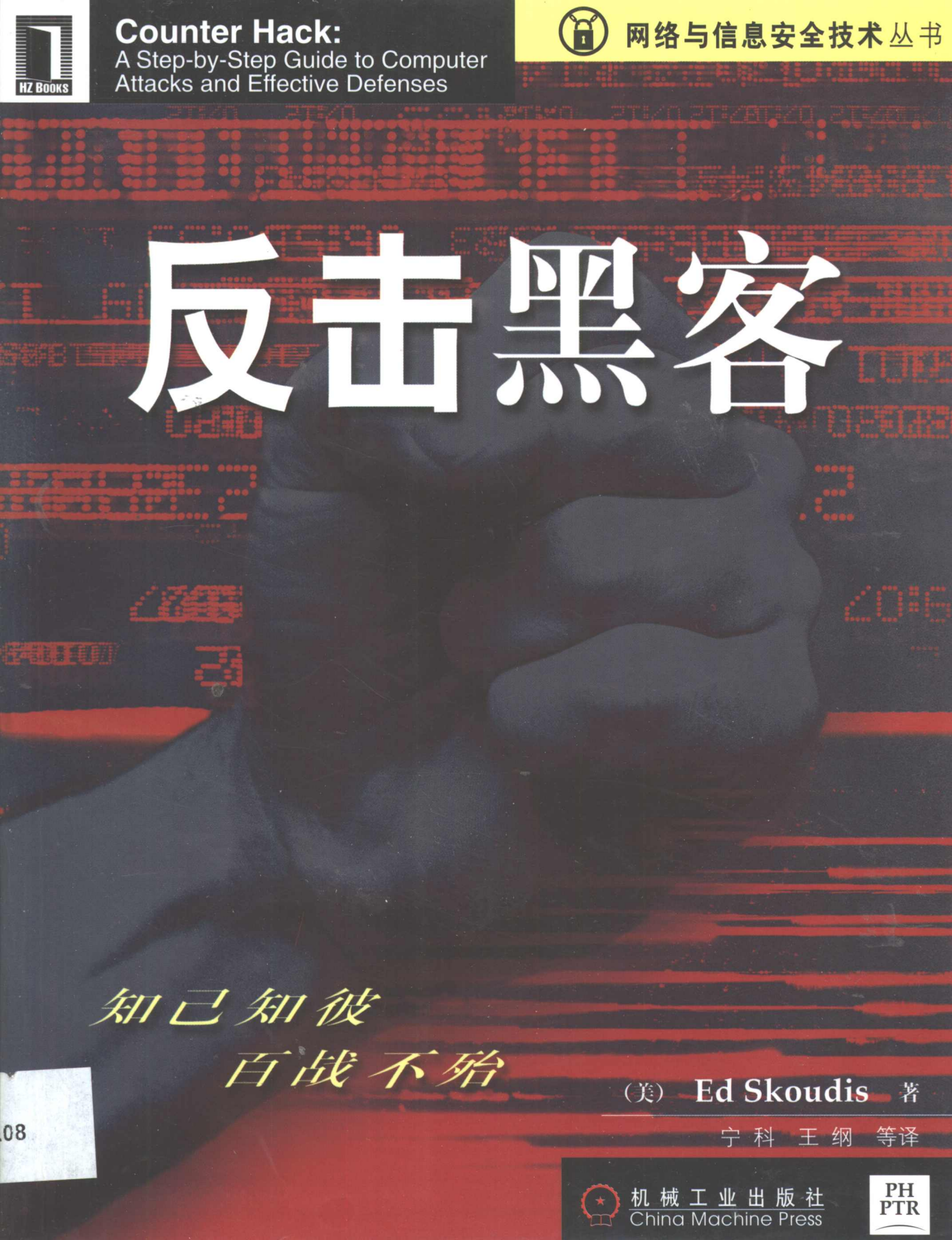
HZ BOOKS
Counter Hack:
A Step-by-Step Guide to Computer Attacks and Effective Defenses
网络与信息安全技术丛书
反击黑客
知己知彼
百战不殆
(美) Ed Skoudis 著
宁科 王纲 等译
机械工业出版社
China Machine Press
PH
PTR

网络与信息安全技术丛书

反击黑客

（美） Ed Skoudis 著

宁 科 王 纲 等译

前导工作室 审校

机械工业出版社
China Machine Press

本书详细介绍防御黑客攻击的技术与方法。主要内容包括：目前网络安全状况的分析、组网技术概述、UNIX 与 Windows 系统结构分析与潜在漏洞介绍、常见黑客工具介绍、各种攻击手段与相应防御策略、攻击的 5 个步骤的详细分析，在最后一章中还给出了三个实际的综合攻击与相应防御实例。

本书由浅入深、循序渐进、涵盖面广，且对问题分析得非常透彻，有助于网络和系统管理员保护计算机系统。

本书版权登记号：图字：01 - 2001 - 3877

图书在版编目（CIP）数据

反击黑客/（美）斯科迪什（Skoudis，E.）著；宁科等译．-北京：机械工业出版社，2002.2

（网络与信息安全技术丛书）

书名原文：Counter Hack: A Step - by - Step Guide to Computer Attacks and Effective Defenses

ISBN 7 - 111 - 09751 - 3

Ⅰ.反… Ⅱ.①斯…②宁… 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（2001）第 097299 号

机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码 100037）

责任编辑：傅仕诤 张鸿斌

北京牛山世兴印刷厂印刷·新华书店北京发行所发行

2002 年 2 月第 1 版第 1 次印刷

787mm × 1092mm1/16·22.25 印张

印数：0 001 - 5 000 册

定价：38.00 元

译 者 序

虽然随着网络的日益普及，没有接触 Internet 的人已经很少，但是对于许多人来说，黑客与破解技术还是新词，充满了神秘感。那些媒体所大力报道的网络安全事件与所谓的黑客天才人物的出现，似乎对于我们普通人来说是很遥远的事。但是我们不要过于乐观，危险就发生在我们周围，黑客也不是什么了不起的人物，他们就在我们的身边。不要说那些金融公司、著名商业网站、政府网络经常遭受的计算机攻击事件，就考虑当有人做恶作剧，盗取你的 QQ 号码密码、当“红色代码”侵袭你的计算机时，你是不是觉得非常可恶？因为是普通用户，所以这还不致于令你痛苦，但是如果有人远程控制你的计算机，将你的硬盘格式化，而你刚好在上面有个写了几个月的文档，我想你一定会欲哭无泪。你可能会想，谁会那么无聊，如果你这么想，那你就错了。事实上，除了那些有特定目的的黑客外，还有大量的想显示自己才能与寻找乐子的人，他们也许会令一位没有半点计算机安全意识的人痛心疾首。

正如本书第 1 章里所说的，本书的特色在于“是一本关于计算机攻击与防御的百科全书，而不是一本字典”，也就是说，本书不是类似索引的介绍，而是对原理的系统阐释。“知己知彼，百战不殆”，本书侧重于对攻击者所采用的技术和工具的分析，并适当地提出所采取的策略，因为虽然对手所采用的技术也许很复杂，但防御的方法却很简单——只要你理解了其中的奥秘。如果你仔细地将本书消化了，你一定可以成为一位出色的黑客，但是作者不希望这样，因为那是违背道德与法律的。相反，你也许可以成为一位计算机网络安全专家，至少不会被那些喜欢恶作剧的人所干扰。

我们相信，本书能够帮助那些被网络安全所困扰的人，也是所有普通用户通向计算机安全领域的大门。当你阅读完本书时，对计算机黑客和各种貌似神秘的网络攻击事件不再感到神秘，你的计算机系统也不会仍然脆弱。

全书由宁科、王纲、赵娟、桑茂栋、李宏杰、赵耀峰、商超、胡敏、朱华敏、陈永宏、孙正宁、李如豹、王刚、叶小松、李林、张巧丽、蒋华、施平安、张勇、鲁金贵、邓勃、钟明辉、董金云、刘芬等进行翻译，前导工作室全体工作人员共同完成了本书的翻译、录排、校对等工作。尽管准确及时是我们的首要追求目标，但由于时间仓促，且译者的水平有限，在翻译过程中难免会出现一些错误，请读者批评指正。

但愿我们的工作会给您带来些许助益，这是身处浮躁中的我们的最大幸福！

2001 年 10 月

序　言

很难想像，这个世界没有 Internet 将会是什么样子。现在，我们在 Internet 上操作银行账户、访问健康记录、得到驾驶方向、与朋友交谈和购物，这些我们都认为是当然的。自从 Internet 联系着客户，有些公司没有它就不能生存。

但是 Internet 不仅仅是使商业者访问客户、医生访问健康记录和朋友互相访问，它还使黑客访问你的系统和你期望达到的系统。

该系统是在非常纯洁的时代建立的，那个时候假定一个为诚实的研究者分享信息而建立的大学环境，或一个在家里用于字处理或玩游戏的个人计算机。Internet ——伴随着人们为开玩笑或宣扬政治观点的目的而攻击系统的想法——发展得如此迅速，以致于该系统来不及发展成应该成为的完全稳固的系统。以此同时，它需要持续地努力，以赶在攻击者的前头。

本书作者曾经宣称站点无希望，然后到佛蒙特养兔子。但是，当饲养几千只兔子变得很容易时，Ed Skoudis 恢复了无穷的力量、热情和乐观。本书反映了他的性格。他使我们相信，我们能赢得这场战斗的胜利。我们必须赢，他将帮助我们。

—— Radia Perlman，Sun Microsystems 公司杰出的工程师

前　言

我的电话响了。我睁开睡意朦胧的眼睛，看看时钟。哎呀！元旦节早晨4点。不用说，我昨晚睡得很少。

我抓起电话筒，听到我的伙伴Fred的狂乱的声音。Fred是一个中等规模的Internet服务提供商的安全管理员，他经常打电话问我关于安全的各种问题。

“我们被‘黑’了！”Fred嚷道，声音在早晨的这个时候显得非常大。

我揉揉眼睛，试图弄清楚是怎么一回事。

“你怎么知道他们闯入了？他们做了些什么？”我问。

Fred回答：“他们篡改了一些Web页。太糟糕了，Ed。我的老板会生气的！”

我问：“他们怎样闯入的？你检查了日志吗？”

Fred结结巴巴地说：“嗯，我没有做很多日志，因为它会减慢性能。我只在两台计算机上做了些日志。可是，在那些我做了日志的系统上，攻击者清除了日志文件。”

“你从操作系统商那里申请了对你的计算机进行最新的安全修补吗？”我问，试图更多地了解Fred的安全态度。

Fred犹豫地回答：“我们每隔3个月申请安全补丁。上一次我们申请补丁的时间是……两个半月之前。”

我抓了一下疼痛的头，说：“上个星期发布了两个主要的缓冲区溢出攻击，你可能中招了。他们安装了任何RootKit（启动工具）吗？你检查了计算机系统上的重要文件的一致性吗？”

“你知道，我正打算安装诸如Tripwire的软件，但从没有付诸实施”Fred承认。

我暗自叹息，说：“OK。保持冷静。我会马上过去，这样我们可以开始分析问题。”

你肯定不想遇到与Fred类似的情况。我想尽量减少在元旦节的早晨4点接到电话的次数。我改变了Fred的名字，以保护他的名声，但这种情况确实发生过。Fred的组织的问题出在没有实施一些基本的安全控制，当攻击者来敲门的时候，他们不得不花费大量资金。以我的经验，许多组织发现他们自己处于未准备信息安全的相同的状态。

但是情况超出这些安全基础。即使你实现了所有在上面的Fred故事里所讨论的控制，仍有各种其他的提示和技巧，你可以使用它们来保卫你的系统。当然，你可以应用安全补丁，使用文件完整性检查工具和拥有足够的日志，但是你最近查找了不安全的调制解调器吗？或者，怎样在重要的网络网段里的交换机上激活端口级别的安全性，以防止强大的、新活跃的嗅探攻击？今天，你考虑过通过实施不可执行的堆栈来防止现在最普遍的一种攻击类型——基于堆栈的缓冲区溢出吗？你准备了内核级的RootKit吗？如果你想深入学习这些主题和更多这方面的知识，请继续读下去。

正如我们在本书中将看到的，每天都在发生威力日益增加的计算机攻击。为建立好的防御，你必须了解对手的攻击技术。在我作为一位系统渗透测试员、事件反应组员和信息安全工

程师的职业生涯中，我见过许多类型的攻击，从无知的新手进行的简单扫描到可耻的地下组织发起的有效攻击。本书立足于来自现实世界攻击的普通和最具破坏力的元素。与此同时，将具体地建议你怎样正确地避免对手所带来的麻烦。我们将详细分析计算机攻击者的活动过程，查看过程的每一步，这样我们就能实施深度防御。

本书的读者对象是系统管理员、网络管理员和安全人员，以及其他想知道计算机攻击者怎样施魔法和怎样制止他们的人。本书列出的攻击和防御技术，应用于现在使用计算机和网络的所有类型的组织，包括从小到大各种规模的企业和服务提供商。

计算机攻击者以非常奇妙的方式分享关于怎样攻击你的系统的信息。他们传播关于受害者的信息效率非常高。我希望本书通过提出实际的建议来改变现状，这些建议是关于怎样保护好你的计算机系统，以免遭坏人的攻击。通过应用本书的防御技术，你能极大地提高计算机安全，在下一个元旦节里我们都能睡好觉。

目　录

第1章 引 言

每一天都有计算机攻击的发生。简单地将一台无害的计算机连接到 Internet，则每天都会有一些人试图刺探该机器 3 次、5 次或 12 次。即使你的计算机没有任何可引起关注的通告或链路，攻击者也会不断地扫描它，以寻找脆弱的受害者。如果计算机用于实际的营业目的，如商业的、教育的、非赢利的或军方站点，那么它将受到更多攻击者的注意。

这些攻击当中的许多只是为了寻找一个系统防御体系中的漏洞而在进行扫描。另外一些是真正熟练的计算机非法闯入者，从最近的新闻标题中可以看到它们越来越频繁地出现。在刚过去的一年里，大多数银行成了攻击者的牺牲品。这些攻击者能查看客户银行账号的详细信息。攻击者曾从 e 商业站点偷走大量信用卡号，而后常常以不公布客户的信用卡信息来勒索 e 商业公司。由于大型数据包泛滥，许多在线贸易公司、新闻单位和 e 商业站点被暂时关闭，这导致由于客户转向其他提供源而使公司蒙受财政损失，从受害者的资本市场中消去了数十亿美元。一个大型的基于 U.S. 的软件开发公司发现攻击者闯入它的网络，盗走了其流行产品将发布版本的源代码。这样的故事还在继续。

本书的目的是说明这些攻击中有多少是可预防的，以使你能保护好你的计算机，使它免遭围攻。通过详细地探讨攻击者使用的技术，我们能学会怎样保护系统，使攻击者无法入侵。

1.1 计算机世界和攻击的黄金时代

在过去的几十年中，我们的社会很快变得非常依赖计算机技术。我们控制了整个文明，并将它负载到数字计算机上。我们的系统负责存储敏感的医学信息、导航环行世界的飞机、管理几乎所有的金融事物、规划食物分配，甚至传递情书。当我还是一个孩子的时候，计算机是提供给那些愚昧的人的，而大部分人都回避它。十年前，Internet 是研究人员和学生的避难所。现在，大多数人因为商务和个人用途而成天盯着计算机屏幕和打电话，这些技术主宰了我们的新闻标题和经济。

我相信你已经注意到，计算机和网络背后的基本技术中存在许多漏洞。当然，也存在许多非直观的用户界面和频繁的计算机事故。除了这些容易观察到的问题以外，在基本的操作系统、应用程序和协议的设计与实现中还存在一些基本的漏洞。通过暗中利用这些漏洞，攻击者能盗走数据、控制系统或者进行报复性破坏。

事实上，我们建立了一个本质上能被攻击的世界。伴随着我们极大地依赖于计算机和在大多数系统中发现大量的漏洞，现在是攻击的黄金时代。每一天都在计算机技术里发现有新的漏洞，它们被整个快速发展的计算机地下组织所共享。通过在自己舒服的家中建立一个实验室，攻击者和安全研究员能创建大公司、政府机构或军方策划部使用的计算机平台的小型拷贝。使用同样的操作系统、路由器和其他工具作为他们的主要目标，通过侦察系统新的漏洞，攻击者能锻炼他们的技术和发现新的可利用的漏洞。

计算机技术继续渗入我们生活的每个角落。公司现在正通过网络连接售卖电子毛毯，因此你能使床温暖、从你的房间到整个地球都温暖舒适。Andy Grove（Intel 主席）经常讨论这样一个未来：你的冰箱将有 Internet 连接，因此当你外出时，它能呼叫本地食品店，订购更多的牛奶。Scott McNealy（Sun Microsystems 的 CEO）谈论有网络连接的电灯泡（是的，电灯泡!）。当一个灯泡要烧坏的时候，它们能呼叫电灯泡公司。这样，利用到将坏的灯泡地址的地图，新的灯泡能够到达，并及时地进行更换。在最近的将来，汽车将有无线网络连接，在你驾驶期间能支持地图下载、远程故障排除和收发电子邮件。那么，所有这些即将到来的未来技术由什么来实现？互相连接在一起的计算机和网络。

伴随着这些进步，当前攻击的黄金时代对于攻击者来说会得到更多的黄金。考虑这样的情形：现在，一个攻击者通过 Internet 连接，利用扫描方式试图闯入你的计算机。在不远的将来，当你正行驶在街道上时，一些人可能试图攻击你启用网络的汽车。你听到了汽车碰撞的声音吗？准备好应付汽车攻击的时代吧。

1.2　为什么要写这本书

如果你了解敌人和自己，那么你不必害怕上百次的战斗结果。

如果你了解自己但不了解敌人，那么每赢得一次胜利，你也将遭受一次失败。

如果你即不了解敌人，也不了解自己，那么你将在每次战斗中都失败。

—— Sun Tzu，《战争的艺术》，Lionel Giles 翻译和注释（Gutenberg 工程的一部分）

“天啊!”你可能会想，“为什么写一本关于黑客攻击的书？你将鼓励他们攻击!”。我尊重你的意见，但不幸的是，这种逻辑有一些漏洞。让我们面对它——怀有恶意的攻击者拥有所有的信息，这些信息是他们需要用来做所有肮脏的事的。如果他们现在没有这些信息，他们会很容易地在 Internet 上，通过正如本书的总结章节里所描述的致力于黑客攻击的各种 Web 站点、邮件列表和新闻组等渠道得到它。有经验的攻击者经常有选择地与新的攻击者分享信息，使他们开始干这个行当。事实上，在计算机地下组织里，攻击者之间的交流渠道往往比计算机专家之间的还好。这本书将使事情变得更平等些。

在本书中，我的目的不是培养一群倾向于统治世界的没教养的黑客。这本书的重点是关于防御。为实施有效的防御，我们必须了解对手所使用的攻击工具。通过了解这些工具怎样真正地工作和了解它们能做什么，我们不仅能更好地明白防御的要求，而且能更好地理解怎样应用正确的防御技术。

此书写给系统管理员、安全维护人员和网络管理员，他们的工作要求他们保护系统、防御攻击。另外，其他的想知道攻击者怎样攻击和对系统防御攻击的技术好奇的人也能从中得到益处。此书包括给一些人的实际的建议，这些人必须照看和维护好系统，使系统正常运转，免受坏人攻击。理解了这些技术，我们可以创建一个环境，在这个环境里有效的防御技术是普通的，而不是特例。正如 Sun Tzu 所说，你必须了解敌人的能力以及你自己的。对于本书中描述的每种攻击技术，也相应地描述了实际的防御技术。你可以利用这些防御技术来测试安全能力，以了解你怎样积累这些知识。在策略、程序和系统薄弱的地方，你能对敌人实施正确的防御。这就是本书所全部讨论的：了解攻击者做什么，以使我们能保卫自己。

1.2.1 为什么讲述这些具体的工具和技术

如今，存在数千种可利用的不同的计算机和网络攻击工具和数万种不同的可利用的技术。为讲述如此多的可能的攻击，本书重点放在一些特定类型的攻击工具和技术上，讨论使用最广泛的和最具破坏力的各种类型的工具。例如，有几百个可利用的工具能使攻击者捕捉和分析网络流量，如一种被称为嗅探（sniffing）的程序。我们现在可利用的每个不描述单独的嗅探工具，只详细分析在嗅探类型里最强大和广泛使用的工具，包括 Dug Song 的 Dsniff。通过了解和正确地防御 Dsniff，你将学会如何保护你的网络，使它免遭所有的嗅探攻击。同样地，通过学习其他类型里最强大的工具，我们能设计和实现最有效的防御。

1.2.2 本书有什么不同

近几年，几本涵盖攻击者和他们的技术为主题的书已经出版，其中的一些写得很好，对于理解攻击机理和有效防御很有作用。那为什么还要写另一本关于这些主题的书呢？本书集中于几种不同的方式，包括：

- **更像一本百科全书，而不是一本字典**。这种类型的其他的书介绍数千种工具，对每个工具都有一段或一页的文字介绍。本书的重点在于深入理解每种类型的工具。因此，其他的书像无根据的攻击工具和防御的字典，而本书的目标是更像一本百科全书。通过更详细地介绍每类攻击工具，我们能最好地理解正确的防御。
- **描述分阶段的攻击视图**。其他的书描述攻击者怎样获得对系统的访问视图，集中于攻击的渗透部分。虽然获得访问是大部分攻击的非常重要的一步，但是我们的对手除了简单地获得访问以外还将做更多的事。一旦获得访问，大多数攻击者操纵系统，以维持访问，并且努力擦除他们的踪迹。通过描述一个攻击的分阶段的方法，本书介绍端到端攻击顺序，因此我们能介绍在围攻的每个阶段上的防御。大部分攻击遵循一个指导方针，包括侦察、扫描、获得访问、维持访问和擦除踪迹。本书描述每个阶段。
- **介绍工具怎样一起使用的实例**。攻击者使用的工具有点像建筑物模块；每一个都有一个特定的（但有限的）目的。只有通过明白攻击者怎样利用模块实施完整的攻击，我们才能理解怎样最好地保护自己。熟练的攻击者采用工具的各个建筑模块，以创造性的方式将它们结合起来，设计出非常优秀的攻击。本书描述怎样利用一个攻击的各阶段视图来一起使用一些工具。另外，为理解系统，第 12 章（“将它们都放在一起”）描述了几个描述怎样一起使用这些工具的实例。
- **使用比方来阐述非明显的计算机概念**。贯穿于全书，我使用比方来阐述各种技术的工作机理。有一些比方可能比较低劣，但我希望它们使内容更有趣和更利于读者理解。

1.3 威胁——永远不要低估你的对手

那么，我们必须防御哪些攻击者呢？经常，当我们谈到计算机攻击者时，人们的脑海里浮现一幅场景：在父母的房子里，一个长满青春痘的十几岁的孩子坐在混乱的卧室里的计算机前，还一边吸吮着 Mountain Dew（山露）。一些人的这种想象降低了他们的防御意识，他们认

为“一个仅仅是长满青春痘的十几岁的孩子能做出多少破坏来?”。这种想法是错误的，至少有三个原因：

首先，以我的经验，许多年轻的攻击者有很好的皮肤，在上面发现不了一个青春痘。第二，也是更为重要的，许多孩子非常擅长于他们所做的，拥有熟练的技术和深层的判断力。当然，这群年轻人中的许多没有掌握大量的技能。然而，如果你的组织面对的是头发蓬乱的高水平的年轻攻击者，他们能对你的计算机做出一些巨大的破坏。不要因为有威胁的人小于 20 岁而松懈防御。

使你不能对十几岁的攻击者松懈防御的第三个原因可能是最重要的。对于大部分组织，你面临的是远比恶作剧的年轻人更可怕的人。你永远不要低估你的对手。不同的组织有不同的弱点暴露给潜在的有威胁的人。在现实中，攻击者来自不同年龄段，有不同的行动目的。除了年轻的攻击者以外，我们遇到发起攻击的外部有威胁的人包括：

- **竞争对手**：你的组织的竞争对手经常倾向于计算机攻击，以试图获得优势。这些攻击包括为获得关于你的未来计划的有趣的新闻而进行的低级侦察，或者深入渗透敏感的系统，以获得你未来策略的细节，或者是大量的拒绝服务式攻击，以阻止客户与你接触。
- **黑客政治家**：如果你的组织做了一些政治上敏感的事，则你可能成为黑客政治家的目标。这类攻击者试图闯入你的系统，宣扬一个关于社会问题的政治观点。黑客政治家可能改动你的 Web 站点，以显示他们的消息，使你的组织难堪，或者降低服务器的处理能力，使你的商务活动减慢。
- **有组织的罪犯**：如果你的组织处理资金（大部分组织都有类似的工作），则你的计算机结构可能成为有组织的犯罪的目标。这些攻击者可能正在寻找一个简单的方法，以获得钱、对他们的商务有用的信息，或用于其他恶意目的的系统访问。
- **恐怖主义者**：如果你的组织被认为是你的国家或世界的重要机构，你会面临来自恐怖主义者的电脑攻击。他们会在整个公司里传播恶意的程序，在敏感时间关闭所有的重要系统，或者导致潜在的危及生命的问题。
- **政府**：大部分政府感兴趣是在它们的环境上操作大量组织的活动。一些政府机构热衷于电脑攻击，以得到对支持法律条文的局部组织的访问和关于它们的信息，得到帮助本国公司与外国公司竞争的信息，甚至镇压叛国者。
- **“雇佣杀手”**：这种类型的攻击者偷取关于客户利益的信息或得到对他们的计算机系统的访问，以寻找生财的机会。这是在这个列表里其他外部有威胁的人当中的一种。

除了这些外部的人以外，记住，大部分的攻击来自内部的人，这些人将直接访问你的计算机系统作为他们的工作职责的一部分或一种商务关系。内部有威胁的人包括：

- **不满的员工**：因为他们可以进行高级别的访问、暴露组织的系统和在它里面得到培训，所以组织内自己的员工经常是计算机系统最频繁和有破坏力的攻击者。
- **客户**：不幸的是，客户有时变换他们的供应商，攻击提供商的计算机系统，以试图获得关于其他客户、变动价格的敏感信息，或者捣乱组织的数据。
- **供应商**：供应商有时攻击客户。在供应商网络上的一个恶意的员工可能以各种方式攻

击你的系统。

- **厂商**：厂商经常因为远程诊断、系统升级和管理而能完全访问系统。利用这种访问，他们不仅能攻击给予他们访问的系统，而且包括整个网络中的潜在的系统。
- **商务伙伴**：加入投机冒险、分享工程和其他商务关系常常需要将网络连接在一起和共享非常敏感的信息。处于连接在一起的网络上的任意的一个攻击者能发起对其他商务伙伴的攻击。安全性经常像是有着最脆弱连接的众所周知的链条。如果你的一个商务伙伴因为有比你低的安全位置而受一个外部攻击者的摆布，那么那个攻击者会通过一个商务伙伴的连接得到对你的网络的访问。
- **契约者、临时雇员和顾问**：过去的十年里的顾问工作使我深深感到，这种类型的内部人员可能特别有害。许多的组织并不像调查长期职工那样调查临时工的详细背景。这些临时工常常可以大量地访问系统和数据。即使出了问题，一些组织不能像对长期职工那样迅速和彻底地移除被临时工访问的账号。我曾看到这样的情况：长期职工的账号在隔离的早上就被关闭，而临时工的账号要拖延好几个月。

当然，这个列表里有威胁的人并不互相排斥。例如，一个有头脑的恐怖主义团体可能将某些人作为临时工打入你的组织，他们从内部获得对系统的访问，并且放置恶意程序。类似地，一个竞争者可能雇请有高技能的年轻攻击者作为“雇佣杀手”，以从一个组织的系统那里偷取特定的信息。他们之间的结合和互换没有限定的。

然而，正如不要低估所面对的有威胁的人那样，你也不要高估了他们。你不必花重金保障安全，防御那些对你的系统或信息没有兴趣的幽灵。没有人会在 1985 年造的破烂的货车上安装昂贵的汽车报警器。然而，在某些地区里，你肯定要锁住这样的汽车门，以防止人们用你的花费来驾驶取乐。你必须坐下来，仔细评估哪些有威胁的人会对你的组织图谋不轨，衡量必须保护的东西的有形和无形的价值，然后应用与这些有威胁的人以及你的系统和信息的价值相匹配的安全控制。

攻击者技能水平——从脚本小孩到杰出的人

在许多种类的计算机攻击者当中，技能水平变化很大。一些攻击者只有初级技能，他们不理解他们的工具如何真正地工作，而仅依赖于其他的人写的已打包的攻击工具。这样的攻击者被嘲笑为“脚本小孩（Script Kiddies）”。他们的技能基于运行更熟练的攻击者写的脚本和其他软件。他们还非常不成熟。脚本小孩经常无辨别地扫描 Internet 上很宽的范围，以寻找容易控制的受害者。通过摘取悬挂较低的果实，脚本小孩得到夸耀的权利和发起更高级进攻的基础。因为现在 Internet 上许多的主机自我保护的性能很差，所以即使是低水平的攻击者也能破坏世界上数十万的系统。现在在 Internet 上有大量的脚本小孩，他们的成长无疑处于国际性的范围。

除了这些简单的脚本小孩以外，我们常常研究有普通技能的攻击者，他们对某种操作系统非常精通。有适度的判断力。这些中级攻击者能导致目标组织的大量破坏。此外，计算机地下组织倾向于吸收有普通或高技能的攻击者与安全专家。通过他们发现计算机系统的漏洞，然后开发出针对已发现漏洞的和易于使用的破坏工具。他们有时在公众论坛里发布这些工具，例如