络白

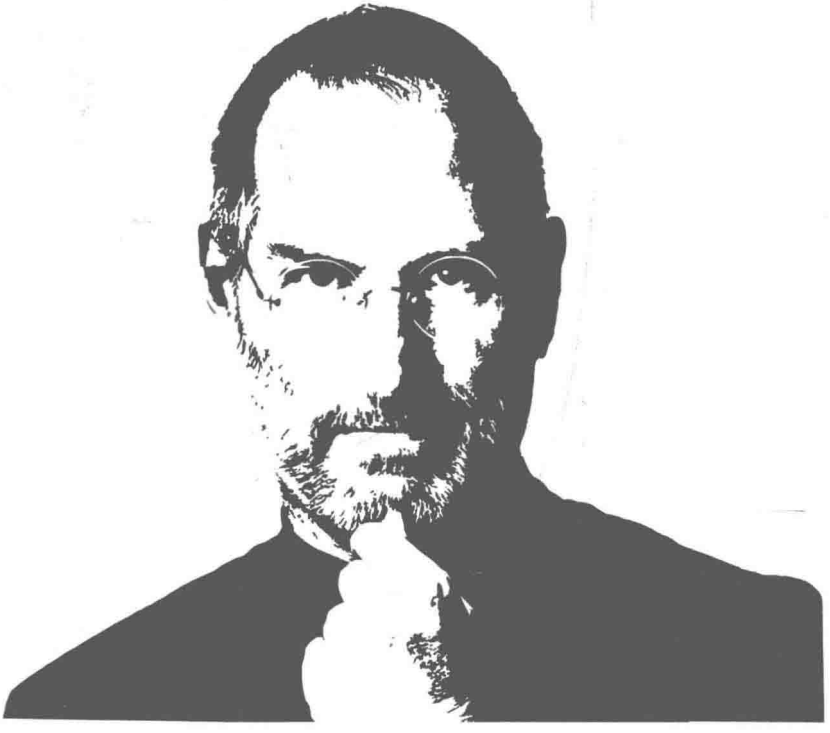
花无涯◎著

网络安全是互联网公司的生命
也是每位网民的最基本需求

一位混迹在网络黑白世界中的黑客与你共分享一场饕餮盛宴

梦想有一天 我们共同进步
让互联网不再饱受安全的困扰

四季出版社



致敬乔布斯

You've got to find what you love

目 录

第一章

你好，黑客

1.1 我的安全之路

本书全文通俗易懂，不需要你懂很高深的东西，你就可以入门，当然对完全不懂互联网的，可以跳过第四、五、六章因为是技术章节，其他的章节都深入浅出，慢慢的品味下去都能理解。

必须感谢支持这本书的所有人，对，是所有人，不管你有没有听说过我和这本书以及任何地方传来的故事，没有你们，就没有这本书的存在！为什么说是黑客入门必备的，本书详细的阐述了黑客入门的世界，并不是媒体或者你原先所认知的那样。

也是信息安全类入门书籍，小白必看，IT 从业者必备书籍！这段先谈谈我的个人经历总结以及让你们感兴趣并受益匪浅的东西！You've got to find what you love!

第一次接触到网络的时候，是小学升初中。那时候学校旁都是网吧，我想这点很多人都会有同感，不玩的话可能失去了原本的乐趣，天天就是打游戏。

现在来谈网吧感触良多，当时的我与所有的网瘾少年别无异样，那些年的青葱岁月还是难以忘却。最初了解到黑客是无意中看黑客帝国这部电影令我印象深刻，其实那时候啥也没看懂，不明觉厉。

心里暗暗的埋下了一颗种子，此后在有限能接触电脑的机会里，找大量相关的资料了解阅读与黑客有关的东西，觉得似乎越来越有趣，大家也别探讨我的身世和年龄，百度都是别人瞎编的。

在那几年中，期间下载过很多外挂、工具、教程，都 TM 有毒，结果就是自己账号啥的都被盗了，很郁闷。这一事件彻底激发了对网络以及病毒木马的研究，思想也成长了不少，总会找些自己感兴趣的东西来研究，看教程学习到技术的乐趣远远大于游戏，过程中也会进行实践其中记载的方法为乐。

同龄人上大学时，而却我宅在家里，在亲爱的父母资助下，我拥有了自己的第一台 PC，这加快了我成长的步伐，与此同时我开始活跃在各大 BBS 和群探讨与交流，后来与一群志同道合的朋友建立了一个自己的网络聚集地。

迄今为止，同时期并存的黑客组织和黑客联盟持续因为不可抗拒的原因都慢慢消逝，黑客协会经历了十多年的风雨，期间经历过站点被封、域名被封、服务器被封，官博被禁，就连黑协的百度贴吧也被封了，哎，这些说多了都是泪，到如今我们培养出来了当今安全行业非常多的优秀人才，同时很多人也非常感恩，我在这里尤其感谢他们这么多年了，还能记得并且不断支持。

对于学黑客从什么地方开始学，我想这是很多小白对此的好奇心和神秘感，个人说几点对你有帮助的，多种命令是要掌握的，基础的操作命令如 DOS 等，其次是工具，很多前辈写的工具用着都是非常顺手。

最重要的思路，百度和谷歌不用再提了，做好充足的准备和周密计划，对于入侵和社工是非常有用的。强调一点中毒中马这个是常有的事情，建议大家可以安装虚拟机或者到沙盒测试，冰点和影子系统也不错，这样不会影响到本机的使用，土豪可以无视直接几台电脑操作备用，就是需要注意一下网络和 IP 地址的问题。

我认为黑客是一种精神的传承，黑客代表是一种精神，它是一种热爱祖国、坚持正义、开拓进取的精神。黑客之道亦是侠客之道，所谓真正的黑客并非是你们想象中的那种网上那些刷企鹅币、刷枪、刷车、刷钻以及盗小企鹅号、淘宝号、YY 号、各种号和恶意攻击网站的这些人，这一类人只是无知无畏好奇心强而已，甚至驱使他们沦为一名恶作剧，搞破坏的一名骇客。

个人认为黑客是指而是能够突破极限的能力，并拥有道德感、开放和共享的精神，最终的目的是推动世界发展朝着一个更好、更安全的世界发展。第一，从数据到知识，一切都是信息。网络安全在中国是奢侈品，安全本质则是对信息的控制权。黑客是未来信息社会重要的平衡力量。

我们不再有地域的阻隔，我们在网络下彼此相识，让互联网延伸彼此的友谊和文化；我们能共筑绿色的网络世界，在宁静和谐的网络中畅游；自由的人们总是不得不在自己的安全和自己的自由之间做出权衡。

回想起过去让我从不曾有过这样的激动和颤栗。真诚不是错误，年少也不是错误。时光静静地流过岁月的河床，有一天我们终会苍老如云，而那时他依然年轻。或许人们不知道，他留给我的一切是怎样充实自我日渐衰竭的生命。

当你白发苍苍的时候，当你步入垂暮之年的时候，你再一次回到计算机前，回到那个心灵曾经找寻过迷失过的网络中，你会清楚的发现，在厚厚的灰尘之下，仍然会残留着富有传奇的身影和保有激情的震撼。

1.2 黑客发展历程

黑客嘛，还是你感兴趣的内容，我们不谈某某某又贡献了什么，找度娘。每个人都有不同的想象。

他们帅吗？酷吗？真的什么都可以搞定吗？对电脑是无所不会的大神吗？好牛逼吗？好奇的问题真多……

带你们脱离网络来到现实，说不定和你乘坐同一班地铁、订同一家快餐诸如此类的。茫茫人海中，他可能是你、是我。擦肩而过，过去也就过去了。

凯文·米特尼克，这位号称世界头号黑客的男人，我想引用他的一句话，他这么说，巡游五角大楼，登录克里姆林宫，进出全球所有计算机系统，摧垮全球金融秩序和重建新的世界格局，谁也阻挡不了我们的进攻，我们才是世界的主宰。

不得不说真牛逼，将社会工程学运用到如此地步，偶像是用来崇拜的。黑客不作恶是将黑客精神的传承，我国的相关法律虽不完善，但也得遵守中华人民共和国法律为前提。

国外的大神比比皆是，MIT 这个曾经是 20 世纪黑客的起源地，你可以知道这个是个类似于俱乐部一样的就行了，英文看不懂没事，你别觉得这是个障碍，可以尝试自己找找资料，但是我想你可以尝试着理解，很多都是缩写，不必要太在意。

许多计算机和生物黑客都是在那里成长的，一场自由软件运动，电子朋客运动和地下安全世界，这看似三个完全不相干的群体却有着共同的哲学背景：黑客伦理或者直接叫黑客精神更为贴切。是黑客精神把这群人聚集在了一起，他们是来自不同领域的黑客。

早期，黑客攻击的目标以系统软件居多。一方面，是由于这个时期的 Web 技术发展还远远不成熟；另一方面，则是因为通过攻击

系统软件，黑客们往往能够直接获取 root 权限，现在手机 root 都应该有了解，这个就是获取管理员权限，或者说是控制权，拥有高权限的账户，这段时期，涌现出了非常多的经典漏洞以及“exploit”。

这个时代 Web 并非互联网的主流应用，相对来说，基于 SMTP、POP3、FTP、IRC 等协议的服务拥有着绝大多数的用户。因此黑客们主要的攻击目标是网络、操作系统以及软件等领域，Web 安全领域的攻击与防御技术都是处于非常原始的阶段。

相对于那些攻击系统软件的 exploit 而言，exploit 可以理解为漏洞利用，就是利用此来进行攻击，基于 Web 的攻击，一般只能让黑客获得一个较低权限的账户，对黑客的吸引力远远不如直接攻击系统软件来的更强烈。

说回到国内来，那个时期是中国互联网处于刚刚开始发展的朦胧时期，也就是在这一年，中国互联网的大门终于面向公众开放了。但是在那个年代，电脑还是一件非常奢侈的电子用品，而互联网对于大众来说更是一个陌生的名词，我们只有在专业性极强的书刊中能够找到与网络相关的名词，而那些上网的群体也多数为科研人员和年轻资本家。

盗版对我们来说还是一个陌生的名词，对于广大计算机用户来说，Copy 就是正版的一种传播方式。于是乎那个时代最早的黑客开始摸索，慢慢的发展。我们没有太多的理想和豪言壮语，一个全新的小软件就几乎是我们计算机的全部生命与理解，而能够 Copy 到国外的最新产品是最大的荣幸，那一张张的小软盘中承载了中国黑客最初的梦想。

“黑客”这一名词已经开始正式的深入广大网友之中，当时初级黑客所掌握的最高技术仅仅是使用邮箱炸弹，并且多数是利用国外的工具，完全没有自己的黑客武器，更不要说什么黑客精神。

1998 年印度尼西亚爆发了大规模的屠杀、强奸、残害印尼华人的排华事件。众多华人妇女被野蛮的强奸杀害，华人的超市被抢夺一空，很多丧失人性的印尼反华分子还将大量残害华人的图片发到了互联网上。

这一系列行为激怒了刚刚学会蹒跚走步的中国黑客们，他们不约而同的聚集在 IRC 聊天室中，并以六至十人为单位，向印尼政府网站的信箱中发送垃圾邮件，用 Ping 的方式攻击印尼网站。这些现在看来很幼稚的攻击方法造就了中国黑客最初的团结与坚强的精神，为后来的中国红客的形成铺垫了基础。

印尼排华事件造就了一大批网友投身于黑客这项活动中来，有些人在攻击过后又回到了现实生活中，有些人则从此开始了对黑客理想的执著追求。同样这次事件也使得，比如红客联盟、黑客协会等黑客组织的名字开始流传至今，并且仿冒的一个比一个多。

2000 年成为了中国网络最为辉煌的一年，网吧也在全国各地蜂拥出现，上网的人群更是增加了一倍多。一时间“你上网了吗？”成为了流行问候语。与此同时中国的黑客队伍也在迅速扩大着，众多的黑客工具与软件使得进入黑客的门槛大大降低，黑客不再是网络高手的带名词，很多黑客很有可能就是一个嘴里叼着棒棒糖手里翻着小学课本的孩子。也正是因为这种局面的出现，中国黑客的队伍开始杂乱。

2015 年巴黎市中心一餐馆和法兰西球场附近等多处发生枪击和爆炸事件，法国总统奥朗德称此次袭击系史无前例的恐怖袭击，并宣布全境进入紧急状态，并关闭了法国所有边境口岸。巴黎的安全形势仍极度紧张，警方高度怀疑仍有袭击者在逃。此外为应对本次恐怖袭击，巴黎警方要求所有市民呆在家中，不要外出。

IS 已经正式发文宣布对巴黎恐怖袭击负责，公告分别用阿拉伯文和法文书写。公告中称法国为他们的头号目标，他们曾仔细研究袭击地点，恐袭由配备自杀式腰带和机枪的战士实施。公告中还表示发动袭击是对侮辱先知穆罕默德所做出的回应，同时也是对法国恐袭 IS 控制区域的回应。IS 同时发布无具体日期视频，其中有武装分子称法国将不会拥有和平，爆炸将继续。

直到今天，人们才惊讶地发现，这个反人性反社会的恐怖组织已成人类公敌，那么它到底打哪儿来？他为什么会出现？如何一步步壮大？他们又为什么如此残暴？没有硝烟的战场除了大量的财富和精锐的武装。

ISIS 在网络战场同样罪行累累，他们拥有世界一流的网络攻击能力，曾数次攻击或入侵过西方国家的要害部门的网络，窃取机密甚至发言挑衅。他们精心拍摄的 YouTube 视频，专业制作的杂志，吸引人的 Facebook 和推特活动，以及利用社交平台做的精心策划，足以与许多老牌美国公司媲美。他们激进、招聘、培训，散布恐惧和不满，并且在世界范围内进行网络集资。

如果说 911 是迄今以来伤亡最大的一次恐怖袭击，那么此次从幸存者的描述中，直面人质时的镇静杀戮，其残忍性或已超过 911 不知道多少，彻底将 ISIS 的反人类本性暴露无遗。而同样，在网络战场，即便看不到刀光血影，ISIS 一次又一次地在制造攻击，窃取机密甚至招募同伙，他们无疑将网络视作最重要的舆论武器。而幸运的的是，越来越多的黑客组织肩负良知和勇气站了出来，即便他们面对的是这世界上最心狠手辣、毫无人道的恐怖组织，即便他们受到了一次又一次的死亡威胁。

1.3 对安全的思考

黑客代表的不仅仅是专业技术上的造诣，更包括了思想，甚至是一种精神。如今娱乐化严重的安全圈，二字早已成为了面子工作者嘴里的谈资。

现在获取信息的渠道越来越多，每天新增的技术文章早已超出了人能够处理的能力范围，很多原来不会上网的，现在到微信里头看文章，转发，加社群，都一样的可以获取到非常多的信息，但是凸显出来的是应该需要如何去发现精华、筛选、归类这些信息是很重要的工作。

说到思考来谈谈大数据时代网络安全的主要威胁，信息时代，大数据平台承载了巨大数据资源，必然成为黑客组织、各类敌对势力网络攻击的重要目标，脱库，被曝光的不在少数。

大数据平台依托于互联网面向政府、企业及广大公众提供服务，但我国互联网从基础设施层面即已存在不可控因素。网站及应用系统的漏洞是更是大数据时代的最大威胁之一。

现如今各行各业广泛采用了各种第三方数据库、中间件，但此类系统的安全状况不容乐观，广泛存在漏洞，及时发现了修复也并不及时，政府类的网站甚至管都没人管，不知道被挂了多少马利用了多少次，某些企业更甚对存在的漏洞表示否认，真不知道这样做是对消费者有好处吗。

现在的网络攻击手段多的一塌糊涂，APT 攻击、终端恶意软件和恶意代码是攻击大数据平台、窃取数据的主要手段之一。其中 APT 攻击非常具有破坏性，毫无疑问，大数据平台也将成为 APT 攻击的主要目标。

目前网络攻击越来越多地是从终端发起的，终端渗透攻击也已成为国家间网络战的主要方式。

“没有网络安全就没有国家安全，没有信息化就没有现代化”习大如此说，并将网络安全形象地比喻为，网络安全和信息化是一体之两翼、驱动之双轮。

我国是网络大国，却算不上网络强国。据不完全统计，我国拥有超过 7 亿网民，其中 79%的网民，也就是 5 亿左右网民曾遇到过网络安全问题。

同时，另外一个有意思的数据显示，在对抽样的 1000 份已知个人网络账号被盗事件的原因进行分析时，超过 50%的原因是由于口令问题，如使用弱口令被破解等，这意味着网民的网络安全意识存在的严重不足成为全球网络安全的一个重要隐患。

我想类似的例子不胜枚举，我写书的目的也非常简单，想让更多的人学习到网络安全知识，提高网络安全意识，很多被曝光被用烂的诈骗手法，但还是有人最基础的意识都没有，导致一次又一次的损失。

核心就是避免此类事件的发生，希望你看完整本书不仅仅学到的是仅有的内容，更加需要学会研究思考，有可能的话推荐给你的亲朋好友，他们或许遇到这样那样的网络上的问题，能实现让使用互联网的人不再饱受安全的困扰，享受信息时代本该拥有的乐趣，我想这才是核心，预防避免了，才能从根本上解决问题。

1.4 如何学习黑客

我想大家看到这本书的时候，本人已经退出这个圈子了，已经不在处理黑客协会的任何事务了，只想有更好的作品或者产品让更多的人体验到，并且学习受益。

每个年龄段有一份责任和应该做的事情，爱好就作为爱好吧。讲个段子，当我成为一名 IT 男后，在父母眼中我就像黑客帝国的主角一样了不起，在亲戚眼中我是在写字楼做办公室吹空调的人，在朋友眼中我就是一个修电脑的，在同行眼里我就是一个泡网吧的，在女友眼中我是一个从保安华丽转身为网络工程师，我理想中的样子应该是和乔布斯、比尔盖茨那样的人。

但我实际上是一个宅在家里抽烟吃零食加班到凌晨三点的人，别人眼中自己的职业形象总是光鲜靓丽，但实际的工作状态却有许多烦恼。

我愿意将现在的黑客归类为 IT 技术人群，啥叫黑客，我也没有办法用长篇大论来说明，简单的定义黑客一词，可以这样理解红客是褒义词，骇客是贬义词，黑客就是中性词。

至于什么客什么客的很多，这个并不是那么重要。现在很多黑客友情检测网站，主动帮忙找出网站系统漏洞。这部分黑客跟窃取个人信息而获得非法所得的黑客有本质差别。也是因为如此，黑客逐渐区分为白帽、黑帽等，这几年各大厂商也都做了自己的漏洞平台，漏洞一直是威胁网站安全的最重要因素。

还有必须说的一点就是编程，编程不算一件容易的事，在学习和解决问题总会碰到障碍。编程中也要经历很多尝试、失败、学习、思考、灵感、成功等，漫长的过程中要不断的学会适应这件枯燥的事情，办法总是比困难多。

学习最感兴趣的莫过于拿着前辈的工具用着真顺手，程序不是自己写的，只是觉得这个算一种捷径，确实也如此。可是现在有些人连工具不会使，天天到处喊找师傅，自己不看不思考你不要来说你学。就是在网络找些教程看效果都会好很多，上论坛、贴吧、群总会有聚集地学到东西。

想从一个菜鸟变成黑客高手 是一个漫长的道路 有了坚持的心才能迈向高手的大门，不是去怎么学那些技术，而是让自己有一个计划，给自己写一份详细的计划书，让他和你一起前进，只有当你有了一个目标才能去实现，路很长在漫长的学习与枯燥中，锻炼的是心境，因此需要坚持的心和一个目标伴随你，才能有成功那一天。

另外培养你对黑客的兴趣，有了兴趣才能让你坚持，让你不会半途而放弃学习，或许你才学不会感受到当你在这条路上走远了，处处碰壁学习杂乱无章中，到头来什么都没学到，你才知道这些的重要性吧。

当你对某一样东西非常熟悉的时候，你就能成为黑客了。学会的东西是自己的，其实创造比破坏更有趣！