Openssl 生成证书实验

1、 实验环境：

ubuntu12.04+apache2+openssl

参考文档：

https://help.ubuntu.com/community/OpenSSL

http://bbs.pediy.com/showthread.php?t=156925

2、 步骤：

为什么使用 **openssl**？因为 **openssl** 是广泛使用的商业级 **ssl** 服务，在本实验中，我们在 **apache** 上使用 **openssl** 用来提供 **https** 服务

生成 **x.509** 证书，广泛用于 **openssl** 中

确认在本机下的 **openssl** 版本：

openssl version

生成 **x.509** 证书之后，有三种方式签名分别为自签名，生成 **CA**，以及由公认的 **CA** 机构签名。我们这里使用的是自签名的证书，它的好处是使用方便，按需生成，但是在连接使用自签名的 **http** 服务器总会报警。所以我们的实验步骤是生成 **x.509** 证书->生成服务器证书->自签名->根证书导入浏览器->测试。

（一） 生成 **x.509** 证书

1、创建初始工作环境，在/home/username 下创建：

cd && mkdir -p myCA/signedcerts && mkdir myCA/private && cd myCA

其中/myCA 用于存放 CA 证书，证书数据库，生成的证书，密钥以及请求。~/myCA/signedcerts 用于保存签名证书的 copy，~/myCA/private 包含私钥。

2、在 myCA 中创建证书库

echo '01'>serial && touch index.txt

注：serial 文件作为证书的序号，然后 index 文件作为证书库，此时 serial 文件的序号为 01

3、创建 ca 配置文件 caconfig.cnf

配置文件内容如下：

[local_ca]

dir = /home/<username>/myCA//以下所有文件的根目录

certificate = $dir/cacert.pem//ca 根证书存放路径

database = $dir/index.txt//前面建立的证书数据库

new_certs_dir = $dir/signedcerts//ca 证书的拷贝

private_key = $dir/private/cakey.pem//ca 证书的私钥

serial = $dir/serial//证书序列号

4、将 caconfig.cnf 添加到环境变量中

该命令为 export OPENSSL_CONF=~/myCA/caconfig.cnf，然后生成 CA 证书和密钥,命令为:

openssl req -x509 -newkey rsa:2048 -out cacert.pem -outform PEM -days 1825

注意此条命令会让用户输入密钥，这个密钥会在后面签名服务器证书的时候使用,不要忘了

之后会在 myCA 目录下生成 cacert.pem：就是我们后面要导入浏览器的证书，也就是 CA 公开证书；以及 cakey.pem 这是 CA 私钥。

（二）创建自签名服务器证书：

1、首先生成服务器的配置文件 exampleserver.cnf

[server_distinguished_name]

commonName = localhost

stateOrProvinceName = NC

countryName = US

emailAddress = root@tradeshowhell.com

organizationName = My Organization Name

organizationalUnitName = Subunit of My Large Organization

注意 commonName 必须和 hostname 匹配，由于这里我们使用的测试主页是 localhost，所以 hostname 设置为 localhost，此外还有一个地方要注意，在 exampleserver 文件末尾：

[alt_names]

DNS.0 = localhost

DNS.1 = localhost

注意 DNS.0 和 DNS.1 要改为 localhost

2、生成环境变量

export OPENSSL_CONF =~/myCA/exampleserver.cnf

生成服务器的证书：

openssl req -newkey rsa:1024 -keyout tempkey.pem -keyform PEM -out tempreq.pem -outform PEM

此时仍然要输入密钥

然后将服务器临时私钥转为非加密文件，此条命令为：

openssl rsa < tempkey.pem > server_key.pem

此时会让你输入在生成服务器证书和密钥时的密码。

（三）对服务器证书签名

export OPENSSL_CONF=~/myCA/caconfig.cn

openssl ca -in tempreq.pem -out server_crt.pem

（四）在 **firefox** 浏览器中导入根证书

（五）修改**/etc/apache2/sites-available** 下的 **default-ssl** 文件即可