<<入侵的艺术>>

图书基本信息

书名：<<入侵的艺术>>

13位ISBN编号：9787302142720

10位ISBN编号：7302142726

出版时间：2007-1

出版时间：清华大学

作者：Kevin D.Mitnick,William L.Simon

页数：290

译者：袁月杨,谢衡

<<入侵的艺术>>

内容概要

四个志同道合的伙伴使用口袋大小的计算机在拉斯维加大把挣钱。
一个无聊的加拿大小伙子居然能够非法访问南部的一家银行。
几个年轻人被拉登的恐怖分子征召去攻击Lockheed Maritn公司和防御信息系统网络。
所以这些故事都是真实的！
如果读者是自己所在单位的安全负责人，本书中的故事完全可能在您管辖的领域内发生。
害怕国家安全官员深夜造访吗？
那就认真阅读本书并在自己管辖的范围内加以防范吧！
而对在真实生活中斗智斗勇的故事感兴趣的读者，可以对本书进行更深入的阅读。
在网络攻击与利用方面的传奇生涯使得Kevin Mitnick成为了真正的黑客英雄人物，这也是他能够获得其他黑客们真实故事的原因。
在每一个故事的后面，Mitnick对其进行了专业的分析——攻击行为其实是可以防范的。
而他确实是有资格推荐安全措施的不二人选。
无论是在黑客社会的传奇经历中，还是在与电脑犯罪的斗争中，Kevin Mitnick都牢牢地掌握着关键武器——对黑客才气与顽强精神的深入了解。

作者简介

KEVIN D. MITNICK是一位著名的黑客，不过他早已金盆洗手，不再做这一行了。
如今，他将他一生积累下来的丰富技能奉献给了企业、组织单位以及政府部门，帮助他们学会保护自身，不被这本书以及他的前一本畅销书《欺骗的艺术》中所描述的种种攻击行为所危害。
KEVIN D. MITNICK是“防御思维”（defensivethinking.com）的创始人之一。
“防御思维”是一家信息安全咨询公司，致力于帮助企业，甚至政府部门保护其至关重要的信息。
他曾受邀在《早安，美国》、《60分钟》、以及CNN的《举证责任》多个节目中出席，并在防范安全攻击以及网络犯罪方面确立了其领导地位。
.

<<入侵的艺术>>

书籍目录

章节摘录

在所有作业显著的安全控制办法中，能有效地发现和防止内部人员作 梗的办法有这些： ·经管责任：现行的引发诸多问题的经管责任方案有两种：一种是所 谓的账户身份——多个用户共同使用一个账户；另一种是共享账户或口令 信息，以便员工不在办公室或无法取得联系时可以登录。
但当出现严重失 误时，这两种方法都容易造成员工以各自的理由推卸责任的局面。
很简单，如果不能完全禁止共享账户信息的话，至少也不应鼓励这样 做。
这包括员工使用的工作站，即使是要求提供注册信息的工作站。
·多目标环境：在大多数公司里，能设法进入放置设备的工作区域的 入侵者，也能轻易找到途径进入系统。
很少有员工在离开工作岗位时会锁 住计算机或使用屏幕保护程序或者启动口令。
对于心怀不轨者来说，在未 受保护的工作站上安装秘密监控程序软件只需要几秒钟。
在银行，出纳员 离开时总会锁上存放现金的抽屉。
不幸的是，我们几乎没有看到这一方法 被其他机构采用。
可以考虑执行这样一种策略：使用屏幕保护口令或其他程序锁住计算 机。
并确保IT部门通过结构管理执行这一策略。
·口令管理：我的女朋友最近被一家在《财富》杂志排名前50的公司 聘用，这个公司采用可预测模式为进入公司内部互联网的用户设置口令： 用户名后随机带上3个阿拉伯数字。
雇员被聘上时口令也就已经设定好了， 并不能由雇员自己更改。
这样对于任何一位雇员来说，写一份简单的脚本，通过它用不了1000次，就能套到到口令——几秒钟而已。
雇员的口令， 不管是由公司设定还是由雇员自己选择，决不能采用能被轻易预测的模式。
·物理访问：熟悉公司网络的聪明雇员，趁旁边没人时，能充分利用 自己的地理位置，攻击系统。
我曾经是加利福尼亚GTE(一家电信公司)的雇 员。
能进入他们的办公楼就如同获得了这个王国的钥匙——所有的信息都 尽收眼底。
任何人都能进入雇员小隔间或办公室里的工作站，并能访问敏 感的系统。
如果雇员通过使用安全BIOS(基本输出系统)口令并注销，或锁定计算 机，来保护自己的桌面、工作站、编写器和个人数字助理装置，内部不法 人员就需要花相当多的时间才能达到自己的目的。
训练雇员能轻松应付身份不明的人，特别是在机密的区域。
使用安全 控制设备，如摄像机和／或徽章读取系统以控制入口，以及监视内部的运 作。
要考虑定期检查出入口登记，以确认是否有诡异的行为存在，特别是 在安全事故发生时。
·“报废”工作间和其他入口点：当雇员离开公司或被调任到其他部 门时，其工作间就空在那里，心怀不轨的内部人员就通过工作间空置的网 络插孔连接上网，同时掩盖了自己的真实身份。
更糟糕的是，工作站通常 位于隔间的后面，与网络相联，供所有人使用，包括心怀不轨的内部人员f除此之外还有发现了搁置工作间的非授权人员。
其他的访问点如会议室，也经常为蓄意搞破坏的内部人员打开方便之 门。
因此要注意将已经停用的网络插孔关闭，以防止匿名或未授权的人员 利用。
并确保闲置工作间里的任何计算机都处于安全状态下，以防止未授 权人员钻了空子。
·监督职员：应该将所有被通知解雇的员工视为潜在的危险。
对这样 的员工访问机密信息都应该给予监视，特别是复制或下载大量资料时。
现 在的一个u盘能容纳上千兆字节，用它只需要花几分钟就可以存下大量的机 密资料，并带着它走出大门。
在通知解雇员工降职或不如愿的调离前，对他们访问权限设限，这应 该作为一项常用的策略。
同样，要考虑监视雇员的计算机使用，以检查他 们是否有未授权的访问或潜在的不利行动。
·安装未授权硬件：心怀不轨的内部人员能轻易进入其他雇员的工作 隔间，安装硬件或击键记录程序以捕获口令和其他机密信息。
同样，U盘也 能帮助轻易盗取资料。

应对的安全措施就是：禁止安装任何未经书面认可 的硬件设备。
但这种方法实施起来也有问题，品行端正的员工会对此感到 不方便，而心怀不轨者则根本无视这一规定。
在某些处理特别机密信息的组织内，在工作站上转移或关闭USB接口是 一个必要的控制方法。
全范围的检查必须定期进行。
检查必须要确保这些事情：计算机里没 有未授权的无线设备，硬件击键记录程序或附加的调制调解器；没有安装 未受权的软件。
安全和IT人员可以通过使用一个支持802.11的PDA，甚至可以通过安装 了Microsoft Windows XP和无线网卡的膝上型电脑，来检查邻近区域的未 受权的无线接入点(access point)。
Windows XP有一个零设置的实用程序，当它检测到邻近区域有一个无线接入点时，就会弹出一个对话框。
·阻挠信息窃取：当职员在进入公司并逐渐了解内部关键的业务流程 后，他们处在了一个有利的位置上，通过“制约与平衡”原则发现公司的 弱点，然后进行欺诈与偷窃。
不诚实的工人有可能偷窃或对公司造成其他 严重的伤害，因为他们很清楚公司的运作。
内部人员可以自由出入办公室，接触文件柜和内部邮件系统，了解日常事务流程。
因此要通过分析机密和关键业务流程，找出自己的薄弱环节，以此来 制定措施。
在某些情况下，建立工作中的职权分离机制。
某个人完成的机 密操作要被另一个人单独检测，这样能够减少安全风险。
·现场访问政策：建立一个外来访问者安全确认方案，确认象包括其 他办室地点的人员。
一个有效的安全措施是，要求访问者进入安全区域前，出示州级以上身份证明，然后在安全记录本上记录这些来访信息。
一旦 安全事件发生，就可以帮助确认始作俑者。
P70-74

媒体关注与评论

坐在自己舒适的座位上，零距离接触计算机犯罪。
Mitnick所书写的内容中，每一章都是与黑客面谈他们真实攻击故事之后编写的。
这是一本对计算机安全感兴趣的人必读的书籍。
——TomParker，GlobalInterSecLLC的创始人　　很难理解这些违法行为会如此聪明，如此天衣无缝。
试想一下吧，如果这些天才们运用他们拥有的技巧为社会做点好事，　　这将会是多么了不起的成就啊!无论是为了娱乐还是教育，我都推荐这本书。
——About.com　　数据安全问题发生的源头往往是人们的无知。
Mitnick让我们发现了“它们”的完美伎俩，并告知我们应该如何防范。
——StephenManes，《财富》杂志

<<入侵的艺术>>

编辑推荐

★挖掘黑客背后的真实故事。

★早已金盆洗手的著名黑客KEVIN D. MITNICK将其一生积累下来的丰富技能汇集成书，使大家免受黑客攻击！

★入侵案例加对策，在每一个故事的后面，Mitnick都进行了专业的分析--攻击行为其实是可以防范的！

凯文·米特尼克(Kevin D. Mitnick)作为一名前黑客和安全技术人员，在信息安全的世界里，他免费乘车、盗打电话、未经授权进入世界上最大的几家公司的计算机系统，并成功渗透一些防范最好的计算机系统的传奇黑客生涯是无人比拟的。

他本身的经历就非常让人着迷、好奇和揣测，现在他将所采访的多个信息安全入侵者的入侵故事记录下来，与读者分享。

书中涉及的人物从学校的学生、监狱的囚犯、公司的安全官员到政府的执法人员，涉及的故事包括入侵公司、政府、组织等，事实上，书中多个故事的主人公正是以作者为榜样来效尤的。

读者阅读本书时，总可以与自己所处的环境结合起来，原来我们自己所使用的计算机系统和物理安全措施就存在不少的安全漏洞。

作者的前一部著作The Art of Deception(《欺骗的艺术》)已经成为了一本畅销书，The Art of Deception中所阐述的某些技术手段和社会工程学知识已经成了公司、政府以及国防信息安全等领域研究的热点，大学教授们经常引用这本书中的案例来充实书面上的理论。

本书作为The Art of Deception的姊妹篇，所阐述的则是其他人的故事，我想，也只有作者这样的前黑客高手才可能采访到那些入侵者，让他们说出埋藏在心底多年的隐秘故事吧。

翻译本书时，我们时常感叹大千世界，无奇不有，这些黑客们所利用的技术、耐心和对社会工程学的娴熟理解常常让我们叹为观止，拍案叫绝。

书中的故事和入侵过程引人入胜，匪夷所思。

但是为了防止有人模仿，作者在有些技术的细节上有意对原来的过程进行了篡改，但这并不影响我们对本书所阐述的精髓的理解。

找一个舒适的地方，泡一杯龙井，慢慢品尝它吧！

版权说明