TP: accès distant à une machine
(Telnet Vs SSH)

N.B: ***Ce Tp a été testé sous ubuntu 14.04 LTS***

I. Outils utilisés:

- Machine ubuntu 14.04 LTS (qui peut jouer le rôle du client et du serveur à la fois). Nous nommons la machine serveur S et la machine cliente C.
- Installez le client ssh (**# sudo apt-get install openssh-client),** le serveur ssh (**# sudo apt-get install openssshserver),** telnetd (sudo apt-get install xinetd telnetd), vsftpd et wireshark (**# sudo apt-get install vsftpd wireshark**)
- Pour que le service telnet fonctionne, ajouter la ligne suivante dans le fichier /etc/xinetd.conf (**telnet stream tcp nowait telnetd /usr/sbin/tcpd /usr/sbin/in.telnetd**) puis redémarrer xinetd (**service xinetd restart**)

II. Travail à faire

Manipulation 1: Accès à distance à une machine serveur: Telnet (non sécurisé) vs SSH (sécurisé)

partie 1: telnet:

1) Dans la machine S, créer un utilisateur "sshuser1" (commande **adduser**) et lancer le serveur telnetd,
2) Dans la machine C, lancer wireshark, puis se connecter au serveur telnetd en utilisant le compte créé.
3) Analyser le trafic échangé entre S et C: Identifier la phase d'ouverture de connexion et le port de telnet, retrouvez le mot de passe.

Partie 2 : SSH

4) Lancer le serveur openssh-server dans la machine S (**#sudo service ssh start**).
5) Au niveau du client C, ouvrir le fichier ~/.ssh/kown_hosts. Vérifiez qu'il est vide.
6) Lancer wireshark pour analyser le trafic. Puis, accéder depuis la machine C à la machine S à travers ssh en utilisant le compte "sshuuser1" et le nom de la machine S. (#ssh sshuser1@S)
7) Expliquez la question affichée au terminal à la première connexion.
8) Après avoir répondu par "Yes", quel est le type d'authentification utilisé par défaut.
9) Vérifiez que le fichier ~/.ssh/kown_hosts n'est plus vide. Que contient-il désormais.
10) Une fois la session ssh ouverte, créez un fichier fichtest1 dans le répertoire personnel de <sshuser1> dans la machine S.
11) Fermer la session avec la commande exit et stopper l'analyse de trafic avec wireshark en sauvegardant. Essayez de vous connecter de nouveau avec le même compte. Que remarquez vous? Expliquez?
12) Dans la Capture de trafic SSH avec WireShark, Affichez l'établissement de la connexion et préciser les différentes phases de l'échange SSH : Echange de versions, Négociation (en montrant les algorithmes choisis), protocole d'achange de clé secrète, données cryptées.
13) Au niveau de la machine S, désactivez l'authentification par mot de passe en utilisant le fichier /etc/ssh/sshd_config.
14) Essayez de vous connecter. Que remarquez vous.
15) Pour établir une authentification par clé privée du client C auprès de la machine S, générer d'abord deux paires de clés en utilisant l'algorithme RSA portant votre prénom : par exemple : islem_rsa et islem_rsa.pub.
16) Copier avec la commande scp la clé publique au niveau de la machine S. Plus exactement dans ~/.ssh/authorized_keys.
17) Réinitialisez la connexion. Que remarquez vous. Expliquez.