|  |  |
| --- | --- |
| **FIEDORCZUCK Dominik**  **MIRICA Constantin**  **SHATSKIY Filipp** | **Coordinateur : VAN DEN SCHRIECK Virginie**  **E.P.H.E.C. Louvain-la-Neuve**  **Groupe 20 - 2TL2**  **16.05.2018** |

Rapport Sécurité

# **Sécurité VPS**

## **Failles envisagées**

Suite à notre expérience, nous avons envisagé différents points pouvant affecter le bon fonctionnement de nos services :

1. La découverte des failles
2. Trop de droits pour certains utilisateurs
3. L’accès au compte root via SSH
4. La connexion par un simple mot de passe aux différents comptes
5. La découverte de nos clés par « brute force »

## **Solutions implémentées**

Afin de résoudre ces problèmes, nous avons mis en place une série de systèmes destinés à remédier à ces failles :

1. Mises à jour systématiques de Ubuntu
2. Bien configurer les droits des différents utilisateurs
3. Couper l’accès au compte root via SSH
4. Nous avons activé une connexion par clé SSH et avons coupé l’accès par mot de passe
5. Nous avons utilisé la méthode Fail2Ban, qui empêche les attaques de types brute force et qui nous envoie des notifications par mail des attaques

# **Sécurité Web**

Pour une sécurité optimale mais aussi par nécessité, nous avons utilisé le certificat HTTPS.

# **Sécurité DNS**

Pour vérifier les connexions mais aussi les essais de connexion sur le serveur, nous envisageons l’utilisation d’une extension de Fail2Ban. Nous comptons aussi ajouter DNSsec pour une meilleure protection.

# **Sécurité Mail**

Un certificat SSL est mis en place, et il serait également judicieux d’utiliser un mot de passe crypté et non pas « plain text ».

# **Sécurité VOIP**

En cours d’analyse.

Pour Fail2Ban, sur les 3 VPS nous les avons réglés pour bloquer l’adresse IP après 3 essais non réussis de connexion. L’adresse IP est débloquée après 1h. Un mail est envoyé au propriétaire pour savoir l’adresse IP en question. Nous considérons que 3 fois c’est assez pour se rappeler un mot de passe.