Configurar PKI

Luis Ángel Cotelo Leyva

1.- Ámbito del problema

Se quiere configurar una infraestructura de clave pública (Public Key Infrastructure) con el objetivo de autenticar a otros en la red.

Una PKI, resumiendo algo, es un conjunto de máquinas, que certifican ante el resto de usuarios de la red que un usuario o servicio es quien dice ser. Esto se hace mediante el uso de claves públicas y privadas.

En el problema que nos atañe, se creará una entidad certificadora raíz (root CA) que sea capaz de certificar a otras entidades certificadoras subordinadas (intermediate CA) para que estas hagan el trabajo de certificar a terceros. Una de las entidades certificadoras subordinadas, certificará a un servidor https con el que más tarde se realizará una conexión para ver si todo ha salido bien.

1.1.- ¿Por qué dos tipos de entidad?

Que haya dos entidades certificadoras, una raíz y otra subordinada supone una capa de seguridad más a la infraestructura, ya que si una de las entidades cae, por el motivo que sea, hay que revocar en cadena todos los certificados que haya firmado esta entidad.

Si se es precavido y se protege a la entidad certificadora más importante, la raíz, apagando y desconectando esta máquina de la red, al producirse un accidente, no habría que volver a montar la infraestructura. Bastaría con revocar los certificados a partir de la entidad comprometida, levantar la CA raíz, volver a certificar alguna entidad intermedia y volver a apagarla.

2.- Configurar CA Raíz

Voy a usar una máquina virtual en Microsoft Azure. No tiene mucha capacidad de cómputo ni especificaciones técnicas, pero tampoco es necesario, ya que en el momento que esta entidad certifique a una subordinada, se apagará y desconectará de la red. También voy a usar OpenSSL para configurar la entidad certificadora.

Una vez montada e iniciada la máquina virtual (Debian 10 en mi caso) hay que configurar el sistema de clave privada/pública.

Lo primero es actualizar los repositorios y actualizar el sistema.

```
cotelo@ca:~$ sudo apt-get update
Hit:1 http://debian-archive.trafficma
Hit:2 http://debian-archive.trafficma
Hit:3 http://debian-archive.trafficma
Hit:4 http://debian-archive.trafficma
Reading package lists... Done
cotelo@ca:~$ sudo apt-get upgrade
```

Una cosa a tener en cuenta tras actualizar el sistema, es que si las entidades raíz y subordinada están en husos horarios distintos, sus horas locales podrían diferir, por lo que podría haber problemas. Para solucionar este inconveniente, simplemente instalo ntp en ambas máquinas.

```
cotelo@ca:~$ sudo apt-get install ntp
```

Ahora hay que crear la estructura de directorios y archivos para la CA raíz. Esta estructura la voy a crear en el directorio / por tanto voy a necesitar cambiar al usuario root por unos instantes.

```
cotelo@ca:/$ sudo -i
root@ca:~# mkdir /root/ca
root@ca:~# cd /root/ca
root@ca:~/ca# mkdir newcerts certs crl private requests
root@ca:~/ca# touch index.txt
root@ca:~/ca# touch index.txt.attr
root@ca:~/ca# echo '1000' > serial
root@ca:~/ca# ls
certs  crl  index.txt  index.txt.attr  newcerts  private  requests  serial
root@ca:~/ca#
```

Los archivos y directorios creados son necesarios para la posterior configuración de OpenSSL.

Ahora hay que llevar unos archivos de configuración al servidor. Estos archivos son los siguientes: https://github.com/cotelus/ConfigurePKI/tree/main/configuracion_raiz

Para ello, puede hacerse con scp, o ayudarnos del repositorio ya que están subidos ahí. Para descargarlos del repositorio, se requiere la visualización de los archivos sin el código html propio de la página.
openssl_csr_san.cnf - openssl_intermediate.cnf - openssl_root.cnf