Procédure Investigation Intrusion

> Avant toutes choses voici les actions à éviter lors de l'investigation pour éviter d'altérer des preuves :
>
> - Ne **redémarre pas** la machine
> - Évite toute mise à jour ou nettoyage
> - Si possible :
> - Travaille avec un **compte sudo dédié**
> - Monte un **répertoire de travail en lecture seule**
> - Sauvegarde les logs avant analyse

---

1. Identifier les connexions suspectes

1.1 Logs d’authentification

Fichiers

- `/var/log/auth.log`
- `/var/log/auth.log.1`
- `/var/log/auth.log.*.gz`

Pourquoi
Ces fichiers enregistrent :

- connexions SSH réussies / échouées
- élévations de privilèges (sudo)
- changements de mots de passe
- ajouts d’utilisateurs

À analyser

```
grep -i "sshd" /var/log/auth.log
grep -i "accepted" /var/log/auth.log
```

```
grep -i "failed" /var/log/auth.log
```

1.2 Historique des connexions

Outils

- `last`
- `lastlog`
- `who`
- `w`

◫ **Pourquoi**
Permet de voir :

- qui s’est connecté
- quand
- depuis quelle IP
- durée de session

```
last -a
lastlog
```

⚠ Attention :
Ces données peuvent être **effacées par un attaquant avancé**, d’où la corrélation avec les logs.

---

2. Vérifier l’élévation de privilèges

2.1 Utilisation de sudo

◫ **Fichier**

- `/var/log/auth.log`

`grep -i "sudo" /var/log/auth.log`

◫ **Pourquoi**
Un attaquant cherche quasi systématiquement à :

- devenir root
- exécuter des commandes sensibles

Points critiques :

- `sudo su`
- `sudo bash`
- Commandes système inhabituelles (`useradd`, `chmod`, `curl`, `wget`)

2.2 Comptes utilisateurs

Fichiers

- `/etc/passwd`
- `/etc/shadow`
- `/etc/group`

Pourquoi
Détecter :

- création de backdoor utilisateur
- UID 0 non autorisé
- comptes sans mot de passe

`awk -F: '$3 == 0 {print}' /etc/passwd`

---

3. Reconstituer les actions de l’attaquant

3.1 Historique des commandes

Fichiers

- `~/.bash_history`
- `/root/.bash_history`
- autres shells (`.zsh_history`)

Pourquoi
Souvent négligé par les attaquants débutants.

⚠ Limites :

- Peut être effacé
- Peut être désactivé (`HISTFILE=/dev/null`)

3.2 Recherche de fichiers récemment modifiés

`find / -mtime -2 -type f 2>/dev/null`

Pourquoi
Identifier :

- scripts déposés
- binaires modifiés
- fichiers suspects dans `/tmp`, `/var/tmp`, `/dev/shm`

Répertoires à **prioriser** :

- `/tmp`
- `/var/tmp`
- `/dev/shm`
- `/usr/local/bin`
- `/etc/cron*`

Revision #3
Created 2026-01-26 15:49:33 UTC by gpatruno
Updated 2026-01-26 16:46:39 UTC by gpatruno