Lecture: Les bons réflexes en cas d'intrusion sur un système d'information

CERT : *Computer Emergency Response Team. (http://www.cert.org/)*

Motivation

Ce document recense de manière non exhaustive, les bons reflexes à acquérir lorsque l'on soupçonne une intrusion sur l'un ou plusieurs ordinateurs reliés à un réseau de type internet (TCP/IP). Il y intrusion sur un système d'information lorsqu'une personne réussit à obtenir un accès non autorisé sur ce système.

Toutes les actions entreprises doivent être conformes à la politique de sécurité et aux procédures définies au sein de l'organisme.

Comment déterminer si l'on a été victime d'une intrusion ?

• Utiliser des outils de détection d'intrusion. Il en existe deux grandes familles :

- ceux qui analysent les journaux des événements se produisant sur les équipements (**host-based**)
- ceux qui capturent et analysent le trafic en certains points du réseau (**network-based**)

Chacune possède ses avantages et inconvénients et il est donc préférable d'utiliser si possible les deux types d'outils. De plus, les outils de détection d'intrusion ne peuvent être efficaces que s'ils sont couplés à une surveillance humaine.

• Prendre au sérieux les messages provenant des CERTs. En effet, lorsqu'une machine est compromise, elle est souvent utilisée par le pirate pour la recherche d'autres ordinateurs vulnérables. Si cette machine est repérée, une des victimes prendra contact avec un CERT qui vous contactera alors.

• Mettre en évidence des comportements inhabituels. Certains signes indiquent que le système a peut-être été compromis :

- impossibilité de se connecter à la machine
- fichier(s) disparu(s), système de fichiers endommagé
- signature de binaires modifiée
- connexions ou activités inhabituelles, services ouverts non autorisés
- création ou destruction de nouveaux comptes
- …

Quels sont les bons réflexes en cas d'intrusion sur une machine ?

• Déconnecter la machine du réseau. Permet de stopper l'attaque si elle est toujours en cours. En revanche, maintenez la machine sous tension et ne la redémarrez pas afin d'analyser l'attaque.

• Prévenir le responsable sécurité. Le responsable sécurité doit être clairement identifié par tous les administrateurs système / réseau avant que l'incident de sécurité ne soit déclaré.

• Prévenir le CERT dont vous dépendez.

• Faire une copie physique du disque. En l'absence de copie, l'altération des données provoquée par l'analyse rendrait inefficace toute procédure judiciaire.

• Rechercher les traces disponibles. Il est utile de rechercher des traces liées à la compromission dans tout l'environnement, les copier, les dater et les signer numériquement.

Quels sont les aspects légaux d'une intrusion ?

• Dépôt de plainte. Seule la direction de l'organisme, qui en porte l'autorité morale, est habilitée à déposer une plainte.

• Dégâts à des tiers. L'organisme pourrait, dans certains cas, être considéré comme pénalement et civilement responsable des dégâts qui seraient causés par un intrus, à partir de ses systèmes d'information.

Comment analyser l'intrusion a posteriori ?

Les grandes étapes de l'analyse de l'intrusion sont :

- Recherche des modifications dans le système, fichiers de config. , les données.
- Recherche des outils et des données laissés par l'intrus.
- Examen des fichiers de journalisation.
- Vérification des autres machines connectées sur le réseau.

Comment repartir sur de saines bases après une intrusion ?

• Réinstaller complètement le système d'exploitation à partir d'une version saine.

• Supprimer tous les services inutiles.

• Appliquer tous les correctifs de sécurité préconisées pour le système d'exploitation et les logiciels utilisés.

• Changer tous les mots de passe du système d'information.

Comment améliorer sa sécurité après une intrusion ?

• Se poser les bonnes questions et apporter les réponses avec soin. Même avec la meilleure politique de sécurité, vous n'êtes jamais complètement à l'abri d'une nouvelle intrusion. Il faut donc faire la liste des informations ou des procédures qui ont manqué :

- Pour protéger plus fortement le système d'information sur lequel il y a eu une intrusion
- pour détecter plus rapidement qu'un incident de sécurité était en train de se produire ou s'était produit.
- Pour réagir plus calmement, de manière plus adéquate, sans risquer de commettre un geste qui ferait empirer la situation.
- Pour déterminer plus vite quelle était la marche à suivre et quelles étaient les personnes à contacter.
- Pour trouver plus aisément la ou les vulnérabilités qui avaient été utilisées.
- …

• En déduire les choses à améliorer. En fonction des questions posées précédemment, les réponses se déclinent en deux catégories : les réponses **techniques** qui demande la mise en place d'outils spécifiques, et les réponses **organisationnelles** qui demande des procédures plus claires ou plus adéquates.

• Garder une trace écrite complète de tout ce qui s'est passé.