TP : Cryptographie

Stéganographie, chiffrement et certificat

Durée : 6h

Présentation :

L'objectif de ce TP est de vous :

- Faire comprendre le fonctionnement de la stéganographie avec un outil simple d'utilisation ;
- Apprendre à échanger des fichiers de manière sécurisée ;
- Guider dans une approche d'entreprise à créer, gérer et installer des certificats.

Pour se faire ce TP est à faire en binôme (trinôme si la classe à un nombre d'étudiant impair).

OS :

Windows / Linux / MacOS.

But du TP :

Dans ce TP vous devrez vous mettre dans la peau d'un collaborateur d'une entreprise. Ainsi vous devrez communiquer à votre manager (le professeur) un rapport qui aura la forme d'une procédure.

Cette procédure sera à faire en binôme et elle devra être suffisamment détaillée pour être utilisée par d'autres collaborateurs de l'entreprise.

Prérequis :

1. Indiquer la distribution et version de l'OS utilisé ;
2. Lister les prérequis (logiciels / paquets nécessaires et leur version).

Stéganographie et Chiffrement :

1. Récupérer une image sur internet ;

2. Utiliser Stegosuite pour intégrer un code de 4 chiffres dans l'image sans communiquer le code à son binôme ;
3. Créer une clé privée RSA :

    a. Générer une clé privée de 2048 bits au format PEM et la stocker dans le fichier « rsaprivatekey.pem ».

    b. Le fichier « rsaprivatekey.pem » contient la partie privée de la clé, et ne peut donc pas être communiqué tel quel (même s'il est chiffré). Avec l'option « -pubout » exporter la clé publique dans le fichier « rsapublickey.pub ».

4. Chiffrer l'image avec la clé publique de votre partenaire ;

5. Envoyer le à votre partenaire afin qu'il le déchiffre avec sa clé privée.

Certificat :

1. Créer une page Web (la page par défaut de votre serveur web sera parfaite) ;

2. Création d'un certificat :
    a. Générer une clé privée de 4096 bits avec l'algorithme de chiffrement AES 256 ;
    b. Créer le fichier de demande de signature de certificat (CSR) ;
    c. Signer le certificat ;
    d. Utiliser le certificat SSL.

3. Améliorer la sécurité de votre site :
    a. Autoriser uniquement le TLSv1.2 ;
    b. Autoriser uniquement des cipher suites.

4. Tester la configuration / sécurité de votre site (uniquement pour les sites accessibles depuis internet) :
    a. Dans un premier temps avec la commande OpenSSL ;
    b. Quand vous pensez avoir atteint un niveau satisfaisant testez avec le lien suivant : https://www.ssllabs.com/ssltest/ ;
    c. Faire une copie d'écran au premier test de la note globale ;
    d. Prendre chaque élément warnings et errors (informations en orange et en rouge) et corrigez les. À chaque élément indiquez ce que vous avez fait pour le corriger.