



金桥电脑工作室

新世纪实用型信息技术人才培养教育系列

黑客攻击



防范技巧



科学技术文献出版社

★新世纪实用型信息技术人才培养教育系列（全六册）

黑客攻击与防范技巧

金桥电脑工作室 编著



科学技术文献出版社

内容介绍

本书主要介绍了 Windows 操作系统的漏洞和安全隐患, 并提供了相应的防范措施。书中还介绍了黑客的基本常识和入侵技术, 并教给了读者防范黑客的方法。本书的后半部分, 主要针对喜欢上网的朋友, 特别介绍了网络安全知识。

通过对本书的学习, 可以预防绝大多数黑客的攻击和病毒带来的不必要的麻烦和损失, 可以放心在网络中遨游。总之, 对广大的 Windows 用户和上网的朋友来说, 本书是一本不可多得的好书, 拥有了它, 你的电脑就拥有“安全”。

图书在版编目(CIP)数据

新世纪实用型信息技术人才培养教育系列. 3. 黑客攻击与防范技巧/金桥电脑工作室 编. -北京: 科学技术文献出版社, 2003. 5

ISBN 7-5023-4195-1

I. 黑… II. 金… III. (1) 电子计算机-基本知识 IV. TP3

中国版本图书馆 CIP 数据核字 (2002) 第 088833 号

新世纪实用型信息技术人才培养教育系列 (全六册)

——黑客攻击与防范技巧

金桥·夏雨 编著

责任编辑: 红鸟

科学技术文献出版社出版

全国新华书店经销

西南师范大学教材印刷厂印刷

开本 787×1092 1/16 印张 19.5 字数 400 千字

版次 2003 年 5 月第 1 版 2003 年 5 月第 1 次印刷

印数: 0001~5000 册

ISBN 7-5023-4195-1/TP·3

全套定价: 156.00 元 (本册定价: 26.00 元)

黑客攻击与防范技巧

第一章 Windows 系统安全隐患	1
第一节 Windows 家族产品简介	1
第二节 Windows 漏洞释义	1
一、什么是 Windows 漏洞	1
二、为什么会存在漏洞	2
第三节 Windows 内嵌的网络协议	2
一、TCP/IP 协议	2
二、NetBEUI 协议	4
三、IPX/SPX 协议	4
第四节 TCP/IP 的缺陷与攻击、防御	4
一、TCP/IP 的缺陷	4
二、常见的针对 TCP/IP 的攻击方法	5
三、防御 TCP/IP 攻击的基本方法	5
四、TCP/IP 的设置	6
第五节 如何防止内部 IP 地址泄漏	8
一、什么是 IIS 对页面文件的响应信息	8
二、解决方法	9
第二章 初步了解黑客	11
第一节 黑客简介	11
一、黑客的分类	11
二、黑客网站的特点	12
三、黑客现象及其危害	12
四、黑客应该具有的技能	13
五、黑客、骇客、朋克及其特征	20
第二节 黑客攻击方法详解	22
一、网络攻击的常见形式	22
二、网络攻击的常用方法	24
第三章 攻击准备——信息收集与端口扫描	28
第一节 信息收集的定义	28
第二节 信息搜索的步骤	28
一、制定目标	28
二、具体信息收集	29
三、总结整理收集结果,进行可行性分析	29
第三节 Windows 自备的网络信息查询命令	30
一、Ping	30
二、WinIPcfg	31
三、Tracert	31

四、Net	31
五、Devicename	32
六、At	32
七、Netstat	33
第四节 端口扫描的定义	33
第五节 基于 Windows 的端口扫描	34
一、端口扫描技术	34
二、从端口扫描中获取的信息	35
三、超级端口扫描器的功能 (SuperScan)	36
第六节 对端口扫描的策略	37
一、利用防火墙技术	37
二、防火墙技术的发展趋势	41
第四章 Windows 9X/Me 的漏洞攻防战	43
第一节 Windows 9X/Me 的漏洞攻击手段及安全对策	43
一、Windows 长扩展名存在缓冲溢出问题	43
二、NetBIOS 协议口令校验缺陷	43
三、“畸形 IPX、NMPI 报文”安全隐患	44
四、Cookie 漏洞	44
五、IE 的安全隐患	44
六、UPNP 服务漏洞	45
七、Windows 9X/Me 本地登录验证漏洞	46
八、SMB 通讯协议漏洞	46
九、拒绝服务攻击	46
十、Windows 98 ARP 拒绝服务攻击漏洞	47
十一、设备名称解析漏洞	47
第二节 Windows 9X/Me 共享攻防战略	47
一、SMB 的定义	47
二、远程共享漏洞	49
三、破解共享密码的方法	50
四、系统设置共享后的安全防范	52
第三节 Windows 9X/Me 蓝屏详解	53
一、系统蓝屏工具简介	53
二、蓝屏攻击的安全预防	54
三、Windows 蓝屏死机密码	55
第四节 密码破译	56
一、PWL 文件的攻击与防范	56
二、屏幕保护密码的攻击与防范	57
第五节 Windows 9X 安全注意事项	58
第六节 Windows 9X/Me 安全配置	59

目 录

一、对系统进行安全控制的基本思路	59
二、电脑操作人员的设置	59
三、对超级用户权限的设置	61
四、对普通用户权限的限制	64
五、对非法用户权限限制	71
六、关键性的系统控制策略	72
第五章 Windows NT 系统攻防战	74
第一节 NT 自身的安全对策	74
一、用户账号和用户密码	74
二、域名管理	75
三、用户组权限	75
四、共享资源权限	75
第二节 NT 网络中的安全性	76
第三节 NT 攻击理论基础	77
一、NT 内置组的权限	77
二、NT 缺省状态下对目录的权限	78
三、系统管理员的管理工具的执行权限	78
四、NT 的口令	78
五、一个攻击 NT 的案例	79
六、得到 NT 的 Admin 以后可以做什么	80
第四节 NT 攻击分类	83
一、获取 Administrator 权限账号	84
二、权限突破	85
三、攻破 SAM	86
四、监听 NT 密码验证交换过程	87
第五节 NT 攻防大全	88
第六节 远程入侵 NT	91
一、通过 NT BIOS 入侵	91
二、NT 口令破解	96
三、在 NT 中置入后门	97
四、本地攻击	98
第七节 攻击 NT 的工具集	99
一、Net 命令	99
二、Nat 工具	100
三、攻击实例	103
第八节 NT 防御工具	109
一、SAM 密码加密工具——Syskey	109
二、审核工具 DumpACL	110
三、防火墙	110

四、EcureIIS.....	111
五、扫描工具.....	111
第九节 NT的安全配置.....	111
一、用户名及密码的安全性.....	112
二、安全配置注意事项.....	113
第十节 NT的安全管理.....	114
一、加强物理安全管理.....	114
二、打上补丁.....	114
三、掌握并使用微软提供但未设置的安全功能.....	114
四、控制授权用户的访问.....	115
五、避免给用户定义特定的访问控制.....	115
六、实施账号及口令策略.....	115
七、设置账号锁定.....	115
八、控制远程访问服务.....	115
九、启用登录工作站和登录时间限制.....	115
十、启动审查功能.....	116
十一、确保注册表安全.....	116
十二、应用系统的安全.....	116
第十一节 NT系统受到入侵之后的恢复步骤.....	116
一、记录下恢复过程中采取的所有步骤.....	116
二、夺回控制权.....	116
三、分析入侵.....	117
四、从入侵中恢复.....	118
五、提高你系统和网络的安全性.....	119
六、重新连上因特网.....	119
七、更新你的安全策略.....	120
第六章 Windows 2000 系统攻防战.....	121
第一节 Windows 2000 的安全性.....	121
一、Windows 2000 安全设置.....	121
二、Windows 2000 中的验证服务架构.....	122
第二节 Windows 2000 漏洞.....	122
一、Telnet 漏洞.....	122
二、本地操作漏洞.....	123
三、登录漏洞.....	123
四、NetBIOS 的信息泄漏.....	124
五、系统崩溃特性.....	125
六、IIS 服务泄漏文件内容.....	126
七、Unicode 漏洞.....	126
八、堵住 Wind2000 ICMP 漏洞.....	138

九、攻击 Windows 2000 的实例	139
第三节 Windows 2000 系统安全配置	145
一、初级安全配置	145
二、中级安全配置	147
三、高级安全配置	149
第四节 Win2000 Server 渗透监测	150
一、基于 80 端口渗透的检测	151
二、安全日志的检测	152
三、文件访问日志与关键文件保护	153
四、进程控制	153
五、注册表校验	153
六、端口监控	153
七、终端服务的日志监控	154
八、陷阱技术	155
第五节 SQL Server 的安全性	156
一、SQL Server 的基本概念	156
二、SQL Server 的安全漏洞	157
三、SQL Server 的 SA 空密码攻击	158
四、SQL Server 的安全见解	159
五、SQL Server 2000 的安全设置	161
六、远程控制软件 PCany Where 的安全性	163
第七章 Windows XP 系统攻防战	165
第一节 Windows XP 的安全性	165
第二节 Windows XP 的缺陷及其防范策略	165
一、UPNP 缺陷	166
二、账号锁定功能缺陷	168
三、Windows XP 远程桌面缺陷	168
四、GDI 拒绝服务缺陷	168
五、终端服务 IP 地址欺骗缺陷	169
六、激活特性缺陷	169
七、防范工作	169
第三节 Windows XP 的安全配置	170
一、充分利用 Internet 连接防火墙功能(ICF)	170
二、利用 Windows XP 内置的 IE6.0 来保护个人隐私	171
三、利用加密文件系统(EFS)加密	171
四、屏蔽不需要的服务组件	172
五、进行适当的文件加密	172
六、利用补丁解决“系统假死”等现象	173
七、关闭系统还原功能	173

八、关闭自动更新、目录共享和远程协助支持	174
九、管理好“用户账户”和“密码”	175
十、使用功能更为强大的 Msconfig	177
十一、学会远程桌面和远程协作	178
十二、禁止使用 Shift 自动登录	178
十三、关闭网络共享	178
十四、去除拨号时的自动保存密码	178
十五、为注册表设置管理权限	179
十六、在线杀毒与在线监测	180
第八章 Windows 日志与入侵检测	185
第一节 日志文件的特殊性	185
一、黑客为何会对日志文件感兴趣	185
二、Windows 系统日志介绍	185
第二节 如何删除系统日志	189
一、Windows 98 下的日志删除	189
二、Windows 2000 的日志删除	189
第三节 发现入侵踪迹的捷径	189
一、遭受入侵时的预兆	190
二、合理利用系统日志做入侵检测	190
三、一款优秀的日志管理软件	190
第四节 入侵检测系统	191
一、入侵检测系统的定义	191
二、入侵检测系统和日志的差异	191
三、入侵检测系统的分类	191
四、入侵检测系统的检测步骤	192
五、系统被入侵后的检查方法	193
六、常用入侵检测工具	193
第九章 Windows 后门大曝光	198
第一节 端口的种类	198
第二节 堵住 Windows 最“黑”的后门	198
一、NetBIOS 的定义	198
二、关住 BIOS 的后门	199
三、NetBIOS 端口	200
第三节 认识了解木马	200
一、木马的定义	200
二、木马的种类	201
第四节 揭开木马之迷	202
一、木马的结构	202
二、木马的攻击过程	202

第十章 IIS 常见漏洞及安全防范工具	207
第一节 IIS 常见漏洞	207
一、Null.htw.....	207
二、MDAC-执行本地命令漏洞.....	207
三、idc & .ida Bugs.....	208
四、+.htw Bug.....	208
五、NT Site Server Adsamples 漏洞.....	208
六、IIS HACK.....	208
七、webhits.dll&.htw.....	209
八、ASP Alternate Data Streams (:.\$DATA)	209
九、ISM.DLL 缓冲截断漏洞.....	210
第二节 IIS 的攻击与防范	210
一、IIS HACK.....	210
二、Codebrws.asp & Showcode.asp.....	210
三、Null.htw.....	211
四、Webhits.dll & .htw.....	211
五、ASP Alternate Data Streams (:.\$DATA)	212
六、ISM.DLL 缓冲截断漏洞.....	212
七、idc & .ida bugs.....	212
第三节 IIS 的安全防范工具	214
一、用 IIS Lock Tool 快速设置 IIS 安全属性.....	214
二、URLScan Tool 过滤非法 URL 访问.....	214
第十一章 Windows 攻击技术的升级	216
第一节 嗅探器	216
一、嗅探器的定义.....	216
二、嗅探器的工作原理.....	216
第二节 反嗅探器技术	219
一、检测网内是否存在嗅探程序.....	219
二、Ping.....	220
三、检测本机嗅探程序.....	220
四、DNS 测试.....	221
五、测试网络和主机的响应时间.....	221
第三节 动态 IP 地址的获取及应用	222
一、IP 地址与 IP 地址的动态分配.....	222
二、点对点 TCP/IP 连接.....	222
三、动态 IP 地址的获取与发布.....	223
四、动态 IP 地址获取发布工具——DynamIP.....	223
五、DynamIP 的安装、设置.....	224
六、DynamIP 应用实例.....	225

第十二章 QQ 安全防范全攻略	227
第一节 如何保护自己的 QQ 号码	227
一、防止 QQ 密码被盗的方法.....	227
二、密码被盗案例.....	227
三、防止 QQ 密码被骗.....	227
四、关于 QQ 的密码.....	228
五、关于 QQ 和木马.....	228
六、如何对你的 QQ 信息进行保密.....	229
第二节 如何防御 GOP	230
一、剖析木马的使用设置.....	230
二、木马的检查.....	231
三、木马的清除.....	231
第十三章 网络的安全攻略	232
第一节 家用电脑上网安全指南	232
一、密码安全.....	232
二、“后门”程序.....	232
三、网上交流.....	233
四、E-mail.....	234
五、家用电脑的安全防护要点.....	236
第二节 局域网上网的安全防范与技巧	237
一、黑客攻击类型.....	237
二、防范黑客的措施.....	237
三、Windows NT 的安全问题.....	238
四、UNIX 的安全问题.....	238
第三节 网上冲浪安全防范技巧	240
一、使用防火墙.....	240
二、设置好浏览器.....	240
三、正确使用密码.....	242
四、删除、关闭和限制不必要的服务,禁用和删除不必要的软件.....	242
五、应用补丁程序.....	243
第四节 网上信息安全防范技巧	243
一、删除来历不明的文件.....	243
二、屏蔽 Cookie 信息.....	243
三、不同的地方用不同的口令.....	244
四、屏蔽 ActiveX 控件.....	244
五、定期清除缓存、历史纪录及临时文件夹中的内容.....	244
六、遇到莫名其妙的故障时要及时检查系统信息.....	244
七、对机密信息实施加密保护.....	245
八、拒绝有威胁站点的访问.....	245

九、加密重要的邮件	245
十、在计算机中安装防火墙	245
十一、建立安全信道	246
十二、少在聊天室里聊天	246
第五节 遭到恶意袭击的恢复实例	246
第十四章 注册表的安全防范	248
第一节 恶意网页修改注册表的十二种现象	248
一、注册表被修改的原因及解决方法	248
二、预防办法	252
第二节 防止恶意修改注册表的方法	253
第三节 提高系统安全的注册表修改秘籍	256
一、隐藏一个服务器	256
二、防止其他人非法编辑注册表	256
三、屏蔽“控制面板”的访问	257
四、不允许其他人对桌面进行任意设置	257
五、抵御 BackDoor 的破坏	257
六、隐藏用户登录名	258
七、不允许用户拨号访问	258
八、屏蔽对软盘的网络访问	258
九、禁止访问“文件系统”按钮	259
十、让“网上邻居”的图标隐藏起来	259
十一、限制使用系统的某些特性	259
十二、限制用户使用指定程序	260
十三、不允许用户设置屏幕保护密码	260
十四、将文件系统设置为 NTFS 格式	260
十五、抵御 WinNuke 黑客程序对计算机的攻击	260
十六、恢复对注册表的错误修改	261
第十五章 教你使用加密和数字签名	262
第一节 数字加密	262
一、文件加密的基本知识	262
二、单密钥加密体系	263
三、公用密钥体系	267
四、安全性能	272
五、消息摘要算法	275
六、机密增强型邮件 (PEM)	275
七、主要加密程序的简要讨论	277
八、公用密钥的结构	278
第二节 椭圆曲线加密	280
第三节 加密原理及实现	281

一、加密原理	281
二、用户身份鉴别	282
三、网络数据加密的三种技术	283
第四节 数字签名消息源	285
一、数字签名的建立	285
二、数字签名的重要性	287
三、数字签名与手写签名的对比	290
四、数字签名的使用	290
第五节 标准的数字签名(DDS)	291
一、关注 DDS	292
二、NSA 的作用	292
三、卷入安全标准发展 NSA	293
四、在 DSS 上的进展	294
五、数字签名和机密增强型邮件(PEM)	295
六、数字签名的未来	296
七、数字签名和文件标识	297

第一章 Windows系统安全隐患

第一节 Windows家族产品简介

1. Windows 3.X

这是个人操作系统的一个里程碑。操作命令的图形化，使其易用易学，但是由于技术和设计上的不成熟，Win3.X当时并未在个人操作系统领域里“一统江湖”。

2. Windows 95

这是Windows家族系列的一个里程碑，虽然Win95功能不健全，频繁死机，安全隐患重重等等，但是，微软正是靠Win95才垄断了个人操作系统市场的。所以Win95应该是微软的骄傲。

3. Windows 97/98/ME/SE

这些只能说是Win95的升级版，只是在功能和安全方面做了很多弥补工作而已。

4. Windows NT/2000

这两种操作系统一般多用在网络服务器使用：NT在局域网领域比较受欢迎，在网络中因为其安全性不佳正逐渐被Win2000所替代。Win2000因为对硬件配置要求较高，因此市场普及还需要一段时间。

5. Windows XP

虽说微软号称这是个人操作系统领域里的第二个里程碑，但是总的感觉来说XP并没有实现从win3.X到Win95那种质的飞跃。

XP的总容量居然达到1.2G，据说程序代码就有4000万行之多，并且号称“永不死机”。是不是真的不死机呢？当然，你用了就知道。不过，奉劝一句，没有P4的配置，你最好还是别“玩”它。

第二节 Windows漏洞释义

一、什么是Windows漏洞

系统漏洞也称安全缺陷，这些安全缺陷会被技术高低不等的入侵者所利用，从而达到

控制目标主机或造成一些更具破坏性的目的。

二、为什么会存在漏洞

漏洞的产生应该大致可分为两类：

1. 在程序编写过程中，编程人员为了达到不可告人的目的，有意的在程序的隐蔽处留下各种各样的后门，供日后使用，随着法律的完善，这类漏洞将越来越少（别有用心的除外）。

2. 由于编程人员的水平问题，经验和当时安全技术加密方法所限，在程序中总会或多或少的有些不足之处，这些地方有的影响程序的效率，有的会导致非授权用户的权利提升。安全与不安全从来都是相对的。

第三节 Windows内嵌的网络协议

网络中不同的工作站、服务器之间能传输数据，源于协议的存在。随着网络的发展，不同的开发商开发了不同的通信方式。为了使通信成功、可靠，网络中的所有主机都必须使用同一语言，不能带有方言。因而必须开发严格的标准，定义主机之间的每个包中每个字中的每一位。这些标准来自于多个组织的努力，约定好通用的通信方式，即协议。

现今已经开发了许多协议，但是只有少数被保留了下来。那些协议的淘汰有多种原因——设计不好、实现不好或缺乏支持。而那些保留下来的协议经历了时间的考验并成为有效的通信方法。当今局域网中最常见的三个协议是Microsoft的NetBEUI、NOVELL的IPX/SPX和交叉平台TCP/IP。

一、TCP/IP协议

每种网络协议都有自己的优点，但是只有TCP/IP允许与Internet完全的连接。TCP/IP是在60年代由麻省理工学院和一些商业组织为美国国防部开发的，即便遭到核攻击而破坏了大部分网络，TCP/IP仍然能够维持有效的通信。Arpanet就是基于协议开发的，并发展成为作为科学家和工程师交流媒体的Internet。

Internet公用化以后，人们开始发现全球网的强大功能。Internet的普遍性是TCP/IP至今仍然使用的原因。常常在没有意识到的情况下，用户就在自己的PC上安装了TCP/IP栈，从而使该网络协议在全球应用最广。

1. TCP/IP整体构架

传统的OSI(开放式系统互连)参考模型，是一种通信协议的7层抽象的参考模型，其中每一层执行某一特定任务。该模型的目的是使各种硬件在相同的层次上相互通信。这7层是：物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。而TCP/IP协议并不完全符合OSI的七层参考模型，它采用了4层结构，每一层都呼叫它的下一层所提供的网络来完成自己的需求。

这4层分别为：

●应用层：应用程序间沟通的层，如简单电子邮件传输协议(SMTP)、文件传输协议(FTP)、网络远程访问协议(Telnet)等；

●传输层：此层提供了节点间的数据传送服务，如传输控制协议(TCP)、用户数据报协议(UDP)等，TCP和UDP给数据包加入传输数据并把它传输到下一层中，这一层负责传送数据，并且确定数据已被送达并接收；

●网络层：负责提供基本的数据封包传送功能，让每一块数据包都能够到达目的主机(但不检查是否被正确接收)，如网际协议(IP)；

●网络接口层：对实际的网络媒体的管理，定义如何使用实际网络(如Ethernet、Serial Line等)来传送数据。

2. TCP/IP中协议的功能

●IP协议

网际协议IP是TCP/IP的心脏，也是网络层中最重要的协议。

IP层接收由更低层(网络接口层：例如以太网设备驱动程序)发来的数据包，并把该数据包发送到更高层——TCP或UDP层；相反，IP层也把从TCP或UDP层接收来的数据包传送到更低层。IP数据包是不可靠的，因为IP并没有做任何事情来确认数据包是按顺序发送的或者没有被破坏。IP数据包中含有发送它的主机的地址(源地址)和接收它的主机的地址(目的地址)。

高层的TCP和UDP服务在接收数据包时，通常假设包中的源地址是有效的。也可以这样说，IP地址形成了许多服务的认证基础，这些服务相信数据包是从一个有效的主机发送来的。IP确认包含一个选项，叫做IP Source Routing，可以用来指定一条源地址和目的地址之间的直接路径。对于一些TCP和UDP的服务来说，使用了该选项的IP包好像是从路径上的最后一个系统传递过来的，而不是来自于它的真实地点。这个选项是为了测试而存在的，说明了它可以被用来欺骗系统来进行平常是被禁止的连接。那么，许多依靠IP源地址做确认的服务将产生问题并且会被非法入侵。

●TCP协议

如果IP数据包中有已经封好的TCP数据包，那么IP将把它们传送到TCP层。TCP将包排序并进行错误检查，同时实现虚电路间的连接。TCP数据包中包括序号和确认，所以未按照顺序收到的包可以被排序，而损坏的包可以被重传。TCP将它的信息送到更高层的应用程序，例如Telnet的服务程序和客户程序。应用程序轮流将信息送回TCP层，TCP层便将它们向下传送到IP层、设备驱动程序和物理介质，最后到接收方。

面向连接的服务(例如Telnet、FTP、Rlogin、Xwindows和SMTP)需要高度的可靠性，所以它们使用了TCP。DNS在某些情况下使用TCP发送和接收域名数据库，但使用UDP传送有关单个主机的信息。

●UDP协议

UDP与TCP位于同一层，但不提供任何顺序或重新排序功能，因此，UDP不被应用于那些使用虚电路的面向连接的服务，UDP主要用于那些面向查询——应答的服务，例如NFS。欺骗UDP包比欺骗TCP包更容易，因为UDP没有建立初始化连接(也可以称为握手，因为在两个系统间没有虚电路)，也就是说，与UDP相关的服务面临着更大的危险。

●ICMP协议

ICMP与IP位于同一层，它被用来传送IP的控制信息。它主要是用来提供有关通向目的地址的路径信息。ICMP的“Redirect”信息通知主机通向其他系统的更准确的路径，而“Unreachable”信息则指出路径有问题。另外，如果路径错误，ICMP可以使TCP连接“体面地”终止。Ping是最常用的基于ICMP的服务。

二、NetBEUI协议

NetBEUI是为IBM开发的非路由协议，用于携带NetBIOS通信。NetBEUI缺乏路由和网络层寻址功能，既是其最大的优点，也是其最大的缺点。因为它不需要附加的网络地址和网络层头尾，所以很快并很有效且适用于只有单个网络或整个环境都桥接起来的小工作组环境。

因为不支持路由，所以NetBEUI永远不会成为企业网络的主要协议。NetBEUI帧中唯一的地址是数据链路层媒体访问控制(MAC)地址，该地址标识了网卡但没有标识网络。路由器靠网络地址将帧转发到最终目的地，而NetBEUI帧完全缺乏该信息。

网桥负责按照数据链路层地址在网络之间转发通信，但是有很多缺点。因为所有的广播通信都必须转发到每个网络中，所以网桥的扩展性不好。NetBEUI特别包括了广播通信的记数并依赖它解决命名冲突。一般而言，桥接NetBEUI网络很少超过100台主机。

近年来依赖于第二层交换器的网络变得更为普遍。完全的转换环境降低了网络的利用率，尽管广播仍然转发到网络中的每台主机。事实上，联合使用100-BASE-T Ethernet, 允许转换NetBIOS网络扩展到350台主机，才能避免广播通信成为严重的问题。

三、IPX/SPX协议

IPX是NOVELL用于NetWare客户端/服务器的协议群组，避免了NetBEUI的弱点。但是，也带来了新的弱点。IPX具有完全的路由能力，可用于大型企业网。它包括32位网络地址，在单个环境中允许有许多路由网络。

IPX的可扩展性受到其高层广播通信和高开销的限制。服务广告协议(Service Advertising Protocol, SAP)将路由网络中的主机数限制为几千。尽管SAP的局限性已经被智能路由器和服务器配置所克服，但是，大规模IPX网络的管理仍是非常困难的工作。

第四节 TCP / IP 的缺陷与攻击、防御

一、TCP/IP 的缺陷

因特网的基石是 TCP/IP 协议，该协议在实现上力求效率，而没有考虑安全因素，因为那样无疑增大代码量，从而降低了 TCP/IP 的运行效率，所以说 TCP/IP 本身在设计上就是不安全的。下面是现存的 TCP/IP 协议的一些安全缺陷：

1. 很容易被窃听和欺骗

大多数因特网上的流量是没有加密的，电子邮件口令、文件传输很容易被监听和劫持，