Groupe 2 :

Crenier Amaury

Castermane Robin

Cotton Victor

Référent :

Van Den Schrieck V.

Système et réseau

WoodyToys

Rapport sécurité

1. Sécuriser un VPS

Lorsque vous commandez votre VPS, aucun protocole de sécurité n'est implémenté nativement. Voici donc quelque commande/pratique à effectuer avant de mettre nos services respectifs en place sur ceux-ci.

Premièrement accédez à votre VPS en tant que root (connexion SSH nécessaire).

Pour des raisons de sécurité vous allez ensuite mettre à jour le système en 2 étapes :

- apt-get update
- apt-get upgrade

Après cela la modification du numéro de port peut être changé, étant donné que les tentatives de piratages cible par défaut le port 22, il pourrait être plus judicieux de le changer.

Une autre étape importante est de créer un utilisateur avec des droits restreints. L'accès direct au root lors de la connexion au VPS n'est pas recommandé en cas de mauvaise manipulation, certaines pourrait être irréversibles.

- adduser nomUtilisateur

Par la suite vous pouvez donc désactiver l'accès au VPS pour l'utilisateur « root ».

En dernier lieu, afin de prévenir contre certaines instruisons comme bloquer les adresses IP inconnues tentant de rentrer dans le système, l'installation/configuration de Fail2Ban est nécessaire.

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

Source :

https://docs.ovh.com/fr/vps/conseils-securisation-vps/