Projet Bash – Compétence C3

December 5, 2025

Contents

1 Description générale du projet

Ce projet met en place une boîte à outils Bash permettant de gérer des archives au format `.tar.gz` issues d'un environnement compromis. Les scripts développés permettent :

- d'initialiser l'environnement de travail,
- d'importer et gérer des archives,
- de lister et restaurer l'environnement,
- d'analyser les archives pour identifier les fichiers impactés.

Ce travail s'inscrit dans le cadre d'une SAE (Situation d'Apprentissage et d'Évaluation), dont l'objectif est de mettre en pratique les concepts liés à l'analyse post-attaque et à la gestion de preuves.

2 Statut du projet et technologies utilisées

Statut : En développement

Technologies :

- Scripts Bash,
- Outils standards Linux : `grep`, `awk`, `sed`, `date`, `tar`, `stat`.

Les scripts doivent être placés dans le dossier de travail de la SAE.

3 Concepts fondamentaux

L'outil repose sur une structure cachée dans le répertoire d'exécution :

3.1 Dossier de stockage : `.sh-toolbox`

Il contient toutes les archives importées.

3.2 Fichier d'index : `.sh-toolbox/archives`

Il sert de registre des preuves.

La première ligne contient un compteur. Les lignes suivantes suivent le format :

```
nom_archive :  date_ajout :  clé
```

4 Instructions pour l'installation et l'utilisation

4.1 1. Initialisation de l'environnement

Exécuter la commande suivante une seule fois :

./init-toolbox.sh

4.2 2. Guide des scripts

Script	Objectif	Syntaxe	Rôle
`init-toolbox.sh`	Initialise l'environnement .sh-toolbox et cree le fichier archives	`./init-toolbox.sh`	Préparation
`import-archive.sh`	Importation d'archives avec confirmation ou mode force (-f),supporte plusieurs fichiers	`./import-archive.sh [-f] <arch>`	Stockage de preuves
`ls-toolbox.sh`	Liste les archives et detecte les incoherences	`./ls-toolbox.sh`	verifications de coherence
`restore-toolbox.sh`	Réparation (corrige incohérences met à jour compteur)	`./restore-toolbox.sh`	Intégrité de la chaine de preuve
`check-archive.sh`	Analyse des archives pour identifier fichier modifiés/non modifiés	`./check-archive.sh`	Analyse d'impact

5 Focus : le script d'audit `check-archive.sh`

Ce script est essentiel pour analyser l'impact d'une compromission. Il s'appuie sur les dates de modification des fichiers (Mtime).

5.1 Étapes de l'analyse

1. Affichage des archives disponibles.
2. Décompression de l'archive dans un répertoire temporaire.
3. Analyse du fichier `var/log/auth.log` pour détecter la dernière connexion réussie de l'utilisateur `admin`.

4. Comparaison avec la date de modification des fichiers du dossier `data`.
5. Affichage des fichiers modifiés après cette connexion (fichiers potentiellement compromis).
6. *Bonus :* Identification des fichiers non modifiés mais identiques (nom et taille) → considérés comme **intacts**.

6 Bugs connus

- **Gestion de l'année :** L'année courante est utilisée pour interpréter les dates du fichier `auth.log`. Si l'archive est ancienne, l'analyse peut être faussée.
- **Limitations du format :** Seules les archives `.tar.gz` sont prises en charge.

7 FAQ

Q : Que se passe-t-il si j'oublie d'utiliser `init-toolbox.sh` ?

Les autres scripts renverront une erreur (code 1 ou 2). Il est possible de recréer la structure via :

```
./restore-toolbox.sh
```

Q : Comment résoudre un conflit lors de l'importation ?

Utiliser l'option `-f` avec `import-archive.sh` pour forcer l'écrasement.

8 Droits d'auteur et licence

- Auteur : Zerrouak Thafsut, Aziz Azwaw
- Année : 2025
- Licence : 2