Bouti-Mazouz Samy/Kapri Anish

Check-List Points de sécurité pour serveur

Liste des points de sécurité (Serveur) :

I. Gestion des mots de passe

Il est nécessaire d'établir une « politique » de mot de passe qui doit impérativement être respectée par les utilisateurs du serveur

-Activez l'authentification à deux facteurs.

-N'utilisez pas de mots du dictionnaire ou d'informations personnelles dans les mots de passe.

-Utilisez des mots de passe complexes d'au moins 10 caractères, comprenant des chiffres, des symboles et des signes de ponctuation.

-Ne stockez pas les mots de passe sur les ordinateurs portables, les smartphones ou les tablettes (tout ce qui se vole ou se perd facilement).

-Utilisez un générateur de mot de passe sécurisé pour générer le mot de passe.

-Fixer une date d'expiration pour un mot de passe.

-Ne pas utiliser le même mot de passe pour plusieurs comptes.

II. Mise à jour du serveur

Il est important de mettre à jour son serveur et ceux de façon régulière puisque les mise à jour récente permettent de lutter contre le piratage, la perte/fuite de données.

III. Services inutiles

Il faut pouvoir désactiver voire de supprimer les services qui ne sont pas essentiels à la bonne fonctionnalité du serveur.

IV. Ports

Il est impératif de désactiver les ports inutilisés, voire de modifier certains ports comme le port SSH (22), très connu par les pirates puisqu'il s'agit du port SSH de base et donc ainsi le plus vulnérable.

V. Pare-feu

Un serveur doit avoir un pare-feu car le pare-feu est capable d'empêcher toutes les connexions qui sont non-autorisés vers ou depuis le serveur.

VI. Attaques

Pour davantage de sécurité, il est important de configurer certains outils qui peuvent prémunir le serveur de certains types d'attaques : Attaque par force Brute,

nous pouvons alors configurer l’outil fail2ban qui vérifiera les fichiers logs, détectera les comportements suspects et bloquera les adresses IP des utilisateurs.