**第四次作业**

**作业要求：**

1. **按小组完成，提交作业文档和PPT。**
2. **每组选择三个任务之一完成，选题不冲突。**
3. **对于每个选题，被选中的小组要求课堂上陈述（请每个小组提前安排好陈述同学），而且每个组准备和现场提问（针对其他每个陈述小组进行提问至少2个问题，否则将影响评分等级）。**
4. **提交文档和PPT时间为12月04日24时，提交给张鑫汇总后发给老师。**

**任务一：权能（Capability）机制源码分析**

**1．在了解权能机制实现方法的基础之上，对Linux 4.X某个版本系统中相关的实现源码进行分析，主要：**

**1）内核中进程相关数据结构中对应权能表示是如何设计的？**

**2）内核中可执行文件相关数据结构中对应权能表示是如何设计的？**

**3) 内核中exec/execve系统调用相关内核函数中是如何实现权能计算的？**

**4）内核中实施了权能权限检查的内核函数或者设计的系统调用有哪些？并通过举例说明权能机制的实际应用示例。**

**任务二：隐蔽通道原理分析和代码实现**

**2．在了解隐蔽通道概念、分类和标识技术的基础之上，安装安胜安全OS，并完成以下任务，主要：**

**1）安装安胜安全OS，并验证其MAC强制访问控制机制的有效性。**

**2）对提供的5种隐蔽通道场景（参见附件），选择至少3种完成发送和接收程序的编写，提交发送方和接收方源程序代码（必须明确注释，并说明选择的同步机制）。**

**3）演示存在的隐蔽通道，并实际测评其带宽（在同学们的实验环境中测试）。**

**任务二：DTE策略表示及在Linux中的实现**

**3．在了解DTE安全策略设计思想的基础之上，主要阅读以下文献：**

**Domain and Type Enforcement for Linux(DTE for Linux)，并完成以下任务，主要：**

**1）分析DTE策略语言的表示技术。**

**2）分析DTE在Linux中实现的核心技术（文中实现，也可以参考分析目前Linux中的TE策略实现技术）。**

**3）分析DTE实现的可行性验证实验和结果分析情况，以及应用案例。**