Pràctica 4b: Mecanismes d'autenticació i control d'accés (autorització)

1- Introducció

L'objectiu de la pràctica és fer un breu estudi dels mecanismes **d'autenticació i autorització** del servidor de pàgines web Apache2.

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 és un fitxer de texte o una base de dades SQL o LDAP.

El mecanisme d'**autorització** és un procés pel qual s'autentica a un usuari i se'l dóna els permisos necessaris per accedir als recursos disponibles en el servidor. Per donar permisos, s'utilitza un sistema de **llistes de control d'accés ACL** als diferents recursos del servidor, com per exemple un directori, un fitxer o una base de dades.

Un conjunt de recursos els quals es troben sota el control dels mateixos mecanismes d'autenticació i autorització, i que fa servir el mateix proveïdor d'autenticació conformen un **realm**. Un **realm** necessita un **nom de realm** per ser identificat.

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

a) S'ha d'habilitar com a mínim un **mòdul d'autenticació**, que indica el tipus d'autenticació utilitzada. Existeixen dos mètodes autenticació. Primer hi ha el **mètode 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 **mod_auth_basic**. El segon, és el **mètode 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 **mod_auth_digest**.

b) S'ha d'habilitar com a mínim un mòdul per indicar el **proveïdor d'autenticació**. Per defecte està habilitat el mòdul **mod_authn_file** que permet desar la llista d'usuaris i contrasenyes dins d'un fitxer de texte pla. Altres mòduls són per exemple **mod_authn_dbd** per desar la llista en una base de dades SQL o **mod_authn_ldap** per desar la llista en una base de dades LDAP.

c) S'ha d'habilitar com a mínim un mòdul d'**autorització** que proporciona el mecanisme per permetre que els usuaris autenticats se'ls doni o denegui el permís per accedir als diversos recursos del servidor per mitjà de **llistes de control d'accés**. Alguns d'aquests mòduls són per exemple: **mod_authz_user, mod_authz_host**, **mod_authz_dbm** o **mod_authz_ldap**.

2- Configurant Apache2 per treballar amb el mecanisme d'autenticació *bàsica*, proveïdor d'autorització de tipus *file* i autorització de tipus *user*.

a) Amb l'ordre **apachectl -M**, verifica que els mòduls "***auth_basic_module***", **authn_file_module** i **authz_user_module** estan instal·lats i habilitats.

b) Crea un directori de nom **/var/www/html/news**.

c) Crea un directori de nom **/etc/apache2/passwd**.

d) Descarrega dins del directori **/var/www/html/news** el fixer **news.tar.gz** que trobaràs a ***aquest enllaç***. Extreu el seu contingut. Comprova que has obtingut els següents fitxers: **index.html**, **sportsnews.html** i **nationalnews.html**. Esborra **news.tar.gz**.

e) Crea un fitxer **proveïdor d'autenticació** de nom **passwords** dins del directori **/etc/apache2/passwd** i que tingui definida la llista d'usuaris i contrasenyes següents:

* Usuari **reader00**, contrasenya **fjeclot00**.
* Usuari **reader01**, contrasenya **fjeclot01**.

Per dur a terme aquesta tasca, s'ha d'utilitzar l'eina **htpassw**. Per crear l'usuari **reader00** i generar el fitxer **passwords** d'acord amb l'ennunciat, has d'executar:

```
htpasswd  -c  /etc/apache2/passwd/passwords  reader00
```

NOTA IMPORTANT: Si vols afegir un nou usuari a un fitxer proveïdor d'autenticació que ja existeix, **NO** has de posar l'opció **-c**. L'opció **-c** crea un fitxer si no existeix, i esborra l'antic i en crea un de nou si el fixer ja existia. Per crear l'usuari **sports** i afegir-lo al fitxer **passwords** d'acord amb l'ennunciat, has d'executar:

```
htpasswd  /etc/apache2/passwd/passwords  reader01
```

f) Fes que el propietari del directori **`/etc/apache2/passwd/`** (i tots els fitxers inclosos) sigui **root** i que el grup amb permisos especials sigui **www-data**. Dóna permisos **rwx** a root, **r-x** a **www-data** i **- - -** a la resta d'usuaris.
NOTA: El servidor **Apache2** treballa amb els permisos de l'usuari de sistema **www-data** que és membre del grup **www-data**.

g) Fes una còpia de seguretat del fitxer de configuració del lloc web virtual per defecte d'Apache2. El fitxer és **/etc/apache2/sites-available/000-default.conf**. Crea una còpia amb el nom **000-default.conf.original**.

h) Modifica l'arxiu de configuració del site principal (**000-default**) per indicar el directori a on es troben els nous recursos recursos que volem afegir. Aquest directori tindrà la següent configuració:

1- Directori: **/var/www/html/news**
2- Opcions: **a)** Mostrar la llista de continguts de la carpeta si no hi ha el fitxer index.html, **b)** Seguir enllaços simbòlics de la carpeta i **c)** Acceptar i treballar amb multiples llengües.
3- No permetre configuracions extres per mitjà de fitxers **.htaccess**.
4- Ordre de processament de directives allow i deny --> allow,deny
5- Equips que poden accedir als recursos: Tots.
6- Autenticació: **basic** (Directiva **AuthType**)
7- Nom del **realm**: **"Àrea privada. Es requereix validació"** (Directiva **AuthName**)
NOTA: A **http://www.admin-linux.fr/?p=7750** trobareu la informació necessària per passar el fitxer de codificació UTF-8 a ISO-8859-1 i això poder veure els accents correctament.
8- Tipus de proveïdor d'autenticació: **file** (Directiva **AuthBasicProvider**)
9- Fitxer proveïdor d'utenticació: **etc/apache2/passwd/passwords** (Directiva **AuthUserFile**)
10- Dóna permis nomes a **reader00** per accedir a **news** (Directiva **Require** i opció **user**).

Per poder realitzar aquesta configuració s'han d'utilitzar les següents directives: Directory, Options, AllowOverride, Order, Allow/Deny, AuthType, AuthName, AuthBasicProvider, AuthUserFile i Require. Pots trobar informació sobre les directives a **http://httpd.apache.org/docs/current/mod/directives.html**

i) Intenta accedir als recursos que es troben a **/var/www/html/news** i al mateix temps captura l'interncanvi de missatges entre el servidor i el client amb **wireshark**. Comprova:

1- El funcionament del **mètode bàsic** d'autenticació.
2- Comprova que **reader00** pot accedir al directori **news**. Comprova que **reader01** no pot accedir a **news**. Comprova que **reader00** pot accedir al directori **news** amb una contrasenya incorrecta.
3- Comprova els missatge enviats pel client i servidor,i identifica el missatge del client a on s'ha enviat el nom d'usuari i la contrasenya. Comprova el valor de l'usuari i contrasenya.

k) Fes una còpia de seguretat del fitxer de configuració que has creat. El nom de la còpia serà: **000-default_basic.conf**.

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

a) Verifica que el mòdul "***auth_digest_module***" està habilitat. En cas negatiu, comprova si tens aquest mòdul disponible a **/etc/apache2/mods-available**, i habilita'l amb l'ordre **a2enmod**.

b) Crea un fitxer **proveïdor d'autenticació** de nom **passwords2** dins del directori **/etc/apache2/passwd** i que tingui definit a l'usuari **reader** amb contrasenya **fjeclot00** i auorització d'accés al realm **news**.

Per dur a terme aquesta tasca, s'ha d'utilitzar l'eina **htpdigest**. Per crear l'usuari **reader** i generar el fitxer **passwords2** d'acord amb l'ennunciat, has d'executar:

```
htdigest -c /etc/apache2/passwd/passwords2 news reader
```

Recorda que per afegir un nou usuari a un fitxer proveïdor d'autenticació que ja existeix, **NO** s'ha de posar l'opció **-c**.

c) Fes que el propietari del fitxer **`/etc/apache2/passwd/passwords2`** sigui **root** i que el grup amb permisos especials sigui **www-data**. Dóna permisos **rwx** a root, **r-x** a **www-data** i **- - -** a la resta d'usuaris.

d) Modifica la configuració d'accés al directori **/var/www/html/news**. Fes els canvis necessaris perquè la configuració sigui:

1- Autenticació: **digest**
2- Nom del realm: **news**
2- Fitxer proveïdor d'utenticació: **etc/apache2/passwd/passwords2**

f) Intenta accedir als recursos que es troben a **/var/www/html/news** i al mateix temps captura l'interncanvi de missatges entre el servidor i el client amb **wireshark**. Comprova:

1- El funcionament del **mètode digest** d'autenticació. Des del punt de vista d'un usuari, hi ha cap diferència entre els 2 mètodes?
2- Comprova que **reader** pot accedir al realm **news**.
3- Comprova els missatge enviats pel client i servidor,i identifica el missatge del client a on s'ha enviat el nom d'usuari i la contrasenya. Comprova el valor de l'usuari i contrasenya.

g) Fes una còpia de seguretat del fitxer de configuració que has creat a l'apartat anterior. El nom de la còpia serà **000_default_digest.conf**.

Comprovació
a) Data de comprovació de la pràctica: **16/11/16**.
1- Comprovació de d'autenticació bàsica amb **reader01** i **reader00**.
2- Captura de **wireshark** amb l'autenticació bàsica. Visualització de la contrasenya de **reader00**.
3- Comprovació de d'autenticació **digest** amb **reader**.
4- Captura de **wireshark** amb l'autenticació **digest**. Visualització de la contrasenya de **reader**.