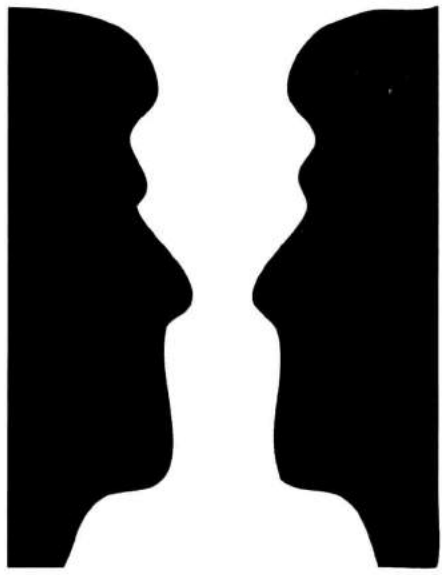

图6-4 你能通过改变现实框架看到不一样的东西吗

O lny srmat poelpe can raed tihs.

I cdnuolt blveiee taht I cluod aulaclty uesdnatnrd waht I was rdanieg. The phaonmneal pweor of the hmuan mnid, aoccdrnig to a rscheearch at Cmabrigde Uinervtisy, it deosn't mttaer in waht oredr the ltteers in a wrod are, the olny iprmoatnt tihng is taht the frist and lsat ltteer be in the rghit pclae. The rset can be a taotl mses and you can sitll raed it wouthit a porbelm. Tihs is bcuseae the huamn mnid deos not raed ervey lteter by istlef, but the wrod as a wlohe. Amzanig huh? yaeh and I awlyas tghuhot slpeling was ipmorantt! if you can raed tihs psas it on !!

翻译过来是：

只有聪明人才能看懂。

我不敢相信自己真的可以看懂这封邮件。这就是人类大脑不可思议的能力。根据剑桥大学的一项研究，单词中的字母顺序并不重要，唯一重要的是首末字母要正确。就算其他字母完全混乱，你也可以看懂。这是因为人类的大脑并不会阅读单词的每个字母，而是将它们作为一个整体来阅读。是不是很神奇？我曾经一直以为拼写很重要呢！如果你能看懂这封邮件，请转发！

我不知道这是否真的是剑桥大学的研究，但是有关这封邮件的很有趣的一点是，很多以英语为主要语言或者可以熟练阅读英文的人可能都可以毫不费力地阅读其中的文字，因为我们的大脑非常高效，能够从混乱中找出规律。

很多时候框架是难以察觉的。公司在市场营销中应用这一点，希望潜意识信息能够改变目标对其产品的认知。他们常常会使用微妙的框架方法植入信息。

例如，图6-5中显示的内容大家可能看到过很多次。

图6-5　你能识别出其中的框架吗

告诉你之后，你可能会彻底改变对FedEx标识的看法——这个标识中隐藏了一个箭头。在与标识设计者的访谈中，他说在标识中嵌入箭头是为了给人们植入一个有关FedEx服务的信息，用以显示FedEx公司的移动、速度和动态特性。

你找到了吗？请看图6-6，我将箭头用圆圈标注了出来。

图6-6　箭头表示永远移动的优质服务

FedEx不是唯一一家应用框架的公司。几十年来，各公司一直在他们的标识中嵌入框架信息，希望人们以其期许的方式记住和看待他们的公司。请看下面几个例子。

你能看出亚马逊公司标识中嵌入的框架信息吗（参见图6-7）？

图6-7　你能看到微笑着的满意的顾客吗

亚马逊的标识中有两个框架信息。一个是客户感到的快乐，以图片中的微笑表示。但是微笑同时也是一个箭头，这个箭头从A指向Z，表示亚马逊公司有你想要的所有东西。

另一个范例是立体脆（Tostitos）的标识。这是一个很有社交色彩的标识，请注意观察图6-8。

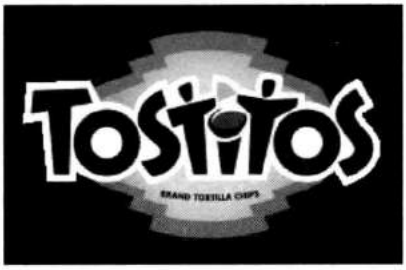

图6-8 这个标识会让你想和他人分享玉米片吗

图中央的两个T代表人们正在分享一块玉米片，中间是一碗洋葱番茄辣酱。2004年，立体脆公司召开了记者会，称："立体脆是一种'社会化小吃'。无论是聚会、观看盛大的比赛时，还是在简单的日常会面中，立体脆都有助于在亲友之间建立联系。这款新标识生动地体现了建立联系的想法。"

这些只是框架应用在市场营销中的一小部分例子。框架不一定要使用图形，重要的是目标感知的价值。目标对一件事物的认知会提高或降低它的价值。以高价位服饰店为例。当你走进去的时候，每件衣服都摆放得井然有序、整整齐齐，看起来非常完美。这时你的认知就是每件衣物的价值都与其所标注的高价相当。然而，如果你将其中的领带、衬衫或其他衣物从架子上拿下来，放到折扣商店中，将它们与其他2.5折商品放在一起，你会觉得这些物品的价值大打折扣。

营销大师利用这一现象影响公众对价值的认知。很多公司的框架战术都很成功，以至于人们会创造一种新型的词语来描述产品。

例如，每个人可能都会说："可以帮我将这个施乐[①]一下吗？"甚至在使用非施乐牌机器的时候也会这么说。施乐是一个品牌名称，不是机器类型。

最近的例子是，不管使用什么搜索引擎，人们都会说"你Google了吗？"，因为谷歌已经成为网络搜索的代名词。人们想用纸巾时，会说："请给我舒洁（Kleenex）。"

还有一些名称，大家可能并没有意识到它们其实是品牌名称（除非你生于它们出现的年代），其中包括：

- 阿司匹林（Aspirin）是德国拜耳公司的产品商标；
- 热水瓶（Thermos）是德国Thermos GmbH公司的产品名称；
- 邦迪（Band-Aid）是美国强生公司的商标；
- 飞盘（Frisbee）是美国Wham-O公司的商标。

① 施乐（Xerox）是最有名和最早的复印机品牌。——译者注

所有这些名字如今已经非常流行，人们在遇到任何类似产品时都会用它们来作为框架参考。我从不服用阿司匹林（通常服用另一品牌的药物），但是我会说“来两片阿司匹林”，而得到的总是我惯用的品牌，对此我很满意。

虽然存在大量与框架相关的信息，但是必须对这些信息进行概括和提炼，形成一些主要的原则，才能将它们运用于真实的社会工程中。前面对框架的概念及其在日常生活中的应用描述得很详细。在进入社会工程之前，先看一下框架联盟的不同类型。

6.3.3　框架联盟的4种类型

亚利桑那大学的戴维·斯诺（David Snow）和内布拉斯加大学的罗伯特·本福德（Robert Benford）合作写了一篇论文，标题为Clarifying the Relationship Between Framing and Ideology in the Study of Social Movements，详情参见http://www.social-engineer.org/resources/book/SNOW_BED.pdf。

斯诺和本福德认为，当个人的框架由于一致或互补而形成关联时，框架联盟就会出现，产生框架的共振，这是对群体进行框架转变的关键。斯诺和本福德随后列出了影响框架努力成果的4个条件。

- **框架努力成果的鲁棒性、完备性和彻底性**　斯诺和本福德找出了3个核心框架任务，对这些任务的关注程度将决定每个参与者投入的程度。

  3个步骤是：

  (1) 诊断框架的问题；

  (2) 分析并找出解决方案；

  (3) 如果成功了，号召行动。

  投入框架的努力越多，人们受框架影响从而采取行动的可能性就越大。

- **提议的框架和大众信仰系统之间的关系**　如果框架与人们的核心信仰或者信仰系统的价值没有任何联系，则人们会忽视该框架或提议的框架。

  如果一个人认为吃肉是虐待动物的行为，那么试图说服他去街上一家很有特色的西餐厅吃饭，肯定会失败的。框架必须与个人的核心信仰一致才能成功（除非你的目标是通过框架改变他的核心信仰），这对框架的应用非常重要。

  进行大规模框架改变的一个尝试是颇有争议的反对吸烟的广告，广告中志愿者将裹尸袋堆积在烟草产业大厦的大门口。裹尸袋代表每分钟、每小时或者每天有无数人因为吸烟而死亡。这次活动就是希望能改变那些支持吸烟的人的思维框架，让他们反思有多少人因吸烟而死亡。

- **框架与参与者现实情况的关联**　框架必须与目标本人相关。与目标经历的相关性必须可信且可验证。

  你不能通过市场营销框架鼓励那些每天吃不饱的人乘坐豪华邮轮，不管你多么擅于使用框架，结果只能是失败。如果要从框架发展到框架联盟，框架不能只是相关，还必须可证明，

哪怕这个证明只是存在于对象的思维中也没关系。

举个例子。2007年，广受欢迎的、可信度较高的新闻杂志《洞察力》（与《华盛顿时报》同属于一家公司）报道说，当时的总统候选人奥巴马曾就读于一所穆斯林学校，该校以教授激进和基本的伊斯兰教义闻名。这则新闻报道发布后，很多人立刻就相信了。为什么？因为这和他们的现实框架相吻合，这则消息似乎很可信，而且出自“可信的”媒体。

另一家声名卓著的新闻媒体CNN派出了调查人员，结果发现这个故事是伪造的，并将其发现报道了出来。

这是一个通过非常可信的渠道（新闻媒体）发布“事实”、改变人们对某一问题的思维框架的范例。那些想相信奥巴马是一个激进穆斯林的人很快相信了那个故事，消息飞快地传播开来。当研究揭示出故事是伪造的时候，很多人的思维模式又转变了回来。

反对的循环：对当前社会变迁的持续关注，以及框架在当前时代出现的时间点 世界上正在发生的事情会影响社会框架。想想几年前，如果建议美国或者其他西方国家的公司进行全身X射线扫描，不啻于痴人说梦。

提倡隐私保护的人会反对这一提议并会获胜，理由是他人会看到你的私处并可能保存这一照片以嘲笑你或者对你进行性骚扰。这一理由足以抹杀机器制造者在销售上所做的努力。然而，在美国发生“9·11恐怖袭击事件”后，恐怖主义活动兴起，于是这些机器被安装在了世界各地的机场，即便反对者大声抱怨，甚至拿出儿童色情法律这一强大武器都没有用。为什么？保障安全的社会框架已经发生了改变，所以这样一种新的做法就被公众接受了。

斯诺和本福德提议，当使用这4点构建适当的框架时，社会将通过框架联盟发生大规模的改变，比如社会运动所必需的那些改变。他们的研究重点在于整个社会，但是这些原则在处理小规模事件甚至是人与人之间的问题时也很有效。

前面讨论的主要是形成框架联盟的过程，事实上在这4个条件都满足的情况下可以产生4种不同类型的联盟。虽然上述很多方面针对的是框架在群体层面的应用，但是下面将讨论这4种框架联盟在个人层面的应用，展示如何将它们用在更小规模的事件上。这不仅适用于社会工程人员，也适用于想要和其他人在框架上达成一致的人。设想将你想进入建筑物的目标与保安想要阻止你的框架达成一致。将他的框架与你的伪装形成一致，就能确保成功。

必须记住一点，即框架从来都不是从头构建出来的。框架总是根据已有文化符号提出的，涉及个人信仰和经验的核心。懂得这一点将有助于你应用框架。

1. 框架桥接

凯西·马什普查和调查研究中心（Cathie Marsh Centre for Census and Survey Research）将框架桥接定义为就某一主题而言思想上一致但结构上互不关联的两个或多个框架的联接。

桥接并不是诱使他人相信你的框架，而是在你深入了解了他们的框架后，发现了两者之间的联系，然后可以利用这一联系将目标带入你的框架。

以你想进入一个区域、大厦或者得到某些信息为例，你的框架是你想完成这一点，而你接近的那个人的框架未必就是要阻止你，他甚至不知道你想要做什么。如果让他认识到这一点，他就会真的这么做，这样你也就没有机会了。

通过了解目标的工作、角色和精神状态，可以掌握他的思维框架，这样就可能发现一种联系，使得他更加容易地进入你的框架。

你的伪装是什么？你要接近的那个人会如何对待你伪装的角色？优秀的社会工程人员只有理解这一点才能成功。“门卫”对待推销员和苏打水送货员的态度是不同的。理解目标的框架意味着知道他将如何对待你——不是如何对待社会工程人员，而是如何对待你伪装的角色。

一个针对个人的例子是考虑你想让他人如何看待你——酷、有能力、有才气或者自信。教授想要显得智力超群，经理想要表现控制力，运动员想要显得冷静和强壮，喜剧演员则希望观众认为他有趣。所有这些都是个人框架，而且希望他人的框架思维能够一致。

以喜剧演员为例，如果碰到一个质疑者，这个人认为他不酷、无趣、不聪明、不自信，怎么办？因为质疑者的认识框架，他们会愤怒、不高兴、不安还是不在乎？如果这个喜剧演员坚持他的框架，他会转换周围人的认识，但是只有当他深入探索并了解一些人的框架来源后，他才能最终在两种框架之间建立桥接联盟。能够应对质疑者的喜剧演员可以先将他对自己框架的恐惧放在一边，对质疑者加以利用。

框架桥接联盟技术可以成为社会工程人员最有力的工具之一，但是需要一些准备工作以确保正确运用。

社会工程人员可以利用这一特殊形式的框架联盟，通过适当的伪装帮助目标将他们看到的和他们应该相信的内容联系在一起。请再次回忆伪装成技术支持人员尝试进入大厦的例子，你的着装、工具和言谈必须和目标认识的技术支持人员匹配。如果做到了，则桥接成功创建，联盟产生。

2. 框架放大

根据戴维·斯诺的定义，框架放大是指“对一个与某议题、问题或者一组事件有关的解释性框架进行阐述及激励”。换句话说，你要扩大或者把焦点放在目标的价值观或信仰上。通过将焦点集中在目标关注的价值观上，就能找到连接两者思维框架的区域，或者至少让目标认为存在一个联盟。

这种类型的联盟是4种联盟中最基本的，因为它主要是一种防御性方法。它通常会涉及强调某一事件比其他事件更加重要，从而使得这个事件能够轻松地与其他事件联系起来。

如果仔细研究前面所述的全身X光扫描器的例子，就能发现其中的框架放大方法。扫描器现在是作为阻止恐怖分子的设备进行销售的，是最近的恐怖主义活动使此类产品有了市场，所以在我们的框架中需要此类设备来满足需求。然而研究显示，市场上此类设备早已存在，只是在9·11

和其他袭击事件发生之前，人们一直拒绝使用。

利用“9·11恐怖袭击事件”以及人们因类似袭击事件而产生的害怕乘飞机的心理，扫描器公司将他们的思维框架与很多人的恐惧心理框架联系起来，从而使人们支持其在全球各机场部署这些设备。

框架放大的另一个用途就是它能够成功让现有的框架产生混乱，使得具有特定信仰的人远离他们的信仰。例如，很多人重视隐私并且认为自己有选择扫描方式的自由，但是他们被X光扫描设备的生产厂家所影响从而改变了框架，因为生产厂家着重强调了其他扫描方法不完善或者不安全，而且为了证明这一观点，还拿出了类似“内衣炸弹”的故事。这些战术放大了他们的框架，说明新的X光扫描设备更好、更安全，利用了人们普遍相信其他方法不安全的心理。

社会工程人员可以通过不同的方法利用这种联盟战术。例如，社会工程人员想要说服保安让他进入现场的垃圾箱区域。伪装成废品处理合约商的工作人员就是一个好方法。这一方法本身就可能成功，如果再说明其中一个垃圾箱出了问题需要处理，则会更容易达到目的，因为它是公司的一个安全隐患。放大这一思维框架可以让你和保安达成一致，让他相信最好的方法就是让你到现场进行检查。

3. 框架扩展

“*框架扩展*是一种变动的成果，通过将提议的框架的边界扩展到一群人的观点、兴趣，特别是情绪，将参与者引入其中。”换句话说，通过扩展框架的边界，将目标的其他主题或兴趣引入其中，就能与他们达成联盟或一致。

例如，那些支持环境保护或者“绿色”主张的人可能会将他们的框架扩展到反核运动，其主要原因就是他们担心环境风险。

不过，使用框架扩展战术可能会削弱人们对原有框架的支持，导致其在一定程度上丧失吸引力。如果在给定框架中包括太多的扩展，就可能出现这种后果，即逐渐地稀释并最终使人们对主框架失去兴趣。

甚至从个人层面来讲，简单的也是最好的。在使用这种框架结盟战术时，尽量使它简单、易于遵循。不要让连接的网络太过错综复杂，以致最终让目标失去兴趣。

社会工程人员可以通过第3章讨论的诱导技术使用这一框架联盟方法。当社会工程人员接近目标时，可以通过聚会中的闲聊，在不经意间套取目标或其公司的信息，也可以伪装成记者。这会赋予社会工程人员询问信息的“权力”，而这种信息通常很难获取。

4. 框架转换

“当提议的框架很难引起共鸣，而且有时与传统的生活方式、礼制以及现有的解释框架背道

而驰的时候，就需要进行框架转换。”换句话说，社会工程人员通过提出新的论点说明为什么他们的框架更好，意图将目标原有的框架思维和信念转换成社会工程人员希望的样子。

在框架转换发生时，需要新的价值观和理念来确保人们参与其中，并得到他们的支持。20世纪70年代，当保守运动的思维框架重新形成或者说转换成一种更加激进的环境保护运动时，就是一种大规模社会框架的转换。

在个人层面，通过宗教信仰的改变，框架转换每天都会发生。此时，个人框架或者整个信仰系统都会发生改变，与新的信仰和新的思维框架形成一致。

转换一个人的框架并不容易，这也是实践中一种最复杂的战术，因为它需要：

- **时间**　改变一个人的整个信仰结构不是一蹴而就的事，它需要用到其他联盟技巧，并且需要花费很长时间才能成功。
- **精力**　了解目标的框架并确定你希望他接受的新框架只是万里长征的第一步。他拒绝的理由和思维障碍是什么？找出这些实非易事。
- **教育**　知识就是力量。必须帮助目标理解你想要他“转换”到的新框架。
- **逻辑**　教育必须合乎逻辑而不全是以情感人。目标必须能够论证并认为其即将采取的行动合理。这只能通过逻辑达到。
- **深厚的感情纽带**　知识是行动的前提。逻辑能够说服他采取行动是对的，但是感情会促成行动的发生。如果你投入了感情，目标会感知它的存在。确保你表达的感情和感受与伪装的角色相匹配。如果你的伪装是指导顾问，而你却表现得像个啦啦队长，那么目标是不会与你结成结盟的。

如果能够让他人的框架与你的框架结盟并且形成一致，就能激励目标做你想要的事情。虽然上述4种结盟方式都很强大，但是只有成功掌握框架转换的社会工程人员才能具有无穷的力量。

请继续了解社会工程人员如何应用这些框架战术。

6.3.4　社会工程人员如何利用框架战术

本节将讨论社会工程人员使用框架战术的多种方法。其中一些方法很强大，如果能够熟练掌握并且准确地利用，你将成为一位影响大师。

要想在社会工程中真正使用框架战术，必须理解其中的4条规则。这4条规则将有助于你清晰地理解框架是如何工作的，以及怎样在社会工程过程中使用它。

请记住什么是框架。框架就是我们思维的概念性结构。这是一个很重要的信息，因为你的目标就是创建一个新的框架，或者与他人形成框架联盟，或者将目标带入你的框架。

这3个目标中的任何一个都需要你掌握下面4条规则，这样才能在社会工程过程中应用框架战术。

规则1：你说的每件事都会唤起一个框架

人们的思维过程就是描绘事物的过程。这一事实是不可能更改的，但是你可以利用它实现自己的目标。

如果我开始和你讨论你的老板，你的大脑就会对其进行描绘。如果我说他在外面打手机并且很愤怒，你的大脑就会开始描绘他愤怒的面容、肢体语言和所说的话。你无法控制这些，这一思维框架会激起你的情绪和反应。

用话语进行描绘是使用框架的一种强大的方法。通过精心选择用词，可以让目标的大脑描绘你想让他描绘的事物，将其移动到你设定的框架中。

你听过某个你认为特别擅长讲故事的人讲的故事吗？为什么？他擅长的原因何在？他能够描绘心理图景，让你在头脑中看见事物，从而激起你的兴趣并融入其中。这一技巧对社会工程人员来说非常重要。这并不是说任何时候都要像讲故事一样说话，但是你要牢记自己准备的词句，因为这些话具有在目标的头脑中勾画情景的强大作用。

这里有个简单的例子：我告诉你我昨晚吃的是意大利面。如果你不是美食家也不是意大利人，或者上次吃意大利面的经历不是那么愉快，那么你的思维框架就不会很强大，也就会无动于衷。

如果我告诉你昨晚我妻子用她自己种的番茄和罗勒做了美味的番茄酱，其中还加入了新鲜的大蒜和牛至，并用红酒调味，之后她将番茄酱浇在精心烹制的面条上，并配以自己做的蒜香面包。这种描述会引起你怎样的反应呢？

不管你是否喜欢意大利面，大脑中都会出现一碟美味的食物。这就是在面对目标时精心选择词句的结果。这种方法描述性更强、更有画面感，也更有冲击力。然而社会工程人员也要小心，你的描述不能太过戏剧化。你的目的是通过话语描绘出一幅画面，而不是让目标关注你或者你的表达。

规则2：框架中定义的词句会唤起思维框架

不必使用最确切的字词来为他人描述你所设想的框架。例如，在阅读下面的句子时，你想到了什么？

“我看到昆虫在网中挣扎想要逃离，但是没能成功。一会儿工夫，它就被包裹在茧中，成了别人的晚餐。”

请注意，我并没有提到蜘蛛，但是你已经想到它了。可见我可以在不提及蜘蛛的情况下让你想到它。这一有关影响和框架的强大规则，使得社会工程人员可以通过间接表达来控制对象的思维。

旨在帮助人们提高表达能力的国际性组织Toastmasters，教导其会员通过语言调动听众的情

绪来打动他们。如果你讲的故事能够让目标描绘出你设想的框架，并让他们投入感情，你就能更好地主导对话。

同样，使用这种框架方法需要事先计划。这一规则的强大之处在于，目标的大脑在处理你提供的信息并生成你描绘的心理图景时，你可以植入想法。与我直接描绘美味意大利面不同，这一规则允许目标自由描绘。

在前面意大利面晚餐故事的结尾，我可以说："之后我妻子将番茄酱浇在了精心烹制的面条上。什么样的面条？我不会告诉你，你必须自己想象。"当你的大脑开始描绘的时候，我会说："当我用叉子卷面的时候，酱很浓稠，附着在每一根面条上。"

这描绘的正是意大利面。还有其他面条需要用叉子卷动吗？（我知道有，但你已了解了重点。）

规则3：否定框架

如果我告诉你不要想象蜘蛛在网中的情景，你会首先在大脑中想象蜘蛛，然后告诉自己不要去想它。

这种否定框架战术很强大。告诉目标要小心、当心或者提防某事，会自动将其引入你想要的框架。这种战术常被专业的社会工程人员使用。在我与一群社会工程人员交流的时候，每个人都同意这种战术很有用。

在一次审计中，我故意丢下几个带有恶意代码的U盘，希望公司里的某个人会不假思索地运行它们。我走近一个已获得其信任的员工，说道："约翰，我听说发出的备忘中提到要注意一些丢落的U盘，他们现在正找呢。"

事情就是这样发生的，你是管理员，丢下几个装有恶意文件的U盘，现在告诉别人要找到它们，这在本质上等于植入了让他们执行你命令的种子。这种表达方式消除了他们在找到带有恶意文件的U盘时的担心，让他们在找到的时候会插入电脑查看这个U盘到底是谁的。

规则4：让目标思考框架会强化框架

每次大脑在关注或考虑某事的时候，该事件都会得到强化。你让目标对你想让其接受的框架考虑或者描绘得越多，框架也就越容易得到强化，目标也就越容易陷入其中。

我们来回顾一下第2章所述的通信模型，分析一下社会工程人员发出的消息是怎样对目标产生影响的。

有一次我去印度旅行。我已经忘记新闻中提到的确切事件了，但是我记得当时乔治·W.布什总统让欧洲人民很生气。我浏览新闻站点，看到欧洲国家的人们把貌似布什的玩偶悬挂在街上，然后用美国国旗将玩偶包裹起来并焚烧殆尽。

我被当时的情景震惊了，当晚和妻子通话时说："哇噢，有关欧洲发生事件的这些新闻真是

疯狂，是不是？”

她没有听到任何有关这方面的事情。为什么？新闻媒体和新闻站点主宰并操纵了人们的思维框架。

社会工程人员可以通过学习媒体的这种技巧来提高自己的能力。通过省略、遗漏故事的细节，或者干脆不提这件事，媒体让人们得出了似乎是自己的结论，事实上这一结论来自媒体。

社会工程人员也可以这样做。通过省略某些细节，仅“透露”想要透露的细节，可以创建出他们想要目标思考或感觉的框架。

媒体使用的另一个战术是贴标签。当想要将某事定义为正面的时候，他们会说：“强大的防卫……”或者“健康的经济发展”。这些语句描绘出的心理图景是稳定和健康，会帮助人们得出正面的结论。同样的规则也适用于否定的框架。类似“伊斯兰恐怖分子”或者“阴谋论”这样的标签描绘出的就是负面的图景。

可以利用这一技巧，通过描述性词句为事物打上标签，将目标带入你设定的框架。有一次，我昂首阔步地往前走，突然被门卫挡了下来，于是我惊讶地看着门卫，歉意地说：“哦，昨天那个乐于助人的保安汤姆检查了我的证件后让我进去了，所以我以为有记录呢。”

将前面一个门卫说成“乐于助人”让现在的门卫自动进入了我设定的框架。如果他也想得到这样一个美好的标签，也应该像汤姆一样“乐于助人”才行。

框架之所以有效，是因为它扭曲了事实但又不至于太过虚假，所以仍然可信。社会工程人员可以创建想要的图景，但不能完全脱离事实。

我读过一个白皮书，标题为Status Quo Framing Increases Support for Torture，作者是克里斯蒂安·克兰多尔（Christian Crandall）、斯科特·艾德尔曼（Scott Eidelman）、琳达·斯基塔卡（Linda Skitka）和斯科特·摩根（Scott Morgan），他们是来自不同大学的研究人员。白皮书中提供了一个非常有趣的数据集，让我对这一课题兴趣盎然。在美国，似乎大多数人都反对在战争中使用拷打的方法获取情报信息。这一研究的目的就是要了解，研究人员是否能够通过不同的框架表达，让一部分人同意拷打并非不可接受的方法。

他们的采集样本有486个人，这些人要阅读两段文字。

第一段内容如下。

> 新闻中说，美国军队在中东地区审讯嫌疑人时采用了压力审讯的方法。根据一些报道，这种压力审讯是一种新的审讯形式，首次在美国军队中广泛使用。美国军方使用了多种方式，包括将嫌疑人绑在木板上浸在水中、将嫌疑人的脸按在睡袋中、用绳子将嫌疑人绑成痛苦的姿势长时间悬吊。此外还会让嫌疑人独处，并且连续多日不眠不休。

这段话让人们认为这些是美国政府为了获取信息而采用的新方法。

第二段内容如下。

> 新闻中说，美国军队在中东地区审讯嫌疑人时采用了压力审讯的方法。根据一些报道，这种压力审讯并不是一种新的审讯形式，已被美国军队使用了40多年。美国军方使用了多种方式，包括将嫌疑人绑在木板上浸在水中、将嫌疑人的脸按在睡袋中、用绳子将嫌疑人绑成痛苦的姿势长时间悬吊。此外还会让嫌疑人独处，并且连续多日不眠不休。

这一段与上一段的内容基本一样，只是第2句话被替换为“根据一些报道，这种压力审讯并不是一种新的审讯形式，已被美国军队使用了40多年。”

这两段话的思维框架分别是“这些是全新的方法”和“这些方法已使用了几十年，经过了反复的检验”。在更改了框架后，结果如何？

白皮书中描述了研究者的测量方法。7个选项形成了一组相互依属的基础变量。这些选项对应7个不同的“按钮”，依次为：强烈反对、基本不同意、有些不同意、不确定、有点同意、基本同意和非常赞同。对各项进行反向打分，得分越高表示越赞同。

结果呢？“描述现状的操纵方法对拷打的最后评价产生了影响——当表述为‘长期使用’而不是‘新方法’的时候，拷打的评分更加正面。让拷打看似一种常用的审讯方式，这提高了参与者对该方法的支持度，也增强了其合理性。”

通过改变框架中的一小部分，研究者和大量参与者建立了联盟，让他们同意（大体上）拷打是一种可以接受的方式。

文章继续评论道：“它们可以应用于很多领域，可以影响人们的判断、决策、审美观以及政治倾向。”而结论是：“适当改变呈现、设定道德选择和价值困境的方式，会对人们的政治选择和政策产生意义深远的影响。”

这一实验证明了框架战术的强大，因为它甚至能改变人们多年秉持的核心观念、判断和决定。对社会工程人员来说，大部分时候不需要设定这么高的目标，并不需要尝试改变人们的观念，只需要让人们采取一些细想时会觉得不妥的行动。

采用这4个框架规则并进行细致的计划，能够让框架成为摧毁性武器，不过这也是恶意社会工程人员每天都在使用这一战术的原因。在美国，特别是“西方文化”中，人们接受的教育就是要接受框架的影响、接受被灌输要思考什么以及怎样思考。

如果我15年前告诉你，几乎每个电视节目都是看真人生活秀，你一定会笑我。为什么？因为观看那样的节目似乎无聊又愚蠢。然而在2006年，《洛杉矶时报》声称现实类电视节目的数目提高了28%（详见http://articles.latimes.com/2010/mar/31/business/la-fi-ct-onlocation31-2010mar31），

而且在此之后没有明显的回落，因为观看这类节目显示了时尚与新潮，因为我们被告知这种节目好看且有趣，而且所有人都在看。这类节目作为一个例子，说明了一件几年前大部人认为愚蠢的事情，现在可以变成适合做的事。

框架绝对是一种艺术形式，在与沟通和影响等科学相结合之后，就会变成熟练社会工程人员手中的强大武器，通过以某种形式传达信息后，社会工程人员就能够“轻易”地与目标形成联盟，促使目标在不会感到内疚的情况下采取行动，改变目标对现实的感知。

框架和影响是社会工程的重要组成部分，但后者经常与社会工程的“黑暗角落”联系起来。本书文前提到了这些角落，下一节内容会改变你对“影响”的看法。

6.4 操纵：控制你的目标

对很多人来说，操纵是一个很黑暗的话题，因为在通常的描述方式中，它会让人产生一种畏惧感。

看一下在互联网上找到的几个关于操纵的定义，就能理解上面一段话的含义。

- “运用精明、迂回的影响，尤其是为了自身的利益”
- “精明、迂回地影响或控制”
- “巧妙地控制或者影响（他人或自己），通常是为了个人的利益”

通过上面的定义，我们能够明白为什么很多社会工程人员偏爱这一主题。通过自身的技巧控制或影响他人，达到自己的目的，你能想象这有多大的吸引力吗？

从阴暗的洗脑手法到销售员使用的隐晦暗示，操纵是每个社会工程人员都应该学习并精通的技巧。操纵的目的就是要战胜目标的批判性思维和自由意志。当目标基于熟悉的流程无法作出决定的时候，操纵的人可以给他灌输想法、价值观、态度或者道理。

操纵有6种使用方法，适用于洗脑及那些不那么阴险的方式。在深入探讨之前我们先简要熟悉一下各个方法。

- **提高目标的暗示感受性** 在最极端的情况下，睡眠或者食物匮乏会提高目标的暗示感受性。在缓和的方式下，时间紧迫的隐晦暗示会让目标更容易受影响。
- **获取目标环境的控制权** 这一技术包括的范围很广，从基本的方法，如控制目标能够访问的信息类型和数量，到某些微妙的方法，如获取目标的社交网站的访问权。在社会工程的背景下，如果能够访问目标的社交媒体，就可以查看目标的交流信息，并对目标收到的信息进行控制。
- **制造怀疑** 动摇并深挖目标的信仰系统，这对控制目标采取你想要的行动会大有裨益。

从社会工程的角度来看，这种方式必须巧妙。不能一上来就贬低目标，相反，可以质疑他们执行的制度、工作或者信念，逐步影响目标作出理性决策的能力。

- **制造无能为力的感觉**　这是应用于战时审问的一种恶意方法，会令目标对自己的信念逐步丧失信心。社会工程人员可以利用这一技术，通过显示你从某一权威人物处获得的“事实”，对目标釜底抽薪，让他们感到无能为力。
- **让目标产生强烈的情绪反应**　强烈的情绪反应包括怀疑、罪恶感及耻辱等。如果情绪足够强烈，就会让目标改变整个信念系统。社会工程人员必须小心翼翼，不能制造破坏性的负面情绪，但是制造害怕失去或害怕受到惩罚等情绪反应，对最终的社会工程目标达成会起到促进作用。
- **严重威胁**　对生理痛苦或者其他可怕情形的畏惧能够让目标在压力之下崩溃。同样，除非是伪装成商业间谍，大多数社会工程人员是不会使用这一方法的。在常规的社会工程活动中，这种方法通常利用权威制造强烈的恐惧感或者有潜在损失的感觉。

不过大部分时候，操纵并不是这样极端。设想一个最简单的场景，你在一个拥挤的房间中，有人叫你的名字，你会有什么反应？你通常会转身问：“谁啊？”此时你就被操纵了，只不过这不一定是带有恶意的操纵。

在心理层面，被操纵的情况更加复杂。请注意前面的反应发生时的具体情况：大脑听到你的名字，你自动形成一个应答（“谁啊？”）。应答和发出声音之间的连接非常短。即使你不出声响应或者那人叫的并不是你，大脑在接收到问题时也会形成应答。

近距离听到两个人交谈并且无意中听到一个问题，你的大脑就会形成一个应答。应答可能是头脑中的一幅画面或者一个声音。如果目标无意中听到两个人在谈论类似他头脑中的某个人，他的大脑中就会出现一个画面。如果你听到两个人在说小鸡过马路的笑话，大脑中就会出现小鸡、马路或者整个场景。

这种类型的操纵对你来说只是个开始，另一种操纵技术则需要条件反射。

通过不断地适应，人们会将特定的声音、行为与感觉和情绪相关联，形成条件反射。如果每次提到积极的事物时目标都会听到钢笔的咔嗒声，那么一段时间后，目标就会将这种声音与积极的感觉相联系。

一个最经典的条件反射的例子出自伊凡·巴甫洛夫之手，我们常称之为“巴甫洛夫的狗”，第5章曾讨论过这个例子。问题是我们能否将这种训练施加于人。虽然让目标流口水并不在大多数社会工程人员的优选策略列表中（这是一个笑话），但是能够训练目标在接收到特定输入时，按照你想要的方式响应吗？

要找出答案，请继续阅读下面的小节，其中提供了几个商业和市场营销领域的操纵实例，为我们讨论和分析如何进行个人层面的操纵奠定了基础。

6.4.1 召回还是不召回

2010年5月，《华盛顿邮报》报导了一个有趣的故事，详见www.washingtonpost.com/wp-dyn/content/article/2010/05/27/AR2010052705484.html。儿童用羟苯基乙酰胺（Tylenol）、布洛芬制剂（Motrin）、可他敏（Benadryl）和仙特明（Zyrtec）的制造商，在液态非处方药中发现一批布洛芬制剂存在缺陷，但是又不想花费一大笔钱来召回，那么公司是如何回应的呢？

他们使用了操纵战术。公司雇用了许多合同工，让他们到每家药店买下所有布洛芬制剂，然后销毁。不幸的是，由于某合同工的疏忽，写有该计划的一份文件失落在了其中一家药店，随后这件事就被报告给了美国联邦药品管理局（FDA）。

根据备忘录，FDA确实让该公司分4次召回所有问题药品，其中的一次召回就达到了1.36亿瓶。只是已经太晚了，因为报告称已经有775名儿童和婴儿由于服用这批药品产生了不良反应，最终有37例病亡。报告中并没有说是问题布洛芬制剂还是对布洛芬制剂的反应导致了死亡。那不是我们讨论的重点。

这是一个非常阴险的操纵实例，至少是尝试操纵。为了保护公司形象，他们竟然放弃了正确的流程且不顾全世界儿童的生命安全。他们尝试对系统进行操纵，结果有人因此而丧命。遗失在药店的文件内容主要是讨论合同工怎样奉命买回产品，只字未提“召回”。

事情败露后，他们执行了很多有趣的操纵战术。他们歪曲事实说之所以这样做，是因为专家认为该制剂对儿童来说并不存在很大的风险。

在此之后，他们正式道歉，并且解雇了6名高管，然后开始进行真正的操纵了。在被质询时，公司说他们不是在尝试人们所说的“隐秘地召回”，而是要检验所谓的有害批次药品，所以让合同工将药品买回来测试。如果发现确实有问题，公司会采取正确的流程。公司尝试使用操纵战术中的*转移*方法，将人们的注意力从他们的事实行为上转移，以使情况看起来没那么糟糕。他们还使用了掩饰方法，操纵那些不认可他们行为的人，声明公司正在尝试测试以确定是否需要召回。

这种类型的操纵值得讨论，因为转移策略也适用于个人层面的操纵。如果你去了不该去的地方，并且被抓住了，那么编一个可信的故事有助于你操纵目标，让你顺利过关。将目标的注意力从当前问题上转移，会为你赢得时间，改变目标的关注焦点。例如，如果你被保安人员逮个正着，不要紧张，冷静地看着他说：“你知道我在这里做什么吗？你听说一些包含非常重要数据的U盘丢失了吗？我们要在明天上班之前找到，这非常重要。你要检查盥洗室吗？”

很多人可能从没有听说过布洛芬制剂召回事件，这也显示了公司在操纵媒体和司法系统方面做得很好，所以没有成为人们关注的焦点。不管怎样，这个故事展示了转移和掩饰方法在操纵战术中的使用。

6.4.2　焦虑的最终治愈

1998年，世界上最大的制药公司之一史克必成（SmithKline Beecham）发起了一波广告宣传，意在向大众传播“社交焦虑症”的概念。他们发布了50个新闻故事及调查，提出“你有社交焦虑症吗？”之类的问题。这些测试和调查都旨在告知人们什么是社交焦虑症以及如何判断自身是否患有该病症。

之后，他们又更改了医学杂志中的宣传广告文案，由“帕罗西汀（Paxil）意味着……从抑郁症、恐慌症和强迫症中恢复平静”改成了“让他们知道自己能……第一种也是唯一一种获得认可的社交焦虑症治疗方法”。这一转变花费了公司大约100万美元。

1999年，他们又发起了新一轮耗资3000万美元的宣传，在平面媒体和电视上宣布史克必成找到了治愈社交焦虑症的良药，它的名字就是帕罗西汀。公司买下了当时一些热门电视节目中的固定节目档，使用调查和测试中获得的数据，吹嘘统计数据表明有1000万美国人患有社交焦虑症，现在他们有希望了。

到2000年，帕罗西汀在这一快速增长的市场中获得了一半的份额。公司斩获“2000年美国新型抗抑郁药（选择性5羟色胺再吸收抑制剂）零售处方市场的第一名”。2001年，FDA批准该公司销售帕罗西汀，用于治疗一般性焦虑症和创伤后应激障碍。

“9·11恐怖袭击事件”导致所有抗抑郁和抗焦虑药物处方量的巨幅增长。在那段时间里，帕罗西汀的广告定位是能够解决恐怖袭击后人们普遍具有的恐惧感和无助感。

我并不是说这类药物完全没有作用，也不是说公司的动机险恶，但是我发现这个案例中对市场的操纵特别有趣，开始时是教育和宣传，最终是销量的大幅增长，在此过程中还创造出了新型的失调。

这种问题构造的操纵方法常用于市场宣传，但是也应用于政治甚至个人层面，首先提出一个可怕的问题，然后提供“事实”作为证据，证明你所说的是真实的。在一期《骗术真相》节目中，保罗·威尔森设置了一个场景，在骗局中他让一位明星从商店里偷CD。商店雇员扣押了明星，等待警察的到来。之后保罗走了进来，说自己就是警察，还将他的钱包在对方眼前晃了一下，钱包中只有他小孩的照片，然后他“逮”走了明星，并且将CD和收银机中的现金一起作为证据带走了，没有人提出质疑。这个故事非常适用于说明这类问题构造的操纵方法。保罗有一个问题（小偷明星），然后将自己装扮成问题的解决方案（警察）。不管场景如何，在提出你的要求之前，要构造一个问题，以方便你这个好人出场，而那个问题会让你想操纵的人接受你的要求。

6.4.3 你不能让我买那个

卡马特[1]。我很想在这一节只写这一个词，但感觉还是得多解释一下。卡马特提出了一种思路，称为产品陈列示意图或者货架图，通过这个图告诉零售商怎样基于产品的颜色、尺寸和其他标准来展示其产品，以刺激顾客购买和消费的欲望。

货架图旨在优化视觉效果和商品摆放。

这些图的使用就是一种形式的操纵，因为研究者仔细分析了人们逛商店、思考和购买的方式。通过对这些方面的理解，他们设计出了控制视觉输入的机制，从而刺激购物者的购买欲望。

软件以及整个公司都致力于计划和执行这些货架图，以期达到让客户尽可能多购物的效果。

他们使用了3种操纵购物者的布局方式。

- **水平放置商品** 要提高顾客对特定商品的注意力，可以将此种商品一个挨一个地水平放置。一些零售商发现，一种商品的最小放置区间在15~30厘米，这样才能有效吸引顾客的注意力（参见图6-9）。

图6-9 水平放置同样或类似的物品以吸引顾客的注意力

- **垂直放置商品** 垂直放置商品是另一种布局方式。这种方式下，每种商品占据不止一层货架的位置，以占据15~30厘米的放置空间（参见图6-10）。

① 财富500强公司之一，总部位于美国，主要从事零售业务。——译者注

图6-10　同样的商品放置在多行货架中

» **块放置**　具有一定共性的商品放置在一个块（品牌）中。可以并排放置、上下堆叠、中心环绕，也可以使用磁力挂钩等各种方式（参见图6-11）。

图6-11　类似商品或品牌的块放置方式

货架图不是操纵购物者的唯一方法。还有一个测试，即在商场内循环播放特别设计的音乐。结果是在播放音乐的情况下，购物者在大卖场内的购物时间平均会增加18%。

杰–查尔斯·沙巴特（Jean-Charles Chebat）和理查德·米琼（Richard Michon）在《商业研究期刊》上发表了一篇有关加拿大大型购物中心的研究论文（详见www.ryerson.ca/~rmichon/Publications/Ambient%20odors.pdf）。研究者在空气中喷洒特别设计的香味，意图促发购物者的快乐情绪、刺激购物。结果是在一周的研究时间里，平均每个购物者会多买50美元的东西。

去大型购物中心和水果店的体验肯定不一样。不过，从这些方法和实验中我们能学到很多。了解大脑对事物的分类方法，有助于你组织自己的“货架”，以便操纵目标的感觉、情绪和思维。

再来说一下色彩，它们是操纵目标情绪的一种主要方式。放置商品的原则同样适用于色彩。你的衣物或者用品的色彩能够对目标产生影响。很多研究的主题是色彩及其效果。下面列出了一些通过色彩影响人们思维或情绪的方法。

- **白色** 白色经常和纯洁、明亮以及干净联系在一起。它给人的感觉是安全、中立、善良和忠诚。这也是为什么白色常用于婚礼服装，或者用于表示投降。
- **黑色** 黑色通常象征权力、高雅、神秘和力量，常用来表示权威、深度和稳定。黑色给人的感觉是平静和宁静。通过对比，它也可以强化其他色彩。
- **红色** 红色和兴奋与喜悦相关联，是充满喜庆、行动和能量的色彩。它象征健康、速度、激情、欲望和爱。红色能够刺激情绪，使得心跳、呼吸加快，血压升高。
  红色能够引发强烈的情绪，在使用时需要注意。它能够表示力量和冲动，也能够代表武力、威胁和征服，甚至是暴力和复仇。请小心使用。
- **橙色** 橙色给人以温暖、热情、吸引、决心、力量和忍耐的感觉。它能给人以鼓舞和活力，甚至能刺激人的食欲。
  橙色是另一个需要审慎使用的色彩。虽然使用橙色有很多好处，例如让对方觉得温暖，增强你和产品的吸引力，但是用得太多或者组合不好的话会产生不安全、无知和迟缓的感觉。
- **金色** 金色常与明亮、智慧、财富和威望联系在一起。
- **黄色** 黄色与能量、乐观、喜悦、高兴、忠诚和精神饱满相关联。它能让对方觉得成为焦点和受重视。
  黄色也能影响一个人的记忆（这就是贴纸多为黄色的原因）。少量应用会激发正面的情绪，但是用得太多会让目标注意力不集中或者感觉吹毛求疵。
- **绿色** 绿色常与大自然、和谐、生命、丰饶、雄心、保护与和平相联系。它能够让人觉得平静、安全。
  绿色是另一种强有力的色彩，但是如果使用不当或者使用过多的话，也能给人以贪婪、内疚、妒忌和混乱的感觉。
- **蓝色** 蓝色是天空和海洋的色彩。它与智慧、直觉、真理、宁静、健康、力量和知识相联系。它具有让人镇定和冷静的力量，会让人的新陈代谢减慢。
  蓝色是眼睛最容易适应的颜色。它有很多正面的效果，但是运用时得注意，不要让目标觉得寒冷或者沮丧。

- **紫色**　紫色与皇家、高贵、奢侈、创意和神秘相关联。
- **棕色**　棕色与地球、可靠、易接近、惯例和秩序相关。它能给人以牢固或相关的感觉，或者一种秩序感。

你要如何使用这些信息呢？这里并不是说穿一身蓝色服装就能让对方感觉平静并将密码告诉你。不过你能利用这些信息筹划攻击方法，确保获得最佳的成功机会，计划中也要包括你的外表和着装。

社会工程人员必须仔细分析即将拜访的目标，确保着装的色彩能够增强操纵目标的能力，而不是让目标反感。例如，了解到绿色可能引发贪婪或野心的感觉，社会工程人员在与慈善机构会面时就不要穿绿色的衣服，因为它可能产生与慈善的使命相违背的感觉或情绪。另一方面，如果穿着蓝色套装拜访律师，就能起到让人冷静的效果，让律师敞开心扉。小心筹划并合理应用这些战术，能够确保社会工程审计的成功。

6.4.4　令目标积极地响应

条件反射用在日常交谈、市场宣传、恶意操纵等各个方面。就像巴甫洛夫的狗一样，通过训练，人们会对特定事物产生条件发射。人类的天性通常被用于操纵大部分人执行操纵者的指令。

大部分人在想到婴儿时会微笑，在说到动物时会感觉“可爱”，我们甚至可能在想到某一流行产品时唱出它的广告歌曲。

这类战术很隐秘，很多时候我们甚至不知道它们已经在起作用了。很多时候我会想穿着暴露的比基尼女郎与啤酒有什么关系。

应用条件反射的一个例子是米其林轮胎。多年以来，这家公司一直在广告中使用婴儿（参见图6-12）。为什么？“因为轮胎承受了很多。”但是这些广告的含义更多。在看到婴儿时，你会微笑，会感到幸福。这种情感激发了一种正面的反应，这一反应让你欣然同意接下来要告诉你的内容。当看到婴儿时你会微笑，看多了以后，一看到米其林轮胎你就会有一种温暖、幸福的感觉。

图6-12　婴儿可爱吗

看到婴儿坐在轮胎旁，同样会让你对这一品牌有积极、幸福的感觉。这是一个操纵的经典例子。

百威啤酒的广告（参见图6-13）也很典型，很多人在想这则广告的含义——记得这些受欢迎的青蛙说出了“百”-“威”-“啊”吗？青蛙和啤酒有什么关系？循着这一思路，再想想最近的广告中出现的克莱兹代尔马和它的动物朋友。这些广告很引人注目，第一次看到的时候还会觉得滑稽，但是无法解释你为什么想买他们的啤酒。

图6-13 青蛙让销量大增

在这种形式的操纵里使用了隐秘的条件反射方法。看到这些广告时你会大笑，随后在开车去买啤酒时，看到厚纸板上的青蛙或骏马又笑了起来，这在你心中产生了积极的情感，让你愿意买这个牌子的啤酒。

以销售和市场为主导的公司经常会使用这种条件反射战术，目的是操纵消费者购买他们的产品而不是竞争对手的。社会工程人员并不销售产品，但想要目标“买”账，认同他们的伪装，采取他们期望的行动。但是为什么要使用操纵战术呢？使用这种强有力的控制方式有何好处？下一节将讨论这一话题。

6.4.5 操纵激励

操纵他人能够得到什么好处？这个问题直抵所有操纵方法、思维和战术的核心。并非所有的操纵都是负面的，但是都和其背后的激励有关。*激励*可能是正面的，也可能是负面的。

什么是激励？可以将激励看成刺激你采取行动的任何东西，比如金钱、爱、成功等，甚至是负面的情感，例如憎恨、嫉妒和羡慕。

人们选择操纵他人的主要原因可以分成三类：金钱激励、意识激励和社会激励。下面会逐个分析每一种激励以及如何将它们应用于操纵。

1. 金钱激励

金钱激励是最常见的，前面提到的例子大多和增加销售额有关。很多骗局的战术背后都有金钱激励的影子。

有多少人为了赢得大奖而每天买彩票？随着时间的推移，他们可能花了几百美元买彩票，但只要中20美元就会很开心，从而继续购买，希望能中更大的奖。

一个非恶意的金钱激励的例子就是优惠券。如果你在特定的商店购买特定的商品，就可以享受X美元X美分的优惠。如果你买东西时精打细算或者想要试用那个商品，就会去那家店。

很多商业机构在推销再教育、职业或技能培训时，会使用金钱激励的方法，为你描绘一幅画面：参加他们的课程和培训后，你的收入会大幅提高。

恶意攻击人员使用操纵战术的激励就是经济收益，因而他们的动机和技术也反映了这一点。例如，如果恶意社会工程人员的目的是让目标出让一部分辛苦挣来的钱，他伪装的角色将是“可以”要钱的人。在这种情况下伪装成慈善组织就比较合适，因为请求捐助或者询问财务信息是再寻常不过的事了。

2. 意识激励

意识激励非常难以描述。每个人的理想都不同，这些理想可以影响激励。如果你的理想是经营一家餐馆，那么这就是你的激情所在。你会长时间工作，比员工投入更多的精力，而且不太在意金钱回报，因为那是你的梦想和目的，而对其他人来说则只是一份工作。

梦想和信念可以深植于一个人的心中，以至于几乎不可能将它们同其人分开。当听到有人说“我有一个梦想”时，你会想到马丁·路德·金吗？有些人的梦想和目标是要成为什么样的人，而不是脑子中的空想。

人们会被拥有类似梦想和目标的人所吸引，所以“物以类聚，人以群分”这句话用在此处非常合适。但这也是很多人能够被操纵的原因。

让我们以基督教电视传道者为例来进行分析。那些信仰或者渴望信任上帝的人聚在一起。具有类似信念的人能够增强彼此的信念和做正确事情的欲望，但是电视传道者可以利用这种意识告诉他们上帝的意愿是让某个教堂繁荣，因而他们的钱包也就能鼓起来。

电视传道者进行几番激励性的布道、洒下一些泪水，突然间人们就将支票不断地送过来。这些传道者同时利用了金钱和社会理想这两种工具（参见下文），将听众的思维转换成他们的思维方式，所以这些人将辛苦挣来的钱捐了出来。有意思的是，如果你问那些追随者，对于“牧师比他们富裕得多”有何感觉，他们相信那是上帝的旨意。他们的思想已经发生了改变或者已经被操纵。

意识激励也能用于对人们进行道德教育，甚至借助恐惧这一激励方法也能对人们产生很大的影响。人们常常通过具有寓意的故事和寓言教育儿童意识激励。《格林童话》就是这种类型激励的最好例子。故事的结局通常是坏人受到惩罚或者死亡，而好人在坚忍不拔地克服各种困难后最终得到了巨大的回报。这些故事借助恐惧让孩子们知道做坏事会受到可怕的惩罚，甚至可能死去。

意识激励也用于市场营销，在“志趣相投”的人“碰面”的地方投放广告。例如，尿布公司在家庭杂志上做广告，动物保护组织选择在动物园做宣传，运动器材公司则瞄准体育赛事等。这种类型的激励使得广告中的商品或服务在具有共同思维模式的人群中热销。

意识激励用来让某人的思维与同类人结盟。通常，操纵战术开始于人们产生共鸣之时。同样，不是所有的操纵都是恶意的，但要以正确的方法使用。

3. 社会激励

社会激励也许是应用最广泛和最复杂的激励形式，特别是在社会工程活动中。

人类具有社会化的天性，这是我们通常的生活方式。社会激励包括所有其他类型的激励。适当的关系会提高你的金钱需求，也会调整、增强你的理想。可以说社会激励要比其他两种类型的激励更加强大。

很多人会受到来自同等地位的人的极大压力，这是显而易见的。对任何人来说，不论是年轻人还是老年人，随大流的吸引力都很大。很多时候，什么可以接受与社会激励直接相关。人们对生活和自身的看法，会受周围人群的极大影响。实际上，即使在没有直接同伴的情况下，也会感受到来自同伴的压力。

我好看吗？要看情况。如果我在美国，那里超级名模穿“零号尺寸”的衣服，男人身上都是肌肉，而我身上没有肌肉，那么我就不好看。如果我在古罗马，那里体格大就意味着富有和权力，那么我就好看。人们的内在自我会受到社会观点的影响。

1975年，美国空军进行了一项名为“空军技术训练中的社会激励鉴别和分析”的研究，尝试分析在训练和演习中培养领导者的社会激励效果。他们在小组中设置了4种不同的场景，分析其对学员的影响。

结果显示，一定的社会激励，通常包括来自同伴或权威人物的赞赏或正面支持，会在学员和教官之间建立起密切的关系。

> 整个研究的主要结论是社会激励的管理是一门艰难的艺术。虽然发现和调整社会激励很容易，但操纵和管理这些激励就难多了。实验数据显示了不同的社会激励的强大吸引力。实战实验的结果显示了熟人和心理契约训练对同伴学员态度的影响。这些发现强调了社会因素的重要性。

换句话说，当我们知道某个人的动力所在时，提高或降低社会激励的吸引力并不难。这种现象在少年中表现尤为突出。当发现他人的顾虑时，他们就可以将这一点作为武器逼其就范。施加压力的人越多，目标顺从的可能性就越大。

上面的句子要仔细琢磨。我同时也在想：如果研究者能够利用今天的众多社交网站，结果又会怎样呢？来自同伴的压力是一种强大的影响力，每个人都想成为大众中的一员。

社会激励很有效。2007年，奥丽埃纳·班迪耶拉（Oriana Bandiera）、伊万·鲍龙考伊（Iwan Barankay）和艾莫然·拉苏尔（Imran Rasul）合作发表了一篇研究论文Social Incentives: The Causes and Consequences of Social Networks in the Workplace，详见www.social-engineer.org/wiki/archives/Manipulation/Manipulation-Social-Incentivespdf.pdf。

这份报告讲述了一项很有趣的研究，该研究与空军的研究很像，只不过研究时间为2007年。基本上，研究者分析了那些在工作中有“朋友”的人，在与朋友一起工作时的情况。他们的结论如下。

> 我们的研究显示社会激励是真实存在的。在排除生产技术、补偿方案等可能带来影响的外部因素后，朋友的存在会影响工作者的效率。由于社会激励的存在，工作者在一起工作时会遵从共同的规范。朋友的存在会提高能力较差者的工作效率，反之，也会降低能力较强人员的工作效率。
>
> 社会激励对工作者的表现具有重要的决定作用。当工作者基于个人生产力按件计酬时，社会激励的表现会导致：(1)那些能力强的人会放弃10%的收入以遵从规范；(2)那些至少有一个比他能力强的朋友的工作者，会提高10%的生产力以符合规范。从总体上来说，工作者能力的分布是后者的影响占主导地位，所以社会激励对公司业绩的净影响是正面的。

朋友的存在意味着他们会更努力或者更放松。在没有外界压力的时候，来自同伴的压力会影响人们的工作效率。这种压力可以理解为标准。为什么？也许一个人能够工作得更快或者更好，但是他可能不想表现出什么都能干或者像拍马屁似的。如果平常比较懒散，他也不想显得懒惰，所以也会适当地更努力一些。不管是何种情况，他们的职业道德都会被朋友所影响。

管理的一个好策略就是总将工作最努力者和天生的领导者放到领头的位置。不过这个研究中还有很多可以学习的地方。

这个方法就是社会工程人员所用的“尾随战术”。混在一大群就餐或者休息回来的人中，装成其中的一员，在通过大门的时候一般保安都不会拦着。

这也是对整个人群进行操纵的方法，让他们认为某种行动或者态度是可以接受的。这一点你可以在娱乐圈中看到，每年可接受行为的标准和道德水平都在下滑，然而这种标准的降低通常打着“自由”的旗号。

实际上并不是只有这三种激励方法。它们可以分化成其他方面，这超出了本书的讨论范畴。不过我们仍然要分析一下社会工程人员怎样应用这些激励方法。

6.5 社会工程中的操纵

操纵并不是让人们喜欢你的所作所为并且感到舒服，而是强迫他们做你想要他们做的事。

强迫不是一个友好的词汇，它的含义是“迫使某人以某种方式行动或思考”或者“通过武力支配、阻止或者控制”。

操纵和强迫利用心理力量改变目标的观念、信仰、态度和行为。使用操纵和强迫的关键是通过一些不可察觉的小步骤逐步进逼。社会工程人员不想惊动他正在操纵的目标。下面的一些方法可能具有很大的争议或者很可怕，但是诈骗犯、身份窃贼等每天都在使用。操纵的一个目的是制造焦虑、紧张和过度的社会压力。当目标有这种感觉的时候，就更可能采取社会工程人员操纵他采取的行动。

通过以上内容，你就会明白为何人们常常对操纵持有负面的看法，但是由于其常用于社会工程中，因而必须加以讨论。

6.5.1 提高目标的暗示感受性

提高目标的暗示感受性通常会使用第5章中讨论的神经语言程序学技巧或者其他视觉提示。前面给出了一些例子，如通过钢笔的咔嗒声或者其他噪音或手势等让他人产生条件反射，甚至无需言语，就能诱发对方的情感。

我曾经亲眼见证过，当时一个人正在操纵目标，他使用钢笔的咔嗒声暗示一种积极的想法。他会说一些正面的东西，然后微笑并且让钢笔发出咔嗒声。慢慢地，在重复4~5次咔嗒声之后，我看到目标开始微笑。随后操纵者提到一个令人沮丧的话题，同时让钢笔发出了咔嗒声，结果目标首先开始微笑，然后立刻感到很尴尬。这种尴尬为操纵者打开了操纵目标的方便之门。

要制造一种他人易受暗示影响的场景，可以通过不断重复想法或者其他方法，使目标接受你的想法。

社会工程人员应该确保整个设置与操纵相配合，如使用的语句、描绘的画面和选择的服装颜色等，所有这一切会提高目标的暗示感受性。

威廉·萨金特（William Sargant）是一位有争议的精神病学家，也是《思维的战场》（*Battle for the Mind*）一书的作者，他谈论了操纵人的方法。根据萨金特的观点，用恐惧、愤怒或者激动等情绪扰乱了目标之后，可以为他植入不同的信念。这些情绪会导致暗示接受性提高和判断力下降。

社会工程人员可以利用这一方式达到自己的目的，首先给目标一个会令其感到恐惧或激动的暗示，然后提供一个解决方案，这个解决方案就是一条建议。

例如，在大受欢迎的BBC电视栏目《骗术真相》中，演员通过一场骗局演示了这种方法的可行性。他们在卖场中设置了一个摊位售卖奖券。购买奖券的人有可能获得三项奖品，其价值远高于所购买的奖券。

一位妇女购买了奖券，当然，她赢得了大奖。她的情绪异常激动，因为她之前从未获得过这样的大奖。此时，保罗·威尔森提出了一个建议从而操纵了她：在这种激动情绪之下，他告诉她必须拨打一个电话，并且需要提供银行信息以领取奖金。

她毫不犹豫地照做了。这个建议很合理，尤其是在她激动的时候。

了解目标、他的喜好、小孩的姓名、钟爱的球队和食物，然后利用这些制造一个易动感情的环境，就会轻松营造出易于接受暗示的气氛。

6.5.2　控制目标的环境

控制目标的环境通常用于在线社会工程、欺诈和身份盗用等场景。

成为同一社交网络和组织的一员，会让攻击者有机会获得操纵目标行动或思维的“会面时间”。如果能够利用目标的社交网络找出他们的情感触发点，效果也很不错。

在一次为客户调查非法诈骗犯的详细联系信息时，我使用了这种方法。在诈骗犯发布“战果”的论坛上，我找到了他的账号，然后进入了他的环境，成为了他的朋友，赢得了他的信任，通过社交网络了解他正在做的事情，最终获得了他的联系信息。

任何用来控制目标环境的方法都可以用在操纵战术中。控制目标环境可能简单到在不打扰目标时接近他，或者让目标看到或者看不到某一可能引起他反应的事物。

当然，除非你计划将目标带入黑暗的密室中，否则并不能真正控制他的整个环境，所以要想尽量控制就需要进行计划和研究了。在找到目标的社交圈子之后，不管是网络世界还是现实世界，你都要花时间设想一下如何进入并控制那个环境。一旦进入，你要控制什么呢？优秀的社会工程人员不会一上来就追求那“致命一击”，而是会慢慢建立关系、获取信息，然后才进行最后一击。

环境控制常用于警察或者战时审讯。审讯环境设置的气氛会让目标感到放松、紧张、害怕、焦虑或者审问者（或者军官）想让目标感到的任何情绪。

6.5.3　迫使目标重新评估

逐渐削弱目标的信念、意识或者对某一情形的情绪控制会让他不安。这一战术具有很强的负

面效果，因为它让目标怀疑他通常认为是对的东西。

邪教组织使用这一战术蚕食那些寻找人生方向的人。感觉迷失或者困惑时，人们常常认为需要重新评估自己的整个信仰系统。当邪教组织获取控制权时，他们会非常有说服力，受害者会彻底相信他们的家人和朋友不知道什么才是最好的。

在个人社会工程层面，你可以让他人重新评估以前被灌输的有关安全的理念，或者什么是公司政策、什么不是。

社会工程人员每天使用相似的战术，提出经过周密思考的问题，让目标重新评估其对某一问题的立场，动摇其信念。

例如，在当前的经济环境下，销售人员渴望提高销售额，也许公司对不经过扫描并采取防范措施就从网上下载PDF文件有严格的限制，但你还是可以致电公司的销售部门，说："你好，我是ABC公司的，想订购你们的产品，可能会超过10 000件。公司要求我获取三项报价，看看双方怎样合作比较好。我已将询价文件上传到了我们公司的网站上，我能将URL发给你吗？两个小时后我要去开会，你能看一下询价文件，在我开会前给出一份基本报价吗？"

你认为这一战术会成功吗？销售员很可能在稍加迟疑之后或者毫不犹豫地就下载并运行那个文件。你迫使他重新评估公司制定的政策。

6.5.4 让目标感到无能为力

让目标感觉脆弱或者无能为力是另一种阴暗但很有效的战术。它常用于社会工程，社会工程人员可以伪装成愤怒的主管或者其他比目标职位高的人。攻击者因目标没有反应或者不能快速回答问题而感到愤怒，于是严厉责备或者威胁目标，迫使他怀疑自己的立场，让他感觉无能为力。

另一种更加微妙的方式是通过社会激励逐渐削弱其信念系统。在一次审计中，我正在对内部网络进行扫描，管理员出面阻止了我。当她理直气壮地阻止我的时候，我的反应是："你知道这家公司每年得处理多少网络入侵事件吗？我在为你们进行安全加固，而你却阻止我工作！"

我的强势让她感觉无能为力，终于败下阵来。

让目标感觉没有时间思考或者情况特别紧急，也会让他觉得无能为力。他没有时间思考怎样处理问题，因此必须立刻作出一个决定。

在最近的海地地震发生后，有人利用了这一战术。有人创建了一个网站，声称上面有可能在地震中失踪的亲人的信息。因为他们声称除了建立网站的人之外，没有人可以提供他们失踪的亲人的信息，所以他们可以要求只有达到特定标准的人才能获取信息。很多觉得没有希望、无能为力的人，提供了太多的信息，点击了他们自己也知道不该点击的内容，结果最终被利用了。BBC发表了这一故事，并列出了一些保护自己的建议，详见http://news.bbc.co.uk/2/hi/business/8469885.stm。

6.5.5　给予非肉体惩罚

与让目标感到无能为力这一战术密切相关的就是让他们觉得内疚、耻辱、焦虑或者丧失特权。这些感觉非常强烈，目标可能会做任何事来“重获青睐”。

如果没有达到别人的期望会觉得丢脸并对自身产生怀疑，这会使得目标按照攻击者想要的方式作出反应。

我并不建议在大多数社会工程场景中应用耻辱这一策略，但是我曾经见过一个社会工程团队将其用在了一个目标身上，也用在了另一个社会工程小组成员身上以“软化”目标，使得他们更容易接纳别人的建议。

第一个攻击者接近处于公共环境中的目标尝试获得信息，他伪装成了一个重要人物。

在对话过程中，一名女性下属（也是团队成员）走向前问了一个问题，激怒了第一个攻击者。他的回应是：“你一定是我见过的最愚蠢的人。”说完，愤怒的他走开了。女性攻击者看上去很沮丧也很受伤，目标很快就开始安慰她，想让她心里好过些。目标的同情给了攻击者操纵他的机会，让他泄露出本不想泄露的更多信息。

6.5.6　威胁目标

威胁也许不是我们设想的传统意义上的社会工程会使用的战术。你不会将目标绑起来用“杰克·鲍尔”[①]的方式对待他，但是可以使用隐晦的方式进行威胁。

暗示目标不能照办的话会被解雇或者造成其他不利后果，就是对目标的一种威胁。政府常常会使用这种战术操纵社会大众相信经济体系正在崩溃，这样他们就能控制那些被统治的人的情绪。

甚至可以在社会工程审计中通过表现出一种威胁的样子来达到效果。看起来很忙、心烦、身负重任会威胁到不少人。如果在谈话中显露权威的表情也能对人产生威胁。

在商业活动中，通过认证的邮件或者快递发送物品隐含一定程度的威胁。让人签收内容不明的包裹，会让一些人感觉受到了威胁。这种操纵战术的目的就是要让目标觉得不自在和忧虑，这会让他做出以后会后悔的事情，但为时已晚。

社会工程和专业审计人员使用这些更为阴暗的操纵技术时得心应手。如果让目标觉得完全无能为力，他就会认为向攻击者屈服是相当合理的。

这是社会工程实践中的操纵和其他形式的影响战术的真正区别所在。在使用负面的操纵战术

① 杰克·鲍尔是美国电视剧《反恐24小时》中的人物，是一名非常有能力的联邦特工。——译者注

之后，社会工程人员丝毫不顾目标的感受就离开了。如果目标后来意识到自己被利用了，也不要紧，因为破坏已经造成，公司或个人已经被渗透了。

社会工程操纵的其他方面一样很有用，但不是这么阴暗。

6.5.7 使用积极的操纵

积极的操纵与消极的操纵目的相同，即最终目标的想法和愿望与你的达成一致。区别则在于实现结果所采用的方式不同。在积极的操纵中，目标在你达到目的后不需要心理治疗。

通过多年的研究，我总结了一些关于父母如何与儿童沟通的建议，以便让他们顺从父母的意愿。其中有几点是关于积极操纵的，对社会工程人员会很有用。下面讨论这些积极的技术。

1. 不要让目标的表现影响你的情绪

不要让目标的表现影响你的情绪，这点非常重要。一旦让你的情绪介入其中，就是目标在操纵你了。你当然会产生情感，但是要控制自己的感觉并注意表露感情的方式。

你不能失去控制。你也要尽量控制负面情绪，这样才能始终控制局面。

控制你的情绪也会让目标感到放松。但这不是说完全不表露情感，那样也会让人不舒服。如果某人真的心烦，表现出适当程度的关心是好的，但是如果显露出太多的情感，就会让目标偏离方向，导致整个行动的失败。

保持情绪与伪装一致。如果你能控制情绪，就能始终控制住局面。优秀的社会工程人员能够做到忽略目标的行为和态度。如果目标表现出不安、生气、好战、粗鲁或者其他负面情绪，优秀的社会工程人员应保持平静、冷静和镇定。

2. 寻找积极的话题

只要有可能，说个笑话或者称赞某物，但是不要显得怪异。你不能在走近门卫的时候说："两个尼姑走进一间酒吧……"这个方法很可能不会奏效。同时，你也不能走向前台直接说："哇，你真漂亮！"

寻找积极的话题能让所有人感到自在，但是必须适当、有涵养、有品味。以前面接近门卫的例子来说，在自我介绍后，可以赞美一下她孩子的照片："哇，她真可爱！多大啊？4岁还是5岁？我也有个女儿。"这样做有助于后续计划的进行。

3. 假定，假定，假定

你可能听别人谈起过有些人喜欢假定或者设想，但是在这里，*请假定一切*。假定目标会依照你想要的方式行动，假定他会回答你想知道的问题，假定他会同意你的所有要求。

假定你要问的问题以及要做的陈述。

“当我从服务器机房回到这里……”

这种表述假定你属于那里，并且已经具有访问权限。就前面提到的门卫的场景来说，在赞美之后可以继续说：“在检查完服务器回到这里时，我给你看一下我女儿的相片。”

假定你想要的会发生也大有好处，因为它会影响你的精神面貌。你必须从精神面貌上表现出你会得到想要的，这种信念会制造出新的肢体语言和面部表情，从而让你更好地伪装。

如果觉得会失败，你就会失败或者至少会影响你的肢体语言和面部表情。如果你的精神面貌是一切顺利，就真的会一切顺利。不过要提醒一句，千万不可自大。

例如，如果你心想“我当然稳操胜券，因为我很了不起，我是最好的”，这会影响你的表现，让目标失去兴趣。

4. 尝试不同的开头

通常交流时都以标准的为什么/什么/何时作为开头，但是也可以尝试不同的方式，看看效果如何。一个流行约会网站www.okcupid.com的研究小组对数据进行整理后发现，非传统的开场白具有一定的价值。

记得前面关于赞美的讨论吗？OkCupid网站的研究小组发现，开始时恭维太过会起到与设想相反的效果。性感、美丽、热辣等词语的效果极差，相反，酷、棒极了、迷人等词语的效果更好。

研究小组发现，在通常的问候语中，“嗨”、“嘿”、“你好”等会让目标觉得平淡，不会被激起兴趣，而“最近怎么样”、“最近可好”、“你好啊”以及“哈罗”等则是更好的开头。

当然，这些是关于约会的统计，但我们要学习的重点是人们针对非传统的问候会给予更好的反馈。

同样，在社会工程场景中，使用不同的接近方法，你会注意到目标对信息的反应程度会有所提高。

5. 使用过去时

当想表达负面情况并且不想让目标重复时，就用过去时。利用这一技巧，可以将过去的负面态度和行为放到他的回忆中，给他一个“重新开始”的机会，让他为你做一些好事。例如：

“当时你说我不能进去找史密斯先生……”而不是说：“你说我不能进去找史密斯先生时……”

虽然只是改变了时态，但效果截然不同。前者给人的印象是该情况发生在很久以前，让我们翻到改进的、崭新的一页吧，而且它也能让目标觉察你当时的感觉。

6. 探讨并摧毁

计划一下怎样处理破坏性或者负面的态度和行为。设想你伪装成技术支持人员，想要进入服务器机房。通过之前的电话交流，你了解到每天上午10点会有一群人出去抽烟。你认为人们不断进出的时候是一个好时机。你准备好了一切，但是在进大楼的时候，前台刚刚得到一些坏消息，情绪很不好。你应该计划好了如何处理这种糟糕的情况。

如果不事先思考如何处理潜在的交流障碍或者破坏性影响，而是等到临场发挥，则大多数情况下会出现问题。这就提出了一种有趣的想法。你必须在行动之前就像目标一样思考：他会提出什么异议？当不认识的人打电话或走过来时，他会说什么？他会提出什么异议？他会是什么态度？仔细考虑这些事情能够帮助你制定出针对这些潜在问题的解决方案。

将你的想法和目标的潜在问题写下来，然后开始演练。让你的配偶或朋友扮演不友好的门卫或者警卫。当然，他们不能模仿出面部表情等元素，但是你可以为他们提供一个拒绝交流时可能出现的情况列表，以测试你的反应。

不断练习，直到你能自如地应对，但是不要照本宣科。要记住，僵硬和死板的应对会让你很难随机应变。

积极的操纵对目标具有非常大的影响，不仅不会让他觉得受到冒犯，而且在操纵得当的情况下，会让他觉得自己做了一件好事，从而有一种成就感。

6.6 小结

操纵是社会工程和影响力中的一个重要部分。本章涵盖了世界上最有智慧的人们几十年来对人类行为领域的研究成果。

对操纵他人这一想法的常见反应可能是：

- “我不想操纵他人。”
- “学习这个是错的。”

这两种意见代表了大多数人对操纵一词的看法。但愿你现在相信操纵不总是黑暗的艺术，它也能用在好的方面。

今天，一些最聪明的心理学家和研究员剖析、研究、分析了影响力。我正是基于这些研究才写出了本章的内容。例如，框架部分一定会改变你和他人交往的方式，回报会让你像社会工程人员一样思考，让你知晓如何利用影响。影响力是一个令人惊异的话题，有关这一主题的书籍有很多。

理解什么会触发目标想要采取某一行动，并让目标觉得这一行动对他来说有好处——这就是影响力的用途。

本章分析了人们行动的心理学和科学基础，并且阐明了社会工程人员是如何应用影响力的。

请记住，影响力和说服的艺术是让他人想要按照你设想的方式去做、去反应、去思考或者去相信的过程。

上面这句话体现了社会工程和操纵的精髓。它是变动任何框架的关键，是打开操纵之门的关键，也是成为影响力大师的关键。

社会工程人员也可以借助很多实物工具，有些看起来就像是电影《007》中用到的。我们将在下一章讨论社会工程工具。

第 7 章
社会工程工具

人是使用工具的动物，没有工具，一事无成；有了工具，无所不能。
——托马斯·卡莱尔（Thomas Carlyle）[①]

工欲善其事，必先利其器。工具是否合适将直接影响社会工程人员的能力和成败。然而，仅有工具还远远不够，还得知道如何熟练地使用工具，这样才能取得成功。

本章将讨论物理工具、电话工具以及基于软件的工具这三者之间的区别。需要注意的是，仅仅拥有最昂贵或最好的工具，并不会使你成为一名社会工程人员。工具在安全审计实践方面的作用，就如同菜肴中的调味品，放得恰到好处便成就美味佳肴，太多或太少则会造成味道太重或淡而无味。你一定不希望自己在执行社会工程任务时看起来像个腰间缠满工具的蝙蝠侠，同样也不愿意面临到了目标的门口却因缺少适当的工具而无法进入的窘境。

社会工程工具的范围十分广泛，本书并非教你怎样开锁或篡改来电显示，而是要为你提供足够的信息，来帮助你决定什么样的工具可以增强你的实战能力。

本章首先着重介绍开锁器、垫片和摄像机等工具。市场上一些新颖奇特的工具会让平凡的社会工程人员感觉自己就像是詹姆斯·邦德。本章将介绍一些这样的工具及其使用方法，同时展示一些工具的图片。此外，本章还会讨论社会工程攻击中如何篡改来电显示，介绍市面上几款最好的基于软件的信息收集工具，最后还将探讨一些密码分析工具。

---

① 托马斯·卡莱尔（1795—1881），苏格兰评论家、讽刺作家及历史学家。——译者注

7.1 物理工具

物理安全是指企业或个人为保障安全所采取的不涉及计算机的措施，通常涉及锁、摄像机及窗户传感器等工具。懂得物理安全并知晓其运作原理是成为优秀社会工程人员的前提之一。你不必精通这些装置，但要对目标所使用的安全机制有清晰的认知，这样能帮助你克服社会工程审计过程中的阻碍，走向成功。

7.1.1 开锁器

在讲开锁之前，我们先来了解一下锁的基本工作原理。

图7-1是简易弹子锁的简单示意图。

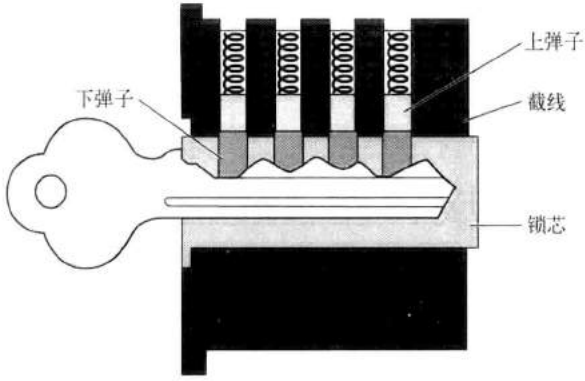

图7-1　弹子锁的简单示意图

弹子锁的基本工作原理是通过钥匙控制弹子。钥匙将下弹子和上弹子推至一定的高度，当两类弹子的截线正好与锁筒和锁栓之间的缝隙一致时，便可以轻松地转动钥匙打开门、服务器机房及陈列柜等。

开锁器模拟了钥匙将所有弹子一个接一个地移动到正确位置的过程，使得锁芯可以自由转动并打开门。开锁时，所需配备的两个主要工具是拨片和扭力扳手。

*拨片*是末端弯曲的长金属片，类似于牙医的工具。使用时将其插入锁的内部，上下拨动弹子直至其处于正确的位置。

*扭力扳手*是小而扁的金属器具，当使用拨片时，它能向锁施加压力。

*耙子*的外形很像拨片，但它用于在锁上“耙”动以操作所有弹子。耙子可以十分迅速地打开大部分锁，这一特性对开锁者极具吸引力，因为这样的话，大部分锁就可以被快速打开了。

要开锁，请遵循下列步骤。

(1) 将扭力扳手插入锁眼，沿着用钥匙开门时转动的方向扭转。关键技巧是知道施加多大的张力，因为力太大或太小，弹子都不会进入正确的位置，从而无法打开锁。若用力恰到好处，则会创建一个小平台，从而让锁芯能卡住销轴。

(2) 插入拨片，一个接一个地拨起弹子，直到感觉它们都处在固定的位置上了。当上弹子就位时，能听到轻微的咔嗒声。所有的弹子都就位后，锁芯便可自由地旋转，锁也就打开了。

上述步骤只能说是开锁的皮毛。欲了解更多有关开锁的知识，请访问下列网站。

- http://toool.us/
- http://home.howstuffworks.com/home-improvement/household-safety/security/lock-picking.htm
- http://www.lockpicking101.com/

这些只是众多致力于开锁教学网站的冰山一角。作为一名社会工程人员，花时间练习开锁是明智的。当需要的信息被锁在服务器机柜、书桌抽屉或者其他设备中时，随身携带的小型开锁套装可能就成了你的制胜法宝。

开锁套装可以很小，图7-2中所示的开锁器只有普通名片大小。

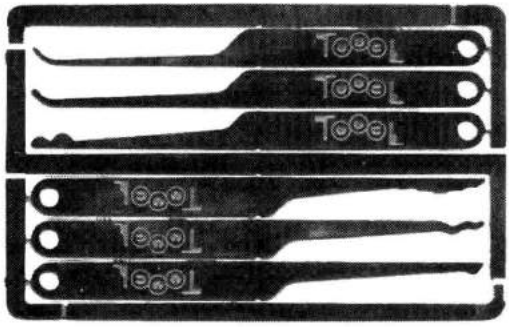

图7-2 这种名片大小的开锁套装很适合放在皮夹或钱包中

不过有时开锁套装也会比较大，就像图7-3和图7-4展示的那样。

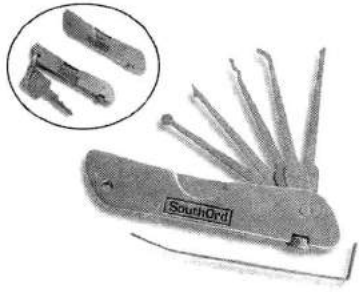

图7-3 这套跟随身小折刀的尺寸差不多

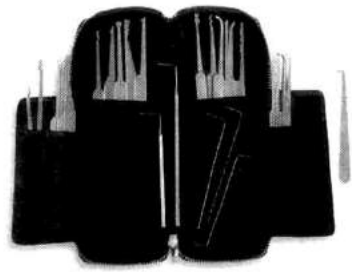

图7-4　该开锁套装比较大，所需工具一应俱全

敬告：要在关键时刻来临前学习使用开锁器。就个人而言，我先买了一些不同尺寸的玛斯特（Master）牌的挂锁。成功地将它们全部撬开后，我又买了一套如图7-5所示的万能钥匙。它们适用于不同弹子类型的锁。弹子类型多样，这无疑会增加开锁的难度。持有不同弹子类型和不同大小的万能钥匙，能使你的练习实现最佳效果。

图7-5　这些透明的锁可以让你看到整个操作过程

我甚至在会议上见过一些极其精巧的装置，它们就像一个自制的锁墙，值得研习。当然，在收集目标信息的时候，拍摄或记录需要打开的锁的类型、品牌和具体型号，也是个不错的主意。了解这些信息能够为你的社会工程实践做好铺垫。

1. 实际应用

在电影和电视描绘的撬锁场景里，某人只要将开锁器插进锁眼中，短短几秒钟，门就奇迹般地打开了。或许某些人的开锁技能确实很高超，但是大多数人的成功之路很漫长，在经历了无数次的失败和挫折后，他们才能真正掌握撬锁和耙锁的技巧。耙锁本身就需要一定的天赋，关键在于使用耙子轻轻地在锁中耙进耙出的同时对扭力扳手施加些许压力。这一简单的方法可以撬开多种类型的锁。学会耙锁后，社会工程人员就知道如何正确地使用扭力扳手了，并能体会锁被撬开时的感觉。

许多公司开始采用射频识别（RFID）、磁卡或其他类型的电子准入技术，这可能让人觉得开锁技术已经过时了。实则不然，锁还在用，开锁技术也仍有用武之地，说不定哪天这项技能就能救你于水火之中。

下面的案例就充分体现了随身携带开锁器的好处。在一次行动中，我遇到一个无法使用社会工程方法来解决的障碍——一扇门。拔出一向值得信赖的袖珍开锁器，使用耙的方式，大约30秒钟之后我就成功进门了。很多社会工程人员都有过类似的经历，懂得锁的原理并携带适合的工具才造就最终的成功。公司会花费数万甚至数百万美元购买硬件、防火墙、入侵检测系统以及其他保护手段，再把它们都扔在一个房间里，最后只用廉价的玻璃和一把20美元的锁来保护它们。这样的情况屡见不鲜。

因为撬锁会面临被发现或被抓住的风险，所以练习是必不可少的。你必须动作迅速以降低风险。有些地方安装了摄像头来监控这种行为，但最终效果不佳，除非当时有人正在监视摄像画面，否则它只是记录了有人非法闯入并窃取服务器的过程而已。

通过一些简单的手法就可逃过摄像头的法眼，比如用LED强光照镜头或者用帽子或头巾遮住面部。

2. 打开磁性锁和电子锁

磁性锁之所以越来越风靡，主要原因在于其运行费用低廉并且提供了一定程度的安全保障，不像传统的弹子锁那样可以被撬开。磁性锁的形状、大小和磁力级别各异。只是从某种程度上来讲，磁力锁也并不安全：如果突然断电，大部分磁力锁将失效，门就被打开了。当然，没有使用后备电源才会产生这样的后果。

强尼·龙是世界知名的社会工程人员和黑客，谷歌黑客入侵数据库的创始人及《非技术黑客》（*No Tech Hacking*）一书的作者。他讲述了自己使用衣架和毛巾绕过磁性锁的故事。他注意到员工从里向外走向门口的动作会触动门锁打开，还注意到门中间有一道足以塞进一个系着毛巾的衣架的间隙。通过摇动毛巾，锁就被打开了，他也就长驱直入了。

我最近实践了一下这一过程。果然只要略微施力，并确定所需衣架的长度，两分钟不到我就

打开了锁。最让人惊讶的是，即便花大价钱安装专业的商务锁、配备防弹玻璃的金属门，同时增加后备电源和断电的情况下自动上锁的栓锁，也防不住衣架和破布。

当然，打开这些锁也可采用一些高科技的方法。有人发明了RFID克隆机，该小型设备可通过获取和重放RFID密码打开门锁。市场上也有多种复制磁性卡的设备。

3. 各种各样的开锁工具

除了扭力扳手和拨片之外，社会工程人员可能也会使用一些其他的工具（比如推刀、撞匙和挂锁垫片等）来进入目标地点。掌握了下列工具的使用技巧后，就可以轻而易举地进入目标场所了。

(1) 推刀

推刀被誉为最快捷的打开旋钮锁门的工具，如图7-6所示。旋钮锁常用于服务器机房或办公室的门。这把刀基本上可以在不破坏门的情况下切进正确的位置释放门闩。

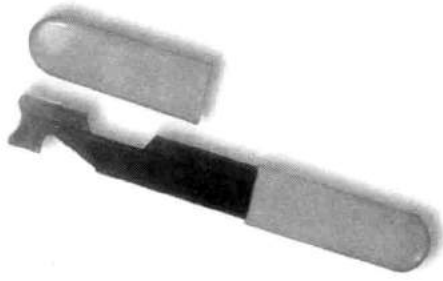

图7-6　典型的推刀

(2) 撞匙

虽然撞匙已经面世多年，但只是因为被用于犯罪行为才在新闻中被广泛关注。撞匙是经过特别设计的钥匙，用户把钥匙插进锁里，轻轻用力使之在适当的位置发生“碰撞”，将所有的弹子排成一条线，这样就可以在不破坏锁的情况下，转动锁芯。基本的技巧是把钥匙插入锁中，拔出一个或两个凹口的长度，然后对钥匙稍稍用些力，用螺丝刀或其他小物体轻轻“碰撞”钥匙。这个动作强行使弹子进入恰当的位置，这样锁芯就可转动了。图7-7展示的就是一把撞匙。

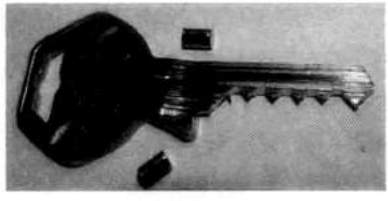

图7-7　典型的撞匙

(3) 挂锁垫片

垫片是插入挂锁底部的一小块薄金属片，用来解除锁定机制。垫片被推入底部的锁轴，将锁轴与锁定机制分开，然后解开锁。如图7–8所示。

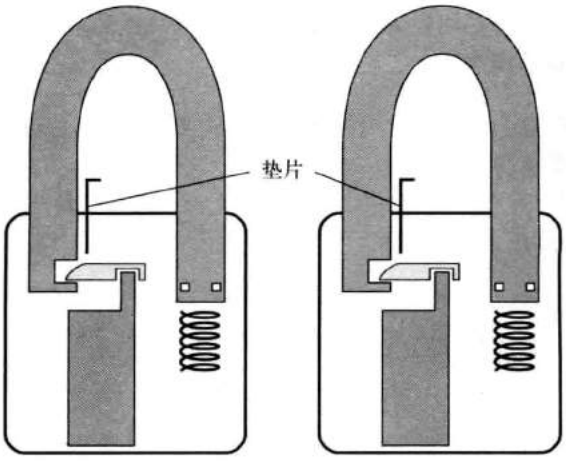

图7-8 垫片的工作原理

图7-9展示的是专业的垫片，也可用铝罐制作。

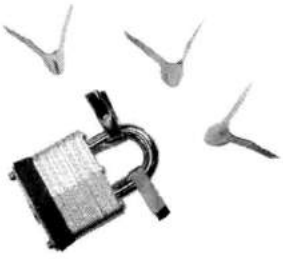

图7-9 专业垫片

近期发生的故事（参见www.youtube.com/watch?v=7INIRLe7x0Y）表明要打开宾馆或者配有链锁的房门简直易如反掌。侵入者在锁链上系上橡皮圈，利用橡皮圈本身的弹力，就可以使链锁脱落。麻省理工学院提供了一个自由发布的开锁指南（详见www.lysator.liu.se/mit-guide/MITLock-Guide.pdf），其介绍更为深入详尽。

你或许会好奇是否存在这样一种锁，它不会被撬开或至少很难被撬开。防撬双锁（Bump Proof BiLock，参见www.wholesalelocks.com/bump-proof-bilock-ult-360.html）就是这样一种锁。双锁孔设计使得它几乎不可能被撬开。

我在职业生涯中，遇到的不是锁的选择问题，而是与锁相关的安全问题。通常情况下，公司

会买一把结实的锁，需要生物识别技术和密钥才能进入服务器机房，但门旁边就是一个单层玻璃的小窗。那么谁还需要开锁器呢？贼可以轻而易举地打破玻璃闯进去。

其寓意在于单凭锁是无法保证安全的。安全是一种意识，而不是一种简单的硬件。

不是每个社会工程人员都必须成为开锁专家，但是知晓锁的基本工作原理并具有开锁经验，可能会影响社会工程行动的成败。

以上只是简单地讨论社会工程人员可能使用的开锁工具。另一个对社会工程人员具有非凡价值的工具是录音录像设备，详见下一节。

7.1.2　摄像机和录音设备

摄像机和录音设备似乎常与“偷窥”联系在一起，所以问题就来了：“为什么？为什么要在社会工程活动中使用针孔摄像机和隐蔽的录音设备？”这个问题提得好，答案很简单：为了证据，也为了自我保护。

我们先来讨论证据的概念。正如前面提到的，社会工程审计是对人进行测试。它是试图帮助一家公司修补基础架构中由人造成的薄弱点，从而提升安全性。不过恶意社会工程人侵者也可能使用相同的方法。许多人不愿意承认自己会被骗，除非证据确凿或者看到同事被骗。人们之所以不愿承认，究其原因可能是因为被社会工程人员欺骗而难堪，亦或是担心老板知道后的反应。录音设备可以提供证据，也可以据此对审计人员和客户进行培训。

使用这些设备的目的不能是让对方员工陷入困境或使其窘迫。不过，这些设备记录的信息会成为以后绝好的学习素材，可以展示员工是怎样认同社会工程人员所伪装的角色的。证明攻击会成功只是第一步，培训公司及其工作人员如何应对恶意的社会工程攻击（即如何注意、避免或者减轻这种攻击）还有很长的路要走。

社会工程活动中使用录音录像设备的第二个原因是为了自我保护，这主要针对专业的社会工程人员。为什么？仅凭肉眼观察并记录稍后可供分析使用的每个微表情、面部表情和小细节是不可能的。摄像机捕捉到的很多细节都可用来详细分析，为后续的攻击做准备。录像设备可以记录并证明你做了什么、没有做什么，而且你也无需将一切都记忆在脑中。对于分析社会工程活动成败的原因，这也是个不错的教育工具。

这项原则被执法部门广泛采用。警察和联邦探员用它来记录交通拦检、会谈和盘问等证据，这些证据可以用于自我保护、培训和法庭证明。

这些原则同样适用于录音。录下通话或谈话内容与之前所说的视频记录的目的相同。这里必须提及的重要一点是，在很多地方，未经许可的录音行为是违法的。社会工程人员必须确保与公司签署的合同中规定了自己有合法使用录音设备的权利。

录音设备的形状和大小各异。我有一个小型录音器，是一支可以使用的钢笔。该装置恰好能放在胸前的口袋里，清晰记录声音的范围可达20英尺（约为6.1米）远。加上2GB的内存，我可以轻松地记录数小时的谈话，然后进行分析。

1. 摄像机

现在可以找到形状像纽扣和钢笔的摄像机，它们可以隐藏在笔尖、时钟、泰迪熊玩具、假的螺帽和烟雾报警器中，基本上能想到的任何设备都可以隐藏摄像机。要像图7-10那样安装摄像机已非难事。

图7-10 隐藏在领带中的摄像机

信不信由你，这条领带隐藏着全彩摄像头，使用12伏电源，并连接一个小型录制设备。戴着这条领带进行社会工程审计，绝对可以录制70度视角以内的一切事物。

使用类似的录制设备好处多多，比如社会工程人员可以全力关注事先准备好的伪装或诱导方案，而不必担心遗忘任何细节。

关于录音设备的使用，我给大家讲个故事，是关于我对一个提供在线售票服务的主题公园进行的一次安全审计。这个公司开设了一个售票窗口，有一名女工作人员在里面操作Windows系统的计算机。我假装在酒店通过网络购买了入场券但是不能打印出来，于是将入场券转换成PDF格式的文件，并以邮件方式将其发送给自己。我对她说："我知道这个要求很奇怪，但是我女儿在一家餐厅看到了你们的广告，接着我们就立刻回酒店使用折扣码买了票，买完后却发现不能打印。酒店的打印机发生了故障，可我不想就这么浪费了入场券，所以把它们转换成PDF文件并发送到自己的邮箱中。您能帮我查看下文档吗？我自己登录也可以。""孩子"就等在一旁，当然，作为父亲，我不想让他失望。工作人员点击PDF的时候自然不会看到我们的票，而她的计算机已被恶意代码感染，这段代码能使我入侵她的计算机并开始自动收集信息。将谈话录音、我使用的方法以及设计的故事情节为该公司上了一堂课，以后碰到类似的情况就不再会被攻击了，从而避免了数千美元的损失。

一种使用现买现付充值卡的设备能通过手机信号给任意指定号码发送音频内容。社会工程人员可以随时拨入聆听录音内容。这个设备可用于在社会工程攻击中获取密码或个人信息，从而为社会工程人员节省了大量的时间。

人们可以花好几十个小时谈论各种精巧超酷的摄像机（我也可以写好几十页）。图7-11和图7-12展示了执法者普遍使用的一些“间谍装备”（www.spyassociates.com）。信不信由你，图片中的所有物品里都隐藏了摄像机或录音设备。可以使用其中任何一种设备秘密记录目标者的信息，以备分析。

图7-11　图中的笔可用来录音，其他物品都带有隐藏的具备录音功能的彩色摄像机

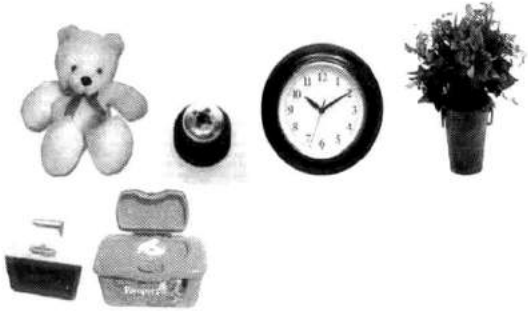

图7-12　这些物品也可通过隐藏的摄像头来录音录像

2. 使用工具

前面概述了一些不同类型的录音录像设备，但问题依旧是应如何使用。使用录音和摄像设备的基本原则与使用社会工程人员手中的其他工具（如伪装或诱导）是一样的。

最重要的还是练习。如果不能确定放置体载摄像机或录音设备的合理位置，最后可能只录到了天花板或者一段模糊的声音。准备并调校要携带的装备，并把摄像机和录音器放在适当的位置是很有必要的。试着坐下、起立、走几步，看看这些动作会不会影响音频和视频的质量。

从专业社会工程人员的角度出发，我必须再次强调合同中列出录音录像权限的重要性。如果没有合同许可，你可能会陷入法律困境。查阅当地的法规，确保使用这些设备不会惹来麻烦，也

是个不错的主意。

社会工程人员绝对不能使用这些设备故意去记录他人的窘态或窥探别人的隐私。

关于这个主题的讨论可以一直持续下去，希望本节对这些工具的概述及其使用方法的介绍能为社会工程人员打开一扇选择的大门。

下一节中，将给出社会工程人员可使用的另外一些工具的例子。

7.1.3 使用GPS跟踪器

社会工程人员通常想知道目标不在办公室时的行踪。目标在上班的路上做了哪些停留，能泄露很多信息。整合并分析这些信息有助于社会工程人员进行合适的伪装，或提出合适的问题，从而诱导目标作出正确的反应。知道目标一天工作的起始时间，对红队[①]的物理攻击也很有帮助。红队的目标是侵入并获取有价值的资产，用以暴露公司物理安全的脆弱性。

跟踪目标的方式多种多样，其中一种方法就是使用跟踪设备。GPS跟踪器是其中的一种，例如大家熟悉的可全球使用的SpyHawk超级GPS跟踪器，该设备可以从www.spyassociates.com网站买到。SpyHawk只是众多同类设备中的一种，售价大约为200~600美元。它能靠磁力吸附在汽车上，可以存储被跟踪目标好几天的信息。下面将讲述如何安装和使用这个小装置。

1. SpyHawk超级GPS跟踪器

要安装设备附带的软件很简单。只需点击运行安装软件，按照屏幕上提示的步骤操作，就可以顺利安装成功。安装后，设置步骤也相当简便。如图7-13所示，跟踪器（TrackStick）的界面很直观，设置也很容易。

如图所示，它提供了日志条数、时区和更多的自定义选项。

2. SpyHawk跟踪器的使用

SpyHawk超级GPS跟踪器很轻，易于使用和隐藏。它仅配备了一个开关键，但其中采用了一些精巧的技术。当它感应到移动时，会启动并开始记录。当移动停止一段时间后，它便停止记录。

说明书上说，该设备具有强磁性，可吸附在金属上以便隐藏，但不适用于表面粗糙或者表面是塑料的地方。第一次使用该设备时难免害怕丢失，因此在引擎盖下找到一个安全的位置，可以让人更安心，记录效果也更佳。当接近目标车辆时（无论是内部还是外部），轮舱、引擎盖下面或者后备厢等带有金属的地方都比较安全。如果你能接触汽车内部，打开引擎盖，将它放在里面，就更不用那么担心被发现或丢失了。

---

① 红队是指计算机和网络安全专家，他们得到系统主人的授权攻击系统，以找出恶意黑客可能利用的安全漏洞。也被称为伦理黑客、入侵测试等。——译者注

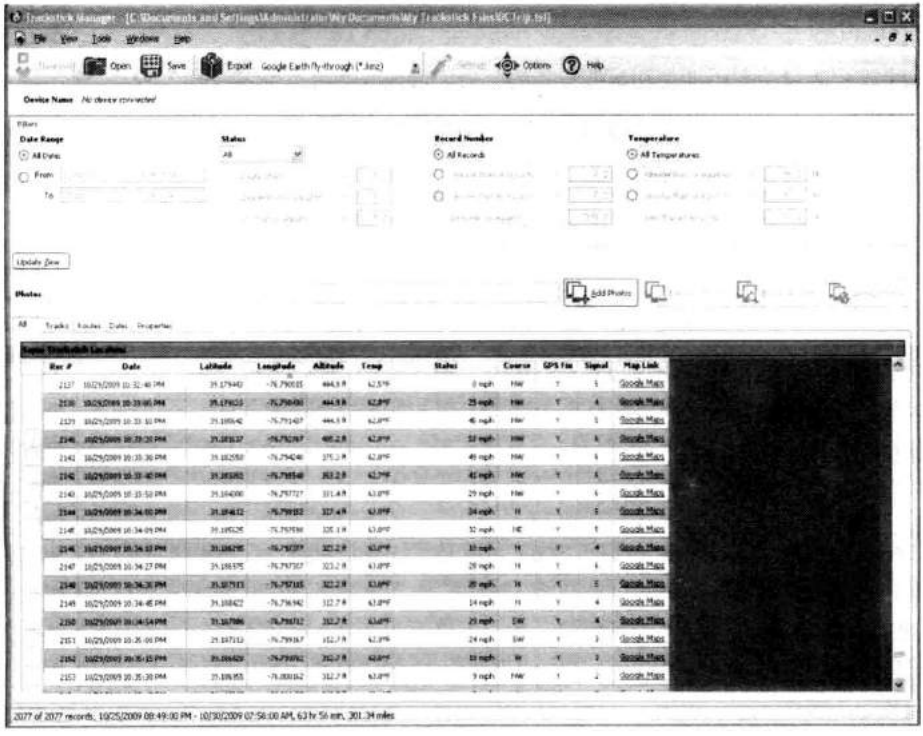

图7-13　跟踪管理器提供了直观易用的用户界面

第一次测试时，我将装置放在了引擎处。即使是隔着金属引擎盖，记录质量也非常完美。另一个理想的做法是，等到目标汽车开锁后，将跟踪器放置在车厢内的脚垫下，或靠近尾灯的位置。根据我的记录，该装置在测试中收集了5天的数据，其中一些可以在下图中看到。如图7-14所示，看起来这个目标喜欢开快车。

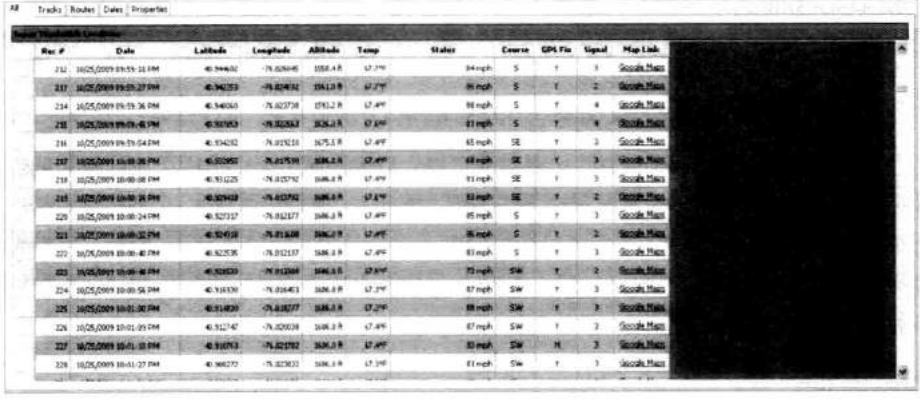

图7-14　目标喜欢开快车

时间、日期和时长标记有助于你勾划出目标的行驶轨迹，如图7-15所示。

All | Tracks | Routes | Dates | Properties

Super Trackstick Dates

Date	Time Period	Record #'s	Total Duration	Distance
[redacted]	08:49:00 PM - 12:00:54 AM	2 - 919	3 hr 11 min	175.59 mi
10/26/2009	12:00:00 AM - 12:00:40 AM	920 - 1373	13 hr 54 min	61.42 mi
10/27/2009	12:00:40 AM - 12:00:00 AM	1373 - 1610	15 hr 13 min	13.02 mi
10/28/2009	12:00:00 AM - 12:00:00 AM	1610 - 1908	14 hr 35 min	16.85 mi
10/29/2009	12:00:00 AM - 10:54:45 PM	1908 - 2244	14 hr 24 min	27.79 mi
10/30/2009	05:19:00 AM - 07:58:00 AM	2245 - 2343	2 hr 39 min	6.51 mi

图7-15 被跟踪目标的行驶轨迹

图7-16显示了信息在谷歌地球上的呈现，包括速度、时间、停止时间及其他信息。

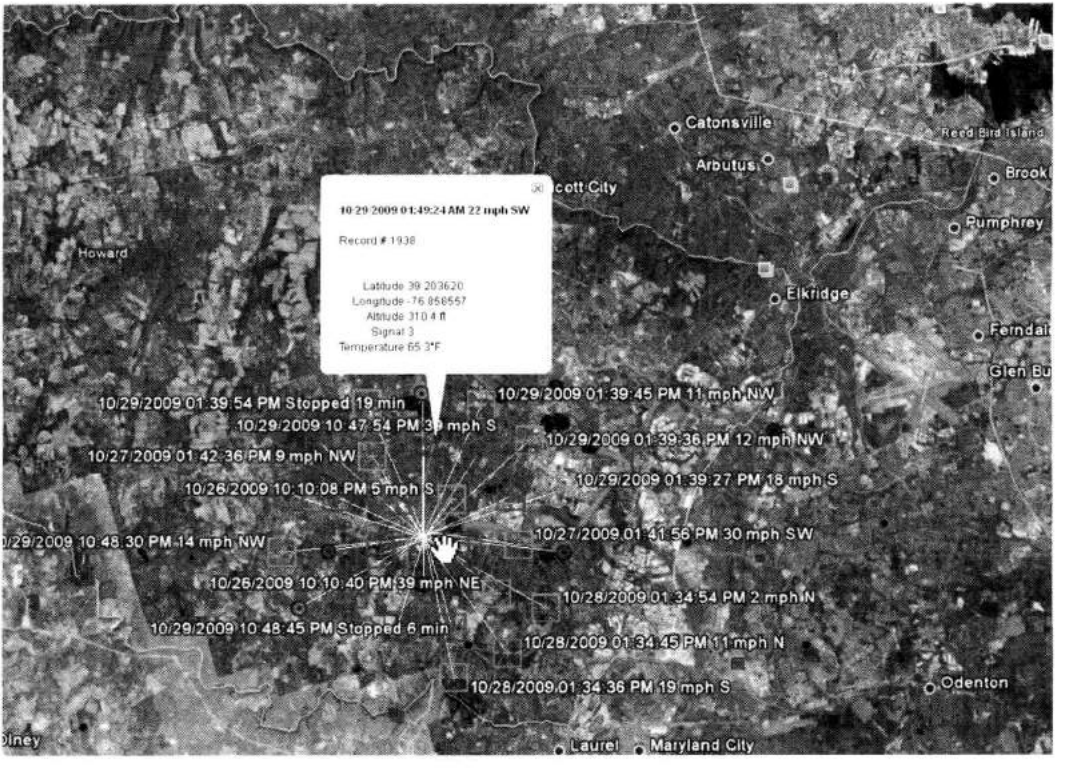

图7-16 装置提供谷歌地图输出

如图7-17所示，软件完美地展示了完整的线路图。

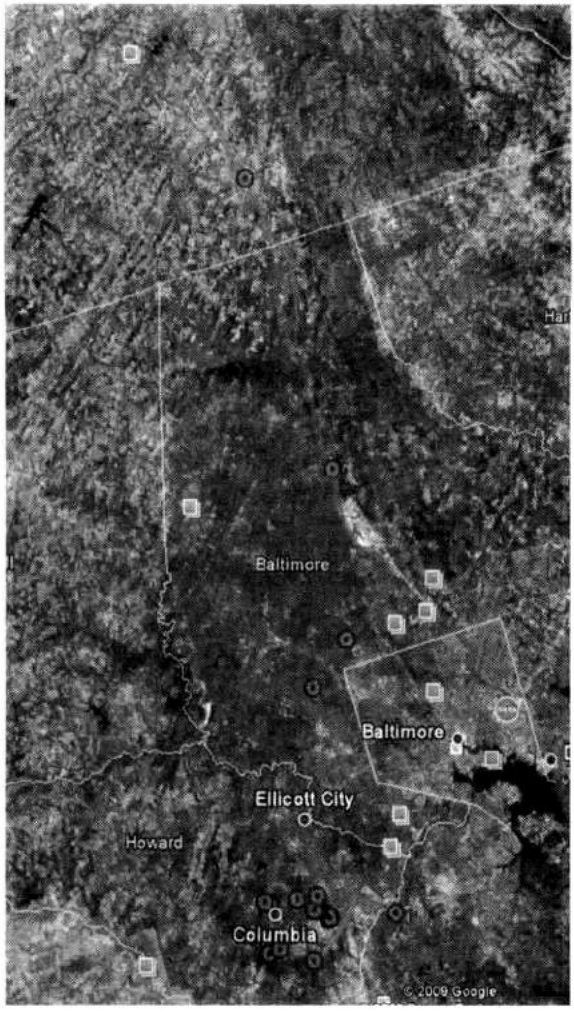

图7-17　跟踪器给出的目标行驶路径

利用谷歌地球或谷歌地图软件，可以放大查看细节（见图7-18）。

3. GPS跟踪器数据分析

跟踪器采集的数据对社会工程人员大有裨益。如果能够跟踪到目标公司的CEO每次喝咖啡的地方、最喜欢的商店以及健身会所等信息，将有助于社会工程人员作出成功率最高的攻击计划。

了解了目标的位置及停留的地方，攻击者就可以确定在何处复制RFID证件或者取得钥匙模印的机会最大。这样做的好处在于不必伪装成邻居悄悄靠近目标。下面的图片展示了攻击者如何利用这些细节占尽上风。

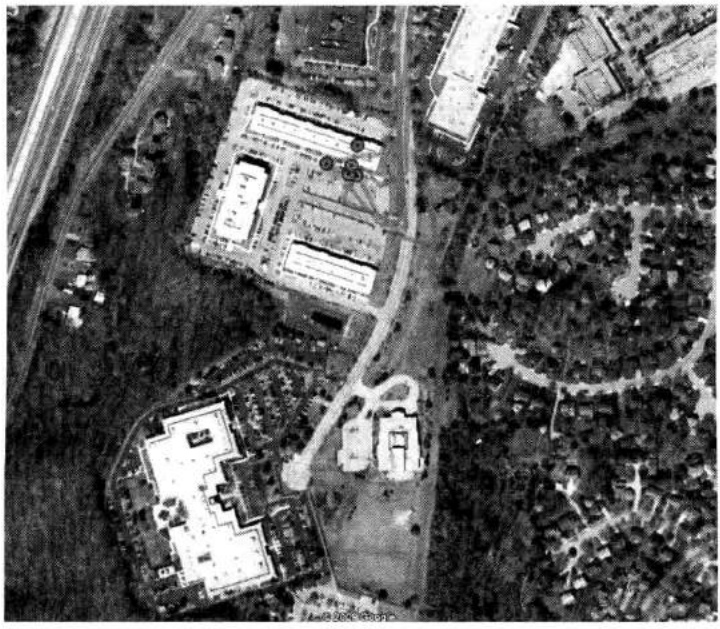

图7-18 放大目标移动的路线

请注意图7-19中的细节。你可以看到目标开车的速度以及停车的日期和具体时间。如果想看到其位置的更多细节，点击谷歌地图链接，点击“导出”按钮，将所有的数据集导出到谷歌地图或谷歌地球中。

图7-19 数据集

在谷歌地球中打开数据集后，你可以看到他的停车点、行驶的路线以及停下的次数等，如图7-20所示。

图7-20　路程中的暂停点

如果你想看他的整个行驶路线，没有问题，只要从众多格式中选择一种输出整个路线，如图7-21所示。

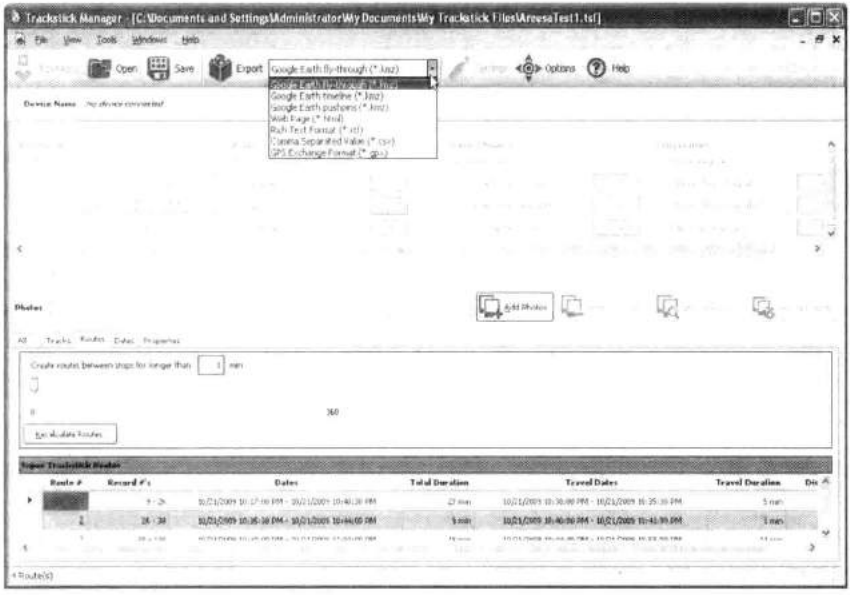

图7-21　导出目标的整个行驶路线

图7-22是从谷歌地图上导出的数据。

图7-22 在谷歌地图上显示目标的移动路线

短短的一节不足以涵盖社会工程人员使用的全部工具，成功的关键在于多练习和研究。知晓什么样的工具能决定审计活动的成败只是成功的基础。作为一名专业的社会工程人员，你必须练习、练习，再练习！了解工具的正确使用方法至关重要。

在网站www.social-engineer.org给出的社会工程人员框架中，我会分析很多提高社会工程人员实践能力的工具。

要想成为成功的社会工程人员，光掌握物理工具还远远不够，因为所有这些工具的应用效果都依赖于其质量及第2章中讨论的全面的信息收集。下一节将讨论世界上最神奇的信息收集工具。

7.2　在线信息收集工具

如前所述，信息收集是社会工程的一个关键方面。若在这一点上投入的精力不足，可能会导致社会工程行动的失败。现在，社会工程人员可以通过多种工具来收集、分类以及运用信息。

这些工具完全改变了社会工程人员查看和使用数据的方式。他们将不再局限于使用常规的搜索方式找寻数据，这些工具为他们打开了互联网的资源之门。

7.2.1　Maltego

收集和分类信息可能是很多社会工程人员的薄弱环节。如果存在一个工具，它可以同时对一个域名、IP地址，甚至是一个人进行几十种搜索；能提示各项信息的权重，显示信息重要与否；有一个GUI界面，可以用不同颜色表示不同的对象，可以导出利用；最重要的是有免费的版本可用，怎么样？

Maltego就是社会工程人员梦想的工具。这个神奇的工具是由Paterva公司（www.paterva.com）的员工开发的。Maltego有一个免费的社区版本，可以从他们的网站下载，BackTrack4的每一个版本中都集成了Maltego程序。如果想要解除免费版在功能上的限制，如可转换的次数及保存数据，花费大约600美元就可以得到完整的授权。

我参与的一次审计充分证明了Maltego的强大威力。当时我的任务是对一家小公司的网站进行安全审计。目标是入侵该公司CEO的计算机，但他是一个严谨、古板、不常使用网络的人。作为印刷公司的老板，他只关心自己的生意，几乎不使用高科技。显然这项任务极具难度。

我首先打开Maltego。通过该公司的域名，提取所有网站页面和Whois数据库中的电子邮件地址，这是个很好的信息基础。然后我深入查看这位CEO的电子邮件是否在其他网站或链接中使用过。我发现他给当地的一家餐厅写了一些评论，并公开了他的电子邮件地址。同样，他在对另一个州的一家餐厅的评论中也给出了电子邮件地址。从评论中可以发现，他去这个州探亲时去过这家餐厅，评论中甚至提到了他兄弟的名字。使用Maltego做进一步调查，我找到了他父母和兄弟在这一地区的住址。通过对姓氏进行搜索，我找到一些新的链接页面，其中提到了他在那里创业时使用的另一个邮箱，以及他与当地教堂发生了矛盾，而后转到了另一家教堂。随后，我发现他Facebook上链接的一篇博文，其中有他们一家人在观看完最喜欢的球队比赛后的一些照片。下面是我花了不到两小时的时间，用Maltego获得的调查结果。

- 他喜欢的食物；
- 他喜欢的餐厅；
- 他孩子的姓名和年龄；

- 他离婚了；
- 他父母的名字；
- 他兄弟的名字；
- 他长大的地方；
- 他的宗教信仰；
- 他喜爱的球队；
- 他家庭成员的相貌；
- 他过去的生意。

一天后，我给目标发送了一封邮件，里面包含针对当地公司的一个摇奖信息。中奖者可以去他喜爱的餐厅享用一顿免费大餐，同时获得三张扬基队的球赛门票。所有参与的公司必须同意与一名销售代表简单讨论当地的慈善活动。如果该公司同意，其名字就会进入摇奖获选序列，并有机会赢取扬基队的球赛门票。我伪装成“乔”，然后准备了一份与该公司CEO通话的提纲。我的目标是让他接收一个PDF文档，那是我们给他设定的圈套。我打电话的时候，他应该已经收到了我的邮件，我也很容易通过这个话题切入：“是的，他正在等我打电话。”

在与“乔”的通话中，CEO接收并打开了包含详细摇奖信息以及恶意加密文件的邮件，该文件会发起一个反向会话，让我侵入他的系统。

当然，他的屏幕上没有显示任何信息，他只是对Adobe不停地崩溃感到沮丧。我告诉他：“我很遗憾，你无法打开文件。我们会将您的名字列入抽奖名单并且今天会发送一些额外的信息给您。”但在发送邮件之前，我召集了一个报告会，讨论目标是如何被完全入侵的。

这次社会工程活动的成功主要在于使用了Maltego。它能帮助我们以最佳方式收集、组织和分类数据。

Maltego是如何帮助我在这次行动中取得成功的呢?

将Maltego视为一个信息的关系型数据库，能发现互联网上信息之间的联系（在应用中称为实体）。Maltego在后台做了很多工作，如挖掘电子邮件地址、网站、IP地址和域信息。举例来说，点击几下鼠标你就可以通过目标域名自动地搜索到所有相关电子邮件的地址信息。只需在屏幕上简单地增加“电子邮件”转换器，输入想要搜索的电子邮件地址，就可以得到图7-23所示的效果。

使用Maltego的原因

Maltego能自动采集大量信息并为用户实现数据的自动关联，可以为用户节省数小时的搜索时间，并展示信息的关联图。Maltego真正的强大之处在于找到这些数据之间的关系。尽管数据挖掘很有用，但是展示信息之间的关系对社会工程人员更有价值。

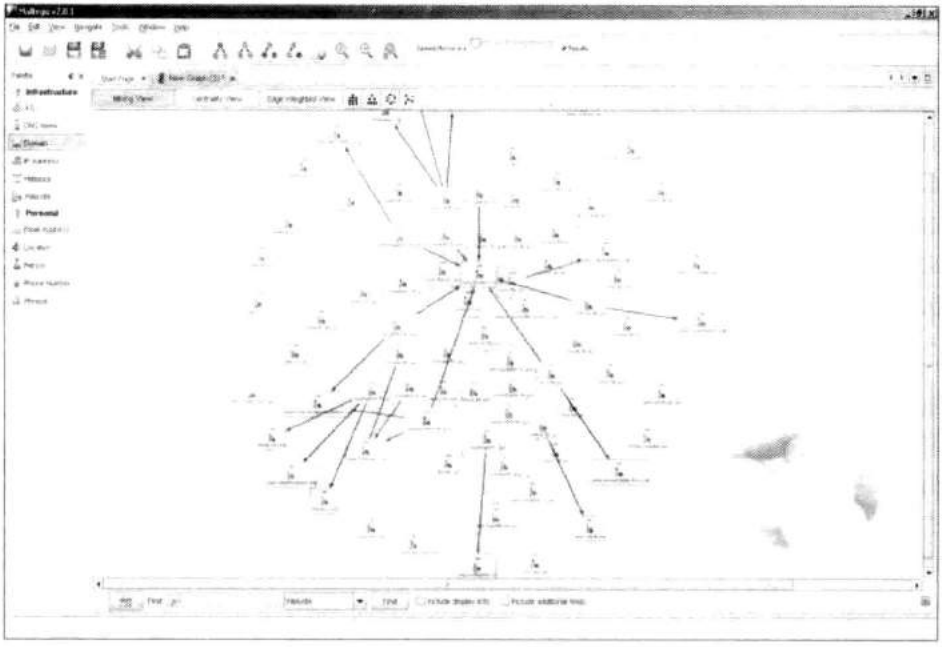

图7-23　Maltego收集的信息展示

我在www.social-engineer.org/se-resources/贴出了一些视频，讲解怎样高效地使用Maltego。前面的案例中Maltego居功至伟，但后续的入侵使用了另外一个强大的工具。

7.2.2　社会工程人员工具包

社会工程人员花费了大量时间来完善自身的技能，然而，许多攻击方式需要通过创建附加恶意代码的邮件或PDF文档来实现。

这些事情都可以利用BackTrack中包含的诸多工具来手动完成。起初搭建www.social-engineer.org网站的时候，我曾和好友戴夫·肯尼迪交谈过。戴夫是流行工具FastTrack的开发者，FastTrack使用Python脚本和网页界面能够自动实现渗透测试中的一些最常用的攻击。我对戴夫说，单独为社会工程人员开发一个类似FastTrack的工具是个不错的主意，这个工具让社会工程人员点击几下鼠标就能创建PDF文件、电子邮件及网站等，这样就可将注意力集中到社会工程中的“社会”这部分上来了。

戴夫仔细思考了这个问题，决定创建一些简单的Python脚本，让社会工程人员可以创建附加恶意代码的PDF文件并随邮件发送。于是社会工程人员工具包（Social Engineer Toolkit，SET）就诞生了。在写本书的时候，SET已经被下载了150多万次，而且很快成为社会工程人员审计时配备的标准工具包。本节将介绍SET的主要特点及使用方法。

1. 安装

安装步骤十分简单，只需安装Python和Metasploit框架。这两个软件在BackTrack发行版中已经存在，所以不用担心。BackTrack 4甚至已经包含了SET。如果需要从头开始安装，过程也十分简单。依据导航进入安装目录，在控制台窗口上运行如下命令：

```
svn co http://svn.secmaniac.com/social_engineering_toolkit set/
```

执行完命令之后，将得到一个名为set的目录，该目录下包含了所有SET工具。

2. 运行SET

运行SET的过程也很简单。只需在set目录下输入./set，就会启动初始SET菜单。

请访问www.social-engineer.org/framework/Computer_Based_Social_Engineering_Tools:_Social_Engineer_Toolkit_%28SET%29，这里有SET菜单的完整展示图，以及对每个菜单选项全面、深入的介绍。接下来介绍SET中两个最常用的功能。

首先讨论鱼叉式网络钓鱼攻击，然后讨论网站克隆攻击。

(1) 鱼叉式网络钓鱼

网络钓鱼是一个术语，描述恶意诈骗犯如何通过定向设计的电子邮件“广泛撒网”，吸引人们访问特定的网站、打开恶意文件或者输入个人敏感信息，为以后的攻击做准备。要在今天的互联网世界生存，必须能够检测并防御此类攻击。

社会工程审计人员使用SET可以创建有针对性的电子邮件对客户进行测试，然后记录有多少雇员上当了。这个信息随后可用于培训，以帮助员工识别和避免这些陷阱。

使用SET进行鱼叉式网络钓鱼攻击，选择选项1。选择1后，会看到如下几个选项：

- 执行群发邮件攻击
- 创建一个文件格式负载
- 创建一个社会工程模板

要进行邮件式钓鱼攻击，选择第一个选项。第二个选项用于创建一个恶意的PDF或其他文件，以备作为邮件附件发送。第三个选项用以创建模板，待日后使用。

在SET中发起攻击十分简便，只需选择正确的菜单选项然后点击启动。例如，如果我想发动邮件攻击，向受害者发送伪装成技术报告的恶意PDF文件，我会选择选项1——执行群发邮件攻击。

接下来，我会选择一个攻击向量（选项6），这种攻击对很多版本的Adobe Acrobat Reader软件

都有效——应用了Adobe util.printf() Buffer Overflow[①]漏洞。

接下来几个选项会设置攻击的技术问题。点击选项2——Windows Meterpreter Reverse_TCP。使用Metasploit接收反向会话或者受害者电脑的IP和端口，以避免入侵检测系统（IDS）或其他系统的报警。

选择443端口，使数据流看起来好像是加密的SSL数据。SET会创建恶意PDF文件并设置监听功能。

执行上述步骤后，SET会询问是否要更改PDF的文件名，例如改成类似TechnicalSupport.pdf等更加隐蔽的名称，然后输入邮件信息以备收发。最后，SET发出一封看起来很专业的电子邮件，引诱用户打开附件中的PDF文件。受害者收到的邮件如图7-24所示。

图7-24　一封无害的电子邮件与一个简单的附件

邮件发送之后，SET会创建一个网络监听器等待目标打开文件。一旦目标点击了PDF，监听器就会执行恶意代码，让攻击者得以进入受害者的计算机中。

真是惊人（也许有人并不这样认为），所有这一切只需点击六七下鼠标，审计者便可将精力集中在攻击中真正的社会工程方面了。

这是一个破坏性很强的攻击，因为它利用了客户端软件的漏洞，而且在大多数情况下，屏幕上不会出现任何提示。

这只是应用SET可以发动的众多攻击中的一种。

(2) Web攻击

SET也允许审计人员克隆任何网站并在本地运行。这种攻击类型的强大之处在于可以让社会工程人员以多种方式诱骗他人访问克隆网站并从中获利。社会工程人员既可以伪装成更新网站的开发者，也可以仅仅对网址进行细微的修改（填加或删除一个字母），最终诱使他人访问克隆的网站。

① 请参见http://www.nsfocus.net/vulndb/12573。——译者注

一旦有人访问了克隆网站，社会工程人员便可以发动多种不同的攻击，包括信息收集、证书收集和直接入侵等。

要在SET中运行此攻击可从主菜单中选择选项2（网站攻击），选择之后，可以看到以下几个选项：

- Java Applet攻击方法
- Metasploit浏览器的入侵模式
- 证书获取的攻击方式
- 标签绑架攻击方法
- 中间人攻击方式
- 回到前面的菜单

选项1中的Java Applet攻击是一种特别邪恶的攻击。一般情况下，Java Applet攻击会在用户界面上弹出一个Java安全警告，说该网站已被ABC公司签名，并让用户同意这一警告。

进行这种攻击，先选择选项1，然后选择选项2——网站克隆（Site Cloner）。

选择网站克隆的时候，需要输入你想克隆的网站地址。这里可以选择想克隆的任何网站——客户的官方网站、客户供应商网站或者政府网站。正如你所想象的，重点在于选择一个对目标有意义的网站。

在这个练习中，假设是克隆Gmail网站。屏幕上会显示如下信息：

```
SET supports both HTTP and HTTPS
Example: http://www.thisisafakesite.com
Enter the url to clone: http://www.gmail.com
[*] Cloning the website: http://www.gmail.com
[*] This could take a little bit...
[*] Injecting Java Applet attack into the newly cloned website.
[*] Filename obfuscation complete. Payload name is: DAUPMWIAHh7v.exe
[*] Malicious java applet website prepped for deployment
```

上述工作完成之后，SET会询问你想要在自己与被害者之间创造什么类型的连接。要想使用本书讨论的技术，选择Metasploit的反向会话界面，也就是Meterpreter。

SET为负载加密提供了多种选项，这是为了避开反病毒系统的检测。

下一步，SET启动内嵌的网站服务器为克隆网站提供服务，同时启动监听器准备捕获浏览该网站的受害者。

现在只需要社会工程人员构造一封电子邮件或给目标打个电话，让目标访问该假冒的网站。最后，用户会看到如图7-25所示的界面。

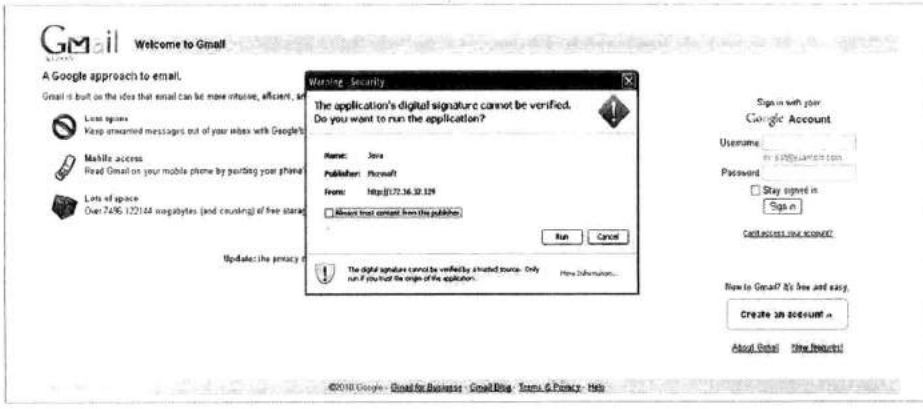

图7-25　谁会不相信微软签名的小程序呢?

最终结果是，一个Java Applet出现在用户面前，告诉他该网站已被微软签名，他需要允许安全证书运行，才能继续访问网站。

只要用户允许了该安全证书，攻击者就可以立刻入侵他的计算机了。

3. SET的其他特性

SET是具有实战思维的社会工程人员开发出来的，所以工具集所提供的都是审计过程中常常会用到的攻击方法。

SET在不断更新和发展。例如，最近几个月，除网站克隆和网络钓鱼攻击之外，SET又增加了一些其他的攻击方式，还增加了一个传染性媒体生成器。传染性媒体生成器允许用户创建带恶意文件的DVD、CD或USB，这些传染源可以混杂在目标对象的办公大楼里。当它们被插入计算机时，将触发恶意负载程序的执行，从而开启受害人机器的入侵之门。

SET也能创建简单的负载和相应的监听器。如果社会工程人员想要通过一个提供反向会话功能的EXE可执行程序连接回他的服务器，可以在审计过程中携带一个U盘。如果面前的机器是他想要远程访问的，便可将U盘插入，导入负载文件，然后点击运行。这样可以在目标机器和自己的机器之间建立起一个快速连接。

有一种较新的攻击方式叫Teensy HID攻击。Teensy设备是一个小的可编程电路板，可嵌入键盘、鼠标或其他可插入电脑的电子设备。

SET可对Teensy编程，设置这个小电路板在插入电脑时将执行何种命令。常见的命令包括创建反向会话或监听端口等。

SET的最新特性之一是提供了一个Web界面。这意味着SET会自动启动Web服务器程序，从而更易于应用。图7-26显示了这个网页界面的概貌。

图7-26 SET的新Web界面

SET是一款强大的工具，它能帮助社会工程审计人员测试出公司存在的常见弱点。SET工具的开发者总是善于听取他人的意见，在工具中增添新的应用，使得其不断完善、越来越流行。如果想更深一步了解这个强大的工具，可以登录www.social-engineer.org网站，上面包含每个菜单选项的详细说明。在使用过程中，可以通过www.social-engineer.org和www.secmaniac.com这两个网站不断更新SET。

7.2.3 基于电话的工具

社会工程书籍中最早介绍的工具之一就是电话。如今，随着手机、网络语音以及自制电话服务器的出现，社会工程人员使用电话的方式越来越多样。

社会工程人员需要熟练掌握电话的使用技巧以便进行成功的审计，因为人们经常会受到电话销售、推销和广告的骚扰。尽管有一些限制，但作为社会工程的工具，电话还是可以用来在短时间内搞定一家公司的。

在一个人人都有手机的时代，人们会在公共汽车、地铁或者其他公共场合，使用手机接打私人电话或进行深入的交谈，使用手机的方式多种多样。利用手机进行窃听或与目标直接通话，这些攻击方式在过去是不可能实现的。随着市场上智能手机和具有计算机功能的手机日益增多，越来越多的人在手机上储存密码、个人数据和私人资料。这为社会工程人员通过不同场合接触目标、获取数据打开了一扇新的大门。

如果拨号者可以通过某种“方式”提高其可信度，那么每天24小时开机就增加了信息泄露的几率。例如，如果来电显示表明电话是从公司总部打来的，则许多人会毫不犹豫地提供信息。苹果和安卓智能手机都有可供利用的应用程序，可以将来电显示号码篡改成任何号码。利用类似SpoofApp（www.spoofapp.com）的应用程序，社会工程人员能够以较低的成本将拨出的号码伪装成从任何地方打来的电话号码。这一切都将提高伪装的可信度。

社会工程中电话的使用可以分为两个不同的领域：背后的技术和编造的借口。

1. 篡改来电显示

来电显示在商务和家用电话中都已成为一项普遍的技术，特别是在当前手机普遍取代固定电话的情况下，来电显示已成为日常生活的一部分。成功的社会工程人员必须意识到这一事实并且知道如何加以利用。

来电显示篡改主要是篡改目标的来电显示信息。换句话说，尽管你使用某一号码拨号，但显示在对方屏幕上的却是另一个号码。

利用该技术的一种方法是伪装成在垃圾箱里找到的目标公司的供应商的号码。如果社会工程人员发现ABC公司是目标的计算机技术支持单位，就可以找到该公司的号码，在打电话跟目标预约下午见面时伪装该号码。通过篡改来电显示，你可以伪装成以下机构或个人：

- 远程办公室
- 办公室内部
- 合作伙伴
- 公用事业/服务公司（电话、水、网络及专业灭虫人员等）
- 上司
- 快递公司

到底怎样篡改来电显示呢？下面将讨论一些可供社会工程人员使用的方法和设备。

2. SpoofCard

最流行的一种篡改来电显示的方法是使用SpoofCard（www.spoofcard.com/）。使用这种卡，可以假冒随卡提供的800个号码，输入PIN码和希望显示的号码，然后输入想拨打的电话号码就可以了。

SpoofCard的一些新特性也很有用，比如对通话内容进行录音、伪装成男声或女声等。这些特性大大提高了拨号者的伪装能力，社会工程人员可以借此欺骗对方提供其所需要的信息。

从另一方面来说，SpoofCard简单易用，除了电话不需要其他额外的硬件或软件，并且有成千上万的用户证实了它的有效性。SpoofCard唯一不好的一点就是需要付费购买。

3. SpoofApp

越来越多的人开始使用苹果、安卓及黑莓等智能手机，这些手机上都有大量的应用可以用来伪造来电显示。SpoofApp将SpoofCard技术实现在了软件包中。

不用真的拨打指定的号码，只需在应用程序中输入想要拨打的电话号码，然后输入想要显示的号码，SpoofApp就会和目标建立连接，而目标电话上显示的就是你输入的想要显示的号码。所有操作只需点击几下按钮即可完成。

4. Asterisk

如果有一台多余的计算机和一个VoIP服务，也可以使用Asterisk服务器来篡改来电显示。可以在www.social-engineer.org/wiki/archives/CallerIDspoofing/CallerID-SpoofingWithAsterisk.html页面上找到一些有关这种手段的信息。Asterisk服务器的运行机制与SpoofCard非常相似，只是用于篡改来电显示的服务器不一样。在这种情况下，你使用的是自己的服务器。这一点很有吸引力，因为它提供更多的自由并且不必担心线路中断或时间耗尽。

Asterisk的优点在于免费、安装好后使用简单并具有很大的灵活性，你可以自己控制它。缺点在于不仅需要额外的计算机或虚拟机，还需要知道如何使用Linux，此外还需要一个可用的VoIP服务提供商。

使用Asterisk的最大好处就是，有关呼叫方和被叫方的信息完全由社会工程人员自己控制。个人信息和账号数据不在第三方手中。

5. 使用脚本

电话是社会工程人员最喜爱的工具。只需稍稍改变一下伪装，社会工程人员就能在不泄露身份的情况下攻击很多目标。

在使用电话进行社会工程活动的过程中，必须考虑使用脚本。脚本是电话社会工程中必不可少的部分，它能确保所有需要的要素都被涵盖和涉及。不过，脚本不是按部就班的演讲稿。对目标来说，没有什么比对方像背台词般说话更不快的了。

写完脚本之后，应该反复练习，这样才能令你听上去真实、真诚、可信。

这就是信息收集至关重要的原因。信息收集得越全面，脚本编写也就越清晰。我发现掌握目

标的一些兴趣和爱好很有帮助，这样更易于构建共识。

搜集的信息充足有助于你勾勒出攻击计划。在前面讨论的攻击印刷公司CEO案例中，我准备的大纲中包括了要说的关键内容、想要涉及的要点，以及一些提示，如在通话过程中要“清楚地表达”、“不要忘了提及慈善部门”及“放慢语速”等，这让我在打电话时得以集中精力。

使用脚本或大纲（而非照本宣科的草稿）可以让你流利且自然地与对方交流，而且在应对意外状况时也能从容镇定。

电话仍然是社会工程人员十分重要的工具，如果在实际应用中与本书提到的技术和方法相结合，便可以获得成功。

7.2.4　密码分析工具

另一组不得不提的工具就是密码（口令）分析工具，它们能帮助你分析目标及其可能使用的口令。在目标信息收集完成之后，下一步就是分析其可能使用的口令和攻击他的方式。社会工程人员可以构建一个潜在的口令列表用于暴力破解。从工具的角度来看，构建可能的口令列表可以加速攻击。本节将介绍几个可用的密码分析工具。

为了完成任务，密码分析工具可能需要持续运行几小时甚至几天。

尽管发出了很多警告，但每年遭到简单攻击的人数仍在不断上升。在网上公开个人信息的人数是惊人的，公开的信息各种各样，关于自己、家庭以及生活琐事等。基于人们在社交媒体上泄露的信息，以及在网络上可以找到的其他信息，凭借接下来讨论的工具，社会工程人员甚者能勾勒出某些人的全部生活。

密码分析卓有成效的原因之一是人们选择密码的方式。实践证实很多人反复使用相同的密码。更糟糕的是很多人使用的密码很容易猜测，而且不需要什么技巧。

最近，BitDefender（一家网络安全公司）的一项研究证实了这一点。BitDefender分析了25万多名用户使用的密码，结果十分惊人：其中75%的用户所使用的邮箱密码和社交媒体账户的密码是相同的。再想想近期有1.71亿Facebook用户的个人信息被人以P2P种子的方式发布到网上，这多么恐怖啊。完整的文章内容参见www.securityweek.com/study-reveals-75-percent-individuals-use-same-password-social-networking-and-email。

2009年，一名昵称为Tonu的黑客做了一项很有趣的研究。通过获取某个流行社交网站近期弃用的URL，他伪造了页面，对试图登录的人进行了一段时间的记录。不过他这样做并没什么恶意。

你可以在www.social-engineer.org/wiki/archives/BlogPosts/MenAndWomenPasswords.html看到研究结果。