Integritat amb AIDE

Técniques de monitorització de la integritat del sistema amb AIDE

`AIDE (Advanced Intrusion Detection Environment)` és una eina de seguretat que s'utilitza per a detectar canvis en la **integritat** dels fitxers i directoris d'un sistema.

Funciona creant una base de dades d'atributs de fitxers, com ara permisos de fitxers, propietat, mida i sumes de comprovació, i després compara periòdicament l'estat actual del sistema amb aquest baseline. Si es produeix algun canvi no autoritzat o inesperat, AIDE pot avisar l'administrador del sistema.

Característiques principals d'AIDE:

- Comprovació d'integritat dels fitxers: supervisa els canvis als fitxers i directoris importants del sistema.
- Algoritmes hash: admet diverses funcions hash criptogràfiques com MD5, SHA1 i altres per garantir la integritat del fitxer.
- Regles configurables: permet la configuració detallada de quins fitxers o directoris s'han de supervisar i quins tipus de canvis cal detectar (p. ex., modificacions, supressió o canvis de permisos).
- Alertes: pot notificar a l'administrador quan es detecten canvis, ajudant a respondre ràpidament a possibles intrusions o alteracions del sistema.

Casos d'ús típics:

- **Detecció d'intrusions:** per detectar modificacions no autoritzades causades per activitat maliciosa, programari maliciós o bretxes de seguretat.
- **Auditoria de compliment:** garanteix que els fitxers sensibles no s'alterin, cosa que és crucial per a les indústries amb requisits de compliment estrictes (p. ex., HIPAA, PCI-DSS).

- **Hardening del sistema:** ajuda a mantenir la postura de seguretat alertant de qualsevol desviació de la configuració prevista.

Com funciona AIDE

- **Inicialitza la base de dades:** després de la instal·lació, AIDE crea una base de dades que registra l'estat inicial dels fitxers i directoris que voleu supervisar.

Això crea un fitxer de base de dades (normalment emmagatzemat a `/var/lib/aide/aide.db` o una ubicació personalitzada).

Compara l'estat actual: periòdicament, executeu AIDE per comparar l'estat actual del sistema amb la línia de base registrada.

AIDE informarà de qualsevol discrepància.

Actualitzar la base de dades: després de validar els canvis (com ara després de les actualitzacions del sistema), és possible que vulgueu actualitzar la base de dades AIDE per reflectir la nova línia de base.

AIDE s'utilitza habitualment en entorns Linux i Unix com a part d'una estratègia de control i reforç de la seguretat

> **Atenció**
>
> Per tal de treballar amb més facilitat, vos recomane conectar-vos per SSH a la màquina virtual de tal forma que, entre altres coses, podreu pegar text en el vostre terminal sense problema:
>
> ```
> ssh vostre_usuari@ip_rocky
> ```

Utilitzant AIDE per a detectar problemes de seguretat mitjantçant la integritat de fitxers

1. Una vegada hem instal·lat correctament Rocky Linux i si no ho hem fet en la mateixa instal·lació, crearem un usuari a més del de *root*. Si no te'n recordes, busca documentació de com fer-lo.
2. Aquest usuari ha d'estar ficat en el fitxer sudoers per tal de poder fer servir el comand *sudo*
3. Si no ho vau fer tampoc en la instal·lació, activeu el repositori epel per a Rocky Linux: `sudo dnf -y install epel-release`
4. Feu un `sudo yum update` i després instal·leu **aide**

5. Dins del vostre home, crear una carpeta amb el nom `scripts` i dins crear un arxiu buit amb el nomb `miscript.sh`
6. Una vegada instal·lat, haureu de modificar l'arxiu de configuració per a incluir un *group* amb el nom **FIPSR** a on es comproven els següents atributs per als arxius:
    - Permisos dels arxius
    - Número inode (cada arxiu ha de tindre un número d'inode que no ha de canviar)
    - Número de links apuntant a l'arxiu
    - Usuari propietari de l'arxiu
    - Grup propietari de l'arxiu
    - Tamany de l'arxiu
    - Hora de modificació de l'arxiu
    - Comprovar integritat de l'arxiu amb hashes md5 i sha256
7. Afegeix també a l'arxiu de configuració les següents línies:

```
/etc/.*\.conf$ FIPSR
/var/log/.*\.log$ FIPSR
/home/.*\.sh$ FIPSR
```

8. Inicialitzar la base de dades d'aide
9. Substituir l'arxiu de base de dades antic per el nou
10. Canviar els permisos de l'arxiu de logs del sistema `/var/log/messages` (permísos del tipus 777)
11. Incloure el text *"Entrada maliciosa"* al final de l'arxiu `/etc/ssh/sshd_config`
12. Elimina l'arxiu `miscript.sh`
13. Fer un ***check*** amb aide i en la exida, identificar les 3 modificacions que heu fet abans i que detecta aide (indiqueu en quina línea vos informa de les modificacions i quin atribut dels configurats abans ha fet servir)
14. Desfés els 3 canvis que has fet i torna el sistema a la seua situació inicial. Després fes un check amb aide i explica que veus.
15. Fes `sudo yum update && sudo yum upgrade` i identifica els canvis detectats però que sí son legítims
16. Actualitza la base de dades i substitueix l'arxiu antic pel nou d'aide per tal de que accepte el nou estat del sistema i fes un nou check, ¿qué veus en la eixida?

Referències

https://jumpcloud.com/blog/how-to-create-sudo-users-on-rocky-linux

https://documentation.suse.com/sles/15-SP5/html/SLES-all/cha-aide.html

https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/7/html/security_guide/sec-using-aide