

TRAVAUX PRATIQUES

SOUTIEN LINUX

Hacker Army !



OBJECTIFS

- Identifiez et corriger des failles de sécurité simples
- Utiliser un client FTP

CONSIGNES

Vous rédigerez un compte-rendu personnel reprenant chacune des commandes nécessaires à la réalisation de ce sujet.

Astuce

Un compte-rendu numérique est recommandé afin de pouvoir facilement y copier vos commandes.

CONTEXTE

La société **PLSCORP** a contacté **ESICORP** pour réaliser l'audit de sécurité de l'un de ses serveurs. Max ayant travaillé dans le passé pour cette société, vous avez été choisi pour cette tâche afin d'éviter tout conflit d'intérêt.

MISSION

- Connectez-vous sur le serveur de **PLSCORP** et prenez-en le contrôle.
- Identifiez les problèmes et proposez une solution pour chacun d'entre eux.
- Trouvez les informations sur les employés.
- Mettez en œuvre vos recommandations.
- Effacez vos traces.

La machine « esi-hack » est disponible à l'adresse « 51.91.145.114 » avec les identifiants esicorp : esirem.

EMPLOYEES

Fiches des employés à compléter

Max



Login _____

Mot de passe _____

Date de naissance _____

Numéro de téléphone _____

Adresse mail _____

Maëlys



Login _____

Mot de passe _____

Date de naissance _____

Numéro de téléphone _____

Adresse mail _____

TIPS

Les commandes suivantes vous sont données à titre indicatif et ne sont pas classées par ordre chronologique de nécessité.

Commandes Shell

Activer un module Apache

```
a2enmod module_name
```

Connexion à distance à une base de données

```
mariadb -h hostname -u username -p
```

Désactiver un compte utilisateur

```
chsh -s /sbin/nologin
```

Déplacer un fichier

```
mv path_of_the_file_to_move destination_path
```

Modifier les droits d'accès à un fichier

```
chmod xxx file_name
```

Afficher l'historique des commandes

```
history
```

Supprimer l'historique des commandes

```
history -c
```

Interdire les connexions à distance à une base de données MariaDB

1. Editez le fichier `/etc/mysql/mariadb.conf.d/50-server.cnf`
2. Indiquez « 127.0.0.1 » comme valeur pour le champ « bind-address »
3. Enregistrez
4. Redémarrez le service « mariadb »

FileZilla

Pour initier une connexion SFTP avec FileZilla :

1. Ouvrez le gestionnaire de sites
2. Créez un nouveau site
3. Sélectionnez le protocole SFTP – SSH File Transfer Protocol
4. Saisissez les informations de connexion
5. Cliquez sur Connexion

Commandes SQL (MariaDB)

Lister les bases de données accessibles

```
SHOW DATABASES;
```

Utiliser une base de données

```
USE db_name;
```

Lister les table présentes dans une base de données

```
SHOW TABLES;
```

Afficher le contenu d'une table

```
SELECT * FROM table_name;
```

Modifier le mot de passe d'un utilisateur

```
UPDATE table_name SET password=PASSWORD('new_password') WHERE  
user='user_name';
```

Supprimer un utilisateur

```
DROP USER user_name;
```

Supprimer les droits d'un utilisateur sur une base de données

```
REVOKE GRANT PRIVILEGES ON db_name.* FROM user_name;
```