Partie Bash

Compétence C3

Contexte

Après une attaque, les fichiers de l'ordinateur attaqué vous sont transmis dans une archive au format `.tar.gz` (Tape ARchiver + codage Lempel-Ziv, LZ77 pour la compression).

Parmi les fichiers dans l'archive, les traces subsistent et elles vous permettent d'identifier ce qui a été impacté. En effet, lorsqu'un programme accède à un fichier, modifie les permissions associés à ce fichier ou change son contenu, la date et l'heure de ces actions sont mémorisées.

Objectifs

Initialisation de l'environnement de travail

Votre boîte à outils exploitera un dossier `.sh-toolbox` dans lequel les archives à traiter et les résultats obtenus seront stockés. Si le dossier n'existe pas, il sera créé. Le nom de ce dossier est imposé et il doit toujours se trouver à côté des scripts.

Dans ce dossier, un fichier nommé `archives` sera créé. Ce fichier contient la valeur `0` car aucune archive n'a été ajoutée.

Créer un script `init-toolbox.sh` qui :

1. Vérifie l'existence du dossier `.sh-toolbox` dans le dossier de travail de la SAE
2. Crée le dossier s'il est manquant et affiche un message indiquant la création
3. Vérifie l'existence du fichier `archives` dans le dossier `.sh-toolbox`
4. Crée le fichier s'il est manquant et affiche un message indiquant la création
5. Affiche un message d'erreur si des fichiers et/ou des dossiers différents du fichier `archives` se trouvent à l'intérieur du dossier `.sh-toolbox`

Le script utilisera les codes de retour suivants :

- 0 si le dossier et/ou le fichier a été créé avec succès
- 0 si le dossier existe déjà et qu'il contient le fichier archives
- 1 si le dossier et/ou le fichier n'a pas pu être créé
- 2 si le dossier contient d'autres fichiers (avec ou sans dossiers)

Après cette étape et exécution du script avec succès, le dossier de travail de la SAE contient les éléments suivants :

```
.
├── .sh-toolbox
│   └── archives
└── init-toolbox.sh
```

Ajout d'une archive à l'environnement de travail

Lors de l'ajout d'une nouvelle archive à l'environnement de travail, le fichier *.tar.gz doit être copié dans un dossier `.sh-toolbox`. La valeur dans le fichier `archives` doit être incrémentée et une nouvelle ligne doit être ajoutée à ce fichier comportant le nom du fichier, la date d'ajout ainsi que la clé de déchiffrement : chaque élément est espacé par le symbole « : ».

Créer un script `import-archive.sh` qui accepte en argument un chemin (relatif ou absolu) jusqu'à une archive à ajouter et qui :

1. Vérifie qu'un fichier portant le nom de l'archive n'existe pas déjà dans le dossier `.sh-toolbox`
2. Si le fichier n'existe pas, copie l'archive dans le dossier `.sh-toolbox`
3. Si le fichier existe, affiche un message de confirmation pour demander à l'utilisateur de valider.
    a) Si l'utilisateur ne valide pas, rien est fait
    b) Si l'utilisateur valide, le fichier existant est écrasé par l'archive importée
4. Met à jour le fichier `archives` si besoin
5. Affiche un message d'erreur si le dossier `.sh-toolbox` n'existe pas
6. Affiche un message d'erreur si l'archive n'existe pas au chemin passé en paramètre
7. Affiche un message d'erreur si la copie a rencontré un problème

Le script utilisera les codes de retour suivants :

- 0 si la copie a été faite
- 0 si la copie a été annulée (l'utilisateur répond « non » à la demande de confirmation)
- 1 si le dossier `.sh-toolbox` n'existe pas
- 2 si l'archive n'existe pas au chemin passé en paramètre
- 3 si un problème a eu lieu au moment de la copie
- 4 si un problème a eu lieu à la mise à jour du fichier `archives`

Exemple d’utilisation

```
./import-archive.sh client1-20250411-1311.tar.gz
```

Après cette étape et exécution du script avec succès, le dossier de travail de la SAE contient les éléments suivants :

```
.
├── .sh-toolbox
│   ├── archives
│   └── client1-20250411-1311.tar.gz
├── import-archive.sh
└── init-toolbox.sh
```

Le contenu du fichier `archives` est le suivant :

```
1
client1-20250411-1311.tar.gz:20251104-131504:
```

Note : la clé n’est pas encore connue.

[BONUS] Amélioration de l’importation

Pour rendre le script plus pratique, vous ajouterez la possibilité de forcer l’importation et/ou d’importer plusieurs archives en une fois.

Exemples d’utilisation

Forcer l’importation avec un paramètre « -f » :

```
./import-archive.sh -f client1-20250411-1311.tar.gz
```

Importation de deux archives (sans forçage) :

```
./import-archive.sh client1-20250411-1311.tar.gz \
                    client2-20250411-1341.tar.gz
```

Liste des archives importées

Afin de connaître le contenu de l’environnement de travail, il est nécessaire d’ajouter un script qui comprend la structure du dossier `.sh-toolbox`

Créer un script `ls-toolbox.sh` qui :

1. Parcourt le fichier `archives` et affiche le nom des archives, la date d’ajout et si la clé est connue ou non
2. Affiche un message d’erreur si le dossier `.sh-toolbox` n’existe pas
3. Affiche un message d’erreur si le fichier `archives` n’existe pas

4. [BONUS] Affiche un message d'erreur si une archive mentionnée dans le fichier `archives` n'existe pas dans le dossier `.sh-toolbox`
5. [BONUS] Affichage un message d'avertissement si une archive existe sans être mentionnée dans le fichier `archives`

Le script utilisera les codes de retour suivants :

- 0 si la liste a été affichée sans erreur
- 1 si le dossier `.sh-toolbox` n'existe pas
- 2 si le fichier archives n'existe pas
- [BONUS] 3 si une archive mentionnée dans le fichier `archives` n'existe pas
- [BONUS] 3 si une archive existe sans être mentionnée dans le fichier `archives`

[BONUS] Restauration de l'environnement de travail

Si l'exécution du script ls-toolbox.sh affiche une erreur, l'environnement de travail est corrompu et il est nécessaire de le restaurer.

Créer un script `restore-toolbox.sh` qui :

1. Identifie tous les problèmes
   a) Dossier `.sh-toolbox` manquant
   b) Fichier `archives` manquant
   c) Archive inexistante mentionnée dans le fichier `archives`
   d) Archive présente dans `.sh-toolbox` et non mentionnée dans le fichier `archives`
2. Corrige les problèmes en demandant à l'utilisateur de confirmer à chaque fois

Identification des fichiers impactés/épargnés

Chaque archive contient les éléments suivants :

- un fichier contenant les logs d'authentification SSH (`var/log/auth.log`)
- plusieurs dossiers contenant des données potentiellement chiffrées (`data/*`)

Dans le fichier des logs d'authentification, il faut rechercher la dernière connexion de l'utilisateur « admin » pour trouver l'instant de l'attaque. Il s'agit du compte qui a été utilisé pour chiffrer une grande partie des fichiers.

Par chance, l'utilisateur « admin » n'est pas « root » : certains fichiers n'ont pas été modifiés pendant l'attaque. Pour les identifier, il faut rechercher les fichiers en lecture seule qui

n’appartiennent pas à l’utilisateur « admin », et qui, de fait, n’ont pas été modifiés après la dernière connexion de l’utilisateur « admin ».

Le chiffrement des fichiers ne modifient pas leur taille sur le disque : nous supposerons que deux fichiers avec le même nom et la même taille sont identiques.

Créer un script `check-archive.sh` qui :

1. Propose la liste des noms des archives disponibles et permet d’en sélectionner une
2. Décompresse l’archive dans un dossier temporaire
3. Parcourt le fichier des logs
4. Affiche la date et l’heure de la dernière connexion de l’utilisateur « admin »
5. Parcourt les données décompressées et/ou celles de l’archive puis affiche la liste des fichiers modifiés après la connexion
6. [BONUS] Parcourt les données décompressées et/ou celles de l’archive puis affiche la liste des fichiers non modifiés qui portent le même nom et ont la même taille que chacun des fichiers modifiés et identifiés

Le script utilisera les codes de retour suivants :

- 0 si toutes les opérations ont réussies
- 1 si le dossier `.sh-toolbox` n’existe pas
- 2 si le fichier `archives` n’existe pas
- 3 si la décompression a échoué
- 4 si le fichier des logs est manquant
- 5 si le dossier de données est vide

Historique des modifications du sujet

Version 1.0.3 – 202511101820

Modification du nom de l’extension pour correspondre au format d’archive utilisé.
Précisions diverses en réponse aux questions.

Version 1.0.2 – 202511071155

Précisions dans la partie « Initialisation de l’environnement de travail ».

Version 1.0.1 – 202511060826

Correction d’une coquille en page 2.

« 3. Si le dossier n’existe pas » → « 3. Si le fichier n’existe pas »

Version 1.0.0 – 202511041900

Version initiale du sujet.