

全方位的功能讲解 ● 全程图解的易学模式 ● 注重实用的实例演练 ● 良心品质

轻松学习 实例演练 良心品质

轻松学

九天科技 编著

黑客攻防



全彩印刷+多媒体光盘

高品质的全彩图书

全方位的功能讲解、全程图解的易学模式、注重实用的实例演练

超丰富的视频光盘

120分钟超长播放的多媒体视听教学光盘，一套生动鲜明的“活教材”

买一送二超值附赠

赠送《轻松学电脑办公》和《轻松学系统安装、重装与优化》全部教学视频



买书参加抽奖赢取iPad



长达120分钟的视频教学

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

轻松学习 实例演练 良心品质

轻松学

九天科技 编著

黑客攻防



全彩印刷+多媒体光盘



买书参加抽奖赢取iPad

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

本书的编写目的是帮助初学者学习电脑安全及黑客攻防的相关知识。本书通过简单实用的操作,介绍了黑客入侵手段、QQ攻防、电子邮箱攻防等内容。这些内容让读者快速掌握电脑安全设置知识和防范黑客入侵电脑的方法。

本书适合没有任何电脑黑客攻防知识的初学者以及大中专院校的在校学生和社会电脑安全培训机构的学员使用,也可作为网络安全从业人员、网络管理员的参考用书。

图书在版编目(CIP)数据

轻松学黑客攻防/九天科技编著. —北京:中国铁道出版社, 2011. 5

ISBN 978-7-113-12609-4

I. ①轻… II. ①九… 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(2011)第029477号

书 名: 轻松学黑客攻防
作 者: 九天科技 编著

责任编辑: 苏 茜
编辑助理: 刘建玮
封面设计: 张 丽
责任印制: 李 佳

读者热线电话: 400-668-0820

封面制作: 郑少云

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: 北京捷迅佳彩印刷有限公司

版 次: 2011年5月第1版 2011年5月第1次印刷

开 本: 880mm×1230mm 1/32 印张: 7.625 字数: 291千

书 号: ISBN 978-7-113-12609-4

定 价: 28.00元(附赠光盘)

版权所有 侵权必究

凡购买铁道版图书,如有印制质量问题,请与本社发行部联系调换。



前言

Foreword

电脑与网络在促进经济发展、推动社会进步和提高人们生活品质等方面发挥着越来越突出的作用，与此同时网络安全问题也变得日趋严重，大量电脑病毒、木马和黑客攻击不断涌现，其花样还时常翻新，严重威胁着我们的电脑安全，需要引起我们格外的重视。

本书的编写目的就是帮助初学者学习电脑安全及黑客攻防的相关知识，并通过简单实用的系统安全设置、修复系统漏洞等操作，常见的黑客入侵手段介绍以及利用 QQ 攻防、电子邮箱攻防等具体的实例演练等内容，让读者快速掌握电脑安全设置知识以及防范黑客入侵电脑的方法。

本书共分为 12 章，其中：第 1 章介绍黑客攻防基础知识入门；第 2 章介绍扫描网络与锁定目标；第 3 章介绍 Windows 远程控制攻防战；第 4 章介绍 Windows 系统漏洞攻防战；第 5 章介绍木马植入攻防战；第 6 章介绍聊天工具攻防战；第 7 章介绍电子邮件攻防战；第 8 章介绍网页攻防战；第 9 章介绍 U 盘病毒攻防战；第 10 章介绍系统安全策略攻防战；第 11 章介绍系统与文件加密；第 12 章介绍黑客攻防实用技巧。

本书配套的多媒体教学光盘，提供累计时间长达 120 分钟的多媒体教学视频，以全过程语音讲解、情景式教学等方式对书中知识点进行深入讲解，逐步使读者掌握黑客攻防知识。此外还随盘赠送《轻松学电脑办公》和《轻松学系统安装、重装与优化》全部光盘资料。

本书适合没有任何电脑黑客攻防知识的初学者以及大中专院校的在校学生和社会电脑安全培训机构的学员使用，也可作为网络安全从业人员、网络管理员的参考用书。

如果读者在使用本书的过程中遇到问题或者有好的意见或建议，可以通过发送电子邮件：E-mail：jtbook@yahoo.cn 或者在线 QQ：843688388 联系我们，我们将及时予以回复，并尽最大努力为您提供学习上的指导与帮助。

本书的编写目的绝不是为那些怀有不良动机的人提供支持，编者及出版社不承担因为技术被滥用所产生的连带责任。本书的目的在于最大限度地唤起大家的网络安全意识，正视网络世界所面临的一场危机并采取相应行动。特此声明！

编者

2011 年 2 月



多媒体光盘使用说明

How to use the DVD-ROM

多媒体教学光盘的内容简介

本书配套的多媒体教学光盘内容包括 113 个视频教程，视频教程对应书中各章节的内容安排，为各章节内容的操作步骤配置演示视频，播放时间长达 120 分钟。读者可以先阅读图书再浏览光盘，也可以直接通过光盘来学习。本光盘内容仅供安全之用，如应用于非法操作，与本社及作者无关。

多媒体教学光盘的播放方法

① 将本书的配套光盘放入光驱后会自动运行多媒体程序，并进入光盘的主界面，如下图所示。如果光盘没有自动运行，只需在“我的电脑”中双击 DVD 光驱的盘符进入配套光盘，然后双击 Autorun.exe 文件即可。



① 光盘目录导航

② 赠送光盘视频

③ 选择背景音乐

④ 音量控制滑块

⑤ 光盘素材文件

⑥ 退出光盘

② 光盘主界面中显示各章的链接，单击进入本章的二级界面，如下图（上）所示。单击“点击查看”按钮，即可打开视频教程所在的文件夹，如下图（下）所示。双击选择需要播放的视频文件，即可观看视频。

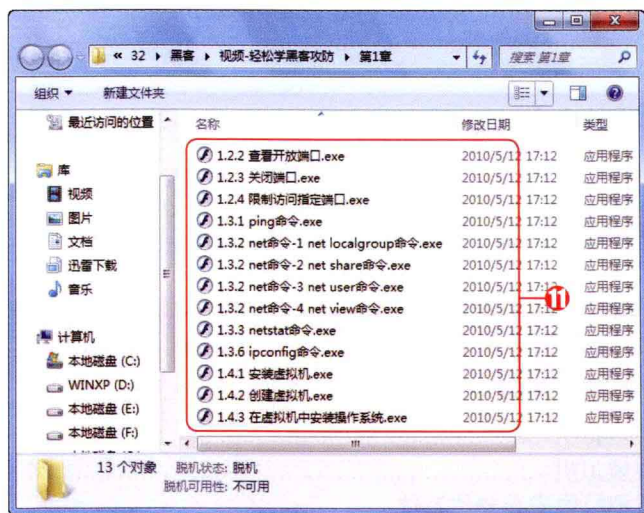


⑦ 点击查看视频

⑧ 返回上一节

⑨ 进入下一节

⑩ 返回主界面



⑪ 双击观看视频

光盘超值附赠视频

- ⑦ 《轻松学电脑办公》光盘视频
长达 180 分钟多媒体教学视频，全面介绍了电脑办公的必备操作技能和方法。
- ⑧ 《轻松学系统安装、重装与优化》光盘视频
长达 150 分钟多媒体教学视频，使读者能够快速掌握系统安装、重装及优化方面的知识。

光盘最佳运行环境

- ⑦ CPU：Pentium 4 及以上。
- ⑧ 内存：215M 及以上。
- ⑨ 硬盘剩余空间：200M 及以上。
- ⑩ 屏幕分辨率：1024 * 768（像素）。
- ⑪ 其他：4 倍速以上 DVD 光驱。



目录 · Contents>>>

第1章 黑客攻防基础知识入门 1

1.1 认识IP地址 2

1.1.1 什么是IP地址 2

1.1.2 IP地址的分类 2



视频教程

1.2 黑客攻击的通道——端口 3

1.2.1 端口的分类 3

1.2.2 查看开放端口 5

1.2.3 关闭端口 6

1.2.4 限制访问指定端口 7



视频教程

1.3 黑客常用的命令 11

1.3.1 ping命令 11

1.3.2 net命令 14

1.3.3 netstat命令 18

1.3.4 ftp命令 19

1.3.5 telnet命令 21

1.3.6 ipconfig命令 21



视频教程

1.4 创建黑客测试环境 22

1.4.1 安装虚拟机 22

1.4.2 创建虚拟机 24

1.4.3 在虚拟机中安装操作系统 27

第2章 扫描网络与锁定目标 31



视频教程

2.1 搜索攻击目标的重要信息 32

2.1.1 获取目标主机的IP地址 32

2.1.2 由IP地址获取目标主机的地理位置 32

2.2 寻找攻击目标的扫描器 33

2.2.1 扫描器的工作原理 33

2.2.2	扫描器能干什么	33
2.3	常见端口扫描器	34
2.3.1	Nmap扫描器	34
2.3.2	SuperScan扫描器	35
 2.4	常见多功能扫描	38
2.4.1	流光扫描器	38
2.4.2	SSS扫描器	43
2.4.3	X-Scan扫描器	48
 2.5	常用网络嗅探工具	50
2.5.1	嗅探利器SmartSniff	50
2.5.2	Iris网络嗅探器	51
2.5.3	网络数据包嗅探专家	54

第3章 Windows远程控制攻防战 56

 3.1	基于认证的远程连接与安全	57
3.1.1	IPC\$入侵与防范	57
3.1.2	Telnet入侵	64
3.2	基于注册表的远程连接与安全	66
3.2.1	开启远程注册表服务	66
3.2.2	修改注册表实现远程监控	67
 3.3	通过Windows XP远程控制入侵	69
3.3.1	Windows XP系统的远程协助	69
3.3.2	Windows XP远程关机	70
3.4	使用远程控制软件入侵	72

第4章 Windows系统漏洞攻防战 75

4.1	系统漏洞及其产生的原因	76
4.2	Windows系统中的漏洞	76
 4.3	系统漏洞防御	82
4.3.1	利用Windows“自动更新”功能	82
4.3.2	使用360安全卫士	84



第5章 木马植入攻防战 86

5.1 木马基础知识 87

5.1.1 木马的结构 87

5.1.2 木马常用的入侵手段 87

5.1.3 木马常用的伪装手段 89



视频教程

5.2 木马的常用制作方法 91

5.2.1 使用“EXE捆绑机”捆绑木马 91

5.2.2 自解压木马 92

5.2.3 网页木马生成器 95

5.2.4 CHM电子书木马 96



视频教程

5.3 木马的清除与防范 98

5.3.1 使用软件清除木马 98

5.3.2 手动清除隐藏的木马 101

5.3.3 防范木马常见措施 102



视频教程

5.4 “冰河”木马的使用与清除 104

5.4.1 配置“冰河”木马的服务器端程序 104

5.4.2 使用“冰河”木马控制远程计算机 105

5.4.3 卸载和清除“冰河”木马 107

5.5 “广外女生”木马的使用与清除 109

5.5.1 “广外女生”木马的使用 109

5.5.2 “广外女生”木马的清除 111

第6章 聊天工具攻防战 112



视频教程

6.1 常见QQ漏洞攻击方式 113

6.1.1 利用“炸弹”攻击 113

6.1.2 破解本地QQ密码 114

6.1.3 查询本地聊天记录 114

6.1.4 非法获取用户IP地址 115



视频教程

6.2 常见QQ安全防范手段 117

6.2.1 保护QQ密码 117

6.2.2 防范IP地址探测 119

6.2.3 加密聊天记录 120



视频教程

6.3 MSN的攻击与防御	121
6.3.1 常见MSN漏洞攻击方式	121
6.3.2 MSN聊天安全防范.....	122

第7章 电子邮件攻防战 124



视频教程

7.1 电子邮件病毒	125
7.1.1 邮件病毒简介.....	125
7.1.2 识别“邮件病毒”的技巧.....	125
7.2 电子邮件炸弹	126
7.2.1 电子邮件炸弹简介	126
7.2.2 电子邮件炸弹的制作方法.....	126
7.3 使用软件探测邮箱密码	127
7.3.1 使用流光.....	127
7.3.2 使用“溯雪Web密码探测器”	128
7.3.3 使用“黑雨”	130
7.3.4 使用“流影”	130
7.4 电子邮件攻击与防范.....	132
7.4.1 电子邮箱日常保护措施	132
7.4.2 找回邮箱密码.....	132
7.4.3 防止炸弹攻击.....	133



视频教程

第8章 网页攻防战 135



视频教程

8.1 什么是“恶意代码”	136
8.2 恶意代码的防范和清除	136
8.2.1 恶意代码的防范	136
8.2.2 恶意代码的清除.....	137
8.3 常见恶意代码攻击的解决方法	138
8.3.1 启动时自动弹出对话框和网页	139
8.3.2 修改起始页和默认主页	139
8.3.3 强行修改IE标题栏.....	140
8.3.4 强行修改右键菜单	140
8.3.5 禁用注册表	141



视频教程

8.4 IE安全设置	141
8.4.1 IE安全设置	141
8.4.2 使用“瑞星卡卡上网助手”	145

第9章 U盘病毒攻防战..... 150



视频教程

9.1 什么是U盘病毒	151
9.1.1 U盘病毒的运行原理	151
9.1.2 常见U盘病毒介绍	151
9.2 U盘病毒的防御	152
9.2.1 关闭“自动播放”功能	152
9.2.2 日常注意要点	153
9.3 autorun.inf文件的构造和运行机制	153
9.4 U盘病毒的查杀	154
9.4.1 用WinRAR软件查杀U盘病毒	155
9.4.2 手动删除U盘病毒	155
9.4.3 使用USBCleaner查杀U盘病毒	156

第10章 系统安全策略攻防战..... 158



视频教程

10.1 设置本地安全策略	159
10.1.1 超过登录时间后强制用户注销	159
10.1.2 不显示上次登录时的用户名	160
10.1.3 限制格式化和弹出可移动媒体	160
10.1.4 对备份和还原权限进行审计	161
10.1.5 禁止在下次更改密码时存储LAN Manager的Hash值	162
10.1.6 设置本地账户共享与安全模式	162
10.1.7 禁止安装未签名的驱动程序	163
10.1.8 不允许SAM账户和共享的匿名枚举	164
10.1.9 让“每个人”权限应用于匿名用户	164
10.1.10 定义IP安全策略	165
10.2 设置组策略	169
10.2.1 设置账户锁定策略	169
10.2.2 设置密码策略	170
10.2.3 设置用户权限	171



视频教程

10.2.4	更改系统默认的管理员账户	173
10.2.5	不允许SAM账户的匿名枚举	173
10.2.6	禁止访问控制面板	174
10.2.7	禁止更改“开始”菜单	174
10.2.8	禁止更改桌面设置	175
10.2.9	禁止访问指定的磁盘驱动器	175
10.2.10	禁用部分应用程序	176



视频教程

10.3 设置计算机管理策略..... 178

10.3.1	事件查看器的使用	178
10.3.2	共享资源的管理	179
10.3.3	管理系统中的服务程序	180



视频教程

10.4 设置注册表编辑器安全..... 181

10.4.1	禁止访问和编辑注册表	182
10.4.2	禁止远程修改注册表	183
10.4.3	禁止运行应用程序	184
10.4.4	禁止更改系统登录密码	185
10.4.5	隐藏控制面板中的图标	186
10.4.6	禁止IE浏览器查看本地磁盘	186
10.4.7	关闭默认共享	187

第11章 系统与文件加密..... 188



视频教程

11.1 为操作系统加密..... 189

11.1.1	设置CMOS开机密码	189
11.1.2	设置系统启动密码	190
11.1.3	设置屏幕保护密码	191



视频教程

11.2 为文件加密..... 193

11.2.1	文本文件专用加密器	193
11.2.2	文件夹加密精灵	195
11.2.3	终极程序加密器	197
11.2.4	万能加密器	198



视频教程

11.3 破解管理员账户..... 202

11.3.1	使用Administrator账户登录	202
11.3.2	强制清除管理员密码	203
11.3.3	创建密码恢复盘	204
11.3.4	使用密码恢复软件	206



第12章 黑客攻防实用技巧 208



视频教程

12.1 系统设置与账户管理技巧 209

- 12.1.1 Windows XP中常见的系统进程 209
- 12.1.2 关闭系统的所有端口 210
- 12.1.3 禁止随机启动程序 211
- 12.1.4 禁用远程协助功能 211
- 12.1.5 设置注册表管理权限 212
- 12.1.6 禁用组策略功能 214
- 12.1.7 启用组策略功能 215
- 12.1.8 禁用“Windows 任务管理器” 215
- 12.1.9 禁用命令提示符 216
- 12.1.10 找出系统隐藏的超级用户 216
- 12.1.11 改变计算机管理员账户Administrator名称 217
- 12.1.12 为自己分配管理员权限 218
- 12.1.13 让系统文件彻底不显示 219
- 12.1.14 删除无关用户账户 219
- 12.1.15 禁止访问“控制面板” 220



视频教程

12.2 IE浏览器安全应用技巧 221

- 12.2.1 清除地址栏中浏览过的网址和中文实名地址 221
- 12.2.2 恢复鼠标右键的复制和粘贴功能 221
- 12.2.3 恢复IE浏览器默认首页 222
- 12.2.4 管理Internet加载项 223
- 12.2.5 设置IE浏览器拒绝运行Java小程序脚本 224
- 12.2.6 隐藏IE地址栏 224
- 12.2.7 解除IE的分级审查口令 225
- 12.2.8 禁止IE访问某些站点 225



视频教程

12.3 常见病毒和木马的防范技巧 226

- 12.3.1 指定Windows 防火墙阻止所有未经请求的传入消息 226
- 12.3.2 处理感染病毒的计算机 227
- 12.3.3 定期检查敏感文件 227
- 12.3.4 识别隐藏的木马程序原文件 227
- 12.3.5 木马程序对通信端口的使用 228
- 12.3.6 木马程序隐藏运行进程的方法 228
- 12.3.7 通过修改文件关联启动木马程序 230
- 12.3.8 防范木马的常用方法 230

第1章

黑客攻防基础知识入门

对防范一个黑客的攻击来说，学会其入侵和破解的方式是必要的。而要做到这一点，则首先要掌握本章所介绍的最基础的知识。因此在学习黑客攻防之前，我们需要先了解一些关于黑客的基础知识，认识 IP 地址、端口和一些黑客常用的 DOS 命令等，为后面的学习打下良好的基础。



本章重点知识

- 认识 IP 地址
- 黑客攻击的通道——端口
- 黑客常用的命令
- 创建黑客测试环境



1.1

认识IP地址

就像每一个人的手机都有一个唯一的电话号码一样，在网络中为了区别不同的计算机，也需要给计算机指定一个号码，这个号码就是“IP 地址”。

>> 1.1.1 什么是IP地址

IP 地址就像是我们的家庭住址一样，如果你要去别人家串门，你就要知道他（她）的地址，这样才能准确找到。计算机信息也是一样，它必须知道另一台电脑的“家庭地址”才不至于走错。计算机在网络中的地址就是 IP 地址，是用二进制数字表示的。

IP 地址的长度为 32 位，分为 4 个字节，每个字节对应 8 位二进制位，即每部分数字不超过 $2^8=256$ 。例如，一个用二进制形式记录的 IP 地址可以表示为：11000000 10011110 00000011 00000101。

为了方便使用，IP 地址的每个字节通常用十进制形式表示，每段数字范围为 0 ~ 255，段与段之间用句点隔开，如上面的 IP 地址就可以表示为：192.158.3.5。IP 地址的这种表示法叫做“点分十进制表示法”，这显然比 1 和 0 容易记忆得多。

>> 1.1.2 IP地址的分类

最初设计互联网络时，为了便于寻址以及层次化构造网络，每个 IP 地址分为网络地址和主机地址两部分。同一个物理网络上的所有主机都使用同一个网络地址，而同一网络上的每个主机都有一个主机地址与其对应。

IP 地址根据网络 ID 的不同分为 5 种类型，即 A 类地址、B 类地址、C 类地址、D 类地址和 E 类地址。

◎ A 类 IP 地址

一个 A 类 IP 地址由 1 字节的网络地址和 3 字节主机地址组成，网络地址的最高位必须是“0”，地址范围为：1.0.0.1 ~ 126.255.255.254（二进制表示为：00000001 00000000 00000000 00000001 ~ 01111110 11111111 11111111 11111110）。可用的 A 类网络有 126 个，每个网络能容纳 16777214 个主机。

◎ B 类 IP 地址

一个 B 类 IP 地址由 2 个字节的网络地址和 2 个字节的主机地址组成，网络地址的最高位必须是“10”，地址范围为：128.1.0.1 ~ 191.255.255.254（二进制表示为：10000000 00000001 00000000 00000001 ~ 10111111 11111111 11111111 11111110）。可用的 B 类网络有 16384 个，每个网络能容纳 65534 个主机。

◎ C 类 IP 地址

一个 C 类 IP 地址由 3 字节的网络地址和 1 字节的主机地址组成，网络地址的最高位必须是 110，地址范围为 192.0.1.1 ~ 223.255.255.254（二进制表示为：11000000 00000000 00000001 00000001 ~ 11011111 11111111 11111110 11111110）。C 类网络可达 2097152 个，每个网络能容纳 254 个主机。

◎ D 类 IP 地址

D 类 IP 地址第一个字节以 1110 开始，地址范围为：224.0.0.1 ~ 239.255.255.254。它是一个专门保留的地址，并不指向特定的网络，目前这一类地址被用在多点广播（Multicast）中。多点广播地址用来一次寻址一组计算机，它标识共享同一协议的一组计算机。

◎ E 类 IP 地址

E 类地址仅用做实验和为将来开发而保留，它以 1111 开始，全 0（0.0.0.0）的 IP 地址指任意网络，全 1 的 IP 地址（255.255.255.255）是当前子网的广播地址，如下图所示。



1.2

黑客攻击的通道——端口

如果把 IP 地址比作一间房子，TCP/IP 协议中的端口指的就是出入这间房子的门。真正的房子只有几个门，但是一个 IP 地址的端口可以有 65536（即 256×256 ）个。端口是通过端口号来标记的，端口号只有整数，范围是从 0~65535 [$256 \times (256-1)$]。

>> 1.2.1 端口的分类

计算机中的端口按不同的标准可以分为很多类，其中最常用的分类标准有以下两种：

1. 按端口号分布划分

按端口号分布划分，可以将端口分为三大类，分别为：公认端口、注册端口和动态和 / 或私有端口。



◎ 公认端口

公认端口（WellKnownPorts）是指那些用户所熟知的端口号，范围从 0 到 1023，它们紧密绑定于一些服务。通常这些端口的通信明确表明了某种服务的协议。例如，80 端口分配给 WWW 服务，21 端口分配给 FTP 服务等。

◎ 注册端口

注册端口（RegisteredPorts）的端口号从 1024 到 49151。它们松散地绑定于一些服务，也就是说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。这些端口大多数没有明确的定义服务对象，应用程序可以根据自己的需要进行定义。例如，我们常用的聊天软件腾讯 QQ 用的就是 4000 端口。

◎ 动态和 / 或私有端口

动态和 / 或私有端口（Dynamicand/orPrivatePorts）的端口号从 49152 到 65535。理论上，不应为服务分配这些端口。但实际上一些较为特殊的程序，特别是一些木马程序常常会使用这些端口，因为机器通常从 1024 起分配动态端口，其不被人们注意，容易隐藏，如 SUN 的 RPC 端口就是从 32768 端口开始的。

2. 按通信服务方式划分

计算机通信的连接方式有以下两种：

第一种是直接与接收方进行的连接，发送信息以后，可以确认信息是否到达，这种方式大多采用 TCP 协议。

第二种是不直接与接收方进行连接，只管把信息放在网上发出去，而不管信息是否到达，也就是“无连接方式”。这种方式大多采用 UDP 协议，IP 协议也是一种无连接方式。

对应使用以上这两种通信协议的服务所提供的端口，也就分为“TCP 协议端口”和“UDP 协议端口”。计算机之间相互通信一般采用这两种通信协议。

使用 TCP 协议的常见端口主要有以下几种：

◎ **FTP**：定义了文件传输协议，使用 21 端口。用户常说某计算机开启了 FTP 服务，便是启动了文件传输服务，下载文件、上传主页都要用到 FTP 服务。

◎ **Telnet**：它是一种用于远程登录的端口，用户可以以自己的身份远程连接到计算机上，通过这种端口可以提供一种基于 DOS 模式下的通信服务。早期的 BBS 是纯字符界面，支持 BBS 的服务器将 23 端口打开，对外提供服务。

◎ **SMTP**：定义了简单邮件传送协议，现在很多邮件服务器都用的是这个协议，用于发送邮件。常见的免费邮件服务中用的就是这个邮件服务端口，所以在电子邮件设置中常看到有 SMTP 端口设置栏，服务器开放的是 25 号端口。

◎ **POP3**：它和 SMTP 对应，POP3 用于接收邮件。通常情况下，POP3 协议所用的是 110 端口。也就是说，只要有相应的使用 POP3 协议的程序（如 Foxmail 或 Outlook），就可以不以 Web 方式登录进邮箱界面，直接用邮件程序就可以收到邮件（例如使用 163 邮箱就没有必要先进入网易网站，再进入自己的邮箱来收信）。