Pràctica 3b: Mecanismes d'autenticació, autorització i control d'accés d'Apache2. Realms d'Apache2.

1- Introducció

L'objectiu de la pràctica és fer un breu estudi dels mecanismes **d'autenticació, autorització** i **control d'accés** del servidor de pàgines web Apache2. Associat a aquests mecanismes existeix el concepte de **Realm** que també s'estudiarà breument.

1.1- Definicions

El mecanisme d'**autenticació** permet demanar a un usuari que vol accedir a un recurs del servidor un **nom d'usuari i una contrasenya** i d'aquesta manera es pot confirmar l'identitat de l'usuari, o en altres paraules, verificar que un usuari és realment qui afirma ser. La llista d'usuaris i les seves contrasenyes es desen en un **proveïdor d'autenticació**, que pot ser per exemple un fitxer de texte, una base de dades SQL o una base de dades LDAP.

El mecanisme d'**autorització** controla de quina manera un usuari autenticat pot accedir a un determintat recurs. Per exemple, controla si un l'usuari autenticat pot o no pot accedir a un document html que es troba dins d'una carpeta. El mecanisme d'autorització està associat bàsicament a l'usuari autenticat i el recurs al qual es vol accedir.

El **control d'accés** és un mecanisme més general de controlar la manera d'accedir a un recurs. Es pot permetre o denegar l'accés a un recurs en funció de l'adreça IP origen, el dia i hora, el navegador que s'utilitza, el port origen i altres criteris. El control d'accés no està associat per tant a un usuari autenticat sino a altres criteris més generals.

Formen part d'un **realm**, un conjunt de recursos:
a) Que estan protegits per un mateix mecanisme d'autenticació.
b) Als quals s'hi accedeix a partir d'una mateixa URL comuna més el nom específic del recurs
c) Que utilitzen el mateix valor de realm, o sigui una mateixa cadena de caràcters per identificar-lo (com si fos un nom de realm).

Un exemple de realm podria ser una carpeta del servidor, amb pàgines html, codis php i fotogràfies jpg. Si poder accedir-hi el navegador ens obre una finestra per posar un nom d'usuari i contrasenya, llavors estem accedint al realm. El valor (el nom) del realm sortirà a la finestra oberta per informar-nos de quin és el realm al qual volem accedir.

Podem existir múltiples realms definits en un servidor.

1.2- Implementació dels mecanismes d'autenticació i autorització

Per poder implementar els mecanismes d'autenticació, autorització i control d'accés cal que el servidor Apache2 tingui habilitats una sèrie de mòduls. Els mòduls necessaris són els següents:

a) El mòduls **authn_core** i **authz_core** són necessaris com a base per poder fer anar a tota la resta de mòduls d'autenticació, autoritzacií i control d'accés i per tant han d'estar habilitats.

b) S'ha d'habilitar un o més **mòduls d'autenticació**, que indiquen el tipus d'autenticació que es poden utilitzar. Existeixen dos tipus de mecanisme d'autenticació:

* El tipus **bàsic**, a on els noms d'usuaris i contrasenyes son enviats dins d'una capçalera HTTP sense encriptar les dades (tot i que estiguin codificades amb el sistema **base64**, que és facilment **reversible**). Per activar-lo cal tenir habilitat el mòdul **auth_basic**

* El tipus **digest** que proporciona confidencialitat aplicant al nom d'usuari i contrasenya l'algorisme **MD5**, que és una **funció hash criptogràfica**, que produeix un valor **hash** de 128 bits. Per activar-lo cal tenir habilitat el mòdul **auth_digest**.

c) S'han d'habilitar un o més mòduls **proveïdors d'autenticació**, que permeten utilitzar una o més maneres diferent d'emmagatzemar els noms d'usuari i contrasenyes. Entre d'altres , podem trobar les següents maneres d'emmagatzematge:

* Dins d'un fitxer de texte. Cal habilitar el mòdul **authn_file**

* Dins d'una base de dades SQL. Cal habilitar el mòdul **authn_dbd**

* Dins d'una base de dades LDAPs. . Cal habilitar el mòdul **authnz_ldap**

d) S'han d'habilitar un o més mòduls d'**autorització**, que permeten utilitzar un o més mètodes de control a quins recursos poden accedir i a quins no poden accedir un usuari autenticat. Alguns d'aquests mòduls són per exemple:

* **authz_user** : Els drets d'accés s'han d'especificar amb la directiva `Require user` dins dels arxius de configuració del servidor (per exemple dins de la configuració d'un lloc virtual) .

* **authz_dbd** : Els drets d'accés s'han d'especificar dins d'una base de dades SQL.

* **authnz_ldap** : Els drets d'accés s'han d'especificar dins d'una base de dades LDAP.

e) S'han d'habilitar un o més mòduls de **control d'accés** per poder utilitzar un o més mecanismes de control d'accés als recursos en base a criteris com el mètode, l'adreça IP, el navegador, etc. Un dels més importants és **authz_host** que s'utilitza per controlar l'accés al recurs basant-se en criteris com adreça IP, nom d'ordinador.

2- Configurant Apache2 per accedir a un realm amb el mecanisme d'autenticació basic, proveïdor d'autorització de tipus *file* i autorització de tipus *user*.

a) Amb l'ordre **apachectl -M**, verifica que per defecte estan instal·lats i habilitats els següents mòduls:

* Els mòduls bàsics **authn_core** i **authz_core**
* El mòdul d'autenticació **auth_basic**
* El mòdul proveïdor d'autenticació **authn_file**
* El mòdul d'autorització **authz_user**

En cas negatiu habilita el mòdul que falti amb l'ordre **a2enmod** i reinicia el servidor.

b) Dins del directori **/var/www/html/asix2s** que vas crear a la pràctica anterior, crea un directori de nom **notes**.

c) Dins de la carpeta **notes**, crea un fitxer de nom **notes.html** amb el següet contingut:

```
<html>
      <head>
            <title> Web de notes d'asix2 M08UF2</title>
      </head>
      <body>
            Joan Pons (jpons):   6<br>
            Anna Lopez (alop):   7<br>
            David Perez (dper):  7<br>
            Antoni Llop (allop): 3<br>
      </body>
</html>
```

d) Crea un directori ocult de nom **.ctsnyes** dins del directori **/etc/apache2**. Dins d'aquest directori, crea un fitxer ocult de nom ***.contrasenyes*** amb els següents usuaris i contrasenyes:

USURI	CONTRASENYA
jpons	fjeclot00
alop	fjeclot01
dper	clotfje00
allop	clotfje01

Per poder crear el fitxer amb la contrasenya i nom del primer usuari, executa dins del directori **.ctsnyes** :

```
htpasswd  -c  .contrasenyes  jpons
```

i per la resta d'usuaris:

```
htpasswd  .contrasenyes  alop
htpasswd  .contrasenyes  dper
htpasswd  .contrasenyes  allop
```

e) Per protegir el contingut el contingut de fitxer d'usuaris i contrasenyes però al mateix temps fer-ho accessible a **apache2**, executa com a **root**:

```
chown -R root:www-data /etc/apache2/.ctsnyes
chmod 750 /etc/apache2/.ctsnyes
chmod 640  /etc/apache2/.ctsnyes/.contrasenyes
```

f) Modifica l'arxiu de configuració **asix2s.conf** que vas crear a la pràctica anterior. La nova configuració completa serà aquesta:

```
<IfModule  mod_ssl.c>
   <VirtualHost  *:443>
         ServerAdmin  webmaster@asix2s.net
         ServerName  www.asix2s.net
         ServerAlias  web.asix2s.net
         DocumentRoot  /var/www/html/asix2s
         ErrorLog  ${APACHE_LOG_DIR}/error.log
         CustomLog  ${APACHE_LOG_DIR}/access.log  combined
         DirectoryIndex  index.html  index.php
         SSLEngine  on
         SSLCertificateFile  /etc/ssl/certs/asix2.crt
         SSLCertificateKeyFile  /etc/ssl/private/asix2.pem
         <Directory "/var/www/html/asix2s/notes">
               AuthType Basic
               AuthName "notes asix2 m08uf2"
               AuthBasicProvider file
               AuthUserFile /etc/apache2/.ctsnyes/.contrasenyes
               Require valid-user
         </Directory>
   </VirtualHost>
</IfModule>
<VirtualHost  *:80>
   ServerName  www.asix2s.net
   DocumentRoot  /var/www/html/asix2s
   Redirect permanent / https://www.asix2s.net
</VirtualHost>
```

g) Reinicia el servidor **apache2** executant **systemctl restart apache2**.

h) Intenta accedir a la web de notes utilitzant l'URL **`https://www.asix2s.net/notes/notes.html`** . Comprova que:

- En el moment d'accedir et demana un usuari i contrasenya.
- Que pots accedir-hi al recurs si utilitzes qualsevol usuari i contrasenya vàlids
- Que no pots accedir-hi si fas servir un nom d'usuari i/o contrasenya invàlids

i) Per comprovar que tots els usuaris funcionen, assegura't de que el navegador no recorda mai l'historial i valida't com usuari **jpons**, **alop**, **dper** i **allop** fent la prova tancant i obrint el navegador,

Comprovació

a) Data de comprovació de la pràctica: **19/12/18**.

b) Comprovacions:

* Accés a la pàgina notes.html amb https i usuari jpons
* Accés a la pàgina notes.html amb https i usuari alop
* Accés a la pàgina notes.html amb https i usuari dper
* Accés a la pàgina notes.html amb https i usuari allop