**要求：**

**（一）每个组从以下四大项中各选择1个小题完成，每组的选题不能重复（每个选题对应相应目录中相同编号的必读和参考文献，如选题二中的4，请参考目录文件“二安全模型”中的标号为04的对应文献即可）。**

**（二）提交课程报告，其中要包括必读文献的核心内容、平台部署或源代码和实现技术分析，如果有实现技术的，请同时提供录制的实验视频或者实验截图。**

**（三）提交的截止日期为2019年1月18日。**

一、目标：熟悉DTE安全策略及其在UNIX、Linux系统中具体实现机制。通过论文阅读仔细分析DTE安全策略的设计与实现技术。可选题目包括：

1. 将DTE安全模型实施于Linux系统的论文研读与示例源码分析
2. 将DTE安全策略实施于UNIX系统的论文研读与示例源码分析

二、目标：熟悉Chinese Wall、RBAC和ABAC等主流安全模型设计目标、核心思想及其在云计算的应用情况。通过论文阅读或实践进行分析。可选题目包括：

1. Chinese Wall安全模型及其在云环境的应用论文研读与应用分析
2. RBAC基于角色的访问控制模型及角色挖掘工程论文研读与方法分析
3. ABAC基于属性的访问控制模型及ABAC策略挖掘论文研读与方法分析
4. OpenStack系统体系结构分析及其ABAC基于属性访问控制模型的实现技术

三、目标：熟悉SELinux开源项目实施支持Flask的安全框架LSM、以及相关安全模型实现机制。通过实际环境部署和案例分析它们的实现技术。可选题目包括：

1. 将SELinux实施为一个支持Flask体系结构的论文研读与示例源码分析
2. 将SELinux实施为一个LSM安全框架的论文研读与示例源码分析
3. 将MLS多级安全模型实施于SELinux系统的论文研读与示例源码分析
4. 将RABC与TE安全策略实施于SELinux系统的论文研读与示例源码分析

四、目标：熟悉Xen虚拟化平台部署，以及现有基于XSM的相关安全策略和实现机制，并了解虚拟机之间的隐蔽通道脆弱性。通过实际环境部署和案例验证它们的工作原理及其有效性。可选题目包括：

1. Xen安全框架XSM的主要安全目标、对Xen的主要修改和安全性分析
2. Xen ACM中STE策略及其实现机制分析与实际测试案例
3. Xen ACM中CHINESE WALL策略及其实现机制分析与实际测试案例
4. XenCC隐蔽通道原理分析与场景实现
5. Xen 的CPU额度调度器原理分析及其窃取CPU时间攻击方案实现