其中的一些信息甚至震惊了资深的社会安全专家。在734 000人中，有30 000人使用自己的名字作为密码，有约14 500人使用他们的姓氏作为密码。更惊人的是下面的统计数字，最常使用的8个密码如下表所示。

密　码	性　别	用 户 数
123456	男	17 601
password	男	4 545
12345	男	3 480
1234	男	2 911
123	男	2 492
123456789	男	2 225
123456	女	1 885
qwerty	男	1 883

17 601位男性使用的密码是123456？真是令人震惊啊。

如果这还不够令人震惊，再看看Tonu公开的统计数据吧：66%以上的用户使用的密码长度为6到8个字符。由于大多数人使用的都是弱口令，通过使用流行的密码破解工具，例如图7-27中展示的“Cain and Abel”，社会工程人员破解这些弱口令并非难事。

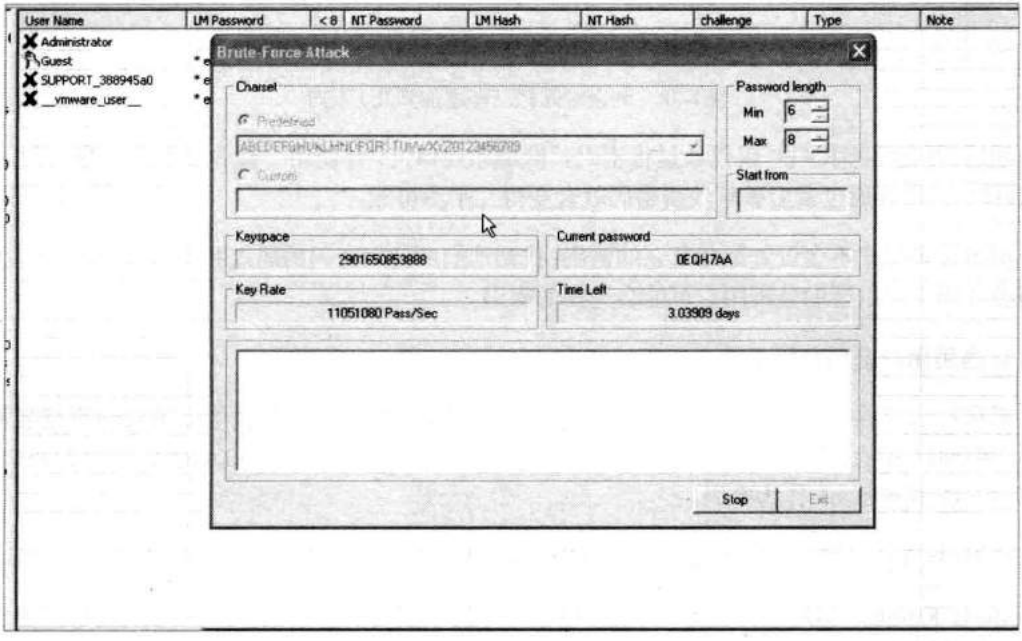

图7-27 破解弱口令只需要3天

请注意剩余时间栏写着3.03909天。对大多数黑客来说，三天就能获得服务器的访问权限算是短的了。难道用三天获取管理员密码算很长吗?

为使这一信息真正切中要害，请看图7-28。如果同一个用户使用14~16个字符的密码，其中包含大小写字母和非字母字符，破解所需要的时间就不是一般地长了。

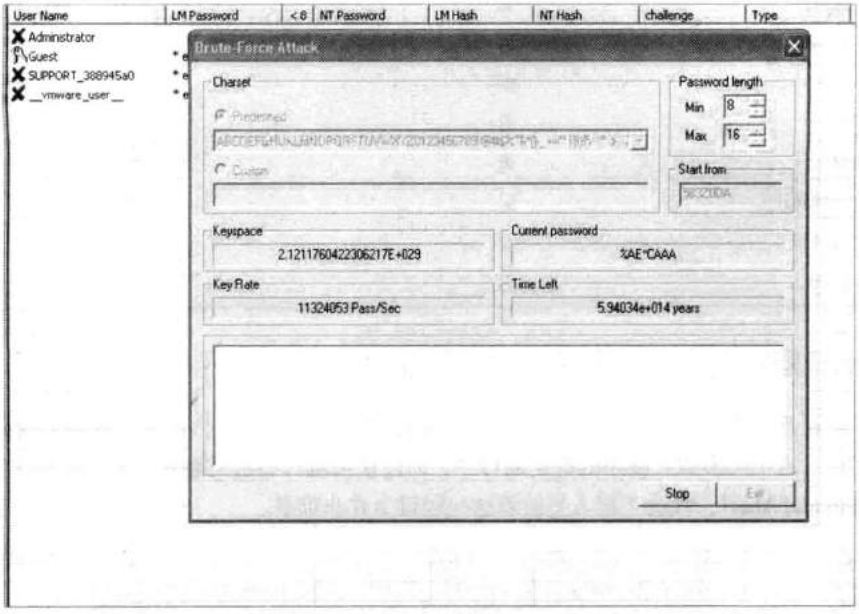

图7-28　剩余时间栏已经增加到几万亿年

超过5万亿年够长吗？仅仅通过将密码长度增加到14位，并使用一些非基本的字符（即*、&、$、%和^），黑客通过暴力破解获得密码就会变得几乎不可能。

由于许多用户不会设置如此复杂的密码，找到他们所使用密码的弱点并不困难。某些工具（下面将会介绍）可以帮助分析用户可能会选择的密码。

1. 通用用户密码分析工具

成功社会工程审计的一项重要工作就是对目标对象进行分析。前面给出的Tonu研究案例显示：734 000人中有228 000人以上只使用6位字符的密码，其中超过17 000人的密码是123456，大约4600人使用password作为密码。

通用用户密码分析工具（Common User Password Profiler，CUPP）使得密码分析工作更加简单。

Muris Kurgas，或称为j0rgan，开发了这个神奇的小工具。它是包含在BackTrack渗透测试工具中的一个脚本，也可以通过www.social-engineer.org/cupps.tar.gz下载。

最普遍的认证形式是用户名加密码或口令短语。如果两个值都与本地存储表中的值匹配，用户就可以成功访问。密码的强度就是猜测、使用加密技术或自动化测试库破解密码的难度。

弱口令可能非常短或只使用数字和字母字符，这样就很容易破解。弱口令也很容易被那些对用户进行分析的人猜到，比如生日、昵称、住址、宠物或亲属的名字，或者God、love、money及password等常用单词。

由于大多数用户使用容易猜到的弱口令，因此CUPP是一个完美的分析工具，它可以用于合法的渗透测试和犯罪取证调查。

以下源自BackTrack 4中使用CUPP会话的内容。

```
root@bt4:/pentest/passwords/cupp# ./cupp.py -i
[+] 输入对象信息以生成字典[小写！]
[+] 如果不知道相关的信息，只需输入回车！;)
> 名字：John
> 姓氏：Smith
> 昵称：Johnny
> 生日 (DDMMYYYY; i.e. 04111985)：03031965
> 配偶名字：Sally
> 配偶昵称：Sals
> 配偶生日 (DDMMYYYY; i.e. 04111985)：05011966
> 子女名：Roger
> 子女昵称：Roggie
> 子女生日 (DDMMYYYY; i.e. 04111985)：05042004
> 宠物名：Max
> 公司名：ABC Paper
> 还要加入一些与目标有关的关键词吗？ Y/[N]：Y
> 请输入每个词，以逗号分隔 [i.e. hacker, juice, black]：christian,polish,sales person
> 需要在每个词的尾部加入特殊字符吗？ Y/[N]：N
> 要在每个词的尾部添加一些随机数吗？ Y/[N]n
> 黑话模式？(i.e. leet = 1337) Y/[N]：Y
[+] 现在生成字典……
[+] 排序并移除重复字符……
[+] 字典保存到文件中，共生成13 672个密码
[+] 现在你可以使用了，祝好运！
```

请注意，根据所提供的资料最后创建了包含13 672个密码的字典文件。此类工具的作用在于减少了社会工程人员猜测密码的工作量。

2. CeWL

据其开发者描述，CeWL是一个Ruby应用程序，它可以通过给定的URL进行指定深度的搜索，并可扩展到外部链接，最终生成一个可用于密码破解的字典文件，John the Ripper等密码破解工具可以使用这个字典进行密码破解。有关CeWL的更多资料请参见www.digininja.org/projects/cewl.php。下面看一下在BackTrack 4中使用的情况。

```
root@bt:/pentest/passwords/cewl# ruby cewl.rb
```

```
 --help cewl 3.0 Robin Wood (dninja@gmail.com)
(www.digininja.org)
Usage: cewl [OPTION] ... URL --help, -h: show help --depth x, -d x: depth to spider to,
default 2 --min_word_length, -m: minimum word length, default 3 --offsite, -o: let the
spider visit other sites --write, -w file: write the output to the file --ua, -u user-
agent: useragent to send --no-words, -n: don't output the wordlist --meta, -a file:
include meta data, optional output file --email, -e file: include email addresses,
optional output file --meta-temp-dir directory: the temporary directory,default /tmp -v:
verbose URL: The site to spider.

root@bt:/pentest/passwords/cewl# ./cewl.rb -d 1 -w pass.txt http://www.targetcompany.
com/about.php
root@bt:/pentest/passwords/cewl# cat passwords.txt |wc -l 430
root@bt:/pentest/passwords/cewl#
```

这是针对某个目标公司网站使用CeWL的案例，从其网站的一个网页中产生了430个可能的密码。

CUPP和CeWL只是用来帮助分析和生成潜在密码的两个工具。运用这些工具做一个有趣的实验，输入自己的信息，看看你的密码是否能够被生成。这样会使你清醒地认识到密码安全的重要性。

7.3 小结

工具是社会工程的一个重要方面，但工具本身不足以成就社会工程人员。仅有工具是没有用的，掌握工具的功能并实际运用才是重点。

本章的核心主题在于熟能生巧。无论是使用电话、基于软件的工具、网络还是其他间谍工具，练习使用才是成功的基石。例如，在社会工程活动中使用电话时，可以篡改来电显示甚至变换说话的声音。然而，如果在使用这些神奇的技术时，你的声音听起来过于生硬、紧张、不安或者准备不足、言之无物的话，那么你所期望的成功就会落空，并且很有可能让一切变得不可信。这项原则在应用伪装技术时同样非常适用。你要伪装的那个人如何谈吐？他会说什么？他会怎么说？他掌握了什么样的知识？他会询问什么样的信息？

不管社会工程人员使用软件工具、硬件工具，还是两者都用，都应该花时间去学习每个工具的详细功能，因为工具的每个特征都会影响审计工作的成败。

工具能节省大量的审计时间，并可弥补审计人员潜在的不足。这一点在第8章的案例分析中体现得尤为明显。

第 8 章

案例研究：剖析社会工程人员

安全之本在于教育。
——马蒂·阿哈罗尼

本书涵盖了如何成为一名杰出社会工程人员的各个方面。若将这些内容运用于实践，社会工程人员会成为难以对付的人。

上学时，学生通过学习历史来了解什么可为、什么不可为。历史是一个很伟大的工具，能告诉我们过去哪些行为成功了以及为何会成功，也能为我们指明前进的方向及方式。

社会工程的历史也不例外，纵观其整个发展史，充满了欺诈和偷窃行为，也有很多人为对抗恶势力鞠躬尽瘁，奉献了一生。

要探讨专业社会工程攻击的方方面面是十分困难的，因为这种行为要么是非法的，要么由于委托合同的限制不能公开讨论。幸运的是，凯文·米特尼克（Kevin Mitnick，世界著名的社会工程人员及计算机安全专家）共享了许多有趣的故事供我们了解。本书从他的著作《欺骗的艺术》中选取了一部分故事。

本章我从米特尼克的书中选取了两个最著名的案例，简单重述了凯文的做法，分析了其中涉及社会工程方面的内容，并且讨论了大家能从中学到什么。

分析完那两个案例之以后，我会分析自己的两个案例，以表明信息获取之简单，以及利用信息入侵整个公司又是何等地轻而易举。最后，我会公开两个不能透露来源的“最高机密”，但你会发现从这些故事中可以学到很多东西。我的目的是告诉你，即使是一丁点信息，若落入技术高超的社会工程人员手中，也会造成极大的破坏性。同时，你也可以看到社会工程人员如何从之前

的成败中吸取经验教训，以提高自己的技能。

下面让我们来看看第一个案例。

8.1　米特尼克案例1：攻击DMV

凯文·米特尼克是世界上最著名的社会工程人员之一。他曾进行过一些举世闻名的、胆大妄为的攻击，下面列出的案例尤其如此。

通过驾照来获取他人的信息是很方便的。通过目标的驾照号，社会工程人员可以获取各种个人信息。然而，天下没有免费的午餐，社会工程或者私家侦探必须耗费一番精力后才能获得这些信息，并利用其对目标进行攻击。

凯文·米特尼克在《欺骗的艺术》一书中讲述了一个叫“反向之刺”的故事。下面几个小节将简要介绍这个故事的背景并展开分析。

8.1.1　目标

在讲述的最精彩的案例之中，米特尼克描述了“艾瑞克”如何利用非公开的机动车辆管理局（DMV）和警察系统获取人们的驾照号。艾瑞克经常需要收集目标对象的驾照信息，而且在这方面很有一套，但是他也担心频繁使用电话社会工程的方法会引起DMV的警觉，甚至会让警察找上门来。

他需要设计出另一种访问DMV网络的方法，而且根据对DMV运作方式的了解，他也知道怎样着手去做。他的目的是双重的，即不仅是DMV，甚至警方也会协助他（当然是在不知情的状况下）获取信息。

8.1.2　故事

艾瑞克知道DMV可以向保险公司、私家侦探和其他特定团体提供机密信息，它们只可以访问对其开放的特定类型的数据。

保险公司和私家侦探可以获取的信息不同，而司法部门可以得到一切信息。艾瑞克的目标是获得所有的信息。

1. 获取非公开的DMV电话号码

艾瑞克所使用的步骤和方法证实了他非比寻常的社会工程技巧。首先，他通过查询台询问DMV总部的电话号码。当然，他得到的是面向公众的号码，而他真正想获得的是更深入的内部信息。

接着，他致电当地县治安官办公室，请求转接呼叫中心，该呼叫中心是协调各司法部门之间信息传递的办公室。在打电话给呼叫中心时，他向工作人员询问司法部门呼叫DMV总部时所使用的专用号码。

在对方不了解来电者身份的情况下，这个举动很可能会以失败告终，但他采取的是下面的做法。

“请问您是？”对方问道。

他必须快速地回答：“我是艾尔。我拨打的电话是503-555-5753。”

他所做的就是随机报一个区号相同、基本号码相同、最后4位数字纯属编造的号码，然后戛然而止。该司法办公室的工作人员可能做出了以下假设：

- 来电者是内部人员，并且知道这个非公开的中心号码；
- 来电者似乎知道DMV所有的号码。

由于工作人员坚信上述两种假设，艾瑞克顺利得到了想要的号码。但是，艾瑞克想要的并非只是一个号码，他想要掌控握尽可能多的信息。

要想实现这一目标需要进行更深入的攻击——通过多种不同方法，多层次、多角度的攻击，而这种攻击是很惊人的。

2. 入侵州电话系统

艾瑞克使用获取的号码致电DMV，并告诉接线员他是北电网络有限公司（Nortel）[①]的工作人员，因为工作涉及DMS-100（一种广泛使用的交换机），所以需要同DMV的技术人员交流。

当与技术人员通话时，艾瑞克又自称是得克萨斯州北电技术服务中心的工作人员，并且解释说他正在更新所有的交换机，更新过程会通过远程进行，只需要对方提供交换机的拨入号码，他就可以从技术服务中心直接进行更新。

这个故事似乎完全可信，所以技术人员照办了，给了艾瑞克所有需要的信息。利用这些信息，他现在能够直接拨入一个州电话交换系统。

3. 获取密码

下一个障碍是整个攻击行动中的关键一环——获取密码。DMV所使用的北电交换机有密码保护。根据以往的经验，艾瑞克知道北电交换机有一个默认的用户账户——NTAS。随后他几次拨入系统，尝试遇到过的标准密码：

- NTAS——失败

① 加拿大著名的电信设备供应商，可参见百度百科的文章http://baike.baidu.com/view/238246.htm。——译者注

- Account name——失败
- helper——失败
- patch——失败
- update——成功

哇噢，真的吗？密码是update。现在他获得了整个交换机和连接线路的控制权限。通过查询电话线路的走向，他很快找到通向同一个部门的19条电话线路。

在检查交换机的内部设置后，他发现交换机的工作机制是先搜索19条线路，直到发现其中一个状态为不忙时，就建立连接。他挑选了18号线路，输入标准转发代码，为这条线路增加了呼叫转移控制。

艾瑞克买了一个预付费的便宜手机，以便于随意丢弃。他将这个号码设置为18号线的自动转接号。这样，只要DMV有17条线路都处于忙碌状态，第18次呼叫就不会进入DMV，而是直接呼叫艾瑞克的移动电话。

启动后不久，大约在第二天上午8点，手机就响了。每次，电话那头都有一位警官来询问某人的信息。艾瑞克可能在家里、餐馆、车里等地方接到警察拨来的电话，不管是在哪里，他都假装成DMV的接线员。

让我啼笑皆非的是下面这个电话。

手机响起，艾瑞克说道："DMV，请问有什么可以帮你的？"

"我是安德鲁·科尔侦探。"

"你好，侦探先生，请问今天有什么可以帮你的吗？"

"我需要查探一下驾照号为005602789的人。"

"好的，让我调一下他的记录。"在假装操作电脑的同时，艾瑞克会开始询问："科尔侦探，您的警局在？"

"杰斐逊县。"

艾瑞克还会接着问如下问题："您的请求代码是？""您的驾照号码是？""您的生日是？"

来电者会将个人信息全盘奉上，艾瑞克只是假装核对，然后假装确认来电者查询的信息。他会假装查阅名字和其他信息，接着说："对不起，我的电脑刚才又死机了。侦探先生，我的电脑这周总是不停地出问题。您能重新打进来找另一位工作人员帮忙吗？"

对侦探来说，这肯定很叫人恼火，但从道理上也说得过去。在这个过程中，艾瑞克已经掌握了那位侦探的身份。这些信息可以用在很多地方，但最重要的是可以随时从DMV获取信息。

在从DMV收集几小时的信息后，艾瑞克再次拨入DMV的交换机，取消转接功能。现在他已经拥有足够多的信息了。

在攻击之后的几个月里，艾瑞克还是能轻易地拨入，打开交换机的呼叫转移功能，继续收集警官的用户信息，然后取消呼叫转移，用警察的身份去获取有效驾照的个人信息，然后出卖给私家侦探或者其他不会在意这些信息来源的人。

8.1.3 社会工程框架的运用

这个故事里，凯文总结了一些促使艾瑞克成功的做法和表现，例如在和警察谈话时要保持淡定以及迂回地处理不熟悉的问题。

你也可以找出艾瑞克所用的社会工程框架及使用方法。

举个例子，任何成功的社会工程审计或攻击的第一步都是信息收集。从这个例子中你可以发现，艾瑞克一定是事先做足了功课才开始攻击的。他对电话系统、DMV的运行方式以及有待渗入的流程颇为熟悉。我不清楚这个攻击发生在多久以前，但是现在有了网络，这种攻击就更加简便了。网络是信息收集的金矿。几年前有人想出了一种攻击Tranax ATM取款机的方法，几个星期之后在互联网上就可以找到实现这种攻击的详细手册了。

同样，如本书之前提到的，选择与你的工作或曾经的身份相似的身份来伪装，能增加成功的几率，因为伪装得越“逼真”，就越有利于收集信息并攻破目标。显然艾瑞克谙熟此道。

也许你还记得，框架的下一步就是诱导，即能通过精心构思的问题来套取信息或获得访问权限。艾瑞克套取信息的能力超群。在与警察通话的过程中，他通过诱导策略证实了自己就是所伪装的角色并且非常了解自己的“工作”。他知道行话以及必要的例行问题。事实上，不问那些问题反而会比问更可能引起警觉。这就是优秀的诱导策略的威力所在。

艾瑞克早就知道他需要套取特定的电话号码去发起攻击。他没有解释自己为什么需要这一信息，而是使用了第3章中提到的假设性问题，简单地说：“我得知道答案，告诉我就好了。”这是强力诱导的另一个例子，你可以细致地分析他使用的方法，并从中学到很多。

大部分优秀的攻击同时也包括大量的伪装，这个例子也不例外。艾瑞克在这次攻击中设计了一些伪装，他必须多次转换身份才能达到目的。他伪装的执法部门的工作人员给人留下了深刻的印象（他做得非常好），但请牢记，这种行为在美国是严重的违法行为。你能从艾瑞克的社会工程过程和使用的方法中学到很多知识，但是在应用时必须小心谨慎。即使在付费的社会工程审计活动中，假冒执法部门的工作人员也是违法的。

要了解当地的法律，这是经验教训，否则就不要害怕被逮捕。尽管实际上是非法的，你仍可以通过分析艾瑞克在攻击中的表现学到很多。他总是很镇定。当伪装成DMV工作人员时，他能

够使用诱导技术来证明自己的身份。伪装成警察时，他的行为、声音和措词都支撑着他的伪装。对很多人来说，转换身份是极具难度的，所以在进行“直播”表演前最好多加练习。

艾瑞克的伪装技术十分精湛，特别体现在伪装成DMV的工作人员和回应警察打来电话的时侯。很多情况下，他可能会露出马脚，但最终似乎掌控得很好。

社会工程中常运用到许多心理学方面的技能，比如眼神和微表情，本例中没有用到，因为这次攻击主要是通过电话完成的。但是艾瑞克确实应用了框架中的一些技术，例如关系构建、神经语言程序学以及思维模式。

艾瑞克似乎是个建立关系的天才。他风度翩翩、平易近人，处理意外情况时泰然自若，能自信地伪装各种角色。他的声音和谈吐让电话那头的人完全有理由信任他。

艾瑞克所使用的提问和交谈策略令人印象深刻，他甚至将这些技巧应用在了谙熟此道的执法人员身上。他成功地运用这些策略并在对方不知不觉中获取了他想要的所有信息。

艾瑞克还很好地掌握并运用了影响策略，在攻击中最明显的表现之一就是他要求警察致电另一位DMV工作人员。这很可能惹恼对方，但是这个策略的成功之处在于艾瑞克之前已经“给”了对方一些信息，也就是他“核实”了对方需要的信息，只不过就在他要为对方提供最后一部分信息的紧要关头，“计算机”挂了。

通过运用一些影响力的规则，艾瑞克轻松地让对方听从了他的意见。

与艾瑞克的伪装密不可分的是他成功运用了框架。回忆一下，框架是令自己和自己的故事可信，从而使目标的思维与你的思维一致。这是伪装的关键之一，能使你的伪装更加完美，并使目标对你的话深信不疑。艾瑞克的伪装技巧精湛可信，但是真正让目标信任他的是他使用的框架。他的框架取决于谈话的对象。有时候他必须让电话那头的办公人员为其提供呼叫中心的号码，有时候他需要成为业务技能娴熟的DMV工作人员。

艾瑞克利用框架使自己高度可信，他假定自己会获得所询问的信息，在应对过程中没有慌乱，并且自信地提出每一个问题，让对方“感觉”作出回答是他的义务。所有这些表现使对方落入他的设计，相信他的伪装，并自然地作出了回应。

正如你所看到的，通过分析艾瑞克的社会工程攻击你能学到很多东西。你能够猜想出，艾瑞克要么练习过所有这些攻击方法，要么进行过多次模拟和演练，以便熟悉如何处理攻击中使用的那些内部系统。

虽然艾瑞克的方法奏效了，但我还想补充一些预防措施。举例如下。

- 处理DMV电话时，我会先确保自己是在“办公室”里再进行呼叫转移。我会设置一个有些背景噪音的办公环境，并准备好记录所有信息所需的设备，以避免我在记录时被服务生或朋友打断而露陷。

- 尽管对反追踪来说，使用一次性手机是个好主意，但还有一种技术可以应用，即利用谷歌语音服务（Google Voice）或Skype号码转拨。我不信任手机信号，因为掉线、信号微弱且不稳定可能瞬间就会导致攻击失败。

除了这两项，他的攻击中基本没什么需要改进的了。艾瑞克充分运用了社会工程框架中的各项技巧，确保了攻击的成功。

8.2 米特尼克案例 2：攻击美国社会保障局

米特尼克的书中曾提到一个名叫基思·卡特的人（Keith Carter），他是一位不那么可敬的私家侦探，受雇调查一位男士，该男士即将离婚，但对妻子隐瞒了存款情况。那位妻子曾资助丈夫创业，如今当初的小生意已发展成为一家价值数百万美元的公司。

离婚是在所难免的，但女方的律师需要找到男方“隐瞒的财产”。这个攻击十分有趣，因为和第一个案例一样，这个案例中也将使用一些不法方式收集信息。

8.2.1 目标

目标是为了查明丈夫乔·约翰逊的资产情况，但那不是社会工程攻击的目标。为了获取乔的信息，私家侦探基思必须对美国社会保障局（SSA）进行攻击。

在社会工程审计活动中，经常会攻击社会保障局。本节介绍了基思为实现目标所使用的方法，但可以说攻击社会保障局不啻于跳崖。随着故事的展开，你会发现这个特殊的攻击有多么地危险。

8.2.2 故事

乔·约翰逊与一个非常有钱的女人结婚后，从她那里得到了好几万美元的投资去实现自己的创业梦想，后来他创立了一家价值数百万美元的公司。

渐渐地，他们的婚姻出现了裂痕，最终双方决定离婚。在办理离婚手续期间，约翰逊夫人“得知”丈夫隐瞒了其真实的财产情况，想要逃过财产分配。

她雇用了基思，一个不那么光明磊落的私家侦探，一个为了达到目的不在乎手段是否违法的人。

在着手分析案情时，基思认定社会保障局就是他的绝佳突破口。他认为，如果能得到乔的财产记录，从中发现不一致的地方，就能给他致命的一击。他想伪装成乔，这样就能够随意地打电话给乔的银行、投资公司以及境外账户查询信息。为此，他还需要一些详细的信息，这促使他决定攻击社会保障局。

基思开始基本的信息收集。他上网找到一本指南，其中描述了SSA的内部系统、内部专业术语以及行话。在了解了系统并将行话背得滚瓜烂熟之后，他给当地社保办公室的公众热线打了一个电话。电话连线后，他要求接通理赔办公室，对话如下。

“你好，我是格雷戈里·亚当斯，329区办公室的。我想找一位理赔调解员，他正在处理一个以6363结尾的账号，具体账号我已经传真过去了。”

“噢，他在3部，号码是……”

真的吗？那么简单？哇噢。几分钟的时间他就获得了一般公众难以获得的内部办公电话。接下来进入较难的部分。

他必须致电3部，改变他的伪装，套取有关乔的有价值的信息。周四早晨，基思的计划似乎已经做好了，他拿起电话拨通了3部的号码。

“这里是3部，我是王梅林（May Linn Wang）。”

“王小姐，我是亚瑟·埃洛丹，从监察长办公室打来的。我可以称您为‘梅’（May）吗？”

“请叫我‘梅林’。”她回答道。

“好的，是这样的，梅林。我们有个新人现在还没有电脑，现在他有些要紧的事，所以用了我的。我要抗议，我们可是美国政府部门，他们竟然说没有足够的预算为新人配置电脑。现在我的上司认为我怠慢工作，不想听我的任何借口，你懂吗？”

“我明白你的意思。”

“你能帮我快速地在MCS上查一些信息吗？”他问道。MCS是查询纳税者信息的计算机系统名称。

“当然，你需要查什么？”

“首先，请帮我按照字母顺序查找约瑟夫·约翰逊（Joseph Johnson），生日是1969年7月4日。”（字母序查找是通过纳税人的姓名进行计算机搜索的一种方式，之后再以出生日期进一步定位。）

“你想知道什么？”

“他的账户号码是多少？”基思问道（即乔的社会保障号）。

她直接就读了出来。

“我还需要你对那个账号做数字查找。”（数字查找类似于字母序查找，只不过是通过数字而不是字母查找。）这需要她报出纳税人的基本数据，梅林回复了纳税人的出生地、母亲结婚前的姓氏和父亲的名字。基思耐心地听着，梅林还给出了乔社会保障号发放的日期和发放单位。

基思接下来请求查询乔的具体收入。

“请问要哪一年的？”

“2001年。”

梅林说：“数额为190 286美元，付款人是约翰逊微技术公司。”

“还有其他收入吗？”

“没有了。”

“谢谢，”基思说，“你人真好。”

基思打算以后每次需要获取信息却“没有电脑可用”时都打电话给她，这是社会工程人员钟爱的一套把戏，因为建立了联系之后他们下次还能和同一个人通话，免去了每次找寻新目标的麻烦。

“下个星期不行。”她告诉他，因为她要去肯塔基州参加姐姐的婚礼。其他时间，她会尽力而为。

此时任务貌似已经完成了。基思获取了他想要的所有基本信息，接下来的任务就简单了，只需再给银行和境外账户打一通电话，获取相关的信息即可。

这真是一场顺利实施并令人惊叹的攻击。

8.2.3 社会工程框架的运用

SSA攻击可能会让你瞠目结舌。从这个应用了社会工程框架的特殊攻击中，你能获益颇丰。

基思首先进行了信息收集。可能你已经听烦了，但是获取信息是所有优秀社会工程人员攻击的核心所在，掌握的信息越多就越有利。

基思首先在网上找到了令人震惊的内部资料，而且现在竟然还能在https://secure.ssa.gov/apps10/poms.nsf/上找到。

这个链接直接指向社会保障局操作程序的在线手册。手册中包含了缩写词、行话、操作指南以及SSA工作人员可以向执法部门提供的信息。掌握了这些信息，基思知道该说什么、问什么、怎样让自己看起来像是那么回事儿，以及什么样的信息是不能问的。

尽管链接提供了大量的信息，但他决定伪装成监察长办公室的工作人员，致电SSA以深入搜集信息。他从外部突围，通过本地公众热线获取了内部号码，随后又伪装成内部工作人员。

基思在此过程中完美地转换了好几次伪装。通过SSA在线手册的帮助，他获得了很多信息从而顺利提问。这本手册简直就是诱导者的梦想之书。通过运用恰当的词句，他听上去真像那么回

事。他还通过构建共识和框架使伪装惟妙惟肖。构建共识并非易事，但是基思在这方面做得很好，证明他之前做了充分的练习。他运用了很多影响策略以使目标对象感觉合情合理，从而放松了警惕。例如，他把义务和将心比心巧妙地结合了起来。当讲述自己没有好工具且无法获得管理层的支持时，他让梅林觉得有义务去帮助他。

他也使用了关键词和短语来博取同情，同时又表明自己是政府部门的工作人员，比如“我的上司对我很不满意”，这句话暗示他处于麻烦之中，而SSA的工作人员梅林可以帮助他。人们在道德层面有一种帮助有需要的人的责任感。很少有人会对求助者置之不理，梅林也是如此，她不仅感到有义务施以援手，甚至还告诉了基思她的个人行程。

最终，基思运用了社会工程框架中一系列不需当面使用的重要技巧。

政府系统是由人管理运行的，这令它们难以抵抗本例中所使用的攻击方法。这里并非建议使用自动化或计算机系统代替人的操作，而是仅仅指出一个事实，即很多系统过于依赖超负荷工作、低薪、处于高压状态的人员来操作，结果造成操纵这些人并非难事。

老实说，要对这次特殊的攻击进行改进很难，因为我一般不会进行这样的攻击，而且基思在应用社会工程框架的过程中已经做得相当杰出了。

许多人都习惯于被虐待和辱骂，些许善意就能令他们不遗余力地伸出援手。正如米特尼克在《欺骗的艺术》一书中声称的，这次特殊的攻击表明依赖于人进行操作的系统很容易被攻击。

8.3　海德纳吉案例1：自负的CEO

我与一位自负的CEO的交锋经历还是比较有趣的，因为那位CEO认为自己绝对不可能被任何社会工程渗透，理由有两个：第一，生活中他不常使用科技类产品；第二，他天资聪颖，完全能够抵抗他所谓的“愚蠢的游戏”。

在内部安全小组了解上述信息之后，他们决定让我将该CEO作为安全审计的目标。他们知道，如果他不能通过审计，那么此后的安全整改工作审批会更容易些，这有益于保障公司的整体安全。

8.3.1　目标

目标是美国一家规模较大的印刷公司，该公司拥有一些工艺专利和供应商，而且一些竞争者在打它们的主意。IT部和安全部门认为公司存在一些薄弱点，并说服CEO有必要进行一次安全审计。在与我搭档的一次通话中，该CEO傲慢地说，他知道攻击他简直是无稽之谈，因为他将会用生命保守这些秘密。即使是他的某些核心雇员也不知道所有的细节。

作为社会工程审计师，我的工作是渗透公司、获取公司某一台服务器的访问权限，并拿到其

中存储的专利信息。就像CEO在电话里提到的，困难之处在于服务器的密码都存储在他的电脑里，没有他的允许，即使是安全部门的职员也无法接触他的电脑。

8.3.2 故事

很明显，不管采用什么方式，都必须通过CEO这一关。这的确是一个挑战，因为CEO已经全副武装，就等着被渗透了。我依照惯例由信息收集开始，通过网络资源和其他工具（比如Maltego）调查该公司。通过这种方式我获得了很多信息，比如服务器位置、IP地址、邮箱地址、电话号码、公司地址、邮件服务器、员工的名字和头衔等。

当然，我把这些信息制成文档以备之后使用。邮箱地址的结构十分重要，在调查他们的网站时，我发现其邮箱地址的结构是“名字.姓氏@公司名.com”。我没能找到CEO的邮箱地址，但网站上的许多文章都提到了他的名字和头衔（姑且称他为Charles Jones，即查尔斯·琼斯）。这些是普通的、不了解详情的社会工程人员都可以获取的信息。

利用“名字.姓氏@公司名.com”的格式，我尝试发了一封邮件给他，但是没能成功。这令我非常失望，因为我确定通过邮件方式能得到许多具体的信息。

我决定尝试一下Charles的昵称Chuck（恰克），于是试了试“chuck.jones@公司名.com”，竟然成功了！我获得了经过验证的邮件地址。现在我要验证一下这个邮箱是属于CEO的，而不是与他同名的某个家伙。

我花了更多的时间通过谷歌和Maltego尽可能地搜集更多的信息。Maltego有一个强大的转换器插件功能，可以像搜索引擎一样搜索域名范围内的任何文件。

我对公司域名范围内的文件进行转换，大量的文件映入我的眼帘。Maltego通过转换插件不断地提供文件名，许多文件包含元数据，其中包括了日期、创建者和其他的细节信息。通过运行Maltego的元数据转换功能，我发现其中很多文件都是由“Chuck Jones”创建的，文件中的许多内容都暗示他就是CEO。

这正是我想证实的，但在浏览的过程中，一个特殊的文件引起了我的注意——InvoiceApril.xls。这是当地一家银行开具的关于某个营销项目的发票，他参与了该项目，其中有银行的名称、日期以及资金数额，但是缺少具体的项目名称信息。

于是我快速查询了银行网站，但是6个月之前的项目已经无法显示了。我该怎么做呢？

我决定给银行市场部的人打一个电话。

“你好，我是某某公司的汤姆。我在整理账本，发现其中夹了一张4月份的面额为3500美元的赞助发票。项目名称没有写，你能告诉我这是什么活动的发票吗？”

“当然可以，汤姆，”伴随着键盘的敲击声她说，“我查到这是银行儿童癌症基金会发起的年度活动，贵公司是银牌赞助商。”

“非常感谢。我是新来的，非常感谢您的帮助。再见。”

我想到了一种可用的攻击方式，但还需要更多的调查研究，然后周密地计划一次电话通话。

我在网站上找到一些关于筹款活动的文章，以及许多公司为癌症治疗研究出资赞助的报道。另外，我对CEO做了更深入的调查并收获良多，我发现了他父母的名字、他姊妹的名字、他放在Facebook上的孩子的照片、他住在父母附近时去过的教堂、他对喜爱的餐厅的评价、他喜欢的球队、他大儿子喜欢的球队、他读的大学及他孩子上的学校等。

我想知道为什么公司要捐款给儿童癌症基金会。尽管利用他人的感情是许多恶意社会工程人员的所为，但我意识到可能自己也不得不这么做，因为我想知道是否是因为他某个儿子是癌症患者他才加入基金会的。我打了个电话给公司市场部的经理。

“你好，我是XYZ的汤姆。受本镇第一国家银行的委托，负责联系4月份儿童癌症基金会的出席者，能耽误您一点时间做个反馈调查吗？”

“当然可以。”市场经理苏说道。

“苏，我看到你们是4月份活动的银牌赞助商。你觉得就宣传结果而言这笔赞助费花得值得吗？”

“嗯，这是我们每年都会做的，在当地会有不少报道。如果网站上能多展示些银牌赞助商的信息就更好了。”

“好的，我记下来了。每年？是的，我看到你们每年都会这么做。个人想了解一下，有那么多基金会，为什么选择了我们？”

“据我所知，恰克总是特别关注这个。他是CEO，我想大概是他家里有人得了癌症吧。”

“噢，我很抱歉。请问是他的孩子吗？”

“不是的，我想可能是他的侄子或表妹吧。我也不是很肯定。”

“好的，十分感谢你们的捐款和支持。”

我又提了一些问题，再次表示感谢，然后结束了通话。

我得到了想要的信息——不是他的孩子患有癌症。我知道这不会阻止一个恶意的社会工程人员进行攻击，但我还是很好奇。在得到这些信息之后，我开始计划入侵攻击。

我知道CEO来自纽约，喜欢一家名叫多明戈的餐厅，并且经常带着孩子看大都会的比赛，然后去多明戈餐厅吃饭。

他给餐厅写了评价，并且列举了最喜欢的三道菜。我从他的Facebook中了解到，目前他还是和父母住得很近，而且经常过去探望。

我计划伪装成癌症研究资金的募集人员，宣称在为三州地区筹款，捐款的人将有机会抽奖，奖品是两张大都会比赛的门票和一张餐厅的优惠券，可从三家餐厅中任选一家，多明戈餐厅就是其中之一。

我会假装自己来自纽约地区，但是工作时间不长，以防他提到一些我不知道的事情。

我的最终目标是让他接收一个包含恶意代码的PDF文件，该代码能够让我反向入侵他的计算机。但如果他没有使用能让我成功入侵的Adobe软件版本，我会接着说服他下载一个zip文件，并执行其中带有恶意文件的EXE安装程序。

为了成功伪装，我针对通话内容进行了一番练习，测试了PDF和EXE文件，并且打开谷歌地图找到了多明戈餐厅的位置以备通话中可能谈到。准备好用来接收受害者反馈信息的电脑后，一切工作准备就绪。

大约下午4点，我拨通了电话，因为通过公司网站我发现该公司周五下午4:30下班。由于以前与他洽谈审计事宜的不是我，而是我的搭档，所以CEO听不出我的声音。

“你好，请问查尔斯·琼斯先生在吗？”

“请稍等。”电话那头的声音有些疲惫，并且该人马上为我转接。

“你好，我是恰克。”

“你好，琼斯先生，我是美国癌症研究会的托尼。我们正在进行一项年度资金募集活动，筹得的资金将用于支持癌症研究，目前不管男女老幼都在饱受癌症的折磨。”

“请叫我恰克。”他打断了我。

这是一个好兆头，因为他并没有以现在很忙等借口挂断我的电话，并且在对话中融入了个人色彩。我继续说道：“恰克，谢谢你。我们正在进行一项募款活动，联系的是原先捐过款的单位，这次是50~150美元的小额捐款。为此，我们为捐款的好心人设置了包含两项大奖的抽奖机会，抽中的话会赢得两张纽约大都会比赛的门票以及一顿免费的双人晚餐，有三家餐厅可供选择。本次抽奖一共会产生5位幸运者。”

“大都会比赛，真的？”

“是的。也许你对大都会的比赛不感兴趣，但餐厅还是非常棒的。”

“不，不，我喜欢大都会，我会那么问是因为我太高兴了。”

“好的，请考虑一下。你不仅能帮助癌症研究，还有机会观看精彩的比赛，而且还能在莫顿、巴塞尔和多明戈三家餐厅中选择一家免费就餐。”

“多明戈！真的？我喜欢这家餐厅。”

“哈，那太好了。你知道我前几天第一次去那，那儿的蘑菇鸡肉真是棒极了！”这是他第三大爱的菜。

“哦，那不算什么，你应该尝尝法式菠萝，那是那家餐厅最棒的菜，我每次去都点它。”

“我周末会再去那，一定要试试。谢谢你的推荐。现在时间也不早了，我不是来要钱的，也不能从电话里拿走钱。我会发一个PDF文件给你，你可以看看，如果感兴趣的话，填一下表格，然后随支票一起发过来就可以了。”

“好啊，发过来吧。”

“好的，还有几个问题，你的邮箱地址是？”

“chuck.jones@公司名.com。”

“如果可以的话，请打开PDF阅读器，单击‘帮助’菜单上的‘关于’，然后告诉我版本号。”

“稍等，版本是8.04。”

“很好，我可不想发一份你打不开的文件。稍等不要挂，我现在就发过去。好了，发过去了。”

“好的，谢谢。真希望我是幸运儿，我太喜欢那家餐厅了。”

“我知道，那儿的菜的确不错。在挂电话之前，你能检查一下邮箱，看看邮件是否收到了吗？”

“好的，我5分钟后就要注销了，不过还能查看。是的，收到了。”当听到双击的声音，我开始检查运行于我的BackTrack电脑上的恶意负载侦听程序Meterpreter（见第7章），它正在响应。我屏住呼吸（这部分从来不会无聊），砰地一声命令行界面出现了。Meterpreter脚本的属主信息改变了，类似于Explorer.exe。

恰克嚷道：“啊，我黑屏了，不能动了。”

“真的吗？真是奇怪了。让我检查一下。”我真正查看的是我是否能访问他的硬盘，并且立刻上传反向命令行，这在他关机重启后还能运行。我说：“很抱歉，我不知道怎么会这样。你能再等我几分钟吗？”

“好的，我去洗洗咖啡杯，离开会儿，不挂电话。”

“好的，谢谢。”这段时间足够我确保下次还能进入他的计算机系统了。很快，他回来了。

“我回来了。”

“恰克，这真让人尴尬，但我不清楚发生了什么。我不想耽误你的时间，要不你先回去，我重新做一个PDF文件再发邮件给你。我们周一再联系。”

“好，没问题。周末愉快!”

“你也是，恰克。”

挂断电话后，令我吃惊又惊喜的是，他的电脑没有关机，并且处于活动状态。是的，他将一切保存在了安全的硬盘中，而且只有他有权访问，不过全都保存在了Word中。我立即开始下载那些Word文档，几个小时后我访问了服务器，打印出他想保护的所有内部工作流程。

我在周一早上联络了他，但不是以基金募集者托尼的身份，而是以安全咨询专家的身份，而且携带了包含他的“秘密”和密码的打印文件，还有与他及其员工的通话录音。

成功攻击后，与客户第一次会面时，他们往往大为震惊，并且会宣称我们使用了不道德的策略，利用人性弱点实现入侵。当我们解释说恶意分子会使用同样的战术时，他们由愤怒变为恐惧，最后会表示理解。

8.3.3 社会工程框架的运用

与之前的案例类似，我们将本案例与社会工程学框架结合，分析该攻击的精彩之处，以及哪些部分还有待改进。

像往常一样，信息搜集是社会工程的关键，在这个案例中也是一样。信息搜集有很多渠道——网站、Maltego及电话等，这些是成功攻击的基础。信息不足将会导致悲惨的失败。

恰当而丰富的信息关系重大，甚至是我不需要的信息，类似他去的教堂、他父母和兄弟姊妹的名字，都在信息收集的范围之中。这些都是以防万一，有备无患，但是邮件地址的惯用格式以及用Maltego找到的服务器上的文件却是非常宝贵的关键信息，正是这些信息为我打开了入侵该公司的大门。

就像第2章提到的，将搜集到的信息分门别类地保存到BasKet或Dradis中，方便随时使用信息也很重要。相反，包含一大堆信息的文本文件会很难利用。信息整理与信息搜集是同等重要的。

像坏人一样思考（尝试挖掘并利用目标的弱点和欲望）并非工作的关键，但是如果专业的审计人员想要保护他的客户，他将会竭尽全力地去证实其客户有多么脆弱。搜集的信息越多，就越容易发现漏洞。这就是通向成功的道路。

增强伪装的真实性和设计话题有助于攻击的成功。你必须提出有力的问题并抓住关键点来吸引目标的注意。通过搜集大量的信息，我能提出有效的问题并制定一个涉及关键词和神经语言程

序学用语的框架，这会大大提高战术影响力的威力，确保攻击的成功。

我不得不经常更换伪装，以员工的身份打电话给公司的供应商，再以供应商的身份打电话给内部员工以获得更多的信息。我必须仔细地准备每个身份，进入角色，这样才能在实战中应对自如。这当然需要很多时间的谋划，以确保每个伪装都合理、自然。

熟能生巧。在发起攻击前我和搭档反复练习。我必须确保PDF文件正常工作，攻击方法合理，还必须具备足够的知识，让所有目标都相信我。

人们常常不理解练习的重要性。练习能使我们弄明白什么策略可行、什么策略不可行，并且确保计划顺利开展和实施，甚至在出现意外的情况下也能从容应对。

之后，我发现做一些小小的改进会让这次攻击变得更有效率。首先，仅仅依靠恶意PDF文件是存在风险的，我会建立一个小网站，模拟真实的癌症研究网站，并把PDF文件上传上去。网站和PDF文件都可以包含恶意代码。这样，成功的几率就增加了一倍，其中一个失败了还能有个后备。

另一个更大的风险是CEO离开办公室后还开着电脑。如果他不这么做，我就必须等到下周一才能继续尝试访问。我应该先发给他一份包含恶意代码的PDF文件，待该文件攻击他的电脑后，再发一份“真实的PDF文件”让他阅读。这样他就会在电脑前停留足够长的时间，也好让我有时间利用漏洞进行攻击。

在这次审计中，我花费了大约一个星期的时间去调查、搜集、整理信息以及练习，最后才发起攻击。一个星期的时间，该公司的机密就可能落入了竞争对手或者更高的出价者手中。多读几遍这个故事，体会其中使用的微妙的方法以及对话方式。书面形式很难体现声音、音调和对话节奏，你要试着想象，如果自己处于这些对话场景，将用什么方式处理。

8.4　海德纳吉案例 2：主题乐园丑闻

对我来说，主题乐园丑闻是个很有趣的案例，因为它涉及一些现场测试。在这个案例中我运用了本书中提到的许多社会工程技巧，这是一场对理论的实战检验。

第二个原因是其本身的商业性质和骗局成功的可能性。如果成功了，社会工程人员可以获取上千个信用卡账号。

8.4.1　目标

本次攻击的目标是检测某主题乐园票务系统的安全性。在登记顾客购票信息时，每个计算机终端都会与后台服务器端的客户信息和金额记录建立连接。主题乐园想看看攻击者能否运用恶意的方式使工作人员采取某种行动从而造成危害。

我的目的不是找工作人员的麻烦，而是为了证明工作人员进行票务登记的计算机被入侵时会带来什么安全危害。此外，我不会采用黑客技术入侵计算机，而是要应用社会工程学方法。

如果这样的入侵发生了，后果会怎么样呢？会泄露什么样的数据？哪些服务器会遭受入侵？但他们并不想考虑得如此深入，只想看看第一阶段，即社会工程入侵是否真能实现。

为了弄清社会工程入侵是否可能，我必须先弄清乐园的售票操作流程，以及工作人员在终端上将会做什么、不会做什么，更重要的是，他们有权做什么、无权做什么。

8.4.2 故事

就像前面提到的，这项工作的目的并不复杂，即我只需弄清楚售票窗口的工作人员是否会允许“顾客”让他做一件明显不被允许的事。在开始具体筹划之前，我必须先了解他们的业务内容。

我浏览了乐园的网站，利用Maltego和谷歌调查了有关该乐园的报道和其他信息。我还做了现场调查，亲自去了乐园，体验在售票窗口买票的过程。在这个过程中，我与工作人员进行了简单的交谈，并且留意他们的布局、电脑结点以及“办公室”的其他方面。

这个“办公室”令我有了眉目。在对话中，我提到自己来自一个非常有名的小城镇。她问我是什么地方，我告诉了她，然后她作出了常规的反应：“那地方在哪？”

“你这能上网吗？”

“能啊。”

“哦，你会喜欢上那里的，打开一下谷歌地图，输入邮编11111，然后转换成卫星视图模式。看那个小镇是多么地小呀！”

“我的上帝啊，真是太小了！我以前从来没听过这个地方。”

在这么短的时间里，我掌握了如下信息：

- 售票员工作场所的布局
- 工作人员是怎样售票的
- 计算机是连外网的

我再次登录乐园的网站，开始寻找新的突破口。我需要找到入侵他们计算机系统的方法。我的伪装（一名带着家人去乐园游玩的父亲）很合理。

我设计的故事情节是这样的：一开始家人和我并没有计划去乐园游玩，但是在酒店上网时看到了乐园的优惠信息，于是去大厅打算购买门票，但是那的价格要比网上贵很多。

当我们再次确认价格时，发现优惠价仅适用于在线支付，于是我们在线付了钱，之后才突然

意识到，门票需要打印出来才能被检票器扫描。我试着在酒店打印，可惜他们的打印机坏了。我已经付了钱，害怕钱就这么浪费了，于是把它们转换成了PDF格式并且发送到自己的邮箱里。这个故事听上去很合理，不是吗？我需要做的就是开始着手我的小阴谋。我先打了一个电话。

“你好，是XYZ主题乐园总办事处吗？”

“是的，有什么需要帮忙的吗？”

我需要同内部人员取得联系，向他们提问并且得到我想要的答案。连线采购部门后，我找到了正确的目标。我说：“你好，我是SecuriSoft公司的保罗。我们正在为新的软件产品做免费测试，它能阅读甚至打印PDF文件。我发给你一个免费下载的地址，请试用一下好吗？”

“可以，但是我不确定我们对此会不会感兴趣，但你可以发一些资料给我。”

“太好了，我能问一下你现在使用的Adobe阅读器是什么版本的吗？”

“我想还是第8版的。”

“好的，今天我就发一些合适的资料给你。”

知道版本信息后，我要做的就是创建一个嵌入反向会话的恶意PDF文件（一旦打开，我就能访问他们的计算机），把它取名为Receipt.pdf，然后发送给自己。

第二天，我带着家人开始了一项社会工程行动。家人站在一边等着，我走上前热情地与售票员攀谈了起来。

“嗨！你好吗……缇娜？”我看着她的胸牌说道。

“你好，需要我帮什么忙吗？”她微笑着询问我。

“是这样的，我和家人决定本周末进行一次短途旅行，现在我们住在这附近的希尔顿酒店。”我指着不远处的家人回答道，“我女儿看到了你们主题乐园的广告，于是求着我们带她来。我们答应她了，然后在网站上看到了优惠的门票……”

“噢，是的，我们只在网上提供优惠，现在十分受欢迎。我能看一下你们的门票吗？”

“呃，这就是我想请你帮忙的地方，我不想得到‘年度最烂老爸奖’。”我女儿正在紧张地笑呢。我解释道：“缇娜，我和妻子看到网上的价格便宜15%，就在酒店的电脑上购买了门票，但是付完钱后，酒店的打印机坏了，无法将票打印出来，于是我把它保存为PDF文件，并发送到了我的邮箱。”

“我知道这是个奇怪的要求，不过你可以登录我的邮箱，然后帮我打印一下吗？”这个邮箱地址很普通，包含一些名为“孩子的照片”、“爸妈结婚纪念日”之类的邮件。

可以看出她在做激烈的思想斗争，我不敢肯定她的沉默是否对我有利，或者我可以再推动一下。我说："我知道这个要求比较怪，但是我的宝贝女儿真的很想去，而且我不想对她说'不'。"我再次指向女儿，她的表情很配合，流露出可爱而又焦虑的神请。

"好的，我要怎么做呢？"

"先登录gmail.com，然后登录我的邮箱Paul1234@gmail.com，密码是B-E-S-M-A-R-T。"（我知道这个密码很糟糕[①]，但是紧要关头的一点警告也无伤大雅。）

几分钟过后，缇娜双击了PDF文件，然后电脑黑屏了。"你在开玩笑吗？或者我哪里操作错了吗？哇，现在我肯定要得'年度最烂老爸奖'了。"

"你知道怎么回事吗，先生？我感到十分抱歉，要不然你购买成人票，我让孩子免费进去。"

"哦，你真是太慷慨了。"我微笑着给了她50美元，谢谢她的所有帮助，然后让她退出了我的邮箱。就当我女儿因进入乐园而感到喜悦的同时，主题乐园的系统也被入侵了。

几分钟过后，搭档发短信告诉我，他已经"进入"并且"收集"了报告所需的数据。几个小时的娱乐过后，我们离开了乐园，回去完成了周一会议所使用的报告。

8.4.3 社会工程框架的运用

正如本案例中所展示的，信息收集不仅可基于网络，还可以亲自到现场收集。这个案例中的大量信息就是我去现场亲自采集的。找到他们所使用的计算机系统、了解目标对特定问题的反应及查出票务系统的运作方式是本次信息收集的主要内容。

这次攻击中最重要的一点是，好的伪装不仅仅是编造一个故事、装扮一下造型、假冒一下口音，而是可以毫不费力地"设身处地"。

在这个场景中，我能自如地把握父亲的口吻、动作和谈吐，因为我就是一个父亲。我对获得"年度最烂老爸奖"的担心是真实的而不是假装的，我的感情是真挚的，所以会让目标觉得我是真心的。这一切让我的言行更加可信。

当然，有一个可爱的孩子站在远处，用渴望的眼神望着售票员，以及酒店打印机坏掉的情节也十分可信。在第2章中曾提到过，有时社会工程人员需要提升伪装能力，或者至少是个说谎能手，但我相信实际上不止这么简单。

从专业角度来看，伪装需要创建一个现实的、能操纵目标感情和行为的角色。人们通常不会被一些简单的谎言所蒙骗。一名社会工程人员必须"就是"那个伪装的角色，所以选择与你生活

① 密码BESMART的含义是"聪明些"，有点警告的含义。——译者注

贴近的角色是一个不错的主意。

“免费试用PDF软件”这个借口存在很大的漏洞。这个借口本身是没问题的，但是可能会被立即拒绝从而影响下一步的攻击。还有一个侥幸就是售票员所使用的PDF阅读器版本和公司所使用的一样，没有升级，这才让我有机会入侵。

通常，我认为利用人类固有的惰性就是一场赌博，但是在这个案例中我成功了。有时候最好的办法就是相信自己提出的要求是理所应当的。这能让你感到自信，让目标相信你的言行是正当合理的。

正如我在第5章中提到的，使用类似“我真的需要你的帮助……”这样句子，是一个非常好的技巧。乐于助人是人类的天性，特别是当别人开口请求时。

即使是完全陌生的人，在面对请求时也会竭尽全力地给予帮助，就像此案例中从别人的电子邮箱中打开一个未知文件。帮助一个“可怜的父亲”，让他可爱的女儿进入乐园，这样一个请求却导致公司系统被入侵。

一旦入侵成功，存储所有客户的信用卡信息的程序就会成为攻击者的猎物。轻松收集一些数据，就可能让乐园蒙受巨额损失、面临诉讼以及陷入困窘。

8.5　最高机密案例1：不可能的使命

每当我和同事参与或者听到一些给力的情节和故事时，都希望它能够被拍成电影。但出于安全因素的考虑，我们不能泄露内情，所以写和说都是不可以的。出于这些原因，我不能提及真实的参与者以及故事中泄露的信息。下面是一个有关一位化名为“提姆”的社会工程人员的故事。

提姆的目标是入侵一台存储着至关重要信息的服务器，如果这些信息被泄漏了，将导致灾难性的后果。这台服务器的合法所有者是一家知名的公司，他们对它设有重重防护。与该公司签订获取信息的合约时，提姆清楚地认识到自己必须用尽全力，这项工作可以说是对他社会工程技能的挑战。

8.5.1　目标

这次攻击的目标是获取一家知名企业的某些商业机密，这些机密绝不能泄露给竞争对手。这些秘密被安全地存储在服务器上，没有任何外部访问通道，信息只能从内网访问。

提姆与该公司签订协议，帮助该公司测试其安全性，防止“恶意人员”入侵并窃取信息。协议是在公司外面签订的，协议内容之前已经通过电话和邮件的方式谈妥了。

8.5.2 故事

提姆面临一个巨大的挑战。按照社会工程的步骤，第一步是信息收集。提姆不知道攻击中会使用到什么样的信息，所以他开始了冗杂的收集过程，内容包括邮件布局、报价申请表、所有能找到的员工姓名、他们参与的社交网站、他们发表的文章、他们参加的俱乐部以及他们的服务供应商信息。

他计划去翻一下公司的垃圾箱，却发现垃圾桶周围的安全戒备森严。许多垃圾箱甚至还与外部隔离，所以除非他能翻墙而入，不然连垃圾箱的标志都看不到。查出处理废品的部门后，他决定按照他绝妙的计划给公司打一个电话。

“你好，我是TMZ垃圾处理公司的保罗。我们是本地区新成立的一家垃圾处理公司，已经有一些大公司选择了我们的服务。我是负责贵公司所在区域的销售人员。我能发送一份服务报价单给你吗？”

“可以，我们对现在合作的对象很满意，不过你可以发一个报价来看看。”

“好的，我能快速地问你几个问题吗？”

“当然。”

“你们有多少垃圾箱？”提姆问道。在询问了他们是否有特殊的针对纸张、U盘和硬盘的垃圾箱之后，他最后又问了几个问题。

“你们通常哪天叫人来收废品？”

“我们每周叫人来收两次，第一区是星期三，第二区是星期四。”

“谢谢。我准备一下报价，然后明天下午发给你。你的邮箱地址是什么？”

“你可以发送到我的个人邮箱：christie.smith@company.com。”

现在他们开始了友好的闲谈，不知不觉中，他们说笑着寒暄了起来。

“太感谢你了。嘿，挂电话之前，你能告诉我你们现在是和哪家公司合作吗？我想做一份与他们的比较报价。”

“恩，你知道的……”她犹豫了，但还是说了，“好吧，我们现在的合作伙伴是‘废物管家’公司。”

“谢谢你，克里斯蒂。我相信你一定会对我们的报价满意的。我们稍后再联系。”

有了这些信息，提姆打开废物管家公司的网站，将他们的公司标志保存为JPG文件。然后他

访问了在线衬衫打印网站，72小时后，他就收到了一件印有该标志的衬衫。因为知道垃圾将在周三周四被回收，所以他决定周二晚上行动。

接着他又给安全部门打了个电话。

“你好，我是‘废物管家’公司的约翰，你们的废品回收服务商。克里斯蒂·史密斯的办公室来电说你们有一个垃圾箱损坏了。我知道收废品的日子是周三，所以我想明天晚上去看一看。如果有损坏的情况，我们会随车装一个新的去。我周二晚上过去方便吗？”

“好的，让我查查。可以，乔明天在。你就停在保安亭旁边，他会给你张出入证的。”

“多谢。”

第二天提姆穿着“公司”的制服，手拿一块记事板出现了。他的伪装非常到位，因为他清楚日期还有内部工作人员的名字。现在，作为一名服务公司的员工，他走到保安亭前。

“乔，我是垃圾清理公司的约翰，昨天来过电话。”

门卫打断说：“是的，我看到你的名字了。”他给了提姆一张出入证和一份地图，告诉他怎样走到放置垃圾箱的地方。“需要有人陪你去吗？”

“不用了，我很熟悉。”

提姆随即驱车前往垃圾箱的放置点。

完美的伪装和一张出入证为他提供了足够的时间进行信息挖掘。他知道第二区存放的是非食品类垃圾，所以就先从那里开始。

没过多久，他就找到了几块硬盘、几个U盘、几张DVD光盘和一些装满纸的袋子，将它们全部放入卡车中。过了一小时左右，他告别门卫，并且对他们说问题解决了，然后开车离开了。回到办公室后，提姆开始深入搜索这堆“垃圾”中的信息，竟然有了意想不到的收获。

公司经常将不要的硬盘和U盘完全毁坏后再丢弃，他们会擦除上面的数据再送到专门的回收部门。但是，总是有些员工不严格遵守回收处理程序，把不能用的U盘或者无法启动的硬盘随手扔掉。他们没有意识到的是，有些软件可以在不启动硬盘或介质的情况下导出其中的数据，甚至在某些介质已经被格式化的情况下，数据也是可以恢复的。

废品中有一袋文件，内容看上去像是属于办公室的。掏空这个袋子后，提姆找到了一些没被粉碎的纸张。他开始阅读，其中有一份是关于IT服务的合同标书，这项服务工作几天后就会开始。这张纸看上去像是擦拭过溢出的咖啡，然后被丢弃的。

这是一个重大发现，但是还需要进一步调查。DVD光盘都是空白的或者不能读，但惊喜的是他在U盘中找到了一些文件。从这些信息中他发现了CFO的名字及其私人专线，以及其他一些重

要的人事信息。

他收集到的信息具有很大的价值，但是我们需要关注的是他的下一步行动。由于掌握了与IT服务公司签约的信息以及服务的内容，提姆故意在第二天午餐时间给合同联系人打了个电话，期望他出去吃午餐了。

“你好，请问塞巴斯蒂安在吗？”

“他不在，出去吃午饭了。请问我能帮你吗？”

“我是XYZ技术公司的保罗。我想确认一下我们团队是否可以明晚到达，然后开始项目。”

“是的，请记住不要影响我们的正常工作，所以尽量不要在下午5:30之前到这里。”

“好的，先生，我知道了。明天见。”

提姆知道第二天他不能与其他“同事”一起到场，但是如果时间安排得好的话，他就不会被IT服务公司和目标公司的人逮个正着。在黑暗的停车场内等候了许久，他看见IT服务公司的人来了。大约30分钟后，他走到门口，解释说他和刚才进去的人是一起的，只不过刚刚返回车中去取一些文件。他获准进入了，现在他可以自由地进入办公区域了。

他还需要侦察一番，他认为最好的方式就是以内部工作人员的身份接近IT服务公司的人。徘徊了一会儿，终于听到有人在交谈，并且从一个人的穿着看出他是IT服务团队的一员。

由于从U盘的文件内容中得知了一些高层管理人员的姓名，并且从合同中获知了合同联系人的姓名，他上前说道：“你好，我是保罗，CFO施瓦茨先生的手下。有人给你解释过prod23生产服务器的事吗？”提姆从收集到的信息中获悉了服务器的名字，而且知道这正是那台需要他入侵的服务器。

“是的，我们知道那台服务器是禁止接触的。CFO向我们说明了它的加密情况和重要性。不用担心。”

几分钟交谈过后，提姆掌握了一些有价值的信息：

- IT服务人员不能接触服务器；
- 服务器采用了整盘加密；
- 内部IT技术人员“炫耀”说，只能通过管理员携带的U盘上的密钥文件访问。

提姆知道，最后一点会增加他任务的难度，因为管理员不在场，他现在不能访问服务器。另外，服务器的物理安全措施也非常坚固，看上去很难闯入。他十分明确一点，就是管理员可以访问服务器，所以决定从这一点下手。

首先，他来到管理员的第一间办公室，但是门是锁着的。他继续检查第二间，然后是第三间。

第三间办公室的门关着但没有关严，他稍稍一推，就进去了。

为了防止自己被当场抓获，他拉上窗帘关上了灯。他随身携带的社会工程工具套装中装有许多软件和衣物，进行此类攻击时他经常携带的一个工具是Linux启动U盘，比如BackTrack。在BackTrack中预装了一个免费的开源虚拟机工具Virtual Box软件。

他将U盘插入管理员计算机后面的USB端口，启动进入BackTrack。之后，通过SSH与自己的计算机建立连接，创建一个监听程序，然后通过管理员的计算机建立反向会话，继而在BackTrack中启动一个键盘记录程序（记录计算机上键盘敲击的所有信息），通过SSH将这些记录发送到自己的计算机上。

接着他给出了致命的一击。他打开Virtual Box软件，新建一个Windows虚拟机，使用本地硬盘作为启动盘，加载虚拟机。换言之就是，它加载了管理员的账户信息和操作系统。他将虚拟机的登录画面切换成全屏模式，隐藏所有的工具栏，将Virtual Box中现有的退出热键修改成一个特别长的组合键。这是为了防止用户误打误撞而暴露他们被攻击的事实。

通过后端U盘将本地硬盘载入虚拟机的方法，随时都存在被抓的风险，但是这个方法奏效的话，他就能得到管理员每次敲击键盘的记录，而且此人计算机上开放的反向连接使得他可以访问所有内容。即使链接不是在虚拟机中，通过管理员敲击键盘的记录，他还是可以使用受害者的用户名和密码进入到虚拟机中。

提姆在办公室里还做了另外几件事情，例如在另一台电脑上也建立了连接，以提供远程访问入口。他还通过手机SIM卡设置了一个远程监听装置，他可以使用任何一部电话拨打这个号码，监听该装置约6米范围内的对话。

几小时后，提姆离开目标公司回到自己的办公室。他很兴奋地检查这些装置是否能正常运行，但是他还有一些想法要实施。

第二天一大早，他确定远程连接还开着，于是拨通了监听装置，听了听人们早晨进入办公室的情况。正如他所期望的，计算机的第一条记录来了，捕获了管理员的用户名和密码。

大约一小时后，提姆看到不断有记录传进来。他知道如果此时有所行动的话，可能会让连接暴露，所以他只能等着。大约12:15左右，记录传送停止了，他猜想管理员一定是去吃午饭了。他立刻检查了反向会话，利用捕获到的服务器密码从管理员的机器上创建了一条到服务器再到自己机器上的通道。

建立完通道后，提姆在下午1点之前发疯似地尽可能复制数据。那时他没有看到任何键盘记录，无意中他听见监听器中有人问："你知道这会还要开多久吗？"

得知管理员可能在开会，他发起了一个更大的传输任务。大约30分钟后，他发现了一些活动迹象，所以暂停了信息收集，想等晚点再看看。他可不想引起管理员的任何怀疑和警惕，因为文

件传输连接可能会减慢其上网的速度。他开始筛选从服务器上抓取的数据，收获颇丰。

工作还没有结束。那天晚上他传输了大量的数据，可以说是尽其所能，然后再次来到了目标公司，像之前一样通过社会工程方法进去了。他来到管理员办公室，发现门是锁住的拉不开，于是用推刀（见第7章）把门打开了。

进去之后，他先关闭虚拟机，然后拔下U盘重启计算机，依老路离开管理员办公室。他收好监听器，确保没留下什么痕迹。

离开大楼，回到自己的办公室后，他整理了一天的收获。当然，去参加报告会时，他带了一叠打印文件和一个装满数据的硬盘。房间里的每个人都目瞪口呆。

8.5.3 社会工程框架的运用

这个故事让我们受益良多。这是一个杰出社会工程人员的例子。这个过程可以总结概况为练习、准备，当然还有信息收集。可以想象，他使用的所有技巧，从推刀的使用到建立通道，再到有效的伪装与信息收集，都是经过不断练习才得以熟练应用的。

对于信息收集的重要性，这里就不再赘述了。我知道大家对此已耳熟能详，但是必须指出的是，如果提姆没有做适当的信息收集，那么此次行动必败无疑。

通过打电话和现场勘查的充足准备，以及恰当硬件设备的选取，提姆的这次行动取得了成功。通过分析这次攻击行动，你可以看到一些社会工程基本原则的实际运用。

提姆是一个信息收集大师，利用网站资源牵出了各种有价值的信息，在打电话时运用了专业的诱导技巧，并且在与目标面对面时运用了杰出的说服技巧。这些技能使得他收集信息的水平远远超出了那些未经专门训练的黑客。

信息收集奠定了提姆伪装与提问的基础。

垃圾箱翻查计划十分精妙。在没有工作服和预约的情况下，他可能进入吗？当然。可是，他的方式到底是多么地有说服力呢？他没有令任何一个和他打交道的人产生怀疑，而且他们都毫不犹豫地按工作流程行事。如果一个人在接触你时丝毫没有引起你的防备和警惕，那他的伪装就堪称完美。提姆做到了，并且可以在垃圾区自由活动。

最精彩的部分是他进入大楼之后发生的事。出问题的几率极大，任何不当的行为都可能让他被逮个正着。他可以进入服务器房间，取走数据然后离开，可能都不会有人阻止他。但是如果采用这种方式就意味着公司不会知道他们的机密是如何被窃取的，也不会意识到他们的计算机曾被入侵过。

提姆冒着极大的风险在管理员的电脑上运行了一个虚拟机。这个特殊策略失败的可能性太高

了。如果有人重启了计算机或者电脑突然宕机，又或者管理员碰巧误按了那个巨长的组合键，都会毁了整个攻击行动，并提醒公司他们的计算机已经被入侵了。

我可能会采取不同的、风险较小的方法，使用定制的EXE程序在他的计算机与我的服务器之间建立反向通道，通过修改计算机的启动脚本，使这个EXE程序不会被杀毒软件检测到，这样失败的可能性更低，但是提姆的方法属于十分有个性的社会工程攻击。

从这次特殊的攻击行动中，我们学到的可能不止一点，但最重要的一点是，“不要轻易相信任何人”这句古老的黑客格言。如果有人打电话说克里斯汀批准了某人检查垃圾箱，但她没有亲自告诉你或者备忘录中也没有，则需打电话向她询问。晚上要关闭电脑，确保它在没有密码的情况下无法通过U盘启动。

当然，这些额外的预防措施意味着更多的工作量和更长的加载时间。是否值得去做得由机器中储存的数据的重要性决定。在这个案例中，这些数据足以使这家公司倒闭，所以保护措施应该做到极致。虽然公司在服务器周围采取了许多先进的预防措施，例如硬盘加密、摄像头及生物锁等，却没能保护那些能够访问最重要的数据的计算机，这可能将会导致整个公司的终结。

8.6　最高机密案例2：对黑客的社会工程

思维不拘一格且快速敏捷是社会工程人员的标准技能，所以对专业的社会工程人员来说，陷入困境的情况很少见。如果在没有事先警告的情况下，让一名渗透测试人员进行社会工程，又会出现怎样的情况呢？

下一个案例就将讲述这一罕见的情况。这是一个非常好的例子，将证明平时多练习社会工程技能在紧急情况下会大有裨益。

8.6.1　目标

“约翰”需要为一个大客户进行一次标准的网络渗透测试。审计大纲中没有任何关于社会工程和现场的工作，这可谓是一次没有任何刺激的渗透测试。然而，他还是很乐意为客户找出网络中的安全漏洞。

在这项审计中，一开始确实没发生什么惊心动魄的事。他按照常规路数扫描并记录数据，测试可能被入侵的端口和服务。

就在一天的工作快结束的时候，他通过Metasploit扫描找到一个开放的VNC服务器，通过这个服务器可以控制网络中的其他计算机。这是个不错的发现，因为全部网络是被限制访问的，所以这种简单进入的方式特别受欢迎。

约翰正在记录所发现的开放VNC会话，突然背景上的鼠标开始在屏幕上移动。这是一个严重的警告，因为此时此刻，客户方是不允许用户进行任何合法的连接和系统使用的。

发生了什么事？约翰注意到这个人并不像是管理员或者一般用户，他显然对系统不是很熟悉。约翰怀疑这是个不受欢迎的入侵者。虽不想把入侵者吓跑，但他想确认这个人究竟是管理员还是入侵了同一个系统的另一个黑客。

很快，约翰的目标从渗透测试变成了找出入侵组织内部的恶意黑客。

8.6.2 故事

约翰立即决定对该名黑客进行社会工程，并且搜集尽可能多的资料来维护客户的利益。他真的没有时间做十分周密的计划，也没有时间做适当的信息收集。

他冒着很大的风险，打开记事本程序，决定伪装成一名“n00b”黑客，也就是一个新手、技术菜鸟，和对方一样，看到这个口开着就进来了。他截取了一些与黑客对话的屏幕截图。注意看一下图8-1，他是如何对黑客进行社会工程的。约翰先开始对话，次行是黑客说的话。

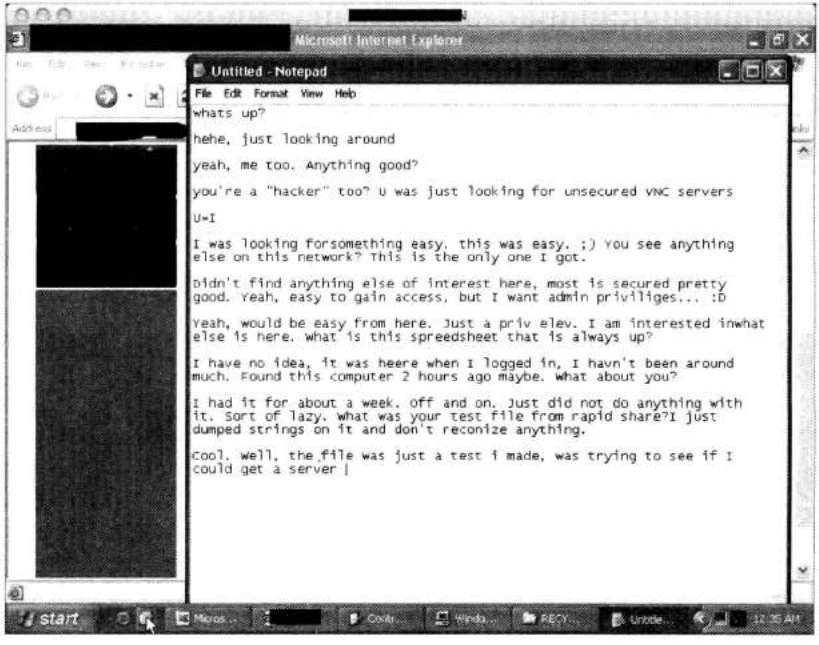

图8-1 事件的屏幕截图

下面是对话的原稿。它很长，其中出现的所有错误和黑话都是未经加工的，但是会揭示出这次攻击的原貌。约翰（宋体）首先开始说话。

– 嗨，什么情况？

– 呵呵，随便看看。

– 呵呵，我也是。有什么好东西吗？

– 你也是“黑客”？你在寻找不安全的VNC服务器。

– 你=我

– 我找的都是简单的系统，这个系统就是。:) 你在这网络中还有什么其他发现吗？我只找到这个。

– 没找到什么有趣的东西，大部分系统都保护得不错。是啊，很容易进来，但是我想要管理员权限…… :D

– 是啊，获取这里的管理员权限再简单不过了，提权就可以了。我感兴趣的是这里还有什么。这个一直打开的电子表单是什么？

– 我也不知道，我进来的时候就是这样了，我还没怎么看呢。大约两小时前刚发现这台电脑。你呢？

– 我发现快一个星期了，时不时进来看看，但还没用它做任何事，有点懒。你在快速共享上的测试文件是什么？我提取了里面的一些字符串，但是看不清。

– 酷。文件是我做的一个测试，我尝试运行一个程序（特洛伊木马），但是被防火墙阻止了。

– 哈哈。我也遇到了相同的问题。我做了个metasploit脚本，但也没有进展，这就是为什么我还在这。你是本地的还是国外的？我知道有些人是丹麦的。

– 我是挪威的，呵呵，我在丹麦有亲戚。

– 你逛什么论坛吗？我以前有几个喜欢的论坛，但后来都消失了。

– 我主要逛编程论坛，其他地方不大去。你做黑客很久了吗？能问一下你的年龄吗？我22岁。

– 我做这个一年左右，主要是为了好玩。我还在上学，16岁，就是找点事做。你去过邪恶地带（evilzone）吗？

– 没有。我做这个也纯粹是为了好玩，只是想看看自己能做什么，测试一下我的技能。顺便说一句，我写了个“VNC探测器”程序，已经找到了很多服务器，但是只有这里还有点意思。

– 哇。你都写了什么代码呀？我能下载吗？你有网名不？

- 我是用PureBasic写的，但发布还为时过早，现在就自己用用，可能以后会共享出来。我可以上传代码，你来编译，但你要先在软件仓库站点下载一些PureBasic编译器程序：P
- 那太酷了。你可以放在irc附带的pastbin站点上，那里可以匿名发帖。我以前没有用过purebasic，只会python和perl。
- 让我想想，我去pastebin站点上传，给我几分钟时间就好。
- 好的，酷！你有网名吗？我的是jack_rooby。
- 网名，有啥用？我不上irc聊天，但你可以通过电子邮件联系我。
- 太酷了。我指的是irc或论坛上用的账号。邮箱也可以。
- 哦，在编程类论坛上我都是用的全名。可能这么做不够聪明。我的邮箱是intruder@hotmail.com。
- 给我发消息，也许我可以加你为MSN好友。
- 会给你发的。认识会编程的人真不错，如果我以后干这种事的时候卡壳了或找到有用的信息，都可以拿来分享。
- 呵呵，是的，现在我们是一伙的了：P
- 酷！pastebin上传好后告诉我。
- http://pastebin.ca/1273205
- 顺便说一声……这还停留在"alpha"阶段，用户界面还没完成，但可以通过一些变量进行配置。
- 酷。我测试下，看看能不能用。谢谢你的共享。如果我做了什么很酷的事情，能发邮件给你吗？
- 好啊，没问题。如果持续运行这个程序几个小时，你会找到很多服务器的。我还编了些代码去检测服务器的安全配置和漏洞，即使有密码保护也能进入系统。这些服务器的检测结果会以“不安全”（insecure）标志显示出来。但有时候也会出错，不安全的其实并非不安全，但这种情况不是很多，你自己测试看看吧。
- 哇。我在这里也看到其他vnc服务器了，但是都要密码。你的工具可以进入吗？
- 只是很少一部分有漏洞的可以进入，但是你必须使用专门的客户端，像这里说的：
- http://intruderurl.co.uk/video/

– 下载zip文件。

– 好的，我会下载看看。太酷了。快速共享中的后门也是你自己写的吗？还是从其他地方得到的？

– 我自己尝试写了大多数的工具，通过这种方式来学习。是的，这是我自己写的，但是还没有完成，我只是想看看能否运行服务器程序，但还不行，呵呵。

– 知道了，我有点想放弃了，但还是觉得应该回来再试试其他方法。我想这里还有些东西吧，但是我没有自己的僵尸网络，有个叫Zoot54的人想卖给我一个，还有人为他担保，但是我根本不信任他。我还不知道怎么写自己的工具，大部分perl和python对于这种windows主机都不起作用，所以我打算用metasploit，但是出现了防火墙错误。你对此有什么想法吗？有什么酷一点的做法吗？还是转向下一台主机？

– Perl和python都是很好的开始，不过我自己没用过。但当你学会一些语言时，学其他的也不难 :P 也许你可以先试试PureBasic，学起来很容易。呵呵，僵尸网络很酷，我想做一个，但是要让它自我传播有点困难，至少在Vista上不容易。可是，我还没打算放弃这台服务器，再尝试一些别的方法，一定能有办法得到更多权限的。:D

– 酷毙了，你就用这台服务器尝试吧，我已经进来好久了，不知道下一步该做什么了。让我看看你会怎么做，我就能学到更多了。这真是太酷了。你有myspace或者facebook之类的账号吗？只用邮箱吗？

– 现在先用邮箱，等我完全信任你以后，也许会在facebook上加你，我没有myspace账号。我会和你保持联系的：）

– 酷，用邮箱也可以。你有命令行通道吗？还是也用这个相同的图形用户界面？这是个多连接的vnc？

– 是的，我只用ThightVNC或者其他工具，确保不会断开其他用户。实际上我不是命令行粉丝，呵呵 :S

– 酷。我用命令行时常常会犯错，导致连接断开。

– 感谢你没把我断开 :D，一开始见你在这乱搞一气的时候，我还想“糟了，撞上管理员了”，呵呵呵……

– 哈，我看过时区设置，这公司在美国中部，所以对他们来说现在是半夜。

– 是的，我也看到了。我还做了网速测试，呵呵。似乎他们的上传速度要大于下载速度，好奇怪啊……但可能会便于DoD攻击。

– 我指的是DoS（拒绝服务攻击）。

– 我还奇怪这个说法是什么呢，还以为是一个很有趣的名称……你进入过这里的其他系统吗？我很早以前看到过一个软件仓库服务器，但是现在已经不在了。

– 我没有发现其他系统。但是我想访问他们所有的网络计算机……可是数量太庞大了，简直像个大学一样。呵呵，我之前输出了“hello world”。

– 哈哈，你发送到打印机还是屏幕啊？这些人要是某天中午看见鼠标在电子表格应用中乱动，一定会吓一大跳的。

– 哈哈，是的。但是VNC服务器不设密码，太白痴了啊？！我向打印机输出了一些东西，希望有人能看到。

– 哈哈，我相信会的……他们不能在没有管理员权限的情况下运行，所以这不是普通用户做的，一定是某个管理员设置的，不然的话我们的后门就能用了，但是它们现在根本不能运行。或者有人更改配置了？

– 嗯，我想你是对的，可能是某个管理员或者怪胎……

– 你靠这个谋生吗？我一直听你说能靠这个赚钱，我想要是我做一段时间，变得更厉害的话，就能靠它吃饭了。你也是这样做的吗？

– 我是靠编程吃饭的，不从事黑客或者安全类的工作。但这是个好主意，人们愿意为测试安全付钱，如果我们做得好的话，或许能靠这个赚一大笔钱。

– 那正是我希望的。我在“有道德的黑客”网站上买了本书，里面有些不错的程序。我不清楚做测试要多大年龄，但是这可能是我从事这些工作的好起点。里面有许多很好的工具，比如metasploit。如果你没看过的话，真应该好好研究下。

– 好的，谢谢，我会去看的：）可是我现在有点累了，呵呵。我不能整天在这简陋的记事本上聊天，呵呵。以后聊，伙计。遇见你真酷，和你聊天很有趣。

– 是啊，在屏幕上看到记事本时还真是吓了一跳。很高兴遇到你，我会发邮件告诉你程序用得怎么样。很想知道究竟会发生什么。祝你顺利，不要被当做坏人抓了哈！

– 呵呵，谢谢，你也是！：）这很有趣，我要把记事本上的聊天内容保存下来，等我一会，哈哈……

– 好的，哈哈，抱歉。

– 再见。

– 再见。

这场闲谈表明约翰能快速地伪装成另一个人。这不是件容易的事，通常需要周密的计划，但是为了维护客户的安全利益、找到入侵者，他不得不将自己伪装成黑客。

最后，约翰取得了黑客的照片、邮箱和联系信息。他将这个恶意黑客报告给了客户，之后系统得到了修正，保证不会再有轻易入侵系统的事情发生。

这个最高机密案例反映了以专业的方式运用社会工程可以很好地保障客户的安全。

8.6.3　社会工程框架的运用

这个案例中有趣的是，公司并非黑客的真正目标。他只是在互联网上寻找易攻击的目标，没想到正好碰到了。对外开放访问权限是十分危险的，若不是刚好被渗透测试人员发现，后果该会多么严重啊！

当然，从这个故事中我们也可以学到许多有关社会工程的知识。约翰刚刚进行检测时并没打算使用社会工程技巧，只是想做一个简单的渗透测试。有时候你必须在毫无准备的情况下运用社会工程技能。

约翰为什么能够在没有回家练习的情况下完成这项任务？很可能约翰每天都在使用这些技巧，至少是经常练习，所以才能运用自如。

从这个案例中学到的最主要的一点可能就是熟能生巧。实际上，约翰本可以在遭遇黑客时，告诉对方自己是管理员，他的所作所为已经被记录，其黑客生涯结束了。他可以使用各种威胁方法，可以将恐惧做为主要战术。

但是这样的话，黑客很有可能会逃跑，之后会返回并试图格式化系统，或者造成更大的破坏以掩盖其入侵痕迹。相反，思维敏捷的约翰在目标身上收集了大量有用的信息，随后利用目标的邮箱、姓名以及Maltego软件，掌握了此人的所有活动。

分析这个故事还能学到的一点就是变通，即随着事态的发展随机应变。当约翰开始从这位黑客身上“收集信息”时，他不确定对方是黑客还是管理员。针对他的第一句话——“嗨，什么情况？”，攻击者可以作出多种回答。在不知道对方会作何反应的情况下，约翰没有时间准备，只能用行话，按照黑客的方式作出反应。

约翰考虑得甚至更远。约翰知道顺应别人的效果最好，于是伪装成n00b，一个水平不高的新手，渴望得到一名技艺超群的真正黑客的教导。在满足了黑客的虚荣心之后，约翰诱导他泄露了各种信息，包括他的联系方式和一张照片。

8.7 案例学习的重要性

本书仅介绍了几个案例，它们远不是最可怕的。每天，政府、核电站、资产几十亿的大公司、公用电网甚至整个国家都会成为恶意社会工程攻击的受害者，此外，诈骗、身份盗用和抢劫等每时每刻都在发生。

要避免这些悲剧，最好的一个方法就是研究案例，各个领域的专家都使用这个方法。为了研究表现人类情绪的微表情，心理学家和医生会花无数个小时观看录像和采访记录。

说服方面的专家会回顾、分析并研究积极和消极的说服方式。这有助于他们了解哪些微妙之处会影响他人，以及如何运用它们来保护客户。

司法部门将案例学习作为日常工作的一部分，以便了解罪犯犯罪的原因。犯罪调查员会分析和剖析歹徒的每一个方面，包括他们的饮食、社交、思维方式以及行为的原因。所有这些信息都有助于他们理解罪犯的思想。

这也是专业侧写员找到并抓捕“坏人”所使用的方法。同样，专业的社会工程人员不仅通过自己的案例来学习，同时也通过实践中接触到的案例以及新闻报道中的案例来学到很多知识。通过研究案例，社会工程人员能真正看到人们心理上的弱点，明白为什么社会工程框架中的策略会如此容易奏效。这也是我孜孜不倦地更新www.social-engineer.org的原因，这样能够确保框架中包含了最新的故事和案例，大家可以用这些来提高自身的技能。

最后，由于人们天性中的盲目轻信、同情、怜悯以及帮助他人的欲望，这些攻击都成功了。在日常生活和交往中，我们不应该丧失这些品性。但同时，这些特点也常常被恶意社会工程人员所利用。可能听起来我像是在鼓励大家要像机器人一样铁石心肠、冷酷无情。尽管这样能让大部分社会工程人员无从下手，但也会使生活黯然失色。我所宣扬的是，提高警觉、不断学习以及准备充分。

8.8 小结

本书宣扬的重点是利用知识来保障安全。只有意识到危险的存在，知道“罪犯”如何思考，同时能够正视并接受“恶人”的存在，你才能真正地保护自己。为此，本书的最后一章将讨论怎样防御和减轻社会工程攻击。

第9章
预防和补救

前面的章节向大家展示了社会工程人员诱骗目标泄露重要信息的各种方法和途径，同时也描述了社会工程人员用来影响和操纵他人的许多心理原则。

有时在听完我的演讲或是安全培训之后，人们会显得非常恐惧和害怕，他们会这样说："似乎根本没有办法保障安全。我该怎么做呢？"

这是一个很好的问题。我建议制定一个良好的灾难恢复计划和事件响应机制，因为就目前而言，被黑客攻击可能不是"是否"会发生的问题，而是"何时"会发生的问题。你可以采取一些防御措施，至少在安全战役中给自己一个反击的机会。

减轻社会工程攻击并非只需确保硬件安全那么简单。按照传统的安全防御思路，你会把钱投到入侵检测系统、防火墙、防病毒程序以及其他维护周边安全的解决方案上。可是在社会工程攻击面前，没有任何软件系统可以安装到你的员工和自己身上以保障安全。

本章列出了我为客户提供的预防和减轻社会工程攻击的6大步骤：

- 学会识别社会工程攻击
- 制定提高个人安全意识的计划
- 充分认识社会工程人员意图获取的信息的价值
- 及时更新软件
- 编制参考指南
- 从社会工程审计案例中吸取经验教训

归根结底，这6点旨在创建安全意识文化。安全意识并非是每年花个40分钟、60分钟或90分

钟做一次培训，而是需要创建一种文化或一套标准，让每个人在一生中都坚定不移地运用。它不只关乎工作或“重要的”网站，而是一个人实现整体安全的方式。

本章涵盖了上述的6点，并分析了为什么创建安全意识文化是防御恶意社会工程人员最有效的措施。

9.1 学会识别社会工程攻击

防御和减轻社会工程的第一步是了解攻击。你不必深入了解这些攻击，不需要知道如何创建恶意的PDF文件或者如何制造完美的骗局。但是你必须清楚地知道打开一个恶意PDF文件时会发生什么，必须知道通过什么迹象来判断是否有人在骗你，这样才能保护自己。你需要了解威胁以及运用威胁的手段。

举例来说，你十分重视自己的家，尤其是家人。你不会在火灾发生时才开始计划、预防和减轻火灾所带来的危害，而是会提前安装烟雾探测器并设计发生火灾时的逃生路线。此外，你还会对孩子进行火灾逃生口诀训练，“停、放、跑”。你会教他们通过摸门来判断温度以及蹲低身子防止吸入烟雾。所有这些方法都是为了防止一场真正的火灾以及减轻火灾带来的危害所做的准备。

这些原则同样适用于保护你自己和你的公司防御社会工程攻击。不要等到攻击发生后才意识到它们的危害会有多严重。不要认为我在自我推销，我建议定期对员工进行社会工程审计，看看他们是否具备抵御攻击的能力，然后再进行培训。

教导你自己和员工面对此类攻击时，如何像逃生口令那样，做到“停、放、跑”。社会工程人员攻击公司的最新案例是什么？就像知道火灾会对你家造成什么后果一样，了解这些是预防的第一步。要了解现代社会工程人员与身份窃贼所使用的方法有何不同。你可以在社会工程网站www.social-engineer.org/framework/Social_Engineering_In_The_News上查看有关社会工程人员、骗子、身份窃贼等的最新故事和案例。

另一个好方法就是阅读本书。本书包含了社会工程人员所使用的操纵对象的所有方法及原则。书中不仅涵盖了案例及绝妙的黑客攻击事件，还分析了恶意社会工程人员的思维方式和所使用的策略。

你还可以登录社会工程网站（www.social-engineer.org）的资源区观看视频，它们真实地演示了行动的过程。普通用户不需要通过视频了解如何亲自去执行这些攻击，只需了解社会工程人员是怎样进行攻击的就可以了。

一般来说，你越了解攻击的方式，就越容易“随时”识破它们。要了解社会工程人员使用的肢体语言、表情和措辞，这样当听到或看到某人使用这些方法时，你就会马上有所警觉。

你无需耗费大量的时间去学习社会工程方法。然而，时不时花几分钟时间阅读一下社会工程网站或其他网站上的新闻和案例有助于你了解现今社会工程人员攻击公司的方法。

在你对这些知识和审计过程有了基本的了解之后，接下来创建安全意识文化就相对简单些了。

9.2　创建具有个人安全意识的文化

2010年7月，我所在的安全专家小组在Defcon第18届安全会议上举办了首次有组织的专业级社会工程竞赛。一群最优秀的、最聪明的人纷纷从世界各地会聚到内华达州的拉斯维加斯，参加每年一次的交流、培训和学习。

我和小组成员都认为，这将是一个举办竞赛的好机会，可以评测美国的公司是否易受此类攻击（对“竞赛”的反应）。于是我们组织了比赛，感兴趣的人都可报名参加，竞赛分成两个阶段：信息收集和主动攻击。

为了保证比赛的合法性和道德性，我们不希望任何人受到伤害，所以规定不准收集任何社保号码、信用卡和个人身份信息。我们的目的不是让任何人遭到解雇，也不是让任何公司陷入窘境，所以我们决定不涉及公司密码或其他与个人安全相关的信息。相反，我们制定了一个有25~30个“旗标”的列表，包括查出公司是否有内部自助餐厅、谁负责处理公司的垃圾、公司使用何种浏览器、用何种软件打开PDF文件等。最后，我们选择的目标公司覆盖了美国的各行各业，如天然气公司、科技类公司、制造商及零售商等。

每位参赛选手都会被秘密地指派一个目标公司，他有两周的时间去做被动的信息收集工作。这就意味着选手不能联系公司、给他们发邮件，也不能尝试用其他社会工程方法收集信息。相反，他们必须使用网络、Maltego和其他工具收集尽可能多的信息，最终完成一份专业的报告。

通过收集到的信息，我们希望选手能找出一些能够在现实世界中合理运行的攻击方法。然后选手必须来到拉斯维加斯的Defcon大会，坐在一个隔音的电话亭里，打25分钟的电话给他们的目标，实施攻击，看看可以得到什么信息。

我原本可以在接下来的20~30页中告诉你竞赛中发生了什么、结果是什么，但我只想说一件事，那就是每个选手都从目标那里获得了足够的信息，这些公司都未通过安全审计。不管选手的经验和伪装处于什么水平，他们都成功完成了预设的目标。关于这次竞赛的详细报告，请浏览www.social-engineer.org/resources/sectf/SocialEngineer_CTF_Report.pdf上的有关文档。

这里要提到的就是安全意识。关注安全问题的公司有员工培训项目，以培养他们提防来自电话、互联网或者个人的潜在安全风险的意识。但我们发现这些公司的安全意识还是很薄弱。为什么？世界500强企业在安全、培训、教育、服务上花费了数百万美元，可为什么雇员的安全意识还是不够强呢？

这就是本节标题所提到的，安全意识不是员工的个人意识。在安全实践中，我经常和雇员聊起他们对攻击事件的看法，他们的反馈常常是："这些又不是我的数据，我担心什么？"这种态度表明了公司想要灌输安全意识却没能切中要害，没有引起重视，没起到效果，最重要的是，没有与个人挂钩。

回顾能找到的许多所谓的安全意识培训材料和方法，我的感觉就是无聊、愚蠢，无法引起参与者的互动或思考。短暂的DVD演示涵盖了太多内容，试图在短时间内给观众灌输过多的细节，却很难深入讲解。

不管你是企业还是个人，我要给你一个挑战，那就是设计一个培训计划，通过互动模式让人们融入其中，并引发人们对安全意识的深思。不要只是告诉员工为什么要设定一个又长又复杂的密码，要让他们见识一下破解一个简单的密码是多么地容易。协助客户进行安全意识培训时，有时我会让一名员工上来，在电脑里输入一个他觉得安全的密码。我会在讲密码安全之前这样做，然后在讲的过程中破解这个密码。通常来说，1~2分钟内密码就会被破解，然后我会向大家公开这个被秘密输入的密码。迅速破解密码会给每个人带来巨大的震撼。做几次类似这样的演示之后，员工就会表示现在他们知道密码安全是多么重要了。

当讨论电子邮件中的恶意附件攻击时，我不会向员工展示如何构造一个恶意PDF文件，而是会向他们展示当恶意PDF文件被打开时，受害者和攻击者的电脑中会出现什么。这可以帮助他们理解一个简单的崩溃如何导致一场灾难。

当然，这种教学方式会引起极大的恐慌情绪。尽管这不是我的目的，但也并不是一个可怕的结果，员工会因此记忆深刻。培训的目的是让他们理解不仅要在使用办公室电脑时这样做，也要在应用个人银行账户、家用电脑时这样做，树立起自我安全意识。

希望每个听过我安全演讲或者读过本书的人都审视一下自己是如何使用互联网的，反复使用的密码是否修改过，密码和个人信息是否存储在了不安全的位置，以及用互联网连接了哪些地方。我曾无数次看到有人坐在星巴克咖啡馆里，使用免费的Wi-Fi连接登录银行账户，或进行网络交易。我很想起身朝那个人大叫，告诉他如果有个坏人进入了同样的网络，他的整个生活就会天翻地覆，但是我没有这么做。

我希望读到这里的人也可以想想自己是如何通过电话泄露信息的。骗子和诈骗专家用许多方法窃取老年人、经济困难的人和其他人的信息。打电话仍旧是一个强有效的方式。充分认识厂商、供应商和银行的政策，了解他们会不会通过电话询问信息，可以帮你避免掉入许多陷阱。例如，许多银行在政策中申明他们永远不会通过电话询问社保号码或银行账号。知道这些有助于你保护自己，以免被骗而变得一贫如洗。

培养安全意识是一个持续不断的过程，需要你安排时间去不断地学习。在了解所有这些有用的信息后，你可以用它们来制定一个计划，以保护你的安全。

9.3　充分认识信息的价值

再次回顾一下Defcon第18届安全会议上的社会工程竞赛，我们还可以学到一条宝贵的经验教训，即当认为信息无用或价值很小的时候，人们就不会付出精力对其进行保护。

这一点虽已反复强调，却被无数次证明是正确的，因为很多目标会心甘情愿地泄露有关餐厅、垃圾处理等的信息。你必须意识到自己手中数据的价值，以及社会工程人员所使用的有意贬低数据价值的战术。

在向某人提供信息前，要判断与你通话或者交涉的这个人是否有得到信息的必要。人类天生乐于帮助那些我们认为需要帮助的人。这是社会工程人员操控目标获取有价值信息的主要手段。分析与你进行沟通的人，判断他是否有权获得他想要的信息，可以免去因上当受骗而带来的尴尬和伤害。

举例来说，在Defcon社会工程竞赛中，一位参赛者伪装成一家经营杀毒产品的大公司的顾客，声称遇到了一个严重的问题——电脑不能上网了，他认为这是由于杀毒软件引起的，希望技术支持代表能做一件简单的事帮他解决这个问题——浏览一个网站。

恶意的社会工程人员经常使用这种攻击方式。通过驱使目标访问一个嵌入恶意代码或恶意文件的网站，他能够入侵目标的计算机和网络。在竞赛的案例中，网站本身并未嵌入恶意代码或文件，但需要强调的是，如果这是场真的恶意攻击的话，那就成功了。

参赛者所做的第一次尝试如下："我无法浏览网站了，我想是你们的产品造成的。你能访问一下这个网站吗？看看到底是否是由你们的软件引起的。"

技术支持代表彬彬有礼地回答："先生，我们的产品不会阻止你访问站点，我是否能访问都不能说明问题。"他拒绝了要求。

参赛者没有放弃，几番交谈之后他再次尝试："你说你们的产品不会阻止我访问站点，但是我是安装了你们的软件之后才不能访问的，所以能请你帮我检查一下吗？"

对方再次拒绝了他的要求："先生，对于你的不便我很抱歉，但是我们的产品绝对不会阻止你访问站点，即使我能访问，也不能帮你解决问题。"

似乎请求会以被拒绝而告终，但参赛者打算再做最后一次尝试："先生，如果你能帮我看看网站我会感觉好过些的。请你帮我看看吧，可以吗？"

这个简单的请求让技术支持代表失控了，最后他打开浏览器，访问了那个网站。一开始，他有准确的判断，甚至有一定的安全意识并作出了正确的回答，但是最终还是因为想让"顾客感觉好过些"而接受了他的要求。如果这是一次恶意攻击的话，这将导致公司遭受巨大的损失。

技术支持代表知道对方的要求与对方电话中所说的问题关系并不大。与他一样，你必须判断并分析对方要求的信息是否是他应该得到的，是否与他息息相关。换一个角度看的话，如果参赛者是一名合法的顾客，技术支持代表拒绝了他的要求，最坏的结果是什么？

顾客在被拒绝后一定会表现出不悦，但这并不会改变结果，他所用的产品并非他痛苦的根源。

社会工程人员经常用天气、工作及产品等话题套近乎，然后挖掘想要的信息。这就需要用安全意识策略来应对——针对骗子可能运用的伎俩对员工进行培训，使他们消除因拒绝客户而造成的顾虑。

在一次审计中，我伪装成CFO的助理。呼叫中心的员工通常会担心因拒绝高层的要求而丢掉工作。为什么？因为他们没有接受过适当的培训，不知道拒绝并不会影响他们的工作。同样，应该为员工提供一份方案，告诉他们什么样的信息要求才是合理的。

受过培训并且具有安全意识的人知道，即使是不起眼的信息也可能造成巨大的损失，因而会对信息价值作出准确的判断。如果知道电话那头的人其实并不需要知道自助餐厅的食物供应商是谁，员工就可以作出恰当的回答。如果你是雇主，就应该帮助员工制定应对这些要求的合理回答。大多数情况下，简单的一句回答就能粉碎社会工程人员很多的阴谋，比如回答说："对不起，我没有此项信息。如果你想知道，请联系采购部。"或者"对不起，我没有提供该信息的权利，你可以发送邮件至info@company.com询问。"

之前提到社会工程人员会营造一种氛围，使目标觉得信息并非具有很大的价值，从而吐露这些"不重要的"信息。

再举一个竞赛中的例子，一位参赛者被要求提供身份信息。他伪装成受雇为对方公司做内部审计的人员，当目标想要核实其身份时，他将话题转到了申请表上。参赛者假装对他的一个同事说："简，XX公司的一位先生想知道申请书上的ID号，你能帮忙从比尔桌上拿一下吗？"

当"简"去取参赛者要求的表格时，参赛者开始与目标闲聊。开始时聊的是"得克萨斯州的天气怎么样啊？"、"你去过查理酒吧吗？"诸如此类的话题，可慢慢聊到了"自助餐厅的食物谁管啊？"及"想看看我们做的超酷网站吗？"。

这一切的闲聊都是为了"等待"ID号。社会工程人员每天都会用这种方法。转移注意力与施展魅力是伪装的关键手法。在"闲谈"中透露的信息通常被认为是没有太多价值的，因为人们的注意力根本没有放在那里。如果社会工程人员是在"核实审计信息"时问同样的问题，则对方的态度可能大不相同。但正因为谈话的氛围很友好，信息才能在无意中被泄露。

对抗这种社会工程策略的正确方式就是不管对话的哪个阶段，都要思量你打算透露的信息的价值。在之前的例子中，目标在得到ID之前应该避免闲谈，这样的态度才是恰当的，才可以防止受骗。

要做到这点并不容易，因为工作中的员工，特别是那些面向客户的员工，不可能因为害怕攻击而不透露任何信息，所以仅仅意识到信息的价值并不能阻止攻击的发生。

9.4　及时更新软件

大多数企业都必须向公众和客户发布一些信息。即便就我的业务而言，我也必须公开电话号码、电子邮箱和网站地址，必须收发PDF文件，必须能够与客户、供货商以及厂商在电话中沟通自如。

然而，前面提到的观点表明向公众公开此类信息就意味着公司与隐私的终结。要想公布某些信息，同时又不会造成信息泄露，应该怎么办呢？

不断更新软件。在竞赛中，60%以上的公司还在使用IE6和Adobe Acrobat 8。这一数据真是令人震惊啊。

这两款应用软件中存在大量公开的漏洞。如果知道目标使用这两款软件，就可以对其发起大规模恶意攻击，连入侵检测系统、防火墙以及杀毒软件都无法阻挡。但是你知道有效的防御措施是什么吗？

答案就是更新升级。软件的最新版本通常修补了其安全漏洞，至少是其中的大部分。如果某款软件的安全记录很糟糕，尽量不要使用它，请选择一些漏洞较少的软件。

问题在于公司怠于进行软件更新。IE6是一款相当古老的软件，微软差不多已经停止对它的安全更新支持了。[①]Adobe 8有几十个已经公开的漏洞。这只是我们在比赛中发现的众多软件中的两个。然而，现实是你不得不发布信息，你必须能够自由地告诉别人你的近况。为了减少担忧，你必须确保你和员工都及时更新软件。

在竞赛中的打电话环节，如果某个员工透露了公司使用的是Firefox、Chrome或其他安全浏览器，又或者是FoxIt或最新的Adobe软件，参赛者就将无从下手了。我并不是说那些软件本身不存在任何问题，某些版本的漏洞肯定仍然存在，但是这些软件明显要更安全。获得这部分信息还是有价值的，只是如果没有漏洞可以利用的话，就无法启动下一步的攻击了。

及时更新软件这一提醒可能会遭受巨大的抨击，因为它的工作量很大且耗资巨大。在旧版本软件依然在运行的情况下更改内部规则和方法是十分困难的，这可能会引起内部系统的整体转换。

然而，如果公司在安全方面不遗余力，并且要树立员工的个人安全意识，那么渐渐地这些变化就将成为企业文化的一部分。

---

① 由于IE6的安全问题，微软在2011年初发布了一个有关停止使用IE6的倒计时站点（http://www.ie6countdown.com/），建议用户尽快停止使用IE6。——译者注

9.5 编制参考指南

另一个值得一提的做法是编制参考指南。不要畏缩，我并不是指在A和B同时出现的情形下，员工必须回答X。我的意思是给出指导大纲，帮助员工进行批判性的思考。考虑如下情景。

如果某人声称自己是CEO的手下，要求你提供密码，该如何应对？如果某人没有预约，但外表和行为上看上去像供应商，他要求进入大楼或其他地方，该怎么处理？

在遇到这些情况时，参考指南能帮助员工作出恰当的反应，并且让他们应对自如。举个例子，有一本参考指南如下。

如果某人打来电话声称自己来自管理层办公室，要求你提供一些信息或内部数据，可以按下列步骤操作。

(1) 询问来电者的员工号和姓名。在得到反馈前不要回答任何问题。
(2) 获取身份信息后，询问他需要这些信息的项目号。
(3) 如果(1)和(2)都对答如流，就可以为他提供信息。如果答不上来，要求他的经理发一份邮件给你的经理申请授权，然后终止通话。

类似这样的简单参考指南可以帮助员工明白在考验其安全意识的情况下该说什么以及该做什么。

9.6 学习社会工程审计案例

如果你有过骨折的经历，就知道在恢复时医生会为你安排一些康复理疗。在康复师进行恢复性理疗时，你会进行一些压力测试。这种类型的测试会帮助医生发现你还有哪些薄弱之处需要加强。同样的方法也适用于公司，只不过社会工程审计不是在“损坏”发生后再进行“测试”，而是在入侵破坏发生前所做的测试。

以下小节回答了一些有关社会工程审计的重要问题，并且阐释了如何选择最优秀的审计人员。在深入学习社会工程审计之前，你需要知道审计的真正含义是什么。

9.6.1 理解什么是社会安全审计

社会工程审计的基本定义为，雇用专业安全人员模仿恶意社会工程人员所使用的攻击方式对企业中的人、规章以及物理环境所进行的安全测试。恶意社会工程人员与专业安全审计人员主要有三点不同：

- 通常，专业的安全审计人员会遵循道德与法律上的约束。
- 专业安全审计人员的目的是帮助客户，而不是窃取客户资料、使客户陷入窘境或者伤害客户。
- 专业的安全审计有一定的范围限制，而真正的攻击者则不受这些限制。

专业的安全审计人员会花费大量的时间去分析和收集“目标”或客户的信息，然后使用这些信息展开真实的攻击。在此过程中，专业的安全审计人员会牢记审计的目标。这是很重要的一点，因为他们可能会偏离路线，从而给社会工程人员和目标都带来可怕的后果。明确定义的目标可以避免社会工程审计人员犯这种错。

9.6.2　设立审计目标

专业社会工程人员的行为必须符合道德和伦理，同时又要跨越界线，戴上真正的“黑帽”，暂时担任恶意社会工程人员的角色。这就意味着需要注意他能利用什么手段入侵公司并暴露公司防御的漏洞或弱点，不管手段有多么低下。

在寻找安全漏洞的同时也要考虑员工。在社会工程安全审计中被入侵的公司通常认为解雇那个在攻击中上当的员工就能修正问题，堵住漏洞。客户没有意识到的是，审计过后，在审计中犯过错的员工很可能成为大楼中安全意识最高的人。

专业社会工程人员必须采取额外的防范措施，确保员工不至于被开除。我个人的做法是尽量不透露责任员工的姓名，并且告诉客户审计的关键点不是员工。如果我无能为力，必须透露员工的姓名，那么在报告中我会重点强调，是公司的培训、规章和防御不完善才导致员工“犯错”。

一般的社会工程审计绝不会对员工落井下石，摧毁他的名誉和生活。和审计人员制定审计目标时，我会针对关键方面列出从0到10不等的强度等级：

- 判断员工是否会点击或打开来自陌生人邮件中的链接或文件
- 判断员工是否会登录某个网站，输入个人或业务相关的信息
- 判断通过电话、在工作场所、个人场所（即酒吧、体育馆、托儿所）或面对面的交流可以从员工口中获取多少信息
- 判断办公环境中的锁、摄像头、传感器和门卫的安全等级
- 确定社会工程人员是否有能力构建一个恶意U盘或DVD，并诱导员工把它用在他的工作电脑上

当然，可以审计和测试的领域很多，但是我只能尽可能列出企业所要求审计的目标。我发现，企业通常不知道他们需要什么。审计人员的职责就是为公司介绍多种入侵公司的方法，然后确定他们到底需要测试哪些方面。

明确目标后，还要列出一张表单，注明审计中不应该包含的事项。

9.6.3 审计中的可为与不可为

检测企业是否存在安全漏洞可以采用多种不同的测试方法。运用本书中所有的原则，可以帮助你编制出一个不错的攻击计划。但是在策划攻击时，需要避免以下几点：

- 攻击目标的家人和朋友
- 伪造犯罪或不忠的证据，让目标名誉扫地
- 根据当地的法律，冒充执法人员可能是违法的
- 闯入目标的家或公寓
- 利用目标的风流韵事或窘迫状况进行敲诈

这样的事要应该不惜一切代价来避免，因为它们与审计目标不符，而且让被审计方有种被侵犯的感觉。然而问题来了，如果在审计过程中出现了诸如此类的证据该如何处理。每个审计人员必须自己决定该如何处理，但也不妨参照一些例子。

在一次审计中，审计人员发现一名员工利用公司的高速网络下载色情影片到外部硬盘中。该员工可能因此被解雇，但审计人员并不想这种结果出现，所以只是过去警告他停止该行为。该员工显得很尴尬、沮丧，并且认为审计人员还是会揭发他，于是决定先发制人、倒打一耙，他跑去和老板说审计人员故意在他的电脑中植入了这些让人反感的证据。

当然，在纠纷发生时，审计人员有日志和屏幕截图为证，最后那名员工还是被解雇了。同时，审计人员也受到了批评，因为公司严令禁止该员工的行为，而审计人员在发现证据时没有第一时间报告。

在另一个案例中，审计人员发现有人下载儿童淫秽视频并在互联网上传播，而且在该人的电脑上同时发现了他妻子和孩子的照片。他知道如果揭露此事，可能导致他妻离子散，身陷囹圄，家庭和事业就此毁于一旦。

当地的法律规定，传播儿童淫秽视频是违法的，而且在道德上也属于恶劣行径。审计人员将此事告知公司和权威部门，该男子因此失去了事业、家庭以及自由。

明确列出“不可为”的事项来强化审计活动，能使你在法律与道德的边缘把握住正确的方向。在与身体语言大师乔·纳瓦罗（Joe Navarro）的一次会面中，他就此发表了自己的观点。他指出，除非你是执法者，否则在介入某事件前，必须决定什么可为以及什么不可为。那么审计人员应该在审计中做些什么呢？

- **网络钓鱼攻击** 有针对性的邮件攻击，查看员工是否容易受到恶意邮件攻击。
- **现场伪装攻击** 选择精确且可控的伪装，然后进行电话或面对面攻击，测试员工是否容易上当受骗。
- **引诱** 一种在设法进入目标建筑物或其他设施后的现场攻击，将包含恶意代码和文件的U

盘或DVD光盘放在现场，测试有没有人上钩。

- **尾随**　一种现场攻击，审计人员试图尾随一群公司员工混入大楼。
- **物理安全（红队）**　试图通过物理方式进入办公室，获取公司有价值的资产或信息。

这个清单可以帮助专业审计人员确立指南，列出在审计中什么可为、什么不可为。此外，许多公司还面临的一个最大的问题是，如何挑选优秀的审计人员来完成这些任务。

9.6.4　挑选最好的审计人员

如果你摔断了骨头，病情十分严重，医生告诉你痊愈的机会只有50%，但是如果是非常出色的医生来医治的话，痊愈的几率会增加，你会尽力寻找这样一位医生来医治你吗？当找到他的时候，你会问什么问题？你不想看看他过去的工作成就吗？你会想要一些证据，证明他具有理论和实践能力，能提高你康复的机率。

你可以依照类似的方式，找寻合适的审计人员。在与审计人员交流时，以下问题可供参考。

- **知识**　这个团队是否发表过研究报告、论文、演讲或者其他显示其社会工程知识的材料？他们是否是这个领域的领先者？你不应该安全审计工作交给那些使用过时方法、不能与时俱进的团队。

  不经过一番调查，很难判断一名审计人员和一个审计团队的知识水平。询问他们是否发表过有关安全审计的论文、文章等是一个不错的主意。确保你雇用的团队是这个领域的佼佼者。
- **经验**　客户通常不愿意被指名道姓、大肆宣扬。以我的经验来看，许多客户不愿被放上网站或市场宣传材料中，因为他们会感到尴尬，也怕导致入侵事件的发生。但你可以通过其他方式判断审计人员的经验。不妨询问他曾使用过的方法以及解决方案。

  审计人员在初次会面时通常不会将所有的秘密全盘托出，但是多问一些他进行过的攻击，能帮助你判定他的技能水平。
- **合同**　为审计活动列出框架、形成文件并设定相应的限制，是审计成功的前奏。个人而言，我不喜欢大量的限制，因为大部分恶意社会工程人员根本不讲什么限制。但至少应该就一些规则和不允许的条目达成一致。

  社会工程人员希望对方准许其进行电话录音，在巡查建筑物或交互的过程中进行录像，尤其是在进行物理安全审计时，可以获得从办公场所拿走一些东西的书面许可。审计人员可不想在完成审计任务后得到一张逮捕令或一份起诉书。

  同时要指派紧急联系人，他知道审计一事并且能为审计人员和他的团队担保。如果审计人员陷入法律纠纷，他可以打电话给紧急联系人。没人想在半夜翻垃圾的时候被警察抓去蹲拘留所。有了紧急联系人，就等于有了“免于司法纠纷”的通行证，长久来看这能省去许多麻烦。
- **共识**　运用本书中的原则去寻找优秀的审计人员。与他通电话或见面时，他给你什么感觉？你看到了什么？你有没有感觉他非常专业，他的目的就是要帮助你？

审计团队对自己的描述和业务方式与你的要求一致吗？如果你是雇用审计人员的项目经理，责任都需要你来承担。审计人员也许不想和整个项目组的人见面，因为越少人知道社会工程团队的外貌，对物理安全审计就越有利。所以他们可能只想见项目组中的一到两个人。这就意味着你必须确保审计人员的素质很高，有足够的能力完成任务。

- **时间** 公司在寻找审计人员时经常会犯一大错误，即不给审计人员足够的时间去完成工作。他们认为打几通电话、上一下网站完全可以在一天内完成。尽管这可能是真的，但是如何进行信息收集、计划和目标研究呢？这些都需要花时间的。时间非常重要，但也是把双刃剑——足够的时间有利于审计工作更好地完成，但时间太长会增加成本。管理，但是不要微管理。

这些只是在为公司挑选合适审计队伍时所要考虑的一部分问题。最后，社会工程团队必须让你感到舒服和满意，让你相信他们是真心想帮助你，他们将尽全力保持专业并遵守规则。

9.7 总结

如果不将知识用于实践，它就没有任何价值。

——安东·契诃夫

本书中提供的知识并不是轻轻松松就能掌握的。许多知识揭示了人们的思考和行为方式存在严重的漏洞。当我和我的导师马蒂共同教授安全课程时，他介绍了一种日语名为“shikata ga nai”的负载编码器，意思是“没办法了”，或者粗略翻译为“没希望了”。

我曾想过将这个短语作为本节的引语，但我认为“没希望了”带有强烈的宿命论色彩，也和我通常的价值观相违背。相反，我觉得契诃夫的这句话更符合本书的主题。我曾反复声明，完善技能并在实践中检测这些技能远非掌握知识这么简单。如果你过于害怕本书中提到的内容，就会对人们被攻击的方法感到愤怒，而这只会使你固步自封。我建议你撇下恐惧，从另一个角度认识本书中的内容：换一个心态，鼓励自己学习、思考并理解“坏人”所使用的方法，从而保护自己不受他们的侵害。

我并不是说已经没有任何可怕的了，适度的恐惧还是必要的。保护你的资料、个人信息和身份信息，同时理解“黑客”的思维方式以及本书中提供的信息，可能会对你更为有利。

我希望你能够在生活和工作中运用以下几个小节的内容，如果你负责公司和客户的安全，更应这样做。此外，阅读这部分内容也有助于你保护自身的安全。

9.7.1 社会工程并非总是消极的

我希望读完本书之后，社会工程留给你的印象不是消极的。不仅是黑客、骗子在使用社会工

程策略，医生、心理医师、社会工作者、父母、孩子、老板、员工……每个人都会或多或少地运用社会工程策略。说服就是日常社交生活中经常使用的策略。

要知道社会工程并不总是可怕、黑暗和邪恶的，这对了解社会工程技能的使用方式大有帮助。了解、实践并精通这些技能后，你就能轻松辨别它们是如何被用来攻击他人的了。

你可以在黑暗角落以外的地方分析这些技能。你可以阅读心理学、说服和销售方面的书籍，了解这些技能在该领域是如何被运用的。

9.7.2　收集与组织信息的重要性

我觉得信息收集的重要性再怎么反复强调也不为过。每一个社会工程项目的质量、专业性以及成功正是取决于信息收集的水平。网络是浩瀚无边的信息源。公司会将财务记录、员工的姓名和职位、联系信息、公司的照片、安全规章、合同、厂商和供应商的名字、人们的个人资料等都发布到网上。员工和普通人也会将私人的照片、地址、购买的东西、租约、合同以及喜欢的食物、团队和音乐等信息放到网上。

掌握了大量的信息之后，社会工程人员可以从中挑选出想要使用的那些，并决定使用什么攻击方式去对付目标。接下来，根据收集到的信息，社会工程人员能设计出针对目标最有效的故事情节和伪装。没有本书反复强调的信息收集工作，社会工程活动很可能以失败告终。

举例来说，如果一个专业的审计人员有一项期限为3周的工作，他应该在信息收集上花去一半的时间。不过，专业的审计人员经常采用使用过的伪装去吸引和接近目标。不要养成这个习惯，在信息收集上多花些时间吧。

与信息收集同样重要的是信息的存储与分类，也许可以使用第2章中提到的方法。不但要学会高效地收集信息，还要知道如何存储信息，这对在实战中高效使用信息大有裨益。不能只是简单地把信息存储在一个文档中，要将它们归类并做上标记，这样信息使用起来会更加方便，特别是在电话攻击的时候。

请牢记，社会工程人员表现的好坏取决于他所获得的信息。我曾见过许多社会工程活动最后都功亏一篑，就是因为信息收集得不当或不全。我也见过许多并不是很出色的说服者或不够有魅力的人，最终因为收集了确切的信息而力挽狂澜。

信息是社会工程的关键，如果你只从本书中学到一点，那么一定要是这一点。

9.7.3　谨慎用词

就像9.7节开篇所描述的，没能投入使用的信息毫无价值。你可以收集所有的信息，然后进行组织和分类，但是你也需要高效地利用它们，为此第一步就是组织你将使用的语句。

之前讨论过诱导和铺垫。这是两种非常重要的技巧，我希望你们多练习使用。使用心锚、关键词和话语为目标灌输感情和想法，使他听你的话。铺垫是一种威力强大的技巧，短时间内并不容易掌握，但是熟能生巧。铺垫的好处是你可以随时随地练习，比如在家、在工作中针对孩子、父母和客户进行练习。

不要认为练习就是要求别人做其不愿意做的事情。要用铺垫来激发别人对某个建议或想法抱有更加开放的态度，而不要恶意地使用它。孩子总是这么做，例如你的女儿说："爸爸，我爱你……"过了几秒又说道："我能要那个新玩具吗？"这就是个铺垫的例子，将"目标"置于一种乐意接受的情感状态下。

一旦掌握了铺垫技巧，或者精于使用铺垫，就可以在你的诱导中加以使用。记住，没有人喜欢被审问的感觉。诱导不是模仿警察审问，它应该是流畅地交流，在不知不觉中完成对目标和主题的信息收集。

学习日常交谈中提问的方法和步骤，不仅能增强社会工程技能，也能提高交流水平。人们喜欢他人关注其生活和工作。将这一技能用于好的方面，可以强化你的社会工程能力。

我有一个好朋友，她能让人们告诉她任何事，这是非常不寻常的。完全陌生的人也会这样，在谈话的最后他们还会奇怪："我真不知道为什么会和你说这些事……"她并不是一个社会工程人员，也不做安全方面的工作，但她是个优秀的诱导者。

掌握铺垫和诱导技能也能提高斟酌言语的能力。这些技能能让你以更加智慧、不那么冒昧的方式寻找和收集信息。

9.7.4 巧妙伪装

记住，好的伪装并不是纯粹的说谎和编故事，而是在短时间内变身成为所伪装的角色。你的一切，包括想法、动作、说话方式和动机，都应该体现所伪装角色的特征。如果你做得足够好，就会取得目标的信任。

另一点要牢记的是，伪装并不只是运用在社会工程中，在生活中也会用到。想象一下这个场景：你刚刚和配偶发生了一番争吵，上班时你不想让任何人知道家里发生了不愉快，所以当同事跟你打招呼说"嘿，吉姆，今天好吗？"时，你的回答会是"很好"。

这与事实正好相反，但你怎样做才能使之变得可信呢？对人微笑，通过手势和肢体语言传达出自信。如果你非常紧张自己的隐私，不想与同事分享太多，你甚至会编造出一个"欢乐的故事"，证明你的生活有多么美好。

这只是一种情况，可以说人们一直在运用伪装。任何时候，只要你试图向人们展示与事实不符的表象，你"编造的故事"就是一种伪装。当然，大多数人不善于此，常常露出破绽，但是在

生活和工作中注意这些情况，能为分析伪装打下基础。

分析这些情景能帮助你找出伪装中需要提高的地方，有助于你掌握这项非常有用的技能。

9.7.5　练习解读表情

我想我可以用几周的时间来谈论微表情。这个话题让我着迷，让我觉得人类有一种内置的机制，可以暴露内心最深处、最黑暗的感觉，而且大部分人都控制不了它。我们的情绪会引起某些肌肉的收缩，从而呈现持续时间为几毫秒的表情，这只是造物主惊人的创造。但是学习注意、读懂并利用这些表情来操纵他人才真正是一门惊人的学问。

练习第5章中讨论的再现微表情的方法。练习的过程中，要注意微表情让你产生的情绪。练习这些表情能帮你读懂其他人的表情。

在练习的过程中，不仅要重视解读他人的微表情，也要注意控制自己的微表情，防止他人读懂你内心的想法。请牢记，解读他人的表情是一种不错的技能，但是掌握自己的微表情、肢体语言和语调是一种更厉害的技能，此技能可以提高你在安全实践和个人社交方面的水平。掌握这些技能后，你就能渐渐体会如何运用第5章中的主要概念之一——人类思维缓冲区溢出。从一个更高的层面来看，人类思维的工作方式很像软件，它也像软件那样可以被模糊测试、检测和颠覆。请重读5.6节，确保你已充分理解该节中提出的原则。

9.7.6　操纵与影响

操纵和影响是社会交往的两个重要方面，会对你接触的人产生巨大的影响。出于这个原因，在使用第6章中的信息时需要特别注意。学会怎样说服和操纵他人对社会工程活动的成败至关重要。每天，人们都在尝试操纵和说服他人去采取某些行动，其中某些不好的行为会给他人造成金钱损失，甚至是个人自由和身份信息的丧失。

将那些场景作为教学工具。分析营销人员、心理学家、律师、教师甚至是同事操纵你的方法。从中挑出你能学习的几点，为你所用。

记住，说服并不总是消极的，它不一定意味着让人们去做他们不愿意做的事情。说服也有积极的影响，很多时候积极的说服更难办到。如果你掌握了这些技巧，并用之来帮助人们维护安全，那当遇到其他人使用消极说服策略时，你可能一眼就会识别出来。

9.7.7　警惕恶意策略

充分了解攻击者会使用什么样的策略可以让你免于入侵之害。专业的审计人员可以使用这些策略培训客户如何发现可能的攻击迹象。请保持警惕，谨慎找出这些策略的应用实例。

例如，“坏人”使用的一种策略就是乱中取胜、浑水摸鱼。当飞机撞上世贸大厦时、当海地遭遇地震袭击时、当亚洲碰上海啸灾难时，很多人因此而丧生，其他人的生活、心灵和感情则遭到了沉重的打击。在这些人们脆弱无助的时候，坏家伙们就会出现并发起攻击。

举个例子，我读过一篇有关狮子在野外捕猎的文章。文章中说，狮子会在一群猎物中制造混乱，然后选择一个受害者。它会朝地面咆哮，而不是向着猎物或者天空，为什么呢？这是因为巨大而令人恐惧的咆哮声会在地面产生混响，猎物们会很迷茫，不知道狮子究竟是从哪个方向来的。结果有些猎物会向左逃窜，有些则会向右，惊慌之中丢下那些年幼、年迈、体弱和未发育成熟的群成员。

这与恶意社会工程人员的手法大同小异。他们以“咆哮”的方式引起或增加混乱。他们利用那些帮助寻找在灾难中逝去亲人的网站，或者声称自己在灾难中失去了家人和朋友。当情感被迷惑时，“目标”就不能识破攻击了。

毫无经验和技术不成熟的受害者首先会给出少量信息，攻击者会据此找到攻击入口。接下来攻击者会发动进一步的攻击，而这些攻击会更加邪恶和残酷。

请留意这些情况，保护你的客户和自己不成为他们的受害者。同样，将这些情况作为课程来学习，分析其中所使用的方法，观察它们是否奏效。如此一来可锻炼你的能力，提高对潜在威胁的警惕性。

不幸的是，狮子与社会工程人员的差异（除了明显的差异外）是社会工程人员从来不会大声嘶吼，他不会在那里大喊：“我要捕猎，你们快跑！”恶意的社会工程人员总是悄无声息地，每年将成千上万的人引入他们部署的精妙的攻击圈套中。

9.7.8 利用你的恐惧

如果本章内容或多或少给你带来了一些恐惧感，我会说“很好”。你需要恐惧，因为适当的恐惧能拯救你的生命，至少可以保护你的身份信息和公司。

积极地利用恐惧，切忌生气和消沉。制定一个改变自我的计划，然后培训自己、家人和员工，学会观察、提防和防御这些攻击。下决心一定不能让自己或公司受到攻击，然后尽量做到这一点。

本书的宗旨可以归结为“安全之本在于教育”。人性攻击是一门艺术，而社会工程是科学、艺术和技能的综合体。如果各种因素搭配得当，结果就是“shikata ga nai”（没办法）。

每年入侵事件给企业造成数百万美元的损失，其中绝大多数的入侵事件都来自社会工程攻击。然而，一种普遍的现象是，当我们希望在渗透测试服务中加入社会工程审计时，他们却拒绝了。

为什么？

企业通常害怕改变。在专业实践中，我无数次地听到聪明且成功的老板这样说道：“我们不需要

社会工程审计，我们的员工不会落入那些圈套的。”然后，在渗透测试中我们会通过打电话（已被准许）套取信息，之后当我们在报告中披露这些信息时，他们会对套取信息竟然如此简单惊叹不已。

在各种企业中，各级员工的安全意识并没有太大的不同。当渗透测试之后，我们和公司说起我们组织的一个安全意识培训项目时，许多人告诉我们，公司从未对呼叫中心和技术支持部门的员工做过正式、认真的培训。而这些部门常常是社会工程攻击的首选目标。

这正是我所说的问题的关键所在。通过培训建立安全意识并非是一句口号，它必须成为一项使命。只有公司以及公司的员工将安全当做自己的事情来认真对待，这个问题才能真正得到解决。与此同时，那些带着严肃态度阅读本书、渴望窥探社会黑暗角落的人，一定能够提高技能，从而使其家庭、自身和公司更加安全。

当“狮子咆哮”时，请成为那个带领大家逃亡的人吧。做一个知道如何应对和防御攻击的榜样。

只要花费足够的时间和努力，可以对任何人进行社会工程。千真万确，事实就是那么恐怖。但是这并不意味着没有希望，它意味着你的工作就是让恶意社会工程变得极为困难且耗时，这样大多数黑客就会放弃，转去摘取那些“低挂的果实”或追逐被落下的猎物。我知道这听起来很冷酷。如果大家都能阅读这本书并因此作出巨大的改变，我将十分欣慰，因为这样公司才会做到真正安全。然而，那就不是我们所处的世界了。

此番言论提出了一个非常严肃的问题。如果真的没有希望做得彻底安全，公司、员工、家庭以及我们每个人要如何来防护这个巨大的漏洞呢？只有公司开始意识到自己很容易被社会工程攻击，他们才会进行个人教育，了解攻击方法和保持警惕，并不断提醒他人。只有这样，我们才有希望在攻击前做好防御准备，或者至少不会后知后觉。

9.8　小结

作为全书的总结，我希望本书为你打开了认识社会工程世界的一扇窗，希望它能帮助你留意潜在的恶意攻击，帮助你对潜在的灾难形成并保持适度的恐惧。

同时，我也希望本书能帮助你保护你的公司、家庭、孩子、投资和生活。希望本书中的信息能让你体会到实现绝对安全和全面保护不是一件完全不可能的事。

我的导师马蒂·阿[redacted]人通常会得逞的原因在于他们付出了足够的时间和精力并且具有明确[redacted]。相反，也不要让过多的恐惧阻止你享受生活。

我希望通过应用本[redacted]高自己读懂他人的能力，并能和周围的人进行更加有效的沟通。不要[redacted]中，要运用于生活的各个方面，这会改变你的生活。社会工程是一门[redacted]！