

搞定黑客 当好网管

仲治国 编著

网管 VS 黑客终极大练兵

想当网管，先做黑客 知己知彼，方能百战百胜！

- ① 黑客是主动的 网管是被动的
- ② 黑客就像是怪盗 网管就是侦探
- ③ 黑客能变成网管 网管也能变成黑客

暗战！恶战！！决战！！

搞定黑客 当好网管

编著：仲治国



电脑报电子音像出版社
CEAP ELECTRONIC & AUDIOVISUAL PRESS

内容提要

黑客是主动的,网管是被动的。

黑客就像是怪盗,网管就是侦探。

黑客能变成网管,网管也能变成黑客。

做一个好网管,先从做一个小黑客开始,这是被普遍认可的信条。

网管的职责之一是维护网络的安全、防范黑客的攻击,当网络出现问题时及时采取措施补救,确保网络正常运作。但这毕竟是比较被动的做法,高水平的网管应当通晓黑客攻击的各种方式,主动发现网络存在的漏洞,及时修补漏洞,化被动为主动。

虽然黑客攻击的方式层出不穷,但归结起来不外乎以下几类:获取口令、放置木马、WWW欺骗技术、电子邮件攻击、通过一个节点来攻击其他节点、网络监听、寻找系统漏洞等。一个合格的网管应该精通黑客攻击的原理,这样才能更好的防御黑客的攻击,做到知己知彼,百战百胜。

本手册就是从黑客攻击的角度出发,以实例为基础,让读者深度了解黑客攻击的各种手法与手段,从而在日常管理工作中做到处变不惊,从容面对并迅速处理各类突发事件。

警告:本手册涉及到的黑客相关知识,仅供读者学习之用,如用于非法用途,后果自负。

光盘要目

- | | |
|-----------|-----------|
| 1. IP工具 | 2. 服务器工具 |
| 3. 密码工具 | 4. 系统安全工具 |
| 5. 网络安全工具 | 6. 网络控制工具 |
| 7. 网络监测工具 | |

版权所有	盗版必究
未经许可	不得以任何形式和手段复制和抄袭

书 名: 搞定黑客,当好网管

编 者: 仲治国

责任编辑: 李志

技术编辑: 黄 斌

出版单位: 电脑报电子音像出版社

地 址: 重庆市双钢路3号科协大厦

邮政编码: 400013

对外合作: (023)63658933

发 行: 电脑报经营有限责任公司

经 销: 各地新华书店、报刊亭

C D 生产: 苏州新海博数码科技有限公司

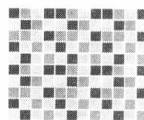
文本印刷: 重庆华林印务有限公司

开本规格: 787mm×1092mm 1/16 21.5印张 400千字

版 号: ISBN 978-7-89476-120-0

版 次: 2009年4月第1版 2009年4月第1次印刷

定 价: 38.00元(1CD+配套手册)



基础篇

第1章 网络安全与黑客攻击

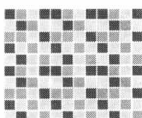
1.1 网络安全隐患所在	2	1.3.2 病毒四个特性	7
1.2 认识黑客	6	1.4 认识木马	9
1.3 认识病毒	6	1.4.1 什么是木马	9
1.3.1 病毒能做什么	7	1.4.2 木马如何利用启动项	10
		1.4.3 终结进程中的木马	14

第2章 黑客常用兵器谱

2.1 扫描探测工具	22	2.5 口令解除工具	35
2.1.1 认识扫描器	22	2.5.1 本地口令的解除	35
2.1.2 X-Scan应用实战	22	2.5.2 共享密码的解除	35
2.2 远程控制工具	23	2.6 加密解密工具	36
2.2.1 命令界面	24	2.6.1 解除Word密码	36
2.2.2 图形界面	25	2.6.2 解除邮箱密码	37
2.3 溢出工具	27	2.7 代理工具	38
2.3.1 什么是缓冲区溢出	27	2.7.1 IP的分类	39
2.3.2 溢出入侵实战演练	27	2.7.2 查找和使用代理服务器	39
2.4 嗅探监听工具	29	2.7.3 使用代理网站	41
2.4.1 什么是嗅探监听	30	2.8 拒绝服务工具	42
2.4.2 嗅探监听实战演练	32	2.8.1 DDoS Ping	43
		2.8.2 TCP连接轰炸	43

第3章 黑客与网管必知DOS命令

3.1 Arp——地址解析	46	3.3 Gettype——获得系统信息	49
3.1.1 命令语法	46	3.3.1 命令语法	49
3.1.2 命令应用实例	47	3.3.2 命令应用实例	50
3.2 Getmac——获得网卡的MAC地址	48	3.4 Hostname——显示主机名称	50
3.2.1 命令语法	48	3.4.1 命令语法	50
3.2.2 命令应用实例	48	3.4.2 命令应用实例	50



目录

搞定黑客 当好网管

CONTENTS

3.5 Ipconfig——显示TCP/IP 网络配置	51
3.5.1 命令语法	51
3.5.2 命令应用实例	52
3.6 Ipxroute——显示路由表	52
3.6.1 命令语法	52
3.6.2 命令应用实例	53
3.7 Nbtstat——显示NetBIOS配置	53
3.7.1 命令语法	53
3.7.2 命令应用实例	54
3.8 Netstat——显示网络状态	55
3.8.1 命令语法	55
3.8.2 命令应用实例	56
3.9 Ping——IP连接测试	57
3.9.1 命令语法	57
3.9.2 命令应用实例	58
3.10 Nslookup——管理DNS服务	59
3.10.1 命令语法	59
3.10.2 命令应用实例	63
3.11 Tracert——检查路由	65
3.11.1 命令语法	65
3.11.2 命令应用实例	65
3.12 Netsh——管理网络配置	66
3.12.1 命令语法	66
3.12.2 命令应用实例	68
3.13 Net——网络综合命令	69
3.14 Cmdkey——管理网络凭据	75
3.14.1 命令语法	75
3.14.2 命令应用实例	76

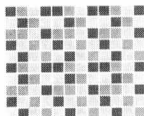
应用实战篇

第4章 黑客VS网吧网管

4.1 网吧安全概述	78
4.1.1 网吧安全问题分析	78
4.1.2 构建安全防御体系	79
4.2 ARP欺骗攻防	80
4.2.1 ARP欺骗入门	80
4.2.2 ARP欺骗实例	81
4.2.3 ARP欺骗防范	86
4.3 实例剖析QQ攻防	87
4.3.1 QQ登录保护	88
4.3.2 聊天记录防范	92
4.3.3 强行聊天防范	92
4.3.4 恶意链接防范	93
4.3.5 QQ木马的查杀	95
4.4 实例剖析网吧攻击防护	97
4.4.1 第三方漏洞攻防	97
4.4.2 突破网吧限制	98
4.5 DLL木马攻防	99
4.5.1 DLL木马攻击实例	100
4.5.2 DLL木马查杀	101

第5章 黑客VS企业网管

5.1 账户攻击与防范	106
5.1.1 账户概述	106
5.1.2 域控制器	106
5.1.3 工作站	107



目录

搞定黑客 当好网管

CONTENTS

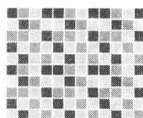
5.1.4 用命令行管理账户	108	5.3.1 邮件炸弹攻击	125
5.1.5 用受限账户提权	112	5.3.2 邮件内容拦截与防护	127
5.1.6 账户“无间道”	114	5.4 恶意程序攻防	133
5.1.7 账户的安全配置	116	5.4.1 对可疑的网络程序进行监控	133
5.2 登录环境攻防	119	5.4.2 禁止恶意程序的运行	135
5.2.1 登录密码窃取攻防	119	5.5 分区攻击与防范	136
5.2.2 网络登录攻防	122	5.5.1 病毒搞丢分区表	137
5.3 邮件安全攻防	125	5.5.2 恶意格式化分区	138

第6章 黑客VS网站网管

6.1 服务器攻防实例	142	6.3.2 网页木马入侵	153
6.1.1 服务器安全概述	142	6.3.3 设计漏洞	156
6.1.2 漏洞攻击实例	142	6.4 使用SSL保护网站	158
6.1.3 第三方组件溢出攻击	144	6.4.1 配置SSL网站	159
6.2 网站攻防基础	146	6.4.2 提交证书	161
6.2.1 网站的安全性	146	6.4.3 访问SSL网站	164
6.2.2 建站技术	147	6.5 数据库实例攻防	164
6.2.3 网站安全十个重点	149	6.5.1 初级数据库下载	165
6.2.4 IIS的安全性策略	150	6.5.2 SQL Server攻防	166
6.3 网站常见攻防实例	152	6.5.3 使用专用工具	167
6.3.1 入侵管理入口	152	6.5.4 源代码分析	168
		6.5.5 数据库防范秘技	169

第7章 黑客暴力攻击与网管防御

7.1 网络炸弹	172	7.4 MSN消息攻击机	178
7.1.1 炸弹的分类	172	7.4.1 MSN消息攻击实战	178
7.1.2 OICQ炸弹攻击实战	172	7.4.2 如何防范攻击	178
7.2 IP炸弹工具IP Hacker	175	7.5 邮箱炸弹的攻防	179
7.2.1 IP Hacker简介	175	7.5.1 初识邮箱炸弹	179
7.2.2 Windows 98攻击	175	7.5.2 邮箱炸弹的防范	180
7.2.3 Windows NT攻击	176	7.6 Printer溢出工具IIS5Exploit	181
7.3 亿虎Email群发大师	176	7.6.1 什么是溢出	181
7.3.1 认识亿虎Email群发大师	176	7.6.2 printer溢出攻击实战	181
7.3.2 邮件群发实战	177	7.7 IDQ攻击溢出工具	182
7.3.3 邮件炸弹的防范	178		



目录

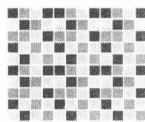
搞定黑客
当好网管

CONTENTS

7.7.1 漏洞初识	182	7.11.1 AtGuard简介	188
7.7.2 入侵IDQ漏洞	182	7.11.2 让烦人的弹出窗口永远消失	189
7.7.3 防范对策	183	7.11.3 定制网络程序	190
7.8 RPC溢出工具	183	7.12 浏览器绑架克星HijackThis	191
7.8.1 漏洞初识	183	7.12.1 系统检测	191
7.8.2 入侵实战	184	7.12.2 编号识别	192
7.8.3 防范方法	185	7.13 揭秘DD.O.S攻击	193
7.9 Windows logon溢出工具	185	7.13.1 拒绝服务攻击原理	193
7.9.1 漏洞初识	185	7.13.2 拒绝服务攻击类型	193
7.9.2 远程溢出实战	186	7.13.3 远程控制与拒绝服务	194
7.9.3 漏洞防范	186	7.13.4 拒绝服务攻击实战	195
7.10 用Google Toolbar解除恶意绑架	187	7.13.4 DD.O.S防御	196
7.10.1 Google Toolbar简介	187	7.14 跳板攻击	198
7.10.2 解除绑架实战	187	7.14.1 实现一级跳板	199
7.11 防暴专家AtGuard	188	7.14.2 实现二级跳级	200

第8章 黑客控制与网管反控制

8.1 远程强制开启对方视频	202	8.5.7 远程关机	212
8.1.1 木马设置	202	8.6 远程自动截取屏幕	212
8.1.2 开启远程视频	203	8.6.1 屏幕间谍简介	212
8.1.3 服务器端清除	203	8.6.2 设置参数	212
8.2 妙用冰河陷阱防控制	203	8.6.3 截取效果	213
8.2.1 冰河陷阱简介	204	8.7 用灰鸽子透过局域网进行远程管理	214
8.2.2 清除冰河木马	204	8.7.1 灰鸽子简介	214
8.2.3 诱骗黑客	205	8.7.2 生成服务器端	214
8.3 用WinVNC远程控制	206	8.7.3 查看控制效果	215
8.3.1 配制服务器	206	8.7.4 卸载灰鸽子	215
8.3.2 客户端连接	207	8.8 用URLy Warning监控远程信息	217
8.4 使用WinShell实现远程控制	207	8.8.1 软件简介	217
8.4.1 WinShell简介	207	8.8.2 监控远程信息	217
8.4.2 配置WinShell	207	8.9 用Simple Bind自制远程控制程序	218
8.4.3 制定计算机运行	209	8.9.1 合并EXE文件	218
8.5 使用QuickIP进行多点控制	209	8.9.2 修改合并后的EXE文件的图标	218
8.5.1 QuickIP能做什么	209	8.10 实战远程控制好帮手PcAnywhere	219
8.5.2 设置服务器端	210	8.10.1 PcAnywhere的安装	219
8.5.3 设置客户端	210	8.10.2 PcAnywhere的基本设置	219
8.5.4 查看远程驱动器	211	8.10.3 应用远程控制功能	220
8.5.5 远程屏幕控制	211		
8.5.6 查看远程计算机进程	211		



目录

搞定黑客当好网管

CONTENTS

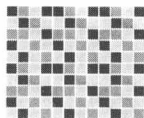
第9章 黑客嗅探与网管监控

9.1 局域网的嗅探	224	9.4 利用NetXray嗅探查找网络故障 ...	230
9.1.1 什么是嗅探	224	9.4.1 NetXray简介	230
9.1.2 嗅探窃密是怎么进行的	224	9.4.2 嗅探查找网络故障	230
9.1.3 嗅探可能造成的危害	225	9.5 SpyNet Sniffer网络监听	232
9.1.4 破解FTP口令	225	9.5.1 播放音乐或视频	232
9.2 利用Iris嗅探监控网络	226	9.5.2 捕获下载地址	232
9.2.1 捕获数据	226	9.6 艾菲网页侦探监控网页	233
9.2.2 分析数据	227	9.6.1 基本设置	233
9.2.3 信息过滤	227	9.6.2 网页内容捕获	233
9.2.4 流量测试	227	9.6.3 下载软件的监控	234
9.3 Project URL Snooper嗅探影片 ...	228	9.7 网管助手Sniffer Portable	234
9.3.1 基本功能	228	9.7.1 安装要点与基本设置	234
9.3.2 软件的配置	228	9.7.2 数据捕获	236
9.3.3 搜索影片下载地址	228	9.8 无线嗅探器之NetStumbler	236
9.4 影音神探嗅探影音	229	9.8.1 无线安全很重要	236
9.4.1 初识“神探”	229	9.8.2 无线嗅探器实战	237
9.4.2 基本设置	229	9.8.3 拒绝笔记本ad-hoc方式接入	238
9.4.3 影片下载实战	229		

网管防线篇

第10章 严密部署权限防线

10.1 权利指派	240	10.3.2 访问控制列表 (ACL)	254
10.1.1 识别权利	240	10.3.3 安全主体 (Security Principal) ...	254
10.1.2 基本的权利指派	243	10.3.4 安全标识符	254
10.1.3 高级权利指派	246	10.3.5 访问令牌 (Access Token)	254
10.2 共享权限	248	10.3.6 安全描述符	255
10.2.1 认识共享权限	248	10.3.7 复制与移动时的权限变化	256
10.2.2 共享权限设置	249	10.4 四项权限原则	256
10.2.3 防火墙与共享权限的关系	251	10.4.1 拒绝优于允许原则	256
10.3 “安全” 权限基本知识	253	10.4.2 权限最小化原则	257
10.3.1 如何激活“安全”选项卡	253	10.4.3 权限继承性原则	257
		10.4.4 累加原则	258



目录

搞定黑客
当好网管

CONTENTS

10.5 NTFS权限的设置258

10.5.1 设置基本的NTFS权限 258

10.5.2 设置特殊的NTFS权限 259

10.5.3 所有权管理 261

第11章 账户的安全管理

11.1 账户基本知识264

11.1.1 账户概述 264

11.1.2 账户的分类 264

11.1.3 内置账户 266

11.1.4 账户组 268

11.2 账户管理工具269

11.2.1 本地用户和组 269

11.2.2 命令行 274

11.2.3 注册表编辑器 279

11.3 账户的安全配置279

11.3.1 账户的安全操作准则 279

11.3.2 账户密码的管理 280

11.4 深入解析账户登录安全283

11.4.1 账户登录系统的过程 284

11.4.2 本地登录的过程 287

11.4.3 域登录 287

11.4.4 网络登录 288

11.4.5 服务登录 290

11.5 配置文件的类型292

11.5.1 本地账户配置文件 292

11.5.2 漫游账户配置文件 294

11.5.3 强制账户配置文件 294

11.5.4 临时用户配置文件 294

第12章 远程访问安全配置

12.1 远程桌面304

12.1.1 什么是远程桌面 304

12.1.2 启用远程桌面功能 304

12.1.3 账户的安全分析 305

12.1.4 使用远程桌面功能 305

12.2 终端服务器306

12.2.1 什么是终端服务器 306

12.2.2 终端服务器的建立 307

12.2.3 用组策略进行安全配置 309

12.2.4 终端用户权限的设置 310

12.2.5 终端服务器的日志审核 311

12.3 Web接口管理312

12.3.1 远程管理打印服务器 312

12.3.2 终端服务器之Web接口管理 316

12.3.3 远程维护Web接口 317

12.3.4 Web连接的安全概要 320

12.4 配置VPN服务321

12.4.1 配置VPN服务器 322

12.4.2 添加权限账号 323

12.4.3 配置VPN客户端 324

12.4.4 拨入VPN服务器 325

12.5 远程管理注册表326

12.5.1 远程编辑注册表 326

12.5.2 安全配置 327

12.6 远程管理组策略328

12.6.1 什么是组策略 329

12.6.2 组策略的结构 329

12.6.3 远程管理组策略 332



第1章

网络安全与黑客攻击

无论是个人 PC, 还是各种网络中的服务器与工作站, 都无法对“安全”这个话题进行回避。特别是随着网络用户的不断倍增、黑客工具与病毒的泛滥, 更是让网络中的安全问题日趋严重——当邮件的内容被偷窥、经商创业的内容被窃取、即时通信中附带病毒、影音娱乐中内藏木马、辛苦编就的文件被恶意删除、电脑应用变得没有安全保障时, 人们开始“谈网色变”。

网络应该是为电脑添加了腾飞的翅膀, 进而成为生活中的一种时尚。可是, 安全问题的悄然来临, 让我们的生活与工作产生诸多不和谐的因素。没有人喜欢用电脑时还有一双眼睛在远程监控你, 没有人愿意自己的电脑慢如蜗牛, 没有人会同意自己的电脑被别人如入无人之境……

在网络环境中, 各种安全隐患是屡见不鲜、防不胜防, 无数的网管员都在为之头疼。对于很多初、中级网管员来说, 如果哪天无人求救, 那天才是真正的休假。否则, 很多休假的日子也会被一个个电话召了回去。

在本章中, 将以中小网络网管员的视角, 谈谈如何面对各种常见的安全问题, 以便让复杂的安全问题条理化, 让脆弱的防御策略堡垒化! 让大家对黑客和网络安全有个全面的认识。



1.1 网络安全隐患所在

十几年前，我们使用的网络大部分是同轴电缆组成的网络，网络出现的问题不外乎就是网络不通。网管要做的任务就是花上几分钟整理一下网线或是网络协议。可是，如今的网络环境早已是日新月异：双绞线、光纤、具有网管功能的交换机、操作复杂的路由器、设置繁琐的网关、功能迥异的服务器，要求熟练运用的技术太多。在这一切已经足以让初、中级网管员头痛的时候，防不胜防的黑客和病毒却又如潮水般涌来……棘手的问题一个接一个，怎是一个“烦”字能说得清？

很多个人电脑用户在谈到网络安全时都不能理解：为什么我只是一个普通的个人电脑用户，却会有这么多莫名其妙的“黑客”对我感兴趣？

其实原因很简单：现在网络上泛滥的黑客工具使任何一个网民都可以随手而得。很多新手喜欢使用扫描类工具对某一 IP 地址段进行大规模的端口扫描，利用这些工具来发现网络上的具有安全隐患的主机，然后再逐个进行入侵或攻击。其实他们在进行扫描之前根本就不知道你究竟是谁。这也就是为什么个人电脑用户屡屡发生安全问题的根本原因。

那么，为什么企业也会有各种各样的安全问题呢？这是因为企业的“出口”太多，每一台电脑都开放了 N 个端口，都在不停地进行着各种应用，这些都会或多或少地与网络安全“挂上钩”。例如，某台电脑中了蠕虫病毒后，当他将电脑中的文件发送给局域网中的同事时，同事的电脑就会被感染，如图 1-1 所示。



图1-1 网络中的每一台电脑都可能是病毒的传播者

当然，稍微“高级”些的病毒就会自动在网络中进行自身的传播——这种“无色无味”的“毒药”基本上是中者必失。所以，网络管理员应该对网络中的每一台电脑都进行把关，例如，要求每一台电脑都要安装杀毒软件等等。一般来说，网络主要面临如下几点安全隐患：

1. 病毒的感染

俗话说得好：“病来如山倒，病去如抽丝。”如果电脑感染了病毒，轻则软件“发烧感冒”，重则连硬件都会遭受破坏。病毒让电脑来个“一病不起”的事儿已是屡见不鲜！

病毒一般具有隐藏性、潜伏性、传染性、破坏性等特点，通常条件好的网络会使用硬件级病毒过滤设备，如图 1-2 所示。



图1-2 网关过滤设备

一般性的网络则会依靠网络版杀毒软件来完成病毒的防御任务，如图 1-3 所示。因为网络规模有多种，所以，网络版杀毒软件也会分为好几种版本，不同版本的杀毒软件不仅设计理念不一样，在功能上、使用上都有很多的不同之处。



图1-3 网络版杀毒软件

2. 黑客的入侵与攻击

与病毒程序相伴相随的就是黑客程序了，它的出现虽然要比病毒程序晚许多，其盛行只是近几年随着计算机网络的普及才开始的，但是它的威胁性和破坏性比病毒更大。

黑客一般会使用三种方法入侵目标电脑，一是使用各种方法向对方电脑植入木马程序，只要

对方上线自己就会立即知道并进行遥控，如图 1-4 所示。

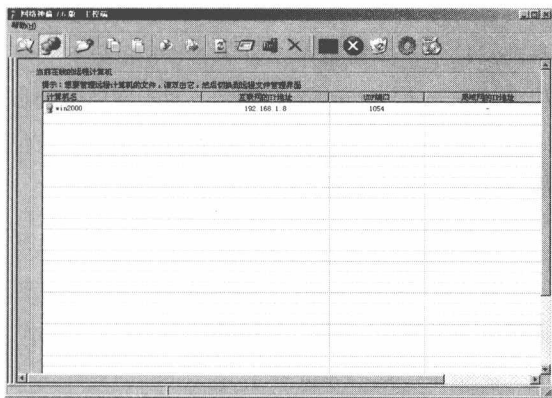


图1-4 服务器端上线

二是扫描目标电脑是否存在什么漏洞，如果存在漏洞——网络中的电脑如果不经专门的漏洞修补的话，基本上每一台电脑都会存在问题，如图 1-5 所示。



图1-5 Windows XP 单机中的常见漏洞列表

很多企业的网管员只在服务器上进行漏洞修补，却忽略了单机的漏洞问题，让黑客有机可乘，这也是安全管理体系上的一个不足。

三是目前攻击效果仍是排在前列的 DDoS（分布式拒绝服务攻击），这种攻击方法是持续使用大量的数据包攻击目标，目的是使目标主机的被访问能力严重下降，如图 1-6 所示。

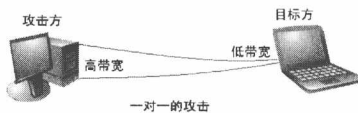


图1-6 DoS攻击方式

在网络中，只有服务器会受到这种攻击，单机一般不会受到这个问题的困扰。但是，由于服务器和单机是使用同一个 Internet 接口，所以，当 Internet 带宽受到严重影响时，单机的 Internet 应用自然也会受到影响。

网络解决这个问题的方法，一般有两种：一是购买硬件防火墙，如图 1-7 所示。

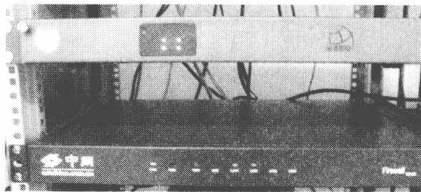


图1-7 硬件防火墙

二是使用软件防火墙，把监测到的攻击 IP 地址屏蔽掉，即丢弃这些发来的数据包，这样也可以起到一定的防御作用，但是效果一般。

事实上，黑客入侵有两种方式，一种网络入侵，还有一种就是本地入侵。后者的使用量甚至还要大于前者，而且也较前者更容易入侵成功。例如，本地入侵中的“输入法漏洞”，就可以让黑客轻松获得 Vista 系统的管理权限。所以，网管员不仅要网络通道严加防范，还应对机房的使用人员进行相应规章的制定。

病毒程序的设计目的大多数都是搞破坏，黑客程序的设计目的则是“深入敌后”，把目标电脑的控制权拿下来，以便获得各种所需的资料。因此，黑客行为或工具一般不具备破坏性，因为把系统破坏了，自己也就没得用了。



3. 账户密码设置不当

对于一台电脑来说，账户就是它的主人姓名，密码就是主人的钥匙。账户是必需存在的主体，密码虽然可有可无，但是没有密码就表示给了黑客一把万能钥匙——推开系统的大门就可以了。这样的电脑安全性毫无保障，即使安装了强大的防黑杀毒的软件也无济于事。所以，默认状态下，在 Windows XP/2003 等系统的组策略中已经禁止使用“空密码”进行远程登录了，如图 1-8 所示。

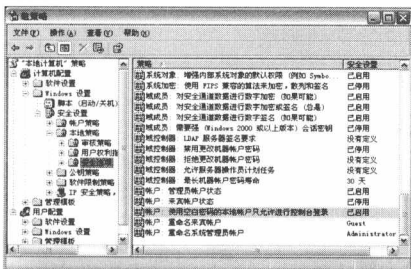


图1-8 组策略设置

4. 权限设置不当

所谓“权限”(Permission)，是指用户对于对象的访问限制。例如，能否新建、读取、删除对象。对象的种类包括文件、文件夹、分区、磁盘和打印机等等，如图 1-9 所示。

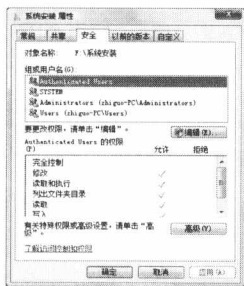


图1-9 权限设置列表

设置权限是以对象为基础，即“设置某个对象有哪些用户可以拥有相应的权限”，而不能是以用户为主，即“设置某个用户可以对哪些对象拥有权限”。这就意味着“权限”必须针对“对象”

而言，脱离了对对象去谈权限毫无意义——在提到权限的具体实施时，“某个对象”是必须存在的。

以文件夹与文件的权限为例，依据是否被共享到网络上，其权限可以分为 NTFS 权限与共享权限 (Shared Permission) 两种。对于网络管理员来说，要清楚地知道权限在网络访问通道中的位置、作用与常见问题。

5. 邮箱被破解或邮件被拦截

对于企业网络来说，邮箱被破解或邮件被拦截都是一个属于“严重”级的问题，如图 1-10 所示。因为邮箱中一般有合同样本等重要的商业秘密或者是个人隐私。这些资料是不能外泄的，否则可能会给企业的运作上带来被动。

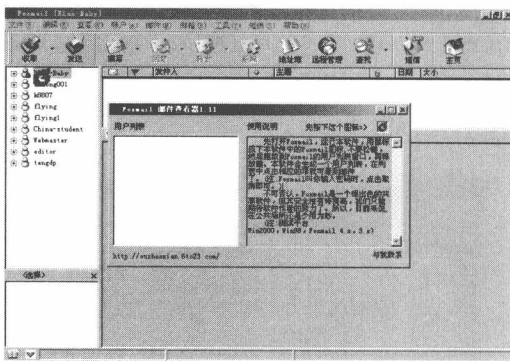


图1-10 Foxmail的邮箱被破解

网管员应该从多个角度对邮箱问题进行防范，有条件的可以通过硬件设备过滤一些包含木马等病毒的邮件，否则可以从软件角度上进行一些防范，如使用 PKI 技术等。

6. 操作系统漏洞

有很多企业网管员只对服务器的系统漏洞加以重视，却忽略了单机的系统漏洞。其实，很多时候面向公众的服务器里提供的反而是不重要的普通资料，有些高级企业管理人员私人电脑中的资料才是企业运行的“核心”内容。因此，对于网管员来说，最好是使用域环境对整个网络的电脑进行统一管理，如统一安装补丁，等等。

什么是系统漏洞？系统漏洞就是 Windows 本身因设计缺陷产生的安全问题。系统漏洞是一个永远不会终结的问题，我们不要期望系统的漏洞能彻底修补好，因为系统漏洞永远是“此补彼现”，如图 1-11 所示。

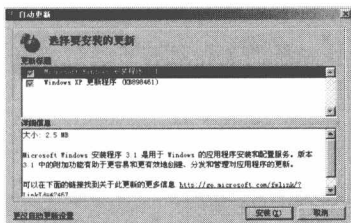


图 1-11 检测到的系统漏洞

7. 文件的非法访问

在电脑中进行的一切数据处理操作都是以文件为基础的。例如，用 Word 编辑了一份文档文件，用“录音机”录制了一个声音文件，用摄像头拍了一幅图像文件，等等。

在企业环境中，有很多数据（如编写的商业合同文件）是不希望被别人随意查看内容的，对于这样的文件可以使用加密的方法进行保护。因此，网管员应熟悉文件夹、文件、克隆文件等重要数据的常见加密与解密方法，并对 EFS 这些系统加密功能加以了解。

8. 交换设备设置不当

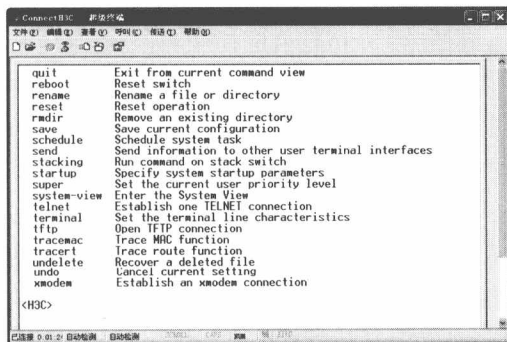


图 1-12 通过终端配置交换机

在网络的中央节点设备中，路由器和交换机

等都是具有网管功能的，对于没有彻底掌握含义的功能最好不要乱设置，因为一不小心把默认的标准策略设置为宽松策略，那么网络就可能面临入侵等糟糕的问题，如图 1-12 所示。

9. 数据存储介质损坏、丢失或维修时泄密

数据可能会因很多原因泄密，其中硬盘、光盘、优盘等存储介质出现损坏、丢失和维修现象时，最容易泄密。特别是对硬盘进行维修时，维修的时间往往需要等待几天，在这个过程中很容易就把数据弄丢或被复制。要解决类似的问题，需要对重要的数据进行加密和备份，并且最好能在有实力、有信誉的维修处目睹维修过程，慎防数据被恶意拷贝。

10. 第三方程序漏洞，如 Serv-U、网站程序等

除去了操作系统外，网管员经常需要在电脑中安装第三方软件，并使用它们（如 Serv-U）与 Internet 进行数据交互，此时，就要谨防这些软件带有安全问题——没有百分百安全的操作系统，也不会有百分百安全的软件。

那么，系统漏洞和应用软件漏洞有什么不一样？要弄明白这一点，需要先搞清楚软件的分类。在电脑软件中，软件可以分为系统软件和应用软件两大类。所谓应用软件（俗称“应用程序”），是指专门为解决各类实际问题而开发的程序，比如，Word 可以提供文字编辑功能，WinRAR 可以提供压缩与解压缩功能，迅雷可以帮助用户从网络中高速下载软件，等等。

那么，如 Windows XP/2003、Vista 之类的操作系统是应用软件吗？答案是：NO！这是因为 Windows XP/2003、Vista 是属于“系统软件”类。一台没有安装软件的电脑通常被称之为“裸机”，裸机需要安装操作系统来运行。操作系统可以完成一系列底层硬件的基本调度，以及提供一些基本功能，例如，开机与关机功能、电影与音乐的播放、文字输入与打印，等等。



但是，由于这些功能都比较简单，所以很多时候为了满足更多的需求，我们就需要为电脑安装一些专业的应用程序来协助工作。例如，由于 Vista 中的文本编辑功能只支持简单的文本编辑，所以，可以通过安装专业的文本编辑软件 Word 来完成复杂的文档编辑。

通过裸机、操作系统和应用程序形成的三层结构，就可以实现电脑中各种各样的功能调用了，如图 1-13 所示。



图1-13 硬件、操作系统与应用软件的结构

显然，裸机是操作系统的平台，而操作系统则可以看成是应用软件的平台。其中，应用程序处于最上端，它离开了操作系统和裸机将无法使用。这就好比演员与舞台的关系，演员必须在平稳的舞台上才能表演，而应用程序也必须在稳定的操作系统中才能执行安装和运行。

通常，在购买个人电脑时第一件要做的事情就是安装 Windows XP、Vista 等操作系统。操作系统是所有软件中最重要的组成部分，它为软件与硬件之间“搭”起了一座交流的“桥”。作为电脑中的软件平台，黑客工具和安全软件都需要操作系统的支持才能运行。

系统漏洞与软件漏洞通常互相影响，例如，系统出现了漏洞，黑客并籍此控制了电脑，那么电脑中的一切应用软件的控制权自然也就拱手送人。

1.2 认识黑客

在这个瞬息万变的效率时代，我们与高科技产物——电脑的接触越来越多，在电脑为我们带来高效运作的同时，无所不在的黑客也同时带来了大量的安全隐患。

什么是黑客？首先要说的是，黑客（Hacker）技术其实是网络安全技术的一部分，是一种从操作系统安全分析的角度进行系统完善的技术。所以，从正面来看可以认为黑客就是研究网络安全技术的一个技术群体，他们大多都是程序员出身，对于操作系统和编程语言都有着深刻的认识，乐于探索操作系统的奥秘且善于通过探索了解系统中的漏洞及其原因所在，他们恪守这样一条准则：“Never damage any system”（永不破坏任何系统）。他们近乎疯狂地钻研更深入的电脑系统知识并乐于与他人共享成果，他们一度是电脑发展史上的英雄，为推动计算机的发展起了重要的作用。例如，Linux 就得益于很多黑客的不懈努力才有了今天的成就。

显然，“黑客”一词原来并没有丝毫的贬义成分。直到后来，少数怀着不良企图的人，他们技术或许很好，也可能只是对技术一知半解，他们专以非法侵入他人网站、恶意破坏电脑中的数据为乐。这类群体就是被人们所了解、所警惕的“Cracker”一族，也就是“骇客”技术。本书中如果有“防范黑客破坏”等用语，其实指的就是这类伪黑客，并非是针对专心研究网络安全技术的黑客而言。

1.3 认识病毒

在网络中，网管员每天都可能与之打交道的安全隐患有三种，即：病毒、木马和恶意代码。对于网管员来说，病毒是头号大敌！病毒（Virus）是六亲不认的，不论是谁都有可能“与毒共舞”。如果是电脑不巧碰上了病毒（这种机会基本上是人人有份，决不落空），用户通常就会手忙脚乱，不知所措。国内用户认识病毒大多始于 1989 年初“大连市统计局的计算机上发现有小球计算机病毒”的报道，如图 1-14 所示。从此以后，计算机病毒以极其迅猛之势在中国大陆蔓延。

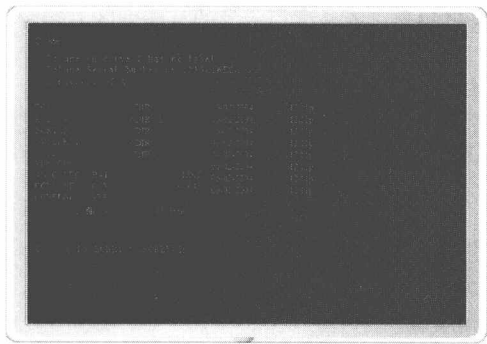


图1-14 小球病毒演示



在“<http://bbs.duze.net/downxx.asp?id=82>”中提供了江民杀毒科技关于此病毒的演示文件和病毒源代码供读者们参考。

那时，大家都在使用 DOS 操作系统（“DISK Operation System”，中文译为“磁盘操作系统”）。由于杀毒软件尚未普及，造成了小球等病毒的大量传播。后来，又有了中央电视台都报道过的 CIH，使得全国计算机用户都对病毒有了一定的了解。

1.3.1 病毒能做什么

病毒究竟是什么？其实病毒也是一种软件（程序），只不过它的功能是搞破坏罢了。那么，为什么称其为病毒？首先，它与医学上的“病毒”有着本质的区别，它不是天然存在的，而是某些计算机程序员利用计算机软、硬件所固有的脆弱性，编写的具有特殊功能的程序。由于它与生物学上的“病毒”同样有传染和破坏的特性，因此这一名词是由生物学上的“病毒”概念引申而来。病毒一旦进入计算机并得以执行，它会搜寻符合其传染条件的程序或存储介质，确定目标后再将自身插入其中，达到自我繁殖的目的。

那么，病毒究竟能做什么呢？下面，列举了

病毒常会去完成的“任务”：

- (1) 大量占用磁盘的可用空间。
- (2) 大量占用 CPU 和内存的可用资源。
- (3) 让系统发出其特定的声音和显示特定的图像等。
- (4) 让 Windows 无法启用或是正常使用。
- (5) 疯狂删除系统及各类文件，让系统崩溃或让用户丢失重要数据。
- (6) 传播自身或其他病毒。
- (7) 盗取用户账号及密码等信息。
- (8) 破坏硬件，如大名鼎鼎的 CIH 病毒。
- (9) 将杀毒软件破坏掉，以便让黑客程序进驻。
- (10) 恶意修改用户的各种设置，如 IE、注册表……

显然，病毒能做的事儿还真就不少。其实，病毒并不可怕——只要我们肯练好查毒和杀毒的“基本功”，就一定能将病毒赶出系统。当然，只要感染了病毒，或多或少系统都会有点损失，例如，数据被恶意删除、系统文件被恶意更换、IE 和注册表被胡乱修改了等等。所以说，最好不要中毒，一旦中了毒，就别老想着“出病毒而不染”——如果病毒能如此善良，那它也别叫病毒了。

1.3.2 病毒四个特性

计算机病毒是能够通过某种途径潜伏在计算机存储介质（或程序）里，当达到某种条件时即被激活，从而对计算机资源进行破坏的程序或指令集合。它具有四个基本特性，即：破坏性、传染性、潜伏性和隐蔽性。

1. 破坏性

80% 以上的病毒具有破坏性，例如，可以自动格式化硬盘、删除系统核心文件等等。象 CIH 等病毒还可以对硬件进行影响，所以，与病毒打交道，要以预防为主，杀除为辅。因为有些文件一旦被感染，就不能再轻易地恢复了，通常只能



使用新的文件进行替换。

例如，“熊猫烧香”等病毒可以终止大量的反病毒软件和防火墙软件进程，会强行删除扩展名为“gho”的文件，使用户无法使用 Ghost 软件恢复操作系统。

2. 传染性

98% 以上的病毒具有传染性，如臭名昭著的 Funlove、熊猫烧香病毒就会瞬间感染系统中所有符合感染条件的文件，在如图 1-15 所示中可以看到感染了“兔宝宝”病毒后，所有的 exe 文件图标就会都变成兔子图标。

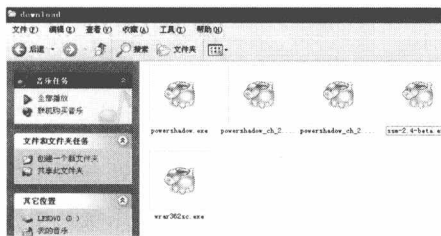


图1-15 感染“兔宝宝”病毒后

病毒具有“传染性”，这意味着它只要有机会就会到处进行传播。是否具传染性，是判别一个程序是否为病毒的最重要条件。

3. 潜伏性

“潜伏性”也是病毒的基本特性之一，目的就是让人们不易发现它。我们可以将其视为“定时炸弹”，因为病毒随时都可能因为某个条件被满足而爆发——病毒使用的触发条件主要有以下三种：一是利用主板上的时钟提供的时间作为触发器，这种触发条件被许多病毒采用，触发的时间有的精确到百分之几秒，有的则只区分年份。二是利用病毒自带的计数器作为触发器，病毒利用计数器记录某种事件发生的次数，一旦计数器达到某一设定的值，就执行破坏操作。三是利用计算机内执行的某些特定操作作为触发器，特定操作可以是用户按下某种特定的组合键，也可以是执行

格式化命令，或是读写磁盘的某些扇区，等等。



有些病毒还可能会悄悄地在系统中发生作用，只是我们很少会轻易地觉察到。例如，有的木马病毒会先把杀毒软件 KILL 了，让其表面上还处于运行状态，实际上已经不起作用，进而满足“潜伏”的需求。

4. 隐蔽性

计算机病毒刚刚开始出现时，由于人们对这种新生事物的认识不足，所以，计算机病毒不需要刻意地采取什么隐蔽技术也能达到广泛传播的目的。当人们越来越了解计算机病毒，并有了一套成熟的检测病毒的方法时，病毒要想广泛传播开来，就必需能够躲避现有的病毒检测技术，以便不被人们发现。例如，弹出一个图片让你欣赏时，病毒在悄悄传播。不过程序代码分析或计算机病毒代码扫描，病毒程序与正常程序是不容易被区分的。

通常，在遇到上述的这些情况时，不管杀毒软件是否报警，都要警惕系统中是否有病毒在运作。



不驻留内存的病毒是一种立即传染的病毒，每执行一次带毒程序，就主动在当前路径中搜索，查到满足要求的可执行文件即进行传染。该类病毒不改动系统的任何状态，因而很难区分当前运行的是一个病毒还是一个正常的程序。驻留型病毒的不同在于它常驻在内存中，它先窃取系统控制权，接着等待系统运行其他程序时进行感染。

设计完善的病毒往往会很好地隐蔽自己，从而可以争取较长的存活期并造成大面积的感染、造成大面积的伤害。例如，有的使用汇编语言编写的大型病毒仅仅只有 2KB 不到，这使得它更容易地在硬盘等存储介质、内存中隐藏自己，甚至