网络安全技术与应用大典

高永强 郭世泽 等 编著
邱盛藩 郝叶力 审校

人民邮电出版社
POSTS & TELECOMMUNICATIONS PRESS

网络安全技术与应用大典

高永强 郭世泽 等 编著
邱盛藩 郝叶力 审校

人 民 邮 电 出 版 社

图书在版编目（CIP）数据

网络安全技术与应用大典 / 高永强，郭世泽编著. —北京：人民邮电出版社，2003.3
ISBN 7-115-11029-8

Ⅰ. 网… Ⅱ. ①高…②郭… 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（2003）第 008737 号

内容提要

本书主要介绍黑客的入侵手段和防护措施。在组织结构上共分 3 个部分：第 1 部分介绍黑客入侵手段与网络安全所必备的基础知识；第 2 部分介绍系统级和网络级各个层次的黑客入侵与安全问题；第 3 部分主要从网络安全防护角度给出了具体实现方法。从技术角度上看，涉及到 Windows 9x、Windows NT、UNIX 和类 UNIX 系统等平台，包括从目标探测扫描、监听、远程控制、炸弹攻击、口令破解以及种种常用的影响较大的攻击手段。安全防护具体实现方法有：防火墙技术、数据加密技术、入侵检测系统和无线网络的安全性等。最后一章对无线网络的应用及安全性问题进行了前瞻性的论述。

本书适合从事网络安全工作的工程技术人员、网管员和大专院校师生阅读。

网络安全技术与应用大典

◆ 编　　著　高永强　郭世泽　等
审　　校　邱盛藩　郝叶力
责任编辑　张丽华
执行编辑　胡芳颖

◆ 人民邮电出版社出版发行　北京市崇文区夕照寺街 14 号
邮编　100061　电子函件　315@ptpress.com.cn
网址　http://www. ptpress.com.cn
读者热线　010-67132692
北京汉魂图文设计有限公司制作
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：26. 5
字数：658 千字　　2003 年 3 月第 1 版
印数：1-5 000 册　　2003 年 3 月北京第 1 次印刷

ISBN 7-115-11029-8/TP・3329

定价：42.00 元

本书如有印装质量问题，请与本社联系　电话：（010）67129223

编委会名单

主　编： 高永强

副主编： 郭世泽　张智慧

主　审： 邱盛藩　郝叶力

编　委： 熊　华　牛　伟　赫晓峰　段　榕

吴志军　权志中　王建伟　程　潜

杨　波　汪　涛　李晓天

前　言

在全球信息技术高度发达的今天，随着因特网的日益普及，网络对于许多人来说已经成为工作和生活中必不可少的一部分。对于企业而言，网络更是占有举足轻重的地位，电子商务已经有逐步取代传统企业经营方式的趋势，但网络在带给人们极大便利的同时，也带来了一个棘手的问题，就是“黑客”和网络安全问题。

由于因特网本身的设计缺陷及其开放性，使其极易受到黑客的入侵。根据美国有关安全部门统计，因特网上98%的计算机受到过黑客的攻击性分析，50%的计算机被黑客成功入侵，而被入侵计算机中有20%的管理员尚未发现自己已经被入侵。网络的安全性已经成为阻碍因特网在全球发展的重要因素之一。在美国包括“雅虎”、“亚马逊”、CNN在内的一些著名网站都遭到过黑客的大规模袭击，蒙受了巨大经济损失，从而引起全世界对网络安全的密切关注。2001年不仅网络病毒更加肆虐地在网上流行，各类网站被黑客入侵的消息也不时见诸于报端和知名安全网站的头条。中美黑客在“五一”期间有组织地在网上展开攻防对抗，甚至让人嗅到了一丝网络战争的味道。越来越多的人意识到，一些黑客的恶意行为已经成为全球新的公害，必须采取有力措施保护网络免受其扰。

在许多人眼中，“黑客”是一些高深莫测的神秘人物，他们利用手中所掌握的技术，肆意入侵网站，盗取商业机密。加上一些媒体对黑客事件不负责任地夸大报道，使得黑客以及黑客技术对大多数普通网民而言更多了一层神秘面纱。其实，黑客以及黑客技术并不神秘，也并不高深。一个普通网民在具备了一定基础知识之后，就可以成为一名黑客，甚至无须任何知识，只要学会使用一些黑客软件，同样可以对网络进行入侵，这也正是如今网络入侵如此盛行的原因之一。

俗话说，“知己知彼，百战不殆”。想要更好地保护自己不受黑客的伤害，就必须对黑客技术有一定的了解。只有对黑客的种种攻击手段有了详尽的认识，才能进行更有效、更具针对性的防护，使自己免受黑客入侵。我们本着使中国广大网民“认识黑客，了解黑客、防御黑客”的原则编写了这本书，从技术的角度对黑客的种种手段做了详尽的介绍，目的在于让普通网民以及网络管理员对黑客技术有一个大致的了解，从而能够保护自己免受伤害，或把损失降低到最小程度。需要强调的是，黑客行为是违反我国有关法律规定的，如果对别人实施入侵并造成了损失，就必须对自己的行为负法律责任。基于上述原因，本书在每介绍一种入侵手法的同时，都会给出与之相对应的详尽的防护方法，希望读者能够善用本书。

本书的重点在于介绍黑客的入侵手段和提供相应的保护措施，在组织结构上共分3个部分。

第1部分重点介绍了学习黑客技术与网络安全所必备的基础知识，并对计算机病毒进行了概括性的论述。其内容包括第1章“网络安全基础知识”，第2章“关于黑客”以及第3章“计算机病毒”。通过这一部分的学习，读者尤其是入门级的读者可以对黑客的概念、黑客的背景知识等有一个全面的认识，可以纠正一些关于黑客的错误概念，掀开披在黑客头上的神秘面纱。同时，读者朋友们也可以在这部分中学到掌握黑客技术最基础的知识，对那些刚涉及网络安全知识的读者而言，这一部分的学习是不可或缺的。

第2部分涵盖了当今最常见的各类黑客技术，既有针对普通计算机用户的入侵手段，更有针对各类网络、网站及公司等集团用户的入侵方法，包括了系统级和网络级各个层次的网

此为试读，需要完整PDF请访问：www.ertongbook.com

络入侵与安全问题。从技术角度上看，这部分涉及到 Windows 9x、Windows NT、UNIX 和类 UNIX 系统等各种平台，包括从目标探测扫描、监听、远程控制、炸弹攻击、口令破解以及种种常用的影响较大的入侵手段。同时还给出了网络入侵及防御的一般步骤，并举例进行了说明。内容包括第 4 章“普通计算机用户的网络安全”、第 5 章“探测与扫描”、第 6 章“Sniffer”、第 7 章“拒绝服务”、第 8 章“防御欺骗攻击”和第 9 章“防御 Web 攻击”。

第 3 部分主要从网络安全防护角度给出了相对独立的几部分内容。包括第 10 章“防范网络入侵实例”、第 11 章“防火墙技术”、第 12 章“数据加密技术与 PGP”、第 13 章“入侵检测系统”和第 14 章“无线网络的安全性”。防火墙已成为每个计算机用户保证与因特网相连的网络安全的必备软件，它可以在网络和因特网之间限制网络数据流，从而保护网络不受外部网络的威胁。防火墙的两种基本技术是包过滤和程序代理网关，本部分对防火墙的日志、规则、报警和认证等各方面作了详细的描述。数据加密技术作为一项基本技术已经成为所有通信安全的基石，它由形形色色的加密算法来实施，在多数情况下，数据加密是保证信息机密性的惟一方法。本部分对常见的数据加密方法以及邮件加密软件——PGP 做了介绍。入侵检测是防火墙的合理补充，帮助系统防御网络攻击，扩展了系统管理员的安全管理能力（包括安全审计、监视、进攻识别和响应），提高了信息安全基础结构的完整性，本书在第 13 章进行了详尽的描述。另外，无线网络正处于蓬勃发展阶段，有着很光明的应用前景，但是随之也会带来更多的安全性问题，本书的最后一章对无线网络的应用及安全性问题进行了前瞻性的论述。

在本书的编写过程中，得到了陈旭、李勇和吕跃广等同志的大力帮助与指导，提出了很多具有指导性的意见，在此向他们表示衷心的感谢。

由于作者水平有限，加上编写时间比较仓促，书中肯定存在许多不足之处，还请读者朋友们批评指正。

编者

2002 年 12 月

目　　录

此为试读，需要完整PDF请访问：www.ertongbook.com

第1章　网络安全基础知识

所谓计算机网络，就是把分布在不同地域的计算机与专门的外部设备用通信线路互联成一个规模大、功能强的系统，从而使众多的计算机可以方便地互相传递信息，共享硬件、软件和数据信息等资源。

计算机网络是现代通信技术与计算机技术相结合的产物。按照网络规模的大小和延伸的范围，可分为局域网（LAN）、城域网（MAN）和广域网（WAN）。Internet 是世界上最大的广域网。

在计算机网络产生初期，每个计算机厂商都有一套自己的网络体系结构，它们之间互不相容。为此，国际标准化组织（ISO）在 1979 年建立了一个分委员会来专门研究一种用于开放系统互联的体系结构（Open Systems Interconnection），简称 OSI。“开放”表示只要遵循 OSI 标准，一个系统可以和位于世界上任何地方的、也遵循 OSI 标准的其他任何系统进行连接。这个分委员会提出了开放系统互联（即 OSI）参考模型，该模型受到计算机界和通信业的极大关注。通过十多年的发展和推进，该模型已成为各种计算机网络结构的参照标准。目前，形成的开放系统互联基本参考模型的正式文件是 ISO 7498 国际标准，又称为 OSI/RM，即 OSI，我国的相应标准是 GB 9387。

OSI 参考模型定义了连接异种计算机的标准框架。它将计算机网络体系结构的通信协议规定为物理层、数据链路层、网络层、传输层、会话层、表示层和应用层等 7 层，如图 1.1 所示。

7	**应用层（Application Layer）**
6	**表示层（Presentation Layer）**
5	**会话层（Session Layer）**
4	**传输层（Transport Layer）**
3	**网络层（Network Layer）**
2	**数据链路层（Data Link Layer）**
1	**物理层（Physical Layer）**

图 1.1　ISO 参考模型的 7 层结构

在系统开放互联过程中，各层的具体传送细节对用户是不可见的，应用进程彼此之间可以理解成直接把数据交给对方。任何两个相同层次（如两个系统的第 4 层）之间，也似乎是直接进行数据传递的，这就是所谓的“对等层”通信。以前经常提到的各层协议，实际上就是在各个对等层之间传递数据时的各项规定。

每一个开放系统都可按照 7 个层次分为 7 个子系统。当信息在开放系统中进行交换时，发送或接收信息的究竟是一个进程、一个文件还是一个终端，都没有实质影响。为此，在 OSI 参考模型中用实体（Entity）这一名词来表示任何可以发送或接收信息的硬件或软件进程。在许多情况下，实体就是一个特定的软件模块。这样，每一层都可以看成是由若干个实体组成

的。不过，实体和子系统并不等同，实体是子系统中的活跃元素，一个子系统内可以包含一个或一个以上的实体。位于不同子系统的同一层内相互交互的实体，就构成了对等实体。控制两个对等第 *N* 层实体进行通信的规则的集合称为第 *N* 层协议。

协议语法方面的规则定义了所交换的信息的格式，而协议的语义方面的规则定义了发送者或接收者要完成的操作，例如在何种条件下数据必须重发或丢弃。

两个第 *N* 层实体之间的通信（在第 *N* 层协议的控制下），使第 *N* 层能够向上一层提供服务，这种服务就称为第 *N* 层服务。接收第 *N* 层服务的是上一层的实体，即第 *N*+1 层实体，也称为第 *N* 层服务用户。每个第 *N*+1 层实体得到的第 *N* 层服务，都是由第 *N* 层实体和另一个第 *N* 层实体通信而提供的，而这两个第 *N* 层实体间的通信，又必须借助于第 *N*-1 层实体的通信而得到。依次类推直到物理层。

第 *N* 层协议的实现保证了第 *N* 层服务得以向上一层提供，但第 *N* 层服务用户只能看见第 *N* 层服务而无法看到第 *N* 层协议。第 *N* 层协议对服务用户是透明的。

协议是“水平的”，即协议控制的是对等实体之间的通信的规则。但服务是“垂直的”，服务是由下层向上层通过层间接口提供的。上层通过与下层的服务原语的交换来使用下层所提供的服务。并且，并非在第 *N* 层内实现的全部功能都称之为第 *N* 层服务，只有那些能被高一层看见的功能才能称为“服务”。一个第 *N* 层实体向上一层提供的服务由下面 3 部分组成。

（1）第 *N* 层实体自己提供的某些功能。

（2）从第 *N*-1 层及其以下各层和本地系统环境得到的服务。

（3）通过与处在另一个开放系统中的对等第 *N* 层实体进行通信而得到的服务。

1.1 TCP/IP

1.1.1 TCP/IP 协议族

TCP/IP 是多台相同或不同类型的计算机进行信息交换的一套通信协议，是美国的高级研究计划署（ARPA）在 20 世纪 70 年代的研究成果，用来使各地的研究网络联在一起，形成一个虚拟网络（也就是 Internet 前身）。原始的 Internet 是采用 TCP/IP 将已有的网络联接到一起而形成的，而这个原始的 Internet 最终成为如今的 Internet 的骨干网。近年来，大部分操作系统都在自身的通信协议中增加了 TCP/IP 接口。几乎所有的操作系统都可以通过 TCP/IP 来实现对 Internet 的访问。如表 1.1 所示的是 TCP/IP 协议族与 7 层协议参考模型之间的关系。

表 1.1　　TCP/IP 协议族与 7 层协议参考模型之间的对应关系

OSI 中的层	功　能	TCP/IP 协议族
应用层	文件传输，电子邮件，文件服务，虚拟终端	TFTP、HTTP、SNMP、FTP、SMTP、DNS 和 Telnet
表示层	数据格式化，代码转换，数据加密	没有协议
会话层	解除或建立与别的接点的联系	没有协议
传输层	提供端对端的接口	TCP 和 UDP
网络层	为数据包选择路由	IP、ICMP、RIP、OSPF、BGP 和 IGMP
数据链路层	传输有地址的帧以及错误检测功能	SLIP、CSLIP、PPP、ARP、RARP 和 MTU
物理层	以二进制数据形式在物理媒体上传输数据	ISO2110、IEEE802 和 IEEE802.2

数据链路层包括了硬件接口和协议 ARP、RARP。这两个协议主要是用来建立送到物理层上的信息和接收从物理层上传来的信息。

网络层中的协议主要有 IP、ICMP 和 IGMP 等，由于它包含了 IP 协议模块，所以，它是所有基于 TCP/IP 网络的核心。在网络层中，IP 模块完成大部分功能。ICMP 和 IGMP 以及其他支持 IP 的协议帮助 IP 完成特定的任务，如传输差错控制信息以及主机/路由器之间的控制电文等。网络层负责网络中主机间的信息传输。

传输层上的主要协议是 TCP 和 UDP。网络层控制着主机之间的数据传递，传输层控制着那些将要进入网络层的数据。两个协议就是管理这些数据的两种方式：TCP 是一个基于连接的协议；UDP 则是面向无连接服务的管理方式的协议，如图 1.2 所示。

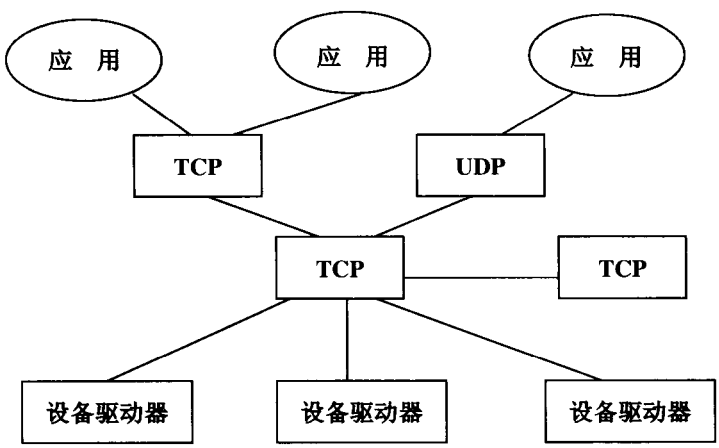

图 1.2　TCP/IP 协议族分层

应用层位于协议栈的顶端，它的主要任务是应用。常用的协议有如下几项。

（1）Telnet：提供远程登录（终端仿真）服务。

（2）FTP：提供远程文件访问等服务。

（3）SMTP：电子邮件协议。

（4）TFTP：提供小文件传输服务，是对 FTP 的一种补充。

（5）SNTP：简单网络管理协议。

（6）DNS：域名解析服务，确定如何将域名映射成 IP 地址。

（7）HTTP:超文本传输协议。

1.1.2　IP

1. IP 地址

互联网中的每台主机和路由器都有一个 IP 地址，它包括网络号和主机号。IP 地址的表示方法有很多种，最常见的表示方法是将它分成 4 个单独的字节，其中左边的数字表示高位，右边的数字表示低位，最高的几位字节是网络的标识地址，低位的字节表示网络中主机的地址。

根据最高位的长度，IETF（Internet Engineering Task Force）把 IP 地址分成了几种类型，分别命名为 A、B、C、D 和 E 类，如图 1.3 所示。

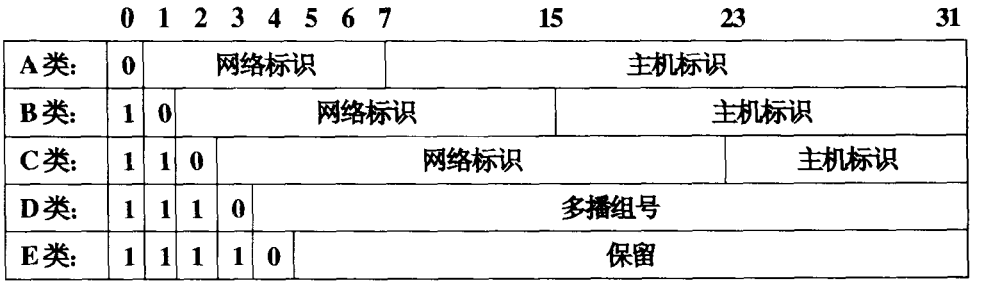

图 1.3 IP 地址分类

A 类地址用 1 个字节作为网络的 ID 号，因此 A 类只能有 127 个不同的网，每个网可以容纳 1600 万台主机，这种地址类型的范围是从 1.0.0.0 到 127.255.255.255。

B 类地址用 2 个字节作为网络的 ID 号，因此，B 类的网络有 16384 个，每一个 B 类的网可以连接 65536 台主机。IETF 规定 B 类地址只分配给客户多于 256 个的网络。B 类地址的范围是从 128.0.0.0 到 191.255.255.255。

C 类地址是目前最常用的地址，它用 3 个字节作为网络的 ID 号，因此，有 2097152 个 C 类网络，每个网络最多可以容纳 256 台主机，C 类网络的地址范围从 192.0.0.0 到 223.255.255.255。C 类网络的典型地址是 192.168.xxx.xxx。

D 类地址是作为对多点播送地址，数据报可以直接发往多个多点播送主机。这类地址很少，地址范围是从 224.0.0.0 到 239.255.255.255。

E 类地址是 IETF 预留的，留做将来“不时之需”的。它的地址范围是从 240.0.0.0 到 247.255.255.255。

另外有一些具有特殊含义的 IP 地址。如 255.255.255.255 表示 Internet 上所有的主机，x.x.255.255 表示该网上所有的计算机，0.0.0.0 用来启动以后不再使用的主机，127.xx.xx.xx 用做回路测试，127.0.0.1 表示本机的地址等。

正确检测 TCP/IP 的 4 个步骤：ping 127.0.0.1（回环地址）如果通过则表示 TCP/IP 已经装入，ping 自己表明客户机正常（主要是网卡），ping 网关表示局域网正常，ping 路由外地址表示完全正常。

2. IP 报文

IP 报文包含各类字段。

版本（Vereion）字段记录了数据报协议的版本。这个字段使得遵从不同版本的协议的主机之间可以互相传输数据。

IHL 字段指示报文头的长度，以 32 位字节长度为 1 个单位，最小值是 5，最大值是 15。

服务类型（Type of Service）字段通知子网主机需要的服务，可能包含各种可靠性和速度的组合。对于数字化声音传输，速度要求高于准确性要求；而对于文件传输，准确性又比速度重要。该字段本身包含（从左到右）1 个 3 位优先顺序（Precendence）字段、3 个标志位（D、T 和 R），还有 2 位未用。优先顺序字段是标志优先级的，从 0（一般）到 7（网络控制分组），3 个标志位表示出主机最关心组合（延迟、吞吐量和可靠性）中的哪一项。理论上，这些字段应该指示路由器的动作，例如，是用有高吞吐量而且高延迟的卫星线路还是用低吞吐量低延迟的租用线路。但实际上，现在的路由器都忽略服务质量（Type of Service）字段。

IP 报的格式如图 1.4 所示。

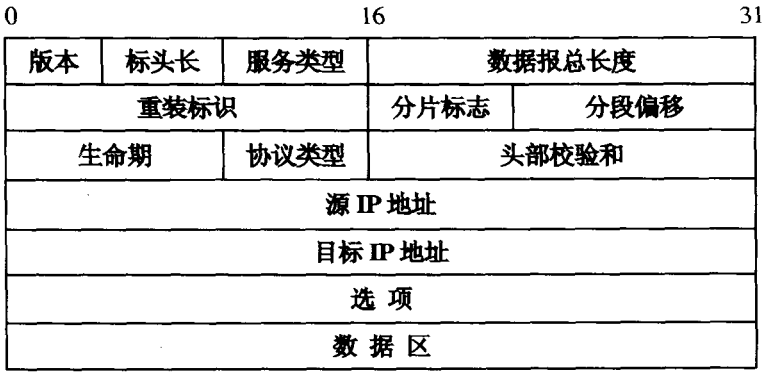

图 1.4　IP 报的格式

总长（Total Length）包括数据报中的所有信息——包括头部和数据，最大长度是 65535 字节。

标识（Identification）字段用来让目的主机判断新来的分段属于哪个分组，所有属于同一分组的分段都会包含同样的标识值。

紧跟着的是 2 个未用的位，然后是 2 个 1 位字段。DF 代表不分段，它告诉路由器不要将数据报分段，因为目的端不能重组分段。例如，当一个计算机启动时，它的 ROM 可能会要求向它发送一个包含内存映像的单个数据报。通过标志数据报的 DF 位，发送者就知道分组应该完整地到达，即使这意味着数据报必须绕过可能在最优路径上的小分组网络而不得不使用次优路由。每台计算机都要能接收 576 字节或更少的分段。

MF 代表还有进一步的分段。除了最后一个分段，所有分段都设置了这一位。它用来标志所有分组是否都已到达。

分段偏移（Fragment Offset）说明分段在当前数据报的什么位置。除了数据报中的最后一个分段外，所有分段都要乘以 8 字节，它是基本分段单位，提供了 13 位，每个数据报最长是 8192 个分组，最大的数据报长度是 65536 字节。

生命期（Time To Live）字段是一个用来限制分组生命周期的计数器。推荐以秒来计数，最长生命周期是 255 s。它必须在每个节点中都递减，而且当在 1 个路由器中排队时间过长时可以倍数递减。实际上，它只以节点数计数，当它减到零时，该分组就要丢弃，并向源主机发送 1 个警告分组，这一特性能防止数据报在网中无限制地漫游（当路由选择表崩溃时就会发生这种情况）。

协议字段说明当网络层组装完 1 个完整分组后，应将该分组送给哪个传输进程（TCP、UDP 或其他）。协议的编号在互联网上是通用的，它在 RFC 1700 中有相应定义。

头部校验和用来校验头部，可以利用校验和检测路由器中的内存坏字。当数据到达时，该算法将头部所有 16 位半字数据累加起来，采用求补运算，再取其结果的补码。由该算法的原理可知，当数据报到达时其头部校验和应该为零。注意，头部校验和在每个节点都要重新计算，因为至少有一个字段总是在变（生命周期字段），但也有技巧可以加速计算。

源地址和目标地址指明了网络号和主机号。

可选项则允许在后续版本的协议中引入最初版本中没有的信息，每个可选项都以一个字节标明内容。有些可选项还跟有 1 字节的可选项长度字段，其后是 1 个或多个数据字节。可

此为试读，需要完整PDF请访问：www.ertongbook.com