电脑报 总策划

滕大鹏 编著

我的黑客女友

首开国内黑客攻防与黑客情感结合之先河

一招招黑客伎俩
一场场黑客激战
VS
一套套防范应对方案
一段段黑客爱恨情仇

一个曲折离奇的黑客情感故事

带你走近黑客 了解黑客

学黑客绝技高招 做网络安全卫士

山东电子音像出版社出版

我的黑客女友

滕大鹏 编著

山东电子音像出版社出版

内容提要

这是一本写给想学黑客攻防、想了解黑客生活的普通电脑用户的IT图书。

与其他讲黑客的图书不同的是，本手册采用小说故事与黑客技术交织的方式，把一招招黑客伎俩与防范技术，展现于一幕幕黑客交战与爱恨情仇中，尤其是主人公阿衣那曲折离奇的爱情故事贯穿全书，更让人读来情感交织，引人入胜。

在黑客技术方面，涉及了黑客入门读者关注的方方面面，如网民们应用最广泛的聊天工具QQ的攻防实例、系统文件账户密码的管理与保护、傻瓜黑客扫描与嗅探实例剖析、木马攻击手段大揭秘与防范措施、远程控制实战演练、系统漏洞的检测与安全巩固以及SQL注入式攻击与防范等内容。本手册采用轻松活泼的语言，以实例的形式演示了黑客攻防的全过程，讲解详细，通俗易懂。

本手册适合所有的电脑初学者以及黑客知识爱好者，将带领大家走近黑客，了解黑客。在你为“黑客女友”唏嘘不已的同时，就能轻松学会黑客的绝技高招。

警告：文中涉及到的黑客攻防相关内容，仅供读者学习之用，如用于非法用途，后果自负！

书　　名：我的黑客女友
编　　著：滕大鹏
执行编辑：曾　茜　李　勇
封面设计：陈　敏
组版编辑：陈　晶
责任编辑：李　萍
监　　制：时均建
出版单位：山东电子音像出版社
地　　址：济南市胜利大街39号
邮政编码：250001
电　　话：(0531) 82060055-7616
发　　行：山东电子音像出版社
经　　销：各地新华书店、报刊亭
CD生产：北京中联光碟有限公司
文本印刷：重庆升光电力印务有限公司
开本规格：787mm × 1092mm　1/16　16.5印张　200千字
版 本 号：ISBN 7-89491-292-1
版　　次：2006年1月第1版　2006年1月第1次印刷
定　　价：25.00元（1CD+配套书）

看黑客七情六欲 学黑客绝技高招

Preface

对于普通用户来说，通往电脑的路只有一条：接上电源、按下开关，然后，要么浏览网页，要么和网友聊聊天、玩玩网络游戏。但对于黑客这群在互联网中神出鬼没的电脑高手来说，却没有这么简单。大多数的网民认为黑客离我们很遥远，其实，黑客就在我们身边。当我们的电脑一连上互联网，我们就生活在一个充满黑客的网络世界里了，而我们都是黑客故事中的一员……

《我的黑客女友》讲述了一个美丽的爱情故事：主人公阿衣是一名在校大学生，他从玩网络游戏开始与“黑客”结缘，并从此自学黑客技术。但就在他陶醉于享受攻击别人的快乐时，却有人一再警告他这并不是黑客，仅仅算是个骇客而已。他们告诫阿衣：

我们是中国的鹰派
我们要做民族的精英
所有正义的人们给了我们力量和勇气
我们会永远战斗不息
……

阿衣充满矛盾地徘徊在红客与骇客的边缘……

一次，当在他在游戏中用木马“作弊”PK别人的时候，遇见了一个叫“咖啡色”的黑客高手并与其展开了多次激烈的黑客大战。最终“鹿死谁手”？隐藏在迷雾深处的“黑客女友”又是谁呢？阿衣在演绎着生活中的黑客传奇，本书将为大家一一揭晓！

神秘的黑客既让人害怕，又让人着迷。在科学技术日益发展的今天，学一点反黑技术已成了行走网络江湖必备的防身术。到底黑客的世界是怎样的？他们用什么技术、哪些工具来攻击目标？更为重要的是我们该如何来防范黑客的攻击……黑客其实也是食五谷杂粮的普通人，黑客也有七情六欲，黑客也不是天生这么厉害的。一个“骨灰级” 的黑客也是经历了从无到有、从低级到高级的成长之路的；一个真正的黑客是致力于保障网络世界的安全，他们的“刺刀”是带着思想的……这才是健康的黑客精神和黑客文化。

现在，就让我们一起走近黑客，看黑客爱情，学黑客技术，演绎传奇黑客，做网络安全卫士吧！

编者
2006年1月

Contents

第一回 做个黑客有什么不好

温暖的阳光慵懒地照在X大学的计算机系的男生宿舍，几个通宵达旦沉迷于网络游戏的男生，不时发出嘈杂和叫骂。在电脑前边抽烟边咳嗽的主人公阿衣随室友玩了两年网游，逃课，挂科无数，背负着不堪回首的糜烂大学生活记忆，胡混人生。

然而，不知道为什么，今天阿衣对男生宿舍的嘈杂和喧闹非常反感，他甚至不能在宿舍继续待下去了，难道就为叶融今天在论坛上发表的一篇文章？

第一章 揭开黑客的神秘面纱

第二回 徘徊在红客与骇客边缘

神秘的黑客吸引了阿衣，他开始试用了一些傻瓜黑客工具。他也经常伙同其他黑客一起对别人的网站进行攻击，盗取了很多的账号密码，分享了无数次成功的喜悦，当然也会自以为是地把自己的攻击经历发布到网上以示炫耀。

就在他“如日中天”的时候，却出现了一个反对的声音向他提问“黑客难道就以攻击为乐？”，这让阿衣开始思索什么是真正的黑客。

第二章 QQ攻击与防范

目录

目录

第三回 木马，网络情缘从此开始

误入歧途的罪犯怎能轻易做到“金盆洗手”？生活在继续，学习在继续，阿衣的黑客生涯也在继续……

这时，一个叫“咖啡色”的黑客高手出现了。阿衣首次在别人面前栽了个大跟斗，接连的黑客攻击皆告失败，极大地打击了阿衣的自尊心。

第四章 傻瓜扫描与嗅探实例剖析

第五章 木马攻击与防范

目录

第四回 女友是“黑”出来的

网络是虚拟的，但是网络并非完全不受限制，道德与法律在网络世界同样发挥作用。黑客技术就是刺刀，但是仅仅有刺刀没有思想是不行的。

“黑”出来的女友叶融的话让阿农开始反思，自己究竟该怎么做，他开始钻研“有思想”的黑客技术。

第六章 远程控制实战演练

第七章 系统漏洞攻击与防范

第五回 我的黑客女友

网上一个你
网上一个我
网上我们没有一句承诺
点击你的名字
发送我的快乐
接收吧！接收吧！！爱的花朵！！！
轻轻地告诉你我是真的爱过
你曾经真真切切闯进我生活
……

黑客让阿衣找到了黑客女友，更是黑客让他选择了“红客”之路，从此踏上了人生的正轨！

目录

第八章 注入攻击与防范实例

第一回

做个黑客有什么不好

温暖的阳光慵懒地照在X大学的计算机系的男生宿舍，几个通宵达旦沉迷于网络游戏的男生不时爆发出嘈杂和叫骂的声音。在电脑前边抽烟边咳嗽的主人公阿衣玩了两年网游，逃课，挂科无数，背负着不堪回首的糜烂大学生活记忆，胡混人生。

阿衣颓废中的惟一乐趣就是钻研黑客技术，这让在常人眼里属于“另类”的阿衣颇有几分成就感和自豪感。

然而，不知道为什么，阿衣今天对男生宿舍的嘈杂和喧闹非常反感，他甚至不能在宿舍继续待下去了，难道就为叶融今天在论坛上发表的一篇文章？

什么是真正的黑客

阿衣神情恍惚地离开了宿舍，独自在校园的小道上漫无目的地走着，论坛上叶融的话就像一根钢针，狠狠地刺向阿衣的心窝：

黑客也是有思想的
黑客并不等于攻击，不等于破坏
黑客的水平不是以“黑”掉多少个网站来衡量的
也不是以盗取了多少密码来评价的
只会攻击的黑客最多算是个“脚客”
就如同社会上的小混混、社会的渣滓
……

真正的黑客是不会发动攻击的
他们检测系统的安全漏洞，发现隐患，消除隐患
……

回想自己进大学以来的所做所为，想着未来的道路该何去何从，阿衣心里滴淌着热泪……

与黑客结缘

初次接触“黑客”是阿衣刚进入大学时，从网络上知道这个词的。那时还不知道什么是红客，什么是骇客，阿衣只是茫茫网海中的一只小菜鸟，闲着没事时总喜欢到机房上网，在无穷无尽的网络资源中“游荡”！

慢慢地，阿衣迷上了游戏，于是网吧就成了阿衣的新“家”。阿衣经常过着与常人完全不同的生活——他的作息时间表与大家截然相反：早上8点，大家都去上课，而阿衣却刚从网吧回宿舍睡觉；而到了晚上10点，大家准备睡觉休息时，阿衣却外出鏖战游戏，这是他一天中精力最好的时候……

阿衣在玩游戏时，意外地学到了一个新词，那就是“木马”。因为听说用木马能盗取别人等级高的游戏账号，阿衣来劲了，并从此与黑客结缘。

黑客，在很多人眼里几乎等同于“神秘”，到底他们是一群什么样的人，让我们一起来揭开他们神秘的面纱吧！

CHAPTER 1

揭开黑客的神秘面纱

1.1 什么是黑客

1. 黑客的定义

现在的黑客一般是指那些利用网络的安全漏洞或安全缺陷未经许可非法闯入别人电脑系统的人。

但最初，黑客并不是这个意思。黑客对应的英文是Hacker，本意是指高水平的计算机专家。他们一般是精通操作系统和网络通信以及软件编程的电脑高手，对计算机知识有着深刻的了解，喜欢疯狂地钻研相关技术，乐于剖析操作系统的奥秘并且善于从中发现系统的漏洞。他们以向防范严密的网络系统挑战为乐趣，以此来检查网络系统的完整性和完全性，改善网络系统的安全，使网络趋于完善。也有一些黑客入侵网络纯粹是为了恶作剧或者以此炫耀自己的技术。

黑客在网络世界穿越

最初，黑客们的行动对计算机网络技术的发展起到了强大的推动作用，他们促使网络系统更加安全，使得信息安全技术蓬勃发展起来了。

2. 什么是骇客和红客

正规的黑客发现系统漏洞侵入系统后并不进行破坏性活动，而是促使网络管理者发现和改善网络安全问题。由于黑客喜欢将自己对网络系统技术的研讨和破解侵入的经历放在网上共享，随着网络的发展，黑客技术和黑客工具逐渐扩散开来，黑客问题逐渐成为网络

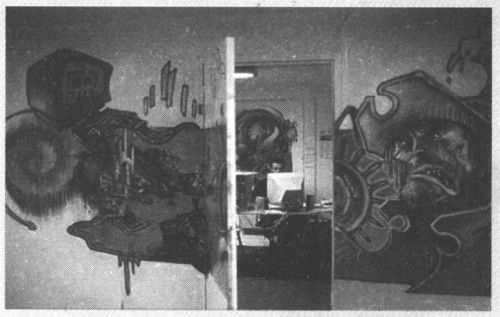
安全必须关注的课题。

黑客队伍的扩大使得这个群体逐渐变得龙蛇混杂、泥沙俱下。一些怀着不良企图的人利用非法获得的系统访问权远程侵入网络系统，窃取或者破坏重要数据，或者为了自己的私利制造麻烦。一般这类非法闯入电脑系统搞破坏的捣乱分子被称作“Cracker”，国内有人将之译成“骇客”，还有人称其为“怪客”。真正恪守职业道德的黑客一般不屑与之为伍，但是多数场合下，人们都是将其混为一谈的。

近年来，骇客的肆意横行给计算机系统和信息网络的安全带来了严峻的考验。他们中有的是涉世未深、法律意识淡薄的的青少年，出于好奇和炫耀技术的目的，利用从网上获取的黑客技术非法侵入了系统；而有的则是居心叵测，以恶意破坏和窃取信息、金钱为目的的犯罪分子。

“红客”这个词语是国内网络爱好者的发明。他们宣称自己是具有强烈正义感的网络高手，他们入侵网站的目的都是出于捍卫祖国的尊严，主张利用黑客技术去打击一切反动或有损祖国利益的网站。这个词语随着2001年中美黑客大战在国内流行开来。

国内网络界对红客很有争议，有人持赞同意见，但是大部分网络安全专家对此表示反对：无论红客的出发点是什么，就其网络攻击的客观行为来说，是一种对网络秩序的挑战和破坏。网络攻击行为，无论在中国还是在外国，都是法律所不允许的。



● 巴黎一所黑客学校
进来就会感到一种另类的气氛

3. 黑客的分类

构成黑客群体的人形形色色，各种各样的黑客大概可以分成以下几类：

（1）典型的计算机黑客

这类人多是一些精通计算机技术的高手，他们以攻入计算机系统为乐事，专门挑战那些防守严密的网络信息系统，以此来证明自己的技术。他们喜欢在网上与朋友们共享其成功经验，交流攻击手段，公布被其破解的一些计算机系统的漏洞、账户、口令等信息。

相对来说，这类黑客危害较低，他们只是为了进行技术测试，有选择地侵入一些计算机系统，一般不会主动破坏被侵入的网络系统中的数据。他们在发现了某些内部网络漏洞后，会主动向网络管理员指出或者干脆帮助其修补网络错误以防止损失扩大。他们能使更多的网络趋于完善和安全，但是未经允许进入别人的电脑系统毕竟是违法的。

（2）伪黑客

这类人的法律意识和道德意识都很淡薄。他们仅仅了解一些黑客技术的皮毛，特别想展示其三脚猫的功夫，利用从网上获得的一些现成的黑客工具，不管三七二十一，不论大小网络还是个人电脑，兴致所至，乱“黑”一气，制造了很多麻烦，有时甚至也可能造成很大的破坏。对大的站点或者网络来说，其威胁程度较低，因为其技术水平有限；对于个

人电脑用户而言，这是最现实的威胁，因为这种人在网上特别多，而且喜欢到处乱窜，聊天室、论坛等场所常能看到他们的身影。

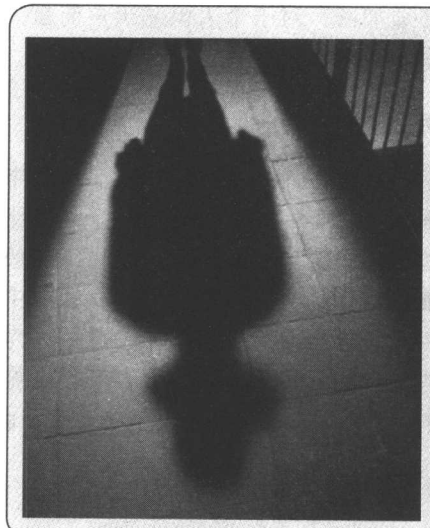
（3）系统内部的心怀不满的人

堡垒最容易从内部攻破，一些心怀不满的或者遭到解雇的员工，出于泄愤或者报复的目的极有可能对系统发动攻击。他们非常了解网络的安全状况和系统的脆弱性，知道部分关键内幕，掌握一定的访问权限，熟悉系统的后门，因此他们的攻击极易得手并可能造成最严重的破坏。

防范这类黑客不仅需要技术上的措施，还得加强内部管理，比如严格权限分配，不让无关的人员接触系统关键问题，尽量缩小知密范围，定期删改账户以及修改密码，对离职人员及时取消其系统访问权限等。对于个人电脑用户而言，这类攻击者一般是局域网内部熟悉你的情况并与你发生某些冲突的那些人。

（4）图谋不轨的罪犯

这类黑客入侵网络系统都有特定的目的，比如侵入系统掌握一定的权限，窃走相关机密信息，埋设逻辑炸弹来要挟系统管理员；或者侵入银行或者证券系统，直接获取经济利益；还有窃走机密信息高价倒卖等。这类黑客一般不会攻击个人电脑用户。



黑客经常像幽灵一样不请自来

（5）网络间谍

这类黑客一般受某些公司或组织雇佣，利用黑客技术手段专门窃取竞争对手的商业机密或者给竞争对手制造麻烦，干扰竞争对手的正常商业行为。更高一级的甚至受雇于政府机构或军方，成为网络特工，专门从事刺探、破坏他国信息网络的活动。

1.2 黑客攻击行为大曝光

黑客侵入别人的电脑系统都会干些什么呢？知道这些，才能有的放矢，有针对性地加强网络安全防护。

1. 非法访问系统

正规的电脑网络系统一定要经过授权才能访问，所以黑客在实施网络攻击前必须要得到访问系统的权力。对于个人电脑而言，一旦接入局域网或者 Internet，就给黑客访问你的电脑提供了可能，因为我们的个人电脑要接入网络，必须要保证与其他电脑的通讯。比如很多使用 Windows 9x/Me 的朋友，习惯使用网络共享来交流数据，黑客就能利用这一点浏览你电脑中的信息。