

反追踪 黑客指南

秘密客 编著

- 追查黑客的来源与地址，包括恶意电子邮件、危险网址、暗藏广告等
- 体验黑客惯用手法，依据“凡走过必留下痕迹”原则追根究底
- 实际操作“反远程控制”、“反木马”、“反监控”程序，向危险网络说“不”
- 记录黑客入侵证据，教会读者如何线上报案，并与网络警察配合缉凶

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

反追踪 黑客指南

责任编辑：苏 茜 荆 波
封面设计：高 洋
上架建议：计算机 / 网络技术 / 网络安全

ISBN 7-113-07449-9



9 787113 074494 >

ISBN 7-113-07449-9/TP·2052
定价：25.00 元



中国铁道出版社

CHINA RAILWAY PUBLISHING HOUSE

中国铁道出版社·计算机图书批销部

地址：北京市宣武区右安门西街8号

邮编：100054

网址：<http://www.tqbooks.net>

读者热线电话：(010) 63563215

销售服务电话：(010) 83550290/91 83550580

目 录

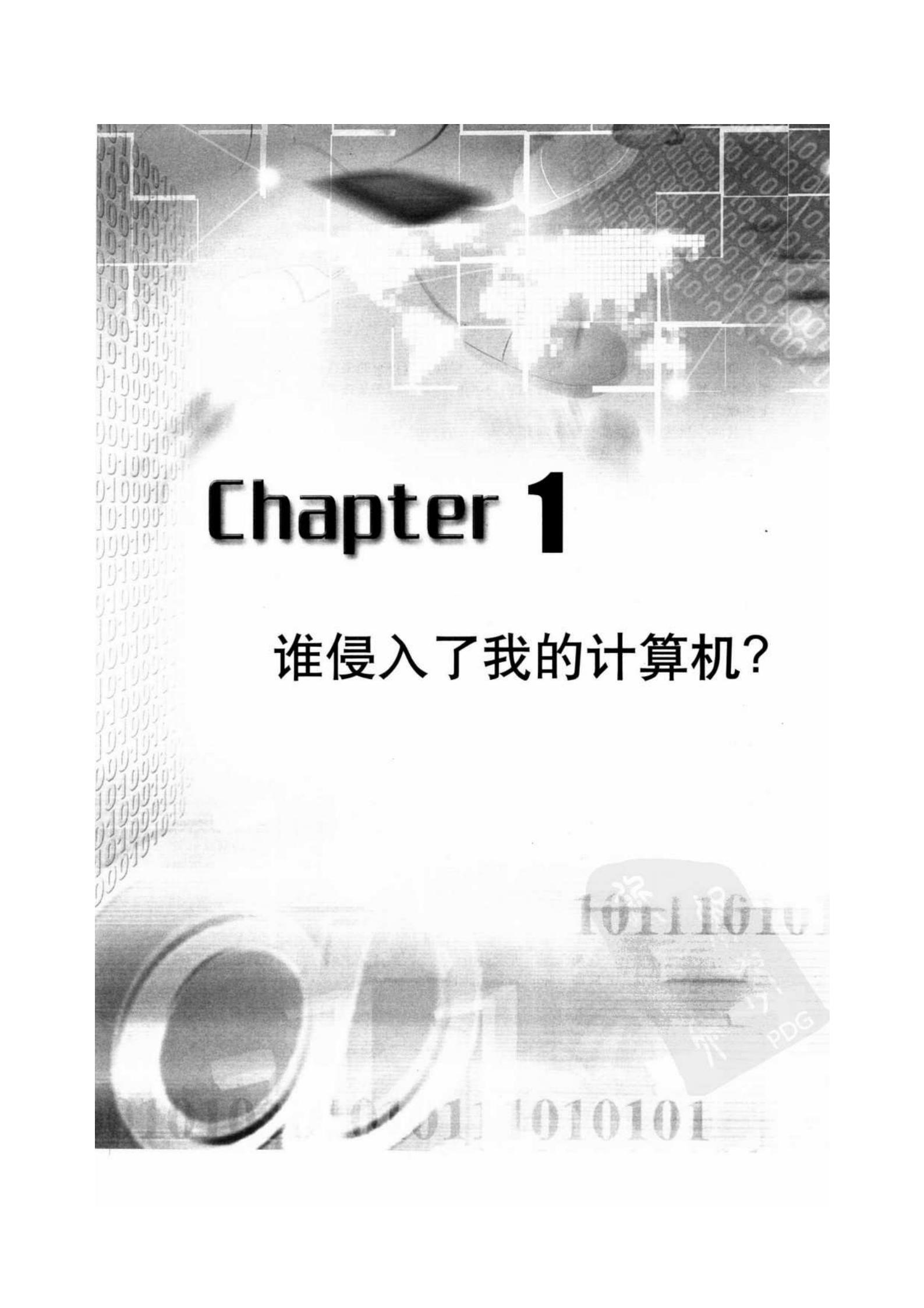
Chapter 1 谁侵入了我的计算机?	1
1.1 解密黑客.....	2
1.2 黑客集散地.....	2
1.2.1 黑客网站.....	2
1.2.2 黑客杂志.....	9
1.2.3 黑客常用的搜索引擎.....	9
1.3 黑客的攻击手法.....	12
Chapter 2 反病毒.....	15
2.1 分析病毒.....	16
2.1.1 认识病毒.....	16
2.1.2 认识蠕虫病毒.....	18
2.2 病毒入侵.....	19
2.2.1 病毒感染计算机的途径.....	19
2.2.2 常见的病毒入侵.....	20
2.3 追踪病毒.....	21
2.3.1 流行的杀毒软件.....	21
2.3.2 实战防病毒.....	22
2.4 病毒的预防.....	35
Chapter 3 反木马程序.....	39
3.1 木马程序.....	40
3.1.1 木马如何入侵.....	40
3.1.2 木马程序的种类.....	46
3.2 反追踪木马程序.....	48
3.2.1 以防火墙监控木马.....	48
3.2.2 清除木马程序.....	69
3.3 做好还原计算机的准备工作.....	71
3.3.1 备份系统分区.....	72
3.3.2 还原系统分区.....	75
3.3.3 制作灾难恢复启动盘.....	79
3.3.4 灾难恢复.....	83



Chapter 4 反键盘记录	87
4.1 认识键盘记录	88
4.1.1 键盘记录的手法	88
4.1.2 常见的键盘记录程序	89
4.1.3 硬件的键盘记录设备	92
4.2 反查键盘记录程序	92
4.2.1 检查与删除暗藏的键盘记录程序	92
4.2.2 专门对付键盘记录的防火墙	99
Chapter 5 扫描黑客	107
5.1 测试黑客计算机	108
5.1.1 Ping 命令	108
5.1.2 取得黑客的路由表	112
5.1.3 反查黑客的域名	114
5.2 认识端口扫描程序	117
5.2.1 什么是端口扫描程序	117
5.2.2 端口种类介绍	117
5.2.3 常见的端口扫描程序	118
5.3 端口扫描程序实战	122
5.3.1 Retina Network Security Scanner	122
5.4 反查黑客所属区域	131
Chapter 6 防御黑客程序	137
6.1 常见的黑客攻击程序	138
6.1.1 电子邮件附件攻击	138
6.1.2 DoS 攻击	138
6.1.3 聊天软件攻击	139
6.2 防御电子邮件附件攻击	140
6.3 防御 DoS 攻击	143
6.4 防御来自聊天软件的攻击	148
6.5 防御来自局域网的攻击	151
Chapter 7 反数据包拦截	163
7.1 认识数据包的拦截	164
7.1.1 认识 Sniffer	164
7.1.2 常见的 Sniffer 软件	164
7.2 拦截数据包	166
7.2.1 检测局域网中的密码是否安全	166
7.2.2 检测局域网内的数据安全	172

目 录

7.3 反制数据包拦截行为	183
7.3.1 硬件设备反制数据包拦截的行为	183
7.3.2 加密无线网络数据包的传送	183
Chapter 8 入侵检测与防火墙监控黑客	187
8.1 入侵检测	188
8.1.1 认识入侵检测	188
8.1.2 执行入侵检测	189
8.2 黑客专用的防火墙	192
8.2.1 天网防火墙的功能	193
8.2.2 访问控制与明文警告	194
8.2.3 应用程序网络使用情况	195
8.2.4 导入官方安全规则库	196
8.2.5 添加病毒 IP 规则	199
8.2.6 日志检查与保存	201
8.2.7 接通断开的网络	202
8.3 检查 Windows 事件查看器	203
8.3.1 检查 Windows 事件查看器	203
8.3.2 免费的在线日志扫描	206
8.3.3 检查 Windows 服务器日志	208
Chapter 9 快速复原系统	211
9.1 删除间谍软件	212
9.1.1 间谍软件简介	212
9.1.2 删除间谍软件	213
9.2 还原文件注册类型	222
9.3 还原损坏的文件	225
Chapter 10 保护自己的计算机	227
10.1 密码保卫战	228
10.1.1 建立用户密码	228
10.1.2 更改密码	231
10.1.3 遗忘密码后的解决方法	233
10.2 加密计算机信息	238
10.2.1 加密文件夹及文件	239
10.2.2 与其他用户共享加密文件	241
10.2.3 解密文件及文件夹	243
10.3 隐藏在磁盘中的文件夹	245
10.3.1 隐藏文件夹	245
10.3.2 取消隐藏	247



Chapter 1

谁侵入了我的计算机？



黑客一词对于一般用户来说既熟悉又陌生，虽然在电影或电视中经常可以看到关于黑客的题材，在报章杂志上也经常能看到某机构被黑客入侵的新闻，甚至一些用户也曾经有被黑客入侵的经历。但是，在现实生活中能认识黑客、了解黑客的人仍然很少。对此，本章将概括介绍有关黑客的一些内容。

1.1 解密黑客

事实上，黑客并非人们想像中那么神秘，根据一份秘密的调查报告显示，绝大多数的黑客本身都有正常的职业，唯一与一般人不同的是，黑客都是技术狂热分子，信奉技术至上的理念。

其实，黑客并不是都会随意地破坏其他人的系统，在黑客的世界里也有一套游戏规则，违反规则的人也会遭到惩罚。寻找系统漏洞、入侵系统、通知系统管理员修补漏洞是黑客入侵的经典过程，由此可见，黑客对于网络安全功不可没。

在黑客的世界中也有善恶之分，除了那些信奉技术至上的“正统”黑客外，还存在着另一种黑客通常我们称之为骇客，称为 Dark-side-Hacker 或者 Cracker。这些人同样具有深厚的计算机技术知识，但是他们却以破坏为乐，其中有一些黑客甚至还受雇于某些公司，为其窃取竞争对手的资料。人们平时所看到关于黑客的报导，绝大部分都是有关 Cracker 的内容，真正的黑客对于这些破坏行为其实是非常反感的。一般来说，由于真正的黑客不容易受到人们的注意，因此绝大部分的人都已经把 Cracker 当成了黑客。为了叙述方便，本书以后的内容将统一使用“黑客”这个称谓，而不再对两者进行区分。

说明：1.3 节以后所涉及的黑客指的是 Cracker。

1.2 黑客集散地

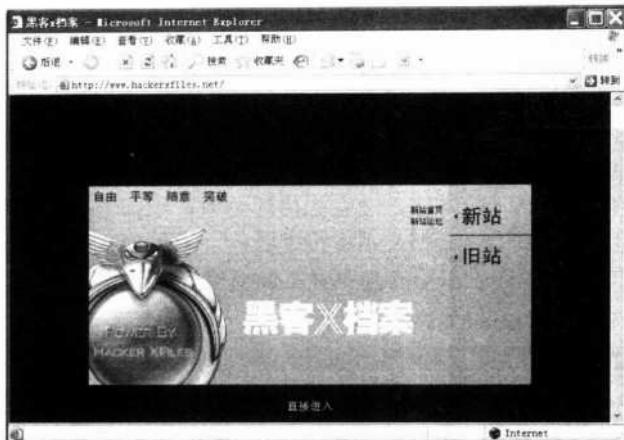
在日常生活中人们难免要与黑客打交道，为了方便交流经验，黑客往往会通过各种方式聚集在一起，例如网站、聊天软件以及黑客杂志等都是黑客的集散地。

1.2.1 黑客网站

网站是黑客互相交流经验的场所，许多网站还专门开设了讨论区，以供黑客互相交流，甚至还有一些为入门黑客开设的讨论区，这类网站在国外及国内都非常多。这些网站经常会发布一些最新的系统安全漏洞信息，因此是黑客最钟爱的地方。下面将介绍一些黑客经常光顾的网站，读者也可通过浏览这些网站，增进对黑客的了解。

● 黑客 X 档案

黑客 X 档案以黑客文化为主题，讲求自由、平等、随意、突破，是一个黑客技术与网络安全的综合性网站，其网址为 <http://www.hackerxfiles.net>。



● 中国鹰派联盟

中国老牌黑客组织【绿色兵团】的成员万涛是中国鹰派联盟的创始人。

网名：eagle,chinaeagle

籍贯：江西

成立中国鹰派联盟并不是他自发的。他经常在网上的军事论坛发帖子，因此有人鼓励他成立俱乐部，于是在酝酿了一年后，成立了中国鹰派联盟。

【我不是黑客】

“之所以说我不是黑客，是因为人们对黑客有误解。黑客是有道义、有良知的技术高手，他与黑客的区别是在进入别人的计算机以后，一个是善意提醒或悄然离开，而另一个则大肆破坏。黑客正如侠客，他是在破坏一些秩序，但是这种反秩序的行为是为了秩序更趋于合理。中国鹰派认为，黑客是未来信息社会重要的平衡力量。”

中国鹰派联盟的网址为 <http://www.chinawill.com/>。



● netXeyes

流光软件开发者小榕的个人网站。



网名：小榕

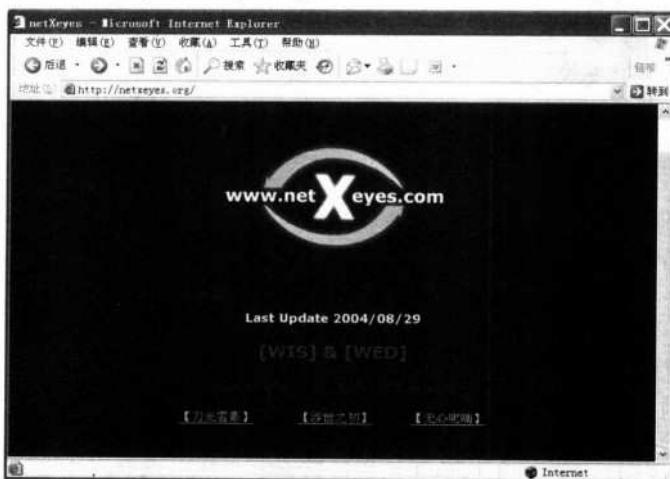
格言：无论在现实或是网络中，我都是孤独的.....

稍有点黑客知识的人，没有不知道流光这个软件的，而小榕就是这个软件的开发者。小榕毋庸置疑是国内目前的顶级黑客，他开发的流光软件是众多小黑客必用的软件之一。

父亲是大学教授的小榕，对黑客的道德观认识得非常清楚：

“黑客像美国西部开发时的牛仔，没有法律的约束，但却有自己的做事准则。黑客要有道德底线，小榕的三条做黑客原则：不能仇视社会，不能给别人制造麻烦，不能给别人带来损失。有人对黑客这样评价：黑客是一种不断研究不断探索的境界”。

netXeyes 的网址为：<http://netxeyes.org/>。



● FETAG.ORG

一代宗师 CoolFire 的个人网站。

网名：CoolFire, Fetag

真名：林正隆

籍贯：中国台湾

林正隆是中国黑客界大师级的人物，他曾经用 CoolFire 这个网名发表过 8 篇黑客入门级的文章，许多人都非常熟悉这样的开头：“这不是一个教学文件，它只是告诉你该如何破解系统，好让你能够将自己的系统做安全的保护，如果你能够将这份文件完全看完，你就能够知道电脑黑客们是如何入侵你的电脑，我是 CoolFire，写这篇文章的目的是要让大家明白电脑安全的重要性，并不是教人 Crack Password”。

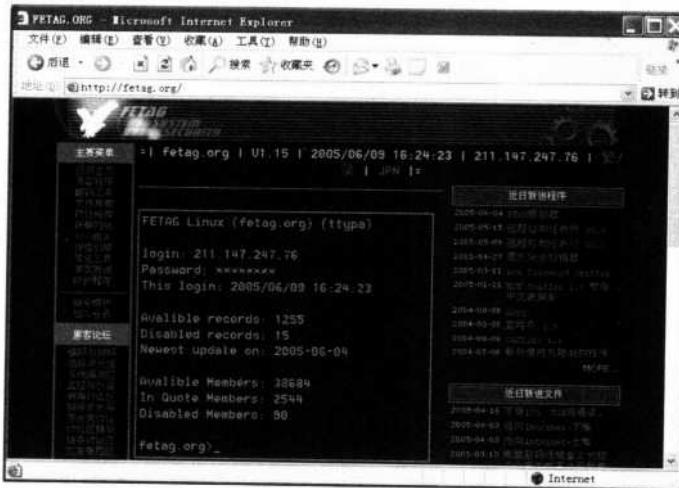
以上是 CoolFire 写的黑客守则，尽管是个人的观点，其中也不乏可取的地方，但是许多人还是将其当作在虚拟世界的一种游戏规则：

不恶意破坏任何系统；恶意破坏他人的软件将导致法律责任；如果只是使用计算机，则仅为非法使用。注意：千万不要破坏别人的软件或资料。

不要修改任何系统文件，如果是为了要进入系统而修改它，可在达到目的后将其改回原状。

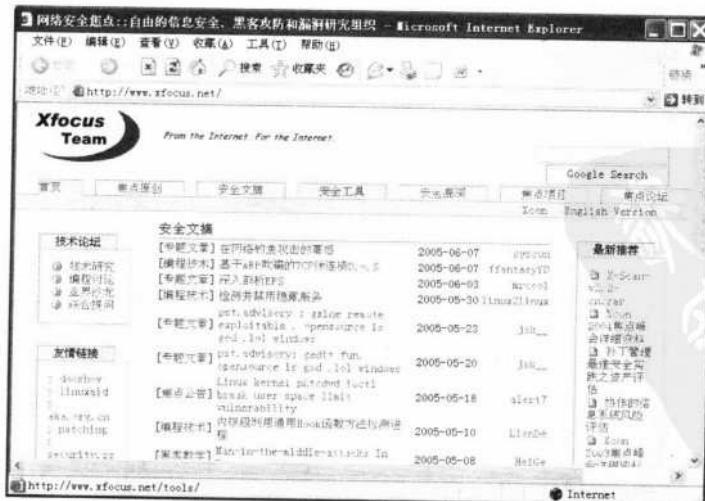
不要轻易地将你要 Hack 的网站告诉不信任的朋友。

不要在 BBS 上谈论你 Hack 的任何事情。
 在公布文章时不要使用真名。
 正在入侵的时候，不要随意离开计算机。
 不要侵入或破坏政府机关的主机。
 不要在电话中谈论你 Hack 的任何事情。
 将笔记放在安全的地方。
 FETAG.ORG 的网址为 www.fetag.org。



● 安全焦点

安全焦点是国内目前最顶级的网络安全站点，其中云集的大批知名黑客足以让其他所有的黑客团体黯然失色。他们开发的网络安全软件已经成为众多网站必选的产品。安全焦点的网址为 <http://www.xfocus.net/>。





● 看雪学院

看雪学院网站是国内顶级的破解论坛、资深的软件加解密技术性网站，主要研究加解密、逆向工程等，其网址为 <http://www.pediy.com/>。

The screenshot shows a Microsoft Internet Explorer window displaying the 看雪学院 homepage. The main content area features a banner for '《软件加密技术内幕》' (Software Encryption Inside Story). Below the banner, there's a search bar and several news items. One prominent item is titled '看雪学院五周年纪念收藏版' (Pediy Academy 5th Anniversary Collection). To the right, there's a sidebar with a '大事记' (Chronicle) section listing various milestones from 2004 to 2009, such as '2004.5 《软件加密技术内幕》出版' (Published) and '2005.6 《看雪教程》(第二版)发布' (Released). Other sections visible include '新闻动态' (News), '软件学习' (Software Learning), and '学习心得' (Learning Experience).

● 黑客基地

黑客基地是由国内外大型IT公司和安全公司的网络精英和安全专家共同联合发起设立，专门从事黑客技术与安全防范研究的非赢利性组织。黑客基地拥有国内最大、最强的黑客安全技术团队，黑客基地成员以前均为高水平的黑客高手，精通漏洞、木马、病毒、蠕虫、攻击/反攻击技术，深刻理解黑客技术精髓，有着丰富的黑客经验，掌握着最新的黑客和反黑客技术，不仅能够实施最强的黑客渗透攻击，而且能够采取最高强度的安全防范措施。

黑客基地的网址为 <http://www.hackbase.com/>。

The screenshot shows a Microsoft Internet Explorer window displaying the 黑客基地 homepage. The header reads '黑客基地' (HackBase). Below the header, there's a large banner with the text '全球最大中文黑客站' (The largest Chinese hacker station). A sub-header below the banner says '专业、诚信、权威' (Professional, Honest, Authoritative). There are several news items listed under the heading '最新动态' (Latest News), including titles like '【原创】小黑扫描快播 V1.0 的秘密' (Original: The secret of Xiaohe Scan Qihoo TV V1.0) and '【原创】浅谈对杀毒软件的恶意代码分析' (Original: A brief discussion on malicious code analysis of anti-virus software). At the bottom of the page, there's a link to '黑客主站' (Main Station).

● 中国 X 黑客小组

中国 X 黑客小组是一个集黑客技术、安全防御、编程技术于一体的黑客网站，内容比较新颖，其网址为 <http://www.cnxhacker.com/>。



● 黑白网络

黑白网络主要介绍各种黑客软件、黑客教程及黑客技术等，其网址为 <http://www.heibai.net/>。

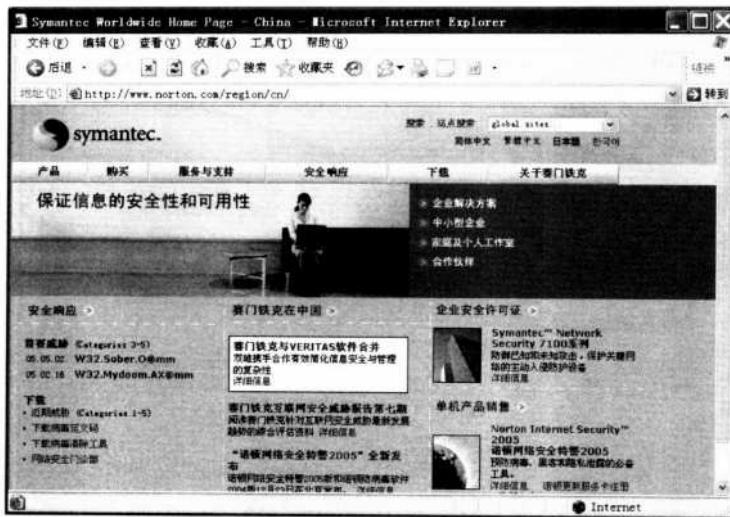


● 赛门铁克

赛门铁克是全球著名的信息安全企业，在安全领域具有相当权威的地位，正因为如此，



其官方提供的技术文件也成为黑客的理想教材。赛门铁克的网址为 <http://www.norton.com/region/cn>。



● 天天安全网

天天安全网是国内一个相当著名的黑客网站，除了提供大量黑客软件及黑客教程外，还提供最新的黑客软件升级信息以及系统、软件的相关安全新闻，其网址为 <http://www.ttian.net/>。



● Microsoft

作为全球最大的个人计算机操作系统开发商，Microsoft（微软）的官方网站上有大量的技术文件，这些文件都是黑客感兴趣的目标。此外，微软为了使其操作系统更安全，每当发现漏洞时就会立即在其官方网站发布系统补丁。但这样做反而为黑客了解操作系统的漏洞提供了方便。微软的中文网址为 <http://www.microsoft.com/china>。



以上介绍的只是黑客经常光顾的一部分网站，如果想了解更多此类网站，可通过本章后续介绍的搜索引擎进行搜索。

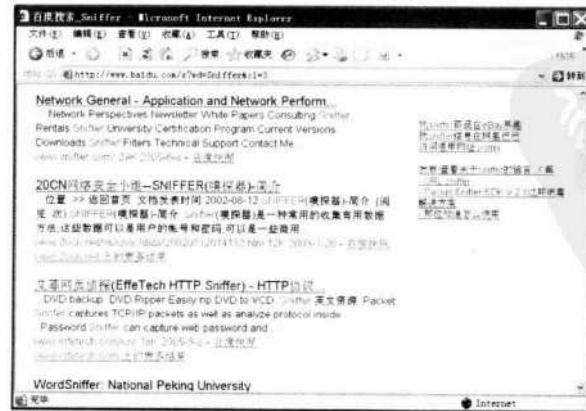
1.2.2 黑客杂志

黑客杂志也是黑客交流经验及了解最新信息的途径之一，世界上有很多国家都没有明文规定不能出版黑客杂志，因此黑客杂志在某些国家是非常流行的。此外，由于黑客技术与网络安全本身有着紧密的关系，因此也有一些黑客杂志公然打着网络安全的旗号出版，例如黑客 x 档案、看雪论坛等网站都有期刊出版，并且会出一些电子版书籍，供用户有偿下载。

值得一提的是，一些黑客杂志也有相关的官方网站，在这些网站上能看到部分杂志的内容。因此在无法购买到杂志的情况下，用户也可通过网站了解关于黑客的信息。

1.2.3 黑客常用的搜索引擎

网络上与黑客相关的信息虽然很多，但是这些信息往往非常杂乱，即使是有经验的黑客也难以在网站中找出自己需要的信息，因此黑客常会借助搜索引擎来寻找信息。例如，某黑客在使用某个 Sniffer 软件时遇到了困难，但一时又找不到关于这个软件的说明，此时就可以通过搜索引擎在网络上寻找相关的信息。

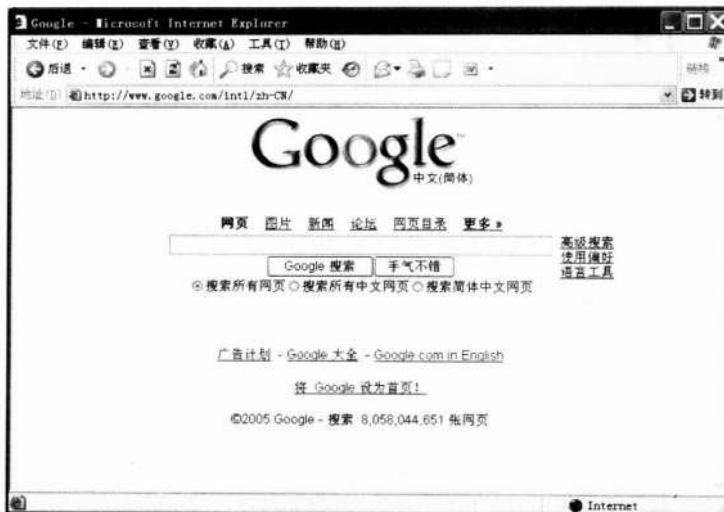




合理地利用搜索引擎，可以获得大量有用的信息，下面将介绍一些功能比较强大的搜索引擎。

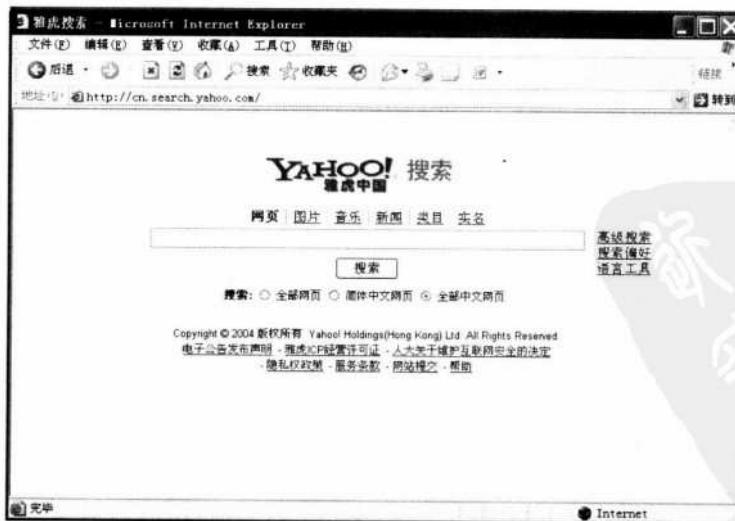
● Google

Google 是世界上用户数量最多的搜索引擎之一，以搜索功能强大而著称，但其缺点是搜索的结果较为散乱，用户必须从中筛选出有用的信息。Google 的网址为 <http://www.google.com/>。



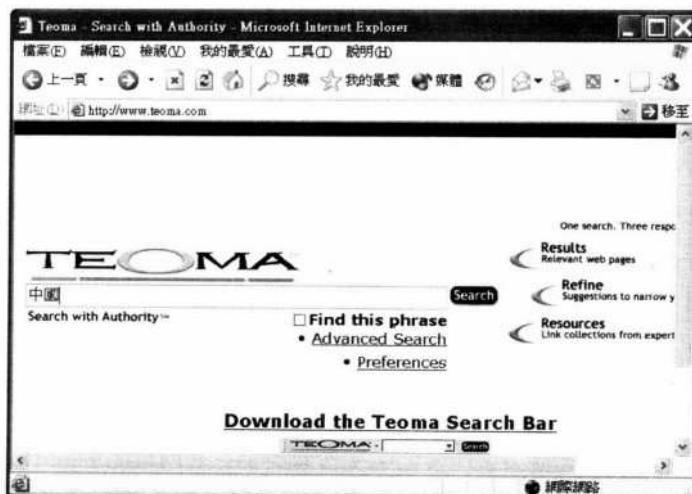
● Yahoo!

Yahoo!的搜索引擎也是黑客常用的引擎之一，与 Google 相比，Yahoo!的功能显然要弱一些，但由于 Yahoo!的搜索结果是经过精心筛选的，因此搜索的准确性要高于 Google，用户更容易从搜索结果中找出所需要的信息。yahoo!搜索引擎的网址为 <http://cn.search.yahoo.com/>。



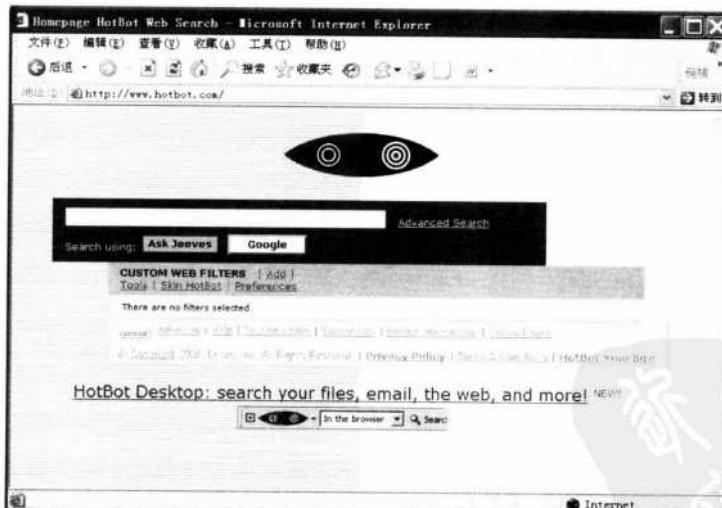
● Teoma

Teoma 是国外黑客较常用的搜索引擎之一，其搜索的准确性也相当高，受到很多用户的推崇。Teoma 的网址为 <http://www.teoma.com>。



● Hotbot

Hotbot 同样是国外黑客较常用的搜索引擎之一，无论是搜索的准确性与速度都相当出色，其网址为 <http://www.hotbot.com>。



● AOL Search

AOL Search 搜索引擎也相当出色，当用其他引擎找不到所需的信息时，不妨尝试一下这个引擎，可能会有意想不到的收获。AOL Search 的网址为 <http://search.aol.com/aolcom/webhome>。



● Baidu

百度搜索网站，是国人最为之骄傲的中文搜索引擎，其网址为 <http://www.baidu.com>。



1.3 黑客的攻击手法

在电影或电视中，黑客总是无所不能，任何防护森严的系统都可以在弹指之间成功入侵，事实上这些影片将黑客的能力夸张化了。现实生活中的黑客并非如此神奇，他们需要不断尝试各种方法，才有可能找到入侵的途径。

● 钓鱼法

钓鱼法顾名思义就是吸引用户上钩，最常见的就是通过广告或邮件吸引用户打开某些网页或执行某些程序，一旦用户上当，黑客就可以通过木马程序入侵这些计算机。

钓鱼法不将入侵的对象集中于某一台计算机，因此入侵成功的几率相当高。但是，这

种方法一般只能用于入侵一些警觉性不高的个人计算机，要想入侵服务器则比较困难。下图为通过广告信件入侵计算机的界面。



● 陷害法

如果直接攻击如果不能奏效，黑客往往也会从杀毒、防火墙软件着手，让这些防护软件出现故障，从而让用户落入病毒、蠕虫等恶意程序的包围，丢失数据，甚至被CIH等类型的病毒破坏硬件。

● 暴力法

暴力法并非指用武力去攻击对方，而是指通过特殊的软件不断猜测，直到找出正确的密码。也许有些读者会认为这种方法相当笨，但事实上这是一种非常实用的方法。因为许多计算机用户在设置密码时都没有足够的安全意识，经常用一些英文单词、生日等作为密码。这样的密码在黑客手中根本是不堪一击，借助软件的能力，黑客在几个小时甚至几分钟内就可以猜出密码。下图为在命令提示符窗口下执行密码猜测程序的界面。

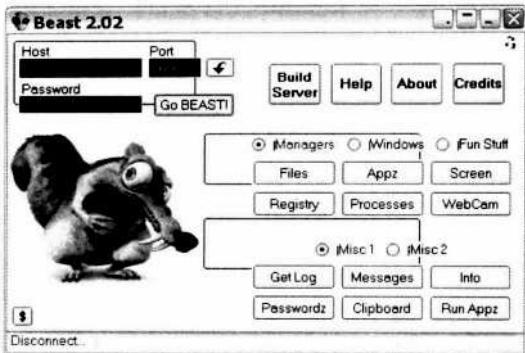
```
the plaintext
plain_len_min:      min length of the plaintext
plain_len_max:      max length of the plaintext
rainbow_table_index: index of the rainbow table
rainbow_chain_length: length of the rainbow chain
rainbow_chain_count: count of the rainbow chain to generate
file_title_suffix:   the string appended to the file title
-bench:              add your comment of the generated rainbow table here

example: rtgen lm alpha 1 7 0 100 16 test
          rtgen md5 byte 4 4 0 100 16 test
          rtgen sha1 numeric 1 10 0 100 16 test
          rtgen lm alpha 1 7 0 -bench

E:\downloads\password\rainbowcrack-1.2-win>
```

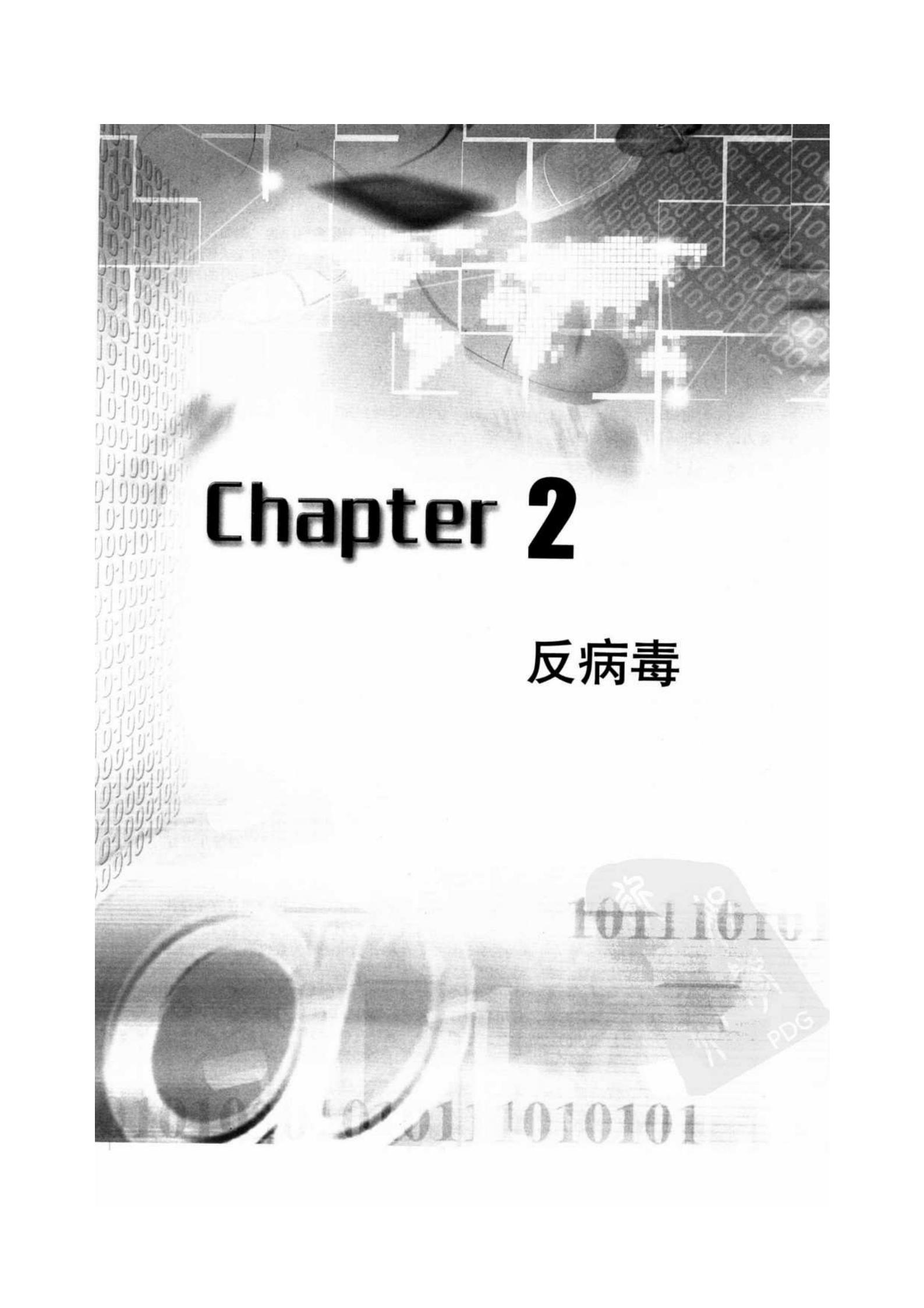
● 后门法

后门法也是黑客最常用的方法之一，这里所说的后门有两类，一类是指因为各种原因感染了木马程序，此时木马程序会在计算机中打开一个隐蔽的后门，黑客就可以通过这个后门自由地进出。下图为木马程序界面。



还有一种后门是指在编写软件时因考虑不周而出现的漏洞，这些漏洞有可能被黑客利用。这种情况在操作系统上最为严重，因为操作系统本身就是结构非常复杂的软件，因此出现漏洞的机会非常多，所以软件开发商不得不经常提供修正文件供用户修补系统漏洞。





Chapter 2

反病毒



随着计算机应用的普及，计算机病毒为人们的生活带来越来越多的困扰。例如，因感染计算机病毒而导致员工的薪资表等重要文件损坏，因为蠕虫病毒袭击网络而无法传递邮件等。更为可怕的是，现在的病毒感染计算机的方式越来越高明，例如曾猖獗一时的冲击波病毒（WORM MS Blaster）就是利用系统的 RPC 漏洞来进行感染的。如果未能及时安装操作系统更新补丁，用户登录网络时不需执行任何操作就有可能感染病毒，使人防不胜防。本章将详细介绍反病毒的方法。

2.1 分析病毒

为了对付病毒，首先要搞清楚它们的来历，这样才能做到知己知彼，百战百胜。下面就为读者揭开病毒的神秘面纱。

2.1.1 认识病毒

直到目前为止，关于计算机病毒的定义仍是一个争论不休的问题，这是因为计算机病毒的发展非常快，因此对其做出的定义很容易会因为新的病毒出现而失效。《中华人民共和国计算机信息系统安全保护条例》中明确定义计算机病毒是指“编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码”，这也是目前我国最具权威性的计算机病毒定义。从这个定义中可以清楚地了解到，计算机病毒具有以下两大特征：

- ① 影响计算机正常使用。
- ② 具有自我复制功能。

下面将对病毒进行深入的分析。

● 计算机病毒的产生

计算机病毒不是自然存在的，而是由一些技巧高超的程序设计人员精心编写，他们之所以会制造计算机病毒，多为以下几个理由：

● 炫耀自己的技术

由于制造计算机病毒往往需要相当高的技术水准，因此制造病毒也成为一些技术人员炫耀自己能力的方法。不过，由于这些技术人员并无恶意，因此这类病毒破坏性比较轻。例如，当病毒程序执行后会显示一段动画、播放一段音乐或者是让用户回答几道智力题等。

● 报复心态

人们在受到不公平的对待之后，难免会产生报复心理，如果这种情况出现在程序设计人员身上，就会比较危险。一些程序设计人员在受到不公平的对待之后，就会编写一些危险的程序对他人进行报复，事实上因为这种原因而产生的计算机病毒为数也很多。

● 版本保护

为了维护自身的利益，一些软件开发商会在自己的产品中加入特殊的病毒，一旦用户非法复制软件，病毒就会发作，对用户的计算机进行破坏。但是根据法律规定，软件开发商的这种行为也是违法的，也要受到法律制裁，因此目前这类计算机病毒已经极少见。

● 计算机病毒的特征

计算机病毒虽然层出不穷，但其基本的特征往往还是相同的，了解这些特征之后，就可以很容易地判断出一个程序是属于计算机病毒还是一般的程序。计算机病毒共有的特征主要有以下几项：

● 传染性

绝大部分的计算机病毒都具有自我复制的能力，它们会感染正常的程序以达到传播的目的，部分计算机病毒甚至还可以通过电子邮件等方式感染其他的计算机。

● 破坏性

计算机病毒在感染计算机后，或多或少地都会对计算机造成影响，但是不同的计算机病毒对计算机的影响程度不同。良性的病毒可能只是显示一段动画或者一些恶作剧，不会对计算机进行破坏；而恶性的病毒则会删除文件、格式化硬盘、破坏操作系统等，甚至有一些病毒还会损坏硬件装置，例如 CIH 病毒。

● 隐藏性

计算机病毒感染计算机后，通常会将自己暂时隐藏起来，例如伪装成正常的系统程序将自身写入系统文件中，以避免被用户察觉。当系统条件成熟时，它就会显露出本来的面目，开始大肆破坏。

● 计算机病毒的种类

由于计算机病毒千变万化，新品种层出不穷，因此有必要对病毒进行合理的分类，以便了解与掌握。

计算机病毒的分类方法有很多种，例如可以按照感染的操作系统分类、按照寄生的方式分类、按照传染的途径分类等。目前，较流行的分类方式是根据病毒的寄生方式与感染途径来分类，可以将病毒分成启动型、文件型、混合型及宏病毒等几大类。

● 启动型病毒

启动型病毒主要感染存储设备的启动分区及文件分配表，在启动计算机的过程中，计算机首先会执行启动分区，因此这类病毒在操作系统启动之前就已经执行。

启动型病毒一般通过软盘来传播，由于目前软驱已经逐渐被淘汰，因此单纯的启动型病毒已经很少见，而是采用与其他类型病毒相结合的方式进行感染。

● 文件型病毒

文件型病毒主要感染 EXE、COM 等可执行文件，用户只要执行了被病毒感染的文件，病毒就会发作。病毒感染计算机后，又会伺机感染计算机内的其他文件。

文件型病毒是较为常见的病毒种类，目前流行的病毒大部分都属于此类，例如 2005 年 5 月 17 日国内反病毒监测网瑞星公司发现的新 CIH 病毒等。

● 宏病毒

宏病毒是病毒中的后起之秀。微软为了方便用户执行重复性的操作，在 Office 系列办公软件中加入了宏功能，虽然宏的确为用户带来了不少方便，但同时也导致了一种新式病毒的诞生。由于宏的使用相对比较简单，因此用宏编写的计算机病毒很快就流行了起来。

宏病毒主要存在于 Word 文档中，用户一旦打开包含有宏病毒的文件，病毒就会发作，



并对计算机进行破坏。由于微软的办公软件被广泛使用，因此宏病毒也随之广泛流行。

● 混合型病毒

顾名思义，混合型病毒是指同时具有前面几种特征的病毒，与单一特征的病毒相比，混合型病毒的危害性更大，更难被防毒软件清除。

● 计算机病毒的历史

事实上，计算机病毒并非是新出现的事物，早在计算机诞生初期，著名的计算机先驱冯·诺依曼（Von Neumann, John）就已经在他的一篇论文《复杂自动装置的理论及组织的进行》里勾画出了计算机病毒程序的蓝图——能够自我复制的【自动机】，但当时大部分计算机专家都认为那是不可能发生的。

1960 年，一名美国计算机专家编写了一个名为【生命游戏】的程序，第一次成功完成了程序的自我复制，当【生命游戏】执行时，会在屏幕上显示许多【生命元素】。当这些生命元素过于拥挤时，就会因缺少生存空间而死亡，而元素过于稀疏时，也会因相互隔绝失去生命支持环境而死亡。只有当处于合适的环境时，生命元素才会大量繁殖，这种可以自我复制的程序可以认为是计算机病毒的雏形。

大约在冯·诺依曼提出计算机病毒概念 10 年后，美国电话电报公司（AT&T）的贝尔（Bell）实验室里的 3 个年轻人，道格拉斯·麦耀莱（H. Douglas McIlroy）、维特·维索斯基（Victor Vysotsky）及罗伯·莫里斯（Robert T. Morris）发明了一种称为磁芯大战（Core War）的游戏。该游戏的规则如下：双方各编写一套计算机程序，然后将程序输入到一台计算机中，开始游戏后两套程序在计算机的存储系统（磁芯）内互相追杀，直到一方将另一方完全消灭为止。用于磁芯大战的程序实际上已经具有了计算机病毒的典型特征：自我复制以及具有破坏性。

由于早期的计算机都是独立工作的，因此当某台计算机被病毒感染而失去控制时，只要将计算机关闭即可。然而，当越来越多的计算机通过网络连接在一起时，计算机病毒就成了灾难。1986 年初，巴基斯坦的巴锡特（Basit）和阿姆杰德（Amjad）两兄弟编写了 Pakistan 病毒，并在一年后流传到全世界；1988 年 3 月，一种苹果机的病毒发作，受到感染的计算机在 3 月 2 日这天停止工作，并显示【向所有苹果计算机的使用者宣布和平的信息】以庆祝苹果机生日；1988 年 11 月 2 日，美国的一名研究生编写了一个蠕虫病毒并将其放到因特网上，导致 6000 多台计算机受到感染。直到今天，计算机病毒不但没有消失，反而越演越烈。

2.1.2 认识蠕虫病毒

蠕虫也属于病毒，具有自我复制的功能，但它又非常特殊，其最大的特征就是通过网络大量传播，阻塞网络或者攻击服务器，进而导致网络瘫痪。

随着 Internet 的不断发展，越来越多的计算机通过网络连接在一起，从而为蠕虫提供了极好的生存空间，一些新出现的蠕虫甚至可以在短短几天的时间内蔓延至全世界。因蠕虫攻击而导致网络瘫痪的新闻屡见不鲜，例如 2003 蠕虫王（Worm.NetKiller2003）、2005 年 5 月 23 日爆发的 Sober.p 蠕虫等。

● 蠕虫的种类

按照蠕虫攻击对象的不同可以大致将其分成两类：一类是专门针对企业级用户的蠕虫，

这类蠕虫大多通过系统的漏洞来入侵网络上的服务器，具有主动攻击的特征，可以在短时间内造成网络服务中断，例如震荡波及其变种（I-Worm/Sasser）、网络天空及其变种（I-Worm/NetSky）、挪威客及其变种（I-Worm/Novarg）等。它们都属于蠕虫病毒，并且都属于主动攻击型病毒；另一类则是针对一般的个人用户，这类蠕虫主要通过电子邮件、网页等方式欺骗用户执行，但也有少部分是通过应用程序的漏洞入侵，例如挪威客蠕虫的新变种就属于此类。

● 蠕虫的危害

蠕虫会在网络上大量繁殖，堵塞网络数据传输，加重网络的负担，导致网络传输速率降低，从而使得用户浏览网页或通过网络传输数据受到影响。此外，蠕虫还会攻击网络上的服务器，使服务器无法正常工作，例如蠕虫大肆攻击网络上的 DNS 服务器，就会导致许多人无法正常浏览网页。

除了导致网络故障外，一些蠕虫还具有破坏用户计算机的能力，例如 Gunsan 蠕虫也会删除操作系统的必备文件防毒软件的文件。

2.2 病毒入侵

通过前面的介绍，我们对病毒的危害性已经有了一定的了解，本节将介绍病毒入侵计算机的途径，从而人们能够有效地防御病毒的入侵。

2.2.1 病毒感染计算机的途径

计算机病毒虽然层出不穷，但其感染途径并非无迹可循，只要针对感染的途径做好防御，就可以有效地阻止大部分病毒入侵。一般来说，病毒感染计算机的途径主要有以下几种：

● 通过可执行文件

这是最常见的病毒感染计算机的方式之一，用户只要执行带有病毒的文件就会被感染。



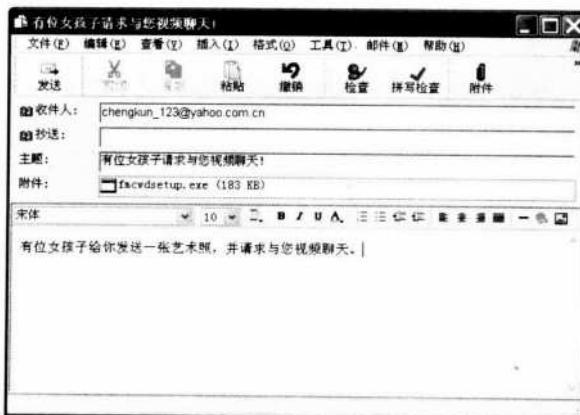


● 通过启动盘

启动型病毒经常会隐藏在软盘中，用户一旦使用带有病毒的启动软盘，病毒就会感染计算机。需要注意的是，非启动软盘也有可能带有病毒。

● 通过电子邮件

一些病毒在感染计算机后，会搜索受害者计算机的通讯簿，并将带毒的邮件传递给通讯簿中的联系人，收到邮件的用户只要阅读这些带有病毒的邮件就会被感染。然后，病毒再次读取被感染计算机中的通讯簿，并发送带病毒的邮件，这样病毒的感染范围就会迅速扩大。



● 通过网页

通常一些病毒还会隐藏在网页中，当用户浏览含有病毒的网页时，病毒就会被自动下载到用户的计算机中并执行其破坏功能。

● 通过软件漏洞

在编写软件过程中，由于各种原因难免会出现考虑不周的情况，包括操作系统在内的各种软件都或多或少地存在着漏洞，如果用户未能及时安装补丁程序，就很容易会感染到这类病毒。

前面介绍的是目前较流行的病毒感染计算机的途径，事实上这里所说的只是其中的一部分，病毒感染计算机的途径远不止这些。另外，通过 FTP、聊天软件等也有可能感染病毒，因此用户在使用时要多加注意。

2.2.2 常见的病毒入侵

前面已经介绍了病毒感染计算机的方式，为了加深印象，下面将以目前较流行的几种病毒为例，以实例说明计算机病毒的入侵过程。

● 爱情森林病毒

【爱情森林】病毒是结合网页与聊天软件来入侵计算机的，当用户浏览含有此病毒的网页时，病毒就会自动下载到浏览器的计算机中，感染计算机后，还会自动搜索并感染计算机中安装的聊天软件。此后，当与他人聊天时，病毒会自动在聊天信息后面加上一个连接到病毒网页的超级链接，当对方打开这个网页时，又会成为下一个受害者。



● Nimda 病毒

Nimda 病毒共有 3 种传播途径，一是通过电子邮件，利用 Outlook 程序的漏洞，用户无须阅读邮件就会中毒，成功感染计算机后，Nimda 会在受害者的计算机上制造和传递大量的病毒邮件，再试图感染其他计算机。

Nimda 病毒的第二种传播途径是通过微软 IIS (Internet Information Services) 程序的一个漏洞，如果作为服务器的计算机未安装修正文件就会被 Nimda 入侵。

Nimda 病毒的第三种传播途径是通过局域网，当局域网内的任意一台计算机感染 Nimda 后，其他的计算机也有感染的危险。

● 口令病毒

口令病毒会不断猜测网络上计算机的密码，一旦成功破解密码后，它就会入侵这台计算机并在这台计算机上安装特洛依木马程序。由于口令病毒会在网络上大量繁殖并不断猜测计算机的密码，所以会造成网络的阻塞。

以上介绍的是目前较流行的几种病毒，用户如果想了解更多、更新的病毒信息，可以浏览各防毒软件开发商的网站，在这些网站上通常会有关于各种病毒的详细信息。

2.3 追踪病毒

一般来说，高级的用户通常会采用手动的方式来删除病毒与蠕虫。如果不具备有这样的技能，也可通过防毒软件轻松地清除计算机中的病毒与蠕虫。

2.3.1 流行的杀毒软件

杀毒软件顾名思义是指专门用于清除计算机病毒的软件，较早期的杀毒软件主要针对病毒，但由于目前病毒与蠕虫之间的界线越来越模糊，许多杀毒软件也把蠕虫当成是病毒的一种，因此市场上的杀毒软件绝大部分都具有清除蠕虫的能力，部分杀毒软件甚至兼有防御黑客入侵的功能。

目前，较流行的杀毒软件主要有赛门铁克公司的 Norton AntiVirus、趋势科技的 PC-cillin 及 McAfee 公司的 McAfee VirusScan 等，下面将分别介绍这些软件。

● Norton AntiVirus

赛门铁克是一家老牌的系统安全开发商，其产品在计算机安全领域有着相当高的地位。

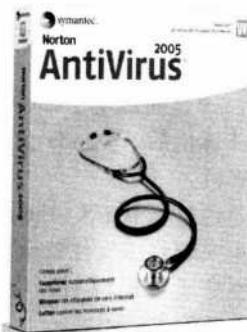


Norton AntiVirus 就是其所开发的专业杀毒软件，共分为两大系列，其中针对企业用户的版本以【X.X】命名，如 Norton AntiVirus 9.0 企业版；而针对个人用户的版本则以【200X】命名，如 Norton AntiVirus 2005。

Norton AntiVirus 是商业软件，用户需要购买后才能使用。赛门铁克的官方网站为 <http://www.symantec.com/region/cn>。

● PC-cillin

趋势科技公司以计算机安全、病毒防治为主要业务范围，旗下的杀毒软件 PC-cillin 已经成为全球知名的杀毒软件之一，不少主板厂商都会在其产品中附赠此软件。下图为零售版盒装 Norton AntiVirus 2005 的外观图。



PC-cillin 同样是商业软件，但用户可以到趋势科技的官方网站下载最新的试用版本。

● McAfee virusscan

McAfee virusscan 也是目前较为流行的杀毒软件之一，是计算机安全公司 McAfee 的产品。McAfee virusscan 以其简便的操作及完善的功能获得很多用户的信赖，其官方网址为 <http://www.mcafee.com/cn/>。下图为零售盒装 McAfee 杀毒软件。



2.3.2 实战防病毒

目前流行的杀毒软件很多，但其功能与操作方式都很相似，用户只要掌握其中一套软件，就能很容易地使用其他软件。

注意：一些用户为了提高防毒效果，可能会在计算机中同时安装多套防毒软件，事实上这种做法是不值得推荐的。因为同时安装两套以上的防毒软件不仅会消耗更多的系统资源，而且还有可能造成杀毒软件之间互相冲突而导致某些功能失效。下面将以目前较为流行的 PC-cillin 2005 为例进行介绍。

● 安装 PC-cillin 2005

PC-cillin 2005 是商业软件，试用版本有时间限制，且不能在线更新，因此为了获得更好的防护效果，建议用户购买正式版本。

趋势科技的官方网站提供了 PC-cillin 2005 网络安全版试用版本的下载功能，可按以下步骤下载安装并进行设置。

STEP1 下载 PC-cillin 2005

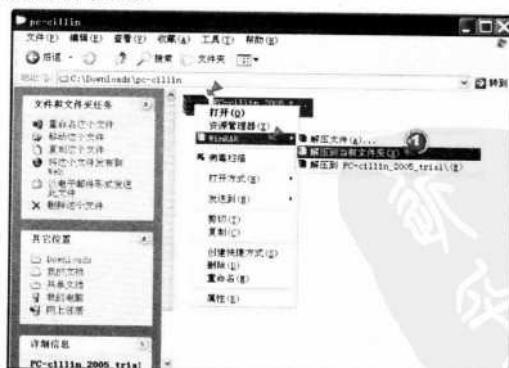
进入趋势科技官方网站的下载专区，下载 PC-cillin 2005 网络安全版。



STEP2 解压缩文件

下载的 PC-cillin 2005 安装文件实际上是一个压缩文件，必须解压缩后才能继续安装，故需设置解压缩文件的储存位置。

- ① 右键单击压缩包并依次选择【WinRAR】→【解压到当前文件夹】命令，解压缩文件

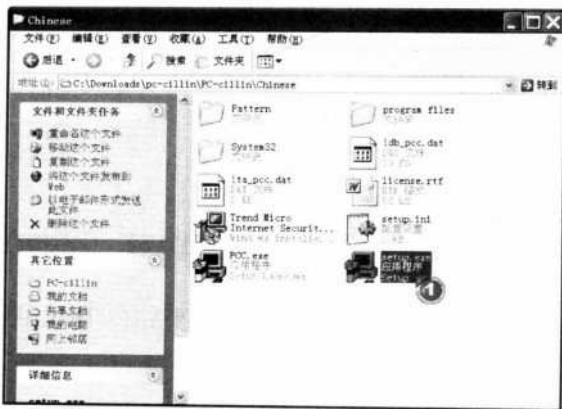


STEP3 执行安装程序

将文件解压缩后进入安装文件夹，双击 setup.exe 文件，进行安装。



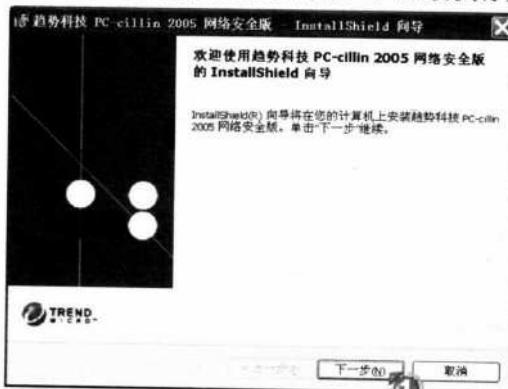
① 双击安装文件



STEP4 跳过欢迎画面

单击【下一步】按钮，跳过安装向导的欢迎窗口，继续执行安装。

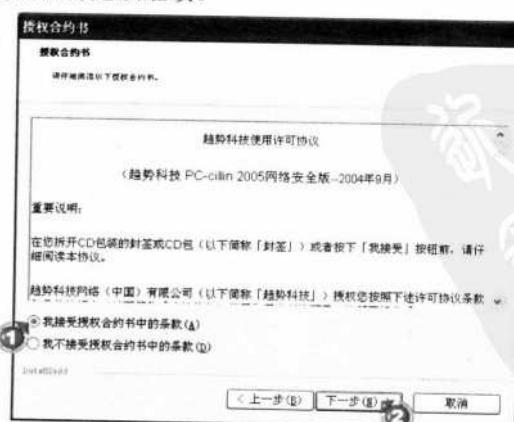
① 单击【下一步】按钮



STEP5 接受授权合约书

在【授权合约书】对话框中，显示趋势科技对此软件的授权合约，阅读完毕后选择【我接受授权合约书中的条款】单选框并单击【下一步】按钮继续安装。注意，如果不接受合约，安装过程将无法继续。

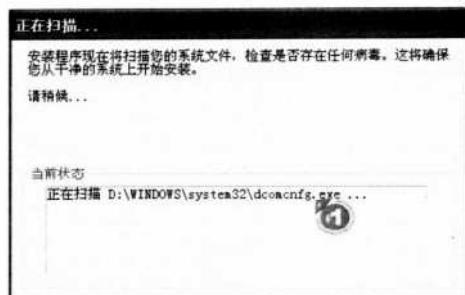
- ① 选择【我接受授权合约书中的条款】单选框
- ② 单击【下一步】按钮



STEP6 安装前进行扫描工作

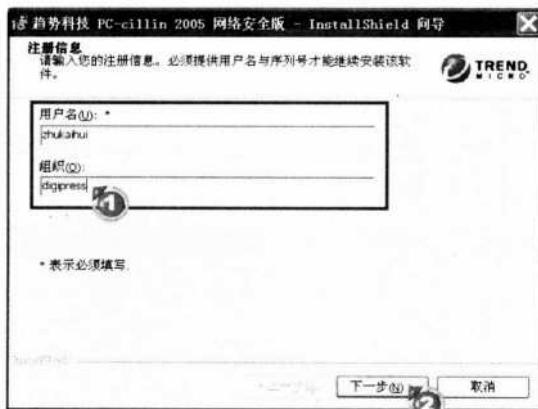
为了确保程序安装成功，向导会先扫描计算机的系统文件，以清除可能存在的病毒及蠕虫。

- ① 正在执行安装前的扫描工作

**STEP7** 输入注册信息

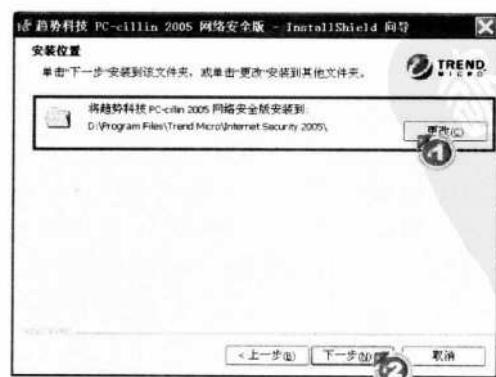
在【注册信息】对话框中输入用户名、组织信息。

- ① 输入注册信息
- ② 单击【下一步】按钮

**STEP8** 设置安装位置

在【安装位置】对话框中，程序已经默认一个安装位置，用户可以单击【更改】按钮更改安装位置，这里保持默认设置即可，然后单击【下一步】按钮。

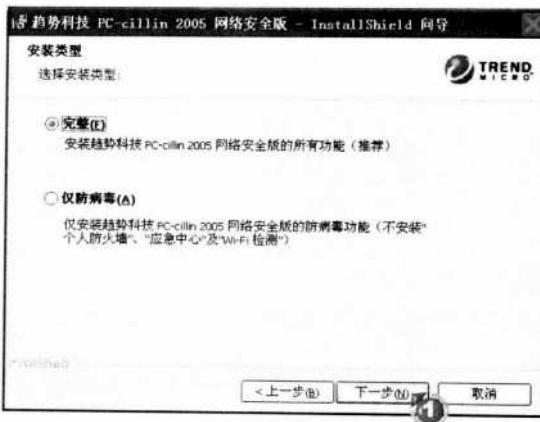
- ① 可单击【更改】按钮
更改安装位置
- ② 单击【下一步】按钮



**STEP9** 设置安装类型

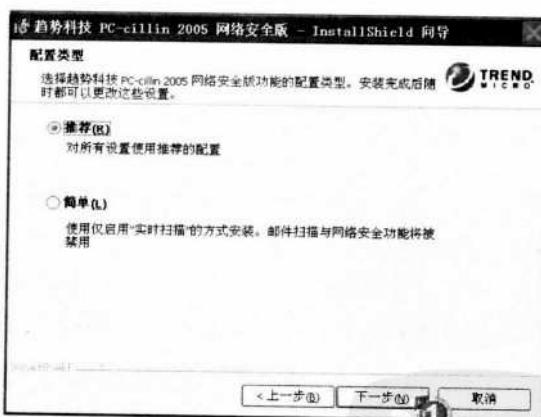
在【安装类型】对话框中，PC-cillin 2005 提供了两种安装类型。默认为【完整】安装，将得到更安全的防护。如果用户的计算机硬件设备配置很低，可以考虑选择【仅防病毒】类型。否则，无需修改此处设置，单击【下一步】按钮即可。

- ① 单击【下一步】按钮

**STEP10** 配置类型

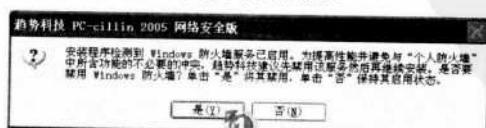
选择好一种安装类型后即可配置类型，如果对 PC-cillin 软件的设置不熟悉，则不要修改此处设置，保持【推荐】配置选项即可。

- ① 单击【下一步】按钮

**STEP11** 停止 Windows 防火墙

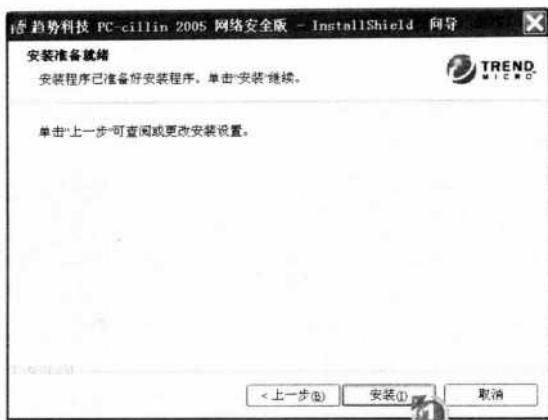
由于 PC-cillin 2005 网络安全版自身集成了防火墙功能，如果用户的操作系统已经升级到最新的 Windows XP SP2，安装 PC-cillin 2005 就有可能同系统自带的防火墙产生冲突，因此在此设置关闭系统自带防火墙功能。

- ① 单击【是】按钮，关闭系统防火墙。



STEP12 开始安装

单击【安装】按钮，开始安装。

① 单击【安装】按钮**STEP13** 完成安装

安装完成后，单击【完成】按钮，结束安装向导，此时会提示用户重新启动计算机使配置生效。

① 单击【完成】按钮，结束安装向导**● 扫描所有磁盘**

为了确保计算机的安全，用户应每隔一段时间就通过PC-cillin 2005扫描计算机中的所有的磁盘，以清除可能存在的病毒及蠕虫。此外，当怀疑计算机感染病毒时，也应扫描所有的磁盘。

由于扫描所有磁盘所需的时间较长，因此一般情况下建议用户选择较空闲的时间执行。

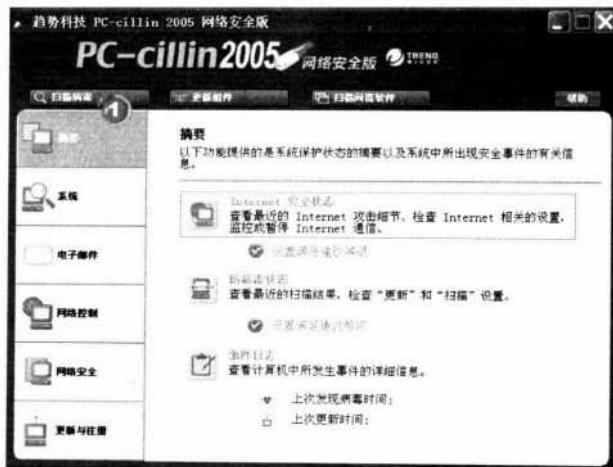
STEP1 扫描病毒

PC-cillin 2005提供了【扫描病毒】的功能，用户只要在程序主窗口中单击【扫描



【病毒】按钮即可对所有磁盘进行扫描。

① 单击【扫描病毒】按钮



STEP2 检视扫描信息

扫描过程中，程序会显示扫描的进度，用户可以单击对应的按钮，暂停或停止扫描工作。扫描时间的长短与磁盘大小有关。

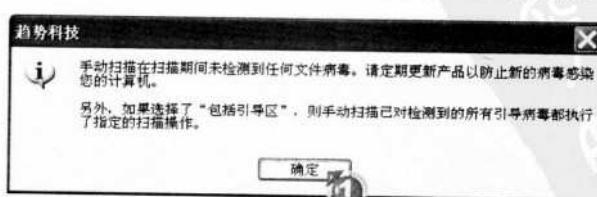
① 扫描的进度



STEP3 检视扫描结果

扫描结束后，程序弹出一个对话框显示扫描结果，检视完毕后单击【确定】按钮。

① 单击【确定】按钮



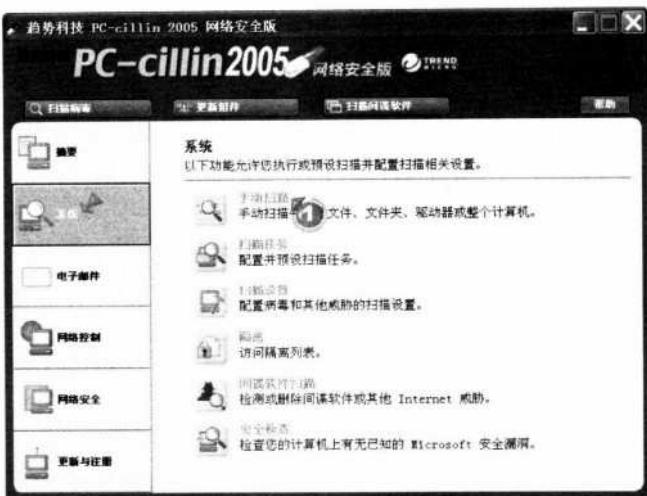
● 手动扫描

前面所介绍的扫描所有磁盘的方式，在清除病毒及蠕虫上较干净彻底，但存在耗时较长的弊病。事实上，在很多时候用户只需扫描某些特定的位置即可，例如在下载文件后，用户只需扫描下载的文件，此时就需要使用下面将要介绍的手动扫描功能。

STEP1 进入手动扫描

在PC-cillin 2005程序主窗口中依次单击【系统】→【手动扫描】项目进入手动扫描窗口。

- ① 依次单击【系统】→【手动扫描】项目



STEP2 选择扫描任务

手动扫描窗口提供了两种扫描方式，一种是通过设置好的任务进行扫描，另一种则比较灵活，用户可设置需要扫描的磁盘或某个文件夹。下面以扫描某个文件夹为例来说明手动扫描。

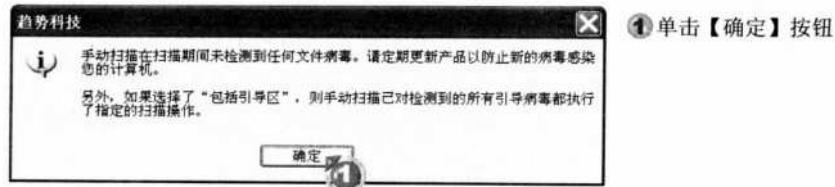
- ① 选中【选择要扫描的驱动器或文件夹】单选框
② 展开分区前面的加号，并选择文件夹
③ 单击【扫描】按钮





STEP3 检视扫描结果

扫描完成后，程序会显示扫描结果，检视完毕后单击【确定】按钮，结束扫描工作。



● 设置 PC-cillin 2005

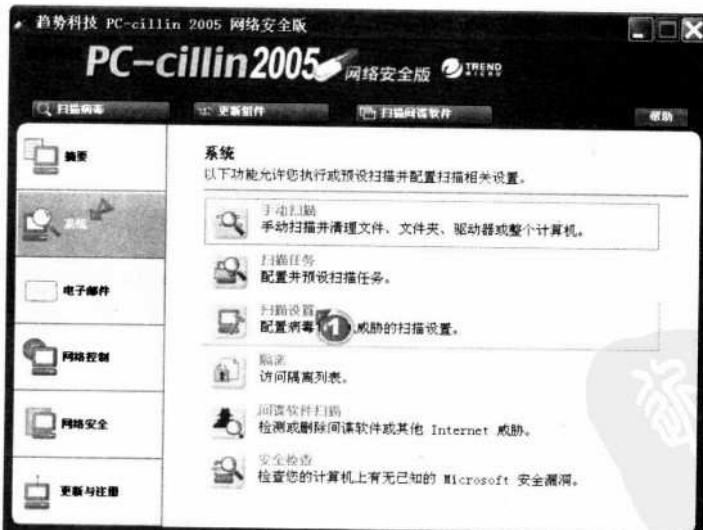
虽然 PC-cillin 2005 的默认选项已经可以满足大部分用户的需求，但程序仍然提供了较丰富的设置选项，用户可以调整程序使其更符合自己的实际需求。

下面将以实例的方式，简单讲解 PC-cillin 2005 的常用设置功能。在设置时需要注意：除非清楚了解设置的结果，否则不要随意更改设置，因为如果一些功能设置不当有可能会导致较严重的后果，例如会误删有用的文件或者漏掉某些病毒等。

STEP1 打开扫描设置窗口

通过程序主窗口中的【系统】项目打开【扫描设置】窗口，以便进行手动扫描设置。

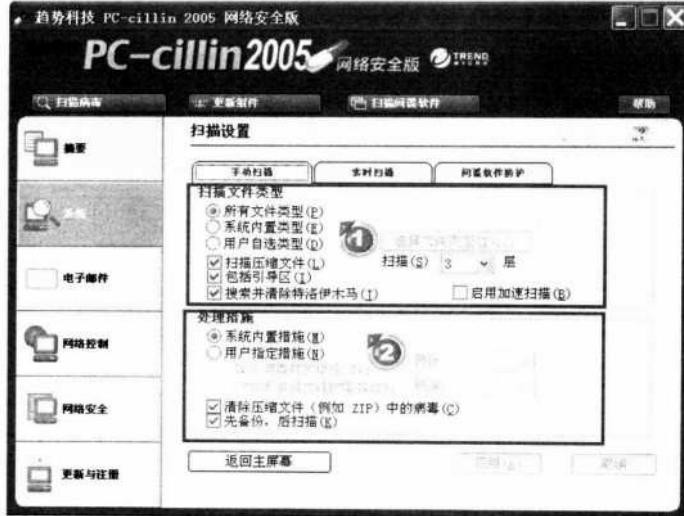
① 依次单击【系统】→【扫描设置】选项



STEP2 设置手动扫描

设置要扫描的文件格式以及发现病毒后可采取处理措施，此设置将会直接影响【扫描病毒】及【扫描所有磁盘】两项功能。

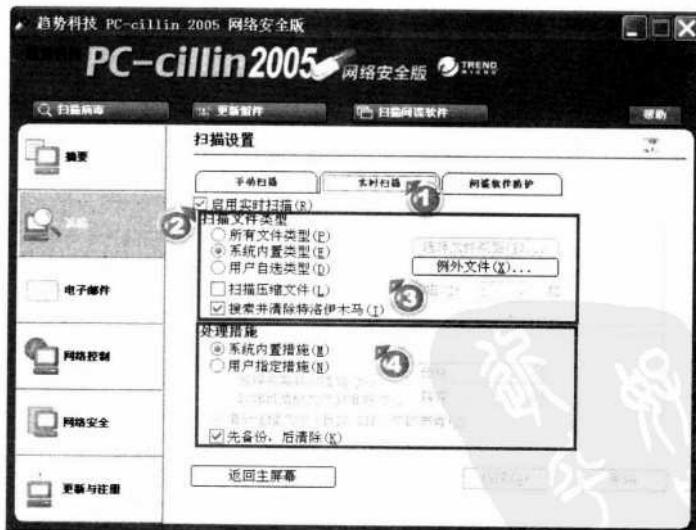
- ① 设置要扫描的文件类型
- ② 设置发现病毒时的处理措施



STEP 3 设置实时扫描

【实时扫描】功能能够拒绝病毒对系统安全漏洞的访问，这是手动扫描所做不到的，因此这项功能相当于病毒防火墙，如果病毒企图入侵计算机，就会立即被拦截并清除。

- ① 选择【实时扫描】选项卡
- ② 选择【启动实时扫描】复选框
- ③ 设置要扫描的文件类型
- ④ 设置发现病毒时的处理措施

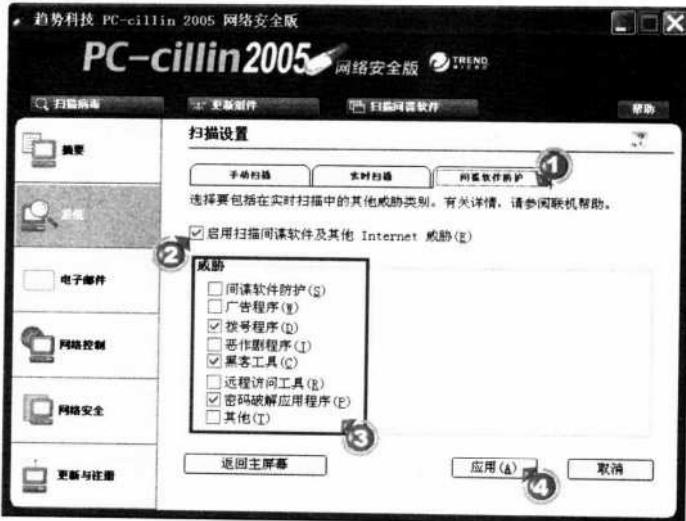


STEP 4 设置间谍软件防护

PC-cillin 2005 可以防护广告程序、恶作剧程序、黑客工具、远程访问工具、密码破解程序等间谍软件。

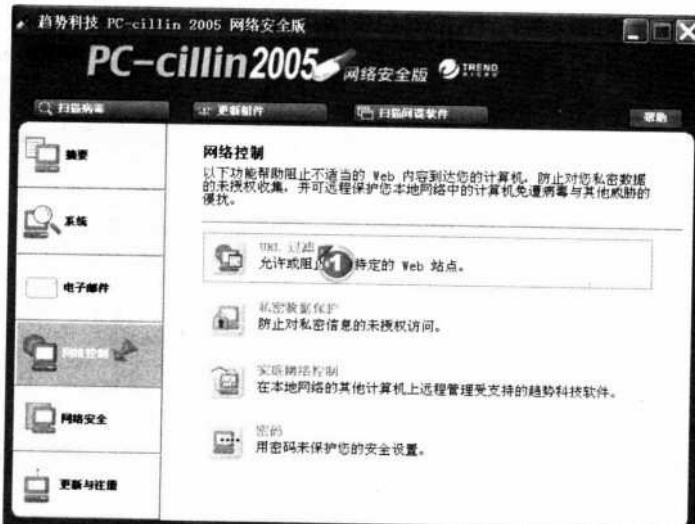


- ① 选择【间谍软件防护】选项卡
- ② 选择【启用扫描间谍软件及其他 Internet 威胁】复选框
- ③ 在【威胁】栏中选择需要防护的选项
- ④ 单击【应用】按钮



STEP 5 打开 URL 过滤面板

URL 过滤功能能够允许或阻止访问特定的站点。

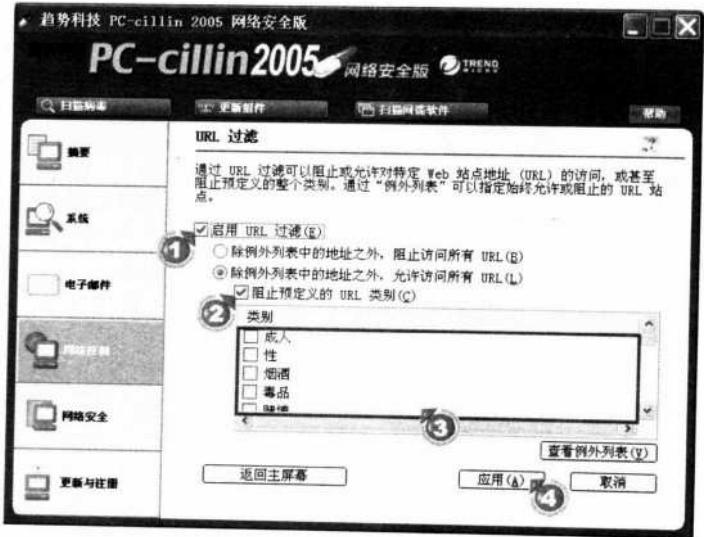


- ① 依次选择【网络控制】→【URL 过滤】选项

STEP 6 启用 URL 过滤

选择【启用 URL 过滤】复选框，再选择【阻止预定义的 URL 类别】复选框，在【类别】列表中即可选择特定的类别。

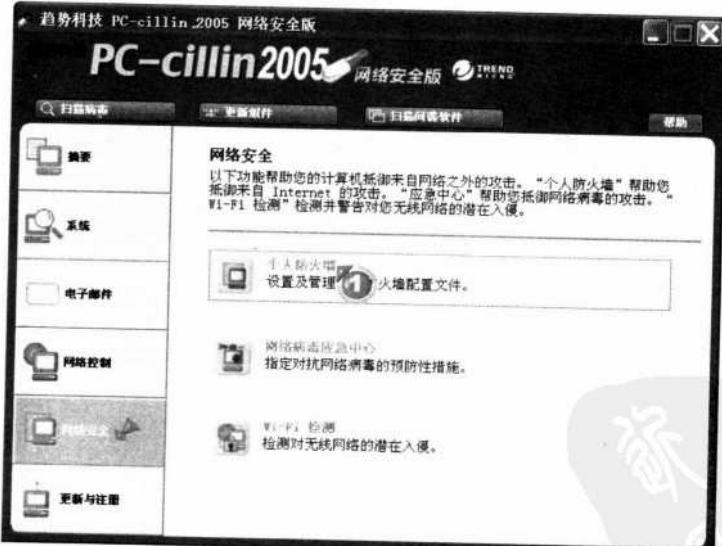
- ① 选择【启用 URL 过滤】复选框
- ② 选择【阻止预定义的 URL 类别】复选框
- ③ 可在此选择预定义的过滤类别
- ④ 单击【应用】按钮



STEP7 进入个人防火墙设置

PC-cillin 2005 提供了个人防火墙功能，这也是主流杀毒软件的发展趋势。单击【网络安全】→【个人防火墙】选项。

- ① 依次单击【网络安全】→【个人防火墙】选项

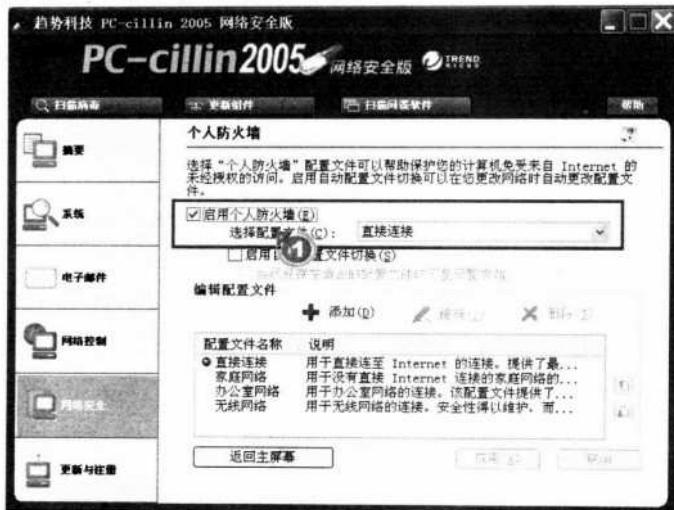


STEP8 启用个人防火墙

PC-cillin 2005 提供的防火墙虽然没有专业防火墙功能强大，但是对于家用网络的安全防护已经足够，默认情况下防火墙是启动的，如果防火墙未曾启动，可在此选择【启用个人防火墙】复选框。



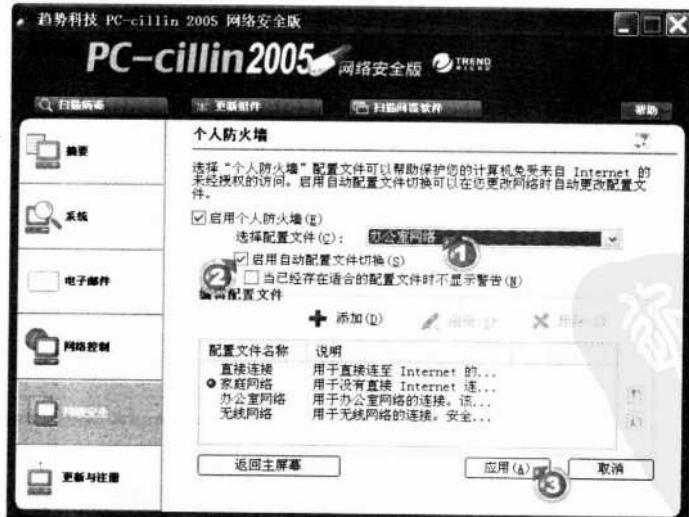
① 可在此选择【启用个人防火墙】复选框



STEP 9 选择连接方式

单击【选择配置文件】右侧的下拉按钮，选择一种连接方式，如果是一台计算机通过 ADSL 上网，则保持默认设置即可；如果家中有多台计算机共享上网，则可选择【家庭网络】选项；如果是公司的局域网，则可以选择【办公室网络】；如果是无线上网，则选择【无线网络】。

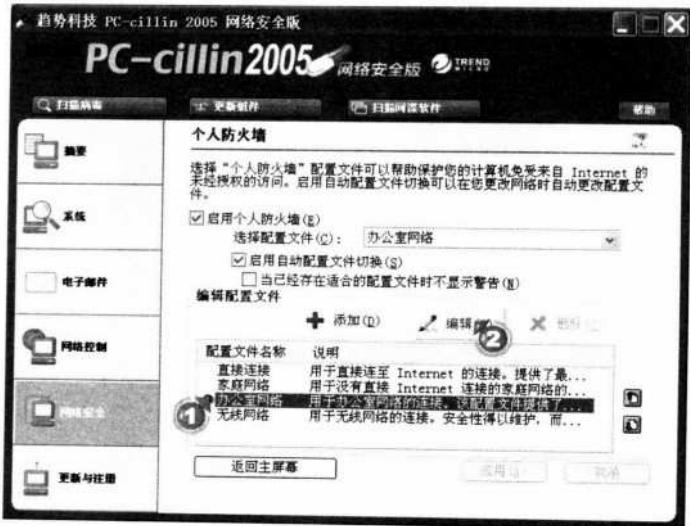
- ① 选择一种连接方式的配置文件
- ② 选择【启用自动配置文件切换】复选框
- ③ 单击【应用】按钮



STEP 10 编辑配置文件

对选择的配置文件进行编辑，以适合系统环境。

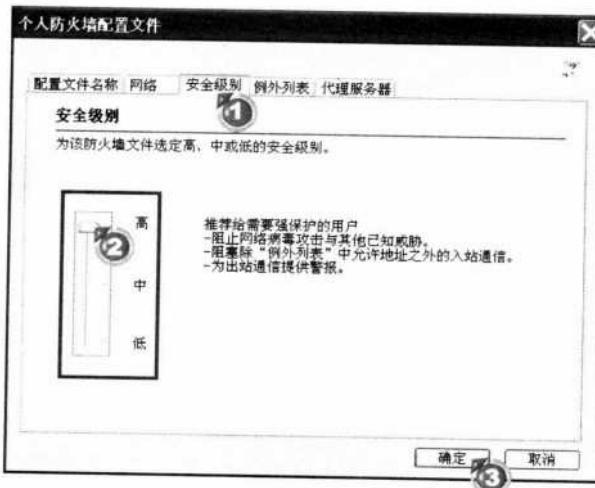
- ① 单击选择的配置
文件名称
② 单击【编辑】按钮



STEP11 设置安全级别

在编辑面板中设置防火墙的安全级别。

- ① 选择【安全级别】选项卡
② 拖动游标至【高】
③ 单击【确定】按钮



2.4 病毒的预防

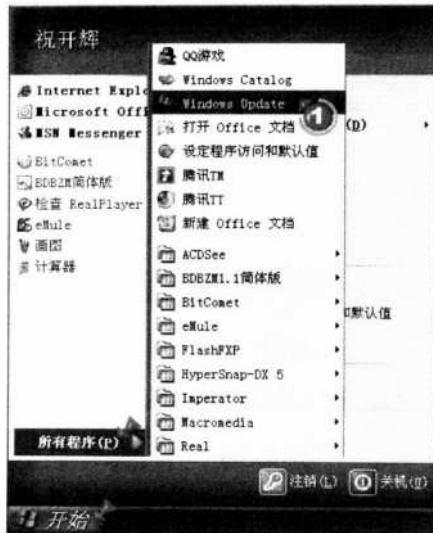
目前，有很多病毒及蠕虫都是利用操作系统及应用程序的漏洞来入侵的，例如 Nimda 病毒可以通过 IIS 的漏洞入侵，而 Blaster 病毒则可通过 RPC 漏洞入侵，因此在清除病毒后，应为应用程序及操作系统安装补丁以修补漏洞。

大部分应用程序都提供了在线更新的功能，通过这项功能就可以自动下载并安装更新补丁。下面将以微软的在线更新功能为例，说明如何安装更新文件修补漏洞，预防病毒及蠕虫再次入侵。



STEP1 执行【Windows Update】功能

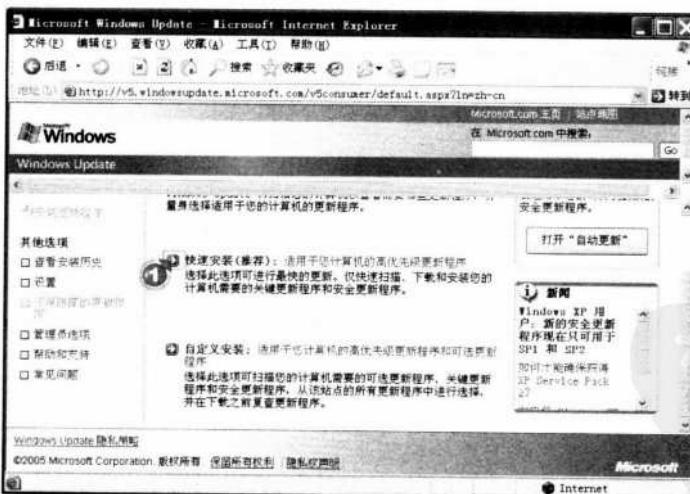
通过【开始】菜单执行【Windows Update】命令，可下载并安装操作系统更新文件。



①依次选择【开始】→【所有程序】
→【Windows Update】命令

STEP2 扫描更新项目

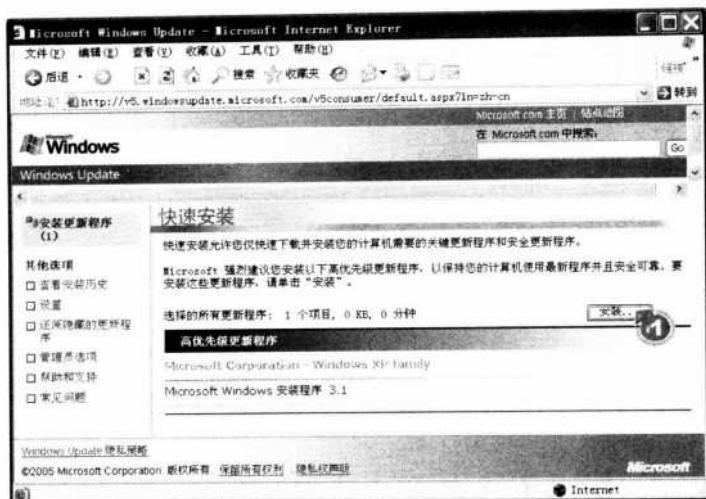
执行【Windows Update】命令后，系统自动打开 Internet Explorer 并连接到微软官方网站，用户可单击【快速安装】链接文字进行更新。



①单击【快速安装】
链接文字

STEP3 检阅更新文件

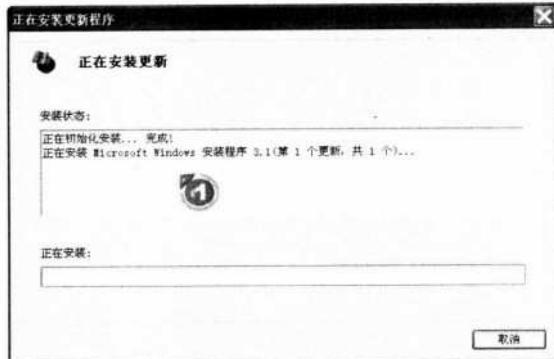
扫描需要更新的程序后，会给出扫描到的结果，单击【安装】按钮即可安装更新。



① 单击【安装】按钮

STEP 4 安装更新文件

弹出【正在安装更新】对话框后，开始自动下载更新，下载完成后会自动安装更新，此时页面显示可用的更新文件，通过【立即安装】按钮即可执行安装更新文件的工作。

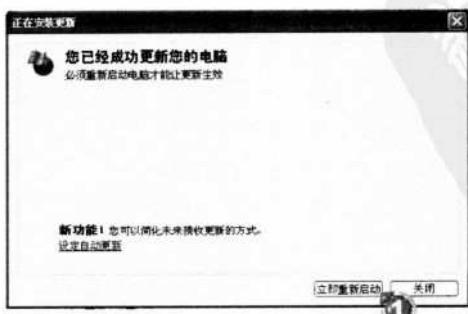


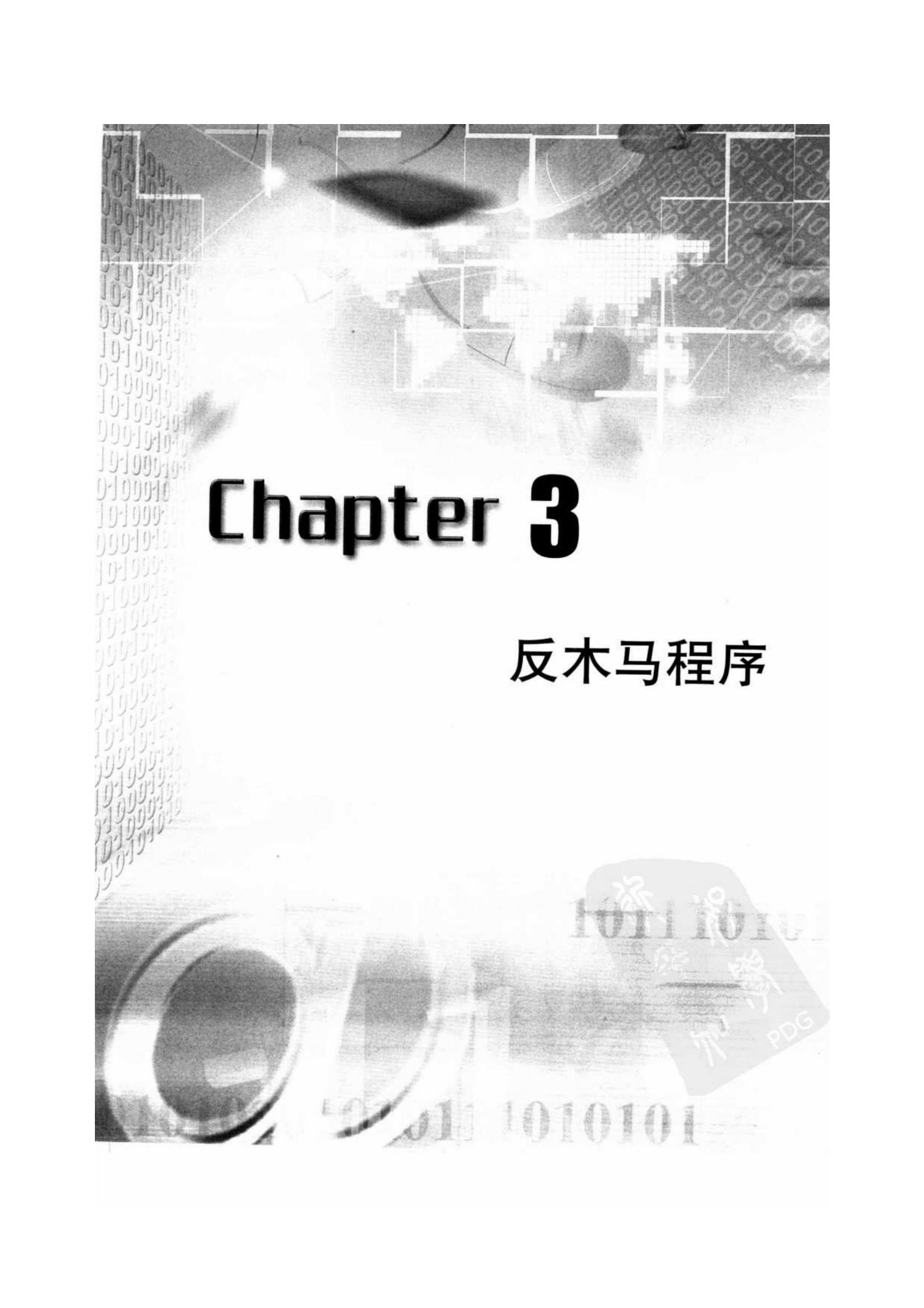
① 正在安装更新内容

STEP 5 完成更新

当更新安装完成后，单击【立即重新启动】按钮即可。

① 单击【立即重新启动】
按钮





Chapter 3

反木马程序



木马程序又称为特洛依木马（Trojan Horse），源于希腊的典故。约在公元前1000年，当时希腊人正在攻打特洛依城，他们制作了一个巨大的木马雕像，并在里面藏了一队精锐的战士，然后假装战败将木马雕像遗留在战场上，使特洛依人误将木马当成战利品抬回城内，就在当晚，躲藏在木马中的战士悄悄打开城门，里应外合地攻破了特洛依城。特洛依木马程序的工作过程和这个典故里的木马非常相似，当用户无意中运行了木马程序后，程序就会在受害者的计算机中悄悄打开一个【后门】，与黑客一起里应外合控制受害者的计算机。

被木马程序入侵后，用户的计算机等于打开了一道任人进出的后门，再无安全性可言。但木马程序亦非无迹可循，只要掌握正确的技巧，即可清除此病毒。

3.1 木马程序

为了更有效地对付木马，首先必须了解一些有关木马的基本知识，例如木马入侵的常用手法、攻击特点及木马的种类等。只有了解这些特性后，才能有效地防止木马程序侵入或清楚木马病毒。

3.1.1 木马如何入侵

从表面上看，黑客要欺骗受害人运行木马程序后才能控制其计算机，但只要不随便运行来历不明的程序即可免受木马之害，其实不然，因为木马的入侵手法千变万化，有不少的用户在被木马入侵后，往往还不知道问题何在。下面就详细介绍一下木马入侵计算机的惯用手法。

● 隐藏在软件中

网络上有着丰富的资源，因此有一些用户往往喜欢在网络上下载各种软件，其实这是一种相当危险的行为。一些非法的网站提供的软件大多未经过严格的病毒检查，极有可能隐藏着木马程序或其他计算机病毒。下图中是从网络上下载的软件，很有可能隐藏木马程序。



补充说明**木马是怎样藏身在文件中的？**

为了达到藏身的目的，木马会将自身与一般的应用程序文件融合在一起，当用户运行程序时，木马即会被同时运行。合并文件后，应用程序的功能不受影响，但程序体积会变大。在黑客之间流传着许多捆绑工具，专门用于将木马程序与一般的应用程序捆绑起来，甚至有一些木马本身就带有捆绑功能，可以将自身与其他应用程序捆绑在一起。下图中 Server.exe 即为具有捆绑命令的木马程序。

**隐藏在共享文件夹中**

在局域网中，人们经常会通过共享文件夹来互相传送资料，用户可以在服务器或自己的计算机上打开一个或多个文件夹，供局域网内的其他用户存取资料。虽然网络共享文件夹为人们带来了很大的方便，但也为木马带来了可乘之机，使其可以通过局域网入侵其他计算机。

木马入侵局域网计算机最简单的方法就是将自己伪装成共享文件。由于有些木马的图标与共享文件夹的图标极为相似，因此如果用户误以为其是共享文件夹而将其打开，就会被木马侵入。



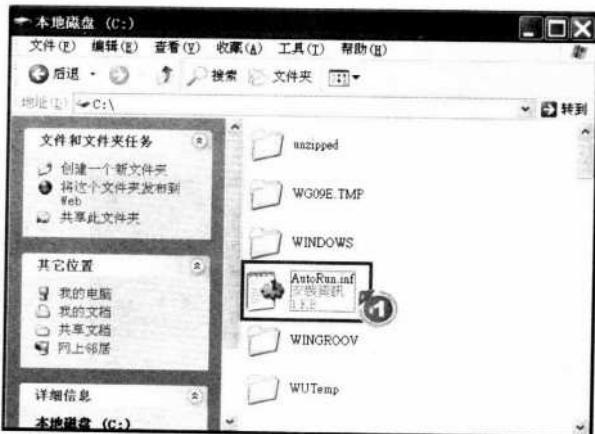
① 伪装成共享文件夹的木马



除了伪装成共享文件夹外，一些木马还会通过修改【AutoRun.inf】文件入侵局域网计算机。这种木马的入侵原理如下：如果磁盘中存在【AutoRun.inf】文件，则用户从磁盘中存取文件时系统就会自动运行此文件的内容。

黑客首先将木马放到共享文件夹，然后编辑【AutoRun.inf】文件加入运行木马程序的命令，一旦用户将共享文件夹设置成网络磁盘驱动器并存取资料时，Windows 就会根据【AutoRun.inf】中的设置自动运行木马程序。

① 自动运行文件

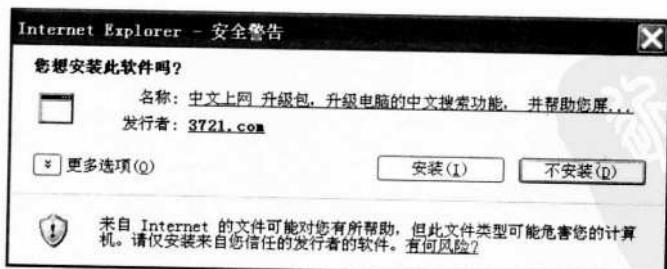


● 隐藏在网页中

随着 Internet 的发展，网页已经成为传播信息的重要途径之一，同时也增加了木马程序入侵的机会。网页中木马的入侵手法主要有以下几种：

● 通过 ActiveX 控件入侵

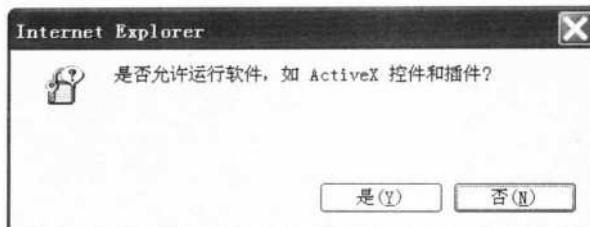
为了增加网页与用户的互动性，一些网页上通常会插入一些 ActiveX 控件，并配合 JavaScript、VBS script 等脚本语言，完成一些特殊任务。这样，虽然方便了用户，但也为木马入侵提供了方便。通常，黑客会以脚本语言配合 ActiveX 控件编写一些特殊的命令嵌在网页上，当用户浏览这些网页时就会被木马入侵。下图为安装基于 ActiveX 的 IE 插件时的警告界面。



是否允许安装基于 ActiveX 的 IE 插件提示

除此之外，ActiveX 控件还可与外挂程序配合运行，这项功能可供用户通过网页播放声音及视频，但也可能被黑客利用运行木马程序欺骗用户，因此当浏览器显示是否运

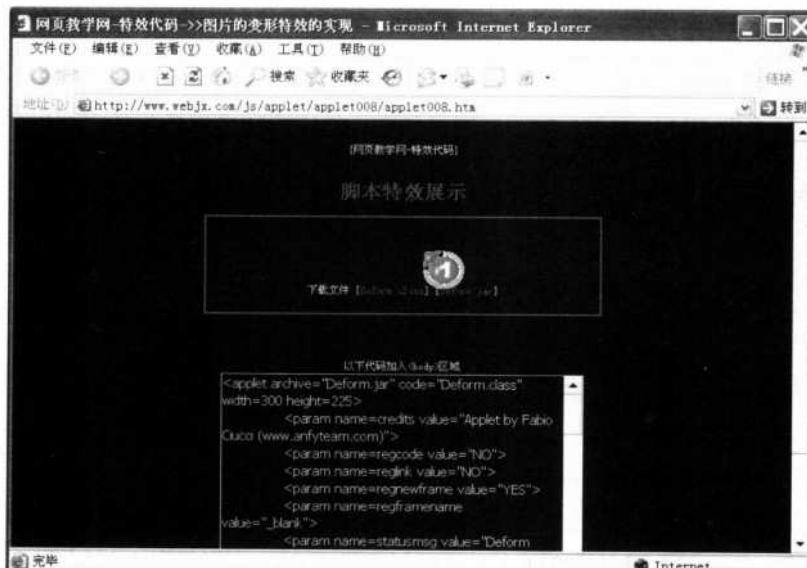
行 ActiveX 控件及插件时，除非可以确定控件将执行什么操作，否则不要随便允许其执行。



● 通过 Java Applet 入侵

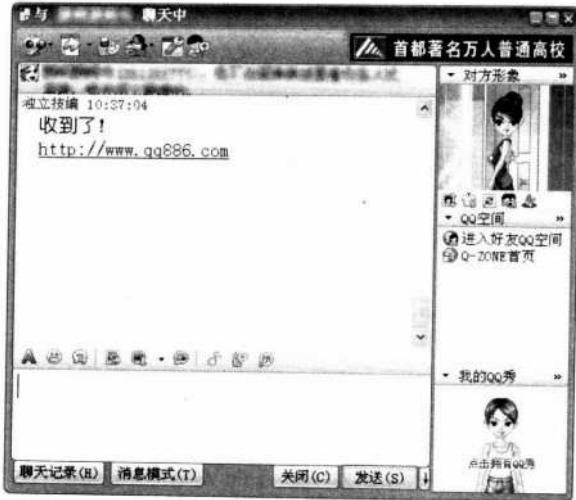
Java Applet 是一种网页特效技术，可以在网页上做出各种特殊的效果，但是在这些网页中同样也隐藏着危机。由于 Java Applet 命令的功能相当强大，甚至可以修改系统配置及登录文件，因此它也成为木马入侵计算机的重要途径。

① Java Applet 特效可能隐藏着木马



● 结合网页与网络聊天软件入侵

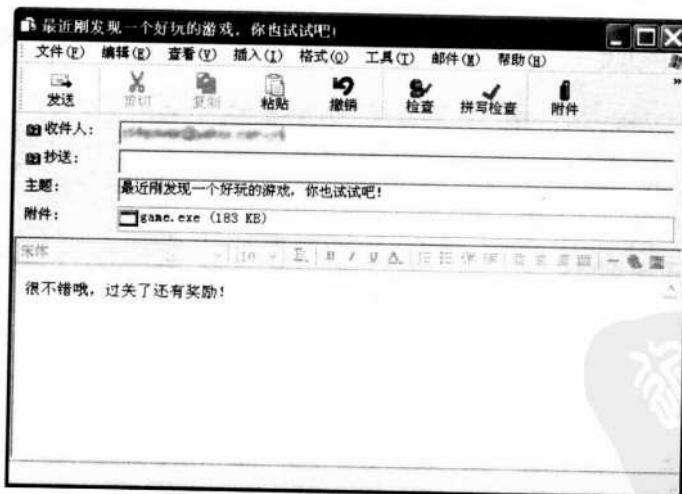
一般来说，大型网站的预防工作相当严密，即使是经验丰富的黑客也不容易将木马放到网页上，因此黑客往往会选择锁定在预防较松懈的小型网站、个人网站上。但由于浏览这些网站的人比较少，因此一些木马就将网页与实时聊天软件结合起来，当木马入侵计算机后，一旦用户使用聊天软件与朋友聊天，木马程序就会自动在信息后面加上一个网页的链接。此时，如果误以为是朋友的推荐而浏览这个网页，网页上的木马就会伺机入侵计算机，使其成为下一个受害者，并通过该计算机继续入侵其他的计算机。



● 通过电子邮件入侵

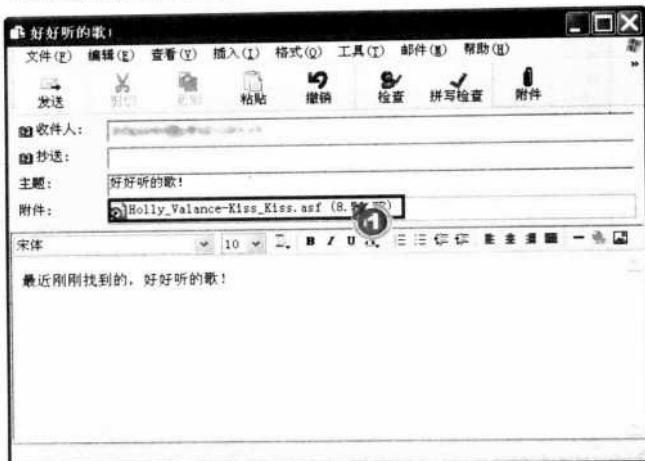
电子邮件是 Internet 上应用最广泛的服务之一，它具有快捷、方便等优势，因此已经成为许多人必备的工具，甚至一些企业用户也通过电子邮件来传送文件及洽谈业务。正是因为电子邮件有着如此广泛的应用，因此它也成为木马入侵的重要通道。

木马通过电子邮件试图入侵的典型过程如下：用户收到一封内容诱人的电子邮件，其中包含一个附件，当用户按照提示运行附件时，木马就会入侵计算机。

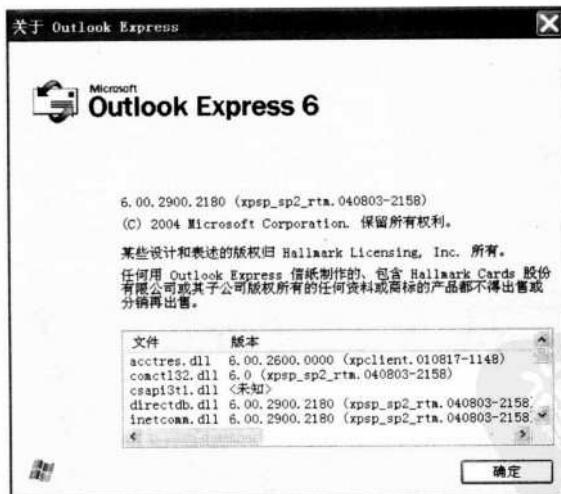


当用户多次被病毒攻击后，安全意识会有很大提高，因此通常不会随意运行邮件的附件。但如果附件是音乐或者图像文件，仍然会有不少用户疏于防范。实际上，附件中的音乐及图像文件同样具有危险性，因为很多木马程序可将自身伪装成图片、音乐、Flash 等看似无害的文件，但当用户运行这些文件时，同样会被木马侵入。

① 伪装成音乐文件的木马



也许有些用户会认为，无论附件是什么，只要一概都不运行就没有问题。但事实并非如此，因为现在黑客的欺骗手段越来越高明，例如一些邮件会伪装成系统管理员或微软来发送系统补丁文件，稍不注意，就会立即被病毒侵入。此外，旧版本的 Internet Explorer（低于 5.5）中存在着一个漏洞，只要用户使用 Outlook Express 预览邮件，附件就会自动运行。而新版本的 Internet Explorer 修正了自动运行附件的漏洞，用 Outlook Express 预览邮件时，附件不会自动运行。



一些病毒入侵计算机后，会从 Outlook 通信簿中搜索用户亲友的电子邮件地址，并以用户的名义向这些地址发送含有木马的邮件，因此在收到亲友寄来的邮件时，同样要提高警觉，因为这些邮件也可能包含着病毒或木马程序。



3.1.2 木马程序的种类

随着网络安全技术的不断提高，木马程序也在不断地更新换代。从技术角度而言，目前的木马主要可分为4代：

● 第一代木马

第一代木马通常只用于窃取网络上的密码，这类木马结构比较简单，甚至不具备隐藏自身程序的功能，稍有经验的用户就可以轻易识破。第一代木马只出现在互联网早期，目前很少见。

● 第二代木马

第二代木马多采用标准的C/S架构，由服务器端与客户端两部分组成。与第一代木马相比，第二代木马的功能有了明显改善，不仅可以窃取网络上的密码，甚至还提供了远程管理、屏幕监视等高级功能。通过第二代木马，用户基本上可以在受控制的计算机上进行任何操作。

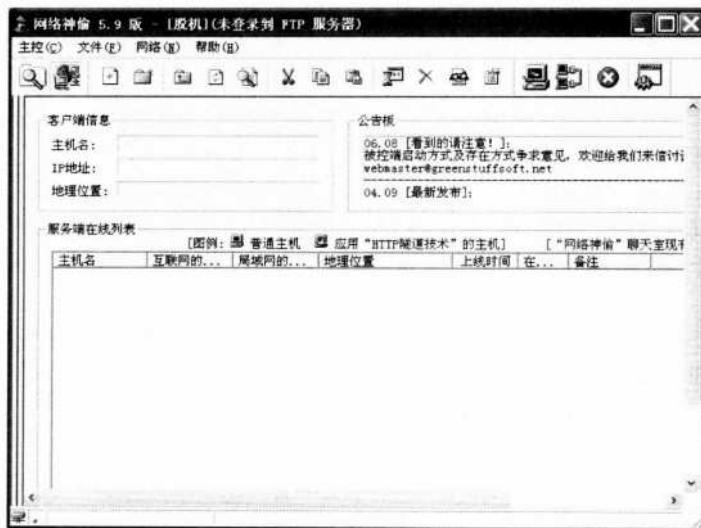
第二代木马是目前流传最广泛的木马，著名的【冰河】、【Amitis】等都属于此类。下图为Amitis木马。



● 第三代木马

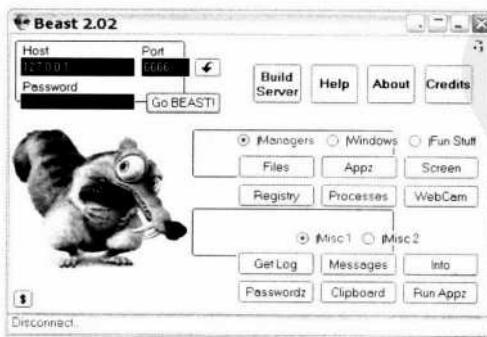
第三代木马又被称为反弹式木马，与第二代木马相比，其功能上并无显著的差异，但其连接方式则完全不同。第二代木马需要由客户端扫描并连接服务器端，而第三代木马的服务器端可以主动连接客户端，即便是防火墙也难以有效阻止。

目前，第三代木马正处于兴起阶段，各种新式木马纷纷出现，如大陆的【网络神偷】、【广外女生】、我国台湾地区的【Peep201】等。下图为网络神偷木马。



● 第四代木马

随着网络安全软件的不断发展，对木马程序的识别能力也在不断提高。为了对抗安全防护软件，第四代木马在隐藏自身的功能上有了明显的突破。前三代木马通常都是独立运行的应用程序，而第四代木马则采用程序注入的方式，将自身伪装成 DLL 文件加载到正常的程序之中，试图避开安全防护软件的扫描。典型的第四代木马有国外的 Beast 等。





3.2 反追踪木马程序

通过前面的介绍，读者对木马已经有了大概的了解，本节将介绍几种对付木马程序的利器，通过这些工具，用户不仅可以找出隐藏在计算机中伺机而动的木马，而且还可以建立一道保护网，将木马程序拒于门外。

3.2.1 以防火墙监控木马

木马一般包括客户端与服务器端两部分，黑客通过木马来入侵计算机时，首先必须用木马程序客户端与受害者计算机中的木马程序服务器端建立连接，才能控制受害者计算机。木马的这种工作原理为人们对付木马提供了一条快捷方式：只要将木马程序的连接阻断，即使受害者计算机已经被木马入侵，黑客也无法通过木马控制计算机，这就是防火墙监控木马的基本原理。

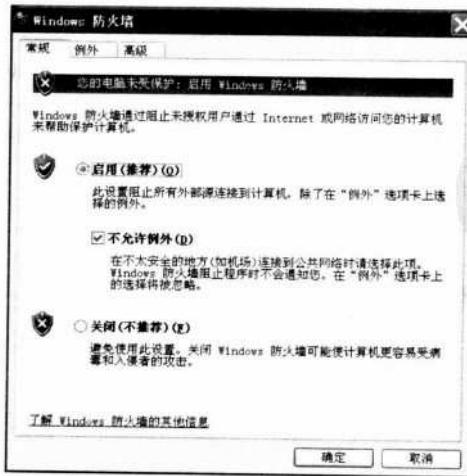
随着技术的发展，目前的防火墙除了具备前面提到的禁止木马连接的功能外，部分防火墙还具有识别木马程序的能力，例如 Norton Internet Security 同时集成了杀毒软件 Norton AntiVirus，用于清除计算机病毒及木马程序。下面将介绍几种常用的防火墙，用户可根据实际需求选用。

注意：不要在计算机中同时安装多个防火墙，因为防火墙软件之间的功能很类似，极有可能导致互相冲突，这样不但不能提高预防效果，而且还有可能导致防火墙无法正常工作。一般来说，用户只要安装一套防火墙软件即可。

● Windows XP 自带防火墙

专业的防火墙软件虽然功能强大，但其设置往往也相当复杂，一般的个人计算机用户较难掌握，如果设置不当，不但起不了预防的作用，反而会为木马大开方便之门。此外，专业的防火墙软件价格也很昂贵，一般用户难以接受。

对于个人计算机用户而言，一般只需用到防火墙的最基本功能，而 Windows XP 自带的防火墙功能已经能够满足使用需求（基于 Windows XP SP2 的防火墙）。



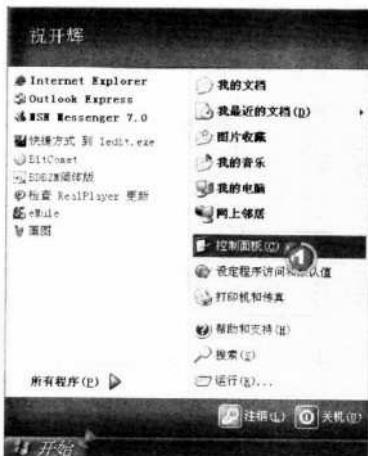
● 打开 Windows XP 自带防火墙

Windows XP 允许用户建立多个网络连接，而且每个连接之间是独立的。为了确保计算机的安全，用户需要单独为每个连接打开防火墙。

Windows XP 自带的防火墙并不具备识别木马程序的能力，但它会禁止来自 Internet 对这台计算机的存取功能，进而阻断木马服务器端与客户端之间的通信。打开防火墙后，用户连接 Internet 的行为不会受影响，而网络上的黑客则无法连接至这台计算机。打开 Windows 自带防火墙的步骤如下：

STEP1 打开【控制面板】窗口

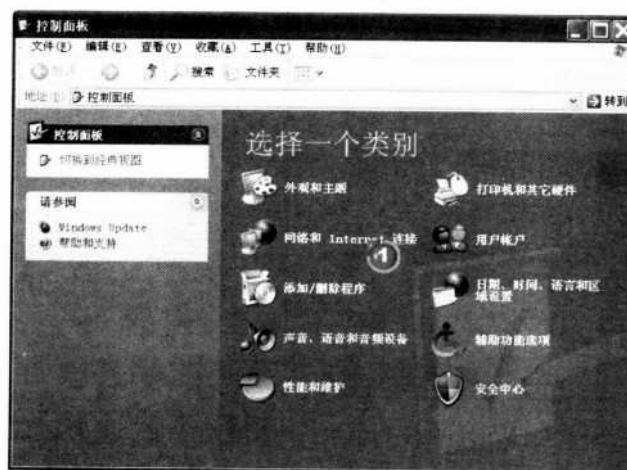
选择【开始】→【控制面板】选项，打开【控制面板】窗口，以便运行 Windows XP 自带防火墙。



①依次选择【开始】→【控制面板】菜单

STEP2 选择【网络和 Internet 连接】类别

控制面板中有不同的类别供用户设置，而 Windows XP 自带防火墙则位于【网络和 Internet 连接】类别中。



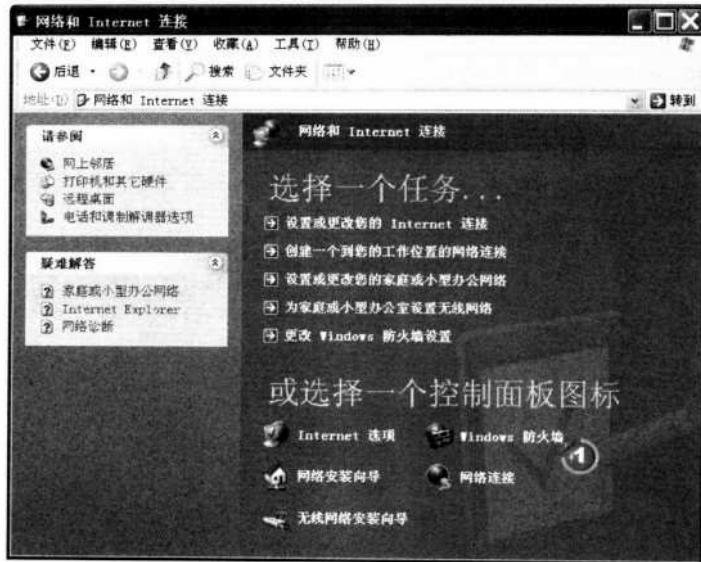
②选择【网络和 Internet 连接】类别



STEP3 打开【Windows 防火墙】窗口

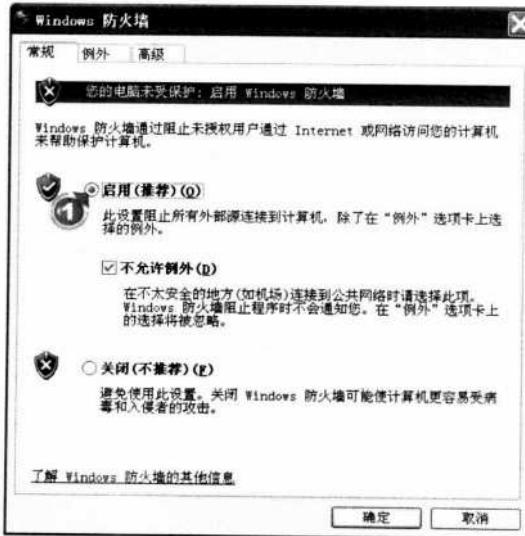
在【网络和 Internet 连接】窗口中，单击【Windows 防火墙】选项即可打开【Windows 防火墙】窗口。

- ① 单击【Windows 防火墙】选项



STEP4 启用【Windows 防火墙】功能

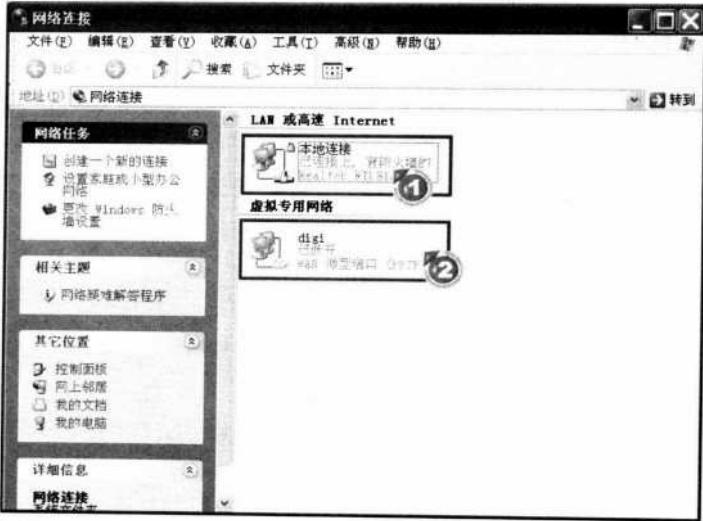
在【Windows 防火墙】窗口的【常规】选项卡中选择【启用】单选框，启动 Windows 防火墙。



- ① 选择【启用】单选框

经过上述设置后，此连接就处于 Windows XP 自带防火墙的保护之下，打开自带防火墙后，连接图标的右上角会出现一把小锁的标志。以此方法可以为多个网络连接打开防火墙。

- ① 已打开防火墙的连接
② 未打开防火墙的连接



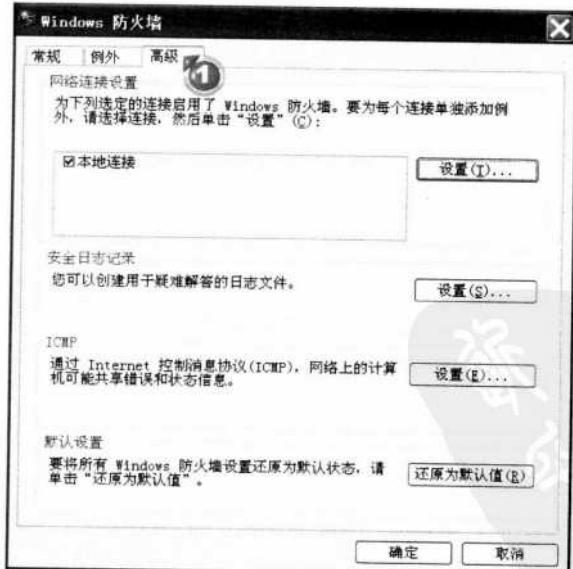
● 设置 Windows XP 自带防火墙

打开 Windows XP 自带防火墙后，用户连接 Internet 的操作不会受到任何影响，但如果用户用这台计算机架设服务器，则需要对防火墙进行设置，否则服务器将无法正常工作。因为 Internet 上其他计算机对这台计算机的访问将全部被防火墙禁止，因此下面将以实例的方式介绍 Windows XP 自带防火墙的设置。

STEP1 打开防火墙的【高级】选项卡

打开防火墙后，选择【高级】选项卡，切换到高级设置窗口。

- ① 单击【高级】选项卡



STEP2 进入【服务】设置

此窗口中共有三项设置，依次为网络连接设置、安全日志记录、ICMP 设置。如果



修改了这些设置，只需单击【还原为默认值】按钮即可恢复为默认设置。首先看一下【网络连接设置】。

- ① 单击【网络连接设置】栏中的【设置】按钮



STEP3 设置允许的服务

【高级设置】对话框中有两个选项卡，其中【服务】选项卡用于设置这台计算机允许打开的服务，例如用户在这台计算机上建立了一个FTP服务器，则需要勾选【FTP服务器】复选框，否则其他计算机用户将无法连接到此服务器。如果用户要添加一个对话框中没有预设的服务，例如某个游戏服务器需要使用TCP 4000端口，则可以单击【添加】按钮将其加入到列表中。



- ① 单击【添加】按钮

STEP4 设置添加服务

单击【添加】按钮后，在弹出的【服务设置】对话框中按序输入服务的描述、IP地址及连接端口，然后单击【确定】按钮即可完成设置。



- ① 输入服务描述
- ② 输入 IP 地址
- ③ 选择协议类型，此处选择【TCP】单选框
- ④ 输入服务的内外部端口号
- ⑤ 单击【确定】按钮

STEP5 检查设置结果

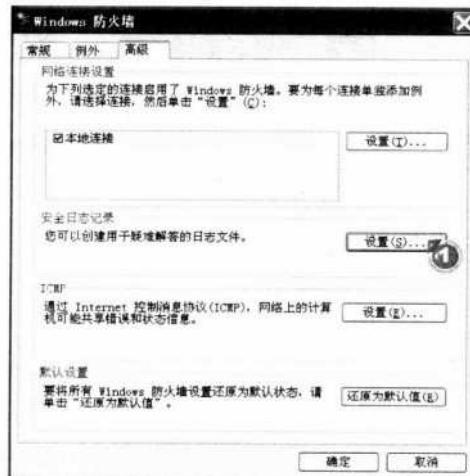
设置完成后，即可在【高级设置】对话框中看到添加的服务，防火墙默认让新添加的服务处于打开状态。

① 添加的服务



STEP6 设置安全日志记录

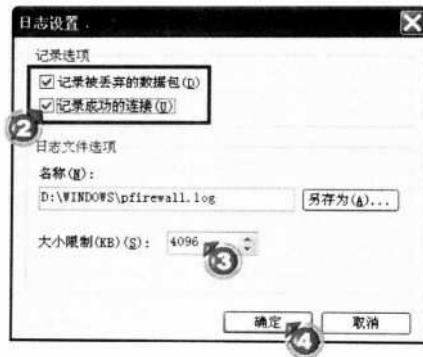
默认状态下，Windows XP 自带的防火墙没有打开安全日志记录，用户需要在防火墙的【高级】选项卡的【安全日志记录】栏中单击【设置】按钮，打开【日志设置】对话框并设置其中的选项。



- ① 单击【安全日志记录】栏中的【设置】按钮



- ② 选中【记录被丢弃的数据包】与【记录成功的连接】复选框
③ 设置记录文件的大小
④ 单击【确定】按钮



STEP 7 设置 ICMP

在【ICMP 设置】对话框中可以对各项关于 ICMP(Internet Control Message Protocol, 因特网控制消息协议)的信息进行控制。ICMP 是用于检测网络的软件, 有可能被黑客利用, 在默认状态下, 防火墙不允许 ICMP 数据包进入系统。进入【ICMP 设置】对话框的方法是, 在防火墙的【高级】选项卡的【ICMP】栏中, 单击【设置】按钮。打开【ICMP 设置】对话框后, 即可对其进行设置。



● Norton Internet Security

Windows XP 自带的防火墙虽然简单易用，但其功能过于简单，例如无法识别木马程序，无法满足高级用户的需求等，因此高级用户一般都倾向于使用专业的防火墙软件。目前，较流行的专业防火墙软件是 Norton Internet Security，这是赛门铁克公司开发的安全防护软件，不仅能够预防木马程序，而且还可以预防黑客入侵。此外，Norton Internet Security 还集成了赛门铁克公司的防毒软件 Norton AntiVirus，可为用户提供全方位的防护。

软件小档案

软件名称：Norton Internet Security 2004（诺顿网络安全特警 2004）

版本：2004 版本

官方网站：<http://www.norton.com> 或 <http://www.symantec.com>

其他下载地址 1：<http://www.onlinedown.net/soft/24268.htm>

其他下载地址 2：<http://download.zol.com.cn/detail/3/27979.shtml>

软件类型：试用软件

下图为 Norton Internet Security 的主窗口



Norton Internet Security 的设置比 Windows XP 自带防火墙要复杂一些，但用户只要按照以下介绍的方法操作，就可以轻松地掌握 Norton Internet Security 的设置方法。

● 安装 Norton Internet Security

STEP1 执行安装程序

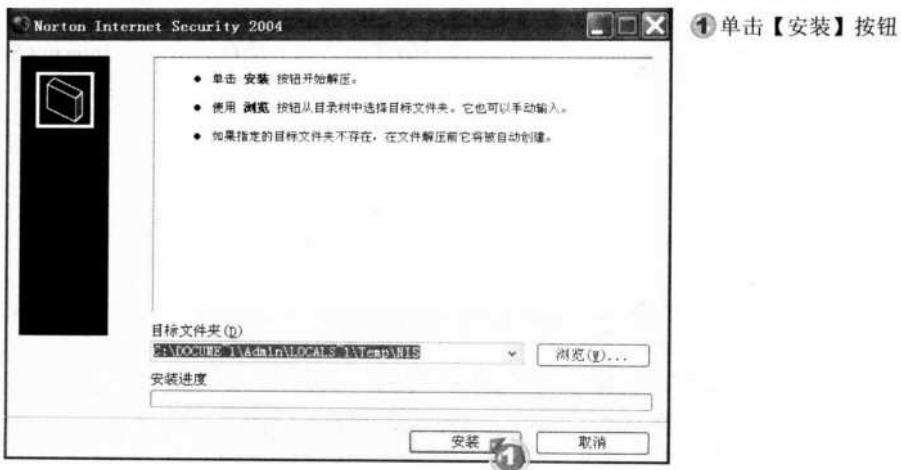
打开安装文件所在的文件夹后，双击安装文件，执行安装程序。





STEP2 设置解压缩临时的文件夹

安装前程序会自动解压缩一些临时安装文件，所以需要设置一个存放区域，通常使用默认值即可。如果需要，也可以单击【浏览】按钮手动更改存放区域。



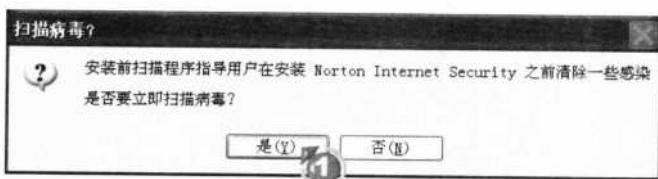
STEP3 进入安装界面

解压缩完毕后自动进入安装接口，准备安装。



STEP4 扫描病毒

为了防止在有毒的系统上安装，造成程序失常，在安装前最好先扫描病毒。



STEP5 跳过安装欢迎

跳过安装欢迎界面，准备开始安装。

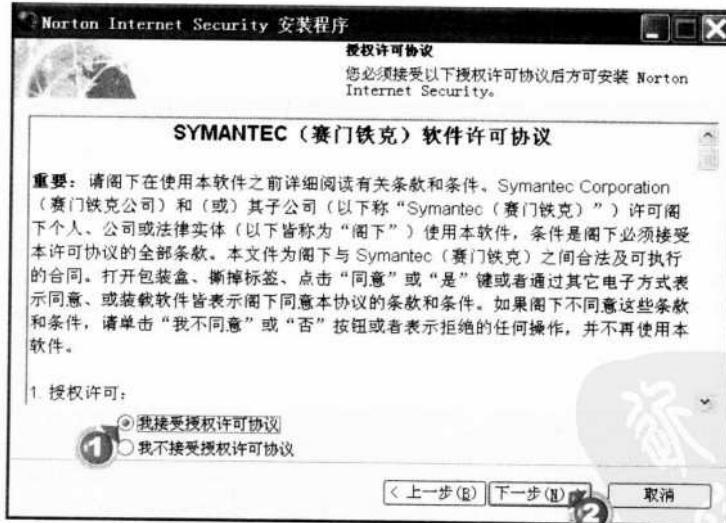
①单击【下一步】按钮



STEP 6 授权界面

同意软件授权协议，才能继续安装软件。

- ①选择【我接收授权许可协议】按钮
- ②单击【下一步】按钮

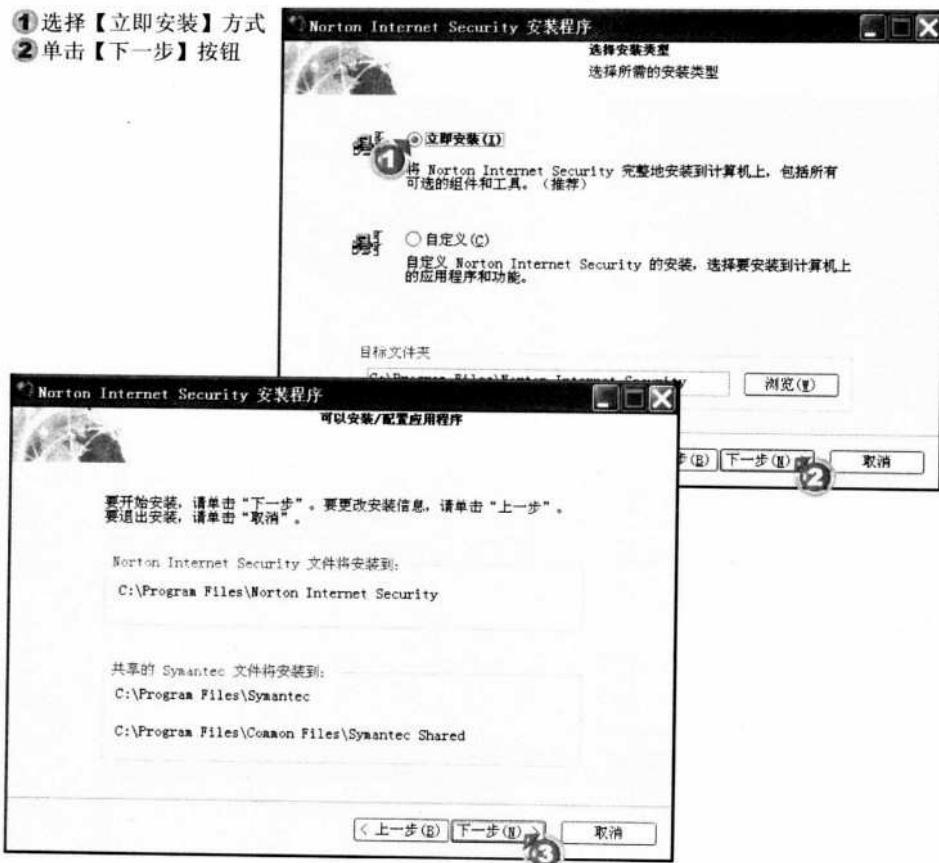


STEP 7 设置安装目录及安装类型

使用默认的【立即安装】方式即可，如果想改变安装路径，可以单击【浏览】按钮手动更改。



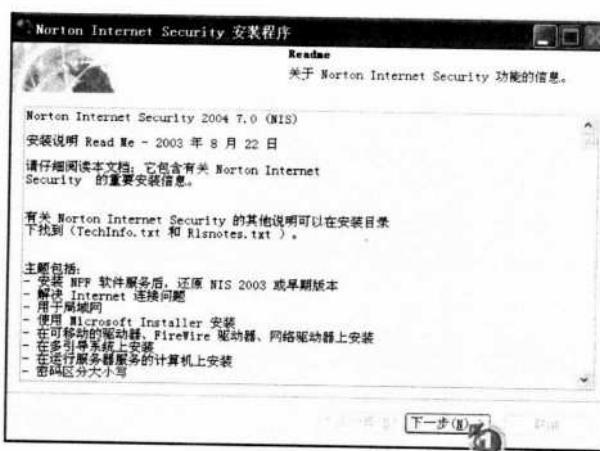
- ①选择【立即安装】方式
②单击【下一步】按钮



STEP 8 完成安装

安装完毕后，系统会给出一些安装信息，向用户说明安装的完成情况，然后重启计算机即可。

- ①单击【下一步】按钮
②单击【完成】按钮，重启计算机



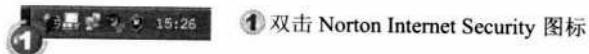


● 运行防火墙

安装 Norton Internet Security 后，每次运行系统时程序都会自动运行，在 Norton Internet Security 程序主窗口中可以看到防火墙的状态，如果防火墙处于关闭状态，则需要手动将其打开。

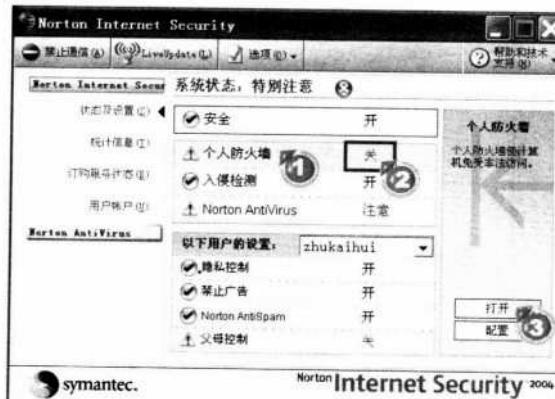
STEP1 打开 Norton Internet Security 程序主窗口

双击系统任务栏上的 Norton Internet Security 程序图标，打开 Norton Internet Security 程序主窗口。



STEP2 运行防火墙

程序主窗口显示防火墙的状态，如果未打开防火墙，可单击【打开】按钮将其打开。



- ① 选择【个人防火墙】选项
- ② 个人防火墙未打开
- ③ 单击【打开】按钮

STEP3 检视结果

设置完毕后，在程序主窗口中可以看到个人防火墙已经显示为打开状态。



① 个人防火墙已打开

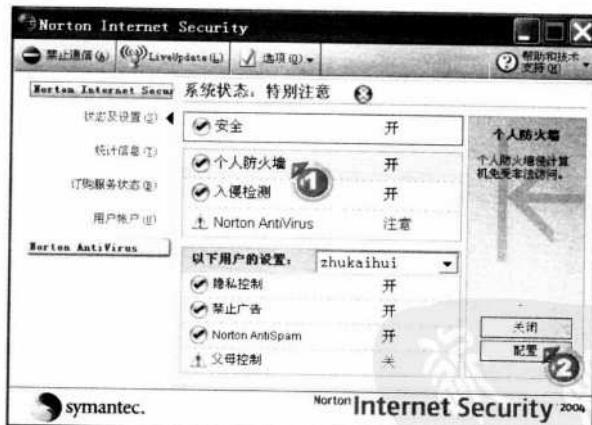
● 设置安全级别

Norton Internet Security 防火墙提供了低、中、高 3 个安全级别，当采用低安全级别时，Norton Internet Security 只提供最基本的防护功能，如隐藏未使用的通信端口等，但此时网络的各种功能如上传、下载等基本上不受影响；而当安全级别设置为高时，防火墙提供了完善的防护功能，但同时亦有部分网络功能会受到影响。综合安全性与功能两方面因素考虑，一般建议用户设置防火墙安全级别为【中】。

STEP1 打开个人防火墙设置

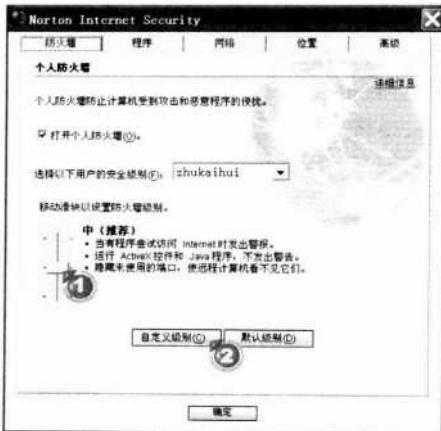
在程序主窗口中选择【个人防火墙】选项，然后单击【配置】按钮，以打开 Norton Internet Security 个人防火墙对话框。

- ① 选择【个人防火墙】选项
- ② 单击【配置】按钮



STEP2 设置防火墙安全级别

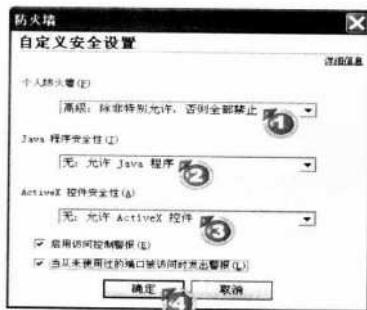
在【Norton Internet Security】对话框中拖动游标设置防火墙安全级别，此时，在游标的右方会显示当前安全级别的详细信息。如果用户需要精确设置防火墙，可单击【自定义级别】按钮打开【自定义安全设置】对话框。



STEP 3 自定义安全设置

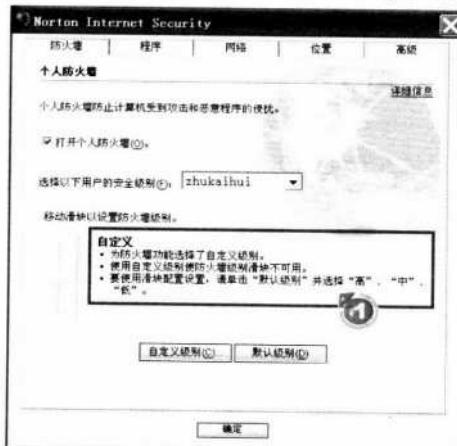
在【自定义安全设置】对话框中，用户可以对防火墙进行更详细的设置。用户可根据实际需求进行设置，建议设置个人防火墙为【高级：除非特别允许，否则全部禁止】，以避免木马程序侵入。

- ① 设置个人防火墙级别
- ② 设置 Java 程序安全性
- ③ 设置 ActiveX 控件安全性
- ④ 单击【确定】按钮



STEP 4 检视结果

设置完成后，在【Norton Internet Security】对话框中会显示自定义的防火墙级别。



- ① 自定义的防火墙级别



● 设置局域网

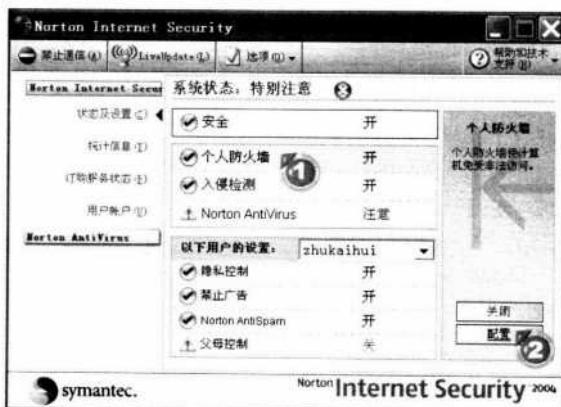
安装 Norton Internet Security 后，默认状态下来自局域网对这台计算机的存取操作会全部被禁止，此时用户将无法与局域网内的计算机共享文件及打印机。为此，Norton Internet Security 提供了一项【信任区域】功能，用户只要将局域网内的计算机加入到【信任区域】，就可以与局域网内的计算机共享文件及打印机。但有一点必须注意，由于 Norton Internet Security 不会监控来自信任区域内计算机的存取行为，因此黑客有可能会通过信任区域内的计算机入侵，所以在将计算机加入到信任区域之前，应先确认它们有足够的安全措施预防黑客攻击。

STEP 1 打开个人防火墙设置

在程序主窗口中选择【个人防火墙】选项，然后单击【配置】按钮，以配置个人防火墙功能。

① 选择【个人防火墙】选项

② 单击【配置】按钮



STEP 2 添加计算机至信任区域

Norton Internet Security 提供了【信任】与【限制】两个区域，通过这两个区域可以轻松地设置来自网络的存取操作。来自信任区域的计算机对这台计算机的存取操作不受任何限制，而来自限制区域的计算机对这台计算机的存取操作则全部被禁止。

① 选择【网络】选项卡

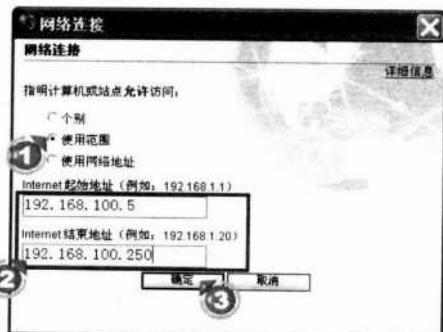
② 单击【信任】按钮

③ 单击【添加】按钮



STEP3 指明计算机或站点

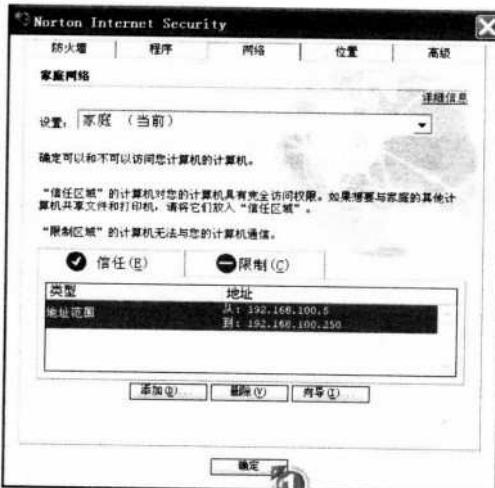
添加计算机至【信任】区域时，用户既可指定添加的计算机，也可指定增加某一段IP地址范围。本例要增加局域网内多台计算机至【信任】区域，因此选择【使用范围】单选框。



- ① 选择【使用范围】单选框
- ② 输入 IP 起始与结束的地址范围
- ③ 单击【确定】按钮

STEP4 检视成果

设置完成后，在【信任】列表中可看到添加的计算机或IP地址范围，确认无误后单击【确定】按钮。



- ① 单击【确定】按钮

● 设置木马规则

黑客通过木马程序入侵计算机时，会在入侵对象的某个连接端口上建立一个连接。一般情况下，木马程序所用的连接端口都是相对固定的，如冰河一般会用7626端口，Beast会用6666端口，因此用户可以通过禁止端口的方法来预防木马入侵。默认状态下Norton Internet Security已经建立了多条木马规则用于禁止各种常见木马程序，而用户亦可手动添加规则以预防默认列表中没有的木马程序。

注意：目前一些较新的木马程序已经能够自定义使用哪一个连接端口，因此木马规则对这类新式木马程序作用不大，但是大部分木马程序还是采用了相对固定的端口，因此这



种方法仍不失为一种较理想的预防手段。

下面将以建立一个预防冰河木马程序的规则为例，说明如何设置木马规则。

STEP 1 打开高级防火墙设置

在程序主窗口中选择【个人防火墙】选项，然后单击【配置】按钮，以设置个人防火墙功能。

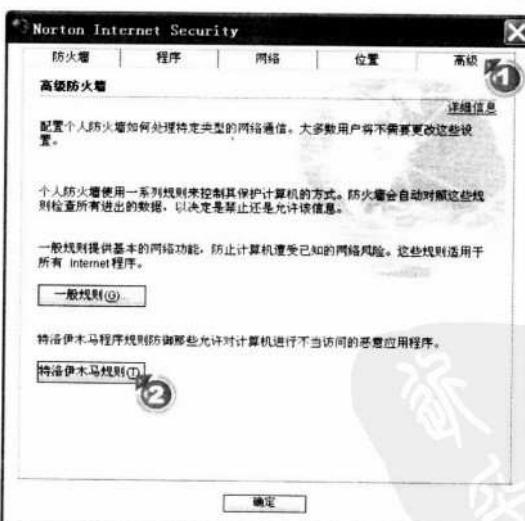
- ① 选择【个人防火墙】选项
- ② 单击【配置】按钮



STEP 2 打开【特洛依木马规则】对话框

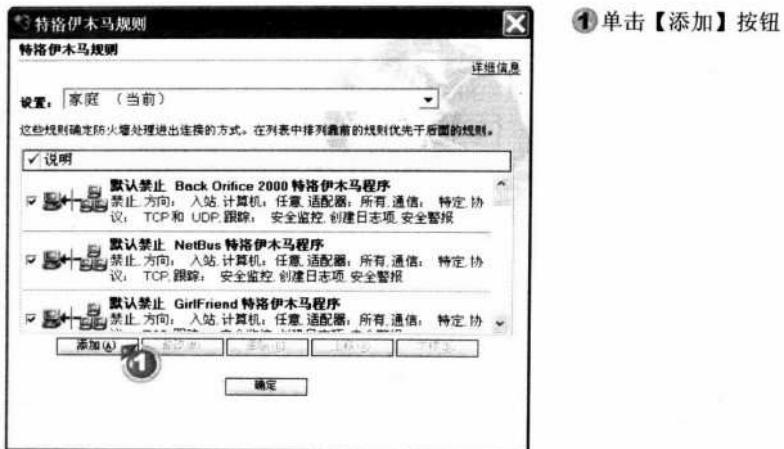
选择【高级】选项卡后，单击【特洛依木马规则】按钮，打开【特洛依木马规则】对话框。

- ① 选择【高级】选项卡
- ② 单击【特洛依木马规则】按钮



STEP 3 添加规则

【特洛依木马规则】对话框中显示了已建立的预防木马程序的规则，用户可通过【添加】按钮添加规则。



STEP4 设置规则的处理方式

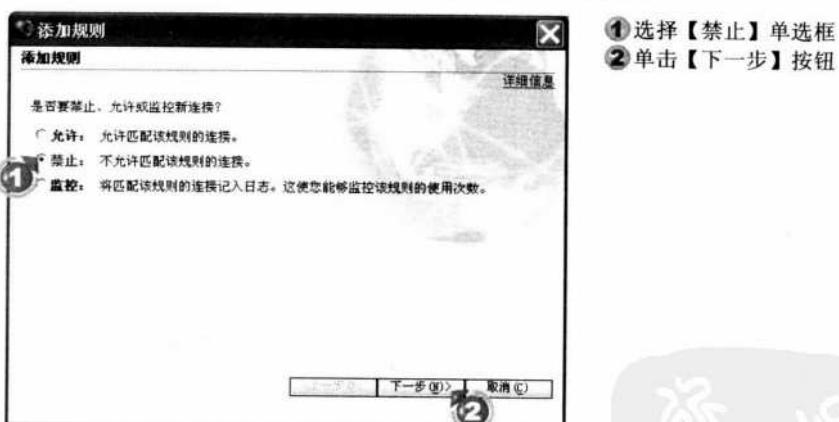
设置规则的处理方式是指当连接符合规则时，防火墙如何处理这个连接，Norton Internet Security 提供了 3 种处理方式：

允许：不禁止符合此规则的连接。

禁止：禁止符合此规则的连接。

监控：不禁止连接，但在日志中记录符合此规则的连接。

本例的目的是禁止冰河木马，因此应选择【禁止】单选框。

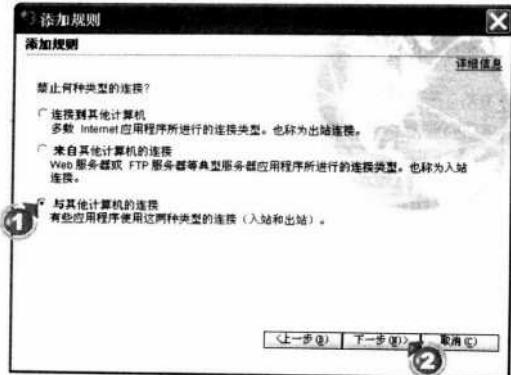


STEP5 设置禁止连接的类型

网络连接可以分成两类：一类是本地计算机连接到其他计算机，称为出站连接；另一类则是其他计算机连接到本地计算机，称为入站连接。由于大部分木马程序都是由客户端连接到服务器端，即入站连接（但也有少数是例外），因此为了确保万无一失，建议选择【与其他计算机的连接】单选框，将上述两种连接全部禁止。



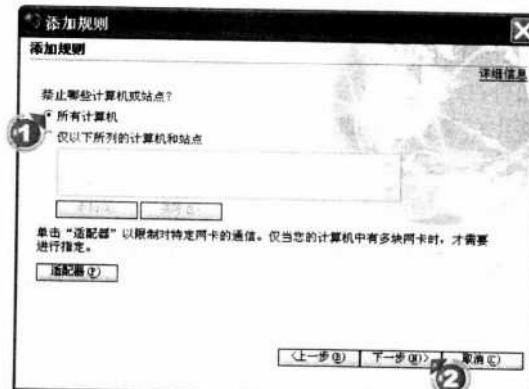
- ①选择【与其他计算机的连接】单选框
②单击【下一步】按钮



STEP 6 选择要禁止的计算机或网站

Norton Internet Security 允许用户设置禁止特定计算机或网站的连接，但就本例而言，由于用户无法确切知道黑客的 IP 地址，因此必须选择禁止所有计算机。

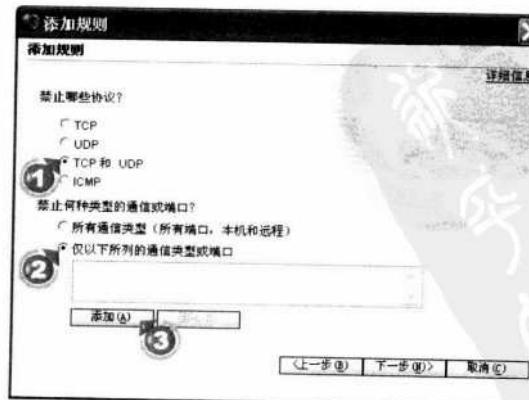
- ①选择【所有计算机】单选框
②单击【下一步】按钮



STEP 7 设置禁止的通信协议及通信端口

根据木马程序采用的通信协议设置禁止哪一种协议，然后选择【仅以下所列的通信类型或端口】单选框，并单击【添加】按钮增加要禁止的通信端口。

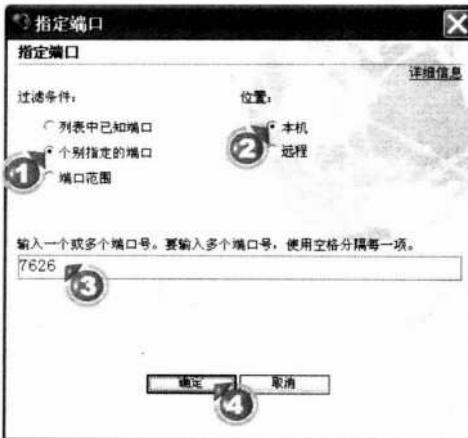
- ①选择要禁止的通信协议
②选择【仅以下所列的通信类型或端口】单选框
③单击【添加】按钮



STEP 8 添加要禁止的通信端口

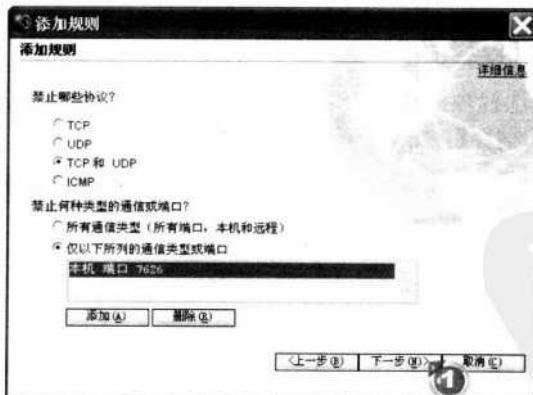
一般情况下，河木马程序采用本机的7626通信端口，因此在指定通信端口时应选择【个别指定的端口】和【本机】单选框。

- ① 选择【个别指定的端口】单选框
- ② 选择【本机】单选框
- ③ 输入通信端口号
- ④ 单击【确定】按钮

**STEP 9** 检视添加的通信端口

设置完成后即可在通信端口列表中看到添加的通信端口或类型，确认无误后单击【下一步】按钮继续操作。

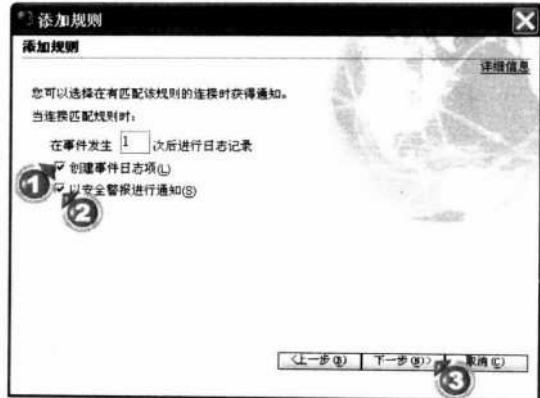
- ① 单击【下一步】按钮

**STEP 10** 设置是否收到通知

为了更清楚了解连接的情况，建议用户选择【创建事件日志项】及【以安全警报进行通知】复选框，当出现符合规则的连接时，Norton Internet Security 会自动将事件记录在日志中，并弹出警示窗口通知用户。

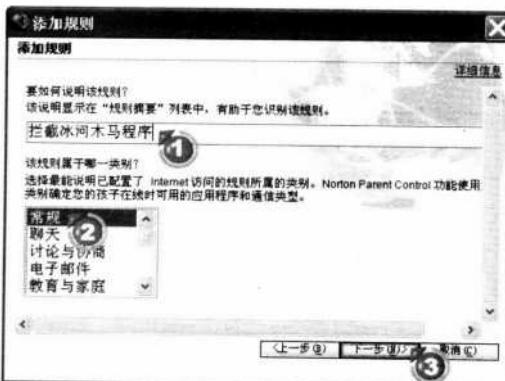


- ① 选择【创建事件日志项】复选框
- ② 选择【以安全警报进行通知】复选框
- ③ 单击【下一步】按钮



STEP 11 设置规则说明及类别

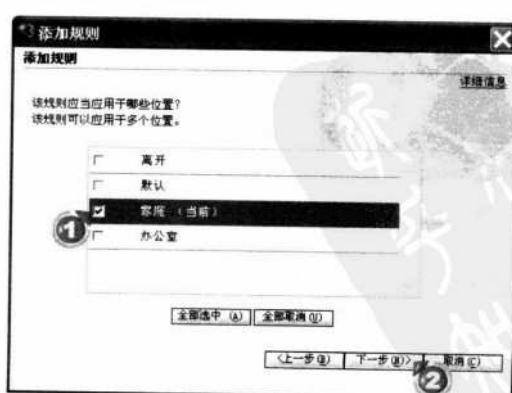
用户需要为规则加一个说明，这个说明将会显示在【规则摘要】列表中。此外，还可为此规则选择一个类别，建议选择类别为【常规】。



STEP 12 选择规则适用地区

在此对话框中选择规则适用的地区，建议选择当前设置的地区，此处针对家庭进行设置，因此选择【家庭（当前）】复选框。

- ① 选择【家庭（当前）】复选框
- ② 单击【下一步】按钮

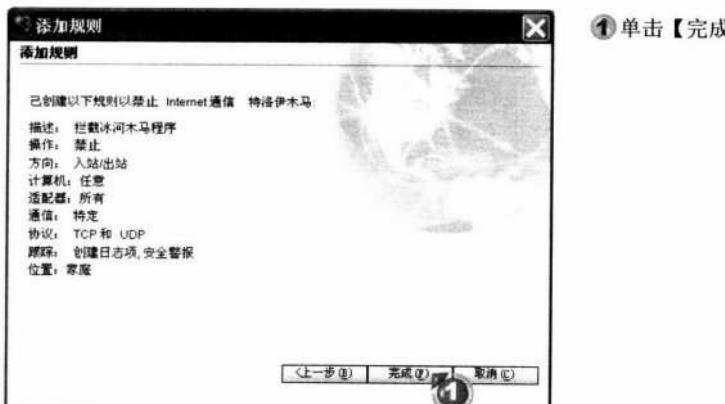


补充说明**为什么要设置【地区】？**

Norton Internet Security 中【地区】的概念与 Windows XP 中的【主题】有点类似。Windows XP 中的每个主题都包括多项显示设置值，用户只要套用主题即可快速变更显示设置；而 Norton Internet Security 亦采用了类似的方法让用户快速改变设置，每个【地区】都包含 Norton Internet Security 的多项设置，供用户在不同的情况下套用。例如当用户在办公室使用计算机时，就可套用【办公室】选项，而当用户在家中使用计算机时，就可套用【家用】选项。

STEP1 完成设置

在设置结束之前，向导会在【添加规则】对话框上显示用户所做的设置，确认无误后单击【完成】按钮结束设置。



3.2.2 清除木马程序

当计算机被木马入侵后，虽然可以通过防火墙软件将木马与黑客之间的通信截断，但留在计算机中的木马程序始终是个不安全的因素，为了避免其伺机而动，应该尽早将其清除。但是，木马程序往往会通过各种手段隐藏起来，甚至伪装成系统进程让用户难以删除，因此需要借助专业的反木马程序。目前，较流行的反木马程序主要有 Trojan Remover、Trojan Hunter、Trojan System Cleaner 等。此外，大部分防毒软件也具备清除木马程序的能力，如 Norton AntiVirus、Pc-cillin 等。由于前面介绍的 Norton Internet Security 中已经集成了 Norton AntiVirus 防毒软件，因此下面就以此为例，介绍如何通过防毒软件清除计算机中的木马。

STEP1 运行【全面系统扫描】命令

Norton AntiVirus 提供了一项全系统扫描的命令，通过这项命令即可对计算机做全面检查，用户每隔一段时间（建议每周）可以运行一次全系统扫描程序，以清除计算机中可能存在的木马程序及病毒。



- ① 单击【Norton AntiVirus】按钮
- ② 选择【全面系统扫描】选项
- ③ 单击【立即扫描】按钮



STEP 2 检视扫描进度

开始扫描后, Norton AntiVirus 将会扫描内存及存储装置, 以搜索病毒及木马程序。在扫描的过程中, 程序会显示已扫描的文件及发现的病毒数量等信息。

- ① 已扫描的文件数量
- ② 发现的病毒数量



STEP 3 检视摘要

扫描完成后, Norton AntiVirus 会显示本次扫描的摘要, 如果用户希望获得更详细的信息, 可以单击【更多详情】按钮。

- ① 单击【更多详情】按钮



STEP 4 检视详细信息

单击【更多详情】按钮后，在打开的窗口中会显示中毒文件的名称及目前的状态，检视完毕后单击【完成】按钮，完成全系统扫描。



3.3 做好还原计算机的准备工作

虽然前面已经介绍了防火墙监控木马和通过防毒软件清除木马的方法，而且结合这些方法也已经可以有效地预防绝大部分木马程序。但是，当今的计算机技术发展日新月异，新的木马及病毒层出不穷，即使最新版的防毒软件也有可能对其束手无策。此外，一些木马还同时具有计算机病毒的特征，会破坏被入侵的计算机。因此，为了对付这些新的木马及病毒程序，用户除了应及时更新防毒软件外，还应定期备份系统，以便需要时可以迅速还原计算机。

虽然 Windows XP 自带了系统还原命令，但由于它采用了备份关键文件的方式，而非备份全部文件，因此这种备份还原方式未必能够有效地清除木马及病毒程序。在此，推荐使用赛门铁克公司的 Norton Ghost 2003，这套软件可以将硬盘内容备份成一个映像文件，当系统因木马及病毒程序而损坏时，可以通过备份的映像文件还原。由于 Norton Ghost 2003 采用了较先进的压缩技术，映像文件的体积一般只有原文件体积的 1/2~2/3，因此可以方便用户存储及转移文件。除此之外，Norton Ghost 2003 还可以【克隆】硬盘资料，网络管理员可通过这项功能为多台计算机快速重装操作系统。

软件小档案

软件名称：Norton Ghost 2003

版本：2003

官方网站：<http://www.norton.com/region/cn/>

其他下载地址：<http://www.pckj.com/Soft/tool/200505/10.html>

软件类型：商业软件

下图为盒装 Norton Ghost 2003 杀毒软件。





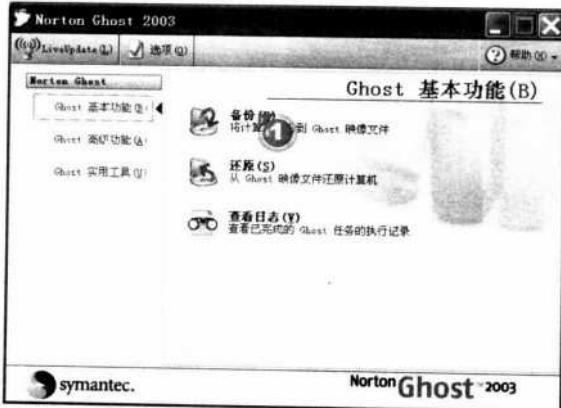
3.3.1 备份系统分区

木马及病毒程序入侵计算机后，往往会隐藏在操作系统中，以便能够在开机时自动运行。因此，除非其他磁盘分区存储着重要的资料，否则以 Ghost 备份时只需备份系统分区即可。下面将以实例的方式介绍如何通过 Norton Ghost 2003 备份系统分区。

STEP 1 运行备份向导

Norton Ghost 2003 的界面非常简洁，用户只需选择窗口中的【备份】选项即可运行备份向导。

① 单击【备份】选项



STEP 2 跳过欢迎界面

选择【备份】选项后，首先出现的是备份向导欢迎界面，单击【下一步】按钮，继续运行备份操作。

① 单击【下一步】按钮



STEP 3 选择要备份的硬盘或分区

Norton Ghost 2003 允许用户选择备份整个硬盘或者单独备份某个分区，此外用户还需选择备份成映像文件或者备份至 CD（或 DVD）光盘中。

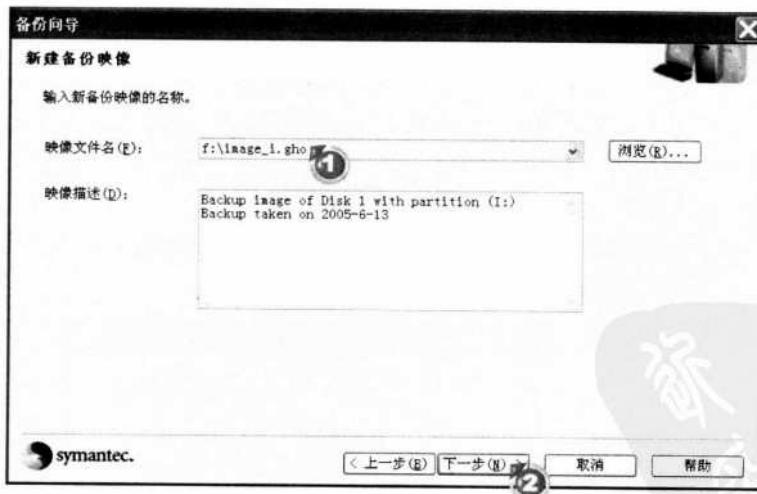
- ① 选择要备份的分区
② 选择【文件】单选框
③ 单击【下一步】按钮



STEP4 设置存储路径

选择映像文件的存储路径，注意存储路径不能位于备份的硬盘或分区中，且要确认有足够的空间可以容纳映像文件。

- ① 设置映像文件的存储路径
② 单击【下一步】按钮

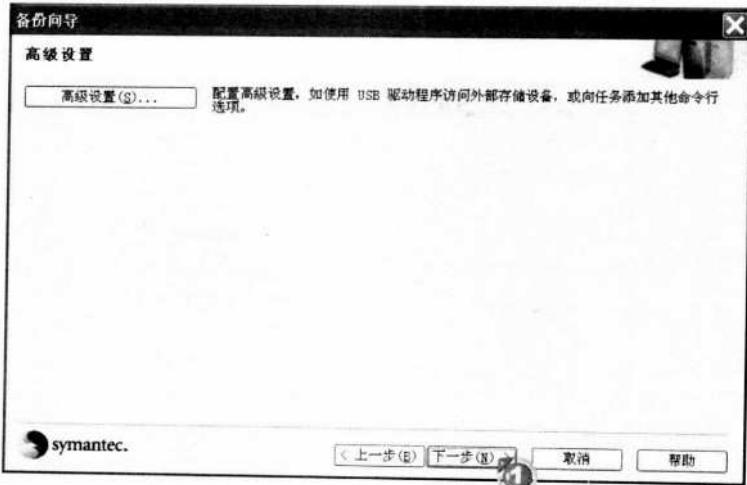


STEP5 设置高级选项

如果用户需要使用 USB 存储装置，可以单击【高级设置】按钮设置高级选项，否则直接单击【下一步】按钮跳过此步骤。



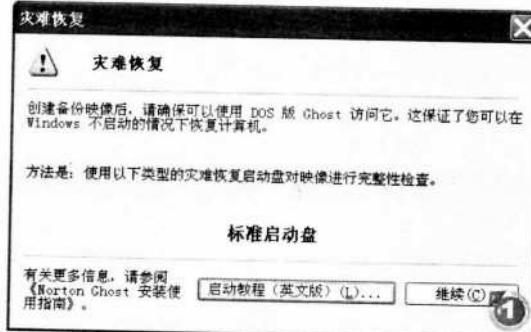
① 单击【下一步】按钮



STEP 6 检视灾难恢复对话框

备份向导会提示用户应在备份完毕后建立一张灾难恢复启动盘，用于在紧急情况下开机执行还原操作，阅读完毕后单击【继续】按钮。

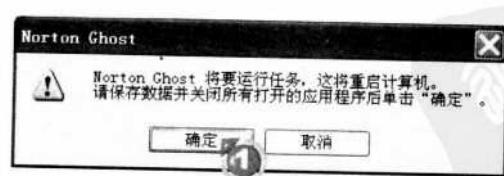
① 单击【继续】按钮



STEP 7 重新启动计算机

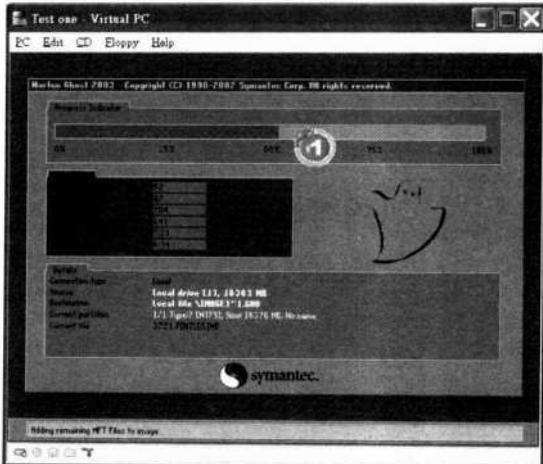
由于 Windows 操作系统正在运行，而 Ghost 需要重新启动计算机才能执行备份操作，因此需要重新启动计算机。

① 单击【确定】按钮



STEP 8 检视备份进度

重新运行计算机后，系统会自动进行备份，在备份过程中 Ghost 会显示备份的进度。

① 备份的进度**STEP 9 检视结果**

备份完成后，重新启动计算机并打开目的文件夹，即可看到备份的映像文件，以后将可使用此映像文件还原系统。

① 备份的映像文件

3.3.2 还原系统分区

当用户遇到无法清除的木马程序或病毒，或者操作系统出现无法修复的错误时，即可通过前面备份的映像文件进行还原。执行还原操作后，硬盘中的资料将被还原至备份时的状态。

还原系统分区同样可通过 Ghost 程序来执行，只有当操作系统已经严重损坏到无法开机时，才需要使用灾难恢复启动盘来执行还原操作。关于制作及使用灾难恢复启动盘的内容将会在 3.3.3、3.3.4 节中进行介绍。

STEP1 运行还原向导

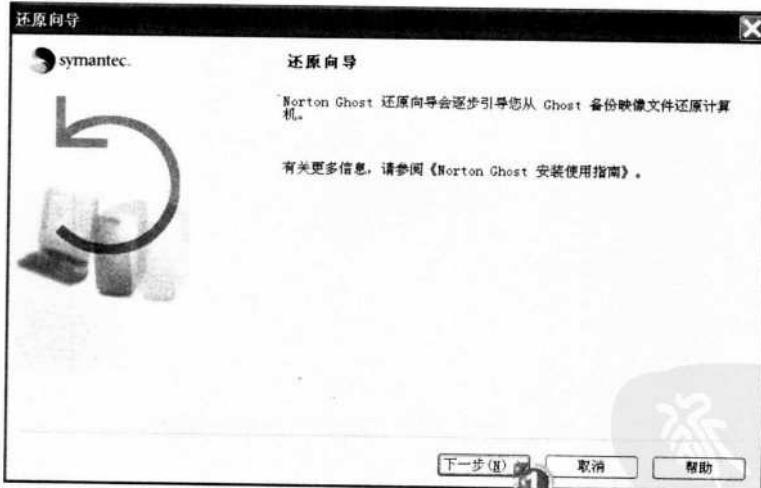
在 Norton Ghost 2003 程序主窗口中选择【还原】选项执行还原向导。

① 单击【还原】选项

**STEP2** 跳过欢迎画面

选择【还原】选项后，首先出现的是还原向导的欢迎界面，单击【下一步】按钮继续执行还原操作。

① 单击【下一步】按钮

**STEP3** 选择映像文件

在【映像文件名】字段中指定前面备份的映像文件的路径及名称，或者单击【浏览】按钮来选择映像文件。

① 指定映像文件的路径及名称

② 单击【下一步】按钮

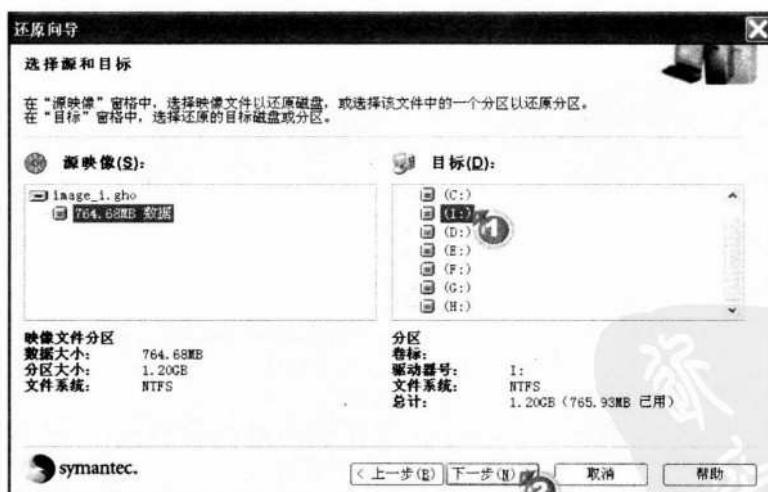


STEP 4 选择目标硬盘或分区

目标硬盘或分区是指要将映像文件还原到哪一个硬盘或分区上，选择完毕后单击【下一步】按钮即可还原。注意：在此切勿选错，否则可能会使硬盘中有用的文件丢失。

① 选择目标分区

② 单击【下一步】按钮

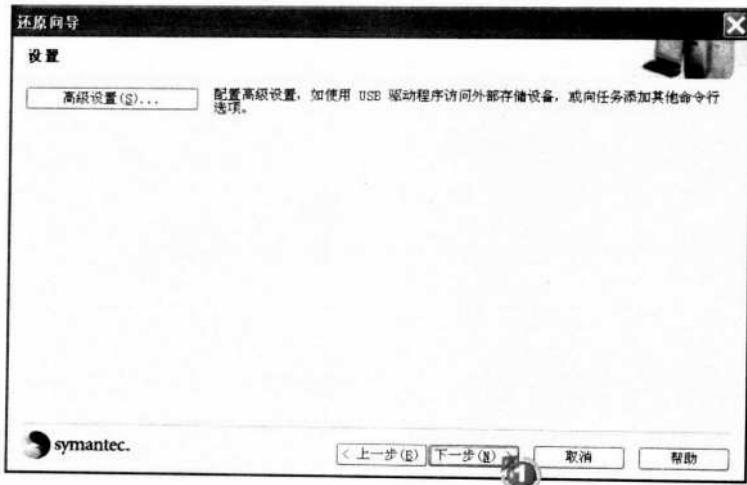


STEP 5 设置高级选项

如果需要使用 USB 存储装置，可单击【高级设置】按钮设置高级选项，否则直接单击【下一步】按钮即可。



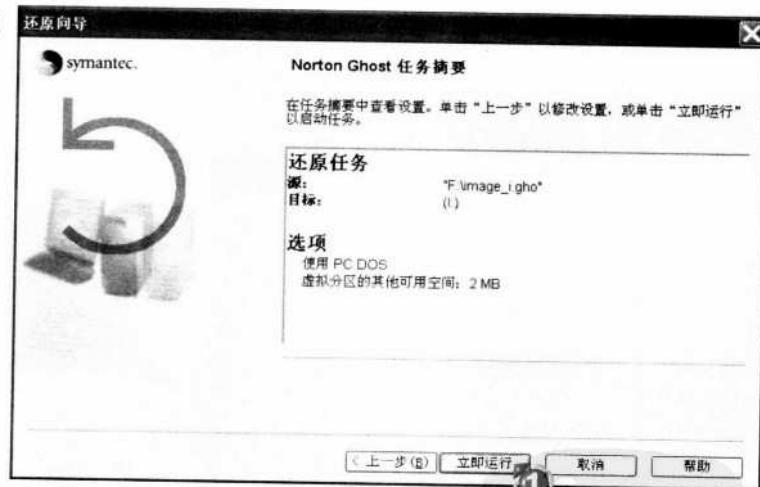
① 单击【下一步】按钮



STEP 6 检视任务摘要

在正式开始还原之前，还原向导会将本次任务摘要显示出来，确认无误后单击【立即运行】按钮开始还原。

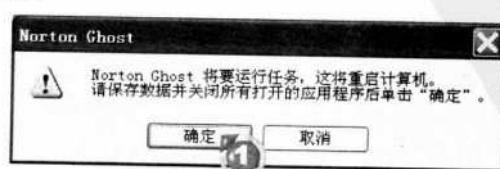
① 单击【立即运行】按钮



STEP 7 重新运行计算机

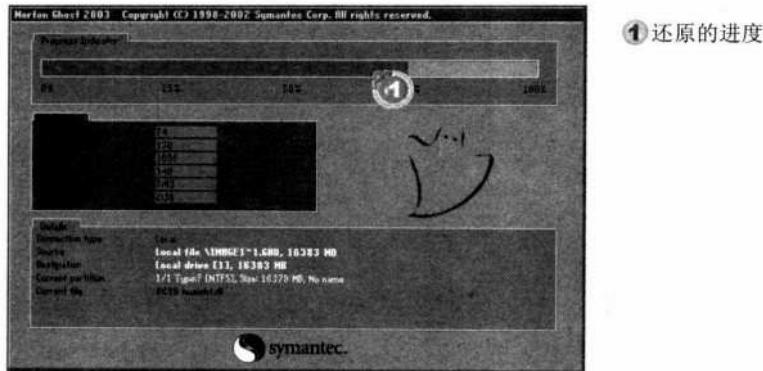
由于操作系统正在运行，而 Ghost 需要重新启动计算机才能执行还原操作，因此需要自动重新启动计算机。

① 单击【确定】按钮，
重新启动计算机



STEP8 检视还原进度

重新运行计算机后，Ghost 将自动执行还原操作，在还原的过程中程序会显示还原的进度。



3.3.3 制作灾难恢复启动盘

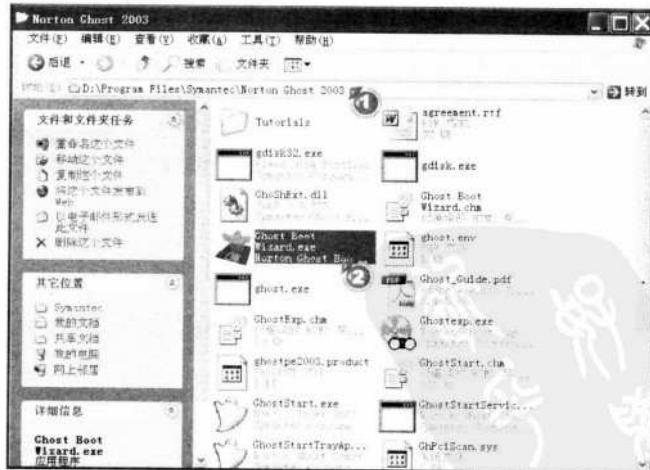
前面介绍的还原系统的方法只适用于操作系统仍可正常运行的情况下，因此为了确保能够在操作系统无法运行时执行还原操作，用户可通过 Norton Ghost 2003 提供的启动盘制作向导（Ghost Boot Wizard）制作一张灾难恢复启动盘，这样当操作系统无法启动时，就可以通过灾难恢复启动盘开机并执行 Ghost 程序，还原系统。

STEP1 执行启动盘制作向导

由于安装向导并未将执行启动盘制作向导的快捷方式添加至【开始】菜单，因此用户必须打开程序文件夹，运行【Ghost Boot Wizard】程序来制作灾难恢复启动盘。

①进入程序的安装文件夹

②双击【Ghost Boot Wizard】图标，执行该程序

**STEP2** 选择制作哪一种磁盘

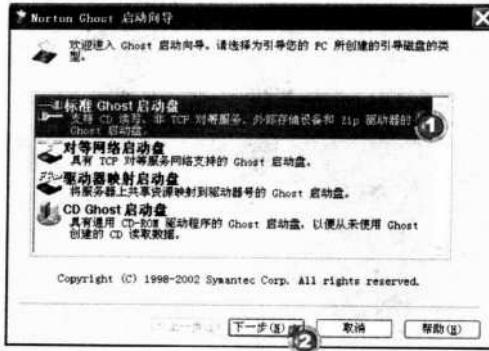
启动盘制作向导可制作多种不同类型的灾难恢复启动盘，例如对等网络启动盘、CD Ghost 启动盘等，一般情况下选择【标准 Ghost 启动盘】即可。



①选择【标准 Ghost 启动盘】

选项

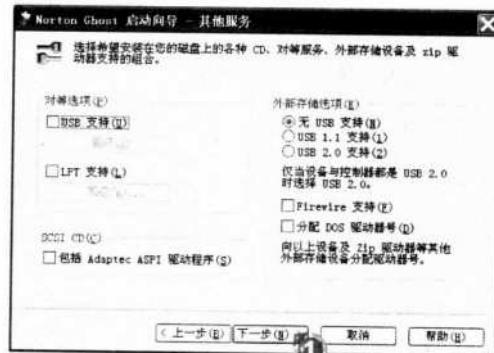
②单击【下一步】按钮



STEP3 设置磁盘附加功能

如果用户需要使用 USB、SCSI 等接口装置，可以在此对话框中选择设置，否则直接单击【下一步】按钮继续。

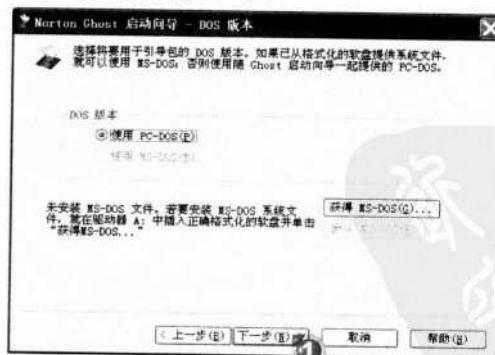
①单击【下一步】按钮



STEP4 设置使用哪一种 DOS 操作系统

启动盘制作向导允许用户选择在灾难恢复启动盘中使用 PC-DOS 或 MS-DOS，由于两者功能极为相似，因此建议采用默认值即可。

①单击【下一步】按钮



STEP5 选择 Ghost 程序位置

为了确保灾难恢复启动盘能够运行 Ghost 程序，启动向导会将硬盘中 Ghost 安装文件夹下 DOS 版本的 Ghost 程序复制到磁盘中，默认状态下启动向导已经自动设

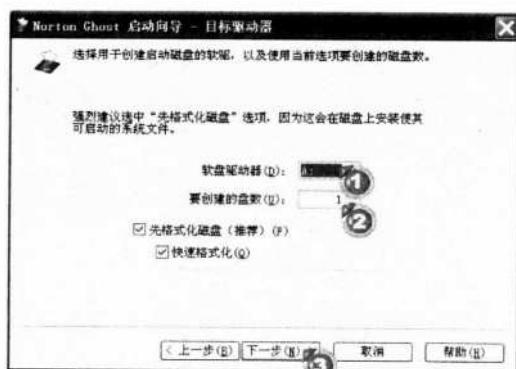
置了程序的路径，用户只要直接单击【下一步】按钮即可。



① 单击【下一步】按钮

STEP 6 设置软盘驱动器路径

如果计算机中有两台软盘驱动器，则需要用户手动指定使用哪一台制作启动盘。此外，用户还可以设置制作启动盘的数量以及是否格式化磁盘。



- ① 指定软盘驱动器
② 设置制作启动盘的数量
③ 单击【下一步】按钮

STEP 7 检视设置

正式开始制作之前，启动向导会将用户所作的设置重新显示出来，确认无误后可单击【下一步】按钮继续操作。



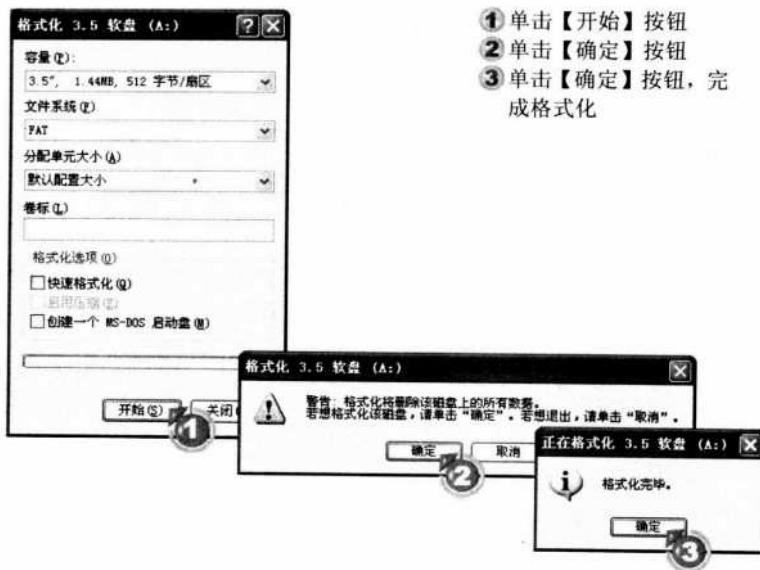
① 单击【下一步】按钮



STEP 8 格式化磁盘

为了确保磁盘有足够的空间，启动向导会格式化磁盘以清除磁盘中的内容，格式化磁盘的设置值无须更改，直接采用默认值即可。

开始格式化之前，会提示格式化磁盘将清除磁盘上的所有资料，单击【确定】按钮确认进行格式化。



STEP 9 开始制作灾难恢复启动盘

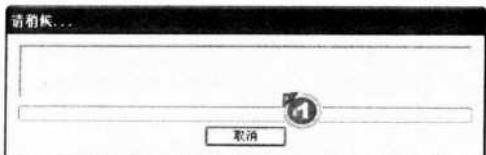
格式化完成后，单击【关闭】按钮关闭【格式化 3.5 软盘】对话框，此后会开始制作启动盘。

① 单击【关闭】按钮



STEP 10 完成启动盘制作

当制作完成灾难恢复启动盘后即可用此盘引导进入系统并执行还原操作。



① 正在制作灾难恢复启动盘

3.3.4 灾难恢复

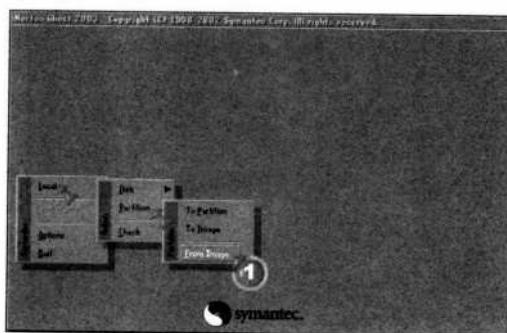
建立灾难恢复启动盘后，应妥善保管磁盘，以后若遇到操作系统严重损坏到无法开机的情况时，即可通过该启动盘还原系统。

注意：灾难恢复启动盘的作用仅提供开机及运行 Ghost 程序的命令，用户仍需配合事先备份的硬盘映像文件才能执行还原操作。由于灾难恢复启动盘中的 Ghost 程序未提供向导，因此对于初级用户而言，可能会存在一定困难。下面就实际演示一下如何通过灾难恢复启动盘还原系统。

用灾难恢复启动盘还原系统时，首先要在 BIOS 中设置以软盘开机。由于设置的方法很简单，因此本文不再介绍，需要的用户可参考介绍 BIOS 设置的相关书籍。

STEP1 打开还原设置

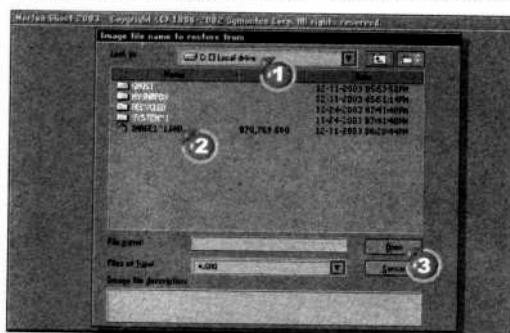
用灾难恢复启动盘开机后，计算机将自动进入 Ghost 程序主窗口，在此窗口中依次选择【Local】→【Partition】→【From Image】命令即可开始还原。



① 依次选择【Local】→【Partition】
→【From Image】命令

STEP2 选择映像文件

选择映像文件的存储位置，然后打开映像文件。

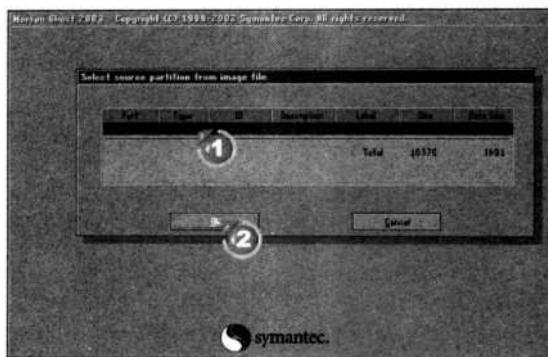


① 打开目标文件夹
② 选择映像文件
③ 单击【Open】按钮

**STEP3** 选择源分区

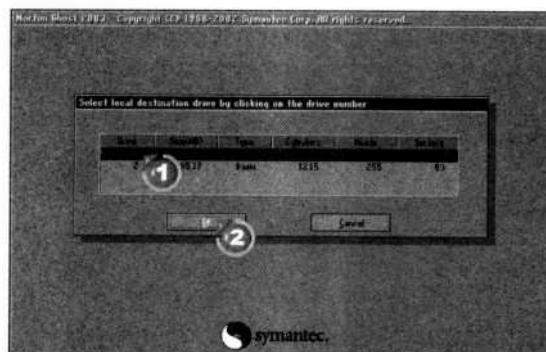
如果映像文件包含了多个分区，则用户可以自由选择还原其中的部分分区。一般情况下，系统分区会显示在列表的最上方，此外用户也可根据分区容量来判断哪一个是系统分区。

- ① 选择源分区
- ② 单击【OK】按钮

**STEP4** 选择目标硬盘

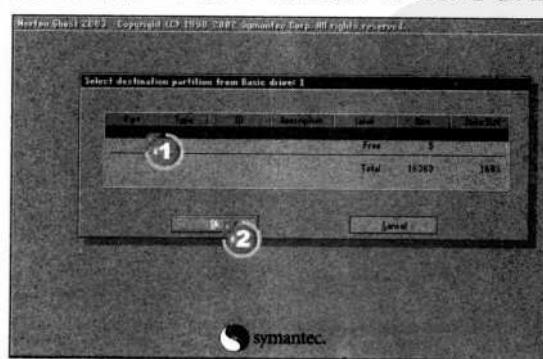
如果计算机中存在多个硬盘，Ghost就会要求用户选择将映像文件还原至哪一个硬盘。

- ① 选择目标硬盘
- ② 单击【OK】按钮

**STEP5** 选择目标分区

选择将映像文件还原至目标硬盘的哪一个分区中，一般情况下系统分区会显示在列表的最上方，但如果硬盘中只有一个分区，则直接单击【OK】按钮即可。

- ① 选择目标分区
- ② 单击【OK】按钮



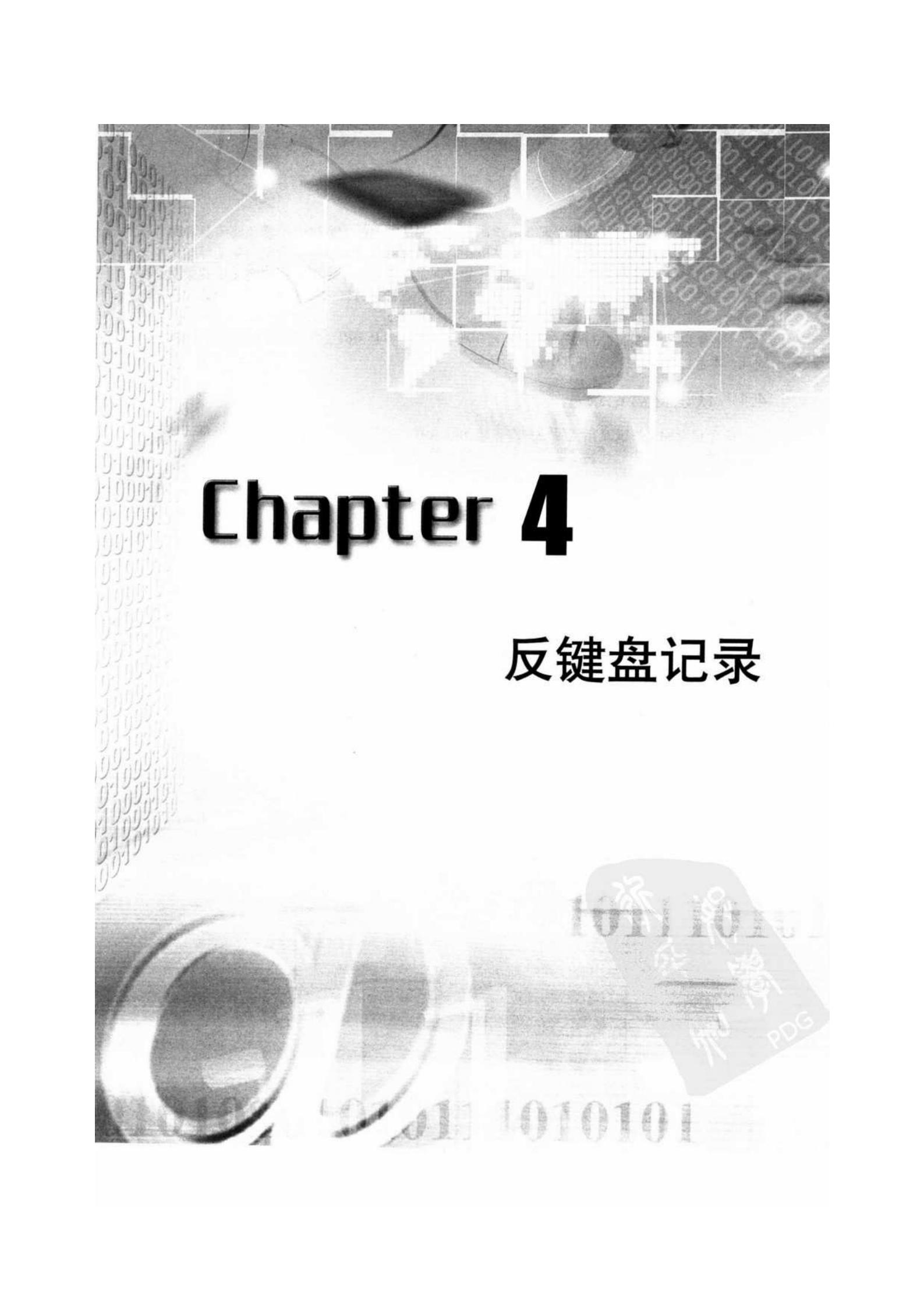
STEP 6 确认执行还原操作

在弹出的窗口中单击【Yes】按钮，确认执行还原操作。



① 单击【Yes】按钮

还原成功后，将灾难恢复启动盘取出并重新启动计算机，系统即可恢复至备份时的状态。



Chapter 4

反键盘记录



在 Internet 越来越发达的今天，用户在享受各种便利服务的同时，也难免要涉及各种密码，如信用卡密码、E-Mail 密码等，甚至在启动计算机时也需要用到密码。从某种意义上来说，这些密码是用户可以享用这些服务的保证，一旦遗失了密码，用户将无法继续享用这些服务。如果密码落在其他用户手中，甚至还会被对方冒名顶替的危险，例如，一些黑客经常用窃取的 E-Mail 账户寄发大量的垃圾邮件等。

一般来说，大部分用户都会对自己的密码严加保护，但是密码被窃的事情还是屡见不鲜。对此，本章将介绍键盘记录在其中扮演的角色。

4.1 认识键盘记录

键盘记录顾名思义是指记录用户键盘输入的内容，在使用计算机时，很多信息都需要通过键盘输入，其中就包括了账户密码之类的重要信息。也就是说，通过记录键盘输入的内容有可能获得其他用户输入的重要信息。

大部分的键盘记录都是通过特殊的软件来完成的，这些软件实际上与木马程序属于同类，但它不像木马程序那样可以控制对方的计算机，而只是默默地记录着对方键盘的输入内容，并从中窃取重要信息。

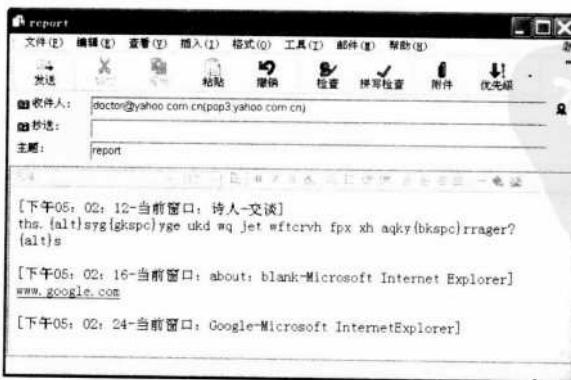
4.1.1 键盘记录的手法

从技术层面来说，以程序记录从键盘输入的内容并不复杂，一个有经验的程序设计人员可以轻松地做到这一点。下面将介绍一下记录信息的存储位置以及黑客取得这些信息的方法。

为了避免让用户发现，键盘记录软件窃取信息后，一般会有两个选择：一是通过 E-Mail 或其他手段及时将其传递给黑客；二是将其隐藏在用户的计算机中，待黑客伺机取走。

● 通过 E-Mail 传递

通过 E-Mail 传递窃取的信息是目前键盘记录程序较常用的方式之一，这种方式效率较高，黑客可以很快取得所需要的信息。但它也有一些不足之处，最明显的就是如果对方的计算机无法连接网络，那么这项功能就会失效；其次就是键盘记录软件在发送 E-Mail 时也很容易会被防火墙发现及拦截。虽然如此，但通过 E-Mail 传递窃取信息的方式仍然被许多键盘记录程序所采用。下图为通过记录软件传递邮件的窗口。

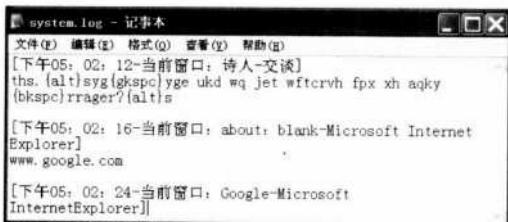


● 记录成 Log 文件

针对通过 E-Mail 发送容易被发现的特点，一些键盘记录软件采用了另一种手段，即将窃取的信息隐藏在用户的计算机中，待黑客伺机取走。此时，键盘记录程序还会将记录的信息伪装成系统或各应用程序的日志文件（Log 文件）。这样，黑客就可以通过键盘记录软件窃取一些一般情况下难以窃取到的信息，例如信用卡账户及密码等数据。

此外，黑客还可以将这类键盘记录程序安装在公共的计算机中（例如网吧里的计算机），这样经过一段时间后，黑客就可以从这台计算机中取得许多用户的重要信息。

下图中显示的是键盘记录软件中的 Log 文件。



4.1.2 常见的键盘记录程序

由于键盘记录程序的制作相对比较简单，因此目前流行的这类软件非常多。下面将介绍几个常用的键盘记录程序，使读者对其有一个概略的认识。

注意：并非所有的键盘记录软件都是恶意的，事实上键盘记录对于计算机的安全管理也非常重要，系统管理员经常需要在某些计算机上安装这类软件以监控计算机的使用情况。

● Tiny Spy Agent

Tiny Spy Agent 是一个简单易用的键盘记录程序，是系统管理员常用的安全管理工具之一。它能够准确记录按键情况，并能够记录按键的时间及输入的内容具体针对哪一个程序。

软件小档案

软件名称：Tiny Spy Agent

版本：2.1.118

官方网站：<http://www.tinystone.com>

其他下载网址 1：<http://download.enet.com.cn/html/060512003122901.html>

其他下载网址 2：<http://www.ttian.net/download/show.php?id=1167>

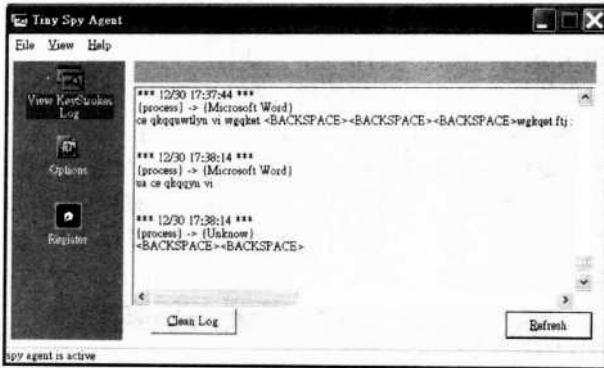
软件类型：共享软件

下图为 Ting Spy Agent 的主界面。

补充说明

安装键盘记录软件

Tiny Spy Agent 及以下介绍的数个键盘记录软件，虽然都是英文软件，但是安装并不复杂，只要按 I Agree、Next 或 Yes 按钮，即可顺利完成安装。



● iOpus STARR

iOpus STARR 是一套功能较完善的键盘记录程序，该软件可记录键盘输入、账户名称、密码、路径、浏览的网站等，另外还可以监视 MSN 等聊天软件的记录。最具特色的是，iOpus STARR 提供了【Standard】和【Secure】两种安装方式，第一种安装方式类似一般的安装应用程序，安装后会在【开始】菜单中增加程序的快捷方式；而第二种安装方式则不会显示任何快捷方式、图标等，用户必须通过特殊的方法才能设置及删除程序。

软件小档案

软件名称：iOpus STARR

版本：Pro v5.00

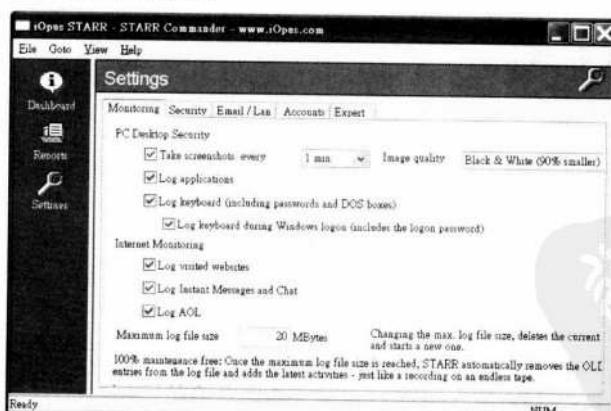
官方网站：<http://www.iopus.com/>

其他下载网址 1：<http://xeqm.com/Software/Catalog38/802.html>

其他下载网址 2：<http://download.pchome.net/system/monitor/9384.html>

软件类型：免费软件

下图为 iOpus STARR 的主界面。



● Keylog

Keylog 是一个非常简单的键盘记录程序，该软件只有一项功能：记录按键情况到一个文本文件中，用户只要执行一次，以后计算机启动时程序就会自动执行。

Keylog 是一个免安装的绿色（不写进注册表）软件，复制文件后按 F12 键即可打开隐

藏的主界面，其最大的优势在于占用的系统资源极少，适合配置较低的计算机使用。

软件小档案

软件名称：Keylog

版本：V2.0

官方网站：<http://www.wanghan.com/>

其他下载网址 1：<http://laoxiang.fjcom.cn/download.asp?id=12762>

其他下载网址 2：<http://www2.skycn.com/soft/12762.html>

软件类型：共享软件



● Active Key Logger

Active Key Logger 是一套专业的键盘记录程序，具有较好的【隐身】效果，执行过程中不会显示在任务管理器中，而且系统栏上的图标亦可隐藏，一般用户难以察觉。当需要设置时，同时按下【Ctrl+Shift+Alt+V】快捷键，即可在系统栏上显示程序图标，使用非常方便。

软件小档案

软件名称：Active Key Logger

版本：V2.8

官方网站：<http://www.winsoul.com/>

其他下载网址 1：http://www.xn163.com/SoftView/SoftView_14831.html

其他下载网址 2：<http://sq.onlinedown.net/soft/12047.htm>

软件类型：免费软件

下图为 Active Key Logger 的主界面。





4.1.3 硬件的键盘记录设备

除了键盘记录程序外，一些厂商还开发了硬件的键盘记录设备，与软件的键盘记录程序相比，硬件的键盘记录设备最大的优势在于不占用任何系统资源。

硬件键盘记录设备的原理并不复杂，它一般是一个连接到键盘上的硬件设备，可以截获键盘输入的信号，并将其储存在自带的存储设备中。

较常见的硬件键盘记录设备有两类，一类连接到键盘上，另一类则直接安装到键盘内部，甚至有些键盘本身就是特制的键盘记录设备。

4.2 反查键盘记录程序

防护键盘记录的方法有两种：一种是主动搜索计算机，删除隐藏的键盘记录程序；另一种则是安装专门的防火墙软件随时监视计算机，一旦发现有程序记录键盘输入即向用户报告。下面将分别介绍防护这两种键盘记录程序的方法。

4.2.1 检查与删除暗藏的键盘记录程序

虽然键盘记录程序经常会成为黑客的工具，但由于键盘记录程序种类繁多，而且其中大部分还是系统管理员经常用到的系统管理工具，因此大多数防毒软件都没有将键盘记录程序当成病毒或木马程序来处理，因此要删除键盘记录程序时，用户必须借助专门的删除程序。

Anti-keylogger 是相当简单易用的键盘记录程序删除工具，用户只需简单的几个步骤就可以删除计算机中的键盘记录程序。下面将以此程序为例，介绍如何检查与删除隐藏在用户计算机中的键盘记录程序。下图为 Anti-keylogger 的官方网站主界面。



软件小档案

软件名称：Anti-keylogger

版本：V6.1

官方网站：<http://www.anti-keyloggers.com/>

其他下载网址 1：<http://www.codedown.cn/soft/11803.htm>

其他下载网址 2：<http://cn.shareware-download.org/anti-keylogger-i20425.php>

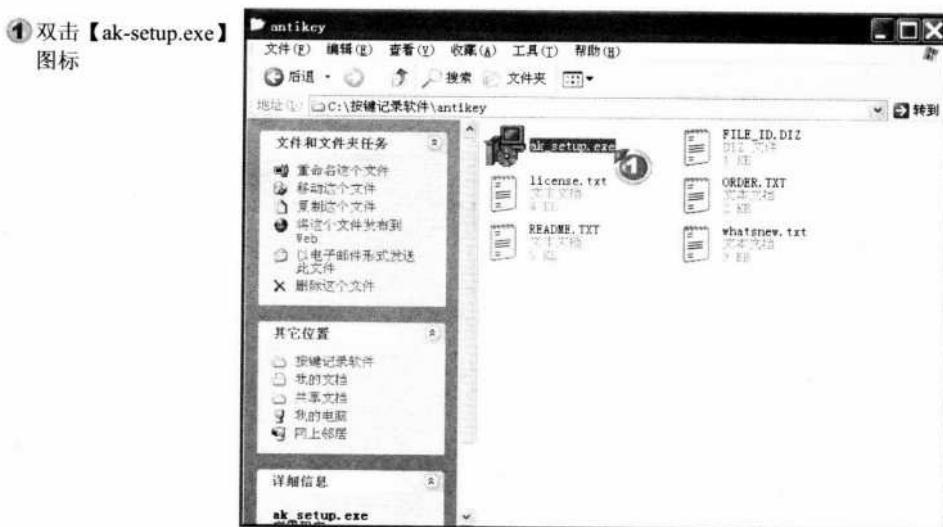
软件类型：共享软件

● 安装 Anti-keylogger

Anti-keylogger 的安装非常简单，下载安装文件后，在下载文件夹中双击安装文件，然后按照向导的提示操作即可。

STEP1 执行安装程序

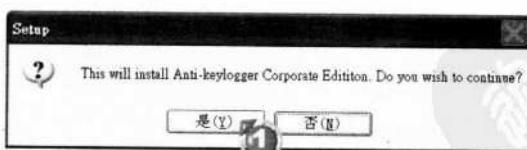
打开安装文件所在的文件夹后，双击安装文件，执行安装程序。



STEP2 确认执行安装程序

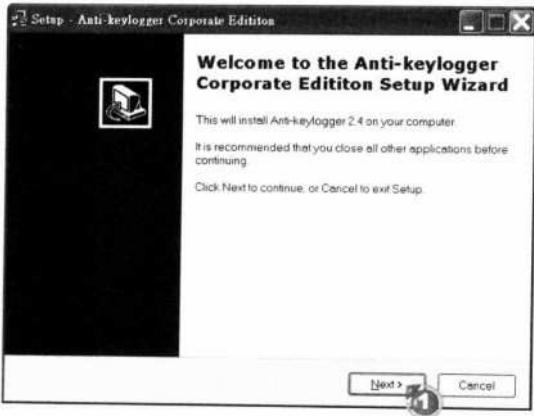
在【Setup】对话框中，单击【是】按钮，确认执行安装程序。

① 单击【是】按钮



STEP3 跳过欢迎界面

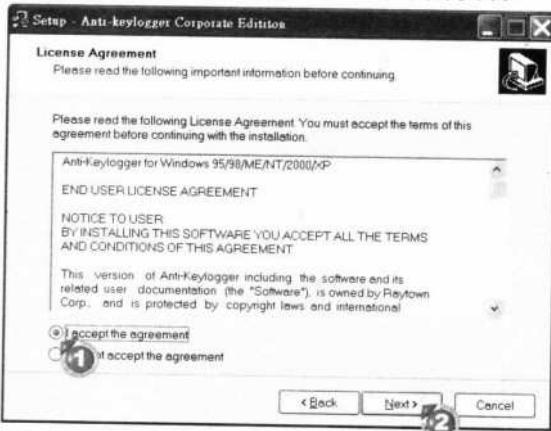
为了避免安装失败，安装向导在欢迎界面中要求用户在安装之前关闭其他应用程序，然后继续安装。



- ① 单击【Next】按钮，继续安装

STEP 4 接受授权协议

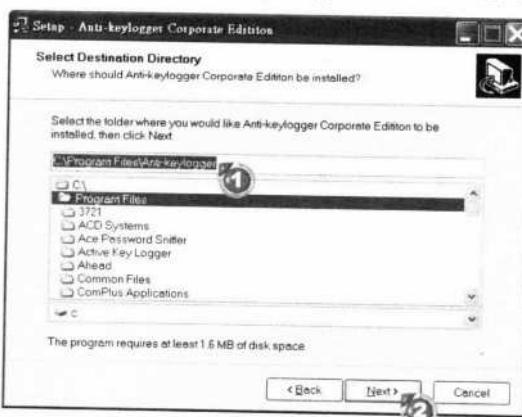
阅读并接受该软件的授权协议，继续执行安装。



- ① 选择【I accept the agreement】单选框
② 单击【Next】按钮

STEP 5 选择安装路径

程序默认安装在系统分区的【Program Files】文件夹中，但用户也可自定义安装路径。



- ① 设置安装路径
② 单击【Next】按钮

STEP6 设置是否新增快捷方式至【开始】菜单

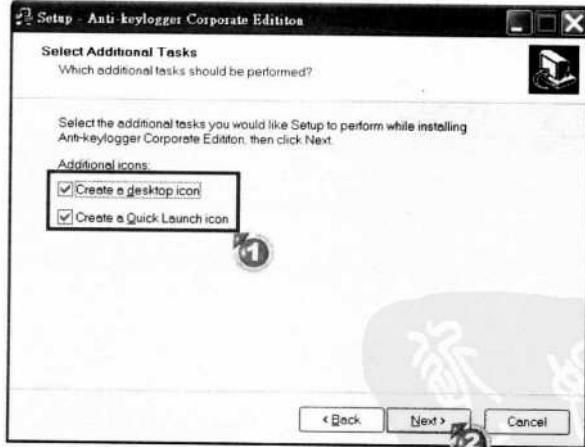
安装向导会在【开始】菜单中添加一个文件夹用于存储程序的快捷方式，用户可以在此指定这个文件夹的名称，建议采用默认值。如果不想在【开始】菜单中增加快捷方式，可以选中【Don't create a Start Menu folder】复选框。

- ①输入文件夹名称
②单击【Next】按钮

**STEP7** 设置是否新增快捷方式至桌面及快速启动栏

如果用户希望在桌面新增程序的快捷方式，可以选择【Create a desktop icon】复选框；如果希望新增快捷方式至快速启动栏，则可以选择【Create a Quick Launch icon】复选框。

- ①选择【Create a desktop icon】及【Create a Quick Launch icon】复选框
②单击【Next】按钮

**STEP8** 开始安装

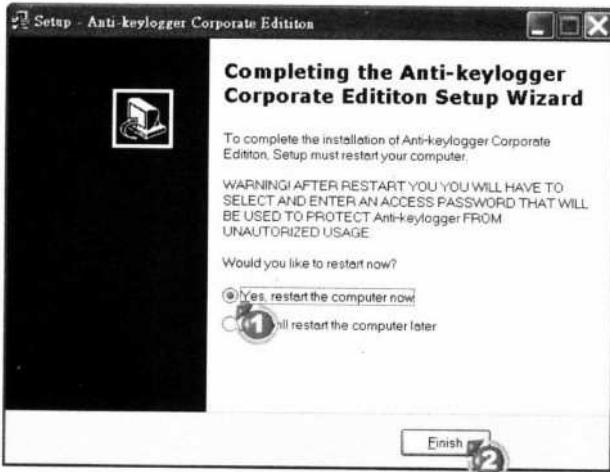
设置完成后，安装向导会显示用户的设置，此时只要单击【Install】按钮即可开始安装。



① 单击【Install】按钮

STEP 9 重新启动计算机

安装完成后需要重新启动计算机，可以选择立即启动或稍后启动。



① 选择【Yes, restart the computer now】单选框

② 单击【Finish】按钮

重新启动计算机后，Anti-keylogger 安装完成，用户可以通过它来清除计算机中隐藏的键盘记录程序。

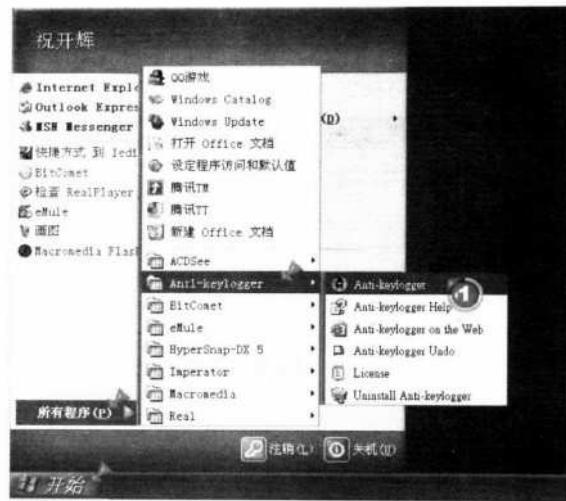
● 删除暗藏的键盘记录程序

Anti-keylogger 的使用方法非常简单，执行程序后，它会对计算机进行全面的扫描，一旦发现键盘记录程序就会将其清除。下面就介绍一下如何通过 Anti-keylogger 清除键盘记录程序。

STEP 1 执行 Anti-keylogger 程序

通过【开始】菜单快速启动 Anti-keylogger 程序。

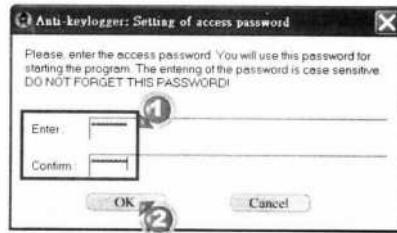
- ① 依次选择【开始】→【所有程序】→【Anti-keylogger】→【Anti-keylogger】选项



STEP2 设置用户密码

第一次使用 Anti-keylogger 程序时，程序会要求用户设置密码，以避免其他用户随意执行此程序。

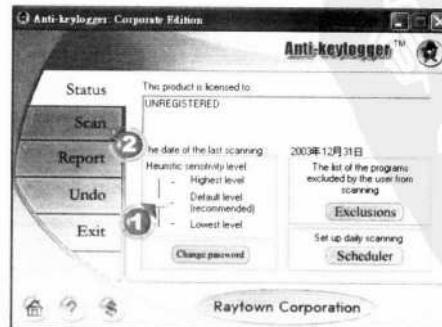
- ① 设置用户密码
② 单击【OK】按钮



STEP3 设置防护等级

Anti-keylogger 提供了 3 个防护等级：【Highest level】防护能力最强，可以侦测到绝大多数的键盘记录程序，但也极有可能将一般的程序误判为键盘记录程序；【Lowest level】与【Highest level】相反，不容易误判，侦测能力也最弱；【Default level】介于【Highest level】和【Lowest level】之间，一般情况下建议设置为【Default level】。

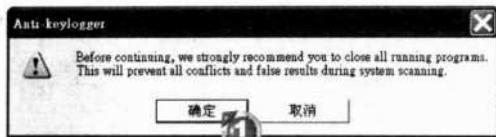
- ① 拖动游标至【Default level】位置
② 单击【Scan】按钮，扫描计算机





STEP 4 执行扫描操作

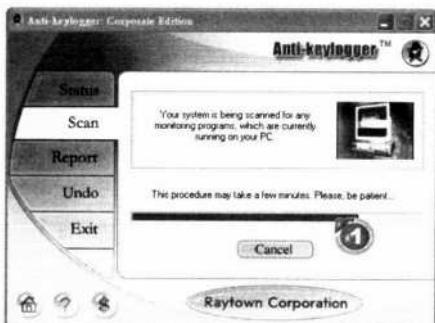
单击【Scan】按钮后，在打开的【Anti-keylogger】窗口中单击【确定】按钮，确定执行扫描操作。



① 单击【确定】按钮

STEP 5 检视扫描进度

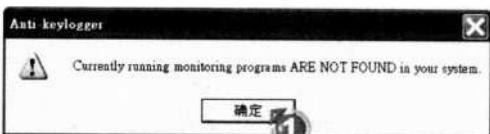
扫描过程中程序会显示扫描的进度。一般来说，扫描所需的时间较长，需耐心等待。需要注意的是，程序会在扫描过程中限制用户执行其他操作，以免影响扫描。如需中断扫描，可单击【Cancel】按钮。



① 扫描的进度

STEP 6 检视扫描结果

扫描完成后，程序会告知用户扫描结果。



① 单击【确定】按钮

STEP 7 检视详细报告

除了简单的扫描报告外，Anti-keylogger 还会显示此次扫描的详细报告。



① 扫描的详细报告

● 变更密码

在第一次执行 Anti-keylogger 时会要求用户设置密码，后续用户必须输入正确的密码才能执行此程序。在使用过程中，用户可能需要变更 Anti-keylogger 的密码。下面就介绍一下变更密码的方法。

STEP1 打开变更密码设置窗口

在程序主窗口中，单击【Change password】按钮可执行变更密码操作。

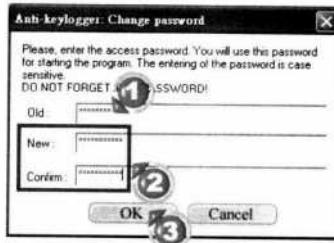
- ① 单击【Change password】按钮



STEP2 设置新密码

在设置新密码时，程序会要求用户先输入旧密码，因此不知道旧密码的用户将无法变更密码。

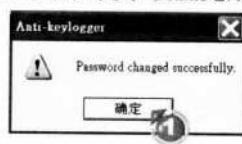
- ① 输入旧密码
② 输入新密码
③ 单击【OK】按钮完成设置



STEP3 完成变更密码

设置完成后，程序会弹出一个对话框提示设置完成，单击【确定】按钮即可。

- ① 单击【确定】按钮



4.2.2 专门对付键盘记录的防火墙

虽然有专门的程序可以用来删除键盘记录软件，但由于键盘记录程序的种类很多，难免会有一些无法清除的键盘记录程序。为了确保计算机的安全，用户还需要安装防火墙软件来防护键盘记录程序，这类防火墙软件会随计算机开机自动启动，一旦监测到有程序记录键盘输入，就会向用户发出警告并阻止这个软件继续执行。



下面将以目前较流行的 Advanced Anti keylogger 为例，介绍如何通过专用的防火墙软件拦截键盘记录程序。

软件小档案

软件名称：Advanced Anti keylogger

版本：3.2

官方网站：<http://www.anti-keylogger.net>

其他下载网址 1：http://219.140.69.6/down/SoftView/SoftView_14014.html

其他下载网址 2：http://www.fbsky.com/SoftDown/SoftDown_3720.html

软件类型：共享软件

下图为 Advanced Anti keylogger 的官方网站。



● 安装 Advanced Anti keylogger

Advanced Anti keylogger 的安装非常简单，下载并执行安装文件后，用户只需按照向导的提示进行操作即可。在执行安装前要先关闭其他程序，以免安装失败。

STEP 1 执行安装程序

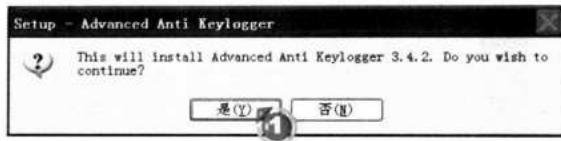
下载文件后，双击安装文件图标，执行安装程序。



STEP2 确认执行安装程序

在【Setup】对话框中单击【是】按钮，确认执行安装程序。

- ① 单击【是】按钮

**STEP3 跳过欢迎界面**

单击【Next】按钮，跳过欢迎界面，继续执行安装。

- ① 单击【Next】按钮

**STEP4 接受授权协议**

阅读并接受授权协议，继续执行安装操作，否则安装将无法继续。

- ① 选择【I accept all...】复选框

- ② 单击【Next】按钮

**STEP5 设置是否在桌面及快速启动栏建立快捷方式**

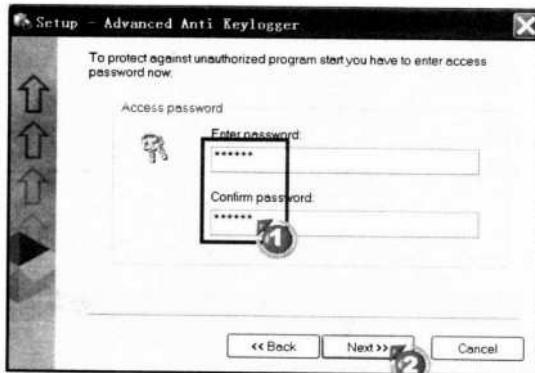
如果需要在桌面建立快捷方式，可选择【Create Desktop icon】复选框；如果需要在快速启动栏建立程序快捷方式，可选择【Create Quick Launch icon】复选框。本例只在桌面建立快捷方式，故只选择前者。



- ① 选择【Create Desktop icon】复选框
- ② 单击【Next】按钮

STEP 6 设置密码

安装向导要求用户设置一个密码，后续用户必须输入正确的密码才能设置 Advanced Anti keylogger，此步骤的目的是为了避免其他用户随意执行此程序。



- ① 输入密码
- ② 单击【Next】按钮，继续安装

STEP 7 开始安装

设置完成后，安装向导会显示出用户所做的设置，检视后单击【Install】按钮开始安装。



- ① 单击【Install】按钮

STEP 8 重新启动计算机

最后，安装向导会要求用户重新启动计算机以完成安装。

- ① 选择【Yes, restart my computer】单选框
- ② 单击【Finish】按钮

**● 以 Advanced Anti keylogger 监控键盘记录程序**

完成安装后，Advanced Anti keylogger 会在启动计算机时自动执行，监控键盘记录程序，一旦发现有程序记录键盘输入内容，就会自动阻止此程序并向用户询问是否允许该程序执行。

STEP 1 打开程序主窗口

Advanced Anti keylogger 程序在执行时会在系统栏上显示程序图标，通过此图标用户可以看到程序是否正常工作。

- ① 双击系统任务栏上的程序图标，打开程序主窗口

**STEP 2 检视程序清单**

在 Advanced Anti keylogger 程序主窗口中会显示出目前正在记录键盘输入的程序，但这些程序未必就是键盘记录程序，因为有许多正常的程序也会自动记录键盘输入，例如输入法软件等。

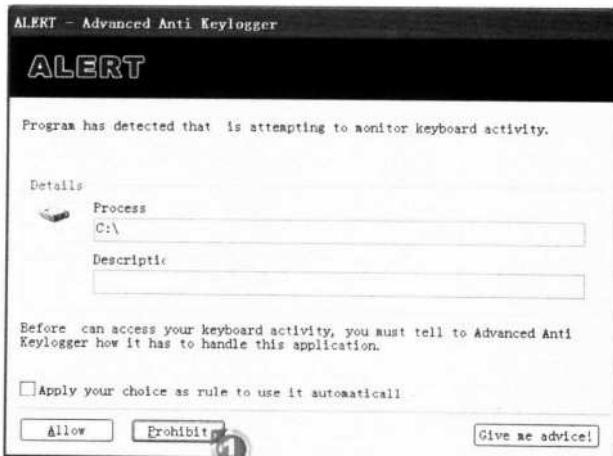
- ① 记录键盘输入的程序清单



**STEP3** 设置是否允许某程序记录键盘输入

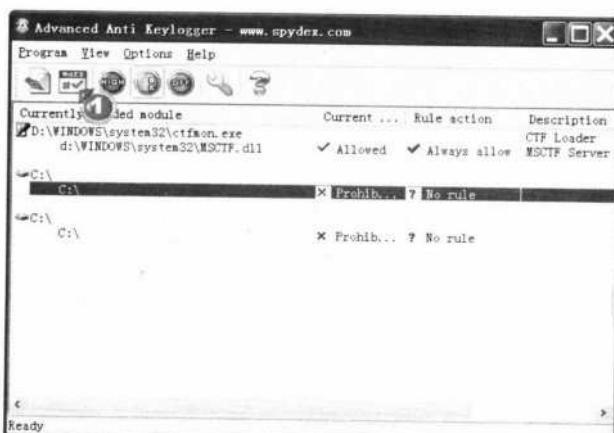
当有应用程序尝试记录键盘输入时，Advanced Anti keylogger 程序会弹出一个警告对话框，询问用户是否允许此程序进行记录，如果用户希望程序不要重复出现此警告对话框，可以选择【Apply your...】复选框为程序建立规则。

- ① 单击【Prohibit】按钮，阻止程序记录键盘输入

**STEP4** 编辑程序规则

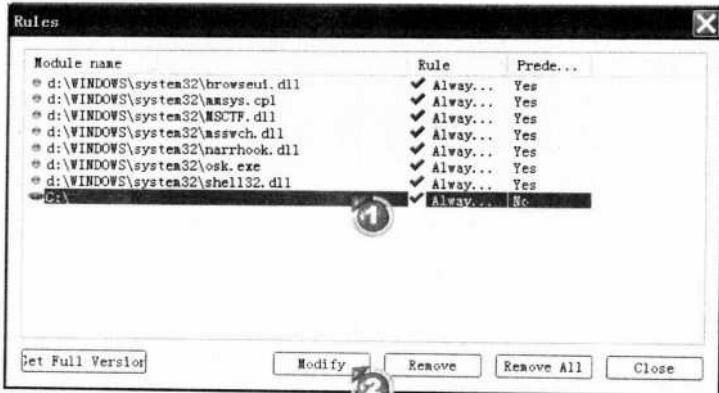
建立规则后，日后此程序再次记录键盘输入时，Advanced Anti keylogger 程序将会自动按照建立的规则设置允许或阻止程序记录键盘输入。用户可以单击【】按钮，打开【Rules】对话框编辑规则。

- ① 单击【】按钮，打开【Rules】对话框

**STEP5** 选择要编辑的规则

在【Rules】对话框中可看到目前已经建立的规则，选择要编辑的项目后可单击【Modify】按钮，打开【Modify rule action】对话框重新设置规则。

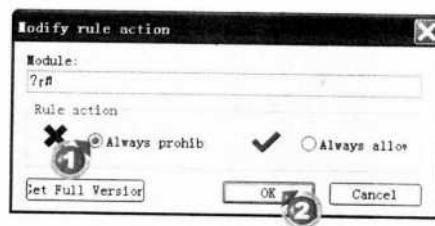
- ① 选择要编辑的规则
② 单击【Modify】按钮



STEP 6 修改规则

在【Modify rule action】对话框中用户可重新指定允许或阻止某程序记录键盘输入，本例选择【Always prohibit】单选框，阻止程序记录键盘输入。

- ① 选择【Always prohibit】
单选框，阻止程序记录
键盘输入
② 单击【OK】按钮



STEP 7 检视结果

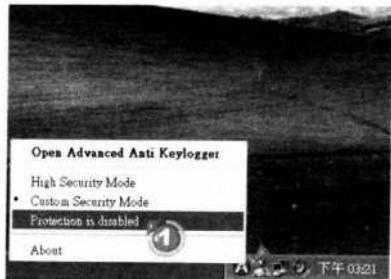
设置完成后，可以在【Rules】对话框中看到规则已经变更。

- ① 修改后的规则



STEP 8 关闭保护功能

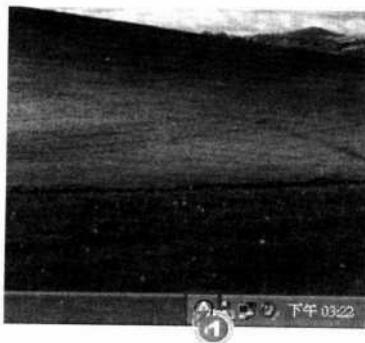
Advanced Anti keylogger 允许用户暂时关闭保护功能，关闭保护功能后，任何程序都可以不受限制地记录键盘输入，因此除非有必要，一般情况下尽量不要关闭保护功能。



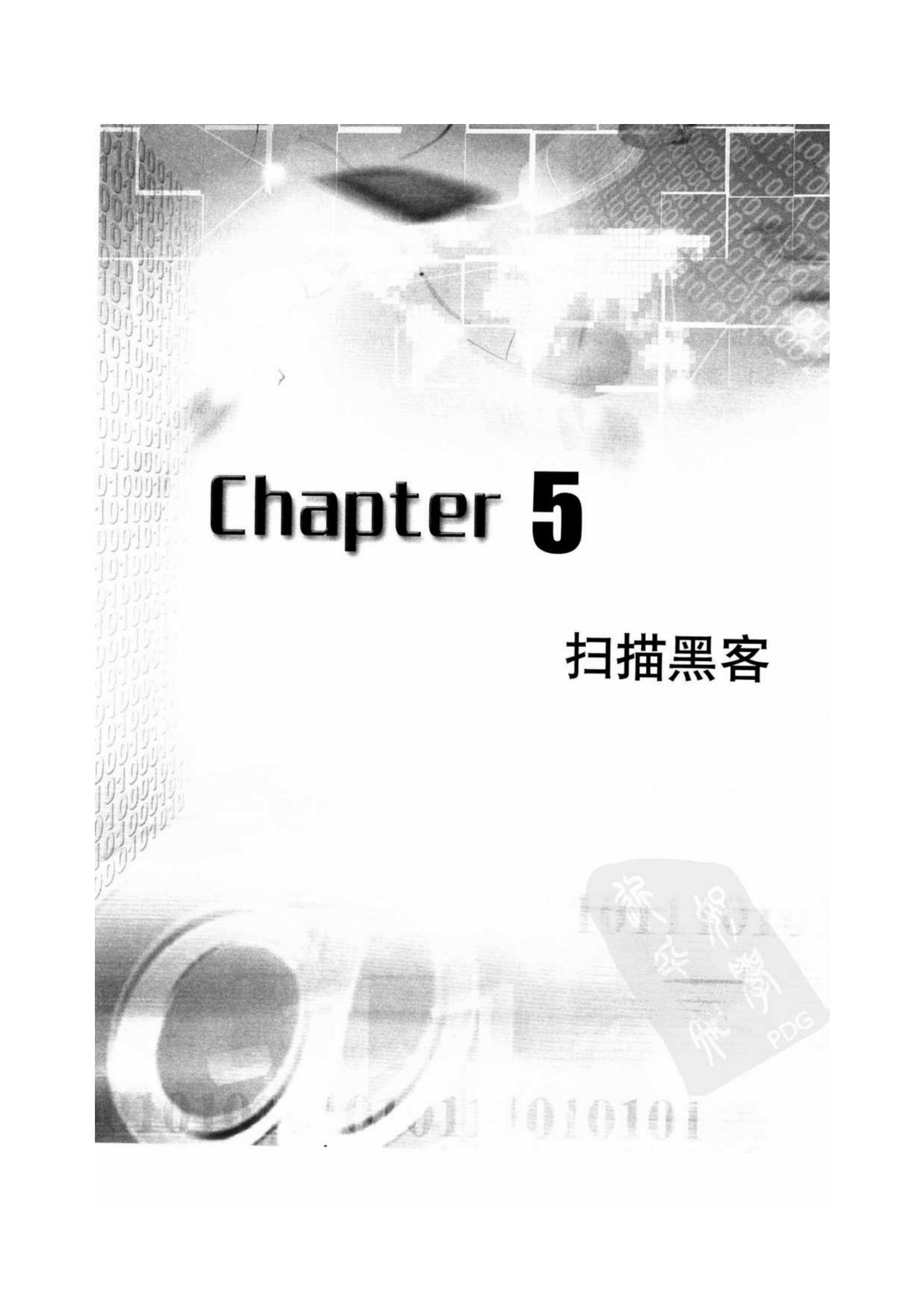
①单击右键，选择【Protection is disabled】命令

STEP 9 关完保护功能后的结果

关闭保护功能后，系统栏上的程序图标会变暗，此时 Advanced Anti keylogger 已经关闭阻止其他程序记录键盘输入的功能。当有需要时，用户可以重新启动保护功能。



①关闭保护功能的图标



Chapter 5

扫描黑客



无论是反木马程序，还是反按键记录，都是在自己的计算机中清除黑客留下的【后门】，是一种被动防御黑客的方法。为了确保自己的计算机安全，有时候还应当主动出击，至少要掌握黑客的虚实，为网络警察追踪黑客提供更多的线索。

部分高水平的黑客一般都不会通过自己的计算机来攻击他人，而是利用其他计算机作为跳板来入侵。如果遇到这种情况，要追踪黑客是比较困难的，因此多获取一些黑客的信息可为网络警察追踪黑客提供帮助，同时也有助于防御黑客再次入侵。

5.1 测试黑客计算机

当用户发现黑客试图入侵计算机时，可以通过各种途径来测试黑客的计算机。Windows本身内建了一些命令，通过这些命令，用户无须借助任何软件即可获取关于黑客的信息。

5.1.1 Ping 命令

Ping 命令是网络管理员最常使用的命令之一，其作用是测试这台计算机与目标计算机之间是否正常连接，并能概括地评估网络状况。Ping 命令检测网络的原理非常简单，执行命令后，系统会向目标主机发送数个特殊的数据包（默认为 4 个，用户也可自定义其数量），对方计算机收到这些数据包后，就会返回同样数量的确认数据包，通过这种方式就可以简单测试两台计算机之间的连接状况。

● 以 Ping 命令测试黑客计算机

Ping 命令的使用方法非常简单，用户只需在 Windows XP 的命令提示符下输入 Ping + 对方 IP 地址即可。

STEP 1 打开【命令提示符】窗口

Ping 命令需要在命令提示符模式下执行，因此需要通过【开始】菜单的快捷方式打开【命令提示符】窗口。

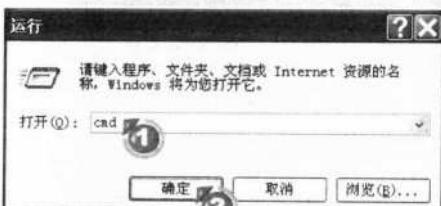
- ① 选择【开始】→【所有程序】→【附件】→【命令提示符】选项



补充说明

还有其他的方法可以打开【命令提示符】窗口吗？

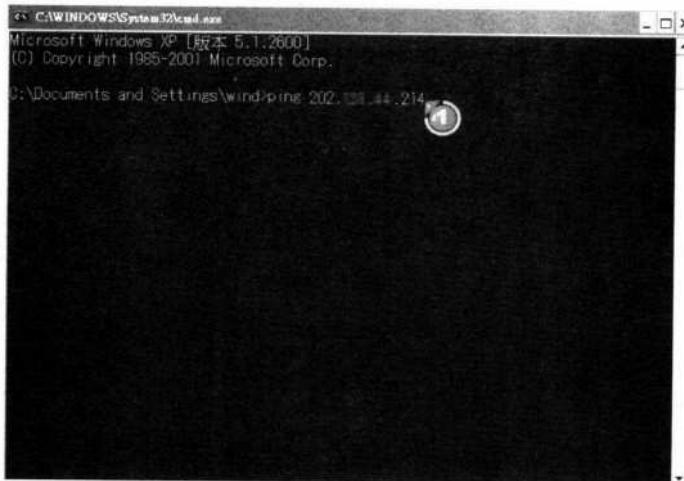
有一部分用户可能在【开始】菜单上找不到打开命令提示符的快捷方式，此时可以在【运行】窗口里输入“cmd”命令来打开【命令提示符】窗口。



- ① 输入“cmd”命令
② 单击【确定】按钮

STEP2 测试黑客计算机

在【命令提示符】窗口中，通过 Ping 命令测试黑客的计算机，命令的格式是：
Ping IP 地址

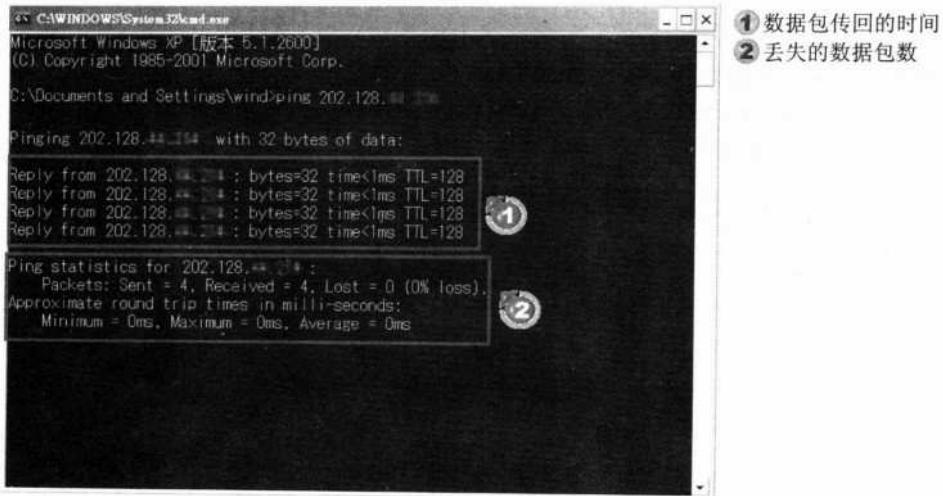


- ① 输入命令

STEP3 检视测试结果

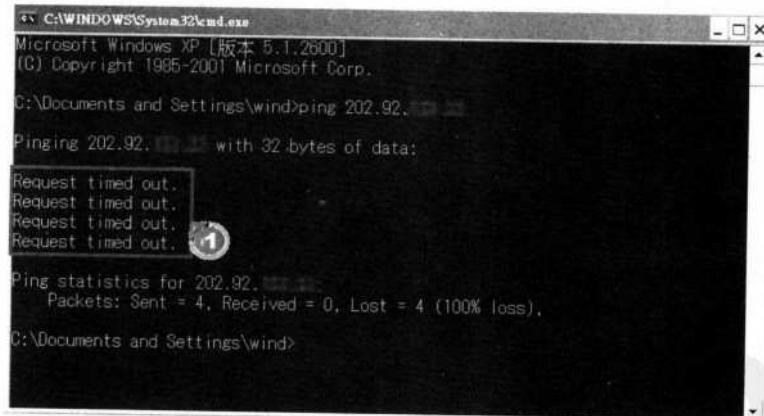
开始测试后，系统会向黑客的计算机发送 4 个特殊的数据包，稍候即可看到测试的结果。在检视测试结果时，要特别注意以下选项：

- time < xms
表示数据包传回的时间，数字越小，说明网络越畅通。
- Lost = x
表示丢失的数据包数量，数字越大说明丢失的数据包越多。一般情况下，每次测试共会送出 4 个数据包，因此当显示“Lost = 4”时，说明所有的数据包全部丢失。



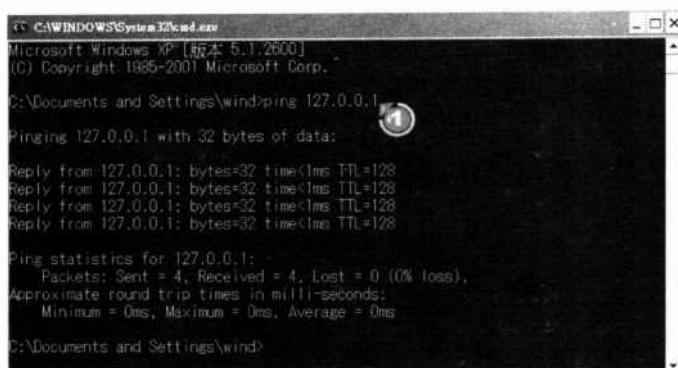
经过上面的步骤，用户就可以了解自己与黑客之间的连接状况。但是，要提醒读者注意的是，用 Ping 命令测试并非万能，因为 Ping 命令是通过 ICMP 网络协议来工作的。假如对方设置计算机禁止响应 ICMP 协议的数据包，则使用 Ping 命令探测时就会收到“Request timed out”的错误信息。此外，如果计算机本身的 TCP/IP 协议没有正确安装，也会出现“Request timed out”的错误。另外，网络连接中断也会导致“Request timed out”错误信息出现。

① “Request timed out”的错误信息



● 以 Ping 命令测试网络协议

为了确定“Request timed out”错误是否由自己的计算机故障引起，用户可以采用“Ping 127.0.0.1”命令来测试网络协议是否正常。127.0.0.1 是一个特殊的 IP 地址，并不对应真实的计算机，而是用来供用户测试网络协议是否正常。如果执行“Ping 127.0.0.1”命令后仍出现“Request timed out”错误，则应重新安装网络协议。



```
C:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\wind>ping 127.0.0.1
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\wind>
```

① 输入“Ping 127.0.0.1”命令

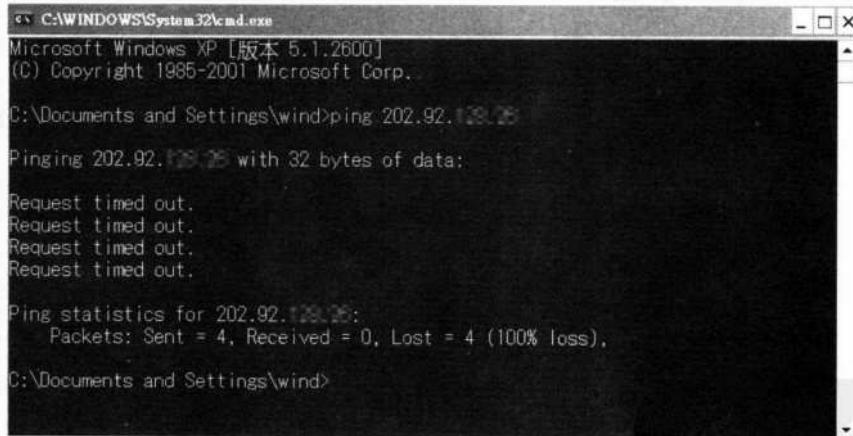
补充说明

Ping 命令的错误信息

Ping 命令常见的错误信息主要有以下几种，其代表的含义如下：

- Request timed out

测试数据包可以到达目标计算机，但没有收到对方的响应数据，出现这种情况一般是因为对方设置了禁止响应 ICMP 协议。此外，对方断开网络连接时也可能出现这样的错误信息。



```
C:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\wind>ping 202.92.129.25
Pinging 202.92.129.25 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 202.92.129.25:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    C:\Documents and Settings\wind>
```

- Destination Net Unreachable

用户指定为网关的计算机出现故障，该计算机的路由表无法提供路由选径所必需的信息时，就会显示该错误。

- Destination host unreachable

出现这个错误信息一般是因为网卡被禁用或出现故障，如果是网卡被禁用，可重新启用，但如果是网卡存在硬件故障，则需更换网卡。

**补充说明****Ping 命令的错误信息**

```
C:\> C:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\wind>ping 202.96.128.68

Pinging 202.96.128.68 with 32 bytes of data:

Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.

Ping statistics for 202.96.128.68:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Documents and Settings\wind>
```

● Destination specified is invalid

测试的 IP 地址是具有特殊作用的 IP，这类 IP 不能使用 Ping 命令测试，当然一般情况下计算机也不可能指定自己的 IP 为这类地址。

```
C:\> C:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\wind>ping 244.1.1.1

Pinging 244.1.1.1 with 32 bytes of data:

Destination specified is invalid.
Destination specified is invalid.
Destination specified is invalid.
Destination specified is invalid.

Ping statistics for 244.1.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Documents and Settings\wind>
```

● Source quench received

数据包可以传送至对方计算机，但对方计算机因为过于繁忙而无法响应，这种错误信息十分罕见，大多数情况下，系统会显示【Request timed out】错误信息。

5.1.2 取得黑客的路由表

经过前面的测试已经大致了解了黑客与计算机之间的基本连接状况，此后可以进一步尝试获取更详细的信息。tracert 是 Windows XP 内建的一个较常用的命令，通过该命令可获取对方的路由传送表，即数据包传送所经过的路径。

从路由传送表中可看出，数据包从黑客计算机到达这台计算机（或由这台计算机到达黑客计算机）时，会经过网络上哪些主机，这是追踪黑客时所需的重要信息之一。

STEP1 打开【命令提示符】窗口

通过【开始】菜单上的快捷方式打开【命令提示符】窗口，以便执行“tracert”命令。

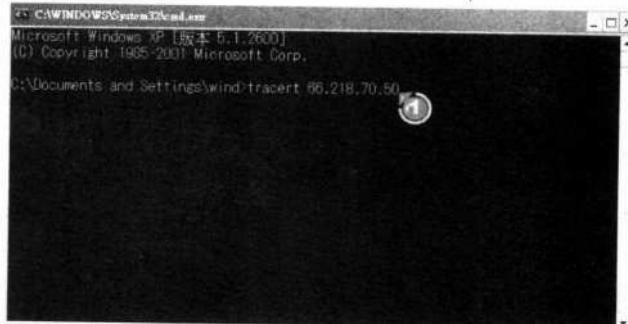


- ① 依次选择【开始】→【有
程序】→【附件】→【命
令提示符】选项

STEP2 获取路由传送表

“tracert”命令的使用方法很简单，用户只要输入“tracert 对方 IP 地址”即可获取对方计算机的路由传送表。

① 输入命令

**STEP3** 检视路由传送表

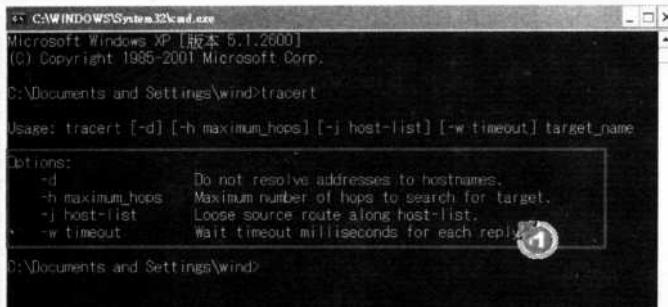
输入命令后，系统将开始尝试获取路由传送表，稍候片刻，屏幕上就会显示出路由传送表。

① 路由传送表



补充说明**检视 tracert 命令的详细用法**

前面介绍的只是 tracert 命令最基本的用法，事实上这项命令还可以搭配适当的参数来执行，如需了解各种参数的作用及使用方法，可直接输入“tracert”命令查找。



```
Microsoft Windows XP [版本 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\wind>tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name

Options:
  -d          Do not resolve addresses to hostnames.
  -h maximum_hops Maximum number of hops to search for target.
  -j host-list  Loose source route along host-list.
  -w timeout   Wait timeout milliseconds for each reply.

C:\Documents and Settings\wind>
```

① tracert 命令的参数

5.1.3 反查黑客的域名

在 Internet 上存在着许多域名服务器（DNS），其作用是将域名与 IP 地址对应起来。正是因为这些域名服务器，才让用户无须记忆枯燥的 IP 地址。由于域名服务器上保存着大量域名和 IP 地址的对应列表，因此在得到黑客的 IP 地址后，用户可以向域名服务器查找这个 IP 地址所对应的国际域名，以便帮助系统管理人员及网络警察追踪黑客。

反查黑客的域名并不复杂，因为 Windows XP 已经提供了向域名服务器查找 IP 地址及域名的命令 nslookup，这项命令使得用户既可通过 IP 地址查找域名，也可通过域名查找 IP 地址。

下面将以反查 IP 地址 66.218.70.50 的 DNS 为例，说明通过 nslookup 命令反查黑客域名的方法。注意：本例中的 IP 地址只是举例说明，并非真的是黑客的 IP 地址。

STEP① 打开【命令提示符】窗口

通过【开始】菜单上的快捷方式打开【命令提示符】窗口，以便执行 nslookup 命令。

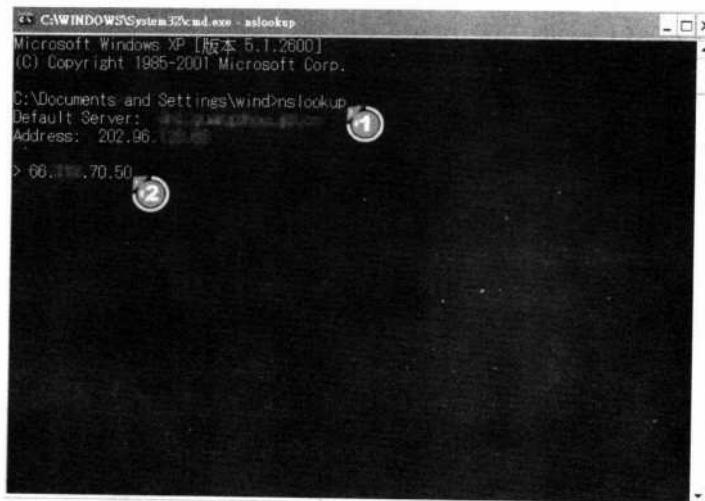


① 依次选择【开始】→【所有程序】→【附件】→【命令提示符】选项

STEP2 反查黑客域名

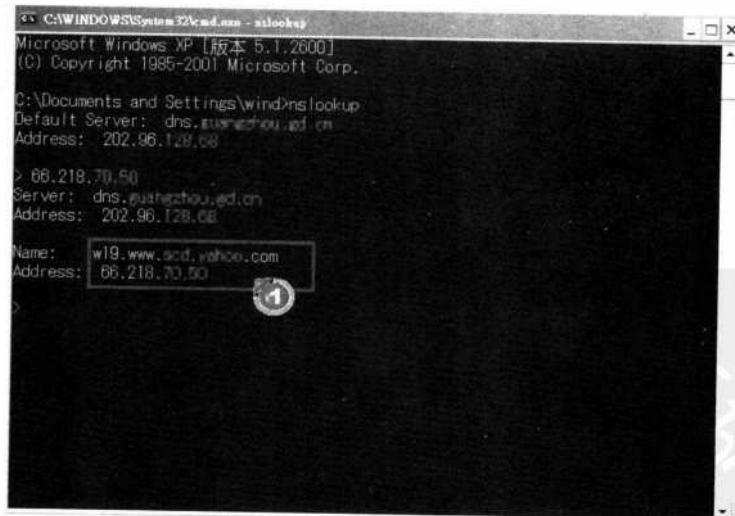
nslookup 命令的使用方法比较特殊，首先输入“nslookup”命令，然后再输入要查找的 IP 地址。

- ① 输入“nslookup”命令
- ② 输入要查找的 IP 地址

**STEP3** 检视查找结果

输入要查找的 IP 地址后，稍候片刻就会显示此 IP 地址对应的 DNS。

- ① 查找结果

**STEP4** 结束查找

查找完毕后，可输入“exit”命令结束查找。



① 输入“exit”命令

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\wind>nslookup
Default Server: dns.w19.202.96.128.68
Address: 202.96.128.68

> 66.218.70.50
Server: dns.w19.202.96.128.68
Address: 202.96.128.68

Name: w19.www.sohu.com
Address: 66.218.70.50

> exit
C:\Documents and Settings\wind>
```

注意：并非所有的查找都会有结果，因为网络上有许多 IP 地址实际上并没有对应的域名，当域名服务器找不到对应的记录时，就会显示类似“dns.xxx can't find xxx: Non-existent domain”的错误信息。

① 域名服务器找不到
对应的记录

```
C:\WINDOWS\system32\cmd.exe - cmd - nslookup
C:\Documents and Settings\wind>nslookup
Default Server: dns.w19.202.96.128.68
Address: 202.96.128.68

> 202.94.128.68
Server: dns.w19.202.96.128.68
Address: 202.96.128.68

*** dns.w19.202.96.128.68 can't find 202.94.128.68: Non-existent domain
```

① 补充说明

检视 nslookup 命令的详细用法

nslookup 命令不仅可以通过 IP 地址反查 DNS 名称，而且还可以通过 DNS 名称查找 IP 地址。另外，这项命令还可以搭配多个参数执行，如需了解 nslookup 命令的详细使用方法，可以在输入“nslookup”命令后，再输入“help”命令来查找。

- ① 输入“nslookup”命令
② 输入“help”命令

```
C:\WINDOWS\system32\cmd.exe - cmd - nslookup
C:\Documents and Settings\wind>nslookup
Default Server: dns.w19.202.96.128.68
Address: 202.96.128.68

> help
Command: [?][{identifiers are shown in uppercase, [] means optional}]
NAME          - print info about the host/domain NAME via the default server
NAME1 NAME2    - an above, but use NAME2 as server
help or ?      - print info on common commands
set OPTION    - set an option
all           - print options, current server and host
noabbrev      - print debugging information
noexit        - print exhaustive debugging information
nosearch      - append domain name to each query
norecurse     - ask for recursive answer to query
noserver      - use domain search list
noverc        - always use a virtual circuit
domain=NAME   - set default domain name to NAME
archalist=N1,N2,.../N[...]  - set domain to N1 and search list to N1,N2, etc.
root=NAME     - set root server to NAME
retry=X       - set number of retries to X
timeout=X     - set initial time-out interval to X seconds
type=X        - set query type (i.e., A, ANY, CNAME, MX, NS, PTR, SOA, SRV)
querytype=X   - same as type
```

5.2 认识端口扫描程序

通过前面介绍的命令已经初步探知黑客的虚实，然而这些信息仍非常有限。为了获取更多的信息，为追踪黑客提供更有用的信息，还需要通过一些特殊的工具软件来扫描黑客。下面将要介绍这些工具软件，通过这类端口扫描程序，用户不仅可以获取更多的黑客信息，甚至还有可能先发制人，反制黑客。

5.2.1 什么是端口扫描程序

首先必须提醒读者注意的是，本文所要介绍的连接端口并非是 PS/2 之类的硬件装置连接端口，而是一种软件形式的概念。通常，服务器在实际使用时往往要同时担任多个不同的角色，例如某台服务器在提供 Web 服务的同时，也可以提供 FTP 服务，甚至还可以再提供其他的服务。服务器可以同时提供多项服务而不会互相冲突的一个重要原因就是服务器使用了不同的连接端口来提供服务，例如大多数服务器都会用 80 连接端口来提供 Web 服务，用 21 连接端口来提供 FTP 服务。也就是说，当用户要浏览服务器上的网站时，就通过 80 连接端口与服务器通信；当需要使用服务器的 FTP 服务时，就通过 21 连接端口与服务器通信。

当计算机打开某项服务时，其对应的连接端口就会处于打开状态，因此通过探测计算机打开了哪些连接端口，就可以知道计算机打开了哪些服务，这就是端口扫描程序的基本原理。

端口扫描程序的作用就是探测目标计算机的连接端口，锁定目标计算机后，它会向其发送各种试探性质的数据包，并根据目标计算机传回的信息判断对方打开了哪些服务。许多服务器在设计之初都因考虑不周而存在漏洞，如果用户未能及时安装更新补丁，这些漏洞就有可能成为入侵的目标。正常情况下，计算机打开的服务相当多，即使是系统管理员也未必清楚全部的服务，黑客当然也不例外，因此通过扫描黑客计算机打开的服务，将有可能获取黑客的更多信息，甚至可以找到反制黑客的机会。

早期的端口扫描程序功能非常简单，主要是扫描目标计算机打开了哪些连接端口。但随着技术的发展，扫描程序的功能也越来越强大，一些扫描程序加入了猜测密码的功能，如果对方的密码设置得过于简单，则有可能会被程序猜中。此外，还出现了一些专门针对系统漏洞的扫描程序，可以扫描系统是否存在特定的漏洞，一旦发现漏洞，就可以直接入侵目标计算机。虽然这类扫描程序黑客用得较多，但也有可能成为反制黑客的工具。

5.2.2 端口种类介绍

在正式开始介绍端口扫描程序之前，用户首先需要了解一些正规的连接端口，这些连接端口主要提供一些计算机常用，甚至是必备的服务。由于这类连接端口几乎是众所皆知的，因此存在的漏洞相对较少。但也有例外，例如一些用户打开了 FTP 服务，却没有设置足够复杂的密码，甚至根本不设置密码，就会成为黑客入侵的最佳入口。

正规的连接端口：



连 接 端 口	提 供 的 服 务
20	FTP (Data)
21	FTP (Control)
23	Telnet
25	SMTP
70	Gopher
79	Finger
80	HTTP
110	POP3

除了这些正规的连接端口外，木马程序也经常使用某些相对固定的连接端口。如果发现计算机中打开了这些可疑的连接端口，应首先怀疑计算机是否被木马程序入侵。

木马程序常使用的连接端口：

连 接 端 口	木 马 程 序
666	Satanz Backdoor
1001	Silencer
1999	BackDoor
2001	Trojan Cow
2140	The Invasor
2801	Phineas Phucker
3700	Portal of Doom
4590	ICQTrojan
5000	Sockets de Troie
5400	Blade Runner
9872	Portal of Doom
11223	Progenic trojan
12361	Whack-a-mole
22222	Prosiak
40421	Masters Paradise
40412	TheSpy
53001	Remote Windows Shutdown
65000	Devil

前面介绍的只是其中较为常见的连接端口及木马程序经常利用的连接端口，事实上计算机可用的连接端口远不止这些。如果用户想了解更多关于连接端口的信息，可参考相关的网络安全书籍。

5.2.3 常见的端口扫描程序

端口扫描程序的种类非常多，其功能也各不相同，有些只是单纯地扫描计算机打开了哪些连接端口，有些则具有猜测密码或利用漏洞入侵计算机的功能。下面将介绍几种较为

流行的端口扫描程序。

● Retina Network Security Scanner

Retina Network Security Scanner 是 Eeye 公司出品的网络安全扫描软件，是目前较为权威的网络安全扫描软件之一，可以有效地检测并修复各种安全隐患和漏洞，且会产生详细的安全检测报告。它可以兼容主流的操作系统、防火墙、路由器等各种网络装置。

软件小档案

软件名称：Retina Network Security Scanner

版本：V5.09 .682

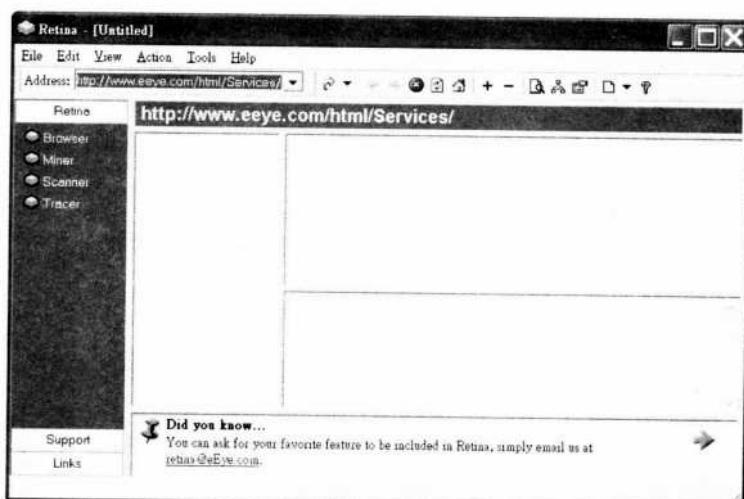
官方网站：<http://www.eeye.com/>

其他下载网址 1：<http://www.ttian.net/download/show.php?id=1675>

其他下载网址 2：<http://www.222pc.com/soft/12990.htm>

软件类型：收费软件

下图为 Retina Network Security Scanner 的主界面。



● Shadow Security Scanner

Shadow Security Scanner 是俄罗斯出品的专业网络安全扫描软件，其功能与前面介绍的 Retina Network Security Scanner 相比毫不逊色，同样是目前最权威的网络安全扫描软件之一。

软件小档案

软件名称：Shadow Security Scanner

版本：V6.9.51

官方网站：<http://www.safety-lab.com/en/index.htm>

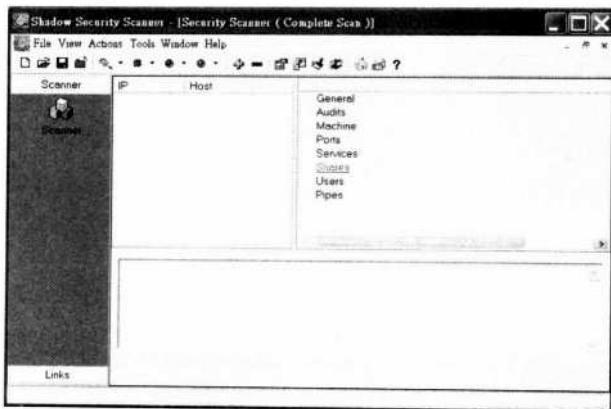
其他下载网址 1：<http://www.tttx.com/Down/html/120/241/2004/200408153617.html>

其他下载网址 2：<http://www.222pc.com/soft/1973.htm>

软件类型：免费软件



下图为 Shadow Security Scanner 的主界面。



● SuperScan

SuperScan 的功能不及前两套软件全面，但就连接端口扫描而言，SuperScan 无论在扫描的效率还是在准确度方面都不错。

软件小档案

软件名称：SuperScan

版本：V4.0

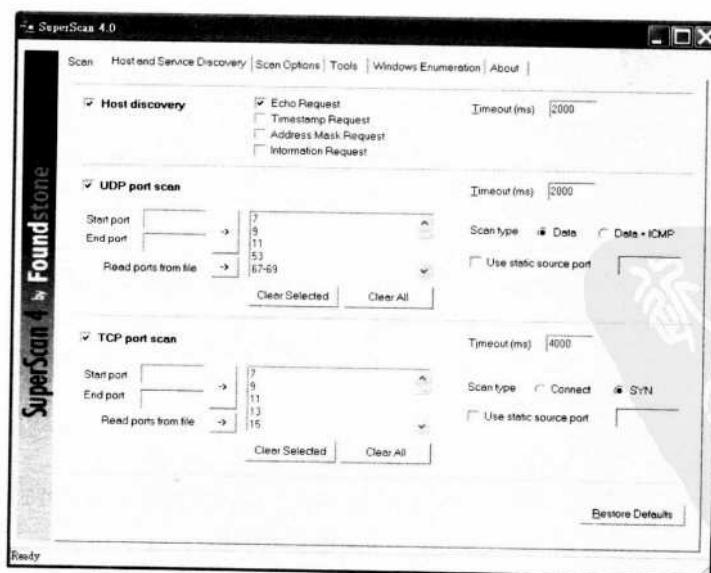
官方网站：<http://www.foundstone.com>

其他下载网址 1：<http://3800cc.com/Soft/smgl/9405.html>

其他下载网址 2：<http://www.wolail.com/Soft/wlrj/yckz/200507/709.asp>

软件类型：免费软件

下图为 SuperScan 4.0 的主界面。



● X-Scan

X-Scan 是一套与 SuperScan 类似的扫描工具，它除了具有较完善的连接端口扫描功能外，还提供了专门的漏洞扫描功能，可以有针对性地扫描目标计算机存在的漏洞。

X-Scan 本身是一个在命令提示符模式下执行的软件，但同时也提供了可在窗口环境下执行的图形用户界面版本，用户可根据实际需求选用合适的版本。

软件小档案

软件名称：X-Scan

版本：V3.1

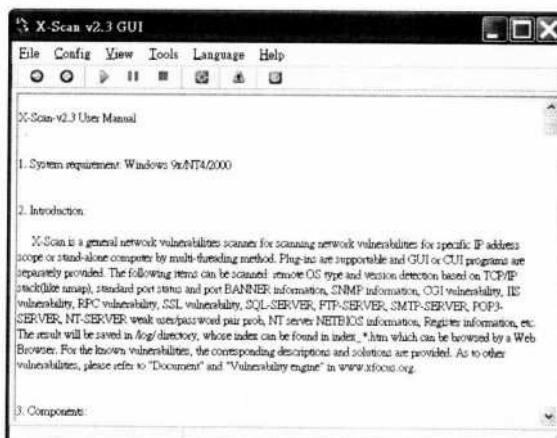
官方网站：未知

其他下载网址 1：<http://www.pc173.com/soft/3196.htm>

其他下载网址 2：<http://www.super-down.net/Soft/html/35/121/2005/943.html>

软件类型：免费软件

下图为 X-Scan 的主界面。



● StealthWasp's Basic PortScanner

StealthWasp's Basic PortScanner 是一个非常简单易用的端口扫描程序，用户只要填入目标计算机的 IP 地址及要扫描的连接端口范围即可开始扫描，但 Stealth Wasp's Basic PortScanner 不具备分析漏洞的功能，用户需要通过自己的知识或其他的软件来分析扫描结果。

软件小档案

软件名称：StealthWasp's Basic Port Scanner

版本：V1.2

官方网站：黑客个人作品，无官方网站，联系邮箱 StealthWasp@hotmail.com。

其他下载网址 1：<http://www.tian.net/download/show.php?id=895>

其他下载网址 2：<http://www.heibai.net/down/show.php?id=3885>

软件类型：免费软件

下图为 StealthWasp's Basic Port Scanner 的主界面。



5.3 端口扫描程序实战

经过前面的介绍，相信大家对端口扫描程序已经有了大概的了解，下面将以其中较流行的几套软件为例，以实例的方式介绍如何扫描黑客计算机的漏洞。需要提醒读者注意的是，扫描黑客计算机的目的只是为了获取更多的信息以追踪黑客，千万不要将本文所介绍的方法用于攻击其他用户的计算机，否则将会触犯法律。

5.3.1 Retina Network Security Scanner

Retina Network Security Scanner 虽然是很专业的网络安全扫描软件，但其使用方法并非十分复杂，用户只要经过简单的学习，很容易就能掌握。下面就以这套软件为例，介绍如何扫描黑客的计算机。

Retina Network Security Scanner 虽然是商业软件，但用户仍可从 Eeye 公司的官方网站下载软件的体验版本。

软件小档案

软件名称：Retina Network Security Scanner

版本：V5.09 .682

官方网站：<http://www.eeye.com/>

其他下载网址 1：<http://www.ttian.net/download/show.php?id=1675>

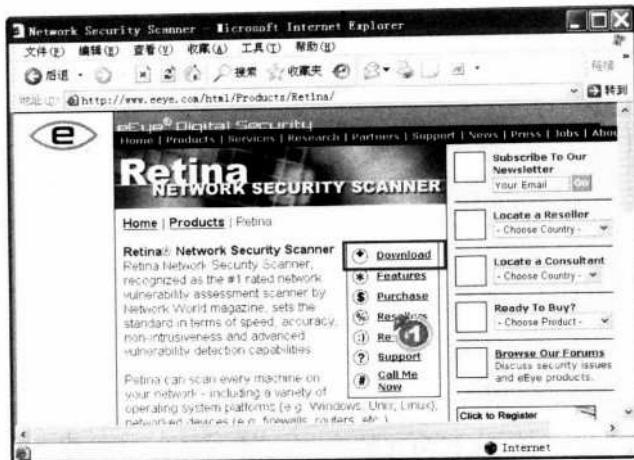
其他下载网址 2：<http://www.222pc.com/soft/12990.htm>

软件类型：收费软件

下图为下载 Retina Network Security Scanner 的官方网站界面。

● 安装 Retina Network Security Scanner

Retina Network Security Scanner 的安装过程并不复杂，用户只需执行安装程序，并按照向导的提示即可完成安装。

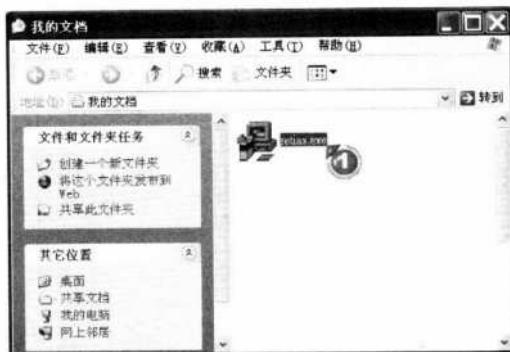


① 单击此超级链接即可立即下载

STEP1 执行安装程序

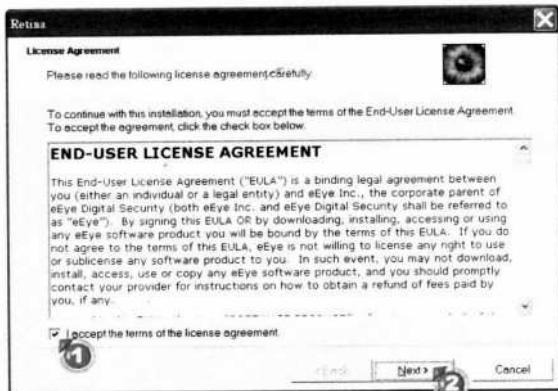
下载完毕后，双击安装程序即可启动向导开始安装。

① 双击安装程序



STEP2 接受授权协议

安装向导启动后，会出现程序授权协议对话框，用户必须接受授权协议，否则无法继续安装。

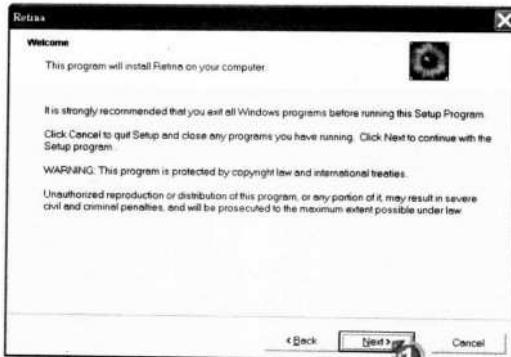


① 选择 accept...复选框
② 单击【Next】按钮

STEP3 跳过欢迎界面

在欢迎界面中，安装向导要求用户结束其他程序，以确保安装顺利进行，单击【Next】按钮后继续安装。

① 单击【Next】按钮



STEP4 选择安装路径

程序默认安装在系统分区的 Program Files 文件夹中，也可通过【Browse】按钮改变安装路径，设置完毕后单击【Next】按钮继续安装。

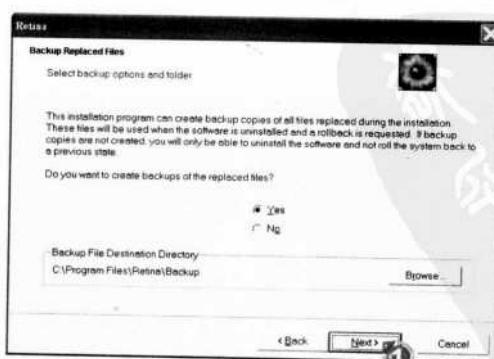


① 单击【Next】按钮

STEP5 建立备份文件夹

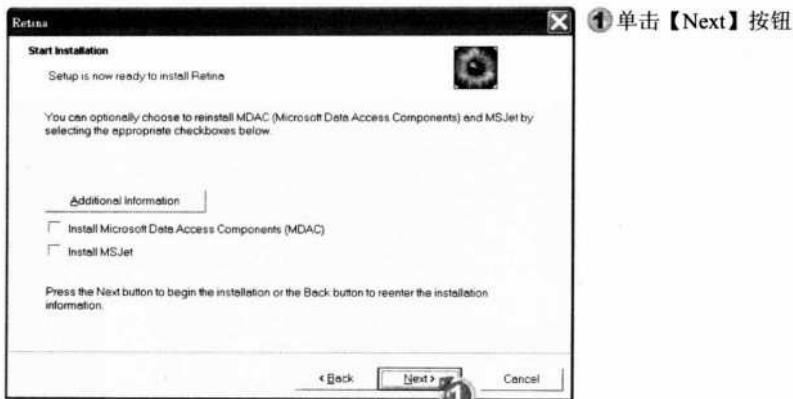
安装向导提示需要建立一个 Backup 文件夹，建议采用默认值，单击【Next】按钮继续安装。

① 单击【Next】按钮



STEP6 设置是否安装 MDAC 与 MSJet

如果需要安装 MDAC 或 MSJet，则需选择对应的复选框，否则直接单击【Next】按钮即可。

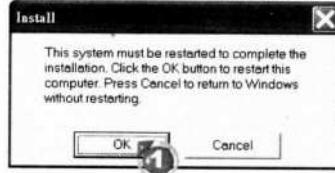
**STEP7** 结束安装

安装所需的时间较长，需耐心等待，安装完成后，单击【Finish】按钮。

① 单击【Finish】按钮

**STEP8** 重新启动计算机

安装完成后，需要重新启动计算机，单击【OK】按钮后，计算机将自动重新启动。



● 扫描黑客计算机

安装完成后，就可以通过 Retina Network Security Scanner 程序来扫描黑客计算机。注

意：扫描需要占用大量的网络带宽及系统资源，因此在执行扫描的过程中，不要执行其他的操作，否则可能会导致系统死机。

STEP1 执行 Retina Network Security Scanner 程序

安装完成后，将会在【开始】菜单中建立程序的快捷方式，以便快速启动程序。

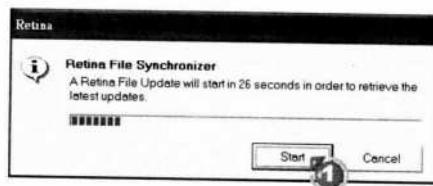


- ① 依次选择【开始】→【所有程序】→【Retina】→【Retina】命令

STEP2 执行更新

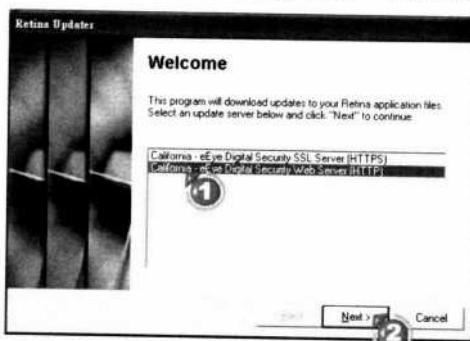
在启动过程中，程序会自动连接到服务器搜索更新文件，如果需要更新程序，可单击【Start】按钮，否则单击【Cancel】按钮取消更新。

- ① 单击【Start】按钮执行更新功能



STEP3 选择更新服务器

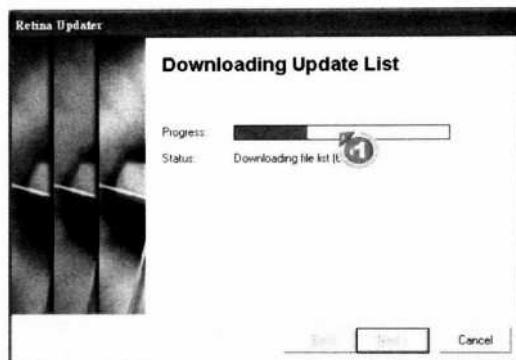
在更新服务器列表中选择任意一个服务器，然后单击【Next】按钮。



- ① 选择更新服务器
② 单击【Next】按钮

STEP 4 下载更新文件

选择服务器后，程序会自动从服务器下载需要更新的文件列表并自动安装，下载过程中界面上会显示下载的进度。



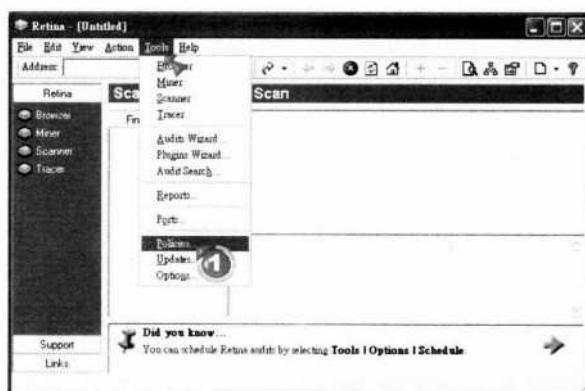
① 下载更新程序的进度

STEP 5 打开【Policies】窗口

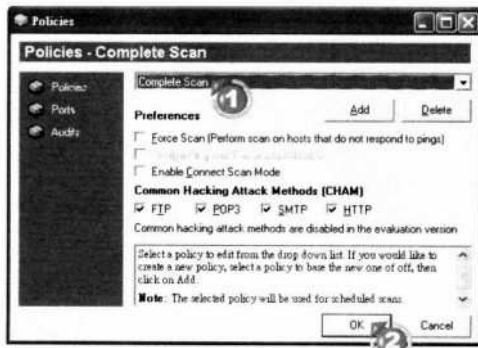
Retina Network Security Scanner 提供了多种默认的扫描策略，用户可以在【Policies】窗口中直接套用这些扫描策略，而无须手动设置每一个扫描选项。

① 选择【Tools】→【Policies】

命令打开【Policies】窗口

**STEP 6** 设置扫描策略

为了获取更全面的信息，建议设置扫描策略为【Complete Scan】，即全面扫描。



① 在下拉菜单中选择

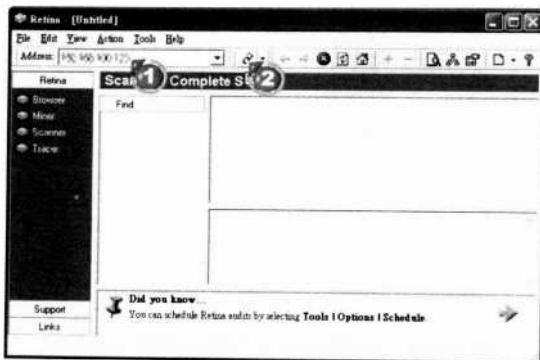
【Complete Scan】选项

② 单击【OK】按钮



STEP 7 开始扫描

将目标计算机的 IP 输入到【Address】栏中，然后单击【Scan】按钮开始扫描。

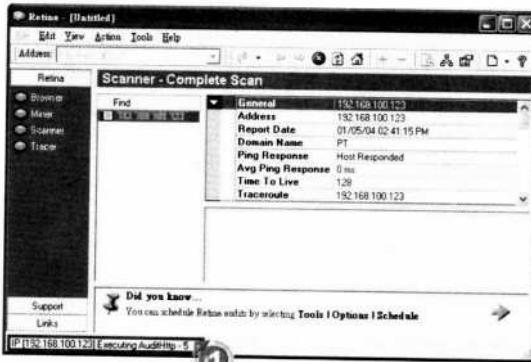


- ①输入目标计算机的IP
②单击【Scan】按钮开始扫描

STEP 8 检视扫描选项

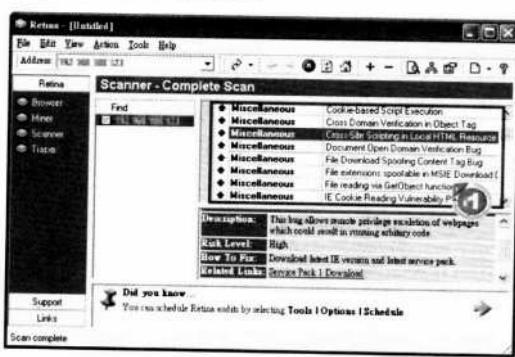
扫描所需的时间较长，需耐心等候，扫描过程中界面下方会显示目前正在扫描的选项。

①正在扫描的选项



STEP 9 检视扫描结果-高度危险的漏洞

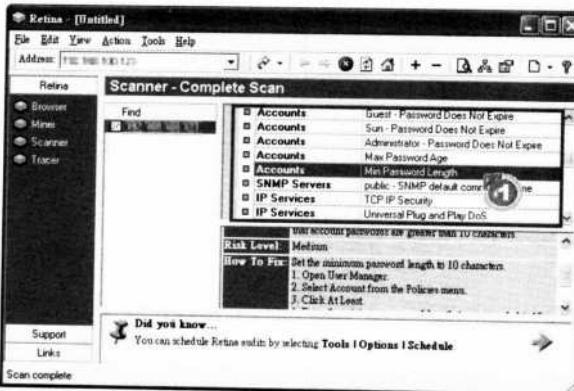
黑客计算机也并非无懈可击，扫描结束后，程序会自动对漏洞的危险性进行评估，标有“•”图标的选项为具有高度危险的漏洞。对于高度危险的漏洞，程序会提供更新补丁的下载链接。



- ①高度危险的漏洞

STEP10 检视扫描结果-中度危险的漏洞

标有“●”图标的选项表示中度危险的漏洞，这类漏洞同样有可能导致计算机被入侵。对于中度危险的漏洞，程序会提出如何修复此漏洞的建议。

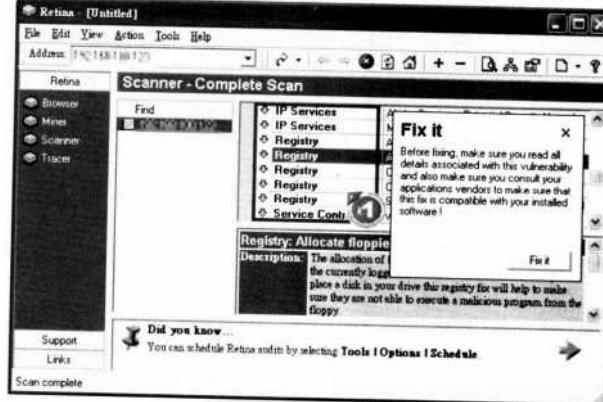


① 中度危险的漏洞

STEP11 检视扫描结果-低度危险的漏洞

标有“○”图标的选项表示低度危险的漏洞，通过这类漏洞入侵的可能性极小，对于此类漏洞，Retina Network Security Scanner 程序提供了修复功能。

① 低度危险的漏洞



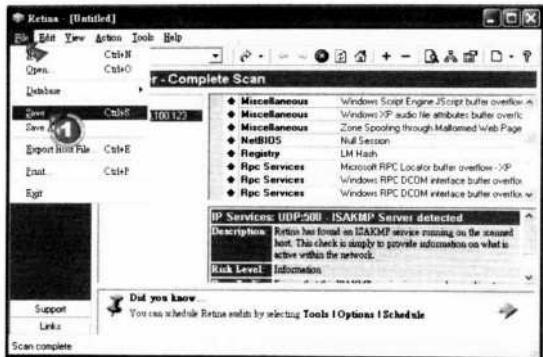
经过扫描后，用户即可掌握黑客计算机的详细信息，这些信息对于反追踪黑客非常有价值。

● 保存扫描结果

由于扫描的结果非常详细，因此用户可将其保存下来仔细分析，此时可以通过程序提供的保存功能将扫描结果保存起来。

STEP1 执行保存功能

选择【File】→【Save】命令或按【Ctrl+S】组合键，打开【Save AS】对话框，以保存扫描结果。

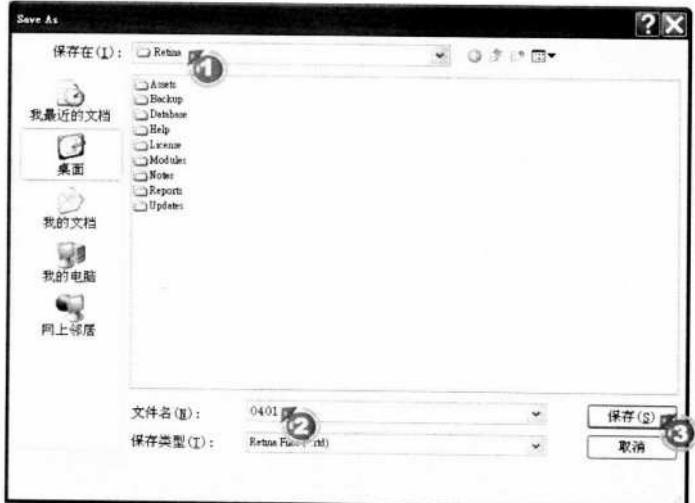


- ① 依次选择【File】→【Save】命令

STEP2 设置保存路径及名称

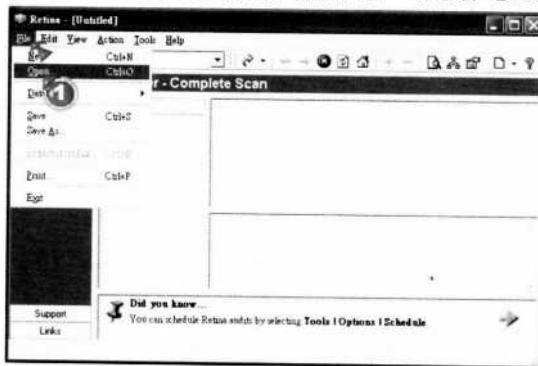
设置扫描结果的保存路径及文件名称，设置完毕后单击【保存】按钮即可保存扫描结果。

- ① 设置保存路径
② 输入文件名称
③ 单击【保存】按钮



STEP3 打开文件

如果要检视刚才保存的扫描结果，可选择【File】→【Open】命令。



- ① 依次选择【File】→【Open】命令

STEP4 选择要检视的文件

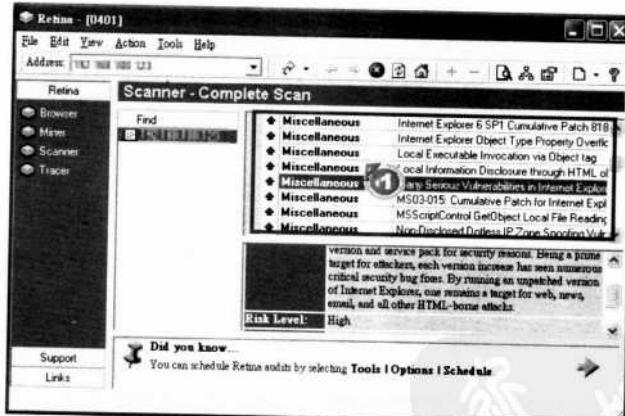
在【Open】对话框中打开扫描结果所在的文件夹，选择要打开的文件后单击【打开】按钮。



- ① 选择扫描结果所在
的文件夹
- ② 选择文件
- ③ 单击【打开】按钮

STEP5 检视扫描结果

打开文件后，即可在 Retina Network Security Scanner 程序主窗口中检视扫描结果。

① 扫描结果

5.4 反查黑客所属区域

通过前面的步骤，我们已经获取了黑客的详细信息，但仍未查出黑客所属的区域，下面就介绍一下反查黑客所属区域的方法。

反查黑客所属区域需要用到一套名为 VisualRoute 的软件，它可以图形方式显示数据包的路由，并在世界地图上显示出目标 IP 地址对应的位置。

此软件的官方网址为 <http://secure.visualware.com/crm/go/getjava-win-us>。



VisualRoute 的使用方法非常简单，用户只要输入目标计算机的 IP 地址（URL、E-Mail 等也可以）并按下【Enter】键，程序就会自动获取路由信息并显示在程序中央的世界地图中。但该程序的安装比较麻烦，因为 VisualRoute 是基于 Java 程序语言编写的，因此用户首先需要先安装 Java 虚拟机，否则将无法安装 VisualRoute。Java 虚拟机可以在 Sun 的官方网站下载。

软件小档案

软件名称：Java 虚拟机

版本：X86

官方网站：<http://cn.sun.com>

其它下载网址 1：http://www.java.com/zh_CN/download/manual.jsp

其它下载网址 2：<http://www.cncatholic.org/Soft/film/200508/456.html>

软件类型：免费软件

● 安装 Java 虚拟机

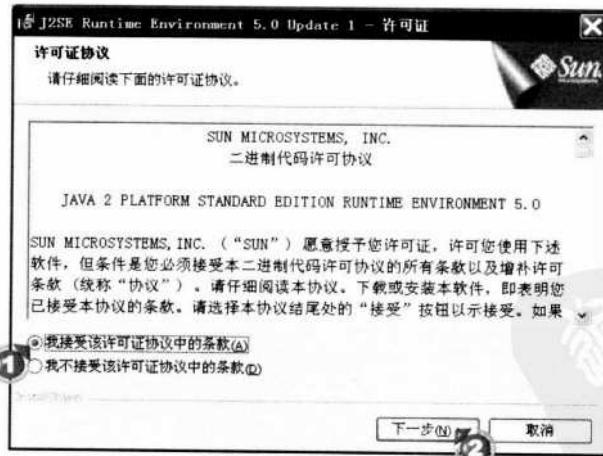
安装 Java 虚拟机并不复杂，执行安装程序后只需按照向导的提示操作即可完成，但一些用户在安装时可能会遇到无法安装的问题，这是因为不同语言版本的操作系统所用的虚拟机不同，此时用户应重新下载与所用操作系统相对应的虚拟机。

STEP① 接受许可证协议

启动安装向导后，首先出现的是程序的许可证协议，用户必须接受才能继续安装。

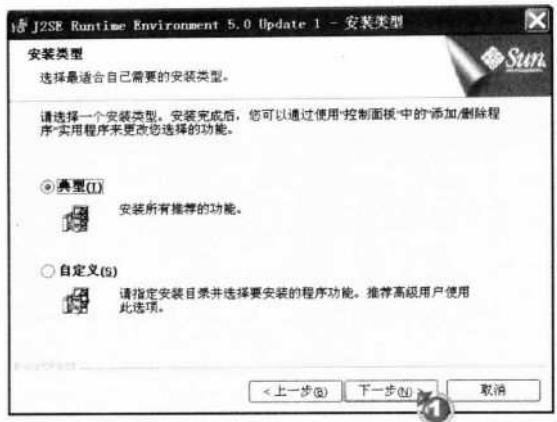
①选择“我接受该许可证协议中的条款”单选框

②单击【下一步】按钮



STEP② 设置安装类型

安装向导提供了两种安装类型供用户选择，保持默认设置即可。



① 单击【下一步】按钮

安装完成后，【开始】菜单中会出现【Java Web Start】的快捷方式，此时 Java 虚拟机已经安装完毕。

① 【开始】菜单中的【Java Web Start】快捷方式



● 安装及使用 VisualRoute

安装 Java 虚拟机后，就可以开始安装 VisualRoute 程序，双击 VisualRoute 安装文件即可启动安装向导。在安装 VisualRoute 时，要先关闭其他程序，以确保安装可以顺利完成。

软件小档案

软件名称：VisualRoute

版本：2006 10.0c

官方网站：<http://download.visualware.com>

其他下载网址 1：<http://www.skycn.com/soft/4003.html>

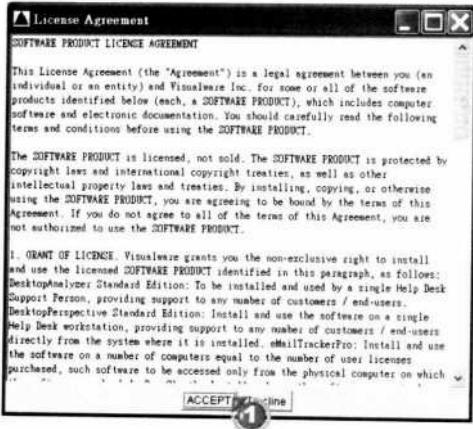
其他下载网址 2：<http://download.enet.com.cn/html/010142001101102.html>

软件类型：共享软件



STEP1 接受授权协议

启动安装向导后，首先出现的是程序的授权协议，用户同样必须接受此协议才能继续安装。

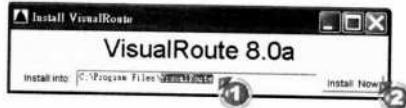


- ① 单击【ACCEPT】按钮，接受授权协议

STEP2 设置安装路径

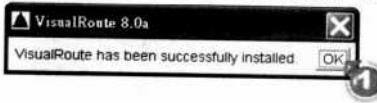
默认状态下，安装向导会将程序安装在系统分区的 Program Files 文件夹中，用户也可以自定义安装路径。

- ① 设置安装路径
- ② 单击【Install Now】按钮



STEP3 结束安装向导

安装完毕后，单击【OK】按钮，结束安装向导。



- ① 单击【OK】按钮

STEP4 执行 VisualRoute 程序

由于安装向导未在桌面及【开始】菜单增加启动程序的快捷方式，因此需要进入程序所在文件夹执行程序。

- ① 打开程序所在的文件夹
- ② 双击【VisualRoute.exe】图标



STEP5 选择语言

VisualRoute 程序支持多种语言，用户可根据自己的需求选择。由于程序未提供中文支持，因此建议选择【English [en]】选项。

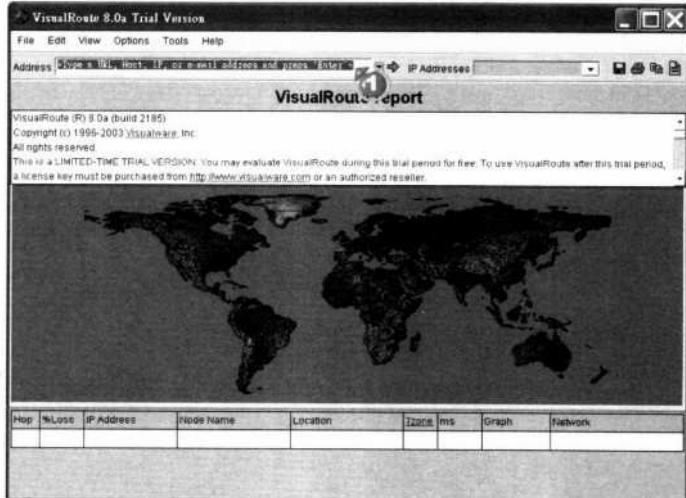


- ① 选择【English [en]】选项
② 单击【OK】按钮

STEP6 反查黑客所属区域

在【Address】栏中输入黑客的 IP 地址后，按【Enter】键即可查找黑客所属的区域。

- ① 输入黑客的 IP 地址
并按下【Enter】键



稍等片刻，程序就会把黑客所在的区域及黑客计算机与这台计算机之间的路由呈现在程序主窗口的世界地图上。

最后，要再次提醒读者，本章所介绍的内容仅可用于获取黑客计算机信息，切不可用于进行不法行为，否则将会追究法律责任。

Chapter 6

防御黑客程序



在前面几章已经了解了计算机病毒、按键记录及木马程序等攻击方法，事实上黑客的攻击方法还不止这些。本章将会分别讲解一些前面未提到的黑客攻击方法及对应的防御方式。下面将要介绍的这些黑客攻击方法，大部分都可以通过前面提到的软件来防御。

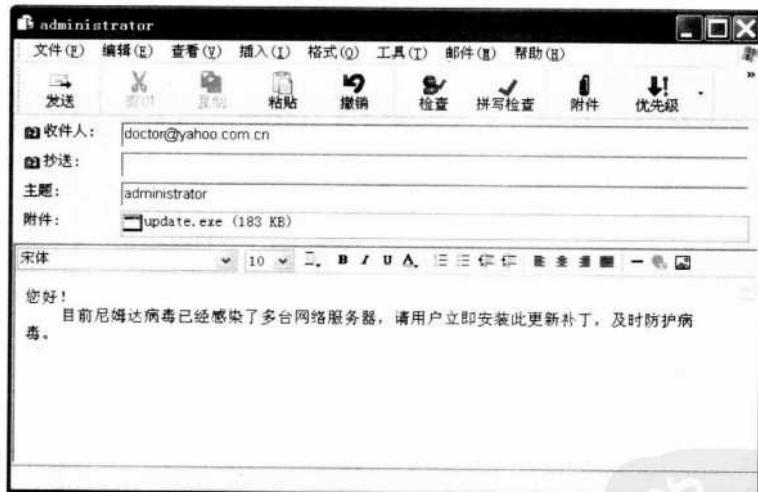
6.1 常见的黑客攻击程序

除了前面几章所介绍的木马、按键记录等攻击方法外，黑客最常用的攻击方式还有通过电子邮件的附件攻击与通过数据包攻击两种。此外，也有一些黑客会攻击 MSN、QQ 之类的聊天软件。

6.1.1 电子邮件附件攻击

通过电子邮件附件攻击是黑客最常用的攻击方法之一。黑客将木马程序或按键记录软件等恶意的程序作为附件附在电子邮件中寄给对方，一旦对方执行了这个文件，计算机就会被黑客入侵。

为了欺骗用户打开附件，黑客通常还会为邮件作各种伪装，如伪装成系统管理员的邮件等。此外，还有一些邮件利用 Outlook 软件的漏洞，让用户在预览邮件时就自动执行附件。

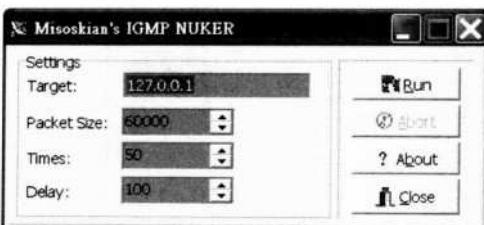


6.1.2 DoS 攻击

DoS 攻击，简单地说就是指通过向目标计算机发送特殊的数据包，导致对方死机或者无法响应正常的服务请求。例如，利用网络协议的漏洞，使局域网内充满垃圾数据包，导致网络无法正常工作，就属于一种 DoS 攻击。

DoS 攻击一般不会直接攻击个人计算机，主要攻击目标为服务器计算机，但这类攻击对个人计算机用户的影响非常大，一旦服务器计算机遭到攻击而不能正常提供服务时，个人计算机用户收发邮件、浏览网页等都会直接受到影响。下图为数据包攻击软件

的界面。



什么是 DoS 攻击？

这里所说的 DoS 并非是指 DOS 操作系统，而是 Denial of Service 的简称，中文译为【拒绝服务】。顾名思义，DoS 攻击的目的就是导致服务器计算机不能响应用户的请求，即拒绝服务，这是目前较流行的黑客攻击方法之一，较经典的 DoS 攻击有【死亡之 Ping】(Ping of Death)、【SYN Flood】、【Smurf】等。用户如需了解 DoS 攻击的原理，可参考相关的网络安全书籍。

6.1.3 聊天软件攻击

电子邮件上附件之类的攻击方法已经广泛流传，对于可疑的邮件，大部分用户都会选择删除，因此黑客开始将注意力转移到其他方面，通过聊天软件攻击就是其中的一种方法。通过聊天软件的攻击方法主要有以下 3 种：

● 通过聊天软件的漏洞攻击

一些聊天软件在撰写程序代码时，也有可能因考虑不周而出现一些可以被黑客利用的漏洞，但相对于操作系统等软件，聊天软件的结构无疑简单得多，因此聊天软件的漏洞也较少见。到目前为止，通过聊天软件漏洞的攻击极为少见，唯一较出名的是某位黑客撰写的针对 QQ 的程序代码，用户只要将这段程序代码通过 QQ 发送给其他用户，对方的 QQ 就会自动关闭。

虽然目前这类攻击仍较少见，但随时都有可能会有新的漏洞被发现，因此用户千万不能掉以轻心。

● 通过文件传输攻击

大部分聊天软件都具有传送文件的功能，以便用户共享资源，因此一些黑客就会利用这项功能将木马程序及病毒传递给对方，以达到攻击的目的。

为了欺骗对方执行木马程序，黑客通常会将其伪装成图片、音乐或者是 Flash 等看起来无害的文件，一旦对方执行了这些文件，就会被黑客入侵。



① 通过聊天软件传送伪装成图片的木马程序

● 结合网页病毒攻击

结合网页病毒进行攻击是一种新出现的攻击方法，目前这类攻击方法主要针对流行的QQ即时通信软件，而在MSN、ICQ上则较少见。以经典的【爱情森林】病毒为例，计算机感染病毒后，当用户用QQ与他人交谈时，【爱情森林】病毒就会自动在对话后面加上一个网页的超级链接，一旦对方单击这个超级链接，就会打开一个带有病毒的网页，而且这个网页利用了Internet Explorer浏览器的一个漏洞，可以使计算机病毒自动下载并执行，且不会向用户发出任何提示。

6.2 防御电子邮件附件攻击

为了防御电子邮件附件攻击，最直接的方法就是不执行任何电子邮件附件，但是在平常的使用过程中用户往往很难做到这一点。因此，用户可通过杀毒软件来查看电子邮件附件是否包含恶意的程序。目前，大部分杀毒软件都包含防御电子邮件附件攻击的功能，下面将以前面介绍过的PC-cillin 2005为例，介绍如何防御电子邮件附件的攻击。

软件小档案

软件名称：PC-cillin 2005

版本：2005网络安全版

官方网站：<http://www.trendmicro.com/>

其他下载网址：<http://www.onlinedown.net/soft/2991.htm>

软件类型：共享试用

STEP1 打开PC-cillin窗口

安装PC-cillin 2005后，程序会随计算机的启动而自动执行，用户只需双击系统任务栏上的PC-cillin2005图标即可打开程序主窗口。



① 双击系统任务栏上的
PC-cillin 2005 图标

STEP2 进入到邮件扫描窗口

在程序主窗口中依次选择【电子邮件】→【邮件扫描】选项，进入【邮件扫描】窗口。

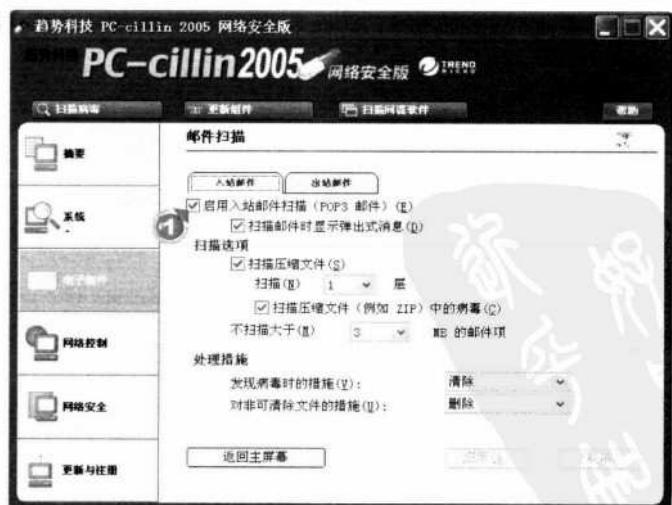


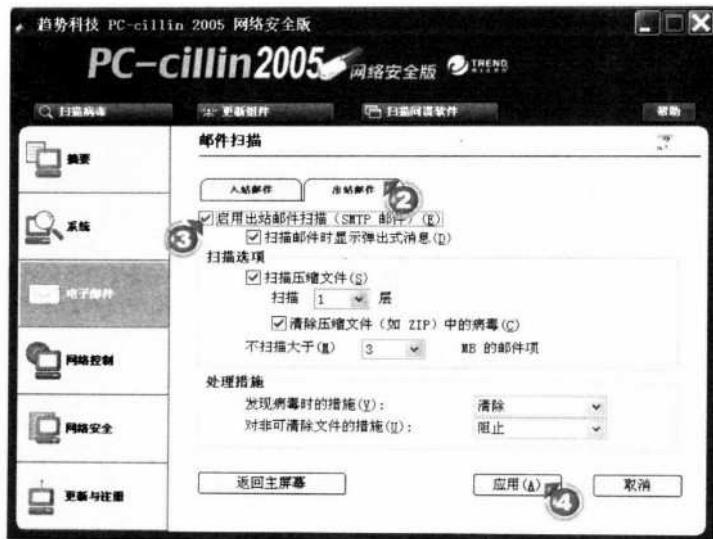
① 依次选择【电子邮件】
→【邮件扫描】选项

STEP3 设置邮件扫描

PC-cillin 2005 提供了【入站邮件】和【出站邮件】扫描功能，默认情况下这些功能未被启用，建议用户启用这些设置以便使 PC-cillin 2005 能够对发送的邮件和接收的邮件进行及时扫描。启用这些功能后，其他的设置保持默认状态即可。

① 选择【启用入站邮件
扫描】复选框





② 单击【出站邮件】

选项卡

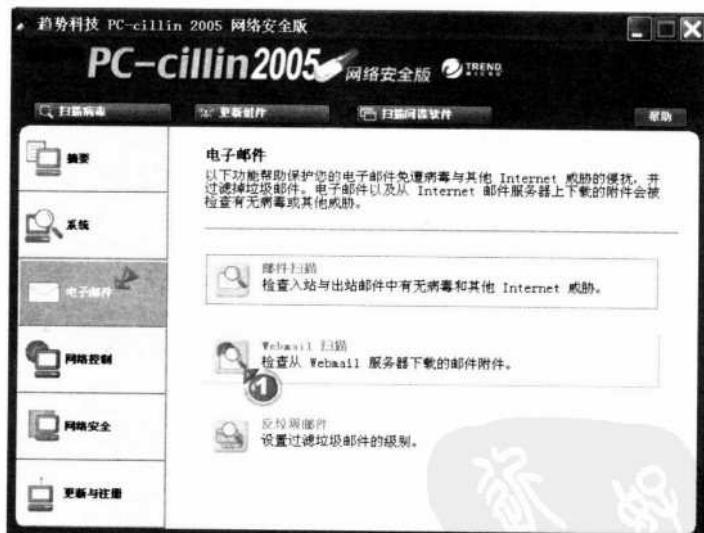
③ 选择【启用出站邮件扫描】复选框

④ 单击【应用】按钮

STEP 4 进入 Webmail 扫描窗口

PC-cillin 2005 提供了针对 Webmail 扫描的功能，通过此功能，用户可打开来自 Webmail 的邮件，PC-cillin 2005 将会自动扫描这些邮件。

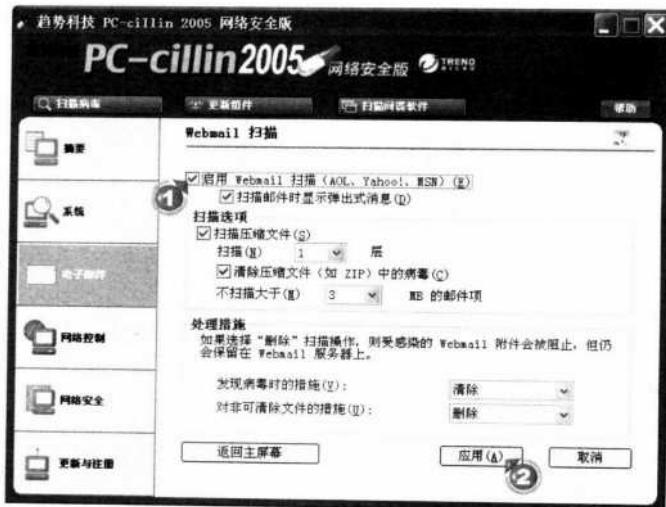
① 依次选择【电子邮件】
→【Webmail 扫描】选
项



STEP 5 设置 Webmail 扫描

默认情况下 Webmail 扫描功能没有启用，因此无法对 Webmail 进行扫描，建议用户启用这项功能，启用这项功能后下面的其他设置保持默认状态即可。

- ① 选择【启用 Webmail 扫描】复选框
- ② 单击【应用】按钮



经过上述设置后，用户收取邮件时，PC-cillin 2005 会首先扫描邮件的附件，一旦发现病毒就会按照用户的设置进行处理。

6.3 防御 DoS 攻击

对于针对 Windows 9x 操作系统的 DoS 攻击，用户只需安装新版本的操作系统（如 Windows XP）即可防御这类攻击，因为新版本的操作系统已经修复了这些漏洞。

DoS 攻击主要是通过 TCP/IP 协议中的 ICMP 子协议来完成的，ICMP 协议一般用于测试网络通信以及在网络间传输一些控制信息，由于该协议的应答过程是自动完成的，因此为了防御这类攻击，用户可以使用防火墙软件拦截所有 ICMP 数据包，这样就可以避免被黑客攻击而导致死机。



服务器设备怎样防御 DoS 攻击？

前面所说的防御方式只对个人计算机用户而言，因为如果被攻击的是服务器，即使没有死机，也会因为网络带宽被大量占用而使其他用户无法访问，从而让 DoS 攻击仍然有效。因此，对于服务器而言，防止 DoS 攻击的最佳方法是请 ISP 协助拦截 ICMP 数据包。

● 用 Windows XP 自带防火墙防御 DoS 攻击

目前，大部分防火墙软件都有拦截 ICMP 数据包的功能，用户只需简单的几个步骤即可进行设置。即使没有安装防火墙软件也没有关系，因为 Windows XP 自带的防火墙也有类似的功能。下面将以 Windows XP 自带防火墙为例，介绍如何防御 DoS 攻击。

STEP 1 打开【本地连接 状态】对话框

Windows XP 的自带防火墙是针对单个连接的，因此需要为每个连接打开防火墙。



双击系统任务栏上的【本地连接】图标可快速打开【本地连接 状态】对话框。

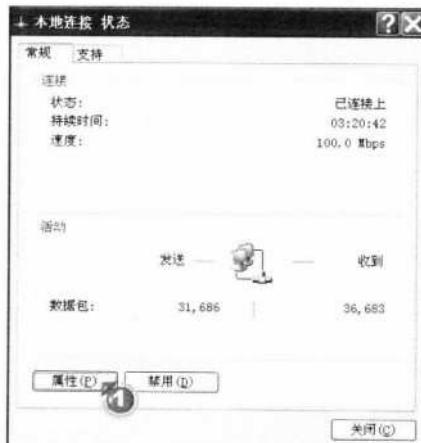


- ① 双击【本地连接】图标，
打开【本地连接状态】
对话框

STEP2 打开【本地连接 属性】对话框

在【本地连接 状态】对话框中，可以查看到当前网络连接的状态，如连接状态、持续时间、速度、发送和收到的数据包数量等，单击【属性】按钮可打开【本地连接 属性】对话框。

- ① 单击【属性】按钮



STEP3 打开 Windows XP 自带防火墙

如果防火墙尚未启动，则需在【高级】选项卡中打开【Windows XP 防火墙】对话框。



- ① 选择【高级】选项卡
- ② 单击【设置】按钮

STEP 4 设置拦截 ICMP 数据包

在【高级】选项卡的【ICMP】栏中单击【设置】按钮，打开【ICMP 设置】对话框，并设置拦截哪些 ICMP 数据包。



经过上述设置后，Windows XP 自带的防火墙将会拦截所有的 ICMP 数据包。由于 ICMP 数据包主要用于传送控制信息及测试网络通信，因此拦截 ICMP 数据包不会影响浏览网页、连接 FTP 等应用，但是部分用于检测网络的指令将无法使用，如 Ping、Tracert 等，如果需要使用这些指令，应暂时关闭防火墙。

以防火墙软件防御 DoS 攻击

除了使用 Windows XP 自带的防火墙外，用户也可通过专业的防火墙软件来拦截 ICMP 数据包，下面将以 Norton Internet Security 2004 为例进行介绍，其他防火墙软件的具体设置步骤可参考防火墙软件的说明文件。

软件小档案

软件名称：Norton Internet Security 2004（诺顿网络安全特警 2004）
版本：2004 版本



官方网站: <http://www.symantec.com>

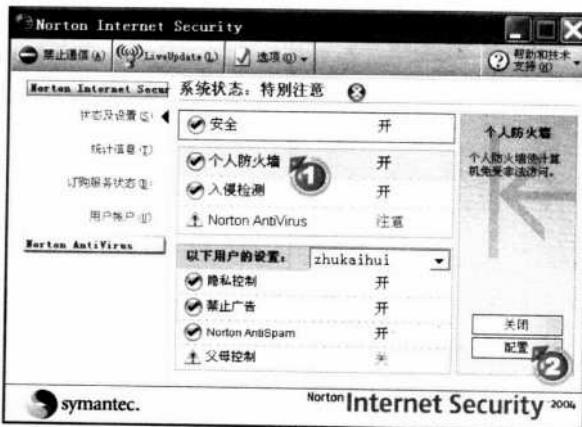
其他下载网址 1: <http://www.norton.com/region/cn/>

其他下载网址 2: <http://www.onlinedown.net/soft/24268.htm>

软件类型: 试用软件

STEP 1 打开个人防火墙配置窗口

在 Norton Internet Security 2004 程序主窗口中单击【个人防火墙】选项，然后单击【配置】按钮，打开个人防火墙配置窗口。

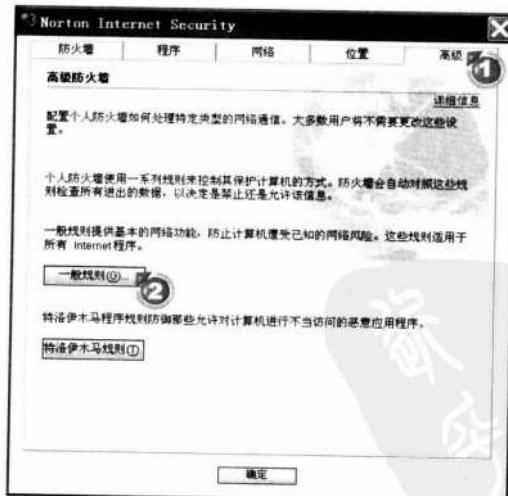


① 单击【个人防火墙】选项

② 单击【配置】按钮

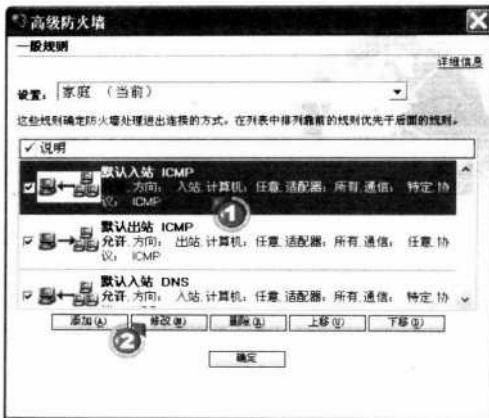
STEP 2 打开【高级防火墙】对话框

选择【高级】选项卡，单击【一般规则】按钮，打开【一般规则】对话框，设置防火墙拦截 ICMP 数据包的规则。



STEP 3 修改【默认入站 ICMP】规则

选择要修改的规则，然后单击【修改】按钮打开【修改规则】对话框，以便禁止不匹配该规则的连接。

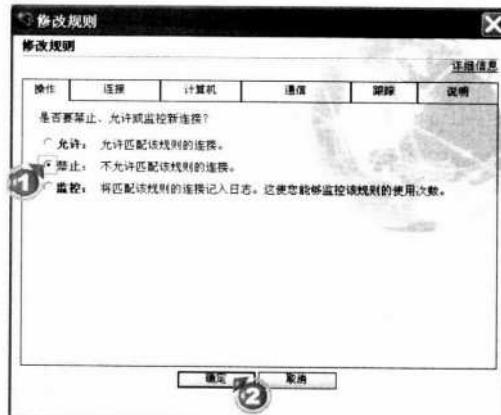


- ① 选择【默认入站 ICMP】
规则
② 单击【修改】按钮

STEP4 设置禁止不允许匹配该规则的连接

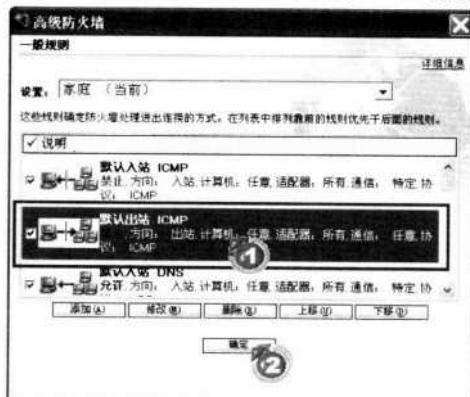
选择【禁止】单选框，禁止不允许匹配该规则的连接，然后单击【确定】按钮。

- ① 选择【禁止】单选框
② 单击【确定】按钮



STEP5 修改【默认出站 ICMP】规则

以相同的方法，设置禁止出站的 ICMP 数据包，设置完毕后单击【确定】按钮。

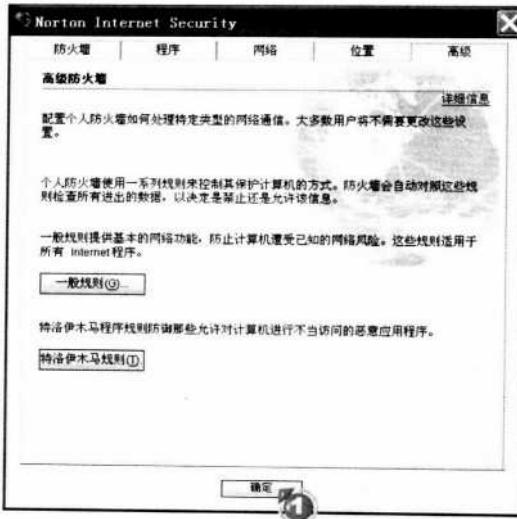


- ① 禁止默认出站 ICMP
数据包
② 单击【确定】按钮

**STEP 6** 完成设置

设置完毕后，单击【确定】按钮，返回 Norton Internet Security 2004 程序主窗口。

① 单击【确定】按钮



经过上述设置后，Norton Internet Security 2004 就会拦截所有入站及出站的 ICMP 数据包，但此时用户也无法使用 Ping 等需要使用 ICMP 协议的网络命令。如果用户需要使用此类功能，只需暂时关闭防火墙软件即可。

6.4 防御来自聊天软件的攻击

大部分聊天软件都提供了文件传输的功能，而这项功能的确也方便了许多用户，但同时也为黑客入侵提供了通道。因此，为了防御这种攻击，用户不应随意接受其他人传送过来的文件。

事实上，大部分有安全意识的用户一般都不会随意打开陌生人传送的文件，但对于朋友传送过来的文件则警觉性不高，不少用户就是这样被入侵的。因为有时连传送文件的人自己也不知道这个文件包含了恶意程序，甚至有时这个用户已经被黑客入侵并冒充。

● 设置聊天软件自动扫描传输的文件

为了防止这类攻击，大部分聊天软件都可与杀毒软件结合使用，下面就以目前流行的聊天软件 MSN 为例，介绍如何设置自动扫描传送的文件。在使用这项功能时，要先确认计算机已经安装了杀毒软件。

STEP 1 打开【选项】对话框

在 MSN 程序主窗口中，选择【工具】→【选项】命令打开【选项】对话框，以便打开 MSN 自动扫描文件功能。



①依次选择【工具-选项】命令

STEP2 设置自动扫描病毒功能

在【文件传输】栏中，选择【使用下列程序扫文件中的病毒】复选框，并通过【浏览】按钮选择杀毒软件。

- ① 选择【文件传输】选项
- ② 选择【使用下列程序扫描文件中的病毒】复选框
- ③ 单击【浏览】按钮



STEP3 选择杀毒软件

打开杀毒软件所在的文件夹，选择要执行病毒扫描的杀毒软件，然后将其打开。



- ① 打开杀毒软件所在的文件夹
- ② 选择杀毒软件主程序
- ③ 单击【打开】按钮



STEP 4 完成设置

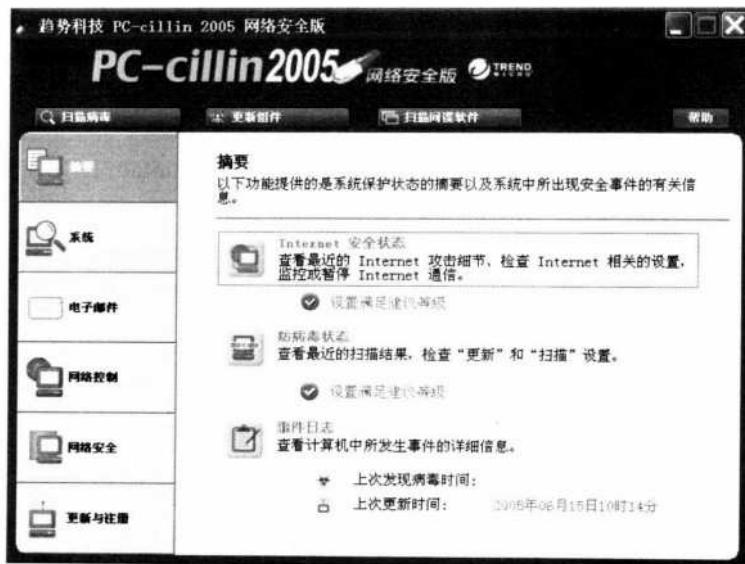
选择杀毒软件后，在【文件传输】对话框中就会出现其路径，查看无误后单击【确定】按钮完成设置。



- ① 单击【确定】按钮

设置完成后，当用户通过 MSN 传送文件时，MSN 就会在传输结束后自动调用杀毒软件扫描文件，如下图所示。

注意：某些版本的杀毒软件可能会与 MSN 有兼容性问题，具体表现为 MSN 可以启动杀毒软件，但软件不会自动扫描所传输的文件，用户必须手动扫描。



6.5 防御来自局域网的攻击

局域网可以将多台计算机连接起来，很方便共享彼此的资源，但是这也为黑客入侵提供了方便。黑客只要成功入侵局域网内的任意一台计算机，就有可能通过这台计算机进一步入侵局域网内的其他计算机。为了提高局域网的安全性，建议用户为网络内的每一台计算机都安装防火墙软件。注意：部分防火墙软件在默认状态下是不允许通过局域网存取资源的（如 Norton Internet Security 2004），用户必须重新设置。

天网防火墙（SkyNet FireWall）个人版是由天网安全实验室开发制作给个人计算机使用的一套相当实用的网络安全防护软件，它可以实时监控网络的存取情况并通知用户，由用户决定是否允许这些存取行为。此软件默认状态下已经设置好了各种网络安全规则，用户只需要在低、中、高3种防护级别中设置一种即可。这对于不了解网络防火墙设置的普通用户来说，相当方便。注意：天网防火墙并非只是一套针对初级用户的产品，它也为高级用户提供了非常完善的设置，使初级用户和高级用户都可以使用。

虽然天网防火墙是付费软件，但用户同样可以从其官方网站下载试用版本，下面就以最新的试用版本为例，介绍如何安装及使用天网防火墙。

软件小档案

软件名称：天网防火墙个人版

版本：V2.7.6.1005 Build 1026

官方网站：<http://pfw.sky.net.cn/>

其他下载网址1：<http://www.onlinedown.net/soft/6958.htm>

其他下载网址2：<http://www.skycn.com/soft/3253.html>

软件类型：共享试用



● 安装天网防火墙

下载完成后，直接安装防火墙即可。以下是安装步骤：

STEP 1 启动安装向导

下载完成后，双击【SkynetPFW_Trial_Release_v2.73_Build0517.EXE】程序即可启动安装向导。

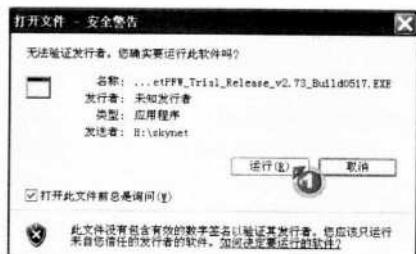


① 双击【SkynetPFW_Trial_Release_v2.73_Build0517.EXE】程序

STEP 2 跳过安全警告

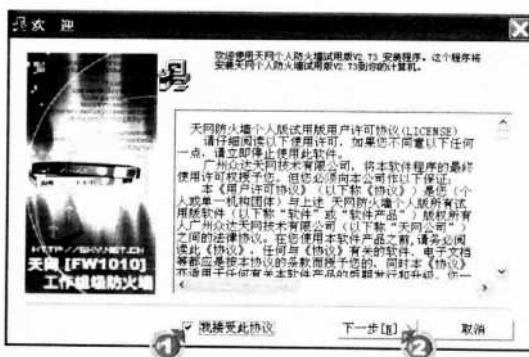
启动安装程序后系统会提示此软件是没有验证的软件，是否确定安装，此时只需单击【运行】按钮即可。

① 单击【运行】按钮



STEP 3 接受许可协议

在【欢迎】对话框中选择【我接受此协议】复选框，并单击【下一步】按钮。



① 选择【我接受此协议】复选框

② 单击【下一步】按钮

STEP4 设置安装位置

在【选择安装的目标文件夹】对话框中，已经提供了默认的安装位置，但用户也可以单击【浏览】按钮改变安装位置。建议保持默认设置，直接单击【下一步】按钮。



① 单击【下一步】按钮

STEP5 设置程序组

程序组安装完成后，程序的快速启动图标将显示在【开始】菜单的位置，保持默认设置即可。

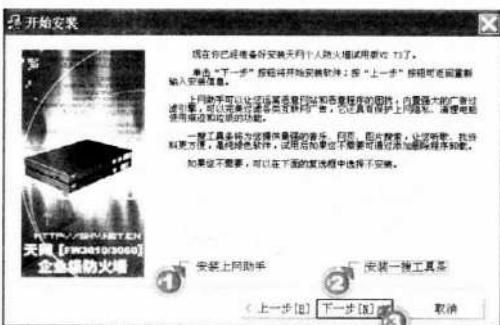
① 单击【下一步】按钮



① 单击【下一步】按钮

STEP6 取消插件的安装

这一步将设置是否安装上网助手和一搜工具条，建议取消选择这些选项，因为用不到这些插件。



① 取消选择【安装上网助手】复选框

② 取消选择【安装一搜工具条】复选框

③ 单击【下一步】按钮



STEP7 开始安装

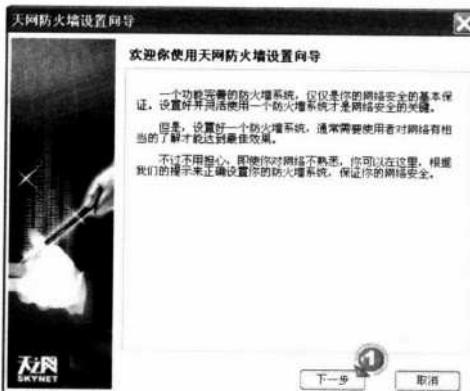
此时，正开始安装程序。

① 安装进度

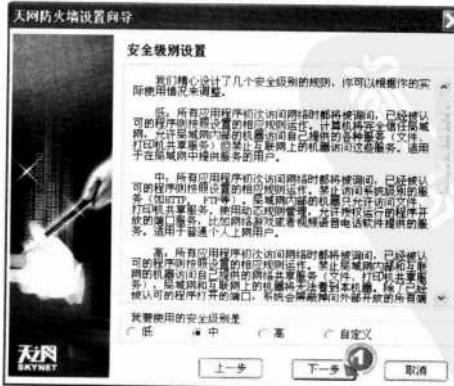


STEP8 跳过防火墙设置向导

当安装快完成后，会弹出设置防火墙向导对话框，单击【下一步】按钮跳过防火墙设置向导，继续下一步操作。



① 单击【下一步】按钮



STEP9 设置安全级别

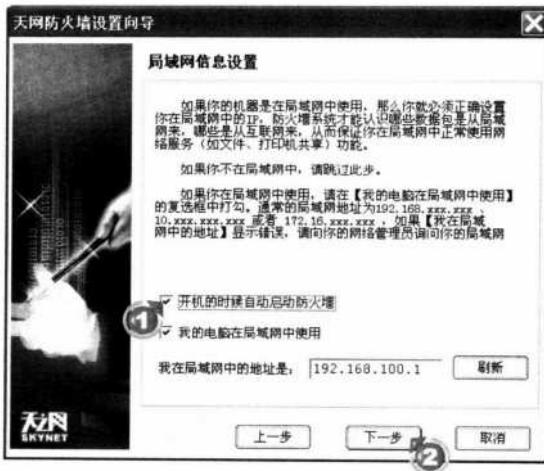
默认状态下安全级别为【中】，用户也可重新设置安全级别，建议保持默认设置。对防火墙规则比较熟悉的用户，可选择【自定义】选项。

① 单击【下一步】按钮

STEP10 设置局域网信息

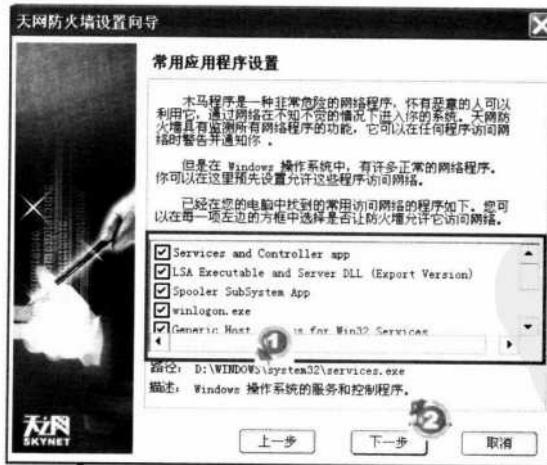
选择【开机的时候自动启动防火墙】复选框，这样在开机后，防火墙将同时对系统进行保护。

- ①选择【开机的时候自动启动防火墙】复选框
- ②单击【下一步】按钮

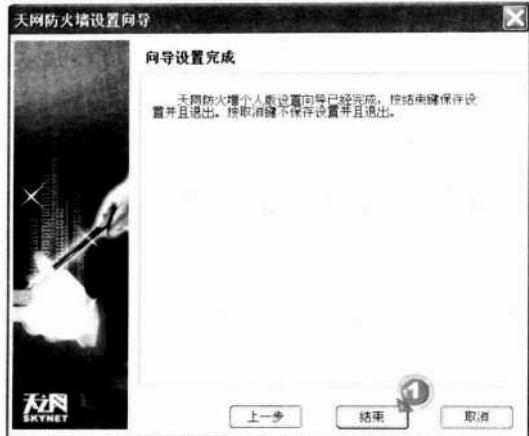
**STEP11** 设置网络程序访问网络权限

在此对话框中，程序识别出了常用的网络程序，用户可在此选择或取消选择程序访问网络的权限。

- ①可选择是否允许这些程序访问网络
- ②单击【下一步】按钮：

**STEP12** 完成向导设置

完成设置后，退出设置向导。

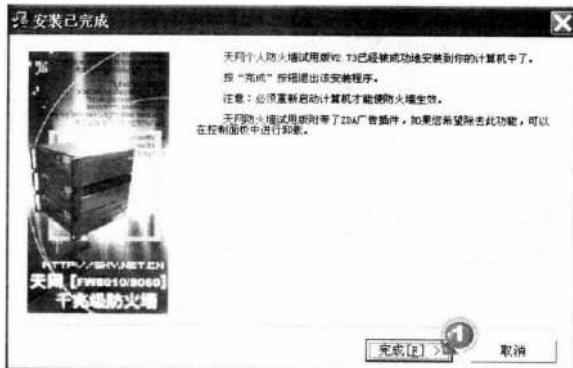


① 单击【结束】按钮

STEP13 完成安装

单击【完成】按钮完成天网防火墙的安装。

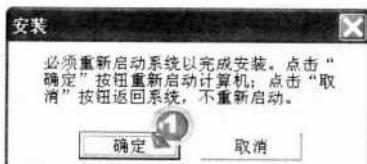
① 单击【完成】按钮



STEP14 重新启动计算机

完成后需要重新启动计算机设置才会生效，因此单击【确定】按钮。

① 单击【确定】按钮



● 设置天网防火墙

天网防火墙共提供了以下 3 种设置：

- ① 应用程序规则设置。
- ② IP 规则设置。
- ③ 系统设置。

以下就分别介绍一下这 3 种设置。

● 应用程序规则设置

天网提供了针对应用程序访问网络的权限设置，通过这些设置，可以有效地屏蔽一些非法程序对网络的访问，因此也就禁止了木马程序向外发送盗取的信息。

STEP 1 进入应用程序规则设置窗口

在程序的主窗口中单击图标，切换到应用程序设置规则窗口。

- ① 单击图标
- ② 切换到应用程序设置规则窗口



STEP 2 选取应用程序

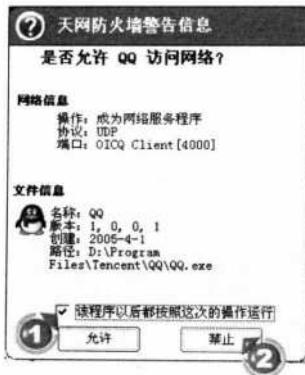
如果想禁止某个应用程序访问网络，只需选择它后单击【删除】按钮即可。

- ① 单击选取程序
- ② 单击【删除】按钮



STEP 3 设置访问权限

删除后，当再次运行这个软件后，会弹出一个对话框，此时，如果想永久禁止该程序访问网络，只需选择【该程序以后都按照这次的操作运行】复选框，然后单击【禁止】按钮即可。



- ①选择【该程序以后都按照这次的操作运行】复选框
②单击【禁止】按钮

STEP 4 改变访问权限

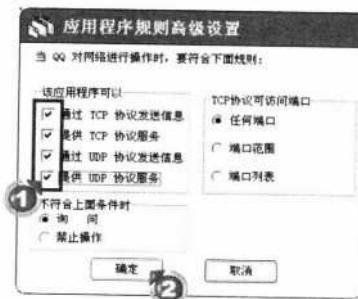
当希望此程序访问网络时，只需在应用程序规则窗口中选择此程序，然后单击程序后面的图标，打开应用程序规则高级设置窗口即可。

- ①选择程序
②单击【】图标



STEP 5 重新设置访问权限

在选项对话框中，选择所有的协议，并单击【确定】按钮，然后再次运行该程序即可。



- ①选择所有协议
②单击【确定】按钮

17 补充说明**其他设置说明**

在应用程序规则窗口还有很多设置，如添加规则，导入、导出规则等，以后在 8.2 节介绍黑客专用防火墙时将做详细的介绍。

● IP 规则管理

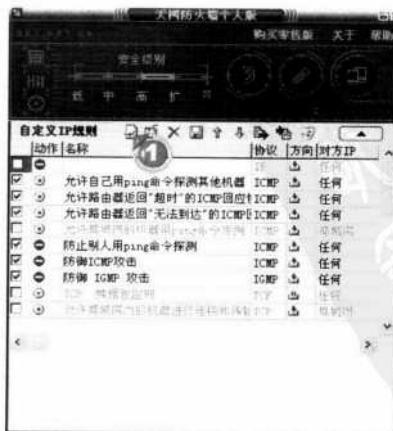
IP 规则是对整个系统的网络层数据包监控而设置的。利用自定义 IP 规则，用户可针对个人不同的网络状态，设置自己的 IP 安全规则，使防御手段更周到、更实用。自定义 IP 规则的方法如下：

STEP1 进入 IP 规则管理窗口

在程序的主窗口中单击图标，即可切换到 IP 规则管理窗口。

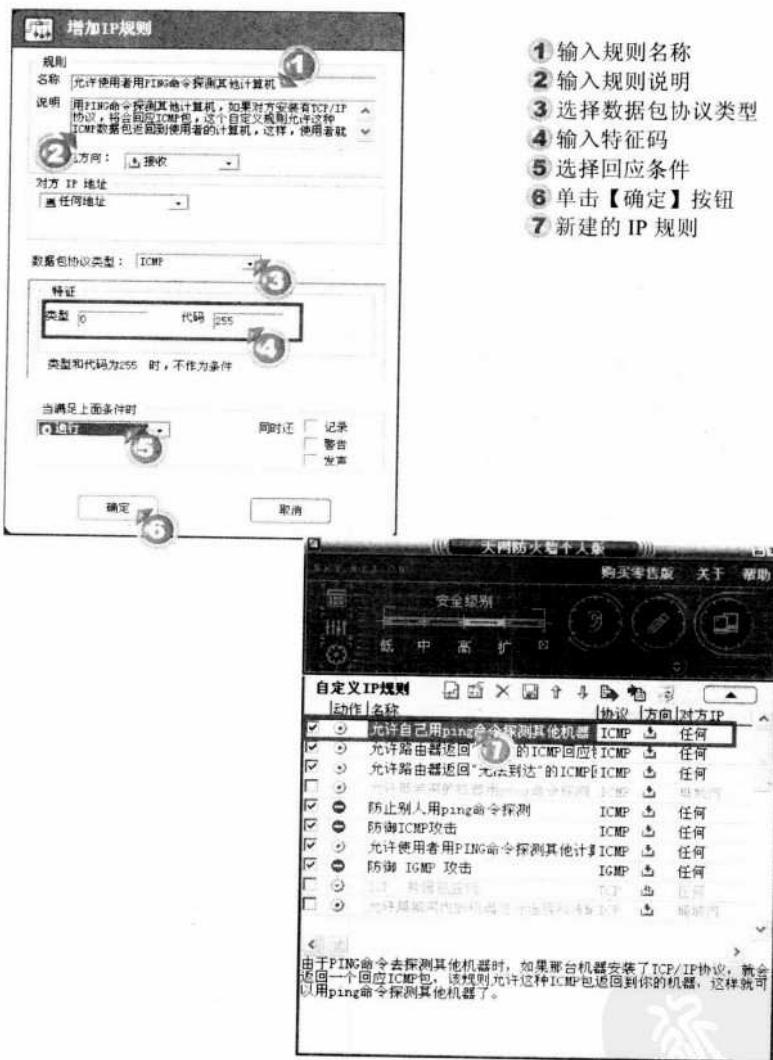
**STEP2 增加规则**

单击图标，添加一个规则。

① 单击图标

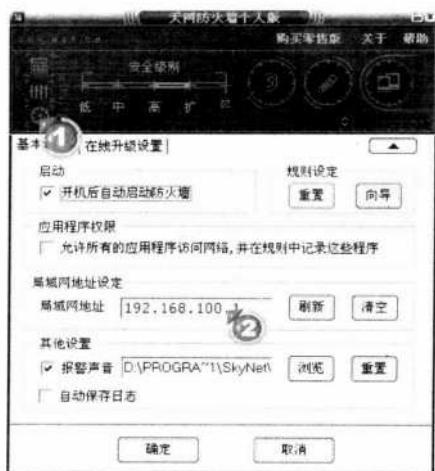
**STEP3** 设置规则

输入规则名称、说明、数据包方向、数据包协议类型、特征码以及判断执行的回应操作，单击确定【按钮】，这样就建立了一个用户自定义的IP规则。

**● 系统设置**

系统设置同时也包括了在安装过程中的防火墙设置向导，通过此向导同时还可以改变防火墙的安全等级。除了可重新运行向导设置功能外，还可以改变IP地址、启动设置和报警声音等。

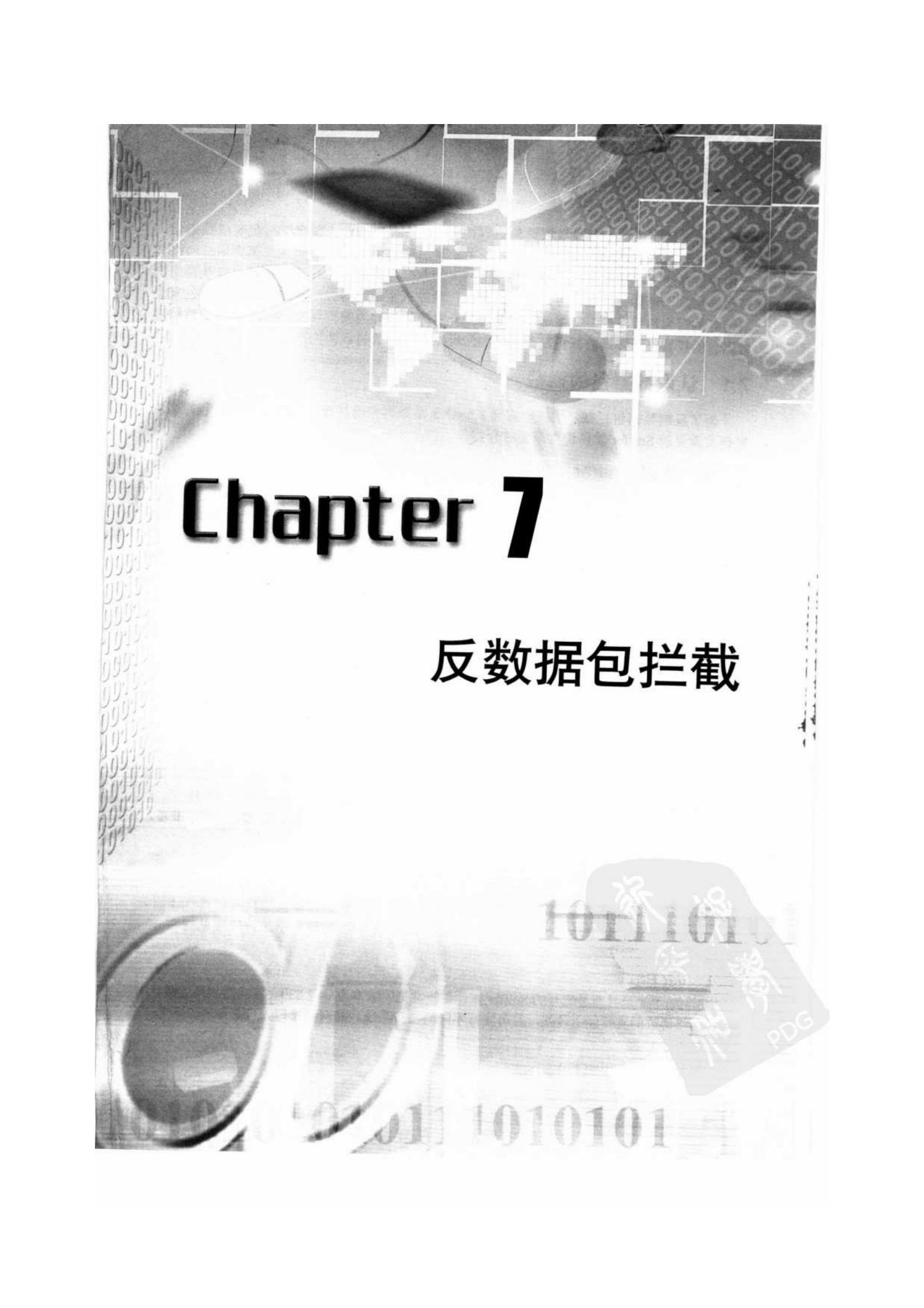
进入系统设置页面时，只需单击主程序窗口中的图标即可。



- ① 单击②图标
② 系统设置窗口

这里介绍的只是天网防火墙的基本的功能，在8.2节介绍黑客专用的防火墙时，还会针对这套软件做更详细的介绍。





Chapter 7

反数据包拦截



网络上所有的数据都是以数据包的方式传递的，所有的信息都会先被包装成数据包，当数据包到达目的地后，再重新组合还原成信息。这种数据传递方式使得黑客通过网络盗取用户信息变得非常方便。黑客只要将网络上的数据包截取下来并还原，就可以获得用户传递的信息，例如聊天的内容、信用卡密码、商业机密信息等。这种通过拦截数据包来盗取信息的行为称为嗅探，利用这种技术原理开发的软件称为嗅探器（Sniffer）。本章将针对数据包的拦截展开详细的剖析，并介绍如何反制数据包的拦截的内容。

7.1 认识数据包的拦截

为了反制数据包拦截，用户首先要了解什么是数据包的拦截，下面将对数据包拦截的原理及常见的 Sniffer 软件进行简要的介绍。

7.1.1 认识 Sniffer

关于 Sniffer 较为流行的定义是：利用计算机的网络连接端口拦截目的地为其他计算机的数据包的工具。通常，网络上的数据包是以类似广播的方式传递的，当网络内某计算机 A 将信息传递给另一台计算机 B 时，在 A 与 B 之间的计算机都会收到 A 传递的数据包。一般情况下，这些计算机在收到 A 发出的数据包后，会检查数据包标头的信息以确认数据包的目的地，当目的地与本机地址相符或者此数据包是广播数据包时就接收此数据包，否则就将其丢弃。

安装 Sniffer 软件后，计算机的网卡会被设置成一种名为混杂（Promiscuous）的工作模式，此时计算机将接收网络上所有的数据包。

事实上，Sniffer 软件并非黑客专用，许多网络管理人员也需要通过它来分析与管理网络。最常见的就是用来分析网络的数据流量，找出网络中潜在的问题，例如当网络上工作不正常，数据传输速率明显下降却又找不到原因时，就可通过 Sniffer 软件来检查数据包的情况，以确定故障发生的精确位置。

然而，Internet 上大部分信息都是未加密的明文，如 MSN 等网络通信软件、Internet Explorer（浏览一般的网页时）等，部分安全性较差的软件甚至在键入账户密码等重要信息时也未加密，因此黑客可通过 Sniffer 软件直接获取用户的重要信息，如信用卡账户、密码等。此外，通过 Sniffer 还可获取 IP 地址、IP 路由等信息，为执行进一步攻击做准备，因此其危害性相当大。

7.1.2 常见的 Sniffer 软件

Sniffer 的软件非常多，其功能也各不相同，有些软件可以对截获的数据包进行详细分析，而有些则只能获取特定类型的信息（如账户或密码），下面将介绍几种较常见的 Sniffer 软件。

● Sniffer Pro

Sniffer Pro 是目前最流行的 Sniffer 软件，较常见的版本为 v4.7.530，其功能相当完善，对各种网络协议的支持能力较强，且可支持不同的操作系统，是网络管理人员必备的工具之一。

软件小档案

软件名称：Sniffer Pro

版本：4.70.530

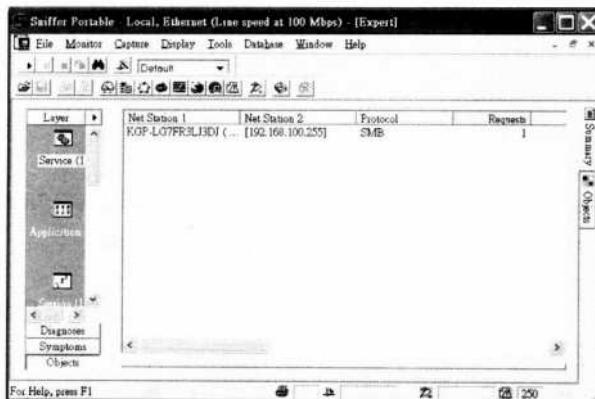
官方网站：<http://www.asl-sniffer.co.uk/>

其他下载网址 1：<http://www.222pc.com/soft/12505.htm>

其他下载网址 2：<http://www.ayxz.com/soft/2918.htm>

软件类型：共享试用

下图为 Sniffer Pro 的主界面。



● IRIS

IRIS 是 Eeye 公司推出的网络流量分析工具，通过这套软件系统管理员可以轻易获得网络用户的情况，并可检查进出网络的数据包，目前较常用的版本为 4.0。

软件小档案

软件名称：IRIS

版本：4.0

官方网站：<http://www.secureuni.com>

其他下载网址 1：<http://www.eeye.com/html/products/iris/download/index.html>

其他下载网址 2：<http://act.it.sohu.com/download/show-3341.html>

软件类型：共享试用

下图为 IRIS v4.0 的主界面。





● Password Sniffer

Password Sniffer 是一款免费的密码嗅探软件，可支持 Windows 9x、Windows 2000 及 Windows XP 操作系统，由于 Password Sniffer 自带嗅探驱动，因此无须另外安装 WinPcap 等嗅探驱动软件。

Password Sniffer 对网络协议的支持相当完善，可支持数十种网络协议，包括 FTP、Telnet、SMTP、HTTP、POP、NNTP、IMAP、SNMP、LDAP 等，适用范围比较广泛，是目前较流行的密码嗅探软件之一。

软件小档案

软件名称：Password Sniffer

版本：1.2

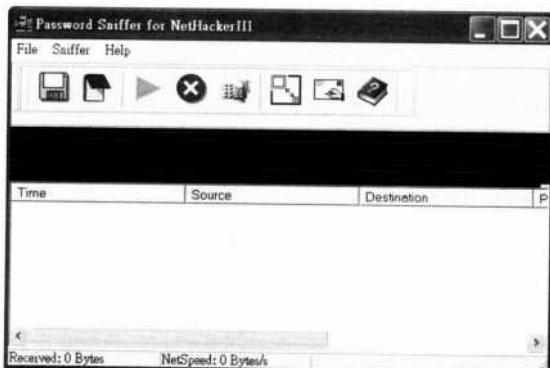
官方网站：<http://www.effetech.com/>

其他下载网址 1：http://down.hiwuhan.com/SoftView/SoftView_17810.html

其他下载网址 2：<http://www.onlinedown.net/soft/20129.htm>

软件类型：免费

Password Sniffer 是一套免费的软件，用户可以自由选择是否注册，且未注册版本没有任何功能限制，其主界面如下。



7.2 拦截数据包

了解了黑客拦截数据包的方法以后，用户也可以尝试用 Sniffer 软件拦截自己所在网络的数据包，以检测网络的安全性。下面将以几套常用的软件为例，介绍如何通过 Sniffer 软件检查网络是否安全。

7.2.1 检测局域网中的密码是否安全

在使用网络上的各种服务时，用户经常需要键入密码，如 FTP 账户密码、电子邮件账户密码等，如果这些密码被黑客盗取，将会造成严重的后果。例如，黑客盗取了某公司 FTP 服务器的密码后，就可以登录服务器盗取公司内部的机密数据。为了避免这种情况的发生，用户可以用嗅探软件检测自己的局域网，如果发现有密码泄漏的情况，应及时采取对应的措施。下面将以目前较流行的密码嗅探软件 Password Sniffer 为例，介绍如何检测局域网内的密码是否安全。

● 安装 Password Sniffer

Password Sniffer 是一套免费的软件，因此用户可以在各大网站自由下载。此程序的安装也比较简单，用户只要按照向导的提示一步步执行即可。为了尽可能获取更多的数据，建议将 Password Sniffer 安装到网关。

STEP 1 执行安装程序

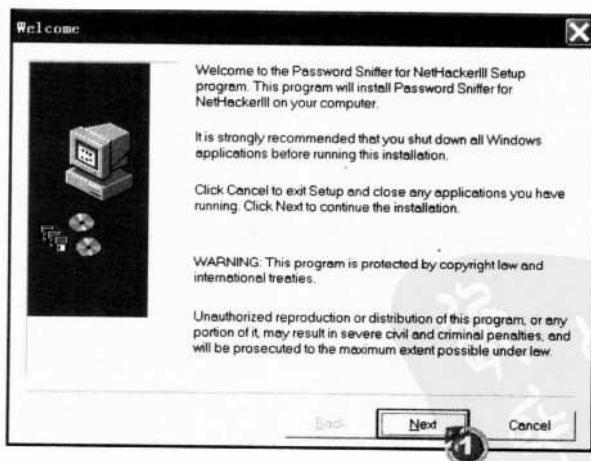
下载文件后，直接双击文件即可执行安装程序。



STEP 2 跳过欢迎界面

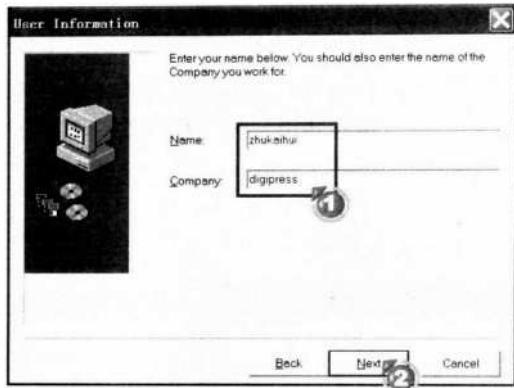
单击【Next】按钮，跳过安装向导的欢迎界面，继续安装。

① 单击【Next】按钮



STEP 3 键入个人信息

在【User Information】对话框中键入用户及公司名称，这里键入的内容不会对后续使用造成影响，可随意键入。

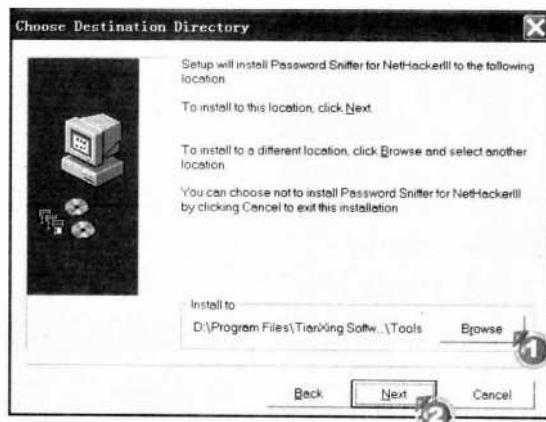


- ① 键入个人信息
- ② 单击【Next】按钮

STEP 4 选择安装路径

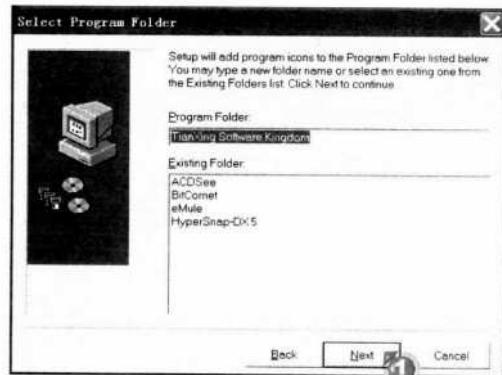
默认状态下，程序会安装在系统分区的【Program Files】文件夹中，如需变更安装文件夹，可单击【Browse】按钮。

- ① 单击【Browse】按钮，
改变安装路径
- ② 单击【Next】按钮



STEP 5 设置程序文件夹名称

在【Select Program Folder】对话框中设置程序文件夹的名称，建议采用默认值即可。

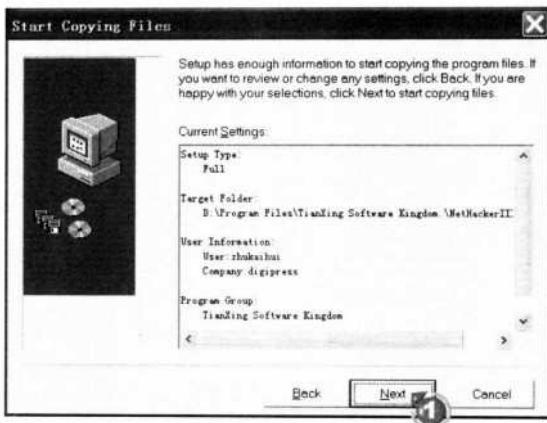


- ① 单击【Next】按钮

STEP 6 开始安装

在【Start Copying Files】对话框中安装向导会显示前面所做的设置，检查无误后单击【Next】按钮开始安装。

- ① 单击【Next】按钮



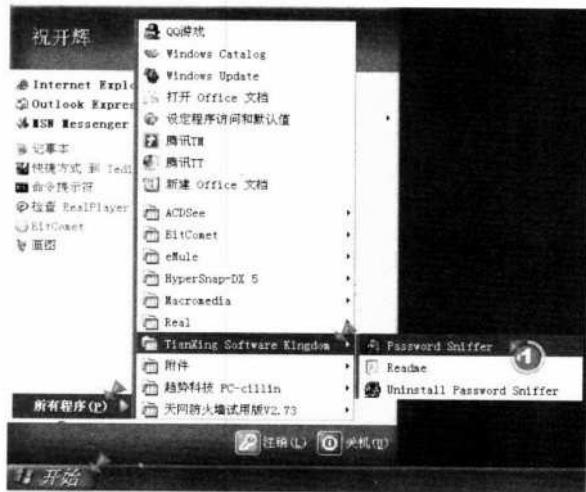
安装完 Password Sniffer 后，就可以用它来检测局域网是否存在密码泄漏的危险。

● 检测局域网内的密码

安装完成后，系统管理员需要手动打开 Password Sniffer 程序，启动程序后系统管理员可要求网络用户尝试使用各项网络的功能，如登入 FTP 服务器、打开电子信箱等，然后检查 Password Sniffer 程序是否拦截到用户密码。

STEP 1 启动 Password Sniffer 程序

安装完成后，会在【开始】菜单里增加程序的快捷方式，通过此快捷方式可快速打开程序。



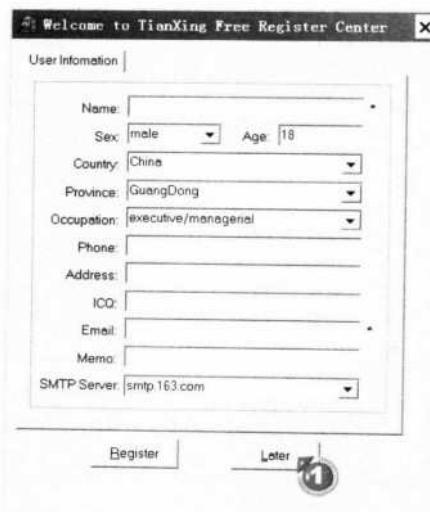
① 依次选择【开始】→【所有程序】→【TianXing Software Kingdom】→【Password Sniffer】选项



STEP2 跳过注册界面

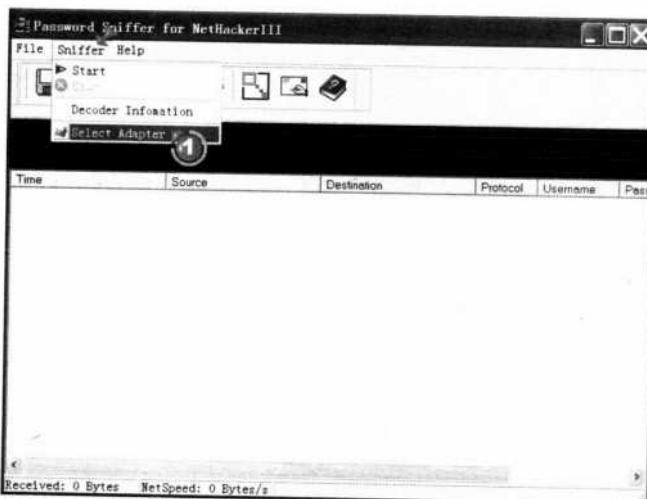
在【Welcome to...】对话框中用户可免费注册，如果暂时不想注册可单击【Later】按钮。未注册也不会影响软件的功能。

- ① 单击【Later】按钮，跳过注册界面



STEP3 设置 Password Sniffer

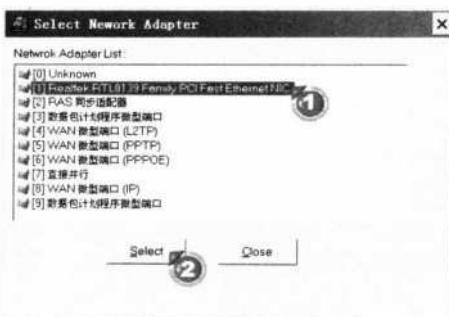
安装完成后，用户还需对 Password Sniffer 做一些简单设置才能使其正常工作，选择【Sniffer】→【Select Adapter】命令打开【Select Network Adapter】对话框，以便进行设置。



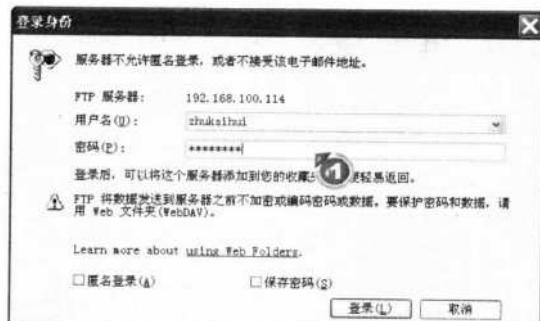
- ① 依次选择【Sniffer-Select Adapter】命令

STEP4 选择要嗅探的网络设备

在【Select Network Adapter】对话框中，选择要嗅探的网络设备，一般情况下选择用于连接局域网的网卡。

**STEP5** 使用网络功能

设置完成后，Password Sniffer 自动开始工作，此时系统管理员可要求局域网的用户尝试使用网络的各项功能，如登入网域、存取数据、登入 FTP 服务器等，以检测是否存在密码泄漏的风险。

① 登入 FTP 服务器**STEP6** 检查嗅探结果

打开 Password Sniffer 检查嗅探的结果，如果盗取密码成功则说明网络存在密码泄漏的风险，应及时修正。例如，本例中成功盗取了某用户登入 FTP 的账户和密码，这时建议采用更安全的登入方式，如采用 CuteFTP Pro 等专业的 FTP 软件。

Time	Source	Destination	Protocol	Username	Password	Raw data
2005-6-16 11:06:03	192.168.100.1.2407	192.168.100.114.21	ftp	anonymous	IEUser@	USER anonymous
2005-6-16 11:06:10	192.168.100.1.2411	192.168.100.114.21	ftp	anonymous	IEUser@	USER anonymous
2005-6-16 11:06:12	192.168.100.1.2412	192.168.100.114.21	ftp	anonymous	IEUser@	USER anonymous
2005-6-16 11:28:48	192.168.100.1.2423	192.168.100.114.21	ftp	zhukaihui	19770403	USER zhukaihui

① 成功盗取的用户名及密码

7.2.2 检测局域网内的数据安全

除了账户及密码外，网络内的许多其他信息也都可能成为黑客的目标，例如某些用户通过实时通信软件（如 MSN）谈论公事时，黑客通过拦截 MSN 的数据包就有可能盗取重要机密；又如，一些用户喜欢直接通过网络传递文件，如果传递的是未加密的文件（如 TXT 文件），则黑客就有可能从数据包中盗取文件的内容。

下面将以网络管理员与黑客都常用的嗅探软件 Sniffer Pro 为例，说明如何拦截局域网的数据包内容。用户可根据下面介绍的方法来检测自己的局域网内是否存在同样的安全隐患。

● 安装 Sniffer Pro

Sniffer Pro 程序可以从其官方网站下载，下载后双击安装文件并按照向导的提示执行操作即可完成安装。

STEP1 启动安装向导

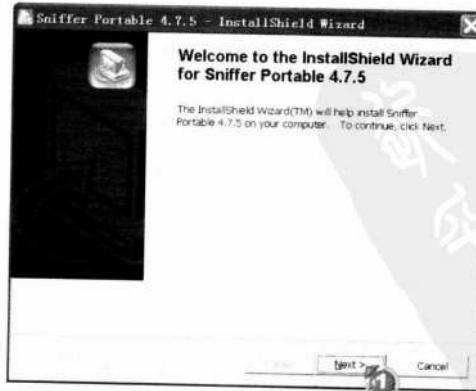
打开安装文件所在的文件夹，双击安装文件即可启动安装向导。



STEP2 跳过欢迎界面

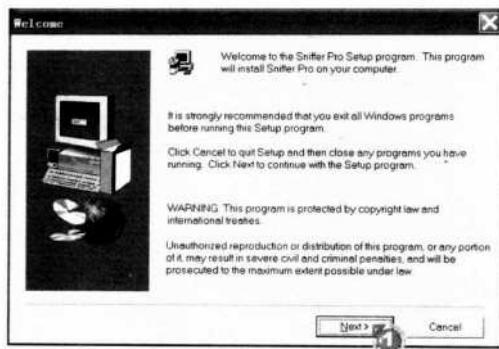
单击【Next】按钮跳过欢迎界面，继续安装。

① 单击【Next】按钮



STEP3 关闭其他无关的程序

为了确保安装成功，向导会要求用户结束其他程序，关闭其他程序后，即可继续执行安装。

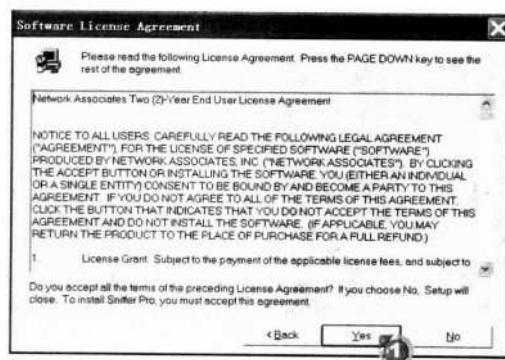


① 单击【Next】按钮

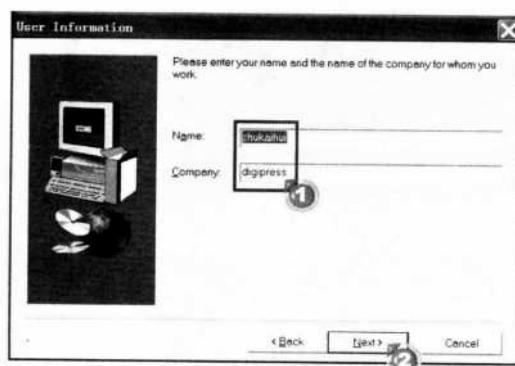
STEP4 接受授权协议

在【Software License Agreement】对话框中显示软件的授权协议，用户只有接受此协议才能继续安装。

① 单击【Yes】按钮，接受授权协议

**STEP5** 键入用户信息

键入用户名及公司名称，这些信息的正确与否不会对后续使用 Sniffer Pro 造成影响。

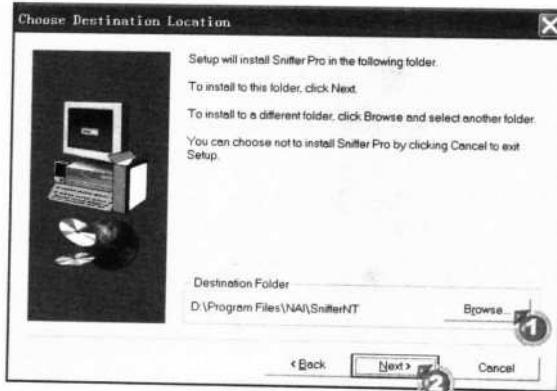


① 键入用户个人信息
② 单击【Next】按钮

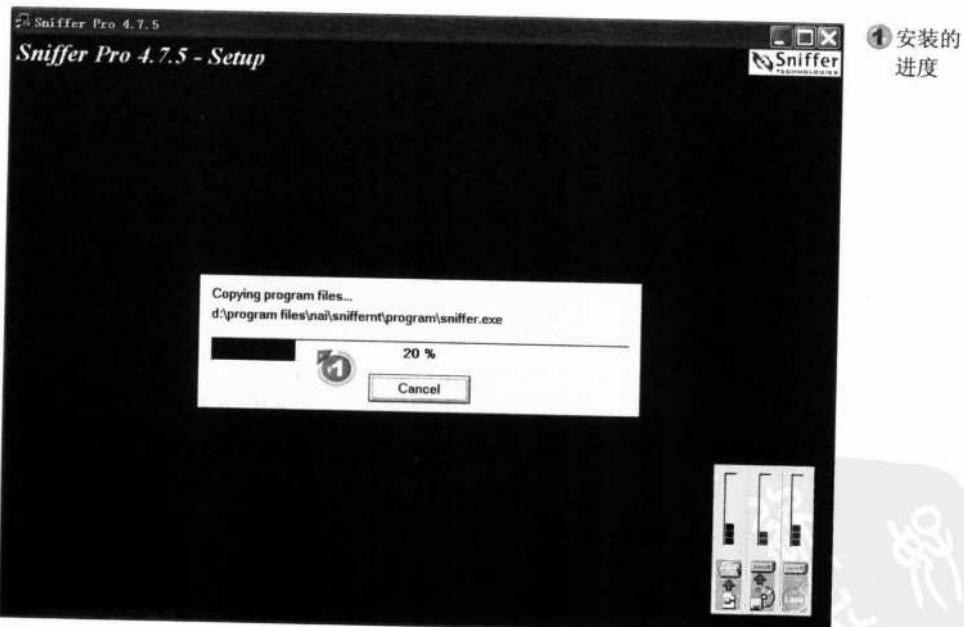
STEP6 设置安装路径

默认状态下安装向导会将程序安装在系统分区的【Program Files】文件夹下，如需安装到其他路径，可单击【Browse】按钮。

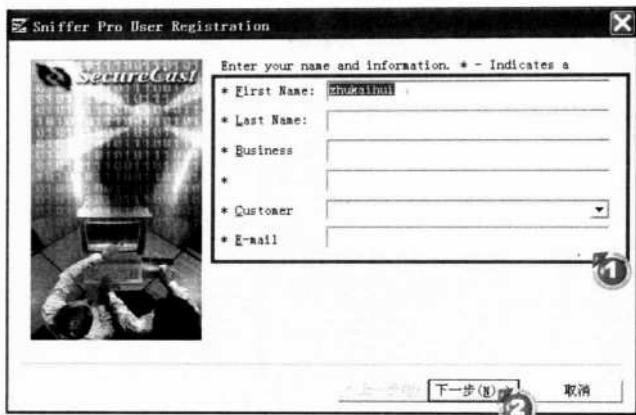
- ① 单击【Browse】按钮，
改变安装路径
- ② 单击【Next】按钮

**STEP7** 检查安装进度

在安装过程中，会显示安装的进度，如需中途结束安装，可单击【Cancel】按钮。

**STEP8** 注册 Sniffer Pro

在【Sniffer Pro User Registration】对话框中输入个人注册信息，如名字、E-Mail 地址等。

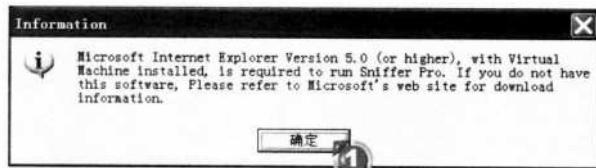


- ① 输入注册信息
② 单击【下一步】按钮

STEP 9 阅读警告窗口

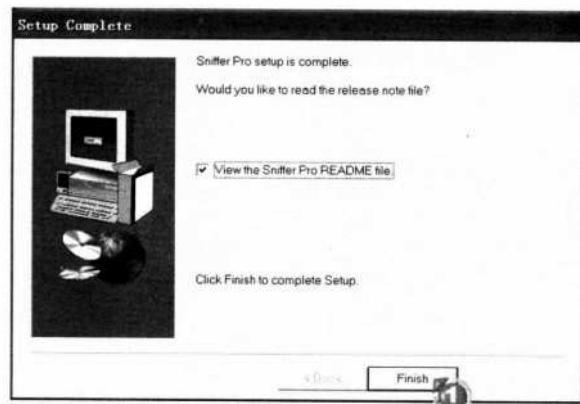
Sniffer Pro 需要用户安装 5.0 以上版本的 Internet Explorer。于 Windows XP 自带 6.0 版本的 Internet Explorer，因此可单击【确定】按钮忽略此警告窗口。

- ① 单击【确定】按钮忽略
警告窗口



STEP 10 结束安装向导

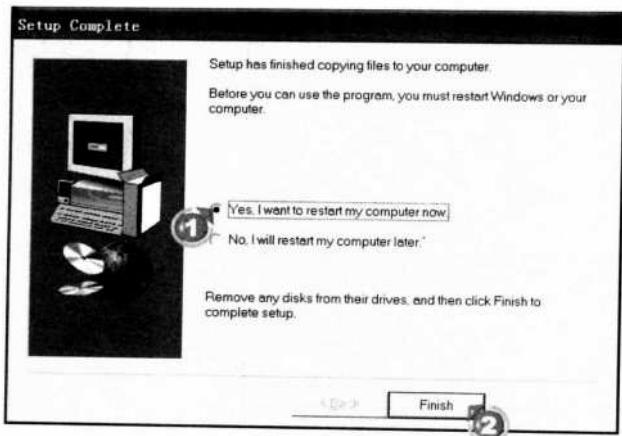
安装完成后，单击【Finish】按钮结束安装向导。



- ① 单击【Finish】按钮，
结束安装向导

STEP 11 重新启动计算机

Sniffer Pro 需要重新启动计算机后才能正常工作，选择【Yes, I want...】单选框并单击【Finish】按钮立即重新启动计算机。

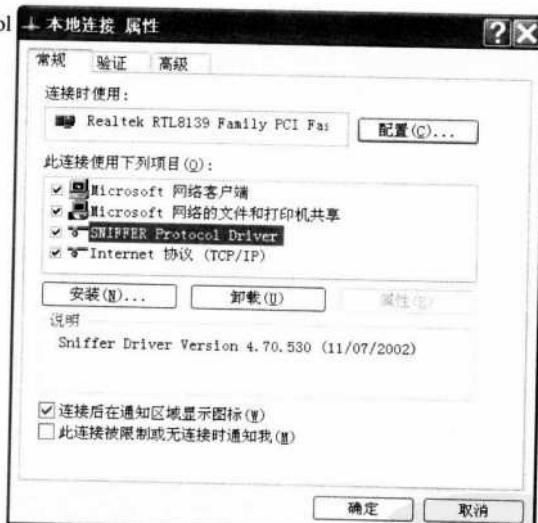


①选择【Yes, I want...】单选框

②单击【Finish】按钮

重新启动计算机后，即可利用 Sniffer Pro 检测网络内的数据包是否安全。安装 Sniffer Pro 后，会在【本地连接 属性】对话框中添加一个名为【SNIFFER Protocol Driver】的选项，即 Sniffer Pro 的驱动程序。如果找不到此选项则说明安装失败，需要重新安装。

①添加的【SNIFFER Protocol Driver】项目



● 检查局域网内的数据包

安装完 Sniffer Pro 后，即可用它来拦截网络内的数据包，以检测数据包的安全性。由于网络内的数据包数量非常庞大，因此网络安全管理人员必须有足够的耐心。下面就介绍一下如何用 Sniffer Pro 来检查网络内的数据包。

STEP 1 启动 Sniffer Pro 程序

安装完成后，用户可通过【开始】菜单上的快捷方式快速启动 Sniffer Pro 程序。

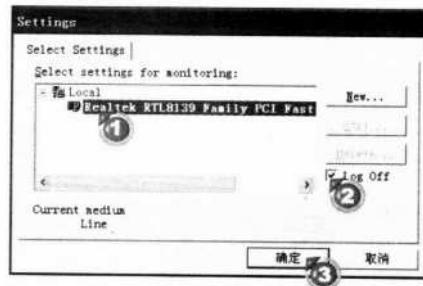


- ① 依次选择【开始】→【所有程序】→【Sniffer Pro】→【Sniffer】选项

STEP2 选择要嗅探的网络设备

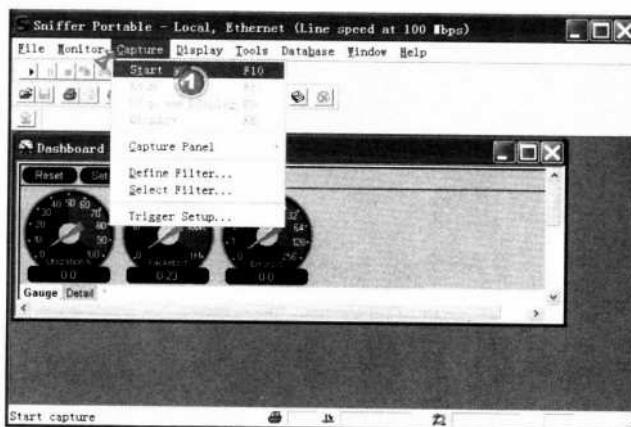
Sniffer Pro 启动时需要用户选择要嗅探的网络设备，如果计算机中只安装了一张网卡，采用默认值即可。

- ① 选择要嗅探的网络设备
- ② 取消选择【Log off】单选框
- ③ 单击【确定】按钮



STEP3 开始获取数据包

在程序主窗口中，选择【Capture】→【Start】命令或按【F10】键，即可开始获取数据包。

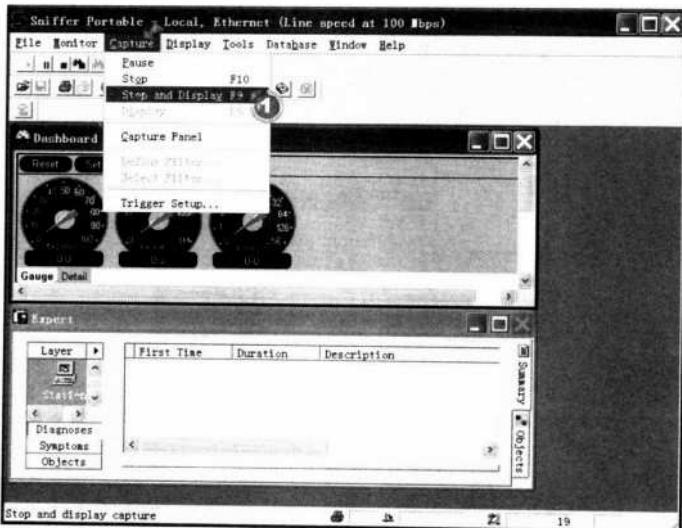


- ① 依次选择【Capture】→【Start】命令，开始获取数据包

**STEP4** 停止获取数据包

为了方便分析，建议在获取到一定数量的数据包后，立即停止获取。如果获取的数据包过多，分析起来会非常困难。

- ① 依次选择【Capture】→【Stop and Display】命令，停止获取数据包

**STEP5** 检查计算机之间的通信

单击【Objects】按钮后，再单击【Application】图标即可检查计算机之间的通信情况，此时程序会显示所有通过这台计算机的数据包。

Layer	Net Station 1	Net Station 2	Protocol	Requests	Frames
Service	APOLLO (192.168.1.1)	[192.168.10.1]	SMB	1	1
Application	DOS-IRC-BFIST (192.168.1.1)	[192.168.10.1]	SMB	2	2
Protocol	E1000EFS-SOCKARO (192.168.1.1)	[192.168.10.1]	SMB	1	1
Diagnostic	KANGCHEN-TAO (192.168.1.1)	[192.168.10.1]	SMB	1	1
Diagnostic	KANGCHEN-TZHEZS (192.168.1.1)	[192.168.10.1]	SMB	1	1
Diagnostic	EC-1000BQD4T101 (192.168.1.1)	[192.168.10.1]	SMB	7	7
Diagnostic	KANGCHEN-TZHEZS (192.168.1.1)	[192.168.10.1]	SMB	5	5
Diagnostic	FEITA-W2200AC (192.168.1.1)	[192.168.10.1]	SMB	1	1
Diagnostic	L782P-KSEAFYDF (192.168.1.1)	[192.168.10.1]	SMB	4	4
Diagnostic	RATMHD-2008 (192.168.1.1)	[192.168.10.1]	SMB	1	1
Diagnostic	SYNTEK (192.168.1.1)	[192.168.10.1]	SMB	125	125
Diagnostic	WS3-699-21L7KE (192.168.1.1)	[192.168.10.1]	SMB	4	4
Diagnostic	ZHANGSHU-95E286 (192.168.10.1)	[192.168.10.1]	SMB	2	2
Diagnostic	[192.168.100.11]	[20.181.217.8]	HTTP	1	1
Diagnostic	[192.168.100.11]	post-3s.bil...	HTTP	1	1
Diagnostic	[192.168.100.11]	www.jiutu...	HTTP	47	111
Diagnostic	w.7obang.com (81...)	[192.168.10.1]	HTTP	1	1

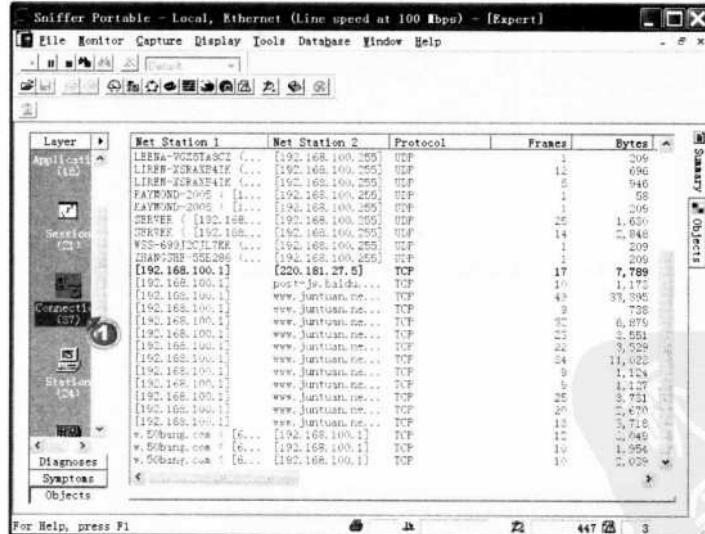
- ① 单击【Objects】按钮
② 单击【Application】图标
③ 计算机之间的通信情况

STEP6 检查通信的详细信息

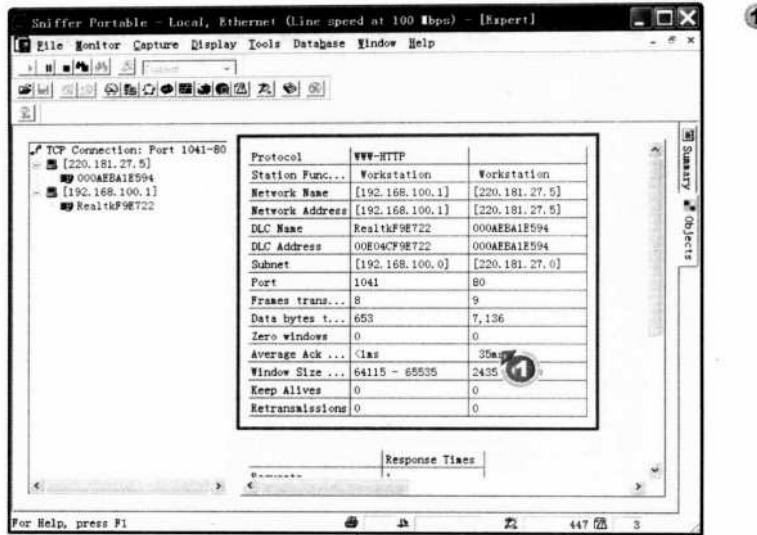
双击要检查的选项，即可检查计算机间通信的详细信息，包括通信主机的地址、名称、连接端口号、数据包类型等。

① 通信的详细信息**STEP 7** 检查计算机之间的连接

单击【Connection】图标可检查计算机之间的连接，包括这台计算机与网络内其他计算机的连接以及其他计算机之间的连接。

① 单击【Connection】图标**STEP 8** 检查连接的详细信息

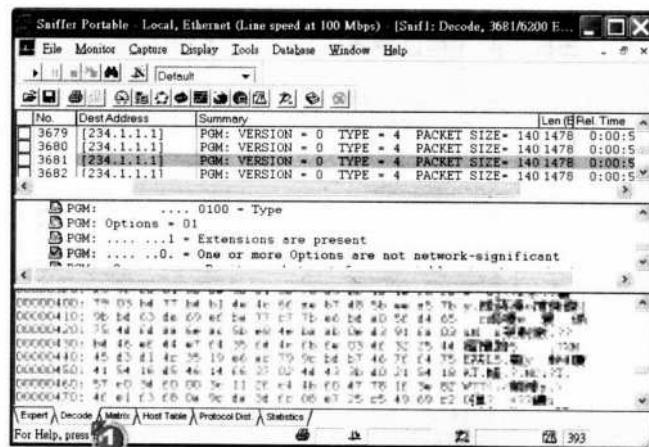
双击连接即可检查其详细信息，包括通信主机的地址、名称、连接端口号、数据包类型等。



① 连接的详细信息

STEP 9 检查数据包的内容

利用【Decode】选项卡可以检查数据包的内容。

① 单击【Decode】
选项卡

● 检测局域网内文件传递的安全性

Sniffer Pro 可对拦截的数据包进行分析，并获取其中的信息。一些用户往往习惯在网络上直接传递各种文件，如果文件未经加密，则黑客截取数据包后就能够获取其中的信息。下面就做一次试验，来证明在局域网内传递文件的风险。

首先，在网关计算机上安装并执行 Sniffer Pro 软件，然后尝试在局域网内传递一个记事本文件，检测 Sniffer Pro 软件是否能拦截记事本文件的内容。

STEP 1 添加记事本文件

添加一个记事本文件，任意写下一些内容，为后续的测试做准备。

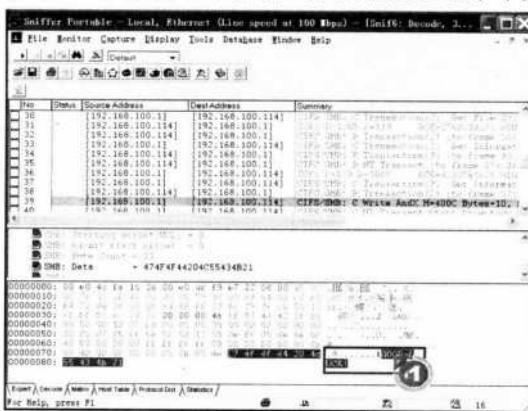
**STEP2** 传递文件

将文件复制到局域网中任意一台计算机内，使文件以数据包的形式在网络内传递。

- ① 复制到局域网其他
计算机中的文件

**STEP3** 检查嗅探结果

复制完毕后，切换到 Sniffer Pro 软件中检查获取的数据包，从搜索结果可看到，在第 39 个数据包中解析出来的就是在记事本文件中键入的内容。



- ① Sniffer Pro 的获取
结果



经过上述试验，相信用户对局域网内传递数据的风险会有所体会，事实上在局域网内传递数据并非不可取，但用户应当采用经过加密的文件类型，如 doc、xls 等，而不要采用未经加密的 txt 文件。

● 检测实时通信软件的安全性

MSN 是目前较流行的实时通信软件之一，很多公司都以其作为员工之间相互沟通的工具。事实上，通过 MSN 传递信息也不够安全，下面将通过检测进行实验。

软件小档案

软件名称：MSN Messenger

版本：7.5

官方网站：<http://www.msn.com>

其他下载地址 1：<http://www1.skyccn.com/soft/799.html>

其他下载地址 2：<http://act.it.sohu.com/download/show-13511.html>

软件类型：免费软件

STEP1 以 MSN 传送信息

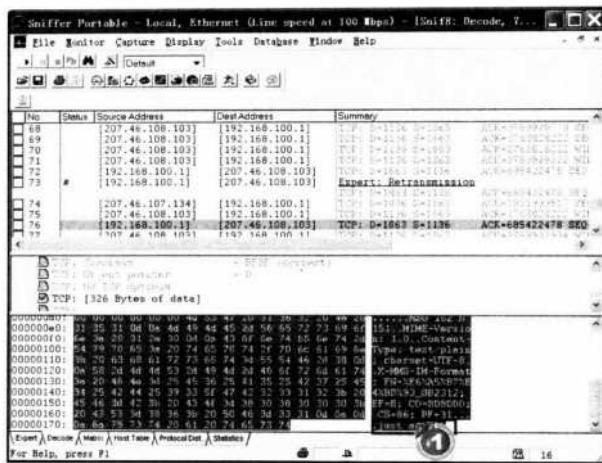
在网关计算机中打开 Sniffer Pro 程序后，在网络内任意一台计算机使用 MSN 传递信息。



以 MSN 传递信息

STEP2 检查嗅探结果

传送完毕后，打开 Sniffer Pro 程序检查获取的数据包，从分析结果可以看到，通过 MSN 传递的信息并未经加密，因此通过 Sniffer Pro 可以直接查阅到前面传送的信息。



① Sniffer Pro 获取到 MSN 传送的信息

除了 MSN 外，用户也可用同样的方法检测其他即时通信软件的安全性，以便从中找出安全性较理想的软件。

7.3 反制数据包拦截行为

由于拦截数据包属于一种【被动】的攻击模式，即黑客只是被动地接收其他计算机的信息，而不会主动发出任何数据包，因此要发现数据包拦截是相当困难的。虽然如此，但数据包拦截也并非无迹可循，下面将介绍常用的反制数据包拦截的手段。

7.3.1 硬件设备反制数据包拦截的行为

以集线器（Hub）构建成的局域网中，网络内所有的计算机都会接收到数据包，因为 Hub 并不会分析数据包的目的地，而只是以广播的形式将信息发送出去。目前，市场上所售的基于 USB 接口的 Hub 很多，一些小型办公局域网，为了节省费用往往都会购买这类集线器。正是因为如此，黑客只要在局域网内任意一台计算机安装了 Sniffer，就有可能拦截网络内其他计算机传递的信息。

根据嗅探器只捕获当前网段数据包的原理，用路由器或三层交换机将网络切分成更小的子网，就可以从硬件层次避免数据包被拦截。但是，这种方法需要购买昂贵的路由以及三层交换设备，所以只有 ISP 或大型企路的内部网络才会使用这种方式。

当然，基于数据链路层的普通交换机以及网桥也可以自动地分析数据包的目的地，为相互传递数据的计算机建立单独的连接，从而在一定程度上可以减少数据包被拦截的风险。但是，它不能抵挡 MAC 欺骗，所以安全性依然很差。

对于资金不多，又渴望高度安全性的用户，建议使用 IPSec 等加密通信方式，对数据包进行软加密，这样即使黑客截取到数据包，也无法解密获得其中内容，从而以低成本实现安全通信。

7.3.2 加密无线网络数据包的传送

随着无线网络功能的不断完善，目前已经逐渐开始被人们所接受，但是对于无线网络

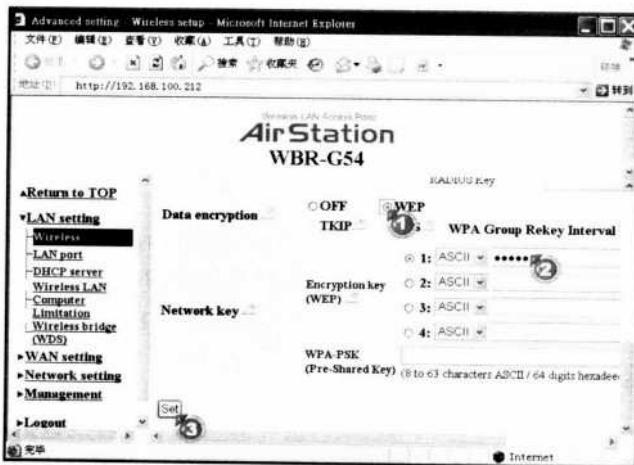


而言，安全性仍是一个不能忽视的问题。由于无线网络不需要物理连接，只需要在户外接收电波就可以拦截数据包，所以为了避免黑客入侵，在使用无线网络时必须使用加密措施。下面就介绍一下如何加密无线网络的数据包。

加密无线网络的操作可分成两阶段：第一阶段，在无线 AP 中设置使用的加密协议及网络密钥；第二阶段，为每台联网的无线网络的计算机启用数据加密功能，并将网络密钥设置为 AP 的密钥。经过上述设置后，网络中所有无线通信都经过密钥加密。由于黑客不知道网络密钥，因此即使截取到数据包，也无法获知包内的数据，从而达到安全通信的目的。

STEP 1 设置无线 AP

在任意一台加入无线网络的计算机上打开 Internet Explorer，并在网址栏中输入无线 AP 的 IP 地址（如 <http://192.168.100.212>），然后就可以在打开的管理窗口中设置此 AP 使用的加密协议及网络密钥。



- ① 选择加密协议
- ② 设置网络密钥
- ③ 单击【Set】按钮
完成设置

STEP 2 设置网络内的其他计算机

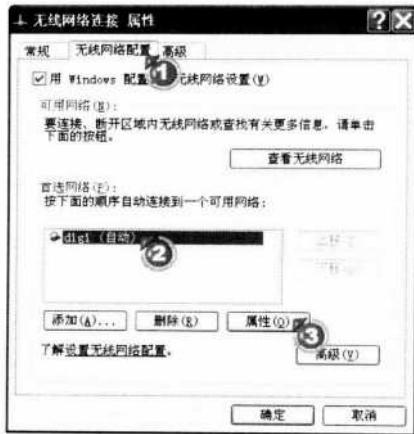
设置无线 AP 后，接着要设置网络内的其他计算机。打开【无线网络连接 属性】对话框，以便对无线网络进行设置。

- ① 单击右键，选择【属性】命令



STEP3 打开【无线网络 属性】对话框

在【无线网络配置】选项卡中选择可用的网络，然后单击【属性】按钮，打开可用的无线网络属性对话框，以便设置计算机加入无线网络。



- ① 单击【无线网络配置】选项卡
- ② 选择可用的网络
- ③ 单击【属性】按钮

STEP4 数据加密

在可用的无线网络连接属性对话框中输入网络密钥，即可对传输的数据进行加密。

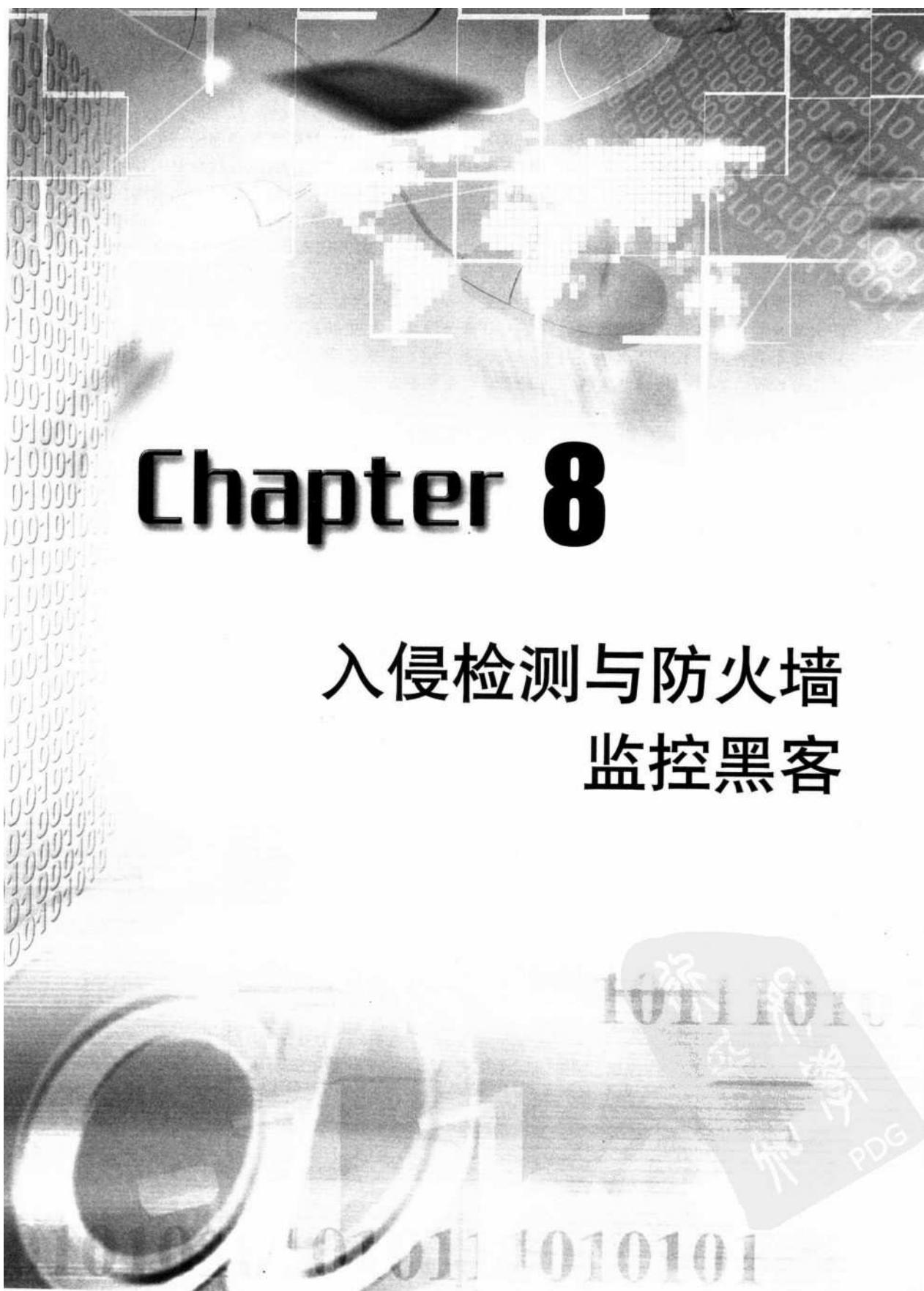
注意：网络密钥必须与 AP 密钥相同。

- ① 取消选择【自动为我提供此密钥】复选框
- ② 输入网络密钥
- ③ 单击【确定】按钮



Chapter 8

入侵检测与防火墙 监控黑客





前面介绍的反木马程序、反按键记录等内容都是被动地针对黑客入侵而设计的防御手段，下面可以换一个角度，从黑客的角度来检查系统是否存在安全漏洞，这也是入侵检测的基本原理。通过入侵检测，用户可以获得关于系统安全隐患的详细信息，作为改善防护方法的依据。例如，某用户通过安全检测发现自己的计算机中存在 RPC 漏洞，那么他就可以安装 Windows 的更新程序来修补该漏洞，进而避免黑客及病毒程序通过 RPC 漏洞入侵计算机。

发现漏洞后，最重要的是安装对应的更新程序修补漏洞。除此之外，还可以通过设置防火墙来阻止黑客通过漏洞入侵。在某些特殊情况下，如更新程序未及时发布或发布的更新程序不完善时，设置防火墙便是唯一的解决之道。前面各章已经分别简单介绍过防火墙的部分设置，本章会将这些内容综合起来进行完整的介绍。

8.1 入侵检测

随着网络的不安全因素日渐增多，为了确保计算机安全，用户不仅要及时更新网络安全软件及杀毒软件，而且还必须安装众多的更新程序以修补系统中的漏洞。入侵检测就是因此需求而产生的，它通过扫描检测，可使用户得知计算机还有哪些安全威胁，为采取对应的防御措施提供必要的依据。

8.1.1 认识入侵检测

在正式开始介绍入侵检测之前，首先要提醒读者注意，本章所说的入侵检测与网络安全专家口中常提到的入侵检测系统（Intrusion Detection System, IDS）是不同的。IDS 是指通过监测网络数据流量，动态地分析、判断入侵行为的系统，而本章所介绍的入侵检测则是指以模拟黑客入侵的手段，检测系统是否存在安全漏洞。

入侵检测一般由专业的网络安全公司提供，用户只要连接到网络安全公司的网站就可以使用这项功能。注意：不同的公司对入侵检测的名称可能有所不同，如赛门铁克就将其称为【安全扫描】。



赛门铁克安全扫描网站的地址为 <http://security.symantec.com/sscv6/default.asp?productid=NIS2004&langid=cs&venid=sym>。

入侵检测的系统需求相对较低，绝大部分计算机都可以达到。例如，赛门铁克公司安全扫描系统的需求为：

操作系统	Windows 98/ME、Windows NT/2000/XP	Mac OS 8.1 或更高版本 Macintosh
需求	Internet Explorer 5.0 或更高版本	Internet Explorer 4.5 或更高版本
	Netscape 4.5 或更高版本	Netscape 4.5 或更高版本

赛门铁克的安全扫描主要包括以下三方面内容：

● 黑客暴露程度检查

黑客暴露程度检查会测试 Internet 应用程序常用的端口是打开、关闭还是隐藏的。打开的端口会响应端口的探查，确定该端口的可用性，同时也最危险。关闭的端口可见，但不对攻击开放。虽然是安全的状态，但是黑客可以使用关闭的端口检测和判断用户计算机的存在，为下一步攻击做准备。隐藏的端口是最安全的。隐藏表示计算机不响应端口探查，这对于扫描 Internet 寻找攻击目标的黑客来说是不可见的。

● Windows 漏洞检查

Windows 漏洞检查用于测试黑客是否能看见计算机的网络标志等基本信息。

● 特洛依木马检查

关于特洛依木马程序的危害在第 3 章已经详细介绍过，这里不再重复。特洛依木马扫描可以检测计算机是否存在可疑的 Internet 连接（如通过某些木马程序常用的通信端口建立连接），以判断计算机是否被特洛依木马程序入侵。



8.1.2 执行入侵检测

通过前面的介绍，相信大家对入侵检测已经有了大概的了解，下面将会进行实际的操作，以便熟悉如何执行入侵检测。虽然提供入侵检测服务的厂商很多，但从易用性及权威性来考虑，下面将以赛门铁克的入侵检测为例进行介绍。



由于入侵检测需要通过 Internet 执行，因此在执行入侵检测之前，要先确认计算机已经连接到 Internet。此外，如果用户通过代理服务器方式进行连接，则只能执行部分安全检测内容。

STEP1 进入计算机安全扫描测试页面

在 Symantec Security Check 页面中单击【进入】按钮，进入计算机安全扫描测试页面。



STEP2 执行安全扫描

单击【开始】按钮，即可执行安全扫描功能。

① 单击【开始】按钮



STEP3 扫描过程

扫描过程则根据网络速度的不同而不同，需要经过一段时间才能得出扫描结果。

**STEP 4 检查扫描结果**

扫描完成后，赛门铁克会通知用户扫描的结果，并向用户提出建议。扫描结果分为【黑客暴露程度检查】、【Windows 漏洞检查】及【特洛依木马检查】三项，单击对应的【显示详细信息】链接，即可查看详细信息。

① 单击【显示详细信息】链接**STEP 5 检查详细信息**

单击扫描结果中对应的【查看您测试结果的详细信息】链接，页面上将会显示扫描说明、扫描结果等详细信息。

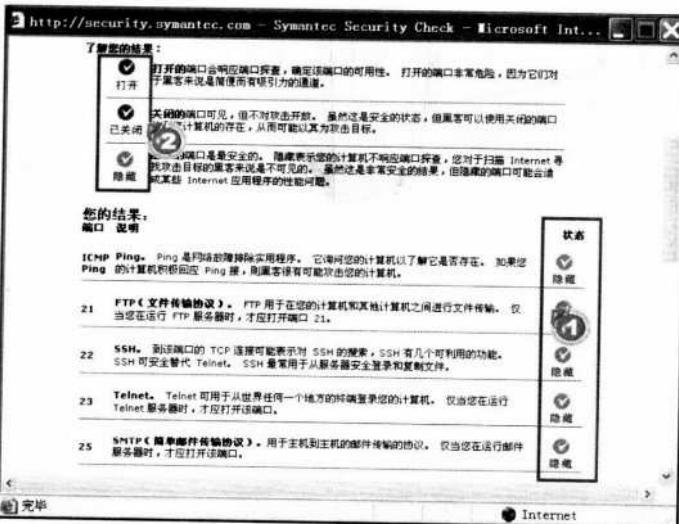


①单击【查看您测试结果的详细信息】链接



STEP 6 信息显示

信息结果的状态分为 3 种，分别是打开的端口、关闭的端口、隐藏的端口。根据测试结果，用户即可判断扫描的结果。



①扫描结果的状态

②3 种标识

通过入侵检测，用户对自己的计算机安全状态有了清楚的了解，根据检测的结果，用户可以有针对性地修补系统中的漏洞，提高计算机安全性。

8.2 黑客专用的防火墙

由于黑客经常入侵其他人的计算机，因此难免会遇到其他高手，为了避免被其他人反黑，他们往往会安装防火墙软件来保护自己。由于要对付的通常是精通网络安全的高手，

所以黑客对防火墙软件的设置必定非常严密。

黑客较常用的防火墙软件主要有 PCGuard、Norton Internet Security、ZoneAlarm 及天网等，其中 Norton Internet Security 在第 3 章中已经有较详细的介绍。下面将以天网防火墙软件为例，介绍如何设置防火墙软件。

天网防火墙是一套简单易用的个人防火墙软件，虽然简单易用，但其功能却相当完备，它能够防御黑客入侵、监控网络进出、设置应用程序规则、设置 IP 规则、查询应用程序网络使用状况、查询日志、接通/断开网络等功能，是目前国内较流行的防火墙软件之一。

天网防火墙分为企业版与个人版两大类，而个人版又细分为零售版、充值版与试用版，其中零售版与充值版需要付费才能使用，而试用版在下载后，再到天网论坛注册，即可获得无限期的试用激活码。以下将针对免费的天网防火墙个人版试用版进行讲解。有关其安装操作已在 6.5 节介绍，所以本节将略过安装部分，直接介绍天网防火墙的使用方法。

下图为天网防火墙官方网站的主界面。



天网防火墙官方网站

8.2.1 天网防火墙的功能

天网防火墙可以为计算机提供全方位的安全防护，除了前面提到的一些功能外，其主要功能还包括以下几点：

- IM 木马专查专杀

主要查杀及清除当前网络上最为流行的 IM 木马。

- 明文传输提示

MSN 等 IM 软件，在传输信息过程中其信息都未曾加密，这样黑客极有可能通过嗅探器截取聊天信息，天网防火墙针对此弊端提供了一套解决方案。



● 网络访问监控

天网的应用程序网络功能是其他程序所没有的，属于天网防火墙首创的特色功能之一。用户通过这项功能，不但可以控制应用程序访问网络的权限，还可以监视应用程序访问网络所使用的数据传输通信协议端口，任何不明的程序（比如木马等）都将在应用程序网络状态功能窗口暴露无遗。

● 修补系统漏洞

系统漏洞是无法避免的，即便是在防火墙背后并且有强大的杀毒软件防护之下，操作系统也无法抵御利用最新漏洞发动的攻击。天网防火墙个人版提供了安全检测修复系统功能，可以修补操作系统的部分严重安全漏洞。

● 日志查看与分析

天网防火墙将会把所有不规则的数据包拦截并记录下来，如果用户选择了监视 TCP 和 UDP 的数据包，则发送和接收的每一个数据包都将会被记录下来，每条记录都将有详细的数据分析内容。

● 断开/接通网络

断开/接通网络功能，将完全控制网络的连接与断开，就像将网线拔下与插入一样。



什么是 IM?

IM 是 Instant Messaging(实时通信)的缩写，它是一种可以让用户在网络上建立某种私人聊天环境的实时通信服务。常见的 IM 软件有腾讯 QQ、微软 MSN、雅虎 Yahoo!、新浪 UC、网易 POPO 等。

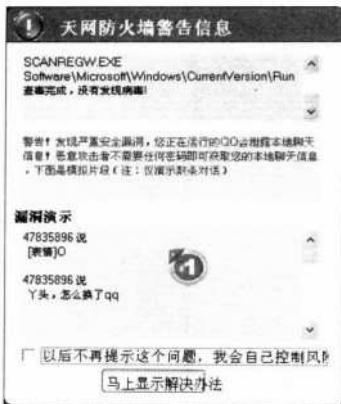
8.2.2 访问控制与明文警告

安装天网防火墙后，当用户打开某个连接网络的软件（如腾讯 QQ 软件）时，防火墙会自动监视其访问网络的动机，并弹出天网防火墙警告信息对话框，用户可单击【允许】按钮确认程序访问网络，或单击禁止按钮取消程序访问网络。



① 天网防火墙警告信息对话框

当用户通过 IM 软件发送信息时，天网防火墙会弹出警告信息对话框，提示用户运行的程序扫描木马的结果，警告信息内容及截取的用户发送信息内容。



① 明文信息截取警告
信息对话框

8.2.3 应用程序网络使用情况

在应用程序网络状态窗口，用户可以查看网络应用程序的路径、版本号、所使用的端口及其协议等相关情况。为了方便用户使用，天网防火墙提供了按协议筛选应用程序的功能，例如选择 TCP 协议时，则只显示 TCP 协议的相关程序在列表中，而自动隐藏使用其他协议的程序。以下是查看的方法：

STEP1 进入应用程序网络状态窗口

在天网防火墙程序主窗口中单击①图标。

- ① 单击①图标
- ② 应用程序网络状态窗口



STEP2 选择通信协议

在【应用程序网络状态】右侧的下拉列表中选择一种通信协议后，在下面的列表中即可显示出使用此通信协议的网络应用程序。



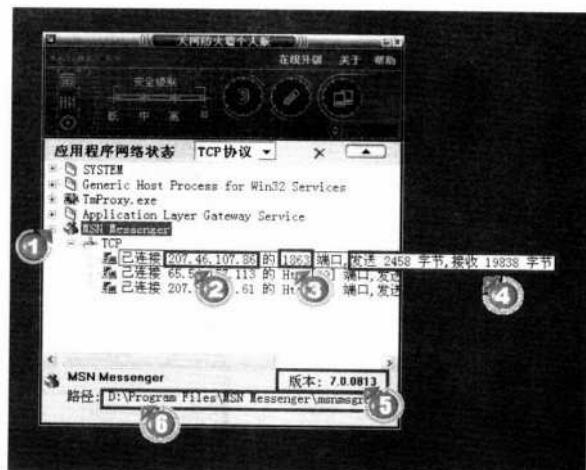
① 选择一种通信协议

② 对应的网络应用程序

STEP3 查看程序详细信息

在列表中可查看程序的详细信息，包括程序连接的 IP 地址、端口、发送的字节数、接收的字节数、程序版本、程序所在路径等信息，为用户判断程序的合法性与非法性提供了可靠依据。

- ① 单击程序前面的 + 图标
- ② IP 地址
- ③ 端口
- ④ 发送与接收的字节数
- ⑤ 程序版本信息
- ⑥ 程序所在路径

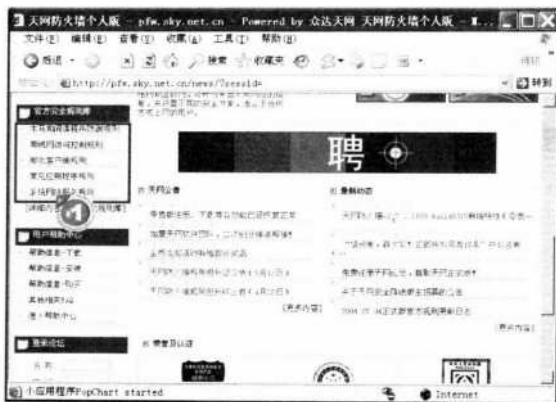


8.2.4 导入官方安全规则库

官方安全规则库是由天网防火墙官方网站提供的，用户可通过下面的网址下载这些规则库。这些规则库包括：

- ① 木马和间谍程序防御规则。
- ② 局域网访问控制规则。
- ③ 游戏客户端规则。
- ④ 常见应用程序规则。
- ⑤ 系统网络服务规则。

规则库下载网址：<http://pfw.sky.net.cn/news>。



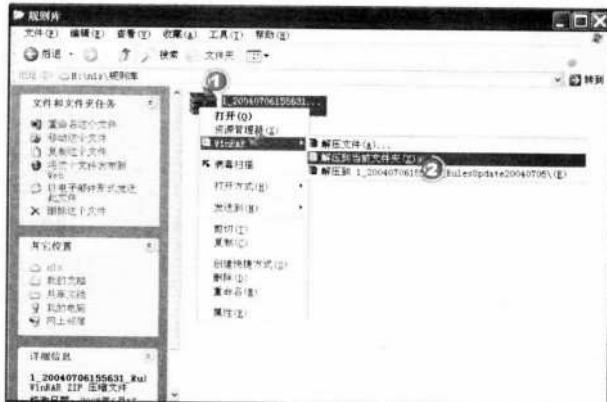
① 官方提供的规则库

下载这些规则库后，需要将其导入才能够使用。具体操作过程如下：

STEP1 解压缩规则库

下载后的规则库为压缩文件，需要将其解压缩后才能导入。

- ① 右键单击压缩文件；
- ② 依次选择【WinRAR】→【解压到当前文件夹】命令



STEP2 导入规则库

规则库需要导入到天网防火墙中才能发挥作用。在天网防火墙主程序中单击图标，切换到IP规则管理窗口，然后单击图标，打开导入对话框。



- ① 单击图标
- ② 单击图标

STEP3 指定规则库

在打开的对话框中，指定规则库所在的文件夹，然后选择规则库文件，最后单击【打开】按钮。

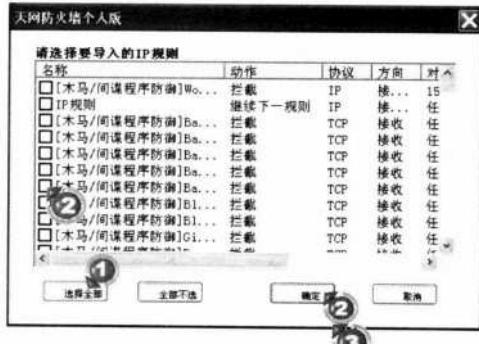


- ① 指定规则库所在的文件夹
- ② 选择规则库文件
- ③ 单击【打开】按钮

STEP4 选择要导入的规则库

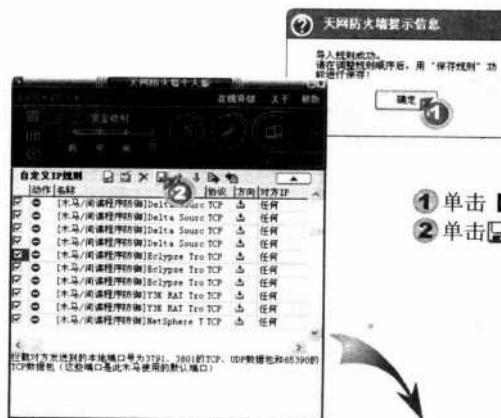
单击【打开】按钮后，会弹出【请选择要导入的 IP 规则】界面，可在对话框中选择需要导入的规则，也可单击【选择全部】按钮选择规则库中的所有规则，一起导入。

- ① 单击【选择全部】按钮
- ② 可选择单一规则并导入
- ③ 单击【确定】按钮



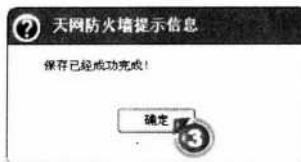
STEP5 保存规则库

当导入成功后会弹出一个对话框确认导入成功，此时单击【确定】按钮即可，然后再单击主程序窗口中的【保存】按钮保存设置，弹出保存已经完成的信息后单击【确定】按钮即可。



- ① 单击【确定】按钮
- ② 单击【保存】按钮

③ 单击【确定】按钮



8.2.5 添加病毒 IP 规则

由于添加病毒【IP 规则】属于较高级的设置，因此在此需要用户了解一些概念，当用户双击需要修改的某个规则后，会打开一个修改对话框，在此窗口中用户会发现有一栏为【TCP 标志位】设置项。



以下将针对 TCP 的 6 个标志位进行简单说明：

URG: 表示紧急指针，它会告诉接收 TCP 模块的紧要指针域指向紧要数据。

ACK: 用来判断数据段的合法性，置 1 时表示确认号为合法；为 0 时表示数据段不包含确认信息，确认号被忽略。

PSH: 用来确认是否缓冲数据段，置 1 时请求的数据段在接收方得到后即可直接送到应用程序，而不必等到缓冲区满时才传送。

RST: 置 1 时重建连接。当接收到 RST 位时，通常发生了某些错误。

SYN: 置 1 时用来发起一个连接。

FIN: 用来判断发送是否完成，置 1 时表示发送端完成发送任务并释放连接，表明发送方已经没有数据发送。

添加一个病毒的 IP 规则，首先需要了解这个病毒的具体技术特征。目前，在网络上有很多网站原创或以转载的形式发布关于病毒的技术性报告，用户可借此添加 IP 规则。

在前面的病毒技术报告页面中，用户会发现病毒会以广播的形式将自身代码通过 1434 端口发送出去，现在以该病毒为蓝本添加一个新的病毒 IP 规则：



① 病毒技术报告

STEP 1 添加规则

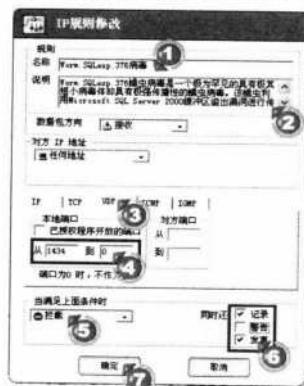
在主程序的自定义 IP 规则中单击【添加规则】按钮，打开【IP 规则修改】对话框。

① 单击【添加规则】按钮



STEP 2 设置 IP 规则

在【IP 规则修改】对话框中添加相应的信息，最后单击【确定】按钮建立 IP 规则。



- ① 输入规则名称
- ② 输入规则说明
- ③ 选择【UDP】选项卡
- ④ 输入本地端口
- ⑤ 展开下拉菜单选择满足条件时的动作
- ⑥ 选择【记录】、【发声】复选框
- ⑦ 单击【确定】按钮

STEP3 保存规则

在主窗口中单击■按钮，保存前面设置好的IP规则。

① 单击■按钮

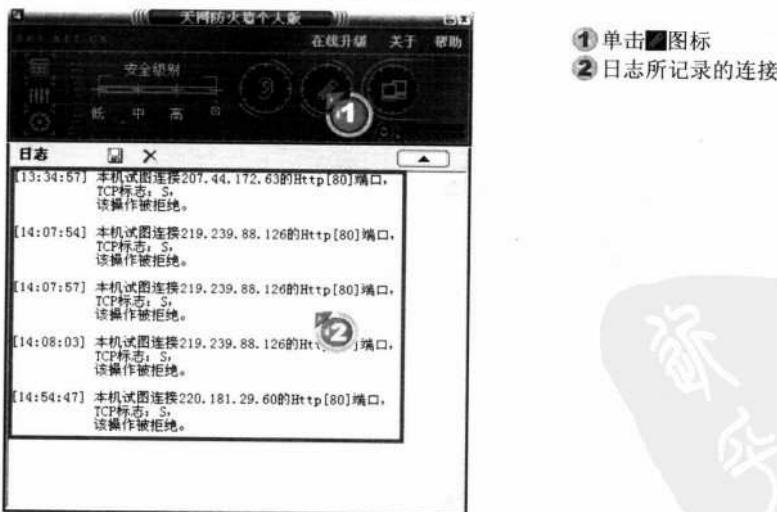


8.2.6 日志检查与保存

浏览日志功能能够查询本机试图连接的端口类型，协议类型及其标志以及操作结果，但是当关闭天网防火墙之后，所有日志将不会被保存，因此需要手工进行保存操作，具体操作步骤如下：

STEP1 进入日志窗口

在主程序窗口中单击■图标，切换到日志窗口。

**STEP2** 保存日志

在日志页面中单击■按钮，进行保存。



① 单击■按钮



STEP 3 设置保存

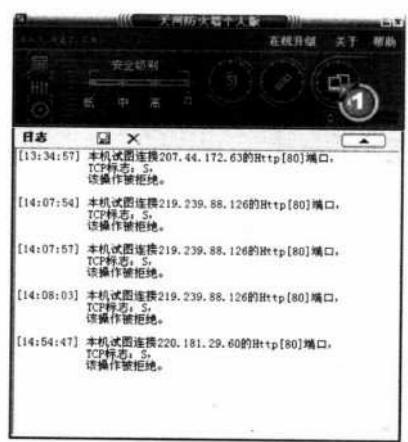
设置保存的路径、文件名，单击【保存】按钮进行保存。



- ① 设置保存路径
- ② 设置文件名
- ③ 单击【保存】按钮

8.2.7 接通断开的网络

此项功能是一种软件控制网络连接的方式，操作非常简单，只需在程序主窗口中单击■图标。当图标变为■样式时，网络已经断开，再次单击这个图标即可访问网络。



① 单击■图标

② 图标变为■样式



8.3 检查 Windows 事件查看器

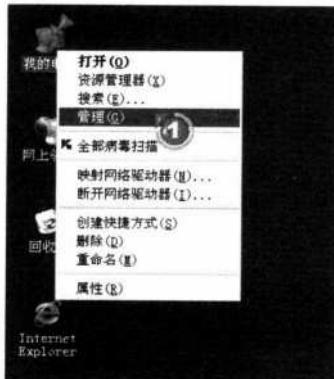
安装防火墙软件并不意味着能完全阻止黑客入侵，因为黑客的入侵手段越来越高明，且操作系统的漏洞亦多不胜数，因此防火墙也可能对一些新出现的攻击方法无能为力。对此，除了最初的 Windows 9x 操作系统外，Windows NT、Windows 2000 及 Windows XP 等操作系统都提供了完备的日志功能，当黑客成功入侵计算机时，往往会在日志中留下记录，通过分析这些信息，将可以知道黑客入侵的时间及采用的方法。这些记录将是人们反追踪黑客的重要信息。

8.3.1 检查 Windows 事件查看器

Windows 事件查看器会记录计算机工作过程中发生的各种事件，如用户登入注销、应用程序启动及关闭、建立及删除文件等，通过 Windows 的事件查看器，用户可以获得关于硬件、软件及用户的重要信息。检查 Windows 事件查看器是追踪黑客踪迹的重要途径之一。

STEP 1 打开【计算机管理】窗口

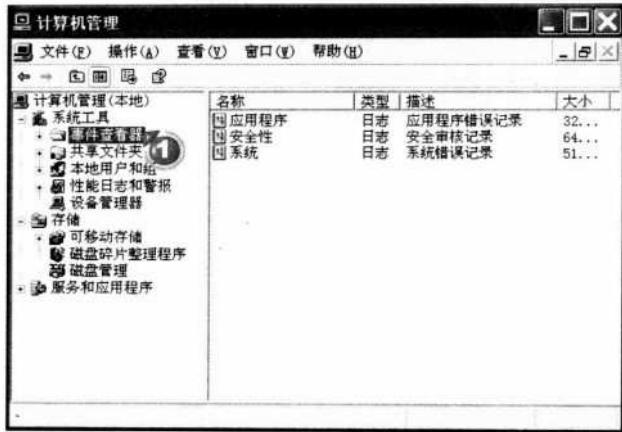
Windows 的事件查看器位于【计算机管理】窗口中，可通过右键快捷菜单打开【计算机管理】窗口。



① 单击右键，选择【管理】命令

**STEP2 展开【事件查看器】选项**

在【计算机管理】窗口左边框架中包含多个选项，事件查看器也位于其中。



①选择【事件查看器】
选项

STEP3 检查应用程序日志

Windows 共包含 3 种日志：应用程序日志、安全性日志及系统日志。其中，应用程序日志用于记录应用程序的各种事件，如失去响应、操作失败等。

① 应用程序日志

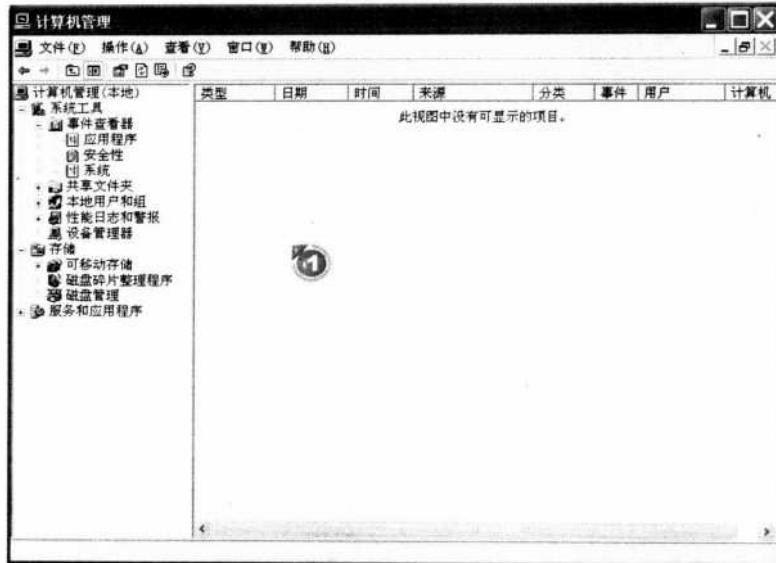
This screenshot shows the Windows Computer Management console with the 'Event Viewer' selected. On the right, a detailed log table is displayed for the Application Log. The columns are: Type, Date, Time, Source, Category, Event, User, and Computer. The log entries show various application events occurring at different times on the same day.

类型	日期	时间	来源	分类	事件	用户	计算机
信息	2005-...	9:24:13	ESSENT	常规	101	N/A	DIGI
信息	2005-...	9:24:13	ESSENT	常规	103	N/A	DIGI
警告	2005-...	9:22:40	EventSystem	(64)	4353	N/A	DIGI
警告	2005-...	9:22:40	EventSystem	(52)	4356	N/A	DIGI
警告	2005-...	9:22:40	EventSystem	(54)	4353	N/A	DIGI
信息	2005-...	9:19:12	ESSENT	常规	102	N/A	DIGI
信息	2005-...	9:19:12	ESSENT	常规	100	N/A	DIGI
警告	2005-...	9:18:31	EventSystem	(54)	4353	N/A	DIGI
警告	2005-...	9:18:31	EventSystem	(52)	4356	N/A	DIGI
警告	2005-...	9:18:31	EventSystem	(54)	4353	N/A	DIGI
警告	2005-...	9:18:31	EventSystem	(52)	4356	N/A	DIGI
警告	2005-...	9:18:31	EventSystem	(54)	4353	N/A	DIGI
警告	2005-...	9:18:31	EventSystem	(54)	4356	N/A	DIGI
警告	2005-...	9:18:31	EventSystem	(52)	4353	N/A	DIGI
警告	2005-...	9:18:31	EventSystem	(52)	4356	N/A	DIGI
警告	2005-...	9:18:31	EventSystem	(54)	4353	N/A	DIGI
警告	2005-...	9:18:31	EventSystem	(52)	4356	N/A	DIGI
警告	2005-...	9:18:31	EventSystem	(54)	4353	N/A	DIGI
警告	2005-...	9:18:31	EventSystem	(52)	4356	N/A	DIGI
警告	2005-...	9:18:31	EventSystem	(54)	4353	N/A	DIGI
警告	2005-...	9:18:28	SecurityCenter	无	1800	N/A	DIGI
警告	2005-...	9:14:11	EventSystem	(54)	4353	N/A	DIGI
警告	2005-...	9:14:11	EventSystem	(52)	4356	N/A	DIGI
警告	2005-...	9:14:11	EventSystem	(54)	4353	N/A	DIGI

STEP4 检查安全性日志

安全性日志主要记录与计算机安全性密切相关的信息，如用户登入系统、建立及删除文件等，在追踪黑客时，应重点检查安全性日志，因为黑客在计算机中执行的操作一般会记录在此。

① 安全性日志



STEP5 检查系统日志

系统日志主要记录 Windows 操作系统本身的事件，如硬件驱动程序加载失败、系统发生错误等。

① 系统日志

类型	日期	时间	来源	分类	事件	用户	计算机
错误	2005-...	14:4...	DDOM	无	1...	SYSTEM	DIGI
信息	2005-...	14:4...	Service Cont...	无	7036	N/A	DIGI
信息	2005-...	14:4...	Service Cont...	无	7036	N/A	DIGI
信息	2005-...	14:4...	Service Cont...	无	7035	SYSTEM	DIGI
信息	2005-...	14:4...	Service Cont...	无	7036	N/A	DIGI
信息	2005-...	14:4...	Service Cont...	无	7035	SYSTEM	DIGI
信息	2005-...	14:4...	Service Cont...	无	7036	N/A	DIGI
信息	2005-...	14:4...	Service Cont...	无	7035	SYSTEM	DIGI
信息	2005-...	14:4...	Service Cont...	无	7036	N/A	DIGI
信息	2005-...	14:4...	Service Cont...	无	7036	N/A	DIGI
信息	2005-...	14:4...	Service Cont...	无	7036	N/A	DIGI
信息	2005-...	14:4...	Service Cont...	无	7035	SYSTEM	DIGI
信息	2005-...	14:4...	Service Cont...	无	7036	N/A	DIGI
信息	2005-...	14:4...	Service Cont...	无	7035	SYSTEM	DIGI
信息	2005-...	14:4...	Service Cont...	无	7036	N/A	DIGI
信息	2005-...	14:4...	Service Cont...	无	7036	N/A	DIGI
信息	2005-...	14:4...	Service Cont...	无	7035	SYSTEM	DIGI
信息	2005-...	14:4...	Service Cont...	无	7036	N/A	DIGI
信息	2005-...	14:4...	Service Cont...	无	7035	SYSTEM	DIGI
信息	2005-...	14:4...	Service Cont...	无	7036	N/A	DIGI
信息	2005-...	14:4...	Service Cont...	无	7035	SYSTEM	DIGI
信息	2005-...	14:4...	Service Cont...	无	7036	N/A	DIGI
信息	2005-...	14:4...	Service Cont...	无	7035	SYSTEM	DIGI
信息	2005-...	11:4...	Sub	无	3019	N/A	DIGI
信息	2005-...	11:4...	Sub	无	3019	N/A	DIGI
信息	2005-...	11:4...	Sub	无	3019	N/A	DIGI
信息	2005-...	11:4...	Service Cont...	无	7036	N/A	DIGI
信息	2005-...	11:4...	Service Cont...	无	7036	N/A	DIGI
信息	2005-...	11:4...	Service Cont...	无	7035	SYSTEM	DIGI
信息	2005-...	11:4...	Service Cont...	无	7036	N/A	DIGI
信息	2005-...	11:4...	Service Cont...	无	7035	SYSTEM	DIGI
信息	2005-...	11:4...	Service Cont...	无	7036	N/A	DIGI
信息	2005-...	11:4...	Service Cont...	无	7036	N/A	DIGI
信息	2005-...	11:4...	Service Cont...	无	7035	SYSTEM	DIGI
信息	2005-...	11:4...	Service Cont...	无	7036	N/A	DIGI
信息	2005-...	11:4...	Service Cont...	无	7035	SYSTEM	DIGI
信息	2005-...	11:4...	Service Cont...	无	7036	N/A	DIGI
信息	2005-...	11:4...	Service Cont...	无	7035	SYSTEM	DIGI
信息	2005-...	11:4...	Service Cont...	无	7036	N/A	DIGI

STEP6 检查日志详细信息

在检查日志过程中，用户如需检查某项事件记录的详细信息，只需双击对应的项目即可。

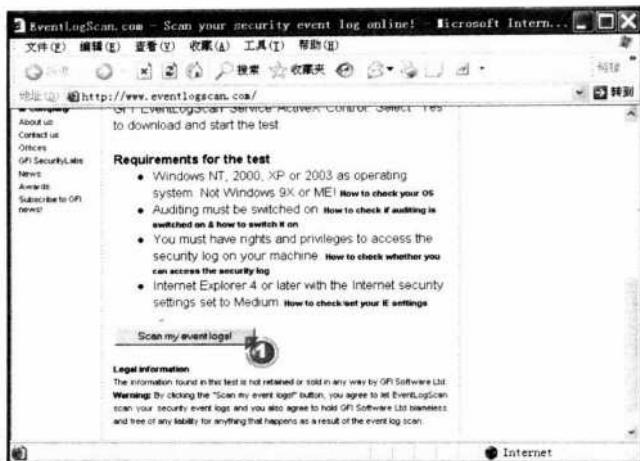


8.3.2 免费的在线日志扫描

Windows 的事件查看器会将系统中的事件全部记录下来，因此日志中存储着大量垃圾信息，因此在实际应用过程中人们往往会先通过各种方法筛选日志，将一些不重要的记录清除掉，以减轻分析日志的工作量。在此笔者介绍一个网站，它可以为用户筛选出日志中较重要的记录，而且这项服务是完全免费的。此网站的网址为 <http://www.eventlogscan.com/>。

STEP ① 执行扫描功能

打开网页后，通过网页最下方的【Scan my event logs!】按钮即可执行扫描操作。



① 单击【Scan my event logs!】按钮，执行扫描操作

STEP2 安装 ATL Explorer 控件

ATL Explorer 是一个支持扫描功能的 ActiveX 控件，对计算机不会造成危害，单击【安装】按钮确认安装。

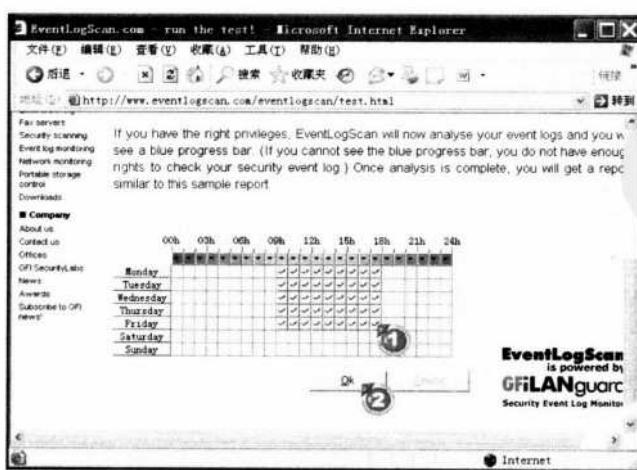
① 单击【安装】按钮



STEP3 选择使用计算机的时间段

在正式开始扫描之前，用户需要输入自己平时会在什么时候使用计算机，输入这些信息的目的是确认哪些登入计算机的行为是可疑的。例如，某用户一般只在日间使用计算机，然而日志中却有一次凌晨登入的记录，则此次登入有可能是黑客所为。

① 选择使用计算机的时间
② 单击【Ok】按钮



**STEP 4 检查扫描进度**

单击【Ok】按钮后，立即执行扫描，在扫描过程中会显示扫描的进度。

① 扫描的进度**STEP 5 检查扫描结果**

扫描的结果会显示在【Critical security events】和【High security events】两个表格中，前者显示重要的安全事件记录，后者则显示一般性的事件记录。用户应重点检查【Critical security events】表格中的记录。

Critical security events							
Date	Time	Event ID	Event Short Description	EventType	Classification	Source	User
12/15/2003 18:04:23	540	Successful Network Logon	Success audit	Critical	Security	ANONYMOUS LOGON	PT
12/15/2003 18:12:12	680	Account Used for Logon	Success audit	Critical	Security	SYSTEM	PT
12/15/2003 18:26:23	540	Successful Network Logon	Success audit	Critical	Security	ANONYMOUS LOGON	PT
12/16/2003 08:47:48	680	Account Used for Logon	Success audit	Critical	Security	SYSTEM	PT
12/16/2003 08:47:57	540	Successful Network Logon	Success audit	Critical	Security	ANONYMOUS LOGON	PT
12/16/2003 08:50:22	680	Account Used for Logon	Success audit	Critical	Security	SYSTEM	PT
12/16/2003 10:06:27	540	Successful Network Logon	Success audit	Critical	Security	ANONYMOUS LOGON	PT
12/16/2003 10:38:27	540	Successful Network Logon	Success audit	Critical	Security	ANONYMOUS U2	PT
12/17/2003 08:52:01	680	Account Used for Logon	Success audit	Critical	Security	SYSTEM	PT
12/17/2003 09:51:10	540	Successful Network Logon	Success audit	Critical	Security	ANONYMOUS LOGON	PT
12/17/2003 09:53:29	680	Account Used for Logon	Success audit	Critical	Security	SYSTEM	PT

[Go to top]

High security events							
Date	Time	Event ID	Event Short Description	EventType	Classification	Source	User
12/15/2003 10:34:20	540	Successful Network Logon	Success audit	High	Security	ANONYMOUS LOGON	PT
12/15/2003 12:42:53	680	Account Used for Logon	Success audit	High	Security	SYSTEM	PT

8.3.3 检查 Windows 服务器日志

随着 Internet 的发展，使用宽带网的人越来越多，不少用户都开始用自己的计算机来建立个人网站或 FTP 服务器，而 Windows XP 自带的 IIS (Internet Information Services) 由于简单易用，因此成为架设服务器首要考虑的软件。

由于服务器会长期【暴露】在 Internet，因此受黑客攻击的可能性也大幅增加，为此 IIS

也提供了日志功能，用户可以通过日志搜索黑客入侵的踪迹。但是，Windows XP 并未为 IIS 提供专用的日志检查程序，因此用户需要手动打开日志文件进行检查。

STEP1 打开存储日志的文件夹

IIS 的服务器日志存储在系统分区的【WINDOWS\system32\Logfiles】文件夹中，在此文件夹中一般会包含两个文件夹，其中【MSFTPSVC1】文件夹用于存储 FTP 服务器的日志文件，【W3SVC1】文件夹用于存储 Web 服务器的日志文件。

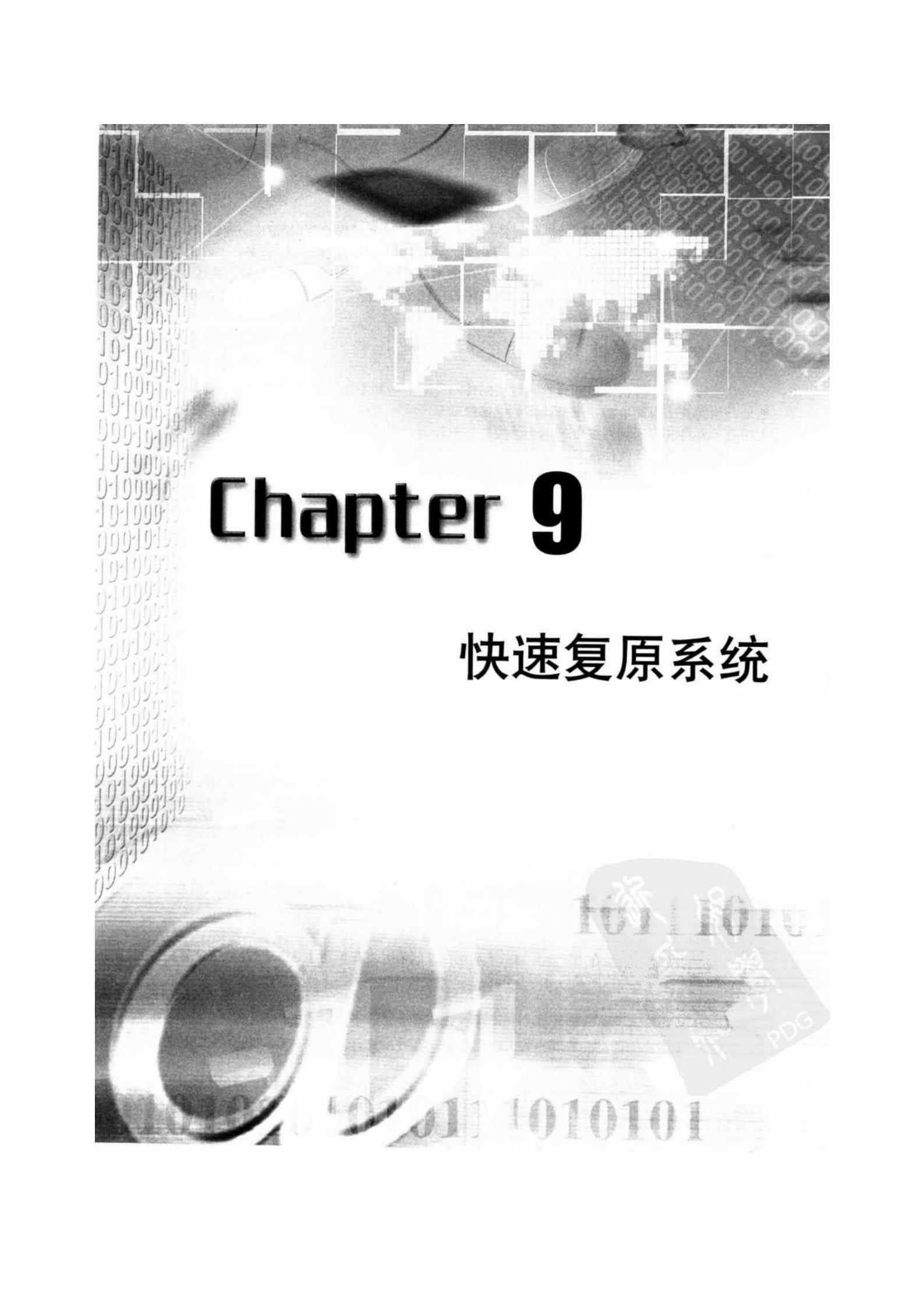


① 打开存储文件夹

STEP2 检查日志文件

在【MSFTPSVC1】及【W3SVC1】文件夹中，每天的日志都会存储成一个 Log 文件，并以日期作为文件名称，用户要检查某天的记录时，只需双击日志文件即可。





Chapter 9

快速复原系统

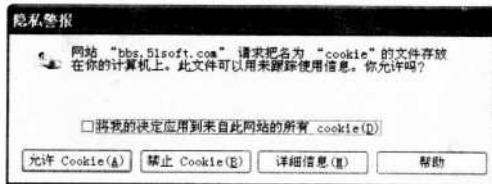


用户在浏览网页或安装软件时，经常会在计算机中留下各种垃圾文件，甚至是恶意的程序，例如一些网站将间谍程序存储在用户的计算机里，用于收集用户的私人信息。此外，一些木马程序及病毒会修改计算机的配置文件，当用户清除木马及病毒后，系统文件也会随之损坏。

面对系统的垃圾文件、间谍软件以及损坏的系统文件，除了重装系统外，也可以采用快速复原系统的方法。

9.1 删除间谍软件

几乎每一位计算机用户都有收到垃圾邮件的经验，但却不知道如何泄漏了自己的邮件地址。原因其实很简单，在每台计算机中都隐藏着一些小程序，它们会随时记录用户的私人信息，并将其发送到网络上。由于这类软件的行为与间谍窃取情报的行为极为相似，因此它们也被称为间谍软件，其中最常见的例子就是浏览器中的Cookie。



因为间谍软件的存在，致使许多用户的私人信息在不知不觉中被发送到网络上，而防止间谍软件最佳的方法就是通过专业的工具程序将其删除。

9.1.1 间谍软件简介

由于间谍软件一般都不会破坏用户的系统及数据，其危害程度远不及病毒与木马，因此大部分用户一般都不会注意它们的存在，部分网络安全软件及杀毒软件甚至认为其是合法的程序。

● 间谍软件的行为

间谍软件最主要的作用就是搜集用户的信息，并将这些信息发送到指定的网站上。一些较【正直】的间谍软件一般只会搜集一些对用户无明显影响的信息，如浏览网站的习惯、经常浏览的网站等，典型的代表就是浏览器的Cookie；而另一些间谍软件则会搜集更多的私人信息，例如 Xupiter 间谍软件会搜集用户的浏览器类型及版本、屏幕分辨率、时区、计算机上安装的软件版本，甚至是用户的姓名、国家、邮政编码等。

一些间谍软件不仅会收集用户信息，而且还会自动打开广告窗口、修改浏览器首页、将网站加入到【收藏夹】中，甚至通过监视用户按键以盗取账户、密码等用户的私人信息。

● 间谍软件的传播

大部分间谍软件都是在用户不知情或未明确同意的情况下安装到计算机中的，从这个意义上说，间谍软件与木马程序及病毒颇有相似之处。常见的间谍软件传播途径主要有以下几种：

● 集成在软件中

网络上流传着许多免费的软件，其中部分软件在安装时会同时安装间谍软件，开发者就是这样收集用户的信息并将其出售给广告商的。在使用这些软件时，用户就会不知不觉地泄露自己的隐私。

● 包含在网页中

将间谍软件嵌在网页上也是常用的手段之一，用户只要浏览网页，软件就会自动安装到计算机中。

除此之外，间谍程序还有可能通过电子邮件、聊天软件等途径传播，甚至会利用操作系统的漏洞进行传播。从某种意义上说，间谍软件的传播方式与木马程序及病毒相比也毫不逊色。

9.1.2 删除间谍软件

通过前面的介绍，大家对间谍软件已经有了一个大概的认识，为了确保自己的隐私不会泄漏，最好的方法就是通过专门的软件将隐藏在计算机中的间谍软件全部删除。目前，较流行的清除间谍软件的工具主要有 Ad-aware、SpyBot Search & Destroy、AluriaSpyware Eliminator 等，下面将以 Ad-aware 为例介绍如何删除间谍软件。

● 安装 Ad-aware

Ad-aware 是一套简单易用的间谍软件清除程序，共分为 3 个版本：个人版、增强版及专业版，其中个人版是免费的，而增强版与专业版则需要付费使用。

个人版在 Ad-aware 的 3 个版本中功能最简单，但对于一般用户而言已经足够。由于是免费的软件，因此用户可以在各下载网站中轻易找到这个软件。

软件小档案

软件名称：Ad-aware

版本：4.55

官方网站：<http://www.lavasoft.de/>

其他下载网址：<http://dl.163.com/html/3/3996.html>

软件类型：共享试用

Ad-aware 的安装步骤非常简单，用户只要按照向导的提示一步步执行操作即可完成。

STEP 1 执行安装程序

从网站下载文件后，双击这个文件即可开始安装。



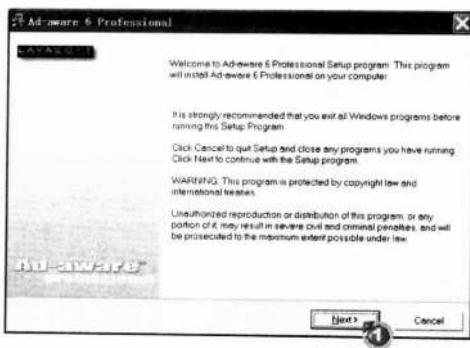
① 双击安装文件



STEP 2 跳过欢迎界面

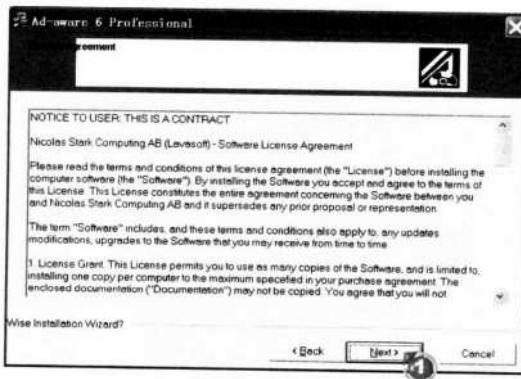
单击【Next】按钮跳过欢迎界面，继续执行安装。

① 单击【Next】按钮



STEP 3 接受授权协议

阅读授权协议后，单击【Next】按钮继续安装，如果用户不接受授权协议，可单击【Cancel】按钮结束安装。



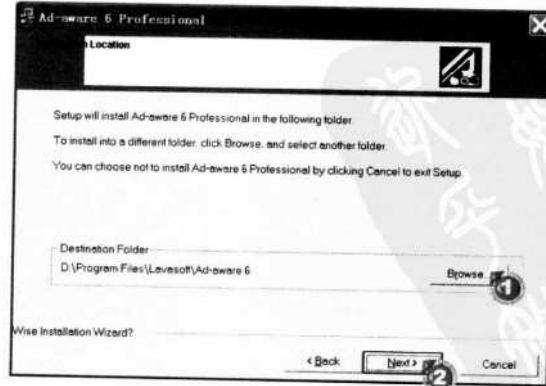
① 单击【Next】按钮

STEP 4 选择安装路径

选择一个路径用于安装 Ad-aware 程序，一般情况下采用默认值即可。

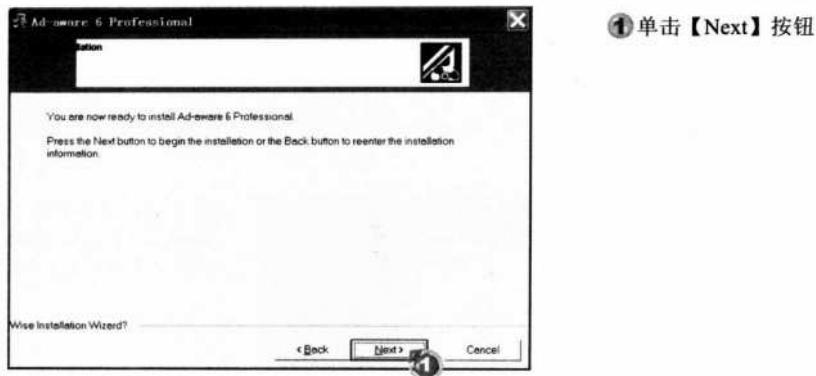
① 单击【Browse】按钮，
选择安装路径

② 单击【Next】按钮

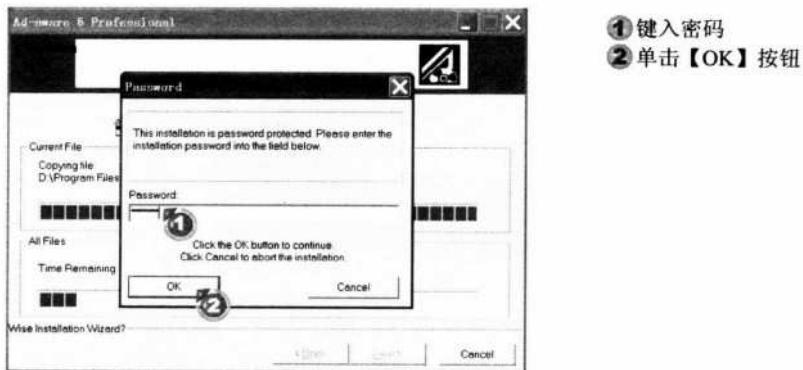


STEP5 开始安装

单击【Next】按钮开始安装，如果希望结束安装可单击【Cancel】按钮。

**STEP6** 键入密码

在弹出的对话框中键入密码，单击【OK】按钮后，安装向导开始复制文件到硬盘中，在安装过程中，会显示安装的进度。

**STEP7** 结束安装程序

安装完成后，单击【Finish】按钮结束安装。

① 单击【Finish】按钮



● 清除间谍软件

安装完成后，用户即可通过 Ad-aware 程序来清除计算机中隐藏的间谍软件。Ad-aware 提供了多种扫描方式，用户既可以完整地扫描整个系统，也可以自定义扫描某些文件夹。

STEP1 执行 Ad-aware 程序

安装向导会在【开始】菜单中添加程序的快捷方式，通过此快捷方式可快速打开 Ad-aware 程序。

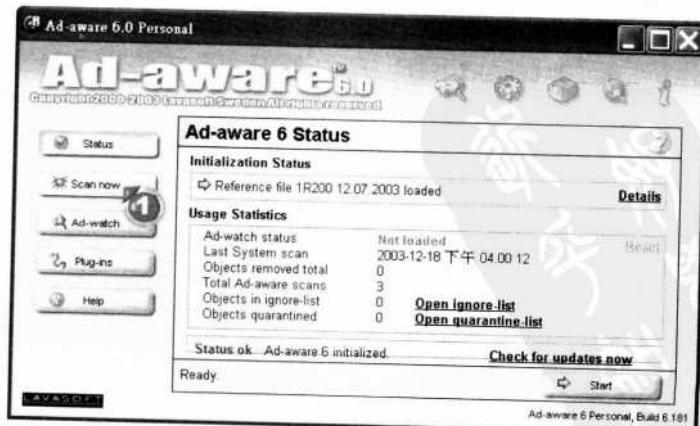


① 依次选择【开始】→【所有程序】→【Lavasoft Ad-aware 6】→【Ad-aware 6】选项

STEP2 执行扫描功能

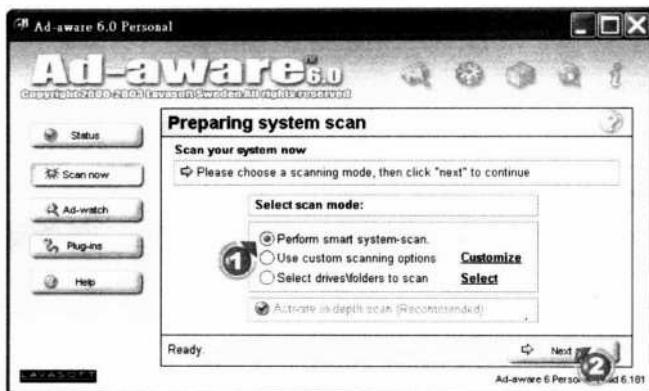
Ad-aware 的界面非常简洁，主要功能都分布在窗口左边的按钮及右上方的图标中，单击其中的【Scan now】按钮可执行扫描操作，以清除隐藏的间谍软件。

① 单击【Scan now】按钮，
执行扫描操作



STEP3 选择扫描方式

Ad-aware 提供了 3 种扫描方式，建议选择【Perform smart system-scan】选项由程序自动执行扫描；如需自定义扫描的文件夹，可选择【Select drives\folders to scan】选项；此外，高级用户也可选择【Use custom scanning options】选项，并单击【Customize】链接文字详细设置扫描命令。

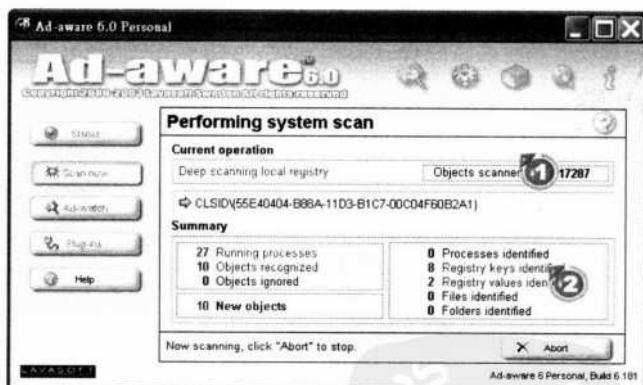


- ① 选择【Perform smart system-scan】选项
② 单击【Next】按钮

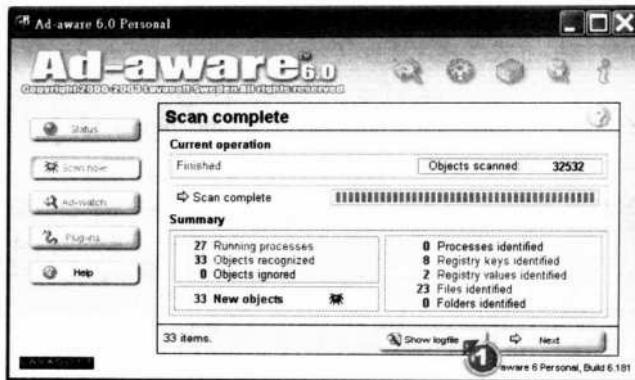
STEP4 检查扫描进度

Ad-aware 扫描所需时间较长，在扫描过程中，程序会显示正在扫描的对象以及已经扫描的文件数量，用户如需在扫描过程中中断扫描，可单击【Abort】按钮。

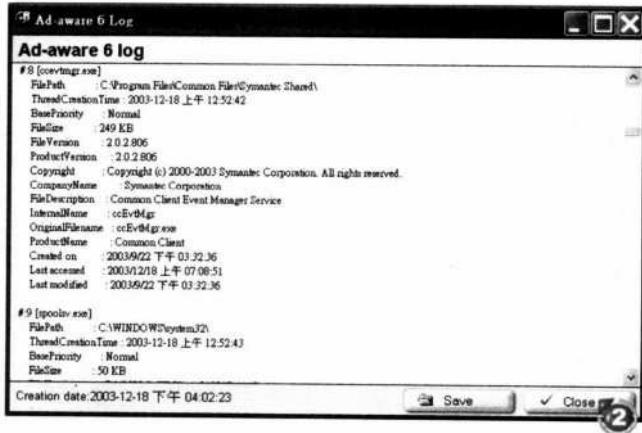
- ① 正在扫描的对象
② 已扫描的文件数量

**STEP5** 检查扫描结果

扫描结束后，程序会显示扫描结果，如需检查更详细的信息，可单击【Show logfile】按钮打开【Ad-aware 6 Log】窗口，检查完毕后可单击【Close】按钮关闭窗口。

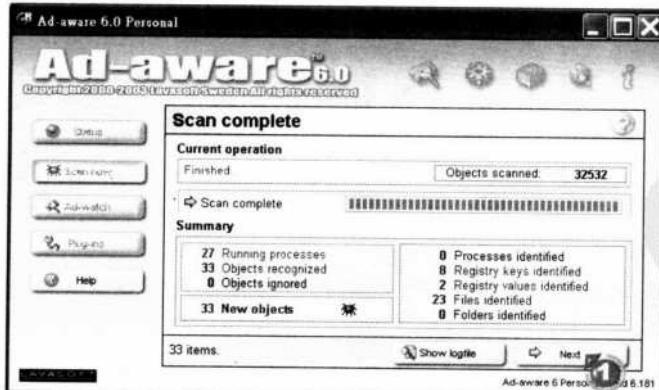


- ① 单击【Show logfile】按钮
- ② 单击【Close】按钮
- ③ 详细的扫描结果



STEP 6 检查需清除的间谍程序

检查结果后，单击【Next】按钮，检查需清除的间谍程序。

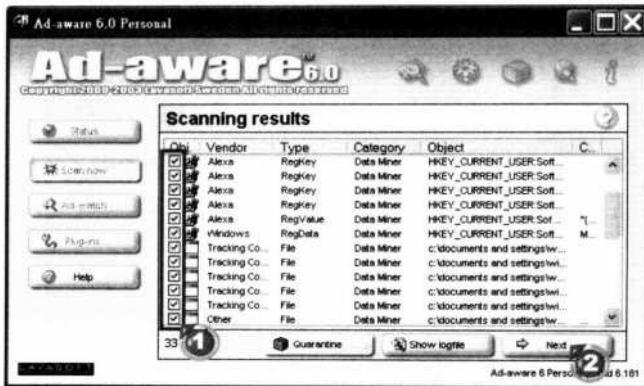


- ① 单击【Next】按钮

STEP 7 选择要清除的间谍程序

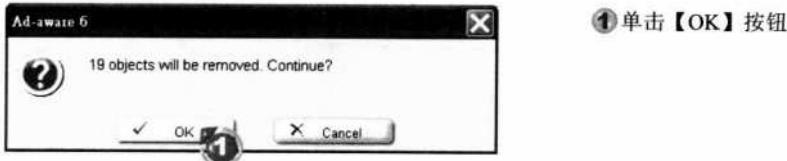
在【Scanning results】栏中列出了计算机中发现的间谍程序，选择要清除的程序后单击【Next】按钮。

- ① 选择要清除的程序
 ② 单击【Next】按钮



STEP 8 确认清除

在【Ad-aware 6】对话框中，单击【OK】按钮，确认清除间谍程序。



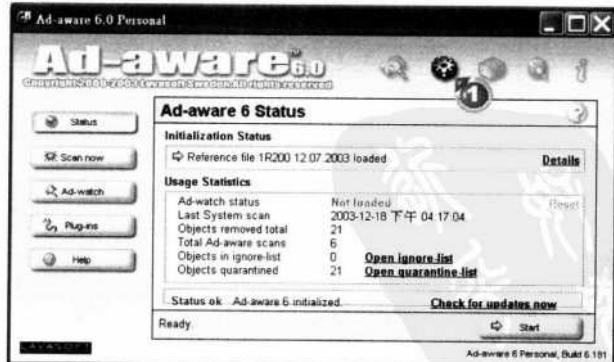
● 设置扫描选项

Ad-aware 提供了多种扫描设置，合理地设置扫描选项可以提高扫描的效率及准确性。例如，当用户要单独扫描系统记录时，可选择【Scan registry】和【Deep Scan registry】选项。

STEP 1 打开【Scan Setting】窗口

在程序主窗口中单击 \odot 按钮，打开【Scan Setting】对话框，以便设置扫描选项。

- ① 单击 \odot 按钮

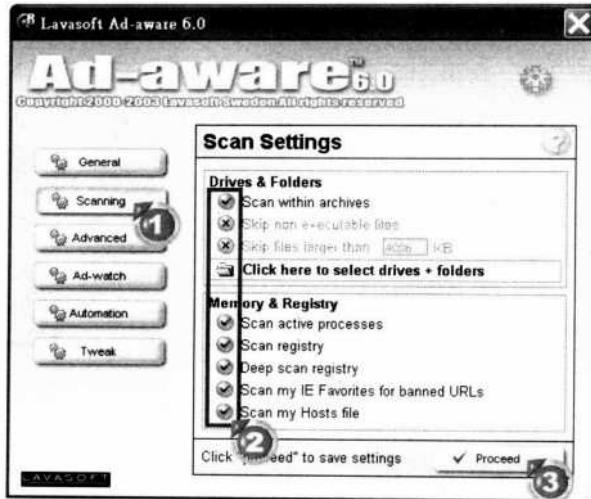


STEP 2 设置要扫描的选项

单击【Scanning】按钮，即可看到关于扫描的设置选项，用户可根据实际需求设



置，设置完成后单击【Proceed】按钮。



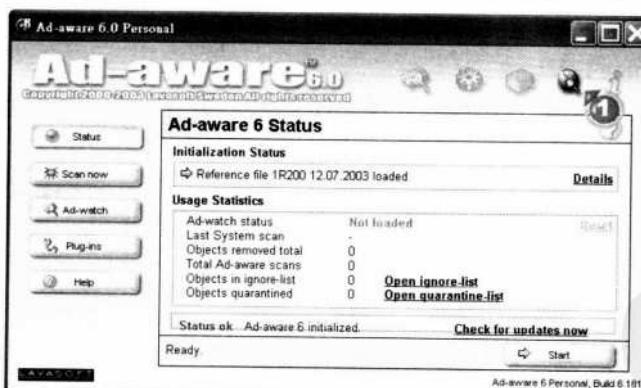
- ① 单击【Scanning】按钮
- ② 选择要扫描的选项
- ③ 单击【Proceed】按钮，完成设置

● 在线更新程序

与木马及病毒类似，间谍软件也在不断更新，因此扫描工具也必须不断更新，以便能清除新出现的间谍软件。Ad-aware 提供了在线更新功能，让用户可以很方便地更新程序。

STEP1 执行在线更新功能

在 Ad-aware 主窗口中，单击 按钮，执行在线更新功能。

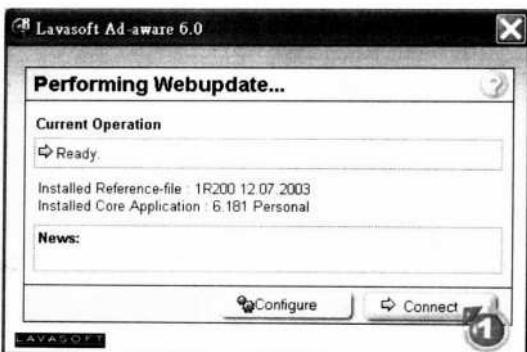


- ① 单击 按钮

STEP2 连接服务器

如果用户是采用 Proxy 方式上网，则需要通过【Configure】按钮设置 Proxy 服务器，否则无法进行更新，而直接连接的用户则可跳过此步骤，直接单击【Connect】按钮连接服务器。

① 单击【Connect】按钮



STEP3 确认下载文件

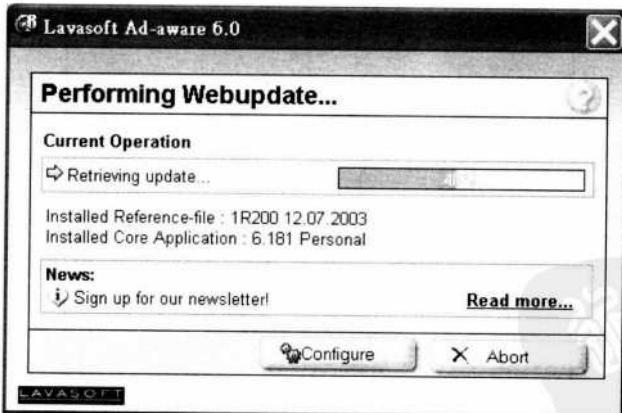
当 Ad-aware 搜索到更新的文件时，会弹出一个对话框询问使用者是否下载并安装此文件，此时单击【OK】按钮即可。



① 单击【OK】按钮

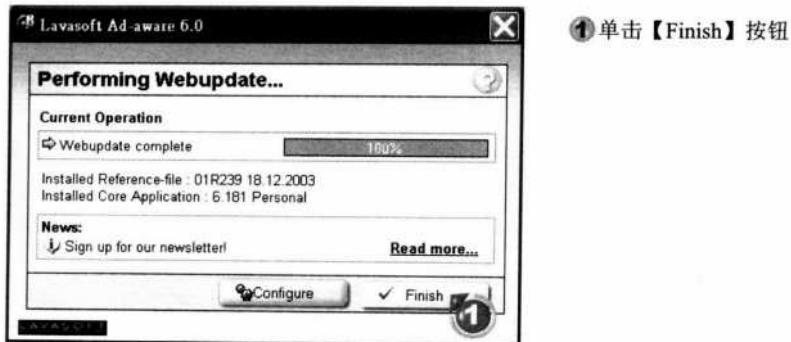
STEP4 检查更新进度

更新程序所需的时间由更新文件的大小及用户的网络连接速度决定，在更新过程中画面上会显示更新的进度，如果用户想中途放弃更新，可单击【Abort】按钮。



STEP5 结束更新程序

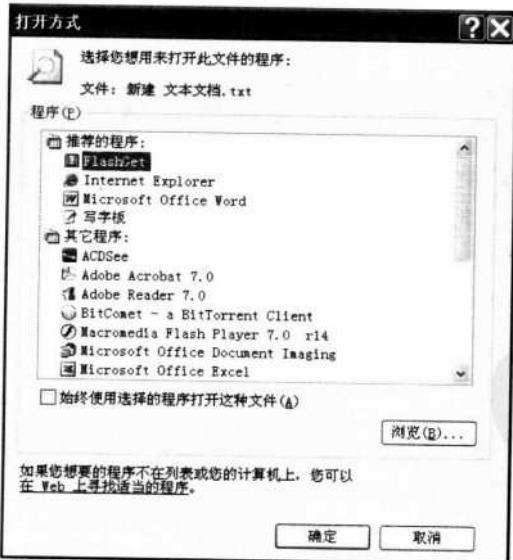
更新完成后，单击【Finish】按钮，结束更新程序。



9.2 还原文件注册类型

部分用户用杀毒软件清除木马程序后，会出现无法打开某类文件的现象，其中最常见的是无法打开记事本文件，这是因为木马程序修改了文件的注册类型：默认状态下，当用户双击扩展名为.txt 的文件时，系统会调用 Windows 自带的记事本程序（Notepad.exe）来打开文件，而一些木马程序则会修改系统的文件注册类型，将.txt 文件的打开方式修改成用木马程序打开。

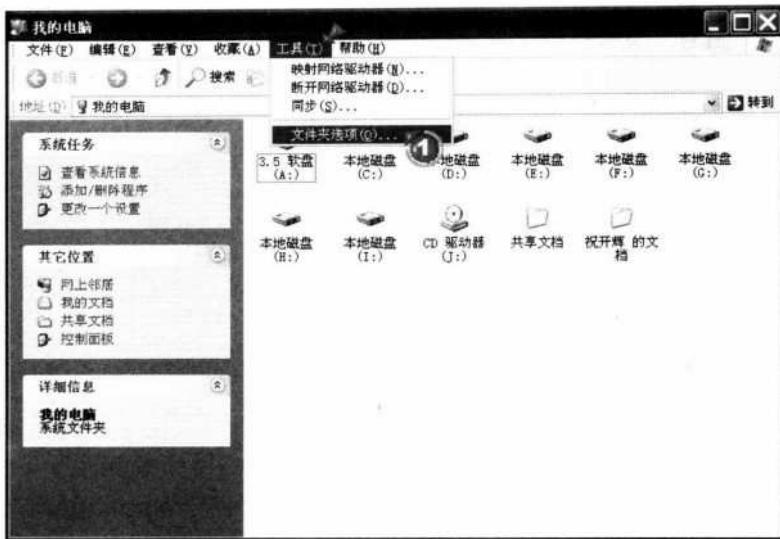
木马程序被清除后，系统由于找不到用于打开.txt 文件的程序，因此就会出现前面所提到的现象。如果遇到这种情形，可以修改文件注册类型，使系统重新以 Notepad.exe 程序来打开.txt 文件。



STEP① 打开【文件夹选项】对话框

在【我的电脑】窗口中，选择【工具】→【文件夹选项】命令，打开【文件夹选项】对话框，以便以后恢复文件注册类型。

① 依次选择【工具】→【文件夹选项】命令



STEP2 打开【编辑文件类型】对话框

在【文件类型】选项卡中可看到系统中全部已注册的文件类型，从中选择要修改的文件类型后，单击【高级】按钮打开【编辑文件类型】对话框。

- ① 选择【文件类型】选项卡
- ② 选择要修改的文件类型
- ③ 单击【高级】按钮



STEP3 打开【编辑这种类型的操作】对话框

在【编辑文件类型】窗口中选择【open】操作，然后单击【编辑】按钮打开【编



辑这种类型的操作】窗口，以便设置打开此文件类型的程序。

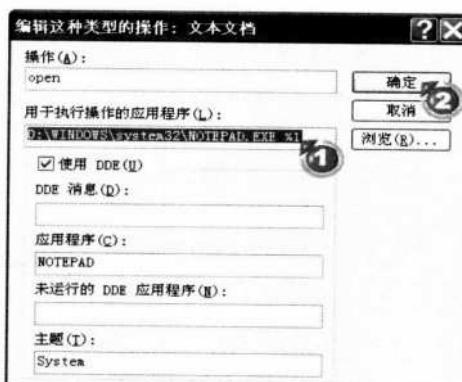


- ① 选择【open】选项
- ② 单击【编辑】按钮

STEP 4 设置执行动作的程序

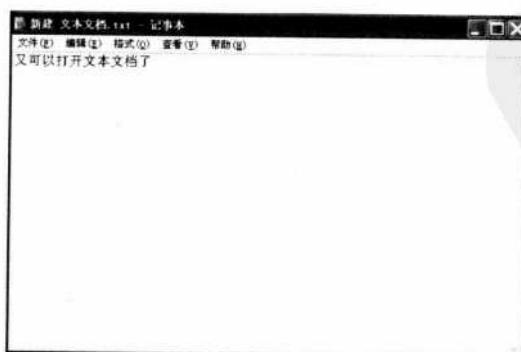
在【用于执行操作的应用程序】栏中，设置打开此文件类型的程序路径。以.txt文件为例，打开.txt文件的程序路径应为【*:\\WINDOWS\\system32\\NOTE PAD.EXE】(*代表系统分区)。

- ① 键入执行动作的程序路径。
- ② 单击【确定】按钮



STEP 5 检查结果

完成设置后，再次双击.txt文件，系统将重新调用记事本程序打开文件。



9.3 还原损坏的文件

一些病毒及木马程序入侵计算机后会把自身与系统文件合并，因此用户在删除木马的同时也可能会导致系统文件损坏。另外，还有某些应用程序在安装过程中也会将部分系统文件换成自己适用的版本，这有可能导致其他应用程序，甚至操作系统本身无法正常工作。当遇到这样的情况时，用户可通过 Windows XP 自带的【Windows 文件保护】功能还原损坏的系统文件。

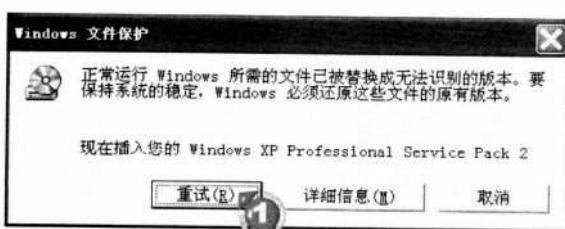
STEP 1 打开【Windows 文件保护】对话框

由于【开始】菜单中没有此程序的快捷方式，因此用户需要在【运行】对话框中键入【sfc.exe /scannow】命令将其打开。



STEP 2 插入 Windows XP 安装光盘

Windows 文件保护功能会逐一检查系统文件是否完整，当发现损坏或遗失的文件时，就会要求用户插入 Windows XP 安装光盘以还原文件。



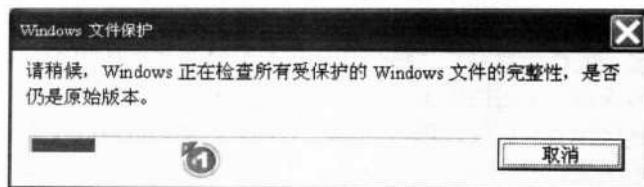
①插入 Windows XP 安装光盘后，单击【重试】按钮



STEP3 检查还原进度

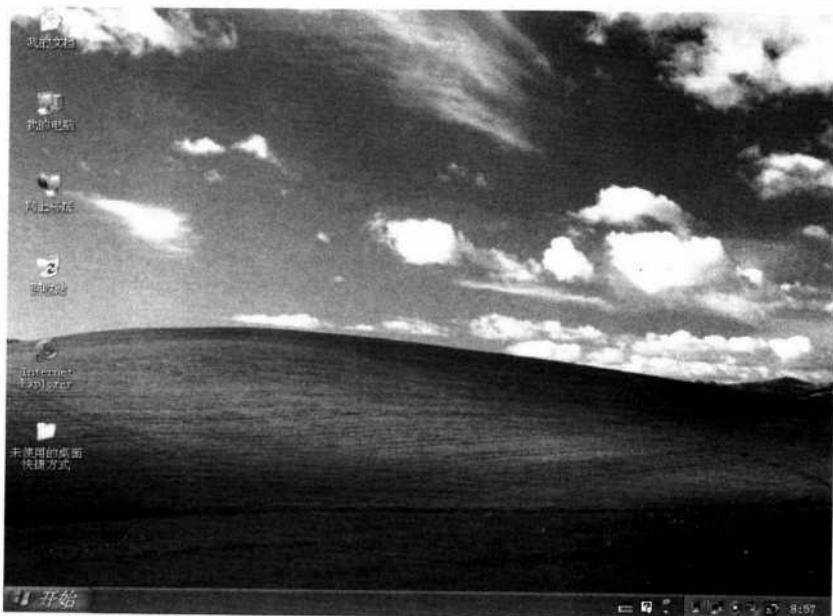
检查及还原系统文件所需的时间较长，窗口中会显示还原的进度。

① 还原的进度



STEP4 重新启动计算机

由于要还原的系统文件大部分正被操作系统使用，因此需要重新启动计算机才能完成还原工作。下图为完成还原后的系统主界面。



Chapter 10

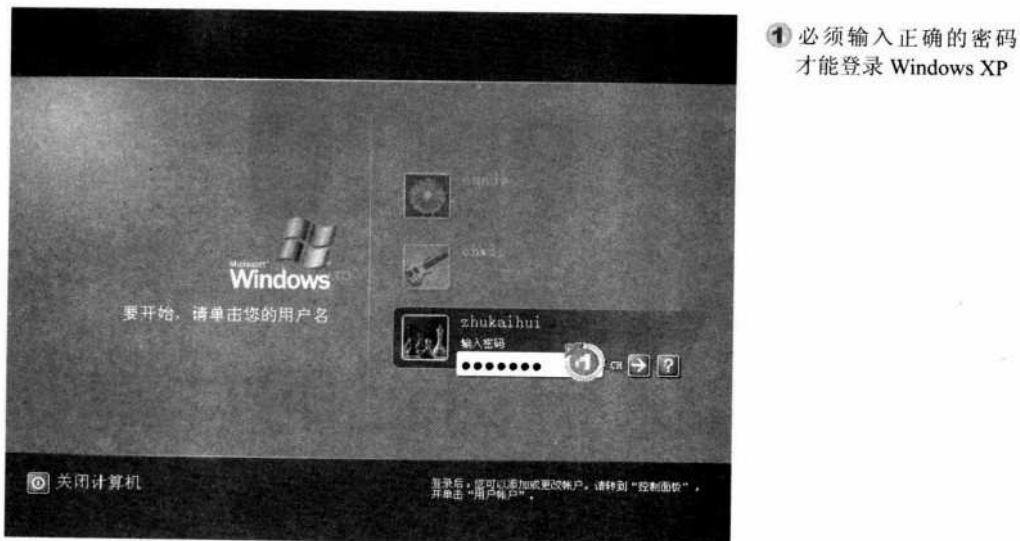
保护自己的计算机



世界上并没有绝对的安全，即使是防护严密的美国国防部也曾有过被黑客入侵的记录，下面将介绍万一黑客突破防火墙的防护成功入侵后，保护计算机中的信息不被窃取的方法。

10.1 密码保卫战

早期的 Windows 操作系统，如 Windows 95、Windows 98 等，其密码形同虚设，用户只要按下 Esc 键就可以避开密码保护，因此这些操作系统几乎毫无任何安全性可言。在 Windows XP 中，微软采用了与 Windows 2000 操作系统类似的登录管理方式，用户必须输入正确的密码后才能进入系统。



Windows XP 的登录密码功能相当实用，但是很多用户因为长期使用 Windows 9x 的原因，对密码设置毫不重视，随意指定一些英文单词或数字就作为密码，甚至根本不设置密码，这些计算机连接到网络上是非常危险的，黑客无须使用任何工具，只要直接用 Windows 自带的【远程桌面连接】程序就能够入侵计算机。由此可见，为了保护计算机的安全，合理地设置 Windows XP 登录密码是不可或缺的。

10.1.1 建立用户密码

在安装 Windows 的过程中，安装向导会要求用户为默认的系统管理员 Administrator 设置密码。但是，在添加其他账户时，默认状态下添加的账户是没有密码的，因此在添加账户之后，应立即为其设置密码。

一些用户习惯用一些简单的数字或字母作为密码，例如生日或者英文单词等，这样的密码是非常不安全的，很容易就会被黑客破解。一般情况下，建议密码至少设置为 8 位以上，且由无意义的字母、数字组合而成。下面将以一个名为【祝开辉】的账户创建密码为例，介绍如何设置用户密码。

STEP1 打开【控制面板】窗口

通过【开始】菜单打开【控制面板】窗口，以便打开【用户账户】窗口。



①依次选择【开始】→【控制面板】选项

STEP2 打开【用户账户】窗口

选择【用户账户】类别目录，打开【用户账户】窗口。

**STEP3** 选择要创建密码的账户

在【用户账户】窗口中列出了这台计算机的所有用户（Administrator 除外），选择要创建密码的账户。

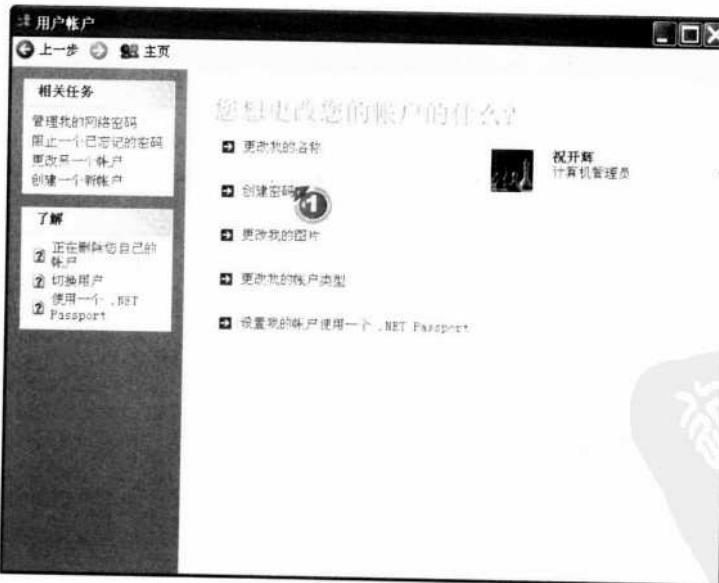


① 选择要创建密码的账户



STEP4 选择【创建密码】选项

选择账户后，画面显示该账户可执行的操作，包括更改我的名称、创建密码、更改我的图片、更改我的账户类型、设置我的账户使用一个.NET Passport等，在此单击【创建密码】选项。

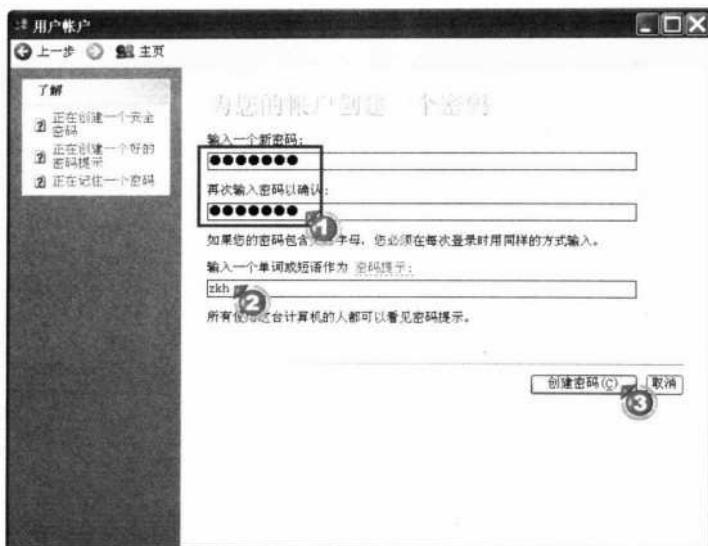


STEP5 创建密码

在输入密码时，为了避免用户无意中输入错误，程序会要求用户重复输入两次，输入完成后，单击【创建密码】按钮即可完成设置。此外，用户还可设置密码提

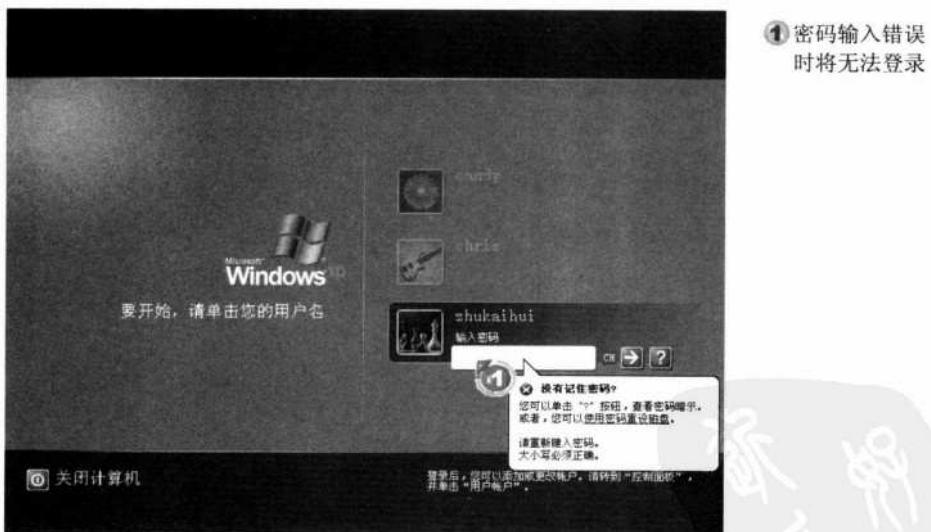
示，以帮助记忆密码，但要注意密码提示切不可与密码有直接关系，以免黑客通过提示猜测密码。

- ① 输入密码
- ② 输入密码提示
- ③ 单击【创建密码】按钮



STEP 6 检查结果

设置密码后，重新启动计算机就会发现必须正确键入密码才能登录系统。



10.1.2 更改密码

从理论上来说，任何密码都是可以被破解的，为了确保密码不会被黑客破解，除了将密码设置得足够复杂外，还应每隔一段时间更改一次密码。更改密码的步骤非常简单，但要注意只有系统管理员才能更改所有账户的密码，而受限制的账户则只能更改自己的



密码。

STEP 1 选择要更改密码的账户

打开【用户账户】窗口后，从中选择要更改密码的账户。

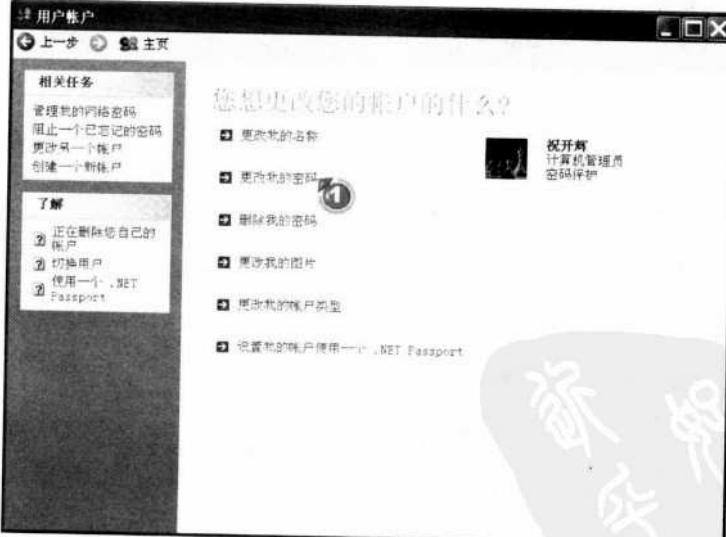


①选择要更改密码的账户

STEP 2 选择【更改我的密码】选项

选择账户后，单击【更改我的密码】选项，进行更改密码的操作。

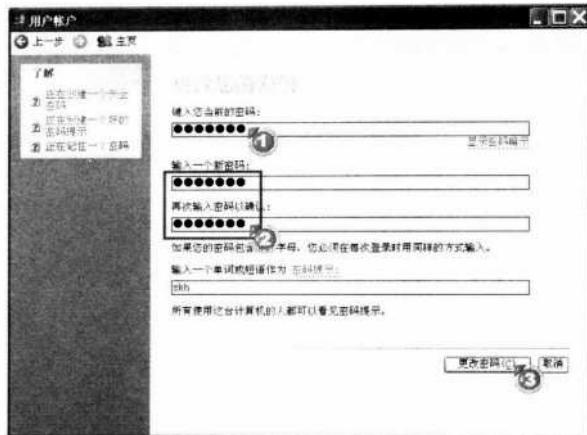
①单击【更改我的密码】选项



STEP 3 设置新密码

设置新密码时，用户必须先输入原来的密码，设置完成后单击【更改密码】按钮即可。

- ① 输入当前的密码
 ② 输入新密码
 ③ 单击【更改密码】按钮



10.1.3 遗忘密码后的解决方法

设置密码可以有效地防止黑客非法登录系统，但如果用户一时不慎遗忘了密码，也同样无法登录系统，为了避免发生这种情况，Windows XP 提供了一项名为【忘记密码向导】的功能，通过这项功能用户可以创建一张特殊的密码重设磁盘，当遗忘密码时就可通过此软盘重新设置密码。

● 创建密码重设磁盘

密码重设磁盘只能由用户自己建立，即使是系统管理员也无法为其他用户创建密码重设磁盘，因此当需要为某个账户建立密码重设磁盘时，首先需要以此账户登录系统，此外还应准备好一张空白的软盘，并检查软驱是否工作正常。

STEP 1 选择账户

在【用户账户】窗口中选择要创建密码重设磁盘的账户，在此必须选择已经登录系统的账户，例如以账户【祝开辉】登录时，就只能选择【祝开辉】账户。



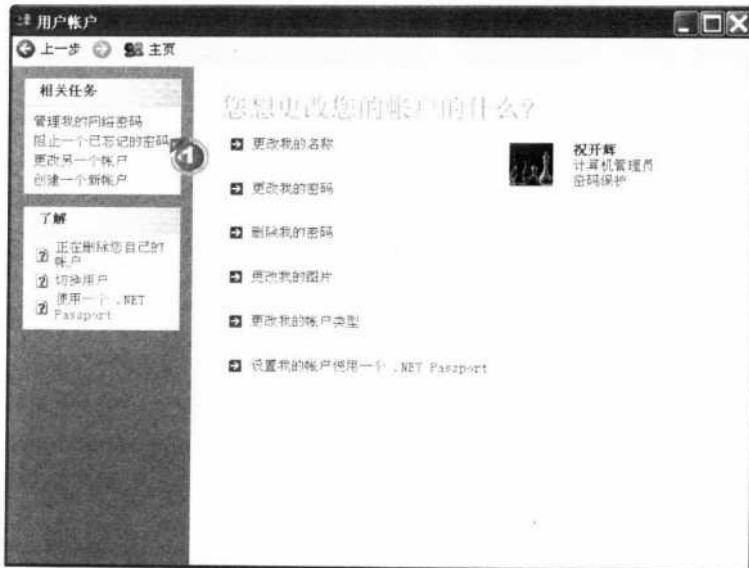
- ① 选择要创建密码重设磁盘的账户



STEP2 打开【忘记密码向导】对话框

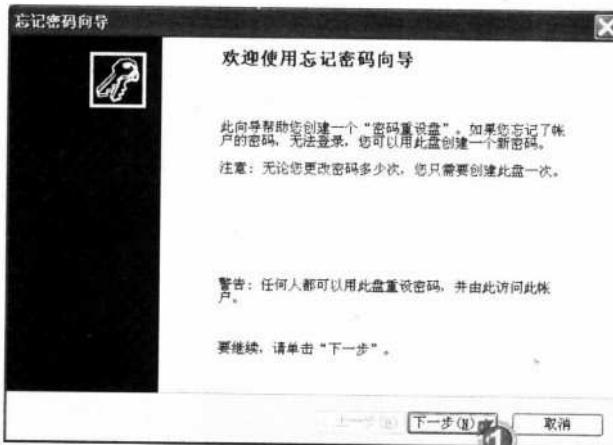
选择账户后，单击【阻止一个已忘记的密码】选项，打开【忘记密码向导】对话框，以便创建密码重设磁盘。

- ① 单击【阻止一个已忘记的密码】选项



STEP3 跳过欢迎界面

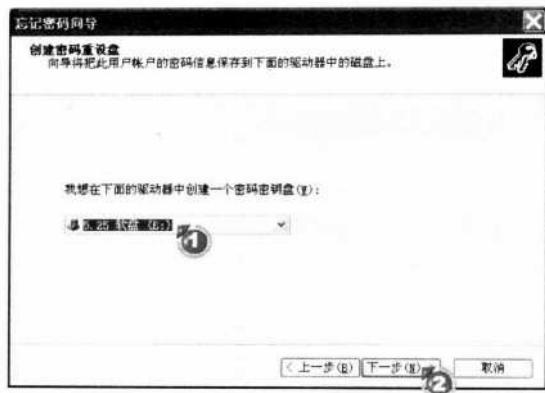
忘记密码向导的欢迎界面会对其功能做一些简单介绍，阅读完毕后单击【下一步】按钮跳过即可。



- ① 单击【下一步】按钮

STEP4 插入软盘

把事先准备的空白软盘插入软驱，选择软盘驱动器后，单击【下一步】按钮继续执行。

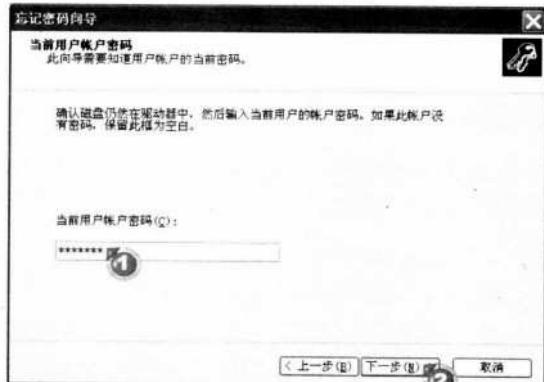


- ① 选择软盘驱动器
- ② 单击【下一步】按钮

STEP 5 输入目前的密码

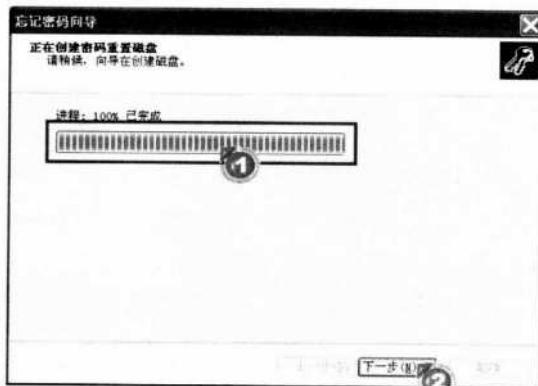
创建密码重设磁盘过程中，向导需要知道目前正在使用的密码，输入密码后单击【下一步】按钮。

- ① 输入目前的密码
- ② 单击【下一步】按钮



STEP 6 查看进程

在创建密码重设磁盘的过程中，界面上会显示已完成的进程，当进程显示【100% 已完成】时，单击【下一步】按钮。

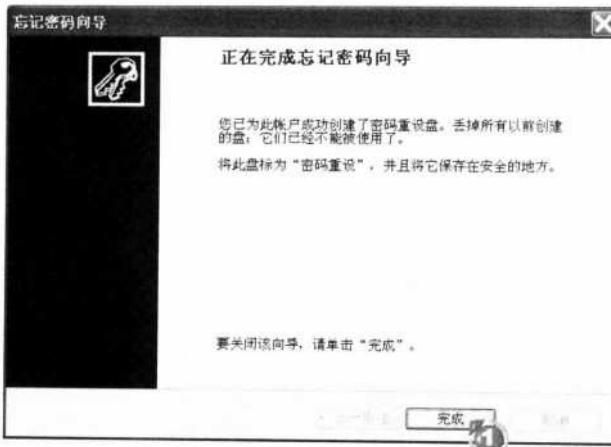


- ① 完成的进程
- ② 单击【下一步】按钮



STEP7 关闭向导

创建密码重设磁盘完成后，单击【完成】按钮，关闭忘记密码向导。



① 单击【完成】按钮

将软盘从软驱中取出并妥善保管，日后遗忘密码时就可以通过这张软盘重设密码。

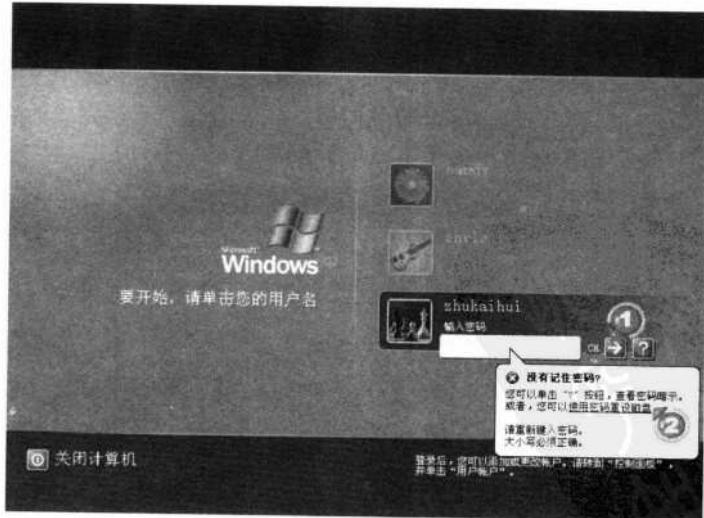
● 重设密码

当不慎遗忘密码无法登录系统时，可先找到之前制作的密码重设磁盘，并根据以下的步骤重设密码。通过密码重设磁盘重设密码时，用户的其他信息不会受到任何影响。

STEP1 打开【重设密码向导】对话框

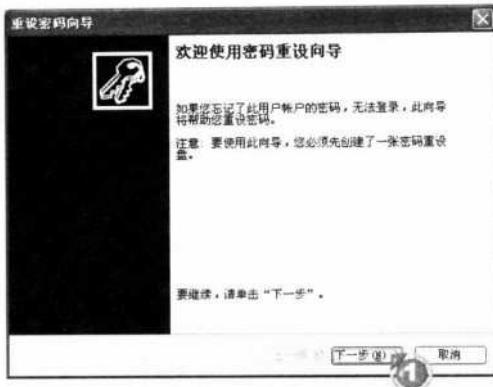
在登录界面中选择遗忘密码的账户后，单击**按钮**，然后单击【使用密码重设磁盘】链接文字打开【重设密码向导】对话框。

- ① 单击**按钮**
- ② 单击【使用密码重设磁盘】链接文字



STEP2 跳过欢迎界面

单击【下一步】按钮，跳过密码重设向导的欢迎界面。

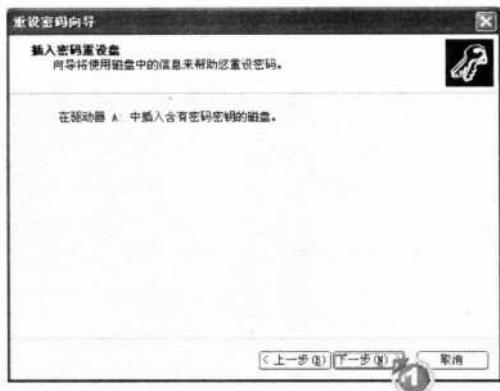


① 单击【下一步】按钮

STEP3 插入密码重设磁盘

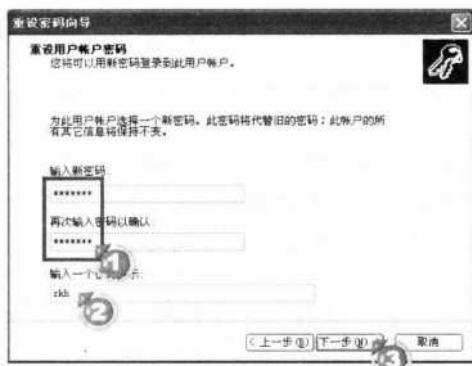
将事前准备的密码重设磁盘插入软驱，然后单击【下一步】按钮。

① 插入密码重设磁盘后，单击【下一步】按钮



STEP4 输入新密码

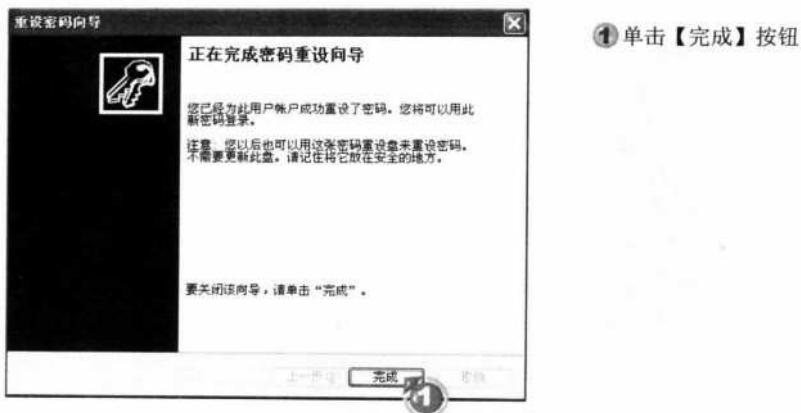
密码重设向导允许用户直接输入新密码，且不会影响用户的其他信息。



① 输入新密码
② 输入密码提示
③ 单击【下一步】按钮

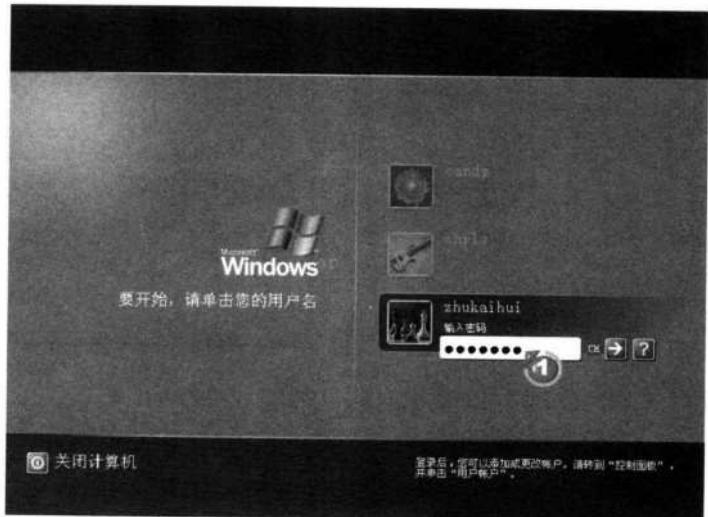
**STEP5** 关闭向导

重设密码完成后，单击【完成】按钮，关闭重设密码向导。

**STEP6** 登录系统

重设密码后，在 Windows 登录界面中输入新密码即可登录系统。

① 输入新密码
登录系统



10.2 加密计算机信息

Windows XP 可采用 NTFS (New Technology File Systems) 格式，使文件不会被未授权的用户存取，但是这种保护功能是以目前正在使用的操作系统为基础的。为了更好地保护计算机中的信息，用户除了正确设置 NTFS 文件权限外，还需要通过其他方法加密计算机信息。

EFS (Encrypting File System) 是微软提供的一项信息加密技术，通过 EFS 加密文件后，未授权的用户即使获得文件，也无法得知文件的内容。EFS 加密、解密的过程都由操作系

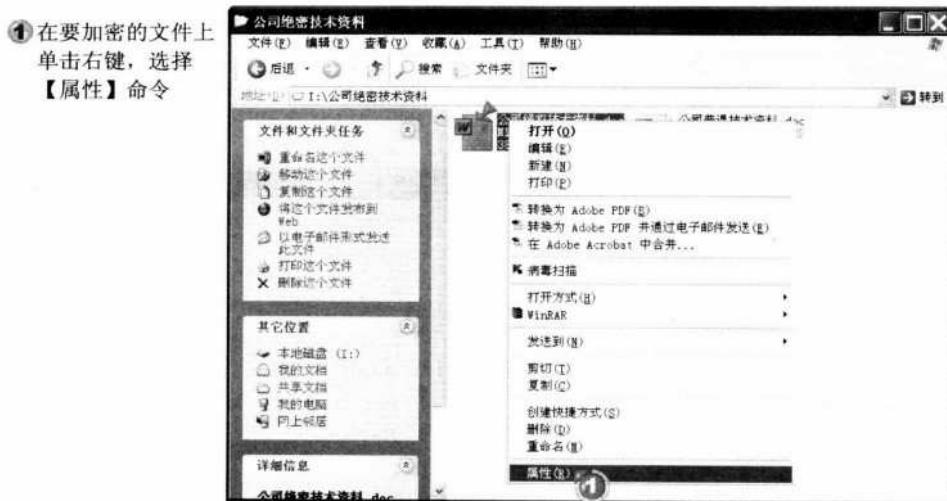
统自动完成，用户在存取加密文件时的步骤与存取一般的文件完全相同。

10.2.1 加密文件夹及文件

使用 EFS 加密文件夹及文件时，首先需要获取一个用于加密文件的证书，此证书可以通过 Internet 的证书机构申请，也可在加密过程中由系统自动产生。下面将使用系统自动产生证书，以加密名为【公司绝密技术资料】的文件为例，说明加密文件夹及文件的方法。

STEP1 打开文件的【属性】对话框

通过右键快捷菜单打开文件的【属性】对话框，以便以后加密文件。



STEP2 打开【公司绝密技术资料.doc 属性】对话框

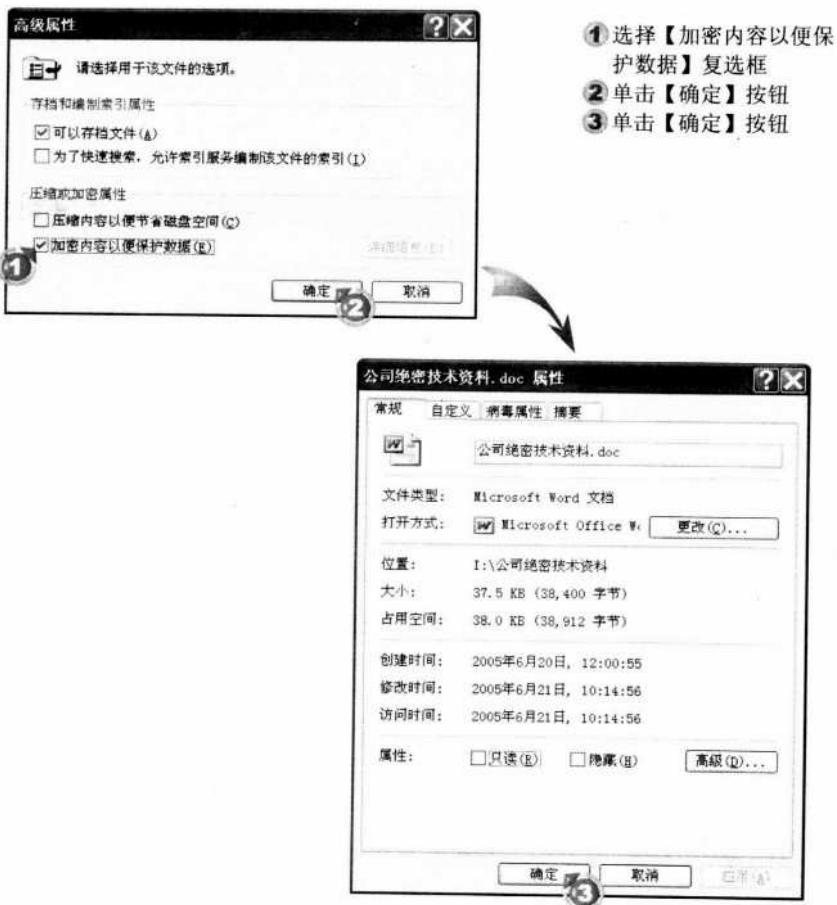
在【公司绝密技术资料.doc 属性】对话框中，单击【高级】按钮，打开【高级属性】对话框。





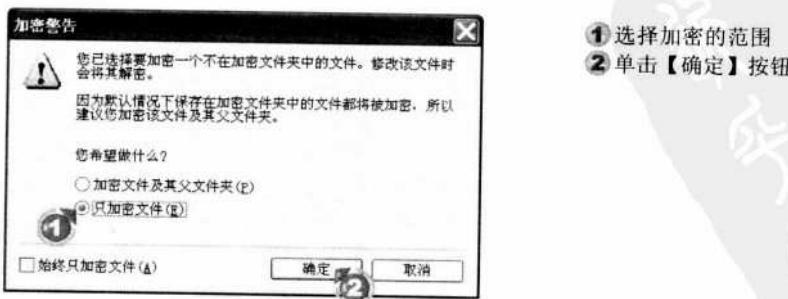
STEP3 设置加密属性

在【高级属性】对话框中，选择【加密内容以便保护数据】复选框即可加密文件，需要注意的是，此项与【压缩内容...】项是互斥的，只能选择其一。



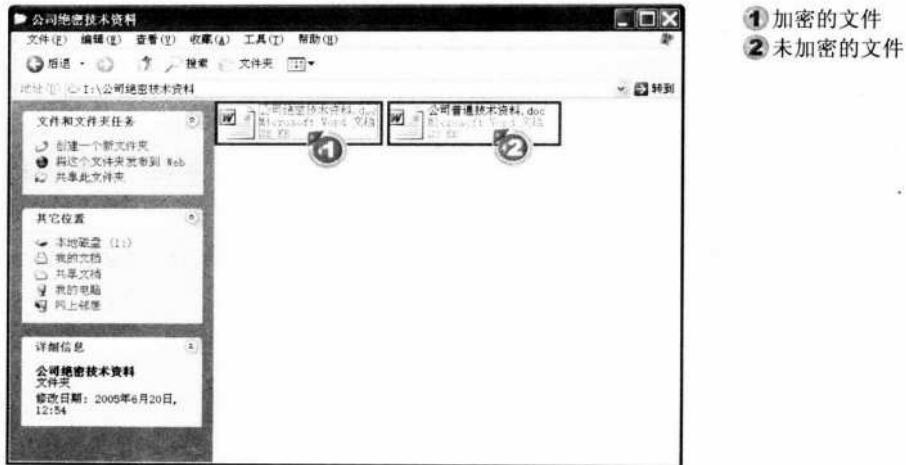
STEP4 选择加密的范围

设置加密属性后，系统会要求用户选择加密的范围，只要根据实际需求选择即可。

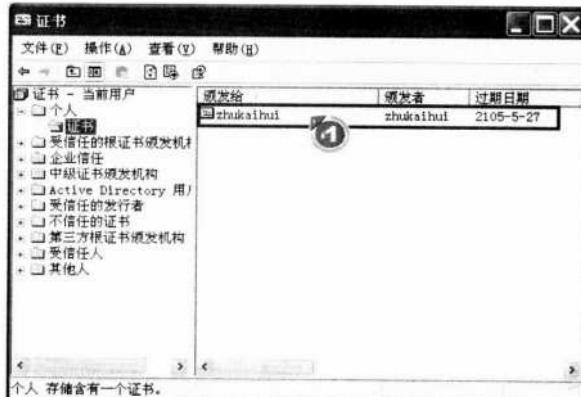


STEP5 查看结果

加密的文件夹及文件会变成绿色，根据颜色的差异用户可以方便地将它们与一般的文件夹及文件区分开。



加密完成后，系统将自动为用户产生一个证书，用户可在【证书】窗口中查看到此证书。注意此证书不可遗失，否则无法打开加密的文件夹及文件。

① 自动产生的证书**补充说明****如何打开【证书】窗口？**

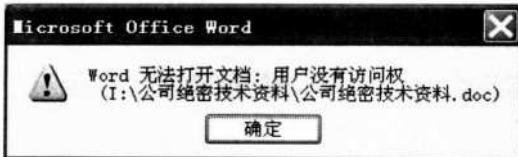
默认状态下，Windows XP 并没有在【开始】菜单中增加打开【证书】窗口的快捷方式，用户需要通过在【运行】窗口中键入【certmgr.msc】命令将其打开。

10.2.2 与其他用户共享加密文件

将文件加密后，只有加密者本人可以存取文件，包括系统管理员在内的其他用户都无法存取。如需与其他用户共享加密文件，则应将其他用户的证书加入允许存取此文件的证

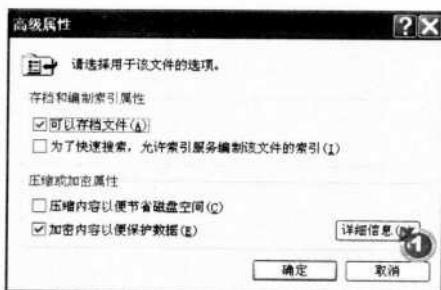


书列表中。



STEP 1 打开加密详细信息对话框

在加密文件的【高级属性】对话框中，单击【详细信息】按钮打开加密详细信息设置对话框，以便添加其他用户证书。



① 单击【详细信息】按钮

STEP 2 添加用户证书

加密详细信息对话框显示了允许存取此加密文件的用户证书，单击【添加】按钮增加其他用户证书。

① 单击【添加】按钮



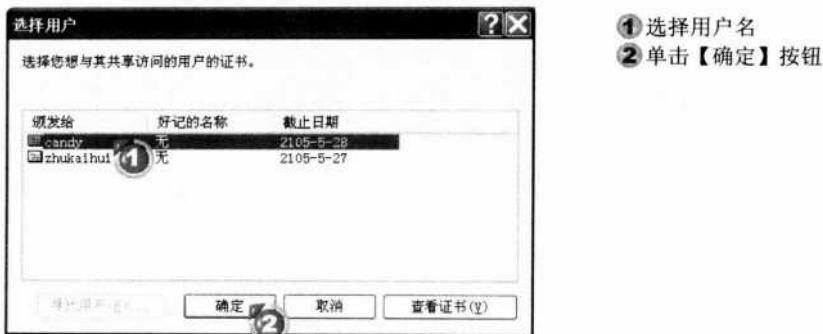
补充说明

找不到用户证书怎么办？

有时用户在添加共享证书时会遇到找不到要添加的用户的情况，这是因为这个用户目前仍未有证书。解决的方法很简单：通知这位用户随意加密某一文件，这样系统就会自动为其产生证书。

STEP3 选择用户名

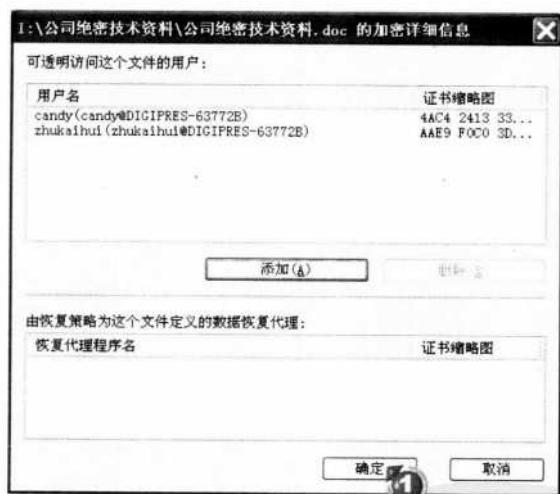
在【选择用户】对话框中会列出这台计算机的所有具备证书的用户，从中选择要共享文件的用户名，然后单击【确定】按钮。



STEP4 完成设置

设置完成后，在加密详细信息对话框中即可看到添加的用户名，查看完毕后单击【确定】按钮关闭窗口。

① 单击【确定】按钮

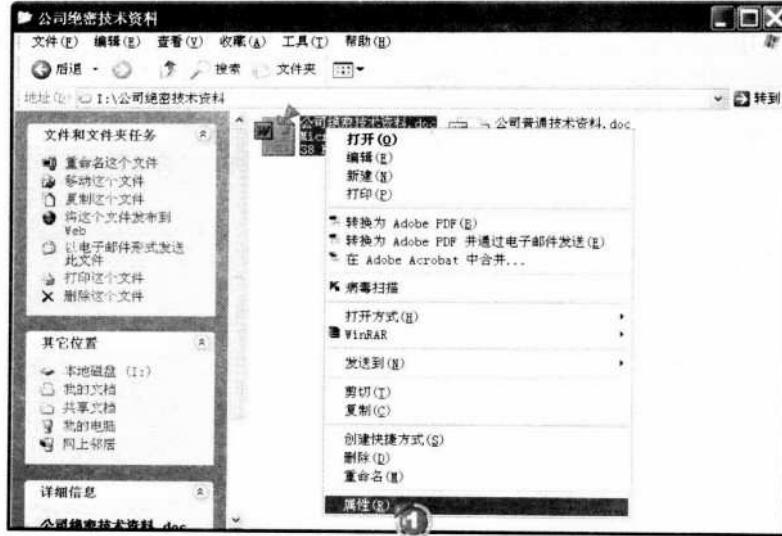


10.2.3 解密文件及文件夹

当用户因为某些原因，已经不再需要加密某文件及文件夹时，只需在文件的【高级属性】对话框中取消选择【加密内容以便保护数据】复选框即可。

STEP1 打开文件的【属性】对话框

通过右键快捷菜单打开解密文件的【属性】对话框，以便打开【高级属性】对话框解密文件。

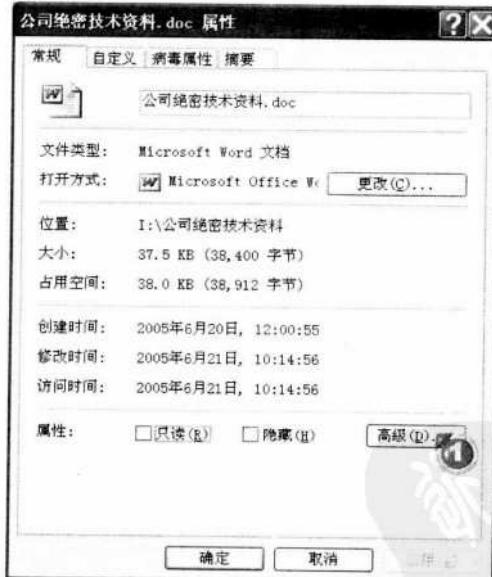


① 在要解密的文件上单击右键，选择【属性】命令

STEP2 打开【高级属性】对话框

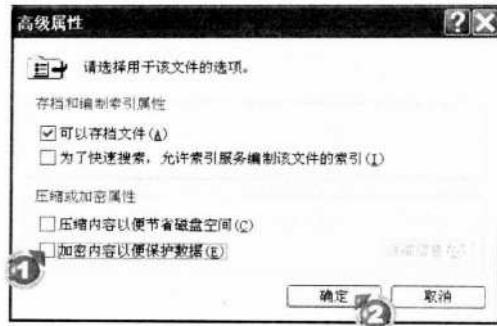
在【属性】对话框中单击【高级】按钮，打开【高级属性】对话框。

① 单击【高级】按钮



STEP3 解密文件

在【高级属性】对话框中取消选择【加密内容以便保护数据】复选框，即可解密文件，设置完成后单击【确定】按钮。

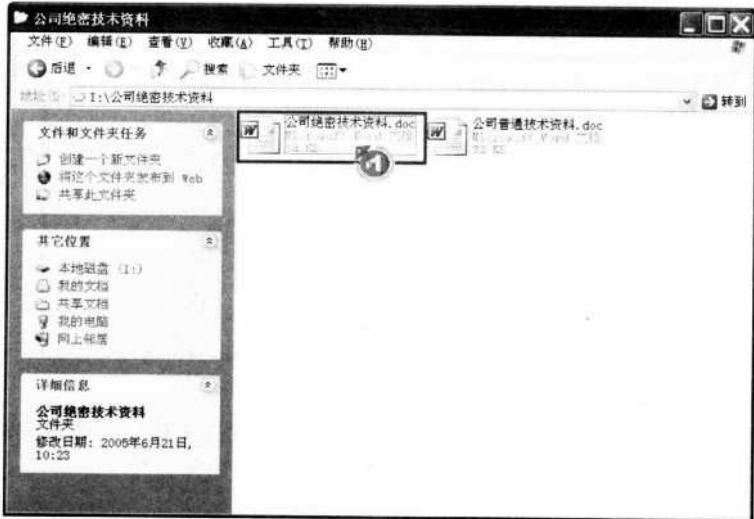


- ① 取消选择【加密内容以便保护数据】复选框
② 单击【确定】按钮

STEP 4 查看结果

设置完成后，将会发现文件由绿色恢复成黑色，此时文件已经成功解密。

① 解密后的文件



10.3 隐藏在磁盘中的文件夹

除了前面介绍的方法之外，实际上还可以用另一种方法来防止黑客窃取信息：隐藏文件夹。将文件加密后，黑客虽然不能存取资料，但仍可看到文件名称，一些水平较高的黑客仍会尝试破解这些加密的文件。因此，对于一些特别重要的信息，不仅要将其加密，而且还应将其隐藏起来。

Hide Folders XP 是一套专门用于隐藏文件夹的软件，其使用非常简便，而且能很好地支持 NTFS 文件系统，并且它能很好地支持中文，能够完全隐藏中文名称的文件夹。Hide Folders XP 是一套共享软件，未注册版本会限制使用部分功能，例如设置隐藏文件的口令等。

10.3.1 隐藏文件夹

安装 Hide Folders XP 后，当用户需要隐藏某文件夹时，只需将其添加到 Hide Folders XP



的列表中即可，用户无论在【我的电脑】中如何设置都无法看到隐藏的文件夹。

软件小档案

软件名称： Hide Folders XP

版本： 2.2

官方网站： <http://www.fspro.net>

其他下载网址 1： <http://download.enet.com.cn/html/060512003020502.html>

其他下载网址 2： <http://dl.163.com/html/44/44539.html>

软件类型： 免费软件

STEP 1 添加文件夹至列表

打开程序后，选择【File】→【Add to list】→【Add any folder or file...】命令添加文件夹至列表中。



①依次选择【File】→【Add to list】→【Add any folder or file...】命令

STEP 2 选择要隐藏的文件夹

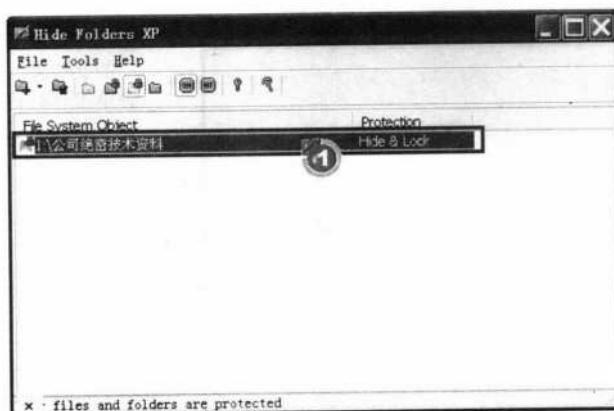
在【浏览文件夹】对话框中选择要隐藏的文件夹，选择完成后单击【确定】按钮即可。

- ①选择要隐藏的文件夹
②单击【确定】按钮



STEP 3 查看隐藏效果

将要隐藏的文件夹添加到程序的列表后，程序会自动将添加到列表中的文件夹隐藏并加锁。

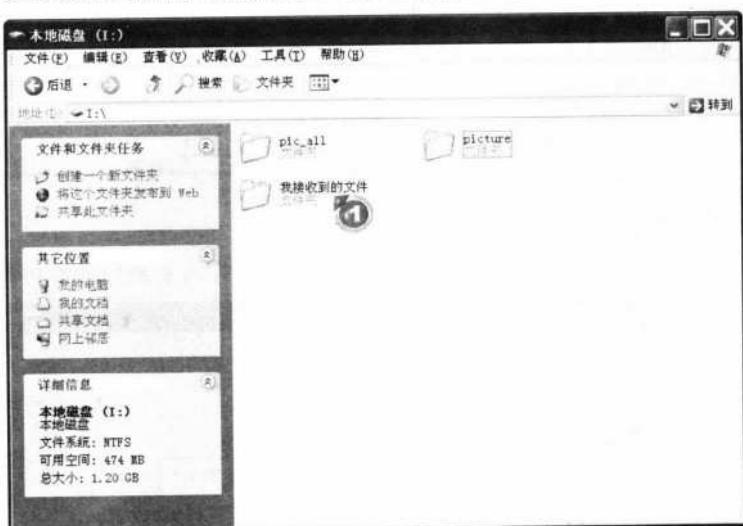


①文件夹隐藏并加锁

STEP4 查看磁盘

设置完成后，查看文件夹所在的磁盘路径，此时文件夹已被隐藏。

②文件夹已被隐藏



隐藏文件夹后，用户应将【开始】菜单及桌面上的 Hide Folders XP 程序快捷方式删除，以免黑客执行程序取消隐藏。如果使用的是已注册的版本，还可以设置程序密码使黑客无法还原文件夹。

当用户需要存取隐藏的文件夹时，可在程序主窗口中单击□按钮暂时取消隐藏。

10.3.2 取消隐藏

□ 按钮只是用来暂时性地取消隐藏，当用户已经不再需要隐藏某文件夹时，应直接将其从 Hide Folders XP 程序的列表中删除。

STEP1 选择【取消隐藏】功能

在列表中选择要取消隐藏的文件夹或程序，然后通过□按钮将其从列表中删除，以便取消隐藏。

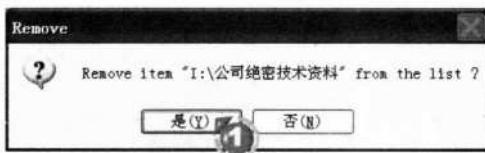


- ① 选择要取消隐藏的文件夹
- ② 单击按钮

STEP2 确认执行的操作

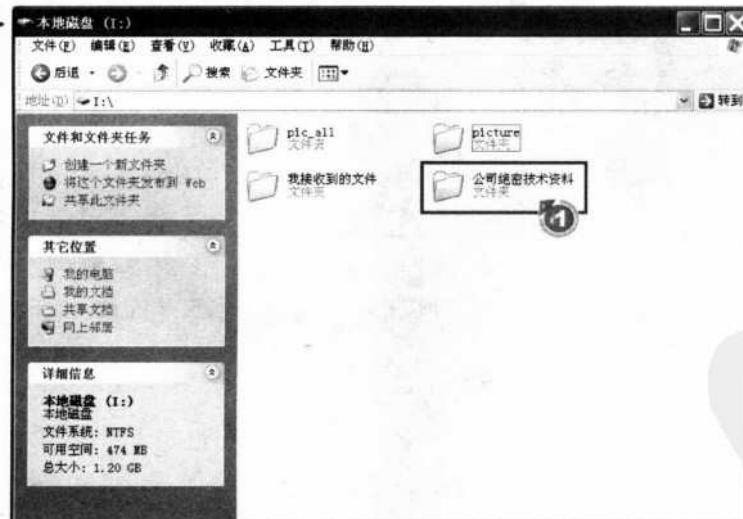
在【Remove】对话框中，单击【是】按钮，确认删除文件夹。

- ① 单击【是】按钮



STEP3 查看结果

设置完毕后，打开文件夹所在的路径，即可看到已经取消隐藏的文件夹。



- ① 取消隐藏的文件夹