<<信息系统攻防技术>>

图书基本信息

书名：<<信息系统攻防技术>>

13位ISBN编号：9787302200185

10位ISBN编号：7302200181

出版时间：2009-9

出版时间：清华大学出版社

作者：程煜，余燕雄 编著

页数：207

前言

如果说30年前美国小说《P一1的春天》描述的病毒控制计算机酿成灾难的故事叫人难以想象，10年前上映的美国大片《黑客帝国》讲述的科幻故事令人着迷而困惑，那么今天隐藏在网络生活中的计算机病毒和黑客却让人们恐惧和愤恨。
近年来，黑客针对自身防范力量比较弱的中小企业网站实施攻击，造成这些企业和个人损失巨大，一些地方甚至形成了只有交“保护费”才能免遭病毒攻击正常运营的局面。
2003年底到2004年初肆虐网络的“熊猫烧香”木马病毒，在短短的两个月内使上百万个人用户、网吧及企业局域网用户遭受感染和破坏。
用户计算机中毒后会出现蓝屏、频繁重启以及系统硬盘中数据文件被破坏等现象，更重要的是它可以盗取网民银行和游戏账号、密码，从而窃取用户的财产或虚拟财产。
连续多年被指为年度十大病毒、被反病毒专家称为最危险的后门程序“灰鸽子”于2001年问世，随着“灰鸽子2007”的发布，于2004年3月集中爆发，病毒仅10多天就有500多个变种产生。
与“熊猫烧香”的“张扬”不同，“灰鸽子”更像一个隐形的“贼”，潜伏在用户“家”中，监视用户的一举一动，甚至用户与MSN、QQ好友聊天的每一句话都难逃“贼”眼。
过去，病毒的制作者多是为了显示自己超人的技术，而今天病毒的制作者更多是为了牟利。
在利益驱使下，病毒制作、销售、传播、盗取信息等已形成了分工明确的黑色产业链条。
互联网“地下经济”已经组织化、规模化、公开化，制造木马、传播木马、盗窃账户信息、第三方平台销赃、洗钱，分工明确，形成了一个非常完善的流水线作业的程序，产业链上的每一环都有不同的牟利方式。
据不完全统计，“灰鸽子”病毒程序直接售卖价值就达2000万元以上，用于窃取账号等的幕后黑色利益可想而知。

<<信息系统攻防技术>>

内容概要

本书全面介绍信息系统各种攻防手段的基本原理和应用技术，对信息安全的相关概念与技术进行了深入探讨，详尽地分析了信息系统的各种攻击技术和相应防御措施。
对于具体攻击技术，本书首先剖析原理，讲述流程，然后结合案例，强调实际应用中所需的信息安全知识，同时给出了相应的用户对策。

本书叙述简洁，结构清晰，理论体系较完整，可作为信息安全专业的“信息安全导论”课程和计算机、电子信息、通信工程等专业的“信息安全”课程的教材。
同时，全书结合实例，讲解透彻，通俗易懂，也可供工程技术人员作为参考用书。

<<信息系统攻防技术>>

书籍目录

章节摘录

插图：2）数字签名数字签名是附加在数据单元上的一些数据，或是对数据单元所作的密码变换。
这种数据或变换允许数据单元的接收者确认数据单元来源和数据单元的完整性，保护数据防止被人（例如接收者）伪造。
数字签名机制包括两个过程：对数据单元签名和验证签过名的数据单元。
第一个过程使用签名者所私有的（即独有的和机密的）信息，或对数据单元进行加密，或产生出该数据单元的一个密码校验值；第二个过程所用的规程与信息是公之于众的，但不能从它们推断出该签名者的私有信息。
签名机制的本质特征为该签名只有使用签名者的私有信息才能产生出来。
因而，当该签名得到验证后，它能在事后的任何时候向第三方（例如法官或仲裁人）证明只有那个私有信息的唯一拥有者才能产生这个签名。
3）访问控制为了决定和实施一个实体的访问权，访问控制机制可以使用该实体已鉴别的身份，或使用有关该实体的信息（例如它与一个已知的实体集的从属关系），或使用该实体的权利。
如果这个实体试图使用非授权的资源，或者以不正当方式使用授权资源，那么访问控制功能将拒绝这一企图，另外还可能产生一个报警信号或记录它作为安全审计跟踪的一个部分来报告这一事件。
对于无连接数据传输，发给发送者的拒绝访问的通知只能作为强加于原发的访问控制结果而被提供。
访问控制机制可以使用下列一种或多种手段。
（1）访问控制信息库：保存对等实体的访问权限。
信息可以由授权中心或被访问韵实体保存，信息的形式可以是一个访问控制表，或是等级结构的矩阵。
使用这一手段要预先假定对等实体的鉴别已得到保证。

<<信息系统攻防技术>>

版权说明