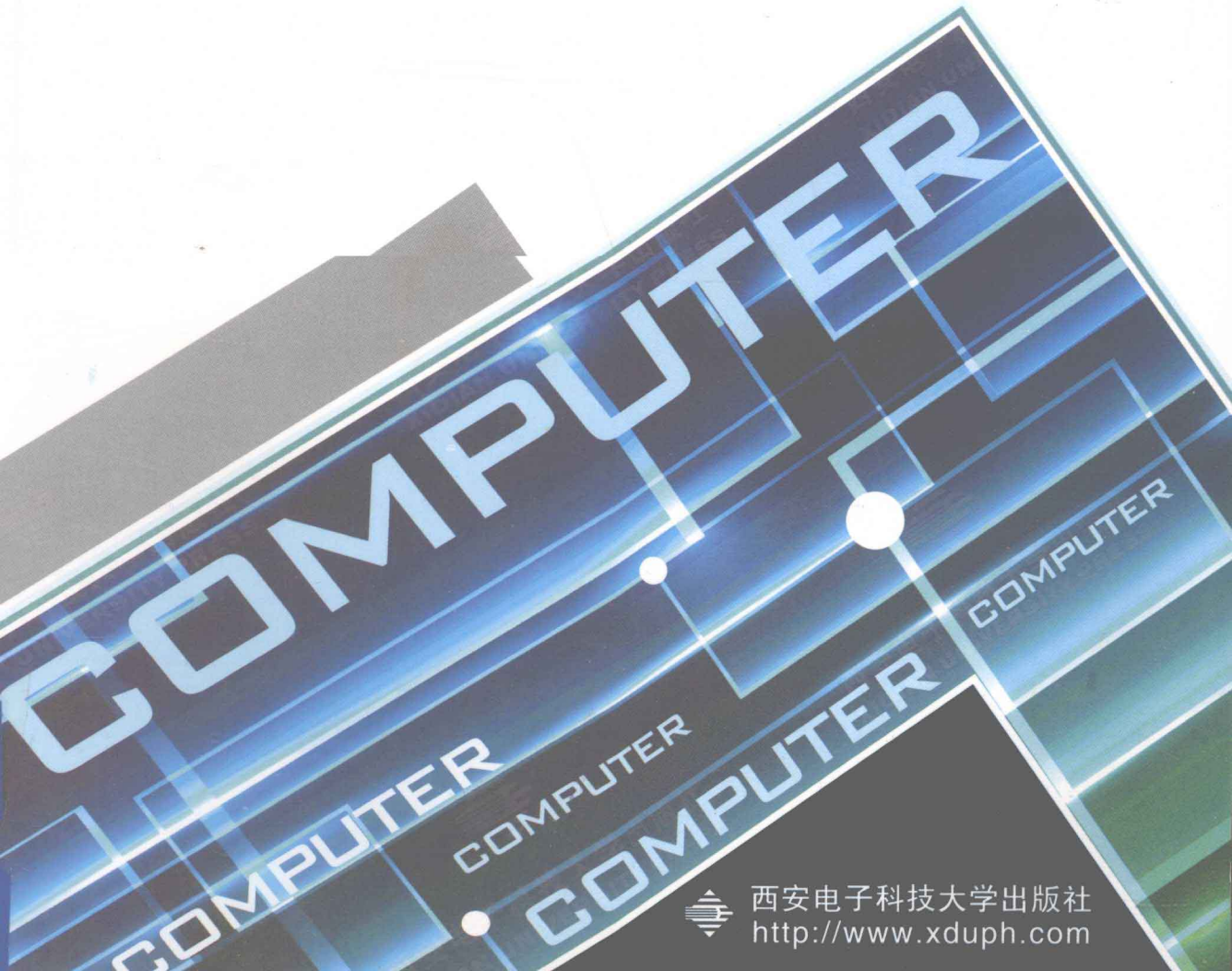
高等学校计算机专业
“十二五”规划教材

信息安全原理与实践教程

马传龙　主编



西安电子科技大学出版社
http://www.xduph.com

高等学校计算机专业“十二五”规划教材

信息安全原理与实践教程

主　编　马传龙

参　编　李　剑　陈　龙　董振兴

蒋文豪　王　练　杨　锋

西安电子科技大学出版社

内 容 简 介

本书从基础知识、系统安全、信息安全、信息安全设备以及网络攻防等方面介绍了信息安全的原理和实验。全书共分5篇13章，包括信息安全概述、信息安全实验平台、Windows系统安全加固、系统安全防御配置、加解密原理及实验、PGP加密电子邮件、数据备份与数据恢复、防火墙原理与配置、计算机取证技术、主动防御系统的配置与使用、端口扫描与网络侦听、网络攻防原理与实验、无线网络与手机安全等。

本书可作为信息安全及相关专业学生的教材，也可作为各企事业单位普通计算机使用者进行信息安全培训的教材，还可供网络安全爱好者及其他相关人员阅读和参考。

图书在版编目（CIP）数据

信息安全原理与实践教程 / 马传龙主编. —西安：西安电子科技大学出版社，2011.10

高等学校计算机专业“十二五”规划教材

ISBN 978-7-5606-2671-0

Ⅰ. ① 信… Ⅱ. ① 马… Ⅲ. ① 信息系统—安全技术—高等学校—教材 Ⅳ. ① TP309

中国版本图书馆CIP数据核字（2011）第177798号

策　　划　陈　婷

责任编辑　杨　柳　陈　婷

出版发行　西安电子科技大学出版社(西安市太白南路2号)

电　　话　(029)88242885　88201467　　邮　　编　710071

网　　址　www.xduph.com　　电子邮箱　xdupfxb001@163.com

经　　销　新华书店

印刷单位　陕西华沐印刷科技有限责任公司

版　　次　2011年10月第1版　2011年10月第1次印刷

开　　本　787毫米×1092毫米　1/16　印　张　15

字　　数　350千字

印　　数　1～3000册

定　　价　26.00元

ISBN 978-7-5606-2671-0/TP • 1302

XDUP 2963001-1

前　言

在互联网高速发展的背后，我们不能忽视互联网安全存在的极大漏洞。期盼互联网增长的不仅有渴望信息的网民，也有心存不善的黑客。屡次发生的网站被攻击事件已经给我们敲响了警钟：“重视互联网安全刻不容缓!”

本书内容全面，分别从基础知识、系统安全、信息安全、信息安全设备以及网络攻防等方面介绍了信息安全的原理和实验。实践是检验真理的唯一标准，本书内容重点在于实验，着重于动手操作能力的培养，具有较强的实践性和可操作性。全书共分 5 篇 13 章，其中，第一篇为基础知识(第 1、2 章)，第二篇为系统安全(第 3、4 章)，第三篇为信息安全(第 5、6、7 章)，第四篇为信息安全设备(第 8、9、10 章)，第五篇为网络攻防(第 11、12、13 章)。

各章具体内容如下：

第 1 章主要介绍信息安全的内涵、现状和发展趋势，并介绍信息安全面临的威胁、信息安全体系结构以及黑客入侵的步骤。

第 2 章主要介绍信息安全实验平台的搭建，使读者能够使用虚拟机工具构建一个网络环境。

第 3 章是 Windows 系统安全加固，主要介绍注册表的配置、帐号和口令的安全设置、文件系统安全设置以及关闭默认共享等实验。

第 4 章是系统安全防御配置，主要介绍 IIS 的基本配置、IIS 的访问限制配置、创建服务器证书和客户端证书映射、微软基本安全评估 MBSA 的使用等。

第 5 章是加解密原理及实验，主要介绍密码学的基础知识、BIOS 的密码设置与破解、Windows 的密码设置与破解、Office 文件密码的设置与破解以及压缩文件密码的设置与破解等。

第 6 章是 PGP 加密电子邮件，主要介绍使用 PGP 保证通信的安全，包括使用 PGP 加解密邮件、创建自解密文档等。

第 7 章是数据备份与数据恢复，主要介绍数据备份与数据恢复的基本概念、Windows 系统备份与恢复、Norton Ghost 备份与恢复和 EasyRecovery 文件恢复等。

第 8 章是防火墙原理与配置，主要介绍防火墙的基本概念、Windows 个人防火墙的配置、易尚防火墙的配置、红墙防火墙的配置等。

第 9 章是计算机取证技术，主要介绍取证技术的基本概念、取证的过程、BitSure Ⅰ现场勘验取证系统的使用、Final Forensics 的使用等。

第 10 章是主动防御系统的配置与使用，主要介绍主动防御的概念、主动防御系统 NAD 的配置与使用、网络安全隔离与文件交换系统 ISM-6000 的使用与配置等。

第 11 章是端口扫描与网络侦听，主要介绍端口扫描与网络侦听的概念、SSS 端口扫描器的使用、网络监听软件 Sniffer 的使用等。

第 12 章是网络攻防原理与实验，主要介绍黑客攻击的步骤、系统漏洞攻防实验、灰鸽

子木马的远程控制实验和利用 ARP 欺骗获取用户名和密码实验等。

第 13 章是无线网络与手机安全，主要介绍无线网络与手机安全的现状、无线网络入侵实验、手机病毒演示和手机蓝牙入侵实验等。

全书由重庆通信学院的马传龙老师主编并统稿，其中第 1～8 章、第 11 章由马传龙编写，第 9 章由重庆邮电大学的陈龙编写，第 10 章由重庆邮电大学的蒋文豪、王练编写，第 12 章由重庆工程职业技术学院的李剑编写，第 13 章由重庆邮电大学的董振兴和重庆君盾科技有限公司的杨锋共同编写。

感谢重庆通信学院的曹龙汉教授及中国信息安全认证中心的张剑博士，他们对本书提出了很多宝贵的建议；感谢中国信息安全认证中心、重庆君盾技术有限公司、重庆爱思网安信息技术有限公司对本书的出版给予的大力帮助。参与本书编写的还有重庆通信学院的杨秀清、高福兵、覃勇、喻石老师和硕士生周超以及重庆邮电大学的硕士生娄晓会、敬凯等，在此对他们一并表示感谢！

由于作者水平有限，书中疏漏及不妥之处在所难免，恳请广大同行和读者批评指正，万分感谢！

严正声明 本书所讨论的技术仅用于研究学习，旨在最大限度地唤醒大家的信息安全意识，提高信息安全防护技能。任何个人、团体、组织不得将其用于非法目的，违法犯罪者必将受到法律的严厉制裁。

编 者

2011 年 5 月

目　录

第一篇　基础知识

第二篇 系 统 安 全

第三篇 信 息 安 全

第四篇 信息安全设备

第五篇 网 络 攻 防

第一篇　基础知识

第 1 章　信息安全概述

1.1　信息安全现状及发展

随着国家信息化战略的推广，信息安全问题凸显出了其重要地位。信息安全问题不仅给国家信息化进程带来现实的挑战，而且基于信息网络的渗透、攻防、电子战等行为，也影响到国防安全，给国与国之间带来新的竞争关系。

1.1.1　信息安全的内涵

信息安全(Information Security，InfoSec)自古以来就是人们关注的问题，但在不同时期，信息安全的侧重点和控制方式有所不同。信息安全指信息的硬件、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，系统能连续、正常、可靠地运行，信息服务不中断。信息安全是一门涉及计算机技术、网络技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

在网络技术飞速发展的信息时代，网络是信息传输的载体，信息依靠网络进行传输，信息安全、网络安全、计算机安全等已没有明确的界限。

信息安全通常强调所谓 CIA 三元组的目标，即保密性、完整性和可用性。它也是信息安全的基本要素和安全建设所应遵循的基本原则。后来，人们对 CIA 进行了扩展，加入了可控性、不可抵赖性等。

(1) 保密性(Confidentiality)——确保信息在存储、使用、传输过程中不会泄露给非授权用户或实体。

(2) 完整性(Integrity)——确保信息在存储、使用、传输过程中不会被非授权用户篡改，防止授权用户或实体不恰当地修改信息，保持信息内部和外部的一致性。

(3) 可用性(Availability)——确保授权用户或实体对信息及资源的正常使用不会被异常拒绝，允许其可靠而及时地访问信息及资源。

(4) 可控性(Controllability)——确保能够监控管理信息和系统，保证信息和信息系统的授权认证和监控管理。

(5) 不可抵赖性(Non-Repudiation)——为信息行为承担责任，保证信息行为人不能否认其信息行为。

1.1.2 信息安全的现状

2010 年全球网络信息安全形势依旧严峻，其间发生的几个重大信息安全事件，如维基解密、震网病毒，以及国内的 3Q 之争等，影响巨大，引起了世界各国的广泛关注。透过这些安全事件所暴露出来的深层安全问题值得我们认真思考和分析。

事件一：维基解密

Wikileaks(维基解密，又译作维基泄密)是一个大型文档泄露及分析网站，成立于 2006 年 12 月，其目的是揭露政府及企业的腐败行为。该网站声称其数据源不可追查亦不被审查。“维基解密”没有总部或传统的基础设施，它仅依靠服务器和数十个国家的支持者。2010 年 7 月 26 日，“维基解密”在《纽约时报》、《卫报》和《镜报》的配合下，在网上公开了多达 9.2 万份的驻阿美军秘密文件，引起轩然大波；10 月 23 日，“维基解密”公布了 391 832 份美军关于伊拉克战争的机密文件；11 月 28 日，维基解密网站又泄露了 25 万份美国驻外使馆发给美国国务院的秘密文件电报。

“维基解密”是美国乃至世界历史上最大规模的一次泄密事件，其波及范围之广，涉及文件之众，均史无前例。该事件引起了世界各国政府对信息安全工作的重视和反思。据美国有线电视新闻网 2010 年 12 月 13 日报道，为防止军事机密泄露，美国军方已下令禁止全军使用 USB 存储器、CD 光盘等移动存储介质。

事件二：震网病毒

震网病毒(Stuxnet)，是世界上首个以直接破坏现实世界中工业基础设施为目标的蠕虫病毒，被称为网络“超级武器”。震网病毒于 2010 年 7 月爆发，截至 2010 年 9 月底，包括中国、印度、俄罗斯在内的许多国家都发现了这种病毒。据统计，目前全球已有约 45 000 个网络被该病毒感染，其中 60%的受害主机位于伊朗境内，并已造成伊朗核电站推迟发电。目前我国也有近 500 万网民以及多个行业的领军企业遭此病毒攻击。

事件三：3Q 之争

2010 年 9 月，奇虎公司针对腾讯公司的 QQ 聊天软件，发布了“360 隐私保护器”和“360 扣扣保镖”两款网络安全软件，并称其可以保护 QQ 用户的隐私及其网络安全。腾讯公司认为奇虎 360 的这一做法严重损害了腾讯的商业利益，称“360 扣扣保镖”是“外挂”行为。随后，腾讯公司于 2010 年 11 月 3 日宣布将停止对装有 360 软件的电脑提供 QQ 服务。由此引发了“360 QQ 大战”，同时引起了 360 软件与其他公司类似产品的一系列纷争，最终演变成为了互联网行业中的一场混战。最终“3Q 之争”在国家相关部门的强力干预下得

以平息，“360 扣扣保镖”被召回，QQ 与 360 恢复兼容。但此次事件对广大终端用户造成的恶劣影响和侵害，以及由此引发的公众对于终端安全和隐私保护的困惑和忧虑却远没有消除。

上述三个典型安全事件均发生在终端，可见终端安全已经成为世界范围内的突出问题，在各国精心构建的信息安全防御体系中，终端安全仍是一个薄弱环节。美国政府历来以防御严密、技术先进著称，尚且发生了维基解密事件，我国在核心技术依赖于国外的情况下，信息安全所面临的严峻形势可想而知，发达国家要使我国的网络信息系统瘫痪或盗窃我国的涉密信息易如反掌。因此，信息安全建设必须走自主之路，而“3Q 之争”又暴露出国内安全厂商和安全产业发展存在的诸多问题，我们的安全意识、技术和管理水平都亟待提高。

1.1.3　信息安全人才培养

尽管创新的科技在很大程度上修补了一些技术上的安全漏洞，然而信息安全中最大的安全漏洞莫过于员工薄弱的安全意识。安全事故很多时候不是因为技术原因造成的，而是人们根本没有认识到信息安全的重要性，以至他们要么忽视安全流程，要么躲避技术控制措施。

我国正大力提倡建立自主创新的科技强国，未来 20 年的科技将处于高速发展的阶段。我国政府也正在积极与各类组织机构合作，规划和建立信息化智能社会，并且通过提供在线视频培训来提高人们的计算机应用水平。普通用户缺乏对信息安全的正确认识是网络犯罪上升的主要原因，因此需要加强对非 IT 人员的计算机安全基础培训。

此外，安全是一项持续的过程，各单位应定期举办各类信息安全意识培训，普及信息安全知识，使更多的非 IT 人士掌握基本的信息安全防护技术，以便能及时维护个人计算机的安全。亡羊补牢，不如未雨绸缪；信息安全，重在防患于未然。

来自教育部的统计资料表明，我国目前具有大学本科以上学历的信息安全人才只有 2100 人左右，具有大专学历的只有 1400 人左右。社会需求与人才供给之间存在着巨大的差距，人才问题已成为当前制约信息安全产业发展的瓶颈。因此，信息安全专业便具有资格证书“硬”、毕业生“少”、需求部门“多”、用人单位“大”、就业前景“广”等就业优势。网络安全和信息安全越来越引起国内外的关注，与此同时信息安全方面的人才需求也会大增。

1.1.4　信息安全展望

针对信息安全现状，在未来的几年中，我们可以做以下工作：

(1) 建立可控的信息交换机制。不同等级网络之间进行数据交换的需求是客观存在的，禁止一切数据交换只会导致“地下”数据交换猖獗，专用 U 盘、光盘、物理隔离都存在安全风险和漏洞。强行“封堵”不如合理“疏导”，建立集中的数据交换渠道，并对交换过程进行全程监控和审计，切实落实信息使用者和管理者的相关责任，才能确保数据安全。

(2) 攻击和窃密是终端安全的外部原因，计算机系统存在缺陷或漏洞、系统配置不当是

终端安全的内部原因。外因通过内因起作用，内因是决定因素，因此，我们应该通过实施终端安全核心配置，对操作系统等系统软件和常用软件进行安全配置，提高系统自身安全性，以减少系统安全漏洞，降低对第三方工具技术的依赖，真正提高终端安全防护的自主性。

(3) 国家应尽快建立政府终端安全保障基础设施。形成从中央到地方多级部署，覆盖全国各级政府部门的终端安全管理应用支撑环境，实现对全国政务终端的统一安全管理和安全状态监测，掌握终端安全态势，提高运行管理效率，以保障国家信息安全。

(4) 国家应加强对信息安全市场的监督管理。应尽快出台有关信息安全、软件行为、信息采集及隐私保护方面的法律法规，规范商业竞争，维护广大用户的合法权益，促进国内安全厂商和信息安全产业的良性发展。

1.2　信息安全面临的常见威胁

每个计算机用户都或多或少地亲身体验过一些网络安全事件。轻则可能使用户的计算机系统运行不正常，重则可以使整个系统中的磁盘数据全盘覆灭，甚至导致磁盘、主板等硬件的损坏。对于个人来说，网络安全事故带来的损失可能还不足以令人重视，但对于企业用户来说，可能会是灭顶之灾。因为这些用户在服务器磁盘中每天都要存储许多非常重要的工作文件和数据库文件，一旦出现网络安全事故，就可能使整个企业网络系统瘫痪，甚至使磁盘系统损坏，其损失往往难以估计。

为了防范这些网络安全事故的发生，每个计算机用户，特别是企业网络用户，必须采取足够的安全防范措施，甚至可以说要在利益均衡情况下不惜一切代价。当然，网络安全策略的实施是一个系统工程，涉及许多方面，既要充分考虑到那些平时我们经常提及的外部网络威胁，又要对来自内部的网络安全隐患有足够的重视。

1.2.1　计算机病毒

计算机病毒的前身只不过是程序员闲来无事编写的趣味程序，后来才发展出了诸如破坏文件、修改系统参数、干扰计算机正常工作等的恶性病毒。病毒的定义比较多，1994 年 2 月 18 日我国正式颁布实施了《中华人民共和国计算机信息系统安全保护条例》(简称《条例》)，在《条例》第二十八条中明确指出：“计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。”此定义具有法律性和权威性。

据中国计算机病毒疫情及互联网安全报告指出，2008 年中国新增计算机病毒、木马的数量呈爆炸式增长，总数量已突破千万。病毒制造的模块化、专业化以及病毒“运营”模式的互联网化成为 2008 年中国计算机病毒发展的三大显著特征。同时，病毒制造者的“逐利性”依旧没有改变，网页挂马、漏洞攻击成为黑客获利的主要渠道，其对抗杀毒软件的特征非常显著。纵观 2008 年的一些流行病毒，如机器狗、磁碟机、AV 终结者等，无一例外均为对抗型病毒，并且一些病毒制作者也曾扬言“饿死杀毒软件”。病毒与杀毒软件对抗主要表现为对抗频率变快、周期变短的特性，各个病毒的新版本更新非常快，一两天甚

至几个小时更新一次来对抗杀毒软件。

计算机病毒发展趋势主要表现在：0Day 漏洞将与日俱增，病毒与反病毒厂商对抗将加剧，新平台上的漏洞也会成为病毒/木马最主要的传播手段。

在病毒制作门槛逐步降低，病毒、木马数量的迅猛增长，反病毒厂商与病毒之间的对抗日益激烈的大环境下，传统“获取样本→特征码分析→更新部署”的杀毒软件运营模式，已无法抵御病毒日益增长及变化的安全威胁；在海量病毒、木马充斥互联网，病毒制作者技术不断更新的大环境下，反病毒厂商必须要有更有效的方法来弥补传统反病毒方式的不足，这时，“云安全”便应运而生。

总而言之，计算机病毒泛滥成灾，对计算机用户的危害性越来越大，它已成为黑客进行破坏的主要工具，并走入了现代信息化战争。计算机病毒更新换代向多元化发展，依赖网络进行传播，其攻击方式多样(邮件、网页、局域网等)，利用系统漏洞成为病毒有力的传播方式，病毒与黑客技术融合在一起，对信息资源起到严重的破坏作用。

1.2.2　木马的危害

木马，又称特洛伊木马(Trojan horse)，其名称取自希腊神话中的特洛伊木马记。计算机世界的特洛伊木马是指隐藏在正常程序中的一段具有特殊功能的恶意代码，它是具备破坏和删除文件、发送密码、记录键盘和攻击等特殊功能的后门程序。

目前，病毒和木马往往结合在一起被黑客利用，所以严格地区分哪些是病毒或者哪些是木马也是比较困难的。

虽然木马程序的攻击手段越来越隐蔽，但是只要加强个人安全防范意识，便可以大大降低“中招”的机率。对此，笔者有如下建议：安装个人防病毒软件、个人防火墙软件；及时安装系统补丁；对不明来历的电子邮件和插件不予理睬；经常浏览安全网站，以便及时了解一些新木马的情况，做到知己知彼，百战不殆。

1.2.3　拒绝服务攻击

拒绝服务(DoS，Denial of Service)攻击自诞生之日起便成为黑客以及网络安全专家关注的焦点。所谓拒绝服务攻击，是指通过欺骗、伪装及其他手段使得提供服务资源的系统出现错误或资源耗尽，从而使系统停止提供服务或资源访问的一种攻击手段。在众多的网络攻击手段中，DoS 攻击已被越来越频繁地提起，其造成的破坏是十分巨大的。

拒绝服务攻击就是想办法让目标机器停止提供服务，其实只要能够对目标造成麻烦，使某些服务被暂停甚至主机死机，都属于拒绝服务攻击。拒绝服务攻击问题一直得不到合理的解决，这是由于网络协议本身的安全缺陷造成的，因此拒绝服务攻击成为攻击者的终极手法。

典型的拒绝服务攻击有两种形式：消耗带宽和消耗资源。在一段时间内，每个网络只能承受来自一定方向的一定网络流量，其大小取决于网络速度、设备性能和设备类型等。拒绝服务攻击占用了全部的网络带宽，这使得网络过于拥挤，正常的数据包无法发送而被网络丢弃，网络的延迟时间增大，网络应用陷入瘫痪状态，这就是消耗带宽的攻击方式。由于网络设备的处理能力是有限的，如果能通过某种方法引起设备对超过其处理能力的数

据包进行响应，就会耗尽网络中的资源，导致系统崩溃，设备无法正常使用，这就是消耗资源的攻击方式。

单一的 DoS 攻击一般采用一对一的方式，随着计算机处理能力的迅速增长和内存的大大增加，同时也出现了千兆级别的网络，使得 DoS 攻击的困难程度加大了。这是由于目标机对恶意攻击包的“消化能力”加强了不少，例如，甲的攻击软件每秒钟可以发送 3000 个攻击包，但乙的主机与网络带宽每秒钟可以处理 10 000 个攻击包，这样一来，甲对乙的攻击就不会产生什么效果。这时，分布式的拒绝服务攻击手段就应运而生了。

分布式拒绝服务(DDoS，Distributed Denial of Service)攻击指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动 DoS 攻击，从而成倍地提高拒绝服务攻击的威力。通常，攻击者将 DDoS 主控程序安装在一个计算机上，设定的时间主控程序将与大量代理程序通信，代理程序已经被安装在 Internet 上的许多计算机中，代理程序收到指令时就发动攻击。利用客户/服务器技术，主控程序能在几秒钟内激活成百上千次代理程序的运行。

DoS 攻击，尤其是 DDoS 攻击很难防范，它对网络危害巨大并难以追查真正的攻击者。要避免系统遭受 DoS 攻击，网络管理员要积极谨慎地维护整个系统，确保无安全隐患和漏洞，而针对更加恶意的攻击方式则需要安装防火墙等安全设备过滤 DoS 攻击，同时建议网络管理员定期查看安全设备的日志，及时发现对系统安全构成威胁的行为。

1.2.4　用户密码被盗和权限的滥用

用户密码被盗和权限的滥用是一个非常严重的安全问题，它可以同时在企业内部和外部网络中发生。有些黑客通过一些木马类的黑客程序就可以盗取一些用户的网络帐号和密码，这样，黑客就可以很轻易地从内部或外部网络中登录进入到企业网络中。如果所盗取的用户帐户权限较高，黑客则可以很轻松地制造出各种网络安全事故，甚至毁坏整个企业网络。

用户帐户和密码的盗取有多种途径。一种是由于用户的大意，在进行网络系统登录，输入帐户名和密码时不小心被他人看见；另一种就是一些用户密码长时间不换，或者换来换去总是几个原密码，这样一些别有用心的人便很容易猜中密码；还有一种是通过远程控制类黑客程序从目标计算机系统中获取，这就是黑客行为；最后一种就是那些非法用户通过各种手段(如穷举法)猜测来获取用户密码，这种方法难度较大，所花时间也较多，一般不会采取。为了预防这种情况发生，建议在网络中采用强密码策略。

1.2.5　网络非法入侵

提起网络非法入侵，有人会立即联想到病毒入侵和黑客攻击，其实这里所说的网络非法入侵主要不单指这方面的。网络非法入侵的方式有多种，如 IP 欺骗、毁损攻击、拒绝服务攻击、邮件洪流攻击、中间人攻击、HTTP 协议攻击和应用层攻击等。这些攻击防不胜防，很难被发现，因为这些攻击通常是采用无连接的 UDP 协议(也有许多是 TCP/IP 类型的)进行的。这类攻击多数是不具有明确目标的，它采取扫描方式寻找主机，只要发现有机可乘，就会实施攻击。

防止这类网络非法入侵的主要安全措施就是架设防火墙。对于个人用户，出于经济成本、性能需求等方面的综合考虑，我们一般选择软件防火墙；对于企业用户来说，建议使用硬件防火墙作为企业内外网的安全屏障。一方面其安全防护能力比软件防火墙更强大，另一方面它的网络连接、包过滤性能远比防火墙强，速度也快，可满足企业多用户的应用需求。防火墙不仅可以在内外网之间架设，还可以在内部网络的关键部门与其他部门之间架设，用于保护关键部门。

1.2.6　社会工程学

社会工程学(Social Engineering)定位在计算机信息安全工作链路的一个最脆弱的环节上，它利用人而非机器成功地突破企业或消费者的安全系统，骗取个人计算机或企业内部网的帐户和密码等重要信息。

(1) 电话访问。例如，某人冒充一个新雇员应聘到某公司窃取公司的商业机密。他打电话给该公司的系统管理员询问系统的安全配置资料，由于是本公司的员工，系统管理员便放松了警惕，告诉他公司网络设备的基本情况及登录密码等。再如，某人冒充某设备生产商(如思科、华为等)，打电话到某公司，询问设备的使用情况是否正常，然后借此机会套出该公司所使用设备的型号、配置、拓扑结构等情况。如果接电话的雇员放松警惕，信以为真，则会在不经意之间就泄露出公司的内部网络信息。

(2) 信任欺骗。当电话社交失败时，攻击者可能展开长达数月的信任欺骗。下面介绍一种典型情况，如通过熟人介绍认识某公司的一些雇员，然后请他们吃饭，慢慢骗取他们的信任；还可以隐藏自己的身份，通过网络聊天或者电子邮件与之相识；有的伪装成工程技术人员骗取别人回复信件，泄露有价值的信息。一般来说，有魅力的异性通常是最可怕的信任欺骗者，不过，不论对于男性还是女性，女性总是更容易令人信任。

网络安全中人是薄弱的一环，加强员工防范措施的教育可以有效地阻止社会工程学攻击。提高本网络现有用户、特别是网络管理员的安全意识，对提高网络安全性能有着非同寻常的意义。作为安全管理人员，避免员工成为侦查工具的最好方法是对他们进行安全教育。

利用社会工程学，违法犯罪分子用他人的身份赢利或盗用企业更多的信息，这不仅损害了企业利益，也侵犯了用户的个人隐私。社会工程学看似简单的欺骗，却又包含了复杂的心理学因素，其危险程度要比直接的技术入侵大得多，对于技术入侵，我们可以防范，但是心理漏洞谁又能时刻警惕呢？毫无疑问，社会工程学将会是未来入侵与反入侵的重要对抗领域。

1.2.7　备份数据的丢失和损坏

备份数据的丢失和损坏并不能算是一个网络隐患，因为它的安全隐患不是来自网络，而多数来自数据和备份媒体的管理。但防止备份数据与存储媒体的损坏和丢失，是所有安全管理的最后一道防线，是保证企业计算机系统安全的一个非常重要的因素。

正是由于许多网络安全隐患的存在，因此，如今无论是企业还是个人都非常重视系统或数据的备份。个人用户的备份通常采用系统自带的备份工具，也采用 ghost 之类的整盘复制软件，或者把这些重要数据单独存放在一个硬盘中，或记录成光盘进行备份。对企业用