TURING

著名安全专家解密社会工程手法的权威著作
社会工程专家的精彩故事令你瞠目结舌
众多专业人士强力推荐，亚马逊读者一致好评

Social Engineering: The Art of Human Hacking

社会工程

[美] Christopher Hadnagy 著　陆道宏　杜娟　邱璟　译

安全体系中的人性漏洞

人民邮电出版社
POSTS & TELECOM PRESS

TURING

Social Engineering: The Art of Human Hacking

社会工程

[美] Christopher Hadnagy 著　陆道宏 杜娟 邱璟 译

安全体系中的人性漏洞

人民邮电出版社
北　京

图书在版编目（CIP）数据

社会工程 ：安全体系中的人性漏洞 /（美）海德纳吉（Hadnagy,C.）著 ；陆道宏，杜娟，邱璟译. — 北京：人民邮电出版社，2013.12
书名原文：Social engineering:the art of human hacking
ISBN 978-7-115-33538-8

Ⅰ. ①社… Ⅱ. ①海… ②陆… ③杜… ④邱… Ⅲ. ①信息安全 Ⅳ. ①TP309

中国版本图书馆CIP数据核字(2013)第263458号

内 容 提 要

本书首次从技术层面剖析和解密社会工程手法，从攻击者的视角详细介绍了社会工程的所有方面，包括诱导、伪装、心理影响和人际操纵等，并通过凯文·米特尼克等社会工程大师的真实故事和案例加以阐释，探讨了社会工程的奥秘。主要内容包括黑客、间谍和骗子所使用的欺骗手法，以及防止社会工程威胁的关键步骤。

本书适用于社会工程师、对社会工程及信息安全感兴趣的人。

◆ 著 [美] Christopher Hadnagy
译 陆道宏 杜 娟 邱 璟
责任编辑 李 瑛
执行编辑 卢秀丽
责任印制 焦志炜

◆ 人民邮电出版社出版发行 北京市丰台区成寿寺路11号
邮编 100164 电子邮件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
北京艺辉印刷有限公司印刷

◆ 开本：800×1000 1/16
印张：18.25
字数：430千字 2013年12月第1版
印数：1－3 500册 2013年12月北京第1次印刷
著作权合同登记号 图字：01-2012-3282号

定价：59.00元

读者服务热线：(010)51095186转600 印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京崇工商广字第0021号

站在巨人的肩上
Standing on Shoulders of Giants

www.ituring.com.cn

站在巨人的肩上

Standing on Shoulders of Giants

www.iturin g.com.cn

版权声明

谨以此书献给我美丽的妻子和可爱的家人。如果没有你们，我根本无法完成本书的写作。Mati，我对你的感激之情无以言表。

序

安全对内外部双方来说都是个难题。从内部来看，我们需要舒适感和安全感；从外部来看，窃贼、黑客和蓄意破坏者在不断寻找突破口。大部分人都觉得自己的家是安全的，直到有一天忽然发现自己被锁在了门外。我们的看法就会在刹那间改变，才明白原来安全漏洞是那么明显。

必须置身事外才能全面地理解安全，从本质上来说就是把自己作为一个局外人，尝试用其他方式来进入系统。问题是大部分人因为自信满满而对潜在的问题视而不见，觉得锁很好、门很厚、安全系统很高级，而且还有看门狗，就足以把大部分人“拒之门外”了。

我不属于这部分人。过去10年中，我比历史上任何人设的骗局都要多。我在赌场赢过庄家、伪造过体育赛事、操纵过拍卖、诱骗过他人交出心爱之物，也轻松侵入过几个号称坚不可破的安全系统。

我的工作就是在热门电视节目《骗术真相》（*The Real Hustle*）中曝光窃贼、说谎者和骗子要的各种伎俩。如果我做了罪犯的话，很可能会变得富有、名噪一时或者难逃一死——也许三者都会发生。人生的大部分时间，我都在研究各种欺骗方式，以便告诉公众他们是多么好骗。

每周，我都和亚历克西斯·康兰（Alexis Conran）一起设局骗人，而被骗的人对于自己身处骗局之中浑然不知。通过隐蔽的摄像头，我们向电视机前的观众演示怎样才能识破同样的骗局。

这种不同寻常的工作使我对罪犯的思维方式有着独到的理解。我逐渐成为一只批着狼皮的羊。以个人经验来看，不管事情看似多么不可能，几乎总会有一种巧妙的、意想不到的解决方法。

举个例子。我曾想证明自己不仅能轻而易举偷取一个女人的钱包，还能让她告诉我信用卡的

提款密码。BBC电视台认为这不可能。当我将这个想法提交给《骗术真相》栏目组，想做一期节目时，BBC台长的批示是“不可能发生”，然后将其退还给我。我们知道这完全可能，因为类似的骗局已在英国各地被报道过，受害者在巧妙的布局下中了计，将密码亲口告诉了盗贼。我们从不同的骗局中提取要素，来切实演示人们到底是怎样受骗上当，并将银行账户的信息和盘托出的。

为了证明我的想法，我们把骗局地点设在本地的一个咖啡厅。咖啡厅位于伦敦牛津大街一个购物广场的顶层。我西装革履地坐在一个相对安静的空桌旁，将公文箱放在桌子上，静候合适的猎物。没过多久，一位女士和朋友一起坐到我的邻桌，她把包放在了旁边的椅子上。也许是个人习惯，她将椅子拉到身边，并一直把手放在包上。

我需要偷取她的包，虽然她的手放在包上而且其朋友就坐在对面，但“悲剧”即将发生。几分钟之后，她的朋友去了洗手间。现在目标只有她一个人，于是我给亚历克斯(Alex)和杰丝(Jess)发了个信号。

亚历克斯和杰丝装成一对夫妻，上前请目标人物帮忙拍个合影，她很高兴能帮上忙。她将手从包上拿开，拿起相机为这对“幸福夫妻”拍照。在她分神的瞬间，我轻松自如地伸手拿起她的包并将其锁进我的公文箱。当亚历克斯和杰丝离开咖啡厅的时候，受害者根本没有注意到椅子已经空了。当亚历克斯从女子的视线中消失之后，他快速奔向停车场。

没过多久，受害者就意识到包不见了。她立即变得很焦躁，她站起身来，疯狂地四处寻找。这正是我们希望发生的情景，我问她是否需要帮忙。

她开始问我有没有看见什么，我告诉她“没有”，安慰她坐下，并让她努力回想包里有哪些东西。她边回忆边说：“一部手机、一些化妆用品、一点现金，还有几张信用卡。”好，进入主题！

在询问完信用卡是哪家银行的后，我便告诉她自己碰巧是那家银行的员工。她真是太“幸运”了！我向她保证不会有事的，但是要马上注销信用卡。我拨通了“客服中心”的号码，事实上是亚历克斯的电话号码，并把电话递给她。她上钩了，接下来就交给亚历克斯，看他怎么让受害人一步步陷入圈套。

亚历克斯在楼下的面包车里，车里的CD播放器播放着我们从网上下载的办公室嘈杂声。他让对方保持冷静，步步为营引诱她入局，然后肯定地告诉她信用卡注销很方便，但为了确认她的身份，需要她在通话手机的键盘上输入信用卡的密码。

我的手机，我的键盘。

接下来就没有任何悬念了。得到密码后，我起身离开了她和她的朋友，径直向门外走去。如果我们是真正的小偷，便可以用她的信用卡和密码在提款机上完成取款/转账等操作，也可以进行各种消费。幸运的是，这只是一档电视节目。当我将包还给她，并告之这只是一场骗局时，她很开心，甚至还感谢我。当然，我只是回答道：“不要感谢我，是我偷了你的包。”

无论系统有多安全，总有方法攻破它。通常，系统中的人是最好欺骗和操纵的。制造恐慌、运用影响力、采用操纵策略和建立信任感等方法都可以让受害者消除戒备。

这个例子可能有些极端，但也证明了，只要使用一点小伎俩，就可以成功实施看似不可能的诈骗。

承认系统有漏洞并且可能被攻破，是让系统更加安全的首要条件。相反，一直坚信系统坚不可摧的人就仿佛蒙着眼睛全速奔跑。社会工程学研究系统中最薄弱的一环——人，以及如何运用人性攻击的技巧攻破看似安全的系统。本书并非黑客指南，因为他们已经知道怎样闯入系统并且每天都在研究新的方法。相反，克里斯·海德纳吉（Chris Hadnagy）揭露了世界上最险恶的黑客、骗子以及社会工程人员的思路和方法，让我们有机会从黑暗的一面，也就是攻击者的视角来看系统安全与防护。

谨记，防御方和进攻方的思维方式是不同的，进攻方会考虑翻、钻、绕甚至穿越等各种方式，以进入为最终目标。就像我经常告诫观众的一样，如果你认为自己不可能被骗，那么你就是我最想骗的那个人。

保罗·威尔逊（Paul Wilson）

2010年10月

前言和致谢

几年前，在一次与良师益友马蒂·阿哈罗尼（Mati Aharoni）聊天的过程中，我决定建立网站www. social-engineer.org。在一群杰出人士的共同努力下，这个想法逐渐成熟，最终成立了一个十分神奇的网站。不久以后，将这几年的研究和经验归纳成书的想法也随之浮现。当我提议著书时，众人随即表示大力支持。在此，要特别感谢那些为本书的问世作出巨大贡献的人们。

从年轻时起，我就一直对操控别人特别感兴趣。当然不是通过卑鄙的方法，我只是对取得意外收获或者将不可能变为可能很感兴趣。有一次，我和一位好友兼商业伙伴参加在纽约贾维茨会议中心举办的技术会议。一家大型公司租用了施瓦茨玩具城来举办一场私人派对。只有持有邀请函的客人才能进入该派对，且派对邀请的都是惠普、微软等知名企业的首席执行官和高层管理人员，而我们俩只是两个小人物。朋友对我说："如果能参加那个派对，就酷毙了！"

我平淡地回应道："我们为什么不能参加呢？"当时我暗想：只要找到正确的方式，我们就可以参加这个派对。所以我走近负责签到的女工作人员，和她们交谈了几分钟。就在这个时候，Linux内核的创始人林纳斯·托瓦兹（Linus Torvalds）走了过来。我从其中的一个验票处拿起一个带有微软标志的长毛绒玩具，然后转向林纳斯，开玩笑地说："嘿，你想在我的微软玩具上签名吗？"

他大笑，扬起票说："不错嘛，年轻人，派对上见。"

我转向负责验收邀请函的女工作人员，便得到了两张该派对的邀请函。

后来我才开始对类似的事情进行分析，并将其称为"海德纳吉效应"。听起来很有趣，但我

发现在自己身上发生的很多事情，与其说是运气好或者命运使然，倒不如说是我知道如何在正确的时间做正确的事。

这并不意味着在前进的道路上我不需要努力工作和他人的帮助。我可爱的妻子正是我的缪斯女神。近20年来，你一直支持我的想法和努力，你是我最好的朋友、我的知己、我的支柱。没有你，就不会有今天的我。此外，你还为我带来了这个世界上最美丽的两个孩子。儿子和女儿是我继续从事这一切的强大动力。如果我的所作所为能使他们更安全一些，或者能够教导他们如何才能保障自身的安全，那就值得了。

我的儿子和女儿，对于你们给予我的支持、爱和动力，再多的语言也不足以表达我的谢意。希望我的小王子和小公主不用和那些心怀鬼胎的人打交道，但我知道那是不可能的。因此，希望本书中的信息多少能使你们俩更安全些。

保罗（Paul，网名 rAWjAW），感谢你对网站的所有支持。作为“维基大师”，你经过数千小时的努力工作，带给我们一个供全世界使用的极佳的网站。“你可以回家休息了！”我对你的谢意溢于言表。汤姆（Tom，网名 DigIp）的完美创造力更是锦上添花，是你们把网站塑造成了一件艺术品。

卡罗尔（Carol），Wiley出版社的编辑，辛辛苦苦地组织和跟进各个零散的进程。你凭借卓尔不凡的工作能力将一群人凝聚到这个伟大的团队中来，并使得我们的想法成为现实。谨在此表示我的谢意。

布莱恩（Brian），说实话，当这一切结束时，我会想念你的。在共事的几个月里，我十分期待你在编辑会议中带给我们的那些智慧的火花。你真诚、坦率的建议和忠告使得本书更为出彩。

同样，我还要感谢吉姆（Jim，网名 Elwood）。如果没有你，许多发生在social-engineer.org网站上以及本书中的事，甚至近几年我生活中的一些事，都不会成为现实。谢谢你使我保持谦逊和严谨。你不间断的核查有助于我集中注意力，使我所扮演的众多角色得到平衡。谢谢你。

利兹（Liz），大约12年前，你就建议我写一本书。我确信你当时所想的和现在不一样，幸而书已付梓。你帮助我度过了相对黑暗的一段时期。谢谢你，我爱你。

马蒂（Mati），我的导师，我的兄弟，若没有你，我会是什么样子呢？马蒂，你是我真正的导师和兄弟。我衷心感谢你给予我写作本书以及创建www.social-engineer.org网站的信心。不仅如此，你不断提供的建议和指导已经融入到本书的创作中，让我实现了自我超越。

你与BackTrack团队以及www.offensive-security.com团队的支持超出了我的预计。谢谢你们帮助我权衡利弊，实现主次有序。我的兄弟，特别感谢你，感谢你的理性，也感谢你在我沮丧的日子里带给我希望。衷心地谢谢你。

这里提到的每个人都在某些方面促成了本书。在他们的帮助、支持和厚爱下，我才能自豪地

在本书的封面署上自己的名字。还有其他支持网站、渠道和我们研究的人，谢谢你们。

编写本书时，它对我产生了极为深远的影响，希望你阅读本书时也能有同样的感受。

爱因斯坦曾经说过："信息并非知识。"这是一个伟大的观点。只是简单地阅读本书并不会将知识植入你的生命中。应用书中的原则，实践书中的内容，使这些信息成为日常生活的一部分。只有这么做，这些知识才能够真正起作用。

克里斯托弗·海德纳吉（Christopher Hadnagy）

2010年10月

目　录

第 1 章
社会工程学初探

知己知彼，百战不殆。
——孙子

社会工程[①]（Social Engineering）在很大程度上被人们误解了，从而导致人们对其定义和工作方式有很多不同的观点。有人简单地将社会工程视为撒谎，可以骗得免费的比萨或骗财骗色等；有人将其归类为罪犯或骗子的工具；也有人将其划到科学的范畴，认为其理论可以分门别类或采用数学公式加以研究；还有人将其视为长久失传的神秘技艺，掌握了社会工程学，从业者就能像魔术师那样制造强大的思维幻觉。

无论你的想法如何，你都可以从本书中获益。每个人每天都会在各种情况下使用社会工程的方法。小孩利用它来得到糖果，雇员利用它来得到晋升。大到政府部门的运作，小到公司的市场行为，或多或少都有社会工程的影子。不过罪犯和骗子之流也利用社会工程达到窃取他人信息和犯罪的目的。与任何工具一样，社会工程无好坏之分，它仅仅是一种多用途的工具。

下面这些问题有助于进一步理解本书的观点。

- 你需要尽可能确保公司安全吗？
- 你是每日阅读最新安全信息的人吗？
- 你是测试客户系统安全的专业渗透测试人员吗？
- 你是主修信息技术专业的大学生吗？

① 中国大陆的书籍和文章中普遍采用的译法是“社会工程”，台湾地区更多翻译成“社交工程”。本书一律依照大陆的译法。——译者注

- 你是需要新的、更好的社会工程观念以应用到实践中的社会工程人员（Social Engineer）[1]吗？
- 你是惧怕欺诈和身份盗用的消费者吗？

不管你是上述哪一类人，本书所包含的内容都会在应用社会工程技巧方面开阔你的视野。你将会了解社会工程的黑暗世界，懂得“坏人”是怎样使用社会工程的方法占据先机的，从而学会有效防御社会工程的攻击。

请注意，本书并非为弱者所作。它会带你领略社会的黑暗面，那里是“坏蛋”及恶意黑客的世界。本书将揭示并深入研究间谍和骗子所使用的社会工程技巧，评述类似007电影中的战术和工具，还将介绍日常情境是怎样成为复杂的社会工程场景的，最后将披露专业社会工程人员甚至是专业罪犯所使用的技巧和花招。

有人曾问我为何愿意公开这些信息，答案很简单：“坏人”不会由于契约限制或道德约束停止犯罪，他们不会因为一次失败就停止尝试，恶意黑客也不会因为公司不喜欢服务器被入侵就自动走开。事实是社会工程、员工被骗和网络欺诈的戏码每天都在上演。在软件公司不断加固程序的同时，黑客和恶意社会工程人员将目光转向基础设施中最薄弱的一环——人。他们的动机只是获得投资回报率，没脸没皮的小黑客会为一个简单的攻击花费上百个小时，而掌握社会工程技术的高级黑客只需一小时甚至更短的时间。

结果是没有绝对的安全，除非你拔掉所有电源并躲进深山老林，但是这种方法操作性不强，也不好玩。本书将讨论如何了解攻击、意识到攻击，并且防御攻击。我的信条是“学而知安全”。当前，社会工程攻击和账户盗用现象日益严重，掌握知识是确保安全的唯一有效方法。卡巴斯基实验室是开发病毒防护软件的顶尖厂商之一，他们估计2009年的社交网络中有10万多个恶意软件样本传播。在最近的一份报告中，卡巴斯基估计“针对社交网络的攻击的成功率是其他形式攻击的10倍”。

俗语“知识就是力量”用在这里很恰当。用户和企业对社会工程攻击的危险和威胁了解越多，理解越深入，对常见攻击场景越熟悉，也就越容易防御、减轻甚至完全阻止这类攻击。这就是知识的力量所在。

1.1　为何本书很重要

市场上有很多关于安全、黑客、渗透测试甚至社会工程学的书籍，其中有不少书为读者提供了很有价值的信息和提示。然而，即使有了这些信息，还是需要一本高阶的社会工程学书籍，来从攻击者的角度详细讲解社会工程攻击。本书并非简单罗列精彩的故事、漂亮的攻击以及疯狂的想法，而是讲述世界上第一个社会工程框架，详细分析成为一名优秀社会工程人员所需具备的基

① Social Engineer，指利用社会工程技术获益的人员，本书统一翻译成“社会工程人员”。——译者注

础要素，并就如何使用社会工程的技巧提供实用的建议，以提高读者测试系统中最薄弱的环节（人）的能力。

1.1.1 本书框架

本书以独特的方法研究社会工程学，其架构和www.social-engineer.org/framework网站中深入彻底的社会工程框架很类似。该框架列出了要成为一名优秀的社会工程人员，需要拥有的工具和掌握的技能（实体、心理和个性方面的）。

本书采用“解析加演示”的写作方法，首先讲解一个课题的原理，随后进行定义、解释和深入分析，最后使用真实故事或案例来演示其应用。本书并不单纯讲精巧的骗局故事，而是要写成一本了解社会工程学中黑暗世界的手册和指南。

全书提供了很多网络链接，可以了解更多的故事、实例账户、安全工具以及其他相关话题，还有很多实用练习，有助于你进一步掌握社会工程框架，同时提高日常沟通的技能。

上述内容对安全专员更加适用。我希望在阅读本书的时候，你能意识到安全并非“业余”工作，不可小视。罪犯和恶意社会工程人员越来越猖獗，对企业和个人生活的攻击在不断增多。自然地，人们也需要得到保护，这也是个人防护软件和设备热卖的原因。虽然这些产品很重要，但最好的防护是掌握知识。减弱攻击影响的唯一正确方法是知晓其存在、掌握其原理并懂得攻击者的思维过程和心理。

掌握这些知识并了解恶意黑客的思维方式，就像拥有了一盏明灯，可以照耀那曾经昏暗的角落，让你看清潜伏的“恶意攻击者”。若能提前知晓攻击方法，就可以采取预防措施，使公司或者个人事务免受攻击。

当然，我依然认为没有绝对的安全，二者并非自相矛盾。即使是重重防护的高级机密，也会而且确实曾经被轻易拿下过。

社会工程网站www.social-engineer.org/resources/book/TopSecretStolen.htm上有一个故事，摘自加拿大渥太华的一份报纸。这个故事很有趣，原因在于一些文档落入了错误的人手中。这些并非一般的文档，而是高度机密的国防文档，其中包括加拿大特伦顿军事基地安全隔离墙的位置信息、加拿大联合响应部队的平面图等。这些文档是怎么得到的？很简单，文档被丢到垃圾桶中，有人从垃圾箱里翻了出来。只要翻翻垃圾箱就能找到一个国家的绝密安全信息！

简单而致命的攻击每天都在发生，所以人们需要掌握知识、改变密码策略、改变远程服务器的访问方式，还需要在面试、交付、雇用和解聘员工方面改变思路。如不具备知识，也便没有改变的动力。

2003年，计算机安全研究所和FBI的一项联合调查发现，77%的被调查公司声称员工报复是

安全入侵事件的主因。赛门铁克公司的数据丢失防护部门Vontu（http://go.symantec.com/vontu/）声称，每500封邮件中就有一封包含机密数据。调查报告中包含如下一些信息（引自http://financialservices.house.gov/media/pdf/062403ja.pdf）。

- 62%的报道事件中存在客户身份被盗的风险；
- 66%的受访者认为他们的同事而非黑客会给客户隐私带来最大的风险，只有10%的受访者认为黑客是最大的威胁；
- 46%的受访者声称，员工从公司数据库中移除敏感信息是件“很简单”甚至是“轻而易举”的事情；
- 32%也就是约1/3的受访者不清楚公司保护客户数据的内部策略。

这些就是令人吃惊且头痛的统计数据。

后续章节会详细讨论这些数字。这些数字显示了安全处理中的严重缺陷。必须未雨绸缪，在被入侵之前掌握安全知识，才能做出改变，从而避免不必要的损耗、痛苦和经济损失。

孙子曰：“知己知彼，百战不殆。”真是至理名言！但只是“知”尚且不够，知行合一才是智慧所在。

本书作为社会攻击、社会操纵和社会工程的手册或指南使用最为有效。

1.1.2　本书内容

本书涵盖了专业和恶意社会工程人员所使用的工具和技能等各个方面。每章会深入探讨其中一项技能，介绍如何利用、提高和完善它。

下一节将定义社会工程学及其在当前社会中所扮演的角色，以及社会工程攻击的不同类型，包括社会工程在日常生活其他领域中的非恶意使用。同时还会讨论社会工程人员怎样利用社会工程框架来计划审计工作或提高自身技能。

第2章是实战课程的正式开始。信息收集是每一次社会工程实战的基础。社会工程人员的箴言是：“我所能做的一切均基于所收集的信息。”社会工程人员可能掌握各种技能，但是如果他不了解目标，没有勾画出所有的细节，那么等待他的只能是失败。信息收集是每一次社会工程实践的关键，虽然个人技能和迅速反应的能力也能使你摆脱棘手的情况，但一般情况下，掌握的信息越多，成功的机会也就越大。

我在第2章中会回答以下问题。

- 社会工程人员使用哪些信息来源？
- 什么样的信息是有用的？
- 社会工程人员怎样收集和组织信息？

- 社会工程人员要多专业?
- 掌握多少信息才够?

在分析了信息收集之后，第2章还会讨论交流模型，这两者是紧密相连的。首先会介绍交流模型的定义及其发展，随后会讨论怎样开发和使用一个正确的交流模型，还会简要介绍社会工程人员怎样使用该模型攻击目标并从中受益。

第3章探讨的是诱导，这是社会工程框架中的下一步。本章深入探讨了怎样通过提问来获取信息、口令，并详细了解目标及其公司的信息。你将学习到什么是好的、正确的诱导方式，以及诱导计划的制定是何等重要。

第3章还涵盖一个重要的话题，即如何使用信息来诱导目标的思维，从而让目标轻易接受你的问题。通过本章的学习，你将清楚地了解成为一个出色的“诱导者”有多么重要，以及如何在安全实践及日常生活中使用该技能。

第4章很重要，它讨论的是伪装，这是很多社会工程人员的关键技能之一。伪装涉及选定社会工程人员在攻击公司时所扮演的角色。社会工程人员可以伪装成客户、厂商、技术支持人员、新进员工，甚至是其他同样现实且可信的角色。伪装不仅需要一个故事背景，而且要角色扮演，要掌握扮演对象的眼神以及说话和行走等行为方式，要确定该人可能具备的知识和工具，了解其方方面面。这样当你以他的身份接近目标时，你就是他，而不仅仅是在演戏。本章会回答如下问题。

- 什么是伪装?
- 怎样选定伪装对象?
- 成功伪装的原则是什么?
- 社会工程人员怎样计划并执行完美的伪装?

框架中的下一步会占用大量的篇幅，而且必须从社会工程人员的角度来进行讨论。第5章讨论的是一些开放式话题，包括眼神的暗示等。例如，专家对眼神暗示有哪些不同观点？社会工程人员怎样使用眼神暗示？本章还会讨论有趣的微表情，以及它对社会工程的启示。

本章主要是研究型的内容，会回答如下问题。

- 安全领域可能会使用微表情吗?
- 怎样使用微表情?
- 微表情有什么好处?
- 人们可以训练自己从而掌握微表情吗?
- 在训练之后，微表情可以带来哪些信息?

第5章最具争议的话题可能是神经语言程序学（Neurolinguistic Programming，NLP）。很多人不确定什么是神经语言程序学以及怎样使用它，第5章简要介绍了NLP的历史及其备受争议的原

因，你可以自己决定社会工程中是否可以用到它。

第5章还会讨论面对面或电话沟通时社会工程的一个关键方面：怎样提出恰当的问题、倾听反馈及追加更多问题。司法人员多年来一直使用审问的方式来引导罪犯认罪及破解疑难案件。这部分内容也是对第3章所述知识的应用。

此外，第5章还会讨论怎样瞬间建立亲密关系，该技巧在生活中亦可应用。本章结尾是我个人的研究结果——“思维缓冲区溢出”，其含义是人类的思维与黑客每天破解的软件有很多相似之处。采用特定的方式，技术娴熟的社会工程人员可以溢出人类的思维并注入他们想要的命令。

与黑客通过溢出程序操纵软件来执行代码相似，人类思维也会接受特定的指令，本质上就是“溢出”目标的思维从而插入定制的指令。第5章是激动人心的一章，将介绍如何使用简单的技术掌握人们的思考方式。

很多人一生都在研究和证明哪些因素可能会影响人们。影响力是一个强大的工具，具有很多层面。第6章讨论说服的基础知识，本章中所阐释的原则将会引导你成为极具说服力的大师。

第6章首先简要讨论当前存在的不同类型的说服方式，并且提供实例来强化其在社会工程中的不同应用。

随后会探讨当前的另一热门话题——框架（Framing）。对于框架的使用存在很多不同的观点，本书展示了生活中的一些实例。通过对每个实例的剖析，你可以学到一些经验教训并练习怎样改变自己的框架，及作为社会工程人员在日常生活中怎样使用框架。

另一个社会工程中的重要主题是操纵。

- 操纵的目的何在？
- 操纵者的动机是什么？
- 社会工程中怎样应用操纵？

第6章展示了社会工程人员所必须掌握的关于操纵的所有内容，以及怎样成功地应用这些技巧。

第7章介绍使社会工程审计更为成功的工具。从隐藏的摄像头等物理工具到软件驱动的信息收集工具，每一节都介绍了社会工程人员可使用的经过测试和检验的工具。

在对社会工程框架有足够的了解之后，第8章将讨论一些实际生活中的案例。我选择了世界知名社会工程专家凯文·米特尼克（Kevin Mitnick）的两段精彩故事。通过分析和解读，为读者提炼这些案例中可供学习之处，并与社会工程框架中的方法相对照，还会将这些攻击载体与当前的实际应用相关联。我也会讨论一些个人的案例并进行分析。

社会工程指南如果不讨论攻击的削弱和防御方法就不能算是完整的，第9章会提供这方面的

信息。我会就缓解攻击方面的一些常见问题给出答案，并且就巩固安全和防御恶意攻击给出不错的建议。

前面只是对本书内容的简要概述，我真诚地希望你喜欢阅读本书，就像我享受写作的过程一样。我对社会工程学充满激情。我相信总有一些人，通过学习和挖掘一些与生俱来的潜质，会成为伟大的社会工程人员。我也相信，只要投入足够的时间和精力，任何人都可以通过对社会工程学的学习和不断的练习，成为一名专业的社会工程人员。

本书中的基本原理并不新颖，你也不会看到令人震惊的、会改变世界的技术。这里没有万能神药。事实上，人们早就拥有这方面的知识。本书只是将所有相关技巧组织在一起，以便读者明确方向，练习这些技巧，并认识到日常生活中的应用场景。所有信息都可以帮助读者正确理解各个章节所讨论的内容。

让我们从最基础的问题开始，先来回答“什么是社会工程”。

1.2 社会工程概述

什么是社会工程？

我曾就此问题询问一组安全爱好者，得到的答案令我非常惊讶。

- “社会工程是欺骗别人以获取信息。”
- “社会工程就是做一个好演员。”
- “社会工程是知道怎样免费获得东西。”

维基百科的定义是：“操纵他人采取特定行动或者泄漏机密信息的行为。它与骗局或欺骗类似，故该词常用于指代欺诈或诈骗，以达到收集信息、欺诈和访问计算机系统的目的，大部分情况下攻击者与受害者不会有面对面的接触。”

虽然常被冠以恶名，从“免费比萨”、“免费咖啡”及“把妹”等就可见一斑，但社会工程学实际上触及生活中的很多方面。

韦氏字典对社会（Social）的定义是“社区中属于或与生活、福利以及人际关系有关的”，对工程（Engineering）的定义则是“对物理、化学等纯粹科学进行实际应用的艺术或科学，如构建发动机、桥梁、建筑物、矿井、船只和化工厂等，技术或制作精巧的发明；机械控制”。

将这两个定义进行组合，很容易就可以发现社会工程学是一门艺术或者说得更好听是一门科学，它有技巧地操纵人们在生活中的某些方面采取某种行动。

这个定义将社会工程人员的活动范围扩大到生活的各个方面。小孩使用社会工程从父母处得

到他们想要的东西，老师采用社会工程与学生互动，医生、律师或心理学家运用社会工程从病人和客户那里得到信息。当然，司法部门也在使用，人们约会时也使用。事实上，从婴儿到政治家，每个人在交往活动中都在运用社会工程。

我对该定义进行了扩展，认为社会工程的真正定义是：一种操纵他人采取特定行动的行为，该行动不一定符合“目标人”的最佳利益，其结果包括获取信息、取得访问权限或让目标采取特定的行动。

举例来说，医生、心理学家及临床医学家通常使用社会工程的一些因素“操纵”病人，使其采取对病人有益的行动。相反，骗子使用社会工程的某些因素说服目标，使其采取给目标自身带来损失的行动。虽然两者的最终结果迥异，但其中的方法却很类似。心理学家使用一系列精心设计的问题，帮助病人得出必须改变的结论。类似地，骗子使用精心构造的问题将目标置于危险的境地。

虽然这两个例子都是社会工程的最真实形式，但是具有不同的目标和结果。社会工程不能仅仅定义为欺骗、撒谎或角色扮演。在我与克里斯·尼克森[Chris Nickerson，电视剧《老虎小组》（*Tiger Team*）中的知名社会工程人员]的一次交谈中，他说：“真正的社会工程不仅是以为自己在扮演角色，而且在那个时刻，你就是那个人，你就是那个角色，你的生活就是那样的。”

社会工程不是任何一种独立的活动，而是由框架中提到的各种技巧组合形成的活动、技巧和科学。同样，一种美食也不会仅有一种成分，而是精心组合、调配及添加多种配料而成的。社会工程就像烹调，而一个优秀的社会工程人员就像是主厨。使用少量的诱因，稍加操纵和伪装，就能成为一名完美的社会工程人员。

当然，本书会讨论其中的一些方面，但重点是你能从执法人员、政治家、心理学家甚至儿童身上学到什么，以提高你在审计及加强自身安全方面的能力。对儿童轻而易举就能“操纵”父母的行为进行分析，可以就人们的思维方式给社会工程人员以启示；分析心理学家怎样组织问题，可帮助我们理解什么能让人放松；分析执法人员成功审问的方法，可以了解如何从目标身上获取信息；分析政府部门和政治家如何传达消息以取得最大影响力，我们能知道哪些行为可行；分析演员怎样进入角色，会令你进入角色扮演的精彩世界；通过研究和分析微表情和说服方面的前沿知识，可以学习其在社会工程中的应用；通过分析世界上最出色的销售人员和谈判专家的动机，可以了解怎样建立密切的关系，使对方放松警惕，从而达成目标。

通过对反面示例（骗子及小偷等）的研究和分析，你会看到他们怎样综合应用这些技巧影响他人，让人们做出一些自己都想不到的事情。

将这些知识和开锁匠、使用隐秘摄像机的间谍、专业信息收集人员的技巧相结合，你会成为一个才华出众的社会工程人员。

一次行动中不需要使用所有这些技巧，你也不可能掌握所有的技巧。通过理解这些技巧的用

法以及使用时间，任何人都可以掌握社会工程学。确实，有些人天生就有这方面的才能，例如凯文·米特尼克，他可以说服任何人做任何事。小弗兰克·阿巴奈尔（Frank Abagnale, Jr.）[①]天生就具有欺骗别人、令别人相信他所扮演的角色的能力。维克多·拉斯体格（Victor Lustig）的所作所为更让人难以置信，他使一些人相信他有权销售埃菲尔铁塔[②]，其最厉害的一次当属欺骗了黑帮老大艾尔·卡彭（Al Capone）。

这些社会工程专家和其他类似人员似乎天生就具有这方面的能力，也拥有无畏的精神，使得他们可以尝试大部分人想都不敢想的事情。不过，今天的恶意黑客在不断提高操纵他人的能力，恶意的社会工程攻击在不断增多。黑暗阅读（DardReading）网站的一篇文章（网址是www.darkreading.com/database_security/security/attacks/showArticle.jhtml?articleID=226200272）中说道，一次数据入侵事件会给相关公司带来100万到5300万美元的损失。网站引用的是波耐蒙（Ponemon）研究所的结果："波耐蒙发现对网站的攻击、恶意代码和恶意的内部人员是最具破坏性的攻击形式。平均每年每个企业因网络犯罪所遭受的损失中，有90%以上是由这三种攻击造成的。一次网站攻击造成的损失是143 209美元，恶意代码造成的损失是124 083美元，恶意内部人员造成的损失是100 300美元。"恶意内部人员进入前三名意味着商业人士需要更加关注来自恶意社会工程方面的威胁，包括来自员工的威胁。

如果人们掌握相关的知识，则很多此类攻击就可以避免，因为人们可以根据所掌握的知识采取行动。有时了解恶意攻击者的思维和行为方式，就能对很多事情作出判断。

举一个简单的例子。近期一位好友告诉我，她很担心金融账户被入侵，担心自己被诈骗。在谈话的过程中，我们说起"猜测"他人的密码到底有多简单。我告诉她很多人的所有账户都使用相同的密码，当她意识到自己就是这样做的时候，我发现她的面色有点发白。我又说起大多数人采用配偶的名字或生日以及纪念日来组合成简单的密码，她的面色转为苍白。我继续说到人们经常选择最简单的"安全问题"，例如"你（或你母亲）的闺名"，而这些信息通过因特网或者几个虚假电话就可以轻易获得。

很多人会将这些信息写在Blippy、Twitter或Facebook账户中。我这个朋友不常使用社交网站，所以我问她是否曾想到过，别人通过几个电话就可以得到这些信息，她当然说不可能。为了说明人们很容易提供个人信息，我告诉她自己曾经在一个餐馆看到一个餐具垫，上面说可提供当地高尔夫球场的50美元抵用券——真是个诱人的礼物。要拿到这个礼物，需要做的就是提供自己的姓名、生日和住址，同时提供一个密码，该密码将用来为你建立账户，该账号随后会发到你的邮箱。（我之所以很快注意到这个，是因为一些人已经在填写表格，并将表格放在了桌子上。）收集此类敏感信息的网站每天都会冒出不少。

一个问询电话或者简单的网络搜索就能够找到生日和纪念日信息。通过这些信息，可以建立

① 他的故事被好莱坞拍成电影*Catch Me If You Can*，译名《猫鼠游戏》或《逍遥法外》。——译者注

② 参见百度百科词条"维克多·拉斯体格"，网址是http://baike.baidu.com/view/3057089.htm。——译者注

口令攻击列表。而且，很多网站在出售各种个人信息，每人9美元到30美元不等。

了解恶意社会工程人员的思维方式、骗子对信息的反应以及诈骗犯诈骗的方式，人们能够对周边发生的事情更为警觉。

我和一些安全爱好者曾经遍搜互联网，找寻有关社会工程方方面面的故事。这些故事有助于回答一个重要的问题——“随着时间的推移，社会工程在现实中有哪些使用形式？”，从而发现社会工程在社会中的位置以及它的恶意应用方式。

1.2.1　社会工程及其定位

前面说起社会工程可以用于生活的很多方面，但是并非所有的应用都是带有恶意或者会带来伤害性结果的。很多时候，社会工程可以激励一个人采取对自身有益的行动。如何才能做到这一点？

考虑下面的情况。约翰需要减肥，他知道自己身体状况不太好，需要改善。约翰的所有朋友都处于超重状态，甚至觉得超重挺好，并且经常开玩笑说：“不用为体型操心，太棒了！”从另一方面来说，这是一种社会工程，体现为社会认可和共识，你可以通过身边好友的认可获得自我认可。因为约翰的好友都觉得超重没什么，所以他更易于接受这一点。不过，如果这些人中有一个减肥成功，并且没有因此而对其他人品头论足，相反却乐于帮助约翰，那么约翰对体重的看法可能会发生变化，开始认为减肥是可行的，而且还不错。

本质上来说，这就是社会工程。通过上面的例子，你可以清晰地看到社会工程在社会和日常生活中的应用。下面会列出几个社会工程、骗局和操纵的实例，并且分析其成功的原因。

1. 419骗局

419骗局又称尼日利亚骗局，已发展成为一种很流行的骗局。可以在www.social-engineer.org/wiki/archives/ConMen/ConMen-Scam-NigerianFee.html找到此骗局的故事和文章。

一般情况下，骗局开始于向目标发送一封邮件（近来是发送一条短信），告诉对方被选中进行一笔很赚钱的交易，但是需要他提供一个小小的帮助。如果目标愿意帮助发信人从一家外国银行提取一大笔钱，那么他也可以分到一部分。一旦目标相信了这件事，并且“愿意帮忙”，就会出现一个问题，而解决这个问题需要目标支付一定的费用。在付出费用之后，另外一个问题又会冒出来，需要支付另一笔费用。每个问题都是“最后一个问题”和“最后一笔费用”，但在几个月之后还会冒出新问题。整个过程中，目标不仅看不到一分钱，而且还会付出1万到5万美元。该骗局的惊人之处在于，过去报道过的骗局，有的采用官方文档、论文、书信抬头甚至面对面的欺骗方式。

最近，此类骗局出现了一种变化，受害者会收到一张真实的支票。诈骗者承诺一大笔钱，谎称自己仅要其中的一小部分。如果目标汇出一小笔钱（例如1万美元），当收到承诺的支票时，他

就可以兑现支票，留下其中的差额。有些案件中，受害者汇出了钱，但拿到的支票是假的，当他兑现支票时，会因兑现假支票而被处罚金。

这种骗局相当成功，因为它利用了受害者的贪婪心理。谁不想用1万美元换得100万，哪怕只是10万美元呢？大部分聪明人都会这样做。当这些人收到来自“政府职员”寄来的官方文档、护照、收据时，他们会信心十足地尽最大努力来完成交易。承诺、一致和义务等观念在其中发挥了一定的作用。我会在后续章节中对这些特征进行详细分析，到时你会看到此种骗局如此强大的原因。

2. 稀缺的力量

www.social-engineer.org/wiki/archives/Governments/Governments-FoodElectionWeapon.html上的文章讨论的是稀缺的原理。

当人们被告知，其需要或者想要的某样东西的供应量有限，且必须赞同某种观点或行为才能得到的时候，我们称这种情形为稀缺。很多时候根本不明确说明需要人们做什么，而是让他们看到行为“得当”的人得到了奖励。

文章中讲述的是南非利用食品赢得选举的例子。当一些人或某个人不支持“正确”的领导人时，粮食会变得稀缺，工作也会被那些支持者“抢去”。人们发现这个问题时，很快就会转变成支持者。这是一种恶意的、带有伤害性的社会工程，但是其思路值得学习。当人们发现某样物品短缺，并且相信某些行为会导致自己得不到该物品时，他们通常会愿意做任何别的事以得到它。上例里使情况更糟的是，政府拿走一些生活必需品，然后造成“短缺”假象，仅仅提供给支持者——这是一种恶意但很有效的操纵策略。

3. 员工窃贼

员工窃取公司信息的现象很普遍，www.social-engineer.org/wiki/archives/DisgruntledEmployees/DisgruntledEmployees-EmployeeTheft.html上发布的统计数据十分惊人，报告指出60%以上的受访员工承认从雇主处带走了各种各样的数据。

很多时候这些数据被卖给竞争对手（例如这个故事中摩根斯坦利员工的所作所为，详见www.social-engineer.org/wiki/archives/DisgruntledEmployees/DisgruntledEmployees-MorganStanley.html）；有时员工窃贼会掌握时间点或其他资源信息，在一些案件中，对公司不满的雇员会带来很大破坏。

有一次，我和客户讨论解雇员工的办法，谈到禁用门卡、关闭网络账户以及护送员工离开大楼等等措施。该公司则认为每个人都是“家庭”一员，这些办法并不合适。

不幸的是，在解雇吉姆的时候发生了问题。吉姆是公司的一个高层人员，解雇过程很顺利，吉姆很友好地表示理解。公司做对的一件事是在下班时间解雇他，这样会避免尴尬和干扰他人。

在握手之后，吉姆问了一个致命的问题："我可以再待一小时，清理桌子并从我的计算机中拷走一些个人照片吗？我会在离开的时候将门卡交给保安。"

由于对会谈结果很满意，他们很快就答应了，然后面带微笑地离开了。吉姆回到他的办公室，将所有个人物品放在一个箱子里，从计算机中复制了图片和其他一些数据，然后连接到网络，将11台服务器的重要数据清空（包括会计记录、工资单、发票、订单、历史数据及图片等），也就花了几分钟时间。吉姆按照约定归还了门卡，冷静地离开大楼，没有留下任何可以证明是他发起了这些攻击的证据。

第二天早晨，该客户打电话向我描述吉姆造成的破坏，期待找到解救的方法。他别无他法，只能尽可能取证恢复，并利用两个月之前的备份开始恢复系统。

一个未被检查的不满员工可能比一群虎视眈眈的专业黑客所造成的破坏还要大。据估计，仅仅在美国，由于员工窃贼导致的商业损失就高达150亿美元。

这些故事给我们提出了问题：社会工程人员到底有多少种？他们是否可以分类？

4. 黑市和斯普林特大师

2009年，一则故事曝光了一个名为"黑市"的地下组织，"黑市"类似于罪犯的网络拍卖市场。该组织联系紧密，主要用于交易被盗的信用卡号、身份盗用工具及身份伪造工具等物品。

穆拉斯基（J. Keith Mularski）是美国联邦调查局的一名探员，他秘密打入了这个地下组织。一段时间以后，穆拉斯基探员成为了该网站的管理员。尽管该组织有很多人对他心存怀疑，但他还是管理这个网站长达3年之久。

在这段时间里，穆拉斯基必须伪装成恶意黑客，说话、行动与思考的方式必须一致。他伪装成一名恶意垃圾邮件发送者，这方面丰富的知识也是他成功渗透的基础。他的伪装和社会工程技巧之所以大获成功，是因为他使用了不起眼的斯普林特大师（Master Splynter）的身份进入了黑市网站，3年之后整个身份盗用团伙被摧毁了。

3年的社会工程渗透行动让59名罪犯落入法网，阻止了7000多万美元的银行欺诈。这仅是社会工程技巧具有积极作用的一个范例。

1.2.2　社会工程人员的类型

前面说到社会工程有很多不同形式，既可以是恶意的，也可以是善意的，既可以具有激励作用，也可以具有毁灭性。在学习本书的核心内容之前，我们首先简单介绍一下各种形式的社会工程人员。

- **黑客** 软件厂商生产的软件的安全性能不断提高，攻击软件因此变得越来越难。由于对于软件和网络的攻击（例如远程入侵）越来越困难，现在黑客开始采用社会工程攻击方式。目前在世界各地，通过利用硬件技术和一些个人技巧，黑客在大大小小的攻击中都会使用社会工程。
- **渗透测试者** 因为现实世界的渗透测试者（也称做渗透者）本质上有很强的攻击性，所以此类人员仅次于黑客。真正的渗透测试人员会学习和使用恶意黑客所使用的技巧，帮助确保客户的安全。他们拥有恶意黑客的技巧，但不会利用攻击中所取得的信息获利，也不会伤害目标。
- **间谍** 间谍把社会工程当成一种生活方式，他们通常会利用社会工程框架（本章稍后会讨论）的每一方面，可以说是这门学科的专家。世界各地的间谍都会学习“愚弄”人的方法，能够让人相信他就是某人或不是某人。除了学习社会工程技巧之外，间谍还或多或少地了解所渗透的企业或政府，这样才能得到他们的信任。
- **身份窃贼** 身份窃贼在当事人不知情的情况下，使用他人的名字、银行账号、地址、生日和社会安全号码等个人信息。这种犯罪的形式多样，包括穿上某种工作服来冒充该行业的人，也包括设置精巧的骗局。身份窃贼也会利用各种社会工程技巧，随着时间的推移，他们会变得更加大胆，对他人的损失更加漠不关心。
- **不满的员工** 在员工对公司感到不满之后，他们和雇主的关系常会进入敌对状态。这经常是单方面的情形，因为员工会故意隐藏不满的程度以降低职业风险。但当不满加剧时，他们就可能进行盗窃及破坏等各种犯罪了。
- **高明的骗子** 骗子总是利用他人的贪婪等心理，诱发人们“发财致富”的想法。高明的骗子会读心术，通过一些小细节就能确定某人是不是合适的“目标”。他们在造势方面也相当有技巧，让目标认为这是天赐良机。
- **高端猎头** 猎头也必须懂得社会工程的技巧，包括诱导和社会工程的心理原则。他们是读懂人们心理和动机的高手。很多时候，猎头不仅需要考虑和迎合求职者的需求，也要全面审视雇主的想法。
- **销售人员** 与猎头类似，销售人员也必须掌握很多人际交往的技能。很多经验丰富的销售人员都说，一名出色的销售人员不需要操纵他人，而应该利用自己的技巧发现人们的需求，并且看看自己是否能满足这些需求。销售的艺术包括信息收集、诱导、影响、心理把握以及很多人际交往的技能。
- **政府** 虽然政府很少被视为社会工程人员，但是政府会利用社会工程来控制信息的发布并管理人民。很多政府部门利用社会认同、权威性和稀缺资源来确保目标的受控性。这类社会工程并不总是负面的，因为一些政府传递的信息是对人民有利的，而且通过利用一些社会工程因素，这些信息会更有号召力，也更容易被广泛接受。
- **医生、心理医生和律师** 从事这些职业的人员似乎与其他社会工程人员不一样，但是他们同样使用上述社会工程人员所采用的方法。他们必须采用诱导、正确的谈话方式和询问策略，以及社会工程的许多（乃至全部）心理原则，来操纵“目标”（客户）采取他们所期望的行动。

不管在哪个领域，你都可以发现社会工程或其某一方面的应用。这也是我坚信社会工程是一门科学的原因。社会工程的各要素相加等于达成的目标。以骗子为例，伪装+操纵+贪婪心理=目标被社会工程套牢。

每一种情况下，困难都在于知道哪些要素会起作用，但是学习每个要素的使用方法就需要技巧了。这是制定社会工程框架的理念基础。正如下一节将讨论的，社会工程框架彻底改变了人们分析社会工程的方式。

1.2.3　社会工程的框架及其使用方法

我根据个人的经验和研究列出了社会工程人员需具备的各个要素。这些要素都很重要，具备所有要素才能成为一名合格的社会工程人员。这些要素并非一成不变。事实上，从建立开始，框架已经有了很大的发展。

这个框架的目的在于为学习这些技巧的人提供足够的信息，它并非每章包含的所有信息的资源参考。例如，第5章中有一部分是关于微表情的，内容源于该领域一些杰出人士的研究和我使用这些信息的经验。这些内容绝不可能替代保罗·艾克曼（Paul Ekman）博士等杰出人士在该领域50年的研究成果。

在通读框架之后，你会发现利用框架中的很多技巧不仅可以提高安全实践水平，而且也可以提高自身安全防护、有效沟通和理解他人的能力。

参考本书目录可大致了解框架，也可以在www.social-engineer.org/framework上查看该框架。框架乍看上去有点难以理解，但本书中对各个课题都进行了分析，你将学会如何应用每个技巧，并不断增强技能。

知识就是力量——诚哉斯言。掌握知识是防御大部分社会工程攻击的最佳手段。即使知识不能提供百分之百的防护，详细了解攻击手法也会让你保持警惕。学习知识不仅可以增强自身技能，而且还可以让你提高警觉。

除了学习，还要动手练习。本书并非仅需阅读一次的手册，而是一本学习指南。你可以根据需要对每节的课题进行学习和练习。框架内容是循序渐进的，因为社会工程攻击也是如此。框架按照社会工程人员在实践中或计划阶段利用技巧的顺序来讨论各个技巧。

框架展现了攻击的要点。在攻击计划完成之后、交付之前，必须要研究、增强和练习相关的技巧。

假设你需要为一家公司策划一次社会工程审计，目的是看你是否能够进入其服务器机房获得其中的数据。

也许攻击计划是伪装成需要进入服务器机房的技术支持人员。那你就需要收集信息，甚至需

要进行垃圾搜寻。

由于需要伪装成技术人员，你可以采用隐秘的摄像工具捕捉相关信息，练习技术人员的语言、脸部表情/声音，让你在行动、声音及表情上看起来就是一名技术人员。

如果能找到为客户提供技术支持的公司的名称，也需要收集他们的信息。你的客户通常要谁来提供服务呢？具体联系人的姓名是什么？攻击需要适当地计划。

不过本书并非仅为执行审计工作的人员所写。很多读者想知道攻击是什么，不是为了保护公司，而是为了保护自身。不清楚恶意社会工程人员的思维方式，其结果就是很容易被攻击。

大学中主修安全的学生也在使用这个框架。框架中列出了这些攻击的实现方法，读者可以深入学习。

一般来说，这些信息也可以提高每个人的日常沟通能力。通晓怎样读取面部表情或怎样提问会让他人更加放松并引出正面的回应，可以提高你与家人和朋友沟通的能力。它会帮助你成为一个好的倾听者，让你更加关注他人的感受。

读懂身体语言、面部表情和语调信息也可以增强你的沟通能力。知道怎样保护自己和你爱的人，会提升你的价值，让你对外部世界更加敏感。

1.3 小结

和其他任何书籍一样，只有付诸实践，书中知识的价值才会得以体现。实践得越多，对这些技能的掌握也就越成功。

前面我说过社会工程和烹调十分相似。通过将各种正确的调料进行适量混和，可做成令人垂涎欲滴的美味佳肴。第一次尝试烹调时，菜可能做得过咸也可能淡而无味，但是你不会轻易放弃，通过不断尝试，终会得偿所愿。社会工程也一样。一些必须掌握的技巧可能轻而易举就学会了，而有些技巧则难学得多。

如果某个课题很难理解或很难掌握，请不要放弃，也不要认为自己学不会。只要付出努力，任何人都能学会和使用这些技巧。

同时也要记住，与烹饪秘方一样，成功的社会工程也需要很多“配料”。第一种配料可能在一段时间后才会发挥作用。有些技巧，例如第5章介绍的“人类思维缓冲区溢出”，只有在你掌握书中的一些其他技巧之后才有意义。

不管怎样，要反复练习，对没搞清楚的课题要进行额外的研究。现在，让我们开始“烹调”吧。你的“秘方”起始于下一章的第一味配料——信息收集。

第2章
信息收集

战争的胜利百分之九十取决于情报。
——拿破仑·波拿巴

人们常说，没有什么信息是不相关的。本章的主题是信息收集，这句话放在这里完全适用。即使是最微小的细节也可能促成社会工程人员的成功入侵。

我的良师益友马蒂·阿哈罗尼在渗透测试方面有十多年的专业经验，他的一次亲身经历是这方面最好的例证。那次，马蒂的任务是入侵一家在网上查不到什么信息的公司，因为能入侵该公司的途径很少，所以这项任务极具挑战性。

马蒂开始通过互联网寻找可能取得突破的任何蛛丝马迹。一次搜索中，他发现该公司一名高管的公司电子邮件地址出现在了一个集邮论坛上，且该高管对20世纪50年代的邮票表现出了浓厚的兴趣。马蒂迅速注册了一个域名，类似于www.stampcollection.com，然后从谷歌上找来一堆20世纪50年代的邮票图片。他快速创建了一个网站展示他的“集邮册”，随后又精心编写了一封电子邮件发给该高管。邮件内容如下。

亲爱的先生，

我在www.forum.com上发现你对20世纪50年代的邮票很感兴趣。最近我的祖父过世了，给我留下一个集邮册，我想出售这批邮票。我建了一个网站，如果你想看的话，请访问www.stampcollection.com。

谢谢！

马蒂

在给目标发送电子邮件前，他想确保产生最大的影响。他找出论坛帖子中该官员办公室的电话号码，给他打了个电话，说："早上好，先生，我是鲍勃。我看见你在www.forum.com上发的帖子。 我爷爷最近过世了，给我留下了一大堆20世纪五六十年代的邮票。我拍了照片，并且做了一个网站。如果感兴趣的话，我可以将链接发给你看看。"

目标非常急切地想看到这些邮票，就等着收电子邮件了。马蒂发送完电子邮件后，便等待他点击链接。马蒂将一个恶意帧嵌入到网站页面中，帧中的代码会利用当时很流行的IE浏览器的已知漏洞，使目标计算机受控于马蒂。

不久，受害人就收到了邮件，而且迫不及待地点击了链接，公司系统的边界防御也就打开了。

短短的一条信息（受害人寻找邮票时留下的公司邮箱地址）就导致了这次入侵的发生。所以我们说，没有信息是不相干的。带着这样的思想，我们来看看信息收集中会碰到的问题。

- 怎样收集信息？
- 社会工程人员收集信息可以利用的资源有哪些？
- 如何利用收集到的信息进一步描述目标？
- 如何对这些信息进行定位、存储及分类，才能够使之最易于使用？

为了完成适当而有效的信息收集工作，这些只是需要解决的问题中的一小部分。在多如牛毛的社交网站上，人们可以轻易地与其所选的人分享自己生活的方方面面，这使潜在的破坏性信息比以往任何时候都多。本章通过社会工程实例讲解信息收集的原则和应用，以及人们发布在网上的信息对于其个人和企业安全有何破坏性的影响。

社会工程人员使用到的很多技巧或方法都来自于其他领域，其中一个典型的例子就是销售。销售人员往往很健谈、随和，而且非常善于收集别人的信息。

我曾经读过一本有关销售的书，作者鼓励销售人员去收集购买者的推荐，其中有个问题是这样的："你认为谁能像你一样从该产品中受益呢？只要说一个人就可以。"

只需要简单的交流就可以让一个人敞开心扉，他可能推荐家人、朋友甚至同事。收集这些信息使销售人员可以在"熟人介绍"的情况下拜访客户，并能够迅速获得对方的信任，不至于吃闭门羹。

销售人员在拜访时可以使用如下开场白："我刚从隔壁的简家里过来，她买了我们的优惠套餐。在了解各种好处之后，她支付了一年的套餐费用，并认为你也能从中受益。请问能耽误你一分钟，听我介绍一下简刚刚买的优惠套餐吗？"

销售人员使用的这些技巧经常被社会工程人员效仿。当然，社会工程人员并不会要求交谈的对象推荐他人，而是自己通过分析得到其中的信息。销售人员从当前客户处收集信息，然后利用这些信息使新的"目标"客户更乐于倾听并接纳自己的建议。此外，通过暗示前一位顾客已购买，

并在交流中使用“优惠”、“优先”等关键词，销售人员在短时间内就使目标兴趣盎然。这种技巧很有效，因为它建立了信任，利用了“熟人”，能让目标跨越最初的沟通障碍，与销售人员或社会工程人员更为自然、舒服地交流。本章以及第3章将深入探讨这些话题。

作为社会工程人员，这两个角度对于理解和有效运用技巧都至关重要。回想一下第1章中对主厨的相关阐述：一位优秀的主厨知道如何辨认出高质量的菜肴、新鲜的蔬菜和优质的肉类。他们很清楚秘方中的配料，但若不能把握好各食材的用量，这道菜要么淡而无味，要么偏咸，甚至会难以下咽。想要成为主厨，仅仅知道菜里需要放盐是远远不够的，还需要了解适量的各种配料如何搭配，这样才能掌握烹饪的艺术。社会工程人员只有牢牢掌握各种技术手段的使用方法和适用场景（“秘方”），才能成为社会工程达人。

本章帮助你找到平衡点。信息便是社会工程人员“秘方”里的首要配料，下一节会详细介绍。信息质量越高，成功的几率就越高。本章从如何收集信息讲起，然后讨论通过哪些途径来收获信息，最后将讨论如何整合各类信息并运用到社会工程中，这样本章在体系上就很完整了。

2.1　收集信息

收集信息就如同盖房子一般。如果想从房顶盖起，肯定是必败无疑。一栋坚固的房子必定是在打下坚实的地基后，从地面往上盖的。收集信息时不要总想着怎么组织和运用这些数据，创建一个文件或信息收集服务来收集信息才是当务之急。

事实上，有很多工具可以帮助我们收集和运用这些数据。在渗透测试和社会工程审计中，我使用Linux BackTrack发行版，BackTrack是专为这一目的而设计的。BackTrack[①]和大部分Linux发行版一样，是免费、开源的，也许它最大的优点便是集成了300多款安全审计工具。

BackTrack中的工具也是开源和免费的。特别吸引人的一点在于这些工具的质量都很高，其中很多都能与同类商业软件媲美，甚至是有所超越。这其中就有两个特别适用于信息收集和存储的工具，一个是Dradis，另一个为BasKet。接下来将分别简要介绍这两款工具。

2.1.1　使用BasKet

BasKet从功能上看有点像记事本，但是比记事本要强大得多。这款软件现在由王凯文（Kelvie Wong）维护更新，你可以从BackTrack中找到，或者到http://basket.kde.org/网站上免费下载。该网站有详细的介绍，教你如何安装。这款软件易于使用，界面也并不复杂。

① BackTrack是基于Ubuntu的自启动运行光盘，它包含了一套安全及计算机取证工具，简称BT，目前最新与最好用的版本是BT5。——译者注

如图2-1所示，界面很简单，很容易上手。在屏幕左侧单击鼠标右键，选择“New BasKet”，会添加一个新的“BasKet”，用以保存数据。

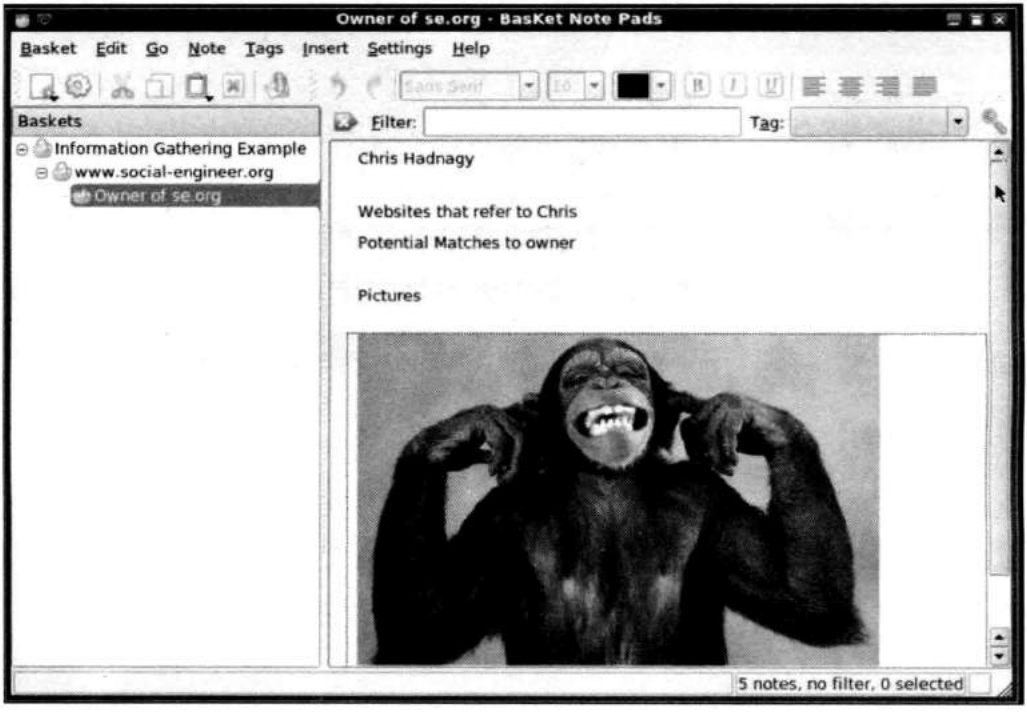

图2-1 信息收集阶段，使用BasKet轻松组织收集到的数据

BasKet新建好以后，便可以往里面复制/粘贴数据，添加屏幕截图，甚至可以添加OpenOffice办公软件或者其他类型的图表数据。

添加屏幕截图的方式有好几种，最简便的方法是复制图片，在新“BasKet”中单击鼠标右键，选择“粘贴”。如图2-1所示，添加图片的操作简单、快捷，同时可以通过输入、粘贴等各种方式为图片添加文字备注。

在通常的安全审计中，BasKet组织和展示数据的方式是它的优势之一。我通常为不同类型的数据建立不同的BasKet，例如域名查询信息、社交媒体信息等。然后，使用谷歌地图或谷歌地球获取目标客户的建筑和设施图片，保存到BasKet中。信息收集完成后，快速提取和使用这些信息也很简单。图2-2展示了一个接近完工的BasKet，其中有很多有用的信息和标签。

如图2-2所示，使用BasKet来存储和组织信息很简单。我尽可能多地往里面存放信息，因为再小的信息也可能是有用的。我收集的信息包括目标客户的网站内容、域名查询信息、社交网络、图片、员工联系方式、简历、论坛、爱好等一切可能与目标公司相关的信息。

图2-2　包括很多有价值信息的几近完整的BasKet截图

信息收集完成之后，直接单击“BasKet”菜单，然后单击“Export”，将整个BasKet导出为HTML网页文件。这对生成报告和共享信息非常有用。

对于一名社会工程人员来说，接下来要详细讨论的数据收集是每次行动的核心。然而，如果信息不能得到及时的重现和运用，将会毫无价值。BasKet及其类似工具使得信息收集和使用工作更加简单。一旦你尝试使用，便会爱不释手。

2.1.2　使用Dradis

尽管BasKet是款非常好用的工具，但是如果要收集的信息很多，或者需要一组人共同完成信息收集、存储和调用操作，那么就需要一款能够供多用户共享数据的工具——Dradis。根据Dradis工具开发者的描述，Dradis是可以提供信息中央存储的独立Web应用，可以统一管理需要收集的信息。

和BasKet一样，Dradis也是一款免费的开源工具，你可以在http://dradisframework.org/网站上免费下载。Dradis可以安装于Linux、Windows和Mac等不同操作系统，http://dradisframework.org/install.html网页上有详细的安装和配置说明。

Dradis安装并设置好以后，就可以浏览你分配的本地主机和端口，或者使用标准端口号3004。只要打开浏览器，在地址栏中输入http://localhost:3004/即可登录使用。

登录进去以后的欢迎界面如图2-3所示。注意左上角的添加分支（Add Branch）按钮，添加分支以后就可以像BasKet一样添加信息，如备注、图片等，甚至可以导入笔记数据。

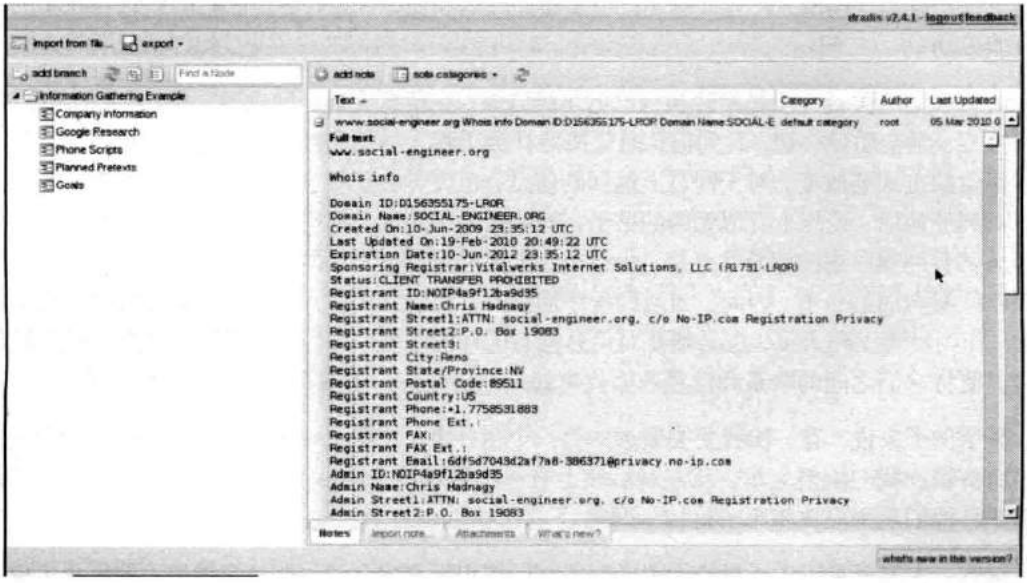

图2-3 Dradis简洁而易用的界面

Dradis和BasKet只是用来收集和存储数据的两款小工具，二者的网站上都有很好的设置说明和使用介绍。

不论操作系统是Mac、Windows还是Linux，你都能找到相对应的工具。重要的是工具用起来顺手，并能处理大规模数据。

基于上面提到的因素，我建议社会工程人员放弃使用Windows或Mac操作系统自带的记事本和文本编辑器。它们无法满足你对于数据格式和相关区域高亮显示的需求。图2-3显示的是我使用的Dradis服务器端，有一部分我专门用来保存电话交谈记录。这个功能很好用，可以记录我根据所收集的信息产生的想法。

这些工具表明了社会工程人员是怎样利用收集到的信息的。利用信息的第一步便是要像社会工程人员一样思考。

2.1.3 像社会工程人员一样思考

拥有几百兆的图片和数据固然很好，但是当你回过头来浏览这些信息时，如何能够保证最大限度地挑出有用的信息呢？

当然，你可以打开浏览器，随机输入冗长的词语进行关键词搜索，这样做可以找到某种形式

的信息，其中一些甚至是有用的。然而，在肚子很饿的情况下，你才不会跑到厨房，不管三七二十一地往锅里随便扔食材，然后就开始翻炒呢。计划、准备并考虑各种会影响菜肴好坏的因素才可能烹饪出佳肴。同理，社会工程人员也要做好计划和安排，想好将要收集的信息和收集的方式才可能成功。

信息收集的关键一步是要转换自己的思维方式。在信息大爆炸的世界，我们必须改变平常的思维方式，学会质疑一切，看到信息时就按照社会工程人员的思维方式来思考。利用网络等方式进行搜索的方式要改变，对于网页上返回的信息，也要学会从社会工程的角度去思考、审视。无意中听到的谈话、论坛上看似无聊的帖子，抑或是一袋垃圾，都应该以不同的方式来对待。我的导师马蒂看到程序崩溃就异常兴奋。为什么？他是渗透测试员，同时也是漏洞编写人员，崩溃是找到软件漏洞的第一步。因此，当遇到程序崩溃时，他感到异常兴奋，而不是为数据丢失而烦躁焦虑。作为社会工程人员，也必须要对信息抱有同样的态度。每当发现目标人物使用多个社交网站时，便将它们之间的联系和信息数据收集起来综合分析，争取得到完整的目标人员档案。

举个例子来说，有一次我要去遥远的另一个州办事，便租了一辆车。我和同事将行李统统装到了后备箱。我们刚要上车，就发现后座上有一小袋垃圾。同事说："如今的服务真差，我们付钱租车，他们至少应该将车子打扫干净吧。"

诚然，大家都希望车子里是干干净净的，同伴想把它扔到旁边的垃圾桶里，我阻止了他，说道："让我看看那个袋子。"我打开袋子，拨开里面的快餐纸袋以后，映入眼帘的物品让我大吃一惊——里面是半张撕碎的支票。我赶紧倒空袋子，从里面找到一张银行收据还有另外半张支票。这是一张面值几千美元的支票，虽然被撕开了，但撕得不是很碎，仅撕成了四大块，然后被扔到装有快餐纸袋的垃圾袋中。将这几片拼接到一起，可以看到这张支票的所有者的姓名、公司名称、地址、电话号码、银行账号及银行流水单号。再加上这张银行收据，我可以清楚地知道他的存款数字。他应该感到庆幸，我不是心存歹念的人，要不然只要再多几步，我就可以从他的账号中窃取存款。

这个故事向我们展示了人们是如何看待自己的重要信息的。这个家伙在我之前租了这辆车，他可能以为将支票撕碎扔掉就安全了，或者说至少当时他是这样认为的。无独有偶，通过www.social-engineer.org/wiki/archives/BlogPosts/LookWhatIFound.html，你可以看到最近发生的这样的故事：有人将非常贵重的物品随意扔掉，或者在旧货市场上廉价出售。

其中包括：

- 一幅被博物馆以120万美元收购的油画；
- 一辆1937年生产的、仅跑了24 000英里的型号为57S Atalante的布加迪跑车[①]，这辆车最终以300万美元出售；

① 布加迪公司在过去70多年时间里仅生产了3辆Atalante原型车，其中只有2辆存世至今，而57S型Atalante轿车在后来的限量生产试验中也仅生产了17辆。目前为止有4辆被保存在法国乡村的博物馆里，该车留存数量极少，找到的这辆57S Atalante布加迪跑车已经消失了半个世纪之久。——译者注

- 《独立宣言》珍本。

如果人们能把《独立宣言》珍本随同一张油画扔掉，那么丢掉账单、医疗记录、旧发票或者信用卡账单又有什么大不了的。

懂得如何在公共场所和人打交道会产生令人意想不到的效果。接下来将讲述我对一家公司进行安全审计的经历。在审计之前，需要收集一些数据。下面就让我们看看，如何利用那些看似无用的信息找到突破口。

对于被审计公司的一位高管，我仅仅跟踪其一两天，便发现了他每天早上同一时间都会去当地一家咖啡馆喝咖啡。在发现他的这一习惯后，我便计划了一场“偶遇”。他一般早上7:30到咖啡店，每次会坐半小时到35分钟的样子，看看报纸，喝一杯中杯拿铁。在他进店3~5分钟后，我也进到店里，点了相同的咖啡，坐到他旁边的位子上。我看到他放在一旁已经看完的报纸，便向他借阅。路上我已经读过了这份报纸，知道第3页上有一篇关于附近一起谋杀案的报道。我装作刚看到这则消息一样，大声说道：“在这么小的一个镇子里，怎么会有如此骇人的事情发生，太可怕了！你是不是也住在这附近啊？”

此时此刻，有两种可能：一是他根本不理我，二是我的肢体语言、说话的语调和表现会让他感到放松。事态的发展证明是第二种情况，我成功了。他答道：“是啊，几年前我因为工作搬到这里。我喜欢小城镇，但正如你所说，这种可怕的事情越来越多。”

我接着说道：“我只是途经这里。我的工作是给大公司提供高品质的咨询服务，我经常在不同的小城镇之间跑来跑去。不过最近这种事情越来越多了，就连乡下也是如此。”之后，我用一种调侃的语气问道：“你不会碰巧是一个需要咨询服务的大公司的领导吧？”

他笑了起来，感觉我刚刚的话是在质疑他的高贵身份一般，说道：“我是XYZ公司的财务副总，不过我不负责那个部门。”

“嘿，我又不是在向你推销产品，喝咖啡而已。不过，不知你明天或者周三有没有空？我可以顺便访问贵公司并为你提供一些信息。”

从这里开始，故事变得有趣了。他说：“我很想应约，但是周三我必须要出去度假。要不你给我发份邮件，我回头给你电话。”并随手递上了他的名片。

“我猜想应该是去和煦而明媚的地方吧？”我问道，心想快达到目的了，是时候结束此次谈话了。

“和我妻子一起乘游艇去南方。”我想他是不会告诉我目的地的，不过这也没关系。我们握了握手，便分道扬镳了。

他会很快忘记我吗？也许吧。不过，我已经得到一些颇有价值的信息了：

- 他的直拨电话号码
- 他出发去度假的日期
- 度假的类型
- 他住在本地
- 他公司的名称
- 他在公司的头衔
- 他是近期搬过来的

当然，其中一些信息在我前期信息收集时就知道了，但是这次会面让我得到了更多信息。现在可以开始我的下一步攻击了，在他去度假的翌日，我拨通了他公司的直线电话，前台告诉我："对不起，史密斯先生度假去了，请问需要留言吗？"

太好了。信息的真实性已被证实，我要开始计划的最后一步了。我穿上西装，带着价值9美元的名片来到他的公司。进去登记好之后，我告诉前台自己和史密斯先生约定10点钟会面。她答道："史密斯先生在度假，你确定是今天吗？"

使用我的微表情技术（第5章会讨论到），我故作惊讶地问道："什么？他的海上航游是在这周？我以为他下周才出发。"

刚刚的这句相当关键。为什么？

我想让前台相信我，相信这个会面是真实的。在我提到海上航游时，说明我和史密斯先生有过亲密的交谈，甚至于知道他的旅行计划。我流露出的无助和失落引发秘书想帮助我的冲动："哦，亲爱的，真的很抱歉，要不我给他的助手打个电话吧？"

"哦，不。"我答道，"我只是想给他带来一些信息。这样吧，我把消息给你，在他回来时，你帮忙转告他。真的是太尴尬了，你可以不告诉他我来过吗？"

"我会保守秘密的。"

"谢谢你。真想快点离开这里，不过在我离开之前，可以用一下这里的洗手间吗？"通常情况下这种要求应该是不被允许的，但是借着刚才融洽的对话、我的无助以及她对我的一点同情，我还是有一些机会的——而且我确实成功了。

我把一个信封放在了洗手间的一个隔间里。信封上贴着"私人"的标签，信封里面是一个带有恶意攻击病毒的U盘。不仅是这里，我在大厅走廊旁的休息间里也放了一个，以增加成功的概率。希望有人会发现当中的一个，并好奇地将U盘插到他们的电脑里。

值得庆幸的是，这种方法百试不爽。可怕的是，如果没有那次咖啡店里看似无足轻重的对话，这次攻击不可能成功。

这个故事不仅是要说明微小的数据也会导致入侵事件，同时也展示了搜集数据的技巧。对待各种数据源必须充分理解、认真测试，直到你能熟练掌握每一种数据源及其收集方法。数据源有很多种，优秀的社会工程人员必须花费一定的时间来了解每一种的优缺点，以及利用它们的最佳方法。这也是下一节要讨论的内容。

2.2 信息源

信息存在多种不同的来源。虽然以下几个小节不能覆盖每一种来源，但是也列出了收集信息的主要途径。

2.2.1 从网站上收集信息

公司或者个人网站是信息的重要来源。优秀社会工程人员的第一步就是尽可能多地从公司或者个人网站上收集信息。在这些网站上花费一些时间是值得的，可以帮助你清晰地了解对象的基本情况：

- 他们做什么
- 他们提供的产品和服务
- 地理位置
- 招聘信息
- 联系电话
- 执行官和董事会成员的简介
- 支持论坛
- 电子邮件命名规则
- 可能用于密码分析的特殊字符或短语

看别人的个人网站是件非常有意思的事情，因为上面的内容涉及他们生活的方方面面：孩子、房子、工作等。这些信息应该分类存储，因为它们常会用于日后的攻击。

同一个企业的员工往往会登录相同的论坛，有着类似的兴趣，甚至会上相同的几个社交网站。如果你在LinkedIn或者Facebook中找到一名员工，很有可能他的好几个同事也在其中。收集这些数据，可以更加清楚地分析这家公司以及它的员工。很多员工会在社交网站上用标签的形式展示自己的职位，这可以令社会工程人员勾勒出公司某个部门的规模以及组织架构。

1. 搜索引擎

强尼·龙（Johnny Long）为渗透测试人员写了本著作，叫做*Google Hacking for Penetration Testers*。这本书让很多人大开眼界——原来谷歌里有如此多的信息。

谷歌中记录了很多你认为已经删除的数据，就如同大型数据库一般。只要设定好查询方式，就能得到你想要的信息。

强尼总结出了一系列用来查询公司信息的语法。例如，在谷歌搜索框中输入site:microsoft.com filetype:pdf，就能得到microsoft.com网站上的所有PDF文档列表。

熟知搜索语法可以帮助你找到和目标相关的信息，这对信息收集来说很重要。我习惯于使用语法（类似于filetype:pdf）来检索PDF、DOC、XLS和TXT文件。当然，员工留在服务器上的DAT和CFG文件以及其他数据库和配置文件等也是值得收集的信息。

强尼的书通篇都在讨论如何利用谷歌来查找数据，不过重点是懂得谷歌提供的各种操作符可以帮助你创造出属于自己的搜索语法。

www.googleguide.com/advanced_operators.html上列出了各种操作符以及详细使用方法。

能够提供惊人信息量的搜索引擎不止谷歌一家。一位名叫约翰·玛瑟利（John Matherly）的研究人员发明了一个叫做“Shodan”的搜索引擎（www.shodanhq.com）。

Shodan的特殊之处在于它提供针对服务器、路由器和特定软件的搜索功能。例如搜索microsoft-iis os:“windows 2003”，就可以得到如下各地的服务器数量信息，这些服务器都是运行IIS服务的，里面装的是微软Windows 2003系统。

- 美国 59 140
- 中国 5361
- 加拿大 4424
- 英国 3406
- 台湾 3027

这个搜索引擎不能针对特定目标，但是它揭示了一个道理：网络上有惊人的信息量供社会工程人员查询分析，以提升信息收集的能力。

2. Whois域名信息查询

Whois能提供域名数据库查询服务。Whois数据库中有很多有价值的信息，有些时候甚至包括网站管理员的完整联系方式。

使用Linux命令行工具或者登录www.whois.net这样的网站，都可以查询到域名的注册信息，包括联系人、电子邮件地址、电话号码，甚至DNS服务器的IP地址。

域名注册信息可以很好地帮助你了解目标公司，特别是他们的服务器。这些都可以用于信息的进一步收集，或者发动攻击。

3. 公共服务器

企业对外的公共服务器往往会提供网站所没有的很多信息，比如服务器的操作系统、安装的应用程序和IP地址，这些信息可以大致反映企业的信息服务架构。了解平台和应用信息之后，便可以和域名信息组合在一起，在公开技术论坛上进一步搜索相关的配置信息。

IP地址可以说明服务器是在本地还是从服务器提供商处租赁的；通过域名解析记录可以看出服务器的名称、功能，以及IP地址分布。

在一次审计的过程中，通过使用Matelgo（第7章中将有详细介绍）搜索网页，我找到了一个对外的网站服务器，上面有几百份文档，其中包含项目数据、客户和文档作者信息。这些信息的泄露，对于公司来说是致命的。

值得一提的是，*端口扫描*（使用诸如NMAP或者其他端口扫描工具去定位公共服务器的开放端口、软件版本和操作系统类型等）在有些地区是违法的。

2003年6月，以色列人艾维·米兹拉希（Avi Mizrahi）因涉嫌未授权访问计算机系统被当地警方提起公诉。当时，他只是对摩萨德网站（Mossad）进行了端口扫描。8个月后，艾维被无罪释放。法官的意见是非恶意的端口扫描不应被禁止（www.law.co.il/media/computer-law/mizrachi_en.pdf）。

1999年12月，斯考特·莫尔顿（Scott Moulton）被联邦调查局以违背佐治亚州《计算机系统防护法》和美国《计算机欺诈与滥用法》为由实施逮捕。当时，他所在的IT服务公司与佐治亚州的切罗基县有着长期的合作关系，一直为911安全中心提供维护和升级的服务（www.securityfocus.com/news/126）。

作为工作的一部分，莫尔顿在为切罗基县的服务器进行例行端口扫描时，扫描到另外一台属于另一家IT公司的网站服务器。这件事情直接导致其被起诉，到了2000年，法官以未对互联网完整性和可用性造成破坏为由，撤销了对他的诉讼。

2007年到2008年间，英国、法国和德国都通过了相关的法律，认为创建、发布和拥有能够导致他人入侵计算机的工具都是违法行为，端口扫描工具也在其中。

当然，如果是收费的信息安全审计，这些都应在合同中描述清楚。对社会工程人员来说，应该熟知当地法律，避免做出违法行为，这非常重要。

4. 社交媒体

很多公司最近开始热衷于在社交网站上做推广和营销。社交网站的营销成本低廉，又有大量的潜在消费群体。这里提供了来自于企业的另外一股信息流：活动安排、新产品发布、新闻报道以及一些能与当前热点事件挂上钩的文章，等等。

近期，社交网络正在逐步显示它们的作用。每当一个站点成名，便会涌现一系列采用类似技

术的站点。有了Twitter、Blippy、PleaseRobMe、ICanStalkU、Facebook、LinkedIn、MySpace等站点以后，人们的生活和行踪被晒在了网上。随后，我们将深入讨论这一话题，你将发现社交网络作为信息源的神奇之处。

5. 个人网站、博客等

像博客、维基、网络视频等个人网站不仅会提供目标公司的信息，还会透漏这些信息上传者的个人观点和信息。在博客上对企业满腹牢骚的员工会和那些持有类似观点的人相聊甚欢。不管以什么样的方式，人们总会在网上张贴大量的数据信息，任何人都可以阅读。

举个例子。让我们一起来看看最近出现的一个网站——www.icanstalku.com（参见图2-4）。不同于它的域名，这个网站并不是鼓励人们去跟踪别人，它跟踪的是那些毫无防范意识的Twitter用户。它遍历Twitter网站，寻找那些蠢到用自己的智能手机拍摄照片并上传的家伙。很多人都没意识到智能手机拍摄的照片会隐藏GPS信息。你上传这些照片的同时，也泄露了自己的拍摄位置信息。

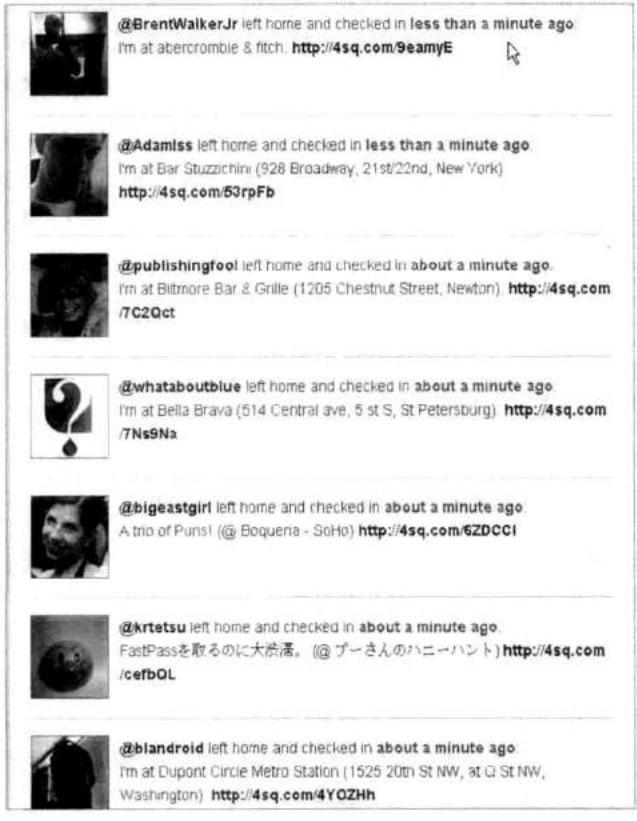

图2-4　ICanStalkU.com网站主页的经典场景

位置信息的泄露是社交网站令人不放心的因素之一。在上传照片的同时，你的位置信息可能在你毫不知情的情况下被泄露了。

像ICanStalkU这样的网站强调了信息泄露的危险。通过一则小故事（还有很多）便可以看到，这些位置信息如何被利用，使受害人遭遇入室盗窃和抢劫等，故事的链接如下：www.social-engineer.org/wiki/archives/BlogPosts/TwitterHomeRobbery.html。

不同种类的信息可以帮助你全面地了解目标。人们喜欢在Twitter上分享自己的地理位置、和谁在一起以及正在做的事情等。Blippy[①]能绑定人们的银行账号，然后向好友推送你的每笔消费信息，包括从哪里购买、花费多少等。含有地理位置信息的照片，以及Facebook这种用来分享个人照片、故事和其他相关信息的社交网站，是社会工程人员特别喜欢的信息源。只需片刻功夫，目标人物的住址、工作、照片、兴趣等信息就呈现在眼前了。

社交网站成为最佳信息源的另一个原因是可以匿名伪装。如果目标人物是一个刚离婚的中年男子，平时热衷于更新Facebook，那么你就可以假扮成一名希望结交新朋友的年轻女士。很多时候，人们在被拍马屁时，会泄露很多重要信息。结合伪装的技术，再加上人们通常认为自己见到、读到的就是真实信息这一安全漏洞，你便很容易得手。

6. 公开报告

公开数据可能来自目标企业内部或者外部，包括季度报告、政府报告、分析报告及公开交易公司的收入信息等。例如，邓白氏集团（Dunn and Bradstreet）以及其他公司的销售分析报告都能以极低的价格买到，而这些报告中通常会包含目标公司的大量详细信息。

稍后会详细讨论的还有背景查询服务，比如www.USSearch.com和www.intelius.com。还有一些类似的有偿查询网站都提供查询服务，价格从每次1美元到49美元包月不等。通过搜索引擎，可以免费查到很多有用的数据，但一些财务明细数据和个人信息就得通过这种合法的付费形式有偿获得。最令人震惊的是，有些公司甚至会向客户提供个人的社会保险号（Social Security Number）。

2.2.2 运用观察的力量

虽然观察并不能称为社会工程工具，但是简单的观察却能给你带来关于目标的不少信息。目标企业员工使用钥匙、门禁卡（射频识别卡）还是其他方式进入办公大楼？有没有指定的吸烟区？垃圾桶有没有上锁？办公大楼有外置摄像头吗？供电系统或空调机组等外围设备的维修公司是哪家？这些信息都可以给社会工程人员的入侵提供可能。

上面仅仅是通过观察可以得出答案的几个问题而已。花上一段时间观察目标，并用隐藏式摄像机录制下来，然后回去慢慢研究和分析，你会学到很多知识并且你的信息量也会暴增。

---

① 一种消费信息分享网站，当你的朋友刷卡购物时，你能马上知道他们买了什么，以及这些东西的价格和购买地点。

2.2.3　垃圾堆里找信息

难以相信在垃圾堆里能找出让我们获利丰厚的信息，就像难以想象我们为什么要去乐呵呵地翻垃圾一样。人们经常会扔掉发票、通知、信件、CD光盘、电脑、U盘以及其他种类繁多的设备和报告，我们可以从中收集到特别多的信息。正如前面提到的，如果人们连价值数百万的艺术品都会扔掉，那么只要认为某物是垃圾，人们都会不假思索地直接扔掉。

有时，公司认为直接将重要文件扔掉会不安全，于是便用碎纸机碎掉再扔，然而一些碎纸颗粒度不高的碎纸机粉碎过的文件还是能轻易拼回去的。如图2-5所示。

图2-5　粗线条单向粉碎过的文件依然有些文字可读

这张图展示的是粉碎后的一些文件，有些字还是可以被整体辨认的。这种情况下，只要肯花时间耐心地用胶带黏一下（如图2-6所示），便能将部分文件拼接回去，从而得到破坏性极强的信息。

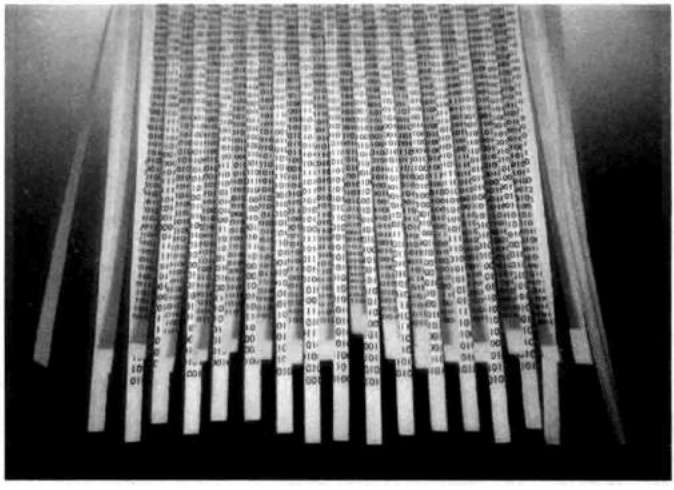

图2-6　只要肯花时间且有耐心，文档是能拼接回去的

不过，使用双向粉碎机进行销毁，就会粉碎得相当细，几乎不可能再拼接起来，如图2-7所示。

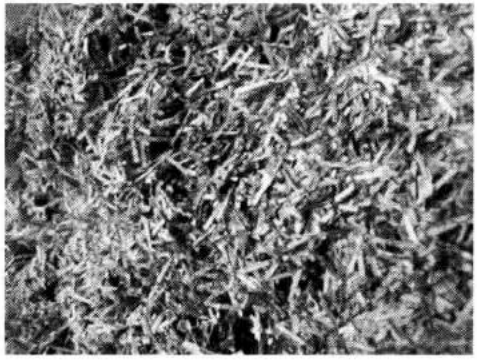

图2-7 很难想象粉碎前它是纸币

很多公司付费将已经粉碎了的文件交给专业公司焚烧。也有一些公司直接将粉碎完毕的文件丢给第三方处理，之后就不管不问了。你大概也能猜到，这样会令入侵者有机可乘。社会工程人员只要找到提供该服务的厂商，就可以轻而易举地冒充成过去收“垃圾”（粉碎过的文件）的工作人员。无论如何，翻找垃圾箱是一种快速收集所需信息的方法。不过，翻垃圾箱时一定要记住以下几点。

- **穿质量好的鞋子或靴子**。没有比跳进垃圾堆，然后被钉子戳到脚更令人抓狂的事了。确保你的鞋子合脚且鞋带系紧了，并能保护脚不为利器所伤。
- **穿深颜色的衣服**。这点不需要过多的解释。你肯定会穿那些丢掉也不会心疼的衣服，而且深色的衣服不容易被发现。
- **带一个手电筒**。
- **拿到了赶紧溜**。除非你是在偏僻到不可能被抓到的地方，否则最好是拿走一些垃圾袋，到其他地方去翻找。

翻找垃圾桶几乎总能找到一些非常有用的信息。只是有的时候，社会工程人员不需要去翻垃圾桶就能得到这些信息。第1章中有一个例子，详见http://www.social-engineer.org/resources/book/TopSecretStolen.htm。加拿大反恐部队计划建造一栋新的办公大楼，然而这栋大楼的一些规划蓝图被当做垃圾扔掉了，甚至都没有经过粉碎。蓝图中包括监控摄像头的安装位置、围栏及其他绝密信息。还好，发现这一图纸的人没有恶意，否则后果不堪设想。

正如该文章所写的，这则故事只是用来展示很多“愚蠢至极”行为中的一种，但是从社会工程人员的角度来看，翻垃圾桶确实是最好的一种信息收集方式。

2.2.4 运用分析软件

第7章将细致讨论社会工程人员会用到的专业工具集，这里仅作简单介绍。

Common User Passwords Profiler（“常用用户密码探查器”，缩写为CUPP）和Who's Your Daddy

（“谁是你爸爸”，缩写为WYD）是两款常用的密码分析工具，社会工程人员可利用它们分析出企业或个人可能使用的密码。

第7章将深入讨论这些工具的使用方法。WYD这样的工具可以将个人或者公司网站上的信息收集起来，根据网站上涉及的词语来创建可能的密码列表。人们通常会使用文字、姓名或者日期作为密码。这种类型的软件能够轻而易举地生成密码列表。

像Paterva制作的Maltego工具（第7章有详细介绍），简直就是信息收集者梦寐以求的。这款工具本身就可以帮助社会工程人员完成基于网页的被动信息收集和查询工作，不需要借用其他任何平台或工具。

之后，Maltego可以存储这些数据并在屏幕上用图形化的方式展现，以用于报告、导出或其他用途。这些对于分析公司的信息相当有用。

记住，收集数据的目的是了解目标企业及其员工。一旦社会工程人员收集到足够多的数据，如何最充分地利用这些数据信息来操纵目标便会了然于胸。应该将目标公司作为一个整体来分析，了解里面的员工大致参加哪些俱乐部、他们的兴趣爱好或者加入的社团名称。他们会不会向特定的慈善机构捐款？或者他们的孩子都就读于同一所学校吗？这些信息对于深入分析都很有帮助。

清晰明了的分析不仅可以帮助社会工程人员很好地伪装，而且还可以让他们知晓要询问哪些问题，什么时候适合打电话及哪天适合当面交流等，还有会令攻击变得更加容易的很多其他线索。

前文提到的所有方法，大多是现实生活中手动的信息收集方式，并未涉及信息收集的技术层面，例如，简单邮件传输协议（SMTP）、域名服务（DNS）、网络基本输入输出系统（Netbios）和简单网络管理协议（SNMP）。第7章中细致地讲解了Maltego软件中有关上述信息的收集功能。这些方法值得探讨，但是技术性较强，并不是本书所关注的“人性”入侵技术。

逻辑上，无论使用何种方法收集信息，首先浮现在你脑海中的问题可能都是：既然知道收集信息的地点、方式以及分类、存储并显示此信息的方法，那么如何使用搜集到的信息呢？

作为一名社会工程人员，信息收集完成后，必须开始规划如何攻击。为此，首先要建立模型，列出信息使用攻略。交流模型的建立便是最佳的开始方式之一。

2.3　交流模型

交流模型越精巧、越清晰，花在交流上的时间就越少。

——约瑟夫·普利斯特利（Joseph Priestley）

交流是将信息从一个实体传送到另一个实体的过程。交流需要至少二者间的互动，可以视为一个双向的过程，这里发生着信息的交换、思维的碰撞、情感的互动，或者想法上的共识。

这个概念和社会工程的定义非常相似，只是这里假定参与交流的人已经有了一个共识，而达成共识是社会工程人员和他人交流的目的。交流可以理解为这样一个过程：信息经过打包，由发送者通过传输媒介送达接收者，接收者解密收到的信息并给发送者送去反馈。所有的交流形式都需要有三个条件：发送者、信息和接收者。社会工程人员理解交流的原理对于构建合适的交流模型异常重要。对于社会工程人员，建立交流模型将帮助确定最好的传送和反馈方法，以及最合适的传输内容。

交流可以采用多种不同的形式。有听觉方式，比如演讲、歌曲和说话的音调，还有非口头方式，比如肢体语言、手语、辅助语言、触摸和眼神交流。

不论使用何种交流方式，对于接收者来说，信息的内容及其传达方式都会有确切的效果。

理解最基本的规则对于为“目标”建立交流模型很重要。一些规则不可以被打破，比如交流总是有一个发送者和一个接收者。同时，每个人的实际情况都会因经验和观念的不同而有所不同。

基于个人的现实情况，人们对事情的感知、体验和阐释总是会有所差异。正因为这样，人们对同一事件的看法会不尽相同。如果你有兄弟姐妹，一个简单的练习就可以证明这一点。问他们对于一件事情，尤其是一个情感事件的解释或记忆，你会发现他们对这件事情的阐释和你的记忆是完全不同的。

每一个人都有身体和精神的私密空间。很多因素会影响你决定是否要允许他人靠近或进入这个空间。无论在何种场合，你和别人交流时，都是在尝试闯入他们的私密空间。社会工程人员的交流是尝试将他人带入其空间，从而了解他人的状况。有效的沟通是试图把所有的参与者带入彼此的精神空间。只要有互动，就会发生这种带入，只是这太普通了，一般人通常不会注意到这点。

人际交流会传送两个层次的信息：语言的和非语言的。

交流经常包括一个文字或语言部分，不管它是以口头、书面还是其他文字形式呈现。通常也会有一个非语言的部分——面部表情、肢体语言，或者情感、字体等一些非语言信息。

暂且不论每一种类型的暗示（语言或非语言）的数量，交流的信息包被传送给接收者，然后接收者根据其自身的情况进行过滤。他将根据其实际情况形成一个概念，然后根据这个概念来解释这个信息包。当接收者解释信息时，便开始整理它的意思，即使那个意思并不是发送者的本意。发送者只能通过接收者给的反馈信息包，确定对方是接受还是拒绝了这个原始信息包，从而得知其信息包是否以既定的方式被接收。

这里所说的信息包是指某种沟通方式，包括言语、信件或发送的电子邮件等。接收者收到信息时，就会去阐释它。许多因素会影响最终被阐释出来的结果，如情绪的好坏、喜怒哀乐等。所

有这些因素和改变接收者认知的其他暗示都将有助于他阐释该信息。

社会工程人员的目的是利用这些语言和非语言的暗示，改变目标的感知，从而达到想要的效果。

下面包含更多的基本交流规则：

- 不要理所当然地认为接收者和你的情况完全一样；
- 不要理所当然地认为接收者将按照你的方式阐释信息；
- 交流不是一个绝对的、一成不变的事情；
- 如果有多人参与交流，应始终假设每个人的情况各不相同。

知道这些规则可以极大地提高你和他人交流的效率。这很好，但是交流和建立模型有什么关系？或者说，这又和社会工程有何关系呢？

2.3.1　交流模型及其根源

正如前面所说，交流的基本含义是发送一个信息包给既定接收者。这些信息也许来自多个信息源，比如视觉、听觉、触觉、味觉和语言。这个信息包随后被接收方处理，用于描绘出对方“所说的意思”。这种评估方法就是所谓的通信过程。通信过程最早是在1947年由社会科学家克劳德·香农（Claude Shannon）和沃伦·韦弗（Warren Weaver）提出的。当时他们发明了香农-韦弗（Shannon-Weaver）模型，也被称为“鼻祖模型”。

根据维基百科的定义，香农-韦弗模型“包含了信息源、信息、发送器、信号、信道、噪声、接收器、信息目的地、误差概率、编码、解码、信息率和信道容量等概念”。

香农和韦弗用图像定义这种模型，如图2-8所示。

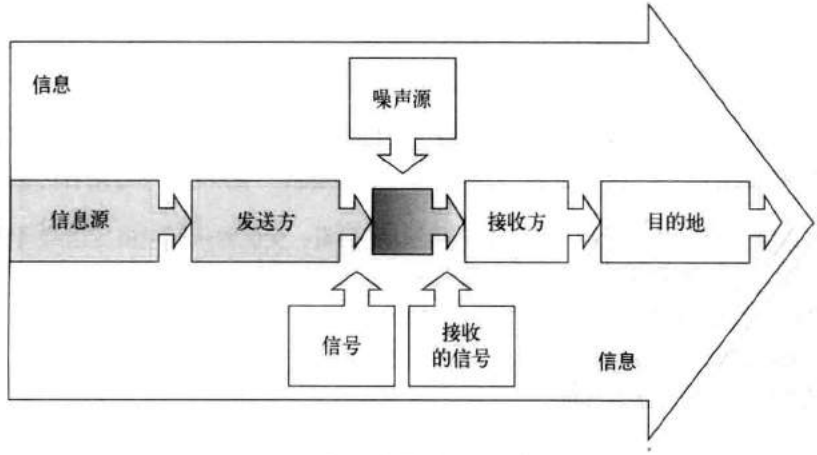

图2-8　香农-韦弗的“鼻祖模型”

在这样一个简单的模型（也被称为传递模型）中，信息或内容从发送者那里以某种形式发送到目的地或接收者那里。通信这一基本概念只是将通信视为发送和接收信息的一种方式。该模型的优势在于简单、通用和可量化。

香农和韦弗构建这个模型的基础如下。

- 一个创造信息的信息源
- 一个把信息编码为信号的发送方
- 一个适合传送信号的信道
- 一个从信号中解码（重构）出信息的接收方
- 一个信息发送的目的地

通过这一理论，他们总结出通信中存在的3个层面的问题。

- 技术问题——信息传送的准确性如何？
- 语义问题——信息表达的精确性如何？
- 效率问题——接收到的信息对行为影响的有效性如何？（社会工程过程中这最后一点很重要，必须牢记。社会工程人员的目的就是创造出一个自己想要的行为。）

差不多15年以后，大卫·贝罗（David Berlo）扩充了香农–韦弗的线性通信模型，发明出发送者–信息–信道–接收者（SMCR）通信模型。SMCR将模型分解成几个清晰的部分，如图2-9所示。

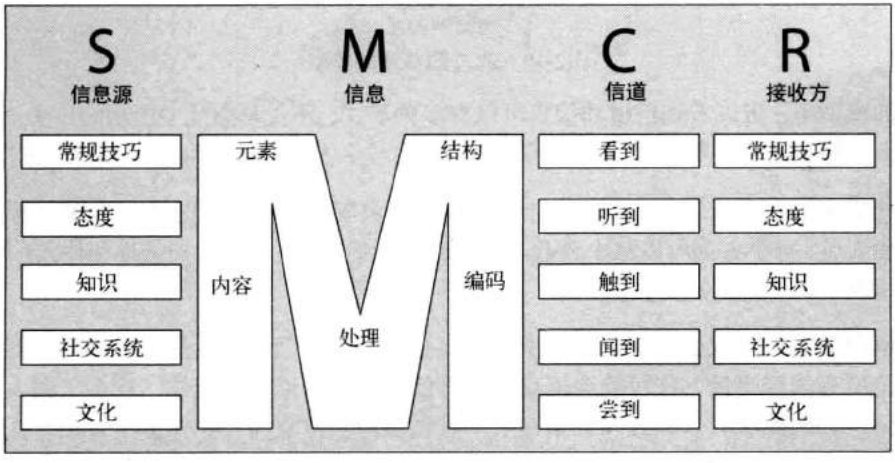

图2-9 贝罗模型

可以认为通信是信息传播的过程，该过程由3个层次的规则控制。

- 符号和标识的形式属性
- 符号/表情及其使用者之间的关系

» 符号和标识间的联系及其含义

因此，可以进一步地将通信定义为社交，即至少两个对象使用一系列共同的符号和规则进行互动。

2008年，另一位研究员D. C. 巴尔芒（D. C. Balmund）将自己的研究与行业先驱的成果结合起来，形成了通信的事务模型，如图2-10所示。

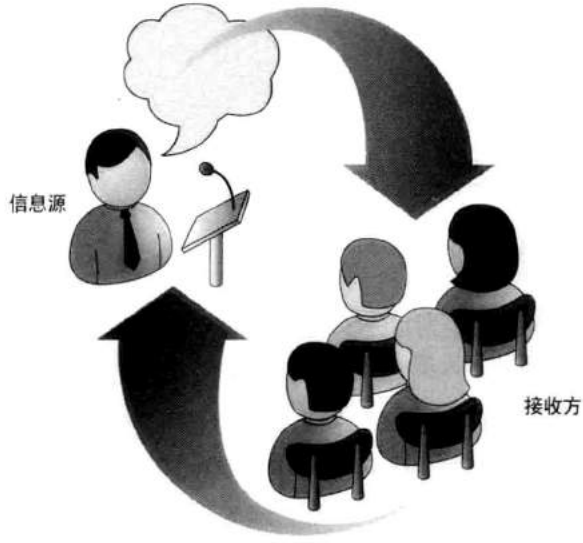

图2-10　改进的新通信模型

在他的模型中，可以看到信道和信息可以有多种形式，不仅是图片中所示的口头语言。信息可以有书面、视频或音频等形式，接收者可以是一人或多人，反馈也可以有多种形式。

将这些成果结合起来进行研究有助于社会工程人员制定出一个稳健的通信/交流模型。不仅是社会工程人员，每个人都可以从中获益。学习如何制订交流计划可以加强你和他人（例如配偶、孩子、上司或下属）之间的交流。

因为本书的重点是社会工程人员，所以需要分析一名社会工程人员可以从中学到什么。在读完该理论所有内容之后，你可能会困惑于怎么使用这些理论。请记住，社会工程人员必须是交流的大师，必须能够有效地进入且留在一个人私密的精神空间，并保证不冒犯目标或令目标反感。制定、实现和实践有效的交流模型是成功的关键。那么，接下来我们就学着制定这样一个交流模型。

2.3.2　制定交流模型

既然已知晓交流模型的关键要素，请以社会工程人员的视角来看待这些要素。

- **信息源**：社会工程人员就是要传递的信息或交流的源。
- **信道**：就是传达方式。
- **信息**：向接收者传达的内容。
- **接收方**：即目标。
- **反馈**：当有效地将信息传达出去之后，你希望对方给予的回应。

如何有效地使用这些要素呢？运用交流模型的第一步是带着目的动手实践，首先从社会工程中上演的经典剧情开始。

- 编写一个网络钓鱼邮件，尝试让25~50个雇员在工作时间访问一个嵌有恶意代码的非商业网站，以达到入侵其公司网络的目的。
- 登门拜访，伪装成一个前来面试的人员，装作不小心将咖啡洒在了简历上，并说服前台工作人员允许你用USB存储器插入到电脑里重新打印一份。

在制定交流策略时，你可能会发现反向使用模型大有裨益。

- **反馈** 你期望得到什么样的回应？期望的回应是，接收邮件的大部分雇员都点击它，这是理想状况。当然，只有少数甚至一个目标人物点击你也会感到高兴，但是你的目的，即期望的反馈是让大部分目标人物上当。
- **接收方** 这就是信息收集技巧派上用场的地方。你需要知道目标人物的全部信息。他们喜欢运动吗？他们中大多数是男性还是女性？他们是当地俱乐部的会员吗？休息的时候他们做些什么呢？他们成家了吗？他们是否年轻？这些问题的答案有助于社会工程人员决定传达什么类型的信息。
- **信息** 如果目标人物主要是25~40岁的男性，并且有几个人是足球或篮球联赛的球迷，那么目标人物就可能会点击运动、女人或者是赛事相关的链接。制定邮件的内容是很重要的，但也要仔细考虑语法、拼写及标点符号等。根据以往的经验，拼写不规范是网络钓鱼邮件露馅的主要原因之一。

  如果收到的邮件内容是“点击这里，输入尔的密码来验证尔的账户设定”，那么内容不正规就是其致命的问题。邮件必须拼写规范并且能够吸引目标人物的注意。即使目的相同，根据目标人物的性别、年龄或其他因素的不同，内容也应有所变化。如果目标主要是女性，发送同样的邮件就很可能会失败。
- **信道** 这个因素的答案很简单，因为你已经知道是用邮件作为传输方式。
- **信息源** 同样，这个因素你也无需费神，因为作为一名社会工程人员，你就是信息源。你的可信度取决于你作为一名社会工程人员的技术水平。

场景一：网络钓鱼邮件

目标人物是45名25~45岁的男性，其中有24名是梦幻篮球联赛的球迷，他们每天都会访问网站www.myfantasybasketballleague.com来进行投票。这些信息是通过论坛上的投票证实的。

我们的目的是要他们去访问一个归你所有的且可访问的网站 www.myfantasybasketballeague.com，该网址和他们经常访问的网址只有一个字母之差。从外观上看，这个网站是他们访问的那个网站的克隆，两者只有一点不同，即这个里面有个内嵌的恶意帧。网页中间会有个登录按钮，点击之后，会返回到真正的网站。在点击和加载之间的延时，嵌入的代码会入侵他们的系统。

怎样写这封邮件呢？下面是我写的一个范本。

> 你好！
>
> 这是来自“我的梦幻篮球联赛”的好消息！我们新增了一些功能，用户能够在投票时拥有更多的控制权，此外还有一些特殊的功能。我们正努力将这些功能提供给所有的会员，但是需要增收部分服务费。
>
> 我们很高兴地告诉你，前100名登录的会员可以免费享受这项全新的服务。点击邮件中的链接，到我们的活动页面，然后点击网页上灰色的登录（LOGIN）按钮进行登录，就可以将这些功能添加到你的账户中。网址为www.myfantasybasketballeague.com。
>
> 谢谢！
>
> 我的梦幻篮球联赛团队

这封邮件至少会使那24名联赛球迷感兴趣，诱导他们去点击链接，查看网站并且免费试用这些功能。

分析一下这封邮件。首先，它有一个吸引梦幻篮球联盟网站现有会员的邀请。然后，他们中的很多人会意识到这个邀请只限定给前100名，所以一收到邮件就会点击链接，而且很可能还是在工作期间。邮件链接的网站含有恶意代码，虽然大部分人会成为受害者，但是只要有一人落入圈套，社会工程人员的目的就已达到。

同样需要注意的是邮件的语法及拼写都是正确的，一个诱人的“钩子”和足够的诱惑力让人快速点击。这就是一封完美的钓鱼邮件，它的基础便是坚实的交流模型。

场景二：USB存储

现场进行社会工程要困难一些，因为是面对面进行的。当着目标的面，你只能“伪装”自己。你必须记住所有的细节，因为现场没有退出或者看提示的机会。要记住，我们往往只有一次机会打动别人，这一点很重要。如果这一出搞砸了，接下来也就不用再演了。

- **反馈**　这个场景的目的是让前台接待员接受你的带有恶意程序的U盘。在U盘插入电脑后，该程序会自动加载并提取系统中所有与账户相关的信息，比如用户名、密码、电子邮件账户以及包含系统中所有账户密码的SAM文件等，然后将这些数据复制到U盘指定

的目录下。同时，从前台的机器创建一个反向连接到你的服务器，从而获得该机器甚至公司网络的访问权限。我喜欢使用Metasploit Framework或者能够和Metasploit搭配使用的社会工程工具（见第7章）。Metasploit可以在受害主机上执行破坏性代码，并且有一个内置的Meterpreter处理工具。使用者可以通过编写脚本完成许多工作，包括键盘记录、屏幕截图及获取受害者电脑的信息等。

- **接收方** 有一个特定的攻击对象时，会感到棘手，因为如果想法不被目标所接受，那么你的计划就没有什么胜算了。你必须热情、友善，且具有一定的说服力。建立信任的过程也必须很迅速，因为时间太长将会让目标起疑心。但是如果处理得太快了，也会引起忧虑和害怕，从而失去机会。所以必须找到一个完美的平衡点。
- **信息** 因为你是面对面地传送信息，所以必须简洁明了。故事的基本内容如下：你在报纸上看到关于招聘数据库管理员的广告，然后打电话给人力资源部门的黛比。她说今天有预约了，但是你可以先把简历送过去，本周晚些时候再进行面谈。在你开车过去的时候，一只松鼠跑了出来，导致你急刹车，使得咖啡洒了出来，溅到了包上，弄脏了简历和其他物品。同时，你还有另外一个约会，但是又很需要这份工作，希望她能够通过你的U盘重新打印一份新简历。
- **信道** 面对面的口头交流，运用声音、面部表情和肢体语言。
- **信息源** 再强调一次，作为社会工程人员，你就是信息源，除非你觉得有必要找一个替身。

手中拿着沾上咖啡渍的文件夹，里面装些湿的文件，会使故事更加逼真。沮丧而无助的表情也会很有帮助。说话的时候要有礼貌并且真诚，以博得她的好感甚至同情。U盘中要有可打印的myresume.doc文件或myresume.pdf文件。PDF是最常用的格式，大多数公司会运行有漏洞的较老版本的Adobe Reader程序。确保简历不是一些特殊的格式，能被大多数人打开。

> 大多数时候人们会伸出援助之手。如果情节真实感人，他们会愿意帮助那些遭遇不幸的人。如果你缺少社会工程人员的天赋，我给你一个特别的建议，你可以在故事中加入这么一段：我今天过来顺路送女儿上学，她在爬过椅子和我吻别时，不小心将咖啡打翻洒进了我的包中。我当时已经离家比较远了，而且要迟到了，来不及回去。您能帮忙重新打印一份吗？

无论如何，这个故事通常都会成功，前台会将U盘插入她的计算机，导致计算机被入侵，我们也就成功入侵了公司的网络。

2.4 交流模型的力量

交流模型是一种很强大的工具，每个社会工程人员都必须掌握。交流模型中最困难的部分是确保收集到的信息是可靠的。

在前面提到的两个场景中，计划和模型准备不充分都将会导致失败。练习交流模型的一个好办法是写下一个操纵熟人（丈夫、妻子、父母、孩子、老板或者朋友）的模型，让他们按照你的想法和希望来行动。

设定目标，但不要怀有恶意，例如，使某人同意改变度假地点，或者说服同伴去你喜欢而他讨厌的餐馆吃饭，或是允许你买一件你通常不会去买的东西。不管你的目标是什么，将5个交流要素写出来，看看在具有书面计划的时候，交流的情形如何。你会发现在目标清晰的情况下，能更好地检验社会工程的交流方法，也更容易实现目标。依次列出如下的5点要素，并逐个填写好，然后在实施过程中将其关联起来。

- 信息源
- 信息
- 信道
- 接收方
- 反馈

交流模型能引出许多非常有价值的信息，没有它，社会工程人员的大多数行动都会失败。就像前面提到的，信息收集是社会工程的关键，但是如果只精通收集信息，却不知如何运用信息，那么终不过是白忙一场。

学习成为一名信息收集大师，然后与交流模型相结合予以实践。这只是个开始，但是它能改变你作为社会工程人员及在日常生活中与他人交流的方式。不过，要构建交流模型中的可靠信息，还有更多知识等待我们去挖掘。

学会如何提问是进行沟通、操纵他人乃至最终成为社会工程人员的关键所在，这方面的知识将在下一章中进行讨论。

第 3 章
诱　导

不战而屈人之兵，善之善者也。
——孙子

有效地引导别人将心里话说出来，是社会工程成功的关键。在人们见到你并和你交流时，你应该让他们感觉很自在，使之主动吐露心声。

你是否碰到过什么人，然后立刻觉得“哇，我喜欢这个人”？为什么会这样呢？他究竟有什么特质让你有这种感觉呢？是他的微笑，他的长相，他对待你的方式，还是他的身体语言？

或许是他与你的想法及期望值比较“一致”。他看你的眼神比较平和，没有偏见，你便立刻觉得和他在一起很放松。

现在设想你也有这样的潜力并能掌握这种能力。不要以为本章只是讲讲“怎样构建友好的关系”，因而置之不顾。本章讲述的是诱导。诱导是间谍、骗子和社会工程人员常用的一种强大的技术，医生、治疗师和司法人员也在使用。如果你希望保护自己，或者希望成为一名优秀的社会工程审计人员，那么就必须掌握这一技巧。有效地使用诱导会产生惊人的效果。

什么是诱导？它是社会工程中少有的几个强有力的工具之一，这也是将它置于社会工程框架顶层的原因之一。仅通过这一种技巧，就能改变人们对你的看法。从社会工程的角度来看，它能改变你在安全实践中的工作方式。本章将详细分析几个专业诱导的实例，深入分析这一技术在社会工程场景中的应用。

千里之行始于足下，我们还是得从基础开始。

3.1　诱导的含义

诱导的意思是引出、套出或者得出一个逻辑上的结论（例如某种事实）。或者，可以将诱导定义为一种引发或者诱发某种特定类型行为的刺激，正如“诱导他说出供词时颇费周章”一句中的意思。

请再看一遍上面的定义，如果没有起鸡皮疙瘩的话，那么你的理解就有问题。想想它的含义。有效地使用诱导意味着你能提出具有诱导性的问题，刺激别人采取你所希望的行动。对于社会工程人员来说，这意味着有效地使用诱导可以将你说话及提问的技能提升到一个全新的层次。从信息收集的角度来讲，专家级的诱导就是指目标愿意回答你的任何问题。

我们再深入一些，因为全球的间谍都会使用诱导技巧，所以很多政府部门会对其公职人员进行培训并给出警示，以对抗诱导。

在美国国家安全局的培训材料中，对诱导的定义如下：在貌似正常和平凡的对话中精妙地获取信息。

这样的会话可能发生在任何地方，比如餐馆、健身房及托儿所等。诱导使用起来效果很好，因为其风险较低且通常很难被察觉。大部分情况下，目标甚至不知道什么时候泄露了信息。如果被怀疑动机不纯，则可以“不过随便问个问题”为由假装生气、蒙混过关。

诱导的效果如此之好的原因如下：

- 大部分人希望看上去比较有礼貌，尤其是对陌生人；
- 专业人士希望自己看起来见多识广、很有才气；
- 如果得到赞赏，大部分人通常会越说越起劲并泄露更多的秘密；
- 大部分人不会为了撒谎而撒谎；
- 大部分人对貌似关心自己的人会比较友善。

大部分人都有这些特点，这使得诱导的成功率极高，也使得人们在说起自己的成就时口无遮拦。

有一次，我的任务是收集某公司的内部资料，我在当地举办的一次商业会议活动中碰到了目标。现场人比较多，我一直在寻找机会，后来终于发现目标走向吧台，于是我也在同一时间走过去。这类会议的目的就是要交换名片、结识更多的人，所以我主动上前打招呼并不会显得冒昧。

我说：“清静片刻？”

他笑着回答：“是啊，还好有这个地方，可以坐下来喝点东西。”

听到他点什么饮料后，我也点了一杯类似的。我伸出手，说道：“我叫保罗·威廉姆斯。”

“我叫拉里·史密斯。”

我拿出准备好的在网上定制的名片，说：“我是一家小型进口公司采购部的经理。”

他也拿出名片递给我，说：“我是XYZ公司的首席财务官。”

我笑着说：“你是管钱的啊，怪不得每个人都在那边围着你。你们公司具体是做什么的？”

他开始说起公司一些产品的情况，当说到一个知名产品时，我说：“哦，原来是你们公司做的啊，我喜欢那个产品。我在《XYZ杂志》上看到过，好像创造了销售记录啊。”我从之前收集的信息中了解到，他个人也很喜欢那个产品，所以我的赞美会起作用。

这时他开始显得有点骄傲了：“你知道那个设备在第一个月的销量就超过了它前后5个产品的销量总和吗？”

“是啊，我知道为什么，因为我自己买了5个。”我笑着附和。

经过一段时间，又喝了一杯之后，我了解到他们最近购买了财务软件、最近在度假的首席安全官的名字，以及拉里不久也要和太太一起到巴哈马度假。

这些看似无用的信息可不是毫无价值。我得到了关于他们的软件、人员和度假的详细信息，这在我计划攻击时会很有帮助。但是我没有满足，而是提出了一个更深入的问题：

“我知道这个问题会很怪，但是我们是个小公司，老板让我研究并购买一套门禁系统。我们现在使用钥匙，但是他认为RFID或者类似的系统会更好。你知道你们公司用什么吗？”

这个问题很敏感，会引起一般人的警觉。没想到他却说：“这个我可没有概念，我只负责签支票购买，不过我进门时使用的就是这个小卡片……”他拿出钱包中的卡片给我看。“我想可能是RFID，不过我只知道进门时晃一下钱包，门就开了。”

我们一起笑了起来，这些信息对我的攻击来说太有帮助了，我满载而归。你们可能注意到了，诱导与信息收集很相似且紧密关联。通过良好的伪装（第4章介绍）和诱导技巧，这个特别的信息收集过程会容易得多。诱导技巧的应用使得问题能够自然地提出，目标在回答这些问题时也觉得很自然。

了解到拉里正在度假中、他们公司使用的财务软件类型以及门禁系统，我就可以策划一次修复“故障”RFID打卡机及出勤记录钟的行动。我与前台的沟通很简单：“拉里在到巴哈马度假之前打电话给我，说生产部门有一个出勤记录钟没有正确注册，我来测试并分析一下，只要几分钟就可以完成。”前台连问都没有问，就让我进去了。

诱导所得到的信息使得前台接待人员对我伪装的角色没有丝毫怀疑，我成功地进入了目标单位。

通过简单、轻松、愉快的谈话就可以从很多人手中获取最好的信息。讨论到现在可以发现，重要的是为了实现最佳结果而明确定义你的目的。诱导不仅用于信息收集过程，也可以强化你的角色伪装，从而获取信息。所有这些成果依赖于定义清晰、经过深思熟虑的诱导模型。

3.2　诱导的目的

请回顾一下诱导的定义，其中清晰指明了你的目的。不过，你可以将其归纳成一条。社会工程人员想要目标对象做某件事，这件事可能简单到只是回答一个问题，也可能复杂到允许他进入一个限制区域。要达到这一目的，社会工程人员需要询问一系列的问题，或者与目标对象进行交谈，最终引导目标对象帮他达到目的。

信息是其中的关键。获取的信息越多，攻击的成功率就越高。因为诱导不具有威胁性，所以很容易成功。请想想一周中你在商店、咖啡馆或者其他地方进行过多少次无意义的短时谈话。谈话的真谛在于使用诱导战术，并且每天都以一种无恶意的方式使用。这也是诱导有效的原因。

在英国当红真人秀节目《骗术真相》的一期节目现场，主持人展示了社会工程攻击是多么地容易。这期节目中，攻击的目的是吸引目标对象参与一个被操控的撞大运游戏。为此，攻击者的一个同伴扮演成陌生人，与攻击者交谈，并且在谈话中表现出极大的兴趣。谈话吸引了周围的人，这样就很容易诱导目标，从而得到所期望的响应。这种方法屡试不爽。

不管采用何种方法，目的都是获取信息，随后利用这些信息引导目标采取社会工程人员所期望的行动。理解这一点很重要。后续章节还会介绍伪装以及其他操纵策略，但不要将它们和诱导相混淆。要意识到，诱导需要通过交谈实现，这一点很重要。虽然它和伪装、肢体语言以及眼神密切相关，但是相较于在谈话中进行的诱导来说，这些活动稍显逊色。

一些专家认为掌握交谈的艺术需要3个主要步骤。

(1) *表现得自然*。如果在交谈中显得不舒服或者不自然，会很快导致谈话失败。要想验证这一点，可以进行如下练习。与他人谈论一些你精通的领域，在这个过程中你可以录像或者让朋友观察，观察你的站姿、动作以及阐述知识的方式。这些行为可以反映出你的自信和自然。然后，尝试参与一些你一无所知的领域的谈话，同样进行录像或者让朋友观察。看看在这种对话中你试图发表“真知灼见”时，这些非语言方面有哪些变化。

这些练习会显示出你表现自然与表现不自然的差异。与你交谈的人很容易就会察觉这一点，不自然的表现会葬送你成功诱导的机会。如何在谈话中表现得自然？我们来看第2步。

(2) *拥有足够的知识*。你必须了解与对象交谈时所涉及领域的知识。本部分应该带有一个巨大的红色警告标志，但是书本中不能有这样的标志，所以我就强调一下：

最要紧的是你不能装成自己不可能成为的人。