# 网络安全

进阶笔记

彭文波　彭圣魁　万建邦　编著

- 实战性强，汇集了来自知名外企、Linux论坛及其他电子商务网络公司的一线作者！
- 为用户提供了安全进阶技术的关键性思维方式和思考方法！
- 介绍了多个操作系统平台的安全要点及跨平台安全的重要内容。
- 高级程序员助阵，有10年的.NET和Java平台开发经验，有助于网管员从另一种视角分析网络安全。
- 详解数字证书应用、EJBCA系统安装及PKI系统开发，符合最新安全技术潮流！
- 定位于“有效解决网络安全技术问题”，介绍典型案例。

清华大学出版社

# 网络安全进阶笔记

彭文波　彭圣魁　万建邦　编著



清华大学出版社
北　京

## 内 容 简 介

本书通过详细而新颖的安全实例，从新入行的大学生、办公室职员、黑客、网管、程序员等读者的角度，由浅入深、通俗易懂地讲解了安全进阶技术。本书内容来自第一线的网络安全工作，实战性强，演示步骤完整。在角色的演变与技术的进阶过程中，能够让读者快速掌握最新的网络安全技术。

本书主要内容包括梳理网络安全要素、构建网络安全平台、防范网络钓鱼攻击、剖析计算机病毒与黑客攻击原理、分析加密与解密原理、制作数字证书与实施 PKI 应用、搭建 Linux 安全平台、掌握 Linux 安全工具、学习安全编程(包括.NET 和 Java)、实现企业网络安全管理等，适合网络管理维护人员、网络安全工程师、网络程序员以及相关领域的其他从业人员阅读和学习。



**图书在版编目(CIP)数据**

网络安全进阶笔记/彭文波，彭圣魁，万建邦编著. --北京：清华大学出版社，2011.1
ISBN 978-7-302-24528-5

Ⅰ. ①网…　Ⅱ. ①彭…　②彭…　③万…　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(2010)第 258480 号

**责任编辑**：张　瑜　宋延清
**装帧设计**：杨玉兰
**责任校对**：周剑云
**责任印制**：李红英
**出版发行**：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
**社　总　机**：010-62770175　　**邮　购**：010-62786544
**投稿与读者服务**：010-62776969，c-service@tup.tsinghua.edu.cn
**质　量　反　馈**：010-62772015，zhiliang@tup.tsinghua.edu.cn
**印 刷 者**：北京密云胶印厂
**装 订 者**：北京市密云县京文制本装订厂
**经　　销**：全国新华书店
**开　　本**：190×260　**印　张**：34.5　**字　数**：833 千字
**版　　次**：2011 年 1 月第 1 版　　**印　　次**：2011 年 1 月第1 次印刷
**印　　数**：1～4000
**定　　价**：58.00 元

产品编号：039260-01

# 前　言

有人提出了这样一个算式，即“100-1=0”。也就是说，1 次网络安全事故，有可能让 100 次网络管理成果付之东流。在信息技术高度发达的今天，网络安全涉及的范围十分广泛，几乎每一种职业都会与网络产生紧密的联系。但是，有的网管对某些设备了如指掌，却对网络编程知之甚少；而有的程序员对开发语言十分熟悉，对程序运行的安全环境却熟视无睹。目前，以理论讲解网络安全的图书很多，但从不同职业视角来讲解网络安全的图书却十分少见。本书的价值在于从普通读者的角度出发，由浅入深、通俗易懂地讲解安全进阶技术，为用户提供关键性思维方式和思考方法。通过与实例结合，定位于“有效解决网管技术问题”，将网络管理中的典型问题归纳成“串”，并按层次铺开讲解。

## 1. 读者对象

本书面向以下读者：

- 如果你对网络安全和黑客攻防感兴趣，那么，这本书的前面章节将会告诉你如何快速入门。如果有进一步发展的需要，建议你在闲暇时，细细品读后面的章节。
- 如果你是高校计算机专业的学生，职业规划应该是你最感兴趣的话题，因为正确的职业规划可以让你快速步入高薪之门。当然，你也可以跳过部分难度较大的章节。这并不妨碍你快速成长为网络工程师或者高级程序员。
- 如果你是一名网络工程师，你可以尝试学习一些网络编程知识；如果你是一名网络程序员，你可以写出更加安全的代码。本书充分考虑进阶技能，尤其适合网络安全从业人员、网络管理员进阶，是提高工作效率的理想读本。
- 如果你对黑客攻防技术十分感兴趣，或者对网络攻击充满了好奇感，本书也可以给你提供满意的答案。

## 2. 内容介绍

阅读本书之前，你最好有一定的网络知识和操作系统知识积累。本书分为 11 章，在内容的安排上，也充分考虑了不同的读者定位。

- 第 1 章　理解网络安全要素。按照不同角色，用故事化语言总结了读者关心的问题。如网络安全的结构是怎样的，交换机与路由器的区别，常见的网络安全术语，TCP/IP 后面的网络协议，网络安全命令等。
- 第 2 章　构建个性化的进阶平台。该章适用于日常系统的安全配置。通过构建虚拟安全测试平台，配置 ASP、PHP、JSP 安全测试环境，确保虚拟主机安全。
- 第 3 章　享受安全的网络办公环境。重点讲解典型的钓鱼式攻击的原理及特点，以及典型的攻击案例。学习该章之后，你的网络办公环境可以明显提高一个安全档次。
- 第 4 章　拒绝恶意代码与神秘的黑客。该章用形象化的语言，讲解计算机病毒、木马的原理，清除常见病毒、木马的思路。为了提高用户的操作技能，还列举了黑客突破的工具，以及 Wsyscheck、VMWare 等工具的使用方法。

- 第 5 章　趣解加密与解密。几乎所有的安全应用都和加密解密技术有关系。该章首先讲述一些加密解密的趣闻轶事。通过 PGP 软件加密解密，阐述更多的安全术语，以及加密系统和加密算法原理；针对网络管理员、网络程序员等需求，还讲解 XML 文档的加密和解密。
- 第 6 章　奇妙的数字证书与 PKI 应用。这也是本书的重要部分。通过数字证书的获得、安装，EJBCA 开源系统的应用，以及 Esign 电子签名、SSL 访问浏览等，完全熟悉数字证书的应用。
- 第 7 章　配置安全的网管 Linux 平台。该章主要是帮助网管提升技能。包括打造安全的 Linux 系统策略，使用 Webmin 进行图形配置，Linux 下的防火墙、邮件系统、Samba 服务器、FTP 服务器，远程安全管理等。
- 第 8 章　掌握实用的 Linux 安全工具。该章同样定位于帮助网管提升操作技能，重点对必备的 Linux 安全工具进行讲解。包括寻找“肉鸡”的 Linux 工具，利用日志信息防范 Linux 入侵，使用 Ettercap 的方法，阻止 Linux 下的非法进程等。
- 第 9 章　举一反三学语言：以.NET 为例。网络管理员也要懂一点编程，这已经成为许多人的共识。该章提倡举一反三学习编程语言，通过熟悉语言的框架，以及具体的开发实例，快速掌握安全编程知识。
- 第 10 章　Java 网络安全应用进阶。对于网络安全技术员来说，不一定要精通每一门语言，但必须熟悉语言环境的配置。该章主要讲解 Java 环境配置，以及常见的 Java 安全编程规范等。
- 第 11 章　企业网络安全进阶。该章主要分析局域网的安全管理隐患，通过网络管理工具构建安全的企业网络。此外，还从技术金字塔、职业金字塔等角度，帮助读者实现更高的职业理想。

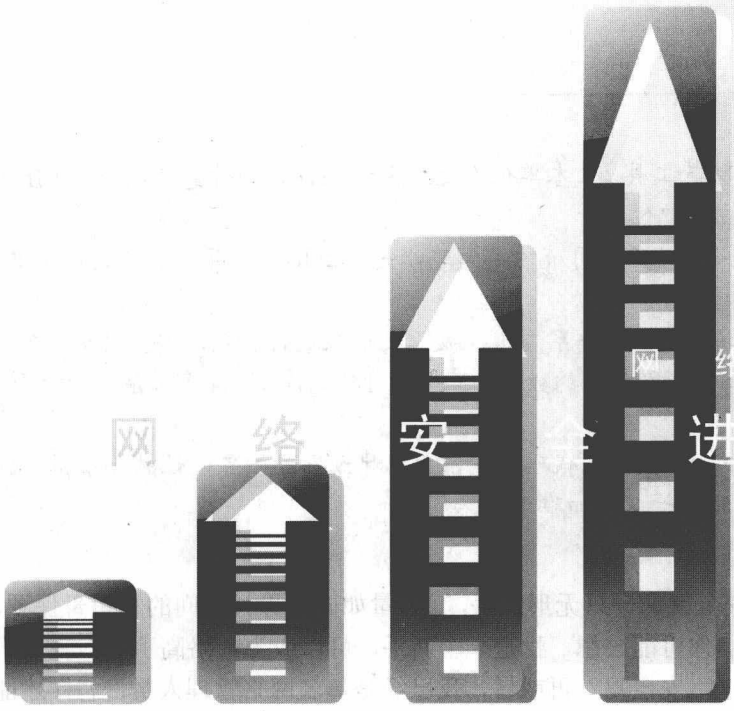
### 3. 本书特点

本书具有以下特点：

- 内容全面，重点突出。本书内容新颖，实践性强，语言生动活泼，通俗易懂。从实用角度出发，由浅入深地对 Windows、Linux 平台下的系统管理及网络服务做了全面、系统的介绍。
- 案例教学，步骤详细，脉络清晰，图文并茂。“案例+图片”的表现形式非常适合于初、中级 Linux 用户。
- 适合多个版本，结构合理，适用面广。汇集了来自北京惠普、Linux 论坛及其他电子商务网络公司的一线作者，内容讲解充分考虑了实战技能。

本书由彭文波、彭圣魁、万建邦编著，参与本书编写的还有刘耀宗、赵晓芳、刘琴、艾维峰、陈蓝、胡必飞、艾梅、邓世健、张慧。本书的编写得到了许多朋友的支持，在此表示感谢。本书专用博客地址为 http://blog.csdn.net/cndes。读者若有任何建议，欢迎到博客留言。

# 目　录




# 第 1 章 理解网络安全要素

我们对“黑客”、“网络安全”这些词语应该是再熟悉不过了。有人可能会思索：网络安全不就是网管关心的那些事儿吗？比如，单位网络瘫痪之后马上给网管打个电话，下班冲浪之时模仿黑客试探进入某个视频网站，不想破费买某个热门软件时找个注册机，再或者，有的人直接写一行十分锋利的代码，导致网络内的机器顷刻间出现问题。其实，网络安全并非某些人日常概念中的那样简单。学习网络安全知识，甚至从职业层面进行系统规划，可以帮助我们面对许多工作、学习中的问题。

在电影《阿甘正传》中，阿甘用自己锲而不舍的信念在向等车的路人讲述自己成功的故事；在《杜拉拉升职记》中，杜拉拉从一个默默无闻的职员，经过自己的不懈努力，成长为一个企业的高管。这种持之以恒的信念，也将是贯穿本书的精髓。这里将从最简单的安全知识着手，结合网络应用、数据保护、安全资源等内容，对网络安全的发展前景(尤其是职业前景)进行分析。本章的学习内容如下：

- 从不同的读者角度进行分析，我们到底面临哪些网络安全威胁？
- 网络安全的基础术语。了解这些术语，就可以弄清某种技术的来龙去脉，而不是只有十分肤浅的认识。

## 1.1 开篇之语：网络安全和我们有什么关系

且看看我们经常会碰到，而且天天在发生的几个故事。

(1) 小A实习时编写的病毒防范工具，让本单位在遇到大型病毒袭击时毫发无损。这让他轻松地获得了本公司的网络安全主管职位。

(2) 小B配置的内部安全防火墙，为公司节约了大笔开支。由此，也得到了老板的赏识，并被提拔为技术部经理。

(3) 小C对数据安全的认识不够，在操作系统出现故障之前未进行有效的安全防范。在一场大型病毒攻击来临之时，导致公司积累数年的数据尽失，公司损失惨重，业务开展严重受阻。小C面临着公司经理的严重质疑。

(4) 小D开发的网站，因为对SQL注入代码防范不力，导致网站被黑，让领导汇报工作时颜面尽失。领导没面子，小D的日子也更加难过了。

……

类似的例子不胜枚举。网络安全就像一只无形的手，其力量如同世界杯期间的章鱼哥保罗，时时刻刻影响着我们的未来生活。你可能会想，我是一个新手，可以成为网络高手吗？我是一个资深的程序员，我还需要了解网络安全吗？再或者，我已经是一名网络管理人员，怎样才能系统地掌握网络安全知识？这就是本书要回答的问题——怎样成为一个合格的网络安全员，并对我们的工作、生活产生积极的正面作用！网络安全与我们的关系如图1.1所示。


图1.1 网络安全与我们的关系

细细地罗列一下，影响网络安全的因素还是很多的。这些因素有些可能是有意的，也可能是无意的；可能是人为的，也可能是非人为的；还可能是外来黑客或内部人员(包括信息系统的管理者、使用者和决策者)对网络系统资源的非法使用等，具体到准内部人员(包括信息系统的开发者、维护者等)、特殊身份人员(具有特殊身份的人，比如审计人员、稽查人员、记者等)、外部黑客或小组、竞争对手、网络恐怖组织、军事组织或国家组织等。细细一想，任何人都可能成为网络安全的受害者，也可能是网络攻击的实施者。下面来看看一张网络安全威胁的图片，如图1.2所示。

从这个图片可以看出，网络安全威胁包括了网络连接威胁、物理威胁、身份鉴别威胁、恶意程序、系统漏洞等。而每一个大类下面，又可以分为更多的细致小类，如图1.3所示。比如，网络连接威胁可能包括冒名顶替、窃听数据、拨号连接等；物理威胁可能包括偷窃设备、硬件回收、商业间谍、伪造证件等；身份鉴别威胁包括利用算法漏洞、猜解口令、利用软件破解密

码等；恶意程序包括病毒、木马、逻辑炸弹等；系统漏洞包括操作系统漏洞、应用软件漏洞等。每一个都与我们每个人息息相关。

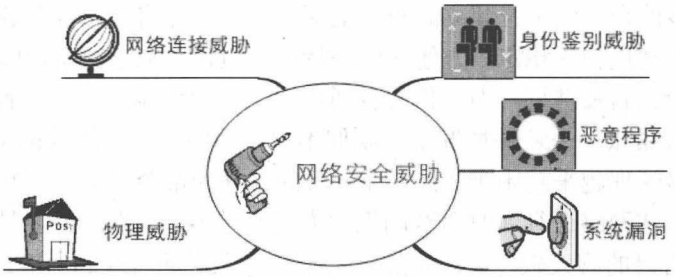



图 1.2　网络中的安全威胁

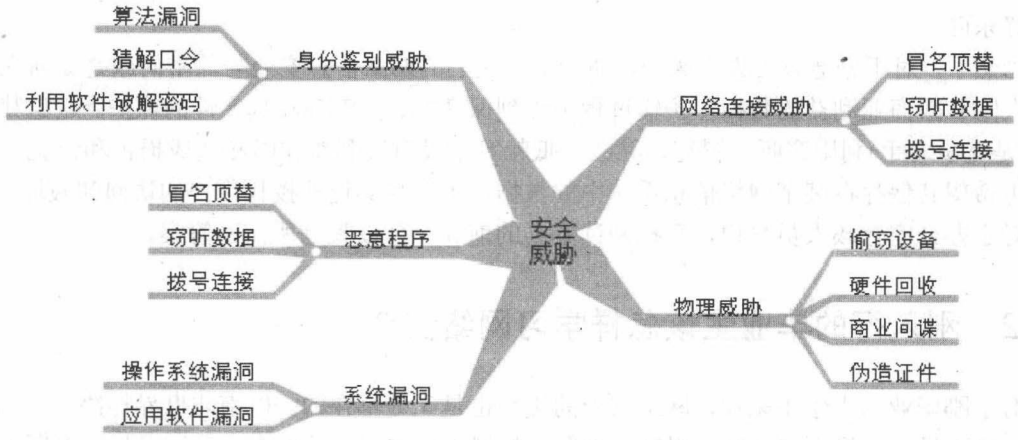



图 1.3　对网络安全威胁的细分

通过上面的场景介绍，我们可以初步了解网络安全的含义。如何更有效地保护重要的信息数据、提高计算机网络系统的安全性已经成为所有计算机网络应用必须考虑和必须解决的一个重要问题。

这里给出一个网络安全的定义。所谓网络安全，是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，确保系统能连续、可靠、正常地运行，网络服务不中断。

网络信息安全与保密是一个涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的边缘性综合学科。从广义来说，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。

## 1.2　从黑客、网管、程序员到 CTO：我们关心什么

网络技术的发展日新月异，从黑客、网管、程序员到 CTO，我们关心什么样的网络安全话题呢？下面来逐一说明。

### 1.2.1 办公室行政人员也要懂网络安全

现在，越来越多的企事业单位建立起自己的局域网络，并将公司内部的信息在局域网中共享。虽然局域网有着速度快、稳定、方便灵活等特性，但是其缺乏安全保障的结构却使其成为病毒肆虐、资料外泄的首要薄弱环节。作为普通用户，我们可能经常会碰到类似情况：办公室空间拥挤、单位资源紧张……这种情况下，我们不得不面临公用网络上的数据安全问题。

在办公室，网络管理越来越困难，员工在上班的时候经常会进行一些与工作无关的网络行为，利用公司的电脑和网络进行即时语音聊天的人越来越多。现在，许多员工上班打开电脑的第一件事就是挂上自己的聊天软件，还有的员工干脆在上班的时候利用 BT 软件或者其他的一些下载工具下载电影，一些受黑客入侵的网站在被访问的时候也将木马或者病毒植入了浏览者的电脑。这样，公司的网络时时刻刻都处在崩溃的边缘，公司的商业机密更成了黑客们拿来挣钱的好东西。

当然了，对于普通办公人员来说，他们最为关心的网络信息安全与保密问题是如何保证涉及个人隐私或商业利益的数据在传输过程中受到保密性、完整性和真实性的保护。避免其他人(特别是竞争对手)利用窃听、冒充、篡改、抵赖等手段对其利益和隐私造成损害和侵犯，同时用户也希望其保存在某个网络信息系统中的数据，不会受其他非授权用户的访问和破坏。

对于办公室行政人员来说，直接阅读本书的前 3 章可以找到所需的答案。

### 1.2.2 刚入行的毕业生该怎样学习网络安全

对于刚毕业的大学生来说，网络安全的影响也是无处不在的。以南非世界杯决赛为例，荷兰、西班牙最后一役上演之时，黑客也把罪恶的黑手伸向了球迷朋友。决赛当日，以所谓提供“2010 年南非世界杯决赛预测”、“世界杯博彩”服务的欺诈网址，包含了大量的恶性欺诈内容，用户在未开启专业安全工具的状态下盲目点击，将面临严重安全威胁。这就是典型的“钓鱼式攻击”。网络生活色彩斑斓，初入行的大学生也面临着诸多诱惑，在上网浏览相关网站、搜索资讯、观看视频、下载相关文件和通过相关社区、微博、博客进行互动时，一不小心，也许你就中招了。

初入行的大学生，或者平时对于电脑操作仅限于聊聊天、打打字、上上网的朋友，就得适当扩大自己的知识面了。例如，“蠕虫”、“防火墙”、“木马”、“黑客”、“QQ 尾巴”、“流氓软件”、“恶意程序”、“黑客视频”这些热门的关键词，尽管耳濡目染，但碰到这些问题的时候，要是能将这些热门词汇的来龙去脉说清楚，还真得下一番工夫了。

如果对自己的职业有更高层次的规划，网络安全将是这个职业规划的起点。以网络安全的兴趣为起点，你可以尝试去成为能够设计和实现多层次网络安全的网络管理员、网络安全工程师，定位于具有深度网络安全防御的技术管理人员、网络系统集成工程师，乃至成为企业网络安全官(Corporate Security Officer)。当然，你现在首先要做的，就是培养自己的兴趣。

如果你是一名初入行的毕业生，阅读本书的前 5 章可以找到答案。如果你发现自己的兴趣更广泛，比如对网络编程更加感兴趣，你可以在本书的后几章找到答案。

## 1.2.3　优秀网络管理员应该具备哪些安全知识

网管与黑客既是矛盾的，又有着千丝万缕的联系。从网络运行和管理者角度来说，最为关心的网络信息安全与保密问题是如何保护和控制其他人对本地网络信息的访问、读写等操作。比如，避免出现“陷门”、病毒、非法存取、拒绝服务、网络资源非法占用和非法控制等现象，制止和防御网络“黑客”的攻击。要防范黑客，首先必须了解黑客。但是，防范黑客攻击并不是网管生活的全部。在这里，网管是一个职业，它具有养家糊口的作用，并能够帮助我们成就一番事业。

国内的信息安全人才可称是“奇货可居”，近几年，在所有 IT 职业中，信息安全类工程师逐步成为行业内的薪资之冠。现有的比较知名的有：中国信息安全产品测评认证中心推出的 CISP 和原信息产业部国家信息化工程师认证考试管理中心的 NCSE。这些考试虽然不如国际市场那样成熟，但有越来越热的趋势。下面，我们来看看几则典型的安全招聘。

**招聘一：以下是天融信(http://www.topsec.com.cn)公司关于安全服务工程师的要求。**

岗位职责：

- 针对网络架构，建议合理的网络安全方案及实施办法。
- 定期进行安全扫描和模拟攻击，分析扫描结果和入侵记录，查找安全漏洞，为网络工程师、操作系统管理员提供安全指导和漏洞修复建议，并督促实施。
- 定期检查防火墙的安全策略及相应配置，提高安全级别。
- 定期检查、分析操作系统的安全漏洞，协助操作系统管理员及时进行应用系统及软件的升级或修补。
- 制定账号开放、口令设置及周期性更新原则，便于网络工程师、操作系统管理员保障账号安全；在可能情况下，采用一次性口令验证机制。
- 定期举办网络安全培训和讲座，讲授安全知识和最新安全问题，以提高网络工程师、操作系统管理员的安全意识。
- 对每次安全事故要进行总结分析，做出书面总结报告；每周/月进行网络安全运行分析、评估，提出改进方案。

任职要求：

- 有 Unix/NT 系统知识经验，能熟练使用 Unix/NT 系统平台下的各种应用系统，如 MSSQL、Oracle、Exchange、Lotus 等，有 DBA、CCNP、CCIE、CISP、CISSP、SUN 等认证等优先考虑。
- 精通 Oracle + Solaris 架构的安全配置，安全优化。
- 有 3 年 IT 行业经验或者 2 年以上安全服务工作经验，有 1 年以上防火墙工作经验者优先考虑。
- 语言表达能力较好，仪表端庄。

**招聘二：华为公司 IT 类的信息安全工程师招聘要求。**

职责：

- 信息安全技术体系的实施管理、负责信息安全基础设施建设。

- 负责信息安全领域的技术研究，制定和维护相关技术规范、标准。
- 负责网络、系统、数据库、应用等的安全风险评估和改进。

职位要求：

- 有 3 年以上信息安全相关工作经验。
- 精通计算机与网络安全技术，熟悉密码学、Unix/NT 等操作系统，熟悉网络原理。
- 精通安全产品和技术，包括防火墙、防病毒、IDS、PKI、攻防技术等。
- 有一定的开发能力和经验。
- 熟悉 ISO 17799 等安全管理标准。

类似的招聘还有很多，这也反映了当前安全行业的就业现状。可见，现在的企业对网管的要求越来越高，除了懂得基本的网络设备管理，还要具有一定的开发能力和经验；除了懂得 Windows 系统管理，还要懂得 Unix/Linux 操作系统管理；除了懂得网络管理知识，还要了解黑客。本书在章节的编排上，充分考虑行业的安全要求，循序渐进地进行规划，在前 8 章阅读过程中，你可以找到自己想要的答案。

### 1.2.4 我是一个想做出一番事业的黑客

黑客让人艳羡。当有“世界头号电脑黑客”之称的天才黑客凯文·米特尼克被克林顿总统邀请到白宫共商网络安全大计时，美国的一本著名周刊曾对黑客进行了这样的描述：“他旁若无人地站在白宫走廊的一角，目光深邃。一台笔记本电脑与他寸步不离，他不时在键盘上敲下某些神秘的指令……”。你也许不是一名资深的黑客，因为一名资深的黑客往往都有宽广的知识面。

从事黑客活动的经历，往往是电脑行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黑客。只是到后来，少数怀着不良的企图利用由非法手段获得的系统访问权去闯入远程机器系统、破坏重要数据或为了自己的私利而制造麻烦的具有恶意行为特征的人逐渐玷污了“黑客”的名声，“黑客”才逐渐演变成入侵者、破坏者的代名词。在这里，我们假设你是一名天马行空的黑客。

你可能是好奇的。顶多你只是在追求技术上的精进，只在好奇心驱使下进行一些并无恶意的攻击，以不正当侵入为手段找出网络漏洞，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修补网络错误，以防止损失扩大。

你可能是恶作剧的。一个偶然的不爽的经历，让你决定闯入他人网站，以篡改、更换网站信息或者删除该网站的全部内容，并在被攻击的网站上公布自己的绰号。这样做的目的，可能是在技术上寻求刺激，也可能是炫耀自己的网络攻击能力。

你也可能是隐秘的。你的性格决定了自己喜欢深深地隐藏起来，然后再以匿名身份从暗处实施主动网络攻击；有时干脆冒充网络合法用户，通过正常渠道侵入网络后再进行攻击。你的职业决定了你可能是一名程序员，也可能是一名技艺高超的网络管理员。可以这样形容你：技术高超，行踪无定，攻击性强。

你还可能是一颗定时炸弹，因为你极具破坏性。在市场化的经济社会中，为了达到某种目的，你可能会通过在网络上设置陷阱，或事先在生产或网络维护软件内置入逻辑炸弹或后门程序，在特定的时间或特定条件下，干扰网络正常运行，或者获得自己想要的东西。

当然了，你还可能是一颗重磅炸弹。你拥有高超的黑客技术去干扰竞争对手的商业行为，或者拥有敏锐的嗅觉去窃取、调阅和篡改高度敏感资料。可以猜测，你的职业可能是网络管理员，也可能是程序开发者。在本书的前 10 章，你可以找到所需要的答案。因为你需要融入这个社会，需要在实现自己兴趣的同时，得到社会的承认。

### 1.2.5　优秀的程序员也要懂网络安全

细数如今的软件项目，随着进入门槛的降低，同等规模的项目总价在下降，软件人员的收入自然会大幅度下降。如今，新招的大学本科生的月薪可能只有 1000 元。而普通的装修工人日收入 200 元还觉得低。难怪有人将程序员誉为“IT 农民工”呢！是什么原因造成程序员地位和收入的逐步走低？

究其原因，无外乎以下几点：编程技术进步使得编程门槛降低，程序员人数不断在增加；随着专业化程度提高，许多软件企业专注于一个行业，程序很难有新意，大部分就是复制了事，这样技能局限的程序员不可有太高的价格；项目价格低，反映在程序员身上的价值就很低。而且，有些技术工作只注重结果而不注重过程和质量，导致技术高、质量好的程序员得不到额外的鼓励，也降低了程序员工作的含金量。

这些情况也引起了我们的深思：一个优秀程序员的出路在哪里？

有些老板为了节约成本，常常会一人多用。比如，老板会让你承担网络安全工程师的职责，或者是当网站信息管理员。在这种趋势下，谁的综合知识更全面，上升的空间也就越大。

也许你会纳闷：我是一名高级程序员，我的安全知识已经足够了。可是，你还是会碰到这样的情况。老板觉得你很厉害，他会让你代理安全系统工程师、高级网络管理员，或者在某一天让你直接成为公司的 CTO。这个时候，你更需要有全面驾驭网络安全业务的能力。当然，你也可能做一辈子的程序员，与网管永远没有交集，这种情况另当别论。

优秀的程序员不但要求新、更要求精，除了在编程方面成为专家和高手，还需要有驾驭全局的能力。这里，我们更需要关注的是这样一个群体。他们懂一点点 JavaScript 的知识，会编写 SQL Server 下的存储过程、触发器，能够使用 C#开发带后台管理的小型企业网站。再或者，看过几本设计模式的图书，但实际操作中很难变通自己已形成的思路。这些程序员面临着许多困惑：比如，新的知识和概念层出不穷，再找份网站开发的工作好像没太大意思；年龄加大的情况下家庭的压力也在加大，将来又该何去何从？

其实，程序员的网络安全转型很有优势，在本书的前 10 章中可以找到答案。

### 1.2.6　成为 CTO，让梦想的距离更近一些

有梦想，有行动，肯定会有结果。暂时做不了 CEO，我们却可以发挥自己的特长，以最快的速度成长为 CTO！CTO(首席技术官)即企业内负责技术的最高负责人。这个名称在 1980 年从美国开始时兴，起源于很多做研究的大公司，如 General Electric、AT&T、ALCOA，主要责任是将科学研究成果转化成为盈利产品。

从网络在中国扎根的第一天开始，你可能做过黑客，也做过网管；你可能做过程序员，也做过系统分析师。或者，你就是一名网络安全爱好者。如果你并不甘心只做一个技术高手，现