第 1 章　网络安全概论

知识目标

◎ 了解当前社会网络安全问题的严重性与紧迫性
◎ 掌握网络安全的定义、目标和网络安全的 5 个特征
◎ 了解网络安全的等级与标准，我国在网络安全上的法律与法规

技能目标

◎ 掌握在网络安全中采用的主要技术
◎ 了解网络安全面临的主要威胁
◎ 掌握网络安全的体系结构，包括网络安全的 PDRR 模型、网络中的 8 个安全机制等

随着计算机技术的迅猛发展，计算机的安全问题成了人们日益关注的核心问题，倘若网络存在大量的安全问题，不单单是计算机无法正常工作，还将导致信息的泄露。本章通过对网络安全的相关知识进行概述，使读者对网络安全有一个大概的认识，为后面各章的学习打下基础。

1.1　网络安全与社会

网络安全问题是与计算机网络的普及分不开的。随着计算机技术、现代通信技术和网络技术的发展，尤其是 Internet 的广泛应用，计算机的应用更加广泛与深入，计算机网络与人们的工作和生活的联系也越来越密切。但是，随之而来的是一系列网络安全问题。

1.1.1　计算机网络的普及

据统计，2009 年年底，全球互联网用户总数达到 17.3 亿。可以肯定的是，在 2020 年之前，全球网络用户数量将一直呈增长之势。美国国家科学基金会预计，到 2020 年，全球网络用户总数有望增至 50 亿。

2010 年 1 月 15 日，中国互联网络信息中心（CNNIC）在北京发布《第 25 次中国互联网络发展状况统计报告》：截至 2009 年 12 月 30 日，中国网络用户规模达到 3.84 亿，普及率达到 28.9%。网络用户规模较 2008 年底增长 8 600 万，年增长率为 28.9%。国际出口带宽达到 866 367 Mbit/s，年增长率为 35.3%。按照每个家庭有 2 个网络用户保守计算，即使每个家庭使用 1 台计算机，网络用户所使用的计算机数量近 2 亿。2002—2009 年中国网络用户

数量的变化示意图如图 1-1 所示。

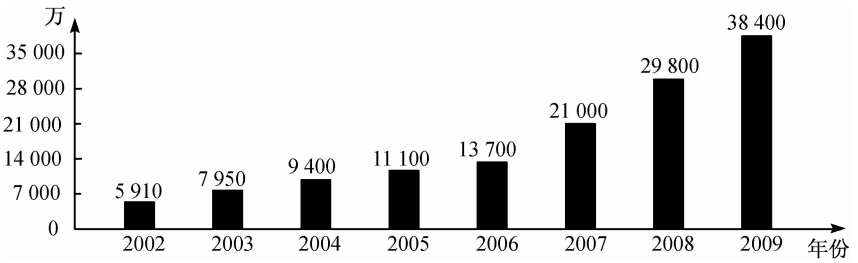

图 1-1 2002—2009 年中国网络用户数量的变化

1.1.2 网络带来的安全问题

通过网络，人们可以与远方的朋友互发函件；可以足不出户地浏览世界各地的报刊杂志，搜索自己所需的信息；可以在家里与世界各个角落的陌生人打牌、下棋……但与此同时，人们也发现自己的计算机信息系统不断受到侵害，其形式多样、技术先进且复杂，令人防不胜防。因此，计算机网络系统的安全问题也变得日益突出和复杂。

据有关方面统计，目前美国每年由于网络安全问题而遭受的经济损失超过 170 亿美元；欧洲各国的小型企业每年因计算机病毒导致的经济损失高达几百亿欧元；在 2009 年，中国由于网络安全带来的损失高达 20 多亿美元。而且，这些数字每年都有较大幅度的增长。

1.1.3 重大的网络安全事件

下面列举一些影响比较大的网络安全事件。

1989 年 10 月，一名黑客为了抗议钚驱动的伽利略探测器的发射而入侵了美国航空航天局的计算机系统，造成了 50 万美元的损失，这可能是历史上有记载的第一次系统入侵。尽管有线索表明此次入侵是一个澳大利亚黑客所为，但并无确凿证据，该案至今悬而未决。

1995 年，来自俄罗斯的黑客弗拉迪米·莱文在互联网上上演了精彩的“偷天换日”。他是历史上第一个通过入侵银行计算机系统来获利的黑客。他侵入美国花旗银行并盗走 1 000 万美元之后，把账户里的钱转移至美国、芬兰、荷兰、德国、爱尔兰等地。

1998 年 2 月，美国国防部声称黑客向五角大楼网站发动了“有史以来最大规模、最系统性的攻击行动”，入侵了许多非政府保密性的敏感计算机网络，查询并修改了工资报表和人员数据。

1998 年 6 月 2 日，一位名叫陈盈豪的台湾大学生所编写的 CIH 病毒，从中国台湾传入大陆地区；1998 年 8 月 26 日，CIH 1.4 版本病毒爆发，首次在全球蔓延；1999 年 4 月 26 日，CIH 1.2 版本病毒首次大范围爆发，全球超过 6 000 万台计算机遭到不同程度的破坏；2000 年 4 月 26 日，CIH 1.2 版本病毒第二次大范围爆发，全球损失超过 10 亿美元。

1999 年，“梅利莎”病毒使世界上 300 多家公司的计算机系统崩溃，该病毒造成的损失接近 4 亿美金，它是首个具有全球破坏力的病毒。该病毒的编写者戴维·史密斯在编写此病毒时仅 31 岁，他被判处 20 个月徒刑。

2000 年 2 月，在 3 天的时间里，黑客使用“拒绝服务式”的攻击手段，使雅虎、亚马逊、电子港湾、CNN 等陷入瘫痪。短短 3 天之内，这些受害公司的损失就超过了 10 亿美元，其中

仅营销和广告收入的损失就高达 1 亿美元。

2000 年 5 月 3 日，在中国香港爆发了“I Love You”病毒（亦称为“爱虫”病毒、“情书”病毒），这是一个用 VBScript 编写、可通过 E-mail 散布的病毒，给全球带来 100 亿～150 亿美元的损失。

2003 年 1 月 25 日上午开始，国际互联网网络速度都变得缓慢。日本、韩国、美国、中国乃至全世界都没能逃脱这场灾难。当天下午，中国的电信骨干网络瘫痪，服务器无法登录，路由器也无法正常登录，防火墙异常，等等。在当天 21 时左右，已经有专家声称这次攻击对中国的互联网造成了 10 多亿元的损失。

2003 年，在全球范围内爆发了冲击波病毒，该病毒运行时会不停地利用 IP 扫描技术寻找网络上系统为 Windows 2000 或 Windows XP 的计算机，找到后就利用 DCOM RPC 缓冲区漏洞攻击该系统，一旦攻击成功，病毒体会被传送到对方计算机中进行感染，使系统操作异常，计算机不断重启，甚至导致系统崩溃。该病毒给全球造成 20 亿～100 亿美元的损失。

2006 年 11 月，一名武汉男生的“熊猫烧香”病毒（Worm. WhBoy.）在年末引发病毒狂潮，“熊猫烧香”病毒利用的传播方式囊括了漏洞攻击、感染文件、移动存储介质、局域网传播、网页浏览、社会工程学欺骗等种种可能的手法。病毒程序本身并不高深，却造成严重的大面积感染，以致人们达到“谈猫色变”的程度。

2008 年，一个全球性的黑客组织，利用 ATM 欺诈程序在一夜之间从世界 49 个城市的银行中盗走了 900 万美元。最关键的是，目前美国联邦调查局还没破案，据说甚至连一个嫌疑人还没找到。

2009 年 7 月 7 日，韩国总统府、国会、国情院和国防部等韩国国家机关，以及金融界、媒体和防火墙企业网站遭到黑客的攻击。7 月 9 日韩国国家情报院和国民银行网站无法被访问。韩国国会、国防部、外交通商部等机构的网站一度无法打开。这是韩国遭遇的有史以来最强的一次黑客攻击。

1.1.4　我国的网络安全情况调查

据调查显示，2009 年，我国网络安全的问题依然非常严峻，可以通过以下数字看出当前网络安全的现状。

- 153 亿元：一年之内，网络用户处理安全事件所支出的服务费用。
- 588.9 元：在实际产生费用的人群中，人均处理网络安全事件的费用。
- 52%：52%的网络用户曾遭遇过网络安全事件。
- 21.2%：网络事件给 21.2%的网络用户带来直接经济损失，包括网络游戏、即时通信等账号被盗造成的虚拟财产损失，网银密码、账号被盗造成的财产损失，以及因网络系统、操作系统瘫痪，数据、文件等丢失或损坏，对其找回或修复产生的费用等。
- 77.3%：77.3%的网络用户反映遇到网络安全事件要付出大量的时间成本。
- 10 小时：平均每人每年用在处理网络安全事件上的时间。
- 45%：45%的网络用户发现过数据、文件被损坏。

1.2 网络安全的概念

网络安全是一个涉及面比较广的概念，内容也非常丰富。本节首先介绍网络安全的一般定义，随后由网络安全的目标引入网络安全的特征。

1.2.1 网络安全的定义

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，不因偶然的或者恶意的原因而遭受破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

从广义来说，凡是涉及网络上信息的保密性、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。网络安全是一门涉及计算机科学、网络技术、通信技术、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。

1.2.2 网络安全的目标和特征

通俗地说，网络安全的主要目标是保护网络信息系统，使其没有危险，不受威胁，不出事故。在这里，可以用 5 个通俗的说法来形象地描绘网络安全的目标。

- 进不来
- 看不懂
- 改不了
- 拿不走
- 跑不掉

从技术角度来说，网络安全的目标可归纳为以下 5 个方面，也就是网络安全的 5 个基本特征。

- 可用性
- 保密性
- 完整性
- 不可否认性
- 可控性

图 1-2 给出了网络安全目标与网络安全特征之间的对应关系。

1. 可用性

可用性是指信息或者信息系统可被合法用户访问，并按其要求运行的特性。如图 1-2 所示，“进不来”、“改不了”和“拿不走”都实现了信息系统的可用性。

通常采用一些技术措施或网络安全设备来实现这些目标。例如，使用防火墙，把攻击者阻挡在网络外部，让他们“进不来”。即使攻击者进入了网络内部，由于有加密机制，会使他们既“改不了”也“拿不走”关键信息和资源。

2. 保密性

保密性是指只有经授权的个人才能访问敏感数据。保密性可防止向未经授权的个人泄

露信息，以及防止信息被加工。

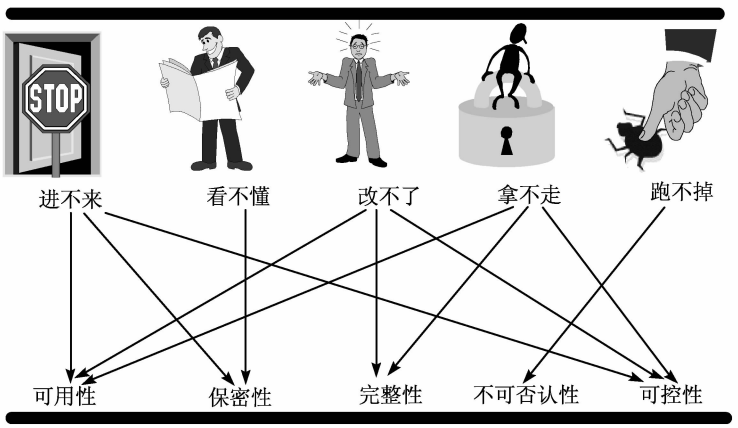

图 1-2　网络安全目标与特征的对应关系

如图 1-2 所示，“进不来”和“看不懂”都实现了信息系统的保密性，表现在：

- 使用口令对进入系统的用户进行身份鉴别，非法用户没有口令就“进不来”，这就保证了信息系统的保密性。
- 即使攻击者破解了口令，进入系统，加密机制也会使得他们“看不懂”关键信息。例如，甲给乙发送加密文件，只有乙通过解密才能读懂其内容，其他人看到的是乱码。由此便实现了信息的保密性。

3. 完整性

完整性是指防止数据未经授权而被意外改动，包括数据的插入、删除和修改等。为了确保数据的完整性，系统必须能够检测出未经授权的数据修改。其目标是使数据的接收方能够证实数据没有被改动过。

如图 1-2 所示，“改不了”和“拿不走”都实现了信息系统的完整性。使用加密机制，可以保证信息系统的完整性，攻击者无法对加密信息进行修改或者复制。

完整性与保密性不同，保密性要求信息不被泄露给未授权的人，而完整性则要求信息不会受到各种原因的破坏。

4. 不可否认性

不可否认性也叫不可抵赖性，即防止个人否认先前已执行的动作，其目标是确保数据的接收方能够确信发送方的身份。例如，接收者不能否认收到消息，发送者也不能否认发送过消息。

如图 1-2 所示，“跑不掉”就实现了信息系统的不可否认性。如果攻击者进行了非法操作，系统管理员使用审计机制或签名机制可让他们无处遁形。

5. 可控性

信息的可控性是指能够控制使用网络资源的人或主体的使用方法。对于网络系统中的敏感信息资源，如果任何主体都能访问、篡改、窃取以及恶意传播的话，安全系统显然就失去

了效用。对访问信息资源的人或主体的使用方式进行有效控制，是网络安全的必然要求。从国家层面看，网络安全的可控性不仅涉及网络资源的可控性，而且与安全产品、安全市场、安全厂商、安全研发人员的可控性紧密相关。

如图 1-2 所示，“进不来”、“改不了”和“拿不走”就实现了信息系统的可控性，这主要是通过操作系统的访问控制来实现的。

1.2.3 网络安全的技术

网络安全的内涵在不断地延伸，从最初的信息保密性发展到信息的完整性、可用性、可控性和不可否认性，进而又发展为“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）”等多方面的基础理论和实施技术。目前信息网络常用的基础性安全技术包括以下几方面的内容。

（1）访问控制：对用户访问网络资源的权限进行严格的认证和控制。例如，进行用户身份认证，对口令加密、更新和鉴别，设置用户访问目录和文件的权限，控制网络设备配置的权限，等等。

（2）数据加密：加密是保护数据安全的重要手段。加密的作用是保证信息被截获后，截获的人不能读懂其含义。

（3）网络隔离：网络隔离有两种方式，一种是采用隔离卡来实现的，一种是采用网络安全隔离网闸实现的。隔离卡主要用于对单台机器的隔离，网闸主要用于对整个网络的隔离。

隔离卡的功能是以物理方式将一台计算机虚拟为两台计算机，实现工作站的双重状态，既可在安全状态，又可在公共状态，两个状态是完全隔离的，从而使一台工作站可在完全安全状态下连接内、外网。

网闸是一种由带有多种控制功能专用硬件在电路上切断网络之间的链路层连接，并能够在网络间进行安全适度的应用数据交换的网络安全设备。

（4）主机加固技术：操作系统或数据库的实现会不可避免地出现某些漏洞，从而使信息网络系统遭受严重的威胁。主机加固技术对操作系统、数据库等进行漏洞加固和保护，提高系统的抗攻击能力。

（5）安全审计技术：包含日志审计和行为审计，通过日志审计协助管理员在网络受到攻击后查看网络日志，从而评估网络配置的合理性、安全策略的有效性，追溯分析安全攻击轨迹，并能为实时防护提供手段。通过对员工或用户的网络行为审计，确认行为的合理性，确保管理的安全。

（6）检测监控技术：对信息网络中的流量或应用内容进行数据链路层至应用层的检测并适度监管和控制，避免网络流量的滥用、垃圾信息和有害信息的传播。

（7）其他措施：其他措施包括信息过滤、容错、数据镜像、数据备份等。

1.3 网络安全的现状与威胁

随着技术的发展，网络安全的内容也在发生变化。了解当前网络安全的现状，以及存在

的主要威胁，有助于更好地进行安全防护。

1.3.1　网络安全的现状

从 1.1.4 的内容可以看到，在我国，网络侵害事件频繁发生，现在面临的网络安全问题主要包括以下几方面。

1. 信息和网络的安全防护能力较差

自 1995 年以来，多个上网工程的全面启动，我国各级政府、企事业单位、网络公司等陆续设立自己的网站，电子商务也正以前所未有的速度迅速发展，但许多应用系统安全防护能力很差，很多网站基本没有采取安全防范措施，存在着极大的信息安全风险和隐患。

2. 基础信息产业严重依靠国外

我国的信息化建设，基本上是依赖国外技术设备而装备起来的。在国际财团涌向我国信息化建设的市场，大举推销电子信息设备之时，我国却在相对缺乏知识和经验的情况下，存在着一些花钱买淘汰技术和不成熟技术的现象，这其中就潜伏着极大的网络安全隐患。

我国的计算机软件也同样面临受人遏制和封锁的威胁。虽然我国的计算机制造业有很大的进步，但其中许多核心部件都是原始设备制造商的，我国对其研发、生产的能力很弱，关键部位完全处于受制于人的地位。我国的计算机软件还面临市场垄断和价格歧视的威胁。国外厂商几乎垄断了我国计算机软件的基础和核心市场，特别是操作系统。

3. 信息安全管理机构权威性不够

目前，国家经济信息安全管理条块分割、各行其是、相互隔离，极大地妨碍了国家有关法规的贯彻执行，难以防范境外情报机构和黑客的攻击。国家在网络安全问题上缺少专门的权威性机构。网络安全相关的民间管理机构与国家信息化领导机构之间还没有充分沟通协调。

4. 全社会的网络安全意识淡薄

大多数网络用户的网络安全知识甚少，安全意识淡薄，例如，U 盘、移动硬盘、手机等存储介质的随意使用；网络管理人员缺乏必要的专业知识，不能安全地配置和管理网络；用户上网身份无法唯一识别，不能有效地规范和约束网络用户的非法访问行为；用户对自己面临的网络安全问题没有足够的认识，缺乏有效的保护。据统计，在 2009 年，仍有 4.4%的网络用户个人计算机未安装任何安全软件；不足 8%的手机网络用户安装了手机安全防护软件。

另外，网络安全领域在研究开发、产业发展、人才培养、队伍建设等方面对迅速发展的经济形势极不适应，只是作为信息化的研究分支立项，投入很少，和国外差距越来越大。

以上问题如果不能切实解决，我国的互联网安全将面临严重威胁，在激烈的信息争夺和信息战中，我国就会处于被动挨打的软弱地位。因此，充分重视互联网安全问题已迫在眉睫。

1.3.2　网络安全的威胁

网络安全威胁是指有可能访问资源并造成破坏的某个人、某个地方或某个事物。目前，计算机互联网面临的安全性威胁表现形式主要有以下几个方面。

1. 人为的无意失误

如操作员安全配置不当造成的安全漏洞，用户安全意识不强，用户口令选择不慎，以及用户将自己的账号随意转借他人或与别人共享等都会给网络安全带来威胁。

2. 系统和软件的漏洞

随着系统规模的发展和软件应用的普及，不可能做到百分之百的无缺陷和无漏洞。人们熟悉的操作系统，如 Windows 或者 UNIX 都存在着一定程度的安全漏洞，特别是 Windows 操作系统；通常使用的软件，如 Office、CAD、ICQ 等也存在着安全隐患。这些漏洞和缺陷恰恰是黑客进行攻击的首选目标，曾经出现过的黑客攻入网络内部的事件，大部分就是因为系统和软件不完善所导致的。

每月的第二个星期二，微软都会为 Windows、Office、IE 等产品发布补丁，修复漏洞，提高安全性。

3. 拒绝服务攻击

拒绝服务攻击是一种破坏性攻击，它不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序使系统响应减慢甚至瘫痪，影响用户的正常使用，甚至使合法用户被排斥而不能进入计算机网络系统或不能得到相应的服务。最早的拒绝服务攻击是“电子邮件炸弹”，它能使用户在很短的时间内收到大量电子邮件，使用户系统不能处理正常业务，严重时会使系统崩溃、网络瘫痪。

4. 计算机病毒

对于很多编程人员来说，编写一个计算机病毒是非常容易的。但是，计算机病毒的破坏性是巨大的，其危害已被人们所认识。单机病毒就已经让人们“谈毒色变”了，而通过网络传播的病毒，无论是在传播速度、破坏性，还是在传播范围等方面都是单机病毒不能比拟的。

5. 破坏数据完整性

破坏数据完整性是指以非法手段窃得对数据的使用权，删除、修改、插入或重发某些重要信息，修改、销毁或替换网络上传输的数据，重复播放某个分组序列，改变网络上传输的数据包的先后次序，以干扰用户的正常使用，使攻击者获益。

6. 陷门

陷门是指为攻击者提供“后门”的一段非法的操作系统程序。这一般是指一些内部程序人员为了特殊的目的，在所编制的程序中潜伏代码或保留漏洞。这些陷门一旦被打开，其造成的后果将不堪设想。

7. 隐蔽通道

隐蔽通道是一种允许以违背合法的安全策略的方式进行操作系统进程间通信的通道，它分为隐蔽存储通道和隐蔽时间通道。隐蔽通道的重要参数是带宽。

8. 信息泄露或丢失

信息泄露或丢失是指敏感数据在有意或无意中被泄露出去或丢失，通常包括：信息在传输中丢失或泄露（如黑客利用电磁泄漏或搭线窃听等方式截获机密信息，或通过对信息流

向、流量、通信频度和长度等参数的分析，推出有用信息，如用户口令、账号等），信息在存储介质中丢失或泄露，通过建立隐蔽通道等窃取敏感信息等。

1.4　网络安全体系结构

网络安全是一个涉及范围较广的研究领域，人们一般都只是在该领域中的一个小范围内进行研究，开发能够解决某种特殊网络安全问题的方案。例如，有人专门研究加密和鉴别，有人专门研究入侵和检测，有人专门研究黑客攻击等。网络安全体系结构就是从系统化的角度去理解这些安全问题的解决方案，这对研究、实现和管理网络安全的工具具有全局指导作用。

1.4.1　网络安全模型

最常见的网络安全模型就是 PDRR 模型。PDRR 是 protection（防护）、detection（检测）、response（响应）、recovery（恢复）的首字母组合。这 4 个部分构成了一个动态的信息安全周期，如图 1-3 所示。

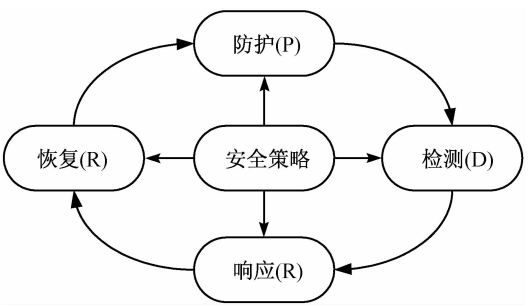

图 1-3　网络安全模型 PDRR

安全策略的每一部分都包括一组相应的安全措施来实现一定的安全功能。安全策略的第一步就是防护。根据系统已知的所有安全问题采取防护的措施，如打补丁、访问控制、数据加密等。安全策略的第二步是检测。攻击者如果穿过了防护系统，检测系统就会检测出来。检测的功能是检测出入侵者的身份，包括攻击源、系统损失等。一旦检测出有入侵，响应系统开始响应，包括事件处理和其他业务。安全策略的最后一步是系统恢复。在入侵事件发生后，把系统恢复到原来的状态。每次发生入侵事件，防护系统都要更新，保证相同类型的入侵事件不能再发生，所以整个安全策略包括防护、检测、响应和恢复，这 4 个方面组成了一个信息安全周期。

1. 防护

防护就是根据系统可能出现的安全问题采取的一些预防措施，主要包括主动防护和被动防护。通常采用的主动防护技术有数据加密、身份验证、访问控制、授权和虚拟网络（VPN）技术；被动防护技术主要有防火墙技术、安全扫描、入侵检测、路由过滤、数据备份和归档、物理安全等。

防护是 PDRR 模型中最重要的部分，通过它可以预防大多数的入侵事件。防护可分为 3 类：系统安全防护、网络安全防护和信息安全防护。系统安全防护是指操作系统的安全防护，即各个操作系统的安全配置、使用和打补丁等，不同操作系统有不同的防护措施和相应的安全工具；网络安全防护指网络管理的安全性及网络传输的安全性；信息安全防护指数据本身的保密性、完整性和可用性，数据加密就是信息安全防护的重要技术。

2. 检测

PDRR 模型的第二个环节就是检测。除掉入侵事件发生的条件，防护系统可以阻止大多数的入侵事件的发生，但它不能阻止所有的入侵，特别是那些利用新的系统缺陷、新的攻击手段的入侵。因此安全策略的第二个安全屏障就是检测，即如果入侵发生就检测出来，这个工具是入侵检测系统(IDS)。

在 PDRR 模型中，防护和检测具有互补关系。如果防护系统过硬，绝大部分入侵事件被阻止，那么检测系统的任务就会减少。

3. 响应

PDRR 模型中的第三个环节就是响应。响应就是已知一个攻击(入侵)事件发生之后，进行处理。在一个大规模的网络中，响应这个工作都是由一个特殊部门负责，那就是计算机响应小组。世界上第一个计算机响应小组 CERT，位于美国 CMU 大学的软件工程研究所(SEI)，于 1989 年建立，是世界上最著名的计算机响应小组。从 CERT 建立之后，世界各国以及各机构也纷纷建立自己的计算机响应小组。我国第一个计算机紧急响应小组 CCERT，于 1999 年建立，主要服务于中国教育和科研计算网。

入侵事件的响应可以是入侵检测系统的报警，也可以是通过其他方式的汇报。响应的主要工作也可以分为两种：第一种是紧急响应；第二种是其他事件处理。紧急响应就是当安全事件发生时采取应对措施，其他事件处理主要包括咨询、培训和技术支持。

4. 恢复

恢复是 PDRR 模型中的最后一个环节。恢复是事件发生后，把系统恢复到原来的状态，或者比原来更安全的状态。恢复也可以分为系统恢复和信息恢复两个方面。

系统恢复指的是修补该事件所利用的系统缺陷，不让黑客再次利用这样的缺陷入侵。一般系统恢复包括系统升级、软件升级和打补丁等。系统恢复的另一个重要工作是除去“后门”。一般来说，黑客在第一次入侵时都是利用系统的缺陷。在第一次入侵成功之后，黑客就在系统打开一些“后门”，如安装一个特洛伊木马。所以，尽管系统缺陷已经打补丁，黑客下一次还可以通过“后门”进入系统。系统恢复都是根据检测和响应环节提供有关事件的资料进行的。

信息恢复指的是恢复丢失的数据。数据丢失可能是由于黑客入侵造成，也可能是由系统故障、自然灾害等原因造成的。信息恢复就是从备份和归档的数据中恢复原来的数据。信息恢复过程跟数据备份过程有很大的关系。数据备份做得是否充分对信息恢复有很大的影响。信息恢复过程的一个特点是有优先级别。直接影响日常生活和工作的信息必须先恢复，这样可以提高信息恢复的效率。

1.4.2 网络安全机制

国际标准化组织(ISO)于 1989 年 2 月公布了《网络安全体系结构》，文件中规定的网络安全机制有 8 项：加密机制、数字签名机制、访问控制机制、数据完整性机制、鉴别交换机制、信息流填充机制、路由控制机制和公证机制。

1. 加密机制

数据加密是提供信息保密的主要方法，可保证数据存储和传输的保密性。此外，加密技

术和其他技术结合使用，可保证数据的完整性。

2. 数字签名机制

数字签名可解决传统手工签名中存在的安全缺陷，在电子商务中应用较广泛。数字签名主要解决否认问题（发送方否认发送了信息）、伪造问题（某方伪造了文件却不承认）、冒充问题（冒充合法用户在网上发送文件）和篡改问题（接收方私自篡改文件内容）。

3. 访问控制机制

访问控制机制用来控制哪些用户可以访问哪些资源，对这些资源可以访问到什么程度。例如，非法用户企图访问资源，该机制就会加以拒绝，并将这一非法事件记录在审计报告中。访问控制机制可以直接支持数据的保密性、完整性和可用性，作用非常明显。

4. 数据完整性机制

数据完整性机制保护网络系统中存储和传输的软件（程序）和数据不被非法改变，如被添加、删除和修改等。

5. 鉴别交换机制

鉴别交换机制主要是通过相互交换信息来确定彼此的身份。在计算机网络中，鉴别主要有站点鉴别、报文鉴别、用户和进程的认证等。通常采用口令、密码技术、实体的特征或所有权等手段进行鉴别。

6. 信息流填充机制

攻击者对传输信息的长度、频率等特征进行统计，然后进行信息流量分析，即可从中得到有用的信息。采用信息流填充技术，可保持系统信息量基本恒定，因此能防止攻击者对系统进行信息流量分析。

7. 路由控制机制

路由控制机制可以指定通过网络发送数据的路径，以便选择可信度高的结点传输信息。

8. 公证机制

公证机制就是在网络中设立一个公证机构来中转各方交换的信息，并从中提取相关证据，以便对可能发生的纠纷作出仲裁。

1.4.3　网络安全策略

安全策略是指在一个特定的环境里，为保证提供一定级别的安全保护所必须遵守的规则。制订网络安全策略的目的是决定一个计算机网络的组织结构怎样来保护自己的网络及其信息。一般来说，安全策略包括两个部分：一个总体的策略和具体的规则。总体的策略用于阐明安全策略的总体思想；而具体的规则用于说明什么活动是被允许的，什么活动是被禁止的。

1. 网络安全策略的等级

网络安全策略可分为以下 4 个等级：

(1)内部网络和外部网络不相连，因此一切都被禁止。

(2)除那些被明确允许的之外，一切都被禁止。

(3)除那些被明确禁止的之外，一切都被允许。

(4)一切都被允许,当然也包括那些本来被禁止的。

可以根据实际情况,在这 4 个等级之间找出符合实际需要的安全策略。当系统自身的情况发生变化时,必须注意及时修改相应的安全策略。

2. 网络安全策略的内容

一个好的网络安全策略应包括如下内容。

1)网络用户的安全责任

该策略可以要求用户每隔一段时间更改其口令;使用符合安全标准的口令形式;执行某些检查,以了解其账户是否被别人访问过。

2)系统管理员的安全责任

该策略可以要求在每台计算机上使用专门的安全措施,登录用户名称,检测和记录过程等,还可以限制在网络连接中所有的主机不能运行应用程序。

3)正确利用网络资源

规定谁可以使用网络资源,他们可以做什么,不可以做什么等。对于 E-mail 和计算机活动的历史,应受到安全监视,并告知有关人员。

4)检测到网络安全问题时的对策

当检测到网络安全问题时,应做什么,应该通知什么部门,这些问题都要明确。

3. 网络安全策略的手段

从技术上,网络安全策略涉及 4 个方面:物理安全策略、访问控制策略、信息加密策略、网络安全管理策略。

1)物理安全策略

物理安全策略的目的是保护计算机系统、网络服务器、打印机等硬件实体和通信线路免受自然灾害、人为破坏和搭线攻击;验证用户的身份和使用权限,防止用户越权操作;确保计算机系统有一个良好的电磁兼容工作环境;建立完备的安全管理制度,防止非法进入计算机控制室和各种偷窃、破坏活动的发生。

2)访问控制策略

访问控制是网络安全防范和保护的主要策略,它的主要任务是保证网络资源不被非法使用和非常访问。它也是维护网络系统安全、保护网络资源的重要手段。各种安全策略必须相互配合才能真正起到保护作用,但访问控制可以说是保证网络安全最重要的核心策略之一。

3)信息加密策略

信息加密的目的是保护网内的数据、文件、口令和控制信息,保护网上传输的数据。

密码技术是网络安全最有效的技术之一。加密网络,不但可以防止非授权用户的搭线窃听和入网,而且也是对付恶意软件的有效方法之一。

4)网络安全管理策略

在网络安全中,除了采用上述技术措施之外,加强网络的安全管理,制订有关规章制度,对于确保网络安全、可靠地运行,也起到十分有效的作用。

1.4.4 网络安全防范体系结构及其设计原则

为了更好、更有效地实施网络安全策略,要掌握网络安全防范体系的层次结构及其设计原则。

1. 网络安全防范体系结构

全方位的、整体的网络安全防范体系也是分层次的，不同层次反映了不同的安全问题。根据网络的应用现状和网络的结构，可以将网络安全防范体系划分为物理层安全、系统层安全、网络层安全、应用层安全和安全管理 5 个层次。

1）物理层安全

该层次的安全包括通信线路的安全、物理设备的安全、机房的安全等。物理层的安全主要体现在通信线路的可靠性（线路备份、网络管理软件、传输介质）、软硬件设备安全性（替换设备、拆卸设备、增加设备）、设备的备份、防灾害能力、防干扰能力、设备的运行环境（温度、湿度、烟尘）、不间断电源保障等。

2）系统层安全

该层次的安全问题来自网络内使用的操作系统的安全，主要表现为 3 个方面：一是操作系统本身的缺陷带来的不安全因素，主要包括身份认证、访问控制、系统漏洞等；二是对操作系统的安全配置问题；三是病毒对操作系统的威胁。

3）网络层安全

该层次的安全问题主要体现在网络方面的安全性，包括网络层身份认证、网络资源的访问控制、数据传输的保密性与完整性、远程接入的安全、域名系统的安全、路由系统的安全、入侵检测的手段、网络设施防病毒等。

4）应用层安全

该层次的安全问题主要由提供服务所采用的应用软件和数据的安全性产生，包括 Web 服务、电子邮件系统、DNS 等。此外，还包括病毒对系统的威胁。

5）安全管理

安全管理包括安全技术和设备的管理、安全管理制度、部门与人员的组织规则等。管理的制度化极大程度地影响着整个网络的安全，严格的安全管理制度、明确的部门安全职责划分、合理的人员角色分配都可以在很大程度上降低其他层次的安全漏洞。

2. 网络安全防范体系设计原则

根据防范安全攻击的安全需求、需要达到的安全目标、对应安全机制所需的安全服务等因素，综合考虑可实施性、可管理性、可扩展性、综合完备性、系统均衡性等方面，网络安全防范体系在整体设计过程中应遵循以下 9 项原则。

1）网络信息安全的木桶原则

网络信息安全的木桶原则是指对信息均衡、全面地进行保护。“木桶的最大容积取决于最短的一块木板”，网络信息系统是一个复杂的计算机系统，它本身在物理上、操作上和管理上的种种漏洞构成了系统安全的脆弱性，尤其是多用户网络系统自身的复杂性、资源共享性使单纯的技术保护防不胜防。攻击者使用的“最易渗透原则”，必然在系统中最薄弱的地方进行攻击。因此，充分、全面、完整地对系统的安全漏洞和安全威胁进行分析、评估和检测（包括模拟攻击）是设计信息安全系统的必要前提条件。安全机制和安全服务设计的首要目的是防止最常用的攻击手段，根本目的是提高整个系统的“安全最低点”的安全性能。

2）网络信息安全的整体性原则

网络信息安全的整体性原则要求在网络被攻击、破坏的情况下，必须尽可能地快速恢复网络信息中心的服务，减少损失。

3)安全性评价与平衡原则

对于任何网络,绝对安全难以达到,也不一定是必要的,所以需要建立合理的实用安全性和用户需求评价与平衡体系。安全体系设计要正确处理需求、风险与代价的关系,做到安全性与可用性相容,做到组织上可执行。评价信息是否安全,没有绝对的评判标准和衡量指标,只能决定于系统的用户需求和具体的应用环境,具体取决于系统的规模和范围、系统的性质和信息的重要程度。

4)标准化与一致性原则

网络安全体系的设计必须遵循一系列的标准,这样才能确保各个分系统的一致性,使整个系统安全地互连互通、信息共享。

5)技术与管理相结合原则

网络安全体系是一个复杂的系统工程,涉及人、技术、操作等要素,单靠技术或单靠管理都不可能实现。因此,必须将各种网络安全技术与运行管理机制、人员思想教育与技术培训、网络安全规章制度相结合。

6)统筹规划,分步实施原则

由于政策规定、服务需求的不明朗以及环境、条件、时间的变化,攻击手段的进步,安全防护不可能一步到位,可在一个比较全面的安全规划下,根据网络的实际需要,先建立基本的安全体系,保证基本的、必需的安全性。今后随着网络规模的扩大和应用的增加以及网络应用和复杂程度的变化,网络脆弱性也会不断增加。所以,必须调整或增强安全防护力度,以保证整个网络最根本的安全需求。

7)等级性原则

等级性原则是指安全层次和安全级别。良好的信息安全系统必然是分为不同等级的,包括对信息保密程度分级,对用户操作权限分级,对网络安全程度分级(安全子网和安全区域),对系统实现结构的分级(应用层、网络层、数据链路层等),从而针对不同级别的安全对象,提供全面、可选的安全算法和安全体制,以满足网络中不同层次的各种实际需求。

8)动态发展原则

要根据网络安全的变化不断调整安全措施,适应新的网络环境,满足新的网络安全需求。

9)易操作性原则

首先,安全措施需要人去完成,如果措施过于复杂,对人的要求过高,本身就降低了安全性。其次,措施的采用不能影响系统的正常运行。

由于互联网的开放性和通信协议的安全缺陷,以及在网络环境中数据信息存储和对其访问与处理的分布性特点,网上传输的数据信息很容易被泄露或破坏,网络受到的安全攻击非常严重,因此,建立有效的网络安全防范体系就更为迫切。实际上,保障网络安全不但需要参考网络安全的各项标准以形成合理的评估准则,更重要的是必须明确网络安全的框架体系、安全防范的层次结构和系统设计的基本原则,分析网络系统的各个不安全环节,找到安全漏洞,做到有的放矢。

1.5　网络安全的管理

针对以上所提到的网络安全问题，为了保护网络信息的安全可靠，除了要对网络安全进行等级划分外，还要运用法律手段对网络用户进行强制约束。

1.5.1　网络安全的等级与标准

计算机信息系统安全产品种类繁多，功能也各不相同，为了更好地对其安全性进行客观评价，满足用户对安全功能和保护措施的多种需求，也便于同类安全产品进行比较，许多国家都分别制定了各自的信息安全标准。典型的信息安全标准主要有美国国防部颁布的《可信计算机系统评估准则》，欧洲的德国、法国、英国、荷兰 4 国联合颁布的《信息技术安全评价准则》，加拿大颁布的《可信计算机产品评价准则》，以及我国国家质量监督局颁布的《计算机信息系统安全保护等级划分准则》。这里简单介绍美国的《可信计算机系统评估准则》和我国的《计算机信息系统安全保护等级划分准则》。

1. 美国的《可信计算机系统评估准则》

为了帮助计算机用户区分和解决计算机网络安全问题，美国国防部颁布了“橘皮书”，其正式名称为《可信计算机系统评估准则》(trusted computer system evaluation criteria，TCSEC)，对用户计算机系统安全级别的划分进行了规定。

橘皮书将计算机安全由低到高分为 4 类 7 级，即 D、C(C1、C2)、B(B1、B2、B3)和 A 四部分。知道这些分类有助于了解在一些系统中固有的各种安全风险，并能洞悉如何减少或排除这些风险。

1)D 级别

D 级别是计算机安全的最低级，不要求用户进行用户登录和密码保护，任何人都可以使用，整个系统是不可信任的，硬件、软件都容易被侵袭。早期的操作系统大多属于该级别，如微软的 DOS、Windows 98。

2)C 级别

C 级别有两个子系统，C1 级和 C2 级。

C1 级称为选择性保护级，可以实现自主安全防护，对用户和数据进行分离，保护或限制用户权限的传播。

C2 级称为访问控制环境保护级，比 C1 的访问控制划分得更为详细，能够实现受控安全保护、个人账户管理、审计和资源隔离。这个级别的系统包括 UNIX、Linux 和 Windows NT。

C 级别属于自由选择性安全保护，在设计上具有自我保护和审计功能，可对主体行为进行审计与约束。C 级别的安全策略主要是自主存取控制，可以实现：

- 保护数据，确保非授权用户无法访问。
- 对存取权限的传播进行控制。
- 个人用户数据的安全管理。

3)B 级别

B 级别包括 B1、B2 和 B3 三个级别，B 级别能够提供强制性安全保护和多级安全。强制

防护是指定义和保持标记的完整性，信息资源的拥有者不具有更改自身的权限，系统数据完全处于访问控制管理的监督下。

B1 级称为标记安全保护级，对网络上的每一个对象都实施保护；支持多级安全，对网络、应用程序工作站实施不同的安全策略；对象必须在访问控制之下，不容许用户自己改变所属资源的权限。B1 级计算机系统的主要用户是政府机构和防护承包商。

B2 级称为结构化保护级，对网络和计算机系统中所有对象都加以定义，给一个固定标签；为工作站、终端、磁盘驱动器等设备分配不同的安全级别；按照最小特权原则取消权力无限大的特权用户；任何一个用户都不能享有操作和管理计算机的全部权力。

B3 级称为安全域级，要求用户工作站或终端必须通过信任的途径连接到网络系统内部的主机上；采用硬件来保护系统的数据存储区；根据最小特权原则，增加了系统安全员，将系统管理员、系统操作员和系统安全员职责隔离，将人为因素对计算机安全的威胁降至最小。

4）A 级别

A 级别称为验证设计级，是目前最高的安全级别。在 A 级别中，安全的设计必须给出形式化设计说明和验证，需要有严格的数学推导过程，同时应该包含隐蔽信道和可信分布的分析，也就是说要保证系统的部件来源有安全保证，例如，对这些软件和硬件在生产、销售、运输中进行严密跟踪和严格的配置管理，以避免出现安全隐患。

综上所述，D 级是不具备最低安全限制的等级；C1 级和 C2 级是具备最低安全限制的等级；B1 级和 B2 级是中等安全保护能力的等级，基本可以满足一般的重要应用的安全要求；B3 级和 A 属于最高安全等级，其成本增加很多，只有极其重要的应用才需要使用这种安全等级的系统。

2. 我国信息安全等级与评价标准

我国根据 1999 年 10 月经过国家质量技术监督局批准颁布的《计算机信息系统安全保护等级划分准则》，将计算机安全保护划分为以下 5 个级别。

（1）第一级为用户自主保护级，它的安全保护机制使用户具备自主安全保护的能力，保护用户的信息免受非法的读写破坏。

（2）第二级为系统审计保护级，除具备第一级所有的安全保护功能外，要求创建和维护访问的审计跟踪记录，使所有用户对自己行为的合法性负责。

（3）第三级为安全标记保护级，除继承前一个级别的安全功能外，还要求以访问对象标记的安全级别限制访问者的访问权限，实现对访问对象的强制保护。

（4）第四级为结构化保护级，在继承前面安全级别安全功能的基础上，将安全保护机制划分为关键部分和非关键部分。其中关键部分直接控制访问者对访问对象的存取，从而加强系统的抗渗透能力。

（5）第五级为访问验证保护级，这个级别特别增设了访问验证功能，负责仲裁访问者对访问对象的所有访问活动。

1.5.2 网络安全的法律与法规

对网络安全的保护，不仅取决于技术的进步，而且依赖于社会法律、法规的完善。

我国政府对信息安全和网络安全问题十分关注，积极推动网络安全管理和安全立法工

作。近几年，陆续颁布了《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际联网管理暂行规定》、《计算机信息网络国际联网安全保护管理办法》、《中国互联网络域名注册暂行管理办法》、《中国互联网域名注册实施细则》等法规性文件，并在新刑法中明确了计算机犯罪与计算机违法行为的区别，从而为我国的网络安全管理提供了法律依据。

1. 计算机信息系统安全保护

为了保护计算机信息系统的安全，促进计算机的应用和发展，保障社会主义现代化建设的顺利进行，国务院于 1994 年 2 月 18 日发布了《中华人民共和国计算机信息系统安全保护条例》(简称《条例》)，要求计算机信息系统的安全保护应当保障计算机及其相关的和配套的设备、设施(含网络)的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。

《条例》规定，计算机信息系统的建设和应用，应当遵守法律、行政法规和国家其他有关规定。计算机信息系统实行安全等级保护。安全等级的划分标准和安全等级保护的具体办法，由公安部门会同有关部门制订。计算机机房应当符合国家标准和国家有关规定。在计算机机房附近施工，不得危害计算机信息系统的安全。运输、携带、邮寄计算机信息媒体进出境的，应当如实向海关申报。计算机信息系统的使用单位应当建立健全安全管理制度，负责本单位计算机信息系统的安全保护工作。

2. 计算机信息网络国际联网安全保护

为了加强对计算机信息网络国际联网的安全保护，维护公共秩序和社会稳定，对境内的计算机网络国际联网安全保护管理，国家制定了《中华人民共和国计算机信息网络国际联网管理暂行规定》和《计算机信息网络国际联网安全保护管理办法》，对从事国际联网业务作了以下规定：

(1)任何单位和个人不得利用国际互联网危害国家安全、泄露国家秘密，不得侵犯国家的、社会的、集体的利益和公民的合法权益，不得从事违法犯罪活动。

(2)任何单位和个人不得利用国际联网制作、复制、查阅和传播下列信息。

- 煽动抗拒、破坏宪法和其他法律、行政法规实施的。
- 煽动颠覆国家政权，推翻社会主义制度的。
- 煽动分裂国家，破坏国家统一的。
- 煽动民族仇恨、民族歧视，破坏民族团结的。
- 捏造或歪曲事实，散布谣言，扰乱社会秩序的。
- 宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖、教唆犯罪的。
- 公然侮辱他人或者捏造事实诽谤他人的。
- 损害国家机关信誉的。
- 其他违反宪法和法律、行政法规的。

(3)任何单位和个人不得从事下列危害计算机信息网络安全的活动。

- 未经允许，进入计算机信息网络或者使用计算机信息网络资源的。
- 未经允许，对计算机信息网络功能进行删除、修改或者增加的。
- 未经允许，对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、修

改或者增加的。

• 故意制作、传播计算机病毒等破坏性程序的。

• 其他危害计算机信息网络安全的。

3.《刑法》对计算机信息安全保护的相关条文规定

1997 年 10 月 1 日起施行的新修订的《中华人民共和国刑法》中的第 285 条、第 286 条和第 287 条中专门就计算机犯罪进行了规定。

(1)违反国家规定,侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的,处三年以下有期徒刑或者拘役。

(2)违反国家规定,对计算机信息系统功能进行删除、修改、增加、干扰,造成计算机信息系统不能正常运行,后果严重的,处 5 年以下有期徒刑或者拘役;后果特别严重的,处五年以上有期徒刑。违反国家规定,对计算机信息系统中存储、处理或者传输的数据和应用程序进行修改、增加的操作,后果严重的,依照前款的规定处罚。故意制作、传播计算机病毒等破坏性程序,影响计算机系统正常运行,后果严重的,依照第一款的规定处罚。

(3)利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家机密或者其他犯罪的,依照本法有关规定定罪处罚。

习 题 1

一、名词解释

网络安全　数据的完整性　网络信息安全的木桶原则

二、填空题

1. 网络安全的特征有_____、_____、_____、_____、_____。

2. TCSEC 将安全分为 7 个安全级别,从低到高依次为_____、_____、_____、_____、_____、_____、_____、_____。

3. 在 PDRR 模型中,一个安全周期包括_____、_____、_____、_____。

三、简答题

1. 网络安全的相关技术有哪些?

2. 网络安全机制主要包括哪些?

3. 网络安全防范体系有哪些设计原则?

4. 请说出国内外网络安全的评价标准。

第 2 章　计算机网络实体安全

知识目标

◎ 了解网络环境中对机房、供电系统、接地系统、监控系统、空调系统的要求
◎ 了解防火、防水、防电磁干扰、防雷击在网络实体安全中的重要性
◎ 了解静电防护与电磁辐射防护的基本方法

技能目标

◎ 掌握保护存储介质和数据的方法

计算机网络实体安全是指要保护计算机设备、计算机系统、网络服务器、网络设备等硬件实体和通信线路设施(含网络)免遭人为破坏、搭线攻击、地震、水灾、火灾、有害气体和其他环境事故(如电磁干扰等)破坏的措施和过程。

保证计算机网络的实体安全,是整个计算机网络系统安全的前提。如果实体安全得不到保证,则整个计算机网络系统的安全就不可能实现。

2.1　计算机网络环境安全

随着技术的发展,计算机网络硬件设备和存储介质的质量和可靠性不断提高,然而,计算机网络硬件设备是由大量电子设备和机械设备组成的,这些设备易受温度、供电、电磁场、自然灾害等环境条件的影响。因此,良好(安全)的环境条件是计算机网络可靠安全运行的重要因素之一。

2.1.1　机房环境

机房是信息系统的中枢,只有构建一个高可用性的整体机房环境,才能保证系统软硬件和数据免受外界因素的干扰,消除环境因素对信息系统造成的影响。计算机网络通信系统的运行环境应按照国家有关标准设计实施,应具备消防报警、安全照明、不间断供电、温度和湿度控制系统、防盗报警,以保护系统免受水、火、有害气体、地震、静电的危害。

要实现安全的机房环境应从以下几个方面进行考虑。

1. 计算机机房的位置

计算机机房的设计应考虑减少无关人员进入机房的机会。同时,机房应避免靠近公共区域,避免窗户直接邻街,应安排机房在内,辅助工作区域在外。机房的位置要满足以下几点:

(1)良好的自然环境。周围无大工厂、震动源和易燃易爆品仓库等,以免有强大的电磁干扰、噪声、震动及污染等。

(2)机房周围有安全保障。设置多层屏障、围墙、栅栏和安全入口等,防止非法暴力入侵。

(3)安装监视和报警装置。在机房内通风孔、隐蔽地方安装监视和报警装置,用于监视和检测入侵者,预报意外灾害等。

(4)机房装饰。采用防静电活动地板,防尘和非易燃材料墙面,封闭门窗或双层密封玻璃等。

2.机房的出入管理

应对计算机及其网络系统的实体访问进行控制,即对内部或外部人员出入场所进行限制。根据工作需要,对每个工作人员可进入的区域应予以规定,而且各个区域应有明显的标记或派专人值守。最好能做到出入验证和出入管理。

(1)出入验证:通过特殊标志、口令、指纹、通行证等对进入人员进行识别和验证。

(2)出入管理:制订完善的安全出入管理制度,关键通道加锁和设置警卫,防止非法用户进入。

3.机房温度、湿度

计算机系统内有许多集成电路器件,不仅发热量大,而且对高温、低温敏感。温度过高,会导致器件性能不稳定,存储信息的磁介质损坏,信息丢失;温度过低,设备表面容易结露,潮湿导致设备绝缘不好,机器锈蚀。另外,机房内空气的湿度也对计算机系统有很重要的影响。湿度过高,使电路和元器件的绝缘性能变差,机器金属生锈,影响磁头的高速运转,降低磁介质强度;湿度过低,易于产生静电。因此,对于一个合格的计算机机房,一定要保持一个合适的温度和湿度范围。

根据《电子信息系统机房设计规范》GB 50174－2008 国家标准,计算机机房内的温度、湿度应满足下列要求:

(1)开/关机时计算机机房内的温度、湿度,应符合表 2-1 的规定。

表 2-1 主机房开/关机时温度、湿度要求

级别项目	技术要求			备 注
	A	B	C	
主机房温度(开机时)	23℃±1℃		18℃～28℃	不得结露
主机房相对湿度(开机时)	40%～55%		35%～75%	
主机房温度(停机时)	5℃～35℃			
主机房相对湿度(停机时)	40%～70%		20%～80%	

4.机房的空气洁净度

灰尘会造成机器接插件接触不良、发热元器件散热效率降低、电子元件的绝缘性能下降等;增加机械磨损,尤其对驱动器和盘片;使磁盘数据的读写出现错误,而且可能划伤盘片,甚至导致磁头损坏。因此必须采取防尘、除尘的措施,保持机房内的清洁卫生。《电子信息系统机房设计规范》GB 50174—2008 国家标准规定主机房内的空气含尘浓度,在静态条件

下测试，每升空气中大于或等于 0.5 μm 的尘粒数，应少于 18 000 粒。

保证机房的空气洁净的措施如下：

(1)保证机房气流组织的合理性。气流组织如被破坏，不但室内的温度分布受影响，而且因为涡流过多使墙角、地面附近的不清洁气流扩散到室内工作区。

(2)保证对机房空气进行二级过滤，要加强净化空调的管理。工作人员应遵守制度和操作规程，保证室内的卫生及净化要求。

(3)经常或按期清洗、更换空气过滤器。

(4)定期测定室内的含尘量。

2.1.2　供电系统与接地系统

电源是计算机网络系统的命脉，电源系统电压的波动或突然断电等意外事件的发生可能会使系统不能正常工作或存储的信息丢失、存储设备损坏等。

要保证计算机设备、场地设备和辅助用电可靠运行，一个完善的计算机供电系统是先决条件。为保证计算机系统安全可靠地运行，必须有可靠的电源和具有高抗干扰能力的供配电系统供电。

1. 供配电系统

供电电源设备的容量应具有一定的余量，所提供的功率一般应是全部设备负载的 125%。计算机机房最好采取专线供电，应该与其他用电设备(如空调、照明等)分开，至少应从变压器单独输出一路给计算机使用。

为保证设备的用电质量和用电安全，电源至少应该有两路供电，并应有自动转换开关，当一路供电有问题时，可迅速切换到备用线路供电。应安装备用电源(如长时间不间断电源)，停电后可供电 8 小时或更长时间。关键的设备应以柴油发电机组作为备用电源。

同时为防止、限制瞬态过压和引导浪涌电流，应配备电涌保护器(过压保护器)。为防止保护器的老化、寿命终止或雷击时造成的短路，在电涌保护器的前端应有诸如熔断器等过电流保护装置。

浪涌电流指电源接通瞬间，流入电源设备的峰值电流。

2. 照明系统

计算机机房的照明分为工作照明、事故照明和安全疏散照明。工作照明是指整个场所的均匀照明，根据规范要求照度为 300～500 lx。事故照明是为正常照明断电后及时处理余留工作而设置的照明，其照度为工作照明的 1/10，平时它也是工作照明的一部分。安全疏散照明是在机房内设置疏散方向指示灯和安全出口指示灯，其照度不低于 0.5 lx。不同性质的照明灯具分别归入不同的供电回路。其中，事故照明和安全疏散照明需要按工程中的最高负荷级别供电，并且应在灯具内配置蓄电池。

3. 接地系统

计算机机房的接地系统一般有交流工作接地、交流保护接地、防雷保护接地、屏蔽接地、

防静电接地(这 5 种接地归纳为联合接地系统)和计算机系统直流接地等几种。

在场地允许的情况下,国内普遍采用直流接地与其他接地分开的做法。联合接地系统,即利用建筑物基础钢筋网形成接地体。另在建筑物基础 20 m 以外单独设置人工接地体作为计算机系统直流接地体,接地电阻应依不同计算机系统的要求而定。联合接地系统内的各个接地系统均应采用一根或几根接地母线单点与接地体相联结,以避免各种接地系统之间的影响。交流工作接地和保护接地是采用热镀锌扁钢作为接地母线。防雷接地系统可利用建筑物的柱内钢筋作为接地引下线。屏蔽接地、防静电接地和直流接地均应采用大截面绝缘屏蔽铜芯导线为接地母线。机房内所需各个接地系统的接地母线应不少于两处。

做好防静电工作的最有效措施就是要有良好的接地,有一个连续的竖向接地排,并在机房活动地板下设置等电位的接地网络或闭合的接地铜排环,铜排面积不小于 100 mm^2;最后用绝缘导线把所有应防静电的器具构件与就近的铜排相连,如计算机设备外壳、导静电地板及支架、导静电桌椅和所有金属管件。

2.1.3 环境设备监控系统

环境设备监控系统主要是对机房设备(如供配电系统、UPS 电源、防雷器、空调系统、消防系统等)的运行状态、温度、湿度,供电的电压、电流、频率以及配电系统的开关状态、测漏系统等进行实时监控并记录数据,为机房的高效管理和安全运行提供有力的保证。

1. 图像监控系统

机房图像监控系统是建立机房安全防范机制不可缺少的环节。它能 24 小时监视并记录下机房内发生的任何事件。

机房中有大量的服务器及机柜、机架。在监控布点时,每一排机柜之间安装摄像机。如果机房有多个房间的话,应在 UPS 房和控制机房内安装摄像机。

2. 门禁管理系统

安装门禁管理系统的主要目的是保证重要区域设备和资料的安全,便于人员的合理流动,对进入这些重要区域的人员实行各种方式的门禁管理,以便限制人员随意进出。

3. 环境监控系统

(1)安装漏水检测系统。机房的水害来源主要有:机房顶棚漏水、机房地面由于上下水管道堵塞造成漏水、空调系统排水管设计不当或损坏漏水、空调系统保温不好形成冷凝水。机房水患影响机房设备的正常运行甚至造成机房运行瘫痪。因此,机房漏水检测是机房建设和日常运行管理的重要内容之一,应安装漏水自动检测报警系统。

(2)安装温感、烟感报警系统,以避免火灾。

(3)安装温度、湿度计,以便于检查。

2.1.4 空调系统

机房中的设备在运行中散热量大而且集中,散湿量极小。即机房设备散热量的 95%是显热,热量大、湿量小,热湿比大。在这种情况下,空气处理可作为一个等湿降温过程。此外,因为计算机设备、网络设备 24 小时不间断运行,所以需要空调系统也应 24 小时不间断地运行。

同时，根据机房的围护结构（主要是墙体、顶面、地面，包括楼层、朝向、外墙、内墙及墙体材料，门窗型式、单双层结构及缝隙、散热）特点、人员的发热量，照明灯具的发热量，新风负荷等各种因素，计算出计算机机房所需的制冷量，据此选定空调的容量。

（1）计算机机房应采用专用空调设备，若与其他系统共用时，应保证空调效果和采取防火措施。空调系统的主要设备应有备份，空调设备在能量上应有一定的余量。应尽量采用风冷式空调设备，空调设备的室外部分应安装在便于维修和安全的地方。空调设备中安装的电加热器和电加湿器应有防火护衬，并尽可能使电加热器远离用易燃材料制成的空气过滤器。空调设备的管道、消声器、防火阀接头、衬垫以及管道和配管用的隔热材料应采用难燃材料或非燃材料。

（2）安装在活动地板上及吊顶上的送、回风口应采用难燃材料或非燃材料。新风系统应安装空气过滤器，新风设备主体部分应采用难燃材料或非燃材料。

2.2　自然与人为灾害的防护

自然与人为灾害的防护就是要保护计算机网络设备、设施以及其他媒体，免遭地震、水灾、火灾等环境事故和人为操作失误或错误及各种计算机犯罪行为而导致的破坏。

2.2.1　防火

防火主要做到以下几点：

（1）根据《建筑设计防火规范》和《计算站场地安全要求》的规定，合理设定主机房的耐火等级，但不应低于二级，应单独设立防火分区，分隔墙要使用防火墙，应有两个以上安全出口。

（2）装饰和建筑材料应使用难燃或非燃材料，能防潮、防火、吸音、不起尘、抗静电，尽量不使用地毯，而使用活动地板。

（3）不要在计算机系统的电源线上接有负荷变化的空调系统等电气设备。

（4）水平电缆沟要采取防潮和防鼠咬措施，并分层敷设强弱电线路，电缆管道在穿过墙壁和楼板时都应设置不燃烧体隔板，穿墙电缆应套金属管，缝隙应用非燃材料封堵。

（5）普通线路也应设在不燃结构内，电线接点应做镀铅锡处理或使用压线冒连接，最好不要绞接。

（6）有暖气装置的机房，沿机房地面周围应设排水沟，应注意对暖气管道定期检查和维修。

（7）配置灭火器应选用磷酸铵盐干粉灭火器、碳酸氢钠干粉灭火器、卤代烷灭火器或二氧化碳灭火器，严禁使用自动喷淋系统。

机房电器设备多，通信容量大，一旦发生火灾，修复难度大，经济损失大，是防火重点部位。防火要做到“人防、物防、技防”三结合。

（1）把好管理责任关。要把机房防火摆上管理的重要议程，严格管理。要落实逐级防火安全责任制，责任到人，严防失职引发火灾。

（2）把好线路敷设关。应采用阻燃型或耐火型的电源线，并加护套保护，穿越机房的管线应暗设。电源线与信号线不能同槽或交叉敷设。

(3)把好可燃物清除关。机房严禁使用易燃材料装修。机房内不得使用可燃用具。要彻底清理机房内使用的木柜、木桌等可燃物。

(4)把好机房封闭关。机房内各通信要害部位的所有孔洞都要进行防火封堵处理。电缆井、管道井应在每层楼板处用阻燃密封,通向其他房间的地槽、墙上孔洞、已装放电缆的墙体孔隙要采用阻燃材料封隔。凡近期不使用的孔洞均应用阻燃材料封闭。

(5)把好外电侵入关。要强化预防外部强电、雷电侵入引发火灾,经常检查,加强监控,及时发现事故苗头,及时排除隐患。

(6)把好消防设施关。机房应装置火灾自动报警、湿度自动报警和气体灭火系统,同时还要配置气体灭火器、防毒面具等,以防患于未然。

(7)把好烟火管理关。机房内严禁抽烟。机房施工中,要切实加强明火管理和随工管理。需要明火作业的,必须由保卫部签发动火证,落实防火措施后方可施工,施工结束时彻底消除火种。

(8)把好消防教育、演练关。要定期对员工进行消防安全教育,增强防火意识,掌握防火灭火知识技能。机房一旦发生火灾,要立即关闭空调,切断着火部位电源,一边报警,一边组织扑救,以尽量避免和减少损失。

(9)把好防火检查关。要严格执行《机关、团体、企业、事业单位消防安全管理规定》,做好每日的防火巡查,及时发现并消除火灾隐患,做好巡查记录。

2.2.2 防水

水患轻者造成机房设备受损,降低使用寿命;重者造成机房运行瘫痪。因此,计算机机房水害的防护是机房建设及日常营运管理的重要内容之一。

防水主要做到以下几点:

(1)在机房内除安装空调设备外,一般不得安装其他水源。

(2)机房的墙壁、天花板和地板不能有渗水、浸水的现象。

(3)防止机房所有的门、窗和馈线进出口雨水渗入。

(4)防止空调设备冷凝水漏在机房里。

(5)机房内不能有水管穿越。

(6)不能用洒水式消防器材。

2.2.3 防电磁干扰

计算机及网络系统和其他电子设备一样,工作时会产生电磁发射,电磁发射可被高灵敏度的接收设备接收并进行分析、还原,造成系统信息泄露。另一方面,计算机及其网络系统又处在复杂的电磁干扰的环境中,这种电磁干扰有时很强,会增加电路噪声,导致电子元器件产生错误动作,严重时将导致系统不能正常工作。

电磁防护的主要目的是通过屏蔽、隔离、滤波、吸波、接地等措施,提高计算机及网络系统和其他电子设备的抗干扰能力,使之能抵抗电磁干扰;同时将计算机的电磁发射降到最低。

为了防止电磁干扰对计算机设备的影响,在机房建设时就要注意以下几个问题:

(1)为了防止在混凝土板内埋设的电力配线产生电磁干扰,机房施工时,在墙内埋设的

各种电器配线应穿金属管，且管壁不能太薄。使用蛇皮管时，要尽量减少接头，并使接头互相嵌入深一些。总之，穿线管的接头除了采用螺丝式以外，不得使用其他形式的连接，这是为了避免接头部位变成高磁阻，失去屏蔽效果，并使该非连续接头部位产生的漏磁通在室内形成磁场，导致各种干扰。同时混凝土内各种配线严禁裸埋。

(2)在室内尽量减少在混凝土内埋设配线，使更多的电缆、电线、信号线敷设在地板下和吊顶上。

(3)机房内使用的所有电力线和信号线都要使用电磁屏蔽线，并穿钢管或蛇皮管。钢管和蛇皮管的使用方法同上。

(4)机房内配线尽量不作环形配线，而采用辐射配线。

(5)对机房内的主要设备或主要区域进行屏蔽，可以有效地抑制电磁信息向外泄漏，衰减外部强电磁干扰，保护内部的设备、器件或电路，使其能在恶劣的电磁环境下正常工作。屏蔽体一般用导电和导磁性能较好的金属板制成。

(6)建立良好的接地系统。接地不仅可以起到保护作用，而且可使屏蔽体、滤波器等集聚的电荷迅速排放到大地，从而减小干扰。

2.2.4　防雷击

雷电能量非常大，闪电直接击中架空在野外的电源线、电话线或天线，严重时会导致线缆熔化，设备的元器件烧焦或炸裂，雷电高压沿线路直接入侵设备，造成设备损坏。

另外，在雷电放电过程中，云对云、云对地之间放电都将产生强大的静电感应和磁场感应。在临近的架空线路、接地线路和导体上产生感应电流和电压，当耦合到电子设备上时，可直接击毁设备。这种由雷电引起的静电感应和电磁感应统称为感应雷。感应雷一般没有直击雷那么猛烈，但因其是通过静电感应和磁感应产生作用，故可在较大范围内多个局部同时发生雷灾。感应雷发生的概率远大于直击雷，尤其是计算机网络、通信系统等常因动力线、网络通信线感应过压或过流而损坏，故对计算机类设备而言，感应雷的危害往往大于直击雷。

防雷应在以下几方面采取措施：

(1)中心机房所在的建筑物应当安装独立的避雷针、避雷网，将整个中心机房所在的建筑物保护起来，将电流引入大地。

(2)在动力室电源线总配电盘上安装专用避雷器构成第一级衰减。

(3)在机房配电柜进线处，安装电源避雷器构成第二级衰减。

(4)机房布线不能沿墙敷设，以防止雷击时墙内钢筋瞬间传导强雷电流时，瞬间变化的磁场在机房内的线路上感应出瞬间的高脉冲浪涌电压把设备击坏。

(5)地极保护器。大楼防雷接地系统与计算机直流接地系统是彼此独立的两个接地系统。当有雷电流泄入大地时，由于防雷接地电阻的存在会造成电位上升至远高于大地电位，而此时直流接地仍是大地电位，这时机房内会因两个接地系统电压差过高而毁坏设备，这种现象称为地电位反击。

为防止地电位反击，设计机房工程方案时在机房入口处的直流接地和防雷接地间安装了一套独立地极保护器。该独立地极保护器使两个接地系统在雷电期间合二为一，两个接地系统电压差为 0。非雷电期间，两个接地系统独立运行，确保直流接地不受干扰。

2.3 静电与电磁辐射的防护

下面介绍如何进行静电和电磁辐射的防护。

2.3.1 静电防护

静电就是物体所带相对静止不动的电荷，是正负电荷在局部范围内失去平衡的结果，是通过电子或离子转移而形成的。

静电是计算机系统半导体元器件的“大敌”，在干燥的季节，许多摩擦现象会生产静电。由于静电原因每年造成的计算机及其元器件损失高达数亿美元，电磁干扰不仅可以使磁记录被破坏，还会造成计算机设备外壳的静电放电，容易导致 MOS 器件栅介质被击穿。

1. 静电的危害

静电放电(electro-static discharge，ESD)引起发光二极管 PN 结的击穿，是 LED 器件封装和应用组装工业中静电危害的主要方式。静电损伤具有如下特点：

(1)隐蔽性。人体不能直接感知静电，即使发生静电放电，人体也不一定会有电击的感觉，大多数情况都是通过测试或者实际应用，才能发现 LED 器件已受静电损伤。

(2)潜伏性。静电放电可能造成 LED 突发性失效或潜在性失效。突发性失效造成 LED 的永久性失效——短路。潜在性失效则可使 LED 的性能参数劣化，如漏电电流加大。

(3)复杂性。在静电放电的情况下，放电电源是空间电荷，因而它所储存的能量是有限的，不像外加电源那样具有持续放电的能力，故它仅能提供短暂发生的局部击穿能量。虽然静电放电的能量较小，但其放电波形很复杂，控制起来也比较麻烦。另外，LED 极为精细，失效分析难度大，使人容易误把静电损伤失效当做其他失效，在对静电放电损害未被充分认识之前，常常归咎于早期失效或情况不明的失效，从而不自觉地掩盖了失效的真正原因。

(4)严重性。ESD 潜在性失效只引起部分参数劣变，如果不超过合格范围，就意味着被损伤的 LED 可能毫无察觉地通过最后测试，导致出现过早失效，这对各层次的制造商来说，其结果是最损声誉的。ESD 以极高的强度迅速地发生，放电电流流经 LED 的 PN 结时，产生的热量使芯片 PN 两极之间局部介质熔融，造成 PN 结短路或漏电。

2. 静电防护

静电防护是为防止静电积累所引起的人身电击、火灾和爆炸、电子器件失效和损坏，以及对生产的不良影响而采取的防范措施。防范原则主要是抑制静电的产生，加速静电的泄漏，进行静电中和等。具体措施为：

(1)设备、仪器不使用塑料、有机玻璃、普通塑料袋。

(2)使用防静电地面，敷设地线网。

(3)工作台/面、工作椅、凳面应采用 ESD 保护材料。

(4)工作人员应穿防静电服、鞋等。

(5)接地，主要有以下几个方面：

- 防静电工作区必须有安全可靠的防静电接地装置。防静电地线不得与电源零线相接，不得与防雷地线共用，使用三相五线制的供电时，其地线可以做防静电地线。

- 工作台/面、地板垫、座椅、凳和其他导静电的 ESD 保护措施均应通过限流电阻接到地线。
- 防静电工作区接地系统，包括限流电阻和连接端子应连接可靠并具有一定载流能力，限流电阻阻值的选择应保证泄漏电流不超过 5 mA，下限值取为 1 MΩ。

2.3.2　电磁辐射防护

电磁辐射干扰对计算机系统的稳定性、可靠性和安全性有着直接影响，电磁辐射对计算机系统及其数据所产生的干扰、破坏、窃取与篡改的危险性与日俱增，现已成为重要的安全问题。电磁辐射防护技术与措施如下。

1. 距离防护

根据电磁场强度在传播过程中随距离的加大衰减很快的原理，可以采取将计算机、网络设备等放置在远离辐射源的地方。根据技术要求，计算机机房场地的选择应当满足以下要求：

- 避开环境污染区，附近无大功率发射设备，无大功率的工业、科学、医疗射频设备，无高压线输电线与大型负载。
- 避开大型震动源，特别是铁路沿线及工业生产震动、冲击的设备应当绝对避开。
- 避开雷电多发区。
- 避免置于高层建筑物上层，计算机机房应当安置在地面第一层或通风良好的地下室。

2. 屏蔽防护

屏蔽机房既可以防止外界电磁场干扰或破坏计算机系统的工作，又可以防止机房内计算机信息的泄露与失密。

屏蔽措施主要包含以下内容：

- 屏蔽机房必须是全屏蔽，实现整个屏蔽机房电气一体化。
- 所有电源线路必须滤波，尽量使用高抗干扰电源。
- 信号线路滤波。

2.4　存储介质与数据保护

在企业对信息的依赖性越来越强的今天，企业的运营时刻都离不开数据，信息已成为企业的生命源泉。然而，因设备的意外损毁、人为操作失误、病毒泛滥、黑客入侵、自然灾难等情况造成的数据丢失及业务停顿的案例屡见不鲜，这些会给企业带来不可估量的损失。为有效防范系统突发事件，提高信息可靠性和可用性，必须对企业数据进行保护和备份，并制订相应的备份及恢复方案，以确保在问题发生时，尽快恢复数据及计算机系统的正常运行。

2.4.1　存储介质保护

存储介质是存储数据的媒介。存储介质的损坏会造成数据的丢失，而存储介质被非授权用户获取会造成信息的泄露，这些都会给企业带来不可估量的损失。

保护存储介质应建立专门的存储介质库(柜)并进行如下管理:

(1)限制少数人接触存储介质库(柜)。

(2)存储介质库(柜)内带盘的目录清单要标明相关参数,并定期检查。

(3)保护存储介质免受意外碰撞。存储介质受到碰撞,极有可能破坏设备,导致数据损坏、丢失。

(4)谨防静电。

(5)存储介质库(柜)房要保持合适的温度、湿度。

(6)磁带装盒。开放磁带盒将增加磁带接触到灰尘、潮湿和阳光的机会,并有可能最终侵蚀磁带,导致其质量和可靠性下降。

2.4.2 数据保护

存储介质保护是针对存储介质丢失和滥用提供的保护,从信息安全角度来看,就是确保数据的保密性、完整性和可用性。信息保护包含的内容如下。

1.保护数据不被泄露

为保护重要数据不被泄露应采取以下方式加以保护:

- 对数据进行加密,对于保密性要求高的数据应采取加密方式进行加密。
- 信息权限管理,对信息的使用要有身份认证和严格的权限控制。
- 密钥管理,数据加密的密钥要妥善保管,一旦密钥丢失极有可能造成数据泄露。
- 数据擦除服务,从老化或损坏磁盘上永久删除数据,以防止私密数据的泄露。

2.保护数据不丢失

对于重要的数据,必须备份,备份文件要存放于防火、防水、防电磁场的保护设备中。保护数据不丢失,可分为多个保护级别,这些级别分别是备份、本地复制、远程复制。

1)备份

备份是为了在系统出现故障时进行数据恢复,包括磁带备份和磁盘备份等。

(1)磁带备份是经典的备份方式,将数据备份到磁带上。磁带备份具有容量大、成本低的好处,但备份和恢复的时间较长,而且恢复成功的概率较小。

(2)磁盘备份是把磁盘阵列作为备份设备,它改善了备份和恢复的性能,提供高可靠性和可用性。

(3)虚拟磁带库又称为磁盘库,用磁盘来存储数据,并且能够仿真成物理磁带库。这种备份方式是磁盘备份的主流方式。它的优点是:相对磁带备份的性能大幅提高,同时,还能沿用原有的磁带备份软件和备份策略。

(4)衍生的备份方式,多级备份是先备份到虚拟磁带库,再备份到磁带,采用这种方式可以充分利用存储空间,将信息存放到适当的存储设备上。

备份应注意备份的数据量,备份和恢复的速度和可靠性,备份、恢复操作的方便性等。为了减少备份数据量、加快备份和恢复的速度,可以通过全面的备份、恢复和归档策略及采用新一代的重复数据删除备份技术。其中,全面的备份、恢复和归档把不活动的、最终形式的数据进行归档,以缩小生成数据的大小,这样就减少了备份的数据量,恢复时间也更短,性能更加稳定,并且可实现分层存储的优势。

任何备份技术的恢复机制都需要一个和备份过程相反的过程,这个过程一般时间会很

长，如果用户对恢复时间要求很高，采用磁带备份就有些无能为力了，为了满足要求就必须采用磁盘备份。

2）本地复制

本地复制包括快照和克隆。快照是数据在某个时间点（复制开始的时间点）的映像。它是基于指针、节省空间的逻辑复制，通常要求少于 30％的源卷容量，速度较快。克隆是数据的完整复制，是真实的复制，它的速度较慢，而且每个副本需要与源卷容量相同的存储空间。

3）远程复制

远程复制为业务连续性和灾难备份提供了强有力的保证，通过远程站点故障切换确保数据和系统的可用性。

远程复制包括同步远程镜像和异步远程镜像。同步远程镜像是指通过远程镜像软件，将本地数据以完全同步的方式复制到异地。异步远程镜像保证在更新远程存储系统前完成向本地存储系统的基本 I/O 操作，而由本地存储系统提供给请求镜像主机的 I/O 操作完成确认信息，远程的数据复制以后台同步的方式进行。

习　题　2

1. 通过哪些方法可以有效预防雷击对计算机网络的危害？

2. 静电防护与电磁辐射防护的意义是什么？

3. 如何对数据进行保护？

第 3 章　网络攻击与防范

知识目标

◎ 理解网络攻击的概念和技术
◎ 掌握端口的概念、端口扫描的原理和防范方法
◎ 掌握网络监听的概念、原理和防范方法
◎ 掌握 Web 欺骗、DNS 欺骗、IP 欺骗和 ARP 欺骗的概念、原理和相关防范方法
◎ 掌握缓冲区溢出和拒绝服务攻击的概念、原理和防范方法
◎ 理解分布式拒绝服务攻击的概念和原理
◎ 掌握电子邮件攻击的原理和防范方法
◎ 掌握木马的概念、原理、防范与清除方法

技能目标

◎ 掌握网络攻击的一般步骤
◎ 了解端口扫描工具和网络监听工具的使用方法
◎ 了解缓冲区溢出攻击的过程
◎ 掌握黑客攻击的一般过程和攻击方法

网络攻击，可以定义为利用网络存在的漏洞和安全缺陷对系统进行攻击，以访问其中的资源。随着网络技术的迅速发展和黑客攻击工具的日益普及，发起网络攻击已不再是黑客的专利，简单易用的黑客软件让更多人学会了攻击。网络攻击频繁发生，造成的损失也越来越大。本章将介绍网络攻击的手段及采取的应对方法。

3.1　网络攻击的概念

由于互联网的开放性、脆弱性以及攻击的普遍性，导致网络中存在大量的安全漏洞并不断被发现。旧的安全漏洞补上了，新的安全漏洞又不断出现。网络攻击正是利用这些存在的漏洞和安全缺陷对系统进行攻击。

3.1.1　什么是网络攻击

“攻击”是指任何非授权的行为，范围从简单的使服务器无法正常工作到完全破坏或控制服务器。

网络攻击主要是通过对信息收集、分析、整理后，利用目标系统的漏洞，有针对性地对目标系统（服务器、网络设备与安全设备）进行资源入侵与破坏、机密信息窃取、监视与控制等的活动。

3.1.2　网络攻击的技术

常见的网络攻击技术包括：端口扫描、网络监听、各种网络欺骗、缓冲区溢出、拒绝式服务、病毒、电子邮件攻击。各种网络攻击技术将在下面详细介绍。

3.1.3　网络攻击的步骤

进行一次成功的网络攻击，一般要经过以下 5 个步骤。

1. 隐藏自己的位置

为了不在目标主机上留下自己的 IP 地址，以防被目标主机发现，一般攻击者都会隐藏自己真实的 IP 地址，老练的攻击者还会尽量通过“代理”或“肉鸡”来进行扫描和攻击，这样在目标主机上留下的是代理计算机或“肉鸡”的 IP 地址。

所谓的“肉鸡”，通常是指攻击者通过后门程序控制的傀儡主机。

2. 寻找并分析目标主机

攻击者首先要寻找目标主机，并对目标主机进行分析。在 Internet 上，能真正标识主机的是 IP 地址，域名只是为了便于记忆主机的 IP 地址而另起的名字，所以只要利用域名和 IP 地址就可以顺利找到目标主机。当然，知道了要攻击目标的位置还远远不够，还必须清楚目标主机的操作系统类型及其所提供的服务等。此时，攻击者可以使用一些扫描工具，了解目标主机上运行的是哪种版本的操作系统，系统有哪些账户，开启了哪些服务，以及服务程序的版本等信息，为入侵做好充分的准备。

3. 获取账号和密码，登录目标主机

攻击者要想入侵一台主机，首先要有该主机的一个账号和密码，否则连登录都无法进行。这样常迫使攻击者先设法盗窃账户文件并进行破解，从中获取某用户的账号和口令，再寻找合适的时机以此身份进入主机。此外，利用某些工具或系统漏洞登录主机也是攻击者常用的方法。

4. 获得目标主机的控制权

攻击者利用各种工具或系统漏洞进入目标主机系统获得控制权之后，首先会做两件事：留下后门和清除记录。留下后门指通过更改某些系统设置、在系统中植入木马或其他一些远程操纵程序，以便日后可以不被觉察地再次进入系统。清除记录指为了避免被目标主机发现，使用清除日志、删除复制的文件等手段来隐藏自己的踪迹，以便开始下一步的行动。

5. 窃取网络资源和特权

攻击者找到攻击目标后，就可以继续下一步的行动，如下载有用信息，窃取账号和密码、

个人资料、信用卡信息等敏感信息，或使网络瘫痪等，这些都可能是攻击者实行网络攻击的目的所在。

3.2 端口扫描

扫描就是对计算机系统或者其他网络设备进行相关的安全检测，以找出目标主机开启的端口、端口上的网络服务等安全隐患和可被黑客利用的漏洞。扫描是一把双刃剑，对攻击者来说，扫描往往是攻击的前奏，通过扫描，搜集目标主机的相关信息，以期寻找目标主机的漏洞；另一方面，网络安全管理人员通过扫描，获取安全信息，以便发现问题，防患于未然。

3.2.1 端口的概念

在网络技术中，端口有两种含义：第一种是物理意义上的端口，是指连接其他网络设备的接口，如集线器、交换机、路由器、网卡的端口。第二种是逻辑意义上的端口，一般是指TCP/IP中的端口。

所谓TCP/IP中的端口，是指在某计算机上运行的应用服务的地址。如果把IP地址比喻成一间房子，端口就是出入这间房子的门。真正的房子只有几个门，但一个IP地址的端口可以有65 536个之多。端口是通过端口号来标记的，端口号范围是0～65 535。当一个应用服务启动时，它必须告诉计算机它所使用的端口号。通过端口号可以识别一台计算机上的多个同时运行的进程，例如，浏览网页服务的80端口、用于FTP服务的21端口等。

80端口、21端口也称为“常用端口”或“公用端口”，用于绑定一些特定的服务。通常这些端口的通信明确表明了某种服务的协议，这种端口不可再重新定义它的作用对象，其端口的端口号从0到1 023。而端口号从1 024到65 535的端口则松散地绑定于一些服务，也就是说这些端口一般不固定分配给某个服务，许多服务都可以使用这些端口。

3.2.2 端口扫描的原理

端口扫描是指通过检测远程或本地系统来判断目标主机的端口开放情况及提供的服务和它们的软件版本，以便了解主机所存在的安全问题。其原理是向目标主机的某些端口发送数据包进行探测，并根据目标端口的响应确定哪些端口是开放的。

3.2.3 端口扫描工具

端口扫描工具又称为扫描器，是一种自动检测远程或本地主机安全性缺陷或漏洞的程序。通过使用扫描器可以搜集到很多关于目标主机的各种有用信息，但扫描器并不能直接攻击网络漏洞，而是帮助用户（包括合法和非法用户）发现目标机器的某些内在的弱点，这些弱点可能是破坏目标主机的关键。一个好的扫描器能对它得到的信息进行分析，以帮助用户查找目标主机的漏洞，可直接或间接地了解远程主机存在的安全问题。

常用的端口扫描工具有以下几种。

1. SuperScan

SuperScan 是一款运行在 Windows 2000/XP/Server 2003 操作系统上的免费扫描工具，具备基于 TCP 的端口扫描、Finger 和主机名解析等功能。它通过多线程和异步技术的运用，使程序具有极快的扫描速度和强大的功能，不但界面友好，而且还能清楚地显示出对方端口的回应信息。

SuperScan 可以通过 ping 命令来检验目标机器是否在线；实现 IP 地址和域名的相互转换；检验目标计算机提供的服务类型和一定范围内目标计算机是否在线及其端口开放情况；允许自定义要检验的端口，并保存为端口列表文件；利用软件自带的木马端口列表文件 trojans. lst可以检测目标计算机是否存在木马，而且也可以自定义修改此木马端口列表文件。SuperScan 的的主界面如图 3-1 所示。

图 3-1　SuperScan 主界面

2. HostScan

HostScan(网络主机扫描)是一款网络扫描软件，具有 IP 扫描、端口扫描和网络服务扫描功能。其中，IP 扫描可以扫描任意范围(0. 0. 0. 0～255. 255. 255. 255)的 IP 地址，找到正在使用中的网络主机；端口扫描可以扫描指定主机的端口，范围为 1～65 535，获得已经打开的端口的信息，通过对端口信息进行分析，可以了解是否有人在自己的电脑上留下了后门；网络服务扫描可以扫描打开的端口，返回端口后台运行的网络服务信息，例如，80 端口在通常情况下运行的是 HTTP 服务。扫描完成后，会给出一份详细的网络扫描报告，以备查阅。HostScan 的主界面如图 3-2 所示。

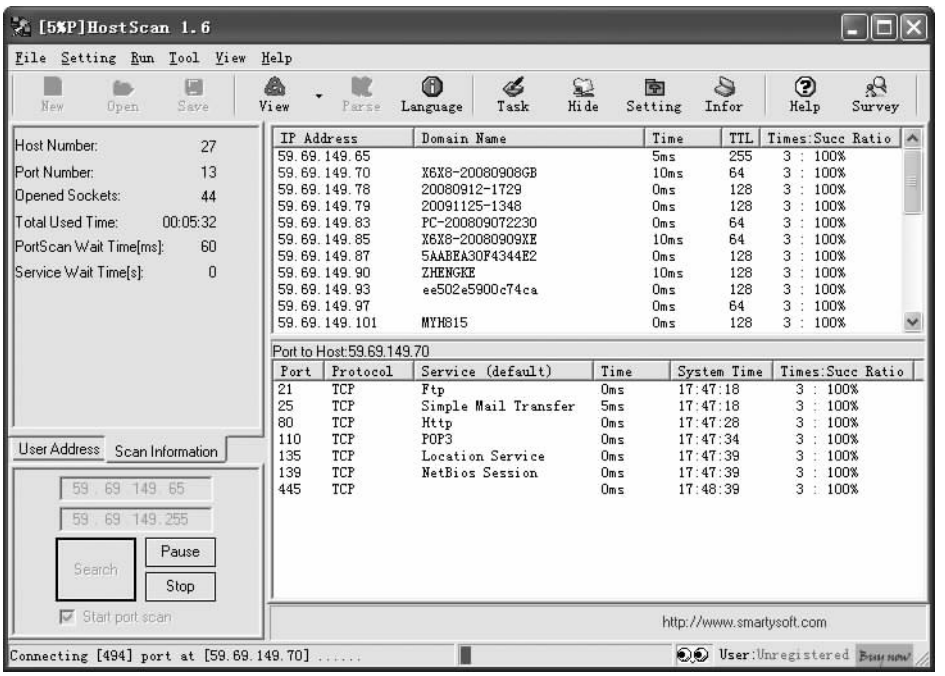

图 3-2 HostScan 主界面

3. X-Scan

X-Scan 是一款国产的扫描软件，是由国内程序员黄鑫开发的，主要运行于 Windows 操作系统。X-Scan 采用多线程方式对指定 IP 地址段（或独立 IP 地址）进行安全漏洞扫描，提供了图形界面和命令行两种操作方式，扫描内容包括：远程服务类型、操作系统类型及版本、各种弱口令漏洞、后门、应用服务漏洞、网络设备漏洞、拒绝服务漏洞等 20 多类。

3.2.4 端口扫描的防范

扫描一般是攻击者对目标主机发起攻击的重要一步。通过扫描可以获取目标主机的有用信息，发掘出系统存在的漏洞和弱点。为了降低主机被攻击的风险，应该从以下几个方面进行防范。

（1）关闭所有闲置和潜在威胁的端口，即将用户需要用到的所有正常计算机端口以外的其他端口都关闭，而一些系统必要的通信端口，如访问网页需要的 HTTP（80 端口）、FTP（21 端口）和 QQ（4 000 端口）等端口不能关闭。

（2）安装防火墙、入侵检测系统等安全软件。防火墙能够检查各端口，一旦发现有端口被扫描的症状，就立即屏蔽该端口；入侵检测能够发现正在进行的扫描，并提供实时报警。

（3）修正系统和网络，使其暴露尽可能少的信息。例如，定制系统和服务器返回给客户端的提示信息，这样当有人对服务器进行端口扫描时，服务器相应的端口不管是否打开，都会按照用户设置的信息进行回复。

3.3　网 络 监 听

网络监听在网络安全上一直是一个比较敏感的话题，作为一种发展比较成熟的技术，监听在协助网络管理员监测网络传输数据、排除网络故障等方面具有不可替代的作用，因而一直备受网络管理员的青睐。然而，另一方面网络监听也给以太网安全带来了极大的隐患，许多网络入侵往往都伴随着以太网内的网络监听行为，从而造成口令失窃、敏感数据被截获等连锁性安全事件的发生。

3.3.1　网络监听的概念

网络监听，也称为网络嗅探，主要工作在网络的底层，通过在互相通信的两台计算机之间利用技术手段插入一台可以接收并记录通信内容的设备，最终实现对通信双方的数据记录。一般要求用做监听途径的设备不能造成通信双方的行为异常或连接中断等，即监听方不能参与通信中任何一方的通信行为，仅仅是“被动”地接收记录通信数据而不能对其进行篡改。一旦监听方违反这个要求，这次行为就不是“网络监听”，而是“劫持”了。由于网络监听的“被动性”和“非干扰”性，使得网络监听具有很强的隐蔽性，让网络信息泄密变得不容易发现。网络监听可以在网上的任何位置实施，如网关、路由器、远程网的调制解调器或者网络中的某一台主机等。

嗅探器(sniffer)是一类用于捕获网络报文的软件。它可以用来进行网络流量分析，以找出网络中潜在的问题，确定在通信所使用的多人协议中，属于不同协议的流量大小，哪台主机承担主要协议的通信，哪台主机是主要的通信目的地，报文发送的时间，主机间报文传送的时间间隔等，是网络管理员常用的一个工具。当一段网络运行不好，速度较慢而又找不出问题所在时，用 sniffer 往往可以作出精确的判断。

sniffer 具有捕获网络报文的功能，也可以被黑客用来捕获网络中传输的用户口令、金融账号、机密或敏感数据、专用数据和低级协议信息等。

sniffer 与一般键盘捕获程序不同，键盘捕获程序捕获在终端上输入的键值，而嗅探器捕获的则是真实的网络报文。

3.3.2　网络监听的原理

为了对网络监听的原理有一个深入的了解，首先介绍一下网卡、局域网及 sniffer 的工作原理。

1. 网卡的工作原理

网卡是主机用来接收网络数据的物理设备。当网卡收到传输来的数据时，网卡内的程序先接收数据头的目的 MAC 地址，然后根据计算机上的网卡驱动程序设置的接收模式判断该不该接收。若认为应该接收，就在接收后产生中断信号通知 CPU，CPU 得到中断信号产生中断，操作系统就根据程序中设置的网卡中断程序地址调用驱动程序接收数据，驱动程

序接收数据后放入信号堆栈让操作系统处理;若认为不该接收,则丢弃不管。

2. 局域网的工作原理

数据在数据链路层以帧为单位进行传输。当同一网络中的两台主机通信时,源主机将写有目的主机地址的数据包直接发向目的主机。但这种数据包不能在 IP 层直接发送,必须从 TCP/IP 的 IP 层交给网络接口,而网络接口是不能识别 IP 地址的,因此在网络接口数据包中又增加了一部分以太帧头的信息。在帧头中有两个域,分别为只有网络接口才能识别的源主机和目的主机的 MAC 地址,这是一个与 IP 地址相对应的 48 位的地址。

传输数据时,包含 MAC 地址的帧从网络接口(网卡)发送到网线上,到达目的主机的网络接口时,正常情况下,网络接口读入数据帧,并进行检查,如果数据帧中携带的 MAC 地址是自己的 MAC 地址或者广播地址,则将数据帧交给上层协议软件,也就是 IP 层软件,否则就将这个帧丢弃,所以不该接收的数据在网卡处就被截断了,计算机根本不知道。

网卡一般有以下 4 种数据接收模式:

- 广播模式:该模式下的网卡能够接收网络中的广播信息。
- 组播模式:该模式下的网卡能够接收组播数据。
- 直接模式:在该模式下,只有目的网卡才接收该数据。
- 混杂模式:在该模式下的网卡能够接收一切通过它的数据,而不管该数据是否是传给它的。

网卡的缺省接收模式包含广播模式和直接模式,即它只接收广播帧和发给自己的帧,对不属于自己的报文则不予响应。但如果局域网中的某台主机的网卡采用混杂模式,则它将接收同一网络内所有的报文和帧,这样就可以达到对网络信息监听的目的。

3. sniffer 的工作原理

sniffer 要捕获的报文必须是物理信号能收到的数据信息。在以太网中,根据连接的网络设备不同,可分为共享式网络和交换式网络。下面分别介绍 sniffer 在这两种网络中的工作原理。

1)共享式网络中的嗅探器

所谓共享式网络,就是使用共享式集线器组建起来的网络。在这个共享式网络中,一个主机发给另一个主机的信息,由共享集线器接收并转发给同一网段的所有网络接口,这样一台计算机就能够接收同一网段中任何两台主机之间通信的信息,这也是 sniffer 捕获信息的根本所在。

在以太网中,每个接口都有一个与其他网络接口不同的 MAC 地址,同时还有一个能够同时向同一网段的所有主机发送数据包的广播地址,一个合法的网络接口应该只响应这两种地址。但如果某台计算机的网卡设置为混杂模式,那么该网卡就可以接收同一网段的所有数据包,而不管该数据包是否属于自己。网卡对数据包的处理过程如图 3-3 所示。

可见,sniffer 工作在网络环境中的底层,它会“嗅”到所有在网络上传输的数据。由于在一个以太网中,账号和口令都是以明文形式传输的,因此一旦入侵者获取了其中一台主机的管理员权限,并将其网卡设置成混杂模式,它就有可能对网络中的其他所有计算机发起攻击。

2)交换式网络上的 sniffer

交换式网络是指通过网桥、路由器或交换机等交换式设备连接而成的网络。与共享式网络不同,由于交换式设备的内部程序能够记住每台主机的网络接口,所以交换式设备可以准确地将数据报文发给目标主机。这样,安装了 sniffer 的主机可能收不到某些数据包,

sniffer 也就不能工作。

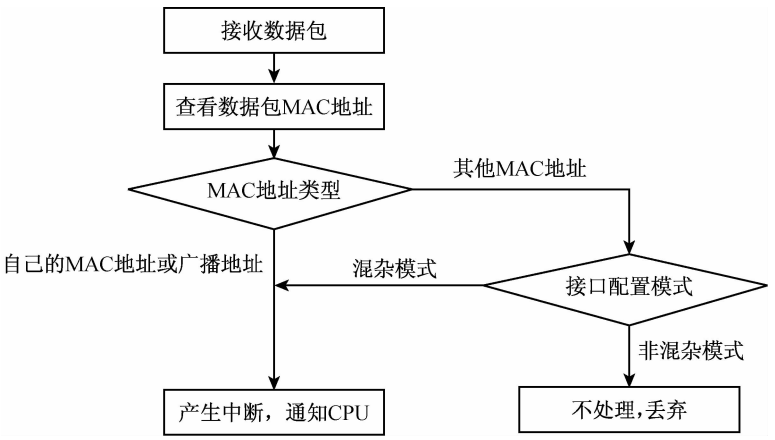

图 3-3　网卡对数据包的处理过程

但是，在交换环境中，sniffer 攻击也并非不可能。一个简单的方法是将安装有 sniffer 软件的计算机伪装成为网关。网关是一个网络与其他网络之间的接口，所有发往其他网络的数据包都必须经过网关转发，即从一个局域网发往其他网络的数据帧的目标地址都是指向网关的。如果把安装有 sniffer 软件的计算机伪装成网关，sniffer 就能“嗅到”本地网络中的数据。比如，一个交换网络中有 3 台主机：A 是普通用户，IP 地址为 202. 113. 240. 1；B 是一个入侵者，其 IP 地址为 202. 113. 240. 2；C 是网关，IP 地址为 202. 113. 240. 3。在正常情况下，B 是无法收到 A 与 C 之间的通信报文的。但是，若在 B 上运行 ARP（地址解析协议，可以将 IP 地址解析为局域网中的 MAC 地址）欺骗的命令 ARPredirect（dsniffer 软件的一部分），并发出一条命令“ARPredirect-t 202. 113. 240. 2 202. 113. 240. 3”就可以将该网络中主机发送的数据报文重定向：ARPredirect 就开始向 A 发送假冒的 ARP 应答，说 B 是网关；A 就会刷新自己的缓存，将 B 的 MAC 地址作为网关地址保存。这样，当 A 需要同其他网络中的主机进行通信时，就会依据缓存中的网关地址（现在是 B），先把数据包发往 B；B 可以先窃取 A 发出的数据包中的有关信息，再用 IP 转发或其他软件将这些数据包转发到 C。对 A 来说，一切都非常正常，但有关内容已经被窃。当然，如果在 A 上用 ARP 命令查看 ARP 高速缓存，可以发现网关地址已经被换掉了。整个地址欺骗过程如图 3-4 所示。

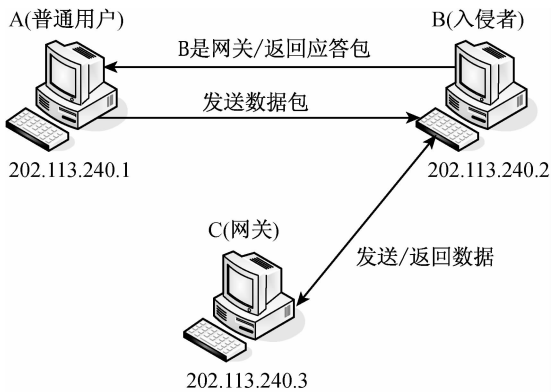

图 3-4　地址欺骗的过程示意图

3.3.3 网络监听的工具

使用嗅探器能够帮助管理员检查和解决在本地计算机上遇到的一些网络问题。例如，可以定位客户端到用户端的连接问题，发现工作请求数目不成比例的计算机，以及标识网络上未授权的用户等。常见的嗅探器有以下几种。

1. Sniffer Pro

Sniffer Pro 是由 NAI 公司推出的功能强大的网络协议分析软件，支持各种 Windows 平台，其专家分析系统协议用于在进行数据包捕获、实时解码的同时快速识别各种异常事件；数据包解码模块支持广泛的网络应用协议，不仅限于 Oracle，还包括 VolP 类协议，以及金融行业专用协议和移动网络类协议等。Sniffer Pro 提供直观易用的仪表板和各种统计数据、逻辑拓扑视图，并且提供能够深入到数据包的点击关联分析能力。

2. Windump

Windump 是 Windows 环境下一款经典的网络协议分析软件，其 UNIX 版本的名称为 Tcpdump。它可以捕获网络上两台主机之间的所有数据包，供网络管理员或入侵者作进一步流量分析和入侵检测。在这种监视状态下，任何两台主机之间都没有秘密可言，所有的流量和数据都被监视，当然加密后的数据虽然能够捕获，但很难解密。对数据包分析的结果依赖于用户的 TCP/IP 知识和经验。

3.3.4 网络监听的防范

sniffer 攻击属于第二层攻击，通常是入侵者进入目标系统后，为了获取更多的信息而采用的攻击手段。为了达到好的攻击效果，它主要被放置在被攻击对象（主机或网络）附近和网关上。所以对 sniffer 的防范主要有以下几种方法。

1. **规划网络**

嗅探器只能在本地网络中捕获数据，这就意味着，网络分段越细，sniffer 收集到的信息越少。在网络分段时，可以将非法用户与敏感的网络资源相互隔离，从而防止可能的非法监听。

2. **采用加密通信**

在网络中，若报文以明文的方式进行传输，嗅探器可以很容易截获这些敏感数据。但数据经过加密后，通过监听仍然可以得到传送的信息，但显示的是乱码。使用加密技术的缺点是影响数据传输速度以及使用弱加密术容易被破解。系统管理员和用户需要在网络速度和网络安全上折中。

3. **监测 sniffer**

监测 sniffer 就是确定网络上有无 sniffer 在运行。当有 sniffer 运行时，会观察到一些诸如丢包率高、网络带宽反常等异常情况，这时网络管理员可以使用 anti-sniffer、promisc、cmp 等工具来检测大型网络上是否有 sniffer，或者检测是否有网络接口设置成混杂模式，因为虽然在非混杂模式下可以运行 sniffer，但只有在混杂模式下才可以捕获共享网络中的所有会话。

3.4　网 络 欺 骗

网络欺骗是指攻击者通过伪造自己在网络上的身份，从而得到目标主机或网络的访问权限。

由于互联网使用 TCP/IP 进行通信，而 TCP/IP 中，TCP 首部和 IP 首部都有固定的结构，任何人都可以很容易地伪造任意内容的网络数据包，因此网络上的主机面临着被欺骗的危险。目前，针对 TCP/IP 的欺骗技术有很多种，包括 Web 欺骗、IP 欺骗、DNS 欺骗和 ARP 欺骗等。

3.4.1　Web 欺骗

Web 欺骗是一种电子信息欺骗，攻击者建立一个令人信服但完全错误的 Web 站点的“复制”，这个 Web 站点复制看起来十分逼真，它具有原网页几乎所有的网页元素。然而，攻击者控制着这个 Web 站点复制，这样被攻击者的浏览器和真正的 Web 站点之间的所有网络信息都被攻击者所截获。

由于攻击者可以观察或修改任何从被攻击者到真的 Web 服务器的信息；同样地，也控制着从真的 Web 服务器到被攻击者的返回数据，也就是说，攻击者充当了被攻击者到真的 Web 服务器的“中间人”，所以攻击者能够监视被攻击者的所有信息，包括账户、口令和其他一些敏感信息。

Web 欺骗之所以能够成功，其关键是攻击者打断了被攻击主机到 Web 服务器之间的正常连接，并建立一条从被攻击主机到攻击主机再到 Web 服务器的连接。为了建立起这样的中间 Web 服务器，攻击者常常采用如下形式的欺骗。

1. Web 欺骗的形式

1）使用相似的 URL

目前，在互联网上注册域名不会受到严格的审查，这就给了攻击者可乘之机。攻击者可以注册一个与目标公司或组织相似的域名，然后建立一个欺骗网站，骗取该公司的用户的信任，以便得到这些用户的信息。例如，针对工商银行，用 www. lcbc. com. cn 来混淆 www. icbc. com. cn。若用户在假冒的网站上出示支付信息，假冒的网站把这些信息记录下来（并分配一个 cookie），然后提示：“现在网站出现故障或者你输入的密码错误，请重试一次”。当用户重试的时候，假冒网站发现这个用户带有 cookie，就把它的请求转到真正的网站上。使用这种方法，假冒网站可以收集到用户的敏感信息。这种攻击多以欺骗用户信用卡号、银行账户、股票信息、游戏账户等获取经济利益为目的。

2）改写 URL

通常，一个网页有若干个超链接，通过这些超链接可以访问其他的网页。一个具有超链接的 Web 页面从 Web 服务器到浏览器的传输过程中，如果其中的内容被修改了，欺骗就会发生，其中最重要的就是改写 URL，即攻击者改写网页上的 URL 链接，把用户指向或重定向到攻击者控制的主机。假设攻击者所处的 Web 服务器是 attack. org，攻击者通过在所有链接前增加 http://www. attack. org 来改写 URL，例如，URL 为 http://www. hollywood. com

的正常网页将变为 http://www.attack.org/http://www.hollywood.com，当用户单击改写过的 http://www.hollywood.com(可能仍显示的是 http://www.hollywood.com 的页面)时，将进入的是攻击者 http://www.attack.org 的网站，然后由 http://www.attack.org 向正确的网站 http://www.hollywood.com 发出请求并获得真正的文档，然后改写文档中的所有链接，最后经过 http://www.attack.org 返回给浏览器。

3)会话劫持

在现实生话中，对于银行一笔交易，如果营业员在检查了顾客的身份证和账户卡之后，抬起头来，发现不再是刚才的顾客，他会把钱交给外面的顾客吗？当然，这只是会话劫持的一个比喻。所谓会话，就是两台主机之间的一次通信，例如，浏览某个网站，这就是一次 HTTP 会话。而会话劫持，就是在一次正常的通信过程中，攻击者作为第三方参与到其中，或者是在数据流(如基于 TCP 的会话)中注射额外的信息，或者是将双方的通信模式暗中改变，即从直接联系变成攻击者。这是一种结合了嗅探和欺骗技术在内的攻击手段，但与欺骗不同的是，欺骗是伪装成合法用户，以获得一定的利益，而会话劫持是积极主动地使一个在线的用户下线，或者冒充这个用户发送消息，以便达到自己的目的。

会话劫持分为被动劫持和主动劫持两种。被动劫持实际上就是藏在后面监听所有的会话流量，常常用来发现密码或者其他敏感信息；主动劫持是找到当前活动的会话，并且把会话接管过来，迫使一方下线，由劫持者取而代之，危害更大，因为攻击者接管了一个合法的会话之后，可以做许多危害性更大的事情。例如，一个关于 TCP 的会话劫持：假设 A、B 和 C 是同一网段的主机，并且 B 是一台被入侵者控制了的主机，A 和 C 是两台正在会话的主机。当 A 和 C 进行通信时，B 由于安装有监听软件，所以能够收到 A 与 C 之间通信的所有数据。B 为了能够冒充 A 与 C 进行会话，可以在 A 远程登录到 C，并成功与 C 建立会话、完成认证后使用拒绝服务攻击等手段使 A 暂时瘫痪。这样，如果 C 正等待 A 的数据包时，B 抢先给 C 一个伪造的数据包，C 就会对这个数据包进行回应。由于 A 无法响应 C，这时 B 可以再次发送伪造的数据包，会话劫持过程如图 3-5 所示。虽然，B 收不到 C 发送给 A 的数据包，但 B 却可以冒充 A 给 C 发送命令以执行某个任务。

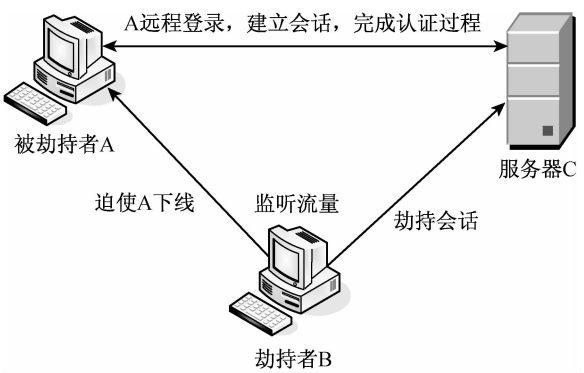

图 3-5 会话劫持过程

2. Web 欺骗的解决方法

Web 欺骗是当今 Internet 上具有相当危害性且不易察觉的欺骗手法，然而用户还是可以采取一些方法进行保护。

1)短期的解决方法

(1)禁止浏览器执行网页中的 JavaScript 程序,这样各类改写信息将原形毕露。

(2)确保浏览器的连接状态是可见的,它将提供当前位置的各类信息,并时刻注意即将打开的网页的 URL 在状态栏中是否能够正确地显示。

(3)养成从地址栏中输入网址来实现浏览所有网站的好习惯。

现在,JavaScript、ActiveX 控件以及 Java 提供越来越丰富和强大的功能,这也为攻击者进行攻击提供了强大的手段。为了保证安全,建议用户考虑禁止浏览器执行这些程序。

2)长期的解决方法

(1)改变浏览器的设置,使之具有反映真实 URL 信息的功能,而不会被虚假的 Web 站点所蒙蔽。

(2)对于通过安全连接建立的 Web 浏览器对话,浏览器还应该将通信双方的 IP 地址、MAC 地址等相关信息显示出来,而不只是显示安全连接状态。

(3)对于所传输的内容进行加密,这样除了接收者之外无人可以读懂。

3.4.2　DNS 欺骗

域名系统(domain name system,DNS)是一种用于 TCP/IP 应用程序的分布式数据库,采用客户机/服务器的模式,由解析器和域名服务器组成。域名服务器是指保存有该网络中所有主机的域名和对应的地址,并具有将网络域名转换为 IP 地址功能的服务器。

1. DNS 的工作原理

由于互联网上的每一台计算机都需要有一个 IP 地址以便通信,而由 32 位二进制数组成的 IP 地址对用户来说不便于记忆和理解,所以域名即常用的网址应运而生。域名是一个用户级地址,通信时两主机之间只能互相认识 IP 地址,DNS 就扮演了翻译的角色。例如,现在有 3 台主机,其中,主机 B 是提供 DNS 解析服务的服务器,主机 A 想要访问主机 C(www. ccc. com),则要经历的工作过程如下:

(1)A 向 DNS 服务器 B 发出一个 DNS 查询请求,要求 B 告诉其 C 的 IP 地址,以便与之通信。

(2)B 查询自己的 DNS 数据库,找不到 C 的 IP 地址,便向其他 DNS 服务器求援,逐级递交 DNS 请求。

(3)某个 DNS 服务器查到了 C 的 IP 地址,向 B 返回结果,B 将这个结果保存在自己的缓存中,并将结果告诉 A。

(4)A 得到了 C 的地址,就可以访问 C 了。

在上述过程中,如果 B 在一定的时间内不能给 A 返回要查找的 IP 地址,就会给 A 返回主机名不存在的错误信息。DNS 的工作过程如图 3-6 所示。

从上面 DNS 的工作过程可以看出,DNS 有两个重要特性:

- DNS 对于自己无法解析的域名,会自动向其他 DNS 服务器发出查询请求。
- 为提高效率,DNS 服务器会将所有已经查询到的结果存入缓存,这样以后再有相同的 DNS 查询请求时,就能直接使用缓存中的结果而不用通过其他 DNS 服务器查询。

正是这两个特点,使得 DNS 欺骗成为可能。

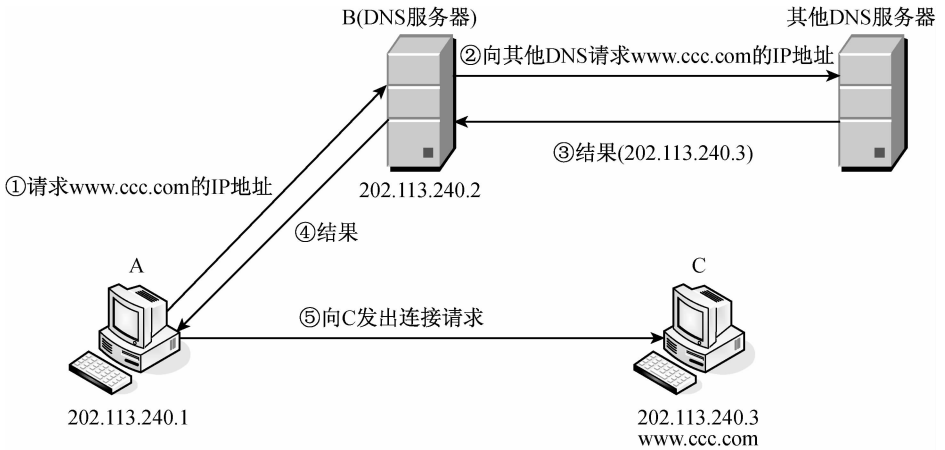

图 3-6 DNS 工作过程

2. DNS 欺骗

DNS 欺骗的思想是:让 DNS 服务器的缓存中存有错误的 IP 地址,即在 DNS 缓存中放一个伪造的缓存记录。为此,攻击者需要先伪造一个用户的 DNS 请求,然后再伪造一个查询应答。但是,在 DNS 的消息格式中还有一个 16 位的查询标识符(Query ID),它将被复制到 DNS 服务器的相应应答中,在多个查询未完成时,用于区分不同的响应。所以回答信息只有 Query ID 和 IP 都吻合时才能被 DNS 服务器接受。因此,进行 DNS 欺骗攻击,还需要能够精确地猜测出 Query ID。由于 Query ID 每次加 1,只要通过第一次向将要欺骗的 DNS 服务器发一个查询包并监听其 Query ID 值,随后再发送设计好的应答包,包内的 Query ID 就是要预测的 Query ID。例如,对于如图 3-6 所示的 DNS 工作过程,其 DNS 欺骗过程如下:

(1)入侵者先向 DNS 服务器 B 提交查询 C 的 IP 地址的请求。

(2)B 向其他 DNS 服务器递交查询请求。

(3)入侵者立即伪造一个应答包,告诉 B 所请求的 C 的 IP 地址是 202.113.240.4(往往是攻击者的 IP 地址)。

(4)查询结果被 B 记录到缓存中。

(5)当 A 向 B 提交查询 C 的 IP 地址的请求时,B 将 202.113.240.4 告诉 A。

从以上欺骗过程可以看出,DNS 欺骗是有一定的局限性的,具体表现如下:

- 入侵者不能替换 DNS 缓存中已经存在的记录。
- 缓存中的记录具有一定的生存期,过期就会被刷新。

对用户来说,可以从两方面进行防范:

(1)尽量少用域名,而是直接用 IP 地址来访问网站,这样可以避开 DNS 欺骗攻击。

(2)加密所有对外的数据流,对服务器来说尽量使用 SSH 之类的有加密支持的协议,一般用户可以使用 PGP 之类的软件加密所有发到网络上的数据。

3.4.3 IP 欺骗

所谓 IP 欺骗,是指入侵者使用一台计算机上网,而借用另外一台主机的 IP 地址,从而

冒充另外一台主机与服务器通信，以达到蒙混过关的目的。被冒充的主机往往具有某种特权或被服务器所信任，这也是入侵者进行 IP 欺骗的关键。入侵者可以利用 IP 欺骗的技术获得对主机未授权的访问，因为他可以伪造一个声称来自内部地址的 IP 包。当目标主机与被冒充主机之间存在高度的信任关系或者利用 IP 地址来验证相互的身份时，入侵者甚至可以获得普通用户或特权用户的权限。

1. IP 欺骗的步骤

假设入侵者知道主机 A(192.168.0.1)和主机 B(192.168.0.2)已经建立了信任关系，入侵者打算欺骗的是主机 A。入侵者要对 A 实施欺骗，就会假扮 B，所以就有必要让主机 B 无法响应任何请求。一般进行一次 IP 欺骗需要经过以下步骤：

(1)确定攻击目标。

(2)使被信任主机的网络暂时瘫痪，以免对攻击造成干扰。

(3)连接到目标主机的某个端口来猜测来自目标主机的初始序列号(initial sequence number，ISN)。

(4)冒充被信任的主机，并发送带有 SYN(TCP/IP 建立连接时使用的握手信号)标志的数据段请求连接。

(5)根据猜测出来的正确序列号(ISN+1)向目标主机发送 ACK 包。

(6)连接建立，进行序列会话。

要对 192.168.0.1 进行攻击，必须知道 192.168.0.1 使用的 ISN。TCP 使用的 ISN 是一个 32 位的计数器，计数范围为 0～4 294 967 295。TCP 为每一个连接选择一个 ISN，为了防止因为延迟、重传等扰乱三次握手，ISN 不能随便选取，不同的系统有不同的算法。理解 TCP 如何分配 ISN 以及 ISN 随时间的变化规律，对于成功地进行 IP 欺骗攻击是很重要的。实际上，系统序列号的产生并非完全随机。当没有外部连接发生时，服务器的 ISN 每秒增加 128 000；有连接时，服务器的 ISN 每秒增加 64 000。

攻击者先与目标主机的一个端口建立起正常连接，并将目标主机的 ISN 存储起来，通常这个过程需要被重复多次。然后还需要对攻击者与目标主机之间的往返时间进行估计，这个时间是通过多次统计平均计算出来的。攻击者通过同目标主机建立实际连接，获得目标系统当前的序列号。攻击者就可以基本确定下一个 ISN 是 128 000 乘以往返时间的一半，如果此时目标主机刚刚建立过一个连接，那么再加上 64 000。

入侵主机向主机 A(192.168.0.1)发送连接请求报文(SYN 置 1)，只是源 IP 地址改成主机 B 的 IP 地址(192.168.0.2)。主机 A 向主机 B 回送连接同意报文(SYN 置 1，ACK 置 1)，但主机 B 已经无法响应，主机 B 的 TCP 层只是简单地丢弃来自 A 的回送数据包。入侵主机会等待一段时间，让主机 A 有足够的时间发送连接同意报文，因为入侵主机接收不到这个数据包。然后入侵主机再次伪装成主机 B 向主机 A 发送 ACK 数据包，此时发送的数据包带有入侵主机预测的目标主机 A 的 ISN+1，如果预测正确，连接过程就会建立，数据传送也就开始了。

问题在于，即使连接建立，主机 A 仍然会向主机 B 发送数据，而不是向入侵主机发送，所以入侵主机仍然无法收到目标主机 A 发往 B 的数据包。但是，入侵主机可以向目标主机 A 发送命令，目标主机 A 将执行这些命令，认为它们是由合法主机 B 发来的。

2. IP 欺骗的防范策略

目前，针对 IP 欺骗的防范策略有以下几种。

1)放弃基于 IP 的信任策略

IP 欺骗是基于 IP 地址信任的,而 IP 地址很容易伪造。因此,阻止这类攻击的一种非常简单的方法是放弃以 IP 地址为基础的验证,而是使用其他方式来进行身份验证,如数字签名。所谓数字签名,是指发送方以电子形式签名一个消息或文件,签名后的消息或文件不仅能在网络中传送,而且能够确认签名者的身份,类似于写在纸上的普通的物理签名。

2)对数据包进行限制

若欺骗来自于网络外部,则可以在局域网的对外路由器上加一个限制;若实施欺骗的主机在同一网段,攻击容易得手,且不容易防范,这时一般通过路由器来进行包过滤。

3)应用加密技术

防止 IP 欺骗的另一种方法是在通信时要求加密传输和通信验证。当有多种手段并存时,加密方法可能是最为适用的。

4)使用随机化的初始序列

序列号是接收方 TCP 进行合法检查的一个重要依据。黑客攻击能够得逞的一个重要因素就是,序列号不是随机选择或者随机增加的。填补这一漏洞的方法就是让黑客无法计算或猜测出序列号。AT&T 公司(美国电话电报公司)的学者 Steven M. Bellovin 提出了一种弥补 TCP 不足的方法,可以用下列公式来说明:

ISN=M+F(localhost,localport,remotehost,remoteport)

其中,M 为 4 ms 定时器,F 为加密 Hash 函数,localhost 为本地主机,localport 为本地端口,remotehost 为远程主机,remoteport 为远程端口。Bellovin 建议 F 是一个结合连接标识符和特殊矢量的 Hash 函数,它产生的序列号不能被计算或猜测出来。

3.4.4 ARP 欺骗

ARP(address resolution protocol)是一种将目标主机的 IP 地址转换成 MAC 地址的协议。在以太网中,如何找到网络中数据包传输最合适的路径是由路由器定义的,但当数据包到达目的网络后,网络中的哪台主机接收这个数据包却是由包中的 MAC 地址来识别,即只有 MAC 地址和该包中的 MAC 地址相同的主机才能接收到这个数据包。为了便于主机之间的通信,每台安装有 TCP/IP 的计算机中都有一个 ARP 缓存表,表中的 IP 地址与 MAC 地址是一一对应的,如表 3-1 所示。

表 3-1 ARP 缓存表

主　机	IP 地址	MAC 地址
A	192.168.0.1	aa-aa-aa-aa-aa-aa
B	192.168.0.2	bb-bb-bb-bb-bb-bb
C	192.168.0.3	cc-cc-cc-cc-cc-cc
D	192.168.0.4	dd-dd-dd-dd-dd-dd

当主机 A(192.168.0.1)向主机 B(192.168.0.2)发送报文时,主机 A 先在本地的 ARP 缓存表中查询是否有目标 IP 地址,若有目标 IP 地址,则找到相应的目标 MAC 地址,将其写入帧中发送即可;若没有找到,主机 A 就会在网络上发送一个目标 MAC 地址是 ff.ff.ff.ff.ff.ff 的广播,向同一网段内的所有主机发出这样的询问:“192.168.0.2 的 MAC 地址是什

么?”网络上其他主机并不响应 ARP 询问,只有主机 B 在收到这个帧之后,才向主机 A 做出这样的回应:“192.168.0.2 的 MAC 地址是 bb-bb-bb-bb-bb-bb”。这样,主机 A 就知道了主机 B 的 MAC 地址,它就可以向主机 B 发送信息了。同时,它还更新了自己的 ARP 缓存表,下次再向主机 B 发送信息时,直接从 ARP 缓存表中查找就可以了。因此,本地高速缓存的这个 ARP 表是本地网络流通的基础,而且这个缓存表是动态的,在一段时间内如果表中的某一主机的 IP 与其 MAC 地址对应关系没有使用,就会被删除,这样可大大减少 ARP 缓存表的长度,加快查询速度。

通常情况下,当某一主机广播了 ARP 请求之后才会接收其他主机发送过来的应答报文。但当某主机没有广播 ARP 请求而收到应答数据包时,同样会对本地的 ARP 缓存进行更新,将应答中的 IP 和 MAC 地址存储在 ARP 缓存表中。因此,当局域网中的主机 B 向主机 A 发送一个伪造的 ARP 应答包,而且这个应答包是主机 B 冒充主机 C 伪造的,也就是说,这个伪造包用的是主机 C 的 IP 地址,主机 B 的 MAC 地址。这样,主机 A 发送到主机 C 的数据包都变成发送给主机 B 的了。主机 A 对这个变化一点都没有意识到,但接下来的事情就让主机 A 产生了怀疑。因为主机 A 和主机 C 连接不上了,主机 B 对接收到的主机 A 发送给主机 C 的数据包并没有转交给主机 C,作为一个“中间人”。这就是一个简单的 ARP 欺骗。

ARP 的基础就是信任局域网内所有的机器,这样就很容易实现在以太网上的 ARP 欺骗。ARP 欺骗分为以下两种。

1. 对路由器 ARP 表的欺骗

攻击者向路由器发送一系列伪造的 ARP 请求报文,并按照一定的频率不断进行,使真实的 ARP 报文无法通过更新保存在路由器的 ARP 缓存表中,因而路由器的所有信息只能发送给伪造的 MAC 地址,造成正常的计算机无法收到信息。

2. 对内网计算机的网关欺骗

假设某局域网网关的 IP 地址为 192.168.0.1,MAC 地址为 aa-aa-aa-aa-aa-aa。攻击者向同一网段的所有计算机发送这样一个报文:“IP 地址为 192.168.0.1 的 MAC 地址为 bb-bb-bb-bb-bb-bb”,这样就建立了一个假的网关。当局域网内的某主机 H 与其他网络的主机 W 通信时,主机 H 发给主机 W 的数据包将发给假网关,主机 H 将无法与主机 W 建立正常的连接。这样,在主机 H 看来,就是上不了网,“网络掉线了”。

3.5　缓冲区溢出攻击

缓冲区是系统为程序运行时在计算机中申请的一段连续的内存,用来保存给定类型的数据。在 C 和 C++ 中,缓冲区通常是为程序中定义的全局变量和局部静态变量分配的内存空间,以及使用 malloc 和 new 函数调用为变量动态分配的内存空间。缓冲区溢出是一种常见的系统攻击手段,通过向程序的缓冲区写入超出其长度的内容,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的指令,以达到攻击的目的。造成缓冲区溢出的原因是程序没有仔细检查用户输入的参数是否符合要求。

为了说明缓冲区的原理,先看一个 C 语言程序(example1.c)的例子。

```
#include <stdio.h>
```

```
#include <string.h>
void function (char *str) {
     char buffer[16];
     strcpy (buffer,str);
}
void main() {
   char large_string[256];
   int i;
   for (i=0;i<255;i++)
        large_string[i]='a';
   function (large_string);
}
```

该程序的功能是通过 strcpy 函数把 str 中的字符串复制到数组 buffer[16]中，如果 str 的长度超过 16 就会造成数组 buffer 的溢出，使程序出错，如图 3-7 所示。

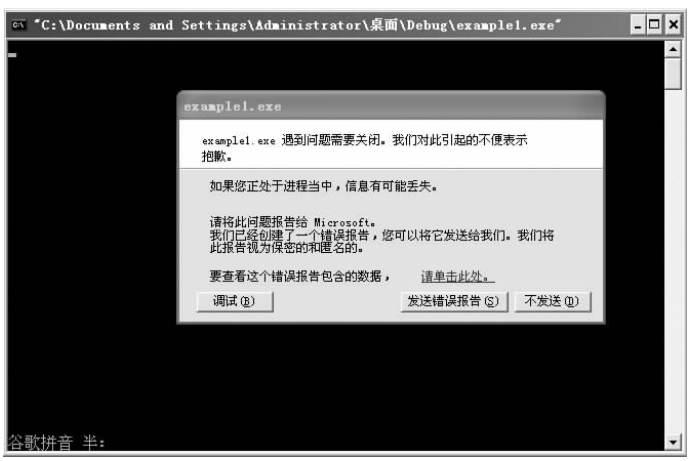

图 3-7 运行时的错误显示

3.5.1 缓冲区溢出的原理

为了更好地理解缓冲区溢出攻击的原理，首先要了解计算机在机器语言级上是如何工作的。在 Windows 操作系统下的 C 语言程序结构中，每个进程都可以占有 4 个主要区域：代码区、数据区、堆栈区和命令行及环境参数区。在内存中，它们的位置如图 3-8 所示。

其中，代码区主要存放着程序的机器码和只读数据，通常不能对其执行写操作。数据区存放着全局变量和静态变量，主要包括 bss 和 data 两部分：bss 包含的是未经初始化的数据，data 包含的是已经初始化的数据。堆栈区包括动态变量、函数和过程的调用。对于每一次过程或函数调用，在堆栈中都必须保存为一种称为“栈帧”的数据结构。栈帧中包含传递给函数的参数、返回地址、函数分配的局部变量以及恢复前一个栈帧需要的数据(基址寄存器 EBP)。堆栈中存放的是与每个函数对应的堆栈帧。当函数调用发生时，新的堆栈帧被压入堆栈；当函数返回时，相应的堆栈帧从堆栈中弹出。栈帧的结构如图 3-9 所示。

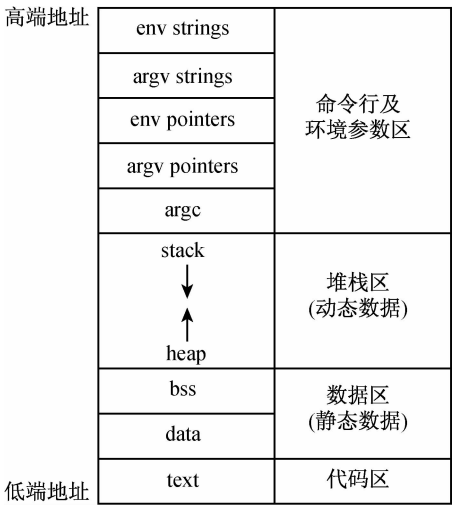

图 3-8　C 语言程序结构中进程占有的区域

图 3-9　栈帧结构

一个堆栈通常都有两个指针：一个称为堆栈帧指针，另一个称为栈顶指针。前者所指的位置是固定的，而后者所指的位置在函数的运行过程中可变。因此，在函数中访问参数和局部变量时都以堆栈帧指针为基础，再加上一个偏移量。当发生数据溢出时，多余的内容就会越过堆栈帧指针，覆盖后面的内容。通常，与堆栈帧指针相邻的内存空间中存放着程序返回地址，从而造成这样的局面：要么程序会取到一个错误的地址，要么因程序无权访问该地址而产生一个错误。

下面仍通过前面的 example1. c 程序为例来说明栈帧的结构。

当程序中发生函数调用时，计算机做如下操作：首先把参数压入堆栈；然后保存指令寄存器(EIP)中的内容作为返回地址(RET)；接着将基址寄存器(EBP)放入堆栈；再把当前的栈顶指针(ESP)复制到 EBP，作为新的基地址；最后为本地变量留出一定的空间，将 ESP 减去适当的数值。

当程序执行到 function 函数调用，但尚未执行 strcpy 时，堆栈中的情况如图 3-10 所示。

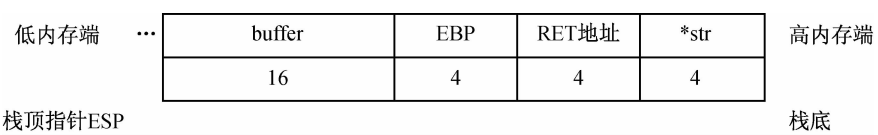

图 3-10　调用 function 后堆栈中的情况

当执行 strcpy 时，程序将 255 字节的 a 复制到 buffer 中，然而 buffer 却只能容纳 16 字节。由于 C 语言把这一艰巨的任务交给了开发人员，要求他们进行边界检查，编写安全的程序。然而，这一要求往往被人们所忽视，从而使黑客有机可乘。所以，结果是 buffer 后面包

括 EBP、RET 返回地址和 large_string 地址在内的 240 字节的内容被覆盖掉了。由于此时 RET 地址变成了 0x61616161h，所以当过程调用结束返回时，它将返回 0x61616161h 地址处继续执行下一条指令。但由于这个地址并不在程序使用的地址空间范围内，所以系统就报“Segmentation Violation”错误，这就是所谓的缓冲区溢出。

3.5.2 缓冲区溢出攻击的过程

缓冲区溢出可能会带来两种结果：一种是过长的数据覆盖了 EBP、RET 返回地址等存储单元，引起程序运行失败，严重的可能导致系统崩溃；另一种是攻击者将精心设计的代码放到缓冲区，通过缓冲区溢出准确地控制跳转地址，将程序流程引向预定的地址，CPU 就会执行这个指令，从而达到攻击的目的。如果入侵者在预定的地址中放置设计好的代码 Shellcode，则当程序被溢出时，入侵者就能获得对系统的控制权。因此，入侵者进行攻击的关键就是修改以较高权限运行的程序跳转指令的地址。

入侵者为了修改以较高权限运行的程序跳转指令的地址，一般要经过以下 3 个步骤。

(1)将需要执行的代码放到目标系统的内存。下面是两种常用的方法：

- 植入法：通过主机，将需要执行的代码(目标平台上可执行的)直接放到缓冲区。
- 利用已经有的代码：只要修改传入参数。

(2)猜测缓冲区的地址。当黑客使用缓冲区进行攻击时，需要确定缓冲区的地址。由于程序不会一次向堆栈中压入成百上千字节的数据，因此一旦知道了堆栈的开始地址，就可以尝试猜测要使其溢出的缓冲区的地址，也就是相对于起始地址的偏移量。

(3)修改返回地址，控制程序跳转，改变程序流程。下面是 3 种常用的方法：

- 修改程序返回地址：用预先设定好的地址替换程序原来的返回地址。
- 在缓冲区附近放一个函数指针，指向入侵者定义好的指令。
- 使用 setjmp/longjmp：C 语言的 setjmp/longjmp 是一个检验/恢复系统，可以在检验点设定 setjmp(buffer)，用 longjmp(buffer)恢复检验点。入侵者可以利用 longjmp(buffer)跳转到预定代码。

3.5.3 缓冲区溢出攻击的防范措施

针对缓冲区溢出攻击，可以采取多种防范措施。

1. 编写安全的代码

编写安全的程序代码是解决缓冲区溢出漏洞的最根本方法。在程序开发时就考虑可能会有的安全问题，以杜绝发生缓冲区溢出攻击的可能性。例如，在 C 程序中使用数组时，注意检查数组边界的溢出情况，那么针对数组的缓冲区溢出就不会发生。

2. 指针完整性检查

堆栈保护是一种提供程序指针完整性检查的编译器技术，通过检查函数活动记录中的返回地址来实现。指针完整性检查是指在程序指针被引用之前先检测它是否被改变，一旦改变就不会被使用。这样，即使攻击者成功改变了程序的指针，也会因先前检测到指针的改变而失效。

3. 关闭不必要的特权程序

由于缓冲区溢出只有在获得更高的特权时才有意义，因此特权程序，例如，UNIX 下的

suid 程序和 Windows 下由系统管理员启动的服务进程经常是缓冲区溢出攻击的目标。所以关闭一些不必要的特权程序可以降低被攻击的风险。

4. 及时给系统漏洞打补丁

事实上，让普通用户解决其遇到的安全问题是不现实的。由于大部分的入侵是利用一些已经公布的漏洞实现的，及时给这些漏洞打上补丁，无疑会增强系统抵抗攻击的能力。

3.6　拒绝服务攻击

在各种网络安全技术中，拒绝服务攻击由于简单易学、攻击简单、容易达到目的、难以防止和追查等原因已经成为比较常见的一种攻击形式。随着 Internet 的日渐壮大和成熟，防范拒绝服务攻击越来越成为一个需要考虑的问题，而分布式拒绝服务（DDoS）攻击作为一种新型的攻击形式，其危害性更大。

3.6.1　拒绝服务攻击的概念

拒绝服务（denial of service，DoS）攻击是一种简单易学、应用广泛、实用性和可操作性强的攻击方式，其目的是使目标主机或网络失去及时响应外界请求的能力。简单地说，任何导致服务器无法对合法用户提供正常服务的攻击都可以称为拒绝服务攻击。

当对诸如网络带宽、磁盘空间、内存、CPU 处理能力等资源的合理请求大大超过系统的处理能力时，就会造成拒绝服务。例如，过多的进程将系统的内存空间耗尽，或者对已经满载的 Web 服务器提出大量的请求，都会使正常的服务因得不到满足而产生拒绝服务。

DoS 攻击一般采用一对一的方式，当攻击目标的 CPU 速度、内存或网络带宽等各项性能指标比攻击者的性能低时，其效果是明显的。随着计算机与网络技术的发展，计算机的处理能力迅速增长，内存大大增加，同时也出现了千兆级的网络，这无疑加大了 DoS 攻击的困难程度。因为目标机器对恶意攻击包的“消化能力”加强了。例如，黑客的攻击软件每秒钟可以发送 3 000 个攻击包，但目标主机的网络带宽每秒钟可以处理 10 000 个攻击包，这样一来攻击就不会产生什么效果，此时分布式拒绝服务攻击应运而生。

分布式拒绝服务（distributed denial of service，DDoS）攻击是在传统的 DoS 攻击基础上产生的一类攻击方式，是指攻击者借助于客户机/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攻击能力。例如，当攻击者的内存、网络带宽等性能比目标机器低时，对目标机器的 DoS 攻击不能起作用，但当攻击者联合 10 台这样的机器，或者 100 台甚至上千台同时对目标机器发动 DoS 攻击时，目标机器就会瘫痪。

3.6.2　拒绝服务攻击的原理

为了说明拒绝服务攻击的原理，下面将对 DoS 攻击和 DDoS 攻击分别进行分析。

1. DoS 攻击

拒绝服务常见的就是入侵者通过向目标机器发送大量的数据包，导致目标网络的所有可用资源全部耗尽。下面通过分析几个典型的攻击实例来说明拒绝服务攻击的原理。

1)Land 攻击

Land 攻击主要是利用 TCP 初始连接建立期间的应答方式存在的问题进行攻击,其攻击的关键在于服务器端和客户端都有各自的序列号。在正常的通信过程中,对于每一次数据传输,接收端都必须发送一个应答包,其中包含期望从发送端所接收的下一个包的序列号。例如,发送端说:“我正在给你发送一个序列号为 5 000 占 1 000 字节的数据包。”接收端则应答:“好,我收到了,现在正在等待序列号为 6001(5 000+1 000+1)的数据包。”

通信双方若要建立 TCP 连接,首先必须完成 TCP 的 3 次握手。客户端作为发送端首先发送一个序列号为 101 的连接请求(SYN=1,ACK=0),这是第一次握手;服务器作为接收端发送一个包含自己的初始序列号 4 999、期待的序列号 101+1 的应答(SYN=1,ACK=1)包,这是第二次握手;客户端收到应答包之后,将对方的序列号加 1,再发送一个序列号为 101+1 的验证应答包(SYN=0,ACK=1)以完成第三次握手。这样,客户端和服务器都知道了对方的序列号,以后就可以进行数据传输了。TCP 的 3 次握手过程如图 3-11 所示。

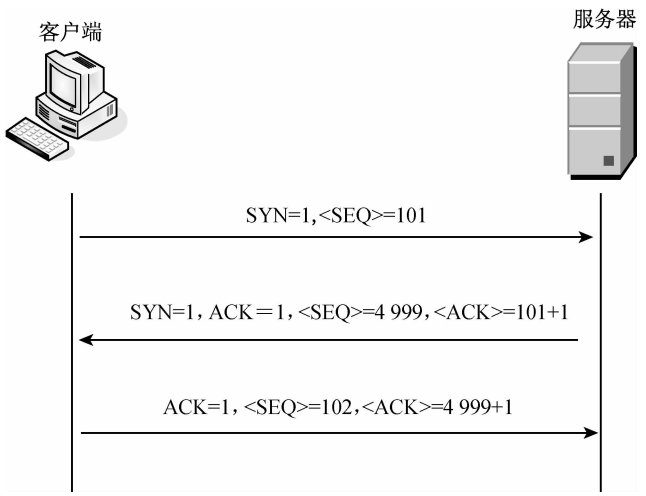

图 3-11 正常的 TCP 三次握手过程

若将源 IP 地址和目的 IP 地址都设成目标机器的地址,目标机器就会把包发送给自己。目标机器等待自己的序列号得到应答,而这个应答包却是它自己刚刚发送出去的,并且其应答序列号是攻击者的序列号(102)。由于这个序列号同目标机器所期望的序列号差别太大(不在接收窗口范围内),TCP 会认为这个包有问题而将之丢弃。这样,目标机器再次重发数据包。这对于 TCP 来说,意味着“那不是我所期望的包,请重发”。这将导致无限循环:目标机器一直给自己发送错误应答,并希望能够看到具有正确序列号的应答返回。

由于 TCP 是具有高优先权的内核级进程,这也就意味着 TCP 相对其他非内核级应用程序具有更高的权限。所以,它可以中断其他的正常系统操作,以声明更多的内核资源来处理进入的数据。这样,无限循环很快会消耗完系统资源,引起大多数系统死机。land 攻击过程如图 3-12 所示。

2)SYN Flood 攻击

SYN Flood 攻击同样是利用 TCP 连接的漏洞进行攻击,但与 Land 攻击不同的是,SYN Flood 攻击通过给目标主机发送伪造的、带有虚假源 IP 地址的 SYN 数据包,而且这个源 IP 都是互联网上不存在的地址。目标主机收到 SYN 请求之后,会按照请求的 SYN 数据包的

源 IP 地址发送一个 SYN/ACK 数据包，由于这个源 IP 地址是虚假不存在的地址，目标主机发送的 SYN/ACK 包根本不能得到回应，服务器会保持这个未完成的连接直到超时。

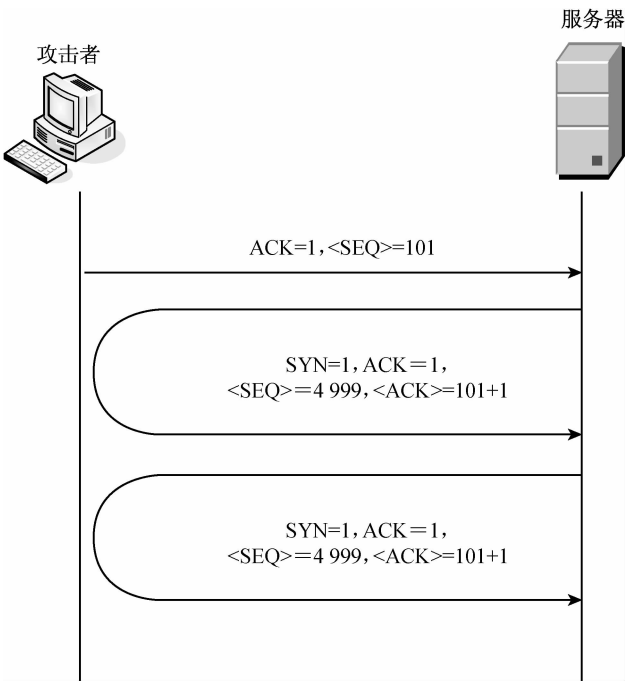

图 3-12　Land 攻击过程示意图

对于每个连接请求，系统为其开辟出一个缓冲区，每个新到的 SYN 请求都会放到等待队列中。由于缓冲区只有有限的空间，若攻击者连续不断地发送 SYN 数据包，就会导致缓冲区充满虚假的 SYN 连接信息，这时服务器就会丢弃新的连接请求，即使缓冲区中有部分连接由于等待超时而释放出空间，也会因连接请求的数量过多而导致正常的 SYN 请求无法得到响应。

3）Smurf 攻击

Smurf 攻击主要利用的是 IP 协议的直接广播特性。其原理是，攻击者发送一个源地址为目标主机的 IP 地址、目的地址为某网络的广播地址的 ICMP echo 请求包，此时，该网络上所有的主机都会向目标主机回应 ICMP echo 应答包。如果这时一个以太网的规模较大，可能会有上百台的主机对收到的 ICMP echo 请求进行回复，从而使目标主机被大量的 echo 信息吞没而导致其无法处理其他任何网络传输，停止为合法的用户提供服务。

2. DDoS 攻击

虽然同样是拒绝服务攻击，但与 DoS 攻击不同的是，DDoS 攻击侧重于利用傀儡主机。在实施 DDoS 攻击前，攻击者首先控制若干个主控傀儡机（是指被攻击者入侵并完全控制，且运行着特定攻击程序的主机，俗称“肉鸡”），然后再由主控傀儡机去控制多个攻击傀儡机。在进行 DDoS 攻击时，攻击者向主控傀儡机发出攻击命令后，每个主控傀儡机再将这个命令向自己控制的攻击傀儡机发送，由攻击傀儡机向目标主机发动拒绝服务攻击。DDoS 攻击过程如图 3-13 所示。

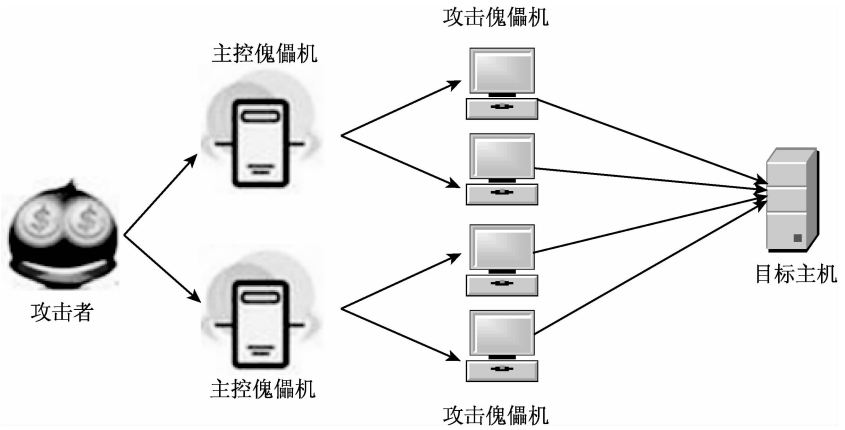

图 3-13 DDoS 攻击示意图

由于攻击者使用的傀儡机越多，目标主机事后的分析依据也越多，所以在占领一台机器后，攻击者会先做好两件事：

- 考虑如何留好后门。所谓“后门”，是指绕过安全性控制而获取对程序或系统访问权的方法。攻击者在利用各种手段入侵到目标主机以后，为了长期入侵该主机，同时也为下次进入系统时更方便一些，往往会留下后门。
- 如何清理日志。简单地说，就是擦掉脚印，不让自己做的事被别人察觉到。对于日志，若攻击者全部删掉的话，网络管理员发现日志都没了就会知道有人入侵，尽管无法从日志发现是谁干的；若攻击者仅仅将有关自己的日志项目删掉，网络管理员就很难发现异常的情况，这样就可以长时间地入侵并利用傀儡机。但在实施 DDoS 攻击时，由于攻击傀儡机的数量太大，即使有很好的日志清理工具，要清理所有攻击傀儡机上的日志工作量也十分庞大。为了避免因为某些傀儡机没有清理或清理得不彻底而导致被攻击者发现的情况出现，攻击者通过控制主控傀儡机来间接控制攻击傀儡机，这样攻击者只需清理主控傀儡机上的日志即可。

3.6.3 拒绝服务攻击的防范

目前，还没有一种有效的方法能够抵御 DoS 和 DDoS 攻击，但可以采取一定的措施确保网络系统在最短时间内恢复正常，并及时准确地收集相关入侵信息以便尽可能地减小损失。

1. 与网络服务提供商合作

与网络服务提供商配合对路由访问进行控制和对网络流量进行监视，以实现对带宽访问量的限制以及不同访问地址在同一时间对带宽的占有率，并在遭受入侵时允许合法用户访问他们的路由器。

2. 优化路由和服务器

对路由器进行合理设置可以降低拒绝服务攻击的风险，例如，在路由器上设置 TCP 监听功能，不允许路由器向外发送不可到达的 ICMP 包等。

对于服务器，可以禁止一切不必要的服务，并且将网站分布在不同的物理主机上，每台主机只包含网站的一部分，这样就可以避免网站在遭受攻击时全部瘫痪。

3. 检查漏洞

网络安全管理员应当对系统和相关安全软件的运用方法和原理了如指掌，时刻注意系统的运行情况，对系统配置和安全漏洞经常进行检查。

3.7　电子邮件攻击

电子邮件攻击也称为邮件炸弹攻击，是目前使用较多的一种攻击手段，是指用伪造的 IP 地址和电子邮件地址或利用某些特殊的电子邮件软件，在一定时间内向同一邮箱发送成千上万的内容相同的大容量邮件，这些邮件也称为垃圾邮件。由于每一个邮箱的容量是有限的，当数量庞大的邮件到达邮箱时，就会挤满邮箱，造成拒绝服务攻击。

3.7.1　电子邮件攻击的原理

电子邮件炸弹可以说是目前网络安全中最为流行的一种恶作剧方法，这些用来制作恶作剧的特殊程序称为 E-mail bomber(邮件炸弹)，攻击者用它来对某个或多个邮箱发送大量的邮件，使网络流量加大、消耗系统资源，从而使系统瘫痪。以下是几种常见的邮件攻击方法。

1. 回复转发的死循环

假设甲要对乙的邮箱进行攻击，甲首先会申请两个电子邮箱：邮箱 A 和邮箱 B。其中，邮箱 A 设置为启动转发和自动回复功能，并且转发的对象为乙的邮箱；邮箱 B 设置为启动自动回复功能。然后，甲利用邮箱 B 向邮箱 A 发送邮件，由于邮箱 A 和邮箱 B 都有自动回复功能，所以会进行循环发信，而邮箱 A 收到的邮件都会转发给乙的邮箱，这样乙的邮箱很快就被填满了。

2. “胀”破邮箱容量

攻击者申请一个邮箱，并开启匿名功能。然后使用诸如 Outlook 等邮件工具向目标邮箱发送一个大容量的附件，在启动并设置 Outlook 中的“邮件拆分大小”(如可以设置成拆分所有大于 20 KB 的邮件)功能后进行发送。这样以后只要使用这个经过设置的邮箱发送邮件，一旦邮件的大小超过了规定的字节数，Outlook 就会自动将邮件进行拆分。若攻击者不间断地进行发送，就会使目标邮箱被大量的邮件塞满，从而导致拒绝服务。

3. 基于软件的攻击

现在，已经有很多种能够自动产生邮件炸弹的软件，而且有逐渐普及的趋势，并且这类软件简单易用，只需在“轰炸地址”中输入需要攻击的邮箱地址，设置邮箱的发送服务器(如 SMTP 服务器)，以及发送量和发送邮件的线程数目等，就可以进行自动攻击。

3.7.2　电子邮件攻击的防范

邮件炸弹的防范工作比较繁琐，而且很难保证万无一失，但可以使用如下方法来尽可能地避免邮件炸弹的袭击，以及做好善后处理。

- 不随意公开自己的邮箱地址。

- 谨慎使用自动回复功能。不要认为邮件发送有回复功能就可以报复发炸弹的人，因为发件人有可能用的是假的地址发邮件，而且这个地址也许就是收件人的地址。
- 设置邮件过滤功能。为邮件设置一个过滤器，这样邮件系统将对任何待接收的邮件进行过滤，一旦发现有可疑之处，立即删除。
- 邮件的备份。当邮箱“中弹”时，有用的备份可以在邮件工具软件清除垃圾邮件后保留有用的信件。

3.8 木　　马

木马是一种非常危险的恶性程序，其作用是偷偷监视用户的操作和窃取用户的敏感信息，例如，偷窃上网密码、游戏账号、网上银行账号等，从而给用户造成巨大的损失。

3.8.1 木马的概念

特洛伊木马(Trojan horse)简称木马，其名称取自希腊神话中的特洛伊木马记。木马是一种潜伏在计算机中、受外部用户控制以窃取本机信息或控制权的黑客工具，具有隐蔽性和非授权性的特点。所谓隐蔽性，是指木马的设计者为了防止木马被发现，往往采用多种手段(如隐藏在其他程序的后面)来隐藏木马，这样服务端即使发现感染了木马，由于不能确定其具体位置，所以无法清除干净；所谓非授权性，是指木马的服务一旦运行并被控制端连接，控制端将享有服务端的大部分操作权限，例如，给计算机增加口令，浏览、移动、复制或删除文件，修改注册表等。

严格地说，木马程序并不能算是一种病毒，因为它不会自我繁殖，也并不“刻意”地去感染其他文件，而是将自身伪装吸引用户下载执行，或者捆绑在网页中，使用户在浏览网页时受到侵害。木马程序向攻击者提供打开被攻击者计算机的门户，使攻击者可以任意毁坏、窃取被攻击者的文件，甚至远程操控被攻击者的计算机。

根据古希腊传说，特洛伊王子帕里斯访问希腊，诱走了王后海伦，希腊人因此远征特洛伊。围攻 9 年后，到第 10 年，希腊将领奥德修斯献了一计，就是把一批勇士埋伏在一匹巨大的木马腹内，放在城外后，佯作退兵。特洛伊人以为敌兵已退，就把木马作为战利品搬入城中。到了夜间，埋伏在木马中的勇士跳出来，打开了城门，希腊将士一拥而入攻下了城池。

3.8.2 木马的原理

一个完整的木马程序一般由服务端程序和控制端程序两部分组成。其中，客户端是用于攻击者植入木马、远程控制的机器，服务端是被种植木马的机器。作为服务端的主机一般会打开一个默认的端口并进行监听，如果有客户端向服务端主机的这一端口提出连接请求，服务端主机上的相应程序就会自动运行，来应答客户端主机的请求，这个程序称为守护进程(UNIX 的术语，一种独立于控制端并且周期性地执行某种任务或等待处理某些发生的事件

的进程，现在已经被移植到了微软系统上）。黑客利用木马工具进行网络入侵一般分为以下几个步骤。

1. 配置木马

木马程序一般都有木马配置程序，主要是为了实现木马伪装和信息反馈两方面的功能。所谓木马伪装是为了在服务端尽可能地隐藏木马而采取的诸如修改图标、捆绑文件、定制端口、自我销毁等多种手段；信息反馈是指对信息反馈的方式或地址进行设置，例如，设置信息反馈的邮件地址、IRC（Internet relay chat 的简称，一种网络聊天工具）号、QQ 号等。

2. 传播木马

木马的传播方式主要有两种：一种通过 E-mail，控制端将木马程序以附件的形式放在邮件中发送出去，收信人只要打开附件就会被种植木马；另一种是软件下载，有的网站以提供软件下载的名义，将木马捆绑在软件安装程序上，一旦下载后运行这些程序，木马就会自动安装。

由于很多人对木马的危害有一定的了解和警惕，为了达到入侵的目的，黑客们开发了多种功能来伪装木马，以达到降低用户警觉、欺骗用户的目的。下面是几种常见的伪装方式：

（1）修改图标。用户在 E-mail 的附件中看到诸如 HTML、TXT、ZIP 等图标的文件有可能就是木马程序，因为现在已经有技术可以将木马服务端程序的图标改成各种常见文件的图标，但这种木马并不多见。

（2）捆绑文件。这种伪装手段是将木马捆绑到一个安装程序上，例如，下载的可执行软件等。当安装程序运行时，木马先进入系统。

（3）出错显示。当用户打开伪装成正常文件的木马程序时，会弹出一个假的诸如“文件已破坏，无法打开！”之类的错误提示框，此时木马已经悄悄地进入了用户的系统。

（4）定制端口。传统的木马程序中，其服务端端口是固定的，所以只要查看一下特定的端口就知道是否感染了木马。木马的设计者也意识到了这个缺陷，所以现在的木马都提供了定制端口的功能。控制端用户可以在 1 024～65 535 之间任选一个端口作为木马的端口，这样就给判断系统是否感染木马以及木马的类型带来了困难。

（5）自我销毁。服务端用户运行木马或捆绑木马的程序后，木马就会将自己复制到 Windows 系统文件（C:\Windows、C:\Windows\system 或 C:\Windows\temp 目录下）中，一般情况下，源木马文件与系统文件夹中的木马文件的大小相同（捆绑文件木马除外），所以若用户发现中了木马，只要在近来收到的邮件或下载的软件中找到源木马文件，然后与系统文件夹中相同大小的文件进行比较就可以找出木马。而木马的自我销毁功能是指安装完木马后，源木马文件将自动销毁，这样服务端用户就很难找到木马的来源，在没有专门查杀木马的工具的帮助下，就很难删除木马了。

（6）木马更名。对于安装到系统中的木马，若名称不作修改的话，用户只要根据名称在系统文件中查找就很容易发现木马。所以，现在的很多木马在安装后将名称设置成与系统文件名差不多的名称，例如，有的木马将名称改为 explor. exe 或 expolr. exe，这样用户就很难发现是系统文件还是木马。

3. 运行木马

木马在安装时首先将自己复制到 Windows 的系统文件夹中，然后在注册表、启动组、非启动组中设置好木马的触发条件，这样木马的安装就完成了。触发条件是指启动木马的条

件，一般出现在注册表、WIN. INI、SYSTEM. INI、Autoexec. bat 和 Config. sys、*. INI、捆绑文件和启动菜单中。

木马被激活后进入内存，并开启木马端口，准备与控制端建立连接。这时服务端用户可以在 MS-DOS 方式下通过输入 netstat -an 来查看端口开放情况，一般个人计算机在脱机状态下是不会有端口开放的，一旦有端口开放就要注意是否感染木马了。在上网过程中由于下载软件、网上聊天、浏览网页等必然会打开一些端口，除了诸如 1 024 以下的端口为保留端口、4 000 为 QQ 的通信端口，以及 6 667 为 IRC 的通信端口等常见的端口外，如果发现还有其他的端口被打开，尤其是数值较大的端口，那就要注意是否感染了木马。

4. 信息泄露

一般木马都有一个信息反馈机制。所谓信息反馈机制，是指木马安装成功后会收集一些服务端的软硬件信息，并通过 E-mail、IRC 等方式告知控制端用户。

5. 建立连接

一个木马要建立连接首先必须满足两个条件：一是服务端已成功安装了木马程序；二是控制端和服务端都要在线。传统的连接是控制端通过端口与服务端建立连接，此时控制端需要知道服务端的 IP 地址才能连接。而现在，由于动态 IP 和路由器的普及，这种连接方式就有了很大的不足。因为对于动态 IP 地址，其频繁更换导致控制端在下次上网时找不到服务端的 IP 地址而无法与服务端连接；由于路由器将网络划分为内网和外网，而且外网是无法访问内网的，这样控制端只能连接到外网的机器而不能连接到内网的机器。

对于这一不足，现在已经产生了一种新的连接方式，即服务端通过端口主动连接控制端。这样，不论服务端的 IP 地址如何变化，还是内网的机器，木马的连接都可以建立。

6. 远程控制

木马建立连接后，控制端通过木马程序对服务端进行远程控制，例如，窃取密码、操作文件、修改注册表和系统操作等。

3.8.3 木马的防范与清除

由于木马危害的严重性，以及新的变种及类型层出不穷，在检测清除木马的同时，用户可以从以下几方面来提高防范意识。

(1)不要下载、接收或执行任何来历不明的软件或文件。下载时，建议到一些信誉高的站点下载。下载的软件在安装前，最好用反病毒软件和木马专杀工具进行检查，确定无毒和无木马后再使用。

(2)不要浏览不健康、不正规的网站。因为这些网站都是“网页挂马”的高发地带，访问这些网站非常危险。

(3)尽量少用共享文件夹。如果因工作等原因必须将文件夹设置成共享，最好将所有需要共享的文件都放到一个新建立的共享文件夹中，但系统目录不要设置成共享。

(4)安装反病毒软件、木马专杀工具和防火墙，并及时升级代码库。

(5)及时给操作系统打上补丁，并经常升级常用的应用软件。

3.9　黑　　客

黑客是 hacker 的音译，其引申意义是指“干了一件非常漂亮的事”。最初的黑客是指独立思考、奉公守法的计算机迷，他们智力超群，对计算机全身心的投入，而且具有超常的编程水平和计算机系统知识。但到了今天，“黑客”一词已被用于那些专门利用计算机网络进行破坏或恶作剧的人，也称为骇客。

3.9.1　黑客的进攻过程

尽管黑客攻击的目标不同、技能有高低之分、手法多种多样，但他们对目标施行攻击的过程却大致相同。

1. 信息收集

黑客首先确定攻击目标。然后利用新闻报道、网站介绍、论坛上的求助信息、网站中的公开信息等社会信息或黑客技术等方法和手段来收集目标主机的各种信息，这些信息包括目标主机的类型、IP 地址、所在网络的类型以及操作系统的类型和版本等，根据这些信息进行分析，可以得到有关目标系统中可能存在的漏洞。这是黑客攻击前最为重要的一步。

2. 扫描

俗话说“苍蝇不叮无缝的蛋”，系统的漏洞会为攻击提供机会和入口。在信息收集的基础上，黑客利用扫描工具，在较短的时间内对目标系统进行扫描，进一步确定攻击对象的漏洞。

3. 模拟攻击

根据信息收集和扫描得到的信息，建立模拟环境，然后对模拟目标机进行一系列的攻击。通过检查目标机的日志，可以了解攻击过程中留下的“痕迹”，这样攻击者就知道需要删除哪些文件来毁灭其入侵证据了。

4. 获取访问权并提升权限

当黑客利用收集到的信息，找到目标系统的漏洞，并取得一定的访问权之后，黑客的入侵也将正式开始。而黑客一旦获取了访问权，就会试图将自己的普通用户权限提升至超级用户权限，以便对系统进行完全控制。

5. 窃取信息

窃取信息是黑客发起网络攻击的主要目的，一旦黑客得到了系统的完全控制权，就可以对一些敏感数据进行篡改、添加、删除和复制，以及通过对敏感数据的分析，为进一步攻击应用系统做准备。

6. 掩盖踪迹

如果完成攻击后攻击者立刻离开而不做任何善后工作，那么其行踪将很快被发现，因为所有的网络操作系统都提供日志记录功能，该功能是将系统上发生的一切操作记录下来。所以，为了不被发现，黑客一般都会清除自己所有的入侵痕迹，其主要工作包括：禁止系统审计，隐藏作案工具，清空事件日志，替换系统常用操作命令等。

7. 创建后门

一般黑客在攻入系统后会不止一次地进入该系统，为了方便下次进入该系统，黑客会留下一个后门。

3.9.2 黑客常用的攻击方法

黑客常用的攻击方法主要有以下几种：

(1)口令入侵。这种方法是指使用某些合法用户的账号和口令登录到目标主机，然后实施攻击。但前提是必须得到该主机上某个合法用户的账号，再进行口令的破译。

(2)放置木马程序。木马程序可以直接侵入用户的计算机并进行破坏，它通常伪装成工具软件或游戏等诱使用户打开，一旦用户打开或执行了这些程序，木马就会自动安装到 Windows 目录下并悄悄执行。这样，当中木马的用户与黑客都上网时，黑客就可以对用户的机器实现远程控制。

(3)Web 欺骗技术。黑客制作一个与用户上网要浏览的网页的复制，或将用户要浏览的网页的 URL 改写为指向黑客自己的服务器，这样，当用户浏览目标网页并填写敏感信息时，黑客就可以窃取用户的个人信息了。

(4)电子邮件攻击。电子邮件攻击主要表现为电子邮件炸弹和电子邮件欺骗两种。电子邮件炸弹是攻击者通过给目标邮箱发送邮件，致使受害人邮箱拒绝提供正常的服务，而电子邮件欺骗则是攻击者佯称自己是系统管理员，然后给用户发送邮件要求用户修改口令或在邮件的附件中插入病毒或木马。

(5)通过结点进行攻击。黑客在入侵一台主机后，往往以此主机为根结点(以隐蔽其入侵路径，避免留下痕迹)，攻击其他主机。同时利用网络监听，尝试入侵同一网络内的其他主机，或者通过 IP 欺骗和主机信任关系，攻击其他主机。

(6)网络监听。将网卡设置为监听模式，便可将同一网段中正在传输的信息截获，而黑客一般都利用网络监听来获取用户口令。

(7)安全漏洞攻击。目前常用的系统都有各种各样的安全漏洞，其中有的是操作系统或应用软件本身就具有的，有的则是由于系统管理员配置错误引起的。这些漏洞会给黑客以可乘之机。

(8)获取特权。黑客利用各种木马、后门程序非法获得对用户机器的完全控制权，或者利用黑客自己编写的能够导致缓冲区溢出的程序进行攻击，使黑客获得超级用户的权限。

3.9.3 黑客常用的工具

黑客常用的工具有以下几种。

1. 扫描器

扫描器是黑客必备的工具之一。所谓扫描器，是指自动检测远程或本地主机安全性弱点的程序，主要通过选择 TCP/IP 端口和服务，并记录目标主机的回答来获得目标主机的相关信息。

2. 木马

木马是指任何提供了隐藏的、用户不希望的功能的程序。这个程序的特点在于欺骗性，

往往伪装成合法程序，从而诱惑用户激活，以便悄悄发挥功能。木马程序由客户端程序和服务端程序组成，一旦目标机器运行了服务端程序，那么黑客就可以利用客户端对目标机器进行远程控制。

3. 网络嗅探器

在以太网或其他共享传输介质的网络上放置网络嗅探器，可以使网络接口处于广播状态，从而截获网上传输的诸如口令、账号等敏感信息。而且由于网络嗅探器的被动监听，所以很难被发现。

4. 攻击工具

这里的攻击工具是指所有黑客用来进行各种攻击的工具。因为攻击的类型是多样的，所以工具也是多种多样的，如各种拒绝服务攻击程序、IP 数据包攻击程序、邮件攻击程序、漏洞溢出程序等。

5. 口令破解

由于当前许多计算机的验证都是基于口令的，因而只要知道了一个账号和密码，黑客就能够利用这个账号进行登录。黑客一般在得到一个账号后，会使用口令破解工具进行破解，所以口令破解工具对黑客而言是十分重要的。口令破解主要分为远程破解和本地破解。所谓远程破解工具，是指利用口令字典对远程服务的某个账户逐个尝试，直至得到正确的密码。本地口令破解工具是指对密码存储的文件(如 UNIX 系统的 password 文件和 Windows 系统的 sam 文件)进行破解。

习　题　3

一、名词解释

端口　网络监听　Web 欺骗　IP 欺骗　DNS 欺骗　拒绝服务攻击　缓冲区溢出　电子邮件炸弹　木马　ARP 欺骗

二、简答题

1. 简述网络攻击的步骤。
2. 网络攻击常用的技术有哪些?
3. 端口扫描的原理及防范措施是什么?
4. 网络监听的原理及防范措施是什么?
5. Web 欺骗、DNS 欺骗、IP 欺骗及 ARP 欺骗的原理及防范措施是什么?
6. 缓冲区溢出的原理、攻击过程及防范措施是什么?
7. 拒绝服务攻击的原理及防范措施是什么?
8. 电子邮件攻击的原理及防范措施是什么?
9. 木马的原理及防范措施是什么?
10. 黑客常用的攻击方法及攻击过程是什么?