|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 班级：信息安全 3班 | 学号：201978030321 | | 姓名：袁航 | | 第 5 周： |
| 实验环境类型： | | Linux版本： | | 内核版本： | |
| **1、实验任务：**  可信计算课程本实验使用TPM模拟器搭建的实验环境进行实验，模拟器为IBM推出的TPM2.0模拟器。软件栈采用Intel推出的TSS相关组件，同时可能还要安装Openssl相关库。参照资料或根据自己电脑系统的需求，下载相应版本的软件，在安装好的虚拟机上搭建可信计算模拟环境，为后续实验打好基础。  参考资料：[TPM模拟器和TPM2-TSS安装\_jianming21的博客-CSDN博客\_tpm2-tss](https://blog.csdn.net/jianming21/article/details/107942585?utm_medium=distribute.pc_aggpage_search_result.none-task-blog-2~aggregatepage~first_rank_ecpm_v1~rank_v31_ecpm-1-107942585.pc_agg_new_rank&utm_term=tpm%E6%A8%A1%E6%8B%9F%E5%99%A8&spm=1000.2123.3001.4430)  **2、实验流程：**  （要求：利用文字和截图描述自己的实验过程）  **3、实验总结（很重要）：**  （要求：对本次实验进行总结，发现不足，寻找后续改进的办法） | | | | | |