<<网络攻防技术教程>>

图书基本信息

书名：<<网络攻防技术教程>>

13位ISBN编号：9787307062320

10位ISBN编号：7307062321

出版时间：2008-6

出版时间：武汉大学出版社

作者：杜晔，张大伟，范艳芳　编著

页数：352

前言

随着计算机和通信技术的飞速发展，网络应用已日益普及，成为人们生活中不可缺少的一部分。
截止2007年12月，我国网民总人数已达2亿人。
电子政务、电子商务得到了进一步推广，有大约22．1%的网民进行网络购物或者商业运作，人数规模达到4640万人。
但在网络服务为我们提供了极大便利的同时，对于信息系统的非法入侵和破坏活动正以惊人的速度在全世界蔓延，同时带来巨大的经济损失和安全威胁。
据统计，每年全球因安全问题导致的损失已经可以用万亿美元的数量级来计算。
在我国，“震荡波”系列蠕虫曾造成有超过138万个IP地址的主机被

<<网络攻防技术教程>>

内容概要

本书详细得介绍了计算机及网络系统面临的威胁与黑客攻击方法，详尽、具体地披露了攻击技术的真相以及防范策略和技术实现措施。
本书理论联系实际。
在技术讨论之后，都会有一套详细的试验方案对相关技术进行验证。
　全书共分4个部分，内容由浅入深，按照黑客攻击通常采用的步骤进行组织，分技术专题进行讨论。
第一部分介绍了网络攻防基础知识，以使读者建立起网络攻防的基本概念。
第二部分介绍信息收集技术，即攻击前的“踩点”，包括网络嗅探和漏洞扫描技术。
第三部分是本书的核心内容，介绍了有代表性的网络攻击技术以及有针对性的防御技术。
第四部分着重防御技术，讨论了PKI网络安全协议和两种得到广泛应用的安全设备，即防火墙的入侵检测系统。
　本书可作为信息安全、计算机、通信等专业本科生、硕士研究生的教科书，也适合于网络管理人员、安全维护人员和相关技术人员参考和阅读。

<<网络攻防技术教程>>

书籍目录

章节摘录

第3章网络嗅探3.1嗅探器概述3.1.1嗅探器简介嗅探器（Sniffer）是一种在网络上常用的收集有用信息的软件，可以用来监视网络的状态、数据流动情况以及网络上传输的信息。
当信息以明文的形式在网络上传输时，便可以使用网络嗅探的方式来进行攻击，分析出用户敏感的数据，例如用户的账号、密码，或者是一些商用机密数据等。
而我们经常使用的FTP、Telent、SMTP、POP协议等都采用明文来传输数据。
大多数的黑客仅仅为了探测内部网上的主机并取得控制权，只有那些黑客，为了控制整个网络才会安装特洛伊木马和后门程序，并清除记录。
他们经常使用的手法是安装Sniffer。
因此，嗅探器攻击也是在网络环境中非常普遍的攻击类型之一。
ISS为嗅探器Sniffer做了以下定义：Sniffer是利用计算机的网络接口截获目的地为其他计算机数据报文的一种工具。
简单地解释：一部电话上的窃听装置，可以用来窃听双方通话的内容，而嗅探器则可以窃听计算机程序在网络上发送和接收到的数据。
后者的目的就是为了破坏信息安全中的保密性，即越是不想让别人知道的内容别人就一定想知道。
可是，计算机直接传送的数据，事实上是大量的二进制数据。
那么，嗅探器是怎样能够听到在网络线路上传送的二进制数据信号呢?可不可以在一台普通的PC机上就可以很好地运作起来完成嗅探任务呢?答案是肯定的。
首先，嗅探器必须也使用特定的网络协议来分析嗅探到的数据，也就是说嗅探器必须能够识别出哪个协议对应于这个数据片断，只有这样才能够进行正确的解码。
其次，嗅探器能够捕获的通信数据量与网络以及网络设备的工作方式是密切相关的。
对于局域网来讲，如果按照介质访问控制方法进行划分的话，可以分为共享式局域网与交换式局域网。
共享式局域网的典型设备是集线器（Hub），该设备把一个端口接收的信号向所有其他端口分发出去。
如图所示，经过3个Hub串联形成的局域网，当主机A需要与主机E通信时，A所发送的数据包通过Hub的时候就会向所有与之相连的端口转发。
在一般情况下，不仅主机E可以收到数据包，其余的主机也都能够收到该数据包。

<<网络攻防技术教程>>

编辑推荐

《网络攻防技术教程:从原理到实践》可作为信息安全、计算机、通信等专业本科生、硕士研究生的教科书，也适合于网络管理人员、安全维护人员和相关技术人员参考和阅读。

<<网络攻防技术教程>>

版权说明