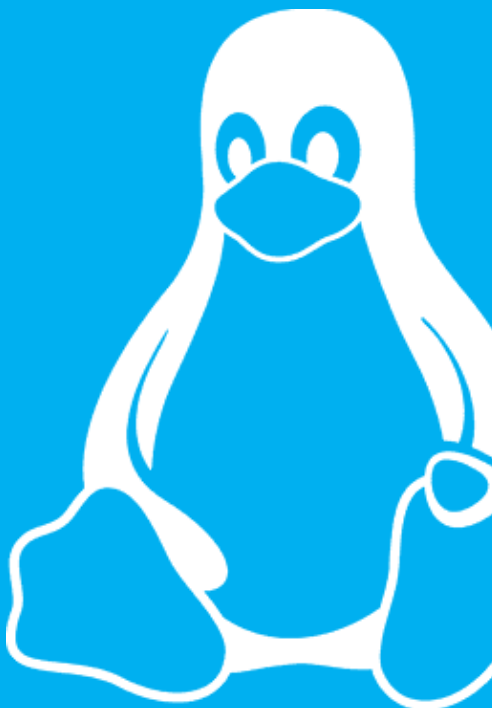


SOUTIEN LINUX

TP 3 – Hacker army !



OBJECTIFS

- Identifiez et corrigez 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. 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 « esihack » est disponible à l'adresse « 57.128.105.207 » avec les identifiants esicorp : esirem.

TIPS

ACTIVER UN MODULE APACHE

```
$ a2enmod [module_name]
```

CONNEXION A DISTANCE A UNE BASE DE DONNEES

```
$ mariadb -h [hostname] -u [username] -p
```

LISTER LES BASE DE DONNEES ACCESSIBLES

```
mariadb SHOW DATABASES ;
```

UTILISER UNE BASE DE DONNEES

```
mariadb USE [db_name] ;
```

LISTER LES TABLE PRESENTES DANS UNE BASE DE DONNEES

```
mariadb SHOW TABLES ;
```

AFFICHER LE CONTENU D'UNE TABLE

```
mariadb SELECT [* | [field_name1, fieldname_2, ...]] FROM [table_name] ;
```

MODIFIER LE MOT DE PASSE D'UN UTILISATEUR

```
mariadb UPDATE [table_name] SET passowrd=PASSWORD([new_password]) WHERE user='[user_name]' ;
```

SUPPRIMER UN UTILISATEUR

```
mariadb DROP USER [user_name] ;
```

SUPPRIMER LES DROITS D'UN UTILISATEUR SUR UNE BASE DE DONNEES

```
mariadb REVOKE GRANT PRIVILIEGES ON [db_name].* FROM [user_name] ;
```

DESACTIVER UN COMPTE UTILISATEUR

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

DEPLACER UN FICHIER

```
$ mv [path_of_file_to_move] [destination_path]
```

MODIFIER LES DROITS D'ACCES A UN FICHIER

```
$ chmod [xxx] [file_name]
```

AFFICHER L'HISTORIQUE DES COMMANDES

```
$ history
```

SUPPRIMER L'HISTORIQUE DES COMMANDES

```
$ history -c
```

INTERDIRE LES CONNEXIONS A DISTANCE A UNE BASE DE DONNEES MARIADB

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

ANNEXES

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 _____