<<计算机网络安全>>

图书基本信息

书名：<<计算机网络安全>>

13位ISBN编号：9787111385370

10位ISBN编号：7111385373

出版时间：2012-8

出版时间：机械工业出版社

作者：谭晓玲　等编著

页数：292

字数：470000

<<计算机网络安全>>

内容概要

《计算机网络安全》(作者谭晓玲、蔡黎、刘毓、代妮娜)重点论述目前计算机网络安全中比较成熟的思想、结构和方法，着力介绍网络安全系统的实践操作方法。
全书共10章，第1章引言，简单介绍计算机网络安全的产生和发展、主要功能、分类以及网络体系结构和ISO/OSI参考模型。
第2
、3章主要介绍网络安全攻击，内容包括计算机网络的入侵及检测和安全扫描。
第4、5章介绍网络安全防御和防火墙技术。
第6、7、8章介绍数据通信网的基本知识及数据安全、病毒防治技术。
第9章介绍如何科学地管理广域
/局域计算机网络的安全。
第10章以案例的形式介绍计算机网络安全法规的相关知识。

《计算机网络安全》可作为高等院校信息技术类专业高年级本科生或低年级硕士研究生的学习资料，也可以作为从事计算机网络工作的技术人员研读和参考用书。

<<计算机网络安全>>

书籍目录

参考文献

章节摘录

版权页： 插图： 4.3.2密码分析还原 密码学等加密技术向人们做出保证，密码的攻破理论上是不可行的，如果采用蛮力攻击，所用的时间将长到足够保证安全的程度。
但现实中，密码的破解却并不如理论中所保证的那样困难。
随着计算机运算速度的指数级提高，相同的运算量所使用的时间明显地缩短。
同时，对加密算法的强度分析以及社会工程学的密码筛选技术的不断发展，现实网络中的大量密码可以在可接受的时间内被分析还原。
密码分析与还原技术不使用系统和网络本身的漏洞，虽然涉及对密码算法的强度分析，但它主要利用的是人的惰性以及系统的错误配置。
应用这类技术手段攻击通常是可以通过人工手段避免的，只要严格要求网络所在用户的密码强度，还是可以避免大部分的攻击，但由于这涉及人员管理，代价也非常大。
目前网络中使用的加密算法，从加密的种类上来分，主要包括对称加密和非对称加密两种基本的类别。
根据分析的出发点不同，密码分析还原技术主要分为密码还原技术和密码猜测技术。
对于网络上通用的标准加密算法来说，攻击这类具有很高强度加密算法的手段通常是使用后一种技术。
在进行攻击时，密码分析还原所针对的对象主要是通过其他侦听手段获取到的认证数据信息，包括系统存储认证信息的文件或利用连接侦听手段获取的用户登录的通信信息数据。
1.密码还原技术 密码还原技术主要针对的是强度较低的加密算法。
通过对加密过程的分析，从加密算法中找出算法的薄弱环节，从加密样本中直接分析出相关的密钥和明文。
对于非对称算法，可以通过对密文的反推将明文的可能范围限定在有限的范围内，达到还原密文的效果。
这种方法需要对密码算法有深入的研究，同时，相关算法的密码还原过程的出现，也就注定了相应加密算法寿命的终结。
对于目前网络上通行的标准加密算法来说，从理论和实践中还没出现对应的密码还原过程，因此密码还原技术的使用并不多。
但对于没有公开加密算法的操作系统来说，由于算法的强度不够，在过程被了解后，黑客就会根据分析中获得的算法漏洞完成密码还原的算法。
现在，对于Windows操作系统来说，用户认证的加密算法就已经被分析攻破，用户只要使用密码破解程序就可以完成对系统上所有密码的破解，获取系统上所有用户的访问权限。
2.密码猜测技术 密码还原技术需要目标系统使用强度不高的、有一定安全漏洞的加密算法，而对于一般的成熟加密算法，密码攻击主要使用的是密码猜测技术。
密码猜测技术的原理主要是利用穷举的方法猜测可能的明文密码，将猜测的明文经过加密后与实际的密文进行比较，如果所猜测的密文与实际的密文相符，则表明密码攻击成功，攻击者可以利用这个密码获得相应用户的权限。
往往这样猜测出来的密码与实际的密码相一致。

编辑推荐

《计算机网络安全》可作为高等院校信息技术类专业高年级本科生或低年级硕士研究生的学习资料，也可以作为从事计算机网络工作的技术人员研读和参考用书。

<<计算机网络安全>>

版权说明