TP Architectures de Sécurité

Apache – Advanced Configuration

Aurélien Monnet-Paquet

1. Authentication by password

1.1 Création du fichier .htpasswd.

Ce fichier va contenir les utilisateurs et mot de passes associés pour accéder à la ressource protégé. Chaque ligne indique l'utilisateur autorisé ainsi que son mot de passe hashé. J'ai choisi de placer ce fichier dans le dossier à protéger.

Par exemple :
martha:$apr1$VgxJZRTi$f2Amr4Q6BN3wvSGPtPzsw0
Theo:$apr1$uVWqR9T9$54DfwulS3qPmPp3qxGrbX.
Carmina:$apr1$a1HgzHEe$FLmB4TNAzuPOoi/sLOlMD.
mika:$apr1$faxHoTNu$MBENWdYAezfXzyKoo3UUL/

1.2 Configuration d'apache

Maintenant il faut configurer apache pour prendre en compte l'authentification. Pour cela j'ai modifié le fichier de configuration : /etc/apache2/sites-enabled/000-default.conf

```
<VirtualHost *:80>
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    <Directory "/var/www/html">
        AuthType Basic
        AuthName "Restricted Content"
        AuthUserFile /var/www/html/admin/.htpasswd
        Require valid-user
    </Directory>
</VirtualHost>
```

Résultat lorsque l'on tente d'accéder à la section admin :

2. Authentification par certificat

2.1. Création de l'autorité de certification

Génération de la clé RSA de 4096 bits :
openssl genrsa -out ampCA.key 4096

Création du CSR :
openssl req -new -key ampCA.key -out ampCA.csr

Génération du certificat auto-signé :
openssl x509 -req -days 65 -in ampCA.csr
-out ampCA.crt
-signkey ampCA.key

2.2. Création du certificat du serveur web

Génération de la clé RSA de 4096 bits :
openssl genrsa -des3 -out ampWEB.key 4096

Création du CSR :
openssl req -new -key ampWEB.key -out ampWEB.csr

Signature du certificat serveur avec l'autorité de certification :
openssl ca -in ampWEB.csr -cert ampCA.crt -keyfile ampCA.KEY -out ampWEB.crt

2.3. Configuration d'apache

Modification du fichier default-ssl.conf :

SSLEngine on

SSLCertificateFile /etc/apache2/ampWEB.crt
SSLCertificateKeyFile /etc/apache2/ampWEB.key

SSLCACertificateFile /etc/apache2/ampCA.crt

SSLVerifyClient require
SSLVerifyDepth 1

Modification du fichier 000-default.conf :

Redirect permanent "/" "https://192.168.142.61/"
Pour rediriger automatiquement les demandes de connexion provenant du port http:80 vers le port https:443.

2.4. Génération du certificat client

Génération de la clé RSA de 4096 bits :
openssl genrsa -des3 -out ampClient.key 4096

Création du CSR :
openssl req -new -key ampClient.key -out ampClient.csr

Signature du certificat client :
openssl ca -in ampClient.csr -cert ampCA.crt -keyfile ampCA.KEY -out ampClient.crt

Conversion du certificat du format PEM vers PKCS12 :
openssl pkcs12 -export -clcerts -in ampClient.CRT
-inkey ampClient.KEY
-out ampClient.P12