LIBER Maxime
VIROUX Nicolas
CONDE Ibrahima

Rapport Sécurité :

Woodytoys

Risque encourus par le VPS

Sans sécurité, il est possible de se faire voler le VPS.

Mesures mise en place contre ces risques

Nous avons mis en place un logiciel qui se nomme Fail2Ban. Celui-ci est utile pour la prévention des intrusions. Nous l'avons utilisé afin qu'il nous envoie un mail à chaque fois qu'il bannit une IP qui a tenté plusieurs fois d'accéder au VPS.

Nous avons également désactivé les identifications par compte root et l'authentification par mot de passe sur nos VPS, actuellement la connexion se fait via clé asymétrique.

En plus de cela, notre site intranet est accessible uniquement à nos employés. Afin d'y parvenir, nous avons utilisé une « access list » dans laquelle on entre les IP des employés concernés.

Risques encourus par les services mis en place

Durant toute la durée de ce projet, nous avons utilisé des containers Docker afin de déployer les services dont nous nous sommes servis. Même si cette technique permet d'isoler les processus et ressources, tout ce qui tourne en root dans un container tournera également en root sur l'hôte. C'est pour cela que nous avons vérifié les vulnérabilités des images que nous avons installé.

Avec l'utilisation de containers Docker, nous avons veillé à séparer chacun de nos services en fonction de la sensibilité des données qu'il contient.

Le service DNS que nous avons mis en place comporte différents risques :

- Interception de paquets
  - Man in the Middle : Ce type d'attaque a pour but d'intercepter les communications entre deux parties sans qu'aucune des deux ne sache que leur canal de communication est infecté et dangereux.
- Corruption de données du serveur
  - Cache poisoning : Cette technique se base sur l'empoisonnement du serveur DNS via des réponse aux requêtes envoyées. Suite à cet empoisonnement, tous les utilisateurs deviennent vulnérables. Ce type d'attaque permet par la suite, d'envoyer les utilisateurs vers des faux sites qui serviront par la suite à une autre technique nommée l'hameçonnage.

Mesures mise en place contre ces risques

Pour ce qui est de la sécurité de notre DNS, nous avons mis en place le protocole DNSSEC qui permet de gérer la protection de données et les enregistrement DNS

A propos de la sécurisation du web, nous avons configuré le certificat SSL pour le serveur Web, nos trois sites sont accessible en HTTPS.

Quant à la sécurisation du serveur mail, nous avons mis en place des certificats STARTLS & SSL/TLS. Ils nous ont été utile afin de sécuriser, fiabiliser nos échanges, vérifier l'identité du serveur et ne plus

avoir à accepter de certificat auto-signé. STARTTLS est le protocole permettant d'améliorer une connexion classique vers une sécurisée en utilisant TLS.

En plus de cela, nous avons utilisé trois normes qui protègeront nos boîtes mails. Celles-ci sont DKIM, SPF et DMARC.

- SPF (Sender Policy Framework) : Limite l'usurpation d'identité en publiant dans les DNS de votre nom de domaine la liste des serveurs, ou plus précisément des adresses IP, qui sont autorisés à envoyer du courrier avec ce domaine.
- DKIM : L'objectif du protocole DKIM n'est pas uniquement de prouver que le nom de domaine n'a pas été usurpé, mais que le message n'a pas été altéré durant sa transmission.
- DMARC : le protocole DMARC permet à l'expéditeur de recevoir les résultats de l'authentification de ses envois.

Dernièrement pour la sécurisation de notre VoIP, nous ne nous sommes pas encore penchés dessus à l'heure actuelle.