

SERVEUR TELNET.
<http://nassih.com>
© MOHAMED NASSIH.

1. Introduction.

L'objectif du protocole Telnet est de permettre l'accès à distance à d'autres ordinateurs sur Internet. La machine serveur doit configurer un service Telnet en attente des connexions. Les clients Telnet utilisent une application cliente pour effectuer la connexion. Telnet est un protocole de la couche application du modèle TCP/IP -et de la couche session du modèle OSI-, qui utilise le protocole TCP de la couche transport pour établir la connexion et échanger les données – Voir Figure 1.1 -.

Application	Telnet, FTP, RPC, etc.
Transport	TCP, UDP
Réseau	IP, ICMP, IGMP
Liaison	Carte réseau et pilote (driver)

Figure 1.1 : Modèle TCP/IP

2. Installation du serveur Telnet.

Nous avons besoin de deux RPMs à télécharger à partir du site <http://rpmfind.net/linux/> :

telnet-server-0.17-25.i386 et xinetd-2.3.10-6.i386.

Xinetd remplace TCP Wrappers (inetd). Il est installé maintenant par défaut sur RedHat. Xinetd gère la connexion de certains protocoles -telnet, pop, ftp,...- et permet d'autoriser ou d'interdire les connexions sur votre machine.

Nous devons installer donc les deux RPMs en utilisant les commandes de la figure 2.1.

```
rpm -ivh telnet-server-0.17-25.i386.rpm
rpm -ivh xinetd-2.3.10-6.i386.rpm
```

Figure 2.1. installation des RPMs.

L'étape suivante est d'autoriser le service Telnet, dans Xinetd. Pour se faire il fallait éditer le fichier `/etc/xinetd.d/telnet` et changer la valeur du champ «disable» à «no» -Voir Figure 2.2-.

```
service telnet
{
    disable = no
    flags           = REUSE
    socket_type     = stream
    wait           = no
    user           = root
    server         = /usr/sbin/in.telnetd
    log_on_failure += USERID
}
```

Figure 2.2. le fichier `/etc/xinetd.d/telnet`.

Pour que Xinetd prend en compte cette modification il faut le réinitialiser en utilisant la commande de la figure 2.3.

```
service xinetd restart
```

Figure 2.3. redémarrage du service Xinetd

On va permettre 10 sessions Telnet sur notre serveur en éditant le fichier `/etc/securetty` et en ajoutant les dix lignes suivantes :

```
pts/0
pts/1
pts/2
pts/3
pts/4
pts/5
pts/6
pts/7
pts/8
pts/9
```

Maintenant vous pourrez se connecter à votre serveur à partir de n'importe quel ordinateur sur le réseau.

3. Conclusion.

C'est très important de mentionner que toute communication est transmise en clair sur le réseau durant une connexion Telnet, mots de passe compris !! Il est facile donc d'intercepter le trafic Telnet, il est préférable d'utiliser des protocoles cryptés -comme SSH- pour obtenir un accès en ligne de commande sécuritaire.