LABO3 – Cryptographie

1 GPG

1.1. GPG et le chiffrement symétrique

Rédigez un rapport personnel que vous nommerez **Lab3-UE19-Nom_Prénom.docx**. Numérotez-y vos chapitres (***1. Conseils à appliquer***).

1.1.1 Vérifications

Le but de ce TP est de vous familiariser avec la notion de signature électronique et de chiffrement clé publique / clé privée en utilisant le logiciel **GPG**. **GPG** est une version libre du logiciel **PGP** (Pretty Good Privacy) crée par Philip Zimmermann. Bien qu'il existe des clients graphiques (**GPA** par exemple), nous allons utilisez l'outil le plus basique (mais aussi le plus puissant) : le programme **gpg** en mode texte.

Sur votre VM Kali Linux, dans un shell, vérifiez que le logiciel est bien installé avec la commande

```
gpg -version
```

Informations complémentaires pour réaliser le laboratoire du mini-HOWTO
https://gnupg.org/howtos/fr/index.html

1.2. Configuration GPG

Pour créer nos clés GPG, nous allons suivre la vidéo en y apportant quelques adaptations.
https://www.youtube.com/watch?v=G7_yBOwYMEY&feature=youtu.be&t=477

Le fichier **~/.gnupg/gpg.conf** est inexistant sur Kali Linux. Vous devez le créer.

Commentez votre fichier de configuration GPG afin de préciser chaque configuration appliquée.

Dans votre rapport, sous le chapitre (***1. Configuration GPG***), copiez la configuration GPG (version commentée) en place sur votre Kali Linux.

1.3. Création des clés

Les clés sont stockées dans un répertoire caché de votre répertoire personnel : **.gnupg**. Vous êtes la seule personne à avoir accès à ce fichier. De plus, vos clés sont protégées par un mot de passe pour renforcer la sécurité. Pour créer votre propre clé publique/clé privée, il faut utiliser la commande **gpg --full-generate-key**

Dans votre rapport, sous le chapitre (***2. Clé GPG***), documentez les commandes utilisées pour créer vos clés GPG, sans compromettre la sécurité de vos clés !!!

1.4. Exercice avec GPG

Une fois vos clés GPG créées, réalisez les opérations suivantes et complétez un rapport en précisant les commandes utilisées :

1. Créez un fichier texte **document.txt** contenant un petit paragraphe, et chiffrez ce document.

LABO3 – Sécuriser sa messagerie

2. Validez le résultat en visualisant le fichier `document.txt.gpg`, et supprimez le document non chiffré.
3. Déchiffrez le document chiffré créé précédemment.
4. Signez le document texte initial. Validez le résultat en visualisant le fichier `document.txt.asc`.
5. Vérifiez le document signé.

Dans votre rapport, sous le chapitre (***3. utilisation GPG***), documentez les commandes utilisées pour chacun des points. Toujours sans compromettre la sécurité de vos clés !!!