Introduction à la cryptographie réseau

Les questions suivantes sont destinées à un premier contact avec la cryptographie appliquée aux réseaux. Elles ne sont pas soumises à évaluation.

Pour les questions portant sur les réseaux, vérifiez vos réponses en utilisant un analyseur de trame (ethereal, tcpdump,...) et en essayant de localiser les informations transmises.

Exercice 1. **1.** Comment sont stockés les mots de passe Unix, comment sont-ils protégés.

2. Pourquoi la plupart des serveurs interdisent-ils la connexion par `telnet` ?

3. Quelle possibilité offre FTP que n'offre pas telnet ? En discuter les limites ?

4. Proposer une amélioration de `telnet` en utilisant un chiffrage ou un hachage du mot de passe.

Exercice 2. **1.** Comment Yahoo protège-t'il la transmission du mot de passe nécessaire pour accéder à un compte ?

2. Comment le CMI protège-t'il la lecture du mèl via l'interface

`https://147.94.64.6/src/login.php`

Exercice 3. **1.** Comment déterminer de manière simple le type (Apache, IIS, etc.) d'un serveur HTTP ?

2. Comment un serveur Apache protège-t'il certaines pages ?

3. Une rapide recherche le 1er novembre 2005 fait apparaître à l'URL

`ftp://ftp.cs.rutgers.edu/cs/AcademicIntegrity/private/.htpasswd`

Le fichier suivant :

`instructor:6zo0T7rbLh4OE`

Avez-vous une chance de vous faire passer pour un enseignant d'informatique de l'université de Rutgers ?

Exercice 4. **1.** Où sont stockés les certificats de votre navigateur ?

2. À quoi servent-ils ?

3. Par quelle méthode obtient-on des certificats ? Est-ce sûr ?

Exercice 5. La page web de Pascal Weil contient une clé GnuPG.

1. À quoi sert-elle ?

2. Sauriez-vous lui envoyer un message crypté (ne pas le faire) ?

Exercice 6. Regarder le programme `crypt`, comprendre son fonctionnement.