WoodyToys - Analyse de sécurité

EPHEC - Groupe 13

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

6 juin 2019

Analyse de sécurité

1. VPS & Docker

1.1. Risques encourus

Ils existent de nombreux risques. Les principaux risques portent sur la confidentialité, la disponibilité et l'intégrité. Nos services doivent également être opérationnels 24 heures sur 24.

1.1.1. Par le VPS

- Usurpation d'identité du serveur
- Attaque sur le mot de passe
- Surcharge du serveur

1.1.2. Par Docker

- Attaque sur le conteneur pour avoir accès à la machine hôte.
- Attaque via la machine hôte vers le conteneur.
- Attaque via le réseau pour avoir accès à la machine hôte.

Certains de nos services fonctionnants avec Docker possèdent des éléments devant rester secrets. En utilisant un hub pour y mettre nos images crées, nous exposons certaines données confidentielles à la vue de tous.

1.2. Contre-mesures mises en place

1.2.1. Pour le VPS

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 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 avons également mis en place `fail2ban` qui empêche toute tentative d'attaque DOS. Cette sécurité va bannir une adresse IP lorsque celle-ci réalise trop de tentatives de connexion refusées. La règle utilisée est de 10 tentatives en 2 minutes maximum, 20 minutes de bannissement de l'adresse IP. De plus, la protection contre l'attaque DDOS et la récidive est également suivie par `fail2ban`.

Nous gardons également notre VPS à jour aussi souvent que possible.

1.2.2. Pour Docker

Nous avons préféré construire nos images en local le temps que nous puissions mettre en place la sécurité dans le conteneur et par la suite les construire via un hub, ici Dockerhub.

2. Services

2.1. Risques encourus

2.1.1. Par chacun des services déployés

2.1.1.1. DNS

- Attaque de type Man in the Middle
- Réponses falsifiées
- Cache poisoning
- Mise avant d'un service commercial
- Blocage de certains sites web
- Attaque par Fast Flux.

Le serveur peut être surchargé l'empêchant de répondre aux requêtes.

2.1.1.2. Service Web

- Accès et modification de la base de données

2.1.1.3. Service Mail

- Confidentialité des mails
- Intégrité au niveau de l'envoyeur
- Spam
- Phishing
- Surcharge des serveurs.

2.1.1.4. Service VoIP

- Confidentialité des appels et des messages vocaux
- Usurpation d'identité
- Surcharge des serveurs.

2.1.1.5. Au niveau intégrité Plusieurs de nos services doivent être fiable au niveau de l'intégrité.

Au niveau du service mail, un utilisateur peut recevoir un mail croyant être un mail officiel dans le but de voler des données personnelles ou bien d'attaquer le service en question.

Pour VOIP, une personne pourrait se faire passer pour un autre utilisateur dans le but de nuire.

2.1.1.6. Au niveau confidentialité La confidentialité est un point où nous mettons toute notre attention. Chacun des services est étudié afin de trouver une solution pour garantir une confidentialité maximale. Au niveau du service web, nous sommes en train de mettre ne place un certificat SSL qui garantit la confidentialité des données personnelles sur notre site web.

Au niveau du mail, nous sommes occupés à chercher un système de boîtes mails virtuelles afin de garantir à chaque utilisateur une confidentialité au niveau de ses mails. Nous cherchons également à sécuriser la base de données concernant les identifiants de chaque utilisateur.

Au niveau du service VOIP, une connexion par mot de passe fort est demandée pour son utilisation.

2.1.1.6. Au niveau disponibilité du service Nos serveurs peuvent être la cible d'attaques visant notamment à surcharger le serveur pour le rendre inutilisable.

2.2. Contre-mesures

2.2.1. Proposition

2.2.1.1. Sécurisation du DNS

- Utiliser la dernière version de BIND.
- DNSSec permet de crypter les enregistrements du DNS.
- DNS interne et externe pour différencier les accès internes et externes de l'entreprise.

2.2.1.2. Sécurisation Web

- Utilisation d'un certificat SSL

2.2.1.3. Sécurisation Mail

- Filtre anti-spam
- Chiffer les emails
- Connexion au compte via mot de passe chiffré fort
- Utilisation d'un proxie mail en DMZ.

2.2.1.4. Sécurisation VOIP

- Connexion au compte via mot de passe chiffré fort

2.2.2. Mise en place

2.2.2.1. Sécurisation du DNS

- Mise en place d'un DNS interne et un DNS externe.

2.2.2.2. Sécurisation Web Afin de garantir une sécurité au niveau de notre infrastructure web, nous avons mis en place un certificat SSL pour que nos sites web soient sécurisé. Par le biais de ce certificat, nos sites internet passent en HTTPS avec certificat signé, prouvant la sécurisation et le respect de la confidentialité.

Pour ce faire, nous avons choisi Let's Encrypt, une autorité de certification gratuite, automatisée, et fourni par le Internet Security Research Group (ISRG).

Le choix de Let's Encrypt, plutôt que d'un certificat auto-signé est simple :

- Le renouvellement de Let's Encrypt est automatique,
- Les certificats générés sont de confiance alors que les certificats auto-signés doivent être manuellement marqué comme de confiance,
- La génération du certificat est aisée et rapide via Let's Encrypt.

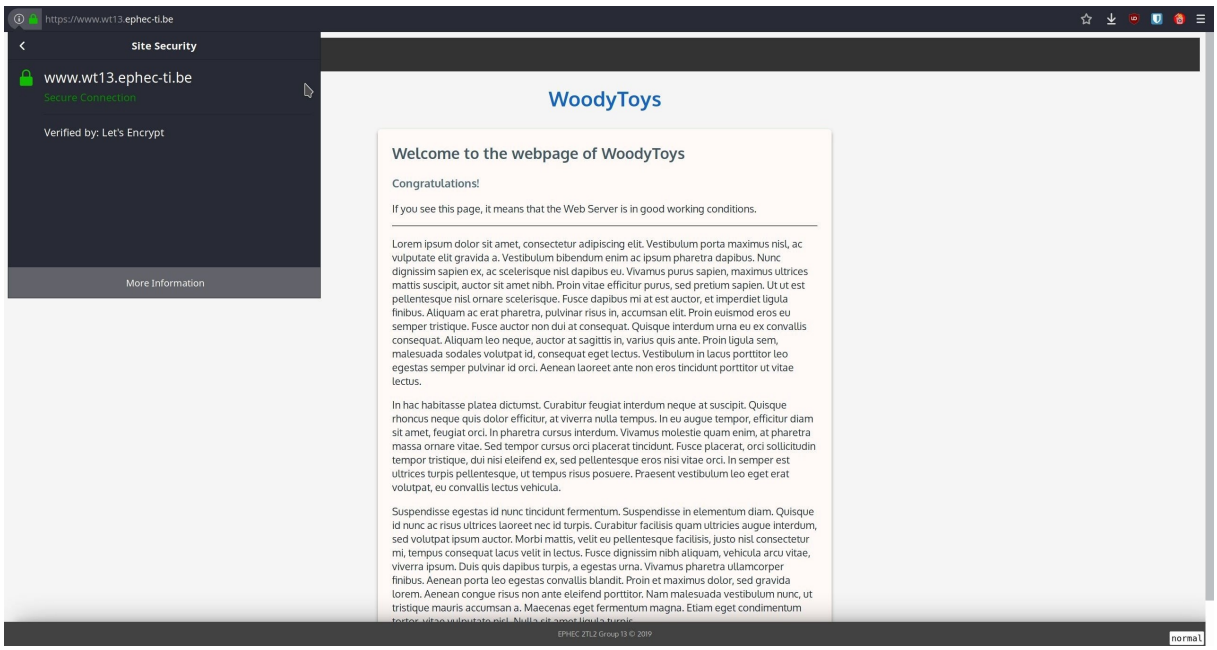

Figure 1: Preuve de la mise en place du certificat Let's Encrypt et de son bon fonctionnement

2.2.2.3. Sécurisation VOIP Nous avons ajouté pour le VoIP une protection supplémentaire afin de maintenir celui-ci opérationnel. La solution utilisée est "fail2ban", où nous avons intégré les protections asterisk-iptables et asterisk-security-tables.

Concrètement, 3 tentatives de connexion maximum sont acceptées avant que l'adresse IP en question soit bannie pour une durée de 24h. La période de renseignement pendant laquelle le log est examiné est de 1h.