网络安全技术 系列丛书

Internet Security Professional Reference, Second Edition

Internet 网络安全 专业参考手册

（美） Derek Atkins 等著
严伟 刘晓丹 王千祥 等译

机械工业出版社
西蒙与舒斯特国际出版公司
New Riders
CMP

本书是一本非常有用的网络安全手册，几乎涵盖了 Internet 网络安全的所有方面，包括从特定的技术到特定的策略；以及保护 Internet 连接安全性的企业决策。

全书共分五大部分：管理 Internet 安全、访问并且保护网关、消息机制——创建安全的通道、当前关注的问题及附录。

本书适合计算机网络安全管理人员、大专院校师生及广大网络用户阅读。

Derek Atkins, et al.: Internet Security Professional Reference, Second Edition.

Authorized translation from the English language edition published by New Riders Publishing.

本书版权登记号：图字：01－98－1440

图书在版编目（CIP）数据

Internet 网络安全专业参考手册/（美）艾肯（Atkins, D.）；严伟等译. －北京：机械工业出版社，1998

（网络安全技术系列丛书）

书名原文：Internet Security Professional Reference, Second Edition

ISBN 7－111－06358－9

Ⅰ.I… Ⅱ.①艾…②严… Ⅲ.因特网-安全技术-手册 Ⅳ.TP309－62

中国版本图书馆 CIP 数据核字（98）第 17579 号

出 版 人：马九荣（北京市百万庄大街 22 号 邮政编码 100037）

责任编辑：傅豫波 李云静

北京忠信诚胶印厂印刷·新华书店北京发行所发行

1998 年 8 月第 1 版第 1 次印刷

787mm×1092mm $^{1}/_{16}$·40.25 印张

印数：0 001-8 000 册

定价：85.00 元（附光盘）

序

你将会发现这本《Internet 网络安全专业参考手册》是一个非常有价值的工具，它能够防止你的 Internet 连接被网络黑客、网络窃贼或其他不幸事件所危害。这本书的适用范围极广，它包括了个人、小型企业、大型企业防止安全性漏洞需要的所有信息。如果你是一位网络安全方面的专家，或者从事咨询、管理及提供 Internet 和网络方面的服务，你会需要这本书，而且会发现它对你非常有帮助。

本书几乎涵盖了 Internet 安全的所有方面，从特定的技术到特定的策略，以及关于保护 Internet 连接安全性的企业决策。作者洞察网络黑客（hacker）所思所想，以子之矛攻子之盾。如果你需要一个安全的 Internet 网络连接，那么这本书再合适不过了。

本书是如何组织的?

本书分为五个部分。

第一部分，管理 Internet 安全，包括在你规划和实现网络连接时需要着重理解的一些主题。第一部分通过 TCP/IP、UUCP、守护程序（daemon）和 audit trails 等章节，使你完全能够处理有关安全策略的问题。

第二部分，访问并且保护网关，这可能是最重要的一步了。如果你的网关不安全，那么其他什么就都不会安全。这一部分要论述电子欺骗（spoofing）、网络窥探（sniffing）和一直都很重要的防火墙，这部分还包括 SATAN 和 Kerberos，因此阅读了第二部分的这些章节之后，你就会清楚有关安全网关的所有问题。

第三部分，消息机制：创建安全的通道，这是问题的核心。如果网络黑客设法通过了你的安全基础设施，你仍然可以保护消息本身。通过详细介绍加密技术和 PGP，你就完全清楚如何充分利用加密方法。

第四部分，当前关注的问题。以深入讨论现代技术如何影响网络安全以及如何实现最佳安全性作为结尾。这部分主要包括 Java 安全性、Windows NT 安全性、CGI 安全性和病毒。

第五部分，附录，包括附录 A 和附录 B。当你查找安全性信息、资源和参考时将会发现这部分非常有用。

New Riders Publishing

New Riders Publishing 的全体员工竭诚为您提供最佳的计算机参考资料。New Riders 出版的每一本书都是作者与工作人员对书中信息经过几个月深入研究和精心筛选的结果。

作为这个承诺的一部分，New Riders 欢迎你的参与。无论是你对这本书爱不释手、对其中提供的信息和例子感到困惑不解，还是对下一个版本有一些忠告，都希望能让我们知道你的意见和建议。

但是请注意：New Riders 的工作人员不能提供有关 Internet 网络安全或软硬件问题方面的技术支持。这方面的问题请参考你的软件附带的文档或者应用程序的帮助系统。

如果你对 New Riders 出版的书籍有疑问或者意见的话，你有多种途径可以与 New Riders Publishing 联络。我们将为尽可能多的读者提供答复。

联系地址如下：

New Riders Publishing
Attn：Publisher
201 W，103rd Street
Indianapolis，IN 46290

如果你愿意的话，可以按下面这个号码给我们发传真：

317－817－7448

你也可以按照下面的电子邮件地址给我们发电子邮件：

jbelbot @ newriders.mcp.com

New Riders Publishing 是 Macmillan Computer Publishing 的标记，要获得本公司的分类目录或信息；或者要购买本公司的书籍，请拨电话 800－428－5331 或者访问我们的 Web 站点：http：//www. mcp. com。

感谢你选择了《Internet 网络安全专业参考手册》！

目　录

第二部分 访问并且保护网关

第五部分 附录

第一部分　管理 Internet 安全

第 1 章　理解 TCP/IP

TCP/IP 是数据通信协议集。这些协议包括从一台机器到另一台机器传递信息的路由、电子邮件和新闻的发送，甚至远程登录功能的使用。

从名字来看，TCP/IP 是指两个主要的协议：传输控制协议（Transmission Control Protocol）和网际互连协议（Internet Protocol）。尽管还有其他一些协议提供操作在 TCP/IP 之上的服务，但这两个协议则是最普遍使用的。

1.1　TCP/IP 的历史

通过 TCP/IP 实现网际互连已经进行了很多年，甚至几乎以 Unix 最初应用就开始了。TCP/IP 或者说传输控制协议/网际互连协议的发展已经超出了国防部高级研究项目机构（Defense Advanced Research Projects Agency，DARPA）的工作。在 1969 年，DARPA 发起了一项称为 ARPANET 的项目。这个网络主要为政府、教育研究性实验室的主要计算机站点提供高带宽的网络互连。ARPANET 为那些用户提供以一个站点传送电子邮件和文件到另一个站点的能力，而 DARPA 则为整个项目提供研究基金。随着项目的发展，人们清楚地意识到可以从中获取广泛的利益和优势，并且有可能提供跨国的网络链接。

1970 年左右，DARPA 继续资助和支持关于 ARPANET 的研究，这时的研究主要集中于点对点租用线路的互连。DARPA 还开始推动各种方式通信连接的研究，例如卫星通信和无线广播通信。就是在这个时候开始形成了公共网络互连技术的框架，由此产生了 TCP/IP。为了使这些协议获得广泛的接受和应用。DARPA 降低费用为用户实现协议。协议的实现主要在加州大学伯克利分校的 BSD Unix 上进行。

DARPA 出资创建 Bolt Beranek and Newman 公司（BBN）来开发 TCP/IP 在 BSD Unix 上的实现。在这个开发项目进行时，许多计算机站点正在采用和开发局域网技术，这时的局域网技术只是基于对以前使用的单个计算机环境的扩展。到了 1983 年 1 月，所有连接到 ARPANET 的计算机都已经运行新的 TCP/IP 协议。除此之外，许多没有连接到 ARPANET 的站点也正在使用 TCP/IP 协议。

因为 ARPANET 一般仅限于一组选择的政府部门、机构使用，所以国家科学基金会创建了 NSFNet。这个网络使用已成功运行于 ARPANET 网络上的协议，并且在某些方面可以说是 ARPANET 网络的扩展，它是连接美国所有超级计算机中心和一些与其互联小型网络的主干网。

由于 NSFNet 所使用的方法，它可以采用各种网络拓扑，而且 TCP/IP 协议并不只限于其中一种网络拓扑。这意味着 TCP/IP 协议可以运行在令牌环、以太网、各种总线结构、点对点租用线路和其他各种拓扑结构之上。然而，TCP/IP与以太网有着非常紧密的联系，以

致这两个词甚至可以互换使用。

从那时起，TCP/IP 的使用以罕见的速率增长，到全球性网际网 Internet 的连接数目也以近乎指数的速率增大。无数人开始通过 Internet 牟利，而且随着当前信息传播的趋势，Internet 将会深入到发达国家中每个人的生活里。

TCP/IP 不是一个单一的协议。事实上，它是由一组协议组成的，其中的每个协议提供一些特定的服务。本章的其余部分将探讨 TCP/IP 的地址使用、网络配置、文件控制与其他各种管理命令和守护程序。

注意　守护程序（daemon）是完成特定功能的程序。它与许多执行后就退出的命令不同，守护程序完成它的任务之后还会等待其他任务。例如 sendmail 是一个守护程序，即使没有邮件处理时，它仍然处于活动状态。

1.2　探究地址、子网和主机名

Internet 上的每台机器必须有一个唯一的地址，就像你的邮寄地址一样，这样发送给每台机器的信息才可以正常传递。这个地址机制由网际互连协议（IP）控制。

每台机器有自己的 IP 地址，IP 地址由两部分组成：网络部分和主机部分。地址的网络部分用于描述主机所在的网络，主机部分则用于标识特定的主机。为了保证网络地址的唯一性，由一个中心机构负责分配地址。

因为 Internet 的最初设计人员不知道 Internet 会发展成什么样，所以他们把地址机制设计得很灵活，使这种机制既适用于带有许多主机的大型网络，也适用于仅有几台主机的小型网络。这种寻址机制引入了地址分类，目前分为 4 类。

IP 地址可以通过几种不同形式表示。第一种是圆点分隔的十进制数表示（dotted decimal notation），对每个字节用一个十进制数字表示，用圆点分隔开，例如 192.139.234.102。另外，这个地址也可以用一个十六进制数表示，例如 0xC08BEA66。然而最常用的还是圆点十进制数表示法。

1.2.1　地址分类

前面提到过，地址有 4 种类型：A 类地址、B 类地址、C 类地址和 D 类地址。A 类、B 类和 C 类地址用于标识共用一个公共网络的计算机。D 类地址，或称多点（multicast）地址，用于标识一组共用一个公共协议的计算机。因为前三类地址的应用非常广泛，所以本章将集中讨论这三类地址。无论哪种类型的地址，都是由 32 位，即 4 个字节组成的，每个字节通常称为一个 8 位位组（octet），因此一个 IP 地址包括 4 个 8 位位组。

每个 8 位位组的数值介于 0 到 255 之间。某些特殊的值有特定的含义，如本章后面的表 1-1 所示。

1.A 类地址

在 A 类地址中，第 1 个 8 位位组表示网络部分，其他 3 个 8 位位组表示主机部分（见图 1-1）。

这类地址表示这个网络可以连接几百万台主机，因为可以使用 24 位（bit）来标识主机地址。在图 1-1 中，你会看到第一个 8 位位组的第 1 位设置为 0，这表示地址的网络部分必

须小于 128。实际上，A 类地址的网络部分范围从 1 到 127。

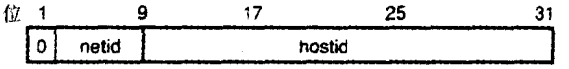

图 1-1　A 类地址的格式

2.B 类地址

B 类地址的结构同 A 类地址很相似，不同之处在于 B 类地址用 2 个 8 位位组表示网络部分，2 个 8 位位组表示主机部分（见图 1-2）。这意味着可以有更多的 B 类网络，每个 B 类网络可以连接几千台主机。

如图 1-2 所示，在 B 类地址的配置中，网络部分和主机部分具有同样数量的地址。网络地址的前 2 位被设置为 1 和 0，表示网络部分的范围从 128 到 191。按照这种格式，每个 B 类地址的网络可以有几千台主机。

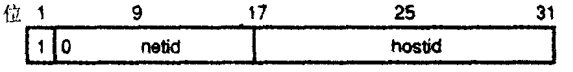

图 1-2　B 类地址的格式

3.C 类地址

C 类地址使用 3 个 8 位位组表示网络部分，使用 1 个 8 位位组表示主机部分。这种安排的结果是可以有更多的 C 类地址的网络，而每一个网络则只能连接少量的主机。因为每个 8 位位组的最大值是 255，而且还要有 2 个保留值，所以每个 C 类地址的网络最多只能连接 253 台主机。这类网络地址的格式如图 1-3 所示。

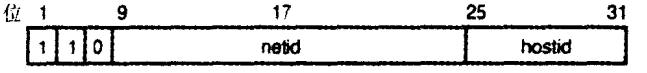

图 1-3　C 类地址的格式

如图 1-3 所示，网络地址的前 2 位均设置为 1。这表明 C 类地址的范围从 192 到 223，其余的值从 224 到 255 用于第 4 类地址。

4. 特殊地址

前面已经提到，有些地址用于特殊目的。这些地址见表 1-1。

表 1-1　保留地址

十进制地址	说　明
0.0.0.0	老式 Sun 网络的所有主机广播地址
num.num.num.0	标识整个网络
num.num.num.255	特定网络的所有主机。(广播地址)
255.255.255.255	对当前网络的所有主机广播

这些保留地址不能用于任何主机或者网络，它们已经被特别保留了下来。你在本章后面将会看到还有一些地址因为其他原因被保留了下来。

1.2.2　子网

网络中的每一台主机都有一个特定的 IP 地址，这样其他主机就可以与它通信。根据网

络类型，一个网络可以连接从 253 台到上百万台主机。然而，如果把 A 类地址或 B 类地址限制于具有千台或百万台主机的一个网络中，则是不现实的。为了解决这个问题，人们开发出子网（subnet）以便把地址的主机部分划分给其他网络。

子网采用网络的主机部分，并通过网络屏蔽（netmask）划分地址空间。网络屏蔽实际上把地址中网络部分和主机部分之间的分隔线从一个地方移动到另一个地方。这样做的作用就是增加可以使用的网络数目，而减少每一个网络可以连接的主机数目。

子网的使用带来很多好处。许多稍小一些的机构只能得到一个 C 类地址，而它们却有许多相互独立的办公室需要连接到一起。如果它们只有一个 IP 地址的话，一台路由器（router）就无法连接两个位置，因为路由器要求每个网络有一个单独的地址。通过把网络划分为子网，就可以使用路由器连接两个网络，因为现在这两个网络具有不同的网络地址。

子网要通过网络屏蔽或者子网络屏蔽来解释。对处于网络屏蔽范围内的位，地址中对应的位解释为网络位（network bit），对于地址中不在网络屏蔽范围内的位，则作为主机地址部分。要注意的是子网只在一个局部范围内起作用；对于 Internet 的其他部分，这个地址看起来仍然是一个标准的 IP 地址。

如下表所示，每一种 IP 地址类型都有一个与之相关联的缺省网络屏蔽。

表 1-2　标准网络屏蔽

地址类型	缺省网络屏蔽
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

为了清楚地理解这种机制的工作方式，考虑一个例子：假如你有一个网络地址 198.53.64.0，而你想要把它划分成子网，为了进一步划分这个 C 类网络，你必须使用地址主机部分，或者地址中最后一个字节（byte）的一些位作为网络部分。尽管这样会增加可以使用的网络数目，然而却会减少每个子网能够连接的主机数目。

Internet RFC 950 还要求保留每个子网的第 1 个和最后 1 个划分（division）。这表示实际可用的子网络数目比全部划分总和还要少两个。例如，如果你要把一个 C 类网络划分成 2 个部分，你就不能连接任何一台主机。如果你想要有六个子网络，那么你必须把你的网络分隔成 8 个划分。

下面的例子说明如何设置最后 1 个 8 位位组中的位，以及对于每一种情况可以创建多少个子网和主机。地址中代表主机部分的可变部分用字母 V 来标识。

8	7	6	5	4	3	2	1	Divisions	Subnets	Hosts/Subnets
F	V	V	V	V	V	V	V	2	0	0
F	F	V	V	V	V	V	V	4	2	62
F	F	F	V	V	V	V	V	8	6	30
F	F	F	F	V	V	V	V	16	14	14
F	F	F	F	F	V	V	V	32	30	6
F	F	F	F	F	F	V	V	64	62	2
F	F	F	F	F	F	F	V	128	126	0

上面的例子说明，可以有效使用的最小划分是 4，其中包括 2 个子网，每个子网包括 62 台主机。最多则可以分成 64 个部分，包括 62 个子网，每个子网连接 2 台主机。第 1 个例子可以用于 2 个分离的以太网，而第 2 个则可以用于一组点到点的协议链路（link）。

然而子网类型的选择要根据每个子网要求的最大用户数目和所需的最小子网数目来确定。

对地址进行划分而得到的网络部分是根据最后一个字节中固定部分的值形成的。回顾上面的例子，要把一个 C 类地址分成 8 个部分或 6 个子网，必须固定最后一个八位位组中的前 3 位。地址中的主机部分是根据最后一个字节中非固定部分的值来确定的。考虑下面这个例子，在这个例子中列出了位的组合，并且说明地址是如何划分成子网的。

Network			Host					
8	7	6	5	4	3	2	1	Decimal Values
0	0	1	0	0	0	0	0	32
0	1	0	0	0	0	0	0	64
0	1	1	0	0	0	0	0	96
1	0	0	0	0	0	0	0	128
1	0	1	0	0	0	0	0	160
1	1	0	0	0	0	0	0	192

如前面的例子所示，3 个高位——第 8、7 和 6 位——是固定的，因此这三位位用作主机地址的一部分。这意味着会有下面这些网络：

Network
N.O.P.32
N.O.P.64
N.O.P.96
N.O.P.128
N.O.P.160
N.O.P.192

C 类地址的标准网络屏蔽是 255.255.255.0。对于经过子网处理的网络，前 3 个字节仍然是相同的，第 4 个字节则是把网络部分设置为 1 同时把主机部分设置为 0，回头看一下前面的例子，你就会清楚网络地址应该是什么。你要使用同样的格式确定网络屏蔽。这些子网的网络屏蔽如下所示：

Network	Broadcast	Netmask
N.O.P.32	N.O.P.31	255.255.255.32
N.O.P.64	N.O.P.63	255.255.255.64
N.O.P.96	N.O.P.95	255.255.255.96

N.O.P.128　N.O.P.127　255.255.255.128

N.O.P.160　N.O.P.159　255.255.255.160

N.O.P.192　N.O.P.191　255.255.255.192

最后结果就是把这个 C 类地址划分成了 6 个子网，因而在不必申请额外网络地址的情况下增加了可用地址空间。

再来看看网络屏蔽，不难发现为什么许多管理员喜欢使用面向字节（byte－oriented）的网络屏蔽——因为这种方式更容易理解。然而若使用面向位的网络屏蔽，则可完成许多不同的配置。例如对一个 C 类地址使用网络屏蔽 255.255.255.192，可以创建 4 个子网络；如果把同样的网络屏蔽用于 B 类网络则可以创建超过 1000 个子网。

1.2.3　主机名

必须给每一个连接到 Internet 的设备分配一个唯一的 IP 地址，但是 IP 地址难于记忆。因而，又通常为每一个设备分配一个主机名，可以通过该主机名来访问设备。网络本身并不需要使用名字，但是这样会使网络更加易于使用。

为了使 TCP/IP 正常地工作，要把主机名翻译成相应的 IP 地址。这项工作可以通过几种不同的方法来完成。例如可以在一个称为主机表（host table）的文件中查找主机名，也可以使用域名服务（DNS）解析名字。

注意　*把主机名翻译成相应 IP 地址的方法和 DNS 将在本章后面讨论。*

一个组织机构内部的主机名必须唯一。主机名由两部分组成：实际主机名和 TCP/IP 域名，域是由一个核心注册机构根据你所在的国家和你所注册的组织类型来分配的。最常用的域包括 .com，.edu 和 .gov，它们分别代表美国的商业、教育和政府机构。尽管有可能在美国以外获得一个使用这些名称的域，但最好不要这样做。

对于美国以外的组织，还有其他一些规则指导域的分配。例如加拿大一家名为 Widgets 的公司可以申请 widgets.ca，这里 .ca 表示这家机构在加拿大。如果同样的公司在英国，那么这个域很可能会是 widgets.co.uk，表示这是英国国内的一家商业性机构。

至于主机的实际名称，Internet Request for Comments（RFC）第 1178 款提供了一些非常好的关于如何命名系统的指导。下面列出一些应牢记的指导原则：

· 使用那些简短、易拼写、易记忆的实际单词。使用主机名而不使用 IP 地址的根本原因就是因为主机名更容易使用。如果主机名难于拼写和记忆的话，那么就与其初衷背道而驰了。

· 使用主题性的名字。一个小组中的所有主机可以使用人类的一些动作命名，诸如 fall、jump 或者 hop，也可以使用卡通人物、食物或者其他分类方式命名。主题名字比那些无规则的随意名字更容易想出来。

· 要避免使用项目名称、个人名字、缩写词或者其他这类隐密性的术语。一般说来，这类主机名在将来要重新命名，这样做可不像听起来那么容易。

注意　*对主机名唯一的要求就是在它所在的域内必须唯一。无论如何选择一个好的*