1 DVD

68段，超过8小时的多媒体讲解视频

黑客攻防实用技巧

精心筛选108个黑客攻防实战技巧，倾情奉献

应用环境、设置和实例三位一体，完整再现

不同技巧展现多角度思维方式和解决方案，举一反三

108招

武新华 编著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

黑客攻防实用技巧

108招

武新华 编著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

本书根据作者多年从事网络安全工作的实践经验，精心选取黑客攻防中的操作技巧，筛选出最实用的108招，并进行详细的分类，以此奉献给读者。全书共分为10章，涉及扫描与反扫描、控制与反控制、嗅探与欺骗、加密与解密、病毒与木马、网络代理与追踪、注入与认证入侵、账号盗取与安全防范、日志和后门清除技术、安全分析与入侵检测等方面的内容。

本书分类明晰、内容丰富、图文并茂、步骤详细、深入浅出，适合作为网络安全从业人员以及网络管理员提升自身操作能力，提高工作效率的案头常备书；同时也可作为广大网络安全爱好者学习提高的指导用书。

图书在版编目（CIP）数据

黑客攻防实用技巧108招/武新华编著. —北京：中国铁道出版社，2009.10
ISBN 978-7-113-10593-8

Ⅰ.黑… Ⅱ.武… 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（2009）第177705号

书　　名：黑客攻防实用技巧108招
作　　者：武新华　编著

策划编辑：严晓舟　荆　波
责任编辑：苏　茜　　**编辑部电话：**（010）63583215
特邀编辑：彭丽群　　**编辑助理：**包　宁
封面设计：付　巍　　**封面制作：**李　路
版式设计：郑少云　　**责任印制：**李　佳

出版发行：中国铁道出版社（北京市宣武区右安门西街8号　　邮政编码：100054）
印　　刷：北京新魏印刷厂
版　　次：2010年1月第1版　　2010年1月第1次印刷
开　　本：787mm×1092mm　1/16　**印张：**24　**字数：**592千
印　　数：4 000册
书　　号：ISBN 978-7-113-10593-8/TP·3590
定　　价：49.00元（附赠光盘）

Preface 前 言

网络给人们的工作带来了极大的便利，但是黑客入侵和网络安全问题困扰着网络的应用。如僵尸网络（Botnet）、网络仿冒（Phishing）、木马及间谍软件、零时间威胁、熊猫烧香、网站挂马事件、木马产业链的曝光等。

为什么写这本书

网上黑客工具的肆意传播，使得稍微有点网络基础的人，就可以使用简单的工具对网络中一些疏于防范的主机进行攻击，并对入侵成功的计算机中的数据信息进行肆意修改。进而使得用户在发现密码被盗、资料被修改或删除、硬盘一片空白时，再想亡羊补牢，却为时已晚。作为一个有一定操作经验的计算机用户，有必要了解一些黑客知识，通过模拟黑客行为准则以及入侵网络的方式、方法，反过来发现自身存在的问题，做好防范工作，从而保证自己的数据信息和网络的安全。

本书写作目的在于让读者了解黑客的攻击与防范技术，使读者在实际应用中碰到黑客攻击时，能够做到“胸有成竹”。

本书特色

为了节省用户宝贵的时间，提高用户的使用水平，本书在组织时尽量达到了如下特色：

- 步步深入，由浅入深地讲解，使初学者和具有一定基础的用户都能逐步提高，快速掌握黑客防范技巧与工具的使用方法。
- 注重实用性，理论和实例相结合，并配以大量插图和配套光盘视频讲解，力图使读者能够融会贯通。
- 介绍大量小技巧和小窍门，提高读者的效率，节省您宝贵的摸索时间。
- 重点突出、操作简练、内容丰富，同时附有大量的操作实例，读者可以一边学习，一边在计算机上操作，做到即学即用、即用即得，让读者快速学会这些操作。
- 以配图、图释、标注、指引线框等丰富的图解手段，再辅以浅显易懂的语言，不但介绍了黑客攻击计算机的一般方法、步骤以及所使用的工具，而且详细地讲述了防护黑客攻击的方法，可使读者在了解基本网络安全知识的前提下，轻松而快速地掌握基本的反黑知识、工具和修复技巧，在遇到别有用心者的入侵时能够不再茫然无措。

本书的精髓在于：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，进而防范黑客的攻击，使自己的网络更加安全。

读者定位

本书作为一本面向广大网络爱好者的速查手册，适合如下读者学习使用：

- 计算机爱好者；
- 各行各业需要网络防护的人员；
- 网络管理人员；
- 大中专院校网络安全专业的学生。

全书结构安排与内容简介

本书通过 10 类，108 个知识点的详细介绍，并给出了相关代表性产品和工具的介绍及使用方法，使得读者可对网络安全主动防护及黑客入侵主动防御等代表性技术有一个全面认识。此外，本书还从黑客入侵、防护、应用角度给出了相对独立内容的论述，使读者可对如何建构一个实用的黑客入侵防范体系有一个基本的概念和思路，并为读者提供了几种典型行业的安全防护系统建设方案的参考和借鉴。

第 1 章 绝对攻略——扫描与反扫描，本章用 10 招的内容介绍了目前存在于网络中的主流的扫描工具与技术，并针对不同的扫描工具给出了防御方案。

第 2 章 反戈一击——控制与反控制，本章用 10 招的内容对远程控制与反控制技术进行了讲解，以帮助读者更好地保护自己的主机。

第 3 章 李代桃僵——嗅探与欺骗，本章用 13 招的内容揭露了黑客技术应用中形形色色的嗅探和欺骗技术，让读者提高警惕，保障运行安全。

第 4 章 针锋相对——加密与解密，本章用 14 招的内容针对越来越重要的数据和软件的加密与解密从工具和技术两方面进行了讲解。

第 5 章 防不胜防——病毒与木马，本章用 10 招的内容介绍了经常威胁计算机运行和数据安全的病毒和木马，知己知彼，做好防御。

第 6 章 深入敌后——网络代理与追踪，本章用 8 招的内容对于隐藏在网络后面的代理服务器和 IP 追踪等内容进行揭示。

第 7 章 十面埋伏——注入与认证入侵，本章用 15 招的内容详细揭露了各种注入工具的攻击原理，

并对各类认证入侵进行了详细阐述，帮助读者认清并防范各类注入攻击与入侵。

第 8 章 暗度陈仓——账号盗取与安全防范，本章用 11 招的内容对于经常被攻击的 QQ 和 MSN 等即时通信工具进行了详细介绍。

第 9 章 踏雪无痕——日志清除技术，本章用 6 招的内容告诉读者黑客如何在入侵后清除自己的痕迹，以便于读者及时发现并防御。

第 10 章 森严壁垒——安全分析与入侵检测，本章用 11 招的内容告诉读者如何正确的从安全方面监测自己主机存在的漏洞，以便防患于未然。

光盘使用说明

随书附赠的 DVD 光盘提供了经过作者精心筛选的多个实用的操作技巧和多种攻防实战技法的教学视频，汇集了众多资深网络管理员的实践经验和黑客高手的操作精华，通过增加读者对主流攻防手法感性认识的方式，帮助读者建立起清晰的网络安全框架，使读者实现高效学习和对所学知识的灵活运用。

感谢

本书由新起点图书工作室武新华编写，一本书的出版，从选题到上市，要经历很多的环节，在此感谢中国铁道出版社以及负责本书的荆波编辑和其他没有见面的编辑，不辞辛苦地为本书出版所做的大量工作。

读者服务

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

编　者

2009 年 12 月

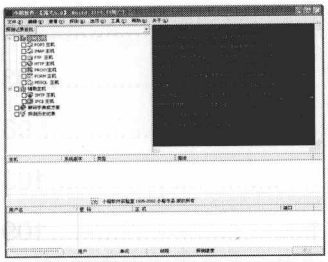
郑重声明

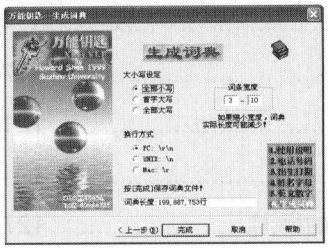
本书的出版目的不是为那些怀有不良动机的人提供技术支持，也不承担技术被滥用的连带责任。希望读者在阅读本书后，不要使用书中所讲技术进行任何违法行为，否则后果自负。切记切记！

Contents

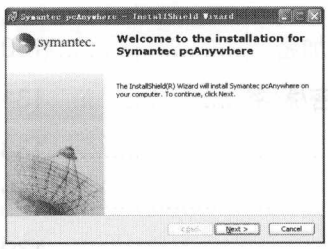
目 录

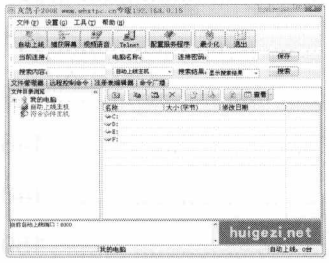
第 1 章 绝对攻略——扫描与反扫描



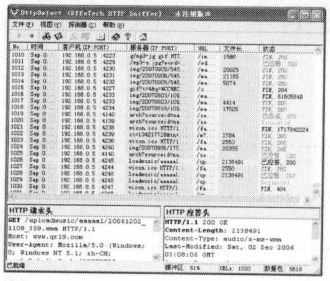


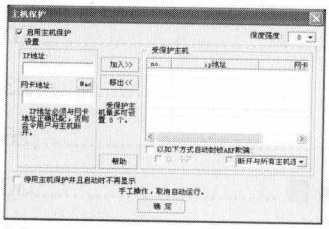
第 2 章 反戈一击——控制与反控制



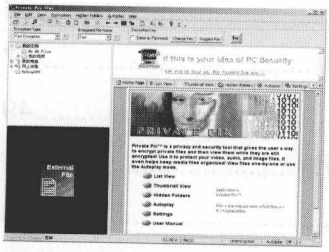


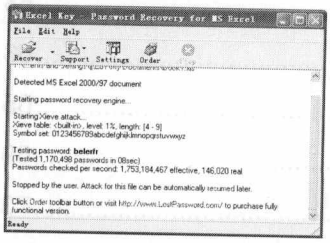
第 3 章　李代桃僵——嗅探与欺骗

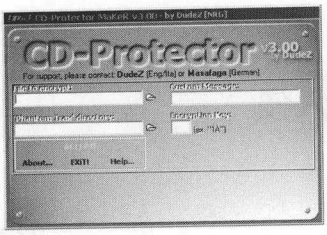




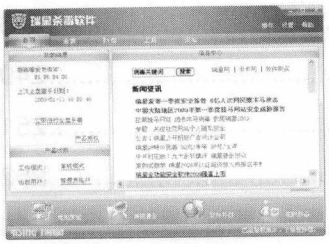
第 4 章　针锋相对——加密与解密



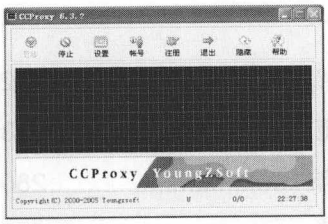


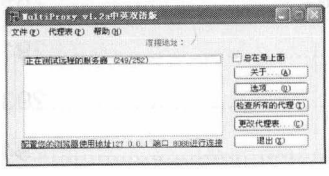


第 5 章 防不胜防——病毒与木马

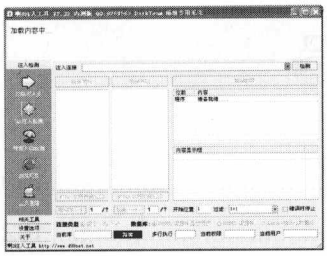


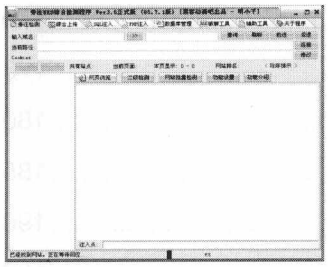
第 6 章 深入敌后——网络代理与追踪



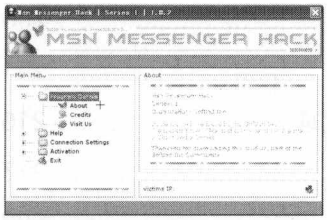


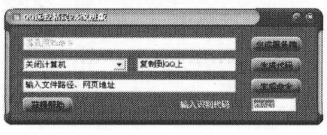
第 7 章　十面埋伏——注入与认证入侵

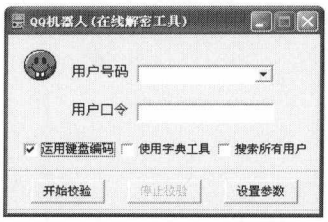




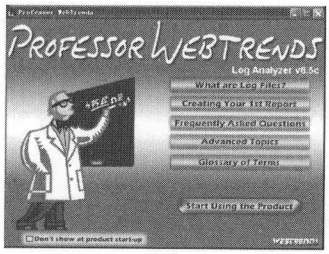
第 8 章　暗度陈仓——账号盗取与安全防范



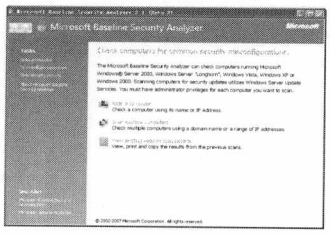




第 9 章 踏雪无痕——日志清除技术



第 10 章 森严壁垒——安全分析与入侵检测

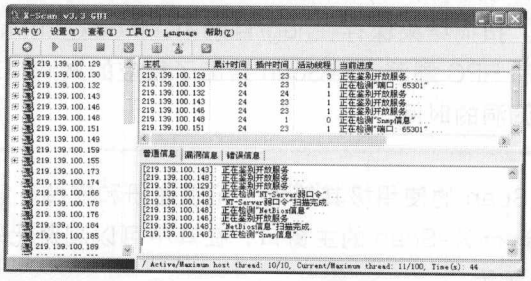


第1章 绝对攻略——扫描与反扫描

本章精粹

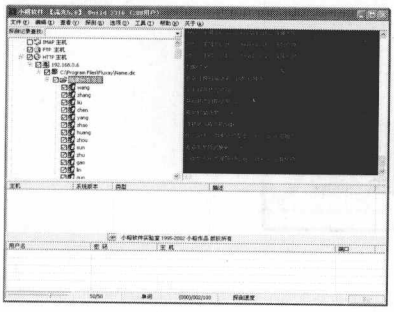
- 扫描工具 X-Scan 查本机隐患
- 用流光扫描主机漏洞
- 用 X-Scan 扫描服务与端口
- 用 MBSA 检测 Windows 系统
- RPC 漏洞扫描
- 用 ProtectX 防御扫描器追踪

内容介绍

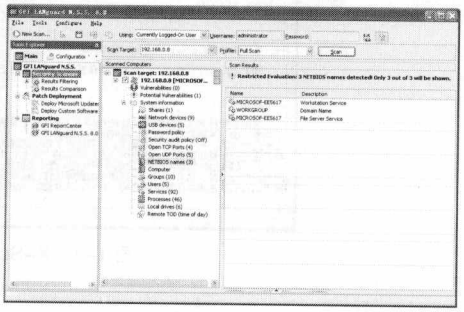


扫描进度

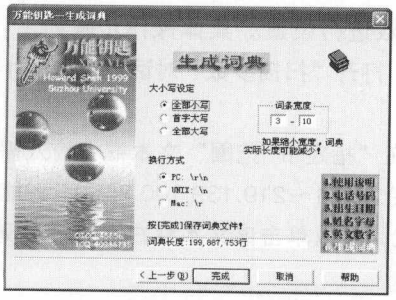
视频链接



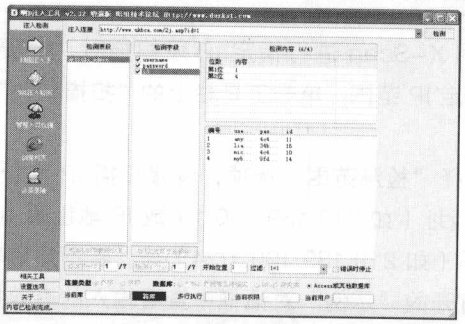
隐藏所有项目



扫描到 NetBIOS 信息



“万能钥匙-生成字典”对话框



检测内容显示

001 招 扫描工具 X-Scan 查本机隐患

招式难度 ★★★
实用程度 ★★★★★

招式解析

X-Scan 是由安全焦点开发的一款功能强大的扫描工具。它采用多线程方式对指定 IP 地址段（或单机）进行安全漏洞检测，支持插件功能，还提供了图形界面和命令行两种操作方式。扫描内容包括：标准端口状态及端口 banner 信息、CGI 漏洞、RPC 漏洞、SQL Server 默认账户、FTP 弱口令，NT 主机共享信息、用户信息、组信息、NT 主机弱口令用户等。扫描结果保存在/log/目录中，index_*.htm 为扫描结果索引文件。对于一些已知的 CGI 和 RPC 漏洞，X-Scan 给出了相应的漏洞描述、利用程序及解决方案，使用户节省了查找漏洞的时间。

X-Scan 的使用极其简单，无须注册和安装。解压缩后双击 X-Scan_gui 应用程序，即可打开并运行 X-Scan 的主窗口，在其中可以浏览此软件的功能简介、常见问题解答等信息，如图 1-1 所示。

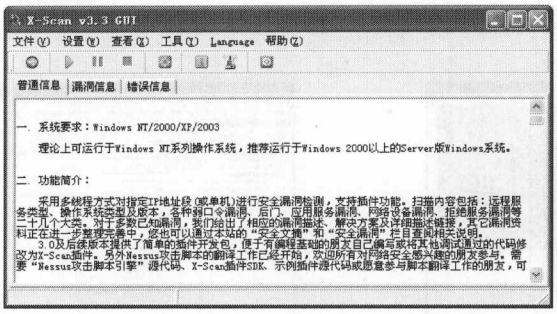


图 1-1 X-Scan 主窗口

1. 设置扫描参数

当使用 X-Scan 进行指定 IP 段扫描时，需要对扫描参数进行设置。具体操作步骤如下：

Step 1 指定 IP 范围。单击工具栏上的“扫描参数”按钮，打开“扫描参数”对话框，如图 1-2 所示。

Step 2 选择“检测范围”选项，设置扫描 IP 地址的范围。在“指定 IP 范围”文本框中输入需要扫描的 IP 地址（如 219.139.100.1）或 IP 地址段（如 219.139.100.1～219.139.100.255），还能增加子网掩码（如 219.139.100.1/24）等。若不知道输入的格式，可以单击该文本框右侧的“示例”按钮，在打开的“示例”对话框中查看输入的有效格式。

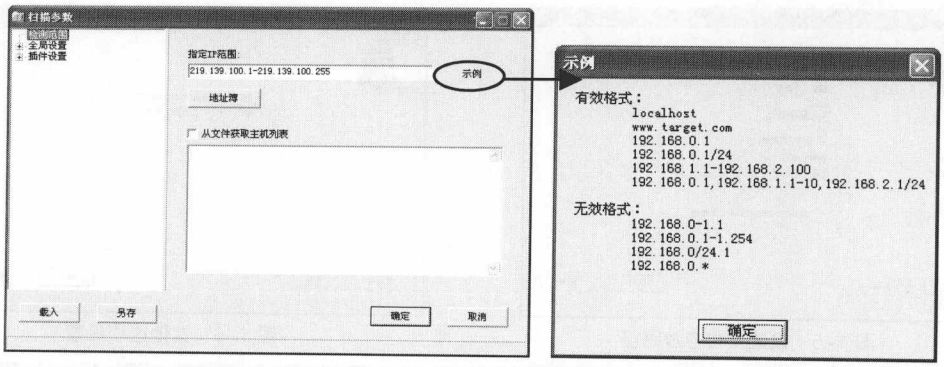


图 1-2　设置扫描 IP 范围

Step 3 选择扫描模块。选择“全局设置”→“扫描模块”选项，则可选择扫描过程中需要扫描的模块，在选择扫描模块时，还可在其右侧窗格中查看该模块的相关说明，如图 1-3 所示。

Step 4 设置扫描线程。因为 X-Scan 是一款多线程扫描工具，所以选择“全局设置”→“并发扫描”选项，可以设置扫描时的线程数量（扫描线程数量要根据自己的网络情况来设置，不可过大），如图 1-4 所示。

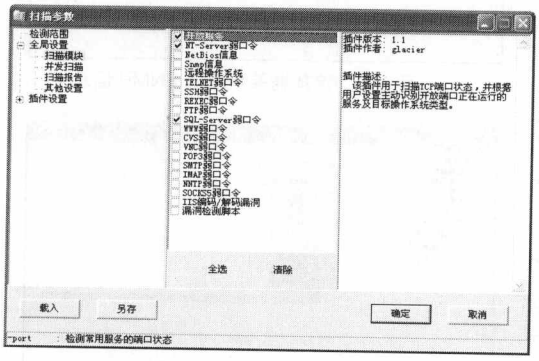


图 1-3　选择扫描模块

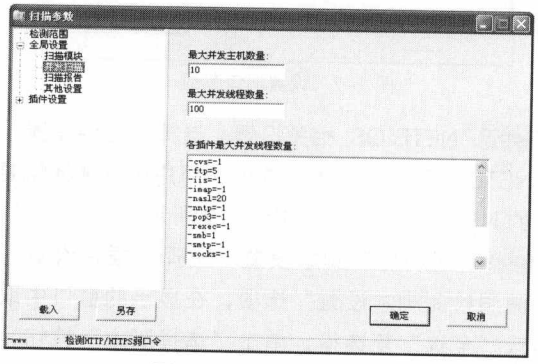


图 1-4　设置扫描线程数量

Step 5 设置扫描报告存放路径。选择“全局设置”→“扫描报告”选项，即可设置扫描报告存放的路径，并选择报告文件保存的文件格式。若需要保存自己设置的扫描 IP 地址范围，则可在勾选“保存主机列表”复选框之后，输入保存文件名称，这样，以后就可以调用这些 IP 地址范围了。若用户需要在扫描结束时自动生成报告文件并显示报告，则可勾选“扫描完成后自动生成并显示报告”复选框，如图 1-5 所示。

Step 6 其他设置。选择“全局设置”→“其他设置”选项，则可设置扫描过程中的其他选项，如勾选“跳过没有检测到开放端口的主机”复选框，如图 1-6 所示。

Step 7 端口相关设置。选择“插件设置”→“端口相关设置”选项，即可扫描端口范围以及检测方式，如图 1-7 所示。若要扫描某主机的所有端口，则可在“待扫描端口”文本框中输入 1～65535。

Step 8 SNMP 相关设置。选择“插件设置”→“SNMP 相关设置”选项，用户可以选择在扫描时获取 SNMP 信息的内容，如图 1-8 所示。

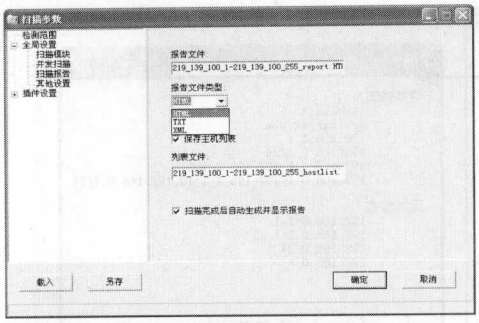


图 1-5　设置报告存放路径

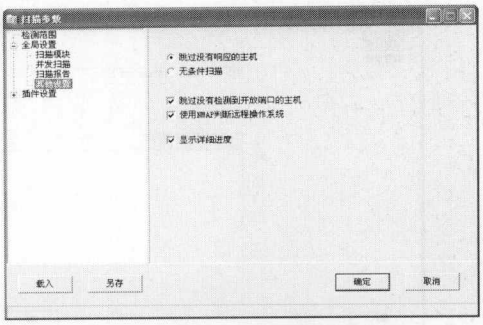


图 1-6　其他选项设置

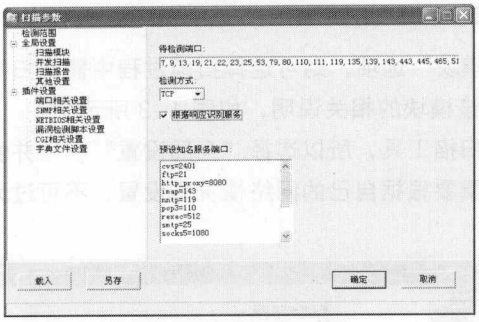


图 1-7　设置端口范围

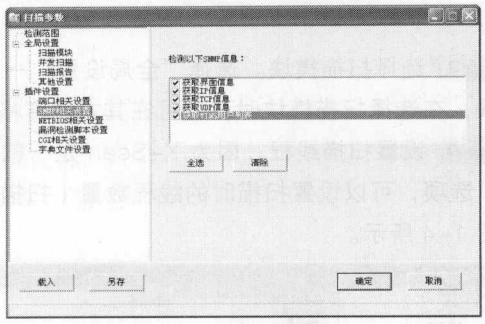


图 1-8　选择需要获取的 SNMP 信息

Step 9 NETBIOS 相关设置。选择“插件设置”→“NETBIOS 相关设置”选项，用户可以选择需要获取的 NETBIOS 信息，如图 1-9 所示。

Step10 漏洞检测脚本设置。选择“插件设置”→“漏洞检测脚本设置”选项，在显示的窗口中取消勾选“全选”复选框，单击“选择脚本”按钮，打开 Select Scripts 对话框，从中即可选择扫描时需要加载的漏洞检测脚本，如图 1-10 所示。

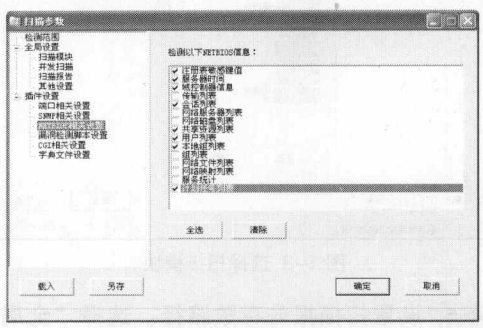


图 1-9　选取需要获取的 NETBIOS 信息

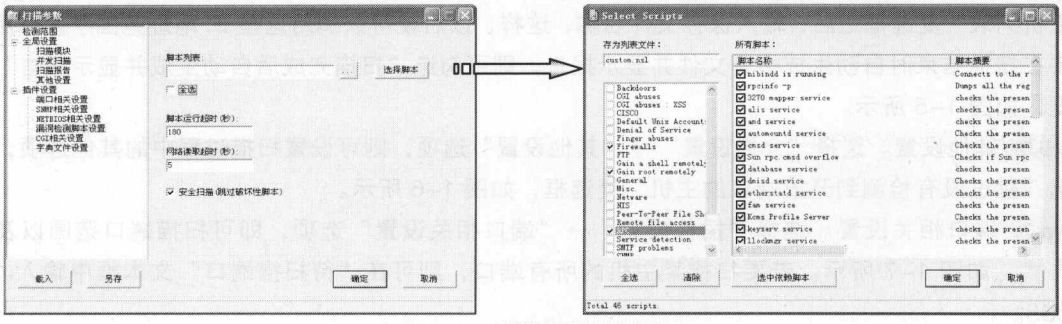


图 1-10　选择漏洞检测脚本

Step11 CGI 相关设置。选择“插件设置”→“CGI 相关设置”选项，即可选择扫描时需要使用的 CGI 选项，如图 1-11 所示。

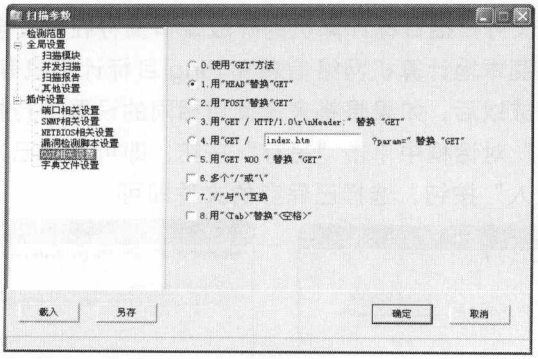


图 1-11　选择 CGI 选项

Step12 选择“插件设置”→“字典文件设置”选项，可选择自己需要的破解字典文件，如图 1-12 所示。在设置好所有选项之后，单击“确定”按钮，即可完成扫描参数的设置。

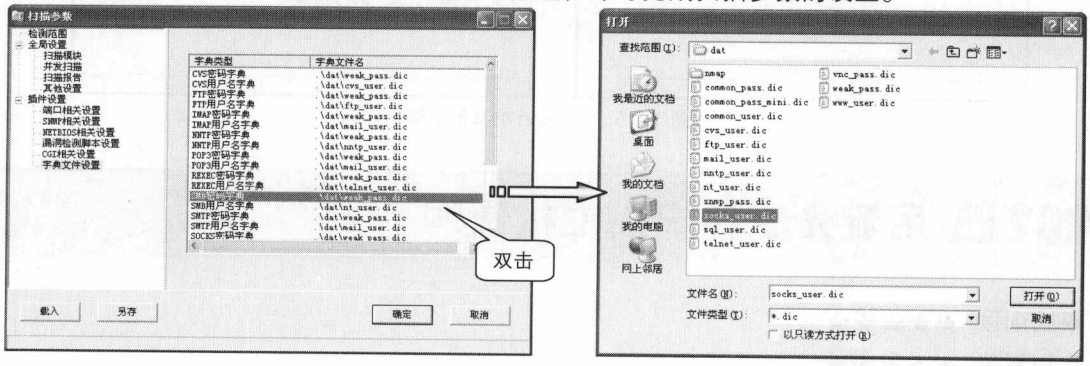


图 1-12　选择破解字典文件

2. 开始扫描

在设置好扫描参数后，就可以开始扫描了。在 X-Scan 工具栏上单击“开始扫描”按钮，即可按设置条件进行扫描，同时显示扫描进程和扫描所得到的信息（可通过选择右下方窗格中的“普通信息”、“漏洞信息”及“错误信息”选项卡，查看所得到的相关信息），如图 1-13 所示。在扫描完成后将自动生成扫描报告并显示出来，其中显示了活动主机 IP 地址、存在的系统漏洞和其他安全隐患，同时还提出了安全隐患的解决方案，如图 1-14 所示。

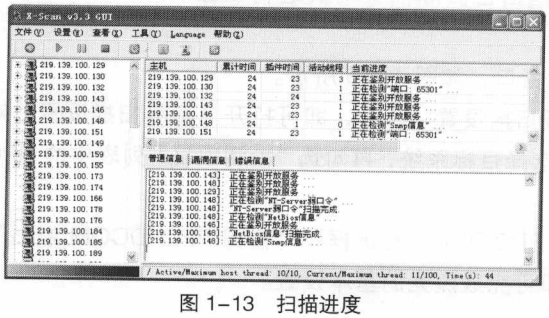


图 1-13　扫描进度

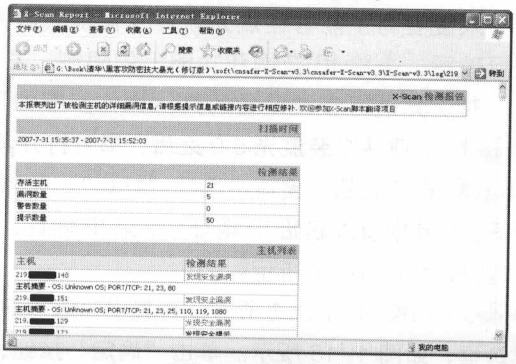


图 1-14　扫描报告