Information

全国高职高专应用型规划教材

信息技术类

计算机网络安全技术

宋西军　主编

北京大学出版社
PEKING UNIVERSITY PRESS

计算机网络安全技术

宋西军　主　编
汪　洋　张照枫　吴梅梅　副主编

北京大学出版社
PEKING UNIVERSITY PRESS

内 容 简 介

计算机网络安全主要包括数据的传输安全和数据的存储安全两大方面，其保障技术涉及计算机科学、计算机网络、计算机通信、密码技术等多方面的知识。

本书主要内容包括计算机网络安全的概况、常见的网络攻击技术、防火墙技术、VPN 技术、公钥基础结构（PKI）技术、入侵检测系统与入侵防御系统、数据安全、网络操作系统的安全性、计算机病毒及其防范 9 个部分。

本书涵盖了常见的计算机网络安全的实现技术，在内容安排上遵循“实用、够用”的原则，将理论知识和实践技能掌握有机结合，并在 Windows 平台和 Linux 平台上给出了应用项目实现的步骤。全书内容难度适中，实用性强。

本书可作为高职高专院校信息安全技术、计算机网络技术等专业的教材使用，也可作为信息安全管理人员、网络工程技术人员、网络管理人员的参考用书。

图书在版编目(CIP)数据

计算机网络安全技术/宋西军主编. —北京：北京大学出版社，2009.8

（全国高职高专应用型规划教材·信息技术类）

ISBN 978-7-301-15399-4

Ⅰ. 计… Ⅱ. 宋… Ⅲ. 计算机网络—安全技术—高等学校：技术学校—教材 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2009）第 101430 号

书　　名：计算机网络安全技术
著作责任者：宋西军　主编
策 划 编 辑：傅　莉
责 任 编 辑：邱　懿
标 准 书 号：ISBN 978-7-301-15399-4/TP·1024
出 版 者：北京大学出版社
地　　址：北京市海淀区成府路 205 号　100871
网　　址：http://www.pup.cn
电　　话：邮购部 62752015　发行部 62750672　编辑部 62765126　出版部 62754962
电 子 信 箱：xxjs@pup.pku.edu.cn
印 刷 者：北京飞达印刷有限责任公司
发 行 者：北京大学出版社
经 销 者：新华书店
787 毫米×980 毫米　16 开本　19.5 印张　474 千字
2009 年 8 月第 1 版　2009 年 8 月第 1 次印刷
定　　价：35.00 元

前言

PREFACE

随着全球信息高速公路的建设和发展，个人、企业乃至整个社会对信息技术的依赖程度越来越大，越来越多的企业将经营的各种业务建立在 Internet/Intranet 环境中。一旦网络系统安全受到严重威胁，不仅会对个人、企业造成不可避免的损失，严重时将会给企业、社会乃至整个国家带来巨大的经济损失。因此，提高对网络安全重要性的认识，增强网络安全防范意识，强化网络安全防范措施，不仅是各个企业组织要重视的问题，也是保证信息产业持续稳定发展的重要保证和前提条件。

本书共 9 章，比较全面地介绍了计算机网络安全涉及的各个方面的技术。第 1 章概述了计算机网络安全技术；第 2 章介绍了进行网络攻击的常用技术；第 3 章介绍了防火墙的基本概念、分类及防火墙的应用实例；第 4 章介绍了 VPN 技术的基本概念与分类，对各种 VPN 实现的技术原理进行了简单比较，并讲解了基于 Windows Server 2003 平台的 VPN 连接的实现；第 5 章介绍了公钥基础结构（PKI）技术，并基于 Windows Server 2003 讲解了密钥证书的管理实现；第 6 章介绍了入侵检测系统与入侵防御系统；第 7 章介绍了数据安全，对实现数据完整性的方法给出了详细的介绍，包括在线技术、备份、归档、分级存储管理、容灾技术和方案等；第 8 章介绍了流行的网络操作系统的安全性实现；第 9 章介绍了计算机常见的病毒及其防范方法。

本书充分体现了以职业需求为导向，以培养职业能力和创新能力为中心的教学思路，内容选用计算机网络安全领域经常用到的技术，通俗易懂，突出实用。

本书由宋西军主编并编写第 1、4、7 章，汪洋编写第 2、3 章，吴梅梅编写第 5、6 章，张照枫编写第 8、9 章。

计算机网络安全技术是一个不断发展的课题，因此编者经验不足和知识不够全面也在情理之中，又因时间仓促，书中难免不足之处。在此恳请同行专家及读者提出批评意见，以便及时补充和修订。

编　者

2009 年 8 月

目　录

第 1 章　计算机网络安全概述

随着计算机和网络技术的迅猛发展和广泛普及，越来越多的企业将经营的各种业务建立在 Internet/Intranet 环境中。于是，支持 E-mail、文件共享、即时消息传送的消息和协作服务器成为当今商业社会中的极重要的 IT 基础设施。然而，大部分企业在充分体会到了互联网的好处的时候，却较少关心网络互联带来的风险。

据报道，现在全世界平均每 20 秒就发生一次计算机网络入侵事件，而全球每年因网络安全问题造成的经济损失也达数千亿美金。现在，人们日常使用的软盘、CD、VCD、DVD 都可能携带恶性代码；E-mail、上网浏览、软件下载以及即时通讯都可能被黑客利用而受到攻击；一台新计算机在连接到网上不到 15 分种即可能被扫描到。所以人们所处的网络环境已没有值得信任的了。

金陵晚报 2009 年 5 月 4 日报道：雇用黑客编写木马程序，再将其挂在网上兜售，用于窃取游戏玩家的账号和密码。由一伙分工明确、制销一条龙的犯罪团伙组成的“木马帝国”，在不到一年的时间内侵入全国数万用户的计算机系统，从中牟利 200 多万元。此案曾一度引发了全国网民的关注，被公安部列为重点挂牌督办大案。

随着全球信息高速公路的建设和发展，个人、企业乃至整个社会对信息技术的依赖程度越来越大，一旦网络系统安全受到严重威胁，不仅会对个人、企业造成不可避免的损失，严重时将会给企业、社会乃至整个国家带来巨大的经济损失。因此，提高对网络安全重要性的认识，增强防范意识，强化防范措施，不仅是各个企业组织要重视的问题，也是保证信息产业持续稳定发展的重要保证和前提条件。

1.1　计算机网络安全的含义

1.1.1　什么是网络安全

从本质上来讲，网络安全就是网络上的信息安全，是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。网络安全涉及的内容既有技术方面的问题，也有管理方面的问题，两方面相互补充，缺一不可。技术方面主要侧重于如何防范外部非法攻击，管理方面则侧重于内部人为因素的管理。如何更有效地保护重要的信息数据、提高计算机网络系统的安全性已经成为所有计算机网络应用必须考虑和必须解决的一个重要问题。

1.1.2　网络安全的特征

网络安全一般包括以下 5 个基本特征。

（1）机密性：确保网络通信信息不会受到未经授权用户或实体的访问。

（2）完整性：确保只有合法用户才能对数据进行修改，即要保证非法用户无法篡改、伪造数据。

（3）可用性：确保合法用户访问时总能从服务方即时得到需要的数据。也就是确保网络节点在受到各种网络攻击时仍能为客户请求提供相应的服务。

（4）可控性：确保可以根据公司的安全策略对信息流向及行为方式进行授权控制。

（5）可审查性：确保在出现网络安全问题后能够提供调查的依据和手段。

1.2 影响计算机网络安全的因素

1.2.1 网络安全的根源

面对层出不穷的网络安全问题，现在的个人或组织一般只是被动的防御，即出现问题后才会在网上找相应的补丁和应对措施，或求助于网络安全公司。这样即使能够解决当前的危机，但也不可避免对个人和组织造成了影响，而且下一次的安全问题也随时都会爆发。所以对于网络安全，为了防范于未然，应首先了解网络安全的根源，然后制定相应的安全策略，做到事前主动防御、事发灵活控制、事后分析追踪。

网络不安全的根源可能存在于下列方面：TCP/IP 协议的安全、操作系统本身的安全、应用程序的安全、物理安全以及人的因素。

1．TCP/IP 协议的安全问题

TCP/IP 协议是进行一切互联网上活动的基础，它使不同的操作系统、不同的硬件设备、以及不同的应用能够在不同的网络环境中进行自由通信。但由于 TCP/IP 协议一开始的实现主要目的是用于科学研究，所以在网络通信的安全性方面考虑得很少，这也适用于当时的网络环境。但当时的开发者没有预料到互联网发展如些迅速，而 TCP/IP 协议也成为了 Internet 网络通信协议的标准和基础。随着 Internet 所具有的开放性、国际性和自由性的逐步体现，TCP/IP 协议由于这种先天不足对网络安全造成的影响也逐步体现出来。所幸的是 TCP/IP 的下一个版本已充分考虑到了这个严重的问题，在 IPv6 内置了 IPSec 等网络安全机制。期待 IPv6 的普及，可以使人们的网络安全得以从根本上解决。

2．操作系统本身存在的安全问题

不管基于桌面的、网络的操作系统，还是基于 UNIX、Windows 以及其他类型操作系统，都不可避免地存在诸多的安全隐患，如非法存取、远程控制、缓冲区溢出以及系统后门等。这从各个操作系统厂商不断发布的安全公告以及系统补丁中可见一二。

3．应用程序本身存在的安全问题

应用程序配置和漏洞问题通常是恶意软件攻击或利用的目标。如攻击者可通过诱使用户打开受感染电子邮件附件以达到攻击系统或使恶意软件在整个网络上传播的目的。而其他如 WWW 服务、即时通讯、FTP 服务以及 DNS 服务等都存在不同程度的安全漏洞，只有通过及时的更新才能防止受到恶意的攻击。

4．物理安全

逻辑上的安全固然重要，但物理的不安全可能导致企业安全策略的失败。物理安全是保护计算机网络设备、设施以及其他媒体免遭地震、水灾、火灾等环境事故以及人为操作失误或错误及各种计算机犯罪行为导致的破坏过程。保证计算机信息系统各种设备的物理安全是整个计算机信息系统安全的前提，也是整个组织安全策略的基本元素。对于足够敏感的数据和一些关键的网络基础设施，可以在物理上和多数公司用户分开，并采用增加的身份验证技术（如智能卡登录、生物验证技术等）控制用户对其物理上的访问，从而减少安全破坏的可能性。

5．人的因素

对于计算机安全，最重要最基本的起点是从涉及计算机的人员开始，即用户、系统管理员以及超级管理员。所以计算机安全最基本的方法也许还是人的因素第一。安全的最大弱点是人们的粗心、疏忽与大意。

因人的因素造成的安全威胁很多，如因无意失误而产生的配置不当、企业由于生存的压力重视生产而疏于安全方面的管理、系统内部人员泄漏机密或外部人员通过非法手段截获企业机密信息等。

1.2.2　网络中潜在的威胁

由于开放性、共享性以及各种新技术、新服务的运用，可以说 Internet 上应用尽有，需要的任何资料只需在搜索引擎中输入关键字就可出现。但在人们享受到 Internet 带来的无穷乐趣的时候，一些别有用心的人也在通过 Internet 这个信息共享通道做起了一些非法的勾当。于是病毒、蠕虫、网络欺诈、黑客攻击等事件越来越多，网络攻击对人们心理造成的影响以及对组织造成的损失也越来越大。

总的来说，网络中存在的潜在威胁主要有内部攻击、社会工程学、组织性攻击、意外的安全破坏以及自动的计算机攻击。

1．内部的攻击

虽然防火墙在企业周边网络建立起了一道安全防线，抵御了绝大多数的外部攻击。但防火墙不是万能的，它解决的只是网络安全周边网络的一部分。据报道，企业面临的各种网络攻击中，来自企业内部的攻击占到 70%～80%。所以机构面临的最大的信息安全威胁更可能是在其办公室内。

据调查结果显示，80%的内部入侵者在对公司发动攻击前，都存在一些不正常或消极的行为，以下是调查得出的一些结果：

- 92%的内部入侵者在工作上遇到过一些不愉快的事情，如降级、调岗，受到警告或被终止合同。
- 在内部攻击中，59%是企业的前雇员或合同工，41%仍然在职。
- 在前雇员中，48%是被开除的，38%是辞职的，7%属于解聘。
- 86%的内部攻击者来自技术部门。其中，系统管理员占 38%，程序员占 21%，工

程师占 13%，另外 14%是 IT 专家。

- 96%的内部入侵者是男性。
- 57%的入侵者在攻击之前被其他人发现情绪不好。
- 主要攻击方式为远程访问。
- 实施内部攻击的主要动机都是为了报复。

由于内部攻击一般具有组织合法用户账号，因此有能力绕过其为了保护网络周边安全设置的物理的和逻辑的控制措施，获得访问大部分基础设施的权限，从而违反了系统制定的信任规则而在该网络中从事恶意的活动，如读取限制的数据、偷窃或者破坏数据。所以在诸多的网络攻击中，内部攻击是最常见，也是对组织网络威胁最大的攻击。

2．社会工程学

社会工程学是利用人性的弱点或其他心理特征（如受害者本能反应、好奇心、信任、粗心大意、贪婪以及同情心、乐于助人等心理）并通过欺骗的方式以获取网络信息的行为。在网络安全技术运用日渐完善的今天，这种攻击方式因其特有的优点而在近年来呈现出迅速上升甚至滥用的趋势。

网络钓鱼是近来社会工程学的代表应用——通常攻击者都是利用向受害者发送垃圾邮件，将受害者引导到一个与某些电子银行网站一模一样的假网站，粗心的用户在输入用户名和口令的时候也就是攻击得逞的时候。

最近出现的鸡尾酒钓鱼术比起网络钓鱼更让人防不胜防。与使用仿冒站点和假链接行骗的网络钓鱼不同，鸡尾酒钓鱼术直接利用真的银行站点行骗，即使是有经验的用户也可能会陷入骗子的陷阱。这种欺骗技术是通过用户点击邮件中包含这种技术的恶意代码的链接登录到真正的网上银行站点时，站点上会出现一个类似登录框的弹出窗口，毫无戒心的用户往往会在这里输入自己的账号和密码，而这些信息就会通过电脑病毒发送到骗子指定的邮箱中。同时由于骗子利用了客户端技术，银行方面也很难发现自己的站点有异常。

3．组织性攻击

随着系统安全保护能力的增强和对网络犯罪惩罚的力度更加严厉，一种更有目的性、破坏力更大的组织性攻击进入了网络犯罪领域。这种攻击一般是由一个犯罪集团组织发起，向商业系统、金融单位、政府部门以及军事机构进行有计划有针对性的攻击。

组织性攻击在战争期间甚至可能会发生在国家之间。2006 年 6 月 28 日以色列为解救一名被绑架的士兵，在加沙发动了猛烈的夏雨行动。让人意想不到的是，虽然以色列的坦克群在加沙几乎没有遇到任何像样的抵抗，但以色列却遭到了来自另一个战场上的密集袭击。据以色列新闻网报道，夏雨行动刚刚启动，以色列国内 750 多个网站立刻遭到了阿拉伯一个名为魔鬼队的计算机黑客组织发起的报复性攻击。该组织对 750 多个以色列公司和组织网站同时发动了大规模密集攻击，报复以军对巴勒斯坦人采取的军事行动，并在瘫痪后的以色列网站首页上打出口号：你们杀死了巴勒斯坦人，我们杀死你们服务商。

组织性攻击一般也会发生在存在竞争的组织之间，为了获取商业或竞争优势，攻击者试图对其他公司的商业机密或它们存储在网络上的其他知识产权进行非授权访问或恶意破坏。

4．意外的安全破坏

意外的安全破坏更多是来源于人的粗心大意或一个规划拙劣的网络。如非故意的授权可能使一个普通用户访问到公司的受限资源。不合适的许可会导致用户无意识地阅读、修改或者删除一些重要数据。所以必须有一个设计周密的安全策略，特别是对用户和组权限的管理和维护需要特别小心。

5．自动的计算机攻击

自动的计算机攻击无须攻击者手动控制，它会自动寻找网络中的弱点进行自动的攻击。如网络病毒、蠕虫以及流氓软件等恶意代码程序。

计算机病毒是攻击者编写的可感染的依附性恶意代码，能够自动寻找并依附于宿主对象，它可以通过软盘、光盘、硬盘等存储介质以及网络进行自动的传播。如在 2004 年出现 WORM_MYDOOM.B 的同型变种病毒，可以通过电子邮件的方式扩散。它的攻击方式为伪装成退信或一般收信常见内容，受害者一旦开启信件或者其所带的附件后，Windows 的“记事本”程序便会自动跳出，而受害者的系统此时便已中毒。同时病毒会自动搜集计算机中的通讯簿，并通过 Email 大量传播。这种病毒危害性较大，不仅会入侵个人计算机窃取私密资料，并能攻陷特定的网站，造成重大的灾情。

蠕虫是攻击者编写的可感染的独立性恶意代码，是一种与计算机病毒相仿的独立程序，可以在计算机系统中繁殖，甚至在内存、磁盘、网络中爬行，但不需要宿主对象。近年来，蠕虫所引发的安全事件此起彼伏，且有愈演愈烈之势。从 2001 年爆发的 CodeRed 蠕虫、Nimda 蠕虫和 SQL 杀手病毒，到 2003 年肆虐的冲击波和 2004 年的震荡波，以及 2006 年横行网络世界的熊猫烧香，无不是蠕虫在作怪。蠕虫病毒会感染目前主流的 WINDOWS 2000/XP/SERVER 2003 系统，如果不及时预防，它们就可能在几天内快速传播、大规模感染网络，对网络安全造成严重危害！

近年来出现的流氓软件是一种不感染的独立性恶意代码。它介于计算机病毒与正规软件两者之间，同时具备正常功能（下载、媒体播放等）和恶意行为（弹广告、开后门），在未明确提示用户或未经用户许可的情况下，在用户计算机或其他终端上安装运行，从而给用户系统带来实质危害和使用上的诸多不便。

现在许多形式的恶意软件嵌入一个电子邮件引擎，以便使得恶意代码利用电子邮件以更快的速度传播，并且避免制造容易被检测到的异常活动。目前，大量的邮件群发器利用受感染系统上的后门来使用这种电子邮件引擎。所以自动的计算机攻击必将愈演愈烈，危害也将越来越大。

1.3　网络攻击的类型

互联网发展至今，除了它表面的繁荣外，也出现了一些不良现象，其中黑客攻击的“木马”技术是最令广大网民头痛的事情，它是计算机网络安全的主要威胁。下面着重分析黑客进行网络攻击的几种常见手法。

1．利用挂马网页进行攻击

用户访问某些网站后，会莫名弹出一大堆网页和广告，严重干扰了正常的电脑使用。经过调查，发现被“挂马”的网站数量呈加速上升态势。用户在浏览不明网站的时候需要谨慎对待，以防中“马”。其中，一种名为 AdWare/Win32.Boran.aj 的广告型木马尤为突出，据监控数据统计，有超过 60%的用户深受其害。

木马传播一般通过“网站挂马”、文件传输、移动介质（如 U 盘）等几种主要方式进行。其中“网站挂马”由于其传播面大、隐蔽性高的特点一直受到木马传播者的青睐。在从 Google 调研全球数以十亿计的网站中抽取的 450 万个网页的分析测试中发现，至少有 45 万个页面中含有恶意脚本，且一直呈上升趋势。Google 也开始在其搜索结果中加上了“不安全网站”的提示。

2．利用网络系统漏洞进行攻击

许多网络系统都存在着这样那样的漏洞，这些漏洞有可能是系统本身所有的，如 WindowsNT、UNIX 等都有数量不等的漏洞，也有可能是由于网管的疏忽而造成的。黑客利用这些漏洞就能完成密码探测、系统入侵等攻击。

对于系统本身的漏洞，可以安装软件补丁；另外网管也需要仔细工作，尽量避免因疏忽而使他人有机可乘。

3．通过电子邮件进行攻击

电子邮件是互联网上运用得十分广泛的一种通讯方式。黑客可以使用一些邮件炸弹软件或 CGI 程序向目的邮箱发送大量内容重复、无用的垃圾邮件，从而使目的邮箱被撑爆而无法使用。当垃圾邮件的发送流量特别大时，还有可能造成邮件系统对于正常的工作反映缓慢，甚至瘫痪，这一点和后面要讲到的拒绝服务攻击（DdoS）比较相似。

对于遭受此类攻击的邮箱，可以使用一些垃圾邮件清除软件来解决，其中常见的有 SpamEater、Spamkiller 等，Outlook 等收信软件同样也能达到此目的。

4．解密攻击

在互联网上，使用密码是最常见并且最重要的安全保护方法，用户时时刻刻都需要输入密码进行身份校验。而现在的密码保护手段大都认密码不认人，只要有密码，系统就会认为你是经过授权的正常用户，因此，取得密码也是黑客进行攻击的一重要手法。取得密码也还有好几种方法，一种是对网络上的数据进行监听。因为系统在进行密码校验时，用户输入的密码需要从用户端传送到服务器端，而黑客就能在两端之间进行数据监听。但一般系统在传送密码时都进行了加密处理，即黑客所得到的数据中不会存在明文的密码，这给黑客进行破解又提了一道难题。这种手法一般运用于局域网，一旦成功，攻击者将会得到很大的操作权益。另一种解密方法就是使用穷举法对已知用户名的密码进行暴力解密。这种解密软件会尝试所有可能字符所组成的密码，但这项工作十分费时，不过如果用户的密码设置得比较简单，如“12345”、“ABC”等，那有可能只需一眨眼的工夫就可搞定。

为了防止受到这种攻击的危害，用户在进行密码设置时一定要将其设置得复杂，也可

使用多层密码，或者变换思路使用中文密码，并且不要以自己的生日和电话甚至用户名作为密码，因为一些密码破解软件可以让破解者输入与被破解用户相关的信息，如生日等，然后对这些数据构成的密码进行优先尝试。另外应该经常更换密码，这样使其被破解的可能性又下降了不少。

5．后门软件攻击

后门软件攻击是互联网上比较多的一种攻击手法。Back Orifice2000、冰河等都是比较著名的特洛伊木马，它们可以非法地取得用户电脑的超级用户级权利，并对其进行完全的控制，除了可以进行文件操作外，同时也可以进行对方桌面抓图、取得密码等操作。这些后门软件分为服务器端和用户端，当黑客进行攻击时，会使用用户端程序登录已安装好服务器端程序的电脑，这些服务器端程序都比较小，一般会附带于某些软件上。有可能在用户下载了一个小游戏并运行时，后门软件的服务器端就安装完成了，而且大部分后门软件的重生能力比较强，给用户进行清除造成一定的麻烦。

当在网上下载数据时，一定要在其运行之前进行病毒扫描，并使用一定的反编译软件，查看来源数据是否有其他可疑的应用程序，从而杜绝这些后门软件。

6．拒绝服务攻击

互联网上许多大网站都遭受过此类攻击。实施拒绝服务攻击（DdoS）的难度比较小，但它的破坏性却很大。它的具体手法就是向目的服务器发送大量的数据包，几乎占取该服务器所有的网络宽带，从而使其无法对正常的服务请求进行处理，而导致网站无法进入、网站响应速度大大降低或服务器瘫痪。现在常见的蠕虫病毒或与其同类的病毒都可以对服务器进行拒绝服务攻击的进攻。它们的繁殖能力极强，一般通过 Microsoft 的 Outlook 软件向众多邮箱发出带有病毒的邮件，而使邮件服务器无法承担如此庞大的数据处理量而瘫痪。

对于个人上网用户而言，也有可能遭到大量数据包的攻击使其无法进行正常的网络操作，所以大家在上网时一定要安装好防火墙软件，同时也可以安装一些能够隐藏 IP 地址的程序，这样能大大降低受到攻击的可能性。

1.4　网络攻击的常见形式

（1）数据驱动攻击：黑客或攻击者把一些具有破坏性的数据藏匿在普通数据中传送到因特网主机上，当这些数据被激活时就会发生数据驱动攻击。例如修改主机中与安全有关的文件，留下下次更容易进入该系统的后门。

（2）报文供给：黑客或攻击者有时利用重定向报文进行攻击。重定向报文可改变路由器，路由器根据这些报文建议主机走另一条“更好”的路径。黑客或攻击者利用重定向报文把连接转向一个黑客或攻击者控制的主机，或使所有报文通过他们控制的主机来转发。

（3）电污染攻击：据有关资料显示，有九成计算机出现的误码、死机、芯片损坏等现象来自“电污染”。究其原因，一是电流在传导过程中会受到诸如电磁、无线电等因素的干扰，形成电子噪声，导致可执行文件或数据文件出错；二是有时由于电流突然回流，造

成短时间内电压急剧升高，出现了电涌现象，这种电涌不断冲击会导致设备元件出现故障。所以恶意攻击者可以利用“电污染”手段损坏或摧毁防火墙。

（4）社会工程攻击：社会工程攻击有时又叫系统管理员失误攻击。黑客或攻击者同公司内部人员套近乎，获取有用信息，尤其在因系统管理人员失误（如 WWW 服务器系统的配置错误）而扩大了普通用户的权限时，就会给黑客或攻击者以可乘之机。

（5）IP 隧道攻击：IP 隧道攻击即在端口 80 发送能产生穿过防火墙的 IP 隧道的程序。如果人们利用因特网加载程序（例如经过因特网加载实音频网关），则可能引入产生 IP 隧道（类似于防火墙中使用的实用网关）的特洛伊木马，造成在因特网和内部网之间的无限 IP 防问。IP 隧道攻击是黑客在实际攻击中已经实现的一种防火墙攻击技术。

（6）基于堡垒主机 Web 服务器的攻击：黑客可以设想把堡垒主机 Web 服务器转变成避开防火墙内外部路由器作用或影响的系统。它也可用于发动针对下一层保护的攻击，观察或破坏防火墙网络内的网络通信量，或者在防火墙只有一个路由器的情况下完全绕过防火墙。这种防火墙技术已被广泛应用并证明有效。

（7）基于附加信息的攻击：基于附加信息的攻击是一种较先进的攻击方法，它使用端口 80（HTTP 端口）传送内部信息给攻击者。这种攻击完全可以通过防火墙实现，因为防火墙允许 HTTP 通过且又没有一套完整的安全办法确定 HTTP 报文和非 HTTP 报文之间的差异。目前有黑客利用这种攻击对付防火墙技术，虽然还不是很广泛。

（8）IP 分段攻击：指采用数据分组分段的办法来处理仅支持给定最大 IP 分组长度的网络部分，一旦被发送，并不立即重新组装单个的分段，而是把它们路由到最终目的地，然后才把它们放在一块给出原始的 IP 分组。除了 IP 头之外，每个分组包含的全部东西就是一个 ID 号和一个分组补偿值。借以清楚地识别各分段及其顺序。因此，被分段的分组是对基于分组过滤防火墙系统的一个威胁，它们把它们的路由判决建立在 TCP 端口号的基础上，因为只有第一个分段标有 TCP 端口号，而没有 TCP 号的分段是不能被滤除的。

（9）IP 地址欺骗：它突破防火墙系统最常用的方法是因特网地址欺骗，它同时也是其他一系列攻击方法的基础。黑客或入侵者利用伪造的 IP 发送地址产生虚假的数据分组，乔装成来自内部站的分组过滤器，这种类型的攻击是非常危险的。

（10）格式化字符串攻击：格式化字符串漏洞同其他许多安全漏洞一样是由于程序员的懒惰造成的。当你正在阅读本文的时候，也许有个程序员正在编写代码，他的任务是：打印输出一个字符串或者把这个串拷贝到某缓冲区内。他可以写出如下的代码：

```
printf("%s", str);
```

但是为了节约时间和提高效率，并在源码中少输入 6 个字节，他会这样写：

```
printf(str);
```

为什么不呢？干嘛要和多余的 printf 参数打交道，干嘛要花时间分解那些愚蠢的格式？printf 的第一个参数无论如何都会输出的！程序员在不知不觉中打开了一个安全漏洞，可以让攻击者控制程序的执行，这就是不能偷懒的原因所在。

为什么程序员写的是错误的呢？他传入了一个他想要逐字打印的字符串。实际上该字

符串被 printf 函数解释为一个格式化字符串（format string）。函数在其中寻找特殊的格式字符比如"%d"。如果碰到格式字符，一个变量的参数值就从堆栈中取出。很明显，攻击者至少可以通过打印出堆栈中的这些值来偷看程序的内存。但是有些事情就不那么明显了，这个简单的错误允许向运行中程序的内存里写入任意值。

（11）COOKIE 欺骗：现在有很多社区网为了方便网友浏览，都使用了 cookie 技术以避免多次输入密码，所以只要对服务器递交给用户的 cookie 进行改写就可以达到欺骗服务程序的目的。按照浏览器的约定，只有来自同一域名的 cookie 才可以读写，而 cookie 只是浏览器的，对通讯协议无影响，所以要进行 cookie 欺骗可以有多种途径：①跳过浏览器，直接对通讯数据改写；②修改浏览器，让浏览器从本地可以读写任意域名 cookie；③使用签名脚本，让浏览器从本地可以读写任意域名 cookie（有安全问题）；④欺骗浏览器，让浏览器获得假的域名。

（12）缓冲区溢出：缓冲区溢出漏洞是指通过往程序的缓冲区写超出其长度的内容，造成缓冲区的溢出，从而破坏程序的堆栈，使程序转而执行其他指令，以达到攻击的目的。

1.5　计算机网络安全层次结构

1.5.1　物理安全

物理安全的类型与解决方案有如下几种。

- 自然灾害（如雷电、地震、火灾等），物理损坏（如硬盘损坏、设备使用寿命到期等），设备故障（如停电、电磁干扰等），意外事故。解决方案是：防护措施，安全制度，数据备份等。
- 电磁泄漏，信息泄漏，干扰他人，受他人干扰，乘机而入（如进入安全进程后半途离开），痕迹泄露（如口令密钥等保管不善）。解决方案是：辐射防护，屏幕口令，隐藏销毁等。
- 操作失误（如删除文件，格式化硬盘，线路拆除等），意外疏漏。解决方案是：状态检测，报警确认，应急恢复等。
- 计算机系统机房环境的安全。特点是：可控性强，损失也大。解决方案是：加强机房管理，运行管理，安全组织和人事管理。

1.5.2　安全控制

微机操作系统的安全控制。如用户开机键入的口令（某些微机主板有“万能口令”），对文件的读写存取的控制（如 Unix 系统的文件属性控制机制）。主要用于保护存贮在硬盘上的信息和数据。

网络接口模块的安全控制。在网络环境下对来自其他机器的网络通信进程进行安全控制。主要包括：身份认证，客户权限设置与判别，审计日志等。

网络互联设备的安全控制。对整个子网内的所有主机的传输信息和运行状态进行安全监测和控制。主要通过网管软件或路由器配置实现。