Protection contre les attaques

Pour se protéger contre des attaques, il est important de protéger le **périmètre** (tout ce qui est vers l'extérieur, tel que le réseau), en installant un firewall au niveau du réseau.

Ensuite, il est aussi important de protéger les **machines** en installant un firewall personnel et un anti-virus.

D'autres choses sont importantes telles que ne jamais travailler avec un compte administrateur.

Sécurité d'un parc informatique

Pour assurer la sécurité d'un parc informatique, on peut utiliser des **scanners de vulnérabilités**, ce sont des programmes qui vont regarder si le système est vulnérable à certaines attaques afin de pouvoir mettre à jour les composants qui en ont besoin.

Il faut aussi pouvoir assurer l'**intégrité des programmes**, on peut donc garder de manière sécurisée les empreintes de tous les programmes et vérifier celles-ci lors de leur lancement. Le seul souci, c'est qu'il faut tenir compte des mises à jour.

On peut aussi utiliser un **système de détection d'intrusion** (IDS), c'est un programme qui tente de repérer des activités anormales sur un système en se basant sur des plans d'attaque connus, en observant l'activité et les journaux systèmes.

Par exemple, `fail2ban` est un IDS qui bannit les adresses IP qui réalisent un certain nombre de tentatives de connexions illicites.

Un IDS peut aussi analyser le comportement de l'utilisateur pour détecter des comportements anormaux (exemple un secrétaire qui compile un logiciel). Il faut cependant faire attention à configurer l'IDS correctement pour éviter les faux positifs. Un autre exemple d'IDS est `Snort`

Enfin, un denier élément important est l'analyse de fichiers journaux. Tous les systèmes d'exploitation consignent des informations sur ce qu'il se passe sur le système, on peut donc utiliser des outils pour analyser automatiquement ces fichiers journaux tel que Splunk, Grafana Loki ou encore Crowdsec.

Revision #1
Created 6 January 2024 15:07:16 by SnowCode
Updated 6 January 2024 19:13:15 by SnowCode