信息安全大系

- 精选近100个案例，为初学者量身打造
- 涵盖E-mail、QQ和MSN密码，远程控制，系统漏洞，扫描与嗅探等实用的攻防技术
- 一线计算机安全专家汇聚多年经验精心编著

黑客攻防

入门与提高

陈芳　秦连清　肖霞　编著

人民邮电出版社
POSTS & TELECOM PRESS

陈芳　秦连清　肖霞　编著

黑客攻防

入门与提高

人民邮电出版社

北京

图书在版编目（CIP）数据

黑客攻防入门与提高 / 陈芳，秦连清，肖霞编著. —北京：人民邮电出版社，2009.4
ISBN 978-7-115-19526-5

Ⅰ. 黑… Ⅱ. ①陈…②秦…③肖… Ⅲ. 计算机网络－安全技术 Ⅳ. TP393.08

中国版本图书馆CIP数据核字（2008）第201710号

内 容 提 要

本书是指导初学者学习如何防御黑客攻击的入门书籍。书中详细地介绍了初学者在防范黑客攻击时必须掌握的基本知识，对初学者在防御黑客攻击时经常遇到的问题给予了专业性的解答，并通过实战案例给读者讲述了多种防范技术的具体应用。主要内容包括黑客攻击防范与端口扫描、Windows NT/2000/XP/2003 系统漏洞检测和安全策略、注册表恶意攻击的防范、蠕虫病毒剖析及防范策略、邮件病毒剖析及防范策略、U 盘病毒剖析及防范策略、专门查杀病毒工具应用、使木马改邪归正、防范木马与编程防范病毒实现等知识。

本书内容丰富，实战性和可操作性强，适合于网络技术爱好者、网络系统管理员阅读，也可作为相关专业学生的学习书籍和参考资料。

黑客攻防入门与提高

◆ 编　　著　陈　芳　秦连清　肖　霞
责任编辑　屈艳莲
执行编辑　张　涛

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京鸿佳印刷厂印刷

◆ 开本：787×1092　1/16
印张：14.25
字数：337 千字　　2009 年 4 月第 1 版
印数：1－4 000 册　　2009 年 4 月北京第 1 次印刷

ISBN 978-7-115-19526-5/TP

定价：28.00 元

读者服务热线：(010)67132692　印装质量热线：(010)67129223
反盗版热线：(010)67171154

前言

随着科学技术的飞速发展，计算机和因特网已基本普及到各家各户，成为人们获取信息和知识的重要工具。然而，病毒与木马的存在，让用户时常陷入困境，在不知不觉中落入病毒和木马的陷阱中。

本书以帮助用户深入了解计算机信息安全知识为出发点，详细地介绍了防御黑客攻击时必须掌握的基本知识，并对经常遇到的问题给予专业性的指导及得力的解决手段。

本书特点

- 内容丰富，实例经典

本书追求理论与实践的结合，用浅显的语言讲述精心设计的经典实例，将黑客攻防的基本理论和实践技巧融入到范例当中，全面覆盖计算机信息安全的各个角落。

- 贴近实战，讲解通俗

内容上作者都结合案例讲解每一个知识点，这些实例都是真实案例的提炼和总结。并且攻防的每一步都通过图解形式给出，通俗易懂、详略得当。

- 知识面宽，重点突出

本书涉及的内容众多，有基本的黑客攻防实战技巧，也有深入的黑客攻防编程技术，这是真正成为防范高手的晋级知识。每章都遵循“学习目标→攻防原理剖析→实战防范技术与技巧→案例总结”这种读者易于学习和实践的方式进行讲解，达到了授之以鱼，更授之以渔的目的。

本书内容

为了方便读者学习，本书分为 3 篇。

第一篇基础篇，主要包括黑客攻击防范与端口扫描、系统漏洞的剖析和防范、Windows 系统漏洞和安全策略、注册表的基本概念和操作、注册表恶意攻击的防范、计算机病毒、木马概述等内容。为了便于实践这些知识，讲述中主要用实例结合概念进行描述，读者可以清晰地学习到对付病毒与木马的各种攻防手段。

第二篇实战篇，包括蠕虫病毒剖析及防范策略、邮件病毒剖析及防范策略、U 盘病毒剖析及防范策略、专门的查杀病毒工具、常见木马的原理揭秘与清除、专门的查杀木马工具、使木马改邪归正等内容。通过本篇的学习，读者可以掌握更多的实战技术和技巧，有选择地进行有效防御和清除黑客的攻击，从而提高自己的实战能力。

第三篇编程篇，包括剖析木马与病毒的编程原理、VBS 脚本病毒解析和典型木马编程防

范等内容。本部分为提高晋级篇，通过了解典型病毒和木马的编程知识，可以从源头上掌握病毒和木马的攻击原理，从而找到更有效的防御途径，制作出有针对性的查杀工具。

本书由陈芳、秦连清、肖霞主编，在编写过程中，张博、范洪斌、裴要强、王洪、管西京、夏添、柯华坤、王大平、林丁报、张英男、张鹏、刘冉、李新峰、李金涛、温才燚、李连闯、李绍文等提供了很大帮助，在此表示感谢。

作者在写作中力求精确、时效，但由于网络病毒与木马发展迅速，加之作者水平有限，书中存有疏漏在所难免，恳请读者批评指正，以便共同提高，联系邮箱为：zhangtao@ptpress.com.cn。

编者

目录

第一篇　基础篇——揭开黑客的神秘面纱

第二篇 实战篇——攻防实战演练

第三篇 编程篇——自力更生查杀病毒

第一篇

基础篇

——揭开黑客的神秘面纱

第1章 黑客攻击防范与端口扫描

学习目标

通过本章的学习，使读者了解黑客对计算机网络系统进行攻击的流程和经常使用的方法，使读者初步认识到黑客如何找到目标计算机的，黑客如何寻找目标计算机漏洞的，从而一步步揭开黑客的神秘面纱。并在此基础上介绍了扫描器的知识，帮助读者理解端口扫描器的定义，通过对扫描工具应用实例介绍，读者可以一览使用扫描器进行扫描的全过程。

1.1 认识黑客攻击

随着网上银行、网络游戏的兴起，现实财富和网络虚拟财富已成为网友们日益关心的焦点。在这个同样存在着危机的虚拟世界里，几乎每位网民都面临着网络安全威胁，稍不注意，一旦受到黑客攻击，将付出惨重的代价。

为了最大限度地降低损失，做好安全防范工作是必要的。下面首先介绍黑客是如何找到计算机中的漏洞，并使用何种方法进行攻击的。只有了解其攻击手段，才能采取准确的对策来对付这些黑客。

1．一般步骤

虽然黑客入侵的目标不同，所使用的方法也不完全相同，但其主要攻击步骤还是有迹可循的。只有了解了这些攻击步骤，才能有效地找到阻止黑客入侵的方法。

黑客攻击一般遵循如下步骤。

（1）寻找目标主机。这是黑客进行攻击的第一步，也是黑客进行攻击的必要前提。通过各种方法得到目标主机的 IP 地址或域名，为攻击该用户打下基础。

（2）扫描目标主机。当找到目标主机的 IP 地址或域名后，利用扫描工具对目标主机进行扫描，然后通过筛选得到有用信息，例如端口、用户账号、网络资源信息等。随着扫描工具功能的日益增多，也可以直接通过扫描 IP 地址段来扫描主机。

（3）获取权限。通过扫描目标主机信息，进行网络攻击服务，获取网络资源，并进行远程口令猜解等操作，从而得到相应的权限，以便进行对磁盘写入操作。

（4）实施攻击。通过获取的权限，可以在目标主机上进行复制、删除等操作。不过，此时最重要的是在目标主机中安装木马程序，开启后门，为以后的再次入侵打好基础。

（5）清除痕迹。在退出目标主机时，进行日志等信息的清除，以免入侵时的记录被发现

后将木马程序删除并关闭后门。

2．常用方法

黑客在进行攻击时，并不是随机的，而是根据目标主机的相应漏洞，选择对应的攻击方法，达到简洁有效的攻击目的。

黑客攻击时常用的攻击方法有如下几种。

（1）获取口令。根据攻击目标的不同，选择获取口令的方法也不相同，获取口令可以分为如下3种。

- 通过网络监听非法获得用户口令，例如使用sniffer进行监听。此种方法虽然有一定局限性，但危害性极大，监听者往往能获得其所在网段的所有用户账号和口令。此种方法对局域网来说，威胁最大。
- 在得到用户的账号后，例如通过QQ查找功能查找到QQ号后，利用一些暴力破解软件强行破解用户口令。此种方法不受网段限制，但在破解时要有足够的耐心和时间。
- 获得服务器上的用户口令文件（如Shadow文件）后，采用暴力破解程序进行破解用户口令。采用此种方法的前提是，黑客必须首先获得口令文件，如Shadow文件。

在这3种方法中第3种方法危害最大，它不像第二种方法那样能反复地尝试登录服务器，而是在本地将加密后的口令与Shadow文件中的口令进行比较就能破解获取用户密码，尤其对一些弱口令用户，更是可以在很短的时间内得到口令。

（2）安装特洛伊木马程序。特洛伊木马程序最大的特点是可以直接侵入用户计算机并进行破坏。此类木马程序经常伪装成工具程序或者游戏软件诱使用户下载，一旦用户下载打开带有特洛伊木马的程序，此木马程序就会自动安装在计算机中。

此后，当用户再次连接到网络上时，此程序会通知攻击者用户上网的各类信息，例如IP地址、端口等。攻击者得到这些信息后，利用其中潜在的程序，可以任意地修改被攻击者计算机中的参数，从而实现控制计算机的目的。

（3）网站欺骗技术。很多人都以为在网络上任意浏览网站，进行注册都不会存在安全问题，事实上并不是这样。一些黑客利用某些网站的漏洞进行网站攻击，篡改网站网页，实现网页与黑客的URL相连接。当用户浏览目标网页时，事实上是向黑客服务器发出请求，此时黑客即可实现欺骗的目的。

（4）电子邮件攻击。目前，电子邮件已基本代替了书信成为人们联系的主要方式之一，一些黑客正是利用这一点来实施攻击的。电子邮件攻击一般有如下两种方式。

- 电子邮件炸弹。此种方法是利用伪造的IP地址和电子邮件地址，向同一邮箱发送无数的电子邮件，导致被攻击者的邮箱被关闭。更为严重的是，能导致电子邮件服务器操作系统死机。
- 电子邮件欺骗。相信网友们都曾遇到过此类信息，无论电子邮件厂商如何进行过滤，此类信息仍是层出不穷。攻击者以系统管理员（伪造）的身份，向用户发送邮件让其修改木马口令，或是发送看似正常的，但却带有木马程序的邮件。

（5）利用“肉鸡”攻击。“肉鸡”就是指黑客攻破的一台机器，但此机器会沦为黑客攻击其他机器的根据地，所有的操作都通过此机器进行。例如，攻击一网段内的一台机器后，利用此台机器的身份进行其他机器的攻击，在用户无防备的情况下，很容易实现攻击

目的。

（6）监听攻击。当两台机器进行通话时，若信息没有进行加密，此时只要使用某些网络监听工具，例如 sniffer，就可以轻易地截取口令、密码等重要信息。此种方法有一定的局限性，监听者一般只能获得所在网段内的用户账户和口令。

（7）利用系统漏洞。没有不透风的墙，同样也没有完全没有漏洞的系统，每个系统都存在或多或少的安全漏洞（Bugs），并且这些漏洞在发现初期是没有补丁可以下载的，如果黑客利用这些漏洞，很容易进行攻击。

（8）直接利用账号进行攻击。一些黑客常常利用系统提供的默认账户和密码进行攻击。一些用户在安装操作系统时，往往使用默认用户名，并且不设置口令，所以黑客很容易实现攻击目的。

1.2 端口扫描

一个端口就是一个通信通道，也可以说是一个入侵通道。通过对目标主机进行端口扫描，可以得到许多有用的信息，从而实现对目标主机的攻击。

在进行端口扫描时，可以手工输入命令进行扫描，也可以通过端口扫描器进行扫描。通过手工扫描的前提是要熟悉各种命令，然后可以对命令执行后的输入进行分析，而使用端口扫描器则相对简单，随着端口扫描方法使用的日益增加，端口扫描器的功能也越来越强，现在端口扫描器一般都对信息进行了详细地分析，让您可以一目了然，从而得到有用的信息。

根据参考对象的不同，端口有不同的划分方法，如果从端口的性质来分，通常可以分为以下 3 类。

1．公认端口（well known ports）

此类端口就是常用端口，其端口号从 0～1 024，它们绑定于一些特定的服务。通常，这些端口的通信明确表明了某种服务的协议，这种端口是不可再重新定义它的作用对象的。

2．注册端口（registered ports）

这类端口的端口号从 1 025～49 151。它们松散地绑定于一些服务，即使有许多服务绑定于这些端口，这些端口同样用于许多其他目的。这类端口一般没有明确的定义服务对象，不同程序可根据实际需要自定义。

3．动态和/或私有端口（dynamic and/or private ports）

这类端口的端口号从 49 152～65 535。从理论上说，不应把常用服务分配在这些端口上，但有些较为特殊的程序，特别是一些木马程序就非常喜欢用这些端口，因为这些端口很隐蔽，不容易被发现。

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地发现远程服务器的各种端口的分配及提供的服务等信息，从而间接地或直观地了解到远程主机所存在的安全问题。

扫描器并不能直接地攻击网络漏洞，它仅仅能帮助发现目标主机的某些内在弱点，但它不会提供进行攻击的详细步骤。

扫描器一般要拥有如下 3 个功能。

（1）发现一台主机或网络。

（2）发现主机后，进而查询此主机正在运行哪种服务。

（3）通过测试这些服务来发现漏洞。

常用的端口扫描工具有如下几种。

（1）TCP connect() 扫描 。这是最基本的 TCP 扫描方式。connect()是一种系统调用，由操作系统提供，用来打开一个连接。如果目标端口有程序监听，connect()就会成功返回，否则这个端口是不可到达的。

此项技术最大的优点是，不需要 root 权限。任何 UNIX 用户都可以自由使用这个系统调用。这种扫描很容易被检测到，因为在目标主机的日志中会记录大批的连接请求以及错误信息。

（2）TCP SYN 扫描 。此项技术被认为是“半开放”扫描，这是因为扫描程序不必打开一个完全的 TCP 连接。扫描程序发送的是一个 SYN 数据包，就像准备打开一个实际的连接并等待反应一样。

其中一个 SYN|ACK 的返回信息表示端口处于侦听状态，一个 RST 返回信号，表示端口没有处于侦听态。如果收到一个 SYN|ACK 信息，扫描程序必须再发送一个 RST 信号，来关闭这个连接过程。

此种扫描技术的优点在于一般不会在目标主机上留下记录，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。一些时候 SYN 扫描都不够秘密。某些防火墙和包过滤器会对指定的端口进行监视，有的程序能检测到这些扫描，此时，FIN 数据包可能会很容易地通过。此种扫描方法的目的是，关闭的端口会用适当的 RST 来回复 FIN 数据包，打开的端口会忽略对 FIN 数据包的回复。

此种方法能否实现和系统有很大的关联，有的系统不管端口是否打开，都回复 RST，此时这种扫描方法则就不管用。

（4）IP 段扫描 。此种方法并不直接发送 TCP 探测数据包，而是将数据包分成两个较小的 IP 段，实现将一个 TCP 头分成好几个数据包，从而过滤器就很难探测到。

（5）TCP 反向 ident 扫描。ident 协议允许（rfc1413）看到通过 TCP 连接的任何进程的用户名，即使这个连接不是由此进程开始的。此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 协议的一个重要特点是它支持代理（proxy）FTP 连接，即入侵者可以从自己的计算机***.com 和目标主机 1111.com 的 FTP server-PI（协议解释器）连接，来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。

（7）ICMP echo 扫描 。从实质上来说，这并不是扫描，但一些时候利用 ping 命令，来判断主机是否开机是很有用的。

1.3 常用端口扫描工具

一款好的端口扫描工具，是黑客进行攻击的重要利器，它可以快速有效地帮助黑客找到所需的信息，为进攻打好基础。

1．端口扫描工具概述

端口扫描工具很多，有综合型的，也有单一型的，根据需要选择相应的扫描工具，不但能减少扫描时间，还可以更有效地扫描出详细信息。

常用端口扫描器如下所示。

（1）IP 端口扫描器。IP 端口扫描器是专门扫描 IP 地址的端口扫描器，利用此工具可以快速查找被攻击者的 IP 地址。常用的有：Free IP Scanner、Angry IP Scanner 等。

（2）远程端口扫描器。利用远程端口扫描器可以快速查找到远程机器开放的端口，显示当外部用户尝试连接该计算机时，哪些端口可以使用。常用的有：ScanPort。

（3）局域网端口扫描器。局域网端口扫描器可以搜索计算机，包括计算机名、IP 地址、MAC 地址、所在工作组及用户；搜索共享资源，包括 HTTP、FTP 服务；搜索共享文件；多线程复制文件；发短消息；高速端口扫描等特点。常用的有：LanSee。

（4）路由器端口扫描器。因为很多服务器都是由防火墙或数据包筛选路由器保护的，所以黑客在进行攻击前对路由器的端口扫描是不可避免的。常用的有：Seekyou。

（5）3389 端口扫描器。3389 是远程连接的端口，用扫描器扫到打开 3389 端口的机器就能用微软自带的登录器远程登录。常用的有：X-Scan。

2．SuperScan

SuperScan 是一款功能强大的扫描器，速度非常快，可以查看本机 IP 地址和域名，可以扫描一个 IP 段的所有在线主机以及其可探测到的端口号。还可以保存和导入所有已探测的信息。是黑客扫描使用的常用工具之一。

使用此软件的具体操作步骤如下所示。

（1）解压下载得到的 SuperScan 文件，如图 1-1 所示。此软件无需安装，运行主程序即可打开如图 1-2 所示的“SuperScan4.0”对话框。

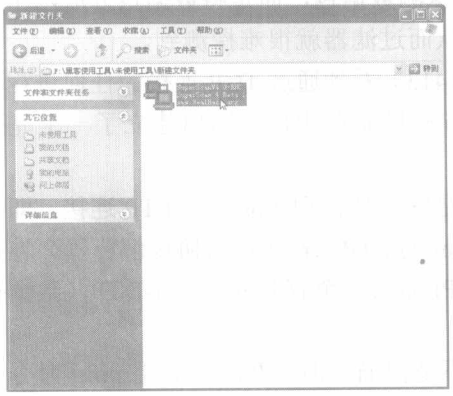

图 1-1 解压文件夹

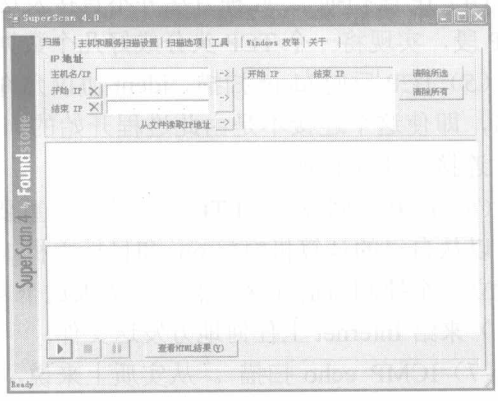

图 1-2 “SuperScan”对话框

（2）单击“主机和服务扫描设置”选项卡，打开如图 1-3 所示的“主机和服务扫描设置”对话框，在此对话框中可以进行如下设置。

● 勾选“查找主机”复选项，默认查找主机方式为“回显请求”，根据实际扫描需要可以进行相应的查找设置。

在“超时设置”文本框中设置超时时间，时间设置越长返回速度越慢，选择默认设置即可。

● 勾选“UDP 端口扫描”复选项，在“开始端口”和“结束端口”文本框中输入端口数，单击“→”按钮实现端口的添加。

在“扫描类型”单选项中有两种方式可以进行选择，Data 和 Data+ICMP 两种，根据需要进行选择。

● 勾选“TCP 端口扫描”复选项，在“开始端口”和“结束端口”文本框中输入端口数，单击“→”按钮添加端口。

在“扫描类型”单选项中选择相应的扫描类型。

（3）单击“扫描选项”选项卡，打开如图 1-4 所示的“扫描选项”对话框，在此对话框中可以进行如下设置。

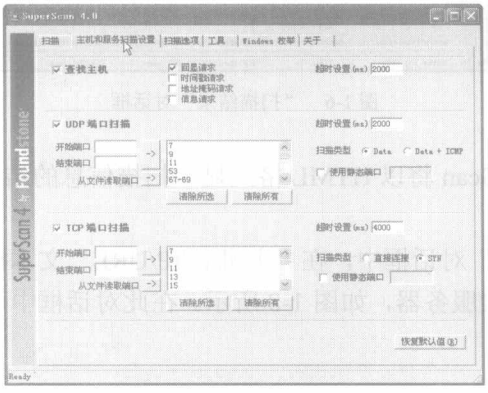

图 1-3 “主机和服务扫描设置”对话框

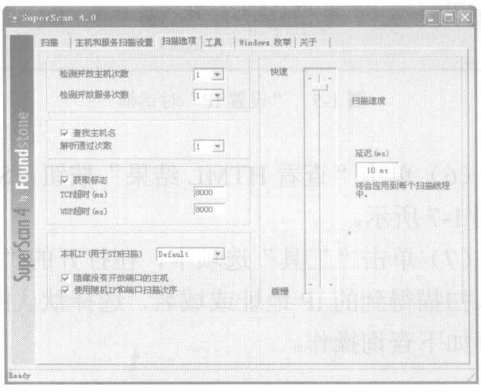

图 1-4 “扫描选项”对话框

● 在“检测开放主机次数”和“检测开放服务次数”下拉项中设置扫描主机的次数，默认值为 1。也就是说，检测一台主机一次，检测开放服务一次；

● 勾选“查找主机名”复选项，在“解析通过次数”下拉项中设置主机名解析的数量，选择默认值即可。

● 勾选“获取标志”复选项，根据此时显示的信息尝试得到远程主机的回应。默认的延迟是 8000ms，如果所连接的主机较慢，可以加大连接时间。

● 在“本机 IP（用于 SYN 扫描）”下拉项中选择显示主机 IP 的类型。

● 勾选“隐藏没有开放端口的主机”复选项，扫描的主机若没有端口开放，则其 IP 地址不在扫描结果中显示。

● 勾选“使用随机 IP 和端口扫描次序”复选项，则在扫描过程中使用随机 IP 端口进行扫描。

● 右边的滚动条可以调节扫描速度，可以调节 SuperScan 在发送每个包所要等待的时间。

（4）设置完成后，返回“扫描”对话框，在“开始 IP”和“结束 IP”文本框中输入扫描的 IP 地址段，单击“”按钮完成 IP 地址的添加，如图 1-5 所示。

（5）单击“”按钮开始扫描，扫描结果如图 1-6 所示。此时在上部分显示了一个主机列表，即关于每台扫描过的主机被发现的开放端口信息，下部分则是扫描的详细信息。

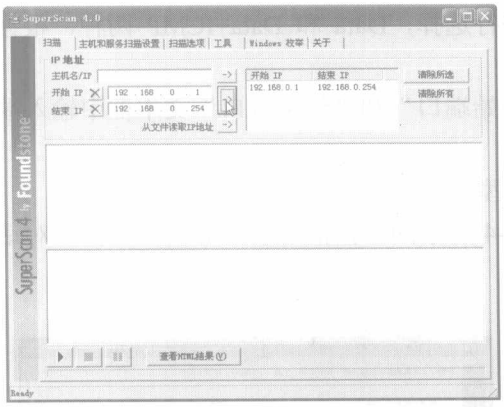

图 1-5 “设置 IP”对话框

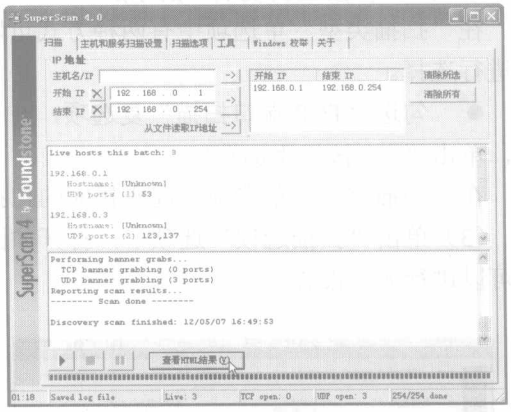

图 1-6 “扫描结果”对话框

（6）单击“查看 HTML 结果”按钮，SuperScan 将以 HTML 格式显示扫描信息的结果，如图 1-7 所示。

（7）单击“工具”选项卡，在打开的“工具”对话框中，在“主机名/IP/URL”文本框中输入扫描得到的 IP 地址或域名，选择默认的连接服务器，如图 1-8 所示。在此对话框中可以进行如下查询操作。

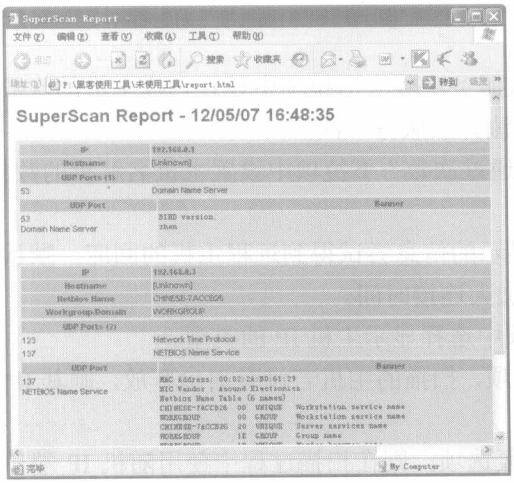

图 1-7 “HTML 结果”对话框

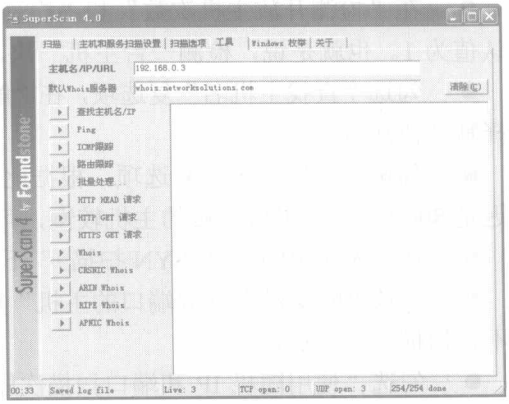

图 1-8 “工具”对话框