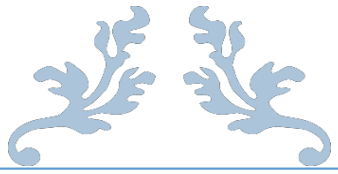
FIEDORCZUCK Dominik
MIRICA Constantin
SHATSKIY Filip

Coordinateur : VAN DEN SCHRIECK Virginie
E.P.H.E.C. Louvain-la-Neuve
Groupe 20 - 2TL2
14.03.2018



Administration Système
WoodyToys - Rapport Sécurité

FIEDORCZUCK Dominik
MIRICA Constantin
SHATSKIY Filip

Coordinateur : VAN DEN SCHRIECK Virginie
E.P.H.E.C. Louvain-la-Neuve
Groupe 20 - 2TL2
14.03.2018

Table des matières

Sécurité VPS *3*

Failles envisagées 3

Solutions implémentées 3

Sécurité Web *3*

Sécurité DNS *3*

FIEDORCZUCK Dominik
MIRICA Constantin
SHATSKIY Filip

Coordinateur : VAN DEN SCHRIECK Virginie
E.P.H.E.C. Louvain-la-Neuve
Groupe 20 - 2TL2
14.03.2018

Sécurité VPS

Failles envisagées

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

1. La découverte des failles
2. Trop des 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

Pour résoudre ces problèmes nous avons mis en place toute une série de systèmes 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 nous 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

La meilleure sécurité, mais aussi une nécessité, nous avons utilisé le certificat HTTPS.

Sécurité DNS

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