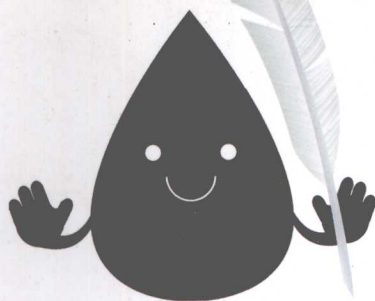




电脑迷

荣誉出品



黑客

入侵手记

- 这是一名黑客的入侵日记，日记详细披露了作者参与经典战役的全过程和心得体会。
- 本书从研究黑客技术、黑客心理与主动防御的角度出发，让黑客应用真正得其门而入。

肖遥 编著

入侵

成功

失败 → 思考

换种方式入侵

成功

失败 → 再思考……成功

牧「马」记

“诱惑”——免费电影网站挂马
暗夜追踪，打开黑客之门
网络“恐龙”大揭密

软件破解

强力爆破，偷窥MM日记
此地无银三百两，软件自爆注册码
稀奇古怪，破解Flash

局域网入侵

破解与克隆，偷玩抠门同学电脑
一波三折的公司网管提权经历
嗅探大丰收，全权控制网络

攻陷网吧

突破限制，行遍网吧无疆界
饭钱节省有道，PUBWIN免费网吧上网

远程入侵

艰难的抓“鸡”历程，TCP/IP过滤突破记
拐弯抹角，渗透信息港网站服务器
接受挑战，盗Q之旅

网站入侵

SQL注入闯关记
网投任我玩，帮助MM刷票
入侵网上商城，免费购物
BT服务器的人侵控制

IM 电脑迷 荣誉出品



黑客

入侵手记

肖遥 编著

光盘导读

特别说明

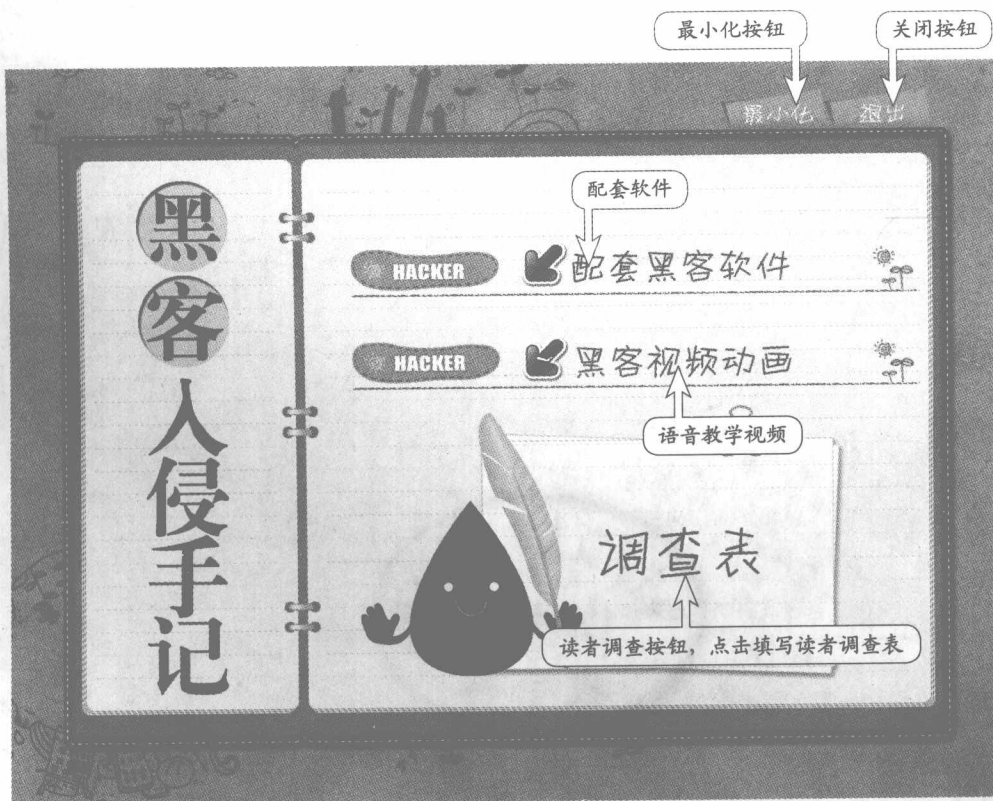
本光盘提供的黑客软件和视频仅供技术研究使用，切勿利用来破坏他人的计算机或数据，否则一切后果自负。

光盘使用说明

将本光盘放入电脑光驱中，光盘会自动运行。如没有自动运行，可以打开“我的电脑”，用鼠标右键单击光驱所在盘符，在弹出菜单中选择“自动播放”即可。

光盘主界面

光盘启动后会打开光盘主界面，具体操作如下图所示：



目录



CONTENTS

注：本目录中凡标有  的章节均在光盘中有全程配音的教学视频

1 局域网入侵

8月3日 晴

内存泄密，机房电脑无限制 1

- 一、内存截取，有些失败2
 - 1. 获取管理员登录进程ID
 - 2. 获取管理员登录密码
- 二、换工具，2003吐密码4
- 三、查看常用密码4

9月7日 阴

IP冲突引发的局域网攻击 6

- 一、揪出IP冲突攻击者信息7
 - 1. 终止IP冲突攻击
 - 2. 追踪攻击者MAC地址
 - 3. 查出攻击者主机名
- 二、以其之道还治其人之身9
 - 1. 安装WinPacapy协议
 - 2. “长角牛”发怒
- 三、戏耍攻击者10
 - 1. 创建监控网段
 - 2. 扫描主机目标
 - 3. 创建攻击策略
 - 4. 网速慢如蜗牛
 - 5. 想下载？没门！
 - 6. 网页、聊天都别想！
- 四、ARP欺骗，栽赃攻击者17
 - 1. 确定伪装者和攻击目标
 - 2. 伪装嫁祸攻击者
 - 3. 执行攻击

7月12日 晴

破解与克隆，偷玩抠门同学电脑 19

- 一、初试失败，“蕃茄”失效20
 - 1. 光盘引导系统
 - 2. 简单破解密码

二、还原SAM文件也失效	22
三、PE系统与暴力破解syskey密码	23
1. 安装进入Windows PE系统	
2. 使用SAMinside破解SYSKEY双重密码	
四、巧留后门，随时进出	28
1. 查看管理员与GUEST账户SID	
2. 导出管理员账号注册表配置	
3. 修改配置进行克隆	

8月20日 晴

局域网资料任我取 30

一、局域网入侵秘密隧道——Recton	31
1. 远程开启3389，拷贝图形界面	
2. 远程桌面连接	
3. 远程桌面文件传输	
二、灰鸽子显神通，轻松拷回文件	33
1. 关闭防火墙与杀毒软件	
2. 配置灰鸽子木马文件	
3. 远程共享上传木马	
4. 远程执行木马	
5. 自动远程种植木马	
6. 远程拷贝文件	
7. 清除记录	
三、遍网共享轻松破	38
1. 局域网超级工具搜共享	
2. 强力破解共享密码	

10月15日 晴

公司中一波三折的提权经历 41

一、初试CSRSS本地溢出提权	41
1. CSRSS本地溢出漏洞简介	
2. 简单溢出，管理员轻松拿	
二、再试WIN键盘提权	43
1. WIN键盘提权ABC	
2. 查看“explorer.exe”进程PID	
3. 溢出	
4. 连接溢出端口	
三、“secdrv.sys”新漏洞，有奇效	45
1. secdrv.sys 本地权限提升漏洞简介	
2. 提权留后门	
四、让后门更隐蔽	47
五、彻底玩转公司电脑	48

11月16日 雨

嗅探大丰收，全权控制公司网络 50

一、局域网嗅探，密码无处可逃	50
二、远程克隆，在服务器上开道门	52
1. 开启远程肉鸡的IPC\$	

2. 设置克隆账号及密码

3. 远程克隆管理员账号

三、嗅探隐无踪54

1. 安装嗅探工具到远程主机

2. 轻松嗅探FTP密码

3. POP/SMTP/HTTP密码统统嗅

4. 嗅探指定端口的密码数据

11月6日 雨

千里耳，嗅听惊天秘密 58

一、无聊人的无聊信息58

1. 配置网卡信息

2. 轻松嗅探MSN信息

二、设个陷阱捉网管60

1. 嗅探网卡设置

2. 让嗅探悄悄进行

3. 外出办事，自动嗅探

12月23日 小雪

正义之战，两败俱伤 62

一、“黑”掉公司主页62

1. 入侵准备

2. ARP欺骗设置

3. 开始欺骗攻击

二、黑客就是要狠一点65

1. 制作网页木马

2. ARP挂马攻击

己 远程入侵

3月13日 晴

校园网之洞，开启无限自由网络 69

一、初探CCProxy溢出漏洞70

二、搜索漏洞主机71

1. 搜索

2. 探测

三、溢出测试73

四、破解代理密码，无限制上网74

1. 获取密文

2. 破解密码

3. 测试代理账号

五、完全控制机房代理服务器77

1. 上传木马

2. 溢出上传木马

4月23日 晴

SP2安全中心大攻击 78

一、初探小菜电脑安全	78
二、Windows XP SP2溢出漏洞	79
三、编译SP2防火墙溢出代码	80
1. 安装Cygwin	
2. 编译C文件	
四、本地溢出SP2防火墙的试验	81
1. 配置启用防火墙	
2. 尝试连接	
3. 绕过防火墙检测	
五、远程攻击小菜	84
六、让SP2防火墙成为“僵尸”	85
1. 搭建本机HTTP服务	
2. 图片木马攻击	

8月12日 晴

艰难的抓“鸡”历程，TCP/IP过滤突破记

88

一、惊现Wins MS04045溢出漏洞	88
1. WINS名称验证远程溢出漏洞简介	
2. 扫描漏洞主机	
二、溢出攻击	90
1. 监听本地端口	
2. 远程溢出	
三、自动溢出，快快抓鸡	91
1. 自动溢出攻击	
2. 批量溢出攻击	
四、一波三折，初试BAT上传	93
1. 转换程序为BAT代码	
2. 上传BAT	
五、再试VBS上传	94
1. 转换VBS代码	
2. 上传木马	
六、真相大白，TCP/IP过滤惹的祸	96
七、TCP/IP过滤的突破方案	97
1. 直接利用MT突破TCP/IP过滤	
2. 更为方便的ChgTcpipFilter	
3. 手工修改注册表突破TCP/IP过滤	

4月1日 晴

拐弯抹角，渗透信息港网站服务器

100

一、学习——了解渗透入侵的原理	100
二、踩点——虚拟主机渗透前奏	101
三、发掘MS05039溢出漏洞	102
1. 确定攻击方式	
2. MS05-039漏洞简介	
3. 扫描漏洞主机	

四、初试MS05039远程溢出攻击	104
五、换个工具来溢出	105
六、反向溢出终成功	106
七、ARPSniffer完美渗透攻击	107
1. 检测网段	
2. 嗅探攻击	

6月14日 晴

接受挑战，盗Q之旅 109

一、锁定挑战者QQ	109
二、挖出QQ邮箱漏洞	110
三、暴力破解，漫长的守候	110
1. 获得QQ邮箱服务器地址	
2. 生成破解字典	
3. 破解设置	
4. 破解QQ密码	
四、随手盗取弱口令QQ	113
五、无奈之举，QQ邮件来盗号	114
1. QQ邮箱挂马漏洞的小测试	
2. 生成盗号木马	
3. 生成网页木马	
4. 伪装QQ邮件代码	
5. 发送攻击	

三 网站入侵

4月20日 晴

Cookie欺骗的魅力，某网上商城的安全检测 121

一、SQL注入先遣	121
二、再试SQL，获得商城信息	122
三、意外的发现	125
四、突破口，COOKIE欺骗	126
1. 失败	
2. 分析	
3. Cookie欺骗	
五、修改管理员密码，登录后台	127
六、真相大白	128

5月16日 晴

SQL注入闯关记 132

一、初探SQL注入	132
二、确定注入	133
三、猜解用户密码	134

四、自动注入，破解失败	135
五、换工具，再试注入	137
六、上传ASP木马	139

3月21日 小雨

网投任我玩，帮助MM刷票 **142**

一、初次——清除Cookie刷选票	143
二、换招——变换IP刷选票	144
三、打造刷票机器人——自动刷投票	145
1. 自动更换IP地址	
2. 自动投票	
四、换平台，再战刷票	147
1. 初探梦痕网络投票系统	
2. 投票系统安全检测	
3. 判断投票检测类型	
五、修改Cookie，手工刷票	149
1. 嗅探数据信息	
2. 手工刷票	

7月16日 阴

● 入侵网站商城，免费购物 **152**

一、搜索目标商城	152
二、暴库下载商城数据库	153
三、破解管理员密码	154
四、登录后台管理页面	156

6月2日 阴

● BT服务器的入侵控制经历 **157**

一、轻取NB文章系统网站	158
1. 搜索NB文章系统网站	
2. 连接上传漏洞页面	
3. 上传ASP木马	
二、连接木马，控制服务器	161
三、突破防火墙，远程控制	162
1. 上传木马	
2. 本地监听	
3. 远程执行木马	
四、连接控制服务器	164

4 牧马记

2月14日 小雨

暗渡陈仓，MP4助兄弟泡MM **165**

一、备马	165
1. 配置木马服务端	
2. 制作自解压木马	

二、驯马	167
三、插马	168
1. MP3音乐陷阱	
2. MP4音乐的陷阱	
四、用马	171
1. 连接	
2. 杀掉防火墙与杀毒软件	
3. 上传木马, 下载MM信息	

2月20日 雨

意外遭受攻击引发的检测 174

一、MSN Messenger惊现溢出漏洞	174
二、似曾相识, 制作溢出图片	175
1. 隐蔽的ActiveX木马攻击	
2. 生成溢出图片	
三、溢出图片的利用	177
1. 设置溢出图片为MSN头像	
2. 远程攻击	

3月18日 阴

“高手”的入侵体验 179

一、IE新漏洞, 与众不同的网页木马	179
1. IE IFRAME溢出漏洞原理简介	
2. 测试IE IFRAME溢出攻击	
二、制作自己的木马网页	180
三、QQ传资料, 攻击别人	181
四、IE IFRAME溢出下马	182
1. 专业版网页木马生成器简介	
2. 隐蔽、全能的内核级后门Ntrootkit	
3. 配置Ntrootkit安装文件	
4. 生成网页木马	
五、高手专用, Ntrootkit后门	184
1. 客户端连接	
2. 使用Telnet连接	
3. 命令控制, 尽显风采	

3月23日 晴

一次图片溢出漏洞的攻击测试 186

一、QQ表情, 让MM中木马	187
1. MS04-028图片溢出漏洞简介	
2. 生成溢出图片木马	
3. 替换QQ表情为木马	
4. 巧用QQ表情传木马	
二、用JPEG图片漏洞进行溢出攻击	189
三、意外之后的对策	191
1. 制作反向溢出图片	
2. 连接控制	
3. 和MM开玩笑	

四、图片溢出，没完	192
五、一天千鸡——疯狂的图片木马	193
1. 简单的跨站攻击——论坛贴图	
2. 网页挂马	
3. 邮件传马	

4月5日 阴

“诱惑”——免费电影网站挂马 196

一、视频木马之源	197
1. 视频木马的原理	
2. 挑马——全能的蜜蜂大盗	
3. 制作网页木马	
二、热门“集结号”，攻击无限	199
1. 转化木马网页格式	
2. 插入木马	
三、新片“见龙卸甲”，埋藏暗招	201
1. MOV视频木马轨道的制作	
2. 添加代码，制作木马	
四、蜜蜂采“密”，远程控制肉鸡	203

5月20日 晴

暗夜追踪，打开黑客之门 204

一、初识黑客之门	204
二、远程溢出，开辟入侵之道	205
1. 扫描漏洞主机	
2. 远程溢出	
三、留下暗门	206
1. 本地配置服务端	
2. 悄悄安装木马	
3. 检查后门是否安装成功	
四、打开系统安全之门	208
1. 使用NC连接	
2. 使用客户端连接	
五、突破封锁的后门	210

10月10日 阴

网络“恐龙”大揭密 211

一、精诚虽至，金石不开	211
二、明修栈道，暗渡陈仓	212
1. 制作强制视频木马	
2. 木马伪装	
3. 文件名伪装	
4. 发送木马	
三、庐山真面目	214
1. 配置军刺木马	
2. 连接后门	

四、揭穿“美女”真面目	215
1. 查获肉麻“情书”	
2. 查获QQ聊天记录	

6月18日 晴

一个U盘，入侵整个办公网	219
一、鱼饵——“文本”陷阱	219
1. 初次试验	
2. 木马伪装	
二、多重加壳，免杀文本木马	221
三、巧用文本玩入侵	222
1. 木马陷阱效果	
2. 连接攻击	
四、制作下载者，感染整个办公网	224
1. 配置U盘蠕虫病毒	
2. 超强蠕虫，共享还原不放过	
3. 锁定IE，QQ尾巴大传播	
4. 网页让木马再生	
5. 下载者与反杀	
五、北斗压缩二次加壳	227

5 网吧沦陷记

3月3日 晴

突破限制，行遍网吧无疆界	229
一、经典破解已受限	229
二、世纪黑马来破限	230
三、QQ记事本巧破硬盘限制	232
1. Realplayer破解硬盘限制	
2. QQ记事本漏洞	
四、下载超强破解工具	234
五、完全突破网吧实录	235
1. 结束网吧管理软件	
2. 解锁注册表	
3. 完全控制网吧	

7月15日 晴

妙手空空破万象	238
一、变态的万象2006	238
二、用系统“时间”打开“帮助”文件	239
三、突破硬盘限制	239
四、突破限制下载	241
五、完全破解万象2006的限制	242
六、万象2006破解总结	243

1月20日

小雪

饭钱节省有道, 免费网吧上网 244

一、准备工作, 打造在线破解244

1. 选择网吧破解工具
2. 利用WMF漏洞, 打造在线网吧破解系统
3. 新漏洞破解严密网吧
4. 无可阻挡Flash破解

二、机时小偷, 偷偷上网249

1. “机时小偷 V6.0”的注意事项
2. 结账注销模式免费上网
3. 结账重启模式免费上网

三、险漏洞, 玩充值252

1. 确定收费服务器IP地址
2. 连接数据库

四、远程溢出, 入侵刷卡254

五、手工刷卡玩充值256

六、PUBWIN EP充值成功257

5月5日

晴

偷窥聊天记录, 识破MM虚情意 258

一、两手准备258

1. 制作压缩程序
2. QQ下载运行破网工具
3. UC网络硬盘破下载

二、意外, 网吧小子来帮助261

1. 在线下载
2. 运行网吧破解工具

三、完全破解网吧限制263

四、QQ嗅探, 锁定MM263

1. 定位, 查出MM的IP
2. 捕捉, 嗅出MM的QQ号
3. 验证MM的IP地址

五、偷窥MM聊天记录266

1. 复制QQ聊天记录
2. 偷窥聊天信息

8月8日

晴

走出失落, PUBWIN2007网吧新破解 268

一、网吧幽灵, 突破下载限制269

二、破解Pubwin 2007客户端270

三、解决补丁, 成功登录271

三、伪装帐号, 免费上网272

四、禁止重启, 完美破解273

01 局域网入侵

8月3日

晴

内存泄密 << 机房电脑无限制



今天的计算机课又是上机实践，依旧是无聊的进行一些简单的文字图表编辑，让人郁闷。

系计算机室中的每台电脑都被作了严格的限制，不能上网，不能下载，也不能打游戏、QQ聊天，只有管理员登录后才能自由的进行各种操作。可恨的是，老师的密码设置太BT，我曾经试了多少次，从老师的生日、口头禅，甚至连老师的女朋友姓名和生日也进行了一番排列组合，依然没能猜出密码是什么……

无聊的WORD操作了一遍又一遍，正自胡乱点击着鼠标刷格式作图表，突然电脑上出现了一片蓝色，一大遍英文字母显示在屏幕上——经典的蓝屏死机又出现了。按下电源开关，重新启动系统，没想到自动登录进入系统后，却再怎么也无法启动WORD了。

——“老师，我的机子出问题了！”我很乐意将问题交给老师，消磨余下的时间。

“要重装一下WORD了。”老师解决问题的方法很简单直接，重新启动，用管理员身份登录进入，开始安装起WORD来……

安装中，老师的手机铃声突然响起。老师接听了电话，一边小声的聊着一边开始走出机房。——从老师笑开花的脸上，可以猜到来电的一定又是老师的女朋友。看来老师这个电话没有个十多分钟是打不完的了。

我开始无聊的等待，等待中，我的心中突然萌生了一个“罪恶”的念头——利用当前登录，破解老师的登录密码，以后无限制的使用机房中的电脑……

一、内存截取，有些失败

无论老师的密码设置得多复杂，保管得多安全，此时未设防的电脑上都可以轻易的将密码截取。

我先从网上下载了用来截取内存中的账号密码两个小工具：“pulist.exe”和“Findpass.exe”。然后点击“开始”菜单→“运行”，输入命令“CMD”，回车后打开命令提示符窗口。

提示 【内存截取登录密码的原理】

在Windows系统中，某个用户登录系统后，其用户名与密码都是以明文的方式保存在内存中的。掌管用户登录的系统进程是“Winlogon.exe”，当有多个用户同时登录系统时，每一个用户登录都会产生一个Winlogon进程（图1）。如果能够查找Winlogon进程访问的内存模块，就可以获得保存在内存中的用户名和密码。也就是说，黑客可以利用远程控制或本地多用户登录，轻松盗取同时登录系统的管理员及其它用户的密码。使用Findpass结合plist工具，就可以查出管理员的密码。

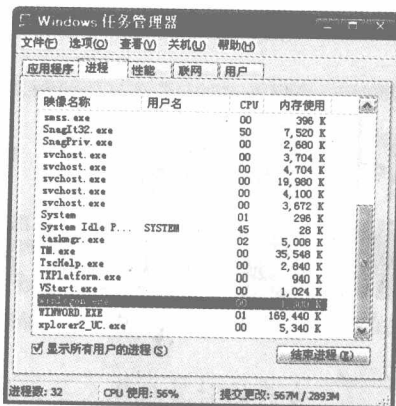


图1 储存登录账号的Winlogon进程

1. 获取管理员登录进程ID

在命令窗口中进入工具所在的文件夹下，输入“pulist”命令，执行“pulist.exe”程序，即可查看到当前在系统中运行的所有进程（图2）。在其中存在“WINLOGON.EXE”进程，列表显示格式如

```
winlogon.exe 612 NT AUTHORITY\SYSTEM
```

其中“WINLOGON.EXE”是进程名，“612”是进程的PID号，“NT AUTHORITY\SYSTEM”表示登录用户类型为管理员。

知道了当前登录的是管理员账号，那么需要查看其管理员账号用户名。查看其它的应用程序进程信息，如：

```
VStart.exe 460 BINGHEXIJIAN\Administrator
```

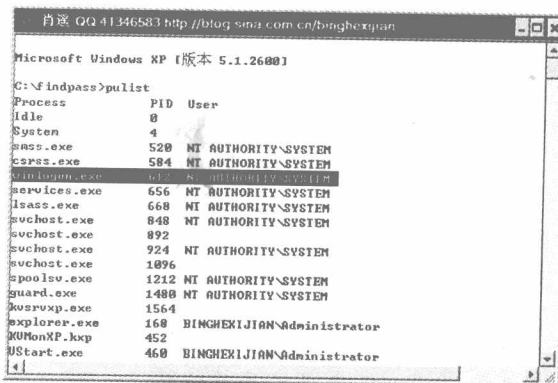


图2 获取管理员登录进程ID

从进程信息可知，管理员用户名为“Administrator”，所在的域为“BINGHEXIJIAN”。

2. 获取管理员登录密码

现在可以根据进程信息, 利用Findpass找出内存中的用户密码。Findpass的命令格式为:
Findpass 域名 管理员用户名 管理员Winlogon进程ID号

根据前面查获的信息, 可在命令窗口中
执行如下命令(图3):

Findpass BINGHEXIJIAN
Administrator 612

回车, 命令运行后很快就有了结果, 可以看到用户名为“puma_xy”的管理员密码“password”。

提示

在Windows XP/2000中, 还有许多查获内存中管理员账号登录密码的工具, 以一个常用的网吧破解工具“精锐网吧辅助工具 v5.9”为例:

在管理员登录状态下, 在系统中运行精锐网吧辅助工具, 选择“本机信息”选项卡, 在下面的“密码”信息中, 即可看到当前登录的管理员用户密码(图4)。

……按道理, 执行了Findpass工具, 应该就可以成功截获老师的登录密码, 可是没想到命令执行后, 竟然提示“*There is no password.*”(图5)。——我突然想起来, 系计算机室中安装的都是Windows 2003系统, 我下载的工具是用于Windows XP和2000的, 因此自然无法找到管理员密码了。于是我重新下载了Windows 2003系统中查获登录密码的工具“findpass2003”。……

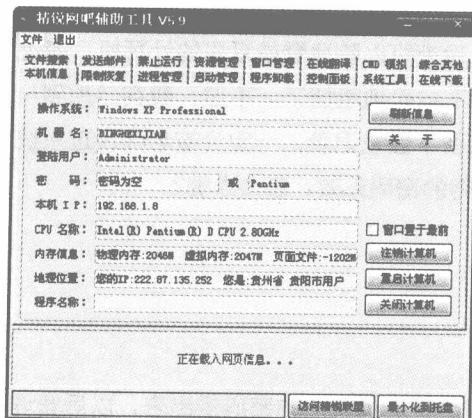


图4 查看管理员账户登录密码

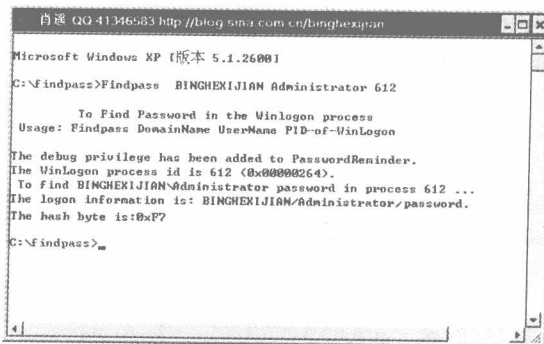


图3 在NT环境中获取管理员登录密码

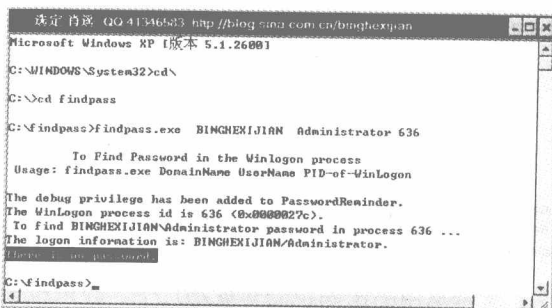


图5 Windows 2003下无法获得管理员密码

提示

老版本的findpass对于Windows 2003是没有用的，因为在Windows 2003中管理员登录后其密码是随机存储在内存中的，而且密码不像在Windows 2000和XP中是以明文的方式保存，这就给在线获取密码增加了难度。可以使用一个叫作“findpass2003”的工具，在线获取Windows 2003管理员密码。

二、换工具，2003吐密码

将Findpass2003下载到本地后解压，在命令窗口中进入工具文件夹，直接输入密码获取工具的程序名“findpass2003”。程序运行后，自动在内存中寻找管理员密码存储位置，并从中分离出密码显示在程序运行窗口中（图6）。

由于Windows 2003的密码在内存中是随机存储的，程序运行后不一定能够百分之百成功得到密码，因此可以再次执行程序命令，直到获得登录密码。

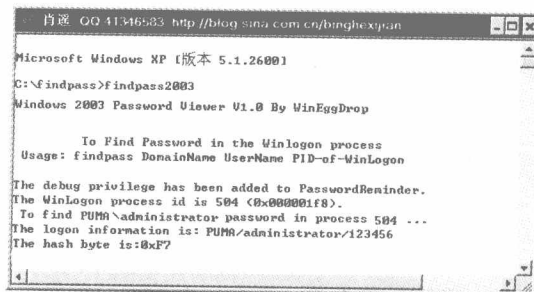


图6 Windows 2003中查获管理员登录密码

提示 【内存管理员密码窃取的防范】

对于这种远程或本地获取内存中管理员账号的方法，没有太好的针对性的防范措施。我们唯一可以作的就是在平时打好各种系统补丁，保证系统的安全可靠；并设置好用户权限，禁止用户运行一些危险的程序；再就是平时进行一般的操作，尽可能不用管理员身份登录。

终于获得了老师的登录密码，只要用这个密码，以后就可以随意登录系里的计算机，毫无限制的执行各种操作了，上网QQ聊天、游戏之类的都不会受到阻挡了。不过，我突然想到一个问题，老师平时一向谨慎，我用管理员账号登录，会留下登录记录，一定会被老师通过系统日志发现的！而且老师有可能更改管理员密码，让我获得的密码无效。怎么办呢？

三、查看常用密码

老师常用的密码也无非就那几个，改来改去的，只要把老师常用的密码揪出来，以后管理员密码被改后，尝试其它的密码就应该可以了。