CRYPTOGRAPHIE
TP N°5

Objectif du TP : *Mettre en oeuvre un site sécurisé avec SSL. Ceci permet de faire du https.... Pas de programmation dans ce TP, mais de l'administration*

ENONCE :

La machine s4m8 (le vieux modèle) est configurée pour servir de serveur web. Elle ne dispose que d'un utilisateur (boss) dont le mot de passe est ...je vous le dirais en cours....

Elle tourne sous une distribution Ubuntu (un peu vieillotte) mais cela suffira. Le serveur http qui tourne dessus est un serveur apache2 avec le support de openssl.

Pour ceux qui ne connaissent pas Ubuntu, les opérations réservées au root peuvent etre faites par l'utilisateur boss en faisant précéder la commande de "sudo". Ce programme vous demandera alors un mot de passe qui est le mot de passe de l'utilisateur boss.

Cette machine dispose également d'un serveur ftp et d'un serveur ssh pour vous permettre de travailler depuis n'importe quelle machine de la salle 4. Attention cependant a ne pas interferer avec les manip des autres groupes.

Exercice 1 :
Vous devrez mettre en place par groupe (par étudiant) un site comportant deux parties : une partie http normale et une partie https. Chaque partie peut très bien ne comporter qu'un seul fichier de test (et des liens permettant de passer de l'un à l'autre).

Exercice 2 :
Lancez ethereal sur la machine s4m8 pour scruter le trafic réseau entre ce serveur et votre machine. Analysez les paquets échangés lors d'une requête http et lors d'une requête https. Vous devez dans le dernier cas retrouver les notions vues en cours concernant le protocole ssl.