Administration Système Groupe 2TL2-9

Rapport Sécurité

G.Lemer A.Nilens F.Janssens

2019 - 2020

Table des matières

1 Etudes des failles de sécurité possibles **1**

2 Sécurité mise en place sur les VPS **1**

3 Sécurisation Globale **1**

4 Choix de la sécurisation des différents composants **1**
4.1 Serveur Web 1
4.2 Serveur de base de donnée 1
4.3 Serveur DNS 2
4.4 Serveur MAIL 2
4.5 Serveur VOIP 2

1 Etudes des failles de sécurité possibles

Pour commencer, nous avons notre réseau entier à sécuriser et éviter les attaques depuis l'extérieur aussi bien sur nos serveurs que sur les équipements internes a l'entreprise.

Pour le DNS, différents risques sont encourus, notamment :

1. l'interception des paquets
2. la falsification des paquets
3. la corruption des paquets
4. les attaques DDOS

Pour le serveur Mail :

1. Faille de Confidentialité
2. Ruptures d'intégrité
3. le SPAM
4. Le Phishing

2 Sécurité mise en place sur les VPS

Afin de sécuriser l'accès à notre VPS, il nous est nécessaire d'utiliser SSH dès son lancement. Si nous n'utilisons pas des connexions sécurisées, nous prenons le risque de nous faire pirater et de perdre l'entièreté de nos données.

Nous avons également mis en place le système, Fail2Ban. Afin de limiter au mieux les attaques de brut, force. Une tentative de connexion échouée a 5 reprises bloquera complètement l'utilisateur qui essaye de ce connecter a notre vps.

Enfin UFW permet de gérer les ports accessibles de notre VPS, ce qui permet de limiter les accès depuis l'extérieur aux ports voulus.

Et pour finir, le service UFW (Uncomplicated FireWall) est mis en place afin de gérer l'accès aux ports de nos vps et de restreindre l'accès a ceux-ci.

3 Sécurisation Globale

Pour commencer, la mise en place d'une zone DMZ va permettre de maintenir en sécurité l'ensemble des installations interne de l'entreprise. Les serveurs et autres composant devant être joignables depuis l'extérieur, et ne devant pas être joignables en local, sera mis dans ce sous-réseau DMZ protégé par un pare-feu. Ce pare-feu bloquera donc l'accès au réseau local pour garantir ça sécurité.

4 Choix de la sécurisation des différents composants

4.1 Serveur Web

Nous utiliserons HTTPS pour sécuriser notre serveur web, afin de garantir la sécurité de ceux-ci. Le serveur interne fait également l'objet de règles particulières limitant son accès aux adresses IP du réseau interne à l'entreprise.

4.2 Serveur de base de donnée

— l'accès au serveur de base de données ce faire par un login password, et ces accès sont restreins au serveur b2b

— l'accès a la base de données ne peut ce faire que depuis un réseau privé reliant le serveur b2b et la base de données. Empêchant ainsi toute modification depuis un accès distant non autorisé.

4.3 Serveur DNS

Sécurisation du DNS par la mise en place du protocole DNSSEC afin de limiter les problèmes de sécurités en lien avec le serveur DNS.

De plus, nous utilisons une infrastructure comprenant un serveur DNS en DMZ pour le contact avec le réseau extérieur, ainsi qu'un serveur Proxy relaient l'information au réseau interne de l'entreprise. Cela permet d'isoler au mieux les 2 réseaux et de maintenir la sécurité visa-vis des paquets au sein de notre entreprise, mais aussi de maintenir le réseau fonctionnel en cas d'attaque DDOS sur le DNS extérieur qui est situé en DMZ.

4.4 Serveur MAIL

Nous avons mis en place Fail2Ban et IPtables pour contrôler les ports de connexion. Nous avons également une sécurisation des comptes utilisateurs par cryptage de mot de passe dans la base de données. Tous les nouveaux comptes utilisateurs ajoutés dans la base de données, passe par un cryptage de mot de passe. Quand les utilisateurs veulent se connecter à leur boîte mail, il se connecte avec un login et un mot de passe, le mot de passe est décrypté au moment de la connexion. De plus, un certificat électronique SLL/TLS a été mis en place pour contrôler l'identité et crypter les échanges. Nous utilisons la norme d'authentification DKIM. Elle constitue une protection efficace contre le spam et l'hameçonnage. En effet, DKIM fonctionne par signature cryptographique. Enfin, nous avons également configuré DMARC, SPF (SenderID) et Spamassassin avec Postfix pour identifier les spams.

4.5 Serveur VOIP

Nous utilisons fail2ban ainsi que UFW afin de limiter les tests de connexion à notre service Asterisk, les adresses se connectant trop de fois sans succès sont automatiquement bannies, et les ports non nécessaires ont été fermés. Cela devrait être mis en place en théorie, mais il semble y avoir une faille dans le système qui devra être instiguée. Afin de limiter au maximum les problèmes liés aux attaques SIP, nous avons changé le port par défaut vers le port 6666, ce qui a presque totalement éliminé ces attaques automatiques.