Agir contre une intrusion web

Les objectifs de l'attaque

En général, il s'agit de maintenir un accès à distance à des fins malveillantes (utilisation du serveur comme vecteur d'attaque, hacktivisme, vol de données...).

Une intrusion web désigne un accès non autorisé à un serveur web. L'attaquant a potentiellement acquis des privilèges d'administrateur et est libre d'y effectuer les actions qu'il souhaite (modification des données, installation d'une porte dérobée, rebond vers d'autres machines, etc.).

Mesures de prévention et d'investigation

Réduire au maximum les droits liés aux environnements d'exécution des applications

Réaliser **une veille sécurité** et **mettre à jour régulièrement** le système et les applications (voir la fiche « Patch management »)

Réaliser des **sauvegardes régulières** et exporter les journaux vers un dépôt central **pour assurer leur intégrité**

Mettre en place une **politique de mots de passe forte**

Réaliser **des audits de sécurité** et **des scans de vulnérabilité** réguliers

Quelques pistes pour rechercher l'origine de la compromission :

Acquérir les données du système pour investiguer (copie de la mémoire vive et du système et calculer l'empreinte de l'image ; s'il s'agit d'une machine virtuelle, réaliser un snapshot)

Analyser les accès dans les journaux d'événements et **analyser les journaux d'événements** de l'ensemble des composants du système ou de tout serveur ou accès d'administration exposé sur Internet. Attention, si l'attaquant a pu obtenir un accès privilégié, celui-ci a pu effacer l'ensemble de ses traces.

Mesures de réaction

Déconnecter le serveur d'Internet et vérifier qu'il n'y a aucune connexion malveillante en cours (netstat)

Rechercher les failles exploitées (logiciel, configuration, etc…) et **le niveau de privilège acquis par l'attaquant** pour réaliser ses actions

Identifier le moyen d'accès de l'attaquant (webshell, au travers d'un proxy/serveur smtp/serveur dns]) et **rechercher les possibilités de rebond** en analysant les accès aux serveurs sur le même segment réseau

Restaurer le système/service et les données à partir de sauvegardes intègres **en ayant vérifié l'absence de compromission potentielle** (Webshell, backdoor, etc…), **en corrigeant les failles** et **en respectant les bonnes pratiques** (mises à jour de sécurité, moindre privilège, etc…)

Changer tous les mots de passe des accès présents sur le serveur. Sinon l'attaquant peut réutiliser les accès précédemment obtenus.

Surveiller le service durant les jours qui suivent sa remise en production (pare-feu applicatif & IDS & journaux d'évènements)

Déposer plainte auprès des services de police ou de gendarmerie. (Voir la fiche « Réagir à un acte de cybermalveillance »)