电子科技大学信息与软件工程学院

**实 验 报 告**

学 号 2017221303023

姓 名 陈奎

（实验） 课程名称 网络安全协议

理论教师 罗绪成

实验教师 罗绪成

合作队友 郑烁（2017221304002）

**电子科技大学教务处制表**

**电 子 科 技 大 学**

**实 验 报 告**

**学生姓名：陈奎/郑烁 学号：2017221303023／2017221304002 指导教师：罗绪成 实验地点：信软楼 实验时间：19.10.22**

**一、实验名称：**TLS 配置与流量分析实验

**二、实验学时：**2学时

**三、实验目的：**

1）理解 TLS 协议原理；

2）掌握 apache 服务器的 HTTPS 配置方法；

3）掌握 TLS 流量分析方法。

**四、实验原理：**

**五、实验内容**

1）配置 TLS 协议分析环境；

2）配置 apache 的 HTTPS 协议；

3）对指定域名发起 HTTPS 请求，抓包分析 TLS 协议流程、提取其中的关键信息。

**六、实验器材（设备、元器件）：**

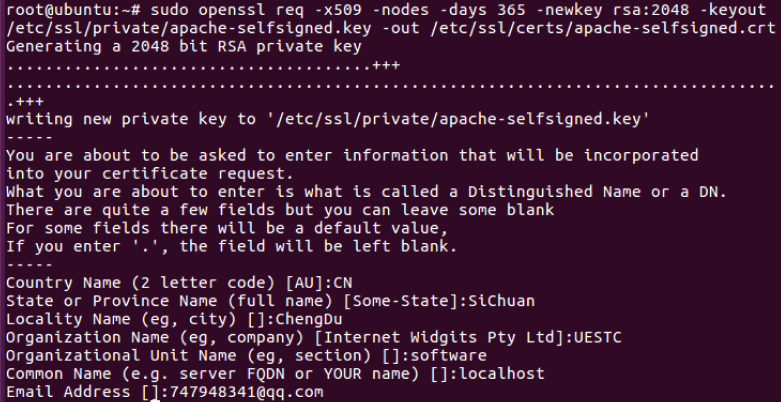
台式机一台，能够安装一台 ubuntu 虚拟机，能够访问互联网。

**七、实验步骤：**

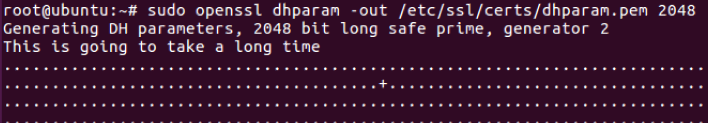
**步骤一、环境搭建**

**步骤二、Linux 服务器上配置 apache 服务器的 HTTPS**

1. **创建证书、密钥等文件**

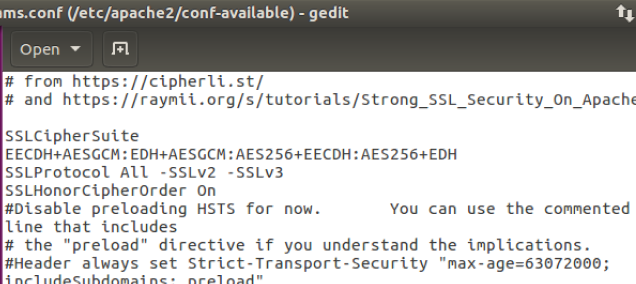


创建一个强的 DH 群



**2、 配置 Apache 服务器**

创建 Apache 配置文件,并进行强加密设置

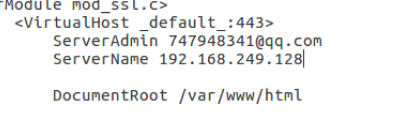


修改默认的 Apache SSL 虚拟主机文件

修改之前，先做一下备份



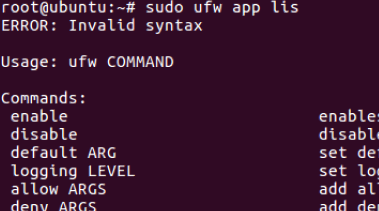
打开/etc/apache2/sites-available/default-ssl.conf 文件进行编辑



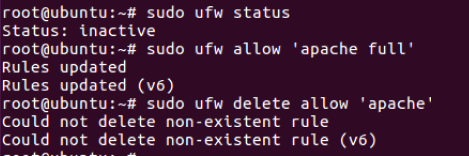
修改未加密的 Virtual Host file 来自动重定向请求到加密的 Virtual host



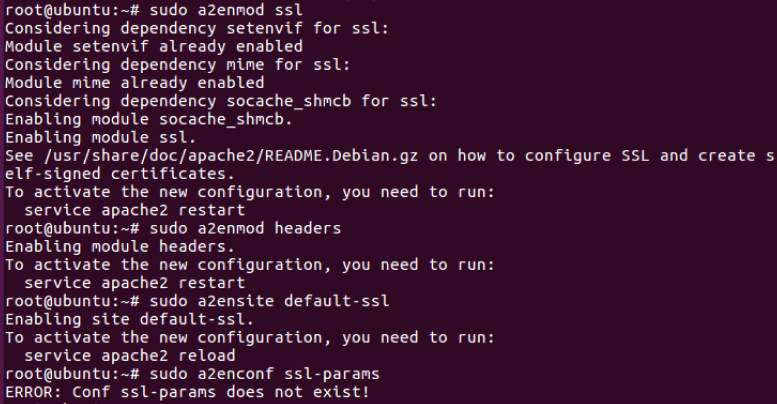
**3、 设置防火墙**

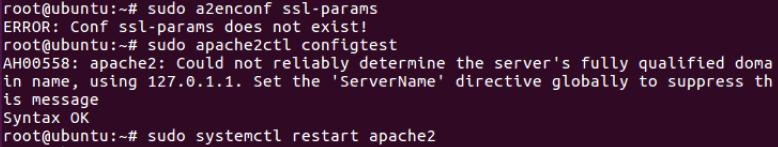


查看当前的设置



**4、 使设置生效：**

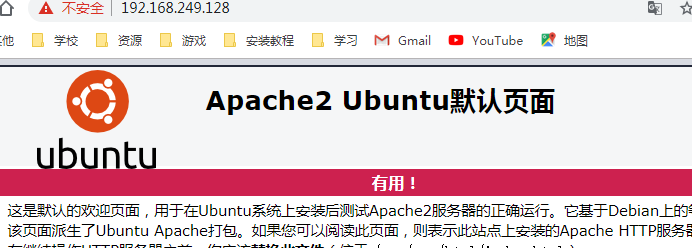




测试配置结果，从浏览器访问服务器

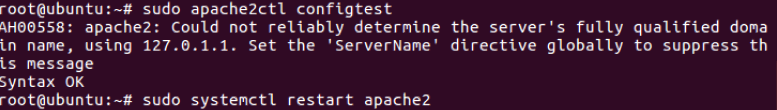


进一步测试 http 重定向 https 设置



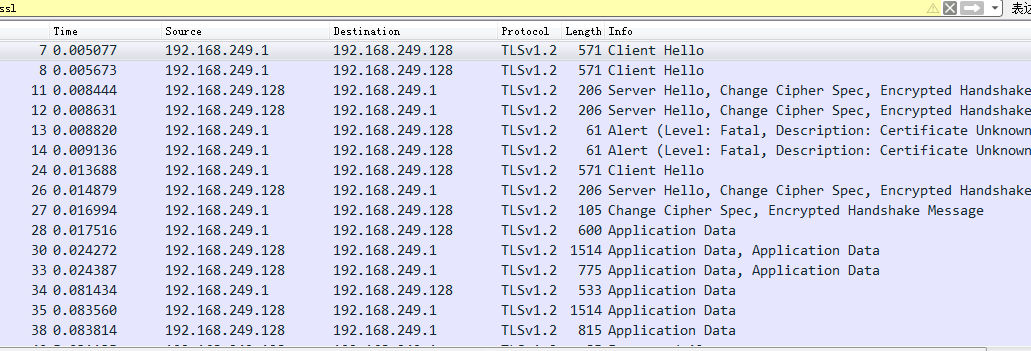
确定只允许加密流量，则可以设置永久重定向





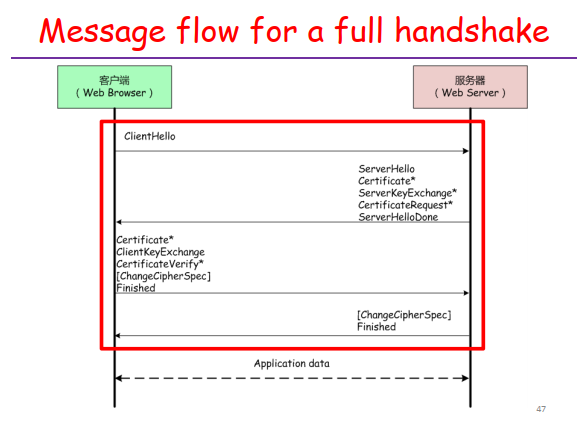
**步骤三、TLS 流量分析**

使用wireshark抓包结果

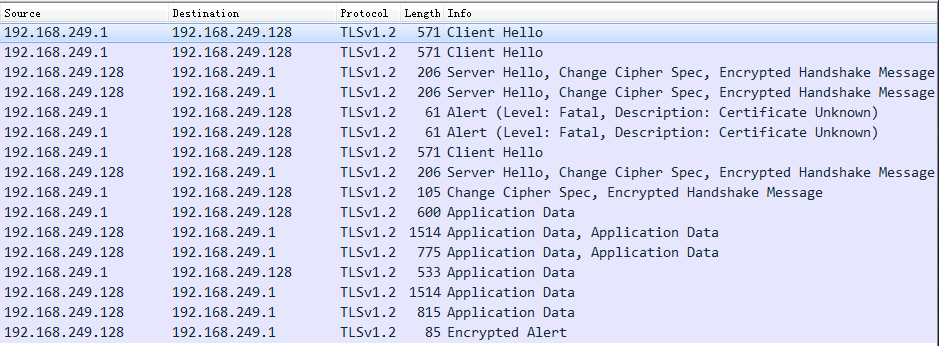


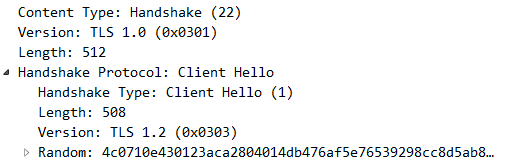
**八、实验结果与分析（含重要数据结果分析或核心代码流程分析）**

TLS handshake过程

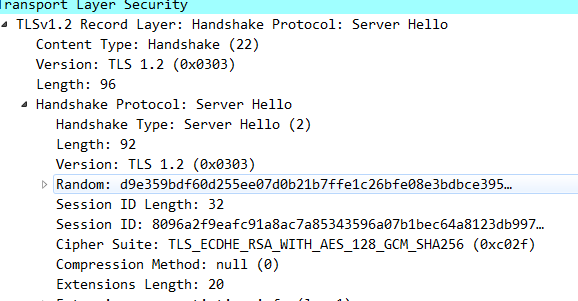


抓包结果分析

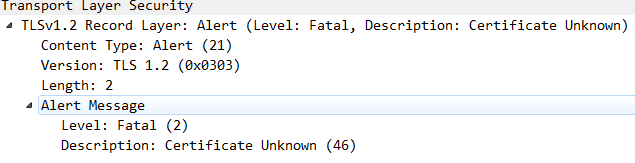




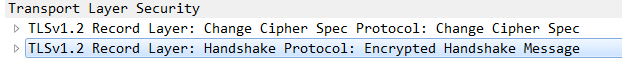
可以看到连接时客户端首先进行Client Hello，从中可以找到客户端支持的协议版本，比如TLS1.2还有客户端的随机数Random，以及支持的加密算法



客户端握手完成后是Sever Hello。进行确认使用的协议版本；服务器生成的随机数2，稍后用于生成"对话密钥"；确认使用的加密算法；并向客户端提供自己的证书；同时请求客服端的证书。



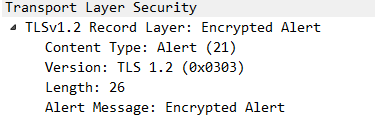
第三步本来应该是Certificate，但是因为证书不知，发生fatal Alert，所以需要断开连接重新进行。重新连接后进行Certificate。包括Change Cipher Spec以及Client Key Exchange



完成后连接成功，开始进行正常的数据传输，可以看到协议是https



当一方没有数据要传输时，会发送一个close\_notify报警消息给对方



**九、总结及心得体会：**

通过本次实验，了解了Apache的基本配置。加深了对Linux操作系统的了解。通过对数据包进行TLS流量分析，加深了对TLS协议的认知。TLS协议可以分为两层，一共有5个子协议，分别是上层的Handshake Protocol、ChangeCipherSpec Protocol、Alert Protocol、Application Data Protocol和下层的Record Protocol。在查看数据包以及进行分析的过程中，能够将理论与实际相结合，感受到了课本知识的实际应用。

**十、对本实验过程及方法、手段的改进建议：**

无。

**报告评分：**

**指导教师签字：**