计算机等级考试三级网络复习纲要[15] PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/179/2021_2022__E8_AE_A1_E7_AE_97_E6_9C_BA_E7_c98_179334.htm 计算机等级考试训练软件《百宝箱》7、信息安息全性等级：（1）美国国防部和国家标准局的可信计算机系统评估准则（TCSEC）：（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。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。C2级为处理敏感信息所需要的最底安全级别。C2级别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。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。B2级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。B3级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。A1级最高安全级别，表明系统提供了最全面的安全。）（2）欧洲共同体的信息技术安全评测准则（ITSEC）（3）国际标准ISO/IEC 15408（CC）（4）美国信息技术安全联邦准则（FC）8、网络安全（1）本质：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。（2）概念：指网络系统的硬件.软件及其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,系统连续.可靠.正常地运行,网络服务不中断.（3）基本要素是实现信息的机密性、完整性、可用性和合法性。（4）组成：物理安全,人员安全,符合瞬时电磁脉冲辐射标准（TEM-PEST）.信息安全,操作安全,通信安全,计算机安全,工业安全.（5）安全性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。（6）网络安全的基本任务： P156 （7）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。（8）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。基本威胁（信息泄露或丢失、破坏数据完整性、拒绝服务、非授权访问）、渗入威胁（假冒、旁路控制、授权侵犯）、植入威胁（特洛伊木马、陷门）、潜在威胁（窃听、通信量分析、人员疏忽、媒体清理）、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。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。（9）安全攻击：中断是系统资源遭到破坏或变的不能使用是对可用性的攻击。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是对真实性的攻击。