Université Paris Descartes – UFR de mathématiques et Informatique

Licence 3 Informatique – Sécurité et Réseaux

TD/TP n°4

OpenSSL et Steghide

1. OpenSSL

OpenSSL est une boîte à outils cryptographiques implémentant les protocoles de chiffrement et déchiffrement symétrique et asymétrique.

Voici quelques commandes de base dans l'outil OpenSSL :

1. `openssl version`: pour obtenir la version d'openSSL
2. `openssl help`: pour obtenir de l'aide
3. `Openssl list -cipher-commands`: pour lister les algorithmes de chiffrement
4. `Openssl prime -hex 111`: pour tester si le nombre en hexadecimal 111 est premier
5. `openssl enc -aes-128-cbc -in <file.txt> -out <file.bin> -pass pass:password`: pour chiffrer un fichier avec l'algorithme AES utilisant le mot de passe *password*
6. `openssl enc -d -aes-128-cbc -in <fichier.bin> -out <fichier.txt> -pass file:/path/to/shared_key.pem`**:** pour déchiffrer un fichier avec l'algorithme AES utilisant un mot de passe sauvegardé dans le fichier *"shared_key.pem"*.

Exercice 1 : chiffrement et déchiffrement symétrique

1. Indiquer la version de votre logiciel OpenSSL
2. Citer 5 algorithmes de chiffrement symétrique dans OpenSSL.
3. Tester si le nombre 512687 est premier
4. Chiffrer un fichier texte (de votre choix) avec la commande suivante :
   ```
   openssl enc -aes-256-cbc -in myfile.txt -out encrypted.bin
   ```
   et ensuite entrer le mot de passe
5. Visualiser le contenu du fichier ″encrypted.bin″. De quel codage s'agit-il ?
6. Est-ce qu'il est facile de copier le contenu du fichier ″encrypted.bin″ dans gmail pour une transmission par courriel ? justifier votre réponse.
7. Donner la signification des termes suivants : enc, aes, 256, cbc, -in et -out
8. Répéter la commande de chiffrement précédente avec l'option *-base64*
   ```
   openssl enc -aes-256-cbc -in myfile.txt -base64 -out encrypted.b64
   ```
9. Afficher le contenu du fichier *encrypted.b64*
10. De quel codage s'agit-il ? donner l'alphabet de ce codage ?
11. Est-ce que c'est facile de copier ou à transmettre le contenu du fichier *"encrypted.b64"* par courriel via gmail ? justifier votre réponse
12. Déchiffrer le fichier *"encrypted.bin"* avec la commande suivante
    openssl enc -d -aes-256-cbc -in encrypted.bin -out file.txt -pass pass:votremotdepasse
13. À quoi sert les options suivantes dans la commande précédente : enc -d, -pass pass:votremotdepasse ?
14. Déchiffrer le fichier *"encrypted.b64"* avec la commande suivante
    openssl enc -d -aes-256-cbc -in encrypted.b64 -base64 -out file.txt -pass pass:./file.txt
15. À quoi sert l'option -base64 ? peut-on omettre cette option ?
16. Quelle est la différence entre les deux commandes utilisées pour déchiffrer le fichier ?
17. Tentez de déchiffrer le fichier *"encrypted.bin"* ou *"encrypted.b64"* avec un mauvais mot de passe. Comment réagit OpenSSL ?

18. Chiffrer un fichier ″toto.txt″ avec l'algorithme Blowfish en mode CBC, avec un mot de passe de votre choix, le fichier chiffré portera le nom de ″toto.enc″. Vérifier si vous pouvez déchiffrer et donner les commandes pour chiffrer et déchiffrer.
19. Chiffrer un fichier ″titi.txt″ avec l'algorithme RC2 en mode CBC, avec un mot de passe de votre choix, le fichier chiffré portera le nom de ″toto.enc″.

Exercice 2 : base64

On considère le fichier texte suivant :

$cat raphael.txt

Quatre consonnes et trois voyelles
C'est le prénom de Raphaël
Je le murmure à mon oreille
Et chaque lettre m'émerveille
C'est le tréma qui m'ensorcelle
Dans le prénom de Raphaël

1. Coder le fichier raphael.txt en base 64 (raphael.b64). Donner la commande pour effectuer ce codage.
2. Donner la commande pour décoder le fichier précédent (raphael.b64)
3. Donner la commande pour coder le mot de passe (azerty) en base 64
4. Donner la commande pour décoder le résultat précèdent
5. Donner deux sites web permettant de coder/décoder un texte en base 64

Exercice 3: Déchiffrement

Le fichier ″encrypted_file.b64″ (disponible sur moodle) a été chiffré avec le système AES en mode CBC, la clé de 256 bits ayant été obtenue par un mot de passe stocker en base64 dans le fichier ″passwd.b64″.

1. Le mot de passe codé en base 64, pourriez-vous le décoder ?
2. Déchiffrer ensuite le fichier ″encrypted_file.b64″ et donner la commande et le résultat de déchiffrement

2. Passwd

La commande ″passwd″ permet de modifier le mot de passe d'un utilisateur connecté. La commande :

```
passwd student
```

Permet de modifier le mot de passe de l'utilisateur student. Si vous ne fournissez pas le login (student), la commande ″passwd″ agit sur le mot de passe de l'utilisateur actuellement connecté.

Exercice 4: mot de passe

1. Dans quel fichier sont stockés les mots de passe sous linux ?
2. Sont-ils lisibles ? comment sont-ils enregistrés ?
3. Noter la différence entre les résultats de commandes suivantes

```
Openssl passwd -1 azerty
```

```
Openssl passwd -2 azerty
Openssl passwd -6 azerty
```

4. Combien des $ y-a-t-il dans le champ mot de passe ?
5. Que signifie 1 ou 2 ou 6 ?
6. À quoi correspond la valeur entre le deuxième et le troisième dollar ? et la valeur entre le troisième dollar et la fin ?
7. Si un utilisateur perd son mon de passe, est-il facile de lui renvoyer ce dernier ?
8. Est-il possible de cracker un mot de passe ? si oui, expliquer le principe.
9. Connaissez-vous un logiciel ? donner la commande pour cracker un mot de passe.

3. Steghide

Cette partie de TP ne peut pas se faire sur les machines de la fac et il est conseillé de le faire sur vos propres machines.

Voici les commandes de base de l'outil steghide :

1. apt-get install steghide: pour installer l'outil steghide
2. steghide embed -ef file.txt -cf image.jpeg (ou steghide embed -ef file.txt -cf image.jpg -p <password>) : pour cacher un fichier texte derrière une image
3. steghide extract -sf image.jpg: pour extraire le fichier caché
4. steghide info image.jpeg : pour récupérer le nom du fichier caché

Exercice 5: stéganographie

Télécharger les images 1.jpg et 2.jpg qui sont disponibles sur moodle et extraire le fichier caché derrière chaque image. Décoder les 2 fichiers et donner le texte en claire (sachant que le texte est en anglais).