KIPS « Kernel Intrusion Prevention System »

Cet outil permet aux administrateurs réseau de configurer une ou plusieurs réactions ainsi que de bloquer certaine action sur la partie système d’exploitation d’une machine.

Le KIPS agit directement sur le « Noyaux » d’un système ce qui permet de réguler les actions et de prévenir toute défaillance ou attaque. En effet, le KIPS va vérifier chaque appel vers le système et va ainsi permettre de détecter un comportement anormal et interdire ces actions.

Le KIPS permet par exemple de protéger un serveur web en restreignant la lecture et l’écriture des fichiers juste à la partie du service web et ainsi empêcher toute possibilité d’ouverture de shell de commande et de lecture sur le reste du serveur.

L’outil KIPS peut aussi détecter toutes les modifications de performance de la machine telle qu’une utilisation trop importante de mémoire et stopper le logiciel ou l’outil entrainant cette utilisation.

Comment ça marche ?

1. La machine initialise une action système
2. L’outil KIPS analyse la commande
3. KIPS vérifie dans sa base de règle si la commande est autorisé

A présent deux possibilité

1. A) L’action est autorisé et est exécutée

B) L’action est refusé et log le problème

Les Avantages du KIPS :

* Détecte et bloque les commandes douteuses
* Envoie une alerte en cas de problème
* Possibilité de configuration nombreuse
* Ajoute des règles de sécurité supplémentaire

Les inconvénients du KIPS :

* Ralenti la machine car vérifie chaque action et dépendance
* Possibilité de faux-positif
* Rarement utiliser sur des serveurs souvent sollicité
* Complexe à configurer