RÉGIS SENET

AIDE, Comment surveiller l'intégrité de votre système ?

Schwierigkeitsgrad:

Advanced Intrusion Detection Environment ou plus communément appelé AIDE est ce que l'on appel couramment un HIDS ou encore Host-based Intrusion Detection System. Par définition, on appelle IDS (*Intrusion Detection System*) un mécanisme écoutant le trafic réseau de manière furtive afin de repérer des activités anormales ou suspectes et permettant ainsi d'avoir une action de prévention sur les risques d'intrusion. Un HIDS assure la sécurité au niveau des hôtes.

AIDE peut être assimilé à une clone amélioré du logiciel de scellement de fichiers bien connu qu'est Tripwire.

Le principe d'AIDE est relativement simple. Il s'agit de construire une sorte de base de données de signatures de l'ensemble des fichiers se trouvant sur la machine, que celle-ci soit une machine cliente ou bien un serveur. Aide va créer une base de signatures grâce à des algorithmes d'empreinte cryptographique des fichiers.

Périodiquement, AIDE va recalculer les empreintes des fichiers qui peuvent régulièrement changer afin d'avoir une base de données de signatures constamment à jour.

Au niveau des vérifications, de manière périodique également (période définit par l'administrateur du système ou du parc informatique), l'ensemble des fichiers présents sur le système vont être comparés aux signatures présentes dans la base de données.

Si les empreintes sont différentes (au niveau du fichier, de sa date, de ses droits d'accès, de son inode ...), le logiciel détectera une modification de fichiers et en avisera l'administrateur par mail ou par fichier de log suivant les paramètres d'avertissements mis en place.

Ces logiciels sont très utiles en cas d'intrusion, afin de découvrir ce qui a été changé (journaux modifiés, fichiers ajoutés à certains endroits, binaires comme netstat, lsof, who, sshd modifiés, fichiers de configuration, pages web, etc.). Parallèlement, AIDE peut s'avérer très utile pour l'administration. En effet, il sera capable de détecter des erreurs commises (fichiers de configuration changés, ajoutés ou effacés, modifications de binaires).

Attention, il est cependant très important de comprendre qu'AIDE n'est pas un outil permettant de protéger votre système d'exploitation. Il a pour simple but de vérifier les possibles modifications qu'il aurait pu y avoir sur le système et de faire remonter les informations. Si personne ne lit les informations retournées par AIDE, alors les modifications tomberont dans l'oublie.

Installation et configuration d'AIDE

Au cours de cet article, la distribution utilisée fut une Debian 5.0 (Lenny) entièrement mise à jour. Attention, il est possible que certaines commandes ne soient pas tout à fait identiques sur une autre distribution. Les installations se réalisant via le gestionnaire de paquet se

CET ARTICLE EXPLIQUE...

L'utilisation et l'installation d'AIDE.

CE QU'IL FAUT SAVOIR...

Systeme Unix/Linux (Les bases).

réaliseront grâce au gestionnaire de paquets propre à un système Debian : APT (*Advanced Package Tool*).

Mise à jour du système

Il est possible à tous moment qu'une faille de sécurité soit découverte dans l'un des modules composant votre système que ce soit Apache ou quoi que ce soit d'autre. Certaines de ces failles peuvent être critiques d'un point de vue sécurité pour l'entreprise. Afin de combler ce risque potentiel, il est nécessaire de régulièrement mettre à jour l'ensemble du système grâce à divers patches de sécurité.

Il est possible de mettre à jour l'ensemble du système via la commande suivante :

```
nocrash:~# apt-get update &&
   apt-get upgrade
```

Le système d'exploitation est maintenant complètement à jour, il est donc possible de mettre en place AIDE dans de bonnes conditions.

Il est possible de ne pas passer par cette étape mais elle est fortement conseillée pour la sécurité ainsi que la stabilité de votre système d'exploitation.

Nous allons réaliser l'installation d'AIDE de deux manières différentes : La première est tout simplement une installation via les dépôts Debian. L'autre, quand à elle va se réaliser grâce aux sources officielle.

Installation d'AIDE via les dépôts

L'installation via les dépôts est extrêmement simple, il suffit de taper la commande suivante avec d'installer AIDE ainsi que tous les paquets associé:

```
nocrash:~# apt-get install aide
```

Installation d'AIDE via les sources

L'installation via les sources est légèrement plus complexe mais vraiment très légèrement. Avant toute chose, il est nécessaire d'installer certain paquet important pour l'installation d'AIDE.

```
nocrash:~# apt-get install -y
build-essential  bison
flex  zlib1g-dev  libgpg-error-dev
libmhash-dev
Nous pouvons à présent installer
AIDE dans de bonnes conditions.
nocrash:~# mkdir /var/aide
nocrash:~# cd /var/aide/
nocrash:~# wget http://
sourceforge.net/projects/aide/
files/aide/0.13.1/
aide-0.13.1.tar.gz/download
nocrash:~# tar xzf
aide-0.13.1.tar.gz
nocrash:~# cd xzf aide-0.13.1/
nocrash:~# ./configure
nocrash:~# make && make install
```

Et voila, l'installation d'AIDE via les sources est terminé. Il est à présent possible de passer à son utilisation.

Initialisation d'AIDE

Maintenant qu'AIDE est correctement installé, nous allons nous pencher sur son utilisation mais dans un premier

temps, nous allons voir de quoi il retourne. Pour des raisons pratiques, je ne mettrais pas ma base de données sur un CD/DVD mais rappelez vous que dans votre cas, cela est complètement indispensable.

Pour voir les possibilités qu'offre AIDE, vous pouvez tapez la commande suivante :

```
nocrash:~# aide --help
Usage: aide [options] command
Commands:
  -i, --init     Initialize
                 the database
  -C, --checkCheck the database
  -u, --update  Check and update
                 the database
                 non-interactively
        --compare   Compare
                 two databases
Miscellaneous:
      --config-check Test the
                 configuration file
  -v, --version  Show version
                 of AIDE and
                 compilation options
  -h, --help Show this
        help message
```

Création de la base de données :

```
nocrash:~# aideinit
```

Suivant le type d'installation que vous avez choisi, il est possible que le fichier de configuration ne soit pas au même endroit. Il est donc nécessaire de le préciser de la manière suivante :

```
nocrash:~# aide --init -c
   /etc/aide/aide.conf
   ### AIDE database at
   /var/lib/aide/aide.db.new
   initialized
```

La base de données est donc créée à l'emplacement */var/lib/aide/aide.db.new initialized*.

La première méthode (aideinit) est fortement conseillé, certains bugs apparaissent avec la deuxième.

Ce processus prend environ une quinzaine de minutes, alors soyez patient.

Si vous ne savez pas ou est votre fichier de configuration vous pouvez utiliser la commande find de la manière suivante :

```
find / -name aide.conf
```

Pour la suite, il est nécessaire de renommer la base de données de la manière suivante :

```
nocrash:~# mv /var/lib/aide/
   aide.db.new
   /var/lib/aide/aide.db
```

Cas pratique

Au cours de ce chapitre, nous allons apporter des modifications qu'un pirate pourrait apporter à votre système d'exploitation pour pouvoir ensuite voir comment AIDE réagit a ce changement de fichier.

Exemple 1 :

Notre pirate a réussi, par une méthode ou une autre, à accéder en écriture, au fichier */etc/passwd*. Afin de pouvoir passer en root sur la machine, il y a ajouté la ligne suivante :

```
system::0:0:system:/:/bin/bash
```

On notera ici, qu'il a simplement créé un utilisateur nommé système, sans mot de passe, qui a le même ID que root. L'intrus pourra ainsi, a tout moment passer root sur la machine, via un simple compte utilisateur, en utilisant la commande su – system

Ce type de backdoor est assez difficile à repérer, étant donné que l'on ne consulte pas le fichier /etc/passwd tous les jours et qu'en plus, le nom system pourrait paraître normal.

Exemple 2 :

Là encore, notre intrus à obtenu les droits root et il voudrait être sêr de pouvoir revenir sous cette identité, à sa guise et même après un changement du mot de passe de ce dernier par l'administrateur. Pour se faire, il pourra positionner un bit SUID, sur les commandes qu'il désire, afin de pouvoir les exécuter ensuite en tant que root :

```
nocrash:~$ cat /etc/shadow
cat: /etc/shadow:
   Permission non accordée
nocrash:~$ su -
Password:
[root@localhost ~]#
   chmod a+s /bin/cat
[root@localhost ~]# exit
nocrash :~$ cat /etc/shadow
root:xxxxx:13449:0:99999:7:::
```

Encore une fois, pour repérer ce genre de manipulation, cela reste difficile, car il faudra régulièrement regarder les bons droits sur les fichiers (avec la commande find / -perm +4000 par exemple).

Vérification

Il est à présent possible de vérifier l'intégrité du système grâce à la commande check. Tout comme la création de la base de données, la vérification prend un peu de temps à se faire.

```
nocrash:~ # aide --check
```

Toujours dans l'éventualité ou le fichier de configuration n'est pas trouvé quand vous lancez cette commande, il est possible de préciser son emplacement grâce à la commande suivante :

```
nocrash:~ # aide --check  -c
   /etc/aide/aide.conf
[…]
changed: /etc/passwd
changed: /bin/cat
[…]
```

Nous pouvons donc voir qu'AIDE à bien détecté les changements qui ont eu lieu entre le moment ou la base de données à été construite et le moment ou on réalise la vérification.

Bien sur, il est possible d'automatiser ces actions grâce à *cron* et même de se faire notifier par mail. Pour les mails, il est nécessaire de démarrer le démon sendmail et de l'installer s'il n'est pas présent sur la machine :

```
nocrash:~ # apt-get install
   sendmail
nocrash:~ # /etc/init.d/
   sendmail start
```