揭开黑客神秘的面纱，黑客就这几招！

讲述黑客惯用的伎俩，见招拆招！
重点提示　任务过程　范例图示
专家讲解　打破常规　层层递进
一书在手　边用边学　即查即用

矛与盾

108招多媒体视频讲解
让你快速从入门到精通

黑客就这几招

武新华　孙世宁　杨平　等编著

机械工业出版社
China Machine Press

揭开黑客神秘的面纱，黑客就这几招！

讲述黑客惯用的伎俩，见招拆招！

重点提示　任务过程　范例图示

专家讲解　打破常规　层层递进

一书在手　边用边学　即查即用

108招多媒体视频讲解
让你快速从入门到精通

客服热线：(010) 88378991, 88361066
购书热线：(010) 68326294, 88379649, 68995259
投稿热线：(010) 88379604
读者信箱：hzjsj@hzbook.com

华章网站 http://www.hzbook.com

网上购书：www.china-pub.com

上架指导：计算机/网络安全

ISBN 978-7-111-28384-3

9 787111 283843

定价：49.80元（附光盘）

前 言

本书写作的目的主要是通过介绍黑客的攻击手段和提供相应的主动防御保护措施，使读者能够循序渐进地了解黑客入侵主动防御的关键技术与方法，提高安全防护意识，并将这些技术与方法应用于实际工作中。希望本书能成为网络信息安全专业技术人员、网络安全管理人员、网络使用者及信息时代的创业者的一本实用的网络安全工具书。

下面简要介绍本书的特点、学习方法以及提供的服务。

本书内容

本书以配图、图释、标注、指引线框等丰富的图解手段，再辅以浅显易懂的语言，通过对黑客攻击前的准备、扫描与反扫描技术、控制与反控制技术、欺骗与反欺骗、加密与解密工具、病毒与木马攻击防御、网络代理与追踪技术、注入工具与溢出攻击、账号盗取与安全防范、日志与后门清除技术、安全分析与入侵检测、流氓软件与间谍程序清除 12 大类，100 多个知识点的详细介绍，给出了相关代表性产品和工具的介绍及使用方法，使得读者可对网络安全主动防护及黑客入侵主动防御等具有代表性的技术有一个全面认识。

此外，本书还从黑客入侵防护应用角度给出了相对独立的内容的论述，使读者可对如何构建一个实用的黑客入侵防范体系有一个基本概念和思路，并可为读者提供几种典型行业的安全防护系统建设方案，以供参考和借鉴。

增值服务

随书所附光盘提供了多种攻防实战的教学视频，汇集了众多高手的操作精华，通过增进读者对主流操作手法感性认识的方式，使读者实现高效学习。

此外，如发现本书中有不妥或需要改进之处，还可通过访问 http://www.newtop01.com 或 QQ：274648972 与编者进行沟通，编者将衷心感谢提供建议的读者，并真心希望在和广大读者互动的过程中能得到提高。

组织方式

本书包含了 3 种学习方式，即简明教程、图解教程和范例教程。

- 简明教程：用最简单明了的语言来讲解，只介绍最重要的知识点及最常见的应用，与此无关的内容均不涉及。
- 图解教程：“理论+实战 图文+视频=让读者快速入门”，编者采用最为通俗易懂的图文解说，即使是电脑新手也能通读全书。
- 范例教程：用任务驱动、情景教学的方式来介绍，在学习案例过程中掌握知识点。最新黑客技术盘点，让读者实现“先下手为强”。学习目的性、指向性最强。

本书特色

本书以情景教学、案例驱动与任务进阶为鲜明特色，在书中可以看到一个个生动的情景案例。通过完成一个个实践任务，读者可以轻松掌握各种知识点，在不知不觉中快速提升实战技能。

- 从基础到实践，完全站在实用的角度，介绍黑客攻防技术，突出了实用性和案例分析，所举实例，来自于实际应用，学以致用，真正解决问题。
- 通俗易学，结合图解、标注和多媒体教学，使神秘、高深、难以掌握的黑客攻防技术学习起来省时、省力，易于上手，非常适合新手、大专院校学生，以及网络从业人员掌握快速掌握实用技术。
- 紧扣“理论+实战　图文+视频=全面提升学习效率!”的主导思想，详细分析每一个操作案例，以实现读者用更少时间尽快掌握加密解密技术的操作，并对实战过程中常见问题作必要的说明与解答。
- 当前最新技术、热点技术和常用相关工具软件都在本书有所涉及，有关黑客攻防技术、方法与思路，也做了重点讲解，并通过实例介绍综合技术的运用手段，最后能够达到举一反三。

读者对象

本书作为一本面向广大网络爱好者的速查手册，适合于如下读者学习使用：

- 电脑爱好者。
- 具备一定黑客知识基础和工具使用基础的读者。
- 网络管理人员。
- 喜欢研究黑客技术的网友。
- 大、中专院校相关学生。

本书作者

本书作者团队长期从事网络安全管理工作，都具有较强的实践操作能力及一线拼杀经验，可带领广大醉心技术者穿越迷雾，把黑客们的伎俩看清楚。参与本书编写工作的有：安向东负责第 1 章，田靖负责第 2 章，孙世宁、李防负责第 3、4、5 章，孙璐红负责第 6 章，王肖苗负责第 7 章，赵慧婷负责第 8 章，杨平负责第 9 章，段玲华负责第 10 章，李伟负责第 11 章，王英英负责第 12 章，最后由武新华通审全稿。我们虽满腔热情，但限于自己的水平，书中仍难免有疏漏之处。因此，还望大家本着共同探讨、共同进步的平和心态来阅读本书。作者心存谨敬，随时恭候您提出的宝贵意见。

最后，需要提醒大家的是：根据国家有关法律规定，任何利用黑客技术攻击他人的行为都属于违法行为，希望读者在阅读本书后不要使用本书中介绍的黑客技术对别人进行攻击，否则后果自负，切记!切记!

编　者

2009 年 8 月

目 录

第1章　黑客攻击前的准备

重点提示

- 探测操作系统
- 探测网站信息
- 探测搜索引擎
- 网络监听与嗅探
- 创建安全测试环境
- Virtual PC 安全测试环境
- 虚拟机网站平台

本章精粹：

本章主要介绍了黑客攻击前应做的准备工作，主要包括：探测操作系统、探测网站信息、探测搜索引擎、网络监听与嗅探等多个方面，有助于读者了解黑客如何运用相关工具进行探测、分析出被攻击主机的详细信息，以便预防黑客入侵。

黑客在进行攻击前往往会花很多时间和精力去做准备工作，比如搜集对方使用什么类型的操作系统、管理账号是否为空口令或者弱口令、系统是否存在某些严重的漏洞……做足了这些准备工作，攻击就会又多了几分胜算，越熟练的黑客花费在准备工作上的时间往往越多。信息搜索、筛选、分析……这是最枯燥却也是最重要的准备工作。

第 1 招　探测操作系统

由于系统本身往往会存在某些弱点与不足之处，黑客之所以能够入侵，就是利用了这些弱点与错误。现在网上流行的各种各样的入侵工具，都是黑客在分析了系统的弱点及存在的问题之后编写出来的。作为一般的黑客，并不需要去编写工具，只要善于使用现成的入侵工具，就可以实现入侵。

1．使用 X-Scan 工具探测系统

X-Scan 扫描器不同于一些常见攻击工具，它能用来发现问题，而不能直接攻击目标机器，执行如下操作可完成对远程计算机的操作系统探测。

使用 X-Scan 探测远程计算机的方法极其简单，具体的操作步骤如下。

步骤 1：先从网上下载并解压“X-Scan”压缩包。双击“X-Scan_gui.exe”应用程序图标，即可进入“X-Scan_gui”扫描器的主窗口，在其中可以浏览此软件的功能简介、常见问题解答等信息，如图 1-1 所示。

步骤 2：选择【设置】→【扫描参数】菜单项，即可打开【扫描参数】对话框，在其中选择“检测范围”选项设置扫描 IP 地址的范围，如图 1-2 所示。在“指定 IP 范围”文本框中输入需要扫描的目标 IP 地址（如 192.168.0.10）、IP 地址段（如 192.168.0.10 ~ 192.168.0.255），还能增加子网掩码（如 192.168.0.10/24）等。若不知道输入的格式，则可以单击该文本框右侧的【示例】按钮，在【示例】对话框中查看输入的有效格式，如图 1-3 所示。

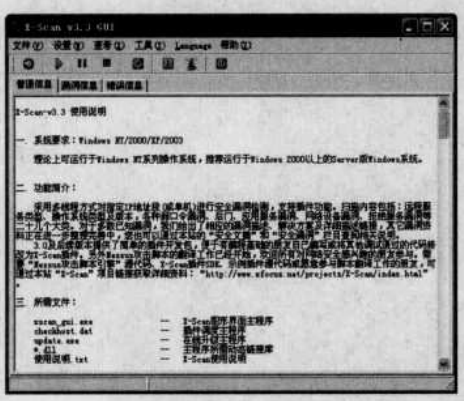


图 1-1　“X-Scan_gui”扫描器主窗口

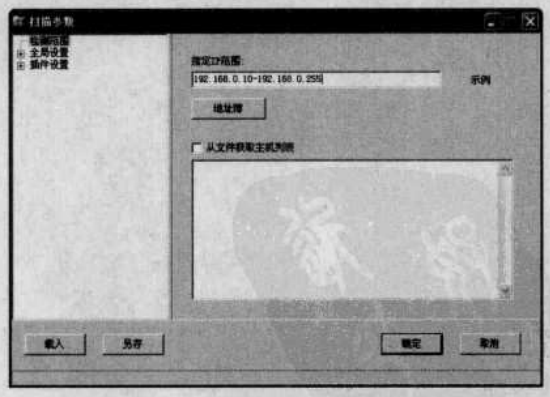


图 1-2　【扫描参数】对话框

步骤 3：展开“全局设置”选项之后，选取其中的“扫描模块”选项，则可选择扫描过程中需要扫描的模块（这里需要勾选“远程操作系统”选项），在选择扫描模块时，还可在其右侧窗格中查看远程计算机的操作系统，识别是否通过“SNMP（Simple Network Management Protocol，简单网络管理协议）、NETBIOS（Network Basic Input/Output System，网络基本输入/输出系统）协议主动识别远程操作系统类型及版本”插件来完成，如图 1-4 所示。

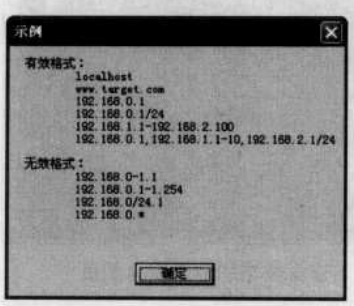


图 1-3 【示例】对话框

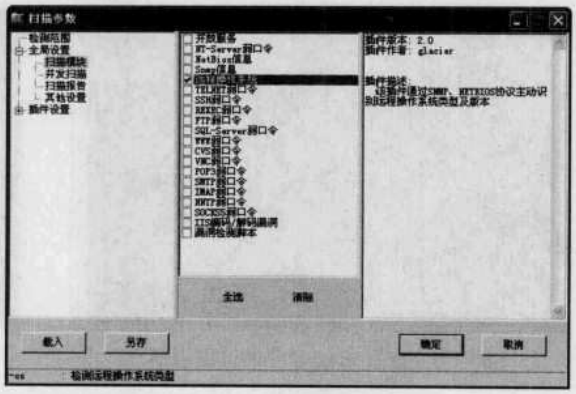


图 1-4 “扫描模块”选项

步骤 4：单击【确定】按钮返回到“X-Scan_gui”主窗口，单击 ▶ 按钮，耐心等待片刻就可以看到如图 1-5 所示的扫描结果了。在左侧的扫描目标右侧，即可看到“Windows XP”的标识，这就说明远程计算机使用的是 Windows XP 操作系统。

图 1-5 显示扫描结果

2. 使用 ping 命令探测系统

ping 命令是测试网络连接、信息发送和接收状况的实用型工具，是一个系统内置的探测工具。对于一个生活在网络上的管理员或黑客，ping 命令是第一个必须掌握的 DOS 命令，它所利用的原理是“网络上的机器都有唯一确定的 IP 地址，用户给目标 IP 地址发送一个数据包，对方就要返回一个同样大小的数据包，根据返回的数据包用户可以确定目标主机的存在，可以初步判断目标主机的操作系统等”。通过在命令提示符下输入“ping /?”命令，即可查看 ping 命令的详细说明，如图 1-6 所示。

- -a：指定对目的地 IP 地址进行反向名称解析。如解析成功，ping 将显示相应的主机名。
- -t：不断使用 ping 命令发送回响请求信息到目的地。要中断并退出 ping，只需要按下“Ctrl+C”组合键。初级黑客常常喜欢使用这个参数对目标计算机进行攻击。
- -n Count：指定发送回响请求消息的次数，默认值为 4。
- -l Size：指定发送的回响请求消息中“数据”字段的长度（以字节表示）。默认值为 32。如图 1-7 所示。Size 的最大值是 65527。

图 1-6　查看 ping 命令的详细说明

图 1-7　查看数据字节的默认长度

- -f：指定发送的回响请求消息带有“不要拆分”标志（所在的 IP 标题设为 1）。回响请求消息不能由目的地路径上的路由器进行拆分。该参数可用于检测并解决“路径最大传输单位（Path Maximum Transmission Unit，PMTU）”的故障。
- -I TTL：指定发送回响请求消息的 IP 标题中的 TTL（Time To Live，存活时间）字段值。其默认值是主机的默认 TTL 值。对于Windows XP 主机，该值一般是 128，TTL 的最大值是 255。
- -V TOS：指定发送回响请求消息的 IP 标题中的“服务类型（TOS）”字段值。默认值是 0。TOS 被指定为 0～255 之间的十进制数。
- -r Count：指定 IP 标题中“记录路由”选项用于记录由回响请求消息和相应的回响应答消息使用路径。路径中每个跃点都使用“记录路由”选项中的一个值。如果可能，可指定一个等于或大于来源和目的地之间跃点数的 Count。Count 最小值必须为 1，最大值为 9。
- -s Count：指定 IP 标题中的“Internet 时间戳”选项用于记录每个跃点的回响请求信息和相应的回响应答消息的到达时间。Count 的最小值为 1，最大值为 4。
- -j Path：指定回响请求消息，使用带有 HostList 指定 IP 标题中的“稀疏资源路由”选项。可由一个或多个具有松散源路由的路由器分隔连接中间目的地。主机列表中的地址或名称最大数为 9，主机列表是一系列由空格分开的 IP 地址（带点的十进制符号）。
- -k HostList：指定回响请求消息，使用带有 HostList 指定的中间目的地集的 IP 标题中的“严格来源路由”选项。使用严格来源路由，下一个中间目的地必须是直接可达的（必须是路由器接口上的邻居）。主机列表中的地址或名称的最大数为 9，主机列表是一系列由空格分开的 IP 地址（带点的十进制符号）。
- -w Timeout：指定等待回响应答消息响应的时间（以微秒计），该回响应答消息响应接收到的指定回响请求消息。如果在超时时间内未接收到回响应答消息，将会显示“请求超时”的错误消息。默认的超时时间为 4 000 000 微秒（4 秒）。
- Target Name：指定目的端，它既可以是 IP 地址，也可以是主机名。

典型示例：

（1）检测本机网卡驱动程序以及 TCP/IP 协议

若想检测本机的网卡驱动程序以及 TCP/IP 协议是否正常，只需要在命令提示符窗口中，输入“ping 192.168.0.7”命令，如图 1-8 所示。

（2）多参数合用检测

若要在命令提示符窗口中输入“ping -a -t 192.168.0.10”命令，即可对 192.168.0.10 的这台计算机进行探测。其探测结果如图 1-9 所示。通过反馈信息可得知上述命令中的参数“-a”检测出了该机器的 NetBios 名为 dns.sq.js.cn；参数“-t”在不断向该机发送数据包。

图 1-8 检测本机

图 1-9 多参数合用检测计算机

通常，ping 命令会反馈如下两种结果：

1）请求超时。表示没有收到网络设备返回的响应数据包，也就是说网络不通。出现这个结果原因很复杂，通常有对方装有防火墙并禁止 ICMP（Internet Control Message Protocol，网际控制信息协议）回显、对方已经关机、本机的 IP 设置不正确或网关设置错误、网线不通等几种可能。

2）来自 192.168.0.10 的回复：字节=32，时间<1ms，TTL=128。表示网络畅通，探测使用的数据包大小为 32 字节，响应时间小于 1ms。TTL 是指一个数据包在网络中的生存期，网管可通过它了解网络环境，辅助维护工作，通过 TTL 值可以粗略判断出对方计算机使用的操作系统类型，以及本机到达目标主机所经过的路由数。

当检查本机的网络连通情况时，通常会使用 ping 命令给某个目标主机（如本机）发送 ICMP 数据包。在本机中生成 ICMP 数据包时，系统就会给这个 ICMP 数据包初始化一个 TTL 值，如 Windows XP 就会生成“128”，将这个 ICMP 数据包发送出去，遇到网络路由设备转发时，TTL 值就会被减去“1”，最后到达目标主机，如果在转发过程上 TTL 值变成“0”，路由设备就会丢弃这个 ICMP 数据包。

TTL 值在网络应用中很有用处，可以根据返回信息中的 TTL 值来推断发送的数据包到达目标主机所经过的路由数。路由发生在 OSI（Open System Interconnection，开放系统互联模型）网络参考模型中的第三层即为网络层。

提示 不同的操作系统，它的 TTL 值也是不相同的。默认情况下，Linux 系统的 TTL 值是 64 或 255，Windows NT/2000/XP 系统的 TTL 值为 128，Windows 98 系统的值为 32，UNIX 主机的 TTL 值为 255。

3. 通过网站判断系统

有时，黑客会通过网站来获得目标的操作系统信息。例如：若某黑客与某台计算机用户通过 QQ 聊天，黑客说：“我的网站不错，欢迎你来访问”，并给出了一个网页地址。很多个人计算机用户不会提防这个要求，于是立即访问了这个网页。

在访问这个网页的同时，此个人计算机用户的操作系统信息实际上已经被写入到数据库中

了。这样，黑客不费吹灰之力就得到了想要的信息。这样，获取指定信息的代码很简单，实现的方法有很多。比如，下面的代码就可以在网页上显示客户端的操作系统等信息。

```
<%
Response.write?Request.ServerVariables("HTTP_ACCEPT_LANGUAGE")&"<br>"Response.write?Re-
quest.ServerVariables("HTTP_USER_AGENT")&"<br>"
%>
```

在访问含有上述代码的网页时，就会看到相应的信息。通过这些信息，可以知道个人计算机用户的 IE 版本、操作系统版本等。并且这些信息都可以用于黑客任务。

提示 上述方法是使用了服务器变量集合保存了随 HTTP（Hyper Text Transfer Protocol，超文本传输协议）头请求一起传送的 HTTP 头的信息，HTTP 头中包含有很多来访者（客户端）的信息，可以通过它获得有关来访者的操作系统版本、浏览器版本等信息。

第 2 招　探测网站信息

网站是黑客入侵或攻击的主要对象之一，由于网站是人人都可以访问的一个内容载体，它只要有一点风吹草动，可能就会产生较大的影响，这很容易让黑客产生“成就感”。黑客在对网站展开任务之前，通常会执行相应的探测操作。

1. 探测域名和 IP

对于购买了域名的网站，既可以直接使用 IP 地址作为网址，也可以使用域名作为网址，在如图 1-10 所示窗口中输入相应的内容，即可看到相应的绑定信息。这就是为什么有的网站只能用 IP 地址进行入侵，有的却可以使用 IP 地址或域名进行入侵的缘故。通常，用户把采用域名系统命名的网址称之为“域名”或“网址”（网站 IP 地址也可称为“网址”）。

域名地址以层次化表示：

1）后缀。最右边的后缀用于标识域名的性质，如 cn 表示中国，edu 表示教育机构。实际上，由于域名申请的开放性，用户可根据自己的喜好来注册.net 或.com。这就好比用户可随意到某个城市（随便使用.com 或.net）居住，但城市名称（.com 这样的后缀）却不能由用户来定义一样。

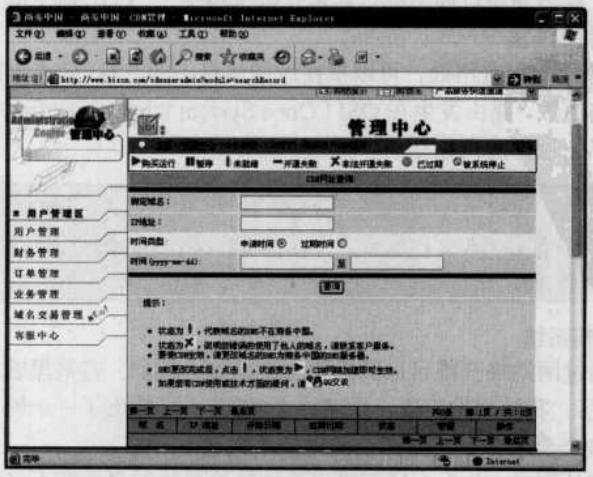


图 1-10　绑定 IP 地址

2）名称。名称即域名中间的网站名称，如 www.xinghuaye924.cn 这个域名中的网站名称就是 xinghuaye924。这是在注册域名时用户需要自定义的部分，它在同一种域名后缀中是唯一的。也就是说，可以有 xinghuaye924.net 和 xinghuaye924.cn。

3）前缀。最左侧的前缀用于标识网站类别，如 www 表示 Web 服务。由于申请的域名是 xinghuaye924.net，所以 www 和 ftp 这样的前缀可自由设置（不设置前缀也可以），如 360sight.cn 等。其中，要注意 www 和 ftp 这样的前缀名，已约定俗成供 Web 服务和 FTP 服务使用了。

通常，用户可以根据前缀看出网址所对应的具体内容。

- www：Web 服务，如 www.xinghuaye924.net。
- ftp：数据上传下载服务，如 ftp.xinghuaye924.net。
- bbs：论坛服务，如 bbs.xinghuaye924.net。
- mail：邮局服务，如 mail.xinghuaye924.net。
- down：下载服务，如 down.xinghuaye924.net。
- news：新闻服务，如 news.xinghuaye924.net。
- movie：电影服务，如 movie.xinghuaye924.net。
- music：音乐服务，如 music.xinghuaye924.net。

除这些约定俗成的名称外，通常用户会以常用英文单词或拼音等来作为前缀，如百度图片搜索就是 http://image.baidu.com/。通常，黑客在访问一个网址前，可凭经验判断出其提供什么服务。对于一名黑客来说，要入侵的网站有哪些域名，以及这些域名解析到哪些 IP 地址，都应该做到心中有数。检测的方法很简单，以检测 bbs.newtop01.com 网站解析到的 IP 地址为例，需要执行如下操作。具体的操作步骤如下。

步骤 1：在【运行】对话框的运行栏中输入“cmd”命令，即可进入命令提示符窗口。如图 1-11 所示。在当前命令提示符下输入“ping bbs.newtop01.com”命令，即可显示该论坛的反馈信息，如图 1-12 所示。

步骤 2：通过上述显示信息，可以看出 bbs.newtop01.com 这个网站解析到的 IP 地址是 203.171.239.143。也即 bbs.newtop01.com 网站内容存储在 203.171.239.143 这台服务器中。要查询域名对应的 IP 地址，可使用 ping 命令。

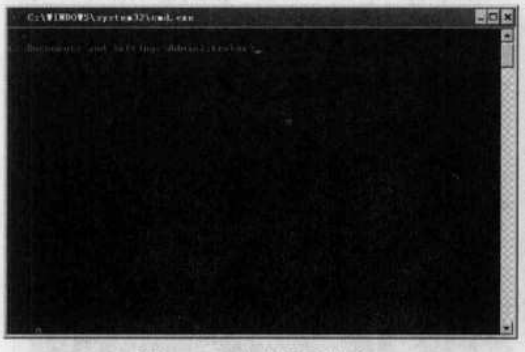


图 1-11 命令提示符窗口

图 1-12 显示论坛的反馈信息

如果希望知道有多少不同的域名指向到某个 IP 地址，可以通过执行如下操作来完成查询，具体的操作步骤如下。

步骤 1：先在 IE 浏览器地址栏中输入“http://www.myipneighbors.com/”网址，即可进入“myipneighbors”的主页，如图 1-13 所示。

步骤 2：在窗口右上角“Search”栏中输入要查询的 IP 地址，单击右边的【search】按钮，即可查看相应的结果。如图 1-14 所示。

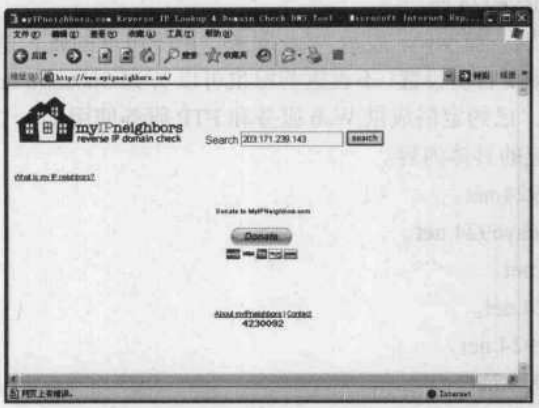


图 1-13 “myipneighbors”的主页

图 1-14 查看该站点的指向信息

步骤 3：在查询完毕后，该站点会将结果信息，以列表的形式反馈出来。最后任意选中一个域名并将其复制，粘贴到 IE 地址栏中，单击【转到】按钮，即可访问这个域名。

有时，一个网站的安全配置很好，并不代表其所在服务器上其他网站的安全配置也好。因此，先透过其他有漏洞的网站来完成服务器的入侵，最后再完成目标网站的破解，也是常见的网站入侵方法。

2. NsLookup 的使用

NsLookup 命令经常会被黑客用于查询域名对应的 IP 地址、A（Address，地址）记录、MX（Mail Exchanger，邮件交换）记录、NS（Name Server，域名服务器）记录、CNAME（Canonical Name，别名）记录等信息。使用 NsLookup 可以从如下几个示例来说明。

示例 1：若要查询 A 记录，则只需按“NsLookup 域名”格式输入命令，如“NsLookup newtop01.com”命令，如图 1-15 所示。

示例 2：若要查询 MX 记录，则只需要按“NsLookup -q=mx 域名”格式输入命令即可。如“nslookup -q=mx bbs.newtop01.com”命令。显示结果如图 1-16 所示。

图 1-15 查询 A 记录

图 1-16 查询 MX 记录

示例 3：若查询 NS 记录，只需按“NsLookup -q=ns 域名”格式输入命令，如“nslookup -q=ns web.newtop01.com”命令，如图 1-17 所示。

有时一台服务器使用的 IP 地址可能不止一个，如何才能获得这个 IP 地址使用列表呢？这里以查询 www.qq.com 网站使用的 IP 地址列表为例，通过如下方法获得这项信息。

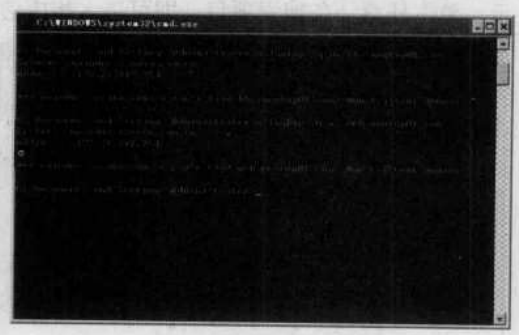


图 1-17 查询 NS 记录

具体的操作步骤如下。

步骤 1：在当前命令提示符下输入“NsLookup”命令，即可查看域名对应的 IP 地址信息。接着在命令提示符“>”右侧输入 www.qq.com 命令，如图 1-18 所示。在返回如图 1-19 所示的信息之后，即可获得 www.qq.com 服务器群的 IP 地址列表。

图 1-18 查看域名对应的 IP 地址信息

步骤 2：获得这个 IP 地址列表对于入侵者非常重要，因为当入侵者在一台服务器上使用各种入侵方法无功而返时，还有机会在另一台服务器中尝试入侵。

除可以进行域名到 IP 地址的查询，如果希望知道某个内网 IP 地址（如 192.168.0.10）对应的域名是哪个，从而确切地知道企业网络服务安装在哪台机器上，只需在命令提示符窗口中输入“nslookup 192.168.0.10”命令。如果能够查到该 IP 对应的域名，将会直接显示出来。比方说，在反馈信息的第二行的 Name 后面将会看到域名。

图 1-19 获得 www.qq.com 服务器的 IP 地址列表

第 3 招 探测搜索引擎

为了使网民搜索信息的速度更加快捷，更加准确，专门在 Internet 上执行信息搜索任务的搜索引擎技术应运而生了。目前，使用率最高的搜索引擎是 www.baidu.com 和 www.google.com。

1．特殊的“关键词”搜索探测

通过搜索引擎网站，黑客可通过搜索特殊的“关键词”来查找到一些具有漏洞的网站。比如，在动态网站中一般会有 Conn.asp 这个文件，它用于存储数据库文件的路径、名称等信息，黑客在搜索引擎中总是喜欢使用它作为搜索关键词。具体的操作步骤如下。

步骤 1：先进入使用率最高的搜索引擎首页，在搜索文本框中输入需要搜索的相关信息，这里以搜索“Inurl：/admin+conn.asp”为例，如图 1-20 所示。其中，admin 表示后台管理目录，通常用于存储所有的管理文件。当然，也可改成其他的目录名，但目录名要在网站中存在才可以。

步骤 2：在其中输入搜索内容并选中想要搜索的方式（这里选择“所有网页”方式），单击

【Google 搜索】按钮，即可打开搜索结果页面，在其中可以看到所有的搜索项目，如图 1-21 所示。单击任意一条搜索项目，即可进入相应信息页面。

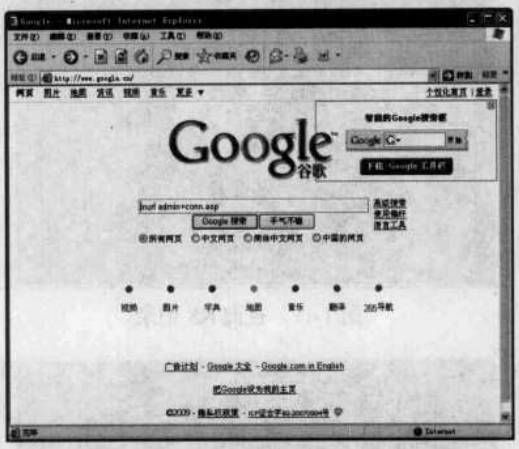


图 1-20　Google 搜索引擎首页

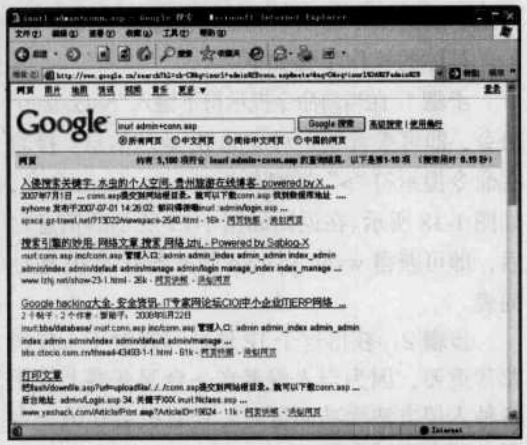


图 1-21　搜索结果页面

提示　在 www.google.com 中黑客使用的关键词有很多，如 upload.asp site:tw、inurl:winnt\system32\inetsrv\等，这些关键词都可以为黑客起到为虎作伥的作用。

2．专用工具搜索探测

Google hacker（Google 黑客）是利用 Google 提供的搜索功能查找黑客们想找到的信息。一般是查找网站后台、网管的个人信息，也可以用来查找某人在网络上的活动。Google hacker 一般是作为黑客在入侵时的一个手段，有时可在入侵过程中查找后台的登录口。

使用“google hacker v2.0”进行搜索的具体操作步骤如下。

步骤 1：下载并解压“google hacker v2.0”压缩包，双击“google hacker v2.0”应用程序图标，即可进入“google hacker v2.0”的主窗口。在“google 搜索专用参数”下拉列表框中，选择一种参数的类型，如图 1-22 所示。

步骤 2：单击【让我们去…】按钮，即可进入相应的搜索页面，如图 1-23 所示。也可在“Google”搜索栏目中输入关键词“163”，单击【搜索】按钮，即可打开 IE 浏览器访问 www.google.com，并会自动输入指定关键词进行搜索，如图 1-24 所示。

图 1-22　“google hacker v2.0”主窗口

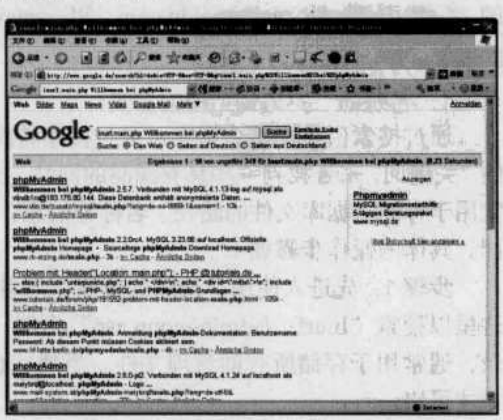


图 1-23　Google 搜索专用参数页面

步骤 3：由于列举的关键词都是常见的漏洞，所以搜索结果的数量通常都会比较惊人。搜索结果显示如图 1-25 所示。

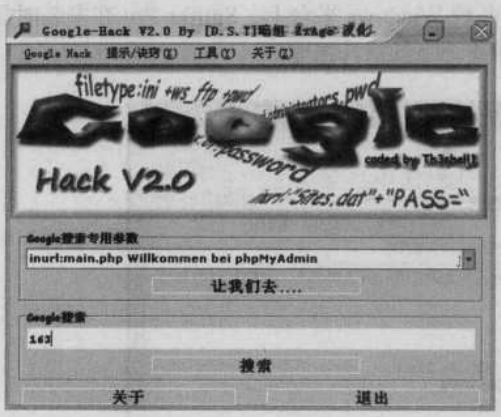


图 1-24 Google 搜索

图 1-25 关键词“163”搜索页面

第 4 招 网络监听与嗅探

起初，网络监听常被网络管理员用于以太网中监测传输的网络数据，它在排除网络故障等方面功不可没，倍受网络管理员的青睐。后来，有许多网络入侵往往都伴随着以太网内网络监听行为，从而造成口令失窃，敏感数据被截获等连锁性安全事件，并有意无意地将这种技术引入到了黑客领域，就给以太网带来了极大的安全隐患。

1．网络监听实例演练

网络监听可有效地对网络数据、流量进行侦听、分析，从而排除网络故障，同时又带来了信息失窃等极大隐患。例如，若要查看当前计算机的 IP 地址，则具体的方法是“在命令提示符下输入‘ipconfig’命令，即可查看当前计算机的 IP 地址，如图 1-26 所示”。若想查看本机网卡的 IP 地址与 MAC（Media Access Control，介质访问控制）地址，只需在命令提示符下输入“ipconfig /all”命令，如图 1-27 所示。

一般而言，网卡有几种接收数据帧的状态，如 unicast（直接模式）、broadcast（广播模式）、multicast（多播模式）、promiscuous（混杂模式）等。

图 1-26 查看当前计算机的 IP 地址

图 1-27 查看本机的网卡和 MAC 地址

在 www.google.cn 中搜索“Sniffer 工具”这个关键词，可以找到非常多的可用方法和工具。搜索结果如图 1-28 所示。下面以一款常见工具 Sniffer Pro 为例介绍一下使用方法。

Sniffer Pro 是一款协议分析软件，可运行在各种 Windows 平台上，Sniffer Pro 在安装时需要填写注册信息，运行时占用内存比较大，否则就会降低运行速度。

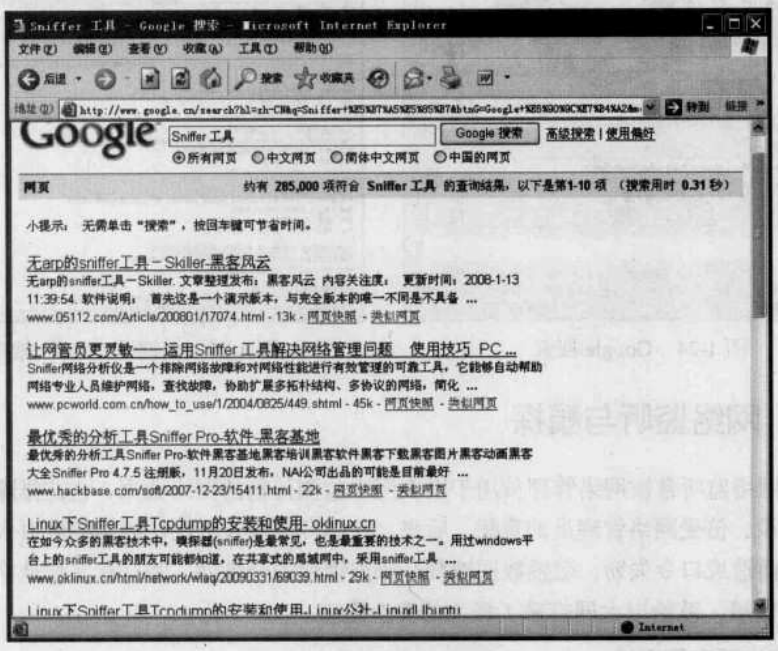


图 1-28 搜索结果

设置和使用 Sniffer Pro 的具体操作步骤如下。

步骤 1：第一次使用 Sniffer Pro 时，用户需要选择监听的适配器，如图 1-29 所示。单击【新建】按钮，即可打开【新建设置】对话框，在其中可根据需要创建新项目。单击【好】按钮，即可完成设置，如图 1-30 所示。

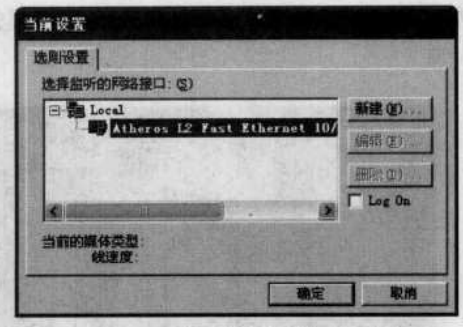


图 1-29 【当前设置】对话框

图 1-30 【新建设置】对话框

步骤 2：单击【确定】按钮，即可打开 Sniffer Pro 操作窗口，如图 1-31 所示。选择【捕获】→【开始】菜单项或单击工具栏中 ▶ 按钮，即可开始进行捕获，如图 1-32 所示。在捕获过程中可以通过查看捕获报文数量和缓冲区利用率等。

图 1-31 【Sniffer Pro】操作窗口

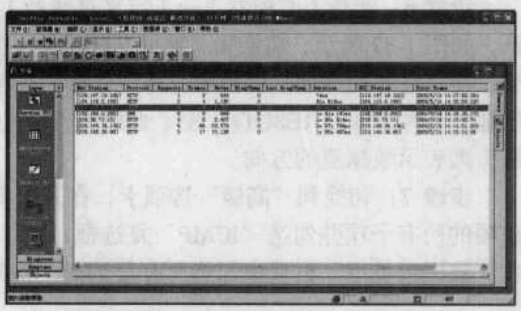


图 1-32 利用 Sniffer Pro 捕捉到的信息

步骤 3：双击任意一个 IP 地址，即可对该报文信息进行详细的查看（即专家分析系统），如图 1-33 所示。专家分析系统提供了一个只能分析的平台——对网络上的流量进行一些分析。而对于某项统计分析可以使用鼠标双击该条记录查看详细的统计信息，同时对于每一项都可以通过查看帮助来了解其原因。

步骤 4：在【Sniffer Pro】主窗口中选择【监视器】→【主机列表】菜单项，即可看到捕获到的主机的详细信息，如图 1-34 所示。选择【捕获】→【停止并显示】菜单项，即可对所捕获的数据进行查看。切换到“解码”选项卡，即可看到所捕获到的数据包，如图 1-35 所示。

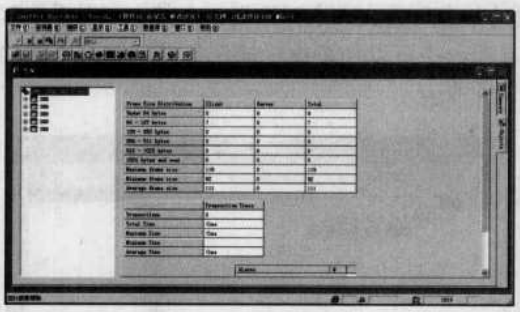


图 1-33 查看报文信息

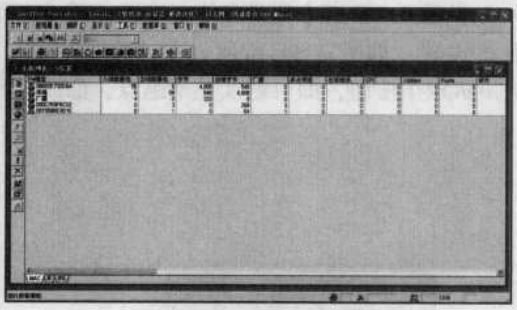


图 1-34 查看主机列表

步骤 5：切换到“矩阵”选项卡，即可看到全网的连接情况，如图 1-36 所示。图中的绿线表示正在发生的网络连接，而蓝线则表示过去的连接。

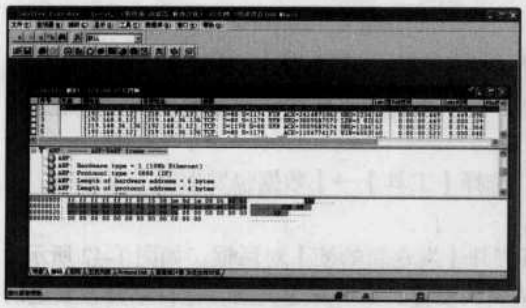


图 1-35 查看所捕获到的数据包

图 1-36 查看全网的连接情况

步骤 6：选择【监视器】→【定义过滤器】菜单项，即可打开【定义过滤器-监视器】对话框，如图 1-37 所示。切换到“地址”选项卡，在“地址类型”下拉列表中选择“Hardware”选项；在“已知的地址”栏目中选择“任意”选项；在“位置 1”栏的第一行中单击并输入链路层地址条件，如 001E8C17B085，此时在“地址 2”栏目中会显示“Any”，而“dir.”栏目中的箭头则表示数据流的方向。

步骤 7：切换到“高级”选项卡，在其中编辑协议捕获条件。如勾选“IP”复选框，展开该项的所有子项并勾选“ICMP”复选框；在“数据包大小”下拉列表中选择“ALL”选项；在“数据包类型”栏目中勾选所有复选框，如图 1-38 所示。

图 1-37　设置“地址”选项卡

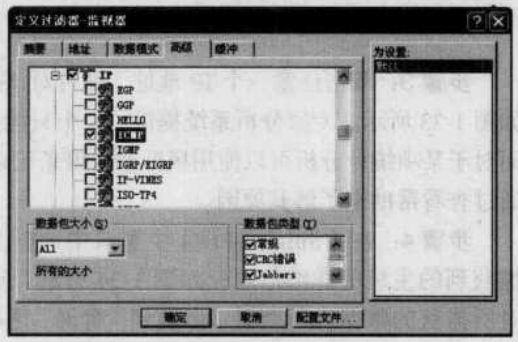


图 1-38　设置“高级”选项卡

步骤 8：单击【配置文件】按钮，即可打开【捕获配置文件】对话框，在其中可以看到默认的设置，如图 1-39 所示。在“数据模式”选项卡中可以任意编辑捕获条件，单击【添加 AND/OR】按钮，即可添加关系结点，如图 1-40 所示。

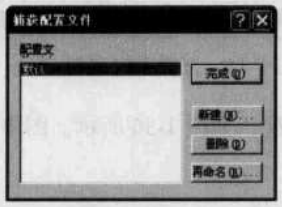


图 1-39　【捕获配置文件】对话框

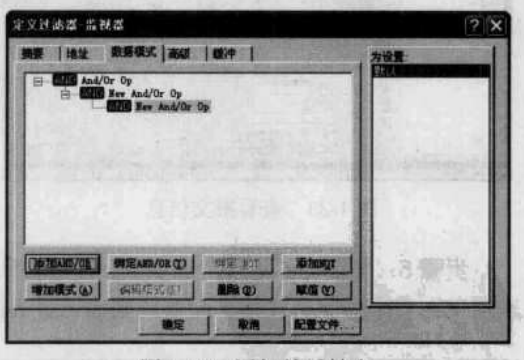


图 1-40　添加关系结点

步骤 9：单击【增加样式】按钮，即可添加模板；单击【添加 NOT】按钮，即可添加排除结点。使用该选项卡可以实现复杂的报文过滤，但一般情况下所截获的报文不多，使用这种方法是得不偿失的。

步骤 10：Sniffer Pro 还具有报文发送功能，选择【工具】→【数据包发生器】菜单项，即可看到【数据包发生器】窗口，如图 1-41 所示。

步骤 11：单击【发送 1 帧】按钮，即可打开【发送新的帧】对话框，如图 1-42 所示。在“发送”栏目中设置要发送的次数，也可保持默认设置；在“发送类型”栏目中设置发送的时间间隔，一般保持默认 1 毫秒。

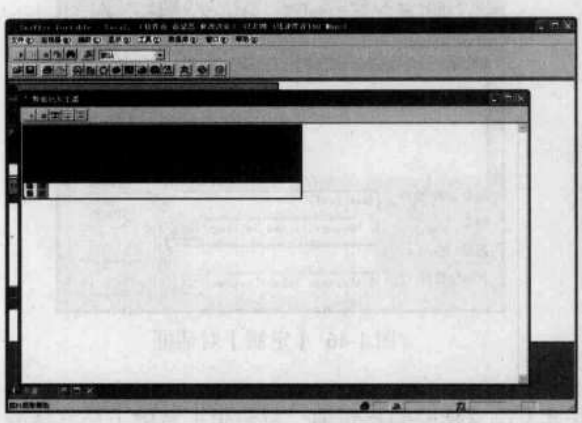


图 1-41 【数据包发生器】窗口

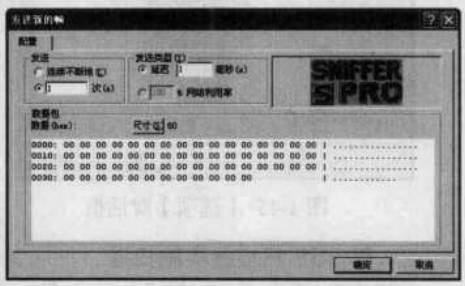


图 1-42 【发送新的帧】对话框

步骤 12：单击【尺寸】按钮，即可打开【设置数据包大小】对话框，如图 1-43 所示。在“新大小”文本框中输入要发送的数据帧的长度，单击【好】按钮返回到【发送新的帧】对话框，此时在“数据包”栏目中可使用方向键对报文的内容进行编辑。

步骤 13：单击【确定】按钮，即可看到该报文处于发送状态，如图 1-44 所示。

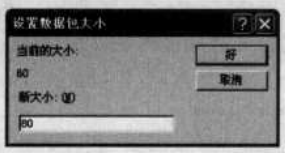


图 1-43 【设置数据包大小】对话框

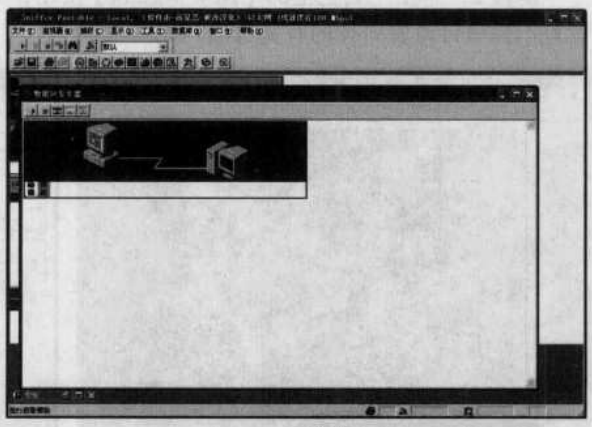


图 1-44 发送报文

使用这种方式发送报文优势在于：当网络发送出现问题时网络流量就会发生异常，可通过网络流时分析图帮助用户及时找出引发流量异常的问题所在。

步骤 14：如果相对 Sniffer Pro 的相关选项进行设置，则选择【工具】→【选项】菜单，即可打开【选项】对话框，在其中设置各个选项卡，如图 1-45 所示。

步骤 15：另外，Sniffer Pro 还允许用户自定义工具。选择【工具】→【定制用户工具】菜单，即可打开【定义】对话框，如图 1-46 所示。单击【添加】按钮，即可添加需要的工具。

Sniffer Pro 不仅可确保网络性能的优化，还可通过对网络连接情况的分析，发现并清除病毒，此功能在网络管理是非常重要的。随着企业对网络性能的要求越来越高，在这些情况下，使用 Sniffer Pro 就成为不错的选择。此外，Sniffer Pro 还具有报文发送、网络监视、解码分析等功能，用户可以通过 Sniffer Pro 帮助文件来获得这方面的信息。

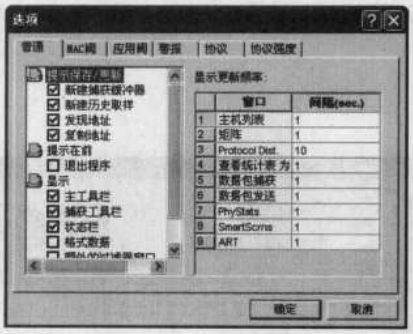


图 1-45 【选项】对话框

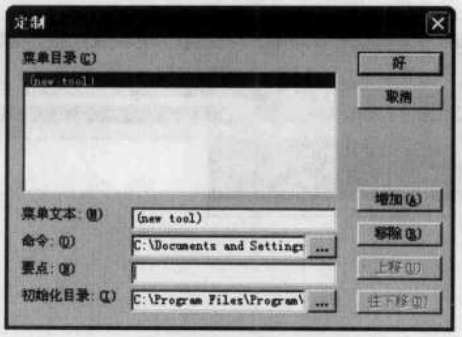


图 1-46 【定制】对话框

2. 用 SSS 扫描器实施扫描

SSS（Shadow Security Scaner）是一款著名的系统漏洞扫描器，可对很大范围内的系统漏洞进行高效、可靠的安全检测，其系统扫描的速度与精度足以让用户敢于向专业的安全机构和那些专门入侵他人计算机系统的黑客叫板。

利用 SSS 扫描器对系统漏洞进行扫描的具体操作步骤如下。

步骤 1：安装好 SSS 软件后，选择【开始】→【程序】→【Safety-lab】→【Shadow Security Scaner】→【Shadow Security Scaner】菜单项，即可进入其操作界面，如图 1-47 所示。

步骤 2：单击工具栏上的【New session】按钮，即可打开【New session】对话框，在其中设置扫描项目设置向导的有关选项，如图 1-48 所示。

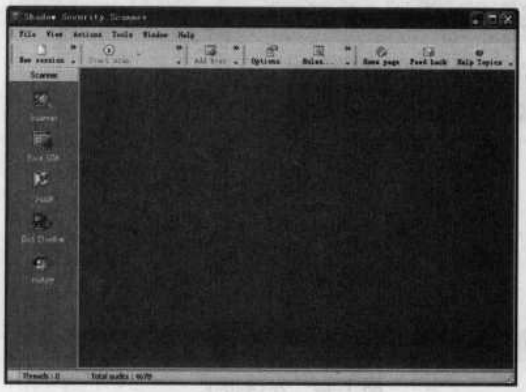


图 1-47 SSS 操作界面

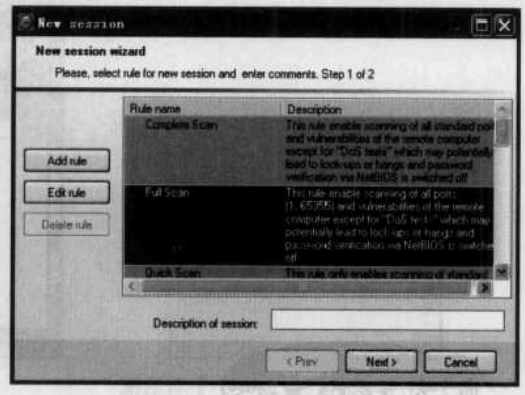


图 1-48 【设置扫描项目】窗口

步骤 3：用户可以选择预设的扫描规则，也可单击【Add rule】按钮，即可打开【Create new rule】对话框，在其中创建新的扫描规则，如图 1-49 所示。

步骤 4：单击【OK】按钮，即可在设置扫描选项对话框中设置新扫描规则的有关选项，如图 1-50 所示。在选择好扫描规则后（如“Complete Scan”选项），单击【Next】按钮，在显示的对话框中单击【Add host】按钮，即可添加扫描的目标计算机，如图 1-51 所示。

步骤 5：选取“Host”单选项，可添加单一目标计算机的 IP 地址或计算机名称；选取“Hosts range”单选项，可添加一个 IP 地址范围；选取“Hosts from file”单选项，可通过指定已存在的目标计算机列表文件添加目标计算机；选取“Host groups”单选项，则可通过添加工作组的方式添加目标计算机，并设置登录的用户名称和密码。在添加好目标计算机之后，单击【Add】按钮，即可完成目标计算机的添加，如图 1-52 所示。

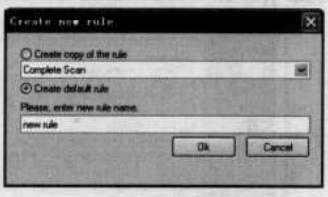


图 1-49 创建扫描规则

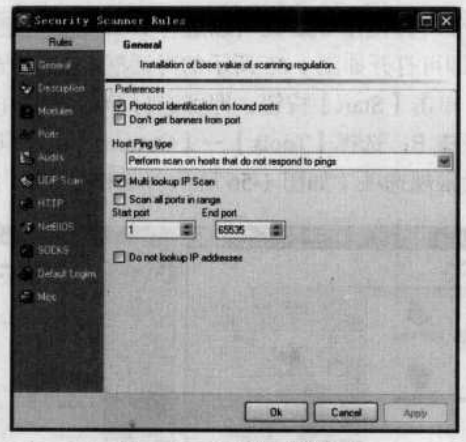


图 1-50 设置扫描选项

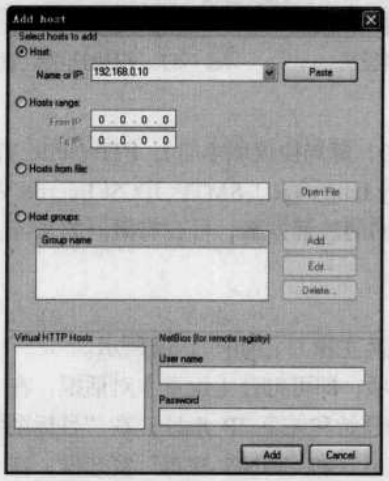


图 1-51 添加扫描的目标计算机

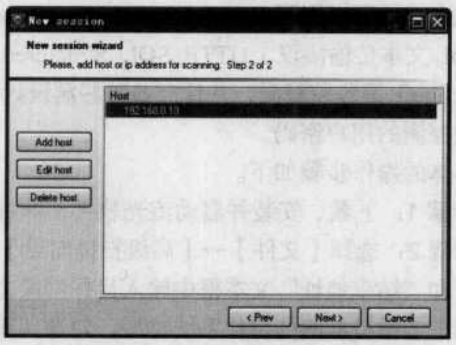


图 1-52 添加目标计算机

步骤 6：单击【Next】按钮，即可完成扫描项目的创建并返回 SSS 主界面。单击工具栏上的【Start scan】按钮，开始对目标计算机进行扫描，并可在“Statistics”标签卡中查看扫描进程，如图 1-53 所示。在“Vulnerabilities”标签卡中查看扫描结果，其中给出了危险程序、补救措施等内容，如图 1-54 所示。

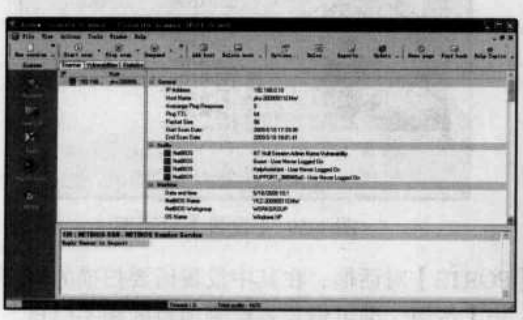


图 1-53 查看扫描结果

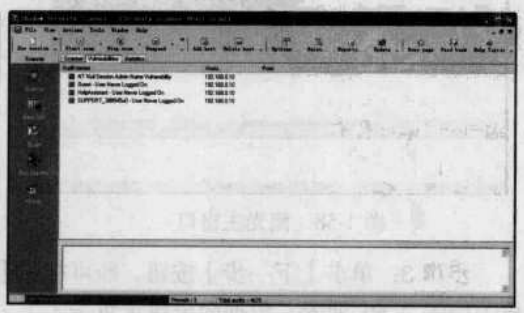


图 1-54 “Vulnerabilities”标签卡中查看扫描结果

步骤 7：使用 SSS 还可以进行 DoS 安全性进行检测。单击左侧窗口中的【DoS Checker】按钮，即可打开如图 1-55 所示的对话框。在其中选择检测的项目，设置扫描的线程数（Threads）之后，单击【Start】按钮，即可进行 DoS 检测并给出检测结果。

步骤 8：选择【Tools】→【Options】菜单项，即可打开 SSS 选项设置对话框，在其中可以设置常规选项（如图 1-56 所示），扫描选项（如图 1-57 所示）等。

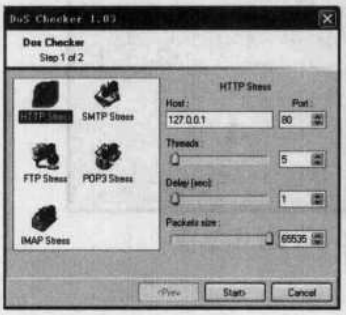


图 1-55　设置 DoS 检测选项

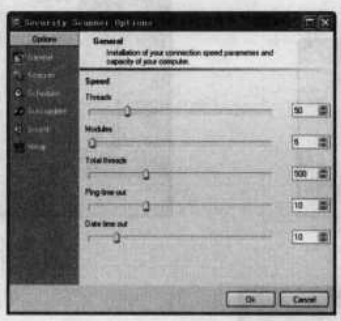


图 1-56　常规选项设置

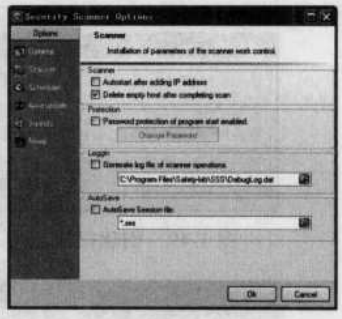


图 1-57　扫描选项设置

3. 用流光扫描弱口令

流光软件可以探测 POP3（Post Office Protocol 3，邮局协议版本 3）、FTP（File Transfer Protocol，文本传输协议）、HTTP、SQL（Structured Query Language）、SMTP、IPC$（Internet Process Connection）等各种漏洞，并针对各种漏洞设计了不同的破解方案，可在有漏洞的系统上轻易得到被探测的用户密码。

具体的操作步骤如下。

步骤 1：下载、安装并启动流光软件，即可进入其主窗口，如图 1-58 所示。

步骤 2：选择【文件】→【高级扫描向导】菜单项，即可打开【设置】对话框，在“起始地址”和“结束地址”文本框中输入目标网段主机的开始和结束 IP 地址，在“目标系统”下拉列表中选择待检测的操作系统类型，勾选“获取主机”和“PING 检查”复选框，在“检测项目”列表框中选择需要扫描的项目，如图 1-59 所示。

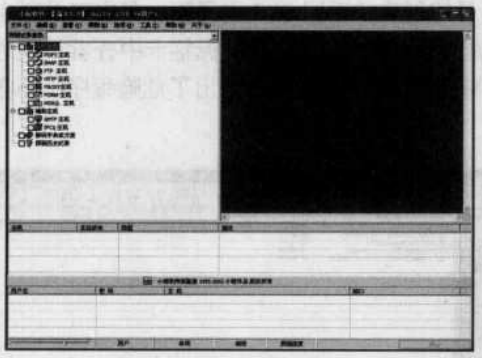


图 1-58　流光主窗口

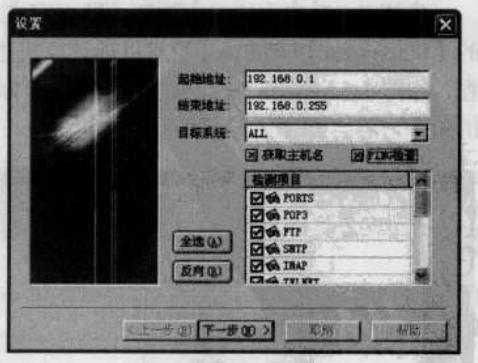
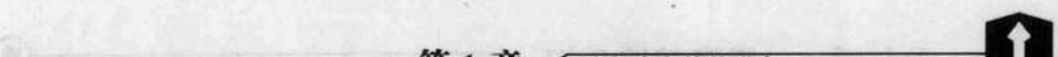


图 1-59 【设置】对话框

步骤 3：单击【下一步】按钮，即可打开【PORTS】对话框，在其中设置所要扫描的端口号，如图 1-60 所示。根据向导提示单击【下一步】按钮，即可设置各检测项目的相关信息。当然，也可以直接采用默认设置。



步骤 4：在设置完毕之后，即可进入【选项】对话框，在其中可根据需要选择猜解用户名字典、密码字典和保存扫描报告的路径，并选择相应的并发线程数目，如图 1-61 所示。

步骤 5：单击【完成】按钮，即可完成设置并弹出【选择流光主机】对话框，在其中选择用于扫描的流光主机，如图 1-62 所示。

图 1-60 【PORTS】对话框

图 1-61 【选项】对话框

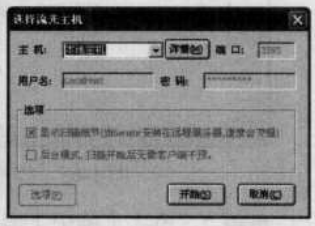


图 1-62 【选择流光主机】对话框

步骤 6：如果只用本机扫描，则单击【开始】按钮，即可自动扫描。如果要选择目标机，则单击【详情】按钮，即可打开【Sensor 管理工具】对话框，如图 1-63 所示。

步骤 7：单击【新增】按钮，即可打开【安装 Fluxay Sensor】对话框，在其中输入目标机的相应信息，如图 1-64 所示。单击【安装】按钮，在安装成功之后再单击【确定】按钮，即可完成设置操作。

图 1-63 【Sensor 管理工具】对话框

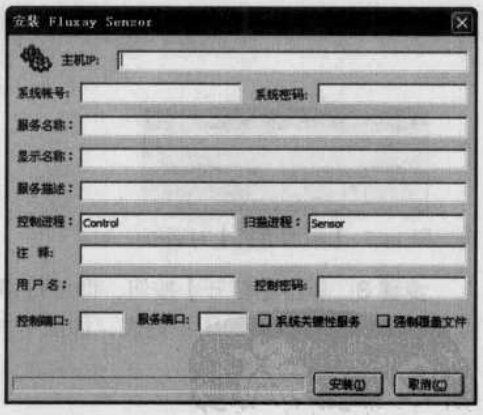


图 1-64 【安装 Fluxay Sensor】对话框

步骤 8：单击【开始】按钮，即可自动进行扫描，扫描完成后将自动生成一个 HTML（Hyper Text Markup Language，超文本标记语言）格式的扫描报告，在其中显示了扫描到的用户密码，如图 1-65 所示。

除使用“高级扫描向导”配置高级扫描外，还可选择【探测】→【高级扫描工具】菜单项，在【高级扫描设置】对话框中设置进行扫描，如图 1-66 所示。如果用户只是希望对某一漏洞进行探测，例如对 POP3 邮箱的弱口令进行扫描，则需要进行如下的操作。

步骤 1：在流光主窗口中右击“POP3 主机”选项，从快捷菜单中选择【编辑】→【添加】选项，即可打开【添加主机】对话框，在其中输入要添加邮箱的名称，如图 1-67 所示。

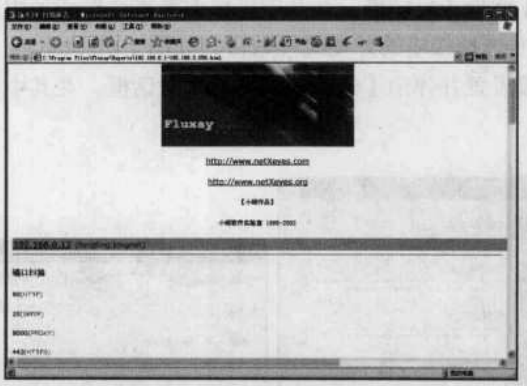


图 1-65　扫描结果显示

图 1-66 【高级扫描设置】对话框

步骤 2：单击【确定】按钮，即可完成邮箱的添加操作，如图 1-68 所示。右击添加的邮箱并选择【编辑】→【从列表添加】选项，即可打开【打开】对话框，在其中选择创建的用户字典，如图 1-69 所示。

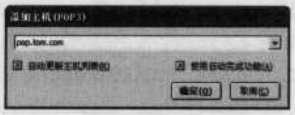


图 1-67 【添加主机】对话框

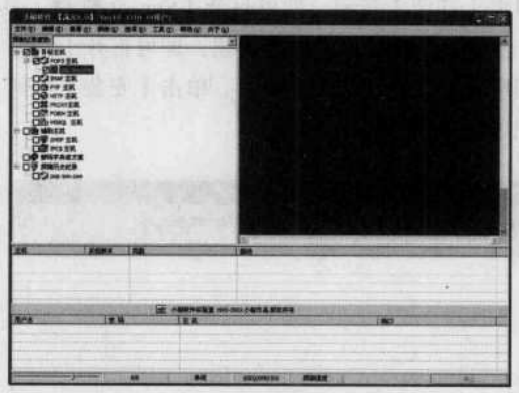


图 1-68　邮箱添加显示

步骤 3：单击【打开】按钮，即可将用户字典添加成功。单击“显示所有项目”选项，即可显示出所有将破解的用户列表，如图 1-70 所示。

图 1-69 【打开】对话框

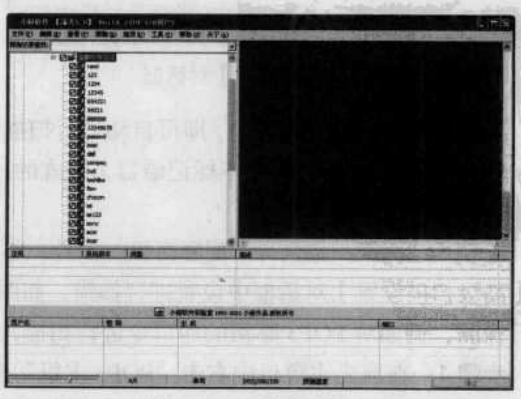


图 1-70　破解用户列表

步骤 4：如果是大量用户，则选择【探测】→【简单模式探测】菜单项，在其中搜索出弱口令用户。如果是少量用户或添加的单个指定用户，则使用密码字典文件进行破解，即右击“解码字典或方案”选项，从快捷菜单中选择【编辑】→【添加】菜单项，即可搜索出相应的弱口令。

4. 命令行嗅探器 Windump

Windump 不仅是一个嗅探器，而且是一个网络报文分析程序。可获得与网络的报文相关的大量的重要底层信息，且能够诊断所有类型的网络问题。

下面举例介绍一下 Windump 工具的使用方法。

例 1：在“命令提示符”窗口中运行“windump -D”命令，即可列出本机可供抓包的全部接口，如图 1-71 所示。

小技巧 当本机存在多个网卡时，使用“windump -D”命令非常有用。例如，某用户机器装有 3 块网卡，若只抓第二块网卡上的包，可用“windump-D”列出机器上所有的网卡，再指定只抓第二块网卡的包，只需继续输入“Windump I 2（2 指网卡序号）”即可。

例 2：在“命令提示符”窗口的命令提示符下输入“windump －n host 192.168.0.12”命令，即可只抓关于 192.168.0.12 主机的包（不管包的方向），如图 1-72 所示。

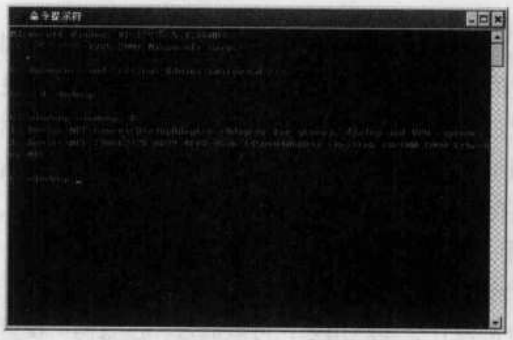


图 1-71 查看本机全部接口

图 1-72 抓取指定主机的包

例 3：也可以通过在命令提示符下输入“windump －n host 192.168.0.12 and udp port 514”命令，则表示只抓关于主机 192.168.0.12 上 udp（User Datagram Protocol，用户数据报协议）协议端口为 514 的包。

例 4：在命令提示符下输入“windump －n net 10.45”命令，则表示只抓 10.45 网段的包（不管包的方向）。

例 5：在命令提示符下输入“windump －n host ！133.191.1.1”命令，则表示抓所有非 133.191.1.1 有关的包。

5. 经典嗅探器 Iris

Iris 网络流量分析监测工具可以帮助系统管理员轻易地捕获和查看用户的使用情况，可以同时检测到进入和发出的信息流，则会自动进行存储和统计，偏重于查看和管理。

具体的操作步骤如下。

步骤 1：初次启动 Iris 时会要求选择绑定网卡，在其中选择好需要绑定的适配器，如图 1-73 所示。单击【确定】按钮，即可进入“Iris”主窗口。单击工具栏上的 ▶ 按钮，即可捕捉所有流经的数据帧，如图 1-74 所示。

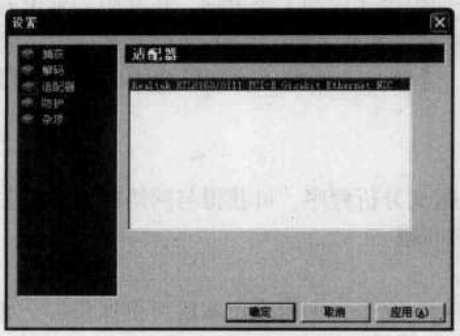


图 1-73　进行网卡绑定

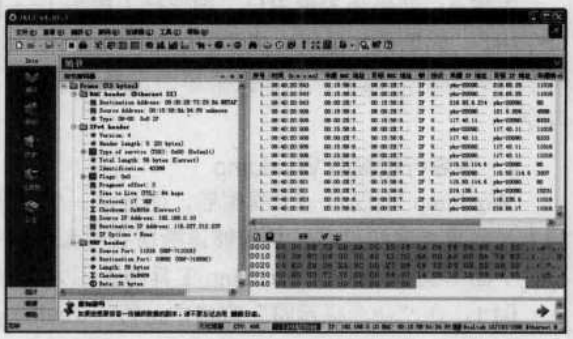


图 1-74　Iris 的主窗口

步骤 2：Iris 可以捕获所在网段里所有的数据包，单击【捕获】按钮图标，主窗口被分为 3 个窗格：左侧“封包解码器”窗格用树型结构显示着每个数据包的详细结构以及数据包每个部分所包含的数据；右下角“封包编辑器”窗格分左右两部分，左边显示数据包的十六进制信息，右边则显示对应的 ASCII 值；右上角“封包列表”窗格显示所有流经的数据包列表（新产生的数据包自动添加到列表里）。在选中特定的数据包之后，其详细信息将会呈树型显示在“封包解码器”窗格中。

步骤 3：单击左侧“Iris”栏目中的【解码】按钮图标，即可对捕获的数据包进行分析，如图 1-75 所示，其主窗口也分为三个窗格。左边的“主机活动”窗格用于列出按照服务类型显示的树型结构的主机传输信息；选中某个服务之后，客户机和服务器之间的会话信息就会显示在“会议列表视图”窗格中，选中某个会话记录可在“会议数据视图”窗格里显示解码后的信息；在“会议列表视图”窗格中每个会话的属性有服务器、客户机、服务器端口、客户机端口、客户机物理地址，还有服务器到客户机的数据量、客户机到服务器的数据量以及总的数据量；右下角的“会议数据视图”窗格显示解码后的会话信息。

步骤 4：流经 Sniffer 的数据很多，但大部分都没什么实际用处，可以通过“过滤器”设置仅处理需要的信息以减少系统资源占用。单击 Iris 主窗口中的【过滤器】图标，即可弹出如图 1-76 所示的配置窗口。

图 1-75　对捕获的数据包进行分析

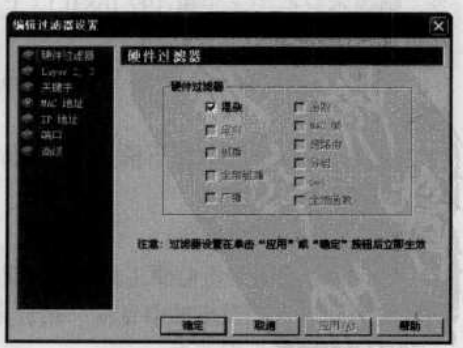


图 1-76　Iris 的配置窗口

步骤 5：单击 按钮，即可按图表形式展示与本机相连数据量最大的 10 台主机，如图 1-77 所示。

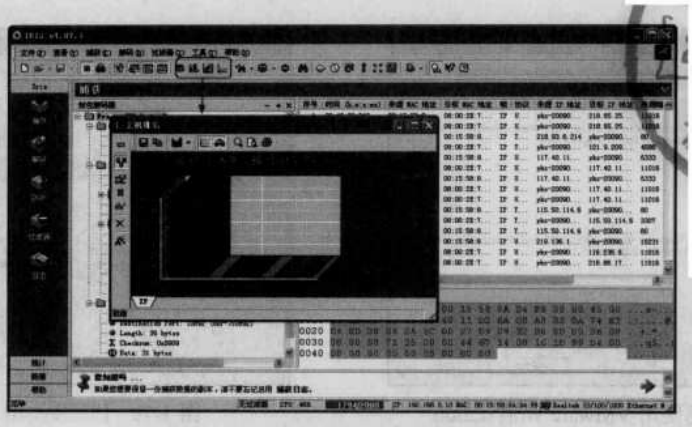


图 1-77 展示与本机相连的主机

在其中可以用多种方式显示（包括饼图、柱状图等），还可在底部状态栏上切换数据包类型（IP 包、MAC 包或 IPX 包）。据此可以查出可疑连接（显然数据通信量最大的几个连接主机都值得怀疑）。

该工具还可以显示 QQ 聊友的 IP 地址，在状态栏上切换到 IP 类型（因为它采用 TCP/IP 协议）后，给聊友发一个信息，图表中马上就可以显示对方的 IP 地址。

提示 硬件过滤是确保选中混杂模式，以确保可捕捉当前网段的数据包。

第 5 招 创建安全测试环境

安全测试环境是指专门用于测试和学习黑客工具操作方法的实验平台，即在已存在的系统中，利用虚拟机创建一个内在的系统，该系统可以与外界独立，但已经与存在的系统建立了网络关系，从而方便使用某些黑客工具进行模拟攻击。即使黑客工具对虚拟机造成了破坏，也可以很快恢复，并不会影响自己已有的计算机系统。

1. 用 VMware 创建虚拟系统

目前，虚拟化技术已经非常成熟，伴随着产品如雨后春笋般地出现：VMware、Virtual PC、Xen、Parallels、Virtuozzo 等，但最流行、最常用的就当属 VMware 了。VMware Workstation 是 VMware 公司的专业虚拟机软件，可以虚拟现有任何操作系统，而且使用简单、容易上手。

安装 VMware Workstation 6.5.2 的具体步骤如下。

步骤 1：下载并双击 VMware Workstation 6.5.2 安装软件，将弹出【VMware 产品安装向导】消息框，并进入【欢迎使用 VMware Workstation 的安装程序】界面，如图 1-78 所示。

步骤 2：在【欢迎使用 VMware Workstation 的安装程序】界面中，单击【Next】按钮，即可打开【安装类型】对话框，在其中选择 VMware Workstation 安装模式，其安装类型包括典型安装和自定义安装两种。这里选择安装类型为“典型（Typical）”安装模式，如果选择“自定义（Custom）”安装模式，则可以进一步选择其安装的组件，如图 1-79 所示。

步骤 3：单击【Next】按钮，即可打开【安装路径】对话框，在其中指定 VMware Workstation 的具体安装位置，如图 1-80 所示。在【安装路径】对话框中默认安装到 C 磁盘，如果想要安装到其他磁盘，单击【Change】按钮，即可打开【更改安装路径】对话框，在其中可以更改软件的安装位置，如图 1-81 所示。

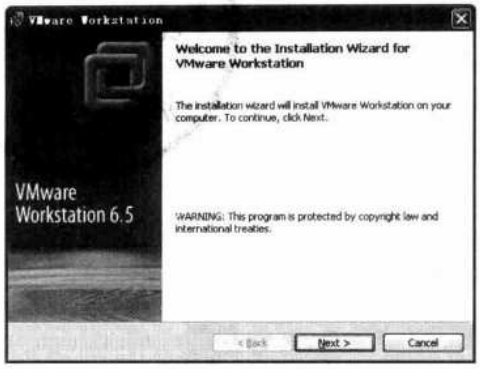


图 1-78 【欢迎使用 VMware Workstation 的安装程序】界面

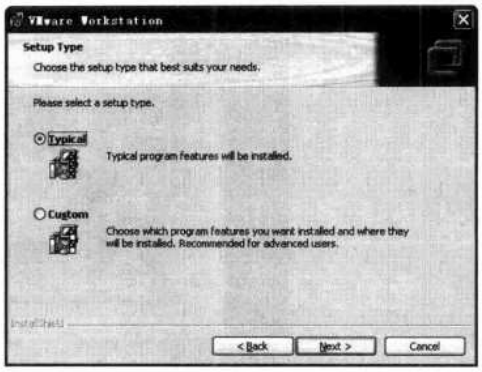


图 1-79 【安装类型】对话框

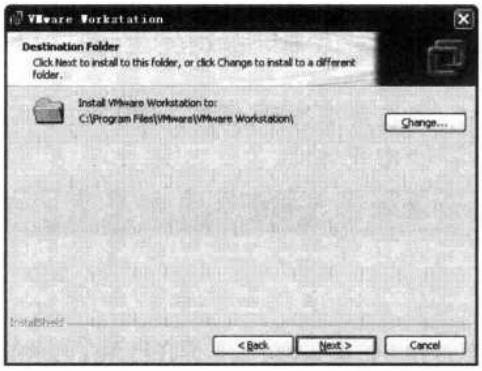


图 1-80 【安装路径】对话框

图 1-81 【更改安装路径】对话框

步骤 4：单击【OK】按钮返回【安装路径】对话框，继续单击【Next】按钮，即可打开【创建程序快捷方式】对话框，在其中设置是否在桌面、开始程序菜单、快速启动栏中创建该程序的快捷方式，如图 1-82 所示。

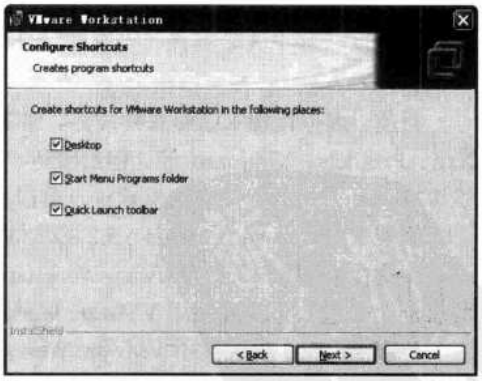


图 1-82 【创建程序快捷方式】对话框

步骤 5：在【创建程序快捷方式】对话框中勾选想要创建的快捷方式，单击【Next】按钮，即可打开【准备安装】对话框，提示用户已经设置完毕，准备开始安装，如图 1-83 所示。如果单击【Back】按钮，则可以返回重新设置安装选项。

步骤 6：在【准备安装】对话框中单击【Install】按钮，即可打开【开始安装】对话框，系统开始安装 VMware Workstation 软件并显示安装进度条，如图 1-84 所示。当安装程序的工作进度完成后，单击【Next】按钮，即可打开【注册信息】对话框，在其中输入个人信息及产品序列号，如图 1-85 所示。若单击【Skip】按钮，则可以跳过此过程。

步骤 7：单击【Enter】按钮，在如图 1-86 所示对话框中单击【Finish】按钮，即可结束 VMware Workstation 6.5 的安装操作。

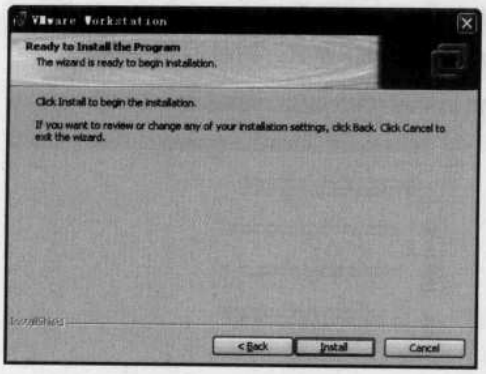


图 1-83 【准备安装】对话框

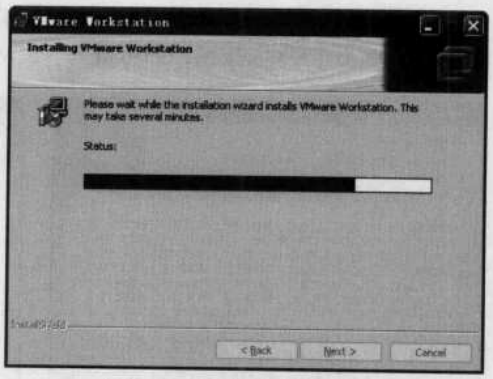


图 1-84 【开始安装】对话框

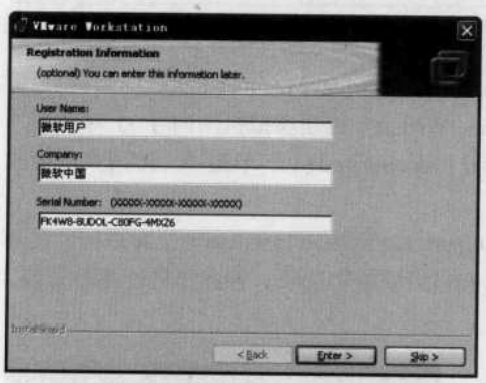


图 1-85 【注册信息】对话框

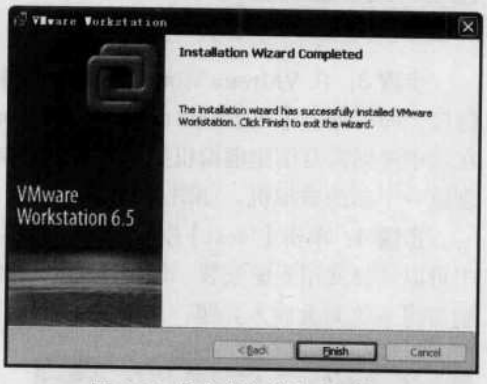


图 1-86 【完成安装】对话框

步骤 8：重新启动计算机后打开“网上邻居”中的网络连接窗口，则看到 VMware Workstation 添加的两个网络连接，如图 1-87 所示。在【设备管理器】窗口中展开“网络适配器”结点，可以看到其中添加的两块虚拟网卡，如图 1-88 所示。

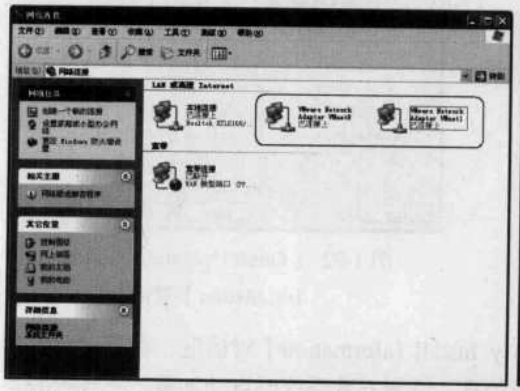


图 1-87 VMware Workstation 安装的两个连接

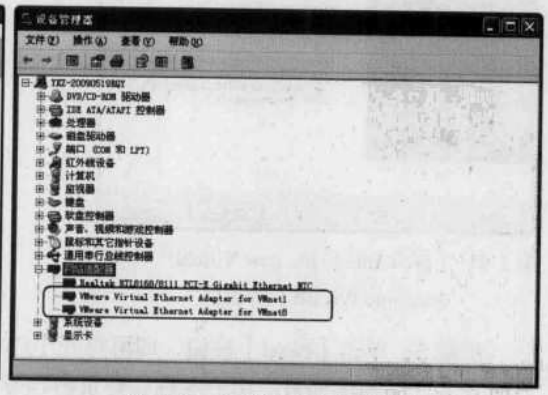


图 1-88 安装的两个虚拟网卡

在安装虚拟操作系统前，一定要先配置好 VMware，下面介绍一下 VMware 的配置过程。

步骤 1：双击桌面上的“VMware Workstation”图标，则系统显示 VMware Workstation 的使用协议，如图 1-89 所示。

步骤 2：选择 “Yes,I accept the terms in the license agreement（我同意批准协议中的条款）”单选项，单击【OK】按钮，即可进入 VMware Workstation 操作界面，如图 1-90 所示。

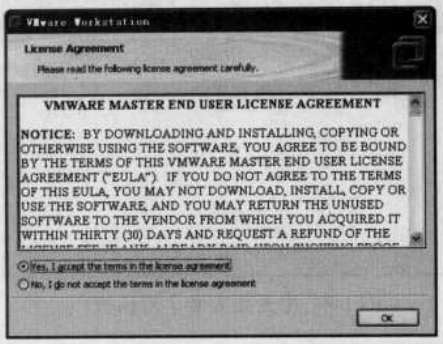


图 1-89　VMware Workstation 的使用协议

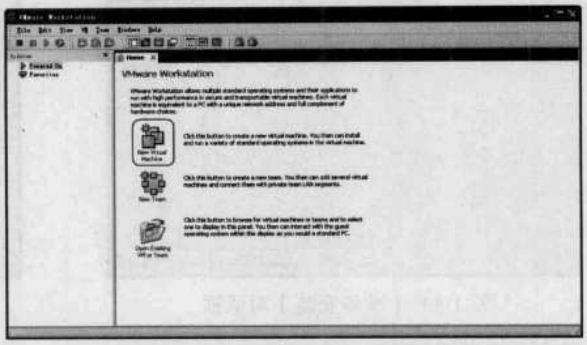


图 1-90　“VMware Workstation”操作界面

步骤 3：在 VMware Workstation 操作界面中单击“New Virtual Machine（新建虚拟机）”超链接，即可弹出【Welcome to the new Virtual Machine Wizard（创建虚拟机的向导）】对话框，在其中根据需要创建虚拟机类型，这里选取“Typical（recommended）”单选项，使用典型模式创建一个新的虚拟机，如图 1-91 所示。

步骤 4：单击【Next】按钮，即可打开【Guest Operating System Installation】对话框，在其中可以选择使用光驱安装、使用系统 ISO 映像安装和以后安装等选项。若选择通过光驱安装，则需将系统光盘放入光驱，如图 1-92 所示。

图 1-91　【Welcome to the new Virtual Machine Wizard】对话框

图 1-92　【Guest Operating System Installation】对话框

步骤 5：单击【Next】按钮，即可打开【Easy Install Information】对话框，在其中可以输入所安装产品的序列号、用户名称、登录密码等信息，以便安装系统时自动加载，实现安装系统的无人值守功能，如图 1-93 所示。

步骤 6：单击【Next】按钮，即可打开【Name the Virtual Machine】对话框，在“Virtual machine name（命名虚拟机）”文本框和“Location”文本框中，分别输入该虚拟机的名字（任意的）以及该虚拟机文件将要存放的位置，如图 1-94 所示。

步骤 7：单击【Next】按钮，即可打开【Specify Disk Capacity】对话框，在“Maximum disk size”中设置主机磁盘空间的大小，如图 1-95 所示。

图 1-93 【Easy Install Information】对话框

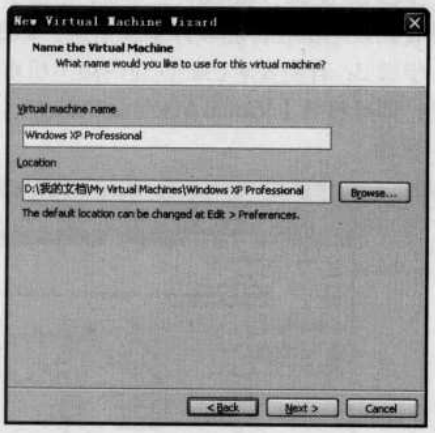


图 1-94 【Name the Virtual Machine】对话框

步骤 8：单击【Next】按钮，即可打开【Ready Create Virtual Machine】对话框，在其中可查看新创建虚拟机的各个选项设置，如图 1-96 所示。

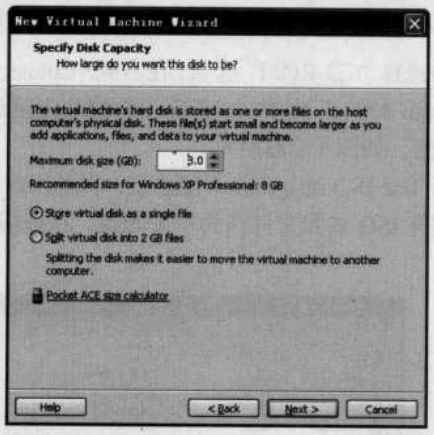


图 1-95 【Specify Disk Capacity】对话框

图 1-96 【Ready Create Virtual Machine】对话框

步骤 9：单击【Finish】按钮，即可完成虚拟机的创建。进入虚拟机存放的路径，将会看到已生成名为“Windows XP Professional.vmx”的虚拟机文件，如图 1-97 所示。

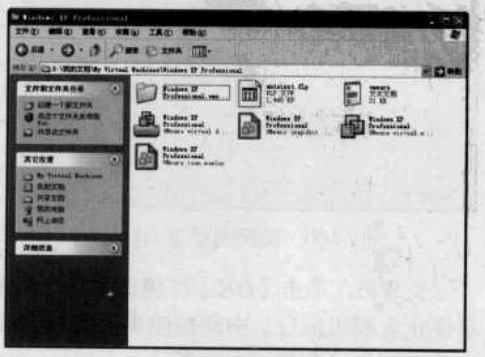


图 1-97 查看虚拟机存放的路径

将其文件夹复制到其他计算机上，可再次用 VMware 导入虚拟机文件，打开建立的虚拟机系统。当成功创建了虚拟机之后，就可以打造攻击目标系统了。

安装虚拟操作系统的具体操作步骤如下。

步骤 1：双击桌面上的“VMware”图标进入

“VMware”主窗口，选择【File】→【Open】菜单项，即可弹出【打开】对话框，在其中指定刚才安装虚拟机的文件路径。单击【打开】按钮，即可打开新创建的虚拟机。

步骤 2：返回 VMware 主界面，单击窗口左侧的“常用”栏，在导入的虚拟机右侧窗口中，即可看到该主机硬件和软件系统信息，如图 1-98 所示。

步骤 3：若需要对已经创建的虚拟机重新进行设置，则单击“Edit Virtual Machine Settings”链接，即可打开【Virtual Machine Settings】对话框，在其中根据硬件需求进行相应修改，如图 1-99 所示。

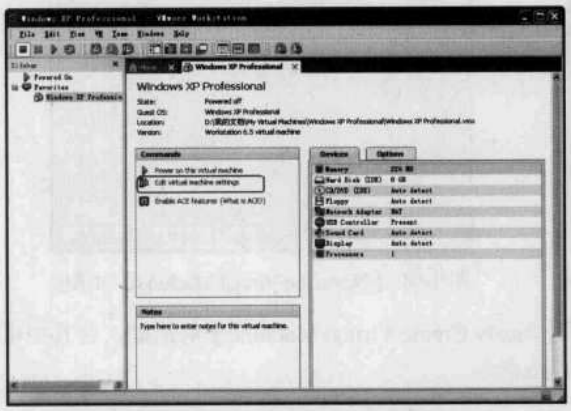


图 1-98　查看该虚拟机的相关信息

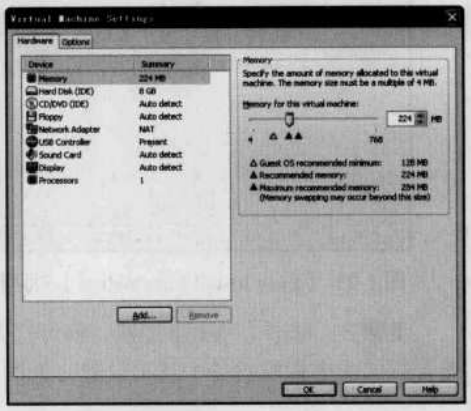


图 1-99　【Virtual Machine Settings】对话框

步骤 4：在【Virtual Machine Settings】对话框中选择“CD-ROM”选项，在右侧“Connection”栏目中选择“Use Physical drive”下拉列表里的“Auto detect”选项。或指定当前物理光驱盘符，单击【OK】按钮，即可在虚拟机中使用当前的光驱，如图 1-100 所示。

步骤 5：如果有光盘 ISO 映像文件，也可勾选“Use ISO image file”复选项，单击【Browse】按钮浏览指定 ISO 映像文件，如图 1-101 所示。即将 ISO 映像文件作为一张光盘，在虚拟机系统中打开。

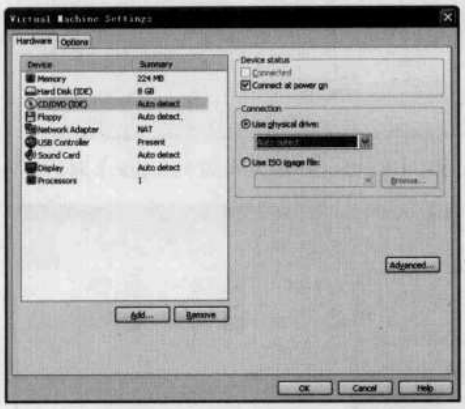


图 1-100　使用物理驱动器

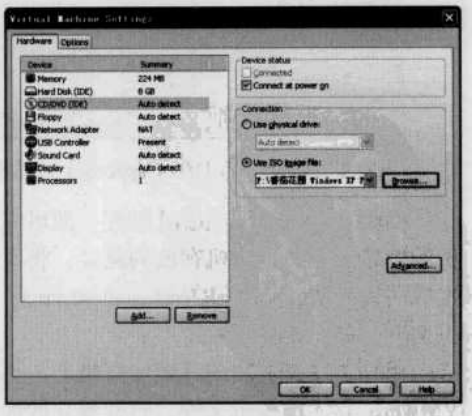


图 1-101　使用 ISO 映像文件

步骤 6：单击【OK】按钮返回到“VMware”主界面中，在工具栏中有三个按钮，红色表示停止虚拟机运行，中间按钮表示暂停虚拟机运行，单击右边第三个绿色三角标志按钮，即可启动虚拟机，如图 1-102 所示。

步骤 7：将鼠标在虚拟机窗口中单击，并按【F2】快捷键进入虚拟机 BIOS 界面。选择“Boot”标签，再选取“CD-ROM Drive”选项，按键盘上的“+”或“-”键，将其调整到最上方，如图 1-103 所示。

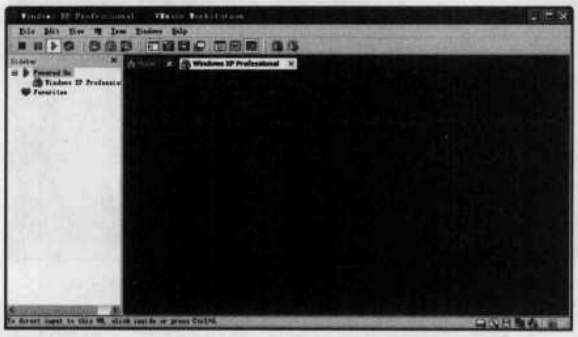


图 1-102 【虚拟机启动】画面

图 1-103 【虚拟机 BIOS】设置界面

步骤 8：按“F10”快捷键，将 BIOS 设置保存并重启虚拟机，在光驱中放入 Windows XP 系统的安装光盘，使用虚拟机从光驱引导系统，如图 1-104 所示。

步骤 9：按实际安装操作系统的方式进行，即可完成虚拟机系统的安装。按“Ctrl+G”组合键将鼠标指针定位在虚拟机窗口中，按“Ctrl+Alt”组合键将鼠标指针从虚拟机释放出来。

2. 虚拟机工具安装

VMware Tools 是 VMware 提供的一套贴心工具，用于提高虚拟显卡、虚拟硬盘的性能，改善鼠标的性能，以及同步虚拟机与主机时钟的驱动程序。安装 VMware Tools 不仅能够提升虚拟机的性能，还可以使鼠标指针在虚拟机内外自由移动，再也不需要使用切换键了。

安装 VMware Tools 的具体操作方法如下。

步骤 1：先启动已经安装好操作系统的虚拟机，单击虚拟机屏幕下方的【Install Tools】按钮，或选择【VM】→【Install VMware Tools】菜单项，即可启动 VMware Tools 安装向导，如图 1-105 所示。

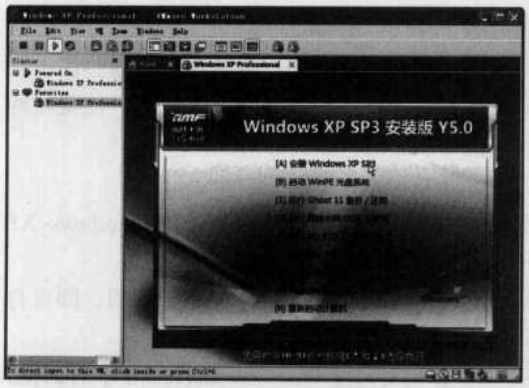


图 1-104 【光驱引导系统】界面

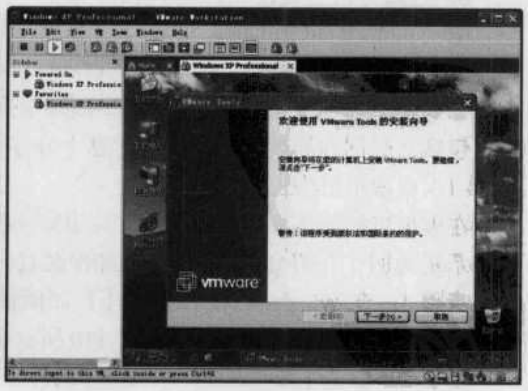


图 1-105 VMware Tools 安装向导

步骤 2：单击【下一步】按钮，在显示的对话框中选择安装方式，如图 1-106 所示。单击【下一步】按钮，即可打开【已准备好安装程序】对话框，如图 1-107 所示。

图 1-106　选择安装类型

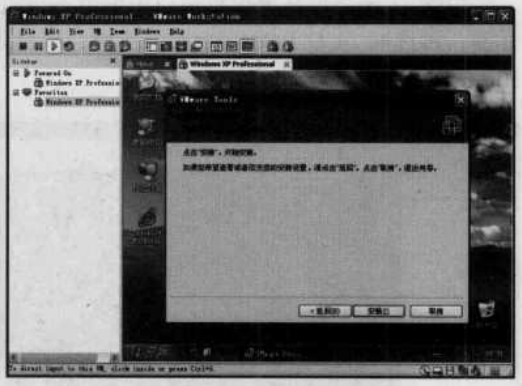


图 1-107 【已准备好安装程序】对话框

步骤 3：单击【安装】按钮，系统开始安装并显示安装进度，如图 1-108 所示。安装完成后，则显示如图 1-109 所示对话框。单击【完成】按钮，重启系统后即可完成安装操作。

图 1-108　开始安装

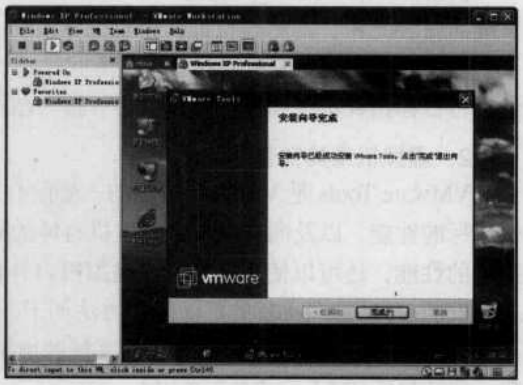


图 1-109 【安装向导完成】对话框

3．在虚拟机上架设 IIS 服务器

IIS（Internet Information Server，互联网信息服务）作为一种 Web（网页）服务组件，包括 Web 服务器、FTP 服务器、NNTP（Network News Transport Protocol，网络新闻传输协议）服务器和 SMTP 服务器，分别用于网页浏览、文件传输、新闻服务和邮件发送等方面，使得在网络（包括互联网和局域网）上发布信息十分容易。

（1）在虚拟机中安装 IIS 服务器

在虚拟机的操作系统中也可以安装 IIS 服务器，这里以在 VMware 中建立的 Windows XP 操作系统为例，介绍 IIS 服务器安装和配置过程。具体的操作步骤如下。

步骤 1：在 Windows XP 系统的【控制面板】窗口中双击“添加/删除程序”选项，即可打开【添加或删除程序】窗口，如图 1-110 所示。

步骤 2：单击【添加/删除 Windows 组件】按钮，即可打开【Windows 组件向导】对话框，在其中勾选“在 Internet 信息服务（IIS）”复选项以设置 IIS 信息，如图 1-111 所示。

步骤 3：单击【详细信息】按钮，即可弹出【Internet 信息服务（IIS）】对话框，在其中取消默认的“SMTP Service”服务和“FTP”服务，如图 1-112 所示。

图 1-110 【添加或删除程序】窗口

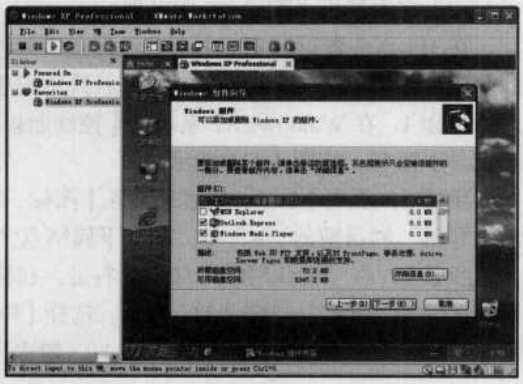


图 1-111 【Windows 组件向导】对话框

步骤 4：在设置完毕之后，单击【确定】按钮，即可返回到【Windows 组件向导】对话框中。此时在光驱中插入 Windows 系统安装光盘，单击【下一步】按钮，即可开始 IIS 服务器的安装，其安装进度如图 1-113 所示。

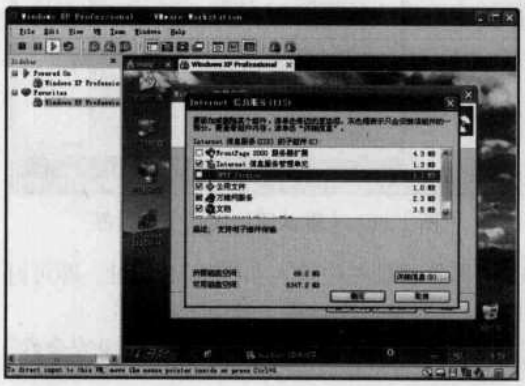


图 1-112 【Internet 信息服务（IIS）】对话框

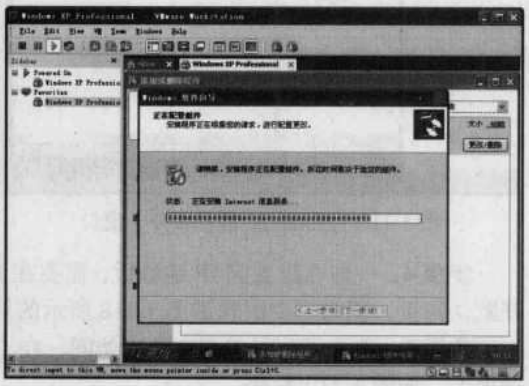


图 1-113 【正在配置组件】对话框

步骤 5：在 IIS 服务器安装完成之后，将会在【Windows 组件向导】对话框中出现相应的提示信息，如图 1-114 所示。

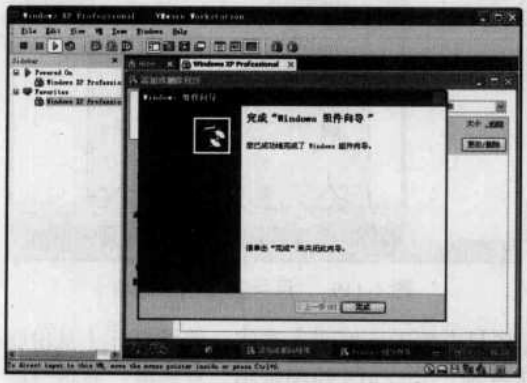


图 1-114 【完成“Windows 组件向导”】对话框

图 1-115 【管理工具】窗口

（2）在虚拟机中配置 IIS 服务器

在 IIS 服务器附加完毕之后，往往还需要进行配置 IIS 服务器的操作。为了方便用户，在此介绍在虚拟机的 Windows XP 操作系统下配置 IIS 服务器的方法。具体的操作步骤如下。

步骤 1：在 Windows XP 系统的【控制面板】窗口中双击【管理工具】图标，即可打开【管理工具】窗口，如图 1-115 所示。

步骤 2：双击【Internet 信息服务】图标，即可打开【Internet 信息服务】窗口，单击“本地计算机”栏目前的“+”号，和其下属结点“网站”前的“+”号，如图 1-116 所示。

步骤 3：在“默认网站”结点上右击，在快捷菜单中选择【属性】选项，即可打开【默认网站属性】对话框，如图 1-117 所示。选择【网站】选项卡“IP 地址”下拉列表框中本机的 IP 地址（如：本机的 IP 地址为 127.0.0.1），单击【确定】按钮，即可完成对网站 IP 地址设置。

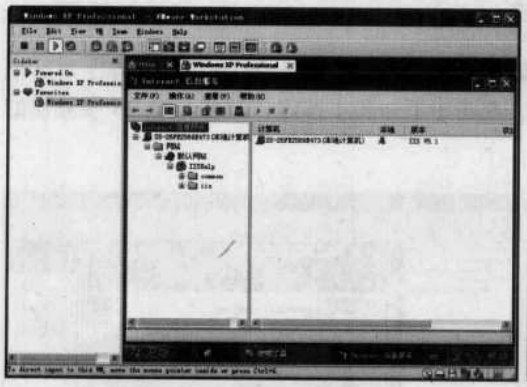


图 1-116 【Internet 信息服务】窗口

图 1-117 【默认网站属性】对话框

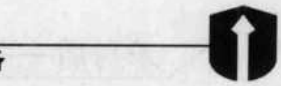
步骤 4：一般在设置完 IP 地址后，需要在 IE 浏览器地址栏中输入本机的 IP 地址，即可打开默认网页，但有时会出现如图 1-118 所示的对话框（这是由于设置了错误的权限）。

步骤 5：首先需要设置允许匿名访问，在【默认网站 属性】对话框中选择“目录安全性”选项卡，如图 1-119 所示。

图 1-118 IE 浏览器地址栏中输入本机的 IP 地址

图 1-119 “目录安全性”选项卡

步骤 6：单击“匿名访问和身份验证控制”栏目右侧的【编辑】按钮，即可打开【身份验证方法】对话框，在其中勾选“匿名访问”复选框和“允许 IIS 控制密码”复选框，并填写匿名访问使用的“用户名”和“密码”，如图 1-120 所示。连续单击【确定】按钮，即可成功设



置权限。在【身份验证方法】对话框中单击“用户名”右侧的【浏览】按钮，即可打开【选择用户】对话框，在其中可以选择用户，如图 1-121 所示。

图 1-120 【身份验证方法】对话框

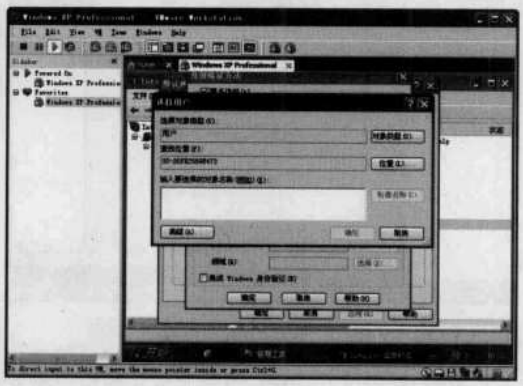


图 1-121 【选择用户】对话框

4．在虚拟机中安装网站

建好了 IIS 服务器，安装了动态域名解析客户端，用户的网站已经有了栖身之所。现在就可以安装网站了。可自己编辑网站程序，也可从网上下载完整的源程序进行安装。

（1）解压安装

解压安装法是目前安装网站最简单的方法，很多网站都是用这种方法安装的。

步骤 1：在网上下载网站源程序并将压缩包解压之后，即可打开【Internet 信息服务】窗口。右击“默认网站”图标，在快捷菜单中选择“属性”选项，即可打开【默认网站属性】对话框，如图 1-122 所示。

步骤 2：在“主目录”选项卡的“本地路径”文本框中输入下载网站源文件所在位置，或单击【浏览】按钮找到网站源文件。切换到“文档”选项卡，在“默认文档”栏目中可以看到各种默认的文档，如图 1-123 所示。

图 1-122 【默认网站属性】对话框

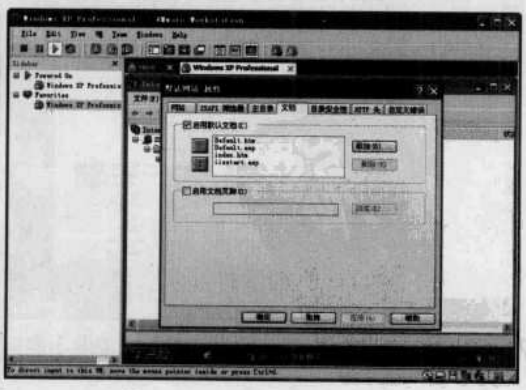


图 1-123 网站的默认文档

步骤 3：单击【添加】按钮，即可打开【添加默认文档】对话框，在“默认文档名”文本框中输入新添加的文档名 index.asp，如图 1-124 所示。

步骤 4：单击【确定】按钮，即可关闭【添加默认文档】对话框，此时在“默认文档”列表中可看到新添加的 index.asp，如图 1-125 所示。

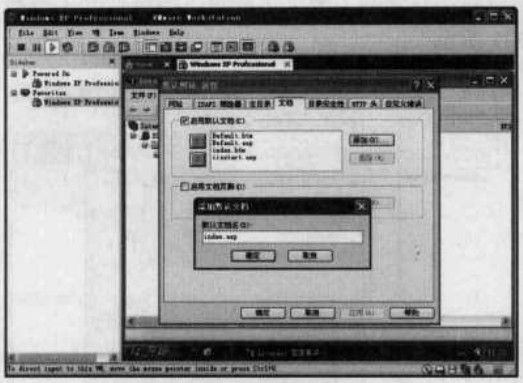


图 1-124 【添加默认文档】对话框

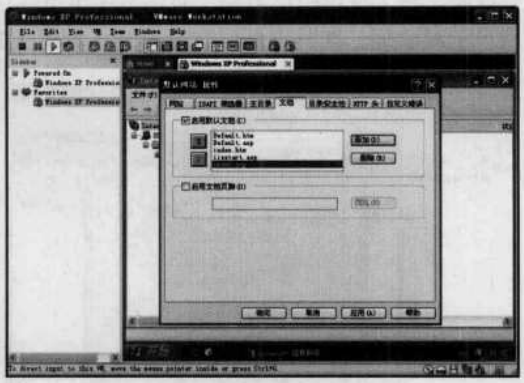


图 1-125 添加的默认文档

步骤 5：在【Internet 信息服务】窗口中将安装后默认存在的几个虚拟目录删掉（如“IISHelp”和“Printers”）之后，重新打开【Internet 信息服务】窗口，在本地计算机的浏览器地址中输入虚拟机 IP 地址，就可以打开刚安装的网站了。

（2）程序安装法

在安装普通软件时只需要单击安装程序就可以了，某些网站程序安装也是这样的，在这里以最常见的动网论坛为例介绍其安装过程。

步骤 1：下载并解压动网论坛程序，在【Internet 信息服务】窗口中把虚拟目录设置为动网论坛所在的文件夹，运行安装程序 dvbbs.exe，即可打开【动网先锋软件（Aspsky.Net）安装】窗口，如图 1-126 所示。

步骤 2：在选择安装目标文件夹之后，单击【安装】按钮，即可完成对动网论坛的安装，如图 1-127 所示。

图 1-126 【动网先锋软件（Aspsky.Net）安装】窗口

图 1-127 安装完毕后的动网论坛文件

第 6 招 Virtual PC 安全测试环境

除 VMware 外，还有一个微软公司开发的非常有名的虚拟机软件 Virtual PC，它与 VMware 虚拟机齐名。它的特点是界面简洁，但功能方面不如 VMware 虚拟机。Virtual PC 与一般软件的安装方法相同，操作也十分简单。

1. Virtual PC 安装流程

在 Virtual PC 程序中没有创建虚拟机前启动 Virtual PC 程序，系统将自动弹出创建虚拟机的安装向导，以方便用户创建虚拟机。在 Virtual PC 程序中创建虚拟机的具体步骤如下。

步骤 1：在 Virtual PC 界面中单击【新建】按钮，即可打开【新建虚拟机向导】对话框，如图 1-128 所示。单击【下一步】按钮，即可打开【选项】对话框，在其中可以选取“新建一台虚拟机”单选项，如图 1-129 所示。

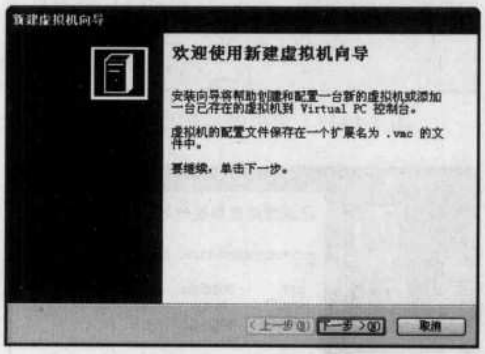


图 1-128 【新建虚拟机向导】对话框

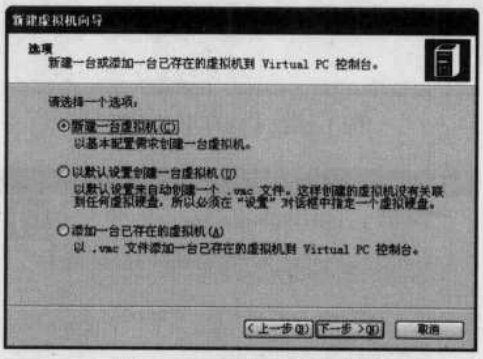


图 1-129 【选项】对话框

步骤 2：单击【下一步】按钮，即可打开【虚拟机的名称和位置】对话框，在其中可以指定虚拟机文件保存的名称和位置，如图 1-130 所示。

步骤 3：单击【下一步】按钮，即可打开【操作系统】对话框，在其中可以选择当前虚拟机所安装的系统版本，如图 1-131 所示。单击【下一步】按钮，即可打开【内存】对话框，在其中可以设置虚拟机运行时使用内存的大小，如图 1-132 所示。

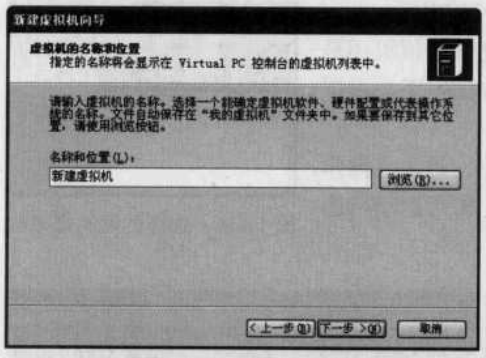


图 1-130 【虚拟机的名称和位置】对话框

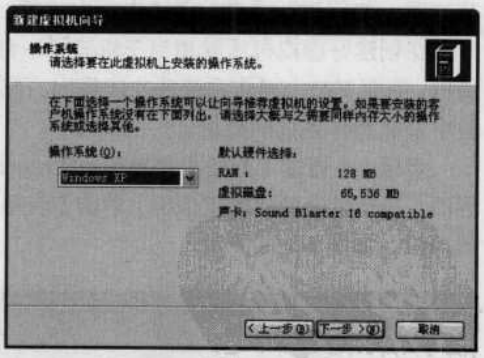


图 1-131 【操作系统】对话框

步骤 4：单击【下一步】按钮，即可打开【虚拟硬盘选项】对话框，在其中根据需要选择一种所需要使用的硬盘方式，这里选取“新建虚拟硬盘”单选项，如图 1-133 所示。

步骤 5：单击【下一步】按钮，即可打开【虚拟硬盘位置】对话框，在其中可以指定虚拟硬盘保存的名称与路径，并可以指定虚拟硬盘的大小，如图 1-134 所示。

步骤 6：单击【下一步】按钮，即可打开【完成新建虚拟机向导】对话框。再单击【完成】按钮，即可结束虚拟机的创建操作，如图 1-135 所示。在创建好虚拟机之后，返回 Virtual PC 操作界面，在其中选择已经创建的虚拟机，如图 1-136 所示。

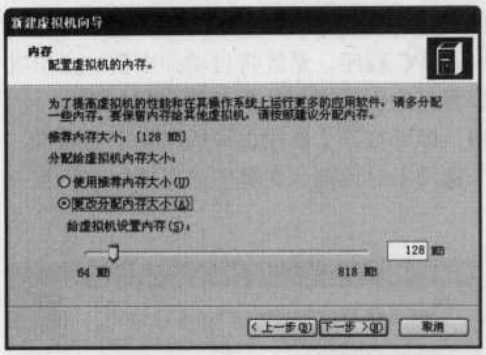


图 1-132 【内存】对话框

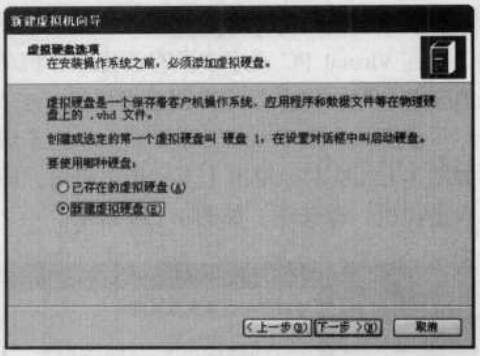


图 1-133 【虚拟硬盘选项】对话框

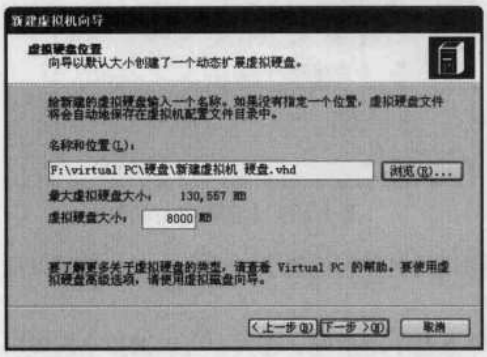


图 1-134 【虚拟硬盘位置】对话框

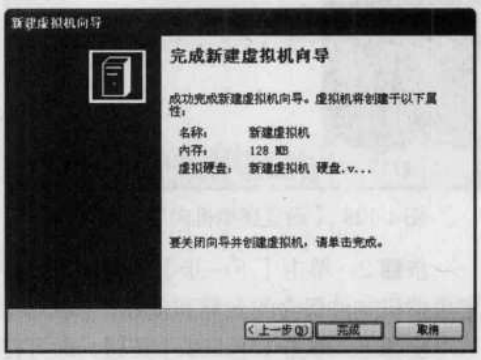


图 1-135 【完成新建虚拟机向导】对话框

步骤 7：最后单击【设置】按钮，即可打开【设置新建虚拟机】对话框，在其中可以设置其选项，如创建新硬盘、调整内存大小等，如图 1-137 所示。

在创建好虚拟机后就相当于组装了一台电脑，此时虚拟机还是裸机，需要安装上操作系统后才能使用。下面简单介绍一下在虚拟机中安装操作系统的方法。

步骤 1：通过【开始】菜单运行 Virtual PC 程序，进入其操作界面，选择已经创建的虚拟机，单击【启动】按钮，即可启动所选虚拟机，如图 1-138 所示。

图 1-136 选择创建的虚拟机

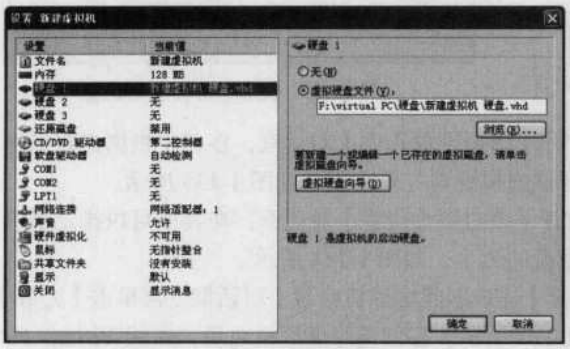


图 1-137 【设置新建虚拟机】对话框

图 1-138 启动虚拟机

步骤 2：在虚拟机启动过程中按【Del】键，即可进入其 CMOS 界面，在其中设置其有关选项，如图 1-139 所示。

步骤 3：按【F10】按钮，将 CMOS 设置保存并重新启动虚拟机，在光驱中放入 Windows XP 系统的安装光盘，使用虚拟机从光驱引导系统，如图 1-140 所示。按实际安装操作系统的方式进行，即可完成虚拟机操作系统的安装。

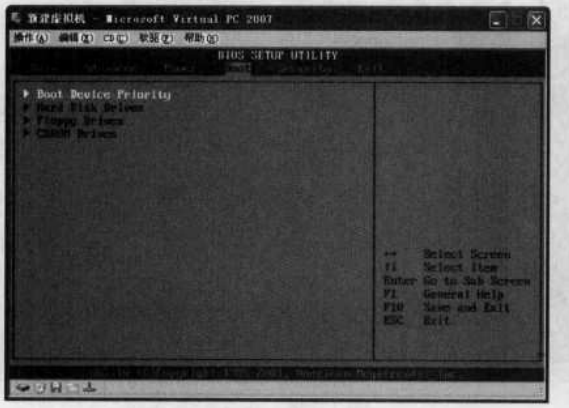


图 1-139 CMOS 界面

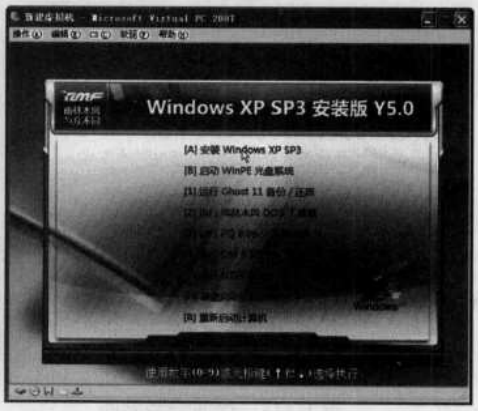


图 1-140 虚拟机系统安装引导界面

小技巧 在 Virtual PC 虚拟机窗口中单击后，鼠标指针就会被锁定在虚拟机窗口中，如果要在主机窗口中使用鼠标，可按【Alt】键将其释放。如果按【Alt+Enter】组合键，则可使虚拟机在全屏或窗口显示模式之间进行切换。

2. Virtual PC 网络设置

为了能够更好地完成对虚拟机的操作，还需安装 Virtual PC 虚拟机的附加模块，以实现在虚拟机中调整屏幕的刷新率、使用网络功能和使用鼠标指针整合功能（使鼠标指针在主机与虚拟机之间随意移动，而不会将鼠标指针局限于虚拟机或主机区域内），还可共享主机硬盘上的文件夹，以及在虚拟机中通过共享文件夹来使用主机物理硬盘上的数据。

安装附加模块的具体操作步骤如下。

步骤 1：在虚拟机界面中选择【操作】→【安装或升级附加模块】菜单项，如图 1-141 所示。同时系统将显示如图 1-142 所示的提示信息。

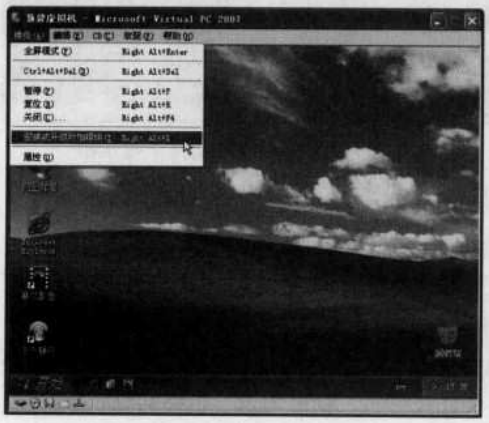


图 1-141 新建虚拟机主界面

图 1-142 【新建虚拟机】提示框

步骤 2：单击【继续】按钮，虚拟机将启动附加模块的安装向导，如图 1-143 所示。

步骤 3：单击【下一步】按钮，虚拟机系统开始安装附加模块并显示安装进度，如图 1-144 所示。在安装完毕后，即可弹出【安装程序已完成】对话框，如图 1-145 所示。

图 1-143　欢迎安装界面

图 1-144　正在安装界面

步骤 4：单击【完成】按钮，即可结束虚拟机附加模块的安装操作，同时弹出【虚拟机添加件】提示框，提示“虚拟机附加模块只有在操作系统安装完毕后才能安装。在虚拟机中安装好附加模块后需要重新启动虚拟机，附加模块的功能才能生效”信息，如图 1-146 所示。

图 1-145　【安装程序已完成】对话框

图 1-146　【虚拟机添加件】提示框

在安装好附加模块后，用户可以利用共享功能，将主机上的文件或文件夹与虚拟机共享，通过虚拟机能够使用主机上的数据。具体的设置方法如下。

步骤 1：在启动虚拟机后，单击虚拟机窗口上方的【编辑】→【设置】菜单项，即可打开当前虚拟机的设置对话框，在其中选取“共享文件夹”选项，如图 1-147 所示。

步骤 2：单击【共享文件夹】按钮，即可弹出如图 1-148 所示的对话框。在其中选择需要共享的文件夹，设置驱动器名称，若需要永久性共享此文件夹，则可勾选“始终共享”复选框，否则该共享在虚拟机重启后将失效。

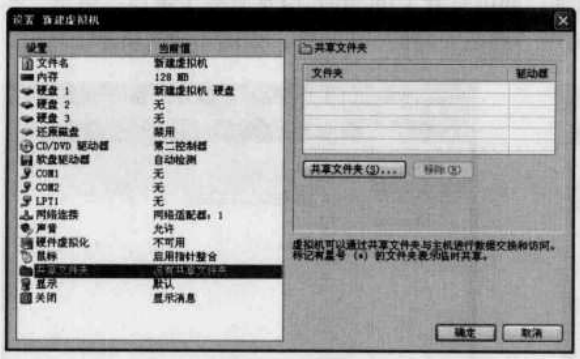


图 1-147 【设置 新建虚拟机】对话框

图 1-148 【浏览文件夹】对话框

步骤 3：单击【确定】按钮，即可将所选文件夹添加共享文件夹列表中，如图 1-149 所示。在共享文件夹设置完毕之后，打开“我的电脑”窗口，即可看到“共享文件夹”的图标，如图 1-150 所示。

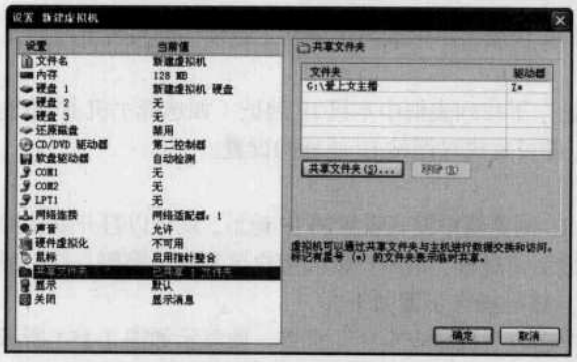


图 1-149 添加共享文件夹

图 1-150 【我的电脑】窗口

第 7 招 虚拟机网站平台

使用黑客工具不仅可攻击个人计算机还可攻击网站，当前动态网站服务器大多使用 ASP（Active Server Page，动态服务器页面）、PHP（Hypertext PreProcessor，超文本预处理）两种网页语言。下面简单介绍一下这两种网络平台在虚拟机中搭建与配置方法，以加深对系统漏洞和程序漏洞的认识。

1. 虚拟机 ASP 网站平台

ASP 是一种 Web 服务器端的开发环境，可以产生和执行动态的、交互的和高性能的 Web 服务应用程序。使用 ASP 架设 Web 动态服务网络平台离不开微软公司开发的 IIS 程序，它在 Windows 2000/XP/2003 系统中作为一个系统组件存在。

（1）在虚拟机中配置 IIS 服务器

在 IIS 服务器附加完毕之后，往往还需要进行配置 IIS 服务器的操作。为方便用户，在此介绍在虚拟机的 Windows XP 操作系统下配置 IIS 服务器的方法。具体的操作步骤如下。

步骤 1：在 Windows 系统的【控制面板】窗口中双击【管理工具】图标，即可打开【管理工具】窗口，如图 1-151 所示。

步骤 2：双击【Internet 信息服务】图标，即可打开【Internet 信息服务】窗口，单击“本地计算机”栏目前的“+”号，和其下属结点“网站”前的“+”号，如图 1-152 所示。

图 1-151 【管理工具】窗口

图 1-152 【Internet 信息服务】窗口

步骤 3：在“默认网站”结点上右击，在快捷菜单中选择【属性】选项，即可打开【默认网站 属性】对话框，如图 1-153 所示。

步骤 4：选择【网站】选项卡“IP 地址”下拉列表框中本机 IP 地址（如选择主机 IP 地址为 192.168.0.18）后，单击【确定】按钮，即可完成对网站 IP 地址的设置。

（2）设置默认网站的访问权限

一般情况下，设置网站的 IP 地址后在 IE 浏览器中输入设置的 IP 地址，就可以打开默认网页，但有时可能会在打开网页时显示一个提示信息框，请用户输入用户名和登录密码，这一般是由于网站登录权限设置不对而引起的。具体的操作步骤如下。

步骤 1：在【默认网站属性】对话框中选取“目录安全性”标签，则显示如图 1-154 所示的对话框。单击“匿名访问和身份证控制”区域中的【编辑】按钮，即可打开【身份验证方法】对话框，如图 1-155 所示。

图 1-153 【默认网站 属性】对话框

图 1-154 “目录安全性”标签页

步骤 2：在确保“匿名访问”复选框处于选取状态，并在“用户名”文本框中输入匿名访问使用的用户名和密码即可。此外，还需要选取“允许 IIS 控制密码”复选框。单击【确定】

按钮，即可完成网站访问权限的设置。

2. 快速架设 ASP（Active Server Page）服务器和 PHP（Professional Hypertext Preprocessor）服务器

现在，Internet 网络上有一些体积较小，操作方便的工具，可以帮助用户快速架设 ASP 或 PHP 服务器，从而节省不少时间。

（1）快速架设 ASP 服务器

除使用 IIS 架设 ASP 网站外，还可使用其他软件，如小旋风 ASP Web 服务器，它体积小巧，但操作非常简单。使用小旋风 ASP Web 服务器架设 ASP 服务器的具体操作步骤如下。

步骤 1：双击“小旋风 ASP Web 服务器”安装程序图标，即可进入【欢迎安装小旋风 ASP Web 服务器向导】对话框，如图 1-156 所示。

图 1-155 【身份验证方法】对话框

图 1-156 【欢迎安装小旋风 ASP Web 服务器向导】对话框

步骤 2：单击【下一步】按钮，即可打开【阅读软件说明】对话框，在其中可以详细阅读软件的说明书，如图 1-157 所示。

步骤 3：在认真阅读完毕后，单击【下一步】按钮，即可打开【选择程序文件夹】对话框，在其中可以设置程序文件夹的名称，如图 1-158 所示。单击【下一步】按钮，即可打开【安装路径选取】对话框，在其中可以选择程序安装的目标位置，如图 1-159 所示。

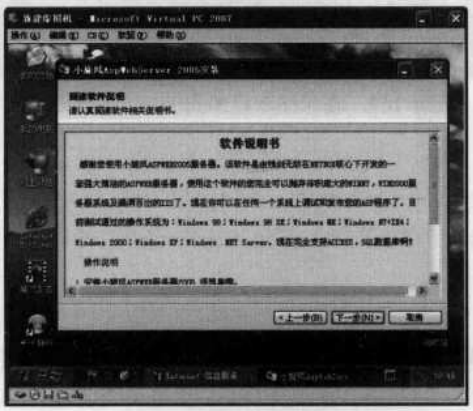


图 1-157 【阅读软件说明】对话框

图 1-158 【选择程序文件夹】对话框

步骤 4：单击【下一步】按钮，程序开始安装并显示安装的进度。当程序安装完成后，即可弹出【安装完成】对话框，在其中勾选“现在运行 Asp Web Server 2005”复选框。如图 1-160 所示。单击【完成】按钮，即可弹出【错误对话框】消息框，提示“服务器启动失败”信息，如图 1-161 所示。

图 1-159 【安装路径选取】对话框

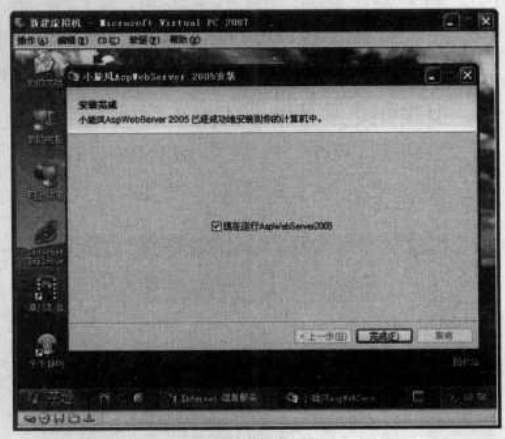


图 1-160 【安装完成】对话框

步骤 5：单击【确定】按钮并重新启动计算机，再双击桌面上的“启动 Asp Web Server 2005”应用程序图标，即可成功启动服务器并在任务栏中看到相应的启动图标，如图 1-162 所示。

图 1-161 【错误对话框】消息框

图 1-162 查看任务栏中启动成功后的图标

（2）快速架设 PHP 服务器

下面介绍一种可以快速架设 PHP 服务器的方法。VertrigoServ 是一款可以在 Windows 系统上安装 Apache 2.x.x、PHP 5.x.x、MySQL 5.x.x 及 PhpMyAdmin 的 all-in-one 安装包，可以让用户在电脑变成支持 PHP 的 Web 服务器。

具体的操作方法如下。

步骤 1：双击从网络下载的压缩包文件，指定其解压的路径，再双击其安装文件，启动其安装程序，如图 1-163 所示。选择“Chinese（Simplified）”项，单击【OK】按钮，需要以简体中文语言进行安装，如图 1-164 所示。

图 1-163 选择安装语言

图 1-164 欢迎安装界面

步骤 2：单击【下一步】按钮，在如图 1-165 所示的对话框中阅读该软件许可协议。单击【我接受】按钮，在其中可以选择安装的组件，如图 1-166 所示。

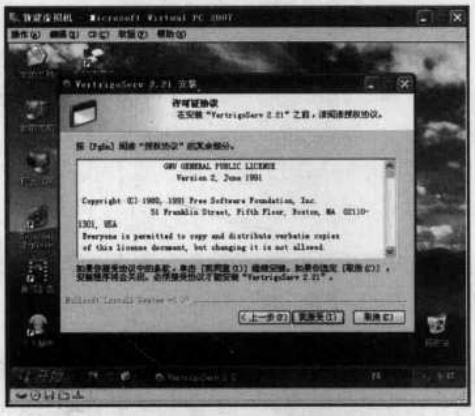


图 1-165 【许可证协议】对话框

图 1-166 【选择组件】对话框

步骤 3：单击【下一步】按钮，指定 VertrigoServ 的安装路径，如图 1-167 所示。单击【下一步】按钮，在其中可以设置“开始”菜单的快捷方式名称，如图 1-168 所示。

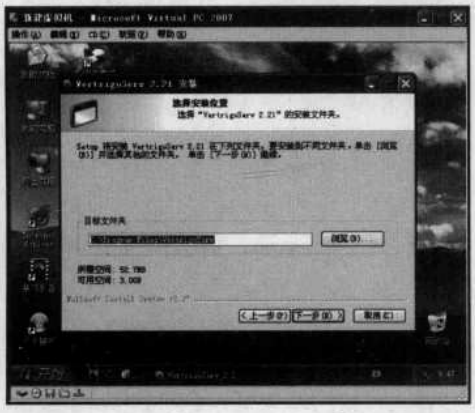


图 1-167 【选择安装位置】对话框

图 1-168 【选择“开始菜单”文件夹】对话框

步骤 4：单击【安装】按钮，即可安装 VertrigoServ 软件并显示其安装进度，如图 1-169 所示。在安装完毕后，在如图 1-170 所示的对话框中单击【完成】按钮，即可结束操作。

图 1-169 【正在安装】对话框

图 1-170 【完成安装】对话框

步骤 5：运行 VertrigoServ 软件后，PHP 服务器也就搭建完成了。此时 VertrigoServ 软件在 Windows 通知栏中显示 标。单击【Hide this window and start server】按钮，即可启动 PHP Web 服务，如图 1-171 所示。此时在 IE 浏览器地址栏中输入 http://localhost，回车后即可看到自己的 PHP 网页，如图 1-172 所示。若想退出服务器，只需单击 图标，在快捷菜单中选择“Shutdown and exit”选项，即可关闭 VertrigoServ 软件。

图 1-171 选项设置消息框

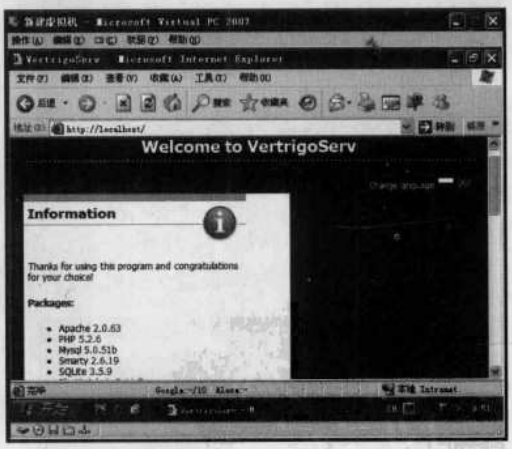


图 1-172 浏览自己生成的 PHP 网页

3. ASP+PHP+CGI 网站平台

这里介绍一款可快速打造 ASP+PHP+CGI 综合网站服务的工具 Abyss Web Server，它具有 Linux 和 Windows 两个版本，并还支持 Windows 最新的 Vista 系统。

使用 Abyss Web Server 架设网络平台的具体操作方法如下。

步骤 1：双击 Abyss Web Server 的安装程序，启动其安装向导，如图 1-173 所示。单击【I Agree】按钮，则显示如图 1-174 所示的对话框，在其中选择需要支持的网站类型。单击【Next】按钮，用户可指定 Abyss Web Server 的安装路径，如图 1-175 所示。

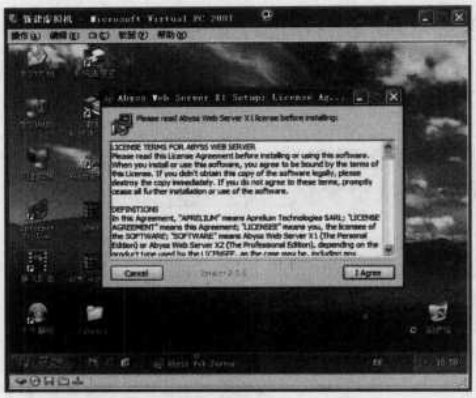


图 1-173 “安装许可协议”界面

图 1-174 选择需要支持的网站类型

步骤 2：单击【Install】按钮，即可开始安装并显示其安装进度，如图 1-176 所示。安装完毕后，显示如图 1-177 所示的对话框，在其中可选择 Abyss Web Server 的启动方式，这里选择用户登录自动启动方式。

图 1-175 选择安装的路径

图 1-176 显示安装的过程

步骤 3：单击【OK】按钮，系统显示安装完毕，是否立即启动 Abyss Web Server 的提示信息，单击【是】按钮，即可启动 Abyss Web Server 并在通知栏显示该程序图标 ，如图 1-178 所示。

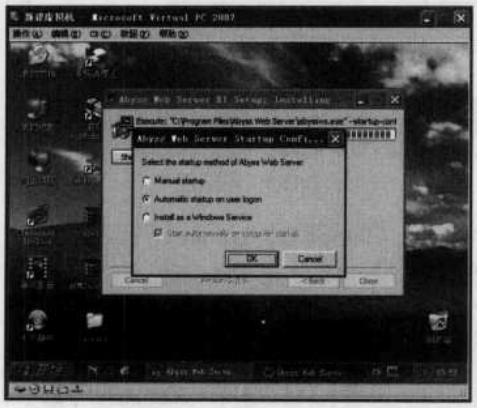


图 1-177 选择 Abyss Web Server 启动方式

图 1-178 Abyss Web Server 安装提示信息

步骤 4：双击通知栏中的图标，则弹出是否增加设置的提示信息，如图 1-179 所示。单击【确定】按钮，即可运行 IE 浏览器并打开 http:// 127.0.0.1:9999/console/language 页面，如图 1-180 所示。

图 1-179　是否增加设置的提示信息

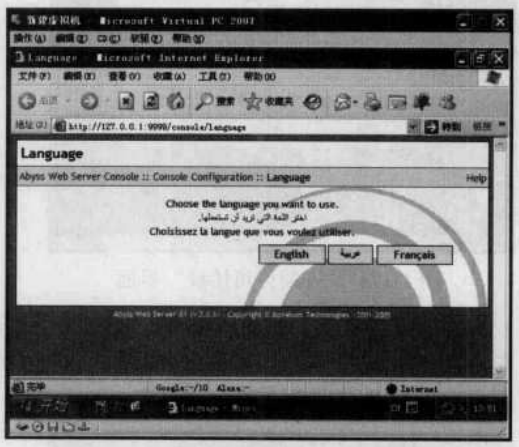


图 1-180　“选择 Language”窗口

步骤 5：单击网页中的【English】按钮，则显示设置用户名称和登录密码的网页，如图 1-181 所示。在设置好用户名和登录密码后，单击【OK】按钮，即可弹出如图 1-182 所示的对话框，在其中输入刚才设置的用户名和密码。单击【确定】按钮进入服务器管理页面，如图 1-183 所示。

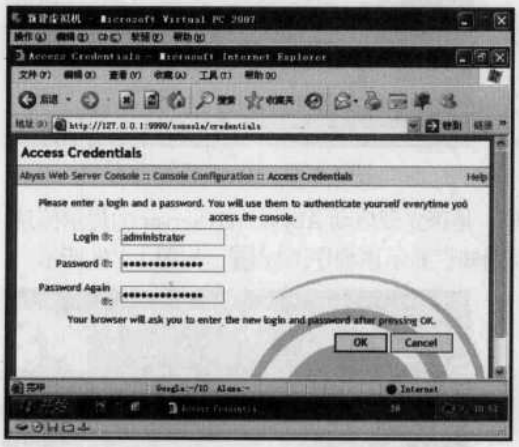


图 1-181　“Access Credentials”窗口

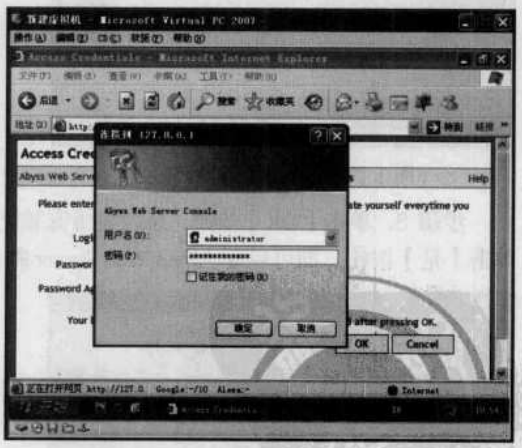


图 1-182　连接用户

步骤 6：单击【Server Configuration】按钮，即可进入“Server Configuration”页面，如图 1-184 所示。再单击【Parameters】按钮，在其中设置服务器根目录、最大连接数、连接超时等选项，如图 1-185 所示。

步骤 7：单击【OK】按钮返回“服务器管理”页面，在其中根据需要进行相应的设置，如图 1-186 所示。再单击【General】按钮，即可设置网站协议类型、默认端口、文档路径等选项，如图 1-187 所示。

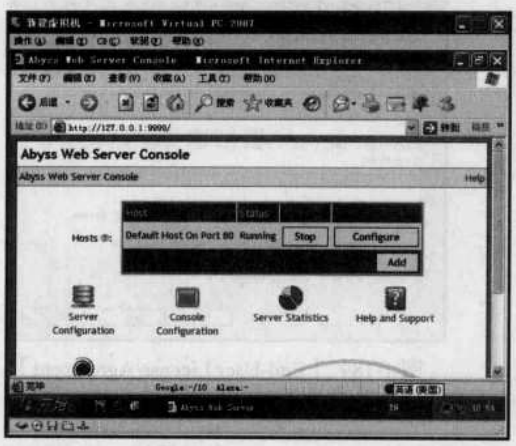


图 1-183 “Abyss Web Server Console”窗口

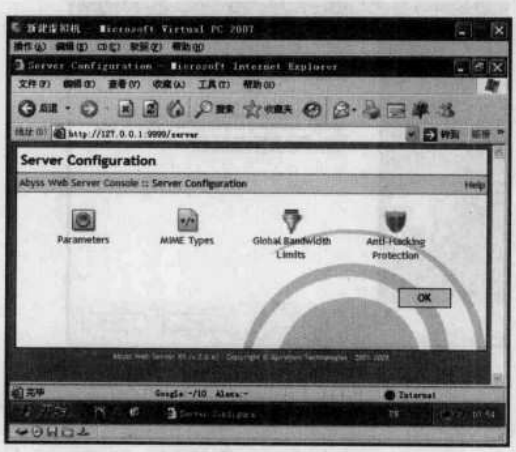


图 1-184 “Server Configuration”窗口

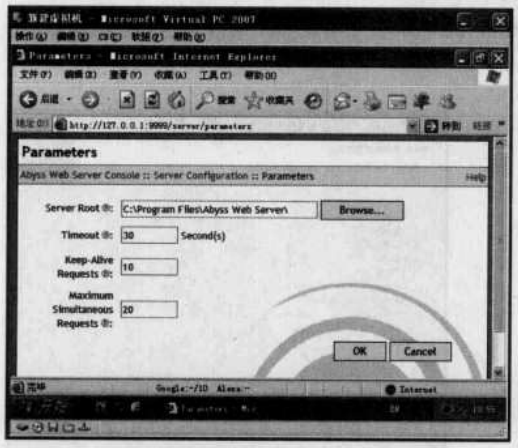


图 1-185 “Parameters”窗口

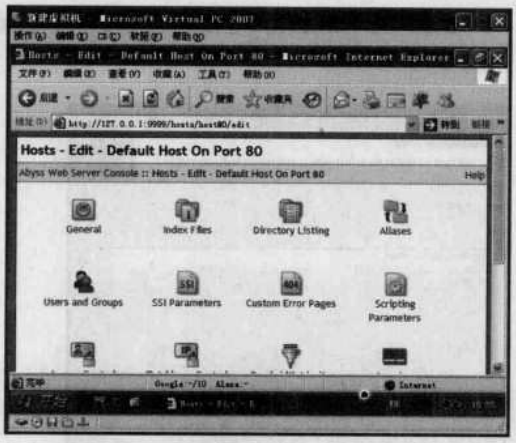


图 1-186 “Hosts-Edit-Default Host On Port 80”窗口

为使所架设的网站支持 CGI（Common Gateway Interface，公共网关接口）程序，可从网络下载 PHP 5.3.0 RC2 for Windows 程序，将其安装到 Windows 系统中。PHP 是一种 CGI 程序编写语言，内置了对文件上传、密码认证、Cookies 操作、邮件收发、动态 GIF 生成等功能，可为很多数据库提供连接，包括 Oracle、Sybase、Postgres、MySQL、Informix、Dbase、Solid、Access 等，完全支持 ODBC（Open Database Connectivity）接口，用户更换平台时无需变换 PHP 代码，可即拿即用。

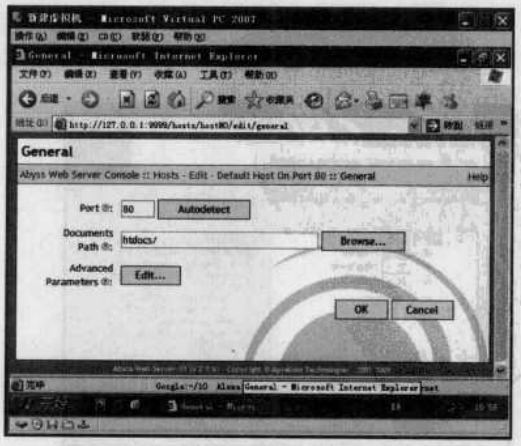


图 1-187 “General”窗口

具体的操作步骤如下。

步骤 1：双击“PHP 5.3.0 RC2 for Windows”应用程序图标，即可进入“PHP 5.3.0 RC2 for Windows 安装向导”主界面，如图 1-188 所示。

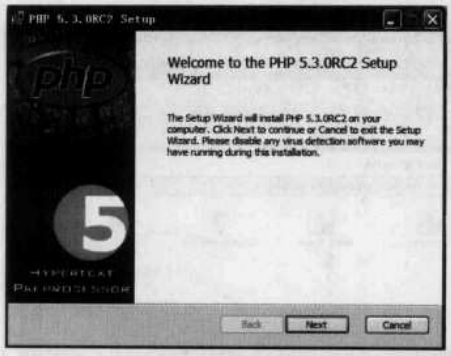


图 1-188 “PHP 5.3.0 RC2 for Windows 安装向导”主界面

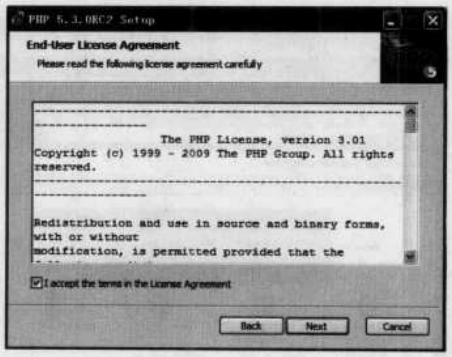


图 1-189 【End-User License Agreement】对话框

步骤 2：单击【Next】按钮，即可打开【End-User License Agreement】对话框，在其中阅读许可协议并勾选“I accept the terms in the License Agreement”复选框，如图 1-189 所示。

步骤 3：单击【Next】按钮，即可打开【Destination Folder】对话框，在其中指定安装路径，如图 1-190 所示。

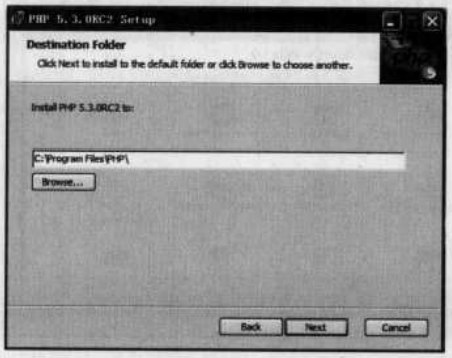


图 1-190 【Destination Folder】对话框

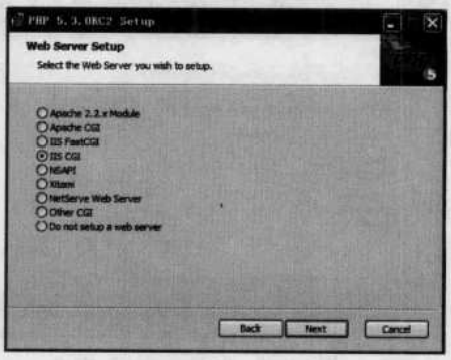


图 1-191 【Web Server Setup】对话框

步骤 4：单击【Next】按钮，即可打开【Web Server Setup】对话框，在其中指定需要支持的服务器类型，如图 1-191 所示。单击【Next】按钮，即可打开【Choose Item to Install】对话框，在其中设置安装的组件，如图 1-192 所示。

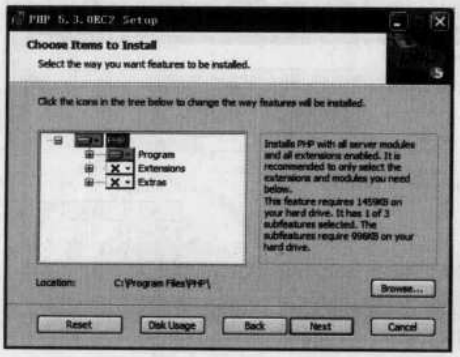


图 1-192 【Choose Item to Install】对话框

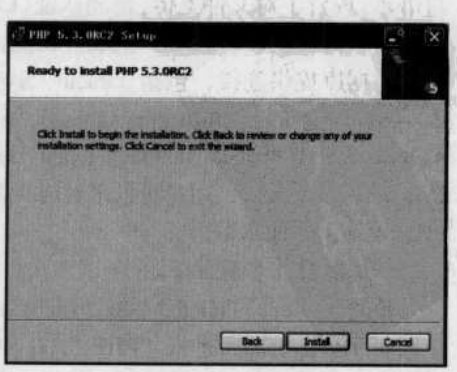


图 1-193 【Ready to install PHP 5.3.0RC2】对话框

步骤 5：单击【Next】按钮，即可打开【Ready to install PHP 5.3.0RC2】对话框，如图 1-193 所示。单击【Install】按钮，即可打开【Installing PHP 5.3.0RC2】对话框，程序开始安装并显示安装进度条，如图 1-194 所示。

步骤 6：在程序安装完毕后，单击【Next】按钮，即可打开【Completed the PHP 5.3.0RC2】对话框。单击【Finish】按钮，即可完成整个安装过程，如图 1-195 所示。

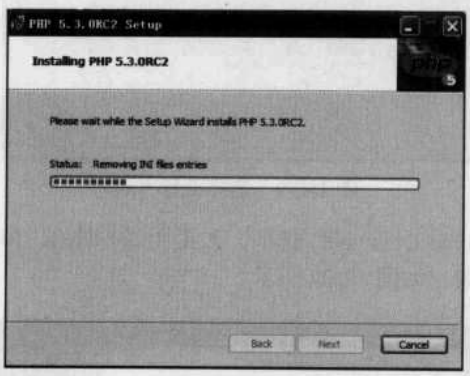


图 1-194 【Installing PHP 5.3.0RC2】对话框

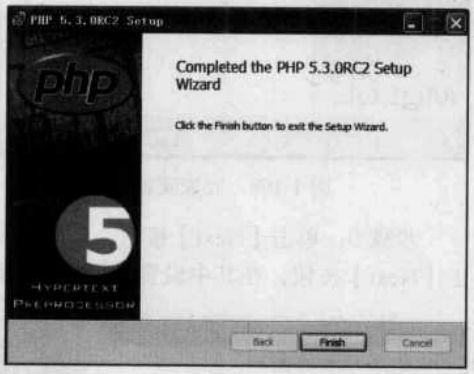


图 1-195 【Completed the PHP 5.3.0RC2】对话框

大部分动态网站都需要 SQL 数据支持，这里使用 MySQL For Windows V6.0 Alpha 代替庞大的 MS SQL 数据。MySQL For Windows V6.0 Alpha 是一个多线程结构化查询语言（SQL）数据库服务器。具体的操作步骤如下。

步骤 1：双击 MySQL For Windows V6.0 Alpha 安装程序，即可进入“欢迎安装 MySQL 6.0 向导”界面，如图 1-196 所示。

步骤 2：单击【Next】按钮，即可打开【Setup Type】对话框，在其中选择一种安装的类型，这里选择“典型安装”类型，如图 1-197 所示。

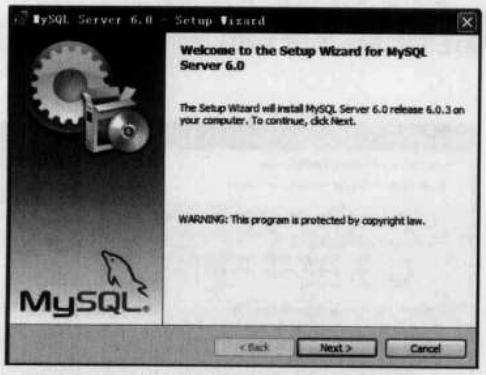


图 1-196 “欢迎安装 MySQL 6.0 向导”界面

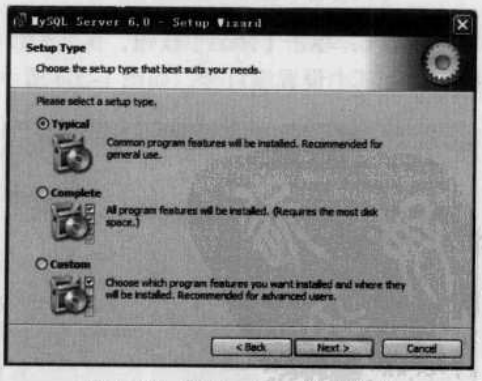


图 1-197 【Setup Type】对话框

步骤 3：单击【Next】按钮，按照向导提示即可完成安装。在完成安装后勾选“Configure the MySQL Server now”复选框，如图 1-198 所示。

步骤 4：单击【Finish】按钮，即可打开设置向导。单击【Next】按钮，用户可以选择设置方式，如图 1-199 所示。在其中选择“Detailed Configuration（简单设置）”模式，单击【Next】按钮，选取“Server Machine”选项，如图 1-200 所示。

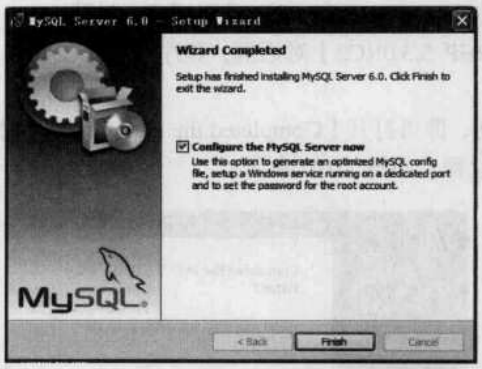


图 1-198　完成安装

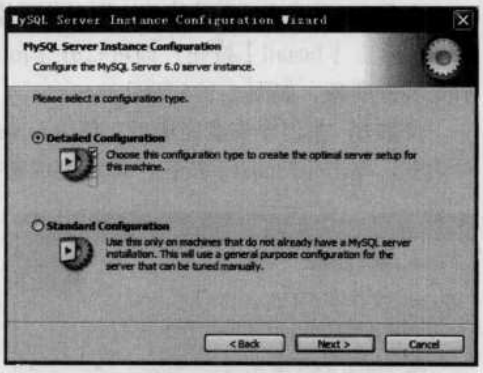


图 1-199　选择设置方式

步骤 5：单击【Next】按钮，选取“Multifunctional Database”选项，如图 1-201 所示。单击【Next】按钮，在其中设置数据库文件保存的位置，如图 1-202 所示。

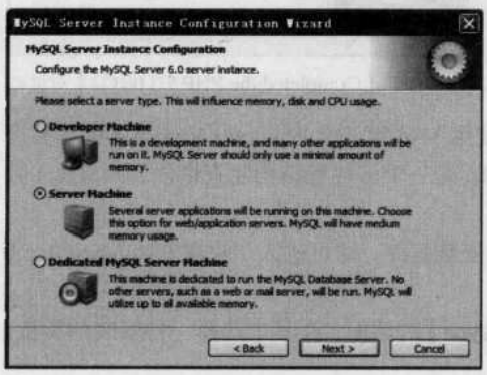


图 1-200　选择一种服务类型

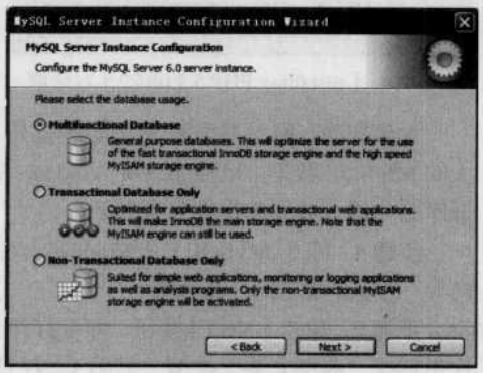


图 1-201　选择数据库用途

步骤 6：单击【Next】按钮，在其中设置服务器连接数量，如图 1-203 所示。单击【Next】按钮，在其中设置端口号，如图 1-204 所示。

图 1-202　设置数据库文件保存的位置

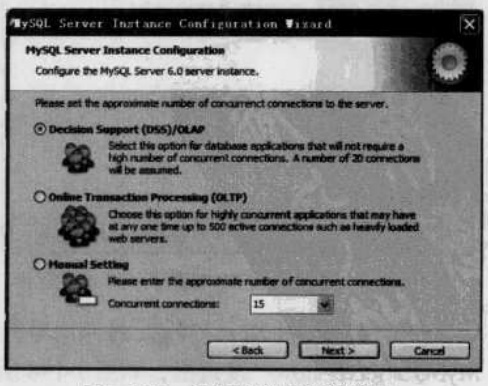


图 1-203　设置服务器连接数量

步骤 7：单击【Next】按钮，在其中设置默认字符，如图 1-205 所示。单击【Next】按钮，在其中设置 MySQL 服务名称及自动加载运行选项，如图 1-206 所示。

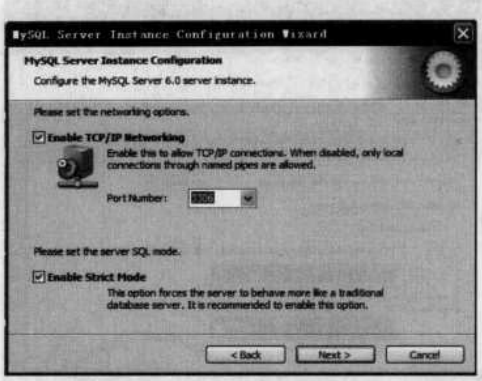


图 1-204 设置端口号

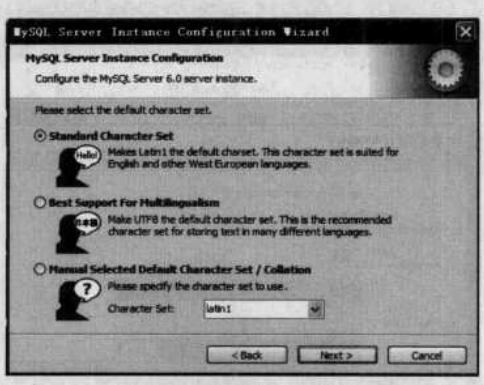


图 1-205 设置默认字符

步骤 8：单击【Next】按钮，在其中设置系统管理员密码，如图 1-207 所示。单击【Next】按钮，再单击【Execute】按钮，即可完成设置，如图 1-208 所示。

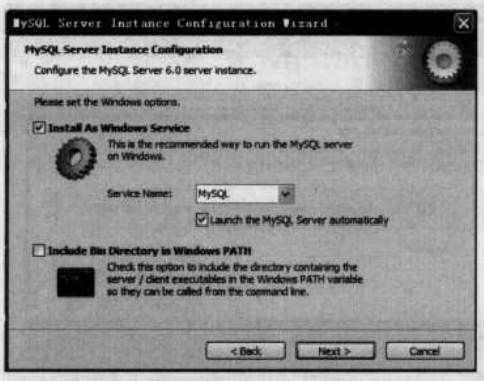


图 1-206 设置 MySQL 服务名称及自动加载运行选项

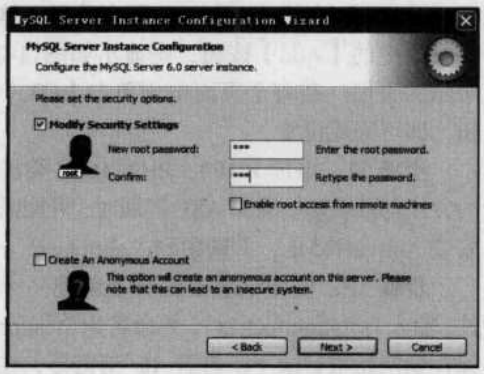


图 1-207 设置系统管理员密码

步骤 9：单击【Finish】按钮，再重新打开 Abyss Web Server 的服务器管理页面，单击【Configure】按钮进入高级设置页面，如图 1-209 所示。单击【Scripting Parameters】按钮，勾选“Enable Scripts Execution”复选框并单击“Interpreters”项中的【Add】按钮，即可打开 PHP 文件添加页面，如图 1-210 所示。

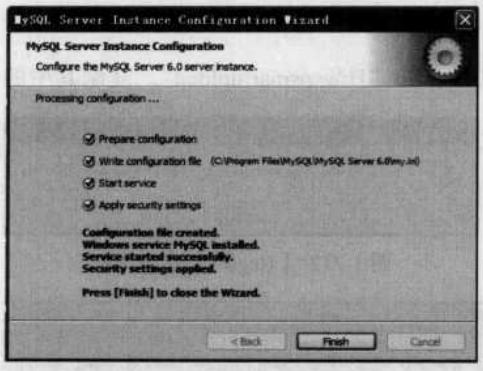


图 1-208 成功完成设置

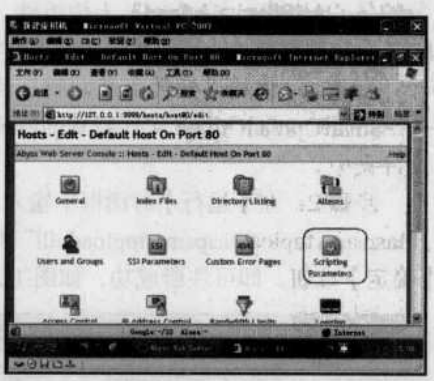


图 1-209 高级设置页面

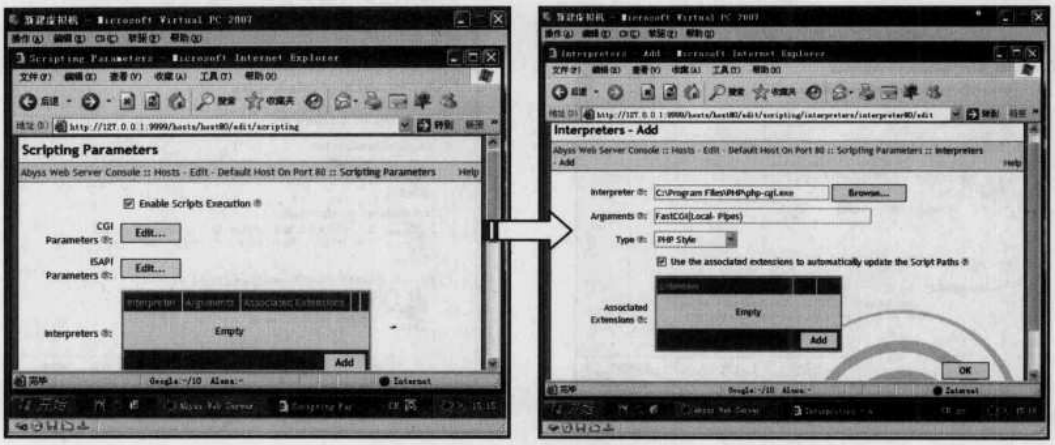


图 1-210　PHP 文件添加页面

步骤 10：设置“Interface”为“FastCGI(Local- Pipes)”，设置“Type”为“PHP Style”，在“Interpreter”输入 php-cgi.exe 所在路径。单击该页面中的【Add】按钮，则显示如图 1-211 所示的页面。在每个页面中均单击【OK】按钮，即可完成设置。

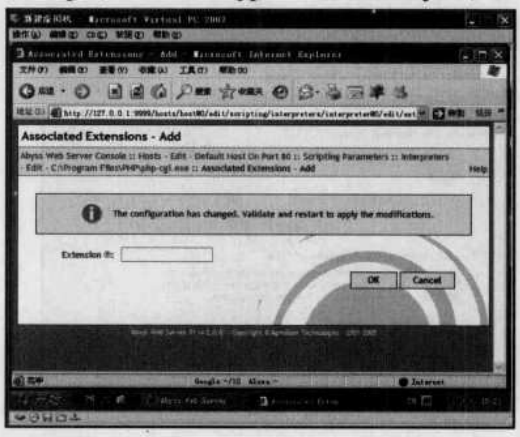


图 1-211　【Associated Extensions-Add】对话框

步骤 11：添加 PHP3、PHTML 之类扩展的方法与此类似。添加 ASP 扩展时，可能需要安装 ActiveHTML，并映射到“ahtml.exe”。

步骤 12：使用记事本编辑器新建一个文件，输入“<?phpinfo();?>”，并命名为“test.php”保存到网站根目录下。打开 IE 浏览器，在地址栏中输入 http://localhost/test.php，若能正常显示网页，则表示 PHP 安装成功。

4．安装网站插件

网站程序的安装一般来说都是大同小异，但对于某些网站还需要一些特殊组件的支持，需要在现有的网站程序中安装此类插件，其中最常见的是上传组件。上传组件很多，这里选择安装的是“ASPSmartUpload”上传组件。

上传组件 ASPSmartUpload 的安装方法如下。

步骤 1：将网站插件下载并解压到某个文件夹中，如“H:\aspsmartupload”，复制其中的 ASPSmartUploadUtil.dll 文件到 Windows\system32 文件夹中。

步骤 2：在【运行】对话框中输入“regsvr32 H:\aspsmartupload\aspsmartupload.dll”命令，单击【确定】按钮，即可注册成功，如图 1-212 所示。

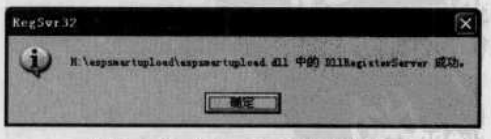


图 1-212　【RegSvr32】对话框

提示　网站可能还需再安装一些插件，如“Scripting.FileSystem Object（FSO 文本文件读写组件）”等，才能正常执行所有的功能，同时为网站增加更多的功能，如动网论坛中的游戏系统。其安装方法都差不多，可参照此操作。

第 8 招 踩点与侦察范围

黑客在攻击其他计算机之前，先要对攻击目标进行扫描，查找出计算机系统的弱点与漏洞，从而根据相应的弱点与漏洞采取适当的攻击方法与策略。踩点与侦察的目的就是为攻击确定目标，为下一步真正的攻击做好准备。

1．实施踩点的具体流程

黑客在进行攻击之前要先探测到对方计算机的存在，使用软件探测出计算机安全等情况，再在使用 Tracert 命令侦察对方的网络情况。实施踩点的具体流程如下。

（1）探测到对方存在

确定对方主机存在最简单的方法就是使用 ping 命令，如在命令提示符窗口中输入“ping 192.168.0.12”，如图 1-213 所示。从运行结果来看，如果 ping 通了，就会从该 IP 地址返回 byte、time 和 TTL 的值，表示这台计算机一定在网络中，这样黑客就具备入侵的目标了。其中 time 时间越短，则表示响应的时间就越快。如果 ping 不通，则会返回“Request time out”提示，表示对方的计算机不在网络上或对方计算机存在，或设置了 ICMP 数据包过滤，如图 1-214 所示。

图 1-213 用 ping 命令显示目标主机的 IP 地址

图 1-214 ping 不通 IP 地址

另外，还可以使用 SuperScan 扫描软件，可以快速检测出目标主机是否存在以及其开放的端口和操作系统类型等。如图 1-215 所示即为 SuperScan 主窗口。在“扫描”选项卡的“IP 地址”栏目中输入起始 IP 和结束 IP，单击【扫描】按钮 ▶，即可进行扫描。

在扫描完毕之后，单击【查看 HTML 报告】按钮，即可打开 HTML 格式的扫描报告，从中可以看到被扫描到的主机详细信息，如图 1-216 所示。

图 1-215 【SuperScan】主窗口

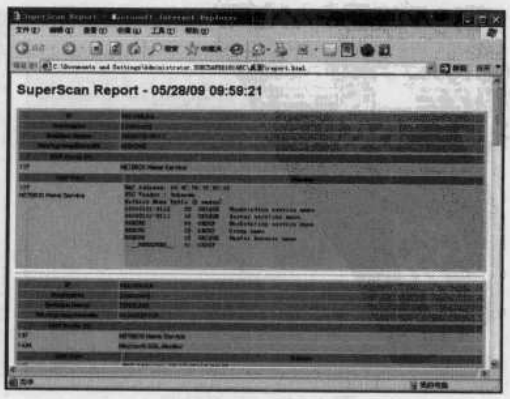


图 1-216 SuperScan 扫描结果

（2）查询对方安全情况

在黑客已经确定目标主机的 IP 地址是否存在以及操作系统之后，还需要继续查看目标主机的安全状态，从而确定哪些漏洞可以利用。GFI LANGuard Network Security Scanner（N.S.S）是一个网络安全扫描器，拥有网络安全扫描和补丁管理解决方案，保护用户的网络免遭攻击。

使用 GFI LANGuard N.S.S 查看计算机安全情况的具体操作步骤如下。

步骤 1：下载安装 GFI LANGuard N.S.S 之后，即可打开【GFI LANGuard N.S.S】主窗口，在“Scam Target”文本框中输入要扫描的 IP 地址，在“Profile”文本框中选择“FullScan”选项，如图 1-217 所示。

步骤 2：单击【Scan】按钮，即可开始进行扫描，等待扫描结束后将会出现【Scan completed successfully!】提示框，如图 1-218 所示。

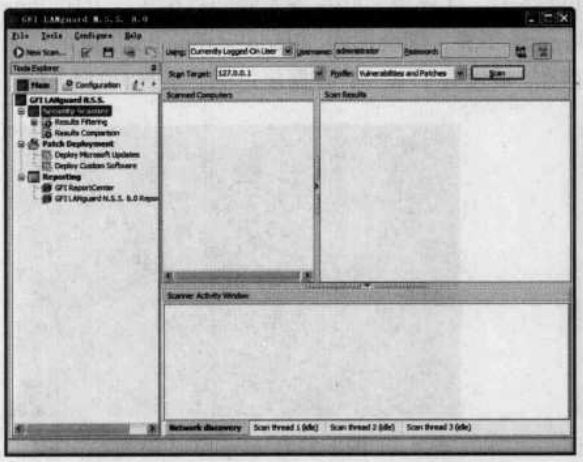


图 1-217 【GFI LANGuard N.S.S】主窗口

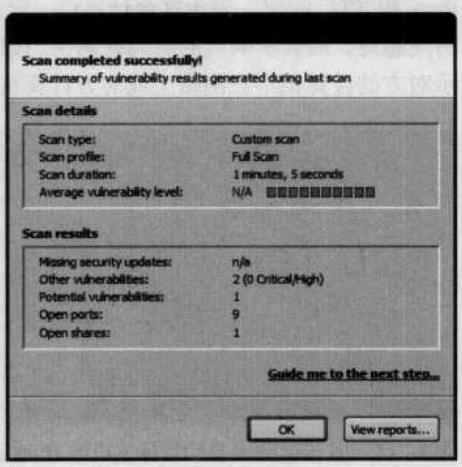


图 1-218 【Scan completed successfully】提示框

步骤 3：单击【OK】按钮，即可看到扫描结果，其中包括目标主机的基本信息，开放的端口以及开启的服务等信息，如图 1-219 所示。

步骤 4：如果想查看扫描出的信息，则单击扫描结果中相应的选项，如选择“Open TCP Ports”选项，即可看到扫描的 TCP 端口，如图 1-220 所示。

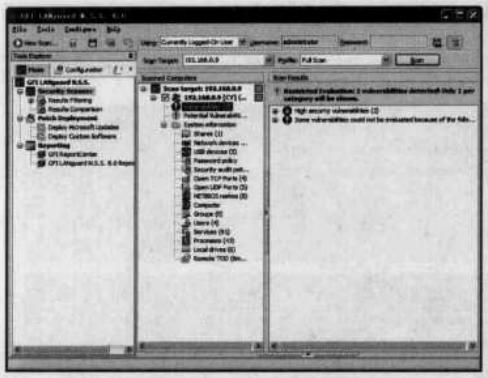


图 1-219 扫描结果

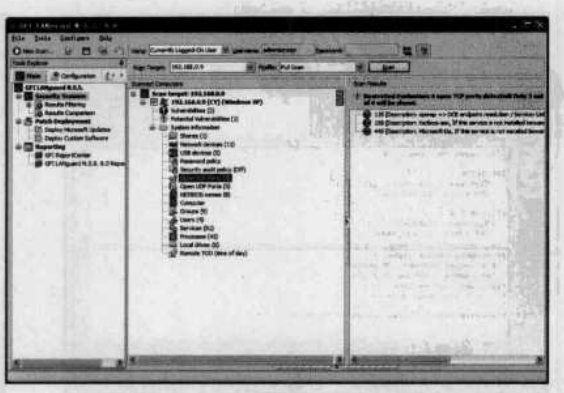


图 1-220 查看开放的 TCP 端口

（3）查询 WHOIS

WHOIS 是一个用来查询已被注册域名详细信息的数据库（如域名所有人、域名注册商、域名注册日期和过期日期等）。通过 WHOIS 来实现对域名注册信息查询（WHOIS Database）。

黑客可以通过如下几种方法来查看域名注册信息。

1）中国互联网信息中心网页上查询。中国互联网信息中心是非常权威的机构，其中记录着所有以.cn 为结尾的域名注册信息，其查询页面如图 1-221 所示。在其中的“查询”文本框中输入要查询的中文域名，并选择“中文域名”单选按钮之后，单击【查看】按钮，即可打开【输入验证码】窗口，如图 1-222 所示。

图 1-221 中国互联网信息中心的查询页面

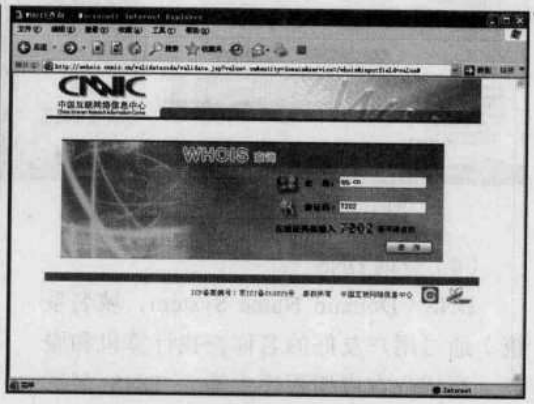


图 1-222 输入验证码窗口

在输入验证码后单击【查看】按钮，即可看到要查询域名的详细信息，如图 1-223 所示。

2）中国万网。中国万网是中国最大的域名和网站托管服务提供商，它提供.cn 的域名注册信息，而且还可以查询.com 等域名信息，如图 1-224 所示即为中国万网首页。在“域名”文本框中输入要查询的域名后，单击【查询】按钮，即可看到相关域名信息，如图 1-225 所示。

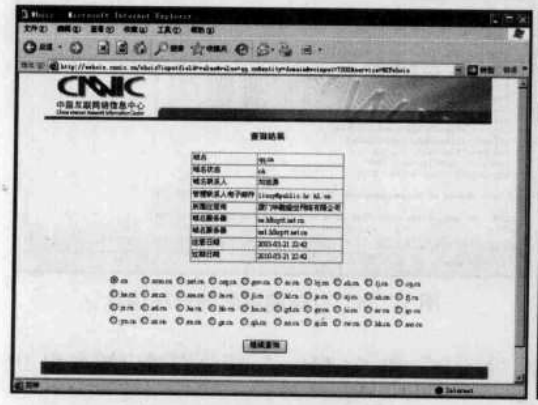


图 1-223 查看域名的信息

图 1-224 中国万网首页

3）利用 NetAlyzer 软件进行查询。NetAlyzer 软件用于收集网络信息、跟踪路由、收集和管理 WHOIS 查询的工具。在安装 NetAlyzer 软件之后，即可打开【NetAlyzer】主窗口，如图

1-226 所示。单击查询域名按钮【Query domain…】，即可打开【Whois】对话框，如图 1-227 所示。在“Please enter domain name”文本框中输入要查询的域名，单击【OK】按钮，即可看到扫描结果，从扫描结果中可查看域名的详细信息，如图 1-228 所示。

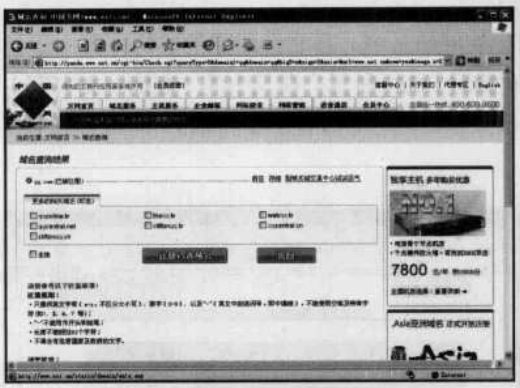


图 1-225　查询的域名信息

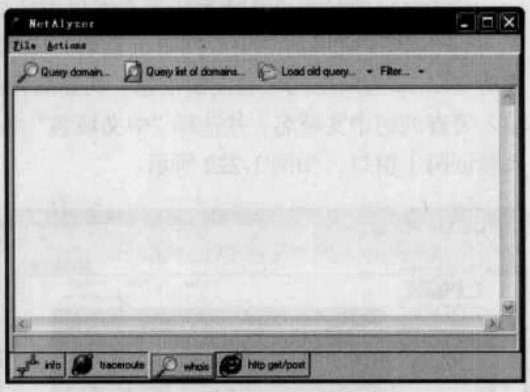


图 1-226 【NetAlyzer】主窗口

（4）查询 DNS

DNS（Domain Name System，域名系统）通过用户友好的名称查找计算机和服务。当用户在应用程序中输入 DNS 名称时，DNS 服务可将此名称解析为与之相关的其他信息，如 IP 地址。因为，在上网时输入的网址，通过域名解析系统解析找到相对应的 IP 地址才能上网。其实，域名的最终指向是 IP。可以使用 Windows 系统自带的 nslookup 工具查询 DNS 中的各种数据，下面介绍两种使用 nslookup 查看 DNS 的方法。

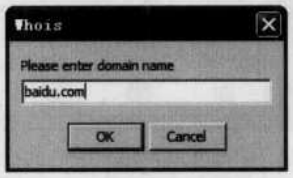


图 1-227 【Whois】对话框

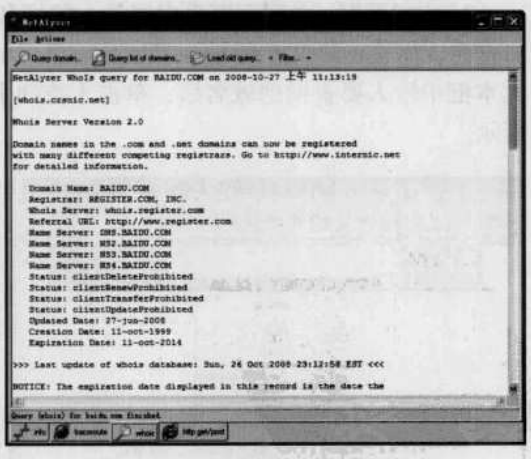


图 1-228　要查询域名的详细信息

1）使用命令行方式。主要用来查询域名对方的 IP 地址，也即查询 DNS 的记录，通过该记录黑客可以查询该域名的主机所存放的服务器。

其命令格式为：nslookup 域名，如要查看 www.baidu.com 对应的 IP 信息，可在【命令提示符】窗口中输入“nslookup www.baidu.com”命令，如图 1-229 所示。在其中可以看到“Name”和“Address”行分别对应域名和 IP 地址，而最后一行显示的是目标域名和注明别名。

2）交互式方式。可以使用 nslookup 的交互模式对域名进行查询，具体的操作步骤如下。

步骤 1：在【命令提示符】窗口中，输入“nslookup”命令，即可查询域名信息，其显示结果如图 1-230 所示。

图 1-229 使用 nslookup 命令行方式查询 DNS

图 1-230 输入“nslookup”命令

步骤 2：再运行“set type=mx”命令，其运行结果如图 1-231 所示。

步骤 3：再在其中输入要查看的网址（去掉 www），如“baidu.com”命令，即可看到百度网站的相关信息，如图 1-232 所示。

图 1-231 输入“set type”命令

图 1-232 查询 DNS 的 MX 关联记录

（5）网络侦察

要想对目标主机实施攻击，还需要了解目标主机的网络机构，只有弄清楚目标网络中防火墙、服务器地址之后，才可进行第一步入侵。可以使用 tracert 命令查看目标主机的网络结构。tracert 命令用来显示数据包到达目标主机所经过的路径并显示到达每个结点的时间。

tracert 命令功能同 ping 类似，但所获得的信息要比 ping 命令详细得多，它把数据包所走的全部路径、结点的 IP 以及花费的时间都显示出来。该命令比较适合于大型网络。

tracert 命令的格式：tracert IP 地址或主机名。要想了解自己计算机与目标主机 www.baidu.com 之间的详细路径传递信息，就可以在“命令提示符”窗口中输入“tracert www.baidu.com”命令进行查看，如图 1-233 所示。

图 1-233 使用 tracert 命令查看网络结构

2. 网络侦察与快速确定漏洞范围

为尽快确定目标主机漏洞的大致范围，黑客往往采用综合扫描器对某个 IP 段中的主机进行扫描，还可快速确定漏洞的大体范围，包括端口扫描、弱口令扫描、系统漏洞扫描以及

主机服务器扫描等。X-Scan 采用多线程方式对指定 IP 地址段（或单机）进行安全漏洞检测，支持插件功能，提供了图形界面和命令行两种操作方式。X-Scan 的扫描结果保存在/log/目录中，index_*.htm 为扫描结果索引文件。使用 X-Scan 扫描漏洞的具体操作步骤如下。

步骤 1：双击 X-Scan_gui 主应用程序，即可打开并运行 X-Scan 主窗口，在其中可以浏览此软件的功能简介和常见问题解答等信息，如图 1-234 所示。

步骤 2：单击工具栏上的“扫描参数”按钮，即可打开【扫描参数】对话框。

步骤 3：选择扫描模块。展开“全局设置”选项之后，选取其中的“扫描模块”选项，则可选择扫描过程中需要扫描的模块。在选择扫描模块时，还可在其右侧窗格中查看该模块的相关说明，如图 1-235 所示。

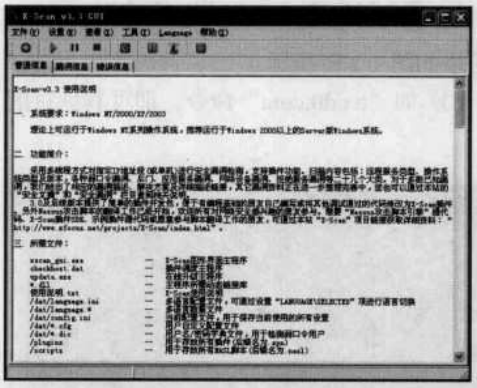


图 1-234 【X-Scan】主窗口

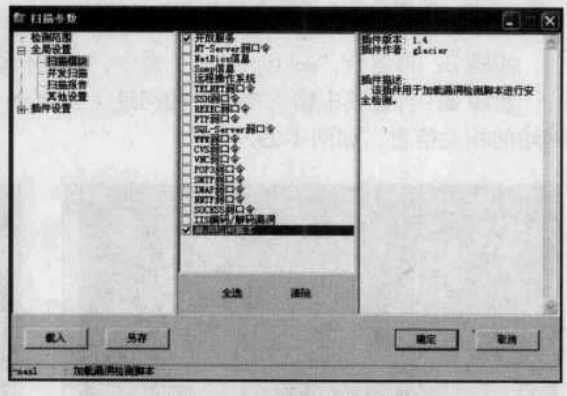


图 1-235 选择扫描模块

步骤 4：选择“检测范围”选项，即可设置扫描 IP 地址的范围。在“指定 IP 范围”文本框中可输入需要扫描的 IP 地址或 IP 地址段，如图 1-236 所示。

步骤 5：字典文件设置的好坏，将直接影响扫描结果，可以在“插件设置”选项中设置字典文件，也可以重新加载自己制作的字典文件，以实现获得更多弱口令，如图 1-237 所示。

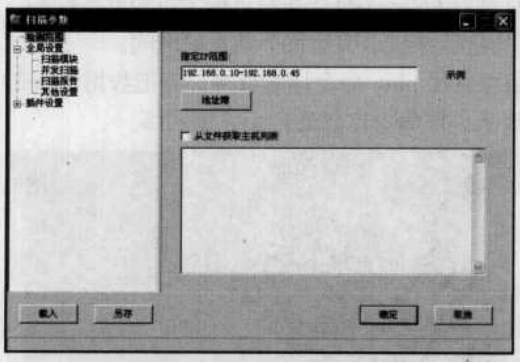


图 1-236 确定扫描范围

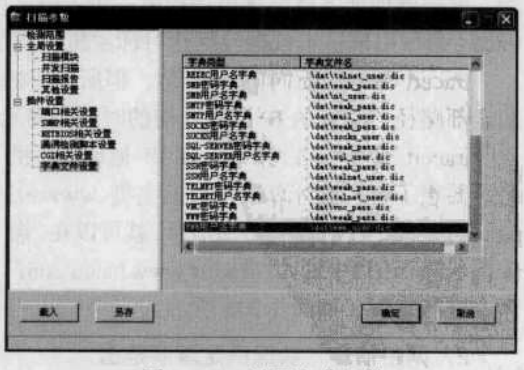


图 1-237 设置字典文件

步骤 6：在【X-Scan】主窗口中单击【扫描】按钮，即可根据自己的设置进行扫描，如图 1-238 所示。在扫描完毕之后，将会显示出相应的扫描报告信息，通过扫描报告可以看出目标主机存在哪些漏洞，如图 1-239 所示。

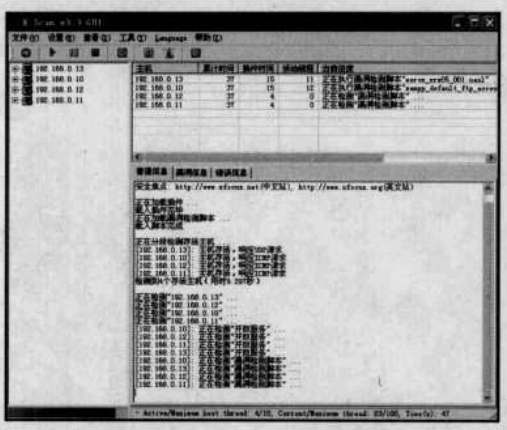


图 1-238 用 X-Scan 进行扫描

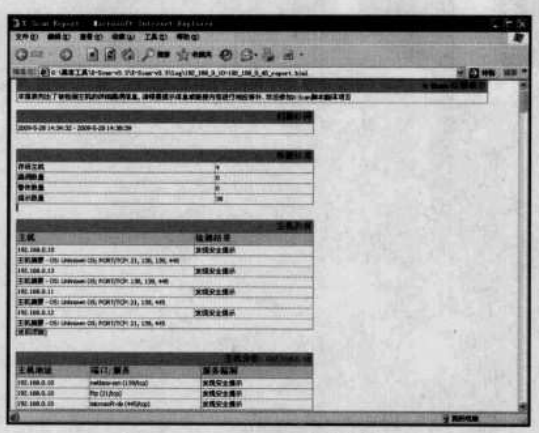


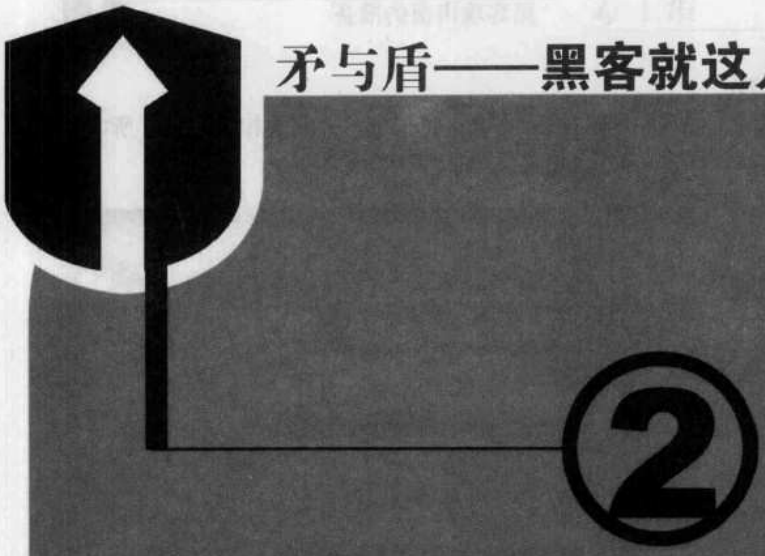
图 1-239 X-Scan 扫描报告

3. 防御网络侦察与堵塞漏洞

由于黑客在攻击一台计算机之前，必须先对该计算机进行扫描，并收集相关信息，所以，用户只要能够阻断黑客对自己计算机的扫描，就能有效地防止黑客的攻击。

如何才能防止黑客的扫描呢？一般来说需要注意以下事项：

- 安装防病毒软件及防火墙，并经常及时升级病毒库，防止有破坏性程序的注入。
- 在网上购物时，不要因为任何原因而允许自己的信用卡资料被商家储存。
- 密码设定最好不要使用自己名字的拼音或生日数字的组合，最好使用无意义的数字和字母组合，并且位数尽量多一些，而且还要经常更换，防止黑客破解。
- 只向有安全保证的网站发送信用卡号码，留意寻找浏览器底部显示的挂锁图标或钥匙形图标。
- 对不同的网站和程序要使用不同的密码，防止黑客的破译。
- 在使用 QQ、MSN 这些聊天工具时，不要轻易同意让陌生人把自己加为好友。
- 使用最新版本的浏览器软件、电子邮件软件以及其他程序。
- 使用可对 Cookie 进行控制的安全程序，因为 Cookie 有时会泄漏用户的一些个人隐私。
- 不要轻易打开来历不明的电子邮件或软件，它很可能包含后门程序或其他有害程序。
- 经常查找自己计算机中存在的漏洞，并下载安装这些漏洞补丁，防止黑客利用这些漏洞进行攻击。



第 2 章　扫描与反扫描技术

重点提示

- 扫描器 X-Scan 查本机隐患
- 用流光扫描主机漏洞
- 用 MBSA 检测 Windows 系统
- 深入浅出 RPC 漏洞扫描
- 用 ProtectX 防御扫描器追踪
- 用 NC 监控与扫描

本章精粹：

安全扫描工具是把双刃剑，黑客利用它可以扫描别人的系统，而系统管理员使用它却可以维护系统的安全。本章主要介绍一些扫描工具的使用，以及如何使用这些工具防范黑客的入侵，从而提高系统的安全性。

扫描工具和嗅探工具是黑客使用最多、使用最频繁的工具，只有充分掌握了被攻击主机的相关信息，下一步操作才能得心应手。当然，合理使用扫描和嗅探工具，也可以把系统配置得“滴水不漏”。

第 9 招　确定扫描目标

通过踩点与侦察，可以锁定一些大致的目标范围，要想具体到某台远程主机，还需要经过一番操作才能确定扫描目标。

1. 确定目标主机 IP 地址

只有设置好网关的 IP 地址，TCP/IP 协议才能实现不同网络之间的相互通信。网关 IP 地址是具有路由功能的设备的 IP 地址，具有路由功能的设备有路由器、启用了路由协议的服务器（实质上相当于一台路由器）、代理服务器（也相当于一台路由器）。

只要计算机连接到互联网上，就会有一个 IP 地址，查询本机 IP 地址的方法如下。

步骤 1：在“命令提示符”窗口中运行“ipconfig”命令，在运行结果中可以看到本机 IP 地址、网关地址等信息，如图 2-1 所示。在“命令提示符”窗口中运行“netstat –n”命令，即可查看本机的 IP 地址，如图 2-2 所示。

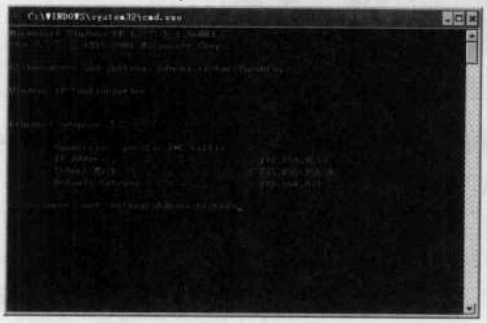


图 2-1　使用“ipconfig”命令查看本机 IP 地址

图 2-2　使用“netstat –n”命令查看本机 IP 地址

步骤 2：如果想攻击某个网站，也需要先获得该网站的 IP 地址，获取网站 IP 地址可使用 ping 命令。在“命令提示符”窗口中运行“ping www.baidu.com”命令，即可查看百度网站对应的 IP 地址，如图 2-3 所示。

步骤 3：要想得到网站的详细信息，在【命令提示符】窗口中运行“nslookup www.qq.com”命令，即可查看新浪网详细信息，其中第 1 个 Address 中 IP 地址就是本机所在域的 DNS 服务器，第 2 个 Addresses 是 www.qq.com 所使用的 Web 服务器群的 IP 地址，如图 2-4 所示。

图 2-3　使用 ping 命令查看网站的 IP 地址信息

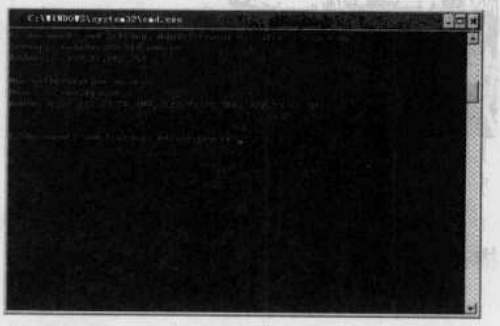


图 2-4　使用 nslookup 命令查看网站的详细信息

2．确定可能开放的端口和服务

在默认情况下，有很多不安全或没有作用的端口是开启的，如 Telnet 服务的 23 端口、FTP 服务的 21 端口、SMTP 服务的 25 端口等。攻击者可以使用扫描工具对目标主机进行扫描，可以获得目标计算机打开的端口情况，还可了解目标计算机提供了哪些服务。

在“命令提示符”窗口中输入“netstat -a -n”命令，即可查看本机开启的端口，在运行结果中可以看到以数字形式显示的 TCP 和 UDP 连接的端口号及其状态，如图 2-5 所示。

图 2-5　查看本机查看的端口

Nmap 是一款非常流行的端口扫描软件，下面以 For Windows 版本为例讲述 Nmap 是如何扫描端口的。利用 Nmap 扫描器对端口进行扫描的具体步骤如下。

步骤 1：将网上下载的“nmap-4.52-win32.rar”解压缩后，可得到“nmap-4.53”文件夹，为了便于操作先将其放到 C 盘的根目录下，如图 2-6 所示。

步骤 2：在“MS-DOS 命令符”窗口中输入“cd C:\setup\nmap-4.53”命令，即可打开 Nmap 的安装目录，如图 2-7 所示。

图 2-6 【nmap-4.53】文件夹

图 2-7　打开 Nmap 安装目录

Nmap 是基于命令格式的扫描软件，可使用 Nmap 命令进行端口扫描。Nmap 对端口的扫描有三种方式。

1）TCP connect()端口扫描。即全连接扫描，使用了“-sT”参数，只需在命令提示符下键入“Nmap –sT 192.168.0.88”命令，即可看到 TCP 全连接扫描的端口，如图 2-8 所示。

2）TCP 同步端口扫描。该方式为半连接扫描，也叫隐蔽扫描。采用了“-sS”参数，在命令提示符下键入“Nmap –sS 192.168.0.88”命令，即可看到 TCP 半连接扫描的端口，如图 2-9 所示。

3）UDP 端口扫描。该方式主要采用“-sU”参数，在命令提示符下键入“Nmap –sU 192.168.0.88”命令，即可看到扫描的 UDP 端口，如图 2-10 所示。

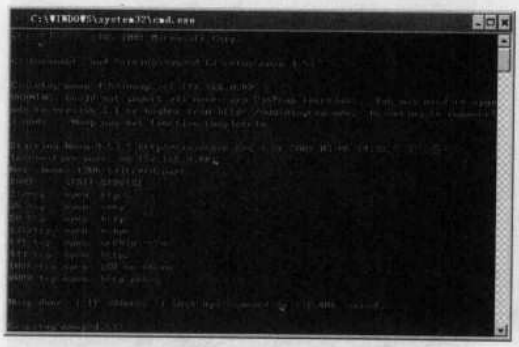


图 2-8 TCPconnect()端口扫描结果

图 2-9 TCP 同步端口扫描结果

Nmap 还支持丰富、灵活的命令参数，比如要扫描一个 IP 地址段的 UDP 端口，还可以在命令提示符下键入“Nmap –sU 192.168.0.1-255”命令，如图 2-11 所示。

图 2-10 UDP 端口扫描结果

图 2-11 IP 地址段扫描结果

3. 常见端口扫描工具

入侵者常常利用一些专门的扫描工具对目标主机的端口进行扫描，目前可以用来扫描端口的扫描工具很多，下面就介绍 3 种常见的扫描工具。

（1）FreePortScanner

FreePortScanner 是一款端口扫描工具，用户可以快速扫描全部端口，也可以制定扫描范围。使用 FreePortScanner 进行端口扫描的具体操作步骤如下。

步骤 1：下载 FreePortScanner 并打开其窗口，在“IP”文本框中输入目标主机的 IP 地址，再勾选“Show Closed Ports”复选框，如图 2-12 所示。

步骤 2：单击【Scan】按钮，即可扫描到目标主机的全部端口，其中绿色标记是开放的端口，如图 2-13 所示。

步骤 3：使用 FreePortScanner 可以只对目标主机开启的端口进行扫描，在“IP”文本框中输入要扫描的“IP”地址之后，再取消勾选“Show Closed Ports”复选框。

图 2-12 【FreePortScanner】主窗口

图 2-13 扫描目标主机所有的端口

步骤 4：单击【Scan】按钮，在扫描完毕之后，即可显示出扫描结果，从扫描结果中可以看到目标主机开启的端口，如图 2-14 所示。

（2）ScanPort

ScanPort 软件不但可以用于网络扫描，同时还可以探测指定 IP 及端口，速度比传统软件快，且支持用户自设 IP 端口又增加了其灵活性。具体的使用方法如下。

步骤 1：运行 ScanPort 主程序，即可打开“ScanPort”主窗口，在其中设置起始 IP 地址、结束 IP 地址以及要扫描的端口号，如图 2-15 所示。

步骤 2：单击【扫描】按钮，即可进行扫描，从扫描结果中可以看出IP地址段中计算机开启的端口，如图 2-16 所示。

图 2-14 只扫描开启的端口

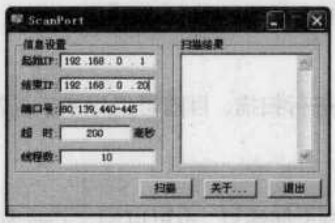


图 2-15 【ScanPort】端口

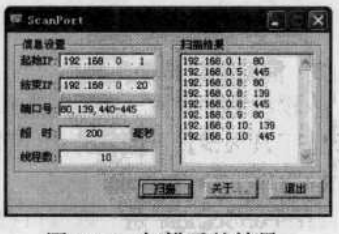


图 2-16 扫描后的结果

（3）S 扫描器

S 扫描器是一款命令行下高速扫描利器，用这工具的好处就在于其扫描速度非常快。究竟如何使用 S 扫描器？下面将一一讲述。

1）命令格式。

- s.exe syn ip1 ip2 端口号 /save。
- s.exe tcp ip1 ip2 端口号 线程数 /save。

2）用法。

- Scanner TCP/SYN StartIP [EndIP] Ports [Threads] [/Banner] [/Save]。

3）参数说明。TCP/SYN -> TCP 方式扫描或 SYN 方式扫描（SYN 扫描需要在 win 2k 或以上系统才行），SYN 扫描对本机无效。

- StartIP：起始扫描的 IP。
- EndIP：结束扫描的 IP，可选项，如果这一项没有，就只是对单个 IP 扫描。
- Ports：可以是单个端口，连续的一段端口或非连续的端口。
- Threads：使用最大线程数去扫描（SYN 扫描不需要加这一项），不能超过 1024 线程。
- /Banner：扫描端口时一并将 Banner 显示出来，这一选项只对 TCP 扫描有效。
- /Save：将结果写入当前目录的 Result.txt 文件中去。

下面举例演示 S 扫描器的几个主要作用。

示例 1：下载并运行 S 扫描器，在命令提示符下键入“S TCP 192.168.0.1 192.168.0.45 80 512”命令，即可实现 TCP 扫描从 192.168.0.1 到 192.168.0.45 这段 IP 中的 80 端口，最大并发线程是 512，如图 2-17 所示。

示例 2：下载并运行 S 扫描器，在命令提示符下键入“S TCP 192.168.0.1 192.168.0.45 21,5631 512 /banner”命令，即可实现 TCP 扫描从 192.168.0.1 到 192.168.0.45 这段 IP 中的 21 和 5631 端口，最大并发线程是 512 并显示 Banner，如图 2-18 所示。

图 2-17　TCP 扫描网段 IP 端口

图 2-18　用 TCP 扫描端口并显示 Banner

示例 3：下载并运行 S 扫描器，在命令提示符下键入“S TCP 192.168.0.1 192.168.0.45 1-200 512”命令，即可实现 TCP 扫描从 192.168.0.1 到 192.168.0.45 这段 IP 中 1 到 200 端口，最大并发线程是 512，如图 2-19 所示。

示例 4：下载并运行 S 扫描器，在命令提示符下键入“S TCP 192.168.0.13 1-200 512”命令，即可实现 TCP 扫描 192.168.0.13 这段 IP 中 1 到 200 端口，最大并发线程是 512，如图 2-20 所示。

图 2-19　用 TCP 扫描 1-200 之间的端口

图 2-20　用 TCP 扫描本机 IP 端口

示例 5：下载并运行 S 扫描器，在命令提示符下键入“S SYN 192.168.0.13 1-65535 /save”命令，即 SYN 扫描 192.168.0.13 段 IP 中的 1～65535 端口，将结果写入 Result.txt 文本文档。扫描结束后 Result.txt 文本文档及所有扫描内容都存放在 S 扫描器所在目录，如图 2-21 所示。

图 2-21　用 SYN 扫描 1-65535 之间的端口

示例 6：下载并运行 S 扫描器，在命令提示符下键入“S SYN 192.168.0.1 192.168.0.20 21 /save”命令，即 SYN 扫描 192.168.0.1 到 192.168.0.20 这 IP 段中的 21 端口，将结果写入 Result.txt 文本文档中。由于这条命令是用来专门找肉鸡的，因此，将会扫描一个 IP 段有没有开 3389 端口或 1433 端口的，如图 2-22 所示。

图 2-22　用 SYN 扫描网段端口

第 10 招　扫描服务与端口

黑客通过端口扫描器可在系统中寻找开放的端口和正在运行的服务，从而知道目标主机操作系统的详细信息。目前网络中大量主机/服务器的口令为空或口令过于简单，黑客只需要利用专用扫描器，即可轻松控制这种弱口令的主机。

1．黑客字典与弱口令扫描工具

所谓黑客字典就是装有各种密码的破解工具，通常情况下，只要知道本地文件的内容，就可以运用黑客字典将其破解。当然，黑客字典文件的好坏，直接关系到黑客是否能够破解到对方的密码，以及破解出密码花费多少时间。

（1）小榕黑客字典

小榕黑客字典是一款功能强大，可根据用户需要任意设定包含字符、字符串的长度等内容

的黑客字典生成器。其具体操作方法如下。

步骤 1：将“小榕黑客字典”软件解压缩后，双击“UltraDict.exe”图标，即可弹出【字典设置】对话框，如图 2-23 所示。

步骤 2：在“设置”标签中可选择生成字符串包含的字母或数字及其范围，在“选项”标签中可根据特殊需要选取相应的选项，如图 2-24 所示。

步骤 3：在“高级选项”标签中可将字母、数字或字符位置进行固定，如图 2-25 所示。

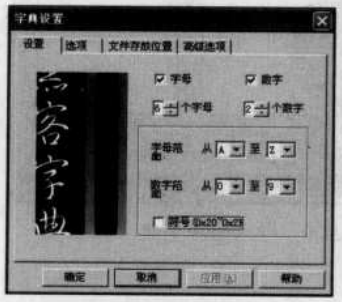


图 2-23 设置字典选项

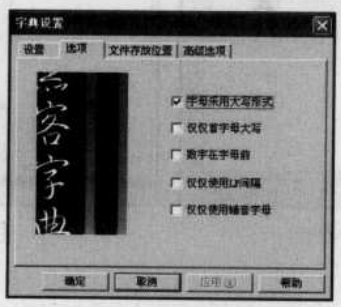


图 2-24 选项设置

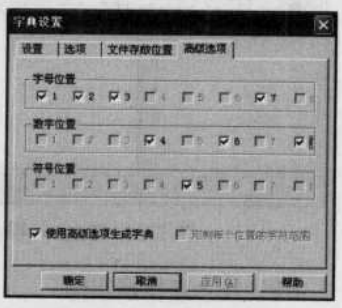


图 2-25 设置高级选项

步骤 4：在“文件存放位置”标签中指定字典文件保存位置之后，单击【确定】按钮，则显示所设置的字典文件属性，如图 2-26 所示。单击【开始】按钮，系统开始生成字典，并显示生成字典的进度，如图 2-27 所示。

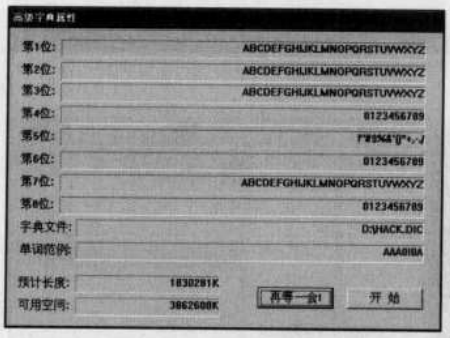


图 2-26 高级字典属性

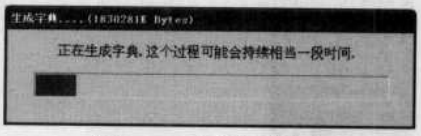


图 2-27 生成字典进度

（2）弱口令扫描器 Tomcat

当字典文件创建好后，就可以使用弱口令扫描器，加载自己编辑的字典文件进行弱口令扫描了。Tomcat 可以根据需要加载用户名称字典、密码字典，对一定 IP 范围内的主机进行弱口令扫描。具体的操作方法如下。

步骤 1：将下载的压缩包解压后双击“Apache Tomcat.exe”图标，即可进入其操作界面，如图 2-28 所示。

步骤 2：单击【设置】按钮，再分别单击“用户名”和“密码”列表框下方的【导入】按钮，即可导入编辑好的黑客字典，如图 2-29 所示。

步骤 3：单击【信息】按钮，在其中输入需要扫描的 IP 地址范围。单击【添加】按钮，即可将其添加地址列表中。单击【开始】按钮，即可开始扫描。若发现活动主机，即可对主机的用户名和密码进行破解。

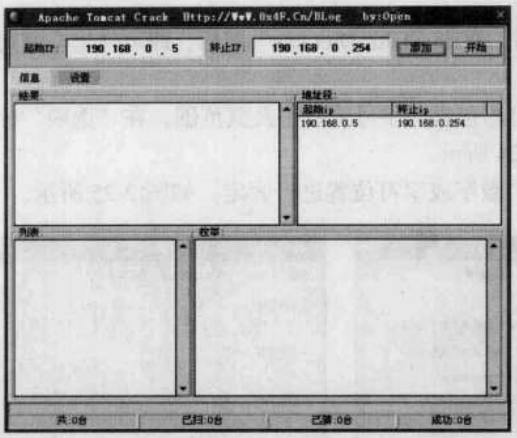


图 2-28 Tomcat 操作界面

图 2-29 导入黑客字典

2. 注入点扫描实例

啊 D 注射工具是一款功能非常强大的注射工具，集旁注检测、SQL 猜解决、密码破解、数据库管理等功能于一身。实现啊 D 注入攻击的一般操作步骤如下。

步骤 1：下载并解压啊 D 注入工具包，即可打开解压后的“啊 D 注入工具文件夹”窗口，如图 2-30 所示。双击“啊 D 注入工具”应用程序图标，即可进入“啊 D 注入工具”主窗口，如图 2-31 所示。

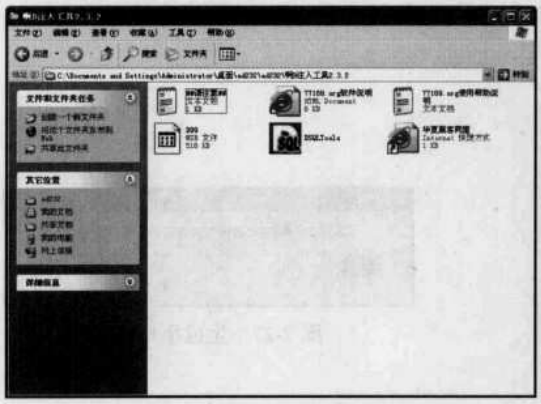


图 2-30 “啊 D 注入工具文件夹”窗口

图 2-31 “啊 D 注入工具”主窗口

步骤 2：在“注入检测”选项栏目中单击【扫描注入点】按钮，即可打开“扫描注入点”页面，在“注入连接”地址栏中输入注入的网站地址。单击 按钮，即可打开该网站并扫描注入点个数，如图 2-32 所示。

步骤 3：若单击“注入连接”右侧的 按钮，在其中对 Cookies 进行修改，如图 2-33 所示。根据需要选中其中的一个注入点，单击“注入检测”选项栏下方的【SQL 注入检测】按钮，即可进入“SQL 注入检测”页面。

步骤 4：单击【检测】按钮等待检测完成后，单击【检测表段】按钮，即可检测出相应表段。再任意选择其中一个表段并单击右边【检测字段】按钮，即可检测出该表对应的字段。选择该表中的所有字段，单击【检测内容】按钮，即可开始检测内容，如图 2-34 所示。

图 2-32 “扫描注入点”页面

图 2-33 对 Cookies 进行修改

步骤 5：稍等一段时间，待内容检测完毕后，在“检测内容”下方的列表框中，即可查看详细的检测内容（包括：用户名、密码、编号等）。显示结果如图 2-35 所示。

图 2-34 “SQL 注入检测”页面

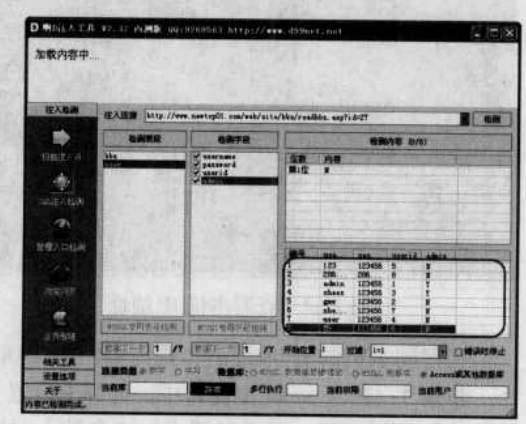


图 2-35 查看详细的检测内容

步骤 6：单击“注入检测”选项栏目下方的【管理入口检测】按钮，即可打开“管理入口检测”页面，在“网站地址”栏目中输入需要管理入口检测的地址，单击【检测管理入口】按钮，等待几秒钟后，即可在下方列表中显示该网站的所有登录入口点，如图 2-36 所示。

图 2-36 “管理入口检测”页面

第 11 招　扫描器 X-scan 查本机隐患

X-Scan 是由安全焦点开发的一个功能强大的扫描工具。它采用多线程方式对指定 IP 地址段（或单机）进行安全漏洞检测，支持插件功能。

1. 用 X-scan 查看本机 IP 地址

利用 X-Scan 扫描器来查看本机的 IP 地址的方法很简单，需要先指定扫描的 IP 范围。由于是本机探测，只需要在“命令提示符”窗口中命令提示符下输入“IPConfig”命令，即可查知本机当前 IP 地址，如图 2-37 所示。

2. 添加 IP 地址

X-Scan 的使用极其简单，解压缩后双击 X-Scan_gui 应用程序，即可打开并运行 X-Scan 主窗口，在其中可浏览此软件的功能简介、常见问题解答等信息，如图 2-38 所示。

图 2-37　查看本机 IP 地址

图 2-38　X-Scan 主窗口

在得到本机的 IP 地址后，则需要将 IP 地址添加到 X-Scan 扫描器中，具体操作步骤如下。

步骤 1：在 X-Scan 主窗口中，选择【设置】→【扫描参数】菜单项或单击工具栏上的“扫描参数”按钮，即可打开【扫描参数】对话框，如图 2-39 所示。

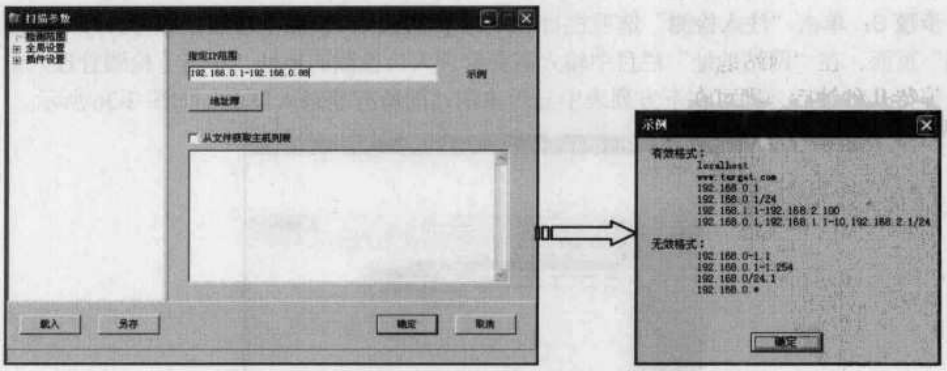


图 2-39　设置扫描 IP 范围

步骤 2：选择“检测范围”选项，即可设置扫描 IP 地址的范围。在“指定 IP 范围”文本框中，可输入需要扫描的 IP 地址（如 192.168.0.1）、IP 地址段（如 192168.0.1 ~ 192.168.0.88），还能增加子网掩码（如 192.168.0.1/24）等。若不知道输入的格式，则可以单击该文本框右侧的

【示例】按钮，在弹出的【示例】对话框中查看输入的有效格式。

步骤 3：除手动输入扫描范围外，还可通过选择“从文件中获取主机列表”选项，从存储有 IP 地址的文本文件中读取待检测的主机地址。在文本文件中，每一行可包含独立 IP 或域名，也可以包含以“-”和“,”分隔的 IP 范围。

步骤 4：在 IP 地址输入完毕后，可以发现扫描结束后自动生成的“报告文件”项中的文件名也在发生相应的变化。通常这个文件名不必手工修改，只需记住这个文件将会保存在 X-Scan 目录的 LOG 目录下。设置完毕后，单击【确定】按钮，即可关闭对话框。

3. 开始扫描

在设置好扫描参数之后，就可以开始扫描了。单击 X-Scan 工具栏上的【开始扫描】按钮 ▶，即可按设置条件进行扫描，同时显示扫描进程和扫描所得到的信息（可通过单击右下方窗格中的“普通信息”、“漏洞信息”及“错误信息”选项卡，查看所得到的相关信息），如图 2-40 所示。在扫描完成后将自动生成扫描报告并显示出来，其中显示了活动主机 IP 地址、存在的系统漏洞和其他安全隐患，同时还提出了安全隐患的解决方案，如图 2-41 所示。

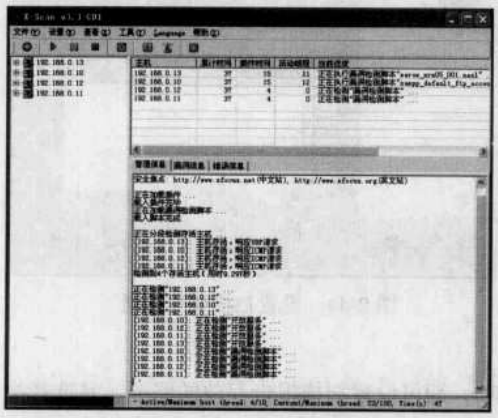


图 2-40 扫描进度

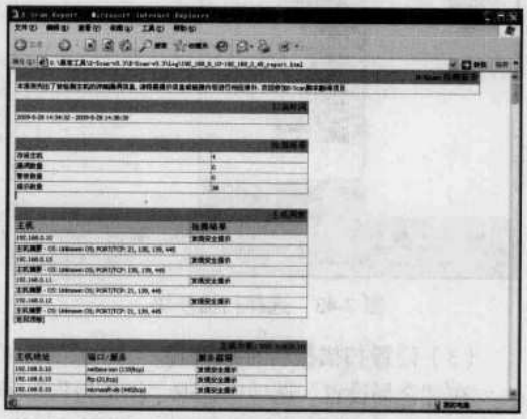


图 2-41 扫描报告

X-Scan 扫描工具不仅可扫描目标计算机的开放端口及存在的安全隐患，而且还具有目标计算机物理地址查询、检测本地计算机网络信息和 Ping 目标计算机等功能，如图 2-42 所示。

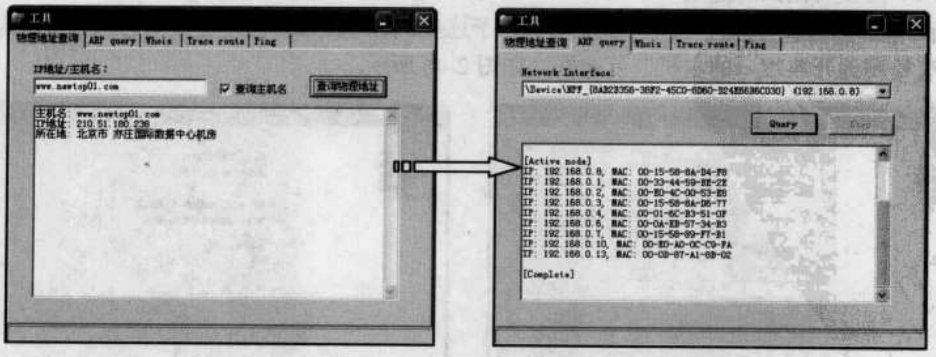


图 2-42 X-Scan 的其他功能

当所有选项都设置完毕之后，如果还想将来使用相同的设置进行扫描，则可以对这次的设置进行保存。在【扫描参数】对话框中单击【另存】按钮，即可将自己的设置保存到系统中。

当再次使用时只需单击【载入】按钮，选择已保存的文件即可。

4．高级设置

X-Scan 在缺省状态下效果往往不会发挥到最佳状态，这个时候就需要进行一些高级设置来让 X-Scan 变得强大起来。高级设置需要根据实际情况来做出相应的设定，否则 X-Scan 也许会因为一些“高级设置”而变得脆弱不堪。

（1）设置扫描模块

展开“全局设置”选项之后，选取其中的“扫描模块”选项，则可选择扫描过程中需要扫描的模块，在选择扫描模块时还可在其右侧窗格中查看该模块的相关说明，如图 2-43 所示。

（2）设置扫描线程

因为 X-Scan 是一款多线程扫描工具，所以在“全局设置”选项下的“并发扫描”子选项中，可以设置扫描时的线程数量（扫描线程数量要根据自己网络情况来设置，不可过大），如图 2-44 所示。

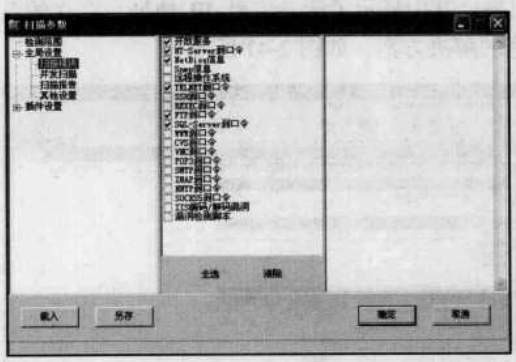


图 2-43　选择扫描模块

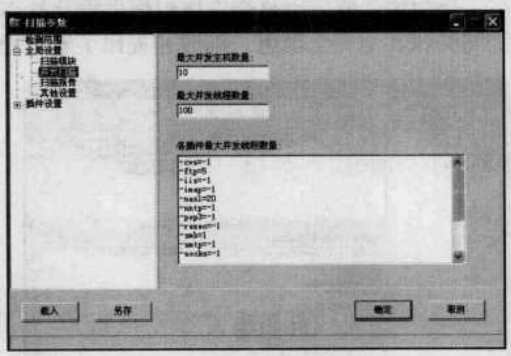


图 2-44　设置扫描线程数量

（3）设置扫描报告存放路径

在“全局设置”选项中选取“扫描报告”子选项，即可设置扫描报告存放的路径，并选择报告文件保存的文件格式。若需要保存设置的扫描 IP 地址范围，则可在勾选“保存主机列表”复选框之后，输入保存文件名称，这样，以后就可以调用这些 IP 地址了。若用户需要在扫描结束时自动生成报告文件并显示报告，则可勾选“扫描完成后自动生成并显示报告”复选框，如图 2-45 所示。

（4）设置其他扫描选项

在“全局设置”选项中选取“其他设置”子选项，则可设置扫描过程其他选项，如勾选“跳过没有检测到开放端口的主机”复选框，如图 2-46 所示。

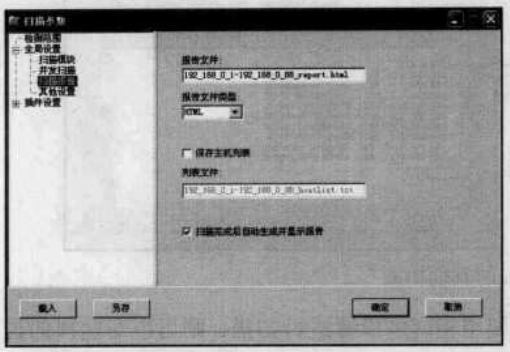


图 2-45　设置报告存放路径

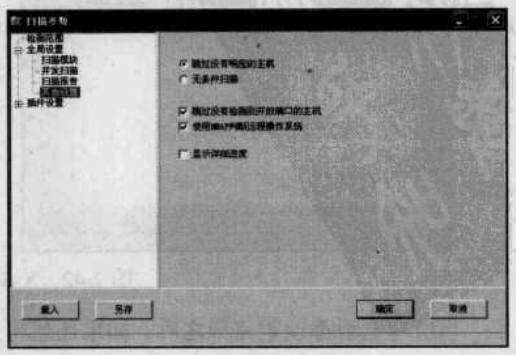


图 2-46　其他选项设置

（5）设置扫描端口

展开“插件设置”选项并选取“端口相关设置”子选项，即可扫描端口范围以及检测方式，如图 2-47 所示。若要扫描某主机的所有端口，则可在“待扫描端口”文本框中输入“1～65535”。

（6）设置 SNMP 扫描

在“插件设置”选项中选取“SNMP 相关设置”子选项，用户可以选取在扫描时获取 SNMP 信息的内容，如图 2-48 所示。

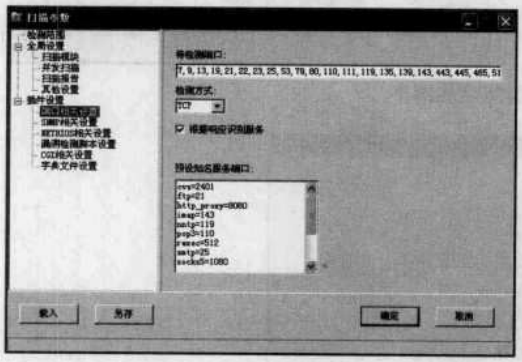


图 2-47 设置端口范围

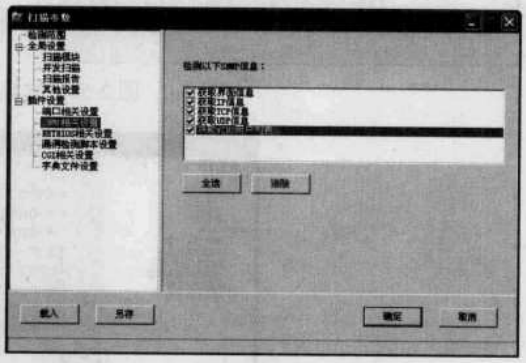


图 2-48 选择需要获取的 SNMP 信息

（7）设置 NETBIOS 扫描

选取“插件设置”选项下的“NETBIOS 相关设置”子选项，用户可以选择需要获取的 NETBIOS 信息，如图 2-49 所示。

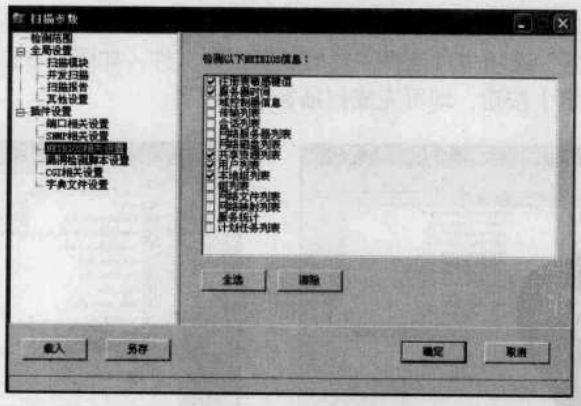


图 2-49 选取需要获取的 NETBIOS 信息

（8）设置漏洞检测脚本

选取“插件设置”选项下的“漏洞检测脚本设置”子选项，在显示窗口中取消勾选“全选”复选框，单击【选择脚本】按钮，即可选择扫描时需要加载的漏洞检测脚本，如图 2-50 所示。

（9）设置 CGI 插件扫描

在“插件设置”选项下选择“CGI 相关设置”子选项，即可选择扫描时需要使用的 CGI 选项，如图 2-51 所示。

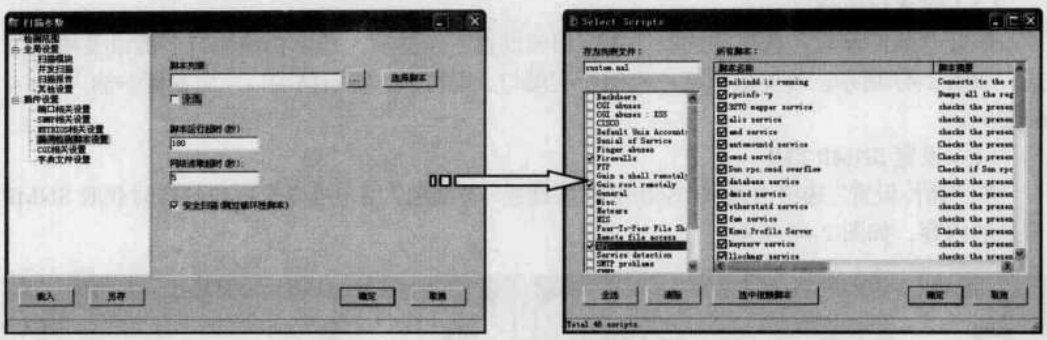


图 2-50　选择漏洞检测脚本

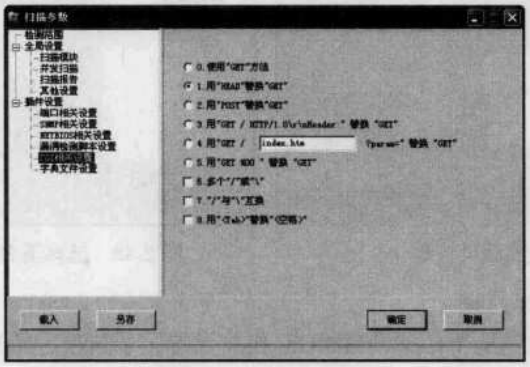


图 2-51　选取 CGI 选项

（10）设置字典文件

在“字典文件设置”选项中可选择需要的破解字典文件，如图 2-52 所示。在设置好所有选项之后，单击【确定】按钮，即可完成扫描参数的设置。

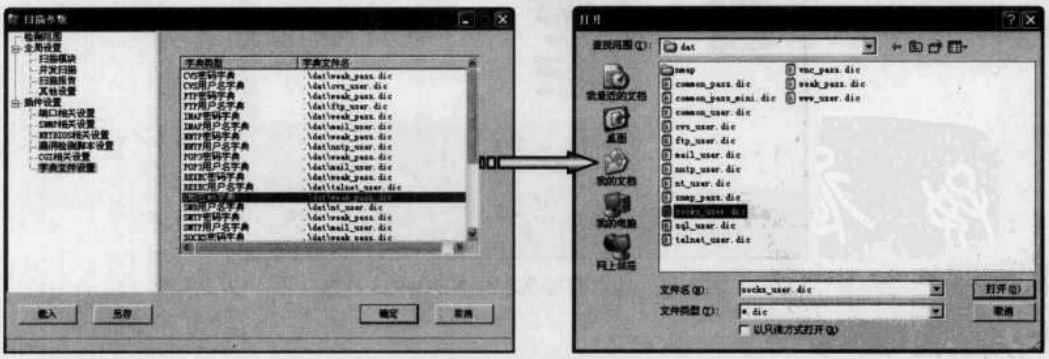


图 2-52　选择破解字典文件

第 12 招　用流光扫描主机漏洞

流光在国内的安全爱好者们心中可以说是无人不晓，它不仅仅是一个安全漏洞扫描工具，更是一个功能强大的渗透测试工具。流光以其独特的 C/S 结构设计的扫描设计颇得好评。

1．批量主机扫描

流光因功能较多，所以对初学者来说显得有点儿繁琐，不过幸好熟悉这个过程需要的时间不会太长，下面将为大家详细讲述用流光扫描主机漏洞的方法。具体操作步骤如下。

步骤 1：在“流光”主窗口中选择【文件】→【高级扫描向导】菜单项或按“Ctrl+W”组合键，即可弹出【设置】对话框，如图 2-53 所示。

步骤 2：在“起始地址”和“结束地址”项右侧文本框中输入起始 IP（如：192.168.0.1）和终止 IP（如：192.168.0.255），将“目录系统”设置为“Windows NT/2000”，如图 2-54 所示。

图 2-53 “流光”主窗口

图 2-54 【设置】对话框

步骤 3：在全选所有检测项目后，单击【下一步】按钮，即可打开【PORTS】对话框，在其中指定扫描的端口范围（这里既可选择“标准端口扫描”项，也可选中“自定端口扫描范围”项），自行设定所需要扫描的端口范围，如图 2-55 所示。

步骤 4：在如图 2-56 所示中全都选择默认状态后，单击【下一步】按钮，直到进入“Telnet”设置界面，则清空“SunOS Login”选项，如图 2-57 所示。

图 2-55 【PORTS】对话框

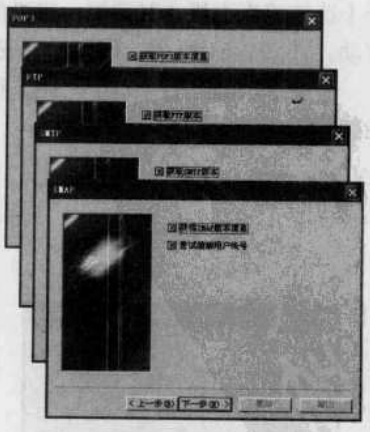


图 2-56 各个选项设置界面

步骤 5：单击【下一步】按钮进入“CGI Rules”设置界面，在操作系统类型列表中选择“Windows NT/2000”项，根据需要选中或清空下方扫描列表的具体选项，如图 2-58 所示。

图 2-57 “Telnet”设置界面

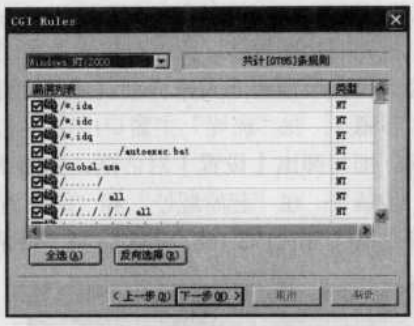


图 2-58 “CGI Rules”设置界面

步骤 6：单击【下一步】按钮，即可在如图 2-59 所示中选择默认状态，也可以根据实际需要清空部分选项。单击【下一步】按钮，即可进入“Plugings”设置界面，将操作系统的类型设置为“Windows NT/2000”选项，如图 2-60 所示。

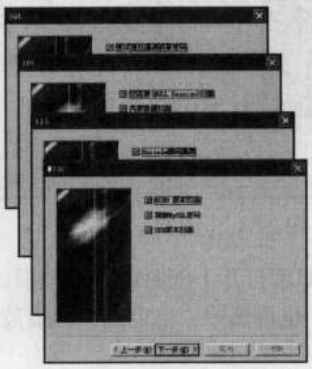


图 2-59 设置扫描各项

图 2-60 “Plugings”设置界面

步骤 7：在完成基本设置后，还需要指定扫描引擎的位置。单击【下一步】按钮，即可打开【选择流光主机】对话框，流光的扫描引擎既可以安装在不同的主机上，也可以直接从本地启动，如图 2-61 所示。如果没有安装过任何扫描引擎，流光将使用默认的本地扫描引擎。

步骤 8：单击【开始】按钮，程序开始进行扫描并可以在流光右上部分的控制台中看到正在扫描的内容，如图 2-62 所示。

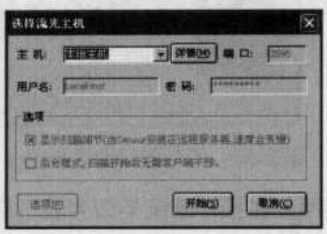


图 2-61 【选择流光主机】对话框

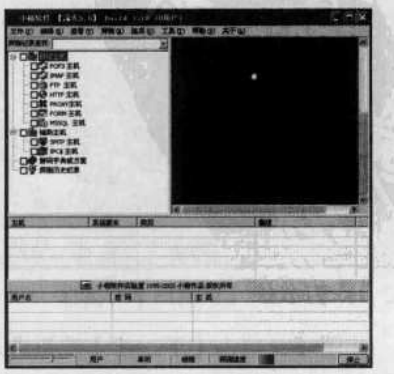


图 2-62 查看正在扫描的内容

步骤 9：当扫描到安全漏洞时流光会弹出一个“扫描结果”窗口，在其中可以看到能够连接成功的主机和其扫描到的安全漏洞信息，如图 2-63 所示。当扫描结束后，流光会弹出一个对话框，询问用户是否立即查看更为详细的扫描结果，如图 2-64 所示。

步骤 10：单击【是】按钮，随即流光将使用 IE 浏览器打开含有扫描报告的网页，在其中可以看到每台主机的详细扫描报告，如图 2-65 所示。

图 2-63 探测结果

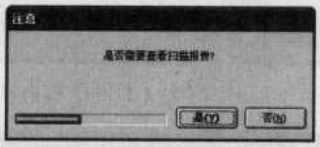


图 2-64 “注意”提示框

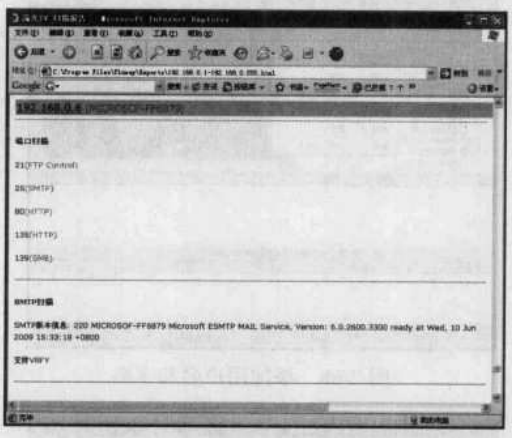


图 2-65 查看详细扫描报告

2. 指定漏洞扫描

很多时候并不需要对指定主机进行全面的扫描，而是根据需要对指定的主机漏洞进行扫描。比方说只想扫描指定主机是否具有 FTP 方面的漏洞，是否有 CGI 方面的漏洞等。

具体的操作步骤如下。

步骤 1：先加入需要破解的站点名称，只需在“流光”主窗口中右击“FTP 主机”，在快捷菜单中选择【编辑】→【添加】菜单项，即可打开【添加主机】对话框，如图 2-66 所示。

步骤 2：在其中输入远程主机的域名或 IP 地址，单击【确定】按钮关闭对话框，如图 2-67 所示。因为要探测主机的 FTP 是否存在漏洞，而这个是从 FTP 是否具有弱口令体现出来的。

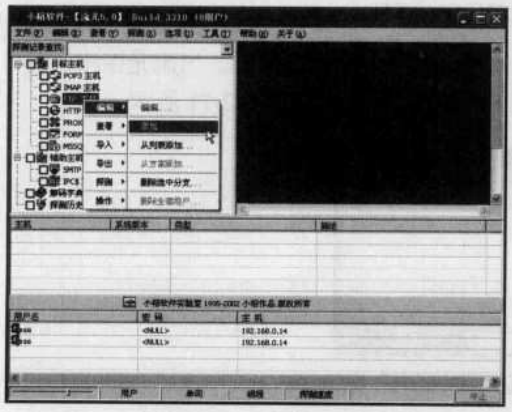


图 2-66 “流光”主窗口

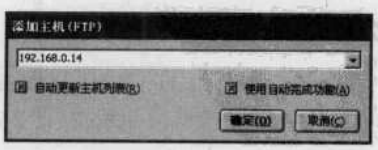


图 2-67 【添加主机】对话框

步骤 3：还需在流光中添加用户和密码的字典。右击添加主机“192.168.0.14”，在快捷菜单中选择【编辑】→【从列表中添加】菜单项，即可打开【打开】对话框，如图 2-68 所示。

步骤 4：在【打开】对话框中选择流光安装目录中含有用户名列表的 Name 文件，如图 2-69 所示。单击【打开】按钮，双击新添加用户列表文件下的“显示所有项目”项，随即“显示所有项目”项将切换成“隐藏所有项目”项，而用户列表中的所有用户都将显示出来，此时可以通过鼠标单击勾选/清除复选框来决定用户名的选用与否，如图 2-70 所示。

图 2-68　添加用户名和字典

图 2-69 【打开】对话框

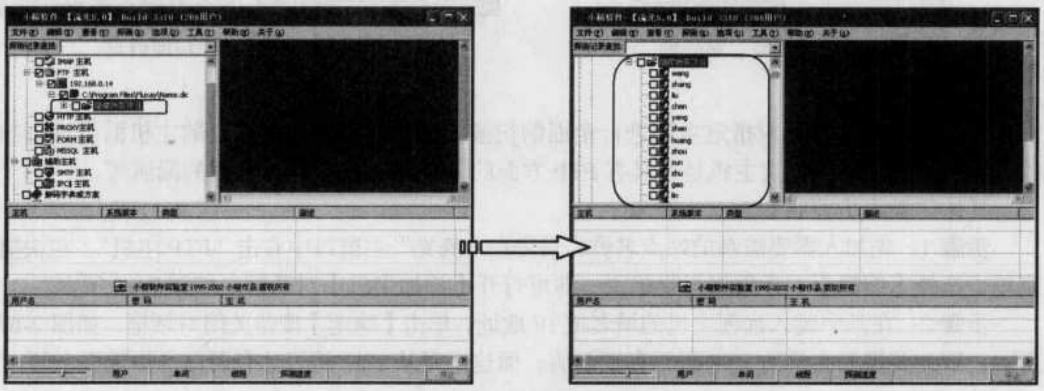


图 2-70　查看隐藏的所有项目

步骤 5：按“Ctrl+F7”快捷按钮，即可令流光开始 FTP 的弱口令探测。当流光探测到弱口令后，在主窗口下方将会出现探测到的用户名、密码和 FTP 地址，如图 2-71 所示。

图 2-71　显示“所有探测的密码”窗口

第 13 招　用 MBSA 检测 Windows 系统

Microsoft 基准安全分析器（Microsoft Baseline Security Analyzer，MBSA）工具允许用户扫

描一台或多台基于 Windows 的计算机，以发现常见的安全方面的配置错误。MBSA 将扫描基于 Windows 的计算机并检查操作系统和已安装的其他组件（如 IIS 和 SQL Server），以发现安全方面的配置错误，并及时通过推荐的安全更新进行修补。

1. MBSA 的安装设置

MBSA 可以执行对 Windows 系统的本地和远程扫描，可以扫描错过的安全升级补丁已经在 Microsoft Update 上发布的服务包。使用 MBSA V2.0 对系统漏洞进行安全分析之前，先要对 MBSA 进行安装设置，具体的操作步骤如下。

步骤 1：下载并双击“MBSA V2.0”安装程序图标，即可进入“Welcome to the Microsoft Baseline Security Analyzer（MBSA V2.0 欢迎安装向导）”界面，如图 2-72 所示。

步骤 2：单击【Next】按钮，即可打开【License Agreement】对话框，在其中阅读安装信息，如图 2-73 所示。

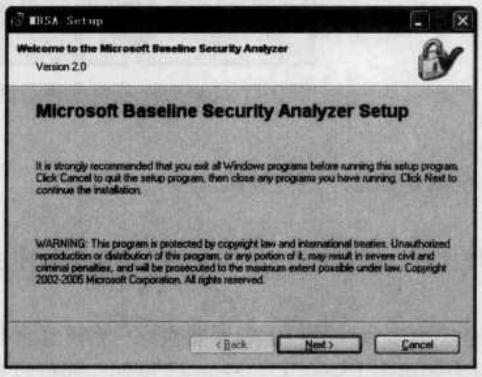


图 2-72 “Welcome to the Microsoft Baseline Security Analyzer”界面

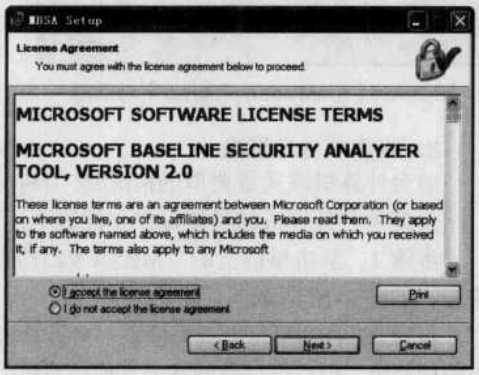


图 2-73 【License Agreement】对话框

步骤 3：在阅读完毕后，选择“I accept the license agreement”单选项，单击【Next】按钮，即可打开【Destination Folder】对话框。单击【Browse】按钮，在其中根据需要选择安装的目标位置，如图 2-74 所示。

步骤 4：在选择好安装的目标位置之后，单击【Next】按钮，即可打开【Start installation】对话框，如图 2-75 所示。若单击【Back】按钮，则返回上一级菜单。

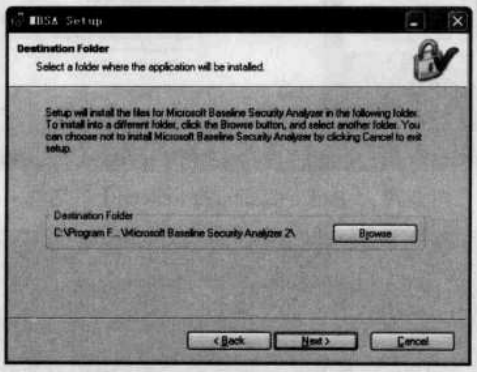


图 2-74 【Destination Folder】对话框

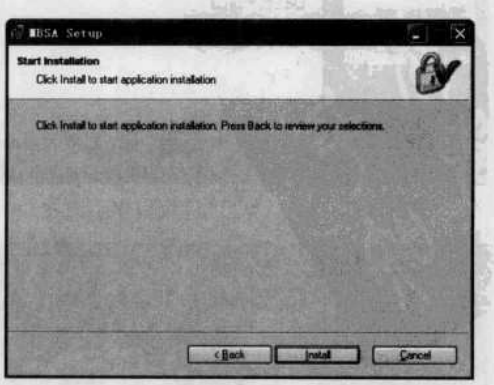


图 2-75 【Start installation】对话框

步骤 5：单击【Install】按钮，即可打开【Installation progress】对话框，程序开始安装并显示安装的进度条，如图 2-76 所示。程序安装完毕后，即可弹出【MBSA Setup】提示框，提示“Microsoft Baseline Security Analyzer Setup has Completed Successfully”信息。单击【OK】按钮，将完成整个安装过程，如图 2-77 所示。

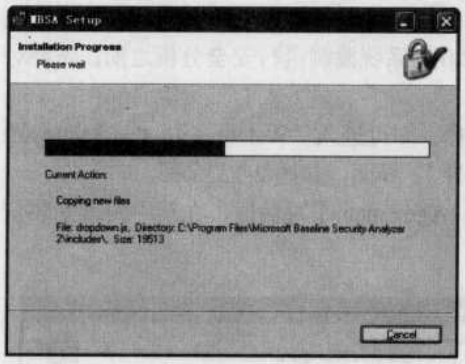


图 2-76 【Installation progress】对话框

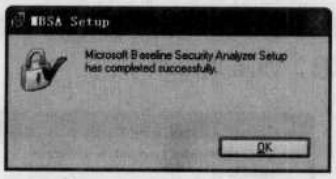


图 2-77 【MBSA 安装】提示框

2．检测单台计算机

单台计算机模式最典型的情况是“自扫描”，也就是扫描本地计算机。

扫描单台计算机的具体操作步骤如下。

步骤 1：双击桌面上的“MBSA V2.0”应用程序图标，即可进入“MBSA V2.0”应用程序主窗口，如图 2-78 所示。

步骤 2：在这里可以选择检测一台计算机，还是检测多台计算机。如果要检测一台（通常是当前计算机，但也可以是网络中其他计算机），则只需要单击【Scan a computer】按钮，即可打开【Pick a Computer to Scan】对话框，在“Computer name”栏中，选择默认的当前计算机名；用户也可以更改，在“IP address”栏中输入需要检测的其他计算机 IP 地址，如图 2-79 所示。

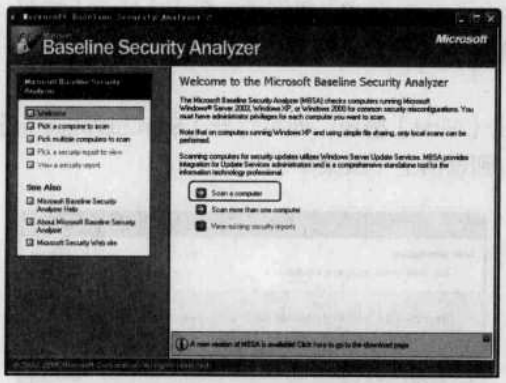


图 2-78 “MBSA V2.0”应用程序主窗口

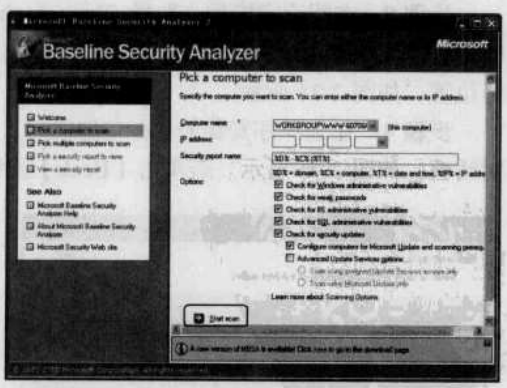


图 2-79 【Pick a Computer to Scan】对话框

提示 要想扫描一台计算机，必须具有该计算机的管理员访问权限才行。在【Pick a Computer to Scan】对话框中有许多复选框。其中涉及到选择扫描检测的项目，包括 Windows 系统本身、IIS 和 SQL 等相关选项，也就是 MBSA 的三大主要功能。根据检测到的计算机系统中所安装的程序系统和实际需要来确定。如果要形成检测结果报告文件，则在“Security report name”栏中输入报告文件名称。

步骤 3：在输入要检测的计算机并选择好要检测的项目后，单击【Start Scan】按钮，即可打开【Scanning】对话框，自动开始检测已选择项目并显示检测进度条，如图 2-80 所示。

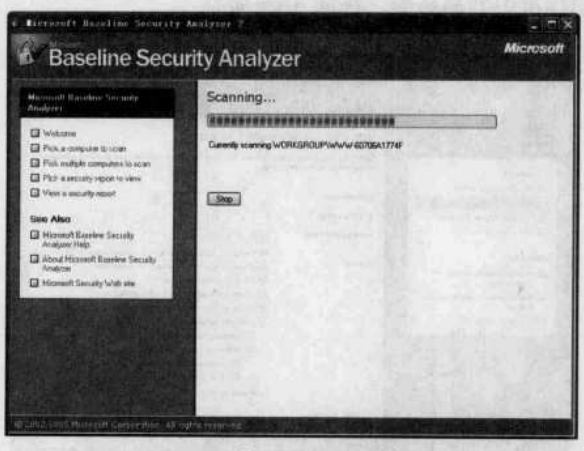


图 2-80 【Scanning】对话框

步骤 4：在检测完成之后，即可弹出【View Security report】对话框，如图 2-81 所示。若单击“Microsoft Baseline Security Analyzer”栏目下方的【Pick a security report to view】按钮，即可查看扫描后的安全报告内容，如图 2-82 所示。

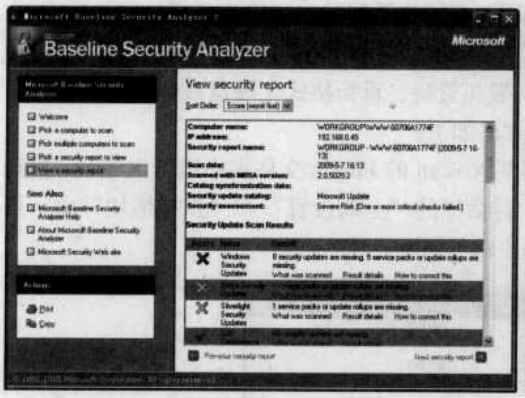


图 2-81 【View Security report】对话框

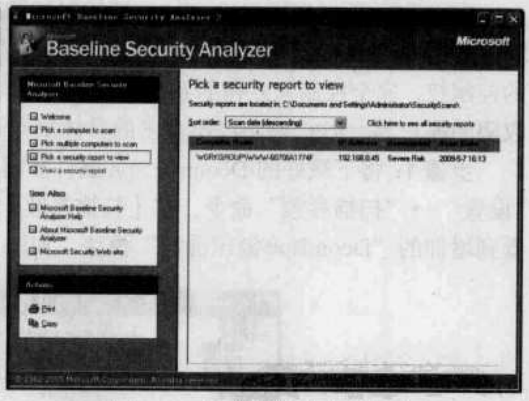


图 2-82 扫描后的安全报告内容

在报告中凡检测到存在严重安全隐患的则以红色“×”显示，中等级别的则以黄色“×”显示。用户还可单击“How to correct this”链接了解如何配置才能纠正这些不正确设置。

在如图 2-81 所示的检测结果中，第一项（Windows Security updates），是严重隐患，说明用户存在安全更新的问题。第二项和第三项（Office Security Updates 和 Silverlight Security Updates）是中等级别的隐患，说明 Office 软件的安全性更新与 Silverlight 的安全性更新等存在问题。

3. 检测多台计算机

多台计算机模式是对某一 IP 地址段或整个域进行扫描。只需单击左侧“Microsoft Baseline Security Analyzer”栏目下方的【Pick a Multiple Computers to Scan】按钮，即可指定要扫描检测的多台计算机。所扫描的多台计算机范围可通过在“Domain name”文本框中输入这些计算机

所在域来确定。这样，可检测相应域中所有计算机，也可通过在“IP address range”栏中输入IP地址段中的起始IP地址和终止IP地址来确定，这样，只检测IP地址范围内的计算机。单击【Start Scan】按钮，同样可以开始检测，如图2-83所示。

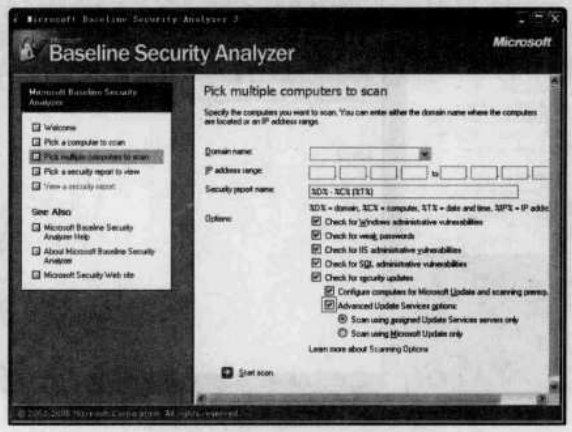


图2-83　检测的多台计算机

第14招　深入浅出RPC漏洞扫描

RPC（Remote Procedure Call，远程过程调用）是操作系统的一种消息传递功能。RPC在处理通过TCP/IP的消息交换部分有一个漏洞。如果成功利用此漏洞，攻击者就可以取得系统的控制权，完全控制被入侵的系统，窃取文件、破坏资料、重新格式化硬盘或建立系统管理员权限的账户等。RPC漏洞溢出攻击的具体操作方法如下。

步骤1：将下载好的Dcomrpc.xpn插件复制到X-scan的Plugin文件夹中运行X-scan，执行“设置”→“扫描参数”命令，在【扫描参数】对话框的“全局设置”和“扫描模块”中，可看到增加的“DcomRpc溢出漏洞”模块，如图2-84所示。

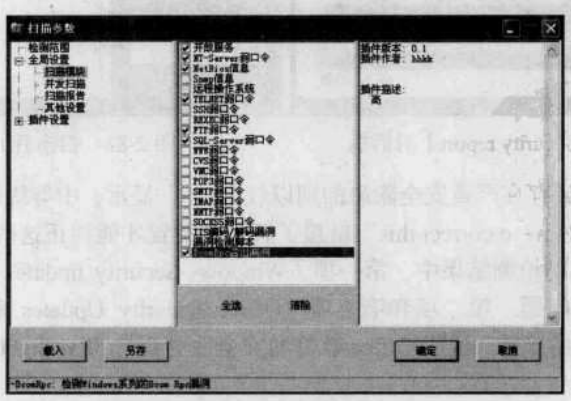


图2-84　添加RPC漏洞扫描模块

步骤2：如果使用rpc_locator.exe专用RPC溢出漏洞扫描工具，则先打开“命令提示符”窗口，进入rpc_locator.exe所在文件夹，执行“rpc_locator起始IP地址结束IP地址”命令后开始扫描并看到最终扫描结果，如图2-85所示。

步骤 3：在扫描到 RPC 溢出漏洞主机之后，可使用 cndcom.exe 溢出工具，执行“Cndcom <Target ID> <Target IP>”命令。

例如：攻击一个 IP 地址为 127.0.0.1，系统版本为英文版 Windows 2000+SP4 的目标主机，其对应的溢出攻击命令如图 2-86 所示。对于存在 RPC 溢出漏洞的系统，用户应及时下载相应的安全补丁并进行安装，同时还应使用防火墙封堵 135 端口。

图 2-85 rpc_locator 的使用

图 2-86 执行溢出工具命令

第 15 招 用 ProtectX 防御扫描器追踪

ProtectX 是一款在用户连接网络时保护电脑的工具，可以同时监视 20 个端口，还可以帮助追踪攻击者的来源。一旦任何入侵者尝试连接到用户的电脑，即可发出声音警告并将入侵者的 IP 位址记录下来，可以防止黑客入侵。

1. ProtecX 实用组件概述

ProtectX 安装过程与一般软件安装过程类似，这里不再赘述。在安装完毕 ProtectX 后重启系统，即可在 Windows 系统的通知栏中看到显示的 ProtectX 图标，双击即可显示操作界面，窗口中间显示的是当前本机状态信息，如图 2-87 所示。

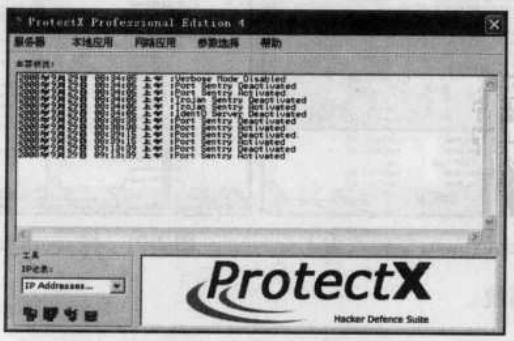


图 2-87 ProtectX 初始界面

ProtectX 提供了几项实用功能组件，依次是端口安全（Port Sentry）、特洛伊安全（Trojan Sentry）和 Identd 服务（Identd Server）等。

1）端口安全。端口安全就是端口扫描监视器，在 TCP 端口 1 上监听，如果有扫描活动触发到 1 号端口，则 Port Sentry 将会报警，如图 2-88 所示。Protectx 便可反跟踪对方，查询其域

名、追溯起路由信息，并显示所截击到的扫描信息，如图 2-89 所示。

图 2-88　Port Sentry 的报警信息

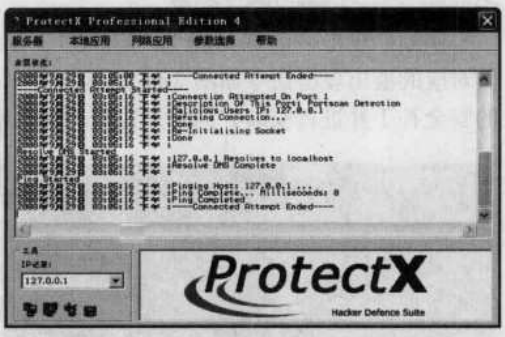


图 2-89　显示所截击到的扫描信息

2）特洛伊安全。特洛伊安全是指在一些木马常用端口上进行监听，一旦发现有人试图连接这些端口，即可报警。

3）Identd 服务。可在计算机上打开一个安全 Identd 服务，初级用户最好不要打开这个服务。

2．防御扫描器入侵

有了 ProtectX 的保护，对于一般的扫描攻击，大家就不用担心了。不过仅仅依靠这个工具，还远远谈不上安全，还需要提前做好防御扫描入侵的准备。

1）对于 Windows 2000/XP 用户，要修改注册表，禁止匿名用户对 IPC$的访问。方法是在注册表编辑器中展开到 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControl Set\Control\Lsa 分支，找到 restrictanonymous 键值并将其值改为 1，如图 2-90 所示。

2）修改注册表，禁止自动管理共享。在注册表编辑器中展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControl Set\Services\Lanmanserver\parameters 分支，找到 AutoShareServer 键值并将其改为 0，同时找到 AutoShareWKs 键值，改为 0，如图 2-91 所示。

图 2-90　将 restrictanonymous 键值改为 1

图 2-91　将 restrictanonymous 键值改为 0

3）及时更新操作系统。

第 16 招　监控局域网计算机

针对机房中的用户经常误设工作组、随意更改计算机名、IP 地址和共享文件夹等情况，可以使用“局域网查看工具 LanSee”非常方便地完成监控，既可以迅速排除故障，又可以解决一些潜在的安全隐患。

1．搜索计算机

LanSee 是一款主要用于对局域网（Internet 上也适用）上各种信息进行查看的工具，采用多线程技术，将局域网上比较实用的功能完美地融合在一起，功能十分强大。

使用 LanSee 工具搜索计算机的具体操作步骤如下。

步骤 1：双击下载的应用程序，即可打开【局域网查看工具】主窗口，如图 2-92 所示。

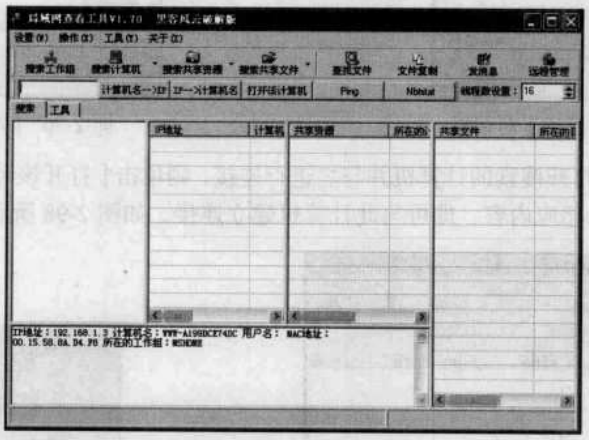


图 2-92 【局域网查看工具】主窗口

步骤 2：单击【设置】按钮，即可在【设置】对话框中选择相应网段形式，并进行相应的设置，如图 2-93 所示。在【搜索计算机设置】选项卡中选择在局域网内搜索计算机的选项，并在其文本框中输入搜索的相关任务，如图 2-94 所示。

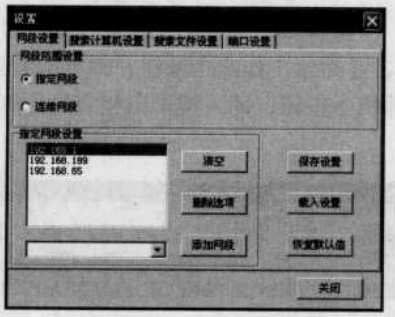


图 2-93 【设置】对话框

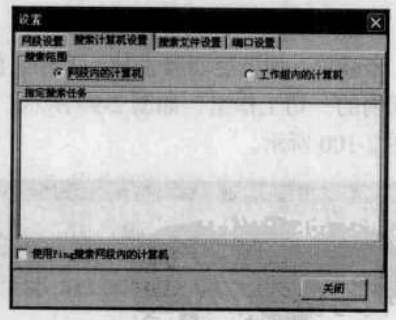


图 2-94 【搜索计算机设置】对话框

步骤 3：在【搜索文件设置】选项卡中没有要使用的文件类型，则可在【添加】按钮左侧的文本框中输入需要的文件格式名，如图 2-95 所示。单击【添加】按钮，即可成功添加。

步骤 4：在选择所需格式之后，单击【保存设置】按钮，即可完成对搜索文件的设置。在【端口设置】选项卡中选择扫描的范围，并在“常用端口设置”中选择要使用的端口，如图 2-96 所示。

步骤 5：打开【局域网查看工具】主窗口后，在“搜索工作组”文本框中输入某台计算机名称，单击【计算机名→IP】按钮，即可在文本框中显示出该计算机 IP 地址，如图 2-97 所示。

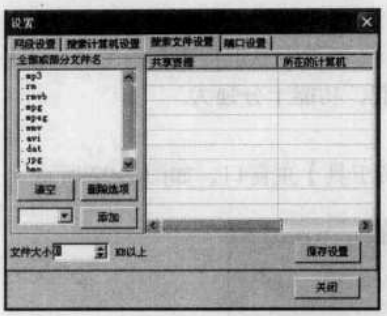


图 2-95 【搜索文件设置】对话框

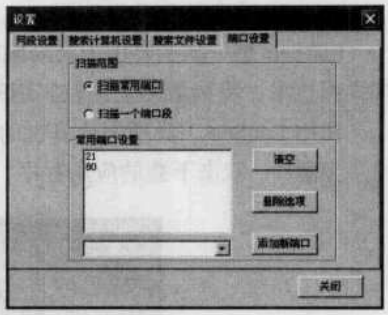


图 2-96 【端口设置】对话框

步骤 6：如果要打开搜索的计算机并与之进行连接，则单击【打开该计算机】按钮，在【连接到】对话框中输入相应内容，即可与此计算机建立连接，如图 2-98 所示。

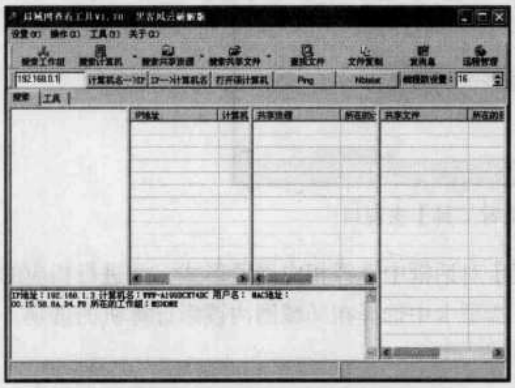


图 2-97 IP 地址的显现

图 2-98 【连接到】对话框

步骤 7：如果想要搜索某一工作组的计算机，则单击【搜索工作组】按钮，即可搜索到局域网内的一切工作组，如图 2-99 所示。单击【搜索计算机】按钮，即可搜索出相应的计算机，如图 2-100 所示。

图 2-99 工作组显现

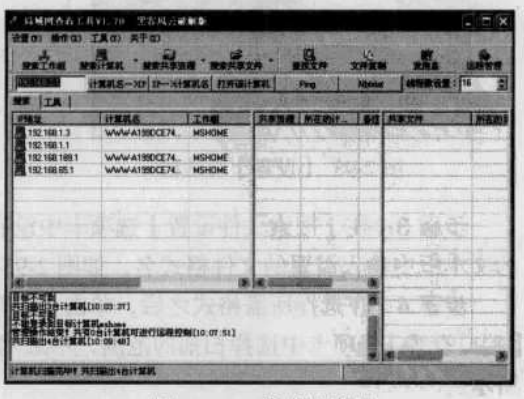


图 2-100 搜索计算机

2. 搜索共享资源

共享资源往往是局域网数据泄漏的“罪魁祸首”，网管要经常检查局域网中是否存在一些

不必要的开放共享资源，在查看到不安全因素后，要及时通知开放共享的用户将其关闭。

在 LanSee 中进行这个操作前需要先搜索出计算机，单击菜单栏中【搜索共享资源】按钮，即可在“共享资源列表”框中看到每台计算机开放的共享资源，如图 2-101 所示。

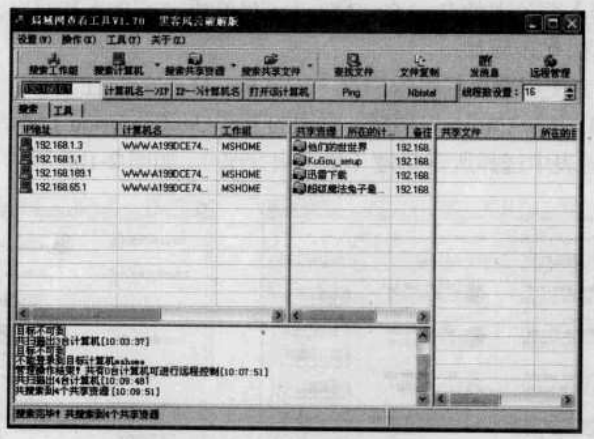


图 2-101 搜索共享资源

第 17 招 Real Spy Monitor 监控网络

Real Spy Monitor 是一个监测互联网和个人电脑，以保障其安全的软件，包括键盘敲击、网页站点、视窗开关、程序执行、屏幕扫描以及文件的出入等都是其监控的对象。

1．添加使用密码

在使用 Real Spy Monitor 对系统进行监控之前，要进行一些设置，具体的操作步骤如下。

步骤 1：在安装完 Real Spy Monitor 之后，双击桌面上的“Real Spy Monitor”应用程序图标，即可弹出“注册”页面，如图 2-102 所示。

步骤 2：在阅读相应的注册信息后，单击【Continue..】按钮，即可打开【SetPassWord】对话框。由于是第一次使用，所以没有旧密码可更改，只需在“New Password”和“Confirm”文本框中输入相同的密码。单击【OK】按钮，即可完成密码设置，如图 2-103 所示。

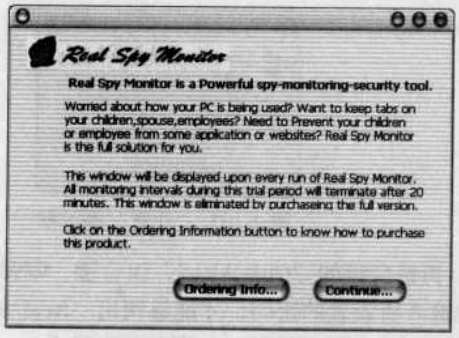


图 2-102 “注册”页面

图 2-103 【SetPassWord】对话框

小技巧 在【SetPassWord】对话框中所填写的新密码，将会在 Real Spy Monitor 的使用中处处要用，所以千万不能忘记密码。

2. 设置弹出热键

需要设置弹出热键，那是因为 Real Spy Monitor 运行时会彻底地将自己隐藏，用户在“任务管理器”等处看不到该程序的运行。要将运行时的 Real Spy Monitor 调出就要使用热键才行，否则即使单击【开始】菜单中的 Real Spy Monitor 菜单项也不会将其调出。

设置热键的具体操作步骤如下。

步骤 1：在设置完使用密码后将返回到“Real Spy Monitor”主窗口，如图 2-104 所示。

步骤 2：单击“Hotkey Choice”图标，即可打开【Configuration】对话框，在“Select your hotkey patten”下拉列表中选择所需热键（也可自定义），如图 2-105 所示。

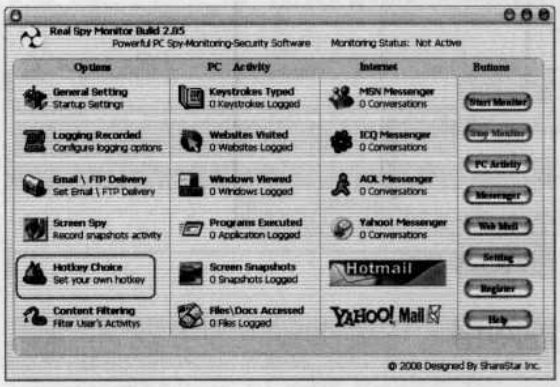


图 2-104 “Real Spy Monitor”的主窗口

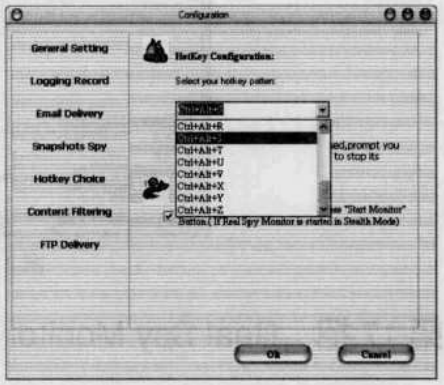


图 2-105 【Configuration】对话框

3. 监控浏览过的网站

在完成了最基本的设置后，就可以使用 Real Spy Monitor 进行系统监控了。下面讲述 Real Spy Monitor 如何对一些最常使用的程序进行监控。监控浏览过的网站的具体操作步骤如下。

步骤 1：单击“Real Spy Monitor”主窗口中的【Start Monitor】按钮，为确保程序的使用者是设置使用密码的那个用户，Real Spy Monitor 将会弹出【密码输入】对话框，只有输入正确的密码后，才可能让 Real Spy Monitor 听从号令，如图 2-106 所示。

步骤 2：单击【OK】按钮，即可弹出“注意”提示框，在认真阅读注意信息后，单击【OK】按钮，如图 2-107 所示。

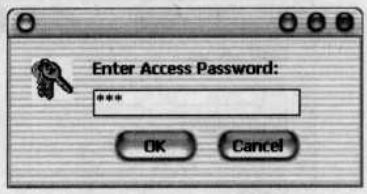


图 2-106 【密码输入】对话框

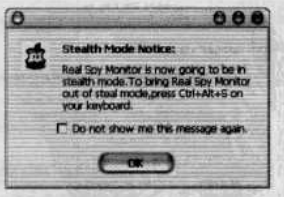


图 2-107 “注意”提示框

步骤 3：使用 IE 浏览器随便浏览一些网站后，再按所设的“Ctrl+Alt+S”组合键，则弹出如图 2-108 所示的窗口。在【密码输入】对话框中输入所设置的密码，才能够调出“Real Spy Monitor”主窗口，可以发现其中“Websites Visited”项下已有了计数，如图 2-109 所示。

步骤 4：在其中可以看出计数的数字为 37，这表示共打开了 37 个网页。单击“Websites Visited”项中的图标后将弹出“Report”窗口，可看到列表里的 37 个网址。这就是 Real Spy Monitor 监控到使用 IE 浏览器打开的网页。

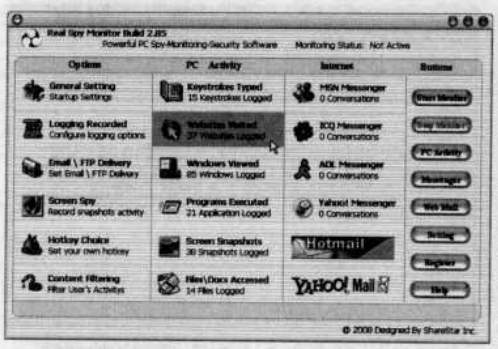


图 2-108 查看 Websites Visited 计数个数

图 2-109 Websites Visited “Report”窗口

提示 如果想要深入查看相应网页是什么内容，只需要双击列表中的网址，即可自动打开 IE 浏览器访问的相应网页。

4．键盘输入内容监控

对键盘输入的内容进行监控通常是木马做的事，但 Real Spy Monitor 为了让自身的监控功能变得更加强大也提供了此功能。其针对键盘输入内容进行监控的具体操作步骤如下。

步骤 1：在输入一些内容后，再按所设的“Ctrl+Alt+S”组合键，则会弹出如图 2-108 所示的窗口。在【密码输入】对话框中输入所设置的密码调出“Real Spy Monitor”主窗口，此时可以发现“Keystrokes Typed”项下已经有了计数，如图 2-110 所示。

步骤 2：在其中可以看出计数的数字为 15，这表示有和计数数字相同的 15 条记录。单击“Keystrokes Typed”项中的图标后，弹出“Report”窗口，在其中可以看到有和计数数字相同的 15 条记录，如图 2-111 所示。

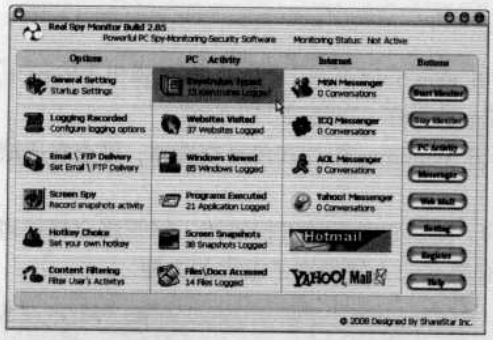


图 2-110 查看 Keystrokes Typed 计数个数

图 2-111 Keystrokes Typed 的“Report”窗口

步骤 3：双击其中任意一条记录，弹出记事本窗口，在其中可以看出“Administrator”用户在某点某时某分输入的信息，如图 2-112 所示。如果用户输入了“Ctrl”类的快捷键，则 Real Spy Monitor 同样也可以捕获到，如图 2-113 所示。

5．程序执行情况监控

如果想知道用户都在计算机中运行哪些程序，只需在“Real Spy Monitor”主窗口中单击“Programs Executed”图标，在弹出报告对话框中可看到运行的程序名和路径，如图 2-114 所示。

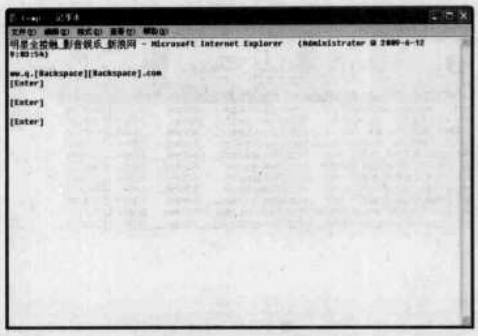


图 2-112　查看记事本

图 2-113　捕获包含“Ctrl”这类的快捷键

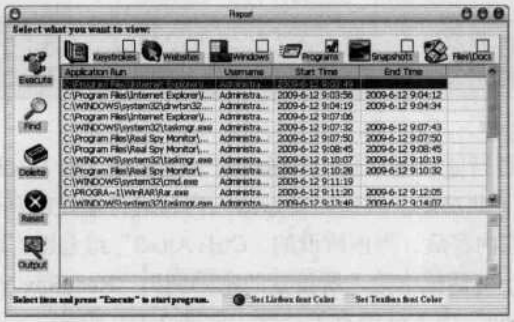


图 2-114　Programs Executed 的“Report”窗口

6. 即时截图监控

用户可以通过 Real Spy Monitor 的即时截图监控功能（默认为一分钟截一次图）来查知用户的操作历史。

监控即时截图的具体操作步骤如下。

步骤 1：在“Real Spy Monitor”主窗口单击“Screen Snapshots”图标，即可弹出【Reprot】对话框，在其中可看到 Real Spy Monitor 对系统进行的操作，如图 2-115 所示。

步骤 2：也可双击其中任意一项截图记录，打开 Windows 图片和传真查看器，可查看所截取的图，如图 2-116 所示。

显然，Real Spy Monitor 的功能是极其强大的。使用它对系统进行监控，网管将会轻松得多。在一定程度上，为查看网管监控系统中是否有黑客的入侵带来了极大的方便。

图 2-115　Screen Snapshots 的“Report”窗口

图 2-116　查看所截取的图

第 3 章　控制与反控制技术

重点提示

- 远程控制经典 PcAnywhere
- 用“冰河陷阱”揪出冰河木马
- 用 QuickIP 进行多点控制
- 用 WinShell 实现远程控制
- 用灰鸽子实现远程管理
- 远程控制命令 PsExec
- 实现 Serv-U 远程控制
- 用 SyGate 突破上网封锁

本章精粹：

本章介绍了远程控制的基础知识，远程控制技术的运用方法，以及黑客远程控制工具的使用技巧等内容。其中包括：远程控制经典 PcAnywhere 工具、冰河木马工具、灰鸽子工具、QuickIP 工具等实例操作，有助于读者对远程控制技术有一个全面认识，以便预防黑客入侵。

在黑客攻击中，远程控制也是非常关键的黑客技术。控制与反控制一直是黑客与安全人员之间的一对矛盾，在相互较量中不断上演着一幕又一幕“魔高一尺，道高一丈”的好戏。

第 18 招　远程控制经典 PcAnywhere

Symantec PcAnywhere 是一款非常经典的远程控制工具，可以提高技术支持效率并减少呼叫次数。使用被控端会议功能，可建立到一个 Symantec PcAnywhere 被控端的多个并发远程连接。使用 PcAnywhere 远程控制软件，需要同时在主控端和被控端计算机上进行安装。

1．设置 PcAnywhere 的性能

在主控端和被控端计算机中分别安装好 PcAnywhere 之后，要想真正让 PcAnywhere 控制远程计算机，要做的第一步工作就是配置被控端计算机。

（1）使用联机向导配置被控端

配置被控端的具体设置步骤如下。

步骤 1：双击“Symantec pcAnywhere”图标，即可进入 pcAnywhere 窗口，如图 3-1 所示。单击【主机】链接选项，即可打开【连接向导-连接方法】对话框，如图 3-2 所示。

图 3-1　pcAnywhere 的操作窗口

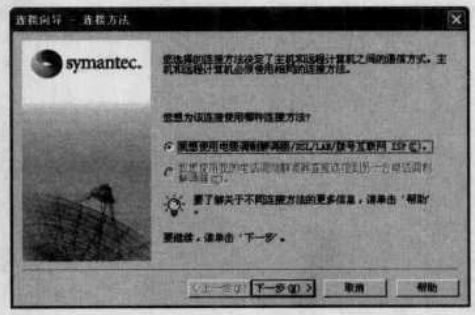


图 3-2 【连接向导-连接方法】对话框

步骤 2：在选择好连接方法之后，单击【下一步】按钮，即可打开【连接向导-连接模式】对话框，在其中选择“等待有人呼叫我”单选项，如图 3-3 所示。

步骤 3：在选择好连接模式后，单击【下一步】按钮，即可打开【连接向导-验证类型】对话框，在其中选择需要的验证类型，如选取“我想使用存在的 Windows 账户”单选项，如图 3-4 所示。

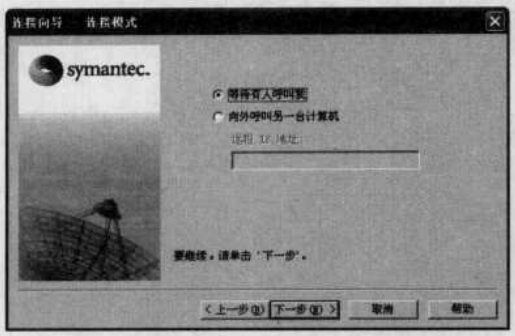


图 3-3 【连接向导-连接模式】对话框

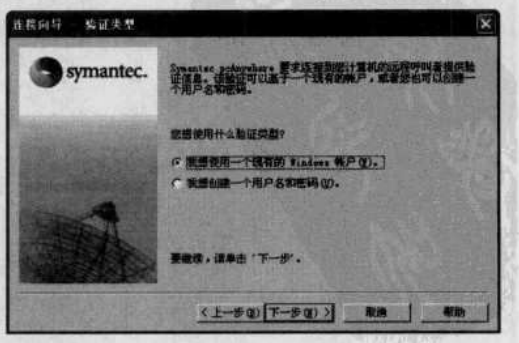


图 3-4 【连接向导-验证类型】对话框

步骤 4：单击【下一步】按钮，即可打开【连接向导-选择账户】对话框，在其中选择远程

登录用户所使用的本地账户，如图 3-5 所示。

步骤 5：继续单击【下一步】按钮，即可打开【连接向导-摘要】对话框，在其中勾选“连接向导完成后等待来自远程计算机的连接”复选框，如图 3-6 所示。

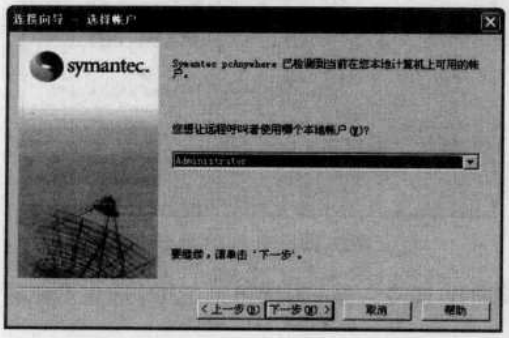


图 3-5 【连接向导-选择账户】对话框

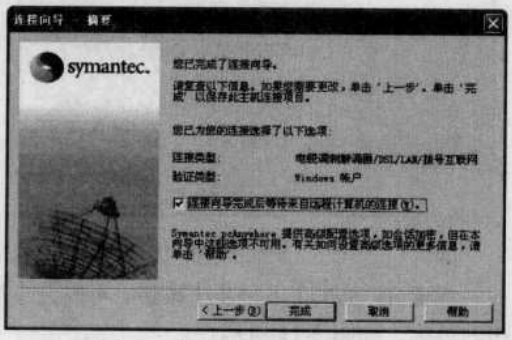


图 3-6 【连接向导-摘要】对话框

步骤 6：单击【完成】按钮，即可关闭连接向导，同时在 Windows 的通知区域中显示一个 图标，表示 PcAnywhere 正在等待远程控制端的连接。右击新添加的远程控制端并在打开的快捷菜单中选择【属性】菜单项，即可打开其属性对话框，如图 3-7 所示。在【安全性选项】选项卡中可设置联机选项、登录选项、会话选项以及数据加密等安全策略，如图 3-8 所示。

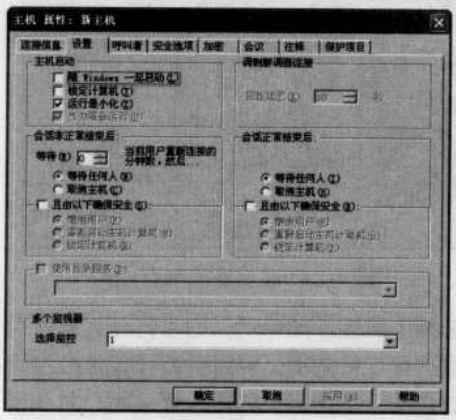


图 3-7 设置选项卡

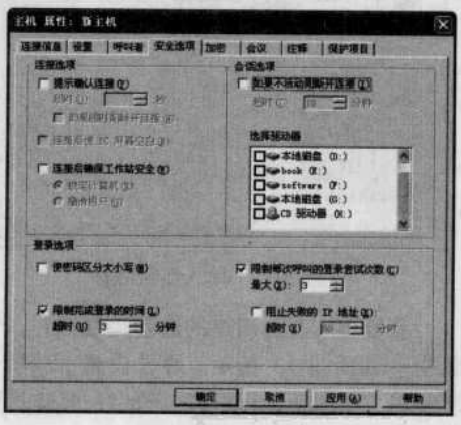


图 3-8 安全性设置

步骤 7：在上述属性都配置好之后，单击【确定】按钮，即可完成被控端的设置。右击主机图标，在快捷菜单中选择【启动主机】菜单项，主机将启动并在系统任务栏上显示一个电脑形状的图标，开始等待远程控制端进行连接。当有用户远程连接时，图标将改变颜色。

提示 在被控端需要有多点传播地址，且此地址必须介于 255.1.1.1～239.254.254.254 之间。

（2）使用联机向导设置主控端

在设置好被控主机之后，还需配置主控制端计算机。配置主控制端的具体操作步骤如下。

步骤 1：在【PcAnywhere 管理器】任务栏中选择【远程】选项，选择【文件】→【新建项目】→【连接向导】菜单项，可打开【连接向导-连接方法】对话框，如图 3-9 所示。

步骤 2：在选择好连接方法之后，单击【下一步】按钮，可进入【连接向导-目标地址】对话框，在其中输入远程计算机的 IP 地址，如图 3-10 所示。

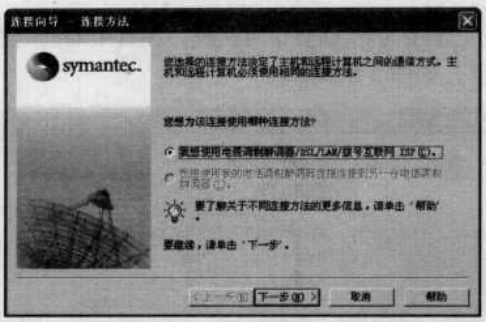


图 3-9　选择连接方式

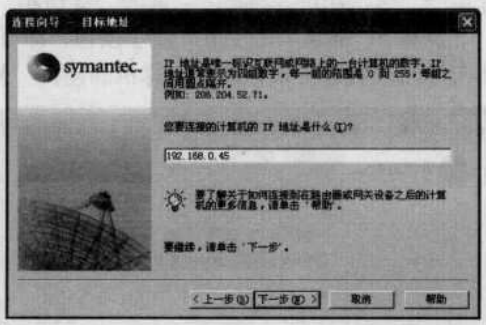


图 3-10　输入 IP 地址

步骤 3：单击【下一步】按钮，可打开【连接向导-连接名称】对话框，在其中输入需要连接的名称，如图 3-11 所示。

步骤 4：单击【下一步】按钮，可打开【连接向导-摘要】对话框，勾选“连接向导完成后连接到主机计算机”复选框，再查看自己的设置是否正确。若无误，则单击【完成】按钮，即可关闭连接向导，如图 3-12 所示。

图 3-11　输入连接名称

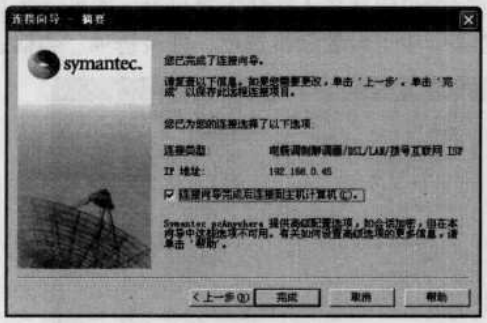


图 3-12　完成连接向导

步骤 5：右击新建的远程控制端并在快捷菜单中选择【属性】菜单项，则可打开其属性对话框，如图 3-13 所示。在【设置】选项卡中可以配置远程连接选项，可以重新设置被控端计算机的 IP 地址，还可以勾选“一旦连接即自动登入被控端”复选框，并输入登录用户名和密码等选项，如图 3-14 所示。

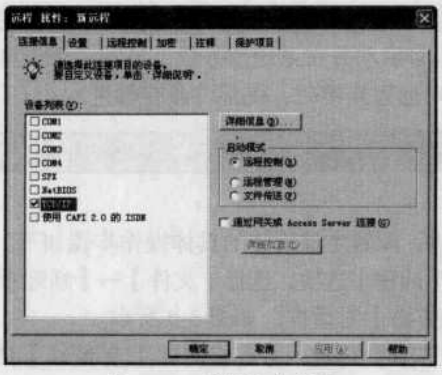


图 3-13　连接信息设置

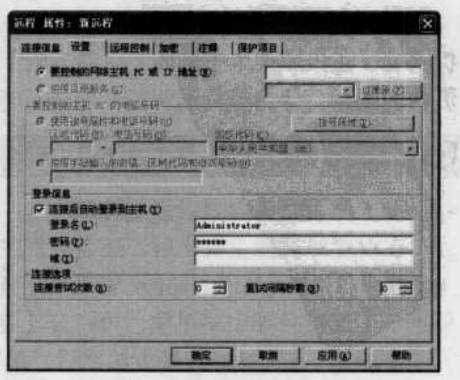


图 3-14　设置登录选项

在【加密】选项卡中可设置该主控端在远程控制过程中使用的加密级别，默认不加密。可按照需要选择使用对称密钥、公钥或 PcAnywhere 加密方式，其中 PcAnywhere 加密方式将前面的两种加密技术结合在一起，具有速度和安全性两方面优点，如图 3-15 所示。

在【PcAnywhere 管理器】任务栏中选择【快速连接】选项之后，需要在其中输入被控主机的 IP 地址、计算机名称，如图 3-16 所示。单击【连接】按钮，可与被控主机建立连接，在“启动模式”下拉列表中可选择“远程控制”、“远程管理”和“文件传送”等选项。

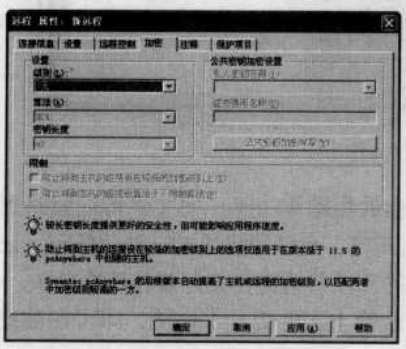


图 3-15 设置加密功能

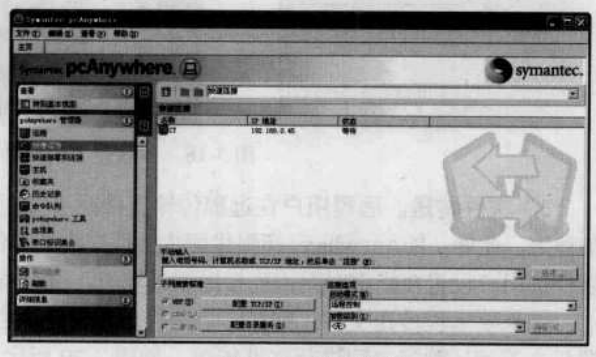


图 3-16 快速连接

（3）快速部署与联机

快速部署与联机的具体操作步骤如下。

步骤 1：在【PcAnywhere 管理器】任务栏中选择【快速部署与连接】选项，可看到已经连接的计算机名称，如图 3-17 所示。

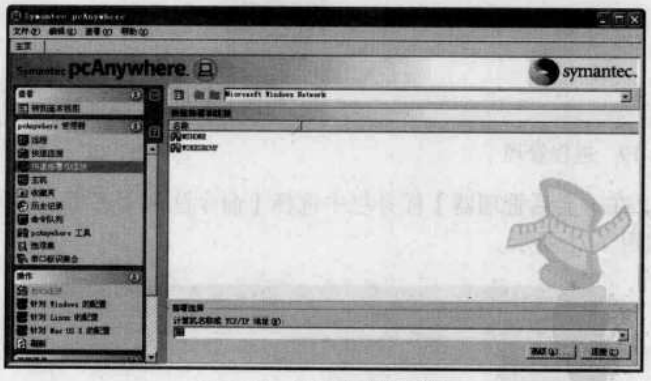


图 3-17 快速部署与联机

步骤 2：双击需要连接的被控主机的计算机名称，可显示如图 3-18 所示的对话框。在其中输入登录用户名和密码之后，单击【确定】按钮，可与被控主机建立连接。

2. 用 PcAnywhere 进行远程控制

与被控主机连接并成功登录，就可以对被控主机进行远程控制。

1）远程控制。在【会话管理器】任务栏中选择【远程控制】选项，即可对被控主机的桌面进行远程控制，如打开或关闭远程窗口、通过被控主机进行网页浏览等。

2）远程管理。在【会话管理器】任务栏中选择【远程管理】选项，即可对被控端计算机运行的应用程序以及进程进行管理，如图 3-19 所示。

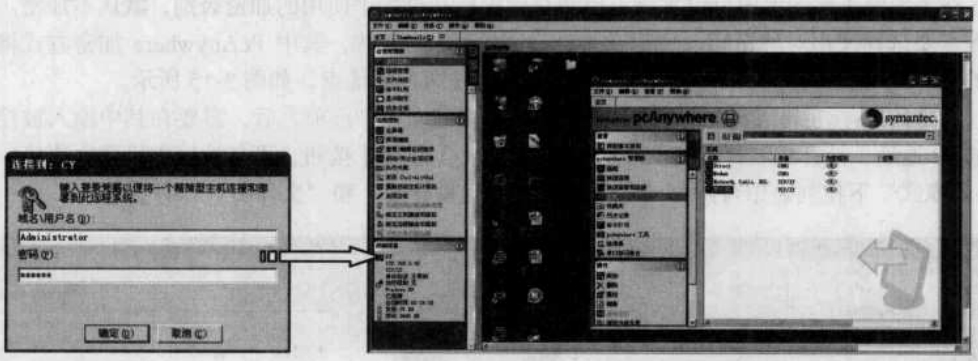


图 3-18　与被控主机成功建立连接

3）文件传送。远程用户在远程传输文件时可暂时中止远程操作功能，使文件传输线路更加稳定。此外，PcAnywhere 还提供同步文件夹的方式传送文件，允许用户通过自动化任务，让软件按用户设置在指定时间内连接远程计算机，进行指定的文件传输操作或同步指定文件夹。

如果要远程传送文件，则在【会话管理器】任务栏中选择【文件传送】选项，即可在被控端与主控端计算机之间进行文件传送，如图 3-20 所示。

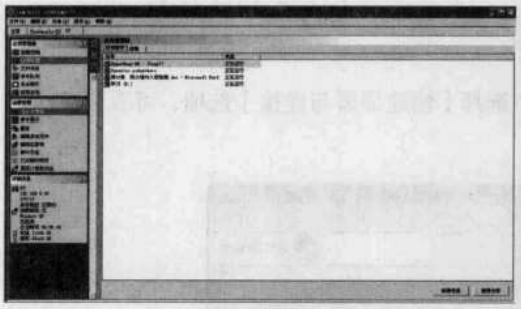


图 3-19　进程管理

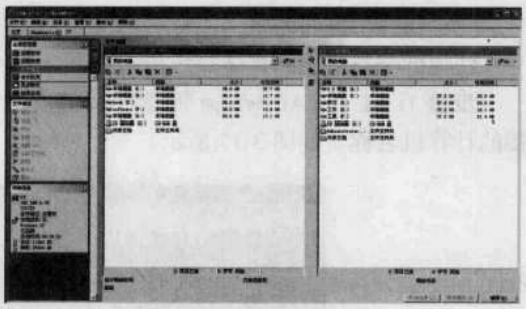


图 3-20　文件传送

4）命令队列。在【会话管理器】任务栏中选择【命令队列】选项，即可通过手动键入命令来进行操作，如图 3-21 所示。

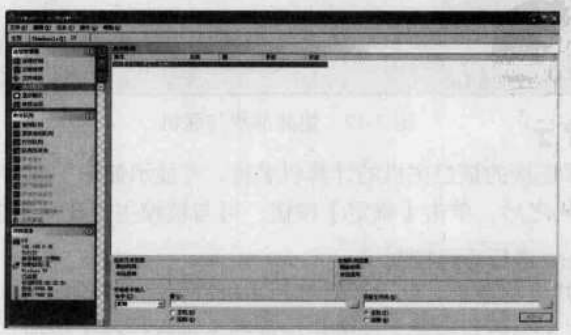


图 3-21　使用命令队列

5）显示聊天。在即时通讯软件流行的今天，大家也许会觉得远程聊天的功能有些多余，恰恰相反，在很多情况下，该功能对于双方沟通起着相当重要的作用。在【会话管理器】任务

栏中选择【显示聊天】选项后，可像在 QQ 中一样进行实时聊天，如图 3-22 所示。

6）结束会话。在【会话管理器】任务栏中选择【结束会话】选项，在显示的对话框中单击【是】按钮，即可结束主控端与被控端之间的会话，如图 3-23 所示。如果用户在联机过程中保存有会话记录，则可以在会话结束之后，双击该记录文件，浏览以前的会话过程。

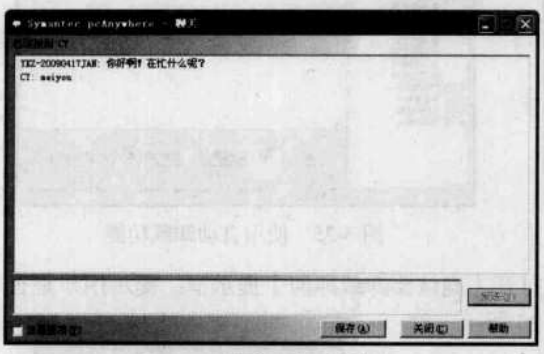


图 3-22 【聊天】对话框

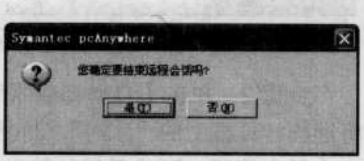


图 3-23 结束会话

第 19 招 用“冰河陷阱”揪出冰河木马

“冰河”木马实际上只是一个网络客户/服务程序。网络客户/服务模式的原理是一台主机提供服务（服务器），另一台主机接受服务（客户机）。作为服务器的主机一般会打开一个默认的端口并进行监听（Listen），如果有客户机向服务器的这一端口提出连接请求（Connect Request），服务器上的相应程序就会自动运行，来应答客户机的请求。

1．冰河陷阱概述

对于冰河，被控制端就成为一台服务器，控制端则是一台客户机，G_server.exe 是守护进程，G_client 是客户端应用程序。“冰河”木马采用标准的 C/S（Client/Server，客户/服务器）结构，包括客户端程序（G_Client）和服务器端程序（G_Server）。由于其简单易用的特点，加上强大的远程控制能力，不易被发觉且很难根除。“冰河”软件开发者开发了一款专门针对“冰河”的工具“冰河陷阱”。用来对付那些把“冰河”用在不正当地方的人。“冰河陷阱”程序主要有两大功能：一是自动清除所有版本“冰河”被控端程序；二是把自己伪装成“冰河”被控端，记录入侵者的所有操作。如果网上的一些朋友们还在受“冰河”的困扰，“冰河陷阱”无疑是最好的选择。

2．清除冰河木马

检测“冰河”木马的最直接、有效的方法就是使用“netstat –a”命令来查看目标主机的网络连接情况，如果发现端口 7626 开放，这台计算机很可能是已经中了冰河木马。反之，如果端口 7626 没有开放，但却发现有其他的可疑端口开放了，这时候就可以在目标主机中查找 Kernel32.exe 或 sysexplr.exe 文件，如果在 Windows 的系统目录中存在这两个文件，如图 3-24 所示，则表明该计算机中了“冰河”木马。清除“冰河”木马的方法有如下两种。

（1）使用控制端程序进行卸载

使用冰河自带的卸载功能很容易完成对控制端的卸载工作。具体的操作步骤如下。

步骤 1：在“冰河”的客户端程序主窗口中，选择【命令控制台】→【控制类命令】→【系统控制】菜单项，即可在打开窗口中看到【自动卸载冰河】按钮，如图 3-25 所示。

图 3-24　查找 Kernel32.exe 或 sysexplr.exe 文件

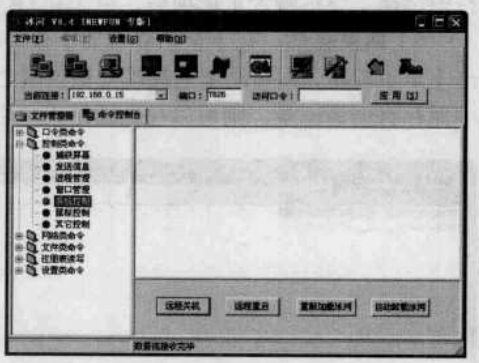


图 3-25　使用自动卸载功能

步骤 2：单击【自动卸载冰河】按钮，可打开【确认要卸载冰河】提示框，提示用户是否将远程计算机上的“冰河”彻底清除，如图 3-26 所示。单击【是】按钮，可将目标计算机中的冰河清除。

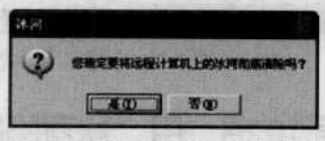


图 3-26 【确认要卸载冰河】提示框

（2）清理注册表

一旦运行了冰河服务端程序，“冰河”木马就会在 C:\Windows\system32 目录下生成 kernel32.exe 和 sysexplr.exe 并删除自身。而 kernel32.exe 会随着系统启动而自动加载运行。所以要想彻底清除冰河木马，则需要通过清理注册表才能实现。具体的操作步骤如下。

步骤 1：在“注册表编辑器”窗口中展开 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run 分支和 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices 分支后，查看两处是否有同名可疑程序名（默认安装为 kernel32.exe 或 kernel32.dll），有则删除，如图 3-27 所示。

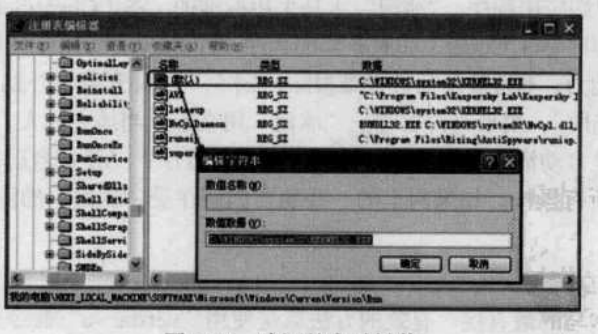


图 3-27　冰河的启动键值

步骤 2：由于冰河服务端程序有自我保护设置，用可执行文件 SYSEX PLR.EXE 关联了 TXT 文件或 EXE 文件。因此，当服务端的程序 KERNE L32.EXE 被删除后，如果打开 TXT 文件或运行 EXE 文件，就会发现 TXT 或 EXE 的关联文件 SYSEXPLR.EXE 会再次把“冰河”服务端程序 KERNEL32.EXE 安装到 Windows 的系统目录中。因此，如果想要完全清除“冰河”木马，就必须取消这种文件关联。

如果关联的为 TXT 文件，则可以采用如下步骤取消这种文件关联。

步骤 1：在 Windows 资源管理器中打开【文件夹选项】对话框，选择【文件类型】选项卡

“已注册的文件类型”列表框中的“TXT 文本文档”选项，如图 3-28 所示。

步骤 2：单击【高级】按钮，即可打开【编辑文件类型】对话框，如图 3-29 所示。

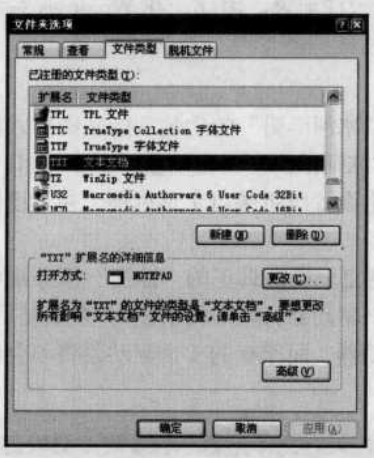


图 3-28 【编辑文件类型】对话框

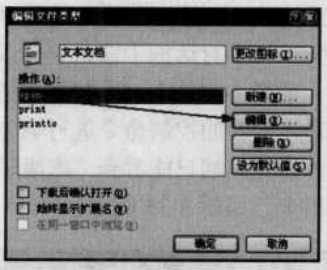


图 3-29 【文件类型】选项卡

步骤 3：在【操作】列表框中选择“Open”并单击【编辑】按钮，即可打开【编辑这种类型的操作：文本文档】对话框，如图 3-30 所示。如果“用于执行操作的应用程序”文本框中不是“Notepad.exe %1”，而是“D:\WINNT\System32\Sysexplr.exe %1”（在 Windows 9x/ 2000/XP 中类似），则把这项内容改为“Notepad.exe %1”。

如果关联的为 EXE 文件，则可以采取如下步骤取消这种文件关联。

步骤 1：打开注册表编辑器窗口并展开到 HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exe file\shell\open\command\，如图 3-31 所示。

提示 最好不要急于先修改注册表，因为如果这时候就对注册表进行修改，则“冰河”服务端程序 sysexplr.exe 的进程立刻就会把它给改回来。

图 3-30 编辑对文件类型的操作

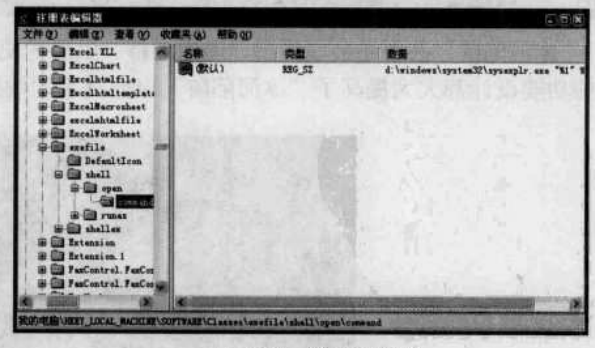


图 3-31 修改注册表

步骤 2：保持注册表管理器打开，按“Ctrl+Alt+Del”组合键并在【任务管理器】中找到 Sysexplr.exe 进程，选中后再单击【结束进程】按钮来关掉这个进程。

步骤 3：把 HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\shell\open\command\的键值由原来的 D：\WINDOWS\System32\Sysexplr.exe "%1" %*改为"%1" %*。

步骤 4：最后删除 D：\WINDOWS\System32\目录下的 Sysexplr.exe 就可以了。

应该在修改注册表后再删除可疑程序，否则对方如果将“冰河”设置为与 EXE 文件关联，那自己就连运行注册表编辑器的机会都没有了。另外，在修改注册表时可能已启动了与 EXE 文件关联的“冰河”，而“冰河”在正常关闭时将会再次修改注册表。因此，在 Windows 系统下通过使用“Ctrl+Alt+Del”组合键来重启计算机至关重要。

3．诱骗骇客

在清除完“冰河”木马之后，再来讲述一下如何利用“冰河陷阱”的伪装功能来诱捕入侵者。由于“冰河”调用了 7626 端口，因此，默认情况下“冰河陷阱”将自动监听 7626 端口，如果需改变“冰河陷阱”的监听端口，则选择【设置】→【设置监听端口】菜单项，在【设置监听端口】对话框中输入要修改的端口号，如图 3-32 所示。

选择【文件】→【打开陷阱】菜单项，“冰河陷阱”将完全模拟真正的“冰河”服务端程序对入侵者的控制命令进行响应。比如被入侵主机原有 3 个驱动器，但“冰河陷阱”在启动后，黑客在控制端只能看到“冰河陷阱”模拟出的两个硬盘驱动器，而原有的 3 个驱动器将不会显示出来，如图 3-33 所示。

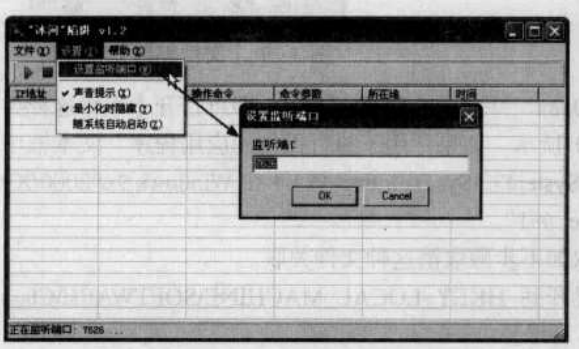


图 3-32　设置监听端口

图 3-33　仅显示两个模拟出的硬盘

小技巧　响应信息以文本方式记录在“冰河陷阱”程序文件夹下的“dat”文件夹中。读者可以通过修改这些文本文件来改变“冰河陷阱”的响应信息，以使其更具有欺骗性。

“冰河陷阱”甚至还会模拟出“虚拟屏幕”供黑客使用冰河的“查看屏幕”等功能时调用，这些功能设计都大大提高了“冰河陷阱”以假乱真的效果，如图 3-34 所示。

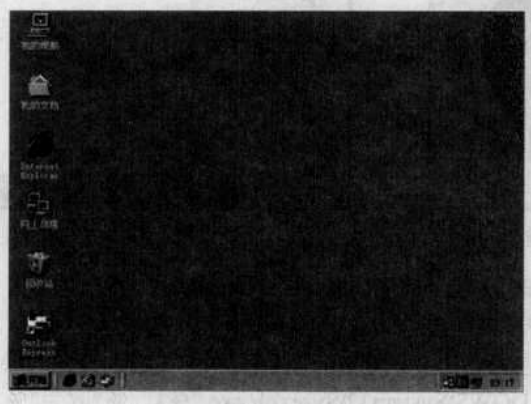


图 3-34　模拟出的屏幕显示

当有入侵者通过“冰河”客户端连接到“冰河陷阱”所伪装的服务端程序上时，可以在系统托盘中看到“冰河陷阱”图标不断闪烁报警，同时还有声音。双击图标打开“冰河陷阱”主界面，在列表中可以看到入侵者的 IP 地址、所在地以及登录密码和详细的操作过程。

此时单击【保存记录】按钮，即可将显示的入侵记录保存在磁盘上以供分析。如果还有兴趣可以和电脑的主人聊聊，则可利用“冰河”自带的【冰河信使】向其发送信息。其实“冰河”的基本操作就是这么简单，以后要接触的木马几乎都与其操作基本类似。

显然，对付“冰河”，使用“冰河陷阱”这款反控制程序，效果十分好，上述实例已充分说明了这一点。

第 20 招　用 QuickIP 进行多点控制

如果想尝试一下“一台计算机同时管理和控制多台计算机、多台计算机也同时管理一台计算机”这样的“多点”控制，QuickIP 无疑是一个很好的选择。QuickIP 可用于服务器管理、远程资源共享、网吧机器管理、远程办公、远程教育、排除故障和远程监控等多种应用场合。QuickIP 可运行在 Windows 9X/Me/NT/2000/XP 等系统上。

1．设置 QuickIP 服务器端

由于 QuickIP 是将服务器端与客户端合并在一起的，所以无论在哪台计算机中都是一起安装服务器端和客户端，这也是实现一台服务器可以同时被多个客户机控制、一个客户机也可以同时控制多个服务器的前提条件。配置 QuickIP 服务器端的具体操作步骤如下。

步骤 1：在程序安装完毕之后，需要先配置服务器端，在最后一步时只选中【立即运行 QuickIP 服务器】复选框并单击【完成】按钮，如图 3-35 所示。

步骤 2：为了实现安全的密码验证登录，QuickIP 设定客户端必须知道服务器的登录密码才能进行登录控制。因此，QuickIP 服务器端运行前会弹出一个设置密码提示框，要求立即设置一个密码，如图 3-36 所示。

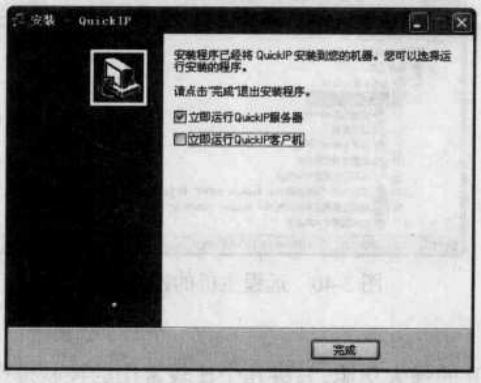


图 3-35　勾选“立即运行 QuickIP 服务器”项

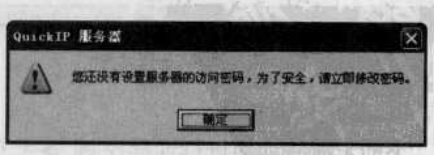


图 3-36　设置密码的提示框

步骤 3：单击【确定】按钮，即可打开【修改本地服务器的密码】对话框，在“新密码”文本框和“重输新密码”文本框中输入两次相同的密码，如图 3-37 所示。单击【确定】按钮，即可看到密码已经设定成功了。

步骤 4：此时就可以看到 QuickIP 的服务器管理窗口了，从右侧提示信息中可以看到“服务器启动成功”的字样，如图 3-38 所示。

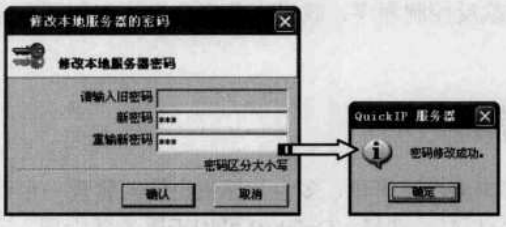


图 3-37　输入两次相同的密码

图 3-38　QuickIP 的服务器管理窗口

2．设置 QuickIP 客户端

客户端的设置就相对简单了，具体的操作步骤如下。

步骤 1：单击工具栏中的【添加主机】按钮添加服务器，在弹出对话框的“主机”文本框中输入远程计算机的 IP 地址，在“端口”和“密码”文本框中输入在服务器端设置的信息，如图 3-39 所示。

步骤 2：单击【确定】按钮，稍后就可以在客户端窗口中的“远程主机”下看到刚刚添加的 IP 地址了，单击该 IP 地址后，从展开的控制功能列表中可看到远程控制功能十分丰富，这表示客户端与服务器端的连接已经成功了，如图 3-40 所示。

图 3-39　添加远程主机

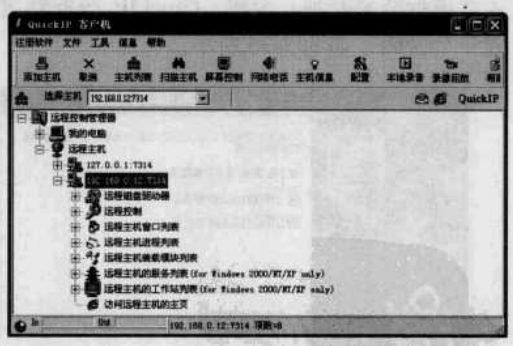


图 3-40　远程主机的控制功能列表

3．实现远程控制

下面来看看如何进行远程控制（鉴于 QuickIP 的强大功能，只讲几个比较常用的控制操作），具体操作步骤如下。

步骤 1：单击【远程磁盘驱动器】选项，即可看到远程计算机中的所有驱动器，如图 3-41 所示。在尝试单击光驱（这里为 E 盘）后，可以发现当前光驱的驱动盘符。显然，QuickIP 对远程计算机光驱具有很好的控制能力。

步骤 2：如图 3-42 所示，单击【远程控制】选项下的【屏幕控制】选项，即可在稍后弹出的窗口中看到远程计算机桌面，可以在该窗口中通过鼠标和键盘来完成对远程计算机的控制。

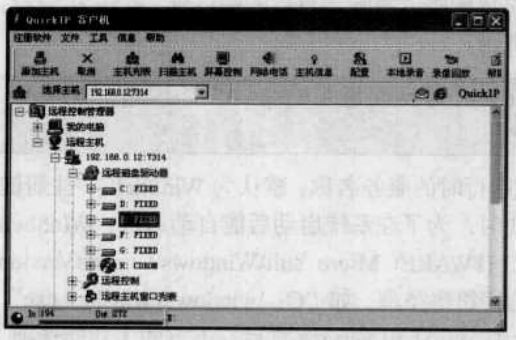


图 3-41 查看远程驱动器

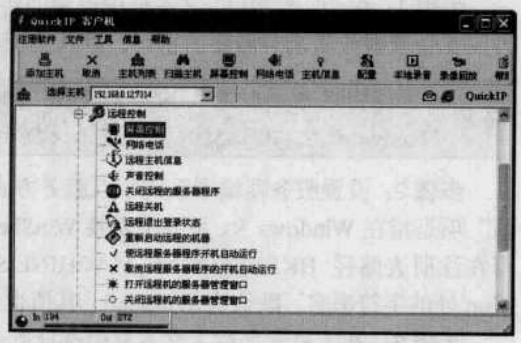


图 3-42 远程屏幕控制

步骤 3：如果远程计算机出现速度忽然缓慢等情况，则可以通过单击【远程主机进程列表】选项，查看远程计算机进程来快速诊断远程计算机的问题所在。

步骤 4：如果对远程计算机的操作已经结束，为了安全起见就应该关闭远程计算机了。单击如图 3-43 所示【远程控制】下的【远程关机】项，在弹出对话框中单击【是】按钮。

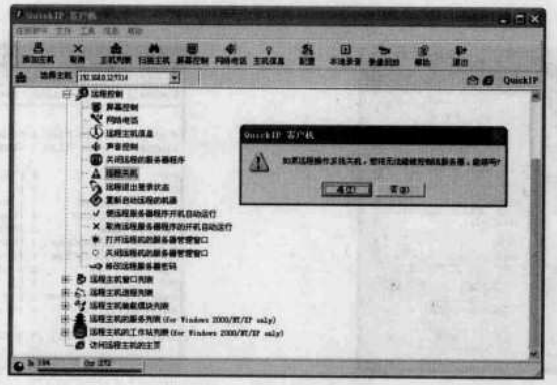


图 3-43 远程关机

限于篇幅，本书无法将该软件的远程控制功能详细讲述，但通过上述的远程控制应用，可以看出，QuickIP 远程控制功能十分强大，是网管和有远程控制需求用户的好帮手。

第 21 招 用 WinShell 实现远程控制

WinShell 是一个运行在 Windows 平台上的 Telnet 服务器软件，主程序是一个仅仅 6KB 大小的 EXE 文件，可完全独立执行而不依赖于任何系统动态链接库，尽管它体积很小，功能却十分强大，支持定制端口、密码保护、多用户登录、NT 服务方式、远程文件下载、信息自定义及独特的反 DDOS 等功能。

1. 配置 WinShell

默认状态下，定制 WinShell 的主程序会生成一个压缩过的体积很小的 WinShell 服务端，当然也可以不选择，而使用其他压缩或保护程序对生成的 WinShell 服务端进行处理。

在安装并运行 WinShell 之后，就可以根据自己要求配置服务器端了，如图 3-44 所示。

具体操作步骤如下。

步骤 1：在“监听端口”文本框中设置即将生成的服务器端运行后的端口号，默认为 5277。再设置登录服务器端时需要的密码，默认为无密码。

注意 “连接密码返回信息”选项是登录 WinShell 时要求输入密码的提示信息，默认为“Password:”，可设置为空，表示无提示信息。

步骤 2：设置服务器端在系统中以服务方式运行时的服务名称，默认为 WinShell。“注册键值”项是指在 Windows 9x 系统中安装 WinShell 时，为了在系统启动后能自动运行，WinShell 写在注册表路径 HKEY_LOCAL_MACHINE\SOFTWARE\ Micro soft\Windows\CurrentVersion \Run 处的字符串名，默认为 WinShell，其值也为字符串类型，如“C：\windows\ winshell.exe”。

步骤 3：在【显示名称】文本框中选择默认值 WinShell Service 之后，下方的【功能选项】描述项是指显示在 NT 服务列表中说明服务具体功能的字符串，默认为“Provide Windows Shell Service”。

步骤 4：勾选“自动安装”复选框后，就可以设置当 WinShell 运行时自动安装本身了。

步骤 5：设置完毕之后，单击【生成】按钮让 WinShell 的主程序生成一个压缩过的体积很小的 WinShell 服务端，稍后将自动弹出一个如图 3-45 所示的文本文件，从中可以看到生成的服务器端的配置信息。

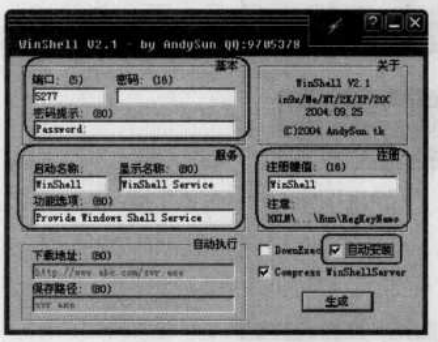


图 3-44　配置服务器端

图 3-45　生成的服务器端的配置信息

步骤 6：查看生成的服务器端文件大小，将会发现服务器端程序大小不足 6KB，如图 3-46 所示。由于这里设计 WinShell 是做一个非常小巧方便的 Telnet 服务器软件，而不是木马程序，所以 WinShell 的进程并没有隐藏，如图 3-47 所示（这里也只是在服务器上运行）。

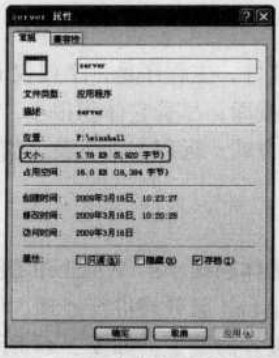


图 3-46　查看生成服务器端文件大小

图 3-47　查看 WinShell 进程

步骤 7：在配置完服务器端程序并在指定计算机中运行之后，就可以使用 Telnet 命令与远程计算机进行连接，执行“Telnet xxx.xxx.xxx.xxx 5277”并输入正确的密码（如果需要的话）后即可成功登录，命令格式为“Telnet 服务器 IP 5277”。

步骤 8：在登录后，需要在命令行中输入“?”并按 Enter 键查看可以操作的命令，如图 3-48 所示。通过反馈信息得知可以使用哪些命令。

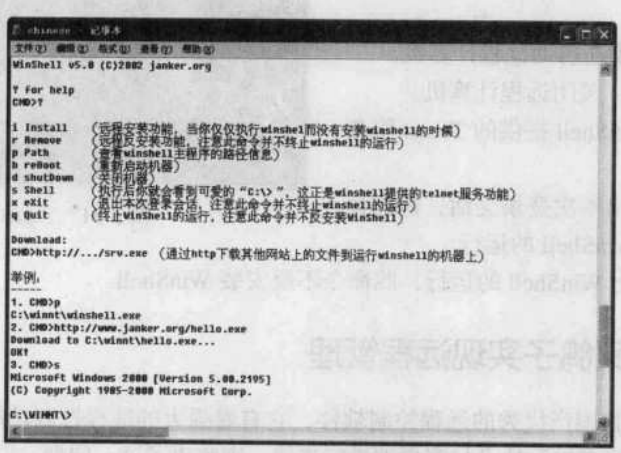


图 3-48 显示的反馈信息

显然，服务器端的制作是十分简单的，而对系统资源的占用却是很小的，加之操作命令并不复杂，因此，需要进行远程管理的朋友可尝试使用 WinShell 来完成任务。

2. 实现远程控制

当配置好 WinShell 服务器并在被控端计算机中运行后，用户可在主控端计算机中利用“命令提示符”窗口输入有关 Telnet 命令与远程计算机建立连接，并进行控制。

具体的操作方法如下。

步骤 1：将已配置好的 WinShell 服务器端复制到远程计算机中并运行。在主控端计算机“命令提示符”窗口中运行“Telnet 服务器 IP 5277”命令，即可成功连接，如图 3-49 所示。

步骤 2：执行“？”命令，即可查看 WinShell 的所有命令参数，如图 3-50 所示。

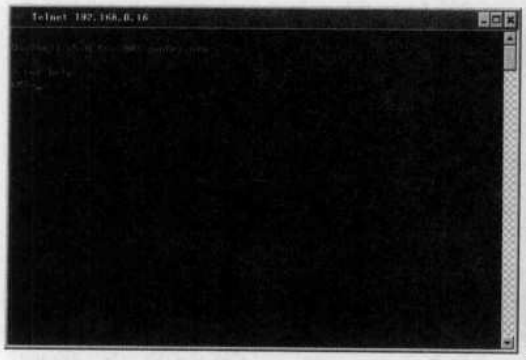


图 3-49 成功建立连接

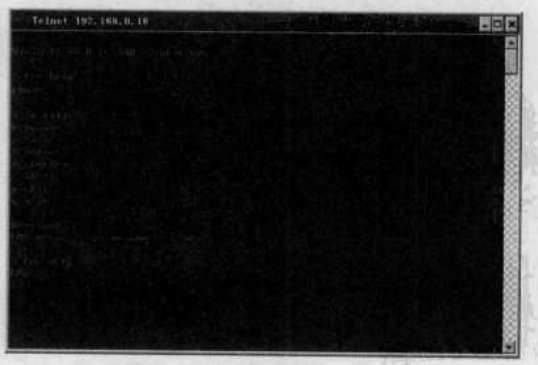


图 3-50 WinShell 命令参数

步骤 3：执行“s”命令，将显示远程计算机的盘符信息，如图 3-51 所示。此时主控端就可以控制远程计算机了。

- WinShell 命令参数及其功能如下：
- i Install：远程安装功能。
- r Remove:远程反安装功能，此命令并不终止 WinShell 的运行。
- p Path：查看 WinShell 主程序的路径信息。
- b reBoot：重新启动远程计算机。
- d shutdown：关闭远程计算机。
- s Shell：WinShell 提供的 Telnet 服务功能。
- x exit：退出本次登录会话，但此命令不终止 WinShell 的运行。
- q quit：终止 WinShell 的运行，此命令不反安装 WinShell。

图 3-51 Telnet 服务

第 22 招 用灰鸽子实现远程管理

灰鸽子作为一款国产优秀的远程控制软件，它有着强大的远程控制功能，“灰鸽子”远程控制软件使用“反弹端口”技术与客户端进行连接，则解决了这一问题，同时也解决了无法了解主机动态 IP 地址的问题，使得局域网内部的计算机也可以进行远程控制。

1．生成木马的服务端

“灰鸽子”分为“客户端”和“服务端”两个部分，它与“冰河”不同的是其“服务端”需要在使用前通过“客户端”来配置生成。具体的操作步骤如下。

步骤 1：将下载的压缩包解压后，双击“灰鸽子 2008.exe”程序，即可进入其操作界面，如图 3-52 所示。

步骤 2：单击【配置服务程序】按钮，即可打开【服务器配置】对话框。在“自动上线设置”标签中输入 IP，IP 通知 URL 地址和网页、DNS 解析域名或固定 IP，如图 3-53 所示。

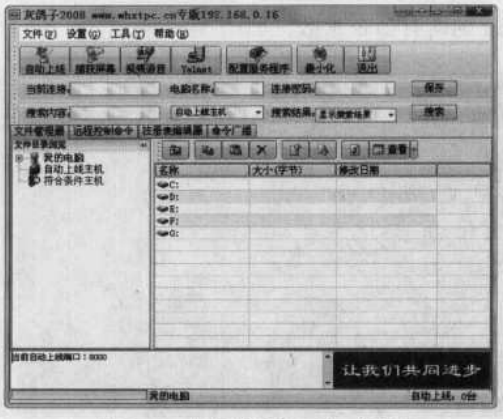


图 3-52 “灰鸽子 2008”主窗口

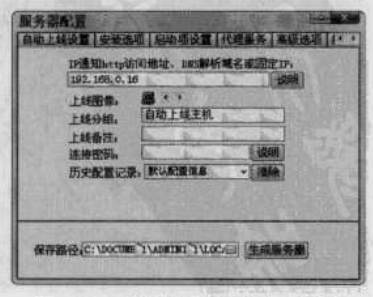


图 3-53 【服务器配置】对话框

步骤 3：在“安装选项”标签中可选择运行服务器程序后的有关选项，如图 3-54 所示。

步骤 4：在“启动选项”标签中可选择是否将服务端程序信息写入系统注册表等选项中，

如图 3-55 所示。在“保存路径”文本框中输入生成服务端的保存位置，单击【生成服务器】按钮，即可生成灰鸽子的服务端程序，如图 3-56 所示。

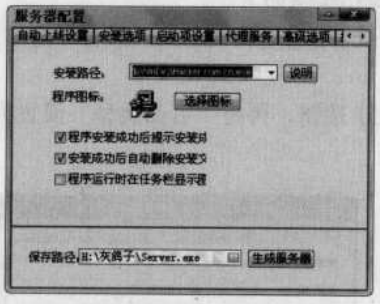


图 3-54 “安装选项”标签页

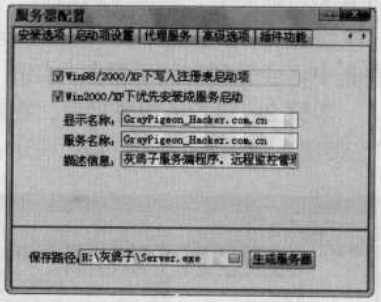


图 3-55 “启动选项”标签页

步骤 5：将生成的服务器程序复制到被控端计算机中并运行。如果在“安装选项”标签中选取相关的复选框，则安装成功后会给出提示，如图 3-57 所示。

图 3-56 提示信息

图 3-57 安装成功提示

2. 查看控制效果

将这个程序在要控制的计算机上运行，当这台计算机与 Internet 连接或通过局域网中其他计算机与 Internet 连接时，就会自动与“客户端”连接，就可以看到远程计算机的 IP 地址已经显示在了“自动上线主机”下了，如图 3-58 所示。

连接成功后可以在远程主机上执行命令，对远程主机进行文件管理，上传、下载文件，修改远程主机的注册表等操作了，如图 3-59 所示。显然，如果将灰鸽子用于远程管理，功能将十分强大，可以很好地满足远程管理的需要。由于“灰鸽子”强大的远程管理功能，加上“服务端”运行过于隐蔽，使得许多人将它用于非法控制别人计算机了。

图 3-58 与被控端连接

图 3-59 对文件进行管理

3. 禁止灰鸽子服务

灰鸽子服务器端在运行后将会自动在系统服务中生成一个名为“Hgzserver”的服务，如果将其关闭则会中止灰鸽子的运行。禁止灰鸽子服务的具体操作步骤如下。

步骤 1：在【运行】对话框的运行栏中输入“Services.msc”命令，即可打开“服务”窗口，在其中将会看到灰鸽子服务，如图 3-60 所示。

步骤 2：双击该服务项后，在属性对话框中单击【停止】按钮，再将“启动类型”设置为“已禁用”项即可，如图 3-61 所示。

图 3-60 “服务”窗口

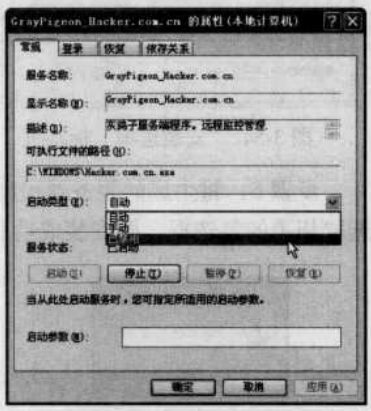


图 3-61 【属性】对话框

4. 灰鸽子的手工清除

灰鸽子远程监控软件分为客户端和服务端两部分，黑客通过在客户端进行配置，生成一个服务端程序之后，再通过多种渠道来传播这个服务端（俗称种植木马），下面介绍两种清除灰鸽子的方法。

（1）手工检测

因为灰鸽子拦截了 API 调用，在正常模式下服务端程序文件和其注册的服务项均被隐藏，也就是说，用户即使设置了“显示所有隐藏文件”也看不到它们。此外，灰鸽子服务端的文件名也是可以自定义的，这都给手工检测带来了一定困难。

其实，无论自定义的服务器端文件名是什么，一般都会在系统安装目录下生成一个以“_hook.dll”结尾的文件。通过这一点，即可较为准确地手工检测出灰鸽子的服务端。由于正常模式下灰鸽子会隐藏自身，因此，检测灰鸽子的操作一定要在安全模式下进行。

具体的操作步骤如下。

步骤 1：在系统重启并进入 Windows 系统启动画面之前，按“F8”键（或在启动系统时按住“Ctrl”键不放），在启动选项菜单中选择“Safe Mode”启动项或“安全模式”启动项。

步骤 2：由于灰鸽子的文件本身具有隐藏属性，因此要设置 Windows 显示所有文件。在“我的电脑”窗口中选择【工具】→【文件夹选项】菜单项，即可打开【文件夹选项】对话框，在“查看”选项卡中取消勾选“隐藏受保护的操作系统文件”复选框，如图 3-62 所示。

步骤 3：选择【开始】→【搜索】→【文件或文件夹】菜单项，即可打开“搜索结果”窗口，在“文件名称”文本框中输入“*_hook.dll”后，搜索位置选择 C 盘，如图 3-63 所示。

步骤 4：单击【搜索】按钮，即可在 Windows 目录（不包含子目录）下发现灰鸽子的木马程序文件，如 Huigezi_Hook.dll 文件。

步骤 5：根据灰鸽子原理分析可知，如果 Hmage_Hook.dll 是灰鸽子的文件，则在安装目录下还会有 Huigezi.exe 和 Huigezi.dll 文件。打开 Windows 系统的安装目录，果然发现这两个文件，同时还有一个用于记录键盘操作的 HuigeziKey.dll 文件。

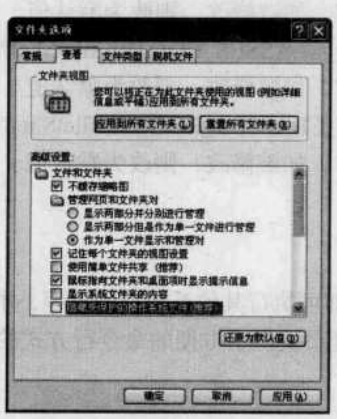


图 3-62 【文件夹选项】对话框

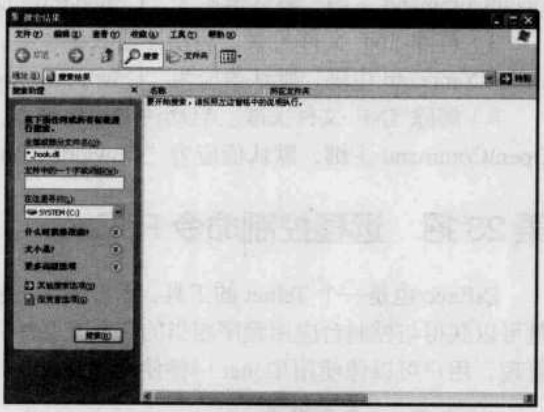


图 3-63 【搜索结果】窗口

经过上述操作之后，基本上均可确定这些文件是灰鸽子服务端程序，所以用户只要手动清除这些程序就可以了（为防止操作失误而引起的麻烦，清除前一定要做好备份）。

（2）手工清除

经过上面的分析，清除灰鸽子就很容易了。清除灰鸽子仍然要在安全模式下操作，主要有两步：清除灰鸽子的服务和删除灰鸽子程序文件。

清除灰鸽子服务的具体操作步骤如下。

步骤 1：在【注册表编辑器】窗口中展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControl Set\Services 注册表项。

步骤 2：选择【编辑】→【查找】菜单项，即可打开【查找】对话框，在“查找目标”文本框中输入“huigezi.exe”，如图 3-64 所示。

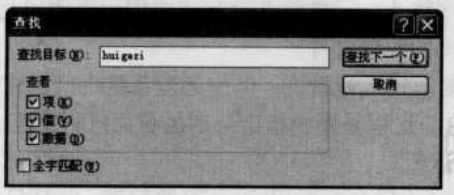


图 3-64 【查找】对话框

步骤 3：单击【查找下一个】按钮，即可找到“灰鸽子”木马的服务项，将其所关联的整个注册表项删除。

删除灰鸽子程序文件非常简单，只需在安全模式下，删除 Windows 文件夹中 Huigezi.exe、Huigezi.dll、Huigezi_Hook.dll 以及 HuigeziKey.dll 文件后重启系统即可。至此，灰鸽子服务端程序就被彻底清除干净了。

5. 解除关联

“灰鸽子”可以设置 4 种文件关联：EXE 文件关联、TXT 文件关联、INI 文件关联、INF 文件关联、INF 文件关联等。解除关联的方法如下。

1）解除 EXE 文件关联。启动注册表编辑器，找到 HKEY_CLASSES_ROOT\Exefile\shell\Open\Command 主键，查看键值是不是系统默认的“%1%*”，如被修改则改为默认值。

2）解除 TXT 文件关联。启动注册表编辑器，找到 HKEY_CLASSES_ROOT\Txtfile\Shell\Open\Command 主键，默认值应为“C:\windows\notepad.exe%1”，如被修改，则改为默认值。

3）解除 INI 文件关联。启动注册表编辑器，找到 HKEY_CLASSES_ROOT\Inifile\Shell\Open\Command 主键，默认值应为“C:\windows\notepad.exe%1”，如被修改，则改为默认值。

4）解除 INF 文件关联。启动注册表编辑器，找到 HKEY_CLASSES_ROOT\Inffile\Shell\Open\Command 主键，默认值应为“C:\windows\notepad.exe%1”，如被修改，则改为默认值。

第 23 招　远程控制命令 PsExec

PsExec 也是一个 Telnet 的工具，无需手动安装客户端软件即可执行其他系统上的进程，并且可以获得与控制台应用程序相当的完全交互性。PsExec 为管理员提供了方便的命令行方式的管理，用户可以像使用 Telnet 一样使用它。

1．PsExec 命令概述

安装 PsExec 时需将 PsExec 复制到可执行路径，输入“psexec”可显示其使用语法。

Psexec[\\computer[,computer2[,...]|@file][-u user [-p psswd]][-n s][-l][-sl-e][-x][-i [session]][-c [-fl-v]][-w directory][-d][-][-a n,n,...] cmd [arguments]

- Computer：指示 PsExec 在指定的一台或多台计算机上运行应用程序。如果省略计算机名称，则 PsExec 将在本地系统上运行应用程序；如果输入计算机名称“*”，则 PsExec 将在当前域中的所有计算机上运行应用程序。
- @file：指示 PsExec 在指定的文本文件中列出的每台计算机上运行命令。
- -a：用逗号分隔可以运行应用程序的处理器，CPU 编号最小为 1。例如，要在 CPU 2 和 CPU 4 上运行应用程序，请输入：“-a 2,4”。
- -c：将指定的程序复制到远程系统以便执行。如果省略此选项，则应用程序必须位于远程系统上的系统路径中。
- -d：不等待应用程序终止。只能对非交互式应用程序使用此选项。
- -e：不加载指定帐户的配置文件。
- -f：将指定的程序复制到远程系统，即使远程系统中已存在该文件。
- -i：运行程序，使它与远程系统中指定会话的桌面进行交互。如果未指定会话，则进程将在控制台会话中运行。
- -l：以受限用户身份（去除 Administrators 组的权限，并且只允许使用分配给 Users 组的权限）运行进程。在 Windows Vista 上，此进程将以“低完整性”运行。
- -n：指定与远程计算机连接的超时（秒）。
- -p：指定用户名的密码（可选）。如果省略此选项，系统将提示您输入隐藏密码。
- -s：在系统帐户中运行远程进程。
- -u：指定用于登录远程计算机的可选用户名。
- -v：仅在指定文件具有更高版本号或该文件比远程系统上的文件新时复制该文件。
- -w：设置进程的工作目录（相对于远程计算机）。
- -x：在 Winlogon 桌面上显示 UI（仅限于本地系统）。
- -priority：指定–low、-belownormal、-abovenormal、-high 或-realtime 按不同优先级运行

进程。

- program：要执行的程序的名称。
- arguments：要传递的参数（注意文件路径必须是目标系统中的绝对路径）。

对于其名称中含有空格的应用程序，可在其两侧加引号，如 psexec \\marklap "c:\long name \app.exe"。按【Enter】键时仅将输入内容传递到远程系统。按“Ctrl+C”组合键可终止远程进程。如果省略用户名，则远程进程将以执行 PsExec 时所使用的相同账户运行。

2．应用实战

在对 Psexec 工具有了进一步了解后，下面讲述使用 Psexec 进行各种操作时的具体过程。

步骤 1：进入 Telnet 操作状态。若想要用 Telnet 一样在远程系统上执行命令，则输入“psexec \\192.168.0.16 -u administrator -p "shining0924" cmd”命令，便可在本地机上打开远程主机 192.168.0.16 上的命令行 Shell，如图 3-65 所示。在该命令行 Shell 中输入的命令会在远程主机上直接执行，就实现了与 Telnet 登录同样的功能。”

步骤 2：执行本地程序。如果想要远程机执行本地 C:\rav2009.exe 文件，则可以输入“Psexec \\192.168.0.16 -u administrator -p shining0924 –c c:\rav2009.exe”命令即可。如图 3-66 所示。

图 3-65　进入 Telnet 操作状态

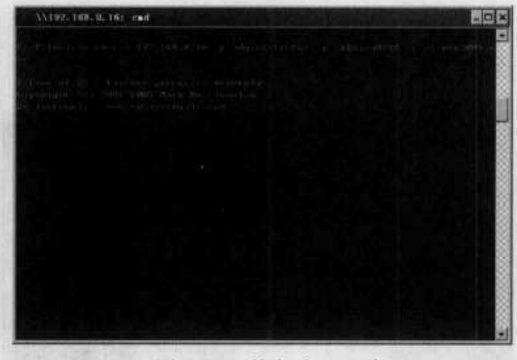


图 3-66　执行本地程序

步骤 3：启动远程服务。如果想要让远程机器执行本地上的 TFTP 服务端，（假设 TFTP 服务端在本地 C:\TFTP.exe），则应输入“psexec \\远程机器 ip -u administrator -p shining0924 –c c:\tftp32.exe -d”命令。

第 24 招　实现 Serv-U 远程控制

Serv-U 除拥有其他 FTP 服务器端同类软件所具备的大部分功能外，还支持断点续传、带宽限制、远程管理、远程打印、虚拟主机等。当用户使用 Serv-U 创建自己的 FTP 服务器后，将自己的一些学习资料放上去，只要能够联网，就可以随时随地进行网上信息的使用了。

1．配置服务端

下载 Serv-U 软件包并解压后，还需要对其进行相应地配置，才可以建立自己的 FTP 服务器。具体配置 Serv-U 的操作步骤如下。

步骤 1：在如图 3-67 所示中双击“Serv-U-Tray”应用程序图标，即可进入“Serv-U 管理控制台”主窗口，在其中选择任意一项进行相应设置，如图 3-68 所示。

步骤 2：单击【新建域】按钮，即可打开【域向导-步骤 1】对话框，在“名称”文本框中

输入新建域的名称，可以随便起名字，反正是内网共享，无须域名转换；在“说明”框中根据需要输入更多详细信息，如图 3-69 所示。

图 3-67 “Serv-U 解压后的文件”窗口

图 3-68 “Serv-U 管理控制台”主窗口

步骤 3：单击【下一步】按钮，即可打开【域向导-步骤 2】对话框，在其中指定用户访问该域所用的协议及端口，如图 3-70 所示。

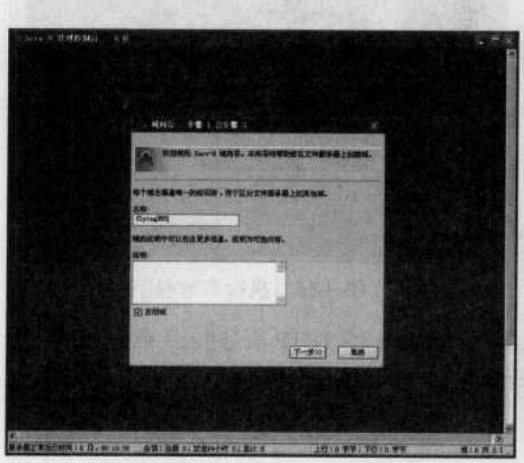


图 3-69 【域向导-步骤 1】对话框

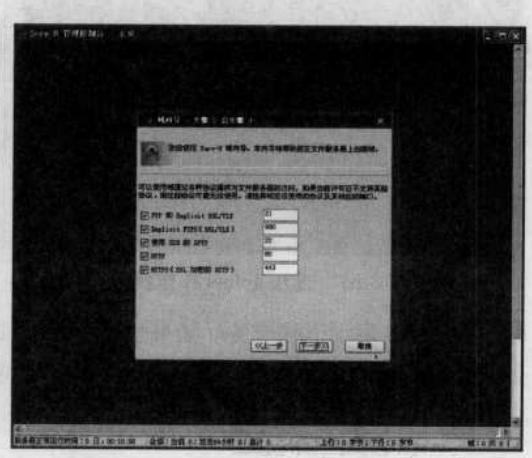


图 3-70 【域向导-步骤 2】对话框

提示 标准文件共享协议是 FTP（文件传输协议），它运行于默认端口 21。然而，任何这些端口值都可更改为自己所选择的数值。若在非默认端口上运行服务器，推荐使用 1024 以上的端口。

步骤 4：单击【下一步】按钮，即可打开【域向导-步骤 3】对话框，在“IP 地址”框中输入指定用于连接该域的物理地址（如：192.168.0.16）。通常是用户指定的 IP 地址，用于在 Internet 上查找的服务器。大多数家庭用户可保留该选项空白，以使 Serv-U 使用计算机上的任何可用 IP 地址，如图 3-71 所示。

步骤 5：单击【完成】按钮，即可弹出“创建用户”提示框，访问是否创建用户账户等信息，如果不需要创建，选择【否】按钮，如图 3-72 所示。

步骤 6：单击【是】按钮，即可弹出“是否要使用向导创建用户”提示框，如图 3-73 所示。

单击【是】按钮，即可打开【用户向导-步骤 1】对话框，在“用户名”文本框中输入账户的唯一用户名。连接域时使用该用户名开始验证过程，用户名对于该域必须唯一，但服务器上其他域可能有账户拥有同样用户名。要创建匿名账户需指定用户名为“anonymous”或“ftp”，如图 3-74 所示。

图 3-71 【域向导-步骤 3】对话框

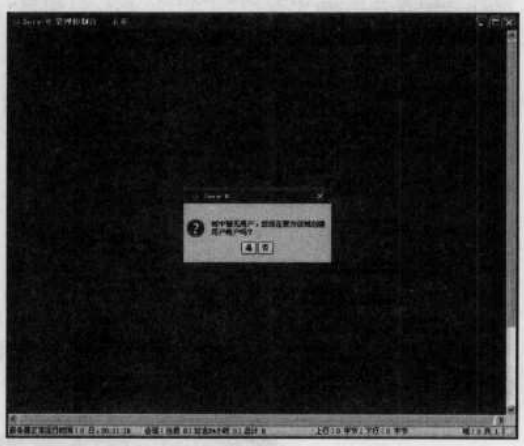


图 3-72 “创建用户”提示框

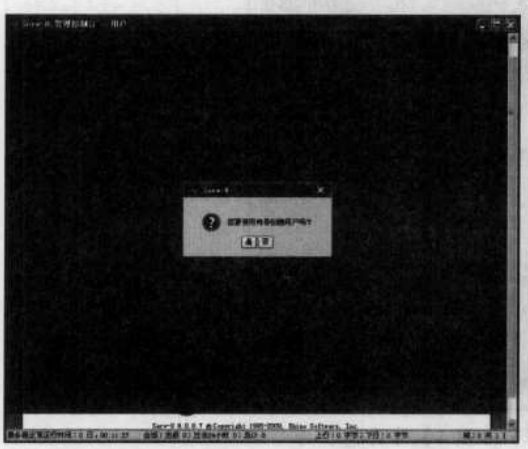


图 3-73 “是否要使用向导创建用户”提示框

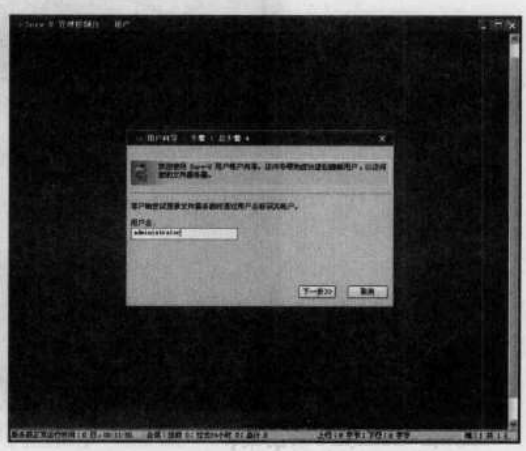


图 3-74 【用户向导-步骤 1】对话框

步骤 7：单击【下一步】按钮，即可打开【用户向导-步骤 2】对话框，在“密码”文本框中输入访问该账户时指定的密码。当用户连接域时，密码是验证用户身份所需的第二条信息。如果有人要连接该域，必须知道第一步中指定的用户名以及此密码。密码可以为空，但将导致知道用户名的任何人都能访问域，如图 3-75 所示。

步骤 8：单击【下一步】按钮，弹出【用户向导-步骤 3】对话框，用于指定账户的根目录，根目录是登录成功时用户账户在服务器硬盘（或可访问的网络资源）上所处的位置。实质上，它是用户账户在服务器上收发文件时用户希望它使用的位置。单击右侧的【浏览】按钮，则将转到硬盘上的某个位置，或手动输入某位置。如果锁定用户至根目录，他们就不能访问其根目录结构之上的文件或文件夹。此外，根目录的真正位置将被屏蔽而显示为"/"，如图 3-76 所示。

图 3-75 【用户向导-步骤 2】对话框

图 3-76 【用户向导-步骤 3】对话框

步骤 9：单击【下一步】按钮，将打开【用户向导-步骤 4】对话框，在其中设置访问的权限（如选择“只读访问”），如图 3-77 所示。

图 3-77 【用户向导-步骤 4】对话框

步骤 10：最后单击【完成】按钮，即可完成整个服务端的配置。

2. 配置客户端

下面再来看看如何详细设置自己的 Serv-U，具体的操作步骤如下。

步骤 1：在“Serv-U 管理控制台-用户”窗口中选择需详细设置的用户，如图 3-78 所示。

步骤 2：单击列表下方的【添加】按钮，即可弹出【用户属性】对话框，在其中根据需要进行相应地设置，如图 3-79 所示。

步骤 3：单击群组列表下方的【添加】和【删除】按钮，分别可以为用户添加更多群组或将用户从选中的群组中删除，如图 3-80 所示。

步骤 4：欢迎消息是用户成功登录后，通常发送给 FTP 客户端的消息。该功能不适用于通过 SSH2（Secure Shell）协议的 SFTP（Secure File Transfer Protocol，安全文件传送协议）登录的用户，因为该协议无法定义将一般纯文本信息发送给用户的方式，如图 3-81 所示。

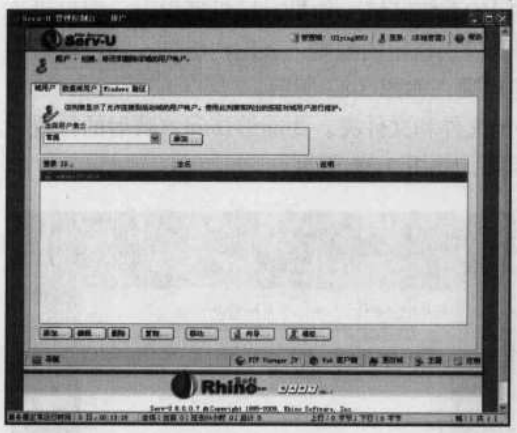


图 3-78 “Serv-U 管理控制台-用户”窗口

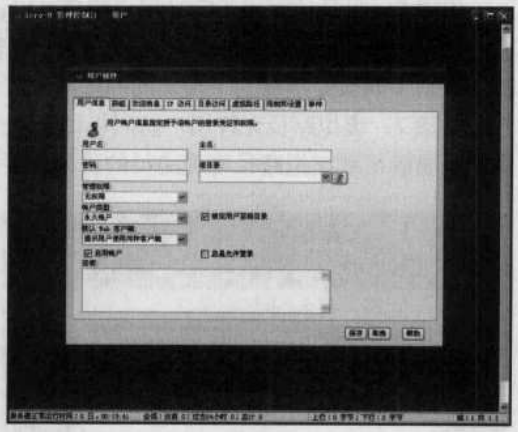


图 3-79 【用户属性】对话框

图 3-80 “群组”选项页面

图 3-81 “欢迎消息”选项页面

步骤 5：IP 访问规则是用户验证的一种补充形式，可限制登录特定 IP 地址、IP 地址群甚至域。当客户端向服务器表明身份时，对 USER 命令响应应用群组和用户级别的 IP 访问规则，如图 3-82 所示。

图 3-82 “IP 访问”选项页面

步骤 6：目录访问用于定义用户账户可以访问的系统区域。如果对域级别指定，则仅供该域内的用户继承。继承的传统应用规则为，在较低级别指定的规则（如用户级别）可以覆盖在较高级别（如服务器级别）指定的冲突或重复的规则，如图 3-83 所示。

步骤 7：虚拟路径允许用户访问根目录以外的文件和文件夹。为能够访问该映射的位置，用户需要满足对虚拟路径物理路径的目录访问规则，如图 3-84 所示。

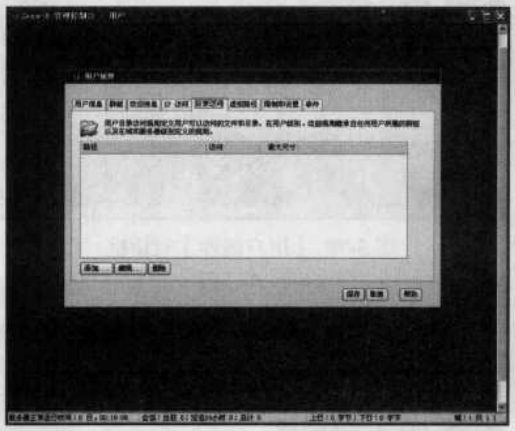


图 3-83 “目录访问”选项页面

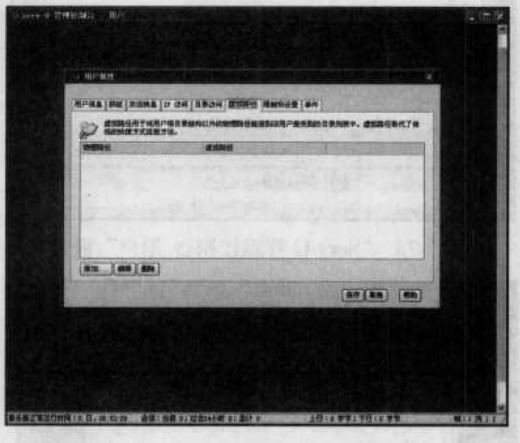


图 3-84 “虚拟路径”选项页面

步骤 8：Serv-U 提供了高级选项用来定制它的使用方式以及将限制和定制设置应用于整个 Serv-U 内的用户、群组、域和服务器的方法。Serv-U 内的限制和设置分为 5 类：连接、密码、目录列表、数据传输和高级，如图 3-85 所示。

步骤 9：Serv-U 允许使用事件处理，执行各种由选定事件列表所触发的操作，如图 3-86 所示。

至此，Serv-U 的配置就全部完成了，如果有防火墙，对防火墙进行相应设置，允许 Serv-U 访问网络，开放相应端口（默认是 21）就可以正常使用该账户了。

图 3-85 “限制和设置”选项页面

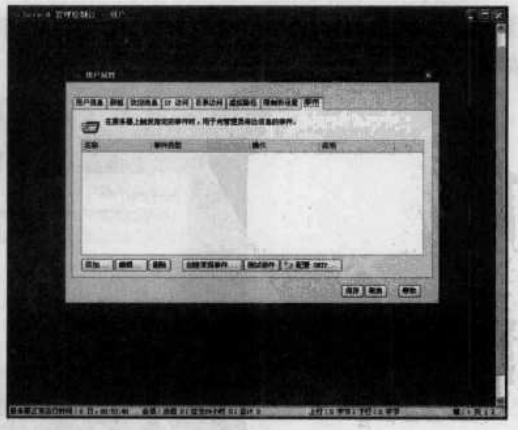


图 3-86 “事件”选项页面

当在自己网站或在网站所在内网中进行管理维护操作时，不要使用域名作服务器地址，尽量使用网站计算机的内网 IP 地址来代替，以避免使用端口映射，便于提高速度。

第 25 招 用 SyGate 突破上网封锁

Sygate Office Network 是局域网共享一至四个 MODEM 访问 Inernet 的软件，基于 SyGate 核心功能，主要为商业网络提供网络连接共享，支持 Modem/ISDN/Cable Modem/ASDL、带宽分配、用户和组的管理、增强的记录分析及设置黑白名单控制用户访问 Inernet。

1．配置 SyGate 服务器

在使用之前应对 SyGate 服务器进行相应配置，具体的操作步骤如下。

步骤 1：在能够上网的计算机上安装 SyGate 的服务器端。运行 SyGate 安装程序之后，会弹出一个【安装设置】对话框，询问是选择服务器模式还是客户端模式，如图 3-87 所示。

注意 由于局域网中所有的电脑都要通过主机才能连接到 Internet，所以这里要选择服务器模式并输入计算机名称。

步骤 2：在完成软件的安装之后，SyGate 会自动进行“网络诊断”并自动获取主机的 IP 地址、网关、DNS 地址等网络信息，从而免去了普通用户自己设置的烦恼，如图 3-88 所示。

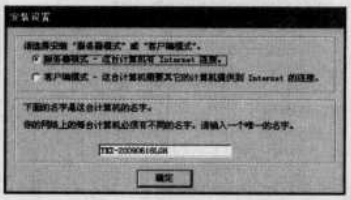


图 3-87 【安装设置】对话框

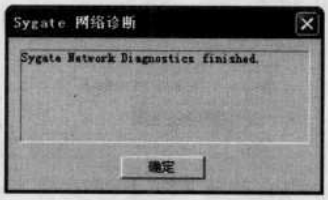


图 3-88 自动进行网络诊断

步骤 3：在【SyGate 网络诊断】对话框中单击【确定】按钮，即可弹出一个【指定 NAT 网关 IP】对话框，如图 3-89 所示。如果自动生成的 IP 和局域网内其他电脑所使用 IP 不冲突，单击【是】按钮，即可指定 NAT 网关 IP。

提示 在其中显示了 SyGate 根据所生成的虚拟网卡而分配的一个用来模拟 NAT 网关的 IP 地址（默认网关 IP 地址是 192.168.0.1，也可改为其他值，只要不发生冲突就行，但客户端上的设置也必须随之改动），如果该地址和局域网内的其他电脑所使用的 IP 地址不冲突，一般保持默认设置即可。

步骤 4：由于上述操作只是设置了 SyGate 的虚拟网卡地址，并不会和真实的网卡设置产生冲突，因此完全不必担心网卡 IP 地址会被更改。

步骤 5：SyGate 安装完毕并重启系统之后，需要单击 SyGate 主窗口中的【开始】按钮，让 SyGate 的 Internet 连接共享功能激活，如图 3-90 所示。

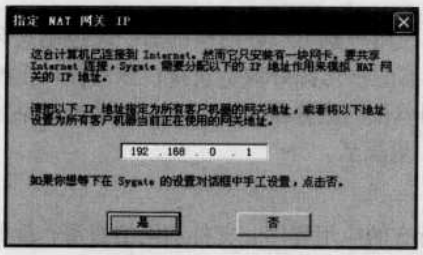


图 3-89 【指定 NAT 网关 IP】对话框

图 3-90 SyGate 主窗口

2．配置 SyGate 客户端

当服务器端设置完毕之后，就可以对客户端的电脑进行设置了，具体的操作步骤如下。

步骤 1：在客户端计算机上右击“网上邻居”图标，从快捷菜单中选择【属性】选项，即可打开“网络连接”窗口。右击【本地连接】图标项，在快捷菜单中选择【属性】选项，即可打开【本地连接 属性】对话框，如图 3-91 所示。

步骤 2：在其中选择【Internet 协议（TCP/IP）】选项并单击【属性】按钮，即可打开【Internet 协议（TCP/IP）属性】对话框。由于 192.168.0.1 已经分配给 SyGate 网关，因此，只要将客户端的 IP 地址设置为 192.168.0.2 ~ 192.168.0.254 之间的任何一个 IP 地址即可（不能和已有的 IP 地址冲突）。

如 IP 地址为 192.168.0.2，子网掩码为 255.255.255.0，则默认网关必须为 SyGate 网关的地址 192.168.0.1，DNS 服务器可以使用 SyGate 网关地址，也可以使用单位的 DNS 服务器地址，如图 3-92 所示。

图 3-91 【Internet 属性】对话框

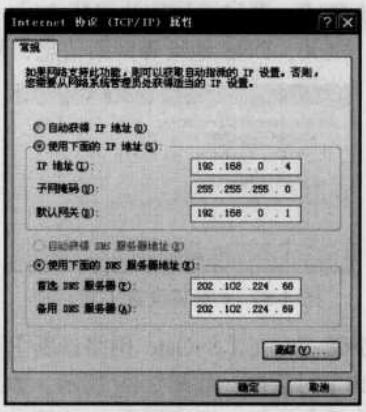


图 3-92 设置 SyGate 网关地址

在进行上述设置并重启系统之后，SyGate 的服务器端和客户端就会自动运行了。在客户端单击【拨号】按钮，自己的电脑就可以顺利地访问 Internet 了。由于 SyGate 基于 NAT（网络地址转换），因此，对电子邮件和浏览器等都不需要进行任何特殊的设置。

第 26 招 Windows XP 远程桌面连接与协助

远程桌面采用了一种类似 Telnet 的技术，远程桌面连接组件是微软公司从 Windows 2000 Server 开始提供的，用户只需通过简单设置即可开启 Windows XP、Windows 2003 和 Windows Vista 系统下的远程桌面连接功能。

当某台计算机开启了远程桌面连接功能后，其他用户就可以在网络的另一端控制这台计算机了，可以在该计算机中安装软件、运行程序，所有的一切都好像是直接在该计算机上操作一样。通过该功能网络管理员可以在家中安全的控制单位的服务器，而且由于该功能是系统内置的，所以比其他第三方远程控制工具使用更方便、更灵活。

1．Windows XP 系统的远程桌面连接

远程桌面可让用户可靠地使用远程计算机上所有的应用程序、文件和网络资源，就如同用户本人就坐在远程计算机的面前一样，不仅如此，本地（办公室）运行的任何应用程序在用户

使用远程桌面（家、会议室、途中）连接后仍会运行。

在 Windows XP 系统中保留了远程桌面连接功能，以实现专家远程控制，帮助用户解决计算机的问题。如果需要实现远程桌面连接功能，可按如下操作进行设置。

步骤 1：选择【开始】→【所有程序】→【控制面板】菜单项，即可打开“控制面板”窗口，如图 3-93 所示。

步骤 2：双击“系统”图标，即可打开【系统属性】对话框，在“远程”选项卡中勾选“允许用户远程连接到此计算机”复选框（若想成功建立远程控制连接，则对方也应勾选此复选框）。单击【选择远程用户】按钮，即可添加那些需要进行远程连接但还不在本地管理员安全组内的任何用户，如图 3-94 所示。

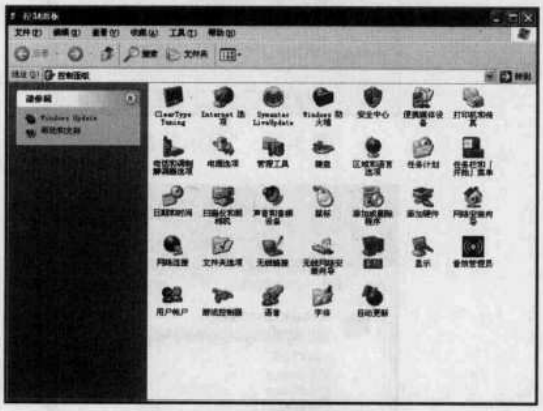


图 3-93 “控制面板”窗口

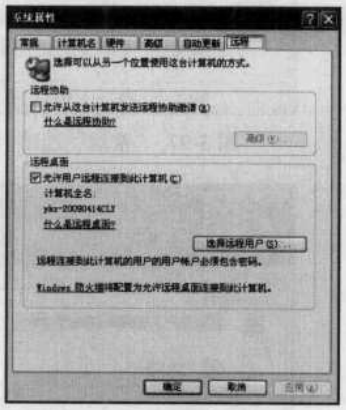


图 3-94 【系统属性】对话框

步骤 3：选择【开始】→【所有程序】→【附件】→【远程桌面连接】菜单项，即可打开【远程桌面连接】对话框，如图 3-95 所示。单击【选项】按钮，即可将有关选项设置项展开，如图 3-96 所示。

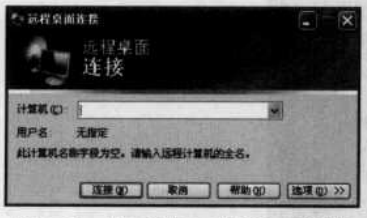


图 3-95 【远程桌面连接】对话框

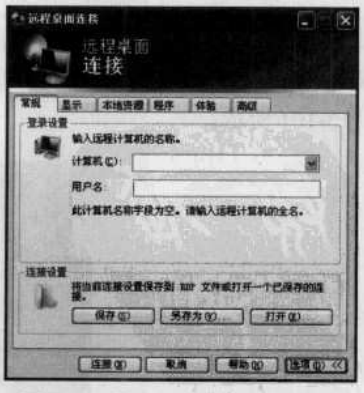


图 3-96 设置远程桌面连接选项

步骤 4：选择“常规”选项卡，在“登录设置”选项组的“计算机”文本框中输入要进行远程桌面连接的计算机名称；在“用户名”文本框中输入登录使用的用户名；若用户要保存凭证，可勾选“允许我保存凭证”复选框，如图 3-97 所示。

步骤 5：在“显示”选项卡中可设置远程桌面显示的大小、颜色质量，如图 3-98 所示。在

“本地资源”选项卡中可设置远程计算机的声音及会话中使用的设备和资源，如图 3-99 所示。在“体验”选项卡中可选择远程连接的速度（建议选择局域网<10mbps 或更高>），如图 3-100 所示。

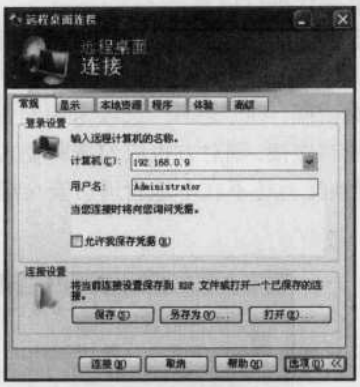


图 3-97 “常规”选项卡

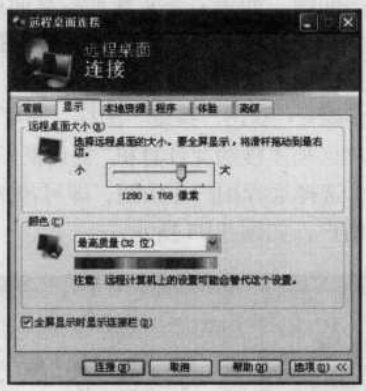


图 3-98 “显示”选项卡

图 3-99 “本地资源”选项卡

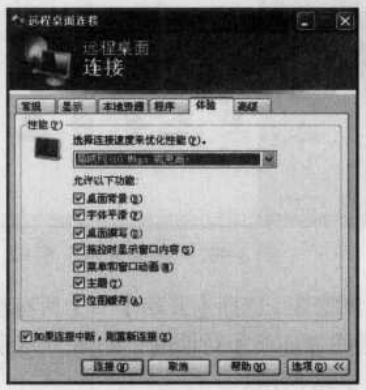


图 3-100 “体验”选项卡

步骤 6：单击【连接（N）】按钮，即可进行远程桌面连接。同时将弹出【登录到 Windows】对话框，在“用户名”文本框中输入登录用户的名称；在“密码”文本框中输入登录密码，如图 3-101 所示。

图 3-101 【登录到 Windows】对话框

步骤 7：单击【确定】按钮，即可登录到远程计算机桌面，此时用户在远程桌面上的操作与在本机上操作无任何差别，如图 3-102 所示。在登录成功之后，就可以使用该远程桌面中的程序进行各项操作了。如这里以打开“我的电脑”为例，如图 3-103 所示。

图 3-102　成功登录到远程计算机桌面

步骤 8：需要断开远程桌面连接时，只需在本地计算机中单击远程桌面连接窗口上的【关闭】按钮，在弹出的提示信息框中单击【确定】按钮，如图 3-104 所示。

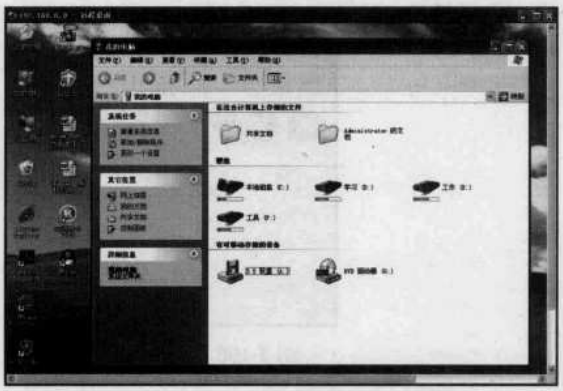


图 3-103　打开远程计算机中的“我的电脑”

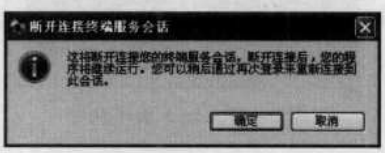


图 3-104【断开连接终端服务会话】对话框

注意　登录远程计算机的用户必须设置密码，否则将不能正常使用远程桌面连接功能。另外，进行远程桌面连接时远程计算机用户将不能登录，若登录则断开远程桌面连接。

2. Windows XP 系统远程关机

Windows XP 默认只有 Administrators 组的用户才能执行远程关闭计算机的操作。一般情况下，访问其他计算机只有 guest 用户权限，此时要执行远程关闭计算机操作，就会出现拒绝访问的提示。为此，用户需要修改被远程关闭的计算机中 guest 用户操作权限。

具体的操作方法如下。

步骤 1：在【运行】对话框中运行“gpedit.msc”命令，即可打开【组策略】窗口，展开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“用户权利指派”结点，如图 3-105 所示。

步骤 2：双击右侧窗口中的“从远端系统强制关机”选项，在弹出的对话框中将 guest 用

户添加到用户或组列表框中，如图 3-106 所示。

图 3-105 “组策略”窗口

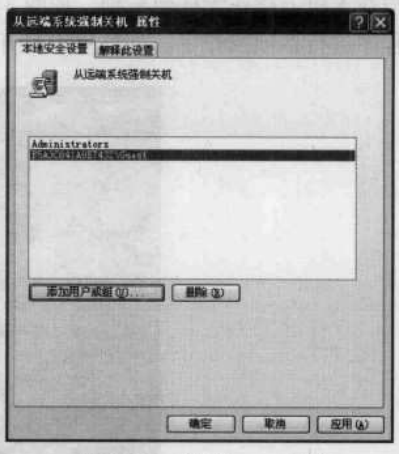


图 3-106 添加 guest 用户

步骤 3：在本地计算机中打开“命令提示符”窗口，在其中输入“shutdown -s –m \\远程计算机名-t 30”命令，其中 30 为关闭延迟时间，如图 3-107 所示。

步骤 4：被关闭的计算机屏幕上将显示“系统关机”对话框，如图 3-108 所示。被关闭的计算机操作员可输入“shutdown –a”命令中止关机任务。

图 3-107 输入关机命令

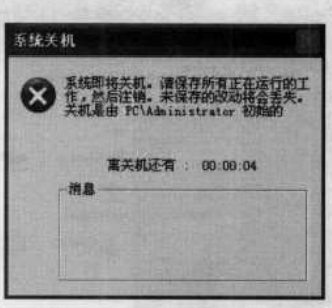


图 3-108 关机提示信息

3. 区别远程桌面与远程协助

“远程协助”是 Windows 附带提供的一种远程控制方法。远程协助的发起者通过 MSN Messenger（或 Windows Messenger）向 Messenger 中的联系人发出协助要求，在获得对方同意后，可进行远程协助，远程协助中被协助方计算机将暂时受协助方（在远程协助程序中被称为专家）的控制，专家可在被控计算机中进行系统维护、安装软件、处理计算机中的某些问题或向被协助者演示某些操作。

使用“远程协助”时还可以通过向邀请方发送电子邮件等方式进行，且通过“帮助和支持”窗口能够查看到邀请与被邀请的有关资料。在使用“远程协助”进行远程控制时，必须由主控双方协同才能够进行，所以 Windows XP 专业版中又提供了“远程桌面连接”控制方式。

利用“远程桌面连接”功能，用户可在远离办公室的地方通过网络对计算机进行远程控制，即使主机处在无人状况，“远程桌面连接”仍然可顺利进行，远程用户可通过这种方式使用计算机中的数据、应用程序和网络资源，也可让同事访问到自己的计算机桌面，以便于进行协同工作。使用“远程桌面连接”功能时，被控计算机用户不能使用自己的计算机，不能看到远程

操作者所进行的操作过程，且远程控制者具有被控计算机的最高权限。

第 27 招　远程管理主机

一个网络，无论是局域网还是网站往往都需要一台主机负责整个网络的管理，而主机的管理则需要一个专门负责的人进行维护。远程管理主机可以实现系统管理员对主机的远程控制，从而减少系统管理员的路途奔波，节省了时间，也提高了效率。

1．利用漏洞入侵主机

一般来说，任何一个计算机系统都会存在漏洞，而黑客的攻击也是基于漏洞开展的。计算机与网络连接后，就需要打开相应的端口，而每个服务都需要相应的端口，如 FTP 端口为 21，HTTP 端口为 80 等，每个服务都可能存在漏洞，黑客根据扫描到的端口信息，就可以入侵到目标主机系统中。

下面以扫描到的 IDQ 漏洞为例介绍黑客的入侵过程（IDQ 漏洞可以使黑客得到 Web 目录有绝对路径，且还能使攻击者获得一个 Shell，Shell 是一种命令解释程序，它能给攻击者提供远程控制接口，从而控制服务器）。具体的操作方法如下。

步骤 1：扫描目标主机存在 IDQ 漏洞后，使用 Snake IIS 溢出工具，在 IP 地址框中输入“127.0.0.1”，端口设定为 80（这里看对方 HTTP 端口而定）。

步骤 2：选择操作系统类型，这里要看服务器是中文的、英文的还是日文的，有没有打开 SP 补丁，一般选择第一项。

步骤 3：选择 cmd.exe 绑定端口。这里可随便使用 1～65535 中一个没有被激活的端口。

步骤 4：单击 IDQ 溢出，如果成功，即可发送 shellcode 到 127.0.0.1：80。

步骤 5：使用 Telnet 工具，在“命令提示符”窗口输入“Telnet 127.0.0.1：813”命令，即可进入对方系统（其中 813 为目标主机未激活端口）。

2．为漏洞主机打补丁

因为所有的计算机系统都存在漏洞，而且对一个固定的系统来说漏洞也还在不断地发现中。为了避免自己的计算机系统被黑客攻击，就需要及时为自己的系统打上漏洞补丁，特别是具有重大安全隐患的漏洞补丁。为系统打补丁的方法很多，最常用的有如下几种。

方法 1：使用 Windows 系统更新功能。Windows 系统具有自动更新功能，选择【开始】→【程序】→【Windows Update】菜单项，即可连接 Microsoft 公司的网站，如图 3-109 所示。

图 3-109　微软更新网站

方法 2：开启 Windows 系统的自动更新功能。在“控制面板”窗口中双击“自动更新”图标，即可打开【自动更新】对话框，在其中选取“自动（建议）”单选项，如图 3-110 所示。Windows 系统将自动下载补丁进行安装。

方法 3：使用专门工具。现在大多数杀毒软件和防火墙都提供系统漏洞扫描功能，可以下载相应的漏洞补丁进行安装。如在瑞星杀毒软件界面中选择“安检”选项卡，单击“扫描系统漏洞并升级补丁”超链接，即可对当前系统进行漏洞扫描并下载相应漏洞，如图 3-111 所示。

图 3-110　启用“自动更新”功能

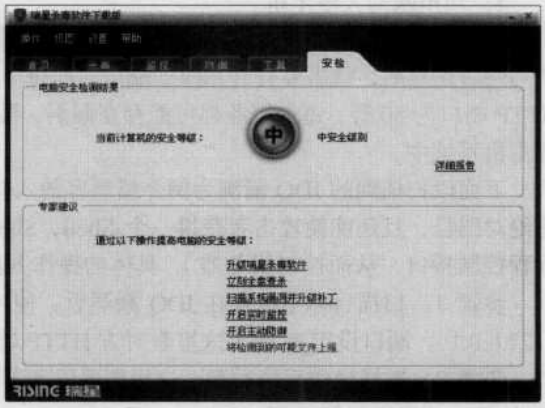


图 3-111　瑞星杀毒软件的漏洞扫描功能

3. 建立隐藏式网站

所谓隐藏式网站就是能够隐藏网站目录，使访问者不能明显地看出网站文件在服务器中保存的位置，从而提高网站的安全性。下面以 IIS 网站为例介绍隐藏网站保存路径操作方法。

步骤 1：通过【开始】→【设置】→【控制面板】→【管理工具】→【Internet 信息服务】菜单项，即可打开“Internet 信息服务”窗口。右击某一个网站，在快捷菜单中执行“资源管理器”选项，如图 3-112 所示。

步骤 2：在打开的网站文件夹中创建一个名称为“new”的文件夹，如图 3-113 所示。

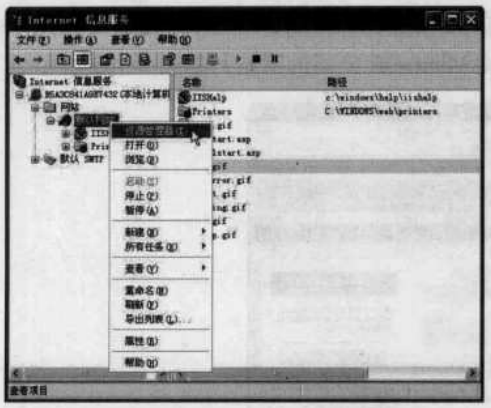


图 3-112　“Internet 信息服务”窗口

图 3-113　创建文件夹

步骤 3：在硬盘的其他位置创建一个名称为“hack”的文件夹，因为该文件夹将存放要隐藏的网站主页，所以隐藏的路径越深越好，如图 3-114 所示。

步骤 4：在【Internet 信息服务】窗口中右击“new”文件夹名称，在快捷菜单中选取“新建”→“虚拟目录”菜单项，即可弹出【虚拟目录创建向导】对话框。单击【下一步】按钮，在其中输入虚拟目录的“别名”，如图 3-115 所示。

图 3-114 创建隐藏网站的文件夹

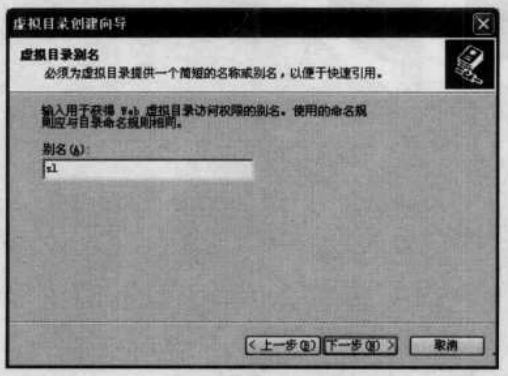


图 3-115 输入虚拟目录别名

步骤 5：单击【下一步】按钮，在显示的对话框中单击【浏览】按钮，指定“hack”目录路径，如图 3-116 所示。单击【下一步】按钮，选择该虚拟目录允许的权限选项，如图 3-117 所示单击【下一步】按钮，再单击【完成】按钮，即可结束虚拟目录的创建操作。

步骤 6：在【Internet 信息服务】窗口中找到新建的“new”文件夹之后，将其删除，即可完成网站存放路径的隐藏操作。

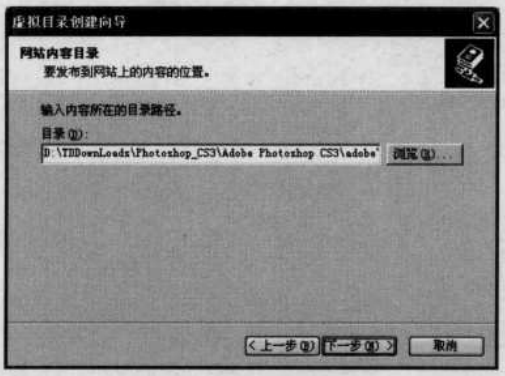


图 3-116 指定虚拟目录路径

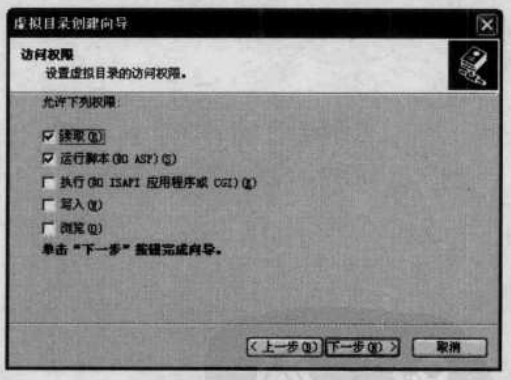


图 3-117 选择允许权限

第 4 章　欺骗与反欺骗

重点提示

- 提防虚假的 Guest 账户
- 防范假终端管理员
- 拒绝恶意接入的网络执法官
- 实现 ARP 欺骗攻击
- 实现 DNS 欺骗攻击
- 行行色色的网络欺骗
- 用 Privacy Defender 清除痕迹

本章精粹：

本章将着重介绍网络欺骗攻击的各种方式和技术，并利用网络欺骗攻击获得网络中限制资源的方法与技巧，还介绍了黑客攻防中各种获取和保护账户密码的方法，有助于读者从中找到更加有效地防御黑客攻击的方法。

网络欺骗就是使入侵者相信信息系统存在有价值的、可利用的安全弱点，具有一些可攻击窃取的资源（当然这些资源是伪造的或不重要的），并将入侵者引向这些错误的资源；可显著地增加入侵者的工作量、入侵复杂度及不确定性，从而使入侵者不知道其进攻是否奏效或成功；且允许防护者跟踪入侵者的行为，在入侵之前修补系统可能存在的安全漏洞。

第 28 招　提防虚假的 Guest 账户

在黑客入侵中，稍有经验的黑客们在入侵时可利用系统中存在的 Guest 账户设置不当的安全隐患，在被入侵主机系统中来去自如，如通过 Guest 账户克隆出无数的管理员账户。

1．改头换面的管理员账户

Administrator 是系统默认的具有最高权限的管理员帐号，而 Guest 账户是系统默认的最低权限的账户，因此，很多系统管理员对 Guest 账户放松了管理，认为黑客即使得到了这类账户的权限，也不会对系统造成任何影响。这样就会使黑客有机可乘，利用 Guest 账户入侵系统。下面就来看看黑客是如何将 Guest 账户变成管理员账户的。

黑客首先利用扫描软件来侦测系统中的 Guest 账户是否具有可入侵性，其判断为该账户是否具有弱口令特征，如果有，该账户将非常容易被盗用。黑客往往会利用 Guest 账户登录被入侵系统，则会在自己的计算机中打开 DOS 命令窗口，在其中输入“Net use\\61.147.*.*（这个 IP 即为入侵地址）”命令。

在出现“密码或用户名在\\61.147.*.*无效”的提示之后，输入扫描得到的用户名和密码，即可看见“命令成功完成”的提示信息。这时黑客已成功利用 Guest 账户登录上被入侵的计算机主机系统，只要使用“Net Localgroup Administrators Guest/add”命令，即可完成账户的欺骗性“权限变更”操作。这样，一个简单的命令就可以将 Guest 变为 Administrator 了。

2．混迹管理员组的 Guest 账户

许多网络系统的管理员在黑客对其账户进行了欺骗式的操作之后，还蒙在鼓里，直到有一天资料被窃取才猛然发现自己被黑了。作为系统管理员，怎样才能及时地识破这一切呢？应先查看 Guest 账户中的“隶属组”，查看当前的账户是否非法存在于管理员组中即可。

具体的查看方法如下。

步骤 1：选择【开始】→【设置】→【控制面板】选项，即可打开“控制面板”窗口，如图 4-1 所示。

步骤 2：双击“管理工具”图标，即可打开“管理工具”窗口。再双击“计算机管理”图标，即可打开“计算机管理”窗口，如图 4-2 所示。

图 4-1 【控制面板】窗口

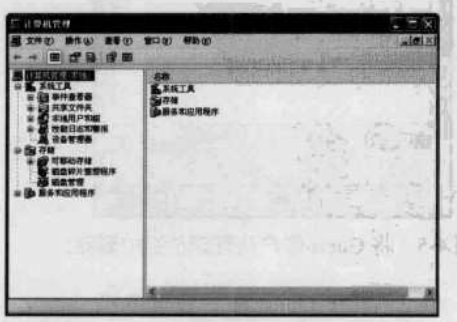


图 4-2 【计算机管理】窗口

步骤 3：逐层单击依次展开【计算机管理】→【系统工具】→【本地用户和组】→【用户】选项，在右侧用户列表中可看到 Guest 账户名的存在，如图 4-3 所示。

步骤 4：右击 Guest 账户，在弹出菜单中选择【属性】选项，即可打开该账户的【属性】对话框，在“隶属于”选项卡中可以看到 Guest 账户隶属于两个组，分别是“Administrator”和“Users”，如图 4-4 所示。由此可见，Guest 账户已经被黑客加入到管理员组中了。

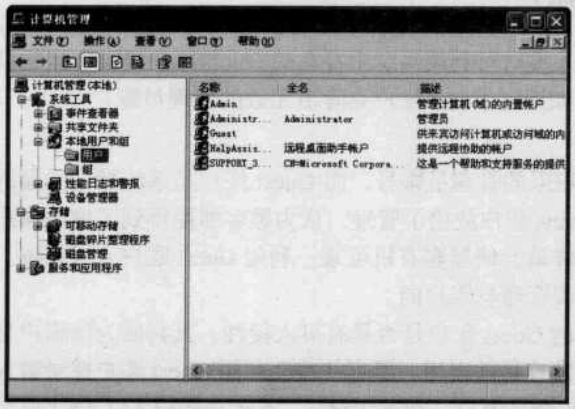


图 4-3　Guest 账户名

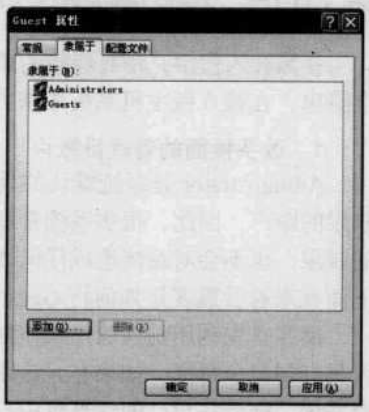


图 4-4　Guest 账户已加入管理员组

3. Guest 账户安全管理

下面讲述作为系统管理员如何对 Guest 账户进行安全的管理，通常有如下 3 种方法。

（1）删除非法加入的组

删除非法加入的组的具体操作步骤如下。

步骤 1：选中“Administrator”组并单击【删除】按钮，即可将 Guest 账户从“Administrator”组中删除，让 Guest 账户只隶属于“Guests 组”，如图 4-5 所示。

步骤 2：切换到“常规”选项卡，在其中勾选“账号已停用”复选框，如图 4-6 所示。这样，黑客就无法使用 Guest 账户登录系统了。

图 4-5　将 Guest 账户从管理员组中删除

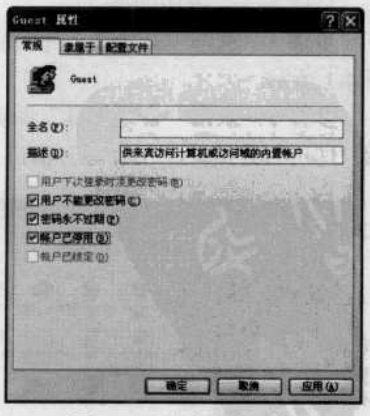


图 4-6　“常规”选项卡

（2）禁止 Guest 账户登录本机

为了更保险地保护 Guest 账户的安全，还可使用组策略来进行管理。具体操作方法如下。

步骤 1：在【运行】对话框的“打开”文本框中输入“gpedit.msc”命令，如图 4-7 所示。

步骤 2：单击【确定】按钮，即可打开【组策略】窗口，依次展开【计算机配置】→【Windows 设置】→【安全设置】→【本地策略】→【用户权利指派】选项，在右侧选项列表中选择“在本地登录”选项，如图 4-8 所示。

步骤 3：双击“在本地登录”选项，即可打开【在本地登录属性】窗口，如图 4-9 所示。在其中选择 Guest 账户，单击【删除】按钮，即完成了 Guest 账户不能登录本机的设置。

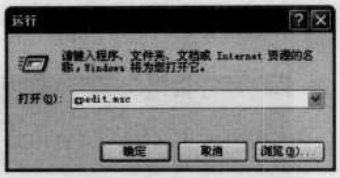


图 4-7 【运行】对话框

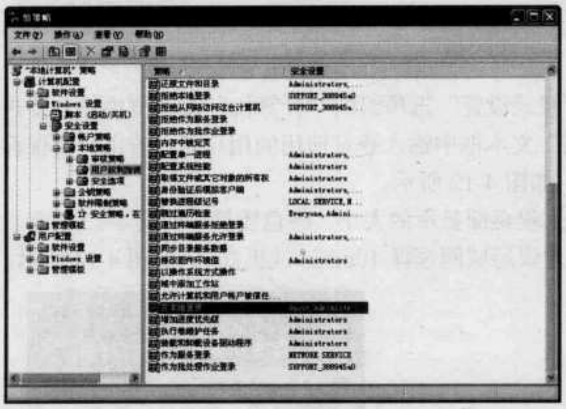


图 4-8 【组策略】窗口

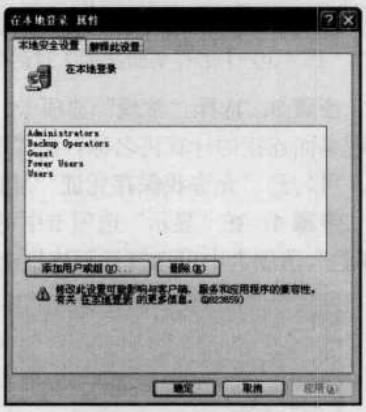


图 4-9 删除 Guest 账户名

（3）牢记 Guest 账户密码的设置规则

Guest 账户的设置方法非常简单，但设置时要注意密码的提示既要让自己能够记牢也得让别人无从猜测。密码设置的原则是：不规律的密码组合+定期的密码更换。一个相对安全的密码应该具有的特征是无规律可循且便于记忆。正确的设置应该是既包含大小写字母，又包含数字和标点的字符串，而且还要便于记忆。混杂密码组合被破解的概率会变得非常低。注意密码不要让自己也无从记起，那样很容易造成密码遗忘，从而导致一些不必要的麻烦。

第 29 招 防范假终端管理员

终端服务（Terminal Services）也叫 WBT（Windows-based Terminal，基于 Windows 的终端），它集成在 Windows.NET Server 中，作为系统服务器服务组件存在。终端服务的工作原理是客户机和服务器通过 TCP/IP 协议和标准的局域网构架联系。通过客户端终端的客户机的鼠标、键盘的输入传递到终端服务器上，再把服务器上的显示传递回客户端。客户端不需要具有计算能力，最多只需要提供一定的缓存能力。众多的客户端可以同时登录到服务器上，仿佛同时在服务器上工作一样，它们之间作为不同的会话连接是互相独立的。

与终端服务器的连接很简单，例如可使用 Windows XP 自带的“远程桌面”程序与终端服务器进行连接，从而启动一个终端会话。具体的操作步骤如下。

步骤 1：在【运行】对话框的“运行栏”中输入“mstsc.exe”命令，即可弹出“远程桌面连接”对话框，如图 4-10 所示。

步骤 2：单击【选项】按钮，将出现完整的远程桌面连接程序设置界面，如图 4-11 所示。

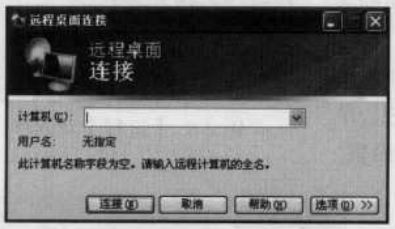


图 4-10 【远程桌面连接】对话框

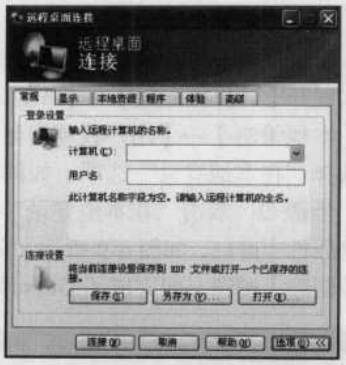


图 4-11 设置远程桌面连接选项

步骤 3：选择“常规”选项卡，在“登录设置”选项组的“计算机”文本框中输入要进行远程桌面连接的计算机名称；在“用户名”文本框中输入登录使用的用户名；若用户要保存凭证，可勾选“允许我保存凭证”复选框，如图 4-12 所示。

步骤 4：在“显示”选项卡中可设置远程桌面显示的大小、颜色质量，如图 4-13 所示。在“体验”选项卡中可选择远程连接速度（建议局域网选择 10mbps 或更高），如图 4-14 所示。

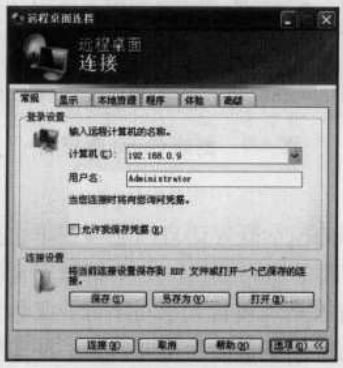


图 4-12 “常规”选项卡

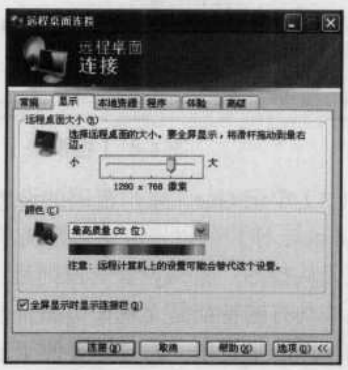


图 4-13 “显示”选项卡

步骤 5：单击【连接（N）】按钮，稍等片刻就会连接到终端服务器上，这时终端服务器的登录界面将会出现在远程桌面连接程序中，在“用户名”文本框中输入登录用户的名称，在“密码”文本框中输入登录密码，如图 4-15 所示。

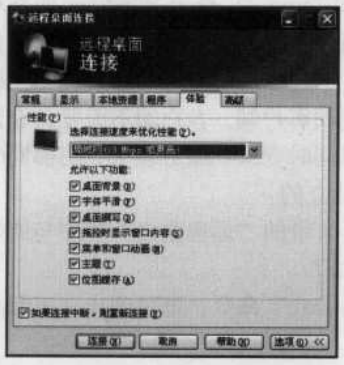


图 4-14 “体验”选项卡

图 4-15 【登录到 Windows】对话框

注意 登录远程计算机的用户必须设置密码，否则将不能正常使用远程桌面连接功能。另外，进行远程桌面连接时远程计算机用户将不能登录，若登录则断开远程桌面连接。

步骤 6：单击【确定】按钮，即可登录到远程计算机桌面，此时用户在远程桌面上的操作与在本机上操作无任何差别，如图 4-16 所示。

图 4-16 成功登录到远程计算机桌面

小技巧 默认情况下，终端服务器在客户端的显示是全屏的，可以单击窗口标题栏右上角的最大化、最小化或关闭按钮对客户端的窗口进行操作。

步骤 7：需要断开远程桌面连接时，只需在本地计算机中单击远程桌面连接窗口上的【关闭】按钮，在弹出提示信息框中单击【确定】按钮，如图 4-17 所示。

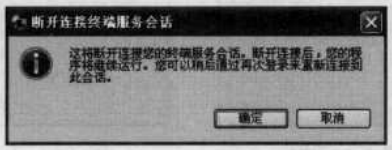


图 4-17 【断开连接终端服务会话】对话框

第 30 招 拒绝恶意接入的网络执法官

“网络执法官”是一款局域网管理辅助软件，采用网络底层协议能穿透各客户端防火墙对网络中的每一台主机（这里的主机是指各种计算机、交换机等配有 IP 的网络设备）进行监控；采用网卡号（MAC 地址）识别用户等。

1．安装网络执法官

“网络执法官”主要功能是依据管理员为各主机限定的权限，实时监控整个局域网，并自动对非法用户进行管理，可将非法用户与网络中某些主机或整个网络隔离，而且无论局域网中的主机运行何种防火墙，都不能逃避监控，也不会引发防火墙警告，提高了网络安全性。

在使用“网络执法官”进行网络监控前应对其进行安装，具体的操作步骤如下。

步骤 1：下载并解压“网络执法官”文件夹，双击“网络执法官”安装程序图标，即可弹出【选择安装语言】对话框，在其中选择需要使用的语言，如图 4-18 所示。

步骤 2：在选择好要使用的语言后，单击【确定】按钮，即可打开【欢迎使用 Netrobocop v3.39

安装向导】对话框，如图 4-19 所示。

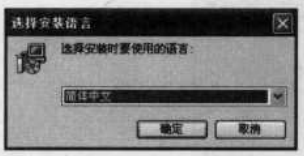


图 4-18 【选择安装语言】对话框

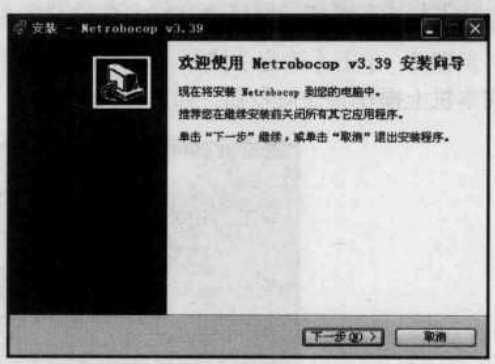


图 4-19 【欢迎使用 Netrobocop v3.39 安装向导】对话框

步骤 3：单击【下一步】按钮，即可打开【选择目标位置】对话框，在其中选择程序安装位置，如图 4-20 所示。选择“Netrobocop v3.39”安装目标位置，单击【下一步】按钮，即可打开【开始菜单文件夹】对话框，在其中选择放置程序快捷方式位置，如图 4-21 所示。

图 4-20 【选择目标位置】对话框

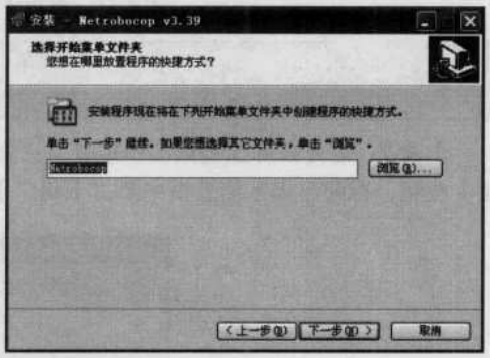


图 4-21 【开始菜单文件夹】对话框

步骤 4：单击【下一步】按钮，即可打开【选择附加任务】对话框，选择安装“Netrobocop v3.39”时要执行的附加任务，如图 4-22 所示。

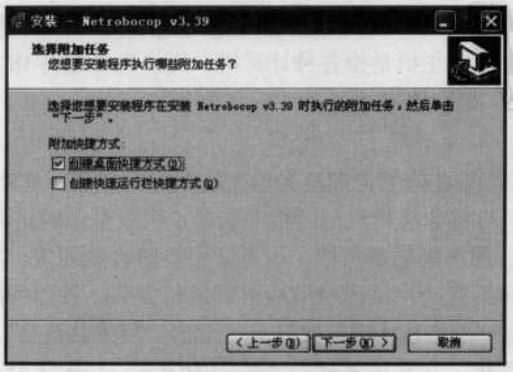


图 4-22 【选择附加任务】对话框

步骤 5：继续单击【下一步】按钮，即可进入【准备安装】对话框，将开始准备安装程序，如图 4-23 所示。单击【安装】按钮，开始安装并显示安装进度。

步骤 6：单击【下一步】按钮，即可弹出【Netrobocop v3.39 安装向导完成】对话框。单击【完成】按钮，即可完成安装，如图 4-24 所示。

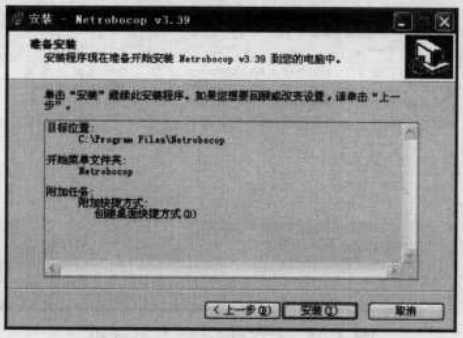


图 4-23 【准备安装】对话框

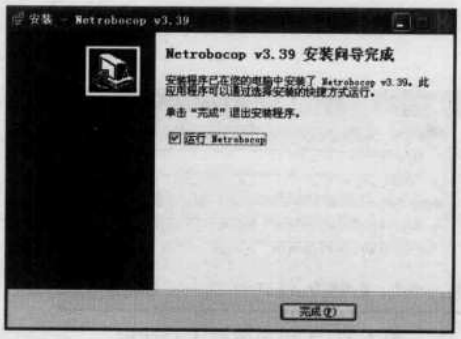


图 4-24 【Netrobocop v3.39 安装向导完成】对话框

步骤 7：在安装完成后，"网络执法官"会在桌面自动生成快捷方式。双击"Netrobocop"快捷方式图标，即可弹出【设置扫描范围】对话框，在其中指定监测的硬件对象和网段范围，如图 4-25 所示。

步骤 8：在设置好要扫描的范围之后，单击【添加/修改】按钮，再单击【确定】按钮，即可进入"网络执法官"操作窗口，其中显示了在同一个局域网下的所有用户，可查看其状态、流量、IP 地址、是否锁定、最后上线时间、下线时间、网卡注释等信息，如图 4-26 所示。

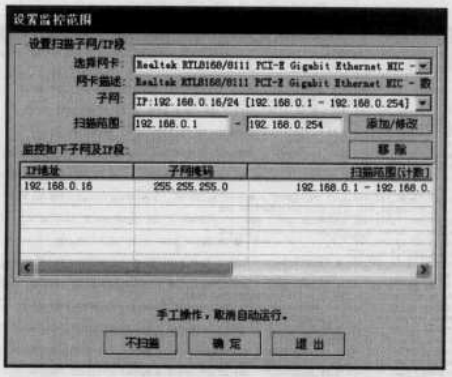


图 4-25 【设置扫描范围】对话框

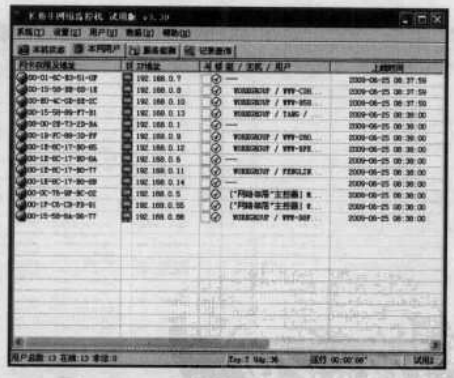


图 4-26 "网络执法官"操作窗口

"网卡 MAC 地址"是网卡的物理地址，也称硬件地址或链路地址，是网卡自身的唯一标识，一般不能随意改变。无论把这个网卡接入到网络的什么地方，MAC 地址都不变。其长度为 48 位二进制数，由 12 个 00～0FFH 的 16 进制数组成，每个 16 进制数之间用"-"隔开，如"00-0C-76-9F-BC-02"。

2．查看目标计算机属性

使用"网络执法官"可搜集处于同一局域网内所有主机的相关网络信息。

具体的操作步骤如下。

步骤 1：在"网络执法官"操作窗口中双击"用户列表"中需要查看的对象，即可打开【用

户属性】对话框，在其中查看用户的网卡地址、IP 地址、上线情况等，如图 4-27 所示。

步骤 2：还可以通过单击【历史记录】按钮，即可打开【在线记录】对话框，在其中查看该计算机上线的情况，如图 4-28 所示。

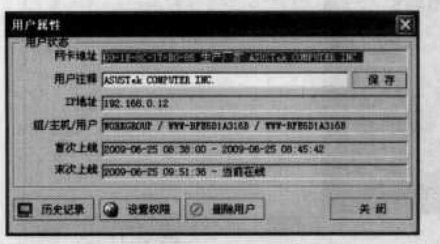


图 4-27 【用户属性】对话框

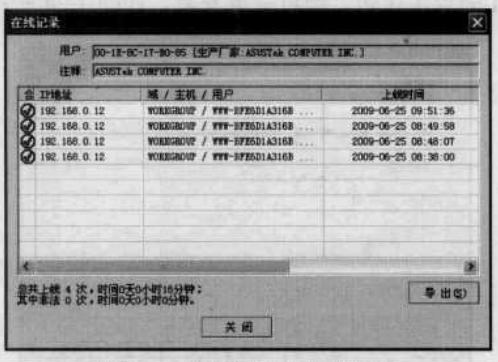


图 4-28 【在线记录】对话框

3. 批量保存目标主机信息

除收集局域网内各个计算机的信息之外，“网络执法官”还可以对局域网中的主机信息进行批量保存。具体的操作步骤如下。

步骤 1：在“网络执法官”操作窗口中选择“记录查询”选项卡，在“IP 地址段”中输入“起始 IP 地址”和“结束 IP 地址”，单击【查找】按钮，即可开始收集局域网中计算机的信息，如图 4-29 所示。

步骤 2：单击【导出】按钮，将所有信息导出为文本文件，如图 4-30 所示。

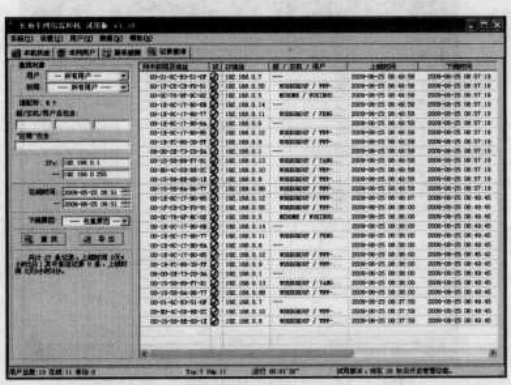


图 4-29 “记录查询”页面

图 4-30 查看记事本文件信息

4. 设置关键主机

“关键主机”是由管理员指定的 IP 地址，可以是网关、其他计算机或服务器等。管理员将指定的 IP 存入“关键主机”之后，即可令非法用户仅断开与“关键主机”的连接，而不断开与其他计算机的连接。

设置“关键主机组”的具体操作方法如下。

步骤 1：选择【设置】→【关键主机组】菜单项，或在【锁定/解锁】对话框中单击【设置】按钮，均可打开【关键主机组设置】对话框，如图 4-31 所示。

步骤 2：在“选择关键主机组”下拉列表框中选择关键主机组的名称。

步骤 3：在设定“组内 IP”之后，单击【全部保存】按钮，将关键主机的修改生效并进行保存。

图 4-31 【关键主机组设置】对话框

5. 设置默认权限

“网络执法官”还可以对局域网中的计算机进行网络管理。并不要求它安装在服务器中，而是可以安装在局域网内的任一台计算机上，即可对整个局域网内的所有计算机进行管理。

设置用户权限的具体操作如下。

步骤 1：单击【用户属性】对话框中的【设置权限】按钮，即可打开【用户权限设置】对话框，在其中对用户权限类型进行相应设置，如图 4-32 所示。

步骤 2：选择“受限用户，若违反以下权限将被管理”单选项之后，如果需要对 IP 进行限制，则可勾选“启用 IP 限制”复选框，并单击【禁用以下 IP 段：未设定】按钮，即可在弹出的 IP 限制对话框中对 IP 进行设置，如图 4-33 所示。

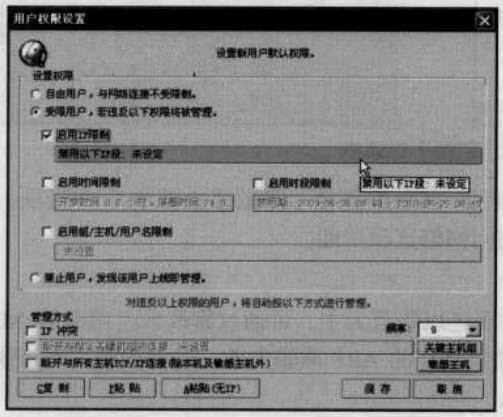


图 4-32 【用户权限设置】对话框

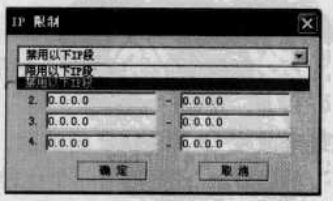


图 4-33 【IP 限制】对话框

步骤 3：选择“禁止用户，发现该用户上线即管理”单选项，即可在“管理方式”复选项中设置管理方式。当目标计算机连入局域网时，“网络执法官”即按照设定的项对该计算机进行管理，如图 4-34 所示。

步骤 4：在“网络执法官”操作窗口中右击“用户列表”的任意一个对象，在快捷菜单中选择“权限设置”选项，即可单独配置该用户的权限，如图 4-35 所示。

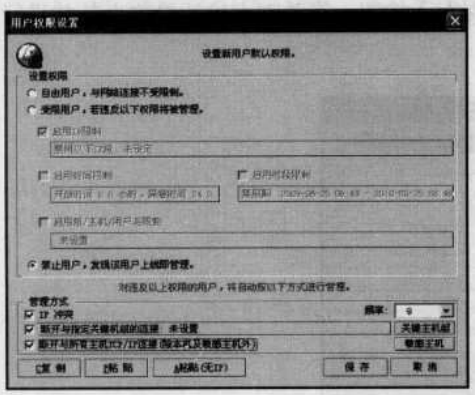


图 4-34　设置管理方式

图 4-35　从“用户列表”中设置用户权限

6. 禁止目标计算机访问网络

禁止目标计算机访问网络是“网络执法官”的重要功能，具体的禁止方法如下。

步骤 1：在“网络执法官”操作窗口中，右击“用户列表”中的任意一个对象，在弹出的快捷菜单中选择“锁定/解锁”选项，即可弹出【锁定/解锁】对话框，如图 4-36 所示。

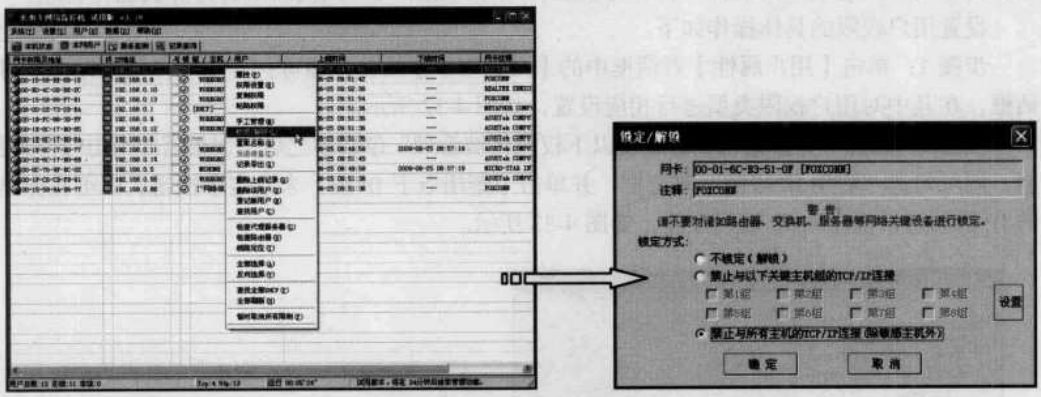


图 4-36　【锁定/解锁】对话框

步骤 2：选中锁定方式为“禁止与所有主机的 TCP/IP 连接（除敏感主机外）”单选项，单击【确定】按钮，即可实现禁止目标计算机访问网络这项功能。

7. 拒绝“网络执法官”的恶意接入

目前，拒绝“网络执法官”的恶意接入主要还以防范为主，可通过修改自己网卡的 MAC 地址来改变 IP 到 MAC 的映射，从而使得网络执法官的 ARP 欺骗失效，进而摆脱“网络执法官”的破坏。下面介绍一个比较常用的方法。

步骤 1：打开【运行】对话框在“打开”文本框中输入“regedit”，单击【确定】按钮，如图 4-37 所示。

步骤 2：在【注册表编辑器】窗口中展开 HKEY_LOCAL_MACHINE\SYSTEM\Current ControlSet\ Control\Class\子项，如图 4-38 所示。

步骤 3：在注册表编辑器右窗口找到说明为“网卡”的目录，比如 36FC9E60-C465-11CF-8056-444553540000。在其下 0000，0001，0002.....分支中找到“DriverDesc”键值，如“DriverDesc”值为“Intel（R）82559 Fast Ethernet LAN on Motherboard”，即为网卡说明。

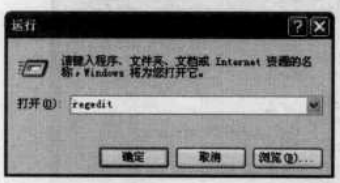


图 4-37 【运行】对话框

图 4-38 展开注册表编辑器

步骤 4：在找到的分支下添加新字符串变量（如在 0000 下找到的，就在 0000 下面添加字符串变量）并将其命名为“NetworkAddress”。在其中输入新网卡 MAC 地址（应该是 12 个十六进制数，如 4F61E87C95BA，不能设置为 000000000000，也不能与别的网卡的 MAC 地址重复）。在设置完毕之后，重启计算机。

第 31 招 实现 ARP 欺骗与防御

ARP（Address Resolution Protocol，地址解析协议）是一个位于 TCP/IP 协议栈中的低层协议，主要负责将某个 IP 地址解析成相对应的 MAC 地址。从防护者角度来讲，网络欺骗具有扰乱入侵者意图，使之按照机主设定方向进行入侵选择；能够迅速检测到入侵者并可及时发现入侵者的技术手段和入侵意图；能够大量消耗入侵者系统资源，使之感到入侵困难。

1. 用 WinArpAttacker 实现 ARP 欺骗

WinArpAttacker 是一款在网络中进行 ARP 欺骗攻击的工具，并使被攻击的主机无法正常与网络进行连接。此外，它还是一款网络嗅探（监听）工具，可嗅探网络中的主机、网关等对象，也可进行反监听，扫描局域网中是否存在监听。具体的操作步骤如下。

步骤 1：将 WinArpAttacker 压缩包解压后，先安装 WinPcap 再双击 WinArpAttacker.exe 程序，即可进入其主界面，如图 4-39 所示。

步骤 2：单击工具栏上的【扫描】按钮，即可扫描出局域网中的所有主机。若选择【扫描】→【高级】选项，则可设置扫描范围，如图 4-40 所示。

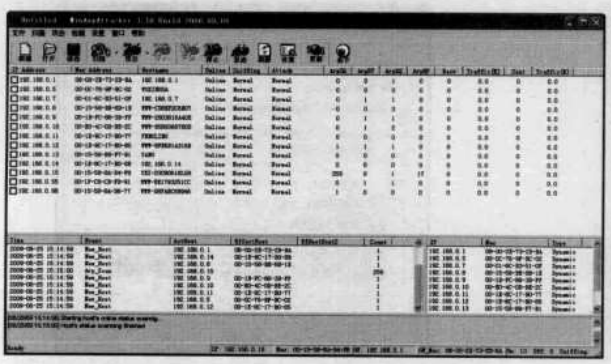


图 4-39 WinArpAttacker 操作界面

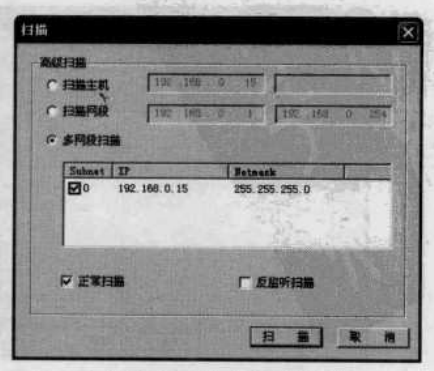


图 4-40 设置扫描范围

步骤 3：单击工具栏上的【设置】按钮，即可打开【Options】对话框，如图 4-41 所示。如果本地主机安装有多块网卡，则可在“适配器”标签卡选择绑定的网卡和 IP 地址。

步骤 4：在“攻击”标签卡中可设置网络攻击时的各种选项，如图 4-42 所示。除 ARP FLOOD 是次数外，其他都是持续时间，如果是 0 则不停止。在“更新”标签卡中可设置自动扫描的时间间隔，如图 4-43 所示。在“检测”标签卡中可设置检测的频率，如图 4-44 所示。

图 4-41　设置适配器

图 4-42　设置攻击选项

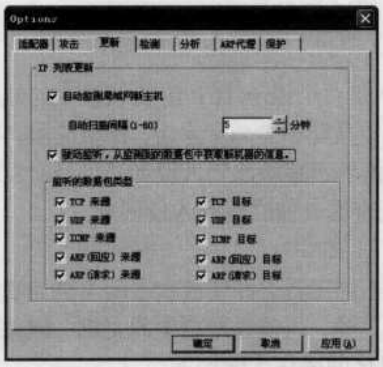


图 4-43　设置更新选项

图 4-44　设置检测频率

步骤 5：在“分析”标签卡中可指定保存 ARP 数据包文件的名称与路径，如图 4-45 所示。在“代理 ARP”标签卡中可启用代理 ARP 功能，如图 4-46 所示。在“保护”标签卡中可启用本地和远程防欺骗保护功能，避免自己的主机受到 ARP 欺骗攻击，如图 4-47 所示。

图 4-45　设置文件名称与保存路径

图 4-46　启用代理 ARP 功能

步骤 6：在选取需要攻击的主机之后，单击【攻击】按钮右侧下拉按钮，在其中选择攻击方式，如图 4-48 所示。受到攻击的主机将不能与 Internet 网络进行正常连接，单击【停止】按钮，则被攻击的主机恢复正常连接状态。

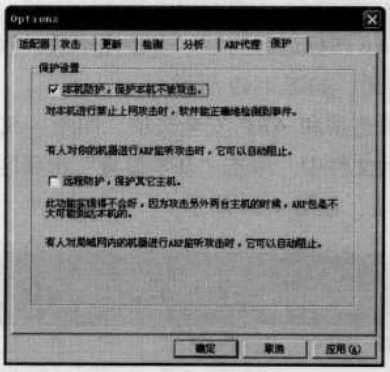


图 4-47　使用防护功能

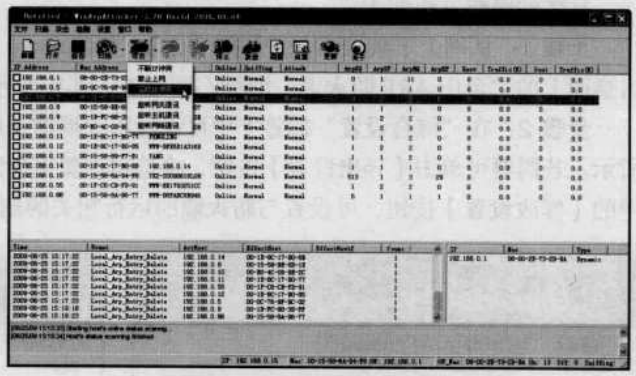


图 4-48　选择攻击方式

步骤 7：如果使用了嗅探攻击，则可单击【探测】按钮开始嗅探。单击【保存】按钮，可将主机列表保存下来，最后再单击【打开】按钮，即可打开主机列表。

步骤 8：如果用户对 ARP 包的结构比较熟悉，了解 ARP 攻击原理，则可自己动手制作攻击包，单击【发送】按钮进行攻击。

提示 ArpSQ 是该机器的发送 ARP 请求包的个数；ArpSP 是该机器的发送回应包个数；ArpRQ 是该机器的接收请求包个数；ArpRP 是该机器的接收回应包个数。

2．网络监听的防御

当成功地登录到一台网络主机并取得了这台主机的超级用户权限之后，往往要尝试登录或夺取网络中其他主机的控制权。而网络监听则常常能轻易获得用其他方法很难获得的信息。在一个以太网中任何一台上网主机上运行监听工具，这是多数黑客的做法。

网络监听的防范一般比较困难，通常可采取数据加密、网络分段和运用 VLAN 技术三种方法。

1）数据加密：数据加密的优越性在于，即使攻击者获得了数据，如果不能破译，这些数据对他也是没有用的。一般而言，人们真正关心的是那些秘密数据的安全传输，使其不被监听和偷换。如果这些信息以明文的形式传输，就很容易被截获而且阅读出来。因此，对秘密数据进行加密传输是一个很好的办法。

2）网络分段。因为网络监听只能监听到本网段内的传输信息，所以可以采用网络分段技术，建立安全的网络拓扑结构，将一个大的网络分成若干个小的网络，如将一个部门、一个办公室等可以相互信任的主机放在一个物理网段上，网段之间再通过网桥、交换机或路由器相连，实现相互隔离。这样，即使某个网段被监听了，网络中其他网段还是安全的。因为数据包只能在该子网的网段内被截获，网络中剩余的部分（不在同一网段的部分）则被保护了。

3）运用 VLAN 技术。运用 VLAN（虚拟局域网）技术，将以太网通信变为点到点通信，可以防止大部分基于网络监听的入侵。

3. 金山 ARP 防火墙的使用

金山 ARP 防火墙能够双向拦截 ARP 欺骗攻击包，监测锁定攻击源，时刻保护局域网内计算机的正常上网数据流向，是一款适合于个人用户的反 ARP 欺骗保护工具。

具体的操作方法如下。

步骤 1：从网上下载压缩包并解压后，双击 KAntiarp.exe 图标进行安装。安装完毕后，双击桌面上的“金山 ARP 防火墙”图标，即可进入其操作界面，如图 4-49 所示。

步骤 2：在“综合设置”标签卡中可设置防火墙的一般选项和 ARP 安全选项，如图 4-50 所示。若需要可单击【导出设置】按钮，将选项设置保存到文件中。单击“基本设置”选项区中的【修改设置】按钮，可设置与防火墙的运行相关的选项，如图 4-51 所示。

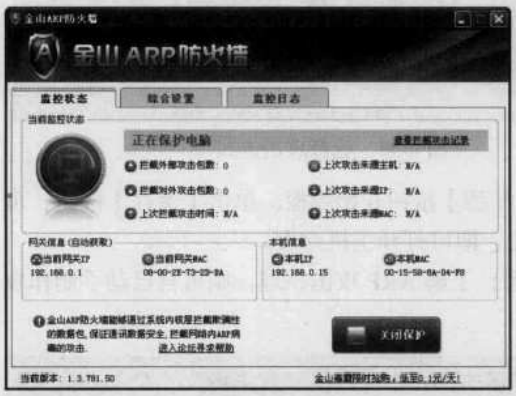


图 4-49 “金山 ARP 防火墙”主界面

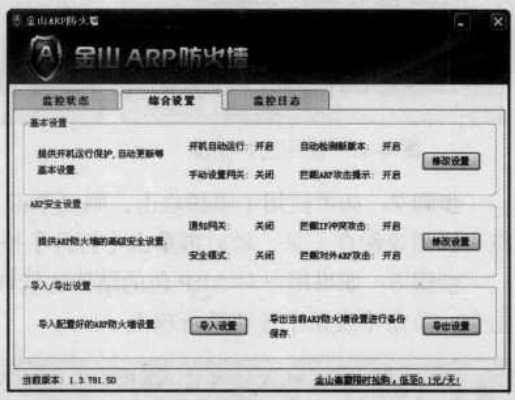


图 4-50 “综合设置”标签卡

步骤 3：单击“ARP 安全设置”选项区的【修改设置】按钮，在其中设置有关 ARP 攻击拦截等选项，如图 4-52 所示。在“监控状态”标签中可看到监控时拦截到的有关信息，如图 4-53 所示。

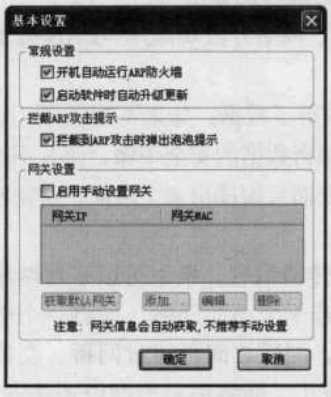


图 4-51 基本选项设置

图 4-52 设置 ARP 选项设置

步骤 4：在“监控日志”标签中可查看到拦截的日志记录，如图 4-54 所示。单击【浏览历史记录】按钮，即可使用记事本打开拦截的历史记录。

步骤 5：单击【清空列表记录】按钮，则可将“监控日志”标签卡显示的记录清除。

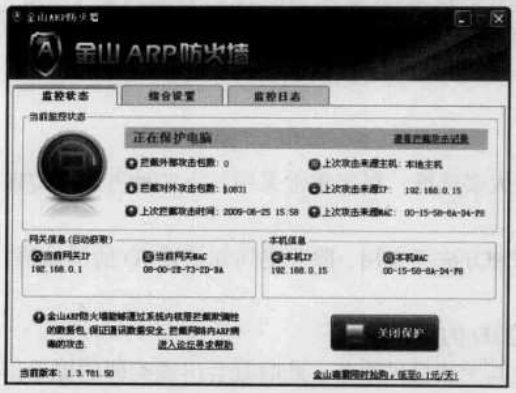


图 4-53 监控信息

图 4-54 日志记录

第 32 招 实现 DNS 欺骗攻击

DNS（Domain Name System，域名管理系统）是一种组织成域层次结构的计算机和网络服务命名系统，DNS 欺骗是一种非常复杂的攻击手段，但使用起来比 IP 欺骗要简单得多。

1. DNS 欺骗的实现过程

DNS 欺骗就是攻击者冒充域名服务器的一种欺骗行为，在局域网和广域网上实现 DNS 欺骗有所不同，相比之下，在局域网中实现 DNS 欺骗显得稍微容易些。

（1）在局域网中利用嗅探器实现 DNS 欺骗

如果已成功控制 203.171.239.143 所属子网中的任意一台主机，而且通过 Sniffer 对整个子网中传输的数据包进行嗅探，可设置只对 203.171.239.143 进行监听，从而获得需要标识 ID。

当 DNS 服务器发出查询数据包时，它会在数据包内设置标识 ID。只有应答包中的 IP 地址和 ID 值都正确时，服务器才接收。该 ID 每次会自动增加 1，所以可以第一次向 DNS 服务器发一个查询包并监听到该 ID 值，随后再发一个查询包，即可发送构造好的应答包，包内的标识 ID 为预测的值，可指定一个范围（如 ID+1 ~ ID+50）以提高成功率。

如某用户（192.168.0.45）向域名服务器 203.171.239.143 发来请求查询 www.newtop01.com 的 IP 地址包，此时 203.171.239.156 要进行欺骗，其看到的地址包的格式如下：

```
192.168.0.45 ---------->203.171.239.143  [Query]
NQY: 1  NAN: 0  NNS: 0  NAD: 0  QID:  1234
QY: www.newtop01.com
```

其中 NQY 和 NAN 等都是查询包的标志位，当这两个标记为 1 时表示查询安保。这是在 203.171.239.156 上监听到的包，得到它的 ID 值为 1234，然后也向服务器 203.171.239.143 发送一次查询，使其忙于应答这个包。查询包的具体内容如下：

```
203.171.239.156 ---------->203.171.239.143 [Query]
NQY: 1  NAN: 0  NNS: 0  NAD: 0
QY: www.newtop01.com
```

再给用户 192.168.0.45 发送伪造的且带预测 QID 的应答包，其具体内容如下：

```
203.171.239.143 ---------->192.168.0.45  [Answer]
NQY: 1  NAN: 0  NNS: 0  NAD: 0
```

```
QY: www.newtop01.com PTR
AN: www.newtop01.com PTR  203.171.239.84
```

其中“203.171.239.84”就是伪造的 IP 地址，这样，DNS 欺骗就完成了。而当用户打开百度主页时，用户还认为这个网站被黑掉了。

（2）在广域网中实现 DNS 欺骗

如果要在广域网上实现 DNS 欺骗，并没有太多选择，黑客常常采用如下四种方式来实现 DNS 欺骗：

1）随机地测试所有 ID 的可能存在的值。该种方法不实用，除非确切知道该 ID 的具体值，或有一些有利的条件可以使其更容易实现。

2）发送更多的 DNS 查询包来提升得知正确 ID 的机会。

3）对 DNS 服务器实行拒绝服务式攻击，使其无法提供服务，此时就会出现类似的提示信息：>> mar 05 18:20:17 ADM named [1931]:db_F_ACTIVE set –ABORT at this time named deamon is out of order。

4）可以利用由 SNI（SecureNetworks，Inc.）发现 BIND 漏洞，利用 BIND 漏洞的 ID 来实现 DSN 欺骗攻击。

2. DNS 的攻击实例

网络守护神是主要针对目前国内机关，企事业单位的网络应用现状，如单位总出口带宽有限、网络滥用、员工无节制上网、聊天等情况，提供了简单、快捷而非常有效的管理功能。

使用网络守护神反击攻击者的具体操作步骤如下。

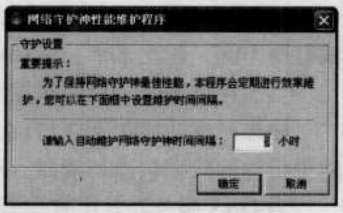


图 4-55 【网络守护神性能维护程序】对话框

步骤 1：安装网络守护神后，首次启动时会弹出要求设置自动维护时间间隔的【网络守护神性能维护程序】对话框，在其中设置自动维护网络守护神的时间间隔，如图 4-55 所示。

步骤 2：单击【确定】按钮，即可打开【网段名称】对话框，在“请输入网段名称”文本框中输入网段名称，如图 4-56 所示。

步骤 3：单击【下一步】按钮，即可打开【接入公网类型】对话框，在其中选择“路由器（企业路由器、宽带路由器等）”单选按钮，如图 4-57 所示。

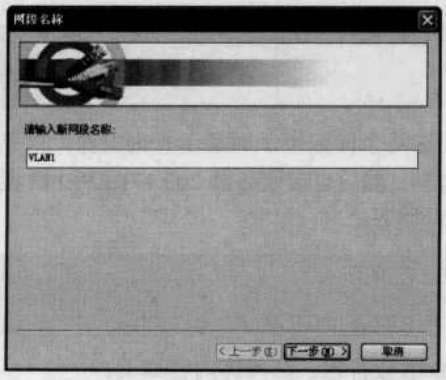


图 4-56 【网段名称】对话框

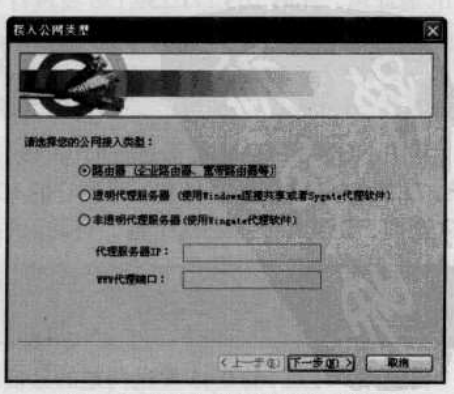


图 4-57 【接入公网类型】对话框

步骤 4：单击【下一步】按钮，即可打开【选择网卡】对话框，在“请为网段选择对应的

操作”下拉列表中选择对应网卡，可看到该网卡的信息，如图 4-58 所示。

步骤 5：在设置完毕之后，单击【下一步】按钮，即可打开【指定网段范围】对话框，在其中设置相应的 IP 地址范围，如 192.168.0.1 ~ 192.168.0.88，如图 4-59 所示。

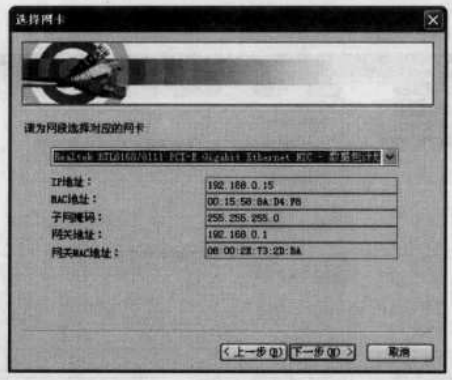


图 4-58 【选择网卡】对话框

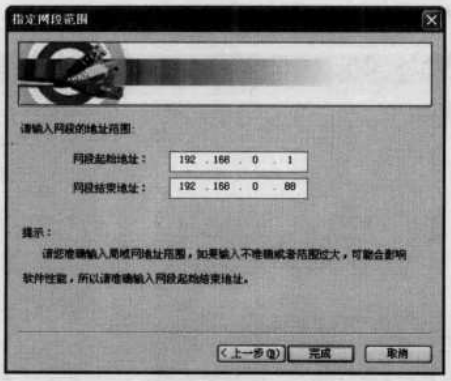


图 4-59 【指定网段范围】对话框

步骤 6：单击【下一步】按钮，即可打开【出口带宽】对话框，在“本网段局域网出口带宽接入带宽”下拉列表中选择“10Mps 及以上（办公局域网）”选项，如图 4-60 所示。

步骤 7：单击【完成】按钮，即可打开【监控网段配置】窗口，在其中选中要监控的网段，如图 4-61 所示。单击【开始监控】按钮，即可启动网络守护神服务，如图 4-62 所示。

图 4-60 【出口带宽】对话框

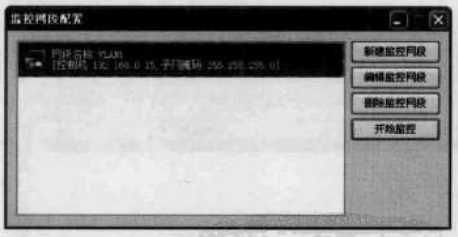


图 4-61 【监控网段配置】窗口

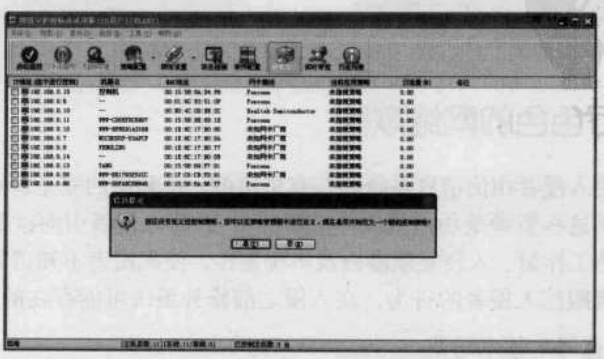


图 4-62 启动网络守护神服务

步骤 8：单击【信息提示】对话框中的【确定】按钮，即可打开【策略管理器】窗口，如图 4-63 所示。单击【新建策略】按钮建立一个策略，在【网络守护神】主窗口中单击【软件配置】图标，即可打开【软件选项】对话框，在其中可以对软件的各种性能进行设置，如图 4-64 所示。

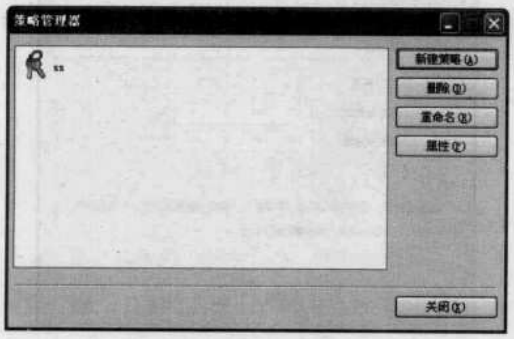


图 4-63 【策略管理器】窗口

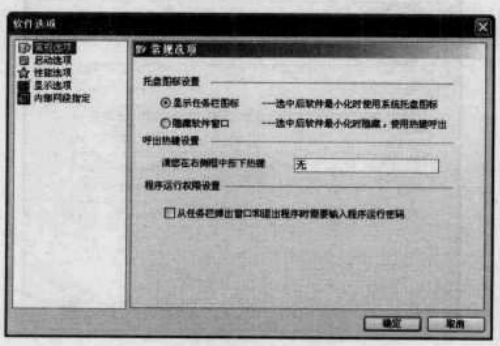


图 4-64 【软件选项】对话框

步骤 9：在【网络守护神】主窗口中单击【攻击检测】图标，在【网络攻击检测】对话框中单击【开始】按钮，即可进行扫描，其扫描结果如图 4-65 所示。单击【IP 绑定】图标，即可打开【IP-MAC 地址绑定设置】对话框，在其中勾选“启用 MAC-IP 地址绑定”复选框，可以添加 MAC-IP 地址绑定，如图 4-66 所示。

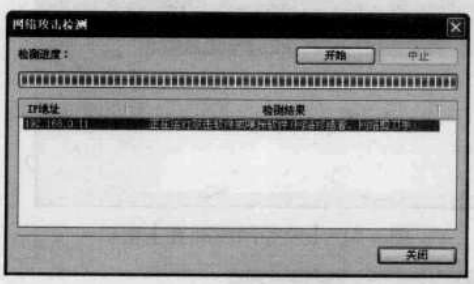


图 4-65 【网络攻击检测】对话框

图 4-66 【IP-MAC 地址绑定设置】对话框

第 33 招　行行色色的网络欺骗

网络欺骗就是使入侵者相信信息系统存在有价值的、可利用的安全弱点，并具有一些可攻击窃取的资源（当然这些资源是伪造的或不重要的），并将入侵者引向这些错误资源。它能够显著地增加入侵者的工作量、入侵复杂度以及不确定性，使入侵者不知道其进攻是否奏效或成功。而且允许防护者跟踪入侵者的行为，在入侵之前修补系统可能存在的安全漏洞。

1．网络游戏“盗号”骗术防范

所以每个玩定都对自己游戏中的角色格外关注，一旦不小心被别人盗取了号码或盗取了自

己游戏角色身上的优秀装备，就会有痛不欲生之感，懊恼之极。为了提高广大游戏玩家的防盗意识，往往需要掌握一定的防盗技巧。

1）用木马盗号。使用木马盗取玩家号码是黑客最常用的一种方法，尤其是在一些公共网络场所。有人会故意在某台机器中种上木马，然后等待其他人使用这台机器玩网络游戏，一旦使用者输入了自己的游戏账号和密码，木马程序就将自动记录下账号与密码，并保存到本地磁盘某个隐藏的文件夹中，或直接发送到种植木马者的电子邮箱中。

针对这种情况，建议用户在使用电脑之前先使用杀毒软件进行查杀，特别是在公共场所使用电脑更应如此。如果为了节省时间，则可使用一些木马专杀工具，减少查杀时间。如果使用的是自己的电脑，建议安装防火墙和杀毒软件并定期查杀，从而拦截木马和病毒的入侵，使用防火墙不仅可以拦截已知木马，还可以在新型木马访问网络时提醒用户，帮助用户识别。

下面介绍手工删除传奇木马的操作方法（本操作适用于 Windows NT/2000/XP/2003 操作系统），具体的操作步骤如下。

步骤 1：按“Ctrl+Alt+Del”组合键打开“Windows 任务管理器”窗口，在其中选择“进程”标签，将传奇木马进程 intren0t.exe 结束。

步骤 2：使用“我的电脑”窗口进入系统所有文件夹（Winnt 或 Windows）中，找到 intren0t.exe 文件将其删除。

步骤 3：打开【注册表编辑器】窗口，展开到 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run 项，将右侧窗口中的"intren0t"="%SystemRoot%\intren0t.exe"删除。再展开到 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run Services 注册表项，将右侧窗口中的"intren0t"="%SystemRoot%\intren0t.exe"删除。

2）远程控制方式盗号。通过远程控制方式可以远程查看和控制目标主机（肉鸡），从而拦截用户的输入，记录用户的游戏账号和密码。针对这种方式，用户同样可使用防火墙和杀毒软件进行查杀，因为现在很多杀毒软件都将具有恶意的远程控制软件加到了病毒库中，一旦发现本地计算机中运行这些程序，就会立即报告并清除。

3）利用系统漏洞盗号。这是一种通过系统漏洞在肉鸡中植入木马或远程控制工具，然后通过第一种或第二种方式进行盗号的活动。针对这种方式，用户可经常利用系统漏洞扫描工具，扫描自己的系统，发现漏洞应及时下载并安装相应的补丁，使盗号者无漏洞可以利用，保护自己的游戏账号与密码的安全。

2．网站上的钓鱼术

由于很多网络游戏都是需要使用充值卡进行充值后才能正常玩，所以有些不法分子就打起了欺骗充值而获得不法收入的主意。这些不法分子注册与游戏商网站相似的域名，并抄袭制作出与游戏商网站完全一致的操作界面欺骗迷惑广大游戏爱好者，使不知情者前往充值，从而达到骗取点卡和游戏账号与密码的目的。

（1）欺骗原理

以网易游戏《大话西游 OnlineII》为例，网易点数卡充值查询中心网站域名为 http://pay.163.com，而曾经欺骗广大用户的非法网站域名为 http://www.pay163.com。若充值者不注意辨别，就可能将该网站错当是网易游戏《大话西游 OnlineII》的充值网站。

还有一些欺骗网站与官方网络游戏网站首页完全相同，各项链接也正确链接到官方网站，但在主页公告中增加一条虚假有奖消息，点击后进入填写资料页面并说明填写后可以中奖。如果用户相信了该虚假消息并真实填写了相应资料内容，就会造成游戏账号与密码的丢失。

（2）防范方法

针对欺骗网站的情况，建议广大网络游戏玩家采取如下措施，避免上当。

1）充值时不要轻信任何非官方网站表单提交程序，一定通过搜索引擎等方式进入网络游戏公司正式页面以确保不会有危险。

2）发现欺骗网站后应及时向网络游戏公司举报，让网络游戏公司对非法网站采取屏蔽等措施，避免其他不知情玩家受骗。

（3）提高防范意识

除伪造网页外，还有些冒充网游管理员骗取玩家的账号和密码。如盗号者申请“发奖员”、“点卡验证员”等名字，利用信件频道发送一些虚假中奖消息，骗取玩家账号和密码。为防止上当受骗，广大网游玩家应具有如下防范措施：

1）在游戏中一般只有一个名字叫“游戏管理员”，其他任何名称都是假冒的，而且“游戏管理员”在游戏中一般不会向用户索取账号和密码的。

2）在游戏中如果有必要索取玩家的账号和密码进行查询时，管理员只会在游戏频道中与用户联系，不会经过其他任何途径索取玩家游戏账号和密码。

3）任何与中奖有关的信息，网游公司只会在主页以公告形式向广大用户公布，不会在游戏中直接与玩家联系。

4）如果用户在游戏过程中发现有人给自己发送中奖消息，应该马上与在线管理员联系，让网游公司进行处理。

建议广大玩家经常登录游戏官方网站，查看有无盗号的相关通知和公告。一般来说，网游公司会在发现黑客的第一时间告诉大家。只要广大玩家随时提高警惕，出现错误登录非法网站从而导致账号丢失的可能性就相当小了。

3. 游戏账户破解防范

现在绝大多数网站与网络游戏登录界面上都有“记住密码”功能，若用户使用了该功能，黑客就可能会利用一款专用工具，提取保留的用户账号与密码，从而实现盗取用户密码。

下面以 Cain V4.9 汉化版为例介绍从缓存提取用户账号与密码的具体方法。

步骤 1：下载并解压后，先安装 WinPcap，双击 svchost.exe 图标进入其操作界面，如图 4-67 所示。

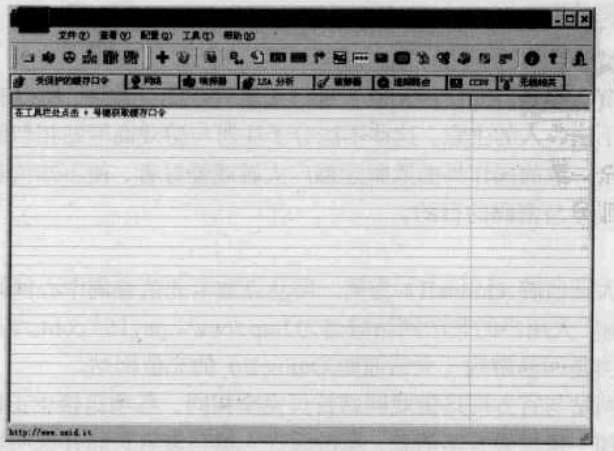


图 4-67　Cain 主界面

步骤 2：单击工具栏上的【添加到列表】按钮 ✚ 即可提取缓存中的账号和密码。由此可以看出，用户最好还是不使用“记录密码”功能为妙。

为了防止自己登录网站或游戏的账号与密码被盗，需记住如下几点防范措施：

1）尽量不要将账号暴露在公共论坛和其他网站，更不要使用“记住密码”功能。

2）在设置密码时尽量设置得复杂一些，位数应在 8 位以上，且数字、字母和其他字符混杂。

3）不要使用可轻易获得的关于自己的信息作为密码，如生日、身份证号码、手机号码、居住的街道名称、门牌号码等。

4）要经常更换密码，因为再复杂的密码也是可以被破解的，所以经常更换密码可以提高密码的安全系数。

5）申请密码保护，也就是设置安全码，安全码不要与密码相同。如果没有设置安全码，别人一旦破解了密码就可以修改全部个人资料与登录密码。

6）进行完善的用户登录权限和软件安装权限管理，并尽可能地使用一些锁定软件在短暂离开时锁定计算机，避免其他人非法使用自己的计算机。

第 34 招　密码大盗的伪装账户

“密码大盗”是一款专门用于盗取 Windows 2000/XP 管理员密码的软件，可以将其视为木马的一种，这里因为它具有木马那种隐蔽性的特征。密码大盗植入的方法有本地和远程两种，需要先了解密码大盗的这两种用法后，才能采取不同的措施将其“绳之以法”。

1. 本地植入密码大盗

使用密码大盗进行“本地植入”的操行非常容易，这种方法是指黑客在当前计算机上进行密码大盗的植入后，窃取系统管理员密码的过程（如使用普通权限的账户登录被入侵主机后，再使用密码大盗进行管理员级别的账户窃取）。具体的操作步骤如下。

步骤 1：从网上下载并解压“Windows 密码大盗”压缩文件，双击“密码大盗”应用程序图标，会发现文件没有什么反应，只是鼠标的光标稍微动了一下，其实这时“Windows 密码大盗”已经自动在系统中增加了一个超级用户名称“admin”，其密码为“stgzs”。选择【开始】→【设置】→【控制面板】→【管理工具】菜单项，即可打开【管理工具】窗口，如图 4-68 所示。

步骤 2：双击“计算机管理”图标，即可进入【计算机管理】窗口，展开“系统工具”→“本地用户和组”→“用户”选项，即可在右侧列表中看到刚添加的“admin”账户，如图 4-69 所示。

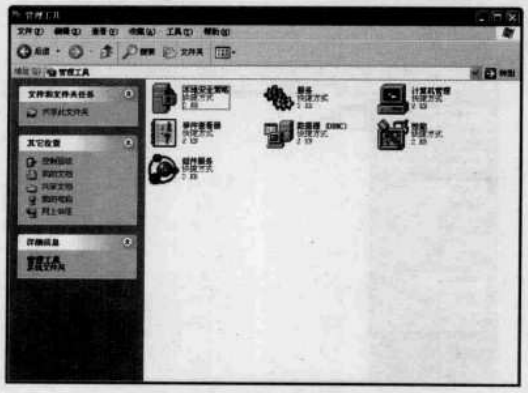


图 4-68　“管理工具”窗口

图 4-69　“计算机管理”窗口

步骤 3：双击“Admin”这个账户，即可弹出【Admin 属性】对话框，切换至“隶属于”选项卡的设置界面后，就会发现这个账户是属于“Administrator”组的（即拥有系统管理员权限），如图 4-70 所示。这个隐藏“admin”账户可使任何人轻松地以系统管理员身份进入系统，而不必再考虑原有的管理员密码是多少。但如果系统中不允许设置管理员账户，则这个账户将看不到。

步骤 4：如果看不到这个“admin”账户，黑客就会等待管理员在重启计算机后用管理员账户进入一次系统后，让“Windows 密码大盗”存放管理员密码的目录“C:\Windows\Temp\”中打开 Config.ini 文件，就可以获取管理员密码了，如图 4-71 所示。

图 4-70 【Admin 属性】对话框

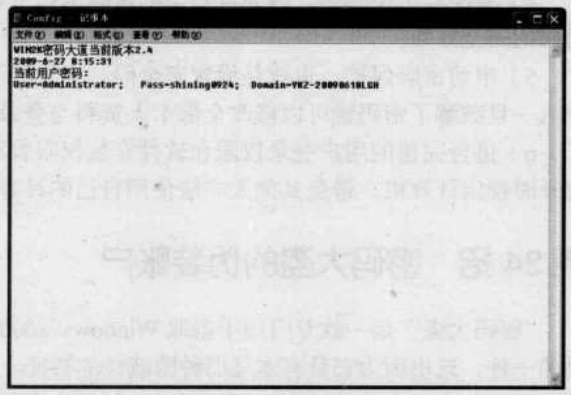


图 4-71 密码显示结果

由上图可以很清楚地显示出当前的用户名是 Administrator，密码是：shining0924。本地植入木马破解系统管理员密码的方法很简单，除随时查看系统中是否有多出来的系统管理员外，还应采取对系统进行严格的使用权限控制和全面加密措施，才能防患于未然。

2. 远程植入密码大盗

再来看看远程植入“密码大盗”的方法，其实远程破解很容易实现，比如在扫描到具有共享漏洞的计算机后，就可以进行相应破解操作。

（1）检查病毒防火墙

在植入木马之前，有经验的黑客往往会先对对方计算机中的病毒防火墙搞些小破坏，比如个人用户常用的瑞星防火墙的安装目录通常在类似于“D:\Program Files\rising\rav”的目录中，黑客就会采取将该目录中的文件“删除”等方法来使程序成为“空架”，如图 4-72 所示。

图 4-72 瑞星防火墙的安装目录

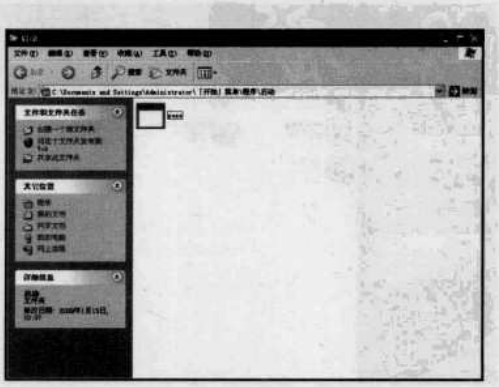


图 4-73 “启动”窗口

（2）植入木马

解除病毒防火墙威胁后，就可以植入“Windows 密码大盗”了。在本机中进入入侵计算机的“C:\Documents and Settings”目录中，查看哪个账户的桌面图标最多，就进入哪个账户的“开始”→“程序”→“启动”目录，并将其设置为隐藏属性的“Windows 密码大盗”程序拷贝到该目录下，如图 4-73 所示。

当被入侵计算机的管理员再次重启系统后，就可以伺机再次利用共享漏洞登录被入侵计算机，并打开“Windows 密码大盗”的密码存放文件，从而获得登录密码。

3．密码大盗防范对策

通过本地和远程植入密码大盗后看到的效果，是不是感觉危险无时不在呢？针对密码大盗的防范，建议从如下几个方面进行。

（1）查看组用户

这个方法比较直观，对于新手来说也很容易。下面以 Windows XP 为例，具体的操作步骤如下。

步骤 1：选择【开始】→【程序】→【控制面板】→【管理工具】菜单项，即可打开【管理工具】窗口。双击“计算机管理”图标，即可进入【计算机管理】窗口。依次展开【计算机管理（本地）】→【系统工具】→【本地用户和组】→【组】选项，即可在右侧的组列表中看到 Administrator 组的存在，如图 4-74 所示。

步骤 2：双击组列表中的“Administrator”项，即可弹出【Administrator 属性】对话框，在其中可看到这个组中的所有成员，从这里就可以判断出管理员组中是否存在非法用户，如图 4-75 所示。如果发现存在非法用户服务，如密码大盗私自添加的“Admin”账户，就应该立即选中这个账户并单击下方的【删除】按钮将其删除。

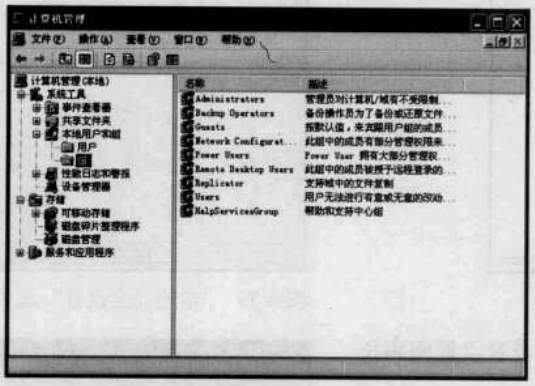


图 4-74 “计算机管理”窗口

图 4-75 【Administrator 属性】对话框

（2）关闭普通用户

一个管理严格的计算机系统通常不会允许有普通用户存在，因为这样会带来诸多安全隐患，所以应采取关闭普通用户或停止使用普通用户来使危险得以下降。

具体的操作步骤如下。

步骤 1：在“计算机管理”窗口中展开【计算机管理（本地）】→【系统工具】→【本地用户和组】→【用户】选项，即可在右侧的组列表中看到所有存在的用户，如图 4-76 所示。

步骤 2：双击任意一个普通用户（如选择“Admin”用户），即可弹出【Admin 属性】对话框，在“常规”选项卡中选择“账户已停用”选项，如图 4-77 所示。

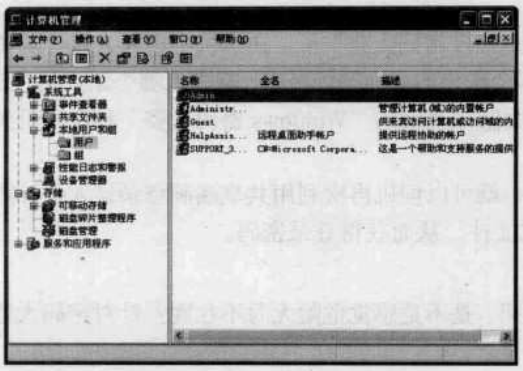


图 4-76　展开“用户”选项

图 4-77　【Admin 属性】对话框

（3）组策略

在组策略中可通过一些选项的设置来管理账户。具体的操作步骤如下。

步骤 1：在【运行】对话框的“运行栏”中输入“Gpedit.msc”命令，即可打开【组策略】管理窗口，如图 4-78 所示。展开【计算机配置】→【Windows 设置】→【安全设置】→【账户策略】→【密码策略】选项，即可在右侧列表中查看密码的所有策略方式。

步骤 2：若在右侧列表中双击“密码长度最小值”选项，即可弹出【密码长度最小值 属性】对话框，再在“本地安全设置”选项卡中设置“不要求密码的字符数”，如图 4-79 所示。

图 4-78　“组策略”管理窗口

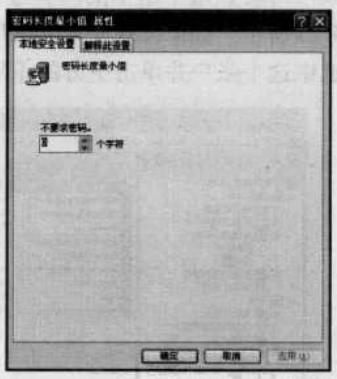


图 4-79　“本地安全设置”选项卡

步骤 3：在“解释此设置”选项卡中可查看设置密码长度具体要求，如图 4-80 所示。

图 4-80　“解释此设置”选项卡

（4）打补丁

安全漏洞原因在于访问本地及远程文件时所使用的“Windows redirector”。由于 Windows XP 中的 Windows redirector 存在未经检测的缓冲器，因此如果有人发送某些特定的数据，就会引起缓冲器溢出，从而导致 OS 异常关闭，或者执行任意指令。

要想恶意使用此漏洞，就必须以对话的形式登录到对象计算机中，然后运行使用 Windows redirector 的程序（比如“Net Use”命令），并将特定数据读取到 Windows redirector

中。另外，无法远程通过网络发动攻击。因此，恶意使用此漏洞的后果是普通用户（或者知道普通用户账号的攻击者）能够取得高于允许权限的“管理员权限”，即“权限提升”。提升权限后，就会允许普通用户变更原本不允许的设置以及运行原本不允许运行的程序等。

对策为安装微软公开的补丁程序。补丁程序可以在 Windows XP 或 Windows XP SP3 环境下安装，还可以通过“Windows Update”安装。此漏洞的严重等级为“重要”，这里建议大家最好要安装。可以发现在 Windows XP 这样安全性已相当高的操作系统中，都会出现账户的漏洞，并且这个漏洞只需黑客有普通用户的权限就可以利用其取得管理员权限了。

针对这个防不胜防的漏洞隐患，及时打好相应的补丁程序就是最好的防范措施。另外，为了不让他人恶意地利用一些安全漏洞，将能够登录到机器上的用户设置为必要的最低权限、正确实施密码管理、在屏保中设置密码等措施，都是值得推荐使用的最基本措施。

第 35 招　Foxmail 账户解除与防范

电子邮件容易暴露人们隐私，能够泄漏邮箱主人邮件内容、电话号码等很私密的东西。下面以国产最著名的免费邮件收发软件 Foxmail6.0 为例，谈谈如何防范邮箱使用口令、账户及密码防止被窃的方法。

1．邮箱使用口令的安全防范

先来了解一下 Foxmail 中邮箱账户使用口令的破解与防范。需要声明的是，对于以下即将了解到的破解 Foxmail 中邮箱账户访问口令知识，希望读者能通过此口令的破解过程知道如何善用这个方法（比方说口令遗忘时），以及学会如何防范这个可能带来的危险。

（1）Foxmail6.0 账户访问口令的设置

在使用 Foxmail6.0 之前应先对其进行相应的设置。

具体的操作步骤如下。

步骤 1：下载并安装“Foxmail6.0”软件，双击桌面上的“Foxmail6.0”应用程序图标，即可弹出【创建新用户账户向导】对话框，在其中填写需要创建的账户名称和密码等，如图 4-81 所示。

步骤 2：单击【下一步】按钮，即可打开【指定邮件服务器】对话框，在其中选择接收邮件服务器的方式、邮件的帐户以及发送邮件所采用的服务器等，如图 4-82 所示。

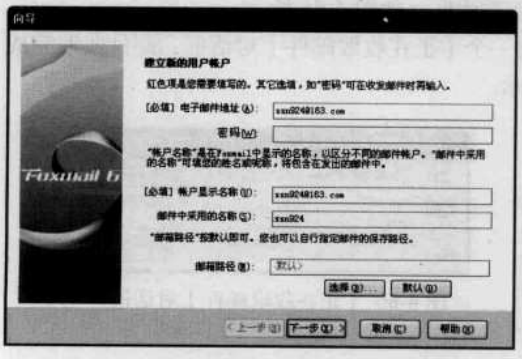


图 4-81 【创建新用户账户向导】对话框

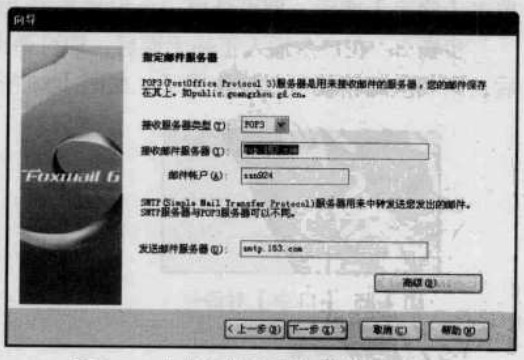


图 4-82 【指定邮件服务器】对话框

步骤 3：继续单击【下一步】按钮，即可打开【账户建立完成】对话框，如图 4-83 所示。

在成功创建用户账户后，再详细地讲述采用“Foxmail6.0”邮箱账户访问口令的具体设置过程了。具体的操作步骤如下。

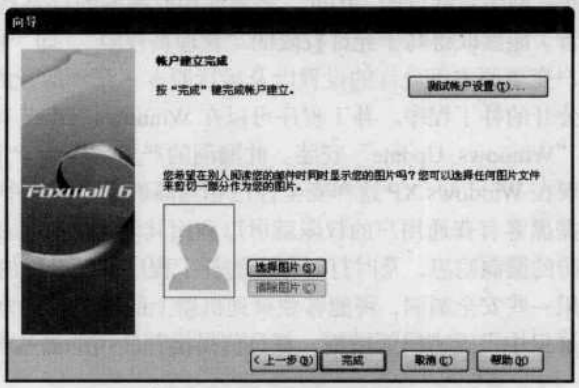


图 4-83 【账户建立完成】对话框

步骤 1：单击【完成】按钮，即可进入“Foxmail”主窗口。在左侧“邮箱账户”列表中右击选中任意一个建立好的邮箱账户，从快捷菜单中选择“设置账户访问口令（A）”菜单项，如图 4-84 所示。

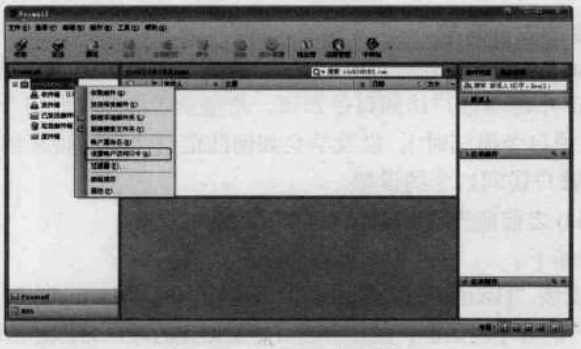


图 4-84 “Foxmail”主窗口

步骤 2：稍后将弹出【口令】对话框，在“请输入口令”文本框中输入所需要的口令后，单击【确定】按钮，即可结束口令设置并关闭该对话框，如图 4-85 所示。

步骤 3：在口令输入正确无误后，即可弹出一个【正在收取邮件】对话框，邮件收取完成后，则相应邮箱就可以被使用了，如图 4-86 所示。

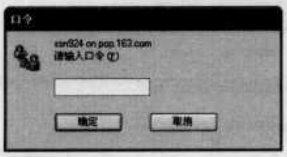


图 4-85 【口令】对话框

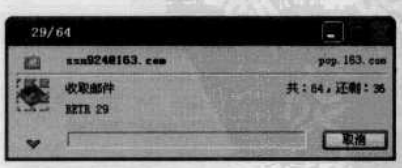


图 4-86 【正在收取邮件】对话框

（2）口令的破解

口令破解如果是针对他人的邮箱账户而言，是一种违法行为。但如果是因自己邮箱访问口令遗忘等原因，而破解自己邮箱账户访问口令则是一种合法行为。

破解 Foxmail 中邮箱账户的访问口令很容易，可通过 Foxmail 为每个邮箱账户设计的配置文件“Account.stg”来完成。配置文件可通过路径“C:\Program Files\Foxmail\Mail**** //****

为邮箱账户名”来找到。在类似路径中找到 Account.stg 文件后用“写字板”程序打开，即可发现其中记录此账户包括账户访问口令、邮箱地址、邮箱密码在内的基本设置，如图 4-87 所示。

既然这个文件包含了邮箱账户访问口令在内等信息，那么就可以通过在 Foxmail 中新建一个不设置访问口令的邮箱账户，将该账户下的“Account.stg”文件复制到设置口令的账户目录中，覆盖“Account.stg”文件即可清空访问口令了，如图 4-88 所示。

（3）防范

针对“Account.stg”文件带来的安全隐患，可以采用“删除账户”的方法来防范非法用户盗用账户。这是一种彻底的防范方法，删除的操作步骤如下。

步骤 1：在 Foxmail 中选中想要删除的账户，单击【账户】→【删除】菜单项，即可将 Foxmail 窗口中的账户删除。

图 4-87 利用写字板打开“Account.stg”程序

图 4-88 复制“Account.stg”文件到口令账户目录中

步骤 2：在“C:\Program Files\Foxmail\Mail\”目录中找到在 Foxmail 窗口中删除的账户同名目录，按“Ctrl+Delete”组合键将其删除。

2. 邮箱账户密码的防范

如果计算机是多用户环境，强烈建议不要在 Foxmail 中建立用户时将邮箱密码也同时设置，因为这也将会使邮箱密码拱手送人。Foxmail 将密码进行简单加密后保存在“Account.stg”文件中，只要知道加密的算法及密钥，即可轻松得到该邮箱的密码以及其长度。

对于不知道算法的初级用户，网上还有很多可以利用 Foxmail 窃取邮箱密码的程序来得到邮箱密码。所以在多用户共同使用一台计算机的环境下，强烈建议不要设置远程邮箱密码，以免邮箱因密码失窃而永远消失。

第 36 招 防范邮箱账户欺骗

邮箱账户欺骗是指伪造邮箱地址发信给他人的行为，这种行为可以是恶意的，也可以用来保护自己。

1. 伪造邮箱账户

邮件地址欺骗是非常简单和容易的，攻击者针对用户的电子邮件地址，取一个相似的电子邮件名（如将“发件人姓名”配置成与用户一样的发件人姓名），然后冒充该用户发送电子邮件，在他人收到邮件时，往往不会从邮件地址、邮件信息头等上面做仔细检查，从发件人姓名、邮件内容等上面又看不出异样，误以为真，攻击者从而达到欺骗的目的。

人们通常以为电子邮件的回复地址就是它的发件人地址，其实不然，发件人地址和回复地址可以不一样，熟悉电子邮件客户端使用的用户也会明白这一点，在配置账户属性或撰写邮件时，可以指定与发件人地址不同的回复地址。

由于用户在收到某个邮件时，虽然会检查发件人地址是否真实，但在回复时并不会对回复做出仔细检查，如果配合 SMTP 欺骗使用，发件人地址是攻击者自己的电子邮件地址，就会具有更大地欺骗性，诱骗他人将邮件发送到攻击者的电子邮箱中。

现在以一个无需 SMTP 服务器中转即可将邮件直接发送到目的邮件地址的软件为例，进行伪造邮箱账户并发送邮件。通过这类软件发出的信件对方往往立即可以收到，并且可以任意设定发件人邮箱地址，这就给伪造邮箱账户创造了条件。

发信人地址是随意取的，而收信人地址则是真实的。正常情况下，是无法完成这个发信操作的——因为没有这个发信人地址的存在。但是通过上图中这类特殊的邮件收发软件就可以完成邮件的发送，而收件人则立即会收到伪名发送的邮件。上述的方法是目前最常见的垃圾邮件发送方法，也是比较恶劣的一种伪造邮箱账户行为。

2．隐藏邮箱账户

有时伪造邮箱账户会带来很多好处，这就像一把枪，在战士手里就是保家卫国的武器，在劫匪手里就是一把凶器。在有些必须要输入电子邮箱地址却又对自己毫无作用的情况下，如在各大论坛注册时、申请某种网络服务时等。这个时候就可以通过伪造或隐藏邮箱账户的方法巧妙地达到“欺骗”的效果。

隐藏自己的电子邮件地址有如下两种方法。

1）干脆来个假邮箱地址，在各大论坛等需要注册时填写邮箱的地方使用。

2）使用小技巧，如将 ssn@public.sq.js.cn 在输入时改成 ssn public.sq.js.cn，大家都会知道这个实际上就是邮箱，但一些邮箱自动搜索软件却无法识别这样的“邮箱”了。

3．追踪仿造邮箱账户发件人

绝大多数接收的邮件都有源 IP 地址内嵌在完整地址标题中，以帮助标识电子邮件的发送者并跟踪到发送者的服务提供商。

在 Foxmail 中可使用查看“邮件”→“邮件信息”→“原始信息”方法来查看详细的发送者 IP 及其邮件地址。如果在接收的垃圾邮件中缺少源 IP，则垃圾邮件的发送者在垃圾邮件中伪造了邮件标题。

对于这类使用“连环跳板”式发来的邮件还是直接在 Foxmail 等软件中将其邮件主题设置成过滤状态比较现实一些，如图 4-89 所示。

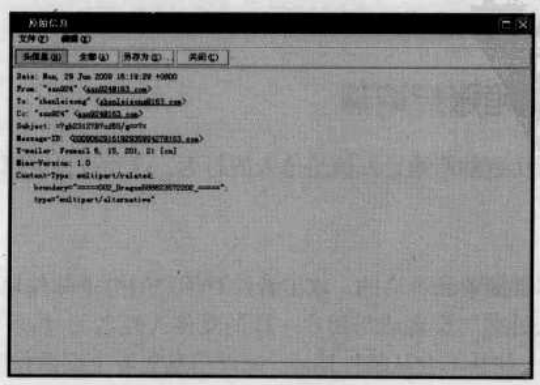


图 4-89 “原始信息”窗口

4. 防范垃圾邮件

网络中这些令人闻风色变的垃圾邮件，以其难以测知的真实邮箱地址让人怒火中烧，却又无可奈何。比较实际的方法，还是先来使用如下这些方式来做到防范于未然。

（1）垃圾邮件及其特征

垃圾邮件是指未经收件人允许或不知情情况下，以匿名或伪名的方式，给众多非法获知（恶意搜索或购买而得）的邮箱重复发送的邮件（如对同一邮箱重复发送 100 次广告邮件）。这种邮件具有如下主要特征：

- 无目的性和恶意性。
- 没有邮件信头或使用特殊的邮件信头。
- 伪造发件人。如发件人是收件人的邮箱地址。
- 经过很多的服务器转发，从而具有反追踪效果。
- 要求确认。如信件内容带有允许收件人不再接受此类邮件的描述，很多收件人信以为真，在回信表示不愿意接收信件后，结果让发送垃圾邮件者轻易知晓其邮箱真实存在。

垃圾邮件对每个网民来说都是有害的，会使网民的邮箱空间被恶意填满，从而导致真正有用的信件无法接收。其实垃圾邮件还往往具有携带病毒的特点，会使用户的邮箱甚至系统瞬间瘫痪掉。因此，作为普通的邮箱使用者，也应尽可能地做好反垃圾邮件的种种措施，采取以逸待劳的方式，让垃圾邮件来势汹汹却不能憾泰山分毫。

（2）Foxmail 防范设置

1）远程管理。远程管理功能可以远程决定邮件服务器上的邮件收取与否。如果发现接收的邮件头明显具有垃圾邮件的特征，立即单击【删除】按钮将其在远程删除掉。

2）反垃圾邮件设置。在 Foxmail 中可以通过规则过滤、贝叶斯过滤等方法，对接收的邮件进行判断识别出是否为垃圾邮件，如果是垃圾邮件将会自动分捡到垃圾邮件箱中，从而最大程度地实现了与垃圾邮件对抗的效果。

在 Foxmail 主窗口中选择【工具】→【反垃圾邮件设置】菜单项，即可进入“反垃圾邮件设置”对话框，在其中可以看到多项有关垃圾邮件防范的设置项，如图 4-90 所示。

3）规则设置。这是指 Foxmail 使用内置的“规则库”对邮件进行对照评估。在“规则过滤”选项卡中勾选“使用规则判定接收到的邮件是否为垃圾邮件”复选框，再根据当前邮箱遭受垃圾邮件“骚扰”的程度来决定“过滤强度”的强弱，如果垃圾邮件“铺天盖地”，则设置强度应为“高”最合适，如图 4-91 所示。

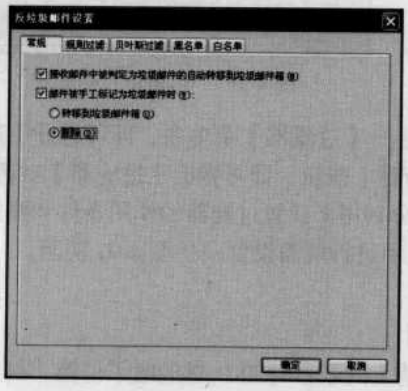


图 4-90 “反垃圾邮件设置”对话框

图 4-91 “规则过滤”选项卡

4）贝叶斯过滤。这是一种智能型反垃圾邮件设计，通过让 Foxmail 对垃圾与非垃圾邮件的分析，来提高自身对垃圾邮件的识别准确率，如图 4-92 所示。若单击【学习】按钮，则会弹出【向导】对话框，在其中可以对邮件做出相应设置，如图 4-93 所示。

图 4-92　设置贝叶斯过滤条件

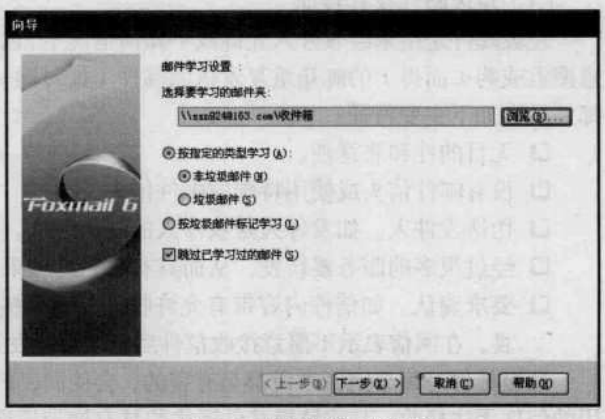


图 4-93 【向导】对话框

5）黑名单。只需将一些确认为垃圾邮件的地址输入到黑名单中，即可完成对该邮件地址发来的所有邮件监控，如图 4-94 所示。

6）白名单。这是一种强制性认为是非法垃圾邮件的设计，在默认情况下，Foxmail 会自动导入已被允许接收的邮件发出地址，如图 4-95 所示。

图 4-94　设置黑名单

图 4-95 “白名单”选项卡

7）过滤器设置。选中任一个账户，选择【邮箱】→【过滤器】菜单项，即可打开【过滤管理器】对话框，如图 4-96 所示。单击左下角的【新建】按钮，即可弹出【过滤器】对话框，可以看出过滤器由条件选项和执行选项两部分组成，分别用来设置过滤器的作用条件和要执行的操作。由于设置非常简单，所以任何人均可立即上手进行所需设置，如图 4-97 所示。

5．邮箱使用规则

根据经验，下面介绍两条最常用的邮箱使用原则。

1）不要将自己的邮箱地址到处传播。特别是申请上网账号时 ISP 送的电子信箱，例如微软新闻组中就绝对不能用重要邮箱注册，否则潮水般涌来的垃圾邮件会让大家后悔莫及。

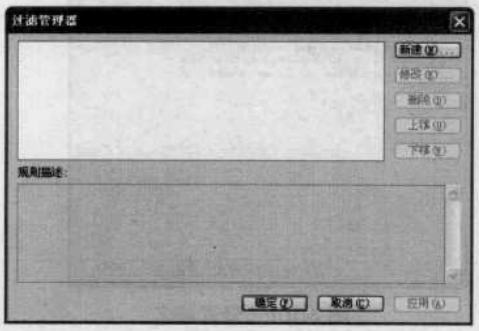


图 4-96 【过滤管理器】对话框

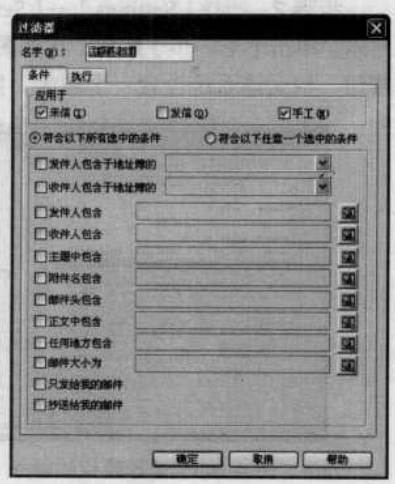


图 4-97 【过滤器】对话框

2）不要回复垃圾邮件。如果收到了垃圾邮件，请不要给发件人回复或使用任何包含在垃圾邮件中的命令。任何回信或命令的使用，都可能会告知垃圾邮件发件者邮箱地址“真实有效”，这样的邮箱地址将被放置在更多垃圾邮件列表中，将会有更多垃圾邮件和用户亲密接触。

第 37 招 蜜罐 KFSensor 很诱人

“蜜罐”技术可以模拟出一个充满漏洞的系统，当恶意入侵者得意洋洋时，用户却早已为反攻赢得了宝贵的时间。蜜罐好像是故意让人攻击的目标，引诱黑客前来攻击。所以攻击者入侵后就可以知道其是如何得逞的，随时了解针对公司服务器发动的最新攻击和漏洞。还可以通过窃听黑客之间的联系，收集黑客所用的种种工具，并且掌握其社交网络。

1. 蜜罐设置

KFSensor 是一款基于 IDS 的安全工具，通过模拟 FTP、POP3、HTTP、Telnet、SMTP 等服务，吸引黑客的攻击。通过详细的安全检测报告，实时监测本地计算机。

具体的操作方法如下。

步骤 1：用户从网上下载并安装后，选择【开始】→【程序】→【KFSensor】→【KFSensor】菜单项，即可进入其操作界面，如图 4-98 所示。

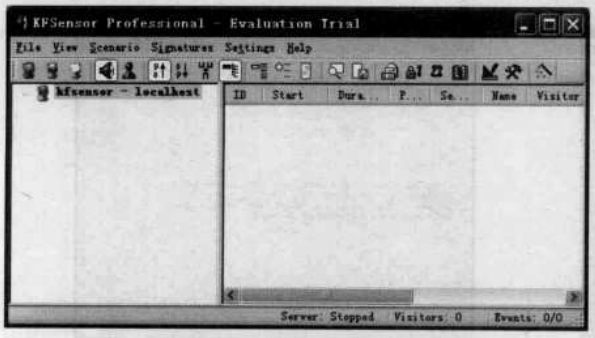


图 4-98 “KFSensor”界面

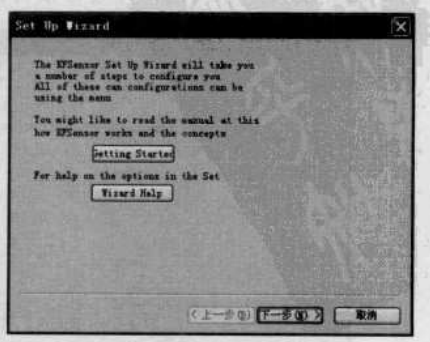


图 4-99 蜜罐设置向导

步骤 2：选择【Settings】→【Set Up Wizard】菜单项，即可打开设置向导对话框，如图 4-99 所示。单击【下一步】按钮，在如图 4-100 所示对话框中选择需要的模拟服务。单击【下一步】按钮，给蜜罐系统设置一个域名，如图 4-101 所示。

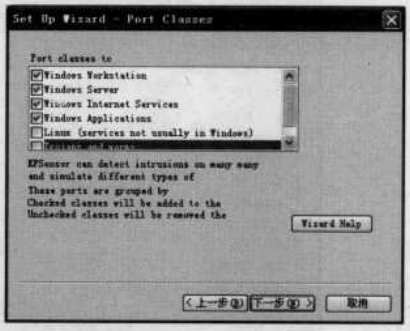


图 4-100　选择模拟的服务

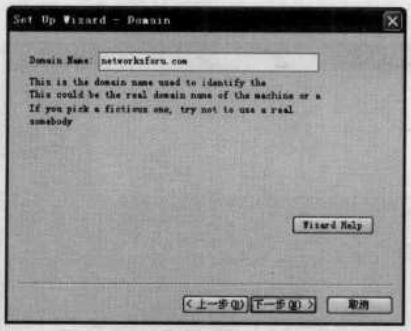


图 4-101　设置域名

步骤 3：单击【下一步】按钮，在其中可以输入的 E-mail 地址，使 KFSensor 能够向该邮箱发送记录信息，如图 4-102 所示。

步骤 4：单击【下一步】按钮，在如图 4-103 所示对话框中设置有关伪装系统的选项。单击【下一步】按钮，在其中勾选“Install as systems service”复选框，如图 4-104 所示。

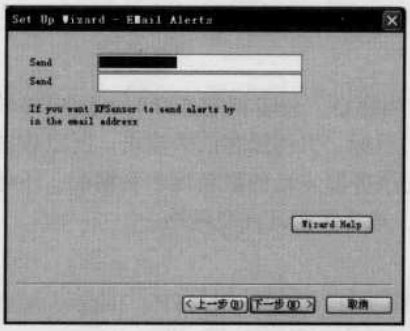


图 4-102　输入邮箱地址

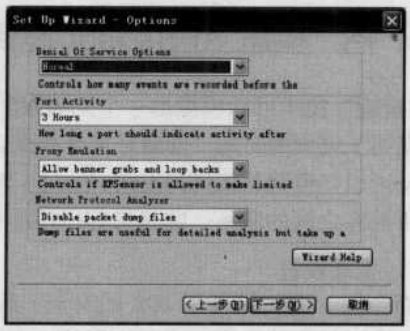


图 4-103　设置有关选项

步骤 5：单击【下一步】按钮，再单击【完成】按钮，即可结束设置向导，如图 4-105 所示。单击工具栏上的【Start Server】按钮，即可启动蜜罐程序。当 KFSensor 发现有人扫描本机时，图标就会变成红色，并进行报警，可以查看日志，了解黑客的扫描手法和入侵行为。

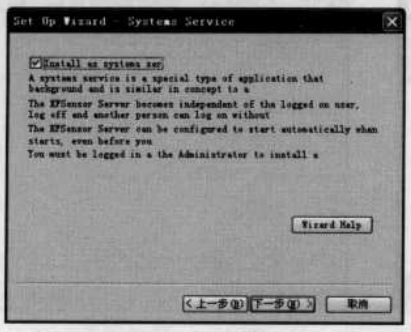


图 4-104　安装伪装系统

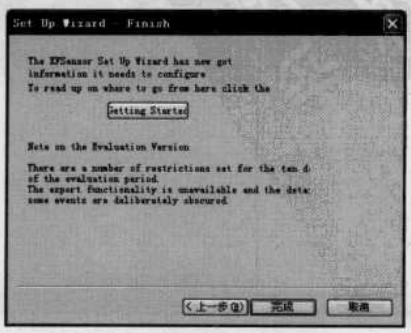


图 4-105　完成设置操作

此时若用扫描器工具对该主机进行扫描，就会发现开放的端口很多，几乎像一台刚装好系统和服务器软件的主机，连一些危险的端口都开放着，还可以扫描到 NT、FTP、SQL 弱口令、CGI、IIS 漏洞等，但这些都是 KFSensor 模拟出来的。

2．蜜罐诱捕

可先采用入侵者的身份对计算机进行扫描，利用 X-Scan、Spuerscan 等常用的端口扫描工具，在 IP 处填写本机 IP，将端口定义为 1～65525，单击【开始】按钮进行扫描，此时，可看到本地主机开放的端口很多，连一些危险的端口也都开放着。但这些开放的危险端口都是 KFSensor 模拟出来的，可以发现 NT、FTP、SQL 弱口令、CGI、IIS 漏洞等。

当发现有人扫描该计算机时，每扫描一个端口 KFSensor 将会对其进行实时记录，通知区域内的图标变成红色并闪烁，同时通过声音报警。此时可打开 KFSensor 的日志记录，分析黑客的扫描和攻击手法等信息。

KFSensor 分为三部分：工具栏、端口栏和日志栏。端口栏是模拟开放的一些端口，日志栏是入侵日志的记录，双击对应端口的日志，就可以看到里面详细记录了扫描的手法，经过上面的诱捕测试，可以确认蜜罐已经安装成功。

蜜罐技术可以通过诱导让黑客们误入歧途，消耗他们的精力，为网络管理员加强防范赢得时间，同时也是用来检验网络安全策略是否正确，防线是否牢固的得力助手。

第 38 招　用 Privacy Defender 清除痕迹

Privacy Defender 是一款能够真正在不重启系统情况下，擦除受系统保护的 index.dat 文件内容。这也是绝大多数 Internet 清除软件所不具有的能力。目前还没有发现有哪个软件能够做到这点。

1．Privacy Defender 安全演示

这里介绍 Privacy Defender 一个非常值得提倡的设计“功能演示”，这个设计可让使用者以最快速度学会软件的应用。打开演示功能的方法为，在如图 4-106 所示的主窗口中选择【工具】→【演示】选项。

图 4-106　主窗口

2．Privacy Defender 清除上网痕迹

经常上网的用户应该知道，在 Internet Explorer 中 index.dat 文件保存着所有 cookies 和历史记录以及缓存的索引。即使用户平时通过手工清理历史记录、删除所有 Internet Explorer 选项的 cookies 和缓存，这些操作均不能影响 index.dat 文件保留在曾经访问的网站列表中。

图 4-107 【选项】对话框

无法删除这些文件，主要因为它们是 Windows 操作系统的一部分，如果试图删除它们，系统会提示出错。但 Privacy Defender 可解决这一问题。单击【选项】按钮，在【选项】对话框中根据需要选择要删除的项，如图 4-107 所示。单击【确定】按钮，即可完成所有的 IE 相关访问痕迹的数据擦除，实现安全地上网。

第 39 招　安全管理 Administrator 账户

Administrator 是系统安装后默认的系统管理员账户，具有对系统进行一切管理的权限。以

Windows XP 为例，系统管理员可管理 Windows XP 中的所有用户，可安装和卸载系统内核级的程序，包括内置或第三方程序、网络设置、硬件驱动等；可使用系统中所有功能。扫描软件通常都是先对 Administrator 账户进行密码猜解，如果不对其进行适当保护将非常危险。

1．防范更改账户名

针对 Administrator 账户潜在的危险，可以采取一些操作简单也很实用的方法来解决这一问题，如将账户更名，可以降低遭受攻击的可能性。具体的操作步骤如下。

步骤 1：选择【开始】→【设置】→【控制面板】选项，即可打开【控制面板】窗口，如图 4-108 所示。

图 4-108 【控制面板】窗口

图 4-109 【管理工具】窗口

步骤 2：单击【管理工具】图标，即可打开【管理工具】窗口，如图 4-109 所示。再单击【计算机管理】图标，即可打开【计算机管理】窗口，如图 4-110 所示。

步骤 3：逐层单击依次展开【计算机管理】→【系统工具】→【本地用户和组】→【用户】选项，在右侧用户列表中可看到 Administrator 账户名已存在，如图 4-111 所示。

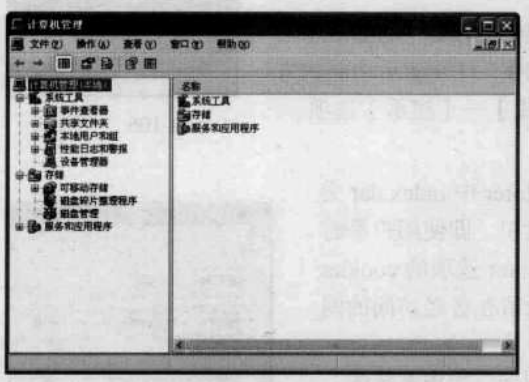


图 4-110 【计算机管理】窗口

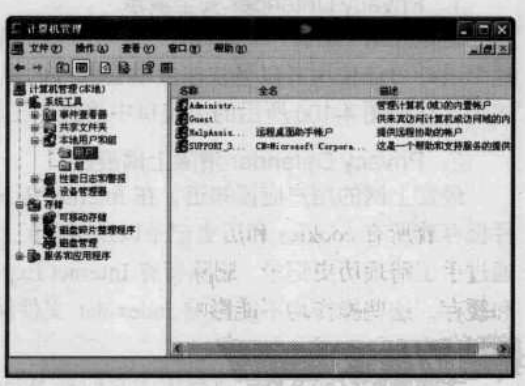


图 4-111 Administrator 账户名

步骤 4：在 Administrator 账户名上右击将弹出右键菜单，如图 4-112 所示。

下面介绍这一菜单中几个功能的作用。

1）设置密码。单击【设置密码】选项，即可打开【为 Administrator 设置密码】对话框，如图 4-113 所示。这是一个非常有用的功能。如果当前账户遗忘了密码，可以使用其他账户登录之后，使用此项功能将账户密码修改，以便当前账户可以继续使用。

2）删除。单击【删除】选项将弹出【本地用户和组】提示框，如图 4-114 所示。这是一种比较彻底的针对默认管理员账户进行安全管理的措施。单击【是】按钮，Administrator 账户将

会自动被删除。

图 4-112 右键菜单选项

图 4-113 【为 Administrator 设置密码】对话框

3）重命名。重命名功能可以对 Administrator 账户进行伪装，例如将 Administrator 账户名更改为“ssn”等无法辨识出属于管理员组的账户名，这样可以在一定程度上迷惑入侵者。

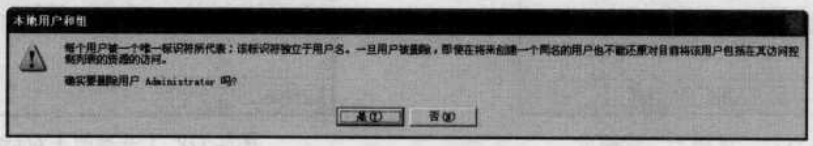


图 4-114 【本地用户和组】提示框

2．防范仿造陷阱账户

另建一个“Administrator”的陷阱账户，不赋予任何权限，并为之加上一个超过 10 位的超级复杂密码，再对该账户启用审核，这就会使一些黑客徒劳。具体的设置方法如下。

步骤 1：在如图 4-115 所示的用户列表空白处右击，在弹出菜单中选择【新用户】选项，即可打开【新用户】对话框。

步骤 2：在其中根据提示依次输入“用户名”、“全名”和“描述”等信息，其中“描述”输入“管理员”，而密码则应输入强度比较大的，如 16 位密码。选中“用户不能更改密码”复选框，可以防止密码被恶意修改，如图 4-116 所示。在设置完毕之后，单击【创建】按钮，即可成功创建一个名为“Administrator”的账户。

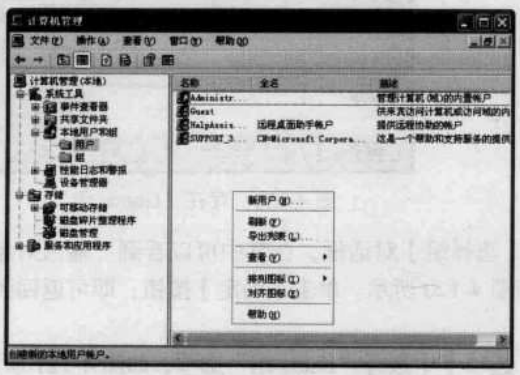


图 4-115 选择新用户

图 4-116 【新用户】对话框

此时的这个账户还不是一个标准“陷阱”式账户，要想使其真正起到陷阱作用，还需要将这个账户加入到 Guests 组中，让其只能拥有普通账户的权限才行。具体的操作步骤如下。

步骤 1：右击刚才建立的“Administrator”账户，在弹出菜单中选择【属性】选项，即可打开该账户的【属性】对话框，如图 4-117 所示。

步骤 2：在“隶属于”选项卡中可以看到刚创建的“Administrator”账户隶属于“Users”组，单击下方的【添加】按钮，即可打开【选择组】对话框，如图 4-118 所示。

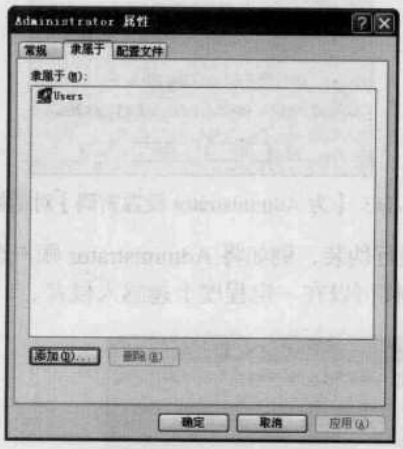


图 4-117 “隶属于”选项卡

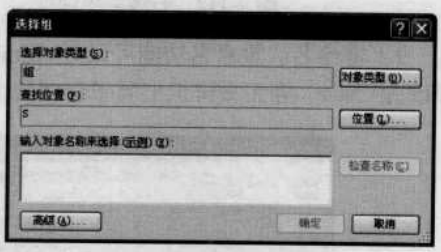


图 4-118 【选择组】对话框

步骤 3：单击【高级】按钮，即可展开选择组到具有搜索功能的界面。单击【立即查找】按钮，即可看到系统中的所有的用户组，在其中选择“Guests 组”选项，如图 4-119 所示。

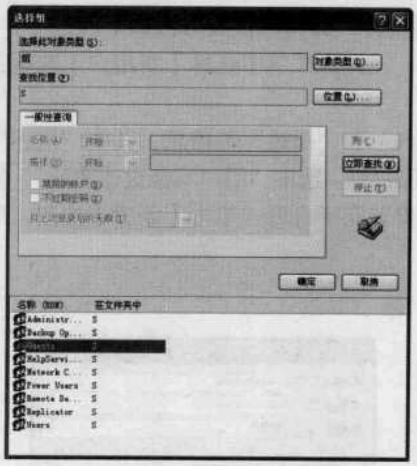


图 4-119 立即查找

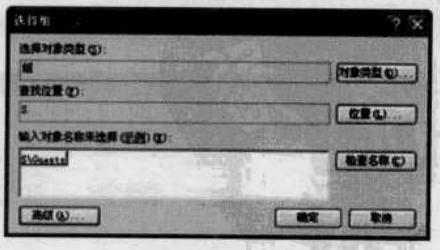


图 4-120 存在“Guests 组”

步骤 4：单击【确定】按钮，即可返回【选择组】对话框，在其中可以看到“输入对象名称来选择”列表中已经有了“Guests 组”，如图 4-120 所示。单击【确定】按钮，即可返回到该账户的【属性】对话框。

步骤 5：在【属性】对话框的“隶属于”选项卡中选择“Users 组”选项，如图 4-121 所示。单击【删除】按钮将其删除，一个具有陷阱效果的“Administrator”账户就创建成功了。

一些高水平的黑客可能会从本地或 Terminal Service 的登录界面中看到用户名，然后去猜测密码，这样一来，刚才设置的陷阱式账户就没有作用了，为了更好地使其发挥作用，还应该进行如下的禁止显示登录的用户名的设置。具体的操作步骤如下。

步骤 1：选择【开始】→【设置】→【控制面板】→【管理工具】→【本地安全策略】选项，即可打开【本地安全设置】窗口，如图 4-122 所示。

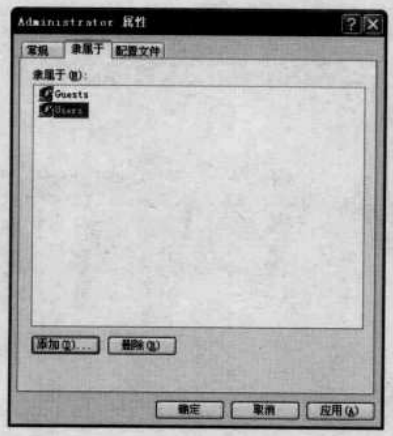


图 4-121 选择 “Users 组”

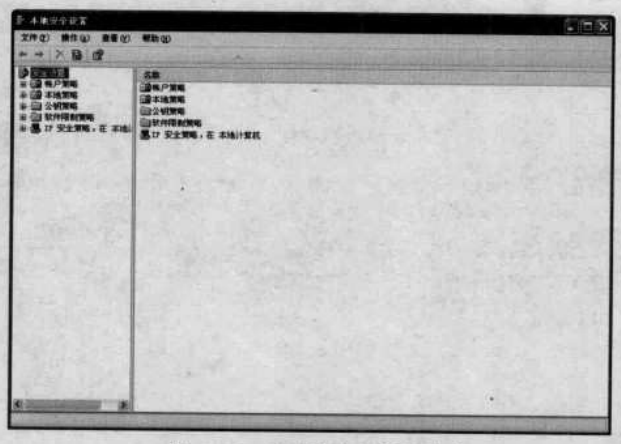


图 4-122 【本地安全设置】窗口

步骤 2：展开【本地策略】→【安全选项】选项，在右侧双击“交互式登录：不显示上次登录的用户名”选项，如图 4-123 所示。

步骤 3：在【交互式登录：不显示上次登录的用户名】对话框中选择“已启用”单选项，如图 4-124 所示。单击【确定】按钮，针对“Administrator”账户进行欺骗的陷阱账户就完全创建成功了。

图 4-123 安全选项

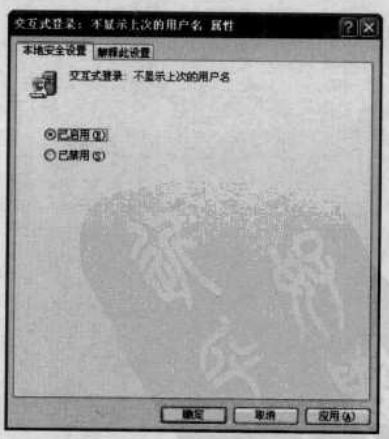


图 4-124 交互式登录对话框

第 5 章　加密与解密工具

重点提示

- NTFS 文件系统加密数据
- 光盘的加密文件与解密技术
- 用“私人磁盘”隐藏大文件
- 使用 Private Pix 为多媒体文件加密
- 用 ASPack 对 EXE 文件进行加密
- 软件破解实用工具
- 给系统桌面加把超级锁
- 系统全面加密 PC Security

本章精粹：

本章主要从加密与解密两个方面讲述加密在计算机安全中的应用与技巧。主要包括：NTFS 文件系统加密数据、光盘的加密文件与解密技术、使用 Private Pix 为多媒体文件加密、给系统桌面加把超级锁、系统全面加密 PC Security 和完全解除网游外挂等。

数据的解密技术和加密技术是矛与盾的关系，它们是在相互斗争中发展起来的，永远没有不可破解的加密技术。然而，一般的解密技术总是滞后于加密技术，也就是说，一般的解密技术总是针对某一类或相关加密技术而产生。

第 40 招 NTFS 文件系统加密数据

Windows 2000/XP 提供了内置的加密文件系统（Encrypting Files System，简称 EFS）。EFS 文件系统不仅可以阻止入侵者对文件或文件夹对象的访问，而且还保持了操作的简捷性。加密文件系统通过为指定 NTFS 文件与文件夹加密数据，从而确保用户在本地计算机中安全存储重要数据。由于 EFS 与文件集成，因此对计算机中重要数据的安全保护十分有益。

1. 加密操作

利用 Windows 2000/XP 资源管理器选中待设置要加密属性的文件或文件夹（如文件夹为“新建文件夹”）。对某文件进行加密的具体操作步骤如下。

步骤 1：在这个文件夹上右击，从快捷菜单中选择“属性”菜单项，即可打开【新建文件夹 属性】对话框，如图 5-1 所示。

步骤 2：单击“常规”选项卡中的【高级】按钮，即可打开【高级属性】对话框，在其中选择用于该文件夹的设置，如图 5-2 所示。勾选“压缩或加密属性”选项区中的“加密内容以便保护数据”复选框，单击【确定】按钮，即可完成文件或文件夹的加密。

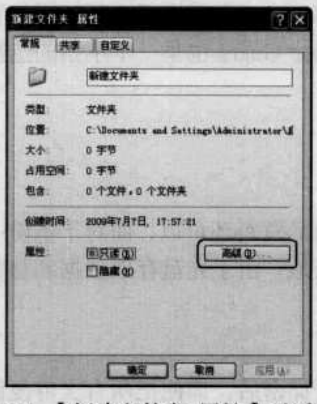


图 5-1 【新建文件夹 属性】对话框

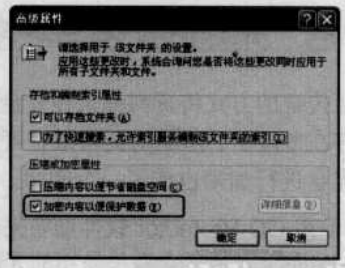


图 5-2 【高级属性】对话框

2. 解密操作

利用 Windows 2000/XP 资源管理器选中设置了加密属性的文件或文件夹（仍然以刚才加密的文件夹为例）。具体的操作步骤如下。

步骤 1：找到刚才加密的文件夹并右击，从快捷菜单中选择“属性”菜单项，即可打开【新建文件夹 属性】对话框。

步骤 2：单击“常规”选项卡中的【高级】按钮，即可打开【高级属性】对话框，清除“压缩或加密属性”选项区中“加密内容以便保护数据”复选框的“√”。

当然进行加密/解密操作时，也应注意如下几点要求。

1）不能加密或解密 FAT 文件系统中的文件与文件夹，而只能在 NTFS 格式的磁盘分区上进行此操作。

2）加密数据只有存储在本地磁盘中才会被加密，而当其在网络上传输时，则不会加密。

3）已经加密文件与普通文件相同，也可以进行复制、移动以及重命名等操作，但是其操作方式可能会影响加密文件的加密状态。

3．复制加密文件

在 Windows 2000/XP 资源管理器中选中待复制的加密文件，右击该加密文件并从快捷菜单中选择“复制”菜单项。切换到加密文件复制的目标位置并右击，从快捷菜单中选择“粘贴”菜单项，即可完成操作。可以看出，复制加密文件同复制普通文件并没有不同。只是进行复制的操作者必须是被授权用户。别外，加密文件被复制后的副本文件，也是被加密的。

4．移动加密文件

在 Windows 2000/XP 资源管理器中选中待复制的加密文件，右击该加密文件并从快捷菜单中选择“剪切”菜单项，再切换到加密文件待移动的目标位置并右击，从快捷菜单中选择“粘贴”菜单项即可完成。

注意 如果把加密文件复制或移动到 FAT 文件系统中时，文件自动解密，所以建议对加密文件进行复制或移动后应重新进行加密。

如果忘记了密码，可以将安装时制作的钥匙盘放进软驱中，随便输入密码，输入第三次后即可进入程序，再选择【Functions】→【Change Your Password】菜单项即可改变密码。也可选择“Creat a New Account”菜单项为自己或他人建立一个新加密账号，最多设立五个，每个账号都有一个密码，只有密码设立人才可看到自己账号内的加密文件，其他人看不到。

当安装 Encrypted Magic Folders 后，磁盘检查程序“Chkdisk”就不能运行，因为它能删除所有隐藏的文件和密码数。在隐藏文件夹的工具中，Folder Guard 也是一个不错的选择，感兴趣的朋友可以自己试一试，这里不再赘述。

第 41 招　光盘的加密与解密技术

按照传统的方式将资料刻录在光盘上，备份一些普通的资料还可以，而对于备份一些重要数据就存在危险了，里面的资料很有可能被其他人非法获取。由于光盘存取数据和材料的特殊性，对光盘进行加密也成了一个问题。

1．使用 CD-Protector 软件加密光盘

CD-Protector 是一个简单易用的光碟加密软件，被它加密后，即使把所有文件复制到硬盘上仍然不能使用。CD-Protector 加密时所使用到的相关软件有 Nero，加密原理是在可执行文件上加一个外壳，该外壳会判断所运行光碟上有没有加密后所产生的相对应的音频轨道，如果有则运行，没有的话则会拒绝运行。CD-Protector 加密时不用修改 Cue 文件，不用交替写入坏轨道，由于使用了 Nero 刻录软件，因此对刻录机要求不高。

CD-Protector 加密的具体的操作步骤如下。

步骤 1：双击“CD-Protector”应用程序，即可打开 CD-Protector 主窗口，如图 5-3 所示。在“File to encrypt”文本框中输入要加密的可执行文件名。在“Custom Message”文本框中输入出错时的提示信息（可自行选择填写，也可不填）；在“Phantom Trax'directory”文本框中输入文件输出时目录；在“Encryption Key”文本框中输入两位十六进制的数字，这里可以输入“00-FF”。不同的十六进制数字代表不同的特殊加密轨道，共有 256 种。

步骤 2：在设置完成之后，即可看到【ACCEPT】按钮变成了红色，如图 5-4 所示。单击红色的【ACCEPT】按钮，即可开始加密文件。加密完成之后，单击【OK】按钮即可。

步骤 3：运行 Nero 主程序，新建一个刻录音频光盘的任务。在【音频光碟】选项卡中取消勾选“在光碟上定稿光碟文字”复选框；在【CDA 选项】选项卡中勾选“刻录前在硬盘上缓存音轨”复选框和“清除*.cda 音轨末尾的静音”复选框；在【刻录】选项卡中勾选“写入”复选框，取消勾选“终结光碟”复选框和“光碟一次性”复选框。

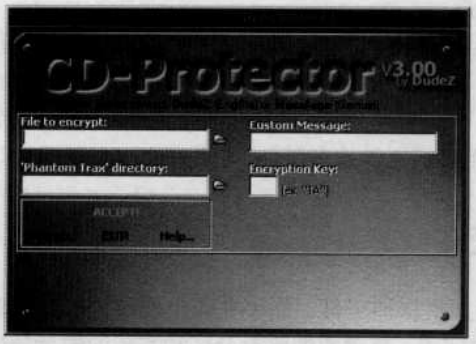


图 5-3 CD-Protector 主窗口

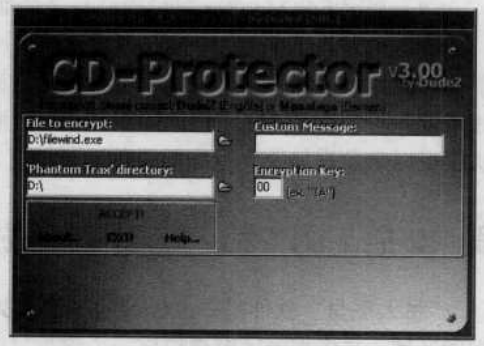


图 5-4 设置加密文件

步骤 4：在全部设置完成后，单击【新建】按钮，就可以开始新建任务了。把用 CD-Protector 加密过的音频文件，拖放到刻录音轨的窗口。刻录完成后，还需要再执行一遍刻录设置，主要是为了用这个方法对同一个音频文件刻录两次。

步骤 5：在 Nero 中再新建一个只读光盘的任务，在【多记录】选项卡中勾选“开记多记录光碟”复选项，其他选项可根据需要进行相应地设置。

步骤 6：完成上述设置之后，单击【新建】按钮，把用 CD-Protector 加密的（除音频文件外）文件都拖放到数据刻录的窗口并开始刻录，刻录的选项和刻录音轨相同。

此时，就可以看到同一个音频文件再次刻录的结果是不同的。使用 CD-Protector 加密过的光盘放进光驱里，文件是可运行的，但复制到自己的硬盘时就不能运行了。CD-Protector 加密的光盘是由两条音轨和一条数据轨道共同组成的，数据轨道中被加密的可执行文件，在运行时将会读取光盘上的音轨，只有相对应时才会继续运行。

2．破解加密光盘

如今市面上有很多加密光盘是以特殊形式刻录的，将它放入光驱后，就会出现一个软件的安装画面将要求输入序列号，如果序列号正确就会出现一个文件浏览窗口，错误则跳回桌面。如果用户从资源浏览器中所观看的光盘文件就是一些图片之类文件，想找的文件却怎么也看不到。这时就需要对光盘进行解密了，下面介绍几种常用的破解加密光盘方法：

（1）用 UltraEdit 等十六进制编辑器直接找到序列号

运行 UltraEdit 编辑器打开光盘根目录下的 SETUP.EXE 文件之后，选择【搜索】→【查找】菜单项，即可弹出【查找】对话框。在“查找什么”栏的“请输入序列号”文本框中输入序列号之后，勾选“查找 ASCII 字符”复选框，在“请输入序列号”后面显示的数字就是序列号了。

（2）用 ISOBuster 等光盘刻录软件直接浏览光盘上的隐藏文件

打开 ISOBuster 光盘刻录软件之后，选择加密盘所在的光驱，单击选择栏旁边的【刷新】按钮，即可开始读取光盘中的文件，这时会发现在左边的文件浏览框中多了一个文件夹，那里面就是要找的文件，可以直接运行和复制这些文件了。

（3）要用到虚拟光驱软件和十六进制编辑器

1）用虚拟光驱软件把加密光盘做成虚拟光盘文件，进行到 1%时终止虚拟光驱程序运行。

2）用十六进制编辑器打开只进行了1%的光盘文件，在编辑窗口中查找任意看得见的文件夹或文件名，在该位置的上面或下面，就可以看到隐藏的文件夹或文件名了。

3）在MS-DOS模式下使用CD命令进行查看目录，再使用DIR命令就可以看到想要找的文件，并可以对其进行运行和复制了。

（4）利用File Monitor对付隐藏目录的加密光盘

File Monitor是纯“绿色”免费软件，可监视系统中指定文件运行状况，如指定文件打开了哪个文件，关闭了哪个文件，对哪个文件进行了数据读取等。通过它可以指定监控的文件有任何读、写、打开其它文件的操作都能被它监视下来，并提供完整的报告信息。使用它的这个功能可以来监视加密光盘中的文件运行情况，从而得到想要的东西。

第42招　用“私人磁盘”隐藏大文件

“私人磁盘”软件是一款极好的文件和文件夹加密保护工具，能够在各个硬盘分区中创建加密区域，并将加密区域虚拟成一个磁盘分区以供使用。该虚拟的磁盘分区和实际的磁盘分区完全一样。用户可以在其中存放文件资料，也可以将软件或游戏安装在里面。

1.“私人磁盘”的创建

“私人磁盘”为绿色软件，下载并解压后，直接双击即可进入主操作界面执行相应地操作，包括：创建、删除、打开、修改和关闭私人磁盘等操作。

创建“私人磁盘”的具体操作步骤如下。

步骤1：先运行私人磁盘程序，因为初始密码为空，所以无需输入密码，直接单击【确定】按钮即可进入，如图5-5所示。如果已经设置了密码则需要输入相应的密码，不然会出现出错提示，无法进入该系统。

步骤2：进入后可以看到一个微型的主界面，如图5-6所示。在其中列出了现有的磁盘分区。单击标题栏的【变】按钮，可以切换到完整界面，如图5-7所示。

图5-5　运行私人磁盘程序

图5-6　微型的主界面

图5-7　完整的主界面

步骤3：和微型界面相比，完整界面多了“修改用户密码”和“操作选择”两大栏目。如果用户想修改用户密码，可以在“修改用户密码”栏目中完成操作。

步骤4：创建私人磁盘。先在私人磁盘文件列表框中单击选择准备在哪个分区上创建私人磁盘（一个分区上只能创建一个，如果创建多个会出现出错提示），单击“操作选择”栏中的【创建私人磁盘】按钮。

步骤5：在很短的时间内，该软件系统就会完成私人磁盘的创建工作。在刚才选定的磁盘

分区的卷标右侧会出现一个“☆”形状的标志，如图 5-8 所示。

注意 由于私人磁盘空间是从各个磁盘分区中的剩余空间中分离出来，私人磁盘的个数和大小受实际分区和所剩空间的限制。

步骤 6：选中要打开的私人磁盘，单击“操作选择”栏中的【打开私人磁盘】按钮或打开“我的电脑”，就会发现多出了一个磁盘分区，该磁盘分区 I 的卷标和源磁盘分区的卷标一致，如图 5-9 所示。

图 5-8 创建私人磁盘

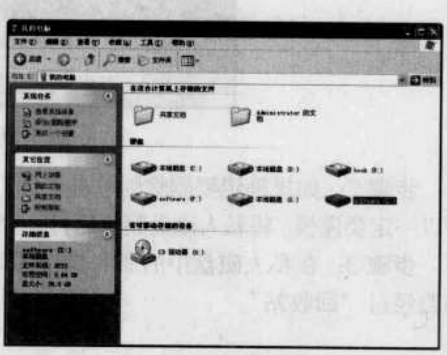


图 5-9 私人磁盘 I 盘

步骤 7：私人磁盘创建完成后，如果需要使用它，可在“我的电脑”中像普通磁盘一样打开它；也可以先在“私人磁盘文件列表”中对应的位置单击，再单击“打开私人磁盘”按键；或双击相应盘符，程序就会打开对应的私人磁盘文件，并虚拟一个磁盘分区供使用，文件操作和普通磁盘相同，只是不能进行“格式化操作”。

步骤 8：为了让该私人磁盘更符合需要，可对它进行配置。单击【私人磁盘设置】按钮，即可弹出【私人磁盘设置】对话框，如图 5-10 所示。

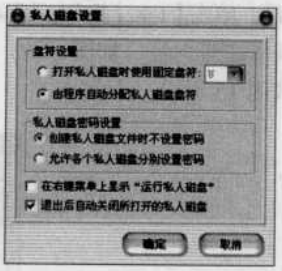


图 5-10 【私人磁盘设置】对话框

步骤 9：在“盘符设置”部分可将私人磁盘的盘符设置为使用某个固定盘符，如：“U”；选择该项则每次打开不同分区的私人磁盘文件时都使用指定盘符，即同一时刻只能打开一个私人磁盘。如果要在私人磁盘中安装软件或游戏，则可使用固定盘符。或由系统自动分配，以同时打开多个私人磁盘文件。打开时将由程序自动分配私人磁盘盘符。

步骤 10：如果将“私人磁盘密码设置”设置为“允许各个私人磁盘分别设置密码”，则在创建私人磁盘时会提示输入密码。如果输入密码为空或选择取消，则视为不使用密码保护。设置密码保护的私人磁盘在打开和删除时也都会提示输入密码。

这样，在登录私人磁盘软件的时候提示输入用户密码，而具体使用文件又需要用到磁盘密

码，这样该私人资料就有双重防护了，并且可以随时使用“修改磁盘密码”来修改选定的私人磁盘文件的密码。同样，如果所设置的新密码为空，则视为取消密码保护。

2.“私人磁盘”的删除

如果要删除创建的私人磁盘，方法正好和创建相反。具体的操作步骤如下。

步骤 1：在主界面中选择将删除的私人磁盘，单击操作选择部分的【删除私人磁盘】按钮，即可弹出“确认”提示框，提示是否删除，如图 5-11 所示。

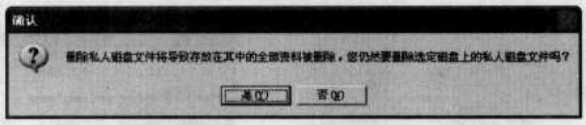


图 5-11 “确认”提示框

步骤 2：如果确定要删除则单击【是】按钮。这个操作会删除所有存在私人磁盘里的文件，所以一定要谨慎。将私人磁盘删除后打开“我的电脑”时，即可看到所创建的私人磁盘已经消失。

步骤 3：在私人磁盘中的所有操作都与普通分区中的操作相同。删除私人磁盘中的文件同样要经过“回收站”。

第 43 招　使用 Private Pix 为多媒体文件加密

Private Pix 是一款功能强大的多媒体加密工具。也支持对音频文件或视频文件进行加密，为用户提供了更全面的功能。Private Pix 提供了简单易用的界面来对图片进行管理、加密和浏览。让用户在查看图片文件的同时还能对图片进行加密，并且具有两种类型的加密方式。

使用 Private Pix 对文件进行加密的具体操作步骤如下。

步骤 1：运行 Private Pix 软件弹出“Enter Password”界面，在“Password”文本框中输入相应的口令。由于是第一次使用，这里应输入默认口令“private”，如图 5-12 所示。

步骤 2：在密码填写正确无误后，单击【OK】按钮，即可打开【Private Pix(tm) Registration】对话框，在其中查看软件信息并填写注册内容，如图 5-13 所示。若无法获取注册码，则不能完成相应地注册时，但是可免费试用 15 天。

图 5-12 “Enter Password”界面

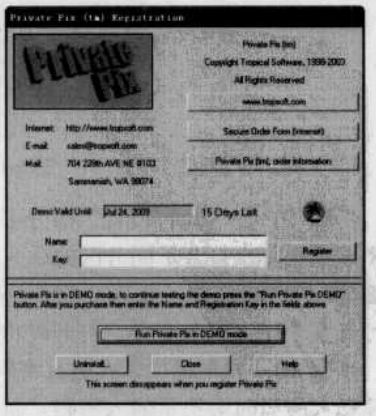


图 5-13 【Private Pix(tm) Registration】对话框

步骤 3：根据需要，这里不进行软件注册操作，则单击【Private Pix(tm) Registration】对话

框下方的【Run Private Pix in DEMO mode】按钮，即可进入【Private Pix】主窗口，如图 5-14 所示。Private Pix 加密工具主要由显示窗口和控制窗口两部分组成。

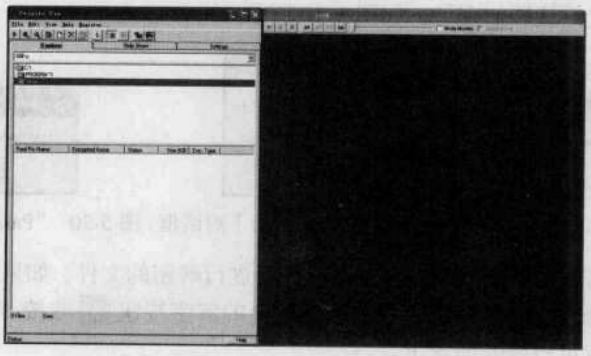


图 5-14 “Private Pix”的主窗口

步骤 4：在左边显示窗口的资源管理器中选择要加密的多媒体文件。如果不设置密钥，则使用默认密钥。因为这里要设置密钥，所以选择【Settings】选项卡，如图 5-15 所示。

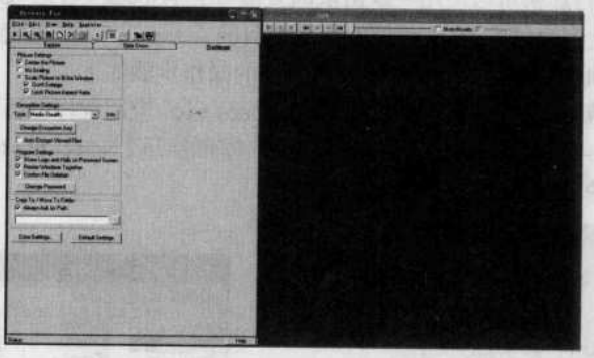


图 5-15 【Settings】选项卡

步骤 5：在“Encryption Settings”栏目中，从“Type”下拉列表中选择一种文件加密的类型并单击【Change Encryption Key】按钮，即可弹出【Enter Password】对话框，在其中输入需要修改的口令，如图 5-16 所示。

步骤 6：单击【OK】按钮，即可弹出【Encryption Key】对话框，在其中输入需要加密图片的密钥，如图 5-17 所示。单击【OK】按钮，即可弹出“Privp”消息框，提示“key has been successfully changed”信息，如图 5-18 所示。

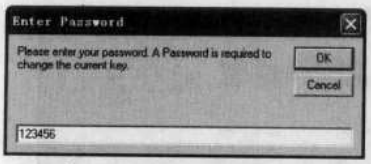


图 5-16 【Enter Password】对话框

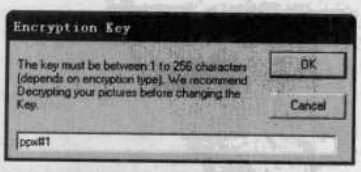
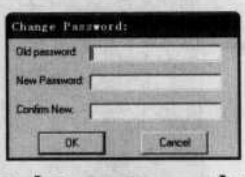


图 5-17 【Encryption Key】对话框

步骤 7：若想改变程序密码，则在“Program Settings”栏目中单击【Change Password】按钮，即可弹出【Change Password】对话框，在其中输入旧的口令以及需要修改的新口令，如图 5-19 所示。

步骤 8：单击【OK】按钮，即可弹出“Password Change”消息框，提示“Password changed successfully”信息。返回【Private Pix】主窗口，单击工具栏的加密按钮 或按“Ctrl+E”快捷键之后，所选的文件就被加密了，如图 5-20 所示。



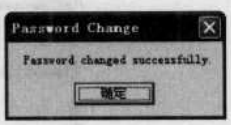


图 5-18 “Privp”消息框　图 5-19 【Change Password】对话框　图 5-20 “Password Change”消息框

解密方法与加密方法类似。用户需要先选择要进行解密的文件，如果要解密的文件与当前密钥不一样，则先修改当前的密钥或单击工具栏上的解密按钮 或按“Ctrl+D”快捷键，这样，被加密的文件就可以恢复原状了。

第 44 招　用 ASPack 对 EXE 文件进行加密

对 EXE 文件进行加密可以使用一款由俄国人编写的 Aspack 软件，该软件能够对 EXE 文件进行压缩，从而达到隐藏 EXE 文件原始信息的目的。Aspack 运行速度相当快，而且稳定，能够将 EXE 文件压缩到原有的 20%～60%。具体的操作步骤如下。

步骤 1：下载并解压“Aspack”文件，双击“Aspack.exe”应用程序图标，即可打开“Aspack”主操作界面，如图 5-21 所示。单击【Open】按钮，即可打开【Select file to compress】对话框，在其中选择要压缩的 EXE 文件，如图 5-22 所示。

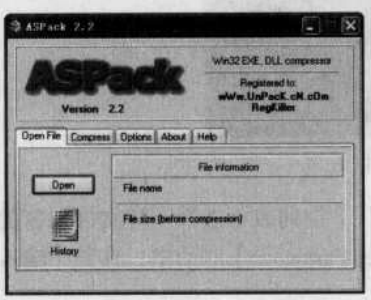


图 5-21 “Aspack”主界面

图 5-22 【Select file to compress】对话框

步骤 2：单击【打开】按钮，Aspack 就开始压缩了，同时显示压缩的进度，如图 5-23 所示。在压缩完成之后，将会显示压缩比例，如图 5-24 所示。

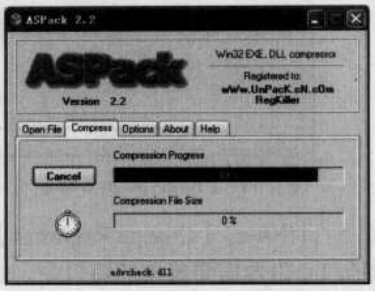


图 5-23 显示 Aspack 的压缩过程

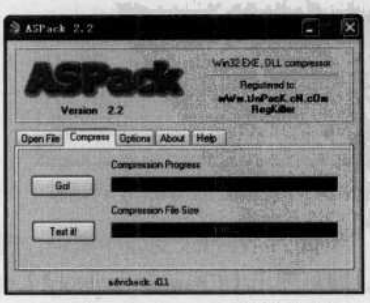


图 5-24 Aspack 压缩完成

步骤 3：在压缩完成之后，单击【Test it!】按钮，即可测试压缩后的程序执行是否正确。如果正确则会出现【Erase Bak】按钮和【Restore】按钮，用以删除原有文件和恢复原有文件，如图 5-25 所示。

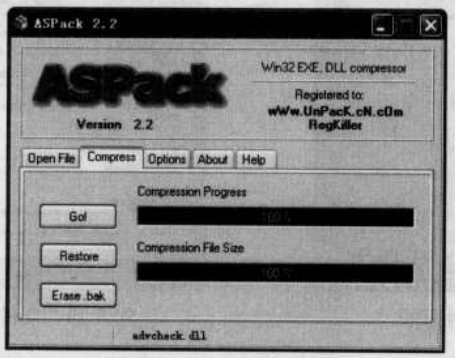


图 5-25 Aspack 测试结束

第 45 招 “加密精灵”加密工具

加密精灵是一款加密速度极快且功能强大的国产加密工具，可用于加密任何格式的文件，几乎集成了当前所有加密工具的功能。

1. 对单个文件进行加密解密

利用加密精灵可以加密任何格式的文件，并且可以同时加密多个文件，这里首先介绍如何对单个文件进行加密解密。其加密的具体步骤如下。

步骤 1：运行加密精灵应用程序，即可弹出“加密精灵”的主窗口，如图 5-26 所示。

步骤 2：在加密精灵主窗口中选择要加密的文件。单击【加密】按钮，即可弹出【加密】对话框，在“输入密码”文本框中输入密码，密码的范围在 8 ~ 128 个字符，如图 5-27 所示。

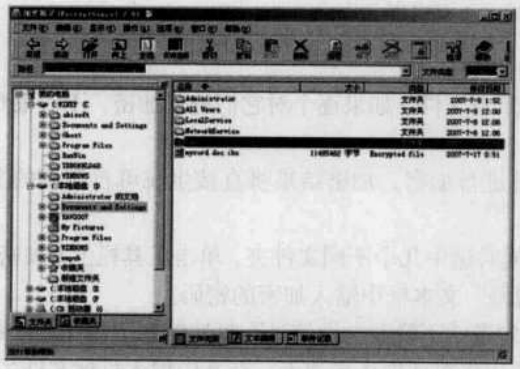


图 5-26 “加密精灵”主窗口

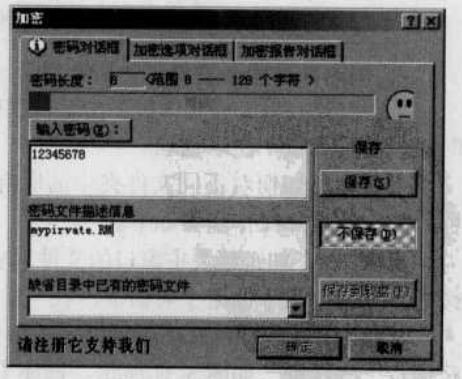


图 5-27 【加密】对话框

步骤 3：在“加密报告对话框”选项卡中默认选择“保存到原文件目录”选项，在“加密后彻底删除原文件”文本框右边选择【YES】选项，如图 5-28 所示。单击【确定】按钮后，就可以开始加密操作了。

步骤 4：在加密结束之后，在程序主窗口的“事件记录”中，即可看到“加密/解密记录”

的详细信息，如图 5-29 所示。

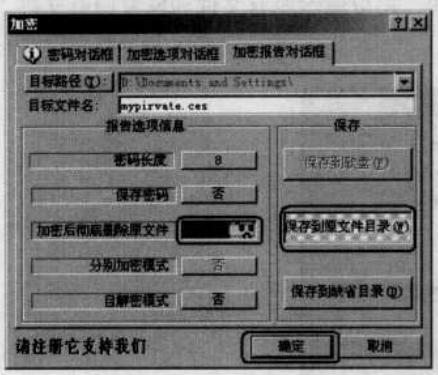


图 5-28　加密报告对话框

图 5-29　文件加密后的事件记录信息

解密的过程与加密过程相似，在文件列表里选择要解密的文件“myprivate.ces”之后，单击工具栏上的【解密】按钮，即可打开【解密】对话框，在“输入密码”文本框中输入密码，如图 5-30 所示。

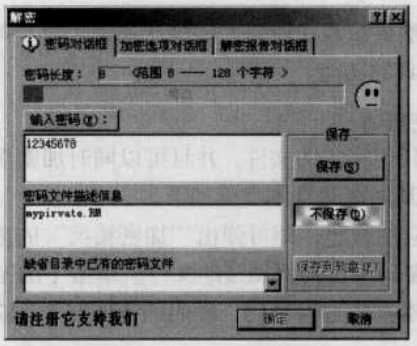


图 5-30 【解密】对话框

2．同时加密多个文件夹的所有文件

某些时候，可能需要保护多个文件夹中的所有文件，如果逐个对它们进行加密，不仅浪费时间，而且也很不便于管理。

下面介绍如何对不同文件夹中的所有文件进行加密，加密结果将直接生成可自解密的文件。加密的具体操作步骤如下。

步骤 1：在加密精灵主窗口的文件列表中同时选中几个不同文件夹。单击工具栏上【加密】按钮，即可弹出【加密】对话框，在“输入密码”文本框中输入加密的密码。

步骤 2：在“加密选项对话框”选项卡中勾选“不隐藏文件信息”复选框和“保存文件路径信息”复选框，如图 5-31 所示。选择【加密报告对话框】选项卡，在其中输入目标文件名，这里输入“MyFolder123.exe”。

步骤 3：单击【确定】按钮，待加密成功之后，在【事件记录】选项卡中将会给出结束提示，同时在根目录 D:\中可以找到自解密文件“MyFolder123”。

在没有加密精灵的情况下，还可以实现对自解密文件进行解密，解密的过程十分简单，具体操作步骤如下。

步骤 1：打开 Windows 资源管理器窗口之后，在其中找到要解密的“MyFolder123”自解密文件。双击自解密文件“MyFolder123”，即可弹出解密密码输入对话框，如图 5-32 所示。

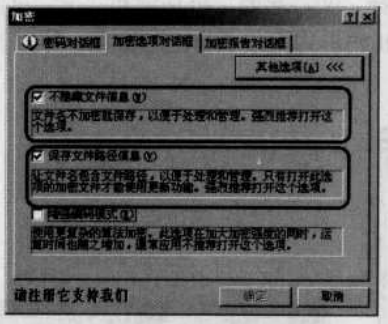


图 5-31 加密选项对话框选项卡

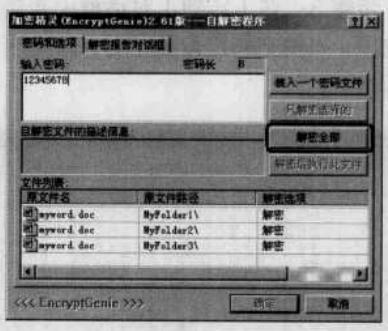


图 5-32 “密码和选项”选项卡

步骤 2：单击解密密码输入对话框右侧的【解密全部】按钮之后，选择【解密报告对话框】选项卡，如图 5-33 所示。

图 5-33 加密报告对话框选项

步骤 3：将“使用原文件路径”选项选择为【是】按钮之后，单击【确定】按钮，就可以开始解密了。如果输入的密码是正确的，文件将会被成功解密。

第 46 招 软件破解实用工具

在加密解密的实现过程中需要用到许多软件破解实用工具，如编辑工具、监视工具以及脱壳工具等，灵活地运用这些工具，往往可以达到事半功倍的效果。

1. 十六进制编辑器 HexWorkshop

HexWorkshop 十六进制编辑器可方便地进行十六进制编辑、插入、填充、删除、剪切、复制和粘贴工作，配合查找、替换、比较以及计算校验等命令，会使工作更加快捷。它速度快，算法精确，并附带有计算器和转换器工具。

HexWorkshop 具体操作步骤如下。

步骤 1：运行“HexWorkshop”应用程序图标，即可进入“HexWorkshop”的主窗口，选择【文件】→【打开】菜单项以打开目标文件（仍以 KuGoo 为例），如图 5-34 所示，左边是文件偏移地址区（默认是十六进制），中间是十六进制数据代码区，右边是文本字符代码区。

步骤 2：在主窗口中修改十六进制代码或 ASCII 代码。假设需要修改的代码距离文件起始

点的偏移地址为 1125，选择【编辑】→【转到】菜单项或按“Ctrl+G”组合键，即可打开【转到】对话框。

步骤 3：在【转到】对话框中直接输入 1125，并选择“文件起始”单选项和“十六进制”单选项，当找到指定偏移量时，即可用十六进制或 ASCII 码形式来修改指定的数据，如图 5-35 所示。

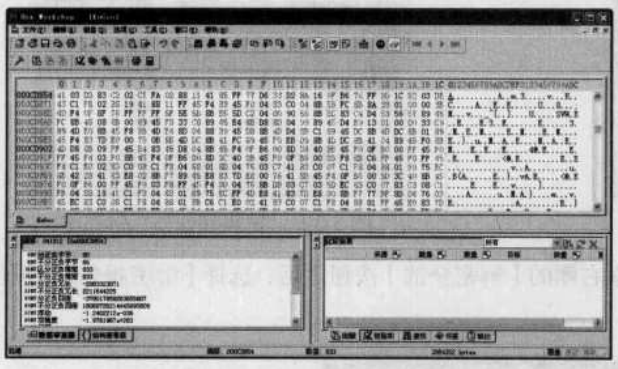


图 5-34　HexWorkshop 主窗口

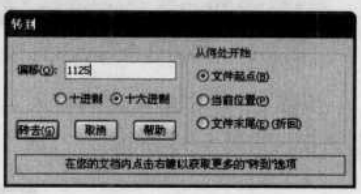


图 5-35 【转到】对话框

注意 在 HexWorkshop 工具的十六进制中是按文件偏移地址（Offset）进行显示，而在 W32Dasm 中和 IDA Pro 中则是按虚拟地址进行显示。

步骤 4：如果建立一个简单的十六进制新文件，则可选择【文件】→【新建】菜单项来建立一个新文件。选择【编辑】→【插入】菜单项，即可打开【插入字节】对话框，其中的第一行是需要增加文件的字节数，第二行是默认填充的数字，如图 5-36 所示。

步骤 5：假设在这里需要加入 0x35 个字节的数据（填充值默认为 0），单击【确定】按钮，就可以有一个 0x35 个字节的文件出现了，此时即可直接对此文件进行编辑。如果还想要删除其中的一些东西，则只需在将其选中之后，直接按【Delete】键即可。

步骤 6：有时候还需要按一定的格式复制 HexWorkshop 所显示的十六进制数据，HexWorkshop 支持 C 语言格式、Java 语言格式、HTML 格式、文本格式、RTF 格式等。此时只要选中一部分十六进制数据，选择【编辑】→【复制为】→【C 源代码】菜单项，即可将所选数据转换成 C 语言格式，如图 5-37 所示。

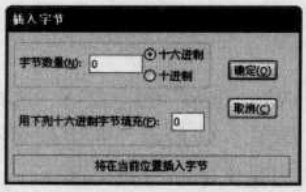


图 5-36 【Insert Bytes】对话框

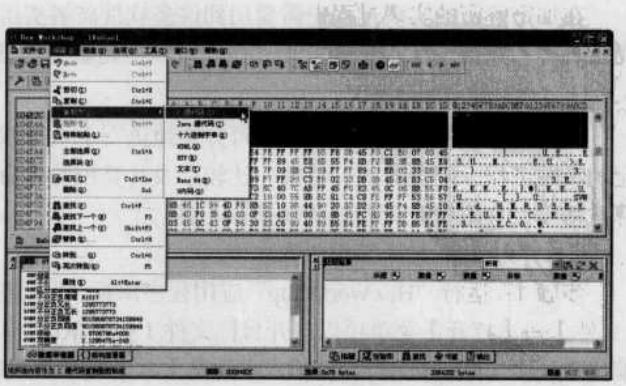


图 5-37　选择相应的菜单项

步骤 7：如果需要对两个相似的文件进行比较，以判断文件是否被修改或修改了何处，则可以选择【工具】→【比较】→【比较文件】菜单项来打开比较工具，在【来源】菜单和【目标】菜单中打开想要比较的两个文件；也可以单击【高级（A）】按钮，在其中设置进行比较的详细范围，单击【确定】按钮，即可开始比较，如图 5-38 所示。

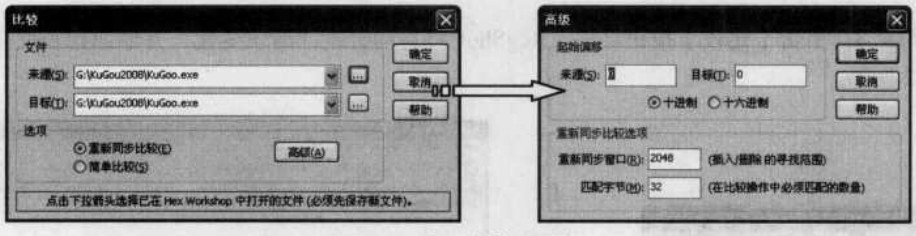


图 5-38 【比较】对话框

步骤 8：在比较结束之后，将会出现比较结果，如图 5-39 所示。此时单击右下角的【替换】选项，即可在主窗口显示被替换的具体字节，如图 5-40 所示。

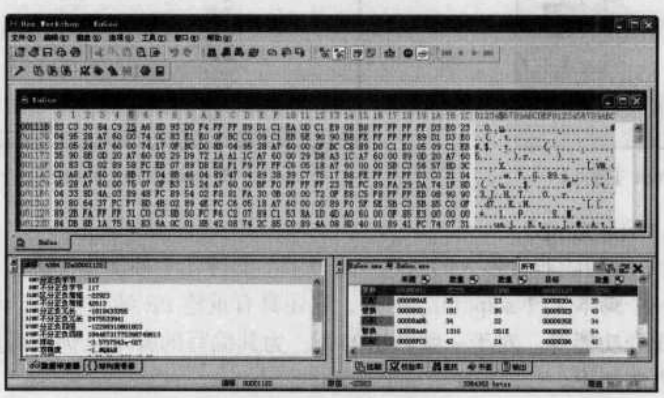


图 5-39 显示比较结果

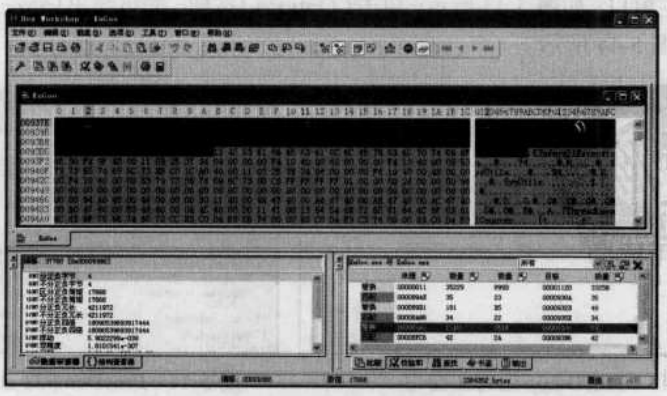


图 5-40 显示被替换的具体字节

2．注册表监视器 RegShot

RegShot 是一款小巧的注册表静态比较工具，可快速发现注册表地变化，甚至通过扫描硬盘来掌握硬盘上某些文件夹（或是整个硬盘）的改变。

RegShot 的具体使用方法如下。

步骤 1：下载并解压“RegShot”压缩文件，双击“RegShot.exe”应用程序图标，即可进入“RegShot”主窗口，如图 5-41 所示。单击【快照（A）】按钮，就可以实现自动记录了。

步骤 2：待被监视对象运行完毕之后，单击【快照（B）】按钮，RegShot 即可自动进行记录。

步骤 3：单击【比较】按钮之后，RegShot 将自动分析注册表变化，并输出比较结果，如图 5-42 所示。

图 5-41　RegShot 主窗口

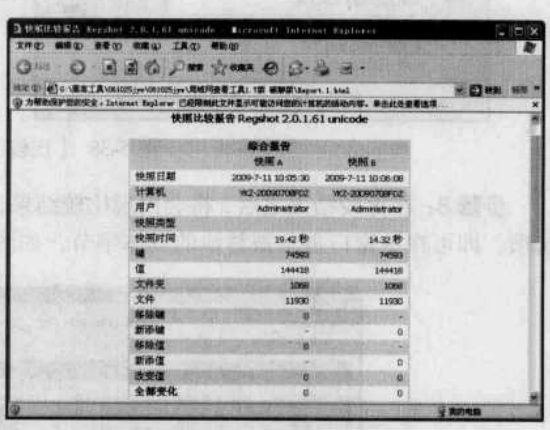


图 5-42　RegShot 输出比较结果

3．脱壳工具 Procdump

ProcDump 是一款功能非常强大的通用脱壳工具，支持几十种加壳工具生成压缩加密软件，最大特点就是有一个脚本文件 scipt.ini。另外，它还具有重建 PE 结构功能，区段编辑功能，未知类型壳的尝试脱壳功能等。对于一些新出的壳，为其编写的脚本也仍然可用。

具体的使用方法如下。

步骤 1：下载并解压缩“ProcDump”文件夹，双击“ProcDump”应用程序图标，即可打开“ProcDump”主窗口，如图 5-43 所示。单击【Options】按钮，即可弹出【ProcDump32 Optinos】设置对话框，如图 5-44 所示。

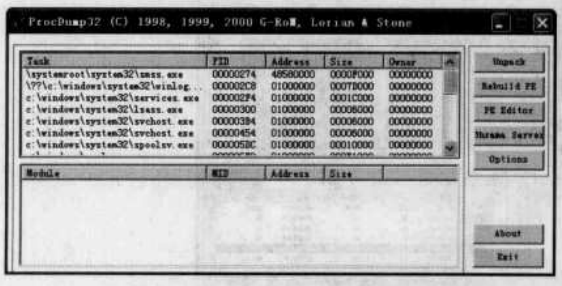


图 5-43　ProcDump 运行主窗口

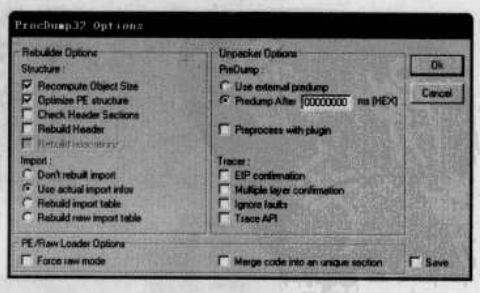


图 5-44　ProcDump32 选项设置对话框

步骤 2：在设置完成之后，单击【OK】按钮，即可返回【ProcDump】主窗口。单击【Unpack】按钮，即可打开【Choose Unpacker】对话框，如图 5-45 所示。

步骤 3：在选择合适的解包器之后，单击【OK】按钮，即可打开【Choose Execut able】对话框，如图 5-46 所示。在其中选择要进行脱壳的软件，就可以对软件进行脱壳了。

图 5-45 选择解包器对话框

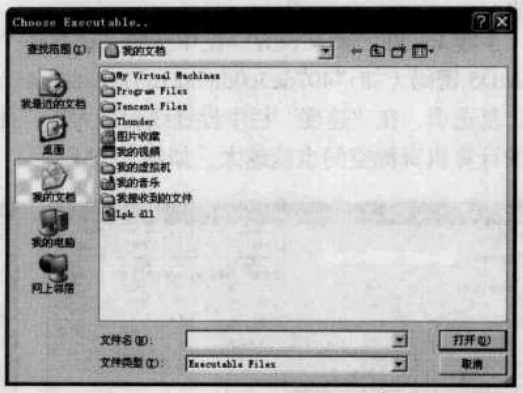


图 5-46 选择可执行文件对话框

下面是用 ProcDump 脱 ASPack 壳的脚本 scipt.ini 扩展，具体的实现代码如下：

```
Pxx=Aspack(All Vetsion)(XX为十六进制)
[Aspack(All Vetsion)]
L1=OBJR
L2=LOOK EB, ?
L3=JZ5
L4=QUIT
L5=BP
L6=WALK
L7=OBJR
L8=LOOK61, 75
L9=BP
LA=STEP
OPTL1=00000000
OPTL2=01010001
OPTL3=01010001
OPTL4=00030000
OPTL5=00000000
```

在添加此代码到脚本中之后，再重新启动 ProcDump 软件，就可以脱掉目前为止所有 ASPack 软件加的壳了。

第 47 招 破解 MD5 加密实例

MD5（Message-digest Algorithm 5，信息-摘要算法）密码转换器主要是对数据进行 MD5 算法转换。ASP 数据库几乎都是这样加密的，虽然解密比较困难，但通过强大的字典解密，效果不错，而且使用这个软件加密的密码很少有人能猜出来。随着 MD5 密码的流行，破解 MD5 的方法也是越来越多，下面从本地和网络两种方式来讲述 MD5 是如何实现暴力破解的。

1. 本地破解 MD5

现在破解 MD5 加密的软件有很多，下面将为大家介绍一款名叫“MD5 加强破解工具”，这个工具功能很齐全，简单易学，很适合黑客初学者使用。

（1）单个 MD5 密码破解

使用 MD5 进行密码破解的具体操作步骤如下。

步骤 1：下载并双击桌面上的“MD5”应用程序图标，即可打开“MD5”主窗口，如图 5-47

所示。

步骤 2：在“密文设置”栏中选择“破解单个密文”单选项，在其后文本框中输入要破解的 MD5 密码（如“407de5e0d85a21d317de8def45fa331b”），在“字符设置”栏中勾选“小写字母”复选项，在“速度”栏中设置线程最大数，此参数值越高，破解所需时间就越短，随之消耗的计算机资源空间也就越大，如图 5-48 所示。

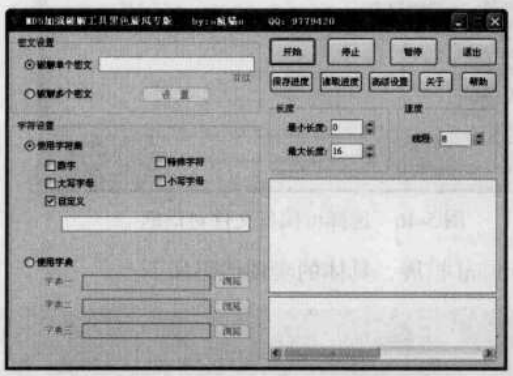


图 5-47 【MD5】主窗口

图 5-48 输入 MD5 密文

步骤 3：在设置完毕后单击【开始】按钮，即可开始破解 MD5 密码，在右下角的列表框中即可看到破解的进度，如图 5-49 所示。待破解完成后，即可弹出【MD5 完成提示】对话框，在右下角横向列表框中可以看到破解结果，如图 5-50 所示。

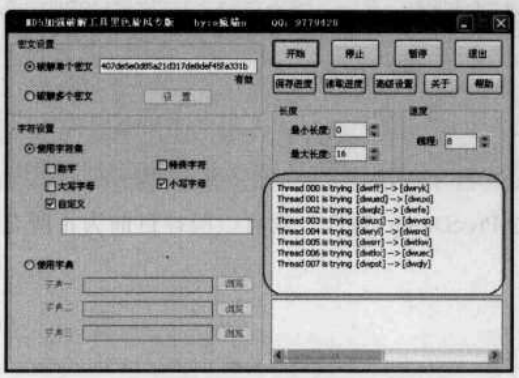


图 5-49 破解进度

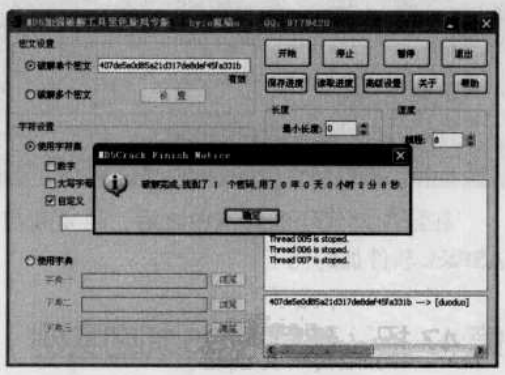


图 5-50 破解结果

（2）多个 MD5 密码破解

多个 MD5 密码破解和单个破解的操作方法很相似。

具体的操作步骤如下。

步骤 1：建立一个名为“md5.txt”的文本文件，用来存放需要破解的多个 MD5 密码，如图 5-51 所示。

步骤 2：在“MD5”主窗口中选择“密文设置”栏目里的“破解多个密文”单选项，单击【设置】按钮，即可打开【MD5Crack Cryptog Seting】对话框，如图 5-52 所示。

步骤 3：选择“从文件中读取”单选项，即可激活【浏览】按钮。再单击【浏览】按钮，即可打开【打开】对话框，在其中选择“md5.txt”文件，如图 5-53 所示。

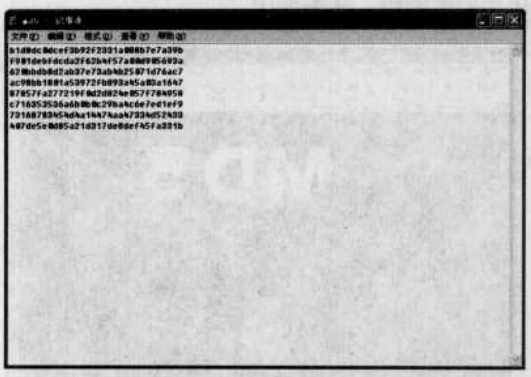


图 5-51 “md5.txt”文本文件

图 5-52 【MD5Crack Cryptog Seting】对话框

步骤 4：单击【打开】按钮，即可返回【MD5Crack Cryptog Seting】对话框，如图 5-54 所示。单击【确定】按钮，即可返回【MD5】主窗口。单击【开始】按钮，即可开始破解 MD5 密码，在右下角列表框中可看到破解的进度。

图 5-53 【打开】对话框

图 5-54 【MD5Crack Cryptog Seting】对话框

步骤 5：待破解完成后，即可弹出【MD5 完成提示】对话框，在右下角横向列表框中可以看到破解结果。

2. 在线破解 MD5

相对于本地密码破解，网上在线破解就容易得多了，现在也有很多能够在线破解 MD5 的网站（如“http://www.xmd5.org/”就是个很受欢迎的 MD5 在线破解网站）。

具体的操作步骤如下。

步骤 1：打开“Internet Explorer”浏览器，在地址栏中输入“http://www.xmd5.org/”，按下回车键后，即可打开“XMD5”网站。将要破解的 MD5 密文（如“407de5e0d85a21d317de8def45fa331b”）输入到输入框中，如图 5-55 所示。

步骤 2：单击【给我转】按钮，即可开始破解密码。等待破解完成后，即可打开“md5 reverse”页面，在其中查看破解的结果，如图 5-56 所示。

3. MD5 密码转换器应用实战

使用“MD5 密码转换器”可以很方便地将一组字符用 MD5 方式完成加密，具体的操作方法为：先打开 MD5 密码转换器，如图 5-57 所示。在“MD5 原码”文本框中输入要转换的字符，

单击【字典转换】按钮，加密后的密文将显示在“加密密码”文本框中。

图 5-55　输入 MD5 密文

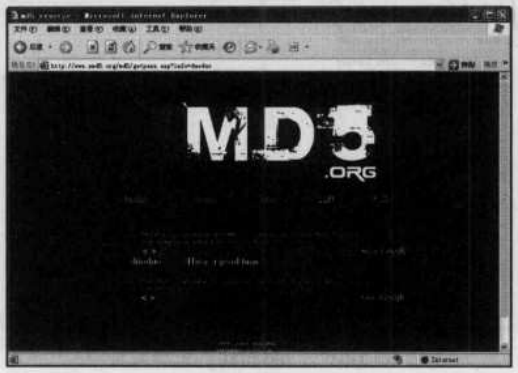


图 5-56　破解后的结果

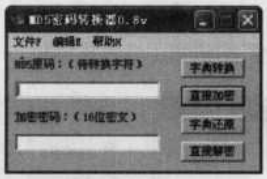


图 5-57　MD5 密码转换器

当然，使用“MD5 密码转换器”可以很方便地破解密文，具体的操作方法为：使用 MD5 密码转换器进行解密时，将要破解的密文直接复制到“加密密码”文本框中，单击【字典还原】按钮，还原后的密码将出现在“MD5 原码”文本框中。

由于 MD5 采用的是不可逆算法，字典还原不可能还原所有密文，当字典中没有要还原密文对应的密码时，“MD5 密码转换器”将会要求启动暴力破解程序。

第 48 招　给系统桌面加把超级锁

为了避免别人趁机动用自己的计算机，用户可使用桌面锁软件 SecureIt Pro 来解决这个问题，该软件可以让任何人（包括自己）都无法在不输入正确的密码情况下使用计算机。

1．生成后门口令

在开始使用 SecureIt Pro 前，因为软件为了防止用户忘记了进入口令，需要先填一些基本信息，并会根据这些信息自动生成一个后门口令，用于必要时登录使用。

具体的操作步骤如下。

步骤 1：下载并安装“SecureIt Pro”软件，双击桌面上的“SecureIt Pro”应用程序图标，即可打开【SecureIt Pro-End User's License Agreement】对话框，在其中认真阅读 SecureIt Pro 软件的使用许可协议，如图 5-58 所示。

步骤 2：勾选“Yes,I agree to be bound by the terms of the license Agreement”单选项，单击【Continue】按钮，即可打开【SecureIt Pro First Time Initialization-1】对话框，在其中查看首次初始化的基本信息，如图 5-59 所示。

步骤 3：单击【Next】按钮，即可打开【SecureIt Pro First Time Initialization-2】对话框，在其中填写注册信息，如图 5-60 所示。

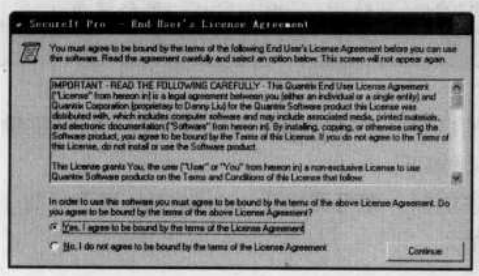


图 5-58 【SecureIt Pro-End User's License Agreement】对话框

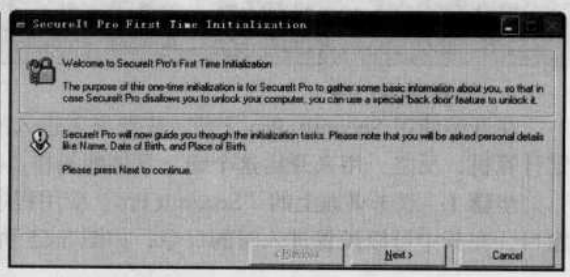


图 5-59 【SecureIt Pro First Time Initialization-1】对话框

步骤 4：单击【Next】按钮，即可打开【SecureIt Pro First Time Initialization-3】对话框，用于查看自动生成的一个后门口令，以便于帮助用户登录时使用，如图 5-61 所示。

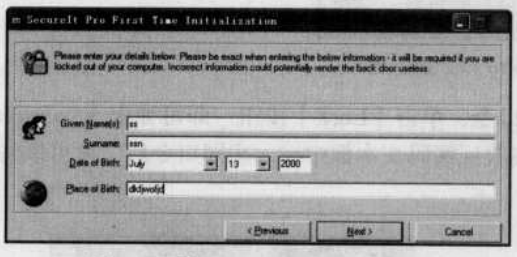


图 5-60 【SecureIt Pro First Time Initialization-2】对话框

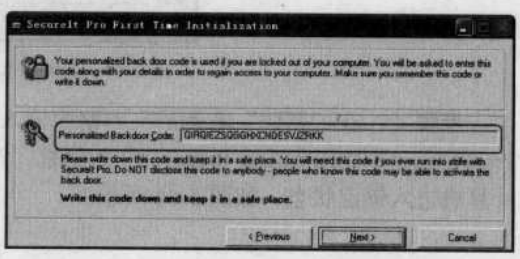


图 5-61 【SecureIt Pro First Time Initialization-3】对话框

步骤 5：单击【Next】按钮，即可打开【SecureIt Pro First Time Initialization-4】对话框，要求用户在仅有的空白文本框中填写前面自动生成的后门口令，如图 5-62 所示。

步骤 6：单击【Next】按钮，即可打开【SecureIt Pro First Time Initialization-5】对话框，如图 5-63 所示。单击右下角 按钮，即可弹出“SecureIt Pro”提示框，提示“已输入的信息不能更改，是否继续？”，单击【是】按钮，即可完成整个初始化操作，如图 5-64 所示。

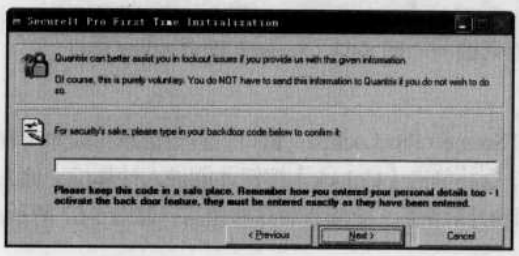


图 5-62 【SecureIt Pro First Time Initialization-4】对话框

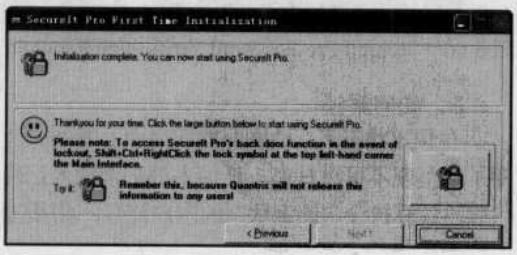


图 5-63 【SecureIt Pro First Time Initialization-5】对话框

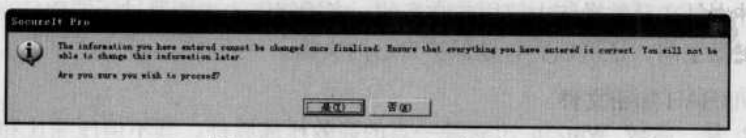


图 5-64 “SecureIt Pro”提示框

注意 在因遗忘密码而被锁定时，如果想使用后门口令，请使用“Shift+Ctrl”组合键并右击SecureIt Pro程序主界面左上角的锁定标记。

2．设置登录口令

在开始使用SecureIt Pro之前，先要设置进入的口令。这样才能在以后利用这个口令来锁定计算机，反之，用来开启这个锁。具体的操作步骤如下。

步骤1：双击桌面上的“SecureIt Pro”应用程序图标，即可弹出【SecureIt Pro口令设置】窗口，在其中可以设置进入时的口令，如图5-65所示。

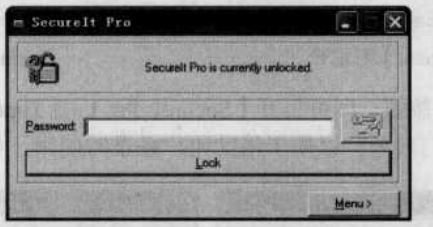


图5-65　SecureIt Pro口令设置窗口

步骤2：在“密码”右侧的文本框中输入口令，单击【Lock】按钮，即可弹出【SecureIt Pro-Password Verification Required】对话框，在验证密码文本框中输入相同口令后，就可以将计算机进入锁定状态，如图5-66所示。

图5-66　SecureIt Pro-Password Verification Required对话框

图5-67　SecureIt Pro-Locked窗口

3．如何解锁

在锁定状态下，他人只能在桌面上看到一个“SecureIt Pro-Locked”窗口，其他信息（如原有程序）都呈现不可见状态。任何人都必须输入正确口令并单击【Unlock】按钮才能进入计算机。他人可以给计算机设定锁定状态的用户留言，当用户回到计算机后，就能查看这些留言，如图5-67所示。

第49招　WinRAR压缩文件加密解密

压缩文件也是在日常操作中使用非常多的，将所制作的文档通过压缩软件来实施加密，不仅可以减小磁盘空间，还可以更好地保护自己的文档。

1．用WinRAR加密文件

WinRAR是一款较WinZip出版晚一点的高效压缩软件，其不但压缩比和操作方法都较WinZip优越，而且能兼容ZIP压缩文件，可以支持RAR、Zip、ARJ、CAB等多种压缩格式，

并且可以在压缩文件时设置密码。具体的操作步骤如下。

步骤 1：用鼠标右击需要压缩并加密的文件，在快捷菜单中选取【添加到压缩文件】选项，在【压缩文件名和参数】对话框中设置压缩文件的名称及压缩格式，如图 5-68 所示。

步骤 2：切换到【高级】选项卡，如图 5-69 所示。单击【设置密码】按钮，即可打开【带密码压缩】对话框，如图 5-70 所示。在其中输入密码后，连续单击【确定】按钮，即可生成加密的 RAR 文件。

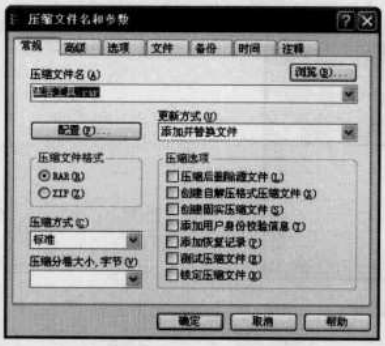


图 5-68 设置压缩选项

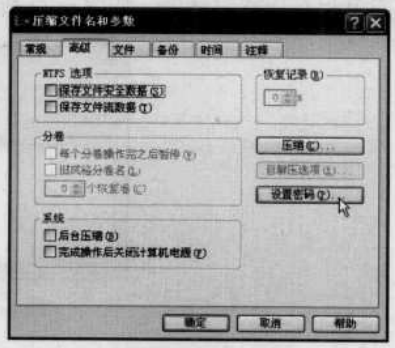


图 5-69 【高级】选项卡

2. RAR Password Recovery

RAR Password Recovery 软件是专为解除 RAR 压缩文件的密码而制作，其操作界面如图 5-71 所示。单击【打开】按钮，在其中选择需要解除密码的 RAR 文件。选择破解方式并在相应选项卡中设置其选项。单击【开始】按钮，即可开始破解。

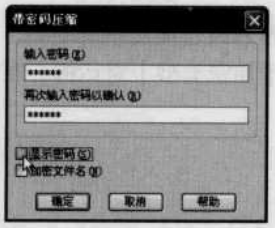


图 5-70 【带密码压缩】对话框

图 5-71 RAR Password Recovery 主窗口

第 50 招 Word 文件的加密解密

大多数文档编辑都是在 Word 中完成的，这就必然涉及一些隐私或机密文件的安全问题。于是，对 Word 文件进行加密就势在必行了。

1. Word 自身功能加密

Word 自身提供了简单的加密功能，可以通过下面两种方法轻松实现。

（1）使用“版本”命令

“版本”功能可以让用户在编辑过程中把文档保存成不同的“版本”，以便日后对文档进行查看与修改。其实利用这个功能，用户还可在一个 Word 文件中隐藏并保存多个独立文档，就像一个 Excel 工作簿具有多个电子表格一样，很利于文件的管理。

具体的操作方法如下。

步骤 1：新建一个文档并输入编辑一个文档内容之后，选择【文件】→【版本】菜单项，即可打开保存版本对话框，如图 5-72 所示。

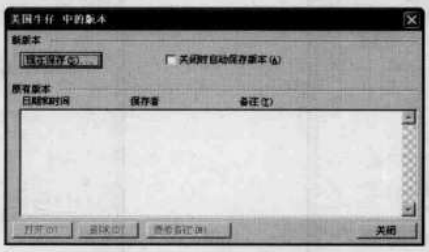


图 5-72　保存版本对话框

步骤 2：单击【现在保存】按钮，即可打开【保存版本】对话框，在“版本备注”文本框中输入当前文档的标题或简单说明之后，单击【确定】按钮，即可将当前文本保存下来。

步骤 3：将原来编辑的内容全部删除之后，再重新输入编辑一个新的文档内容，并重复上述操作，将新文档内容保存成另一个版本。将工作区中的所有内容全部删除，并选择【文件】→【保存】菜单项，将当前文档保存。

这样，当别人打开该文档时眼前就会显示一片空白，还以为是一个空白文档呢？只有选择【文件】→【版本】菜单项，在打开的对话框中选择所需版本并单击【打开】按钮，才可以浏览到其中的内容。

（2）利用【选项】功能

利用选项功能进行加密的具体操作方法如下。

步骤 1：编辑或打开一个需要加密的文档，选择【工具】→【选项】菜单项，即可打开【选项】对话框，如图 5-73 所示。

步骤 2：在【安全性】选项卡中可以设置当前文档的密码以及修改当前文档的密码（这两个密码可以相同，也可以不同），单击【高级】按钮，即可打开【加密类型】对话框，在其中选择密码类型以及密钥长度，如图 5-74 所示。

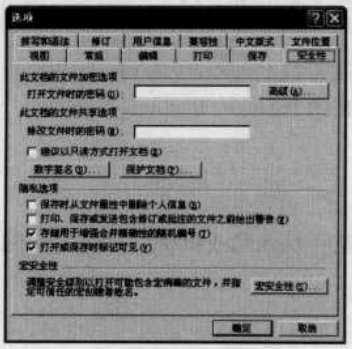


图 5-73　【安全性】选项卡

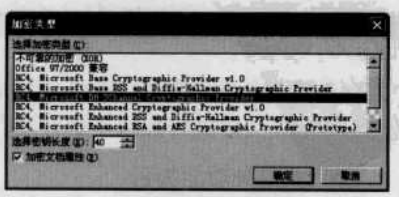


图 5-74　【加密类型】对话框

2．使用 Word Password Recovery 解密 Word 文档

Word Password Recovery 是一款专门用于对 Word 文档进行解密的工具，其操作界面如图 5-75 所示。在该软件中用户可设置不同解密方式，从而提高解密的针对性，加快解密速度。

具体的操作步骤如下。

步骤 1：单击【Browse】按钮，即可在打开的对话框中选择需要解密的 Word 文档。

步骤 2：在【Brute-force】选项卡中可设置解密时密码的长度范围以及允许参与密码组合的字符；在【Booost-Up Engine】选项卡中可选择最佳密码组合以及破解速度和密码破解能力；在【Dictionary】选项卡中可选择破解时所使用的字典文件；在【Options】选项卡中可设置破解过程中自动保存的时间间隔等。

步骤 3：在设置完成之后，单击【Start】按钮，即可开始破解。在破解完毕之后，将弹出【Password recovered】对话框，并在“Statistics”区域中显示相关信息，如图 5-76 所示。

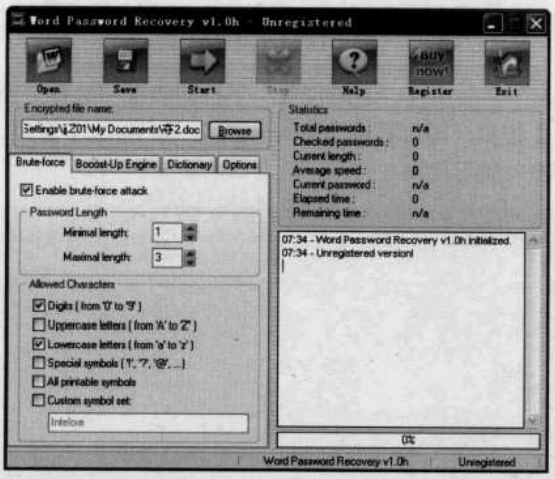


图 5-75 Word Password Recovery 操作界面

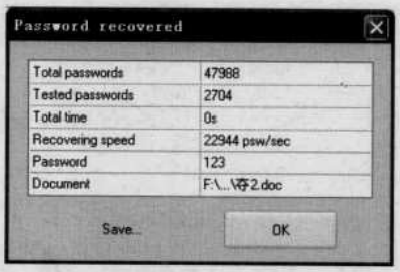


图 5-76 【Password recovered】对话框

第 51 招 宏加密解密技术

在 Microsoft Office 套件中内嵌了一个 Visual Basic 编辑器，它是宏产生的源泉。使用宏同样可将 Word 和 Excel 文档进行加密。对 Word 文档而言，最大的敌人当然就是宏病毒了。

1．使用宏进行加密

在 Word 里使用宏进行防范设置十分简单，选择【工具】→【宏】→【安全性】菜单项，即可打开如图 5-77 所示的对话框，确保选中“高”或“中”选项。这样，以后每打开一个文档，系统都会检查它的数字签名，一旦发现是不明来源的宏，即可将它置之门外。

另外，为阻止可恶的宏病毒在打开文件时自动运行并产生危害，可以在打开一个 Office 文件时，很容易阻止一个用 VBA 写成的在打开文件时自动运行的宏的运行。

选择【文件】→【打开】菜单项，在【打开】对话框中选择所要打开的文件名称，在单击【打开】按钮时按住 Shift 键，Office 将在不运行 VBA 过程的情况下，打开该文件。按住 Shift 键阻止宏运行的方法，同样适用于选择【文件】菜单底部的文件（最近打开的几个文件）。

同样，在关闭一个 Office 文件时，也可以很容易地阻止一个用 VBA 写成，将会在关闭文件时自动运行的宏。从中选择【文件】→【关闭】菜单项，在单击【关闭】按钮时按住 Shift

键，Office 将在不运行 VBA 过程的情况下关闭这个文件（按住 Shift 键同样适用于单击窗口右上角的“×”关闭文件时阻止宏的运行）。其实，还可以利用宏来自动加密文档，选择【工具】→【宏】→【宏】菜单项，即可打开【宏】对话框，如图 5-78 所示。

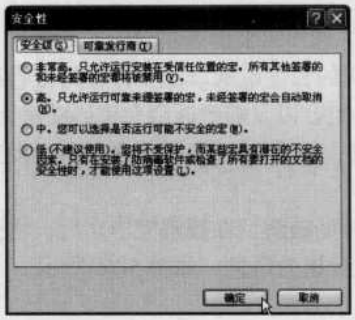


图 5-77 【安全性】对话框

图 5-78 【宏】对话框

在“宏名”文本框中输入“AutoPassword”之后，在“宏的位置”下拉列表框中选择“所有的活动模板和文档”选项，再单击【创建】按钮，即可显示【Microsoft Visual Basic】窗口，如图 5-79 所示。在“End Sub”语句的上方插入如下代码：

```
With Options
    .AllowFastSave = True
    .BackgroundSave = True
    .CreateBackup = False
    .SavePropertiesPrompt = False
    .SaveInterval = 10
    .SaveNormalPrompt = False
    End With
    With ActiveDocument
    .ReadOnlyRecommended = False
    .EmbedTrueTypeFonts = False
    .SaveFormsData = False
    .SaveSubsetFonts = False
    .Password = "2009"
    .WritePassword = "2009"
    End With
    Application.DefaultSaveFormat = ""
```

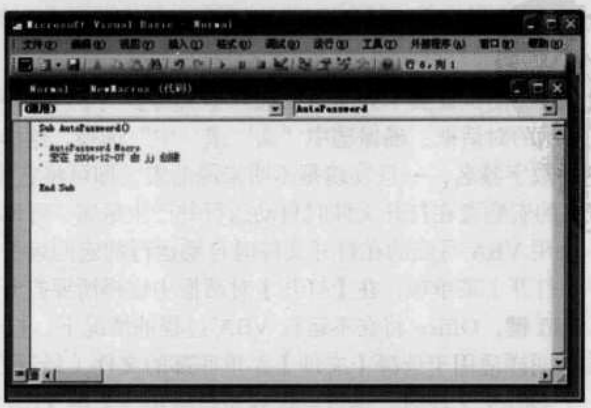


图 5-79 Microsoft Visual Basic 窗口

其中的.Password = "2009"表示设置打开权限密码，.WritePassword="2009"表示设置修改权限密码。在输入完上述代码之后，选择【文件】→【保存 Normal】菜单项，再执行关闭并返回到 Microsoft Word 即可。

2．解除宏密码

VBA Key 是一款专门用于 Office 文档通过宏加密后的解密工具，其操作界面如图 5-80 所示。其操作方法非常简单，只需单击【Recover】按钮，在【Recover】对话框中选择需要破解的文档。单击【打开】按钮，即可按照用户设置好的条件进行破解。在找到密码之后，将给出具体提示信息。

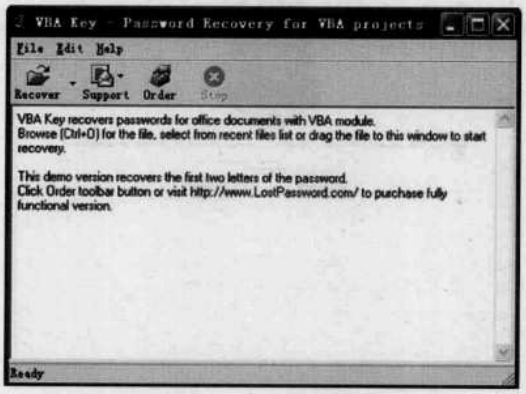


图 5-80　VBA Key 操作界面

第 52 招　系统全面加密 PC Security

系统级的加密工具 PC Security 可以帮助大家锁定互联网、任何文件与目录、任何磁盘分区和系统等。

1．锁定驱动器

使用 PC Security 锁定驱动器是很简单的事情，以锁定存储有重要文件的 D 盘为例，在 PC Security 安装完毕后，在【我的电脑】窗口中右击 D 盘盘符，从快捷菜单中选择【PC Security】→【Lock】选项，即可完成对 D 盘的锁定操作，如图 5-81 所示。

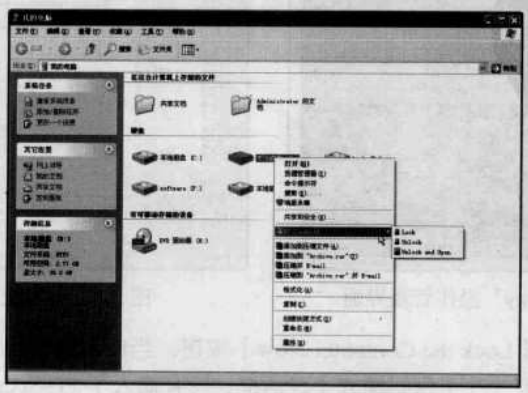


图 5-81　“我的电脑”窗口

2. 锁定系统

PC Security 可以完成多种方式的系统锁定，下面逐一进行讲述。

（1）即时锁定系统

如果需要暂时离开计算机，为防止他人恶意操作自己的计算机，就可以即时锁定自己的计算机系统。具体的操作步骤如下。

步骤 1：下载并安装“PC Security”软件，双击桌面上的“PC Security”应用程序图标，即可弹出“密码输入”窗口，如图 5-82 所示。

图 5-82 “密码输入”窗口

步骤 2：在“Password”文本框中输入正确的登录密码（默认为 Security），即可登录“PC Security”操作管理界面。如图 5-83 所示。

步骤 3：在登录操作管理界面后，单击“System Lock”链接，即可进入“系统锁定”设置界面，如图 5-84 所示。

图 5-83 “PC Security”操作管理界面

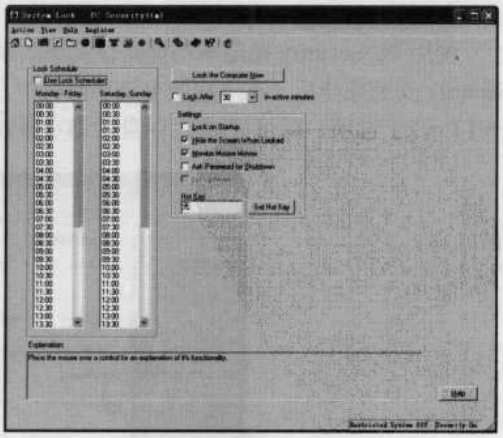


图 5-84 “系统锁定”设置界面

步骤 4：单击右侧【Lock the Computer Now】按钮，当前系统将自动切换到类似屏幕保护的状态，在屏幕窗口中有一个【密码输入】对话框，只有输入了 PC Security 的登录密码才能恢复系统的正常使用状态。

（2）启动时锁定系统

采用启动时锁定系统功能，可彻底地解决 Windows XP 系统不需密码就登录系统的安全隐患。在此功能启用后，当用户登录 Windows XP 系统时，在【登录】对话框中单击【确定】按钮，将会自动进入类似屏幕保护状态的 PC Security 登录状态。使用方法很简单，只需单击“系统锁定”界面中的“Lock on Startup”选项即可，如图 5-85 所示。

（3）指定时间锁系统

若勾选“Lock After‘ ’in-active minutes”选项，在数字栏中输入所需的数字后，PC Security 就会自动地在指定的时间内若无活动就将系统锁定，如图 5-86 所示。

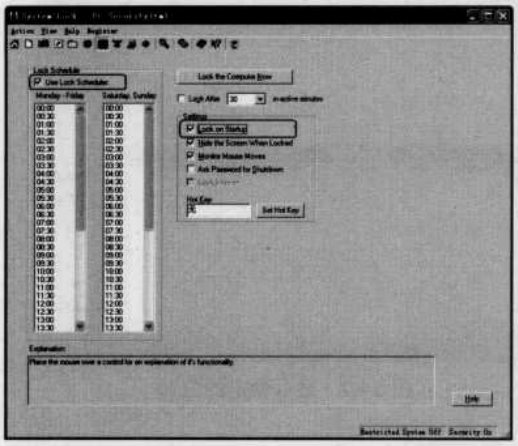


图 5-85 设置“Lock on Startup”选项

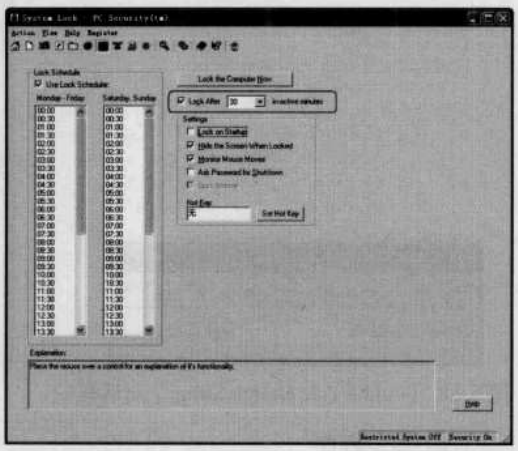


图 5-86 设置“Lock After‘ ’in-active minutes”选项

（4）锁定活动窗口

如果大家在运行程序时来了一个朋友要借用一下计算机，这个时候往往不方便将正在运行的程序关闭，但又不想让朋友打开正在运行的程序。这个看起来很麻烦的问题，通过 PC Security 将会很容易地被解决。具体的操作步骤如下。

步骤 1：在登录操作管理界面中单击“Windows Lock”链接项，即可打开“窗口锁定”设置界面。如图 5-87 所示。

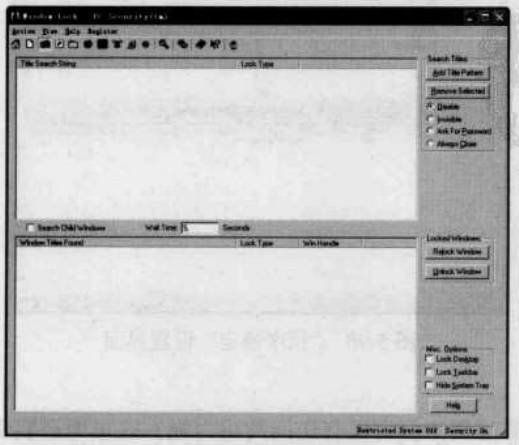


图 5-87 “窗口锁定”设置界面

步骤 2：单击窗口【Add Title Pattern】按钮，即可弹出【Add a Title Search String】对话框，再单击“Window Title”右侧下三角按钮，在当前运行程序列表中选择要锁定的程序，单击【OK】按钮，返回“窗口锁定”设置界面，如图 5-88 所示。

步骤 3：在“窗口锁定”设置界面中勾选“Disable”、“Invisible”等所需选项后，单击【Relock Window】按钮，即可打开【窗口锁定】窗口。此时可看到选中的程序列表，从其下方状态列表中可以看出当前程序为禁止使用状态，如图 5-89 所示。

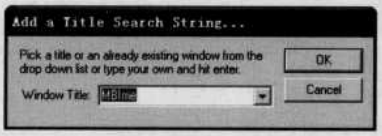


图 5-88 【Add a Title Search String】对话框

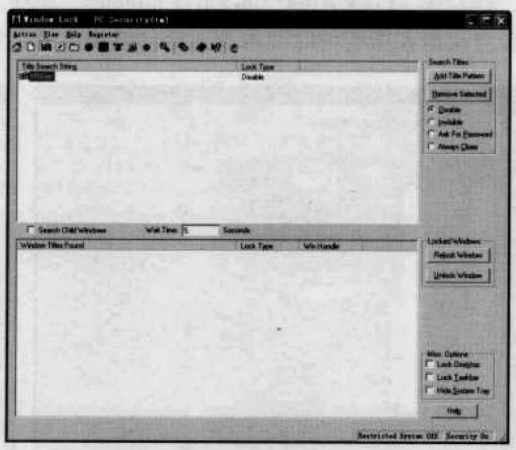


图 5-89 显示锁定的窗口

（5）锁定程序

如果系统中有一些很重要的程序不方便被其他使用，也可以使用 PC Security 来完成程序的锁定。在登录操作管理界面中单击“Program Lock”链接项，即可打开“程序锁定”设置界面。通过展开目录选项中需锁定的程序，单击中间的锁定方式（只读或完全），单击【Lock】按钮，即可锁定程序，如图 5-90 所示。

图 5-90 “程序锁定”设置界面

3. 验证加密效果

究竟锁定目录对于非法用户们有没有访问约束力呢？这里通过实例介绍一下，先使用 PC Security 将服务器的 D 盘下的 IMA 目录锁定，通过局域网中另一台计算机对服务器进行木马控