号：7115230463

出版时间：2010-7

出版社：人民邮电

作者：朱锡华//刘月铎//侯伟

页数：441

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu111.com

《暗战亮剑》

前言

本书以讲解渗透攻防技术为主线，用实例剖析了黑客的渗透手法，揭示了黑客的渗透内幕，由浅入深、循序渐进地介绍了网络渗透攻防的核心技术。渗透攻防是一项综合性很强的技术，以往的有关安全的书籍讲解这方面的知识显得理论多于实战，且观念陈旧，无法跟上高速发展的网络技术。很多内容都停留在几年前的黑客攻防水平，使得新型安全技术无法在书籍中再现，这样也阻碍了新技术的普及，而黑客一旦掌握了最新的攻击技术，就可以肆意破坏整个网络，正是由于这些原因，笔者决定撰写一本技术新颖、实战性和扩展性强的网络渗透攻防书籍。书中讲解了最流行的渗透攻防技术，每章都精选经典渗透攻防案例，从案例出发再现真实攻防场景，将真实攻防环境“搬”到书中。在本书的编写过程中，随时关注最新的安全技术，将国内外最新的攻防技术吸收到本书中，这样读者不仅可以掌握国内黑客的攻防秘籍，更重要的是可以了解到国外高端安全攻防的前沿技术。本书包括黑客攻防入门、高级缓冲区溢出技术、各类高级web渗透攻防技术、主流数据库攻防技术、最新服务器提权渗透攻防技术、专业网络渗透工具剖析、内网高级渗透攻防等。在了解了黑客渗透技术后，本书还提供了专业性、针对性极强的安全防御方案，让读者学以致用地管理好自己的网站、计算机系统、服务器等免受黑客渗透攻击，打造更加坚固的安全防御遁甲。

《暗战亮剑》

内容概要

《暗战亮剑:黑客渗透与防御全程实录》是一本全面剖析黑客渗透攻防技术的书籍，剖析了黑客对网络系统进行渗透的技术，帮助读者了解计算机系统的脆弱环节及安全缺陷，教给读者有针对性地采取安全措施，堵住黑客入侵的通道，加固系统安全。

《暗战亮剑:黑客渗透与防御全程实录》包括黑客攻防入门、高级缓冲区溢出技术、高级Web渗透攻防技术、主流数据库攻防技术、最新服务器提权渗透攻防技术、专业网络渗透工具剖析、内网高级渗透攻防等。在了解了黑客渗透技术后，《暗战亮剑:黑客渗透与防御全程实录》还提供了专业性、针对性极强的安全防御方案，让读者知己知彼地管理自己的服务器及计算机系统免受黑客渗透，打造更加坚固的安全防御盾牌。《暗战亮剑:黑客渗透与防御全程实录》可作为网络安全评估人员、网络安全开发人员、黑客攻防研究人员、企业和电子商务网络安全维护人员，以及网络安全机构认证培训等机构的辅助学习教材，同时也可作为计算机院校师生的网络安全教学参考书。

《暗战亮剑》

作者简介

侯伟，笔名“猪猪”，2004年创办 [岁月联盟] 网络安全团队与网站。担任多家企事业单位安全顾问，多次应邀参加国内安全峰会，参与国家电网公司多项安全检查工作。现参与西安交通大学多个安全合作项目。朱锡华，笔名“晓华”，精通多种网络安全技术，尤其热衷于研究网络渗透与安全防御技术。拥有丰富的安全实战攻防经验以及安全项目实施经验，曾在国内著名黑客杂志《黑客手册》发表过若干网络攻防类技术文章，现为国内著名黑客组织“岁月联盟”核心成员，参与团队内部技术研究与管理工。酷爱摩托车越野极限运动，曾多次穿越川西高原。

书籍目录

第1章 渗透攻防实践技术	1.1 命令行下的黑色艺术	1.2 扫描器下的黑色艺术	1.2.1	
扫描器基本概述	1.2.2 国产黑客扫描利器——X-Scan	1.2.3 著名黑客工具——SuperScan		
	1.2.4 SuperScan扫描使用技巧	1.2.5 SuperScan实战利用	1.2.6 超速S扫描器使用技巧	
巧	1.2.7 暴力破解利器——HSCAN	1.3 黑客远程控制技术剖析	1.3.1 远程控制软件结构	
	1.3.2 高级远程控制软件——Pcshare	1.3.3 Pcshare客户端设置	1.3.4 Pcshare上线方式	
—VNC	1.3.5 Pcshare服务端配置	1.3.6 Pcshare更新IP	1.3.7 远程控制软件—	
上传	1.3.8 黑客的忠实守护者——随意门剖析	1.4 黑软上传技术剖析	1.4.1 TFTP	
攻击手法揭秘	1.4.2 FTP上传	1.4.3 VBS脚本上传	1.4.4 超短VBS上传	1.5 黑客常见攻击
服务	1.5.1 端口扫描	1.5.2 口令破解	1.5.3 缓冲区溢出	1.5.4 拒绝
攻击	1.5.5 网络嗅探	1.5.6 SQL注射攻击	1.5.7 会话劫持	1.5.8 网页挂马攻
实战剖析	1.5.9 网络钓鱼	1.6 社会工程学欺骗剖析	1.7 域名劫持	1.8 常见系统端口渗透
	1.8.1 网络端口概述	1.8.2 端口渗透剖析	1.8.3 端口渗透剖析	
	1.8.4 端口渗透剖析	1.8.5 端口渗透剖析	1.8.6 端口渗透剖析	1.8.7 /445端口渗
透剖析	1.8.8 端口渗透剖析	1.8.9 1端口渗透剖析	1.8.10 6端口渗透剖析	
	1.8.11 端口渗透剖析	1.8.12 端口渗透剖析	1.8.13 1端口渗透剖析	1.8.14 端口
透剖析	1.8.15 80端口渗透剖析	1.9 常见加密算法破解技术剖析	1.9.1 MD5密码破	
解剖析	1.9.2 CFS编码加密破解	1.9.3 电子邮件客户端软件密码破解剖析	1.9.4	
RDP远程桌面密码破解剖析	1.9.5 FlashFXP密码破解剖析	1.9.6 本地破解VPN客户端登		
录密码剖析	1.9.7 常见JS加、解密	1.9.8 雷池新闻系统加、解密	1.9.9 RAR压缩软	
件密码破解剖析	1.9.10 常见文字类文档加密破解	1.9.11 其他加密算法的破解	
第2章 缓冲区溢出和漏洞挖掘攻防实战	第3章 漏洞攻防实战	第4章 数据库渗透安全攻防	第5	
章 抢占权限的制高点	第6章 精通常见网络安全工具及技术	第7章 内网渗透防御攻略		

章节摘录

黑客在实施渗透的时候，很少会用到图形化操作界面，一般是用系统命令实现的。为了真实地剖析黑客的渗透行为，我们所讲的整个操作过程都将在命令行下完成，以便剖析出黑客渗透并控制远程计算机的踪迹。学习系统命令不仅可以了解黑客用来实施渗透攻击的秘密，而且对维护操作系统的安全也有特别的意义。通常黑客在攻击过程中，一般会进行创建用户、上传黑客工具、开启远程桌面服务等操作，这些操作在图形化界面下很难完成，利用系统命令实施对系统的控制是最佳途径。了解系统命令可以更深入地了解系统的底层，是安全高手必备知识。本节主要讲解在渗透过程中比较常用的系统命令。

1. 打开命令提示符打开DOS命令提示符有很多种方法，比较常用的就是依次单击“开始”-“运行”项，在弹出的窗口中输入cmd命令即可，如图1.1所示。另外，也可以建立一个批处理文件用以打开DOS命令提示符，值得注意的是，批处理文件所在的路径是打开cmd后所处的路径，如图1-2所示。通过这种方式省略了目录切换的麻烦，也非常实用。

《暗战亮剑》

媒体关注与评论

面对困难永远不要放弃，你的下一次单击回车键也许就有奇迹发生，感谢作者让我们能有机会亲自见证这些奇迹。——goodwell（龚巍）

关于书中的内容，只有仔细看过的人才能真正体会到她的价值，希望每个人拥有这本书的朋友，只要你想在黑客安全技术方面有所突破，一定要认真细致地学一学、练一练，真正把里面的知识吃透，练实，再深入学习就不是什么难事了。——逆风飞扬（周剑）

网络安全管理一直是整个网络管理的难点，特别是在当前开放的网络环境中，本书集中介绍了各种操作系统，应用软件和设备安全弱点及解决方案，使你做到真正有的放矢。——网络实战专家 王达（茶乡浪子）

黑客技术，羚羊挂角，照书索骥，有迹可求，故其妙处，透澈玲珑。——著名黑客LCX（李春晓）

《暗战亮剑》

编辑推荐

27个核心渗透攻防技术案例，100个疑难解答，寻踪攻击原理，解析渗透安全核心问题，120个实战技巧，提升读者的实战能力，400个安全实例，涵盖操作系统，网站应用程序，主流数据库、内部网络的渗透安全攻防技术。

精彩短评

1、国产老书

《暗战亮剑》

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:www.tushu111.com