# 电子科技大学信息与软件工程学院

**标 准 实 验 报 告**

**（实验）课程名称网络安全攻防技术实验**

**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：XXXXX 学 号：XXXX 指导教师：XXXXX**

**实验地点：xxxx 实验时间：XX.XX.XX**

**一、实验室名称：** 网络安全专业课程实验室

**二、实验项目名称：**TLS配置与流量分析实验

**三、实验学时： 4**

**四、实验原理：**

………………

**五、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。

**六、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。

**七、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。

**八、实验步骤：**

**步骤一、环境搭建**

Windows下安装wireshark和虚拟机，确保宿主机和虚拟机能够网络联通，并测试是否能够抓包。

**步骤二、 配置apache服务器的HTTPS**

1. **创建证书、密钥等文件**

命令：

sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/apache-selfsigned.key -out /etc/ssl/certs/apache-selfsigned.crt

openssl: 创建和管理OpenSSL证书、密钥等的基本工具。

req：子命令，用于说明要使用X.509证书签名请求（CSR）管理。

-X509：进一步说明要创建一个自签证书。

-nodes：用于说明跳过对证书的口令保护，这样就避免每次读取证书文件时需要输入口令。

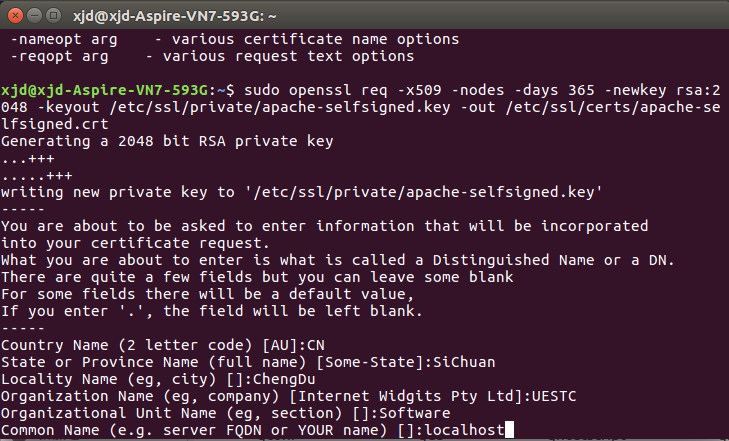
-days 365：设置证书有效期为365天。

-newkey rsa:2048：用于说明要同时生成一个新的证书和新的密钥。rsa:2048用于说明生成的RSA key是2048比特。

-keyout：说明私钥文件的存放位置

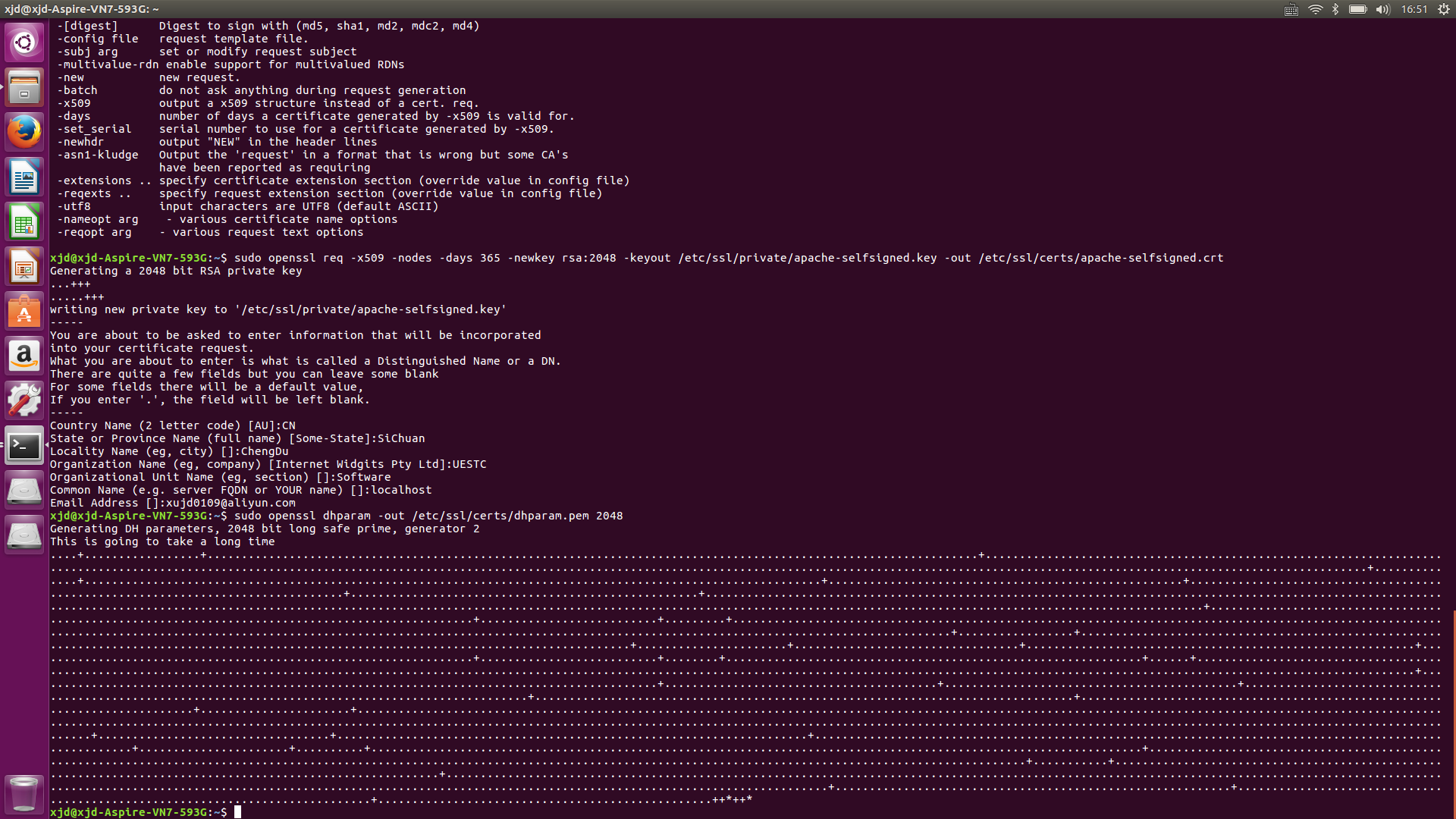
-out：说明证书文件的存放位置

在创建证书的过程中，程序会需要提供一些信息，这些信息会嵌入到证书中。最重要的信息是Common Name，你需要以服务器的域名或者IP地址来回答。下面是截图示例：



为了协商前向安全秘密（Perfect Forward Secrecy），还需要创建一个强的DH群。命令为：

sudo openssl dhparam -out /etc/ssl/certs/dhparam.pem 2048



1. **配置Apache服务器**

前面已经准备好密钥和证书文件，下面我们将利用这些文件来配置apache服务器。包括:

1. 创建Apache配置文件,并进行强加密设置

如果没有安装apache2服务器，通过下述命令进行安装：

sudo apt install apache2

在/etc/apache2/conf-available目录下创建一个新文件，命名为：ssl-params.conf。文件内容为：

|  |
| --- |
| # from https://cipherli.st/  # and https://raymii.org/s/tutorials/Strong\_SSL\_Security\_On\_Apache2.html  SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH  SSLProtocol All -SSLv2 -SSLv3  SSLHonorCipherOrder On  # Disable preloading HSTS for now. You can use the commented out header line that includes  # the "preload" directive if you understand the implications.  #Header always set Strict-Transport-Security "max-age=63072000; includeSubdomains; preload"  Header always set Strict-Transport-Security "max-age=63072000; includeSubdomains"  Header always set X-Frame-Options DENY  Header always set X-Content-Type-Options nosniff  # Requires Apache >= 2.4  SSLCompression off  SSLSessionTickets Off  SSLUseStapling on  SSLStaplingCache "shmcb:logs/stapling-cache(150000)"  SSLOpenSSLConfCmd DHParameters "/etc/ssl/certs/dhparam.pem" |

需要注意的地方是，把上述文件的最后一行的参数设置为前面生成的DH文件。

（详细的信息可参看：https://cipherli.st/）

1. 修改默认的Apache SSL虚拟主机文件

默认的Apache SSL虚拟主机文件为：

/etc/apache2/sites-available/default-ssl.conf

修改之前，先做一下备份。命令为：

sudo cp /etc/apache2/sites-available/default-ssl.conf /etc/apache2/sites-available/default-ssl.conf.bak

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

原文件的内容大致如下：

|  |
| --- |
| <IfModule mod\_ssl.c>  <VirtualHost \_default\_:443>  ServerAdmin webmaster@localhost  DocumentRoot /var/www/html  ErrorLog ${APACHE\_LOG\_DIR}/error.log  CustomLog ${APACHE\_LOG\_DIR}/access.log combined  SSLEngine on  SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem  SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key  <FilesMatch "\.(cgi|shtml|phtml|php)$">  SSLOptions +StdEnvVars  </FilesMatch>  <Directory /usr/lib/cgi-bin>  SSLOptions +StdEnvVars  </Directory>  # BrowserMatch "MSIE [2-6]" \  # nokeepalive ssl-unclean-shutdown \  # downgrade-1.0 force-response-1.0  </VirtualHost>  </IfModule> |

修改后的版本如下：

|  |
| --- |
| <IfModule mod\_ssl.c>  <VirtualHost \_default\_:443>  ServerAdmin your\_email@example.com  ServerName server\_domain\_or\_IP  DocumentRoot /var/www/html  ErrorLog ${APACHE\_LOG\_DIR}/error.log  CustomLog ${APACHE\_LOG\_DIR}/access.log combined  SSLEngine on  SSLCertificateFile /etc/ssl/certs/apache-selfsigned.crt  SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key  <FilesMatch "\.(cgi|shtml|phtml|php)$">  SSLOptions +StdEnvVars  </FilesMatch>  <Directory /usr/lib/cgi-bin>  SSLOptions +StdEnvVars  </Directory>  BrowserMatch "MSIE [2-6]" \  nokeepalive ssl-unclean-shutdown \  downgrade-1.0 force-response-1.0  </VirtualHost>  </IfModule> |

注意对上面红色字体部分是修改后的内容。

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

为了更好的安全性，通常也推荐设置为自动重定向http访问到https访问，通过修改配置文件/etc/apache2/sites-available/000-default.conf来完成。

打开文件进行编辑，仅需要加入一个Redirect指令来指向SSL版本的站点，示例如下：

|  |
| --- |
| <VirtualHost \*:80>  . . .  Redirect "/" "https://your\_domain\_or\_IP/"  . . .  </VirtualHost> |

注意上面的红色字体。

1. **设置防火墙**

如果系统设置ufw防火墙，则需要进行配置，以使得SSL流量能够进入。在安装的时候，apache会在ufw注册一些profile，以方便设置。命令查看：

sudo ufw app list

示例结果：

|  |
| --- |
| Available applications:  Apache  Apache Full  Apache Secure  OpenSSH |

查看当前的设置。命令：

sudo ufw status

输出示例：

|  |
| --- |
| Status: active  To Action From  -- ------ ----  OpenSSH ALLOW Anywhere  Apache ALLOW Anywhere  OpenSSH (v6) ALLOW Anywhere (v6)  Apache (v6) ALLOW Anywhere (v6) |

为了放行SSL流量，执行如下命令：

sudo ufw allow 'apache full'

然后，在删除一条冗余的profile：

sudo ufw delete allow 'apache'

1. **使设置生效**

需要使模块mod\_ssl、mod\_headers（配置文件中某些设置需要）生效。命令为：

sudo a2enmod ssl

sudo a2enmod headers

接下来使得SSL虚拟主机生效，使用命令：

sudo a2ensite default-ssl

ssl-params.conf生效，命令为：

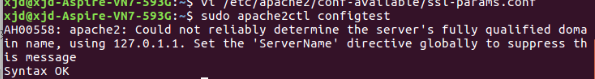
sudo a2enconf ssl-params

到这一步，服务器已经加载了必要的模块。为了进一步检查配置文件里面是否有语法错误，输入命令：

sudo apache2ctl configtest

如果都没有问题，示例输出为：

|  |
| --- |
| AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message  Syntax OK |



下一步，重启服务器：

sudo systemctl restart apache2

测试配置结果，从浏览器访问服务器：

https://ip

因为是自签证书，因此浏览器会弹出警告。

进一步测试http重定向https设置。

http://ip

如果测试通过，你确定只允许加密流量，则可以设置永久重定向。编辑文件：

/etc/apache2/sites-available/000-default.conf

结果如下：

|  |
| --- |
| <VirtualHost \*:80>  . . .  Redirect permanent "/" "https://your\_domain\_or\_IP/"  . . .  </VirtualHost> |

进一步需要测试配置语法是否正确：

sudo apache2ctl configtest

重启服务器：

sudo systemctl restart apache2

**步骤三、TLS流量分析**

启动wireshark，设置显示过滤器。因为只对TLS协议数据进行分析，所以这里仅显示TLS协议数据即可。设置显示过滤器为：ssl。开启抓包模式。如果浏览器启动后就会访问一些未指明的域名，可以等这一阶段过后，重新开启抓包模式。

启动firefox浏览器（或者IE浏览器、Chrome浏览器），访问前面配置好的apache服务器或者域名www.baidu.com（缺省就为HTTPS）或者www.amazon.com等。为了防止wireshark占用太多资源，这个时候可以停止抓包功能。

根据TLS协议的原理，按照消息交换的顺序对每条消息的关键信息进行截图，并说明协议的流程和每个消息的关键字段的信息。

**九、实验数据及结果分析：**

**十、实验结论：**

…………

**十一、总结及心得体会：**

**十二、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：**