

电脑爱好者



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 编 著
彭爱华 张忠将 齐文普

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. B5… 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)



第1章 黑客攻击是怎么产生的

1.1 为什么会有攻击	2
一、黑客攻击的前提	2
二、攻击实施的工具	2
三、黑客攻击产生的危害	2
1.2 攻击的主要方式	2
1.2.1 获取口令	3
一、暴力破解	3
二、欺骗	3
三、监听和嗅探(Sniffer)	3
1.2.2 电子邮件攻击	4
一、邮件炸弹	4
二、邮件病毒	4
三、邮件欺骗	4
1.2.3 特洛伊木马攻击	5
1.2.4 寻找系统漏洞	5
一、漏洞原理	6
二、利用漏洞攻击过程	6
三、防范 WebDAV 漏洞	7
1.3 找到自己的漏洞——使用扫描器	8
1.3.1 扫描器原理	8
1.3.2 SuperScan 的攻击过程	9
一、软件介绍	9
二、获得方式	9
三、扫描的使用	9
四、主机和服务器扫描设置	10
五、扫描选项设置	10
六、工具选项设置	11
七、Windows 枚举选项设置	11
1.3.3 X-Scan 的使用	12
一、软件介绍	12
二、扫描模块设置	12
三、“基本设置”页	12
四、“高级设置”页	13
五、“端口相关设置”页	13
六、“NASL 相关设置”页	13
七、“网络设置”页	14
1.4 对你发动攻击	14
1.4.1 获取权限	14
1.4.2 拒绝服务	15
一、死亡之 ping (ping of death)	15
二、泪滴 (teardrop)	16
三、UDP 洪水 (UDP flood)	16
四、SYN 洪水 (SYN flood)	16
五、Land 攻击	16
1.5 攻击后的处理	16
1.5.1 巩固权限——留后门	16
1.5.2 删除日志——清除踪迹	17

1.6 防范入侵基本方法	18
1.6.1 提高安全意识	19
1.6.2 常规的防范措施	19

第2章 保护操作系统

2.1 Windows 9X 安全漏洞和防范	22
2.1.1 Windows 9x 本地漏洞及其防范	22
一、0 级漏洞	23
二、长文件名漏洞	24
三、匿名登录漏洞	24
四、文件扩展名欺骗漏洞	26
五、自动运行漏洞	26
2.1.2 Windows 9x 远程漏洞攻击防范	27
一、设备名称解析漏洞	27
二、共享文件夹漏洞	28
2.2 Windows 2000 安全漏洞和防范	29
2.2.1 系统典型漏洞	29
一、输入法漏洞	29
二、Unicode 漏洞	29
三、系统管理权限漏洞	29
四、RDP 漏洞	30
五、IIS 漏洞攻击防范	30
2.2.2 密码探测攻击防范	31
一、密码探测介绍	31
二、密码探测攻击的种类	32
三、密码探测攻击的防范	33
2.2.3 远程缓冲区溢出攻击防范	33
2.2.4 拒绝服务攻击 (DoS) 与防范	34
一、报文洪水攻击 (Flood DoS)	34
二、UDP flood 拒绝服务攻击	34
三、死 Ping 攻击	35
2.2.5 后门制作与防范	36
一、后门概念及分类	36
二、后门入侵原理	36
三、后门防范	37
2.2.6 攻击后隐藏踪迹与防范	39
2.3 Windows XP 安全漏洞和防范	40
2.3.1 快速用户切换漏洞	40
2.3.2 RPC 漏洞	41
2.3.3 终端服务漏洞	41
2.3.4 热键漏洞	41
2.4 用好个人防火墙	42
2.4.1 使用系统自带的防火墙	42
2.4.2 使用第三方的个人防火墙	43
2.4.3 使用病毒防火墙	45
2.5 实例	46
实例1：使用网络命令查看端口和网络连接，看是否有黑客入侵	46
实例2：使用工具随时监听端口和网络连接，看是否有黑客入侵	47



实例 3: 快速关闭被入侵的端口	48
实例 4: 关闭某些服务, 防范黑客入侵	49
实例 5: 如何知道黑客查看、更改了注册表	49
实例 6: 对重要文件夹或文件采取特殊安全措施	51
实例 7: 手工删除 DLL 类型的后门程序	52
实例 8: IP 地址隐藏技术	54
实例 9: 使用 Windows XP SP2 安全中心保护上网安全	57
实例 10: 系统出现 1 分钟重启现象的解决办法	59
实例 11: 禁止别人通过 ping 主机来了解自己的网络情况	61
实例 12: 关闭不必要的服务, WinXP 如何关闭信使服务	64

第 3 章 本地安全

3.1 概述	68
3.1.1 本地电脑面临的安全威胁	68
3.1.2 如何防范	68
3.2 用户名密码保护	69
3.2.1 Windows 98/Me 用户名保护	69
一、在 Windows Me 中添加新用户	69
二、更改用户设置和密码	70
3.2.2 Windows 2000 用户名保护	70
一、认识 Windows 2000 中的用户、组和组策略概念	70
二、添加新用户	71
三、设置用户权限	72
四、用户安全策略设置	74
五、Windows 2000 下的其他安全设置	76
3.2.3 Windows XP 用户名保护	77
一、新建用户	77
二、设置用户	78
3.3 密码保护	78
3.3.1 设置 CMOS 密码	79
3.3.2 防护屏幕保护密码	80
3.3.3 防护 Office 文件密码	80
一、给 Word 和 Excel 文件加密	80
二、设置 Access 密码	81
3.3.4 防护压缩文件密码	81
3.3.5 防护 Windows 9x 登录密码	82
3.3.6 防护 Windows 2000 登录密码	83
3.3.7 防护 Windows XP 登录密码	83
一、设置双重保护密码	83
二、密码软盘的制作	84
3.4 隐藏保护	84
3.4.1 隐藏文件和文件夹	84
3.4.2 隐藏分区	85
一、一般方法隐藏分区	85
二、使用软件隐藏分区	85
3.5 清除操作痕迹	86
一、清空“回收站”	86
二、清除我最近访问的“文档”记录	86

三、清除 Office 等文档的记录	86
四、清除 IE 临时记录	87
五、删除临时文件	87
3.6 实例	87
实例 1: 忘了 CMOS 密码怎么办	87
一、软件破解法	87
二、通用密码法	88
三、CMOS 放电法	88
实例 2: 忘了屏幕保护密码怎么办	88
一、硬件冲突破解法	88
二、光盘破解法	88
三、注册表修改法	89
实例 3: 忘了 Office 文档和压缩文件夹密码怎么办	89
实例 4: 用“隐私保护专家”保护你的隐私	90
实例 5: 在 NTFS 分区上设置用户权限	90
实例 6: 利用 EFS 系统为文件加密	91
实例 7: EFS 系统出了问题怎么办	92
一、删除用户后如何打开加密文件	92
二、备份密钥	93
实例 8: 硬盘保护卡的使用与防破解	93
一、硬盘保护卡的安装	93
二、硬盘保护卡的保护与破解	94
实例 9: 恢复被误删的文件	94
实例 10: PDF 文件的加密与解密	95
一、加密 PDF 文档	95
二、解密 PDF 文档	95
实例 11: 恢复 Office 文档	96

第 4 章 网页浏览安全

4.1 浏览器的发展和原理	98
4.2 IE 威胁和安全防范	99
4.2.1 网页炸弹的威胁和防范	99
一、常见网页炸弹的威胁	100
二、网页炸弹防范方法	101
4.2.2 缺德网站留下的后遗症	104
一、缺德网站留下后遗症的实例	104
二、缺德网站留下后遗症的防范方法	105
4.3 Cookies 安全问题	110
4.3.1 什么是 Cookies	110
4.3.2 Cookies 带来的安全隐患	111
4.3.3 安全配置 IE 浏览器中的 Cookies	111
一、IE 5.0 中安全配置 Cookies	111
二、IE 6.0 中安全配置 Cookies	112
4.4 脚本和脚本病毒	113
4.4.1 什么是脚本	113
4.4.2 如何清除脚本病毒	114
4.5 实例	115
实例 1: 注册表中的 IE 设置选项	115



●过滤IP(适用于 Windows 2000)	115
●禁止显示IE的地址栏	115
●允许DHCP(WinNT 适用)	115
●禁止更改IE的辅助功能设置	115
●禁止使用“重置Web 设置”	115
●禁止更改IE的链接设置	115
●打开IE的时候,窗口最大化	116
●禁止更改IE的语言设置	116
●清理IE网址列表	116
●禁止使用代理服务器	116
●在IE中禁止显示工具栏	116
●在IE中禁止显示状态栏	116
●更改“应用程序”的文件夹的路径	116
●更改“应用程序数据”的文件夹路径	116
●更改Internet Explorer的标题	116
●更改Outlook Express的标题	117
●禁止使用网上邻居	117
●显示“频道栏”	117
●禁止更改IE默认的检查(WinNT 适用)	117
●禁止IE显示“工具”中“Internet 选项”	117
●改变“超级链接”处点击前后的颜色	117
●清理访问“网络邻居”后留下的字句信息	117
●改变和增加IE自动搜索的顺序	117
●在“开始”菜单中增加“网上邻居”	117
●禁止在“控制面板”中显示“网络”属性	118
●禁止在“网络”中显示“标识”属性	118
●禁止在“网络”中显示“整个网络”属性	118
●更改IE的缓冲路径	118
●改变下载的路径	118
●禁止查找用户	118
●改变收藏夹、Cookies、启动、历史记录的路径	118
●创建“拨号网络”在开始菜单中	118
●网址URL的调整	118
●取消登录时选择用户	119
●隐藏上机用户登录的名字	119
●禁止使用IE“Internet 选项”中的高级项(WinNT 适用)	119
●屏蔽Internet Explorer选项卡类	119
实例2:使用“3721 上网助手”安全设置IE	120
一、安装“3721 上网助手”	121
二、修复IE	122
三、安全防护IE	123
四、保护用户隐私	126
五、广告拦截	128
实例3:清除IE分级审核密码	129
实例4:拆解恶意网页窗口炸弹	130
实例5:恶意代码自我保护功能	131
实例6:使用组策略安全设置IE	133
实例7:IE 升级	135

一、手动更新	135
二、自动更新	135
三、升级 IE 版本	136
实例 8: 对你的孩子负责——IE 分级审查	136
实例 9: Windows XP Service Pack 2 中的 IE 安全设置	137
实例 10: 安全配置 Windows Messenger 服务	139

第 5 章 电子邮件安全

5.1 电子邮件工作原理	146
5.1.1 SMTP 协议	146
5.1.2 POP3 协议	146
5.2 电子邮件常见的安全漏洞和威胁	147
5.2.1 WEB 信箱隐私漏洞威胁和防范	147
5.2.2 电子邮件炸弹漏洞威胁和防范	147
5.2.3 密码的威胁和防范	148
一、邮箱密码的设置	150
二、密码使用的注意事项	150
5.2.4 邮件监听漏洞威胁	150
5.2.5 邮件病毒威胁和防范	151
一、预防	151
二、防范邮件病毒	151
5.3 Outlook Express 的安全和防范	152
5.3.1 Outlook Express 常见的漏洞	152
MIME 简介	153
5.3.2 升级 Outlook Express	155
5.3.3 Outlook Express 安全设置	155
一、“安全”选项的设置	155
二、邮件规则设置	155
5.4 WEB 信箱的安全设置	156
5.4.1 密码安全	156
5.4.2 反垃圾邮件	157
5.5 电子邮件实例	159
实例 1: Norton AntiSpam 防垃圾邮件	159
一、调整电子邮件过滤	159
二、识别授权的发件人和禁止垃圾邮件发件人	159
三、使用 Norton AntiSpam 标记垃圾邮件和正常邮件	160
四、定义 Norton AntiSpam	161
实例 2: Norton AntiVirus 2004 电子邮件防毒	162
实例 3: 对邮件的加密——数字证书的安装和使用	163
一、数字证书的用途	163
二、数字证书的获得及安装	163
三、查看数字证书	165
四、使用数字证书发送安全邮件	165
实例 4: 邮件地址泄露	166
一、导出	166
二、导入	166

第 6 章 QQ、MSN 聊天安全



6.1 QQ 工作原理和攻击防范	168
6.1.1 QQ 工作原理	168
一、QQ 的登录过程	168
二、QQ 使用的网络协议	169
三、QQ 消息收发	169
四、QQ 的 IP 地址	170
五、QQ 的端口	170
六、QQ 的 IP 地址及端口	171
6.1.2 常见安全威胁	171
一、QQ 盗号的常见手段	171
二、QQ 消息攻击的常用手法	174
6.1.3 QQ 安全措施	176
一、保持自己使用最新的 QQ 版本	176
二、清理本地记录	177
三、设置复杂密码	177
四、使用杀毒软件	178
五、使用防盗工具	178
六、申请密码保护	179
七、本地消息加密	179
八、QQ 防攻常规及参数设置	180
九、使用代理服务器隐藏自己的 IP	180
6.2 MSN 工作原理和攻击防范	181
6.2.1 MSN 的常见漏洞	181
一、MSN 简介	182
二、MSN 的已知问题	182
三、MSN 攻击事件	183
四、MSN 偷盗事件	183
五、MSN 大事记	184
6.2.2 MSN 的安全设置	184
一、使用最新版本	185
二、设置复杂密码	185
三、删除本地账户信息	185
四、阻止匿名消息	185
五、关闭远程连接	186
六、使用杀毒软件	186
七、建立良好上网习惯	186
6.3 实例	186
实例 1: QQ 尾巴病毒的防御	186
实例 2: QQ 消息本地窥探与防御	187
实例 3: QQ 消息攻击与防御	188
实例 4: 使用 QQ 防盗专家	189
实例 5: 通过密码保护功能找回 QQ 密码	189
实例 6: MSN 本地盗号与防御	190
实例 7: MSN 攻击机使用与防御	190
第 7 章 网络游戏的安全	193
7.1 概述	194
7.2 常见外挂威胁和防范	194

7.2.1 常见外挂原理	194
7.2.2 游戏厂商的反外挂	196
一、从技术核心防止外挂	196
二、引导玩家用公正的心态游戏	196
三、用法律武器打击外挂的制作	196
7.3 常见的盗号威胁	197
7.3.1 人为骗取威胁与防范	197
冒充 GM	197
7.3.2 游戏木马威胁和防范	197
传奇黑眼睛	198
7.3.3 病毒威胁和防范	198
“边峰”网游病毒	198
7.3.4 网络漏洞利用	199
一、利用操作系统漏洞	199
7.3.5 Web 欺骗威胁与防范	201
一、Web 欺骗原理	201
二、攻击者对 Web 欺骗的完善	203
三、Web 欺骗的防范	203
7.4 本地盗号威胁的防范	204

第8章 局域网安全

8.1 局域网概述	208
8.1.1 局域网的发展	208
8.1.2 局域网的原理和特性	208
8.1.3 局域网的组成	209
一、局域网的组成	209
二、局域网的几种工作模式	210
三、局域网最常见的三种拓扑结构	210
8.1.4 局域网安全概述	211
一、补丁问题	211
二、数据安全	211
三、账户密码安全	211
四、服务安全	211
8.2 文件共享安全设置	212
8.2.1 设置共享访问权限	212
一、共享文件需要满足的条件	212
二、创建共享文件	212
三、设置共享访问权限	213
四、权限累加	214
五、拒绝优先	214
六、舍大取小	214
8.2.2 实现 DFS 保护共享数据安全	214
一、分布式文件系统特性	215
二、独立的分布式文件系统配置方法	216
三、局域网的分布式文件系统的配置方法	217
8.2.3 概述默认共享的安全性	218
8.3 数据传输安全	220
8.3.1 考察局域网数据传输安全性	220



8.3.2 配置 IP Sec 实现对局域网传输数据的保护	221
一、网络认证协议	221
二、封装安全载荷协议	221
三、密钥管理协议	222
四、IPSec 的工作原理	222
五、启用 IPSec 策略	222
六、IPSec 中的身份验证	223
七、IPSec 中的传输模式的选择	224
八、IPSec 中传输数据的加密算法	225
九、在局域网中利用组策略发布 IPSec	226
十、配置 IPSec 成为防火墙	227
8.3.3 配置 EFS 保护局域网的重要数据	229
一、图形界面方式加密	230
二、命令行方式加密	231
8.4 局域网补丁分发设置	233
8.4.1 修补程序的管理流程	233
8.4.2 使用 Windows Update 管理修补程序	234
一、用户发起访问方式	234
二、自动更新方式	235
三、用户发起访问具体操作方法	235
四、自动更新具体操作方法	235
五、组策略发布 Windows Update 自动更新	235
8.4.3 使用 SUS 管理局域网补丁	236
一、SUS 的工作方式	237
二、SUS 客户端	237
三、SUS 服务端	237
8.5 实例	239
实例 1：防御 IPC\$ 带来的安全隐患	239
实例 2：检测局域网中的蠕虫病毒	241
实例 3：防御 Telnet 服务带来的安全隐患	243
实例 4：局域网防火墙构架的拓扑结构	246
一、包过滤防火墙	246
二、屏蔽主机防火墙	247
三、屏蔽子网防火墙	247
四、单目壁垒型结构	247
五、双目壁垒型结构	247
六、三目壁垒型结构	248
七、背靠背型结构	248
实例 5：配置软件限制策略，保护局域网安全	248
实例 6：管理局域网中用户，账号和密码安全	250

第 9 章 木马攻防实战

9.1 木马概述	254
9.1.1 什么是木马	254
关于木马的概念	254
9.1.2 木马的发展	255
一、第一代木马只是简单的密码窃取发送	255
二、第二代木马是网络传播性木马	255

三、第三代木马能够隐藏进程	256
四、第四代木马是反弹端口木马	256
9.1.3 传播的条件	256
一、深入敌后	256
二、神龙见首	256
三、做贼心虚	257
四、隐姓埋名	257
9.1.4 木马的危害	257
9.1.5 木马的特点	257
一、广谱感染	257
二、模块化设计	257
三、狡兔三窟	258
四、在线通知	258
9.2 木马常见的加载方式	258
9.2.1 win.ini 和 system.ini	258
9.2.2 修改注册表	259
9.2.3 捆绑文件	260
9.2.4 在 Winstart.bat 中启动	261
9.3 SubSeven 剖析与防范	262
9.3.1 EditServer.exe 设置	262
一、常规设置 (server setting)	262
二、启动方式 (startup methods)	263
三、文件捆绑 (binded files)	263
四、服务器图标和伪造出错设置 (exe icon/other)	264
五、自动通知 (notifications)	264
六、如虎添翼——插件	265
9.3.2 SubSeven.exe 设置	266
工具栏介绍	266
9.4 如何清除木马	267
9.4.1 手工删除	267
一、SubSeven 2.2	267
二、广外女生	268
三、冰河	268
四、BO 2000	268
五、初恋情人 (Sweet Heart)	268
六、Netspy (网络精灵)	269
七、WAY2.4 (火凤凰、无赖小子)	269
八、网络神偷 (Nethief)	270
九、网络公牛 (Netbull)	270
十、聪明基因	271
9.4.2 Trojan Remover 帮你忙	271
一、扫描木马	272
二、系统设置	273
9.5 实例	273
实例 1: 通过查看端口来检测木马	273
一、使用 Windows 本身自带的 netstat 命令	274
二、使用 Windows 2000 下的命令行工具 fport	274
实例 2: 中国黑客木马病毒	274

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机系统漏洞为乐趣的“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。

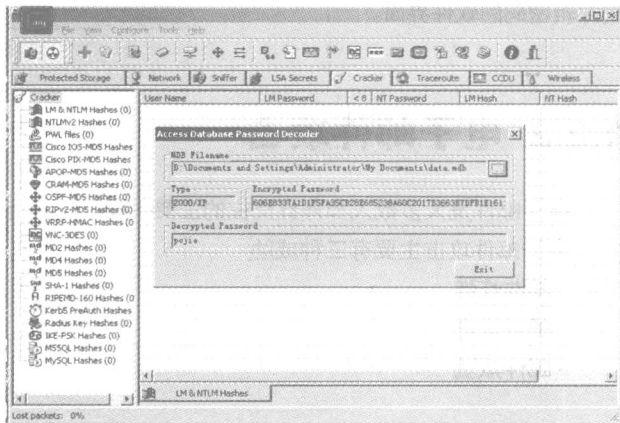


图 1-2-1 攻击者用 cain 破解 Access 数据库密码

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——这就好比给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。

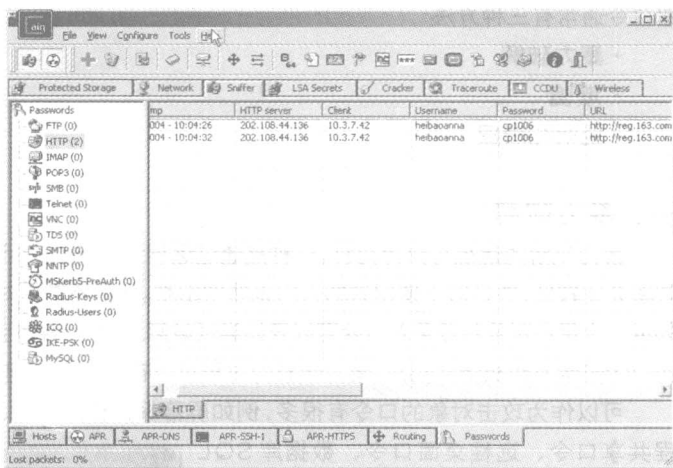


图1-2-2 利用cain可以嗅探邮箱密码

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