TP3-1 : Netcat et ssh
M1-DNR2I

Gaétan Richard

25 janvier 2012

1 Découverte

Le logiciel *netcat* accessible par l'intermédiaire de la commande **nc** permet d'établir des connexions en écoutant (avec l'option *-l*) ou en se connectant à un port donné.

Lancez un **nc** qui écoute sur le port `13579` de votre machine. Connectez-vous sur ce port (à l'aide de la commande **nc** également).

Question 1 *Que se passe-t-il ?*

Question 2 *Comment se passe la fin de connexion ?*

Relancer la commande **nc** pour écouter sur un port précis de votre machine.

Question 3 *Que se passe-t-il si vous choisissez un port inférieur à* 1024 *?*

Demandez alors à votre voisin de se connecter sur le port de votre machine sur lequel votre service est à l'écoute.

Question 4 *Que se passe-t-il ?*

Question 5 *Que faudrait-il faire pour que le service continue après la fermeture de la connexion.*

2 Faire un serveur

Pour faire simplement un serveur, il est possible d'utiliser la variante **nc.traditional** qui accepte l'option *-c* donnant un script a exécuter (note : par rapport à **nc**, il faut faire précéder le port d'écoute de l'option *-p*).

Question 6 *Écrire un script qui à chaque fois qu'il reçoit le mot clef* `LIST` *sur l'entrée standard, renvoie la liste des fichiers présents dans le répertoire courant.*

Question 7 *Faire de ce script un service disponible sur le réseau à l'aide de la commande* ***nc.traditional****.*

Question 8 *Enrichir ce service pour reconnaître les commandes suivantes :*
- *`QUIT` pour quitter ;*
- *`HEAD` <*fichier*> pour afficher les premières lignes du fichier donné en argument.*

Question 9 *Que se passe-t-il si votre voisin se connecte sur ce service ? Quels sont les droits utilisés ?*

3 Forward ssh

La commande **ssh** permet de se connecter (de manière sécurisée) sur une machine distante.

Question 10 *Connectez-vous sur la machine de votre voisin et observer les différences obtenues sur les commandes* ***hostname*** *et* ***who****.*

Question 11 *Comment reconnaître sur quelle machine se trouve un terminal ?*

La commande **ssh** accepte également de prendre une commande comme argument supplémentaire.

Question 12 *Essayez de lancer la commande* ***ps*** *sur la machine distante.*

Il est également possible d'utiliser **ssh** pour effectuer des rebonds de connections par l'intermédiaire des options *-L* et *-R*.

Question 13 *À l'aide du manuel de* ***ssh*** *faites en sorte que le site web* www.google.com *soit accessible sur le port* 8080 *de votre machine.*