Vérification d'intégrité

1. Contexte

Lors du téléchargement des images `iso` des distributions GNU/Linux qu'un administrateur système et réseau souhaite déployer dans l'infrastructure de son entreprise, celui-ci doit être en mesure de certifier que les fichiers téléchargés correspondent bien aux sources officielles afin de ne pas mettre en péril la sécurité de l'infrastructure de l'entreprise. En effet, le fichier téléchargé peut être corrompu pour de multiples raisons :

- erreur de lecture/écriture lors du téléchargement,
- code malveillant introduit par des hackers sur le fichier mis à disposition,
- autres.

Nous allons voir dans cette activité les outils utilisés pour assurer ce type de mission.
Nous prendrons comme cas d'usage le téléchargement et la vérification d'une image `iso` correspondant à l'installation d'un système GNU / Linux Debian.
Pour cela vous utiliserez la VM Debian Gnome déjà utilisée en TP.
La VM sera configurée comme indiqué dans les annexes.

2. Téléchargement de l'image iso

Tout d'abord nous avons besoin de télécharger le fichier `iso` associé à l'image.
Celui sur lequel nous travaillerons aujourd'hui est l'image « network install » qui est une version relativement légère en termes de poids et est compatible avec les architectures à processeurs 64 bits.
Le fichier à télécharger est nommé : « `debian-xx.xx.xx-amd64-netinst.iso` », avec les x remplacés par la numérotation de version actuelle.

1. **Quelle est la version actuelle de la distribution Debian GNU/Linux en version stable. Vous devez fournir le numéro de version et le nom de code associé (remarque : les noms de codes sont associés aux personnages de la licence « Toy Story » des studios Pixar) ?**

nom de code : **Bullseye**
numéro de version : **debian-11**

Ce fichier est disponible au téléchargement par plusieurs moyens :

- En utilisant un lien de téléchargement sur une page dédiée du site officiel ;
- En téléchargeant le fichier fourni par votre enseignant sur une ressource mutualisée sur l'infrastructure pédagogique (fichier disponible sur le serveur ftp sionas dans le répertoire « images-iso »), et ceci afin de ne pas surcharger la demande en bande passante externe de l'établissement ;
- En copiant sur une clé USB un fichier téléchargé par l'un de vos camarades (attention montage clé USB dans une VM voir annexes) ;
- En utilisant un logiciel de téléchargement pair à pair (peer to peer) tels que par exemple les logiciels comme aMule (qui utilise les protocoles ed2k et kademlia) ou Transmission (protocole BitTorrent). Ce moyen n'est pas disponible sur l'infrastructure pédagogique où les flux peer2peer sont bannis au niveau de la politique de parefeu.
- Par tout autre moyen disponible permettant de récupérer une copie numérique du fichier

`iso`.

3. Téléchargement des empreintes de l'image et des signatures de celles-ci

Vous devez récupérer sur l'un des sites officiels de Debian les empreintes numériques de l'image téléchargée (ou récupérée par un autre moyen) correspondant aux fonctions de hachages suivantes :

1. MD5
2. SHA1
3. SHA256
4. SHA512

Vous devez également télécharger les signatures associées à ces fichiers d'empreintes afin de pouvoir les authentifier.

2. **Trouver en naviguant sur le site officiel, l'URL permettant de récupérer les fichiers d'empreintes et de signature associés à l'image iso téléchargée. Copier / Coller l'URL en réponse ici.**

https://wiki.debian.org/coreutils

Coreutils permet d'installer toutes les empreintes en même temps. Avec la commande *dpkg -L coreutils* on obtiens la liste de tous les fichiers présent.

Faire une copie d'écran de l'ensemble des fichiers obtenus ici :

```
/usr/share/man/man1/runcon.1.gz
/usr/share/man/man1/seq.1.gz
/usr/share/man/man1/sha1sum.1.gz
/usr/share/man/man1/sha224sum.1.gz
/usr/share/man/man1/sha256sum.1.gz
/usr/share/man/man1/sha384sum.1.gz
/usr/share/man/man1/sha512sum.1.gz
```

```
/usr/bin/logname
/usr/bin/md5sum
/usr/bin/mkfifo
/usr/bin/nice
/usr/bin/nl
```

On peut voir ici une tout petite partie de ce que contient coreutils comme les différents fichiers d'empreintes et de signatures.

4. Outils nécessaires à la vérification

Afin d'être sûr de pouvoir vérifier l'intégrité de l'image iso, nous allons utiliser les logiciels suivants :

- gpg
- md5sum
- sha256sum
- sha512sum

Ces programmes sont inclus dans les paquets logiciels « coreutils » et « gpg » de toute distribution GNU/Linux.

3. **Donnez les commandes qui exécutées à partir d'un terminal vous permettront de vous assurer que ces programmes sont bien disponibles dans votre environnement de travail. Astuce : une commande avec apt et une autre avec apt-file (installer apt-file s'il n'est pas déjà installé dans votre OS).**

sudo apt list gpg
sudo apt-file search md5sum
sudo apt-file search sha256sum
sudo apt-file search sha512sum

On peut vérifier ensuite également que la commande gpg est fonctionnelle dans votre environnement en tapant la directive suivante :
`$gpg –list-keys`

Remarques :

1. *Si c'est la première fois que cette commande est exécutée dans votre environnement de travail elle générera l'ensemble des fichiers de l'environnement nécessaires à l'éxécution correcte de l'utilitaire gpg (répertoire .gnupg, trousseau de clés et base de données de confiance associée à l'utilisateur) ;*

```
root@debian:/# gpg --list-keys
gpg: répertoire « /root/.gnupg » créé
gpg: le trousseau local « /root/.gnupg/pubring.kbx » a été créé
gpg: /root/.gnupg/trustdb.gpg : base de confiance créée
root@debian:/#
```

2. *attention il faut taper cette commande dans l'environnement « utilisateur : user » et non pas en étant connecté comme l'administrateur « root ». En effet, lorsqu'un utilisateur va générer des clés, le comportant attendu est que ces clés soient stockées dans l'environnement personnel de l'utilisateur (`/home/user`) et non pas dans l'environnement de l'administrateur (`/root`).*

Télécharger les empreintes wget + url de la signature

5. Vérification des fichiers d'empreinte téléchargés

Pour s'assurer de l'authenticité des fichiers de vérification d'empreinte que vous avez téléchargés, vous devez utiliser l'utilitaire gpg pour vérifier que ces fichiers ont bien été signés par une clé officielle Debian.

Il faut télécharger avec les commandes :

wget https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/SHA512SUMS.sign
et
wget https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/SHA512SUMS

5.1. Vérification de signatures

4. **Donnez ici les commandes gpg qui permettent de vérifier pour chaque fonction de hachage l'authenticité des fichiers d'empreintes avec leurs signatures associées :**

gpg –verify SHA512SUMS.sign
gpg –verify SHA526SUMS.sign
gpg –verify MD5SUMS.sign

5. **Effectuer des copies d'écran que vous placerez ici pour illustrer les résultats obtenus.**

```
root@debian:/# gpg --verify SHA512SUMS.sign
gpg: les données signées sont supposées être dans « SHA512SUMS »
gpg: Signature faite le sam. 17 déc. 2022 20:07:08 CET
gpg:                avec la clef RSA DF9B9C49EAA9298432589D76DA87E80D6294BE9B
gpg: Impossible de vérifier la signature : No public key
root@debian:/#
```

Il se peut que vous obteniez des résultats équivalents à celui-ci :

```
gpg: Signature faite le dim. 06 déc. 2020 02:46:08 CET
gpg:                avec la clef RSA DF9B9C49EAA9298432589D76DA87E80D6294BE9B
gpg: Impossible de vérifier la signature : No public key
```

Le message vous indique qu'il n'est pas possible de vérifier l'authenticité de la clé, car vous ne possédez pas, au sein de votre trousseau, la clé publique qui permet d'effectuer cette vérification.

5.2. Téléchargement de la clé publique Debian

6. **Donnez ici la commande qui permet de télécharger cette clé publique de Debian en utilisant l'utilitaire gpg (astuce utilisez gpg avec les options keyserver et recv-keys en indiquant avec ces options les valeurs appropriées) :**

Clé publique de debian : ***gpg --keyserver keys.openpgp.org --recv-keys 0x9D6D8F6BC857C906***

5.3. Vérification de signatures

Maintenant que vous possédez la clé publique qui est censée avoir été utilisée pour signer les fichiers d'empreinte, vous pouvez procéder à la phase conforme de vérification des fichiers signature.

7. **Donnez ici les commandes gpg qui permettent de vérifier pour chaque fonction de hachage l'authenticité des fichiers d'empreintes avec leurs signatures associées :**

8. **Effectuer des copies d'écran que vous placerez ici pour illustrer les résultats obtenus et concluez.**

5.4. Vérification des empreintes

À ce stade de l'activité vous devez avoir obtenu des fichiers d'empreintes certifiés par une clé officielle Debian. Si ce n'est pas le cas, reprenez les étapes précédentes jusqu'à obtenir cet état attendu avant de passer à la suite.

Vous possédez donc désormais les empreintes certifiées conformes correspondant aux différents algorithmes de hachage qui ont été utilisés sur les fichiers images. Vous allez donc désormais procéder à la validation ultime de la conformité des téléchargements en vérifiant que les programmes des fonctions de hachages installés sur votre poste produisent bien les mêmes empreintes que celles enregistrées dans les fichiers d'empreintes certifiés.

9. **Donnez ici les commandes ainsi que les copies d'écran qui permettent pour chaque fonction de hachage d'établir que votre fichier « `debian-xx.x.x-amd64-netinst.iso` » :**

- correspond bien à la version officielle de la distribution GNU / Linux Debian ;
- qu'il n'est donc pas corrompu ;
- et que vous pouvez ainsi vous en servir sans risque pour déployer des postes dans l'infrastructure de l'entreprise.

Installer l'empreinte MD5 :
wget https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/MD5SUMS

Puis nous vérifions l'empreinte :
md5sums debian-11.6.0-amd64-netinst.iso

La sortie doit ressembler à cela :
32a8c7e712a79788bf3b3b3a5c5f5fb5 debian-11.6.0-amd64-netinst.iso

Ceci confirme que notre fichier debian correspond a la version officielle de Debian

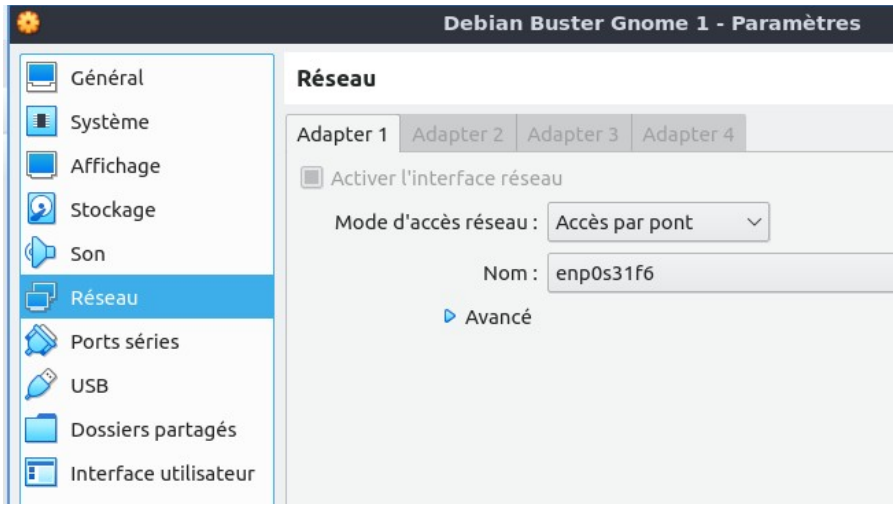
Annexes

6. Configuration de la VM

On se servira d'une VM GNU/Linux ou d'un poste de travail sous OS GNU/Linux déjà utilisée au préalable.

6.1. Configuration Réseau

La VM doit être reliée au réseau SIO en mode « Accès par pont » afin de lui permettre d'accéder aux services de l'environnement pédagogique.

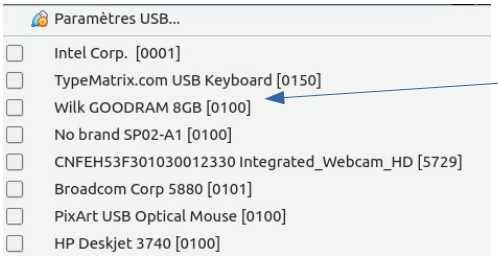


6.2. Montage d'une clé USB

Une fois démarrée si vous souhaitez récupérer le contenu d'une clé USB, c'est possible en montant la clé dans la VM plutôt que dans le système hôte lors de l'insertion de celle-ci dans le port USB.

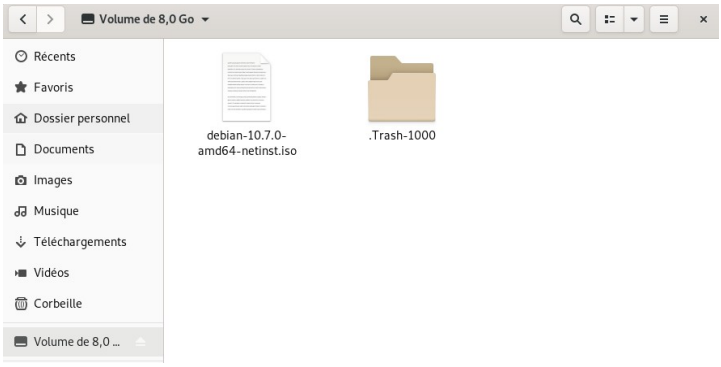
- Refuser l'ouverture automatique de la clé
- Monter la clé dans la VM en utilisant le menu contextuel dédié :

1 : clic droit



2 : sélection du périphérique USB correspondant à la clé (ici indice « 8GB »)

3 : la clé est disponible dans la VM et on peut afficher son contenu en utilisant le gestionnaire de fichier.



7. Ressources

- Guide d’installation Debian (lien consulté le 11/01/2021)
- How to verify your Ubuntu Download (lien consulté le 11/01/2021)
- Verifying authenticity of Debian CDs (lien consulté le 11/01/2021)
- **How can I verify the downloaded ISO images and written optical media?** (lien consulté le 11/01/2021)
- script « check_debian_iso » (lien consulté le 11/01/2021)
- Arborescence des téléchargement d’images officielles Debian (lien consulté le 5/10/2021)