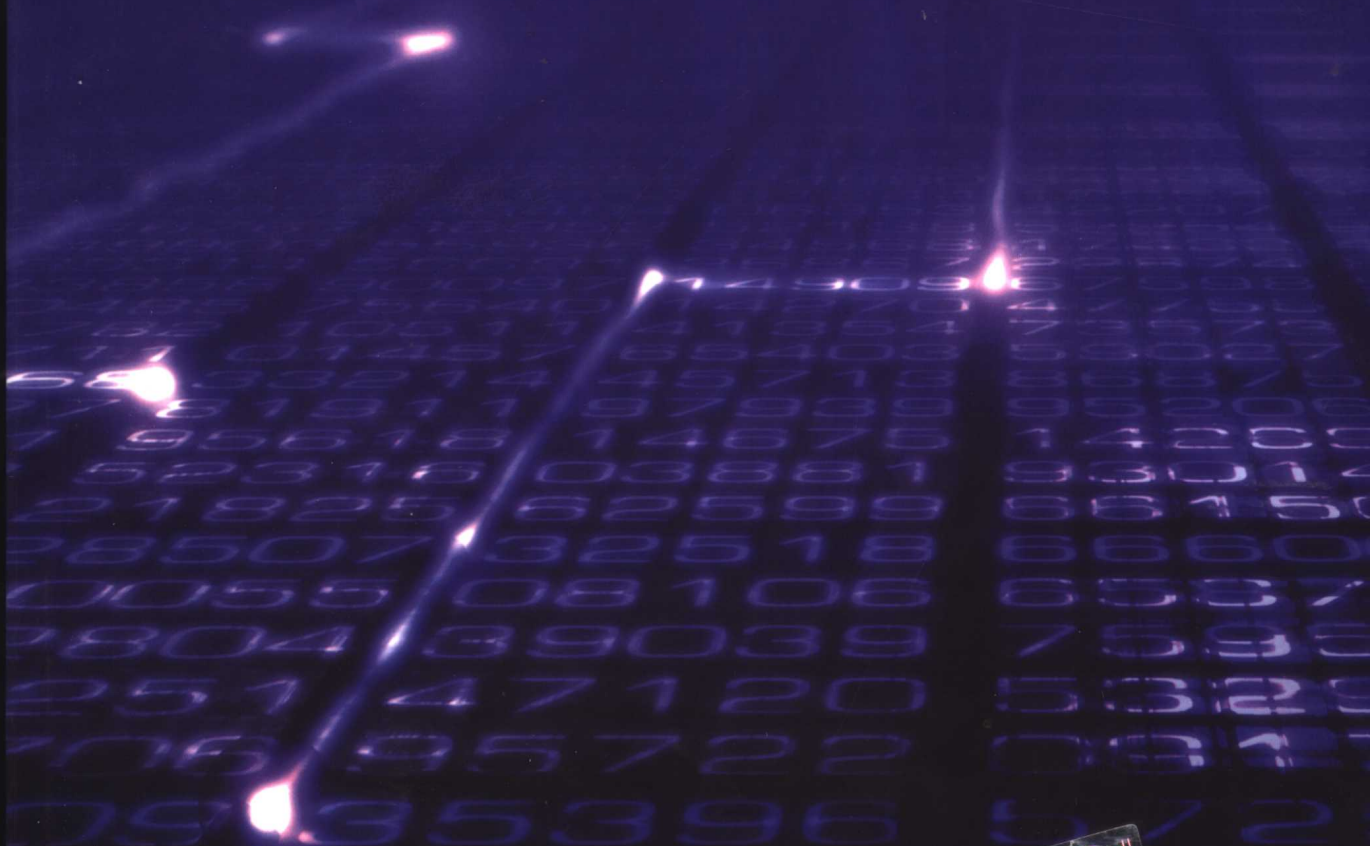
21世纪 高等学校电子信息类专业规划教材

网络安全概论

郑连清 主 编
崔 捷 马哲元 汪胜荣 张串绒 副主编



清华大学出版社
http://www.tup.tsinghua.edu.cn
北京交通大学出版社
http://press.bjtu.edu.cn

21世纪高等学校电子信息类专业规划教材

网络安全概论

郑连清　主编

崔捷　马哲元　汪胜荣　张串绒　副主编

清华大学出版社
北京交通大学出版社

·北京·

内 容 简 介

全书共分为9章及附录A：第1章介绍了网络安全的相关问题，包括网络安全威胁、网络信息对抗、网络安全措施体系；第2章讲述了密码学的主要方法，包括密码学基础知识、密码体制、常用加密算法、数字签名和认证等；第3章讲述了公钥基础设施（PKI）技术及其相关标准和协议；第4章讲述了防火墙技术，包括防火墙的概念、原理、体系结构及关键技术；第5章介绍了网络安全协议：SSL协议、SET协议和IPSec协议，以及虚拟专用网（VPN）技术；第6章介绍了网络安全体系结构、网络安全标准、信息安全测评与认证；第7章分析了电子商务与政务系统的安全问题与解决方案；第8章分析了Windows 2000、UNIX和Linux操作系统的安全漏洞及对策；第9章介绍了系统入侵检测，包括入侵手段、入侵检测技术、入侵检测系统；附录A列出了密码学方法所用到的数学基础知识，包括数论基础、代数基础及计算复杂性理论。此外，每章都附有小结和习题。

图书在版编目（CIP）数据

网络安全概论/郑连清主编. —北京：清华大学出版社；北京交通大学出版社，2004.9
（21世纪高等学校电子信息类专业规划教材）
ISBN 7-81082-403-1

Ⅰ. 网… Ⅱ. 郑… Ⅲ. 计算机网络－安全技术－高等学校－教材 Ⅳ. TP393.08

中国版本图书馆CIP数据核字（2004）第0856246号

责任编辑：张晋民
出 版 者：清华大学出版社　　邮编：100084　　电话：010-62776969
　　北京交通大学出版社　　邮编：100044　　电话：010-51686045，62237564
印 刷 者：北京鑫海金澳胶印有限公司
发 行 者：新华书店总店北京发行所
开　　本：185×260　　印张：14.75　　字数：356千字
版　　次：2004年9月第1版　　2004年9月第1次印刷
书　　号：ISBN 7-81082-403-1/TP·146
印　　数：1～5000册　　定价：20.00元

前　言

计算机网络已经成为人类社会的重要组成部分，无论是在国家经济、政治和军事中，还是在人们的交流、工作和学习中，都发挥着越来越重要的作用。其实，计算机网络已经成为社会财富的重要源泉和社会基础设施的重要组成部分，也自然成为人类竞争和冲突的手段与目标。这是计算机网络面临安全威胁和需要加强安全防护的根本原因。

频繁发生的网络“病毒”破坏、“黑客”入侵窃密和网络金融犯罪等活动，使人们深刻意识到了网络安全威胁的严重性和安全防护的迫切性，网络安全这门科学技术领域中的新兴学科已经成为国家安全战略的重要组成部分和IT行业中新的经济增长点。在这种形势下，为了适应网络安全的教学与研究，我们编写了此书。

本书第1章概括了网络安全的相关问题；第2章讲述了密码学的主要方法；第3章讲述了公钥基础设施（PKI）技术；第4章讲述了防火墙技术；第5章介绍了网络安全协议与虚拟专用网（VPN）技术；第6章介绍了网络安全体系结构与标准；第7章分析了电子商务与政务系统的安全问题与解决方案；第8章分析了操作系统的安全漏洞与防范措施；第9章介绍了网络入侵检测方法；附录A列出了密码学方法所用到的数学基础知识。

第1章、第5章和第8章由郑连清同志编写，第2章和第3章由崔捷同志编写，第4章和第6章由马哲元同志编写，第7章和第9章由汪胜荣同志编写，附录A由张申绒同志编写。

书中难免有不妥或错误之处，望读者批评指正。

作　者

2004年5月

目　录

第 1 章　网络安全问题

本章首先介绍网络安全面临的威胁，包括攻击意图、方法和途径等。了解攻击是搞好防御的基础，第 1.1 节是全书内容的一个基础。第 1.1 节从信息对抗角度，分析网络攻防的实质，以使大家更好地理解网络安全措施的意图和作用。第 1.3 节介绍网络安全措施体系的框架，它全面反映了网络安全所需要的措施。

1.1　网络安全威胁

目前计算机网络面临的威胁很严重，如频繁的黑客（通常指对网络和网络信息进行非授权使用或操作，并侵犯了网络主人或用户利益的人）入侵事件、计算机病毒事件和电子金融盗窃事件等。这些威胁的有关要素如图 1-1 所示。

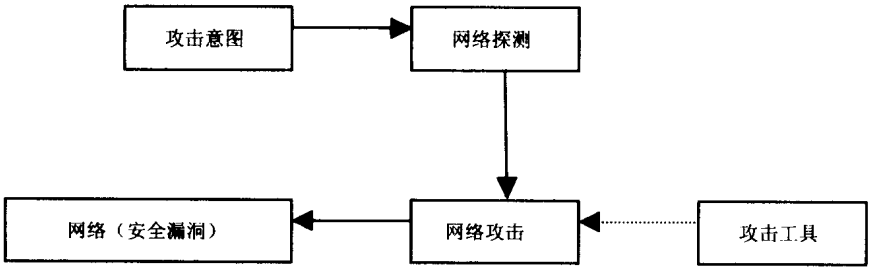


图 1-1　网络安全威胁要素

1.1.1　攻击意图

攻击意图指攻击者的攻击动机，或者说为什么要实施网络攻击。目前，计算机网络已成为社会各个领域的重要手段和财富，通过网络攻击可以达到多方面的意图，如反对领土侵占的政治意图、盗窃电子现金的经济意图、（黑客）满足个人好奇心的兴趣意图、通过系统“捣鬼”（指计算机生产厂商在芯片或软件中预埋可遥制的“后门”或逻辑炸弹等）的网络控制意图等。攻击意图是属于主观领域（非技术领域）的安全威胁要素。

网络安全的人文环境指可以影响网络安全的外界个人、团体或阶层的心理状态、思想道德和文化意识等。这些方面的不利因素，会使一些有恶意的外部人员威胁网络的安全或网上信息的可控性。纵观当前的全球局势，可以说网络安全面临的人文环境是：心理状态千差万别，思想道德各行其道，文化意识层出不穷，价值观念多种多样，个人表现欲望日益强烈，社交手段越来越信息化等。在这些因素的驱使下，网络安全面临着政府组织、生产企业、宗教团体、恐怖分子和黑客进行的网络攻击、系统“捣鬼”、信息泄密、金融诈骗、政治宣传、心理操纵、个性扩张等威胁。

总之，目前网络攻击的意图是多方面的、强烈的，网络安全面临的形势日趋严重。

1.1.2 安全漏洞

目前，没有安全漏洞的计算机网络几乎是不存在的。而正是这些漏洞使得攻击能够成功，从而引起了攻击者的兴趣。安全漏洞是网络攻击的客观原因，主要是属于客观领域内的安全威胁要素，它与许多技术因素有关。

1. 漏洞概念与发现

漏洞是硬件、软件或使用策略上的缺陷。这些缺陷使得网络能够被电脑“黑客”或计算机病毒攻击。每个星期，世界上都会有几十个漏洞产生，它们会影响到很大范围内的网络安全，包括路由器、客户端和服务器软件、操作系统和防火墙等。产生如此多漏洞的原因可以归结为诸如系统越来越复杂而难以检测和IT厂商为市场竞争仓促推出新技术、新产品等。

下面看一个漏洞危害的例子。1995年，有人发现一台行式打印机可以通过缺省的空口令登录到IRIX6.2，并且这个信息在几小时内就发给了“黑客”新闻组。当晚的子夜，一些黑客使用如Web Crawler T和ActaVista这样的搜索引擎来定位一些易受攻击的站点。到第二天早晨，就有几百个主机遭受了破坏。

漏洞是由于系统设计人员、制造人员、检测人员或管理人员的疏忽或过错而隐藏在系统中的。发现漏洞的人主要包括计算机专家、黑客、安全服务商、安全组织、系统管理员和个人用户等。当他们发现一个漏洞时，就根据所处理的事务，把信息发给不同的人。计算机专家和安全服务商组织的成员通常会向安全组织机构发出警告。而黑客也许不会警告任何官方组织，而是在他们之间分发信息。黑客发现新漏洞后会采用新的攻击方法进行网络攻击，新的攻击方法意味着新漏洞的发现，因此黑客是通过网络攻击活动间接发布漏洞信息的。

著名的信息安全组织是计算机紧急事件反应小组（CERT）。CERT是1988年的Morris蠕虫事件后，在美国Carnegie-Mellon大学的软件工程学院成立的。从那时起，CERT已经发布了几百个安全建议。CERT的服务包括：

- 针对新的安全漏洞发布建议；
- 24小时全天候为那些遭受破坏的用户提供重要技术意见；
- 利用它的Web站点提供有用的安全信息；
- 出版年报，让用户深入了解安全统计信息。

然而，在修复漏洞的方法开发出来以前，CERT并不会发布关于“漏洞”的信息。为此，CERT不是一个专门发布漏洞的机构，而是发布针对漏洞和攻击破坏进行完整修复的信息机构。它提供的信息通常包含下载补丁的地址和一些生产厂商正式介绍的信息。从这些站点，用户能够下载可以弥补系统漏洞的代码或工具。

获得CERT建议的方法有几种，包括：

- CERT邮件列表。CERT邮件列表分发CERT建议和公告到每个成员处，通过向certadvisory-request@cert.org发邮件并且在主题行中署上邮件地址，就可以成为邮件列表的成员。

- CERT Web站点。如果不想让自己的邮件用于接收建议，那么可以从CERT的Web站点获取建议。网址是：http://www.cert.org/new/alerts.html。

● CERT FTP 站点。如果不能通过浏览器访问，也可以从 fttp://ftp.cert.org/pub/ 通过 FTP 获得 CERT 建议。

2. 漏洞类型

根据漏洞的载体（网络实体）类型，漏洞可以分为操作系统漏洞、系统工具（如浏览器）漏洞、网络协议漏洞、计算机语言（如 Java 和 ActiveX）漏洞和应用软件漏洞。另外，使用漏洞（指使用硬件和软件方法上的缺陷）也是最主要的一种漏洞。有实验数据表明，80%以上的黑客攻击事件是由于网络管理员或用户对网络安全产品（防火墙、路由器和操作系统）的设置不当造成的。

本书第 8 章将介绍 Windows 2000、UNIX 和 Linux 操作系统中的常见漏洞。

协议漏洞的一个典型例子是 Microsoft 公司的点对点通道协议（Point-to-Point Tunneling Protocol，PPTP）。PPTP 协议用于在 Internet 上建立虚拟专用网（Virtual Private Network，VPN）。VPN 具有安全机制，在 Internet 的两端点之间进行加密传输，这样，就可以减少租用线路。Microsoft 对 PPTP 的实现方式被称为是用户所能得到的最佳安全标准。并且 PPTP 已经获得了不小荣誉。在计算机杂志上，它总是被作为一种工业标准的解决方案。然而，在 1998 年 PPTP 被一个著名的密码专家破译了。这则消息震惊了整个安全界。有评论写到："难道 Microsoft 不能做得更好吗？也许你认为 Microsoft 会的，但 Microsoft 所提供的保密机制任何一个蹩脚的密码'黑客'都能够破译。这种加密机制根本就没有考虑到它的效果。Microsoft 的文档宣称密匙有 128 位长，但实际上并没有使用那么长。并且，由 Hash 函数所保护的口令是如此的脆弱，以致在大多数时候它们很容易被人发现。还有，PPTP 控制通道的方法设计得如此草率，以致每个人都可以造成服务器'胀死'。"研究人员发现了 PPTP 实现方式中的五个缺陷，包括口令杂凑中的漏洞以及验证和加密中的不足等。简而言之，PPTP 的实现方式很糟糕。

使用漏洞的一个典型例子是缺省口令。多数厂家在防火墙、路由器等网络产品中设有默认的用户名和口令，如 Administrator。如网络管理员不把这些产品中的此用户名和口令删除掉，那么攻击者就可能使用它们登录自己所管理的网络。

3. 网络典型结构及安全漏洞

图 1-2 示出了计算机网络的典型结构及安全漏洞（或安全脆弱点）。这些安全漏洞及其原因是：

(1) 不充分的路由器访问控制。配置不当的路由器 ACL 会使得透过 ICMP、IP 和 NetBIOS 发生信息泄露成为可能，从而导致对目标网点 DMZ 上服务器提供的服务进行未授权的访问。

(2) 没有实施安全措施且无人监管的远程访问网点，容易成为攻击者侵入网络的入口。

(3) 不经意的信息泄露给攻击者提供了操作系统和应用程序版本、用户、用户组、共享资源、DNS 信息（通过区域传输做到）以及运行中的服务（如 SNMP）等信息。

(4) 运行非必要的服务（如 FTP 等）的主机提供了进入内部网络的通路。

(5) 工作站级别脆弱的、易于猜中的和重用的口令会给服务器带来入侵厄运。

(6) 具有过度特权的用户账号或测试账号。

(7) 配置不当的 Internet 服务器，特别是 Web 服务器上 CGI 脚本和匿名 FTP。

(8) 配置不当的防火墙或路由器允许直接或在侵害某个 DMZ 上服务器后访问内部系

统。

(9) 没有打过补丁的、过时的、脆弱的或遗留在默认配置状态的软件。

(10) 过度的文件和目录访问控制（NT/95 共享资源、UNIX NFS 出口清单）。

(11) 过度的信任关系（如 NT 的 Domain Trusts）能够给攻击者提供未授权访问敏感信息的能力。

(12) 不加认证的服务，如 Windows XX 等。

(13) 在网络和主机级别不充足的登记、监视和检测能力。

(14) 没有采纳公认的安全策略、规程、指导和最低基线标准。

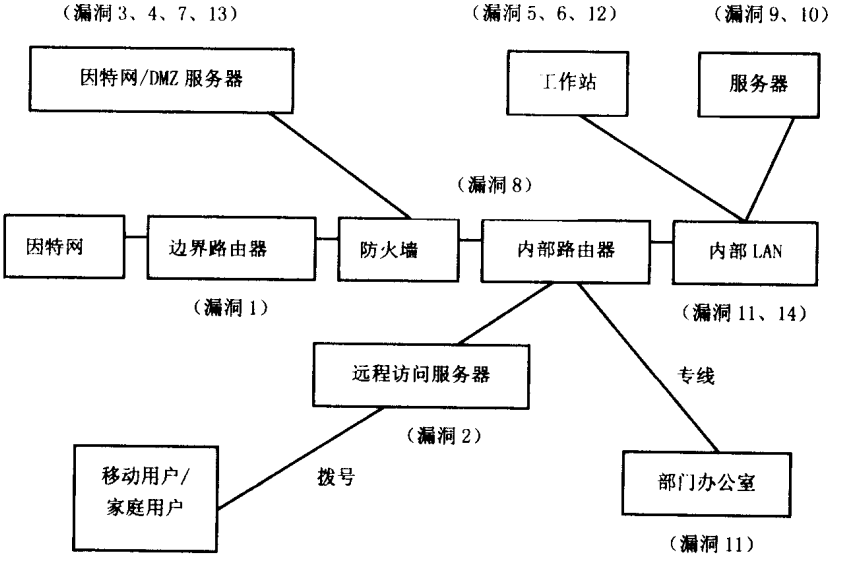


图 1-2　计算机网络的典型结构及安全漏洞

1.1.3　网络探测工具及步骤

网络探测的目的是发现网络的漏洞或脆弱点。它既可以用于攻击目的，也可以用于防御目的。扫描软件和嗅探器是两种典型的探测工具。

1. 扫描软件

扫描软件通过查询 TCP/IP 端口并记录目标的响应信息来工作，如通过探测以下活动和内容收集关于目标主机的有用信息：

- 当前正在进行什么服务？
- 哪些用户拥有这些服务？
- 是否支持匿名登录？
- 是否有某些网络服务需要鉴别？

扫描软件之所以重要，是因为它们能揭示一个网络的脆弱点。在负责任的人手里，可以使一些烦琐的安全审计工作得到简化；在不责任的人手中，会对网络的安全造成威胁。

大多数扫描软件都是强大的工具，它们可以为安全审计收集初步的数据。在这方面应用中，扫描程序如同一杆霰弹猎枪——大范围地快速捕获已知的脆弱点。

SATAN 是一个完善的扫描软件。它不仅可对大多数已知的脆弱点进行扫描，而且一旦

发现脆弱点，就会用指南提醒用户。这些指南详细地说明了脆弱点及如何利用它们、堵住它们。

2. 嗅探器（Sniffer）

嗅探器是能够捕获网络报文的设备，其正当用处是分析网络的流量，以便找出所关心的网络潜在问题。

从安全角度讲，嗅探器可能被黑客用来造成以下比较严重的危害：

- 捕获口令；
- 捕获机密的或者专用的信息；
- 危害邻居网络的安全。

嗅探器工具举例：

- Network Associates 公司的 ATM 嗅探式网络分析器；
- Shomiti 系统公司的 Century LAN 分析器。

3. 口令攻击软件

口令攻击软件是用来对加密的口令进行解密并使得口令显露出来的程序。

Crack 是一个攻击 UNIX 网络相对脆弱的口令的工具。

4. 网络探测步骤

网络探测过程一般可以分为 3 个阶段：

(1) 踩点：发现有攻击价值和可能性的组织的网点，即网络攻击目标。分析拨号上网的电话号码、网络 IP 地址和域名等，是踩点的基本方法。

(2) 扫描：探测进入目标网络的途径或入口。扫描软件、嗅探器和口令攻击软件都是扫描工具。

(3) 查点：查找系统中可攻击的薄弱环节或有价值的资源。

1.1.4　主要的网络攻击方法

网络攻击是指利用目标计算机网络系统的安全缺陷，为窃取、修改、伪造或破坏信息及降低、破坏网络使用效能而采取的各种措施和行动。网络攻击所涉及的技术和手段很多，主要有：

1. 拒绝服务攻击

拒绝服务(DoS) 攻击是指攻击者通过向目标系统建立大量的连接请求，阻塞通信信道、延缓网络传输，挤占目标机器的服务缓冲区，以致目标计算机疲于应付，直至瘫痪。

一般的 DoS 攻击的基本过程：首先攻击者向服务器发送众多的带有虚假地址的请求，服务器发送回复信息后等待回传信息，由于地址是伪造的，所以服务器一直等不到回传的消息，分配给这次请求的资源就始终没有被释放。当服务器等待一定的时间后，连接会因超时而被切断，攻击者会再度传送新的一批请求。在这种不断反复发送伪地址请求的情况下，服务器的 CPU 时间、内存等资源最终会被耗尽。

为增加攻击的成功率，实际攻击中多采用分布式拒绝服务攻击（DDoS），也就是同时操控多台计算机同时对目标实施攻击。2000 年 2 月 7 日至 9 日，美国著名的 Yahoo!、eBay、CNN 等网站相继遭到不明身份的黑客分布式拒绝服务攻击，导致网站瘫痪，服务中断，引起了各国政府和企业界的极大关注。

2. 入侵攻击

入侵攻击是指攻击者利用操作系统内在缺陷或者对方使用的程序语言本身所具有的安全隐患等，非法进入本地或者远程主机系统，获得一定的操作权限，进而窃取信息、删除文件、埋设后门、甚至瘫痪目标系统等行为，这种入侵行为相对难度较高。

入侵攻击建立在对目标系统的漏洞和薄弱环节掌握的基础上，最经常用的技术手段是利用目标机器的缓冲区溢出漏洞，远程控制具有一定权限程序的流程，从而跳转到事先设计的侵权代码上，最终远程获得系统的控制权。

3. 病毒攻击

计算机病毒一般指专门用来破坏计算机正常工作的特殊程序，它隐藏在计算机资源中，能够自我复制、传播和侵入到其他程序中去，并篡改正常运行的程序，损害这些程序的有效功能。随着计算机网络技术的发展,计算机病毒的范畴有了扩展，除了一般意义的病毒外,广义上的病毒还包括木马、后门、逻辑炸弹、蠕虫等有害代码或恶意逻辑。

4. 邮件攻击

传统的邮件炸弹大多只是简单的向邮箱内扔去大量的垃圾邮件，从而充满邮箱，大量地占用了系统的可用空间和资源，使机器暂时无法正常工作。

由于邮件在网络上都是透明传输的，可能经过不同的网络，并由那些网络上的路由器和邮件服务器转发，才能到达目的计算机，因此对基于这种运行机制的邮件系统可以实施多种攻击，如：对邮件服务器攻击、修改或丢失邮件、否认邮件来源等。

此外，邮件攻击一旦和其他攻击方法结合起来，则其威力就大大增加了。例如，通过邮件传播病毒、埋设木马等，常常使邮件接收者不知不觉成了攻击者的协同方，不仅仅是本机安全受威胁，更使得攻击者可以利用这些受控制的机器完成诸如 DDoS 等攻击。事实上很多病毒的广泛传播是通过电子邮件传播的，如“I love you”病毒、“中国 1 号”病毒等就是典型的例子。

5. 诱饵攻击

诱饵攻击指通过建立诱饵网站，当用户浏览网页时，便会遭到不同形式的攻击。利用在页面上嵌套 Javascript 技术，可以使浏览者在浏览时执行特定的命令，比如删除系统文件等。通过在正常应用程序中嵌入木马，当浏览者下载并运行正常的应用程序时，木马将在毫无察觉的情况下种植到浏览者的计算机上。这些手段都需要浏览者无意中的参与，不同于其他主动攻击方式，因此又称为被动攻击。

1.1.5 网络攻击工具

攻击工具能够扰乱计算机系统的正常工作、导致系统拒绝服务、破坏系统的数据或在系统内造成安全隐患等。

1. 电子邮件炸弹

电子邮件炸弹往电子邮箱里发送大量的邮件垃圾，以扰乱系统的正常工作或导致系统拒绝服务。

电子邮件炸弹程序包能够自动用电子邮件炸弹攻击别人的系统。最常用的电子邮件炸弹程序包有 Up Yours、The Windows E-mail Bomber 和 UNIX Mailbomber 等。

2. 蠕虫和细菌

蠕虫和细菌的机理是类似的，只不过蠕虫是在网络上传播的，而细菌是在单机上传播

的。它们扰乱系统的正常工作或导致系统拒绝服务。

蠕虫是一段自主独立的程序，它通过爆炸性的自我复制方式在计算机网络上传播，从而影响系统的可用性。形象地说，蠕虫能像癌细胞一样，一个分裂成两个，两个分裂成四个……

与计算机病毒不同的是，蠕虫是一类能通过在通信网络上完全复制自己来进行扩散的独立程序，它不感染或破坏其他程序。如果将计算机病毒比作恶性肿瘤的话，那么蠕虫就像一种良性肿瘤。

3. 计算机病毒

与 Internet 相关的是，病毒在 Internet 安全中代表了一种特殊的安全威胁。这是因为，当病毒被释放到网络环境时，它的扩散能力无法预测，并且没有其他的环境能比 Internet 更适合于病毒活动。

目前已经发现的病毒有几万种，并且还在以每月 500 种以上的速度飞速发展。大多数病毒是针对 DOS 和 Windows 环境的，而不能感染运行 Digital 公司的 VMS、UNIX 和大型机操作系统及 Macintosh 的计算机平台。这主要是因为，PC 在全世界普遍使用，微软的操作系统容易得到、学习和操作，因而也容易被有针对性地侵入。总体来说，UNIX 和大型机系统价格高，操作系统的安全性好，一般人不易访问和掌握它们，因此只有少数病毒能侵害它们。但是，它们对病毒同样不具免疫力。

病毒一般由 4 个部分组成：

(1) 安装部分：负责病毒的组装、联结和初始化工作。

(2) 触发部分：由触发条件构成。

(3) 感染部分：将病毒程序传染到别的可执行程序上。

(4) 破坏部分：实现病毒编制者的破坏意图。

病毒的危害性特点包括：隐蔽性、感染性（繁殖）、潜伏性和破坏性。

病毒发作时可进行如下破坏活动：

(1) 减少存储器的可用空间；

(2) 使用无效的指令串与正常运行程序争夺 CPU 时间；

(3) 破坏系统中的文件或数据；

(4) 造成机器不能启动或死机；

(5) 破坏显示、打印等 I/O 功能；

(6) 破坏系统硬件，如 CIH 病毒；等等。

4. 特洛伊木马

特洛伊木马（程序）是隐藏着恶意代码的程序。这些程序表面是合法的，能为用户提供所期望的功能，但其中的恶意代码会执行不为用户所知的破坏功能。它与病毒的区别是，特洛伊木马不感染其他文件，而且破坏行为隐蔽，一般很难被用户察觉，因而也很难发现它的存在。

为了准确地理解特洛伊木马的含义，有必要了解一下“特洛伊木马”（Trojan Horse）一词的来历。在公元前 12 世纪，特洛伊王子劫持了 Sparta 女王为妻，为此希腊军队和特洛伊交战了 10 年，但他们的努力全部白费了，因为特洛伊城太坚固了，攻不进去。后来，足智多谋的奥德塞做了一匹巨大的空心木马，放在特洛伊城外。当奥德塞和许多希腊英雄

藏在木马肚子里后，全体希腊将士则假装撤退，隐蔽在附近。而特洛伊人以为希腊人已经撤退，就把木马当成战利品拖进城内。结果到了半夜，在特洛伊人好梦正酣时，藏在木马肚子里的希腊人爬了出来，发出暗号，里应外合杀进城内，取得了胜利。

特洛伊木马的关键是采用有效的潜伏机制来执行非授权的功能。大多数情况下，特洛伊木马以不可读格式隐藏在二进制代码文件里。它在被发现以前，可以潜伏几周或几个月。它执行的非授权功能包括在目标平台传输病毒或蠕虫、设置后门、删除数据等。它与病毒不同，无感染和复制机制。

目前，Internet 上比较流行的“BO”（Back Orifice）工具就是一个典型的特洛伊木马。它自称是个远程 Windows 9X 管理工具，但其中包含一个 boseve.exe 的可执行程序，只要运行了这个程序，就等于在该计算机上为攻击者开了一个后门。该程序在开机后自动调入内存并在后台运行，攻击者则可以通过这个后门方便地浏览、复制甚至删除该计算机上的所有文件。更有助于理解特洛伊木马的例子是，Bosniffer 软件自称是反“BO”工具，实际上它本身就是伪装的“BO”。

5. 逻辑炸弹

逻辑炸弹是蓄意隐藏在系统中的、可在特定指令或时间等条件触发下进行破坏的恶意代码。例如，1996 年 5 月，上海某寻呼台工程师因待遇问题离开该台，临行前在寻呼系统程序中安置了逻辑炸弹。该程序于 7 月 1 日发作，致使该台计算机系统主、备份程序和数据库资料均遭彻底破坏。逻辑炸弹与病毒的区别是它不感染其他文件，或者说不繁殖；与特洛伊木马的区别是，特洛伊木马通常伪装在有诱惑力的软件中，由用户自己不经意地装入自己的系统中，它进行的破坏是秘密的、长期的，一般不易被发觉，而逻辑炸弹通常是由程序开发员、管理员或系统供应商直接蓄意埋入到用户的系统中的，它的发作是爆炸式的，往往一次发作就能被用户发觉。

6. 后门

后门是指存在于目标系统（或用户的系统）上的、可提供非法访问目标系统机制的口令和程序等。比如，网络供应商提供的网络设备的默认口令就是最简单的后门，因为若这些默认口令不被用户删除或修改，“黑客”就可以用这些口令轻易地侵入用户的系统。如今，黑客可利用许多网络工具如 Netcat，在防护薄弱的系统上设置后门（暗通道或反向通道），并通过它来入侵系统。

以上几种工具有时也被笼统地称为“病毒”。

1.1.6　网络入侵攻击步骤

网络入侵攻击的途径和步骤可以用图 1-3 所示的模型来表示。从刺探、渗透、用户访问、根目录访问、捕获直到侵害，其入侵深度不断加强，如用户访问表明入侵者得到了一般用户的对网络资源的操作权限，而根目录访问表明入侵者得到了网络管理员的对网络资源的操作权限。图中的轰炸拨号指通过连续地扫描某些范围内的电话号码，来发现拨号上网的用户。