T.P. Analyse et diagnostic du réseau.

But : Prise en main et utilisation de wireshark.

I. Analyse des trames émises par msn messenger et récupération des données :

Matériel : un poste client XP + wireshark + msn

1. Téléchargement et installation de wireshark.
2. Sélectionner l'interface d'écoute.
3. Mettez tcp port 1863 and http comme filtre de capture.

Lancer la capture et mettre : msnms contains «test/plain » comme filtre d'affichage afin de ne pas montrer que les messages textes.

II. Mise en évidence de la différence entre une connexion sécurisée et non sécurisée :

Matériel : un poste client XP + wireshark + filezillaserver et client

1. Télécharger et installer filezillaserver.
2. Créer un compte test_numero_etabli et partager un répertoire.
3. Utiliser un logiciel ftp pour vous connecter à votre serveur et en utilisant les filtres appropriés (port…) déterminer à l'aide de wireshark le nom d'utilisateur et le mot de passe du compte.
4. Utiliser un logiciel sftp pour vous connecter à votre serveur et en utilisant les filtres appropriés (port…) déterminer à l'aide de wireshark le nom d'utilisateur et le mot de passe du compte.
5. Expliquer les différents réglages effectués et comparer les questions 3 et 4 et expliquez la différence entre sftp et ftp.

III. Diagnostic du réseau :

Matériel : un poste client XP + un poste serveur + wireshark

1. Donner des commandes utilisant le protocole ICMP.
2. Réaliser et donner un script permettant de saturer le réseau en commandes utilisant le protocole ICMP.
3. A l'aide de wireshark déterminer les filtres permettant de mettre en évidence le dysfonctionnement de la machine.