用电脑不求人系列之十六

GOTOP

实战黑客

不求人

林东和 编著
樊小溪 改编

你知道 你的电脑已成为 黑客跳板 了吗？

如何发现？如何预防？

- Windows $共享名和密码剖析
- Windows远程死机漏洞大公开
- 黑客跳板隐身实战
- BO2K特洛伊木马入侵实战
- 特洛伊木马现形实战
- 防火墙保护实战

人民邮电出版社
www.pptph.com.cn

实战黑客不求人

林东和　编著

樊小溪　改编

人民邮电出版社

图书在版编目(CIP)数据

实战黑客不求人/林东和编著.-1 版.-北京：人民邮电出版社，2001.3
(用电脑不求人系列之十六)
ISBN 7-115-00000-0

I.选… II.林… III.电子计算机-硬件-基本知识 IV.TP33

中国版本图书馆 CIP 数据核字(1999)第 00000 号

用电脑不求人系列之十六

实战黑客不求人

◆ 编　　著　林东和
改　　编　樊小溪
责任编辑　俞　彬

◆ 人民邮电出版社出版发行　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ pptph.com.cn
网址　http://www.pptph.com.cn
读者热线:010-67129212　010-67129211(传真)
北京汉魂图文设计有限公司制作
北京顺义向阳胶印厂印刷
新华书店总店北京发行所经销

◆ 开本:720×980　1/16
印张:20
字数:384 千字　　2001 年 4 月第 1 版
印数:1－7 000 册　　2001 年 4 月北京第 1 次印刷

著作权合同登记　图字:01－2001－0141 号
ISBN 7-115-09147-1/TP·2102

定价:34.00 元

第一章 概述

1-1 引言

自从笔者出版了《防范黑客不求人》之后，读者的反应非常热烈，许多人都想进一步地了解更多的黑客入侵伎俩。

为了不辜负读者的厚爱，笔者就再次收集各项黑客实战的伎俩，希望能够让读者远离黑客的危害。

本章概述了全书的主要内容，读者可以从中快速了解全书的结构安排。主要内容包括：Windows CONCON 死机漏洞；Windows $共享名和密码剖析；常见的特洛伊木马；如何发现特洛伊木马；跳板入侵原理及实现；防火墙软件的使用；黑客攻击流程；防范黑客入侵流程。

1-2 Windows CONCON 死机漏洞实战

Windows 系统有下列三个设备驱动程序：

- CON：输入及输出设备驱动程序；
- NUL：空设备驱动程序；
- AUX：辅助设备驱动程序。

然而，在 Windows 95/98 的版本中，存在有这三个设备驱动程序的死机漏洞，只要在“开始”菜单中的“运行”对话框中打入如图 1-1 所示命令，就会出现蓝底白字的 CONCON 死机画面，如图 1-2 所示。

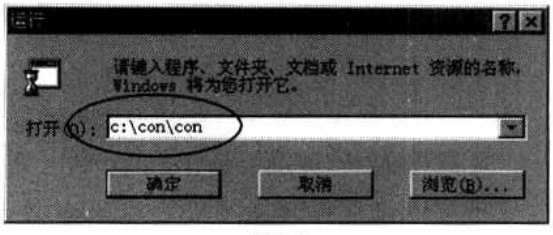


图 1-1

图 1-2

有关 Windows CONCON 死机漏洞详情，请参考第四章的详尽解说。

1-3 Windows $共享名和密码剖析实战

如果你不想要让公司其他人共享资源，你就可以用$共享名技巧，只要在磁盘或文件夹名称后面加上 $ 就可以了，如图 1-3 所示。

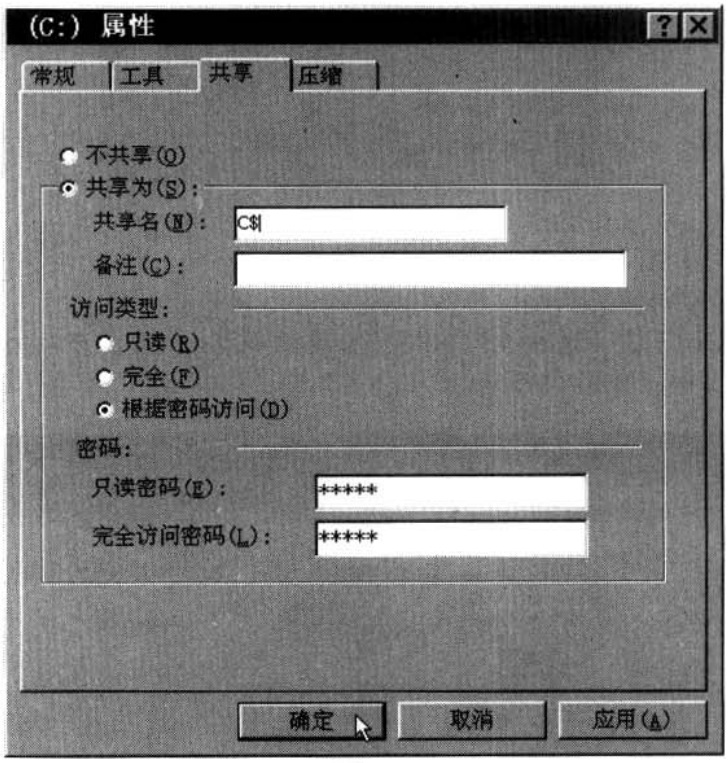


图 1-3

如此一来，公司其他人联机到你的电脑时就不会出现该共享的磁盘或文件夹。想不想让 $ 共享名现形？没问题！笔者将在第五章介绍 $ 共享名现形大法。Windows 资源共享的密码有下列两种（见图 1-4）：

•

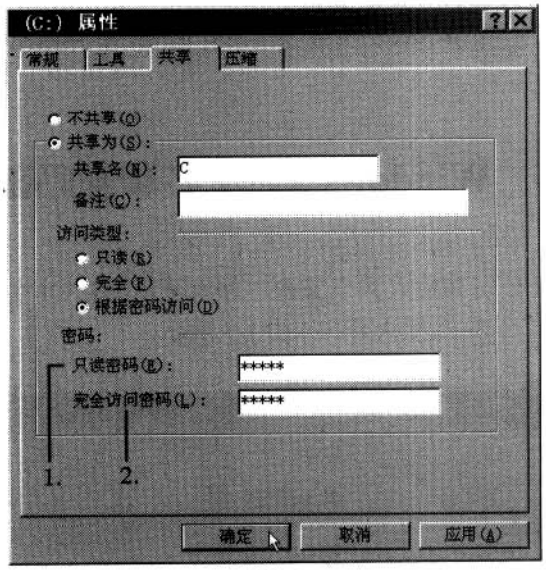


图 1-4

- 1 为只读密码；
- 2 为完全访问密码。

这两种密码不像其他密码一样以文件的方式保存，而是保存在注册表编辑器（regedit.exe）中，如图 1-5 所示。

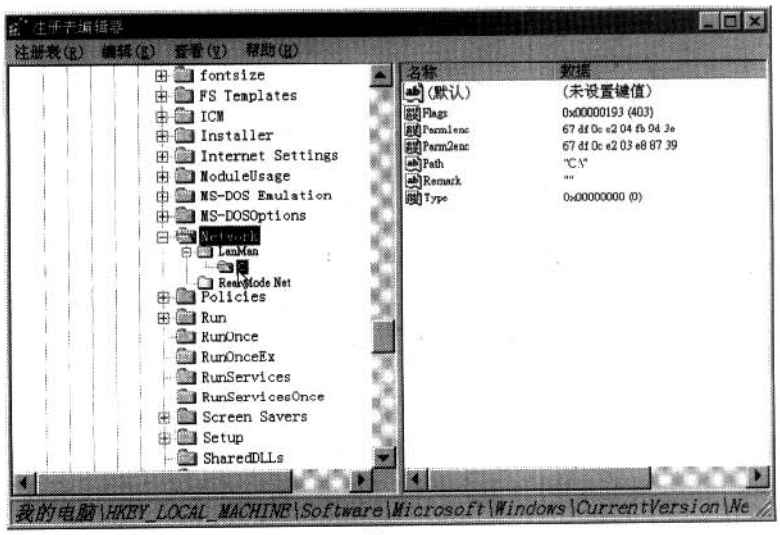


图 1-5

在图 1-5 中，Parm1enc 是完全访问密码。

Parm2enc 是只读密码。

想不想破解这两个密码？没问题！笔者也会在第五章介绍资源共享密码破解大法。

1-4 特洛伊木马实战

特洛伊特洛伊木马是本书的重点，笔者在本书中介绍了两个重量级的特洛伊特洛伊木马，分别是 Back Orifice 2000 和 Subseven 2.1。

一、Back Orifice 2000（见图 1-6）

图 1-6

有关 Back Orifice 2000 详情，请参考第六章。

二、Subseven 2.1（见图 1-7）

有关 Subseven 2.1 详情，请参考第七章。

此外本书也在第八章详细介绍了另外 4 个小巧的另类特洛伊木马，它们各有各的用途。

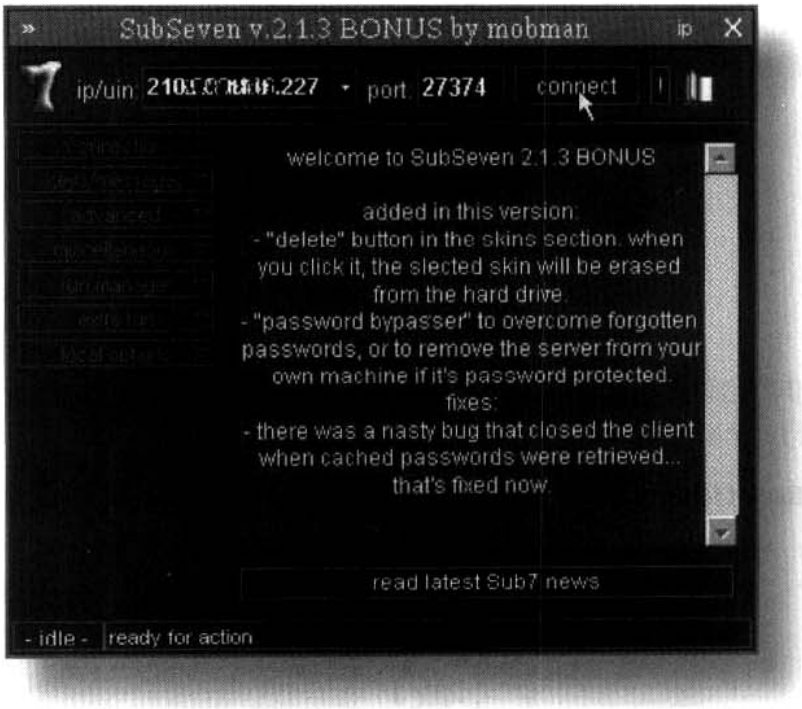


图 1-7

1-5 特洛伊木马现形实战

特洛伊木马软件都是“偷偷摸摸”地活动的，让被黑者很难查觉到，更别说要防范了。

那如何知道被特洛伊木马入侵了呢？笔者将在第九章介绍特洛伊木马现形大法，并用特洛伊木马扫描软件 Cleaner（见图 1-8）进行扫描，让隐藏在电脑中的特洛伊木马一一现形。

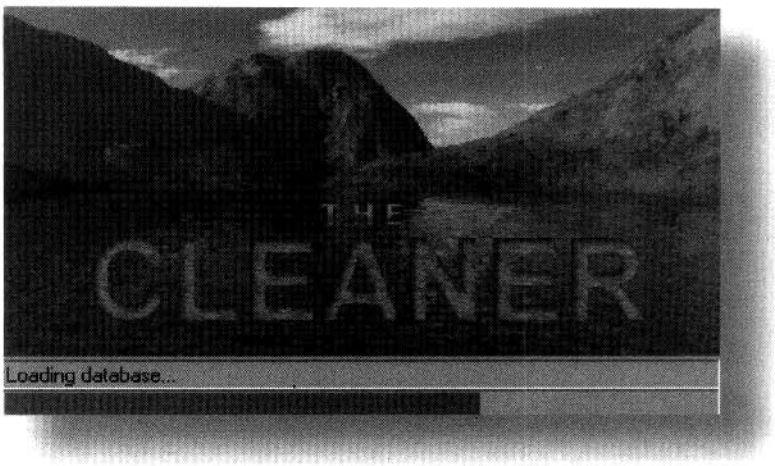


图 1-8

1-6 跳板入侵实战

所谓“跳板入侵”，是指黑客先控制一台电脑当成跳板，再利用该电脑来入侵另一台电脑。例如，黑客控制甲电脑入侵乙电脑时，乙电脑是黑客真正要入侵破坏的目标，而甲电脑只是黑客利用的跳板。

当乙电脑发现电脑系统被入侵破坏时，根据 IP 记录所找到的电脑只是甲电脑而已，并非黑客本身的电脑 IP，如此一来，甲电脑就成了无辜的代罪羔羊，而黑客仍然逍遥法外。

想不想了解跳板入侵的伎俩？没问题！请参考第十章的详尽解说。

1-7 防火墙实战

也许你没有“上网防黑”的观念，使得黑客可以轻易入侵你的电脑，你是不

是发现拨号上网费用暴增？或是电脑常常容易重新开机？小心，你的电脑很有可能已经被黑客入侵了。

有鉴于此，笔者在第十一章要教你一套上网防黑大法，那就是安装 Zonealarm 个人防火墙软件（见图 1-9）。

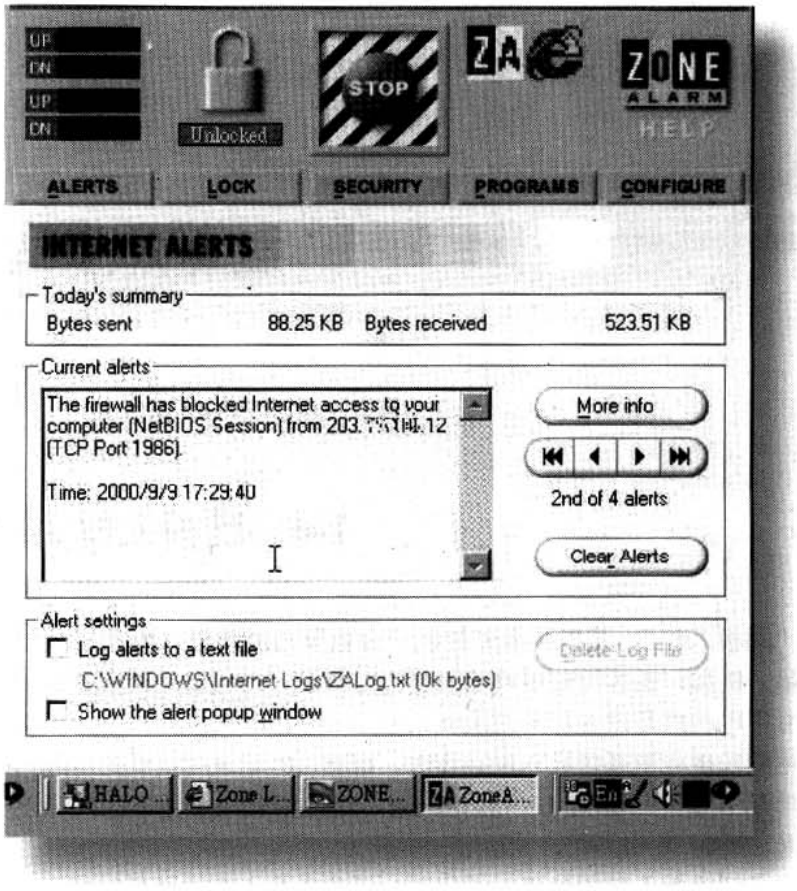
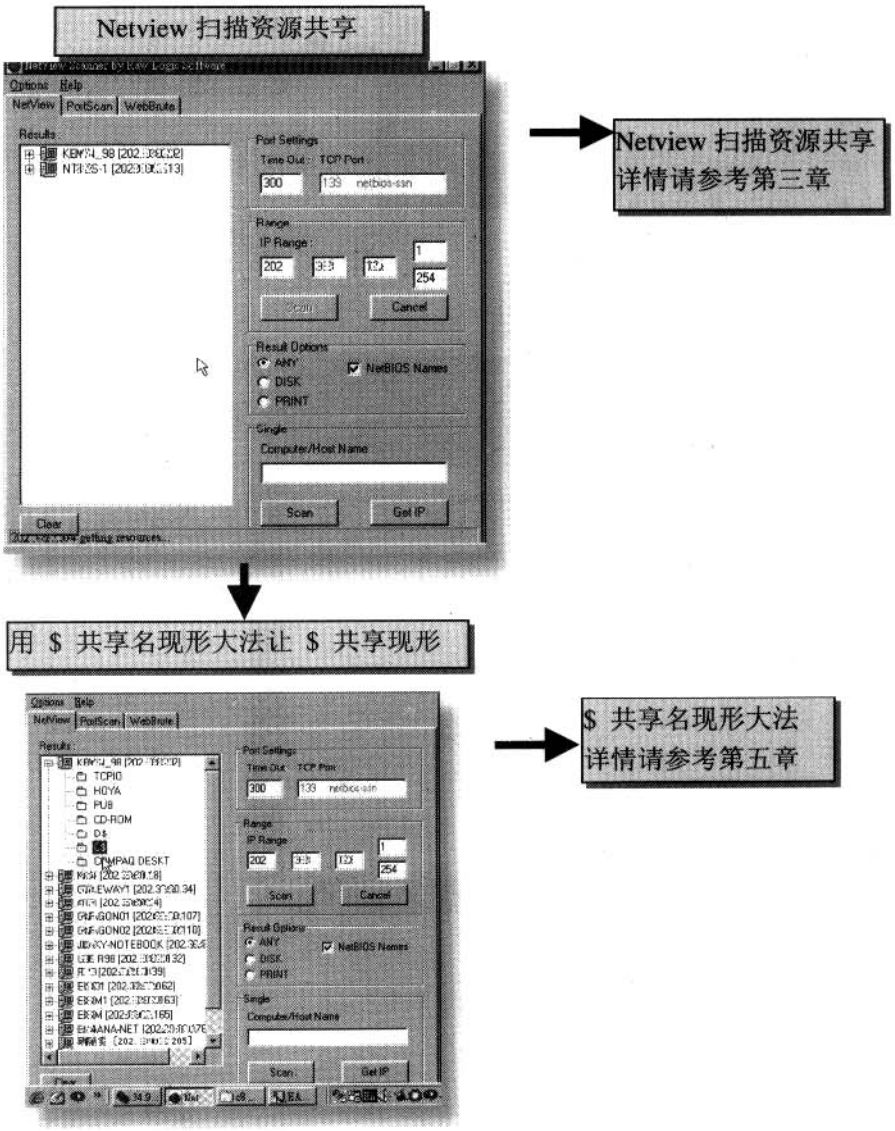
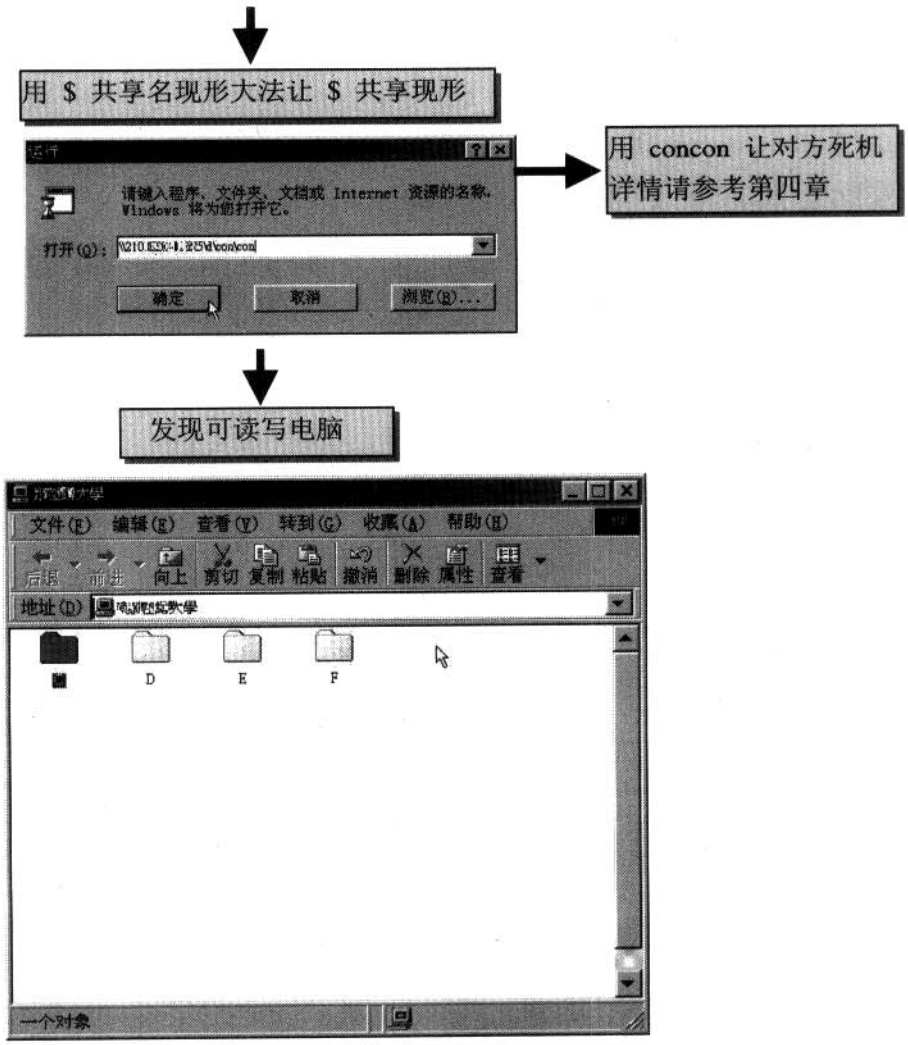


图 1-9

1-8 黑客攻击实战流程


Netview 扫描资源共享
Options Help
NetView PortScan WebBrute
Results
Port Settings
Time Out TCP Port
300
139 netbios-ssn
Range
IP Range :
202
1
254
Scan
Cancel
Result Options
ANY
NetBIOS Names
DISK
PRINT
Single
Computer/Host Name
Scan
Get IP
Clear
Netview 扫描资源共享
详情请参考第三章
用 $ 共享名现形大法让 $ 共享现形
TCPIO
HOYA
PUB
CD-ROM
OEMPAQ DESKT
$ 共享名现形大法
详情请参考第五章


用 $ 共享名现形大法让 $ 共享现形
运行
请键入程序、文件夹、文档或 Internet 资源的名称，Windows 将为您打开它。
打开(O):
确定
取消
浏览(B)...
用 concon 让对方死机
详情请参考第四章
发现可读写电脑
文件(F) 编辑(E) 查看(V) 转到(G) 收藏(A) 帮助(H)
后退 前进 向上 剪切 复制 粘贴 撤消 删除 属性 查看
地址(D)
D
E
F
一个对象

植入特洛伊木马控制该电脑

植入特洛伊木马控制该电脑，详情请参考第六～八章

当成入侵跳板

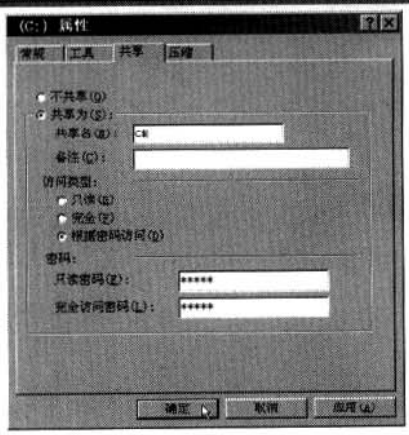
当成入侵电脑
详情请参考第十章

1-9 防范黑客入侵实战流程

Netview 扫描资源共享

Netview 扫描资源共享详情请参考第三章

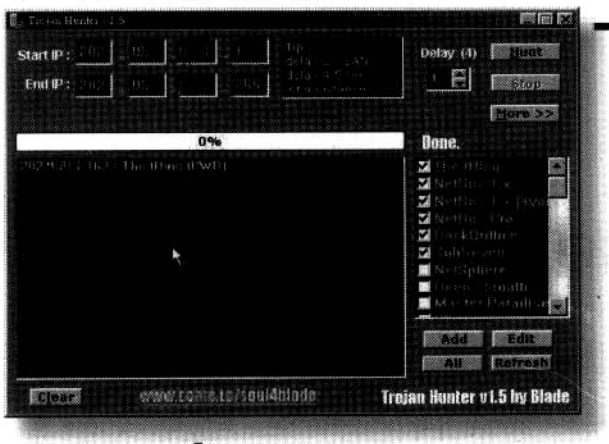
发现有资源共享，赶快关闭或加上密码以免被 concon 命令导致死机



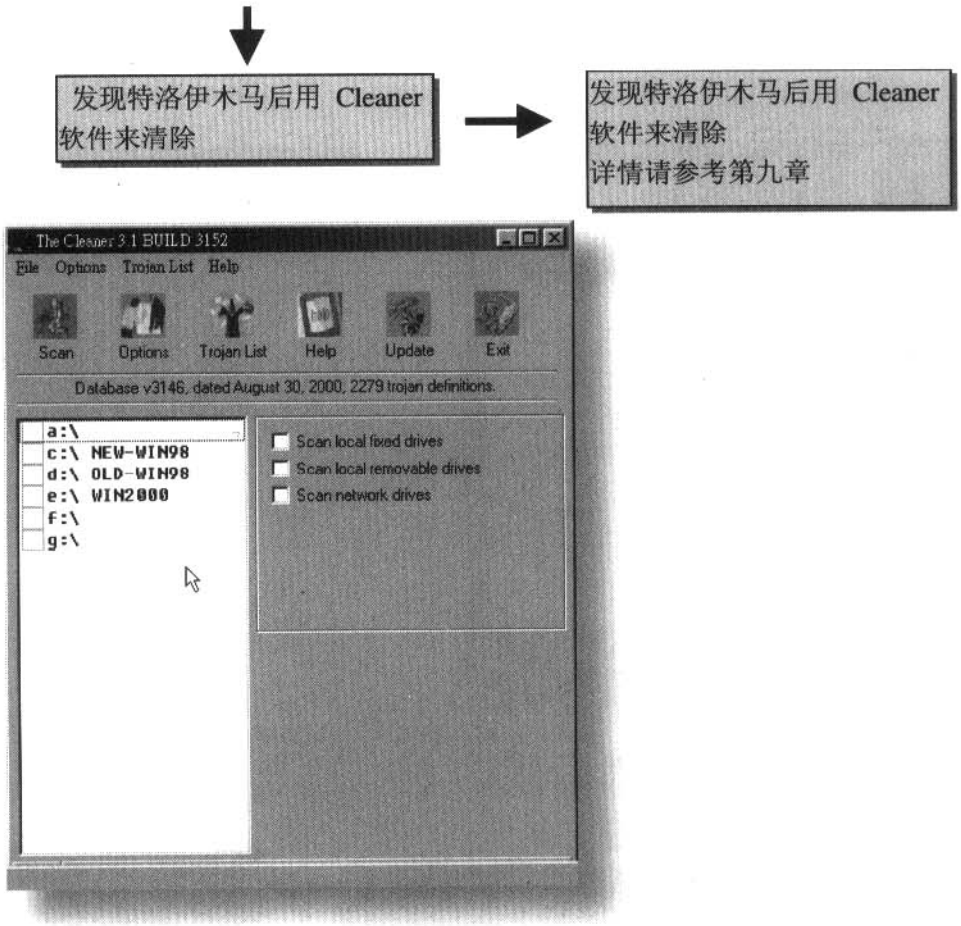
安装 ZoneAlarm 防火墙

安装 ZoneAlarm 防火墙
详情请参考第十一章

用木马猎人扫描是否
被植入特洛伊木马



用木马猎人扫描是否
被植入特洛伊木马
详情请参考第九章



1-10 本书黑客实战主题

本书所介绍的黑客实战主题共分成四大单元，分别如下：

一、第一单元：Windows 系统实战

- 第三章 Windows 资源共享实战：