AUDITD

“Laisser sa trace dans un fichier”


```
{
   "signature": {
     "nom": "Phil Leblond",
     "fonction": "Consultant en Securite/Pen Tester"
     }
}
```

AUDITD WTF?

- Service qui permet de suivre certains éléments de securité sur vos systèmes.
- Basé sur des règles pré-définies.
- Enregistre les événements systèmes dans un fichier journal.

Cas d’Usage

- Surveillance d’accès aux fichiers
  - Ex: accès,modification,execution ou changement des attributs sur le fichier /etc/passwd.
- Surveillance des “System Calls”
  - Ex: génère un log lorsque kill (sys_kill) est invoqué.
- Suivi des commandes par usagers (UID)
  - Ex: surveillance des commandes exécutées par un usager.
- Enregistre les évenements de sécurité
  - Ex: enregistre tous les tentatives de connexion non-réussites.
- Recherche d’évenements
  - Ex: Recherche dans le fichier de journal pour certaines conditions particulières.
- Génération de rapports
  - Ex: Création de rapports journaliers.

Installation

- Présent par défaut dans une installation de base de RHEL 7. Aucunes règles de définies par contre.

- Si pour X raisons le package n’est pas installé, installez le avec la commande suivante:

root@box01[~]# yum install audit

Configuration

- La configuration du daemon se fait via le fichier suivant:

/etc/audit/auditd.conf

- Une liste complète des paramètres de configuration se retrouvent dans le “man page” audit.conf(5).

- Comme la plupart des fichiers de configuration, les lignes vides et le caractère dièse (#) sont ignorés.

Mise en route

- Démarrer le service Audit avec cette commande:

root@box01[~]# service auditd start

- Voici les actions possibles à la commande précédente:

stop	Arrête le service
restart	Redémarre le service
reload ou ***force-reload***	Relis les modifications du fichier /etc/audit/auditd.conf
status	Affiche l'état du service
resume	Réactive le service
condrestart ou ***try-restart***	Redémarre le service seulement s'il était actif.

Édition des règles

- Les règles peuvent être écrites via l'outil ***auditctl*** (non-persistent) ou directement à la main dans le fichier de configuration ***/etc/audit/audit.rules*** (persistent).

- 3 types de règles possibles:

  - "**Control Rules**" - Permet de changer la configuration du daemon.
  - "**File System Rules**" - Permet de surveiller l'accès aux fichiers.
  - "**System Call Rules**" - Permet l'audit des appels systèmes.

Édition des règles (suite)

- Des règles pré-définies existent pour différent standards de certifications. Elles sont dans le répertoire **/usr/share/docs/audit-version/** (Ex: NIST, CAPP,STIG …)

Dissection du fichier journal

- Le fichier de journal par défaut est ***/var/log/audit.log***
- Exemple d'entrée dans le fichier:

type=USER_AUTH msg=audit(1364475353.159:24270): user pid=3280 uid=500 auid=500 ses=1 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:authentication acct="root" exe="/bin/su" hostname=? addr=? terminal=pts/0 res=failed'

- Que s'est-il passé?
- Liste et explication de toutes les valeurs "type" possibles ici:

https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Security_Guide/sec-Audit_Record_Types.html

Auditd ++

- Outils qui peuvent vous faciliter la vie.

ausearch	Permet de faire des recherches dans le fichier de journal.
aureport	Création de rapports basés sur le fichier journal.
ausyscall	Mapping entre les numéros et noms des “syscall”

DEMO

FAQ

Références:
Linux Audit:
http://people.redhat.com/sgrubb/audit/

Redhat Security Guide:
https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Security_Guide/chap-system_auditing.html