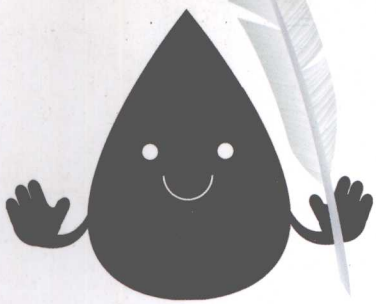
电脑迷 荣誉出品



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

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

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

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

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

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服务器的入侵控制

云南出版集团公司 • 云南科技出版社

电脑迷 荣誉出品

黑客入侵手记

肖遥 编著

云南出版集团公司 • 云南科技出版社

光盘导读

特别说明

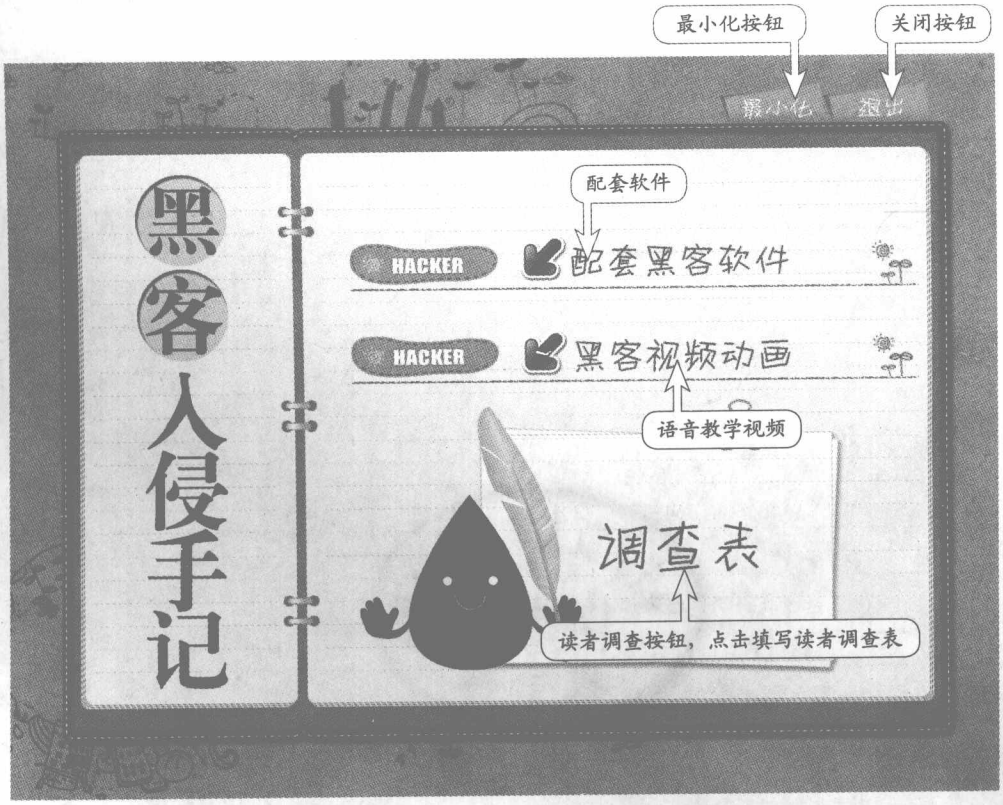
本光盘提供的黑客软件和视频仅供技术研究使用，切勿利用来破坏他人的计算机或数据，否则一切后果自负。

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

9月7日　　阴

7月12日　　晴

CONTENTS

4 牧马记

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。

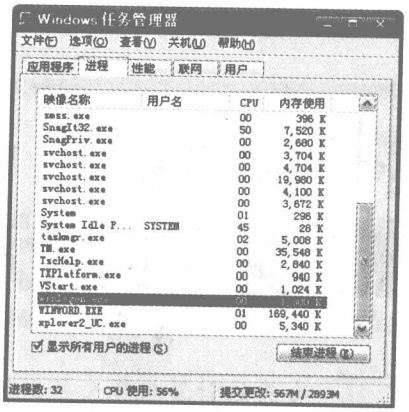


图1 储存登录账号的Winlogon进程

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

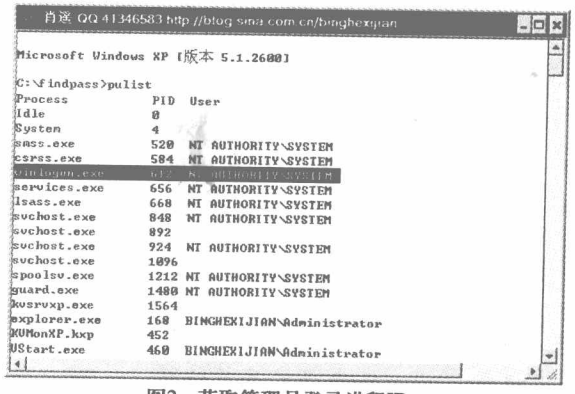


图2 获取管理员登录进程ID

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Winlogo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”。

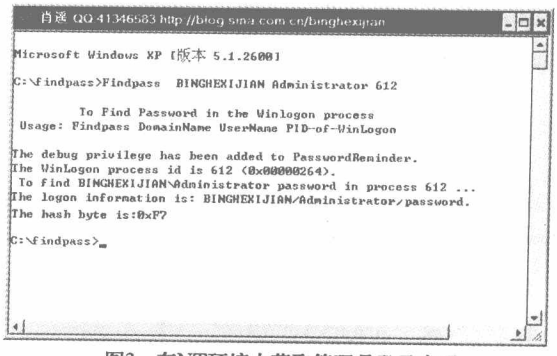


图3 在NT环境中获取管理员登录密码

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”。……

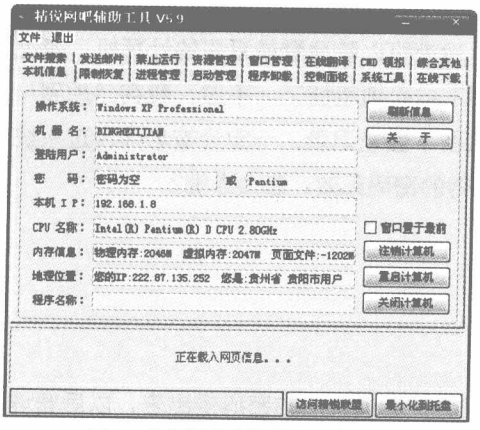


图4 查看管理员账户登录密码

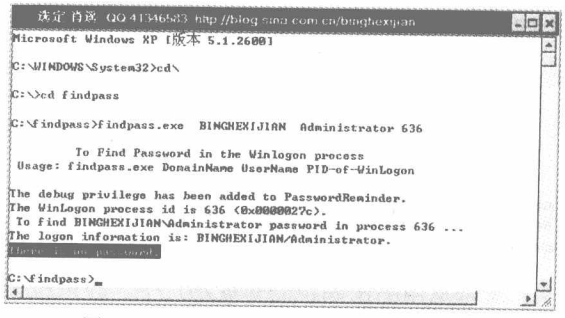


图5 Windows 2003下无法获得管理员密码

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。

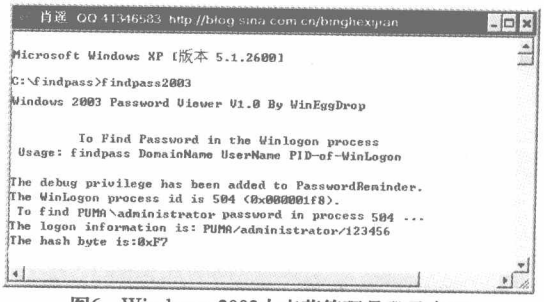


图6 Windows 2003中查获管理员登录密码

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。