网络安全专家
Network security experts

暗战强人

黑客攻防
实战高级演练

武新华　陈艳艳　等编著
飞思科技产品研发中心　监制

重点提示　任务过程　范例图示
专家讲解　打破常规　层层递进
一书在手　边用边学　即查即用

DVD 强人 视频大讲堂

共6小时40课高品质语音教学视频
额外超值赠送2.5小时28课新视频

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

网络安全专家
Network security experts

暗战

黑客攻防
实战高级演练

武新华　陈艳艳　　等编著
飞思科技产品研发中心　监制

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内容简介

本书紧紧围绕黑客防范技巧与工具展开，在剖析用户进行黑客防御中迫切需要用到或想要用到的技术时，力求对其进行“傻瓜”式的讲解，使读者对网络防御技术形成系统了解，能够更好地防范黑客的攻击。全书共分为14章，包括：黑客文化漫谈、黑客入侵前的准备、嗅探与扫描技术、欺骗与攻击技术、拒绝服务攻击技术、Web攻击技术、常见软件安全攻防、日志与后门清除技术、网络安全防御、病毒技术及其防御、木马入侵与清除技术、防火墙与入侵检测技术、全面提升自己的网络功能、远程控制攻防技术等内容。随书所附的DVD光盘提供了多种攻防实战的教学视频，汇集了众多黑客高手的操作精华。

本书内容丰富、图文并茂、深入浅出，不仅适用于广大网络爱好者，而且适用于网络安全从业人员及网络管理员。

图书在版编目（CIP）数据

暗战强人. 黑客攻防实战高级演练 / 武新华等编著.—北京：电子工业出版社，2009.9
（网络安全专家）
ISBN 978-7-121-09174-2

I. 暗… II.武… III.计算机网络－安全技术 IV.TP393.08

中国版本图书馆 CIP 数据核字（2009）第 107796 号

责任编辑：杨　鸽
印　　刷：北京天宇星印刷厂
装　　订：三河市皇庄路通装订厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编：100036
开　　本：787×1092　1/16　印张：28.5　字数：729.6 千字
印　　次：2009 年 9 月第 1 次印刷
印　　数：4 000 册　　定价：55.00 元（含视频 DVD 1 张）

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

随着网络攻击手段的日趋复杂，有组织、有预谋、有目的、有针对性、多样化攻击和破坏活动的频繁发生，攻击点也越来越趋于集中和精确，攻击破坏的影响面不断扩大并产生连环效应，就势必需要构筑一种主动的安全防御，才有可能最大限度有效应对攻击方式的变化。本系列图书依托作者长期从事网络安全管理苦心积累的心得与一线拼杀的经验，以深入体验来揭示实战精要，带领广大醉心技术者穿越迷雾，把黑客们的伎俩看清楚。

下面，我们为大家简要介绍本套丛书的特点、学习方法及我们提供的服务。

“暗战强人”系列的组成及特色

本套“暗战强人”系列共包含了 3 本图书，即《暗战强人：黑客攻防入门全程图解》、《暗战强人：黑客及反黑客工具快速精通》、《暗战强人：黑客攻防实战高级演练》。关于 3 本图书的说明如下。

图书组成	特　色	适合人群	增值服务
暗战强人：黑客攻防入门全程图解	● 内容合理：精选入门读者最迫切需要掌握的知识点，构成一个实用、完整的知识体系 ● 举一反三：本书力求通过一个知识点的讲解让读者彻底理解和掌握类似场合的应对思路 ● 高效模式：全程图解模式可彻底克服攻防操作的学习障碍	没有多少电脑操作基础的广大读者、需要获得数据保护的日常办公人员、广大网友等	随书所附的 DVD 光盘提供了多种攻防实战的教学视频，汇集了众多黑客高手的操作精华，通过增加读者对主流攻防手法感性认识的方式，使读者实现高效学习
暗战强人：黑客及反黑客工具快速精通	● 理论+实战、图文+视频=让读者不会也会！作者采用最为通俗易懂的图文解说，即使是电脑新手也能理解 ● 任务驱动式的黑客软件讲解，揭秘每一种黑客攻击的手法 ● 最新的黑客技术盘点，让读者实现“先下手为强” ● 攻防互参的防御方法，全面确保用户的网络安全	喜欢钻研黑客技术但编程基础薄弱的读者、网络管理员、广大网友等	
暗战强人：黑客攻防实战高级演练	● 技术内容新颖：网络攻击手法日新月异，导致已有图书时效性降低，本书力求摒弃过时内容并考虑前瞻性 ● 知识体系完整，注重攻防操作与原理、思路的印证，以培养读者举一反三、可灵活应对未来攻击的分析与实践能力 ● 案例丰富，注重时效，克服其他图书因无法再现攻防现场而泛泛而谈的弊病	具备一定黑客知识基础和工具使用基础的读者、网络管理人员、喜欢研究黑客技术的网友等	

针对不同的读者群和不同的读者需求，上述 3 本书可使读者有选择、有针对性地根据自己的阅读喜好和操作水平进行选择。

关于本书

作为系列图书中的高级实战演练部分，本书更注重对操作技巧的剖析，不但介绍了黑客攻击计算机的一般方法、步骤，以及所使用的工具，而且向读者详细地讲述了防止黑客攻击的方法，使读者在遇到别有用心者的入侵时能够尽可能心中有数，从中采取相关的方法来制定相应自救措施。

本书特色

本书以情景教学、案例驱动与任务进阶为鲜明特色，在书中可以看到一个个生动的情景案例。通过完成一个个实践任务，读者可以轻松掌握各种知识点，在不知不觉中快速提升实战技能。

- 情景教学：紧扣“理论+实战、图文+视频，全面提升学习效率！”的主导思想，采用最为通俗易懂的图文解说，为读者阐述操作流程。
- 案例驱动：盘点最新黑客技术，并采用攻防互参的方法详述范例完整操作过程，便于读者实战演练。
- 任务进阶：详细分析每一个入侵步骤，以推断入侵者在每一入侵步骤的目的及所要完成的任务，并对入侵过程中常见问题进行必要的说明与解答。

本书适合人群

本书作为一本面向广大网络爱好者的速查手册，适合如下读者学习使用：

- 电脑爱好者、提高者；
- 具备一定黑客知识基础和工具使用基础的读者；
- 网络管理人员；
- 喜欢研究黑客技术的网友；
- 大、中专院校相关学生。

本书作者

本书作者团队长期从事网络安全管理工作，都具有较强的实践操作能力及一线拼杀经验。

本书编写情况：冯世雄负责第 1 章，李防负责第 2 章，王肖苗负责第 3 章，陈艳艳负责第 4、5、6 章，杨平负责第 7 章，段玲华负责第 8、9 章，李伟负责第 10 章，郑静负责第 11 章，王英英负责第 12 章，孙世宁负责第 13 章，张晓新负责第 14 章，最后由武新华通审全稿。我们虽满腔热情，但限于自己的水平，书中仍难免有失误、遗漏之处，因此，还望大家以宽容为本，慈悲为怀，本着共同探讨、共同进步的平和心态来阅读本书。我们随时恭候您提出的宝贵意见。

最后，需要提醒大家的是：

根据国家有关法律规定，任何利用黑客技术攻击他人的行为都属于违法行为，希望读者在阅读本书后不要使用本书中介绍的黑客技术对别人进行攻击，否则后果自负，切记，切记！

编　著　者

联系方式：

咨询电话：（010）88254160　88254161-67
电子邮件：support@fecit.com.cn
服务网址：http://www.fecit.com.cn　　http://www.fecit.net
通用网址：计算机图书、飞思、飞思教育、飞思科技、FECIT

目　录

第 1 章 黑客文化漫谈

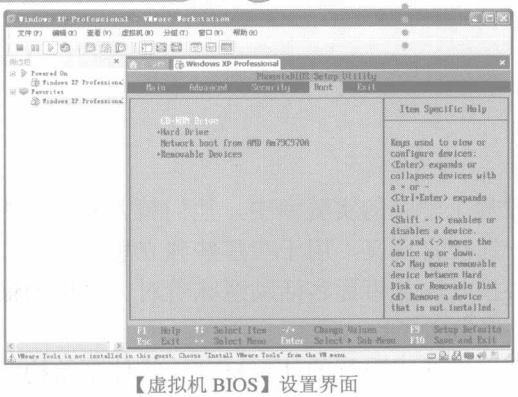
本章精粹

- 黑客的过去、现在和未来
- 黑客的行为准则
- 黑客应该怎样学习

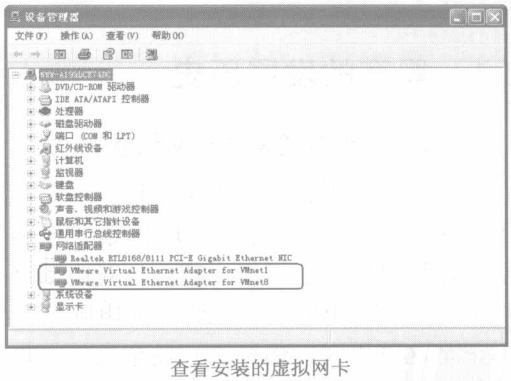
内容介绍

本章着重介绍了黑客的过去、现在和未来，以及黑客的行为规则、黑客必须掌握的各种资源等内容，有助于读者掌握一些防止黑客攻击的基本方法，并熟悉黑客常用的命令和工具，为自己实现安全防御带来便利。

视频链接

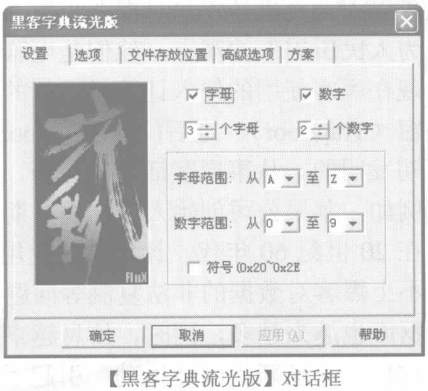


【虚拟机 BIOS】设置界面



查看安装的虚拟网卡

在虚拟机重启动系统



【黑客字典流光版】对话框

01 黑客文化漫谈

随着网络发展和普及的势头突飞猛进，网站、电子邮件、电子商务、网虫等名词扑面而来。在这个仅仅存在数十年的网络虚拟社会中，自然孕育了一套独特的规章制度，但由于时间和空间的过度压缩，以及发展的极度膨胀，造成了网络制度和网络自由的冲突，也出现了一群新的团体——黑客。

1.1 黑客的过去、现在和未来

目前有很多关于黑客的定义，其实黑客来自于英文“Hacker”。Hacker 原指用斧头做家具的人，专指那些手艺高超、不需要太好的工具，只用斧头也可以做出好的东西。延用到计算机领域，可以引申为那些乐于深入探究系统的奥秘，寻找系统的漏洞，为别人解决困难，同时不断克服网络和计算机限制的高手。神秘、隐蔽、怪异正是黑客的特点。

随着 Internet 的迅速发展、网络带宽的快速提升、网络用户群体也在增加，网络的安全问题也变得越来越突出。网络攻击的便利性和简易性，以及我国网络信息系统的安全脆弱性，致使黑客攻击呈多发性的特点。

1.1.1 黑客的发展历史

1. 国际上黑客的发展与文化状况

一般认为，黑客起源于 20 世纪 50 年代麻省理工学院的实验室中，他们精力充沛，热衷于解决难题。20 世纪六七十年代，“黑客”一词极富褒义，用于指那些独立思考、奉公守法的计算机迷，他们智力超群，对电脑全身心投入，从事黑客活动意味着对计算机的最大潜力进行智力上的自由探索，为电脑技术的发展做出了巨大贡献。

正是这些黑客，倡导了一场个人计算机革命，倡导了现行的计算机开放式体系结构，打破了以往计算机技术只掌握在少数人手里的局面，开辟了个人计算机的先河，提出了“计算机为人民所用”的观点，他们是电脑发展史上的先驱者。

现在黑客使用的侵入计算机系统的基本技巧，例如，破解口令（Password Cracking）、开天窗（Trapdoor）、走后门（Backdoor）、安放特洛伊木马（Trojan Horse）等，都是在这一时期发明的。从事黑客活动的经历，成为后来许多计算机业巨子简历上不可或缺的一部分。例如，苹果公司创始人之一乔布斯就是一个典型的例子。

在 20 世纪 60 年代，计算机的使用还远未普及，还没有多少存储重要信息的数据库，也谈不上黑客对数据的非法复制等问题。到了 20 世纪八九十年代，计算机越来越重要，大型数据库也越来越多，同时，信息越来越集中在少数人的手里。

这样，一场新“圈地运动”引起了黑客们的极大反感。黑客认为，信息应共享而不应

被少数人所垄断，于是将注意力转移到涉及各种机密的信息数据库上。而这时，电脑化空间已私有化，成为个人拥有的财产，社会不能再对黑客行为放任不管，而必须采取行动，利用法律等手段来进行控制。黑客活动受到了空前的打击。

2．国内黑客的发展与文化状况

随着 Internet 在中国的迅速发展，国内上网的人数也在持续增长，随着网民的日益活跃，“黑客”事件也时有发生。国内黑客发展主要经历了如下 3 个阶段。

1）第 1 代（1996—1998 年）

1996 年因特网在中国兴起，但是由于受到各种条件的制约，很多人根本没有机会接触网络。当时计算机也没有达到普及的程度，大部分地区还没有开通因特网的接入服务，所以中国第 1 代黑客大都是从事科研、机械等方面工作的人，只有他们才有机会频繁地接触计算机和网络。他们有着较高的文化素质和计算机技术水平，凭着扎实的技术和对网络的热爱，迅速发展成为黑客。有的人专门从事网络安全技术研究或成为网络安全管理员，有的则开了网络安全公司，演变为派客（由黑客转变为网络安全者）。

1998 年 8 月暴发了东南亚金融危机，并且在一些地区发生了严重的针对华人的暴乱，当时残害华人的消息在新闻媒体上报道到后，国内计算机爱好者怀着一片爱国之心和对同胞惨遭杀害的悲痛之心，纷纷对这些行为进行抗议。中国黑客对这些地区的网站发动了攻击，众多网站上悬挂起中华人民共和国的五星红旗。当时黑客代表组织为“绿色兵团”。

2）第 2 代（1998—2000 年）

随着计算机的普及和因特网的发展，越来越多的人有机会接触计算机和网络，在第 1 代黑客的影响和指点下，中国出现了第 2 代黑客。他们一部分是从事计算机行业的工作者和网络爱好者；另一部分是在校学生。这一代的兴起是由 1999 年 5 月 8 日某国轰炸驻中国南斯拉夫大使馆事件引发的黑客代表组织为原“中国黑客联盟”。

3）第 3 代（2000 年至今）

这一代黑客主要由在校学生组成，其技术水平和文化素质与第 1 代、第 2 代相差甚远，大都只是照搬网上一些由前人总结出来的经验和攻击手法。现在网络上所谓的入侵者也是由这一代组成。但领导这一代的核心黑客还是那些第 1 代、第 2 代的前辈们。这一代兴起是由 2001 年 4 月的一起撞机事件而引发的，黑客代表组织为“红客联盟”、“中国鹰派”。

1.1.2　黑客的现状及发展

1．现状

国内黑客站点门派繁多，但整体素质不如人意，有的甚至十分低劣。主要表现在如下 6 方面。

1）叫法不一，很不正规

黑客，甚至包括骇客，这两个单词都是在相关资料如词典、黑客界等领域有章可循的。目前对“黑客”一词的各种叫法极不规范。

2）技术功底薄弱，夸大作风

比如国内几大黑客组织的站点，只顾如何教他人攻击别人的电脑，刷Q币、盗密码等，以适应初学者的口味。站点用色彩绚丽的界面和震撼的音乐等手段，来吸引众人尤其是青少年的眼球。青少年不成熟，崇尚自由、冒险和刺激，有强烈的表现欲，黑客行业正符合这一特点，所以众多黑客站点投其所好，使青少年趋之若鹜，来提高自己的站点访问量，而不是靠实力提高站点的知名度。

3）内容粗制滥造

内容粗制滥造，应付了事，原创作品少，且相互抄袭。曾有一篇文章说，中国黑客一代不如一代。

4）效率低，更新少，可读性差，界面杂乱

有些站点很少更新，还经常会出现死链接，打不开；站点杂乱。

5）整体技术水平不高，研究层次级别低

目前国内几大黑客站点大都进行商业化运作，安全培训。以追求最大经济效益为目的，只要能赚到钱就够了。至于深层次的研究，是没有的。只是每天更新一些新闻、黑客教程、软件等，用户只能学到一些编程知识，数据库知识，再看看一些教程，借用一些黑客工具，就去攻击别人的站点、盗号等。而国外的黑客则是研究系统级别的漏洞，制造的也是世界级别的系统病毒，扰乱全球网络。

6）缺少一个统一协调中国黑客界行动发展的组织

虽然目前好多站点都包含有“联盟”字样，但其实都只是一家，各自为政，这就使得在抗击外来网络入侵时缺少统一指挥，大大降低中国黑客界整体的力量。

黑客并不是大家所想象的专搞恶意破坏的不良分子，他们是一群纵横驰骋于网络上的侠客，他们是一群热衷于网络安全技术的爱好者，追求共享、免费，提倡自由、平等。黑客的存在是由于计算机技术的不健全而造成的，从某种意义上来讲，计算机的安全需要更多黑客去维护。

2．趋势

目前中国黑客的发展总体可以归为以下5大趋势。

1）黑客年轻化

由于中国互联网的普及，形成全球一体化，甚至连很多偏远的地方也可以从网络上接触到世界各地的信息资源，所以越来越多对这方面感兴趣的中学生，也已经涉足到这个领域。

2）黑客的破坏力扩大化

由于互联网的普及，电子商务也在蓬勃发展，全社会对互联网的依赖性日益增加，黑客的破坏力也日益扩大化。仅在美国，黑客每年造成的经济损失就超过100亿美元，可想而知，对于网络安全刚起步的中国来说破坏的影响程度就更大了。

3）黑客技术的迅速普及

黑客组织的形成和黑客傻瓜式工具的大量出现导致的一个直接后果就是黑客技术的普及，虽然在市面可能看不到一本介绍如何做黑客、传授黑客技术的书。但是在Internet上，黑客与黑客组织办的传授黑客技术的站点却比比皆是。