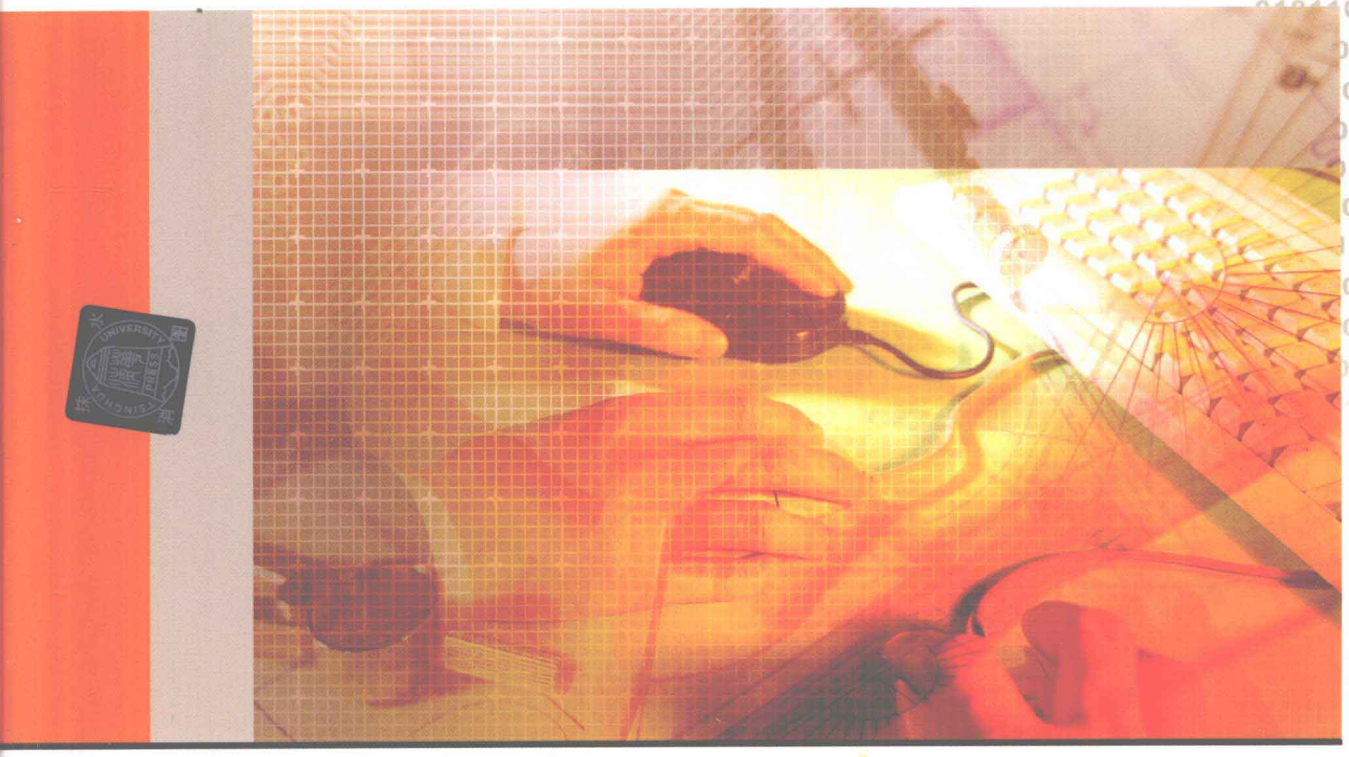
高等院校计算机教育系列教材



网络安全与管理

张素娟　吴　涛　朱俊东　编著

- 知识点新，突出实践教学，强化能力培养
- 理论知识+感性认识+动手实践，完美结合
- 内容简明扼要，突出知识要点
- 以实用为宗旨，实例丰富，用实例引导读者模仿学习

赠送电子课件

清华大学出版社

高等院校计算机教育系列教材

网络安全与管理

张素娟　吴　涛　朱俊东　编著

清华大学出版社
北 京

内 容 简 介

本书结合作者多年从事网络管理的经验，由浅入深地介绍了网络安全和网络管理的相关内容。从基础理论知识，到实际应用，再到具体配置，结合例证和最新技术发展及趋势，全面介绍了如何加强网络的安全性和可管理性。本内容理论充足，覆盖范围广泛、层次分明。

全书共分为11章，各章的主要内容说明如下：第1、2章介绍了网络安全的基本概念、基本要求、安全体系和安全协议等基础理论知识；第3章介绍了加密及加密算法的相关理论；第4～6章分别从操作系统、Web站点和邮件系统出发介绍了相关的安全知识；第7章介绍了如何使用防火墙加强内网的安全性；第8章介绍了病毒的危害、种类及如何预防；第9章介绍了网络攻击及防护的相关知识；第10、11章介绍了网络管理的基本理论和技术，以及相关的网管软件。综观全书，既有理论讲解，也有实际应用；既介绍了主流技术，也介绍了新技术的发展动向。

本书既可以作为大学本科计算机及信息相关专业的教材，也为网络管理人员提供了很好的参考。

图书在版编目(CIP)数据

网络安全与管理/张素娟，吴涛，朱俊东编著. --北京：清华大学出版社，2012
(高等院校计算机教育系列教材)
ISBN 978-7-302-29949-3

Ⅰ. ①网… Ⅱ. ①张… ②吴… ③朱… Ⅲ. ①计算机网络—安全技术—高等学校—教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2012)第203475号

责任编辑：汤涌涛
封面设计：刘孝琼
责任校对：王　晖
责任印制：李红英

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn,010-62791865
印 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：25.75　　**字　　数**：622千字
版　　次：2012年10月第1版　　**印　　次**：2012年10月第1次印刷
印　　数：1～4000
定　　价：45.00元

产品编号：046602-01

前　言

为何编写本书

随着网络迅速发展，网络的开放性、互联性、共享程度不断提高，来自外部的黑客攻击和内部的威胁使网络安全和管理问题日益突出，网络安全正面临着重大挑战。另一方面，网络的日益壮大给网络管理提出了更高的要求，完全依靠人员的管理已经行不通了。

目前，网络安全和网络管理已自成体系。不仅有威胁网络安全的各种计算机病毒、木马、恶意软件，以及黑客变化多端的网络攻击行为，还有针对这些威胁的各种网络安全技术、设备和软件等。网络安全和管理已经带动了多个新兴产业的兴起和壮大。

网络安全和管理涉及面非常广，不但包括计算机科学、网络技术、通信技术、密码技术，还包括数学、数论和信息论等内容。给学习者带来了很大的困难，本书立足于大学本科专业教材，同时也为网络管理人员提供参考。

本书内容特色

1. 内容丰富、知识全面实用

本书首先介绍网络安全的基础知识，以及加密和加密技术；然后介绍操作系统、Web站点、邮件系统、防火墙、病毒防护、网络入侵等方面的安全知识和技术；最后介绍网络管理涉及的技术和方法，以及流行的网络管理软件。

本书内容由浅入深，从基础知识讲起，每个部分的内容也是先理论后应用，理论联系实际。另外，本书在编写时联系当前技术的发展，加入了大量新的技术和新的应用内容，既充分体现了时代特色，又实实在在地让读者领略到新技术所带来的实惠。

由于本书内容覆盖范围广泛，不可能介绍最基础的理论知识，因此对读者有一定的专业知识要求，读者应该具备基本的网络理论知识，学习过计算机网络课程。

2. 结构严谨、系统

本书除第 1、2 章的基础理论介绍外，各个章节基本上相互独立，内容无交叉，结构严谨，可单独构成系统，方便学习和查阅。这些相互独立的章节组合在一起，涵盖了网络安全的方方面面。

3. 重点突出，方便教学

书中内容重点突出，在各部分的介绍中，突出强调网络安全的防护机制、措施或安全配置。这样就可以使读者全面系统地进行学习。

4. 更多专业、实用的经验和技巧

作者通过多年从事网络管理和教学的经验，积累的许多专业、实用的经验技巧，以及

对学生和管理人员真正需求的充分了解，在本书中得到了全面体现。

总之，通过阅读本书，可以使读者全面了解和掌握网络安全和管理的相关知识和技术，以便更好地进行学习和网络管理工作。

适用读者群

- 计算机或信息相关专业本科生、其他专业研究生。
- 从事网络管理的技术人员。

参加本书编写、校验工作的人员还有：章昊、范志杰、王新春、李晓颖、杨红霞、王慧然、蔺剑锋、张春平，在此一并表示由衷的感谢。由于笔者水平有限，加之时间仓促，尽管花了大量时间和精力校验，但书中可能还会存在一些疏漏，敬请各位读者批评指正，万分感谢！

编　者

目　录

第1章

网络安全概述

计算机网络的出现给人们提供了一个全新的世界，它不断地发展壮大改变了人们工作和生活的方式：可以和远在天涯的亲人视频联络，可以足不出户地浏览自己所需的信息。但网络给人们带来方便的同时，也带来了安全隐患：私人信息被公开、商业机密被窃取，安全事件频繁出现。

网络安全是一个系统，不是一种技术或者一个产品所能解决的，它涉及网络的组成和通信系统、网络的层次结构、网络协议、互联设备、操作系统和网络服务等内容，相关内容会在以后章节简要介绍。

1.1 网络安全现状及趋势

网络安全正在得到人们越来越多的关注，本节主要讲述网络安全的现状和发展趋势。

1.1.1 网络安全的主要威胁

随着信息化水平的不断提高，人们的生活、工作越来越依赖于网络，网络已经变成一个无处不在的基本工具，国家的经济、文化、军事和社会生活与网络也息息相关。然而在带来便利的同时，网络也带来了巨大的安全风险，加上信息安全规范标准不统一，且跟不上技术发展的现状，使得安全威胁越来越猖獗。

【案例 1-1】2006 年 8 月 17 日 17 岁黑客发威，腾讯 QQ 网站被黑

事件回放:

2006 年 7 月 31 日开始，湖北某市 17 岁黑客鄢某利用腾讯公司的系统漏洞，非法侵入该公司的 80 余台计算机系统，并通过这些电脑分析数据后逐步取得该公司的域密码及其他重要资料，进而取得多个系统数据库的超级用户权限，在 13 台服务器中植入木马程序。在获得大量网络虚拟财产后，鄢某通过打电话和发短信的方式，称已获取该公司的网络管理漏洞，向腾讯公司及其总裁进行敲诈勒索。事后，警方以涉嫌破坏计算机信息系统罪，将该黑客刑拘。

原因解密:

此黑客在腾讯官方论坛发布一帖子，声称发现该公司系统漏洞，并制作一木马压缩后上传至论坛，后被腾讯论坛管理人员下载后并在本地执行，随之木马被运行，黑客得到服务器的控制权。

其实道理很简单，如今黑客工具泛滥成灾，入侵随时都可能发生，浏览的网页可能被挂马，下载的文件可能含有恶意代码。本次入侵，究其原因在于腾讯工作人员安全防范意识不够，在面对狡猾的犯罪分子时缺乏应有的警惕性，同时对于安全防范技能也急需提高。

【案例 1-2】美伊战争引发美国历史上最大的黑客恐怖袭击

事件回放:

2003 年 3 月 20 日，美伊战争爆发。在炸弹持续向伊拉克倾泻之际，黑客有组织地篡改美国和英国的网站事件每 1 分钟就会有 3～4 起发生，这次黑客攻击在数量和速度上都大大超过以往。

原因解密:

此次黑客大战，使用了两种攻击手段。

Microsoft IIS 5.0 默认提供对 WebDAV 的支持，WebDAV 可以通过 HTTP 向用户提供远程文件存储的服务。IIS 5.0 包含了 WebDAV 组件不充分检查传递给部分系统组件的数据，远程攻击者利用这个漏洞对 WebDAV 进行缓冲区溢出攻击，就能够以 Web 进程权限在系统上执行任意指令。

DoS 拒绝服务攻击也是本次黑客大战常见的攻击方法，由于 TCP/IP 协议本身的缺

陷，DoS 攻击不可防御。

据统计，全球约每 20 秒钟就会发生一次网络入侵事件，约 1/4 的防火墙被攻破过，并且随着技术的不断进步，网络安全面临的威胁呈现多种多样的形式，如图 1-1 所示。

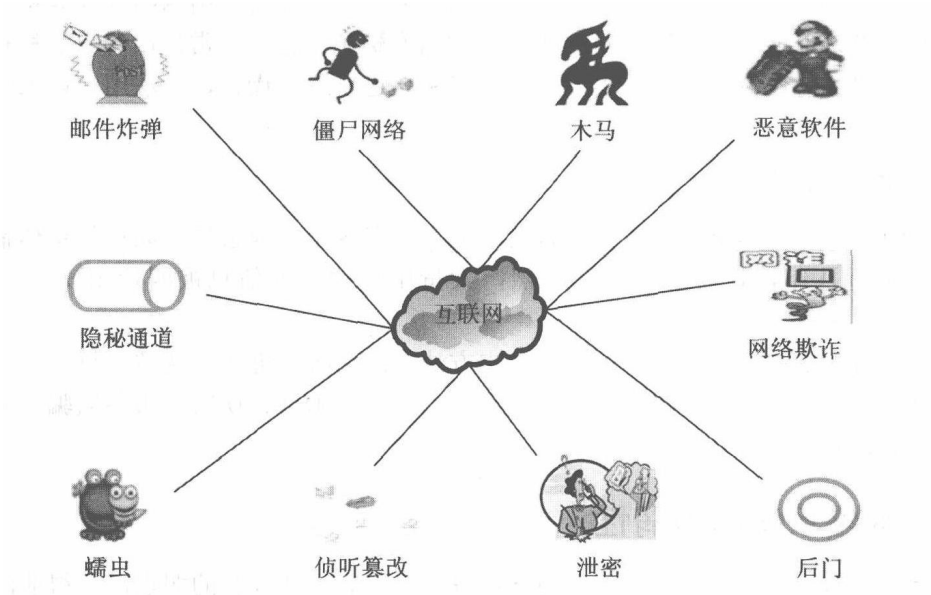


图 1-1　网络安全面临的各种威胁

计算机网络安全面临的主要威胁可以总结为以下几种情况。

1. 人为疏忽

人为疏忽主要是由于安全意识薄弱或者管理者责任心不强造成的，是可以尽力避免的。操作员由于安全配置不当，或者没有及时打补丁而引发的攻击时有发生；另外用户安全意识差、密码选择不慎，或者把自己的密码随意在网上发送给别人，也是信息失窃的主要原因之一。

2. 人为攻击

人为攻击包括主动攻击和被动攻击两种类型。

主动攻击是以各种方式有选择地破坏信息的有效性和完整性，很容易被发现。主动攻击包括拒绝服务攻击、信息篡改、资源使用和欺骗等攻击方法。

被动攻击的目的是收集信息而不是进行访问，在不影响网络正常工作的情况下，攻击者通过嗅探、信息收集等攻击方法，截获、窃取、破译网络数据来获得重要机密信息。被动攻击不易被发现，对网络安全危害极大，尤其是近年来呈现出智能型、严重性、隐蔽性和多样性的特征。

虽然被动攻击的检测十分困难，然而阻止这些攻击的成功是可行的。对被动攻击强调的是阻止而不是检测。

3. 软件漏洞

网络软件由于种种原因总是存在这样那样的漏洞和缺陷，成为黑客攻击的首选目标，

软件的隐秘通道一旦被打开，后果不堪设想。

4. 非授权访问

非授权访问主要是指在预先没有经过同意的前提下，擅自使用网络或计算机资源，如故意避开身份认证或访问控制，对服务器或数据库资源进行非正常使用等。非授权访问主要包括：假冒、身份攻击、非法用户进入网络系统进行违法操作，合法用户以未授权方式进行操作等。

5. 信息泄露或丢失

信息泄露或丢失是指敏感数据被有意或无意地泄露出去或丢失，如在信息传输中丢失或泄露。最近几年，这种势头愈演愈烈，大量用户的个人信息被叫价出卖，行为十分恶劣。

以上网络安全的各种威胁中主要的攻击方法有：窃听、讹传、伪造、篡改、截获、拒绝服务攻击、行为否认、旁路控制、物理破坏、病毒、木马、窃取、服务欺骗、陷阱、消息重发和信息战等。

1.1.2 网络系统的脆弱性

除前面叙述的各种网络威胁外，网络本身也存在着一些固有的弱点，使得非法用户可以利用这些弱点入侵系统，破坏数据。网络系统的脆弱性主要表现在以下几方面。

1. 操作系统的脆弱性

网络操作系统为了升级和维护方便提供了一些服务，这些服务虽然为厂商和用户提供了便利，但同时也为黑客和病毒提供了后门，比如为了方便打补丁的动态链接、可以远程访问的 RPC，以及系统为方便维护而提供的空口令等。

网络操作系统允许在远程节点上创建和激活进程，加上超级用户的存在，给黑客提供了入侵的通道，如黑客将木马附到超级用户上，避开作业监视程序的检测。

2. 计算机系统的脆弱性

计算机系统本身的软硬件故障也可能影响系统的正常运行。硬件故障包括电源故障、芯片故障、驱动器故障和存储介质故障等，存储介质尤其用于服务器时，使用频繁，很容易出现故障，另外由于其存有大量信息，也容易被盗窃或损坏；软件故障指应用软件和驱动程序等存在漏洞，又不能及时维护，从而给黑客以可乘之机。

3. 数据库系统的脆弱性

数据库管理系统(DBMS)采用分级管理机制，且必须与操作系统的安全配套，攻击者攻破操作系统后，很容易侵入数据库。数据库是信息的主要载体，一旦被攻破，损失巨大，而对数据库中的数据加密又会影响数据库的运行效率。另外 B/S 架构的应用程序的某些缺陷也可能威胁数据库的安全。

4. 网络通信的脆弱性

通信介质在应对这种威胁时，显得非常脆弱。非法用户可以对有线线路进行物理破

坏、搭线窃取数据；对无线传输侦听、窃听等。各种通信介质还可能由于屏蔽不严造成电磁信息辐射，进而导致机密信息外泄。

通信协议也存在安全漏洞。按照 RFC793 实现的 TCP 协议就存在安全漏洞，正常的 TCP 连接可以被非法第三方复位，因此，攻击者可以插入虚假数据到正常的 TCP 会话中；SMTP 存在封装 SMTP 地址的漏洞，导致攻击者能够绕过 RELAY 规则发送有害信息；ARP 协议漏洞导致 ARP 欺骗；FTP 的允许匿名服务等，都是通信协议脆弱性的表现。

1.1.3　网络安全现状

从 1998 年 Robert Morris Internet 蠕虫开始，到 2001 年蠕虫病毒全面爆发，给人们造成了巨大的损失。病毒破坏计算机资源和数据信息，除了造成资源和财富的损失，还可能造成社会性的灾难。据统计，几乎每天都有新的病毒产生，目前全球存在至少上万种病毒，病毒技术也朝着智能化、网络化和可控制化方向发展。一些国家的军方试图利用病毒作为现代战争的攻击手段，正在大力开发攻击性计算机病毒。

黑客攻击的目标不但包括计算机和网络设备，还包括手机等无线终端，并开始向着获取利益方面转移。

正因为网络安全的威胁无处不在，才导致对安全的相关研究越来越多。在安全协议理论和技术方面的研究经过一段时间的摸索和实践，已日趋成熟，它包括协议的安全性分析方法和各种实用安全协议的设计。目前，大量的实用安全协议已经投入使用，例如，简单网络管理协议(SNMP)、IPSec 协议、S-HTTP 协议等。安全协议的总趋势是标准化，制定统一的协议规范。

在密码技术研究上，主要包括基于数学的密码技术和基于非数学的密码技术。对于公钥密码、认证码和序列密码这几项基于数学的密码技术的研究已经日趋成熟，并取得了一些成果。目前国际上对非数学密码技术的讨论非常活跃，它包括信息隐形、量子密码、基于生物特征的识别技术等。信息隐形中的数字水印技术已经应用在一些网站中；用以保护版权，基于生物特征的指纹识别和语音识别也已经被广泛使用，一些笔记本电脑增加了指纹识别功能，手机增加了语音识别功能等，极大地方便了用户。

安全产品方面，目前市场上比较流行的主要有：防火墙、安全路由器、虚拟专用网(VPN)、安全服务器、电子签证机构——CA 和 PKI 产品、用户认证产品、安全管理中心、入侵检测系统(IDS)、安全数据库和安全操作系统等。

1.1.4　网络安全的发展趋势

由于网络系统自身的脆弱性以及网络威胁不断发展升级，因此对网络安全提出了更高的要求，未来网络安全将呈现如下发展趋势。

1. 网络安全体系化

随着信息化程度的不断提高，网络安全变得更为复杂，不再是某个安全产品或某项安全技术所能解决的。未来的网络安全将会纵向、横向全面发展，成为综合防御体系，更注重应用安全和安全管理。“三分技术，七分管理”，安全管理在网络安全中所占的比重会越来越大，国家十分重视网络和信息的安全性问题，将会逐步建立和完善信息安全保

障体系。

2. 技术发展两极分化

技术发展的两极分化包括技术的专一和技术的融合。由于一些大的集团企业和对安全要求比较高的政府部门网络，要应对各种各样的安全威胁，对产品性能要求很高，因此为了应对这种需求像防火墙、入侵检测系统和防毒杀毒产品等，越做越专。

目前市场上出现了融合两种或几种安全功能于一体的产品，用于一些规模较小的网络，既保证了功能，又节约了成本。另外越来越多的网络设备都集成了防火墙的部分功能，用以提高设备自身和所辖区域网络的安全性，如现在大部分三层交换机都具备防火墙的过滤功能。防毒防攻击的功能被集成到越来越多的软件系统中，大量网络管理软件都增加了防范恶意程序的功能。

3. 安全威胁利益化、产业化、职业化

黑客和病毒制作人员不再单纯地追求个人“荣誉感”，而更关注商业财富利益，甚至有些人已经变成了专业化程度很高、有组织的职业罪犯。电子商务成为热点后，针对网上银行和支付平台的攻击越来越多，病毒从开始的破坏系统、销毁数据，到窃取隐私和财富，从早期的盗窃虚拟价值转向直接的金融犯罪，已经形成了一个专业化程度很高的产业链：专业的病毒木马编写人员、专业的盗号人员、有组织的销售渠道和专业的玩家。最近，部分网站被曝用户信息被窃取的消息，有些网站给用户发邮件要求他们修改密码，以保护个人账户的安全。

另外，越来越多的恶意软件削弱了病毒特征，增加了钓鱼欺骗元素，目标直指商业利益。网页挂马成为木马传播的又一“帮凶”，不但大量消耗了服务器的系统资源和带宽，也严重威胁着客户端用户的信息安全。

4. 网络威胁由静态转为动态

传统的网络威胁是静态的，目标多指向服务；现在很多威胁是动态存在的，不破坏服务的提供，反而把自己隐藏在网络数据和应用之中，利用服务来传播，比如在通信流、文件和电子邮件中夹杂恶意代码，通过相应的网络服务达到传播的目的，这种威胁更难防御。自动邮件发送工具也日趋成熟，垃圾邮件和病毒邮件势必更加猖狂。

5. 漏洞攻击更为迅猛

攻击者越来越关注系统漏洞和软件漏洞，有时在补丁发布之前，利用漏洞的攻击已经出炉，尤其在一些嵌入式系统中，漏洞难以修复。

6. Web 2.0 产品受到挑战

Web 2.0 更注重用户的交互，用户既是网站内容的浏览者，也是网站内容的制造者，参与网站的建设，像博客、RSS、百科全书(WiKi)、网摘、社会网络(SNS)、P2P、即时消息(IM)等。Web 2.0 产品虽然提供了丰富的信息和展现自我的机会，但另一方面也更容易被病毒利用，它们往往成为网络钓鱼首要的攻击目标。

【案例 1-3】2011 年年末上演“密码危机”

事件回放:

2011 年 12 月 21 日上午，黑客在网上公开了开发者技术社区 CSDN 网站 600 余万个注册用户的信息，其中包括注册邮箱以及明文密码。之后天涯、人人网、开心网等多家网站的用户数据也被相继公开，以压缩文件的形式公然提供下载，多达千万的用户信息中不乏名人的资料，是中国互联网史上规模最大的一次用户资料泄露事件。目前 4 人被拘留，8 人被治安处罚。

原因解密:

此次密码泄露事件的原因有两个：很多网站管理者安全意识不足，没有对密码进行加密存储，长期使用明文密码；并且为了吸引客户，纵容用户使用简单密码，给黑客留下可乘之机。

黑客攻破一家网站的服务器后，获得大量的用户信息(包括常用邮箱和密码)，大多数用户习惯用同一个密码登录多家网站，甚至用相同的账号和邮箱，因此很容易导致网上支付等其他账号也一并丢失，黑客“托库”后试探盗号，导致更多网站信息被盗。

另外一些软件厂商由于利益驱使，大量非法搜集潜在用户的行为，也起到了推波助澜的作用。

1.2　网络安全概述

本节主要讲述网络安全的含义、主要的技术特征、研究目标和内容、防护技术等。

1.2.1　网络安全的含义及技术特征

1. 网络安全的含义

网络安全是一个系统，不是杀毒软件，不是防火墙，不是入侵检测，也不是认证和授权，不是单纯地依靠技术、依靠产品，虽然技术和产品都扮演着很重要的角色。网络安全非常复杂，需要成熟的安全架构、统一的安全标准、管理者较强的安全意识、严密完善的安全策略、不断改进的安全管理、逐步提高和升级的安全技术和产品。所有这些因素结合在一起才能提高网络的安全性，缺一不可。另外单纯就技术而言，网络安全涉及计算机科学、网络技术、通信技术、应用数学、密码技术和信息论等多个学科。

比如对于 80 端口的蠕虫病毒来说，有很多方法可以减轻其对公共服务器和其他主机的危害：

(1) 在主机上正确配置防火墙，既可以阻止病毒入侵，也可以防止病毒传染至其他主机或网络。

(2) 利用私有虚拟局域网(PVLAN)有助于防止 Web 服务器感染同一网络中其他的主机系统。

(3) 利用入侵检测 IDS 阻止和检测对 Web 服务器的入侵企图。

(4) 及时升级杀毒软件特征库，使之能够检测到蠕虫病毒或其他恶意代码。

(5) 加强网络管理，及时打补丁、定期扫描漏洞、加强操作系统防范、完善 Web 服

务安全策略等。

综合利用这些因素，可以大大提高服务器抵御80端口蠕虫病毒的能力。

因此，网络安全(Network Security)是指利用网络管理控制和技术措施，保证在网络环境中数据的保密性、完整性、网络服务可用性和可审查性受到保护；保证网络系统硬件和软件的连续运行；保证提供的服务免遭干扰和破坏；保证信息的完整性和保密性。

有时把网络安全分成两部分：系统安全和信息安全。保证信息安全是网络安全的最终目的。

同其他事物一样，网络没有绝对的安全，只要联网就存在威胁，管理者需要依据实际情况，在性能和安全上寻求一个平衡点。另外，网络安全最重要的是与时俱进，密切关注网络中的各种威胁、系统漏洞和安全技术产品的最新动向，做到新的威胁到来时能提前预防。

2. 网络安全的技术特征

网络安全主要的技术特征是：保密性、完整性、可用性、可靠性、可控性和不可否认性。

1) 保密性

保密性是指网络信息未经允许不泄露给其他用户或实体的过程，信息只有授权用户才能够使用，并且用户必须按照指定的要求使用，不得超出约定的使用范围，未经允许不得转借他人，不得用于商业目的。

常用的保密技术有：防侦收、防辐射、信息加密、物理隔离。

2) 完整性

完整性是指网络信息在存储、传输、交互和处理的过程中保证信息的原样性，未经授权不得修改、破坏和删除，是信息安全中最基本的特性。

保证完整性的主要方法有：协议、编码方法、密码校验、数字签名和认证。

3) 可用性

可用性是指网络和信息可以被授权实体正确使用，并且在非正常情况下能够恢复访问的特征。在系统正常运行时，实体能够正常使用网络，能够访问所需的信息；当网络和系统被攻击(比如拒绝服务攻击)和破坏时，能够迅速恢复使用。可用性一般用系统正常使用时间与整个工作时间之比来衡量。

可用性应该满足以下要求：身份识别与确认、访问控制、业务流控制、路由选择控制、审计跟踪。

4) 可靠性

可靠性是指网络和信息的抗毁性、生存性和有效性，即在人为破坏、随机破坏的情况下，能够保证网络和信息可放心使用和有效的特性，包括硬件可靠性、软件可靠性、人员可靠性和环境可靠性等。

5) 可控性

信息可控性是指对流通在网络系统中的信息传播及具体内容能够有效控制的特性，授权机构可以随时控制信息的机密性，对网络信息实施严密的安全监控。而对于网络的可控性是指安全部门能够保证网络不被非法利用和控制的特性。