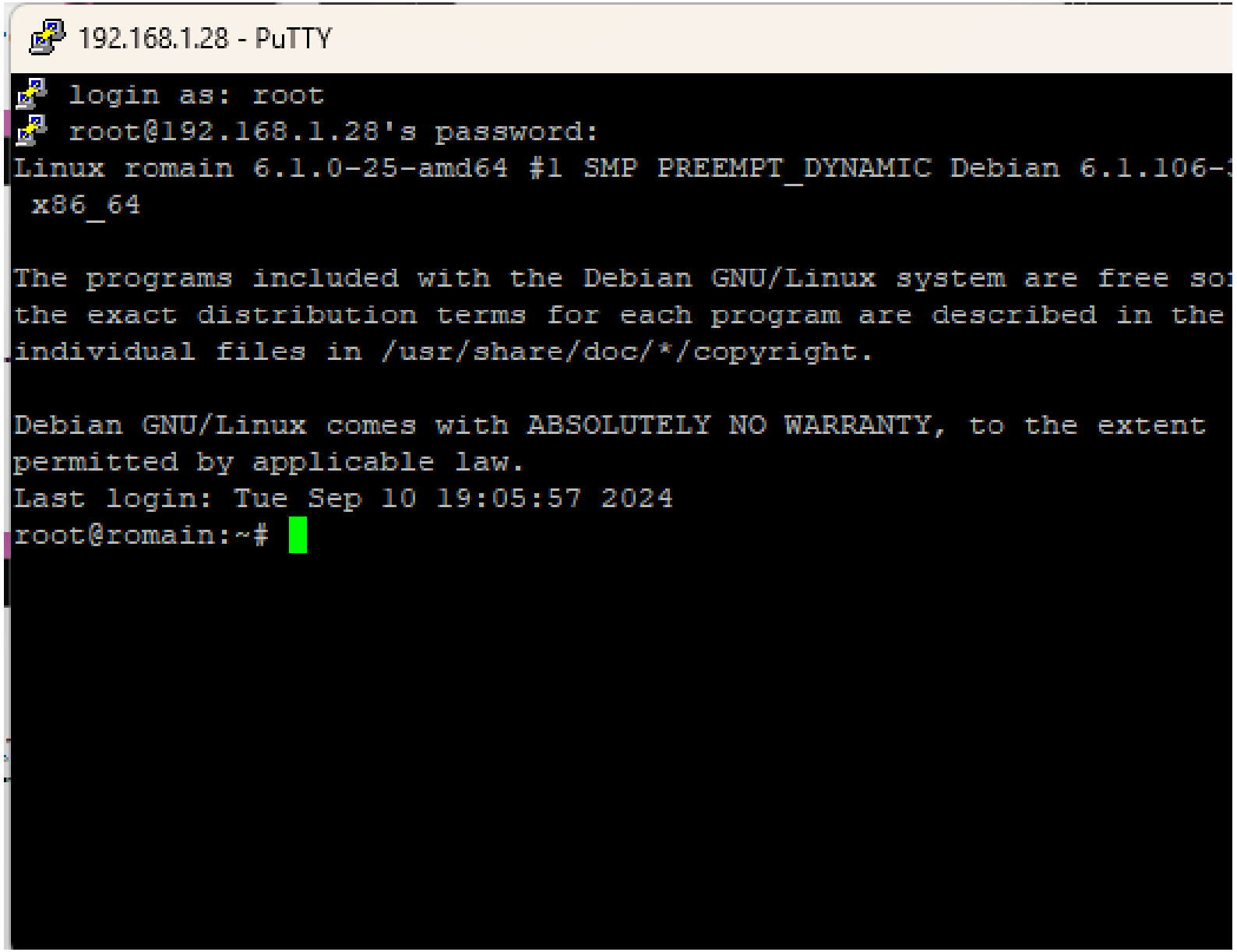
Romain Lheureux

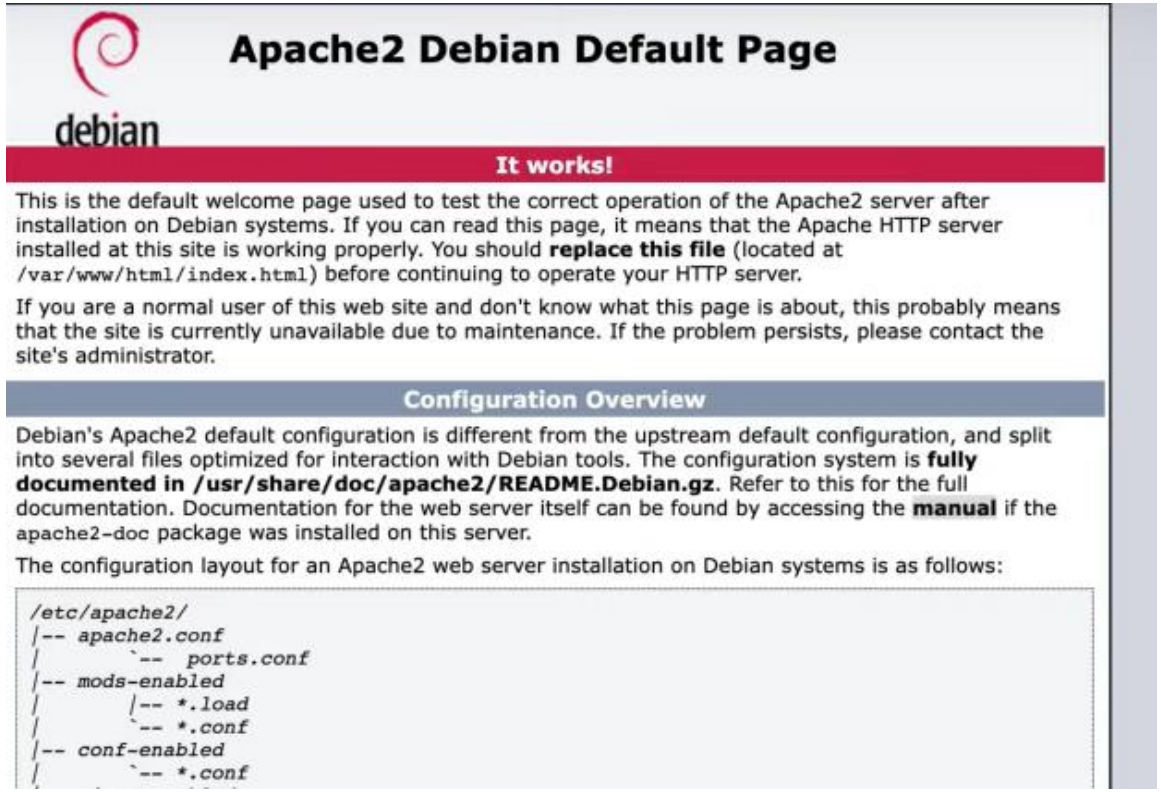
TP SERVEURS

BTS SIO 2 SAINT LUC CAMBRAI **Session 2024-2025**

TP SERVEURS

- Dans un premier temps nous allons installer un ssh pour cela il nous suffit d'effectuer la commande suivante: **« apt install openssh-server »**
- Comme nous pouvons le voir le ssh et bien en place



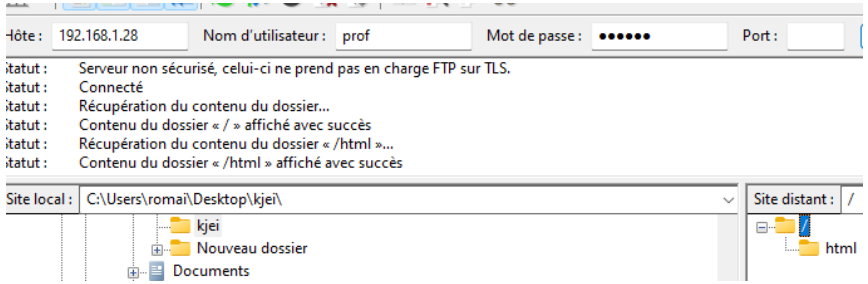


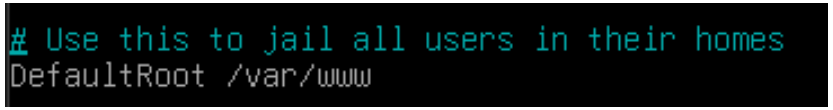
TP SERVEURS

- Ensuite pour le serveur lamp nous allons utiliser apache2, pour se faire nous allons utiliser la commande***: apt install apache2 -y .*** Une fois apache installer nous avons juste à taper l'adresse IP de la Debian et de la rechercher sur internet, ce qui devrait nous donner une page web.

TP SERVEURS

- Ensuite nous allons pouvoir ajouter un ftp dans debian pour se faire nous allons utiliser la commande « **apt get install proftpd** »
- Et nous allons faire en sorte que les utilisateurs créer soit directement diriger dans le dossier /var/www pour se faire nous devons modifier le fichier avec la commande cd /etc/proftpd pour y ajouter « defaultRoot /var/www »





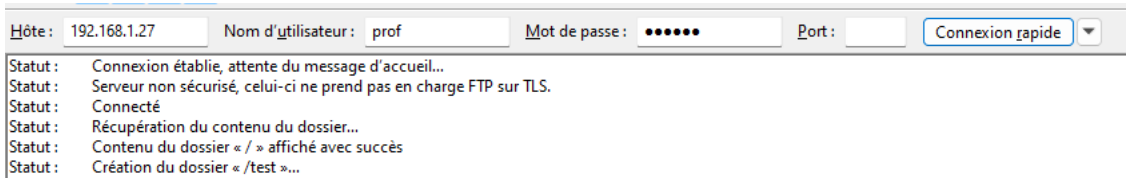
TP SERVEURS

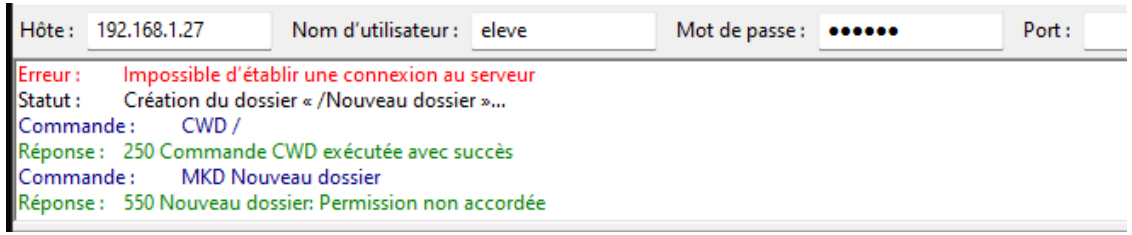
```
root@romain:/var# chown prof /var/www
root@romain:/var# ls -l
total 40
drwxrwxrwx  2 root root  4096  5 sept. 08:40 backups
drwxrwxrwx 22 root root  4096  5 sept. 08:46 cache
drwxrwxrwx 56 root root  4096  5 sept. 08:46 lib
drwxrwsrwx  2 root staff 4096 28 janv.  2024 local
lrwxrwxrwx  1 root root     9  2 sept. 09:30 lock -> /run/lock
drwxrwxrwx 13 root root  4096  5 sept. 08:46 log
drwxrwsrwx  2 root mail  4096  2 sept. 09:30 mail
drwxrwxrwx  2 root root  4096  2 sept. 09:30 opt
lrwxrwxrwx  1 root root     4  2 sept. 09:30 run -> /run
drwxrwxrwx  6 root root  4096  2 sept. 09:35 spool
drwxrwxrwx 11 root root  4096  5 sept. 09:09 tmp
drwxrwxrwx  3 prof root  4096  4 sept. 08:53 www
```

```
root@romain:/var# addgroup eleves
Ajout du groupe « eleves » (GID 1004)...
Fait.
root@romain:/var# usermod -G eleves -a eleve
```

```
root@romain:/var# chmod 750 /var/www
root@romain:/var# chgrp -R eleves /var/www
root@romain:/var# chown -R prof /var/www
root@romain:/var# chmod -R 750 /var/www
root@romain:/var# _
```

- Maintenant nous allons définir les droits entre les différents utilisateurs pour se faire nous allons créer un groupe élevé et y ajouter l'utilisateur élevé avec la commande usermod –G eleves –a eleve
- Nous allons définir l'utilisateur prof comme le propriétaire avec la commande chown ce qui lui permettra de modifier le dossier comme il le souhaite.





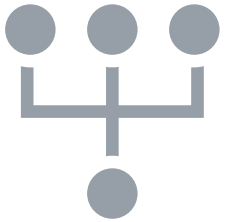
TP SERVEURS

- Maintenant on va essayer si les droits fonctionnent bien pour se faire nous allons utiliser l'outil Filezilla
- Et comme nous pouvons le voir, l'utilisateur prof peut effectuer des modification et l'utilisateur élevé ne peut que regarder,

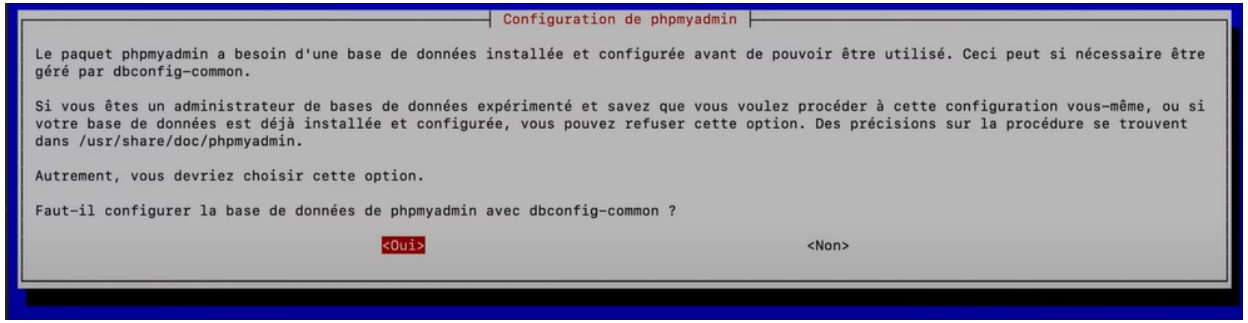
TP SERVEURS

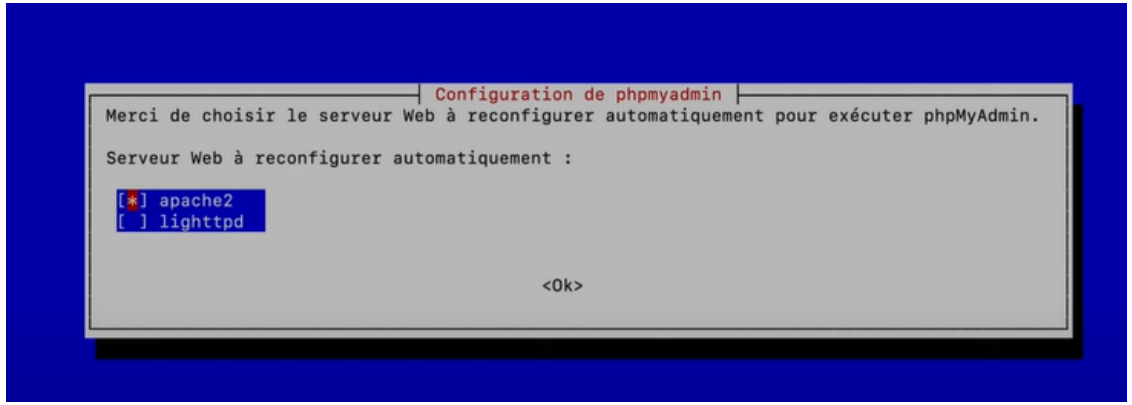
Ensuite nous allons mettre en place phpMyAdmin pour se faire nous allons avoir besoins de php et de mysql

Pour php nous allons utiliser la commande apt install php, pour MySQL utiliser la commande apt install maradb-server –y.



Et pour finir nous allons installer PhpMyAdmin avec la commande : apt install phpmyadmin –y





TP SERVEURS

Ensuite nous allons choisir apache2 et autoriser la configuration de la base de données de phpMyAdmin

TP SERVEURS

Nous allons maintenant administrer les droits a un utilisateur pour qu'il accédé à MySQL et phpMyAdmin

Pour se faire nous allons utiliser la commande : GRANT ALL PRIVILEGES ON (etoile) (point) (etoile) TO 'votre_utilisateur'@'localhost' IDENTIFIED BY 'votre_mot_de_passe' WITH GRANT OPTION;

Nous allons mettre commande dans mysql pour se faire nous allons taper la commande: mysql

TP SERVEURS

Nous allons définir un mot de passe pour accéder à la page web afin de restreindre l'accès a certain utilisateur pour se faire nous allons devoir utiliser un dossier .htaccess

Pour se faire nous allons créer le fichier avec la commande: htpasswd –c /var/www/html/.htpasswd prof. Il faut noter que l'option "-c" (pour créer) n'intervient que si le fichier n'existe pas déjà.

```
root@romain:/var/www/html# htpasswd -c /var/www/html/.htpasswd prof
```

Pour vérifier si tout fonctionne nous allons taper la commande suivante: nano /var/www/html/htpasswd

```
prof:$apr1$kZQyEG8x$PsT7PIAmcH78.qVs5h10c0
```

TP SERVEURS

- Dans le fichier htpasswd nous allons définir des autorisations pour effectuer c modification nous pouvons utiliser le ftp puis sélectionner le fichier et l'édité
- AuthUserFile : Désigne le chemin du fichier où seront stockés les identifiants qui seront valident pour la connexion*
- AuthName "Accés restreints - Veuillez-vous authentifier" : C'est ce qui va être affiché sur la boite de dialogue d'authentification qui apparaitra sur l'écran de l'utilisateur.
- require valid-user : Désigne les conditions qui doivent être validées pour laisser passer l'utilisateur. Ici il ne s'agit que de la validation des identifiants saisis par l'utilisateur. Tous les utilisateurs valident pourront donc accéder à la ressource en question

```
AuthUserFile /var/www/html/.htpasswd
AuthName "Accès restreints - Veuillez vous authentifier"
AuthType Basic
Require valid-user
```

TP SERVEURS

- Nous allons ensuite procéder à la configuration d'apache pour se faire nous allons utiliser la commande suivante nano /etc/apache/sites-available/000-default.conf
- Voici ce qu'il faut mettre dans le fichier
- Le paramètre "**AllowOverride**" permet de déterminer quel fichier ou configuration est autorisé à prendre en priorité la configuration d'Apache 2. Si on le paramètre à "**All**", Apache 2 pourra lire les fichier ".**htaccess**"

```
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html
        <Directory /var/www/>
        AllowOverride all
        </Directory>
        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
```

TP SERVEURS

- Comme nous pouvons le voir, les parameters ont bien été pris en compte