

# Rapport Sécurité

Groupe 7

Crompton Glenn, Hassaine Celia, Foureau Emmanuel

## 1. La liste des risques encourus par notre VPS et notre infrastructure Docker

- piratage de données

  - Serveur OVH

  - Mot de passe

  - informations de la base de données

  - ...

- Serveur qui plante et par conséquent, plus d'accès possible.

- Mail : Un manque de sécurité au niveau du service de messagerie peut engendrer la réception de nombreux spams.



## 2. Contre-mesures mises en place

### a. Authentification par clé

Nous avons toujours utilisé le système d'authentification par mot de passe jusqu'à présent. Cependant, il est également possible de s'identifier via une clé qu'on génère grâce à la ligne de commande

```
ssh-keygen
```

Grâce à ça, le VPS sera accessible uniquement par les personnes qui auront la paire de clé correspondant à ce que le serveur possède.

### b. Fail2ban

Installer et configurer le paquet Fail2ban

Fail2ban est un framework de prévention. il est capable de bannir pour une durée à déterminer les adresses IP qui auront obtenues un nombre (à paramétrer) d'échecs lors de l'authentification à l'un des daemons installés sur votre serveur. Ce paquet est recommandé, voire indispensable, pour nous prémunir contre toutes tentatives de force brute sur nos services.

L'installation de ce paquet s'effectue avec la commande suivante :

```
apt-get install fail2ban
```

Une fois le paquet installé, il a fallu modifier le fichier de configuration de ce dernier pour l'adapter au nôtre. Avant toute modification, il nous a été recommandé de faire une sauvegarde de ce fichier en tapant la commande suivante :

```
cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.conf.backup
```

Nous avons apporté nos modifications sur le fichier :

```
nano /etc/fail2ban/jail.conf
```

Dans ce dossier, nous avons ajouté les lignes suivantes pour créer une "prison":

```
[ssh]
enabled = true
port    = ssh
filter  = sshd
logpath = /var/log/auth.log
maxretry = 6
```

Une fois l'opération terminée, nous avons dû redémarrer le service à l'aide de cette commande :

```
/etc/init.d/fail2ban restart
```

Au niveau des règles, nous avons laissé les règles par défaut.

### c. Firewall

#### Configurer le Firewall Network d'OVH

OVH vous propose un pare-feu à l'entrée de l'infrastructure appelé le Firewall Network. Sa mise en place et sa configuration permettent le blocage des protocoles avant même leur arrivée sur notre serveur.

Il est possible d'activer le firewall et de le configurer par nous-mêmes.

Au niveau des règles, nous n'avons implémenté aucune nouvelle règle et nous nous sommes contentés des paramètres par défaut.

### d. Bloquer l'accès en root et donner toutes les permissions à d'autres utilisateurs

Il est plus sûr de bloquer sudo étant donné qu'il est créé par défaut sur toutes les machines linux.

Tout d'abord, on crée un nouvel utilisateur grâce à la commande

```
Adduser <username>
```

Ensuite, on lui donne accès à tout avec la commande

```
usermod -aG sudo <username>
```

Enfin, on va modifier le fichier "/etc/ssh/sshd\_config" et plus précisément, la ligne "PermitRootLogin yes" en "PermitRootLogin no". Enfin, on redémarre le service SSH avec la commande

```
apt-get update
apt-get upgrade
```

`service ssh restart`

### 3. Liste des risques encourus par chacun des services

#### a. Web

##### i. Risques

- Interception de données privées : lors d'une transaction en ligne, les numéros de cartes bancaires peuvent être volés.
- les données ne sont pas cryptées.

##### ii. Contre-mesure

Mise en place d'un certificat SSL: est la technologie de sécurité standard utilisée pour établir un lien crypté entre un serveur Web et un navigateur. Il crée un canal sécurisé entre deux machines communiquant sur Internet ou un réseau interne. Ce lien garantit que toutes les données transmises entre le serveur Web et les navigateurs restent privées et intégrales. SSL est une norme de l'industrie et est utilisée par des millions de sites Web pour la protection de leurs transactions en ligne avec leurs clients.

#### b. DNS

##### i. Risques

- Interception de paquets : l'auteur modifie alors le paquet pour, par exemple, falsifier la réponse.
- Corruption des données du serveur : pour faire du cache poisoning ou la mise en avant d'un service commercial.
- Dénier de service : généralement dû à une surcharge de serveur.

##### ii. Contre-mesure

Une solution possible est DNSSEC. DNSSEC est un protocole de sécurité qui permet la signature cryptographique des enregistrements DNS. La sécurité peut également être assurée grâce à une architecture appropriée. Pour qu'une architecture DNS soit considérée comme sécurisée, il faut que les serveurs soient à la bonne place. Par exemple, les se