<<巧学活用网络安全与维护>>

图书基本信息

书名：<<巧学活用网络安全与维护>>

13位ISBN编号：9787121193750

10位ISBN编号：7121193752

出版时间：2013-2

出版时间：丁文彦 电子工业出版社 (2013-02出版)

作者：丁文彦

<<巧学活用网络安全与维护>>

内容概要

《巧学活用网络安全与维护/巧学活用系列》编著者丁文彦。

网络安全是指网络系统中的硬件、软件及其数据受到保护，不因偶然或恶意的原因而遭受破坏、更改、泄露，使系统连续、可靠、正常地运行，网络服务不被中断。
从其本质上来讲，网络安全就是网络上的信息安全。
本书系统介绍了网络安全基础知识，TCP／IP基础知识，网络攻击、检测与防范技术，操作系统的安全漏洞，计算机病毒与反病毒技术，防火墙技术，web服务的安全性，以及常见网络安全故障处理。

《巧学活用网络安全与维护/巧学活用系列》适合企事业单位从事网络安全与维护的技术、管理人员阅读，也可作为相关岗位职业培训的教学用书。

<<巧学活用网络安全与维护>>

书籍目录

章节摘录

版权页： 插图： 2.放置特洛伊木马 特洛伊木马程序（简称木马）能直接侵入用户的计算机并进行破坏活动，它常被伪装成工具程序或游戏等诱使用户打开带有木马的邮件附件或从网上直接下载，一旦用户打开了这些邮件的附件或执行了这些程序后，它们就会像古代特洛伊人在敌人城外留下的藏满士兵的木马那样，留在自己的计算机中，并在自己的计算机系统中隐藏一个能在操作系统启动时悄悄执行的程序。
当用户链接到互联网上时，这个程序就会通知攻击者，来报告用户的IP地址及预先设定的端口。
攻击者在收到这些信息后，再利用这个潜伏在其中的程序，就能任意地修改用户的计算机的参数设定、复制文件、窥视整个硬盘中的内容等，从而达到控制用户计算机的目的。
3.WWW的欺骗技术 在网上，用户可以利用IE等浏览器进行各种各样的w曲站点的访问，如阅读新闻组、咨询产品价格、订阅报纸、电子商务等。
然而，一般的用户恐怕不会想到有这些问题存在：正在访问的网页已被黑客篡改过，网页上的信息是虚假的。
例如，黑客将用户要浏览的网页的URL改写为指向黑客自己的服务器，当用户浏览目标网页时，实际上是向黑客服务器发出请求，那么黑客就能达到欺骗的目的了。
一般Web欺骗使用两种技术手段，即URL地址重写技术和相关信息掩盖技术。
利用URL地址，使这些地址都转向攻击者的Web服务器，即攻击者能将自己的wreb地址加在所有URL地址的前面。
这样，当用户和站点进行安全链接时，就会毫不防各地进入攻击者的服务器，于是用户的所有信息便处于攻击者的监视中。
但由于浏览器一般均设有地址栏和状态栏，当浏览器和某个站点链接时，可以在地址栏和状态栏中获得链接中的w曲站点地址及其相关的传输信息，用户由此可以发现问题，所以攻击者往往在URL址重写的同时，利用相关信息掩盖技术，即一般用JavaScript程序来重写地址栏和状态栏，以达到其掩盖欺骗的目的。
4.电子邮件攻击 电子邮件是互联网上运用得十分广泛的一种通信方式。
攻击者可以使用一些邮件炸弹软件或CGI程序向目的邮箱发送大量内容重复、无用的垃圾邮件，从而使目的邮箱被“撑爆”而无法使用。
当垃圾邮件的发送流量特别大时，更有可能造成邮件系统对于正常的工作反应缓慢，甚至瘫痪。
相对于其他的攻击手段来说，这种攻击具有方法简单、见效快等特点。

<<巧学活用网络安全与维护>>

编辑推荐

《巧学活用网络安全与维护》适合企事业单位从事网络安全与维护的技术、管理人员阅读，也可作为相关岗位职业培训的教学用书。

<<巧学活用网络安全与维护>>

版权说明