NAME

suidchecker — Vérifie les fichiers ayant le bit SUID du système

SYNOPSIS

suidchecker --init|--reinit|--add|--check
suidchecker –h|--help

DESCRIPTION

Indexe puis vérifie l'intégrité de tous les fichiers portant le bit SUID. La base de donnée est gérée avec sqlite3, il faut donc que ce logiciel soit installé.

Options

–h, --help
Affiche un message d'aide et quitte le programme.

--init Initialise la base de données, cherche les fichiers portant le bit SUID, et les ajoutes, avec leur somme de contrôle et leur taille, dans la base de données. Échoue avec le code 1 si la base a déjà été initialisée.

--reinit Réinitialise la base de données, en la supprimant puis en l'initialisant comme avec init. À utiliser quand un fichier existant a été légitimement modifié, par exemple suite à une mise à jour. Pour ajouter de nouveaux fichiers, préférer **--add**, qui ne supprime pas l'historique des contrôles et ne réinitilise pas les informations des fichiers existants.

--add Cherche les fichiers portant le bit SUID, et ajoute dans la base ceux qui n'y était pas indexés. À utiliser lors qu'un nouveau fichier portant le bit SUID est ajouté dans le système.

--check
Vérifie, pour chaque fichier indexé dans la base, sa présence, sa somme de contrôle et sa taille. Indique sur la sortie standard si le fichier a été modifié, supprimé ou s'il est identique aux informations d'origines. L'historique des contrôles est stocké dans la base de données.

FILES

/etc/suidchecker.conf
contient la configuration du script. Normalement généré à l'installation, il peut être modifié pour utiliser une autre base de données.

AUTHOR

Breizh <breizh.craft.98@openmailbox.org>