Lab2 PKI

环境配置

1. 进入实验目录:

/home/seed/Desktop/Labs\_20.04/Cryptography/Public-Key Infrastructure (PKI) Lab/Labsetup/

1. 创建容器镜像和启动容器

在一个窗口中运行以下命令:



1. Dockps命令查看docker ID，然后docksh命令连接容器。

因为步骤和前面几个实验相同，这里就不展示了。

1. 开启HTTPS服务

开启HTTPS服务首先需要使用openssl签发证书，签发证书需要一个CA，这里我们自己生成CA，然后使用我们自己的CA签发证书。

1. 生成CA的公钥证书和私钥。
2. openssl req -x509 -newkey rsa:4096 -sha256 -days 3650 \
3. -keyout ca.key -out ca.crt \
4. -subj "/CN=www.modelCA.com/O=Model CA LTD./C=US" \
5. -passout pass:dees

当前文件夹下应该有ca.crt和ca.key两个文件。

1. 生成一个CSR。
2. openssl req -newkey rsa:2048 -sha256 \
3. -keyout server.key -out server.csr \
4. -subj "/CN=www.bank32.com/O=Bank32 Inc./C=US" \
5. -passout pass:dees \
6. -addext "subjectAltName = DNS:www.bank32.com, \
7. DNS:www.bank32A.com, \
8. DNS:www.bank32B.com"

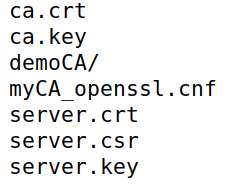
之后会在当前文件夹下生成server.csr和server.key文件。

1. 使用前面的CA签发证书。

首先先把/usr/lib/openssl/openssl.cnf文件复制到当前文件夹，重命名为myCA\_openssl.cnf，然后再改文件中修改两个地方，即去掉copy\_extensions = copy前的注释以及unique\_subject = no前的注释。

然后在当前目录创建myCA\_openssl.cnf中指定的文件夹demoCA，在demoCA文件夹下创建certs和newcerts子文件夹，以及index.txt文件(内容为空)，还有serial文件(文件内容为一个序列号，比如1000)。

所以当前文件夹应该有以下文件:



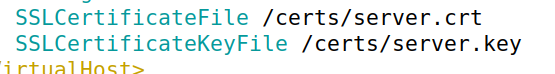
demoCA文件夹下有certs/ newcerts/ index.txt 和 serial。

然后使用如下命令签发证书。

1. openssl ca -config myCA\_openssl.cnf -policy policy\_anything \
2. -md sha256 -days 3650 \
3. -in server.csr -out server.crt -batch \
4. -cert ca.crt -keyfile ca.key

之后文件夹下应该有名为server.crt的证书。

1. 有了证书之后在apache配置文件中设置证书的位置，我们将证书和私钥server.key和server.crt拷贝到/certs文件夹中，然后再修改apache的配置文件/etc/apache2/sites-available/bank32\_apache\_ssl.conf文件，修改cert和key的位置，修改如下:



1. 之后就可以开启网站服务了。

Service apache start 开启网站，这时需要输入密码，之后输入dees即可(证书需要的)。

1. 在到浏览器访问之前，先到VM主机的/etc/hosts文件修改IP地址和域名的对应关系，即添加以下条目:



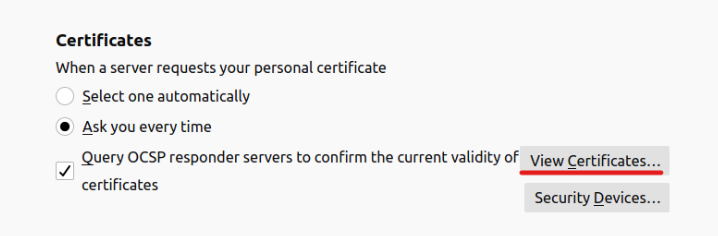
1. 之后到浏览器访问<https://www.bank32.com>，结果并没有出现想要的内容。

问题在于Firefox需要CA的公钥证书取验证网站的证书，但是浏览器并没有CA的公钥证书，所以无法验证。因此需要将CA的公钥证书添加到浏览器中。

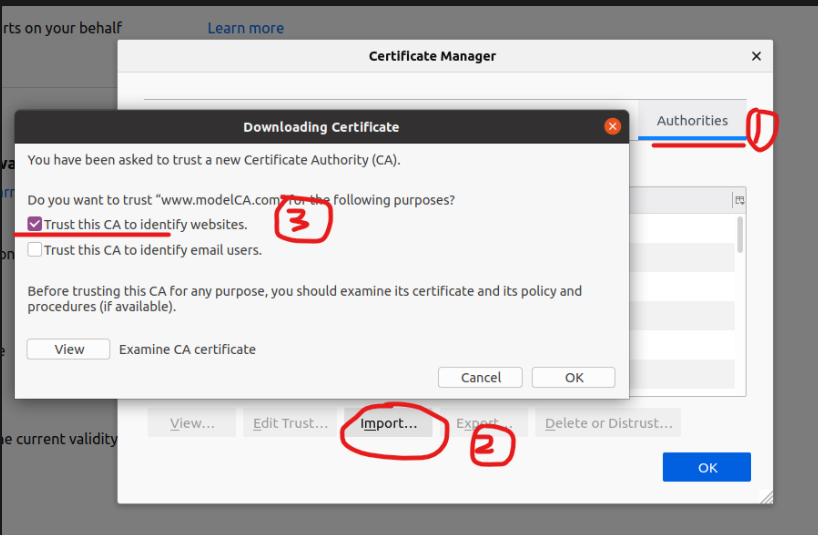
1. Firfox添加CA证书。

添加的是CA证书，也就是ca.crt。

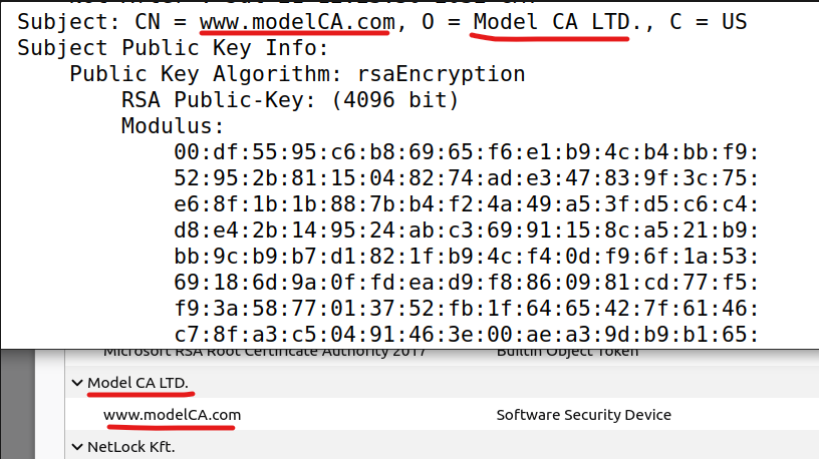
1. 在浏览器地址栏输入以下内容：about:preferences#privacy
2. 进入设置界面后，找到并点击红色区域:



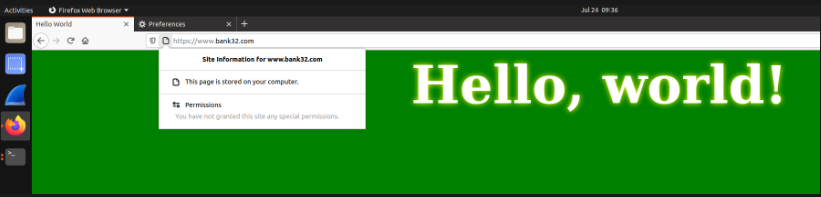
1. 之后添加证书，但是证书ca.crt还在docker 容器中，所以先把证书拷贝到/volumes文件夹中用于同步到VM主机。然后Import同步到VM主机中的volumes共享目录中的证书，进行导入，点击步骤如下图所示：



然后会发现我们导入的证书已经出现在了证书列表中，并且内容和当初生成自签名CA证书时的Subject相同，如下图所示：



1. 之后再次访问浏览器，就没有问题了，结果如下：



MITM攻击

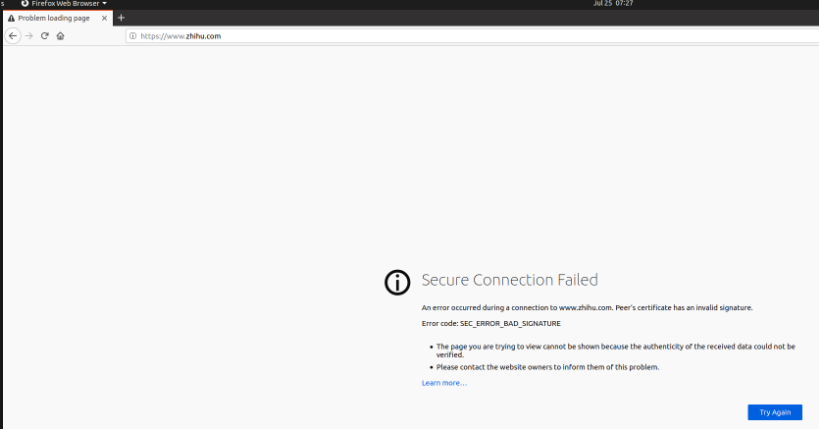
1. 选择一个网站，这里以www.zhihu.com为准，在apache中再次开启一个site，也就是将/etc/apacha2/sites-available/bank32\_apache\_ssl.conf复制一份，命名为zhihu\_apache\_ssl.conf，命令如下:

**cp /etc/apacha2/sites-available/bank32\_apache\_ssl.conf \**

**/etc/apacha2/sites-available/zhihu\_apache\_ssl.conf**

然后把文件中的bank32.com修改为zhihu.com，DocumentRoot就不要修改了。

1. 在浏览器访问https://www.zhihu.com就会出现如下界面:



这个实验中我们使用的证书还是前面生成的证书，但是那个证书的域名是bank32.com，并不是zhihu.com，所以攻击是不可能成功的。

**PKI可以抵御中间人攻击，是因为attacker无法获取CA对相应域名签名的证书，自签名的证书或者访问域名和证书域名不对应都不能完成攻击，因为自签名的证书浏览器没有对应的CA证书，域名无法对应也会异常。**