WoodyToys - Analyse de sécurité n°1

EPHEC - Groupe 13

Melvin Campos Casares, Guillaume Vanden Herrewegen,
Hubert Van De Walle

14 mars 2019

Analyse de sécurité n°1

VPS & Docker

Risques encourus

Les risques encourus étaient le piratage de nos VPS.

Par le VPS

Nous avons commencé par changer le mot de passe d'accès à nos VPS. Nous avons ensuite sécurisé l'accès à notre VPS avec SSH. Cet accès est sécurisé car il utilise une clé unique par machine pouvant se connecter. En plus de cette clé, il faut entrer une pass-phrase pour pouvoir s'y connecter.

Nous comptons également mettre un place "Fail2Ban" pour éviter toutes tentatives de connexion par brutforce.

Par l'infrastructure Docker

Aucun risque encouru pour l'infrastructure Docker étant donné qu'à l'heure actuelle, il n'y en a aucune.

Contre-mesures mises en place

Nous avons mis en place l'authentification par clé et, par conséquent, désactivé l'authentification par mot de passe. De plus, le compte `root` à directement eu un changement de mot de passe par un nouveau à chiffrement fort. Depuis la mise en place de la connexion par clé, le compte `root` n'est plus accessible de manière externe.

Nous comptons mettre en place "Fail2Ban" incessamment sous peu.

Services

Aucun risque encouru pour les services étant donné qu'à l'heure actuelle, il n'y a aucun service réellement mis en place. Les seuls services mis en place sont à l'heure actuel désactivé.

Risques encourus

Par chacun des services déployés

Au niveau intégrité

Au niveau confidentialité

Au niveau disponibilité du service

Contre-mesures

Proposition

Mise en place