Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ

asipsanté
AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

REAGIR A UNE INTRUSION WEB – REFLEXES

QU'EST-CE QU'UN INTRUSION WEB ?

Une intrusion web désigne un accès non autorisé à un serveur web.

OBJECTIFS DE L'ATTAQUE

Les objectifs d'une intrusion web peuvent être multiples. En général, il s'agit d'y pérenniser un accès discret à des fins malveillantes. (e.g : vol de données, utilisation du serveur comme vecteur d'attaque, demande de rançon, défaçage…).

RISQUES

- ➔ **PERTE D'IMAGE**
- ➔ **VOL DE DONNEES**
- ➔ **UTILISATION DU SERVEUR COMME VECTEUR POUR D'AUTRES ATTAQUES**

SYMPTOMES

DECOUVERTE D'UN CODE MALVEILLANT
ENVOI DE SPAMS / REALISATION D'ATTAQUES DEPUIS LE SERVEUR
COMPORTEMENT INHABITUEL, LENTEUR, CHARGE CPU ANORMALE
PAGE D'ACCUEIL MODIFIEE

ORIGINES

- Erreur de configuration / faiblesse de sécurisation
- Via un site vulnérable hébergé sur la même plate-forme
- Mot de passe faible / Faiblesse du système de gestion ou du stockage des mots de passe
- Absence des derniers correctifs de sécurité ou de recommandations de configuration
- Corruption du poste servant à l'administration du site
- Erreur de programmation
- Faille 0day

QUE FAIRE

- **ARRETER LE SERVEUR WEB**
- **AVERTIR LES TECHNICIENS**
- **DEPOSER PLAINTE AUPRES DE LA POLICE OU DE LA GENDARMERIE**

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ

asipsanté
AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

REAGIR A UNE INTRUSION WEB – REFLEXES

GRAVE OU PAS ?

Une intrusion web est critique pour un SI, elle est signe que le serveur est passé aux mains de l'attaquant. Par conséquent, ce dernier est libre d'y effectuer les actions qu'il souhaite (modification des données, installation d'une porte dérobée, rebond vers d'autres machines, etc.).

LES BONNES PRATIQUES

- Installer les correctifs de sécurité du système et des logiciels
- Réaliser des sauvegardes régulières
- Durcir le serveur web
- Mettre en place une politique de mots de passe forte
- Réaliser une veille régulière sur les logiciels utilisés par le serveur
- Réaliser des audits de sécurité et des scans de sécurité réguliers
- Installer un WAF sur le serveur web (Web Application Firewall)
- Exporter les journaux système

RESSOURCES

- Service d'alerte de vulnérabilités
- Les bons réflexes en cas d'intrusion sur un système d'information

REPARER ET ENQUETER

LES PRINCIPALES ETAPES DE L'ENQUETE •

- **Acquérir les données du système: faire une copie de la mémoire vive, faire une copie du système et calculer l'empreinte de l'image; s'il s'agit d'une machine virtuelle, réaliser un snapshot**
- **Déconnecter le système du réseau, réaliser les opérations de sauvegarde des preuves pour investigation, de dépôt de plainte et arrêter le serveur web**
- **Identifier la source de l'intrusion**

La méthode la plus simple pour déterminer la source de l'intrusion d'un serveur web est d'analyser les accès réalisés dans les journaux d'événements. Attention la source de l'intrusion peut être autre que le serveur web (outils d'administration, serveurs d'applications, etc.). Attention, si l'attaquant a pu obtenir un accès privilégié, celui-ci a pu effacer l'ensemble de ses traces. Selon le système d'exploitation, analyser les journaux d'événements issus de :

- Du serveur web (IIS, Apache, Nginx)
- Des outils d'administration (SSH, VNC, RDP, etc.)
- Des applications accessibles à distance (SGBD, serveurs d'applications)
- Des serveurs frontaux si présents (reverse-proxy, cache, etc.)

- **Réinstaller le système**

La réinstallation totale à partir d'un système sain (et donc le reformatage) du système s'avère souvent nécessaire pour s'assurer que le poste n'est plus infecté.

- **Restaurer les données**

Il est indispensable de posséder des sauvegardes, afin de permettre une reprise de l'activité dans un délai acceptable. Attention aux fichiers issus de ces sauvegardes qui peuvent être infectés/corrompus.

- **Changer tous les mots de passe des accès présents sur le serveur**

Sans changement des mots de passe, l'attaquant peut réutiliser les accès précédemment obtenus.

- **Identifier les possibilités de rebond**

Si le serveur piraté est présent dans un réseau interne, analyser les serveurs connectés afin de déterminer si d'autres accès ont pu avoir lieu.

- **Dépôt de plainte**

Il faut garder à l'esprit que seule la direction de l'organisme est habilitée à déposer une plainte.