求是科技

网络与信息安全

# 攻击与防护

## 网络安全与实用防护技术

■求是科技 董玉格 金海 赵振 编著

第 1 章 网络概述

第 2 章 Visual C++ 编程基础

第 3 章 攻击工具及典型代码分析

第 4 章 黑客攻击的常用方法剖析

第 5 章 病毒原理分析

第 6 章 操作系统的安全漏洞

第 7 章 数据加密

第 8 章 远程控制技术原理与编程实现

第 9 章 网络入侵检测

人民邮电出版社
POSTS & TELECOMMUNICATIONS PRESS

求是科技

网络与信息安全

# 攻击与防护

## 网络安全与实用防护技术

求是科技 董玉格 金海 赵振 编著

人民邮电出版社

**图书在版编目（CIP）数据**

攻击与防护：网络安全与实用防护技术 / 董玉格，金海，赵振编著. —北京：人民邮电出版社，2002.8
ISBN 7-115-10419-0

I. 攻… II. ①董… ②金… ③赵… 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（2002）第 048921 号

## 内容提要

本书向读者介绍了有关网络安全技术方面的内容，为了了解黑客对网络实施攻击时常用的方法，必须要熟悉网络编程技术。因此，全书分为两个部分，第一部分主要是网络基础知识和 Visual C++网络编程技术，第二部分是本书的核心内容，给读者分析了网络（包括本地主机）攻击的原理、典型的技术手段，并给出相应的防范措施和工具。此外，本书还介绍了网络系统安全漏洞问题、信息加密技术等，除此之外，本书还给出很多的简单示例，以便读者更容易理解和掌握相应的防护技术。

本书内容丰富，讲解由浅入深，有很强的实用性和指导性，适于从事网络安全开发和维护人员阅读，也可供对网络安全感兴趣的读者阅读。

网络与信息安全

**攻击与防护——网络安全与实用防护技术**

◆ 编　著　求是科技　董玉格　金　海　赵　振
责任编辑　张立科

◆ 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　010-67180876
北京汉魂图文设计有限公司制作
北京鸿佳印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：25. 5
字数：621 千字　　2002 年 8 月第 1 版
印数：1-5 000 册　　2002 年 8 月北京第 1 次印刷

ISBN 7-115-10419-0/TP・2959

定价：36.00 元

# 关于本书

自20世纪90年代以来，网络得到了惊人的发展。在网络给人们带来诸多好处的同时，也带来了一些不可避免的负面影响，比如遭受网络攻击、信息被盗等。为了有效地防范网络攻击，维护自己的权益不受侵犯，就需要我们尽量了解网络攻击的各种原理和手段、网络中存在的各种漏洞，以便及时维护我们的系统。

全书共分为两大部分内容：

第一部分主要讲解网络基础知识和Visual C++网络编程技术的基础，读者通过学习该部分内容，可以为理解和掌握本书后面的网络安全技术做充分准备。第1章主要介绍了计算机网络的基础知识，围绕着最重要的TCP/IP协议向读者介绍OSI模型，TCP/IP的安全性能的改进等内容。第2章是Visual C++的网络编程技术，希望读者至少掌握一种网络编程工具，这样对后续章节的攻击手段分析和系统漏洞介绍会有更深的理解。

第二部分是本书的核心内容，向读者介绍了网络（包括本地主机）攻击的原理、典型的技术手段以及范例代码分析，并给出相应的防范措施和工具。此外，还介绍了网络系统安全漏洞问题、信息加密技术等，例如如何通过远程控制等方法对网络进行攻击，如何防范CIH病毒、红色代码、尼姆达和爱虫等典型病毒的侵害等内容。

第3章介绍了黑客进行网络攻击所使用的手段和相应工具，如扫描器、嗅探器、口令攻击器、特洛伊木马、网络炸弹和ASP攻击等，并且给出了相应的防范措施。

第4章分析了网络攻击的常用攻击方法，例如缓冲区溢出方法、各种网络欺骗方法等。

第5章介绍了病毒的原理，并且介绍和分析了近年来4种影响比较大的病毒：CIH、红色代码、尼姆达和“爱虫”病毒，具体总结了各自的特点，同时对其代码也作了针对性分析。

第6章介绍了Windows和UNIX两类平台的漏洞，以便读者在使用这两种操作系统时做到心中有数。

第7章介绍了数据加密的基本原理和手段，以便读者更好地保护自己的重要信息不被窃取。

第8章分析了远程控制技术的原理和相关技术手段，如客户和服务端程序的编写、运行，木马程序的驻留和启动等。

第9章向读者介绍了系统入侵检测技术。虽然它还有待不断丰富和完善，但该技术具有良好的前景，希望读者能先有个初步理解。

本书比较详尽地介绍了防范网络遭受攻击所涉及到的各方面问题，希望通过本书能让读者对网络安全问题有一个总体性的了解。由于编者水平有限，对于本书的错误或是不足之处，恳请广大读者给以指正。本书源代码，读者可到http://www.ucbook.com下载。

编者

# 目　录


第 1 章　网络概述 …… 1
1.1　网络与黑客的历史 …… 1
1.1.1　网络的历史 …… 1
1.1.2　黑客的历史 …… 3
1.2　OSI 模型 …… 4
1.2.1　模型 …… 4
1.2.2　OSI 安全服务 …… 6
1.3　TCP/IP 概貌 …… 7
1.3.1　TCP 层 …… 9
1.3.2　IP 层 …… 11
1.3.3　以太网（Ethernet）层 …… 12
1.4　UDP 和 ICMP 协议 …… 13
1.5　路由（Routing） …… 14
1.6　端口号 …… 15
1.7　数据包的分离和重新组装 …… 15
1.8　以太网封装——地址解析协议（ARP） …… 16
1.9　TCP/IP 协议安全性能的改进 …… 17
1.9.1　TCP 状态转移图和定时器 …… 17
1.9.2　网络入侵方式 …… 18
1.9.3　利用网络监控设备观测网络入侵 …… 20
1.10　本章小结 …… 21
第 2 章　Visual C++编程基础 …… 23
2.1　什么是套接字 …… 23
2.2　Socket 模式 …… 24
2.2.1　Berkeley Socket …… 24
2.2.2　Winsock …… 29
2.2.3　程序举例——简单扫描器 …… 39
2.3　MFC 的 Winsock 编程 …… 40
2.3.1　MFC 网络编程概述 …… 40
2.3.2　CASynCSocket 类和 CSocket 类 …… 41
2.3.3　CAsyncSocket 类和 CSocket 类的成员函数和变量 …… 46
2.4　WinInet 类 …… 48
2.4.1　MFC WinInet 类 …… 49
2.4.2　WinInet 实例 …… 50

2.5 虚拟内存编程控制 …… 68
2.5.1 虚拟内存概述 …… 68
2.5.2 Windows 9x 中的虚拟内存 …… 69
2.5.3 Windows 2000 虚拟内存 …… 71
2.5.4 Windows 2000 虚拟内存编程控制 …… 73
2.6 本章小结 …… 78
**第 3 章 攻击工具及典型代码分析** …… 79
3.1 网络攻击综述 …… 79
3.1.1 准备阶段 …… 79
3.1.2 实施阶段 …… 79
3.1.3 善后处理阶段 …… 79
3.2 扫描器(Sniffer)…… 80
3.2.1 攻击原理 …… 80
3.2.2 nmap 实例 …… 81
3.2.3 常用程序介绍 …… 84
3.2.4 典型代码分析 …… 86
3.3 网络监听——嗅探器（Sniffer） …… 89
3.3.1 攻击原理 …… 89
3.3.2 怎样发现嗅探器 …… 91
3.3.3 sniffe 实例 …… 91
3.3.4 常用程序介绍 …… 96
3.3.5 典型代码分析 …… 97
3.3.6 防范措施 …… 99
3.4 口令攻击器 …… 101
3.4.1 口令攻击原理 …… 101
3.4.2 口令攻击实例 …… 103
3.4.3 常用程序介绍 …… 108
3.4.4 典型代码分析 …… 109
3.4.5 防范措施 …… 117
3.5 特洛伊木马 …… 119
3.5.1 木马的攻击原理 …… 119
3.5.2 Subseven 实例 …… 121
3.5.3 常用程序介绍 …… 126
3.5.4 典型代码分析 …… 128
3.5.5 防范措施 …… 133
3.6 网络炸弹 …… 135
3.6.1 网络炸弹的原理 …… 135
3.6.2 网络炸弹实例 …… 136
3.6.3 网络炸弹的防范 …… 142
3.6.4 网页炸弹 …… 144

3.7 ASP 攻击 …… 146
3.7.1 引言 …… 146
3.7.2 ASP 漏洞集锦 …… 147
3.8 本章小结 …… 154
**第 4 章 黑客攻击的常用方法剖析** …… 155
4.1 缓冲区溢出 …… 155
4.1.1 基本原理 …… 155
4.1.2 缓冲区溢出攻击代码分析 …… 158
4.2 欺骗攻击 …… 160
4.2.1 IP 攻击 …… 160
4.2.2 DNS 欺骗 …… 163
4.2.3 Web 欺骗 …… 165
4.3 利用后门攻击综述 …… 169
4.3.1 UNIX 系统中存在的后门 …… 170
4.3.2 系统后门的解决方案 …… 173
4.4 经典入侵过程 …… 174
4.4.1 米特尼克利用 IP 欺骗攻破 SanDiego 计算中心 …… 174
4.4.2 一次入侵 Windows 2000 Server 的全过程 …… 179
4.5 本章小结 …… 181
**第 5 章 病毒原理、源代码分析及对策** …… 183
5.1 病毒概述 …… 183
5.1.1 病毒简史 …… 183
5.1.2 病毒定义 …… 184
5.1.3 病毒的特征 …… 184
5.1.4 病毒的分类 …… 185
5.1.5 病毒的防治 …… 186
5.2 CIH 病毒 …… 187
5.2.1 CIH 病毒的侵害原理 …… 187
5.2.2 CIH 病毒源代码分析 …… 189
5.2.3 CIH 病毒查杀手段 …… 197
5.3 红色代码（CodeRed） …… 198
5.3.1 红色代码的侵害原理 …… 198
5.3.2 CodeRedIII 源代码分析 …… 200
5.3.3 红色代码 3 的清除 …… 203
5.4 尼姆达（Nimda）病毒 …… 204
5.4.1 尼姆达病毒的侵害原理 …… 204
5.4.2 尼姆达病毒的源代码分析 …… 205
5.4.3 尼姆达病毒的查杀手段 …… 211
5.5 “爱虫”病毒 …… 212
5.5.1 “爱虫”病毒侵害原理 …… 213

5.5.2 “爱虫”病毒源代码分析 …… 213
5.5.3 “爱虫”病毒源代码 …… 217
5.5.4 绝杀“爱虫”病毒 …… 217
5.6 本章小结 …… 218
**第 6 章 操作系统的安全漏洞** …… 219
6.1 Windows 操作系统 …… 219
6.1.1 Windows 9x 远程漏洞发掘 …… 219
6.1.2 Windows 9x 的本地漏洞发掘 …… 222
6.1.3 Windows 千年版（Me） …… 227
6.1.4 小结 …… 228
6.2 Windows 2000/NT …… 228
6.2.1 Windows 2000 漏洞 …… 228
6.2.2 Windows 2000 Server 的安全配置 …… 241
6.2.3 Windows NT 系统安全 …… 246
6.2.4 用户管理安全 …… 250
6.2.5 Windows NT 服务器的安全维护 …… 252
6.3 UNIX 系统的安全 …… 260
6.3.1 系统的安全管理 …… 260
6.3.2 用户的安全管理 …… 281
6.3.3 通用 UNIX 系统安全检查列表 …… 286
6.4 本章小结 …… 293
**第 7 章 数据加密** …… 295
7.1 密码学概述 …… 295
7.1.1 为什么要进行数据加密 …… 295
7.1.2 什么是数据加密 …… 295
7.1.3 加密的原理 …… 296
7.1.4 加密技术及密码分析 …… 297
7.2 对称秘钥算法 …… 303
7.2.1 对称密钥密码学简介 …… 303
7.2.2 DES 算法 …… 303
7.2.3 IDEA 加密算法 …… 307
7.2.4 对称密钥加密模式 …… 308
7.3 非对称密钥密码系统 …… 310
7.3.1 非对称密钥密码概论 …… 311
7.3.2 RSA 非对称密钥密码技术 …… 312
7.3.3 DSA 数字签名技术 …… 314
7.3.4 Difnie-Hellman 密钥交换系统 …… 316
7.3.5 单向杂凑函数 …… 317
7.4 广泛应用的 PGP …… 332
7.4.1 PGP 简介 …… 332

7.4.2 PGP 的安全性问题 …… 335
7.5 本章小结 …… 342
**第 8 章 远程控制技术原理与编程实现** …… 343
8.1 远程控制技术原理 …… 343
8.1.1 引言 …… 343
8.1.2 远程控制技术原理 …… 344
8.1.3 远程唤醒 …… 344
8.2 客户/服务器 …… 345
8.2.1 引言 …… 345
8.2.2 客户与服务器的特性 …… 345
8.2.3 客户/服务器原理 …… 346
8.3 一个简单的客户服务器程序 …… 349
8.3.1 程序的核心技术 …… 349
8.3.2 源程序 …… 352
8.3.3 演示程序结果 …… 360
8.4 作为木马的远程控制程序 …… 361
8.4.1 木马的自启动方式 …… 362
8.4.2 木马的隐藏方式 …… 364
8.5 远程控制编程 …… 369
8.5.1 实现远程关机 …… 370
8.5.2 添加系统文件 …… 374
8.5.3 改写注册表 …… 376
8.6 本章小结 …… 387
**第 9 章 网络入侵检测** …… 389
9.1 概念定义与功能描述 …… 389
9.2 技术途径 …… 389
9.2.1 收集信息 …… 389
9.2.2 数据分析 …… 390
9.3 入侵检测的分类 …… 392
9.3.1 按检测技术分类 …… 392
9.3.2 按输入数据的来源分类 …… 392
9.3.3 按检测行为分类 …… 392
9.4 入侵检测的评估 …… 393
9.5 入侵检测的产品 …… 394
9.6 问题与发展 …… 395
9.7 本章小结 …… 397

# 第 1 章　网络概述

五彩缤纷的网络世界是多么的奇妙，它把整个世界变得如此紧凑，以至于我们坐在家里就可以观赏世界各地的人文风景和奇闻趣事。当收到远方亲友的电子邮件时，我们激动万分；当回顾过去的经典影片时，我们会心地微笑；当聆听当年的 MP3 时，我们思绪万千，渐渐地我们已经离不开网络了。

但是，我们在登录网站时，是否听说过路由选择和域名服务（DNS）；当发送邮件时，是否想过它与 SMTP 有什么联系；可否考虑过传输在网络中的数据包（Package）是怎么回事？全部的这些都是因为有了 TCP/IP 协议的支撑。Internet 就是以 TCP/IP 作为它的协议的。因此我们要研究 TCP/IP 协议，发现网络的漏洞，采取措施保证网络安全，为大家更好的服务。

## 1.1　网络与黑客的历史

### 1.1.1　网络的历史

网络的历史不长，但是自从它诞生就焕发出勃勃的生机，并且以惊人的速度膨胀着。而且正向着社会的每一个角落渗透。可以这样说，自从有了网络，人类的生活就翻开了崭新的一页！

#### 1. Internet 在世界的发展

1972 年，ARPANet 在首届计算机后台通信国际会议上首次与公众见面，并验证了分组交换技术的可行性。由此，ARPANet 成为现代计算机网络诞生的标志。ARPANet 在技术上的另一个重大贡献是 TCP/IP 协议簇的开发和使用。1980 年，ARPA 投资把 TCP/IP 加进 UNIX（BSD 4.1 版本）的内核中，在 BSD 4.2 版本以后，TCP/IP 协议即成为 UNIX 操作系统的标准通信模块。

1982 年，Internet 由 ARPANet、MILNet 等几个计算机网络合并而成，作为 Internet 的早期骨干网，ARPANet 试验并奠定了 Internet 存在和发展的基础，较好地解决了异种机网络互联的一系列理论和技术问题。

1983 年，ARPANet 分裂为两部分：ARPANet 和纯军事用的 MILNET。该年 1 月，ARPA 把 TCP/IP 协议作为 ARPANet 的标准协议，其后，人们称呼这个以 ARPANet 为主干网的网际互联网为 Internet，TCP/IP 协议簇便在 Internet 中进行研究、试验，并改进成为现在使用方便、效率极高的协议簇。与此同时，局域网和其他广域网的产生和蓬勃发展对 Internet 的进一步发展起了重要的作用。其中，最为引人注目的就是美国国家科学基金会 NSF（National Science Foundation）建立的美国国家科学基金网 NSFnet，1986 年，NSF 建立起了 6 大超级

计算机中心，为了使全国的科学家、工程师能够共享这些超级计算机设施，NSF 建立了自己的基于 TCP/IP 协议簇的计算机网络 NSFnet。NSF 在美国建立了按地区划分的计算机广域网，并将这些地区网络和超级计算中心相联，最后将各超级计算中心互联起来。地区网的构成一般是由一批在地理上局限于某一地域，在管理上隶属于某一机构或在经济上有共同利益的用户的计算机互联而成，连接各地区网上主通信结点计算机的高速数据专线构成了 NSFnet 的主干网。这样，当一个用户的计算机与某一地区相联以后，它除了可以使用任一超级计算中心的设施，可以同网上任一用户通信，还可以获得网络提供的大量信息和数据。这一成功使得 NSFnet 于 1990 年 6 月彻底取代了 ARPANet 而成为 Internet 的主干网。

NSFnet 对 Internet 的最大贡献是使 Internet 向全社会开放，而不像以前那样仅仅被计算机研究人员、政府职员和政府承包商使用。然而，随着网上通信量的迅猛增长，NSF 不得不采用更新的网络技术来适应发展的需要。1990 年 9 月，由 Merit、IBM 和 MCI 公司联合建了一个非赢利性的组织——先进网络和科学公司 ANS（Advanced Network & Science, Inc）。ANS 的目的是建立一个全美范围的 T3 级主干网，它能以 45Mbit/s 的速率传送数据，相当于每秒传送 1400 页文本信息。到 1991 年底，NSFnet 的全部主干网都已同 ANS 提供的 T3 级主干网相通。

回想 1969 年 12 月，当 ARPANet 最初建成时只有 4 个结点，而 1994 年，Internet 上的主机数目达到了 320 万台，连接了世界上的 35000 个计算机网络。现在，全世界已有 100 多万个网络，1 亿台主机和超过 10 亿的用户，Internet 发展速度如表 1-1 所示。

表 1-1　　Internet 的发展速度

| 年份（年） | Internet 的结点数（个） |
|---|---|
| 1969 | 4 |
| 1972 | 23 |
| 1988 | 56 000 |
| 1994 | 3 200 000 |
| 2000 | 超过 100 000 000 |

今天的 Internet 已不再仅仅是计算机人员和军事部门进行科研的领域，而是变成了一个开发和使用信息资源的覆盖全球的信息海洋。在 Internet 上，按从事的业务分类包括了广告公司、航空公司、农业生产公司、艺术、导航设备、书店、化工、通信、计算机、咨询、娱乐、财贸各类商店、旅馆等等 100 多类，覆盖了社会生活的方方面面，构成了一个信息社会的缩影。

### 2. Internet 在中国的发展

中国早在 1987 年就由中国科学院高能物理研究所（简称高能所）首先通过 X.25 租用线实现了国际远程联网，并于 1988 年实现了与欧洲和北美地区的 E-mail 通信。1993 年 3 月经电信部门的大力配合，开通了由高能所到美国 Stanford 直线加速中心的高速计算机通信专线。1994 年 5 月高能所的计算机正式进入了 Internet 网。与此同时，以清华大学为网络中心的中国教育与科研网也于 1994 年 6 月正式联通 Internet 网。1996 年 6 月，中国最大的 Internet 互联子网 CHINAnet 也正式开通并投入营运，在中国兴起了一种研究、学习和使用 Internet 的浪潮。现在，中国已成为 Internet 的重要增长点。中国的用户已经越来越走进 Internet，而 Internet

则已经越来越成为中国人科研工作甚至日常生活的一个重要组成部分。

### 1.1.2　黑客的历史

黑客的身影已经存在了一个多世纪。最早的黑客可以追溯到 19 世纪 70 年代的几个青少年，它们用破坏新注册的电话系统的行为挑战权威。下面就来看一看最近 35 年来黑客们的忙碌身影。

20 世纪 60 年代初，装备有巨型计算机的大学校园，比如 MIT 的人工智能实验室，成为黑客们施展拳脚的舞台。最开始，黑客（Hacker）这个词只是指那些可以随心所欲地编写计算机程序实现自己意图的计算机高手，并没有任何贬义。

20 世纪 70 年代初，John Draper 发现通过一种饼干盒里发出的哨声可以制造出精确的音频输入话筒让电话系统开启线路，从而可以借此进行免费的长途通话。Draper 后来赢得了“嘎扎上尉”的绰号。整个 20 世纪 70 年代，Draper 因盗用电话线路而多次被捕。雅皮士社会运动发行了 YIPL/TAP 杂志（青年国际阵营联盟/技术协助计划）来帮助电话黑客（称为“Phreaks”，即电话线路盗用者）进行免费的长途通话。加利福尼亚 Homebrew 电脑俱乐部的两名成员开始制做“蓝盒子”，并用这种装置侵入电话系统。这两名成员一个绰号“伯克利蓝”（即 SteveJobs），另一个绰号“橡树皮”（即 SteveWozniak），它们后来创建了苹果电脑。

20 世纪 80 年代初，作家 William Gibson 在一部名叫巫师（Neuromancer）的科幻小说中创造了“电脑空间”一词。美国联邦调查局开始逮捕犯罪的黑客，在最初的几起黑客罪案中，名为 Milwaukee-based414s 的黑客小组（用当地的分区代码取名）颇引人注目，其成员被指控参与了 60 起计算机侵入案，被侵对象包括 Sloan-Kettering 癌症中心甚至洛斯阿莫斯国家实验室。新颁布的综合犯罪控制法案赋予联邦经济情报局以法律权限打击信用卡和电脑欺诈犯罪。两个黑客团体相继成立，它们是美国的“末日军团”和德国的“混沌电脑俱乐部”。“黑客季刊”创刊，用于电话黑客和电脑黑客交流秘密信息。

20 世纪 80 年代末，新颁布的电脑欺骗和滥用法案赋予联邦政府更多的权利。美国国防部为此成立了计算机紧急应对小组，设在匹兹堡的卡耐基-梅隆大学，它的任务是调查日益增长的计算机网络犯罪。经验丰富的黑客 Kevin Mitnick 秘密监控负责 MCI 和数字设备安全的政府官员的往来电子邮件，Kevin Mitnick 因破坏计算机和盗取软件被判入狱一年。芝加哥第一国家银行成为一桩 7000 万美元的电脑抢劫案的受害者。一个绰号“FryGuy”的印第安那州的黑客因侵入麦当劳系统，被警方强行搜捕。在亚特兰大，警方同样搜捕了“末日军团”的 3 名黑客成员。

20 世纪 90 年代早期，由于 AT&T 的长途服务系统在马丁路德金纪念日崩溃，美国开始实施全面打击黑客的行动。联邦政府逮捕了圣路易斯的”Knight Lightning”。在纽约抓获了“欺骗大师”的 3 剑客“Phiber Optik”、“Acid Phreak”和“Scorpion”。独立黑客“Eric Bloodaxe”则在德克萨斯被捕。由联邦经济情报局和亚里桑那打击有组织犯罪单位的成员成立了一个取名 Operation Sundevil 的特殊小组，在包括迈阿密在内的 12 个主要城市进行了大搜捕，这个持续 17 周的亚里桑那大调查，最后以捕获黑客 Kevin Lee Poulsen（绰号“黑色旦丁”）而宣告终结。“黑色旦丁”被指控偷取了军事文件。黑客成功侵入格里菲思空军基地，然后又袭击了美国国家航空航天管理局（NASA）以及韩国原子研究所的计算机。德州 A&M 的一名教授不断收到一个从校园外登录到其计算机的黑客发出的死亡威胁，该教授被迫用其互联网址

发送了 2 万多封种族主义内容的电子邮件。Kevin Mitnick 再次被抓获，这一次是在纽约的 Raleigh，他被圣迭哥超级计算中心的 Tsutomu Shimomura 追踪并截获。

20 世纪 90 年代末，美国联邦网站大量被黑，包括美国司法部、美国空军、中央情报局和美国航空航天管理局等。美国审计总局的报告表明仅仅 1995 年美国国防部就遭到黑客侵袭达 25 万次之多。一个加拿大的黑客组织“男孩时代”，因对其成员受错误指控非常愤怒，而侵入了加拿大广播公司的网站并留下一条信息称“媒体是骗子”。该组织的黑客被媒体指控对加拿大的某个家庭进行电子追踪，但稍后的调查表明该家庭 15 岁的儿子才是进行电子追踪的真正元凶。黑客们成功穿透了微软公司的 NT 操作系统的安全屏障，并大肆描述其缺陷。流行的电子搜索引擎 YAHOO！被黑客袭击，黑客声称如果 Kevin Mitnick 不被释放，一个“逻辑炸弹”将于 1997 年圣诞节在所有 YAHOO！用户的电脑中爆发。

1998 年，反黑客的广告开始在电视频道 Super Bowl XXXII 上播出，这是互联网协会的一则 30 秒的广告，花费 130 万美元。广告的内容是两个俄罗斯导弹发射基地的工作人员担心黑客通过计算机发出发射导弹的指令，它们认为黑客可能以任何方式决定这个世界的毁灭。1 月，联邦劳动统计局连续几天被成千上万条虚假请求信息所淹没，这种黑客攻击方式名为“spamming”。黑客们侵入美国儿童基金会网站，并威胁如不释放 KevinMitnick 将会有大屠杀。黑客声称已经侵入五角大楼局域网，并窃取了一个军事卫星系统软件。黑客们威胁将把软件卖给恐怖分子。美国司法部宣布国家基础设施保护中心的使命是保护国家通信，科技和交通系统免遭黑客侵犯。黑客组织 L0pht 在美国国会听证会上警告说，它可以在 30 分钟内关闭全国范围内的所有进出互联网的通道。

1999 年 5 月~6 月，美国参议院、白宫和美国陆军网络以及数十个政府网站都被黑客攻陷。在每起黑客攻击事件中，黑客都在网页上留下信息，但是这些信息很快就被擦去。1999 年 11 月，挪威黑客组织“反编译工程大师”破解了 DVD 版权保护的解码密钥。该组织编制了一个 DVD 解码程序公布在互联网上，这个举动引发了一系列诉讼案。2000 年 2 月，在三天的时间里，黑客使美国数家顶级互联网站（雅虎、亚马逊、电子港湾、CNN）陷入瘫痪。黑客使用了一种称作“拒绝服务式”的攻击手段，即用大量无用信息阻塞网站的服务器，使其不能提供正常服务。

2001 年中美黑客大战，涉及的人员之广，破坏的面积之大也是空前的。黑客从单打独斗，已发展成集团的协作。

以上大家了解了网络及黑客的历史，下面转入正题，先从 OSI 模型开始，大致介绍一下网络协议方面的知识。

## 1.2 OSI 模型

### 1.2.1 模型

在计算机网络产生之初，每个计算机厂商都有一套自己的网络体系结构的概念，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连（Open Systems Interconnection，简称 OSI）的体系结构，“开放”这个词

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。这个分委员提出了开放系统互联，即 OSI 参考模型，它定义了连接异种计算机的标准框架。OSI 参考模型分为 7 层，分别是物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。各层的主要功能及其相应的数据单位如下：

1. **物理层**(Physical Layer)

大家知道，要传递信息就要利用一些物理媒体，如双纽线、同轴电缆等，但具体的物理媒体并不在 OSI 的 7 层之内，有人把物理媒体当作第 0 层，物理层的任务就是为它的上一层提供一个物理连接，以及它们的机械、电气、功能和过程特性。如规定使用电缆和接头的类型，传送信号的电压等。在这一层，数据还没有被组织，仅作为原始的电流或电气电压处理，单位是比特。

2. **数据链路层**(Data Link Layer)

数据链路层负责在两个相邻结点间的线路上，以帧为单位传送数据。每一帧包括一定数量的数据和一些必要的控制信息。和物理层相似，数据链路层要负责建立、维持和释放数据链路的连接。在传送数据时，如果接收点检测到所传数据中有差错，就要通知发送方重发这一帧。

3. **网络层**(Network Layer)

在计算机网络中进行通信的两个计算机之间可能会经过很多个数据链路，也可能还要经过很多通信子网。网络层的任务就是选择合适的网间路由和交换结点，确保数据及时传送。网络层将数据链路层提供的帧组成数据包，包中装有网络层包头，其中含有逻辑地址信息：源站点和目的站点地址的网络地址。

4. **传输层**(Transport Layer)

该层的任务是根据通信子网的特性最佳地利用网络资源，并以可靠和经济的方式为两个端系统（也就是源站和目的站）的会话层之间提供建立、维护和取消传输连接的功能，负责可靠地传输数据。在这一层，信息的传送单位是报文。

5. **会话层**(Session Layer)

这一层也可以称为会晤层或对话层，在会话层及以上的高层次中，数据传送的单位不再另外命名，统称为报文。会话层不参与具体的传输，它提供包括访问验证和会话管理在内的建立和维护应用之间通信的机制。如服务器验证用户登录便是由会话层完成的。

6. **表示层**(Presentation Layer)

这一层主要解决用户信息的语法表示问题。它将欲交换的数据从适合于某一用户的抽象语法转换为适合于 OSI 系统内部使用的传送语法，即提供格式化的表示层和转换数据服务。数据的压缩和解压缩、加密和解密等工作都由表示层负责。

7. **应用层**(Application Layer)

应用层确定进程之间通信的性质以满足用户需要，以及提供网络与用户应用软件之间的接口服务。

## 1.2.2 OSI 安全服务

为了适应网络技术的发展，国际标准化组织的计算机专业委员会根据开放系统互联参考模型 OSI 制定了一个网络安全体系结构，包括安全服务和安全机制。该模型主要解决对网络信息系统中的安全与保密问题。针对网络系统受到的威胁，OSI 安全体系结构要求的安全服务如下所述。

1. **对等实体鉴别服务**

这种服务是在两个开放系统同等层中的实体建立连接和数据传送期间，为提供连接实体身份的鉴别而规定的一种服务。这种服务防止假冒或重放以前的连接，即防止伪造连接初始化这种类型的攻击。这种鉴别服务可以是单向的也可以是双向的。

2. **访问控制服务**

这种服务可以防止未经授权的用户非法使用系统资源。这种服务不仅可以提供给单个用户，也可以提供给封闭的用户组中的所有用户。

3. **数据保密服务**

这种服务的目的是保护网络中各系统之间交换的数据，防止因数据被截获而造成的泄密。包括以下内容：

(1) 连接保密

对某个连接上的所有用户数据提供保密。

(2) 无连接保密

对一个无连接的数据包的所有用户数据提供保密。

(3) 选择字段保密

对一个协议数据单元中的用户数据的一些经选择的字段提供保密。

(4) 信息流安全

对可能从观察信息流就能推导出的信息提供保密。

4. **数据完整性服务**

这种服务用来防止非法实体（用户）的主动攻击（如对正在交换的数据进行修改、插入使数据延时以及丢失数据等），以保证数据接收方收到的信息与发送方发送的信息完全一致。具体提供的数据完整性服务有以下 5 种。

(1) 恢复的连接完整性

该服务对一个连接上的所有用户数据的完整性提供保障，而且对任何服务数据单元的修改、插入、删除或重放都可使之复原。

(2) 无恢复的连接完整性

该服务除了不具备恢复功能之外，其余同前。

(3) 选择字段的连接完整性

该服务提供在连接上传送的选择字段的完整性，并能确定所选字段是否已被修改、插入、删除或重放。

(4) 连接完整性

该服务提供单个无连接的数据单元的完整性，能确定收到的数据单元是否已被修改。

(5) 选择字段无连接完整性

该服务提供单个无连接数据单元中各个选择字段的完整性，能确定选择字段是否被修改。

**5. 数据源鉴别服务**

这是某一层向上一层提供的服务，它用来确保数据是由合法实体发出的，它为上一层提供对数据源的对等实体进行鉴别，以防假冒。

**6. 禁止否认服务**

这种服务用来防止发送数据方发送数据后否认自己发送过数据，或接收方接收数据后否认自己收到过数据。该服务由以下两种服务组成（这两种服务实际是一种数字签名服务）：

(1) 不得否认发送

这种服务向数据接收者提供数据源的证据，从而可防止发送者否认发送过这个数据。

(2) 不得否认接收

这种服务向数据发送者提供数据已交付给接收者的证据，因而接收者事后不能否认曾收到此数据。

## 1.3 TCP/IP 概貌

TCP/IP 和 OSI 模型一样也是一个协议的分层集合。首先看一个例子——E-mail。首先，有一个 E-mail（POP3、SMTP）的协议。它定义了从一台计算机向另一台计算机发送邮件的命令集合，即指定谁是信息的发送者、谁是接受者以及信息的内容。该协议假定已经存在一条在两台计算机之间通信的可靠通道。和其他应用协议一样，E-mail 协议简单定义了一个命令集以及要发送的内容。它被设计为和 TCP / IP 一起使用。TCP 保证命令被发送到另外一端，它跟踪要发送的东西，并在发送失败时重发信息。如果信息的内容（邮件长度）太长了，大于一个数据包的长度，TCP 会把它们拆成几个数据包分别发送，并保证它们能够正确到达。因为这些函数在许多应用中都能用到，它们被打包成一个单独的协议，而不是作为 E-mail 协议的一部分。从编程的角度看，可以认为 TCP 协议是一个函数库，调用它们可以和另一台计

算机进行可靠的网络通信。与此类似，TCP 又要调用 IP 提供的服务。尽管很多应用都使用 TCP 提供的服务，也有一些应用不需要它。可是，也存在一些每个应用都需要的服务。它们就被一起放进 IP 协议之中。像 TCP 一样，可以认为 IP 是一个 TCP 要调用的函数库，当然，其他未用到 TCP 的协议也可以直接调用它。这种构造几个不同层次的协议的策略被成为“分层”。把 TCP、IP 这样的应用程序看作是各个相互独立的“层”，它们都调用位于自己“下面”的那个层提供的服务。

所以，TCP/IP 分成 4 个层：

- 应用层：应用协议如 Mail 协议。
- 运输层：一个为其他应用提供服务的协议，如 TCP。
- 网络层（IP 和路由）提供最基本的服务，把数据包送到目的地。
- 链路层：一个需要处理特定物理传输介质的协议，如以太网或点到点连接。

下面把 TCP/IP 与 OSI 模型进行对比，看看它们之间的联系，如表 1-2 所示。

表 1-2　　TCP/IP 协议和 OSI 模型对比

| OSI 模型 | TCP/IP 协议 |
|---|---|
| 应用层 | 应用层（Telnet、FTP 和 WWW 等） |
| 表示层 | |
| 会话层 | |
| 传输层 | 运输层（TCP/IP 和 UDP） |
| 网络层 | 网络层（IP 和路由） |
| 数据链路层 | 链路层（网卡驱动） |
| 物理层 | |

TCP/IP 是基于“catenet”模型的。该模型假设许多个相互独立的网络通过网关连接在一起。用户可以从网络的任何地方访问其上的计算机和资源。数据包在到达目的地之前通常要经过许多不同的网络。完成此任务的路由工作对用户应该是完全不可见的。

对用户而言，所有需要知道的只是另一个系统的“Internet 地址”。这是一个类似 162.105.25.85 这样的地址。它实际上是一个 32 位二进制数字。但是，它经常被写为 4 个 10 进制数字，每个数字代表地址的 8 位。Internet 文档用“octet”一词表示这样的 8 位数据块，而不用“字节”，因为 TCP/IP 也被其他一些非 8 位字节的计算机（在这些计算机中，1 个字节并非是通常的 8 位）所支持。通常，该地址本身就向你透漏了些如何到达它们的信息。

例如，162.105 是由有关负责机构分配给北京大学的网络号。北京大学使用下一个 octet 来表示哪个校园的以太网。162.105.25 刚好是北大力学系所使的以太网。最后那个 octet 可以用来表示该以太网上 254 个不同的系统。因为 0 和 255 被禁用，原因稍后详述。162.105.25.1 和 162.105.38.1 将分属不同的系统。稍后再详细讨论 Internet 地址的结构。

通常在上网时，用户用名称而不是 Internet 地址来表示一个系统。当指定一个名称，网络软件就去查找数据库，返回它对应的 Internet 地址。TCP/IP 基于无连接技术。信息作为一个“数据包”序列传递。“数据包”是数据集，它作为一个单独的信息发送。这些“数据包”各自独立通过网络。有一些关于建立连接的条文在某些层会被拆分成数据包，这些数据包被网络单独传送。

比如，假设你要传一个 15000 字节的文件。很多网络无法处理这么大的数据包。因此，协议会把它分成 30 个 500 字节大小的数据包，分别传送到网络的另一端，然后再重新组装成