HACKER

黑客揭秘与反黑实战

人人都要懂社会工程学

新阅文化 编著

赠送资源

- 140 个 Windows 系统常用快捷键大全
- Windows 文件管理手册
- Windows 系统安全与维护手册
- Windows 硬件管理手册
- 74 个教学视频（扫描书中二维码进行观看）

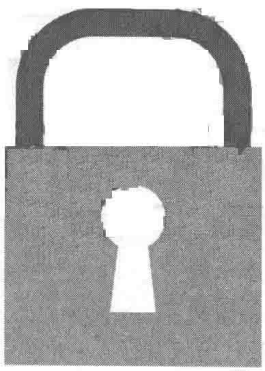
中国工信出版集团 人民邮电出版社 POSTS & TELECOM PRESS

非外借

黑客揭秘与反黑实战

人人都要懂社会工程学

新阅文化　编著



人民邮电出版社
北　京

图书在版编目（CIP）数据

黑客揭秘与反黑实战 : 人人都要懂社会工程学 / 新阅文化编著. -- 北京 : 人民邮电出版社, 2018.12
ISBN 978-7-115-49582-2

Ⅰ. ①黑… Ⅱ. ①新… Ⅲ. ①黑客－网络防御 Ⅳ. ①TP393.081

中国版本图书馆CIP数据核字(2018)第231766号

内 容 提 要

本书全面详细地介绍个人计算机的网络安全反黑技术，并提供大量实用工具和操作案例。本书从社会工程学角度出发，首先讲解了信息的搜索，然后说明如何防止黑客挖掘用户隐私；在介绍如何防范商业间谍窃密时，列举了黑客惯用的手段，如黑客攻击、跨站攻击、欺骗攻击、反侦查技术等；对日常生活中所面临的网络钓鱼风险，网上冲浪、社交媒体中存在的安全威胁，以及电信诈骗等内容进行了详细讲解；最后讲解了网络安全铁律及扫描工具和防范黑客常用的入侵工具。

本书图文并茂，通俗易懂，适用于黑客及网络安全技术初学者、爱好者，也适用于企事业单位从事网络安全与维护的各类读者。

◆ 编　　著　新阅文化
责任编辑　李永涛
责任印制　马振武

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
山东百润本色印刷有限公司印刷

◆ 开本：787×1092　1/16
印张：21.5
字数：421 千字　　2018 年 12 月第 1 版
印数：1－3 000 册　　2018 年 12 月山东第 1 次印刷

定价：59.80 元

读者服务热线：(010)81055410　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广登字 20170147 号

计算机是现代信息社会的重要标志，掌握一定的计算机知识已经成为信息化时代对每个人的要求。但是随着社会的信息化发展，黑客也就随之产生，在我们每天上网的过程中，可能就有黑客正在浏览计算机的某些数据。他们入侵成功之后，便会对其中的程序和数据进行破坏。然而当我们发现时，再想亡羊补牢，却为时已晚。

本书内容

为了使读者能够在最短时间内轻松掌握计算机防护方面的基本知识，快速解决实际生活中遇到的问题，提高信息化社会的信息安全意识，我们特意为广大读者朋友定制了这套《黑客揭秘与反黑实战》图书。本书作为指导初学者快速掌握黑客攻防知识的入门书籍，从社会工程学角度出发，帮助初学者了解黑客利用社会工程学进行攻击的常用手段，找到相应的防范方法，确保个人计算机与网络的安全。

本书特色

（1）从实例出发，讲解全面，可轻松入门，能够快速打通初学者学习的重要关卡。

（2）真正以图来解释每一步操作过程，通俗易懂，阅读轻松。

（3）学习目的性、指向性强，通过最新黑客技术盘点，让读者实现“先下手为强”。

读者对象

本书作为一本面向广大网络安全反黑初学者的速查手册，适合以下读者学习使用。

（1）网络安全初学者、爱好者。

（2）需要获取数据保护的日常办公人员。

（3）网吧工作人员、企业网络管理人员。

（4）喜欢研究黑客技术的爱好者。

（5）大中专院校相关专业的学生。

（6）培训班师生。

本书主要由褚姣姣、张婷婷、朱琳、李阳、沈秋洽、张晓宇编写。我们虽满腔热情，但由于水平有限，书中难免存在不足、遗漏之处，希望大家本着共同探讨、共同进步的平和心态来阅读此书，敬请广大读者批评指正。

最后，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，希望广大读者在阅读本书后不要使用书中介绍的黑客技术对别人进行攻击，否则后果自负。切记勿忘！

新阅文化

2018.7

目录 CONTENTS

第 15 章　防范黑客常用的入侵工具.....300

第1章 社会工程学

黑客入侵系统的环境存在很多的局限性，社会工程学攻击可以充分发挥其优势，利用人为的漏洞进行欺骗来获取系统控制权。这种攻击表面是难以察觉的，不需要面对面的交流，不会在系统中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，本章主要介绍常见的社会工程学攻击及防范社会工程学攻击的方法。

1.1 社会工程学的意义

社会工程学攻击将入侵攻击手段最大化，不仅能够利用系统的弱点进行入侵，还能通过人性的弱点进行入侵，也是一种利用人性的弱点，以顺从人的意愿、满足人的欲望的方式，让人上当的一些方法、一门艺术与学问。下面就来深入了解一下社会工程学。

1.1.1 社会工程学攻击概述

现实社会生活中，骗子的欺骗手段形形色色，随着网络和通信技术的发展，其骗术花样也日益翻新，令人防不胜防。比如，有人轻信中奖短信而受骗，有人因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应用到攻击网络系统上面，就发展成为社会工程学攻击。

社会工程学是近期比较流行的一种攻击方式。社会工程学攻击是黑客利用人际关系的交互性发出的攻击：通常黑客在没有办法通过物理入侵的方式直接取得所需要的资料时，就会通过发电子邮件或打电话来骗取所需要的资料，再利用这些资料获取主机的权限以达到其目的。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，如收集管理员的各种信息以破解其设置的密码。

社会工程学攻击可以分为两种，即狭义社会工程学攻击和广义社会工程学攻击，它们之间的区别可以参考表 1-1。

表 1-1 狭义社会工程学攻击与广义社会工程学攻击的区别

社会工程学攻击	是否有计划、有针对性地获取信息	是否单纯通过网络搜索信息	是否需要知道相关术语信息
狭义社会工程学攻击	否	是	否
广义社会工程学攻击	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为是否会与受害者进行交互式行为。

社会工程学攻击之所以受到黑客们的喜爱，是因为他们可以通过信息搜索及无孔不入的社交直接索取密码，使入侵渗透更加容易，究其根本原因，还是网络管理人员的管理失职。网络管理人员的素质高低直接影响整个网络的安全程度。

随着安全产品技术的日益完善，使用这些技术的人就成为整个环节上最脆弱的部分。有些人具有贪婪、自私、好奇、轻信等心理弱点，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的信息。

真正的社会工程学师是不会碰运气胡乱下载网站与论坛数据库的，他们清楚地知道自己需要什么信息，应该怎样去做，并从收集的信息中分析出有用的信息，与受害者进行交互，从而达到自己的目的。

1.1.2 非传统信息安全不可忽视

社会工程学是非传统的信息安全，并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。所以有的时候，即使你将所有安全手段全用上，也制定了精密的安全解决方案，防护措施做得再好，也会被社会工程学大牛轻易绕过。

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重要的一环，因为人才是所有安全措施的最终实施者。为规避安全风险，专家们精心设计安全解决方案，但这些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，都有可能成为潜在的安全风险与威胁因素。

社会工程学比其他黑客攻击更复杂，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，主张信息安全防护应当采取“先发制人”的策略，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“顾头不顾尾”的现状。

社会工程学无处不在，社会生活中的各个领域都有它的身影。其实在现实生活中，我们也常常在无意中用到社会工程学，只是浑然不觉而已。比如，当遇到问题时，我们知道应该寻找有决定权的人来解决，并寻求周遭人的帮助，这也是社会工程学。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 长驱直入攻击信息拥有者

信息安全的本质是信息拥有者与攻击者间的较量。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，而是直接针对拥有者的脆弱点进行攻击，可以避免一些不必要的麻烦，如口令变化、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与技巧，但社会工程学攻击会打破这种常规。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，俗话说“相似才相吸”，他们总是面带微笑地与你保持一致，使你对他们产生好感。

一个经验丰富的社会工程学师，凭借其战略、战术，几乎能够接近任何他感兴趣的信息。他们会用大量的时间研究非传统信息安全，巨大的商业价值是吸引他们的条件，这种有效的信息入侵对他们非常有诱惑性。他们善于拿捏好你的问题，以帮助你解决问题为诱饵，提出“互惠原则”。

社会工程学攻击受攻击者们欢迎还有一个原因，就是很多企业盲目追求商业利益最大化，他们不注重建立企业品牌，忽略了对员工进行安全培训。而攻击者就利用社会工程学，从相关的方面收集相关的信息从而达成其目的。比如，一家银行从信用卡公司取得信息需要什么文件或 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姓名等，攻击者只要通过某些途径从这些毫无安全意识的企业内部员工的口中得到这些信息，即可成功窃取信息，而那些没有安全威胁意识的企业会在这个问题上栽一个大跟头。

就现阶段来说，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，就必须加强对他们的安全培训。

1.2 常见的社会工程学攻击方式

随着网络安全防护技术及安全防护产品应用的日益成熟，很多常规的入侵手段越来越难以奏效。在这种情况下，更多的攻击者将攻击方式转向了社会工程学攻击，同时利用社会工程学的攻击手段也日趋成熟，技术含量也越来越高。攻击者在实施社会工程学攻击之前必须掌握一定的心理学、人际关系、行为学等知识和技能，以便搜集和掌握实施社会工程学攻击行为所需要的资料和信息等。

结合目前网络环境中常见的社会工程学攻击方式和手段，可以将其划分为以下几种方式，即结合实际环境渗透，引诱、伪装欺骗、说服、恐吓、恭维被攻击者，以及反向社会工程学攻击。下面简要介绍这几种常见的社会工程学攻击方式。

1.2.1 结合实际环境渗透

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、邮箱等，通过这些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。

1.2.2 引诱被攻击者

网上冲浪时经常碰到中奖、免费赠送等内容的邮件或网页，引诱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”其身份，利用人们疏于防范的心理加以引诱，这通常是攻击者早已设好的圈套，利用这些圈套来达到他们的目的。

1.2.3 伪装欺骗被攻击者

伪装欺骗被攻击者也是社会工程学攻击的主要方式之一。利用电子邮件伪造攻击、网络钓鱼攻击等攻击手法均可以实现伪装欺骗被攻击者，比如新年贺卡、求职信病毒等都是利用电子邮件和伪造的 Web 站点来进行诈骗活动的。据调查结果显示，在所有的网络伪装欺骗的用户中，有高达 5% 的人会对攻击者设好的骗局做出响应。

1.2.4 说服被攻击者

说服是对互联网信息安全危害较大的一种社会工程学攻击方式，它要求被攻击者与攻击者达成某种一致，进而为黑客攻击过程提供各种便利条件，当被攻击者的利益与攻击者的利益没有冲突时，甚至与黑客的利益一致时，该种手段就会非常有效。如果目标内部人员已经心存不满，那么只要他稍加配合就很容易达成攻击者的目的，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。

黑客在施行攻击时，经常会争取维修人员、技术支持人员、保洁人员等可信的第三方人员配合，这点在一个大公司是不难实现的。

因为每个人不可能都认识公司中的所有人员，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领导，所以他们会为那些有权利的人提供他们所需要的信息。

1.2.5 恐吓被攻击者

黑客在实施社会工程学攻击过程中，常常会利用被攻击者对安全、漏洞、病毒等内容的敏感性，以权威机构的身份出现，散布安全警告、系统风险之类的消息，使用危言耸听的伎俩恐吓、欺骗被攻击者，并声称不按照他们的方式去处理问题就会造成非常严重的后果，进而实现对被攻击者敏感信息的获取。

1.2.6 恭维被攻击者

社会工程学攻击手段高明的黑客需要精通心理学、人际关系学、行为学等知识和技能，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攻击陷阱，实施欺骗，并控制他人意志为己服务。他们通常看上去十分友善，讲究说话的艺术，知道如何借机去恭维他人，投其所好，使多数人友善地做出回应。