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

Pour commancer, nous avons notre réseau entier a sécuriser et éviter les attaques depuis l'extérieur aussi bien sur nos serveurs que sur les équipement interne a l'entrepise.

Pour le DNS, différentes risques sont éncouru, notament :

1. l'interception des paquets
2. la falsificaton 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 mis 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'entiereté de nos données.

Nous avons également mis en place le system, 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 port voulu.

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

3 Sécurisation Globale

Pour commancer, la mise en place d'une zone DMZ vas permettre de maintenir en sécurité l'ensemble des instalations interne de l'entreprise. Les serveurs et autres composant devant être joignable depuis l'extérieur, et ne devant pas être joignable en local, seront mis dans ce sous-réseau DMZ protégé par un pare-feu. Ce pare-feu bloquera donc l'accès au réseau local pour garantir ca sécuritée.

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,

4.2 Serveur de base de donnée

— l'accès au serveur de base de donnée ce faire par un login password, et ces accès sont restrain au serveur b2b
— *l'accès a la base de donnée ne peut ce faire que depuis un réseau privé reliant le serveur b2b et la base de donnée. Empêchant ainsi toute modifications 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 sécuritées en lien avec le serveur DNS.

Deplus, nous utilisons une infrastucture comprenant un serveur DNS en DMZ pour le contact avec le réseau extérieur, ainsi que un serveur Proxy reléant l'information au réseau interne de l'entreprise. Cela permet d'issoler au mieux les 2 réseau et de mainternir la sécurité vis-a-vis des paquets au seins de notre entrepise, mais aussi de maintenir le réseau fonctionnelle en cas d'attaque DDOS sur le DNS extérieur qui est situé en DMZ.

4.4 Serveur MAIL

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.

4.5 Serveur VOIP

Nous utilisons fail2ban ainsi que UFW afin de limiter les test de connexion a notre service Asterisk, les addresses ce connectant trop de fois sans succes sont automatiquement bannie, et les ports non nécéssaire on été fermé.