Groupe 2 :

Crenier Amaury

Castermane Robin

Cotton Victor

Référent :

Van Den Schrieck V.

Système et réseau

WoodyToys

Rapport sécurité

1. Sécuriser un VPS

Attention à la formulation de phrases et aussi au copié collé ! (Même texte sur un site)

1.1 Objectif

Aucun protocole de sécurité n'est implémenté nativement lorsque vous commandez votre VPS. Il est donc nécessaire de sécuriser votre machine.

1.2 Prérequis

Être connecté en SSH à votre VPS (accès en root).

1.3 En pratique

- Mettre à jour le système :

Les mises à jour de paquets sont très souvent effectuées pour des raisons de sécurité. Cela permet de profiter des corrections des failles de sécurité, il est donc nécessaire d'effectuer cette opération régulièrement.

    - 2 étapes :
        - apt-get update
        - apt-get upgrade

- Modifier le port d'écoute par défaut du service SSH :

L'écoute est par défaut définie sur le port 22. La plupart des tentatives de piratage sont donc de cibler par défaut le port 22. Afin de leur compliquer la tâche il est important de modifier son paramétrage.

- Création d'un utilisateur avec des droits restreints :

Permet de ne pas être directement connecté avec l'utilisateur Root lors de la connexion au VPS.

Créez un nouvel utilisateur grâce à la commande suivante :

    - adduser nomUtilisateur

- Désactiver l'accès au VPS pour l'utilisateur « root » :

Permet de limiter l'accès au compte root car celui-ci possède des droits plus élevés sur votre système ainsi que la possibilité d'effectuer des opérations irréversibles.

- Installation et configuration de Fail2Ban :

Permet de prévenir contre les intrusions, de bloquer les adresses IP inconnues qui tentent de pénétrer dans le système.

2. Serveur DNS

Utilisation de DNSSsec ainsi que l'utilisation d'un serveur proxy. Celui-ci vérifiera la validité des échanges. Il aura donc un rôle de filtre et de serveur cash.

3. Serveur Web

Utilisation du protocole HTTPS port 443 (prochainement).

4. Serveur Base de Donnée

5. Infrastructure du client

Nous utilisons un Firewall qui se trouvera au cœur du schéma réseau, celui-ci filtrera les échanges avec le monde extérieur et pourra donc filtrer les menaces.

Exemple de différentes utilisations qui seront protégés :

- Infiltration à la boîte mail
- Accès à la base de données
- Sécuriser les serveurs