Exercice 3

SSH et Telnet sont deux protocoles réseau qui permettent aux utilisateurs de se connecter à des systèmes distants et d’exécuter des commandes sur ceux-ci.

L’accès à la ligne de commande d’un hôte distant est similaire dans les deux protocoles, mais la différence principale de ces protocoles dépend de la mesure de sécurité de chacun. SSH est hautement sécurisé que Telnet.

Par défaut, SSH utilise le port 22 et Telnet utilise le port 23 pour les communications, et les deux utilisent le standard TCP.

SSH envoie toutes les données dans un format crypté, mais Telnet envoie les données en texte brut. Par conséquent, SSH utilise un canal sécurisé pour transférer des données sur le réseau, mais Telnet utilise une manière normale de se connecter au réseau et de communiquer.

De plus, SSH utilise le cryptage à clé publique pour authentifier les utilisateurs distants, mais Telnet n’utilise aucun mécanisme d’authentification.

Exercice 9

1) netstat : Il livre des statistiques de base sur toutes les activités de réseau et donne par exemple des indications sur le port et l’adresse sur lesquels une connexion (TCP, UDP) est établie, mais également des indications sur quels ports sont ouverts pour des demandes.

2) option de la commande netstat :

.netstat -a lister tous les ports (TCP et UDP) en état d'écoute

.netstat-at

lister uniquement les connexions du port TCP (Transmission Control Protocol)

.netstat -au affiche

toutes les connexions du port UDP (User Datagram Protocol)

.netsat-r permet d'afficher la table de routage IP du noyau