 网络安全与网络管理技术 266. 计算机系统安全内容：安全理论与策略、计算机安全技术、安全管理、安全评价、安全产品以及计算机犯罪与侦查、计算机安全法律、安全监察等。 267. DoD(TCSEC)可信计算机系统评估标准：是美国国防部在1985年正式颁布的，它将计算机安全等级划分为四类七级，这七个等级从低到高依次为：D、C1、C2、C3、B1、B2、B3、A1。 268. 计算机系统安全问题分类：计算机系统安全问题共分为三类，它们是技术安全、管理安全和政策法律安全。 269. 技术安全：指通过技术手段(硬件的和软件的)可以实现的对于计算机系统及其数据的安全保护，要求做到系统受到攻击以后，硬件、软件不受到破坏，系统正常工作，数据不泄漏、丢失和更改。 270. 管理安全：指和管理有关的安全保障，如使得软硬件不被物理破坏，非法人员进入、机密泄露等。 271. 政策法律安全是指政府及相关管理部门所制订的法律、法规、制度等。 272. 信息安全的构成：信息安全包括计算机安全和通信安全两部分。 273. 信息安全的目标：维护信息的保密性、完整性、可用性和可审查性。 274. 保密性：使系统只向授权用户提供信息，对于未被授权使用者，这些信息是不可获取或不可理解的。 275. 完整性：使系统只允许授权的用户修改信息，以保证所提供给用户的信息是完整无缺的。 276. 可用性：使被授权的用户能够从系统中获得所需的信息资源服务。 277. 可审查性：使系统内所发生的与安全有关的动作均有说明性记录可

查。 278. 安全威胁：是指某个人、物、事件或概念对某一信息资源的保密性、完整性、可用性或合法使用所造成的危险。基本的安全威胁包括：信息泄露、完整性破坏、业务拒绝和非法使用。 279. 安全威胁的表现形式：包括信息泄露、媒体废弃、人员不慎、授权侵犯、非授权访问、旁路控制、假冒、窃听、电磁/射频截获、完整性侵犯、截获/修改、物理侵入、重放、业务否认、业务拒绝、资源耗尽、业务欺骗、业务流分析、特洛伊木马、陷门等。 280. 安全攻击：所谓安全攻击，就是某种安全威胁的具体实现。它包括被动攻击和主动攻击两大部分。 281. 被动攻击：是对信息的保密性进行攻击，即通过窃听网络上传输的信息并加以分析从而获得有价值的情报，但它并不修改信息的内容。它的目标是获得正在传送的信息，其特点是偷听或监视信息的传递。它包括信息内容泄露和业务流分析两大类。 282. 主动攻击：主动攻击是攻击信息来源的真实性、信息传输的完整性和系统服务的可用性。主动攻击一般包括中断、伪造、更改等。 283. 防护措施：一个计算机信息系统要对抗各种攻击。避免受到安全威胁，应采取的安全措施包括：密码技术、物理安全、人员安全、管理安全、媒体安全、辐射安全和生命周期控制。 284. 信息系统安全体系结构：包括安全特性、系统单元和开放系统互连参考模型(OSI)结构层次三大部分。 285. GB-17858-1999计算机系统系统安全保护等级划分的基本准则，规定计算机系统的安全保护能力划分为5个等级，最高等级为5级。 286. 网络安全：指分布式计算机环境中对信息传输、存储、访问等处理提供安全保护，以防止信息被窃取、篡改和非法操作，而且对合法用户不发生拒绝服务，网络安全系

统应提供保密性、完整性和可用性三个基本服务，在分布网络环境下还应提供认证、访问控制和抗抵赖等安全服务。完整的网络安全保障体系应包括保护、检测、响应、恢复等四个方面。 287. 网络安全策略：就是有关管理、保护和发布敏感信息的法律、规定和细则，是指在某个安全区域中，用于所有与安全活动相关的一套规则。这些规则上由此安全区域中设立的一个安全权力机构建立，并由安全控制机构来描述、实施和实现。 288. 安全策略包括：安全策略安全策略目标、机构安全策略、系统安全策略三个等级。 289. 安全策略目标：指某个机构对所要保护的特定资源要达到的目的所进行的描述。 290. 机构安全策略：指一套法律、规则及实际操作方法，用于规范某个机构如何来管理、保护和分配资源以达到安全策略的既定目标。 291. 系统安全策略：描述如何将某个特定的信息技术系统付诸工程实现，以支持此机构的安全策略要求。 292. 安全策略的基本组成部分：安全策略的基本组成包括授权、访问控制策略、责任。 293. 安全策略的具体内容：网络管理员的责任、网络用户的安全策略、网络资源的使用授权、检测到安全问题时的策略。 294. 安全策略的作用：定义该安全计划的目的和安全目标、把任务分配给具体部门人员、明确违反政策的行为及处理措施。受到安全策略制约的任何个体在执行任务时，需要对他们的行动负责任。 295. 安全服务：是指提高一个组织的数据处理系统和信息传递安全性的服务，这些服务的目的是对抗安全攻击，它们一般使用一种或多种安全机制来实现。国际标准化组织对开放系统互联参考模型规定了5种标准的安全服务，它们是：认证服务、访问控制服务、数据保密服务、数据完整性服务、防

抵赖服务。 296. 安全机制：指用来检测、预防或从安全攻击中恢复的机制。它分为两大类，一是与安全服务有关，二是与管理有关。它包括：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、防业务流分析机制、路由控制机制、公证机制等8种。 297. IP层安全协议：指在TCP/IP协议集的网络层上的安全服务，用于提供透明的加密信道以保证数据传输的安全。它的优点在于对应用程序和终端用户是透明的，即上层的软件，包括应用程序不会受到影响，用户的日常办公模式也不用改变。典型的网络层安全协议是IPSec协议。 298. IP安全协议，即IPSec是一个用于保证通过IP网络安全通信的开放式标准框架。它保证了通过公共IP网络的数据通信的保密性、完整性和真实性。 299. IPSec标准包括4个与算法无关的基本规范，它们是：体系结构、认证头、封装安全有效载荷、InterNet安全关联和密钥管理协议。 300. 认证头协议(AH)：为IP数据报提供了三种服务，对整个数据报的认证、负责数据的完整性、防止任何针对数据报的重放。 编辑推荐： 2011年计算机等级考试三级网络复习资料汇总 2011年计算机三级网络技术考试要点汇总 百考试题网校2010年全国计算机三级网络技术考后名师专访 2011年计算机三级网络技术基础笔记汇总 2011年计算机三级网络技术课后填空题汇总 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com