I.U.T.
Université d'Artois

Sécurité des serveurs web

Fiche de TP n.2 – Apache

1 Autorisation ou interdiction d'accès

Il est possible d'autoriser ou d'interdire l'accès de certaines pages Web (des pages d'un répertoire par exemple) à des adresses IP, à des noms d'hôtes, à des groupes d'adresses IP ou bien encore des groupes de noms d'hôtes. Pour cela, on utilise les commandes `allow from ...` (pour autoriser) et `deny from ...` (pour interdire). Par exemple :

- `allow from all` : autorise l'accès à tout le monde,
- `allow from 12.23` : autorise l'accès aux adresses IP commençant par 12.23,
- `deny from .fr` : interdit l'accès à tous les noms d'hôtes du domaine .fr,
- `deny from belgique.iut-lens.univ-artois.fr` : interdit l'accès à l'hôte belgique.iut-lens.univ-artois.fr.

La directive `Order` permet de spécifier quelle est la propriété la plus prioritaire entre `allow` et `deny` :

```
Order deny, allow
```

spécifiera que `allow` est prioritaire (il a le dernier mot) par rapport à `deny`.

```
Order allow, deny
```

spécifiera que `deny` est prioritaire par rapport à `allow`.

Ainsi, les directives suivantes :

```
<Directory rep1>
  Order allow, deny
  Allow from all
  Deny from 123.34.56.45
</Directory>

<Directory rep2>
  Order deny, allow
  Allow from all
  Deny from 123.34.56.45
</Directory>
```

font en sorte que `rep1` est accessible à tout le monde sauf au client ayant pour adresse IP `123.34.56.45`, tandis que `rep2` est accessible à tout le monde.

M0. Créez un répertoire `<homeUserDir>/web/confidentiel1` contenant un fichier `fichier1.txt`. Interdisez l'accès à tout le monde sauf à l'IP `127.0.0.1`. Créez un répertoire `<homeUserDir>/web/confidentiel2` contenant un fichier `fichier2.txt`. Interdisez l'accès à tout le monde sauf à l'hôte voisin où voisin est le nom de la machine voisine. Testez ces permissions.

2 Authentification par mot de passe

Il est possible de protéger l'accès de fichiers par mot de passe. Pour cela il faut utiliser les directives `AuthType` pour indiquer le type d'accès utilisé (`Basic` ou `Digest`), `AuthName` pour indiquer le domaine dans lequel les noms et les mots de passe doivent être valides. `AuthUserFile` indique le fichier contenant les noms d'utilisateurs et leur mots de passe, `AuthGroupFile` indique un fichier dans lequel est défini un ensemble de groupes d'utilisateurs. `Require` permet d'indiquer quels sont les utilisateurs qui pourront accéder aux documents du répertoire après authentification, on peut spécifier des noms d'utilisateurs, des noms de groupes d'utilisateurs ou bien encore `valid-user` pour indiquer tous les utilisateurs du fichier de mots de passe. Ainsi, la directive suivante :

```
<Directory rep>
  AuthType Basic
  AuthName secret
  AuthUserFile /home/jean/.htpasswd
  Require valid-user
</Directory>
```

spécifie que les documents du répertoire `rep` sont accessibles uniquement pour les utilisateurs spécifiés dans le fichier `/home/jean/.htpasswd` après une authentification par mot de passe de type `Basic`.

M1. Créez le répertoire `<homeUserDir>/web/confidentiel3` contenant un fichier `fichier3.txt`. Rajoutez dans `httpd.conf` les directives indiquant que le contenu de ce répertoire est protégé par une authentification (de type `Basic`) par mot de passe (fichier `.htpasswd` de `confidentiel3`) pour tout le monde (`valid-user`) et que le royaume de ce répertoire est secret. En utilisant mozilla, tentez d'accéder à fichier3.txt. Recommencez avec telnet, pour noter les détails de la réponse du serveur (les entêtes et le statut).

M2. Personne ne peut accéder à `fichier3.txt` puisque le fichier de mots de passe `.htpasswd` de `confidentiel3` n'est pas créé. Utilisez l'utilitaire `htpasswd` pour créer ce fichier contenant l'utilisateur `suzhen` et son mot de passe `chowchow`. Tentez d'accéder à `fichier3.txt` avec l'utilisateur `suzhen`.