<<网络安全技术>>

图书基本信息

书名：<<网络安全技术>>

13位ISBN编号：9787508492452

10位ISBN编号：7508492455

出版时间：2012-1

出版时间：水利水电出版社

作者：吴锐

页数：256

<<网络安全技术>>

内容概要

《高职高专教育“十二五”划教材：网络安全技术》立足于“看得懂，学得会，用得上”的原则，结合目前国内高职高专学生的实际情况，舍弃了大篇幅的原理介绍，而将重点放在与实践中密切相关的黑客技术、网络入侵、密码技术及系统安全等当代网络安全突出问题上，并注重实用，以实训为依托，将实训内容融合在课程内容中，使理论紧密联系实际。
在本书中引用了大量实例，并设置了实训操作练习，帮助读者掌握计算机网络安全方面存在的漏洞，以期更好地管理计算机系统。

全书共12章。
分别从理论、技术、应用各个角度对网络安全进行分析和阐述，主要内容包括网络安全概述、网络安全基础、加密技术、病毒与反病毒、系统安全、应用安全、网络攻击与防御、防火墙、入侵检测、网络安全管理、网络安全的法律法规、安全实训。

本书适合于计算机及相关专业的学生作为教材或参考书，也可作为对网络安全感兴趣的初学者的自学教材。

<<网络安全技术>>

书籍目录

章节摘录

版权页： 插图： 与之相对应，密码分析学（Cryptanalysis）就是破译密文的科学和技术。
密码分析学是在未知密钥的情况下从密文推演出明文或密钥的技术。
密码分析者（Cryptanalyst）是从事密码分析的专业人员。
在密码学中，有一个五元组：｛明文、密文、密钥、加密算法、解密算法｝，对应的加密方案称为密码体制（或密码）。
明文：是作为加密输入的原始信息，即消息的原始形式，通常用m或p表示。
所有可能明文的有限集称为明文空间，通常用M或P表示。
密文：是明文经加密变换后的结果，即消息被加密处理后的形式，通常用c表示。
所有可能密文的有限集称为密文空间，通常用C来表示。
密钥：是参与密码变换的参数，通常用k表示。
一切可能的密钥构成的有限集称为密钥空间，通常用K表示。
加密算法：是将明文变换为密文的变换函数，相应的变换过程称为加密，即编码的过程（通常用E表示，即c＝Ek（p））。
解密算法：是将密文恢复为明文的变换函数，相应的变换过程称为解密，即解码的过程（通常用D表示，即p＝Dk（c））。
3.1.5密码学的作用 密码学主要的应用形式有数字签名、身份认证、消息认证（也称数字指纹）、数字水印等几种，这几种应用的关键是密钥的传送，网络中一般采用混合加密体制来实现。
密码学的应用主要体现了以下几个方面的功能： 1.维持机密性 传输中的公共信道和存储的计算机系统非常脆弱，系统容易受到被动攻击（如截取、偷窃、复制信息）和主动攻击（如删除、更改、插入等操作）。
必须加密信息系统中的关键信息，让别人看不懂，也就无从攻击。
2.用于鉴别 由于网上的通信双方互不见面，必须在相互通信时（交换敏感信息时）确认对方的真实身份，即消息的接收者应该能够确认消息的来源，入侵者不可能伪装成他人。
3.保证完整性 消息的接收者能够验证在传送过程中消息是否被篡改；入侵者不可能用假消息代替合法消息。
4.用于抗抵赖 在网上开展业务的各方在进行数据传输时，必须带有自身特有的、无法被别人复制的信息，以保证发生纠纷时有所对证，发送者事后不可能否认他发送的消息。
3.2密码分析 密码分析者是在不知道密钥的情况下，从密文恢复出明文。
成功的密码分析不仅能够恢复出消息明文和密钥，而且能够发现密码体制的弱点，从而控制通信。
常用的密码分析方法有4类：唯密文攻击（ciphertext-only attack）、已知明文攻击（known-plaintext attack）、选择明文攻击（chosen-plaintext attack）和选择密文攻击（chosen-ciphertext attack）。
1.唯密文攻击 密码分析者已知一些消息的密文，这些消息都用同一加密算法加密。
密码分析者的任务是恢复尽可能多的明文，或者最好是能推算出加密消息的密钥，以便采用相同的密钥解出其他被加密的消息。
2.已知明文攻击 密码分析者不仅可以得到一些消息的密文，而且也知道这些消息的明文。
分析者的任务就是用加密消息推出用来加密的密钥或推导出一个算法，此算法可以对用同一密钥加密的任何新的消息进行加密。
3.选择明文攻击 密码分析者不仅可以得到一些消息的密文和相应的明文，而且他们也可以选择被加密的明文。
这比已知明文攻击更有效，因为密码分析者能选择特定的明文块去加密，那些块可能产生更多关于密钥的消息，分析者的任务是推出用来加密的密钥或导出一个算法。
此算法可以对用同一密钥加密的任何新的消息进行解密。

<<网络安全技术>>

编辑推荐

《高职高专教育"十二五"规划教材:网络安全技术》在《高职高专教育"十二五"规划教材:网络安全技术》中引用了大量实例，并设置了实训操作练习，帮助读者掌握计算机网络安全方面存在的漏洞，以期更好地管理计算机系统。
使读者对网络安全有一个系统而全面的认识。
《高职高专教育"十二五"规划教材:网络安全技术》适合于计算机及相关专业的学生作为教材或参考书，也可作为对网络安全感兴趣的初学者的自学教材。
希望读者在读完《高职高专教育"十二五"规划教材:网络安全技术》之后，可对网络安全技术有进一步的了解，并体验到掌握知识的乐趣。

版权说明