计算机系统安全的重要性与评测标准 ：

1. 你知道下面哪些是 开源的操作系统软件 吗: Linux Android
2. 你知道下面哪些是 开源的虚拟化软件 吗: KVM+Qemu Xen
3. 计算机系统的安全性 主要来自哪几个方面的要求： 信息保护要求 人身安全要求 资产保护要求 法律法规要求
4. 下面哪些是针对计算机系统的 典型攻击模式 ：恶意代码、拒绝服务。人员错误
5. 加密是否可以解决所有计算机系统面临的所有安全性问题： 否
6. 面哪些安全操作系统是通过认证达到了美国可信计算机系统评估准则 (TCSEC)B2 级以上 的实际产品： Trusted XENIX 、 DTOS 分布式可信微内核操作系、 Multics
7. 信息安全领域内具有里程碑意义的彩虹系列中包括一个标准和一套体系，这个标准在发布时使用的纸质封皮是橘色的，也被称为 橘皮书 ：TCSEC
8. TCSEC 和 CC 标准可以用于 评估哪些计算机系统 的可信级别或评估保证级别： 操作系统、应用程序、网络组件、数据库管理系统
9. TCSEC 的可信等级划分包括 D, C1 ， C2 ， B1， B2， B3, A 四类七个等级。请问，从哪个级别开始要求 实施强制访问控制 ：标记安全保护级 (B1,
10. CC 标准中的 TOE 是评估对象， PP 是安全保护轮廓， ST 是安全目标。下面的描述正确的有哪些： 【1】 PP 是指满足特定用户需求的、一类 TOE 的、一组与实现无关的安全要求【 2】 ST 是作为一个既定 TOE 的评估基础使用的一组安全要求和规范。 【3】 TOE 是指作为评估主体的 IT 产品或系统，以及相关的指导性文档。

计算机系统基本安全概念和设计思想

1. 访问控制思想涉及主体和客体的概念，操作系统中的 主体 通常指的是什么 :进程、用户
2. 一个安全的计算机系统通常需要包括哪些 安全需求 ？： 完整性、可用性、机密性
3. 机密性 是指要对数据的内容或者存在性保密，通常采取的保护机制是什么？ ：加密、访问控制
4. 完整性 是指对数据或资源的可信赖程度，它通常用于表述防止不当或未经授权的修改。完整性包括数据的完整性和来源的完整性，通常采取的保护机制是什么？： 访问控制、记录与审计、检测与恢复
5. 计算机系统的 安全性设计应该包括的三大要 素是指什么？： 安全策略、保证、机制
6. 基于 UNIX 的视窗系统 X11 提供了一种语言，以控制对控制台（用于 X11 显示视图的）的访问，如 xhost +groucho – chico 表达了一种安全策略，即允许来自主机 groucho 的连接请求，拒绝来自主机 chico 的连接请求，试问，这里采用的是高级策略描述语言吗？ 不是
7. 访问控制 的理论基础 是什么？： 引用监控器
8. 安全内核 的设计与实现应符合的 基本原则 有那些？： 完整性、隔离性、可验证性原则

9. 安全模型是 安全策略 的清晰表述，具有的主要特点包括哪些？ ：1 只涉及安全性质，不限制系统的功能与实现 2 是简单的和抽象的，易于理解 3 是精确的，无歧义的

10. 计算机系统中 负责实施安 全 策略的软件、 硬件和人员 等 一起组成系统 的可信计算 基 (Trusted Computing Base, TCB) ，下面哪些部分不属于操作系统的 TCB ？不涉及敏感信息访问的应用程序

访问控制机制

1. 访问控制的主要任务 是什么？： 访问实施、决策、授权

2. 自主访问控制的 自主性体主要现在哪些方面 ：1 一个特定授权的用户（非所有者）能够自主地将访问权或访问权的某个子集授予其他用户 2 一个用户可以自主地将他所拥有的资源授予其他用户访问

3. 针对自主访问控制实现技术描述正确的有哪些？： 1Linux2.6 以上版本系统支持一个用户 X 将其拥有的文件 file1 只授予 Y 用户写访问 2Linux 2.6 以上版本系统支持 ACL 访问控制列表的实现模式 3Linux2.6 以上版本系统支持一个用户 X 将其拥有的文件 file2 授予所有用户读访问 4Linux 2.6 以上版本系统支持 Owner/Group/Others 9bit 位自主访问控制的实现模式

4. 基于行 的自主访问控制实现技术，是将访问控制列表信息与用户或主体的信息关联在一起，下面哪些属于基于行的自主访问控制实现技术？： 前缀表、能力表、基于口令的访问控制机制

5. 在 Linux2.6 以上系统中，如果一个用户 X 要将其文件 file 的读的权限授予 Y 用户， Y 用户与 X 用户属于统一用户组 group1 ，下面哪个操作是正确的？： chmod 740 file 、chmod g+r file 、setfacl –m u:Y:r, file

6. 木马是一段计算机程序，表面上在执行合法功能，实际上却完成了用户不曾料到的非法功能。受骗者是程序的用户，入侵者是这段程序的开发者。木马必须具有那些功能才能成功地入侵？： 1 入侵者必须有某种手段回收由木马发作为他带来的利益 2 入侵者要写一段程序进行非法操作，其行为方式不会引起用户的怀疑 3 入侵者必须设计出某种策略诱使受骗者接受这段程序 4 入侵者必须使受骗者运行该程序

7. 对强制访问控制的描述 不正确 的是什么？： 由系统来判定拥有某安全属性的主体是否允许访问某客体，但是客体的拥有者可以不受此约束。

8. 多级安全定义了安全级由密级和范畴集合组成，假设主体 A 的安全级为 {top secret: NATO ，NUCLEAR ， CRYPTO} ，客体 X 的安全级为 {secret: NATO ， NUCLEAR} ，客体 Y 的安全级为 ：{top secret: NATO ， CRYTPO} ，请根据 BLP 简单安全规则和 *规则，判定 A 对 X,Y 的访问权限 ？：A 允许读 X，允许 读 Y

9. 在操作系统实施强制访问控制时，需要控制的 客体资源 主要包括哪些类型？： 目录、文件和有名管道、消息队列、信号量集合和共享存储区、进程

10. 客体重用的定义为： “包含一个或多个客体的存储介质 (例如，页面，磁盘扇区，磁带 )的主体的重新分配。通过标准系统机制，为新的主体重新分配时不应含有任何可用的残留数据。 ”，残留数据主要会发生在下列哪些过程中？： 文件系统格式化之后的物理块空间、重新分配的内存空间、文件或目录删除之后的物理块空间、重新分配的高速缓存空间

1-3 阶段测试

1. TCSEC 的可信等级划分包括 D，C1， C2， B1， B2， B3，A 四类七个等级。请问，从哪个级别开始要求建立形式化安全模型、设计安全体系结构、并 分析和审计隐蔽存储通道？ 结构化保护级 (B2, Structured Protection )

2. 美国 Trusted Information System 研制的 Trusted XENIX 4.0 系统曾经达到过美国可信计算机系统评估准则 (TCSEC) 的那个等级？ B2

3. vSphere 是 VMware 公司推出一套服务器虚拟化解决方案，其目前的 5.0 版本已经通过认证达到了 CC 标准的哪个可信级别或评估保证级别？ EAL4+

4. 访问控制思想涉及主体和客体的概念，操作系统中的 客体 通常指的是什么？ 文件、目录

5. 基于列的自主访问控制实现技术，是将访问控制列表信息与客体的信息关联在一起，下面哪些属于 Linux 系统中实现的 基于列 的自主访问控制机制？： ACL 模式 9bit 模式

可追究机制

1. 可追踪机制 主要包括哪些机制？： 可信路径、安全审计、标识与鉴别

2. 系统中的 用户标识 必须满足那些条件？： 系统中的用户标识是不能被伪造的、系统中的用户标识必须满足唯一性

3. 基于口令的鉴别机制 是一种常用技术，其实现时需要注意的事项包括哪些？： 1 对口令允许尝试的次数进行限制 2 对每一次口令的使用和修改进行审计 3 对口令进行加密存储和访问控制 4 对传输过程中的口令进行保护

4. 用户在登录、定义用户的安全属性或改变文件的安全级时，他必须确定自己是在与真实的安全内核通信，而不是与一个特洛伊木马打交道。为此，系统必须提供的机制是什么？： 可信路径

5. 对用户建立可信路径的实现方法是，使用通用终端向核心发一个特殊信号，这个信号是不可信软件无法拦截、覆盖或伪造的，这个信号称为安全注意键。 Linux 系统中实现的安全注意键是那些键的组合？： Alt + SysRq + k

6. 审计活动 就是对系统中安全相关的行为采取的一些做法，这些做法包括哪些？： 记录、审核、检查

7. 安全审计 的主要目的是 检测和阻止 那些行为？： 1 非法用户对计算机系统的入侵行为 2 管理员的权限滥用 3 合法用户的误操作

8. 为了确保审计员获得有价值的审计记录，系统必须保证做到哪几点？： 1 保证审计追踪过程的完整性 2 保证审计记录的完整性 3 审计所有必要的事件

9. 审计事件 主要分为主体审计事件和客体审计事件，在针对主体审计事件的记录中，通常需要包括哪些信息？ 1 主体的标识 t 2 主体的当前安全级别 3 主体所属用户的标识 4 主体执行的当前事件（如：系统调用）及其结果（如成功或失败）

10. 安全审计在操作系统内核进行实现时，主要需要完成如下哪些工作？： 1 实现内核级的统一循环缓存区，用于缓存系统实时产生的各种审计记录 2 在安全相关系统调用中实现内核级的审计点，负责判定审计条件和记录审计数据 3 实现审计相关的管理接口和管理命令，用于审计的开关、审计事件和参数的设置等 4 实现一个内核级审计线程，负责监听循环缓存区是否写满，若写满，将其写入磁盘

最小特权管理、系统完整性

1. 连续保护机制 主要包括哪些机制？： 隐蔽通道分析、可信恢复、系统完整性保护、最小特权管理

2. 最小特权原则 主要是为了减少哪些危害行为？ 管理员滥用特权、特权程序被恶意利用、特权程序意外出错、管理员的误操作

3. 在操作系统中，恰当特权通常代表的是什么能力？： 超越自主访问控制策略的能力、超越强制访问控制策略的能力、执行特定受限 /安全攸关操作的能力

4. Linux 系统参照 POSIX 标准定义了一组权能，下面哪个权能代表可以执行改变属主操作？ ：CAP_OWNER

5. 在操作系统中实现最小特权管理，需要将超级用户的特权进行划分，并通常是分别分配给 4 个不同的管理员，包括：安全管理员、安全操作员、审计员和网络管理员等。根据课程介绍，你认为系统安全策略的配置权限应该分给如下哪个管理员？： 安全管理员

6. POSIX 标准建议进程 和程序文件的权能状态集合有三种，他们是什么？ ：Permitted 许可集 Inheritable 可继承集 Effective 有效集

7. 操作系统的系统调用 exec 是以新的进程映像去代替原来的进程映像，也就是说， exec 系统调用并没有创建新的进程，只是替换了原来进程上下文的内容，例如：进程的代码段、数据段、堆栈段被替换了。关于 exec 这种说法正确的本质原因是什么？： exec 时，进程的 PID 保持不变

8. Linux 中实现的权能遗传算法主要是在 exec 调用一个程序的过程中完成，新的进程权能状态主要与下面哪些因素有关？： 系统对所有进程限定的最大权能集、被调用程序文件的权能状态、原进程的权能状态

9. 系统的完整性 要求主要包括哪些方面？： 传输数据的完整性、处理数据的完整性、存储数据的完整性

10. 传输过程中对数据的完整性进行保护有多种要求，其中要求由接收者 TCB 自己，无需来自源可信 IT 产品的任何帮助，即能恢复被破坏的数据为原始用户数据，这属于那种要求？： 目的数据交换恢复

隐蔽通道分析与标识

1. 隐蔽通道 主要会导致什么后果？ : 数据被泄露

2. 关于隐蔽通道的描述，下面不正确的是哪个？ ：在实施了强制访问控制的多级安全操作系统中，隐蔽通道是指利用系统设计的通信机制来传递信息的信道，如进程间通信机制：共享内存、消息队列、信号量等。

3. 根据收发双方利用的共享资源不同，隐蔽通道通常分为哪两种类型？ 隐蔽定时通道 /隐蔽存储通道

4. TCSEC 从哪个级别开始要求对系统的隐蔽通道进行分析， CC 标准又是从哪个级别开始要求的？ ：TCSEC B2, CC EAL 5

5. 判别隐蔽存储通道的公认标准是 Kemmerer 标准，其中必须满足如下哪些条件？ ：1 接收方进程能察觉该共享资源的状态变化。 2 发送方和接收方进程能访问共享资源的同一属性。 3 发送方进程能改变该共享资源的状态。 4 发送方与接收方进程之间有同步机制。

6. 80 年代 以后出现了系统的 隐蔽通道分析方法 ，它们主要包括？ ：Kemmerer 等人提出的共享资源矩阵法 /Goguen 等人提出的无干扰法 /Tsai 等人提出的带有语义分析的信息流法

7. 隐蔽通道分析可以在从抽象的安全模型到系统机器代码的任何一个层次上进行，共享资源矩阵法主要适用于在哪个层次进行隐蔽通道分析？ ：描述性顶层规范级

8. Tsai 等人提出的带有语义分析的信息流法，可以从源代码级标识隐蔽通道。试问，从源代码级标识隐蔽通道具有的明显优点有哪些？ ：能评估访问控制检查点是否设置得合适 /能找出所有隐蔽存储通道（除了硬件导致的通道以外） /能找出放置审计代码、延迟和噪音的位置

9. 隐蔽通道标识后需要通过带宽计算来度量每个隐蔽通道的危害程度。下面哪些属于影响隐蔽通道带宽计算的主要因素？ ：噪音因素，即干扰进程对通信变量进行操作 /延时因素，即干扰进程分享 CPU 时间导致通信速度下降 /编码因素，即好的编码方案可以提高信道带宽 /原语因素，即是否使用了速度最快的系统调用来实现通信

10. 隐蔽通道的常用处理方法主要有消除、限制带宽和审计三种，根据你对本课程提及的基于进程标识符 pid 的隐蔽通道原理的理解，你认为这种通道应采取哪些方法进行处理？ ：审计、加入噪音

安全模型

1. 开发一个形式化 安全模型 需要满足那些基本要求？： 一致性、完备性、简明性、正确性

2. 操作系统内核变量非常多，如果采用状态机模型来建立其安全模型，容易导致状态爆炸，所以状态机模型不适合用来建立操作系统的安全模型，你认为这种描述正确吗？ :NO

3. 下面哪些安全模型可以用于 保证系统的完整性 ？:DTE/RBAC/BIBA

4. BLP 安全模型 中考虑了主体对客体的多种访问模式，他们主要包括哪几种？ :E 执行模式、 R 读模式、 W 写模式、 A 追加模式

5. BLP 安全模型 中考虑了主体对客体的多种访问模式，他们主要包括哪几种？： 1 仅能处理单级客体，缺乏处理多级客体 BLP 模型注重保密性控制，而缺少完整性控制，不能控制 “向上写 ”，不能有效限制隐蔽通道 2BLP 模型注重保密性控制，而缺少完整性控制，不能控制 “向上写 ”，不能有效限制隐蔽通道 3 不支持系统运行时动态调节安全级的机制 4 可信主体不受 *特性约束，访问权限太大，不符合最小特权原则

6. 如果说一个客体的完整性被破坏，通常是指在信息的传输路径中存在对该客体的不可靠信息流，这个不可靠的信息流可能的来源是什么？： 来自低完整性客体、来自低完整性主体

7. BIBA 模型包 含了低水印策略、环策略和严格策略，它们的安全性如何？： BIBA 环策略的安全性最低， BIBA 低水印策略的安全性最高

8. 在 Sandhu 的 RBAC96 模型中， RBAC2 模型主要增加了那些约束关系？： 角色的成员数限制、角色之间的静态互斥关系。、角色之间的动态互斥关系。

9. 根据中国墙模型，假定公司 A、公司 B 属于同一个利益冲突类 P；公司 X、公司 Y 属于另外一个利益冲突类 Q，如果某个用户 u 曾经读取了公司 A 的数据之后，试问： 用户 u 能否继续读取公司 B 的数据？它可以继续读取公司 X 的数据吗？： 不可以读取 B 的数据，可以读取 X 的数据

10. 在 DTE 安全策略中，需要根据安全目标制定域定义表 (Domain Definition Table) 和域交互表 (Domain Interaction Table) ，其中用于描述主体动态域转换的是哪个： 域交互表

安全体系结构

1. 安全体系结构 描述的是一个系统如何组织成一个整体以满足既定的什么要求： 安全性要求

2. 某种类型的安全体系结构是为理解或者其它目的而提出的，它是满足某个假设的需求集合的一个设计，显示了把一个通用体系应用于具体环境时的基本情况。这种安全体系结构属于哪种类型的安全体系结构？： 逻辑体系

3. 下面哪些属于安全体系结构设计的 基本原则 ？： 1 应尽量考虑未来的安全需求 2 安全相关功能必须结构化 3 实施安全控制的极小化和隔离 4 从系统设计之初就考虑安全性

4. GFAC 广义访问控制框架 的主要优点是将访问控制机制的哪两个部分进行了分离？： 访问控制实施部分、访问控制决策部分

5. Spencer 等人提出的 FLASK 体系结构认为对策略灵活性的支持应该包括哪些内容？： 1 可实现细粒度的访问控制 2 支持多种安全策略 3 能够撤回先前已授予的访问权限 4 能够确保访问权限的授予与安全策略保持一致

6. FLASK 体系结构为解决多种需求之间的冲突，提供了两个策略独立的数据类型来标识客体，这两个数据类型是什么？： 可变长字符串类型的安全上下文、具有固定长数值类型的安全标识

7. FLASK 体系结构中的客体管理器（ OM）主要需要为客户端提供访问哪些决策接口？： 多实例化决策接口、访问决策接口、标记决策接口

8. FLASK 体系结构中的安全服务器（ SS）主要需要提供哪些功能？ 1 为新创建的客体提供 SIDs（Security Identifier ）2 保持 SIDs 和安全上下文之间的映射 3 安全策略决策

9. LSM 以内核补丁的形式实现，下面哪些方面是 LSM 对内核的修改？ 1 新增安全系统调用 2 新增钩子函数的调用 3 在关键内核数据结构中新增安全字段 4 新增安全模块管理

10. 按照功能来分的话， LSM 的钩子函数可以分为以下哪几类？ 1 内核对象改变后，用来改变相应安全字段的钩子函数 2 进行访问权限检查的钩子函数 3 在创建或者释放新的内核对象时同时创建或者释放安全字段的钩子函数

可信计算技术

1. TCPA/TCG 可信工作组定义了可信计算的属性，它们包括下面哪几个属性？： 私密性：用户相信系统能够保证信息的私密性、完整性：用户确保信息能被正确传输、身份认证：计算机系统的用户可以确定与他们通信的对象身份

2. TCG 可信计算工作组的使命就是要发展并推动开放的、厂商中立的、多种平台间的可信计算构造单元及软件接口的业界标准规范。为此 TCG 技术委员会下设了许多工作组，其中最为基础和核心的一个工作组是指的哪个工作组： TPM 可信平台模块工作组

3. 可信平台模块 TPM 的主要设计原则，除了需要考虑安全性、私密性原则之外，还需要包括哪些设计原则： 易用性原则、可控性原则、可互操作性原则、数据可移植性原则

4. 可信平台模块 TPM 至少提供如下哪些功能： 完整性度量、加密、签名认证、安全存储

5. PCR （Platform Configuration Register ）平台配置寄存器主要用户保存平台当前状态的完整性度量值。一个典型 TPM 通常包含 24 个 PCR 寄存器，默认情况下，不同编号的 PCR 用于保存平台不同运行状态的完整性度量值。试问，系统启动时状态默认保存在哪里？： PCR 0 ~ PCR7

6. 可信计算平台模块管理的公私钥对有很多种，其中哪个公私钥是 TPM 的唯一标识，它永久性保存在 TPM 内部，并且禁止在外部使用？： EK, Endorsement Key

7. 与可信平台模块相关的信任状主要包括哪些？： 1 平台信任状，颁发者证明具有某特性的平台是它们生产的 2 认可/背书信任状，颁发者证明对应 EK 的一个 TPM 是它们生产的 3 一致性信任状，颁发者证明具有特定 TPM 的某可信平台符合 TCG 的相关标准/规范 4 证实标识信任状，颁发者证明带有对应 AIK 的平台经证明已确认是一个可信平台

8. 可信平台模块提供的可信根有三种，他们指的哪三种？： 可信存储根（ RTS），提供密码机制保护存储在 TPM 之外的信息（数据和密钥）、可信报告根（ RTR），提供密码机制对 TPM 状态及信息进行签名、可信度量根（ RTM），由平台提供的可对平台状态进行度量的机制

9. 可信平台模块 TPM1.1 的身份认证采取的是 Privacy CA 认证方案，其基础理论依据是什么？ TPM1.2 的身份认证采取的是 DAA 直接匿名认证方案，其基础理论依据又是什么？： 一次一密，群签名和零知识证明

10. 与 TPM1.2 规范相比， TPM2.0 规范的重要改进主要体现在那些方面？： 1 清理了 TPM 设计，使其更简单、更便宜、更强壮和更易用等 2 增加了灵活性，支持更多的应用场景、使 TPM 变得更易用和可管理等 3 提供了支持更多加解密算法的接口 4 增加了一个安全/半安全时钟，与 TPM1.2 中的计数器相比更便宜

安全操作系统的设计与实现技术案例

1. J.H. Saltzer 在 1975 年提出安全系统八大设计原则，试问下面哪些原则不在其中？： 基于“禁止”的安全（最小特权。完全的访问仲裁、机制经济性 ）

2. 安全内核的四种开发方法中，其中哪一种开发方法可以做到：不变的支持现有的应用程序，且兼容非安全操作系统（ ISOS）的现有和将来的版本？： 虚拟机法

3. 安全系统开发过程中进行的脆弱性评定通常需要包括哪些工作？ 1 隐蔽通道存在性分析 2 可信计算基 TCB 的误用或不正确设置的可能性 3 攻破系统的概率或排列机制的可能性 4 可信计算基 TCB 的开发和操作中引入可利用脆弱性的可能性

4. 安全系统开发过程中如果安全性与性能、兼容性发生矛盾，三者权衡顺序应该是？： 安全性、兼容性、性能

5. 安胜安全操作系统达到了中国国家标准 GB17859-1999 的哪个安全等级？ 3、4 级

6. 符合中国 GB17859-1999 的安胜安全操作系统主要建立了哪几个形式化安全模型？ 1 支持 POSIX 权能的最小特权控制形式化安全模型 2 一种改进的可动态调节的机密性安全模型 3 基于 DTE 技术的完整性保护形式安全模型

7. 基于 DTE 技术的完整性保护形式安全模型中引入了那些新的概念/关系？： 可信管道与良构事务的分配关系、域之间的不可控制关系、可信管道与角色的分配关系

8. 支持 POSIX 权能的最小特权控制形式化安全模型中主要提出了管理层、功能控制层和应用层的层次化控制原则，它主要结合了那些策略和机制的设计思想？ POSIX 权能机制、 TE 基于型的强制实施策略、 RBAC 基于角色的访问控制模型

9. Kuhnhauser 指出，一个灵活支持多策略的安全体系结构需要解决的主要问题有哪些？ 策略实施、冲突、协作、重用

10. 回溯搜索法主要适用于系统开发过程中哪个层次的隐蔽通道分析？ 源代码级

基于安全操作系统的应用 - 数据库安全

1. 在如下各安全特性中，早期的多级安全数据库管理系统设计偏重于？： 机密性

2. 不属于多级安全数据库管理系统研究范畴的是？： 数据库水印

3. B2 级以上高等级 DBMS 多采用以下哪些体系结构？ 集中式、复制式

4. 在多级安全数据库中，易导致数据库隐通道出现的原因包括： 事务调度。多级别用户共享内存。多级别用户共享多级数据实体。资源耗尽

5. 下面属于外包数据库安全研究范畴的是： 数据库水印、查询完整性验证、密文检索

6. 在以下各类区间密文检索方案中，效率与可用性最好的是： 保序加密

7. 数据库水印系统应满足的要求包括？ 可探查性、不可察觉性、强健性、盲系统

8. 外包数据库查询完整性验证方法中，目前已有方法包括： 基于 MHT 树的方法、基于脆弱性水印的方法、基于签名链的方法

系统虚拟化安全与虚拟可信平台技术

1. 数据中心的 系统虚拟化技术 主要分为那几种？： 桌面虚拟化、 PC/ 服务器虚拟化

2. 虚拟机监控器 的实现方法主要包括哪几种？ 泛虚拟化、全虚拟化、硬件辅助虚拟化

3. 虚拟化技术给计算平台带来安全性的同时，也带来了与传统计算模式不同的一系列安全问题，这些问题主要有哪些？： 虚拟机迁移带来的问题、虚拟机短暂存在性问题。虚拟机的标识困难问题、虚拟机状态多样性问题

4. 虚拟化计算平台的安全性需要通过多个方面的 安全保障，主要包括哪些方面？ 虚拟机的安全迁移。虚拟机之间的隐蔽通道分析。虚拟机监控器的安全保障。虚拟机状态的安全监控

5. Xen 安全框架 XSM 设计目标是支持多种使用模型，主要包括哪几种使用模型？ ：用于保护平台核心的安全服务、用于分解 Dom0 （特权域）、用于划分资源、用于保护平台免受第三方软件攻击

6. 基于 XSM 的 ACM 模块 主要实现了哪几种安全策略？ ：修改后的 Chinese Wall 策略 /STE（Simple Type Enforcement ）策略

7. 对 虚拟机迁移 请求进行安全决策过程中主要需要考虑哪些要素？ ：虚拟机目标物理平台的完整性 /虚拟机源物理平台的完整性 /虚拟机自身的完整性

8. XenAccess 是一个安全灵活的虚拟机监控架构，为第三方安全监控软件提供了一整套的安 AP，可以使用户对虚拟机的那些资源操作进行监控？ 磁盘 /内存

9. 目前人们发现了一些虚拟机之间的 隐蔽通道，下面哪些是属于隐蔽存储通道？ ：基于 mfn2pfn 映射表的隐蔽通道

10. 虚拟可信平台技术中，选用生成 EK 证书的解决方案是实现虚拟 TPM 实例信任链扩展的关键，如果要求虚拟 TPM 和硬件 TPM 之间存在强连接，应该采取其中的那一种实施方案？ ：不使用虚拟 EK 证书，而是根据为硬件 TPM 发布的 AIK 为虚拟 TPM 实例发布 AIK 证书。/构建“发给一个虚拟 TPM 实例的 EK 证书”到“发给硬件 TPM 的 AIK 证书”的证书链。