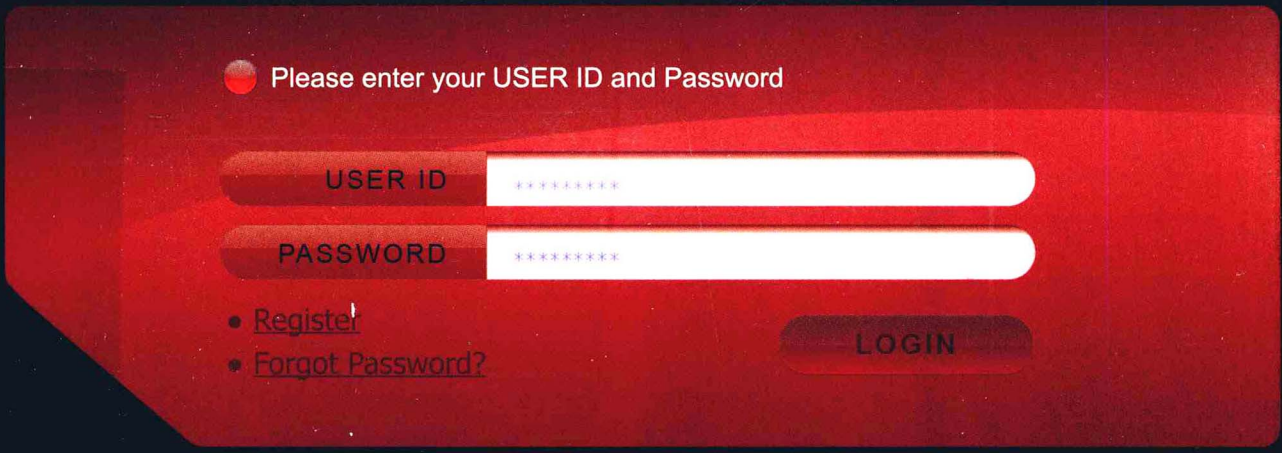
The Practice Detailed Annotation of Hacking and Defence with Command Line

黑客命令行攻防

实战详解

至诚文化 编著



中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

黑客命令行攻防

实战详解

至诚文化　编著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

本书秉承通过黑客常用命令行保障网络安全的原则，以黑客常用命令为主线，详细介绍了远程连接、系统远程管理、防火墙管理等相关操作命令及其应用环境。在此基础上，进一步介绍批处理及 Windows PowerShell 脚本等关键技术，让读者可以根据网络安全需求，高效利用命令完成网络扫描、远程主机探测、漏洞侦测、弱口令探测、证书导出等任务。在应用层面，本书使用大篇幅实例介绍了本地入侵、网络扫描、跳板利用、痕迹消除、反追踪、局域网嗅探、网页挂马、数据库注入、无线网络破解、加密文件破解等内容，旨在帮助读者认识黑客的攻防技术，进而有效地防止黑客入侵。

本书适合有一定基础的网络安全从业人员和对命令行感兴趣的广大读者。

图书在版编目（CIP）数据

黑客命令行攻防实战详解/至诚文化编著. -- 北京
：中国铁道出版社，2011.9
ISBN 978-7-113-13049-7

Ⅰ. ①黑… Ⅱ. ①至… Ⅲ. ①计算机网络－安全技术
Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2011）第 104692 号

书　　名：黑客命令行攻防实战详解
作　　者：至诚文化　编著

策划编辑：荆　波　　**读者热线电话：**010-63560056
责任编辑：荆　波　　**编辑助理：**张　丹
封面设计：付　巍　　**封面制作：**郑少云
责任印制：李　佳

出版发行：中国铁道出版社（北京市宣武区右安门西街 8 号　　邮政编码：100054）
印　　刷：化学工业出版社印刷厂
版　　次：2011 年 9 月第 1 版　　2011 年 9 月第 1 次印刷
开　　本：787mm×1092mm　1/16　**印张：**20.25　**字数：**470 千
书　　号：ISBN 978-7-113-13049-7
定　　价：45.00 元（附赠光盘）

前　言　Foreword

谈起黑客命令，很多人都会认为那是网络高手的杀手锏，利用它们可以监视网络中的一举一动，简单的几个字母可拒敌于千里之外，因为黑客命令行是非常有用、针对性极强的网络安全维护工具，可以更有效地帮助读者保护好自己的数据。

首先，在本书的开篇章节，我们以大篇幅深入介绍黑客文化，让读者了解黑客的起源，白帽黑客、黑帽黑客群族，世界十大著名黑客等。接着从兴趣、心态、知识、技能四大方面，以及程序语言、电脑硬件、操作系统、密码学、社会工程学、网络通信六大基础起步，让所有读者都能深入理解黑客技术并利用它保护电脑正常运行和数据安全。

随后本书以系统管理、远程连接、远程管理、防火墙管理等黑客常用的命令为起点，让入门黑客初步掌握命令行的精髓。在此基础之上，我们准备了丰盛的批处理脚本和Windows PowerShell脚本大餐，让掌握命令行的读者初探黑客的程序世界，了解黑客如何通过自制程序完成网络扫描、远程主机探测、漏洞侦测、弱口令探测、证书导出等任务。然后就是网站挂马、数据库注入、WiFi 无线入侵等热点话题了。在这些独立的话题中，我们吸收了国外教材的优点，着重于原理讲解，给予源程序级别的分析，让读者可以真实深入地了解黑客是如何看待问题、思考问题、解决问题的，最后再辅以点题的实作提升动手能力，旨在帮助读者（主要是网络管理员）知己知彼地了解黑客的思维方式和入侵手段，有的放矢地制定完善的网络安全维护方案。

本书的详细架构如下：

第1章深入讲解黑客文化的起源，包括黑客的两大族群，互联网历史上著名的黑客，以及要成为黑客所必须具备的各种基础，此外还简单介绍黑客的常用工具。

第2章开始将会详细讲解黑客常用的命令，首先是Windows的系统管理命令，例如文件管理命令、磁盘管理命令、进程管理命令、服务管理命令、账户及组管理命令。

第3章主要讲解远程连接及管理命令，包括远程管理及文件传输（如Telnet、FTP、IPC$）、连接测试命令（如跃点追踪命令tracer、网络连接命令Netstat等）、TCP/IP配置命令、多功能网络命令Net、网络组件命令行及脚本处理Netsh。

第4章主要讲解Windows的防火墙管理命令，并且通过大量实例进行演示，例如查询当前防火墙配置和状态、修改防火墙明细规则。

第5章讲解批处理的运用，首先会介绍批处理编程的基础知识，例如回显控制、输入控制、批处理的各种变量及流程控制语句等。掌握这些基础后，接下来通过大量实例演示批处理在黑客攻防中的应用，例如使用批处理删除系统日志、制作后门程序、结束

任务管理器进程等，最后还会讲解系统管理员如何防范黑客使用批处理入侵及攻击。

第 6 章讲解 Windows 系统管理的重头戏：PowerShell，首先对 Windows PowerShell 的来龙去脉进行介绍，然后讲解 PowerShell 基础的语法和命令，以及 Cmdlet，最后本章会精选一些实用的 PowerShell 脚本，进行详细的分析讲解，帮助读者将前面学习的基础知识融会贯通。

第 7 章讲解本地入侵和防护的相关知识，包括使用 MSDaRT 光盘破解操作系统登录密码、使用 Windows PE 入侵本地电脑等，此外还会讲解如何定制自己的本地入侵工具光盘。

第 8 章讲解端口扫描与端口保护的相关知识，包括寻找网络中活动的主机、扫描主机开放端口、判断目标主机操作系统、扫描系统漏洞等。本章对著名的系统漏洞扫描分析软件 Nessus 进行了详细的讲解。

第 9 章讲解痕迹清除，首先讲解通过代理服务器及 Tor 隐身，然后讲解系统日志清除、文件粉碎等内容，最后还讲解了如何检验清除的效果。

第 10 章讲解局域网入侵的常用手段：网络嗅探，首先分析网络嗅探的原理，然后以实例方式，演示 CAIN&Abel 及 Sniff Pro 等专业嗅探工具的配置及使用，最后本章会讲解如何侦测及防御网络嗅探。

第 11 章介绍了现在流传最广泛、危害极大的网页挂马。首先解析网页挂马的过程，然后从木马制作开始讲解，详细讲解木马加密免杀、网页木马生成及经典的挂马代码，最后本章以网页挂马的模拟入侵为例，演示黑客如何通过一个 0Day 漏洞，入侵网站并在网页上挂马的完整过程。最后本章还介绍了防御网页挂马的方法，以及如何清除网站上的木马。

第 12 章讲解 SQL 数据库注入及防御的相关知识，包括 SQL 注入攻击的原理及危害性，然后通过大量的实例，演示黑客使用 SQL 注入攻击的过程，包括猜解数据表及字段名称、怎样构造注入语句等。在本章的最后，讲解如何防御 SQL 注入攻击。

第 13 章讲解 WIFI 无线网络入侵及防御，首先介绍 WIFI 无线网络的架构及入侵的原理，并且着重介绍了无线入侵所需的硬件设备，然后以实例方式演示如何破解加密的无线网络，最后讲解防御无线网络入侵的相关知识。

第 14 章主要讲解加密和解密的相关知识，并且演示各种常见的解密方法，例如压缩文件解密、Office 文档解密、PDF 文档解密等。此外还着重讲解了 Windows EFS 加密与破解。在本章的最后，介绍了如何应对破解的挑战，包括使用 Bitlocker 及 AES 加密。

本书附赠光盘中提供了多媒体视频，对应书中相应章节把具体操作转化为直观影像，从命令的应用到端口的保护一一讲述，帮助读者更加深入和轻松地掌握黑客命令。

编　者

2011 年 5 月

郑重声明

本书的目的绝不是为那些怀有不良动机的人提供支持，也不承担因为技术被滥用产生的连带责任；本书的目的在于最大限度地唤起大家的网络安全意识；读者切勿用本书中所讲技术进行违法行为活动，否则后果自负，切记！

读者意见反馈表

亲爱的读者：

感谢您对中国铁道出版社的支持，您的建议是我们不断改进工作的信息来源，您的需求是我们不断开拓创新的基础。为了更好地服务读者，出版更多的精品图书，希望您能在百忙之中抽出时间填写这份意见反馈表发给我们。随书纸制表格请在填好后剪下寄到：北京市宣武区右安门西街8号中国铁道出版社综合编辑部 荆波 收（邮编：100054）。或者采用传真（010-63549458）方式发送。此外，读者也可以直接通过电子邮件把意见反馈给我们，E-mail地址是：jb@163.jb18803242@yahoo.com.cn。我们将选出意见中肯的热心读者，赠送本社的其他图书作为奖励。同时，我们将充分考虑您的意见和建议，并尽可能地给您满意的答复。谢谢！

- -

所购书名：_____

个人资料：

姓名：_____性别：_____年龄：_____文化程度：_____

职业：_____电话：_____E-mail：_____

通信地址：_____邮编：_____

- -

您是如何得知本书的：

□书店宣传 □网络宣传 □展会促销 □出版社图书目录 □老师指定 □杂志、报纸等的介绍 □别人推荐

□其他（请指明）_____

您从何处得到本书的：

□书店 □邮购 □商场、超市等卖场 □图书销售的网站 □培训学校 □其他

影响您购买本书的因素（可多选）：

□内容实用 □价格合理 □装帧设计精美 □带多媒体教学光盘 □优惠促销 □书评广告 □出版社知名度

□作者名气 □工作、生活和学习的需要 □其他

您对本书封面设计的满意程度：

□很满意 □比较满意 □一般 □不满意 □改进建议

您对本书的总体满意程度：

从文字的角度 □很满意 □比较满意 □一般 □不满意

从技术的角度 □很满意 □比较满意 □一般 □不满意

您希望书中图的比例是多少：

□少量的图片辅以大量的文字 □图文比例相当 □大量的图片辅以少量的文字

您希望本书的定价是多少：

本书最令您满意的是：

1.

2.

您在使用本书时遇到哪些困难：

1.

2.

您希望本书在哪些方面进行改进：

1.

2.

您需要购买哪些方面的图书？对我社现有图书有什么好的建议？

您更喜欢阅读哪些类型和层次的计算机书籍（可多选）？

□入门类 □精通类 □综合类 □问答类 □图解类 □查询手册类 □实例教程类

您在学习计算机的过程中有什么困难？

您的其他要求：

目 录 Contents

第 1 章 黑客！黑客！

第 2 章 系统管理命令

第 3 章 远程连接及管理命令

第 1 章　黑客！黑客！

在信息和信息技术发达的今天，你可能无数次看到或听到有关黑客的新闻，甚至 DISCOVERY（探索发现）频道也凑热闹拍了一个有关黑客的专辑 *The History Of Hacking Documentary*。然而，这些可能依然无法满足你对黑客的好奇心。所以，在本章中，我们会对黑客进行一个客观的描述，告诉读者黑客的起源、趣闻；并从技术方面对黑客有一个全面的阐述，以便在网络安全中做到知己知彼。

1.1　认 识 黑 客

在目前主流媒体的报道中，黑客通常与犯罪、违法事件密切相关。事实上，出现在报道中的黑客仅仅是庞大黑客世界中的冰山一角。在这一节中，我们将追本溯源，深入了解黑客文化，并通过十大黑客的人生足迹还原真实的黑客本貌。

1.1.1　黑客追本溯源

要了解什么是黑客，我们首先让时光倒流半个多世纪，回到电脑发明没多久时的美国。二十世纪五六十年代的美国，电脑处于大型机时代，造价昂贵且体积巨大，一般只开放给航空、武器设计等高科技领域的科研人员使用。为了让更多人接触、了解和使用电脑，位于马萨诸塞州的麻省理工学院（Massachusetts Institute of Technology，MIT）率先推出了分时系统，学生通过终端访问分时系统，开始使用大型电脑。随后出现了大量对计算机和网络知识有着狂热兴趣的学生，他们挑战当时的权威理论，勇于革新技术并主张信息共享。例如，当时大型主机终端严格区分优先等级，如果教授登录主机，学生终端便立即断开，键盘也处于锁定状态，要求平等使用大型主机的学生们破解口令，修改优先权记录，这一行为受到大量学生的追捧，他们还创造了一个新名词 Hacker（黑客），以褒扬手法巧妙、技术高明的电脑高手。

二十世纪六十年代早期，小型机开始进入麻省理工学院，该学院的学生史蒂夫·斯拉格·拉塞尔（Steve Russell）提出了在电脑中进行游戏的设想，并与格拉兹（S.Graetz）和考托克（A.Kotok）两名同学一起编写程序。1961 年世界首款电脑游戏“空间大战”（Spacewar）在 MIT 人工智能实验室闪耀登场，两艘飞船装备 31 枚导弹，玩家可操纵飞船航向并相互投弹攻击，第一代黑客在“空间大战”游戏中体验到电脑应用的“魔力”，纷纷展现自己的才智，编写并共享具有实用价值的电脑程序，例如制作象棋推算程序展现电脑向智能化发展的可能性，制作留言系统以使用电脑相互通信，设计地铁换乘程序帮助人们高效使用地铁出行，设计画板软件开创互动式电脑制图、辅助设计（CAD）等崭新领域。其实，最早期的黑客，不但不是罪犯，而且是与信息不对称的旧工业时代抗争的先锋。没有他们，电脑及互联网就不会发展得如此迅猛，或者时至今天可能还像许多科研设备一样被局限于武器设计、科研计算等小范围、小圈子使用；电子邮件、共享信息的万维网、BBS 等公众网络服务的推出与普及，更可能无限期延后，图 1-1 所示为空间大战设备及游戏画面。

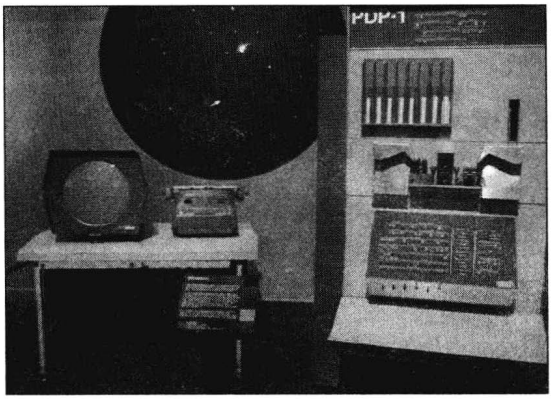


图 1-1　空间大战设备及游戏画面

二十世纪六十年代中期以后，黑客这一新生名词随着早期的计算机革命者而名扬四海，成为反权威却奉公守法的计算机英雄的荣耀之称。黑客文化也伴随着 MIT 毕业生走进商业圈，自由、共享的黑客精神也广泛传播至美国各地，创造了一个又一个传奇故事。例如邓尼斯·里奇（D.Ritchie）和肯·汤姆森（K. Thompson）为贝尔实验室开发文书处理软件，磨破了嘴皮才获得购买小型电脑的 10 万美元经费。他们却用购入的小型电脑开发了 UNIX 操作系统，并说服 AT&T 公司将此成果以低廉的价格甚至免费供给学术机构及教学使用。查德·斯德尔曼（R.Stallman）为了让自由使用软件得到法律支持，在 1984 年发起成立自由软件基金会，架构出 GNU 通用公共许可证（GNU General Public License，GPL）这个法律框架，为自由软件的发展铺平了道路。

提 示

许多用户将自由与免费混为一谈，事实上，GNU 包含三个许可证条款，它并不排斥对自由软件进行商业性质的包装和发行，但它要求开放源代码，以方便人们对软件进行修改和完善，并在此基础上开发出更优秀的软件。

进入二十世纪七十年代，早期的黑客精神虽然不乏支持者，但是黑客的行为随着技术的普及而变得多元化，一些黑客背离了原来的精神，利用技术大量盗打电话，这一行为令黑客的荣耀光环在公众眼中开始褪色。进入二十世纪八十年代，更多的入侵行为彻底破坏了早期的黑客形象。如 1988 年美国康奈尔大学 23 岁学生罗伯特·莫里斯（Robert Morris）向互联网络释放了“蠕虫病毒”，导致美国 1/10 的电脑中毒，许多科研机构与政府网站因此停止工作，造成无法统计的经济损失。这一系列不光彩的黑客事件，令黑客最终沦为电子窃贼、破坏者的代名词。

1.1.2　黑客两大群族

尽管黑客形象一落千丈，但这并不妨碍黑客文化的发展。目前，黑客已经分化成两大阵营：白帽黑客（white hat hacker）与黑帽黑客（black hat hacker）。

白帽黑客是指合法使用黑客技术的黑客，他们通常是学术研究人员或电脑安全顾问，在合法的情况下攻击指定的系统，以便进行安全测试、寻找可能存在的安全漏洞，并协助用户解决各种安全问题。例如 IOActive 公司渗透测试总监 Dan Kaminsky 就是一位著名的白帽黑客，他在 2008 年发现了可能引发互联网大面积崩溃的 DNS 协议漏洞，协助 DNS 服务器管理员修复这个漏洞并及时发布