Mugisha Rodrigue

Administration Système & Réseau : Rapport Sécurité

Failles envisagées :

VPS

1. Trop de droits pour certains utilisateurs
2. L'accès au compte root via SSH
3. La connexion par un simple mot de passe aux différents comptes
4. La découverte de nos clés par « brute force »

Serveur DNS *:*

1. *Cache poisoning : lorsqu'un serveur DNS est obligé d'interroger un autre serveur DNS pour obtenir l'adresse IP d'un nom de domaine faisant l'objet d'une requête*
2. *Attaques DDoS : le but de l'attaque est de bloquer le fonctionnement de la ressource Web (déni de service total)*

Mail *:*

1 *Phishing : Envoyer des mails avec le domaine de l'entreprise « @domaine.be » pour tromper les internautes et la plupart du temps en les dirigeants vers un formulaire où ils complètent leurs informations personnelles*

2 *Spam : envoyer énormément de mails peut bloquer relativement vite une boite mail*

Solutions envisagées :

VPS

1. Mises à jour systématiques de Ubuntu
2. Bien configurer les droits des différents utilisateurs
3. Couper l'accès au compte root via SSH
4. Activer une connexion par clé SSH et couper l'accès par mot de passe. Cette configuration est faite grâce à la commande « ssh-keygen » qui crée une clé publique et privée. Il faut copier la clé publique sur un serveur distant dans le fichier « authorized-keys ». Pour couper l'accès par mot de passe, modification à apporter au niveau du fichier « sshd_config ».
5. Fail2Ban qui empêche les attaques de types brute force, il s'agit d'un framework de prévention contre les intrusions, qui bloque les adresse IP qui se connectent trop de fois. Cette vérification est faite par une quantification du nombre d'échecs de connexion.

Mugisha Rodrigue

Sécurité Web

Pour une sécurité optimale mais aussi par nécessité, le certificat HTTPS est une bonne contre-mesure. Le HTTPS et un protocole qui sert à crypter les communications qui rentre et qui sorte de la page web.