

Rapport de sécurité V3

Dans la mise en place de services réseaux, il faut prendre en considération les différents risques encourus par les infrastructures mises en contact avec Internet. Voici les problèmes courants et la résolution mise en place pour lutter contre ceux-ci.

Les VPS et l'infrastructure Docker

Risques

- Attaque en force (Bruteforce) de tout type (par dictionnaire, force pur, ...) dans le but de trouver les identifiants de connexion.
- Interceptions des identifiants et des mots de passes si ceux-ci sont faibles ou peu protégés.
- Attaque par le conteneur (pour Docker). Il y a plusieurs failles dans certaines implémentations de conteneurs.

Résolutions

- Installation de Fail2Ban qui permet de limiter le nombre d'essai pour se connecter (avec bannissement temporaire de l'adresse qui essaye de se connecter en cas d'échec répétés.
- Changements des identifiants au départ puis configuration pour une communication en ssh + mise en place de groupe d'utilisateur et d'accès privilégiés, suppression du root user.
- Bonne implémentation des conteneurs et mise-à-jour permanente.

Configurations de base

*est-ce réellement très sécurisée d'exposer les configs ?

Les différents services déployés

*à diviser par services peut-être ?

Risques

- Attaque de la base de données pour modifier, supprimer, ajouter des données et ainsi corrompre son intégrité.
- Attaque par Phishing (mail frauduleux).
- Deny of Service sur les sites Webs.
- Attaque Man in the Middle : hacking du DNS et trafic passant du coup par un tiers frauduleux.

Résolutions

- Mise en place d'une DMZ protégée par un Dual Firewall (protégeant ainsi les services exposés en externe.
- Infrastructure réfléchie pour mettre en externes seulement les services qui ont besoin de l'être, privilégié l'interne.
- Configuration de la base de données pour n'accepter que certaines requêtes.

Configurations de base

Nous avons mis en place Fail2Ban sur tous les VPS afin de protéger VPS de la méthode Brute force et nous avons aussi mis dans la whitelist nos adresse IP respective afin de ne pas s'auto-ban.

Nous avons laissé en place le pare-feu du VPS par défaut.

Nous avons mis en place le SOA externe afin que les personnes extérieures à l'entreprise ne puissent pas accéder aux données internes.

Les connexions en ssh de chaque user sont mise en place.

Nous avons un pare-feu qui ne comporte que les fonctionnalités de bases.

L'utilisateur root est supprimé.