http://www.phei.com.cn

信息安全实验

Information Security Experiment

李 剑 谭建龙 田 华 编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

信息安全实验

Information Security Experiment

李 剑 谭建龙 田 华 编著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书作为信息安全方面的一本实验教材，讲述了信息安全方面一些最基本的实验内容。这些实验包括 SuperScan 网络端口扫描、流光综合扫描与安全评估、SSS 综合扫描与安全评估、ISS 扫描器的使用、N-Stalker 网站安全扫描与评估、Sniffer 网络嗅探器、DoS 与 DDoS 攻击、黑雨软件破解邮箱密码、冰河木马的使用、LC5 账号口令破解、Norton 个人防火墙的使用、Windows 下配置虚拟专用网 VPN 及入侵检测 Snort 系统、Windows 操作系统安全配置及 PGP 软件的使用、文件恢复工具 EasyRecovery 的使用、360 安全卫士的使用、Windows 下 Web 和 FTP 服务器的安全配置。

利用本书在做实验的时候，不需要购买防火墙、入侵检测、VPN 等硬件设备。本书适合于高等学校信息安全专业及相关专业本科学生进行信息安全实验，也适合于各企事业单位、公司员工进行信息安全方面的教育培训和技术研讨等。

图书在版编目（CIP）数据

信息安全实验 / 李剑，谭建龙，田华编著. —北京：电子工业出版社，2009.3
ISBN 978-7-121-08256-6

I. 信… II. ①李… ②谭… ③田… III. 信息系统－安全技术－教材 IV. TP309

中国版本图书馆 CIP 数据核字（2009）第 016805 号

策划编辑：刘宪兰
责任编辑：张 帆
印 刷：北京机工印刷厂
装 订：三河市鹏成印业有限公司
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
开 本：720×1000 1/16 印张：14.75 字数：252 千字
印 次：2009 年 3 月第 1 次印刷
印 数：4000 册 定价：25.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。
服务热线：（010）88258888。

前　言

为了解决信息领域中的使用安全问题，达到“普及信息安全知识”这一目的，作者编写了《信息安全实验》这本教材。本书讲述了信息安全方面一些最基本的实验内容。利用本书在做实验的时候，不需要购买防火墙、入侵检测、VPN 等硬件设备。本书适合于信息安全相关专业本科学生进行信息安全实验，也适合于各企事业单位、公司员工进行信息安全方面的教育培训和技术研讨等。

在讲解时，教师可以根据所要教的对象来选择要教的内容及其深度。全书包括 18 个实验。实验 1 是 SuperScan 网络端口扫描，主要讲述了如何使用 SuperScan 软件进行网络端口扫描。实验 2 是流光综合扫描与安全评估，主要讲述了如何采用流光综合扫描软件，对目标计算机进行综合扫描探测。实验 3 是 SSS 综合扫描与安全评估，主要讲述了如何采用国外优秀综合扫描软件 SSS 对目标计算机进行综合扫描探测。实验 4 是 ISS 扫描器的使用，主要讲述了如何采用国外优秀综合扫描软件 ISS 对目标计算机进行综合扫描探测。实验 5 是 N-Stalker 网站安全扫描与评估，主要讲述了如何采用目前最优秀的网站扫描工具 N-Stalker 对网站进行安全扫描。实验 6 是 Sniffer 网络嗅探器，主要讲述了如何采用 Sniffer 软件对网络数据包进行嗅探、分析。实验 7 是 DoS 与 DDoS 攻击，主要讲述了一些典型的 DoS 攻击和 DDoS 攻击的实验，包括 Land 攻击、UDP Flooder 攻击、CC 攻击等。实验 8 是黑雨软件破解邮箱密码，主要讲述了如何使用黑雨软件来破解电子邮箱密码。实验 9 是冰河木马的使用，主要讲述了如何使用冰河木马来控制别人的计算机，了解木马的工作原理等。实验 10 是 LC5 账号口令破解，主要讲述了如何使用 LC5 软件对操作系统口令进行破解。实验 11 是 Norton 个人防火墙的使用，以 Norton 个人防火墙为例子，讲述了如何使用防火墙封锁一个 IP 或一个端口。实验 12 是 Windows 下配置虚拟专用网 VPN，主要讲述了如何在 Windows 下配置 VPN 的服务器和客户端。实验 13 是 Windows 下配置入侵检测 Snort 系统，主要讲述了如何在 Windows 下配置入侵检测 Snort 系统。实验 14 是 Windows 操作系统安全配置，主要讲述了 Windows 操作系统下一些安全配置。实验 15 是 PGP 软件的使用，主要讲述了 PGP 软件的使用，包括加解密邮件、加解密文件、文件粉碎等。实验

16 是文件恢复工具 EasyRecovery 的使用，主要讲述了如何使用 EasyRecovery 软件来恢复已经删除的文件。实验 17 是 360 安全卫士的使用，主要讲述了如何使用 360 安全卫士来给操作系统打补丁，以及如何使用 360 安全卫士来删除操作系统中的恶意软件等。实验 18 是 Windows 下 Web、FTP 服务器的安全配置，主要讲述了如何在 Windows 操作系统下配置 Web、FTP 服务器。

本书实验 13 至实验 17 由中科院计算所的谭建龙副研究员编写，实验 18 由石家庄邮校的田华老师编写，其余各章由北京邮电大学计算机学院李剑副教授编写。

感谢北京邮电大学信息安全中心杨义先教授、钮心忻教授、罗群副教授，他们对本书的编写提出了宝贵的意见和建议。感谢我的博士导师北京理工大学的曹元大教授，曹老师对于本书的编写给予了极大的支持与帮助。

感谢中国电信研究院的赵阳博士、北京交通大学的姚正林博士，他们对本书的出版给了很大的支持。其他参与本书审阅编写等工作的还有景博、李景加浩、景绍达、白小梅、李胜斌、陈彦侠、益德全、李美丽、李建保、李建龙、杨芬珍、李胜武、李磊、李凯、马一帆、黄正全、郑世慧、王励成等，这里一并谢过！

本教材也是国家信息产业部重点软课题项目“基于互联网内容安全的关键问题研究”（课题编号：2007-R-103）和国家 863 课题“IPS、IMS 关键技术研究”（课题编号：2005143040）的资助成果。

由于本书作者水平有限，书中难免疏漏与错误之处，恳请广大同行和读者批评指正，我们将在今后再版中改正。我的电子邮箱是 lijian@bupt.edu.cn。

李　剑

北京邮电大学

目　录

实验 1

SuperScan 网络端口扫描

SuperScan 是由 Foundstone 开发的一款免费的，但功能十分强大的工具，与许多同类工具比较，它既是一款黑客工具，又是一款网络安全工具。一名黑客可以利用它的拒绝服务攻击来收集远程网络主机信息，而作为安全工具，该软件也能够帮助发现网络中的弱点。

1.1 实验概述

1.1.1 实验目的

通过 SuperScan 的使用，了解网络端口扫描的工作原理及使用方法。

1.1.2 实验环境

一台安装有 Windows XP 或 Windows 2000 操作系统的主机和 SuperScan 软件。

1.1.3 SuperScan 概述

虽然 SuperScan 是一款专门的 IP 和端口扫描软件，但它的额外功能还是很多的，是其他扫描器无法相比的。该软件具有以下功能：

（1）通过 Ping 来检验 IP 是不是在线；

（2）IP 和域名相互转换；

（3）检验目标计算机提供的服务类别；

（4）检验一定范围内目标计算机的在线和端口情况；

（5）工具自定义列表检验目标计算机的在线和端口情况；

（6）自定义要检验的端口，并可以保存为端口列表文件；

（7）软件自带一个木马端口列表 trojans.lst，通过这个列表可以检测目标计算机是不是有木马，同时可以自定义修改该木马端口。

可以看出，这款软件几乎具有与 IP 扫描有关的所有功能，并且每个功能都很专业。

1.2 使用 SuperScan 进行网络端口扫描

1.2.1 锁定主机、端口扫描和木马扫描功能

打开 SuperScan 软件，出现如图 1.1 所示界面。

1. 锁定主机

输入域名，单击“锁定”按钮，得到域名对应的 IP 地址，如图 1.2 所示。

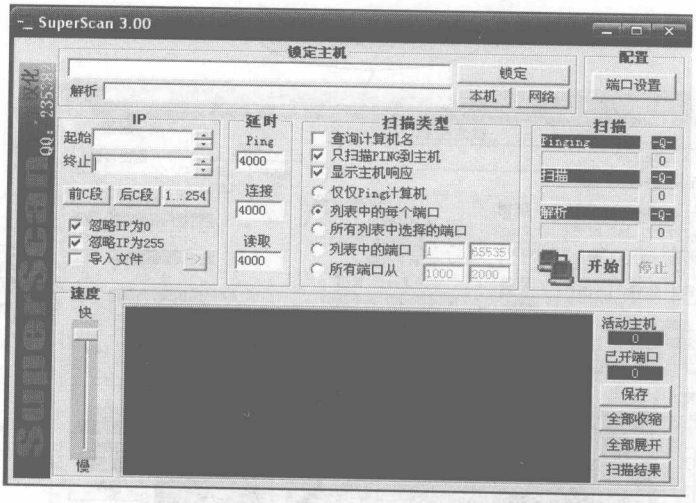

图 1.1　SuperScan 3.00 主界面

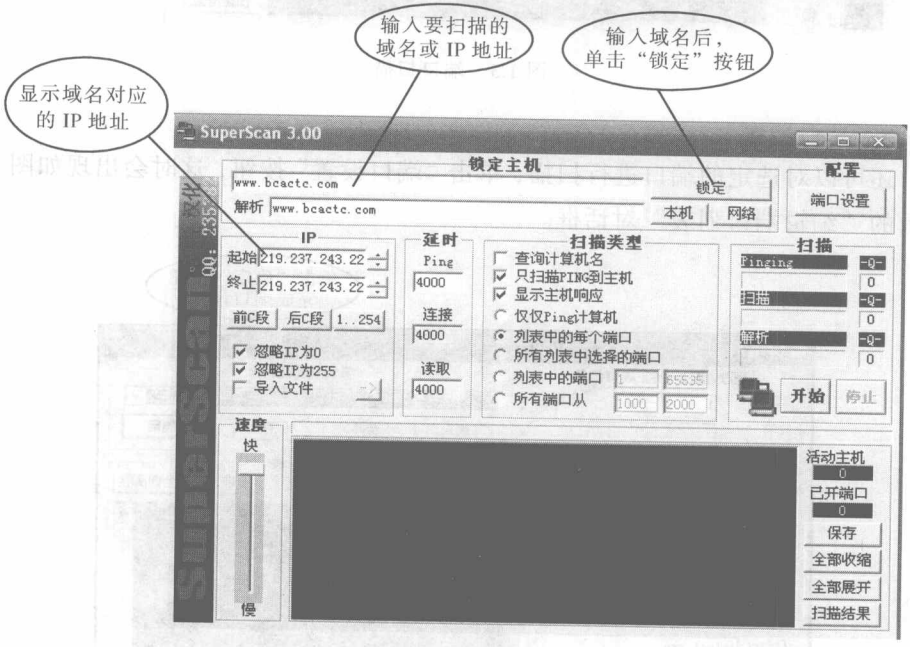

图 1.2　锁定主机

2．端口扫描

选择扫描类型，单击“开始”按钮，对端口进行扫描，如图 1.3 所示。

图 1.3 端口扫描

3. 端口设置

还可以对选定的端口进行扫描，单击“端口设置”按钮，这时会出现如图 1.4 所示的“编辑端口列表”对话框。

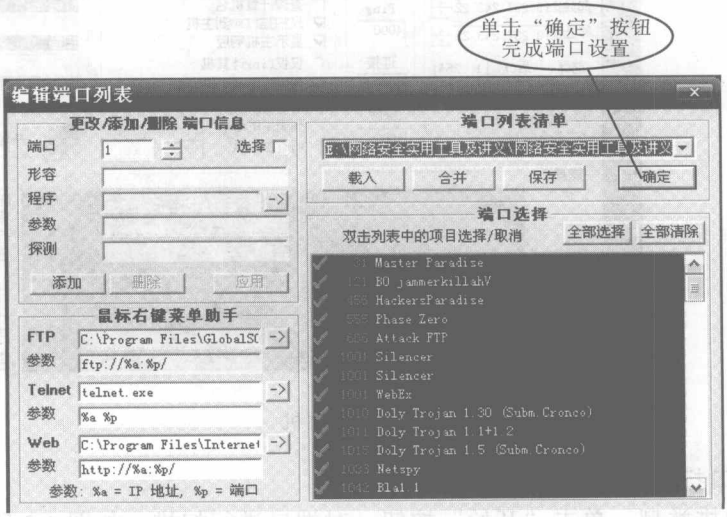

图 1.4 “编辑端口列表”对话框

选择完端口后，就可以对其进行扫描了，使用自定义端口的方式需了解以下几点：

（1）选择端口可以详细了解端口信息；

（2）选择的端口可以自己取名保存，以利于再次使用；

（3）可以要求工具有的放矢地检测目标端口，节省时间和资源；

（4）根据一些特定端口，可以检测目标计算机是不是被攻击者利用、种植木马或打开了一些危险的端口。

4．木马检测

上面提到了可以自定义端口来检测目标计算机有没有被种植木马，步骤如下。

单击“端口设置”按钮，如图 1.5 所示。

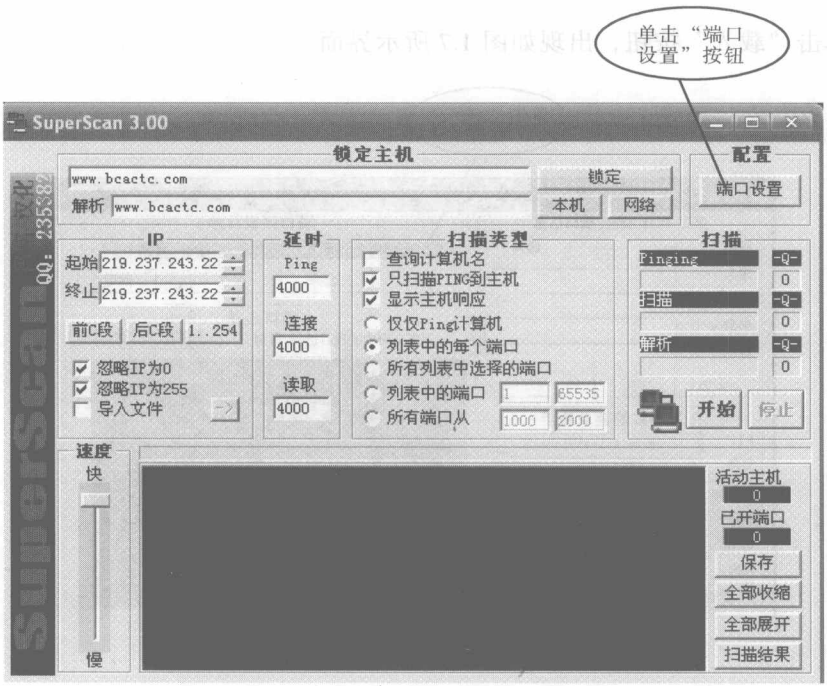

图 1.5　端口设置

出现“编辑端口列表”对话框，如图 1.6 所示。