e时代自由软件系列

Linux 防火墙技术探秘

博嘉科技　主编

国防工业出版社

·北京·

内 容 简 介

本书结合对 Linux 网络源代码的分析，深入地讨论了 Linux 最新内核稳定版本（Linux2.4 内核）中实现的防火墙功能。

本书主要介绍防火墙的预备知识，防火墙的基本原理，最新的防火墙技术（如连线跟踪、动态包过滤、源 NAT 以及目的 NAT 等），防火墙的配置和策略，防火墙功能模块的设计，与防火墙相关的知识（如入侵检测系统、防火墙数据加密技术、防火墙体系结构等），与阅读 Linux 源代码以及编写防火墙模块相关的数据结构和系统调用，以及列出的防火墙加密算法的源代码和目前市面上比较有影响的防火墙厂商的防火墙产品。

本书集原理和实例为一体，可作为信息安全和 Linux 防火墙源代码的实用指南，也可作为从事防火墙研究和技术开发人员理想的参考资料。

图书在版编目(CIP)数据

Linux 防火墙技术探秘/博嘉科技主编. —北京：国防工业出版社，2002.10
（e 时代自由软件系列）
ISBN 7-118-02829-0

Ⅰ.L... Ⅱ.博... Ⅲ.Linux 操作系统-安全技术 Ⅳ.TP316.81

中国版本图书馆 CIP 数据核字(2001)第 012018 号

国防工业出版社出版发行
（北京市海淀区紫竹院南路 23 号）
（邮政编码 100044）
北京奥隆印刷厂印刷
新华书店经售
*
开本 787×1092 1/16 印张 28½ 659 千字
2002 年 10 月第 1 版 2002 年 10 月北京第 1 次印刷
印数：1－4000 册 定价：38.00 元

前　言

随着计算机技术的快速发展，网络应用已经在全球得以推广，人类已经进入了网络时代。电子邮件、远程教育、远程医疗、电子商务等，使人类充分享受到了计算机及其网络带来的无穷乐趣，体验到了高科技的无穷魅力。网络已经成为人们日常生活中不可缺少的一部分，并在国民经济中发挥着日益重要的作用。然而，网络安全也同时成为人们日益关注且必须解决的问题。

网络上的黑客、商业间谍出于各种目的，对人们在网络上所传输的信息表示出了极大的兴趣。这些信息在没有被加密的情况下传输，是很容易被"窃听"的。这些信息如果是重要的、有价值的，就可能对用户造成无法挽回的损失。

几乎所有的用户都知道计算机病毒，也了解病毒的危害。曾经遭遇过计算机病毒的用户可能如今想起还心有余悸。病毒是可怕的，它会干扰人们的工作、破坏资料、甚至会造成计算机系统的瘫痪。但是，这还不是网络安全的全部。计算机安全是一个很广泛的话题，其中防火墙技术就是实现计算机安全的一种非常重要的技术。

防火墙作为一种网络或系统之间强制实行的访问控制机制，是确保网络安全的重要手段。目前社会上各种商业防火墙产品非常多，有基于通用操作系统设计的防火墙，也有基于专用操作系统设计的防火墙。由于 Linux 源代码的开放性，以及编写 Linux 内核源代码的高手很多就是黑客。所以，Linux 成为研究防火墙技术的一个很好的平台。又因为它是完全免费的(可以自由拷贝和下载)，不涉及到版权问题，所以 Linux 已经成为很多防火墙厂商不错的选择。

Linux 系统包含了建立 Internet 网络环境所有服务的软件包，如 Apache Web 服务器、DNS、Mail 服务器、防火墙、Database 服务器等软件包。同时随着 Linux 系统的不断完善以及新技术的不断涌现，Linux 自身也具有了很多新特性，如 IPv6、Proxy(代理)、IP Masquerading(伪装)、IP Port Forwarding(端口转发)等。本书的主要内容就是讨论 Linux 防火墙技术，这些技术包括连线跟踪、包过滤、IP 伪装、地址转换、包处理、防火墙数据加密技术，以及入侵检测系统等的基本原理及其实现过程，并结合这些原理和实现过程讨论了防火墙策略以及如何设计防火墙功能模块。

本书主要内容

本书由 11 章和两个附录构成。第 1 章根据 TCP/IP 网络参考模型概述目前所应用的一些网络安全技术。第 2 章介绍了黑客常用的攻击手段，在本章中讨论计算机病毒和一些黑客常用的攻击工具，如：特洛依木马、一些扫描器等。第 3 章介绍 Linux 防火墙的一些必备知识，主要介绍 Linux 2.4 内核的一些新特性、如何下载和升级 Linux 内核、如何下载和安装 Linux 2.4 内核防火墙的套件 netfilter 及其配置工具 iptables，接着介绍

Linux 的系统结构、makefile 文件，最后简单介绍 Linux 的 Shell 编程技巧。第 4 章介绍了 Linux 从内核 2.0 版本到 2.4 版本所实现的防火墙功能，从中也可以看出防火墙技术的发展进程。因为 Linux 防火墙功能是向下兼容的，所以 2.4 内核版本也包括 2.0 版本和 2.2 版本的防火墙功能，本章最后介绍了 2.4 版本的防火墙新功能。第 5 章介绍了 Linux 2.2 版本的配置工具 ipchains 以及 Linux 2.4 版本的配置工具 iptables，并介绍了配置防火墙的一些通用规则。第 6 章详细介绍了模块的原理以及如何编写 Linux 防火墙模块，其中包括在 Linux 2.2 内核和 Linux 2.4 内核中实现的简单实例。第 7 章介绍了入侵检测系统以及在 Linux 中的一些入侵检测系统套件如 LIDS、OpenWall 等。第 8 章介绍了现在比较流行的防火墙结构以及构建防火墙结构的具体实例。第 9 章介绍了防火墙的数据加密技术，讨论了对称型加密、非对称型加密以及单向散列函数，其中对称型加密讨论了 DES 加密算法、非对称型加密讨论了 RSA 算法、单向散列函数讨论了 MD5 和 SHA 算法，这些算法的 C 语言实现源代码列在附录 A 中。第 10 章介绍了 Linux 2.4 内核中的网络数据结构，同时分类介绍了用于防火墙的数据结构。第 11 章列出了 Linux 2.4 内核中一些主要的系统调用，介绍了这些系统调用的功能和参数，在编写防火墙功能模块时将用到这些系统调用。附录 A 给出了第 9 章介绍的加密算法的源代码。附录 B 介绍了目前市面上比较有影响的防火墙厂商的产品。

特点

内容新颖：本书是基于 Linux 最新的 2.4 内核版本进行介绍的，其防火墙套件 netfilter 也是最新实现的防火墙功能套件。该防火墙套件实现了最新提出的防火墙技术，如状态检测、包处理、动态包过滤、目的地址转换等。

涉及面广：本书除了介绍防火墙的原理和策略外，还介绍了很多相关的知识。如黑客常用攻击手段的原理和防御方法，入侵检测系统的原理和特点，防火墙数据加密技术等。

原理性强：本书是一本原理性极强的书，作者在介绍 Linux 防火墙时通过分析 Linux 的源代码来让读者深入地了解其工作原理；在介绍黑客常用攻击手段时也是从这些攻击手段的工作原理入手，并逐一进行剖析；在介绍入侵检测系统以及防火墙数据加密技术时，主要介绍其工作原理。

实例充分：本书除原理性极强外，也为读者提供了丰富的实例。在介绍防火墙的策略时，提供了很多相关的脚本供读者参考；在介绍防火墙模块编程时为读者提供了一个完整的模块；在介绍防火墙体系结构时也提供了多个实例供读者参考。

适用对象

本书要求读者对 C 语言以及 TCP/IP 协议有一定了解，适合于对 Linux 操作系统和网络安全技术感兴趣的读者。

编写分工

编者在写这本书的时候得到了王刚等朋友的无私帮助，在此对他们表示深深的谢意。特别要感谢的是王松老师，感谢他做的协调工作，使本书能在较短的时间内以较高的质量面向读者。

本书由张恒汝编著。另外，参与编写的其他成员有：贺宗玲、柏祝、张越、王译、佘磊、王伟、王依中、杜强、李加佳、宋志泉、王强、姚砺、卢德凉、宋海、马莉、焦君、刘磊、冯冰、耿素素、吕万军、肖定一、代智、刘果、唐莺、郭燕、袁兆军、赵子灵、柳过、张洋、缪世和、杜希京、田红、孙忠、刘小伟、邓勇、欧阳劲、张云勇、卢军、唐寅、邹思轶等，在此一并致谢。

对于本书，虽然我们都全力以赴进行编写，但个人的学识、能力毕竟有限，如果发现了书中的谬误，欢迎通过各种方式指正批评并提出宝贵意见和建议。若有意见或建议，欢迎联系：◆电话：(028)5404228 ◆ E - mail:bojiakeji@163.net◆通信地址：四川大学西区建筑学院成都博嘉科技资讯有限公司，邮编：610065。

编　者

目　录

第1章　网络安全技术概述

本章导读：

本章概述性地介绍了网络安全的基本概念、基本需求和基本技术以及网络的体系结构。通过本章的学习读者可以了解到防火墙技术、网络的基本体系结构、网络安全的基本概念以及网络安全管理策略等。

1.1　防火墙技术

防火墙被用来保护计算机网络免受非授权人员的骚扰与黑客的入侵。这些防火墙尤如一道护栏隔在被保护的内部网与不安全的非信任网络之间。人们目前广泛使用的互联网便是世界上最大的不安全网，近年来媒体报导的很多黑客入侵事件都是通过互联网进行攻击的。

防火墙是一个或一组实施访问控制策略的系统。它在内部网络(专用网络)与外部网络(功用网络)之间形成一道安全保护屏障，防止非法用户访问内部网络上的资源和非法向外传递内部信息，同时也防止这类非法和恶意的网络行为导致内部网络运行遭到破坏。建立防火墙的目的就是通过各种控制手段保护一个网络不受来自另一个网络的攻击。它可以实施比较广泛的安全策略来控制信息流，防止不可预料的入侵破坏。防火墙结构可以采用双宿主主机结构、主机过滤结构、子网过滤等多种结构。

防火墙可以是非常简单的过滤器，也可以是精心配置的网关，但它们的原理是一样的，都是监测并过滤所有内部网和外部网之间的信息。防火墙保护着内部网络敏感的数据使其不至被偷窃和破坏，并记录内外通信的状态信息日志，如通信发生的时间和进行的操作等。

基于路由器的防火墙向用户化、通用系统化发展。防火墙技术和产品随着网络攻击和安全防护手段的发展而演进，并将网关与安全系统合二为一。目前防火墙主要运用的新技术包括透明网关技术、多级过滤技术、网络地址转换技术、Internet 网关技术，安全服务器网络技术等。

防火墙是目前最为流行也是使用最为广泛的一种网络安全技术。在构建安全网络环境的过程中，防火墙作为第一道安全防线，正受到越来越多用户的关注。防火墙是一个系统，主要用来执行两个网络之间的访问控制策略。它可为各类企业网络提供必要的访问控制，又不至成为网络的瓶颈，并通过安全策略控制进出系统的数据，保护企业的关键资源。

通常一个公司在购买网络安全设备时，总是把防火墙放在首位。那么，防火墙是如何保证网络系统的安全，又如何实现自身安全的呢？

防火墙并不是真正的墙，它是一类防范措施的总称，是一种有效的网络安全模型，是系统总体安全策略的一部分。它阻挡的是对内、对外的非法访问和不安全数据的传递。

在 Internet 上，通过它隔离风险区域(即 Internet 或有一定风险的网络)与安全区域(内部网)的连接，增强内部网络的安全性。防火墙可以作为不同网络或网络安全域之间信息的出入口，能根据企业的安全策略控制出入网络的信息流，且本身具有较强的抗攻击能力。它是提供信息安全服务，实现网络和信息安全的基础设施。在逻辑上，防火墙是一个分离器、限制器、也是一个分析器，有效地监控了内部网和 Internet 之间的任何活动，保证了内部网络的安全。

新一代的防火墙甚至可以阻止内部人员将敏感数据向外传输。企业在把公司的局域网联入 Internet 时，肯定不希望让全世界的人随意翻阅公司内部的工资单、个人资料或是客户数据库。即使在公司内部，同样也存在这种数据非法存取的可能性。例如一些对公司不满的员工可能会修改工资表和财务报告。而在设置了防火墙以后，就可以对网络数据的流动实现有效的管理：允许公司内部员工使用电子邮件、进行 Web 浏览以及文件传输等服务，但不允许外界随意访问公司内部的计算机，同样还可以限制公司中不同部门之间互相访问。将局域网络放置于防火墙之后可以有效阻止来自外界的攻击。

防火墙负责管理风险区域和内部网络之间的访问。在没有防火墙时，内部网络上的每个节点都暴露给风险区域上的其他主机，极易受到攻击。也就是说，内部网络的安全性要由每一个主机来决定，并且整个内部网络的安全性等于其中防护能力最弱的系统的安全性。由此可见，对于连接到 Internet 的内部网络一定要选用适当的防火墙。

通常应用防火墙的目的有：限制他人进入内部网络；过滤掉不安全的服务和非法用户；防止入侵者接近防御设施；限定人们访问特殊站点；为监视局域网安全提供方便。一个成功的防火墙产品应该具有下述基本功能：

- 防火墙的设计策略应遵循安全防范的基本原则——“除非明确允许，否则就禁止”。
- 防火墙本身支持安全策略。
- 如果组织机构的安全策略发生改变，可以加入新的服务。
- 有先进的认证手段或有挂钩程序，可以安装先进的认证方法。
- 如果需要，可运用过滤技术允许和禁止服务。
- 可以使用 FTP 和 telnet 等服务代理，以便先进的认证手段可以被安装和运行在防火墙上。
- 拥有界面友好、易于编程的 IP 过滤语言，并可以根据数据包的性质进行包过滤。数据包的性质有目标和源 IP 地址、协议类型、源和目的 TCP/UDP 端口、TCP 包的 ACK 位、出站和入站网络接口等。

如果用户需要 NNTP(网络消息传输协议)、XWindow、HTTP 和 Gopher 等服务，防火墙应该包含相应的代理服务程序。防火墙也应具有集中邮件的功能以减少 SMTP 服务器和外界服务器的直接连接，并可以集中处理整个站点的电子邮件。防火墙应允许公众对站点的访问，把信息服务器和其他内部服务器分开。

1.2 网络安全的本质与基本需求

由于计算机网络最重要的资源是它向用户提供的服务及其拥有的信息。所以，计算

机网络安全可定义为：保障服务的可用性（Availability）和信息的完整性（Integrity）。前者要求向所有用户有选择地提供应得到的服务，后者则要求保障信息的完整性、准确性。

网络安全的主要威胁包括非授权访问、信息泄露或丢失、破坏数据完整性、破坏通信规程和协议、拒绝合法服务请求、设置陷阱和重传攻击等。要保证信息安全就必须想办法在一定程度上克服各种威胁，采取安全技术策略，确保信息系统的安全。

安全需求包括五个方面，即数据的保密性、完整性、可用性、可控性以及不可否认性。安全工作通过采用合适的安全技术与安全管理措施提供安全需求的保证。网络安全的主要内容包括保护网络系统中的硬件、软件及其数据不受偶然或者恶意的破坏、更改、泄露，保障系统连续可靠地正常运行以及网络服务不中断。

1.3 网络分层安全体系结构

计算机网络是具有层次结构的系统，网络安全也具有相应的层次结构。在基于国际标准化组织(ISO)的 OSI 开放系统互联参考模型中，网络安全贯穿于整个 7 层模型，各层有不同的安全需求和不同的解决方案。针对网络系统实际运行的 TCP/IP 协议模型，网络安全贯穿于信息系统的 4 个层次。

国际标准化组织的计算机专业委员会(ISO/IEC JTCI/SC21)根据网络开放系统互联 7 层模型(OSI/RM)制定了一个网络安全体系结构，用来解决网络系统中的信息安全问题。各层对安全的需求如表 1-1 所示。

表 1-1 网络安全层次及安全需求

网络层次 / 安全服务	物理层	数据链路层	网络层	传输层	会话层	表示层	应用层
对等实体鉴别			◆	◆			◆
访问控制	◆	◆	◆	◆			◆
连接保密	◆	◆	◆	◆		◆	◆
选择字段保密						◆	◆
报文流安全	◆		◆				◆
数据的完整性			◆	◆			◆
数据源鉴别							◆
禁止否认服务							◆

物理层：保证物理层信息安全，主要是防止对物理通路的损坏、对物理通道的窃听和对物理通路的攻击干扰等。

数据链路层：需要保证通过网络链路传送的数据不被窃听。主要采用划分 VLAN(虚网)、加密通信(远程网)等手段。

网络层：需要保证网络只给授权的客户享受授权的服务，保证网络路由正确，避免被拦截或监听。网络层的安全性问题核心在于网络是否得到控制，目标网站通过对来源 IP

进行分析，便能够初步判断来自这一 IP 的数据是否安全，是否会对本网络系统造成危害，以及来自这一 IP 的用户是否有权使用本网络的数据。一旦发现某些数据来自不可信任的 IP 地址，系统便会自动将这些数据阻挡在系统之外。并且大多数系统能够自动记录那些曾经造成过危害的 IP 地址，使它们的数据无法造成第二次危害。

应用层：应用层使用应用平台提供的安全服务来保证基本安全，如采用通信内容安全保护、通信双方的认证、审计等手段。

1.4 网络安全管理策略

网络安全管理所要做的是确定网络资源的安全职责划分。当制定安全策略时，需要首先确定的最重要原则是：准许访问除明确拒绝以外的全部服务，还是拒绝访问明确准许以外的所有服务，一般选择后者作为总的原则。前者由于用户可能使用不安全的服务而危及网络安全，只有在网络的实验阶段才可采用。总的原则确定后还应考虑以下几点：

- 将系统资源分类，确定需保护的资源及保护级别。规定可以访问资源的实体和能够执行的动作。
- 根据企业的实际需要确定内部网的服务类型，规定内部用户和外部用户能够使用的服务种类。
- 规定审计功能，记录用户的活动及资源使用情况。

1.5 网络安全的基本措施

不同环境和应用中的网络安全各有不同的含义和侧重点，相应的安全措施也各不相同。常用的安全措施包括防火墙、身份认证、数据加密、数字签名、安全监控等。

- 防火墙

防火墙对于网络安全是必不可少的。它是位于两个网络之间的屏障，主要功能就是控制对受保护网络的非法往返访问。它通过监视、限制、更改通过网络的数据流，一方面尽可能屏蔽内部网的拓扑结构，另一方面对内屏蔽外部危险站点，用以防范内、外部的非法访问。

- 身份认证

身份认证是实现网络安全的重要机制之一。在安全的网络通信中，涉及的通信各方必须通过某种形式的身份验证机制来证明他们的身份，验证用户的身份与所宣称的是否一致，然后才能实现对于不同用户的访问控制和记录。

- 数据加密

加密是通过对信息的重新组合使得只有收发双方才能解码还原信息的传统方法。数据加密技术在网络安全方案中得到广泛应用，它不需要特殊的拓扑结构的支持，对网络服务及开放性影响较小。

- 数字签名

这种方法主要用于防止非法伪造、假冒并篡改信息。从概念上讲，数字签名就是用信息发送者的专用密钥进行加密，而签名的验证就是用其公钥进行解密，信息被验证后证明其在发送期间未被篡改，发送者被验证后表明他就是合法的发送者。

- 安全监控

高效的网络安全性关键因素之一就是安全监控。监控网络安全性的方法就是检查网络中的各个系统的文件和登录情况。

第 2 章　黑客常用攻击手段

本章导读：

本章主要介绍了黑客在攻击目标时所使用的一些分析工具和破坏工具。读者通过本章的学习，可以了解到这些黑客工具的基本原理和一般的防御措施。这些黑客工具主要有：病毒、拒绝服务攻击、密码破解、欺骗攻击、网络监听、扫描器、特洛依木马等。本章主要分析这些工具的基本原理。

2.1　黑客历史

人们在谈论计算机的时候，一提到“黑客”这个词，首先想到的就是网络破坏者。事实上，“黑客”分为两类，一类就是人们常见到的“黑客”，这些人并不是攻击者，而是创造者，有着过人的才能和乐此不倦的创造欲，是真正的电脑程序员。而另一类就是“骇客”，这些人以攻击别人为乐，怀有极强的破坏欲望。由于人们通常的习惯，所以在此仍然以“黑客”来泛指那些以电脑为生，以发现系统漏洞为乐的计算机程序员。下面简单介绍黑客的来历及其发展的历史。

最早的黑客可以追溯到 19 世纪 70 年代的几个青少年，这些青少年用破坏新注册的电话系统的行为挑战权威。20 世纪 60 年代初，装备有巨型计算机的大学成立了计算机相关科系并建立了计算机网络，比如麻省理工大学（MIT）的人工智能实验室。黑客们就开始利用这些计算机及其网络来施展自己的拳脚。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，来实现自己意图的计算机高手，没有任何贬义。

从 1969 年起，随着 ARPANET 的组建，这群人在电脑技术上不断有重大的突破和贡献。ARPANET 是第一个横跨美国的高速网络，由美国国防部出资兴建，从一个实验性质的数据通信网络，逐渐成为联系各大学、国防部以及研究机构的大型网络。ARPANET 所构建的信息高速公路，使得全世界的黑客可以聚在一起，不再像以前那样孤立地工作，而是形成了一股强大的合力。

20 世纪 70 年代初，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是“伯克利蓝”（Steve Jobs），另一个绰号是“橡树皮”（Steve Wozniak），这两个人后来创建了苹果公司。

在 1975 年出现了第一部 PC 机，其后苹果公司在 1977 年成立，成立不久就取得了很快的发展速度。PC 的潜力吸引了很多年轻的黑客。这些黑客最初最喜欢的编程语言是 BASIC，但这种语言过于简单。

随着黑客的发展，其引起的破坏作用也引起了美国联邦调查局的注意，于是美国联邦调查局开始逮捕犯罪的黑客。从那时候开始，黑客的意义在某种程度上也发生了一些变

化。在最初的几起黑客案中,名为 Milwaukee-based 414s 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,被侵入对象包括纪念 Sloan-Kettering 癌症中心甚至洛斯阿莫斯国家实验室。

针对这些黑客犯罪,美国政府颁布了新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。

随着微软的崛起,一个新的黑客时代也随之来临。20 世纪 80 年代,随着工业化进程的推进,在技术方面,黑客们越来越多地把精力放到寻找各种各样的系统漏洞上,并通过暴露网络系统中的缺陷、非法更改服务器的行为来达到表现自我、反对权威的目的。

随着黑客技术的发展,一些反黑客技术以及法律法规也在不断发展。例如美国在 20 世纪 80 年代末新颁布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,该小组的任务是调查日益增长的计算机网络犯罪。

随着信息技术的高度发展,黑客出现了很多新的特征。黑客已经不再是单兵作战了,他们变得越来越组织化、集团化。黑客之间信息交往更加频繁,整体水平也越来越高,黑客们利用各自的不同特长进行合作攻击,世界上也因此诞生了很多的黑客组织。

由于受利益的驱动,现代黑客也越来越商业化,很多黑客已经把掌握和使用黑客技术作为自己谋生的手段。这些人受雇于各种网络安全公司,为这些互联网公司提供较为有效的安全防护手段。

现代黑客也不断地受到政治的影响,因为网络在人们生活中越来越重要和普遍,网络安全越来越重要,信息战、网络战在一个国家的国防中起着越来越重要的作用。

总之,黑客的行为由历史背景及特征所决定,包括病毒的创造。20 世纪 60 年代,黑客们利用一些技术破坏计算机网络的使用。70 年代因为美国的特殊背景,黑客们提出了计算机应该为人民所用的口号,这些黑客是计算机史上的英雄。到了 80 年代,PC 已经很便宜了,美国与欧洲的经济得到了长足的发展,黑客们开始为信息共享而奋斗。当时美苏争霸,黑客们认为应该使两国处于平衡状态,任何一个国家都不能过分强大,否则就会给新的和平带来威胁。于是积极联络各国,把通过黑客技术拿到的资料卖给各国。一方面自己获得了经济收入,另一方面也认为这样做有助于世界和平,为世界和平作出了贡献。90 年代可以说是黑客的灾难和混乱时期,作为信息共享的产物,Internet 一方面为人们的日常生活提供了极大的便利;另一方面,由于使用的人多了,技术也不再专有,越来越多的人都掌握了这些技术,导致了黑客的概念与行为都发生了很大的变化。

2.2 计算机病毒

2.2.1 概述

计算机病毒与人们生活中所熟悉的生物病毒有着很多相似之处,也有很多不同,从机理上来说,计算机病毒是一个程序,一段可执行代码。但计算机病毒具有和生物病毒一样的特征,就是有独特的复制能力,可以很快地蔓延,而且常常难以根除。这些计算机病毒附着在各种类型的文件上,随着文件的复制,在用户之间传播。