La configuration réseau sous Linux (2)

Arnaud Goulut et Ludovic Terrier

Avril 2010

1 Partie 1 : Les niveaux d'exécution

1.1 Paramétrage du service réseau

On retrouve le paramétrage du service réseau dans le fichier : `/etc/init.d/network` :

```
#! /bin/bash
#
# network       Bring up/down networking
#
# chkconfig: 2345 10 90
# description: Activates/Deactivates all network interfaces configured to \
#              start at boot time.
#
### BEGIN INIT INFO
# Provides: $network
# Should-Start: iptables ip6tables
### END INIT INFO
```

La ligne contenant *chkconfig* nous indique que ce service est par défaut démarré dans les runlevels 2, 3, 4 et 5 avec la priorité 10. De plus, il est stoppé dans les autres runlevels (1 et 6) avec la priorité 90.

1.2 Exécution des scripts

Les commandes liées à l'exécution des scripts sont situées dans le dossier `/etc/init.d/` qui sont les cibles des liens symboliques situées dans le dossier `/etc/rcX.d`, où `X` est le numéro du runlevel.

1.3 La commande chkconfig

Cette commande permet de modifier le paramétrage des différents services dont celui du réseau. On peut tout d'abord vérifier les états au démarrage d'un service donné pour chaques runlevels avec la commande :

```
chkconfig --list network
```

De plus, on peut modifier l'état au démarrage d'un service pour les runlevels avec la commande :

```
chkconfig --level 5 network off
```

Dans ce cas, le service `network` ne démarrera pas dans le runlevel 5.

2 Partie 2 : le super-serveur xinetd

Le serveur xinetd permet d'économiser des ressources en stoppant temporairement les services qui ne sont pas utilisés. Quand il est installé et rattaché à un service, xinetd se met en écoute à la place du service et le redémarre pour traiter les requêtes qui lui sont destinées.

2.1 Configuration de telnetd

Dans le cadre du TP la configuration de telnetd pour xinetd a simplement consisté en l'installation de ces deux paquets. En effet, en installant le paquet telnetd sur une machine xinetd s'installe automatiquement (sous Fedora). De plus, l'installation créée automatiquement le fichier de configuration du service telnet pour xinetd : `/etc/xinet.d/telnet`. Cependant, pour que le serveur telnet accepte des connexions, il faut indiquer dans ce fichier `no` à la place de `yes` à la ligne suivante :

```
        disable             = no
```

2.2 Les services à rattacher à xinetd

Il est préférable de rattacher à xinetd des services qui sont peu utilisés, tels des services d'accès à distance. En revanche, pour des services recevant de nombreuses connections (tel que web, ldap et messagerie) on n'utilisera pas xinetd.

2.3 Capture de session telnet

```
192.168.3.129   192.168.3.1     TCP      53105 > telnet [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=4820896
192.168.3.1     192.168.3.129   TCP      telnet > 53105 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
192.168.3.129   192.168.3.1     TCP      53105 > telnet [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSV=4820897 TS
```

FIGURE 1 – Etablissement d'une connexion TCP pour telnet.

Nous voyons ici les échange SYN, SYN/ACK et ACK à l'initiative du client pour établir la connexion telnet. Nous pouvons remarquer le port utilisé par le client : 53105. Le Maximum Segment Size (MSS) est de 1460 octets et la fenêtre (Win) à une taille de 5840 octets pour le client.

```
    15 0.367325          192.168.3.129        192.168.3.1          TELNET   Telnet Data ...

▽ Transmission Control Protocol, Src Port: 53105 (53105), Dst Port: telnet (23), Seq: 156, Ack: 55, Len: 3
    Source port: 53105 (53105)
    Destination port: telnet (23)
    [Stream index: 0]
    Sequence number: 156    (relative sequence number)
    [Next sequence number: 159    (relative sequence number)]
    Acknowledgement number: 55    (relative ack number)
    Header length: 32 bytes
  ▷ Flags: 0x18 (PSH, ACK)
    Window size: 5888 (scaled)
```

FIGURE 2 – Paquet numéro 15 de la communication TCP.

La figure précédente montre en détail le contenu TCP du paquet 15. Le client envoie l'ACK 55, c'est à dire qu'il attend l'octet 55 dans le prochain paquet. On remarque aussi la taille de la fenêtre (« Window size ») qui est de 5888 octets. Dans le paquet suivant (Figure 3), on voit que le serveur envoie effectivement l'octet numéro 55 (Seq). Ce qui correspond bien aux attentes du client.

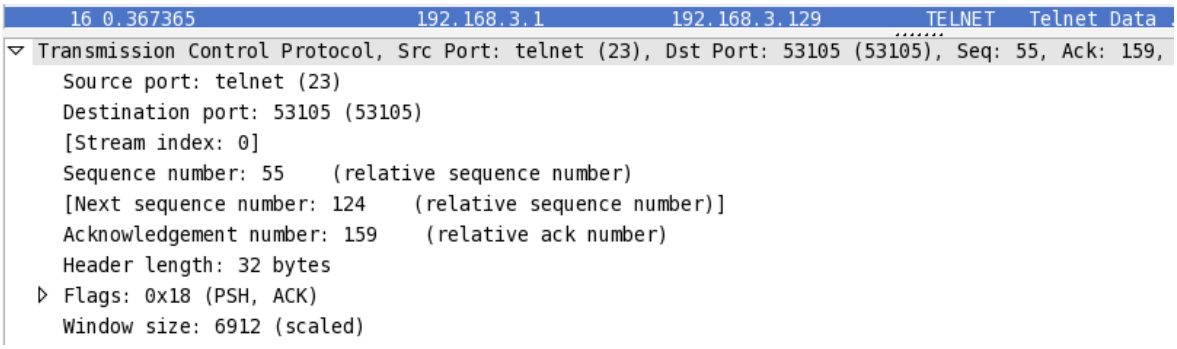

FIGURE 3 – Paquet numéro 16 de la communication TCP.

2.4 Filtrage d'accès

Ils existent deux moyens pour filtrer l'accès à un service :
- via les fichiers `/etc/hosts.allow` et `/etc/hosts.deny` (utilisant le TCP Wrapper),
- dans le fichier de configuration du service.

2.4.1 `host.deny` et `host.allow`

Pré-requis : le fichier *allow* est prioritaire sur le fichier *deny*.

```
# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
ALL EXCEPT in.telnetd: 192.168.3.0/255.255.255.0
```

Ainsi, avec la ligne précédente on autorise personne (`ALL`) sauf pour le service telnet (`in.telnetd`) qui sera autorisé pour le réseau local (`192.168.3.0`).

2.4.2 fichier de configuration

```
# default: on
service in.telnetd
{
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        only_from       = 192.168.3.0
        log_on_failure  += USERID
        disable         = no
}
```

2.4.3 permissif ou restrictif ?

La stratégie qui semble la plus sûre est celle utilisant un filtrage restrictif puisque l'on spécifie explicitement ce que l'on veut autoriser ; donnant plus de contrôle sur les accès à destination de la machine.

3 Partie 3 : Serveurs d'accès distant

3.1 Attache à xinetd

Pour rattacher un nouveau service, ici ssh, à xinetd, il suffit de créer un fichier de configuration dans `/etc/xinet.d/` en ajoutant le paramètre `server_args = -i` et en stoppant le service ssh :

```
# default: on
service ssh
{
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/sshd
        server_args     = -i
        log_on_failure  += USERID
        disable         = no
}
```

Après divers tests on s'aperçoit que le temps d'accès au service ssh n'est que sensiblement augmenté après le rattachement de celui-ci à xinetd.