反黑
教学基地

VIP精品指南
特别奉献

反黑风暴

黑客社会工程学攻防演练

DVD
超大容量 超值享受

- 理论+实战 图文+视频=让读者不会也会
- 任务驱动式讲解，揭秘多种黑客攻击手法
- 攻防互参，全面确保用户网络安全
- 挑战自我，享受黑客攻防的乐趣

武新华 李 伟 等编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

反黑风暴

黑客社会工程学攻防演练

武新华　李　伟　等编著

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

本书由浅入深、图文并茂地再现了黑客社会工程学攻防演练的全过程，内容涵盖：全面认识社会工程学、无所不能的信息搜索、扫描工具应用实战、黑客常用入侵工具、商业窃密常用伎俩、诠释黑客的攻击方式、诠释网络钓鱼攻击方式、跨网站攻击技术、刨根问底挖掘用户隐私、真假莫辨的防范欺骗攻击、形形色色的反侦查技术、安全威胁防御技术等一些应用技巧，并通过一些综合应用案例，向读者讲解了黑客与反黑客工具多种应用的全面技术。

本书内容丰富全面，图文并茂，深入浅出，面向广大网络爱好者，同时可作为一本速查手册，也适用于网络安全从业人员及网络管理者。

图书在版编目（CIP）数据

黑客社会工程学攻防演练 / 武新华等编著. —北京：电子工业出版社，2011.1
（反黑风暴）
ISBN 978-7-121-12575-1

Ⅰ. ①黑… Ⅱ. ①武… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2010）第 247380 号

策划编辑：郭鹏飞
责任编辑：鄂卫华
印　　刷：中国电影出版社印刷厂
装　　订：中国电影出版社印刷厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×1092　1/16　印张：21　字数：538 千字
印　　次：2011 年 1 月第 1 次印刷
定　　价：48.00 元（含光盘 1 张）

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前 言 FREFACE

社会工程学（Social Engineering）是一种通过对受害者心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱采取诸如欺骗、伤害等危害手段，获取自身利益的手法，近年来已呈迅速上升甚至滥用的趋势。其实，社会工程学并不能等同于一般的欺骗手法，社会工程学尤其复杂，即使自认为最警惕、最小心的人，一样可能会被高明的社会工程学手段损害利益。很多社会工程学攻击是很复杂的，包括周详的计划，且综合运用了相当的技巧。但也可以发现，一些熟练的社会工程学攻击者经常可只用简单的方法达到其目的，直接进行询问获得所需信息常常是行之有效的。

社会工程学技术则将黑客入侵进行了最大化，不仅能利用系统的弱点进行入侵，还能通过人性的弱点进行入侵，当这两种技术融为一体时，将根本不可能有安全的系统存在，技术高超的社会工程学师最终可以击溃几乎所有的安全防线。

关于本书

本书以配图、图释、标注、指引线框等丰富的图解手段，再辅以浅显易懂的语言，不但介绍了黑客攻击计算机的一般方法、步骤，以及所使用的工具，而且详细讲述了防护黑客攻击的方法，可使读者在了解基本网络安全知识的前提下，轻松而快速地掌握基本的反黑知识、工具和修复技巧，在遇到别有用心者入侵时能够不再茫然无措。

本书内容

本书讲述的具体内容有：全面认识社会工程学、无所不能的信息搜索、扫描工具应用实战、黑客常用入侵工具、商业窃密常用伎俩、诠释黑客的攻击方式、诠释网络钓鱼攻击方式、跨网站攻击技术、刨根问底挖掘用户隐私、真假莫辨的防范欺骗攻击、形形色色的反侦查技术、安全威胁防御技术等，使得读者可以对黑客社会工程学攻击与防护等具有代表性的技术有一个全面认识。

此外，本书从黑客社会工程学攻击与防护应用角度给出了相对独立的内容的论述，使读者可对如何构建一个实用的黑客社会工程学攻击与防范体系有一个基本概念和思路，并可为读者提供几种典型行业的安全防护系统建设方案，以供参考和借鉴。

本书特色

本书以情景教学、案例驱动与任务进阶为鲜明特色，在书中可以看到一个个生动的情景案例。通过完成一个个实践任务，读者可以轻松掌握各种知识点，在不知不觉中快速提升实战技能。

- 高效模式：全程图解模式可彻底克服攻防操作的学习障碍。
- 内容合理：精选入门读者最迫切需要掌握的知识点，构成一个实用、够用、完整的知

识体系。

- 举一反三：初学者学习中习惯机械记忆，不求甚解，力求通过一个知识点的讲解，让读者彻底理解和掌握类似场合的应对思路。

本书将向读者展示鲜为人知的社会工程学攻击内幕，由浅入深、全面讲解社会工程学攻击的具体实施与细节，让读者清楚地知晓他们的攻击伎俩，所提供案例可形象地认识到所带来的威胁并提供了完整的解决方案，可使读者免受信息伤害，并使企业知道如何通过培训及相关防护来阻止社会工程学的攻击。

本书适合人群

本书将围绕个人及企业的信息威胁进行完整的部署，包括信息跟踪、隐私挖掘、商业窃密、钓鱼攻击、心理学攻击、反侦查对抗等前沿的信息安全，旨在帮助人们及政府、商业机构认识到社会工程学攻击所带来的威胁，以使个人及机构重要机密免遭窃取或被入侵的危险。

本书作为一本面向广大网络爱好者的速查手册，适合于如下读者学习使用：

- 电脑初、中级用户
- 电脑爱好者、提高者
- 各行各业需要网络防护的人员
- 网络管理人员
- 大中专院校相关学生

本书作者

本书作者团队长期从事网络安全管理工作，都具有较强的实践操作能力及一线拼杀经验，可带领广大醉心技术者穿越迷雾，把黑客们的伎俩看清楚。本书的编写情况是：杨平负责第 1 章，王英英负责第 2 章，陈艳艳负责第 3、4、5 章，安向东负责第 6 章，李伟负责第 7 章，郑静负责第 8 章，王肖苗负责第 9 章，吕志华负责第 10 章，张晓新负责第 11 章，孙世宁负责第 12 章，最后由武新华统审全稿。

需要提醒大家的是：根据国家有关法律规定，任何利用黑客技术攻击他人的行为都属于违法行为，希望读者在阅读本书后不要使用本书中介绍的黑客技术对别人进行攻击，否则后果自负，切记切记！

我们的联系方式：zhangbg@phei.com.cn

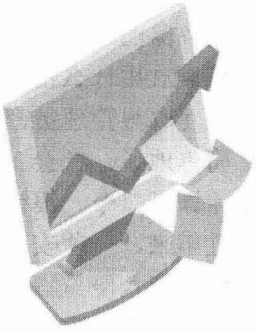
编著者

2010 年 10 月

目 录 CONTENTS

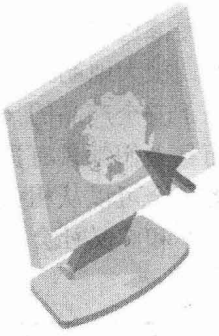
第1章

全面认识社会工程学



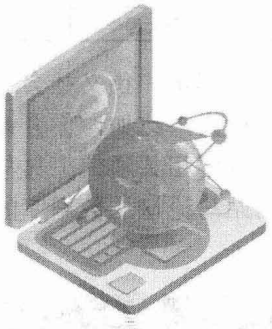
重点提示：

- 什么是社会工程学
- 生活中的社会工程学攻击案例
- 防范社会工程学



传统的计算机攻击者在系统入侵的环境下存在很多的局限性，而新的社会工程学攻击则将充分发挥其优势，通过利用人为的漏洞缺陷来取欺骗手段来获取系统控制权。

这种攻击表面上是难以察觉的，不需要与受害者目标进行面对面的交流，不会在系统留下任何可被追查的日志记录。为了更好地认识社会工程学攻击，本章将介绍生活中常见的社会工程学攻击安全，以及防范社会工程学攻击的方法。



社会工程学理论是关于建立通过自然的、社会的和制度上的途径并特别强调根据现实的双向计划和设计经验来一步一步地解决各种社会问题。严格来说社会工程学不是一门科学，而是一门欺骗的艺术和窍门的方法。它利用人的弱点，以顺从你的意愿、满足你的欲望的方式让你上当。

1.1 什么是社会工程学

社会工程学是一种攻击行为，攻击者利用人际关系的互动性所发出的攻击：通常攻击者当没有办法通过物理入侵直接取得所需要的资料时，就会通过电子邮件或者电话对所需要的资料进行骗取，再利用这些资料获取主机的权限以达到其本身的目的。

1.1.1 社会工程学攻击概述

现实社会中的骗子欺骗伎俩形形色色，随着网络和通信技术的进步，其骗术花样也不断翻新，令人防不胜防。例如，有的人因试图获得手机中奖短信中的奖品、奖金而上当受骗，有的人轻信骗子打来的亲人发生车祸、急病住院等电话后被骗取钱财等。这些现实社会中的欺骗手段一旦被黑客延伸应用到攻击网络系统，就发展成为社会工程学攻击。

社会工程学也是最近黑客界流行的一种入侵方式。社会工程学攻击主要采取非常规手段取得服务器的权限或网站的权限，比如搜集管理员的各种信息，如管理员喜欢进哪些网站，管理员喜欢用什么密码，在管理员进入的网站里面挂网页木马，破解管理员常进网站的数据库，从而取得管理员密码。

简单地说，社会工程学攻击就是利用人们的心理弱点，骗取用户的信任，获取机密信息（如计算机口令、银行账户信息）等不公开资料，为黑客攻击和病毒感染创造有利条件。

近年来，一些安全杂志上相继出现了相关社会工程学攻击的文章，黑客们也逐渐将目光从传统系统入侵与脚本攻击的热潮中转向社会工程学攻击上。

社会工程学攻击之所以让大多数的黑客看到曙光，通过信息搜索与社交直接索取密码，使得入侵渗透更加容易。究其原因，还是由于网络管理人员的管理问题。网络管理人员的素质高低，极大地制约了整个网络的安全程度。

由于安全产品的技术越来越完善，使用这些技术的人，就成为整个环节上最为脆弱的部分。而且人们都具有贪婪、自私、好奇、信任等心理弱点，因此，通过恰当的方法和方式，入侵者完全可以从相关人员那里获取入侵所需信息。社会工程学攻击可以分为两种：狭义社会工程学和广义社会工程学。它们之间的区别可以参考表 1-1。

表 1-1 社会工程学

社会工程学	是否有计划、针对性获取信息	是否单纯通过网络搜索信息	是否需要知道相关术语信息
狭义社会工程学	否	是	否
广义社会工程学	是	否	是

其实，狭义社会工程学攻击与广义社会工程学攻击最明显的区别是会与受害者进行交互式行为，比如，你会设置一个陷阱使对方跳入，或是伪造一封来自内部的虚假电子邮件，或是利用相关通信工具与他们交流获取敏感信息。真正的社会工程学师是不会碰运气乱去下载网站与论坛的数据库的，他们清楚地知道自己需要什么样的信息，并且应该怎么样去做，从

搜集的信息中分析出有用的信息，并与受害者进行互动行为，这样才称之为社会工程学。

1.1.2 无法忽视的非传统信息安全

社会工程学是非传统的信息安全，它是一种利用受害者本能反应、好奇心、信任、贪婪等心理陷阱采取诸如欺骗、伤害等危害手段，取得自身利益的手法，而不是利用系统漏洞入侵的。普通用户经常会安装硬件防火墙、入侵监测系统（IDS）、虚拟专用网络，或是安全软件产品，但这并不能保障安全。

社会工程学师只需拨打一个电话，使用专业的术语，报出内部人员使用的ID，让一个系统管理员登录系统，并将其传真过来即可窃取信息。事实上，很多安全行为就是出现在骗取内部人员（信息系统管理、使用、维护人员等）的信任上，从而轻松绕过所有技术上的保护。

信任是一切安全的基础，对于保护与审核的信任，通常被认为是整个安全链条中最薄弱的一环。为规避安全风险，技术专家精心设计的安全解决方案，却很少重视和解决最大的安全漏洞——人为因素。无论是在现实世界还是在虚拟的网络空间，任何一个可以访问系统的人，都有可能构成潜在的安全风险与威胁。

社会工程学较之其他黑客攻击复杂，即使自认为最警惕、最小心的人，一样会受到高明的社会工程学手段的损害。因为“社会工程学”主导着非传统信息安全，所以通过对它的研究可以提高应对非传统信息安全事件的能力。非传统信息安全是传统信息安全的延伸，主张信息安全防护采取“先发制人”的战略，突破传统信息安全在观念上的指导性被动，主动地分析人的心理弱点，提高人们对欺骗的警觉，同时改进技术体系和管理体制存在的不足，从而改变信息安全“头痛医头，脚痛医脚”的现状。

社会工程学无处不在，在商业交易谈判和司法等领域都存在。其实在生活中，我们也常常在无意中使用，只是浑然不觉而已。比如，当遇到问题时，会知道应该寻找有决定权的人来解决，并让周遭的人帮助解决。这其实也是社会工程学。社会工程学是一把双刃剑，既有好的一方面，也有坏的一方面。

1.1.3 攻击信息拥有者

信息安全的本质是信息拥有者与攻击者间的战斗。信息拥有者是无价的信息宝藏，攻击者大可不必因为一个口令而把大量精力花费在系统入侵与破解上，直接针对拥有者的脆弱性开始进行攻击，可以避免一些不该发生的事，比如口令变、系统补丁升级等。

一般来说，经验丰富的黑客攻击者往往缺乏人际交往的知识经验与技巧，但社会工程学攻击会打破这种格局。在大多数情况下，成功的社会工程学师都有着很强的人际交往能力。他们有魅力、讲礼貌、讨人喜欢，并具有快速建立起可亲、可信感的特点。

一个经验丰富的社会工程学师，使用他自己的战略、战术，几乎能够接近任何他感兴趣的信息。他会开始用大量的时间研究非传统信息安全，庞大的商业价格是吸引他的条件，这种有效的信息入侵对他非常有诱惑力。

社会工程学攻击还有一个受黑客们欢迎的原因，那就是中国企业盲目追求商业利益最大化，他们不注重建立企业品牌，忽略对员工进行安全培训投资。比如，一个社会工程学使用者想从一家信用卡公司获取一些情报，但又没有相关的证明他可以合法地从这家公司拿到这些情报。那么，他就可以利用社会工程学，从和这家信用卡公司相关的银行搜集相关的信息从而达到目的。例如，这家银行从信用卡公司取得信息需要什么文件或者ID号码证明，又或

者是经常与信用卡公司进行业务联系的职员的姓名等，攻击者只要通过某些途径从这些毫无任何价值观念的企业内部员工的口中得到这些信息，即可成功窃取信息。而没有安全威胁意识的企业会在这个问题上栽一个大跟头。

因此，从现阶段来说，信息拥有者是社会工程学攻击的主要目标，也是无法忽视的脆弱点，要防止攻击者从信息拥有者身上窃取信息，必须加强对他们进行安全培训投资。

1.1.4 常见社会工程学手段

现代的网络纷繁复杂，病毒、木马、垃圾邮件接踵而至，给网络安全带来了很大的冲击。同时，利用社会工程学的攻击手段日趋成熟，其技术含量也越来越高。社会工程学攻击在实施之前必须掌握心理学、人际关系、行为学等知识与技能，以便搜集和掌握实施入侵行为所需要的资料和信息。下面介绍几种常见的社会工程学攻击手段。

1. 环境渗透

对特定的环境进行渗透，是社会工程学为了获得所需的情报或敏感信息经常采用的手段之一。社会工程学攻击者通过观察目标对电子邮件的响应速度、重视程度以及可能提供的相关资料，比如一个人的姓名、生日、ID 电话号码、管理员的 IP 地址、电子邮箱等，通过这些搜集信息来判断目标的网络构架或系统密码的大致内容，从而获取情报。

2. 引诱

网上冲浪经常碰到中奖、免费赠送等内容的电子邮件或网页，诱惑用户进入该页面运行下载程序，或要求填写账户和口令以便“验证”身份，利用人们疏于防范的心理引诱用户，这通常是黑客早已设好的圈套。

3. 伪装

目前流行的网络钓鱼事件以及更早以前的求职信病毒、圣诞节贺卡，都是利用电子邮件和伪造的 Web 站点来进行诈骗活动的。有调查显示，在所有接触诈骗信息的用户中，有高达 5%的人都会对这些骗局做出响应。

4. 说服

说服是对信息安全危害较大的一种社会工程学攻击方法，它要求目标内部人员与攻击者达成某种一致，为攻击提供各种便利条件。个人的说服力是一种使某人配合或顺从攻击者意图的有力手段，特别地，当目标的利益与攻击者的利益没有冲突，甚至与攻击者的利益一致时，这种手段就会非常有效。如果目标内部人员已经心存不满甚至有了报复的念头，那么配合就很容易达成，他甚至会成为攻击者的助手，帮助攻击者获得意想不到的情报或数据。

攻击者在施行攻击时，经常会采用维修人员、技术支持人员、经理、可信的第三方人员，或者是企业同事等角色，这点在一个大公司是不难实现的。

因为每人不可能都认识公司中的每个人员，而身份标识是可以伪造的，这些角色中的大多数都具有一定的权利，让别人会不由自主地去巴结。大多数的雇员都想讨好老板，所以他们会点头哈腰地对那些有权力的人提供他们所需要的信息。

5. 恐吓

社会工程学师常常利用人们对安全、漏洞、病毒、木马、黑客等内容的敏感性，以权威机构的身份出现，散布安全警告、系统风险之类的信息，使用危言耸听的伎俩恐吓、欺骗计

算机用户，并声称如果不按照他们的要求去做，会造成非常严重的危害或损失。

6. 恭维

高明的黑客精通心理学、人际关系学、行为学等社会工程学方面的知识与技能，善于利用人们的本能反应、好奇心、盲目信任、贪婪等人性弱点设置陷阱，实施欺骗，控制他人意志为己服务。他们通常十分友善，很讲究说话的艺术，知道如何借助机会去迎合人，投其所好，使多数人友善地做出回应，乐意与他们继续合作。

7. 反向社会工程学

反向社会工程学是指攻击者通过技术或者非技术的手段给网络或者计算机应用制造“问题”，使其公司员工深信，诱使工作人员或网络管理人员透露或者泄漏攻击者需要获取的信息。这种方法比较隐蔽，很难发现，危害特别大，不容易防范。

1.2 生活中的社会工程学攻击案例

社会工程学作为信息时代发展出来的一门“欺骗的艺术”，在现今不论是虚拟的网络空间还是现实的日常生活场景，凡是涉及信息安全的方面，无不有社会工程学的应用。

本节将介绍几种生活中常见的有关社会工程学攻击的安全，希望大家能够进一步地了解社会工程学，并提高警惕。

1.2.1 巧妙地获取用户的手机号码

社会工程学就是一种与计算机技术相结合的行骗过程，而社会工程学的实施者，则可以看作是一个精通计算机的超级骗子。

下面通过一个虚拟的例子，说明如何通过社会工程学获取用户的手机号码。

假设攻击者试图入侵某个公司的内部办公系统，但无法破解管理员的登录密码。可先利用一些手段获得管理员的手机号，再想办法得到管理员的登录密码即可。

首先，打开公司的网站，在网站首页的左上角有一个“内部办公系统登录”链接，在该链接下有一个快速登录口，在“登录名”和“密码”文本框中输入相应的内容，即可进入该公司的内部办公系统，如图 1-1 所示。

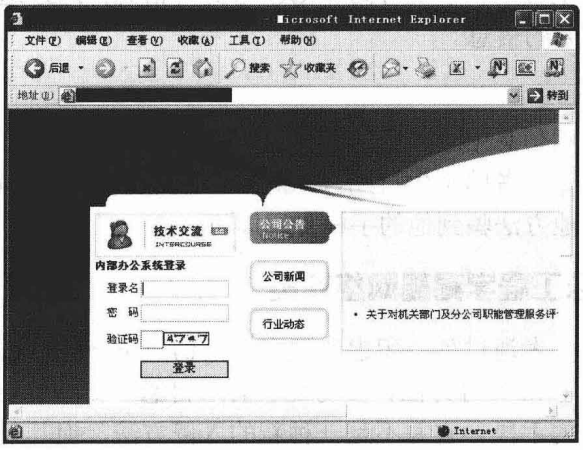


图 1-1 进入公司首页

或者直接单击“内部办公系统登录”链接，在打开的“内部办公系统”页面中可直接登录进入公司的内部办公系统，如图 1-2 所示。现在要做的就是获得管理员的登录密码，但可以先从管理员的手机号码上入手，得到他的手机号码后，再想办法获取登录密码。

图 1-2 内部办公系统登录页面

攻击者要想成功获得管理员的手机号，需要按照下面的方法进行。

1. 查询用户网络信息

攻击者可以使用社会工程学，详细地搜集管理员在网上的各种信息。比如，管理员常用的邮箱，通常来说，经常在网络上活动的管理员，当它们注册一些论坛或博客站点服务等，都会用到邮箱。因此，攻击者可以将这些邮箱地址作为关键字，在百度或 Google 等搜索引擎中搜索相关信息。

从搜索结果中可以看到许多有用的信息，如管理员注册了哪些论坛。同样，可以用管理员的其他邮箱、QQ 号和 MSN 地址等信息为关键字在网上进行搜索，也可以搜索到不少信息。

另外，还可以在当下流行的“校内网”和“校友网”等社交类型的网络上搜索更详细的信息，以获得用户的真实资料等信息。在这两个网站上注册的用户通常都会在注册信息中填写真实的家庭住址、出生日期、手机号码和 QQ 号码等信息，通过这种方式可以了解到管理员的手机号码或其他重要的信息。

2. 获得手机号码

如果从网络中的搜索信息中可以直接得到目标的手机号码，就可以利用这个手机号码进行欺骗。如果只得到了目标者的出生日期、家庭住址或 QQ 号码，则可以先将管理员的 QQ 号加为好友，再通过其他方法骗到他的手机号码即可。

1.2.2 利用社会工程学揭秘网络钓鱼

网络钓鱼就是指入侵者通过处心积虑的技术手段伪造出一些以假乱真的网站和诱惑受害者根据指定方法操作的 E-mail 等方法，使得受害者“自愿”交出重要信息或被窃取重要信息（例如银行账户密码）的手段。它并不是一种新的入侵方法，但其危害范围却在逐渐扩大，并成为近期威胁网络安全的最大危害之一。