Internet Firewall

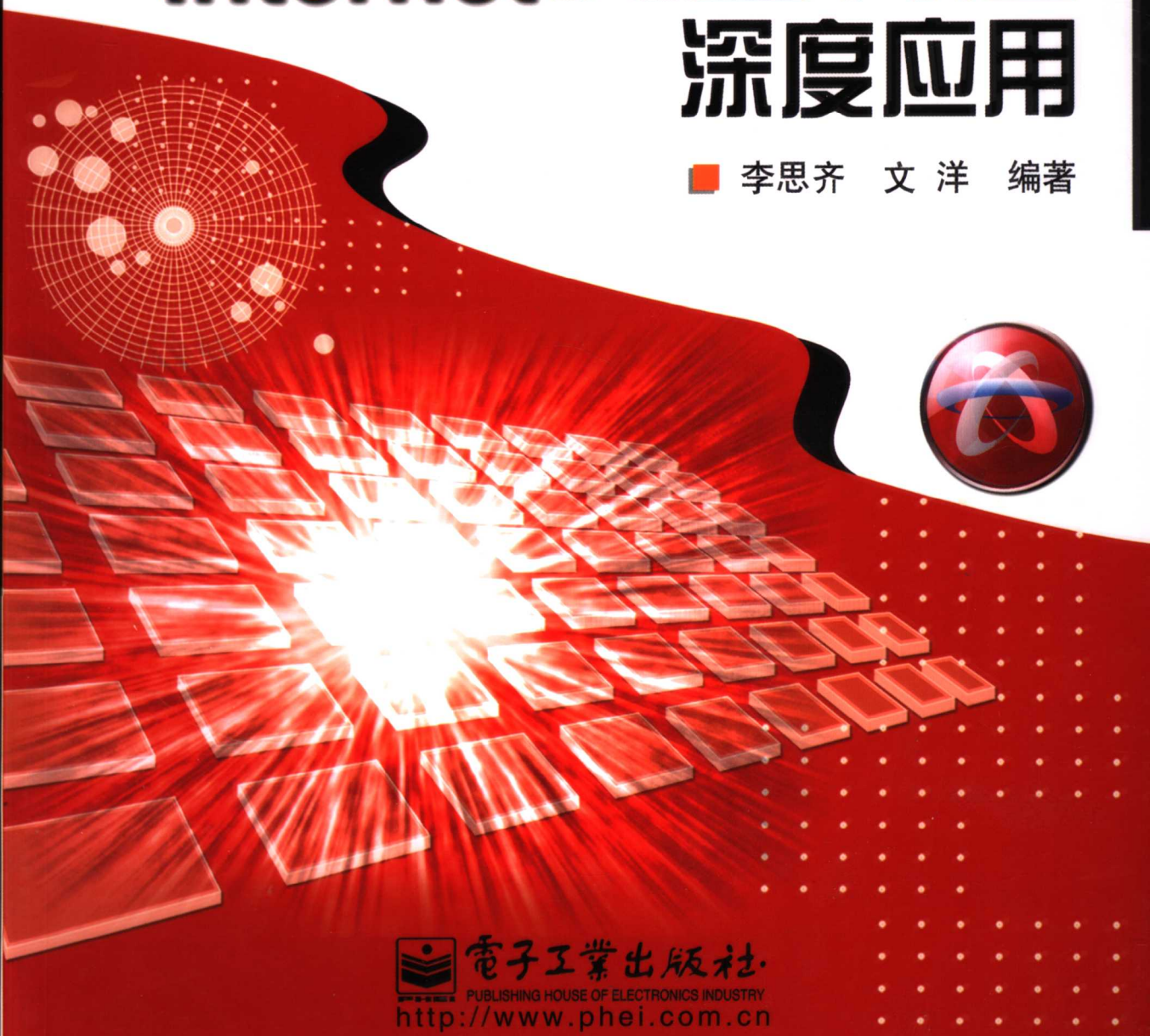
有力地防护、安全地构建

防火之道

Internet 安全构建

深度应用

李思齐 文洋 编著



電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

防火之道

——Internet安全构建深度应用

李思齐　文　洋　编著

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

内 容 简 介

网络与公司生存息息相关，因此网络安全对任何公司都至关重要。数据的丢失和更改、机密信息被盗取等，都将给公司造成难以估计的损失。而实现网络的安全，第一步就是在网络中部署防火墙。本书详细地介绍了Internet和局域网基础、防火墙规划与设计、防火墙关键技术、企业防火墙产品配置、个人防火墙产品配置、入侵检测、漏洞分析、监控与扫描、日志分析、恶意代码、常见病毒的处理以及常用的反黑、反攻击方法。

本书叙述清楚，语言通俗易懂，可供网络管理人员、网络安全爱好者、高校及中职中专院校计算机专业的师生和计算机网络用户阅读参考。

图书在版编目（CIP）数据

防火之道——Internet安全构建深度应用/李思齐，文洋编著.—北京：电子工业出版社，2006.5
ISBN 7-121-02422-5

Ⅰ.防… Ⅱ.①李… ②文… 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（2006）第024347号

责任编辑：徐云鹏
特邀编辑：卢国俊
印　　刷：北京天竺颖华印刷厂
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
　　北京市海淀区翠微东里甲2号　邮编：100036
经　　销：各地新华书店
开　　本：787×1092 1/16　印张：23.75　字数：590千字
印　　次：2006年5月第1次印刷
定　　价：36.00元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换，若书店售缺，请与本社发行部联系。联系电话：010-68279077。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。

前　言

随着计算机网络技术的发展和Internet的广泛普及，网络安全事故也逐年增加，网络系统的管理责任越来越重大。尤其是黑客、计算机病毒对网络安全的危害，使得人们不得不重视防火墙技术。防火墙是一种行之有效的网络安全机制，是在网络的内部与外部之间实施安全防范的系统。为使网络管理人员能对防火墙有一个详尽的了解，并能建立防火墙，提高防火墙与防火墙技术应用水平，我们编写了《防火之道——Internet安全构建深度应用》一书，供从事网络安全的管理人员学习参考。

本书由13章组成，具体内容如下：

第1章主要介绍Internet和局域网的基础知识。内容包括Internet服务基本概念、TCP/IP与OSI模型、Internet的安全策略、Intranet服务基本概念、Intranet服务类型和Intranet安全策略。

第2章主要介绍防火墙的规划与设计。内容包括防火墙基本概念、创建防火墙的步骤、防火墙的体系结构、防火墙体系结构的组合形式、防火墙保护的类型以及防火墙的高级设置。

第3章主要介绍针对防火墙建立的规则和约束。内容包括针对防火墙建立的规则和约束、包过滤技术、代理技术、代理中的Socks技术、状态检查技术、NAT技术、VPN技术、身份鉴别技术、数据加密技术和内容检查技术。

第4章主要介绍企业防火墙产品的配置。内容包括对Cisco PIX防火墙的安装配置和对Microsoft ISA Server 2004防火墙的安装配置。

第5章主要介绍个人防火墙产品的配置。内容包括诺顿个人安全防火墙的安装配置和瑞星个人防火墙的安装配置。

第6章主要介绍入侵检测。内容包括入侵检测基本概念、入侵检测系统架构、入侵检测的分类、安全策略文档和可接受的使用策略、Session Wall、带入侵检测功能的网络体系结构等。

第7章主要介绍漏洞分析。内容包括网络安全漏洞基本概念、漏洞分类、漏洞等级、Internet服务的安全漏洞、网络常见漏洞防范方法、系统漏洞防范方法以及系统漏洞防范案例。

第8章主要介绍监控与扫描。内容包括监控与扫描的基本概念、活动监测、

内容扫描、启发式扫描、完整性检查、实时扫描、错误警告、常用监测工具的介绍以及扫描监测设计案例。

第9章主要介绍日志分析。内容包括日志工具的介绍、网络检测和数据采集、常用日志文件分析工具、Windows系统日志分析、Linux系统日志分析、网络安全日志分析和系统日志分析。

第10章主要介绍恶意代码。内容包括恶意代码的类型、恶意代码的特征、恶意代码的传播方式、木马程序的防范、Droppers程序、后门程序、蠕虫病毒、恶作剧程序。

第11章主要介绍常见病毒的处理。内容包括引导扇区病毒、文件病毒、DOS病毒、Windows病毒、UNIX病毒、宏病毒、脚本病毒、Java病毒、邮件病毒、QQ病毒、MSN病毒、复合型病毒的特征及清除方法。

第12章主要介绍反黑、反攻击的具体方法。内容包括扫描程序的防御、口令攻击程序的防御、嗅探器的防御和远程攻击的防御。

第13章主要介绍典型网络安全解决方案。内容包括大型网站、证券网络、政府网络、电子政务的安全解决方案。

本书由李思齐、文洋编著，在整个写作过程中，尹凤霞博士、张军博士、贾岩博士、吴佑莲博士、李春安研究员、王刚教授对本书提出了许多修改意见并进行了稿件的整理工作，在此对他们表示感谢。感谢网络安全联盟网、趋势科技为本书提供的写作便利。感谢电子工业出版社和北京美迪亚电子信息有限公司的各位教师的指导和帮助。

由于本书涉及许多新的内容和研究领域，尽管作者已经尽了最大努力，但仍旧难免存在问题，对书中的错误和不当之处，欢迎各位同仁批评指正。

目　录

第1章

Internet和局域网基础

- Internet服务的基本概念
- Internet客户机/服务器体系
- TCP/IP与OSI模型
- Internet的安全策略
- Intranet服务的基本概念
- Intranet服务类型
- Intranet协议
- Intranet安全策略

Internet为应用者提供了非常丰富的功能，我们也将其称为服务。这些服务包括：快速方便地交换信息（通过电子邮件、FTP）、访问资深人士和专家（通过USENET日常更新的专题信息mailinglist以及实时在线交谈）等。

在本章中，将向大家介绍Internet的基本概念、相关协议以及基于协议上的安全策略等。

1.1 Internet服务的基本概念

Internet的全称是Internet Network，中文名为因特网。它是一种计算机网络的集合，以基础的TCP/IP网络协议进行通信，将各地众多的计算机连接在一起，使原本分散的计算机或局域网上的资源通过它进行共享。

1.2 Internet客户机/服务器体系

Internet中的C/S结构，即Client/Server（客户机/服务器）结构。此结构把数据库内容放在远程的服务器上，而在客户机上安装相应软件。C/S软件一般采用两层结构，由两部分构成：前端是客户机，接受用户的请求，并向数据库服务提出请求，通常是一个PC机；后端是服务器，即数据管理，将数据提交给客户端，客户端将数据进行计算并将结果呈现给用户。另外，还要提供完善的安全保护及对数据的完整性处理等操作，并允许多个客户同时访问同一个数据库。在这种结构中，服务器的硬件必须具有足够的处理能力，这样才能满足各客户的要求。

C/S结构在技术上很成熟，它的主要特点是交互性强、具有安全的存取模式、网络通信量低、响应速度快、利于处理大量数据，但是该结构的程序是针对性开发，变更不够灵活，维护和管理的难度较大，通常只局限于小型局域网，不利于扩展，并且，由于该结构的每台客户机都需要安装相应的客户端程序，分布功能弱且兼容性差，不能实现快速部署安装和配置，因此缺少通用性，具有较大的局限性。

1.3 TCP/IP协议

在本节中，将详细介绍Internet上使用最广泛的TCP/IP协议以及OSI模型。其中TCP为传输控制协议，IP为Internet协议。本节并不详细讲述TCP/IP协议的具体内容，而是通过对基本协议的讲解为下面章节的学习奠定基础。

1.3.1 TCP/IP协议的分层结构

网络协议通常分不同层次进行开发，每一层分别负责不同的通信功能。比如TCP/IP协议，它是一组不同层次上的多个协议的组合，通常被认为是一个四层协议系统。每一层负责不同的功能。

（1）链路层：也称做数据链路层或网络接口层。通常包括操作系统中的设备驱动程序和计算机中对应的网络接口卡。它们一起处理与电缆（或其他任何传输媒介）的物理接口细节。

（2）网络层：处理分组在网络中的活动，例如分组的路由选择。在TCP/IP协议组件中，网络层协议包括IP协议（网际协议）、ICMP协议（Internet控制报文协议），以及IGMP协议（Internet组管理协议）。

（3）传输层：主要为两台主机上的应用程序提供端到端的通信。在TCP/IP协议组件中，有两个互不相同的传输协议：TCP（传输控制协议）和UDP（用户数据报协议）。TCP为两台主机提供高可靠性的数据通信。它所做的工作包括：把应用程序交给它的数据分成合适的小块交给下面的网络层，确认接收到的分组，设置发送最后确认分组的超时时钟等。由于传输层提供了高可靠性的端到端通信，因此应用层可以忽略所有这些细节。而另一方面，UDP为应用层提供了一种非常简单的服务。它只是把数据报从一台主机发送到另一台主机，但并不保证该数据报能到达另一端。任何必需的可靠性必须由应用层来提供。这两种运输层协议分别在不同的应用程序中有不同的用途。

（4）应用层：负责处理特定的应用程序细节。各种不同的TCP/IP实现都会提供下面这些通用的应用程序：

- Telnet远程登录
- FTP文件传输协议
- SMTP用于电子邮件的简单邮件传输协议
- SNMP简单网络管理协议

1.3.2 OSI参考模型与Internet协议簇

图1.1给出了OSI参考模型与Internet协议簇的结构示意。这将使我们对TCP/IP协议有更加全面的了解。

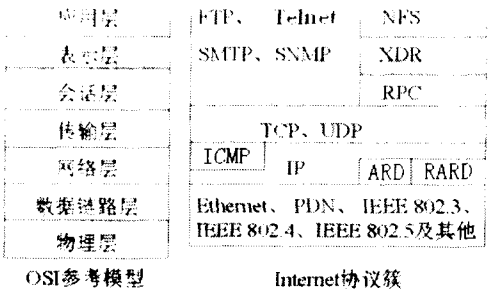


图1.1 OSI参考模型与Internet协议簇

注意：通过对每一个协议簇中各种协议结构的详细了解，有助于我们了解防火墙的架构体系。

1.3.3 TCP/IP测试

作为一名网管，肯定会遇到各种各样的网络故障，通常最多的就是针对TCP/IP的故障，所以测试TCP/IP需要有效的工具来作为支撑。

1. Ping命令

Ping命令是Windows 9X/NT中集成的一个用于TCP/IP协议的测试工具，Ping命令可以查看网络上的主机是否在工作，它是通过向该主机发送ICMP ECHO_REQUEST包进行测试而达到目的的。一般凡是应用TCP/IP协议的局域或广域网，不管用户是只有几台电脑的家庭、办公室局域网，还是校园网、企业网甚至Internet，当客户端与客户端之间无法正常进行访问或者网络工作出现各种不稳定的情况时，首先应该用Ping命令来测试一下网络的通信是否正常。

Ping命令的完整格式如下：

ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [[-j host list] | [-k host-list]] [-w timeout] destination-list

从这个命令中可以看出它的复杂程度，Ping命令后面都是它的执行参数，现对其参数进行详细讲解。

- -t：有这个参数时，当用户Ping一个主机时系统就不停地运行Ping命令，直到用户按下Ctrl+C。
- -a：解析主机的NETBIOS主机名，如果想知道用户所Ping的计算机名，则要加上这个参数，一般是在运用Ping命令后的第一行就显示出来。
- -n count：定义测试所发出的测试包的个数，默认值为4。通过这个命令可以自己定义发送的个数，对衡量网络速度很有帮助。比如，想测试发送20个数据包的返回平

均时间为多少、最快时间为多少、最慢时间为多少时，就可以通过执行带有这个参数的命令获知。

- -l length：定义所发送缓冲区的数据包的大小，在默认的情况下，Windows的Ping发送的数据包大小为32B，也可以自己定义，但有一个限制，就是最大只能发送65 500B，超过这个数时，对方就很有可能因接收的数据包太大而死机，所以，微软公司为了解决这一安全漏洞，于是限制了Ping的数据包大小。
- -f：在数据包中发送“不要分段”标志。一般用户所发送的数据包都会通过路由分段再发送给对方，加上此参数以后路由就不会再分段处理。
- -i ttl：指定TTL值在对方的系统里停留的时间，此参数同样是帮助用户检查网络运转情况的。
- -v tos：将“服务类型”字段设置为“tos”指定的值。
- -r count：在“记录路由”字段中记录传出和返回数据包的路由。一般情况下，用户发送的数据包是通过一个个路由才到达对方的，但到底是经过了哪些路由呢？通过此参数就可以设定用户想探测经过的路由的个数，不过限制在了9个，也就是说用户只能跟踪到9个路由。
- -s count：指定“count”指定的跃点数的时间戳，此参数和-r差不多，只是这个参数不记录数据包返回所经过的路由，最多也只记录4个。
- -j host-list：利用“computer-list”指定的计算机列表路由数据包。
- -w timeout：指定超时间隔，单位为毫秒。
- destination-list：是指要测试的主机名或IP地址。

用Ping命令可以来测试网络是否通畅，这在局域网的维护中经常用到。方法很简单，只要在DOS或Windows的“开始”菜单下的“运行”子项中用Ping命令加上所要测试的目标计算机的IP地址或主机名即可（目标计算机要与用户所运行Ping命令的计算机在同一网络，或通过电话线或其他专线方式已连接成一个网络），其他参数可全不加。如要测试IP地址为196.168.1.21的工作站与服务器是否已联网成功，就可以在服务器上运行：ping -a 196.68.123.56，如果工作站上TCP/IP协议工作正常，则会以DOS屏幕方式显示如下所示的信息：

```
Pinging cindy[196.168.1.21] with 32 bytes of data:
Reply from 196.168.1.21: bytes=32 time<10ms TTL=254
Reply from 196.168.1.21: bytes=32 time<10ms TTL=254
Reply from 196.168.1.21: bytes=32 time<10ms TTL=254
Reply from 196.168.1.21: bytes=32 time<10ms TTL=254
Ping statistics for 196.168.1.21:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

从上面可以看出目标计算机与服务器连接成功，TCP/IP协议工作正常，因为加了“-a”这个参数，所以还可以知道IP为196.168.1.21的计算机的NetBIOS名为cindy。

如果网络未连成功，则显示如下错误信息：

```
Pinging[196.168.1.21 ] with 32 bytes of data
```

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistice for 196.168.1.21:
Packets:Sent=4, Received =0, Lost\=4 (100% loss),
Approximate round trip times in milli-seconds
Minimum=0ms, Maximum=0ms, Average=0ms
```

2. ipconfig/Winipcfg

与Ping命令有所区别，利用ipconfig和Winipcfg工具可以查看和修改网络中TCP/IP协议的有关配置，如IP地址、网关、子网掩码等。这两个工具功能基本相同，只是ipconfig是以DOS的字符形式显示，而Winipcfg则用图形界面显示，也就是说它们其实是一个工具，只不过一个是DOS下的版本，另一个为Windows下的版本。但要注意，在Windows NT中只能运行DOS方式下的ipconfig工具。

ipconfig命令的语法格式：

```
ipconfig[/all][/batch file][/renew all][/release all][/renew n][/release n]
```

- all：显示与TCP/IP协议相关的所有细节信息，其中包括测试的主机名、IP地址、子网掩码、节点类型、是否启用IP路由、网卡的物理地址、默认网关等。
- batch file：将测试的结果存入指定的“file”文件名中，以便于逐项查看，如果省略file文件名，则系统会把测试的结果保存在系统的“winipcfg.out”文件中。
- renew all：更新全部适配器的通信配置情况，所有测试重新开始。
- release all：释放全部适配器的通信配置情况。
- renew n：更新第n号适配器的通信配置情况，所有测试重新开始。
- release n：释放第n号适配器的通信配置情况。

Winipcfg工具的功能与ipconfig基本相同，只是Winipcfg是以图形界面的方式显示，在操作上更加方便，同时能够以Windows的32位图形界面方式显示。当用户需要查看任何一台机器上TCP/IP协议的配置情况时，只需在Windows 95/98上选择【开始】|【运行】命令，在出现的对话框中输入命令“winipcfg”即可出现测试结果。单击【详细信息】按钮，在随后出现的对话框中可以查看和改变TCP/IP的有关配置参数。当一台机器上安装有多个网卡时，可以查找到每个网卡的物理地址和有关协议的绑定情况。

3. Netstat

与上述几个网络检测软件类似，Netstat命令也是可以运行于Windows 95/98/NT的DOS提示符下的工具，利用该工具可以显示有关统计信息和当前网络连接的情况，用户或网络管理人员可以得到非常详尽的统计结果。当网络中没有安装特殊的网管软件时，就是Netstat大显身手的时候了。

它可以用来获得用户网络连接的信息（使用的端口和使用的协议等）、收到和发出的数据、被连接的远程系统的端口等。

Netstat命令的语法格式：

netstat [-a] [-e] [-n] [-s] [-p protocol] [-r] [interval]

参数解释如下：

- -a：用来显示在本地机上的外部连接，也显示远程所连接的系统、本地和远程系统连接时使用和开放的端口，以及本地和远程系统连接的状态。这个参数通常用于获得用户的本地系统开放的端口，用它可以自己检查系统上有没有被安装木马，如果在用户的机器上运行Netstat后，如返回诸如Port 12345（TCP） Netbus、Port 31337（UDP） Back Orifice之类的信息，则用户的机器上就很有可能感染了木马。
- -n：这个参数基本上是-a参数的数字形式，它是用数字的形式显示以上信息，这个参数通常用于检查自己的IP时使用。
- -e：显示静态以太网统计，该参数可以与s选项结合使用。
- -p protocol：用来显示特定的协议配置信息，它的格式为：Netstat -p xxx，xxx可以是UDP、IP、ICMP或TCP，如要显示机器上的TCP协议配置情况，则可以使用Netstat -p tcp。
- -s：显示机器在默认情况下每个协议的配置统计，默认情况下包括TCP、IP、UDP、ICMP等协议。
- -r：用来显示路由分配表。
- interval：每隔多少秒重复显示所选协议的配置情况，直到按Ctrl+C中断。

4. Nbtstat

该命令用于查看当前基于NetBIOS的TCP/IP连接状态，通过该工具用户可以获得远程或本地机器的组名和机器名 。虽然用户使用ipconfig/Winipcfg工具可以准确地得到主机的网卡地址，但对于一个已建成的大型局域网，要去每台机器上进行这样的操作就显得过于费事了。网管人员在自己上网的机器上使用DOS命令Nbtstat，便可获取另一台上网主机的网卡地址。

语法格式：

Nbtstat [[-a RemoteName] [-A IP address] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [interval]]

参数说明：

- -a RemoteName：说明使用远程计算机的名称并列出其名称表，此参数可以通过远程计算机的NetBIOS名来查看当前状态。
- -A IP address：说明使用远程计算机的IP地址并列出名称表，与“-a”不同，它只能使用IP，其实“-a”就包括了“-A”的功能了。
- -c：列出远程计算机的NetBIOS名称的缓存和每个名称的IP地址。这个参数就是用来列出在用户的NetBIOS里缓存的用户连接过的计算机的IP。
- -n：列出本地机的NetBIOS名称，此参数与上面所介绍的“Netstat”中加参数“-a”的功能类似，只是这个是检查本地的，如果把Netstat -a后面的IP换为自己的IP，就和Nbtstat -n的效果一样了。
- -r：列出Windows网络名称解析的统计。在配置使用WINS的Windows 2000计算机上，此选项返回要通过广播或WINS来解析注册的名称数。

- -R：清除NetBIOS名称缓存中的所有名称后，重新装入Lmhosts文件，这个参数就是清除nbtstat -c所能看见的缓存里的IP。
- -S：在客户端和服务器会话表中只显示远程计算机的IP地址。
- -s：显示客户端和服务器会话，并将远程计算机IP地址转换成NetBIOS名称。此参数和-S差不多，只是这个会把对方的NetBIOS名解析出来。
- -RR：释放在WINS服务器上注册的NetBIOS名称，然后刷新它们的注册。
- interval：每隔多少秒重新显示所选的统计，按Ctrl+C键可停止重新显示统计。如果省略该参数，Nbtstat将打印一次当前的配置信息。此参数和Netstat的一样，Nbtstat中的“interval”参数是配合-s和-S一起使用的。

1.3.4 多重地址TCP/IP配置

地址的多次转换能将欺骗网络和真实网络分离开来，这样就可利用真实的计算机替换低可信度的欺骗，增加了间接性和隐蔽性。其基本的概念就是重定向代理服务（通过改写代理服务器程序实现），由代理服务进行地址转换，使相同的源和目的地址像真实系统那样被维护在欺骗系统中。例如，从m.n.o.p进入到a.b.c.g接口的访问，将经过一系列的地址转换：由a.f.c.g发送到10.n.o.p再到10.g.c.f，最后将数据包欺骗形式从m.n.o.p转换到真实机器上的a.b.c.g，并且还可将欺骗服务绑定在与提供真实服务主机相同类型和配置的主机上，从而显著地提高欺骗的真实性。

1.3.5 TCP/IP协议的安全缺陷

随着计算机技术的高速发展，原来认为非常神秘的因特网随着新世纪的到来已大步走进千家万户。上网已成为人们生活、工作中的一个重要组成部分。

但就像任何其他新生事物一样，因特网的发展也不是一帆风顺的。关心因特网发展的人一定知道，最最让人们担心的就是因特网上的安全问题，也是因特网发展的最大阻力。因特网上的安全性问题最突出地体现在网络信息的窃听和劫持。也许用户还记忆犹新，曾几何时，网络的安全问题给认为因特网已经或必将完全胜任商务活动的人们泼了一盆冷水，也给把重宝全押在因特网上的商家留下一个永远无法愈合的伤痕。就因为这样，因特网曾一度几乎要被其安全性问题扼杀于摇篮之中。

TCP/IP协议是进行一切因特网上活动的基础，没有它就不可能在不同操作系统、不同通信协议中来去自由。也许是因为当时网络软、硬件设备的局限性，当初设计该协议时就在着重考虑了网络的速度，而对网络的安全性没做太多的考虑，甚至根本没做考虑，也许是当时开发TCP/IP协议的人根本没有预料因特网会发展如此之迅速。所以说TCP/IP本身在安全设计上就先天不足。

TCP/IP协议虽然经过了一次又一次的改版、升级，但终因先天和软件的可继承性等原因，仍存在诸多安全缺陷，不能就在原程序上修修改改而得以全部解决。目前因特网的安全性主要体现在：

1. 网上信息易被窃取

大多数因特网上的信息是没有经过加密的（这也许是与人们通常交流的习惯有关），

如电子邮件、网页中输入口令或填写个人资料、文件传输等，这一切都很容易被一些别有用心的人监听和劫持，其实这就是TCP/IP通信协议在安全性方面的一个漏洞。

为什么因特网上极易被窃取呢？这就要从因特网连接的特点来说了。因特网是一种网间网技术，也就是说其实它就是把无数的局域网相连起来形成的一个大网，这个大网又与其他由无数局域网连接起来的大网相连来组成一个更大的网，就这样不断地互联就形成了通常所说的因特网，它没有绝对的大小。但它说到底也是个类局域网。正因为因特网的庞大，所以它的拓扑结构比一般局域网更复杂。因特网的拓扑是一种逐步细化的树状结构，虽然因特网上的传输是点对点的，但一般因特网上的主机往往是处于某一个局域网中，局域网（如以太网、令牌网等）都是广播型网络，也就是说一台主机发布消息，网上任何一台机器都可以收到这个消息，就像在局域网中用Netsend命令发布消息一样。

一般情况下，以太网在经过比较后发现是别人的消息时会自动丢弃消息，而不向上层（即本机）传递消息。但以太网卡的接收模式可以设置成混合型，这样网卡就会捕捉所有的数据包，并把这些数据包向上传递，这就是为什么以太网可以被窃听。其实FDDI、令牌网也存在这样问题。ATM网络技术是绝对的点对点通信的，它不像以太网的广播式那样容易被窃听。

因特网上的信息容易被窃听和劫获的另一个原因是，当某人用一台主机和另外一个远程主机进行通信时，它们之间互相发送的数据包要经过很多机器重重转发。具体要经过多少主机、多少路由器和多少网络，用户可以用一个网络调试工具得到，即Traceroute，它在各种操作系统中都有，如Windows 98、Windows NT和UNIX，名字上可能会有所差异。

因特网的这种工作原理不仅节约了资源，而且简化了传输过程，符合TCP/IP简单高效的宗旨，但这也带来了安全问题。这些用来转发消息包的机器完全可以把用户的信息窃取下来，同样，如果黑客使用一台处于某用户的数据包传输路径上的主机，那么他就也可以窃听或劫持用户的数据包。这一切听起来是多么恐怖，但用户也不必过于紧张，因为一般来说，个人用户数据对于这些专业黑客是没有多大利用价值的，当然也不是说不用去考虑。

面对这一切，虽然不能改变目前所存在的一切安全性问题，但要意识到这种问题，并以其他办法来提高安全性，如通常所讲的加密方法。时至今日，实现对数据安全加密的方法是多种多样的，最为突出的如Windows 2000、Outlook 5.0以上版本软件自带的加密功能；第三方加密软件也很多，如PGP就是一款非常不错的邮件加密软件。

2. *脆弱的TCP/IP服务*

应用TCP/IP协议的主要目的是为了在Internet上进行服务，虽然TCP/IP协议已是事实上通信协议的标准，但仍不可避免的一个问题就是它的安全性问题，不仅TCP/IP协议本身，现在很多基于TCP/IP的应用服务都在不同程度上存在着严重的安全问题，一些新的处于测试阶级的服务就有更多的安全缺陷。基于TCP/IP协议的服务很多，如WWW服务、FTP服务、电子邮件服务、TFTP服务、NFS服务、Finger服务、NDS服务、DHCP服务和WINS服务等等，详细了解这些服务在安全性方面的不足对于用户设置防火墙保护自己的网络有重要意义，平时为单位设置防火墙时就需要考虑该提供哪些服务、要禁止哪些服务以及哪些服务该如何配置等，在这里仅对一些常用服务做简单介绍。

（1）WWW服务

WWW服务相对于其他服务出现比较晚，是基于超文本（HTML）传输协议HTTP的，它是因特网、多媒体网页制作技术飞速发展的必然产物。它是由瑞士日内瓦欧洲粒子物理实验室发明的，并在短时间内得到迅猛发展，是人们最常使用的因特网服务。随着Netscape公司推出安全套接字层SSL，WWW服务器和浏览器的安全性得到大大的提高，现在人们把这种技术应用于电子商务E-Business。例如，人们可以在因特网上进行股票买卖和购物。安全套接字层SSL使WWW服务的安全性提高了很多，但它主要解决的是数据包被窃听和劫持的问题。但除此之外，WWW服务还有其他问题，如下面要讲的WWW服务所使用的CGI程序、服务器端附件（Server Side Include, SSI）和Java Applet小程序等。

最初WWW服务只提供静态的HTML页面，这种页面显得很呆板，于是人们引入了CGI程序，CGI程序让人们的主页鲜活起来。CGI程序可以接收用户的输入信息，一般用户是通过表格把输入信息传给CGI程序的，然后CGI程序可以根据用户的要求进行一些处理，一般情况下会生成一个HTML软件包，利用它可做一些非法的事情，如把/etc/passwd文件传送给黑客、删除服务器上的文件等等。还有，很多人在编CGI程序时，可能对CHI软件包中的安全漏洞并不了解，多数情况下不会重新编写程序的所有部分，只是对其加以适当的修改，这样很多CGI程序就不可避免地具有相同的安全漏洞。所以，用户若要编写一个安全的CGI程序，就应先去了解这些软件包中的安全漏洞。另一个CGI程序很多是用Perl来编写的，Perl本身的功能很强大，但它同样也很不安全，其中有很多UNIX的特殊字符可用来执行UNIX的系统命令，一般入侵者就是利用这些特殊字符实施攻击的。这也是造成CGI程序安全的先天性不足，在某种意义上来讲也是TCP/IP协议先天安全性不足的重要因素之一。

（2）电子邮件服务

电子邮件服务给人们提供了一种便宜、方便和快捷的服务，E-mail地址也开始写在现代都市人的名片上了，但是电子邮件程序本身就存在许多安全性问题。如在UNIX环境下的电子邮件Sendmail，它是一个复杂且功能强大的应用软件，正因为如此它的安全漏洞就更多。程序越大、越复杂则安全漏洞可能越多，这似乎已是一个不争的事实，就拿Windows系列来讲，版本在不断更新，新功能在不断添加，老的BUG也据说是一个个被Kill，但新的问题总是层出不穷。

Sendmail在UNIX环境下以root运行，所以如果该程序被黑客利用，用户的主机的损失将会是十分巨大的。因特网蠕虫病毒曾经震惊世界，它使大批的UNIX服务处于瘫痪之中，这种病毒就是利用Sendmail安全缺陷来进攻的。如果要使这些功能以更安全的方式实现，需要对Sendmail进行重新设计和重新实现，但人们又会担心新的版本会有更多的人们难以预料的安全漏出现，于是Sendmail的开发者们只好对其修修补补。

除此之外，电子邮件中附着的Word文件或其他文件中有可能带有病毒，如Word的宏病毒等。电子邮件炸弹也是一个令人头疼的问题，但这个问题时至今日仍无法有任何有效措施来预防，更不要说彻底解决了。

（3）FTP服务和TFTP服务

这两个服务都是用于传输文件的，但使用的场合不同，安全程度也不同。