11 mai 2020

Haute Ecole Economique et Technique

Projet Administration système et réseau

Rapport Sécurité

Groupe 2TL1-8
Quirynen Gilles, Lambert Maximilien, Gassmann Mathias

Risques de sécurité

OVH met à notre disposition un VPS sans mesures de sécurité préétablies, le travail nous revient donc de s'assurer que nous sommes préparés pour tous les risques qu'il pourrait encourir.

1. Tentatives d'intrusions par des individus extérieurs
2. Attaque par force brute pour trouver les identifiants
3. Tentative d'accès au serveur en root pour effectuer des modifications
4. Exploitation de failles de sécurité sur des VPS non mis à jour

Contre-mesures mises en place :

1. Installation de Fail2Ban pour éviter les intrusions
2. Modifier le mot de passe de root et s'assurer qu'il ne puisse pas modifier le serveur mis en place
3. Mettre en place une authentification sécurisée (clef)
4. S'assurer que le serveur soit à jour et qu'aucune faille de sécurité connue ne persiste.
5. Création d'utilisateurs pour éviter l'utilisation du "root"
6. Mise en place d'un firewall. Seuls les ports nécessaires au bon fonctionnement des différents services implémentés sont ouverts.

Règles Fail2Ban :

Nous avons laissé sur tous les vps les configuration de base de fail2ban à savoir :
10 minutes de bannissement pour l'hôte qui se retrouve dans la prison
10 minutes de "fourchette" dans laquelle l'hôte va pouvoir essayer de se connecter et que notre compteur d'essais va être actif
5 essais maximum d'erreur lors de la connexion

Règles Firewall :

Le firewall utilisé sur nos VPS est UFW. Voici une liste non-exhaustive des différentes règles que nous avons appliqués sur nos VPS :

- VPS de Mathias :
    - Ports ouverts :
        - 22 (ssh)
        - 53 (dns)
        - 80/443 (web)

- VPS de Maximilien :
    - Ports ouverts :
        - 22 (ssh)
        - 25/587 (smtp)
        - 143/993 (imap)
        - 110/995 (pop3)
        - 5060 (voip)

- VPS de Gilles :
    - Ports ouverts :
        - 22 (ssh)
        - 8022 : (web backend)
        - 8070 : (web vitrine)⇒ **uniquement depuis l'adresse IP 51.178.40.70**, afin que le serveur reverse-proxy sur le VPS de Mathias puisse accéder aux sites web externes présent sur le VPS de Gilles.
        - 8080 : (web b2b) ⇒ Idem 8070.

Risques encourus par chacun des services

Web

Les serveurs webs sont régulièrement la cible d'attaques en tout genre par des individus mal intentionnés. Cela pose des risques à la fois aux utilisateurs des services utilisés ainsi qu'aux administrateurs.
On utilise donc des certificats SSL afin de s'assurer de la sécurisation des liens entre le serveur et les utilisateurs.
Les sites sont donc configurés avec l'accès https pour un maximum de sécurité.
Nous avons également mis en place un reverse proxy dans la DMZ qui s'occupe de la redirection vers les sites dans un VPS sécurisé.

DNS

La sécurisation des données envoyé par notre DNS est actuellement compromise. En effet, aucun protocole de sécurité n'a encore été mis en place pour sécuriser l'intégrité des données.

Contre-mesures :

Nous prévoyons de mettre en place le protocole DNSSEC permettant de résoudre des problèmes de sécurité lié au DNS. Celui-ci permettra de protéger les données et les enregistrements DNS de bout en bout.

Mail

Les mécanismes DKIM et SPF sont mis en places sur notre serveur mail et fonctionnels.
Ils constituent une protection efficace contre le spam et l'hameçonnage.

VoIP

Notre serveur Asterisk est régulièrement la cible d'attaques de brute-force par des individus mal intentionnés. Ces individus essayent de nombreuses combinaisons de login / password.
Voici un screenshot provenant du CLI de notre Asterisk :

Contre-mesures :

Adapter notre configuration Fail2Ban afin que notre serveur Asterisk ne puisse plus être la cible d'attaques brute-force.