Auditd

Auditd est un processus Linux capable de monitorer l'intégralité des événements systèmes. Un maximum d'informations sont collectés par défaut, de façon à suivre la totalitée des événements systèmes provoqués par des programmes ou par des utilisateurs.
Si un règle de sécurité est activée, il sera alors possible de la retracer de manière précise jusqu'à son déclencheur.
La puissance d'Auditd réside dans sa grande modularité au niveau des règles de filtrages, et en sa capacité en émettre des messages au format IDMEF, compatibles avec d'autres éléments de sécurités.

Les différentes fonctionnalités d'Auditd sont les suivantes :

- Surveillance d'intégrité de fichiers.
- Surveillance des appels systèmes.
- Enregistrement des commandes exécutés.
- Enregistrement des évènements de sécurités.
- Surveillance des paramètres réseaux.
- Génération de rapports de sécurités plus ou moins détaillés.

Architecture
Auditd se compose de plusieurs modules.
Premièrement, le module *Auditd*, configurable sous */etc/audit/* va permettre de définir les règles de filtrages effectives, et les paramètres généraux du processus.

Le second module, *Audisp*, est capable de récupérer des événements générés par Auditd, puis de les transmettre à d'autres applications. Ceci permet de gérer en temps réel les alertes de sécurités, au travers de plusieurs programmes.

Enfin, le module *Auditctl* interagit avec les modules Auditd pour générer des rapports statistiques et définir les condition du déclenchement des alertes.

Règles de filtrages

Les règles de filtrages sont nécessaires pour monitorer les appels systèmes et l'intégrité des fichiers. Leurs syntaxe est un peu particulière, mais permet de définir de manière précise les conditions d'alertes.

Les règles sont à créer dans le fichier de configuration : */etc/audit/audit.rules*.

Une règle Audit d'appel système dispose du format suivant par défaut :

-a <action>,<filter> -S <syscall> -F <option> = <valeur> -k <log-id>

Argument	Description	Valeur
<action>	*Indique les actions à entreprendre quand la règle est activée.*	*always / never*
<filter>	*Indique à quel moment l'audit du système aura lieu.*	*task / exit / user / exclude*
<syscall>	*Nom de l'appel système.*	-
<option>	*Type de l'option additionnel.*	*arch / userid / pid / path*
<valeur>	*Valeur que l'option doit atteindre pour activer la règle.*	-
<log-id>	*Nom de l'alerte dans les logs.*	*ids-exec-med*

Par exemple, pour monitorer l'ensemble des commandes de modification des droits utilisateurs sur des fichiers, pour les machines d'architecture x86, et concernant les utilisateurs à l'UID supérieure à 100, la règle est la suivante :

-a always,exit -F arch=b64 -F auid>100 -S chmod -k ids-exec-info

Les règles d'intégrités de fichier restent très similaires dans leurs constructions :

-w <path> -p <permissions> -k <log-id>

Argument	Description	Valeur
<path>	*Chemin relatif jusqu'au fichier à monitorer.*	*chemin/relatif/fichier.c*
<permission>	*Permission à surveiller : la violation des règles de permissions définie déclenche l'alerte liée à la règle.*	*r(ead) / x(execute) / w(rite) / a(ttribute)*
<log-id>	*Nom de l'alerte dans les logs.*	*ids-file-low*

Par exemple, pour surveiller la modification et la lecture du fichier /etc/shadow :

-w /etc/shadow *-p rw -k ids-file-low*

Le processus Auditd doit être redémarré pour que les modifications prennent effets :
/etc/init.d/auditd restart

Dans le cas ou il est nécessaire de retirer le monitoring d'un certain types de logs, les modifications sont aussi à effectuer sous */etc/audit/audit.rules*. Par exemple, dans le cas ou il est nécessaire de retirer toutes les alertes de type "PATH", la ligne suivante devra être ajoutée au fichier de règles :

-a exclude,never -F msgtype=PATH