电脑爱好者 精品图书

150个
安全攻防的案例分析

150个攻击和漏洞防范的案例分析，
展示一个防黑高手的成长历程！

由0晋身200%
防黑高手

张晓兵 陈鹏 谢巍 彭爱华 张忠将 齐文普 编著

怎样才能保证你的电脑更加安全？本地电脑安全、Internet下的操作系统安全、网页浏览安全、电子邮件安全、QQ和MSN聊天安全、下载文件安全、局域网安全，还有网络游戏安全，一个都不能少！一个都不能不懂！

分析各种常见操作中隐藏的漏洞，讲述对付恶意攻击最有力的反击手段，同时详细分析黑客进攻的常见手法，悉数讲解攻击产生的详细过程和防范！

随书配送
“超级急救盘”，即使不幸遭遇攻击，也可以进行检测和清除！

内蒙古科学技术出版社

由0晋身200%防黑高手

张晓兵 陈 鹏 谢 巍
彭爱华 张忠将 齐文普 编著

内蒙古科学技术出版社

图书在版编目(CIP)数据

由0晋身200%防黑高手 / 张晓兵等编著. —赤峰:内蒙古科学技术出版社, 2005.3
ISBN 7-5380-1295-8

Ⅰ.由… Ⅱ.张… Ⅲ.计算机网络—安全技术
Ⅳ.TP393.08

中国版本图书馆CIP数据核字(2005)第015900号

内容简介

本书讲述对付恶意攻击最有力的反击手段,同时详细分析黑客进攻的常见手法,悉数讲解攻击产生的详细过程和防范!

怎样才能保证安全?本地电脑安全、Internet下的操作系统安全、网页浏览安全、电子邮件安全、QQ和MSN聊天安全、下载文件安全、局域网安全,还有网络游戏安全,一个都不能少!一个都不能不懂!

随书赠送"超级急救盘",即使不幸遭遇攻击,也可以轻而易举地检测和清除!

本书适合初中级的电脑用户阅读。

出版发行:内蒙古科学技术出版社
地　　址:赤峰市红山区哈达街南一段4号
电　　话:(0476)8224848　8231924
邮　　编:024000
责任编辑:马洪利　李渊博
印　　刷:赤峰彩世印刷有限公司
开　　本:787×1092　1/16
印　　张:18
字　　数:580千
版　　次:2005年3月第1版
印　　次:2005年3月第1次印刷
定　　价:25.00元(含1CD)

目 录

第1章

黑客攻击是怎么产生

1.1 为什么会有攻击

一般认为，黑客起源于20世纪50年代麻省理工学院的实验室中，他们精力充沛，热衷于解决难题。

20世纪六七十年代，“黑客”一词极富褒义，用于指代那些独立思考、奉公守法的计算机迷，他们智力超群，对电脑全身心投入，从事黑客活动意味着对计算机的潜力进行智力上的自由探索。

到了20世纪八九十年代，计算机越来越重要，大型数据库也越来越多，同时，信息越来越集中在少数人的手里——这一场新时期的“圈地运动”引起了黑客们的极大反感。黑客认为，信息应共享，而不是被少数人所垄断，于是开始将注意力转移到涉及各种机密的信息数据库上。因此而产生了破解口令（Password cracking）、开天窗（Trapdoor）、走后门（Backdoor）、安放特洛伊木马（Trojan horse）等黑客活动，还利用操作系统和程序的相关漏洞进行的创造性攻击。

如今的黑客鱼龙混杂，既有善意的以发现计算器系统漏洞为乐趣的“计算机黑客”（Hacker），又有玩世不恭、好恶作剧的“计算机黑客”（Cyberbunk），还有纯粹以私欲为目的、任意篡改数据，非法获取信息的“计算机黑客”（Cracker）。

一、黑客攻击的前提

网络通信协议自身存在漏洞或因配置不当而产生安全漏洞；

用户使用的操作系统存在安全漏洞；

用户使用的程序语言本身具有安全隐患。

二、攻击实施的工具

通过使用网络命令进行攻击；

使用专用软件（例如，X-scan等网络扫描软件）；

攻击者自己编写软件，非法进入本地或者远程用户的主机系统。

三、黑客攻击产生的危害

获得、修改、删除用户系统的信息，或者在用户系统上增加垃圾（或有害信息）。

1.2 攻击的主要方式

随着网络攻击技术的飞速发展，网络世界的安全性不断受到挑战。对于攻击者自身来说，要闯入大部分人的电脑实在是太容易了。如果你要上网，就免不了遇到攻击，所以必须知己知彼，才能在网上保证自身安全。那么常用攻击手段有哪些呢?

1.2.1 获取口令

产生攻击的前提之一是获得目标电脑的口令，所以我们需要把守的第一关就是保护好自己的口令。获取口令通常有三种方法：

- 暴力破解
- 欺骗
- 监听和嗅探

一、暴力破解

暴力破解的途径可分为两种，一种是通过远程试探（通俗的说法就是进行猜测），显然这样反复试探的效率会比较低，并且对于使用者的入门也非常困难。他们不需要对被攻击方的服务器有太深入的了解，只要知道一个用户账号和登录入口就可以开始尝试破解。另外一种是获取对方的密码文件后在本地破解。对于那些口令安全系数极低的用户，暴力破解的过程可以在几十秒时间内将其破解。

可以作为攻击对象的口令有很多，例如屏幕保护程序口令、Windows登录口令、局域网共享口令、远程共享口令、远程桌面口令、数据库SQL Server 7.0/2000口令、数据库Access Database口令等。

如图1-2-1所示是用破解软件Cain破解Access数据库密码的过程，这个软件破解能力极强，几乎可以捕获所有的账号口令。

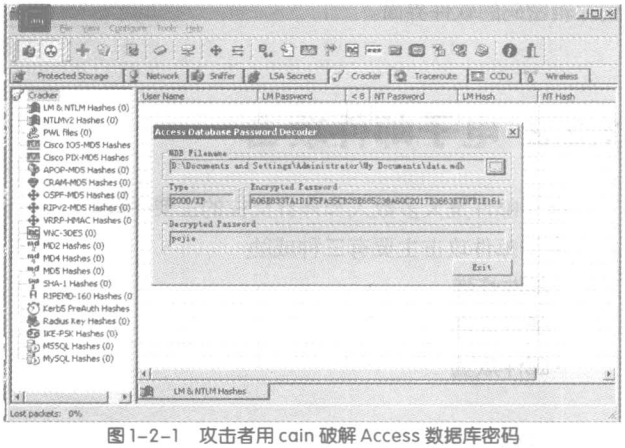

图1-2-1 攻击者用cain破解Access数据库密码

二、欺骗

在网上，用户可以利用IE等浏览器进行各种各样的WEB站点访问，如阅读新闻组、咨询产品价格、订阅报纸、开展电子商务等。然而一般的用户恐怕不会想到，正在访问的网页可能已经被黑客篡改过，网页上的信息是伪装的！黑客可以将用户要浏览的网页URL（网址）改写为指向黑客自己的服务器，当用户浏览目标网页的时候，实际上是向黑客服务器发出请求，这样黑客就达到了欺骗的目的。

三、监听和嗅探(Sniffer)

网络的一个特点就是数据总在流动中，从一处到另一处；而互联网是由错综复杂的各种网络交汇而成的，也就是说，当你的数据从网络的一台电脑传到另一台电脑的时候，通常会经过大量不同的网络设备，用tracert命令就可以看到这种路径是如何进行的。如果传输过程中，有人看到了传输中的数据，那么问题就出现了——这就好比你给别人发了一封邮件，在半路上被人拆开偷看了。这样说或许你还不是很担心，但试想一下，如果这个传送的数据是你的信用卡账号和密码，后果又会怎么样呢……

嗅探监听主要有两种途径：

一种是将监听工具软件放到通过Internet连接的其他设备上，或者放到可以控制网络连接设备的电脑

上，例如网关服务器和路由器。当然，要实现这样的效果可能也需要其他黑客技术，比如通过木马方式将嗅探器发给某个网络管理员，使其不自觉的为攻击者进行安装。

另外一种是通过局域网将监听工具放到个人电脑中，实现对整个局域网的监听。

其原理是这样的：共享Hub获得子网内需要接收的数据时，并不是直接发送到指定主机，而是通过广播方式发送到每个电脑上；真正的接受者电脑会收下该数据，而其他非接受者的电脑则会扔掉这些数据，这些操作本来与电脑操作者无关，是系统自动完成的。但是若其他非接收者有意收集数据的话，他是可以将那些原本不属于他的数据打开的，这就是安全隐患！

如图 1-2-2 所示是利用 Cain 嗅探到邮箱密码的软件界面。

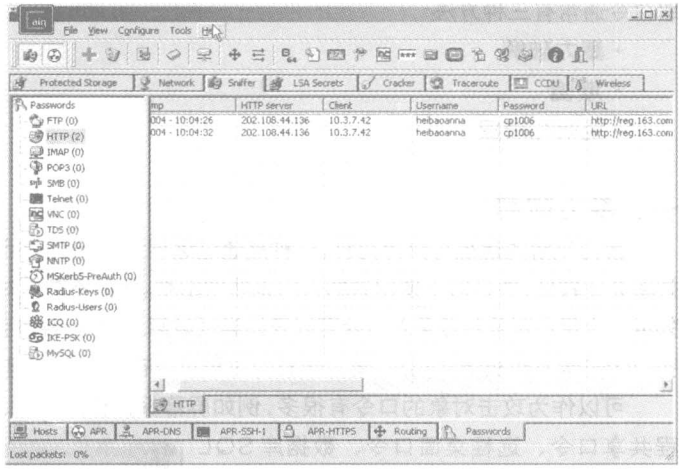

图1-2-2 利用 cain 可以嗅探邮箱密码

1.2.2 电子邮件攻击

电子邮件是大多数人和外界交往的主要手段之一，它也因此成为恶意攻击的重要目标。

电子邮件攻击主要有三种威胁：

- 邮件炸弹
- 邮件病毒
- 邮件欺骗

一、邮件炸弹

电子邮件炸弹，英文是Email Bomb。相对于其他的攻击手段来说，这种攻击方法可谓简单，实质就是发送地址不详、容量庞大、充满了乱码或者谩骂的恶意邮件，也可称之为大容量的邮件垃圾。由于个人邮件信箱通常都容量有限，因此当庞大的邮件垃圾到达信箱时，就会把信箱完全占据，把正常的邮件给冲掉。同时，由于它占用了大量的网络流量，常常导致网络“塞车”，使大量的用户不能正常地工作。所以说邮件炸弹的危害是相当大的。现在已经有很多种能自动产生邮件炸弹的软件程序，而且有逐渐普及的趋势。

二、邮件病毒

“邮件病毒”得名于它的传播途径，其实性质和普通的电脑病毒一样。它们一般是通过在邮件中夹带“附件”的方式进行扩散。只有当你运行了该附件中的病毒程序以后，这个病毒才能感染你，一度流行的“美丽杀手”、“Happy99病毒”等就是邮件病毒。

三、邮件欺骗

通过将自己的邮件地址伪装成系统管理员，攻击者冒充系统管理员给用户发送邮件，要求用户修改口