Rapport - Analyse de sécurité
2Tl2 - Groupe 3

Louis Arys Brogniet Geoffrey Martin Pardeans
Jean-Michael Tang

11 mai 2020

1 Introduction

Ce rapport est destiné à lister les risques ainsi que les solutions apportées à ces risques de l'entreprise WoodyToys tant au niveau infrastructure de celle-ci mais aussi du prototype que nous fournissons.

Mission 2 :

2 Risques de l'infrastructure réseau

- `Les VPS :` Les plus grands risques ou failles qui puissent survenir sur nos VPS sont l'accès à Root en ssh qui est vivement déconseillé, le brute force qui permetra de décourvrir nos mots de passe et les droits trop présents pour les utilisateurs
- `Le DNS :` Nous écrivons le code permettant de faire fonctionner le logiciel sans Docker. Une fois que le code est fonctionnel, nous écrivons un **Dockerfile**, permettant d'installer/copier les fichiers de configuration nécessaire dans une nouvelle image Docker. Nous testons ensuite le bon fonctionnement du conteneur, et écrivons des scripts permettant de le déployer automatiquement. Nous faisons des tests sur le conteneur pour s'assurer qu'il fonctionne correctement. Une fois un conteneur fonctionnel, nous `pushons` l'image de celui-ci sur notre **Docker Hub**.
- `Déployement d'un nouveau conteneur :` Pour déployer un conteneur sur un VPS, nous `pullons` l'image de notre **Docker Hub**(ou nous la construisons localement via notre projet Github), puis nous le déployons à l'aide de scripts écrit précédemment, et permettant un déployement automatique. Nous testons à nouveau le bon fonctionnement du conteneur, puis nous inspectons notre structure Docker pour vérifier que tout fonctionne correctement.
- `Update d'un conteneur :` Nous faisons les changements en local, en manipulant les fichiers de configuration de l'image. Une fois les changements effectuer, nous testons le conteneur sur un réseau local. Si tout est correct, nous pushons la nouvelle image sur notre **Docker Hub**.

3 Les solutions aux risques

Le prototype peut conduire à plusieurs gros risques tant au niveau du VPS qu'au niveau des Dockers utilisés et empruntés sur le WEB.

Les risques du VPS sont les suivants :

- Les performances d'un VPS n'atteignent pas celles d'un véritable serveur. Généralement, les fournisseurs des VPS limitent les performances des serveurs afin de maximiser le nombre d'unité qu'un serveur physique peut contenir. Ce qui rejoint le risque de la disponibilité expliqué ci-dessus.

- Les VPS sont généralement des virtualisation du serveur, ce qui permet de créer un isolation entre chaque serveur. Mais le risque zéro n'existe pas et il est conseillé d'éviter les environnements partagés.

Les risques au niveau du Docker sont simplement l'exécution de code, la confiance des Docker mis à disposition ainsi que le déni de service. Afin de contrer ces risques, il faut prévenir tout cela en utilisant des sources de confiance ou alors utiliser des outils qui pourront analyser notre Docker.

Et enfin nous pourrons aussi privilégier l'utilisation d'un Fail2ban qui va analyser le nombre de tentative d'accès et bloquer l'utilisateur après 3 tentatives par exemple grâce à son adresse IP. Cela veut dire qu'avec l'adresse utilisée pour se connecter, l'utilisateur ne pourra plus essayer de se connecter pendant un moment prédéfinis.

Mission 3 : Du à beaucoup d'erreurs dans le précédent rapport, nous avons décidé de refaire entierement le rapport, d'où l'indication mission 2 et mission 3. Lors du rapport final, nous retirerons les précédentes missions pour en garder que la version finale.

4 Risques de l'infrastructure réseau

- `Les VPS :` *Les plus grands risques ou failles qui puissent survenir sur nos VPS sont l'accès à Root en ssh qui est vivement déconseillé, le brute force qui permetra de découvrir nos mots de passe et les droits trop présents pour les utilisateurs*
- `Le DNS :` *Le cache-poisonning est un grand risque sur nos DNS, c'est à dire une corruption d'envoie de données via une ardesse ip falsifiée. Mais il y a également les attaques DDos, qui, sont but, est de bloquer le fonctionnement de la ressource. Et enfin les messages non authentifié comme les attaques de type Man in the Middle*
- `Le mail :` *Les spam et les fishings sont les dangers majeurs pour nos mails. Envoyer un grand nombre de mail en peu de temps peut bloquer une boite mail et envoyer des emails avec le domaine de la société pour tromper les clients et non clients en les dirigeants vers un formulaire dans le but de leurs soutirer des informations.*
- `VOIP :` *Pour cette partie, les risques sont nombreux comme par exemple la découverte du mot de passe par brute force (courant sur SIP), usurpation d'identité, l'écoute, les spams, les abus d'utilisation et encore plus.*
- `La base de données :` *Le risque sur la base de données est le changement d'une donnée ou d'une table à cause d'une mauvaise sécurité de cette base de données.*

5 Les solutions aux risques

- *`Les VPS :` Nous avons enlevé l'accès à ROOT et nous avons supprimer une connection via mot de passe et remplacé par une passphrase et clé ssh via keygen. Nous avons aussi installé Fail2ban qui va exclure après 5 tentatives de connexion l'adresse ip qui essaye de se connecter.*
- *`Le DNS :` Nous avons différencier le DNS externe et interne afin d'avoir une architecture sécurisé.*
- *`Le mail :` Nous avons mis en place une sécurité StartTLS, une mise en place d'un outil anti-spam et d'un mot de passe crypté et non plein est en construction.*
- *`VOIP :` Nous mettrons en place plusieurs sécurisation afin d'éviter un grand nombre de risque mais tout d'abord une mise en place de Fail2Ban pour les connexions sera important, nous mettrons une limite à trois connexions et préviendront par mail le propriétaire de la tentative de connexion. Nous allons également mettre en place un pare-feu UFW qui va tout simplement simplifié la création des ip-tables .*
- *`La base de données :` Un mot de passe sécurisé est mis en place.*
- *`Web :` Une mise en place d'HTTPS en cours sur les sites.*