高职高专计算机技能型紧缺人才培养规划教材

计算机网络技术专业

计算机网络安全技术

林涛 主 编
耿壮 副主编

免费提供教学相关资料

人民邮电出版社
POSTS & TELECOM PRESS

高职高专计算机技能型紧缺人才培养规划教材

计算机网络技术专业

计算机网络安全技术

林 涛 主 编

耿 壮 副主编

人民邮电出版社

北 京

图书在版编目（CIP）数据

计算机网络安全技术／林涛主编．—北京：人民邮电出版社，2007.9
高职高专计算机技能型紧缺人才培养规划教材．计算机网络技术专业
ISBN 978-7-115-16442-1

Ⅰ.计… Ⅱ.林… 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（2007）第 091875 号

内 容 提 要

本书是从实战出发，以应用为目的，防范手段为重点，理论讲述为基础的系统性、实战性、应用性较强的网络安全教材。本书主要内容包括：网络安全技术概述、网络安全基础知识、计算机病毒及其防治、特洛伊木马及其防治、Windows 操作系统的安全机制、Windows 操作系统的安全管理、Linux 操作系统的安全机制、网络攻击与防护及防火墙技术与应用。本书以培养学生能力为目的，全面讲解网络安全领域的最新技术。本书采用阶段能力培养的方式，每个能力阶段为一个章节，首先介绍问题的背景，然后讲述处理手段和方法，最后系统讲述涉及的理论问题。书中安排多项实训内容，使读者通过实战演练培养综合运用书中所讲技术的能力。

本书可作为高职高专院校计算机相关专业教材，也可作为自学和相关技术人员的参考书。

高职高专计算机技能型紧缺人才培养规划教材
计算机网络技术专业
计算机网络安全技术

◆ 主　　编　林　涛
副 主 编　耿　壮
责任编辑　赵慧君

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京铭成印刷有限公司印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：17.75
字数：426 千字　　2007 年 9 月第 1 版
印数：1－3 000 册　　2007 年 9 月北京第 1 次印刷
ISBN 978-7-115-16442-1/TP

定价：26.00 元

读者服务热线：(010)67170985　印装质量热线：(010)67129223

编 者 的 话

信息技术的飞速发展，不仅使人们的生活发生了很大改变，同时也促进了社会的发展。互联网是一个面向大众的开放系统，对信息的保密措施和系统的安全性考虑得并不完备，由此引起的网络安全问题日益严重。因此，如何保护计算机信息的内容，也即信息内容的保密问题显得越来越重要。网络安全可以认为是网络上的信息安全，从广义上来说，凡是涉及到网络信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。信息安全技术主要包括监控、扫描、检测、加密、认证、防攻击、防病毒以及审计等几个方面，其中加密技术是信息安全的核心技术，已经渗透到大部分安全产品之中，并正向芯片化方向发展。

本书从理论和技术两个方面对网络信息安全的相关知识进行全面和系统的介绍。首先，本书结合最新网络信息安全方面的案例，介绍网络安全领域面临的问题、出现安全问题的原因，解决网络安全问题的技术手段与方法，以及未来安全问题的发展趋势；第二，从全面安全的角度，介绍了构造完整网络安全保障体系的几个方面；第三，详细分析了主流操作系统Windows、Linux中的安全问题及解决手段；第四，从网络体系的角度分析了黑客常见的攻击手段，网络的安全结构和问题，以及对付黑客的技术方法；第五，分析了网络病毒的传播方式、机理和预防方法，介绍了主流防病毒软件的工作原理和使用方法；第六，分析了防火墙技术的理论和防火墙体系结构，介绍了主流防火墙产品的工作原理及使用方法；最后，本书设计了几个网络安全管理实训内容，使读者能够综合运用所学知识进行网络安全管理。

作者有多年信息安全企业的工作经验，并在计算机网络安全领域从事了多年科研和教学工作。本书的编写体现了技术的实用性、系统性和先进性，介绍了信息安全领域最新的技术。在编写过程中，力求使本书具有以下特点。

- 在内容安排上，尽量适合学生学习的特点，循序渐进，深入浅出，注重计算机网络安全的应用方法和技能的传授。
- 注重教材的先进性，力求反映当前计算机网络安全技术发展的最新成果。
- 兼顾教材的系统性与科学性，既考虑知识和技能的科学体系，又遵循教育规律，注意内容的取舍与相关课程的衔接，尽量避免内容重复。
- 力求文字精炼，语言流畅，并注重向学生传授灵活的学习方法。
- 习题具有思考性和启发性，注重培养学生的创新能力。

通过对本书的学习，读者可以系统地掌握计算机网络安全的基础知识和技能。

深圳信息职业技术学院林涛副教授对本书的编写思路与大纲进行了总体策划，并编写了第2章～第9章；耿壮副教授编写了第1章。广东证券公司毛丰山工程师对本书的编写思路提出了很好的建议并审阅了全书。在此，一并致谢。

由于时间仓促，加之作者水平有限，书中难免存在不当之处，恳请读者批评指正。作者的E-mail地址是lint@sziit.com.cn。

编 者

2007年5月

目　录

第 1 章

网络安全技术概述

本章介绍网络安全的基本问题、网络安全体系结构与模型、网络安全策略等问题。

1.1 网络安全的基本问题

在网络出现以前，信息安全指的是对信息机密性、完整性的保护，即面向数据的安全。互联网出现以后，信息安全除了包含上述内容以外，其内涵又扩展到面向用户的安全。综合而言，网络安全包括物理安全威胁、操作系统的安全缺陷、网络协议的安全缺陷、应用软件的实现缺陷、用户使用的缺陷和恶意程序等 6 个方面。

1.1.1 物理安全威胁

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。物理安全是指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。

在物理安全方面，与网络相关的问题主要在于传输数据的安全性。TCP/IP 是一种分组交换协议，各个分组在网络上都是透明传输的，经过不同的网络，由路由器转发，最后到达目的计算机。由于分组都是直接经过这些网络的，所以这些网络上的计算机都有可能将其捕获，从而窃听到正在传输的数据。物理上的传输安全问题对网络安全非常重要。

由于物理网络的传输限制，并不是在网络上的任何位置都能捕获分组信息。较老的共享式以太网能在任何一个位置窃听所有流经网络的分组信息，因此安全性不高；而新式的交换式以太网能够在交换机上隔离流向不同计算机的数据，因此安全性高。然而，无论何种类型的网络，路由器总是一个非常关键的设备，所有流入和流出网络的数据都要经过它，如果攻击者在路由器上窃听，就会造成非常严重的安全问题。

目前主要的物理安全威胁包括以下 3 大类。

- 自然灾害（例如，地震、水灾和火灾等）、物理损坏（例如，硬盘损坏、设备使用寿命到期和外力破损等）和设备故障（例如，停电或电源故障造成设备断电和电磁干扰等）。这类安全威胁的特点是突发性、自然因素性、非针对性。这类安全威胁只破坏信息的完整性和可用性，无损信息的秘密性。
- 电磁辐射（例如，监听计算机操作过程）、乘虚而入（例如，进入安全进程后半途离开）和痕迹泄露（例如，口令、密钥等保管不善，易于被人发现）。这类安全威胁的特点是难以察觉性、人为实施的故意性和信息的无意泄露性。这类安全威胁只破坏信息的秘密性，无损信息的完整性和可用性。

• 操作失误（例如，删除文件、格式化硬盘和线路拆除等）和意外疏忽（例如，系统掉电、操作系统死机等系统崩溃）。这类安全威胁的特点是人为实施的无意性和非针对性。这类安全威胁只破坏信息的完整性和可用性，无损信息的秘密性。

1.1.2 操作系统的安全缺陷

操作系统介于用户和硬件之间。任何操作系统都自带一系列的系统应用程序，为用户使用计算机提供有效和方便的操作。实际上，这些应用程序也是一种软件。不同于用户应用程序的是，操作系统的应用程序在用户安装操作系统的时候都是缺省安装的。如果这些应用程序有安全缺陷，那么就会使系统处于不安全的状态。因此，了解操作系统经常出现的安全缺陷是很有必要的。

目前，人们使用的操作系统分为两大类：UNIX/Linux 系列和 Windows 系列。下面分别举例说明这两大类操作系统中存在的安全缺陷。

1. 安全缺陷的检索

大多数信息安全工具都包含一个信息安全缺陷的数据库，例如，CERT 安全公告和 Bugtraq ID 等。但是，这些数据库对信息安全缺陷的描述格式各不相同。因此，有时很难确定在不同数据库中所描述的缺陷是否是同一个缺陷。每一个数据库都使用自己的编号以及描述格式，这样给使用者带来了诸多不便。

CVE（Common Vulnerabilities and Exposures）是信息安全确认的一个列表或者词典，它在不同信息安全缺陷的数据库之间提供一种公共索引，是信息共享的关键。有了 CVE 检索之后，一个缺陷就有了一个公共的名字，从而可以通过 CVE 的条款检索到包含该缺陷的所有数据库。

2. UNIX 操作系统的安全缺陷

（1）远程过程调用（Remote Procedure Calls，RPC）

远程过程调用允许一台机器上的程序执行另一台机器上的程序，它们被广泛地用于提供网络服务，如 NFS 文件共享和 NIS。很多 UNIX 操作系统的 RPC 软件包中，包含具有缓冲区溢出缺陷的程序。

（2）Sendmail

Sendmail 是在 UNIX 和 Linux 操作系统中用得最多的发送、接收和转发电子邮件的程序。

Sendmail 在因特网上的广泛应用，使它成为攻击者的主要目标。它存在若干个缺陷。第一个建议是 CERT/CC 在 1988 年提出的，指出了 Sendmail 中一个易受攻击的缺陷。其中最为常用的是攻击者可以发送一封特别的邮件消息给运行 Sendmail 的机器，Sendmail 会根据这条消息要求受劫持的机器把它的口令文件发送给攻击者的机器，这样口令就会被破解。UNIX 和 Linux 的大部分版本都会受到该漏洞的影响。Sendmail 有很多易受攻击的弱点，因此必须定期地检查 Sendmail 最新版本和补丁版本，并予以更新。如果没有更新版本或安装补丁文件，就可能受攻击。

3. Windows 系列操作系统的安全缺陷

（1）Unicode

Unicode 是 ISO 发布的统一全球文字符号的国际标准编码，它是一种双字节的编码。不论何种平台、何种程序、何种语言，Unicode 为每一个字符提供了唯一的序号。Unicode 标准

被包括 Microsoft 公司在内的很多软件开发商所采用。通过向 IIS（Internet Information Server）服务器发出一个包括非法 Unicode UTF-8 序列的 URL，攻击者可以迫使服务器逐字“进入或退出”目录并执行任意脚本，这种攻击称为目录转换（Directory Traversal）攻击。

判断是否存在这个缺陷的最好方法是运行 Hfnetchk。Hfnetchk 是一个用来帮助网络管理员判断系统所打补丁情况的工具。

解决上述问题的方案是如果不需要使用 Web 服务器，就把 IIS 服务器关闭。一般来说，Windows 2000 Server 的缺省安装都是把 IIS 服务器打开的。如果实在需要 IIS 服务器，应下载 Microsoft 的最新补丁。另外，IIS Lockdown 和 URL Scan 都可以避免这类攻击。IIS Lockdown 可以帮助系统管理员锁住 IIS 服务器；URL Scan 是一个可以过滤很多 HTTP 请求的过滤器，它可以过滤包含 UTF-8 编码字符的请求。

（2）ISAPI 缓冲区溢出

Microsoft IIS 是在大多数 Microsoft Windows NT 和 Windows 2000 服务器上使用的服务器软件。在安装 IIS 的时候，多个 ISAPI（Internet Service Application Programming Interface）被自动安装。ISAPI 允许开发人员使用多种动态链接库 DLLs 来扩展 IIS 服务器的性能。一些动态链接库（例如 idq.dll）有编程错误，使得它们进行不正确的边界检查。特别是，它们不阻塞超长字符串。攻击者可以利用这一点向 DLL 发送数据，造成缓冲区溢出，进而控制 IIS 服务器。

安装 Microsoft Index Server 2.0 的系统和 Windows 2000 中的 Indexing Service，都具有 idp.dll 缓冲区溢出缺陷。Windows 2000 Professional 也具有 DLL 的缺陷，但不是缺省安装。如果可能，应使用 Group Policy，禁止基于网络的打印。Windows XP 没有这个缺陷。

如果安装了 IIS 服务器，并没有打过补丁（SP2），那么该系统很可能会受到这种攻击。可以用 Hfnetchk 工具检查系统补丁的情况。

解决上述问题的方案是如果发现系统具有这种缺陷，则安装最新的 Microsoft 补丁。同时，应检查并取消所有不需要的 ISAPI 扩展，经常检查这些扩展是否被恢复。还要记住最小权限规则，系统应运行正常工作所需的最少服务。另外，IIS Lockdown 和 URL Scan 均可以避免这类攻击。

1.1.3　网络协议的安全缺陷

TCP/IP 是目前 Internet 使用的协议。从 Internet 的发展来看，它起源于美国国防部赞助研究的 ARPANET 网络，它通过租用的电话线连接了数百所大学和政府部门。当卫星和无线网络出现以后，已有的协议在和它们互连时出现了问题，所以需要一种新的参考体系结构。这个体系结构在它的两个主要协议出现以后，被称为 TCP/IP 参考模型。它之所以有今天如此广泛的使用，是因为它在设计原则上有很多优点，如简单、可扩展性强和尽力而为等。这些优点给使用 TCP/IP 的用户带来非常方便的互连环境，使得 Internet 的用户迅速地增加。但是，TCP/IP 也存在着一系列的安全缺陷，有的缺陷是由于源地址的认证问题造成的，有的缺陷则来自网络控制机制和路由协议等。这些缺陷，是所有使用 TCP/IP 的系统所共有的，以下将讨论这些安全隐患。

1. TCP 序列号预计

TCP 序列号预计由莫里斯首先提出，是网络安全领域中最有名的缺陷之一。这种攻击的

实质，是在不能接到目的主机应答确认时，通过预计序列号建立连接。这样，入侵者可以伪装成信任主机与目的主机建立连接，并执行非法操作。

这种攻击就是常说的IP欺骗攻击（IP Spoof）。除此以外，入侵者还可以利用TCP序列号预测方法去预测一个正在进行的正常连接中的TCP序列号的变化过程，从而在该连接中随意插入自己的数据，甚至切断该连接。这种攻击也属于IP欺骗类型，另外它还叫做IP劫持（Hijacking）攻击。

IP地址欺骗是黑客经常用来隐藏自己踪迹的一种手段。例如，常见的smurf攻击就利用了路由的特性向数以千计的机器发出一串数据包，每一个数据包都假冒受害主机的IP地址作为源地址，于是上千台主机会同时向这个受害的主机返回数据包，导致该主机或网络崩溃。

2. 路由协议缺陷

（1）源路由选项的使用

在IP包头中的源路由选项用于该IP包的路由选择，这样，一个IP包可以按照预先指定的路由到达目的主机。现在，假设目的主机使用该源路由的逆向路由与源主机进行通信，这样的处理是相当合乎情理的，因为在一般情况下，一端使用源路由选项常常表示这一端有充足理由（如拥塞避免、故障路由的回避，以及效率方面的考虑）认定源路由有更好的表现。

但这样也给入侵者创造了良机，当预先知道某一主机有一个信任主机时，即可利用源路由选项伪装成受信任主机，从而攻击系统，这相当于使主机可能遭到来自所有其他主机的攻击。

这种攻击很难避免。在网关上禁止使用源路由包的通过是一种简单的防治方法，但这种方法对于来自同一子网内机器的攻击则束手无策，而且这种方法完全禁止了源路由选项，未免不尽情理。理论上可以让每一主机得知路由状况，以智能判断源路由选项是否合法，然而，这在实际中是不可能做到的。也许最好的防治方法是完全避免基于IP地址的认证方式，如R协议、X协议等。

对于Cisco路由器，禁止源路由包可通过命令：no ip source-route实现。

（2）伪造ARP包

伪造ARP包是一种很复杂的技术，涉及到TCP/IP及以太网特性的很多方面。伪造ARP包的主要过程是，以目的主机的IP地址和以太网地址为源地址发一ARP包，这样即可造成另一种IP Spoof。

这种攻击主要见于以太网中，在交换式以太网中，交换集线器在收到每一ARP包时更新Cache。不停发送Spoof ARP包，可使送往目的主机的包均送到入侵者处，这样，交换式以太网也可被监听。

当然，当ARP包从一主机发出时，目的主机会出现异常反应，这样会使目的主机警觉。但是，由于TCP有重发机制的保护，所以恰当的选择ARP包发出的频率，可以使同一IP以太网地址的使用呈现分时特征，并均可以正常进行。

解决上述问题的方法是：将交换集线器设为静态绑定；另一可行的方法是当发现主机运行不正常（网速慢，IP包丢失率较高）时，反映给网络管理员。

（3）RIP的攻击

RIP（Routing Information Protocol）是用于自治系统（Autonomous System，AS）内部的一种内部路由协议（Internal Gateway Protocol，IGP）。RIP用于在自治系统内部的路由器之间

交换路由信息，使用的是距离向量路由器算法。该算法的主要思想就是向相邻路由器宣布可以通过它达到的路由器及其距离。值得注意的是，接受方并不去检查这一信息。这样，一个入侵者有可能向目的主机以及沿途的各网关发出伪造的路由信息。如果入侵者宣布经过自己的一条通向目的主机的路由，将会导致所有发往目的主机数据包发往入侵者。于是，入侵者就可以冒充是目的主机，也可以监听所有目的主机的数据包，甚至在数据流中插入任意的包。

解决上述问题的方法是：注意路由的改变信息，一个聪明的网关可以有效地摈弃任何明显错误的路由信息。RIP 的认证、加密也是一种较好的方法。

（4）OSPF 的攻击

OSPF（Open Shortest Path First）协议是用于自治域内部的另一种路由协议。OSPF 协议使用的路由算法是链路状态（Link-State）算法。在该算法中，每个路由器给相邻路由器宣布的信息是一个完整的路由状态，包括可到达的路由器，连接类型和其他相关信息。和 RIP 相比，虽然 OSPF 协议中实施了认证过程，但是该协议还存在着一些安全的问题。

3. 网络监听

TCP/IP 的设计原则是保持简单，它的唯一功能就是负责互连（传输），尽可能把复杂的工作传给终端去处理，所以在设计 TCP/IP 的时候，设计者没有考虑传输数据的加密。可以看到，TCP 包和 IP 包都没有留给数据加密的项目或选项，这使得在网上传输的数据，如果在终端没有加以处理的话，都是明文传输。

以太网是目前使用最广泛的连网方式。由于以太网特有的工作方式，网络请求一般以广播的方式传送，这个广播是非验证的，也就是同网段的每个计算机都可以收到。除了目标接收者会应答这个信息外，其他的接受者都将忽略这个广播。如果有一个网络设备专门收集广播而决不应答，那么，它就可以看到本网的任何计算机在网上传输的数据。也就是说，如果数据没有经过加密，那么它就可以看到所有的内容。Sniffer 就是一个在以太网上进行监听的专用软件。监听对网络的安全威胁是相当大的，因为它可以做到以下几点。

（1）抓到正在传输的密码。Telnet、FTP 和 POP3 等主要协议的密码都是明文传输，如果这些密码在网上传输的时候被攻击者抓到，它就可以获得相应计算机的控制权。

（2）抓到别人的秘密（信用卡号）或不想共享的东西。个人敏感信息、商业机密等信息在网上传输都不希望被第三者看到。可如果这些信息没有经过加密而在网上传输，就很可能被监听到。

（3）暴露网络信息。有时候，监听虽然看不到数据的内容，但是可以看到哪些主机开设了哪些服务，哪些主机之间进行了通信，从而可以分析出主机之间的信任关系。这些信息都可以帮助黑客对系统进行攻击。

1.1.4　应用软件的实现缺陷

这里所指的软件是运行在计算机和设备上的程序。操作系统就是一种软件，应用软件通常是运行在操作系统上的。一般来说，一个操作系统常常自带一些标准的软件包，所以这里谈到的软件实现缺陷，也会出现于操作系统。有关操作系统所特有的缺陷，将会在操作系统缺陷的小节中讨论。

软件实现缺陷是由于程序员在程序设计的时候没有考虑周全而造成的。软件缺陷一般可以分为以下几种类型：

- 输入确认错误；
- 访问确认错误；
- 特殊条件错误；
- 设计错误；
- 配置错误；
- 竞争条件错误；
- 其他。

1. 输入确认错误

在输入确认错误的程序中，由用户输入的字符串没有经过适当的检查，使得黑客可以通过输入一个特殊的字符串造成程序运行错误，比如程序运行不正确、不稳定，异常终止等结果。最危险的是黑客可以利用这样的程序进行一些非法操作，从而造成缓冲区溢出漏洞。缓冲区溢出是一个重要的软件实现缺陷。

输入确认错误的另一个子集就是边界条件溢出，指的是程序中的一个变量值超过它自己边界条件时的程序运行错误。这个变量可以是用户输入值，也可以由系统自己生成。因此可以说，边界条件溢出的缺陷和输入确认错误的缺陷有一定的交叉。边界条件溢出的缺陷可能导致系统运行不稳定，如系统没有足够内存、硬盘或者网络的带宽占满等。著名的拒绝服务攻击就是利用这样的缺陷进行的。

程序中的一个变量超过它的边界条件的原因有很多，有可能是用户的输入错误，有可能是由于一个公式里边的分母为零，也有可能是由于出现一个死循环使得一个变量无限量增大。

2. 访问确认错误

访问确认错误指的是系统的访问控制机制出现错误。错误并不在于用户可控制的配置部分，而在系统的控制机制本身。这样的缺陷有可能使得系统运行不稳定，但是基本上不会被利用去攻击系统，因为它的运行错误不受用户的控制。

3. 特殊条件错误

未处理特殊条件的缺陷指的是程序运行的时候，会在某些特殊条件或者环境下出现问题。

4. 设计错误

设计错误指的是程序在实现和配置的时候并不存在错误，错误是在程序的设计方案上。回想一下上面谈过的 TCP/IP 缺陷，这些缺陷都属于设计缺陷。

5. 配置错误

配置错误指的是程序由于用户的配置错误（故意或者意外地）引起系统运行不稳定。这个缺陷并不在于程序的设计和实现，而在于程序的配置。值得注意的是，很多软件在安装的时候都有一个缺省配置，用户在安装的时候基本上按照这个配置进行修改。如果缺省配置出现问题，那么系统就会出现漏洞。

一个很重要的例子就是旧的 Sendmail 版本的缺省配置是没有关闭邮件转发功能，使得黑客可以利用这个服务进行垃圾邮件的转发。

6. 竞争条件错误

竞争条件错误是程序的安全检查模块在一些非常特殊的情况下出现错误而引起的。例如，一个程序在运行的时候都要执行多个操作。在执行每个操作之前，程序都要检查该操作

是否合法，然后才执行它。模块化编程都将安全检查工作交给安全检查模块完成，但是，在安全检查模块检查的那个时刻和程序执行操作时刻之间的一瞬间，一些条件有可能会改变，如环境条件使得安全检查模块的结果根本没有什么意义。攻击者很可能利用这个很小的机会去攻击这个系统。

1.1.5　用户使用的缺陷

系统和网络实际上都是由用户（管理员）来操作的。由于用户（管理员）缺乏安全知识，他们在使用系统和网络的时候会无意给攻击者提供入侵的机会。用户使用的缺陷体现在以下几个方面：

- 密码易于被破解；
- 软件使用的错误；
- 系统备份不完整。

1. 密码易于被破解

大多数系统都把口令作为第一层和唯一的防线。用户的 ID 是很容易获得的，而且大多数公司都使用拨号的方法绕过防火墙。因此，如果攻击者能够确定一个账号名和密码，他就能够进入网络。易猜的口令或缺省口令是一个很严重的问题，但更严重的问题是有的账号根本没有口令。实际上，所有使用弱口令、缺省口令和没有口令的账号都应从系统中清除。密码之所以被破解是由于以下几个原因造成的。

（1）缺省密码

很多系统有内置的或缺省的账号，这些账号在软件的安装过程中通常是不变的。攻击者常通过查找这些账号对系统进行攻击，因此，所有内置的或缺省的账号都应从系统中移出。

（2）密码与个人信息有关

很多人都习惯把密码设为自己的生日、亲人的名字、爱好和宠物等。由于个人的账号比较容易得到，所以，容易根据账号拥有者的个人信息去判断密码。

（3）密码为词典中的词语

很多人为了方便就把密码设为词典中的一个单词或者词组。Crack 软件使用的词典的容量可以越来越大，而密码被破解的可能性也就越来越高了。

（4）过短密码

有时候用户使用的密码不是词典中的词，而是一些随机的字符。如果密码长度过短（如小于 4 个字符），也可以被 Crack 软件破解出来。这是因为，Crack 软件使用的词典是由黑客自己建立的，他可以把长度小于等于 4 个字符的所有字符串加入词典，这样的词典可以破解以上所说的过短密码。如果 Crack 软件的词典中的词建立成足够长，那么长的密码也有可能被破解，但是词典的词越长，词典的容量就越大，破解的速度当然就越慢。

（5）永久密码

很多人没有修改密码的习惯。这样，密码如果被黑客抓到（如通过监听），系统就会受到很大的损害。还有人习惯在多个账号上用一个通用的密码，这样，一个账号被破解会引发所有的账号都被破解。特别是当这个人把自己的通用密码用在一个不可靠的站点上时，这种情况很可能就会发生。

2. 软件使用的错误

大多数软件，包括操作系统和应用程序，都附带安装脚本或安装程序。这些安装程序的目的是尽快安装软件，在尽量减少管理员工作的情况下，激活尽可能多的功能。为实现这个目的，脚本通常安装了大多数用户所不需要的组件。软件开发商的逻辑是最好先激活还不需要的功能，而不是让用户在需要时再去安装额外的组件。这种方法尽管对用户很方便，但却产生了很多危险的安全漏洞，因为用户不会主动地给自己不使用的软件组件打补丁，而且很多用户根本不知道实际安装了什么，很多系统中留有安全漏洞就是因为用户根本不知道安装了哪些程序。

那些没有打补丁的服务为攻击者接管计算机铺平了道路。对操作系统来说，缺省安装几乎包括了额外的服务和相应的开放端口，攻击者可以通过这些端口侵入计算机系统。一般说来，打开的端口越少，攻击者用来侵入计算机的途径就越少。对于应用软件来说，缺省安装包括了不必要的脚本范例，尤其对于 Web 服务器来说更是如此。攻击者会利用这些脚本侵入系统，并获取他们感兴趣的信息。绝大多数情况下，被侵入系统的管理员根本不知道他们安装这些脚本范例。这些脚本的编写水平极为低劣，经常忘记出错检查，给缓冲区溢出类型的攻击提供了机会。

3. 系统备份不完整

当事故发生时（这在每一个组织均有可能发生），从事故中恢复系统要求及时的备份和可靠的数据存储方式。一些组织的确每天做备份，但是并不去确认备份是否有效，其他一些组织建立了备份的策略和步骤，但却没有建立存储的策略和步骤。这些错误往往在黑客进入系统并已经破坏了数据后才被发现。

第二个问题是对备份介质的物理保护不够。备份保存了和服务器上同样敏感的信息，它们也应该同样受到保护。

怎样判断系统是否易受攻击？应首先列出一份紧要系统的列表，然后对每一个系统可能遇到的风险和危险进行分析，应根据这些重要的服务器制定备份方式和策略。一旦确认了这些重要系统，应明确以下重要问题：

- 系统是否有备份？
- 备份间隔是可接受的吗？
- 系统是按规定进行备份的吗？
- 是否确认备份介质正确地保存了数据？
- 备份介质是否在室内得到了正确的保护？
- 是否在另一处还有操作系统和存储设施的备份？
- 存储过程是否被测试及确认？

1.1.6 恶意代码

前面几节的内容包括物理安全威胁、操作系统的安全缺陷、网络协议的安全缺陷、应用软件的实现缺陷和用户使用缺陷，所谈论的问题都有共同的特点，就是安全威胁不是人们故意创造出来的，一般都是在设计、实现或者使用的某个环节出现了差错而无意造成的。在网络上还会出现另一种安全风险，即人为地创造出来。这些安全风险包括计算机病毒、特洛伊木马以及其他恶意代码。