IT 培训认证系列教程

新编网络安全教程

北京希望电子出版社　总策划
中科希望技术培训学校　主　编

科学出版社
www.sciencep.com

IT 培训认证系列教程

新编网络安全教程

北京希望电子出版社　总策划
中科希望技术培训学校　主　编

科学出版社
www.sciencep.com

内 容 简 介

本书主要介绍了网络安全和防护方面最重要的概念及相关知识。通过本教程的学习，读者将具备必要的网络安全知识，并且能够利用这些基础知识和相应的安全防护工具，比如防火墙、入侵检测系统等，提供的安全措施对系统进行安全保护。

全书共分为 10 章，内容包括：网络安全基础知识，网络防护设计，风险分析和安全策略设计，选择和设计防火墙，配置防火墙，加强和管理防火墙，虚拟专用网（VPN），入侵检测系统，计算机犯罪及计算机取证以及 Windows 系统安全应用等。本书内容新颖全面，是系统安全工程师、网络安全管理员和信息系统工程师以及有志于从事系统和网络安全管理的工程人员的首选书籍。

需要本书或技术支持的读者，请与北京中关村 083 信箱（邮编 100080）发行部联系，电话：010-82702660 010-82702658 010-62978181 转 103 或者 238，传真 010-82702698，E-mail：tbd@bhp.com.cn。

图书在版编目（CIP）数据

新编网络安全教程 / 中科希望技术培训学校主编. —北京：科学出版社，2005.6

（IT 培训认证系列教程）

ISBN 7-03-015295-6

Ⅰ. 新… Ⅱ. 中… Ⅲ. 计算机网络—安全技术—技术培训—教材 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2005）第 026902 号

责任编辑：郭淑珍 / 责任校对：向 云

责任印刷：东 升 / 封面设计：梁运丽

科学出版社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

北京市东升印刷厂印刷

科学出版社发行 各地新华书店经销

*

2005 年 6 月第 一 版 开本：787×1092 1/16

2005 年 6 月第一次印刷 印张：24 1/4

印数：1—3 000 字数：561 000

定价：30.00 元

前　言

随着计算机网络的发展，网络的开放性、共享性以及互连程度随之扩大，普通用户上网的机会也越来越多。与此同时，网络入侵事件日益增多，网络安全性问题也就日益严重。本书主要介绍了网络安全和防护方面最重要的概念及相关知识。通过本书的学习，读者将具备必要的网络安全知识，并且能够利用这些基础知识和相应的安全防护工具所提供的安全措施来保护系统。本书的主要目的是向读者介绍网络安全方面的基础知识，主要内容包括：安全策略开发以及通过实施网络地址转换（NAT）、包过滤，通过安装代理服务器、防火墙、虚拟专用网（VPN）实施安全策略的具体方法和步骤。

本书由 10 章组成。第 1 章网络安全基础介绍了网络安全的基础知识，重点讲述了入侵者入侵的方式、TCP/IP 协议以及工作站的安全性等方面的知识。第 2 章介绍了网络防护设计方面的知识，内容涉及建立网络安全防护层次的方法，以及有关加密、认证、包过滤以及病毒防护等方面的概念。此外，在本章中读者还将学习到怎样利用入侵检测系统对攻击活动进行检测，以及怎样对安全报警进行响应。第 3 章重点讨论了风险分析的基本概念，风险分析方法以及安全策略的设计步骤。第 4 章讨论了防火墙的基本概念以及建立防火墙周边以及确定所需要的安全组件的方法。第 5 章配置防火墙，向读者介绍了一个防火墙具有的基本功能。第 6 章主要讲述如何强化防火墙功能和对防火墙进行有效管理的基本常识。第 7 章对 VPN 的概念、技术、协议，以及 VPN 的加密方案等进行详细的讨论。第 8 章从概念和理论知识方面讲述入侵检测系统的分类、入侵检测技术、主要的入侵检测模型等内容；然后从应用的角度讨论入侵检测系统的组件以及入侵检测系统的部署。第 9 章讨论了计算机取证的相关内容。第 10 章介绍了在 Windows 系统中保障系统安全的方法。

本书中插入的大量应用范例及图表，对读者掌握书中介绍的知识和技能提供了很大帮助。本书条理清楚，结构明晰，既有理论知识，又有动手操作，是一本很好的培训及参考用书。本书在编写过程中参考了许多网络上的资源，在此对这些作者表示感谢。

本书得到以下项目的资助：

国家高技术研究发展计划（863）资助（项目编号：2003AA144030）

国家自然科学基金资助（项目编号：90204016）

国家 973 项目资助（项目编号：2004CB318004）

本书主要由刘在强、王大印、姜中华、王为编写，其中吴庆畅、姚婉芹、雷启军、徐津、程斌、宝力高、杨宁、钟仕增、丁国栋、马喜、王飞、付华杰、魏新在、肖建芳也参与了本书的部分内容的编写和编排工作，在此表示感谢。尽管编者尽心尽责，但由于时间仓促，疏漏之处在所难免，望广大读者提出宝贵意见。

编者衷心感谢信息安全国家重点实验室的林东岱研究员以及中国科学院信息安全国家重点实验室的各位同志在本书写作过程中给予的指导和协助。

目　录

第 1 章　网络安全基础知识

本章重点：

- ✓ 入侵范式剖析
- ✓ 认识攻击者
- ✓ 网络安全目标
- ✓ TCP/IP 网络
- ✓ 路由技术
- ✓ 工作站安全防护

随着计算机网络的发展，网络的开放性、共享性、互连程度随之扩大。普通用户上网的机会也越来越多。与此同时，网络入侵事件日益增多，网络安全性问题日益严重。来自美国首都华盛顿的消息说，根据美国联邦调查局的一项最新调查结果，大部分大型企业和政府机构都遭到过计算机黑客的攻击。这次调查的被访者说他们遭遇每次计算机犯罪平均会损失至少 4.55 亿美元，而前一年的平均损失为 3.77 亿美元。由此可见，在网络给社会带来极大便利的同时，也使使用计算机上网、发布及传输信息的用户、公司、企业等单位遭受攻击的风险。

目前造成网络不安全的主要因素是在协议、系统及数据库等设计上存在缺陷。网络互连一般采用 TCP/IP 协议，它是一个工业标准的协议簇，但该协议簇在制订之初，对安全问题并没有考虑太多，协议中存在很多的安全漏洞。对于操作系统，由于目前使用的计算机网络操作系统在本身结构设计和代码设计时偏重于考虑系统的使用方便性，导致了系统在远程访问、权限控制和口令管理等许多方面存在安全漏洞。同样，数据库管理系统（DBMS）也存在权限管理、数据的安全性及远程访问等许多方面问题，在 DBMS 或应用程序中能够预先安置从事情报收集、受控激发破坏程序。由此可见，针对协议、系统及数据库等，无论是其本身的设计缺陷，还是由于人为因素造成的各种漏洞，都可能被一些另有图谋的攻击者利用进行网络攻击，因此要保证网络信息的安全，必须熟知黑客网络攻击的一般过程，在此基础上才能制定防范策略，确保网络安全。

本章将介绍基本的与网络安全相关的知识。在本章的开始向读者介绍了攻击者通常采用的入侵广式，并对其进行了分析和演示，希望读者通过这部分内容认识入侵者采用的攻击技术以及攻击者的攻击步骤和方法，明确计算机及网络安全防范的目标和责任；随后，本章引导读者进一步认识各种不同的入侵和入侵者，以及网络安全和入侵检测的目标；接下来，本章介绍了与网络安全息息相关的知识点，包括：TCP/IP 协议、路由、访问控制以及怎样保护个人计算机。最后，介绍了有关怎样保护 Web 服务器和基于 Web 的通信的安全性方面的知识。

1.1 入侵范式剖析

本节将介绍入侵者通常采用的典型的入侵范式，并介绍一次典型的入侵过程。通过此节内容的学习，可以使读者认识入侵者采用的攻击技术以及攻击者的攻击步骤和方法，同时也可使读者了解计算机及网络安全防范的目标和责任，以便在今后的网络安全防护工作中，做到知己知彼，有的放矢。

1.1.1 入侵范式介绍

大部分入侵者常常采用的一种入侵流程或模式，并遵循一定的规律，这就是入侵范式。对其掌握并不需要高级的技术。通常情况下，借助于一些现成的入侵工具普通用户就可发动入侵。入侵范式不仅适用于 Windows 2000/XP 操作系统，也同样适用于 Linux 及其他其他类型的操作系统，只是具体使用的入侵工具以及利用的系统漏洞有所差别。入侵范式大致可以分为收集信息、暴力破解、提升权限、安装后门、隐藏行踪等几个过程，这些过程之间并没有严格的顺序限制，反而，往往这些过程相互交叠。

（1）收集信息

信息收集通常是攻击者发动攻击的第一步工作。信息收集本身并不会对目标本身造成危害，只是被用来为进一步入侵提供有用的信息。攻击者常使用下面的一些方法或者下面方法的组合实施对目标系统的信息收集。

- 扫描技术

  扫描技术包括地址扫描、端口扫描、反响映射以及慢速扫描等方式。地址扫描是指运用 ping 这样的程序探测目标地址，对此作出响应的表示其存在。端口扫描指使用一些软件，对一定范围的主机连接一系列的 TCP/UDP 端口，扫描软件报告它成功地建立了连接的主机所开的端口的扫描方式。反响映射扫描通常是指向主机发送虚假消息，然后根据返回的消息特征判断出哪些主机存在。目前由于正常的扫描活动容易被防火墙侦测到，黑客转而使用不会触发防火墙规则的常见消息类型，这些类型包括：RESET 消息、SYN/ACK 消息、DNS 响应包等方式。慢速扫描方式是一种为了逃避扫描检测工具的检测而采用的是一种扫描方式。由于一般扫描检测工具的实现机制基于监视某个时间段内一台特定主机发起的连接的次数（例如每秒 10 次）来决定是否在被扫描，这样攻击者可以通过使用扫描速度慢一些的扫描软件逃避扫描检测工具的检测。

- 体系结构探测

  攻击者借助具有已知响应类型的数据库的自动工具，向目标主机发送伪造的数据包，然后对目标主机响应返回的消息进行分析以确定目标主机系统的类型。由于每种操作系统都有其独特的响应方法（比如 Windows NT 和 Solaris 的 TCP / IP 堆栈具体实现有所不同），通过将此独特的响应与数据库中的已知响应进行对比，攻击者经常能够确定出目标主机所运行的操作系统。

- 利用信息服务

利用信息服务进行信息收集的方式包括 DNS 域转换、Finger 服务、LDAP 服务等。DNS 域转换是指 DNS 协议通常不对信息进行身份认证，攻击者可以利用此特点发动攻击。攻击者只需实施一次域转换操作就能得到一台公共的 DNS 服务器上的所有主机的名称以及内部 IP 地址。Finger 服务信息搜集方式是指使用 finger 命令来刺探一台 finger 服务器以获取关于该系统的用户的信息的方式。LDAP 服务信息搜集方式是指通过 LDAP 协议窥探网络内部的系统和它们的用户信息的方式。

（2）暴力破解

得到帐号列表后，可借助于密码破解工具和字典工具，用暴力试验的方法得到用户帐户和密码。根据实现的原理，暴力破解分为本地离线破解和远程破解两种方式。

- 字典

  所谓字典，其实就是一个包含有许多密码的文本文件。字典的生成有两种方式：用字典软件生成和手动添加。一般字典软件能生成包含生日、电话号码、常用英文名等密码的字典，不过由于这样生成的字典体积大，而且不灵活，所以攻击者往往会手动添加一些密码到字典里去，形成一个“智能化”的密码文件。

- 本地离线破解

  本地离线破解是指用软件选择一个在本地登录过的用户号码，然后挂上字典进行密码核对，或者借助于某些专用工具（@stake 公司的 LC4）对获取的密码文件或加密数据进行破解的方法。LC4 是破解 WINDOWS 密码文档 SAM 的专用工具，支持 WIN2000 的 SAM 破解，LC4 的工作方式是用字典结合暴力破解，LC4 本地破解的破解速度很快，而且成功率也比较高。本地破解又可以按顺序增加和通过字典对比两种方式破解。比如现在我要破解用户名为“Admin”的密码，我可以用 1 作为密码进行核对，如果正确则成功，如果不正确，则用 2 来核对，还不正确，则用 3，以此顺序增加，直到和密码相同为止。不过这样的破解效率是很低的，因为许多人的密码并不只是数字，所以这种方法并不常见。平时常用的是通过对比字典中密码的方法，因为字典可以做得很“智能化”，所以这种破解效率相对较高，特别是当你的密码是简单的数字，或是数字加一些英文名时特别明显。

- 远程破解

  远程破解和本地破解类似，只不过远程破解是通过向服务器发送信息来进行破解的，通常它受很多因素的影响，如计算机速度，网速、目标系统认证延迟系统等，因此通常较本地破解来说更为困难。不过，在不能获得密码文件或其他信息时，攻击者大多数情况下，采用这种方法。攻击者可以使用 Enum 等程序进行远程破解，猜口令，Enum 也可以使用指定的字典对远程主机的某个用户进行破解。

（3）提升权限

在上一步中，如果攻击者能获得目标系统的管理员密码，那么攻击者已经获得了目标系统的完全控制权。但通常情况下，管理员密码不易获得，常常得到的是普通用户的用户名和密码，这时攻击者还要设法通过已有的普通用户权限获得更高的管理员权限。从普通用户权限到 Administator 管理员的权限提升，也可以借助于一些专用黑客工具来实现。常用的权限提升方法包括：

- 缓冲区溢出

缓冲区溢出是进行攻击的最好办法，因为一般都可以获得系统权限或者管理员权限；不过很多远程溢出攻击不需要事先有执行程序的权限，而本地溢出就恰好适合提升权限。例如：Win NT4 的 IIS4 的 ASP 扩展有一个本地溢出漏洞，Windows 2000 的静态图像服务也有一个溢出漏洞，利用该漏洞，攻击者可以获得系统权限。

- 特殊漏洞利用

  特殊漏洞利用权限提升方法比较特殊，通常它依赖于具体的系统，不具有通用性。在 Windows 2000 进行权限提升的事例如下：在 TELNET 服务进程建立时，该服务会创建一个命名管道，并用它来执行命令。但是，该管道的名字能被预见。如果 TELNET 发现一个已存在的管道名，它将直接用它。攻击者利用此漏洞，能预先建立一个管道名，当下一次 TELNET 创建服务进程时，便会在本地 SYSTEM 环境中运行攻击者代码。这种攻击方法不适用于其他系统。

- 上传木马

  攻击者可以上传木马，然后运行木马，系统重起动后，木马就是本地登录用户的身份了，然后攻击者连接后就有了本地登录用户的权限。因为一般总是管理员本地登录系统，因此这样很可能就获得了管理员的权限。

（4）留后门

一般黑客都会在攻入系统后不只一次地进入该系统。为了下次再进入系统时方便一点，黑客会留下一个后门，特洛伊木马就是后门的最好范例，除此之外，留后门的方法还有很多，下面介绍几种常见的后门：

- Rhosts ++ 后门

  在 Linux 及 Unix 系统中，类似 Rsh 和 Rlogin 的服务是基于 rhosts 文件里的主机名使用简单的认证方法。用户可以轻易地改变设置而不需口令就能进入。入侵者向可以访问的某用户的 rhosts 文件中输入“++”，就可以允许任何人从任何地方无须口令便能进入这个帐号。

- 校验和及时间戳后门

  以前许多入侵者用自己的 trojan 程序替代二进制文件，系统管理员便依靠时间戳和系统校验和的程序辨别一个二进制文件是否已被改变，如 Linux 系统中的 sum 程序。时间戳后门就是入侵者为了对抗系统管理员的检查而发展的使 trojan 文件和原文件时间戳同步的新技术，其实现原理如下：先将系统时钟拨回到原文件时间，然后调整 trojan 文件的时间为系统时间。一旦二进制 trojan 文件与原来的精确同步，就可以把系统时间设回当前时间。Sum 程序是基于 CRC 校验，很容易骗过。入侵者设计出了可以将 trojan 的校验和调整到原文件的校验和的程序。

- 网络通行后门

  入侵者不仅想隐匿在系统里的痕迹，而且也要隐匿他们的网络通行。这些网络通行后门有时允许入侵者通过防火墙进行访问，有许多网络后门程序允许入侵者建立某个端口号并不用通过普通服务就能实现访问。因为这是通过非标准网络端口的通行，管理员可能忽视入侵者的足迹。这种后门通常使用 TCP、UDP 和 ICMP，但也可能是其他类型报文。

（5）隐藏踪迹

入侵者在离开目标系统之前，通常要隐藏自己的行踪，以便被发现或跟踪。入侵者常用的踪迹隐藏技术包括：

- 修改日志文件

  修改日志文件是指入侵者通过删除目标计算机审计系统中的与入侵相关连接记录、活动和操作等的日志文件或者日志文件中的记录来隐藏自己的方法。修改或删除日志文件可通过手工或者借助于第三方工具，比如 elsave.exe 等。

- 修改系统时间

  入侵者通过修改系统时间，使目标系统审计系统记录的日志的时间发生紊乱，从而达到迷惑系统管理员的目的。

- 进程隐藏

  进程隐藏是指入侵者使用重定向技术或者木马程序躲避 Windows 系统任务管理进程显示窗口或者 Linux 系统 ps 命令的显示技术。

1.1.2　入侵范式事例

1. 准备入侵工具和平台

（1）操作系统 Windows 2000/XP/2003。

（2）“流光”4.7。

（3）Windows 2000/XP/2003 系统下自带工具 net。

（4）日志清除工具：elsave.exe。

2. 工具介绍

（1）工具下载

- “流光”4.7 可从流光主站下载：http://www.netxeyes.com。
- 日志清除工具 elsave.exe 也可从流光主站下载。

（2）“流光”4.7 功能说明

流光 4.7 是网络安全管理人员的一个功能强大的渗透测试工具，同时也是一个攻击者实施攻击的利器。

- 扫描功能

  流光的漏洞扫描较为强大，除了提供全面的扫描功能以外，利用 C/S 结构设计的扫描思想更是在众多复杂的应用场合脱颖而出。流光目前的漏洞扫描包括：POP3、FTP、IMAP、TELNET、MSSQL、MYSQL、WEB、IPC、RPC、DAEMON 等。

- 暴力破解功能

  提供 POP3/FTP/IMAP/HTTP/PROXY/MSSQL/SMB/WMI 的暴力破解功能。

- 网络嗅探功能

  利用 ARP 欺骗，对交换环境下的局域网内主机进行嗅探。和流光的漏洞扫描模块一样，网络嗅探也采用了 C/S 的结构，可以提供远程网络的嗅探功能。

- 渗透工具

包括 SQLCMD/NTCMD/SRV/TCP Relay 等辅助渗透工具。

● 字典工具

可以定制各种各样的字典文件，为暴力破解提供高效可用的字典。

（3）“流光”4.7 安装说明

“流光”4.7 的安装过程像其他 Windows 系统下的程序一样简单，双击下载的 Fluxay47Setup 安装文件，运行安装程序，然后按照提示进行，即可进行安装。

（4）“流光”4.7 主界面，如图 1-1 所示。

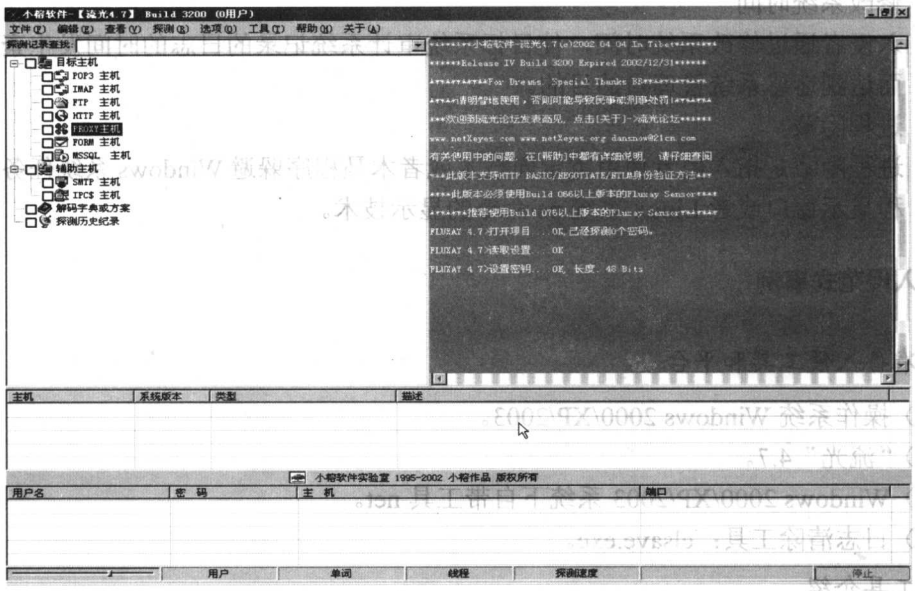

图 1-1 流光 4.7 主界面

（5）NET 命令

此命令的语法是：

```
NET [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
      HELPMSG | LOCALGROUP | NAME | PAUSE | PRINT | SEND | SESSION |
      SHARE | START | STATISTICS | STOP | TIME | USE | USER | VIEW ]
```

具体使用方法，请参考 Windows 系统下的帮助。

（6）日志清除工具 elsave.exe

日志清除工具 elsave.exe 是一款可以远程清除系统日志、应用程序日志、安全日志的软件。elsave.exe 使用起来很简单，首先利用获得的管理员账号与对方建立 IPC（进程间通信）会话：

```
net use \\targetIPAddress  password  /user: user
```

然后在命令行下执行如下命令：

```
elsave -s \\targetIPAddress  -l  logNameToClean  –C
```

这样就删除了安全日志。

3. 实施入侵

入侵者是怎么攻击网站或者他人计算机的？下面根据上面讲述的入侵范式，使用流光 4.7 等工具演示入侵者发动攻击的较简单的一种方法，以帮助读者加深对入侵范式的理解。

注意

下面讲述的内容仅供学习目的使用，其中的某些操作可能对网络其他用户有害。如果由此带来的一切法律后果由使用者自负。

（1）首先扫描一段 IP 地址，确定攻击目标。

步骤 1：运行流光 4.7，进入如图 1-1 所示的主界面。

步骤 2：选择 “探测”菜单下的“高级扫描工具”菜单项（见图 1-2），会出现“高级扫描设置”对话框（见图 1-3）。

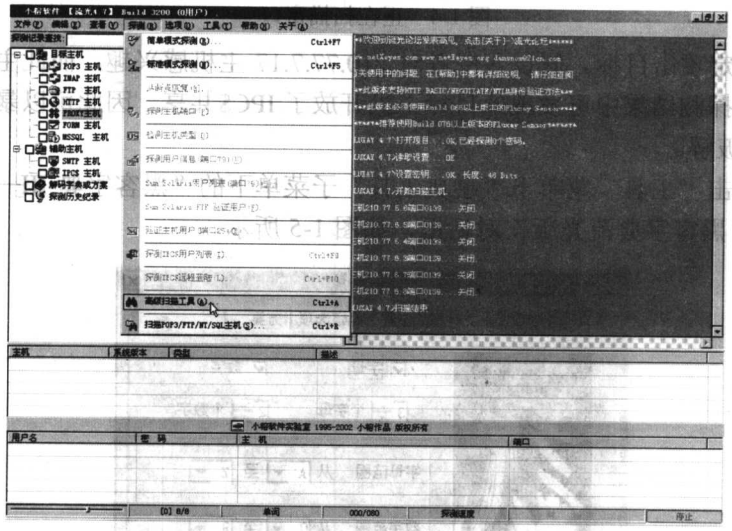

图 1-2　“高级扫描工具”菜单项

图 1-3　“高级扫描设置”对话框

步骤 3：在“设置”属性页面中，设置“开始地址”文本框为“210.77.7.1”，设置“结束地址”文本框为“210.77.7.255”；“目标系统”选择“ALL”。

步骤 4：单击“开始”按钮开始扫描，扫描探测结果如图 1-4 所示。

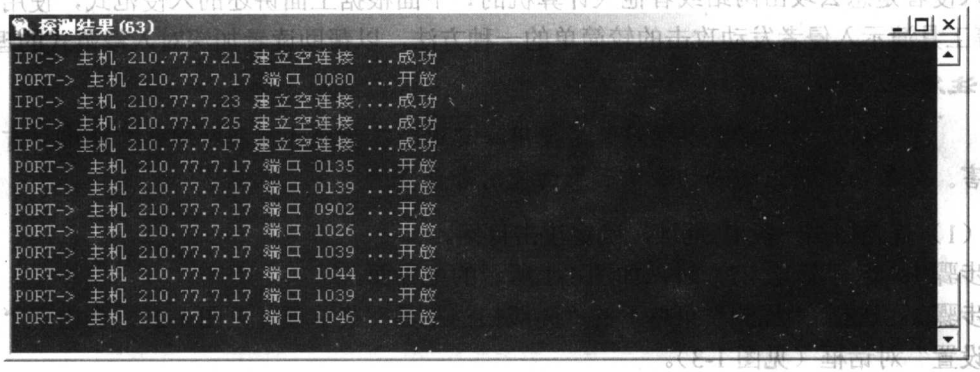

图 1-4 正在扫描窗口

步骤 5：确定攻击目标。假设入侵者对 210.77.7.17 主机感兴趣，而此主机开放了很多端口，从图 1-4 探测结果中可发现此目标主机开放了 IPC$共享，因此可以暴力破解。

（2）暴力破解。

步骤 1：单击“工具”菜单下“字典工具”子菜单下的“黑客字典 III—流光版”菜单项。弹出“黑客字典流光版”对话框，如图 1-5 所示。

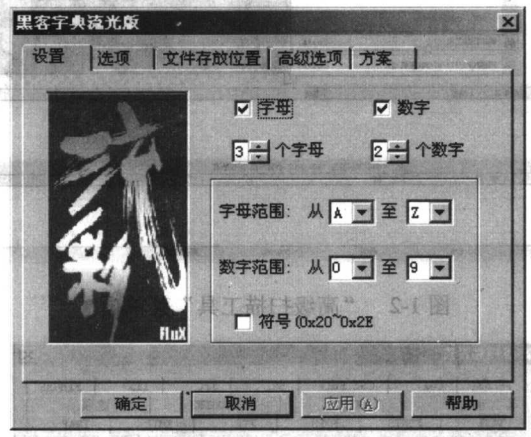

图 1-5 “黑客字典流光版”对话框

步骤 2：使用如图 1-5 所示流光的字典工具分别生成用户名字典和密码字典。

步骤 3：重新打开“高级扫描设置”对话框，在“设置”属性页面下重新设置“开始地址”文本框和“结束地址”文本框的值为“210.77.7.17”；选择“选项”属性页并设置“猜解用户名字典”和“猜解密码字典”分别为步骤 2 中生成的字典，如图 1-6 所示。

图 1-6　“高级扫描设置”对话框

步骤 4：单击“确定”开始暴力破解。破解结果如图 1-7 所示。

用户名	密码	主机	端口
lhy(Admin)	1976	210.77.7.17	IPC

图 1-7　破解结果

（3）提升权限。

由图 1-7 可知，入侵者以获得管理员权限。可直接进入下一步。

（4）留后门。

步骤 1：在命令提示符窗口中输入

```
C:\>net use \\210.77.7.17\IPC$ "1976" /user:"lhy"
```

这是用流光扫到的用户名为“lhy”，密码为"1976"的 IP 地址。

步骤 2：在命令提示符窗口中输入

```
C:\>copy srv.exe \\210.77.7.17\admin$
```

先复制 srv.exe 上去，在流光的 Tools 目录下就有（这里的$是指 admin 用户的 c:\winnt\system32\）。

步骤 3：在命令提示符窗口中输入

```
C:\>net time \\210.77.7.17
```

查查时间，发现 210.77.7.17 的当前时间是 2004/3/21 上午 10:35，命令成功完成。

步骤 4：在命令提示符窗口中输入

```
C:\>at  \\210.77.7.17  10:38  srv.exe
```

用 at 命令启动 srv.exe。

步骤 5：使用 net time 命令再查一查目标主机的时间。如果目标主机的当前时间是