# Travaux pratiques

# UE SR2I204

# A. Serhrouchni – Mounira Msahli

# Authentification : analyse et mis en œuvre.

**Exercice 1** : Analyse du protocole HTTP

Deux modes d’authentification par mot de passe sont supportés par le protocole HTTP (RFC2617). Pour cet exercice il s’agit d’identifier et d’analyser ces différents modes d’authentification. Le site test supporte ces deux modes. En interceptant les échanges au niveau du protocole HTTP identifiez et analysez ces échanges. Pour cela il faut installer le plugin Live HTTP headers sur votre browser.

NB : Le protocole SIP supporte le RFC2617. En annexe vous trouverez une trace au format *pcap* d’une authentification SIP.

**Exercice 2**: Etude du codage Base64 en mode Basic.

Installez un plugin de codage/décodage Base64. Etudiez par l’exemple le codage base64.

Décoder le message suivant : cGFub3JhbWl4DQoNCg==

**Exercice 3**: Identification du mode d’authentification

Identifiez le mode d’authentification avec le site : intranet.infres.enst.fr . Qu’en concluez-vous ?

Identifiez le mode d’authentification avec le site : eole.telecom-paristech.fr . Qu’en concluez-vous ?

# Mécanismes d’authentification en mode Basic :

Dans cet exercice, il est demandé d’implémenter une authentification des clients en mode http Basic. Ces clients « authentifiés » auront le droit d’accéder à un dossier sur l’espace web appelé secret.

Nous commençons par télécharger les fichiers sources (html et php) et les dossiers associés.

[http://137.194.x.x/TP-auth](http://137.194.165.177/TP-auth) (le fichier site.tar.gz)

Décompressez ce fichier et copiez-le dans l’espace Web du serveur apache

**tar zxvf site.tar.gz**

**mv www /var**

Créez le fichier contenant les mots de passes pour l’authentification en mode Basic

**touch** **/etc/apache2****/.htpasswd**

Créer des comptes avec la commande htpasswd /etc/apache2/.htpasswd another\_user

**htpasswd /etc/apache2/.htpasswd *nom\_utilisateur***

Créez le fichier .htaccess qui permet le contrôle d’accès sur le répertoire secret1. Les fichiers .htaccess fournissent une méthode pour modifier la configuration du serveur au niveau de chaque répertoire.

**touch** **/var/www/html/secret1/.htaccess**

Activez le contrôle d’accès en mode Basic dans le fichier .htaccess en copiant ces options à l’intérieur

AuthName "Entrez le login et le mot de passe "

AuthType Basic

AuthUserFile "/etc/apache2/.htpassword"

Require valid-user

Ouvrez le fichier de configuration du site par défaut

gedit /etc/apache2/sites-enabled/000-default.conf

Placez le contexte de secret1 dans ce fichier à l’intérieur de la directive VirtualHost par défaut

<Directory "/var/www/html/secret1">

Options Indexes FollowSymLinks MultiViews

AllowOverride All

Order allow,deny

allow from all

</Directory>

Appliquez les modifications en redémarrant le serveur web

service apache2 restart

Créez un compte et réalisez une authentification en mode Basic par le bais du site disponible sur le <http://localhost> à partir du browser.

**Exercice 4 :** Mettre en œuvre l’authentification Basic et réalisez une trace en vous basant sur Wireshark.

**Mécanismes d’authentification en mode Digest :**

Dans cet exercice, il est demandé d’implémenter une authentification des clients en mode http Digest. Ces clients « authentifiés » auront le droit d’accéder à un dossier sur l’espace web appelé secret2.

Créez le fichier contenant les mots de passes pour l’authentification en mode Digest

touch /etc/apache2/.htdigestpasswd

Créez un ou plusieurs utilisateurs avec la commande htdigest de Apache en ligne de commandes (domaine est secret2)

htdigest /etc/apache2/.htdigestpasswd "domaine" utilisateur

Les mêmes opérations concernant les fichiers .htaccess dans /var/www/html/secret2 (en remplaçant AuthType Basic par AuthType Digest) et le fichier 000-default.conf en créant un nouveau contexte pour le répertoire /var/www/html/secret2 contenant exactement le même contenu qu’il y a dans le mode Basic.

N’oubliez pas de charger le module mod\_auth\_digest de Apache s’il n’est pas disponible dans le répertoire /etc/apache2/mods-enabled (faire un lien symbolique depuis /etc/apache2/mods-available/auth\_digest.load)

ln -s /etc/apache2/mods-available/auth\_digest.load /etc/apache2/mods-enabled/

Enfin redémarrer le serveur apache

**Exercice 5 :** Mettre en œuvre l’authentification Basic et réalisez une trace en vous basant sur Wireshark.

**Mécanismes d’authentification par OTP :**

Téléchargement du module d’authentification OTP pour apache :

<http://137.194.x.y/TP-auth/mod_authn_otp-1.1.7.tar.gz>

Décompression des fichiers

tar xzvf mod\_authn\_otp-1.1.7.tar.gz

Compilation du module

cd mod\_authn\_otp-1.1.7

./configure

make

make install

Chargement du module dans Apache : ajoutez cette ligne à la fin du fichier /etc/apache2/apache2.conf

LoadModule authn\_otp\_module /usr/lib/apache2/modules/mod\_authn\_otp.so

Création d’un fichier d’utilisateurs de OTP pour Apache

cd /etc/apache2

mkdir otp

touch otp/otp.users

Configuration d’un site avec un accès protégé par OTP

Mettez la configuration suivante pour une authentification Basic par OTP dans le VirtualHost par défaut

<Directory "/var/www/html/secret">

AuthType basic

AuthName "Dossier protégé par OTP"

AuthBasicProvider OTP

Require valid-user

OTPAuthUsersFile /etc/apache2/otp/otp.users

OTPAuthLogoutOnIPChange On

OTPAuthMaxLinger 600

</Directory>

Puis on redémarre Apache

service apache2 restart

**Exercice 6 :** Mettre en œuvre OTP et réalisez une trace en vous basant sur Wireshark.