三级网络笔记第六章网络安全技术 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/349/2021_2022__E4_B8_89_E7_BA_A7_E7_BD_91_E7_c97_349888.htm 第六章 网络安全技术 网络管理包括五个功能：配置管理，故障管理，性能管理，计费管理和安全管理。 代理位于被管理的设备内部，它把来自管理者的命令或信息请求转换为本设备特有的指令，完成管理者的指示，或返回它所在设备的信息。 管理者和代理之间的信息交换可以分为两种：从管理者到代理的管理操作；从代理到管理者的事件通知。 配置管理的目标是掌握和控制网络和系统的配置信息以及网络各设备的状态和连接管理。现代网络设备由硬件和设备驱动组成。 配置管理最主要的作用是可以增强网络管理者对网络配置的控制，它是通过对设备的配置数据提供快速的访问来实现的。 故障就是出现大量或严重错误需要修复的异常情况。故障管理是对计算机网络中的问题或故障进行定位的过程。 故障管理最主要的作用是通过提供网络管理者快速的检查问题并启动恢复过程的工具，使网络的可靠性得到增强。故障标签就是一个监视网络问题的前端进程。 性能管理的目标是衡量和呈现网络特性的各个方面，使网络的性能维持在一个可以接受的水平上。 性能管理包括监视和调整两大功能。 记费管理的目标是跟踪个人和团体用户对网络资源的使用情况，对其收取合理的费用。记费管理的主要作用是网络管理者能测量和报告基于个人或团体用户的记费信息，分配资源并计算用户通过网络传输数据的费用，然后给用户开出帐单。 安全管理的目标是按照一定的方法控制对网络的访问，以保证网络不被侵害，并保证

重要的信息不被未授权用户访问。 安全管理是对网络资源以及重要信息访问进行约束和控制。 在网络管理模型中，网络管理者和代理之间需要交换大量的管理信息，这一过程必须遵循统一的通信规范，我们把这个通信规范称为网络管理协议。 网络管理协议是高层网络应用协议，它建立在具体物理网络及其基础通信协议基础上，为网络管理平台服务。 目前使用的标准网络管理协议包括：简单网络管理协议SNMP，公共管理信息服务/协议CMIS/CMIP，和局域网个人管理协议LMMP等。 SNMP采用轮循监控方式。代理/管理站模式。管理节点一般是面向工程应用的工作站级计算机，拥有很强的处理能力。代理节点可以是网络上任何类型的节点。SNMP是一个应用层协议，在TCP/IP网络中，它应用传输层和网络层的服务向其对等层传输信息。 CMIP的优点是安全性高，功能强大，不仅可用于传输管理数据，还可以执行一定的任务。 信息安全包括5个基本要素：机密性，完整性，可用性，可控性与可审查性。 3 D1级。D1级计算机系统标准规定对用户没有验证。例如DOS。WINDOS3。X及WINDOW 95（不在工作组方式中）。Apple的System7。X。 4 C1级提供自主式安全保护，它通过将用户和数据分离，满足自主需求。 C1级又称为选择安全保护系统，它描述了一种典型的用在Unix系统上的安全级别。 C1级要求硬件有一定的安全级别，用户在使用前必须登陆到系统。 C1级的防护的不足之处在与用户直接访问操作系统的根。 9 C2级提供比C1级系统更细微的自主式访问控制。为处理敏感信息所需要的最底安全级别。C2级别还包含有受控访问环境，该环境具有进一步限制用户执行一些命令或访问某些文件的权限，而且

还加入了身份验证级别。例如UNIX系统。XENIX。Novell 3。0或更高版本。WINDOWS NT。 10 B1级称为标记安全防护，B1级支持多级安全。标记是指网上的一个对象在安全保护计划中是可识别且受保护的。B1级是第一种需要大量访问控制支持的级别。安全级别存在保密，绝密级别。 11 B2又称为结构化保护，他要求计算机系统中的所有对象都要加上标签，而且给设备分配安全级别。B2级系统的关键安全硬件/软件部件必须建立在一个形式的安全方法模式上。 12 B3级又叫安全域，要求用户工作站或终端通过可信任途径连接到网络系统。而且这一级采用硬件来保护安全系统的存储区。 B3级系统的关键安全部件必须理解所有客体到主体的访问，必须是防窜扰的，而且必须足够小以便分析与测试。 30 A1 最高安全级别，表明系统提供了最全面的安全，又叫做验证设计。所有来自构成系统的部件来源必须有安全保证，以此保证系统的完善和安全，安全措施还必须担保在销售过程中，系统部件不受伤害。 网络安全从本质上讲就是网络上的信息安全。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。 安全策约是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。安全策约模型包括了建立安全环境的三个重要组成部分：威严的法律，先进的技术和严格的管理。 网络安全是网络系统的硬件，软件以及系统中的数据受到保护，不会由于偶然或恶意的原因而遭到破坏，更改，泄露，系统能连续，可靠和正常的运行，网络服务不中断。 保证安全性的所有机制包括以下两部分： 1 对被传送的信息进行与安全相关的转换。 2 两个主体共享不希望对手得知的保密

信息。 安全威胁是某个人，物，事或概念对某个资源的机密性，完整性，可用性或合法性所造成的危害。某种攻击就是某种威胁的具体实现。 安全威胁分为故意的和偶然的两类。故意威胁又可以分为被动和主动两类。 中断是系统资源遭到破坏或变的不能使用。这是对可用性的攻击。 截取是未授权的实体得到了资源的访问权。这是对保密性的攻击。 修改是未授权的实体不仅得到了访问权，而且还篡改了资源。这是对完整性的攻击。 捏造是未授权的实体向系统中插入伪造的对象。这是对真实性的攻击。 被动攻击的特点是偷听或监视传送。其目的是获得正在传送的信息。被动攻击有：泄露信息内容和通信量分析等。 主动攻击涉及修改数据流或创建错误的数据流，它包括假冒，重放，修改信息和拒绝服务等。假冒是一个实体假装成另一个实体。假冒攻击通常包括一种其他形式的主动攻击。 重放涉及被动捕获数据单元以及后来的重新发送，以产生未经授权的效果。 修改消息意味着改变了真实消息的部分内容，或将消息延迟或重新排序，导致未授权的操作。 拒绝服务的禁止对通信工具的正常使用或管理。这种攻击拥有特定的目标。另一种拒绝服务的形式是整个网络的中断，这可以通过使网络失效而实现，或通过消息过载使网络性能降低。 防止主动攻击的做法是对攻击进行检测，并从它引起的中断或延迟中恢复过来。 从网络高层协议角度看，攻击方法可以概括为：服务攻击与非服务攻击。 服务攻击是针对某种特定网络服务的攻击。 非服务攻击不针对某项具体应用服务，而是基于网络层等低层协议进行的。 非服务攻击利用协议或操作系统实现协议时的漏洞来达到攻击的目的，是一种更有效的攻击手段。 网络安全的基本目标是实

现信息的机密性，完整性，可用性和合法性。 主要的可实现威胁： 3 渗入威胁：假冒，旁路控制，授权侵犯。 4 植入威胁：特洛伊木马，陷门。 病毒是能够通过修改其他程序而感染它们的一种程序，修改后的程序里面包含了病毒程序的一个副本，这样它们就能继续感染其他程序。 网络反病毒技术包括预防病毒，检测病毒和消毒三种技术。 1 预防病毒技术。 它通过自身长驻系统内存，优先获得系统的控制权，监视和判断系统中是或有病毒存在，进而阻止计算机病毒进入计算机系统对系统进行破坏。这类技术有：加密可执行程序，引导区保护，系统监控与读写控制。 2．检测病毒技术。 通过对计算机病毒的特征来进行判断的技术。如自身效验，关键字，文件长度的变化等。 3．消毒技术。 通过对计算机病毒的分析，开发出具有删除病毒程序并恢复原元件的软件。网络反病毒技术的具体实现方法包括对网络服务器中的文件进行频繁地扫描和检测，在工作站上用防病毒芯片和对网络目录以及文件设置访问权限等。 网络信息系统安全管理三个原则： 1 多人负责原则。 2 任期有限原则。 3 职责分离原则。保密学是研究密码系统或通信安全的科学，它包含两个分支：密码学和密码分析学。 需要隐藏的消息叫做明文。明文被变换成另一种隐藏形式被称为密文。这种变换叫做加密。加密的逆过程叫组解密。对明文进行加密所采用的一组规则称为加密算法。对密文解密时采用的一组规则称为解密算法。加密算法和解密算法通常是在一组密钥控制下进行的，加密算法所采用的密钥成为加密密钥，解密算法所使用的密钥叫做解密密钥。 密码系统通常从3个独立的方面进行分类： 1 按将明文转化为密文的操作类型分为：置换密码和易位密码。

所有加密算法都是建立在两个通用原则之上：置换和易位。2 按明文的处理方法可分为：分组密码（块密码）和序列密码（流密码）。 3 按密钥的使用个数分为：对称密码体制和非对称密码体制。 如果发送方使用的加密密钥和接受方使用的解密密钥相同，或从其中一个密钥易于的出另一个密钥，这样的系统叫做对称的，但密钥或常规加密系统。如果发送放使用的加密密钥和接受方使用的解密密钥不相同，从其中一个密钥难以推出另一个密钥，这样的系统就叫做不对称的，双密钥或公钥加密系统。 分组密码的加密方式是首先将明文序列以固定长度进行分组，每一组明文用相同的密钥和加密函数进行运算。 分组密码设计的核心上构造既具有可逆性又有很强的线性的算法。 序列密码的加密过程是将报文，话音，图象，数据等原始信息转化成明文数据序列，然后将它同密钥序列进行异或运算。生成密文序列发送给接受者。 数据加密技术可以分为3类：对称型加密，不对称型加密和不可逆加密。 对称加密使用单个密钥对数据进行加密或解密。 不对称加密算法也称为公开加密算法，其特点是有两个密钥，只有两者搭配使用才能完成加密和解密的全过程。 不对称加密的另一用法称为“ 数字签名 ”，既数据源使用其私有密钥对数据的效验和或其他与数据内容有关的变量进行加密，而数据接受方则用相应的公用密钥解读“ 数字签名 ”，并将解读结果用于对数据完整性的检验。 不可逆加密算法的特征是加密过程不需要密钥，并且经过加密的数据无法被解密，只有同样输入的输入数据经过同样的不可逆算法才能得到同样的加密数据。 加密技术应用于网络安全通常有两种形式，既面向网络和面向应用程序服务。 面向网络服务的加密技术通

常工作在网络层或传输层，使用经过加密的数据包传送，认证网络路由及其其他网络协议所需的信息，从而保证网络的连通性和可用性不受侵害。 面向网络应用程序服务的加密技术使用则是目前较为流行的加密技术的使用方法。 从通信网络的传输方面，数据加密技术可以分为3类：链路加密方式，节点到节点方式和端到端方式。 链路加密方式是一般网络通信安全主要采用的方式。 节点到节点加密方式是为了解决在节点中数据是明文的缺点，在中间节点里装有加，解密的保护装置，由这个装置来完成一个密钥向另一个密钥的变换。