TCP/IP

TCP/IP

网络实验程序篇

〔日〕村山公保 著

- TCP/IP 实际应用解析
- TCP/IP 案例 + 基本概念
- 网络与计算机知识技能的结合

科学出版社
www.sciencep.com

TCP/IP

TCP/IP
网络实验程序篇

〔日〕村山公保 著
冯 杰 闫鲁生 译
真 丁殿明 徐维川 校

科学出版社
北京

前　言

“打算更加详细地了解 TCP/IP 协议”的人数不胜数。为了更加深入地学习 TCP/IP 协议，不仅需要在理论上加以学习，而且还需要实际操作一台计算机，发送或接收一些数据包。只有做具体的实验，才能收到实际效果。

本书将通过一些计算机网络的实用程序设计来介绍 TCP/IP 协议。本书中所介绍的实例程序，不仅是通常的应用程序，而且还是直接操作 TCP/IP 的包报头的程序，有关这方面的程序还有许多。如果使用这些实例程序，那么读者可以深入地掌握各个协议的报头和具体结构。

为了使读者对计算机网络的实验更加感兴趣，在本书中还介绍了一些对 TCP/IP 通信协议的弱点进行突破的具有一定刺激的程序。例如，其中包括了能够使一些特定的主机不能进行通信的程序，还包括了借助 TCP 连接做一些非法操作的程序等。通过理解这些程序，并利用计算机网络做一些实验，读者可以掌握各种协议的特性、问题点及在应用时必须注意的各个方面等知识。

为了能够使这些程序高效地发挥作用，对在本书介绍 Ethernet 中传输的一些包进行监控的同时，还将介绍用容易理解的报头结构的形式来表示的软件。一边使用包监控工具，一边进行实验，从而能够加深对协议或协议报头的理解。

我们从日常生活中的“黑客的孕育”谈起，这里所说的黑客，并不是传媒中所指的一般黑客，而是指古代改良时代所使用的原来正面意义下的黑客。

Internet 协议是由请求评论文档(RFC)所定义的规则,但是,其中也包含有黑客等术语集合。其中,RFC 1983 年"Internet User's Glossary(网际用户术语集)"对于"hacker(黑客)"这个术语解释如下:

hacker

A person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks inparticular. The term is often misused in a pejorative context, where "cracker" would be the correct term. See also: cracker.

上述的英文翻译如下:

黑客:特指对系统、计算机和计算机网络内部的操作有深刻理解,并乐此不疲地对这些知识加以记忆的人。目前,这个术语经常被以贬义误用,准确的表达贬义的术语应该是"骇客(cracker)"。

参阅:骇客(cracker)。

人们总是认为:所谓黑客是"对计算机的内部操作、计算机网络协议的技术性能了解比较详细"的人,并且这些人对自己具有这样渊博的知识感到自豪和骄傲。

在该术语集中,关于骇客(cracker)的定义如下:

cracker

A cracker is an individual who attempts to access computer systems without authorization. These individuals are often malicious, asopposed to hackers, and have many means at their disposal forbreaking into a system. See also: hacker, Computer Emergency Response Team, Trojan Horse, virus, worm.

上述的英文翻译如下:

骇客(cracker):指未获得允许而企图访问某个计算机系统的人。这些人与黑客是不同的,他们总是带着某种

恶意。为了能够顺利地进入到某一个系统，他们不择手段，使用许多方法和工具。

参考：黑客、CERT（计算机紧急情况处理小组）、特洛伊木马、病毒和蠕虫。

在《开放源代码软件 他们能够成为商业标准吗?》（克里斯·迪博纳等著，仓骨彰译，OREILLY·Japan 发行）中，黑客是“真正的程序员”、“天才的程序员”，编制 UNIX 的美国的茨·汤普逊和 GNU 项目的理查德·斯图尔顿都可以称得上是黑客。另外，编制 Linux 的美国的理纳斯·陶巴尔兹也是一个对计算机有着深刻理解的人，在这种正面意义下他也是一名黑客，并从事于 Linux 的开发。一般地，被称为黑客的人都具有强烈的好奇心和求知欲，他们竭力想知道和理解计算机系统的内部操作，在这种想法的支配下，他们自己进行调查和研究，并且掌握了许多在用户手册中没有写到的知识。

我们中的大多数人都很难达到这样的层次，但是，将来可以培育一些黑客的种子。本书就是基于“培养（原来正面意义下的）黑客”这种强烈的想法而编写的。

为了激发广大读者心灵深处所蕴藏的好奇心，引起大家的兴趣，本书收入了许多用于深刻理解 TCP/IP 协议的程序。实际上，读者最好建立一个实验环境，分别执行这些程序，看看会产生什么样的结果。读者不仅需要通过读书来理解“表面现象”，而且也需要真正理解这些协议的内涵。另外，本书在部分章节中设置了“挑战擂台”。如果只是抱着通过读书来学习其中的内容，则学不到真正的知识，不能提高实际的技术水平。希望读者多动脑筋，去深入地思考一些问题，并且反复进行实验，直到获得满意的结果为止。通过实验所获得的知识和经验是从书本上学不到的，这样获得的真正技术在今后的业务、学习和研究中必将发挥很大的作用。

衷心地希望读者通过对本书的学习，从学习比较好的读者中，能够产生“对 Internet 技术和高度信息化社会的发展有所贡献的善良的黑客”。

“如果要详细地掌握计算机网络知识，首先必须具备计算机方面的知识”。在撰写本书的时候，我再次意识到这一点是正确的。对于读者来讲，如果感觉到自己在计算机方面的相关知识不足，则尽可能地基于本书的知识努力地去理解。但是，如果仍然还有不能够理解的知识，那么必须去阅读本系列的《TCP/IP 计算机网络篇》。本书是以“如果要详细地掌握计算机网络知识，则首先必须具备计算机方面的知识”为前提而编写的书籍。关于《TCP/IP 计算机网络篇》的内容，在本书中有不同程度的体现，本书的一部分内容是由该书的部分内容发展而来的。因此，对阅读过《TCP/IP 计算机网络篇》这本书的读者来讲，有可能感觉到部分内容与本书有点相似，希望读者能够给予谅解。本书没有依赖于该书，这样可以使读者尽可能地只阅读本书就能够理解所要讲的内容。

最后，在本书出版之际，感谢日本计算机系统公司（株）的大崎达郎先生、Acceliria 公司（株）的阿部哲士先生、东芝工程公司（株）的村山正宗先生，他们给予我很大的帮助和鼓励。另外，仓敷艺术科学大学产业科学技术学部软件学科的村山研究室和小林研究室的诸位学生、欧姆社（株）开发部以及（资本）技术部的各位先生，也给本书提供了许多宝贵的意见，这些帮助和意见对于本书的出版是非常有益的，为此再一次表示衷心的感谢。

村山公保

使用本书应该注意的问题

关于表示方法

在本书中，当表示数字的时候，使用了下面的表示规则。特别是，必须注意十进制和十六进制的表示方法是不同的。

项　目	表示方法	实　例
十进制	使用阿拉伯数字表示	12345
十六进制	在开始处使用 0x 来表示	0x0800
MAC 地址	使用十六进制数字表示，以 8 位为一个单位，中间使用(冒号:)来分隔	00:80:45:12:21:05
IPv4 地址	使用十进制数字表示，以 8 位为一个单位，中间使用(圆点.)来分隔	192.168.0.1
IPv6 地址	使用十六进制数字表示，以 16 位为一个单位，中间使用(冒号:)来区分	FE80:0:0:0:250:DAFF:FE8F:A67A

关于本书中程序的运行环境

本书中所编制的程序，在下面的环境下，经过编译后可以执行：

Linux LASER5 6.4

FreeBSD 4.2

MacOS X 10.0

PS2 Linux Beta Release 1

但是，关于第 9 章中的 IPv6 协议的程序，经过确认它只能在 FreeBSD 系统上运行。如果是标准的 BSD 系列的 UNIX 系统或 Linux 系统，那么即使对其他的操作系统或运行环境不做任何修改也可运行，或者只稍微修改就可以运行。

对于本书中所描述的程序，可以单独进行编译，在源程序列表中，我们给出了整个源程序的所有模块。其中没有使用包函数、单独的 include 文件和函数库的追加安装等。如果在 C 程序和安装标准库的环境下，则能够原封不动地对这些源程序加以

编译。

在编译源文件的时候，输入下面的命令：

```
cc  -o  执行文件名  源文件名
```

例如，在编译 scanhost.c 的时候，输入下面的命令：

```
cc  -o  scanhost  scanhost.c
```

关于程序的执行方法，请参照本书的有关章节。

使用本书程序需要注意的问题

为了突破各个协议所存在的弱点，在本书所给出的实例程序中，包含有一些与破译(cracking)工具相类似的程序。如果使用本书中的程序，则有可能造成与计算机网络相连的计算机无法通信的后果，也有可能造成系统崩溃(crush)，此时必须重新启动才能正常工作。因此，要绝对禁止将这些程序用于非法的目的。

另外，将这些程序作为教材发表，其目的是为了“提高学习的兴趣”。当然，这并不是要倡导读者去做什么非法的事情。

- 在执行程序的时候，读者可能是忐忑不安地等待着执行结果，我们之所以给出这样的程序，其目的是引起读者的兴趣。
- 如果读者自己不能够适当地设定报头值，那么就无法进行正确的操作。另外，即使所设定的值是正确的，有时也有不能够进行通信的情况存在。为了便于理解所发生的各种各样的情况，本书提供了这些程序，对于读者来讲，它们都是非常容易学习的，对于实验和研究也是合适的。
- 对程序的执行结果感到惊异，读者可以一边带着极大的兴趣，一边阅读程序，这样能够很快地提高读者的技术水平。

为了防止某些故障的发生，在一些实例程序中，我们嵌入了只有私有 IP 地址才能运行的安全措施。所谓的私有 IP 地址，是指下面范围的 IP 地址：10.0.0.0 ～ 10.255.255.255，168.16.0.0 ～ 168.31.255.255，192.168.0.0 ～ 192.168.255.255。在程序中使用了 CHKADDRESS()这样的宏汇编程序，可以对是否在私有 IP 地址环境下操作进行检查。

在学习本书程序的时候，使用私有 IP 地址，读者可以构筑本书中所介绍的实验用的计算机网络，并且可以在该计算机网络上进行实验。如果在其他人所使用的计算机网络上做实验，则需要读者在自己的管理、责任和监督的基础之上，必须加以细心的注意，绝对保证不给别人带来任何麻烦。

对于本书中所发表的程序，无论引起什么样的损害，作者和出版社都是不负任何责任的，因此，读者在使用时必须要加以注意。

关于“挑战擂台”专栏

在本书中，我们设立了“挑战擂台”专栏，作为给读者的练习题。该专栏是为提高读者的技术水平而编写的。由于时间有限，作者和出版社没有给出这个“挑战擂台”的提示和答案，所以希望读者能够给予谅解。

关于注解、输出实例等的换行

如果输入命令或输出实例等在一行中表示不下，则使用“↩”符号作为换行的标志。

目　录

第 1 章　TCP/IP 协议栈的基础知识

第 2 章　TCP/IP 协议与报头的结构

第 4 章 包监控程序的使用

第 5 章 TCP/IP 通信的识别