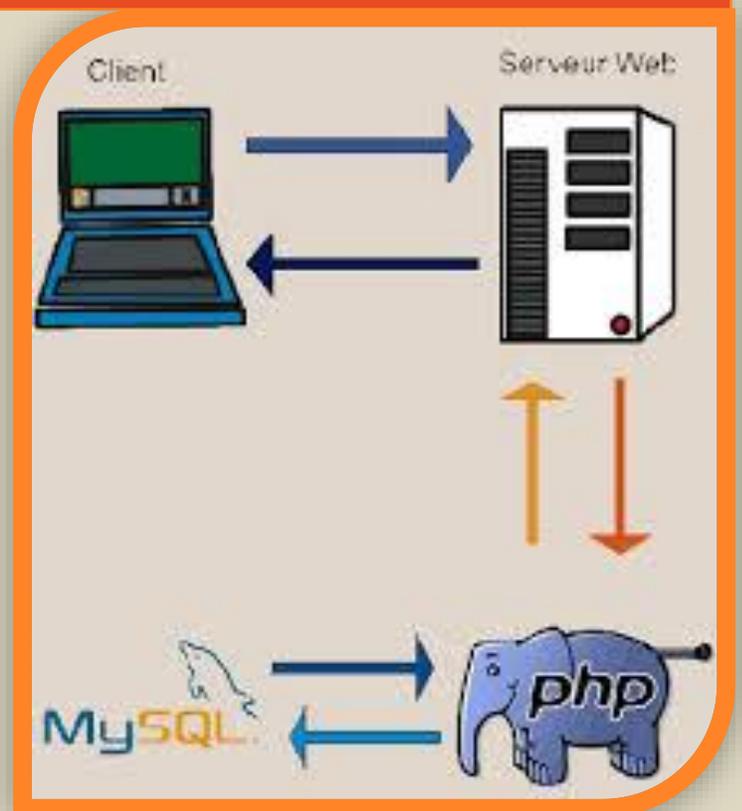


TP SERVEUR WEB



NGUELE YVES GABIN

2^{ème} année BTS SIOR

10 Octobre 2013

CONSIGNES

Remplacez ce texte par le vôtre. Vous pouvez également remplacer les images (sur la page précédente et à droite) par les vôtres.

Rédiger un document relatif à l'installation du serveur APACHE (mode opératoire, vos choix de configuration...)

Rédiger un document qui présente les choix de sécurisation du serveur APACHE.

Pour chaque option de sécurité préciser:

- le principe de sécurisation (en quoi consiste cette sécurisation)
- son implémentation (extrait des fichiers de configuration)
- les éléments utilisés pour vérifier le bon fonctionnement de l'option de sécurité (copies d'écrans, messages, rapport de log...)

Ces deux documents seront enregistrés dans un fichier nommé TP_securisation_VotreNom.pdf.

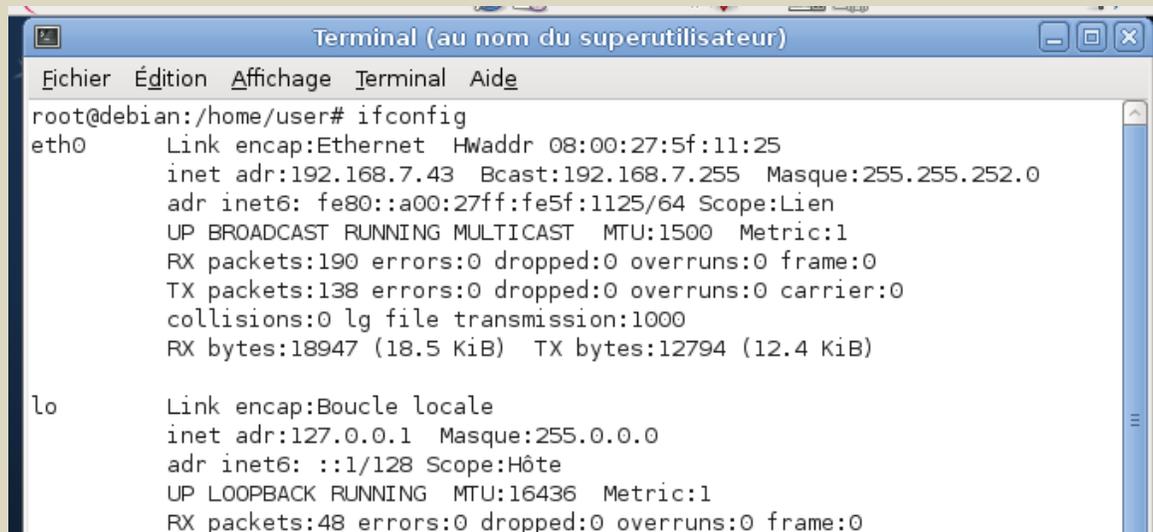
Détaillez le plus possible vos réponses et soignez la forme.

PARTIE 1 : INSTALLATION DU SERVEUR

- 1- Mettre le serveur en adresse fixe 192.168.7.43 et la machine cliente 192.168.7.44

```
root@debian:/home/user# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:5f:11:25
          inet adr:192.168.7.44  Bcast:192.168.7.255  Masque:255.255.252.0
          adr inet6: fe80::a00:27ff:fe5f:1125/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:162 errors:0 dropped:0 overruns:0 frame:0
          TX packets:169 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          RX bytes:18008 (17.5 KiB)  TX bytes:14761 (14.4 KiB)

lo        Link encap:Boucle locale
          inet adr:127.0.0.1  Masque:255.0.0.0
          adr inet6: ::1/128 Scope:Hôte
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:48 errors:0 dropped:0 overruns:0 frame:0
          TX packets:48 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:0
          RX bytes:3876 (3.7 KiB)  TX bytes:3876 (3.7 KiB)
```



```
Terminal (au nom du superutilisateur)
Fichier Édition Affichage Terminal Aide
root@debian:/home/user# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:5f:11:25
          inet adr:192.168.7.43  Bcast:192.168.7.255  Masque:255.255.252.0
          adr inet6: fe80::a00:27ff:fe5f:1125/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:190 errors:0 dropped:0 overruns:0 frame:0
          TX packets:138 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          RX bytes:18947 (18.5 KiB)  TX bytes:12794 (12.4 KiB)

lo        Link encap:Boucle locale
          inet adr:127.0.0.1  Masque:255.0.0.0
          adr inet6: ::1/128 Scope:Hôte
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:48 errors:0 dropped:0 overruns:0 frame:0
```

- 2- Création d'une base de données pour héberger le site appelé `worlds_cook` avec 5 tables

```
mysql> show databases;
+-----+
| Database          |
+-----+
| information_schema |
| mysql             |
| worlds_cook       |
+-----+
3 rows in set (0.02 sec)

mysql>

Database changed
mysql> show tables;
+-----+
| Tables_in_worlds_cook |
+-----+
| adherent              |
| chef                  |
| cours                 |
| inscription           |
| session               |
+-----+
5 rows in set (0.00 sec)
```

- 3- Création d'un utilisateur avec tous les droit sur la base de donnée `worlds_cook` appelé `worlds_cook` et son mot de passe `worlds_cook`

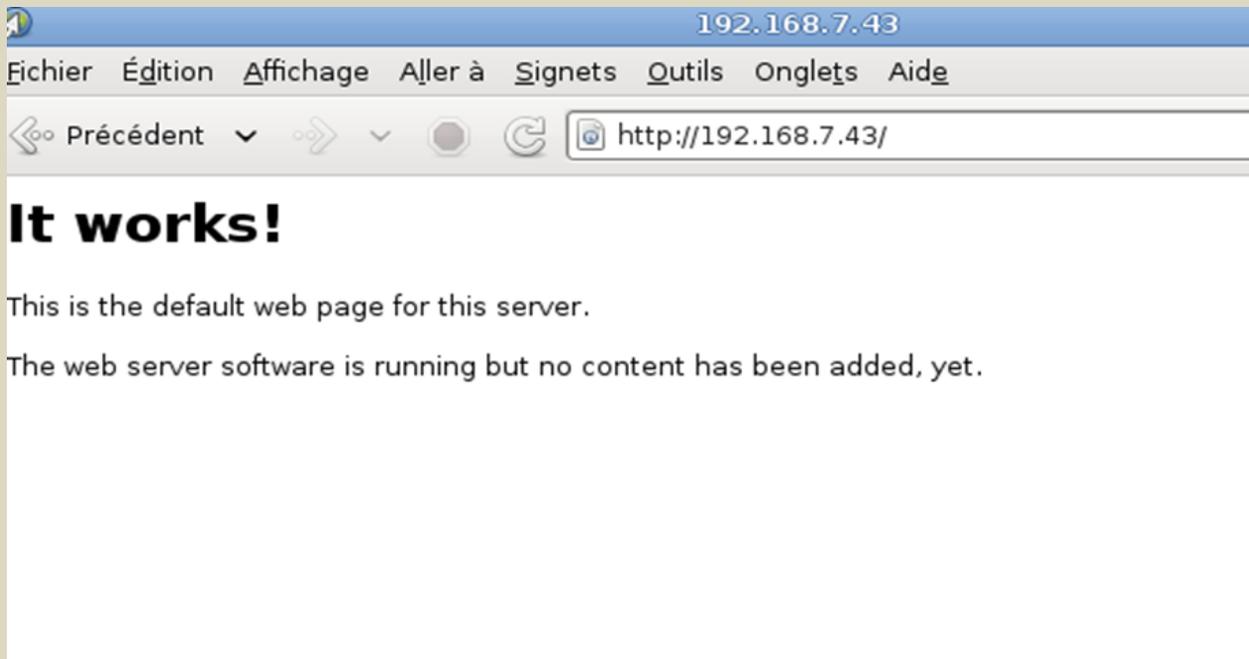
```
mysql> select user from user;
+-----+
| user          |
+-----+
| words_cook    |
| worlds_cook   |
| root          |
| root          |
| debian-sys-maint |
| root          |
+-----+
6 rows in set (0.00 sec)

mysql> █
```

- 4- Installer des paquets `apache2` (et, pour les versions d'Ubuntu avant 10.04, installer manuellement les paquets `apache2.2-common` et `apache2-utils`) pour la version de base
- 5- Pour ajouter des fonctions d'authentification, la gestion du multi-processing et la possibilité de changer le service en mode `root` :

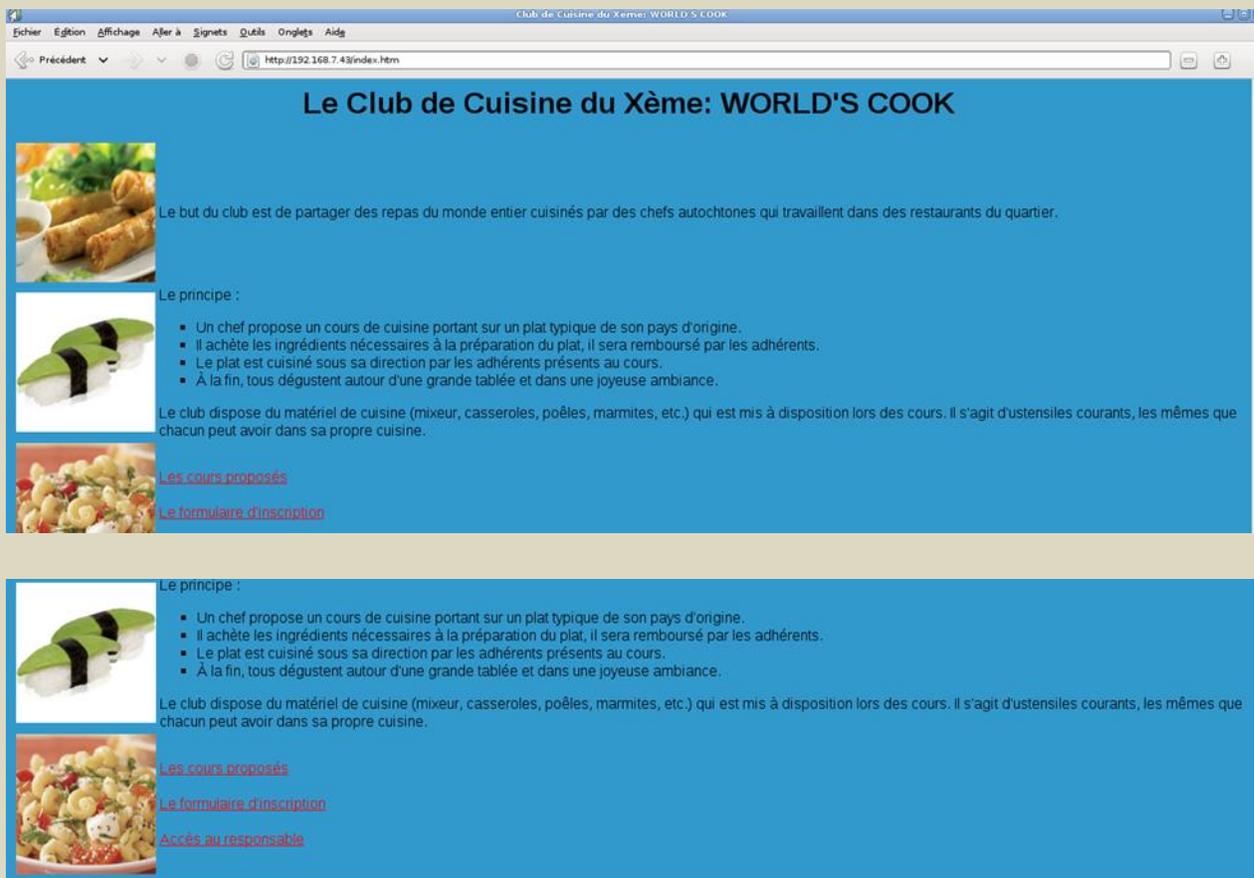
installer les paquetages apache2-mpm-prefork, libapache2-mod-chroot, libapache2-mod-auth-pam, libapache2-mod-auth-sys-group

6- Test du bon fonctionnement du serveur web à partir du client



7- Copie des fichiers du site web que j'ai fait expressément pour le TP dans le WWW

```
root@debian:/home/user# cd /var
root@debian:/var# cd /www
bash: cd: /www: Aucun fichier ou dossier de ce type
root@debian:/var# ls
backups  cache  games  lib  local  lock  log  mail  opt  run  spool  tmp  www
root@debian:/var# cd www
root@debian:/var/www# ls
connect.inc.php  images  scriptcuisine.sql  valide.php
cours.php        index.htm  sessions.php
fonction.inc.php  listeadherents.php  style.css
formulaire.htm   responsable.htm  validation.php
root@debian:/var/www#
```



Club de Cuisine du Xème: WORLD'S COOK

Le but du club est de partager des repas du monde entier cuisinés par des chefs autochtones qui travaillent dans des restaurants du quartier.

Le principe :

- Un chef propose un cours de cuisine portant sur un plat typique de son pays d'origine.
- Il achète les ingrédients nécessaires à la préparation du plat, il sera remboursé par les adhérents.
- Le plat est cuisiné sous sa direction par les adhérents présents au cours.
- À la fin, tous dégustent autour d'une grande table et dans une joyeuse ambiance.

Le club dispose du matériel de cuisine (mixeur, casseroles, poêles, marmites, etc.) qui est mis à disposition lors des cours. Il s'agit d'ustensiles courants, les mêmes que chacun peut avoir dans sa propre cuisine.

[Les cours proposés](#)

[Le formulaire d'inscription](#)

Le principe :

- Un chef propose un cours de cuisine portant sur un plat typique de son pays d'origine.
- Il achète les ingrédients nécessaires à la préparation du plat, il sera remboursé par les adhérents.
- Le plat est cuisiné sous sa direction par les adhérents présents au cours.
- À la fin, tous dégustent autour d'une grande table et dans une joyeuse ambiance.

Le club dispose du matériel de cuisine (mixeur, casseroles, poêles, marmites, etc.) qui est mis à disposition lors des cours. Il s'agit d'ustensiles courants, les mêmes que chacun peut avoir dans sa propre cuisine.

[Les cours proposés](#)

[Le formulaire d'inscription](#)

[Accès au responsable](#)

PARTIE II : SÉCURISATION DU SERVEUR WEB

1- Pour améliorer la sécurité du site, j'ai fait un mot de passe pour avoir accès à l'administration du site dans la rubrique accès au responsable.

Ca va permettre déjà de mettre une première sécurité pour que n'importe qui n'accède à cette partie-là.



2- Cacher la version d'Apache et autres informations sensibles

Par défaut, Apache affiche la version du système d'exploitation j'utilise, ainsi que d'autres informations. Une personne malveillante peut utiliser ces informations pour mieux cibler son attaque mon serveur, je vais donc le cacher.

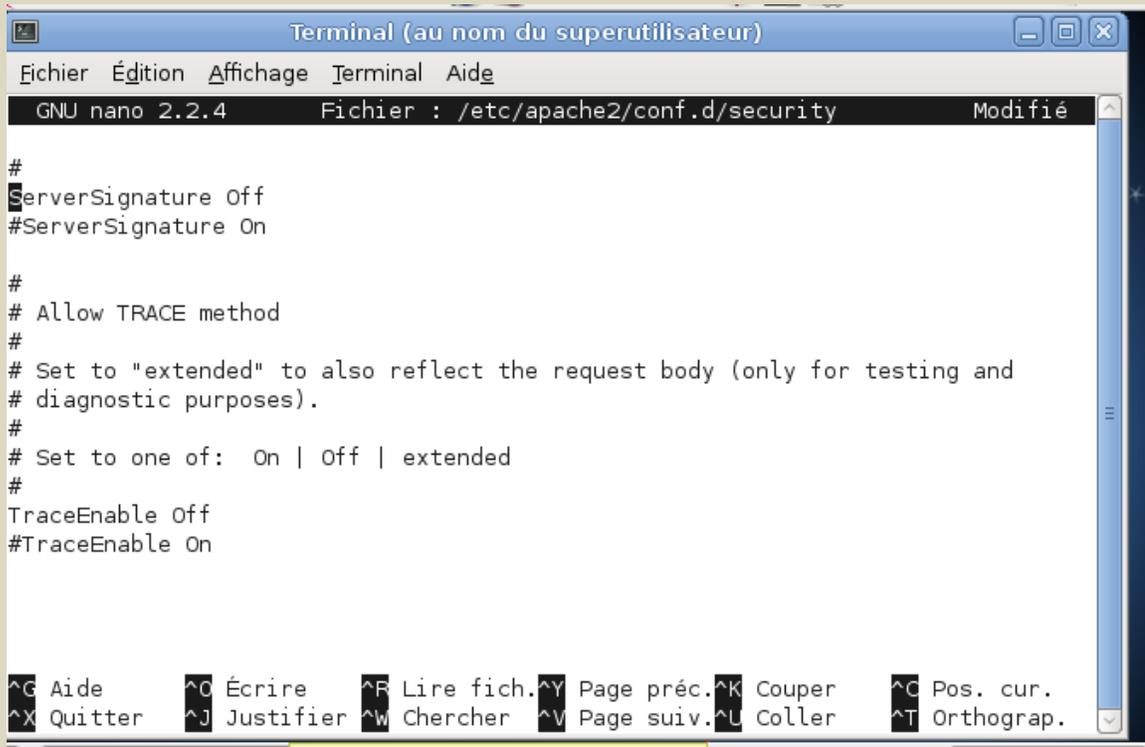
A screenshot of a terminal window titled "Terminal (au nom du superutilisateur)". The terminal shows the GNU nano 2.2.4 editor editing the file /etc/apache2/conf.d/security. The visible content is as follows:

```
#      Order Deny,Allow
#      Deny from all
#</Directory>

# Changing the following options will not really affect the security of the
# server, but might make attacks slightly more difficult in some cases.

#
# ServerTokens Prod
# This directive configures what you return as the Server HTTP response
# Header. The default is 'Full' which sends information about the OS-Type
# and compiled in modules.
# Set to one of: Full | OS | Minimal | Minor | Major | Prod
# where Full conveys the most information, and Prod the least.
#
#ServerTokens Minimal
```

At the bottom of the terminal, there are keyboard shortcuts: ^G Aide, ^O Écrire, ^R Lire fich., ^Y Page préc., ^K Couper, ^C Pos. cur.



```
Terminal (au nom du superutilisateur)
Fichier Édition Affichage Terminal Aide
GNU nano 2.2.4 Fichier : /etc/apache2/conf.d/security Modifié

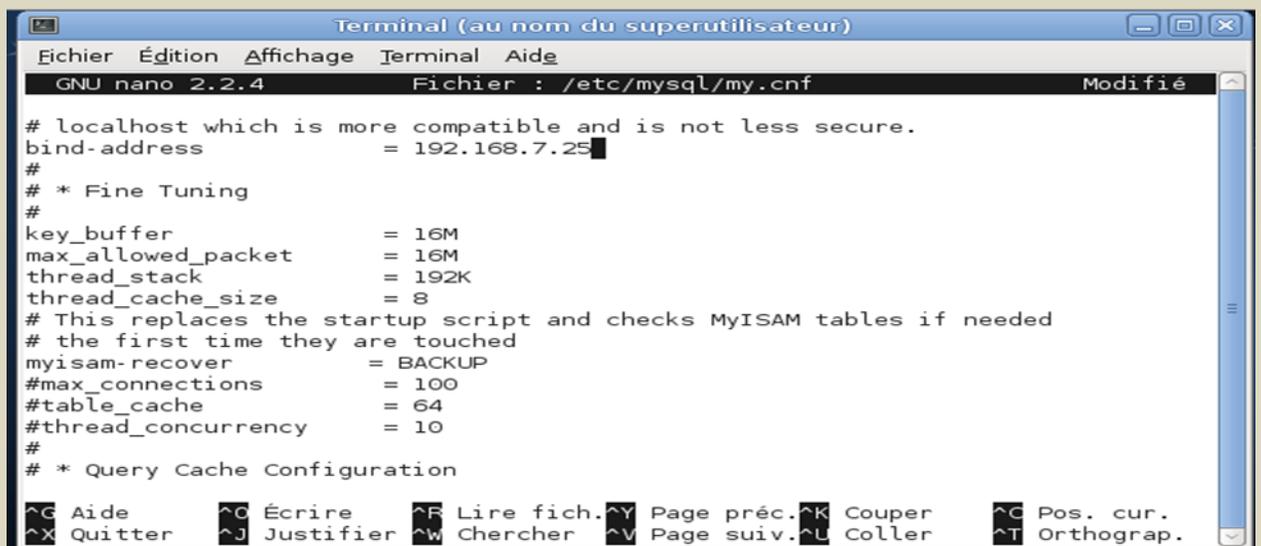
#
ServerSignature Off
#ServerSignature On

#
# Allow TRACE method
#
# Set to "extended" to also reflect the request body (only for testing and
# diagnostic purposes).
#
# Set to one of: On | Off | extended
#
TraceEnable Off
#TraceEnable On

^G Aide      ^O Écrire    ^R Lire fich.^Y Page préc.^K Couper     ^C Pos. cur.
^X Quitter   ^J Justifier ^W Chercher  ^V Page suiv.^L Coller    ^T Orthograp.
```

Pour ce faire je devais modifier les lignes ServerSignature et mettre ServerSignature Off et aussi ServerTokens par ServerTokens Prod

3- Rendre accessible ma base de donnée uniquement par mon serveur avec l'IP 192.168.7.43 en changeant le fichier /etc/mysql/my.cnf



```
Terminal (au nom du superutilisateur)
Fichier Édition Affichage Terminal Aide
GNU nano 2.2.4 Fichier : /etc/mysql/my.cnf Modifié

# localhost which is more compatible and is not less secure.
bind-address      = 192.168.7.25
#
# * Fine Tuning
#
key_buffer        = 16M
max_allowed_packet = 16M
thread_stack      = 192K
thread_cache_size = 8
# This replaces the startup script and checks MyISAM tables if needed
# the first time they are touched
myisam-recover    = BACKUP
#max_connections  = 100
#table_cache      = 64
#thread_concurrency = 10
#
# * Query Cache Configuration
```

4- Empêcher de faire le parcours du répertoire

Pour ce faire j'Ai modifié le fichier `/etc/apache2/sites-available/default` et j'Ai inséré

```
<Directory />
```

```
Order Deny,Allow
```

```
Deny from all
```

```
Options None
```

```
AllowOverride None
```

```
</Directory>
```

```
<Directory /web>
```

```
Order Allow,Deny
```

```
Allow from all
```

```
</Directory>
```

5- Installation de ModSecurity

C'est un module d'Apache spécialisé dans la sécurité. Il permet donc de sécuriser la couche applicative avant l'arrivée des requêtes sur le site hébergé sur l'Apache en question. Même s'il s'agit d'un module, ses fonctionnalités sont vastes et permettent de toucher à tous les points de sécurité nécessaire. Comme utilisations possible, citons la détection de tentatives d'inclusions, la lutte anti-spam, l'utilisation d'exploits (il permet de cacher les numéros de versions utilisées sur les pages d'erreur renvoyées par le serveur Web), l'application d'une liste noire (ou blanche), etc...

6- Installation et Configuration de Brutelock

Brutelock est un programme qui surveille les divers journaux de logs d'un système et bloque immédiatement les IP malveillante visant à attaquer votre serveur.

Brutelock ne protège pas seulement contre les attaques ssh, mais aussi d'autres services communs, comme FTP, POP et IMAP etc...